

諸外国の個人情報保護制度に係る最新の動向に関する調査研究

報 告 書

平成 30 年 3 月

渥美坂井法律事務所・外国法共同事業

はじめに

慶應義塾大学名誉教授・弁護士
安富潔

「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」(平成 27 年 9 月 9 日法律第 65 号)により改正された「個人情報の保護に関する法律」(平成 15 年 5 月 30 日法律第 61 号)が、平成 29 年 5 月 30 日に全面施行されたところである(以下、改正後の個人情報の保護に関する法律を「法」という。)。法附則第 12 条第 3 項は、法の施行後 3 年ごとに、個人情報の保護に関する国際的動向、情報通信技術の進展、それに伴う個人情報を活用した新たな産業の創出及び発展の状況等を勘案し、新法の施行の状況について検討を加え、必要な措置を講ずることを求めている。この際、国際的動向として、諸外国の個人情報保護に関する制度の概要及び最新の動向を適切に捉えた上で、検討することが必要である。

また、「個人情報保護委員会」(法第 59 条)は、個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報の適正な取扱いの確保を図ることを任務としており、そのために「法第 61 条第 1 号ないし第 6 号に掲げる事務を行うために必要な調査及び研究に関すること。」及び「所掌事務に係る国際協力に関すること。」を所掌事務としており(法第 61 条第 7 号及び第 8 号)、諸外国の個人情報保護に関する制度についての調査及び研究を行うことや適切な国際協力のために情報収集をすることとされている。

このため、本調査では、諸外国の個人情報保護制度に係る最新の動向について、調査を行うこととし、特に、今後の個人情報取扱事業者の個人情報の取扱いなどに関する監督のあり方の検討に資するため、個人情報の漏えい等事案発生時の本人や監督機関等への報告義務などについて、調査を行った。

その対象国及び国際機関は次のとおりである。

北米 : 米国、カナダ

アジア・大洋州 : インド、インドネシア、オーストラリア、韓国、シンガポール、タイ、中国、ニュージーランド、フィリピン、ベトナム、ロシア

国際機関 : アジア太平洋経済協力 (APEC)、経済協力開発機構 (OECD)、欧州評議会 (CoE)

調査事務局においては、国内外で個人情報保護の実務に携わる法律専門家によって法令、年次報告書、裁判例及び学術文献等の調査を行うことに加え、諸外国の個人情報保護に知見を有する有識者に複数回のヒアリングを行い、2 名のアドバイザーによる監修を経た。

これにより、個人情報の漏えい等事案発生時の本人や監督機関等への報告義務を中心に、上記諸国及び国際機関の個人情報保護に関する制度及び最新の動向を収録することができ

た。

現在では、事業者の多くは、各国に拠点を設け、インターネットを通じて世界中で事業を営んでおり、我が国以外の個人情報保護法（Data Protection Act）への対応を迫られている。このことから、各国の個人情報保護に関する制度に対する事業者の関心は高いものとなっている。

上記諸国及び国際機関の中には、我が国との取引等が増大しており、これに伴って個人情報のやり取りが盛んになっているにもかかわらず邦語文献が極めて乏しい国や、体系化された個人情報保護制度が構築されておらず、散逸した法令等を理解しなければ個人情報保護に関する制度の理解が困難な国が含まれており、本報告書は、上述した状況下にある事業者に対して有益な情報提供となろう。

最後に、本調査にご協力いただいた有識者、膨大な報告書の執筆及び監修を行っていた調査事務局及びアドバイザー、有益なご示唆を頂いた個人情報保護委員会事務局に深く御礼申し上げる次第である。

以上

諸外国の個人情報制度に係る最新の動向に関する調査研究
有識者・アドバイザー名簿

<有識者>

林 いづみ 桜坂法律事務所 パートナー弁護士

寺田 麻佑 理化学研究所 革新知能統合研究センター 客員研究員

湯浅 壘道 情報セキュリティ大学院大学学長補佐・情報セキュリティ研究科 教授

小向 太郎 日本大学 危機管理学部 教授

横田 明美 千葉大学大学院社会科学研究院 准教授

<アドバイザー>

生貝 直人 東京大学大学院 客員准教授

板倉 陽一郎 ひかり総合法律事務所 パートナー弁護士

一般財団法人日本情報経済社会推進協会 (JIPDEC)

Data Protection Acts



目次

一覧表	6
I. 諸外国	9
1. アメリカ.....	9
2. カナダ.....	47
3. オーストラリア.....	70
4. ニュージーランド.....	96
5. 中国.....	112
6. 韓国.....	139
7. シンガポール.....	170
8. タイ.....	197
9. ベトナム.....	222
10. フィリピン.....	246
11. インドネシア.....	266
12. インド.....	281
13. ロシア.....	304
II. 国際機関	328
1. OECD.....	328
2. APEC.....	341
3. CoE.....	367

一覧表

項目/国名	アメリカ	カナダ	オーストラリア	ニュージーランド	中国	韓国	シンガポール
法令の名称	連邦取引委員会法(FTC法)の他、グラム・リーチ・ブライリー法(GLBA)等はあるものの、包括的な個人情報保護法が無い(セクトラル方式)。州法も存	民間部門は個人情報保護及び電子文書法(PIPEDA)、公的部門は、ブライバシー法(Privacy Act)が規律する。業法や州法あり。	1988年ブライバシー法などの他、州法も存在する。	1993年ブライバシー法。これは、公的部門及び民間部門のすべての事業者等に適用される。	包括的な個人情報保護法は存在せず、個別分野ごとの法令等が散在している。サイバーセキュリティ法(CS法)など。	個人情報保護法の他、主な個別法として、情報通信網法、信用情報保護法、位置情報保護法がある。	PDPA他、2014年個人データ保護規則などの個別法がある。
監督機関の名称	連邦取引委員会(FTC) アメリカ合衆国保健福祉省(HHS) 連邦通信委員会(FCC)	ブライバシー・コミッション 事務所(OPC) カナダラジオテレビ・電気通信委員会(CRTC) 各州のブライバシー規則に関する独自の機関	オーストラリア情報コミッショナー事務局(OAIC) オーストラリア通信メディア庁(ACMA) 州の機関	ブライバシー・コミッション 事務局(The Office of the Privacy Commissioner, OPC)	国家インターネット情報弁公室(CAC)	個人情報保護委員会(PIPC)、行政安全部、放送通信委員会(KCC)、科学技術情報通信部等。	個人情報保護委員会(PDPC)、シンガポール情報通信メディア開発庁(IMDA)
漏えい等事案発生時の本人及び監督機関等への報告義務に関する規定	FTC法は個人情報漏えいについての報告義務を明示的に課していないが、FTCは企業に消費者の個人情報に関する安全管理措置を行うことを求める。	2015年、デジタルブライバシー法により、漏えい通知のルールがPIPEDAに追加された。	2017年、データ漏洩の通告義務要件をブライバシー法に盛り込んだ、改正法を制定した。	ブライバシー法上、違反の当局への報告義務はない。ガイドラインにより、ブライバシー・コミッショナー及び被害者に対する報告が推奨されている。	CS法は、ネットワーク運営者の個人情報漏洩、改ざん、毀損の不作为義務などを定めている。	個人情報保護法によると、個人情報処理者は個人情報の流出を知ったとき、遅滞なく当該情報主体に通知しなければならない。	PDPAに明確な規定がないが、PDPCはその各種ガイドラインで、組織が、影響を受けた個人とPDPCに対して自主的に通知を行うよう奨励。
安全管理措置に関する規定	FTCは、企業に対して、消費者をデータの窃用又は悪用から保護する義務を課している。	PIPEDAは情報の機密性に見合った保護措置による個人情報の保護を義務付けている。	APP11項は、事業者に対し、個人情報の安全性を確保する積極的な措置を取ることを義務付けている。	ブライバシー法は、情報ブライバシー原則により個人情報の不正利用防止のための安全管理措置を採るべきことが定められている。	各業界の個別規定以外に、CS法の下に存在する。	個人情報保護法は、個人情報取扱者が、個人情報を紛失・漏洩等しないよう内部管理計画等の安全性確保に必要な技術的・管理的・物理的措置を要請。	PDPAは、不正なアクセス、収集、使用、改ざん、処分等及び類似のリスクを防止するため適切なセキュリティの実施を義務づけている。
紛争処理手続き	連邦取引委員会に権限あり。ブライバシー侵害の集団訴訟はよく見られる。	PIPEDAの定める紛争解決手続きにより、ブライバシー・コミッショナーが関与する。	ブライバシー法は、ブライバシー権が侵害されたと考えた場合、OAICコミッショナーに訴えることができる旨定める。	ブライバシー侵害の申立はブライバシー・コミッショナーに対して行い、調査、追加措置発動の検討、和解勧告、及びオンブズマン等への付託等なされる。	個人情報が侵害されたという理由で直接に損害賠償請求訴訟が可能(民法総則、消費者保護法等)。CS法には情報の削除、訂正要求の定めがある。	個人情報関連紛争の調整を求める者は、個人情報紛争調整委員会に紛争調停を申請することができ、審査後に調停案が作成される。	民事訴訟、PDPCによる調停の指示といった手段がある。PDPCは、申立てにより、組織の回答を調査し、組織に必要な措置を行うよう指示できる。
越境移転	アメリカと欧州の間にブライバシー・シールドがある。またアメリカとAPEC間にはAPEC越境ブライバシー・シールド・システムがある。	PIPEDAに特別な定めはないが、PIPEDA上の説明責任原則に従う。PIPEDAを含むカナダの法律によると越境移転について国の監督機関に届出又は許可を得る必要はない。	越境開示はAPP8項に従う必要がある。APP8項は、越境開示にアカウントビリティの手法を導入し、国外の受領者に対する個人情報の開示も制限している。	ブライバシー法上移転に対してコミッショナーへの通知義務はない。事業者が同一法人内の国外事業所にデータ移転したとき当該個人情報にも情報ブライバシー原則の適用あり。	CS法に規定があり、業務の需要の為に国外向けに提供する場合によっては安全評価を受ける義務を定めている。	個人情報保護法には情報主体の同意を受けなければならない。同法に違反して個人情報の国外移転に関する契約を締結してはならない旨の規定がある。	個人情報保護規則に海外移転の要件が規定されている。APECのCBPR及びブライバシー取扱者認証制度への加盟も果たした。

※この表は、本調査の主要な調査事項(監督機関、漏えい等事案発生時の本人及び監督機関等への報告義務に関する規定安全管理措置に関する規定、紛争処理手続き等)を一覧性を重視して要点のみ簡潔にまとめたものです。法令の名称については、民間部門、公的部門の別がある場合、また州法が存在する場合には、それらが存在している旨記載しています。

項目/国名	タイ	ベトナム	フィリピン	インドネシア	インド	ロシア
法令の名称	個人情報保護法は草案段階。憲法はプライバシー権に対する保護を与えており、その他、コンピュータ犯罪防止法、公的情報法等がある。	サイバー情報保護法などの個別法により分野ごとに規制がある。	Data Privacy Act of 2012 (DPA)。DPAは民間及び公的部門の双方に適用されるが、例外あり。	ITE法、GR82/2012、MoCI Reg. 20/2016、銀行法等	2000年IT法、2011年個人情報規則。その他、何らかの形でデータ保護の付与を根拠づける、一定の付随的法律、方針及び指針がある。	個人情報法が公的部門・民間部門に適用される。その他産業部門ごとに個別法が規定されている。
監督機関の名称	中央監督機関は存在しないが、特定の産業及び政府機関の個人情報保護対策を管轄する監督機関がある。公的情報法に基づく情報公開裁判所等。	個人情報保護に関連する法律の執行監督について単独で責任を負う政府機関は設置されていない。	National Privacy Commission (NPC)	特定の機関は存在しないが、個人データ保護実施状況の監督は、MoCI及び/又は部門規制・監督機関の長官により直接的/間接的に行われる。	データ保護及びデータ・プライバシーを扱う特定の当局はないが、CA(IT法に基づき監督任務を行う)、CCA(電子署名証書に関する監督当局)が存在。	連邦通信・情報技術・マスコミ監督庁 (Roskomnadzor)
漏えい等事案発生時の本人及び監督機関等への報告義務に関する規定	公的情報法には、個人情報が流出し、公衆に知られる可能性が発生した場合、国家機関は、本人に通知しなければならないと定められている。	監督機関や個人等に対する報告義務を規定する法令はないが、サイバー情報保護法は、サイバー情報保護のために適切な措置を講じる義務を定める。	個人情報管理者は、個人情報が無権限者に取得される場合、NPCに通知し、本人に損害が発生する場合、個人情報管理者/NPCが、本人に通知。	MoCI Reg. 20/2016にESPの通知義務あり。GR 82/2012も、個人データの所有者への書面通知を要求。ITE法は、監督当局及び本人に対する報告義務に関する条文を定めていない。	IT法に漏えい時の当局への報告義務の定めあり。個人情報規則は苦情申立について規定。	強制的なデータ漏えい通知について定める法律はない。データ漏えいの排除についてデータ対象者及びRoskomnadzorに通知する要件がある。
安全管理措置に関する規定	個人情報保護法草案において義務規定あり。その他、2017年改正コンピュータ関連犯罪法などの法令に、安全管理措置に関する規定が定められている。	サイバー情報保護法は、管轄の国家機関並びにその他の組織及び個人との協力等による、安全管理措置をとることを要求している。	DPAに、データ保護担当者等の任命義務、物理的安全管理措置義務、技術的安全管理措置義務が規定されている。	MoCI Reg. 20/2016はESPに対し義務を課している。ITE法、GR 82/2012には、安全管理措置に関する条項はない。	個人情報規則に、合理的セキュリティ実務に関する規定がある。	個人情報法が、データ管理者が取るべき措置を定めている。
紛争処理手続き	公的情報法下で、国家機関が、本人の要求に沿って個人情報を修正、変更、削除しなかった場合、情報開示裁判所に異議を申し立てることが可能。	個人情報保護に関する紛争手続きについて特別な定めはなく、個人情報処理に関する紛争処理手続きには、一般的な手続規則が適用される。	NPCは、個人情報管理者によるDPA 遵守を確保することを任務とするが、苦情を受け、調査を実施し、ADR手続により紛争解決を調整する機能を有する。	MoCI Reg. 20/2016に規制あり。個人データ所有者及びESPIは、MoCIに対し、個人データの保護の怠慢に苦情を申立て、審議/和解等を通じて解決される。	IT法違反が生じた場合、裁定官に申し入れを行うことができる。裁定官は、民事裁判所としての権限を有し、裁定する。	データ保護の特別な手続は無く、一般手続に係る規則が適用される。事業活動の実施に関連する紛争は、特別商事裁判所により解決される。
越境移転	電子通信業法は越境移転の場合には利用者の同意等が必要であるが、情報の海外送信ないし移転を規制する通知が権限ある委員会によって発せられることがあると規定する。	ベトナム法では越境移転について定める法令は存在しない。	DPAには越境移転の規定が存在しないが、個人情報管理者は国内又は国際的であるかを問わず第三者に対して移転された個人情報について引き続き責任を負うと定めている。	MoCI Reg. 20/2016には電子システム提供者が管理する個人情報を域外に移転する場合には監督機関と連携して行う等の規制が存在する。	個人情報規則によると、法人がインド国外の法人に対して個人情報を移転することを許可しているが、契約の履行の為に必要であることや本人が同意した場合に限定されている。	個人情報法は個人情報の移転先の法域の適切性によって越境移転の条件を区別し、個人情報は同法の一般規則に従い十分なレベルの保護が与えられている法域に移転できる。

項目／機関名	OECD	APEC	CBPRs	CoE
法令の名称	OECD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	APECプライバシー・フレームワーク(APEC Privacy Framework)	APEC越境プライバシー・ルール・システム(APEC Cross Border Privacy Rules System, CBPRs)	欧州評議会条約第108号(個人データの自動処理)、欧州評議会条約第181号(監督機関、越境データ移転)
漏えい等事案発生時の本人及び監督機関等への報告義務に関する規定	重大なセキュリティ違反の場合、監督機関に対し、及びデータ主体に悪影響を及ぼす可能性が高い場合には、個別のデータ主体に対し報告義務あり。	漏えい等事案発生時の報告義務に関する具体的な規定は定めていない。		現時点で存在しないが、現在改定が検討されている条約のドラフトにおいて、新たにデータに関する違反の申告義務が追加されている。
安全管理措置に関する規定	個人データは、損失又は不正アクセス、破壊、使用、修正又は開示に対する合理的なセキュリティ管理措置で保護する(安全管理保護の原則)。	個人情報管理者は、個人情報情報の滅失、不正アクセス、不正な破壊、利用、変更及び開示のようなリスクに対する適切な安全管理措置を整備すべきとする。	CBPRsにおいても安全管理措置に関する規定が存在する。	自動化されたデータファイル内に保存される個人データの保護に関し、適切なセキュリティ対策を講じなければならない旨、一般的に規定されている。
越境執行協力(制度の名称、採択・施行時期)	2007年6月12日に、プライバシー保護法の執行に係る越境協力に関する勧告(「OECD勧告」)が採択された。	APEC越境プライバシー執行協定(CPEA) 2009年11月、APECの閣僚会議において承認され、2010年7月から開始。	CBPRsは、2011年11月閣僚会議で承認。2012年7月に公表。CPEAへの参加はCBPRsに参加するための前提条件とされている。	条約第108号及び追加議定書に加盟国間の協力に関する規定が含まれる。
越境執行協力の適用範囲(対象国及び拘束の程度)	OECD勧告では、加盟国が、プライバシー保護の有効性向上のため、自国の執行制度と法律を改善する誓約が示されているが、加盟国に拘束力はない。	10のAPECエコノミーがCPEAに参加。拘束力ある義務を創設せず、国際・国内法の義務に影響を及ぼさず、参加エコノミーの法体系で義務を創設しない。	米国、メキシコ、日本、カナダ、韓国及びシンガポールがCBPRsに参加している。	条約第108号及び追加議定書に準拠するものであり、署名国に宛てられ、これらに対して拘束力を有することとなる。
越境執行協力の内容	協力実現のための措置を構築し、プライバシー執行機関による国際協力を促進することを加盟国に求め、これを受けてGPENが設置された。	CPEAは、APECエコノミー間での、越境プライバシー執行における協力の実践的な多国間のメカニズムを提供する。	個人情報管理者たる事業者が、越境個人情報保護に係る取組みに関し、APECプライバシー・フレームワークの諸原則に適合しているかを認証する。	各加盟国間の相互支援、協力について定められている。

I. 諸外国

1. アメリカ

(1) 制度概要

① 法体系の概要

アメリカ合衆国における個人情報保護は、連邦法においては包括的な個人情報保護法は策定されておらず、分野ごとに個別法が定められるセクショナル方式となっているほか、州内に関する事項については、50州における多くの州法によって規制されており、また、ワシントンD.C.においても同様に規制がなされている。

監督機関としては、連邦取引委員会（Federal Trade Commission、以下「FTC」という。）が連邦取引委員会法（Federal Trade Commission Act of 1914、以下「FTC法」という。）第5条¹に基づくその執行権限を用いてプライバシー及びセキュリティに関する実務運用を規制している²。

民間部門に適用される連邦法として重要なものは、原則としてすべての民間企業を適用対象とするFTC法、金融機関による個人情報のプライバシー及びセキュリティを規制するグラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act、以下「GLBA」という。）³と一般に呼称される金融サービス近代化法（Financial Services Modernization Act of 1999）、患者の医療情報を取扱う官民いずれの医療関連の事業者も規制する「医療保険の携行性と責任に関する法律」（Health Insurance Portability and Accountability Act of 1996、以下「HIPAA」という。）、「経済的及び臨床的健全性のための医療情報技術に関する法律」（Health Information Technology for Economic and Clinical Health Act、以下「HITECH Act」という。）、子供のプライバシーについて取り扱う「児童オンラインプライバシー保護法」（Children's Online Privacy Protection Act of 1998、以下「COPPA」という。）、電子通信等による通信等を保護する電子通信プライバシー法（Electronic Communications Privacy Act of 1986、以下「ECPA」という。）及び通信事業者に対して広く適用されるプライバシー規定を含んでいる連邦通信法（Communications Act of 1934、以下「連邦通信法」という。）等がある。これらの法律の適用範囲は、アメリカ合衆国及びその領土全域であり、FTC法は域外適用もなされ得る。

¹ 15 U.S.C. § 45。なお、U.S.C.は、United States Code（合衆国法律集）の略語である。

² <https://www.ftc.gov/site-information/privacy-policy> FTC法が原則としてすべての民間企業を適用対象としており、本分野においてFTCが第三者機関となる。

³ 法案審議を主導したグラム上院銀行委員長、リーチ下院銀行委員長、ブライリー下院商業委員長の名からGramm-Leach-Bliley Actと称される。なお、上下両院法案の審議段階では、Financial Services Modernization Act（1999年金融サービス近代化法）が正式名称であった。

公的部門に適用される連邦法としては、1974年プライバシー法（Privacy Act of 1974）がある。また、公的部門による医療分野については、HIPAA及びHITECH Actが適用される。

アメリカ合衆国は、アメリカ合衆国及び欧州連合における企業間のデータ移転を規制する欧州連合・アメリカ合衆国間のプライバシー・シールドを締結している。また、アメリカ合衆国は、APECプライバシー・フレームワーク（APEC Privacy Framework）及びAPEC越境プライバシールール・システム（APEC Cross-Border Privacy Rules System, CBPR system）に参加している。

② 民間部門に適用される主な連邦法

①で述べたように、アメリカ合衆国の連邦法において包括的な個人情報保護法は策定されておらず、分野ごとに個別法が定められるセクトラル方式となっている。個人情報に関する主要な連邦法は下記のとおりである。個別分野における規律としては、FTCレポートや民間における自主規制も重要な役割を果たしている。

- ・ 1914年「連邦取引委員会法」（FTC法）
顧客に対して行われたプライバシー及びセキュリティ保護に対して広く適用されると解釈されている、不公正若しくは欺瞞的な行為又は慣行（unfair or deceptive acts or practices）を規制する連邦法。
- ・ 1999年「グラム・リーチ・ブライリー法」（GLBA）
金融機関による個人情報の取扱いを規制する連邦法。
- ・ 1970年「公正信用報告法」（Fair Credit Reporting Act of 1970、以下「FCRA」という。）
消費者信用報告機関及び消費者信用情報の開示を規制する連邦法。
- ・ 1996年「医療保険の携行性と責任に関する法律」（HIPAA）及び2009年「経済的及び臨床的健全性のための医療情報技術に関する法律」（HITECH Act）
医療上のプライバシーを規制する連邦法。
- ・ 1998年「児童オンラインプライバシー保護法」（COPPA）
児童のプライバシーを規制する連邦法。
- ・ 1986年電子通信プライバシー法（Electronic Communications Privacy Act of 1986, ECPA）
個人による有線通信、口頭での通信及び電子通信に関し、その通信がなされた場面、通信中の場面及び通信がコンピュータに保存された場面において、それらの通信について保護する連邦法。
- ・ 1934年連邦通信法（Communications Act of 1934）
ラジオ、テレビ、有線通信、衛星通信に関する業務を取り扱う電気通信会社を規制する連邦法。

また、FTC は、テレマーケティングその他の電子メール、電話又は携帯電話のメールによるマーケティングを制限する電話勧誘拒否登録制度 (Do-Not-Call Registry) 及びスパム規制法 (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003、CAN-SPAM 法) に対する権限も有する。

その他にも、適用範囲が限定的な連邦法が存在する。例えば、1988 年ビデオ・プライバシー保護法 (Video Privacy Protection Act of 1988、以下「VPPA」という。) は、個人がビデオテープ提供者 (オンライン・コンテンツの提供者を含む。) に要請又は同提供者から取得したビデオのタイトルも対象とする旨定義されている「特定の個人を識別可能な情報 (Personally identifiable information, PII)」の取扱いについて定める。

③ 公的部門に適用される主な連邦法

1974 年プライバシー法 (5 U.S.C. § 552a) は、公的部門における個人情報の取扱いを規制する。連邦政府機関が記録システムにおいて維持する個人に関する情報の収集、保全、利用及び提供について定める公正情報実務諸原則 (Fair Information Practice Principles, FIPPs) を制定している。HIPAA 及び HITECH Act は、保護対象医療情報 (protected health information, PHI) を取扱う公的部門について規制する。

④ 個人情報に関する州法

アメリカ合衆国において、連邦法は州際に関与する事項を規定し、州法は州内の事項を規定する。また、連邦法は州法に優位する⁴。個人情報に関連する州法は 100 を超える。

例えば、カリフォルニア州においては、25 を超える個人情報に関する州法が制定されている。2013 年に、未成年のプライバシー保護の一環として、未成年者のオンラインでのプロフィールを制限する規定や、未成年者からソーシャルメディアなどにおける投稿内容の削除要請があった場合はそれに応じなければならないといった規定を設けている。

個人情報漏えいなどのセキュリティ侵害に関する消費者等に対する報告義務については、連邦法には基本的に規定されていないが、多くの州法において規定がある。2002 年にカリフォルニア州が初めてセキュリティ侵害に関する通知を要求する州法を制定し、現在では、ほぼすべての州とワシントン D.C. においてセキュリティ侵害についての消費者等に対する報告義務要件を設けている。一般に、これらのセキュリティ侵害の通知に関する州法は、企業に対して、クレジットカード番号、社会保障番号、運転免許証番号という列挙された

⁴ 最高法規条項 (Supremacy Clause, United States Constitution (Article VI, Clause 2) アメリカ合衆国憲法第 6 編 2 項) により、連邦法の州法に対する優位が定められており、連邦法に専占 (preemption) される場合には連邦法が適用される。

トリガー・データ⁵と組み合わせられた氏名への権限のないアクセスについて、消費者に対し通知することを要求しており、さらに、規制機関又は報道機関に対しても通知を要求することもある。なお、窃取されたデータが暗号化されていた場合には、企業は通知を行う義務を免除されることになっているが、暗号化キー（encryption key）やセキュリティ証明書（security credential）も共に漏えいした場合にはこの限りではない⁶。

（２） 主な連邦法の概要

① 連邦取引委員会法（Federal Trade Commission Act of 1914、FTC法）

ア 法律の概要

FTC法では、第5条(a)において、「不公正な競争方法」（unfair methods of competition）及び「不公正若しくは欺瞞的な行為又は慣行」（unfair or deceptive acts or practices）を禁止している⁷。FTCは本条文を企業のプライバシー及びセキュリティデータ保護ポリシーを規制するために用いてきている⁸。例えば、不公正若しくは欺瞞的な行為又は慣行として、消費者のプライバシー侵害や不適切な広告表示も含まれるとされる。違反行為に対する措置としては、差止請求、排除命令、民事制裁金、和解手続等が規定されている。

イ 個人情報定義

FTC法の中には明示的規定はないが、「FTC報告書：急速に変化する時代における消費者プライバシー保護」（FTC Report: Protecting Consumer Privacy in an Era of Rapid Change）⁹（2012年3月）にあるように、FTCは「特定の消費者、コンピュータその他の機器に合理的に結び付けることのできるデータ」（consumer data that can be reasonably linked to a specific consumer, computer, or other device）を個人情報として保護すべきものとしている。

⁵ いくつかの州は、トリガー・データを、医療情報、生体認証識別子（biometric identifier）、パスワード、さらに署名も含める形で拡張している。

⁶ カリフォルニア州法（2017年改正）等

⁷ FTC法は独占を禁止する法律として1914年に可決され、1938年には「不当な競争手段」に加え、「不公正若しくは欺瞞的な行為又は慣行」を禁止すべく改正された（FTC法5条、15 U.S.C. §45(a)(1)、(2)）。

⁸ 小向太郎「米国FTCにおける消費者プライバシー政策の動向」2頁を参照。

http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/08/08-6komukai2014.pdf

⁹

<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

ウ 主な規制・権利の内容

FTC 法は、原則としてアメリカ合衆国内のすべての企業に対して適用される¹⁰。

FTC 法第 5 条は、「不公正若しくは欺瞞的な行為又は慣行」に適用される。FTC 法第 5 条に基づき、FTC は、排除命令を出し、民事制裁金を課し、提訴を行う権限を有する。

FTC は、FTC 法第 5 条の文言の解釈について、1980 年に「不公正に関する政策表明」(FTC Policy Statement on Unfairness)¹¹を公表し、また、1983 年に「欺瞞に関する政策表明」(FTC Policy Statement on Deception)¹²を公表し、不公正又は欺瞞に該当するか否かを判断するために必要な諸要素を示している。それによれば、「不公正」(Unfairness)については、消費者の権利侵害に関して、①その侵害が実質的 (substantial) なものか、②その侵害によってもたらされる不利益が、その侵害によってもたらされる消費者や競争上の利益を超えるものであるか、③その侵害が消費者が合理的に避けることができないものであるか、という要件を掲げている。また、「欺瞞」(deception) に該当するか否かは、①その慣行などが消費者にとってミスリーディングか、②合理的に行動する消費者の観点からその慣行などを吟味する、③その慣行などが重大なものであるか、といった点から検討するとしている。

FTC 法は、全ての消費者データ (consumer data) に適用される。データ処理は、FTC 法の「告知及び同意」(notice and consent) のアプローチによるデータ主体の同意に基づいて、FTC により全般的に規制を受ける。なお、同意の形式については、FTC 法では特定されておらず、一般的には、事業者のプライバシーポリシーへの黙示の同意も許容される。ただし、FTC により、一部の状況において、個人情報収集に先立ち、「積極的な明示の同意」(affirmative express consent) が義務付けられる場合がある¹³。この同意は、事業者がデータ収集時に定めた方法と著しく異なる方法により消費者の個人情報を利用することを予定している場合又は「センシティブデータ」(sensitive data) を収集する際に必要とされる。例えば、事業者は、そのプライバシーポリシーについて著しくかつ重大な変更を行った場合、消費者から「積極的な明示の同意」を取得することが義務付けられる場合がある。なお、情報セキュリティに関して言えば、多数の個人への小規模な被害も実質的なもの (substantial consumer injury) を構成し得るとされている。

¹⁰ 非営利事業体は、FTC 法の対象となっておらず、また、一定の企業 (電話会社、預貯金取扱金融機関及び保険会社等の一般的な通信事業者) についても対象とされていない。

¹¹ <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>

¹² https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf

¹³

https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf の P14 以下を参照。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

FTC 法は個人情報漏えいについての報告義務を明示的には課していないが、FTC は下記のように企業に消費者の個人情報に関する安全管理措置を行うことを求めている。

オ 安全管理措置

FTC は、企業に対して、消費者をデータの窃用又は悪用から保護する義務を課している。また、判例法によれば、企業はセンシティブな個人情報を保護するための内部的手段を確保しなければならず、その手段には、①セキュリティに関する責任を負う従業員を指名すること、②セキュリティの欠損に対処するインシデントへの対応計画を策定すること、③一定の権限を与えられた利用者のみがデータを利用できるように制約するアクセス・セキュリティを確保すること、④従業員に強力なパスワードの使用を要求すること、⑤ファイアウォールのように、インターネット上で部外者が企業のコンピュータにアクセスするのを妨げるメカニズムを利用することが含まれる。また、センシティブデータを保有する企業は、複雑なパスワードの要求などの特別な顧客保護手段を採用する必要がある。なお、企業は、顧客の個人情報を受領するベンダーを適切に監督する義務も負っている。加えて、企業は、セキュリティ、秘密及び個人情報の完全性に対する合理的に予見し得る内部的及び外部的リスクを特定するように努める必要があるほか、企業としては、FTC からその責任を追求されるのを防ぐという観点から、従業員に対して合理的なデータセキュリティ訓練を行うべきであるとされている。

カ 適用除外内容

FTC 法は、原則としてアメリカ合衆国内のすべての企業を対象とするが、FTC 法第 5 条 (a) (2) において例外が規定されており、銀行、貯蓄貸付機関 (savings and loan institutions)、連邦信用組合 (Federal credit unions)、通商を規制する法令の適用のある公衆通信業者 (common carriers)¹⁴、航空運送業者及び外国航空運送業者、並びに、パッカーズ・ストックヤード法 (Packers and Stockyards Act) が適用される個人、組合又は法人は、FTC 法の対象とはならない。

キ 小規模事業者の取扱い

FTC 法においては、小規模事業者に関する特別の規定は定められていない。

¹⁴ 電話会社等が含まれる。

ク 域外適用

明文の規定はないが、アメリカ合衆国の商業（commerce）に影響を与える場合には FTC 法の域外適用が可能である¹⁵。

ケ 紛争処理手続き

FTC は、執行措置（enforcement action）及び調査を開始する権限が与えられている。また、アメリカ合衆国連邦裁判所に訴訟を提起することもでき、その結果、その執行措置及び調査に関する和解合意である「同意命令」（consent order）が命じられる場合がある。

② 1999 年グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act, GLBA）

ア 法律の概要

GLBA に規定される財務情報に関する個人情報保護ルールは、2001 年に完全施行がなされており、具体的には 15 U.S.C. § 6801 以下において規定されているところである¹⁶。GLBA 第 501 条は議会の「プライバシー義務ポリシー」(Privacy Obligation Policy” of Congress) について以下のとおり定める。

501 条 非公開個人情報の保護（Protection of Nonpublic Personal Information）

(a) プライバシー義務ポリシー（Privacy Obligation Policy）

個々の金融機関がその顧客のプライバシーを尊重し、顧客の非公開個人情報（nonpublic personal information）の秘密やセキュリティを保護する積極的かつ継続的な義務（affirmative and continuing obligation）を負わせることが議会のポリシーである。

(b) 金融機関のセーフガード（Financial Institutions Safeguards）

(a) に定めるポリシーの促進にあたり、505 条 (a) に規定される行政機関（agency or authority）は、その管轄下にある金融機関について、①組織的（administrative）、②技術的（technical）及び③物理的（physical）なセーフガードに関し、以下の目的のために、適切な基準を確立する。

(1) 顧客の記録及び情報について、そのセキュリティと機密性を確保すること

¹⁵ FTC その他のアメリカの規制機関は、プライバシー及びデータセキュリティに関するアメリカの法令・規則は、アメリカ国外に移転されたデータにも同様に適用されるという立場を取っているとされている（森大樹編集代表『日米欧 個人情報保護・データプロテクションの国際実務』別冊 NBL162 号 157 頁）。

¹⁶ 提案されたプライバシー規則は、採択から 6 か月後に発効した。

- (2) かかる記録に関するセキュリティ又は完全性について予想される脅威又は危険から保護すること、及び
- (3) かかる記録又は情報について、顧客にとって重大な損害若しくは不都合をもたらすような不正アクセス又は不正な利用から保護すること。

イ 個人情報の定義

GLBA は、第 509 条 (4) において、「非公開個人情報」(nonpublic personal information) を、個人を特定可能な財務情報を意味すると定義しており、(i) 消費者から金融機関に対して提供され、(ii) 消費者との間の取引若しくは消費者のために履行されたサービスの結果又は(iii) 金融機関により別途取得されたものに適用される。

ウ 主な規制・権利の内容

GLBA は、金融機関が顧客から収集した個人情報を保護するための「セーフガード規則」(Financial Institutions and Customer Information: Complying with the Safeguards Rule) を設けており、プライバシー保護の運用基準を設けてこれを顧客に通知する等の「プライバシー規則」(Privacy Rule) を遵守することを義務付けている¹⁷。これは「副題 A: 非公開個人情報の開示」(Subtitle A: Disclosure of Nonpublic Personal Information) (15 U. S. C. § § 6801-6809) において成文化された。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

GLBA は個人情報漏えいについての報告義務要件について明示的には定めていないが、下記のように金融機関が顧客の個人情報に関する安全管理措置を行うことを求めている。

オ 安全管理措置

上記ウに記載のとおり、GLBA は、金融機関が顧客から収集した個人情報を保護するための「セーフガード規則」を設けており、組織的、技術的、物理的な安全管理措置を求めている。

¹⁷

<https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

カ 適用範囲

GLBA 及び同法のプライバシー要件は、「副題 A：非公開個人情報の開示」(Subtitle A: Disclosure of Nonpublic Personal Information) (15 U.S.C. § § 6801-6809) において示されているように、「金融機関」(financial institutions) に対してのみ適用される。

キ 小規模事業者の取扱い

GLBA においては、小規模事業者に関する特別の規定は定められていない。

ク 国際的な情報移転に関する規定

アメリカの金融機関は、その金融機関が利用しているサービス・プロバイダーについても、その金融機関に適用のある GLBA の規定を遵守させなければならないが、これはアメリカ国外のサービス・プロバイダーを利用している場合についても同様にあてはまる。例えば、GLBA 第 502 条(a)及び(b)は、プライバシーポリシー等の通知要件のほか、金融機関が非関連第三者 (nonaffiliated third party) に対して非公開個人情報 (nonpublic information) を開示する場合、顧客にオプトアウトの機会を提供するように定めているが、国外の非関連第三者への開示はここから除外されていない。従って、非関連第三者に対する非公開個人情報の国外移転についても、同条に基づきオプトアウトによる規制がかかってくる。もっとも、同条(e)においては、同条(a)及び(b)の例外が規定されているところ、同条(e)も国外移転か否かを区別せずに適用がなされることから¹⁸、個人情報の国外移転が当該金融機関のグループ外のサービス・プロバイダーに対して行われる場合であっても、当該国外移転が同条(e)に規定される目的で行われるようなときには、金融機関の顧客は、オプトアウトすることができない。しかしながら、この場合であっても、金融機関が負担している顧客の個人情報保護に関する「積極的かつ継続的な義務 (affirmative and continuing obligations)」の一環として、金融機関にはかかるサービス・プロバイダーの行動を監督すべき義務があるとされている。

③ 1996 年医療保険の携行性と責任に関する法律 (Health Insurance Portability and Accountability Act of 1996, HIPAA) 及び 2009 年経済的及び臨床的健全性のための医療情報技術に関する法律 (Health Information Technology for Economic and Clinical Health Act of 2009, HITECH Act)

¹⁸ 例えば、GLBA 第 502 条(e) (1)は、消費者から要求のあった又は承認された取引の執行等を行うために必要な場合には、非公開個人情報を開示できるとしているが、これは開示先が国外か否かで開示の必要性が変わるわけではないため、国外移転の場合にも適用されると考えられる。

ア 法律の概要

HIPAA は、1996 年に可決及び制定された。2009 年には、HIPAA に執行機能 (enforcement mechanism) を追加する HITECH Act がアメリカ復興・再投資法 (American Recovery and Reinvestment Act of 2009) の一部として成立した。HITECH Act の要件の多くが制定後 1 年以内に発効されたが、その一部は、別の予定日に発効されている。

HIPAA 前文は以下のことを規定している。

この法は、①団体及び個人の市場における医療保険の補償範囲の携行性及び継続性 (portability and continuity) を改善すること、②医療保険及び医療供給 (health care delivery) の浪費、詐欺及び濫用に対抗すること、③医療貯蓄口座 (medical savings accounts) の利用を促進すること、④長期のケアサービスへのアクセス及びその保障範囲を改善すること、⑤医療保険の運営をシンプルなものにすること、及び、⑥その他の目的のために、1986 年内国歳入法 (Internal Revenue Code) を修正する。

イ 個人情報 の定義

HIPAA は、プライバシー規則 (Privacy Rule) の中で、その保護対象となる医療情報を、「保護対象医療情報」(protected health information, PHI) と規定している。これはプライバシー規則の § 160.103 (45 CFR Part 160 and Subparts A and E of Part 164¹⁹に置かれている) で「特定の個人を識別可能な医療情報」(individually identifiable health information) として定義される。それは、(i) 医療機関によって作成又は受領され、(ii) 医療又は医療の提供に関連し、(iii) 当該情報について、個人を特定識別するために用いることができるかと判断する合理的根拠があるものである。

ウ 主な規制・権利の内容

医療関係の事業者は、HIPAA に基づく「プライバシー規則」(Standards for Privacy of Individually Identifiable Health Information, Privacy Rule) 及び「セキュリティ規則」(Security Standards for the Protection of Electronic Protected Health Information, Security Rule) を遵守することが義務付けられる。HIPAA は、プライバシー規則にその概要を定める特定の状況において又は個人が書面同意を行った際に限り、事業者による特定の個人を識別可能な医療情報の開示を認めている。HIPAA プライバシー規則は、45 CFR Part

¹⁹ なお、CFR は、Code of Federal Regulations (連邦行政命令集) の略語である。

160 and Subparts A and E of Part 164²⁰にあるほか、HIPAA セキュリティ規則は、45 CFR Part 160 and Subparts A and C of Part 164にある²¹。なお、HITECH Act による改正により、HIPAA におけるプライバシーやセキュリティに関する保護が強化されている²²。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

HIPAA は、個人情報漏えいについての報告義務要件について、明示的には定めていない。他方、HITECH Act は、保護対象医療情報が漏えいした場合、各個人に対する通知やアメリカ合衆国保健福祉省（The U.S. Department of Health and Human Services, HHS）に対する通知を義務付けるとともに、500人以上のPHIが漏えいしたときは、メディアに対して通報を行うように義務付けている²³。

オ 安全管理措置

HIPAA プライバシー規則及びHIPAA セキュリティ規則は、特定の個人を識別可能な医療情報に関して、その安全管理措置及びその基準を定めている。セキュリティ規則は、「適用対象の組織体」（covered entities）が個人の「電子的に保護すべき医療情報」（Electronic protected health information, e-PHI）を保護するために整備しなければならない技術及び非技術的セーフガードの概要を定めている。

（ア）HIPAA プライバシー規則

対象の事業者は、対象となる医療情報を保護するために、「組織的、物理的及び技術的セーフガード」（administrative, physical, and technical safeguards）を整備することが義務付けられている。

（イ）HIPAA セキュリティ規則

「電子的に保護すべき医療情報」（e-PHI）に対してのみ適用され、保護すべき医療情報の秘密を保持するために講じるべき処理及び技術的なセキュリティ対策に関する基準を定める。HIPAA セキュリティ規則は、「不正アクセス、改ざん、削除及び送信から保護すべき医療情報を保護するための基本的な保障措置を実施する」（implement basic

²⁰ <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>

²¹ <https://www.hhs.gov/hipaa/for-professionals/security/index.html>

²² 黒田佑輝「アメリカにおける医療情報・健康情報の利活用を支える保護制度（上）－HIPAAを中心とする保護制度の概説と事例」NBL1082号24頁を参照。

²³ <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

safeguards to protect e-PHI from unauthorized access, alteration, deletion and transmission) ことを許容する可能な方法の概要を定める。セキュリティ規則上、紙ベースのファックス、テレビ会議、音声メッセージ及び指名通話電話は、送信前に電子的形態で存在していないため、「電子的に保護すべき医療情報」(e-PHI) とはみなされない。

(ウ) HITECH Act

セキュリティ保障措置違反の基準及び違反に対する罰則を定めることで、HIPAA プライバシー規則及び HIPAA セキュリティ規則を補足している。なお、HITECH Act は、セキュリティ監査についても義務付けている。

カ 適用範囲

HIPAA は、医療機関及び医療供給者 (health-care institutions and providers) に対してのみ適用される。

これらの HIPAA プライバシー規則の適用対象の組織体 (covered entities) には、(1)健康計画 (health plans)、(2)医療情報センター (health care clearinghouses)、(3)アメリカ合衆国保健福祉省 (HHS) が採用した基準の対象となる処理に関連して全ての医療情報を電子送信する医療提供者 (health care providers) が含まれる。なお、HITECH Act は、HIPAA の直接的な適用範囲に、協力事業者 (Business associates) を追加している²⁴。

キ 小規模事業者の取扱い

HIPAA セキュリティ規則は柔軟性のある規定ぶりとなっており、適用対象の組織体が組織の規模に応じていかなる措置が適切であるかを判断するにあたり、自らその必要性を分析することを許容している。セキュリティ規則上、適用対象の組織体にとって何が適切であるかは、その組織体の規模やリソースによって異なってくる。

ク 紛争処理手続き

アメリカ合衆国保健福祉省 (HHS) は、HIPAA 違反があった場合には、連邦裁判所を通じてその執行を行うことができるほか、「課徴金」(monetary penalty) を課すこともできる。

²⁴ 前掲・黒田 26 頁以下を参照。

④ 児童オンラインプライバシー保護法 (Children's Online Privacy Protection Act of 1998, COPPA)

ア 法律の概要

COPPA は、1998 年にアメリカ合衆国議会によって可決され、2000 年に施行された。

COPPA の目的は、児童²⁵のプライバシー保護である。

イ 個人情報の定義

COPPA は、「個人情報」(personal information) (COPPA 第 6501 条 (8)) に関して、氏名、住所、オンライン上の連絡先情報、電話又は社会保障番号、生涯・時間の経過と共に、異なるオンラインサービスを通じて、ユーザーを認識するために用いることのできる「永続識別子」(persistent identifier)²⁶、児童の画像又は音声が含まれる写真、映像又は音声ファイル、正確な地理位置情報その他収集され、これら要素のいずれかと共に組み合わせられた情報を含む「特定の個人を識別可能なオンラインで収集された個人に関する情報」(individually identifiable information about an individual collected online) と定義している。

なお、FTC は、児童に関する情報、財務及び医療情報並びに正確な地理位置情報をセンシティブデータに含まれるとしている²⁷。

ウ 主な規制・権利の内容

COPPA は、収集前に「親の検証可能な同意」(verifiable parental consent) を得ることなく、13 歳未満の児童の個人情報を収集することを禁止している。これは児童オンラインプライバシー保護規則 (Children's Online Privacy Protection Rule) 第 312.5 条で定義されている²⁸。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

COPPA は、個人情報漏えいについての報告義務について、明示的には定めていない。

²⁵ 「児童」(Child) は、COPPA 第 6501 条(1)により、13 歳未満の個人 (an individual under the age of 13) をいうと定義されている。

²⁶ 16 CFR 312.2

²⁷ 前掲・森大樹編集代表『日米欧 個人情報保護・データプロテクションの国際実務』別冊 NBL162 号 147 頁を参照。

²⁸ 16 CFR Part 312

オ 安全管理措置

COPPA には、安全管理措置に関する規定は置かれていない。

カ 適用範囲

COPPA は、児童オンラインプライバシー保護規則において、1 回限りのデータ収集 (one-time collection of data)、同意のための両親のデータ (parental data for consent) その他限定された目的による収集について、児童の個人情報の収集を認める例外を定めている。

キ 紛争処理手続き

FTC は、同意命令及び COPPA の違反等に対して金銭的なペナルティを科すこともできる。

⑤ 電子通信プライバシー法 (Electronic Communications Privacy Act of 1986, ECPA)

ア 法律の概要

ECPA は、1986 年に制定及び施行された。

ECPA は、3 つの章から成っている。まず、第 1 章は、1968 年犯罪防止・街頭安全総合法 (Omnibus Crime Control and Safe Streets Act of 1968) (以下「連邦盗聴法」(Federal Wiretap Act of 1968) という。) の第 3 章を修正するものである。次に、第 2 章は、通信保存法 (Stored Communications Act, SCA) を創設するものである。第 3 章は、ペン・レジスター法 (the Pen Registers and Trap and Trace Devices Act) を創設するものである。

ECPA における改正で大規模なものとしては、1994 年の捜査当局等に対する通信傍受支援法 (Communications Assistance to Law Enforcement Act, CALEA) による改正、2001 年の米国愛国者法 (USA PATRIOT Act) による改正、2006 年の米国愛国者再認証法 (USA PATRIOT reauthorization acts) による改正、2008 年の外国情報監視法改正法 (FISA Amendments Act) による改正がある。

イ 個人情報の定義

連邦盗聴法は、有線通信、口頭の通信及び電子通信について、18 U. S. C. § 2510 において、以下のように定義している。

有線通信 (wire communication) とは、州際・国際的な通信、又は、州際又は国際商取引に影響を及ぼす通信のための施設の提供・運営に従事する者によって設置・運営された、電話線、ケーブル、又は、元の場所と受領する場所をつなぐもの (交換局 (switching station) のそのようなコネクションの使用を含む) による、通信のための機材を全般にわたり又は一部でも使用した音声の移転 (aural transfer) を意味する (18 U.S.C. § 2510 (1))。

口頭の通信 (oral communication) とは、傍受がされないことを正当に期待し得る環境下において、傍受されないことの期待 (expectation) を示す者によってなされる口頭の通信である。ただし、電子通信 (electronic communication) は含まない (18 U.S.C. § 2510 (2))。

電子通信 (electronic communication) とは、州際又は国際商取引に影響を及ぼす有線、無線、電磁気 (electromagnetic)、光電子 (photo electronic) 又は写真光学 (photo-optical) システムによって、全部又は一部が送信された性質のサイン、シグナル、書面、画像、音、データのことをいう。しかし、(A)有線又は口頭の通信、(B)音のみの呼出装置を通じた通信、(C)追跡装置 (tracking device) を使用した通信、(D)電子的な保管場所 (electronic storage) やファンドの移転のために使用される通信システムにおいて、金融機関によって保管された情報を移転する電子ファンドは含まない (18 U.S.C. § 2510 (12))。

通信保存法は、電子的な保管 (in electronic storage) がなされた電子通信 (electronic communications) について規制している。ここで、「電子的な保管」とは、(A)電氣的な移転に付随して生じる、有線又は電子的通信の一時的かつ中間的な保管 (temporary, intermediate storage)、及び、(B)かかる通信のバックアップの保護を目的とする電子的通信サービスによる通信の保管をいうと定義されている (18 U.S.C. § 2510(17))。

ペン・レジスター法は、有線の通信と電気通信の内容に関連して、加入者の電話利用状況記録装置 (pen register) ²⁹及びトラップ&トレース装置 (trap and trace devices) ³⁰の政府の使用の制限によって、有線通信と電子通信を規制している。

ウ 主な規制・権利の内容

ECPA は、①通信がなされた時点 (communications are being made)、②通信中の時点 (in transit)、③コンピュータに保存された時点 (when they are stored on computers) において、有線通信、口頭の通信及び電子通信 (wire, oral and electronic communications) を保護する法律である。ECPA は、連邦盗聴法 (Federal Wiretap Act of 1968) を改正したものである。改正の理由は、連邦盗聴法は、有線の電話回線 (hard telephone lines) で行われる通信の傍受について定めていたが、コンピュータでの通信その他デジタル通信及

²⁹ 18 U.S.C. § 3127(3)で定義されている。

³⁰ 18 U.S.C. § 3127(4)において定義されているが、基本的には、特定の通信について受信・発信元等を識別する機器類をいうとされている。鈴木滋「米国自由法—米国における通信監視活動と人権への配慮」(『外国の立法』267号)8頁を参照。

び電子通信の傍受には適用がなかったためである。さらにその後も、米国愛国法 (The USA PATRIOT Act) といったいくつかの法律が制定され、新たな通信手段やテクノロジーの発展に合わせて、ECPA も改正されていった。これらの改正の中には、法律による強制執行に基づき保存されている通信内容にアクセスすることの制限が緩和されたというものも含まれている。ECPA は、E メール、電話での会話、電子的に保存されているデータに対して適用がある。ECPA は、プライバシー情報を含む資料について、プライバシー保護を及ぼすという一般的なアプローチを採用している

具体的な内容としては、まず、ECPA の第 1 章である通信傍受法 (Wiretap Act) は、いくつかの例外はあるものの、①手段を問わず、故意による有線通信、口頭の通信及び電子通信の傍受、又は、②法律違反を犯して入手した通信内容の利用若しくは開示を禁止するというものである (18 U.S.C. § § 2510-2522)。

次に、ECPA の第 2 章である通信保存法 (Stored Communications Act、SCA) は、①サービス・プロバイダーによって保存されているファイルの内容のプライバシー、及び、②サービス・プロバイダーによって保持されている加入者 (subscriber) に関する記録内容 (例えば、加入者の名前、支払履歴、IP アドレスなどがある) のプライバシーを保護するというものである (18 U.S.C. § § 2701-12)。SCA は、権限なくして (又は権限を超えて)、有線通信又は電子通信のために利用されるシステムへのアクセスを禁止し、かつ、当該アクセスを通じて、そのシステムに保存されている有線通信又は電子通信について、アクセス、入手若しくは改ざんをし、又は、他者の権限あるアクセスを妨害することを禁止している。また、SCA は、連邦法及び州法に関して、保存されている通信内容 (stored communication) について、開示を強制するための執行手続を規定しているほか、顧客の通信内容及び記録に関するサービス・プロバイダーによる開示についても規制している (18 U.S.C. § § 2701-2712)。

ECPA の第 3 章は、加入者の電話利用状況記録装置 (pen register) 及びトラップ&トレース装置 (trap and trace devices) について定めている。第 3 章によれば、国家機関 (government entities) は、電話利用状況記録装置又はトラップ&トレース装置の設置及び利用については、その設置及び利用権限を与える裁判所の授権命令 (authorization order) を取得しなければならないとされている。ただし、実際に行われる通信それ自体については、電話利用状況記録装置やトラップ&トレース装置によって傍受されることはない。授権命令の発出は、申請者による証明書 (certification) によってなされ得る。当該証明書は、申請者が所属する機関が実施している継続中の犯罪についての捜査について、傍受によって入手できる可能性が高い情報が当該捜査に関連しているということを示している必要がある。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

ECPA には、個人情報漏えいした場合に、監督官庁等に報告を義務付けるような規定は、直接的には存在しない。しかしながら、ECPA に基づき、個人情報の漏えいに関して報告をしなかった会社に対しては、連邦訴訟 (Federal actions) が提起されている。ECPA では、故意又はそれと知って、会社が、通信内容を漏らしてしまうような電子通信サービス又はリモート・コンピューティング・サービスを提供することが禁止されている。

オ 安全管理措置

ECPA には、安全管理措置に関して直接定めた規定は存在しない。しかしながら、上記と同様に、安全管理措置を定めていない会社に対しては、連邦訴訟 (Federal actions) が提起されている。

カ 適用範囲

ECPA の第 1 章は、オペレーター及びサービス・プロバイダーについて、①サービスを提供するにあたって必要となる行為に従事する間、通常生じるような利用 (uses in the normal course of his employment)、及び、②有線通信、口頭の通信又は電子通信の傍受若しくは外国情報監視法 (Foreign Intelligence Surveillance Act of 1978, FISA) 第 101 条に規定される電子盗聴 (electronic surveillance) を法律上認められている者に関する適用除外を定めている (18 U.S.C. § 2511)。

また、ECPA は、連邦、州、その他の政府機関の職員について、有線通信、口頭の通信又は電子通信の傍受をするには、裁判所の許可が必要であると規定しているほか、許可された通信傍受を通じて取得した情報の利用及び開示を規制している (18 U.S.C. § 2516-18)。裁判官は、18 U.S.C. § 2516 に列挙されている「特定犯罪」 (particular offense) を個人が犯したこと (犯していること、犯しつつあることも含まれる) の証拠を傍受が明らかにするということを示す相当な理由 (probable cause) がある場合、30 日間を上限として、通信を傍受することを許可する令状 (warrant) を発付することができる (18 U.S.C. § 2518)。

米国連邦裁判所第 9 巡回区控訴裁判所 (The U.S. Court of Appeals for the Ninth Circuit) は、第一審裁判所の召喚状 (subpoena) の破棄について判断した際、外国人は ECPA の保護を受けるとした (18 U.S.C. §§ 2510-2522 (*Suzlon Energy Ltd. v. Microsoft Corp.*, No. 10-35793 (9th Cir. Oct. 3, 2011)))。かかる判示をするにあたって、裁判所は、ECPA は、「全ての者」 (any person) について適用され、従って、米国に保存されている全てのデータについて適用があるとした。なお、ECPA は、米国外に保存されているデータについては、適用はない。

キ 小規模事業者の取扱い

ECPA においては、小規模事業者に関する特別の規定は定められていない。

ク 域外適用

上記のとおり、米国連邦裁判所第 9 巡回区控訴裁判所 (The U.S. Court of Appeals for the Ninth Circuit) によれば、ECPA は、「全ての者」(any person) に対して適用があるとされているところである。しかしながら、アメリカ国外において保管されているデータには、ECPA の適用はないとされている。

ケ 紛争処理手続き

ECPA に違反した場合、最高で、5 年以下の懲役又は 2 万 5000 ドル以下の罰金に処せられる。被害者は、当該違反により実際に生じた損害のほか、懲罰的損害賠償 (punitive damages) 及び弁護士費用を請求するため、民事訴訟を提起する権限を有する。

政府によって違法に収集された証拠については、裁判所に提出することはできない。SCA に基づき、政府のかかる違反について、金銭賠償を求めることもできる。

ECPA によれば、政府は、裁判所の許可命令を取得することで、ECPA によって保護された情報にアクセスすることができる。この場合、各法律によって、データにアクセスできる基準が異なる。通信傍受法 (Wiretap Act) は、声又はデータ通信の内容を政府がリアルタイムに傍受するための命令を裁判官から得るには、相当な理由 (probable cause) が必要であるとしており、これは高いハードルの基準であると言われている。SCA の場合について言えば、E メールその他電子通信及び取引記録 (加入者が特定できる情報、ログ、料金の記録など) への政府によるアクセスに関し、E メールにアクセスするために充たすべき基準は厳しい基準となっている一方で、取引記録にアクセスするために充たすべき基準は緩いものとなっている。ペン・レジスター法においては、電話利用状況記録装置が設置された電話回線上でダイアルされた (又は送信された) 電話番号について、リアルタイムで政府が傍受を行うために充足すべき基準も緩いものとなっている。

⑥ 連邦通信法 (Communications Act)

ア 法律の名称、概要、施行時期

連邦通信法は 1934 年に成立した。連邦通信法は、1934 年以降、1984 年ケーブル通信政策法 (Cable Communications Policy Act of 1984)、1992 年ケーブルテレビ消費者保護・競争法 (Cable Television Consumer Protection and Competition Act of 1992) 及び最

も重要である 1996 年電気通信法 (Telecommunications Act of 1996) 等によって改正がなされたほか、1994 年の通信傍受支援法 (Communications Assistance for Law Enforcement Act、CALEA) 及び 2001 年の米国愛国者法 (USA PATRIOT Act) による改正も行われた。また、連邦通信法は、新しい通信技術に関しても、定期的に改正がなされている。

イ 個人情報の定義

連邦通信法は、第 222 条で定義する「顧客専属ネットワーク情報」(customer proprietary network information, CPNI) を保護している。第 222 条(f)項(1)は「顧客専属ネットワーク情報」を、(A) 電気通信事業者 (telecommunications carrier) の顧客が加入する電気通信サービスの数量、技術構成、種類、相手先及び利用量に関する情報であって、顧客と電気通信事業者の関係のみに基づいて、顧客が電気通信事業者を利用可能とした情報、及び、(B) 電気通信事業者の顧客が区域内電話サービス又は長距離電話サービス (telephone exchange service or telephone toll service) に関して受領した請求書に記載された情報と定義している。但し、連邦通信法は、同法のプライバシー規定の範囲から第 222 条で定義される「集計情報」(aggregate information)³¹及び「加入者リスト情報」(subscriber list information)³²を除外して、両者の異なる取り扱いを禁止している。

連邦通信法第 631 条(a)項(2)は、サービス加入者の「特定の個人を識別可能な情報」(personally identifiable information) を保護しているが、同条に基づき保護される「特定の個人を識別可能な情報」の定義から「特定の個人を識別しない集計データに係る記録」(any record of aggregate data which does not identify particular persons) を除外している。

ウ 主な規制・権利の内容

連邦通信法 (Communications Act) は電話、電信、テレビ、及び無線通信に関する規制について定めている。連邦通信法に基づき設立された連邦通信委員会 (Federal Communications Commission, FCC) は、これらの通信等を監視し、規制を行っている。

連邦通信法は、電気通信企業 (telecommunications companies) の顧客のプライバシーを保護する第 222 条から第 229 条の条項を含み、周波数の割り当て、レートや料金の基準、

³¹ 第 222 条(f)項(2)において定義されている。それによれば、「集計顧客情報」(aggregate customer information) とは、サービス又は顧客の区分又は種類に関する集計データであって、個々の顧客の身元及び特徴が除去されているものをいうとされている。

³² 第 222 条(f)項(3)において定義されている。それによれば、(A) 加入者の掲載された氏名、電話番号、住所若しくは主な広告区分 (サービス開始時に割り当てられた区分)、若しくは、それらの氏名、電話番号、住所若しくは区分の組み合わせを明らかにする情報、又は、(B) いかなる名簿の形式であれ、電気通信事業者又は関連会社が発行し、発行させられ又は受領した情報を意味する。

競争、加入者によるアクセスの条件、広告、公共の利益に資する放送、管理 (government)、通信システムの使用について規制している。また、連邦通信法は、FCC に対して、これらの事項について規則を公布し、監督を行う幅広い権限を与えている。

まず、一般的な義務として、電気通信事業者は、顧客の専有情報 (proprietary information) の秘匿性を保護する義務を負っている (第 222 条(a))。そのうえで、顧客の専有するネットワーク情報 (customer proprietary network information, CPNI) の秘匿性を図るためのその他の要件が規定されている (第 222 条(c))³³。

また、連邦通信法第 229 条は、盗聴法 (Communications Assistance for Law Enforcement Act, CALEA) の遵守を確実にするための規定を含んでいる。第 229 条によれば、一般の事業者が通信の傍受又は通話識別情報 (call-identifying information) へのアクセスを作動させる適切な権限の付与を確実にして無権限の傍受やアクセスを防ぐ手続きを確立することが要請されるとともに、当該権限の有無に関わらず、あらゆる傍受又はアクセスの安全かつ正確な記録を保持することが要請される。

連邦通信法第 631 条は、ケーブル加入者の顧客情報を保護している。第 631 条によれば、ケーブル事業者は、ケーブルサービス又は他のサービスを加入者に提供する合意をする際に通知を発するとともに、毎年加入者に対して、一定の事項³⁴を知らせることが要請されている。

個人情報の収集に関しては、ケーブルオペレーターは、ケーブル加入者による事前の書面又は電磁的方法による同意がなければ、当該ケーブル加入者に関する個人として識別可能な情報を収集するために、ケーブルシステムを使用することはできない (第 631 条 (b) (1))³⁵。また、加入者やケーブルオペレーター以外の者は、当該情報に無権限でアクセスすることを防止するため、ケーブル加入者の事前の書面又は電磁的方法による同意がなければ、ケーブルオペレーターは当該情報を開示することはできないとされている (第 631 条(c) (1))³⁶。

また、ケーブル加入者には、ケーブルオペレーターが収集した当該情報へのアクセス及

³³ 例えば、第 222 条(c) (1)によれば、顧客の承諾がある場合などを除き、電気通信事業者は、個別に識別可能な CPNI について、その資料、開示又はアクセスの許可が禁止されている。また、顧客からの書面の要請があれば、電気通信事業者は、CPNI を顧客に開示する (第 222 条(c) (2))。

³⁴ ①ケーブル加入者について収集された個人として識別可能な情報の性質及び当該情報に関わる使用に係る性質、②開示の性質、頻度及び目的、③ケーブルオペレーターによる管理期間、④ケーブル加入者がアクセス可能な時間及び場所、並びに、⑤ケーブルオペレーターによる情報収集及び開示に関する制約及び当該制約を強制するためのケーブル加入者の権利などである。

³⁵ ただし、ケーブルオペレーターが、ケーブルサービスを顧客に提供する目的でかかる情報を収集し、又はケーブル通信の無権限の受信を調査することについては、例外が定められている (第 631 条(b) (2))。

³⁶ 当該禁止の例外は、裁判所の命令に従い開示がケーブルサービスの提供に必要な場合、又はケーブルオペレーターが加入者に開示を制限する機会を提供し、当該開示がケーブル加入者のレビューや使用、若しくはケーブル加入者によるケーブルサービス上の取引の性質を明らかにしない場合である。

び当該情報の誤りを訂正する合理的な機会が与えられなければならないとされているほか、当該情報が、その収集の目的からみて不要となった場合には、ケーブルオペレーターは原則として当該情報を破棄する必要がある（第 631 条(d)）。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

FCC は、連邦通信法に関する規則を公布しており、それによれば、電気通信事業者は、データ侵害を含む不正な CPNI へのアクセスの試みを発見し、報告し、これから保護する合理的な方法をとることが求められている。

すなわち、「顧客の専有ネットワーク情報の使用に必要なセーフガード」(Safeguards required for use of customer proprietary network information) (FCC Rule 47 CFR 64.2009(c)) によれば、全ての電気通信事業者は、顧客の CPNI を使った自己及び関連会社の売上げ及びマーケティングキャンペーンの記録を、電磁的方法その他の方法で保管する必要がある。また、全ての電気通信事業者は、CPNI が第三者に開示若しくは提供される場合、又は第三者が CPNI へのアクセスを許可される場合には、それらに関する全ての事例の記録を保管しなければならない。当該記録には、各キャンペーンの詳細、当該キャンペーンで使用された特定の CPNI、及び当該キャンペーンの一環として提供された製品やサービスについての説明を含まなければならない。なお、事業者は少なくとも 1 年間は当該記録を保持しなければならない。

さらに、FCC Rule 47 C.F.R. 64.2009(e)に基づき、電気通信事業者は、毎年、役員に、当該事業者の代理人として、コンプライアンス証明書 (compliance certificate) に署名をさせ、FCC に提出させなければならない。

また、47 CFR 64.2006 に基づく新しい FCC データ侵害通知の要件も、議会の合同決議 (Joint Resolution) により、2017 年 6 月 2 日の施行前に廃止された。

オ 安全管理措置

顧客の専有ネットワーク情報の使用に必要なセーフガード (Safeguards required for use of customer proprietary network information) (FCC Rule 47 C.F.R. § 64.2009) は、連邦通信法において必要とされるセーフガードについて規定している。

かかるセーフガードとして、以下のものがある。

(ア) 電気通信事業者 (telecommunication carrier) は、CPNI の使用の前に、顧客の承認に関する状況が明確な形で証明可能なシステムを導入しなければならない。

(イ) 電気通信事業者は、CPNI について、①その使用が承認されている場合と②その使用が

承認されていない場合との区別についてそのスタッフに教育を施さなければならない、また、電気通信事業者は、所定の明示的な懲戒手続 (express disciplinary process) を用意しなければならない。

(ウ) 全ての電気通信事業者は、顧客の CPNI を使った自己及び関連会社の売上げ及びマーケティングキャンペーンの記録を、電磁的方法その他の方法で保管しなければならない。全ての電気通信事業者は、CPNI が第三者に開示若しくは提供される場合、又は第三者による CPNI へのアクセスが許可される場合には、その全ての事例 (instances) の記録を保管しなければならない。当該記録には、各キャンペーンの詳細、当該キャンペーンで使用された CPNI、及び、当該キャンペーンの一環として提供された製品及びサービスについて記載されなければならない。なお、事業者は、少なくとも 1 年間は当該記録を保持しなければならない。

(エ) 電気通信事業者は、アウトバウンド・マーケティングに係る状況に関するルールについて、かかるルールの遵守に関する監督上の検証プロセス (supervisory review process) を確立しなければならない。なお、かかる遵守に関する記録については、少なくとも 1 年間は保持されなければならない。特に、販売スタッフは、アウトバウンド・マーケティングの承認を顧客に要請するに当たっては、監督者からの承認を得なければならない。

(オ) 電気通信事業者は、毎年、役員に、当該事業者の代理人として、コンプライアンス証明書 (compliance certificate) に署名をさせたいうで、FCC に提出させなければならない。当該役員は、証明書において、電気通信事業者が本サブパートに関する連邦通信法のルールを遵守するために十分な運営手続 (operating procedure) を確立しているかという点について、個人的な知識 (personal knowledge) を有していることを記載しなければならない。当該電気通信事業者は、かかる証明書と共に、当該運営手続によってどのように当該ルールを遵守しているのか (又は遵守していないのか) について説明する陳述書 (statement) を提出する必要がある。

(カ) 電気通信事業者は、オプトアウトの仕組みが適切に作用していないために、顧客がオプトアウトできないという状況が例外的な場面とはいえない場合には、書面による通知を 5 営業日以内に FCC に提出しなければならない。かかる通知には、使用しているオプトアウトの仕組みの説明、発生した問題、その解決策及びその実施時期等を記載することとされている。

特定の必要な安全コントロール策の概要については、47 CFR 64.2005 に基づく 2016 FCC

Privacy Order における新 FCC データセキュリティ義務において示されていた。これは、2017 年 3 月 2 日に有効となったものの、2017 年 4 月 3 日に法律となった議会の合同決議 (Joint Resolution) によって廃止されることとなった。

FCC の規制管轄下にある会社は、FCC 規則により、年間の CPNI 証明書 (CPNI certifications) を提出することが求められている。この要請は、2017 年 1 月 3 日に FCC 2016 Privacy Order により削除された。しかし、2017 年 4 月 3 日、議会の合同決議 (Joint Resolution) がトランプ大統領による署名の上法案化され、2016 Privacy Order の全てが廃案とされた後、この要請は復活した。FCC は、FCC 規則の適用に係る助言 (FCC Enforcement Advisory) と共に、FCC 規則を遵守するための推奨テンプレートを出している³⁷。CPNI 証明書において会社が証明すべき事項の中には、47 C.F.R. § 64.2001 以下に定められているルールを遵守するために十分な運営手続 (operating procedure) を確立しているかというものがあり、そこには安全管理措置 (safety control measures) に関する規定も含まれている。

さらに、CPNI を合理的に保護できなかった場合には、連邦通信法第 222 条の義務違反であり、不当かつ不合理なプラクティス (unjust and unreasonable practice) を構成するものとして連邦通信法第 201 条に違反するものとされる。FCC は執行命令 (enforcement order) を介して、電気通信事業者が、専有又は個人的顧客に係る情報 (proprietary or personal customer information) を保護するために、「全ての合理的な予防策」 (every reasonable precaution) をとることを明らかにした。また、電気通信事業者が合理的な安全管理措置の導入を怠った場合には、FCC は、連邦通信法第 222 条(a)に基づき、執行措置 (enforcement action) をとることができる。

カ 適用範囲

FCC は、連邦通信法第 1 条及び第 4 条³⁸に基づき、電気通信プロバイダー (telecommunications providers) に関して重大な取締権限を有しており、ラジオやテレビ、電話線、衛星、ケーブルによって全てのアメリカの州及び外国の通信機関を規制している。なお、2015 年、FCC は、連邦通信法の第 2 章に基づき、ブロードバンド・インターネット・サービスプロバイダーを「公衆通信事業者」 (common carriers) として分類することにより、その対象範囲をブロードバンド・インターネット・サービス・プロバイダーまで広げたが、2017 年に議会の合同決議 (Joint Resolution) によって発効前に無効となった。

緊急事態及び法執行の目的のためのデータ開示については、連邦通信法第 222 条(d)及び(g)は、プライバシー条項に関する例外が規定されている。例えば、モバイルサービスの利

³⁷ Enforcement Advisory については、<https://www.fcc.gov/general/enforcement-advisories> を参照。テンプレートは、例えば、EA2016-01: Annual CPNI Certifications Due March 1 などに添付されている。

³⁸ 47 U.S.C. § 151 及び 47 U.S.C. § 154

ユーザーが緊急のサービスを要請する場合には医療、公共安全、若しくは法執行機関に対して、利用者の位置情報を開示することを認めている。

なお、政府機関が EPCA に基づいて適切な権限を有している場合には、連邦通信法はかかる政府機関への開示に対しては適用されない。

キ 小規模事業者の取扱い

連邦通信法は小規模事業者の取扱いに関して特別な条項を置いていない。しかし、1996年「小規模事業者に対する規制の公正な適用に関する法」(Small Business Regulatory Enforcement Fairness Act) 第 212 条に従って、FCC はウェブサイト上で小規模事業者の法令遵守ガイド (small entity compliance guides)³⁹を公表している。法令遵守ガイドは、小規模事業者に対し、「平易な言葉」(plain language) で、新しい規則への遵守という観点から、FCC が何を求めているのかを説明している。

ク 域外適用

連邦通信法は、州際通信及び国際通信 (interstate and foreign communication) であって、アメリカ国内から発信されたもの又はアメリカ国内において受信されたものや、かかる通信をアメリカ国内で行っている全ての者などに対して適用される⁴⁰。この点、FCC による法執行の影響がアメリカ国外の企業などに及んだとしても、そのことのみによって FCC の権限を超越しと判断されるわけではないことから (*Cable and Wireless v. FCC*, 166 F.3d at 1231)、連邦通信法は域外適用がなされ得るといえる。

ケ 紛争処理手続

FCC は連邦通信法及び規制を執行し、FCC の執行局 (enforcement bureau) は調査を行い、行政罰を課し、違反者に対する行政審判を開始することができる。FCC による行政罰は 1000 万米ドル程度の高額な単位になる可能性もある。FCC は行政審判官局 (Office of Administrative Judges) を有している。なお、FCC の命令 (order) 等については、連邦裁判所 (Federal court) に上訴することが可能である。

(3) 監督機関・第三者機関

FTC は、FTC 法及び COPPA を所管し、HIPAA 及び GLBA の一部を執行する競合管轄権

³⁹ <https://www.fcc.gov/general/compliance-guides-small-businesses>

⁴⁰ 47 U.S.C. § 152

(concurrent jurisdiction) を有しており、会社及び顧客のプライバシー保護に係る実務運用に広く及ぶ権限を有する唯一の連邦の執行機関 (federal agency) である。ただし、「不公正及び欺瞞的」 (unfair and deceptive) であると判明した行為のみを執行対象にし、加えて、COPPA、HIPAA 及び GLBA に基づく一定のプライバシー規則に従って執行するため、その権限は限定的である。

また、HIPAA については、アメリカ合衆国保健福祉省 (The U. S. Department of Health and Human Services, HHS) が一義的な権限を有する。

更に、GLBA については、FTC、商品先物取引委員会 (Commodity Futures Trading Commission, CFTC)、証券取引委員会 (Securities and Exchange Commission, SEC) 等を含む 8 の連邦政府機関が法執行する。

連邦通信法については、同法に基づいて設置された独立行政委員会である連邦通信委員会 (Federal Communications Commission, FCC) が電気通信事業者に対する規制を行っている。

なお、各州は、FTC のような消費者保護法を執行し、また、州の一定のプライバシー及びデータセキュリティ法を部分的に執行することのできる州の司法長官 (State Attorney General) を設置している。

① 連邦取引委員会 (FTC)

Federal Trade Commission

FTC の連絡先等は、以下のとおりである。

連絡先	https://www.ftc.gov/contact 電話番号は (202) 326-2222 など。 個人向けの連絡先なども上記サイトで公開されている。	
所在地	Headquarters: 600 Pennsylvania Avenue, NW, Washington, DC 20580	
委員長・委員 ※	委員長代理 (Acting Chairman)	Maureen K. Ohlhausen
	委員 (Commissioner)	Terrell McSweeney

※ 委員の定員は 5 名だが、2018 年 3 月現在 3 名が空席となっている。

FTC の主たる業務は、不正な競争方法 (unfair methods of competition) の規制に加えて、不公正若しくは欺瞞的な行為又は慣行 (unfair and deceptive acts or practices) の規制することであり、プライバシー保護は後者の規制の一環として行われている。

FTC は、FTC 法第 5 条に基づく監督権限として、一般的な調査権限のほか強制的な調査権限を有している。FTC は、調査結果を踏まえて、同意命令 (consent order / consent decree)

を発することができる⁴¹。例えば、FTC は、(i)その行為又は慣行を差し控えるよう会社に要請し (FTC 法第 5 条(b))、(ii)包括的なプライバシー及びデータセキュリティ・プログラムの策定を会社に命じ (なお、定期的な FTC による監査を義務付けることもできる) (FTC 法第 5 条(b)、第 6 条(a))、又は、(iii)プライバシー侵害及び既存の同意命令に関して民事制裁金を課すこと (FTC 法第 5 条(1)、Commission Rule 1.98(c)) を内容とする同意命令を発することができる。また、FTC は、GLBA 違反、COPPA 及び HIPAA 違反に対する罰金を科す権限も有する。

FTC は、消費者保護局 (Bureau of Consumer Protection)、競争局 (Bureau of Competition) 及び経済局 (Bureau of Economics) の 3 つの局を設置している。消費者保護局は、FTC 法第 5 条に基づき個人情報保護及びプライバシー法を執行している。FTC の規模感を表す資料の 1 つとして、FTC は、2019 年度において、309,700,000 米ドル及び 1140 名の正規職員 (full-time equivalent, FTE) 分の予算を要求しているということが挙げられる⁴²。

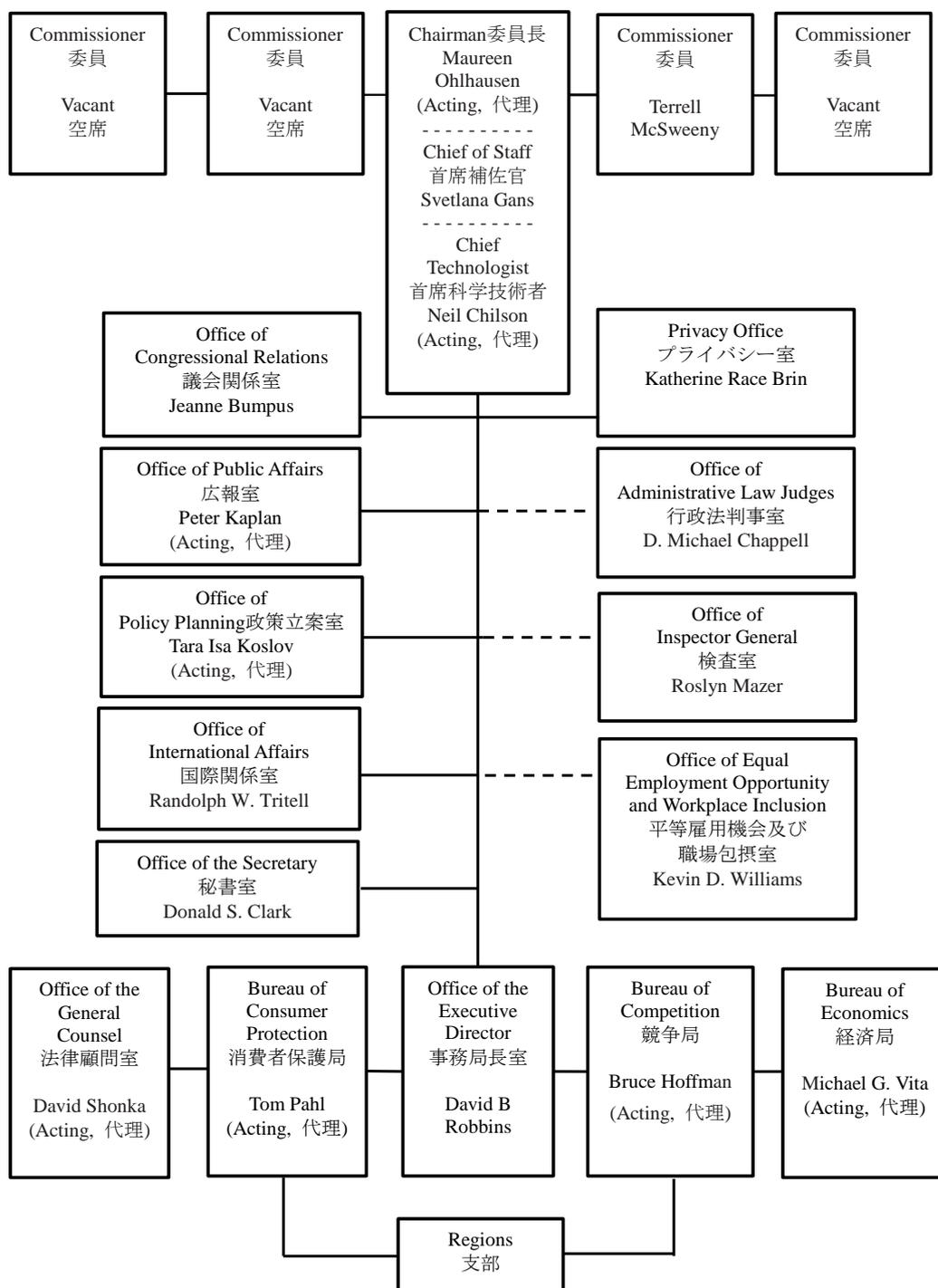
⁴¹ 16 CFR 1605.13. また、A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority

(<https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>) を参照。

⁴² FY 2019 Congressional Budget Justification

(<https://www.ftc.gov/reports/fy-2019-congressional-budget-justification>)

連邦取引委員会 (FTC) の組織図 ⁴³



⁴³ FEDERAL TRADE COMMISSION Organization Chart
https://www.ftc.gov/system/files/attachments/about-ftc/orgchart_ftc_aug_21_2017.pdf、
 2018年3月12日最終閲覧) を翻訳したもの。

FTC は、下記のように事業者に対して制裁金の賦課を含む法執行を行っているほか、FTC 法を執行するにあたり、300 を超える事業者との間で同意命令を締結している。

- ・ 2011 年、FTC は、Google の「Buzz」ソーシャル・ネットワーキング・サービスの立上げにおける欺瞞的 (deceptive) な実務運用に関し、Google との間で、同意命令を締結した。FTC は、かかるサービスによるユーザー情報の収集及び Gmail ユーザーについての当該サービスの自動設定に関して、当該立上げが Google の個人情報保護方針に違反していると判断した。同意命令において、Google は、20 年間コンプライアンス・プログラム等の義務を履行することが義務付けられた。
- ・ 2012 年、FTC は、Facebook が顧客に対して自社の情報削除に関する方針及びユーザーの提供した情報がアプリによって本人の友人に共有され得る旨の開示を怠ったことなど、FTC が「誤解を招く」(misleading) とみなした実務運用について、Facebook との間で同意命令を締結した。同意命令の一部として、Facebook は、20 年間コンプライアンス・プログラム等の義務を履行することが義務付けられた。
- ・ 2012 年、Google は、Apple のウェブブラウザの追跡禁止の設定を迂回し、ユーザーのウェブ閲覧履歴を追跡していたとして、上記の Buzz の件で合意された和解条件に違反したとして、FTC との間で、2250 万ドルの制裁金を支払うことに合意した。
- ・ 2013 年、FTC は、HTC 社の携帯機器のセキュリティ欠陥の結果、ユーザー・データの収集及び開示がなされた件について、HTC 社との間で同意命令を締結した。FTC は、HTC 社が第三者アプリケーションとの間の「権限チェック」(permission checks) 及び合理的な保障措置の実施を怠り、そのためにユーザー・データの開示を許すこととなったと判断した。
- ・ 2014 年、FTC は、TRUSTe の認証プライバシーシールプログラムについて、FTC は、TRUSTe との間で、毎年実施すべき認証先企業の検査を怠り、また、TRUSTe が非営利組織であるとの誤った情報を提供することについて、ウェブサイトに許可していたことに関し、金銭支払いを含む和解を行った。

② アメリカ合衆国保健福祉省 (The U. S. Department of Health and Human Services, HHS)

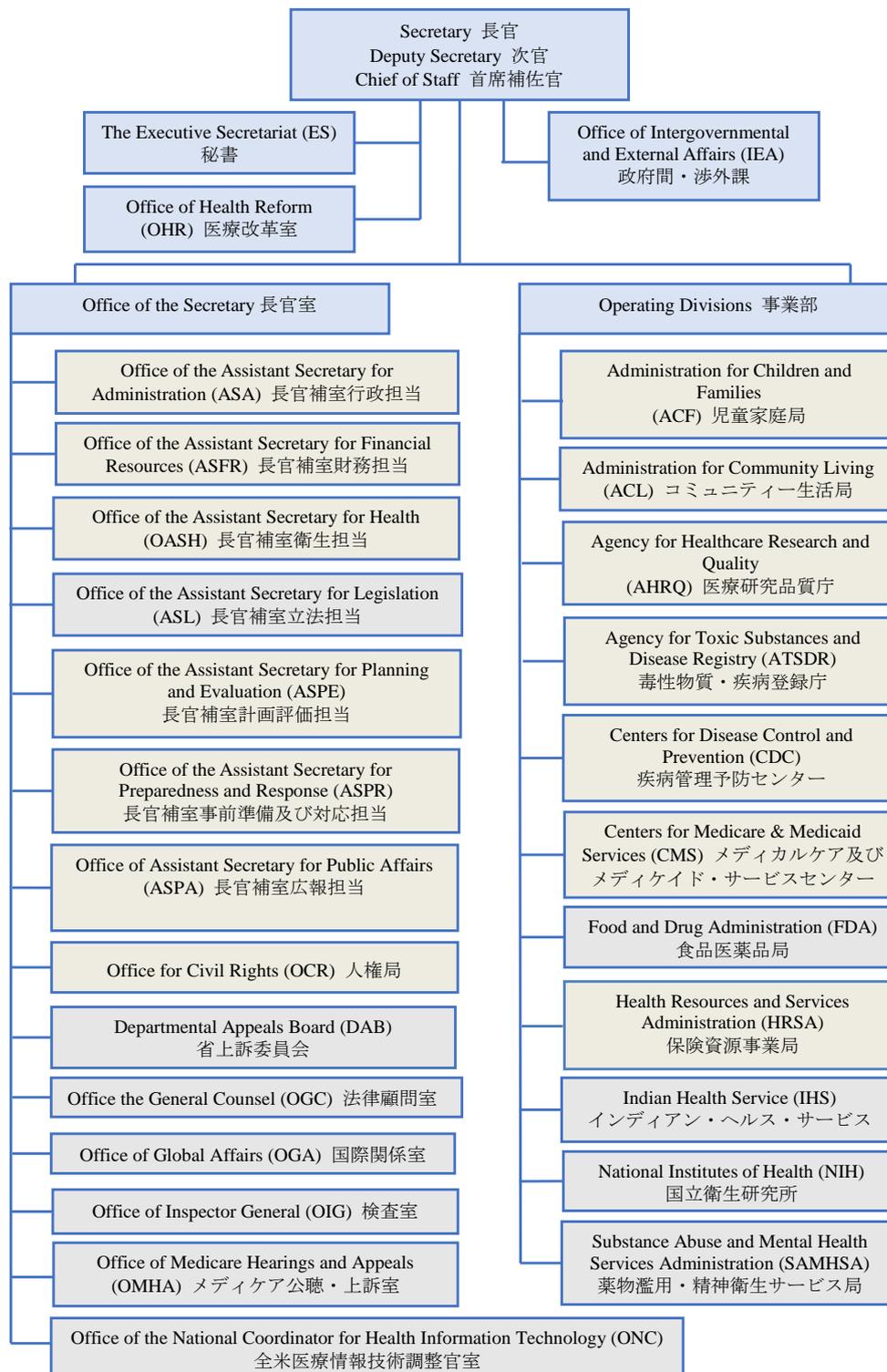
保健福祉省の連絡先等は以下のとおりである。なお、保健福祉省のうち、プライバシーについて所管しているのは人権局 (Office of Civil Rights) であるため、人権局の連絡先等についても記載する。

保健福祉省 (HHS)	
連絡先	https://www.hhs.gov/about/contact-us/index.html 電話番号は Toll Free Call Center: 1-877-696-6775 である。
所在地	200 Independence Avenue, SW, Room 509F, HHH Building Washington, D.C. 20201
長官 (Secretary)	Alex Azar

人権局 (Office of Civil Rights)	
連絡先	https://www.hhs.gov/ocr/about-us/contact-us/index.html 電話番号は Toll Free Call Center: 1-800-368-1019 など。 各地の支部のメールアドレスなども上記サイトで公開されている。
所在地	Headquarter: 200 Independence Avenue, SW, Room 509F, HHH Building Washington, D.C. 20201 なお、上記サイトにあるように、各地に支部もある。
局長 (Director)	Roger Severino

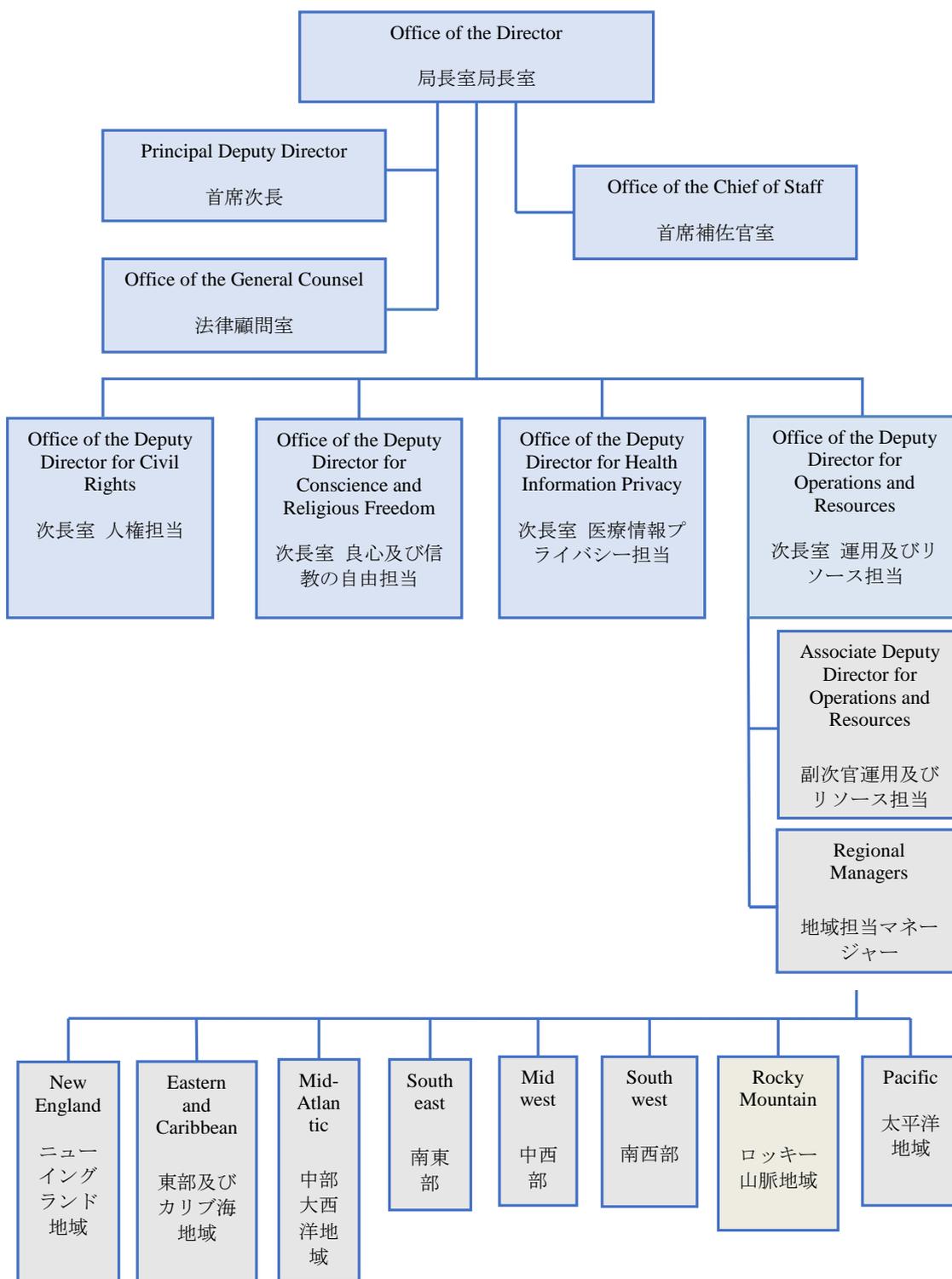
アメリカ合衆国保健福祉省は、医薬品の承認審査・安全対策などを所管しており、特に個人の医療上のプライバシーに関しては、人権局 (Office of Civil Rights, OCR) が管轄しており、執行措置を開始及び請求する権限、HIPAA 違反に対して罰金を科す権限も有する。人権局は、保健福祉省からサービスなどを受ける個人が違法な差別を受けないことや、思想良心の自由や信教の自由を行使できることや、その健康情報についてアクセスすることや、プライバシーやセキュリティが守られることを保障している。

保健福祉省（HHS）の組織図⁴⁴



⁴⁴ HHS Organizational Chart (<https://www.hhs.gov/about/agencies/orgchart/index.html>、2018年3月12日最終閲覧)を翻訳したもの。<https://www.pmda.go.jp/files/000157086.pdf>を翻訳に当たり参照した。

OCR の組織図⁴⁵



⁴⁵ Office for Civil Rights - Organizational Chart (<https://www.hhs.gov/ocr/about-us/leadership/organizational-chart/index.html?language=es>、2018年3月12日最終閲覧)を翻訳したもの。

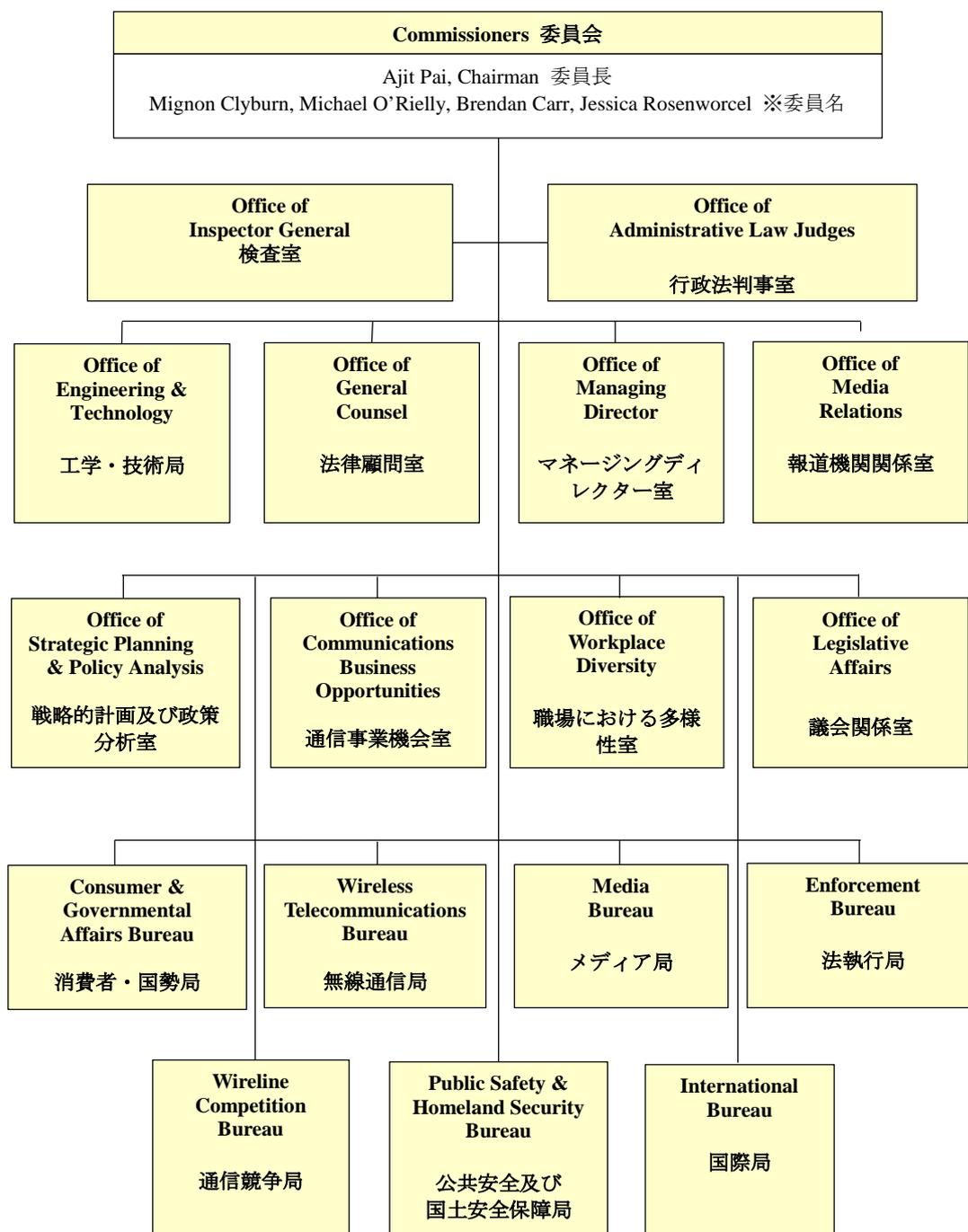
③ 連邦通信委員会 (Federal Communications Commission, FCC)

FCC の連絡先等は以下のとおりである。

連絡先	https://www.fcc.gov/about/contact 電話番号は Toll-Free Voice:1-888-CALL FCC (225-5322) など。 各部署や委員長・委員のメールアドレスも上記サイトで公開されている。	
所在地	445 12th Street SW, Washington, DC 20554	
委員長・委員	委員長 (Chairman)	Ajit Pai
	委員 (Commissioner)	Mignon Clyburn
	委員 (Commissioner)	Michael O' Rielly
	委員 (Commissioner)	Brendan Carr
	委員 (Commissioner)	Jessica Rosenworcel

FCC の一般的な職務は、アメリカにおける州際的及び国際的なラジオ放送、テレビ放送、有線通信、サテライト通信及びケーブル通信についての規制を行うことであり、連邦通信法 222 条に基づき、電気通信事業者に対するプライバシー政策を実施し、法執行を行っている。

組織図⁴⁶



⁴⁶ Organizational Chart of the Federal Communications Commission (<https://www.fcc.gov/sites/default/files/fccorg-08112017.pdf>、2018年3月12日最終閲覧)の一部を翻訳したもの。

(4) 最近のトピック

① 制度改正の検討状況

ECPA をクラウド化した情報社会の法運用が可能となるように改正するため、電子メールプライバシー法案 (Email Privacy Act, (H.R. 387)) が、2017 年から 2018 年のアメリカ合衆国第 115 回連邦議会に提案された⁴⁷。同法案は、2017 年 2 月 6 日に下院 (House) を通過したが、上院 (Senate) は通過していない⁴⁸。同法案によれば、大要、警察が 180 日以前になされた E メールなどの内容をサービス・プロバイダーから取得するには、令状 (warrant) がなければならないとされている。

現在、個人情報保護及びプライバシーに関して、アメリカ合衆国連邦議会において審議中のその他法案が多数あるが、中でも注目すべきは、以下の法案である。

- ・ 2015 年個人データプライバシー及びセキュリティ法 (The Personal Data Privacy and Security Act of 2015)
データ漏えい及び個人情報の悪用に関して罰金を引き上げるもの。
- ・ 2015 年オンライン追跡防止法 (The Do Not Track Online Act of 2015)
顧客によるオンライン追跡からのオプトアウトを認めるよう FTC に義務付けるもの。
- ・ 2015 年児童追跡防止法 (The Do Not Track Kids Act of 2015)
COPPA を改正して、児童に対する追加的なプライバシー保護を加えるもの。

消費者プライバシー権利章典の関係では、アメリカ合衆国連邦議会において、包括的な一般消費者のプライバシー権利章典 (Consumer Privacy Bill of Rights)⁴⁹についても引き続き議論されている。

なお、2012 年 2 月にオバマ政権は政策大綱「ネットワーク化された世界における消費者データプライバシー」(Consumer Data Privacy in a Networked World)⁵⁰を発表しており、消費者のオンラインプライバシーを守るための 7 か条からなる「消費者プライバシー権利章典」(Consumer Privacy Bill of Right)⁵¹が含まれている。2012 年に制定された消費者

⁴⁷ <https://www.congress.gov/bill/115th-congress/house-bill/387/text>

なお、電子メールプライバシー法案は、2010 年 12 月 4 日のアメリカ合衆国連邦第 6 巡回区控訴裁判所の *United States v. Warshak* 事件 (631 F.3d 266 (6th Cir. 2010)) の判示を立法化する内容である。同事件の判決では、第三者の管理するサーバー内に蔵置された電子メールの内容にはアメリカ合衆国憲法修正第 4 条の保障するプライバシーの合理的期待が存在すると判示されている。

⁴⁸ 2017 年 7 月 27 日時点で、上院では、読会が 2 回行われ、司法委員会に付託がなされているが (Read twice and referred to the Committee on the Judiciary)、その後、特に動きはないようである (<https://www.congress.gov/bill/115th-congress/senate-bill/1654>、2018 年 3 月 12 日最終閲覧)。

⁴⁹ <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>

⁵⁰ <https://www.hsdl.org/?view&did=700959>

⁵¹ <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>

プライバシー権利章典において、第一原則が「個人のコントロール」(Individual Control)とされており、個人による選択の仕組みとして追跡拒否 (Do Not Track, DNT) が明記されている。また 2014 年に公表されたいわゆるビッグデータ・レポート (BIG DATA: Seizing Opportunities, Preserving Values)⁵²においては、その政策提言の一つとして、消費者プライバシー権利章典の立法化が提言されている。2015 年には「2015 年消費者プライバシー権利章典法」(Consumer Privacy Bill of Rights Act of 2015) の草案及び関連法案が公表されたが、未成立である。

② 個人情報に関連した政策動向

FTC は、オンラインプライバシーに関して、2009 年 2 月に「スタッフレポート：オンライン上の行動ターゲティング広告に関する自主行動原則」(FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising)⁵³を公表しており、業界団体等による自主規制による対応を求めている。

FTC は、2012 年に、「FTC 報告書：急速に変化する時代における消費者プライバシー保護」(FTC Report: Protecting Consumer Privacy in an Era of Rapid Change)⁵⁴を発表しており、消費者のプライバシー保護のため、企業が採用すべきプライバシーの枠組みとして、①プライバシー・バイ・デザイン、②消費者へのシンプルな選択肢の提供、③透明性の増進を挙げており、追跡拒否 (Do Not Track, DNT)、モバイル、データ仲介者 (消費者プロフィールを蓄積し、これを他社に販売する会社)、大規模プラットフォーム・プロバイダー、自主規制基準の推進等に取り組むとした。FTC は、2013 年には携帯電話位置情報追跡について、2014 年にはデータ仲介者の事業活動について包括的な報告書を発表している⁵⁵。FTC は広告配信に関して個人のウェブ上での行動追跡を禁止する追跡拒否の仕組みを導入すべきとし、欺瞞的慣行 (deceptive practices) がある場合には制裁金を課している事例もある。

FTC は、2016 年 1 月にはビッグデータに関するスタッフレポート (FTC Report: Big Data:

⁵²

https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

⁵³

<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>

⁵⁴

<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

⁵⁵ https://www.ftc.gov/system/files/documents/public_comments/2014/03/00019-89125.pdf

A Tool for Inclusion or Exclusion?)⁵⁶を公表している。

FTCは、2017年1月に、「クロス・デバイス・トラッキング：FTCスタッフレポート⁵⁷」(Cross-Device Tracking: An FTC Staff Report)⁵⁸という報告書において、2015年11月のクロス・デバイス・トラッキングワークショップからのコメントと協議に基づく勧告を含めている。FTCスタッフレポートでは、クロス・デバイス・トラッキングは、複数のデバイス（例えば、スマートフォン、タブレット、パソコンなど）を同一人の消費者と関連付け、それらのデバイス間をまたいで消費者行動をリンクさせるが、これがどのようにしばしば消費者の知識なしに、またトラッキングのコントロールについての消費者の限られた選択のもとに行われるかについて検討されていた。この理由から、FTCはその職員の報告の中で、事業者は、透明性、選択及びセキュリティといった伝統的な原則を新たな実践に最も良く適用し得る方法を勧告した。その勧告はすなわち、(1) 事業者はトラッキングを消費者やビジネスパートナーに開示すること、(2) 消費者に対し、どのように自分たちの行動がトラッキングされるかの選択を提示すること、(3) センシティブな消費者情報をクロス・トラッキングし正確な地理的位置情報を収集又は共有する前に、表明される肯定的な同意を取得すること、そして(4) クロス・デバイス・トラッキングから集められたデータのセキュリティを確かなものにするることである。

FTCは2018年1月に「2017年プライバシー・データセキュリティ・アップデート」(Privacy & Data Security Update: 2017)⁵⁹を公表している。アメリカ合衆国の大手企業、とりわけ、2017年の消費者信用情報会社エクイファクス (Equifax Inc.) から最大1億4300万人のデータが漏えいした事件や2014年のアメリカ合衆国の大手ディスカウントストア・チェーンであるターゲット (Target) 社が攻撃され、4,000万件にも及ぶ顧客のクレジットカード情報（以下「カード情報」という。）がPOS 端末から流出した重大なデータ漏えいにより、データ漏えい及びセキュリティの問題に引き続き焦点を当てていくと思われる。

なお、欧州連合及びアメリカ合衆国企業間でのデータ移転及び共有を認める欧州連合・アメリカ合衆国間のプライバシー・シールドの枠組みがある。2017年9月に行われた米国政府による同枠組みの年次評価を踏まえ、2017年10月18日、欧州委員会はEUとアメリカ

56

<https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>

57

https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

58

https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

59

https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf

合衆国のプライバシー・シールドの機能について最初の年次報告を発行した⁶⁰。この報告の中で、欧州委員会は、プライバシー・シールドは「適切なレベルの保護を確かなものにし続け」(continues to ensure an adequate level of protection)、そして維持されるべきという調査結果を確認した。また、その報告はプライバシー・シールドの機能を向上させるいくつかの勧告をも含んでいた。それはすなわち、(1) アメリカ合衆国商務省 (US Department of Commerce) により課される企業のプライバシー・シールドの義務の遵守に対するモニタリングを向上させること、(2) どのように苦情を申し立てるかということを含む、どのように個人がプライバシー・シールド下で自身の権利を行使できるかという意識の向上を EU において図ること、そして (3) アメリカ合衆国商務省、FTC 及び EU データ保護機関 (Data Protection Authorities、DPAs) との間でより緊密に協力すること (これは企業や執行官のためのガイドラインの策定を含む)、である。また、その報告は、アメリカ合衆国内での外国情報監視法 (Foreign Intelligence Surveillance Act、FISA) のセクション 702 の再授権と改革 (reauthorization and reform)⁶¹、及びアメリカ合衆国における常勤のプライバシー・シールドのオンブズマンを任命するプロセス、並びにプライバシー及び市民的自由監視委員会 (Privacy and Civil Liberties Oversight Board、PCLOB) の空席のポストを埋めることについての議論に関する勧告も含んでいた。その報告は、欧州議会、データ保護当局の第 29 条ワーキンググループ、及びアメリカ合衆国当局へ送られた。欧州委員会は 2018 年初頭の数か月間にその勧告をフォローアップしてアメリカ合衆国当局と協働し、そしてプライバシー・シールド・フレームワークの機能のモニタリングを継続することを計画している。

