JIPDEC IT-Report 2016 Winter

特集

国内外における
個人情報保護施策の最新動向

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 2016 Winter」では、「国内外における個人情報保護施策の最新動向」と題し、特集を組みました。

わが国では2015年に個人情報保護法が改正され、個人情報を取り扱うすべての事業者に対し「安全管理措置」が義務化されました。政令、委員会規則の策定とともに、これまで法適用対象外とされていた「中小規模事業者」を含め、事業者が取り組むべき事項を例示した「ガイドライン」が公表され、この中で安全管理措置については、中小規模事業者に配慮した特例的な対応が示されています。現在、個人情報保護委員会において、2017年の全面施行に向けた最終調整が進められています。

今回の法改正にあたっては7つのポイントが挙げられていますが、その中で、JIPDECも2005年以降、経済産業省および総務省から認定を受けている「認定個人情報保護団体」に対し、事業特性に応じた自主ルール（指針）や匿名加工情報作成ルール等の策定を担う役割が期待されています。

2015年12月に発行した「JIPDEC IT-Report 2015 Winter」では、改正時点での個人情報保護法の概要を紹介していますが、本誌では、政令、委員会規則、ガイドラインを基に、具体的に7つのポイントの改正概要と、認定個人情報保護団体の役割についてご紹介します。

また、海外の動向として、EUでは2016年4月14日に「一般データ保護規則（GDPR）」が欧州議会本会議で正式に可決され、2018年からの運用開始が予定されています。本規則では、個人データの定義にオンライン識別子や生体情報が含まれるなど、保護対象の範囲拡大とともに、データ管理者に対する規制として、「大規模機微情報処理時のデータ保護評価の実施」「データ保護オフィサーの設置」「忘れられる権利」「個人に対するデータポータビリティの権利」が義務付けられるなど、個人情報保護に対し、より一層の強制力を持つものとなりました。

さらに、EU-米国間ではデータ移転に関する「セーフハーバー協定」の無効判決を受け、より規制強化された「プライバシーシールド」制度が提案・承認されたことから、近年のEUの個人情報保護強化策がEU域外に与える影響がどのようなものか、十分性認定を受けていない日本にどのような影響があるのかを、個人情報保護の第一人者である弁護士　福本洋一氏に解説をお願いしました。

あわせて、国内外の個人情報保護関連の年表と2016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。

2016年12月

一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2016 Winter

目　　次

【特集】国内外における個人情報保護施策の最新動向

Ⅰ 改正個人情報保護法の施行に向けた最新動向

個人情報保護委員会事務局

Ⅰ-1.個人情報保護法の改正ポイント

（本章Ⅰ-1は個人情報保護委員会事務局による講演概要をJIPDECがとりまとめたものです。）

はじめに

2003年公布・2005年に施行された個人情報保護法は10年間の情報技術の進展による環境の変化（個人情報をめぐるグレーゾーン拡大、パーソナルデータを含むビッグデータのビジネスへの利活用、グローバル化等）に対応するため、2015年9月に改正・公布された。今回の改正で、2014年にマイナンバー法に基づき設置された特定個人情報保護委員会が個人情報保護委員会（以下、「委員会」という。）に改組され、改正法施行後には、第三者機関として個人情報取扱事業者に対する監督権限が各主務大臣から委員会に集約・一元化される。

改正法の公布から2年以内の全面施行に向け、委員会において、関係政令、委員会規則の検討を行い、2016年10月に「個人情報の保護に関する法律施行令」の一部改正（以下、「政令」という。）および「個人情報の保護に関する法律施行規則」（以下、「委員会規則」という。）が制定された。また、法律・政令・規則の詳細について、例示を交えながら解説した「個人情報の保護に関する法律についてのガイドライン（通則編、外国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編）」（以下、「ガイドライン」という。）を11月に決定した。

本章では、改正個人情報保護法の全面施行に向けた最新動向を紹介する。

1.改正個人情報保護法の7つのポイント

改正個人情報保護法（以下、「改正法」という。）のポイントとしては、次の7つが挙げられる。

1.個人情報の定義の明確化
2.要配慮個人情報の規定の新設
3.匿名加工情報の規定の新設（ビッグデータ対応）
4.第三者提供に係る確認・記録義務（いわゆる名簿屋対策）
5.外国の第三者への個人データの提供（グローバル化への対応）
6.認定個人情報保護団体の活用
7.中小規模事業者への配慮（5,000件以下の個人情報取扱事業者対応）

以下、政令、委員会規則、ガイドラインを基に、ポイント別に解説する。

1-1.個人情報の定義の明確化－「個人識別符号」の新設

個人情報の範囲に関するグレーゾーンを解消すべく、個人情報の定義を明確化するため、情報単体でも個人情報に該当することとした「個人識別符号」という概念が新設され、その定義が定められた。

個人識別符号とは以下のいずれかに該当するもので、政令・規則で個別に指定されている。

①身体の一部の特徴を電子計算機のために変換した符号：DNA情報、指紋・掌紋、声紋、顔、虹彩、手指の静脈、歩行の態様
②サービス利用や書類で対象者ごとに割り振られる符号：公的な番号（旅券番号、基礎年金番号、運転免許証番号、住民票コード、マイナンバー、各種保険証番号等）

①の身体の一部の特徴を電子計算機のために変換した符号については、特定の個人を識別するに足りるものとして委員会規則で定める基準（特定の個人が識別できる水準）に適合するものが該当することとされており、具体的にはガイドラインにおいて示されている。たとえば、顔については「顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状から抽

出した特徴情報を、本人を認証することを目的とした装置やソフトウェアで本人認証をすることができるようにしたもの」が、「個人識別符号」に該当することとなる。

②の符号は、公的付番のみが今回は対象とされたが、今回指定されなかったクレジットカード番号や携帯電話番号等についても、これら番号が氏名、住所などと一緒に管理されていたり、他の情報と照合することで特定の個人を識別できる場合には、従来同様に「個人情報」に該当することとなる。

個人識別符号の取扱いについては、それ単体で個人情報となるため、従来の個人情報と同様に、法令に基づき適正に取得・利用・管理する必要がある。

1-2.要配慮個人情報の規定の新設

要配慮個人情報とは、法定されている人種、信条、社会的身分、病歴、前科・前歴、犯罪被害情報に加え、その他本人に不当・偏見が生じないように特に配慮を要するものとして、政令で定めるものと定義されている。

政令では、まず、病歴に準ずるものとして、身体・知的・精神障害、健康診断等の検査の結果、保健指導、診療・調剤情報などが定められている。たとえば、遺伝子検査結果に含まれるゲノム情報は、「健康診断等の検査の結果」に当たることから、要配慮個人情報として取り扱う必要がある。また、前科・前歴に準ずるものとして、被疑者または被告人として逮捕、捜索等、刑事事件手続が行われた事実(結果的に無罪となった場合も含む)と、非行少年またはその疑いのある者として、保護処分等の少年保護事件手続が行われたことも要配慮個人情報に該当するとしており、法律に掲げられている事項に準ずる内容を限定的に取り上げている。ガイドラインでそれぞれの具体的な範囲や考え方が示されている。

要配慮個人情報については、原則、取得・第三者提供時の本人同意が必要となることから、これまでオプトアウトを利用して要配慮個人情報を第三者提供していた事業者の場合、今後は事前の本人同意がなければ要配慮個人情報の第三者提供ができなくなることを意識しておく必要がある。ただし、人の生命・身体・財産の保護に必要な場合等には、本人同意なく取得・第三者提供することが認められる例外規定が用意されている。

なお、たとえば、ある個人が宗教関連書籍を購入したという情報だけでは、その人の信条を推定できるだけであるため、要配慮個人情報(信条)には該当しないと解される。このような例示がガイドラインに示されているので、確認してもらいたい。

1-3.匿名加工情報の規定の新設

今回の法改正では、データ利活用を促進することを目的に「匿名加工情報」についての規定が新設された。

匿名加工情報とは、特定の個人を識別できないように個人情報を加工し、当該個人情報を復元できないような形にしたもので、これについては目的外利用や第三者提供の際の本人同意を不要とし、自由な利活用が可能となっており、これによりデータ利活用ビジネスの活性化が期待される。

