JIPDEC

IT-Report

2018 Winter

特集 データの利活用と個人情報保護施策の現状

JIPDEC
一般財団法人日本情報経済社会推進協会

今年度第２号となる「JIPDEC IT-Report 2018Winter」は、「データの利活用と個人情報保護施策の現状」と題し、特集を組みました。

わが国では改正個人情報保護法の全面施行から１年が経過しましたが、法改正で推奨されている匿名加工情報を活用したビッグデータビジネスに加え、個人から預託されたデータを管理し、個人の指示に基づきデータを第三者に提供する「情報銀行」事業の確立に向け、政府が事業者認定スキームを公表し、具体的に「情報銀行」ビジネスに参入する企業も出てきています。また、法改正を受け、JIS Q 15001（個人情報保護マネジメントシステム－要求事項）が昨年12月に11年ぶりに改正されました。

一方、海外ではEU域外での個人データの取扱いに対し厳しく規制する一般データ保護規則（GDPR）が2018年５月に施行されるとともに、現在GDPRを補完する位置づけとして、Webサイトを訪問したユーザにクッキー付与の同意可否を委ねる「eプライバシー規則（Cookie法）」の審議が進められています。

GDPRに関しては「十分性認定」に向けて日-EU間でのデータ移転の円滑化に向けた準備が進められていますが、米国やアジア諸国でも新たな法規制の動きがみられています。

本誌では、一昨年発行の「IT-Report 2016 Winter」で紹介した以降の、国内外の個人情報保護施策や日本企業への影響、情報銀行やJIS改正に関する最新動向について、有識者の方に解説をしていただくとともに、個人情報保護関連の年表と2018年４月から９月の情報化動向を掲載しています。

本誌を個人情報を取り扱う事業者はもとより、個人の皆様にも参考としていただければ幸いです。

2018年12月

一般財団法人 日本情報経済社会推進協会

JIPDEC IT-Report 2018 Winter

Contents

【特集】「データの利活用と個人情報保護施策の現状」 …… 01

Ⅰ. 国内におけるデータの利活用と個人情報保護への取組み …… 01

Ⅰ-1 改正個人情報保護法施行後１年の動き
個人情報保護委員会事務局 …… 01

Ⅰ-2 「情報銀行」について
総務省 情報流通行政局情報通信政策課 …… 06

Ⅰ-3 JIS Q 15001:2017改正のポイント
一般財団法人日本データ通信協会 Pマーク審査部長／
JIS Q 15001 改正原案作成委員会 委員　小堤 康史 … 11

Ⅰ-4 認定個人情報保護団体としての役割について
JIPDEC認定個人情報保護団体事務局長　篠原 治美 … 16

Ⅱ. 海外における個人情報保護の取組み …… 19

Ⅱ-1 各国の動向 …… 19

Ⅱ-2 日本企業への影響
EYアドバイザリー・アンド・コンサルティング株式会社
テクノロジーリスク パートナー　梅澤 泉 …… 23

〈資料-1〉国内外の主な個人情報保護関連の年表 …… 28

〈資料-2〉情報化に関する動向（2018年4月～9月） …… 31

特集

「データの利活用と個人情報保護施策の現状」

Ⅰ 国内におけるデータの利活用と個人情報保護への取組み

Ⅰ-1 改正個人情報保護法施行後１年の動き

個人情報保護委員会事務局

2015年９月に成立した「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年法律第65号。以下「平成27年改正法」という。）の一部施行により、2016年１月１日から個人情報保護委員会が個人情報保護法を所管し、個人情報保護関連の制度が政府全体として統一的かつ整合的に運用されるよう、個人情報の保護に関する基本方針の策定と関連施策の総合的かつ一体的な推進を図る役割を担っている。さらに、平成27年改正法による改正後の個人情報保護法が2017年５月30日に全面施行されたことに伴い、それ以前は各主務大臣が行使していた監督権限について、個人情報保護委員会が一元的に所掌することとされた。

本稿においては、改正個人情報保護法の全面施行から１年間の動きについて俯瞰するとともに、この１年間の個人情報保護委員会の活動に関するトピックとして、2018年７月17日に公表された日EUの相互の円滑な個人データ移転を図る枠組み構築の最終合意に至るまでの経緯と、今後の見通しについて解説する。

1. 監督権限の一元化に伴うルールの整備・広報啓発等の取組

改正個人情報保護法の全面施行に伴い、2017年５月30日以降、個人情報取扱事業者に対する監督権限について、個人情報保護委員会が一元的に所掌することとなった。これに伴い、原則として個人情報保護委員会がすべての分野に共通に適用される汎用的なガイドラインを作成し、ウェブサイトで公表することとした。また、金融関連分野・医療関連分野等の各分野別に、各省と連名で具体的な留意点・事例等を示したガイドライン等を作成・公表した。

また、認定個人情報保護団体（以下「認定団体」という。）については、改正個人情報保護法の全面施行により、認定団体が作成する個人情報保護指針の届出について、個人情報保護委員会が受付等を行うこととなった。個人情報保護委員会は、認定団体の活動状況を把握するための調査を実施したほか、認定団体連絡会議において、積極的に取り組んでいる認定団体のベストプラクティスを共有したり、認定団体の活動の普及促進のためのシンポジウムを開催するなどの周知・広報活動を行い、業界・事業分野ごとの自主的な取組を支援している。

また、改正個人情報保護法の内容を周知するため、同法の基本的な義務規定を解説した広報資料を作成し、全国の商工会議所等へ配布するなど、改正個人情報保護法にすべての事業者が円滑に対応できるようにするための広報・啓発を行った。さらに、消費者センターの相談員等が参照できるよう、個人情報に係る相談処理に関するマニュアルを作成したほか、消費者向けウェブページの開設や子ども向けハンドブックの作成等により、幅広い対象に向けて改正個人情報保護法の周知啓発を行った。

加えて、改正個人情報保護法の全面施行により、オプトアウト手続に係る届出が義務付けられたことを踏まえ、個人情報の第三者提供事業（名簿等個人

データの販売事業等）等の実態調査を行い、届出義務を履行していない未届事業者に対して事業内容等に関する調査を開始するとともに、名簿等個人データの適正な取扱いや利用に関する注意喚起をウェブサイトに掲載した。また、ウェブサイト運営事業者のセキュリティ対策、個人を狙ったサイバー攻撃等への対応策等をウェブサイトに掲載するなど、不正アクセス等に対する対応についての広報・啓発も行っている。

2．改正個人情報保護法に基づく監督等の実施状況

改正法の全面施行に伴い、監督対象となる事業者が大幅に増え、個人情報取扱事業者に対する監督権限も個人情報保護委員会に一元化された。2018年度上半期には、全面施行後初めてとなる立入検査を２件実施し、個人情報の大量漏えい事案について、安全管理措置等の状況を確認するとともに、再発防止策の実施や個人情報の適正な取扱いを行うよう指導・助言を行うなどした。

これらに加え、最近の事案等から重要性を増しているのが国外に所在する事業者への対応である。改正法の全面施行後、フェイスブック社が提供する「いいね！」ボタンが設置されているウェブサイトを閲覧した場合、ボタンを押さなくともユーザIDやアクセス履歴等の情報がフェイスブック社に送信されてしまうことや、性格診断アプリにより取得した個人情報の一部がコンサルティング会社に不正に提供されていた事案が判明した。さらに2018年９月末には、同社のシステムの脆弱性を利用したハッキングによって約2,900万人の個人情報が不正アクセスを受けたことが判明した。

これに対して個人情報保護委員会は、2018年10月にフェイスブックインクに対して個人情報保護法第41条および第75条の規定に基づく指導を行った。具体的には、ユーザへのわかりやすい説明や本人からの同意の取得の徹底および同社がプラットフォーマーとしての責任を認識し、プラットフォーム上のアプリケーションの活動状況の監視を徹底すること、不正アクセス事案についても本人への通知、原因究明と再発防止策の策定、引き続き個人情報保護委員会へ報告すること等を求めた。

この他、海外の個人情報保護当局に対し、個人情報保護委員会の対応状況について情報提供を行うとともに、漏えい等事案の発生原因や再発防止策について情報の共有を求めるなど、海外の個人情報保護当局との執行協力を含めて、事案の国際化に対応しているところである。

3．日EU間の相互の円滑な個人データ移転を図る枠組み構築に係る最終合意について

個人情報保護委員会と欧州委員会は2018年７月17日、個人データの越境移転枠組みに関する日EU相互認証（個人情報保護委員会がEUを「わが国と同等の水準にある個人情報保護制度を有する国」であることを、また、欧州委員会がわが国を「十分な個人情報保護の水準が保障されている国」であることを、相互に認め合うことにより、日EU双方向での個人データの円滑な流通を確保すること）に向けた対話の終結を確認し、両委員による共同プレステートメントを公表した。

2016年の春を端緒とし、同年７月の個人情報保護委員会による決定「個人データの円滑な国際的流通の確保のための取組について」によって本格的な取組方針が確認され、２年以上にわたって行われてきたこの対話は、わが国事業者がEUと関連する事業を展開するにあたって必然的に伴うこととなる、日EU間の個人データの越境移転に係る負担を軽減し、わが国事業者の積極的な事業展開を後押しすることが目的であった。この目的を達成することは、2018年７月に署名され、発効に向けて手続が進められている日EU経済連携協定を補完することを意味し、これによる日EU間の貿易・投資促進効果を一層強化する効果が期待されるところである。

（１）EUの越境移転規制と十分性認定の重要性

EUにおいては、GDPR（一般データ保護規則）が2018年５月25日に適用開始される以前、データ保護指令（およびこれに基づきEU加盟各国で制定・施行されていたデータ保護法）の時代から、EU域内から域外への個人データの移転が厳しく制

限されてきた。データ保護指令における個人データの越境移転規制を基本的に受け継いだGDPRにおいては、

①十分な個人情報保護の水準が保障されていることを欧州委員会が認めた国への移転であること

②欧州委員会が認めた標準データ保護条項やデータ保護機関の承認を受けた拘束的企業準則によって、移転先事業者における適切な個人情報保護を確保すること

③本人の明示的な同意を得ること

という３点が、主な移転ツール（EU域内から域外へ個人データを移転するために依拠することのできる法的根拠）として用意されている。

つまり、日EU相互認証が発効するまでの間は、わが国の事業者がEU域内からわが国に個人データを移転する場合（たとえば、EUを含む海外現地法人の従業員に関する情報や、全世界の顧客に関する情報を日本の本社に一元管理するといった場合が考えられる）には、主に標準データ保護条項、拘束的企業準則または本人同意のいずれかに依拠する必要がある。一方で、標準データ保護条項または拘束的企業準則に依拠するにあたっては、これを適法に行うために、現地法律事務所への相談を経るなど、少なからぬ負担が生じているものと思われ、また、本人同意についても、GDPRにおいては本人の自由な意思に基づくものであること等の要件が定められており、またいつでも撤回が可能とされていることも踏まえると、EUからわが国への個人データの移転を必要とする事業者の負担の軽減や、地位の安定のために、いわゆる十分性認定を受けることの重要性が指摘されていた。

（２）個人情報保護法の改正と相互の同等性評価の枠組み

これまでに欧州委員会によって行われてきた「十分な個人情報保護の水準が保障されている国」の認定は、いずれも欧州委員会が相手国の個人情報保護の水準を評価するというものであったが、今般の個人情報保護委員会の取組は、2017年５月30日に全面施行された改正個人情報保護法において、

①わが国と同等の水準にある個人情報保護制度を有すると個人情報保護委員会が認めた国（※）への移転であること

②個人情報保護法に基づき個人情報取扱事業者が講ずべき措置を継続的に講ずるための体制を整備している者への移転であること

③外国にある第三者に対する提供について本人の同意を得ること

という３点が、国内にある第三者に対して提供する場合と同様に、個人データを提供するための条件として設けられ、越境移転規制について、個人情報保護法がGDPRと比較的似た制度的フレームワークを有することとなったことを契機として、日EUが対等の立場で相互に相手方における個人情報の保護について評価し、その同等性を見出すというものである。

（※）なお、①については、2017年12月７日から2018年１月５日までパブリックコメントの募集を行った上で、５月９日に「個人情報の保護に関する法律施行規則の一部を改正する規則」が公布・施行され、わが国と同等の水準にある個人情報保護制度を有する国と認められるための具体的な要件が定められた。

当然のことながら、個人情報の保護に関する法制度は、その国の文化や社会を背景とするものであるがゆえに、国ごとに規律の内容が異なり得る。そして、このことはわが国とEUについても同様であり、個人情報保護法とGDPRには大小さまざまな差異がある。個人情報保護委員会と欧州委員会の２年以上にわたる対話の多くは、これら差異を前提として、両者の同等性を見出すため、法制度とこれによる個人情報の保護の状況についての相互理解にあてられた。その結果、個人情報保護法についての次の５つの規律整備を行うことにより、日EU双方において同等に個人情報の保護が図られるとの共通理解に至った。

①GDPRにおいて、原則として取扱いが禁止される特別な種類の個人データに該当する「性生活、性的指向または労働組合に関する情報」について、要配慮個人情報と同様に取り扱うこととする

②６カ月以内に消去することとなる個人データについても、開示請求権等の本人の権利行使の対

象に含める

③個人データの提供を受けた第三者において、提供元によって特定された利用目的による制限を受けることとする

④外国にある第三者への提供について、本人の同意を根拠とする場合には、本人が同意に係る判断を行うために必要な移転先の状況についての情報を提供することを要することとし、提供先による体制の整備を根拠とする場合には、契約その他の形式の拘束力のある取決めまたは企業グループにおける拘束力のある取扱いによって提供先における適切な体制の整備を確保することを要することとする