2016 年 10 月、アメリカ合衆国商務省は、その APEC 越境プライバシールール・システム (APEC Cross-Border Privacy Rules System、CBPR system) に対する取組みについて確認した⁶²。同システムは、欧州連合とアメリカ合衆国間のプライバシー・シールド・フレームワーク同様、企業がアメリカ合衆国と APEC 加盟国間における情報の移転及び共有に関する認証を行うことのできる任意のシステムである。

③ 個人情報に関連した主要な裁判例

アメリカ合衆国では、プライバシー侵害、特にデータ漏えいに関するものに基づく集団訴訟が多く見られる。かかる訴訟は州法又は私的訴権 (private right of action) につい

⁶⁰ http://europa.eu/rapid/press-release_IP-17-3966_en.htm

⁶¹ これは米国法の下におけるアメリカ人以外の者のデータプライバシーの保護に影響するものである。

⁶²

<https://blog.trade.gov/2016/11/29/the-apec-cross-border-privacy-rules-advancing-privacy-and-digital-trade-in-asia/>

て規定している連邦法⁶³に基づいて提起される。

個人情報保護及びプライバシー規制に関する FTC 法に基づくアメリカ合衆国の広範囲に渡る権限は、2015 年にアメリカ合衆国連邦第 3 巡回区控訴裁判所 (United States Court of Appeals for the Third Circuit) *FTC v. Wyndham Hotel* 事件において確認された⁶⁴。本件では、ニュージャージー連邦地裁 (New Jersey federal district court) において Wyndham Hotels が FTC により、データ保護違反の疑惑で訴えられ、少なくとも 2 年以内にホテルチェーンにおいて 3 つのデータ侵害があったとされていた。Wyndham Hotels は、FTC が FTC 法第 5 条の不正要件に係るサイバーセキュリティ規制権限を欠いていたということに基づき訴えの却下 (dismiss) を求めた。また、Wyndham Hotels は、FTC が FTC 法に基づいてデータ保護違反による訴えを提起する権限を有していたとしても、公平な通知 (fair notice) を受領していないことから、そのサイバーセキュリティ実務は不正要件を充足しないとも主張した。連邦地裁は訴えを棄却しなかったが、控訴審裁判所はこの問題に係る即時控訴 (immediate appeal) の審理することとした。控訴審において、控訴審裁判所は、規制権限に関する連邦地裁の判断を是認したほか、公平な通知に関する主張も否定した。*FTC v. Wyndham Hotel* 事件により、アメリカ合衆国におけるデータプライバシー及び保護について FTC の第一次的な権限を支持したものと広く理解されるようになっている。

⁶³ 私的訴権を定めている制定法としては連邦通信法、ケーブル通信政策法、VPPA 等がある。

⁶⁴

<https://www.ftc.gov/news-events/blogs/business-blog/2015/08/third-circuit-rules-ftc-v-wyndham-case>

2. カナダ

(1) 制度概要

① 法体系の概要

カナダにおける個人情報保護については、民間部門は個人情報保護及び電子文書法 (Personal Information Protection and Electronic Documents Act、以下「PIPEDA」¹という。) が規律し、公的部門は、プライバシー法 (Privacy Act)²が公共部門を規律する。

PIPEDA は、原則として、カナダ領域内の民間部門におけるすべての商業活動に適用される。PIPEDA は、2015 年のデジタルプライバシー法 (Digital Privacy Act) の制定の際に改正された。当該改正に合わせた PIPEDA の規則は、2017 年末又は 2018 年の初めまでには完全に整備され、施行される見通しである。

デジタルプライバシー法 (Digital Privacy Act, DPA³) は、2015 年 6 月 18 日に可決され、多くの点において、PIPEDA を改正するものである。主な改正点は、データ漏えい時の通知の導入である。カナダ政府は、2017 年 9 月 2 日、関連規則を公表したが⁴、デジタルプライバシー法はまだ施行されていない。

プライバシー法は、カナダの連邦政府の各部局及び機関のデータ保護慣行を広く規制する。州の法令も、状況に応じて、これらの連邦法に優先又は補完する。

上述したとおり、PIPEDA は、カナダでの商業活動におけるすべての個人情報の収集、利用及び開示について規制する統一法典であり、金融、医療、IT その他商取引に従事する一切の部門に適用される⁵。

一方、民間部門の個人情報の取扱いを規制する主な法令としては、PIPEDA 及びデジタルプライバシー法の他に、業界特有の法令又は業界のデータ保護基準として、1993 年電気通信法⁶ (電気通信業界に関する規制)、スパム対策法⁷ (商用電子メールに関する規制)、銀

¹ Personal Information Protection and Electronic Documents Act

<http://laws-lois.justice.gc.ca/eng/acts/P-8.6/>

² Privacy Act

<http://laws-lois.justice.gc.ca/eng/acts/p-21/>

³ Digital Privacy Act

<http://www.parl.ca/DocumentViewer/en/41-2/bill/S-4/royal-assent>

⁴ Breach of Security Safeguards Regulations

<http://gazette.gc.ca/rp-pr/p1/2017/2017-09-02/html/reg1-eng.html>

⁵ 健康情報の利用、収集及び開示に携わる事業者・組織に適用される州法が、PIPEDA に加え又は代わりに適用される。

⁶ Telecommunications Act

<http://laws-lois.justice.gc.ca/eng/acts/T-3.4/>

⁷ Canada's Anti-Spam Legislation (CASL)

<http://fightspam.gc.ca/eic/site/030.nsf/eng/home#>

行法⁸（連邦政府の規制対象金融機関に関する規制）、及び諸州法（特に医療情報に関する規制）がある。

② 民間部門の概要

PIPEDA は、商業活動におけるすべての個人情報の収集、利用及び開示について規制する。PIPEDA は、実質的にこれに類似する独自の法令を有していないすべての州において、個人情報に対して適用される（現在、ケベック州、ブリティッシュコロンビア州及びアルバータ州に関しては、実質的にこれに類似する法令が存在する。）。上述した通り、デジタルプライバシー法は、民間企業を対象として新たなデータ漏えい通知義務を定め、PIPEDA を改正する。

1993年に制定された電気通信法は、プライバシーを含む電気通信を規制する。同法第41条はとりわけ、全国電話勧誘拒否リストの制定について定めている。迷惑な商用電気通信（電話、ファックス）は、同法に従って採択された規則により規制されている。具体的には、カナダラジオテレビ・電気通信委員会迷惑電話制度の規制に関する連邦規則（Canadian Radio-television and Telecommunications Commission Unsolicited Telecommunications Rules）には、(i)消費者向けのレジストリを作成する全国電話勧誘拒否リストに関するルール、(ii)消費者へのテレマーケティングに関する基本的行動規範、及び、(iii)自動発信案内装置に関するルールが含まれる。

スパム対策法は、商用電子メールに関する一定の要件を定める規定を定めている。

銀行法には、連邦政府の規制対象金融機関による個人の金融情報の利用及び開示を規制する規定が定められている。

また、カナダは、APEC 越境プライバシールール・システムの加盟国でもある。

③ 公的部門の概要

プライバシー法は、連邦政府、部局及び機関による個人情報の取扱実務について定める。この他、情報へのアクセス法（Access to Information Act）は国民に対し、政府が自己に関して保有する情報へのアクセス権を認め、カナダ人権法（Canadian Human Rights Act）も

（正式な法令の名称）An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act

<http://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html>

⁸ Bank Act

<http://laws-lois.justice.gc.ca/eng/acts/B-1.01/>

データ保護に関する規定を定めている。

すなわち、情報へのアクセス法及びプライバシー法のいずれも、連邦政府及びその機関の管理する記録及び情報へのアクセス権を個人に認めている。情報へのアクセス法に基づき、個人は、連邦政府に記録されているプログラムやアクティビティに関して、情報へアクセスする権利を要求することができる。申請にはそれぞれ、要求に応じて異なる要件があり、各法律に基づいて提供された情報は異なる場合がある。多くの州に、これに相当する情報公開法がある。

④ 個人情報に関する州法⁹

連邦法である上記各法律に加え、民間部門の特定の業種において、州法が適用される場合がある。特に健康情報の利用、収集及び開示に携わる組織に適用される州の法令がこれにあたる。州の法令は、連邦企業を除く各州の公共部門による個人情報の収集、利用及び開示にも適用される場合がある。

また、知事は、その州法が PIPEDA の規定と実質的に同等であると判断した場合、知事は、その州の組織・団体に関しては、PIPEDA は適用されないようにすることができる (PIPEDA 26 条(2))。

また、州の法令は、各州の公共部門による個人情報の収集、利用及び開示に適用される。

(2) 主な法律の概要

① PIPEDA

ア 法律の概要

PIPEDA は、個人情報、及び合理的な者がその状況において適切とみなす目的で組織が個人情報を収集、利用又は開示する必要性に関し、個人のプライバシー権を尊重する形で、個人情報の収集、利用及び開示を規制する規則を定めることを目的とする (PIPEDA 第3条 (パート1))。

PIPEDA は、カナダの国会において、2000年4月13日に可決された。具体的な施行時期は、以下の通りである。

2000年4月13日	第1章(Division1, Protection of Personal Information)
2000年5月1日	パート2(Electronic Documents) パート3(Amendments to the Canada Evidence Act)

⁹ 州法については、石井夏生利「カナダのプライバシー・個人情報保護法」情報法制研究(1) 2017年5月19頁以下を参照

	パート4(Amendments to the Statutory Instruments Act)
2001年1月1日	パート1(Protection of Personal Information in the Private Sector)
2009年6月1日	パート5(Amendments to the Statute Revision Act)

イ 個人情報の定義など

PIPEDA 第2条(1)において、「個人情報」(Personal Information)が「特定可能な個人に関する情報」としてPIPEDAに定義されている。

PIPEDAは、センシティブインフォメーション(Sensitive Information)について特段の配慮を求めているものの(PIPEDA4.3.6、同4.7.2、同4.9.1)、PIPEDAはセンシティブインフォメーションの定義を明確に規定していない。例えば、PIPEDAは、「ニュース冊子の購読者の名前や住所は、センシティブインフォメーションではないが、特別な分野の冊子の名前や住所はセンシティブインフォメーションに該当し得る」と規定している(PIPEDA4.3.4)。

ウ 主な規制・権利の内容

PIPEDAは、データ保護オフィサーの任命について定めている。組織は、組織の個人情報保護方針・プライバシー慣行に責任を負う者及び苦情や問い合わせの転送先の者の氏名又は役職及び住所を公表しなければならない。PIPEDAはまた、同法別紙1(Schedule 1)に、以下の通り情報処理についての義務を規定している(原則4.1-4.10)。

原則4.1(説明責任):

要求に応じて、組織における個人情報の責任者を開示(説明責任原則)

原則4.2(目的の特定):

個人情報収集の目的が当該情報を収集する時点以前に組織によって特定

原則4.3(同意):

法律で別途認められる場合を除き個人情報の収集、利用又は開示には、個人への告知及び当該個人の同意が必要

原則4.4(収集の制限):

個人情報の収集が組織が特定した目的のために必要なものに限定されること。情報が公正かつ適法な手段で収集されること

原則4.5(利用、開示及び保有の制限):

収集した情報の利用、保有及び開示がその収集目的に限定

原則4.6(正確性):

個人情報がその利用目的に必要なとされるだけ、正確、完全及び最新であること

原則4.7(保護):

個人情報が情報の機密性に適した保護措置によって保護

原則 4. 8(情報公開):

組織の方針・慣行についての情報を提供する際に開放性を義務付け

原則 4. 9(本人によるアクセス):

本人による個人情報への本人アクセス権

原則 4. 10(コンプライアンスに関する異議申立):

指定された個人又は組織のコンプライアンスに責任を負う個人に対して、個人が上記原則へのコンプライアンスに関して異議申立を行う権利を有するべき

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

2015年に、デジタルプライバシー法により、漏えい通知のルールがPIPEDAに追加された。これらの新たな要件に基づき、組織は、当該違反が個人に対する重大な損害の現実的リスクをもたらすと合理的に考える場合、その管理する個人情報に関する保護措置違反をプライバシー・コミッショナーに報告しなければならない。その場合、法律で別途禁止されている場合を除き、組織は、個人の個人情報に関する保護措置違反について、本人に通知する。また、組織は、その管理する個人情報に関する保護措置違反をすべて記録し、これを維持しなければならない。

オ 安全管理措置に関する規定

PIPEDA は、別紙 1 (同法原則 4. 7「保護」)において、情報の機密性に見合った保護措置による個人情報の保護を義務付けている。

原則 4. 7. 1:

保護措置により、紛失又は盗難及び不正アクセス、開示、複製、利用又は改ざんから個人情報を保護しなければならないことを明示している。

原則 4. 7. 2:

保護の性質が情報の機密性、情報の量、分布及び形式並びに保管方法によって異なり、機密性の高い情報についてはより高い保護水準により保護される旨明示している。

原則 4. 7. 3:

保護手段には、(a)施錠された書類整理棚やオフィスへのアクセスの制限等の物理的手段、(b)「関係者以外極秘」としてアクセス権限を付与し、アクセスを制限する等の組織的手段及び(c)パスワードや暗号化の利用等の技術的手段を含むべきであると明示している。

原則 4. 7. 4:

従業員に対して個人情報の機密性を保持することの重要性を認識させることを義務付けている。ま

た、第三者代理人(処理業者)による処理を規制する特定の規則がある。

組織は、処理のために第三者に移転された個人情報に対して責任を負う。そのため、PIPEDA は、第三者処理業者による個人情報の保護水準を同程度とするよう、組織に契約その他の手段を利用することを義務付けている。

カ 適用範囲、適用除外内容

(ア) 原則

PIPEDA は、カナダの領域内において民間部門で行われるすべての商業活動に適用され、公共部門の活動に対しても限定的に適用される。PIPEDA は、実質的に同様の法令がある州においては、同州内の連邦企業に対して適用される場合を除き、適用されない¹⁰。同法は、カナダの企業又は者／個人が行った活動に対しては、当該活動がカナダの領域に入らない限り、基本的に適用されない。

(イ) 例外 (Lawson 対 Accusearch2、「現実的かつ重要な関係」)

2007年連邦裁判所判決の一つ、Lawson 対 Accusearch2 において、PIPEDA が域外適用されない場合であっても、当該活動について、カナダとの「現実的かつ重要な関係」がある場合、プライバシー・コミッショナーは、申立てについて調査する権限を有するとの判決が下された。Lawson において、裁判所は、会社が海外に本社を置いていたため、申立人が苦情を申し立てた活動がカナダで発生しなかったとはいえ、申立人がカナダの住民であり、相手方がカナダ国内でサービスを提供している会社で、カナダ人従業員がおり、カナダ版のウェブサイトを運営しており、カナダの顧客からデータを収集していたため、プライバシー・コミッショナーが当該事件に対する権限を有するだけの「現実的かつ重要な関係」がなおカナダとの間にあると判断した。この事件は、同法の適用範囲を全般的に広げるものと理解されている。

キ 小規模事業者の取扱い

¹⁰ 現在は、ブリティッシュ・コロンビア州、アルバータ州、ケベック州（民間部門）、オンタリオ州、ニュー・ブランズウィック州、ノヴァスコシア州、ニューファンドランド&ラブラドル州のルールが実質的に類似するとの判断を受けている。

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/

デジタルプライバシー法の項目 ((2) ②) で述べる。

ク 国際的な情報移転に関する規定

PIPEDA は、データの越境移転に関して、具体的な制約を定めていない。ただし、国際的な移転を含み、第三者処理業者に対する個人情報の移転はすべて、PIPEDA 上の「説明責任」原則に従う。そのため、組織は、その保有又は保管する個人情報に関し、処理のために当該情報が第三者に移転された後も引き続き責任を負う。組織は、第三者処理業者による保護水準を同程度とするために、契約その他の手段を利用するものとする。

PIPEDA を含むカナダの法律によると、データの越境移転¹¹について、国の監督機関に届出又はその許可を得る必要はない。

ケ 紛争処理手続き

PIPEDA パート 1、第 2 章 (Division 2)、救済手段 (第 11 条乃至第 17 条) (苦情の申立 (第 11 条)、苦情の調査 (第 12 条)、調査の中断 (第 12.2 項)、コミッショナーの報告 (第 13 条)、裁判所による聴取 (第 14 条) 及びコンプライアンス契約 (第 17.1 項)) は、同法に基づき利用可能な紛争解決手続について概説している。

これらの手続は、プライバシー・コミッショナーが、(i) 個人からの申立てを調査し、(ii) PIPEDA の違反があったと信ずべき理由があった場合に、自らの主導権を発動して調査を開始し、(iii) 法律違反となるおそれがあると判断した場合に、組織との間で強制執行可能なコンプライアンス契約を締結することが可能であることを明示している。コミッショナーには、合理的期間内に提起されなかった場合又はその他の審査手続が求められるべきであった場合に苦情の調査を拒否する裁量がある。

調査中、コミッショナーは、(i) 証人を召喚し、証言又は記録を提示するよう強制し、(ii) 敷地内を捜査して組織のセキュリティ要件を確認する (敷地内の者に聴取を行い、敷地において記録の写しを取ることを含む。) 権限を有する。また、PIPEDA 第 12 条(1)(c) は、コミッショナーがその強制執行において利用した証拠が裁判手続において証拠能力を有する必要はないことを明示している。

コミッショナーは、その調査後、調査結果及び提言と共に報告書を発表することができる。申立人は、当該発表後、裁判所の手続を申請する権利を有する。報告書の発表後、申立人が裁判所の審理を申請した場合、連邦裁判所は、(i) 組織にその行為を是正するよう命

¹¹ 以下の 2009 年 1 月付け「国境を越えた個人データ処理のためのガイドライン」を参照。
https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/.

じ、(ii) 是正措置の通知を公表し、(iii) 申立人に対する損害賠償を認めることをはじめとする措置を講じることができる。

また、OPC¹²は、公益開示・名指し、監査、コンプライアンス契約及び報告違反を含む PIPEDA に関する他の強制執行ツールを有する。

② デジタルプライバシー法 (Digital Privacy Act、DPA)

ア 法律の概要

デジタルプライバシー法 (DPA) (S. C. 2015 年、第 32 章) (正式には、PIPEDA を改正し、別の法律に対する派生的改正を行う法律) は、2015 年 6 月 18 日に可決され、連邦政府が関連規則を策定し、整備された段階で、施行される見通しである。DPA は、PIPEDA を改正する法律である。

イ 個人情報の定義

DPA 第 2 条(1)は、以下のとおり明示している。

「第 2 条(1) PIPEDA 第 2 項(1)における「個人情報」の定義は、以下の文言と読み替える。「個人情報」とは、識別可能な個人に関する情報をいう。」

なお、DPA は、「センシティブインフォメーション」を定義していない。

ウ 主な規制・権利の内容

2017 年 9 月 2 日、カナダ政府は、DPA に関する、データ漏えいについての規則の草案を公表した。

これらの規則は、保護措置上のデータ漏えいの報告 (以下「本件漏えい」という。) について定める。PIPEDA の改正により、本件漏えいによって、その状況において個人に対する「重大な損害に関する現実の危険」が生じると合理的に考えられる場合、プライバシー・コミッショナーへの報告が義務付けられる。

同規則は、以下に対する同法上の要件を詳述する。

1. コミッショナー宛て本件漏えい報告の内容
2. 本件漏えいの影響を受ける個人への通知の内容
3. 通知の方法
4. 記録保持要件

現在、アルバータ州は、カナダで唯一、データ漏えい報告が義務付けられている。その

¹² Office of the Privacy Commissioner の通称。3.2.3.1 において詳述。

ため、これら新たな規制を解釈する際に、アルバータ州における実務及び先例を参照することができる。

エ 適用範囲、適用除外内容

DPA は PIPEDA の改正法であるため、適用範囲及び適用除外内容は PIPEDA の定義に従う。

オ 小規模事業者の取扱い

上述した通り、2017 年 9 月 2 日、カナダ政府は、デジタルプライバシー法に基づきデータ漏えい規則の草案を発表した。当該規則は、影響を受けた個人に対して間接的に通知を行う場合がある際の状況についても定めている（間接的通知オプション：企業は、自社のウェブサイト上に、本件漏えいに関する情報を目立つように公表するか又は影響を受けた個人に届くような広告を出すもの）。

間接的通知オプションが許される場合として、直接の通知を行う費用が組織にとって高額である場合が定められている。この規定は、多くの個人に影響を与える本件漏えいに関与した中小企業にとっては有益となる。

③ 電気通信法 (Telecommunications Act)

ア 法律の概要

電気通信法は、国会で 1993 年 6 月 23 日に可決された。

イ 個人情報の定義

電気通信法に基づき公布された迷惑電話制度の規制に関する連邦規則のフレームワーク及び全国電話勧誘拒否リストは、同規則に基づき保護された個人情報を認識するにあたり、基本的に PIPEDA を踏襲する。

なお、電気通信法は、「センシティブインフォメーション」を特別に定義していない。

ウ 主な規制・権利の内容

電気通信法に基づき公布された迷惑電話制度の規制に関する連邦規則のフレームワーク及び全国電話勧誘拒否リストは、電話業者による不招請勧誘電話やファックスからの顧客の保護について定める。

エ 適用範囲、適用除外内容

迷惑電話制度の規制に関する連邦規則のフレームワーク及び全国電話勧誘拒否リストは、カナダの顧客の保護について定めている。同規則は、電話の発信地を問わず、適用される。カナダ国外から電話をかける電話業者は、同規則を遵守しなければならない。

オ 紛争処理手続き

個人は、迷惑電話制度の規制に関する連邦規則違反に関して、カナダラジオテレビ・電気通信委員会（以下「CRTC¹³」という。）に苦情を申し立てることができる。

CRTC は、苦情に関する詳細な情報を得るために、苦情を申し立てた者に連絡を取る場合がある。CRTC は、苦情に関してどのようなことが行われたかを知らせるために、苦情を申し立てた者に連絡を取るようなことはない。CRTC は、同規則の違反に関して、電話業者に対し、個人の場合には1,500ドル、法人の場合には15,000ドル以下の課徴金を科す場合がある。

④ スпам対策法 (Canadian Anti-Spam Legislation, CASL)

ア 法律の概要

スパム対策法（正式には、商業活動の電子的な実施手段への依存を妨げる一定の活動を規制することでカナダ経済の効率性及び適応性を推進し、カナダラジオテレビ・電気通信委員会法、競争法、個人情報保護及び電子文書に関する法律並びに電気通信法する法律を改正する法律（S.C. 2010年、第23章））は、商業活動を行う際に電子的手段の利用を妨げる商行為を規制することにより、カナダ経済の効率性及び適応性を推進することを目的とする。その理由として、かかる行為が以下に該当するためである（第I部第3条）。

- (a) 商業活動を行う際の電子的手段の可用性、信頼性、効率性及び最適な利用を害する。

¹³ Canadian Radio-television and Telecommunications Commission の通称。3.2.3.2において詳述。

- (b) 企業及び消費者に追加費用を課す。
- (c) プライバシーを侵害し、秘密情報保護違反となる。
- (d) カナダ及び海外においてカナダ人が商業活動を行う際の通信の電子的手段の利用において、カナダ人の信頼を損なう。

CASL は、2010 年 12 月 15 日に可決され、2014 年 7 月 1 日に施行された。2017 年 7 月 1 日より、CASL 違反の影響を受けた個人は、私訴権によっても救済を求めることができるようになった。

イ 個人情報 の定義

CASL は PIPEDA の特別法であるため、個人情報の定義は、PIPEDA の定義に従う。なお、「センシティブインフォメーション」は、CASL において法的に定義されていない。

ウ 主な規制・権利の内容

第 6 条(1)は、不招請商業電子メッセージを禁止している。同条(1)(a)は、商業電子メッセージを送信する前に、同意又は黙示の同意を得ることを義務付けている。同条(2)は、商業電子メッセージの内容が所定の要件に適合する様式によることを義務付けている。

エ 適用範囲、適用除外内容

CASL は、カナダの顧客への商業電子メッセージの内容及び送信について制限している。第 2 条は、法律において制限された商業電子メッセージをウェブサイトその他のデータベース上のコンテンツへのハイパーリンクがメッセージ内に含まれるもの又はメッセージ内の連絡先情報による場合は、商業活動への参画を奨励することを目的とし、若しくは目的の一つとしていると合理的に断定できるものと定義している。第 5 条、第 6 条、第 7 条及び第 8 条は、適用範囲を商業活動（個人的関係を有する者又は家族関係者に送信された商業電子メッセージ、アプリケーションに関するメッセージ、特定の商取引を促進するために送信されたメッセージその他関連する目的等を除く。）に限定している。

オ 紛争処理手続き

CASL 第 14 条は、カナダラジオテレビ・電気通信委員会（CRTC）がスパム対策法違反に対する罰金を適用する旨定めている。CRTC は、法令遵守を検証するにあたって、同委員会への支援要請を行うことができる。第 20 条(3)は、CRTC が罰金の額を決定する際に考慮に入

れるべき要素に関する概要を定める。第 27 条は、CRTC が行った決定又は命令に関する連邦裁判所への上訴手続の概要を定める。

⑤ 銀行法 (Bank Act)

ア 法律の概要

銀行法は、カナダの国会において、1991 年 12 月 13 日に可決された。

イ 個人情報の定義

銀行法第 606 条(1)及び第 636 条(1)は、「秘密情報」を「公認の外資系銀行の事業若しくは事務又は公認の外資系銀行と取引を行っている者に関する一切の情報であって、議会制定法の運営又は執行により、監督庁又は監督庁の指揮命令に従って行為する者によって取得された情報及び当該情報から作成された一切の情報」と定義している。

第 955 条(1)は、「秘密情報」を「銀行持株会社の事業若しくは事務又は銀行持株会社と取引を行っている者に関する一切の情報であって、議会制定法の運営又は執行により、監督庁又は監督庁の指揮命令に従って行為する者によって取得された情報及び当該情報から作成された一切の情報」と定義している。

なお、「センシティブインフォメーション」は、銀行法においては特に定義されていない。

ウ 主な規制・権利の内容

第 606 条(1)、第 636 条(1)及び第 955 条(1)は、銀行による顧客個人の金融情報の利用及び開示を制限している。

エ 適用範囲、適用除外内容

第 606 条(1)、第 636 条(1)及び第 955 条(1)に基づき、個人の金融情報の違法開示から金融機関の全顧客を保護する。

⑥ プライバシー法 (Privacy Act)

ア 法律の概要

プライバシー法は、政府機関が保有する個人に関する個人情報に対する当該個人のプラ

イバシーを保護するカナダの現行法を拡大し、個人に当該情報へのアクセス権を与えることを目的とする（第1部第2条）。

プライバシー法は、1983年7月1日に施行された。

イ 個人情報の定義

「個人情報」は、第3条（定義）において、「その記録形態を問わず、特定可能な個人に関する情報」と定義される。

「センシティブインフォメーション」は、プライバシー法においては特に定義されていない。

ウ 主な規制・権利の内容

プライバシー法は、連邦政府機関による個人情報の取扱実務について定め、個人又は連邦政府の従業員に関するかを問わず、連邦政府が収集、利用及び開示する一切の個人情報に適用される。

第4条は、政府機関に対し、同機関の運用中の計画又は活動に直接関係するものでない限り、個人情報の収集を禁止している。第5条(1)は、個人情報は、本人から直接収集することを義務付けている。第5条(2)は、個人が[収集]目的について通知を受けることを義務付けている。第6条(1)は、個人情報の保存を義務付けている。第6条(2)は、政府機関に対し、その保有する個人情報の正確性を確保するために、すなわち、当該情報が正確、最新のものであり、可能な限り完全であるよう、あらゆる合理的措置を講じることを義務付けている。第6条(3)は、政府機関に対し、規則に従って個人情報を処理することを義務付けている。第7条は、政府機関の管理下にある、本人の同意なき個人情報の利用について、これが取得された目的と矛盾しない目的又は第8条(2)に定める特定の政府目的での利用以外の利用を制限している。第8条(1)は、第8条(2)に定める特定の政府目的に基づく場合を除き、個人情報の開示を制限している。第8条(5)は、第8条(2)(m)に基づき個人情報が開示された場合（すなわち、政府機関の長が開示に対する公益が開示によって生じ得るプライバシー侵害に上回る又は開示が明らかに、当該情報に関わる個人の利益となると判断した場合）に、その個人情報の開示について、合理的に実施可能な場合、プライバシー・コミッショナーに書面による通知を行うことを政府機関に義務付けている。第8条(5)に基づき、プライバシー・コミッショナーは、その後、当該情報に関わる個人に対して、開示について通知する場合がある。第8条(4)は、政府機関に対して、第8条(5)(2)(e)に基づく開示（すなわち、カナダの法律を執行することを目的とした調査機関による要請により行われた開示）に関して受領したすべての要請の写しを保持することを義務付けており、これらの写し及び記録をプライバシー・コミッショナーに提供するよう義務付けられる場

合がある。

また、同法は、連邦政府機関が保有する個人情報に関するアクセス権及び訂正請求権を個人に与えている。第 12 条は、個人情報バンクに含まれる個人に関する個人情報その他政府機関の管理下にある個人に関する個人情報へのアクセス権について定めている。同法第 13 条は、アクセス請求に関する要件の概要を定めている。

エ 適用範囲、適用除外内容

プライバシー法は、カナダの政府機関による個人情報の不正収集、利用又は開示からすべての個人を保護する。第 12 条(1)は、政府機関が保有する情報へのアクセス権をカナダの国民又は永住者に制限している。

オ 紛争処理手続き

第 29 条は、同法に基づく苦情に関する手続の概要を定める。第 29 条(1)は、プライバシー・コミッショナーに対して、同法第 12 条(1)に基づき、政府機関による個人情報の不正開示又はアクセス権の拒否を理由とする同法の違反に関する苦情を受け、これを調査することを義務付けている。第 31 条は、調査意向通知に関する要件及びプライバシー・コミッショナーによる手続の規制を含む同法に基づく調査に関する手続の概要を定める。第 34 条に基づき、プライバシー・コミッショナーは、同法に基づく苦情の調査にあたり、人々を召喚し、宣誓を行い、証拠を受領及び採用し、敷地内に立入り、敷地内で会話・聞き取りを行う権限を有する。同法第 35 条に基づき、プライバシー・コミッショナーは、調査に基づく認定事実及び勧告を行うことができる。政府機関は、プライバシー・コミッショナーの報告書に基づく勧告を実施し、又は苦情を申し立てた者に情報へのアクセス権を付与することを義務付けられる場合がある。第 35 条(5)に基づき、苦情を申し立てた者は、裁判所に申請することにより、再検討の権利を有する。

(3) 監督機関・第三者機関

① プライバシー・コミッショナー事務所 (Office of the Privacy Commissioner of Canada, OPC)

ア 設置の経緯

カナダのプライバシー・コミッショナー事務所 (OPC¹⁴) は、連邦政府の各部門及び機関の個人情報取扱い実務を規制するプライバシー法が可決されたことを受けて、1983年に設立された。

2001年に、OPCの任務が拡張され、PIPEDAの対象である民間部門の企業を含むようになった。

OPCの使命は、個人のプライバシー権を保護、促進することである。OPCの権能は、プライバシー法及びPIPEDAへのコンプライアンスを監視することである。政府から独立したカナダのプライバシー・コミッショナーは、国会に直属する。

イ 連絡先及びURL

OPC

30, Victoria Street

Gatineau, Quebec

K1A 1H3

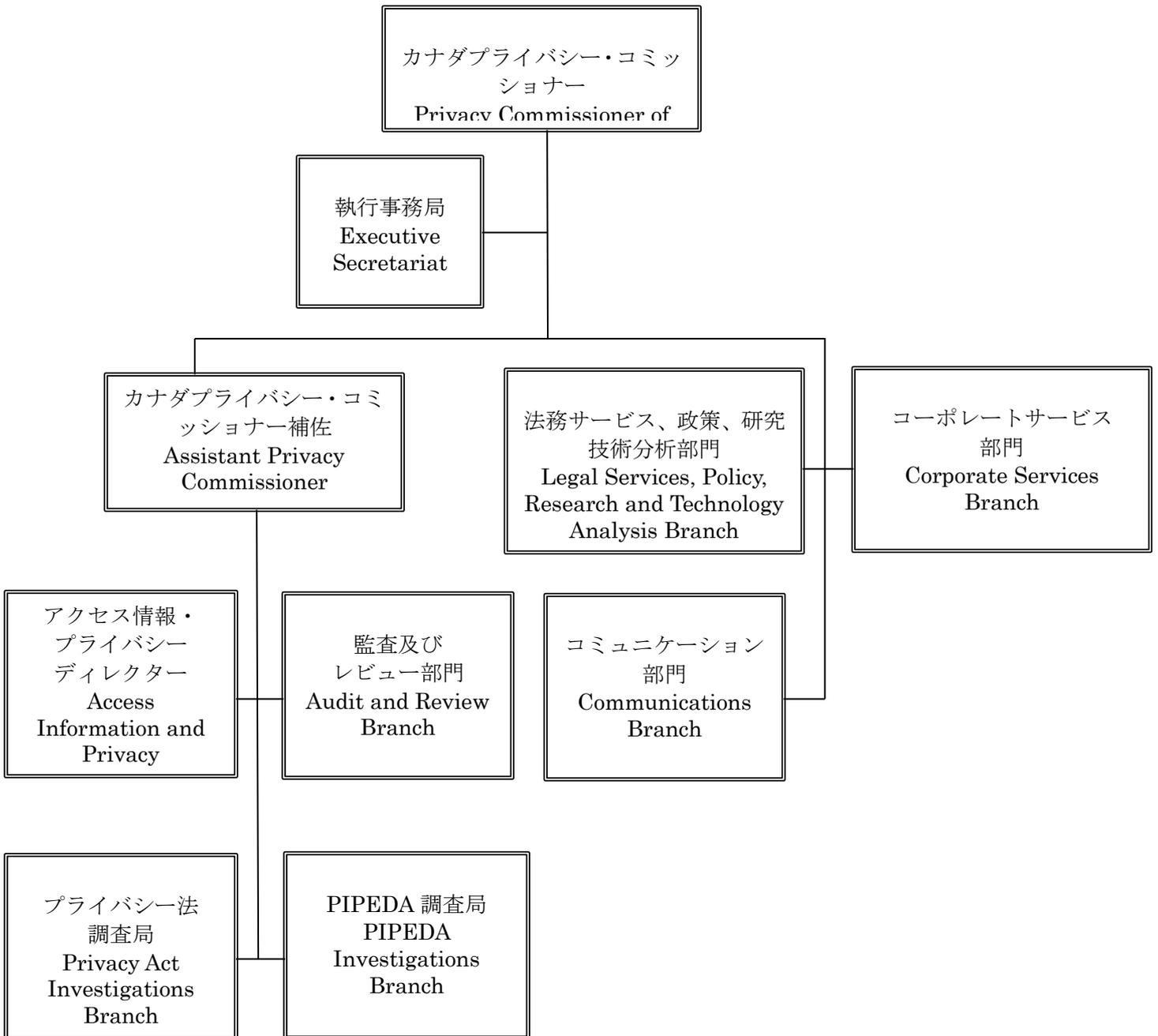
フリーダイヤル: 1-800-282-1376

電話: (819) 994-5444

ウェブサイト: www.priv.gc.ca

¹⁴ Office of the Privacy Commissioner of Canada の通称名

ウ 組織図¹⁵



15

https://www.priv.gc.ca/en/about-the-opc/opc-access-to-information-and-privacy/annual-reports-on-the-access-to-information-and-privacy/2016-2017/ar_201617_ati/?wbdisable=true

エ 制度の概要

カナダのプライバシー・コミッショナー事務所（OPC）には、3つの主要なプログラム及び内部サービスがある。3つのプログラムは、コンプライアンス活動、研究及び方針策定並びにパブリック・アウトリーチである。2016年から2017年の、OPCの実際の支出は、23,760,728ドルであった。2016年から2017年、OPCは、133名の人員について予算を計上し、実際には124名の人員を擁している。2017年から2018年及び2018年から2019年において、OPCは、それぞれ181名の人員について予算を計上した。

オ 運用実態

プライバシー・コミッショナーは、調査権限を有する。具体的に、ある企業に対して、プライバシーに関する苦情が申し立てられた際、プライバシー・コミッショナーは、当該企業のデータ保護慣行の調査を選択することができる。これらの調査に基づき、コミッショナーは、拘束力のない調査結果を交付することができる。コミッショナーがその報告を発行した後、その調査結果に不服のある申立人は、裁判所に聴取を申請することができる。この手続を通じた申立人による一定の事案は、裁判所における集団訴訟に発展している。

OPCは、2013年、プライバシー法に関して1,154件の事案において、また、PIPEDAに関しては587件の事案において、調査結果を交付した。

上述した通り、デジタルプライバシー法は、違反報告に関連する新たな規定をはじめとするPIPEDAに対する多くの改正を盛り込んでいる。違反規定は、理事会において知事の命令により改正される日においてのみ発効することになっており、2018年2月時点では未施行である。

これらの改正は、(i)コンプライアンス契約及び(ii)PIPEDAの違反（データ漏えいを含む。）に関する公益開示について定める際のコミッショナーの権限に追加される。

また、これらの改正は、影響を受けた個人に「重大な損害に関する現実的リスク」を生じさせる「保護措置違反」（すなわち、データ漏えい）について、組織がOPCに報告を行い、影響を受けた個人及び第三者に通知するための新たな要件を含んでいる（デジタルプライバシー法第10.1(3)）。デジタルプライバシー法第10.1(7)上、重大な損害は、とりわけ、身体的傷害、名誉棄損、信用又は関係性への毀損、雇用、事業又は専門的職務の喪失、財務上の損失及び個人情報盗難を含むものとして定義されている。第10.1項(8)は、組織が違反を報告すべきか判断する際に、違反のあったデータの機密性及びデータの悪用の可能性を考慮しなければならないことを明示している。

同法第10.2項は、違反通知の時間的要件を定めている。同法は、組織による違反の認識後可及的速やかなOPC及び個人への通知を義務付けている。また、デジタルプライバシー

法は、組織が被害の軽減に資すると考える他の組織や政府機関に通知を行うことを義務付けている。

同法第 10.3 項は、記録管理要件を定めており、組織にすべての個人情報違反の記録の写しを OPC に提供するよう義務付けている。

当該改正は、違反通知及び違反記録管理要件の違反に対する一定の金銭的な行政罰も盛り込んでいる。当該規定の違反に対しては、100,000 ドル以下の罰金が科せられる場合がある。さらに、申立人は、苦情の調査が中止されたとのコミッショナーの報告又は通知を受けた後、苦情が申し立てられた事項に関して、裁判所に対して聴取を申請することができる。裁判所は、その後、損害賠償を認める場合がある。

2015 年の PIPEDA 改正以前は、プライバシー・コミッショナーによる罰金は、組織の一般的慣習ではなかった。これらの改正法が発効することによって、罰金による OPC の強制執行措置が大幅に増加するかについては、未だ明らかではない。

これらのデジタルプライバシー法が発効するまで、PIPEDA に基づくデータ漏えい報告は、引き続き任意のものである。¹⁶

② CRTC

ア 設置の経緯

CRTC は、電気通信及び放送システムに関連したプライバシーに関する問題に対して監督権限を有する。CRTC は、公益にある放送及び電気通信を規制及び監督する行政裁判所である。その権能は、カナダの国会から委託され、カナダ文化遺産担当大臣を通じて管理されている。同委員会は、放送法、電気通信法及びスパム対策法において定められた方針の目的を達成することに注力している。

イ 連絡先及び URL

CRTC

住所 (Central Office):

Les Terrasses de la Chaudière

1 Promenade du Portage

Gatineau, Québec

¹⁶ 例えば、以下の「デジタルプライバシー法及び PIPEDA」を参照。

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/legislation-related-to-pipeda/02_05_d_63_s4/

J8X 4B1

住所（郵送先）：

カナダラジオテレビ・電気通信委員会

Ottawa, Ontario

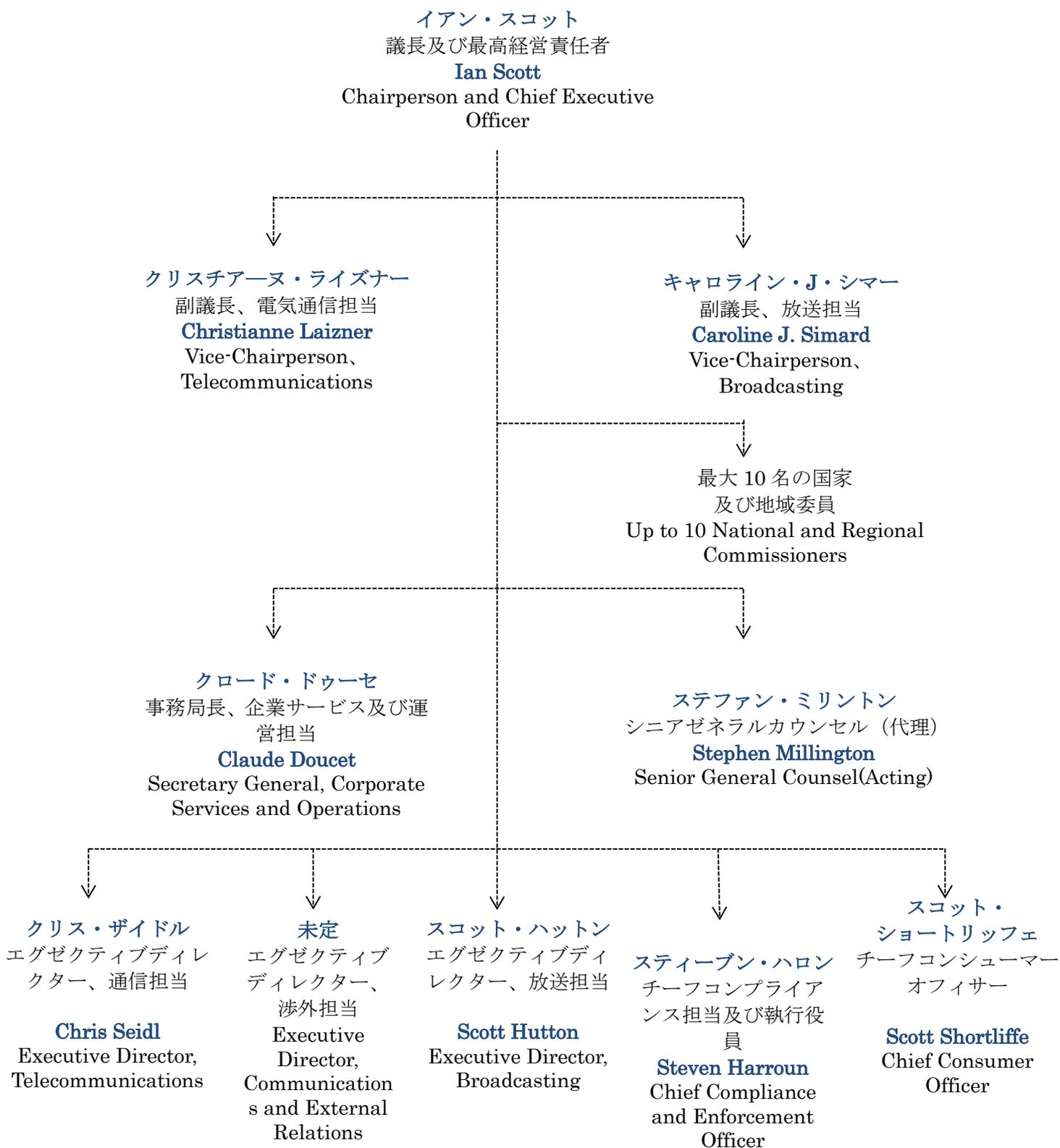
Canada, K1A 0N2

Fax: 819-953-0997/819-994-0218

電話: 819-997-4484

ウェブサイト: www.crtc.gc.ca/eng/home-accueil.htm

ウ 組織図



エ 制度の概要

CRTC の主な責務には、規制政策の策定、法の施行及び規制、利害関係者とのパブリック・アウトリーチ（現場出張サービス）及びエンゲージメント並びに監視、コンプライアンス及び強制執行が含まれる。

CRTC の主な役割は、迷惑電話制度の規制に関する連邦規則（Unsolicited Telecommunications Rules）、スパム対策法及び選挙人名簿（Voter Contact Registry）をはじめとする法令及び規制の遵守を推進及び執行することである。

CRTC には、3 つの戦略的成果及び内部サービス（カナダのコンテンツ作成、通信システムへの接続、通信システム内の保護及び内部サービス）を含む 4 つの主なプログラムがある。

オ 運用実態

CRTC は、スパム対策法及び迷惑電気通信規則の執行に責任を負う。

そのために、CRTC は、規制の遵守を推進、強化し、国内及び国際的な執行及び監督機関と協力して情報共有を高め、対象の特定を改善し、運営上の対応を調整する。CRTC は、行政裁判所として、主に「金銭的な行政罰」（Administrative monetary penalty）を科すこと、「裁判外紛争解決手続」（Alternative Case Resolutions）、出頭命令、違反通知及び保証／引受けにより、これを行っている。

（４） 近時のトピック

① 立法並びに行政機関ないし監督機関及び第三者機関の動向

2010 年に、プライバシー影響評価方針とプライバシー及びデータ保護方針に関する従前のガイドラインを置き換えるプライバシー影響評価に関する指令が発効した。この指令は、プライバシー法第 3 条で定義されるすべての政府機関（親会社である国有企業及びその完全出資子会社を含む。）が義務付けられたプライバシー影響評価（PIA）を行うためのガイドラインを定める。これらの PIA は、新たな又は再設計された連邦政府プログラム又はサービスの潜在的なプライバシーの危険を特定することが義務付けられている。ガイドラインに基づき、完了した PIA は、OPC 及び国家財政委員会事務局（TBS）に提出しなければならない。

2015 年の「OPC プライバシー優先順序設定」に関する協議に基づき、OPC は、2016 年に、PIPEDA に基づく同意の潜在的な強化に関する協議を開始した。提案された変更点には、個人情報収集に関する同意の要件を緩和し、代わりに説明責任や情報の倫理的利用又はリ

スクに基づく手法を用いることが盛り込まれている。OPC は、2016 年 5 月号で審議文書を発表し、同意書雛形の継続的実行可能性及びその他同意関連のトピックに関する意見を提供することで協議に参加するよう利害関係者を招待した。

2017 年 9 月 21 日、OPC は、その 2016 年から 2017 年の年次報告書の一部として、この協議の結果を概説する同意に関する報告書を発表した。同報告書は、その協議に基づき要約された 3 つの提言に焦点を当てたものである。最初の提言は、プライバシー通知のための要件、同意の様式及び青少年に対する制限を通じて、より有意義な同意を行うこと並びに PIPEDA 第 5 項(3)に基づき個人情報の適切な利用に関する指導を公表することに関するものである。二つ目の提言は、PIPEDA に基づく同意に代わるもの（匿名化、公表されている個人情報に特定する PIPEDA の規則に対する変更及び新たな同意の例外を設けることを含む。）を定めることである。三つ目の提言は、PIPEDA の統治／ガバナンス及び執行の強化に関するもの（現在の苦情申立てモデルに代わる、PIPEDA に基づく罰金賦課及び金銭的和解、要求に応じて OPC のコンプライアンスを検証する権限の強化並びに私的訴権の創出を含む。）である。

報告書によると、カナダのプライバシー・コミッショナーは、PIPEDA の違反に対してより重い罰則を定めるべく、PIPEDA に対する法改正についても提言している。プライバシー・コミッショナーも、OPC が自らの提言に基づく法改正前であっても、カナダ人に対するプライバシーの保護を推進するべく直ちに行動を開始することを示している。

また、OPC は、このほど、PIPEDA に基づき企業が関与する 2016 年以降の二つの事案につき、新たな概要を掲載した。一つの事案（PIPEDA 事例概要 #2016-011）において、OPC は、民事訴訟に対する防御は、PIPEDA 上、商業活動とみなされない旨判断している。もう一方の事案（早期解決事例概要 #2016-01）において、OPC は、PIPEDA に基づき、組織が個人に対し、最低費用又は無償で、アクセス請求に応じなければならないと判断した。

② 近時の主要な裁判例

Nammo 対 TransUnion of Canada, [2010] F.C. 1284 の判決において、カナダの連邦裁判所は、PIPEDA に基づき初めて損害賠償を認めた。*Lawson 対 Accusearch*, [2007] F.C. 125 において、連邦裁判所は、PIPEDA が域外適用を予定していない旨判断した。ただし、カナダのプライバシー・コミッショナー事務所は、PIPEDA がなお、カナダにおける個人に関する個人情報を収集及び開示する外国の事業体を対象とすることができると指摘している。別の重要な事案は、*State Farm Mutual 対プライバシー・コミッショナー*[2010] F.C. 736 であり、その中で、カナダの連邦裁判所は、国営農業がその被保険者を訴訟において防御する過程で個人情報を収集、利用又は開示する場合は、「商業活動」を行っているとは言えず、PIPEDA は適用されない旨判断した。

③ Google のストリートビューサービスやデータ収集行為に関する OPC の対応

Google は、2007 年 5 月、米国でストリートビューを開始した。プライバシー・コミッショナーは、Google がカナダにおいてサービスをスタートさせる前である 2007 年 9 月、PIPEDA に基づくカナダ人のプライバシー権が保護されることを要請するために、書簡を Google に送ったというプレスリリースを発表した。その書簡に対応するために、Google は、2007 年 9 月、カナダのストリートビューの画像において、識別可能な顔やナンバープレート番号の画像をぼかし始めた。

プライバシー・コミッショナーは、2009 年 8 月、ストリートビューについて、カナダ人の同意の必要性を確認させるための書簡を Google に送付した。その時は、Google のデータ保持ポリシーに関する懸念が高まった。

プライバシー・コミッショナーは、2010 年 6 月、Google の Wi-Fi を通じたデータ収集に関する調査を開始し、同年 10 月、「Google のストリートビューサービスのための自動車は、機密性の保証がない (unsecured) Wi-Fi ネットワークから、人件費に関する情報を収集したので、Google は PIPEDA に違反した。」と判断した。この調査では、Google がパスワード、電話番号、自宅住所などのデータを収集したことが判明した。プライバシー・コミッショナーは、制裁措置や罰金を勧告しなかったが、収集したデータを破棄し、プライバシー保護の実践を改善し、従業員にプライバシーの訓練を提供するよう Google に指導した。

OPC は、2011 年 1 月、調査報告書を発行した¹⁷。調査報告書は、「Google が収集の制限、目的と同意の特定に関する PIPEDA の要件に違反していた。」、「Google は OPC の勧告を完全に採用することに同意し、既に特定のプライバシー管理と対策を約束した。」、「OPC は、報告書の 1 年以内に Google が修正措置を実施したことを確認する予定である。」という内容である。

¹⁷ Google Inc. WiFi Data Collection
<https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigation-s-into-businesses/2011/pipeda-2011-001/>

3. オーストラリア

(1) 制度概要

① 法体系の概要

オーストラリアでは、1988年プライバシー法 (Privacy Act 1988)¹ (以下「プライバシー法」という。) が個人情報の取扱いについて規制している。またプライバシー法は消費者信用報告制度、納税番号及び医療研究のプライバシーに関する内容についても規制している。

プライバシー法に加え、オーストラリアにはその他プライバシーに関連する法律が多数存在する。個人情報に関する義務を詳細に定めるその他の法令には以下のものが含まれる。

- ・ 1953年税制管理法 (Taxation Administration Act 1953) 1953年3月4日制定
- ・ 2003年スパム法 (Spam Act 2003) (Cth²) 2003年12月12日制定
- ・ 2006年電話勧誘拒否登録法 (Do Not Call Register Act 2006) 2006年6月30日制定
- ・ 2006年マネーロンダリング／テロ資金供与防止法 (Anti-Money Laundering and Counter-Terrorism Financing Act 2006) 2006年12月12日制定
- ・ 2009年動産担保法 (Personal Property Securities Act 2009) 2009年12月14日制定
- ・ 2010年医療ID法 (Healthcare Identifiers Act 2010) 2010年6月28日制定
- ・ 2012年個人管理電子保険医療記録法 (Personally Controlled Electronic Health Records Act 2012) 2012年6月26日制定
- ・ 2015年電気通信傍受法改正 (データ保全) 法 (Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015) 1997年4月22日制定

② 民間部門・公的部門に適用される主な連邦法

プライバシー法は、会社その他の企業を含む民間部門を規制対象とすると同時に、オーストラリアの連邦政府及びその機関並びにオーストラリア首都特別区政府及びその機関による個人情報の取扱いに適用される。

¹ 1988年末にオーストラリア議会により可決され、1989年に施行された。経済協力開発機構 (OECD) 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並びに「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)」の第17条に基づく義務を履行するというオーストラリアの合意を実行に移すものと位置付けられている。

² 「Cth」は連邦法であることを示す略称である。

民間組織及び公的機関をあわせて APP (Australian Privacy Principles) 事業者と呼ばれ、プライバシー法の多くの規定がすべての APP 事業者に応用されるが、公的機関又は民間組織にのみそれぞれ適用されるものもある。APP 事業者には、民間組織（自然人、法人、組合その他の法人格のない団体及び信託など）及び連邦政府機関（オーストラリア証券投資コミッショナー（企業及び金融サービスに関する規制機関、オーストラリア競争消費者コミッショナー（競争及び公正取引に関する規制機関）など）が含まれる。

③ 個人情報に関する州法

州レベルでもさまざまなプライバシー法令が存在している。これらは全般的に以下について規制している。

- ・ 公的部門による個人データの取扱い
- ・ 公的、民間の双方の部門による健康関連の個人データの取扱い、監視及び前科情報の取扱い等

なお、プライバシー法は州又は地域の政府機関には適用がない。

（2）主な法律の概要

① プライバシー法

ア 法律の概要

プライバシー法は、個人データ（本法において「個人情報 (Personal information)」という。）の収集、利用及び開示について規定している。プライバシー法は、オーストラリア・プライバシー原則の導入を含め、2014年3月に大幅な改正が施行された。

同法には、13のオーストラリア・プライバシー原則(Australian Privacy Principles, APP)が含まれる。この原則は、ほぼ全てのオーストラリア及びノーフォーク島政府機関、年間売上高が300万ドル（以下、「ドル」はオーストラリアドルをいう。）以上のAPP事業者による個人情報の取扱い、利用及び管理についての概要を定めている。

APPは行為規範であり、各事業者は、自社の状況に原則がどのように適用されるかを判断しなければならない。同原則の概要は、以下のとおりである³。

- ・ APP 第1項 オープンで透明性の高い個人情報のマネジメント
- ・ APP 第2項 匿名性と仮名性

³ 個人情報保護における国際的枠組みの改正動向調査報告書、205頁以下参照。

(https://www.ppc.go.jp/files/pdf/personal_report_260328caa.pdf、アクセス日：2018年3月12日)

- ・ APP 第 3 項 個人情報と機微情報の収集
- ・ APP 第 4 項 望まぬ個人情報の取り扱い
- ・ APP 第 5 項 収集通知
- ・ APP 第 6 項 利用又は開示
- ・ APP 第 7 項 ダイレクトマーケティング
- ・ APP 第 8 項 越境開示
- ・ APP 第 9 項 政府関連識別子の採用、利用又は開示
- ・ APP 第 10 項 正確性
- ・ APP 第 11 項 安全管理
- ・ APP 第 12 項 開示
- ・ APP 第 13 項 訂正

イ 個人情報の定義

プライバシー法は、第 6 条 (1) において「個人情報 (Personal information)」を以下のように定義している。

「特定の個人又は合理的に特定可能な個人に関する情報又は意見をいい、

- a. 情報又は意見が真実であるか否かを問わず、かつ
- b. 情報又は意見が有体物に記録されているか否かを問わない。」

本定義は、時代の変化に伴う情報取扱実務のさまざまな変化に常に十分な対応をすべく、中立的な内容となっている。また、国際的な基準及び前例とも合致している。さらに、個人情報の定義には、個人の私的又は家族生活に関する情報に留まらず、合理的に個人を識別可能な個人に関する一切の情報又は意見にも及ぶ。かかる情報には、個人の行う事業又は職業に関する情報が含まれる。個人情報は、センシティブ情報や機密情報から公的に入手可能な情報にまで及ぶ。その定義は、不正確な情報であっても個人情報であることを明らかにしている。

「個人情報 (Personal information)」という用語には、広範囲の情報が含まれる。プライバシー法上、個人情報はさまざまな異なる種類の情報から構成されるものと明示的に確認されている。例えば、以下の情報はすべて個人情報の一種である。

- ・ 「センシティブ情報 (Sensitive information)」（個人の人種的若しくは種族的出身、政治的意見、宗教的信念、性的指向又は犯罪歴に関する情報又は意見を含む。ただし、かかる情報又は意見が別途個人情報の定義を満たすことを条件とする。）
- ・ 「健康情報 (Health information)」（これは「機密情報 (Sensitive information)」でもある。）
- ・ 「信用情報 (Credit information) 」
- ・ 「雇用者記録 (Employee record) 」情報 (例外あり。)

・ 「納税番号情報 (Tax file number information) 」

センシティブ情報とは、付加的な保護を与えられる個人情報の部分的な集合をいい、同条において以下のように定義されている

- (a) 以下の各号に関する個人の情報又は意見
 - (i) 人種又は民族に関する出自
 - (ii) 政治的意見
 - (iii) 政治組織への加入
 - (iv) 宗教的信念又は信仰
 - (v) 思想
 - (vi) 専門職又は事業者団体への加入
 - (vii) 労働組合への加入
 - (viii) 性的嗜好又は性癖
 - (ix) 犯罪歴

のうち個人情報でもあるもの又は

- (b) 個人に関する健康情報
- (c) 健康情報以外の個人に関する遺伝子情報
- (d) 自動生体照合又は生体認証に用いられる生体情報
- (e) 生体テンプレート

情報は、同法において個人情報として明示的に認められていなくとも、他の法令に基づき明確に個人情報とみなされる場合もある。例えば、1979年電気通信傍受法 (Telecommunications (Interceptions and Access) Act 1979) (Cth) 上、一定の電気通信データ (「メタデータ (Metadata)」をいう場合もある。) は、同法における個人情報とみなされる。

医療情報は、個人情報の中でも特に慎重な取扱いが求められる類型のものと考えられている。このため、同法では、その取扱いに関してより一層の保護を定めている。例えば、組織体は通常、健康情報を収集する前に、個人の同意を必要とする。さらに、医療サービスを提供し、健康情報 (従業員記録に含まれるものを除く。) を保有するすべての組織は、中小企業も含めて、同法の適用対象となる。

ウ 個人情報漏えい時等における監督当局及び本人に対する報告義務等に関する条文

2017年2月13日、連邦議会は、データ漏えいの通告義務要件をプライバシー法に盛り込んだ、2017年プライバシー改正 (通告を要するデータ漏えい) 法 (Privacy Amendment (Notifiable Data Breaches) Act) を制定した。これらの規定は、現在、オーストラリア情報コミッショナー事務局 (Office of the Australian Information Commissioner, OAIC) により施行されているデータ漏えいの任意通告ガイドラインに代わるものと位置づけられ

る。これは、関係する個人に対し深刻な侵害を及ぼす可能性があるとして一般人が判断すると
思料される「対象データ漏えい (Eligible data breach)」を APP 事業者が経験した場合には、
オーストラリア情報コミッショナー (Australian Information Commissioner。以下「情報
コミッショナー」という。) 及び影響を受けた個人の双方に通告を行うことを、APP 事業
者に対して義務付けるものである。

「対象データ漏えい (Eligible data breach)」は、以下の場合に発生する。

- ・ 事業者が保有する個人情報について、不正アクセス、不正開示又は紛失が生じた場合
- ・ アクセス、開示又は紛失が、当該情報の対象者たる個人に重大な損害をもたらす可能性
がある場合

改正法においては、「重大な損害 (Serious harm)」は定義されていないが、重大な損害
の可能性の有無の判断に関連する事項を複数列挙しており、これには情報の種類、情報の
機密性、実施されているセキュリティ保護、情報を入手した者又は人々の種類、並びに損
害の性質等が含まれる。かかる要素を適用すると、消費者のパスワードデータ入手を目的
とした標的型ハッキングが行われた場合について通知が義務づけられる可能性が高い。

損害の種類観点において、通知義務を生じさせる重大な損害の最も典型的な形態として
は、重大な経済的損害又は身体的損害のリスクが想定される。しかし、場合によっては、
重大な心理的又は精神的損害、名誉棄損その他の重大な損害のリスクも存在し得るとい
う合理的意見もあり得る。例えば、対象データ漏えいにおいて医療情報その他の「センシテ
ィブ情報 (Sensitive information)」が含まれている場合が考えられる。

通知義務にはいくつかの例外があり、それらのなかには法執行機関の活動を妨げること
や他の法律の守秘義務規定と矛盾する場合に情報開示することを避けるという公共の利益
のための例外が含まれる。例外を除き、ある事業者において対象データ漏えいが発生した
と疑うべき理由がある場合、当該事業者には、状況に関する合理的かつ迅速な評価を行い、
いずれの場合もその評価を 30 日以内に完了すべく一切の合理的な措置を取ることが義務付
けられている。

ある事業者において対象データ漏えいが発生したと信ずべき合理的な理由がある場合、
当該事業者は、評価やその他の措置をとった後に、情報コミッショナー及び影響を受けた
個人に通告しなければならない。合理的理由とは、直接的な証拠又は間接的な推認のい
ずれかとなる。例えば、同一の内容の申立てが複数あった場合、当該事業者において対象デ
ータ漏えいが発生したと信じるべき合理的な理由があると考えられる場合がある。

情報コミッショナーに対する通告の様式は、「第 26WK (2) (a) (i) 項書面」による。通
告の際に必要なとされる情報には、事業者の身元及び連絡先情報、事業者が発生したと信ず
べき合理的理由のある対象データ漏えいの内容、関連情報の種類、及びデータ漏えいに対
して個人が取るべき措置に関する提言が含まれる。かかる提言は、自己の情報が対象デー
タ漏えいに含まれていた個人に対し、漏えいの結果発生し得る損害を軽減するために取る
べき措置に関する一般的な助言を提供することを目的としている。例えば、対象データ漏

えいが信用を利用した詐欺を惹起し得る場合、その報告書の写しを求めるよう個人に勧めている。

情報コミッショナーは、データ漏えい通告義務を遵守しないという疑いについて調査し、場合によっては当該不遵守を是正するよう事業者に義務付ける決定を下す権限を有している。情報コミッショナーは既に、たびたびデータ漏えいの通告を受けており、かかる通告の判断において豊富な経験を有している。新規規定は、移行期間が設けられており、要件の中には、同法の運用が開始されるまでは適用しないものもある。

エ 安全管理措置に関する規定

プライバシー法に含まれる 13 の APP のうち、APP 第 11 項は、APP 事業者に対し、自己の保有する個人情報の安全性を確保する積極的な措置を取ること、及び自らがかかる個人情報を保持することを認められているか否かを積極的に検討するよう義務付けている。

具体的には、APP 第 11.1 項は、個人情報を保有する APP 事業者について、濫用、妨害及び紛失並びに不正アクセス、改ざん又は開示から情報を保護するための合理的な措置を取らなければならないと定めている。

APP 事業者は、APP 第 11.2 項に基づき、自己が保有する個人情報について、APP に基づくその利用又は開示目的のために必要なくなった場合には、直ちにこれを破棄又は匿名化するための合理的な措置を取らなければならない。この要件は、個人情報が「連邦記録 (Commonwealth record)」に含まれる場合又は事業者が法律若しくは裁判所や審判所の命令により個人情報の保持を義務付けられる場合には適用されない。

なお、事業者が個人情報を「保有する (Holds)」とは、「当該事業者が個人情報の含まれる記録を保有し又は管理している」場合を指す。「保有する (Holds)」とは、物理的な保有に限らず、事業者が取り扱う権利又は権限を有する記録を含む。例えば、個人情報の保管を第三者に委託していても、当該情報を取り扱う（これにアクセスし、変更することを含む。）権利を保持している事業者は、当該個人情報を「保有している (Holds)」と言える。

また、個人情報の安全を検討する際、APP 第 8 項（個人情報の越境開示）及び APP 第 12 項（個人情報へのアクセス）等のプライバシー法上の他の義務についても検討する必要がある。さらに、すべての事業者は、個人情報の安全に関するその他の義務を課す関連法令（APP を除く。）についても認識しておく必要がある。

同法パート IIIA 及び登録 CR コード⁴の対象である信用状況報告を行う団体若しくは信用供与者、2011 年納税番号ガイドラインの対象である納税番号受領者、又は 2012 年個人管理電子保険医療記録法若しくは 2010 年医療 ID 法の対象であるヘルスケア提供者は、追加的な個人情報に関する安全義務を負う場合がある。

⁴ CR コードとは、信用状況報告 (Credit Reporting) についての実務を文書化したものをいう (第 26N 条 (1))。

オ 適用範囲及び適用除外

オーストラリア政府機関（及びノーフォーク島政府）並びに年間売上高が 300 万ドルを超えるのすべての企業及び非営利団体は、一定の例外を除き、プライバシー法に基づく責任を負う。また、以下のような一定の中小規模事業者（年間売上高が 300 万ドル以下の組織）は、同法の対象となる。

- ・ 民間医療サービス提供者及び医療サービスを提供する組織には下記が含まれる。
 - ・ 私立病院、日帰り手術、医師、薬剤師及び医療従事者等の従来の医療サービス提供者
 - ・ 自然療法医やカイロプラクター等の補完療法士
 - ・ ジム及び減量クリニック
 - ・ 託児所、私立学校及び私立第三教育機関
- ・ 個人情報売買を行う企業
- ・ 信用報告を行う団体
- ・ 連邦契約 Commonwealth contract に対する委託業務提供者
- ・ 2009 年公正労働（登録組織）法（Fair Work（Registered Organisations） Act 2009）に基づき登録され又は認められる従業員組合
- ・ 同法に同意した企業
- ・ 同法の対象企業の関連企業
- ・ 2013 年プライバシー規制において指定される企業

さらに、以下を含む他の中小規模事業者の特定の行為及び実務が同法の対象となる。

- ・ 2006 年マネーロンダリング／テロ資金供与防止法（Anti-Money Laundering and Counter-Terrorism Financing Act 2006）並びにその規制及び規則に関連する報告事業者又は授権代理人の活動
- ・ 住居テナントのデータベースの運用に関連する行為及び実務
- ・ 保護措置の投票（Protection action ballot）の実施に関連する活動

また、同法は以下の特定の個人の取扱いに適用される。

- ・ 消費者信用報告情報（信用報告を行う団体、電力会社、水道局及び通信サービス提供者を含む信用供与者、並びに一定のその他の第三者を含む。）
- ・ 納税番号ガイドラインに基づく納税番号
- ・ 動産担保登記簿に含まれる個人情報
- ・ 連邦消滅前科スキームに基づく過去の有罪判決情報
- ・ 2012 年マイ・ヘルス・レコード法（My Health Records Act 2012）に基づくマイ・ヘル

ス・レコード情報及び 2010 年医療 ID 法 (Healthcare Identifiers Act 2010) に基づく個人ヘルスケア識別番号

他方、以下は同法の適用除外となる。

- ・ 州又は地域の政府機関 (州及び地域の法令の対象となっている州又は地域の公共病院及び医療機関を含むが、マイ・ヘルス・レコード及び個人ヘルスケア識別番号に関連する一定の行為及び実務や 2013 年プライバシー規制において指定される組織を除く。)
- ・ 自己の資格において行為する個人 (隣人を含む。)
- ・ 私立大学及びオーストラリア国立大学以外の大学
- ・ 公立学校
- ・ 一定の状況において、現在及び過去の雇用関係に関連する、組織による雇用者記録の取扱い
- ・ 中小規模事業者 (例外が適用される場合を除く (上記参照))
- ・ ジャーナリズムに携わるメディア機関 (組織が公表されたプライバシー基準の遵守を公にしている場合)
- ・ 登録政党及び代議士

カ 個人情報の開示

個人情報について規制対象となる行為又は慣習は、個人情報の利用又は開示である。よって、個人情報の保管及び管理が外部委託処理サービスの提供者に移転するか否かは関係がない。何らかの形で個人情報へのアクセスの提供を受ける際にその提供者を通じた開示があれば十分となる。

そのため、オーストラリアにおいて外部委託処理サービスを提供する事業者への個人情報の移転は、プライバシー法上の個人情報の開示とみなされる。同法は、外部委託処理サービス提供者への個人情報の開示と個人情報のその他の第三者への開示を区別していないことに注意が必要である。

開示は、APP 第 6 項に従って行われる必要がある。

APP 第 6 項の内容は、組織による個人情報の開示が情報収集の第一次目的又はそれに関連する二次的目的に合致しない限り、これを全般的に禁止するというものである。すなわち、個人情報は特定の目的にしか用いることは出来ず、その他の目的には利用できないのが原則である。ただし、関連法人による利用又は開示に関連して、同法に基づく例外がある。関連法人は、広くプライバシー規制の目的において、単一事業者として取り扱われる。

キ 個人情報の越境移転

他方、越境開示はAPP第8項に従って行われる必要がある。

APP 第 8 項は、越境開示にアカウントビリティの手法を導入し、オーストラリア国外の受領者に対する個人情報の開示についても制限を課している。これらの制限は、APP 第 6 項に基づく開示制限に加重適用される。

一例として、オーストラリアの規制対象個人情報に関連して、組織はオーストラリアの規制対象個人情報をオーストラリア国内の自己の支店等からオーストラリア国外の別の支店等へ移転すること、又は自己のオーストラリアに所在するデータベースへの電子アクセスを自己の海外支店等に提供することができる。ただし、オーストラリアの規制対象個人情報の第三者たる「海外受領者 (Overseas recipient)」(開示者の関連法人を含む。)に対する移転又は電子アクセス(読取専用を含む。)の提供は、個人情報の開示に該当する。個人情報が開示された第三者がオーストラリア国外に所在する場合、APP 第 8 項(越境開示)が適用される。

APP 第 8 項は、委託先ホスティングサービスの提供者に対する暗号化されたオーストラリアの規制対象個人情報の保管及び管理の提供に関する共通のシナリオについて特段言及していない。委託先ホスティングサービスの提供者又は個人情報へのアクセスができると合理的に考えられる者が個人情報を解読し、少なくともこれを閲覧する能力を有している可能性があるという合理的な可能性がない限り、海外の受領者に対する当該個人情報の「開示 (Disclosure)」は存在しないとするのが妥当な見解である。この見解に基づき、かかる能力は、委託先ホスティングサービスの提供者又は個人情報へのアクセスを有すると合理的に考えられる者の技術的な能力並びに解読その他の濫用に対する運用上及び契約上の対策を総合的に考慮の上、判断する必要がある。APP 第 8 項に関する OAIIC の APP ガイドラインは第 8.14 項において、以下の場合、限定的な目的(保管及びオーストラリアの規制対象事業者が当該情報にアクセスできるように確保すること。)のための海外に所在するクラウドサービス提供者に対する個人情報の提供については、オーストラリアの規制対象事業者による「開示 (Disclosure)」ではなく、むしろ「利用 (Use)」であると OAIIC が見なすであろうと示唆している。

- ・ 提供者との契約において、当該提供者が限定的な目的のためにのみ情報を取り扱うことを義務付けられている場合
- ・ 提供者との契約において、提供者の再委託先が同様の義務に同意しなければならない旨義務付けられている場合
- ・ 提供者との契約において、個人情報の海外事業者による取扱い方法の実質的な管理をオーストラリアの事業者任せしている場合。OAIIC によると、APP 事業者が情報の実質的な管理権を保持することを示す契約上の指標には、当該事業者が個人情報にアクセスし、これを変更又は検索する権利又は権限を保有しているか否か、その他いかなる者が何の目的で個人情報にアクセス可能であるか、個人情報の保管及び管理についてどのような種類の安全措置が用いられるのか、及び契約終了時において不要となった場合に、事業

者が個人情報を検索し又は恒久的に削除することができるか否かが含まれる。

APP 第 8 項及びプライバシー法第 16C 条は、個人情報の越境開示に対し、説明責任によるアプローチを採用している。APP 第 8 項及びプライバシー法第 16C 条の説明責任要件は、第一受領者及びそれに続く受領者について提供される。ただし、オーストラリア国外において行われる行為又は運用は、それが外国の適用法により義務付けられるものである場合は、APP 違反とはならない。

APP 第 8.1 項の内容は、組織は、個人情報を海外の受領者に開示する前に、海外の受領者が当該情報に関連して APP（APP 第 1 条を除く。）に違反しないよう、合理的な措置を取らなければならないというものである。一定の状況下においては、APP に違反していると思料される海外の受領者が行った行為又は実行は、組織による APP の違反と見なされる。一般的に、これは以下の場合に適用される。

- APP 第 8.1 項が開示に適用される場合（APP 第 8.1 項は、APP 第 8.2 項の例外が提供される場合を除き、すべての個人情報の越境開示に適用される。）
- 海外の受領者が APP の対象ではないが、対象であったとすれば、その行為又は実行が APP 違反となる場合

APP 第 8.2 項は、APP 第 8.1 項に対するさまざまな例外を挙げている。例えば、以下の例外が存在する（以下の場合、APP 第 8.1 項は以下の場合には適用されない）。

- 受領者が全般的に APP と実質的に類似する方法によって情報を保護する効果を有する法律又は拘束力を有するスキームの対象となっていること、及び当該法律又は拘束力を有するスキームの保護を施行するメカニズムが個人に提供されていると組織が合理的に信じる場合（APP 第 8.2 項 (a))
- 同意すれば APP 第 8.1 項が適用されなくなる旨を組織が明示的に連絡した後、個人が越境開示に同意する場合（APP 第 8.2 項 (b))⁵
- 越境開示がオーストラリア法又は裁判所／審判所の命令により又はこれに基づき、必要とされ又は認められる場合（APP 第 8.2 項 (c))
- いずれかの個人の生命、健康又は安全に対する重大な脅威を緩和又は防ぐために開示が必要であると組織が合理的に考える場合（APP 第 8.2 項 (d) 、第 16A 条第 1 号）
- その機能又は活動に関連する違法な活動又は重大な性質の違法行為の疑いに関連して措置を取るために開示が必要であると組織が合理的に考える場合（APP 第 8.2 項 (d) 、第 16A 条第 2 号）
- APP 事業者、団体又は個人が、行方不明とされている者を発見するのを支援するために

⁵ APP 第 8.2 項 (a) 及び (b) の二つの例外はそれぞれ、解釈及び適用は容易ではない。例外を持ち出せば、大きな議論及び規制上の監視の対象になる可能性が高いであろう。APP 第 8.2 項 (a) に関しては、その法律又は拘束力を有するスキームが全般的に APP と実質的に類似する方法によって情報を保護する効果を有し、かつ、適切に効果的で利用可能な執行メカニズムを可能とするとして OAIC が判断する国の一覧を OAIC は発表していない。

開示が必要であると組織が合理的に考える場合（APP 第 8.2 項（d）、第 16A 条第 3 号）

ク 紛争解決手続き

プライバシー法第 36 条は、オーストラリア人は、プライバシー権が侵害されたと考えた場合、OAIIC コミッショナーに訴えることができる旨定めている（ただし、承認済みのプライバシー・コードに基づき、自己の紛争解決の仕組みを有する組織によりプライバシーが侵害された場合を除く）。情報コミッショナーは、申立ての調査を決定することができ、かつ、一定の場合においてこれを調査しなければならない、また、第 44 条に基づき他の者から関連する証拠を取得することができる。一定の場合を除き、情報コミッショナーの決定に対し、裁判所又は審判所への上訴はできない。第 45 条は、情報コミッショナーが国民に対して聴取することを認めており、国民は、真実を述べる旨を宣誓しなければならない場合がある。情報コミッショナーに対し陳述することを怠った者は、2,000 ドル以下の罰金若しくは 1 年間の禁固刑、又はその両方に処される場合がある（第 65 条）。情報コミッショナーは、第 64 条に基づき、その職務を遂行するために自己が当事者となり得る訴訟に対する免責も与えられている。

情報コミッショナーが申立てを受理しない場合、オーストラリア人は第 63 条に基づき法的援助を受けることができる。オーストラリア連邦裁判所に申立てが提起された場合、一定の状況において、他の者も法的援助を得ることができる。

② 1953 年税制管理法（Taxation Administration Act 1953）（Cth）

同法は、一定の納税者情報の開示を禁止し、税務署員に対しかかる情報について厳格な義務を課している。

③ 1997 年電気通信法（Telecommunications Act 1997）（Cth）

同法は、電気通信又はインターネット・サービス提供者の顧客に関する個人データの無断開示を禁止している。情報コミッショナーは、1997 年電気通信法の執行に関してさまざまな権限を有し、義務を負う。

④ 2003 年スパム法（Spam Act 2003）（Cth）

同法は、「オーストラリアとの関連性（Australian link）」を伴う「未承諾商業電子メッセージ（Unsolicited commercial electronic messages）」（いわゆるスパム）の送付を禁止している。オーストラリアで発生し若しくは送信された場合、又は海外で発生したがオ

オーストラリアでアクセスされた住所に送付された場合に、メッセージはオーストラリアとの関連性を有するとみなされる。

スパム法は、電子メール、携帯電話のテキスト・メッセージ（SMS）、マルチメディア・メッセージング（MMS）、インスタント・メッセージング（iM）その他の商業的な性質の電子メッセージに適用される。ただし、同法は、音声又はファックスによるテレマーケティングには適用されない。テレマーケティング目的の電話及びファックスは、ドゥ・ノット・コール・レジスターの対象である。

⑤ 2006年電話勧誘拒否登録法（Do Not Call Register Act 2006）（Cth）

同法は、国のドゥ・ノット・コール・レジスターに登録された電話番号にテレマーケティング目的の電話をかけることを禁止している。

⑥ 2006年マネーロンダリング／テロ資金供与防止法（The Anti-Money Laundering and Counter-Terrorism Financing Act 2006, AML/CTF）

同法及びマネーロンダリング／テロ資金供与防止規則（AML/CTF規則）は、特定のサービス（「指定サービス（Designated services）」）を提供する金融部門、ギャンブル部門、送金（資金移転）サービス、貴金属商その他の専門家又は企業（「報告事業者（Reporting entities）」）に対しさまざまな義務を課すことにより、マネーロンダリング及びテロ資金供与を防止することを目的としている。かかる義務には、当該サービスの提供時に顧客の身元に関する一定の「身元確認」（Know Your Customer, KYC）情報を収集、検証することが含まれる。

（3）監督機関・第三者機関

① オーストラリア情報コミッショナー事務局（OAIC）

www.oaic.gov.au/

電話番号：1300 363 992

電子メール：enquiries@oaic.gov.au

ア 概要

OAIC は、2010年オーストラリア情報コミッショナー法（Australian Information Commissioner Act 2010）に基づき設立された独立機関である。OAIC は、プライバシー遵守

を促進するために調査を行い、申立てを取り扱い、一般市民及び業界に対し情報を提供する責任を負う独立機関である。そのプライバシー遵守機能に加えて、OAIC は、情報法に関する政府の自由を監視する責任を負う。OAIC は、2010 年度に行われた情報の自由に関する連邦法令に対する主な変更の一環として設立された。旧プライバシー・コミッショナー事務局 (OPC) は、2010 年 11 月 1 日付けで OAIC に統合された。

OAIC の三つの主な機能は以下のとおりである。

- ・ 情報コミッショナーについての機能-オーストラリア政府機関への情報方針及び管理実務に関する助言
- ・ プライバシーについての機能-1998 年プライバシー法その他の法令に従った適切な個人情報取扱いを確保することによる個人のプライバシーの保護
- ・ 情報の自由についての機能-1982 年情報の自由法 (Freedom of Information Act 1982, FOI) に基づく、オーストラリア政府が保有する文書へのアクセス権に関する一般市民への啓蒙活動

OAIC は、オーストラリア情報コミッショナーを長としている。全コミッショナーは、その役職にかかわらず、プライバシー及び情報の自由に対する権能を行使することができる。OAIC の責任には、下記が含まれる。

- ・ 調査の実施
- ・ FOI 法に基づきなされた決定の精査
- ・ 申立ての取扱い
- ・ 公的機関運営の監視
- ・ 教育及び啓蒙プログラム
- ・ 一般市民、政府機関及び企業に対する助言の提供

平均人員数は、75 名である。予算措置につき、予算書第 2: 2016-17 は、政府が 4 年間にわたり、OAIC の運営を継続させるために、8100 万ドルを提供することを定めている。さらに、プライバシー機能について毎年 6700 万ドルがオーストラリア人権委員会から OAIC に送金され、毎年 60 万ドルが情報の自由機能のために、法務省から送金される。

プライバシー法において、オーストラリア情報コミッショナーは、納税番号 (Tax file numbers) の取扱いに関連するさまざまな監視、助言及び評価関連の役割を担うこととされている。

OAIC は、適切な個人情報の取扱いを確保することによる、個人のプライバシー保護を目的とする一連の機能及び権限を有する。これらの機能及び権限は、プライバシー法及びプライバシー保護規定を定めるその他の法令により付与される。

OAIC の方針は、プライバシー法その他の法令によりコミッショナーに付与された規制上の権限の行使に関連するものである。かかる権限には、OAIC にコンプライアンス及びベスト・プラクティスによるプライバシー実務を促進するために、規制対象事業者と連動し、協働することを認める権限、並びにプライバシー違反を是正するための調査及び執行権限

が含まれる。コミッショナーの権限のほとんどは、OAIC の職員に委任され、OAIC の職員が行使することができる。

プライバシー法の規制対象である事業者は、同法の関連規定及び同法に基づき策定される法規書を遵守するよう義務付けられている。この義務は、APP 又は登録 APP コード⁶を遵守しなければならない機関及び組織、(信用状況報告に関連する) パート IIIA 及び登録 CR コードを遵守しなければならない信用状況報告参加者、並びにプライバシー法第 17 条に基づき発行された 2011 年納税番号ガイドラインを遵守しなければならない納税番号受領者に適用される。

これらの規定のいずれかの違反は、「プライバシーの侵害 (Interference with privacy)」とみなされる。「プライバシーの侵害 (Interference with privacy)」は、他の法令に定められた規定の違反からも発生し得る。OAIC は、申立て又は情報コミッショナー自身のイニシアティブ (情報コミッショナー開始調査 (Commissioner Initiated Investigation, CII)) のいずれかに従って、プライバシー侵害の疑い (及び一定の他のプライバシー違反) を調査することができる。申立て又は CII により、執行措置が取られることがある。

情報コミッショナーはまた、個人的に収集された電子健康記録 (Personally Controlled Electronic Health Record, PCEHR) システムに関連して、プライバシー規制の責任を負う。ただし、2013 年 PCEHR (情報コミッショナー執行権限) ガイドラインは、齟齬がある場合は、OAIC の方針に定められた内容に優先する。

OAIC は、プライバシー規制措置を取る際、以下の原則に従う。

- ・ 独立-OAIC は、独立して行為し、公平かつ客観的な措置を取る。
- ・ 説明責任-OAIC は、一連の精査及び上訴権を通して、そのプライバシー規制措置について説明責任を負い、権利保有者がそれらの権利を認識するようにする。
- ・ 相応性-OAIC のプライバシー規制措置は、該当する状況又は行為に相応なものとする。
- ・ 一貫性-OAIC は、OAIC 方針に従い、これを反映した方法で、一貫した行動を取るよう努める。
- ・ 適時性-OAIC は、可及的速やかに規制措置を取り、解決を図るべく努める。
- ・ 透明性-OAIC は、関連ガイダンスの公表による方法を含め、自己のプライバシー規制権限の行使及び自己が取る規制措置について情報開示するものとする。

プライバシー規制措置を取るにあたって、OAIC は、2017 年に行政審査委員会 (Administrative Review Council) により公表されたベスト・プラクティス・ガイドにおいて説示されている根拠のある意思決定という一般原則に従う。具体的には、OAIC は、公正かつ自然的正義 (又は手続上の公平性) の原則に従って行動する。プライバシー法その他の法令の違反の疑いに対処する際、OAIC は、かかる違反の疑いについて個々に検討し、すべての関連諸事情を考慮する。

⁶ APP コードとは、情報プライバシーについての実務を文書化したものをいう (第 26C 条 (1))。

訴訟が発生した場合、OAIC は、2005 年法務サービス指令 (Legal Services Directions) に従って模範となる訴訟当事者として行動するという義務に従う。

イ 情報コミッショナーの権限

プライバシー法は、情報コミッショナーに対し調査及び執行権限を含む一連の規制権限を付与しており、それらは、エスカレーション・モデルに基づいている。プライバシーに関する法的義務及びベスト・プラクティスによるプライバシー実務の遵守を促進するために、OAIC は事業者と協働することを認められており、そのプライバシー規制権限は以下を含む。

- ・ APP コード若しくは CR コードを策定し、登録すべきコードについて情報コミッショナーに申請するよう又は情報コミッショナーにコードを策定し、この登録申請をするよう、事業者、事業者のグループ、機関又は団体に要請する権限 (第 26E 条 (2)、第 26G 条、第 26P 条 (1) 及び第 26R 条)
- ・ 情報コミッショナーにプライバシー・インパクト・アセスメント (第 33D 条) を与えるよう、(組織ではなく) 機関に指示する権限
- ・ 事業者が法律により義務付けられるところにより個人情報を維持し、取り扱っているかの監視又はアセスメントを実施する権限 (第 28A 条及び第 33C 条)

プライバシーへの干渉の疑いを調査し、又はそれ以外に対処するにあたって用いることのできるプライバシー規制権限は、プライバシー法パート V に定められており、かかる権限には以下を行う権限が含まれる。

- ・ 申立て (第 40 条 (1)) 又は情報コミッショナー自身のイニシアティブ (すなわち、CII。) (第 40 条 (2)) に従い、事案を調査すること。
- ・ 申立ての調停を試みること (第 40A 条)。
- ・ 申立ての調査又は再調査を拒否すること (第 41 条)。
- ・ 調査を開始するか否かの予備調査を行うこと (第 42 条)。
- ・ (申立てについては) 申立人若しくは被申立人又は (CII については) 被申立人の要請に応じて、ヒアリングを行うか否かを決定すること (第 43A 条)。
- ・ 情報若しくは書類を提示し、又は情報コミッショナーの面前に出頭し、誓約の上質問に回答するよう要求すること (第 44 条及び第 45 条)。
- ・ 申立人、被申立人その他関連する者に情報コミッショナーが進行する申立てに関連する会議に出席するよう指示すること (指示に従わないことは犯罪とみなされる。) (第 46 条)。
- ・ 申立てを第 50 条に定める代替紛争解決機関に付託すること。

比較的軽度なものからより重大な規制措置にまで及ぶ執行権限には、以下を行う権限が含まれる。

- ・ 実行可能な約束を容認すること（第 33E 条）。
- ・ 実行可能な約束を執行するための手続きをとること（第 33F 条）。
- ・ 決定を行うこと（第 52 条）。
- ・ 決定を執行するための手続きをとること（第 55A 条及び第 62 条）。
- ・ CII、監視行為又は評価に続いて、一定の場合において、大臣に報告すること（第 30 条及び第 32 条）
- ・ 調査前、調査中若しくは調査後を含め差し止め命令又は別の規制権限の行使を求めること（第 98 条）
- ・ 民事罰規定の違反について、民事罰命令を裁判所に求めること（第 80W 条）。

特定の事案に対処するために行使するプライバシー規制権限の組合せについては、OAIC の裁量による。

ウ プライバシー規制権限を利用したアプローチ

OAIC の望ましい規制上のアプローチは、法律及びベスト・プラクティスの遵守を促進するため、事業者と協働することである。これは、プライバシー法の目的を追求するより効率的かつ効果的な方法と考えられている。OAIC は、このアプローチの一環として一連の措置を講ずることができ、そのうちのいくつかについてのみ規制権限の行使が関与する。

講じられ得る一連の措置には以下が含まれる。

- ・ ガイダンスを提供し、ベスト・プラクティスの遵守を促進し、プライバシーに関する懸念を発生した時点で特定し、対処を試みる。例えば、事業者に対するポリシーガイダンスの提供、事業者に対する関連 OAIC リソースの提供、OAIC と特定の事業者との間の開かれた対話の実施、及びプライバシー義務を遵守していない可能性があるとの OAIC の懸念を当該事業者に通知し、かかる懸念に対処する機会を当該事業者に与えることが含まれる。
- ・ 任意にかつ積極的に OAIC にデータ漏えい事故を通知する規制対象事業者に対応すること。例えば、事故の抑制及び対処について事業者に情報を提供することを含む。
- ・ 適用されるプライバシー法に基づく義務（APP 等）に従って個人情報維持、取り扱われているか否かの評価の実施（第 33C 条）。評価により、OAIC がプライバシーリスク及び不遵守箇所を特定し、事業者がどのようにプライバシーリスクを軽減し、不遵守箇所に対処することができるかを勧告に含めることができる。
- ・ 事業者が個人に関する個人情報の取扱いを伴う新しい活動若しくは機能に従事することを申し出た場合や、情報取扱実務への変更を申し出た場合に、事業者にプライバシー・インパクト・アセスメント（Privacy Impact Assessment, PIA）を行うよう勧告す

ること。PIA とは、ある活動又は機能に関する体系的な書面によるアセスメントで、当該活動又は機能が個人のプライバシーに対し与え得る影響を特定し、かかる影響を管理し、最小限に抑え又は取り除くための勧告を定めるものである。

- ・ 事業者が個人情報の取扱いを伴う活動に従事する場合で、OAIIC がかかる活動又は機能が個人のプライバシーに対し多大な影響を及ぼす可能性があると考える場合に、PIA を実施するよう機関に対し正式に指示すること（第 33D 条）。

事業者が OAIIC と協力的に協働したという事実は、規制措置を取るか否か及びどの規制措置を取るかの決定において考慮される。

エ 調査及びプライバシーの侵害の疑い

OAIIC は、申立てを受領した場合又は CII として、疑いのある又は申し立てられたプライバシーの侵害について調査を開始することができる。

OAIIC は、一定の条件が満たされ（第 36 条及び第 40 条）、第 41 条に基づき申立てが拒否されず又は第 50 条に従い代替紛争解決機関に付託されない場合は、個人又は集団のプライバシーの侵害であると疑われる行為又は慣行について、プライバシー法に基づきなされた申立てを調査することを義務付けられる。

申立ての調査に際し、OAIIC は、申立ての調停を合理的に試みなければならない（第 40A 条）。ほとんどの申立ては、このようにして解決される。合理的な調停の見込みがない場合は、OAIIC は申立ての調査又は再調査を拒否することができる（第 40A 条（4））。

コミッショナーは、自発的に個人のプライバシーの侵害又はオーストラリア・プライバシー原則第 1 項の違反である可能性のある行為又は実行を調査する決定をすることができる（第 40 条（2））。コミッショナーは、申立て若しくはデータ漏えい事件の通知後に CII を開始することを決定し、又は申立て若しくは通知とは関係なく CII を開始することができる。

CII を開始するか否かを決定するに際して、OAIIC は事業者がデータ漏えい事件を自発的かつ速やかに OAIIC に通知したか、違反に対処すべく適切な措置を取ったか、また当該違反の是正において OAIIC に協力したか否かを検討する。

申立ての調査又は CII の実施に際し、OAIIC は関連当事者と協働するよう努める。情報コミッショナーは、必要な場合、個人又は事業者に対し情報及び書類の提供を求めるなど、プライバシー法により付与された正式な権限を行使することができる（第 44 条）。

申立て調査又は CII を受けて、情報コミッショナーは事業者に対し執行措置を取るかを決定する。利用可能な執行権限は、段階的に、それほど深刻でないものからより重大な選択肢にまでわたる。

オ 適切なプライバシー規制措置の選択

プライバシー侵害の疑い又はその他のプライバシーに関する懸念は、以下を含むさまざまな手段を通して OIAC の知るところとなる可能性がある。

- ・ 個人による申立て又は代表による申立て
- ・ データ漏えい通知
- ・ 権利保有者との協働
- ・ 別の規制機関又は外部紛争解決スキームからの照会
- ・ メディア及びソーシャルメディア
- ・ 情報提供者からの情報
- ・ 法執行機関からの情報
- ・ OIAC によるアセスメント又は調査

上述の通り、OIAC は一定の条件が満たされた場合、申立てを調査する義務を負うが、他のプライバシー規制措置（CII の開始を含む。）を取るよう指図することができる。

まずは事業者と協働するアプローチが望ましいことを認識したうえで、OIAC はその裁量で、プライバシー規制措置の根拠となる事項を選択し、ターゲットとする。これには、個人情報保護を促進、確保するという目標に対しある事項が及ぼすリスクと措置を取ることにより提示される機会の双方を考慮することが含まれる。例えば、より多くの人々の個人情報に関与する場合、リスクが大きくなることを見込まれるが、その一方で違反の疑いが業界内に蔓延していることが疑われる場合は機会が最大となり、OIAC は規制措置を通して当該業界に対してメッセージを送る。

カ 考慮される要因

規制措置を取るか否かについて裁量がある場合、OIAC は、プライバシー規制措置のための事項を優先し、その状況において最も適切な権限を選択しなければならない。プライバシー規制措置を取る時期、またどのような措置を取るかの決定に際し、OIAC が考慮する要因には以下のことが含まれる。

- ・ プライバシー法の目的（第 2A 条）
- ・ 事件の深刻度又は以下を含む調査対象となる行為（又は提案を行った場合の潜在的な影響）
 - ・ 潜在的に影響を受ける者の人数
 - ・ センシティブ情報その他の機密性の高い情報が関与する事項
 - ・ 事件又は行為により発生する一人又は複数の個人に対して引き起こされた又は引き起こされる可能性のある有害な影響
 - ・ 不利な又は弱者のグループが特に悪影響を受け又はターゲットとなった可能性があるか否か

- ・ その行為が意図的であったか否か
- ・ その行為について責任を負う一人又は複数の者の職位又は経験値
- ・ 行為、提案又は活動に関連する公共の利益又は懸念のレベル（重大な公共の利益又は懸念が存在する場合は、規制措置が取られる可能性が高くなる。）
- ・ 規制措置から発生し得る事業者に対する負荷が個人情報の保護に対して及ぼされたりリスクによって正当化できるものであるか否か
- ・ 特定のプライバシー規制措置の教育的、抑止的又は優先的な価値（訴訟を起こすことが法律を検証又は明確化するか否かといったことを含む。）
- ・ 事件又は行為に対して責任を負う事業者が OAIC による過去のコンプライアンス又は規制上の執行措置の対象であったか否か、及び当該措置の結果
- ・ 事業者が将来、プライバシー法その他コミッショナーに対しプライバシーに関する機能を付与する法令に違反する蓋然性の有無と程度
- ・ 行為が単独の事由であるか否か、又はかかる事由が（該当事業者内又は業界内における）潜在的なシステム上の問題若しくは継続的なコンプライアンス若しくは執行問題を提起する可能性のある問題を示すか否か
- ・ 行為の結果を是正し、対処するために事業者が取った措置について、事業者が違反又はデータ漏えいを隠匿しようとしたか否か、並びに事業者が違反の抑制及び調査において OAIC に協力したか否か
- ・ 行為が発生してからの時間
- ・ OAIC が執行措置を通して適切な是正を達成するためにかかる費用及び時間
- ・ 蓋然性のバランスに照らして、違反を証明するために利用可能又は法廷で採用可能な十分な証拠があるか否か
- ・ 新たな個人情報取扱い活動若しくは機能又は既存の個人情報取扱い活動若しくは機能への変更が計画されており、又は新たな個人情報取扱い実務が最近導入され、又は既存の実務が変更したこと。
- ・ その状況において OAIC が関連するとみなすその他の要因（行使される特定の規制権限に関連する要因を含む。）

OAIC はまた、覚書に基づき特設資金が提供されている場合は、事業者の評価を行うことができる。OAIC は、さまざまな政府機関との間の覚書の当事者となっている。覚書は、OAIC のウェブサイトで公開されている。アセスメントに対する資金提供の詳細は、事務局の年次報告書に記載されている。

キ 情報源

OAIC は、特定の事案において、いつプライバシー規制措置を取るか、またどの措置を取るかを決定するに際し、上記に概略したアプローチ及び要因を用いる。ただし、OAIC は、

プライバシー規制措置のターゲットとなり得るシステム上の問題及び深刻度の問題の双方を特定するよう努める。OAIIC は、この目的のために以下を含むさまざまな情報源を用いる。

- ・ 個々の申立て及びデータ漏えい通知
- ・ 申立て及びデータ漏えい通知の傾向
- ・ 国際的な動向
- ・ メディアの報告
- ・ 情報提供者
- ・ 調査
- ・ プライバシー・アセスメント
- ・ コミッショナー開始調査
- ・ 信用報告機関年次報告書
- ・ 広く認められた外部紛争解決スキームからの情報(OAIIC に提供される年次報告を含む。)
- ・ APP コード管理機関からの報告

情報は、プライバシー規制措置の根拠となる、政府若しくは業界内の特定の部門又は反復的な行為若しくは慣行を特定するためにも用いられる。これらの部門又は行為若しくは慣行は、OAIIC が個人情報の保護及び取扱いに対し相当な影響を持たせるために必要であるとプライバシー規制措置が考える分野である。例えば、その申立ての統計により、相当数の申立が特定の業界に関連するものであることが証明された場合、当該業界をプライバシー規制措置が必要な業界として特定することができる。上記リストの優先要因を用いることに加えて、OAIIC は、特定の部門に該当する又は特定の行為若しくは慣行を伴う事項を優先して扱う。部門又は行為若しくは慣行が特定された場合は随時、OAIIC のウェブサイトに記載される。

ク 他の申立て及び規制機関との協働

プライバシー法第 35A 条に基づき、情報コミッショナーは、特定のプライバシー関連の申立ての取扱いを外部紛争解決 (External Dispute Resolution, EDR) スキームに委ねることができる。EDR スキームは、三段階の申立てプロセスの第二段階である。

- ・ 個人はまず、被申立人事業者に対し書面で申立てを行い、当該事業者に対応するための合理的な時間を与える。
- ・ 対応又は結果に不服である場合、個人は自己が会員となっている広く認められた EDR スキーム (もしあれば) に対し申立てを行うことができる。
- ・ EDR プロセスの結果に不服である場合、個人は OAIIC に対し申し立てることができる。OAIIC は、申立てを受理するか又はプライバシー法第 41 条に基づき調査を拒否するか否かを検討する。

通常、申立人が、被申立人が会員となっている広く認められた EDR スキームにまず申立

てを行っていない場合、OAIC が申立てを受理する前に、EDR スキームに申立てを行うよう助言される。そうでない場合、OAIC は通常、広く認められた EDR スキームに正式に付託する（第 50 条）よりもむしろ、広く認められた EDR スキームによって取り扱われている又は取り扱いが可能な申立てを拒否する権限を行使する（第 41 条（dc）及び（dd））。

通常 OAIC は、安定的かつ効率的な規制上の成果を得ることを目的として、広く認められた EDR スキームと協働するよう努める。OAIC は、OAIC と当該スキームとの間で情報及び経験が共有され、また申立てに関する情報を送信するための明確な手続きが確立されるよう、開かれたコミュニケーションの慣習を取り入れるよう努める。

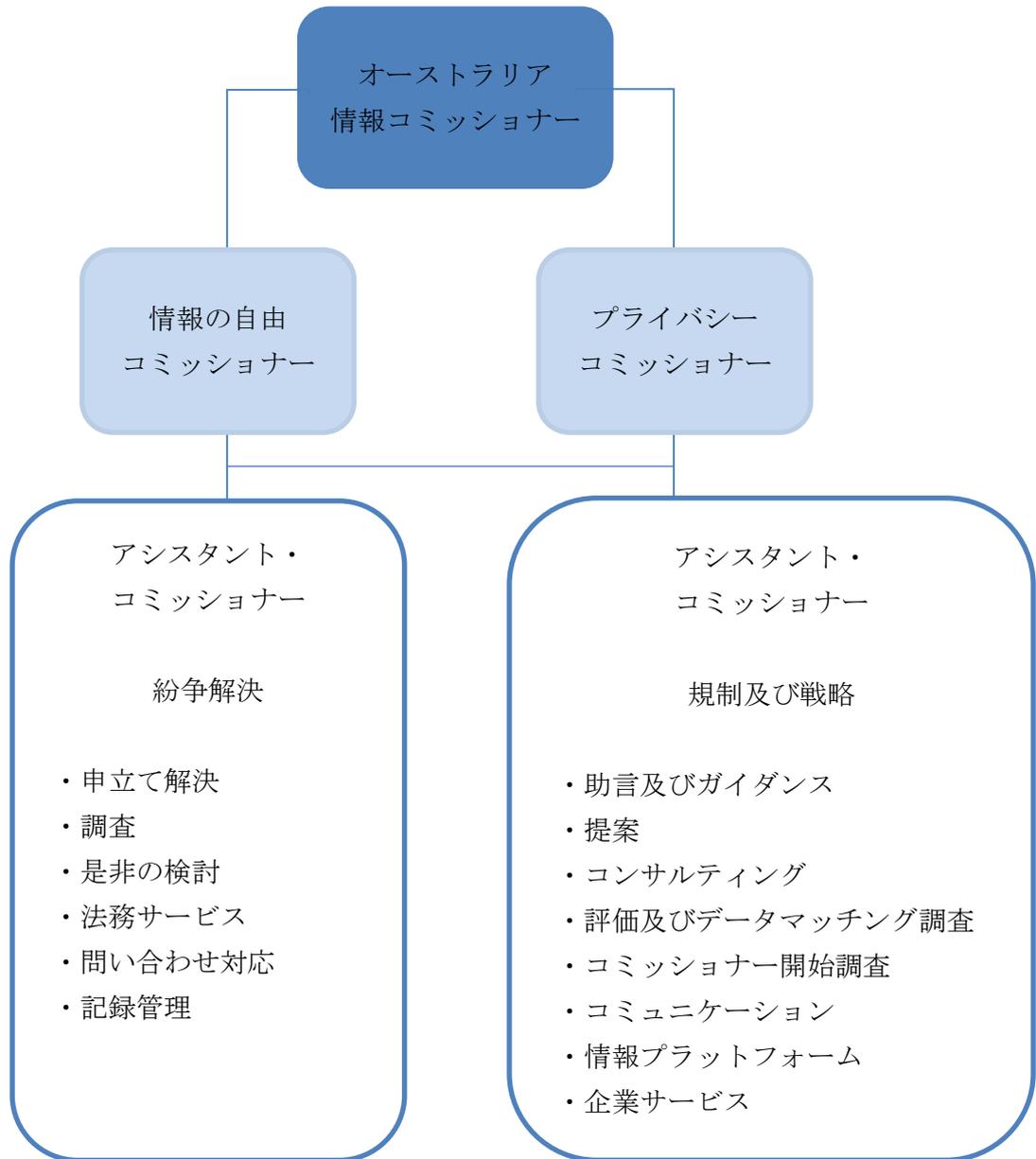
ケ 国内規制機関と代替紛争解決機関との協働

ある事項が OAIC と別のオーストラリアの規制機関の双方の管轄下（州及びテリトリーのプライバシー規制当局、他の部門における規制機関並びに法執行機関を含む。）に該当する場合がある。

OAIC は、その実務的及びリソース上の利点を認識した上で、他の規制機関と協働する。これは、連携のための書面のプロトコル若しくは原則への署名、プライバシーに関する定期的な連絡、情報及び経験の共有、並びに OAIC とその他の規制機関の規制プロセスの調整を含む。ただし、OAIC は常に、自己の法的な枠組み内（情報共有が可能な限度を含む。）で独立して機能する。

OAIC が申立てを受理した場合、OAIC が必ずしも常に当該申立てを調査、解決するのに最適な機関であるとは限らない。OAIC は、代替的な適用法令又は紛争取扱い機関が存在する場合には調査を拒否し、又は一定の状況において申立てを他の紛争解決機関に付託するさまざまな権限を有する。通常、拒否する権限が正式に事案を付託することに優先して行使される。さらに、拒否権限が適用されない場合に、OAIC は、事案を正式に付託する前に、代替紛争解決機関に対し申立てを行い又は申請することを申立人に提案することができる。

コ 組織構造⁷



⁷ Australian Government Office of the Australian Information Commissioner, Chapter Two — Organisation overview, Chart 2.1 Organisation structure as at 30 June 2015 (<https://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201415/chapter-two-organisation-overview#organisation-structure>) アクセス日：2018年2月13日

② オーストラリア通信メディア庁 (ACMA)

www.acma.gov.au/

Phone: 1300 850 115

Email: info@acma.gov.au.