匿名加工方法の基準については委員会規則で定めることとされており、多種多様な事業分野、多岐にわたる個人情報すべてに適用されるルールを示す必要があることから、委員会規則では最低限の規律を設け、詳細は自主ルールに委ねることとされた。

今後、匿名加工情報を作成するにあたっては、まず、加工対象がどのような個人情報であっても、特定の個人が識別できず、元の個人情報が復元できないよう、最低限の規律として、以下①から④までの措置を講ずることが委員会規則で求められている。

①特定の個人を識別可能な記述等(氏名等)の全部または一部を削除(置換を含む。以下同じ。)すること。

②個人識別符号の全部を削除すること。

③個人情報と他の情報を連結する符号を削除すること。

④特異な記述等(例:日本最高齢者であることが判断可能な実年齢)を削除すること。

ガイドラインでは、匿名加工情報の作成方法に係る上記基準についてわかりやすく例示するとともに、「匿名加工情報」等の用語の定義や、作成時の公表等の義務の詳細について解説している。

たとえば、統計情報に関しては複数名の情報から共通要素に係る項目を抽出して集計したデータであり、特定の個人との対応関係が排斥されている限り「個人に関する情報」に該当しないため、個人情報保護法による規制の対象外となることが示されている。

また、個人情報取扱事業者は、匿名加工情報を作成したときには、インターネット等を利用して当該匿名加工情報に含まれる情報の項目を公表しなければならないが、ここでいう「作成したとき」とは、匿名加工情報として取り扱うために、個人情報を加工する作業が完了した場合のことを指す。たとえば、安全管理措置対策として個人情報の一部を削除しあるいは分割して保存、管理した場合や、個人情報から統計情報を作成するために個人情報を加工した場合は、「作成した」には含まれない。また、加工作業が完了していない場合は、加工が不十分で匿名加工情報として取り扱うことが適切でない場合が考えられるため、「匿名加工情報を作成した」とは位置付けられていない。

なお、匿名加工の手法、データ処理等については、認定個人情報保護団体による自主ルールを作成する際の参考となる事項、考え方をまとめた「事務局レポート」の作成・公表などにより、今後も情報提供を行っていくこととしている。

1-4.第三者提供に係る確認・記録義務

近年発生した大規模個人情報漏えい事案を受け、いわゆる名簿屋対策として、個人データの第三者提供に係る確認・記録と一定期間の保存が義務付けられた。第三者との間で個人データを提供・受領する場合、提供元・提供先が相互に相手の氏名・社名等を記録するとともに、提供先が提供元のデータ取得経緯等を確認・記録することで、トレーサビリティが確保され、情報流出があった場合にその流出経路の追跡が可能となる。

ただ、提供・受領の都度、企業間で確認・記録作業が発生することで、一般的なビジネスに支障が及ぶことがないよう、以下のような配慮がなされている。

・記録事項

第三者提供に関する本人同意がある場合、提供年月日の記録は不要とする。

・記録の保存期間

原則3年だが、本人に対する物品等提供に関し、本人同意のもと第三者提供した場合は、1年保存とする。

・本人との契約等に基づく提供の場合は、必要事項が記載された既存の契約書等で代替可能とする。

・反復継続して提供する場合は、包括的な記録で足りることとする。

なお、以下の場合は、一般のビジネスの実態に配慮し、確認・記録義務がかからないと整理されることがガイドラインに示されている。

・本人による提供と整理できるケース(例:SNS等に記載されている本人発信によるプロフィール)

・本人に代わって提供されたと整理できるケース(例:銀行振込)

・本人側への提供と整理できるケース(例:同席している家族)

・受領者にとって「個人データ」に該当しないと整理できるケース(例:名刺1枚)　等

1-5.外国の第三者への個人データの提供(グローバル化への対応)

改正法では、以下のいずれかの条件のもと、国内と同様に外国の第三者への個人データの提供が可能になると規定されている。

①外国にある第三者へ提供することに対し、本人が同意している場合

②外国にある第三者が、委員会規則で定める基準に適合する体制を整備している場合

基準については、一般的なビジネスの実態に配慮し、以下が該当する旨、委員会規則およびガイドラインで規定・説明されている。

・提供を受ける者における個人データの取扱いについて、適切かつ合理的な方法(例:委託契約、グループ企業内での共通の内規・プライバシーポリシー等)で個人情報保護法の趣旨に沿った措置(例:利用目的の特定、安全管理措置等、OECDプライバシーガイドラインやAPECガイドライン等の国際的な枠組みの基準を参照としながら記載)の実施が確保されていること。

・個人データを受ける企業が、個人情報の取扱いにかかる国際的な枠組み(例:APEC CBPRシステム)[1]に基づく認定を受けていること。

③外国にある第三者が個人情報保護委員会の認めた国に所在する場合

[1] APEC CBPR(Cross Border Privacy Rules)システム(越境プライバシールールシステム)
2011年に開始された、APEC参加国・地域において、事業者のAPECプライバシーフレームワークへの適合性を認証する仕組み。日本は2014年4月に参加が認められた。

なお、③については、各国の個人情報保護法制を綿密に調査する必要があり、また、主要国の個人情報保護制度が過渡期にあるため、改正法施行段階で委員会が具体的な国を定める予定はないことから、事業者は当面は①または②の条件で対応することが想定されている。

委員会では、国際的データ移転の確保のため、委員会としての方針を「個人データの円滑な国際的流通の確保のための取組みについて（平成28年7月29日個人情報保護委員会決定）」として決定し、これに基づき、諸外国との協調を進めるとともに、従来から一定の対話を続けている米国やEU（英国のEU離脱の影響についてその動向を注視）については、相互の円滑なデータ移転を図る枠組みの構築を視野に活動しているところである。

1-6.認定個人情報保護団体の活用

改正法により、認定個人情報保護団体は個人情報保護指針を作成した際には委員会への届け出が義務付けられ、委員会はその指針を公表することとされた。

また、個人情報保護指針を遵守させるための対象事業者に対する指導・勧告等が義務化されている。これにより、対象事業者における個人情報の不適正な取扱いに対して、認定個人情報保護団体において明確に対応してもらうことが、法律上、強く求められることとなる。

加えて、個人情報保護指針の作成時に、消費者代表等の関係者から意見聴取を行うよう努めることとされた。これは、いわゆるマルチステークホルダープロセスの考え方を採り入れることが定められたものである。

このような改正を踏まえ、個人情報保護指針を基に、個人情報取扱事業者が認定個人情報保護団体とともに、個人情報を適正に取り扱うための自主的な取組みを進めることが、今後も大いに期待されるところである。

認定個人情報保護団体の役割に関しては、次章「Ⅰ-2.認定個人情報保護団体の役割と期待」で詳細を解説する。

1-7.中小規模事業者への配慮

改正法により、これまで義務規定の適用対象外だった、取り扱う個人情報の数が5,000人分以下の事業者も適用対象となり、個人情報保護法への対応が必須となったことから、ガイドラインにおいて、中小規模事業者に配慮した記述を設けている。

具体的には、法律第20条に定める「安全管理措置」に関し、マイナンバー法ガイドラインに準じて定められた一般的な事業者が講ずべき措置の例示に加えて、中小規模事業者における具体的な手法を例示している。