⑤匿名加工情報として取り扱う場合に、GDPRにおける匿名データと同様に、加工方法に関する情報を削除することにより、匿名化された個人の再識別の可能性を排除することとする

この５つの規律について、個人情報保護委員会は、2018年４月25日から５月25日までパブリックコメントの募集を行った上で、９月７日に「個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」（平成30年個人情報保護委員会告示第４号）を公布した。この「補完的ルール」については、欧州委員会がGDPR第45条に基づき行う、日本が個人データについて十分な保護水準を確保しているとの決定が効力を生ずる日から施行することとされている。

〈参考〉個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール

【EUから十分性認定に基づいて移転した個人データのみに適用】

項　目	現行法令	内　容	実務への影響
要配慮個人情報の範囲	「性生活」、「性的指向」、「労働組合」に関する情報は、要配慮個人情報に該当しない。	「性生活」、「性的指向」、「労働組合」に関する情報を、要配慮個人情報と同様の取扱いとする。	そもそもこのような情報がEUから移転されてくることは想定されず、影響は大きくない。
開示請求権	６か月以内に消去することとなる個人データについては認められない。	国内法上は、６か月を越えて保有する個人データのみ対象となっているが、６か月以内に消去することとなる個人データも同様に請求に応じることとする。	保有期間にかかわらず請求に応じている企業は多い。 また、そもそも６か月以内に消去することとなる個人データがわざわざEUから移転されてくることは想定しにくい。
利用目的の承継	ー	第三者から提供を受ける個人データを、提供元が特定した利用目的の範囲内で、利用することとする。	企業においては当然対応していると想定される。
日本から外国への個人データの再移転	①本人の同意がある場合、 ②移転先のデータ保護が確保されている場合、 ③提供先が個人情報保護委員会が指定した外国に所在する場合に提供可能。	左記②について、提供先の事業者における体制整備を根拠として、外国へ個人データを移転する場合には、契約等により個人情報保護法と同等の保護を確保することとする。	企業においては当然対応していると想定される。
匿名加工情報	加工方法に関する情報が残存している場合でも、安全に分離保管されていれば匿名加工情報として扱われる。	匿名加工情報として扱う場合、加工方法に関する情報を削除することにより、何人にとっても再識別を不可能とする。	仮IDを付与しての時系列分析を行うことはできなくなるが、現時点において、EUから移転した個人データとの混合分析について強いニーズがあるとは考えにくい。

2017年12月の委員同士の会談において、双方の制度間の関連する相違点に対処するための解決策として、EUから日本へ移転された個人情報に係る補完的ルールの策定について合意したことを踏まえ、当該ルール案を作成した。意見募集を実施（2018年５月25日募集終了）し、意見を踏まえた修正を行い、官報に掲載した（2018年９月７日）。

（3）今後の予定

今後は、個人情報保護委員会と欧州委員会それぞれにおいて、相互認証の発効に向けて必要な内部手続きを進めていくこととなる。

具体的には、個人情報保護委員会側の手続として、個人情報の保護に関する法律施行規則第11条第１項各号所定の要件に照らして「わが国と同等の水準にある個人情報保護制度を有する国」としてEUを指定すること、欧州委員会側の手続として、日本に対する十分性認定について、その案に対する欧州データ保護会議の意見を聴取し、正式決定を行うこと等がある。

これらの手続が完了し、日EU相互認証が実現した暁には、前述の補完的なルールを遵守することを条件として、標準データ保護条項や拘束的企業準則によることなく、EU域内からわが国に対して個人データを安定的に移転することができるようになることが期待される。

個人情報保護委員会としては、早期に枠組みの運用が可能となるよう、引き続き取り組んでいきたい。

参考URL（2018年11月時点）

・個人情報保護委員会
https://www.ppc.go.jp/
・個人情報保護法について
https://www.ppc.go.jp/personalinfo/
・法令・ガイドライン等
http://www.ppc.go.jp/personal/legal/
・認定個人情報保護団体
https://www.ppc.go.jp/personal/nintei/
・欧州各国との対話実績
https://www.ppc.go.jp/enforcement/cooperation/cooperation/dialogues-Europe/

Ⅰ-2 「情報銀行」について

総務省　情報流通行政局情報通信政策課

はじめに

IoT等の技術の発展により、さまざまなデータの蓄積などが可能になり、新たなサービスの創出による生活の利便性の向上が期待されている。

現在でも、個人が生活の中で各種サービスを利用する際、プロフィール、位置情報、購買履歴、検索履歴等の個人情報が企業によって収集され、その一部は第三者に提供されている。この場合、個人情報保護法に基づき企業が消費者の同意を取得してはいるが、実態として消費者本人の意識が十分ではないケースがある。結果として、消費者側は、第三者提供に同意したと意識していない、何に使われているか十分に理解していない、第三者提供をやめさせる方法がわからないといった不安を抱えており、企業側には、消費者が同意内容を正確に理解しているか不安、レピュテーションリスクからデータの利活用を進められないなどの問題が出てくる。こうした状況を踏まえ、個人側・企業側の双方が安心できる形で個人情報の流通、活用を進める仕組みとして、「情報銀行」に関する検討が進められてきた。

本稿では、「情報信託機能の認定に係る指針Ver1.0」（以下「指針」という。）の公表までの検討状況を中心に、「情報銀行」に係る総務省等の取組みについて概要を記載する。

1．「情報銀行」に関する検討の経緯および関連動向

1-1.「情報銀行」に関する政府等における検討

（1）データ流通環境整備検討会における検討

2016年９月より、内閣官房IT総合戦略室において開催された「データ流通環境整備検討会」の下の「AI、IoT時代におけるデータ活用ワーキンググループ」では、特に個人情報を含むパーソナルデータの流通・活用について検討が行われた。2017年２月にとりまとめられた「中間とりまとめ」では、パーソナルデータの流通を実現させるために有効な仕組みの一つとして、個人の関与の下でデータの流通・活用を進める「情報銀行」が挙げられている。ここで「情報銀行」は「個人とのデータ活用に関する契約等に基づき、PDS等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、データを第三者（他の事業者）に提供する事業」と定義されている。（図１）

（2）情報通信審議会における検討

総務省の情報通信審議会情報通信政策部会の下の「データ取引市場等サブワーキンググループ」では、本人に代わって個人情報を管理・提供する情報銀行の機能を「情報信託機能」と定義し、この機能の提供に対するニーズが高まってくることから、その信頼性を確保するための社会的な仕組みが必要とされた。

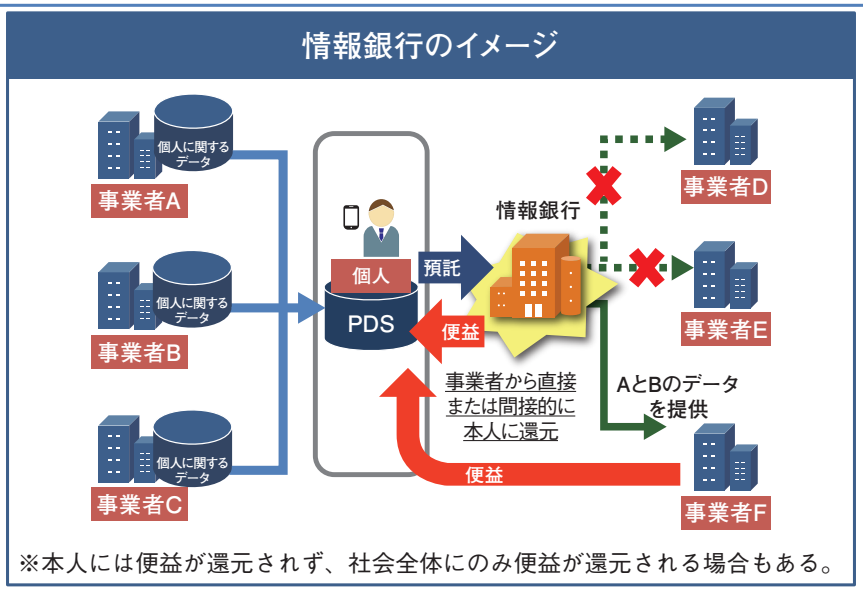
さらに、現段階で、情報信託機能を担うビジネスを行っている事業者はなく、今後事実関係をさらに積み上げていく必要があると考えられること、また、今後の発展が期待される市場については、当事者が実態に即したルールを形成していくことが望ましいとの観点から、国による認定等の法制度整備ではなく、民間の団体等によるルールの下、任意の認定制度が実施されることが望ましいとされた。

1-2. その他の関連動向

（1）国内制度の動向

2016年12月に公布施行された「官民データ活用推進基本法（平成28年法律第103号）」第12条に「個人に関する官民データを当該個人の関与の下で適正に活用することができるようにするための基盤の整備」が盛り込まれ、データの適正かつ効果的な活用の推進が求められた。

情報銀行（情報利用信用銀行）とは、個人とのデータ活用に関する契約等に基づき、PDS等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、データを第三者（他の事業者）に提供する事業。



「AI、IoT時代におけるデータ活用ワーキンググループ　中間とりまとめの概要」（内閣官房IT総合戦略室）より作図

図1　「情報銀行」とは

（2）海外制度の動向

欧州連合（EU）では、一般データ保護規則（GDPR）が2018年５月に施行され、データポータビリティ権に関する規定が創設されるなど、個人に係るデータの保護を強化しつつ、本人の意思を重視したデータ活用を実現しようとする流れが見られる。

2.「指針」の検討と公表

2-1. 検討経緯

1.1-1.（2）の情報通信審議会におけるとりまとめを受け、総務省および経済産業省において「情報信託機能の認定スキームの在り方に関する検討会」（以下「検討会」という。）を2017年11月から18年４月の間に６回開催し、「指針」をとりまとめた。

「指針」は、一定の水準を満たす事業者を認定し、社会的な信頼性を確保することを目的としているため、認定を必須とするものではなく、当該認定によって消費者が安心してサービスを利用するための判断基準を示すという観点から作成されている。この観点から、特にポイントとなるのは、消費者個人を起点としたデータの流通（コントロールできる機能の充実）、消費者からの信頼性確保である。これらの主な論点について、「検討会」では以下のようにとりまとめている。

（1）利用者がコントロールできる機能

「検討会」においては、情報銀行の普及を促進する目的に照らし、個人情報に関する個人のコントローラビリティを確保することが重要である一方で、情報銀行が市場に登場し、競争する環境を整備することが重要であることから、コントローラビリティとサービスの多様性のバランスを考慮し、認定基準を検討した。「指針」においては、操作が容易なユーザインターフェイス（UI）の提供により、以下の機能を実現することが認定要件とされている。

1）情報銀行は、個人情報の提供先、利用目的、データ範囲について、個人が選択できる選択肢を提供すること
2）個人が、個人情報の第三者提供の履歴を閲覧できること（トレーサビリティ）
3）個人が、情報銀行に委任した個人情報の第三者提供および利用を停止させることができること（同意の撤回）

4）個人が、情報銀行に委任した保有個人データの開示の請求（個人情報保護法第28条に基づく請求）を容易に行うことができること

（2）消費者からの信頼性確保

「検討会」では、情報銀行の信頼性を確保するとの観点から認定基準を検討しており、消費者が安心して利用できるようにするための主な認定要件として以下を定めている。

1）データ倫理審査会（仮称）の設置

各情報銀行において、社外委員を含めさまざまな観点から、データ利用に関して定期的に報告し、チェックする体制を整備すること。

2）個人情報の提供の制限

情報銀行が個人情報を提供した提供先の第三者からの再提供について禁止するとともに、個人が求めた場合、当該個人情報の第三者提供・利用を停止すること。

3）損害賠償責任について

情報銀行が個人情報を第三者提供した提供先の第三者において情報漏えい等の問題が生じることも考えられるが、個人に対しては、情報銀行が苦情相談窓口を設置して一義的な説明責任を負うとともに、損害が生じた場合には個人に対する賠償責任を負うこと。（提供先第三者に対しては、必要に応じ情報銀行から求償。）

2-2.「指針」の構成

「指針」は、（1）情報信託機能の認定基準、（2）情報信託機能のモデル約款の記載事項、（3）情報信託機能の認定スキームから構成されている。

それぞれの概要は以下のとおり。

（1）情報信託機能の認定基準

情報銀行の認定基準は、「指針」に基づき認定を行う団体（以下「認定団体」という。）が認定を行うための基準として、認定を受ける情報銀行が満たすべき要件を示している。認定基準の構成および概要については以下のとおりである。

1）事業者の適格性

①経営面の要件、②業務能力について要件を定めている。業務の健全な遂行や、損害賠償請求が発生した場合の対応について適切に行うことができるような体制・能力をもつことが要件とされている。

2）情報セキュリティ等

情報銀行は個人情報を取り扱うことを業務とするため、適切なセキュリティ・プライバシー体制が取られることが求められる。プライバシーマークまたはISMS認証を取得していることを基本とし、必要なガイドライン等を遵守することなどが要件とされている。

3）ガバナンス体制

「指針」の目的である、消費者からの信頼性確保ということを担保するため、データ倫理審査会（仮称）によるチェック体制を整備することが要件とされているほか、消費者による相談を受け付ける体制の設置や透明性の確保なども求められる。

4）事業内容

情報銀行は、個人に代わって個人情報を取り扱うことから、主に個人情報保護法を遵守した適切な同意取得と、個人のコントローラビリティを高めるための機能提供について条件を設けている。

（2）情報信託機能のモデル約款の記載事項

「指針」においては、情報信託機能を提供する「情報銀行」のサービスについて、債権債務の内容や情報銀行の責任範囲を明確化するため、個人と情報銀行の間を委任関係に関する契約上の合意と整理することとされている。