ア 概要

オーストラリア通信メディア庁 (Australian Communications and Media Authority, ACMA) は、放送、インターネット、無線通信及び電気通信の規制について責任を負う機関である。ACMA は、オーストラリア放送当局とオーストラリア通信当局の統合により 2005 年 6 月 1 日に設立された、集中型通信規制機関の一つである。ACMA は、主に 4 つの法律に基づく責任を負う。1992 年放送サービス法 (Broadcasting Services Act 1992)、1997 年電気通信法 (Telecommunications Act 1997)、1999 年電気通信 (消費者保護及びサービス基準) 法 (Telecommunications (Consumer Protection and Service Standards) Act 1999) 及び 1992 年無線通信法 (Radiocommunications Act 1992) である。この他、同当局がスパム、ドット・ノット・コール・レジスター及び双方向ギャンブリング等の分野において対応する 22 の法律がある。ACMA はまた、無線通信、スパム及び電気通信規制並びに無料放送局のためのライセンス・エリア・プランを含む 523 以上の法的効力を伴う文書を作成し、実施している。

ACMA は、議長、副議長及び 2 名の非常勤の構成員から構成される通信及びメディアを監督する独立機関である。ACMA は、議長 (同機関のチーフ・エグゼクティブ・オフィサーを兼務する。)、副議長、4 名のゼネラル・マネージャー及び 9 名のエグゼクティブ・マネージャーからなるエグゼクティブチームにより管理されている。組織構造は、4 つの部門 (通信インフラ、コンテンツ・消費者及び市民、企業及び調査並びに法的サービス) から成る。同機関は、445 名の従業員が所属し、2015 年の予算は年間約 1 億 800 万ドルであった。

ゼネラル・マネージャーは、以下の 4 つの広範な分野について責任を負うが、これらの分野はさらに、特定の事務機能を有する部門やセクションに細分化される。

- ・ 通信インフラ
- ・ コンテンツ、消費者及び市民
- ・ 企業及び調査
- ・ 法的サービス

ACMA は、スパム法を執行する責任を負い、同法の違反について以下のいずれかの措置を取ることができる。

- ・ 正式な警告
- ・ 個人又は会社からの実行可能な合意を承諾すること (この合意は通常、同法の特定の要

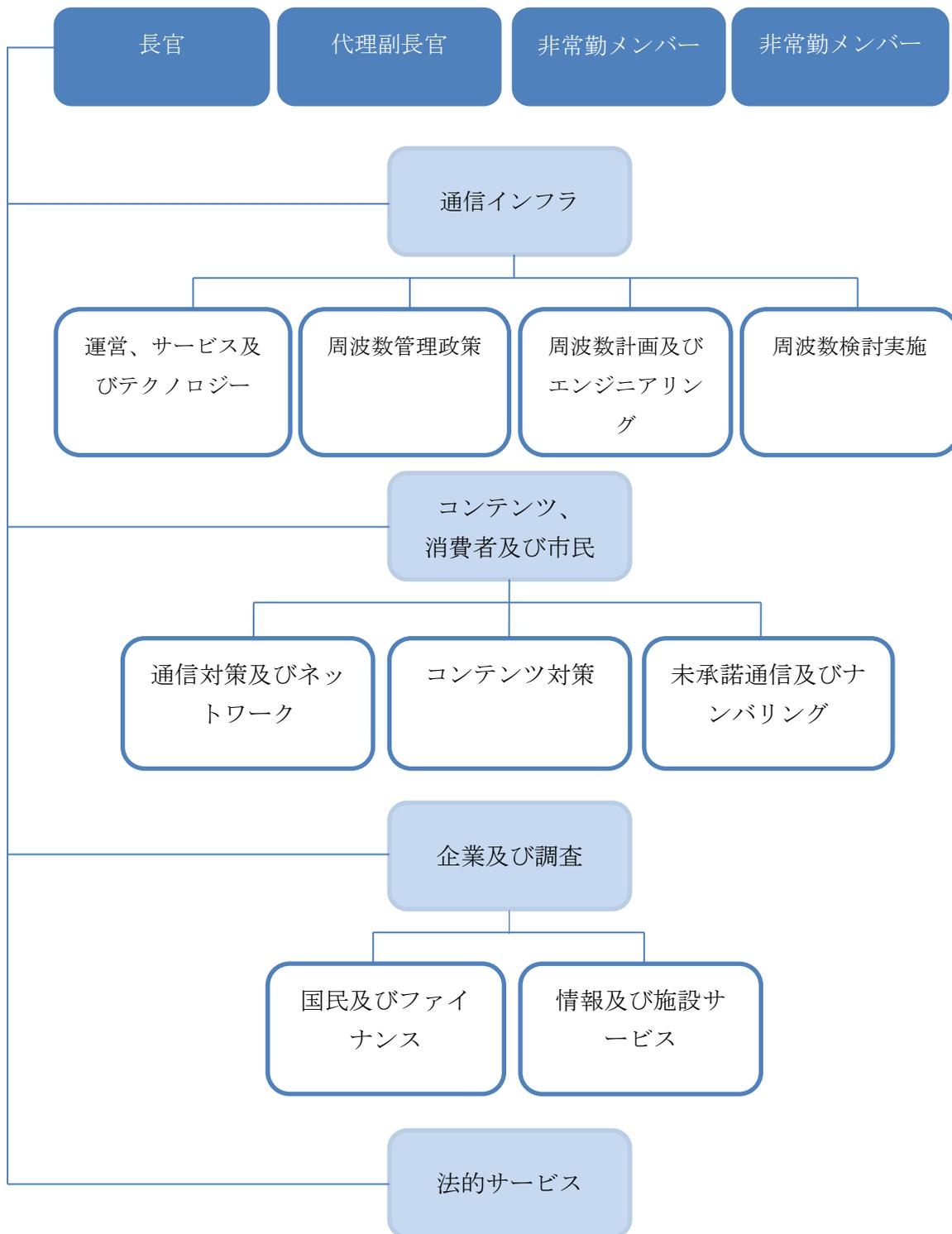
件を遵守する正式な合意を含む。合意に従わない場合、ACMA は連邦裁判所に履行命令を申し立てることができる。)

- 侵害通知の発行
- スパムの送信を止めさせるよう、連邦裁判所に差し止め命令を求めること
- 連邦裁判所に公訴を提起すること

スパム法において言及される罰金の単位は、各 210 ドルである。例えば、スパム法第 25 条 (5) (b) に基づくスパム行為の前歴があり、任意の日において同意なく一通又は複数のスパムメッセージを送りつけた会社に対する罰金は、罰金の最高額を 10,000 単位とする。すなわち、最高 2,100,000 ドルの罰金に相当する。

スパム法は、ACMA に対し、同法違反の場合に敷地内を捜索し、機器を差し押さえ、罰則を課し、これを執行する権限を付与している。同法はまた、スパムから得られた利益の没収及びスパム被害者への賠償金の支払についても定めている。

イ 組織構造⁸



⁸ The Australian Communications and Media Authority (the ACMA), Organisational structure (<https://www.acma.gov.au/theACMA/About/Corporate/Structure-and-contacts/organisational-structure-acma>) アクセス日：2018年2月13日

(4) 最近のトピック

① 制度改正の検討状況、個人情報に関連した政策動向

データ漏えいの強制通告スキームの導入は、情報コミッショナーにとって最重要課題であったことから、データ漏えいの強制通告義務をプライバシー法へ組み込むこととなった。

オーストラリア生産性委員会 (Productivity Commission) は、公的及び民間データの利用可能性と利用を改善するための方法を模索することを目的とした、データの利用可能性と利用に関する 12 か月にわたる公聴会を完了した⁹。

② 個人情報に関連した主要な裁判例

ア プライバシー・コミッショナー対 Telstra Corporation Limited[2017] FCAFC 4¹⁰

2017年1月19日、オーストラリア連邦裁判所大法廷は、情報プライバシー・コミッショナー対 Telstra Corporation Limited [2017] FCAFC 4 において決定を下した。本件は、1998年プライバシー法に基づく「個人情報 (Personal information)」の意味を検討した最初の重大な司法判断であり、個人を特定する一切の情報が必然的に当該個人に関する情報であると一般的見解とは距離をおいたものである。

イ ドードー事件

ドードー事件において、ACMA は、オーストラリアのドゥ・ノット・コール・レジスターに加入する個人に対し、執拗な電話勧誘を行ったとして、オーストラリアを拠点とする電気通信プロバイダーである、Dodo Australia Pty Ltd に 147,000 ドルの罰金を課した¹¹。

⁹ 報告書は下記 URL で閲覧可能である。Australian Government Productivity Commission, Data Availability and Use (<https://www.pc.gov.au/inquiries/completed/data-access/report>)
アクセス日：2018年2月13日

¹⁰ FEDERAL COURT OF AUSTRALIA, Digital Law Library
(http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/full/2017/2017fcaf_c0004) アクセス日：2018年2月13日

¹¹ 下記は、2010年11月1日以降、第52条に基づきなされたプライバシーに関する決定（調停により事案が解決されていない場合又はコミッショナー開始調査に関連するプライバシー侵害の申立てに関する決定。）の詳細の概要を示す表へのリンクである。Australian Government Office of the Australian Information Commissioner, Determinations (<https://www.oaic.gov.au/privacy-law/determinations/>) アクセス日：2月13日

4. ニュージーランド

(1) 制度概要

① 法体系の概要

ニュージーランドでは、1993年プライバシー法 (Privacy Act¹) (以下「プライバシー法」という。) が個人情報の取扱いについて規定している。プライバシー法には、12の情報プライバシー原則 (Information Privacy Principles) が含まれる。この原則は、各事業者等が収集、使用、保有、保管、開示その他の形式で取り扱う一切の個人情報に関して各事業者等が遵守すべき原則を定めたものである。

プライバシー法は、すべてのエージェンシー (agencies) (以下「事業者等」という。) に適用される。同法の定義によれば、事業者等とは、一切の個人又は団体を意味し、法人格の有無ないし公的部門か民間部門かを問わない。

プライバシー法は、12の情報プライバシー原則により、ニュージーランドにおける事業者等によるすべての個人情報の収集、使用及び開示について規制している。プライバシー法は、法人格の有無ないし民間部門か公的部門 (政府機関を含む。) かを問わず、すべての事業者等に適用される。

プライバシー法及び同法を構成する情報プライバシー原則の他、情報プライバシー原則の適用基準、適用除外類型、又は遵守方法を定めるものとして、実務規則 (Code of Practice) が定められる場合があり、これにより情報プライバシー原則の柔軟な適用が可能とされている。

当該実務規則は、コミッショナーによる随時の改正又は廃止が可能であるが、プライバシー法等と同様、規制とみなされることから、改正等にあたっては、改正案等の代議院 (House of Representative。ニュージーランドの立法府) への提出と、委員会 (Regulations Review Committee) の審査を要する。

上記の他、公的部門における情報の取扱いに関しては、1982年行政情報に関する法 (the Official Information Act 1982²) 及び1987年地方自治体行政情報会議法 (the Local Government Official Information and Meetings Act 1987³)、プライバシー法とは別途、定めを置いている。

¹ <http://www.legislation.govt.nz/act/public/1993/0028/latest/whole.html>

² <http://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html>

³ <http://www.legislation.govt.nz/act/public/1987/0174/latest/DLM122242.html>

また、電子メッセージの送信に関しては 2007 年未承諾電子メッセージ法 (Unsolicited Electronic Messages Act 2007⁴) が、有害な内容の通信に関しては 2015 年有害デジタル通信法 (Harmful Digital Communications Act 2015⁵) がそれぞれ規制を定めている。

② 民間部門に適用される主な法律

- ・ プライバシー法
プライバシー法は、公的部門及び民間部門のすべての事業者等に適用される。
- ・ 2007 年未承諾電子メッセージ法
電子メッセージの送信に関する規制を定める法律。
- ・ 2015 年有害デジタル通信法
有害な内容の通信を規制する法律。

③ 公的部門に適用される主な法律

プライバシー法は、公的部門及び民間部門のすべての事業者等に適用される。もともと、一部の規定は、公的部門の事業者等のみに関連する規定である。当該規定には、公的部門の事業者等との間の情報共有契約及び情報マッチングプログラム (information matching programmes) に関する規定が含まれる。

また、公的部門における情報の取扱いに関しては、1982 年行政情報に関する法 (the Official Information Act) 及び 1987 年地方自治体行政情報会議法 (the Local Government Official Information and Meetings Act)、プライバシー法とは別途、定めを置いている。

(2) 主な連邦法の概要

① プライバシー法

ア 法律の概要

プライバシー法は、1993 年 7 月 1 日付で施行された。

4

http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html?search=qs_act%40bill%40regulation%40deemedreg_SPAM+Act_resel_25_h&p=1&sr=1

⁵ <http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html>

同法は、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 理事会勧告に従い、個人のプライバシーの促進及び保護全般を目的とする。具体的には、以下の目的が挙げられる。

- (a) 次に掲げるものに関する一定の原則を定めること。
 - (i) 公的部門及び民間部門の事業者等による個人に関する情報の収集、使用及び開示
 - (ii) 公的部門及び民間部門の事業者等が保有する個人情報に対する個人によるアクセス
- (b) 個人のプライバシーの侵害に係る苦情等の請求を調査するコミッショナーの任命に関する規定を定めること。
- (c) 上記に付随する事項に関する規定を定めること。

イ 個人情報の定義

プライバシー法において、個人情報は、「特定可能な個人に関する情報をいい、1995 年出生、死亡、婚姻及び関係登録法 (the Births, Deaths, Marriages, and Relationships Registration Act 1995) 又はそれ以前の法律 (1995 年出生、死亡、婚姻及び関係登録法において定義されるものをいう。) に基づき戸籍当局の長官が維持する死亡に関する情報も含む。」と定義されている。

センシティブ情報 (sensitive information。機微情報) は、プライバシー法上定義された用語ではない。この点は、プライバシー法以外のニュージーランドの個人情報保護法制においても同様である。

同法上、健康に関する個人情報の定義が置かれている。すなわち、プライバシー法において、「健康情報」 (health information) は、1956 年保健法 (Health Act) 第 22 条 B において定義された意味を有し、特定可能な個人に関しては以下の情報を意味するものとされる。

- (a) 当該個人の健康に関する情報 (当該個人の診療履歴を含む。)
- (b) 当該個人が現在有する又は過去に有した障害に関する情報
- (c) 当該個人に現在提供されている、又は過去に提供された、健康関連のサービスに関する情報
- (d) 当該個人の身体の一部又は身体組織の提供に関連して当該個人が提供した情報
- (e) 上記規定に拘らず、第 22 条 E においては、以下の情報をいう。
 - (i) 個人が提供した身体の一部又は身体組織の試験又は検査により得られた情報
 - (ii) その他提供された身体の一部若しくは組織に関連する情報、又は提供者に関連する当該提供に関する情報

ウ 主な規制・権利の内容

プライバシー法の運用を担う当局として、プライバシー法上、プライバシー・コミッショナー (Privacy Commissioner) (以下「コミッショナー」という。) が任命される。同法は、各事業者等において、1 名以上の Privacy Officer (以下「プライバシーオフィサー」という。) を設置することを義務付けており、プライバシーオフィサーは、同法の遵守、同法に基づき事業者等に対して行われた要請・指導等への対応、及び同法に基づく調査に関してコミッショナーに協力することを任務とする。

同法の規制は、広範な射程を有する 12 の情報プライバシー原則 (同法第 6 条において規定される) を中心に構成されており、各原則の内容は大要以下の通りである。

- 原則 1: 収集の目的—事業者等による個人情報の収集は、事業者等の業務に関連する適法な目的に従い、かつ、当該目的のために必要である場合を除き、行われてはならない。
- 原則 2: 個人情報の情報源—事業者等は、一定の例外に該当する場合 (個人の同意がある場合、情報が一般に公開され入手可能である場合、遵守が実現困難な場合、個人が特定されない形で情報を使用する場合等) を除き、個人情報に係る個人から当該個人情報を収集しなければならない。
- 原則 3: 情報の収集—個人情報が個人情報に係る個人から収集される場合、事業者等は、収集の事実、収集の目的、受領予定者、事業者等の連絡先並びに個人の情報アクセス権及び訂正を求める権利について当該個人が認識できるよう、合理的な措置を講じなければならない。実務上は、事業者等は、個人が自己の個人情報を提供する前に閲覧可能なプライバシーポリシーに上記事項を掲載することにより本原則を遵守したものとみなされるのが一般的である。
- 原則 4: 収集方法—事業者等は、不法又は不正な手段若しくは個人の私生活を不当に侵害する手段により個人情報を収集してはならない。
- 原則 5: 保管及びセキュリティ—個人情報を保有する事業者等は、情報の不正な流出、不正利用、不正アクセス及び不当開示を防止するために合理的な安全管理措置によって情報が保護されるよう確保しなければならない。
- 原則 6: 情報へのアクセス—事業者等が容易に検索可能な個人情報を保有する場合、当該個人情報に係る個人は、(i) 当該情報が保有されているかどうかを事業者等に確認する権利、(ii) 当該情報にアクセスする権利、及び (iii) アクセス権が付与されない場合、個人は原則 7 に基づく権利につき周知される権利を有する。
- 原則 7: 情報の訂正—事業者等が個人情報を保有する場合、当該個人情報に係る個人は、当該個人情報の訂正を求め、又は訂正を求めたが訂正が行われていない旨の文言を当該個人情報に添付するよう求めることができる。
- 原則 8: 情報の正確性—事業者等は、情報の正確性、最新性及び誤解を招くものでな

いことを確保するための合理的な措置を講ずることなく個人情報を使用してはならない。

原則 9: 情報の保有期間—事業者等は、個人情報の適法な使用目的のために必要な期間を超えて個人情報を保有してはならない。

原則 10: 使用制限—ある目的のために個人情報を保有する事業者等は、他の目的のためにこれを使用してはならない。ただし、複数の目的が相互に直接の関連性を有する場合、個人が特定されない形で情報が使用される場合、又は個人が使用を許可した場合等の例外に該当する場合を除く。

原則 11: 開示制限—個人情報を有する事業者等は、第三者にこれを開示してはならない。ただし、開示が情報収集目的に直接関係する場合、情報が一般に入手可能な場合、又は個人が開示を許可した場合等、いずれかの例外に該当すると事業者等が合理的に判断する場合を除く。

原則 12: 一意識別子 (Unique Identifiers) —いずれの事業者等も、その業務を円滑に運営するために必要な場合を除き、個人に対して一意識別子を割り当ててはならない。

上記のプライバシー法及び同法を構成する情報プライバシー原則の他、コミッショナーは事業者等が属する特定の業界に適用される規則 (Code of Practice) (以下「実務規則」という。) を定める場合がある。この場合、情報プライバシー原則の他、事業者等には、当該実務規則が適用される。実務規則においては、情報プライバシー原則の適用基準、適用除外類型、又は遵守方法が定められ、これにより、情報プライバシー原則の柔軟な適用が可能となる。

上記の実務規則は、特定の情報ないし特定の種類の情報や、特定の事業者等、業務、業態、職業等を対象として定められるが、実務規則は、個人が (i) 当該個人に係る個人情報に関する公的部門の事業者等による保有状況の確認、(ii) 公的部門の事業者等が保有する個人情報の照会、又は (iii) 公的部門の事業者等が保有する個人情報の訂正、を求める権利を制限するものであってはならない。

実務規則は、コミッショナーによる随時の改正又は廃止が可能であるが、実務規則は、規制とみなされることから、改正等にあたっては、代議院 (House of Representative。ニュージーランドの立法府) への提出が必要となり、委員会 (Regulations Review Committee) の厳格な審査の対象となる。現在、ニュージーランドでは7つの実務規則 (Justice Sector Unique Identifier Code、Health Information Privacy Code 1994、Credit Reporting Privacy Code、Superannuation Schemes Unique Identifier Code、Telecommunications Information Privacy Code、Expired and Revoked Codes of Practice、Civil Defence National Emergencies (Information Sharing) Code 2013)⁶が実施されており、医療情報、通信情報、信用情報、

⁶ <https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/>

退職年金（superannuation）、司法部門及び民間防衛に関する情報等が対象となっている。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

現在、プライバシー法上、違反に関する監督当局への報告義務は規定されていない。しかし、コミッショナーが公表するプライバシー違反ガイドライン（Privacy Breach Guidelines）により、違反の際にコミッショナー及び被害者たる個人に対する報告が推奨されており、また、当該報告の時期及び方法等が定められている。

現在、同法上、違反の際の報告は任意であるが、この取扱いは近い将来変更される可能性がある。ニュージーランド法委員会（New Zealand Law Commission）及びコミッショナーの双方は、ニュージーランド政府に対して、報告制度を義務的なものとするよう勧告した⁷。この勧告は、前政権によって概ね承認されており、勧告に係る報告制度は二段階の構成からなる。すなわち、(i) 事業者等は、重大な違反につきコミッショナーに対する通知義務を負い、(ii) さらに重大な違反（個人が損害を被る切迫した危険性がある場合）については、コミッショナー及び被害者たる個人に対する通知義務を負う。もっとも、2017年10月の政権交代により、新たな報告制度の実施時期の見通しは立っていない。

オ 安全管理措置

情報プライバシー原則第5は、個人情報保有する事業者等が遵守すべき義務として以下の内容を明記している。

- (a) 個人情報の漏えい、事業者等の承諾なく行われる個人情報へのアクセス、使用、変更又は開示その他個人情報の不正な利用を防止するために、合理的な安全管理措置を講ずること。
- (b) 事業者等のサービス提供に関連して個人に情報が提供される場合、当該情報の不正な使用又は開示を防止するため、当該事業者等が採り得る一切の措置を講ずること。

プライバシー法は、データ保護に関して原則ベースによる規制を想定しており、個人情報の安全管理措置について、技術面での基準等、具体的な履行方法は規定されていない。そのため、情報プライバシー原則第5の遵守のために採るべき措置の内容は、事業者等の業務内容や具体的状況により異なることになる。一般的には、事業者等がその属する業界の最善の実務慣行に従っており、当該実務慣行が国際標準やセキュリティに関する最新の实務慣行に準拠している場合は、安全管理措置の不履行とみなされるおそれは低いと考えられる。

7

<https://privacy.org.nz/the-privacy-act-and-codes/privacy-law-reform/new-zealand-law-commission-privacy-review/>

カ 適用範囲

プライバシー法は、個人情報保有する一切の公的部門及び民間部門の事業体に適用される。

事業者等が、自身による使用又は開示を目的とせず、第三者のために保管又は処理することのみを目的として、個人情報を当該第三者の代行者として保有する場合は、個人情報は当該第三者により保有されるものとみなされる（プライバシー法第3条（4））。これにより、個人情報の物理的な所在ないし物理的な保管・管理の主体に拘らず、第三者に処理又は保管を行わせることのみを目的として個人情報を第三者に移転した事業者等は、当該個人情報に関して従前通りプライバシー法上の義務を負うことになる。

ニュージーランド国内で業務を行う全ての事業者等は、本店等の所在地に拘らず、プライバシー法の適用を受ける。プライバシー法の適用関係において、ニュージーランド国内で業務を行う外国事業者等も、ニュージーランドに本店等を置く事業者等と同様の義務を負うことになる。

キ 小規模事業者の取扱い

ニュージーランドのプライバシー法においては、小規模事業者に関する特別の規定は定められていない。

ク 国際的な情報移転に関する規定

プライバシー法上、国際的なデータ移転に関して、コミッショナーへの通知又はコミッショナーからの承諾の義務付け、その他ニュージーランド国外へのデータ流通自体を制約する特段の規制は存在しない。もっとも、事業者等が、ニュージーランド国内の事業所から同一法人内の国外の事業所にデータ移転をした場合、当該国外の事業所において保有される個人情報についても、事業者等は情報プライバシー原則に則って処理する必要がある。

第3条（4）は、海外の第三者に個人情報を移転する場合においても適用される。すなわち、個人情報の物理的な所在ないし物理的な保管・管理の主体に拘らず、第三者に処理又は保管を行わせることのみを目的として個人情報を海外の第三者に移転した事業者等は、当該個人情報に関して従前通り同法上の義務を負うことになる。

上記の他、コミッショナーは、他国からニュージーランドに移転し、又は移転される予定の個人情報が、同法と類似又は同様の保護を定める法令が適用されない第三国へ移転される可能性があり、これにより、OECDの「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」（OECD プライバシーガイドライン）のパート2に定める国内適用の基

本原則に違反するおそれがあると合理的に認める場合、同法パート 11 に基づき、ニュージーランドから当該第三国への個人情報の移転を禁止することができる（法 114B (1)）。ただし、当該移転が法令、条約により義務付けられる場合又は法令により許容される場合はこの限りでない（法 114B (3)）。移転の禁止の決定にあたっては、コミッショナーは、法 114B (1) に定める要件の他、(a) 当該移転の個人に与える影響、(b) ニュージーランドと他国との間の自由な情報流通の促進の必要性、(c) 国際的なデータ移転に関する国際標準（OECD ガイドライン、個人データ処理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 EU 指令 95/46/EC を含むが、これらに限られない。）についても考慮する必要がある（法 114B (2)）。

ケ 紛争処理手続

- ・ 申立て

個人のプライバシーの侵害又はそのおそれがある場合は、いずれの者もコミッショナーに対して申立てを行うことができる（法第 67 条）。同法上、個人のプライバシーの侵害とは、情報プライバシー原則又は実務規則に違反する行為であって、コミッショナーが (i) 個人に対して損害を与え又は与えるおそれがあり、(ii) 個人の権利又は義務に悪影響を及ぼし又は及ぼすおそれがあり、又は (iii) 当該個人に著しい屈辱、尊厳の喪失又は精神的打撃を生じさせ又は生じさせるおそれがあると判断する行為、と明記されている。

- ・ 調査等

コミッショナーは、個人のプライバシーの侵害又はそのおそれがある行為を調査し、当該行為について仲裁人として行動し、同法に従って追加の措置を講ずることを任務とする（法第 69 条）。コミッショナーは、個人のプライバシーの侵害に関して個人又はコミッショナーが行った申立てについて調査することができ、申立てを受理した場合は、その裁量によりその他の措置を講ずべきか否かを決定することができる。

- ・ 他の機関への付託

コミッショナーは、各機関の所管法令等に照らして、申立てに係る事項がオンブズマン、健康・障害コミッショナー（Health and Disability Commissioner）又は情報保安検査官（Inspector-General of Intelligence and Security）による処理がより適切であるとコミッショナーが判断する場合、当該申立ての処理をこれら他の機関に付託することができる（法第 72 条乃至第 72 条 C）。また、コミッショナーは、申立てにつき、海外のプライバシー保護当局の管轄とするのがより適切である場合、申立ての処理について、海外のプライバシー保護当局への付託又は当該海外のプライバシー保護当局との

協議を行うことができる。

- 手続

コミッショナーは、調査を開始する前に申立人及び調査対象者に対して、調査開始の意向があること、調査の具体的内容及び調査対象者が申立てに対して書面により回答を提出できる権利について通知しなければならない（法第 73 条）。

コミッショナーは、当事者を申立てに係る事項の協議に召喚する権限を有し、当該事項の解決のため当事者間で合意（和解）するよう勧告する権限を有する（法第 76 条）。

コミッショナーは、調査に関連して、適切と判断する限度で、事業者等に対する照会又は事業者等からの聴取若しくは情報収集を行うことができる。事業者等は、実務上合理的な範囲で可及的速やかにコミッショナーの要請に従わなければならない（法第 92 条）。事業者等がコミッショナーの要請に従わなかった場合、コミッショナーはその旨をニュージーランド首相に報告することができる。

プライバシー法に基づき証拠の提供を求められた者は、裁判所における証人と同一の権利を有する（法第 94 条）。コミッショナーに対して陳述又は提供された情報はすべて、裁判手続により照会等がされた場合と同様の方法により、秘密保持の対象となる（法第 96 条）。

- 裁判所（Human Rights Tribunal）の権限

コミッショナーは、当事者間で和解が成立しない場合、又はプライバシー違反の事実について確証を得られない場合、申立てに係る事項を人権手続ディレクター（the Director of Human Rights Proceedings）（以下「ディレクター」という。）に委託することができる。ディレクターは、その裁量により、調査対象者に対して裁判所（the Human Rights Review Tribunal）における民事手続を開始するか否かを決定することができる。

裁判所は、プライバシーの侵害の事実を認定した場合、以下のいずれか又は複数の救済手段を採ることができる（法第 85 条）。

- (i) 被申立人の行為が個人のプライバシーの侵害に該当する旨の宣言
- (ii) 侵害の継続又は反復を禁止する旨の被申立人に対する命令
- (iii) 損害賠償
- (iv) 侵害を是正するための行為を被申立人に行わせる旨の命令
- (v) 裁判所が適切とみなすその他の救済措置の命令

- ② 1982 年行政情報に関する法

- ア 法律の概要

1982年行政情報に関する法（Official Information Act）は、1983年7月1日付で施行された。

1982年行政情報に関する法は、立法府に対して行政府が責任を負う旨の原則に従い、同法が以下の目的を有することを明記している（法第4条）。

- (a) 次に掲げる事項を目的として、ニュージーランド国民に対する行政情報の利用可能性を漸次推進すること。
 - (i) 法令その他諸規則等の策定及び運用に対する国民の実効的な参画を可能とすること
 - (ii) 行政府の長及び職員の説明責任の促進上記により、法令遵守とニュージーランドにおける民意に沿った政治を促進すること。
- (b) 自己の行政情報に対する適切なアクセスを提供すること。
- (c) 公益及び個人のプライバシーの保護との調和を図りつつ、行政情報を保護すること。

イ 主な規制・権利の内容

1982年行政情報に関する法は公的部門における情報の取扱いを定めるものであり、同法により、ニュージーランド国民は、政府が同国民について保有する情報へのアクセス権を付与されている。同法の目的は、行政情報の利用可能性を高め、各人による自己に関する行政情報への適切なアクセスを提供することである。同法は、閲覧又は提供を制限する正当な理由がある場合を除き、閲覧又は提供を可能とするとの原則に基づき運用されている。

「正当な理由」の要件は、同法において定められている。同法の適用を巡る苦情等の請求は、公的部門の事業者等を監視するオンブズマンに対して行う必要がある。閲覧等の要請がなされる行政情報が、要請をする国民の「個人情報」に関連する限り、当該閲覧等の要請は、プライバシー法に従って処理されなければならない。オンブズマンは、1982年行政情報に関する法に基づく最終意見を形成する前に、コミッショナーとの協議が必要となる点が重要である。

③ 1987年地方自治体行政情報会議法

ア 法律の概要

1987年地方自治体行政情報会議法(Local Government Official Information and Meetings Act)は、1988年3月1日付で施行された。

1987年地方自治体行政情報会議法は、以下の目的を有することを明記している(同法第4条)。

- (a) 次に掲げる事項を目的として、地方自治体が保有する行政情報の国民による利用を漸次推進し、地方自治体における公開の審議を促進すること。
 - (i) 地方自治体の活動及び決定に対する住民による実効的な参画を可能とすること
 - (ii) 地方自治体の役職員の説明責任の促進上記により、法令遵守とニュージーランドにおける民意に沿った政治を促進すること。
- (b) 自己の行政情報に対する適切なアクセスを提供すること。
- (c) 公益及び個人のプライバシーとの調和を図りつつ、行政情報の保護及び地方自治体における審議の確保を図ること。

イ 主な規制・権利の内容

1987年地方自治体行政情報会議法は公的部門における情報の取扱いを定めるものであり、同法により、ニュージーランド国民は、政府が同国民について保有する情報へのアクセス権を付与されている。同法の目的は、行政情報の利用可能性を高め、各人による自己に関する行政情報への適切なアクセスを提供することである。同法は、閲覧又は提供を制限する正当な理由がある場合を除き、閲覧又は提供を可能とするとの原則に基づき運用されている。

「正当な理由」の要件は、同法において定められている。同法の適用を巡る苦情等の請求は、公的部門の事業者等を監視するオンブズマンに対して行う必要がある。閲覧等の要請がなされる行政情報が、要請をする国民の「個人情報」に関連する限り、当該閲覧等の要請は、プライバシー法に従って処理されなければならない。オンブズマンは、1987年地方自治体行政情報会議法に基づく最終意見を形成する前に、コミッショナーとの協議が必要となる点が重要である。

④ 2007年未承諾電子メッセージ法

ア 法律の概要

2007年未承諾電子メッセージ法（Unsolicited Electronic Messages Act 2007）（以下「SPAM法」という。）は、2007年9月1日付で施行された。

SPAM法は、以下の目的を有することを明記している（同法第3条）。

- (a) 次に掲げる事項を目的として、ニュージーランドのリンク（.nzドメイン）を含む未承諾の商業電子メッセージの送信を禁止すること。
 - (i) ニュージーランドにおける情報及び通信技術の利用のためのより安全かつ確実な環境を推進すること
 - (ii) ニュージーランドの企業及び広範な地域社会における情報及び通信技術の受容及び効果的利用に対する障害を削減すること
 - (iii) 未承諾の商業電子メッセージに起因して企業及び広範な地域社会が負担するコストを削減すること
- (b) 商業電子メッセージにおいて、メッセージの送信を許可した者に関する正確な情報の記載及び受信者が今後自己に対してメッセージを送信しないよう送信者に指示するための受信拒否設定機能の記載を義務づけること。
- (c) 同法に違反して、未承諾の電子メッセージの送信に関連してアドレス収集ソフトウェア又は収集されたアドレスのリストを使用することを防止すること
- (d) 国民による情報及び通信技術の不適切な利用を抑止すること

イ 主な規制・権利の内容

SPAM法は、ニュージーランドにおける情報及び通信技術の使用に関して、より安全かつ確実な環境を促進し、国民による情報や通信技術の不適切な利用を抑止することを目的として、受信者の承諾を得ない電子メッセージの送信を禁止している。

具体的には、SPAM法上、受信者が受信に同意していない商業的電子メッセージを送信すること及び第三者に送信させることが禁止される。受信者の同意は、(i) 明示的になされる場合、(ii) 受信者の行為、業務等から同意が合理的に推測される場合、又は (iii) 電子メールアドレスが公表されており、公表にあたって、アドレス保有者は未承諾電子メッセージの受信を希望しない旨の記載がなく、かつ、当該メッセージがアドレス保有者の業務等に関連する場合、のいずれかに該当する同意でなければならない。

SPAM法上、商業電子メッセージには、(i) メッセージの送信を許可した者の氏名及び連絡先が表示され、(ii) 受信者が今後送信者からの電子メッセージの受信を拒否（opt out）するための受信拒否設定が含まれている必要がある。

⑤ 2015 年有害デジタル通信法

ア 法律の概要

2015 年有害デジタル通信法 (Harmful Digital Communications Act 2015) (以下「HDC 法」という。) は、2015 年 7 月 2 日付で施行された。

HDC 法は、以下の目的を有することを明記している (同法第 3 条)。

- (a) デジタル通信によって個人が被る損害を抑止、防止及び軽減すること
- (b) 有害なデジタル通信の被害者に、迅速かつ効果的な是正手段を提供すること。

イ 主な規制・権利の内容

HDC 法の目的は、有害なデジタル通信の抑止にある。有害なデジタル通信には、(i) 脅迫的又は攻撃的な内容の送信又は公表、(ii) 不利益な噂の拡散、(iii) わいせつな写真やビデオ等のセンシティブな個人情報の送信又は公表が含まれる。同法においてデジタル通信は、広範囲な定義とされており、文字、写真、画、録音等、電子メッセージについての全ての形態を含むとされている。デジタル通信の有害性については、当該通信により深刻な精神的苦痛を与えることを意図していたことが要件とされる。この主観的要件についても広範なものが含まれ得るものとされている。

HDC 法は、デジタル通信による加害という新たな類型の刑法犯を定めるものであり、法定刑として、個人については 2 年以下の禁固又は 50,000NZ ドル以下の罰金、法人については 200,000NZ ドル以下の罰金を定めている。個人の場合、他者が送信又は公表した有害なデジタル通信の内容については、HDC 法所定の手続による簡易迅速な削除請求が可能である。HDC 法は、有害なデジタル通信の調査と紛争解決を任務とする苦情処理機関の設置を定めている。明白な違反が存在するにも拘らず苦情処理が困難である場合、当該苦情処理機関は、地方裁判所に紛争解決を付託することができる。

HDC 法は、情報プライバシー原則の特則としての位置付けも有する。すなわち、HDC 法は、法人又は個人によるデータ使用が不正かつ不合理なものであり、かつ、当該データの使用又は開示により第三者に深刻な精神的苦痛を与える場合は、当該法人又は個人が情報プライバシー原則第 10 及び同第 11 の違反について責任を負う場合がある旨明記しており、この限りにおいて、情報プライバシー原則の適用は変更される。

(3) 監督機関・第三者機関

① 設置の経緯

プライバシー・コミッショナー事務局(Office of the Privacy Commissioner⁸) (以下「OPC」という。)は、プライバシー法第12条に基づいて、同法の施行に伴い1993年に設立された独立の政府認可法人(2004年政府認可法人法上の政府認可法人をいう。)(Crown entity)であり、個人情報の収集、利用及び開示に係る規制を所管する。OPCは、同法に定める広範な業務を行うことを任務としており、その一環として、プライバシー違反に関する申立の調査、教育プログラムの実施、法律案の査定及び当該法律案が個人のプライバシーに与え得る影響の査定等がある。コミッショナーは、その業務についての報告を、司法省大臣を通して代議院に対して行う。

OPCの連絡先、幹部構成は以下の通り。

[連絡先]

Wellington: Level 8, 109 - 111 Featherston Street

Auckland: Level 13, 51 - 53 Shortland Street

PO Box 10 094, The Terrace, Wellington 6143

Fax: (04) 474 7595

Email: orders@privacy.org.nz

[幹部構成]

プライバシー・コミッショナー	John Edwards
アシスタント・コミッショナー	Joy Liddicoat
アシスタント・コミッショナー	Blair Stewart
ゼネラル・マネージャー	Gary Bulog
パブリック・アフェアーズ・マネージャー	Annabel Fordham
ゼネラル・カウンセル	Jane Foster

② 制度の概要

2017/2018年OPC趣意書(OPC's Statement of Intent⁹)は、OPCの任務について、プライバシー侵害事案についての処理状況を改善すること、プライバシーに関する法令遵守の促進のためにOPCの権限を最大限に活用すること、その影響力拡充のためのネットワーク

⁸ <https://www.privacy.org.nz/>

⁹

<https://www.privacy.org.nz/news-and-publications/corporate-reports/office-of-the-privacy-commissioner-statement-of-intent-1-july-2017-30-june-2021/>

の構築及び拡大を図ることを定めている。また、OPC は、プライバシーに関する人権の強化のためにプライバシー改革 (Privacy Reform) を推進し、ニュージーランドの法律を情報技術の変化や国際基準の変更に適合させていくことを明記している。

2017/2018 年度において、コミッショナーは、政府予算に基づき 497 万 NZ ドルの配算を受けた。コミッショナーは、プライバシーに関して、ガイダンス/教育、情報共有/情報マッチング、政策及び研究、並びに法令遵守の 4 つの歳出科目を定めることを約束した。

③ 運用実態

コミッショナーによる 2017 年度の年次報告¹⁰によると、2016 年のプライバシー法の運用状況は概ね以下の通りである。

- ・ 5 社につき、プライバシー法への違反事業者等としての公表措置を採った。
- ・ プライバシー侵害事案のうち、和解により解決したものは 48% であった。
- ・ 事業者等からの提案に対する回答 (186 件)、一般からの照会に対する回答 (7, 320 件)、OPC ウェブサイト経由の照会に対する回答 (8, 433 件) を行った。
- ・ プライバシーに関する教育の一環として、OPC によりオンライン・トレーニング・モジュールが提供されており、2, 761 人が同モジュールを受講した。

(4) 最近のトピック

① 制度改正の検討状況

コミッショナーにとっての重要課題の一つは、プライバシー改革 (Privacy Reform) である。コミッショナーは、プライバシー原則に基づいたプライバシー法の適用・運用が、従前通り、概ね同法の目的に則ったものであるとする一方、技術の変化・革新に対応し、かつ、コミッショナーによるプライバシー法の適用・執行の実効性を強化するために改善を要する分野もあり、これにより、情報プライバシーに関する国民の自信と信頼が高まると考えている。2011 年及び 2017 年において、法律委員会 (Law Commission) 及びコミッショナーはそれぞれ、司法省に対して報告書を発表しており、プライバシー法の強化のための一連の改革を行うべきことを勧告している。勧告には以下の内容が含まれている。

- データポータビリティに対する権利
- 個人情報再特定化 (re-identification) に関する統制
- 義務的な違反通知体制

¹⁰

<https://www.privacy.org.nz/news-and-publications/corporate-reports/annual-report-of-the-privacy-commissioner-2017/>

- 申出に関して強制力のある決定を行うためのコミッショナーの権限の新設
- 法令遵守通知（compliance notices）を発行し、事業者等による個人情報の取扱いに関する監査を要請するコミッショナーの権限の新設
- プライバシー法の遵守に関する証明を事業者等に要請する権限の新設
- 重大違反又は違反状態の継続に対する民事上の罰則の新設
- コミッショナーによる調査を妨害する者の防御方法の制限

また、EU は、2012 年 12 月 19 日、ニュージーランドの個人データ保護が十分であると認定し、国際間の個人データの流通の促進を円滑にするようにした¹¹。

② 個人情報に関連する最近の主要な裁判例

Westpac New Zealand Limited 及び Hager—プライバシー・コミッショナー捜査報告書¹²

・ 事案の概要

事業者等に対する警察による捜査の過程で個人の口座情報が開示された事案。Westpac 銀行は、警察の捜査に対して、Hager 氏の帳簿（センシティブな政府情報が含まれていた。）を開示した。警察は、Hager 氏が帳簿の作成に使用した情報をどのように入手したのかを捜査する過程で、Westpac 銀行に対して Hager 氏に関する情報を求めたところ、これに対して、Westpac 銀行は Hager 氏の数か月分の取引情報を警察に開示した。

・ コミッショナーの意見

Hager 氏による申立後、コミッショナーは、調査を行い、上記事案に関する意見を記載した報告書を Hager 氏に提供した。コミッショナーの意見は法的拘束力を有するものではないが、コミッショナーによるプライバシー法の解釈に関する有益な基準を提供するものである。

コミッショナーは、申出の内容を認め、Hager 氏の取引情報を警察に提供したことにより Westpac 銀行が Hager 氏のプライバシーを侵害したと判断した。Westpac 銀行は、自行の内規により警察への情報提供が認められるとの反論を行ったが、コミッショナーは、当該内規の適用は、警察からの一般的照会の場面ではなく詐欺及び不正行為の場面に限定されているとの理由で、当該内規により本件の情報提供が認められると解するのは合理的ではないと判断した。また、警察による捜査に協力するために銀行内部での調査が必要であったことを立証する令状その他の証拠が一切 Westpac 銀行に対して提供されていないことから、開示が法令等により義務付けられる場合に当該開示が許容されるとのプライバシー法上の例外にも該当しないと判断した。

¹¹ http://europa.eu/rapid/press-release_IP-12-1403_en.htm

¹² <https://www.privacy.org.nz/blog/hager-and-westpac/>

5. 中国

(1) 制度概要

① 法体系の概要

中国本土には包括的な個人情報（中国語は「个人信息」）保護法は存在しないが、多くの法律、行政法規、省令（以下、総称して本節において「法令等」という。）並びに地方政府規則、司法解釈及び国家基準において、個人情報保護に関する規定が分散している。

一般法としては、2017年に施行された民法総則（中国語は「民法总则」。主席令12届第66号、2013年3月15日公布、2017年10月1日施行）が存在する。民法総則第111条は、個人情報の取得の際の法律の遵守及び情報安全の確保の義務を規定し、違法な個人情報の収集・利用・加工・伝送・売買・提供・公開等の禁止を定めている。

また、消費者権益保護法（中国語は「消费者权益保护法」。主席令12届第7号）第29条1項は、事業者が消費者の個人情報の収集・使用にあたり、適法性、正当性、必要性の原則を尊重し、収集・使用の目的、方式及び範囲を明示し、消費者の同意を得なければならないと規定し、同法第56条は、個人情報の侵害に対して、違法所得の10倍以下の過料を定めている。

また、刑法（中国語は「刑法」。主席令12届第80号の刑法修正案（十）による改正後のもの）第253条の1は、違法な個人情報の販売又は提供等に対する懲役刑、罰金等の処罰を規定する。個人情報に関する刑事的な規範として、司法解釈（「公民個人情報刑事案件の法律適用の若干問題に関する最高人民法院（注：最高裁判所）及び最高人民検察院の解釈」、法積[2017]10号。中国語は「最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释」。）や、裁判例（最高人民法院及び最高人民検察院が2017年5月10日付で公布した公民個人情報侵害犯罪の代表的な判例7件、中国語は「最高人民法院、最高人民检察院发布7起侵犯公民个人信息犯罪典型案例」。最高人民検察院が2017年5月16日付で公布した公民個人情報侵害犯罪の代表的な判例6件、中国語は「最高人民检察院发布6起侵犯公民个人信息犯罪典型案例」。）においても、個人情報保護の侵害に対し刑事責任が追及されることが強調されている。

分野ごとの立法としては、電気通信、金融・信用調査、送達サービス、労働者保護、未成年者保護や患者保護等の分野・対象について個別の法令等において規定されている（本報告書では、その内の重要な部分を記載する。）。

個人情報の定義などの重要な概念は整理・統一されていないが、2017年に施行¹されたサイバーセキュリティ法（インターネット安全法とする翻訳例もある。中国語では「网络安全法」。主席令12届第53号。以下「CS法」という。）及びその実施規定・国家基準は、個

¹ 2016年11月7日公布、2017年6月1日施行

個人情報の定義や個人情報の越境移転を含む内容を体系的にまとめたものであり、CS 法と直接関係がない分野を取り扱う場合でも、中国法の実務においては、CS 法の内容が参考にされている。CS 法は、個人データの越境移転制限の明確に規定する法律であり、個人情報・重要データの中国国内での保存義務を定め、業務上必要であるとして国外向けにデータを提供する必要がある場合には、「安全評価」を受ける義務も定めている（CS 法第 37 条）。

中華人民共和国国民経済及び社会発展第 13 次 5 年計画綱要（2016 年-2020 年）（中国語は「中华人民共和国国民经济和社会发展第十三个五年规划纲要」。2016 年 3 月 17 日公布。）の第 28 章において、データ資源の安全保護強化、インターネット空間の科学的管理、重要情報システム安全の全面保障などを実施するとしている。CS 法の整備は、この計画に沿った動きであると考えられる。

また、個人情報の漏えいの際の通知義務については、2018 年 5 月 1 日に施行される「個人情報セキュリティ規範」が、初めて比較的詳細な条文を定めている（詳細は(2)主な法律の概要②個人情報セキュリティ規範 エ 漏えい等事案発生時の本人及び監督機関等への報告義務に関する規定を参考。）。

国務院の「十三・五」国家情報化計画通知（中国語は「“十三五”国家信息化规划的通知」。国発〔2016〕73 号）²第 4 条(10)は、暗号法（中国語は「密码法」³）、個人情報保護法（中国語は「个人信息保护法」⁴）、未成年者のインターネット保護条例（中国語は「未成年人网络保护条例」）の立法を進めることを述べている。中国政府は、暗号法と未成年者インターネット権益保護条例について「意見募集」を行ったが、個人情報保護法については 2003 年から検討を開始したものの、現在に至ってもなお「立法計画」にさえ入っていない。中国の最高立法機関である全国人民代表大会の常務委員会の法制工作委員会は、2018 年 2 月 26 日、同委員会が関連部署と合同で CS 法等の法律実施状況をまとめる上で、個人情報保護法の関連問題について検討し、インターネットとビッグデータの発展の新しい特徴に応じて、個人情報保護の制度をさらに整備し、確実に個人情報権益の保護を強化すると表明したが⁵、個人情報保護法制定の具体的なスケジュールは定まっていない。

² http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm

³

<http://www.oscca.gov.cn/sca/hdjl/2017-04/28/1011759/files/96dc262159be40aab0b23f5329bb2f4.pdf>

⁴ http://www.sohu.com/a/203902011_500652

⁵ <http://npc.people.com.cn/n1/2018/0227/c14576-29835723.html>

② 法体系・分野ごとの規制の概要（法体系・分野の整理）

ア CS 法

CS 法は、中国のサイバーセキュリティにおける基本法であり、「ネットワーク運営者」及び「重要情報インフラ運営者」の義務を定め、「ネットワーク製品及びネットワークサービス」についての規制を設け、サイバーセキュリティに関連する個人情報保護の規定を設けている。上述した通り、中国においては包括的な個人情報保護を保護する法律はまだ存在していないため、仮に中国において今後サイバーセキュリティが関係せず個人情報保護が問題となる場合、CS 法における個人情報保護規定（例えば、個人情報の定義、個人情報保護の原則、データローカライゼーション、国外移転規制、個人情報提供禁止の例外の規定）が参照されることとなる。

イ 中央省庁である「公安部」と「工業・情報化部（中国語は「工业和信息化部）」が所管する法令

サイバー空間における個人情報保護に関しては、中国の社会安全管理を管轄する「公安部」と電気通信及びサイバーサービス管理を管轄する「工業・情報化部」が、それぞれ関連法令を公布・執行している。

「公安部」は、「パソコン情報システム安全保護条例」と「情報安全等級保護管理弁法」に基づいて情報安全等級保護管理という制度を設け、管理規範や技術基準を定めている。「パソコン情報システム安全保護条例」（中国語は「计算机信息系统安全保护条例」。国务院令 588 号、1994 年 2 月 18 日公布・施行、2011 年 1 月 8 日改正・施行）は、パソコン情報システムの安全を確保するために、安全等級保護制度及び安全監督を規定するものである。「情報安全等級保護管理弁法」（中国語は「信息安全等级保护管理办法」。公通字 [2007]43 号、2007 年 6 月 22 日公布・施行）は、「情報安全等級保護管理」を規範化するために、等級に応じて情報システムの運営者と利用者が「等級保護作業」を具体的に実施し、技術基準に基づいて等級要求に適合した「情報安全施設」を建設し、「安全管理制度」を制定・実施し、情報システムの測定評価を定期的に行う義務等を含む等級保護の実施と管理を定めている。

「工業・情報化部」は、「電信法」と「インターネット情報サービス管理弁法」に基づいて、電信業務事業者とインターネット情報サービス提供者に対する個人情報取扱管理に関する法令を定めている。個人情報に関連して、主に注目されている電気通信及びインターネット利用者の個人情報保護に関する規定（中国語は「电信和互联网用户个人信息保护规定」。工業・情報化部令 24 号、2013 年 7 月 16 日公布、2013 年 9 月 1 日施行）は、電気通信及びインターネット利用者の個人情報保護規定として、事業者が、電気通信及びイン

ターネットサービスの提供において利用者の個人情報の収集・使用することを規制し、適法・正当・必要の原則を定め、個人情報の安全に対する責任、利用者の同意の取得、説明開示義務や安全保障措置等の内容を規定している。

ウ インターネットセキュリティに関する実施規定と国家基準

CS 法を執行する国家機関である国家インターネット情報弁公室（中国語は「国家互联网信息办公室」。Cyberspace Administration of China, CAC）は、CS 法実施規定である各種省令の制定を推進し、また、中国国家標準化管理委員会の下部組織である全国情報セキュリティ標準化技術委員会⁶への業務指導を通じて、国家基準の制定も推進している。

以下は、2017 年 2 月末までに公布された実施規定と国家基準の一覧である（同月末までに公開された「意見募集稿⁷」を含む）。

1. 実施規定名（CAC が制定）	日付
モバイル・インターネット・アプリ・プログラム情報サービス管理規定（中国語「移动互联网应用程序信息服务管理規定」）	2016 年 6 月 28 日公布、 2016 年 8 月 1 日施行
インターネット情報検索サービス管理規定（中国語「互联网信息搜索服务管理規定」）	2016 年 6 月 25 日公布、 2016 年 8 月 1 日施行
重要情報インフラ施設セキュリティ保護条例（中国語「关键信息基础设施安全保护条例」）（意見募集稿）	2017 年 7 月 10 日公開
個人情報・重要データの越境移転安全評価弁法（中国語「个人信息和重要数据出境安全评估办法」）（意見募集稿）	2017 年 4 月 11 日公開
インターネットニュース情報サービス事業者コンテンツ管理人員管理弁法（中国語「互联网新闻信息服务单位内容管理从业人员管理办法」）	2017 年 10 月 30 日公布、 2017 年 12 月 1 日施行
インターネットニュース情報サービス新技術・新アプリ安全評価管理規定（中国語「互联网新闻信息服务管	2017 年 10 月 30 日公布、 2017 年 12 月 1 日施行

⁶全国情報セキュリティ標準化技術委員会の定款によると、同委員会は、国家標準化管理委員会の統率の下に CAC の業務指導を受けるものとする。定款の全文は下記ショットカット参考。

https://www.tc260.org.cn/front/tiaozhuan.html?page=/front/gywm/gzgd_Detail

⁷パブリックコメントを意味する。

理規定)	
インターネットグループ情報サービス管理規定（中国語「互联网群组信息服务管理规定」）	2017年9月7日公布、 2017年10月8日施行
インターネット利用者パブリックアカウント情報サービス管理規定（中国語「互联网用户公众账号信息服务管理规定」）	2017年9月7日公布、 2017年10月8日施行
インターネット掲示板・コミュニティサービス管理規定（中国語「互联网论坛社区服务管理规定」）	2017年8月25日公布、 2017年10月1日施行
インターネットコメント書き込みサービス管理規定（中国語「互联网跟帖评论服务管理规定」）	2017年8月25日公布、 2017年10月1日施行
インターネット情報コンテンツ管理行政法令執行手続き規定（中国語「互联网信息内容管理行政执法程序规定」）	2017年5月2日公布、 2017年6月1日施行
インターネットニュース情報サービス許可管理実施細則（中国語「互联网新闻信息服务许可管理实施细则」）	2017年5月22日公布・施行
インターネット生放送サービス管理規定（中国語「互联网直播服务管理规定」）	2016年11月4日公布、 2016年12月1日施行
国家インターネットセキュリティ事件応急プラン（中国語「国家网络安全事件应急预案」）	2017年1月10日公布・施行
インターネット製品・サービス安全審査弁法（試行）（中国語「网络产品和服务安全审查办法」（試行））	2017年5月2日公布、 2017年6月1日施行
インターネット重要設備・インターネット安全専用製品目録（第1回）（中国語「网络关键设备和网络安全专用产品目录」（試行））	2017年6月1日公布・施行
2. 国家基準（中国国家標準化管理委員会が制定）	
情報セキュリティ技術—公的及び商業サービスのための情報システム内での個人情報保護ガイドライン（中国語「GB/Z28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南」）	2012年11月5日公布、 2013年2月1日施行

個人情報セキュリティ規範（中国語「GB/T35273-2017 个人信息安全规范」）	2017年12月29日公布、 2018年5月1日施行
スマート移動端末の個人情報保護技術要求（中国語「GB/T34978-2017 移动智能终端个人信息保护技术要求」）	2017年11月1日公布、 2018年5月1日施行
個人情報匿名化ガイドライン（意見募集稿）（中国語「个人信息去标识化指南」）	2017年8月25日公開
重要情報インフラ施設安全検査評価ガイドライン（意見募集稿）（中国語「关键信息基础设施安全检查评估指南」）	2017年8月30日公開
重要情報インフラ施設安全保障評価指標システム（意見募集稿）（中国語「关键信息基础设施安全保障评价指标体系」）	2017年8月30日公開
インターネット製品とサービス安全通用要求（意見募集稿）（中国語「网络产品和服务安全通用要求」）	2017年8月30日公開
インターネットセキュリティ等級保護測定評価プロセスガイドライン（意見募集稿）（中国語「网络安全等级保护测评过程指南」）	2016年11月3日公布
インターネットセキュリティ等級保護測定評価要求（各部分内容）（意見募集稿）（中国語「网络安全等级保护测评要求（各部分内容）」）	第1部分：2016年11月3日公布 第2部分：2017年1月11日公布 第3部分：2016年11月3日公布 第4部分：2017年1月11日公布 第5部分：2017年1月11日公布
データ越境安全評価ガイドライン（意見募集稿）（中国語「数据出境安全评估指南」）	2017年8月25日公開
重要情報インフラ施設識別ガイドライン（制定中）（中国語「关键信息基础设施识别指南」）	（制定中）

上記の一覧中、個人情報保護に関して最も注目されるのは、「情報セキュリティ技術—公的及び商業サービスのための情報システム内での個人情報保護ガイドライン」（指導性技術基準 GB/Z28828-2012、以下「個人情報保護ガイドライン」という。）と、「情報セキュリティ技術—個人情報セキュリティ規範」（指導性技術基準 GB/T35273-2017、以下「個人情報セキュリティ規範」という。）である。二つとも、国家推奨標準⁸に該当し、法的強制力がな

⁸ 主席令 12 届第 78 号による改正後の標準化法によると、標準とは農業、工業、サービス業及び社会事業等分野において統一を必要とする技術要求を指し、国家強制標準とは、人体

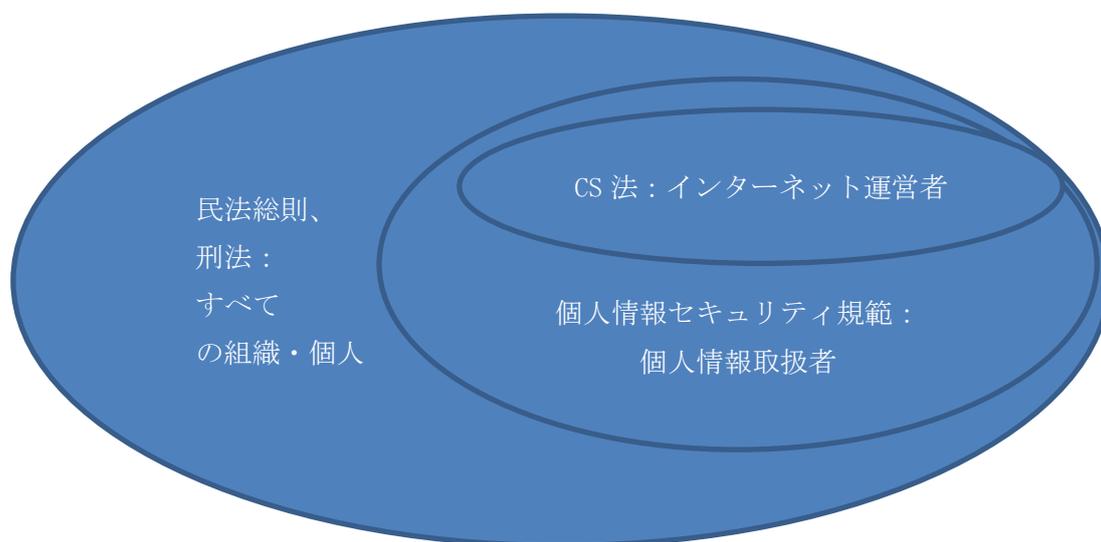
いが、業種横断的な規定として特別法の解釈の際にも事実上参照されることが多く、実務的な重要性が高い。

「個人情報保護ガイドライン」は、初めての個人情報保護の国家標準として、情報システムを経由する個人情報の取扱いを規制するものであり、通信事業者・金融業者及び医療事業者などの民間事業者に適用される（個人情報保護ガイドライン第1条）。

「個人情報セキュリティ規範」は、民間事業者などの組織体による、個人情報の取扱いを規律し（個人情報セキュリティ規範第1条）、事業者のプライバシーポリシーの制定と個人情報管理の規範化に関するガイドラインを示すものである。個人情報セキュリティ規範は、直接に拘束力のある規範ではなく、推奨的な基準に過ぎないが、GDPRやAPECプライバシー・フレームワーク等の先進主要国家の最新の立法成果を参考として制定されている。

「個人情報セキュリティ規範」は、上記の「個人情報保護ガイドライン」と内容的に重なるところが多いものの、「個人情報保護ガイドライン」より適用範囲が広く、より詳細な内容を規定している。本報告書においては、「個人情報セキュリティ規範」を主に説明することとする。

CS法、個人情報セキュリティ規範、民法通則・刑法との適用対象範囲の関係を概念図として示すと下記のようなになる。



の健康、人身、財産の安全、国家安全、生態環境安全を保障し、及び経済社会管理の基本需要を満たす技術要求を指し、国家推奨標準とは、基礎通用を満たし国家強制標準と組合せ各関連業界に対して指導の役割を發揮する等の需要を満たす技術要求を指す（標準化法第2条1項、10条1項、11条1項）。推奨標準については、国はその採用を奨励するとされている（標準化法第2条3項）。

エ その他の関係法令（金融・情報通信分野）

銀行業金融機関による個人金融情報保護の向上に関する通達（中国語は「关于银行业金融机构做好个人金融信息保护工作的通知」。銀発[2011]17号、2011年1月21日公布、2011年5月1日施行）は、銀行業を営む金融機関による個人の金融情報の収集・保管・使用・対外提供行為を規制している。金融消費者の適法な権利を保護する法令として、対象情報の範囲や適法合理の原則、情報安全装置や内部体制の構築完備や委託先への監督等を定めている。

就業サービス及び就業管理規定（中国語は「就业服务与就业管理规定」。2007年11月5日公布、2008年1月1日施行、2015年4月30日改正）は、使用者が労働者の個人情報に対して守秘義務を負い、その公開には本人の書面同意が必要と規定している。

配達サービスにおけるユーザー個人情報セキュリティ管理規定（中国語は「寄递服务用户个人信息安全管理规定」。国郵発[2014]52号、2014年3月19日公布、2014年3月19日施行）は、配達サービスの経営及び使用に関わる利用者個人情報安全について、事業者の守秘義務、安全保障措置の整備、配達明細書に関する情報安全管理を規定している。

信用調査業管理条例（中国語は「征信业管理条例」。2013年国務院令第631号、2013年1月21日公布、2013年3月15日施行）は、企業や個人の信用情報に対する収集・整理・保管・加工・提供の活動を規制し、本人の同意の取得や個人不良情報（情報主体の信用状況に対してマイナスの影響を与える情報の意味）の提供前の本人への事前通知、個人の不良情報保管期限、情報主体の本人信用報告書の無料取得権利、収集された情報の整理・保管・加工を中国のみにおいて行う、といった信用調査業務の規則及び情報主体の異議及びクレームの権利を規定する。

③ 民間部門・公的部門の区別

中国の個人情報保護に関する法令は、適用対象が民間部門に限定されるもの（又は民間部門を中心とするもの）がほとんどであり、公的部門を適用対象とする個人情報保護の専門法令は、未だ存在していない。ただし、近年では、政府当局が取得する個人情報の保護に関する義務を定める条文を設ける立法例も増えている。

例えば、CS法第73条は、当局が職務履行において取得した情報をその他の用途に利用する場合、直接の責任者や担当者に対して法に従い処分を科すと定めている。裁判所に関して、「人民法院が刑事案件第一審普通手続法廷調査規程（試行）」（2017年6月6日公布・施行）は、証人・鑑定人・被害者の個人情報を公開しないとの保護措置を定めている。

④ 国家法令と地方法令の存在

中国の各地方においては、その地方特有の個人情報に関する規定が存在する。例えば、中国において特に IT 産業が発達している浙江省や広東省等においては、社会/公共信用情報条例や情報化促進条例といった規定が多く存在する。これらの地方性法規⁹は事業者の安全保障義務や罰則等に関する規則を定めている。

例えば、「広東省情報化促進条例」（中国語は「广东省信息化促进条例」。2014年9月1日施行）第28条は、個人情報収集の際に対象者の同意の取得や用途の説明や所定用途内での情報使用に関する義務、第31条は、公民情報の漏えい・改ざん・毀損・販売・不法提供の禁止、第71条は、第31条への違反行為に対して当局の是正命令と1万人民元以上5万人民元以下の課徴金及び違法所得の没収等の行政処罰を定めている。

また、「浙江省公共信用情報管理条例」（中国語は「浙江省公共信用信息管理条例」。2017年9月30日公布、2018年1月1日施行）も注目されている。同条例第14条は、個人の宗教信仰、ゲノム、指紋、血型、病気と病歴情報等の収集禁止、及び本人の同意なしに個人の収入、預金、有価証券、商業保険、不動産及び納税額等の情報の収集禁止を定めている。同条例第35条は、個人情報侵害行為に対する罰則として、違法所得の没収、組織に対しては、1万人民元以上10万人民元以下の課徴金、個人に対し1,000人民元以上1万人民元以下の課徴金を定めている。

したがって、特定地域において個人情報の取得・保管・利用を行う場合、当該地域の地方規程に留意する必要がある。なお、広東省や浙江省のような IT 経済発達地域の立法・執行動向が他の地域に浸透していくプロセスも今後注目される。

⑤ 紛争処理手続き

中国の現行法令の中に、個人情報権利が侵害された個人情報主体が、行政当局に対して苦情を述べ、行政当局が苦情に基づいて斡旋・調停又は行政処分・指導等を行う旨の行政救済措置は、現時点で確認できていない。よって、個人情報保護に関する紛争処理手続きは、行政手続きは存在せず、民事訴訟（司法手続き）のみであると考えられる。

個人情報に関する紛争の民事訴訟は、他の民事訴訟と同様に、基礎人民法院による第一審及び中級人民法院による第二審により構成される二審終審制度が適用される（主席令12届第71号による改正後の民事訴訟法第10条、第17条）。

民法総則施行前には、個人情報は、「権利侵害責任法」におけるプライバシー権として一定レベルの保護を受けるが、プライバシー権の定義に関する明文規定が存在しないため、民事法上のプライバシー権に基づく個人情報保護の効果は限定的であった。情報ネットワ

⁹ 「地方性法規」とは、省・自治区・直轄市の人民代表大会（日本の都道府県議会に相当する）が制定した規範を意味する（中国立法法78条）。実務では、「地方性法規」の名称として「条例」を使用することが多いが、「実施弁法」や「規定」等を名称として使用することがある。

ークを利用した個人情報侵害紛争を対処するために最高人民法院は「情報ネットワークを利用した人身権の侵害に係る民事紛争事件の審理における法律適用の若干問題に関する規定」（中国語は「最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定」。法积[2014]11号、2014年8月21日公布、2014年10月10日施行。）第12条において、「インターネット利用者又はネットワークサービス提供者がインターネットを利用して自然人のゲノム情報、病歴資料、健康診断資料、犯罪記録、家庭住所、個人的活動等個人のプライバシーその他の個人情報を公開することにより、他人に損害を与えた場合、被害者は不法行為責任を追及できる。」と定めた。また、同法积第18条は、損害賠償の対象を「侵害行為を制止するための合理的な支出（弁護士費用、調査・証拠取得の合理費用を含める。）」とする（財産損失又は収益を確定できない場合は、人民法院が50万人民币以下の範囲内において損害賠償金額を決めることができるとする）。また、同法积は、精神的損害に基づく損害賠償も明記している。

上記の司法解釈が出された後、個人情報の権利を規定する民法総則が公布された。民法総則は、個人情報の権利を定めているので、個人情報の権利主体は、個人情報の権利が侵害された場合、民法総則を根拠法として、侵害者に対して民事訴訟を提起することが可能となった。この個人情報の権利侵害に関して、民事責任の負担の方法として、民法総則第179条は侵害の停止、妨害の排除、危険の除去、原状の回復、履行の継続、損害の賠償、違約金の支払、影響の除去、名誉の回復、謝罪等を規定する。

消費者保護法第50条によると、経営者が消費者の個人情報の権利を侵害した場合、侵害行為停止、名誉回復、影響排除、謝罪、損害賠償を行わなければならない。また、同法第56条は、経営者が違法に他人に消費者の個人情報を提供した場合、消費者に損害賠償を行うものとし、賠償金額は違法提供の収益と規定する（なお、消費者に生じた損失額が、収益の額を超えた場合、賠償金額は消費者の損失額に準じ、収益と実際損失が確定できない場合、賠償金額は500人民币を下回ってはならないとされている）。また、消費者に嚴重な精神損害を与えた場合、3000人民币を下回らない精神損害賠償を支払うものとされている。

中国消費者權益保護法は、省レベルの消費者權益保護委員会に対して公益訴訟の起訴権を与えている（法第47条）。

(2) 主な法律の概要

①CS 法

ア 法律の概要

上述した通り、CS 法は、中国のサイバーセキュリティにおける基本法であり、「ネットワーク運営者¹⁰」及び「重要情報インフラ運営者¹¹」の義務を定め、「ネットワーク製品及びネットワークサービス」についての規制を設け、サイバーセキュリティに関連する個人情報保護の規定を設けている。

CS 法の目的は、「サイバーセキュリティを保障し、サイバー空間の主権及び国家の安全・社会公共利益を維持し、公民・法人及びその他の組織の合法的権益を保護し、経済・社会の情報化の健全な発展を促進すること」である（法第 1 条）。

イ 個人情報の定義

「個人情報」とは、電子又はその他の方式で記録した単独又はその他の情報と組み合わせることで自然人（個人）の身分を識別することができる、自然人の氏名、生年月日、身分証番号、個人の生体認証情報、住所、電話番号等を含むがこれらに限らない各種情報をいう（法第 76 条（五））。

ウ 主な規制・権利の内容

「ネットワーク運営者」は、収集した利用者情報について厳格に秘密保持し、利用者情報保護制度を構築・整備しなければならない（法第 40 条）。

個人情報の収集・使用について、「ネットワーク運営者」は、合法、正当、必要の原則を遵守する義務を負い、収集、使用についてのルールを公開する。情報を収集、使用する目的、方式及び範囲を明示するとともに、本人の同意を取得し、その提供するサービスに関係のない個人情報を収集してはならない。法律、行政法規の規定及び双方間の取決めに違

¹⁰ 「ネットワーク運営者」とは、情報を収集、保管、送信、交換及び処理するパソコン及びその他の情報端末並びに関連設備からなるシステムであるネットワークの所有者・管理者及びサービスプロバイダーを含む者である（CS 法第 76 条）。

¹¹ 「重要情報インフラ運営者」は、ネットワーク運営者に含まれる亜集団として、公共通信・情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政府等の重要な産業及び分野、並びにひとたび機能の破壊、喪失又はデータの漏えいに遭遇した場合、国の安全、国民経済と民生、公共の利益に重大な危害を与え得るその他の重要情報インフラについて、国によりサイバーセキュリティ等級保護制度に基づき、重点保護を実施される重要情報インフラの運営者、と間接的に定義されている（CS 法第 31 条）。

反して、個人情報を収集、使用してはならず、かつ法律、行政法規の規定及びユーザーとの取決めに従い、その保存する個人情報を処理しなければならない（法第 41 条）。

個人情報の保護について、「ネットワーク運営者」は、その収集した個人情報を漏えい、改ざん、毀損してはならず、被収集者の同意を得ずに他人に個人情報を提供してはならない（ただし、処理作業を経て、特定の個人を識別できず、かつ復元できない場合を除く。法 42 条 1 項）。「ネットワーク運営者」は、技術的措置及びその他必要な措置を講じ、その収集した個人情報の安全を確保し、情報の漏えい、破損、紛失を防止しなければならない。個人情報の漏えい、破損、紛失が発生した又は発生する恐れがある場合は、直ちに救済措置を講じ、規定に従って速やかにユーザーに告知するとともに、関連の主管部門に報告しなければならない（法第 42 条 2 項）。

個人の権利について、個人は、「ネットワーク運営者」が、法律、行政法規の規定又は双方間の取決めに違反して、その個人情報を収集、使用していることを発見した場合、ネットワーク運営者にその個人情報の削除を要求する権利を有し、「ネットワーク運営者」が収集、保存したその個人情報に誤りがあることを発見した場合は、「ネットワーク運営者」に訂正を要求する権利を有する（法第 43 条）。

なお、個人情報の不法取得、売却、提供は禁止されている（法第 44 条）。

サイバーセキュリティについて監督管理責任を負う部門やその人員は、職務履行において知り得た個人情報、プライバシー及び営業秘密について厳格に秘密保持する義務を負い、漏えい、販売又は違法に第三者に提供してはならない（法第 45 条）。

「ネットワーク運営者」、「ネットワーク製品又はサービスの提供者」が個人情報権利を侵害した場合、関連管理当局が是正命令を下し、警告し、違法所得を没収し、違法所得額の 10 倍以下の課徴金を課する（違法所得がない場合、100 万人民元以下の課徴金を課する。直接個人情報を管理する者及びその他の直接的な責任者に 1 万人民元以上 10 万人民元以下の課徴金を課する。）。また、深刻な状況の場合、関連業務の一時停止、業務停止、ウェブサイトの閉鎖、関連業務許可証書又は営業許可証を取り消すことができる。（法第 64 条 1 項）

窃取又はその他の方法によって個人情報を違法に取得し、違法に販売し、又は、他人に対して違法に提供を行なった場合、仮に刑事上の犯罪行為に該当しない場合¹²であっても、公安機関は、行政処分（違法所得の没収及び違法所得額の 10 倍以下の課徴金（違法所得がない場合、100 万人民元以下の課徴金））を課す（法第 64 条 2 項）。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

法第 42 条は、「ネットワーク運営者」は、その収集した個人情報を漏えい、改ざん、毀

¹² 例えば、100 人以上に個人情報を販売した場合に刑事罰を課すと規定しているとき、50 人に個人情報を販売しても刑事罰は課されないが、行政罰は課され得る。

損してはならず、被収集者の同意を得ず、他人に個人情報を提供してはならないといった不作為義務を定めると同時に、技術的措置及びその他必要な措置を講じ、その収集した個人情報の安全を確保し、情報の漏えい、破損、紛失を防止しなければならず、個人情報の漏えい、破損、紛失が発生した又は発生する恐れがある場合は、直ちに救済措置を講じ、規定に従って速やかにユーザーに告知するとともに、関連の主管部門に報告しなければならないといった作為義務も定めている。

オ 安全管理措置に関する規定（第 21 条～第 27 条、第 29 条）

CS 法に基づき、中国政府は、サイバーセキュリティのレベル別保護制度を実施することとなる。「ネットワーク運営者」は、サイバーセキュリティレベル別保護制度の要件に基づき、次の各号に掲げる安全保護義務を履行し、ネットワークが妨害、破壊又は無許可アクセスを受けないよう保障し、ネットワークデータの漏えい又は窃取、改ざんを防止しなければならない。

- (一) 内部安全管理制度及び操作規定を制定し、サイバーセキュリティ安全責任者を確定し、サイバーセキュリティの保護に係る責任の所在を明確にする。
- (二) コンピュータウイルス及びサイバー攻撃、ネットワークへの不正侵入等サイバーセキュリティを脅かす行為を防止するための技術的措置を講じる。
- (三) ネットワークの運用状態、サイバーセキュリティ事件を監視し、規定に従って、少なくとも 6 か月間、関連するログファイルを保存する。
- (四) データの分類、重要データのバックアップ及び暗号化等の措置を講じる。(法第 21 条)

法第 22 条は、インターネット製品とサービスに対して、関連国家基準の強制的な要求への適合、悪意あるプログラムの設置禁止、安全欠陥・バグ等のリスクへの即時処理措置及び利用者への告知と主管当局への報告義務、継続的な安全維持の提供義務、利用者情報機能を有するインターネット製品とサービスについて明示と同意取得義務を定めている。

法第 23 条は、インターネット重要設備とインターネット安全専用製品の認証検測義務を定めている。

法第 24 条は、インターネット運営者が利用者の本人確認義務を定めている。

法第 25 条は、インターネット運営者のインターネットセキュリティ事件応急予備方案の制定義務、システムバグ、パソコンウイルス、インターネット攻撃、インターネット侵入等セキュリティリスクの処理義務、インターネットセキュリティを害する事件が発生する際に、応急予備方案の起動や相応的な処理や主管当局への報告を定めている。

カ 適用範囲

CS 法は、中国国内においてインターネットの設置、運営、維持、使用、及びサイバーセ

セキュリティの監督管理を適用対象とする（法第2条）。しかし、国が措置を講じて監督予測、防御、処理するサイバーセキュリティリスクが、中国国外から由来したのも対象となる。さらに、法第75条は、海外の機構・組織・個人が中国の重要情報基礎施設への攻撃・侵入・阻害・破壊等活動に従事し重大な結果をもたらした場合、法律に基づいて法的責任を追及し、公安部門と関連当局は当該機構・組織・個人に対して財産凍結又はその他の必要な制裁措置を講じることを決定することができる。

キ 国際的な情報移転に関する規定

CS法は、個人情報・重要データを中国国内に保存する義務を定めるが、その例外として「安全評価」を受ける義務を履行する前提で、中国国外向けに提供する業務上の必要のある場合を認めている（法第37条）。

CS法は、2017年6月1日に施行されたが、安全評価を含む実施規則については、制定準備中である。

2017年4月11日に、CS法の実施規則の一つとなる「個人情報・重要データの越境移転安全評価弁法」（以下「安全評価弁法草案」という。）の意見募集稿が、公開された。安全評価弁法草案は、適用対象者を「重要情報インフラ運営者」から、「ネットワーク運営者」まで拡大しており、この点について、中国で事業を営む者の一部から反対があった。

この反対意見を受け、上記の安全評価弁法草案は修正され、また、猶予期間を設けて施行される予定であるが、本報告書作成の時点で実施時期は未定、実施予定される案文も確定していない。

また、上述したとおり、法第37条は、一定の場合に例外的に越境移転を認めている。しかし、安全評価弁法草案第11条は、次の①～③の場合を、個人情報・重要データの越境移転の禁止類型として定めている。

- ① 個人情報の越境移転について個人情報の主体の同意を得ていないとき、又は個人の利益を害するおそれがあるとき
- ② データの外国への移転が国家の政治、経済、科学技術、国防等の安全にリスクをもたらす、国家安全に影響し、社会公共利益を損なうおそれがあるとき
- ③ その他、国家ネットワーク通信部門、公安部門、安全部門等の関連部門がデータの外国への移転をできないものと認定したとき

中国国内に保存する義務のある重要データについて

「重要データ」については、CS法では定義されていないが、「情報安全技術 データ出国安全評価ガイドライン」という国家標準草案における附録A「重要データ識別ガイドライン」¹³の冒頭において、「重要データ」は定義されている。

¹³ CS法実施細則の一つとして、2017年5月27日に公布

それによれば、「重要データ」とは、中国政府・企業・個人が中国国内において収集・生成する、国家秘密に関わらないが、国家安全・経済発展及び公共利益に緊密に関連するデータ（原始データ及び派生データを含む）であり、それらのデータが無断に開示・紛失・濫用・改ざん又は破壊され、又は集合・整合・解析される場合に、国家安全・国防利益・国家財産・社会公共利益と個人の合法的な利益に損害を与え、国家政治・国土・軍事・経済・文化・社会・科技・情報・生態・資源・核施設等その他の国家安全事項に影響又は損害を与える結果をもたらすおそれのあるデータである。

「重要データ識別ガイドライン」は、27 の業界にわたり、それぞれの重要データをリストアップしており、ネットワーク運営者が取り扱う情報は、一般的に「重要データ」に該当しないと考えられている（ただ、「重要データ識別ガイドライン」の最後における A27「電子商取引」に記載される「電子商取引記録及び関連の個人消費習慣と企業経営データ等」に該当すると判断されるおそれがある）。

越境移転のために必要な手続・登録等

個人情報を超境移転させる場合、個人情報の主体に対してデータの外国への移転の目的、範囲、内容、移転先及び移転先が所在する国家又は地区について説明し、かつ、その同意を得なければならない。未成年者の個人情報の越境移転にはその監護者の同意を得なければならない（安全評価弁法草案 4 条）。

「ネットワーク運営者」は、以下の内容についての評価に重点を置き、データを外国へ移転させる前にデータの当該移転に対する「安全評価」を自ら行い、かつ、評価結果に対して責任を負わなければならない。

- ・ 移転の必要性
- ・ 個人情報の状況はどのようなものであるか、データ主体の同意が得られているか
- ・ 重要データの状況はどのようなものであるか
- ・ データ受領者が導入している保護措置、データ受領者のデータ保護のセキュリティ、送付先の国又は地域のデータ保護の環境
- ・ データ漏えい、破損、改ざん、濫用のリスク
- ・ 国の安全、社会及び公共の利益、個人の合法的な利益に関連するリスク（安全評価弁法草案第 7 条、第 8 条）

データの外国への移転に以下の状況のいずれかがある場合、ネットワーク運営者は、業界主管又は監督部門に安全評価の実施を申請しなければならない（安全評価弁法草案第 9 条）。

- ・ 500,000 名を超える人の個人情報の移転
- ・ 1,000GB を超えるデータの移転
- ・ 核施設、化学生物学、国防又は軍事、公衆衛生、大型工事プロジェクト、海洋環境、機密情報にまつわる地理情報の分野に関するデータの移転

- ・ 重要情報インフラ運営者のシステムの脆弱性及びセキュリティ防護策に関するネットワークセキュリティ情報の移転
- ・ 重要情報インフラ運営者による海外受領者に対する個人情報又は重要データの提供に関するデータの移転
- ・ 国の安全及び公共の利益に潜在的に影響を及ぼすその他の移転、又は業界の主務官庁又は監督官庁によるレビューを必要とする移転

国境を越えてのグループ会社間の個人情報・重要データの共有・共同利用

国境を越えてのグループ会社間の個人情報・重要データの共有・共同利用について、CS法及び各実施規則（草案を含む）は、全く言及しておらず、特別な取扱いの規定は現在のところ存在していない。

②個人情報セキュリティ規範

ア 法律の概要

個人情報に係るセキュリティ問題について、個人情報の取扱者が収集、保存、利用、提供、譲渡、公開開示等の情報処理プロセスにおける関連行為を規律し、個人情報の違法収集、濫用、漏えい等の「混乱現象」を抑止し、個人の適法権益と社会公共利益を最大限に保護することを目的とする。

イ 個人情報の定義

中国の個人情報に関する定義は、業界ごとにいくつかの法令において規定されているが、必ずしも一致していない。個人情報セキュリティ規範における個人情報と個人センシティブ情報の定義は、特徴を説明し、例示列举という形で行い、現時点で中国において権威的なものといえる。

第 3.1 条は、個人情報を、「電子又はその他の方法で記録され、単独又はその他の情報との結合で特定自然人の身分を識別できる、又は特定自然人の活動状況を反映できる各種情報」と定義する。さらに、第 3.1 条注 1 は、氏名、生年月日、身分証明書番号、個人の生体認証情報、住所、通信連絡方法、通信記録と内容、アカウント暗証番号、信用情報、移動履歴、宿泊情報、健康生理情報、取引情報等を個人情報として列举し、第 3.1 条注 2 は、別添 A で個人情報の範囲及び類型を定めると注記している。

別添 A は、個人情報の判断に当たり、識別（EU の個人情報の要素：identified or identifiable）と関連（アメリカの個人情報の要素：linked or linkable）のいずれに該当するかという判断方法を定めるとともに、表 A1 で個人情報例 13 種類を列举している。

個人基本資料	個人氏名、生年月日、性別、民族、国籍、家族関係、住所、個人電話番号、電子メールアドレス等
個人身分情報	身分証明書、軍官証、パスポート、免許証、勤務証、出入証、社会保険カード、居住証等
個人の生体認証情報	ヒトゲノム、指紋、声紋、掌紋、耳介、虹彩、顔特徴量等
インターネットのID情報	システムアカウント、IPアドレス、メールアドレス及びそれらの暗号、パスワード、パスワード保護回答、利用者の個人データ証書等
個人の健康生理情報	個人の、病気や治療等によって生じた関連記録。例えば、病症・入院歴・医師の診断書・検査報告・手術及び麻酔記録、看護記録、薬品使用記録、薬物・食物アレルギー情報、出産情報・既往歴、診療治療状況、家族病歴、現病歴、伝染病歴等。また、個人の身体の健康状況によって生じる関連情報及び体重、身長、肺活量等
個人の教育、就業情報	個人の職業、職位、勤務先、学歴、学位、教育経歴、職務経歴、研修記録、成績書等
個人の財産情報	銀行口座、認証情報（パスワード）、預金情報（資金数量、出入金記録などを含む）、不動産情報、ローン記録、信用情報、取引及び消費記録、一定期間の取引明細等、及び仮想通貨、仮想通貨取引、ゲーム類のシリアルコード等仮想通貨情報
個人の通信情報	通信記録、内容、SMS、MMS、電子メール、及び個人の通信を記述したデータ（通常はメタデータという。）等
連絡先情報	連絡先リスト、友人リスト、グループリスト、電子メールアドレスリスト等
個人のインターネット利用記録	日誌に保管されているユーザー操作記録で、ウェブサイト閲覧記録、ソフトウェア使用記録、クリック記録等
個人の常用デバイス情報	ハードウェアのシリアル番号、デバイスのMACアドレス、ソフトウェアリスト、固有のデバイス識別コード（例えばIMEI/android ID/IDFA/OPENUDID/GUID、SIMカードIMSI情報等）等を含む個人の常用デバイスの基本状況を記述した情報
個人の位置情報	移動履歴、GPS情報、宿泊情報、経緯度等
その他の情報	結婚歴、宗教・信仰、性的指向、未公開の違法犯罪記録等

第 3.2 条は、個人センシティブ情報を「一旦漏えい又は違法提供又は濫用されると人身又は財産安全に害したり、個人の名誉・心身健康に損害を与えたり、差別待遇等されたりする恐れのある個人情報」と定義する。また、第 3.2 条注 1 は、身分証明書番号、バイオメトリクス、銀行口座、通信記録と内容、財産情報、信用情報、行動追跡記録、宿泊情報、健康生理情報、取引情報、14 歳以下児童の個人情報等を個人センシティブ情報として列挙し、第 3.2 条注 2 は、別添 B で個人センシティブ情報の範囲及び類型を定めると注記している。

別添 B は、個人センシティブ情報の判断方法を説明するとともに、表 B.1 で個人センシティブ情報例 6 種類を列挙している。

個人の財産情報	銀行口座、認証情報（パスワード）、預金情報（資金数量、出入金記録等を含む）、不動産情報、ローン記録、信用情報、取引及び消費記録、一定期間の取引明細等、及び仮想通貨、仮想通貨取引、ゲーム
---------	--

	類のシリアルコードなど仮想財産情報
個人の健康生理情報	個人の、病気や治療等によって生じた関連記録。例えば、病症、入院歴、医師の診断書、検査報告、手術及び麻酔記録、看護記録、薬品使用記録・薬物・食物アレルギー情報、出産情報、既往歴、診察治療状況、家族歴、現病歴、伝染病歴等。また、個人の身体の状態によって生じる関連情報等
個人の生体認証情報	ヒトゲノム、指紋、声紋、掌紋、耳介、虹彩、顔の特徴量等
個人の身分情報	身分証、軍官証、パスポート、運転免許証、職員証、社会保険カード、居住証等
インターネットのID情報	システムアカウント、メールアドレス、及び左記に関する暗証番号、パスワード、パスワード保護質問の答え、ユーザー個人のデジタル証明書等
その他の情報	個人電話番号、性的指向、結婚歴、宗教・信仰、未公開の違法犯罪記録、通信の記録及び内容、移動履歴、ウェブサイト閲覧記録、宿泊記録、精確な測位情報等

ウ 主な規制・権利の内容

個人情報セキュリティ規範は、GDPR を参考にして個人情報処理の目的・方法等を決定する権利を有する組織又は個人、すなわち個人情報取扱者（personal data controller）を規制対象主体としている（第 3.4 条）。同規範は、収集・保管・利用・提供・譲渡・公開開示等の個人情報処理活動を規制対象行為とし、それらの活動の際に遵守すべき原則及びセキュリティ要求を定めている（第 1 条）。

第 3 条「定義」は、個人情報、個人センシティブ情報、個人情報取扱者を除いて、個人情報主体、収集、明確な同意、ユーザープロファイリング、個人情報セキュリティ影響評価、削除、公開開示、譲渡、提供、匿名化、非特定化について定義を定めている。

第 4 条「個人情報セキュリティ基本原則」は、権利責任一致原則、目的明確原則、選択同意原則、最小限の十分な利用の原則、公開透明原則、セキュリティ確保原則、主体関与原則という 7 つの原則を定めている。

第 5 条から第 9 条は、取扱、保存、利用、譲渡、開示及び通用セキュリティといった個人情報処理全周期の各段階・方面におけるセキュリティ規範要求を定めている。

第 5 条「個人情報の取扱」は、適法性、最小限、直接取得と間接取得を区別し個人情報主体の授権同意の取得を要求するとともに、授権同意取得の例外場合を列挙し、個人センシティブ情報の収集に明確な同意の取得を要求し、かつ別添 C で個人情報主体の同意権選択を保障するための方法を例示している。さらに、第 5.6 条は、プライバシーポリシーの内容及び形式について定め、別添 D でプライバシーポリシー雛形を例示している。同プライバシーポリシー雛形は、2017 年 9 月に CAC により展開された個人情報保護向上行動のプライバシーポリシーキャンペーンにおいて数多くの大手ネットワーク会社が利用した。

第 6 条「個人情報の保存」は、保存期間最小化、非特定化処理、個人センシティブ情報の伝送と保管の際の暗号化等セキュリティ措置、個人情報支配者が製品又はサービスの運営を停止する際に個人情報取扱の即時停止、運営停止という旨を個人情報主体にお知らせ、保有する個人情報を削除又は匿名化処理すると定めている。

第 7 条「個人情報の利用」は、アクセス制限措置、表示制限、利用制限、個人情報主体に対して情報アクセスの提供、個人情報訂正・削除、個人情報主体の同意の撤回（個人情報の継続処理禁止、ビジネス広告の伝送の拒否権）・アカウントの閉鎖（閉鎖方法の確保、操作の便利さ、閉鎖後の個人情報の削除又は匿名化処理）・個人情報副本の取得、情報システムの自動決断への制限、個人情報主体の請求への対応（30 日以内）、苦情管理に関して個人情報支配者の義務を定めている。

第 8 条「個人情報の委託処理、提供、譲渡、公開開示」は、個人情報取扱者が同意範囲を超えて委託してはならず、委託行為に対して個人情報セキュリティ影響評価を行い、契約書又は監査を通じて受託者に対して監督すると規定している。個人情報の提供・譲渡は、原則として禁止されるが、提供・譲渡する必要がある場合、個人情報主体の明確な同意を取得するものとされている。買収・合併・再編に伴う個人情報譲渡について、個人情報取扱者は告知する義務を負い、且つ利用目的を変更する場合に改めて個人情報主体の明確な同意を取得するものとされている。また、公開開示も原則的に禁止され、法律に基づいて又は合理的な事由があり公開開示する必要がある場合、個人情報セキュリティ影響評価を行い、個人情報主体に公開開示の目的と類型を告知し、個人センシティブ情報の公開開示前に係る個人センシティブ情報の内容を告知し、バイオメトリクス情報を公開開示してはいけない。なお、第 8.6 条は、プラットフォームと電子商取引のベンダーのような共同個人情報支配者に対して、契約等の方法で個人情報セキュリティに関するそれぞれの責任義務を明確にし、個人情報主体に明確に告知すると義務づけている。

第 9 条「個人情報セキュリティ事件処理」は、セキュリティ事件応急処置と報告、及びセキュリティ事件告知（詳細は、第 3.9. 2.5 を参考。）を定めている。個人情報取扱者は、個人情報セキュリティ事件応急プランを作成し、定期的に（少なくとも年一回）内部関連人員を組織し応急対応研修と訓練を行い、個人情報セキュリティ事件の発生後に事件内容を記録し影響評価を行い、事態コントロール措置を講じリスクを排除し国家インターネットセキュリティ事件応急プランに基づいて直ちに報告するものとされている。

最後、第 10 条「組織的管理要求」は、個人情報取扱者に対して、責任部署と人員を明確にし、個人情報セキュリティ影響評価を行い、データセキュリティ能力を整備し、人員管理と研修を実施し、セキュリティ監査を行うと各種要求を定めている。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務に関する規定

今までの法令では、漏えい等事案発生時の監督機関への報告義務に関する規定は多いが¹⁴、本人への報告義務について、個人情報セキュリティ規範は、初めて個人情報取扱者に対して比較的明確な義務を定めている。第 9.2 条「セキュリティ事件告知」によると、個人情報取扱者は、直ちに事件の関連状況をメール、手紙、電話、通知の送付等の方法で影響される個人情報主体に告知し、個別の告知が難しい場合に合理・有効的な方法で公衆に関連する警告情報を公布し、且つ告知内容として、①セキュリティ事件の内容及び影響、②講じた又はこれから講じる処理措置、③個人情報主体に対してリスク防犯と削減に関するアドバイス、④個人情報主体に対して提供する救済措置、⑤個人情報保護責任者と個人情報保護専門機構の連絡方法は含まれるが、それらに限られない。

第 9.1 条 c)3) は、個人情報支配者による当局への報告義務も定めている。すなわち、国家インターネットセキュリティ事件応急プランの関連規定に従い直ちに報告し、報告内容として、個人情報主体の類型、数量、内容、性質等の全体状況、事件がもたらし得る影響、講じた又はこれから講じる処理措置、事件処理関連人員の連絡方法は含まれるが、それらに限られない。

オ 安全管理措置に関する規定

第 10 条「組織的管理要求」は、組織的措置を定めている。

第 10.1 条によると、個人情報取扱者は、その代表者が個人情報セキュリティに対して全面的なリーダー責任（個人情報セキュリティ作業のために人材、財力、物資を確保することを含む）を負うことを明確にし、個人情報保護責任者と個人情報保護部署を任命するものとされている。

個人情報保護責任者と部署の責任は、下記の通りである。

- (ア) 組織内の個人情報セキュリティ作業を全面統括し実施、個人情報セキュリティに対して直接責任を負うこと。
- (イ) プライバシーポリシー及び関連規定の制定、公布、実施、定期的な更新。
- (ウ) 組織により保有される個人情報リスト（個人情報の類型、数量、出所、受取者等を含む）及び訪問許可制度の構築、維持と更新。
- (エ) 個人情報セキュリティ影響評価の実施。

¹⁴ 公共インターネットサイバーセキュリティ突発事件応急予備方案（工業・情報化部網安[2017]281号、2017年11月14日公布・施行）は、本人及び監督機関等への報告義務について、電気通信事業者及びインターネット情報サービス提供者が、インターネット上で大量の個人情報漏えい事件が発生した場合、サイバーセキュリティ突発事件に該当し、緊急予備方案に従うことになる。10万以上のインターネット利用者情報漏えいは一般事件、100万以上は比較的大きい事件、1000万以上は重大事件、1億以上は特別重大事件として、事件発生の事業者は、直ちに当局へ報告するとともに、自社の緊急予備方案を起動し、応急処置を行い、利用者と社会への影響を低減するよう努める義務を負う旨定めている。

(オ)個人情報セキュリティ研修実施の組織

(カ)製品又はサービスの導入・リリース前に検測を行い、未知の個人情報収集・利用・提供等の処理行為を避けること。

(キ)セキュリティ監査の実施

さらに、個人情報セキュリティ影響評価の実施に関して、定期的に行い（少なくとも年1回）、主に処理活動において個人情報セキュリティ基本原則への遵守状況、個人情報処理活動による個人情報主体の適法権益への影響について評価するとされている。また、所定場合によって、個人情報セキュリティ影響評価を改めて実施し、評価報告書を作成し、それに基づいて個人情報主体の保護措置を講じリスクを受入可能な水準までに低減し、評価報告書を適宜に保管し適宜な方法で对外公開するとされている。

人員管理と研修に関して、個人情報取扱者は、下記を要求されている。

(ア)個人情報処理に従事する人員と秘密保持契約書を締結し、大量的に個人センシティブ情報にアクセスする人員に対して背景調査を行うこと。

(イ)内部で個人情報処理に係る異なる職位のセキュリティ職責、及びセキュリティ事件の発生時の処罰体制を明確にすること。

(ウ)個人情報処理職位の人員に対して職位転換又は労働契約終了の際にも守秘義務の継続履行を要求すること。

(エ)個人情報へアクセスする可能性のある外部人員が遵守すべき個人情報セキュリティ要求を明確にし、秘密保持契約書を締結し監督すること。

(オ)定期的に（少なくとも年1回）又はプライバシーポリシーにおいて重大な変更が生じた場合、個人情報処理職位の人員に対して個人情報セキュリティ専門家研修及び評価を行い、それらの人員がプライバシーポリシーと関連規程を熟知することを確保すること。

セキュリティ監査に関して、個人情報取扱者は、下記を要求されている。

(ア)プライバシーポリシーと関連規程及びセキュリティ措置の有効性に対して監査すること。

(イ)自動監査システムを構築し、個人情報処理活動をモニタリングし記録すること。

(ウ)監査プロセスにおいて作成された記録は、セキュリティ事件の処置、応急対応及び事後調査に資すること。

(エ)監査記録への無断アクセス、改ざん又は削除を防止すること

(オ)監査プロセスにおいて発見された個人情報の違法利用、濫用等の状況を直ちに処理すること。

カ 適用範囲

個人情報セキュリティ規範は、各種組織の個人情報処理活動への規範に適用し、監督当局又は第三者評価機構等の組織が個人情報処理活動に対する監督、管理及び評価にも適用する（第1条）。

キ 小規模事業者の取扱い

中国現在の関連法令には、小規模事業者の取扱いに関する規定は見あたらないが、第10.1条は、①主業が個人情報処理にかかり、且つ従業員が200人以上、又は②50万人を超える個人情報を処理し、又は12カ月以内に50万人の個人情報の処理を予測される組織に対して、専任の個人情報保護責任者と個人情報保護機関を設置することを義務付けている。

③ 電気通信及びインターネット利用者の個人情報保護に関する規定

ア 法律の概要

電気通信及びインターネット利用者の合法的権益を保護し、インターネット情報セキュリティを維持することを目的とする。

イ 個人情報の定義

「個人情報」とは、電気通信事業者及びインターネット情報サービス提供者がサービスを提供する過程において収集した利用者氏名、生年月日、身分証明書番号、住所、電話番号、ユーザー名及び暗証番号等単独的又はほかの情報と合わせると利用者を識別できる情報、及び利用者のサービス利用時間、場所等情報をいう（第4条）

ウ 漏えい等事案発生時の本人及び監督機関等への報告義務

第14条によれば、電気通信事業者及びインターネット情報サービス提供者により保管される利用者個人情報に関して漏えい・毀損・紛失が発生した又は発生する恐れがある場合、直ちに救済措置を講じ、重大な結果を生じた又は生じる恐れがある場合、直ちに所管の電信管理機構に報告し、関連部門が行う調査と処理に協力するとされている。

エ 安全管理措置に関する規定

電気通信事業者及びインターネット情報サービス提供者は、利用者の個人情報漏えい、毀損、改ざん又は紛失を防ぐために以下の措置を講じるものとする（第13条）。

- (ア)各部門、部署及び支店の利用者個人情報の安全管理責任を確定すること。
- (イ)利用者個人情報の収集、使用及びその関連活動の業務手順及び安全管理制度を構築すること。
- (ウ)職員及び代理人に対して権限管理を実行し、情報の大量エクスポート、複製、廃棄について審査を行い、かつ秘密漏えい防止措置を講じること。
- (エ)利用者個人情報を記録した紙媒体、光媒体、電磁的媒体等の媒体を適切に保管し、かつ相応の案件保存措置を講じること。
- (オ)利用者個人情報を保存する情報システムについてアクセス審査を行い、かつ侵入防止、ウィルス防止等の措置を講じること。
- (カ)利用者個人情報についてオペレーションを行った人員、時間、場所、内容等の情報を記録すること。
- (キ)電気通信監理機構の規定に従い通信ネットワーク安全防護業務を行うこと。
- (ク)その他の電気通信監理機構が定める必要な措置を講じること。

なお、従業員に対して利用者個人情報保護に関する知識、技能及び安全責任のトレーニングを行い、利用者個人情報保護の状況について少なくとも年1回に自ら検査を行い、検査で見つかった安全リスクを排除するものとする（第15条、第16条）。

（3） 監督機関・第三者機関

① 設置の経緯

個人情報保護に関する監督機関は統一・整理されておらず、中国において個人情報の法令執行・摘発・保護の専門行政部署はまだできていない。現在の法令執行は、公安機関・検察院・人民法院による不定期の個人情報侵害犯罪の摘発キャンペーンに頼るのが現状である。行政当局については、CACが、サイバーセキュリティ業務及び関連監督管理作業の統括調整を担当する主たる監督機関であり、工業・情報化部と公安部及びその他の部門は、それぞれの職責範囲内で担当する（CS法第8条）ことにより、インターネットにおける個人情報の保護を限定して監督機能を担っている。

CACは、2011年5月4日に国務院がインターネットに関して多部門管理の状態を整理するために、国務院新聞弁公室に設立し（但し、行政レベルで部（注：我が国でいうところの「省」）レベルに該当する）、インターネット情報伝送方針政策の推進とインターネット情報伝送法制度の整備、関連部門によるインターネット情報の内容管理への指導・調整・催促、法律に基づいて違法・不正なウェブサイトの取り締まりという役割を位置づけられ

た¹⁵。CAC は、組織再編を経て、2014 年 8 月 26 日、「インターネットコンテンツ管理作業を CAC への授権に関する国務院通達」（中国語は「国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知」。国発[2014]33 号）¹⁶に基づいて全国のインターネットコンテンツ管理作業を担当し、且つ法律執行への監督管理も担当し始め、公安部の一部の権限を譲渡された。CAC の内部組織構成は、公式な資料はないが、2014 年 10 月の CAC 募集情報によると、インターネット評論局、インターネット社会工作局、移動インターネット管理局、インターネット安全協調局、国際合作局を設置していると考えられる。

パソコン情報システム安全保護条例第 6 条によると、公安部は全国パソコン情報システム安全保護作業を主管し、及び情報安全等級管理弁法 3 条によると、公安部は情報安全等級保護作業の監督、検査、指導を担当する。公安部において、直接の担当部署は、従来に公安機関公共情報インターネット安全監察部門であったが、2010 年からインターネットセキュリティ保衛局（中国語は「网络安全保卫局」）に改名した（いわゆる、インターネット警察）。

電信条例第 3 条とインターネット情報サービス管理規定第 18 条は、電信主管部門、すなわち工業情報化部が電気通信事業とインターネット情報サービスの主管当局として定めている。工業情報化部において、直接の担当部署は、通信保障局であったが、2015 年にインターネット安全管理局（中国語は「网络安全管理局」）に改名し、下には総合処、情報安全処、インターネット・データ安全処、重要通信処が設置されている。¹⁷

1983 年に設立された全国情報安全標準化技術委員会は、現在、国家標準化管理委員会の指導を受けるが、業務上、CAC の指導も受ける。同委員会は、個人情報保護を含むインターネット安全関連の国家基準を数多く制定している。それらの基準は、立法とは言えず、推奨的な基準も多いが、当局又は社会的な共通認識を反映している。特に最近公布された「個人情報セキュリティ規範」は国内外の概念と制度を集大成しているといわれる。

② 制度の概要

CAC の設立当初は、国務院新聞弁公室の責任者（中国語は「主任」、閣僚級）が CAC の責任者を兼務し、公安部副部長と工業情報化部副部長はそれぞれ CAC の副責任者を兼務していたが、2014 年に組織再編とインターネットコンテンツ管理の授権の取得後は、積極的に規

¹⁵ 国家インターネット情報弁公室の設立に関する公的な報道：

<http://www.scio.gov.cn/zhzc/8/5/Document/1335496/1335496.htm>

¹⁶ 中国語原文：http://www.cac.gov.cn/2014-08/28/c_1112264158.htm

¹⁷ 工業情報化部主要職責の内設機構と人員編制規定：

<http://www.miit.gov.cn/n1146285/c3722500/content.html>。インターネット安全管理局ホームページ：
<http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057725/c3635780/content.html>

則制定や法令執行を推進し始め、CS 法可決以降は加速的に、前述(1)②ウのインターネットセキュリティに関する数多くの実施規定と国家基準の制定を推進している。

③ 運用実態

2017年、CACは、ウェブサイトを経営する事業者(2,003社)に事情聴取(指導)するとともに、1,370社のウェブサイト更新を停止し、22,587社の違法ウェブサイトライセンス又は届出の取り消し及び閉鎖を行った¹⁸。CACは、2016年1月15日に、中国IT大手の百度(Baidu)の責任者を事情聴取し個人情報漏えいを含める違法行為を指摘した。

工業情報化部インターネット安全管理局は、2018年1月に、百度(Baidu)、アリババ傘下の金融子会社アリペイ(アントフィナンシャル)及び今日頭条など人気移動端末ニュースアプリの運営会社の責任者を事情聴取し、CS法と電気通信及びインターネット利用者の個人情報保護に関する規定への遵守に関して、これら三社における利用者個人情報収集利用規則、利用目的の告知が不十分だと指摘し、利用者の知る権利及び選択権利を保護する原則に基づいて是正するよう命令した¹⁹。

2017年7月―9月に、CAC、工業産業化部、公安部、国家標準化管理委員会は、合同でプライバシーポリシー審査キャンペーン業務を展開し、中国の代表的なインターネット製品・サービスであるとして、Wechat、Sinaブログ、京東商城、Baidu地図、航旅縦横、Ctripに対して、より厳しいプライバシーポリシーの制定と適用を指導した。

公安部は、直近2年間、公民個人情報への電信インターネット詐欺犯罪を取り締まり、個人情報侵害犯罪の案件3,700件以上を摘発し、犯罪疑者11,000名以上を逮捕し、全国法院は、2014年から2017年8月までにインターネットを通じた個人情報侵害犯罪案件1,529件を審理したといわれる²⁰。2017年6月に、公安局は、データの違法取引への取締りをはじめ、業界内の代表的なビッグデータ会社を含む30社以上を調査して、個人情報の収集・利用におけるコンプライアンスを審査していた。

(4) 近時のトピック

① 制度改正の検討状況

¹⁸ CAC2017年全国法律行政執行作業報告：
http://www.cac.gov.cn/2018-02/05/c_1122368756.htm

¹⁹ 下記の記事を参考にした。
<http://news.163.com/shuangchuang/18/0112/11/D7US54IH000197V8.html>

²⁰ 2017年12月24日付で中国全国人民代表大会常務委員会法律執行検査チームの「CS法」と「全国人民代表大会常務委員会のインターネット情報保護強化に関する決定」の実施状況への検査報告書：http://www.npc.gov.cn/npc/xinwen/2017-12/24/content_2034836.htm