なお、ガイドラインで示す「中小規模事業者」とは、従業員数100名以下の事業者で、以下の事業者を除く事業者を指している。

①取り扱う個人情報の数が5,000人分超の事業者

②委託に基づいて個人データを取り扱う事業者

以下、ガイドラインで紹介されている、安全管理措置に関する中小規模事業者を対象とする手法の例を一部抜粋して紹介する。

講じなければならない措置		中小規模事業者における手法の例示
個人データの取扱いに係る規律の整備について		個人データの取得、利用、保存等を行う場合の基本的な取扱方法を整備する。
組織的安全管理措置	（1）組織体制の整備	個人データを取り扱う従業者が複数いる場合、責任ある立場の者とその他の者を区分する。
	（2）個人データの取扱いに係る規律に従った運用	あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任ある立場の者が確認する。
	（3）個人データの取扱状況を確認する手段の整備	あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任ある立場の者が確認する。
	（4）漏えい等の事案に対応する体制の整備	漏えい等の事案の発生時に備え、従業者から責任ある立場の者に対する報告連絡体制等をあらかじめ確認する。
	（5）取扱状況の把握及び安全管理措置の見直し	責任ある立場の者が、個人データの取扱状況について、定期的に点検を行う。
人的安全管理措置		従業者教育については、 ・個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う。 ・個人データについての秘密保持に関する事項を就業規則等に盛り込む。
物理的安全管理措置	（1）個人データを取り扱う区域の管理	・個人データを取り扱うことのできる従業者及び本人以外が容易に個人データを閲覧等できないような措置を講ずる。
	（2）機器及び電子媒体等の盗難等の防止	・個人データを取り扱う機器、個人データが記録された電子媒体又は個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する。 ・個人データを取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤー等により固定する。
	（3）電子媒体等を持ち運ぶ場合の漏えい等の防止	個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。
	（4）個人データの削除及び機器、電子媒体等の廃棄	個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄したことを、責任ある立場の者が確認する。
技術的安全管理措置	（1）アクセス制御	個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。
	（2）アクセス者の識別と認証	機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する。
	（3）外部からの不正アクセス等の防止	・個人データを取り扱う機器等のオペレーティングシステムを最新の状態に保持する。 ・個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。
	（4）情報システムの使用に伴う漏えい等の防止	メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。

ガイドラインには、中小規模以外の個人情報取扱事業者の「手法の例示」も示しているので、それらを参照のうえ、自社の企業規模に即した対策を講じてもらいたい。

2016年10月に委員会が公表した「平成27年度個人情報の保護に関する法律施行状況の概要」によると、50,000人を越える規模の個人情報漏えい事案について、不正アクセス・不正ログイン・サイバー攻撃が最も多い原因となっていることから、安全管理措置に関し、一定規模以上の個人情報データベースを保有する事業者については、最新動向を把握し、対処してもらいたい。

2.今後のスケジュール

改正法の全面施行に向け、すでに政令、委員会規則、ガイドラインが策定されている。今後、匿名加工情報に関する事務局レポートの公表などの情報提供や、全国での周知広報を行いつつ、2017年春頃の全面施行を目指して準備を進めていく。

全面施行により各省庁から委員会に監督権限が移行することから、現在、各省庁との調整を図っているところである。情報漏えい時の報告については、原則、委員会へ報告することとなる予定だが、これまでの各省庁のガイドラインにおける規定を踏まえて詳細を検討し、ガイドラインとは別途の告示を定める方向で検討を進めている。

委員会としては、引き続き認定個人情報保護団体や各事業者等との意見交換を行いながら、改正法の円滑な施行に向けて最善を尽くしてまいりたい。

参考URL（2016年11月現在）

- 個人情報保護委員会
  http://www.ppc.go.jp/
- 個人情報保護法について（法令、ガイドライン、広報資料、各種説明会、各種問合せ窓口等）
  http://www.ppc.go.jp/personalinfo/
- 改正法の施行準備について
  http://www.ppc.go.jp/personal/preparation/

I-2.認定個人情報保護団体の役割と期待

わが国では、個人情報の保護に関する法律（以下、「法」という。）の制定以前から、事業者団体等が独自のガイドライン等を策定し、それらを基礎として、関係事業者において個人情報の保護に関する自主的な取組みが展開されてきたところであり、これを受けて、法の制定にあたり、民間の団体によってなされる自主的な取組みを支援する仕組みとして、認定個人情報保護団体の制度が規定されることとなった。認定個人情報保護団体の役割については法第37条第1項各号に規定されているとおり、対象事業者に関する苦情の処理、対象事業者に対する情報の提供、その他対象事業者の個人情報の適正な取扱いの確保に関するものであり、その一環として個人情報保護指針を作成し、公表するよう努めることが法第43条において規定されている。

2015年9月3日に成立し、同年9月9日に公布された改正法では、現状各主務大臣が有する個人情報取扱事業者に対する監督権限が個人情報保護委員会に一元化され、これに伴って各主務大臣が事業分野ごとに策定している個人情報の保護に関するガイドライン等についても、原則として個人情報保護委員会（以下、「委員会」という。）が策定するすべての事業分野を対象とするガイドラインに集約されることが予定されている。しかしながら、委員会が策定するガイドラインは、すべての事業分野に共通して適用されるものであるため、その内容は汎用的なものとならざるを得ない。それゆえ、改正法下においては、事業分野ごとの事情に即した個人情報の保護に関する取組みの担い手として、認定個人情報保護団体に対し、より大きな期待がかかることになる。本稿では、法の改正を踏まえた認定個人情報保護団体の役割とこれに対する期待について、述べることとしたい。

改正法においても、認定個人情報保護団体は従前と同様に、対象事業者に関する苦情の処理、対象事業者に対する情報の提供、個人情報保護指針の作成に努めることが役割とされているところである。そして、事業分野ごとの実情に即した個人情報および匿名加工情報の適正な取扱いの確保に向けて認定個人情報保護団体の役割への期待が大きくなることを踏まえ、これら従前の役割を基礎として、次の４点が改正されることとなった。

第一に、個人情報保護指針の作成にあたって、消費者の意見を代表する者をはじめとする関係者の意見を聴く努力義務が課せられたことである。いわゆるマルチステークホルダープロセスの考え方が制度として定められたものであり、これにより事業者に限られない、さまざまな利害関係を有する主体の意見が集約され、個人情報保護指針の内容が公平かつ適正なものとなることが期待されている。

第二に、作成した個人情報保護指針の委員会への届け出が義務付けられ、委員会によって各個人情報保護指針が公表されることとなったことである。現在は、認定個人情報保護団体自身によって公表することが努力義務とされているにとどまるが、ここでも外部の目によって個人情報の一層適正な取扱いが促進されるよう、どのような（種類の）事業者がどのような個人情報保護指針の下で個人情報を取り扱っているかをわかりやすくすることを狙って、改正されたものである。

第三に、対象事業者に個人情報保護指針を遵守させるために必要な指導、勧告その他の措置を取ることが、現在の努力義務から、義務へと強化されたことである。個人情報保護指針の公開が必ず行われるようにすることとあわせて、個人情報保護指針に則った個人情報等の適正な取扱いの徹底を図ることを目的としている。認定個人情報保護団体においては、対象事業者における個人情報保護指針の遵守状況を確認し、適切に遵守されていない場合にはこれに対して指導や勧告を行うための体制整備が求められる。

第四に、匿名加工情報についても、その業務の対象とすることができるようになったことである。今般法改正によって導入された匿名加工情報の制度に関しては、事業分野ごとの個人情報の取扱いの実情に応じて個人情報を匿名加工情報とするための加工方法を定めることが望ましいことから、法令および委員会のガイドラインは必要最小限の規定とし、具体的な加工の方法等は認定個人情報保護団体の個人情報保護指針において規定されることが期待されている。そこで、事業の性質上匿名加工情報の利用・流通が見込まれる分野の事業者を対象とする認定個人情報保護団体において、匿名加工情報について、マルチステークホルダープロセスを踏んだ上でそれぞれの事業分野の特質を反映した個人情報保護指針として定められることが期待される。

①個人情報保護指針の作成に関する手続の充実

- 個人情報保護指針の作成にあたって消費者の意見を代表する者その他の関係者の意見を聴く努力義務を規定。いわゆるマルチステークホルダープロセスの考え方を制度化。

②作成された個人情報保護指針の公表を担保する措置

- 作成した個人情報保護指針の個人情報保護委員会への届け出を義務化。
- 個人情報保護委員会において届け出られた個人情報保護指針を公表することで、作成された個人情報保護指針の公表を担保。

③対象事業者による個人情報保護指針遵守を担保する措置

- 対象事業者に個人情報保護指針を遵守させるために必要な指導、勧告その他の措置を取ることを義務化。

④業務範囲の拡大

- 対象事業者における匿名加工情報の取扱いについても、その業務の対象とすることが可能に。
- 事業分野ごとの特質を反映した個人情報保護指針として、具体的な加工の方法等が規定されることを期待。