この委任関係を、より個人のコントローラビリティを確保した、消費者個人を起点としたサービスの実現に資するものとするため、個人への便益や委任の内容などの具体的条件を契約関係として整理する標準的な契約条項を、（1）認定基準にも沿う形で「モデル約款の記載事項」として示している。特に、委任関係の内容を契約等でわかりやすく整理し、個人情報保護法上の第三者提供においても有効な包括的同意（または個別同意）を取得できるよう整理することが重要となる。

各認定団体は、本「モデル約款の記載事項」に準

ずるモデル約款を各認定団体で作成することとし、モデル約款に記載すべき事項についてとりまとめた。

（3）情報信託機能の認定スキーム（図２）

情報信託機能の認定スキームでは、認定団体が適切に認定を行うための認定スキームとして、以下について整理している。

1）認定団体の適格性
2）認定する際の審査の方法
3）認定証について
4）認定事業者が認定内容に違反した場合、個人情報漏えいが起こった場合の対応
5）認定団体と認定事業者との間の関係
6）認定団体の運用体制

3. 情報銀行の普及に向けた今後の展開

3-1.「指針」に基づく認定制度の開始に向けた動き

「指針」に基づき、一般社団法人日本IT団体連盟（以下「IT連」という。）において、情報銀行の認定を行うことが９月12日に発表されている。IT連では新しく、情報銀行推進委員会を設置し、今秋以降、情報銀行の認定事業や普及啓発活動を行うこととしている。10月19日には、認定に関心のある事業者等を対象に、IT連による認定事業や普及啓発活動についての説明会が行われ、200社400名以上が参加した。

IT連は、IT産業に関わる日本最大級のIT団体の連合体であり[1]、IT連が認定団体として今後認定を行っていくことで、「指針」の趣旨にあるとおり、情報銀行の社会的な信頼性が高まり、情報銀行の普及が大きく進むことが期待される。

3-2. 情報銀行の実証事業

総務省では、情報銀行の実証事業を通じてモデルケースの創出と、情報銀行の要件や関係者間に必要なルール等の検証、課題の抽出等を行い、パーソナルデータの流通・活用の促進を図るため、2018年度の新規の予算事業として「情報信託機能活用促進事業」を実施している。情報銀行については、５件の実証事業を採択しており、今後実証を通じて、情報銀行のサービスの具体化などが進むことが期待される。

また、「指針」をとりまとめた時点では情報銀行

1　加盟団体に所属する企業以外に対しても認定を行う予定。

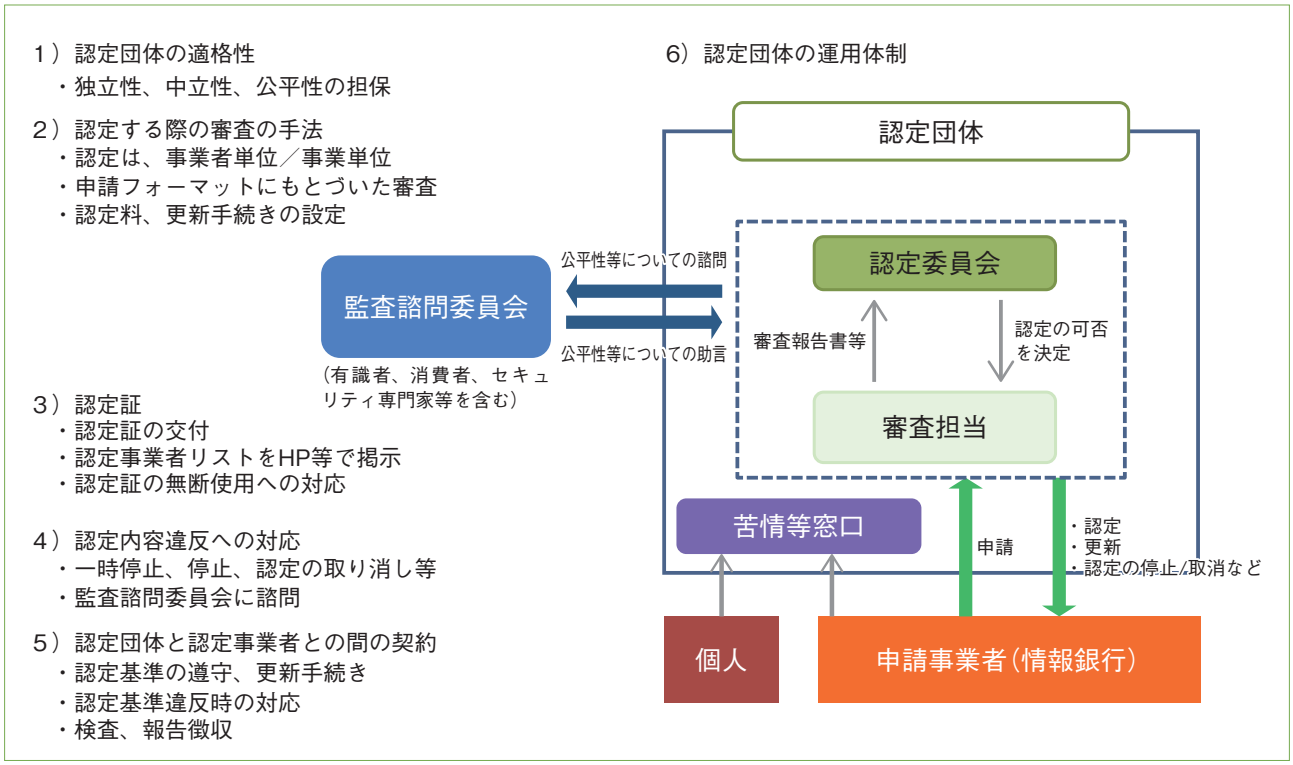


図2　認定団体の運用スキーム

は存在していない中での検討であったため、実証事業における具体的なサービスを通じて「指針」の内容についても検証し、必要に応じて追加検討に繋げることとしている。

3-3.「指針」の見直し

「指針」は、早期のサービス実証を見据えてver1.0として取りまとめを行ったが、今後も、3-2.の実証事業やその他の新たなサービスの展開、関連制度の運用状況等を踏まえ、継続して議論・見直しを行っていくことが求められる。特に、現在要配慮個人情報として一部が認定の対象外となっている医療・健康分野と、キャッシュレス化の進展を受けてデータの利活用の進展が期待される金融分野についてはニーズが高いため、2018年９月から、「検討会」のもとに金融分野、医療・健康分野のワーキンググループを設置し、追加的な検討を開始しているところであり、今後、「指針」のver2.0への見直しに繋げていくことを予定している。

3-4. 終わりに

今後、「指針」とIT連による認定事業により、情報銀行の信頼性が高まることや、実証事業を通じたサービスの具体化などにより、情報銀行の事業が多様な展開を見せていくことが期待される。

参考URL（2018年11月時点）

・情報信託機能の認定スキームの在り方に関する検討会『情報信託機能の認定に係る指針ver1.0』
http://www.soumu.go.jp/main_content/000559366.pdf
・一般社団法人日本IT団体連盟『情報銀行認定事業開始について』
https://www.itrenmei.jp/registration/

Ⅰ-3 JIS Q 15001:2017改正のポイント

一般財団法人日本データ通信協会　Pマーク審査部長
兼　電気通信個人情報保護推進センター（認定個人情報保護団体）所長
JIS Q 15001改正原案作成委員会　委員
小堤（おづつみ）　康史（やすし）

2017年12月20日に改正されたJIS Q 15001（JIS Q 15001:2017、以下「2017年版」という。なお、改正前のものを「2006年版」という。）は、2015年９月に改正され、2017年５月30日に全面施行された個人情報保護法（以下「改正法」という。）に合わせることを主な目的としている。以下では、これらを概観する。

１．改正の経緯、目的

工業標準化法の下で日本工業規格を制定する主務大臣は、JISの種類に応じて、経済産業大臣をはじめとして、国土交通大臣、文部科学大臣、総務大臣、環境大臣、厚生労働大臣、農林水産大臣である。JIS Q 15001「個人情報保護マネジメントシステム－要求事項」も、経済産業大臣を主務大臣として検討が行われ、改正された。

改正の対象は、2006年版のJIS Q 15001（厳密にいえば、2010確認版）である。

2016年秋から改正の検討が行われ、最終的に2017年12月20日に改正された。

検討体制は、規格書の解説４に記されており、それによれば「JIS Q 15001改正原案作成委員会」が組織化され、その中の一部メンバーがJIS Q 15001改正作業部会委員として任命され、経済産業省商務情報政策局情報経済課等を関係者とし、JIPDECが事務局であった。

今回の改正の趣旨は、規格書の解説２に要約が記されている。一部言回し等を改め、箇条書きにすると、以下のようになる。

①この規格のマネジメントシステム規格としての位置づけを明確化した。
②改正個人情報保護法に対応する管理策を追加した。
③2006年版の規格の解説の内容を精査して、附属書（参考）とした。
④要求事項の基本的な考え方を変更せず、今回の規格の改正が不適合を生じないように配慮した。

この明快な説明に対して蛇足となるが、あえて噛み砕いて説明すると、以下のようになる。

つまり、改正法の完全施行によって、それまでの分野ごとの主務大臣制から、個人情報保護委員会による法執行に一本化されることとなり、大きく舵が切られた。

従前、個人情報保護法の法執行を行うためのガイドラインとして、経済産業省においては「経済産業分野を対象とするガイドライン」が作成・公表されていたが、改正法の施行に合わせて、このガイドラインは廃止となった。

JIS Q 15001は、最初の個人情報保護法の施行直後の2006年版によって“個人情報保護法に基づく個人情報保護ルールおよびマネジメントシステムを併せもった規格”とされていたところ、この前半部分である“個人情報保護法に基づく個人情報保護ルール”の法執行が個人情報保護委員会に移動したことから、その部分について根拠を失ったことになる。

そこで、2017年版では個人情報保護法の条文の解釈と執行は個人情報保護委員会である、としつつ、マネジメントシステム部分を規格として維持することに専念する必要があった。ただし考え方の継続性について十分な配慮が必要であり、これを可能な限り実施した。これが上記の趣旨である。

ここは、2017年版を読み解く「鍵」となっているので、あえて紹介させていただいた。

2．改正のポイント

一見して、2006年版と2017年版には大きな違いがある。それは規格の構造に大きな変化が生じていることである。また、用いられている用語にも違いがある。さらにより本質的な違いとして内容にも変化が生じている箇所がある。

以下では、このそれぞれに分けてみることにしよう。

(1) 規格の構造の変化

2006年版は「規格本文」と「解説」の二編で構成されていた。もちろん「解説」は規格そのものではなく、規格の一部をなしているものでもない。なお、2010年頃に「解説」の見直しが行われ、解説内容の大幅な拡充が実施された経緯がある。

2017年版で採用された構造は、「規格本文」「附属書A」「附属書B」「附属書C」「附属書D」の５編となっている。これだけを見ると大きな違いとなっていると感じることだろう。

しかも複雑なことに、2006年版の「規格本文」と2017年版の「規格本文」は、簡単に比較ができないほどの変貌を遂げた。それもそのはずで、2017年版ではJIS Q 27001:2014の「規格本文」を、“情報セキュリティ”を“個人情報保護”に変更した以外はほとんどそのままで用いて、2006年版から見るとまるで借り物のようなものが「規格本文」となったのである。これは、マネジメントシステム規格の共通テキスト化、という考え方に基づく。2006年版の精通者にとっては、今後、慣れが必要であろう。一方、JIS Q 27000シリーズ等他のマネジメントシステムの精通者にとっては、座りが良い改正となったと感じられたことだろう。

それでは2006年版の「規格本文」はどうなったか、というと、これが基本的には2017年版の「附属書A」（規定）となったのである。ただし、本文に対して管理策と称することになった。JIS Q 27000シリーズでは、管理策を選択することが可能で、「適用宣言」という概念で整理されているが、2017年版では、この「適用宣言」という概念は採用されていない。なぜならば2006年版において「規格本文」に対する選択の余地はなく、2017年版の管理策となっても同様だからである。ただし、第三者提供の有無、共同利用の有無、匿名加工実施の有無など、実質的に選択の余地がある管理策もあるので、ここは若干の留意（運用上の配慮）が必要と考える。

同様に2006年版の「解説」は2017年版では原則として「附属書B」（参考）となっている。これらによって、“要求事項の基本的な考え方を変更せず、今回の規格の改正が不適合を生じないように配慮”されていることになる。

2017年版の「附属書C」（参考）は、これも借り物のように、JIS Q 27002:2014の「規格本文」そのものを、ほぼ「情報」を「個人情報」と読み替えて作成されている。その主な理由は、「経済産業分野を対象とするガイドライン」が廃止されたことによる。

2006年版の解説に“安全管理措置については、同ガイドライン等を参考にした対策を講じる必要がある”とあった。そのリンク先が廃止されてしまったために、今後のリンク先をどうするか議論が行われた結果である。個人情報保護委員会のガイドライン（通則編）の示す安全管理措置とする考えもあったし、JIS Q 15001として独自に整理する考え方もあった。しかし、結論としては、これまでの事業者の取組み状況を踏まえると、比較的高い水準を示す必要もあり、独自に整理するにしては今後の見直しの保証ができるのか、といった課題も感じられたために、JIS Q 27000シリーズをそのリンク先として選んだ格好となった。