個人情報保護法の制定に対する社会からのニーズはなお高いが、2003年から立法作業が始まったものの、個人情報保護法の制定見通し不明である。

一方、個人情報への侵害事件は頻発し、社会に大きな衝撃を与える事件も多いため、CS法の実施を通じて立法機関である全国人民代表大会常務委員会と行政機関であるCAC・公安部及びNGO組織である消費者権益保護委員会は、社会の安定のため、個人情報の保護を重視する姿勢を示し、部門や地域横断的な合同調査・摘発キャンペーンを行っている。キャンペーン対象は、著名インターネット企業とどまらず、大学や地方政府当局ウェブサイト等の非営利主体も含まれている。

全国人民代表大会常務委員会は、2017年8月から10月にSCの実施状況に関する検査を行い、2017年12月24日に実施状況検査報告書（中国語は「全国人民代表大会常務委員会執法检查组关于检查《中华人民共和国网络安全法》《全国人民代表大会常務委員会关于加强网络信息保护的決定》实施情况的报告」）²¹を公開した。また、各地方の消費者権益保護委員会は、インターネット運営者の個人情報の保護についてインタビュー調査を行い、個人情報への侵害嫌疑で大手インターネット企業に対する公益訴訟を提起したこともある。

② 個人情報に関連した政策動向

現在、CS法の実施規則や関連基準等の整備は進行中であり、個人情報の越境移転規則、個人情報保護国家基準、個人情報匿名化等一連の国家基準を作成中である。行政摘発司法民事保護及び個人情報侵害罪の摘発は強化しつつあり、個人情報保護の関連事例の公開も進みつつある。

③ 個人情報に関連した主要な裁判例

最高人民法院と最高人民検察院は、個人情報侵害の刑事案件に関する司法解釈を2017年5月8日に公布し2017年、個人情報侵害罪に関する典型的な判例を合計で13件公布した²²。

個人情報侵害行為への責任追及に関して、プライバシー権侵害を参考適用する従来の司法保護から、直接、個人情報権利に基づいて救済した事例も増えている。外国人による個人情報の違法取得に関する刑事裁判例も出ている²³。

上記の司法解釈は、個人情報保護強化の姿勢を示し、刑法第253条（個人情報侵害罪）

²¹ http://www.npc.gov.cn/npc/xinwen/2017-12/24/content_2034836.htm

²² 関連内容の中国語全文：司法解釈：

<http://www.court.gov.cn/fabu-xiangqing-43942.html>。

判例：http://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170516_190645_3.shtml。

²³ 2014年に、上海第一中級人民法院はイギリス国籍人とアメリカ国籍人に対して個人情報の違法取得のために刑事責任を追及した。

http://epaper.bjnews.com.cn/html/2014-08/09/content_528548.htm?div=-1

について犯罪認定しやすい基準を定めている。例えば、刑事責任追及に必要となる個人情報の違法取得・販売・提供の情状について、①行き先情報を販売又は提供し、他人により犯罪活動において利用された場合、②他人が個人情報を利用し、犯罪を実施することを知らずながら販売又は提供した場合、③行き先情報・通信内容・信用情報・財産情報 50 件以上を違法取得・販売・提供した場合、④宿泊情報・通信記録・健康生理情報・取引情報等人身・財産安全に影響し得る個人情報 500 件以上を違法取得・販売・提供した場合、⑤③と④以外の個人情報 5,000 件以上を違法取得・販売・提供した場合、⑥数量が③ないし⑤の基準に達しないが関連比率合計で関連数量基準に達した場合、⑦違法所得が 5,000 人民元以上であった場合、⑧職務履行又はサービス提供過程において取得した個人情報を他人に販売又は提供し、数量又は金額が③ないし⑦における基準の半分以上に達した場合等のいずれも回答するとされている。

また、判決までに至っていないが、最近に注目された訴訟案件として、江蘇省消費者權益保護委員会は、中国 IT 会社 3 強企業である百度 (Baidu) 公司に対して提起した公益訴訟がある。すなわち、同委員会は、同社の二つのアプリが消費者の個人情報を違法取得している疑いでヒアリングしても、同社が積極的に対応していなかったため、2017 年 12 月 11 日に南京市中級人民法院に起訴し、民事公益訴訟として 2018 年 1 月 2 日に正式に立件された。立件を受けて同社は、同委員会と真剣にコミュニケーションを取り、消費者の情報セキュリティを確実に保証するために改善するとしてことを受け、同委員会は 2018 年 3 月 12 日に起訴を取り下げた²⁴。今後は、消費者組織が公益訴訟を通じて事業者の個人情報取扱コンプライアンスを監督する事件も増えると予測される。

²⁴ 案件経緯の詳細は、下記ウェブサイト記事を参考にした。
http://aic.jiangsu.gov.cn/art/2018/3/14/art_59555_7520812.html

6. 韓国

(1) 制度概要

① 法体系の概要

ア 個人情報保護制度の概要、法体系

韓国では、個人情報保護に関連して様々な法律を定めており、その内、個人情報保護法（法律第 14839 号）（개인정보 보호법）、情報通信網利用促進及び情報保護等についての法律（法律第 14839 号）（정보통신망이용촉진 및 정보보호등에 관한 법률）（以下「情報通信網法」という。）、信用情報の利用及び保護に関する法律（法律第 14823 号）（신용정보의 이용 및 보호에 관한 법）（以下「信用情報法」という。）が代表的な法律に該当する。

個人情報保護法は個人情報の保護に関する一般法であり、業務目的にて個人情報を扱う公共機関、法人、個人等全ての者について適用される。特別法である情報通信網法は情報通信サービス提供者（e. g. オンラインサービス）がそのサービス利用者の個人情報を処理することに関して、信用情報法は金融取引等、商取引において扱われる個人信用情報について規定している。

個人情報の保護に関し、個人情報保護法、情報通信網法、信用情報法の基本的な構造は類似しており、すなわち、個人（信用）情報の収集、利用、第三者への提供、処理の委託、破棄等、個人（信用）情報の処理全般について規定し、原則として情報主体の事前同意を個人（信用）情報の処理の要件として定め、一部において事前同意の例外事由を定めているのが特徴である。更に個人（信用）情報の流出、個人情報保護のために行うべき対応処置についても規定している。

一方で、（個人）位置情報の取扱い全般並びに管理及び技術的な保護措置については位置情報の保護及び利用などに関する法律（法律第 14840 号）（위치정보의 보호 및 이용 등에 관한 법률）（以下「位置情報法」という。）において別途規律している。位置情報法は位置情報を収集し、位置情報を利用したサービス事業を行う者に対して同情報を提供することを事業とする位置情報事業についての許可（第 5 条）や、位置情報を利用したサービスを提供することを事業としている位置基盤サービス事業についての届出（第 9 条）を規定しているのが特徴である。

イ 法体系・分野ごとの規制の概要

上記のとおり、個人情報保護法は、業務目的として、個人情報を処理する公共機関、企業、団体及び個人（いわゆる「個人情報処理者（개인정보처리자）」）に口して、適用され

る。つまり、個人情報保護法は公共部門と民間部門の区別をせずに適用される一般法的な性格を有している。そのため、他の法律に特別な規定がある場合には、当該法律が個人情報保護法に優先して適用される。これは該当分野の特殊性を考慮したものである。

実際に、情報通信網法、信用情報法、位置情報法等多数の個別法が個人情報の処理及び保護に関する規定を置いており、当該規定は個人情報保護法に関する特別法として原則的に個人情報保護法に優先して適用される。

具体的には、情報通信網法は、情報通信サービス提供者（e.g. オンラインサービス提供者）と利用者の関係において、法に特別な規定がある場合に優先的に適用され、信用情報法は信用情報会社等と信用情報主体との関係において法に特別な規定がある場合に優先的に適用される。また、位置情報法は個人位置情報の取扱いに関して優先適用される。

② 民間部門・公的部門の区別

個人情報保護法上の「個人情報処理者」の概念には、上記の通り「公共機関、法人、団体又は個人など」が含まれている（同法第2条第5号）。個人情報保護法は公共機関などが属している公的部門と、法人、団体、個人等が属している民間部門とを区別しておらず、同一の法律によって同一の個人情報保護原則を適用する単一法主義を採用しているものといえる。上記公共機関の概念には、国会、裁判所、憲法裁判所、中央行政機関及びその所属機関、地方公共団体などが含まれる（同法第2条第6号）。法の適用対象及び義務の主体は「個人情報処理者」であるが、「個人情報処理者」が公共機関である場合については、下表のとおり、他の個人情報処理者に比べ義務が加重される規定及び義務が緩和される規定がある。

公共機関について義務を加重している条項	公共機関について義務を緩和している条項
<ul style="list-style-type: none"> ・ 公共機関は、個人情報処理者が例外的に個人情報を目的外に利用したり、第三者に提供できる場合の内、情報主体から別途の同意を得た場合又は犯罪の捜査及び公訴提起のための場合を除いたすべての場合において（同法第18条第2項第1号から第6号ないし第8号及び第9号）、その利用及び提供の法的根拠、目的及び範囲等についての必要事項を官報又はインターネットホームページ等に掲載しなければならない（同法第18条第4項）。 	<ul style="list-style-type: none"> ・ 公共機関が法令等で定める所轄業務を行うために不可欠な場合、個人情報を収集することができ、かつその収集目的の範囲内で利用することができる（同法第15条第1項第3号）。 ・ 公共機関は、個人情報を目的外の用途で利用し、又は第三者に提供しなければ、他の法律で定める所轄業務を行うことができない場合として保護委員会の審議、議決を経た場合、条約そのほかの国際協定の履行のために外国政府又は国際機構

<ul style="list-style-type: none"> 公共機関の長が、例外的に公共の場で映像情報処理機器の設置、運営が許される場合（同法第 25 条 1 項各号）にこれを行う時は、公聴会、説明会を開催するなど、各関係専門家及び利害関係人の意見を受領しなければならない（同法第 25 条第 3 項）。 公共機関が映像情報処理機器の設置、運営について業務委託をする場合には、大統領令において定める手続及び要件に従わなければならない（同法第 25 条第 8 項）。 公共機関の長が、個人情報ファイルを運用する場合には、①当該ファイルの名称、②当該ファイルの運用根拠及び目的、③当該ファイルに記録される個人情報の項目、④個人情報の処理方法、⑤個人情報の保有期間、⑥個人情報を反復又は継続的に提供する場合にはその提供を受ける者、⑦その他大統領令で定める事項について、行政安全部長官に登録しなければならない。登録事項が変更される場合にも同じである（同法第 32 条）。 公共機関の長は大統領令で定める基準に該当する個人情報ファイルの運用により情報主体の個人情報が害される恐れがある場合には、その危険要因の分析と改善のためのアセスメントを行いその結果を行政安全部長官に提出しなければならない（同法第 33 条）。 情報主体が公共機関に対して自身の個人情報についての閲覧を請求する場合は、公共機関に直接閲覧を請求するか、又は 	<ul style="list-style-type: none"> に提供するために必要な場合、犯罪の捜査や公訴提起及び維持のために必要な場合、裁判所の裁判業務の遂行のために必要な場合、刑罰及び監護保護処分の執行のために必要な場合（同法第 18 条第 2 項第 5 号から第 9 号）、個人情報の目的外利用及び第三者への提供ができる（同法第 18 条第 2 項但書）。 個人情報処理者は個人情報処理方針を定めなければならないところ、公共機関は、第 32 条に基づき登録対象となる個人情報ファイルについて個人情報処理方針を定めれば足りる（同法第 30 条第 1 項）。 公共機関は、租税の賦課徴収又は還付に関する業務、各教育施設での成績評価及び入学者選抜に関する業務、学歴技能及び採用に関する試験及び資格審査に関する業務、保証金及び給付金算定等について進行中の評価及び判断に関する業務、及びその他の法律に基づき進行中の監査及び調査に関する業務を遂行するとき、各業務に重大な支障が生じる恐れがある場合には、情報主体にその旨を告げて個人情報の閲覧を制限又は拒絶することができる（同法第 35 条第 4 項第 3 号）。 公共機関が、個人情報を処理しなければ、その他法律で定める所轄業務を遂行できない場合、情報主体から自己の個人情報処理の停止請求があつたとしてもこれを拒絶することができる（同法第 37 条第 2 項第 3 号）。 公共機関が処理する個人情報の内、統計
---	--

<p>大統領令に定めに従って行政安全部長官を通じて閲覧を請求することで、自身の個人情報の閲覧ができる（同法第 35 条第 2 項）。</p>	<p>法（法律第 14843 号）（통계법）に基づき処理された個人情報に対しては、個人情報保護法の第 3 章から第 7 章（条文番号では第 15 条から第 57 条。なお、それぞれの章題は、第 3 章「個人情報の処理」、第 4 章「個人情報の安全な管理」、第 5 章「情報主体の権利保障」、第 6 章「個人情報紛争調停委員会」、第 7 章「個人情報団体訴訟」である。）は適用されない（同法第 58 条第 1 項第 1 号）。</p>
--	--

一方で、個人情報保護法以外の特別法は、営利を目的とする情報通信サービス提供者（情報通信網法）、信用情報会社、金融取引など商取引関係にある信用情報提供・利用者（信用情報法）、位置情報事業者、位置基準サービス事業者（位置情報法）などを適用対象として明示しているため、法人、団体、個人等が属している民間部門を主な適用対象としている。

③ 法律及び条令の存在

韓国は、個人情報の保護に関して、一般的に法律、施行令、施行規則及び行政規則を使用して規律している。いくつかの地方自治体では、地方自治団体所属の行政機関、条例で設立された公企業及び政府出捐機関に適用される個人情報保護条例、個人映像情報の保護及び映像情報処理機器設置・運営条例等を制定して運用している。

（２） 主な法律の概要

① 個人情報保護法

ア 法律の概要

個人情報保護法は 2011 年 3 月 29 日に制定され、2011 年 9 月 30 日に施行された。その後計 14 回の改正を経ており、2017 年 7 月 26 日に改正された法第 14839 号が 2017 年 10 月 19 日から施行されている。

近時の主要な改正内容は以下の通りである。

- ・ 2015 年 7 月 24 日に一部改正され、2016 年 7 月 25 日に施行された個人情報保護法
個人情報保護委員会の機能を強化（政策・制度の改善勧告権及び履行の点検、資料提

出請求権、個人情報紛争調整委員の選任権付与等)、懲罰的損害賠償及び法定損害賠償制度の導入(第39条第3項、第4項及び第39条の2)等。

- 2016年3月29日に一部改正され、2016年9月30日に施行された個人情報保護法
一定の基準に該当する個人情報処理者が情報主体以外から個人情報を収集して処理する場合、収集の出所等について、告示をすべき義務を新設(第20条第2項から第4項)、敏感情報(민감정보)¹に対する安全性確保のために必要な措置の新設(第23条第2項)、行政安全府の長官による一定の基準に該当する個人情報処理者に対する固有識別情報処理時の安全性確保に必要な措置の履行についての定期的な調査(第24条第4項及び第5項)等。
- 2017年4月18日に一部改正され、2017年10月19日に施行された個人情報保護法
個人情報処理者が書面等で情報主体からの同意を得る際に、情報の収集・利用目的、収集・利用しようとする個人情報の項目等、大統領令で定める重要な内容を行政自治府令で定める方法によって明確に表示し分かりやすくするための規定を新設(第22条第2項)。

イ 目的規定の有無、その内容

個人情報保護法は、個人情報の処理及び保護に関する事項を定めることにより、個人の自由と権利を保護し、さらに個人の尊厳と価値を守ることを目的とする(法第1条)。

ウ 個人情報の定義

個人情報保護法において定める、「個人情報」とは、生存する個人に関する情報であつて、氏名、住民登録番号(韓国における個人識別番号)、又は映像などを通じて個人を認識可能な情報を意味し、また、たとえその情報だけでは特定の個人を認識することができなくても、他の情報と照合することにより容易に個人を認識できる情報も含む概念である(法第2条第1号)。

そして「敏感情報」とは、思想・信条、労働組合・政党の登録・退会などの政治的見解、健康、性生活等に関する情報、その他の情報主体のプライバシーを著しく侵害するおそれがある個人情報を意味する(法第23条)。

¹ いわゆるセンシティブデータに相当する。以下同じ。

エ 主な規制・権利の内容

個人情報保護法は、個人情報の収集・利用（第 15 条）、第三者提供（第 17 条）、目的外利用・提供の制限（第 18 条）、情報主体以外の第三者から収集した個人情報の収集先の通知（第 20 条）、個人情報の破棄（第 21 条）、同意を得る方法（第 22 条）、敏感情報、固有識別情報、住民登録番号の処理の制限（第 23 条から第 24 条の 2）、映像情報処理機器の設置・運営制限（第 25 条）、個人情報の処理委託（第 26 条）等、個人情報の処理全般に関する事項を規律している。

また、個人情報の流出についての通知（第 34 条）、個人情報の紛失・盗難・漏えい・偽造・変造又は毀損を防止するための技術的・管理的及び物理的保護措置（第 29 条）についても規定している。

一方、個人情報保護法は、情報主体の権利に関して、個人情報の閲覧（第 35 条）、個人情報の訂正・削除（第 36 条）、個人情報の処理の停止（第 37 条）を規定している。そして個人情報処理者が個人情報保護法の違反行為により情報主体に損害を与えた場合における損害賠償責任（第 39 条第 1 項）、個人情報処理者の故意又は重過失に起因して個人情報の紛失・盗難・漏えい・偽造・変造又は毀損が生じ、情報主体に損害が発生した時には、裁判所がその損害額の 3 倍を超えない範囲で損害賠償額を定めることができるという懲罰的損害賠償責任（第 39 条第 3 項）、個人情報処理者の故意あるいは過失によって、個人情報の紛失・盗難・漏えい・偽造・変造又は毀損が生じた場合に 300 万ウォン以下の範囲で相当な金額を損害額として賠償請求できるという法定損害賠償責任（第 39 条の 2）を規定している。

オ 漏えい等事案発生時の本人及び監督機関等への報告義務

個人情報処理者は、個人情報が流出したことを知った時は、遅滞なく当該情報主体に対し、(i) 流出した個人情報の項目、(ii) 流出した時期とその経緯、(iii) 流出により発生し得る被害を最小化するために情報主体が行うことができる対応等についての情報、(iv) 個人情報処理者の対応措置及び被害救済手続、(v) 情報主体に被害が発生した場合、被害申告を受け付けることができる担当課及び連絡先、等を伝えなければならない（第 34 条第 1 項）。

1 千人以上の情報主体の個人情報が流出した場合、個人情報処理者は、上記に述べた情報主体に対する通知及び被害を最小化するための対策と必要な措置を履行した結果を遅滞なく行政安全部長官又は韓国インターネット振興院に申告しなければならない（法第 34 条第 3 項、同法施行令第 39 条）。

カ 安全管理措置

個人情報処理者は、個人情報が紛失・盗難・漏えい・偽造・変造又は毀損しないように、内部管理計画の樹立、個人情報へのアクセス記録の保管など安全性確保に必要な技術的・管理的及び物理的措置をしなければならない（法第 29 条、同法施行令第 30 条）。

上記の規定などの委任を受けて制定された行政安全部告示「個人情報の安全性確保の措置の基準」（告示第 2016-35 号）(개인정보의 안전성 확보조치 기준) は技術的・管理的及び物理的安全措置に関する最低限の基準として、①個人情報の安全な処理に向けた内部管理計画の策定・施行（第 4 条）、②個人情報処理システムに対するアクセス権限の管理（第 5 条）、③個人情報に対するアクセス制限（第 6 条）、④個人情報を安全に保管・送信できる暗号化技術の適用又はこれに相応する措置（第 7 条）、⑤個人情報処理システムへのアクセス記録の保管及び点検（第 8 条）、⑥不正プログラム等防止・修復できる修理ソフトなどのセキュリティプログラムの設置・運営（第 9 条）、⑦管理用端末機に対する安全措置（第 10 条）、⑧個人情報の安全な保管のための保管施設の設立又はロック装置の設置など物理的な安全措置（第 11 条）、⑨火災、洪水などの災害・災難に備えた安全措置（第 12 条）、⑩個人情報の破棄（第 13 条）を規定している。

キ 適用範囲

個人情報の保護に関しては、他の法律に特別な規定がある場合を除き、個人情報保護法に定めるところによる（法第 6 条）。

個人情報保護法は、上記に述べたとおり個人情報保護に関する一般法として全ての個人情報処理者と情報主体の関係において適用される。ただし、情報通信網法に基づく情報通信サービス提供者と情報通信サービス利用者との関係、及び信用情報法による信用情報業者と信用情報主体との関係について各法律に特別な規定があれば、その規定が優先的に適用される。

映像情報処理機器、影響評価、固有識別情報及び敏感情報処理の制限、集団紛争調整制度、権利侵害行為、団体訴訟、情報主体以外から収集した個人情報の収集元の告知等、特別法に規定がなく、個人情報保護法においてのみ規定されている内容については当然のことながら個人情報保護法が適用される。

ク 小規模事業者の取扱い

個人情報保護法に基づく委任に従い制定された「個人情報の安全性確保の措置の基準」は、常時労働者数が 10 人未満で、1 万人未満の情報主体に関する個人情報を保有している「小商工人」については、上記基準上規定された安全措置の一部のみを適用している。

具体的には、上記カで説明した安全措置のうち、①個人情報処理システムに対するアクセス権限の管理（第5条、ただし第2項から第5項まで適用）、②個人情報に対するアクセス制御（第6条、ただし第1項、第3項、第6項及び第7項のみ適用）、③個人情報を安全に保存・送信できる暗号化技術の適用又はこれに相応する措置（第7条、ただし第1項から第5項まで、第7項）、④個人情報処理システムへのアクセス記録の保管及び点検（第8条）、⑤不正プログラム等を防止・修復できるソフトなどのセキュリティプログラムの設置・運営（第9条）、⑥管理用端末機の安全措置（第10条）、⑦個人情報の安全な保管のための保管施設の設立又はロック装置の設置など物理的な安全措置（第11条）、⑧個人情報の破棄（第13条）が適用される（個人情報の安全性確保の措置基準[別表1]）。

ケ 国際的な情報移転に関する規定

個人情報保護法は、個人情報を国外の第三者に提供する場合、(i)「提供を受ける者」、(ii)「提供を受ける者の利用目的」、(iii)「提供する個人情報の項目」、(iv)「提供を受ける者の保有及び利用期間」、(v) 同意を拒否する権利があるという事実及び同意拒否に基づく不利益がある場合にはその不利益の内容を情報主体に知らせ、同意を受けなければならないと規定している（同法第17条第3項）。

② 情報通信網法

ア 法律の概要

情報通信網法は2001年1月16日全面改正され、2001年7月1日から施行されており、その後計42回の改正があり、現在、法律第14839号として2017年7月26日に施行された情報通信網法が適用されている。

近時の主要な改正内容は以下の通りである。

- ・ 2015年12月1日に一部改正されて2016年6月2日に施行された情報通信網法
情報通信サービスを利用しない利用者の個人情報保護のために、情報通信サービスを使用していない利用者の個人情報の破棄義務が発生する期間を1年と明示し、情報セキュリティマネジメントシステム認証の義務対象を、業務のために情報通信網を活用する者として大統領令で定める規模以上である者とし（第29条）、その他に認証審査の信頼性・公正性を確保するために審査業務のみを専門的に遂行する専門機関の指定について定め、認証の義務違反時に科す過怠金を1,000万ウォン以下から3,000万ウォン以

下に引き上げる等、現行制度の運営において生じた一部の不備等を改善・補完した（第47条第2項、第3項、第6項及び第7項など）。

- 2016年3月22日に一部改正され2016年9月23日から施行された情報通信網法
「個人情報保護法」の規定に従って個人情報の「取扱」を「処理」に変更するなど、用語を統一し（第24条の2第3項など）、個人情報処理業務を委託する場合に委託者に対し受託者への教育義務を付与し（第25条第4項）、個人情報取扱業務を委託する場合に書面によらし、受託者は委託者の同意を受けた場合に限り委託を受けた業務を第三者に再委託できること（第25条第6項及び第7項の新設）、個人情報セキュリティの責任者は、個人情報保護に関連してこの法及び他の関係法令の違反事実を知ることになった場合には直ちに改善措置を執らなければならない、必要な時には事業主等に報告しなければならないこと（第27条第4項の新設）、わいせつ物や人の名誉を毀損する等、流通が許されていない不法情報（ 불법정보）の範囲に「法令に違反して、個人情報を取引する内容の情報」を明示的に含める（第44条の7第1項第6号の2の新設）等。
- 2016年3月22日に一部改正され2017年3月23日に施行された情報通信網法
スマートフォンのアプリケーションプログラムの開発者及び開発会社が利用者のスマートフォンへのアクセス権限を必要とする場合、プログラム本来の機能を遂行するにあたって必ず必要な権限とそうではない選択的権限とを区分し、それぞれについて細かい項目とその理由を利用者が明確に認知するように教示した上で、利用者から同意を受けることを義務付けた（第22条の2第1項の新設）。また、かかる開発者及び開発会社が、プログラム本来の機能を遂行するために必ずしも必要ではない選択的アクセス権限に利用者が同意しないという理由で利用者がプログラム自体を利用できないようにすることを禁止した（第22条の2第2項の新設）等。

イ 目的規定の有無、その内容

情報通信網法は、情報通信網の利用を促進するとともに、情報通信サービスを利用する者の個人情報を保護し、情報通信網を健全かつ安全に利用できる環境を造成して国民生活の向上と公共福祉の増進に資することを目的とする（法第1条）。

ウ 個人情報の定義

情報通信網法上「個人情報」とは、生存する個人に関する情報であり、氏名・住民登録番号などにより特定の個人を識別できる符号・文字・音声・音響・映像などの情報（当該

情報だけでは特定の個人を調べることができなくても他の情報と容易に照合して調べられる場合には、その情報を含む)をいう(第2条第1項第6号)。

そして「敏感情報」とは、思想、信念、家族や親戚・姻戚関係、学歴・病歴、その他社会活動の経歴など個人の権利・利益やプライバシーを明確に侵害する恐れがある個人情報の意味する(法第23条第1項)。

エ 主な規制・権利の内容

情報通信網法は個人情報の収集・利用(第22条)、目的外利用制限(第24条)、第三者提供(第24条の2)、個人情報の処理委託(第25条)、同意を受ける方法(第26条の2)、個人情報の破棄(第29条)、敏感情報、住民登録番号処理の制限(第23条第1項、第23条の2)など、個人情報の処理全般に関する事項を規律している。

また、個人情報の流出などの通知・申告(第27条の3)、個人情報の紛失・盗難・漏えい・偽造・変造又は毀損を防止するための技術的・管理的措置(第28条)も規定している。

一方、情報通信網法は、情報主体の権利に関して、個人情報の収集・利用・提供などについての同意撤回権(第30条第1項)、個人情報の閲覧・提供及び訂正要求権(第30条第2項)を規定している。そして情報通信サービス提供者が情報通信網法に違反したことにより、情報主体に損害を与えた場合の損害賠償責任(第32条第1項)、情報通信サービス提供者の故意又は重過失により個人情報が紛失・盗難・漏えい・偽造・変造又は毀損した場合、裁判所がその損害額の3倍を超えない範囲で損害賠償額を定めることができる懲罰的損害賠償責任(第32条第2項)、情報通信サービス提供者が故意又は過失により情報通信網法第4章の規定に違反した場合又は個人情報を紛失・盗難・漏えい・偽造・変造又は毀損した場合、情報主体は300万ウォン以下の範囲で相当な金額を損害額として賠償を請求できる法定損害賠償責任(第32条の2)などを規定している。

オ 漏えい等事案発生時の本人及び監督機関等への報告義務

情報通信サービス提供者は、個人情報の紛失・盗難・流出(以下「流出等」という。)の事実を知ったときは、遅滞なく(i)流出等をした個人情報の項目、(ii)流出等が生じた時期、(iii)利用者に取り得る措置、(iv)情報通信サービス提供者等の対応措置、(v)利用者の相談等を受け付けることができる部署及び連絡先を当該利用者に知らせ、放送通信委員会又は韓国インターネット振興院に申告しなければならない(同法第27条の3第1項)。

ただし、利用者の連絡先を知ることができない等、正当な事由が存在する場合にはインターネット上のホームページにおいて上記5つの事項を30日以上掲示することで通知に代えることができる(同法第27条の3第1項ただし書、同法施行令第14条の2第3項)。

カ 安全管理措置

情報通信サービス提供者は、個人情報を処理する場合、個人情報の紛失・盗難・漏えい・偽造・変造又は毀損を防ぎ、個人情報の安全性を確保するために内部管理計画の樹立・施行、接続記録の偽造・変造防止のための措置等、技術的・管理的措置を行わなければならない（法第 28 条、同法施行令第 15 条）。

上記規定の委任を受け制定された放送通信委員会の告示である「個人情報の技術的・管理的保護措置基準」（告示第 2015-3 号）（개인정보 기술적 관리적 보호조치 기준）は、技術的・管理的保護措置に関する最低限の基準として、①個人情報を安全に処理するための内部管理計画の樹立及び施行（第 3 条）、②個人情報に対する違法な接近を遮断するための遮断システムなど接近統制装置の設置及び運営（第 4 条）、③個人情報処理システムへのアクセス記録の偽造・変造防止に向けた措置（第 5 条）、④個人情報を安全に保存・送信できる暗号化技術などを利用したセキュリティ措置（第 6 条）、⑤修復ソフトの設置・運営など不正プログラムによる侵害防止措置（第 7 条）、⑥個人情報の安全な保管のための保管施設の設立又はロック装置の設置等、物理的な安全措置（第 8 条）、⑦個人情報の読み出し・コピーの際の保護措置（第 9 条）、⑧個人情報の照会、出力等の業務を遂行する過程での個人情報表示制限保護措置（第 10 条）を規定している。

キ 適用範囲

情報通信網利用促進及び情報保護等については、他の法律で特別に規定された場合を除き、情報通信網法が優先的に適用される（法第 5 条）。

上述のとおり、情報通信分野の個人情報保護に関する事項を規定する情報通信網法は個人情報保護法の特別法としての地位を有する。したがって、情報通信サービス提供者等は、情報通信網法に基づく個人情報保護措置を遵守しなければならない。ただし、情報通信網法上に規定はないが、個人情報保護法上にある規定については一般法である個人情報保護法が適用される。

一方、提供されるサービスと商品の種類によっては他の法律に個人情報の保護に関し規定されている可能性がある。つまり、情報通信網法ではなく他の個別法において特別に個人情報に関する事項を規定している場合には、当該別の法律が適用される。例えば、金融取引記録などの信用情報の処理については信用情報法が規定している。すなわち、銀行等の金融機関が情報通信サービスを提供し、信用情報を処理すれば、信用情報法が情報通信網法に対して原則として優先的に適用されることとなる。

ク 小規模事業者の取扱い

情報通信サービス提供者は、利用者の個人情報を保護し、個人情報と関連した利用者の苦情を処理するために個人情報セキュリティの責任者を選定する義務がある（同法第 27 条第 1 項）。

ただし、従業員の数が常時 5 人未満の情報通信サービス提供者（ただし、インターネットで情報通信サービスを提供することを主たる業とする情報通信サービス提供者の場合には、従業員の数常時 5 人未満であり、前年度末から直前 3 ヶ月間の提供している通信サービスの 1 日平均利用者が 1 千人以下である者）の場合においては、個人情報セキュリティの責任者を指定する義務を免除されている（法第 27 条第 1 項ただし書）。

ケ 国際的な情報移転に関する規定

情報通信網法によると、情報通信サービス提供者等は、利用者の個人情報について、この法律に違反する事項を内容とする契約を締結してはならず、利用者の個人情報を国外に提供し、取扱いの委託をし、又は保管する場合は、(i) 移転される個人情報の項目、(ii) 移転先の国、(iii) 移転の日時及び方法、(iv) 移転先の氏名・名称、(v) 移転先の利用目的及び保有・利用期間」を利用者に知らせ、利用者から同意を得なければならない（法第 63 条第 1 項、第 2 項）。ただし、上記の処理の委託・保管が情報通信サービス提供に関する契約を履行し、利用者の利便性の向上等のために必要な場合には、上記の通知事項を個人情報の処理方針に基づいて一般に公開する方法などによって利用者に知らせることにより同意を省略することができる（第 2 項ただし書）。

一方で、情報通信網法に基づいて、個人情報を国外に移転する場合、(i) 個人情報保護のための技術的・管理的対策、(ii) 個人情報の侵害に対する苦情処理及び紛争解決に関する事項等の保護措置をしなければならず、契約締結時、上記の内容を事前に協議し、反映しなければならない（同法第 63 条第 4 項、同法施行令第 67 条第 2 項、第 3 項）。

③ 信用情報法

ア 法律の概要

信用情報法は 1995 年 1 月 5 日に制定され 1995 年 7 月 6 日から施行された。その後計 33 回の改正があり、現在 2017 年 4 月 18 日に一部改正された法律第 14823 号が 2017 年 10 月 19 日施行されている。

近時の主要な改正内容は以下の通りである。

- ・ 2009 年 4 月 1 日に全面改正され、2009 年 10 月 2 日に施行された信用情報法
信用情報会社の業務領域を拡大して、信用情報主体の自己情報統制権を補強して個人

のプライバシー保護を強化して、信用照会会社などに信用情報を保護するための厳格な内部統制の手続きを設けるようにして信用情報の利用、活用についての責任を厳格にし、金融消費者の信頼を高めるなど、現行制度の運営上現れた一部不備な点を改善・補完した。一方で、法文を原則として、ハンゲルで記載し、難しい用語をやさしい用語に変え、長くて複雑な文章は、体系などを整備して簡潔にするなど、国民が法を理解しやすいように整備した。

- 2011年5月19日に一部改正されて2011年8月20日に施行された信用情報法
法律で信用情報を項目別に具体的に定義するものの、細部の内容は大統領令に委任すること（法第2条第1号）、信用情報主体に不利益を与える信用情報は最長5年以内に削除することとし、当該信用情報の具体的な種類や記録保存期間などは大統領令で定めるようにした（法第18条第2項及び第3項）。信用照会事業者に対し、信用情報の利用範囲、利用期間、提供の対象者などを金融委員会に報告するようにした。かかる報告義務に違反した者に対して1千万ウォン以下の過料を賦課することとした（法第22条の2、第52条第3項第4号の2）。改正前の法第32条第5項は、他人の個人情報を第三者に提供しようとする者は信用情報の主体に対して情報提供の事実及び目的を知らせなければならないと規定していたが、改正法ではかかる義務の主体を「提供しようとする者又は提供を受けた者」と定め、信用情報主体の保護のため、信用情報主体に知らせる手段として原則を通知とし、公示を例外とした（法第32条第5項）。
- 2015年3月11日に一部改正されて2015年9月12日又は2016年3月12日に各施行された信用情報法
信用照会業の付随業務を本人認証と信用情報主体の識別確認業務として金融委員会が承認した業務並びに信用評価モデル及びリスク管理モデルの開発及び販売業務に制限（第4条第1項第1号）、信用照会会社の営利目的での兼業を禁止することとし（第11条第2項の新設）、業務停止命令に違反したり、業務停止に該当する行為をした信用情報会社が過去3年以内に業務停止処分を受けた事実がある場合の許認可を取り消すことができるようにした（第14条第1項第5号）。信用情報収集・調査は必要最小限の範囲でなければならず、信用情報収集の際、当該信用情報主体の同意を受けるようにした（第15条）。信用情報処理委託の際、識別情報の暗号化などの保護措置、受託者教育、安全な情報処理に関する事項の委託契約の反映を義務化して、金融委員会が認める場合以外に信用情報処理の再委託を禁止した（第17条第4項から第7項までに新設）、等。

イ 目的規定の有無、その内容

信用情報法は、信用情報業を健全に育成して信用情報の効率的利用と体系的管理を図り、信用情報の誤用・乱用からプライバシーの秘密などを適切に保護することで、健全な信用秩序の確立に貢献することを目的とする（法第1条）。

ウ 個人情報 の定義

信用情報法は、個人情報の定義を明示的に規定していないが、個人信用情報については「信用情報のうち、企業や法人に関する情報を除外した、生存する個人に関する情報として氏名・住民登録番号などを通じて、個人を調べられる情報（当該情報だけでは特定の個人を識別できない場合であっても、他の情報と容易に結合して調べられる情報を含む）をいう」と定義しており、（同法施行令第2条第2項）、實際上、前述の個人情報保護法、情報通信網法上の個人情報の概念と同一視されている。

そして「敏感情報」とは、個人の政治的な思想、宗教的信念、その他、信用情報と関係のないプライバシーに関する情報を意味する（法第16条第1項第3号）。

エ 主な規制・権利の内容

信用情報法は、個人信用情報の収集（第15条）、信用情報の処理委託（第17条）、個人信用情報の保有期間（第20条の2）、個人信用情報の提供・活用（第32条）、個人信用情報の利用（第33条）等、個人信用情報の処理に関する事項を規律している。

また、信用情報の漏えい通知（第39条の2）、信用情報の電算システムに対する第三者の不法アクセス、入力された情報の変更・毀損及び破壊、その他の危険に対する技術的・物理的・管理的及びセキュリティ対策の樹立（第19条）も規定している。

一方、信用情報法は、信用情報主体の権利に関して、個人信用情報の提供・利用の同意の撤回権（第37条）、信用情報の閲覧及び訂正請求権（第38条）、信用照会会社に対して個人信用情報を照会した事実の通知の要請（第38条の2）、個人信用情報の削除要求（第38条の3）などを規定している。そして信用情報会社などその他の信用情報利用者が信用情報法に違反して信用情報主体に損害を与えた場合に対する損害賠償責任（第43条第1項）、信用情報会社などその他の信用情報利用者が故意又は重過失に基づき、信用情報法を違反したことにより、個人信用情報の漏えいや紛失・盗難・漏えい・改ざん及び破壊があり、信用情報主体に損害を与えた場合、その損害額の3倍を超えない範囲で賠償する責任を規定した懲罰的損害賠償責任（第43条第2項）、信用情報会社などその他の信用情報利用者に対し、信用情報法第43条による損害賠償を請求する代わりに、300万ウォン以下の範囲で相当な金額を損害額として賠償を請求できる法定損害賠償責任（第43条の2）を規定している。

オ 漏えい等事案発生時の本人及び監督機関等への報告義務

信用情報会社などは信用情報が業務目的以外に漏えいしたことを知ったときは、遅滞なく、当該信用情報主体に (i) 漏えいした信用情報の項目、(ii) 漏えいした時期とその経緯、(iii) 漏えいにより発生できる被害を最小化するために信用情報主体ができる方法などに関する情報、(iv) 信用情報会社などの対応措置及び被害救済手続、(v) 信用情報主体に被害が発生した場合、申告などを接受することができる担当課室及び連絡先を通知しなければならない (同法第 39 条の 2 第 1 項)。

仮に 1 万人以上の信用情報主体に関する個人信用情報が漏えいした場合、先に言及した信用情報主体に対する通知及び被害を最小化するための対策作成と必要な措置を履行した結果を遅滞なく金融委員会又は金融監督院に申告しなければならない (同法第 39 条の 2 第 3 項、同法施行令第 34 条の 2)。

カ 安全管理措置に関する規定

信用情報会社などは信用情報の電算システムに対する第三者の不法アクセス、入力された情報の変更・毀損及び破壊、その他のリスクに対して技術的・物理的・管理的セキュリティ対策を立て、これを実行しなければならない (法第 19 条、同法施行令第 16 条)。

委員会の規定の委任によって制定された金融委員会告示「信用情報業監督規定」の別表 3 は、信用情報の技術的・物理的・管理的セキュリティ対策の具体的な基準として、①信用情報に第三者が不法にアクセスするのを遮断するための侵入遮断システムなど統制装置の設置・運営に関する事項、②個人信用情報処理システムへのアクセス記録の偽・変造防止、③個人信用情報の暗号化、④個人信用情報処理システム及び個人信用情報処理者が個人信用情報処理に利用する情報処理機器に対する不正プログラム防止のための修復ソフトの設置、⑤個人信用情報処理システムで個人信用情報の出力及びコピーの際の保護措置、⑥信用情報管理の業務遂行、⑦個人信用情報の照会権限の区分、⑧個人信用情報の利用制限、⑨個人信用情報の誤用・乱用に対する独自の制裁基準の準備などを規定している。

キ 適用範囲

信用情報法は「信用情報の利用及び保護に関して他の法律に特別な規定がある場合を除いては信用情報法が定めるところによる」、そして「個人情報の保護に関してこの法に特別な規定がある場合を除いては、個人情報保護法に定めるところによる」と規定している (同法第 3 条の 2)。

したがって、個人信用情報の場合には信用情報法がまずは適用されるが、信用情報法に規定されていない事項は、個人情報保護法が適用される。ただし、信用情報法に規定され

ていない事項のうち、個人情報保護法だけでなく、情報通信網法の適用対象にも該当する場合には（例えば、オンラインサービス事業者の利用者に対する個人情報処理）、個人情報保護法の特別法である情報通信網法が優先的に適用される。

ク 小規模事業者の取扱い

信用情報法上、小規模事業者に関連した規定はない。

ケ 国際的な情報移転に関する規定

信用情報法上、信用情報の国外移転に関連した規定はない。

④ 位置情報法

ア 法律の概要

位置情報法は 2005 年 1 月 27 日に制定され、2005 年 7 月 28 日に施行された。その後計 21 回の改正を通じて、現在、2017 年 7 月 26 日に改正された法律第 14840 号が適用されている。

近時の主要な改正内容は以下の通りである。

- 2014 年 10 月 15 日一部改正され、2014 年 10 月 15 日に施行された位置情報法
禁治産・限定治産制度を廃止し、成年後見や限定後見制度を導入する内容で民法が改正された（法律第 10429 号、2011. 3. 7. 公布、2013. 7. 1. 施行）。これを踏まえ、禁治産者及び準禁治産者を被成年後見人又は被限定後見人と変更するなど、関連規定を整備した。
- 2015 年 2 月 3 日一部改正され、2015 年 8 月 4 日に施行された位置情報法
位置情報産業の活性化に向けて位置情報事業と位置基盤サービス事業の参入規制を緩和して、位置情報事業の許可などに原則許可規制体系を導入し、迅速な緊急救助に向けて緊急救助機関が家族関係登録電算情報を利用できるようにするなど現行制度の運営上に現れた一部不備な点を改善・補完した。
- 2015 年 12 月 1 日一部改正され 2016 年 6 月 2 日に施行された位置情報法
個人の位置情報を不法に利用する事例が増加して社会問題となり、位置情報を収集する位置情報事業者の欠格事由規定が不十分で、補完を必要としていた。また、現行法第

6条では、位置情報事業者の役員についての欠格事由のみを規定していたため、センシティブな個人位置情報にアクセスが可能な位置情報事業者の職員に対する規定が不足していた。しかも、現行法と趣旨及び機能が類似した信用情報法では信用調査会社の欠格の対象を役職員の従事者としてより幅広く規定しているため公平の観点からも問題があった。そこで、位置情報事業者の欠格事由の対象に位置情報アクセス権限者である従業員を追加し、より厳格な統制方を講じた。

イ 目的規定の有無、その内容

位置情報法は位置情報の流出・誤用や乱用からプライバシーの秘密などを保護して位置情報の安全な利用環境を造成して位置情報の利用を活性化することにより、国民生活の向上と公共福祉の増進に資することを目的とする（法第1条）。

ウ 個人情報の定義

位置情報法は個人情報の定義を明示的に規定していないが、個人位置情報に関して、「特定の個人の位置情報（位置情報だけでは特定の個人の位置を知ることができない場合にも他の情報と容易に結合して特定の個人の位置を知ることができるものを含む）をいう」と規定している（法第2条第2号）。

位置情報法は敏感情報に関連した規定はない。

エ 主な規制・権利の内容

位置情報法は位置情報を収集して位置基盤サービス事業をする者に提供することを事業として営む位置情報事業の許可（第5条）、位置情報を利用したサービスを提供することを事業として営む位置基盤サービス事業の申告（第9条）を規定しており、位置情報主体の同意のない位置情報の収集などの禁止（第15条）、位置情報の保護措置（第16条）、位置情報の漏えいなどの禁止（第17条）など位置情報の保護だけでなく、個人位置情報の収集（第18条）、個人位置情報の利用又は提供（第19条）、位置情報事業者による個人位置情報の提供など（同法第20条）、個人位置情報などの利用・提供の制限（第21条）、個人位置情報の破棄（第23条）など、個人位置情報の保護に関する内容を規定している。

一方、位置情報法は個人位置情報主体の権利として、(i) 位置情報事業者等に対する同意の全部又は一部の撤回、(ii) 個人位置情報の収集、利用又は提供の一時的な中止要求、(iii) 個人位置情報主体に対する位置情報収集・利用・提供の事実の確認資料及び個人位置情報主体の個人位置情報がこの法又は他の法律の規定により第三者に提供された理由及び内容の閲覧又は告知、訂正要求などを規定している（第24条）。

さらには個人位置情報主体が位置情報事業者等による法第 15 条から第 26 条の規定の違反行為で損害を被った場合、位置情報事業者等の損害賠償責任も規定しており（第 27 条）、位置情報事業者等と利用者は、位置情報に関する紛争について当事者間で協議が行われず、又は協議が整わない場合には個人情報紛争調停委員会に調停を申請することができる（第 28 条）。

オ 漏えい等事案発生時の本人及び監督機関等への報告義務

位置情報法上、位置情報の流出についての申告又は個人位置情報主体に関する通知の規定はない。

カ 安全管理措置

位置情報事業者等は位置情報の漏えい、変造、棄損などを防止するため位置情報の取扱いの指針を制定したり、アクセス権限者を指定するなどの管理的措置とファイアウォールの設置や暗号化ソフトウェアの活用などの技術的措置をしなければならない（法第 16 条）。

具体的には、(i) 管理的措置には、①位置情報の管理責任者の指定、②位置情報の収集・利用・提供・破棄など各段階別アクセス権限者指定及び権限の制限、③位置情報処理者の義務と責任を規定した取扱い手順及び指針の策定、④位置情報提供事実などの記録台帳の運営・管理、⑤位置情報保護措置に対する定期的な自主監査の実施の内容が含まれなければならない、(ii) 技術的措置には、①位置情報及び位置情報システムのアクセス権限を確認できる識別と認証実施、②位置情報システムへの権限のないアクセスを遮断するための暗号化・ファイアウォールの設置などの措置、③位置情報システムに対するアクセス事実の電子的自動記録・保存装置の運営、④位置情報システムの侵害事故防止のためのセキュリティプログラムの設置及び運営の内容が含まれなければならない（同法施行令第 20 条）。

一方、位置情報事業者等は位置情報の収集・利用・提供の事実に関する確認資料を位置情報システムに自動的に記録されて保存されるようにしなければならない（同法第 16 条第 2 項）。

キ 適用範囲

位置情報法第 4 条は「位置情報の収集、保存、保護及び利用などに関して他の法律に特別な規定がある場合を除いては、位置情報法が定めるところによる」と規定している。つまり、位置情報法は位置情報に関しては一般法としての法的性格を持つところ、位置情報の収集、保存、保護、利用などに関しては同法が優先して適用される。

一方、位置情報法の適用を受ける個人位置情報は情報通信網法上、個人情報にも該当するところ、位置情報法は個人位置情報と関連しては、情報通信網法の特別法的な位置付けにあると見ることができる。したがって、個人位置情報の収集、保存、保護、利用などに関しては、位置情報法が優先して適用され、位置情報法で別途に規定していない部分については、情報通信網法が補足的に適用される。

ク 小規模事業者の取扱い

位置情報法上、小規模事業者に関連した規定はない。

ケ 国際的な情報移転に関する規定

位置情報法上、情報の国外移転に関する規定はない。

(3) 監督機関・第三者機関

個人情報関連法令を所管する機関としては、行政安全部、放送通信委員会、科学技術情報通信部、金融委員会、韓国インターネット振興院、個人情報紛争調整委員会、個人情報保護委員会などが存在する。これまで見てきた個人情報保護法、情報通信網法、信用情報法、位置情報法と各機関との対応関係は、下表のとおりである。

法律	所管の機関(監督・執行の内容)
個人情報保護法	行政安全部(個人情報取扱者に対する報告徴収・立入検査、法令違反があった場合の処分) 個人情報保護委員会(個人情報の保護に関する政策及び法改正についての審議、個人情報の保護に関連する公共機関の間の意見調整) 個人情報紛争調整委員会(個人情報の処理に関する紛争の調整)
情報通信網法	放送通信委員会(情報通信網を通じて収集等される個人情報の保護及び関連技術の開発及び普及並びに漏えい事故発生時等の監督先) 科学技術情報通信部(情報通信網を通じて収集等される個人情報の保護及び関連技術の開発及び普及) 韓国インターネット振興院(漏えい事故発生時等の監督先)
信用情報法	金融委員会及び金融監督院(漏えい事件発生時等の監督先)
位置情報法	放送通信委員会(位置情報の保護及び利用等のための施策の策定、位置情報事業の許可等)

行政安全部と科学技術情報通信部は、政府組織法に基づいて設立された中央行政機関であり、放送通信委員会は、放送通信委員会の設置及び運営に関する法律に基づいて設立された韓国大統領所属の中央行政機関であり、金融委員会は、金融委員会の設置等に関する法律に基づいて設立された国務総理所属の中央行政機関である。

このほか、個人情報保護法第 7 条によって個人情報保護に関する事項を審議・議決するために大統領直属である個人情報保護委員会、同法第 40 条によって個人情報に関する紛争の調整のために設置されている個人情報紛争調整委員会、及び情報通信網法第 52 条により情報通信網の利用と保護、個人情報保護のための対策の研究、その他の個人情報に関する法令所管省庁から委託を受けた事業を行うことなどを目的として設立された韓国インターネット振興院などが存在する。

個人情報保護委員会及び個人情報紛争調整委員会を除く各機関は、個人情報に関連する法令を担当する部門を設置し、個人情報に関連する業務を処理している。各機関の定員や人事システム、予算などは政府組織法（法律第 14804 号）（정부조직법）、行政機関とその所属機関職制（大統領令第 20233 号）（행정자치부와 그 소속기관 직제）などの関連法令によってその内容が決まる。

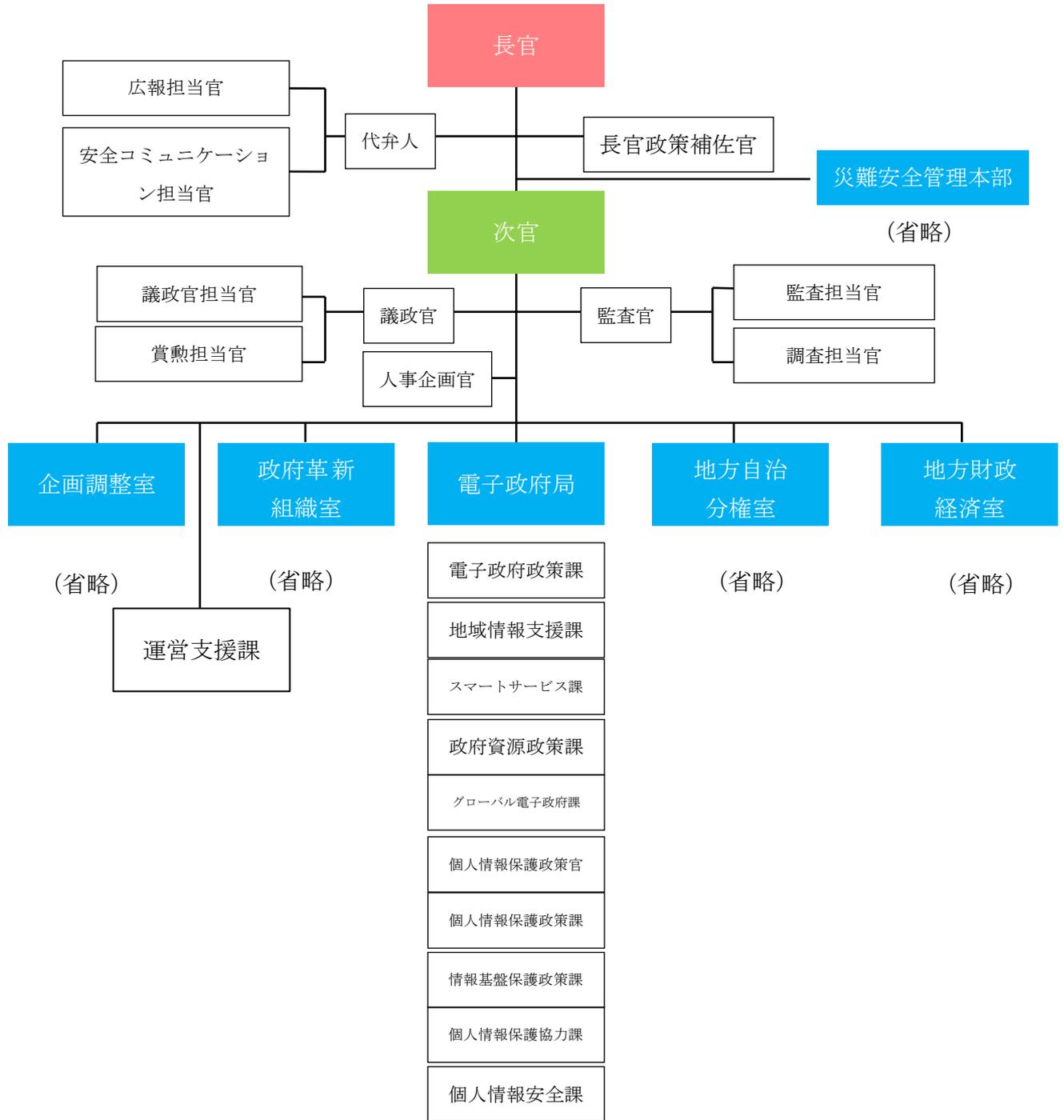
① 各機関の概要

ア 行政安全部 (<http://www.mois.go.kr>)

行政安全部は、個人情報保護政策、情報基盤保護政策、個人情報保護の協力、個人情報安全や閣僚会議の庶務、法令及び条約の公布、政府組織と定員、叙勲、政府革新、行政効率、電子政府、個人情報保護など国家の行政事務として他の中央行政機関の所管に属しない事務を所掌する（行政機関とその所属機関職制の第 3 条）。

行政安全部は下部組織として運営支援課、政府革新組織室、電子政府局、地方自治分権室、地方財政経済室及び災難安全管理本部などを置き、約 60（行政安全部とその所属機関職制の第 4 条）、1,433 人の職員で構成されている。（行政機関とその所属機関職制の[別表 1]）。

組織図



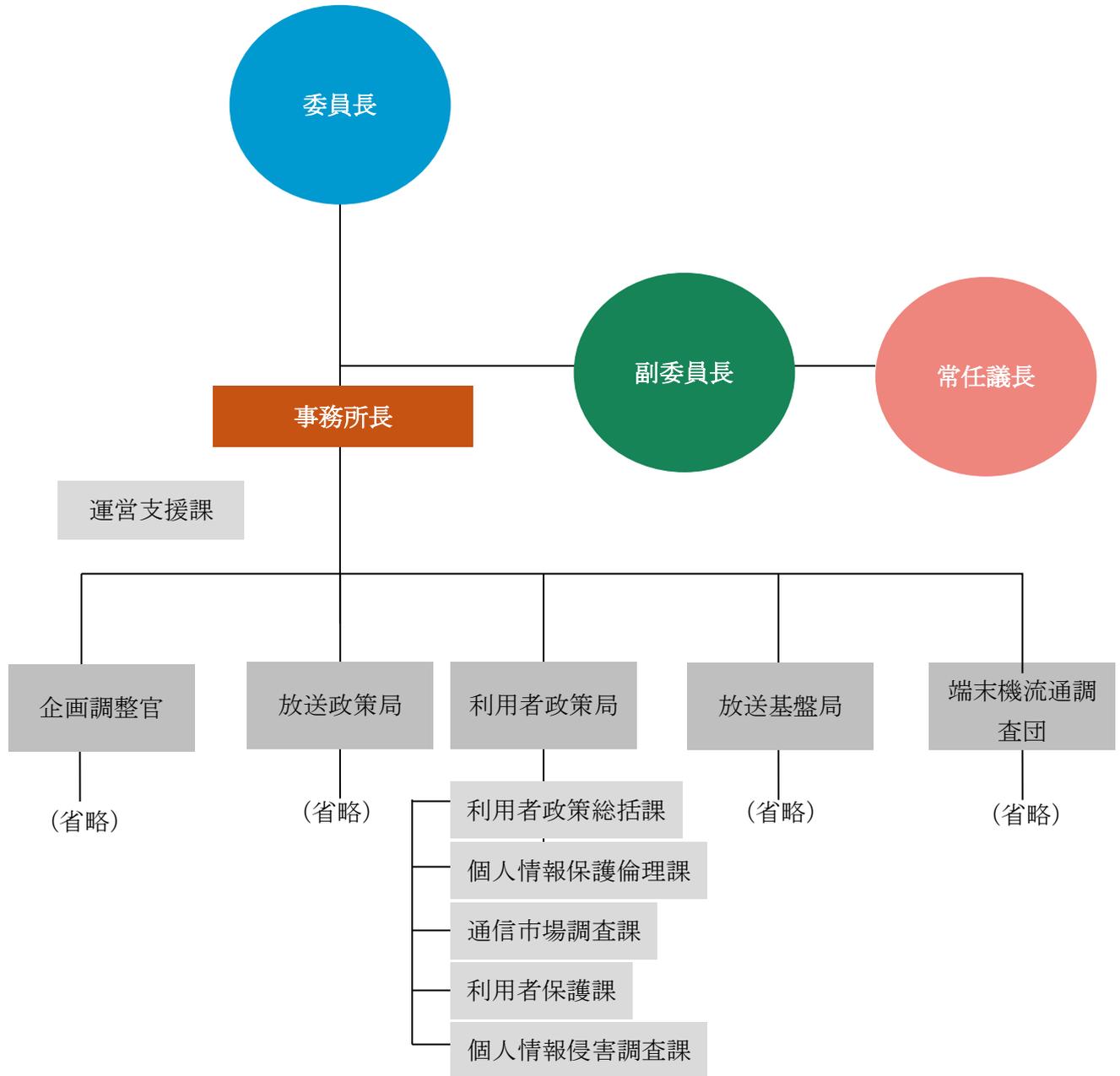
(<http://www.mois.go.kr/frt/sub/a07/orgranFunction/screen.do>)

イ 放送通信委員会 (www.kcc.go.kr)

放送通信委員会は、放送広告政策、編成評価政策、放送通信の利用者保護、個人情報保護倫理、放送用周波数管理に関する事項などを所掌事務としている（放送通信委員会の設置及び運営に関する法律(法律第 13580 号)(방송통신위원회의 설치 및 운영에 관한 법률) 第 11 条)。

放送通信委員会は下部組織として運営支援課、放送政策局、利用者政策局及び放送機局を置き（放送通信委員会の職制(大統領令第 28211 号)(방송통신위원회 직제) の第 4 条)、214 人の職員で構成されている（放送通信委員会の職制の[別表 1]）。

組織図



<http://www.kcc.go.kr/user/organoHR.do?page=A04060100&dc=K06050100>

ウ 科学技術情報通信部 (www.msip.go.kr)

科学技術情報通信部は科学技術政策の樹立・総括・調整・評価、科学技術の研究開発・協力・振興、国家情報化企画・情報保護・情報文化、情報通信産業などに関する事務を所管する（科学技術情報通信部とその所属機関職制（大統領令第 28400 号）(과학기술정보통신부와 그 소속기관 직제) の第 3 条)。

科学技術情報通信部は、下部組織として運営支援課、研究開発政策室、未来人材政策局、情報通信政策室、放送振興政策局、通信政策局、電波政策局及び科学技術革新本部を置き（科学技術情報通信部とその所属機関職制の第 4 条）、777 人の職員で構成されている（科学技術情報通信部とその所属機関職制の[別表 2]）。

エ 金融委員会 (www.fsc.go.kr)

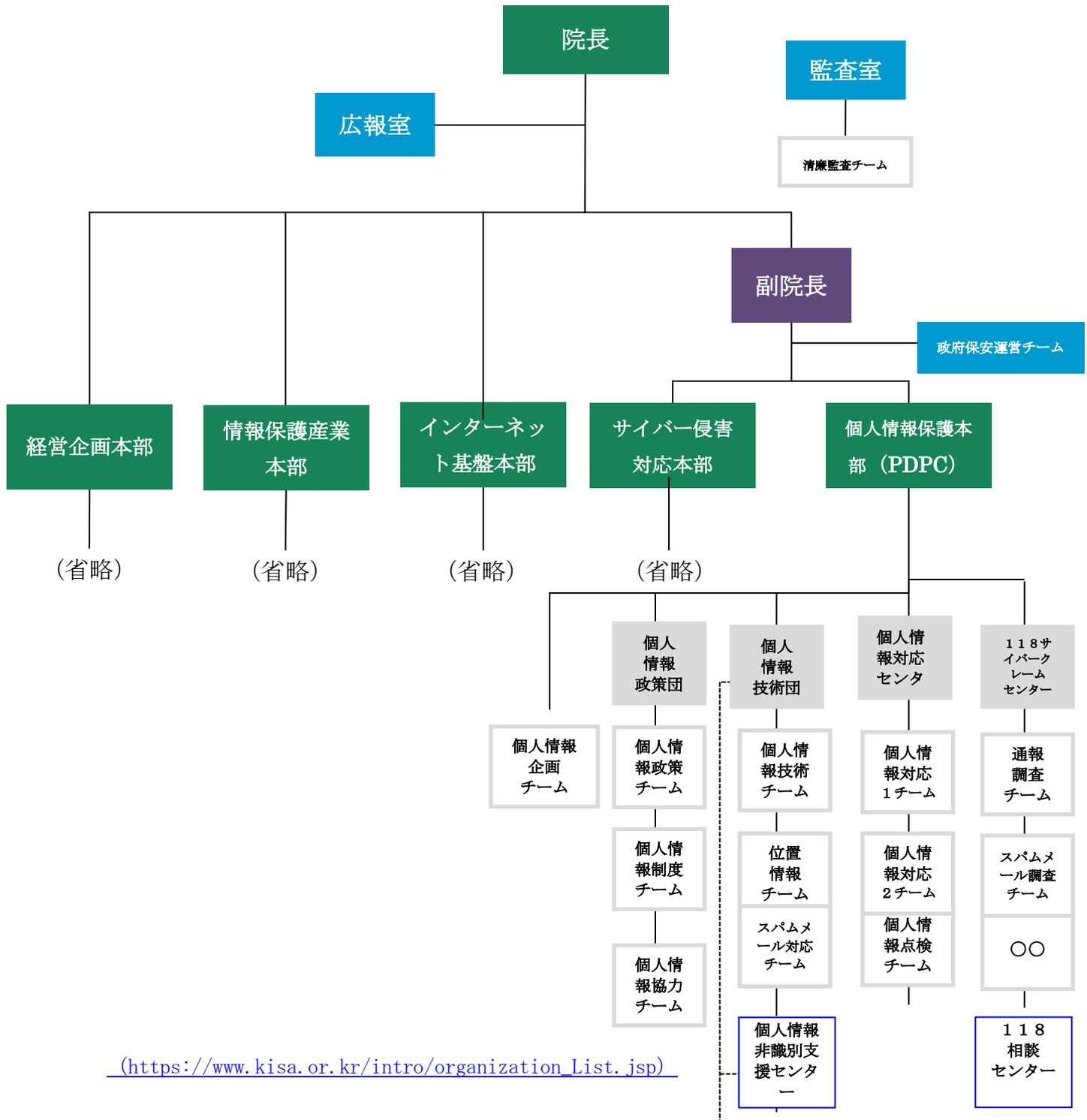
金融委員会は、金融産業の先進化と金融市場の安定を図り、健全な信用秩序と公正な金融取引慣行の確立などに関する事務を所掌する（金融委員会とその所属機関職制（大統領令第 28218 号）(금융위원회와 그 소속기관 직제) の第 3 条)。金融委員会は事務を処理するために行政人事課、資本市場調査団、金融政策局、金融サービス局及び資本市場局を置く（金融委員会とその所属機関職制の第 6 条）。職員は計 203 人である（金融委員会とその所属機関職制の[別表 1]）。

オ 韓国インターネット振興院 (www.kisa.or.kr)

政府は情報通信網の高度化（情報通信網の構築・改善及び管理に関する事項を除く）と安全な利用促進及び放送通信と関連した国際協力・国外進出支援の効率的に推進するため、韓国インターネット振興院を設立した（情報通信網法第 52 条）。韓国インターネット振興院は、公共機関として、情報通信網の利用及び保護、放送通信と関連した国際協力・国外進出などのための法・政策及び制度の調査・研究など情報通信網法第 52 条第 3 項に規定された事業を遂行する。

韓国インターネット振興院は経営企画本部、情報保護産業本部、インターネット基盤本部、サイバー侵害対応本部、個人情報保護本部を下部組織に置いており、2016 年基準の職員数は約 618 人である。

組織図



カ 個人情報紛争調整委員会 (<https://www.kopico.go.kr>)

個人情報保護法は個人情報に関する紛争の調整のため、個人情報紛争調整委員会(개인정보분쟁조정위원회)(以下「紛争調整委員会」という。)を置いている(同法第40条)。紛争調整委員会は、情報主体の被害又は権利侵害が多数の情報主体に同じか似たような類型に発生する場合として、一定した事件に対する集団紛争調停事件も処理している(同法第49条)。

紛争調整委員会は委員長1人を含めた20人以内の委員で構成し、委員は充て職委員と委嘱委員で構成される(同法第40条第2項)。委員長は委員の中で公務員ではない者に個人情報保護委員会委員長が委嘱する。委員長と委嘱委員の任期は2年で、1回に限り再任することができる(同法第40条第4項、第5項)。

一方、紛争調整委員会は、紛争調停の業務を効率的に遂行するために必要とされれば、一定のところにより調停事件の分野別に5人以内の委員で構成される調整部を置くこともあり、この場合、調整部が委員で委任され、議決した事項は紛争調整委員会で議決したものと見ている(同法第40条第6項)。

個人情報と関連した紛争の調整を求める者は、紛争調停委員会に紛争調停を申請することができる。この場合、紛争調整委員会はその申請内容を相手に知らせなければならない(同法第43条)。また、紛争調整委員会は、紛争調停申請を受けた日から60日以内にこれを審査し、調停案を作成しなければならず、(同法第44条)、調停案には、調査対象の侵害行為の中止、原状回復、損害賠償、その外に必要な救済措置など一定の事項を含めて作成することができる(同法第47条)。

キ 個人情報保護委員会 (www.pipc.go.kr)

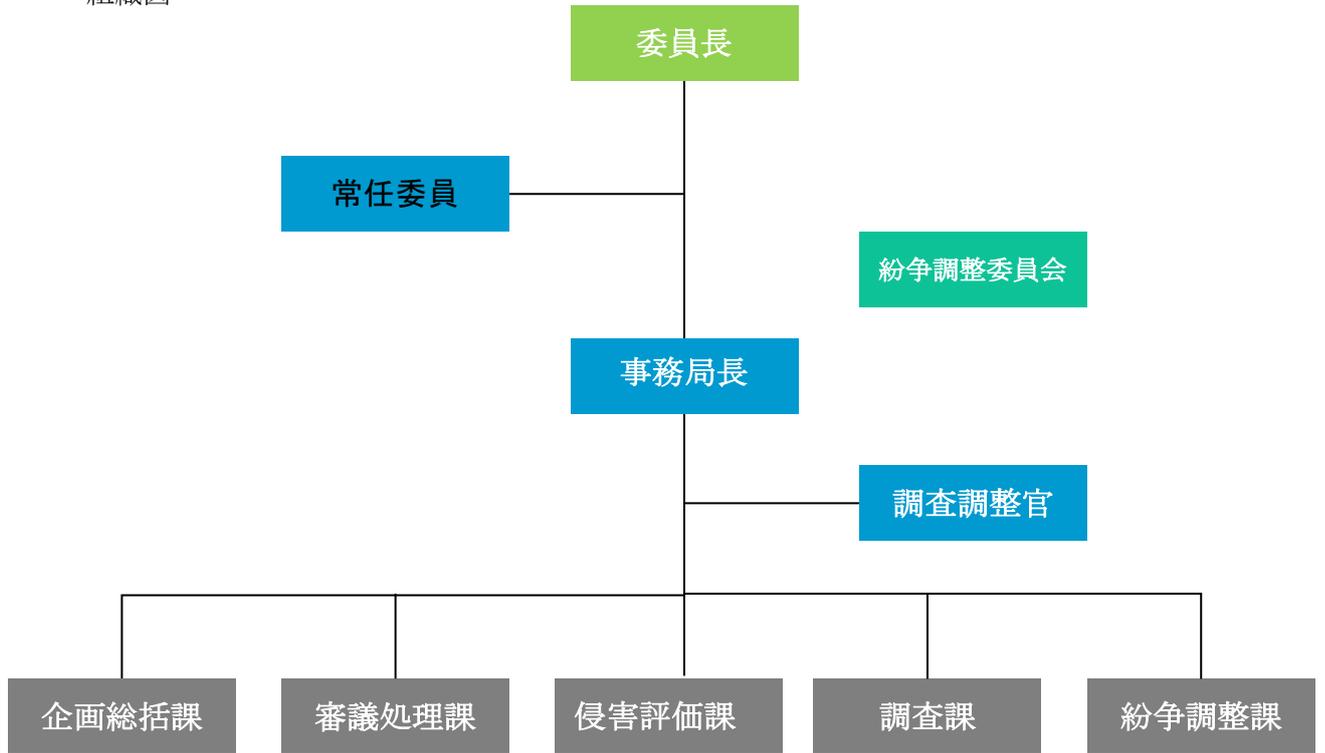
個人情報保護法は個人情報保護に関する事項を審議・議決するために大統領所属で個人情報保護委員会(개인정보보호위원회)(以下「保護委員会」という。)を置いている(同法第7条)。保護委員会は委員長1人、常任委員1人を含めた15人以内の委員で構成し、常任委員は、政務職公務員に任命する(同法第7条第2項)。

委員は、法第7条第4項各号の一つの資格要件を満たさなければならない。委員は、当該資格要件を満たす者のうちから大統領が任命し、委嘱する。この場合、委員のうち5人は国会が選出する者から、5人は最高裁長官が指名する者をそれぞれ任命し、委嘱する(同法第7条第4項)。委員長は委員の中で公務員ではない者に大統領が委嘱する。委員長と委員の任期は3年とし、1回に限り再任することができる。

保護委員会は、個人情報侵害要因の評価に関する事項、個人情報保護と関連した政策、制度や法令の改善に関する事項など法第8条第1項各号の事項を審議・議決し、必要な場合、(i) 関係公務員、個人情報保護に関する専門知識を有する者や市民社会団体及び関連

事業者からの意見聴取、(ii) 関係機関等に対する資料提出や事実の照会を要求することができる (同法第 8 条)。

組織図



<http://www.pipc.go.kr/cmt/int/ent/intEntitySrc.do>

② 運用実態

行政安全部は、個人情報保護法と関連した個人情報管理実態の現場点検などを定期的に施行して、違反事項が発見された場合は過怠料・課徴金付加処分などを執行している。そして金融委員会は信用情報法の所管省庁として、信用情報法上の信用情報業の許可、信用情報法違反行為に対する実態の点検などの業務を遂行している。

一方、放送通信委員会は、情報通信網法、位置情報法と関連した各種許認可や実態点検、過怠料・課徴金付加処分などの業務を遂行しており、科学技術情報通信部は、情報通信網法の所管省庁として、営利目的の広告性情報伝送（同法第 50 条）、情報保護最高責任者の指定申告（同法第 45 条の 3）などに関連した業務を放送通信委員会とともに遂行している。

具体的な法執行事例で、最近宿泊アプリ利用者の個人情報が流出した事案では、情報通信網法による個人情報流出申告を受けた放送通信委員会は、科学技術情報通信部・警察庁・韓国インターネット振興院などと共に、上記流出事故を調査しており、調査の過程で宿泊アプリ運営事業者の個人情報の技術的・管理的保護措置の違反を発見して、これに対する課徴金、過料、是正命令などの行政処分を課した事例も存在する。

特に、実務上、個人情報の流出事故発生時、利用者に対する通知や規制機関のための申告義務は不可欠な要素として理解されている。これにより、規制機関は、通知と申告義務を履行するかどうかを流出事故に対する法律違反かどうかの判断時に考慮している。実際、放送通信委員会は、2016 年のオンラインショッピングモール事業者が個人情報流出事故を起こした際、正当な事由なしに利用者に対する通知及び申告が遅延したことについて、行政上の制裁事由により判断した事例がある。

一方で、韓国インターネット振興院は、情報主体の個人情報への権利又は利益の侵害時に、その内容を通報することができる「違法スパム対応」、「個人情報・情報保護侵害事故通報案内」制度などを運営して、個人情報に関連する苦情を処理している。

また、個人情報保護法は、個人情報への紛争の調整のための個人情報紛争調整委員会を規定し、個人情報処理者及び情報主体の間で発生した個人情報に関する紛争を処理することができる手続きを用意している。

そして個人情報保護委員会は、個人情報の保護に関連した主要な政策の審議や議決及び法令、制度の改善や、個人情報保護に関連している公共機関の間の意見調整等を行っている。

（４）近時のトピック

① 立法並びに行政機関ないし監督機関及び第三者機関の動向

個人情報関連省庁等は、2016 年 6 月 30 日「個人情報以外の識別措置ガイドライン」を発

刊した。上記のガイドラインにおいては、個人情報の非識別措置の基準と、非識別情報の活用範囲などを明確に提示して、企業の投資と産業の発展を図る一方で、国民の個人情報に関する人権の保護を目的としており、「個人情報の判断基準の合理的な基準」、「上記のガイドラインに従った非識別措置を経た情報は、個人情報ではないと推定する」などを主たる内容としている。現在、非識別措置に関する個人情報保護法案と情報通信網法案も国会において審議中である。

一方、2017年10月19日に施行された個人情報保護法施行令及び施行規則は、同意を得る方法について、重要な内容については、文字のサイズ(9ポイント以上)、字の色、太さ、下線などの方法で読みやすく表示すべき旨の規定を新設した。これは以下②で説明している、いわゆる「1mm事件」が生じた後に行われた立法措置である。

なお、行政安全部は2017年9月13日に個人映像情報保護法制定案を立法する予定について述べた。上記制定案は、個人映像情報の処理の段階別の保護基準、安全な管理のための措置等の内容を含んでいる。今後、国会の議決を通じた上記制定案の施行の有無に注目が必要である。

② 近時の主要な裁判例

近時における、個人情報関連法令について参考すべき最高裁判所の判例は、次のとおりである。

・ 最高裁 2016年8月17日宣告 (2014 だ 235080 判決)

最高裁判所は、法律情報提供サイトの運営者が法律大学の教授として在職中のAの個人情報を、上記法学学科のホームページなどを介して収集して、上記のサイト内の「法曹人」の項目において有料で提供した事件において、すでに公開された個人情報は、情報主体の同意があったと客観的に認められる範囲内で収集・利用・提供等の処理をするときには、情報主体の別途の同意は不要であるとの前提の下、上記運営者の行為が、Aの個人情報の自己決定権を侵害する違法な行為であるとか、個人情報保護法に違反した行為であるとみることはできないと判断した。

・ ソウル高裁 2017年2月16日宣告 (2015 な 2065729 判決)

ソウル高等裁判所は、個人情報の市民活動家6名がグーグルアカウント及びサービス利用状況を第三者に提供した内訳を公開するように求めた訴訟に対して、第1審に引き続き、韓国の個人情報保護法第30条第4項に基づき、グーグル本社は利用者が閲覧しようとする個人情報及びその利用の内訳を公開しなければならないとの判決を下した。被告であるグーグルは、本社が国内に所在していないことや、国内法人であるグーグル코리아は国内利用者の個人情報を収集及び利用していないことを理由に利用者による

閲覧権を否定してきたが、高裁はかかる主張を受け入れなかった。また、本高裁判決は、第1審とは異なり、グーグル코리아について国内の利用者らを対象としてグーグルのサービスを提供する重要な役割を担っていた点を認め、グーグル코리아にも責任がある旨を明らかにし、グーグル코리아が利用者に対して個人情報及びサービス利用の内訳を第三者に提供した内訳を公開する義務を負っていると判断した。

- ・ 最高裁 2017 年 4 月 7 日宣告（2016 も 13263 判決）

最高裁判所は、顧客のために抽選会のイベントにおいて、支給された賞金応募券の裏面に、個人情報の収集・利用目的などの通知を、約 1mm の大きさの文字で記載して個人情報を収集し、第三者に提供した事案において、約 1mm サイズの文字は、消費者の立場から見て、その内容を読むことは容易でなく、上記の内容を利用して、上記景品イベントが保険会社などの第三者に顧客の個人情報を提供することの見返りとして行われているとの事情を正確に把握するのは難しい点などを根拠に、「虚偽その他の不正な手段や方法を通じた個人情報の収集」に該当すると判断した。

さらに、上記の判例は、個人情報の処理の委託と第三者提供の区別基準について、既存の判示した「個人情報の移転による業務処理及び利益の帰属主体」のほか、個人情報の取得目的と方法、対価の授受の有無、受託者の実質的な管理・監督の有無などの区別の基準を、従前より具体化した。

7. シンガポール

(1) 制度概要

① 法体系の概要¹

シンガポールでは、従来、銀行法 (Banking Act)²、コンピュータ誤用及びサイバーセキュリティ法 (Computer Misuse and Cybersecurity Act)³などの個別法により個人情報の保護が図られてきたが、2012年に一般的な個人情報保護立法として個人情報保護法 (Personal Data Protection Act, PDPA) (2012年法律第26号)⁴が制定され、2013年1月2日から施行された。PDPAは一般的に、個人情報の収集、使用及び開示に先立ち同意を取得するよう組織に義務づけている。また、PDPAは、「電話禁止登録簿」 (Do Not Call Registry, DNC) の制度についても別途規定している。同法は、個人情報保護委員会 (Personal Data Protection Commission, PDPC) によって執行されているが、情報通信省 (Ministry of Communications and Information, MCI) 管轄下の法定意思決定機関であるシンガポール情報通信メディア開発庁 (Info-communications Media Development Authority of Singapore, IMDA) も同法により監督権限を付与されている。

PDPA第26条に基づき制定された2014年個人情報保護規則 (Personal Data Protection Regulations 2014)⁵は、海外に向けた個人情報の移転に関する要件について規定し、その他PDPAに基づき個人が自己の個人情報にアクセスし、同データを訂正するための手順を定めている。この他、PDPAの細則を定める規則として、PDPCが示談することができるPDPA違反行為について規定されている2013年個人情報保護 (違反行為の示談) 規則 (Personal Data Protection (Composition of Offences) Regulations 2013)⁶、電話禁止登録簿制度の利用手続等の詳細について規定されている2013年個人情報保護 (電話禁止登録簿) 規則 (Personal Data Protection (Do Not Call Registry) Regulations 2013)⁷、PDPCのレビュー手続、個人情報の廃棄などのPDPAが行う指図、及びPDPA遵守の調査権限の実行などのPDPCによるPDPAの執行の詳細について規定されている2014年個人情報保護 (執行) 規則 (Personal Data Protection (Enforcement) Regulations 2014)⁸、並びにPDPCの指図又は決定に対する不服申立手続の詳細について規定されている2015年個人情報保護 (不服

¹ シンガポールの法令については、Singapore Attorney-General's Chambersが運営する「Singapore Statutes Online」にて確認することができる。

<https://sso.agc.gov.sg/Index>

² <https://sso.agc.gov.sg/Act/BA1970>

³ <https://sso.agc.gov.sg/Act/CMCA1993>

⁴ <https://sso.agc.gov.sg/Act/PDPA2012>

⁵ <https://sso.agc.gov.sg/SL/PDPA2012-S362-2014?DocDate=20140519>

⁶ <https://sso.agc.gov.sg/SL/PDPA2012-S759-2013?DocDate=20140819>

⁷ <https://sso.agc.gov.sg/SL/PDPA2012-S709-2013?DocDate=20150529>

⁸ <https://sso.agc.gov.sg/SL/PDPA2012-S455-2014?DocDate=20140702>

申立) 規則 (Personal Data Protection (Appeal) Regulations 2015) ⁹が定められている。また、PDPC は、PDPA の解釈及び PDPC が PDPA に基づく訴えをどのように取り扱うかを判断する際に参照されるデータ保護規定の執行に関するアドバイザリー・ガイドライン (Advisory Guidelines on Enforcement of the Data Protection Provisions) ¹⁰を発行している他、保健省 (Ministry of Health) との協力により、個人の保健情報に適用される、保健部門に関するアドバイザリー・ガイドライン (Advisory Guidelines for the Healthcare Sector) を発行するなど、各種ガイドラインを発行している ¹¹。

なお、PDPA は、民間部門の包括的個人情報保護法であるが、同法は、シンガポールにおけるデータ保護及びプライバシーを対象とする他の法律と同時に適用されることが意図されており、PDPA の一定の規定については、特定の業界に関する特別法・規制が優先する (4 条 (6))。かかる業界特有の他の法律には、コンピュータ誤用及びサイバーセキュリティ法 (Computer Misuse and Cybersecurity Act)、銀行法 (Banking Act) (第 19 章)、2012 年電気通信競争コード (Telecom Competition Code) ¹²、マスメディア・サービスの提供における市場行動実務規範 (Code of Practice for Market Conduct in the Provision of Mass Media Services) (「メディア市場コード」) ¹³、電子商取引法 (Electronic Transactions Act) ¹⁴などがある。

国際的データ移転組織に関しては、シンガポールは、2017 年 7 月に、アジア太平洋経済協力 (Asia-Pacific Economic Cooperation, APEC) のクロスボーダー・プライバシー・ルール (Cross-Border Privacy Rule, CBPR) 及びプライバシー取扱者認証 (PRP) 制度 (Privacy Recognition for Processors Systems) への加盟を申請し、2018 年 2 月に認められている。

② 民間部門に適用される主な法律

PDPA は、個人情報の収集及び使用の双方を規制する包括的なデータ保護法である。PDPA 9 章は、消費者が組織からの広告資料の受領につきオプトアウトすることを可能にする「電話禁止登録簿」(DNC) の制度について規定している。PDPA 第 26 条に基づき制定された 2014 年個人情報保護規則は、個人情報の海外移転の要件について規定している。なお、①でも述べたとおり、PDPA の解釈の指針となる各種ガイドラインが PDPC から発行されている。

⁹ <https://sso.agc.gov.sg/SL/PDPA2012-S20-2015?DocDate=20150122>

¹⁰

[https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-enforcement-of-dp-provisions-\(210416\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-enforcement-of-dp-provisions-(210416).pdf)

¹¹ 主要なガイドラインについては、PDPC の以下のウェブサイトを参照：

<https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines/Main-Advisory-Guidelines>

¹²

<https://www.imda.gov.sg/regulations-licensing-and-consultations/frameworks-and-policies/competition-management/telecom-competition-code>

¹³ <https://sso.agc.gov.sg/SL/S148-2010>

¹⁴ <https://sso.agc.gov.sg/Act/ETA2010>

民間部門において個人情報を規制するその他のシンガポールの法令として以下のものが挙げられる。

- ・ コンピュータ誤用及びサイバーセキュリティ法（第 50 章 A）
- ・ 秘密保持に関する判例法（law of confidence）
秘密情報の誤用及び公表に関するコモンロー上の禁止である。
- ・ 銀行法（第 19 章）
- ・ 2012 年電気通信競争コード
- ・ マスメディア・サービスの提供における市場行動実務規範（「メディア市場コード」）
- ・ 電子商取引法（第 88 章）
- ・ テクノロジー・リスク・マネジメントに関する通知（Notice on Technology Risk Management）¹⁵

③ 公的部門に適用される主な法律

公務機密法（Official Secrets Act）（第 213 章）¹⁶、統計法（Statistics Act）（第 317 章）¹⁷並びに法定機関及び政府系企業機密保護法（Statutory Bodies and Government Companies（Protection of Secrecy） Act）（第 319 章）¹⁸における秘密保持及び開示に関する法律等、個人情報の処理に関連する多くの法律が公的部門に適用される。

（2）主な法令の概要

① PDPA

ア 法令の概要

（1）②で述べたとおり、PDPA は、個人情報の収集及び使用の双方について規定する個人情報の保護に関する一般法であり、個人情報を収集するすべての産業及び組織に適用される。PDPA は、2012 年に可決され、2013 年 1 月 2 日に施行された。2014 年 1 月 2 日から電話禁止登録簿に関する規定の適用が開始され、その他の部分についても 2014 年 7 月 2 日から適用が開始された。PDPA の解釈に際しては、PDPC が公表した各種ガイドラインが参照されている（PDPA の重要概念に関するアドバイザー・ガイドライン（Advisory Guidelines

¹⁵

http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/IID%20Notices/Notice%20CMGN02_2014.pdf

¹⁶ <https://sso.agc.gov.sg/Act/OSA1935>

¹⁷ <https://sso.agc.gov.sg/Act/SA1973>

¹⁸ <https://sso.agc.gov.sg/Act/SBGCPSA1983>

on Key Concepts in the PDPA) 、PDPA の選択トピックについてのアドバイザリー・ガイドライン (Advisory Guidelines on the PDPA for Selected Topics) など) 。

PDPA 第 3 条は、同法の「目的」について、以下のとおり規定している。

本法の目的は、個人が自己の個人情報を保護する権利、並びに当該状況において適切とみなすことが合理的と言える目的において組織が個人情報を収集、使用及び開示する必要性の双方を認める方法で、組織による個人情報の収集、使用及び開示について規定することである。

イ 個人情報の定義

「個人情報」は、PDPA 第 2 条において、「真実か否かを問わず、当該情報から、又は当該情報と当該組織が有する若しくはアクセスし得る他の情報と合せて、その個人が識別可能な情報」と定義されている。PDPC の各種アドバイザリー・ガイドラインは、典型的な個人情報として、氏名、パスポート番号、個人の携帯電話番号、顔写真、指紋、個人の音声、DNA プロフィールなどが例示されている。PDPA では、原則として、死後 10 年を経るまでの死者の個人情報も保護の対象となる (4 条 (4) (b)) 。

なお、PDPA は、「個人の名前、役職、名称若しくは職位、業務用電話番号、業務用住所、業務用電子メールアドレス若しくは業務用ファックス番号その他個人に関する類似の情報のうち当該個人の目的のためのみに提供された情報でないもの」と定義される「商業上の連絡先情報」 (Business Contact Information, BCI) を一般的に同法の適用から除外している。

ウ 主な規制・権利の内容

PDPA は、シンガポール国内の民間部門におけるすべての組織による個人情報の収集、使用及び開示について規定しており、個人に対して自己の個人情報を保護する権利を付与している。第 5 条は、同法に基づく権利を行使するための個人情報保護委員会の設置について規定し、第 13 条は、個人情報の収集、使用及び開示のすべてについて同意を義務づけている。第 14 条には、「通知義務」が含まれており、かかる義務により、個人は、自己の個人情報が収集される前に、当該データが収集、使用若しくは開示されている目的、又は収集、使用若しくは開示される目的について通知を受ける権利を有する。

また、個人は、組織の保有するデータにアクセスし (第 21 条) 、これが不正確である場合、訂正する (第 22 条) 権利を有する。第 16 条は、組織による個人情報の収集、使用及び開示に対して、合理的な通知を行ったうえでいつでも同意を撤回できる権利を個人に与えている。

第 11 条は、PDPA の重要概念に関するアドバイザリー・ガイドラインにおいて言及されるデータ保護オフィサー (data protection officer, DPO) の指名を義務づけている。DPO は、PDPA の遵守について責任を負う。DPO の業務上の連絡先は、公開されていなければならない。

第 23 条は、収集された個人情報に正確かつ完全であるよう合理的な努力を払うよう組織に義務づけている。同法第 24 条は、合理的なセキュリティ体制の設置による個人情報の保護を義務づけており、第 25 条は、不要となった書類の保有をやめるよう組織に義務づけている。

さらに、第 36 条乃至第 48 条 (9 章) は、シンガポールにおける電話禁止登録簿制度について規定している。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

PDPA は、データ違反があった場合に、個人又は PDPC 宛てに通知を行うよう義務づけてはいない。ただし、PDPC は、その各種ガイドライン (データ違反管理ガイド (Guide to Managing Data Breaches) を含む。) において、組織は、影響を受けた個人及び PDPC の双方に対して自主的に通知を行うよう奨励している。組織が通知を行った場合、PDPC は、当該組織がその管理下又は保有下にある個人情報について第 24 条に基づいて義務づけられる適切な保護を行ったか否かを判断するにあたり、当該通知を考慮することができる。

PDPC は現在、義務的なデータ違反通知の導入を検討しており、この点について、2017 年 8 月から 9 月にパブリックコンサルテーションを実施した。

オ 安全管理措置

第 24 条は、「保護義務」について規定しており、組織に対して、不正なアクセス、収集、使用、開示、複製、改ざん、処分及び類似のリスクを防止するために適切なセキュリティ上の用意をすることにより、個人情報を保護するよう義務づけている。

カ 適用範囲

PDPA は、シンガポール国内の民間部門における個人情報の収集、使用及び開示その他の取扱いすべてに適用される。PDPA は域外適用され、①シンガポール所在の個人の情報か、又は②シンガポールで個人情報を取得、利用もしくは開示するのであれば、その組織の規模や設立場所を問わず、原則として、あらゆる組織に PDPA は適用される。つまり、個人、企業、団体などの区別を問わず、またシンガポールで設立されたかどうか、シンガポールに事務所を有しているかなどを問わずに PDPA の適用があるため、シンガポールに拠点を持

たない日本企業にも PDPA の適用はあり得る。

第 4 条は、PDPA の適用が除外される場合を複数規定しており、これには、少なくとも 100 年以上存在している記録に含まれる個人情報又は死亡後 10 年が経過している個人に関する個人情報が含まれる。業務上の連絡先情報も、一般的に同法の保護から除外される。

キ 小規模事業者の取り扱い

PDPA 上、小規模事業者に関する特別な規定は定められていない。ただし、PDPC は、その 2014/2015 年間報告書において記載のとおり、特に中小企業に対して、個人情報保護指針及び実務の策定を指導及び支援する継続的な努力を行っている。

ク 国際的な情報移転に関する規定

シンガポール国外へのデータ移転は、第 26 条の移転制限義務の対象となる（企業グループ間開示を含む。）。

ケ 紛争処理手続き

組織による PDPA 違反があった場合、損害を被った者は、PDPA に基づき民事訴訟を提起することができ、裁判所は、差止め又は宣言、損害賠償、その他裁判所が適切と考える救済を与えることができる（第 32 条）。PDPC は、適切と考える場合は、調停その他の ADR により紛争を解決することを試みるように紛争の当事者に指示することができる（第 27 条）。PDPC は、当事者からの申立てがあった場合は、第 21 条又は第 22 条による個人の請求に対する組織の回答を調査し、組織に必要な措置を行うよう指示することができる（第 28 条）。

PDPC は、組織の PDPA の遵守状況を調査することができ、その際、書類や情報の提示要求、敷地への立ち入りを行うことができ、PDPA を遵守するために必要な措置を指図することができる（第 29 条、第 50 条）。かかる指図には、①PDPA 違反の個人情報の取得、使用又は開示の差止め、②PDPA に違反して収集された個人情報の廃棄、③100 万シンガポールドル以下の制裁金が含まれる。

PDPC による指示は、地方裁判所への提示後、司法命令に転換することができる。

② 2014年個人情報保護規則

ア 法令の概要

(1) ①で述べたとおり、2014年個人情報保護規則は、海外に向けた個人情報の移転に関する要件について規定している。同規則は、PDPA 第26条に基づき公布され、2014年7月2日に施行された。

イ 個人情報の定義

2014年個人情報保護規則第2条及び第8条の両規定において、「個人の個人情報」が定義されている。第2条は、「個人情報へのアクセス及び同データの訂正に関する要請」に関する規制2章において、「個人の個人情報」を「個人に関する個人情報」と定義しており、第8条は、「個人情報のシンガポール国外への移転」に関する規制3章において、「個人の個人情報」を「当該個人に関する個人情報」と定義している。同規則はPDPAに基づき制定されているため、同規則の「個人情報」の意味は、PDPAにおける「個人情報」の定義に従うこととなる。

同規則は、機微情報 (sensitive information) について定義していない。もっとも、PDPAは、個人情報の管理に際して合理的なセキュリティの確保をすることを企業等に対して求めているが、監督官庁であるPDPCが発行した各種アドバイザリー・ガイドラインでは、適切なセキュリティ水準を決定する上で、対象となる個人情報の性質を考慮に入れる必要があるとされており、機微情報に該当するか否かも考慮要素になるものと思われる。そのため、機微情報に該当する個人情報に関しては、情報の管理に際して、一般の情報よりも厳格なセキュリティ手段を講じるなどの対応が必要になるものと考えられる。

ウ 主な規制・権利の内容

2014年個人情報保護規則2章(第2条乃至第7条)は、個人が組織に対して個人情報へのアクセス及び同データの訂正を申請するための要件を定めている。同規則3章(第8条乃至第10条)は、シンガポール国外への個人情報の移転に関する要件を定めている。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

2014年個人情報保護規則には、データ違反報告義務は含まれていない。

オ 安全管理措置

2014 年個人情報保護規則には、安全管理措置に関する規定は定められていない。

カ 適用範囲

2014 年個人情報保護規則は PDPA に基づき制定されたものであるため、PDPA と同様の適用範囲となる。

キ 小規模事業者の取り扱い

2014 年個人情報保護規則において、小規模事業者に関する特別な規定は定められていない。

ク 国際的な情報移転に関する規定

2014 年個人情報保護規則は、個人情報の海外への移転要件について規定している。同規則第 9 条(1)(b)によれば、移転組織は、個人情報をシンガポール外の国又は領域に移転する前に、シンガポール外の国又は領域における個人情報の受領者が、移転された個人情報に対して少なくとも PDPA 上の保護水準と同等の保護水準となる、法的に守らせることができる義務を確保するために適切な措置を講じなければならない。同規則第 10 条は、同要件に基づき十分とみなされる法的に守らせることができる義務を、以下を含むものとして特定している。

(a) 法律

(b) 少なくとも PDPA 上の保護水準と同等の保護水準の規定を受領者に義務づけ、かつ、契約に基づき個人情報が移転され得る国及び領域を特定する契約

(c) 拘束力を有する会社規則で同規制の要件を満たすもの

(d) その他一切の法的拘束力を有する文書

また、同規則第 9 条(3)は、シンガポール国外へのデータ移転が認められる上記とは別の要件として、同規制の同意要件に従って個人情報の移転に対する個人の同意が付与されており、かつ、個人情報の移転が契約の履行に必要であること、又はデータがその他シンガポールにおいて公表されていることを要する旨明記している。

同規則第 9 条(4)は、同意の前に、当該法律に基づく水準に匹敵する水準において個人情報保護される国や地域に移転されるということを適切に書面で、その要約を提出すること、又は商品若しくはサービスを提供する条件として個人の同意が求められていた場合においては、個人に対する商品若しくはサービスの提供にあたり当該移転が合理的に必要なであったことを要件としている。

③ コンピュータ誤用及びサイバーセキュリティ法（第 50 章 A）

ア 法令の概要

コンピュータ誤用及びサイバーセキュリティ法（第 50 章 A）は、データへの不正アクセスを刑事上の犯罪と定めたもので、当初 1993 年に施行され、直近では 2017 年に改正された。直近の改正は、2017 年 4 月 3 日に可決され、2017 年 6 月 1 日に施行された。

イ 個人情報の定義

コンピュータ誤用及びサイバーセキュリティ法第 3 条は、「一切のコンピュータにおいて保管されるプログラム又はデータ」への不正アクセスを禁止しており、同法第 2 条は、「データ」を「コンピュータでの使用に適した形式で作成される又は作成された、情報又は概念の表示」と定義している。

コンピュータ誤用及びサイバーセキュリティ法第 8 条 A は、「個人情報」の開示を禁止している。

ウ 主な規制・権利の内容

コンピュータ誤用及びサイバーセキュリティ法第 3 条は、すべてのコンピュータにおいて保有される情報又はデータについて規制し、当該情報又はデータへの不正アクセスを刑事上の犯罪と規定している。改正法の新第 8 条 A は、個人情報が同法に違反して取得されたことを知っている又はそう信ずる理由がある場合には個人情報の使用が刑事上の犯罪に該当するとしている。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

コンピュータ誤用及びサイバーセキュリティ法には、データ違反報告義務は含まれていない。

オ 安全管理措置

コンピュータ誤用及びサイバーセキュリティ法には、安全管理措置に関する規定は定められていない。

カ 適用範囲

コンピュータ誤用及びサイバーセキュリティ法は、域外適用の効力を有し、シンガポール国内に所在するコンピュータに対して海外で実行された行為を刑事上の犯罪としている。同法第 11 条は、同法の適用範囲を定めており、違反の時点においてかかる者がシンガポールにいた場合、該当の時点でコンピュータ、プログラム若しくはデータがシンガポールにあった場合、又は違反によりシンガポールにおいて深刻な被害の重大なリスクが発生する場合、「その国籍又は市民権を問わず、シンガポール内外における一切の者」に対して効力を有するとしている。

キ 小規模事業者の取り扱い

コンピュータ誤用及びサイバーセキュリティ法において、小規模事業者に関する特別な規定は定められていない。

ク 国際的な情報移転に関する規定

コンピュータ誤用及びサイバーセキュリティ法において、国際データ移転に関する規定は定められていない。

④ 銀行法（第 19 章）

ア 法令の概要

銀行法（第 19 章）は、1970 年に施行され、直近の修正は 2008 年に施行された。同法は、銀行業の免許（資本要件、株主及び議決権支配規制、準備金要件、配当規制などを含む）及び兼業規制（投資規制を含む）などを定めている。また、同法は、金利、銀行検査及び破産の他、クレジットカード事業の免許などについても定めている。同法は、顧客情報の保護という位置づけで個人情報の保護を定めている。

イ 個人情報の定義

銀行法第 47 条（「銀行業務上の秘密」）は、「顧客情報」の開示を禁止している。同法第 40 条 A は、銀行に関連する「顧客情報」を以下のとおり定義している。

- (a) 銀行の顧客口座に関連する情報又は詳細をいい、当該口座がローン、投資又はその他一切の種類取引に関するものであるかを問わないが、指定の顧客又は指定の顧客グループを特定できない情報は含まない。
- (b) 預金情報（以下に関連する一切の情報を含む。）
- i. 銀行顧客の預金
 - ii. 顧客の資金のうち銀行が運用しているもの（例えば、（銀行又はいずれかの金融機関の）顧客の資金又は資産のうち、運用又は投資を目的として当該銀行に置かれているもの）
 - iii. 顧客が銀行において維持する貸金庫又は保護預かり合意。ただし、指定の顧客又は指定の顧客グループを特定できない情報は含まない

ウ 主な規制・権利の内容

銀行法第 47 条（「銀行秘密」）は、銀行に対して法定の秘密保持義務を課し、顧客情報の開示を禁止している。同法において明示的に規定される例外を除き、銀行（シンガポールにおいて有効な銀行ライセンスを有する銀行又はシンガポール国外で設立された当該銀行の支店及び営業所でシンガポール国内に所在するもの）又はその役員は、いかなる方法によっても顧客情報を他の者に開示してはならないとされている。かかる例外は、同法の別表第三（情報の開示）において詳述されている。同法第 47 条(8)に基づき、銀行は、より高度な秘密保持を顧客に提供することを選択することができる。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

銀行法には、データ違反報告義務は含まれていない。

オ 安全管理措置

銀行法には、安全管理措置に関する規定は定められていない。

カ 適用範囲

銀行法は、シンガポールの銀行が保有するすべての顧客情報を保護しており、同法第 2 条の定義によれば、ここでいう「シンガポールの銀行」には、シンガポールにおいて有効な銀行ライセンスを有するすべての銀行又はシンガポール国外で設立された当該銀行の支店及び営業所のうちシンガポール国内に所在する支店及び営業所、並びにその役員が含まれる。

キ 小規模事業者の取り扱い

銀行法において、小規模事業者に関する特別な規定は定められていない。

ク 国際的な情報移転に関する規定

銀行法において、国際データ移転に関する規定は定められていない。

⑤ 2012 年電気通信競争コード

ア 法令の概要

電気通信法 (Telecommunications Act) (第 323 章) に基づき公布された 2012 年電気通信競争コードは、2012 年に施行された。同コードは、電気通信加入者情報に関するもので、エンドユーザーたる加入者の電気通信ライセンス情報の取扱いについて言及している。

2012 年電気通信競争コード第 1.2 条は、同コードの「目的」について、以下のとおり規定している。

本コードの目的は、以下のとおりである。

(a) シンガポールにおける情報通信産業の効率及び競争力の促進

(b) シンガポールにおけるすべての人々にとって電気通信サービスを適度にアクセス可能なものとし、可能な限り効率的及び経済的に、かつ、シンガポールにおける社会的、産業的及び商業的需要を合理的に満たす実施基準で電気通信サービスを提供すること。

(c) シンガポールにおける、電気通信技術に関連する商業活動に従事する者の間での公平かつ効率的な市場行動及び有効な競争の促進及び維持

(d) (シンガポール内外の市場における) シンガポールの情報通信産業の全分野による効果的な参加の促進

(e) シンガポールの情報通信産業における産業自主規制の奨励、支援及び促進

(f) シンガポールにおける情報通信産業に対する投資並びに同産業の確立、発展及び拡大の奨励、支援及び促進

イ 個人情報 の定義

同コード第 3.2.6 条は、エンドユーザー・サービス情報（「EUSI」）の不正使用を防止するために免許人が合理的な措置を講ずるよう義務づけている。

EUSI は、同コード第 3.2.6.1 条において、「免許人が提供するサービスをエンドユーザーが使用した結果免許人が入手する一切の情報」と定義しており、それには、以下に関する情報を含むがこれらに限られないとされている。

「(a) エンドユーザーの利用パターン（架電回数、架電時刻、通話時間及び架電相手を含む。）

(b) エンドユーザーが利用したサービス

(c) エンドユーザーの電話番号及びネットワーク設定

(d) エンドユーザーの位置情報

(e) エンドユーザーの請求先氏名、住所及びクレジット履歴」

ウ 主な規制・権利の内容

電気通信法（第 323 章）に基づくすべての免許人に適用される電気通信コード（Telecom Code）は、エンドユーザー・サービス情報（「EUSI」といい、顧客の請求先氏名、サービスの利用パターン及びクレジット履歴等の情報を含む。）の不正開示を禁止している。同

コード第 3.2.6 条は、EUSI の不正使用を防止するために合理的な措置を講ずるよう免許人に義務づけている。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

2012 年電気通信競争コードには、データ違反報告義務は含まれていない。

オ 安全管理措置

電気通信競争コード第 3.2.6 条は、免許人が、エンドユーザー・サービス情報（「EUSI」）の不正使用を防止するために「適切な対策」を講じなければならない旨明記している。もっとも、同コードにおいて、具体的な安全管理措置に関する規定は定められていない。

カ 適用範囲

電気通信競争コード第 1.4 条は、消費者保護に関する規定が電気通信法に基づく一切の電気通信免許人に適用される旨規定している。

キ 小規模事業者の取り扱い

電気通信競争コードにおいて、小規模事業者に関する特別な規定は定められていない。

ク 国際的な情報移転に関する規定

電気通信競争コードにおいて、国際データ移転に関する規定は定められていない。

⑥ マスメディア・サービスの提供における市場行動実務規範（「メディア市場コード」）

ア 法令の概要

放送法（Broadcasting Act）（第 28 章）及びシンガポール・メディア開発庁法（Media Development Authority of Singapore Act）（第 172 章）に基づき公布されたメディア市場コードは、当初 2003 年に導入され、直近の修正は 2016 年に施行された。その主な目的は、シンガポールのメディア産業における公正な市場行動及び有効な競争の実現及び維持、並びにシンガポールのメディア産業における産業自主規制の奨励などにある。同コードは、規制対象者の顧客に対する義務、不正競争の禁止、支配免許人に対する特別な義務などを

規定するとともに、規制対象者の顧客に対する義務の一環として加入者サービス情報を保護する義務について規定している。

メディア市場コード第 1.1 条は、同コードの「目的」について、以下のとおり規定している。

本コードの目的は、以下のとおりである。

- (a) シンガポールのメディア産業における公正な市場行動及び有効な競争の実現及び維持
- (b) シンガポールにおける総合的品質のメディア・サービスの供給の確保
- (c) シンガポールのメディア産業における産業自主規制の奨励
- (d) シンガポールのメディア産業に対するさらなる投資及び同サービスにおける発展の促進
- (e) 公益の保護

イ 個人情報の定義

メディア市場コード第 3.6 条は、「加入者サービス情報」(SSI) を保護する義務について規定している。第 3.6.1 条は、同情報を以下のとおり定義している。

「SSI は、加入者が加入サービスを使用した結果規制対象者が入手する、加入者に関する一切の情報から構成される。かかる情報は、以下に関する情報を含むが、これらに限られない。

- (a) 加入者が注文したサービス又は機器
- (b) 加入者のサービス利用状況
- (c) 加入者の請求先氏名、住所、クレジット情報及び履歴

なお、同コード第 1.5 条(b)(xxxi)において、「加入者」は、「規制対象者から加入サービスを購入することに合意した、又は購入した最終顧客」と定義されている。