図1　認定個人情報保護団体に関する制度改正のポイント

これらに加えて、個人情報取扱事業者において法第20条所定の安全管理措置に関する不祥事案、すなわち個人データの漏えい、滅失または毀損等が生じた場合、個人情報取扱事業者には、安全管理措置の一環として、その旨を委員会に報告するよう努めることが求められるところであるが、認定個人情報保護団体においては、対象事業者に対する指導や勧告の一環として、不祥事案に係る報告の取次ぎを行う体制を整備することも、また期待されるところである。

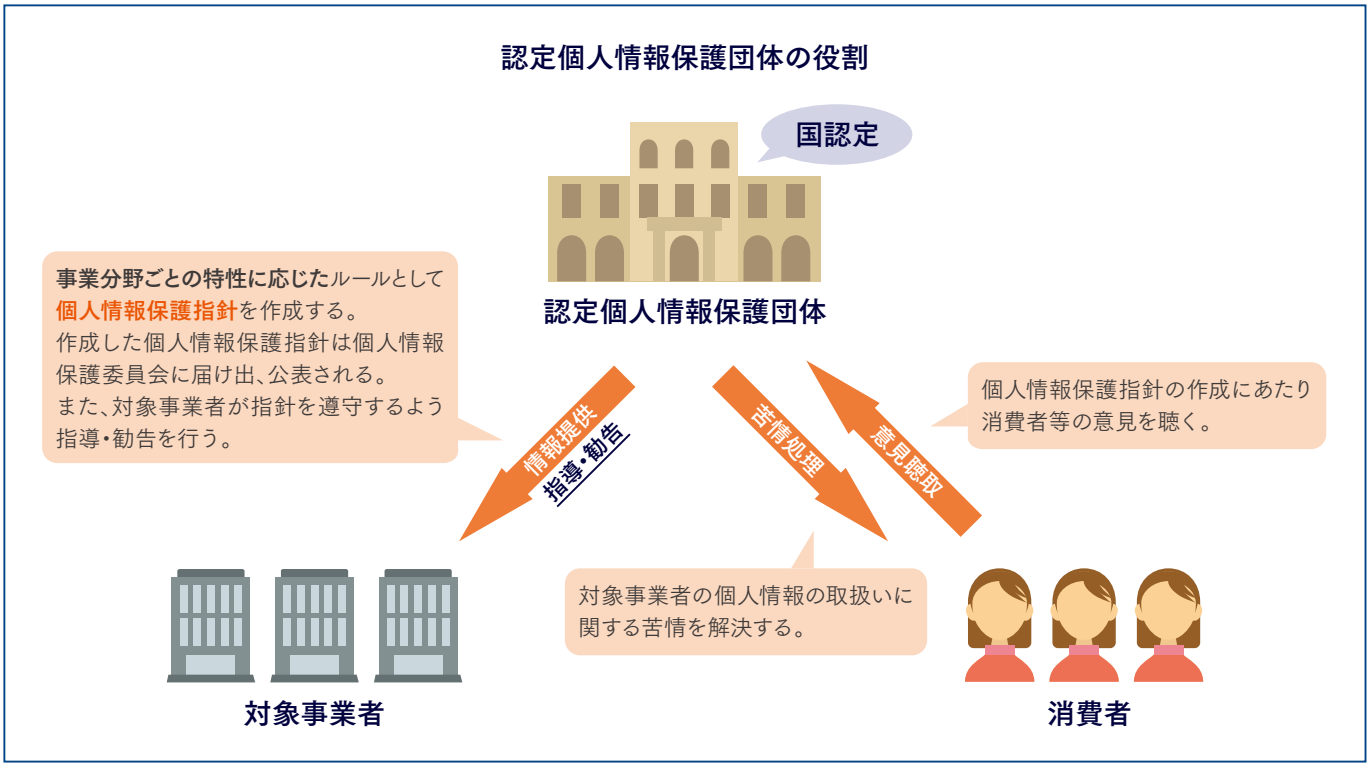

図2　認定個人情報保護団体の役割

以上述べたとおり、認定個人情報保護団体は、事業者における個別具体的な個人情報の取扱いを適正ならしめるために重要な役割を担っているものである。法の目的が達成されるよう、各認定個人情報保護団体には、その役割の重要性を認識し、適切にこれを果たしていけるよう、取り組まれることを期待するものである。

Ⅱ 海外における個人情報保護の取組みと日本の事業者に及ぼす影響

弁護士法人第一法律事務所　弁護士　福本　洋一

1.一般データ保護規則（GDPR）

1-1.沿革

欧州議会本会議において、2016年4月14日にEU一般データ保護規則（General Data Protection Regulation、以下、「GDPR」という。）が可決された。

EUにおいては、1995年にEUデータ保護指令（Data Protection Directive、以下、「DPD」という。）が採択され、1998年から発効されているが、急速なICTの進歩およびグローバル化の進展によるデータ共有・収集の規模の劇的な増大、オンライン環境における信頼性の確保に対応するために、DPDの見直しが求められるようになった。

また、各EU加盟国はDPDに基づき国内法を制定しているが、EU加盟国間における個人データの保護レベルに差異が生じており、情報の流通を妨げる点が問題視されていた。EU域内における情報の流通の障害を取り除くために、各EU加盟国において立法措置を要する「指令」から、EU加盟国に直接適用される「規則」に変更され、欧州委員会から2012年1月25日にGDPR提案が発表されるに至った。

その後、2014年3月に欧州議会において修正案が可決、2015年6月に閣僚理事会において修正案が承認された後、2016年4月14日に欧州議会本会議で可決され、4年以上にも及ぶ歳月をかけてGDPRが成立するに至った。なお、GDPRの発効は2018年5月25日に予定されている。

1-2.GDPRの概要

(1) グローバル化への対応

ア　データ移転規制（44条以下）

GDPRにおいては、DPDと同様に、EU域外への個人データの移転規制がなされている。すなわち、EU域外の第三国へ個人データを移転することは、原則として、当該第三国が十分なレベルの保護措置（adequate level of protection）を確保している場合以外は禁止されている。欧州委員会から十分性認定を受けているのは、カナダ、スイス、ニュージーランド等の11の国と地域のみであり、日本、米国、中国等の主要各国は、十分性認定を受けていない。

これらの欧州委員会による十分性認定を受けていない国の第三者に、EU域内のデータ主体の個人データを移転するには、当該移転の当事者において、以下のいずれかの適切な保護措置が講じられていることが必要となる。なお、①ないし③の保護措置はいずれもDPDにおいて認められていたものであり、GDPRでは、主に中小規模の企業において利用されることを前提として、新たに④の保護措置が導入された。

①データ主体からの明確な同意の取得

②EU域内の提供元とEU域外の提供先との間における欧州委員会が認めた標準データ保護条項（standard data protection clauses）の締結

③グローバルなグループ企業内で適用される拘束的企業準則（Binding Corporate Rules、以下、「BCR」という。）の策定および管轄監督機関による承認

④EU域内のデータ移転元において、認証機関または管轄監督機関から、GDPRを事業内容に合わせて遵守することを定めた行動規範（Codes of conduct）の承認あるいは一定の認証メカニズム（certification mechanism）を取得するとともに、EU域外のデータ移転先において、拘束的および執行力のある公約（binding and enforceable commitment）を実施

上記の保護措置の利用状況について、上記①のデータ主体の同意取得に関しては、そもそも特定のサービスの提供等のために個人データを取得する際に、すべてのデータ主体から同意を得ることは困難であるし、またデータ主体が一旦同意をしたとしても、事後的に任意に同意を撤回することができるため、移転先にとって情報管理上のコストがかかることから、実務上は利用困難であるとされる。

また、③のBCRに関しては、EU域内の関係国のデータ保護機関(Data Protection Authority、以下、「DPA」という。)から承認を取得する必要があるため、相当の時間と費用を要することから、大規模な多国籍企業において利用されているのみで、現在のところ、日本の企業においては利用されていない。

④の行動規範とデータ保護認証については、GDPRにおいて新たに導入された制度であるため、具体的な内容については現時点では明らかではない。

したがって、GDPRの発効後も当面の間は、②の標準データ保護条項(DPDにおいては標準契約条項、SCC)の締結が主に利用されるものと思われる。

なお、上記のデータ移転規制に違反した場合には、制裁金として、最大で2,000万ユーロ(約23億円)または全世界の年間総売上の4%のいずれか高い方の金額を課されうることになる。