2017年版の「附属書D」（参考）は、「新旧対応表」となっているので、2006年版に精通している方が2017年版を読み解くためには役に立つだろう。

(2) 用語の変化

全般的に改正法の用語に合わせた見直しが行われ

ている。

たとえば、JIS Q 15001においては、用語として「個人情報」のみが用いられていたが、個人情報保護法に合わせて「個人データ」も用いられることになった。ただし、事業者の取組みを引き下げることが趣旨ではないので、若干の補正が行われている。（A.3.3.1の注記）

同様に、JIS Q 15001においては、用語として「開示対象個人情報」という用語が用いられていたが、こちらも個人情報保護法の用語である「保有個人データ」が用いられることになった。ただし、こちらも同様に、事業者の取組みを引き下げることが趣旨ではないので、若干の補正が行われている。（A.3.4.4.1の注記）

その他、「特定の機微な個人情報」という用語に代えて、「要配慮個人情報」が用いられることになった。こちらは、そもそも定義に遡って違いがある（ただし、考え方によっては些細な違いである）ために、個人情報保護マネジメントシステムへの実装にあたっては、要配慮である（単に用語の置き換えだけではない、という意味において）。

改正法とは関係なく見直されたところもある。

たとえば、「事業者」という用語は「組織」に置き換わった。これについて実は原案作成段階と、最終的に公表された2017年版とには差がある。

2017年版では、“組織”は、個人情報保護法に定める“個人情報取扱事業者を意味する”（1. 適用範囲）。しかしこのフレーズは、2017年９月に公表された「パブコメ版」にはなかったため、そのあとに追記されたことが明らかである。JISといえども、法律への適合が必要であることは自明なので反論のしようもないが、規格としては柔軟性を失った、といわざるを得ない。（たとえば、地方自治体の中の一部門である「交通局」「水道局」などを単位としたマネジメントシステムとしての取組みに支障が生じないか、など。）この点は、他のマネジメントシステム規格にはない制約であるため、留意が必要である。

その他、「トップマネジメント」「残留リスク」などは、JIS Q 27000シリーズ等で用いられている用語との整合を行ったためである。ただし、マネジメントシステムによって、微妙な歴史的経緯を持っている場合もあるので、単に用語の置換えなのか、それとも、用語の持つ概念のレベルまでを考慮すべきか、規格の利用者にとって少々悩ましいかもしれない。

（3）内容の変化

内容に変化が生じた主な要因の一つは、改正法対応である。これは、そもそもJIS改正の主な趣旨である。

改正法の成立過程においては、「名簿事業者規制」「個人情報の海外移転」「データの利活用」等も検討され、それぞれの条文に定着化された。そこで、2017年版でも当然ながらこれらが踏襲され、実装されている。

典型的なところでは、A.3.4.2.8.1「外国にある第三者への提供の制限」、A.3.4.2.8.2「第三者提供に係る記録の作成など」、A.3.4.2.8.3「第三者提供を受ける際の確認など」、A.3.4.2.9「匿名加工情報」、そしてA.3.4.2.3「要配慮個人情報」もそうである。これらはいずれも改正法由来であるので、対応が必要な組織においてはすでに（2017年版が出る前に）対処が終わっているところと考えられる。

直接書面取得とそれ以外（2006年版の3.4.2.4と3.4.2.5）の関係も、個人情報保護法の条文の並び順に整合させるために、A.3.4.2.4「個人情報を取得した場合の措置」とA.3.4.2.5「A.3.4.2.4のうち本人から直接書面によって取得する場合の措置」に書き改められた。2006年版では3.4.2.4と3.4.2.5がいわば並列的な関係であったが、2017年版では、A.3.4.2.4が全体の管理策、そのうち直接書面取得時の管理策がA.3.4.2.5となっている。本質は変わらないのだが、一見しただけでは番号の入れ替えがあったように読めてしまうので、ここも留意が必要かもしれない。

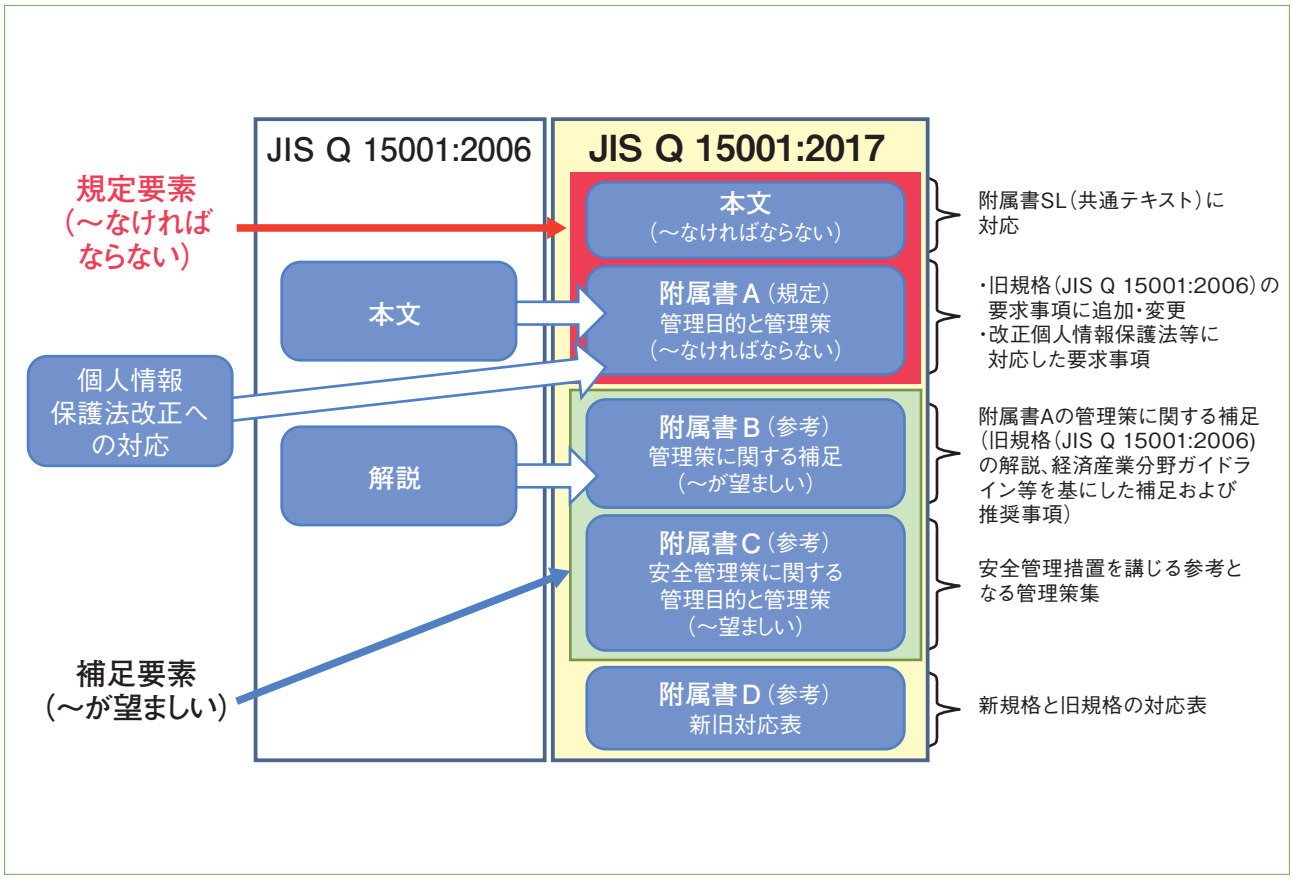


図1　JIS規格2006年版と2017年版の比較

出典）JIPDEC個人情報保護研修会2018「テーマ1　JIS改正にともなう審査基準の改定について」資料p10

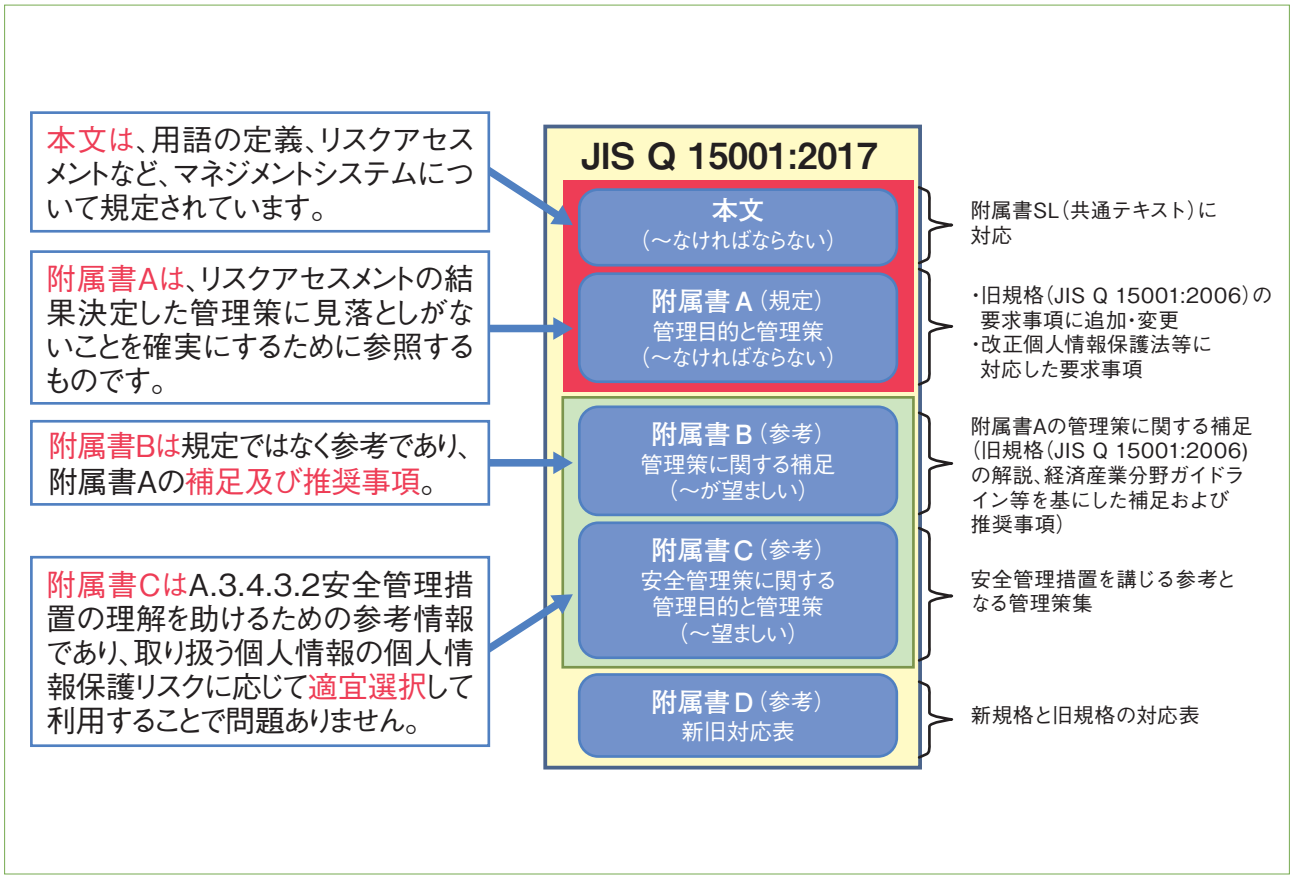


図2　新規格（JIS Q 1500:2017）の文書体系

出典）JIPDEC個人情報保護研修会2018「テーマ1　JIS改正にともなう審査基準の改定について」資料p11

一方、独自に検討した結果で内容に変化が生じたところもある。

たとえば、2006年版の3.2「個人情報保護方針」が、2017年版ではA.3.2.1「内部向け個人情報保護方針」、A.3.2.2「外部向け個人情報保護方針」と二つの管理策に分離された。これは、組織の内部に向けた方針と外部に向けた方針とでは、その目的も趣旨も（微妙に）異なる可能性を考慮したものである。その意味を理解したうえで、内部向けと外部向けを従来同様同一のものとするのか、または分離するのかは、個々の組織の判断となることであろう。

3. 参考書籍等

2017年版の解説書としては、新保史生編著「JIS Q 15001:2017 個人情報保護マネジメントシステム要求事項の解説」（2018年、日本規格協会）が出版されている。その第１章の中で、「1.3　JIS Q 15001改正の経緯」として、その背景、改正の趣旨、改正された規格の構造が詳しく説明されている。

本書は、タイトルのとおり、2017年版の深い理解をするために必読の書である。

また、JIPDEC編「JIS Q 15001:2017対応　個人情報保護マネジメントシステム導入・実践ガイドブック」（2018年、日本規格協会）も出版された。こちらは、2018年１月に公表された「プライバシーマーク付与適格性審査基準」（審査項目、確認方法・エビデンス、留意事項）に、規格等との関係、実施上のポイントが追加記載されている。その第一部の中で、「2. JIS Q 15001:2017の構成と主な改正点」として、詳しく説明されている。こちらも2017年版を理解するうえでは、ぜひ参考にされたい。

ついでに、筆者は一般財団法人日本データ通信協会の職員であるので、以下も紹介させていただく。弊協会では、「日本データ通信」と称する機関誌を発刊している。その通巻219号（2018年７月号）で、『特集「“JIS Q 15001改正”」～個人情報保護とPマーク審査業務への影響～』として、現JIPDEC（元 経済産業省商務情報政策局情報経済課　法執行専門官）の篠原氏、および弊協会のメンバーで、改正に至る経緯、改正に伴う実務対応、審査基準はどう変わるか、を分担執筆し掲載した。弊協会のホームページにも掲載しているので、一読いただければ幸いである。