ウ 主な規制・権利の内容

メディア市場コード第 3.6 条は、シンガポール・メディア開発上法 (MDA) に基づき規制される事業体 (entity) による「加入者サービス情報」 (SSI) の開示を禁止している。同コード第 3.6.2 条は、SSI の使用に対する具体的制限について規定しており、規制対象の事業体による加入者の SSI の使用を、「(i) 当該加入者が注文した加入サービスの計画、提供及び請求、(ii) 不良債権の管理及び加入サービスの提供に関連する詐欺の防止、(iii) 政府当局若しくは規制当局によって要請され得る規制対象者間の協力の促進、又は(iv) 法の執行若しくはその他の政府機関に対する支援の提供」のみに制限している。さらに、規制対象の事業体は、加入者が許可を与えた場合を除き、規制対象の事業体が「(i) 他の商品若しくはサービスの開発若しくはマーケティングのために加入者の SSI を使用し、(ii) 一切の関係会社若しくは第三者に対して SSI を開示又は提供し、又は(iii) いずれかの関係会社又は第三者に対する SSI の開示又は提供の原因となる不作為若しくは状況を承認、許可若しくは許容」しないよう、「商業的に十分な手続」を採用しなければならない。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

メディア市場コードには、データ違反報告義務は含まれていない。

オ 安全管理措置

メディア市場コードには、安全管理措置に関する規定は定められていない。

カ 適用範囲

メディア市場コード第 3.2 条において、最終消費者に対する義務 (免許人の全加入者に対するデータ保護義務を含む。) は、シンガポール・メディア開発庁 (MDA) 法に基づく規制対象者にしか適用されないことが明記されている。

キ 小規模事業者の取り扱い

メディア市場コードにおいて、小規模事業者に関する特別な規定は定められていない。

ク 国際的な情報移転に関する規定

メディア市場コードにおいて、国際データ移転に関する規定は定められていない。

⑦ 電子商取引法（第 88 章）

ア 法令の概要

電子商取引法（第 88 章）は、電子商取引の安全と利用について定めたものである。具体的には、書面及び署名要件、電子記録の保持、形式、並びに契約の有効性についての規制を含む、電子記録、電子署名、及び電子契約について規定している他、電子記録及び署名の保護、セキュリティ手続、並びに公的機関による電子記録及び署名の利用についても規定している。同法は、電子記録の形態による第三者資料の開示に関するネットワークサービス提供者の責任として個人情報の保護に言及するとともに、同法に基づく権限の行使及び義務の履行に基づき取得した情報の秘密保持義務についても規定している。

第 3 条は、同法の「目的」について、以下のとおり規定している。

本法は、当該状況において商業上合理的とされる解釈に従って、かつ、以下の目的が有効となるよう解釈される。

(a) 信頼性のある電子記録を用いた電子通信の促進

(b) 電子商取引の支援、書面及び署名要件に関する不確実性に起因する電子商取引における障害の除去、安全な電子商取引の実施に必要な法律上及びビジネス上のインフラの開発促進

(c) 公的機関への書類のオンライン届出の促進、信頼できる電子記録を用いた公的機関による効率的なサービス提供の促進

(d) 偽造電子記録の発生、意図的及び非意図的な記録の改ざん、電子商取引その他の電子取引における詐欺の発生率の最少化

(e) 電子記録の認証及び整合性に関する統一的な規則、規制及び基準の確立の支援

(f) 電子記録及び電子商取引の整合性及び確実性における国民の信頼の促進、並びに一切の電子メディアにおける通信に対する認証及び整合性の付与のための電子署名の利用を通じた電子商取引の発展の促進

(g) 2005 年 11 月 23 日に国連総会において採択された国際契約における電子通信の使用に関する国連条約の実施及び同条約の規定に従った電子取引に関するシンガポール法の制定（関係当事者の事業所が別の国にあるか否かを問わない。）

イ 個人情報の定義

第 26 条は、「電子記録の形態による第三者資料」の開示に関するネットワークサービス提供者の責任について言及している。第 2 条(1)は、「電子記録」を「情報システムにおいて、又は、一つの情報システムから別の情報システムへの送信を目的として、電子的手段により生成、通信、受信又は保管された記録」と定義している。

ウ 主な規制・権利の内容

第 26 条は、「電子記録形式による第三者資料」の開示に関して、データ仲介者としてのネットワークサービス提供者の責任について言及している。同条第 1 項 A は、「第(2)項に従い、ネットワークサービス提供者は、同提供者がアクセスを提供しているに過ぎない電子記録形式による第三者資料について 2012 年個人情報保護法に基づく責任を負わない。」と規定している。

また、第 28 条は、同法に基づく一定の権限の行使を通して取得された情報について規制している。また、電子商取引法は、同法違反の起訴等法的な目的がある場合を除き、当該情報の開示を禁止している。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

電子商取引法には、データ違反報告義務は含まれていない。

オ 安全管理措置

電子商取引法には、安全管理措置に関する規定は定められていない。

カ 適用範囲

電子商取引法には、第三者による情報開示についてネットワークサービス提供者が負う責任に関する規定が定められている。

キ 小規模事業者の取り扱い

電子商取引法において、小規模事業者に関する特別な規定は定められていない。

ク 国際的な情報移転に関する規定

電子商取引法において、国際データ移転に関する規定は定められていない。

⑧ テクノロジー・リスク・マネジメントに関する通知

ア 法令の概要

テクノロジー・リスク・マネジメントに関する通知は、シンガポール金融管理局 (Monetary Authority of Singapore, MAS) のテクノロジー・リスク・マネジメント・ガイドライン (Technology Risk Management Guidelines) の一部として証券先物法 (Securities and Futures Act) (第 289 章) 第 46 条、第 46 条 ZK、第 81 条 R、第 101 条及び第 293 条に基づき公布された。同通知は、金融機関に対して、一定のセキュリティ対策を講じるよう義務づけているもので、2013 年に発行され、2014 年に修正された。

イ 個人情報の定義

第 9 条は、金融機関に対して「顧客情報」を保護するよう義務づけている。

ウ 主な規制・権利の内容

イで述べたとおり、第 9 条は、「顧客情報」を保護するよう金融機関に義務づけている。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

第 7 条は、金融機関に対して、データ違反の「該当事案」(「該当 IT 事案」を含む。) の判明後、可及的速やかに (ただし、遅くとも 1 時間以内に) MAS に通知を行うよう義務づけている。「該当事案」は、同通知第 2 条において、「システム故障又は IT セキュリティ事案のうち、金融機関の運営において深刻かつ広範囲な影響を及ぼすもの又は金融機関の顧客に対するサービスにおいて重大な影響を及ぼすもの」と定義されている。「該当 IT 事案」は、第 2 条において、「重要なシステムに対するハッキング、侵入若しくは DoS 攻撃又は顧客情報のセキュリティ、整合性若しくは秘密保持に危害を加えるシステム等のセキュリティ違反に関連する事案」と定義されている。

オ 安全管理措置

第 9 条は、金融機関に対して、顧客情報を不正なアクセス又は開示から保護するために「IT 管理を実施する」よう義務づけている。

カ 適用範囲

第 1 条は、以下のすべてに対して適用される旨規定している。

- (a) 承認された取引所
- (aa) ライセンス取得済みの取引情報蓄積機関
- (b) 承認された手形交換所
- (ba) シンガポールで設立された認可済み手形交換所
- (c) キャピタル・マーケット・サービス・ライセンス保有者
- (d) シンガポールで設立され、認定市場運営者
- (e) 証券先物法 286 条に基づき認可され、かつ、ユニット型投資信託として設立された集団投資スキームの受託者として行為を行うことを、同法第 289 条に基づき承認された者（それぞれを「金融機関」という。）

同通知は、上記機関における全顧客の情報に適用される。

キ 小規模事業者の取り扱い

テクノロジー・リスク・マネジメントに関する通知において、小規模事業者に関する特別な規定は定められていない。

ク 国際的な情報移転に関する規定

テクノロジー・リスク・マネジメントに関する通知において、国際データ移転に関する規定は定められていない。

⑨ 公務機密法（第 213 章）

ア 法令の概要

公務機密法（第 213 章）は、当初 1935 年に導入され、直近では 2012 年に改正されたもので、公的書面及び公的情報の公表について定めたものである。具体的には、スパイ行為の禁止、スパイ行為に対する制裁、許可を得ない撮影の禁止を定めるとともに、報告書の改ざん及び偽造文書の規制、並びに外国代理人との接触、及び軍人又は警察官の妨害の禁止などを定めている。同法では、外国勢力又は敵にとって有益となり得る情報の開示及び収集を禁止するという形で、情報保護について言及されている。

イ 個人情報の定義

第 3 条は、「外国勢力又は敵にとって直接又は間接的に有益である若しくは有益となり得ると考えられる又は有益となることが企図されている、秘密の公的隠語、合言葉、パスワード、写真、描写、計画、モデル、記事若しくはメモ又はその他の書類若しくは情報」を入手、収集、記録、公表又は他の者に伝達することを禁止している。

ウ 主な規制・権利の内容

第 3 条は、公的役職に就いていること、又は就いていたことを理由に秘密情報として委託された情報について規制している。同法は、いかなる者も、外国勢力又は敵にとって直接又は間接的に有益である若しくは有益となりうると考えられる又は有益となることが企図されている一切の情報を入手、収集、記録、公表又は他の者に伝達することを禁止している。

第 5 条は、当該個人が情報に対して適度な注意を払い、その処分が法的に義務づけられる場合は当該情報を保持してはならない旨定めている。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

公務機密法には、データ違反報告義務は含まれていない。

オ 安全管理措置

公務機密法には、安全管理措置に関する規定は定められていない。

カ 適用範囲

第 3 条の開示制限は、公的役職に就いていること、又は就いていたことを理由に秘密情報として委託されたすべての情報について適用される。

キ 小規模事業者の取り扱い

公務機密法において、小規模事業者に関する特別な規定は定められていない。

ク 国際的な情報移転に関する規定

公務機密法において、国際データ移転に関する規定は定められていない。

⑩ 統計法（第 317 章）

ア 法令の概要

統計法（第 317 章）は、1973 年に施行されたもので、政府機関による統計の収集及び利用について定められたものである。具体的には、情報収集の権限及び機関、統計の収集に関連する違反行為（統計官のなりすまし及び情報の公表を含む）、並びに同法違反に対する刑罰について定めている。同法では、同法に基づき収集された情報の違法な公表を禁止するという形で、情報保護について言及されている。

イ 個人情報 の定義

第 7 条(1)は、統計局長（Chief Statistician）又は第 5 条及び第 6 条に基づく研究統計団体のディレクターが「個人を特定可能な形式で」入手した「一切の事項又は情報」の開示を禁止している。第 7 条(2) (a)乃至(e)は、上記の禁止規定から、「(a)いかなる者も特定しない統計としての事項又は情報、(b) (i) 公的機関又は(ii)別紙 3 に特定されたクラスに該当するその他一切の者に対する匿名のマイクロデータとしての事項又は情報、(c) 本法に基づく違反に係る手続又は当該手続の報告を目的とする事項又は情報、(d) 機関が提供する製品又はサービス、機関の従業員数若しくは住所に関連する一般的性質を有する事項又は情報、又は(e)既に公知となっている事項又は情報」を除外している。

第 2 条は、「匿名化されたマイクロデータ」を「いずれかの者に付随する事項又は情報で、かかる者の身元が当該事項又は情報から容易に判別又は確認されないよう当該事項又は情報を統計的形式その他によって表すことによりかかる者の身元を隠匿又は保護した状態のもの」と定義している。

ウ 主な規制・権利の内容

統計法は、同法に基づき取得された個人情報規制している。第7条(1)は、統計局長又は同法に基づく研究統計団体のディレクターが「個人を特定可能な形式で」入手した「一切の事項又は情報」の開示を禁止している。かかる規定により、「匿名化されたマイクロデータ」は、同法の保護対象から除外される。情報の保有者は、該当の個人に対する通知を行い、かつ、大臣が適切な期間が経過したと判断する場合を除き、当該情報を開示してはならない旨同法により規定されている。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

統計法には、データ違反報告義務は含まれていない。

オ 安全管理措置

統計法には、安全管理措置に関する規定は定められていない。

カ 適用範囲

第7条(1)の開示制限は、統計局長又は研究統計団体のディレクターによって取得された一切の情報について適用される。

キ 小規模事業者の取り扱い

統計法において、小規模事業者に関する特別な規定は定められていない。

ク 国際的な情報移転に関する規定

統計法において、国際データ移転に関する規定は定められていない。

⑪ 法定機関及び政府系企業機密保護法（第319章）

ア 法令の概要

法定機関及び政府系企業機密保護法（第319章）は、1983年に施行されたもので、法定

機関及び政府系企業の情報の秘密保持について定めたものである。具体的には、法定機関又は政府系企業のメンバー又は旧メンバー等が、役職を理由に入手した秘密の若しくは機密の書類又は情報の開示を禁止し、その違反行為の刑罰を定めている。

イ 個人情報の定義

第 3 条は、別紙に記載された法定機関又は政府系企業の現職メンバー若しくは旧メンバー、役員、従業員又は代理人が、当該メンバー、役員、従業員又は代理人としての役職を理由に入手した「一切の秘密の若しくは機密の書類又は情報」の開示を禁止している。

ウ 主な規制・権利の内容

第 3 条は、公的役職に就いていること、又は就いていたことを理由に秘密情報として委託された情報について規制している。イで述べたとおり、同条は、別紙に特定する法定機関又は政府系企業の現職メンバー若しくは旧メンバー、役員、従業員又は代理人が、「当該メンバー、役員、従業員又は代理人としての役職に就いていることを理由に入手又はアクセスした一切の秘密又は機密の書類又は情報」の開示を禁止している。

同法は、当該個人が情報に対して適切な注意を払い、その処分が法的に義務づけられる場合は当該情報を保持しないよう定めている。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

法定機関及び政府系企業機密保護法には、データ違反報告義務は含まれていない。

オ 安全管理措置

法定機関及び政府系企業機密保護法には、安全管理措置に関する規定は定められていない。

カ 適用範囲

第 3 条の開示制限は、同法の別紙に具体的に記載された法定機関又は政府系企業の現職メンバー若しくは旧メンバー、役員、従業員又は代理人に適用される。

キ 小規模事業者の取り扱い

法定機関及び政府系企業機密保護法において、小規模事業者に関する特別な規定は定められていない。

ク 国際的な情報移転に関する規定

法定機関及び政府系企業機密保護法において、国際データ移転に関する規定は定められていない。

(3) 監督機関・第三者機関

① 個人情報保護委員会 (Personal Data Protection Commission, PDPC) ¹⁹

PDPC は、PDPA 第 5 条に基づき 2013 年に設立された、PDPA 枠組を管理する主たる規制当局である。PDPC は、データ保護に関する政府への助言、PDPA の管理、研究の実施及びデータ保護の促進等、多数の機能を備えている。

PDPA は、最大 17 名から成る PDPC の、大臣による任命について規定している。また、大臣は、PDPC の予算を管理し、PDPC に対して管理上の支援を行う管理機関を任命することができる。

なお、大臣は、PDPA における諮問委員会を任命する権限を有する。また、大臣は、外国のデータ規制当局と協業契約を締結することができる管理機関を任命する権限を有するとともに、PDPA に基づく様式及び手続に関する規制を作成する権限を有する。

<連絡先>

460 Alexandra Road #10-02 PSA Building

Singapore 119963

電話番号: +65 6508 7333

FAX 番号: +65 6273 7370

<幹部>

PDPC

Commissioner	Tan Kiat How
Executive Chairman (DPAC)	Leong Keng Thai
Deputy Commissioner	Yeong Zee Kin

諮問委員会

¹⁹ <https://www.pdpc.gov.sg/>

Executive Chairman	Leong Keng Thai
--------------------	-----------------

PDPC は、PDPA 施行以来、PDPC の運用及び DNC 登録簿に関するガイドラインの発行を通じて PDPA 枠組の確立に注力するとともに、PDPA に基づく研修及び特に SME が法律を遵守するための支援、ワークショップの開催及び法令遵守のためのツールやサービスの公表に注力している。PDPC はまた、近時、マーケティング活動における同意の取得及び撤回に関するガイドライン並びにデータ保護及びデータ違反管理に関する指針を発表した。

PDPC は、同法の施行以来、データ保護に関する執行について警告及び詳細を複数回発行している。例えば、PDPC は、最近では 2017 年 7 月に、データ保護規制に対する違反を犯した 2 社の会社に対して行われた訴えに対する判決の根拠を公表した。1 社は、乗客データを含んだ乗員乗客名簿の適切な処理を怠った事案であり、もう 1 社は、顧客宛ての請求書の裏面に別の顧客の詳細を印刷して送付した事案であった。いずれの会社も、これらの事案において PDPA 第 24 条に違反するものと判断された。

② シンガポール情報通信メディア開発庁 (Info-communications Media Development Authority of Singapore, IMDA) ²⁰

IMDA は、シンガポール・メディア開発庁法 (第 172 章) に基づき 2003 年 1 月 1 日に設立されたもので、PDPA 第 5 条に基づき PDPA の管理組織として任命されている。

IMDA は、MCI の法定の意思決定機関である。同庁は、法定の意思決定機関として、MCI の方針及び指示等、MCI の権限に服する。同庁は、PDPC と並び、シンガポールにおけるメディアに関する国家規制当局である。同庁の 2015/2016 年間報告によると、2016 年 3 月 31 日を末日とする 2015/2016 会計年度における IMDA の費用総額は、営業費用について 67,445,000 シンガポールドルに達しており、同年の政府助成金総額は、55,459,000 シンガポールドルに達している。

<連絡先>

10 Pasir Panjang Road #10-01 Mapletree Business City
Singapore 117438
電話番号: +65 6377 3800
電子メール: info@imda.gov.sg

<幹部>

Board of Directors	Chan Yeng Kit, Janet Ang, Lily Chan, Chey Chor
--------------------	--

²⁰ <https://www.imda.gov.sg/>

	Wai, Robert Gilby 及び Vivek Kumar 他 12 名
Senior Management	Tan Kiat How, Leong Keng Thai, Aileen Chia, Philip Heah, Tan Kiat How 及び Philip Heah

(4) 最近のトピック

① 制度改正の検討状況

2017年7月10日、シンガポール情報通信省 (Singapore Ministry of Communications and Information) 及びシンガポール・サイバーセキュリティ委員会 (Cyber Security Agency of Singapore) は、共同でサイバーセキュリティ法案をパブリックコメントに付した。パブリックコメントに関する報告書は、同年11月13日に公表された。

また、PDPCにおいて、2017年8月から9月にかけて、一定のデータ違反の報告を義務化する法律の改正案に関するパブリックコンサルテーションが実施された。

なお、前述のとおり、APECのCBPR及びAPECプライバシー取扱者認可制度へのシンガポールの加盟が2018年2月に認められている。

② 個人情報に関連した主要な裁判例

PDPCは、2017年3月21日、ある会社について、同社スタッフ及びボランティア研修生によるWhatsAppのチャット履歴を、同人らからの同意の取得及び同人らに対する開示目的の通知を行わずに開示した件に関する捜査について[2017]SGPDPC3判決を公表した。かかる開示が意図的に行われ、かつ、非常にセンシティブな情報 (sensitive information) であったが、これが従業員及び元従業員間の紛争に関連して開示されたものであったとの理由から、PDPCは、当該組織に対する是正措置又は罰金支払の命令を発行することを拒否する決定を行った。PDPCは、その代わりに、同組織によるPDPA第13条及び第20条に基づく義務違反について同組織に警告を発行することを決定した。

8. タイ

(1) 制度概要

① 法体系の概要

タイにおいては、現在、個人情報保護（the personal information protection, การคุ้มครองข้อมูลส่วนบุคคล）に関する法律の制定が検討されており、個人情報保護法草案（the Draft Bill of Personal Information Protection, ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล）（以下「個人情報保護法案」という）が存在するが、内閣の閣議決定はまだされていない。基本法の性格を有する個人情報保護法はまだ存在しないが、タイにおいても個人情報は法的に保護されている。

個人情報保護の根本的な土台は、タイ王国憲法である。タイ王国憲法（the Constitution of the Kingdom of Thailand, รัฐธรรมนูญแห่งราชอาณาจักรไทย）第32条（2017年4月6日制定）はプライバシー権を保障している。公共の利益による必要性のために制定された法律上の規定による場合を除き、いかなる方法によってもプライバシー権を侵害ないしこれに影響を与える行為、また個人情報を利用する行為は認められない。

タイの民商法典（Civil and Commercial Code (CCC), ประมวลกฎหมายแพ่งและพาณิชย์）は個人情報保護の対象とする。すなわち、データの「公開」もしくは「移転」がデータ主体に損害を与える場合、不法行為に該当する。このことから、タイにおいては、一般的なビジネスの契約書に、「個人情報を開示する前に本人から同意を得なければならない」という趣旨の条項が規定されることが多い。また、データの取扱いが秘密漏えいや名誉棄損に該当する場合、刑法（Penal Code, ประมวลกฎหมายอาญา）が適用される。

タイにおいては、各事業を規制する特別法において、個人情報が保護される。個人情報保護を保護する特別法としては、金融機関事業法（Financial Institution Business Act, พระราชบัญญัติธุรกิจสถาบันการเงิน）、国民健康法（National Health Service Act, พระราชบัญญัติสุขภาพแห่งชาติ）、電気通信事業法（Telecommunication Business Act, พระราชบัญญัติกิจการโทรคมนาคม）及び信用情報事業法（Credit Information Business Operation Act, พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต）を挙げることができる。

また、タイにおいては、公的情報法（Official Information Act）が存在し、これによって、公的機関が保有する個人情報の開示が定められている。

② 民間部門に適用される主な法令

民間部門における個人情報保護に関する法律及び規制は、産業ごとに、以下の通り分類することができる。

- ・ まず、金融機関事業法 (Financial Institution Business Act) は、一般的に金融機関 (同法第 4 条によれば、金融機関は商業銀行事業、ファイナンス事業、及びクレジットフォンシェ事業を指す) の事業を監督し、規制している。この点について、同法第 154 条は、同法により与えられた権限に基づく事業において取得した顧客の秘密情報を漏えいした者に対し、罰則を科している。
- ・ 次に、電気通信事業法 (Telecommunication Business Act) 第 50 条は、電信通信事業者が事業運営にあたり、電気通信を介した利用者の個人情報保護、プライバシー権、コミュニケーションの自由に関する方針を遵守する義務を定めている。
- ・ その他、信用情報事業法 (Credit Information Business Operation Act) は、信用情報を取り扱う事業者を規制する法である。同法も個人情報の開示及び保存の禁止に関し定めている。

③ 公的部門に適用される主な法令

公的部門における個人情報を規制する主要な法律は、公的情報法 (Official Information Act) であり、情報へのアクセシビリティを確保するために、主に国家機関に対し一部特定情報の開示を求めており、個人情報を管理する国家機関の責任を規定している。同法第 3 章は個人情報保護に関する規定である。

公的部門における個人情報保護に関する他の規制は、国家による電子取引の基準及び手続きに関する勅令 (Royal Decree on Criteria and Procedure in Making Electronic Transactions by State, B.E. 2549 (2006)) に基づき発布された、電子取引委員会の通知 : 国家機関による個人情報保護の政策及び運用に関する指針 (ガイドライン) (Notification of Electronic Transactions Commission, Policy and Practice Guidelines for Personal Data Protection of State Agencies, B.E. 2553 (2010)) である。国家機関との電子取引又は政府機関による電子取引に関し、その安全性及び信頼性を確保するため、この規定が適用される。また国家機関は、個人情報保護に関する書面による政策及び運用指針を提供しなければならない。

(2) 主な法律の概要

① 金融機関事業法 (Financial Institution Business Act, B.E. 2551 (2008))

ア 法律の概要

金融機関事業法は、以下の目的により制定され、2008 年 8 月 4 日に施行された。

「商業銀行事業、ファイナンス事業、及びクレジットフォンシェ事業に対する監督及び

規制は、案件の内容によって、それぞれ商業銀行、ファイナンス事業、証券事業、及びクレジットフォンシェ事業に関する法令によって行われていたが、金融機関の事業運営は、同じ基準で行われるべきである。また、タイは以前、深刻な経済危機に見舞われ、それは金融機関に直接的な衝撃を与え、国民及び預金者の金融機関システム全体への信頼にも影響を及ぼした。従って、金融機関の監督及び規制の方法をより効果的に改善し、商業銀行、ファイナンス事業、証券事業、及びクレジットフォンシェ事業に関する法律を改善して、統制及び監視が同じ基準で行われるように一つの法律にまとめ、同時に関連犯罪行為に対する罰則もより適切な内容に改正すべきである¹⁾。

金融機関事業法は、その金融機関の行動についての規制の一つとして、顧客の秘密情報の開示を禁止している。

イ 主な規制・権利の内容

金融機関事業法第 154 条は、「法律上与えられた権限及び義務に基づき金融機関の事業に関する情報を取得し、かかる情報が通常の場合において開示してはならないものであるとき、かかる情報を他人に漏えいしてはならない。」と規定し、罰則を設けている。違反者は、1 年以下の懲役ないし 10 万バーツ以下の罰金、ないしその併科とされる。

ウ 適用範囲、適用除外内容

本法は、金融機関事業における全ての情報を対象とし、これが通常の場合においては第三者に開示ないし漏えいしてはならないとして、かかる情報を保護している。違反者に対しては懲役及び罰金刑が科されるが、既に公共に開示された金融機関の顧客の秘密情報の開示、及び顧客の同意を得たうえでの秘密情報の開示については除外される(第 154 条)。

② 信用情報事業法 (Credit Information Business Operation Act, B.E 2545 (2002))

ア 法律の概要

信用情報事業法は、以下の目的により制定され、2003 年 3 月 14 日に施行された。

「本法は、金融機関が顧客に融資ないし信用供与を行う際、顧客の財務実態、債務返済の履歴、顧客の諸記録、顧客の他の金融機関に対する残債務額に関し、十分な情報が必要であることから発布された。過去には、金融機関による融資又は信用供与の延長が、十分な情報を取らずに行われていた。そのために、不良債権が増え、当該金融機関及び金融機関システム全体の安定性に問題を引き起こした。加えて、現在の信用情報事業の運営に関

¹⁾ 金融機関事業法の備考 (Remarks) に同法の目的が記載されている。

しては、信用情報取引の規則、手続き及び条件を規定する法律も、情報の対象者本人を保護する個別法もない状態である。従って、この法律を制定する必要がある。」²

信用情報事業法は、信用情報事業の運営が許可された会社に対し、個人情報の本人の同意を事前に得ない限り、その情報を開示又は提供することを禁止している。また、信用情報会社、情報管理者、及び情報処理者は、障害、遺伝に関わる情報、捜査対象ないし刑事裁判中の人物の情報、ないし当局機関の通知に規定されるその他いかなる情報にも関連しない、自然人の情報を保管することが禁じられる。

イ 個人情報の定義

信用情報事業法は、「個人情報」を直接には定義していない。第3条において「信用情報」、「情報処理」、「禁止情報」の定義に関し、以下のように定めている。

「信用情報」とは、信用供与の申請を行う顧客に関する以下の事実を意味する。

(1)信用供与を申請する顧客の同一性と資格を示す事実:

(a) 自然人の場合、個人の氏名、住所、生年月日、(社会的)地位、婚姻関係、職業、住民証明書番号、公務員証明書番号、旅券番号、納税者登録番号(ある場合)をさす。

(b) 法人の場合、法人の名称、所在地、法人登録番号又は納税者登録番号をさす。

(2)信用供与を申請する顧客の、信用申請及び承認履歴、融資への返済履歴(クレジットカードによる商品ないしサービスへの支払履歴を含む)」

「情報処理」とは、情報を取り扱う一切の行動をさす。例えば、収集、記録、編集、保存、修正、回復、使用、開示、印刷、アクセス、削除又は情報の破壊が該当し、信用マーク及び統計レポートの準備及び開示を含む。」

「禁止情報」とは、サービスの利用、信用供与の申請とは関係がない自然人の情報、もしくは情報主体の感情に影響を与え、情報主体の権利及び自由を侵害する可能性があり、もしくは明らかにそれに影響を与える情報をさす。その内容は以下の通りである。

(1) (身体等)障害の記述;

(2) 遺伝に関する記述;

(3) 捜査ないし刑事裁判の対象となっている人物の情報;

(4) 委員会の通知に記載されたその他のいかなる情報。」

ウ 主な規制・権利の内容

信用情報事業法は、主に信用情報事業の運営を規制する法である。規制内容は、金融機関による個人への融資ないし信用供与の審査のための、金融機関への個人の財務関連情報

² 信用情報事業法の備考(Remarks)に同法の目的が記載されている。

の提供に関連している。

個人情報保護に関しては、取得した信用情報（個人情報）の保護を確保するため、信用情報会社の義務を規定している。信用情報会社の義務は、具体的には以下の通りである。

- ①信用情報会社、情報管理者（information controller）、情報処理者（information processor）は、障害に関する情報などの「禁止情報」（prohibited information）³を保存・蓄積（store）することができない（第10条）。
- ②信用情報会社は、情報を処理する⁴にあたり、少なくとも信用情報事業法17条所定のシステム及び要件を設定しなければならない。例えば、保管された情報の分類システム、情報改訂システム、情報の機密と安全（確保）システム、等である。
- ③信用情報会社は、そのメンバー（member, สมาชิก）と呼ばれる金融機関⁵、もしくは、サービス利用者（service user, ผู้ใช้บริการ）に対して、情報を開示又は提供する場合、情報主体から同意を既に得た場合を除き、その都度本人の事前の同意を得なければならない（第20条）。かかる同意は、信用情報保護委員会の通知（メンバー及びサービス利用者への情報開示及び提供、情報対象者の同意⁶）に従い付与されなければならない。ただし、以下の場合においては、信用情報会社は、情報主体から事前の書面による同意がなくても、その情報の開示及び提供が認められる。しかし、この場合でも、書面で本人にこれを通知しなければならない。

（ア）裁判所命令ないし令状に基づく場合又は一般に公開された訴訟に係わる情報

（イ）尋問担当官から金融事業に関する刑事犯罪についての尋問を目的とした通知書を受領した場合で、かつ当該担当官が当該捜査を担当していること

（ウ）財務省、タイ中央銀行、及び証券取引委員会から、関連法令に基づき、金融機関の監督又は検査を目的とした通知書を受領したとき

（エ）第二次抵当公社を規制する法令に基づき第二次抵当公社から、証券化事業を営む

³ 信用情報事業法第3条（定義規定）は以下の内容を定めている。

：「禁止情報」は、サービスの利用者やクレジットの申請とは関係がない自然人の情報、もしくは情報主体の感情に影響を与え、情報主体の権利及び自由を侵害する可能性があり、もしくは明らかにそれに影響を与える情報をさす。その内容は以下の通りである。

- (1) (身体等)障害に関する説明；
- (2) 遺伝に関する説明；
- (3) 捜査ないし刑事裁判の対象となっている人物の情報；
- (4) 委員会の通知に記載されたその他の情報。

⁴ 同法第3条は以下の内容を定めている。

「情報処理とは、情報を取り扱う一切の行動をさす。例えば、収集、記録、編集、保存、修正、回復、使用、開示、印刷、アクセス、削除又は情報の破壊が該当し、信用マーク及び統計レポートの準備及び開示を含む。」

⁵ 信用情報会社がメンバーとして認めた金融機関（信用情報事業法第3条）

⁶ Notification of Credit Information Protection Committee, the Disclosing and Providing Information to Member and Service User and the Consent of Information Subject

特別目的事業体を規制する法律に基づき証券化事業を営む特別目的事業体から、関連法令に基づき証券化のために提供された資産の評価を行う目的のもと、通知書を受領したときで、状況に応じて必要な場合（信用情報保護委員会の承認も必要となる）。

(オ)タイ資産管理公社を規制する法令に基づきタイ資産管理公社から、金融機関の資産管理会社を規制する法令に基づき金融機関の資産管理会社から又は資産管理会社を規制する法令に基づき資産管理会社から、それぞれ関連法令に基づき、購入され又は譲渡された資産の価格査定を行う目的のもと、通知書を受領したときで、状況に応じて必要な場合（この場合も、信用情報保護委員会の承認が必要となる）。

最後に、信用情報事業法は、個人情報保護のため、情報主体に権利を認めている。例えば、いかなる情報が保管されているかを知る権利、検証する権利、訂正請求権、誤った情報に対する異議申立権等がある。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

第 18 条に従い、信用情報事業のメンバーには、その顧客の情報をメンバーとして属する信用情報会社に送信し、送信日から 30 日以内に、当該顧客に対し書面にて送信した情報を通知する義務がある。

オ 安全管理措置に関する規定

情報処理に関して、第 17 条 (3) は、信用情報会社もしくは同会社に任命された人物は、情報の乱用を防ぎ、権限無く情報にアクセスされるのを防ぐために「情報の秘密及び安全システム」を策定し、また、情報が不適切に又は許可なく変更され、損傷を受け、破壊されるのを防ぐためのシステムを策定しなければならないと規定する。更に、かかるシステムは、情報処理に関するシステム及び要件設定についての規則、手続き及び条件に関する信用情報保護委員会の通知を順守したものでなければならない。同通知は、以下のように要件を規定する。

(ア) 認証システム（ユーザーID 及びパスワード）を必要とする。

(イ) メンバーないしサービス使用者のアクセス/訂正は記録される必要がある。

(ウ) 信用情報会社の情報基盤に接続したコンピュータ及び他の装置は、安全システム及び警報システムを設定しなければならない。

カ 適用範囲、適用除外内容

信用情報事業法は、信用情報をメンバーないしサービス利用者に提供するべく信用情報の管理及び処理をしている信用情報会社に適用される。財務省が本法の適用について責任

を負っている。

キ 紛争処理手続き

個人情報保護に関する紛争解決手続きについては、第 25 条において規定され、情報対象者は信用情報保護委員会に申立て、信用情報の正確性についての情報対象者及び信用情報会社間の争いについて解決を求めることができる。

③ 電気通信事業法 (Telecommunication Business Act, B.E. 2544 (2001), พระราชบัญญัติกิจการโทรคมนาคม)

ア 法律の概要

電信通信事業者の義務として、国家電信通信委員会が利用者の個人情報及びプライバシー権保護のために制定した方針を遵守する義務を規定している。更に同法は、電信通信を介して伝達された情報を違法に開示した全ての者に対し刑事責任を課しており、2002 年 3 月 17 日に施行された。

イ 個人情報の定義

第 1 条は、「個人情報は利用者の電気通信番号、直接的ないし間接的に個人を識別できる利用者に関する事実及び詳細情報、サービス情報、電気通信番号、利用者による電気通信の利用を含む。但し、電気通信ネットワークの管理目的、通信目的、免許を取得した運営者による事業運営目的のために、必要な技術的情報を除く。」と定めている。

ウ 漏えい等事案発生時の本人及び監督機関等への報告義務

第 50 条は、監督当局及び電気通信事業被免許者の義務として、委員会もしくは被免許者が通信手段によってサービス利用者の個人情報保護ないしプライバシー権の侵害を発見した場合、かかる侵害を除去し、これを情報主体であるサービス利用者に迅速に報告しなければならないと定めている。

エ 国際的な情報移転に関する規定

電気通信事業法のもと発布された、電気通信利用者の個人情報保護対策に関する通知は次のように定める。免許を受けた電気通信事業者による個人情報の移転ないし送信は、(i) 利用者による同意がなければならない、(ii) 当該事業者の電気通信事業を行う目的に基づ

くものでなければならない、(iii)本通知における規制に従うものでなければならない（通知第3条(1)(2)(3)）。加えて、通知第5条は更に、情報の海外送信ないし移転を規制する通知が権限ある委員会によって発せられることがあると規定する。

オ 紛争処理手続き

電気通信事業法に関する紛争解決手続きは、同法第5章（サービス利用者の権利）に規定されている。被免許者による電気通信サービスの提供が原因で、困難に陥り、又は損害を被る者は、権限のある委員会に対し書面により申立てを行う権利を有する。委員会による申立ての審査期間中、申立人から要求のあった場合、委員会は、同法第45条に基づき、被免許者に対し、一時的に、申立人の損害を回復する何らかの行為を求める権限を有する。

委員会が、被免許者が法律、免許付与の条件又はサービス提供に関する契約を侵害する行為を行ったとみなす場合、又は、サービス提供の適切な基準に満たない行為を行ったとみなす場合（この場合、個人情報に関する保護及び安全対策の基準を参照することとなる）⁷、委員会は本法第46条に基づき、被免許者に対し、特定の期間内に修正措置を講じるよう命令する権限を有する。

個人情報保護の紛争解決手続きについては、本法第50条が次の手続きを明記している。個人情報に関連する利用者保護対策に関して、サービス利用者の権利を侵害する者がいると考えられる場合、被免許者又は委員会は、かかる侵害を阻止する行動をとり、利用者迅速に知らせなければならない。更に、国家電子通信委員会の通知：個人情報、プライバシー権、電気通信手段によるコミュニケーションの自由に関連した、電気通信サービス利用者の権利を保護するための方針の第17項もまた、サービス利用者の申立ての権利について次のように強調している。「サービス利用者は、個人情報、プライバシー権、電気通信手段によるコミュニケーションの自由が侵害された場合、サービス利用者の申立ての受領及び審査のための手続きに従って、申立てを提出することができる」⁸。

④ 2006年5月18日発布の国家電気通信委員会の通知：電気通信を介した利用者の個人情報保護、プライバシー権、コミュニケーションの自由に関する方針（Notification of the National Telecommunications Commission Re: Measures for Protection of Telecommunications Service Users' Rights Related to Personal Information, Privacy

⁷ 国家電気通信委員会の通知：個人情報、プライバシー権、電気通信手段によるコミュニケーションの自由に関連した、電気通信サービス利用者の権利を保護するための方針（2006年5月18日発布）・第5章（被免許者の義務）

⁸ 国家電気通信委員会の通知：個人情報、プライバシー権、電気通信手段によるコミュニケーションの自由に関連した、電気通信サービス利用者の権利を保護するための方針（2006年5月18日発布）・第17項

Rights and Freedom to Communicate by Means of Telecommunications (issued on the 18th day of May B. E. 2549 (2006))

ア 主な規制・権利の内容

第3項において、電気通信に関する個人情報処理の方針について次のように定めている。電気通信被免許者は、サービス利用者の同意があり、電気通信事業運営のために利益となり、通知記載の基準に従う場合にのみ、個人情報を処理することができる。しかし、上記基準については第4項に以下の例外が定められている。電気通信被免許者は、(1) 国家安全保障法のもと、もしくは人々の平和及び秩序ないし道徳を維持するために、政府機関ないし政府職員に個人情報を開示することができる。(2) サービス利用者の生命、身体ないし健康への危害を防止し、又は対処するために必要な場合、個人情報を活用ないし開示することができる。(3) 国家電気通信委員会 (NTC) に個人情報を転送することができる。

しかし、電気通信被免許者は、通知第7項において、サービス利用者の機微情報を収集してはならないとされている。機微情報には、身体的障害（利用者の利益のためでない場合）、遺伝的特徴、利用者の感情に悪影響を及ぼし、又は権利及び自由に損害を及ぼす可能性のある、もしくは明白に影響を及ぼすいかなる情報も含まれる。

イ 安全管理措置に関する規定

国家電気通信委員会は、電気通信事業法⁹によって、個人情報、プライバシー権及び電気通信手段によるコミュニケーションの自由に関する利用者の保護のための方針を設定することが求められる。被免許者は、第1段落における委員会によって定められた方針に従う義務を負う。

上記委員会による方針に関して、通知第5章において、電気通信事業の被免許者に対し義務を課す、個人情報に関する安全管理対策について規定されている（国家電気通信委員会によって電気通信事業の免許を付与された被免許者で、電気通信事業法が施行される前に TOT 公開株式会社ないし CAT 電気通信公開株式会社から委任、移譲、請負により権利を得た者を含む）¹⁰。例えば第10項において、被免許者は、技術的及び内部組織的運営の双方の側面から、各種の電気通信サービスに適した、個人情報に関する保護及び安全対策を制定しなければならないとされている。

特に、個人情報に関する保護及び安全対策の技術的側面については、少なくとも、(1) 個人情報の安全を維持するために使われるエンコード及びデコードシステムは、少なくとも毎3か月おきに修正されなければならない、(2) 安全システムのレベルは、技術の発展

⁹ 電気通信事業法第50条

¹⁰ 本通知第1条

に伴い発生するリスクに合わせて適切に調整されなければならない。

第 11 項によると、被免許者は電気通信手段によるコミュニケーションの秘密性を高めなければならない。この点に関し、被免許者は、以下の行為を行うことが禁止され、また以下の行為を除去する保護システムを構築しなければならない。(1) 手段を問わず、個人が伝達した信号の盗聴、調査、傍受ないし電気通信によるメッセージの開示。但し、国家安全法の規定によってなされる場合、もしくは平和及び秩序、公衆道徳を維持するためになされる場合、また各法律の定める手続きに従いなされる場合を除く。(2) 情報の意味を変える目的をもったいかなる行為。

更に、第 15 項によって、被免許者は、サービス利用者の個人情報に関する権利保護、プライバシー権、電気通信による伝達の自由のために、本通知及び関連法規に従った基準を設定しなければならず、委員会に提出して事前の承認を得、その後サービス利用者に通知し、一般に公開しなければならない。

ウ 適用範囲、適用除外内容

電気通信サービス利用者の個人情報は、容易かつ迅速に多数の人々に使用され拡散される可能性があり、これによりプライバシー権及び電気通信手段によるコミュニケーションの自由に悪影響が及ぶため、国家電気通信委員会 (NTC) は、電気通信手段による個人情報に関連した電気通信サービス利用者の権利を保護するため、法的手段を定めた。

本通知は、特に電気通信事業者に適用され、NTC によって電気通信事業の免許を付与された被免許者、及び権限ある委員会から委任、移譲、請負により権利を得たその他のいかなる事業者も含む。本通知は、個人情報、プライバシー権、電気通信手段によるコミュニケーションの自由に関連する事項に関する、電気通信事業利用者の個人的権利を保護するために特別の適用範囲を設けている。

⑤ 2016 年電子取引委員会の通知：電子支払サービス事業遂行における要件、手続き、条件 The Notification of Electronic Transactions Commission Re: Requirements, Procedures, and Conditions for Undertaking Electronic Payment Service Business B. E. 2559 (2016)

ア 安全管理措置に関する規定

第 11 条は、本法において定義づけられたサービス提供者に対し、顧客情報のデータプライバシー、データ分類、データへのアクセスについての方針を設定するよう特定の義務を課している。加えて、サービス提供者は、信頼性のあるデータ保有手続きを整備し、権限

のない者が保管されている顧客情報にアクセスないし改ざんすることを防がなければならない。

加えて、第 12 条は、個人情報の公開の禁止及び例外について規定している。同条によれば、サービス提供者は顧客の個人情報をサービス期間中及びサービス使用終了後においても公開しないことによって、秘密情報として保護しなければならない。但し、以下の場合を除く。

- (ア)顧客の許可を得た情報の開示。当該許可は、サービス提供者の定める書面ないし電子的方法によることができる。
- (イ)捜査ないし裁判の目的による情報の開示。
- (ウ)サービス提供者の会計検査官に対する情報の開示。
- (エ)法律上の要請に基づく情報の開示。
- (オ)タイ中央銀行による決済システムの監督のために有益な情報の開示。

イ 紛争処理手続き

電子支払サービス事業に関する紛争解決手続きは、第 15 条において次のように規定されている。通知において定義づけられたサービス提供者は、顧客から申立てないし紛争を受領した場合、以下の処置をとらなければならない。また以下のように解決のための時間枠を設定しなければならない。

- (ア)顧客からの申立て受領のための回線及び手段を設定する。少なくとも、電話番号及び事務所の住所もしくは有効な E メールアドレスを置かなければならない。
- (イ)書面によって、解決のための過程及び手続きを設定する。サービス提供者は、申立てを審査し、解決のための経過、過程、タイムラインを、申立て受領から 7 日以内に顧客に対し通知しなければならない。
- (ウ)迅速に申立てを解決し、顧客に結果を通知する。

⑥ 国民健康法 (National Health Act B.E. 2550 (2007) , พระราชบัญญัติสุขภาพแห่งชาติ)

ア 法律の概要

個人の健康に関する情報は秘密情報であると定めており、2007 年 3 月 20 日に施行された。

イ 主な規制・権利の内容

この法律は特に、定期的に個人の健康に関する情報を保有する医療供給者ないし事業者

に関連するもので、個人の健康に関する情報の開示を禁止し、罰則の対象としている。同法第 7 条においては、個人の健康に関する情報は、情報主体（患者）の意思ないし同意による場合か、もしくは法律によって許容されている場合を除いて開示することができないとされている。しかし、第 7 条は、個人の健康情報に関する書類の譲渡については厳しく禁止しており、法律による許可ないし権限などいかなる状況においても、個人の健康情報に関する書類は、情報主体以外のいかなる者にも与えてはならないと定めている。

上記の禁止に対する違反への罰則は、6 か月以下の懲役及び/又は 1 万バーツ以下の罰金とされている。但し、第 7 条における個人の健康情報に関する違反は、示談可能な犯罪である。

加えて、第 10 条において、国家機関による公衆への健康ないし病気に関する情報の提供及び開示は、いかなる個人の権利（個人情報に関する権利を含む）も侵害する態様でなされてはならないと定められている。

⑦ 公的情報法 (Official Information Act, B.E. 2540 (1997), พระราชบัญญัติข้อมูลข่าวสารของราชการ)

ア 法律の概要

情報へのアクセシビリティを確保するために、主に国家機関¹¹に対し一部特定情報の開示を求めている。さらに、個人情報管理する国家機関の責任を規定している。すなわち、国家機関の透明性及び説明責任を明確化し、政府の方針策定及びその実施への人々の参加を支えることを目的としている。同法は、全ての公共機関に対し、市民から要請のあった全ての公的機関の情報の開示及び個人情報の保護を義務づけている。1997 年 11 月 9 日に施行された。

イ 個人情報の定義

「個人情報」は、「個人に係わるすべての詳細な情報をさす。例えば、教育、財務状態、健康記録、犯罪歴、職歴又は、個人の名前、数字、暗号、又は他の個人を特定する指紋、個人の音声録音されているテープないしフロッピーディスク、写真、また故人の個人詳細に関する情報も含む」(第 4 条)。

ウ 主な規制・権利の内容

本法における個人情報保護は、まず、本法第 21 条に基づき、いわゆる「個人」は、タイ

¹¹ ‘国家機関’とは、中央官庁、県官庁、地方公共団体、国営企業、国会の管轄下にある政府機関、訴訟審判に係る部分以外の裁判所、職業統制機関、国の独立機関及び省令で定められたその他の機関を意味する（公的情報法第 4 条）。

国籍を有する自然人、及びタイ国籍を有さないがタイに住所を有する自然人に限定されている。更に、本法 24 条に基づき、非開示情報に係わる（個人情報の）保護は、国家機関の管理する情報に限られる。しかしながら、同法は一般的に、国家機関の個人情報の管理義務を規定し、情報主体の自身の個人情報保護に関する権利を認めている。その概要は、以下の通りである。

(ア) 個人情報システムの提供に関する国家機関の義務(第 23 条)に関して、個人情報を保管し処理するシステムの提供は、当該システムが国家機関の職務に関連し、且つ必要なものである場合に限る。特に個人の利益が害される可能性のある時は、情報の収集は情報主体から直接得よう努める。個人情報システムのために、適切な安全システムを提供する。

(イ) 個人情報の開示(第 24 条)は、国家機関が自ら管理している個人情報に関し、以下の状況に該当する場合を除き、事前に、もしくは迅速に情報主体から同意を得ない限り、開示してはならないと定めている。

- a 当該機関の権限及び義務に従った使用の目的のための、当該機関内部の公務員への開示。
- b 個人情報システム設置の目的の範囲内における通常利用のための開示。
- c 計画、統計、（国勢）調査を行い、個人情報を非開示に保つ義務を負う国家機関への開示。
- d 研究又は調査のため、氏名、もしくはその個人情報に関係する個人を識別できる部分を伏せた状態での開示。
- e 当該情報の保管価値を評価する目的による、国立公文書館部及び芸術局、又は第 26 条第 1 段落における他の国家機関への開示。
- f 法律違反又は法令不遵守の防止、調査、質問ないしあらゆる法的措置をとる目的による、公務員への開示。
- g 人の生命ないし健康への危険の防止又は除去のために必要な開示。
- h 裁判所、公務員、国家機関又は法律に基づき当該情報の開示を請求する権利を有する者への開示。
- i その他、勅令に定めがある場合。

(ウ) 情報主体が自己の情報につき検査し訂正する権利(第 25 条):情報主体から書面により要求を受けた場合、情報を管理する国家機関は、当該本人による情報の検査を許可

しなければならない。情報の訂正に関しては、本法は、情報主体から要求があった場合に、訂正、変更又は削除を許可する国家機関の義務を定めていない。但し、情報主体の訂正請求が拒否された場合、本人は拒否処分を受理した日から 30 日以内に情報公開裁判所に不服申立を提起することができる。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

本法には、監督機関への報告義務に関する法的規定は存在しない。しかし、第 23 条第 3 段落において、個人情報流出し、その結果、公衆に知られる可能性が発生した場合、国家機関は、当該流出が情報の通常の使用形態に一致しない限り、情報主体に通知しなければならないと定められている。

オ 安全管理措置に関する規定

本法は、安全管理対策の詳細についての規定を特段明記していない。しかし、第 23 条(5)によれば、国家機関には、情報の不適切な使用ないし、情報の対象となる人物の権利を侵害するようないかなる情報の使用をも防ぐために、個人情報の「適切な安全システム」を策定することが求められている。

カ 適用範囲、適用除外内容

本法は、2つの重要な適用範囲を定めている。すなわち、全ての市民に対し法律により禁止されたものを除く全ての公的情報へのアクセスの自由を保障し、また全ての国家機関に対し個人情報の保護を求めている。

キ 紛争処理手続き

国家機関が、情報主体の要求に沿って個人情報を修正、変更ないし削除しなかった場合には、当該本人は情報開示裁判所に異議を申し立てることができる。

⑧ コンピュータ関連犯罪法 (Act on Commission of Offences relating to Computer, B.E. 2550 (2007), พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์)¹²

ア 法律の概要

他人のコンピュータ上のデータに対する犯罪を処罰するものである。

¹² 2007 年 6 月 18 日官報掲載、2007 年 3 月 20 日施行

同法の前文には、以下の記述がある。

「最近、コンピュータシステムは、事業運営及び人々の生活スタイルに重要な役割を果たしてきている。もし何者かが、プログラムを使ってコンピュータに誤作動を起こしたり、指示通りに実行できなくしたり、コンピュータシステムにおける他人の個人情報に違法にアクセスしたり、それを傷つけたり、改竄したり、破壊したり、もしくはコンピュータシステムを利用し、虚偽の情報やポルノ情報を流したりする等の行為を犯したら、社会、経済、及び国家安全（公序良俗を含む）に損害及び悪影響を与えることになる。従って、このような行為を予防、抑制できる措置を課す法律として、本法を發布することは有益なことである。」

イ 主な規制・権利の内容

サイバー行動は同法によって規制され、同法はいくつかのサイバー行動を禁止し、罰している。対象となる行動には以下のものを含む。アクセス者の利用のためのものではなく、特定のアクセス防止策が存在するコンピュータデータ¹³への不正アクセス（第7条）。コンピュータシステムにおける他の人物の送信中のコンピュータデータで、公共の利益や公共用途のために利用できないものを、遮断するためにあらゆる電子的手段を違法に用いること（第8条）。他の人物のコンピュータデータに対し、全体的ないし部分的に、違法に損害を与え、破壊し、改変し、修正し、加筆すること（第9条）。

重要な点は、同法は写真の形による個人情報の違法な流布行為を除外している。その代り、他人の写真を表示するコンピュータデータを一般にアクセス可能なコンピュータシステムに入力し、かかる行為が他人の評価を傷つけ、ないし侮辱、嫌悪、屈辱を与える可能性がある方法によって行われた場合、かかる行為を行った者を罰している。

これらのサイバー犯罪を犯した犯罪者には、同法に基づき重い罰金と懲役刑が科せられる。更に、上記のサイバー犯罪は、特別に規制の対象となるセクターに適用される法律及び規制違反にもなり得る。

ウ 安全管理措置に関する規定（組織的・物理的・人的・技術的措置）

本法第26条によれば、安全管理対策において、データがコンピュータシステムに入力された日から少なくとも90日間は、「サービス提供者」（他人の利益のためにコンピュータデータの保管に関するサービスを提供する者）¹⁴は「コンピュータトラフィックデータ」（コ

¹³ コンピュータデータとは、「データ、テキスト、コマンド、プログラム、その他のコンピュータシステム内に保護され処理されるもので、電子取引に関する法律に基づく電子データを含む」（コンピュータ関連犯罪法第3条）

¹⁴ コンピュータ関連犯罪法第3条

ンピュータシステムベースのコミュニケーションに関するデータであり、発信元、出発点、目的地、ルート、時間、日付、ボリューム、期間、サービスの種類ないし、他のコンピュータシステムコミュニケーションに関連するものを示すもの)¹⁵を保管しなければならない。

特に、同法に基づき発布された規制は、サービス利用者の個人情報保有に関してサービス提供者に要件を課し、特定の種類の個人情報について、保有しなければならない旨、またどのように保管すべきかについて定めている。¹⁶

エ 適用範囲、適用除外内容

本法の主な適用範囲は、違法なサイバー行動にある。サービス利用者の個人情報保護のために、サービス提供者に対しても適用され、そのコンピュータシステム内にトラフィックデータを組み込み、担当者が同システムを通して違法なサイバー行動を調査することを可能にするよう求めている。

(3) 監督機関・第三者機関

全ての規制対象産業を管轄する中央監督機関は未だ存在しないが、いくつかの産業及び政府機関については、個人情報の保護対策を管轄する監督機関が存在する。各分野の監督機関の例は以下のとおりである。

① 国家電気通信委員会 National Telecommunications Commission

ア 設置の経緯

電気通信事業法のもと、国家電気通信委員会は、利用者の個人情報、プライバシー権、電気通信によるコミュニケーションの自由を保護するための方針を策定する権限を有する。保護の方法としては、侵害状態を停止し、可能な限り早期に利用者に通知すること¹⁷、また第74条においては、電気通信事業者によって違法に伝達された他人の情報を開示した者は、2年以下の懲役又は40万バツ以下の罰金、ないしはその併科とすることが定められている。

¹⁵ 同上

¹⁶ 2007年デジタル経済社会省通知：サービス提供者によるトラフィックコンピュータデータ保有の基準

¹⁷ 電気通信事業法第50条

イ 制度の概要

国家電気通信委員会（NTC）は、独立した国家組織であり、電気通信事業に携わるための免許発行¹⁸、基本的電気通信サービス¹⁹及び利用者の個人情報、プライバシー権及びコミュニケーションの自由を保護するための対策を提供する責任を有している²⁰。加えて、NTCは合計1,256人のメンバーを有し、2016年の歳入は10,247,406バーツ、2015年は9,214,021バーツであった。

② 信用情報保護委員会 Credit Information Protection Committee, คณะกรรมการคุ้มครองข้อมูลเครดิต

ア 設置の経緯

信用情報事業法によれば、金融機関、メンバー（信用情報会社がメンバーとして認めた金融機関）、信用会社、データ所有者、情報主体の間で争いが生じた場合には、情報主体はかかる争いについて信用情報保護委員会に申し立てることができる²¹。この組織は、同法第29条に基づいて設立され、信用情報事業を監督する責任を有する。かかる権限及び義務は、同法の適用についての通知ないし命令の発布、同法に基づく申立てについての審査を含む²²。

イ 制度の概要

信用情報保護委員会は2003年3月14日に設立され、信用情報事業の監督、特に信用情報に関する申立てに対する決定について責任を有する。更に、委員会はまた、会社に対し会社の一般事項及び特定事項の双方についての報告ないし説明を命じ、また本法に従うよう通知ないし命令を発する権限を有する²³。

③ 情報公開裁判所 Information Disclosure Tribunals, ของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร

ア 設置の経緯

公的情報法第35条に基づき情報公開裁判所は設立され、個人情報に関連する当局の命令に対する異議申立てについて審査し決定する権限を有する²⁴。

¹⁸ 電気通信事業法第7条

¹⁹ 電気通信事業法第17条

²⁰ 電気通信事業法第50条

²¹ 信用情報事業法第27条

²² 信用情報事業法第30条

²³ 信用情報事業法第30条

²⁴ 公的情報法第35条

イ 制度の概要

情報公開裁判所は、専門的分野に基づき細分化されている。5つの分野があり、①国外情報及び国家安全開示、②国家経済及び金融情報開示、③社会情報、行政及び法執行開示、④医療及び公衆衛生開示、⑤化学、技術、産業及び農業情報開示²⁵。2017年の情報公開裁判所の予算は58,902,500バーツ計上され、2016年は24,839,000バーツであった²⁶。

④ デジタル経済社会省 The Ministry of Digital Economy and Social

コンピュータ関連犯罪法によって、同法の執行を担う権力を持つ役職を任命できる権限がデジタル経済社会省に与えられている²⁷。義務の例としては、申立て、裁判所への証拠の提出、また本法、知的財産法、又は公衆道徳違反に基づくコンピュータ情報の流布の停止ないし削除を要求することが該当する²⁸。

⑤ 個人情報保護委員会 Personal Data Protection Commission

個人情報保護法案が完全に施行されるときに、個人情報保護委員会は設立される。個人情報保護法案第13条のもと、委員会は個人情報保護法案の目的を達成するための権力及び義務を有することになる。例えば、個人情報の維持及び保護のための戦略的計画を構築する義務、個人情報保護に関する対策を決定する権力、公共機関を統制し監視する義務、申立てについて調査する義務である。

更に、個人情報保護法案第37条に基づき、情報主体の申立てを受領したとき、委員会は、個人情報管理者（個人情報の管理に関して決定（本法に基づく収集、使用、開示を含む）を下す権力及び義務を有する者²⁹）に対して、情報主体に損害を加える疑いのあるいかなる行為についても、それについて立証するよう命じることができる。立証の結果、関係者に損害を当たらせようことが認められる場合、委員会は、かかる行為を禁じ、又は個人情報管理者に対して、個人情報を変更ないし修正できない場合にはその削除を命じる権力を有する。

⑥ 運用実態

²⁵ <http://www.oic.go.th/web2017/en/role02.htm>

²⁶ <http://www.oic.go.th/web2017/>

²⁷ コンピュータ関連犯罪法第4条

²⁸ コンピュータ関連犯罪法第20条

²⁹ 個人情報保護法草案第5条

特定の産業を管轄する個人情報保護規制について、現在多くは存在していない。かかる規制の一例については、情報開示裁判所において担当されている。

情報開示裁判所は、公的情報の開示に関する命令に対する異議申立てについて、検討する義務を負う。同裁判所の様々な決定が、いかなる種類の情報が開示の許されない個人情報に該当するかを示唆している。情報開示裁判所によって個人情報として解釈される例としては、社会保障登録情報、公立大学による成績評価³⁰、歳入局による納税者への特定の事業に対する課税情報に関する決定³¹、また市民登録関連の情報³²も含む。一方、個人情報としてみなされない情報の例としては、公立学校の入学試験の解答用紙³³がこれに当たり、これは試験者が学校によって決められた規則と手続きに従って用意した書面であり、個人情報ではないと決定された。

(4) 最近のトピック

① 立法並びに行政機関ないし監督機関及び第三者機関の動向

個人情報保護法草案は未だ閣議決定がなされていない状態であるが、政府機関は個人情報保護法案への人々の意見を積極的に受け入れている。

② 個人情報保護法草案 (Draft Bill of Personal Data Protection)

ア 法律の概要

個人情報保護法草案の制定目的は、草案の提案理由に記載されており、以下のとおりである。「プライバシーを侵害する事例が数多く生じており、また情報技術及び通信システムの進歩により、個人情報の収集、利用、開示の容易性、利便性、及び迅速性が高められたことに伴い、個人情報の本人から事前の同意を得ず、また本人に事前に通知せずに、個人データを商業利用されたり、開示されたりすることにより、生活妨害や損害発生の可能性がある。また、個人情報保護に関し、一部の分野においてすでにそれを規制する法令があるが、個人情報保護に関する一般原則としての規則、仕組み、方針がないのが現状である。従って、本法を制定する必要がある。」

イ 個人情報の定義

³⁰ 情報開示裁判所決定 No. 51/2552

³¹ 情報開示裁判所決定 No. 101/2552

³² 最高裁判所決定 No. 15591/2557 <https://deka.in.th/view-579816.html>

³³ 最高裁判所決定 No. 4126/2543 <https://deka.in.th/view-36394.html>

第5条は、「個人情報」の定義について、「本法における「個人情報」とは、直接又は間接を問わず、特定の人を識別できるすべてのデータ（情報）を意味する」と定めている。

個人情報保護法案は「機微情報（ข้อมูลส่วนบุคคลที่มีลักษณะอ่อนไหว）」の定義を定めていない。しかし、機微な個人情報に関して、個人情報保護法案の中で特に保護されるように意図されている。第25条は、機微な個人情報の収集に関して特に次のように規定している。

「人の民族、人種、政治理念、教義、宗教信仰、哲学理念、性行動、犯罪歴、健康記録、又は委員会の規定による、他人の感情を害する可能性のあるいかなる個人情報をも、情報の本人ないし関係者の同意を得ない限り、収集することを禁止する。但し、(1) 第23条 (2) (3) (5) の例外規定が適用される場合、及び (2) その他省令に規定される場合を除く」。

ウ 主な規制・権利の内容

個人情報保護法案は、個人情報保護委員会の設立に関し、定めている(第1章)。第2章には、個人情報保護に関する条項があり、その内容は個人情報の収集、利用、開示、情報主体の権利に分けられる。個人情報に関する収集、利用、開示、訂正又はその他すべての行為は、個人情報保護法案に従い行えば、合法的な行為とみなされる。かかる法的規定の概要は、以下のとおりである。

(ア) 個人情報の収集は、次の場合でない限り認められない。(i)個人情報管理者（本法に基づき、個人情報の管理、収集、利用、開示に関する決定権限及び義務のある者）³⁴の行為に直接関連する合法的目的のためであること、(ii)情報収集の範囲は、必要範囲内に限る（第21条）。

(イ) 個人情報の利用及び開示は、その目的に沿い、且つ情報主体の事前の同意を取得した場合しか認められない(第26条)。

(ウ) 情報主体の権利は、個人情報へのアクセシビリティ(第28条)を含み、自分の個人情報が正確に保たれることを確保する(第30条)。また、個人情報管理者が情報主体に対して、個人情報保護政策を行う義務も含む(第31条)。例えば、個人情報の違法な損失、アクセス、変更、訂正、及び開示を防止するための安全対策を設定することである。

加えて、個人情報保護法案は個人情報保護に関する運用指針も定めている(第3章)。個人情報保護委員会は、個人情報保護の運用に関する指針を發布することができる(第34条)。さらに、個人情報保護委員会が、個人情報保護の基準をクリアした個人情報管理者にトラ

³⁴ 個人情報保護法草案第5条

ストマークを付与する制度もある（第 35 条）。

第 5 章は、主に個人情報保護法案の規制内容への違反があった場合の苦情申立の手続きに関する規定である。なお、個人情報保護法案に違反するときの民事及び刑事責任はそれぞれ第 5 章及び第 6 章に定められている。

エ 安全管理措置に関する規定

第 31 条 (1) において、権限無く個人情報を（に）喪失、アクセス、改ざん、収集ないし開示されること、もしくは個人情報が違法に使用されることを防ぐ目的のために、個人情報管理者が「適切な安全対策」を実施することが義務付けられている。この点において、個人情報管理者がかかる第 31 条 (1) の義務に違反した場合、第 44 条に従い刑事罰の対象となる。

また、安全管理対策は第 33 条に基づき発布される個人情報管理者の個人情報保護要領として設定される見込みである。個人情報保護法案は、要領がいかなる要素によって構成されるべきかについて定めていないが、委員会がかかる要領に関するガイドラインを作成する見込みである。この要領の設定の目的については、第 42 条において、個人情報管理者が完全に個人情報保護に関する当該要領に従っていれば、同人は民事責任の対象とならないと定められている。

オ 適用範囲、適用除外内容

個人情報保護法案は、一般的に、全ての人（自然人ないし法人、第 5 条による）の保護を対象としている。適用範囲に関しては、個人情報保護法案は単に、適用されない場合を次の 2 パターン規定している。(i) 個人情報の特定の範囲について規制するために制定された特定の法ないし規則があり、かかる法ないし規則が、公平性を保証し、個人情報保護法案に規定されたものと同等以上の基準を有している場合。(ii) 個人情報管理者が、勅令に規定されるような特定の方法ないし行動をとる場合。

カ 国際的な情報移転に関する規定

個人情報保護法案は、個人情報の国際的な移転についての制限を第 27 条に規定し、個人情報保護に関する規制が本法に基づく基準よりも実質的に下回る国への個人情報の送信ないし移転を禁止する。但し、次の場合を除く。(1) 法律上の規定に基づく場合、(2) 情報主体の同意が得られた場合、(3) 情報主体が当事者である契約、ないし情報主体の利益のために存在する契約から生じる義務履行の目的のために必要な場合、(4) 同意を示すことができない者のために利益となる場合、(5) 委員会により、個人情報保護に係る認定を受けた者に対する移転の場合、もしくは国際協力ないし国際任務の枠組みによる移転の場合。

加えて、電気通信業、銀行・金融業、保険業、証券業、ヘルスケア事業、消費者信用事業、電子支払サービス会社、政府機関において業務を行う者によって保持される個人情報の安全については、特別な規制の対象となる可能性がある。

キ 紛争処理手続き

第4章（申立て）は、個人情報保護委員会の権限として、個人情報保護法案第36条に基づき、個人情報管理者に対し情報主体に損害を与える疑いのある行為について証明するよう命令する権限を規定する。かかる行為が情報主体ないし第三者の個人情報に損害を与える可能性があり、個人情報管理者がかかる損害を防止することが不可能であることが立証された場合、委員会は、かかる行為を禁止する権限を有する。かかる行為の是正ないし変更が不可能な場合は、委員会は、第36条第2段落に基づき、個人情報を削除する権限を有する。

個人情報に関する情報主体の権利が侵害され、又は侵害される可能性のあるとき、情報主体は第37条に基づき委員会に申立てをすることができる。申立の規則及び手続については、委員会の定めるところによる。

② 近時の主要な裁判例

現在、タイにおける個人情報保護規制違反に特化した裁判例は存在しない。しかし、個人情報保護に関連した事例のほとんどは以下のとおり、民商法典上の不法行為及び/又は刑法上の名誉棄損罪ないし侮辱罪に関わるものである。

ア 最高裁判所判例 No. 4893/2558³⁵によると、最高裁は、個人の性的画像をニュースにおいて公表する行為は、民商法典第420条に基づき、対象人物に対するプライバシー権の侵害に当たると判断した。

イ 最高裁判所判決 No. 253/2520³⁶によると、最高裁は、原告の個人情報が記載された封書を開封し、かかる情報を他人に開示した行為について、被告に刑法第322条の罪³⁷を認めた。

³⁵ <https://deka.in.th/view-585752.html>

³⁶ <http://deka.supremecourt.or.th/search>

³⁷ 刑法第322条（信書開封）「何人も、その内容を確認、ないし公開する目的で、封がされた手紙、電報ないしその他全ての他人の所有に属する書類を開封ないし持ち去り、かかる行為が他人の権利を侵害する可能性がある場合、6か月以下の懲役もしくは1000バーツ以下の罰金、又は又はその併科となる。」

ウ しかし、個人情報の使用が法律によって許容される場合、当該使用は個人情報に関する権利の侵害とはみなされない。これは最高裁判所判例 No. 5372/2552³⁸の判断に見られる。原告は、被告である国家信用機関に対し訴訟を提起した。提訴前、原告は自分の個人情報である氏名、年齢、債務残高及び債務返済についての記録を、被告のデータベースから除去するよう要請した。しかし被告はこれを拒否し、原告はかかる被告の行為が原告に対する不法行為を構成すると主張した。

裁判所は次の通り判断した。「情報主体の保護に関しては、第 25 条において既に、いかなる管理がなされるかについて情報主体に権利が与えられている。しかし、自分の情報を削除ないし除去する権利については与えられていない。第 1 被告による情報の収集については、かかる情報をそのメンバーに対し通知し提供することも含め、法律上の義務である。よってかかる行為は原告に対する不法行為には該当しない」³⁹。

(5) 資料：法令関係の URL 一覧

公式の法令ウェブサイトはタイ語表記であり、英語表記のウェブサイトは翻訳である。

① 個人情報保護法草案 (The Draft Bill of Personal Information Protection, ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล)

https://ictlawcenter.etcha.or.th/de_laws/download_file/1_Cabinet_Draft-de_la_ws_data-privacy-act.pdf (タイ語版)

<https://thainetizen.org/wp-content/uploads/2015/01/personal-data-protection-bill-20150106-en.pdf> (英語版)

② 民商法典 (Thai Civil and Commercial Code (“CCC”), ประมวลผลแพ่งและพาณิชย์)

<http://appthea.krisdika.go.th/Naturesig/CheckSig?whichLaw=law4&folderName=%bb03&lawPath=%bb03-20-9999-update> (タイ語版)

<http://www.thailawonline.com/en/thai-laws/civil-code.html> (英語版)

③ 国営企業の個人情報保護に関する方針及び運用に関する電子取引委員会の通知 (the Notification of the Electronic Transaction Committee on the Policy and Practice relating to the Personal Data Protection of the State Enterprises of B.E. 2553 (A.D. 2010). ประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์)

<https://www.etcha.or.th/files/1/files/16.pdf> (タイ語版)

³⁸<https://deka.in.th/view-501968.html>

³⁹ 最高裁判所判決 No. 5372/2552

④ 金融機関事業法 (The Financial Institution Business Act, พระราชบัญญัติธุรกิจสถาบันการเงิน)

<http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%b812&lawPath=%b812-20-9999-update> (タイ語版)

<http://www.krisdika.go.th/wps/wcm/connect/8148970043c8cb87be5cfe25b7244636/FINANCIAL+INSTITUTION+BUSINESS+ACT%2C+B.E.+2551+%282008%29.pdf?MOD=AJPERES&CACHEID=8148970043c8cb87be5cfe25b7244636> (英語版)

⑤ 国家健康事業法 (the National Health Service Act, พระราชบัญญัติสุขภาพแห่งชาติ)

<http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%ca71&lawPath=%ca71-20-9999-update> (タイ語版)

http://www.thailawforum.com/laws/National%20Health%20Act_2007.pdf (英語版)

⑥ 電気通信事業法 (Telecommunication Business Act, B.E. 2544 (2001)、พระราชบัญญัติกิจการโทรคมนาคม)

<http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%a1110&lawPath=%a1110-20-9999-update> (タイ語版)

http://www.krisdika.go.th/wps/portal/general_en!/ut/p/c5/04_SB8K8xLLM9MSSzPy8xBz9CP0os3g_A2czQ0cTQ89ApyAnA0__EIOAQGdXAwNdc6B8JG55dzMCuv088nNT9SP1o8wRqowczd0MHC29vA08PUMM3Z3N9CNzUtMTkyv1C3IjyvMdfRUByl01jw!./d13/d3/L01Jsklna2shL01CakFBRX1BQkVsq01BISEvWUZOQzFOS18yN3chLzdfTjBDNjFBNDFJMkE3RjBBOUpLUEtJVDFHQzY!/?PC_7_NOC61A41I2A7F0A9JKPKIT1GC6_WCM_CONTEXT=/wps/wcm/connect/ksdkwebcontent_en/legal+translation/legal+english/telecommunications+business+act+be+2544+%282001%29 (英語版)

⑦ 信用情報事業法 (Credit Information Business Operation Act, พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต)

<http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%a1112&lawPath=%a1112-20-9999-update> (タイ語版)

http://web.krisdika.go.th/data/outsitedata/outside21/file/CREDIT_INFORMATION_BUSINESS_OPERATION_ACT,B.E._2545.pdf (英語版)

⑧ タイ王国憲法 (Constitution of the Kingdom of Thailand enacted on 6 April 2017, รัฐธรรมนูญราชอาณาจักรไทย)

<http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law1&folderName=%c306&lawPath=%c306-10-2560-a0003> (タイ語版)

<http://www.krisdika.go.th/wps/wcm/connect/d230f08040ee034ca306af7292cbe309/CONSTITUTION+OF+THE+KINGDOM+OF+THAILAND+%28B.E.+2560+%282017%29%29.pdf?MOD=AJPERES&CACHEID=d230f08040ee034ca306af7292cbe309> (英語版)

⑨ 刑法 (Penal Code、ประมวลกฎหมายอาญา)

<http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law4&folderName=%bb06&lawPath=%bb06-20-9999-update> (タイ語版)

<https://www.thailandlawonline.com/table-of-contents/criminal-law-translation-thailand-penal-code> (英語版)

⑩ コンピュータ関連犯罪法 (Act on Commission of Offences relating to Computer, B.E. 2550 (2007), พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์)

<http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%c771&lawPath=%c771-20-9999-update> (タイ語版)

⑪ 公的情報法 (Official Information Act, B.E. 2540 (1997), พระราชบัญญัติข้อมูลข่าวสารของราชการ)

<http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%a203&lawPath=%a203-20-2540-001> (タイ語版)

http://www.krisdika.go.th/wps/wcm/connect/b837b0804ba4d080a47ba78b0853d392/OFFICIAL_INFORMATION_ACT%2C_B.E._2540.pdf?MOD=AJPERES&CACHEID=b837b0804ba4d080a47ba78b0853d392 (英語版)

⑫ 電子取引法 (Electronic Transactions Act, B.E. 2544 (2001), พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์)

<http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%c763&lawPath=%c763-20-9999-update> (タイ語版)

<http://www.krisdika.go.th/wps/wcm/connect/037ab90043c8052dbcd7fc25b7244636/ELECTRONIC+TRANSACTIONS+ACT%2C+B.E.+2544+%282001%29.pdf?MOD=AJPERES&CACHEID=037ab90043c8052dbcd7fc25b7244636> (英語版)

9. ベトナム

(1) 制度概要

① 法体系の概要

ベトナムにおいては、個人情報保護について包括的に定めたいわゆる「個人情報保護法」は制定されておらず、憲法、民法の他、個別分野ごとに数多くの法令が制定されている。

まず、2013年11月28日に公布され、2014年1月1日より施行されたベトナム社会主義共和国憲法 (Constitution of the Socialist Republic of Vietnam) ¹では、私的生活、個人の秘密及び家族の秘密について、不可侵の権利が定められており、自らの名誉及び威信を擁護する権利、並びに信書、電話の内容、電信及びその他の個人的な情報交換形式に対するプライバシー権を有すると規定されている (憲法第21条)。

また、改正民法 (法律第91/2015/QH13号) (Civil Code No. 91/2015/QH13、以下「民法」という。) ²においても、私的生活、個人の秘密及び家族の秘密は不可侵のものとされる等の個人情報保護についての原則が規定されている。

分野ごとの立法としては、情報技術及び電気通信、消費者保護、銀行、ヘルスケア等の特定分野ごとの多くの法令において個人情報保護に関連する規定が定められているが、個人情報の定義や取扱規則、監督機関等は統一・整理されていないのが現状である。

そのような状況の中で、サイバー情報保護活動について広範に定めたサイバー情報保護法 (法律第86/2015/QH13号) (No. 86/2015/QH13 Law on Cyber Information Security, 以下「LOCIS」という。) ³が2015年11月19日に公布され、2016年7月1日より施行された。同法は、商業目的での電気通信やコンピュータネットワークを經由した環境での個人情報の取扱いに関する活動を規制対象とし、個人情報の定義や安全管理措置などについて体系的に規定するものである。

② 民間部門・公的部門の区別

ベトナムにおいて、個人情報保護に関連する法令に民間部門・公的部門の明確な区別はないが、裁判記録法 (法律第28/2009/QH12号) (Law No. 28/2009/QH12 on Judicial Records)

¹ https://www.jica.go.jp/project/vietnam/021/legal/ku57pq00001j1wzj-att/legal_03_20151215.pdf (出典 国際協力機構 (JICA))

² https://www.jica.go.jp/project/vietnam/021/legal/ku57pq00001j1wzj-att/legal_60.pdf (出典 国際協力機構 (JICA))

³ <http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf>

や公民身分証明書法（法律第 59/2014/QH13 号）（Law No. 59/2014/QH13 on Citizen Identification）は主に公的部門について規定するものである。

（２）主な法律の概要

① 民法

ア 法律の概要

民法は 2015 年 11 月 24 日に公布され、2017 年 1 月 1 日より施行された。

本法は、自然人及び法人の法的地位、自然人及び法人の行為に関する法的基準、平等、意思の自由、財産の独立及び自己責任を基礎として形成される各関係における自然人及び法人の人格及び財産に関する権利及び義務について規定している。

イ 個人情報の定義

民法においては、個人情報の定義規定は設けられていない。後述する LOCIS の他、以下のとおりいくつかの法令が個人情報について定義規定を設けている。

電子商取引に関する政令（2013 年 5 月 16 付、第 52/2013/ND-CP 号）（Decree 52/2013/ND-CP dated 16 May, 2013 of the Government on E-Commerce）第 13 条第 3 項では、「個人情報」とは、特定の個人の識別に寄与する情報（個人の氏名、年齢、自宅住所、電話番号、医療情報、口座番号、個人の決済情報及び個人が機密に保つことを希望するその他の情報を含む。）をいうとされる。

インターネット・サービス及びオンライン情報の管理、提供及び使用に関する政令（2013 年 7 月 15 日付、第 72/2013/ND-CP 号）（Decree 72/2013/ND-CP dated 15 July, 2013 of the Government on the management）第 3 条第 16 項では、「個人情報」とは、個人の識別に関連する情報（氏名、年齢、住所、ID 番号、電話番号、E メールアドレスその他法律により定義付けられるその他の情報を含む。）をいうとされる。

ベトナム法では、「機微情報」という用語は正確には規定されていない。

ウ 主な規制・権利の内容

本法第 38 条は、以下のとおり規定している。

- ・ 個人の私生活、個人の秘密及び家族の秘密は、不可侵であり、法令により保護される。

- ・ 個人の私的生活に関する情報の収集、保有、使用及び公開は、当該者の同意を得た上で行わなければならない。家族の秘密に関する情報の収集、保有、使用及び公開は、家族全員の同意を得た上で行われなければならない。但し、別途法令で規定される場合を除く。
- ・ 各契約の当事者は、契約の確立、及び履行の過程において知り得た他方当事者の私的生活、個人の秘密又は家族の秘密に関する情報を漏えいしてはならない。但し、別途合意する場合を除く。

エ 小規模事業者の取扱い

ベトナム法において、小規模事業者の特別な取扱いについて定める法令は存在しない。

オ 国際的な情報移転に関する規定

ベトナム法において、国際的な情報移転について定める法令は存在しない。

カ 紛争処理手続き

個人情報保護に関する紛争解決については、一部個別法で紛争解決手段の選択等について言及がある他、原則的には一般的な管轄権を有する裁判所により解決されることになる。

② LOCIS

ア 法律の概要

LOCISは2015年11月19日に公布され、2016年7月1日より施行された。

LOCISは、サイバー情報保護活動、並びにサイバー情報保護を確保する際の機関、組織及び個人の権利及び責任、民間暗号化、サイバー情報保護に関する基準及び技術規制、サイバー情報保護の分野における取引、サイバー情報保護のための人的資源の開発、及び国家のサイバー情報保護の管理について規定している。

イ 個人情報の定義、機微情報の定義

第3条第15項では、「個人情報」という用語は、単に「特定の個人の識別に関する情報」と定義されている。

ウ 主な規制・権利の内容

データ主体の権利：データ主体は、個人情報を処理する組織及び個人に対し、これらが収集又は保存している個人情報を更新、改変若しくは消去し、又は第三者に対する個人情報の提供を停止するよう要求することができる（LOCIS 第 18 条第 1 項）。

個人情報を処理する組織又は個人の義務：個人情報を処理する組織又は個人は、個人情報の収集及び利用に当たって以下に従わなければならない（LOCIS 第 17 条第 1 項）。

- ・ データ主体から、収集及び利用される情報の範囲及び目的について承諾を得た後にはじめて個人情報を収集する。
- ・ データ主体から、同意を得た後にはじめて、収集された個人情報を当初の目的から異なる目的で利用する。
- ・ データ主体から同意を得る、又は当局機関からの要求を受けない限り、いかなる第三者に対しても、収集され、アクセスされ、又は管理される個人情報を共有、拡散してはならない。

また、個人情報の所有者から個人情報の更新、改変若しくは消去に関し、又は第三者に対する個人情報の提供の停止に関し通知を受領した場合、以下に従わなければならない（LOCIS 第 18 条第 2 項）。

- ・ 要求に従い、当該所有者に対し通知し、又は所有者がその個人情報を更新、改変又は削除することができるよう、情報へのアクセス権を付与する。
- ・ 個人情報を保護するために適切な措置を講じ、所有者が技術上その他の理由により要求の遵守を怠った場合、当該所有者に通知する

個人情報を処理する機関、組織及び個人は、以下の義務を負う。

- ・ 自己が処理する情報に関するサイバー情報保護を確保し、個人情報の処理及び保護に関する措置を講じ、公表する（第 16 条第 2 項及び第 16 条第 3 項）。
- ・ 保管中の個人情報について、使用目的を達成し又は保存期間が終了したものを削除し、当該個人情報の所有者にその旨通知する。但し、別途法令により規定される場合を除く（第 18 条第 3 項）。
- ・ 収集及び保存した個人情報を保護するため、適切な管理的及び技術的措置を講じ、サイバー情報保護の保証に関する基準及び技術規制を遵守する（第 19 条第 1 項）。
- ・ サイバー情報保護に関する事象が生じた場合又はそのおそれがある場合、可及的速やかに是正措置及び停止措置を講じる（第 19 条第 2 項）。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

本法では、個人情報漏えいした場合等における監督機関及び関連する個人等に対する報告義務を明確に定める規定は見受けられないが、サイバー情報保護に関する事象に対応するために適切な措置を講じる義務を間接的に規定する規制が複数存在する。以下に例を挙げる。

- ・ サイバー情報保護に関する事象（サイバー情報保護に関する事象とは、情報の完全性、機密性又は有用性に影響を及ぼし、情報又は情報システムに損害を及ぼす事象をいう。）が生じた場合又はそのおそれがある場合、個人情報を処理する組織及び個人は、可及的速やかに是正措置及び停止措置を講じる（第19条第2項参照）。
- ・ サイバースペースにおいてサービスを利用する機関、組織及び個人は、サイバー情報保護の妨害行為又は事象につき、サービス提供企業又は特別事象対応ユニットに対し速やかに通知する（第15条第2項参照）。
- ・ 情報システムの運用担当者（情報システムの管理者が、当該システムの運用を任命する機関及び組織をいう。情報システムの管理者が、情報技術サービスを外注する場合、情報システムの管理者は、当該サービスの提供者とする。）は、発生が認識された日から5日以内に、以下に報告しなければならない。

（ア） 情報システムの管理者（情報システムを直接管理する権限を与えられた当局、組織及び個人をいう。政府機関及び当局においては、情報システムの管理者は、当該情報システムの構築、設定、アップグレード及び拡張に関する投資プロジェクトにおいて裁量を与えられた大臣、大臣級の機関、政府機関、地方の人民委員会又は事業体をいう。）

（イ） 国家監視機関

（ウ） 事象を取り扱うタスクフォース・ユニット

（エ） 事象を取り扱うネットワークのメンバー

（2017年9月12日付情報通信省通達第20/2017/TT-BTTTT号（Circular No.20/2017/TT-BTTTT dated 12 September 2017 of Ministry of Information and Communications）第9条第2項参照）

さらに、第20条第1項は、サイバースペースにおける個人情報のセキュリティ保証に関する陳情書及び報告書を公衆から受領するためのオンライン情報チャネルの構築により、迅速な措置を講じるための手段について定めている。

オ 安全管理措置

本法における、安全管理措置に関する規定は以下のとおりである。

- ・ セキュリティ機関、サイバー情報保護活動に従事する組織及び個人は、サイバー情報保護の確保において、管轄の国家機関並びにその他の組織及び個人と協力する。さらに、サイバースペースにおいてサービスを利用する機関、組織及び個人は、サイバー情報保護の妨害行為又は事象について、サービス提供企業又は特別事象対応ユニットに対し速やかに通知する（第15条）。
- ・ 個人は、サイバースペース内でサービスを利用する際には、自己の個人情報を保護し、個人情報の提供に関する法律を遵守する（第16条）。
- ・ 個人情報を処理する機関、組織及び個人は、自己が処理する情報に関するサイバー情報保護を確保し、個人情報の処理及び保護に関する措置を講じ、公表する。
- ・ 個人情報を処理する組織及び個人は、自己が収集、保存した個人情報を保護するため、適切な管理的及び技術的措置を講じ、サイバー情報保護の保証に関する基準及び技術規制を遵守する。サイバー情報保護に関する事象が発生した場合、又はそのおそれがある場合、個人情報を処理する組織及び個人は、可及的速やかに是正措置及び停止措置を講じる（第19条）。
- ・ サイバースペースにおける個人情報を保護するに際し、国家管理機関は、(i)サイバースペースにおける個人情報のセキュリティ保証に関する陳情書及び報告書を公衆から受領するためのオンライン情報チャネルの構築、及び(ii)毎年、個人情報を処理する組織及び個人を検査及び調査し、必要に応じて臨時的検査及び調査を実施する（第20条）。
- ・ 情報システム保護の任務には、(i)情報システムのセキュリティ・グレードを決定し、(ii)情報システムに対するセキュリティリスクを評価及び管理し、(iii)情報システム保護を要請、監督及び調査し、(iv)情報システム保護のための措置を講じ、(v)報告体制を遵守し、(vi)サイバー情報保護に関する認識を深めるための情報公開を実施することが含まれる（第22条）。
- ・ 情報システムの保護のための措置には、(i)情報システムの設計、開発、管理、運用、使用、更新又は廃止に際する、サイバー情報保護の保証に関する規制を公布し、(ii)サイバー情報保護に対するリスクを防止し、これと戦い、事象を是正するために、サイバー情報保護に関する基準及び技術規制に従って管理的及び技術的措置を適用し、(iii)規制の遵守を調査及び監督し、適用される管理的及び技術的措置の有効性を評価し、(iv)情報システムのセキュリティを監視することが含まれる（第23条）。
- ・ 情報システムのセキュリティ監視とは、監視対象の選定、当該情報システムのセキュリティに影響を及ぼす要因を特定することを目的に、当該対象に関する情報の状況の収集、及び分析、サイバー情報保護を侵害する行為又は当該情報システムにサイバー情報保護

に関する事象を生じさせるおそれのある行為について報告及び警告する行為、サイバー情報保護の状況に影響を及ぼす主要な要因の分析、及び技術的措置の変更の提案、といった行為をいう（第 24 条）。

- ・ 情報システムのセキュリティ監視の対象は、ファイアウォール、アクセスコントロール、主要な情報のルート、重要サービス、重要機器及び重要端末機器である。
- ・ 電気通信事業者、情報技術サービスを提供する事業者、サイバー情報保護サービスを提供する事業者は、管轄の国家機関の要求に基づき、情報システムのセキュリティを監視する際に、情報システムの管理機関と協力する。
- ・ 国家重要情報システムの構築、拡張又はアップグレード時には、本システムの稼働及び利用前に情報セキュリティを検査するものとする（第 26 条）。
- ・ 情報通信省は、発布に向けて首相に提出する国家重要情報システムのリスト作成に主要な責任を負い、国防省、公安省並びに関連する省及び部門と協力する。
- ・ 国家重要情報システムの管理機関は、以下のとおり、国家重要情報システムに関するサイバー情報保護を確保する責任を負う（第 27 条）。

国家重要情報システムの管理機関は、以下に従う。

- ・ 本法第 25 条第 2 項の規定を遵守する。
- ・ 管轄の国家機関が指定する特別組織に、サイバー情報保護リスクを定期的に評価させる。
- ・ 情報システムに関し、スタンバイ措置を講じる。
- ・ 国家重要情報システムの保護のために訓練を計画及び実施する。

情報通信省は、以下に従う。

- ・ 国家重要情報システムに関するサイバー情報保護の指導、要請、検査及び調査に対し主要な責任を負い、国家重要情報システムの管理機関、公安省並びに関連する省及び部門と協力する。但し、本条第 3 項及び第 4 項に定める場合を除く。
- ・ 電気通信事業者、情報技術サービス提供事業者及びサイバー情報保護サービス提供事業者に対し、国家重要情報システムのサイバー情報保護に関する事象に対する技術的助言及び支援を提供し、これに対応するよう要請する。

公安省は、その管理下にある国家重要情報システムに関するサイバー情報の保護を指導、要請、検査及び調査し、管轄の国家機関からの要請に応じて、その他の国家重要情報システムの保護において、情報通信省、国家重要情報システムの管理機関及び関連する省、部門及び人民委員会とあらゆるレベルで協力する。

国防省は、その管理下にある国家重要情報システムに関するサイバー情報の保護を指導、要請、検査及び調査する。

政府暗号化委員会は、国家機関、政治組織及び政治・社会組織の国家重要情報システム内の情報を保護するため、暗号化の利用を体系化し、法令に従い、サイバー情報保護の監督において国家重要情報システムの管理機関と協力する。

カ 適用範囲、適用除外内容

本法は、ベトナム国内でサイバー情報保護活動に直接関わり又は関連しているベトナムの機関、組織及び個人並びに海外の組織及び個人に適用される。

③ 情報技術法(法律第 67/2006/QH11 号)(Law No. 67/2006/QH11 on Information Technology、以下「情報技術法」という。)

ア 法律の概要

情報技術法は 2006 年 6 月 29 日に公布され、2007 年 1 月 1 日より施行された。

本法は、情報技術の応用及び開発活動、情報技術の応用及び開発を確保するための措置、並びに情報技術の応用及び開発活動に従事する機関、組織及び個人の権利義務を規定している。

イ 主な規制・権利の内容

データ主体の同意：第 21 条は、法令により別途規定される場合を除き、ネットワーク環境で第三者の個人情報収集、処理及び使用する組織及び個人は、当該第三者の同意を取得しなければならないと規定している。

第三者の個人情報を収集、処理及び使用する組織及び個人の義務：(i) 当該第三者に対し、個人情報の収集、処理及び使用の形式、範囲、場所及び目的について通知し、(ii) 収集した個人情報を適切な目的に使用し、これを法律に定められる期間又は両当事者間で合意した期間に限り保存し、(iii) 個人情報が紛失、盗難、開示、変更又は破壊されないことを確保するために必要な管理的及び技術的措置を講じ、(iv) 本法第 22 条第 1 項に従い、情報の再検査、修正又は消去が要求された場合には、該当する個人情報が修正されるまで、これを提供又は使用することを控えるために、必要な措置を直ちに講じる。

本法第 22 条に基づき、個人は、自らの個人情報をネットワーク環境に保存する組織又は個人に対し、当該情報を検査、修正又は消去するよう要求することができる。別途法律により定める場合、又は個人が同意する場合を除き、組織若しくは個人は、当該個人の個人

情報を第三者に提供することができない。個人は、個人情報の提供における違反により生じた損害につき、損害賠償を請求することができる。

情報の安全性及び機密性の保証：第 72 条は、ネットワーク環境において交換、送信又は保存される組織及び個人の法的な個人情報は、法令に従い機密に保たれるものとし、以下の行為を行ってはならないと規定している。

- ・ ネットワーク環境における、その他の組織又は個人の情報へのハッキング、変更又は削除。
- ・ 情報システムによるサービス提供の妨害。
- ・ ネットワーク環境における、その他の組織又は個人の情報へのアクセスの妨害。ただし、法令により許可される場合を除く。
- ・ ネットワーク環境における、その他の組織又は個人のパスワード、コード又は情報のクラッキング、窃盗又は利用。
- ・ ネットワーク環境において交換、送信又は保存するその他の組織又は個人の情報の機密性に対し危険性を生じさせ、又はこれを開示するその他の行為。

ウ 適用範囲、適用除外内容

本法は、ベトナム国内で情報技術の応用及び開発活動に従事しているベトナム及び海外の組織及び個人に適用される。

④ 電気通信法（法律第 41/2009/QH12 号）（Law No. 41/2009/QH12 on Telecommunication）

ア 法律の概要

電気通信法（法律第 41/2009/QH12 号）は 2009 年 11 月 23 日に公布され、2010 年 7 月 1 日より施行された。

本法は、電気通信活動（電気通信投資及び事業を含む。）、公共事業電気通信、電気通信管理、電気通信工事、電気通信活動に従事する組織及び個人の権利義務を規定している。

イ 主な規制・権利の内容

電気通信サービス利用者の権利：第 16 条第 1 項第 dd 号は、電気通信事業者は法令に基づき、サービス利用者の個人情報を機密に保たなければならないと規定している。

電気通信事業者の義務：第6条第4項に基づき、電気通信事業者は、電気通信サービスユーザーに関する個人情報（氏名、住所、発信者番号、受信者番号、発信者の位置、受信者の位置、通話時間及びユーザーが電気通信事業者との契約時に提供したその他の個人情報を含む。）を開示することができない。公共電気通信ネットワークを通じて送信されるすべての組織及び個人の個人情報は、機密に保たれ、ユーザーから許可を得た上で、ユーザー情報が提供される。

ウ 適用範囲、適用除外内容

本法は、ベトナム国内で電気通信活動に直接従事し又は関連している国内及び海外の組織及び個人に適用される。

⑤ 電子取引法（法律第51/2005/QH11号）（Law No. 51/2005/QH11 on E-transactions）

ア 法律の概要

電子取引法（法律第51/2005/QH11号）は2005年11月29日に公布され、2006年3月1日より施行された。

本法は、国家機関が民間、事業、商業その他法律により定められる部門において運用する電子取引について規定している。

イ 主な規制・権利の内容

第46条第2項は、機関、組織及び個人は、電子取引において自己がアクセス可能な又は自己の管理下にある、私的及び個人的な事情に関する情報又はその他の機関、組織及び/若しくは個人に関する情報を、これらの同意を得ずに使用、提供又は開示してはならないと規定している。但し、別途法令により定められる場合を除く。

ウ 適用範囲、適用除外内容

本法は、電子的手段での取引を選択する機関、組織及び個人に適用される。

本法の規定は、土地使用権の証明書、家屋その他の不動産の所有権の証明書、相続文書、婚姻証明書、離婚決定書、出生証明書、死亡証明書、為替手形その他の有価文書には適用されない。

⑥ 消費者権利保護法（法律第 59/2010/QH12 号）（Law No. 59/2010/QH12 on Protection of Consumers Rights）

ア 法律の概要

消費者権利保護法（法律第 59/2010/QH12 号）は 2010 年 11 月 17 日に公布され、2011 年 7 月 1 日より施行された。

本法は、商品者の権利義務、消費者と物品及び/又はサービスを取引する組織の責任又は個人の責任、消費者の利益を守る社会組織の責任、消費者と、物品及び/又はサービスを取引する組織又は個人との間の紛争解決、消費者の利益を守る国の責任について規定している。

イ 主な規制・権利の内容

第 6 条は、消費者の情報は、消費者が取引に参加、物品又はサービスを利用する際には、安全かつ機密に保たれるものと規定している。但し、管轄の国家機関が情報を要求した場合を除く。

さらに、消費者情報の収集、使用及び転送に際し、物品及び/又はサービスを取引する組織又は個人は、以下に従わなければならない。

- ・ 消費者情報の収集及び使用を行う前に、その目的を消費者に対し明確かつ公に通知する。
- ・ 消費者に通知した目的に従い、かつ、消費者の同意を取得した上で情報を使用する。
- ・ 消費者情報の収集、使用及び転送中の安全性、正確性、完全性を確保する。
- ・ 情報が不正確であることが判明した場合、自ら情報を更新又は調整するか、又は消費者が更新及び調整を補助する。
- ・ 消費者の同意が得られた場合に限り、消費者情報を第三者に転送する。但し、別途法令により定められる場合を除く。

ウ 適用範囲、適用除外内容

本法は、ベトナムの領域内で物品、サービスを取引する消費者、組織又は個人、消費者の利益保護活動に関わる機関、組織又は個人に適用される。

⑦ 公民身分証明書法（法律第 59/2014/QH13 号）（Law No.59/2014/QH13 on Citizen Identification）

ア 法律の概要

公民身分証明書法（法律第 59/2014/QH13 号）は 2014 年 11 月 20 日に公布され、2016 年 1 月 1 日より施行された。

本法は、公民身分証明書、公民身分証明書データベース及び国家人口データベース、国民の身分証明書の管理及び利用、並びに関連機関、組織及び個人の権利、義務及び責任について規定している。

イ 主な規制・権利の内容

第 15 条は、特に以下の情報が個人情報とみなされると規定している。

(i) 姓、ミドルネーム及び名、(ii) 生年月日、(iii) 性別、(iv) 出生届出地、(v) 出身地、(vi) 民族性、(vii) 宗教、(viii) 国籍、(ix) 婚姻関係、(x) 永住地、(xi) 現住所、(xii) 血液型（国民が自らの血液型の更新を要求し、血液型証明書を提示した場合）、(xiii) 性、ミドルネーム及び名、(xiv) 個人識別番号又は身分証明書番号、及び両親、配偶者又は法定代理人の国籍、(xv) 世帯主の姓、ミドルネーム及び名、個人識別番号又は身分証明書番号、及び世帯主との関係、(xvi) 死亡又は行方不明となった日/顔写真、(xvii) 個人を識別するための特徴、(xviii) その他の姓及び名、(xix) 身分証明書の番号並びに発行日及び場所、(xx) 職業（兵役中の軍人を除く。）、(xxi) 最終学歴。

上記の情報は、完全、適切かつ速やかなる方法で収集及び更新されなければならない。

国民（「データ主体」）の主な権利：第 5 条第 1 項は、国民が以下の主な権利を有すると規定する。(i) 個人の秘密及び家族の秘密を、国家人口データベース及び公民身分証明書データベースで機密に保ち（但し、法令の定めに従って情報及び文書を提供する場合を除く。）、(ii) 法令に従い、公民身分証明書管理機関に対し、国家人口データベース及び公民身分証明書データベース又は国民の身分証明書で利用可能となっていない自己の情報を更新し、又は不正確な情報若しくは変更のあった情報を変更するよう要求し、(iii) 法令に従い、公民身分証明書、国家人口データベース及び公民身分証明書データベースに関する法律違反について苦情を申し立て若しくは告発し、又は訴訟を提起する権利。

公民身分証明書管理機関の責任：第 6 条第 1 項は、公民身分証明書管理機関が、以下の主な責任を有すると規定する。(i) 国民の情報を正確に収集及び更新し、(ii) 国民の情報が不正確であり又は変更されたと信じるに足る根拠がある場合、速やかにこれを変更し、

(iii)本法に従い、機関、組織及び個人に関する公民身分証明書、国家人口データベース及び公民身分証明書データベースに係る行政手続を揭示及び指導し、(iv)国家人口データベース及び公民身分証明書データベースにおける情報の安全性及び機密性を確保し、(iv)法令に従い、機関、組織又は個人からの要求があった場合、国民に関する情報及び文書を完全、速やかかつ正確に提供し、(v)法令に従い苦情及び告発を解決し、違反を処理する。

第7条は、次の禁止行為を規定している。(i)国民の身分証明書の内容を偽造、変更及び改ざんすること、(ii)第三者の国民の身分証明書を盗用し又は不正に使用すること、(iii)国民の身分証明書を借用、貸付、担保権設定、担保として受領し又は破壊すること、(iv)偽造された国民の身分証明書を使用すること、(v)国家人口データベース及び公民身分証明書データベース内の情報に不正にアクセスし、これを変更、削除、消去又は拡散すること。

ウ 安全管理措置

公民身分証明書法（法律第 59/2014/QH13 号）における安全管理措置に関する規定の概要は、以下のとおりである。

公民身分証明書データベースの構築及び管理に関する要件は、以下のとおりである（第 14 条）。

- ・ 公民身分証明書データベースは、公安省の公民身分証明書管理機関、省又は中央直轄都市の公共セキュリティ部門及び農村地域、市部、街又は地方都市の公共セキュリティ部門、並びにこれらと同等の管理ユニットに構築され管理される。
- ・ 公民身分証明書データベースは、国家人口データベースへの接続を確保し、データベース基準並びに情報技術に関する基準及び技術規制を充足するように構築される。
- ・ 書類の扱いに関する規則、電子取引及び情報技術に関する規制及び体制を遵守する。
- ・ 安定的運用、安全性及びセキュリティを確保するために、完全、正確かつ速やかに情報を収集及び更新する。

国家人口データベース及び公民身分証明書データベースの情報インフラの保証は、以下のとおりである（第 29 条）。

- ・ 国家人口データベース及び公民身分証明書データベースの情報インフラは、質、同調性、正確性、適性及び適時性を確保して開発され、中央から地方レベルまで、中央集権化かつ統一されて構築され、管理される。
- ・ 国家は、国家人口データベース及び公民身分証明書データベースの情報インフラを、国防、国家安全保障及び社会経済の発展に関する要件を満たすよう確保する。

エ 適用範囲、適用除外内容

本法は、ベトナム国民並びに関連機関、組織及び個人に適用される。

⑧ 戸籍法（法律第 60/2014/QH13 号）（Law No. 60/2014/QH13 on Civil Status）

ア 法律の概要

戸籍法（法律第 60/2014/QH13 号）は 2014 年 11 月 20 日に公布され、2016 年 1 月 1 日より施行された。

本法は、戸籍、戸籍の登録に関する権利、義務、原則、権限及び手続、戸籍データベース及び国家による戸籍の管理について規定している。

国籍及び養子縁組に関する事項の解決のための権限及び手続は、ベトナムの国籍法及び養子縁組法に従わなければならない。但し、別途本法に定める場合を除く。

イ 主な規制・権利の内容

第 74 条により、戸籍データベース内の情報コンテンツの消去、改変又は改ざん、及び登録戸籍を通じて知り得た個人情報の公開は禁止される。

⑨ 刑法（法律第 100/2015/QH13 号）（Criminal Code No. 100/2015/QH13）⁴

ア 法律の概要

刑法（法律第 100/2015/QH13 号）は 2015 年 11 月 27 日に公布され、2018 年 1 月 1 日より施行された。

本法は、ベトナムの国家主権及び安全保障、社会主義体制、人権、公民の権利を守り、各民族間の平等を守り、国家の利益を守り、法秩序を体系化しこれを守り、犯罪行為を罰し、すべての人に法遵守に関する意識啓発を行い、犯罪を防止し、犯罪と闘うことを意図し、犯罪及び刑罰について規定している。

⁴ https://www.jica.go.jp/project/vietnam/021/legal/ku57pq00001j1wzj-att/legal_20160531_04.pdf（出典 国際協力機構（JICA））

イ 主な規制・権利の内容

本法は、個人情報保護のため、以下を含むいくつかの行為を犯罪と規制している。

- ・ 秘密情報、信書、電話、電信その他の個人的な情報交換形式の侵害（本法第 159 条）。
- ・ コンピュータネットワーク、電気通信ネットワーク又は電子機器に有害なソフトウェアプログラムの拡散（本法第 286 条）。
- ・ コンピュータネットワーク、電気通信ネットワーク又は電子機器の妨害又は混乱（本法第 287 条）。
- ・ コンピュータネットワーク又は電気通信ネットワーク上での違法な情報提供又は使用（本法第 288 条）。
- ・ コンピュータネットワーク、電気通信ネットワーク又は第三者の電子機器への違法な侵入（本法第 289 条）。
- ・ コンピュータネットワーク、電気通信ネットワーク又は電子機器を使用した財産奪取行為（本法第 290 条）。
- ・ 銀行口座に関する情報の、不正収集、所有、交換、取引、公開（本法第 291 条）。

⑩ その他関連法令

ア. ベトナム民間航空法（法律第 66/2006/QH11 号）（Vietnam Civil Aviation Law No. 66/2006/QH11）

ベトナム民間航空法（法律第 66/2006/QH11 号）は 2006 年 6 月 29 日に公布され、2007 年 7 月 1 日より施行された。

本法は、航空機、空港、飛行場、航空スタッフ、航空施設、航空運送、航空安全、民事責任、一般的航空その他民間航空に関連する活動を含む民間航空活動について規定している。

第 126 条は、電子予約システムで取引を行う企業が、自己の顧客の個人情報を機密に保つべきことを規定している。但し、管轄の国家機関からの要請がある場合を除く。

イ. プレス法（法律第 103/2016/QH13 号）（Law No. 103/2016/QH13 on Press）

プレス法（法律第 103/2016/QH13 号）は 2016 年 4 月 5 日に公布され、2017 年 1 月 1 日より施行された。

本法は、プレス、国民のプレスにおける発言の自由、プレスの組織及び運営、プレス活動に参加又は関連している機関、組織及び個人の権利義務、プレスに対する国家の管理について規定している。

本法は、個人の情報プライバシー及び機密情報の開示を禁止している。また、管轄当局、

<p>組織及び個人は、プレスに対する個人のプライバシーに関する情報の提供を拒絶する権利を有する。</p>
<p>ウ. 広告法（法律第 100/2015/QH13 号）（Law No. 16/2012/QH13 on Advertising）</p> <p>広告法（法律第 100/2015/QH13 号）は 2012 年 6 月 21 日に公布され、2013 年 1 月 1 日より施行された。</p> <p>本法は、広告活動、広告活動に参加する組織及び個人の権利義務、国家による広告の管理について規定している。本法では、政治活動における伝播及び流布は規制されていない。</p> <p>第 8 条に基づき、第三者の写真、言葉又は文章を含む広告を、当該第三者の許可を得ることなく使用することは禁止される。但し、別途法令により許可される場合を除く。</p>
<p>エ. 金融機関法（法律第 47/2010/QH12 号）（Law No. 47/2010/QH12 on Credit Institutions）</p> <p>金融機関法（法律第 47/2010/QH12 号）は 2010 年 6 月 16 日に公布され、2011 年 1 月 1 日より施行された。</p> <p>本法は、金融機関の設立、組織、経営、特別管理、再編及び解散、並びに外資系銀行の支店、外資系金融機関の駐在員事務所及び銀行業務に従事するその他の外資系機関の設立、組織及び経営について規定している。</p> <p>第 14 条に基づき、金融機関及び外資系銀行の支店は、その顧客の口座、預金、預かり資産及び取引に関する秘密情報を維持し、顧客の同意を得た場合に限り第三者に対し当該情報を提供することを許可される。</p>
<p>オ. 診断治療法（法律第 40/2009/QH12 号）（Law No. 40/2009/QH12 On Medical Examination and Treatment）</p> <p>診断治療法（法律第 40/2009/QH12 号）は 2009 年 11 月 23 日に公布され、2011 年 1 月 1 日より施行された。</p> <p>本法は、患者、医師、診断及び治療施設の権利義務、医師、診断及び治療施設の条件、診断及び治療に関する専門的及び技術的要件、新技術及び手法の診断及び治療への適用、専門的及び技術的ミス、診断及び治療に関する苦情、告発及び紛争の解決、並びに診断及び治療を確保するための条件について規定している。</p> <p>本法は、患者の健康状態及び患者のカルテに記載される個人情報機密が機密に保たれなければならないと規定している。</p> <p>診断及び治療に関する情報を改ざんするためにカルテを消去及び変更することは禁止される。患者の健康状態及び患者のカルテに記載される個人情報の開示には、患者の同意を得なければならない。但し、患者を直接治療する医師の間における、診断、患者のケア及び治療の質の改善を目的とした、又は法令により定められるその他の場合の情報及び経験の交換については、この限りではない。</p>
<p>カ. HIV/AIDS 予防及び管理法（法律第 64/2006/QH11 号）（Law No. 64/2006/QH11 on HIV/AIDS Prevention and Control）</p> <p>HIV/AIDS 予防及び管理法（法律第 64/2006/QH11 号）は 2006 年 6 月 29 日に公布され、</p>

<p>2007年1月1日より施行された。</p> <p>本法は、HIV/AIDSの予防及び管理措置、HIV感染者のケア、治療及び支援、HIV/AIDSの予防及び管理措置の導入条件について規定している。</p> <p>第8条に基づき、本法に定めるいくつかの場合を除き、HIV感染者の氏名、住所及び画像の開示、又は第三者に対するHIV感染に関する情報の開示を行う際には、当該者の同意を得なければならない。</p>
<p>キ. 人の組織及び臓器の提供、摘出及び移植、並びに遺体の提供及び回復についての法律（法律第75/2006/QH11号）（Law No. 75/2006/QH11 on Donation, removal and transplantation of human tissues and organs and donation and recovery of cadavers）</p>
<p>人の組織及び臓器の提供、摘出及び移植、並びに遺体の提供及び回復についての法律（法律第75/2006/QH11号）は2006年11月29日に公布され、2007年7月1日より施行された。</p> <p>本法は、人の組織及び臓器の提供、摘出及び移植、並びに遺体の提供及び回復、組織バンク及び国立臓器移植調整センターの組織及び運営について規定している。但し、輸血及び骨髄移植については、本法では規定されていない。</p> <p>第4条、第11条及び第38条に基づき、臓器提供者及び移植者に関する情報は暗号化され、機密に保たれなければならない。</p>
<p>ク. 伝染病予防及び管理法（法律第03/2007/QH12号）（Law No. 03/2007/QH12 on Prevention and control of infectious diseases）</p>
<p>伝染病予防及び管理法（法律第03/2007/QH12号）は2007年11月21日に公布され、2008年7月1日より施行された。</p> <p>本法は、伝染病の予防及び管理、国境検疫、蔓延防止、及び人の伝染病の予防及び管理の確保条件について規定している。</p> <p>第8条及び第33条は、伝染病にかかっている者に関する情報は、機密に保たれなければならないと規定している。</p>
<p>ケ. 薬事法（法律第105/2016/QH13号）（Law No. 105/2016/QH13 on Pharmacy）</p>
<p>薬事法（法律第105/2016/QH13号）は2016年4月6日に公布され、2017年1月1日より施行された。</p> <p>本法は、調剤薬局及び調剤薬局業界の発展、調剤、調剤薬局業、医薬品及び薬効成分の登録、販売、リコール、薬草成分及び伝統薬、医薬品情報、医薬品の安全性監視、医薬品の広告、臨床薬理学、医療施設における医薬品の管理、医薬品の治験（以下「治験」という。）及び医薬品の生物学的同等性試験、医薬品の品質と薬効成分の管理、並びに医薬品の価格に関する国家の方針について規定している。</p> <p>本法は、治験対象及び生物学的同等性試験の対象者に関する情報は、機密に保たれなければならないと規定する。</p>
<p>コ. 裁判記録法（法律第28/2009/QH12号）（Law No. 28/2009/QH12 on Judicial Records）</p>
<p>裁判記録法（法律第28/2009/QH12号）は2009年6月12日に公布され、2010年7月1</p>

日より施行された。

本法は、裁判記録情報の提供、受領及び更新のための順序及び手続、裁判記録の編集、裁判記録データベースの体系化及び管理、裁判記録カードの発行、並びに国家による裁判記録の管理について規定している。

第2条、第4条及び第9条に基づき、個人のプライバシーは保証される。裁判記録データの不正利用若しくは使用、改ざん又は破壊、裁判記録カードの消去、変更又は偽造といった行為は禁止される。さらに、裁判記録情報は、本法に定める順序及び手続を厳に遵守して適切かつ正確に提供、受領、更新及び処理される。

サ. 刑事訴訟法（法律第100/2015/QH13号）（Criminal Procedure Code No. 100/2015/QH13）⁵

刑事訴訟法（法律第100/2015/QH13号）は2015年11月27日に公布され、2018年1月1日より施行された。

本法は、犯罪情報の申し立て及び処理に関する手続及び形式、起訴、捜査、公訴、判決、及び刑事判決の執行に関する特定の行動指針について規定している。

第12条は、いかなる者も、第三者の住居、プライバシー、個人の秘密、家族の秘密、信書、電話、電信その他の個人的な情報交換形式の安全性及び機密性を不正に侵害することはできないと規定している。住居の捜索、及び信書、電話、電信その他の個人的な情報交換形式の押収若しくは一時的差し押さえは、本法を遵守して行わなければならない。特別な場合には、個室で裁判が行われる。

（3） 監督機関・第三者機関

ベトナムにおいては、個人情報保護について包括的に規定した法律は制定されていない。そして、法律の執行の監督について単独で責任を負う政府機関も設置されていない。

実際、既存の法令の大部分は、情報セキュリティの確保に関する個人、組織、企業及び政府機関の権利及び責任にのみ焦点を当てており、これらの規制の履行及び執行方法についてはあまり取り上げられていない。例えば、LOCIS及び情報技術法は、サイバー情報保護に関する問題について定める2つの主要な法律であるが、関係する個人、組織及び企業の責任及び利益を確保する手段については明確に規定されていない。また、データ主体の権利及び利益の保護に関する制裁措置についても、法制化されていない。

さらに、情報漏えいといった個人情報に関する事象が発生した場合の管轄当局への報告義務について規定する規制も存在しない。

但し、サイバー情報保護に関する主要法令としてのLOCISにおいては、情報通信省（Ministry of Information and Communications、以下「MIC」という。）⁶がこの任務の主

⁵ https://www.jica.go.jp/project/vietnam/021/legal/ku57pq00001j1wz_j-att/legal_20160531_05.pdf（出典 国際協力機構（JICA））

要機関に任命されている。MICにおいてサイバー情報保護は、2017年8月30日付情報通信大臣決定第1439/QĐ-BTTTT号⁷に基づき設置された情報安全局（Authority of Information Security、以下「AIS」という。）⁸、及び2017年8月30日付情報通信大臣決定第1443/QĐ-BTTTT号⁹に基づき設置されたベトナムコンピュータ緊急対応チーム（VIETNAM COMPUTER EMERGENCY RESPONSE TEAMS、以下「VNCERT」という。）¹⁰に割り当てられている。

① AIS

AISは、主として政策立案の機能を有している。AISの主な任務は、MIC大臣に対する、コンピュータ及び情報セキュリティに関する事象に対応したスキーム及びプロジェクトに関するMICの法的文書、年間計画及び戦略の作成及び提出、個人情報に対する損害の防止及び阻止の指導、調整及び体系化への参加、今後起こるサイバー犯罪の攻撃に関し内部組織及び国民を保護及び警告し、大臣により割り当てられるその他の任務を行うことである。またAISは、LOCISの執行の管理及び体系化において、MIC大臣を支援する。AISは主に、情報システムに関する情報の安全性を確保するために、法律文書、戦略、計画及びプロジェクトを指導、体系化及びその構築を検査することに取り組んでいる。さらに、AISは、MICの許可に基づき、ネットワーク情報セキュリティ製品又はサービスの販売に関する申請文書を評価し、営業許可証を付与、再付与又は更新している。

AISは、(i)財務計画部、(ii)政策・国際協力部、(iii)ライセンス部、(iv)監督及び管理部の5つの部門、及び(v)その他のオフィス、並びに(i)情報の安全性の検査センター及び(ii)情報セキュリティ運用のコンサルティング及びサポートセンターの2つの連携ユニットから構成される。

<本部連絡先・幹部>

住所: 8th Floor, The Authority of Radio Frequency Management Building, - 115 Tran
Duy Hung Street - Trung Hoa Ward - Cau Giay District - Hanoi.