イ　域外適用(3条)

GDPRにおいては、EU域外の管理者または取扱者(管理者のために個人データの取扱いを行う者)に対しても、EU域内にあるデータ主体から個人データを収集する一定の場合については、GDPRを直接適用するという域外適用規定が設けられた。すなわち、EU域外の管理者等であっても、EU域内にあるデータ主体に対し、有償・無償を問わず、商品またはサービスを提供する場合や、EU域内にあるデータ主体の行動をモニタリングする場合には、GDPRの義務を履行することが求められる。

たとえば、EU域外にある事業者が、EU域内にあるデータ主体に対し、インターネットを利用した商品の通信販売を行い、発送先情報または課金情報としてEU域内のデータ主体の個人データを取得する場合や、マーケティングのためにEU域内の顧客の購買履歴を継続的に収集したり、EU域内の海外関連会社の従業員のWebの利用履歴等をモニタリングしたりする場合などが想定される。

ウ　EU域内への代理人の設置義務(27条)

GDPRが直接適用されるEU域外にある管理者または取扱者は、EU域内に代理人(representative)を設置して、書面にて明示しなければならない。代理人は、GDPRの遵守を確実にする目的のために、管理者または取扱者から、管理者もしくは取扱者とともに、またはこれを代理して、取扱いに関連するすべての問題について、監督機関およびデータ主体に対応する権限が与えられていることが求められる。

上記規制に違反した場合には、制裁金として、最大で1,000万ユーロ(約11億円)または全世界の年間総売上の2%のいずれか高い方の金額を課されうることになる。

エ　EU域外へのデータ移転の困難性

以上のように、EU域外の事業者にとっては、EU域内にあるデータ主体の個人データをEU域外に持ち出すと、標準データ保護条項の締結または域外適用によって、EU域外における個人データの取扱いについてもGDPRに基づく厳格な義務を遵守することが求められることになるため、負担する管理コストの削減の観点から、EU域内のデータ主体の個人データについては、できる限りEU域内において処理を完結させるようにビジネススキームを構築せざるを得ず、EU域内における個人データの囲込みが成立することになる。

このような意味において、GDPRはグローバルなデータ移転に対して保護主義を採用しているといえる。

(2) データ主体の権利強化

ICTの進歩によって、米国の大手IT企業をはじめとする、ビッグデータの利活用において特権的な地位を有するグローバルプ

ラットフォームが、ビジネスにおいて大量の個人データを利活用し、データ主体は自己に関する情報を十分にコントロールすることが困難な事態が生じている。GDPRはこのような事態を踏まえて、以下のようなデータ主体の権利の強化を図っている。

ア　「個人データ」の概念の拡張（4条(1)）

GDPRにおける保護の対象は、「個人データ」（personal data）である。「個人データ」とは、識別された、または識別可能な自然人に関するすべての情報とされており、日本における「個人データ」のように、データベース等を構成するものであることは求められておらず、単一の個人に関する情報でも「個人データ」に該当する。

また、「識別可能な自然人」とは、直接的もしくは間接的に、とりわけ氏名、識別番号、位置データ、オンライン識別子といった識別子を参照することによって、または身体的、生理的、遺伝的、精神的、経済的、文化的ならびに社会的なアイデンティティに特有の1つまたは複数の要素を参照することによって、識別されうる者とされている。

このように、GDPRにおいては、ICTの進歩に伴い、「個人データ」への該当性につき、位置データやオンライン識別子も識別方法として取り込み、「個人データ」の概念が拡張されている。他方、日本における改正個人情報保護法においても「個人識別符号」が含まれるものは「個人情報」として定められたが、「個人識別符号」は、顔認証データや指紋認証データ等の生体認証データおよび、運転免許証番号や健康保険証番号といった限定されたものに止まっており、位置データやオンライン識別子は含まれていない。

なお、GDPRにおいては、生体認証データも遺伝データや健康に関するデータと同様に、「特別の種類」の個人データとして、取扱いが原則禁止されている（9条）。

イ　削除権（忘れられる権利）（17条）

DPDにおいては、データ主体に不完全または不正確な個人データの消去を求める権利を認めていたが、GDPRにおいては、取得時の利用目的に照らして個人データの必要性がなくなった場合や、データ主体が同意を撤回した場合等に、データ主体が管理者に対し、自己に関する個人データの消去を請求し、当該個人データの拡散を防止するための措置を請求する権利を認めている。いわゆる「忘れられる権利」（right to be forgotten）として、GDPR提案が公表された際に話題になった権利である。

このような考え方は、2014年5月13日の欧州司法裁判所によるスペインでのGoogleに対する検索結果の削除義務の裁定が基礎にある。すなわち、自らの名前をGoogleで検索すると新聞社の1998年の記事（社会保障費の未払いにより差し押さえられた不動産物件が競売に付されるとの公告）へのリンクが表示されるとして当局に苦情を申し立てたことを契機に、Googleのリンク削除義務が争われた事例である。欧州司法裁判所は、情報内容の機微性と最初の公表からの時間的経過を考慮して、データ主体には当該情報を氏名と紐付けられない権利が認められると判断した。

なお、日本においては、さいたま地裁平成27年12月22日決定において「忘れられる権利」が認定されたが、その後、控訴審において、当該決定は取り消されており（東京高裁平成28年7月12日決定）、あくまでプライバシーの侵害の問題として整理されており、「忘れられる権利」という形では認められていない。

ウ　データポータビリティの権利（20条）

GDPRにおいては、データ主体が、①自らが提供した個人データについて、管理者から一般的に利用され、機械的に可読である体系的なデータ形式（ex. CSV形式等）にて提供を受ける権利と、②ある管理者（移行元のサービス事業者のプラットフォーム）から妨害されることなく、他の管理者（移行先の新規のサービス事業者のプラットフォーム）に対して、自らの個人データを直接移行させる権利を認めている。

データ主体は、Webメールサービス、SNSやECサイト等をはじめとした特定のITプラットフォームにより自らの個人データが囲い込まれており、他の同種のサービスを利用しようとする場合には、新たなプラットフォームに過去のデータを引き継ぐことができないことが多い。データポータビリティの権利は、こうした状況を改善し、データ主体に自らの個人データのコントロールを取り戻させ、データ主体による自らの個人データの利用機会の拡大を図ることを可能とすることを目的としたものである。

エ　取扱いに対する異議申立権（21条）

データ主体は、ダイレクトマーケティングの目的で自己の個人データが取り扱われ、またはそのような目的で「プロファイリング」に利用されている場合、管理者に対し、異議を申し立てることができ、管理者においては、そのような利用を行うことが禁止される旨が定められている。

「プロファイリング」とは、自然人に関する特定の個人的傾向を評価するために（特に、当該自然人の職務上の成果、経済状況、健康状態、個人的嗜好、関心、信頼性、行動、位置情報もしくは活動に関する傾向を分析または予測するために）、個人データを利用して行うすべての個人データの自動処理をいうとされている。

ICTの進歩に伴い、ECサイト等におけるオンラインでの商品購入の際に、ダイレクトマーケティングの目的で、過去の購買履歴等の個人データが、推薦する商品の選定・表示等のためのプロファイリングに利用されている。データ主体に対して、これらの利用を拒否する権利を付与し、自らの個人データの利用についてのコントロールを取り戻すことを目的とするものである。

オ　プロファイリングに基づく措置に服さない権利（22条）

データ主体に、自らに法的効果または重大な影響を与える措置であって、「プロファイリング」等の自動化された取扱いに基づく決定に服しない権利が認められた。

スマートフォンアプリ等を利用したオンラインサービスの普及に伴い、アルゴリズムやAIを用いて、オンラインサービス、スマートフォンやIoT（Internet of Things）機器から収集され蓄積された個人に関するデータをプロファイリングすることで、自動的に個人を類型化して管理することが可能となる。その結果、単なるターゲットマーケティング目的での利用に止まらず、与信評価に基づく融資の決定、健康状態の評価に基づく保険契約における保険加入の可否および保険料率の決定、行動モニタリングに基づく人事評価の決定等の、個人にとって重大な影響を受ける決定事項が、機械的かつ自動的に行われるようになってきている。