URLは以下のとおり（2018年11月時点）。

https://www.dekyo.or.jp/info/2018/07/（Web版）

Ⅰ-4 認定個人情報保護団体としての役割について

JIPDEC　認定個人情報保護団体事務局長　**篠原 治美**

1．はじめに

JIPDECは、2005年６月に「個人情報の保護に関する法律」に基づき、経済産業大臣および総務大臣より認定個人情報保護団体として認定を受けている。

さらに、2015年９月３日に成立し、2017年５月30日から全面施行された改正個人情報保護法で求められている個人情報保護指針について、施行日同日に個人情報保護委員会に届け出ている。改正法では今まで以上に認定個人情報保護団体の役割に大きな期待がかかっていることは個人情報保護委員会からも発信されているが、当協会においても、認定個人情報保護団体としての役割の重要性が増してきている。

2．認定個人情報保護団体の対象事業者になることのメリット

個人情報保護法の改正に伴い、個人情報を取り扱う事業者の範囲が拡大した。

さらに、匿名加工情報の作成など、事業者に判断が委ねられる場面が増えている。そうした中、当協会の対象事業者になることにより、以下のようなメリットがあり、消費者にとっても信頼性が高まる。

- 認定個人情報保護団体が第三者機関として関与することで迅速・円滑な苦情の解決が期待できる。
- 認定個人情報保護団体から適切な情報が提供されることによって、適切な個人情報保護の取組みが維持できる。
- 個人情報等の事故が発生した場合、当協会の監督の元で適切な指導等が行われるため、法律に基づいた立入り検査権限による権限行使がいきなり行われるということがなくなる。（例外あり）
- 個人情報の取扱いや、匿名加工情報の作成等、特性に適した方法で扱うための相談ができる。

3．匿名加工情報

当協会では、個人情報保護法の改正において新たに法定された匿名加工情報について、施行前から啓発活動を推進している。

特に、匿名加工情報に関する事業者ヒアリングや事業者相談を元に作成した匿名加工情報の事例集は、多くダウンロードされ、事業者において一定の参考になっている。

匿名加工情報は、具体的な加工方法は事業者の競争力や営業秘密などにあたる場合があることも確認されていることから、個人情報保護委員会ガイドラインを遵守することとしたうえで、細かな加工方法は事業者の判断に委ねる方式を採用している。

このため、当協会では、事業者から具体的な匿名加工のルール作成等の相談を受け付け、必要に応じ審議する体制を整備した。

そこで対象事業者向けに、匿名加工情報の検討会を開催し、その取扱いに助言等を行い、安全な利活用が促進されるように支援を行っている（図1）。

事例集を含め、「匿名加工情報」に関する支援については以下のサイトで紹介している。（2018年11月時点）

https://www.jipdec.or.jp/protection_org/anonymously_processed.html

匿名加工情報は、目的を持って利用されることで付加価値向上や経済活性化に寄与するものと考えられることから、当協会では以下が重要と考える。

- **匿名加工情報の取扱いにあたっては、十分なリスク分析を行うこと。**
- **匿名加工情報の取扱い、苦情処理に必要な措置を執り、公表すること。**

匿名加工情報は、個人情報保護委員会規則等に基

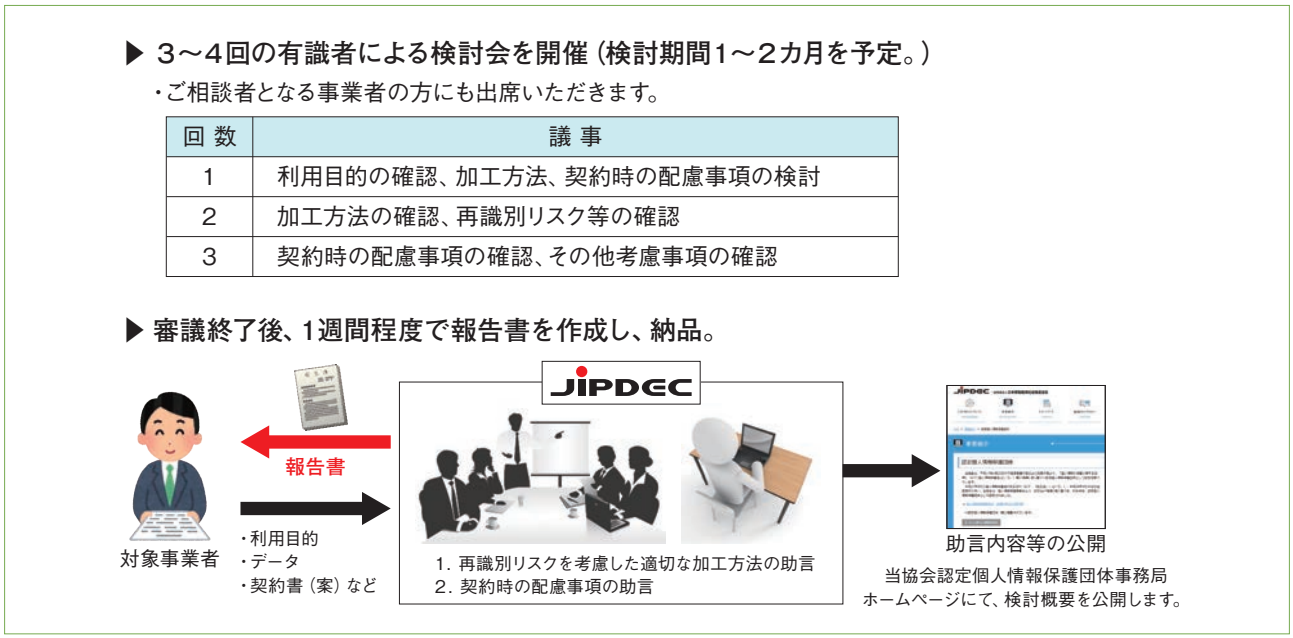


図1　JIPDEC匿名加工情報支援策の概要

づき、本人を特定できないよう加工することによって、個人情報の枠外に置き、利用目的・第三者提供の制限を受けることなく自由に利活用できるようにするものであるが、その目的に応じて加工方法が異なるため、事例を公開し、相談窓口を設置し、オーダーメイド的な対応を行う必要がある。

改正法以前から、統計情報として利用していたものを匿名加工情報の定義に当てはめて過剰に対応しようとする事例も見受けられる。

事業者が、適正に加工していると判断している加工基準についても、検討会の有識者からは高いリスクの指摘があり、再識別リスクについての認識が理解されていない。

このため、今後も事例を増やし、相談の内容を踏まえて指針の作成を行っていく予定である。

4．改正法とCBPRシステムの関係について

改正個人情報保護法では、個人情報取扱事業者が個人データを外国にある第三者に提供する場合は、あらかじめ「外国にある第三者への個人データの提供を認める旨の本人の同意」を得なければならない規定が新たに盛り込まれた。ただし、以下のいずれかに該当する場合は除くとされている（表1）。

同意を得る必要のない場合	具体的な内容
当該第三者が、わが国と同等の水準にあると認められる個人情報保護制度を有している国として個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第３号。以下「規則」という。）で定める国にある場合	現時点ではない （EUとの間で、相互に個人データの移転を認める最終合意に達し、現在EU議会で承認の手続き中である。）
当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として規則で定める基準に適合する体制を整備している場合	外国にある第三者が個人情報保護委員会の規則で定める基準に適合する体制を整備している。 委託契約やグループ企業の内規・プライバシーポリシー、提供元または提供先の個人情報取扱事業者がアジア太平洋経済協力（APEC）のCBPRシステムの認証を取得している場合等
法第23条第１項各号に該当する場合	－

表1　外国の第三者への個人データ提供時に同意の除外事項

個人情報保護委員会の規則で定める基準に適合する体制を整備している基準として越境プライバシールール（CBPR：Cross Border Privacy Rules）システムの認証を規定している。

5．APEC CBPRシステムにおけるAAとしての役割

2011年にAPEC電子商取引運営グループ（ECSG：Electronic Commerce Steering Group）で策定されたCBPRシステムは、APEC域内において国境を越えて流通する個人情報に対する消費者や事業者、行政機関における信用を構築するシステムである。

アカウンタビリティ・エージェント（Accountability Agent、略称「AA」という。）は、参加する事業者の個人情報保護方針や実務がCBPRシステムの要求事項を遵守しているかを認証するという重要な役割を担っている。紛争が発生した場合はこれを解決すべく、事業者や消費者、政府と協働することとなる。

当協会は、2016年１月に、日本で初めてとなるAPECのCBPRシステムのAAに認定された。

AAとしての役割は、まずは執行機関に対して、認証事業者の適正な個人情報の取扱いについて、当協会の基準を満たし、適正に運用していることを説明することと、認証を受けた事業者のAPEC域内からの苦情・相談、事故等について、ケースに応じて調整を行うことである。

当協会は、APECプライバシー原則に則り、国内個人情報保護法に沿った基準を作成し、それに基づいた審査を行っているため、事業者は消費者等へもデータ移転の際の個人情報の取扱いについて対外的にアピールすることができる。

さらに事業者は、組織のプライバシーポリシーを国際的な基準に合わせることができ、お互い信頼することができるため、コンプライアンスの重みを低減でき、貿易上の摩擦を減らせるともいわれている。

特に、中小企業にとって組織のポリシーを国際的な基準に合わせることができるというメリットもある仕組みであるといえる。

この仕組みを国内外に広め、安心でスムーズな越境の仕組みが広がるよう活動を進めていかなければならないと考えている。

6．おわりに

当協会は認定個人情報保護団体として従来の苦情の処理はもちろん、対象事業者の個人情報漏えい等の事故の対応、とりわけ不正アクセス等の大きな事故があった場合、速やかに報告を受け付けることにより、消費者への連絡方法や対応すべき対策等を専門機関と連携しながら、事故の拡大防止や再発防止策の助言を継続する。

匿名加工情報に関しては、検討会を踏まえた情報発信をする予定である。

また、CBPRシステムの認証事業者も増えてきており、わが国の個人情報の保護のあり方を世界に発信する機会も増えている。

多数の対象事業者を擁している立場から、さらなる認定個人情報保護団体としての運営に注力し、わが国の個人情報保護の取組みの一端を担えるよう貢献する所存である。

参考URL（2018年11月時点）

・認定個人情報保護団体
https://www.jipdec.or.jp/protection_org/about.html
・CBPR認証
https://www.jipdec.or.jp/protection_org/cbpr/index.html

Ⅱ 海外における個人情報保護の取組み

EY アドバイザリー・アンド・コンサルティング株式会社
テクノロジーリスク パートナー　**梅澤 泉**

Ⅱ-1 各国の動向

(1) 概観

海外で事業を展開する日本企業にとって、進出国における各種規制対応は重要課題の一つであり、その理解と対策なしに活動を継続していくことは困難である。本稿では個人情報保護に関する法規制について取り上げ、主要国における動向と特徴、および日本企業が留意すべき事項について解説を加えていくこととする。

すでに多くの日本企業は世界各国に現地法人を設立し、あるいは支店、工場を構えることでビジネス領域を拡大してきている。外務省の統計データによれば、日系企業の主要拠点の推移は表1のとおりであり、上位10拠点のうちアメリカとドイツを除く８拠点をアジア諸国が占めている。また、全体を見た場合でも、日系企業の海外総拠点数約75,000拠点のうち、およそ７割にあたる52,000拠点がアジアに進出しているという状況であり、昨今のグローバルビジネスにおけるアジア諸国の重要な位置づけが色濃く反映されている。

以下においては、圧倒的多数の拠点を有する中国を筆頭に、堅調に拠点数が増えているアメリカ、その他増加傾向の高いアジアの主要国を中心に、各国の個人情報保護に係る法規制について触れることとする。

(2) 中国

中国では包括的な個人情報保護に関する法令は制定されておらず、2017年６月に施行されたサイバーセキュリティ法（中華人民共和国網絡安全法、Cybersecurity Law of the People's Republic of China、インターネット安全法、ネットワーク安全法ともいう）において、主として情報通信やインターネット関連に携わる情報ネットワーク運営者に対してさまざまな規制が課されている。

具体的には個人情報の収集にあたっての同意取得（同法第41条）、本人同意なしの第三者提供禁止（第

国名	拠点数（2017.10）	拠点数（2012.10）	過去５年間の増加率
1. 中国	32,349	31,060	4.2%
2. アメリカ	8,606	6,899	24.7%
3. インド	4,805	1,713	180.5%
4. タイ	3,925	1,469	167.2%
5. インドネシア	1,911	1,397	36.8%
6. ベトナム	1,816	1,211	50.0%
7. ドイツ	1,814	1,527	18.8%
8. フィリピン	1,502	1,214	23.7%
9. マレーシア	1,295	1,056	22.6%
10. シンガポール	1,199	757	58.4%

表1　日系企業の国別拠点数と推移
外務省：「海外在留邦人調査統計」より作成

42条）といった個人情報保護に関する一般的な規定をはじめ、収集した個人情報の安全管理義務（第21条）、ネットワーク製品およびサービス提供に際し中国の国家基準製品に強制適合しなければならない義務（第22条）、ネットワークのセキュリティに関する緊急対応プランの策定義務（第25条）などが取り決められている。

なお本法の適用対象事業者として、図１のとおり情報ネットワーク運営者と重要情報インフラ運営者という２階層の事業者があげられている。

本法における大きな特徴の一つとして、情報ネットワーク運営者のうち、重要情報インフラ運営者に該当する事業者には、上記に加えて中国国内で収集された個人情報やデータを国内で保管することが義務化され、国外へのデータ移転は原則的に禁止されるとともに、業務上やむを得ず国外に提供する必要がある場合には別途制定される法令（安全保護弁法）に従って安全評価を実施しなければならない（第37条）、という点が挙げられる。中国においてはこうしたデータ移転に関する規制が色濃く反映されており、近年トピックとなっているデータ・ローカライゼーションの典型例として注目を浴びている。