Website: <http://ais.gov.vn>

Telephone: +84 24 3943 6684

Fax: +84 24 3943 6684

⁶ <http://english.mic.gov.vn/Pages/home.aspx>

⁷ <http://mic.gov.vn/Upload/VanBan/Q%C4%901439.signed.pdf>

⁸ <https://ais.gov.vn/>

⁹ <https://www.mic.gov.vn/Upload/VanBan/Q%C4%901443.signed.pdf>

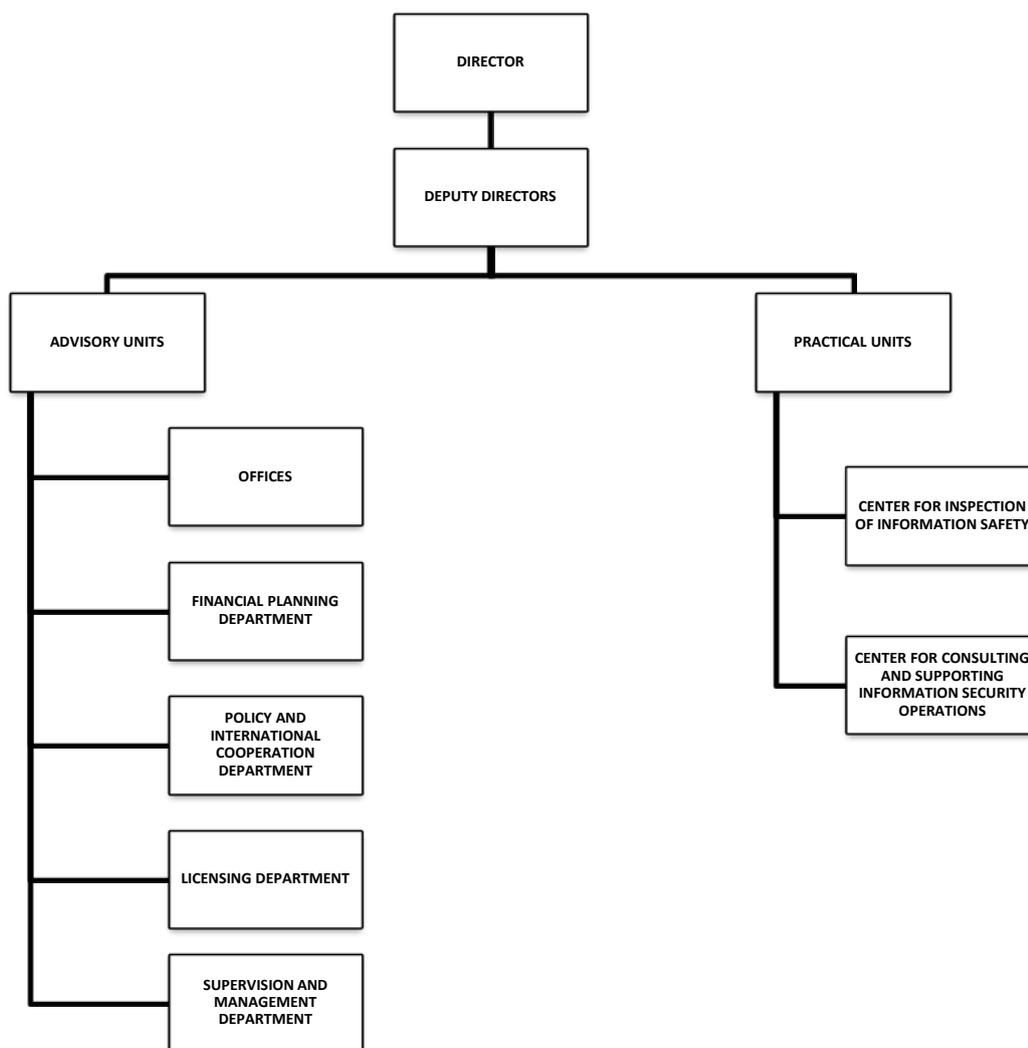
¹⁰ <http://www.vncert.gov.vn/>

情報安全局局長: Mr. Nguyen Thanh Hai

Tel: +84 243943 6999

Email: thanhhai@mic.gov.vn

<組織図>



(出典) <https://ais.gov.vn/co-cau-to-chuc.htm>

② VNCERT

VNCERT は、AIC と比較し、より運用的な任務を割り当てられている。VNCERT はコンピュータクラッシュ時の対応及び情報セキュリティの活動を全国的に調整している。また、すべての機関、組織及び企業におけるコンピュータ緊急対応チーム (CERT) の形成及び発展を促進している。VNCERT もまた、海外の CERT 組織と協力するベトナムの公的機関である。

VNCERT は、情報セキュリティネットワークを監視、収集及び解析し、情報の安全性に関する技術、テクニック及び解決策をリサーチ、開発及び伝達している。

VNCERT は、(i)管理部、(ii)財務計画部、(iii)調整及び対応部、(iv)システムエンジニアリング及び監督部、(v)研究開発部、及び(vi)カウンセリング及び訓練部の6つの部、並びにホーチミン市及びダナンの2つの支部から構成される。

<本部連絡先・幹部>

住所: 5th floor - The Building of Authority of Radio Frequency - 115 Tran Duy Hung
- Trung Hoa Ward - Cau Giay District - Hanoi.

Email: vncert@mic.gov.vn / office@vncert.vn

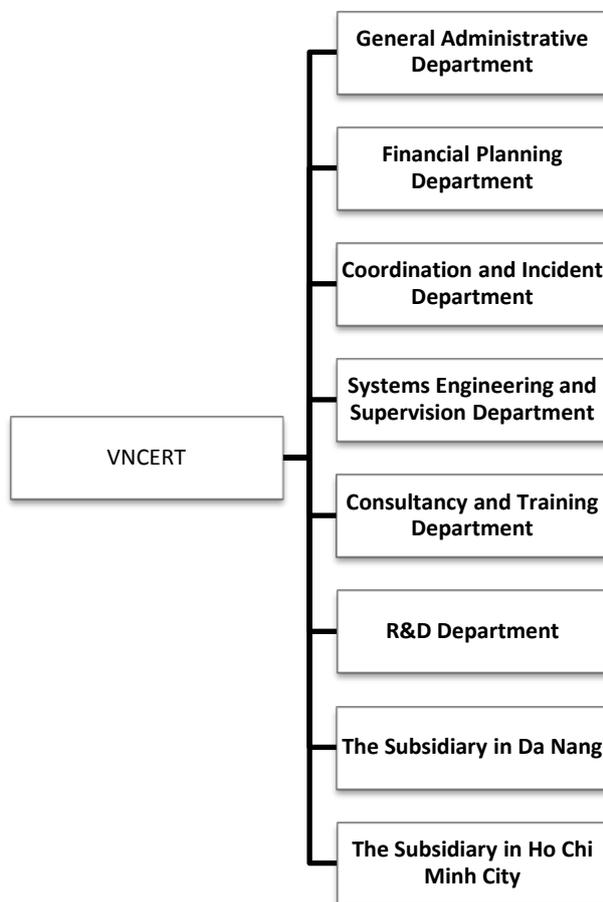
Website: <http://www.vncert.gov.vn>

Telephone: 024.6404423

ダイレクター : Mr. Nguyen Trong Duong

Email: ntduong@vncert.vn

〈組織図〉



(出典) <http://www.vncert.gov.vn/gioi-thieu.php>

(4) 近時のトピック

① 制度改正の検討状況

近年、特にサーバー犯罪に関連した以下のような法令が公布されている。

- ・ 2016年7月1付、民間暗号化製品及びサービスの販売及び提供、並びに民間暗号化製品の輸出入に関する政令第58/2016/ND-CP号
- ・ 2016年7月1付、情報システムのセキュリティの分類に関する政令第85/2016/ND-CP号

- ・ 2016年7月1付、サイバー情報保護サービス及び製品の提供に関する詳細規制に関する政令第108/2016/ND-CP号
- ・ 2016年10月14付、インターネット上での情報紛争の防止に関する政令第142/2016/ND-CP号
- ・ 2017年9月20付、国家情報セキュリティに関する事象の監視及び対応に関する通達第20/2017/TT-BTTTT号
- ・ 情報アクセス法（法律第104/2016/QH13号）は、国民の情報へのアクセス権の行使、情報へのアクセス権を行使するための原則及び手続、国民の情報へのアクセス権の保証に対する国家機関の責任が規定している。本法は、2018年7月1日に施行される。
- ・ 2017年6月6日にサイバーセキュリティ法案（Cyber Security Bill）がパブリックコメントのため公表された後、同法案は継続的に国会で審議されている。同法案は、サイバーセキュリティに関する法的枠組みを確立すること等を目的とし、国家の機密保持活動、インターネット上における秩序及び社会保障を確保のための原則、内容、方法、及び政府機関、法人並びに個人の責任について規定している。同法案審議の過程では、オフショア通信及びインターネット・サービス提供者にベトナムユーザーのデータが管理されるサーバーについて、ベトナム国内に設置することを義務付けることも議論の対象とされている。もっとも、2018年1月に常任委員会で審議された草案では当該義務について定めた条項は削除されている。
- ・ 2018年1月1日に施行された2015年刑法にも、サイバー犯罪に関する新たな条項が加わった。当該条項は、資産の奪取を目的にコンピュータ、電気通信ネットワーク又は電子的手段を使用する行為、銀行口座に関する情報を不正に収集、保存、転送及び開示する行為、並びに有害な方法で無線周波数システムを故意に妨げる行為を罰するものである¹¹。

② 個人情報に関連した主要な裁判例

事例1. クレジットカード情報の窃盗¹²: 2015年12月10日、ハノイ人民裁判所は、Le Dang Hoang Duc氏（1988年生、ホーチミン市1区在住）を、「コンピュータネットワーク、電気通信ネットワーク、インターネットを利用した財産の横領」により第一審公判を開き、懲役36か月の判決を下した。2010年、Duc氏は連続2件の犯罪に成功し、クレジットカード情報を盗み、オンラインで商品を購入し、これらを再販する目的でベトナムに送った。

¹¹ <http://dnrtv.org.vn/tin-tuc-n2176/thao-luan-ve-du-an-luat-bao-ve-bi-mat-nha-nuoc-va-luat-an-ninh-mang.html>

¹² <http://vietnamnet.vn/vn/kinh-doanh/thac-si-an-cap-tien-the-tin-dung-mua-hang-hieu-278308.html>

事例 2. クレジットカード情報の窃盗¹³ : 2017 年 8 月、Nguyen Duong Son Ba 氏率いる 5 名のハッカーで構成される犯罪グループが、ハノイ人民裁判所での裁判にかけられた。この犯罪グループは、海外の信用情報を入手する目的でマルウェア及びブラックコードを作成した。その後、Ba 氏とその仲間は、この情報を利用してオンラインで物品を購入し、クレジットカード情報を再販して利益を得た。

¹³ <https://news.zing.vn/thu-linh-nhom-hacker-danh-cap-thong-tin-the-tin-dung-linh-7-nam-tu-post773985.html>

10. フィリピン

(1) 制度概要

① 法体系の概要

ア フィリピンにおける個人データ保護は、主として単一の法律、すなわち Republic Act No. 10173 (別称 データプライバシー法、The Data Privacy Act of 2012, DPA) によって規制される。同法は、当該分野のフィリピンにおける最初の法律にあたり、民間及び公的部門の双方を規定する。

あらゆる場合に包括的に適用される法律である DPA は、一定の例外を除いて、個人情報に関係する限り一切の取引に適用される。個人情報の利用を規制する産業分野を限定した法律はないものの、秘密情報の開示に対して刑罰を科す法律が複数存在し、その大半が犯罪に関する内容である。本報告書において、秘密情報とは、必ずしも個人情報を含まない。DPA に基づき定義される通り、個人情報 (personal information) とは、身元情報に合理的に関連付けることのできる一切の情報をいう。一方で DPA は、センシティブ個人情報 (sensitive personal information) とみなされる情報を列挙している (ジェンダー、婚姻の有無及び政府発行の個人認証番号等)。

DPA は、特にデータ保護担当者 (Data Protection Officer, DPO) の任命を義務付ける。同法はまた、データ対象者 (data subject) の権利を規定しており、適法な目的、合法的処理、正確性、適切性、指定された目的のためのみの保持及び容易に認証可能な様式での保管の原則等により定められる。DPA に基づく違反通知手続は、国家プライバシー委員会 (National Privacy Commission, NPC) が後に発した通知及び通達において詳細が明示された。

DPA には、越境データ移転に関する特定のガイドライン又は制約に関する規定は存在しない。しかし、DPA に規定されたアカウントビリティの原則に沿って、個人情報管理者は、国内又は国際的であるかを問わず、第三者に対して移転された個人情報について引き続き責任を負うものとする。

フィリピンにおいて DPA は、フィリピンにおける基準となる個人情報保護法規として制定された。DPA は、適用対象となるフィリピンにおけるデータ対象者の個人情報の処理について規定する。¹ その後、フィリピンにおける主たるプライバシー規制監督庁である NPC は、その施行規則及び規制 (Implementing Rules and Regulations, DPA IRR) を発行した。NPC はまた、データ保護担当官 (designation of data protection officers)²、政府機関にお

¹ Explanatory Note to House of Representatives Bill 890, Explanatory Note to House of Representatives Bill 1554, Explanatory Note to Senate 355.

² National Privacy Commission, Advisory no 2017-01, 14 March 2017.

ける個人データのセキュリティ³、政府機関の関与するデータ共有⁴及び個人データ違反管理⁵等の一定の法律要件に関するガイドラインを規定する通達を定期的に発行している。

イ DPA とは別に、個人情報保護に関するその他の法規が以下の通り存在する。

- a. Anti-Photo and Video Voyeurism Act of 2009（写真及びビデオ盗撮禁止法）こと Republic Act 9995 は、一名又は複数の人物がプライバシーを有すると合理的にみなされる状況で、関係当事者の同意なく、性行為又は同様の行為を行う人物を写真又はビデオに撮る行為又は個人の私的エリアの撮影行為を処罰する。
- b. Anti-Wiretapping Law（盗聴禁止法）こと Republic Act 4200 は、盗聴その他の個人の通信のプライバシー侵害を処罰する。
- c. Philippine AIDS Prevention and Control Act of 1998（フィリピン・エイズ予防及び制御法）こと Republic Act 8504 は、HIV 検査を行う個人がその匿名性及びプライバシーを留保する仕組みについて規定する。
- d. Juvenile Justice and Welfare Act of 2006（少年司法及び福祉法）こと Republic Act 9344 は、未成年に関する訴訟手続の記録が公開されることを禁止する。
- e. Special Protection of Children Against Child Abuse, Exploitation and Discrimination Act（児童虐待、搾取及び差別に対する児童の特別保護法）こと Republic Act 7610 は、裁判所が事例に関する管轄権を取得するまで、児童の氏名を公開することを差し控えることを定める。
- f. Anti-violence Against Women and their Children Act of 2004（女性とその子供に対する暴力防止法）こと Republic Act 9262 は、被害当事者に関する記録の秘密性を保持する義務について規定する。
- g. Secrecy of Bank Deposits Act（銀行口座秘密法）こと Republic Act 1405 は、預金に関する情報の機密性の維持及びその例外について定める。
- h. Foreign Currency Deposit Act（外貨預金法）こと Republic Act 6426（その後の改正を含む。）は、外貨預金口座に対する完全な機密性を付与する。さらに、大統領令（Presidential Decree, PD）第 1246 号は、外貨預金口座が預金者の書面による許可によってのみ閲覧することができる旨を定める。
- i. National Internal Revenue Code（国家国内歳入法典）の第 270 条は、納税者の確定申告に関する情報に対して最高度の機密性を付与するものと規定する。さらに、同法第 6 条(F)(3)は、銀行及び金融機関に対して、その保有下にある税務情報を取り扱う際に機密性を確保するよう義務づける。
- j. Credit Information System Act（信用情報システム法）こと Republic Act No. 9510

³ NPC Circular 16-01, 10 October 2016.

⁴ NPC Circular 16-02, 10 October 2016.

⁵ NPC Circular 16-03, 15 December 2016.

は、信用情報の機密性を保持する義務について規定する。

- k. Anti-Money Laundering Act of 2001（資金洗浄防止法）こと Revised Rules and Regulations implementing Republic Act No. 9160 の規則第 9.3.d 項は、該当機関及びその職員に対して、該当する又はその疑いがある取引報告が行われた事実、その内容又はそれに関するその他一切の情報を開示することを禁止する。

② 民間及び公的部門の区分

民間及び公的部門の主な差異として、法の適用範囲が挙げられる。DPA の対象とならない情報の分類の一つに、「独立中央金融官庁並びに法執行規制機関による憲法及び制定法上命ぜられた機能を実行するための個人データの処理を含む、公権力の任務遂行のために必要な情報（information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions.）」がある。⁶

さらに、データプライバシー原則⁷、データ対象者の権利⁸、個人情報のセキュリティに係る規則⁹及び個人情報のアカウントビリティに係る規則¹⁰は、民間及び公的部門に等しく適用されるものの、行政官庁及び機関¹¹によって保持されるセンシティブ個人情報のセキュリティに係る特別規則が存在する。当該規則は、官庁又は組織の長に責任を課し、セキュリティ・クリアランス資格¹²を有する場合を除き、従業員に対してオフラインでのアクセスを禁止し、セキュリティ要件の規定¹³を義務付ける。

③ 連邦法及び州法（Federal and State Law）の存在

フィリピンは連邦国家ではないため、法域内に連邦法又は州法は存在せず、州レベルでの個人データ保護に関する条例等は存在しない。

（2）主な法律の概要

⁶ DPA 第 4 条(e)

⁷ 同法第 11 条以下

⁸ 同法第 16 条以下

⁹ 同法第 20 条

¹⁰ 同法第 21 条

¹¹ 同法第 22 条

¹² 同法第 23 条

¹³ 同法第 32 条、NPC Circular 16-01, 10 October 2016. も参照

① データプライバシー法 (The Data Privacy Act of 2012, DPA)

ア 法律の概要

DPA は、正式名称を「An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes」といい、個人情報の保護を直接の立法目的としたフィリピンにおける唯一の法律である。DPA は、2012 年 8 月 15 日付けで制定され、2012 年 9 月 8 日付けで発効した。同法の施行規則及び規制 (DPA IRR) は、2016 年 8 月 24 日付けで公布された。その後 DPA IRR は、2016 年 9 月 9 日付けで発効した。

DPA にはその制定の背景にある目的を規定する条項がないものの、その第 2 条において方針が規定されており、以下の通り記載されている。

国の方針において、改革及び成長を促進するための情報の自由な流れを保証しつつ、通信のプライバシーに係る基本的人権を保護する。国は、国家建設における情報及び通信技術の不可欠な役割並びに政府及び民間部門の情報及び通信システムにおける個人情報保護されることを保証する本来の義務について認識している。

上記に照らして、DPA の存在意義は、情報の自由な流れを阻害することなく情報に対する権利が十分に保護される法的枠組みを構築することである。

イ 個人情報及びセンシティブ個人情報の定義

個人情報及びセンシティブ個人情報という、DPA に基づく 2 つの重要な概念は、法律上異なる扱いを受け、それらの定義も異なる。DPA の第 3 条 (g) に基づき、個人情報は、以下の通り定義される。

個人情報は、実体的な様式で記録されたか否かにかかわらず、一切の情報に言及する (個人認証が明らかであるもの、情報を保管する企業によって合理的、かつ、直接的に確認が取れるもの又は他の情報と組み合わせたときに直接的かつ確実に個人を特定し得るものを含む。)

他方、DPA の第 3 条 (1) は、以下の方法でセンシティブ個人情報を定義する。

センシティブ個人情報とは、以下の各号に該当する個人情報をいう。

- (1) 個人の人種、民族的出自、婚姻状態、年齢、皮膚の色及び宗教的、哲学的又は政治的所属に関するもの
- (2) 個人の健康、教育、遺伝若しくは性生活又は当該人物によって犯された若しくは犯されたと申し立てられる犯罪に関する手続、当該手続の処理又は当該手続における裁判所の判決に関するもの

- (3) 政府機関から特定の個人に対して発行されたもの（社会保障番号、過去又は現在の健康記録、免許若しくはその拒絶、停止若しくは取消並びに納税申告書（tax returns）を含むがこれに限らない。）
- (4) 執行命令（executive order）又は国会の法律（act of Congress）によって具体的に機密と指定されたもの

ウ 主な規制及び権利の内容

DPA の中核となるのは、情報がいかに適法に処理されるかである。DPA の第 11 条に基づき、個人情報の処理は一般的に認められるが、DPA その他情報の一般開示を認める法律の要件遵守を条件とする。個人情報の適法処理には、透明性の原則、適法な目的及び均衡性の遵守も求められる。

他方で DPA の第 12 条は、個人情報の適法な処理に係る基準を以下の通り規定する。

個人情報の処理は、別途法律により禁止されていない場合に限り、かつ、以下の条件のうち少なくとも一項目が存在する場合、認められるものとする。

- (a) データ対象者が自己の同意を付与した場合
- (b) 個人情報の処理が必要であり、かつ、データ対象者との契約の締結に関連しており、又は契約の締結に先立ち、データ対象者の要請で手続きを踏むために必要である場合
- (c) 個人情報管理者が対象となる法的義務の遵守が処理のために必要である場合
- (d) データ対象者の生死にかかわる重要な利益（生命及び健康を含む。）を保護するために処理が必要である場合
- (e) 国家の緊急事態に対応するため、公共の秩序及び安全要件を遵守するため又は公権力の機能を遂行するために処理が必要である場合（当該任務を遂行するために個人データの処理を必ず含む場合とする。）
- (f) 個人情報管理者又は第三者若しくはデータが開示された当事者によって追求される適法な利益の目的のために処理が必要である場合（ただし、当該利益よりもフィリピン憲法に基づき保護が義務付けられるデータ対象者の基本的権利及び自由が優先する場合を除く。）

DPA の第 13 条は、センシティブ個人情報の処理について言及し、一般的にセンシティブ個人情報は処理されないものとするが、以下の場合を除く。

- (a) 処理に先立ち、データ対象者が目的について特に自己の同意を付与している場合又は秘匿情報の場合については、処理に先立ち交換に関わるすべての当事者がその同意を付与する場合
- (b) 処理が既存法令によって規定されている場合。ただし、当該規制の制定は、センシ

ティブ個人情報及び秘匿情報の保護を保証するものとする。さらに、データ対象者の同意は、センシティブ個人情報又は秘匿情報の処理を認める法令によって義務付けられないものとする。

- (c) データ対象者又は他者の生命及び健康を保護するために処理が必要であり、データ対象者が処理に先立ち、法的又は物理的に自己の同意を示すことができない場合
- (d) 処理が公的機関及びその組織の適法、かつ、非商業的な目的を達成するために必要である場合。ただし、当該処理が当該機関又は組織の善良な職員に関する場合のみとする。さらに、センシティブ個人情報が第三者に対して移転されていないものとする。最後に、データ対象者の同意が処理に先立ち取得されているものとする。
- (e) 処理が治療の目的のために必要であり、医療従事者又は医療機関によって遂行され、個人情報の十分な保護水準による場合
- (f) 処理が裁判所手続、法的請求権の申立て、行使若しくは抗弁において又は政府若しくは公的機関に提供される際、自然人又は法人の適法な権利及び利益の保護に必要な個人情報に関係する場合

適法な処理に係る水準に加えて、個人情報管理者はまた、DPA に規定される多様な組織的、物理的及び技術的セキュリティ対策を遵守することが見込まれている。

同時に、データ対象者は、DPA に基づく一定の権利を享受する。データ対象者は、何についての個人情報が処理され、それがどのように影響するか、個人情報の保護に反対する権利、要求があった場合、処理されている個人情報に関連する一定情報に対する合理的なアクセス権、処理されている個人情報を是正する権利及び当該情報を消去する権利又はその処理を遮断する権利を有する。¹⁴

エ データ違反の報告義務

DPA の第 20 条(f)に基づき、個人情報管理者は、身分詐称を可能とするために使用される可能性のある個人情報又はセンシティブ個人情報が無権限者によって取得されたと合理的に信じられる場合、NPC 及び影響を受けるデータ対象者に対して通知するよう義務づけられる。データ対象者に対する通知義務は、個人情報管理者又は NPC が、不正取得によって影響を受け得るデータ対象者に深刻な損害の実際的なリスクが発生する可能性があると感じるべき事実がある場合も認められる。¹⁵

オ 安全管理対策

¹⁴ DPA 第 16 条

¹⁵ NPC Circular 16-03 も参照

DPAに規定されるセキュリティ対策は、3つに分類することができる。すなわち、組織的、物理的及び技術的なセキュリティ対策である。これらの対策についてはDPA第20条において簡潔に言及されているが、DPA IRRの第26条、第27条及び第28条においてさらに論じられている。NPC通達16-01は、NPCによってDPA IRRにおけるセキュリティ規定を補強するために発行され、政府機関における個人データのセキュリティに正式に対処することを目的とする。

組織的なセキュリティ対策を規定するDPA IRRの第26条に基づき、個人情報管理者及び処理者の双方は、(i) データ保護担当者及びプライバシー・コンプライアンスオフィサー¹⁶を任命しなければならず、(ii)適切なデータ保護方針を導入する義務を負い、(iii)処理活動の記録を維持し、(iv)個人情報の機密性を保持すべく人的資源を監督及び管理し、(v)データ対象者が権利を行使するための手続き及び方針を開発、実施及び精査し、(vi)個人データの収集、同意の取得、特定の適法な目的のために必要な限度における処理、アクセス管理、及びセキュリティ事故発生時に従うべきプロトコルに関する方針及び手続を開発しなければならず、(vii)記録の削除又は処分の条件及び期限管理するデータ保有スケジュールを策定しなければならない。

物理的なセキュリティ対策を規定するDPA IRRの第27条に基づき、DPAは、個人情報管理者及び処理官が電子メディアのアクセス監視、アクセス制限、移転、除外、処理及び再利用に関する方針及び手続を実施及び導入し、個人データを処理する者のプライバシーを確保する方法でオフィススペース及びワークステーションを設計し、職責を決定し、ファイル及び装置の機械的破壊を防止する方針及び手続を開発することを義務付ける。

技術的セキュリティ対策を規定するDPA IRRの第28条に基づき、DPAは、個人情報管理者及び処理者に対して、個人データの処理に関するセキュリティ方針を維持し、偶発的、違法又は不正使用からコンピュータネットワークを保護する保護措置を導入し、機密性、全体性、入手可能性、その処理システム及びサービスの回復力を確保及び保全する能力を開発し、セキュリティ違反の定期的な監視を提供し、物理的又は技術的な事由が発生した場合、個人データの入手可能性及びアクセス権を回復する能力を開発するよう義務づける。

しかし、DPAにおいて採用されるべき特定の対策を規定していないため、DPAにおいて規定されるセキュリティ対策は、これを遵守することとなった場合に民間部門の企業に対し、一定の余地を設けていることに留意すべきである。ただし、NPC Circular 16-01は、一定の制御(AES-256規定の実施等)を策定したために政府機関については、より強固なセキュリティ対策を義務付けている。

カ 適用範囲及び適用除外

DPA第4条に基づき、DPAの規定は、あらゆる種類の個人情報の処理並びに当該処理に関

¹⁶ NPC Advisory Opinion 2017-01も参照

与する自然人及び法人（フィリピンに所在しないものの、フィリピンに所在する装置を使用し、又はフィリピンにおいて事業所、支店若しくは代理店を有する企業を含む。）に対して適用される。換言すると、DPA は一般的にすべての者に適用される。

しかし、DPA の広範な適用範囲にもかかわらず、その領域外の一定項目が未だ存在する。DPA の第 4 条は、以下の通り法律が適用されない特定の事例について規定している。

- (a) 過去又は現在において政府機関の役員又は従業員である一切の個人に関する当該個人の職位又は権能に関する以下を含む情報
 - (1) 個人が現在又は過去に政府機関の役員又は従業員であった事実
 - (2) 個人の役職、勤務先住所及び勤務先電話番号
 - (3) 個人が属する職位に関する分類、収入レベル及び責任
 - (4) 政府による雇用過程において個人が作成した書類上の個人名
- (b) 政府機関のための契約に基づき現在又は過去に業務を履行したのある個人に関する履行业務に関する情報（契約条件、当該業務の履行過程において付与された個人名を含む。）
- (c) 政府から個人に対して与えられる免許又は許認可の付与等、財務的性質の裁量的給付に関連する情報（個人名及び当該便宜の具体的な性質を含む。）
- (d) 報道、芸術、文学又は研究上の目的のために処理される個人情報
- (e) 独立中央金融官庁及び法執行規制機関による、憲法上及び制定法上命ぜられた機能の履行のための個人データの処理を含む、公権力の機能を遂行するために必要な情報。同法におけるいかなる規定も、Republic Act No. 1405（別称「Secrecy of Bank Deposits Act」）、Republic Act No. 6426（別称「Foreign Currency Deposit Act」）及び Republic Act No. 9510（別称「Credit Information System Act (CISA)」）を改正又は廃止したものと解釈されないものとする。
- (f) 独立中央金融官庁又はフィリピン中央銀行（Bangko Sentral ng Pilipinas）の管轄に基づき銀行その他の金融機関が Republic Act No. 9510 及び Republic Act No. 9160（その後の改正を含む。）（別称「Anti-Money Laundering Act」）その他適用法を遵守するために必要な情報
- (g) 外国法域の法律（データプライバシーに関して適用される法令を含む。）に従って当該外国法域における居住者から当初収集された、現在フィリピンにおいて処理が進行中の個人情報

キ 小規模事業の取扱い

上述の通り、DPA の適用可能性は、組織の複雑性又は広範性を考慮しない。さらに、小規模事業も、DPA の規定を遵守しなければならない。ただし、すべての組織体はデータ保護担当者を登録しなければならないものの、すべての組織体がそのデータ処理システムを登録

しなければならないとは限らないことに留意すべきである。¹⁷ 一般的に、従業員が 250 名未満の企業は、上記を義務付けられていない。ただし、当該企業が実行する処理がデータ対象者の権利及び自由に対するリスクを課す虞がある場合、個人情報の処理が不定期でない場合又は処理が 1000 名以上のセンシティブ個人情報を含む場合を除く。¹⁸

ク 情報の越境移転

個人情報の越境又は国際移転を取り扱う DPA の唯一の規定は、同法第 21 条である。

第 21 条 アカウンタビリティの原則 (Principle of Accountability.)

各個人情報管理者は、自己の管理又は管轄下における個人情報（処理のために第三者に対して移転された情報（国内又は国際的であるかを問わず、越境取極及び協力を条件とする。）を含む。）について責任を負う。

- (a) 個人情報管理者は、同法の要件遵守について責任を有し、情報が第三者によって処理されている間、同程度の保護水準を提供するための契約上その他の合理的な手段を用いるものとする。
- (b) 個人情報管理者は、組織による同法の遵守について責任を負う一名又は複数名の個人を任命する。任命された個人の身元は、要請された場合、データ対象者に対して通知されるものとする。

越境移転に関する責任に対するフィリピンの方策は、至って単純である。その管理又は監督下にある個人情報の保護を確保することについて責任を有するのは、当該個人情報が処理のために国外の第三者に対して移転されている場合でも、個人情報管理者である。個人情報管理者は、処理のために個人情報が移転される第三者がフィリピンにおけるものと同程度の保護を提供するよう確保するために契約上その他の手段を用いるよう義務づけられている。

ケ 監督当局及び第三者機関

The National Privacy Commission (NPC) は、DPA の規定を管理及び実施し、データ保護のために設定された国際基準の国による遵守を監視及び確保するために同法によって設立された独立機関である。¹⁹

¹⁷ DPA IRR、規則 XI、 § 47; NPC 通達 17-01 別紙 I も参照

¹⁸ DPA IRR、規則 XI、 § 47; NPC 通達 17-01 別紙 I も参照

¹⁹ DPA 第 7 条

NPC は、個人情報管理者による DPA の遵守を確保する²⁰。NPC は、苦情を受領し、調査を実施し、代替紛争解決プロセスを用いて苦情の解決を調整又は可能とすることができる。²¹ NPC は、同法に基づき、司法省に対して違反の刑事訴追及び刑罰の賦課を奨励する権限を有するが²²、それ自身では当該行為の執行を行うことができない。苦情又は調査を解決するにあたり、NPC は、合議体として行為し、苦情の対象となる個人情報に対するアクセス権及びその機能を履行するために必要な情報を収集する権利を付与されている。²³ NPC の知るところとなり、所有下に置かれることとなる一切の情報は、秘密情報とみなされる。²⁴ 同委員会はまた、処理が国家の安全及び公共の利益を害すると判断した場合、排除措置命令を発行し、個人情報の処理に係る一時的又は恒久的禁止を課す権限を有する。²⁵ その独立性をさらに強化するため、法律により、その命令を遵守し、又はデータプライバシーに影響を与える事項について措置を行うために委員会が企業、政府機関又は組織に対して強制力を行使し、又は申立てを提起する権限が認められている。²⁶

政府機能の履行に従った個人情報の処理は DPA の範囲外であるものの、NPC は、他の機能に従った政府による個人情報の処理について管轄権を有している。NPC は、セキュリティ及び技術対策について他の政府機関又は組織の遵守を監視し、DPA の最小限の水準を充足するために必要な措置を勧告するよう任命されている。²⁷

NPC はさらに、国家のデータプライバシー方針の開発を任ぜられている。第一に、同委員会は、必要に応じてデータプライバシー又はデータ保護に係るフィリピン法に対する立法、改正又は修正を提案することができる。²⁸ 委員会はまた、提案された国又は地域の制定法、規制又は手続のデータプライバシーに関する傾向についてコメントし、助言的意見を発行し、DPA その他データプライバシー法の規定に解釈を加えることができる。²⁹ 同法は、他の政府機関及び民間部門と協力し、国内における個人情報保護を強化するための計画及び政策を策定及び実施するよう義務づけている。³⁰ 法律の実務的な解釈を補助するため、委員会はまた、データ保護に関するすべての法律についての指南書を定期的に発行するよう任命されている。³¹ 同委員会は、個人情報管理者によって任意に遵守されるプライバシー法

²⁰ 同法第 7 条(a)

²¹ 同法第 7 条(b)

²² 同法第 7 条(i)

²³ 同法第 7 条(i)

²⁴ 同法第 8 条

²⁵ 同法第 7 条(c)

²⁶ 同法第 7 条(d)

²⁷ 同法第 7 条(e)

²⁸ 同法第 7 条(m)

²⁹ 同法第 7 条(l)

³⁰ DPA 第 7 条(f)

³¹ 同法第 7 条(g)

規を精査、承認、却下し、又は修正を要求することができる。³² 委員会はまた、国若しくは地方政府機関、民間企業又は個人の要請により、プライバシー又はデータ保護に関する事項に係る支援を提供することができる。³³

NPC は、他国のデータプライバシー規制機関及び民間のアカウントビリティ機関と共に適切、かつ、効率的な協調を確保し、データプライバシー保護のための国際的及び地域的なイニシアチブに参加するよう任命されている。³⁴ 個別のプライバシー法の越境適用及び実施について委員会は、他国のその他のデータプライバシー当局と交渉し、連絡を行うことができる。³⁵ 委員会はまた、海外のプライバシー又はデータ保護法令に対応するために海外で事業を行うフィリピンの会社を支援³⁶し、国境を越えたデータプライバシー保護の実施を容易にするために必要な行為全般を履行するよう任命されている。³⁷

(ア) 監督当局の組織概要

NPC は、情報通信技術省 (The Department of Information, Communications and Technology, DICT) の外局にあたる。NPC は、(1) Privacy Commissioner 1 名 (現 Raymund Liboro 氏) 及び(2) Deputy Privacy Commissioners 2 名によって統括されている。11 部門から構成される 4 事務所から成り、職員数は 99 名である。事業所及び各事業所の部門は、以下の通りである。³⁸

1. Data Security and Compliance Office (データセキュリティ及びコンプライアンスオフィス)
 - ・ Compliance and Monitoring Division (コンプライアンス及び監視部門)
 - ・ Data Security and Technology Division (データセキュリティ及び技術部門)
2. Legal and Enforcement Office (法務及び執行オフィス)
 - ・ Legal Division (法務部門)
 - ・ Complaints and Investigation Division (苦情及び調査部門)
 - ・ Enforcement Division (執行部門)
3. Finance and Administrative Office (財務及び管理オフィス)
 - ・ Financial Planning and Management Division (財務計画及び管理部門)
 - ・ Administrative Services Division (管理サービス部門)

³² 同法第 7 条(j)

³³ 同法第 7 条(k)

³⁴ 同法第 7 条(n)

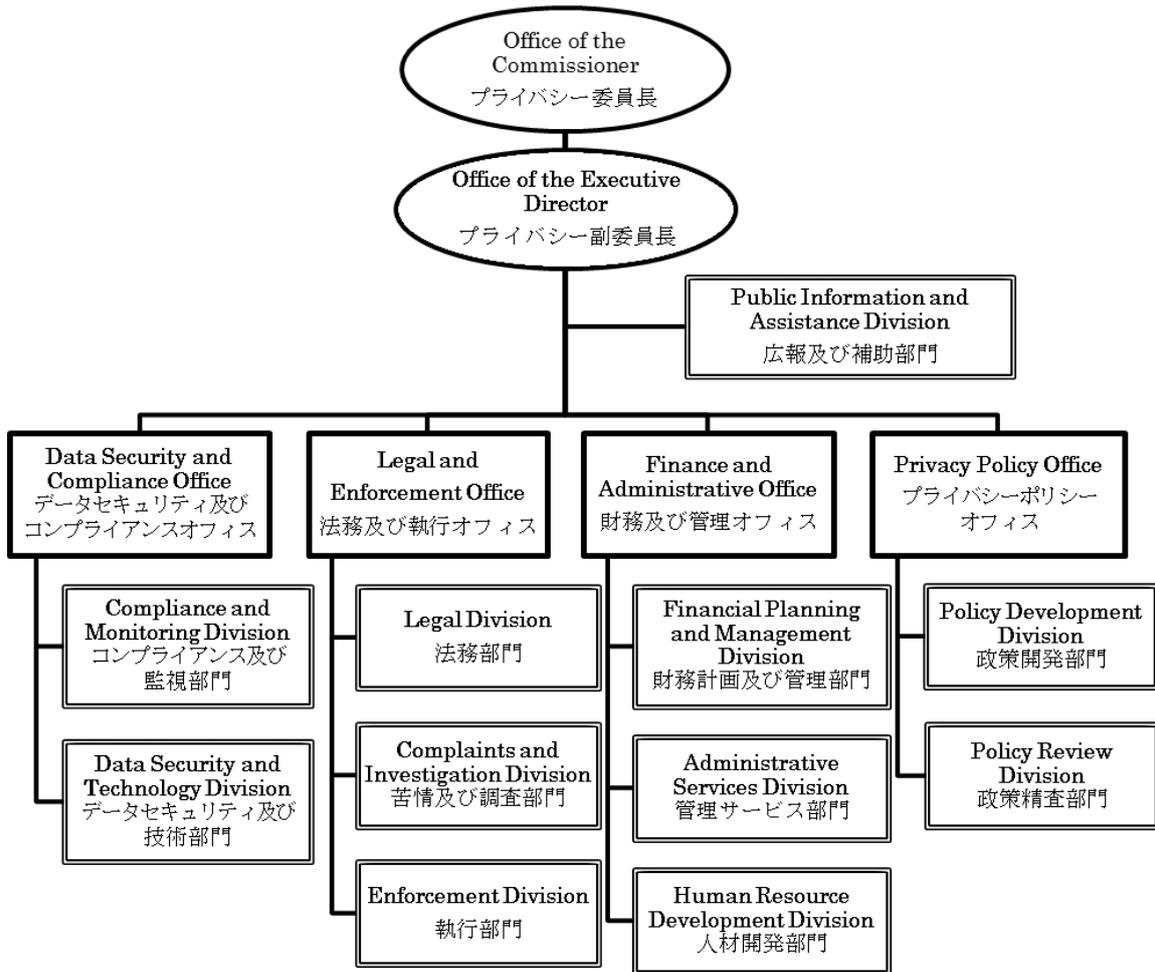
³⁵ 同法第 7 条(o)

³⁶ 同法第 7 条(p)

³⁷ 同法第 7 条(q)

³⁸ <https://privacy.gov.ph/about-us/#comms> (アクセス日 : 2018 年 2 月 26 日)

- Human Resource Development Division (人材開発部門)
- 4. Privacy Policy Office (プライバシーポリシーオフィス)
- Policy Development Division (政策開発部門)
- Policy Review Division (政策精査部門)



DPA の第 41 条において、国は NPC に対して 2,000 万ペソの当初割当てを提供するよう義務づけられており、設立時に特別目的基金から 1,500 万ペソ及び職員諸給付基金 (Miscellaneous Personnel Benefits Fund) から取得された 1,271 万 2,289 ペソの資金を割り当てた。³⁹ 当初割当てに加えて、同法はまた、NPC が国より毎年 1,000 万ペソを受領するよう規定している。⁴⁰

(イ) 監督当局による執行

DPA 施行により影響を受ける既存の産業、事業及び事務所は、DPA を遵守するために、2017 年 9 月 9 日まで又は DPA の施行規則及び規制の公布から 1 年の猶予を付与される。⁴¹ 以来、NPC は、主要数社に対して遵守監査を実施した。国の投票者データベースがインターネット上で漏えいされた 2017 年の Comeleak 事件期間中、NPC は、データ違反について選挙委員長 の J. Andres D. Bautista 氏に対する委員会の刑事訴追を勧告した。⁴²

② 個人情報保護に関するその他の法令

ア 写真及びビデオ盗撮禁止法 (Anti-Photo and Video Voyeurism Act of 2009) (2010 年 2 月 15 日制定)

(ア) 関連法の背景にある目的

目的条項はないものの、第 2 条において、以下の方針を明らかにしている。国は、すべての人間の尊厳及びプライバシーに価値を置き、人権に対する完全な尊重を保証する。この目的に向けて、国は、誇り、尊厳及び品位を損なう可能性のある行為を処罰する。

(イ) 主たる規制及び権利の内容

第 4 条は、「一名又は複数の人物がプライバシーを有すると合理的にみなされる状況で、関係当事者の同意なく、性行為若しくは同様の行為を行う一名若しくは複数名のグループ又は個人の私的なエリア」を撮影した写真又はビデオを違法としている。

³⁹ NPC 2016 Annual Report P. 34

⁴⁰ DPA 第 41 条

⁴¹ 同法第 39 条

⁴²

<https://privacy.gov.ph/privacy-commission-finds-bautista-criminally-liable-for-comeleak-data-breach/> (アクセス日：2018 年 2 月 26 日)

イ 盗聴禁止法 (Anti-Wiretapping Law) (1965 年 6 月 19 日発効)

(ア) 関連法の背景にある目的

同法は、目的条項を有しない。

(イ) 主たる規制及び権利の内容

同法は、当事者によって承認されていない「ディクタフォン、ディクトグラフ、電話盗聴器、トランシーバ又はテープレコーダー（その他の呼称を問わない。）として一般に知られている装置を使用して当該通信又は話し言葉を秘密に盗聴、傍受又は記録する」行為を違法としている。

ウ フィリピン・エイズ予防及び制御法 (Philippine AIDS Prevention and Control Act of 1998) (1998 年 2 月 13 日制定)

(ア) 関連法の背景にある目的

目的条項はないものの、第 2 条において表明されている方針において、HIV/AIDS 感染者又はその疑いがある者の人権の保護を完全にするため、プライバシー権が保証されることが明らかにされている。

(イ) 主たる規制及び権利の内容

同法第 1 条において、国は、「匿名での HIV 検査についての仕組みを提供し、当該検査の実施における匿名性及び医療上の機密性を保証するものとする (shall provide a mechanism for anonymous HIV testing and shall guarantee anonymity and medical confidentiality in the conduct of such tests)。」と規定している。

エ 少年司法及び福祉法 (Juvenile Justice and Welfare Act of 2006) (2006 年 5 月 21 日発効)

(ア) 関連法の背景にある目的

目的条項はないものの、第 2 条において表明されている方針において、国連児童の権利

に関する条約の第 40 条に従い、国は、刑法に抵触したと申し立てられ、訴追され、判断又は認識されたすべての児童の権利は、児童の年齢及び当該児童の社会への復帰願望を考慮して、児童の尊厳及び価値を促進させるような方法で取り扱われるべきである旨が明らかにされている。

(イ) 主たる規制及び権利の内容

同法第 43 条は、「当初の接触から最終処置までの法律上の紛争に児童を関与させる一切の記録及び手続は、極秘、かつ、機密とみなされるものとする ([a]ll records and proceedings involving children in conflict with the law from initial contact until final disposition of the case shall be considered privileged and confidential.)」よう義務付けている。

オ 児童虐待、搾取及び差別に対する児童の特別保護法 (Special Protection of Children Against Child Abuse, Exploitation and Discrimination Act) (1992 年 6 月 17 日承認)

(ア) 関連法の背景にある目的

目的条項はないものの、第 2 条において表明されている方針において、公的又は民間を問わず、社会福祉機関、司法裁判所、行政当局及び立法機関によって行われる児童に関する一切の措置において、国連児童の権利に関する条約において明言されている「子ども最優先 (First Call for Children)」の原則に従った最大の考慮がなされるべきことが明らかにされている。

(イ) 主たる規制及び権利の内容

同法第 29 条に基づき、「加害当事者からの要請があった場合、その氏名は、裁判所が当該事例に関して管轄権を取得するまで、公開を差し控えることができる (at the instance of the offended party, his name may be withheld from the public until the court acquires jurisdiction over the case.)」。

カ 女性とその子供に対する暴力防止法 (Anti-violence Against Women and their Children Act of 2004) (2004 年 3 月 27 日発効)

(ア) 関連法の背景にある目的

目的条項はないものの、第 2 条において表明されている方針において、国は、女性及び子供に対する暴力に対処するため、憲法及び世界人権宣言の規定 (Constitution and the Provisions of the Universal Declaration of Human Rights)、女性に対するあらゆる形式の差別の撲滅に関する条約 (the convention on the Elimination of all forms of discrimination Against Women)、子どもの権利条約 (Convention on the Rights of the Child) その他フィリピンが加盟国となっている国際人権法に基づき保障された基本的自由を保持することにおいて努力すべきことが明らかにされている。

(イ) 主たる規制及び権利の内容

同法第 44 条は、「自治行政区 (barangay) におけるものを含む女性及びその子供に対する暴力に関する一切の記録は、機密であり、一切の公的担当者及び従業員並びに公的又は民間診療所及び病院は、被害者のプライバシー権を尊重するものとする ([a]ll records pertaining to cases of violence against women and their children including those in the barangay shall be confidential and all public officers and employees and public or private clinics to hospitals shall respect the right to privacy of the victim.)。」と義務付ける。

キ 銀行口座秘密法 (Secrecy of Bank Deposits Act) (1955 年 9 月 9 日発効)

(ア) 関連法の背景にある目的

同法には、目的条項がない。

(イ) 主たる規制及び権利の内容

同法第 2 条は、「フィリピンにおける銀行又は金融機関のすべての預託(フィリピン政府、政府部門及びその機関による発行債券への投資を含む。)は、絶対的に機密の性質とみなされるものとし、調査を行ってはならない ([a]ll deposits of whatever nature with banks or banking institutions in the Philippines including investments in bonds issued by the Government of the Philippines, its political subdivisions and its instrumentalities, are hereby considered as of an absolutely confidential nature and may not be examined …)。」としている。

ク 外貨預金法 (Foreign Currency Deposit Act) (1974 年 4 月 4 日発効)

(ア) 関連法の背景にある目的

同法には、目的条項がない。

(イ) 主たる規制及び権利の内容

同法第 8 条は、「本法律（その後の改正を含む。）に基づき PD 第 1035 号によって承認された一切の外貨預金及び PD 第 1034 号に基づき承認された外貨預金は、絶対的に秘密の性質とみなされるとここに明示する（[a]ll foreign currency deposits authorized under this Act, as amended by PD No. 1035, as well as foreign currency deposits authorized under PD No. 1034, are hereby declared as and considered of an absolutely confidential nature…）」と規定する。

ケ 国家国内歳入法典 (National Internal Revenue Code) (1998 年 1 月 1 日発効)

(ア) 関連法の背景にある目的

目的条項はないものの、第 2 条は、以下の通り方針を明らかにしている。

フィリピンの内国歳入税制 (internal revenue tax system) (税務管理を含む。) の合理化を通じた持続可能な経済成長を促進し、可処分所得の水準を高め、経済活動を増大させるためにより多くの納税者に対して衡平法上の救済手段を可能な限り提供し、地域及び世界市場において企業のより良い競争が可能となるよう強固な事業環境を創造し、並びに政府がその管轄及び管理下にある者のニーズを提供できるよう国が確保する国家としての方針をここに明示する。

(イ) 主たる規制及び権利の内容

同法第 270 条は、内国歳入局 (the Bureau of Internal Revenue) の職員又は従業員に対して、「納税者の事業、収入若しくは資産、製造業者若しくは生産者の秘密、経営、様式若しくは業務、器具又は納税者の事業に関する秘密情報をいずれの者に対して漏えいし、又は法律により規定された方法を除くその他一切の方法により公開する (to any person or makes known in any other manner than may be provided by law information regarding the business, income or estate of any taxpayer, the secrets, operation, style or work, or apparatus of any manufacturer or producer, or confidential information regarding the business of any taxpayer, …)」ことを禁止する。

コ 信用情報システム法 (Credit Information System Act) (2008年10月31日承認)

(ア) 関連法の背景にある目的

目的条項はないものの、第2条は、以下の通り方針を明らかにしている。

国は、金融システムに参加しているすべての事業体の信用及び信用関連活動に関係する又はこれに起因する公正、かつ、正確な情報の収集及び拡散のための包括的、かつ、中央集権的な信用情報システムの構築の必要性を認識している。信用情報システムは、借主の信用状態及び履歴に関する信頼できる信用情報の必要性に直接対処する。

信用情報システムの運用及びサービスについて、特に中小企業及び零細企業の信用の全体的な利用可能性を大きく改善し、信用のコスト効率化を図るメカニズムを提供し、与信枠を確保するための担保への過度の依存を減少させることが期待されている。

国は、すべての参加者に対して最小のコストで信用情報が提供されるよう努力し、消費者の権利保護及び産業界における公正競争を常に確保するものとする。

また、効率的な信用情報システムにより、金融機関がその全体的な信用リスクを減少し、より健全、かつ、安定した金融システムに貢献することが可能となる。

(イ) 主たる規制及び権利の内容

同法第8条は、「[信用情報]会社、提出企業、アクセス企業、外注先企業、特別アクセス企業及び適式に授権されたアクセス企業でない企業は、厳格な秘密保持に基づき信用情報を保管するものとし、これを借主の信用力を確立する明示された目的のためだけに使用するものとする ([Credit Information] Corporation, the submitting entities, the accessing entities, the outsource entities, the special accessing entities and the duly authorized non-accessing entities shall hold the credit information under strict confidentiality and shall use the same only for the declared purpose of establishing the creditworthiness of the borrower.)」と義務付ける。

サ 資金洗浄防止法 (Anti-Money Laundering Act of 2001) (2012年8月23日承認)

(ア) 関連法の背景にある目的

目的条項はないものの、第2条は、以下の通り方針を明らかにしている。

国は、フィリピンが違法収益のマネーロンダリングの場とされないよう銀行口座の健全性と機密性を保護及び維持する。また、国は、外交政策の一環として、マネーロンダリン

グがどこで行われたかに関わらず越境捜査とマネーロンダリング関与者の訴追に対し国際協力をするものとする。

(イ) 主たる規制及び権利の内容

同法第 9 条(c)は、適用対象機関が取引発生から 5 営業日以内に資金洗浄防止評議会 (Anti-Money Laundering Council, AMLC) に対して当該取引について報告するよう義務づけ、第 14 条(d)は、懲役に関する当該報告の秘密保持に違反した場合、処罰する旨規定する。

(3) 最近のトピック

① 制度改正の検討状況、個人情報に関連した政策動向

DPA の可決以来、いかなる類似の立法も可決されていない。しかし NPC は、DPA の規定に関して明確性を期すため、定期的に通達及び助言的意見を発表している。NPC は、政府における個人情報のセキュリティ⁴³、政府機関におけるデータ共有合意⁴⁴、個人データ違反管理⁴⁵、NPC に対する苦情の届出手続規則⁴⁶及びデータ処理システムの登録⁴⁷に関するガイダンス等を提供している。

② 個人情報に関連した主要な裁判例

本報告書の日付現在、フィリピン最高裁判所は、未だ DPA を正面から取り扱う事項に対処していない。

⁴³ NPC Circular 16-01

⁴⁴ NPC Circular 16-02

⁴⁵ NPC Circular 16-03

⁴⁶ NPC Circular 16-04

⁴⁷ NPC Circular 16-05

1 1. インドネシア

(1) 制度概要

① 法体系の概要

インドネシア政府 (the Government of Indonesia, *Pemerintah Indonesia*¹) は、本報告書の作成時点までの間、個人情報や個人データの保護に特化して規制する法律 (Law, Undang-Undang/UU) を公布しておらず、個人データの保護に関する規定は、銀行についての法律や以下に定義する電子情報・取引法をはじめとする複数の法律に盛り込まれてきた。以下に定義する 2016 年電子システム通信情報省規則 (MoCI Reg. 20/2016) では、電子システムプロバイダ (Electronic System Providers, *Penyelenggara Sistem Elektronik*) による個人データの保護の要件を定めるに当たって、個人データの一般的な保護を実施するレギュレーションが法制化され、より詳細なアプローチが取られた。2016 年電子システム通信情報省規則において、「個人データ」(Personal Data, *Data Pribadi*) は、保管され管理された一定の個人のデータであって、その正確性が維持され、かつ、その秘密性が保護されなければならないものをいうと定義されている。「機微情報」(Sensitive Information, *informasi sensitif*) は、インドネシアにおけるデータ保護の規則において、法的に定義されていない。電子情報・取引法に定められているとおり、個人データ保護の規則は、同法によって規制されるインドネシアの法域内外における法律行為であって、インドネシアの法域内若しくは当該法域外又はその双方において法的効力を及ぼし、インドネシアの利益を害するものを行う、いかなる者にも適用される。通信情報省²は現在、個人データの越境移転を含む個人データ保護の実施を監督している。

なお、個人データの保護に関して、民間部門と公的部門の間には区別がない。本件において、現行のインドネシア法において規定される個人データの保護は、官民いずれの部門におけるデータに対しても適用される。ただし、公共サービスの電子システム運用者が、国家主権の執行による法執行及びインドネシア国民のデータ保護を目的として、インドネシアの領域内に、データセンター及び災害復旧センターを設立する義務を負う。

¹ インドネシアにおける業務の利便性の観点から、インドネシアについては、英語表記に続けて、インドネシア語を記載する。

² 通信情報大臣は、Minister of Communication and Informatics といい、一般的に MoCI と略称される。同大臣のインドネシア語は、*Menteri Komunikasi dan Informatika* である。

② 適用される主な連邦法

ア インドネシア共和国 1945 年憲法

インドネシアの法令における最高法規は、インドネシア共和国 1945 年憲法であり、全ての人々が自己の「プライバシー権」に関して保護を受ける権利を有すると定める第 28G 条第 (1) 項は、個人データの保護に関する規範を黙示的に包含している。個人データの保護に関する規定は、以下のものをはじめとする法令に定められている。

イ 2008 年電子情報及び取引に関する法律 (2008 年法律第 11 号。2016 年法律第 19 号により改正。) (Law No. 11 of 2008 regarding Electronic Information and Transactions, as amended by Law No. 19 of 2016、*Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana diubah dengan Undang-Undang No. 19 Tahun 2016*) (以下「電子情報・取引法」という。)

ウ 2012 年電子システム及び取引の実行に関する政府規則 (2012 年政府規則第 82 号) (Government Regulation No. 82 of 2012 regarding the Implementation of Electronic Systems and Transactions、*Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*) (以下「2012 年電子システム規則」という。)

エ 2016 年電子システムにおける個人データの保護に関する通信情報大臣規則 (2016 年通信情報大臣規則第 20 号) (Minister of Communication and Informatics Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic Systems、*Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik*) (以下「2016 年電子システム通信情報省規則」という。)

オ 1992 年銀行法 (1992 年法律第 7 号。1998 年法律第 10 号により改正。) (Law No. 7 of 1992 as amended by Law No. 10 of 1998 on Banking、*Undang-Undang No. 7 Tahun 1992 tentang Perbankan sebagaimana diubah dengan Undang-Undang No. 10 Tahun 1998*) (以下「銀行法」という。)

カ 決済システムサービスの顧客の保護に関する 2014 年インドネシア中央銀行規則 (2014 年インドネシア中央銀行規則第 16/1/PBI) (Bank Indonesia Regulation No. 16/1/PBI/2014 concerning the Protection of Payment System Service Consumers) (以下「2014 年インドネシア中央銀行規則」という。)

③小規模事業者の取扱いについての特則の有無

小規模事業については、個人データ保護に関する特定の規制は存在しない。したがって小規模事業は、個人データ保護に関する一般規制に従う。

(2) 主な法律の概要

① 1945年インドネシア共和国憲法

ア 概要

1945年にインドネシア共和国憲法(the 1945 Constitution of the Republic of Indonesia、*Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*) が制定され、その後 1999年、2000年、2001年及び2002年に改正されている。

イ 主要な規制及び権利

インドネシアの法令における最高法規は、インドネシア共和国 1945年憲法であり、全ての人々が自己の「プライバシー権」に関して保護を受ける権利を有すると定める第 28G 条第(1)項は、個人データの保護に関する規範を黙示的に包含している。インドネシア共和国憲法裁判所(The Constitutional Court of the Republic of Indonesia、*Mahkamah Konstitusi Republik Indonesia*) は、この規定を情報プライバシー権(データ保護)を内実とする「プライバシー権」(“right to privacy”、“*hak rahasia pribadi*”)を保障するものと解釈している。個人データの保護に関する規定は、以下のものをはじめとする法令に定められている。

② 電子情報・取引法

ア 法律の概要

電子情報・取引法が制定され、2008年4月21日付で施行された。

イ 目的規定

第4条第(2)項は、その目的を以下のとおり定める。すなわち、情報技術及び電子取引の利用は、(i)国際情報社会の一部としての国民生活を啓蒙すること、(ii)人民の福祉を向上させるために貿易及び国家経済を発展させること、(iii)公共サービスの有効性及び効率性を向上させること、(iv)情報技術を利用及び活用する現場において、各人が最適、かつ、責任をもって、自己の思考や能力を向上させる機会を可能な限り広げること、(v)情報技術の利用者及び提供者に安心感、公平感及び法的確実性を与えること、以上の5つの目的をもって実行される。

ウ 個人情報 の定義、機微情報の定義

個人情報及び機微情報 (sensitive information) の定義を定めていない。

エ 主要な規制及び権利

第26条第(1)項の注釈によると、個人データ保護をプライバシー権の一部と定義している。プライバシー権とは、(i)いかなる脅威も受けることなく自己の私生活を楽しむ権利、(ii)秘密裏に監視されることなく他者と通信する権利及び(iii)私生活及びデータに関連する情報アクセスを管理する権利をいう。法令に別途定める場合を除き、ある者の個人データが含まれる電子媒体経由での情報の利用は、電子情報・取引法第26条第(1)項によれば、本人の同意をもって、行わなければならない。電子情報・取引法上、権利を侵害された者は、被った損害について賠償を請求することができる。

本規定は、個人データの処理を適法に行う根拠として、(i)同意及び(ii)現行法といった2つの法的根拠を定めている。これらの根拠によらず個人データの処理が行われた場合、当該処理は違法となる。さらに、個人データ保護の責任及び義務は、一義的に、電子媒体内にある個人データの各利用者（データ管理者又はデータ処理者であるかにかかわらず、データ利用者）が負う。

オ 漏えい等事案発生時の本人及び監督機関等への報告義務

監督当局及び本人に対する報告義務に関する条文を定めていない。

カ 安全管理措置に関する規定

安全管理措置に関する条項はない。

キ 適用範囲、適用除外内容

2016年電子システム通信情報省規則は、電子情報・取引法及び2012年電子システム規則の施行規則であるため、その適用範囲は、電子情報・取引法第2条（以下のとおり。）に従う。「本法は、インドネシアの法域の内外にかかわらず、インドネシアの法域内及び法域外で法的効力を有し、インドネシアの利益に弊害をもたらす法律行為を本法に従って行う者に適用される。」

ク 国際的な情報移転に関する規定

国際的な情報移転に関する条項はない。

③ 2012年電子システム規則

ア 法律の概要

2012年電子システム規則が制定され、2012年10月15日付で施行された。

イ 目的規定

目的条項を定めていない。

ウ 個人情報の定義、機微情報の定義

第1条第(27)項は、個人データを、「個人データとは、保管及び管理された一定の個人データであって、その正確性が維持されなくてはならず、その秘密性が保護されなくてはならない情報をいう。」と定義している。なお、2012年電子システム規則は、機微情報の定義を定めていない。

エ 主要な規制及び権利

2012年電子システム規則には電子情報・取引法の手続ガイドラインが存在している。第1条第(27)項は、保管及び取扱われており、かつ、その真実性及び秘密性が保護されなければならない特定の個人のデータを、個人データと定義している。さらに、第15条は、電子システム運用者が以下の行為を行わなければならないと定めている。すなわち、(i)管理さ

れる個人データの秘密性、完全性及び入手可能性を確保すること、(ii)規則によって別途定められる場合を除き、個人データの取得、使用及び利用が個人データ所有者の承認に基づいて行われるよう確保すること、(iii)詳細にわたる内容の使用又は開示が、当該個人データ所有者の承認に基づき、かつ、データ取得時に個人データ所有者から取得した目的に従って行われるよう確保することを求めている。

また、同規則では、データの完全性が規制されているため、個人データを保護できなかった場合、当該個人データの所有者に書面により通知しなければならない。

オ 漏えい等事案発生時の本人及び監督機関等への報告義務

監督当局及び本人に対する報告義務に関する条文を定めていない。

カ 安全管理措置に関する規定

安全管理措置に関する条項はない。

キ 国際的な情報移転に関する規定

国際的な情報移転に関する条項はない。

④ 2016年電子システム通信情報省規則

ア 規則の概要

2016年電子システム通信情報省規則が制定され、2016年12月1日付けで施行された。通信情報省により発令された、電子システムに含まれる個人データの保護に特化した2012年電子システム規則の実施規則である。

イ 目的規定

目的条項を定めていない。

ウ 個人情報 の定義、機微情報の定義

2012年電子システム規則に沿って、2016年電子システム通信情報省規則第1条第1項は、個人データを「個人データとは、保管及び管理された一定の個人データであって、その正

確性が維持されなくてはならず、その秘密性が保護されなくてはならない情報をいう。」と定義している。さらに、第1条第2項は、「一定の個人データ」を、各個人に結びつく、直接的であるか間接的であるかを問わず、当該個人を特定可能な、その目的が法令に従っている、正確かつ事実に関する情報、と定義している。以上から、インドネシア法は、機微情報について定義されていない。本件において、保管及び管理され、その秘密性が維持されなければならない、個人に結びついた、当該個人を特定可能な機微情報は、個人データに該当し、2016年電子システム通信情報省規則に基づき保護される。

エ 主要な規制及び権利

2016年電子システム通信情報省規則は、電子システム内における個人データの保護を規制しており、以下の保護を定めている。

個人データの取得及び収集は、以下の通り、第7条乃至第11条で規制されている。すなわち、(i)個人データの取得は、当該データの取得目的に従い、関連する情報に限定され、(ii)個人データ所有者に対し、(a)個人データの秘密性及び非秘密性並びに(b)個人データの変更、追加又は更新に関する選択権を電子システムにおいて提供しなければならない、(iii)個人データは、個人データ所有者の承認又は法令に基づいて取得しなければならないことに加え、(iv)取得した個人データは、個人データ所有者からの確認を取らなければならない、(v)電子システムは、相互運用性及び互換性を備えていなければならない、正規ソフトウェア上で実行しなければならない。

個人データの処理及び解析については、以下の通り、第12条乃至第14条に定められている。すなわち、(i)個人データは、データの取得及び収集時に明示された電子システム提供者の要請に従った場合に限り処理及び解析することができる。(ii)個人データの処理及び解析は、個人データ所有者の承認をもって行わなければならない。(iii)処理及び解析された個人データは、その正確性が検証された個人データでなければならない。(iv)個人データの保管については、以下の通り、第15条乃至第20条に定められている。(v)電子システムに保管されている個人データは、その正確性が検証された個人データでなければならない。(vi)個人データは、暗号化された形式で保存しなければならない。(vii)個人データは、(a)個人データの保存期間について定める法令に基づき、又は、特に定められていない場合は、5年以上の期間にわたり、かつ、(b)セキュリティ手続及びセキュリティ手段に従って、電子システムに保存しなければならない。(viii)公共サービスの電子システム提供者は、現地のデータセンター及び災害復旧センターを設立しなければならない。(ix)個人データ所有者は、法令に従って、各自の個人データの削除を求めることができる。

個人データの掲載、公開、送付、拡散又は個人データへのアクセスについては、以下の通り、第21条乃至第24条に定められている。すなわち、(i)個人データは、本人の承認を取得した場合に限り、当該データの取得目的に則してその正確性が検証された後に、表示、

公開、送信、拡散又はアクセスすることができる。(ii)電子システム提供者は、その電子システム又はその電子システムから生じた個人データに記載される個人データを法執行担当官に提供しなければならない。(iii)表示、公表、送信、配布又はアクセスされた個人データは、承認に基づいて、かつ、当該データの取得目的に沿って使用及び利用しなければならない。

インドネシア所在の、政府機関、地域政府若しくは地域コミュニティ又は地域の私的なグループによって行われる場合は、通信情報省と連携しなければならない、かつ、国境を越えた個人データのやりとりに関する法令の規定を遵守しなければならない。

個人データの消去は、以下の通り、第 25 条に定められている。すなわち、(i)個人データは、電子システムにおける個人データの保存期間の満了又は個人データ所有者からの要請を理由とする場合のみ削除することができる。(ii)削除する際には、個人データ所有者の承認の上で、電子システム提供者が管理する個人データに関する文書の全部又は一部を消去しなければならない。さらに、2016 年電子システム通信情報省規則は、個人データ所有者の権利、利用者の義務、電子システム提供者の義務、紛争解決、政府及び社会の役割、監督及び行政処分についても定めている。

オ 漏えい等事案発生時の本人及び監督機関等への報告義務

第 28 条は、電子システム提供者がその管理する電子システムにおいて、個人データを保護しなかった場合、電子システム提供者は、個人データの所有者に対して書面により通知しなければならない旨を定める。通知に際しては、以下に従わなければならない。

個人データの秘密性を保護しなかった理由又は原因を通知に記載しなければならない。

通知は、個人データの所有者が自己の個人データ収集時に承認した場合、電磁的に行うことができる。

当該不履行に当事者に対する潜在的損害が含まれている場合、個人データの所有者が通知を受領していることを把握しなければならない。

書面による通知は、秘密性の保護を怠った日から 14 日以内に、個人データの所有者に送信しなければならない。

個人データの所有者の権利の一つに、電子システム提供者が個人データの保護を怠ったことによって生じる個人データに関する紛争について、通信情報省に苦情を申し立てる権利があることに留意する必要がある(第 26 条(b))。上記に関連して、同規則の施行に関する監督当局は、通信情報省又は部門規制・監督機関の長官である(第 35 条。)。この点、通信情報省は、電子システム提供者に対して、個人データの保護に関するデータ及び情報を要請する権利を有する。かかる要請は、定期的には又は必要に応じて行うことができる。

カ 安全管理措置に関する規定

第 5 条では、すべての電子システム提供者は自己が管理する個人データの保護の懈怠を回避するための予防措置として、社内個人データ保護規則を導入しなければならないと規定している。当該社内規則作成の際には、技術応用、人的資源、方法及び費用といった面を考慮し、同規則その他の関連規制の規定を参照しなければならない。

さらに、第 5 条は、すべての電子システム提供者に対し、その管理下にある個人データの保護の懈怠を防止するため、その他の予防措置を講じるよう義務付けており、当該予防措置は、少なくとも以下の形式とされる。

自己が管理する電子システム提供者における個人データの保護を提供するため、それぞれの環境下における人員の意識啓蒙を行う。

当該環境において、人員に対し、自己が管理する電子システムの個人データ保護に関する訓練を実施する。

上記に加えて、同規則の定めに従い、電子システム提供者は、受領及び収集した個人データの保存に使用される電子システムを、(i)相互運用可能かつ互換性を有するものとし、(ii)適法なソフトウェア上で動作させ(第 11 条参照。)なければならない。通信情報省は、電子システム提供者が現行法令(第 28 条第(a)項参照。)に従って管理する電子システムを認証する。

キ 適用範囲、適用除外内容

上記を前提として、同規則において規制される個人データの保護は、インドネシアの域外に居住する電子システム提供者が、インドネシア国民の個人データを収集、解析及び保存する場合には、当該電子システム提供者にも適用される。

第 2 条第(1)項に定められるとおり、電子システムにおける個人データの保護には、個人データの収集、処理及び解析、保存、掲載、公開、送付、拡散及びアクセス並びに削除が含まれる。

現行のインドネシア法令は、個人データの保護の適用に関し、例外を特に定めていない点に留意する必要がある。

ク 国際的な情報移転に関する規定

第 22 条第(1)項は、インドネシア共和国の域内に居住する政府又は地方自治体及び公的機関又は民間機関における電子システム提供者が管理する個人データの、インドネシア共和国の域外に対する者への移転は、以下に従わなければならないと規定している。

- (a) 通信情報省若しくは、監督権限を有する担当官又は機関と連携して行う。

(b) 国境を越えた個人データのやり取りに関する法的規制の規定を適用する。

かかる第(a)項に記載の連携は、以下の、2016年電子システム通信情報省規則第22条第(2)項に定める形を取るものとする。

- (i) 少なくとも正式国名、受領者の氏名、実行日及び移転の理由や移転先が含まれる、個人データの提出に関する実行計画に係る報告書。
- (ii) 必要な場合、弁護士による助力を求める。
- (iii) 活動結果を報告する。

現時点では、インドネシア政府は第22条第(1)項(b)に定める国境を越えた個人データのやり取りに関して規則を制定していないことに留意する。

ケ 紛争処理手続き

電子システムにおける個人データの秘密性の保護の懈怠に関する紛争解決は、第29条乃至第33条において規制される。すべての個人データの所有者及び電子システム提供者は、通信情報省に対し、個人データの保護の懈怠について申立書を提出できる。当該申立書は、審議による又はその他の代替の和解を通じた紛争解決措置を構成する。

以下の(i)又は(ii)を理由として、上記の申立書の理由とすることができる(第29条第(3)項)。すなわち、(i)電子システム提供者から個人データ所有者又は当該個人データに関連するその他の電子システム運用者に対し、個人データの秘密性の保護の懈怠に関連して潜在的又は非潜在的損失に関する書面通知が提供されないこと。(ii)個人情報の秘密保護の懈怠に関する書面通知が行われたものの遅延し、個人データの秘密性の保護の懈怠に関連して個人データ所有者又はその他の電子システム提供者に対し損失が生じたこと。

通信情報省は、当該苦情に対処するため、部門規制・監督機関の長官と協力することができる。総局(以下に定義される。)は、個人データに関する紛争解決パネルを設置することができる。

第30条に定めるとおり、通信情報省は、個人データに関する紛争を解決する権限を情報申請総局(以下「総局」という。)に委任していることに留意する。総局は、個人データに関する紛争に関するパネルを設置することができる。

第32条に定めるとおり、紛争を審議又はその他の代替の和解を通じて解決しようとする措置が不成功となった場合、個人データ所有者及び電子システム提供者は、現行の規制に従い、個人データの秘密性の保護の懈怠について民事訴訟を提起することができる。

さらに、現行法令に従い、法執行手続において法執行担当官により差し押さえが行われる必要がある場合、第33条に定めるとおり、その電子システムが差し押さえられていない

訴訟事件に関連する個人データに限って差し押さえることができる。差し押さえられた個人データを提供、保存又は管理する電子システム提供者は、当該個人データの改変又は損失につながり得る措置を講じることを禁止され、自己が管理する電子システムのセキュリティを維持し、又は個人データの秘密プライバシー保護を提供することが義務付けられる。

⑤ 銀行法

ア 法律の概要

銀行法が制定され、1998年11月10日付で施行された。

イ 個人情報の定義、機微情報の定義

第40条は、銀行が預金者又は顧客及びその預金に関する情報の秘密を保持しなければならないと定めている。そのため、当職らの見解では、銀行法に規定される銀行顧客に関する個人情報の定義は、銀行における顧客及びその預金に関する一切のデータ及び情報を含むものであり、2016年電子システム通信情報省規則に定められる個人データの定義よりも広義である。

ウ 主要な規制及び権利

第40条は、以下の場合を除き、銀行は、預金者又は顧客及びその預金に関する情報の秘密を保持しなければならないと定めている。

インドネシア中央銀行総裁は、課税の目的で、特定の預金者や顧客の財務状況に関する情報を税務官に開示し、証拠書類及び文書を税務官に提出することを求める書面による命令を、銀行に対して発することができる（第41条）。

インドネシア中央銀行総裁は、国家債務・競売及び国家債務委員会（State Debt and Auction Affair/State Debt Affair Committee）に移転した銀行の債権を決済するため、銀行から、預金者や顧客の預金に関する情報を得る目的で、同委員会の担当官に令状を発することができる（第41A条）。

インドネシア中央銀行総裁は、刑事事件における裁判手続のために、銀行から、犯罪の疑いがあり又は刑事責任を問われている預金者又は顧客の預金に関する情報を得る目的で、警察官、検察官又は裁判官に対して許可状を発することができる（銀行法第42条）。

銀行及び顧客の間の民事訴訟において、当該銀行の取締役会は、当該顧客の財務状況に関する情報その他関連する情報を裁判所に開示することができる（銀行法第43条）。

銀行間の情報の授受の目的で、銀行の取締役会は、顧客の財務状況を他の銀行に開示す

ることができる（第 44 条）。

銀行は、預金者又は顧客からの書面による要請、承認又は委任状を受けた場合、当該銀行における預金者又は顧客の預金に関する情報を当該預金者又は顧客が指名した者に提供する（第 44A 条）。

第 40 条に基づき秘密の保持が義務付けられる秘密情報を故意に開示した理事会（Board of Commissioners）の構成員、取締役、銀行員その他の関係者は、2 年以上 4 年以下の拘禁刑及び 40 億以上 80 億以下インドネシア・ルピアの罰金が科せられることに留意する必要がある。

第 40 条は、以下の 5 つの例外を除き、銀行は、預金者又は顧客及びその預金に関する情報の秘密を保持しなければならないと定めている。すなわち、(i) 課税の目的で、インドネシア中央銀行総裁は、特定の預金者や顧客の財務状況に関する情報を税務官に開示し、証拠書類及び文書を税務官に提出することを求める書面による命令を、銀行に対して発することができる（第 41 条）。(ii) インドネシア中央銀行総裁は、国家債務・競売及び国家債務委員会に移転した銀行の債権を決済するため、銀行から、預金者や顧客の預金に関する情報を得る目的で、国家債務・競売及び国家債務委員会の担当官に令状を発することができる（第 41A 条）。(iii) インドネシア中央銀行総裁は、刑事事件における裁判手続のため、銀行から、犯罪の疑いがあり又は刑事責任を問われている預金者又は顧客の預金に関する情報を得る目的で、イ警察官、検察官又は裁判官に対して許可状を発することができる（第 42 条）。(iv) 銀行及び顧客の間の民事訴訟において、当該銀行の取締役会は、当該顧客の財務状況に関する情報その他関連する情報を裁判所に開示することができる（第 43 条）。(v) 銀行間の情報の授受の目的で、銀行の取締役会は、顧客の財務状況を他の銀行に開示することができる（第 44 条を参照）。

⑥ 2017 年情報技術に基づく融資業務に関する情報技術リスクのガバナンス及び管理に関する金融庁通達（金融庁通達第 18/SE0JK.02/2017 号）

2017 年情報技術に基づく融資業務に関する情報技術リスクのガバナンス及び管理に関する金融庁通達（金融庁通達第 18/SE0JK.02/2017 号）が制定され、2017 年 4 月 18 日付けで施行された。

⑦ 2014 年インドネシア中央銀行規則

ア 法律の概要

2014 年インドネシア中央銀行規則が 2014 年 1 月 16 日付で制定され、2014 年 1 月 21 日付で施行された。

イ 主要な規制及び権利

本規則は、決済システムサービス顧客の保護に関するものであるが、決済システムサービス顧客の保護とは、第1条第(2)項に定める決済システムサービスの顧客を保護するための法的確実性を確保するあらゆる試みをいう。また、本規則において、決済システムサービスの顧客とは、取引のためではなく顧客自らのために、提供者からの決済システムサービスを利用する個人をいうとされる。

決済システムの顧客保護に関連して、第1条は、決済システムサービスの全提供者に、顧客データ及び情報の秘密を保持することを義務付けている。当該提供者は、同規則第15条に定めるとおり、顧客が書面により承認しており、又は現行法令上義務付けられている場合を除き、顧客のデータ又は情報を他者に提供することが禁じられていることにつき留意する必要がある。

第3条は、消費者保護の原則が(i)正当性及び信頼性、(ii)透明性、(iii)顧客データ又は情報保護並びに(iv)効果的な苦情の処理及び解決を対象とする旨定めている。さらに、顧客データ又は情報保護の原則は、提供者が顧客データ又は情報の秘密を保持し、そのセキュリティを維持し、消費者が認める利益及び目的に従った場合に限り、当該データ又は情報を利用することを確保している。

また、第14条は、決済システムサービスの全提供者に、顧客データ又は情報の秘密を保持することを義務付けている。この目的のために、提供者は、顧客データ又は情報保護方針を整備し、実施しなければならない。消費者が書面による承認を取得している場合又は同規則第15条において規制される現行法令によって義務付けられる場合を除き、提供者が顧客データ又は情報を他者に開示することが禁じられている旨にも留意する必要がある。決済システムサービス提供者による同規則第14条及び第15条の違反は、(i)文書による警告、(ii)罰金、(iii)決済システムサービス活動の一部又は全部の一時停止及び(iv)決済システムサービス実施免許の取消しの形態により、行政処分の対象となる。

決済システムサービス顧客の保護に関する紛争に関連して、2014年インドネシア中央銀行規則第26条は、決済システムサービスの提供者がインドネシア中央銀行総裁に対して消費者からの苦情処理及び解決に関する報告書を交付しなければならないと定めている。

(3) 監督機関・第三者機関

① 機関及び組織の設置背景

個人データ保護の実施状況を監督するために設置される特定の機関や組織は存在しない。個人データ保護の実施状況の監督は、2016年電子システム通信情報省規則第35条におい

て規律されている。当該監督は、通信情報省又は部門規制・監督機関の長官により直接的又は間接的に行われる。通信情報省は、電子システム提供者から個人データの保護に関するデータ及び情報を請求する権利を有し、当該請求は、定期的に又は必要に応じていつでも行うことができる。

2016年電子システム通信情報省規則第35条第(5)項に定めるとおり、通信情報省は、その監督権限を総局に委任していることに留意する必要がある。

決済システムサービスの顧客の保護に関し、インドネシア中央銀行は、決済システムサービス提供者による顧客情報保護の導入を監督しなければならない(2014年インドネシア中央銀行規則第27条)。かかる規律は、銀行法第29条の規定に従うものであり、当該規定により、銀行は、インドネシア中央銀行により監督される。また、2014年インドネシア中央銀行規則の導入のために、インドネシア中央銀行は関連機関と協力することができる。

連絡先及びURL

通信情報省

Jl. Medan Merdeka Barat No. 9,

Jakarta 10110

電話：(021) 345 2841

Eメール：humas@mail.kominfo.go.id

ウェブサイト：<https://www.kominfo.go.id/>

(4) 最近のトピック

① 制度改正の検討状況

インドネシアの国会(The House of People's Representatives of the Republic of Indonesia、Dewan Perwakilan Rakyat Republik Indonesia)は、特に個人データの保護を規定する個人情報保護法案(Draft Law、Rancangan Undang-Undang/RUU)を作成した³。個人情報保護法案は一般公開され、インターネットでアクセス可能である。個人情報保護法案は、2015年から2019年までの国家立法計画に盛り込まれる。

しかしながら、現時点では、当該ドラフトが法律として承認される予定年月日は明らかになっていない。

2015年に国会において個人データ保護法案が起草され、各種会議の結果、これに修正が加えられ、2017年草案が完成した。当該草案の特徴は、以下のとおりである。

3

<http://203.148.85.149/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html> 参照。

(a) インドネシアに所在するインドネシア人及び外国人を対象とし、(b) 官民のセクターに対して包括的に適用され、(c) 域外適用も存在し、(d) 侵害に対して裁判所への補償を求める権利を付与し、(e) 調査及び侵害判決を下し、また執行可能な仲裁判断を下す仲裁を行う機関として、また、行政罰として 7 万 5000 米ドル（上限はその 25 倍の金額までとされる。）を科する権限を与えられた委員会が設立される。

② 個人情報に関連した主要な裁判例

2011 年、南ジャカルタ地方裁判所（the District Court of South Jakarta、Pengadilan Negeri Jakarta Selatan）は、銀行 B 及び銀行 C の顧客である H 氏が南ジャカルタ地方裁判所に対して提起した、銀行 B 及び銀行 C による銀行法第 40 条、第 47 条、第 49 条、第 50 条及び第 51 条の違反に関する民事訴訟について判決を下した。この訴訟は、銀行 B 及び銀行 C が、カード支払による決済文書⁴に基づくオンラインネットワーク相互接続に関する契約（当該契約に基づき、銀行 B 及び銀行 C がそれぞれの顧客の個人データ（H 氏の個人データを含む。）に関するすべての情報を移転及び提供することを義務付けられていた。）を締結したために提起された。

裁判所は、H 氏が銀行 B 及び銀行 C の顧客であり、それは H 氏が銀行 B 及び銀行 C のそれぞれに対する個人データの提供に同意したことを意味するとの主張に基づき、特に個人データの移転について、H 氏による訴訟を完全に棄却した。⁵よって、銀行 B 及び銀行 C は銀行法の違反にはならない。

⁴ Card-Based Payment Instruments、*Alat Pembayaran Berdasarkan Kartu*

⁵ <https://putusan.mahkamahagung.go.id/putusan/bbffd91b0534eb60d08ee300a694b6b2> 参照。

12. インド

(1) 制度概要

① 法体系の概要

インドは、中央政府を置く準連邦制度を採用しており、中央（Center）及び各州における各政府において、行政機関を置いている。憲法は中央議会、州の立法機関の立法権限について、一定の規律を設けている。すなわち、「連邦リスト（union list）」に記載されている事項は、中央議会（Union Parliament）のみが立法することができ、「州リスト（state list）」において言及されている事項は、州の立法機関のみが立法することができる。さらに、「共同管轄リスト（concurrent list）」に記載されている事項は、行政機関国会及び州立法機関の双方が制定することができる。

立法に関する中央又は州の別は、憲法別表 7 に記載されている。同別表 7 に基づき中央で制定される法律及び個人情報規則のうち、本調査報告書の対象となるものは、IT 法、個人情報規則、電信法、医療評議会規則、情報権法、銀行帳簿証拠法、信用情報会社（規制）法、公的金融機関法、統計収集法、国勢調査法、支払決済システム法、ID 番号法、刑法、契約法、及び著作権法である¹。

これらの他、インド準備銀行開示指針及び電気通信規制庁守秘義務指針は、中央政府の制定法に基づき設立された当局が公布した指針である。

② 公的部門に適用される主な連邦法

公的部門について具体的に言及する法律は、以下のとおりである。

ア 憲法：プライバシー権を保障する（憲法 21 条）。

イ IT 法：当局による電子的統制（electronic-governance）について規定している（IT 法第Ⅲ章）。

ウ 情報権法：一定の限度でデータ保護及び当該情報への市民による請求権についても規定している。

エ ID 番号法：中央政府が固有識別番号庁（Unique Identification Authority）を設置し、市民に識別のための番号（以下「アドハーナンバー」という。）を付与する権限を与えている。

オ 国勢調査法：中央政府が国勢調査の実施を宣言した場合の、国勢調査スタッフによる

¹ これらの法令の略称は、下記（2）①の表において定義される名称によっている。

インド市民の情報の収集を定める。

③ 民間部門に適用される主な連邦法

公的部門に特有の上記法律を除き、本調査報告書において言及するその他の法律、個人情報規則、指針、法律の条項、すなわち、IT 法、個人情報規則、インド準備銀行開示指針、電気通信規制庁守秘義務指針、電信法、医療評議会規則、銀行帳簿証拠法、信用情報会社（規制）法、公的金融機関法、統計収集法、支払決済システム法、刑法、1986 年消費者保護法、契約法、著作権法等は、民間部門及び公的部門の双方を広く規律する。

(2) 主な法律の概要

① 個人情報保護を規律している法律の名称、成立・施行時期は以下のとおりである。

	法律、規則、指針、方針	施行日
基本法		
1.	1950 年インド憲法（以下「憲法」という。）	1950 年 1 月 26 日
2.	2000 年情報技術法（Information Technology Act, 2000）（以下「IT 法」という。）	2000 年 10 月 17 日
3.	2011 年情報技術（合理的安全管理実務及び手続並びに機微情報）規則（Information Technology (Reasonable Security practices and Procedures and Sensitive Personal Data or Information) Rules, 2011）（以下「個人情報規則」という。）	2011 年 4 月 13 日
周辺法		
1.	インド準備銀行の開示指針（Disclosure Policy of the Reserve Bank of India）（以下「インド準備銀行開示指針」という。）	2017 年 9 月 11 日
2.	2010 年加入者の秘密情報及び通信のプライバシーに関するインド電気通信規制庁（以下「電気通信規制庁」という。）の指針（Direction of the Telecom Regulatory Authority of India regarding confidentiality of information of subscribers and privacy of communications dated 26th February 2010）（以下「電気通信規制庁守秘義務指針」という。）	2010 年 2 月 26 日
3.	1885 年インド電信法（Indian Telegraph Act, 1885）（以下	1885 年 10 月 1 日

	「電信法」という。)	
4.	2002年インド医療評議会(職業倫理)規則(Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002)(以下「医療評議会規則」という。)	2002年4月6日
5.	1986年消費者保護法	1987年4月15日
6.	1872年インド契約法(Indian Contract Act, 1872)(以下「契約法」という。)	1872年9月1日
7.	1957年著作権法(Copyright Act, 1957)(以下「著作権法」という。)	1958年1月21日
8.	1860年インド刑法(Indian Penal Code, 1860)(以下「刑法」という。)	1862年1月1日
9.	2016年国民ID番号(金銭的助成金その他の補助、利益及びサービスの交付対象)法(Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act)(以下「ID番号法」という。)	2016年7月12日及び2016年9月12日(部門別)
10.	2005年情報権法(Right to Information Act, 2005)(以下「情報権法」という。)	2005年10月12日
11.	1891年銀行帳簿証拠法(Bankers' Books Evidence Act, 1891)(以下「銀行帳簿証拠法」という。)	
12.	2005年信用情報会社(規制)法(Credit Information Companies (Regulation) Act, 2005)(以下「信用情報会社(規制)法」という。)	2006年12月14日
13.	1983年公的金融機関(忠実義務及び秘密保持に関する義務)法(Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983)(以下「公的金融機関法」という。)	
14.	2007年支払及び決済システムに関する法律(Payment and Settlement Systems Act, 2007)(以下「支払決済システム法」という。)	2008年8月12日
15.	1948年国勢調査法(Census Act, 1948)(以下「国勢調査法」という。)	1948年9月3日
16.	2008年統計収集法(Collection of Statistics Act, 2008)(以下「統計収集法」という。)	2010年6月11日

インドにおけるデータ保護の基本法は、憲法、IT 法及びこれに付随する規則である。インド国内で施行される一切の法律は憲法の枠内で制定され、IT 法は個人情報及びオンライン記録の保護をより具体的な形で規定する。

以上に加え、スリクリシュナ専門委員会 (Srikrishna Committee of Experts) (以下「委員会」という。) の 2017 年 11 月 28 日付勧告においては、インドにおける実施可能かつ効果的のデータ保護体制の構築に関して言及しているため、別途、本調査報告書で言及する。

主要又は付随的なデータ保護法のいずれにおいても、事業規模による特別な規定は定められていない。上記法律は、事業の規模を問わず画一的に適用される。さらに、Justice KS Puttaswamy v Union of India 事件の 2017 年 8 月 24 日最高裁判決に従い、正当な国家の利益がかかわっている場合は、データ保護法制によるデータ保護は制限される。

② 憲法

ア 概要

インド国内で施行される一切の法律は憲法の枠内で制定される。憲法 21 条は、生命及び個人の自由に関する基本的人権について規定しており、最高裁判所は、近時、プライバシー権が基本的人権であると判断した。

イ 主な規制・権利の内容

憲法第 21 条は、法律に定められた手続による場合を除き、いかなる者もその生命及び個人の自由をなく奪われないと規定している。同条は、基本的人権の根拠規定とみなされており、基本的人権は、法律の制定や基本的人権を侵害する措置によって国家により制限されてはならない。同条における「生命」(life) という言葉の意味は、インドの裁判所により解釈されており、その解釈によると多様な人権を含んでいる。

同条に基づき保障されるプライバシー権は、原則として、同権利が、憲法 12 条における「国家」に該当する主体によって侵害された場合に保障される。国家によって権利を侵害された者は、憲法 32 条に基づき最高裁判所に対して、基本的人権の侵害に対する憲法上の救済を申し立てることができる。ただし、一定の場合において、公的役割を担う民間の当事者に対して 226 条に基づく権利を行使することも可能である。

ウ 判例

Justice KS Puttaswamy v Union of India [2017 (10) SCALE 1]事件 2017年8月24日判決において、プライバシー権は、憲法 21 条において謳われる基本的人権の一つであると示された。

さらに、ID 番号法に基づくアドハーナンバーの付与の強制の合憲性について現在最高裁判所で争われている。詳細は後述する。

③ IT 法

ア 概要

IT 法は、電子的記録、電子的形態において作成、使用又は保存された情報に対する適切な保護の提供、そして、データプライバシー違反、データ窃盗及びサイバー犯罪に対する罰則を制定するために制定された特別法である。なお、インドには具体的なデータ保護法は存在せず、インドの国会は、最高裁判所の判断内容（以下、本調査報告書において言及する）に従い、近い未来にデータ保護法が公布されるように進めているところである。

IT 法の目的及び理由に関するステートメント（添付付属書類 - 1 参照）及び 2006 年 IT 改正法案に従い、以下の目的を達成するために施行された。すなわち、(i) 世界規模の情報技術の最大限の利用の文脈において、電子取引の成長を加速させ、e コマース及び電子取引を法的に整理し、電子政府を促進し、サイバー犯罪を防止し、安全管理実務及び手続を確保し、(ii) 個人データ及び個人情報の保護並びに電子通信に対する安全管理実務及び手続を実施し、(iii) 治安、経済、公衆安全衛生のための重要な情報インフラを保護し、(iv) サイバー犯罪防止のための刑罰規定を制定し、2001 年に国際連合国際商取引法委員会（UNCITRAL）が採択した電子署名に関するモデル法に従った、電子記録及びデジタル署名の法的整理並びに電子署名における代替技術に関する規定を制定し、さらに、(v) 中央政府又は州政府が定める基準に基づく適切なサービス料による事業者に対する中央政府又は州政府からの認可に関する規定の制定がその目的である。

イ 個人情報の定義

「機微個人データ及び機微個人情報」(sensitive personal data or information) は、43 条 A の注釈 (Explanation) (iii)において、中央政府が適切と判断する専門機関と協議の上、中央政府が定める個人情報を意味すると説明されている。後述する個人情報規則において当該概念はさらに詳細に言及されている。なお、後述するとおり、個人情報規則は、第 1 条(2)に従い、これに基づき制定され IT 法の促進のために、IT 法の目的を広範にわたり規律する。

ウ 主な規制・権利の内容

第 III 章は、中央政府若しくは州政府又は政府当局若しくは法の定める当局による電子的統制 (electronic-governance) について規定している。

IT 法は、罰則を課すことによりデータを保護しようとしており、さらに、中央政府又は州政府が、国益増進のために一定の状況下で個人データを保護するために私人の権利を制限することを認めている。ただし、IT 法は、データ保護を目的として制定されたものではないため、同法に基づく保護の範囲は制限的である。関連条項は、付属書類-2 として本書に添付されている。

デジタル署名証書の公開鍵 (public key) に対応する秘密鍵 (private key) が漏えいした場合、加入者は、42 条に基づき、直ちにかかる事実を認定当局に報告する義務を負う。データに関する不正行為及びコンピュータシステムにおける違反事例又は第 43 条に基づく行為が発生した場合、権利を侵害された当事者は、第 46 条に基づき指名された裁定官に申し入れを行うことができる。第 34 条は、デジタル署名証書によって保証されたデジタル記録及びデジタル契約に関して、かかる証書の信頼性に重大な悪影響が生じた場合、当該証書を発行する認証当局に開示するよう義務づけている。さらに、認証当局のコンピュータシステムの整合性に重大な悪影響が生じた場合、認証当局は、当該事実を開示し、コンピュータシステムの整合性が損なわれることによって影響を受ける可能性のある者に対して合理的な通知を行う義務を負う。

第 43 条は、無権限で以下の行為をした者に損害賠償をさせるという形で民事救済を規定している。具体的には、所有者又は責任者の許可を得ないコンピュータシステムへの不正アクセス、情報の無断使用、権限保持者に対するアクセス拒否、損害を与える目的でのコンピュータ・ソース・コードの窃盗、隠ぺい、削除若しくは改ざん等の不正行為である。かかる不正行為には、第 66 条に基づき罰金若しくは禁錮又はその両方が課される。

第 43 条 A は、法人が誰かに不当な損失又は利益を及ぼすような個人情報の取扱いに関して合理的な安全措置を講じなかった場合に、影響を受けた者に対して損害賠償を支払うことを義務づけることで、法人に対してデータごとに関する責任を課している。

第 69 条は、国内の秩序維持などインドの国家治安及び防衛のために、中央政府や州政府又はその権限ある職員に対して、情報の遮断や監視等をする権利を付与している。第 69 条 A は、国内の秩序維持などのインドの国家治安及び防衛の追求のために、中央政府や州政府又はその権限ある職員に対して、一切のコンピュータ・リソースを通じた情報の閲覧を禁止する権利を与えている。

第 69 条 B は、国内におけるサイバーセキュリティのために、中央政府に対して、一切のコンピュータ・リソースを通じて情報を監視及び収集する権限を政府機関に付与する権利を与えている。

第 72 条は、特定の者によって保有される電子的記録、帳簿、登記、情報又は書類等を閲覧した者が保有者の同意を得ずに、閲覧した情報を開示した場合、その者が罰金及び禁錮に処される旨規定している。

第 79 条は、ネットワークサービス事業者等の仲介業者の責任の免除について規定している。例えば、仲介業者の役割は情報が一次的に保管されている通信システムへのアクセス提供のみに限定されていたこと、かつ、仲介業者が発信、送信した情報の変更又は送信の受領者の選択に関与していないことを立証できる場合が挙げられる。さらに、仲介業者が公開された情報について知らず、かつ、データを保護するために適切な措置をすべて講じたことが立証される場合には、責任の免除の適用を受けることができる。

エ 適用範囲及び域外適用

IT 法は、インド国内のみならず、インド国外にいる者によって実行された違反にも適用される（第 1 条(2)）。IT 法の域外適用については、第 75 条においても言及されている。すなわち、第 75 条は、違反がインドに所在するコンピュータ、コンピュータシステム又はコンピュータネットワークに関連する場合に限り、違反者の国籍を問わずいかなる違反者に対しても適用される旨規定されている。IT 法は、他の一切の有効な法律に対して優先的効力を有する（第 81 条）。但し、同法の条項は、著作権法又は 1970 年特許法に基づく一切の権利を行使することを制限するものではない。