このような大量の個人データを集積して分析することにより、機械的かつ自動的にデータ主体の人物像が形成されて評価がなされることは、個人に対する評価の固定化を招き、個人の人格権を侵害するおそれがある。ビッグデータ時代における自らの個人データに対するコントロール権として、非常に重要な権利であると思われる。

カ　小括

以上のように、GDPRにおいては、ビッグデータの利活用において特権的な地位を有するグローバルプラットフォームから、EU域内にあるデータ主体に自らの個人データに関する実質的なコントロールを取り戻すために、データ主体の権利を強化する制度が導入されているといえる。

(3) 個人データの取扱いの厳格化

GDPRは、DPDにおける個人データの取扱いに関する規定を踏襲しているが、個人データの管理者（controller）の義務に加えて、管理者のために個人データの取扱いを行う取扱者（Processor）自身の義務を設けている。

また、GDPRにおいては、以下に詳述するとおり、「プライバシー・バイ・デザイン（Privacy by Design、PbD）」や「プライバシー影響評価（Privacy Impact Assessment、PIA）」といった、他国が実施する個人データの保護に関する仕組みが積極的に取り込まれている。

その背景としては、EUが世界的に最も保護レベルが高い制度を維持することで、他国との関係において個人データの移転規制を受けず、EU域内への個人データの集積をグローバルに促進させることにあるものと思料される。

ア　取扱者の義務等（28条）

取扱者（Processor）とは、管理者のために個人データの取扱いを行う自然人、法人、公的機関、行政機関またはその他の団体をいう（3条(8)）。日本の個人情報保護法においては、「個人情報取扱事業者」としての管理者から個人データの取扱

いの受託を受けた「委託先」に相当する者と理解される。

管理者は、GDPRの要件に適合し、データ主体の権利の保護を確実にする取扱方法で、適切な技術的かつ組織的な措置を実施することを十分に保証する取扱者のみを利用することが義務付けられている。

そして、取扱者は、事前の特定または管理者の一般的な書面の承諾なしに他の取扱者を従事させるといった再委託を禁止されており、他の取扱者に再委託する場合には、当該取扱者に契約で規定されているのと同じデータ保護義務が、契約によって他の取扱者に課されていなければならないとされている。

また、取扱者への委託に際して契約を締結することが求められており、特に取扱者が以下の事項を行うように規定しなければならないとされている。

①取扱者が従うべき EU 法または加盟国の国内法によって取扱いの実施が要求されていない限り、第三国または国際機関への個人データの移転に関することを含め、管理者からの書面による指示においてのみ個人データを取り扱うこと。当該法律によって取扱いの実施が要求される場合、取扱者は、当該法律が重要な公共の利益に基づき通知を禁止していない限り、事前に当該法的要件を管理者に通知しなければならないこと。
②個人データを取り扱うことを許可された者が機密保持を確約するか、または適切かつ法定の機密保持義務の下で管理されることを保証すること。
③第 32 条（取扱いの保護）により要求されているすべての対策をとること。
④他の取扱者を従事させることに関して第 2 項および第 4 項で定める条件を遵守すること。
⑤取扱いの性質を考慮し、可能な限りにおいて、管理者が第 3 章に定められたデータ主体の権利行使の要求に応じる義務を履行するため、適切な技術的かつ組織的な措置によって管理者を支援すること。
⑥取扱いの性質および取扱者の利用可能な情報を考慮し、第 32 条から第 36 条による義務（取扱いの保護、個人データ侵害の監督機関への通知、データ主体への個人データ侵害の通知、データ保護影響評価、事前協議）の遵守を確実にすることにおいて管理者を支援すること。
⑦管理者の選択により、取扱いに関連したサービスの提供終了後にすべての個人データを消去または管理者に返却することおよび、EU 法または加盟国の国内法が個人データの保存を要求しない場合に限り、存在する複製物を消去すること。
⑧本条項に定められた義務の遵守を証明するとともに、管理者または管理者により委任された他の監査人によって実施される調査を含めた監査への準備および寄与を行うために必要なすべての情報を管理者が入手可能にすること。

イ　情報処理の記録義務（30条）

管理者またはその代理人には、個人データの取扱いに関し、以下の事項を書面（電磁的記録を含む。）にて記録する義務が定められている。ただし、従業員の数が250名未満の中小規模の企業等には適用されない。

①管理者（その代理人、データ保護オフィサー）等の氏名・名称および連絡先
②利用目的
③データ主体の種類および個人データの種類
④個人データが開示されるまたは開示されうる場合の提供先の種類
⑤第三国または国際機関への個人データ移転の事実等
⑥可能であれば、データの種類ごとの消去の予定期限
⑦可能であれば、技術的・組織的安全管理措置の概要

また、取扱者またはその代理人には、書面にて、以下の事項の記録義務が定められている。ただし、従業員の数が250名未満の中小規模の企業等には適用されない。

①取扱者および管理者（それらの代理人、データ保護オフィサー）等の氏名・名称および連絡先
②管理者のために実施している取扱いの種類
③第三国または国際機関への個人データ移転の事実等
④可能であれば、技術的・組織的安全管理措置の概要

ウ　個人データの漏えいの通知義務等（33条・34条）

管理者は、個人データの漏えいが発生した場合には、原則として、当局に対し、当該事実の発生を知ってから72時間以内に通知を行う義務を負う。具体的には、少なくとも以下のような事項を通知しなければならない。

①個人データの漏えいの性質（可能であれば、関係するデータ主体の種類と概数、関係する個人データの種類と概数）
②データ保護オフィサーの氏名・連絡先
③個人データの漏えいにより想定される影響
④個人データの漏えいに対する対処措置（漏えいによる影響を軽減するための対策）

また、取扱者においては、自らの管理下において個人データの漏えいが生じ、当該事実の発生を知った場合には、遅滞なく管理者に通知する義務を負う。

管理者は、個人データの漏えいに関する事実ならびにその影響および対応策を含めて、すべての個人データの漏えいについて書面で記録する義務を負い、当該書面をもって監督機関が上記の義務の遵守状況を確認できるようにしなければならない。

また、個人の権利および自由に対し、高いリスクを生じさせるおそれがある場合には、管理者は、遅滞なく影響を受けた個人に対して通知する義務もあり、その際には、少なくとも上記の②ないし④の事項について通知することが求められる。

なお、上記の通知義務は、米国カルフォルニア州において、2002 年に制定された「California Security Breach Notification Act」（セキュリティ侵害通知法）を参考に導入されたものである。同法においては、データの漏えいの発見または通知があった際には、暗号化されていないその個人情報が、許可されていない人によって取得された、または合理的に考えて取得されたと考えられるカリフォルニア州住民に対して、システムからの情報漏えいを開示することを義務付けている。

エ　データ保護・バイ・デザイン／デフォルト（25条）

データ保護・バイ・デザイン（Data protection by design）として、管理者は、GDPRの要件を満たし、データ主体の権利を保護するために、個人データの取扱方法の決定時点と取扱時点のいずれの時点においても、たとえば仮名化のように、適切な技術的かつ組織的な対策を実施することが義務付けられており、そのような対策として、たとえばデータ最小化のように、データ保護の原則を効果的な方法で履行すること、および必要な保護措置を個人データの取扱いの中に組み込むことが求められる。

また、データ保護・バイ・デフォルト（Data protection by default）として、管理者は、既定で具体的な特定の利用目的のために必要な個人データのみが取り扱われることを確実にするために、適切な技術的かつ組織的な対策を実施する義務を負う。

上記の制度は、カナダで提唱されたプライバシー・バイ・デザイン（PbD、情報技術に関する仕様の設計段階からプライバシー保護の対策を組み込むという考え方）を取り込んだものである。

オ　データ保護評価の実施（35条）

新しい技術を用いた取扱いが、自然人の権利および自由に対し、高いリスクを及ぼすおそれがあると想定される場合には、管理者は、取扱いに先立ち、予定されている取扱作業に対する個人データの保護に与える影響評価（Data protection impact assessment、以下、「DPIA」という。）を実施する義務を負う。特に、プロファイリングを含めた自動処理に基づいて