（3）アメリカ

アメリカにおいては現在のところ個人情報保護に関する一般法はなく、業界別の連邦法、州法、民間企業の自主規制による規制が行われている状態が続いている。EUでは2018年５月に一般データ保護規則（GDPR）が適用開始となったが、そのEUとの関係でいえば、EU－アメリカ間における個人データの移転を許容する枠組みであるプライバシーシールドが2016年８月に発効し、米国企業は自国の商務省に登録することでEUから個人データを持ち出すことが可能になった経緯がある。しかしながら、大手プラットフォーマー、データアナリティクス会社を通じた個人データの不正利用が取り沙汰され、欧州議会は2018年７月にプライバシーシールドの枠組みを停止する旨を決議した。今後仮にプライバシーシールドの停止が執行された場合、米国企業はEUから個人データを持ち出すためにEUの現地法人との間でSCC（標準的契約条項）を締結するか、グループ企業内でBCR（拘束的企業準則）を策定するといった追加措置をとらねばならず、対応に要する時間とコストを考えると該当企業にとっての負担は大きなものとなる。

また州法に関しては、2018年６月にカリフォルニア州で消費者プライバシー法（The California

情報ネットワーク運営者

ネットワークの所有者及び管理者並びにネットワークサービスの提供者（第76条(3)）。

重要情報インフラ運営者

情報ネットワーク運営者のうち、重要な情報インフラ、すなわち

「公共通信及び情報サービス、エネルギー、交通、水利、金融、公共サービス、電子行政サービス等の重要業界及び分野や、一旦機能の破壊若しくは喪失又はデータ漏えいに遭遇すると、国の安全、国民の経済・生活及び公共の利益に重大な危害を及ぼす恐れおそれのある重要な情報インフラストラクチャー」（第31条）

を運営する事業者

図1 中国サイバーセキュリティ法／対象事業者

日本貿易振興機構（JETRO）公表資料（ネットワーク安全法 仮訳）にもとづき筆者作成

Consumer Privacy Act of 2018）が成立し、話題を呼んだ。この法律の適用を受けるのは同州で事業を手掛けており、年間売上高や取り扱う個人情報の件数等に関し、所定の条件を満たす企業である（同法1798.140（c））。該当企業は収集する個人情報の内容や利用目的をデータ主体に通知することが求められるとともに、データ主体からの個人情報の削除請求にも応じなければならない。これらはGDPRや日本の個人情報保護法においてもすでに適用されている個人の権利に関して、アメリカの中でも同様に認めるべきという考えが広がり始めていることを意味しており、今回の制定によって、特にシリコンバレーを中心とした同州に本拠地を構えるIT企業やデジタルメディア企業にとってはインパクトの強い法規制となる。なお本法は2020年１月に施行予定であり、意図的に違反した個人、企業、サービスプロバイダには、違反の都度、最大で7,500ドルの罰金が科されることが定められている（同法1798.155（b））。

（4）インド

インドでは2000年に情報技術法（Information Technology Act）が制定され、主に電子データや電子商取引などの情報通信に係る情報の取扱いについて取り決めている。またこれを補完する形で情報技術（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）が2011年に策定され、コンピュータ上で取り扱われる個人情報の取得、保管、移転に関して定めている。

本規則の中では個人情報をセンシティブ情報とそれ以外の個人情報に分け、それぞれの取扱いに関する規制を定めているが、このうちセンシティブ情報の中にはパスワードやクレジットカード情報なども含まれており（同規則第２条）、いわゆる本人に対する不当な差別や偏見に係る不利益といった一般的な観点とは異なる要素が加わっている点に特徴がある。

なおインドにおいては、データ保護に留意しつつ、デジタルエコノミーの成長を推進していく方針のもとで、2017年11月にデータ保護の枠組みに関する白書（White Paper of The Committee of Experts on A Data Protection Framework for India）が策定され、さらに本白書の内容をベースとして、2018年７月には個人情報保護法案（The Personal Data Protection Bill）が議会に提出されている。このようにインドにおいては個人情報保護に対する法制化が急速に進んできており、今後の動向にも注視する必要がある。

（5）タイ

タイでは個人情報保護を規制する明確な法令が現時点においては存在していない。ただし個人データ保護法案（The Data Protection Act）が2018年５月に閣議決定し、議会での審議を経て2018年内ないし2019年初頭を目途に施行される見通しとなっている。同法案はGDPRをベースとした内容となっており、管理者と処理者の責任を取り決めた上で不適切な利用が行われた場合の罰則も定めている。

タイでは2018年に入って大手通信キャリア事業者へのハッキングによるユーザ情報の大量流出事故が発生したこともあり、個人情報保護に対する社会的な要請も高まってきている。こうした背景の中で、インド同様今後の法制化に向けた動きが加速していくことが期待される。

（6）インドネシア

インドネシアでは電子情報法（Electric Information Law）および電子システムにおける個人データ保護規則（Protection of Personal Data in the Electronic System, Regulation No.20）が2016年に制定され、いずれも2018年12月から施行が予定されている。個人データを電磁的に利用している事業者が対象であることから、日系企業の多くが適用を受けることになると考えられる。個人情報に関して「個人データ」および「特定の個人情報」という二つの概念が存在し（同法第１条）、海外へのデータ転送に際してはインドネシア政府の情報通信省と調整（計画報

告、転送結果報告、同意取得等）が求められている（第22条）点など、他国の個人情報保護法制と比べてインドネシア特有の規制があるものの、具体的な内容が不明確な点もあり、このあとガイドラインの公表によってこうした点が補完されることが予定されている。

（7）シンガポール

2012年に制定され、2014年７月から全面施行となったシンガポールの個人データ保護法（Personal Data Protection Act, PDPA）は、シンガポールにおけるすべての事業者が適用対象となっており、個人情報を１件でも有していれば同法の規定に沿って対処する必要がある。PDPA自体はGDPRに近い内容となっているが、特徴としてはビジネス目的の連絡先（名刺情報など）は事業者が遵守すべき主な規制の対象外となっている点や、消費者は自らの個人情報に基づく電話勧誘を希望しない場合、個人情報保護委員会（The Personal Data Protection Commission, PDPC）に電話番号を登録することで、事業者からの電話勧誘を回避することができるという仕組み（Do not call制度）が整備されている（同法第９章）、といった点などが挙げられる。

また2018年２月にはAPEC（Asia-Pacific Economic Cooperation, アジア太平洋経済協力）内における越境データの取扱いをルール化したCBPR（Cross Border Privacy Rules）システムへの参加を果たし

国名	関連法令の名称	制定年月 （改正年月）	主な特徴、補足説明等
日本	個人情報保護法	2003/5 （2017/5）	改正により、 ・個人情報保護委員会を設置 ・要配慮個人情報、匿名加工情報を新設
中国	インターネット安全法 （サイバーセキュリティ法）	2016/11	情報ネットワーク運営者が対象。このうち重要情報インフラ運営者に対しては、データ・ローカライゼーション規制等が上乗せ措置として定められている。
インド	情報技術法 情報技術規則 個人情報保護法（案）	2000/6 2011/4 —	2017年11月公表の白書に基づいた個人情報保護法案が今後制定される見込み。
タイ	個人データ保護法	2018/5 ※未施行	個人情報保護法案が2018年５月に閣議決定され、2018年中に施行される見込み。
インドネシア	電子システムにおける 個人データ保護規則	2016/12	2018年12月施行予定。不明瞭な箇所が多く、今後ガイドラインにより明確化される見込み。
ベトナム	サイバー情報セキュリティ法 サイバーセキュリティ法	2015/11 2018/6	サイバー情報セキュリティ法では、サイバー空間における個人情報の適正な収集、利用、同意取得について取り決め、サイバーセキュリティ法では対象となる個人情報につき、一定期間ベトナム国内のサーバに保存する義務がある旨定められている。
フィリピン	データプライバシー法	2012/6	一定の要件を満たす事業者は、個人情報を処理するシステムについて、フィリピン当局であるNPC（National Privacy Commission）に登録することが義務付けられている。
マレーシア	個人データ保護法	2010/6 （2016/6）	特定の11業種（通信、金融、医療その他）に関しては、個人情報の取扱いについて個人情報保護委員会（Personal Data Protection Commissioner, PDPC）への登録が義務付けられている。
シンガポール	個人データ保護法	2012/11 （2014/7）	違反時には、PDPCが最大で100万シンガポールドル（8,000万円）の制裁金を科すことができる旨が定められている。
韓国	個人情報保護法 情報通信網法	2011/3 （2016/9） 2001/12 （2016/3）	情報通信網法では、データ侵害時において発覚から24時間以内に当局への届出義務が定められている。

表2　主要なアジア諸国における個人情報法規制の比較

ており、個人データをAPEC域内において幅広く流通させるための取組みについても進めているところである。

なおデータ侵害時の通知または公表に関しては現法において特段義務付けられていないが、PDPCが2017年７月に公表した改正方針において、データ侵害時には事業者に対し、PDPC および本人へ72時間以内の通知義務を課す旨が提言されている。

（8）その他のアジア諸国

アジア諸国に関しては、個人情報保護に係る法規制の整備が経済発展のスピードに十分に追いついていない国がある一方で、GDPRをモデルとした法令の制定や法改正が進められている国も徐々に増え始めているのが現状である。

主要なアジア諸国の法規制の動向についてまとめると表2のとおりとなる。アジア諸国の法規制は総じて過渡期にあるといえることから、各国法令の新設やアップデートに対してこまめにキャッチアップできる体制を整えておくことが重要である。また、法令違反による制裁金等の法執行はアジア各国においても加速していく可能性があり、今後の当局の動きに関しても併せて注目していくことが望ましい。

Ⅱ-2 日本企業への影響

（1）GDPR（General Data Protection Regulation）

GDPRは個人データ（personal data）の取得・処理・移転に関するルールを定めたEUの個人情報保護法であり、主な特徴は表3のとおりである。

GDPRは2018年５月に適用開始となったが、現時点においても多くの日本企業がGDPRへの対応につき道半ばといった状況であるように見受けられる。こうした中で、海外では外部からのハッキングによる個人データの漏えいといったセキュリティインシデントやプライバシー保護団体による活動、あるいは監督当局によるモニタリング活動等を通じて、GDPRに係る違反行為が摘発されたり、GDPRに抵触する恐れのある企業の取組み姿勢などが指摘されたりといった状況が相次いでいる（表４）。

GDPRの特徴および日本法との主な相違点

1	個人データ（personal data）の定義
2	EU域外への個人データの移転規制
3	個人データ侵害時の72時間以内の通知
4	GDPRに準拠していることの説明責任
5	データ保護責任者（DPO）の設置
6	取扱活動の記録
7	適法な取扱いの整理（同意の取得を含む）
8	個人情報保護に関する新たな権利（忘れられる権利、データポータビリティ、同意の撤回、プロファイリングに係る機械的な処理の拒否等）への対応
9	大規模、リスクを伴うデータ処理におけるデータ保護影響評価（DPIA）の実施
10	プライバシー・バイ・デザイン（PbD）の導入
11	高額な制裁金

表3　GDPRの主な特徴

時期／対象となった企業	概要	監督機関との関連
2018年５月 大手IT企業（米国）	**【同意の取得に関するGDPR第７条に抵触するとの異議申し立て】** プライバシー保護活動を推進する非営利団体が、米IT企業４社に対し、個人データ収集時の同意取得に関して、GDPR違反を問う異議申立てをEUのデータ保護機関へ提出した。	CNIL（フランス）など４機関に対し異議申立てが行われた
2018年６月 ホテル事業者（日本等）	**【取扱者の利用に関するGDPR第28条に抵触する可能性】** 委託先（処理者）であるホテル予約サイト運営事業者（フランス）のサーバが２回にわたり外部から不正アクセスされ、同予約サイトを利用する日本国内の複数ホテルの宿泊者データ（氏名、住所、クレジットカード等）、計12万件超が流出するインシデントが発生した。	事案発覚後、一部のホテル事業者からはCNIL（フランス）、PPC（日本）等に対し72時間以内の侵害通知を実施
2018年７月 データ分析企業（カナダ）	**【個人情報の適正な取扱いに関するGDPR第5条（1）、第６条、第14条（1）（2）（5）に抵触】** 2016年のEU加盟継続の是非を巡る国民投票に向け、個人情報を本人が知り得ない目的（SNSサイトにおけるターゲット広告配信）のために利用したとして、監督機関による違反通告が行われた。	ICO（英国）より違反通告を受ける

表4　GDPR適用開始後の違反、もしくは違反が疑われる事案

日本企業からすると、GDPRは海外の法規制ということもあって対応の必要性あるいは優先度合がおろそかになりがちであるが、法令遵守はもとより、リスクマネジメントの観点からも、自社にとってGDPRが適用対象となるのかどうか、該当する場合はどのような業務にどのくらいのインパクトが発生しうるのかについて正しく把握することが重要である。日本法に沿って従来適切に安全管理対策を図ってきた企業であっても、先に示した表3にもあるように、たとえばデータ侵害時の監督機関への通知手順や、データ主体が有する新たな権利（同意の撤回、忘れられる権利、データポータビリティの権利など）に対する適切な対応など、日本法では要求されていない追加的な措置を考慮し、計画的に対策を講じる方針のもとで進めていくことがポイントになる。