オ 裁定及び上訴

第 43 条（コンピュータ、コンピュータシステム又はコンピュータネットワークに関連する不正アクセス、複製、使用又は活動等）又は第 43 条 A（個人の秘密データ又は情報の保護における法人の過失）に関して違反が生じた場合、権利の侵害を受けた者は、第 46 条(1)に従い中央政府に指名された裁定官に申し入れを行うことができる。

かかる裁定官は、5,000 万ルピー以下の請求についてのみ管轄権を有している。同金額を超える場合は、当該請求について必要な金銭的管轄権を有する裁判所が当該事件を裁定する。この場合における裁定官は、民事裁判所としての権限を有し、その権限は、第 58 条に基づくサイバー上訴裁定所によって付与される。裁定官は、その後第 47 条に従って、違反に起因する不正な利得の金額、損失額等の要因及び不履行の反復性に基づき補償金額を裁定する。

第 57 条に基づき、裁定官による決定について、権利侵害を受けた者が裁定官の決定の写しを受領した日から 45 日以内にサイバー上訴裁定所に対して上訴を行うことができる。かかる時点を過ぎてから上訴の申し立てを行った場合、その遅延について十分な理由が示された場合に限り、かかる上訴が許可される可能性がある。サイバー上訴裁定所は、1908 年民事訴訟法の拘束を受けず、自然法の原則に則るものとし、民事裁判所としての権限を行

使うことができる。

第 61 条に基づき、いずれかの裁定官又は上訴裁定所が当該案件について判断する権限を与えられる場合、民事裁判所の管轄権が除外される点について注意すべきである。

第 62 条に従い、上訴裁定所の決定に起因する法律又は事実に対する疑義について、権利侵害を受けた者は当該決定が通知されてから 60 日以内に該当の高等裁判所に対して上訴を行うことができる。申し立てにおける遅延は、かかる遅延について十分な理由があるときは認められる場合がある。

高等裁判所の決定については、最終的に最高裁判所に対して上訴を行うことができる。

また、第 63 条に基づき、同法違反は、裁定官による示談となる可能性がある点につき留意が必要である。

④ 個人情報規則

ア 概要

IT 法の促進のために、IT 法の上記目的を広範にわたり規律する個人情報規則が施行された。第 1 条(2)に従い、これに基づき制定された個人情報規則は、IT 法に従い、インド全国のみならず、インド国外にいる者によって実行された違反にも適用される。情報提供者の同意を得ない法人による情報開示は禁止されているが、個人情報規則第 6 条において、政府機関の場合の例外事由が定められている。

イ 個人情報の定義

第 2 条(i)において、「個人情報」(Personal Information)とは、法人において入手可能であるか、又は入手可能となる可能性のある他の情報との組み合わせにより、直接又は間接的に個人を特定することができる一切の情報、と定義されている。個人の特定につながる場合にのみ、当該情報は個人情報とみなされる。

第 3 条は、「機微個人データ又は機微個人情報」(sensitive personal data or information)の範囲について言及しており、パスワード、銀行口座又はクレジットカード若しくはデビットカードその他の支払手段に関する詳細等の金融に関する情報、身体的、生理学的若しくは精神的健康状態、性的指向、診療記録や履歴、生体情報、適法な契約に基づくサービスの提供又は情報の処理若しくは保存を目的として法人に対して提供された詳細な情報等に関連する個人情報を含むとしている。ただし、同規則上、情報権法に基づき無料で入手可能とされ又は公表されている情報は、同規則の範囲から除外される。

ウ 主な規制・権利の内容

第3条は、同規則における個人情報の概念について言及している。第3条は、「個人情報」の定義に、パスワード、銀行口座又はクレジットカード等の支払手段に関する明細等の金融情報、心身の健康状態、性的指向、診療記録契約に基づくサービスの提供等を目的として法人に対して提供された情報等の個人情報も含まれるとしている。ただし、同規則上、情報権法に基づき自由に入手できる情報は、かかる定義から除外される。

第4条は、法人に対して契約に基づいて法人に提供された個人情報を適切に取扱い、プライバシーポリシーを自社のウェブサイト上で公表するように義務づけている。第4条は法人に対して、当該法人の運用実態、収集した個人情報の種類及び目的、第6条に従った個人情報の開示、並びに第8条に従った合理的な安全措置に関する声明を容易にアクセス可能で明確な形で提供するよう義務づけている。

第5条は、個人情報の提供者から情報を収集する前に、提供者から使用目的に関する同意を書面で取得するように法人に義務づけている。さらに、同規則は、情報収集の目的が適法でなければならない、かつ、情報収集が同目的のために必要でなければならない旨規定している。また、直接個人から情報を収集する場合、法人は、その情報提供者が当該情報収集の事実、目的、情報の受領予定者、情報の収集事業者、情報の保有事業者の名称及び住所について知っているようにしなければならない。また、法人は、収集目的に必要な期間を超えて個人情報を保有してはならず、当該情報の収集目的以外の目的で情報を使用してはならない。情報提供者は、自ら提供した情報を確認し、正確性の確保のために不備の削除や訂正を依頼することができる。情報提供者は、サービスを利用する間いつでも、書面の同意を撤回することができ、サービスを利用する前に、ある特定の情報を提供することを拒否し、サービス利用中でも同意を撤回することができなければならない。また同規則は、苦情担当職員についても規定しており、苦情担当職員は苦情を受領した日から1か月以内に速やかに当該苦情を処理しなければならないとしている。

第6条は、法人が個人情報を第三者に開示する際は、当該開示が契約において合意されている場合、又は当該開示が法的義務の遵守のために必要である場合を除き、情報提供者の事前の許可を要する旨規定している。また、同規則は、情報提供者の事前の同意を得ずに第三者に対して情報を開示できる場合として、身元の特定、犯罪（サイバー事件を含む。）の防止、発見、捜査、起訴及び処罰の目的で、個人情報を取得することを法律上委任された政府機関と情報を共有することについても規定している。政府機関は、法人に対して要請する際、当該情報を求める目的を伝えるとともに当該目的を他の者に公言してはならない旨を明確に伝えることを同規則により義務づけられている。同規則は、正当な国家（政府）の目的の下で、政府に個人情報にアクセスする権利があるという原則を内包している。

第7条は、法人が個人情報を、同法人が遵守するデータ保護水準と同程度の水準を保証する、インド国内又は国外の他の法人に対して移転することを許可している。ただし、かかる移転は、法人及び情報提供者間の契約の履行のために必要なものであるか、又は、データ移転について本人が同意した場合に限られる。

第 8 条に基づいて、法人又はこれを代理する者は、合理的な安全措置を実施し、かつ、保護される情報の性質に見合った技術上のセキュリティ対策を含んだ、包括的な情報セキュリティ方針が文書化されている場合に、合理的な安全措置を遵守しているとみなされる。情報セキュリティの違反が生じた場合、当該法人又はこれを代理する者は、要請された場合に限り、自社の情報セキュリティ方針に従ってセキュリティ対策を実施したことを立証しなければならない。法人は、データ保護のためにベスト・プラクティスの IS、ISO 又は IEC 規程を遵守するか、中央政府によって承認されたデータ保護に関する独自の規程を使用することができる。IT 法においては、当該対策の性質について規定する具体的条項は定められていない。同条は安全措置について柔軟な対応を許容しているため、法人は、保護される情報の性質において十分かつ相応な技術上及び運用上のセキュリティ対策を自由に策定及び実施することができる。

⑤ 情報権法

ア 概要

情報権法は、データ保護について規定しており、公的機関において閲覧可能な情報及び記録も規制している。また、同法は、当該情報開示の請求権を市民に付与することにより、当局の透明性を確保する。

イ 主な規制・権利の内容

データ保護及び当該情報への市民による請求権について規定している。すなわち、第 3 条は、すべて市民は情報への権利を有する旨を規定しており、「情報への権利」とは、公的当局により保持され又は支配されている、情報権法の下でアクセスすることができる権利を意味すると定義されている（第 2 条(j)）。市民は、情報権法で除外され又は免除されている場合を除き、公的当局により保持され、又は支配されている一切の情報への権利を有する。ここで、公的当局とは、憲法、議会による制定法、州議会による制定法、管轄権を有する政府が発出した通達により組織された自治機関や団体を意味する（第 2 条 (h)）。さらに、第 2 条(f)は、「情報」を、記録、書類、メモ、電子メール、意見、助言、プレスリリース、通達、命令、日誌、契約、報告、新聞、サンプル、モデル、電子的形態により保持される媒体を含むあらゆる形態体による、有効な法律に基づき公的当局によりアクセスされ得る民間の主体に関連する情報をいうと定義している。

情報権法は、主に、公共団体による書類の開示に関して制定されたものであるが、一定の書類に対して第 8 条(付属書類-8 に記載する。)に基づき、開示を免除している。例えば、第 8 条は、インドの主権、経済的利益、外交等悪影響を与える情報、違反を扇動する情報、裁判所によって公表を明示的に禁止された情報、その開示が裁判所に対する侮辱罪に該当

し得る情報、議員不逮捕特権に違反し得る情報、知的財産、第三者の競争上の立場を害し得る情報、外国政府から秘密情報として入手した情報、何者かの生命若しくは身体的安全を危機にさらす情報、違反者の捜査や司法手続の妨げとなる情報、決定が行われる前の内閣文書等の開示を禁止している。

⑥ ID 番号法

ア 概要

中央政府が固有識別番号庁 (Unique Identification Authority) を設置し、市民にアドハーナンバーを付与する権限を与えている。

イ 主な規制・権利の内容

ID 番号法は、市民に対して助成金及び利益を与えるために、固有識別番号庁が市民の個人データを収集し、当該市民にアドハーナンバーを付与する権限を与えている。

第 28 条は、当局が個人の身元情報及び認証記録のセキュリティを保障しなければならない旨規定している。当局は、情報へのアクセスが発生しないよう一切の必要な措置を講じなければならない。また、当局は、技術上及び組織上のセキュリティ対策を決定及び実施し、かつ、代理機関、コンサルタント、アドバイザー又はなんらかの役割を履行するために選任若しくは委託されたその他の者に当該適切なセキュリティ対策を実施させ、また、代理機関、コンサルタント等との契約において同法に基づき当局に課される義務と同等の義務を負わせる条項を入れなければならない。

第 29 条は、生体データの保護について規定しており、当該情報は、誰かのため又はアドハーナンバーの作成及び同法に基づく認定以外の何らかの目的のために、いかなる者とも共有されてはならないとしている。

以上の条項は、付属書類 13 として本書に添付されている。

⑦ 電信法、電気通信規制庁守秘義務指針

ア 概要

電気通信業界には、データプライバシー及びデータ保護を目的として、加入者情報の秘密保持や通信の秘密を規定している。第 24 条及び第 25 条は、電信に含まれるデータ保護、プライバシー権について規定している。但し、情報保護の範囲は、電信の傍受によって違法に取得された電信内容の情報に制限されている。

イ 主な規制・権利の内容

第 24 条は、メッセージの内容を違法に取得する目的で、第 23 条に基づきいずれかの行為（電信会社への不法侵入や障害物の生成等）の実行を試みた者は、禁錮に処される旨規定している。さらに、第 25 条は、権限なくメッセージ内容を傍受しようとした者や、メッセージの送信配信を妨害しようとした者に対する罰則を定めている。

電気通信規制庁守秘義務指針において、電気通信規制庁は、電気通信業界における消費者の利益のために、携帯電話サービス事業者及びユニファイドアクセス・サービス事業者（Unified Access Service Providers）に対して、以下の指針を発表した。

- ・ライセンス条件における規定に従って情報の秘密保持を確保し、通信の秘密に対する違反を防止するために適切なメカニズムを実施すること。
- ・その保護においてサービス事業者が講じた措置の詳細を、電気通信規制庁守秘義務指針の発行から 15 日以内に当局に対して提供すること。

⑧ 医療評議会規則

ア 概要

医療業界では、医療評議会規則により、医師患者間の守秘義務が規定されている。医療評議会規則は、1956 年インド医療評議会法により職業倫理等の策定権限を授権されている。

イ 主な規制・権利の内容

第 2 章は、医者が自己の患者に対して負う義務について定めており、医者患者間の守秘義務並びに患者の生活及び健康等の個人情報の保護について規定している。ただし、州法により義務づけられる場合又は感染症から市民を保護するために当該情報を公表することが必要である場合には、医者による情報の開示が許可されている。

⑨ 銀行帳簿証拠法、支払決済システム法、信用情報会社（規制）法及び公的金融機関法

ア 概要

銀行、信用情報会社及び公的金融機関に関して、これらの法律はいずれもデータ保護を要求している。

イ 主な規制・権利の内容

銀行帳簿証拠法第 2 条 A は、不正なデータ変更の防止及び発見、権限ある者によるシステム運用の確保、紛失データの回復、システム改ざんの防止、保存機器等の保管及び保存

の手配のために採用された保護対策を詳述している。また同条は、データ移転方法及びデータが正確に移転されたことを確保するための確認方法等を記載した証明書をコンピュータシステムの責任者に義務づけることにより、銀行帳簿におけるあらゆる種類の振替又は記録におけるデータが法律違反や漏えいから十分に保護されるとしている。

支払決済システム法第 15 条は、支払システムに関する市民のデータ保護について規定しており、支払システムの効率性、セキュリティを保護するため、銀行業務上の利益又は公共の利益のために該当者の情報が必要であるとみなされる場合を除き、インド準備銀行によって入手された情報については、その秘密が保持されなければならない旨定めている。

信用情報会社（規制）法第 20 条は、すべての信用情報会社、信用機関及び特定の利用者が、入手し得る信用情報の収集、処理、照合、記録、保存、秘密、共有及び利用に関して、認められた使用目的のためだけに利用し、情報の正確性を確保し、情報を保護及び削除するために、一定のプライバシー原則を採用するとしている。同規則第 29 条は、いかなる信用情報会社も、その会員等に関連する情報又は会員の事業や問題に関連する情報を漏えいしてはならない。また、信用情報会社の役員や構成員等を含む全員は、守秘義務及び忠実義務を負う旨の契約書を作成しなければならない旨規定している。

公的金融機関法第 3 条は、法律や慣例に従う場合若しくは公的金融機関による当該情報の開示が必要又は適切である場合を除き、公的な金融機関が、その構成員又は事業に関連する情報を開示してはならない旨規定している。同法第 4 条は、公的金融機関の役員及び従業員が、守秘義務及び忠実義務を負う旨の契約書の作成を義務づけている。同法は、法律上義務づけられる場合を除き、公的金融機関はいかなる情報も開示しないとしている。公的金融機関の役員及び従業員に対する守秘義務及び忠実義務を負う旨の契約書に必要な条項として、かかる者に対してプライバシー及びデータを保護する義務を課している。

⑩ 刑法

ア 概要

窃盗の処罰規定を根拠として、情報やデータの保護がなされる可能性がある。

イ 主な規制・権利の内容

インド刑法第 378 条は、窃盗について規定している。人々は、自らの同意を得ない他者が動産を移動させたことを証明することにより、同条に基づき自己のデータを保護することができる可能性がある。当該データが含まれた書類やディスク等の移動は、本人の同意を得ない他人による動産の移動と呼ばれ得る。よって、刑法第 378 条において、データが保護される一定の可能性がある。

⑪ 契約法

ア 主な規制・権利の内容

同法においては、データ保護に関する具体的条項は置かれていないが、契約の履行について規定されている。それゆえに特に、事業者が公衆から情報を得ようとする場合の守秘義務及び秘密保持に関する条項を置くことが多い標準契約においては、データ保護がなされる余地がある。企業がデータを誤用又は開示したときは、権利侵害を受けた者は、同法に基づき賠償を請求することができる。もっとも、契約に違反した情報の無断開示は、IT 法第 72 条 A に基づき罰則の対象となる。

(3) 監督機関・第三者機関

① 認証当局管理者

インドにはデータ保護及びデータプライバシーを扱う特定の当局が存在しないが、IT 法に基づき監督任務を行う特定の管理者その他の職員が選任されており、かかる管理者の監督のもとで、電子署名証書の保管者として行為を行い、電子署名証書の秘密及びプライバシーを維持するための適切なセキュリティ手続を遵守する特定の認証当局 (Certifying Authorities) (以下「認証当局」という。) が設置されている。この点において認証当局の管理者 (Controller of Certifying Authorities) (以下「認証当局管理者」という。) は、電子署名証書に関する主たる監督当局であり、2000 年 11 月 1 日に認証当局管理者の事務局が設立された。IT 法第 17 条に基づき、中央政府は、認証当局の管理者並びに適当と認める人数の副管理者及びアシスタント・管理者を選任することができる。副管理者 (Deputy Controllers) 及びアシスタント・管理者 (Assistant Controllers) は、管理者によって課された役割に従って行動する。

IT 法第 18 条に従い、認証当局管理者は、認証当局に対する監督及びこのような認証当局に係る基準及び規則の制定について責任を負う。また、認証当局管理者は、認証当局の公開鍵の認証並びに認証当局及びその申込者の利益相反の解決についても責任を負う。

また、同法第 28 条は、認証当局管理者又はこれによって授権されたその他の者に対して、同法における違反について捜査を行う権限を付与している。

認証当局の管理者の住所は以下のとおりである。

認証当局管理者
Electronics Niketan
6 CGO Complex, Lodhi Road,

New Delhi - 110003

ファックス: 91-011-24369578

電子メール: info@cca.gov.in

- インドにおいてライセンスを受けた認証当局の一覧は、以下のとおりである。
 - Safescrypt 認証当局
 - 住所: Sify Technologies Limited.
2nd Floor, "Tidel Park",
4 Rajiv Gandhi Salai, Taramani
Chennai - 600 113
 - 権限ある代表者: S Shankara Narayanan
 - 電話番号: 91-044-22540770
 - 電子メール ID: N/A
 - IDRBT 認証当局
 - 住所: IDRBT, Castle Hills,
Road No 1, Masab Tank,
Hyderabad-500057
 - 権限ある代表者: N/A
 - 電話番号: 91-40-23294002
 - 電子メール ID: directoroffice@idrbt.ac.in
 - National Informatics Centre
 - 住所: A-Block CGO Complex,
Lodhi Road,
New Delhi -110 003
 - 権限ある代表者: Parminder Bakshi
 - 電話番号: 91-11-24366176
 - 電子メール ID: casupport@nic.in
 - n(Code) Solutions 認証当局
 - 住所: (n)Code Solutions
(A division of Gujarat Narmada Valley
Fertilisers & Chemicals Limited),
403, GNFC InfoTower,
S G Highway, Bodak Dev,
Ahmedabad - 380 054.
 - 権限ある代表者: Girdhar M Varliani
 - 電話番号: +91 79 40007334, +91-79-4007300,
+91-79-26857316/17/18
 - 電子メール ID: gvarliani@ncode.in
 - e-Mudhra 認証当局
 - 住所: eMudhra Limited,
3rd Floor, Sai Arcade,

No. 56 Marathahalli Outer Ring Road,
Devarabeesanahalli,
Bangalore - 560103

権限ある代表者: N/A
電話番号: 080 - 42275300
電子メール ID: info@e-Mudhra.com

- CDAC 認証当局

住所: C-DAC, Pune University Campus,
Ganeshkhind Road,
Pune-411007,
Maharashtra

権限ある代表者: Dr N. Subramanian
電話番号: 020 - 25704301 / 25704210
電子メール ID: N/A

- Capricorn 認証当局

住所: G-5, Vikas Deep Building, Plot-18,
Laxmi Nagar District Centre,
Delhi - 110092 .

権限ある代表者: Rajesh Mittal
電話番号: 011 4244 8288
電子メール ID: sales@Certificate.Digital

- NSDL e-gov 認証当局

住所: NSDL e-Governance Infrastructure Ltd.
1st Floor, Times Tower, Kamala Mills Compound,
Senapati Bapat Marg, Lower Parel,
Mumbai 400013.

権限ある代表者: Mr. Hiten Mehta, Senior Vice President,
Mr. Milind Mungale, Senior Vice Presiden

電話番号: 022 4090 4242/ 40904232 / 40904540/
40904467 /40904805 / 40904408

電子メール ID: esign@nsdl.co.in

第 43 条及び第 43 条 A の違反に関する裁定において、裁定官は、IT 法第 46 条に基づき中央政府によって選任される。2003 年 3 月 25 日付けの通知第 G. S. R. 240(E)号に従い、各州又は連邦直轄領の情報技術局の書記官で通常取締役以上の役職の者であり、かつ、情報技術の分野において必要な経験及び必要な法律又は司法に関する経験を有する者が、IT 法に基づき裁定官として選任される。認証当局管理者又は裁定官の決定については、IT 法に基づき設立されたサイバー上訴裁定所に対して上訴することができる。同裁定所の住所及び連絡先は、以下のとおりである。

サイバー上訴裁定所
電子情報技術局

通信情報技術省
Jeevan Bharti (L. I. C.) Building, Ground Floor,
Outer Circle, Connaught Place,
New Delhi - 110001
+91-11- 23355881 (事務所)
+91-11- 23354689 (ファックス)

② 公開鍵インフラストラクチャー

インドでは、公開鍵 (Public Key) 及び秘密鍵 (private key) を構成する非対称暗号システムを通じて電子取引、契約及び書類の保護を確保する目的で、監督規制当局を設立するために公開鍵インフラストラクチャー (以下「PKI」という。) システムが開発された。PKI には、主たる監督当局としての認証当局管理者が含まれる。認証当局管理者は、PKI ヒエラルキーにおいてその下位で機能する認証当局の規制及びライセンス付与を行う。また、IT 法第 18 条 (b) に基づき、認証当局管理者は、認証当局の公開鍵のデジタル署名を行う目的で、インド・ルート認証当局 (以下「インド・ルート認証当局」という。) を設立した。インド・ルート認証当局は、権限を付与された認証当局管理者職員によって運営されている。

現在、認証当局管理者の公式ウェブサイトによると、当該組織には、一定数の従業員に加え、9 名のメンバーがいる。また、認証当局の管理者は、権限を与えられた監査人パネルを有する。

③ 裁定及び上訴裁判所

各州又は連邦直轄領の IT 書記官が、同法に基づく裁定官となる。認証当局管理者又はいずれかの裁定官による決定については、IT 法第 57 条に基づきサイバー上訴裁定所に対して上訴を行うことができる。2017-2018 年度 2 について認証当局管理者に割り当てられた予算は、7,000 万ルピーであり、サイバー上訴裁定所及び Cert-In (インド・コンピュータ緊急対応チーム) に割り当てられた予算は、合計で 4 億 480 万ルピーである。

④ 運用実態

訴えについては、法律違反の性質により、該当の事件に対する管轄権を有する各州/連邦直轄領の裁定官又は認証当局管理者に対して行うことができる。IT 法第 43 条及び第 43 条

² <http://indiabudget.gov.in/ub2017-18/eb/sbe26.pdf> において閲覧可能。

Aに基づくデータプライバシーの侵害があった場合、権利侵害を受けた者は、当該事件に対して管轄権を有する該当の裁定官に申し出を行うことができる。

訴えについては、原告の詳細、訴因、違反の日時及び場所、事件の簡潔な説明、請求された損害額等といった事項に言及詳述する 2003 年情報技術規則の付属書類（裁定官の資格及び経験並びに調査の方法）に規定される仮の訴えとして、裁定官に対して申立てを行うことができる。裁定官に対して申し立てが行われた一切の訴えは、2003 年情報技術規則の規則（Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003）第 8 条（裁定官の資格及び経験並びに調査の方法）に定める手数料を添えるものとする。

インドの裁定官は、IT 法に基づくその権限を行使する形で、データ及び金融情報の保護を促進する目的ですでに複数の決定を行っている。例えば、Umashankar Sivasubramanian v. ICICI Bank 事件において、タミル・ナードゥ州の裁定官は、2010 年 4 月 12 日付の決定において、ICICI 銀行が、適切な検証水準及び認証水準を有する安全なインターネット・バンキング・システムの設定を怠り、これにより IT 法第 43 条に基づく原告のセンシティブ金融情報に対する不正アクセスが発生し、その結果重大な金銭的損失が原告に生じたと判断した。

Poona Auto Ancillaries Pvt. Ltd. v. Punjab National Bank 事件においても、原告の金融データの侵害の防止における銀行の過失に関して、マハーラーシュトラ州の裁定官により 2013 年 2 月 23 日の同裁定官の決定において類似の判断が行われた。

裁定官又は認証当局の決定によっていずれかの者の権利が侵害された場合、かかる者は、当該決定についてサイバー上訴裁定所に対して上訴を行うことができる。

サイバー上訴裁定所に対して申し立てを行うには、サイバー上訴裁定所の登録官に対して様式-1 を提出し、送金小切手又は支払指図の方法により 2,000 ルピーの裁判所費用を添え、紙面による申立書を 6 部添える。申立人は、被告の完全な住所を記載した空の封筒（被告が複数いる場合は複数の封筒）を呈示し、申立の受領を確認する登録官によって署名された申立受理書を添付することができる。

2009 年以降現在まで、サイバー上訴裁定所は、合計 17 件の事件について最終判決を下している。さらに現在、68 件がサイバー上訴裁定所において係属中である。

（４）最近のトピック

① 制度改正の検討状況

2017 年データ（プライバシー及び保護）法案（Data Privacy Bill）は、近時の 2017 年 7 月 21 日に、インドのローク・サバー閣僚議員によりローク・サバー議会（Lok Sabha of the Parliament of India）へ提出された（以下「2017 年データプライバシー法案」という。）。

2017 年データプライバシー法案の目的は、デジタルプライバシーに対する権利の保護及び定義づけ並びに個人データを保護するためのデータプライバシー当局の設立であった。プライバシーに関する法案が議会に提出されたのは本法案が初めてではなく、過去にも特定の制定法の範囲に基づくプライバシーを確立するために複数の試みがなされていた。しかしながら、いずれのプライバシー法案も現段階では議会によって承認されていない。2017 年データプライバシー法案も、ロック・サーバーにおいて未決となっている。2017 年データプライバシー法案とは、他の複数の国においては既に認められているデータプライバシー権をインド国民に付与しようとするものである。2017 年データプライバシー法案に顕著な特徴を以下に概説する。

ア 2017 年データプライバシー法案

2017 年データプライバシー法案は、法定のプライバシー権を付与するものであるが、「言論及び表現の自由に対する権利 (Right to Freedom of Speech and Expression)」及び「生命に対する権利 (Right to Freedom of Speech and Expression)」について言及するインド憲法第 19 条及び第 21 条に基づき同様の付与が行われている。Justice KS Puttaswamy v Union of India (以下に記載する。) 事件において最高裁判所がプライバシー権を基本的権利と判断したため、2017 年データプライバシー法案に基づく本規定は、これに応じて改正される見込みである。

同法案は、政府機関、政府組織及び/又はこれらを代理するその他の者に適用される。2017 年データプライバシー法案に基づく「第三者」の定義にも、公共団体が含まれる。2017 年データプライバシー法案に政府当局を含めるという案は、対象を法人及び当該法人を代理する者のみに限定し、政府当局をその対象に含めなかった個人情報規則に基づく既存の体制からの重要な転機を象徴している。

同案は、包括的枠組みの策定によりインドにおけるデータ保護体制を整備し、かつ、「データプライバシー及び保護当局 (Data Privacy and Protection Authority)」以下の設立を提案している。データプライバシー保護当局は、規制当局及び IT 法に起因する紛争の仲裁機関として機能し、かつ、データ処理者及びデータ管理者に対する職権による行為 (Suo Moto Action) を開始する権限を有する。「データ管理者」(Data Controller) という用語は、同法案に基づき「単独で又は他の者と連帯若しくは共同で、一切の個人データの使用又は処理の目的又は方法を決定する者」を意味すると定義づけられた。また、個人データに関する「データ処理者」とは、データプライバシー法案に基づき「データ管理者の従業員以外の者で、独立して又はデータ管理者を代理してデータを処理する者」を意味すると定義づけられた。

さらに、同法案は、すべての者が、プライバシー通知の発行により情報の処理について適切に情報を提供されると規定している。個人情報規則に基づく既存の体制には、法人の

ウェブサイトにおけるプライバシー方針の公表に関する規定がおかれているが、同法案は、さらに一歩進んでプライバシー通知の内容及び様式を特定している。同法案は、開示されるデータの種別に応じて個別化される法定枠組みを設定する手助けとなり、かつ、意図された目的以外の目的で提供されたデータが使用され、又は保管について同意がなされた期間よりも長い期間にわたってデータが保管された場合に、データ処理者又はデータ管理者に責任を負わせる選択権を当該データ開示者に与えている。

同法案は、提供されたデータの削除を求める権利を付与している。データ削除を求めるかかる権利は、データ処理者及びデータ管理者に対してさらに重い責任を課すことになり、データ処理者及びデータ管理者は、自己に提供されたデータを規定された期間内に削除しなければならない。この点において、個人情報規則において同意の撤回権に関連する類似の条項がおかれている点につき注意が必要である。

同法案は、当該法案に基づく一切の違反を裁判権内にある違反と位置づけ、既存の一切の違反について罰金を増額し、懲役期間を延長した。同法案に基づき、個人データ及びセンシティブ個人データに関連する違反の場合、違反が適時に是正されるための適切な措置が違反者によって強制的に実施されるよう懲役及び違反の日数に応じた日割の罰金の性質を有する罰則が課された。

委員会は、2017年11月28日に、インドのデータ保護枠組みに関する白書を公表した。これにより、委員会はデータ保護及び情報プライバシーに関する様々な問題及び要因に着目し、これに関する暫定的な見解を作成したうえで、一般からの提案及び意見を募集した。同委員会は、データ保護法案を作成する予定であり、白書は、特にデータ保護に関する法律の制定に向けた前進となる。本白書における委員会の見解は、暫定的である旨明記されているが、データ保護法のあらゆる側面に関して見解が述べられている。同白書は、データ保護法が準拠すべき7つの原則を提示した。

(i) 技術不可知論 (Technology Agnosticism)

法律は、技術については不可知論に基づかなければならない。技術の変化及び法令順守の基準の変更を考慮する柔軟性がなければならない。

(ii) 総体的適用 (Holistic Application)

法律は、民間部門の事業者及び政府の双方に適用されなければならない。一定の正当な国家の目的のために、特質的な義務を別途設定することができる。

(iii) インフォームド・コンセント (Informed Consent)

同意は、人間の自立性に関する表現である。かかる表現を本来的なものとするため、同意は、情報を得たうえで行われ、かつ、意味を持つものでなければならない。法律上、同意が上記の基準を満たすことを保証されていなければならない。

(iv) データの最小化 (Data Minimization)

処理されるデータは、データが要求される目的その他それと調和するデータ対象にとって有益となる目的に合致する必要最小限なものでなければならない。

(v) 管理者の説明責任 (Controller Accountability)

データ・管理者は、自己又は自己が処理を行うにあたりデータを共有した事業者による一切のデータ処理について、説明責任を負う。

(vi) 体系的な執行 (Structured Enforcement)

データ保護枠組は、十分な能力を有する高い地位の法定当局により執行されなければならない。これは、適切に分散された執行メカニズムと共存しなければならない。

(vii) 抑止的罰則 (Deterrent Penalties)

不正処理に対する罰則は、抑止力の確保のために適切なものでなければならない。

イ 委員会

委員会は、効果的なデータ保護の目的において、効率的な監視及び捜査、基準設定並びに啓蒙促進のために、別個かつ独立の規制当局が必要となる場合がある旨記載している。また、国家の利益を正当化するために、データ管理者がデータ保護法の対象から除外され得る場合の一定のシナリオも想定されている。

コメントの公募及び提案の最終提出日は、2018年1月31日であった。

時系列的には、2017年データプライバシー法案が先であり、白書が後である。委員会は、データ保護法案の起草を求められており、同法案は導入段階である。委員会がデータ保護法案の起草を求められていることから、同法案の起草にあたり2017年データプライバシー法案の内容のすべてではなく一部のみが委員会によって採用される可能性もあるため、2017年データプライバシー法案に含まれる規定が変更される可能性がある。

② 個人情報に関連した主要な裁判例

近時、最高裁判所は、Justice KS Puttaswamy v Union of India³事件において、プライバシー権について判断し、データ保護の概念について詳しく言及した。最高裁判所は、2017年8月24日判決において、プライバシー権がインド憲法第21条に基づく生命及び個人の自由に対する基本的権利に含まれる基本的な権利である旨言い渡した、M.P. Sharma vs. Satish Sharma, District Magistrate, Delhi⁴及びKharak Singh v. State of Uttar Pradesh⁵

³ 2017 (10) SCALE 1

⁴ (1954) SCR 1077

⁵ (1964) 1 SCR 332

の判決においてプライバシー権が憲法上保障された権利ではないとした判断を覆した。Jagdish Singh Khehar 最高裁判官長、R. K. Agrawal 裁判官、S. Abdul Nazeer 裁判官及び D. Y. Chandrachud 裁判官博士を代表して、D. Y. Chandrachud 裁判官博士によって判決が言い渡されたが、J. Chelameswar 裁判官、S. A. Bobde 裁判官、Abhay Manohar Sapre 裁判官、Rohinton Fali Nariman 裁判官及び Sanjay Kishan Kaul 裁判官は、別途判決意見を言い渡した。

D. Y. Chandrachud 裁判官博士によって言い渡された判決意見のパート S は、情報プライバシーの概念について述べている。J. Chandrachud 裁判官博士は、その判決意見において、同時に複数の者による閲覧可能性、データ窃盗が探索不可能であること及びさらなるデータをアウトプットするためのインプットとしてのアウトプット・データの活用という観点から情報の本質について述べている。また、「同意の問題に関連するものとして、データ移転及び利用に関して、情報のデータ受領者による開示を要する透明性の要件がある。」とも述べている。さらに、同氏は、国家及び国家以外の主体からのデータプライバシーに対する高まりつつある脅威についても言及し、個人データの保護における個人の利益と正当な国家の利益のバランスを取ることの必要性について述べ、正当な国家の利益のために、国家の治安維持その他の福祉目的を問わず、国家は、個人データの収集保管にあたり、同データが不正に使用又は無関係の目的のために使用されないよう保障すべきであることを説明した。

同氏はまた、プライバシー権を制限するにあたり国家が充足すべき 3 つの要件についても説明した。「プライバシーの制限を正当化する法律が存在していなければならないとする第一の要件は、憲法第 21 条における明確性の要件である。第二に、必要性の要件がある。かかる要件は、正当な国家の目的という観点から、制限を課す法律の性質及び内容が憲法第 14 条の求める合理性の範囲内であることを担保しており、国家の恣意的な行為に対する制限となる。第三の要件は、立法府によって採用されるかかる手段が、法律によって充足しようとする目的及び必要性に比例していることである。比例要件により、権利に対する侵害の性質及び本質が法律の目的に対して不相応でないことが保証されるという理由から、比例要件は、国家の恣意的な行為に対する制限において不可欠である。生命及び自由に関する権利において本質的であるプライバシー権並びに本判決第 III 部における自由は、かかる自由に適用される制約と同一の制約の対象となる。」

同氏は、強固なデータ保護の構築について、すでにその検討を開始していた中央政府にこれを委ねたが、同氏は、情報プライバシーがプライバシー権における重要な側面であると結論付け、個人のプライバシー権及び正当な国家の利益とのバランスを考慮に入れたうえで、新しいデータ保護体制を敷くよう中央政府に託した。

さらに同氏は、同氏の判決意見において、国家による個人データに関する電話の盗聴及びインターネットのハッキング行為もまた、プライバシーの領域に該当する分野であると述べている。

J. Kaul 裁判官は、同氏の判決意見の第 13 項において、監視、データの収集及び保管等を通じた国家によるプライバシー侵害の可能性に関する懸念を表明した。同氏は、国家によるセキュリティを目的としたデータ傍受の望ましさについて認めたが、それでも、かかる行為は適切に規制されるべきであると述べた。

同氏は、ヨーロッパ連合 (European Union) における「忘れられる権利 (Right To Be Forgotten)」の認識について言及する一方、第 69 項において、「もし我々が類似の権利を有することになるとすれば、そこでは、自己の個人データに関する処理又は保管をこれ以上望まない個人が、個人データ又は個人情報ですでに不要、無関係又は不正確となり、かつ、正当な利益に寄与しない場合に、システムからかかるデータを削除することを可能とすべきである。そのような権利は、表現及び情報の自由 (freedom of expression and information) の権利行使、法的義務の遵守、公衆衛生の分野における公益を理由とした公益のために実行される責務の履行、公共の利益における目的達成、科学的若しくは歴史的調査の目的若しくは統計上の目的、又は法的請求の申立て、行使若しくは抗弁のために当該情報、データが必要である場合には、行使できない。」と意見を述べた。

同氏はさらに、EU の 2016 年規則 (European Union's Regulation of 2016) に言及すると同時に、プライバシー権は、他の権利同様絶対的なものではなく、比例原則等による一定の制限、例えば、他の人権、正当な国家安全保障の利益、科学的若しくは歴史的調査の目的又は統計上の目的を含む公益、刑事犯罪及び公安に対する脅威に関する捜査、匿名情報、税法に基づく捜査等による制限の対象となると述べている。

2017 年 8 月 24 日の Justice KS Puttaswamy v Union of India 事件における前述の最高裁判所による暫定的判決の後も、アドハー及び ID 番号法がインドの法律に基づく個人のプライバシー権を侵害するかという問題は、最高裁判所において保留され、アドハー (Aadhar) の憲法上の効力に異議を唱える申立の審理のために 5 名の裁判官による法廷が特別に構成された。

最高裁判所は、2017 年 12 月 15 日に、上記の事件における最終判断が行われるまでの間、アドハーと中央政府の各種計画との強制的紐付けに関して以下の方針を示した。

- (a) アドハーナンバー (Aadhar Number) と各省庁によるすべてのサービス及び計画との強制的紐付けの期限を 2018 年 3 月 31 日に延長した。
- (b) 銀行口座に関しては、アドハーナンバーの紐付けの期限は、2018 年 3 月 31 日に延長されたが、新規の銀行口座保有者については、酌量措置としてアドハーの申請を行えば足りるとし、アドハーの申請を行ったことの証明として申請番号を銀行に提出することができるとした。
- (c) さらに、強制的アドハーをベースにした e-kyc (すなわち、電子ベースの顧客確認) の期限も、2018 年 3 月 31 日に延長された。
- (d) 上記のとおり 2018 年 3 月 31 日に延長された、中央政府の省庁による一切の計画に関する期限は、すべての州政府にも適用される。

13. ロシア

(1) 制度概要

① 法体系の概要

1993年12月12日付ロシア連邦憲法 (Constitution of the Russian Federation, 以下「憲法」という。) ⁶は、プライバシーに関する基本的な個人の権利及び自由について定めている (同法第24条)。

ロシアにおける個人データ保護一般について定めたのが、2006年7月27日付連邦法第152-FZ号「個人データについて」 (Federal Law “On Personal Data” dated July 27, 2006 No. 152-FZ⁷、以下「個人情報法」という。) である。同法は、公共・民間の両部門に適用されるロシアにおける個人データ保護に関連する基本規制を定めている。

2006年7月27日付連邦法第149-FZ号「情報、情報技術及び情報保護について」 (Federal Law “On information, information technologies and protection of information” dated 27 July 2006 No 149-FZ, 以下「情報、情報技術及び情報保護に関するロシア連邦法」という。) は、ロシアにおける情報の取扱い及び処理に関する規制を定めている。

2001年12月30日付ロシア連邦法第197-FZ号ロシア連邦労働法典 (Labour Code of the Russian Federation dated December 30, 2001 No. 197-FZ、以下「労働法」という。) は、従業員の個人データの処理に関する具体的な規則を定めている (同法第86乃至90条)。同法は、公共・民間の両部門に適用される。ただし、公共部門においては、(公職雇用に関する) 具体的な規則が労働法に優先する。

また、ロシアの規制は、連邦法に限らず、ロシア連邦政府、連邦通信・情報技術・マスコミ監督庁 (Federal Service for Supervision of Communications, Information Technology, and Mass Media、以下「Roskomnadzor」という。) ⁸、連邦技術・輸出管理局 (Federal Service for Technical and Export Control、以下「FSTEC」という。) ⁹、連邦保安庁 (Federal Security Service、以下「FSB」という。) ¹⁰等の国の執行機関の法規 (規制、命令、政令) においても定められているため注意が必要である。

民間部門・公的部門の区別については、原則的には主たる規制法である個人情報法が民間部門・公的部門の両部門に適用されることになるが、別途特定の具体的な規制が定めら

⁶ <https://web.archive.org/web/20101017004036/http://archive.kremlin.ru/eng/articles/ConstIntro01.shtml>

⁷ 一般に、ロシアにおける法律の記載に際しては、法律の名称・公布された年月日・制定された年における法律の通し番号が表記される。なお、「FZ」はФедеральный Закон (連邦法) の略称である。

⁸ <https://eng.rkn.gov.ru/>

⁹ <https://fstec.ru/en/>

¹⁰ <http://www.fsb.ru/>

れている場合がある。また、国家機密を構成する個人データの処理は、民間部門・公的部門又は産業について例外なく、1993年7月21日付国家機密に関するロシア連邦法(第5485-1号)(Federal Law on State Secrecy dated July 21, 1993 No. 5485-1、以下「国家機密法」という。)により規制される。

② 民間部門に適用される主な連邦法

民間部門においては、個人情報法、労働法が直接適用される他、産業別の法令に従い具体的な規制が適用される場合がある。

2003年7月7日付連邦法第126-FZ号「電気通信について」(Federal Law “On Telecommunications” dated July 7, 2003 No. 126-FZ、以下「電気通信法」という。)は、ユーザーの個人データの処理、通信の秘密を確保し、電気通信サービスが提供されるユーザーを特定する電気通信プロバイダーの義務、及び大量メール送信への同意の取得に関する事項を規制している(同法第44条、第44.1条、第53条及び第63条)。

1990年12月2日付連邦法第395-1号「銀行及び銀行業務について」(Federal Law “On Banks and Banking” dated December 2, 1990 No. 395-1、以下「銀行法」という。)は、顧客の銀行取引、口座及び預金に関する情報の機密性の確保に関連する具体的な規制を定めている(同法第26条)。また、同法は、かかる情報を開示できる状況を定めている。例えば、自然人の口座及び預金に関する情報は、裁判所決定の執行を確保することを認められる裁判所又は国家公務員に対し提供することができる(同法第26条)。銀行秘密の保護対象となっている個人データの処理に関してはより厳格な規制が定められている。

2011年11月21日付連邦法第323-FZ号「ロシア連邦における国民の健康保護の基礎について」(Federal Law “On the Basics of Citizens’ Health Protection in the Russian Federation” dated November 21, 2011 No. 323-FZ、以下「健康保護法」という。)は、医療秘密並びに患者及び医療従事者の個人データの処理に関する事項を規制している(同法第13条及び第92条乃至第94条)。医療秘密の保護対象となっている個人データの処理に関する規制は、より厳格である。

公証、弁護士、保険等に関連する秘密についても、産業別の規制が適用される。さらに、一定の種類秘密を構成する情報の保護には、産業別の規制が包括的なサイバーセキュリティ規制(決済システムに適用されているもの等)が定められている。

③ 公的部門に適用される主な連邦法

国家機密法は、ロシア連邦の安全を確保するため、国家機密としての情報の定義付け又は国家機密の地位の取消し及び国家機密の保護に関連して発生する関係について規定している(同法第1条)。同法は、軍事、外交政策、経済、諜報及び対諜報活動、捜査活動の分

野における国家による保護の対象となっている情報で、その開示がロシア連邦の安全に害を与え得るものに適用される。

2003年5月27日付連邦法第79-FZ号「ロシア連邦の国務体制について」(Federal Law “On the System of the State Service of the Russian Federation” dated May 27, 2003、以下「国務体制法」という。)及び2004年7月27日付連邦法第79-FZ号「ロシア連邦の国家公務員について」(Federal Law “On State Civil Service of the Russian Federation” dated July 27, 2004 No. 79-FZ、以下「国家公務員法」という。)は、国家公務員の個人データの処理に関する一定の具体的な規制を定めている。

2007年3月2日付連邦法第25-FZ号「ロシア連邦の地方公務員について」(Federal Law “On Municipal Service of the Russian Federation” dated March 02, 2007 No. 25-FZ、以下「地方公務員法」という。)は、地方(市町村)公務員の個人データの定義や、個人データについて規定した労働法14章の適用について規定している。

2008年12月22日付連邦法第262-FZ号「ロシア連邦における裁判所の活動に関する情報へのアクセスの確保について」(Federal Law “On Ensuring of Access to the Information on Activities of the Courts in the Russian Federation” dated December 22, 2008 No. 262-FZ)は、インターネット上で正式に公表される裁判所決定に含まれる個人データの匿名化に関し規定している。

④ 個人情報に関する州法

ロシアの法体系は、連邦及び州(地方又は市町村)法の存在を予定している。しかしながら、個人データ保護の問題は、憲法によると、プライバシーに対する人権の観点から慎重を要することを前提に、連邦法の管轄であるとされている。

(2) 主な法律の概要

① 個人情報法

ア 法律の概要

個人情報法は、2007年1月1日より施行された。

本法は、連邦政府機関、ロシア連邦に属する政府機関その他の地方政府機関、地方自治体、法人及び自然人による、例えば情報・電気通信ネットワークの分野における自動化機能(設定されたアルゴリズムに従って、物質媒体に記録され、カードファイルその他の体系化された個人データの集成において入手可能な個人データの検索及び/又はかかる個人データへのアクセスを可能とする手段)による、又はかかる機能を用いない個人データの

処理が、自動化機能を用いた個人データに対する行為（操作）の性質に調和する場合にはかかる機能によらない、個人データの処理に関連する関係について規定している（第1条第1項）。

本法の目的は、個人データの処理における個人及び国民の権利及び自由の保護（私生活、個人的及び家族の秘密の不可侵権の保護を含む。）について規定することである。（第2条）

イ 個人情報 の定義

個人データは、「特定された又は特定可能な個人（データ対象者）に直接又は間接的に関連する一切の情報」と定義されている（第3条第1項）。

センシティブデータは、個人データの特殊カテゴリーと同義であり、「個人データ対象者の人種、国籍、政治的、宗教的、哲学的その他の信念、健康、私生活に関する情報」と定義されている（第10条第1項）。

ウ 主な規制・権利の内容

本法は、情報セキュリティの分野における一般規定及びその執行に関する一定の仕組みについて定めている。具体的には、流布された情報がロシア連邦の個人情報法に違反する場合における情報源をブロックするための仕組みについて定めている（第15.1条）。

エ 漏えい等事案発生時の本人及び監督機関等への報告義務

データ漏えい通知

現在ロシアには、データ対象者（又は関与するデータ管理者）による強制的なデータ漏えい通知について定める法律はない。ただし、当該通知は、各データ対象者若しくはデータ管理者との契約又はデータ管理者の内部方針に基づき義務付けられる場合がある。かかる通知は、ベストプラクティス・アプローチ及び安全措置として推奨されている。

なお、データ漏えいの排除についてデータ対象者及び Roskomnadzor（漏えい排除要請が当該国家機関により提起された場合）に通知するという要件はある（第21条第3項）。

Roskomnadzor への登録

個人データを処理する際、第23条に基づき、Roskomnadzor に通知を届出ることが原則とされる。ただし、いくつかの例外があり、それは個人データが(a)雇用法規に従って処理される場合、(b)データ対象により公に入手可能とされる場合、又は(c)データ対象者の名字、名前及びミドルネームのみから構成される場合等である。

Roskomnadzor は、これらの例外を極めて狭義に解釈している。従業員データが第三者（関

係会社を含む。)に移転された場合で、ロシア連邦法により移転が定められていない場合は、かかる処理は例外(すなわち、処理がロシアの雇用法規に基づき義務付けられる場合)に該当しないため、Roskomnadzor への登録を要する。近年の執行実務は、求職者の個人データ及び/又は前従業員の個人データの処理がこれらの例外のいずれにも該当しないことを示している。

通知は、すべてのデータ処理活動(従業員、クライアント、取引先の代表者、販売促進イベントの参加者等の全データ対象者に関連するもの)について届出なければならない。データ処理活動に何らかの変更があった場合、データ管理者は、10 営業日以内にかかる変更につき Roskomnadzor に通知しなければならない(第 22 条)。

Roskomnadzor は、登録申請が提出された場合、30 日以内に事業体のデータ管理者としての登録について決定を行わなければならない(第 22 条)。

オ 安全管理措置

データ管理者の基本的義務は、法的、組織的及び技術的な措置を取ることにより、個人情報法その他の関連規制法の要件の遵守を確保し、処理された個人データの安全と秘密を確保することである。個人情報法は、データ管理者が取るべき措置の一覧を以下項目のとおり定めている(第 18.1 条及び第 19 条)。

- ・ 個人データ処理のアレンジについて責任を負う者(データ保護オフィサー)の任命。
- ・ データ管理者の個人データ処理方針、個人データ漏えいとその影響の防止及び検知を目的とする手続を決定する内部書類の採用、並びに自己の個人データが処理対象となっている個人データ対象者がこれらの書類に自由にアクセスできるよう確保すること。個人データが、ウェブサイトを通して処理される場合、プライバシーポリシーをウェブサイト上で公表しなければならない。
- ・ 内部統制並びに(又は)個人データ処理のロシアのデータ保護法令及び地方の規範的法規への遵守の監査の実施。
- ・ データ保護法令の違反により個人データ対象者が被り得る潜在的な害悪を推定し、当該害悪、及び個人データ保護のために講じられた措置を相関させること。
- ・ 個人データの処理を行う全従業員に対する、ロシアのデータ保護法令及び個人データ処理に関連する問題に関する内部書類の周知。
- ・ 個人データが個人データ情報システム上で処理されている間の、個人データの安全に対する脅威の検知。
- ・ 個人データが個人データ情報システム上で処理されている間の、個人データの安全を確保するための組織的及び技術的措置の適用。
- ・ 遵守評価手続を通過したデータセキュリティ・ツール(認証された暗号化ツール等)の適用。

- ・ 個人データ情報システムの試運転に先立ち、個人データの安全を確保するために取られた措置の効果の評価。
- ・ 個人データを内包する媒体の記録の維持。
- ・ 個人データへの不正アクセスの検知及び対策。
- ・ 不正アクセスにより変更又は破壊された個人データの復元。
- ・ 個人データ情報システムにおいて処理された個人データへのアクセスに関する規則の設定、及び個人データ情報システム上で個人データに対してなされたすべての処置の記録。
- ・ 個人データの安全を確保するために取られた措置、及び情報システム上での個人データの保護の安全レベルの監視。
- ・ 手動の個人データの処理に関するロシア法令により設定された要件の遵守。

実際にデータ管理者が取るべき安全措置の具体的な範囲は、データ管理者自身が、処理された個人データの安全に対する実際の脅威の評価及び個人データ保護の求められるレベルに基づき決定する（第 18.1 条及び第 19 条）。

決定のためのマトリックスは、2012年11月1日付ロシア連邦政府政令(第1119号) (Decree of Government of the Russian Federation dated November 1, 2012 No. 1119) により承認された「個人データの情報システム上で処理される個人データのセキュリティに関する要件」(“Requirements to Security of Personal Data Processed in Information Systems of Personal Data”) において以下のように規定されている。

マトリックス 1 個人データセキュリティへの脅威のタイプ

「個人データのセキュリティに対する脅威」とは、情報システム上で処理される場合の個人データの破壊、変更、ブロック、複製、提供又は開示その他の違法行為をもたらし得る、個人データに対する不正（偶発を含む。）アクセスの危険を暗示する一連の条件及び要因を指す（第 19 条）。

かかる脅威には以下の 3 タイプがある。

脅威のタイプ	内容
タイプ 1	情報システムで使用されるシステムソフトウェアにおいて、脅威その他の事象が、書面化（宣言）されていない可能性の存在に関連するものを含む情報システムに関するもの

タイプ 2	情報システムで使用される応用プログラムにおいて、脅威その他の事象が、書面化（宣言）されていない可能性の存在に関連するものを含む情報システムに関するもの
タイプ 3	情報システムで使用されるシステムソフトウェア及び応用プログラムにおいて、脅威その他の事象が、書面化（宣言）されていない可能性の存在に関連するものを含む情報システムに関するもの

マトリックス 2 セキュリティレベル

報システム上で個人データを処理するに際して、4段階の保護のレベルが定められている。

個人データ保護のレベル	必要条件(少なくとも以下に挙げる特定のレベルの条件の一つ)	講じるべき必要最低限の措置
データ保護レベル 1	<ul style="list-style-type: none"> 情報システムに関し、タイプ 1 の脅威が存し、情報システムが個人データの特殊カテゴリー¹¹若しくは生体個人データ¹²、又は個人データのその他のカテゴリー¹³を処理する場合 情報システムに関し、タイプ 2 の脅威が存し、情報システムが管理者の従業員を除き 100,000 人以上の個人データ対象者の個人データの特殊カテゴリーを処理する場合 	<ul style="list-style-type: none"> レベル 2、3 及び 4 について定められた全ての措置 データ管理者の従業員の情報システムに含まれる個人データへのアクセス権限変更の電子セキュリティ・ログにおける自動登録の確保 情報システム上の個人データのセキュリティについて責任を負う組織的な部署（部）の設置、又は当該機能の既存の組織的な部署（部）の任命
データ保護	<ul style="list-style-type: none"> 情報システムに関し、タイプ 1 の脅 	<ul style="list-style-type: none"> レベル 3 及び 4 について

¹¹ 個人データの特殊カテゴリーとは、人種、国籍、政治的信条、宗教又は哲学的信念、健康状態、私生活の事実に関する情報（法令において明示される場合を除く。）をいう（第 10 条）。

¹² 生体個人データとは、本人を特定し得る任意の個人の生理学的及び生物学的特徴をいう（第 11 条）。

¹³ 個人データのその他のカテゴリーとは、「生体個人データ」、「個人データの特殊カテゴリー」、「公に入手可能な個人データ」に該当しない個人データを指す。

個人データ保護 のレベル	必要条件(少なくとも以下に挙げる特定 のレベルの条件の一つ)	講じるべき必要最低限の措置
レベル 2	<p>威が存し、情報システムが公に入手可能な個人データ¹⁴を処理する場合</p> <ul style="list-style-type: none"> ● タイプ 2 の脅威は、情報システムに関するもので、情報システムが管理者の従業員の個人データの特殊カテゴリー又は管理者の従業員を除く 100,000 人以下の個人データ対象者の個人データの特殊カテゴリー ● タイプ 2 の脅威は、情報システムに関するもので、情報システムが生体個人データを処理する場合 ● タイプ 2 の脅威は、情報システムに関するもので、情報システムが管理者の従業員以外の 100,000 人以上の個人データ対象者の公に入手可能な個人データを処理する場合 ● タイプ 2 の脅威は、情報システムに関するもので、情報システムが管理者の従業員以外の 100,000 人以上のデータ対象者の個人データのその他のカテゴリーを処理する場合 ● タイプ 3 の脅威は、情報システムに関するもので、情報システムが管理者の従業員以外の 100,000 人以上のデータ対象者の個人データの特殊カテゴリーを処理する場合 	<p>定められた全ての措置</p> <ul style="list-style-type: none"> ● 電子メッセージログの内容へのアクセスが業務遂行のためにこれらの情報を必要とする管理者の役員（従業員）又は権限保有者のみ可能であるように確保すること
データ保護 レベル 3	<ul style="list-style-type: none"> ● タイプ 2 の脅威は、情報システムに関するもので、情報システムが管理者の従業員の公に入手可能な個人 	<ul style="list-style-type: none"> ● レベル 4 について定められた全ての措置 ● 情報システム上の個人デ

¹⁴ 公に入手可能な個人データという場合、個人データ対象者本人がかかるデータを公開したこと又はかかるデータが法的な公に入手可能なリソースから受領されたことを示唆する(第 6 条第 1 項第 10 号及び第 8 条)。

個人データ保護 のレベル	必要条件(少なくとも以下に挙げる特定の レベルの条件の一つ)	講じるべき必要最低限の措置
	<p>データ又は管理者の従業員以外の 100,000人以上の個人データ対象者 の公に入手可能な個人データを処理 する場合</p> <ul style="list-style-type: none"> ● タイプ2の脅威は、情報システムに 関するもので、情報システムが管理 者の従業員の個人データのその他 の категория又は管理者の従業員 以外の100,000人以下のデータ対 象者の個人データのその他のカテ ゴリーを処理する場合 ● タイプ3の脅威は、情報システムに 関するもので、情報システム管理者 の従業員の個人データの特殊カテ ゴリー又は管理者の従業員以外の 100,000人以下のデータ対象者の個 人データの特殊カテゴリーを処理 する場合 ● タイプ3の脅威は、情報システムに 関するもので、情報システムが生体 個人データを処理する場合 ● タイプ3の脅威は、情報システムに 関するもので、情報システムが管理 者の従業員以外の100,000人以上 のデータ対象者の個人データのそ 他のカテゴリーを処理する場合 	<p>データのセキュリティにつ いて責任を負う役員（従 業員）の任命</p>

個人データ保護 のレベル	必要条件(少なくとも以下に挙げる特定 のレベルの条件の一つ)	講じるべき必要最低限の措置
データ保護 レベル 4	<ul style="list-style-type: none"> ● 情報システムに関し、タイプ 3 の脅威が存し、情報システムが公に入手可能な個人データを処理する場合、又は ● 情報システムに関し、タイプ 3 の脅威が存し、情報システムが管理者の従業員の個人データのその他のカテゴリー又は管理者の従業員以外の 100,000 人以下の個人データ対象者の個人データのその他のカテゴリーを処理する場合 	<ul style="list-style-type: none"> ● 情報システムが設置される場所のセキュリティについて、かかる場所へのアクセスを認められていない者によるかかる場所への非制御アクセス又は滞在を防止することによるセキュリティの確保 ● 個人データの媒体のセキュリティの確保 ● 職務遂行のために個人データへのアクセスを必要とする個人の一覧を定める書類の管理者の経営陣による承認 ● 遵守評価手続を通過したデータセキュリティ・ツール（認証された暗号化ツール等）の利用（ただし、個人データへの実際の脅威を無効化するためにかかる手段が必要である場合とする。）

上記のマトリックスに加え、FSTEC 及び FSB が策定した以下の命令が併せて考慮される。

- ・ 2013 年 2 月 18 日付連邦技術・輸出管理局 (FSTEC) 命令 (第 21 号) (Order of the Federal Service for Export and Technical Control (FSTEC) dated February 18) により承認された「個人データの情報システム上で処理された個人データのセキュリティを確保するための組織的・技術的措置の範囲及び構成」(“Scope and Composition of

Organizational and Technical Measures to Ensure Security of Personal Data Processed in Information Systems of Personal Data”)

- ・ 2014年7月10日付連邦保安庁命令(第378号)(Order of the Federal Security Service dated July 10, 2014 No. 378 - in force since September 28, 2014)により承認された「各セキュリティレベルについてロシア連邦政府が提示する個人データセキュリティ要件を遵守するために必要とされる情報の暗号保護を用いた、個人データの情報システム上で処理された個人データのセキュリティを確保するための組織的・技術的措置の範囲及び構成」(“Scope and Composition of Organizational and Technical Measures to Ensure Security of Personal Data Processed in Information Systems of Personal Data with Use of Cryptographic Protection of Information Required to Comply with Personal Data Security Requirements Stated by the Government of the Russian Federation with respect to each Security Level”)

公共部門については、情報(国家情報システム上で処理された個人データを含むが国家機密を構成する情報を除く。)保護の要件は、2013年2月11日付連邦技術・輸出管理局(FSTEC)命令(第17号)(Order of the Federal Service for Export and Technical Control of the Russian Federation (FSTEC) dated February 11, 2013 No. 17)により承認される。

カ 適用範囲、適用除外内容

本法は、個人データが自動化手段(通信ネットワークの使用を含む。)によって処理される場合、及び自動化手段がない場合は、非自動処理が自動処理に類似する場合(すなわち、ハードに固定され、登録簿その他の体系化されたデータベースに記載された個人データの検索及びかかる個人データへアクセスすることを可能とする場合)、連邦国家機関、地方組織、市町村(地方)自治体、法人及び個人が行う個人データの処理を規制する(第1条第1項)。

ただし、個人情報法は、以下の場合には適用されない(第1条第2項)。

- ・ 個人データが自然人により私的かつ家族の目的のためにのみ処理される場合(ただし、データ対象者の権利が侵されない場合に限る。)
- ・ 個人データが公文書に関するロシア法に従って保管、説明及び使用される公文書に含まれる場合
- ・ 個人データが国家機密を構成する場合

なお、国家機密法は、国家機密を構成する情報の具体的な体制を定めており、これは個人情報法に従って確立されたものよりはるかに厳格なものである。

本法の地理的適用範囲は、一般規則によるとロシア連邦の領土に限られる。ただし、インターネットの越境性及びインターネット上の個人データ保護の必要性を考慮し、ロシア連邦通信マスコミ省（Ministry of Telecom and Mass Communications of the Russian Federation、以下「Mincomsvyaz」という。）により、特定の情報リソース（ウェブサイト又はモバイル・アプリケーション）において行われた個人データ処理が個人データ保護に関するロシア法令の要件を遵守しているか否かを判断するために適用されるいわゆる「ターゲットテスト」（“Target Test”）が策定されている。

当該テストには、以下の主な状況の分析が含まれる¹⁵。

- ・ ウェブサイトのドメイン名がロシア及びロシアの地域に関連するか否か
（e.g., .ru, .рф, .su, moscow等）及び／又は
- ・ ウェブサイトがロシア語版を有するか否か又はその内容のロシア語への（自動）翻訳を手配するオプションがあるか否か

これらに加えて、以下の「二次的」要素もまた、当該情報リソースとロシア人との繋がりを証明し得るものである。

- (a) ルーブルが支払通貨となっている、又は
- (b) ロシアへの配送又はロシアのユーザーをターゲットとする広告、又は
- (c) リソースの所有者がその事業戦略においてロシア市場を考慮していることを示すその他の要素。

キ 小規模事業者の取扱い

ロシア法は、小規模事業者について特別の取扱いを定めていないため、個人データの処理の一般要件が適用される。ただし、ある程度ロシアの規制が柔軟であり、処理された個人データへの実際のセキュリティの脅威を評価し、必要とされる保護レベルを決定するのはデータ管理者の責任であることを前提とすると、小規模事業者が取るべき措置の実際の範囲は、大規模な事業者に比べると狭まると考えられる。

ク 域外適用

個人データの国際的（又は越境）移転とは、外国に所在する外国の機関、外国の自然人又は外国の法人への個人データの移転を指す（第3条第11項）。

¹⁵ <http://minsvyaz.ru/ru/personaldata/>

本法は、個人データの越境移転に関する具体的な規制を定めている（第 12 条）。かかる規制は、個人データの移転先の法域のいわゆる適切性によって、個人データの越境移転の条件を区別している。

個人データは、個人情報法の一般規則（第 6 条に定める個人データ処理の一般的な正当理由）に従って、十分なレベルの個人データ保護が付与されている法域（適切法域）に移転することができる。

適切な法域は、個人データの自動処理に係る個人の保護に関する条約（1981 年ストラスブルグ ETS 第 108 号）（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, Strasbourg, 1981)）の加盟国及び Roskomnadzor により適切であると認められた国を指す。同条約の加盟国に加えて、適切な法域の一覧は、2013 年 3 月 15 日付 Roskomnadzor 命令（第 274 号）（Order of Roskomnadzor dated March 15, 2013 No. 274）により承認されている。

ケ 紛争処理手続き

ロシア法は、データ保護問題に関する特別な規制を定めておらず、一般手続に係る規則が適用される。

まず、裁判外の紛争処理手続きとして、データ対象者は、Roskomnadzor に請求することにより、データ管理者の行為に異議を申し立てることができる（本法第 17 条）。

また、Roskomnadzor は、個人データ保護に関連する以下の権限を有する（本法第 24 条）。

- ・ 個人データ対象者の権利の保護（不特定多数の個人の保護を含む。）を求めて、裁判所に訴訟を提起し、訴訟手続において個人データ対象者を代理する権限
- ・ 国の検察庁に対し、個人データ対象者の権利の侵害に関する刑事手続きの開始を申し出る資料を届け出る権限
- ・ 個人情報法により定められる要件の遵守を怠った個人及び法人に対し、行政責任措置を課す権限

ロシアにける裁判所は、憲法裁判所と最高裁判所下の裁判所の 2 系統に分かれ、最高裁判所の系統は、更に通常裁判所と商事裁判所の 2 系統に分かれている。このうち、商事裁判所が民事・行政事件のうち経済紛争及び企業活動・経済活動に関連するその他の事件を管轄する。

事業活動の実施に関連する紛争で、データ管理者が Roskomnadzor の命令に異議を唱える場合等は、特別商事裁判所（Special Arbitrazh Courts）により解決される。データ対象者が関与する場合、一般管轄権を有する裁判所によって解決される。

具体的には、データ対象者は、自らが被った損害賠償の裁定及び精神的損害賠償を請求することができる（第 24 条）。

② 情報、情報技術及び情報保護に関するロシア連邦法

ア 法律の概要

情報、情報技術及び情報保護に関するロシア連邦法は 2006 年 8 月 9 日より施行された。

本法は、1) 情報の検索、受領、移転、提示及び流布に対する権利の行使、2) 情報技術の応用及び、3) 情報保護の確保から発生する関係を規制する（第 1 条第 1 項）。

イ 主な規制・権利の内容

本法は、ロシアにおける個人情報法の範囲及び目的を定め（第 1 条、第 2 条及び第 4 条）、法的定義を述べ（第 3 条）、個人データ処理の一般原則（第 5 条）、個人データ処理の正当な理由（第 6 条）、公的情報源に含まれる個人データの処理の細目（第 8 条）、センシティブデータ（第 10 条）及び生体データ（第 11 条）について規定し、個人データ処理に対する同意の一定の義務要件を定め（第 9 条）、個人データの越境移転に関する事項（第 12 条）、データ対象者の権利（第 14 条乃至第 17 条）、データ管理者の義務（第 18 条、第 20 条、第 21 条、第 22 条、第 22.1 条）、データセキュリティ措置（第 18.1 項及び第 19 条）について規制し、データ保護当局の地位を定めている（第 23 条）。

③ 労働法

ア 法律の概要

労働法は 2002 年 2 月 1 日から施行された。

労働法の目的は、市民の労働の権利及び自由の国による保証の設定、好ましい労働環境の創出、被雇用者及び雇用者の権利及び利益の保護であるとされ、労働法令の主な課題は、労働関係の当事者の利益、国の利益の最適調整を達成するために必要な法的条件、並びに本法所定の項目に係る、労働関係及びそれに直接関連するその他の関係の法的規制の創出であるとされる（第 1 条）。

イ 主な規制・権利の内容

本法は、従業員の個人データの処理（第 86 条）、従業員の個人データの移転（第 88 条）、個人データに関する従業員の権利（第 90 条）に関する一般要件を定めている。

ウ 国際的な情報移転に関する規定

従業員の個人データは、従業員の書面同意がある場合に限り（ただし、かかる移転が従業員の生命及び健康への害を防ぐために必要とされる場合又はかかる移転がロシア連邦法により直接定められる場合を除く。）、国内又は海外の第三者に移転することができる（第 88 条）。

④ 国務体制法

ア 法律の概要

国務体制法は 2003 年 5 月 27 日から施行された。

本法は、憲法に従いロシア連邦の国務体制（ロシア連邦の国務管理体制を含む。）の法的・組織的基礎について規定している（前文）。

イ 主な規制・権利の内容

本法は、国家公務員の個人データの処理に関する一定の具体的な規則を定めている（第 14 条）。

⑤ 国家公務員法

ア 法律の概要

国家公務員法は 2004 年 7 月 27 日から施行された。

本法は国務体制法に従い、ロシア連邦の国家公務員に関する法的、組織的かつ財務・経済的基盤を定めている（前文）。

本法によって規制される対象事項は、ロシア連邦の国家公務員の採用、職務遂行及び退職、並びにロシア連邦の連邦国家公務員及び国家公務員の法的資格の定義に関連する関係である（第 2 条）。

イ 主な規制・権利の内容

本法は、国家公務員の個人データの処理及び対応する人事プロセスに関する一定の具体的な規則を定めている（第 10.1 条第 4.2 項乃至第 4.4 項）。

⑥ 地方公務員法

ア 法律の概要

地方公務員法は 2007 年 6 月 1 日から施行された。

本法の規制対象は、ロシア連邦の国民、外国（外国国民も地方公務に就き、さらには国民に仕える権利を有するとするロシア連邦の国際協定の加盟国）の民の公務に対する給与、地方公務員の採用及び解任、並びに地方公務員の法的地位（地位）の決定に関連する関係である（第 1 条第 1 項）。

ただし、代議士、地方自治政府の選出組織のメンバー、地方自治政府の選出役人、任期のない市町村の選挙委員会のメンバーのうち法人である者のうち、特定者として投票権を持つ者で地方政府役人ではない者の地位については定めていない（第 1 条第 2 項）。

イ 主な規制・権利の内容

本法は、個人データについて規定した労働法 14 章の適用を定めた規定を含んでいる（第 29 条）。

⑦ 電気通信法

ア 法律の概要

電気通信法は 2004 年 1 月 1 日から施行された。

本法は、ロシア連邦の領土及びロシア連邦の管轄下にある領土における通信分野での活動に関する法的原則を定め、通信分野における国家権力を有する組織の権限並びに本活動に従事し又は通信サービスを利用する者の権利及び職務を定義している（前文）。

本法において定められる目的は以下のとおりである（第 1 条）。

- ロシア連邦全土における通信サービスの提供条件の設定
- 有望な技術の導入に対する援助の提供
- 通信分野において経済主体の活動に従事する通信サービスのユーザーの利益の保護
- 通信サービス市場の効率的かつ公平な競争に関する規定

- ロシアの通信インフラの開発及び国際通信ネットワークとの統合のための条件の設定
- 軌道周波数資源及び番号資源を含む、ロシアの無線周波数資源の中央管理に関する規定
- 政府機関の通信における要件、国防及び国家安全の必要性の充足条件の設定、並びに法律及び命令の確保のための条件の設定

イ 主な規制・権利の内容

本法は、ユーザーの個人情報を含むデータベースの維持（第 53 条）、大量メール送信（第 44.1 条）及びユーザーの身元情報（第 44 条）について規制している。

⑧ 銀行法

ア 法律の概要

銀行法は 1990 年 12 月 2 日から施行された。

イ 主な規制・権利の内容

本法は、銀行秘密を確保する責任を負う事業者、銀行秘密の範囲及び合法的な開示の状況（第 26 条）について定めている。

⑨ 健康保護法

ア 法律の概要

健康保護法は 2011 年 11 月 22 日から施行された。

本法は国民の健康保護の分野において発生する関係を規制し、以下の事項について規定している（第 1 条）。

- 1) 国民の医療の法的、組織的及び経済的基盤
- 2) 健康保護の分野における人類及び国民の権利及び義務、並びに特定のグループの民衆の権利及び義務、並びにこれらの権利の実現の保証
- 3) 健康保護の分野におけるロシア連邦の政府機関、ロシア政府の構成主体の政府機関及び地方自治体の権限及び責任
- 4) 健康保護の分野の活動に従事する、医療組織、その他の組織及び個人事業主の権利及び責任
- 5) 医療従事者及び薬剤師の権利及び責任

イ 主な規制・権利の内容

本法は、医療秘密に関する事項（第 13 条）並びに患者（第 92 条及び第 94 条）及び医療従事者（第 92 条及び第 93 条）の個人データの処理について規制している。

（3） 監督機関・第三者機関

Roskomnadzor は、2008 年 5 月 12 日付「連邦執行機関の体制及び組織の問題」に関するロシア連邦大統領令（第 724 号）（Order of the President of the Russian Federation “Questions of System and Structure of the Federal Executive Bodies” dated May 12, 2008 No. 724）第 5 項に従って設置されたロシアデータ保護機関である。

Roskomnadzor は、通信、情報及びマスメディア分野を監督する機関であり、その設置及び全般的な権限については、個人情報法第 23 条で定められている。

連絡先及び URL

109074, Moscow, Kitaygorodsky ave., 7 bld. 2

URL: <http://eng.rkn.gov.ru/>（ウェブサイトのいくつかの機能は英語で利用可能である。）

電話番号（495）983-33-93

ファックス番号（495）587-44-68

電子メール: rsoc_in@rkn.gov.ru

報道官: press@rkn.gov.ru and（495）587-42-92 ext. 170

賄賂防止ホットライン:（495）983-33-93

Roskomnadzor 組織図

Roskomnadzor 長官 (Head of the Federal Service for Supervision of Communications, Information Technology, and Mass Media)			
Alexander Alexandrovich Zharov			
副長官 (Deputy Head)	副長官 (Deputy Head)	副長官 (Deputy Head)	副長官 (Deputy Head)
O. A. Ivanov	A. A. Priezzheva	V. A. Subbotin	A. A. Pankov
通信許可証発行部局 (Telecommunication Permit Issuing Department)	個人データ保護部局 (Protecting Rights of Personal Data Subjects Department)	マスコミュニケーション許可証発行部局 (Mass Communication Permit Issuing Department)	組織業務管理部局 (Department of organizational works management)

通信管理監督部局 (Telecommunication Control and Supervision Department)		マスコミュニケーション管理監督部局 (Mass Communication Control and Supervision Department)	管理部局 (Administrative Department)
			財政部局 (Finance Department)
			法務部局 (Legal Department)
			情報技術監督部局 (Information Technology Supervision Department)

(出典) <http://rkn.gov.ru/about/structure/>

Roskomnadzor は、中央オフィスに加え地方オフィスを有している。各地方オフィスは、各々のウェブサイトをも有する¹⁶。

Roskomnadzor の 2017 年の予算は、81.2 億ルーブル (約 154.2 億円) だった。2018 年の予算見込み額は 79.4 億ルーブル (約 150.8 億円)、2019 年は 77.8 億ルーブル (約 147.8 億円) である。この情報は、2016 年 12 月 19 日付連邦法「2017 年の連邦予算及び 2018 年・2019 年の計画期間について」(Federal Law “On the Federal Budget for 2017 and the Planned Period of 2018 and 2019” dated December 19, 2016) で確認することができる。

実際の執行実務は、Roskomnadzor が統計の形で公表している。2017 年前期については、以下の統計がある¹⁷。

定期検査の結果

合計検査数当初予定されていた 587 件中 532 件が実際に行われた。26 件の検査が取り消された。

違反が検知された合計検査数：348 件

¹⁶ 例えば、中央地域の Roskomnadzor のオフィスのウェブサイトは、下記で閲覧可能である：
<https://77.rkn.gov.ru/>

¹⁷ 当該期間以前の期間の全統計については以下のウェブサイトでも閲覧可能である。
<https://rkn.gov.ru/plan-and-reports/reports/p449/>

個人データ保護の分野で違反が検知された合計検査数：1254 件

即時／不定期検査の結果

合計検査数：32 件

違反が検知された合計検査数：7 件

個人データ保護の分野で違反が検知された合計検査数：23 件

系統的監視の結果（主にインターネット上で実施）

監視事由の合計数：1064 件が予定され、1088 件が実際に実施された。

個人データ保護の分野で違反が検知された合計検査数：504 件

責任措置

Roskomnadzor が発行した違反是正命令の合計数：191 件

開始された行政手続／事件の合計数：1763 件

罰金合計額：1,172,300 ルーブル（2,226,380 円）

国民の請求及び要請

当該期間中に Roskomnadzor に届け出された国民の請求及び要請の合計件数：請求及び要請 15,770 件

特定の期間において Roskomnadzor が検討したデータ対象者の請求の合計件数：請求 14,378 件

検討されたデータ対象者の請求に基づき検知された違反の割合：6.9%

情報リソースのブロック

2015 年 9 月 1 日以来、Roskomnadzor は、個人情報法に違反する情報の流布のあった 160 のリソースをブロックしてきた。

（4）最近のトピック

① 制度改正の検討状況

個人データ処理の国内化

2015 年 9 月 1 日、2014 年 7 月 21 日付連邦法第 242 号「情報・通信システム上における個人データ処理の処理手続きに関するロシア連邦の一定の法令の一部改正について」（Federal Law "On Amending Certain Legislative Acts of the Russian Federation in Part of Processing Procedure of Personal Data Processing in Information and Telecommunication Systems" dated July 21, 2014 No. 242、以下「ローカライゼーション法」という。）が施行され、ロシアにおいて活動する又はその活動のターゲットをロシア市場とするデータ管理者にとって最も重要な法律の一つとなっている。

データ管理者は、ローカライゼーション法に従い、個人データに関する一定の操作につ

いて、ロシアに所在するデータベースを用いて行われるように確保しなければならない（ローカライゼーション要件）。これには、個人データの記録、体系化、蓄積、保管、翻案、変更又は検索が含まれる。

個人データは一旦収集されると、主にロシアに所在するデータベース（サーバー施設等。必要に応じてここで維持・アップデートされる。）を経由してホストされる。個人データはその後、海外に所在する他のデータベースに送信することができる。

ローカライゼーション要件により、データ管理者が個人データを海外に送信することを妨げられることはない。ただし、一定の前提条件が充足されることを条件とする。具体的には、個人データは当初、その収集場所であるロシアに所在し、維持される主要データベースに置かれる等の条件がある。主要データベースに内包される個人データはその後、海外に送信し、他のデータベース（二次的データベース）に置くことが可能である¹⁸。

最後に、Mincomsvyaz の勧告¹⁹に従い、データ対象者から個人データを収集した場合、ローカライゼーション要件の遵守を確保する義務が発生する。収集とは、データ対象者から直接又はデータ収集を委託された第三者から個人データを受領する定められたプロセスを意味する。

上記の義務については、個人情報法第 18 条第 5 項に規定がある。

対テロ対策法（「ヤロヴァヤ法（“Yarovaya Laws”）」）

2014 年及び 2016 年において、広範囲の連邦法に対する包括的な改正を導入する 2 グループの法令が採用された。これらの改正は、「対テロ対策法」又は「ヤロヴァヤ法」として知られている（これらの法令の採用を指導した、ロシアの国会議員である、立法者のイリーナ・ヤロヴァヤ（Irina Yarovaya）にちなんで名付けられている。）。現在、プライバシーの分野に影響を及ぼす一定の改正が電気通信法第 64 条及び情報、情報技術及び情報保護に関するロシア連邦法第 10.1 条において反映されている。

同法第 10.1 条への改正は、とりわけ、以下のデータ保持及び電気通信プロバイダー及びインターネットによる情報流布の管理者（すなわち、電子メッセージの交換及び／又は処理を目的とするアプリ又はウェブサイト等の情報リソースを運営する事業体）に課される適法な遮断義務について定めている。

- ・ ユーザーの音声情報、テキスト情報、画像、オーディオ／ビデオその他のメッセージの受領、送付、配信及び（又は）処理の事実を当該行為の完了時点から 1 年間（インターネットによる情報流布の管理者の場合）及び 3 年間（電気通信プロバイダーの場合）ロシア領内で保管すること。

¹⁸概要については、以下のウェブサイトでご覧可能である：

<http://minsvyaz.ru/ru/personaldata/>

¹⁹ <http://minsvyaz.ru/ru/personaldata/> でご覧可能。

- ・ 2018年7月1日から、ユーザーのテキスト・メッセージ、音声情報、画像、オーディオ／ビデオその他のメッセージを（インターネットによる情報流布の管理者及び電気通信プロバイダーの双方について）最長6か月間ロシア領内で保管すること。
- ・ 保持された情報及び暗号解読が必要とされる情報（かかる技術が使用されている場合）を要請に応じて管轄国家当局に提供すること。

さらに、2018年1月1日以降、メッセージャーの運営者であるインターネットによる情報流布の管理者に一定の具体的な義務が課されている（情報、情報技術及び情報保護に関するロシア連邦法第10.1条第4.2項乃至第4.4項参照）。

重要なインフラの情報セキュリティ

2017年7月26日、重要なインフラの安全に関する事項を規制することを目的とする以下の法令が採用された。

- ・ 2017年7月26日付連邦法第187-FZ号「ロシア連邦の重要情報インフラのセキュリティについて」(Federal Law dated July 26, 2017 No. 187-FZ “On Security of Critical Information Infrastructure of the Russian Federation”、以下「CII法」という。)
- ・ 2017年7月26日付連邦法第194-FZ号「連邦法「ロシア連邦の重要情報インフラのセキュリティについて」採用に関するロシア連邦刑法及びロシア連邦の刑事手続法第151条の改正について」(Federal Law dated July 26, 2017 No. 194-FZ “On Amendments to the Criminal Code of the Russian Federation and Article 151 of Criminal Procedure Code of the Russian Federation with regard to Adoption of the Federal Law “On Security of Critical Information”)
- ・ 2017年7月26日付連邦法第193-FZ号「連邦法「ロシア連邦の重要情報インフラのセキュリティについて」採用に関するロシア連邦の様々な法令の改正について」(Federal Law dated July 26, 2017 No. 193-FZ “On Amendments to the Different Legislative Acts of the Russian Federation with regard to Adoption of the Federal Law “On Security of Critical Information Infrastructure of the Russian Federation”)

これらの法令は、医療、科学、輸送、通信、防衛、エネルギー、銀行及び金融、原子力、鉱業、化学、宇宙ロケット、金属学、燃料等の主要産業において運営される施設での情報セキュリティの確保を目的としている（CII法第7条）。

CII法に従い、かかる施設を所有する事業体に対し、一定の情報セキュリティ義務が課される。上記の法令は、2018年1月1日に施行された。

ただし、当該法令は、一般的な規制の枠組みを定めるものであり、包括的かつ詳細な規制法が採用されることになる。FSTECは、2017年11月25日付大統領令（第596号）により重要なインフラのセキュリティ分野における国家当局に任命された。

未成年者の個人データの処理に関する法案

2017年11月3日連邦法第305068-7号「連邦法「個人データについて」の改正について」の法案が国家院（下院）に提出された²⁰。

本法案は、未成年者（18歳未満）の個人データの処理の問題を解決することを目的とする。

具体的には、改正案によると、未成年のデータ対象者の個人データの処理に対する同意は、その法定代理人により付与されるものとされている。

原則的に、個人データはセンシティブ個人データに帰属するため、対応する制約的な規制が適用される（個人情報法第10条に定める。）。

なお、14歳になったデータ対象者で、法律に基づき雇用される者は、その雇用活動に関連して個人データ処理が行われる場合、自ら同意を付与することができる。

② 個人情報に関連した主要な裁判例

LinkedIn 事件—2016年11月10日付モスクワ市裁判所決定（事件番号33-38783/16号）²¹

2016年11月、人気のソーシャル・ネットワーキング・サービスであるLinkedInがロシアのユーザーに対しブロックされた際に、ローカライゼーション要件の大きかりな「テスト」が行われ、著名な外国企業に対しローカライゼーション要件を執行しようとするRoskomnadzorの意思が示された。本件の主要なポイントは以下のとおりである。

裁判所は、Roskomnadzorがロシアに事業所を有さず、ウェブサイトを通して事業を行う外国企業について、「ターゲットテスト」を用いた。かかるテストには（とりわけ）、(i)ドメインがロシアに関連しているか（.ru、.su、.рф等）、(ii)ウェブサイトのロシア語版の有無及びロシアのユーザーを取り込もうとするウェブサイトのオーナーの意思を示すその他の基準（ルール建て決済、注文品のロシアへの配送オプション等）の検査を含む。LinkedIn事件において、裁判所は、ウェブサイトのコンテンツのロシア語での展開の事実を強調し、ウェブサイトでのロシア語の広告の展開についても指摘した。

- ・ Roskomnadzorの主張は、主にLinkedInウェブサイトに掲載されていた情報に依拠するものであった。これに対して、LinkedInは、Roskomnadzorが実際のデータ処理活動に言及せず（かつこれを証明できず）、データ管理者による情報提供に依拠していること反論した。
- ・ 結果的に、裁判所は法令への違反を理由にロシアにおけるLinkedInのブロックを認めた。2018年3月時点においてLinkedInへのアクセスは依然として認められていない。
- ・

²⁰ 一切の関連書類及びタイムラインは以下のウェブサイトでご覧可能：

<http://sozd.parlament.gov.ru/bill/305068-7>

²¹ <http://mos-gorsud.ru/mgs/cases/docs/content/c364d1d9-e30c-4ffa-aabb-327c8977adab>

Double Data 対 VKontakte —事件番号 A40-18827/2017 号、2017 年 10 月 12 日付モスクワ商事裁判所決定

2017 年 1 月、ロシアのソーシャルネットワーク VKontakte のオーナーが、データベースに係る知的財産権の侵害を主張して、“Double” LLC (Double Data ソリューションのデベロッパー) 及び国家信用履歴局 (National Bureau of Credit Histories、以下「NBCH」という。) ²²を訴えた。

Double Data ソリューション (“Double” LLC が開発) は、個人のさらなるプロファイリングを目的として、ソーシャルネットワークその他の公開ソース (VKontakte を含む。) で入手可能なデータを収集することを目的としている。このソリューションは、NBCH によって使用された。この点に関して、VKontakte のオーナーは、VKontakte からの情報の収集は、自己の知的財産権の侵害に該当すると主張した。

訴訟の過程において、原告と NBCH は、友好的な合意を結び、裁判所は紛争を原告と “Double” LLC との間でのみ解決した。

モスクワ商事裁判所は、原告が自らデータベースを作成したゆえ、データベースに係る知的財産権も自己の所有に係ると証明することができなかったことを考慮し、当初の請求を棄却した。

その後、2018 年 2 月 6 日、第 9 控訴裁判所はモスクワ商事裁判所の決定を覆し、“Double” LLC の行為は違法であり、VKontakte の知的財産権の侵害を構成するとしている。

Roskomnadzor 対 Double Data —事件番号 A40-5250/2017 号：2017 年 5 月 5 日付モスクワ商事裁判所決定、2017 年 7 月 27 日付第 9 控訴裁判所決定及びモスクワ商事裁判所決定

本件は、上記と並行する紛争である。Roskomnadzor は、国家信用履歴局に対しソーシャルネットワーク (VKontakte、インスタグラム、ツイッター等) においてクライアントの情報を検索するための Double Data ソリューションの使用に関して、行政事件を提起した。

裁判所は、個人データがソーシャルネットワーク上で公開されている場合であっても、データ管理者が自由に処理可能な公に入手可能な個人データとはみなされないと述べている。

上記に基づき、裁判所は個人情報法の観点から当該行為を違法とした。

²² <https://www.biiia.com/category/company/national-bureau-of-credit-histories-russia>

II. 国際機関

1. OECD

(1) 制度概要

経済協力開発機構（OECD, Organisation for Economic Co-operation and Development）は、1961年に設立された。自由な意見交換・情報交換を通じて、経済成長、途上国支援、貿易の自由化に貢献することを目的とした国際機関である。現在、EU加盟国や米国、日本を含む35ヶ国が加盟している。

OECDの各加盟国において、長らく個人情報保護法制の指標となっていたのが、1980年9月23日に採択された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（Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data）である。この1980年採択のガイドラインは、プライバシー諸原則に関する最初の国際的合意であり、加盟国だけでなく、世界のプライバシー保護立法に大きな影響を与えてきたとされる¹²。

その後、インターネットその他の情報通信技術の発展に伴う、個人情報保護をめぐる環境の大きな変化等に対応するため、2013年7月11日にOECD理事会勧告として、ガイドラインの改正案（Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data）（以下、改正前のものと併せて「OECDプライバシーガイドライン」という。）が採択されることとなった。

改正のガイドラインは、「OECDプライバシー・フレームワーク（The OECD Privacy Framework）³」と題する書面で公表されており、これは、2013年に改定されたガイドラインに関する理事会勧告、改定版ガイドライン勧告に関する補足説明資料、当初のガイドラインに関する背景説明資料、及びプライバシー保護法の執行に係る越境協力に関する勧告等から構成される。なお、上述のとおり、OECDプライバシーガイドラインは、世界のプライバシー保護立法に大きな影響を与えてきたもので、その意義は疑いようもないところであるが、ガイドラインであるため、これらの文書は、OECD加盟国に対し、基本的には法的拘束力を持たないとされている⁴。

¹ 石井夏生利「新版 個人情報保護法の現在と未来－世界的潮流と日本の将来像－」（勁草書房、2017年）10頁

² OECDプライバシーガイドラインの30周年記念を機にOECDから公表された「The evolving privacy landscape: 30 years after the OECD Privacy Guidelines」と題する報告書においても、当該ガイドラインは、OECD加盟国のデータ保護法の発展に影響を与えてきただけでなく、APECプライバシー・フレームワークにも影響を与えてきたものであり、目覚ましい成功を収めてきたと総括されている。

³ https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

⁴ 日本の裁判において、OECDプライバシーガイドラインの法的拘束力が争われた事例もい

当該ガイドラインは、OECD から、OECD 加盟国（及び非加盟国（前文 II））に対する、データ保護に関する最低限の標準としてガイドラインを導入すべきとの勧告（前文 I）とみなされる（第 6 条）。

OECD プライバシーガイドラインの前文には以下の内容が記載されている。

- ・ プライバシーの基本的価値 (fundamental values of privacy)、個人の自由 (individual liberties) 及び情報の世界的で自由な流れ (global free flow of information) を促進及び保護する加盟国の共通の利益
- ・ プライバシー・フレームワークにおける相互運用の改良の必要性、及びプライバシー執行機関 (privacy enforcement authorities) の越境協力 (cross-border co-operation) の強化の必要性
- ・ プライバシー保護のためのポリシー及び管理措置の展開におけるリスク評価の重要性
- ・ 加盟国間の自由な情報の流れの更なる促進、並びに加盟国間の経済的及び社会的関係の発展に対する不当な妨害 (unjustified obstacles) の回避に関する決定

(2) 個人情報の定義

第 1 条 b) 項では、「個人データ」を、「識別された (identified) 又は識別され得る (identifiable) 個人 (データ主体) に関するあらゆる情報」と定義している。

センシティブデータは、OECD プライバシーガイドラインでは定義されていない。一方で、OECD プライバシーガイドラインに関する当初の背景説明資料⁵（以下「当初説明資料」という。）では、センシティブデータは、加盟国それぞれの伝統及び考えによって、加盟国毎に定義されると記載されている⁶。

(3) 主な規制・権利の内容

第二部 - 国内適用における基本原則 (Basic Principles of National Application)（第 7 条乃至第 14 条）において主要な規定が定められている。個人データに関する 8 つの原則が、以下のとおり定義されている。

- ・ 第 7 条 収集制限の原則 (Collection Limitation Principle)
- ・ 第 8 条 データ内容の原則 (Data Quality Principle)

くつか存在するが（東京高判平成 19 年 8 月 28 日判タ 1264 号 299 頁、東京地判平成 19 年 2 月 8 日判時 1964 号 113 頁、東京地判平成 18 年 3 月 24 日判時 1938 号 37 頁等）、明確に OECD プライバシーガイドラインの法的拘束力を認めた裁判例はないものと思われる（板倉陽一郎「OECD 改正ガイドライン」個人情報保護における国際的枠組みの改正動向調査報告書（消費者庁、平成 26 年 3 月 28 日）158 頁以下参照）。

⁵ Original Explanatory Memorandum to the OECD Privacy Guidelines (1980)

⁶ OECD、The OECD Privacy Framework、2013、53 頁

- ・ 第9条 目的明確化の原則 (Purpose Specification Principle)
- ・ 第10条 利用制限の原則 (Use Limitation Principle)
- ・ 第11条 安全保護の原則 (Security Safeguards Principle)
- ・ 第12条 公開の原則 (Openness Principle)
- ・ 第13条 個人参加の原則 (Individual Participation Principle)
- ・ 第14条 責任の原則 (Accountability Principle)

(4) 監督・登録制度

OECD プライバシーガイドラインは、特定の監督制度について定めていない。監督及び登録のスキームは加盟国毎に個別に取り扱われる。

第19条 c)項には、加盟国は、自己の権利を有効に行使し、客観的、公平かつ一貫した判断を下すために必要なガバナンス、リソース及び技術的専門性を有するプライバシー執行機関を設置し、これを維持するものと記載されている。

(5) 漏えい等事案発生時の本人及び監督機関等への報告義務

OECD プライバシーガイドラインでは、重大なセキュリティ違反があった場合、それぞれの監督機関に対し、及びデータ主体に悪影響を及ぼす可能性が高い場合には、個別のデータ主体に対し報告を行う義務について定めている。

第15条 a)項 v. では、データ管理者は、問い合わせへの回答及び問題の対処に関する計画を含むプライバシー管理プログラムを整備するよう規定されている。

さらに、第15条 c)項には、データ管理者は、個人データに影響を及ぼす重大なセキュリティ違反があった場合、必要に応じてプライバシー執行機関又はその他の関連機関に対し通知を行うよう規定されている。違反が、データ主体に悪影響 (adversely affect) を及ぼす可能性が高い場合、データ管理者は影響を受けたデータ主体に通知すべきであるとされている。

「プライバシー執行機関」とは、第1条 d)項において、各加盟国が決定する、プライバシー保護法の施行に責任を負い、執行手続きにつき調査し、これを追及する権利を有する公共機関 (public body) と定義されている。

また、「悪影響」とは、経済的損失だけでなく、それ以外の要素も含めて幅広く解釈されるべきである一方、通知義務自体は、さらなる損害の発生を予防又は軽減できるように柔軟であるべきともされる。例えば、データ主体へのリスクを増大させ、又は法執行調査を妨げるような場合には、データ主体への通知が不適切な場合もあり得ることとなる⁷。

⁷ 前掲・石井 28 頁

(6) 安全保護措置に関する規定

OECD プライバシーガイドラインの第 11 条では、安全保護の原則 (Security Safeguards Principle) が定められており、個人データは、データの損失 (loss) 又は不正アクセス (unauthorised access)、破壊 (destruction)、使用 (use)、修正 (modification) 又は開示 (disclosure) に対する合理的なセキュリティ管理措置により保護されなければならないと記載されている。

当初説明資料では、安全保護の原則において、第 11 条は、例えば、人的、物理的、組織的及び情報に関する措置を含む非常に広範な適用範囲を有すると記載されている⁸。

安全保護措置には、物理的措置 (physical measures) (例えば、ドアの施錠及び ID カード)、組織的措置 (organisational measures) (データへのアクセスに関する権限レベル) 及び特にコンピュータシステムにおいては情報措置 (informational measures) (暗号化 (enciphering) 並びに異常な活動 (unusual activities) 及びこれに対するレスポンスといった脅威の監視等) が含まれる。組織的措置の種類には、データ処理者の守秘義務が含まれることが強調されている。第 11 条は、広範な適用範囲を有する。規定に記載される例は、ある程度重複している (例えば、アクセス/開示)。データの「損失」とは、偶発的なデータの消去、データ記憶装置の破壊 (それによるデータの破壊) 及びデータ記憶装置の盗難を含む。「修正された」という用語には、データの不正入力 (unauthorised input) が含まれ、「使用」には、不正な複製 (unauthorised copying) が含まれるものと解釈される。

(7) 適用範囲、適用除外内容

OECD プライバシーガイドラインの適用範囲及び例外は、第 2 条乃至第 6 条に定義されている。

第 2 条では、一般的範囲が以下のとおり定められている。

本ガイドラインは、公的又は民間部門を問わず、処理方法、又はその性質若しくは使用される状況により、プライバシー及び個人の自由に対しリスクをもたらす個人データに適用される。

OECD プライバシーガイドラインの対象は加盟国であり、加盟国はこれを自国の法制度に導入することが推奨される。これについては、第 19 条において、国内的実現に関する原則として詳細に定められている。

⁸ OECD, The OECD Privacy Framework, 2013, 57 頁

本ガイドラインの導入に際し、加盟国は、以下に従う。

- a) 他国の政府機関との協調的アプローチを反映した国家的プライバシー戦略 (national privacy strategies) を発展させる。
- b) プライバシー保護法を整備する。
- c) 自己の権利を有効に行使し、客観的、公平かつ一貫した決定を下すために必要なガバナンス、リソース及び技術的専門性を有するプライバシー執行機関を設立し、これを維持する。
- d) 行動規範その他の形式を問わず、自主規制を推奨及び支援する。
- e) 個人が自己の権利を行行使するための合理的手段について定める。
- f) プライバシー保護法の遵守を怠った場合の適切な制裁及び救済措置を定める。
- g) 補完措置 (complementary measures) (教育、意識改革、スキル開発及びプライバシー保護を助ける技術的措置の促進) の採用を検討する。
- h) データ管理者以外の当事者の役割を、その個別の役割に適切な方法で検討する。
- i) データ主体に対し不公正な差別が存在しないことを保証する。

OECD プライバシーガイドラインは最低限の基準とみなされ、プライバシー及び個人の自由の保護に関する追加措置が補完される可能性があり、これによって個人データの国際流通に影響が及ぶ場合がある (第 6 条)。

異なる保護措置が、個人データの性質並びにその収集、保有、処理及び提供の状況に応じて、違う種類の個人データに適用される場合がある (第 3 条 a) 項)。第 3 条 b) 項では、OECD プライバシーガイドラインの解釈において、基本的権利である、表現の自由を不当に制限するべきではないことが規定されている。

第 4 条では、加盟国が導入する例外について、以下のとおり定めている。

本ガイドラインの例外 (国家主権、国家安全保障及び公序良俗) に関連するものを含む) は、以下のとおりとする。

- a) 可能な限り少なくする。
- b) 公知にする。

(8) 小規模事業者の取扱い

OECD プライバシーガイドラインでは、データ管理者の規模を考慮している。大規模データ管理者は、小規模又は中規模データ管理者よりも厳しいコンプライアンス手法を導入しなければならない。

第 15 条 a) 項 ii) では、データ管理者は、その経営の構造、規模、ボリューム及びセンシティブティに適合したプライバシー管理プログラム (privacy management programme) を

整備するものと規定されている。

改定版 OECD プライバシーガイドラインに対する補足説明資料⁹では、第 15 条 a) 項(ii) において、プライバシー管理プログラムの整備に際しては、柔軟性が必要と強調されている、と記載されている¹⁰。例えば、多数の管轄区域に拠点を有する大規模データ管理者は、単一拠点のみを有する小規模又は中規模データ管理者とは異なった内部監督メカニズム (internal oversight mechanisms) を検討する必要がある。

(9) 国際的な情報移転に関する規定

第 16 条乃至第 18 条は、国境を越えた個人データの自由な流れ及びその法的制約について定めている。

データ管理者は、データの所在にかかわらず、その管理下にある個人データにつき引き続き責任を負う (第 16 条)。

国家間の個人データの国際流通は、相手国が実質的に OECD プライバシーガイドラインを遵守し、又は十分な管理措置が存在する場合 (OECD プライバシーガイドラインに沿った継続的な保護レベルを確保するため、有効な執行メカニズム (effective enforcement mechanisms) 及び適切な措置が、データ管理者により整備されている場合を含む。) には制限されるべきではない (第 17 条)。

個人データの国際流通に対する制限は、データのセンシティブリティ、並びに処理の目的及び状況を考慮した上で、顕在するリスクに見合うものであるべきである (第 18 条)。

「個人データの国際流通」 (Transborder flows of personal data) は、第 1 条 e) 項において、国境を越えた個人データの移動と定義されている。

さらに、第 20 条乃至第 23 条は、国際協力及び相互運用性 (以下参照) について定めている。

(10) 越境執行協力

① 制度の名称、概要、採択・施行時期

OECD プライバシーガイドラインには、第 20 条乃至第 23 条に国際協力及び相互運用性に関する規定が含まれている。さらに、2007 年 6 月 12 日に OECD は、プライバシー保護法の執行に係る越境協力に関する勧告 (Recommendation of the Council on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy) (以下「OECD 勧告」とい

⁹ Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)

¹⁰ OECD、The OECD Privacy Framework、2013、24 頁

う。)を採択した。

OECD 勧告の第 2 条乃至第 6 条は、その目的及び範囲について、以下のとおり定めている。

2. 本 OECD 勧告は、情報又は個人の所在にかかわらず、個人情報保護の課題に取り組むために、他国のプライバシー執行機関 (Privacy Enforcement Authorities) との国際協力を発展させることを意図している。本 OECD 勧告では、加盟国が、プライバシー保護の有効性を向上させるために必要な場合には、自国の執行制度及び法律 (enforcement systems and laws) を改善する旨の誓約 (commitment) が示されている。
3. 本 OECD 勧告の主な焦点は、プライバシー執行機関の権限及び執行活動である。但し、刑法執行機関 (criminal law enforcement authorities)、公的及び民間組織のプライバシー責任者並びに民間部門監督グループ (private sector oversight groups) 等の他の事業者も、国境を越えたプライバシーの有効な保護に重要な役割を担っていることが認識されており、これらの事業者との適切な協力が推奨される。
4. 越境執行協力が複雑かつ資源集約的 (resource-intensive) であるとする、本 OECD 勧告は、プライバシー保護法の違反という性質的に最も深刻な違反に関する協力を焦点を当てている。検討すべき重要事実には、違反の性質、損害又はリスクの大きさ及び影響を受けた者の人数が含まれる。
5. 本 OECD 勧告は、主として民間部門について規定するプライバシー保護法の施行における協力を促進することを目指しているが、加盟国は、公的部門における個人データの処理に関する事項において協力することも希望している。
6. 本 OECD 勧告は、国家主権 (national sovereignty)、国家安全保障 (national security) 及び公序良俗 (public policy) に関連する、政府の活動を妨げることを意図していない。

② 適用範囲 (対象国及び拘束の程度)

適用範囲は、OECD 勧告の第 2 条乃至第 6 条 (上記①を参照) に規定されているが、OECD プライバシーガイドラインがデータ保護の最低水準 (OECD プライバシーガイドライン第 6 条) を勧告しているにすぎないのと同様に、OECD 勧告は、OECD 加盟国に対し、何ら拘束力を持たない。

③ 内容

OECD 勧告は、加盟国に対し、協力を実現するための措置を構築し (第 III 部)、加盟国のプライバシー執行機関による当該国際協力を促進する (第 IV 部) ことを要請している。

「プライバシー執行機関」は、第1条 b)項において、プライバシー保護法の施行に責任を負い、調査を実施し又は施行手続を達成させる権限を有する、各加盟国により決定される公共機関 (any public body) と定義されている。

第 III 部では、プライバシー執行機関による海外及びその他の国内のプライバシー執行機関との協力を許可する有効な国内の枠組みの導入について扱っている (第 7 条)。個人がプライバシー保護法違反によって損害を受けた場合に、どこにいたとしても利用可能な救済手段を改善するための方法を考慮すべきことなども規定されている (第 9 条)。この枠組みは、プライバシー執行機関が、自国で発生し又はその域内に影響を及ぼすプライバシー保護法の違反を防止し、これに対し適時に行動するために必要な権限を有していることが保証されることを前提に導入される (第 11 条)。さらに、協調性 (ability to co-operate) を改善するため、第 12 条では、加盟国が要請に基づき、かつ適切な管理措置に従って、以下の事項により、海外のプライバシー執行機関と協力するため、そのプライバシー執行機関の能力改善のための措置を講じるものと規定している。

- a) プライバシー執行機関に対し、プライバシー保護法の違反の可能性に関し、外国機関と関連情報を共有するメカニズムを提供する。
- b) プライバシー執行機関が、プライバシー保護法の違反の可能性に関連して外国の機関に支援 (とりわけ、いずれかの者からの情報入手、文書又は記録の入手、又は関与する組織若しくは者、又は事柄の配置又は特定に関する支援) を提供することを可能とする。

第 IV 部は、国際協力について扱っている。第 13 条には、加盟国及びそのプライバシー執行機関は、OECD 勧告及び国内法の規定に従い、プライバシー保護法の施行により生じる国境を越えた問題に対処するため、互いに協力すると定められている。当該協力は、適切な二国間又は多国間の執行の取り決めにより促進することができる。

OECD 勧告は、相互支援に関する更なる勧告 (第 14 条乃至第 18 条)、相互支援を支持する集団的イニシアティブ (collective initiatives) への関与 (第 19 条乃至第 21 条) 及び他の機関及び利害関係人との協力 (第 22 条) について定めている。

相互支援 (第 14 条乃至第 18 条) では、他国のプライバシー執行機関に支援を要請する場合の考慮事項 (利用される情報の目的の特定等) や、プライバシー執行機関は、勧告の範囲外である等の一定の場合には、支援要請を断ったり、条件を付けたりすることができること、支援を行う場合の留意事項 (非公開情報の利用等) などが記載されている。

相互支援を支持する集団的イニシアティブへの関与 (第 19 条乃至第 21 条) では、加盟国は、相互支援及び協力のため、国内の連絡先を指定すること、プライバシー執行機関は、プライバシー方執行の結果に関する情報を共有すべきであること、加盟国は、プライバシー執行機関の情報ネットワークの確立を進めるべきことなどが記載されている。

他の機関及び利害関係人との協力 (第 22 条) では、加盟国は、刑法執行機関、公的及び

民間組織のプライバシー責任者又は市民社会（civil society）及び事業者（business）等との協力を推奨すべきことが記載されている。

④ Global Privacy Enforcement Network (GPEN)

OECD 勧告では、加盟国に対し、プライバシー執行機関の非公式なネットワークの設立を促進することを求めており、これを受けて、Global Privacy Enforcement Network（以下「GPEN」という。）が2010年3月に設置された。GPENは、プライバシー法執行協力の実務的側面を議論すること、越境執行問題に対処するための最適なプラクティスを共有すること、共有された執行の優先事項を展開させること、並びに共同執行イニシアティブ及び意識向上キャンペーンをサポートすることを目的としている。日本の個人情報保護委員会は2016年5月に正式に参加承認を受けた。