自然人に関する個人的側面が体系的かつ広範囲に評価され、その評価に基づいて当該自然人に法的効果または重大な影響を与える決定がなされる場合や、特別な種類の個人データ(いわゆる機微情報)または有罪判決および犯罪に関する個人データを大規模に取り扱う場合、第三者が立ち入れない場所において大規模なモニタリングを行う場合には、DPIAを実施することが求められる。

上記のDPIAは、米国、カナダやオーストラリア等で行われてきたプライバシー影響評価(PIA、情報システムにおけるプライバシー保護策に対する評価手法)を取り込んだものである。

カ　データ保護オフィサーの設置義務(37条以下)

管理者または取扱者の主要事業において、①その性質、適用範囲および／または目的によって、大規模にわたるデータ主体の定期的かつ系統的なモニタリングが必要となる場合、②機微情報等の「特別な種類」の個人データまたは犯罪関連データの大規模な取扱いが必要となる場合には、データ保護オフィサー(Data Protection Officer、以下「DPO」とする。)を設置することが義務付けられている。「特別な種類」の個人データとは、人種、民族、政治的思想、宗教的信条、労働組合の加入、遺伝データ、生体情報、健康、性生活、性的指向に関するデータをいう。

DPOは、専門家としての資質に基づいて指名されるものとし、特にデータ保護法および慣例に関する専門知識ならびに事業者における個人データの取扱いを、独立した立場で監督・指導する業務を遂行する能力を有することが求められる。

キ　制裁金(83条)

管理者または取扱者がそれぞれに課される義務に違反した場合には、制裁金として、最大で1,000万ユーロ(約11億円)または全世界の年間総売上の2％のいずれか高い方の金額を課される。また、主としてデータ主体の権利を侵害した場合には、制裁金として、最大で2,000万ユーロ(約23億円)または全世界の年間総売上の4％のいずれか高い方の金額を課される。

なお、制裁金を課すか否かの決定および個別案件において支払われるべき制裁金の金額の決定に際しては、以下の事項を考慮することになっている。

①取扱いに関する性質または目的ならびに影響を受けたデータ主体の数およびデータ主体の受けた損害の程度を考慮した、違反の性質、重大さおよび期間
②違反の故意または過失
③データ主体に及ぼす損害を軽減させるために、管理者または取扱者が講じた措置
④管理者または取扱者によって実施された技術的かつ組織的な措置を考慮した、管理者または取扱者の責任の程度
⑤管理者または取扱者の過去の関連するすべての違反
⑥違反の是正および違反により想定される悪影響の軽減のため、監督機関との協力の程度
⑦違反によって影響を受ける個人データの種類
⑧監督機関に対する違反通知措置（管理者または取扱者による違反の通知の有無およびその程度等）など

以上のように、GDPRが個人データの取扱いに関して多額の制裁金を課すことにしたのは、グローバルプラットフォームを運営する事業者においては、少額な制裁金であれば納付することでGDPRを遵守しないことが想定されるため、これに対する牽制を意図したものといわれている。

ク　効果的な司法救済(79条・82条)

データ主体の権利が侵害された場合、管理者または取扱者に対する訴訟は、管理者または取扱者が事業所を有する加盟国の裁判所あるいはデータ主体が居住する加盟国の裁判所に提起することができる旨が定められている。

また、GDPR違反の結果により有形的または無形的損害を受けたあらゆる者は、その受けた損害に対し、管理者または取扱者から賠償を受ける権利を有するものとされている。

(4) GDPRが及ぼすグローバルな影響

EUは、上記のように、GDPRにおいて世界各国において実施されている個人データの保護措置を積極的に取り込み、高いレベルでの個人データの保護措置を要求している。その結果、EU域外の他国に対しては、保護レベルにおいて十分性を有する地域となり、他国が設定する移転規制の例外に該当しやすくなるため、他国にあるデータ主体の個人データが流入し、個人データが集約されやすい環境ができる。

他方で、他国がEU域内にあるデータ主体から個人データを取得しようとすると、EU域外の事業者であるにもかかわらず、標準データ保護情報の締結または域外適用によって、自国で義務付けられる保護レベルよりも厳格な管理を求められることになる。その結果、EU域内にあるデータ主体の個人データに対しては、EU域内において処理を完結することがコスト負担の軽減という意味において合理的になるため、結果として、EU域外への個人データの移転が事実上困難になる。

さらに、ビッグデータを活用したビジネスにおいては、データを特定の拠点に集積して分析することが必要となるところ、上記のようにEU域内のデータ主体の個人データをEU域外に持ち出せないため、グローバルな分析拠点はEU域内に置かざるを得ず、他国における個人データもEU域内に集積させることになる。

以上のように、EUは、GDPRによって、EU域内において個人データに対する最先端の高い保護レベルを要求し続けることによって、他国への個人データの流出を防ぎ、他国からの個人データの集積を促進する体制を整備しており、グローバルな視点からみれば、EUに世界の個人データが集積するハブ機能が根づく基礎を設けることに成功したといえる。

1-3.GDPRが日本の事業者に及ぼす影響

(1) 域外適用の影響

日本の事業者がGDPRの直接適用を受ける場合として、①EU域内にあるデータ主体に対して商品またはサービスの提供を行う場合としては、日本企業がEU域内に居住する消費者に対し、インターネットを通じて日本の工芸品の通信販売を行い、EU域内のデータ主体の住所やクレジットカード情報を取得する場合等が想定される。

また、②EU域内にあるデータ主体の行動に対するモニタリングを行う場合としては、日本企業が人事管理を目的として、インターネットを通じてEU域内の海外関連会社の従業員のWebの利用履歴の情報をモニタリングする場合等が想定される。

これらの場合、日本企業は、EU域内に代表者を設置することが求められ、日本国内において個人データを取り扱っているが、EU域内と同様にGDPRを遵守することが求められる。

以上のように、日本企業においても、EU域内の消費者を対象とした取引を行う場合やEU域内の関連会社の人事管理を日本の本社においてオンラインで一括管理するような場合には、早急にGDPRの遵守に向けた体制整備を行う必要がある。

(2) 移転規制の影響

日本の事業者がGDPRの移転規制を受ける場合としては、典型的には、EU域内の企業から日本の企業がEU域内にあるデータ主体の個人データを受領することが想定される。

もっとも、それ以外にも、日本企業がインターネットを通じて、EU域内に設置されたサーバ内でEU域内の関連会社が保有するEUにおける個人顧客や従業員に関する情報にアクセスする場合や、日本企業がEU域内の事業者から個人データに関する処理を受託して、ASPやクラウド等のオンラインサービスを提供する場合等も該当しうる。

これらの場合には、日本企業とEU域内の企業との間で、標準データ保護条項またはBCRによるデータ移転を利用することが想定され、また、日本企業が取扱者として個人データを受領する場合には、EU域内の委託企業（管理者）との間で、取扱者である日本企業がGDPRに従った保護措置を講じることを義務付けられた契約を締結することが想定される。

したがって、日本企業は、いずれの場合においても、当該契約等に基づいてGDPRに従った個人データの管理を求められることになる。

このような場合、日本企業において個人データの漏えい等が生じた場合には、EU域内の管理者が多額の制裁金を課されるおそれがあり、日本企業としてはその損害の賠償責任を問われるおそれがある。したがって、EU域内の企業との契約において、準拠法との関係で条項の有効性を検証する必要はあるが、一定の金額を損害賠償額の上限とするような賠償制限条項を入れ

ておくことが望ましいと思料される。

なお、日本企業が取扱者として受領する場合については、取扱者の義務違反によって個人データの漏えい等が生じた場合には、日本企業自体が直接制裁金を課される可能性もあるものと思料される。

(3) 小括

以上のように、日本企業であったとしても、EU域内の個人データを取り扱うと、EU域内にあるか否かを問わず、GDPRの直接適用または契約等を通じたGDPR遵守を求められることになる。そのような意味において、GDPRは日本企業にとっても重大な影響を及ぼす規則である点に留意が必要である。