（2）e-プライバシー規則（案）

EUにおいては、電子通信分野における特別なプライバシー保護のルールを定めた電子通信プライバシー指令（e-privacy directive、以下「e-プライバシー指令」という。）が2002年に制定され、通信の機密性や行動ターゲティング広告等に用いられるブラウザのクッキー情報利用などについての規律が定められている。

個人情報保護全般に関しては、1995年より適用されたEUデータ保護指令（Data Protection Directive 95）が2018年５月からGDPRに移行したが、e-プライバシー指令についても当初GDPRの適用開始とタイミングを合わせるべく、2017年１月に欧州委員会によって新たに電子通信プライバシー規則案（a proposal for a Regulation on Privacy and Electronic Communications、以下「e-プライバシー規則（案）」という。）として公表され、欧州議会および欧州理事会によって審議が進められてきた。

その後加盟国間での意見調整が図られる中で交渉が長期化し、同規則の成立には至っていない（※）が、GDPRと同様に従来の「指令」を「規則」に格上げし、GDPRと一体的な運用を可能とする方向で法整備が進んでいる。

（※）2018年10月執筆時点

本規則（案）では、企業はネットの利用者から収集するクッキー等のユーザ情報について、当該利用者からの明示的な同意がなければ収集することがで

GDPR	eプライバシー規則（案）
1．すべての**個人データ**を対象としている。（伝送手段に依拠しない）	1．個人データかどうかにかかわらず、ユーザのデバイスにおける電子的な通信手段および**情報の完全性**を対象としている。
2．個人情報保護の権利について定義している。	2．通信に関わるプライバシーと機密保持の権利について定めている。
3．個人の新たな権利と企業が果たすべき義務を組み込んでいる。	3．ユーザが通信するモバイルアプリまたはインターネットサービスが、通信内容を妨害・傍受、記録、盗聴、侵害・侵入できないことを確実にする。
4．2018年5月25日に運用開始。	4．2017年1月10日に提出され、欧州議会および欧州理事会で現在審議中。

“ePrivacy factsheet”（2018年5月、欧州委員会公表資料）より筆者仮訳、作成

図2　GDPRとe-プライバシー規則（案）の特徴比較

きなくなる。すなわち、クッキーの収集・利用については原則としてオプトインとしつつ、一方で企業にとってサービス提供に必要不可欠な場合や第三者提供を伴わないウェブの解析等に係るクッキーについては同意の取得は不要とし（本規則（案）（21））、加えてウェブブラウザの提供事業者にはクッキー収集の拒否または同意が容易に選択できる方法（選択肢のポップアップ表示等）の提供を義務付けている（同（23））。その意味では、企業にとってはクッキーの取扱いルールが従来に比べて合理化され、規制と利用のバランスが図られるようになるものと考えることができる。

なお本規則（案）は、EU域内に拠点を持たない場合であっても、EUのネットユーザからクッキー情報等を収集するようなケースは適用対象となる。そのため、オンラインビジネスを手掛ける企業やネット広告に携わる事業者などを含め、日本企業であっても対応が必要となる可能性があることに注意すべきであり、GDPRと併せて検討を進めておくことが重要となる。

（3）越境プライバシールール（CBPR）

アジアを含む環太平洋地域では、APECにおいて2004年にOECD8原則をベースとしたAPECプライバシー原則が採択され、本フレームワークに沿った形での国内個人情報保護制度の策定、推進が奨励されてきた。

そうした中で、2007年にはAPEC域内で国境を越えて個人データを取り扱う事業者に対し、同フレームワークへの適合性を認証する制度である「越境プライバシールールシステム」（Cross Border Privacy Rule System, 以下「CBPRシステム」という。）が構築され、越境する個人情報が適切に保護されるための仕組みが用意された。CBPRシステムには現在アメリカ、メキシコ、日本、カナダ、韓国、シンガポールの６カ国が参加しており、さらにはフィリピン、台湾、オーストラリアなども参加の意思を公式に表明している。今後はアジアパシフィックにおいてさらなる広がりが期待されるところである。

日本の改正個人情報保護法においては、企業は日本から外国の第三者に個人データを提供するにあたり、一定の要件を満たさない限り、その旨につき本人同意を得なければならない（同法第24条）が、CBPR認証を取得することにより企業は当該同意を得ることなく、国境を越えた個人データの移転が可能とされている。（※）

（※）個人情報委員会規則第11条、個人情報保護ガイドライン（外国第三者提供編）3-1参照

このように、日本企業においてもCBPRシステムに沿った個人情報保護の管理体制を構築し、さらには当該認証取得に向けた取組みを進めていくことで、国境を越える企業間のデータ取引に信頼性を付

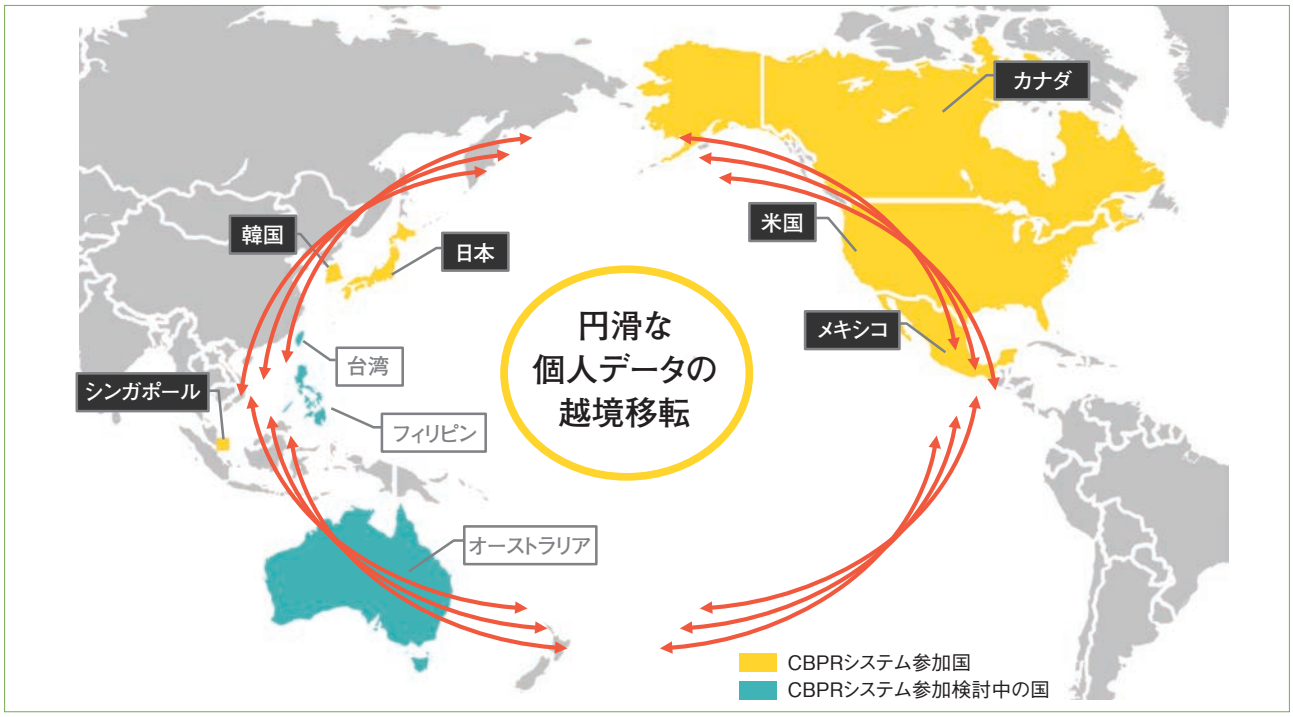


図3　CBPRによる個人データの流通

与しつつ、グローバルビジネスの活性化につなげていくことが期待できる。

（4）中国サイバーセキュリティ法

昨今、多くの国が個人データの域外移転について何らかの規制を定めている。中でも中国のサイバーセキュリティ法では、重要情報インフラ運営者は中国国内で収集された個人情報や重要データに関しては中国国内で保存することが義務付けられており、違反時には最大50万元（約800万円）の制裁金に加え、一時業務停止、ウェブサイトの閉鎖、営業許可証の取消といったさまざまな行政処分を科すことができる旨が規定されている（同法第66条）。このように、中国では自国のデータを国内に留めておくというデータ・ローカライゼーションの意識が色濃く反映されている。EUなどのように個人のプライバシー保護を主目的として域外移転に制限をかけるというよりは、国内の産業保護、安全保障の確保、法執行や犯罪捜査の観点など、自国の情報を他国から守るという国策的な意味合いが強いと考えられる。

重要情報インフラ運営者についてはその範囲が不明瞭な部分もあり、日系企業がどこまで該当するかどうか定かではないが、仮に該当する場合にはこうしたデータ・ローカライゼーションの適用を受けることで個人データの維持・管理に想定以上のコストがかかることも考えられ、注意を払う必要がある。

また情報ネットワーク運営者に関しては、中国に拠点を有する日系企業が幅広く該当する可能性があり、先に述べたようなさまざまな規制について適切に対処する必要がある。本法における当局の権限は比較的強く、セキュリティ不備による罰則を科されるような事態を回避する上で、日本企業としても本社主導によるセキュリティ体制の強化について取り組むことも重要である。

（5）デジタル課税

個人情報保護に関する直接的な規制ではないが、近年デジタルエコノミー社会が進展する中で、国際的な法人課税のルールについて見直しが検討されている。従来、特定の所在国において工場や支店のような物理的な施設（恒久的施設）を持たない企業が、当該国内において電子商取引のようなオンラインビジネスを行っていた場合であっても、当該企業に対して課税することができず、制度上の課題となって

	EU／指令案	英国／Policy paper ; DST Budget 2018
対　　象	世界売上高が7.5億ユーロ超、かつEU域内でのデジタルサービスに係る売上高5,000万ユーロ超の企業	世界売上高が５億ポンドを超える黒字企業（ただし2,500万ポンドまでの売上高については課税の対象外）
税　　率	EU加盟国ごとのサービス提供に係る売上高の３％	英国におけるサービス提供に係る売上高の２％
適用時期	2020年１月（可決された場合）	2020年４月

表5　デジタルサービス税（Digital Services Tax, DST）の概要

いた。

このような背景のもとで、EUでは2018年３月に欧州委員会がデジタルサービス課税に係る指令案(※1)を提出し、2020年１月の施行に向けて協議を進めている。また2018年７月にブエノスアイレスで開催されたG20においても、公正、持続可能かつ現代的な国際課税制度の実現に向けて対処していく旨につき合意形成されており、OECDからは2020年までに加盟国からの合意を得て当該課税ルールの統一を図る旨が公表されている(※2)。

（※1）Proposal for a COUNCIL DIRECTIVE on the common system of a digital services tax on revenues resulting from the provision of certain digital services, European Commission, March 2018

（※2）OECD Secretary-General Report to G20 Finance Ministers and Central Bank Governors, OECD, July 2018

こうした国際的な流れのもとで、英国ではいち早くデジタルサービス税の導入を決定した。適用開始は2020年４月を予定しており、大手IT企業を中心とした所定の条件を満たす事業者が英国の利用者向けに提供するデジタル事業によって得られた売上に対し、当該サービス税が課されることになる（表５）。

このようなデジタル課税は、対象国において大量の個人データを収集、保有し、これらを活用してビジネスを幅広く展開する事業者、すなわち検索エンジン、ソーシャルメディア・プラットフォーム、オンラインサービスなどを手掛ける企業が主なターゲットになっていると考えられる。日本企業においても、自社が課税対象事業者に該当しないかどうか、すなわち英国やEU域内における取引高がどの程度の規模なのかについて現状把握を実施しておくことが望ましい。その結果、課税によってもたらされるインパクトの大きさに応じて国ごとの売上シェアを検証し、見直しを図るなど、ビジネス戦略の再構築も想定されることから、そのための準備・対応コストも含めて、さまざまな影響や負担が発生しうることに注意が必要である。

（6）適切なデータ保護と円滑なデータ流通に向けて

GDPRは近年における個人データの加速的な流通、広がりと、個人の権利およびプライバシーの保護という二つの異なるベクトルに対し、両者のバランスを整える意味で意義のある法制度であると言える。今後GDPRは個人データの取扱いに関するグローバルスタンダードとして、各国の法規制や企業の取組方針に影響を与えることになると考えられる。日本企業においても、さらなるグローバル化が図られる中で、GDPRをベースとした個人情報保護対応を進めていくことが事業の発展に向けて重要なカギとなってくる。

ビッグデータとしての個人情報の利活用がますます高まる一方で、企業は個人情報の取扱いに厳しい視線を注ぐ一般消費者や監督当局に対して、説明責任を果たせるような体制が適切に構築されているかが改めて問われることになる。悪意を持ったサイバー攻撃からどのように情報を守るのか、データを海外に持ち出すことを規制するデータ・ローカライゼーションの動向に対してどのように対処するのか、企業にとっても検討課題は尽きないが、これらの諸問題を適切に認識するとともに、真摯に向き合う姿勢が求められることになる。