2012年6月に採択されたアクションプラン¹¹（2013年1月に一部改定）の綱領（Statement of Mission）では、GPENは世界各国のプライバシー執行機関をつなぎ、プライバシー保護法の越境執行協力の促進及びサポートをすることが謳われている。協力の促進は、主に、（1）関連する問題、傾向及び経験についての情報交換、（2）トレーニング機会の設置、並びに執行のノウハウ、専門知識及び実務の共有、（3）プライバシー執行の役割を担う機関との協議の促進、並びに（4）二者間又は複数者間の協力を有益なプロセス又はメカニズムの設置、維持及びサポートを行うこと等によるものとされている。

なお、このアクションプランは参加者による、又は参加者間におけるいかなる法的拘束力ももたらすものではなく、また、このアクションプランに基づく協力は、参加者の国内法及び参加者に適用される国際的義務に従うものとされている。

（11）最近の議論の動向

① データ駆動型イノベーションに関する報告書

2013年に実施されたガイドラインの改定は、1980年の当初の採択からの最初の修正であった。国際的に合意された最初のプライバシー原則であり、技術的に中立（technology-neutral）であったが、技術の進歩及び個人データ利用状況の変化により、2013年の改定が必要となった。

2015年、OECDは「データ駆動型イノベーション：成長と幸福のためのビッグデータ」（Data-Driven Innovation: Big Data for Growth and Wellbeing）と題する報告書をリリースした。これには、データ駆動型イノベーションのためのプライバシー保護に関する章

¹¹ Action Plan for the Global Privacy Enforcement Network (GPEN)
<https://www.privacyenforcement.net/public/activities>

が含まれており（216 頁-227 頁）、ガイドラインへの多くの参照が含まれている。報告書は、以下のようなデータ駆動型イノベーション（DDI）及びビッグデータに関して生じる懸念を扱っている。

- ・ 包括的データ収集（comprehensive data collection）（ソーシャルメディア・プラットフォーム、検索エンジン、インターネットサービス・プロバイダー（ISPs）又は金融サービスプロバイダー及び携帯端末を通じた位置情報又はヘルスデータからの広範な経済的及び社会的データを含む。）
- ・ 大容量データの保存スペースの増加。これにより当該データの盗難又は不正使用のリスクが高まる可能性がある。
- ・ 事業者間のパターン、相関関係及び相互作用（correlations and interaction）を明らかにすることができるデータ解析。IoT は、容易な分析が可能であり、行動パターンを創造することができ、例えばカスタマイズ広告（tailored advertising）に使用されるデバイスにより、より多くのデータが作り出されるリスクを高める。
- ・ データ駆動型意思決定（data driven decision making）、プロファイリング及び差別化の可能性（possible discriminatory outcomes）。例えば、消費者のプロファイルにより差別化された価格決定（pricing discrimination）、又は信用レポートシステム若しくは健康データにより差別化された保険、雇用若しくはクレジット（insurance, employment or credit discrimination）

当該報告書では、当該挑戦は、透明性、個人のアクセス及び権限委譲の見直し並びに責任を持った個人データの使用を促進することによって対応可能であると記載している。ガイドラインは、一般的に、一般的な枠組みとみなされるが、現代のデータ利用の規模を鑑みて、その適用に様々な挑戦が行われている。主な挑戦は、管理者にデータを提供するデータ主体の積極的役割（最近では、時にはデータ主体が認識していない場合でも、膨大な個人データが受け身的に収集されることにより、更なる挑戦となっている。）をガイドラインが引き受けている点である。

当該報告書では、データ主体が引き続き、自己の個人データ、プライバシー通知、プライバシー強化技術（privacy enhancing technologies）を管理するデータポータビリティ（data portability）等の透明性イニシアティブ（transparency initiatives）の採用が推奨されている。

② OECD セキュリティガイドライン

ア はじめに

OECD セキュリティガイドライン（OECD security guidelines）は、当初 1992 年に「情

報システムのセキュリティのためのガイドライン」(Guidelines for the Security of Information Systems)として提出された。当該当初ガイドラインは、2002年に「情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて」¹²(以下「2002年セキュリティガイドライン」という。)に取って代われ、さらに2015年9月、現行のセキュリティの枠組みである「経済的社会的繁栄のためのデジタルセキュリティ・リスクマネジメントに関する理事会勧告」(Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity)¹³に取って代わられた。

現行のセキュリティの枠組みである経済的社会的繁栄のためのデジタルセキュリティ・リスクマネジメントに関する理事会勧告¹⁴は、勧告(5乃至15頁、以下「本勧告」という。)及び勧告付属書(17乃至69頁)から構成される。当該付属書は、「性質上説明的かつ事例的なものであり、本勧告の一部を構成しない。」(17頁)とされている。

本勧告の採択により、技術的なものだけでなく、官民組織の経済的かつ社会的な目的に対処するリスクマネジメントに焦点が当てられている。「技術的解決策を必要とする技術上の問題として取り扱われるのではなく、デジタルリスクは、経済的リスクとしてアプローチされるべきであり、それゆえ、組織のリスクマネジメント全般及び意思決定プロセスの不可欠な部分とすべき」であり、さらに、「デジタルセキュリティ対策は、他者の利益を考慮して策定し、直面するリスクに対し適切かつ相応しいものであり、保護対象となる経済的・社会的活動を弱体化させるものであってはならない。」と述べられている(4頁)。

イ 原則

本勧告は、最初に、「8つの首尾一貫した、相互関連・相互依存する補完的な高水準の原則の枠組み」を定めている(4頁)。これらは、4つの一般原則(General Principles)(1.-4.)及び4つの運用原則(Operational Principles)(5.-8.)に区分することができる。本原則とは、以下のとおりである(9頁以下)。

1. 認識、スキル及び権限付与(Awareness, skills and empowerment)

「全利害関係者は、デジタルセキュリティリスク及びその管理方法を理解するべきである。」

2. 責任(Responsibility)

「全利害関係者は、デジタルセキュリティリスクの管理責任を負うべきである。」

¹²<https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm>

¹³ <https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm>

¹⁴ OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: <http://dx.doi.org/10.1787/9789264245471-en>

3. 人権及び基本的価値 (Human rights and fundamental values)

「全利害関係者は、透明かつ人権及び基本的価値と調和する方法でデジタルセキュリティリスクを管理するべきである。」

4. 協力 (Co-operation)

「全利害関係者は、国境を超える場合を含め、協力するべきである。」

5. リスクアセスメント及び取扱いサイクル (Risk assessment and treatment cycle)

「指導者及び意思決定者は、デジタルセキュリティリスクが継続的リスクアセスメントに基づき取り扱われるよう確保するべきである。」

6. セキュリティ対策 (Security Measures)

「指導者及び意思決定者は、セキュリティ対策がリスクに対し適切かつ相応しいものであるよう確保するべきである。」

7. イノベーション (Innovation)

「指導者及び意思決定者は、イノベーションが考慮されるよう確保するべきである。」

8. 準備及び継続性 (Preparedness and continuity)

「指導者及び意思決定者は、準備及び継続計画が採用されるよう確保するべきである。」

ウ 国家戦略

次に、本勧告は、その実施に関する「国家戦略」(National Strategies) (11 頁以下) について定めている。要点は、以下のとおりである。

- A. デジタルセキュリティ・リスクマネージメントに関する国家戦略は、本原則と一致するとともに、全利害関係者が経済的・社会的活動に対するデジタルセキュリティリスクを管理し、デジタル環境に対する信頼と信用を促進するための状況を創出するべきである。
- B. 国家戦略は、政府が以下の各号のようにできる対策を含むべきである。
 1. 模範を示して指導すること。
 2. 国際協力及び相互支援を強化すること。
 3. その他の利害関係者と関わりを持つこと。
 4. 全利害関係者がデジタルセキュリティ・リスクマネージメントにおいて協調するための状況を創出すること。

エ OECD プライバシーガイドラインとの相互関連性

2002 年セキュリティガイドラインは、既に OECD プライバシーガイドラインと合致したものであったが (2002 年セキュリティガイドライン 9 頁、13 頁)、2015 年の本勧告でも、「デジタルセキュリティ・リスクマネージメントは、OECD プライバシーガイドラインにおける

『安全保護の原則』を実施するための堅固な基礎を提供するものであり、より一般的には、本勧告及び OECD プライバシーガイドラインは、相互に補強している。」とされている（7 頁）。

2. APEC

(1) APECにおける個人情報保護の取組みの概要

アジア太平洋経済協力 (Asia-Pacific Economic Cooperation, APEC) は、1989年に発足したアジア太平洋地域の21のエコノミー¹が参加する経済協力の枠組みである。APECの活動の特色は、「協調的自主的な行動」(APECメンバーを法的に拘束せず、各メンバーの自発的な行動により取組みを推進すること)と「開かれた地域協力」(自由で開かれた貿易・投資というAPECの活動の成果を域内だけでなく、域外の国・地域とも共有すること)である²。APECは、アジア太平洋地域の持続可能な成長と繁栄を目的として、貿易・投資の自由化、ビジネスの円滑化、人間の安全保障、経済・技術協力等の多彩な協力活動に取り組んでおり、個人情報保護の分野に関しても、その一環として、APECの電子商取引運営グループ (Electronic Commerce Steering Group, ECSG)³及びその下部組織であるデータプライバシーサブグループ (Data Privacy Subgroup, DPS) が中心となって議論がなされている⁴。

APECにおける個人情報保護への取組みは、1998年の閣僚会議で合意された「電子商取引に関する行動のためのAPECの計画」(APEC Blueprint for Action on Electronic Commerce)に始まる。その後、2004年10月に、APEC域内における個人情報保護に関する基本原則を定めたAPECプライバシー・フレームワーク (APEC Privacy Framework) (以下「APECプライバシー・フレームワーク」という。)が策定され、メンバー・エコノミーの閣僚会議で承認された。2007年9月には、APEC域内における責任ある個人情報の越境移転を達成する

¹ APECでは、APECメンバーの国と地域をエコノミーと呼ぶ。現在、APECに参加している21のエコノミーは、オーストラリア、ブルネイ・ダルサラーム、カナダ、チリ、中華人民共和国、香港、インドネシア、日本、大韓民国、マレーシア、メキシコ、ニュージーランド、パプアニューギニア、ペルー、フィリピン、ロシア、シンガポール、中華民国台北、タイ、米国及びベトナムである。

² 外務省「APECの概要」、<http://www.mofa.go.jp/mofaj/gaiko/apec/soshiki/gaiyo.html> (平成30年3月12日閲覧)。

³ APEC高級実務者会合の下部組織で、1998年「電子商取引タスクフォース」が設立、1999年に現在の組織に改編。

⁴ Electronic Commerce Steering Group, <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group> (平成30年3月12日閲覧)。「電子商取引運営グループ」に属することからも分かるように、APECにおける個人情報保護は、基本的に商取引の文脈であって、民間分野における取扱いのみが想定されている。APECの会合で用いられた文書はThe Meeting Document Database (MDDb) (<http://mddb.apec.org/Pages/default.aspx>)で公表されており、同データベースによると、2017年8月の第36回ECSGの会議資料が最新である。また、ECSGにはDPSの他にペーパーレス・トレーディング・サブグループ (Paperless Trading Subgroup, PTS) が設置されているが、2016年8月の第26回会合を最後に開催されていない。

ための計画として、APEC データ・プライバシー・パスファインダー計画 (APEC Data Privacy Pathfinder) (以下「APEC パスファインダー計画」という。) が採択された。

その後、2009 年 11 月には、APEC 域内におけるプライバシー執行機関間における執行協力の枠組を提供する、APEC 越境プライバシー執行協定 (APEC Cross-border Privacy Enforcement Agreement, CPEA) が承認された (2010 年 7 月運用開始)。さらに、2011 年 11 月、APEC 首脳宣言によって、APEC 越境プライバシールール・システム (APEC Cross Border Privacy Rules System, CBPRs) (以下「CBPR システム」という。) の実施が示された。CBPR システムは、個人情報管理者 (Controllers) である事業者の越境個人情報保護に係る取組みについて、APEC プライバシー・フレームワークへの適合性を認証することで、越境データの流通と効果的な個人情報の保護との調和を図るための制度である。加えて、2015 年 8 月、APEC 域内における個人情報処理者 (Processors) である事業者に対する認定システムとして、取扱者のための APEC プライバシー承認制度⁵ (APEC Privacy Recognition for Processors System, PRPs) (以下「PRP システム」という。) の運用が開始されている。

本報告書では、これらの APEC における個人情報保護の取組みにつき、(2)APEC プライバシー・フレームワーク、(3)CPEA、(4)CBPR システム、(5)PRP システムの順に概要を述べ、(6)において、最近の議論の動向について触れる。

(2) APEC プライバシー・フレームワーク

① 採択・施行時期・概要

APEC プライバシー・フレームワークは、APEC 域内における情報流通に対する障害を避けつつ、効果的な個人情報保護への取組みを促進することが重要であるとの認識のもと、「情報の流れに対する障壁を回避する効果的なプライバシー保護の発展の重要性を認識し」

(recognizing the importance of the development of effective privacy protections that avoid barriers to information flows) て⁶、2003 年から整備され、2004 年 11 月の閣僚会議で承認された⁷。そして、(6)最近の議論の動向において後述するように、2016 年 11 月に、アップデートされた APEC プライバシー・フレームワーク (Updates to the APEC Privacy Framework)⁸ (以下「改訂 APEC プライバシー・フレームワーク」という。) が閣僚会議に

⁵ 石井夏生利『新版個人情報保護法の現在と未来』(勁草書房、2017 年) 374 頁

⁶ APEC 域内のプライバシー法は、その形態も、執行の方法も様々であることから、APEC プライバシー・フレームワークは、例えば EU データ保護指令が指令に適合した措置 (主としてデータ保護法の制定) を要求するように各エコノミーを縛ることをしていない。2016 年にアップデートされた APEC プライバシー・フレームワークにおいても、“Privacy Laws in APEC member economies come in a variety of forms.” とされている (“Updates to the APEC Privacy Framework” (2016/CSOM/012app17) p.8)。

⁷ APEC プライバシー・フレームワーク第 4 章の国際実施の部分は、2005 年に承認。

⁸ “Updates to the APEC Privacy Framework” (2016/CSOM/012app17),

において承認されている。

なお、本(2)においては、2004年の採択当時のAPEC プライバシー・フレームワークについて説明し、必要に応じて、改訂APEC プライバシー・フレームワークに言及するものとする。

② 目的規定の有無、その内容

APEC プライバシー・フレームワークには、その目的を明確に述べる条項は含まれていないが、「第1章 序文」において、「APEC エコノミーは、APEC 域内における適正な情報プライバシーの保護の発展を促進させ、自由な情報の流通を保証する重要な手段」としてAPEC プライバシー・フレームワークを承認し（第4条）、以下の認識の重要性から展開されたとしている（第8条）⁹。

- ア 個人情報のための適切なプライバシー保護、特に、個人情報に関する好ましくない侵害や誤用をもたらす有害な結果からの保護を展開させること。
- イ 情報の自由な流通が、先進国及び発展途上国の双方の市場経済において、経済的及び社会的成長を維持させるために不可欠であることを認識すること。
- ウ APEC エコノミーにおいて、データを収集し、アクセスし、利用し、又は取扱う国際的な事業者が、個人情報のグローバルなアクセス及び利用を当該事業者内で行うための統一的なアプローチを展開・実践できるようにすること。
- エ 執行機関が情報プライバシー保護のために自らの使命を果たせるようにすること。
- オ 情報プライバシーを促進しかつ執行し、APEC エコノミー間及びその取引相手との間での継続的な情報流通を維持するための国際的仕組みを発展させること。

③ 個人情報の定義、機微情報の定義

APEC プライバシー・フレームワークは、「第2章 適用範囲」のうち「定義」の項におい

http://mddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf

⁹ 改訂APEC プライバシー・フレームワークにおいては、さらに、事業者が管理する個人情報へのその責任を促進すること、APEC プライバシー・フレームワーク、CPEA やCBPR システムのようなその実施制度及び他の法域におけるプライバシーの取決めの相互運用を促進することの重要性が加えられている（改訂APEC プライバシー・フレームワーク 第8条）。

て、「個人情報 (Personal Information) 」を「識別された又は識別可能な個人に関するあらゆる情報」と定義している (第 9 条)。

機微情報については、定義はされていないが、「第 3 章 APEC 情報プライバシー諸原則」の「安全保護措置」の項の中で、情報の機微性に応じた安全保護措置を講ずべきとしており、機微情報についての考慮が見られる (第 22 条)¹⁰。

④ 主な規制・権利の内容 (APEC 情報プライバシー諸原則及び実施指針)

APEC プライバシー・フレームワークは、以下の 4 つのパートから構成されている。

第 1 章 序文	(Part I. Preamble)
第 2 章 適用範囲	(Part II. Scope)
第 3 章 APEC 情報プライバシー諸原則	(Part III. APEC information privacy principles)
第 4 章 実施	(Part IV. Implementation)

そして、APEC プライバシー・フレームワークの具体的内容は、「第 3 章 APEC 情報プライバシー諸原則」及び「第 4 章 実施」において定められている。

ア APEC 情報プライバシー諸原則

APEC プライバシー・フレームワークでは、「第 3 章 APEC 情報プライバシー諸原則」(第 14 条乃至第 26 条)において、以下のプライバシー保護に関する 9 つの原則が定められている。これらの原則は、1980 年 OECD プライバシーガイドラインに準拠したものである。

(ア) 【第 1 原則】 損害の回避 (Preventing Harm) (第 14 条)

個人情報保護は、個人情報の不正使用の防止を図るものであること、特定の義務はかかる不正使用から生じる損害のリスクを考慮すべきであり、救済措置は、情報の収集、

¹⁰ 改訂 APEC プライバシー・フレームワークでは、このほかに、「第 4 章 実施」の「A. 国内実施のための指針」の「III. プライバシー管理プログラム (Privacy Management Programmes) 」において、プライバシー管理プログラムは、個人情報管理者が保有する個人情報の機微性に合うように調整されるべきとの指針を示し (改訂 APEC プライバシー・フレームワーク 第 44 条(a))、また、「第 4 章 実施」の「B. 国際実施のための指針」の「IV. 越境移転 (Cross-border transfers) 」において、個人情報の越境流通の制限は、情報の機微性を考慮しつつ、移転によってもたらされるリスクに比例されるべきである (改訂 APEC プライバシー・フレームワーク 第 70 条) との指針を示しており、情報の機微性に関する考慮がみられる。

使用及び移転による損害のおそれや重大性とつりあったものにすべきことを謳う原則である。自主規制の取組み、教育及び啓蒙活動、法律、規制そして執行のメカニズムを含む個人情報保護措置が取られるべきとする。

(イ) 【第2原則】 通知 (Notice) (第15条乃至第17条)

個人情報管理者 (Personal Information Controller) は、個人情報の収集の事実、収集の目的、開示される第三者の種別、個人情報管理者の名称・所在、個人情報の利用・提供の制限及び開示・訂正のための方法を含む、個人情報に関するポリシー及び体制等を、アクセス可能な方法で提供すべきとする原則である。

なお、「個人情報管理者 (Personal Information Controller)」とは、個人情報の収集、保有、取扱い及び使用を行う者又は組織を意味すると定義されている (第10条)。

(ウ) 【第3原則】 収集の制限 (Collection Limitation) (第18条)

個人情報の収集は、収集の目的の範囲に制限されるべきであり、適法かつ公正な手段で収集されるべきとする原則である。

(エ) 【第4原則】 個人情報の利用 (Uses of Personal Information) (第19条)

個人情報の利用は、原則として、収集目的及び関連する目的の遂行のためだけになされるべきであり、個人の同意がある場合、個人の要求による役務又は商品の提供のために必要な場合並びに法令等による場合にのみ例外的に目的外利用が許されるという原則である。

(オ) 【第5原則】 選択の機会 (Choice) (第20条)

個人情報の収集、利用及び開示に関して個人が選択できるために、明確で、広く知られ、簡単に理解でき、利用しやすく、求めやすい仕組みが提供されるべきとする原則である。

(カ) 【第6原則】 個人情報の正確性 (Integrity of Personal Information) (第21条)

個人情報の利用目的に必要な限度で、個人情報は、正確で、完全で、最新であるべきとの原則である。

(キ) 【第7原則】 安全保護措置 (Security Safeguards) (第22条)

個人情報管理者は、個人情報の滅失、不正アクセス、不正な破壊、利用、変更及び開示のようなリスクに対する適切な安全保護措置を整備して、個人情報の保護を図るべきとする原則である。

(ク) 【第8原則】 アクセス及び訂正 (Access and Correction) (第23条乃至第25条)

個人は、個人情報管理者が自己の個人情報を保有しているかどうかの確認を得られるべきであり、十分な本人確認の後、合理的な方法で、個人情報を伝えられるべきであり、情報の正確性について疑義がある場合には、訂正、削除等を求めることができるべきであるとする原則である。さらに、かかる個人からの要求が拒絶された場合、その理由を要求することができるべきとする。

(ケ) 【第9原則】 アカウンタビリティ (Accountability) (第26条)

個人情報管理者は、上述の(ア)から(ク)の8つの原則を実施する措置に従うことにつき責任を負うべきとの原則である。そして、個人情報が、国内外を問わず、他の者や組織に移転される場合において、個人情報管理者は、個人の同意を得るか、個人情報の受領者や組織に対して審査を行い、かかる個人情報の受領者や組織が、上述の(ア)から(ク)の原則と一致する個人情報の保護を行うことを確保する合理的な措置を取らなければならないとする。

イ APEC プライバシー・フレームワークの実施指針

APEC プライバシー・フレームワークの「第4章 実施」においては、APEC エコノミーに対し、「A. 国内実施 (A. Guidance for domestic implementation) と「B. 国際実施 ((Guidance for International implementation) 」に分けて、APEC プライバシー・フレームワークの実施のための指針を提供している。

(ア) 国内実施のための指針

「A. 国内実施のための指針」は、以下の6つの項目から構成される¹¹。

- a. プライバシー保護と情報流通の利益の最大化 (Maximizing Benefits of Privacy Protections and Information Flows)
- b. APEC プライバシー・フレームワークの実施 (Giving Effect to the APEC Privacy Framework)
- c. 国内的なプライバシー保護の教育及び普及 (Education and publicising domestic privacy protections)
- d. 公的部門及び民間部門間の協力 (Cooperation between the Public and Private Sectors)
- e. プライバシー保護違反時に行う適切な救済 (Providing for appropriate remedies in situations where privacy protections are violated)
- f. APEC プライバシー・フレームワークの国内実施を報告するための仕組み (Mechanism for Reporting Domestic Implementation of the APEC Privacy Framework)

(イ) 国際実施のための指針

「B. 国際実施のための指針」は以下の3つの項目から構成される。

- a. エコノミー間での情報共有 (Information sharing among Member Economies)
APEC エコノミー間における、プライバシー保護に重大な影響を与える事案に関する情報の交換、調査の共有すること、プライバシー保護違反の調査における多様な方法についての経験や紛争解決の規制戦略を共有すること等が推奨され (第40条、第42条等)、エコノミーは、プライバシー保護に関する越境協力及び情報共有の促進について責任を有する公的機関を指名し、他のエコノミーに対して公表すべきとの指針を示す (第43条)。

¹¹ 改訂 APEC プライバシー・フレームワークにおいても、これらの6つの指針とほぼ同様の指針が示されているが、さらに、以下の2つの指針が加えられている。

- ① プライバシー管理プログラム (Privacy Management Programmes) に関する指針 (改訂 APEC プライバシー・フレームワーク第43条乃至第45条)
- ② プライバシー保護のための技術的手段の促進 (Promotion of technical measures to protect privacy) に関する指針 (改訂 APEC プライバシー・フレームワーク第46条及び第47条) の2つが追加されている。

b. 調査及び執行における越境協力 (Cross-border Cooperation in Investigation and Enforcement)

エコノミーは、プライバシー法の執行における越境協力を促進するための協力協定及び手続の展開を考えるべきとの指針を示す(第44条)。そのうえで、プライバシー法の執行における越境協力協定には、以下の5つの側面が含まれ得ることを示す(第45条)。

- (a) 調査又はプライバシー執行事例を他のエコノミーにより指名された公的機関へ、迅速、体系的かつ効率的に通知する仕組み。
- (b) 越境プライバシーの調査及び執行の事例における協力を成功させるために必要な効果的な情報共有の仕組み。
- (c) プライバシー執行事例における調査支援のための仕組み。
- (d) 個人情報やプライバシーの違法な侵害の深刻さ等に基づき、他のエコノミーの公的機関との協力について、事例を優先する仕組み。
- (e) 協力協定に基づく情報交換に関する適切なレベルの機密性を維持するための措置。

c. 越境プライバシー・ルール の 共同 展 開 (Cooperative Development of Cross-border Privacy Rules)

越境プライバシー・ルール の 共同 展 開 の 指 針 と し て 、 以 下 が 示 さ れ て い る 。

- (a) エコノミーは、事業者が依然として国内のデータ保護の要件及びすべての適応法を遵守する責任を負うことを認識し、APEC 域内における事業者の越境プライバシー・ルールの発展及び認証・受入を支援する努力を行うであろうこと(第46条)。
- (b) 越境プライバシー・ルールを実施するために、エコノミーは、エコノミー間のかかる越境プライバシー・ルールの相互の認証・受入のための枠組又はメカニズムを発展させるために、適切な利害関係者とともに取組みへの努力を行うであろうこと(第47条)。
- (c) エコノミーは、越境プライバシー・ルール及びAPEC 域内における事業者の越境プライバシー・ルールの認証・受入の仕組みが、越境情報流通への不必要な障壁を作ることなく、責任ある越境データ移転及び効果的なプライバシー保護を促進させることを確実にすべく努力を行うべきこと(第48条)。

上述の a. 及び b. は CPEA の、 c. は CBPR システムの基礎となった。

なお、改訂 APEC プライバシー・フレームワークにおいては、CBPR システムの開始を受け、c. の越境プライバシー・ルール の 共同 展 開 の 記 載 は な く な り 、 代 わ り に 次 の 3 つ の 指 針 が 規 定 さ れ て い る 。

- (a) 越境プライバシーの枠組み (Cross-border privacy mechanisms) (改訂 APEC プライバシー・フレームワーク第 65 条乃至第 68 条)
- (b) 越境移転 (Cross-border transfers) (改訂 APEC プライバシー・フレームワーク第 69 条及び第 70 条)
- (c) プライバシー・フレームワーク間の相互運用 (Interoperability between privacy frameworks) (改訂 APEC プライバシー・フレームワーク第 71 条及び第 72 条)

⑤ 監督制度

APEC プライバシー・フレームワークにおいては、具体的な監督制度については定められていない。もっとも、「第 4 章 実施」の A. 国内実施のための指針において、参加エコノミーは、国内における APEC フレームワークの実施及びその進展について、定期的なデータプライバシーの IAP 報告 (Data Privacy Individual Action Plan) を通じて、APEC に対し報告すべきとの指針が示されている (第 39 条)。

⑥ 漏えい等事案発生時の本人及び監督機関等への報告義務

APEC プライバシー・フレームワークは、データ漏えい等事案発生時の本人及び監督機関等への報告義務、通知要件に関する具体的な規定を定めていない。

⑦ 安全保護措置に関する規定

前述したとおり、個人情報管理者は、個人情報の滅失、不正アクセス、不正な破壊、利用、変更及び開示のようなリスクに対する適切な安全保護措置を整備すべきとする安全保護措置の原則が規定されており、かかる安全保護措置は、差し迫った損害の可能性や重大性、情報の機微性や保有の状況に応じて整備されるべきとする。さらに、安全保護措置の定期的な審査及び見直しを行うべきとする (第 22 条)。

⑧ 適用範囲、適用除外内容

APEC プライバシー・フレームワークの「第 2 章 適用範囲」は、APEC プライバシー・フレームワークの原則が適用される範囲を規定する。

まず、「第 2 章 適用範囲」の「定義」の項においては、APEC プライバシー・フレームワークにおいて使用される、「個人情報管理者 (Personal Information Controller)」及び「公に入手可能な情報 (Publicly Available Information)」の定義が設けられているが、

これらの定義そのものに例外が設けられており、そのため、APEC プライバシー・フレームワークの第3章の諸原則の適用範囲が限定される。

すなわち、前述したとおり、「個人情報管理者 (Personal Information Controller) 」とは、個人情報の収集、保有、取扱い及び使用を行う者又は組織を意味するが、この概念には、他の者又は他の組織に対し、自らに代わって、個人情報の収集、保有、処理、利用、移転又は開示 (以下「収集等」という。) をするよう指示する者又は組織は含まれるが、逆に、他の者又は他の組織から指示を受けて個人情報の収集等を行う者又は組織は除外するとされる。また、個人の私的な、家族又は家族内の事柄との関係で個人情報を収集等する個人も除外される。この点、「第3章 APEC 情報プライバシー諸原則」の第2原則「通知」、第7原則「安全保護措置」及び第9原則「アカウントビリティ」は、個人情報管理者に対して適用されるものであるため、個人情報管理者の定義に含まれない者及び組織には、適用がないこととなる。

また、「公に入手可能な情報 (Publicly Available Information) 」とは、個人に関する情報であって、当該個人が意図的に公開し若しくは公開を許可したもの、又は(1)公に入手可能な政府の記録、(2)新聞雑誌報道、若しくは(3)法の要請により公に入手可能とされた情報から、適法に収集され、入手された情報をいうとされる。この公に入手可能な情報については、第2原則「通知」及び第5原則「選択」の原則から適用を除外される (第9条乃至第11条)。

さらに、「第2章 適用範囲」の「適用」の項において、APEC プライバシー・フレームワークの諸原則についての柔軟性と、諸原則の例外について定められている。すなわち、APEC プライバシー・フレームワークの諸原則は、各エコノミーの社会的、文化的、経済的及び法的バックグラウンドの違いの観点から、柔軟に実施されるべきとされる。APEC 域内のすべての法令や体制等が、個人情報の範囲を含むすべての面において一致していることは、電子商取引にとって重要ではなく、むしろ APEC エコノミーの間で両立できる情報プライバシー保護に対するアプローチの方がより国際的な商取引を促進するとする (第12条)。

また、国家主権、国家安全保障、公共の安全及び公の秩序に関連するものは諸原則の例外であるとされる。もっとも、このような諸原則の例外は、関連する例外の目的に見合う範囲に制限され、かつ、一般に公開されるか、又は法に基づくべきことが求められている (第13条)。

⑨ 小規模事業者の取扱い

APEC プライバシー・フレームワークにおいては、データ管理者の規模について具体的に考慮した規定は具体的に置かれていない。

⑩ 国際的な情報移転に関する規定

前述したとおり、APEC プライバシー・フレームワークの「第3章 APEC 情報プライバシー諸原則」の第9原則「アカウントビリティ」の項においては、個人情報、国内外を問わず、他の者や組織に移転される場合において、個人情報管理者は、個人の同意を得るか、あるいは個人情報の受領者や組織に対して審査を行い、かかる個人情報の受領者や組織が、「第3章 APEC 情報プライバシー諸原則」の第1原則から第8原則と一致する個人情報の保護を行うことを確保する合理的な措置を取らなければならないとしている。

(3) APEC 越境プライバシー執行協定 (CPEA)

① 採択・施行時期

2009年11月、CPEA¹²が、APECの閣僚会議において承認され、2010年7月から開始された。CPEAは、APEC域内におけるプライバシー執行機関 (Privacy Enforcement Authorities¹³)間のプライバシー法 (Privacy Laws) の執行における執行協力を促進させるための枠組を提供する協定である。

ここに「プライバシー執行機関 (Privacy Enforcement Authority)」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い、「プライバシー法 (Privacy Law)」とは、APECエコノミーの法及び規制であって、その執行がAPECプライバシー・フレームワークに沿う個人情報の保護の効果を有するものと定義される (第4.1条)。

前述したとおり、APECプライバシー・フレームワーク「第4章 実施」のB.国際実施のための指針は、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取決めの検討をすべきとの指針を示しており、これを受けてCPEAが承認された。これに加えて、CPEAの採択は、APECパスファインダー計画の1つの成果であり、また、2007年のOECD越境執行協力勧告が背景にあるといわれる。

CPEAへのプライバシー執行機関の参加は、後述するCBPRシステムにエコノミーが参加するための前提条件とされている。

¹² CPEAのウェブサイト

(<https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>) からCPEAの全文がダウンロードできる (平成30年3月14日現在)。また、CPEAの仮訳は、個人情報保護委員会のウェブサイトにおいて閲覧可能である

(http://www.ppc.go.jp/files/pdf/APEC_CPEA.pdf)。

¹³ 欧州ではDPA (Data Protection Authority、データ保護機関) と称されるのが通常であるが、APECではPEA (プライバシー執行機関) と称される。APECの各文書が前提とするプライバシー法の多様性によるものと思われる。

② 目的規定の有無、その内容

次の4つの項目が、CPEAの目的として掲げられている（第1条）。

- ア 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の促進。
- イ プライバシー法の執行における、プライバシー執行機関間の効果的な越境協力（事案の照会や、並行的共同的な調査又は執行行為を通じたものを含む。）を促進するメカニズムの構築。
- ウ 越境プライバシー・ルール（Cross-Border Privacy Rules）を執行する際のプライバシー執行機関の協力促進。
- エ プライバシー調査や実施における、APEC 域外のプライバシー執行機関との情報の共有及び協力の促進（CPEA と OECD 勧告に基づき発展した協力取決めのような類似の協力取決めとの緊密な連携の確保を含む。）。

なお、「越境プライバシー・ルール（Cross-Border Privacy Rules）」とは、APEC プライバシー・フレームワーク第46条乃至第48条¹⁴と同義とされる（第4.1条）。

③ 適用範囲（対象国及び拘束の程度）

現在、APEC の10のAPEC エコノミー（米国、カナダ、メキシコ、ニュージーランド、オーストラリア、日本、シンガポール、香港、フィリピン及び韓国）がCPEAに参加し、12のプライバシー執行機関¹⁵がCPEAの参加プライバシー執行機関となっている。

¹⁴ (2)④イ(イ) c. 参照。

¹⁵ CPEA のウェブサイト

(<https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>) によると、①オーストラリア情報コミッショナー事務局（The Office of the Australian Information Commissioner, OAIC）、②オーストラリア・ビクトリア州情報コミッショナー事務局（The Office of the Victorian Information Commissioner, OVIC）、③ニュージーランドプライバシーコミッショナー事務局（The New Zealand Office of the Privacy Commissioner, NZOPC）、④米国連邦取引委員会（The United States Federal Trade Commission, US FTC）、⑤香港プライバシーコミッショナー事務局（The Office of the Privacy Commissioner for Personal Data, Hong Kong, China, PCPD）、⑥カナダ連邦プライバシーコミッショナー事務局（The Office of the Privacy Commissioner of Canada, OPCC）、⑦韓国内務省（Ministry of Interior - Korea, MOI）、⑧韓国情報通信委員会（Korea Communications Commission, KCC）、⑨メキシコ連邦情報公開データ保護院（Federal Institute for Access to Information and Data Protection of Mexico）、⑩シンガポール個人データ保護委員会（Personal Data Protection Commission, Singapore, PDPC）、⑪日本国個人情報保護委員会（Personal Information Protection Commission of Japan, PPC）及び⑫フィリピン国家プライバシー

APEC エコノミーのプライバシー執行機関であれば、CPEA に参加することができ（第 2.1 条）、上述したプライバシー執行機関の定義に該当するプライバシー執行機関であれば、APEC エコノミーは、複数のプライバシー執行機関の参加を認められる（第 2.3 条）。

CPEA への参加を希望するプライバシー執行機関は、CPEA の共同運営管理者（co-Administrator）¹⁶に対して、申請者が第 4.1 条に定義された意味でのプライバシー執行機関であることが示された ECSG のエコノミー代表等による確認書とともに、通知書を送付する。そして、運営管理者が、申請者が第 4.1 条に定義された意味でのプライバシー執行機関であることの検証をし、正式に通知書を受諾した後に、プライバシー執行機関の参加が発効する（第 8.1 条）。

CPEA の性格は、「拘束力のある義務を創設すること、国際法若しくは国内法に基づく既存の義務に影響を及ぼし、又は参加エコノミーの法体系の下で義務を創設すること」（第 6.2 条(i)）や、「CPEA への参加プライバシー執行機関の主権や法域の範囲を超える義務や期待を創設すること」（第 6.2 条(v)）を意図するものではないとされている。

④ 内容

CPEA は、APEC エコノミー間での、越境プライバシー執行における協力の実践的な多国間のメカニズムを提供するものであるが、具体的には、プライバシー違反が疑われるような事案が発生した場合において、プライバシー執行機関が、任意ベースで、情報を共有し、一定の方法で支援を要請¹⁷又はこれを提供する枠組みを設定している（第 2.1 条）。

例えば、日本の事業者 A が、他の APEC エコノミーの事業者 B に対して個人情報の取扱いの委託をしている場合において、個人情報の漏えいが行われているなどのプライバシー違反が疑われる事案が発生したとする。このような事案におけるプライバシー違反の調査の過程において、日本のプライバシー執行機関は、CPEA の枠組みに基づき、プライバシー違反の証拠を得るため、あるいは、調査対象の事業者 B の協力を求めるために、他のエコノミーのコンタクト・ポイントに対し、支援を要請でき、要請を受けた他のエコノミーは、その裁量に基づき、支援を提供する。逆に、他のエコノミーの事業者 C が日本の事業者 D

委員会（The National Privacy Commission - Philippines, NPC）の 12 機関である（平成 30 年 3 月 12 日現在）。日本は個人情報保護法の平成 27 年改正以前は主務大臣（省庁）全て（復興庁設立後は復興庁を含む）が参加機関となっていたが、主務大臣制の廃止に伴って個人情報保護委員会が参加機関となっている。

¹⁶ ECSG によって指定された、(i)APEC 事務局、(ii)プライバシー執行機関又は(iii)APEC 事務局及びプライバシー執行機関の共同のいずれかが運営管理者となる（第 5.1 条）。平成 30 年 3 月 12 日現在は、個人情報保護委員会と米国連邦取引委員会が共同運営管理者となっている。

¹⁷ 「支援要請（Request for Assistance）」には、(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の協力要請、(iv)プライバシーに関する苦情の移転を含むが、これに限定されないとされる（第 4.1 条）。

に対して個人情報の取扱いの委託等をしているときに、プライバシー違反が疑われるような事案が発生したとする。このような場合において、CPEA の枠組みに基づき、他のエコノミーのプライバシー執行機関は、日本の個人情報保護委員会に対して、支援を要請でき、日本側が裁量に基づき支援を行うこととなる。

具体的な支援要請の手続は、以下の通り行われる。

ア 支援要請を出すプライバシー執行機関に対し求められる行為（第 9.7 条）

(ア) APEC「支援要請」様式（'Request for Assistance' form）（付属書 A）を使用して問題となっている事項の主要な情報を伝達する。

(イ) 当該要請の実行過程でとるべき特別な予防措置等、受領機関 (Receiving Authority)¹⁸ が講じるべき措置に関する十分な追加的情報（もしあれば）を提供する。

(ウ) 受領機関から要求された情報の利用目的及びその情報が移転される者を特定する。

(エ) 照会を受けた事柄に関する処理を支援するために、受領機関より要求された情報やその他の支援を提供する。

イ 支援を要請されたプライバシー執行機関が求められる行為（第 9.8 条）

(ア) 支援要請を受領後、可及的速やかに支援要請を確認する。

(イ) 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。

(ウ) 当該要請の受諾又は拒否の決定を行うために、要請機関 (Requesting Authority)¹⁹ からのさらなる情報が必要な場合、速やかに確認し、要請機関に明確に連絡する。

(エ) 支援要請を拒否する場合、当該決定の根拠を提供し、また実現可能かつ適切な場合は、当該要請を処理し得る組織を要請機関に紹介する。

¹⁸「受領機関 (Receiving Authority)」とは、他の参加者から支援要請を受領した参加者をいう。また、「参加者 (Participant)」とは、CPEA に参加した APEC エコノミーのプライバシー執行機関をいう（第 4.1 条）。

¹⁹「要請機関 (Requesting Authority)」とは、別の参加者に支援要請を行った参加者をいう。

(オ) 支援範囲を制限する場合、当該決定の根拠を提供し、支援をなすために課される条件を提示する。

(カ) 支援要請を受諾する場合、(i) 通常の方針及び慣行に従って当該要請を処理し、(ii) 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支援となり得る事項について要請機関と連絡を取り、(iii) 実行可能かつ適切な場合、照会された事柄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。

(4) APEC 越境プライバシー・ルール (CBPR) システム

① 採択・施行時期・概要

CBPR システムは、2011 年 11 月の閣僚会議で承認され、2012 年 7 月に公表された。

CBPR システムは、個人情報管理者 (Controllers) である事業者が、越境個人情報保護に係る取組みに関し、APEC プライバシー・フレームワークの諸原則に適合しているか否かを認証する制度である。

CBPR システムへの参加を申請する事業者は、自己の越境個人情報保護に関するポリシー、体制等に関して自己審査を行い、その内容について、APEC により認定された認証機関であるアカウントビリティ・エージェント (Accountability Agent) (以下「AA」という。) による審査を受ける。AA により、CBPR の認証を受けた事業者は、越境移転における個人情報の取扱いに関して、APEC プライバシー・フレームワークの諸原則に適合した取扱いを行っている事業者であることを示すことができることになる。

CBPR システムは、APEC プライバシー・フレームワークの目的である「適切な情報プライバシー保護策の策定を奨励し、アジア太平洋地域での情報の自由な移動を保証する際の重要な手段」を具体化する運用制度として、その実施が示された。また、CBPR システムは、APEC パスファインダー計画の成果であり、APEC パスファインダー計画の中掲げられた 4 つの要素 (自己評価 (self-assessment)、適合性審査 (compliance review)、認証/受諾 (recognition/acceptance)、紛争解決及び執行 (dispute resolution and endorsement) が反映されている。

CBPR システムに関しては、(i) CBPR システムの概要及び要素、参加手順、ガバナンス構造、国内法及び規則との関係等を説明する「CBPR システムの方針、基準及び指針 (APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines)」(以下「CBPR ガイドライン」という。)、(ii) AA の CBPR システム参加に関する申請手順書である「AA の APEC 認定申請に係る手順書 (Accountability Agent APEC Recognition Application)」、(iii) 申請事業者のプライバシーポリシー等が、APEC プライバシー・ルールに適合しているか否かの自己評価に利用される「CBPR システム受入質問票 (APEC Cross-Border Privacy

Rules System Intake Questionnaire) 」 (以下「CBPR 質問票」という。)等の文書が公表されている。

② 適用範囲 (対象国及び拘束の程度)

これまで、米国 (2012 年)、メキシコ (2013 年)、日本 (2014 年)、カナダ (2015 年) 及び韓国 (2017 年) が、それぞれ CBPR システムに参加しており、また、2018 年 3 月、シンガポールが 6 番目の CBPR システム参加国となったことが APEC により公表されている²⁰。

CBPR システムは、エコノミーの国内法規制を代替し、変更するものではなく (CBPR ガイドライン第 43 項)、CBPR システムは、エコノミーに対して国内法規制を変更すべきか、あるいはどのように変更すべきかということについて命令する目的はない (CBPR ガイドライン第 46 項) とされる。しかしながら、CBPR システムへの参加を考えたとき、エコノミーは CBPR システムの必要要素の実施を確実にするために、国内法規制の変更を行う必要がある可能性があり、例えば、エコノミーは、CBPR システムにおけるプライバシー執行機関とするために、CPEA において定義される適切な規制当局を特定するようになる (CBPR ガイドライン第 48 項) と指摘されている。

ある事業者が CBPR システムへの参加者として認証されると、CBPR プログラムの要件への適合性は義務的なものとなり、執行可能となる (CBPR ガイドライン第 8 項)。

③ 内容 (要素・手続)

ア CBPR システムの要素

CBPR システムは、(1) 自己評価 (self-assessment)、(2) 適合性審査 (compliance review)、(3) 認証／受入 (recognition/acceptance) 及び (4) 苦情処理及び執行 (complaint processing and enforcement) の 4 つの要素からなる (CBPR ガイドライン第 9 項)。個々の具体的な内容は以下のとおりである。

(ア) 自己評価 (self-assessment)

CBPR システムは、APEC が認定した CBPR 質問票を使った、事業者の自己評価に依拠しており (CBPR ガイドライン第 10 項)、CBPR システムに参加しようとする事業者は、まず、CBPR 質問票に答えることにより、自らの個人情報保護のポリシーや体制等が、APEC プライバシー・フレームワークの諸原則に合致することについて自己評価を行う。完成

²⁰ APEC, News Release, “Singapore Joins APEC Data Privacy System”
https://www.apec.org/Press/News-Releases/2018/0307_CBPR (平成 30 年 3 月 14 日閲覧)

した CBPR 質問票と付属書類は、認証のために、APEC が認定した AA に提出される（CBPR ガイドライン第 11 項）。APEC が認定した AA によって、当該事業者のプライバシーポリシー及び体制等が CBPR システムの要件に適合していることが認められた事業者は、CBPR 適合者として認証され、APEC のウェブサイトにおいて公表される。これにより、消費者や他の利害関係者は、当該事業者が CBPR システムの参加者であることを認識できることになる（CBPR ガイドライン第 14 項）。

(イ) 適合性審査 (compliance review)

CBPR システムにおける APEC が認定した AA となるためには、APEC エコノミーが満足する確立した認定基準を充足しているかの認定を受けなければならない（CBPR ガイドライン第 15 項）。

認定にあたっては、利益相反回避のための方針及び手続、認証手続の手順、適合性審査の継続モニタリングの手順、再認証手続、苦情処理及び調査のメカニズム、CBPR プログラム要件の執行のメカニズムなどについて確認される（CBPR ガイドライン第 16 項）²¹。

APEC が認定した AA が事業者のプライバシーポリシー及び体制等を評価するときには、CBPR システムのプログラム要件に照らして評価しなければならない。このプログラム要件は、評価手続が参加エコノミーと調和するようなされるために、最低限の基準を与えるものでなければならず、AA の評価手続は、この基準を超えることは許されるが、下回することは許されない（CBPR ガイドライン第 20 項）。

(ウ) 認証／受入 (recognition/acceptance)

CBPR 適合者として認証された事業者のディレクトリが APEC エコノミーによって公表される（CBPR ガイドライン第 22 項）。公表されるディレクトリには、当該事業者の連絡先、認証した APEC が認定した AA の連絡先、関連するプライバシー執行機関が含まれ、消費者等が直接、適切な連絡先に質問や苦情を申し立てることができることとなる（CBPR ガイドライン第 22 項）。

(エ) 苦情処理及び執行 (complaint processing and enforcement)

CBPR システムは、AA 及びプライバシー執行機関によって執行可能でなければならず、AA は、法律や契約を通じて CBPR システムの要件を執行する必要がある、また、プライバシー執行機関は、CBPR システムの要件に適合する個人情報保護の効果を有する適用の

²¹ AA 認定申請手順書の Annex B “ACCOUNTABILITY AGENT RECOGNITION CRITERIA CHECKLIST” 参照。

ある国内法規制の下で、執行行為を行う権限をしている必要がある（CBPR ガイドライン第 24 項）。

イ CBPR システム参加の手続

APEC エコノミーが CBPR システムの利用するための手続は、エコノミー参加、AA の認定、事業者の認証の 3 つのプロセスを経る。

（ア）エコノミーの参加手続

APEC エコノミーが CBPR システムに参加するためには、以下の条件を充足する必要がある（CBPR ガイドライン第 28 項、Annex A ‘Charter of the Joint Oversight Panel’ 第 2.2 項）。

- a. CBPR システムへの参加意思表示を示し、当該エコノミーにおいて CPEA に参加しているプライバシー執行機関が 1 機関以上存在していることを確認する内容の書簡を ECSG 議長に対し提出すること。
- b. APEC が承認した AA を、少なくとも一つ利用する意思を有すること。
- c. 共同監視パネル（Joint Oversight Panel）との相談後、どのように CBPR システムの要件を当該エコノミーにおいて執行されるかの説明文書を ECSG 議長に対して提出すること。
- d. 共同監視パネルが ECSG 議長に対し、上記 a. 乃至 c. の条件がどのように充足しているかの報告書を提出すること。

その後、エコノミーは、1 つ以上の AA を指名する。APEC により、AA が認定されると、事業者は、CBPR システムへの参加手続を進めることができるようになる。

（イ）AA の認定手続

まず、エコノミーが当該エコノミーの域内において活動している AA を指名するか、又は共同監視パネルに対し、かかる認定の申請を受領したことを通知し、受領済み申請書と関連書類を提出する。その際、エコノミーは、AA に適用される関連する国内法及び規制、これらの法規制に関連する執行機関について説明しなければならない。プライバシー執行機関が AA の役割も行う場合、CPEA の参加者であること、どのように CBPR システムのプログラム要件の執行が許されるのかについて確認することが認められる（CBPR ガイドライン第 30 項）。

認定要請の受領後、共同監視パネルは、認定基準を充足しているか確認するため、必要書類の審査を開始する（CBPR ガイドライン第 33 項）。認定にあたっては、利益相反回避のための方針及び手続、認証手続の手順、適合性審査の継続モニタリングの手順、再認証手続、苦情処理及び調査のメカニズム、CBPR プログラム要件の執行のメカニズムなどについて確認される（CBPR ガイドライン第 16 項）²²。

かかる審査手続が完了した場合、APEC エコノミーに対し、AA として認定するか否かについて勧告を出す。一定期間内に反対の意見が提出されない場合、ECSG によって認定が許されたものとみなされる（CBPR ガイドライン第 33 項）。APEC エコノミーは、AA の認定申請を拒否する権利を有する（CBPR ガイドライン第 34 項）。

APEC の認定は、認定日から 1 年間で失効する。AA は、失効期間満了の 1 か月前までに認定の再申請を行わなければならない。再認定の手続は上記と同様である（CBPR ガイドライン第 36 項）。

これまでに、アメリカの民間企業である TrustArc（旧 TRUSTe、2013 年）及び日本の一般財団法人日本情報経済社会推進協会（JIPDEC、2016 年）が AA の認定を受けている。

（ウ）事業者の認証

申請事業者は、その域内の AA を利用しなければならない（CBPR ガイドライン第 38 項）。APEC に認定された AA は、申請事業者に対し、CBPR 質問票を配布し、その審査ガイドラインに基づき、又は、APEC 認定のドキュメントと審査手続を利用して、その回答及び付属書類を審査する（CBPR ガイドライン第 39 項）。

日本においては、申請事業者は、APEC の原則に照らした個人情報の取扱いに関する 50 の質問が記載された事前質問書に記載をし、AA である JIPDEC に提出する²³。

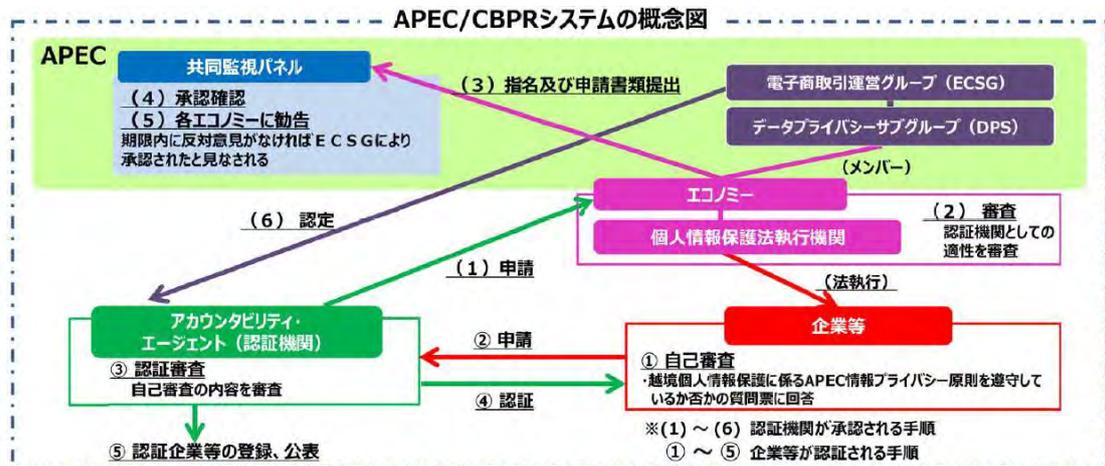
本報告書作成時点で、日米で 20 の企業が CBPR システムに基づく認証を受けており、アメリカの TrustArc は、AA として、米 IBM（2013 年 8 月）を皮切りに、Apple、HP 等を認証している。また、日本では、インタセクト・コミュニケーションズ株式会社が 2016 年 12 月に、JIPDEC により第 1 号認証を受けており、2017 年に更新をしている。

²² AA 認定申請手順書の Annex B “ACCOUNTABILITY AGENT RECOGNITION CRITERIA CHECKLIST” 参照。

²³ JIPDEC による事業者の認定手続については、JIPDEC が公表している APEC/CBPR 認証申請ガイドブック（平成 28 年 6 月）

（https://www.jipdec.or.jp/protection_org/JIPDEC_AOP_CBPR_008.pdf）及び JIPDEC のウェブサイトにおける事業者の CBPR 認証審査要領

（https://www.jipdec.or.jp/protection_org/cbpr/application.html）において、詳細な説明がされている（平成 30 年 3 月 14 日閲覧）。



(経済産業省資料
(<http://www.meti.go.jp/press/2016/12/20161220004/20161220004-1.pdf>) より抜粋)

(5) 取扱者のための APEC プライバシー承認制度 (PRP システム)

① 採択・施行時期・概要

2015 年 8 月、APEC は PRP システムを策定した。

PRP システムは、個人情報管理者 (Controller) による個人情報の取扱い義務の遵守を個人情報処理者 (Processors) が支援し、かつ、個人情報管理者が適格で責任ある個人情報処理者を特定できるように設計された制度である。CBPR システムが個人情報管理者に適用されるものであるのに対し、PRP システムは個人情報処理者を対象とする制度である。

PRP システムについても、CBPR システムと同様、PRP システムの概要及び要素、参加手順、ガバナンス構造、国内法及び規則との関係等を説明した「PRP システムの方針、基準及び指針 (APEC Privacy Recognition for Processors System POLICIES, RULES AND GUIDELINES)」

(以下「PRP ガイドライン」という。)、 「PRP システム受入質問票 (APEC Privacy Recognition For Processors Intake Questionnaire For Personal Information Processors)」 (以下「PRP 質問票」という。) 等の文書が公表されている。

PRP システムの管理は、DPS が責任を負う (PRP ガイドライン第 47 項)。

共同監視パネルは、CBPR システムにおけるその役割と同様、PRP システムにおいても、PRP システムの監視を行う (PRP ガイドライン第 50 項)。

② 適用範囲（対象国及び拘束の程度）

2017年7月に、CBPRシステムへの参加とあわせて、PRPシステムに参加する意思表明の通知を提出したシンガポールが、2018年3月、米国に次いで2番目の参加国となったことがAPECにより公表されている²⁴。

PRPシステム自体は、エコノミーの国内法規制を代替したり、変更したりするものではなく（PRPガイドライン第40項）、エコノミーに対して国内法規制を変更すべきか、あるいは、どのように変更すべきかということについて命令する目的はない（PRPガイドライン第44項）。しかしながら、PRPシステムへの参加を考えたとき、エコノミーはPRPシステムの必要要素の実施を確実にするために、国内法規制の変更を行う必要がある可能性がある（PRPガイドライン第45項）。

PRPシステムに参加することを選択した事業者は、個人情報管理者に代わって取り扱う個人情報のためのPRPシステムの要件と調和したプライバシーポリシー及び体制等を実行しなければならず、かかるプライバシーポリシー及び体制等はAPECの認定したAAによって評価される。ある事業者がPRPシステムへの参加者として認証されると、PRPプログラムの要件への遵守は義務的なものとなり、執行可能となる（PRPガイドライン第3項）。

PRPシステムへの参加は、参加事業者の国内法の義務にとって代わるものではない。国内法の要件がPRPシステムの要件を超える場合には、超える部分の国内法規制の適用が継続されるし、逆にPRPシステムの要件が国内法規制を超える場合には、事業者は、PRPシステムへの参加のために、かかる追加の要件を自主的に実行する必要がある（PRPガイドライン第41項）。

③ 内容（要素・手続）

ア PRPシステムの要素

CBPRシステム同様、PRPシステムは、(1) 自己評価（self-assessment）、(2) 適合性審査（compliance review）、(3) 認証／受入（recognition/acceptance）及び(4) 苦情処理及び執行（complaint processing and enforcement）の4つの要素からなる（PRPガイドライン第4項）。個々の具体的な内容は以下のとおりである。

（ア）自己評価（self-assessment）

²⁴ APEC, News Release, “Singapore Joins APEC Data Privacy System”
https://www.apec.org/Press/News-Releases/2018/0307_CBPR（平成30年3月14日閲覧）

PRP システムは、APEC が認定した PRP 質問票を使った、事業者の自己評価に依拠している (PRP ガイドライン第 5 項)。事業者によって完成された PRP 質問票と付属書類は、APEC が認定した AA に提出され、当該事業者のプライバシーポリシー及び体制等が PRP システムの要件と調和しているか否かが評価される。APEC の認定した AA によって、PRP システムの要件に適合していることが認められた事業者は、PRP 適合者として認証され、APEC のウェブサイトにおいて公表される。これにより、他の利害関係者は、当該事業者が PRP システムの参加者であることを認識できることになる (PRP ガイドライン第 9 項)。

(イ) 適合性審査 (compliance review)

PRP システムにおける APEC が認定する AA となるためには、APEC エコノミーが満足する確立した認定基準を充足しているかの認定を受けなければならない (PRP ガイドライン第 10 項)。

認定にあたっては、苦情処理手続、利益相反回避のための方針及び手続、認証手続、再認証手続、適合性審査、監督、プログラム要件の執行などの手続について、確認される (PRP ガイドライン第 11 項)。

APEC が認定した AA が事業者のプライバシーポリシー及び体制等を評価するときには、PRP システムの要件に照らして評価しなければならない (PRP ガイドライン第 15 項)。この要件は、評価手続が参加エコノミーと調和するようなされるために、最低限の基準を与えるものでなければならず、AA の評価手続は、この基準を超えることは許されるが、下回ることは許されない (PRP ガイドライン第 15 項)。

(ウ) 認証/受入 (recognition/acceptance)

AA によって PRP システムへの適合性を認証された事業者の事業者のディレクトリが、APEC エコノミーによって公表される (PRP ガイドライン第 17 項)、公表されるディレクトリには、当該事業者の連絡先、認証した AA の連絡先、関連するプライバシー執行機関が含まれ、消費者等が直接、適切なコンタクト・ポイントに質問や苦情を申し立てることができることとなる (PRP ガイドライン第 17 項)。

(エ) 苦情処理及び執行 (complaint processing and enforcement)

PRP システムの下で認証された個人情報処理者の効果的な監督を可能とするために、参加エコノミーが利用可能な執行のメカニズムとして、以下のようなものが含まれる (PRP ガイドライン第 21 項)。

- a. 直接的なプライバシー執行機関に支持された個人情報処理者の PRP プログラムの要件に対する遵守の執行。
- b. AA と個人情報処理者間の契約に基づく執行。前述 a の執行に関し、AA が一義的な責任を負う。
- c. 政府による AA の監視及び Accountability Agent Recognition Criteria に基づく義務の不履行の際の AA の停止を推奨する共同監視パネルの権限を通じた DPS による執行。
- d. AA と個人情報処理者の契約に基づく PRP ガイドラインプライバシー執行の効果的なメカニズム。

イ PRP システム利用のための手続

APEC エコノミーが PRP システムの利用するための手続は、エコノミー参加、AA の認定、事業者の認証の 3 つのプロセスを経る。

(ア) エコノミーの参加手続

APEC エコノミーが PRP システムに参加するためには、以下の条件を充足している必要がある (PRP ガイドライン第 25 項、Annex A ‘Charter of the Joint Oversight Panel’ 第 3.1 項)。

- a. PRP システムへの参加意思表示及び PRP システムのもとで認証された個人情報処理者の監督が、プライバシー執行機関を通じた直接的な政府が支持する執行を含むことを示し、当該プライバシー執行機関が CPEA に参加していることを確認する内容の書簡を ECSG 議長に対し提出すること。
- b. APEC が承認した AA を、少なくとも一つ利用する意思を有すること。
- c. 共同監視パネルとの相談後、仮に直接的な政府が支持する執行が適用されない場合であっても、当該エコノミーにおいて PRP システムのもとで認証された個人情報処理者の効果的な監督を確実なものとするために、利用可能な監督及び執行のメカニズムの説明文書を ECSG 議長に対して提出すること。
- d. 共同監視パネルが ECSG 議長に対し、上記 a. 乃至 c. の条件がどのように充足しているかの報告書を提出すること。

その後、エコノミーは、APEC 認定のための 1 つ以上の AA を指名する。

(イ) AA の認定手続

まず、エコノミーが当該エコノミーの域内で活動する AA を指名し、又は共同監視パネルに対し、かかる認定要請を受領したことを通知し、受領済み申請書と関連書類を提出する。その際、エコノミーは、AA に適用される関連する国内法及び規制、これらの法規制に関連する執行機関について説明しなければならない。プライバシー執行機関が AA の役割も行う場合、CPEA の参加者であること、どのように PRP システムの要件の執行が許されるのかについて確認することが認められる（PRP ガイドライン第 27 項）。

認定要請の受領後、共同監視パネルは、認定基準を充足しているか確認するため、必要書類の審査を開始し、かかる審査手続が完了した場合、APEC エコノミーに対し、AA として認定するか否かについて勧告を出す。一定期間内に反対の意見が提出されない場合、ECSG によって認定が許されたものとみなされる（PRP ガイドライン第 30 項）。APEC エコノミーは、AA の認定申請を拒否する権利を有する（PRP ガイドライン第 31 項）。

APEC の認定は、認定日から 1 年間で失効する。AA は、失効期間満了の 1 か月前までに認定の再申請を行わなければならない。再認定の手続は上記と同様である（PRP ガイドライン第 33 項）。

（ウ）事業者の認証

申請事業者は、その域内の AA を利用しなければならない（PRP ガイドライン第 35 項）。AA は、申請事業者に対し、自己審査のための質問票を配布し、その審査ガイドラインに基づきその回答及び付属書類を審査し、又は、APEC 認定のドキュメントと審査手続を利用して審査する（PRP ガイドライン第 36 項）。

（6）最近の議論の動向

① APEC プライバシー・フレームワークのアップデート

ECSG/DPS は、APEC プライバシー・フレームワークのアップデートを終え、2016 年 11 月に閣僚会議において改訂 APEC プライバシー・フレームワークが承認された²⁵⁾。このアップデートは、自由な情報及びデータの越境流通と特にオンラインマーケットにおける信用のための効果的な個人情報の保護との調和を確保するために、e コマースにおける方針及び規制のフレームワークのギャップに取り組んだものであり、また、OECD ガイドライン（2013 年）で導入されたコンセプトを取込んでいる（改訂 APEC プライバシー・フレームワーク 第 5 条）。

²⁵⁾ “Updates to the APEC Privacy Framework” (2016/CSOM/012app17), http://mddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf

② CBPR システムと BCR 制度の相互運用に向けた取組み

2012年9月に、APEC及びEUの合同ワーキンググループ(EU/APEC BCR-CBPR working team)が結成され、APECのCBPRシステムとEUの拘束的企業準則(Binding Corporate Rules System, BCR)との相互運用性を探るための検討が行われている。

2014年1月、APEC及びEUの合同ワーキング委員会は、比較文書(APEC/EU Referential for the Structure of the EU System of Binding Corporate Rules and APEC Cross Border Rules System) (以下「比較文書」という。)を作成した。この比較文書は、企業の両システムの相互認証(mutual recognition)を目的としたものではないが、BCRシステムの承認とCBPRシステムの認定の申請をしている企業に対し、非公式の実用的なチェックリストを提供し、二重認証(dual certification)の基礎となり得るものとされる²⁶。

比較文書においては、CBPRシステムとBCRシステムのそれぞれの重要な原理及び要件²⁷ごとに、それぞれのシステムに共通する主要な要素(common elements)が示されるとともに、それぞれのシステムの認証・承認に必要な追加の要素(additional elements)が示されている。

さらに、2015年以降、両サイドのCBPRシステムとBCRシステムの相互運用性に向けた協力の可能性が議論されており、EUは、2015年5月29日付のJoint work on BCR and CBPRと題するDPS宛への文書²⁸において、以下について合意している。

ア 短期的には、

(ア) 企業の二重認証(dual certification)を促進するため、BCRの申請様式であるWP133とCBPR質問票をベースとしたと両システムの共通の申請書の作成

(イ) 企業が双方のシステムを遵守していることを示すため、共通の質問票とともに提出されることになる、共通の企業のポリシー、関連する個人データ及びプライバシーのプラ

²⁶ 実際に、米国をベースとしている企業であるMerckは、2016年3月1日、この比較文書を利用して、BCRシステムの承認とCBPRシステムの認証を得た初めての企業となった(IAPP、“Merck first company to win BCRs via APEC’s CBPRs”、<https://iapp.org/news/a/merck-first-company-to-win-bcrs-via-apecs-cbprs/>) (平成30年3月14日閲覧)。

²⁷ 事業者の個人データ保護やプライバシー・ルールの基本方針、範囲、執行、データ主体や第三者に対する賠償などを含む27項目の原理・要件について記載がある。

²⁸ ARTICLE 29 Data Protection Working Party” Joint work on BCR and CBPR” Brussels, 29 May 2015” ,
<http://www.apec.org/Groups/Committee-on-Trade-and-Investment//-/media/Files/Groups/ECSG/2015/ARTICLE-29-Data-Protection-Working-Party.pdf>

ティスや提出書類の整理表（mapping）の作成

イ 長期的には、PRP と個人情報処理者向け BCR システムの比較文書、整理表の作成
APEC 及び EU の合同ワーキンググループは、現在、共通の質問票の作成を継続している。

3. CoE¹

(1) 制度概要

欧州評議会 (Council of Europe, CoE) は、人権、民主主義、法の支配の分野で国際社会の基準策定を主導する汎欧州の国際機関として 1949 年に設立された国際組織であり、現在 47 の国が加盟している。日本は、1996 年 11 月にアメリカ、カナダに次いで、3 番目のオブザーバーになった。オブザーバー国は、原則として、閣僚委員会以外の会合、専門家委員会に参加することが可能であり、投票権はないが発言権を有している。日本は、閣僚委員会へも招請があれば参加が可能となっている²。

欧州評議会は、拘束力を有する法律を制定する権利を有さず、加盟国間の国際協定を促進する権利のみを有している。したがって、以下に記載の条約のみが、加盟国がこれに署名した場合に限って適用される。非加盟国は、オブザーバーとしての立場にいるか、又は国際協定に参加することができる。以下に記載のデータ保護に関する条約の場合、欧州評議会の加盟国に加えて、8 の非加盟国が、これに参加している。当該条約は、特にヨーロッパ諸国の法制を見るうえで重要な役割を果たしてきたとされる³。

欧州評議会は、欧州人権裁判所 (European Court of Human Rights, ECtHR) を通じて国際的な契約を執行する権利を有している。欧州人権裁判所は、人権と基本的自由の保護のための条約 (European Convention on Human Rights, ECHR) の解釈及び適用を監視している。裁判所は、国内法を直接的に無効にするための管轄権を有さないが、その判決は、加盟国が条約を遵守して法的枠組みを作成するにあたり拘束力を有する。

欧州評議会の体制におけるデータ保護は、ECHR 第 8 条私生活及び家庭生活の尊重に関する権利 (right to respect for private and family life) に基づいている。

1. すべての者は、その私生活及び家庭生活、住居及び通信を尊重される権利を有する。
2. 公的団体は、本権利の行使に干渉してはならない。但し、法律に従う場合、民主主義社会における、国家安全保障、公衆の安全又は国の経済的福祉の利益のため、混乱又は犯罪の防止、衛生又は倫理の保護、第三者の権利及び自由の保護のために必要な場合を除く。

¹ 第 108 号条約の現代化版ドラフト (Council of Europe, Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data) の邦訳については、原則として石井夏生利「新版 個人情報保護法の現在と未来—世界的潮流と日本の将来像—」(勁草書房, 2017 年) 251 頁以下に依拠させていただいた。

² 外務省「欧州評議会 (Council of Europe) の概要」

<http://www.mofa.go.jp/mofaj/area/ce/gaiyo.html>

³ 前掲・石井 243 頁

個人情報保護に関するものとして、以下の条約が採択されている。

- ・ 条約第 108 号 - 個人データの自動処理に関する個人の保護のための条約 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) (ETS 第 108 号) (1981 年 1 月 28 日に加盟国の署名に付され、1985 年 10 月 1 日に発効。以下「第 108 号条約」という⁴。)
- ・ 1999 年 6 月 15 日に採択された欧州諸共同体の加盟を許可するための変更
- ・ 条約第 181 号 - 監督機関及び越境データ移転について個人データの自動処理に関する個人保護のための条約の追加議定書 (Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows) (ETS 第 181 号) (2001 年 11 月 8 日に加盟国の署名に付され、2004 年 7 月 1 日に発効。以下「追加議定書」という⁵。)

第 108 号条約には自動執行力はなく、条約自体から直接個人の権利が導き出されるものではないが、締約国には、データ保護の各規定について、国内法に導入することが義務づけられている (Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (以下「第 108 号条約解説」という。)) 第 38 項⁶)。国内法は、各国の法制度に依り、行政ガイドライン (administrative guidelines) など異なる形態で導入され得るが、第 108 号条約を全面的に遵守する形でなければならない (第 108 号条約解説第 39 項)。

欧州評議会では、2010 年以降、第 108 号条約を現代化する改革プロセスが実施された。これには、公の協議や委員会による提案書の作成が含まれる。新たに設置されたデータ保護特別委員会 (Ad hoc Committee on Data protection) (CAHDATA) により、2013-2014 年に最終的な提案書のレビューが行われた。CAHDATA は、2016 年 9 月に、現代化版の個人データの処理に関する個人の保護についての第 108 号条約のドラフト (以下「現代化版第 108 号条約ドラフト」という。)⁷及び改定版第 108 号条約解説のドラフト (以下「改定版第 108 号条約解説ドラフト」という。)⁸を公表した。

第 108 号条約第 1 条は、その意図及び目的について、以下のとおり定めている。

⁴ <https://rm.coe.int/1680078b37>

⁵ <https://rm.coe.int/1680080626>

⁶ <https://rm.coe.int/16800ca434>

⁷ Council of Europe, Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data
<https://rm.coe.int/16806a616c>

⁸ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108], Draft Explanatory Report
<https://rm.coe.int/16806b6ec2>

本条約の目的は、国籍又は居住地にかかわらず、すべての個人に関する個人データの自動処理（automatic processing）に関し、各締約国の域内において当該すべての個人を保護し、その権利及び基本的自由、並びに特にそのプライバシー権を尊重することである（「データ保護」）。

現代化版第 108 号条約ドラフトでは、個人データの自動処理（automatic processing of personal data）から個人データの処理（the processing of their personal data）へと対象が拡大されている（現代化版第 108 号条約ドラフト第 1 条）。

この保障は、国籍や居住地に関わらず、全ての個人に及ぶとされている（第 108 号条約解説第 26 項、改定版第 108 号条約解説ドラフト第 14 項）。

なお、データ保護の権利は、絶対的な権利ではなく、表現の自由や他の基本的権利及び自由との間の慎重な衡量が行われなければならない（改定版第 108 号条約解説ドラフト第 10 項）。

（2） 個人情報の定義

① 個人情報

第 108 号条約第 2 条において、「個人データ」を、「識別された（identified）又は識別され得る（identifiable）個人（以下「データ主体」という。）に関するあらゆる情報」と定義している。

現代化版第 108 号条約ドラフトでもこの定義に変更はない。

記述、口頭によるコミュニケーション、監視カメラのフィルムを含む映像・画像、及び音声も個人データに含まれると解されている⁹。

個人の識別に不合理な時間、努力又はリソースを必要とする場合、「識別され得る」とは判断されない（改定版第 108 号条約解説ドラフト第 16 項）。

ID 番号、仮名、生体若しくは遺伝データ、位置データ、IP アドレス又はその他の識別子を参照することによって、個人は識別され得る。すなわち、仮名又はデジタル識別子を用いても、データの匿名化とはいえない（改定版第 108 号条約解説ドラフト第 17 項）。

データは、データ主体の再識別が不可能か、又は再識別に不合理な時間、努力又はリソースを必要とする場合、匿名とみなされる。但し、物理的、生理的、遺伝的、経済的及び社会的データ（年齢、性別、職業、住所、家族状況等）等を用いて、個人を識別できる場合、匿名とはいえない（改定版第 108 号条約解説ドラフト第 18 項）。

⁹ 板倉陽一郎「OECD 改正ガイドライン」個人情報保護における国際的枠組みの改正動向調査報告書（消費者庁，平成 26 年 3 月 28 日 110 頁）

② 機微情報

第 108 号条約第 6 条は、人種や政治的見解、信条等の特別な種類のデータについて定めている。

人種、政治的見解、宗教その他の信条を示す個人データ、及び健康又は性生活に関する個人データは、自動処理することができない。但し、国内法において適切な保護措置 (appropriate safeguards) が定められる場合を除く。これは、刑事上の有罪判決に関する個人データにも適用される。

現代化版第 108 号条約ドラフトでは、遺伝データ、犯罪、刑事手続及びセキュリティ対策に関わる個人データ、生体データ、民族的出自並びに労働組合への加入情報などのデータが特別な種類のデータに該当するものとして、新たに追加されている。また、当該保護措置が、データ主体の利益、権利及び基本的自由へのリスク、特に差別のリスクを防止するものでなければならないことが追記されている(現代化版第 108 号条約ドラフト第 6 条)。

ここでいう適切な保護措置としては、データ主体の明示的同意やデータ処理の例外を定める法等がある(改定版解説第 108 号条約ドラフト第 54 項)。

(3) 主な規制・権利の内容

第 II 章(第 108 号条約第 4 条乃至第 11 条)では、データ保護に関する基本原則が定められている。締約国は、実施に責任を負う。締約国は、本章(第 4 条第(1)項)に定めるデータ保護に関する基本原則を実行するため、国内法において必要な措置を講じる。

主な原則としては、データの質に関する条項(第 108 号条約第 5 条)、特別な種類のデータ(第 108 号条約第 6 条。上記(1)②参照)、データセキュリティ(第 108 号条約第 7 条)及びデータ主体に関する追加の保護措置(第 108 号条約第 8 条)がある。

① データの質及びデータの処理の合法性

データの質に関する条項(第 108 号条約第 5 条)では、個人データの公正かつ合法的な入手及び処理、利用目的の明確化と制限、並びにデータ保持の適切性・正確性などが定められている。

現代化版第 108 号条約ドラフトでは、新しく、(i)データ処理は、合法的目的との関連でつりあいが取れており (be proportionate)、他の権利や利益、自由との公正なバランスが取れていなければならないこと(現代化版第 108 号条約ドラフト第 5 条第(1)項)、(ii)

各締約国は、データ主体の同意又は法が定める正当な根拠 (legitimate basis) に基づき、データ処理が実施されなければならないことを定めなければならないこと (現代化版第 108 号条約ドラフト第 5 条第(1)項)、(iii)個人データは適法に処理されなければならないことが定められている (現代化版第 108 号条約ドラフト第 5 条第(3)項)。その上で、現代化版第 108 号条約ドラフト第 5 条第(4)項において、データは、(iv) (1) 公平かつ透明性がある態様で処理されなければならない (fairly and in a transparent manner) (同項(a)号)、(2) 明確、特定かつ合法的目的で収集され、その目的に合致した方法で処理され (同項(b)号)、(3) 処理の目的に十分なもので、関連している、過度のものではなく (not excessive) (同項(c)号)、(4) 正確で、必要に応じ最新な状態で保存されており (同項(d)号)、(5) データ処理の目的のために必要な期間を超えて、データ主体を特定できる形式で保存してはならないものとされている (同項(e)号)。

現代化版第 108 号条約ドラフト第 5 条第(2)項における、データ主体の同意は、自発的なもので、確かな情報に基づく明確かつ特定のもの (free, specific, informed and unambiguous) でなければならない。単なる沈黙や不作為、事前に準備されたフォーム等は同意を構成しない (改定版第 108 号条約解説ドラフト第 40 項)。

データ主体は、いつでも同意を撤回できる (改定版第 108 号条約解説ドラフト第 43 項)。

同じく現代化版第 108 号条約ドラフト第 5 条第(2)項における、正当な根拠 (legitimate basis) には、データ主体を当事者とする契約の履行、データ主体又は第三者の重大な利益、管理者が遵守すべき法的義務、公共の利益、及び管理者又は第三者の優越する正当な利益等を含む (改定版第 108 号条約解説ドラフト第 44 項)。

現代化版第 108 号条約ドラフト第 5 条第(4)項 c 号における、過度ではない(not excessive) とは、データ処理を、その目的のために必要な範囲に限定するということを意味する (改定版第 108 号条約解説ドラフト第 50 項)。

現代化版第 108 号条約ドラフト第 5 条第(4)項 e 号は、データ処理の目的達成後は、当該データを削除するか、データ主体を識別し得ない方法でのみ保持することができることを意味している (改定版第 108 号条約解説ドラフト第 51 項)

② 透明性及び追加義務

現代化版第 108 号条約ドラフトでは、データ処理の公正とデータ主体の権利行使の観点から (改定版第 108 号条約解説ドラフト第 65 項)、透明性に関する規定が追加された。

締約国は、管理者は、管理者の情報、意図するデータ処理の目的及び根拠、個人データの種類、個人データの受領者、並びにデータ主体の権利の行使方法等の情報をデータ主体に通知するよう定めなければならない (現代化版第 108 号条約ドラフト第 7 条 bis)。

また、現代化版第 108 号条約ドラフトでは、締約国は、(i) 管理者及び処理者が、本条約を遵守してデータ処理を行っていることを証明できるように、適切な措置を講じることを

定めなければならないこと（現代化版第 108 号条約ドラフト第 8 条第(1)項 bis）、(ii)データ主体の権利及び基本的自由に与える影響を評価したうえで、データ処理の設計を行うことを求めること（同条第(2)項 bis）、(iii)データ処理の全ての段階での個人データを保護する権利の実施に関する技術的及び組織的措置の実施を求めること（同条第(3)項 bis）とする規定が新設されている。

条約の遵守の証明に係る適切な措置としては、データ保護オフィサーの設置がある（改定版第 108 号条約解説ドラフト第 84 項）。

③ データ主体の権利

データ主体に関する追加の管理保護措置（第 108 号条約第 8 条）では、何人も、(i)自動処理された個人データファイルの存在、その主たる目的、及びファイル管理者の身元等を確認することができること（同条(a)号）、(ii)合理的な期間でかつ過度な遅滞又は支出を伴うことなく、自己に関する個人データが自動処理されたデータファイルに蓄積されているか否かを確認することができること（同条(b)号）、及び (iii)条約の基本原則を実施する国内法の規定に違反してデータ処理が行なわれた場合に、当該データを訂正又は消去することができること（同条(c)号）が定められている。また、要求が認められないときの救済についても規定されている（同条(d)号）。

現代化版第 108 号条約ドラフトでは、「データ主体に関する追加の管理保護措置」との第 108 号条約第 8 条の見出しが、「データ主体の権利」に修正された。そして、主に、(i)自己の見解が考慮されない状況で、データの自動処理のみによって、自己に重大な影響を及ぼす決定に従わない権利（現代化版第 108 号条約ドラフト第 8 条第(1)項(a)号）、(ii)合理的な期間でかつ過度な遅滞又は支出を伴うことなく、個人データ処理の確認、処理されるデータの理解しやすい形式での伝達、並びに、データの情報源及びデータの保存期間に関する取得可能な情報等を請求できる権利（同項(b)号）、(iii)データ処理の結果が自己に適用される場合に、データ処理の根拠に関する知識を求める権利（同項(c)号）、(iv)データの訂正又は消去について、無料でかつ過度の遅滞なく請求できる権利（同項(e)号）、等の権利が認められるという修正が加えられている。

また、管理者がデータ処理の合法的な根拠を証明しない限り、データ主体はいつでも意義を述べる権利が追加された（現代化版第 108 号条約ドラフト第 8 条第(1)項 d 号）。

さらに、救済に関し、監督機関の援助が得られることが明記された（現代化版第 108 号条約ドラフト第 8 条第(1)項 g 号）

これらの権利は、他の権利や合法的な利益との調整が必要となる場合がある（改定版第 108 号条約解説ドラフト第 71 項）。

マーケティング目的でのデータ処理への異議については、無条件での消去又は削除が認

められるべきであるとされている（改定版第 108 号条約解説ドラフト第 77 項）。

④ 保護の拡大等

第 108 号条約第 11 条に従い、締約国は条約に定められるよりも、広範なデータ保護措置を導入することができる。制裁及び救済手段は、締約国毎に定められる（第 108 号条約第 10 条）。

（４） 監督・登録制度

第 108 号条約には監督機関に関する規定はなかったが、追加議定書において、各締約国における監督機関の設置及びその権限について定められた（第 1 条）。監督機関は、完全に独立してその任務を執行するものとされ、調査及び介入を行う権限を有するものとされている。

- (1) 各締約国は、条約第 II 章及び第 III 章、並びに本議定書に記載の原則を実行する、国内法における措置の遵守を確保することに責任を負う 1 つ又は複数の機関を定める。
- (2)
 - a. 上述の機関は、とりわけ調査及び介入を行う権限（powers of investigation and intervention）、並びに法的手続を行い又は管轄の司法当局（competent judicial authorities）に対し、本議定書第 1 条第(1)項に記載の原則を実行する国内法の規定違反について通報する権利を有している。
 - b. 各監督機関は、その権限の下で行われる個人データの処理に関し、いずれかの者より、当該者の権利及び基本的自由の保護に関して申し立てられる請求を受け付ける。
- (3) 監督機関は、完全に独立（complete independence）してその任務を執行する。
- (4) 監督機関の決定につき苦情がある場合、裁判所を通じて申し立てを行うことができる。
- (5) 第 IV 章の規定に従い、かつ、条約第 13 条の規定を損なうことなく、監督機関は、その任務の履行に必要な範囲において、とりわけあらゆる有益情報（useful information）を交換することにより、互いに協力する。

現代化版第 108 号条約ドラフトでは、監督機関の独立性がさらに強化され、権限の行使や義務の履行に際し、指示を求めまた受けてはならないとされた（現代化版第 108 号条約ドラフト第 12 条 bis 第(4)項）。

また、監督機関の権限として、データ移転に関する職務、条約違反について決定を下す権限及び制裁権限、並びに監督機関の職務及びデータ主体の権利等の周知活動に関する責任などが新たに規定された(現代化版第 108 号条約ドラフト第 12 条 bis 第(2)項 b 号、c 号、e 号)。

さらに、監督機関の協力に関して、関連する有益な情報の交換による相互支援、相互協力、調査又は介入の協力、共同行為の実施、及びデータ保護に関する実務の情報又は文書の提供などが明記された(現代化版第 108 号条約ドラフト第 12 条 bis 第 7 項)。

監督機関は、単体の他、合議体が考えられる(改定版第 108 号条約解説ドラフト第 111 項)。

監督機関は、迅速かつ効果的な行動をとるために、必要となる設備、財政的、技術的及び人的リソースを有するべきであるとされている(改定版第 108 号条約解説ドラフト第 112 項)。

締約国には、監督機関の設置に関し、一定の裁量が認められるが、監督機関は、少なくとも調査及び介入を行う権限並びに条約違反について決定を下す権限を有していなければならないとされている(改定版第 108 号条約解説ドラフト第 113 項)。

監督機関には、管理者及び処理者に対し、個人データ処理に関する情報について質問し、それを取得する可能性についての調査権限が与えられなければならないとされている(改定版第 108 号条約解説ドラフト第 114 項)。

(5) 漏えい等事案発生時の本人及び監督機関等への報告義務

現時点で存在しない(第 108 号条約に規定はない)。但し、現代化版第 108 号条約ドラフトにおいて、新たに第 7 条第(2)項として、データ保護に関する違反の申告義務が追加されている。

各締約国は、管理者は遅滞なく、少なくとも、本条約第 12 条の意義の範囲における、管轄の監督機関に対し、データ主体の権利及び基本的自由を著しく阻害し得るデータに関する違反につき通知する旨、定めるものとする。

データ侵害が発生した場合、管理者は、監督機関への通知に際し、データ侵害の起こり得る結果への対策も合わせて通知するべきであるとされている(改定版第 108 号条約解説ドラフト第 63 項)。

データ侵害により、個人の権利や自由に対する重大なリスクが生じる可能性がある場合、管理者は監督機関だけでなく、データ主体へも通知が必要であると認識する場合もあるとされている(改定版第 108 号条約解説ドラフト第 64 項)。

(6) 安全保護措置に関する規定

第 108 号条約では、締約国はデータセキュリティ対策を講じるものであると、非常に一般的に規定されている。

第 7 条 データセキュリティ

自動処理されたデータファイル (automated data files) 内に保存される個人データの保護に関し、付随的若しくは不正な破壊、又は付随的損失及び不正アクセス、改変若しくは漏えいに対する適切なセキュリティ対策が講じられるものとする。

現代化版第 108 号条約ドラフトでは、本条を新たな第 7 条第(1)項として、以下のように言い換えている。

各締約国は、管理者、及び該当する場合には処理者が、個人データへの付随的若しくは不正アクセス、個人データの破壊、損失、使用、修正又は開示といったリスクに対する適切なセキュリティ対策を講じる旨、規定する。

管理者は、技術的及び組織的保護措置を講じる際には、個人への潜在的な悪影響、処理される個人データの量及び質、データ処理を実施する技術設計の脆弱性の程度、データへのアクセス制限の必要性、長期間保存の要件などを考慮すべきとされている (改定版第 108 号条約解説ドラフト第 60 項)。

また、当該措置は、セキュリティ対策及び手段の最新の状況を考慮すべきであり、その費用は、潜在的リスクの重大性及び見込みと釣り合ったもの (be commensurate) であるべきであるとされている (改定版第 108 号条約解説ドラフト第 61 項)。

(7) 適用範囲、適用除外内容

① 適用範囲

第 108 号条約は、署名国に宛てられ、これらに対して拘束力を有する。一般適用範囲は、第 108 号条約第 3 条第(1)項に記載される。

締約国らは、民間・公的部門における自動処理された個人データファイル及び個人データの自動処理に対し、本条約を適用することを保証する。

現代化版第 108 号条約ドラフトでは、民間・公的部門の管轄に服するデータの処理 (data

processing) に対して、適用されるという形に修正されている（現代化版第 108 号条約ドラフト第 3 条第(1)項）。

ここでいう「データの処理」とは、データの収集、蓄積、保存、変更、復旧、開示、入手、消去若しくは破壊、又は論理的及び/又は算術的操作等の実施をいうとされている（現代化版第 108 号条約ドラフト第 2 条第(b)項）。

民間部門における処理は、締約国の領土と十分な関係を有する場合に、管轄に服するとされる。例えば、データの処理が当該領土内で行われる場合やデータ処理が当該領土内に所在するデータ主体へのサービス又は物品の提供に関連する場合等に、管轄に服するとされる（改定版第 108 号条約解説ドラフト第 24 項）。

また、現代化版第 108 号条約ドラフトでは、純粋な個人的活動又は家庭内活動に関するデータ処理については、条約の適用範囲外であることが明示されている（現代化版第 108 号条約ドラフト第 3 条第(1)項 bis）。

ここでいう個人的又は家庭内活動とは、個人の私生活に密接かつ客観的に関連するものであって、他者の領域に重大な影響を与えないものをいうとされている（改定版第 108 号条約解説ドラフト第 26 項）。例えば、友人の連絡先リストを作成することは、これに該当するが、一般に公開するウェブサイトなどは該当しない（改定版第 108 号条約解説ドラフト第 26 項、第 27 項）。

例外（及び適用範囲を、より広範にする可能性）は、第 108 号条約第 3 条第(2)項[1999 年 6 月 15 日付の変更の様式]において、及び締約国が署名する時又は後日、条約に参加した日に、締約国の裁量により定められる。

締約国又は欧州共同体は、署名時又はその批准書、受諾書、承認書又は加入書の寄託時、又はそれ以降のいずれかの時点で、欧州評議会の事務局長（Secretary General）に宛てた宣言書（declaration）により、以下の事項について通知を行うことができる。

- (a) 本条約を、特定の種類の自動処理された個人データファイルに適用しないこと（適用除外する特定分野のリストを寄託する。）。但し、このリストには、当該締約国又は欧州共同体の国内法に基づきデータ保護規定の対象となる種類の自動処理されたデータファイルを含めない。そのため、締約国又は欧州共同体は、追加の種類の自動処理された個人データファイルが、自国の国内法に基づきデータ保護規定の対象となる場合いつでも、本リストを新たな宣言書に変更する。
- (b) 本条約を、個人により直接的又は間接的に構成される、団体、組合、基金、会社、企業その他の機関（当該機関の法人格の有無を問わない。）に関する情報にも適用すること。
- (c) 本条約を、自動処理されない個人データファイルにも適用すること。

かかる規定に続いて、第 108 号条約第 3 条第(3)項乃至第(6)項は、当該通知に関する手続上の規則について定めていたが、現代化版第 108 号条約ドラフトでは削除されている。

② 適用除外

第 108 号条約第 9 条では、国家安全保障、公衆の安全、国家の財政上の利益の保護若しくは犯罪行為の抑止、又はデータ主体若しくは他のデータ主体の権利及び自由の保護を理由として、保護の基本原則が制限され得ること、また、統計又は学術研究の目的のために使用される場合、データ主体の権利行使の制限をする法律を定めることができるとされている。

現代化版第 108 号条約ドラフトでは、適用が制限される項目について、一般の公共の利益の本質的な目的等が追記された他、他のデータ主体の権利及び自由として表現の自由が明記された（現代化版第 108 号条約ドラフト第 9 条第(1)項）。また、民主主義社会の目的を達成するために必要かつ適切な措置であれば、法律によって越境データ移転の規制に関して、適用制限を定めることができる規定が追加されている（現代化版第 108 号条約ドラフト第 9 条第(3)項）。

さらに、第 108 号条約には、第 24 条に以下のような地域的条項（territorial clause）が含まれている。

(1) 締約国は、その批准書、受諾書、承認書又は加入書への署名時又は寄託時に、本条約が適用される 1 つ又は複数の地域を指定することができる。

第(2)項及び第(3)項は、宣言書及び当該宣言書の取下げにより、適用日を、より遅い日に延期することについて定めている。

第 108 号条約第 23 条には、CoE 非加盟国が条約に加盟することができる旨、定められている。

(8) 国際的な情報移転に関する規定

第 108 号条約第 12 条は、個人データの国際流通（Transborder flows）及び国内法について扱っている。原則として、データ保護を目的として、他の締約国へのデータ移転を制限してはならないとされ、同等の保護水準がなく、一定の種類 of 個人データについて特別の規定がある場合や、非締約国へデータ移転する場合について制限可能となっている。

- (1) 以下の規定は、その媒体を問わず、自動処理される又は自動処理される目的で収集された個人データの国境を越えた移転に適用される。
- (2) 締約国は、プライバシー保護を唯一の目的として、他の締約国の地域への個人データの国際流通を禁止し、又は特別な承認 (special authorisation) の取得を条件付けてはならない。
- (3) 上記にかかわらず、以下の場合、各締約国は第(2)項の規定を適用除外とする権利を有する。
 - (a) 法律に、一定の種類個人データ又は自動処理された個人データファイルに関し、当該データ又はファイルの性質により、特定の規則が含まれる場合。但し、他方締約国の規則に同等の保護が規定されている場合を除く。
 - (b) 締約国の地域から、他の締約国の地域の仲介者を通じて、非締結国の地域に移転する場合、当該移転が本項の初めに記載する締約国の法律の抜け道 (circumvention) となるのを回避するため。

その後、追加議定書第 2 条では、条約の締約国の管轄権の対象となっていない受領者に対する個人データの国際流通について定められた。ここでは、個人データ保護について十分な保護レベルにある国の場合や、データ主体の特定の利益になる場合に認められるデータ移転に関し定められている。

- (1) 各締約国は、条約の締約国ではない国又は組織の管轄権の対象となっている受領者に対する個人データの移転について定める (当該国又は組織が、意図されたデータ移転に関し、十分な保護レベルを確保する場合に限る。) 。
- (2) 本議定書第 2 条第(1)項から逸脱して、各締約国は、以下の場合、個人データの移転を許可することができる。
 - (a) 以下の理由により国内法により定められる場合
 - データ主体の特定の利益 (specific interests) のため
 - 正当かつ優越的な利益 (legitimate prevailing interests) 、特に重要な公共の利益のため (important public interests)
 - (b) とりわけ契約条項に起因する管理措置が、移転に責任を負う管理者により定められ、管轄の機関がこれを国内法に従い適切とみなす場合

保護のレベルについては、ケースバイケースで評価が行われるものとされ、その際には、データの種類、移転されるデータの処理の目的及び期間、移転前の国と最終移転先、国・組織に適用される一般・個別法、並びに専門的セキュリティのルールなどを考慮して判断

されるとされていた（追加議定書の解説書¹⁰（以下「追加議定書解説」という。）第 27 項）。

また、正当かつ優越的な利益とは、ECHR 第 8 条第(2)項、第 108 号条約第 9 条第(2)項、法的主張の行使若しくは防御、又は公的登録からのデータ抽出などから特定される重要な公共の利益の保護をいう（追加議定書解説第 31 項）。

現代化版第 108 号条約ドラフトでは、データ保護を唯一の目的として、他の締約国へのデータ移転を制限してはならないという原則を維持しつつ、締約国が、地域的国際機関に属する国によって共有される保護の調和的規則に拘束される場合、又は受領者が締約国でない国や国際機関の管轄下にある場合で、本条約の規定に基づき適切な保護レベル（appropriate level of protection）が確保されているときには、個人データの移転が可能であるという形に修正された（現代化版第 108 号条約ドラフト第 12 条第(1)項、第(2)項）。第(1)項は、締約国間のデータ移転に適用されるものであり、第(2)項は、締約国の管轄に服さない受領者への越境個人データ移転について定めたものである。

そして、ここでいう適切な保護レベルは、国際条約や国際合意を含む国若しくは国際機関の法、又は特別な若しくは承認された標準的な保護措置によって確保され得るとされた（現代化版第 108 号条約ドラフト第 12 条第(3)項）。

また、締約国が、個人データの移転を可能とする旨を定めることができる場合として、(i)適切な保護措置がないことによるリスクの通知を受けたうえで、明確な、特定かつ自由な同意を与えた場合（現代化版 108 号条約ドラフト第 12 条第(4)項(a)号）、(ii)データ主体の特定の利益に必要である場合（同項(b)号）、(iii)優越的かつ正当な利益（prevailing legitimate interests）、特に重要な公共の利益が法で定められ、その移転が民主主義社会において、必要かつ釣り合いの取れた措置を構成している場合（同項(c)号）、及び(iv)表現の自由のために民主主義社会において、必要かつ釣り合いの取れた措置を構成している場合（同項(d)号）が規定されている。

（9）越境執行協力

① 制度の名称、概要、採択・施行時期

第 108 号条約及び追加議定書（上記を参照）には、締約国間の協力に関する規定が含まれる。

② 適用範囲（対象国及び拘束の程度）

¹⁰ Council of Europe, Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows
<https://rm.coe.int/16800cce56>

(7) を参照

③ 内容

第 108 号条約第 IV 章は、相互支援について定めている。特に第 108 号条約第 13 条では、締約国間の協力について定めている。各監督機関は、他の監督機関からの要求に基づき、一定の例外的場合を除き（第 108 号条約第 16 条）、情報提供や適切な措置を講じることなどの相互支援を行う。

- (1) 締約国は、本条約を施行するために相互支援 (mutual assistance) を提供することに合意する。
- (2) 当該目的において、以下のとおりとする。
 - (a) 各締約国は、1 つ又は複数の機関を指名し、それぞれの名称及び住所を欧州評議会の事務局長に通知する。
 - (b) 1 つ又は複数の機関を指名した各締約国は、前項に記載の通知において、各機関の権能 (competence of each authority) を記載する。
- (3) 締約国から指名された機関は、他方締約国が指名した機関からの要求に基づき、以下のことを行う。
 - (a) データ保護の分野における、その法律及び管理実務 (administrative practice) に関する情報を提供する。
 - (b) その国内法に従い、かつプライバシー保護の目的に限り、その地域で実施される特定の自動化プロセスに関する事実情報提供のためのあらゆる適切な措置を講じる（但し、処理される個人データを除く。）。

第 108 号条約第 14 条乃至第 17 条は、ある締約国から、他の締約国に居住するデータ主体に対する支援や、相互支援の費用・手続き等について定めている。

第 108 号条約のこれらの規定は、追加議定書により補足される。条約に定められる原則の執行及びその遵守は、第一次的には、国の監督機関に委任される。追加議定書第 1 条第 (1) 項には、以下のとおり定められている。

各締約国は、条約第 II 章及び第 III 章、並びに本議定書に記載の原則を実行する国内法における措置の遵守を確保することに責任を負う 1 つ又は複数の機関を定める。

追加議定書第 1 条第 (5) 項は、異なる締約国の監督機関の国際協力について定めている。

第 IV 章の規定に従い、かつ、条約第 13 条の規定に反することなく、監督機関は、その任務の履行に必要な範囲において、とりわけあらゆる有益情報を交換することにより、互いに協力する。

現代化版第 108 号条約ドラフトでは、以下のとおり定められているが、その内容において従前から大きな変更はない。

第 13 条 締約国間の協力

- (1) 締約国は、本条約を施行するために相互支援を提供することに合意する。
- (2) 当該目的において、以下のとおりとする。
 - (a) 各締約国は、本条約第 12 条 bis に意味するところの 1 つ又は複数の監督機関を指名し、それぞれの名称及び住所を欧州評議会の事務局長に通知する。
 - (b) 1 つ又は複数の監督機関を指名した各締約国は、前項に記載の通知において、各監督機関の権能を記載する。

第 14 条 データ主体への支援

- (1) 各締約国は、その国籍又は居住地に関わらず、あらゆるデータ主体に対し、本条約第 8 条に基づく権利を行使するための支援を行うものとする。
- (2) データ主体が、他の締約国に居住する場合、当該データ主体は、当該締約国が指定した監督機関を通して、請求を出すことができる。
- (3) 支援請求は、すべての必要な項目、とりわけ次に掲げるものに関する情報を含むものとする。
 - (a) 氏名、住所及び請求をするデータ主体を特定する他のあらゆる情報
 - (b) 請求に関連する処理又はその管理者
 - (c) 請求目的

第 15 条 指定監督機関が行う支援に関する保護措置

- (1) 他の締約国の指定監督機関から情報を受領した、ある締約国の指定監督機関は、支援要請に伴うものであるか自らの支援要請に対する回答であるかに関わらず、当該情報を特定された支援の要請以外の目的のために利用してはならない。
- (2) いかなる場合においても、指定監督機関は、データ主体の自発的かつ明示の承諾なく、当該データ主体の代わりに支援要請をすることは認められない。

第 16 条 支援要請の拒否

本条約第 13 条に基づき、支援要請を受けた指定監督機関は、次に掲げる場合を除き、それに応じることを拒否してはならない。

- (a) その要請が、自らの権限に適合しない場合
- (b) その要請が、本条約の規定に従っていない場合
- (c) その要請に応じることが、監督機関を指定した締約国の主権、国家の安全若しくは公の秩序、又は当該締約国の管轄下にある個人の権利及び基本的自由と適合しない場合

第 17 条 支援の費用及び手続

- (1) 本条約第 13 条に基づき締約国が相互に提供する支援、並びに本条約第 8 条及び第 14 条に基づき締約国がデータ主体に提供する支援は、専門家及び通訳に関して発生するものを除き、いかなる費用又は報酬の支払いを発生させるものではない。専門家及び通訳に関する費用又は報酬は、支援要請を行う監督機関を指定した締約国が負担する。
- (2) データ主体は、相手方締約国の居住者が法律上支払うものとされているものを除き、当該締約国の領域内で、その者のために講じられた措置に関するいかなる費用又は報酬の支払いも求められない。
- (3) 特に形式、手続及び使用言語に関する支援についてのその他の詳細は、直接関連締約国間で定めるものとする。

相互支援は、第 108 号条約第 16 条の場合を除き、義務とされている（改定版第 108 号条約解説ドラフト第 135 項）。

(10) 最近の議論の動向

① 制度改正の検討状況

前述のとおり、2010 年以降、第 108 号条約を現代化する改革プロセスが実施され、新たに設置されたデータ保護特別委員会（CAHDATA）が、2016 年 9 月に、現代化版第 108 号条約ドラフト及び改定版第 108 号条約解説ドラフトを公表した。

改定版第 108 号条約解説ドラフトには、改革プロセスに関し、「条約の規定については、一般的かつ技術的に中立な性質（general and technologically neutral nature）が維持されなければならない。」と記載されている。条約の、他の法的枠組みとの一貫性及び適合性が保たれなければならない、条約の公開性（open character）（これにより、条約に、世界標準としての固有の可能性（unique potential as a universal standard）が加わる。）が再確認されなければならない。」（改定版第 108 号条約解説ドラフト第 2 項）

② 個人情報に関連した最近の裁判例

欧州人権裁判所は、長年、個人データの保護に関する多数の事件を扱ってきた。2017 年に限ってみても、これまでに、以下の判決が裁判所により下されている。

- ・ Mustafa Sezgin Tanrıkulu 対トルコ (2017 年 7 月 18 日) ¹¹
裁判所は、トルコにいる全ての者の通信の傍受を許可する 2005 年のトルコ国内の裁判所の判決について、ECHR 第 8 条及び 13 条 (有効な救済手段に対する権利) (right to an effective remedy) の違反があったとした。
- ・ Bărbulescu 対ルーマニア (2017 年 9 月 5 日、大法廷) ¹²
会社が、かつての従業員の E メール及び内容を監視した後に当該従業員を解雇した件について、裁判所の判決によりこれが認められたが、欧州人権裁判所は、ECHR 第 8 条の違反があったとした。
- ・ Aycaguer 対フランス (2017 年 6 月 22 日) ¹³
国の電子化された DNA データベース (FNAEG) への加入のために生体サンプルを提供するよう命令され、これを拒絶した事実により刑事上の有罪判決となった件について、裁判所は、志願者の私生活を尊重する権利 (right to respect for his private life) が侵害されており、ECHR 第 8 条の違反があったとした。
- ・ Satakunnan Markkinapörssi Oy 及び Satamedia Oy 対フィンランド (2017 年 6 月 27 日、大法廷) ¹⁴
2つの会社が 120 万人の個人の税務情報を公表したことに対し、国内機関が、かかる大量の個人データの公表は、データ保護法の違法であるとし、将来における当該大量公表を禁止し、裁判所は、ECHR 第 10 条 (表現の自由) の違反を否定した。

¹¹ ECtHR, Mustafa Sezgin Tanrıkulu v. Turkey, No.27473/06, 18 July 2017

¹² ECtHR, Bărbulescu v. Romania, No.61496/08, 5 September 2017

¹³ ECtHR, Aycaguer v. France, No.8806/12, 22 June 2017

¹⁴ ECtHR, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No.931/13 27 June 2017

諸外国の個人情報制度に係る最新の動向に関する調査研究

執筆者名簿

<プロジェクト責任者>

鈴木 由里 渥美坂井法律事務所・外国法共同事業 パートナー

<執筆者>

臼井 康博 渥美坂井法律事務所・外国法共同事業 パートナー

大串 淳子 渥美坂井法律事務所・外国法共同事業 パートナー

落合 孝文 渥美坂井法律事務所・外国法共同事業 パートナー

小幡 映未子 渥美坂井法律事務所・外国法共同事業 パートナー

三部 裕幸 渥美坂井法律事務所・外国法共同事業 パートナー

アシッシ・ジェジュルカール 渥美坂井法律事務所・外国法共同事業 パートナー

花田 さおり 渥美坂井法律事務所・外国法共同事業 パートナー

湯澤 正 渥美坂井法律事務所・外国法共同事業 パートナー

上東 亘 渥美坂井法律事務所・外国法共同事業 アソシエイト

金 貞伊 渥美坂井法律事務所・外国法共同事業 アソシエイト

ジョイ・カルグ 渥美坂井法律事務所・外国法共同事業 アソシエイト

陳 鳳琴 渥美坂井法律事務所・外国法共同事業 オブ・カウンセラー

都筑 大輔 渥美坂井法律事務所・外国法共同事業 アソシエイト

フェイジー・パークス 渥美坂井法律事務所・外国法共同事業 アソシエイト

細田 浩史	渥美坂井法律事務所・外国法共同事業	アソシエイト
松岡 史朗	渥美坂井法律事務所・外国法共同事業	オブ・カウンセラー
三浦 康晴	渥美坂井法律事務所・外国法共同事業	アソシエイト
南 智樹	渥美坂井法律事務所・外国法共同事業	アソシエイト
村川 耕平	渥美坂井法律事務所・外国法共同事業	オブ・カウンセラー
八巻 展孝	渥美坂井法律事務所・外国法共同事業	アソシエイト
吉田 千鶴	渥美坂井法律事務所・外国法共同事業	アソシエイト
安富 潔	渥美坂井法律事務所・外国法共同事業	顧問

(五十音順)

諸外国の個人情報制度に係る最新の動向に関する調査研究
海外協力法律事務所

ニュージーランド	MinterEllisonRuddWatts
韓国	Lee & Ko
タイ	SIAM CITY LAW OFFICES LIMITED
ベトナム	APAC International
フィリピン	Disini & Disini Law Office
インドネシア	HPRP Lawyers
インド	Lakshmikumaran & Sridharan
ロシア	Law Firm ALRUD