〈資料－1〉国内外の主な個人情報保護関連の年表

国　内	年	海　外	
	1970	ドイツ	ヘッセン州において世界初の「データ保護法」採択
徳島県徳島市「電子計算機処理に係る個人情報の保護に関する条例」施行 コンピュータ処理された個人情報の適正な管理が目的（6/28）	1973		
	1974	アメリカ	「プライバシー法」制定
「電子計算機処理データ保護管理準則」策定	1976		
	1977	ドイツ	「データ処理における個人データの濫用防止に関する法律（連邦データ保護法）」制定（1月）（2009年に改正）
	1978	フランス	「データ処理・データファイル及び個人の自由に関する法律」制定
		カナダ	「カナダ人権法」制定
	1979	コミッショナー	「プライバシー・コミッショナー会議」開始
	1980	欧州評議会	閣僚委員会が「個人データの自動処理に係る個人の保護に関する条約（条約第108号）」採択（9/17）
		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に関する理事会勧告」採択（9/23）
	1981	欧州評議会	「個人データの自動処理に係る個人の保護に関する条約（条約第108号）」発布（1/28）
	1982	カナダ	「連邦プライバシー法」制定
	1983	ドイツ	ドイツの憲法にはデータに関連したプライバシーの権利が含まれていないが、連邦憲法裁判所が個人の「情報を自己決定する権利」を公式に認める
福岡県春日市にて「個人情報保護条例」可決（7/4）。10/1施行	1984	アメリカ	「ケーブル通信政策法」制定
		イギリス	「データ保護法」制定（1998年に改正）
	1985	欧州評議会	「個人データの自動処理に係る個人の保護に関する条約（条約第108号）」発効（10/1）
JIPDEC、民間事業者を対象とした「個人情報保護に関する調査研究」に着手	1986	アメリカ	「電子通信プライバシー法」制定
「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律案」閣議決定	1988	アメリカ	「コンピュータ・マッチング及びプライバシー保護法」制定
JIPDEC、「民間部門における個人情報保護のためのガイドライン」策定（5月）			
「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」公布（12/16）（「行政機関の保有する個人情報の保護に関する法律」で全部改正） 1989年10月1日に第三章と23条以外の規定が施行 1990年10月1日に全面施行			「ビデオプライバシー保護法」制定

国　内	年	海　外	
	1994	韓国	「公共機関における個人情報保護に関する法律」制定
		フランス	フランス憲法では明示的にはプライバシーの権利は保護されていないが、憲法裁判院がプライバシーの権利は憲法に内在的に含まれていると裁定
	1995	香港	「個人データ（プライバシー）法」制定
		台湾	「1995年コンピュータ処理に係る個人情報の保護に関する法律」制定
		EU	「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する欧州会議及び理事会の指令」公示（10/24） （加盟国に3年以内の個人情報保護法制の整備を求める）
	1996	アメリカ	「電気通信法」制定
通商産業省、「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」公表（3/4）	1997		
JIPDEC、プライバシーマーク制度開始（4/1） （1997年の「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」に基づく）	1998	アメリカ	「児童オンラインプライバシー保護法」成立（10/21）
		EU	「EUデータ保護指令」施行（10/24）
			スウェーデンで、アメリカン航空に対してスウェーデン国内で収集した搭乗者の個人情報を米国内の予約センターに移転することを禁じる（11月）
		イギリス	「人権法」採択（11月）
「JIS Q 15001個人情報保護マネジメントシステムー要求事項」制定（3/20）	1999		
	2000	カナダ	「個人情報保護及び電子文書法」制定
		EU-アメリカ	EU・米国間における「セーフハーバー協定」締結（7月）
	2001	アメリカ	「米国愛国者法」制定（10/26）（2015年6月失効）
「個人情報保護法」公布・一部施行（5/30）	2003		
	2004	APEC	「APECプライバシーフレームワーク」採択（10/29）
「個人情報保護法」全面施行（4/1）	2005		
「JIS Q 15001：2006」改正（5月）	2006		
	2007	APEC	「越境プライバシールール」策定 「パスファインダープロジェクト」の試験的な取組み開始
	2012	EU	「EUデータ保護規則案」提出
		アメリカ	「消費者プライバシー権利章典」が掲載された行政白書にオバマ大統領が署名（2/23）
「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」および関連法公布（5/31）	2013	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に関する理事会勧告」改正（7/11）

国　内	年	海　外	
特定個人情報保護委員会発足（1/1）	2014		
APEC越境プライバシールール（CBPR）システムに参加（4月）			
「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」成立（9/3）	2015	アメリカ	・「米国自由法」成立（6/2） ・「サイバーセキュリティ情報共有法」にオバマ大統領が署名（12/18）
		EU-アメリカ	欧州で「セーフハーバー協定」無効判決（10月）
特定個人情報保護委員会が改組し、個人情報保護委員会発足（1/1）	2016	EU	欧州本会議「一般データ保護規則（GDPR）」を正式可決（4/14）
APEC-CBPRシステムの認証団体として、JIPDECがアカウンタビリティ・エージェント（AA）に認定（1月）			
個人情報保護委員会、アジア太平洋プライバシー機関フォーラム（APPA）の正式メンバーに就任（6月）		EU-アメリカ	EU・米国間における「プライバシーシールド」がEU諸国で承認（7/12）。8月から米商務省への参加申請受付開始
「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の施行に伴う関係政令の整備及び経過措置に関する政令」および「個人情報の保護に関する法律施行規則」制定（10月）			
「改正個人情報保護法」全面施行（5/30）	2017	EU	欧州委員会、電気通信分野のプライバシー保護を目的とする「e-プライバシー規則案」公表（1月）
「JIS Q 15001：2017」改正（12/20）		中国	「中華人民共和国サイバーセキュリティ法（インターネット安全法）」施行（6/1）
		ドイツ	「連邦データ法」全面改正（6/30）
情報銀行に求められる「情報信託機能の認定に係る指針ver.1.0」公表（6/26）	2018	EU	「EU一般データ保護規則（GDPR）」施行（5/25）
日-EU間の相互の円滑な個人データ移転を図る枠組み構築に係る最終合意確認、および個人データの越境移転に言及した共同声明発出（7/17）		ベトナム	「サイバーセキュリティ法」公布。国内でのデータ保存と事務所設置を義務化。2019年1月1日施行へ（6/12）
		フランス	「個人データ保護に関する法律」制定（6/20）
「個人情報の保護に関する法律に係るＥ域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」策定（９月）		EU-米	欧州議会、「プライバシーシールド」がEUの求める保護水準に達していないとして米国当局の対応を要求（7/5） 米商務省は「準拠している」と声明（8/30）
		ベルギー	「個人データの処理に関する保護法」制定（7/30）
		イタリア	「改正個人データ保護法典」施行（9/19）
		EU	欧州委員会、日本の個人情報保護に対する十分性認定の採択手続きに着手（9月）

〈資料－2〉情報化に関する動向（2018年4月～2018年9月）

国　内	海　外
2018年4月	
・総務省、楽天子会社を携帯電話事業者として認可。2019年にサービス開始予定。 ・政府、インターネット上の海賊版サイトへの緊急対応策として、ブロッキング実施を検討。法的整備に着手。 ・経済産業省、14年ぶりにシステム監査基準、システム管理基準改訂。ITガバナンスなどの国際規格との整合性、IT環境を反映。 ・ソフトバンク、2020年7月末に簡易型携帯電話（PHS）の個人向けサービス終了を発表。1995年7月に開始されたPHSサービスの幕切れ。	・米百貨店チェーンSaks Fifth Avenue、Saks OFF 5TH、Lord & Taylo、顧客の決済カード情報約500万件流出。 ・米ベーカリーチェーンPanera Bread、利用客の個人情報700万件以上流出。最大3,700万件への影響の可能性も。 ・Facebook、Cambridge Analyticaが収集したデータは最大8,700万人と発表。日本で最大10万人の情報流出の可能性も。米連邦議会の公聴会に召集され、ザッカーバーグCEOが謝罪。 ・ブラジルアマゾナス州連邦裁判所、Facebookに約36億円の罰金。情報開示命令に応じず。 ・米Verizon調査、1年間でのランサムウェア被害急増。従業員へのフィッシング詐欺メールが原因に。 ・Facebook、Microsoft等34社、政府主導のサイバー攻撃を支援しない「Cybersecurity Tech Accord」に署名。 ・米連邦捜査局、国土安全保障省、英国家サイバーセキュリティセンター、ロシア政府が関与するサイバー攻撃に対し共同警告。 ・Facebook、Twitter、一般データ保護規則（GDPR）対応でサービス規約改定。

国　内	海　外
2018年5月	
・次世代医療基盤法（医療ビッグデータ法）施行。匿名加工情報を研究機関に提供。 ・改正著作権法成立。著作権者の許諾なく書籍全文の電子化、インターネット検索が可能に。 ・日本年金機構、2015年の個人情報約125万件流出事件時効成立。捜査終了。 ・経済産業省とIPA、サイバー・フィジカル・セキュリティ対策のための情報交流の場、コラボレーション・プラットフォーム設置。 ・経済産業省調査、BCP策定率、中小企業は3割。	・オーストラリア政府、Googleによるアンドロイドユーザ数百万人の位置情報収集問題を調査。Googleは許可済と回答。 ・Facebookザッカーバーグ CEO、欧州議会で情報の不正利用、フェイクニュース拡散を謝罪。 ・欧州連合（EU）、GDPRを欧州経済領域（EEA）で施行。違反企業には巨額な制裁金。 ・米シスコシステムズ調査、54カ国、50万台以上のデバイスがマルウェア感染の可能性。

国　内	海　外
2018年6月	
・森永乳業、通販サイト利用者約9万人の顧客情報流出の可能性。 ・神奈川県警他、仮想通貨取引のマイニングで他人のPC無断使用に対し、不正指令電磁的記録併用容疑で16人を逮捕。マイニング行為では初立件。 ・総務省、電子委任状の管理事業者としてニセコムトラストシステムズとNTTネオメイトを認定。 ・仏ファストブッキング、ホテル予約システムへの不正アクセスにより、国内401カ所のホテル利用者、約32.5万件の個人情報流出。	・Facebook、4月の公聴会での2,000件以上の質問に対し、229ページにわたる追加回答文を提出。非ログインユーザの情報収集方法などを説明。 ・米連邦通信委員会、ネット中立性規則廃止。 ・英家電チェーンDixons Carphone、590万件の決済カード、120万件の個人情報への不正アクセス発覚。 ・韓国仮想通貨交換業者Bithubm、約35億円相当の仮想通貨流出。 ・AppleとSamsung、2012年から続いたデザイン特許訴訟で和解成立。

国　内	海　外
2018年7月	
・世界経済フォーラム、日本に第四次産業革命日本センター開設。AI、IoTの課題解決に着手。 ・日-EU間、越境個人データ移転に関する枠組み構築で最終合意。今秋運用開始を目指す。 ・金沢工業大学、画像刺激による脳波を利用した新しい個人認証方法開発。 ・政府、新サイバーセキュリティ戦略を閣議決定。 ・内閣サイバーセキュリティセンター、サイバー攻撃による重要インフラサービス障害等の深刻度評価基準（初版）公表。	・欧州委員会、Googleに対し約5,700億円の制裁金。携帯メーカへの自社アプリ搭載強要や未承認OS搭載電話の販売禁止が原因。 ・シンガポールの医療機関SingHealth、医療データベースへのサイバー攻撃により150万人分の患者情報流出。同国史上最悪。 ・欧州議会、EU-米間のプライバシーシールド停止を決議。Facebook問題などで米企業の対応が水準に達していないと判断。米側に遵守求める。

国　内	海　外
2018年8月	
・トレンドマイクロ調査、オンライン銀行詐欺ツールに感染させる日本語スパムメール、１日で29万通確認。 ・日の丸交通とSMP、自動運転タクシーでの営業走行実験。世界初。 ・大阪医科大生、勉強のために教員のPCからカルテ情報を含む約46万件のデータを無断コピー。不正指令電磁的記録供用容疑で逮捕。 ・厚生労働省調査、「インターネット依存」の疑いのある中高生は全国で93万人。前回12年度調査から倍増。 ・個人情報保護委員会、「個人情報保護法に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」公表。	・米通信会社T-Mobile、不正アクセスで200万人の顧客情報流出の可能性。 ・Google、Facebook等、2017年に撤廃された「ネット中立性」規則復活を求め、控訴裁判所に申立て。 ・中国ホテルチェーン大手Huazhu Hotels Groupの利用客情報1億3,000万件が売りに出される。 ・中国SNSサイトから不正アクセスで約30億件の個人情報流出。

国　内	海　外
2018年9月	
・日本IT団体連盟、2018年6月に総務省・経済産業省が公表した「情報信託機能の認定に係る指針ver.1.0」をベースに、情報銀行認定事業の開始を発表。 ・日本ハッカー協会設立。ホワイトハッカーの活躍の場の構築を目指す。 ・仮想通貨取引所Zaif運営のテックビューロ、不正アクセスで約67億円相当の仮想通貨流出。金融庁から業務改善命令。10月にフィスコに事業譲渡。 ・警察庁調査、2018年上半期の標的型メール攻撃被害は約2,600件。前年下半期より減少。 ・中部電力、働き方改革推進で10月から全従業員1.5万人をテレワーク対象と発表。 ・個人情報保護委員会、名簿等販売事業者の実態調査結果発表。保護法の履行により名簿等販売事業の継続が困難に。	・日-ASEAN特許庁長官会合開催、IoT、AI等新技術に対応した知財協力プログラム策定。 ・米国防総省、「サイバー戦略」公表。中国、ロシアをけん制。 ・Apple、EC命令でアイルランドに追徴課税と利息約143億ユーロを全額支払い。アイルランドとApple共に税制優遇の適切性を訴える。 ・Apple、Amazon他、上院公聴会で自社の個人情報保護対策を説明。連邦レベルでの個人情報保護法制定への支持を表明。 ・Facebook、5,000万ユーザのアカウントの不正利用被害を発表。アクセストークンの流出が原因。

JIPDEC

JIPDEC IT-Report 2018 Winter

2018年12月13日発行（通巻第12号）
発行所　一般財団法人日本情報経済社会推進協会
〒106-0032 東京都港区六本木1-9-9 六本木ファーストビル内
TEL：03-5860-7555　　FAX：03-5573-0561
制　作　株式会社ウィザップ