すでにEU域内にあるデータ主体の個人データを取り扱っている日本企業においては、すでにDPDの標準契約条項の締結等によって、一定の情報管理の体制整備はなされているはずであり、DPDに基づくEU加盟国の国内法に基づく義務からGDPRによって変更された義務に対して、新たに対応することが求められる。

2.プライバシーシールド制度

2-1.制度制定の背景・経緯

(1) セーフハーバー協定

米国は、EUから現在も十分性の認定を受けていないため、DPDによるデータ移転規制を受けることになるが、EUと米国との間における個人データの移転については、1999年に欧州委員会と米国商務省の間で締結された「セーフハーバー協定(Safe harbor Agreement)」によって認められていた。

同協定は、米国の事業者がDPDに準じたデータ保護ができていることを自己宣言し、米国商務省がこれを承認して登録することで、当該事業者に限って個人データの移転を認めるというものである。

(2) スノーデン事件の影響

セーフハーバー協定については、同協定に基づいて米国の事業者が受領した個人データの保護については、米国の国家安全上の必要性によって限定されており、米国の事業者は、協定上の義務にかかわらず、米国法の遵守が求められるものであった。その結果として、米国政府は、「外国諜報監視法」(Foreign Intelligence Surveillance Act・FISA)によって、米国の事業者がEUから受領した個人データに対して諜報目的でアクセスできるという問題点をEU側から懸念されていた。

実際にその懸念が顕在化したのが、2013年のスノーデン事件であった。米国のNSA(国家安全保障局)およびCIA(中央情報局)の元局員であるスノーデン氏が、NSAやCIAによる外国首脳の電話盗聴、大使館への盗聴等の事実と、Microsoft、Yahoo!、Google、Facebook、YouTube、Skype等の大手IT企業が諜報活動に協力させられていた事実を暴露した。スノーデン事件を契機として、EUにおいて米国政府および米国企業に対する不信感が広がった。

(3) セーフハーバー協定の無効の判決

オーストリア市民のFacebookユーザが、スノーデン事件を受けて、Facebook によって十分な保護措置がなされていない米国に対して自身の個人データが転送されたとして、アイルランドのデータ保護機関に対して、自己の個人データの米国への提供の禁止を求めたが、審査を拒否されたため、訴訟となった。

アイルランド上級裁判所は、欧州司法裁判所に対して、欧州委員会が決定したセーフハーバー協定の有効性に対する申立てに対し、アイルランドのデータ保護機関が欧州委員会決定の内容について審査をすることができるか否かの判断を求めた。

欧州司法裁判所は、セーフハーバー協定については、自己認証した上で個人データを受領する事業者を拘束するもので、米国の行政機関が遵守すべき基準にはならないことや、米国の安全保障上の必要性を一方的にEU市民の基本権よりも優先させている点等を指摘して、2015年10月にセーフハーバー協定を無効とする判決を行った。

2-2.プライバシーシールド制度の概要

(1) 概要

上記欧州司法裁判所によってセーフハーバー協定が無効とされたことで、欧州委員会は、米国商務省との間でこれに代わる新たなフレームワークについての協議を重ね、2016年2月に、EU-USプライバシーシールド（EU-US Privacy Shield）の原案を公表し、2016年7月に正式に合意して発効された。

(2) プライバシーシールド制度とセーフハーバー協定との違い

プライバシーシールド制度においては、セーフハーバー協定に関して指摘された問題点を踏まえて、米国政府によるアクセスに対する明確な保護措置と透明性が求められ、米国の政府当局が無差別・大量の調査をしないことの保証が定められている。

また、事業者に対しても義務が強化され、米国商務省および連邦取引委員会（FTC）に強力な監視および執行権限が付与されている。

米国の事業者には、プライバシーシールドの要件への適合性について年次の自己確認の実施、Webサイトへのプライバシーポリシーの公表、個人からの救済申請に対して45日以内の回答、人材に関する個人データを扱っている場合のEUのデータ保護機関への協力等が求められる。

2-3.日本の事業者に対する影響

プライバシーシールド制度は、あくまでEUと米国との間の個人データの移転規制に関する例外であるため、直接的に日本の事業者に適用されるものではない。

現在、日本においても、2016年10月28日に閣議決定された「個人情報の保護に関する基本方針」に基づき、個人情報保護委員会が、同年11月に公表した「国際的な取組について」に基づき、米国との間では、APEC越境プライバシールール（CBPR）システムの活性化の取組みを進め、EUとの間では、改正個人情報保護法を前提として相互の個人データ流通が可能となる枠組みを想定し、それぞれと定期的な協議を行っていくことが予定されている。

3.その他の国の動向

3-1.APEC越境プライバシールールシステムに関する動向

アジアにおいては、国境を越えて移転する個人情報を適切に保護するため、APEC越境プライバシールールシステム（Cross Border Privacy Rules System、CBPR システム）によって、事業者のAPECプライバシーフレームワークへの適合性の国際的な認証が行われており、日本も2014年4月に参加が認められた。

事業者がこの認証を受けるためには、アカウンタビリティエージェント（Accountability Agent、以下、「AA」という。）から、CBPRシステムの最低限の要求事項を遵守しているかの審査を受けることが必要となるが、2016年1月に、日本で初めて一般財団法人日本情報経済社会推進協会（JIPDEC）がAAとして認定された。

3-2.日本における影響

日本の改正個人情報保護法において導入された「外国にある第三者への提供制限」（24条）については、海外の第三者が「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の基準」に適合する場合には適用されないが、この基準の1つとしてCBPRの認証を得ていることが想定されており、今後日本においても、日本の個人データを海外の関連会社や委託先へ提供するために、CBPRシステムの活用が期待されるところである。

Ⅲ 国内外の個人情報保護関連の年表

日本	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」制定（10 月）
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
	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		

日本	年	海外	
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－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	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（2015 年 6 月に失効）
「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）
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）			

〈資料〉 情報化に関する動向（2016年4月～2016年9月）

2016年4月

国内

- 警視庁、サイバー犯罪対策本部新設。2020年東京五輪・パラリンピックを見据えたサイバー犯罪の最新情勢、捜査情報の一括集約を目指す。
- DeNA、自社運営のゲームサイト「モバゲー」への不正ログインにより、10.4万件の利用者情報が閲覧可能に。
- 国立情報学研究所（NII）、「サイバーセキュリティ研究開発センター」設置。サイバー空間上の学術研究機関の安全な研究環境の確保とともに、大学と連携した人材育成も。
- 消費者庁、名簿販売事業者ヒアリング調査結果を発表。調査に応じた8事業者が取り扱う個人情報DBの形態や名簿等の買取・取得単価価格などを公表。
- 理化学研究所、AIPプロジェクト（人工知能、ビッグデータ、IoT、サイバーセキュリティ統合プロジェクト）を担う研究開発拠点として、革新知能統合研究センター設置。
- サイバーセキュリティ基本法改正。国による不正通信の監視、調査、原因究明等の対象範囲を独立行政法人、特殊法人・認可法人にまで拡大。
- 日本テレビ、サイバー攻撃により視聴者等の個人情報約43万件が流出。7月に調査報告書公表。
- J-WAVE、Webサイトへの不正アクセスによりリスナーの個人情報約64万件が流出。6月に調査報告書公表。
- ブロックチェーン推進協会設立。国内におけるブロックチェーン技術の普及啓発、研究開発促進、関連投資促進等が目的。
- 東京都、サイバーセキュリティ対策強化に向け、警視庁、中小企業支援機関5団体と相互協力協定締結。相談窓口の設置や対策強化支援のための「東京中小企業サイバーセキュリティ支援ネットワーク」を設立。
- 警察庁、テロ対策として、SNSなどインターネット上の情報を常時点検し、テロ関係者などの情報を自動に収集・分析する「インターネット・オシントセンター」設置。
- 日本ブロックチェーン協会発足。ブロックチェーン技術の社会インフラへの応用、政策提言や国内での仮想通貨ビジネス振興・普及を目指す。
- 経済産業省、ドイツ経済エネルギー省とIoT/インダストリー4.0協力に係る共同声明に署名。日独間でIoT/インダストリー4.0の課題（産業サイバーセキュリティ、国際標準化、規制改革等）解決に向けて連携。
- 情報処理推進機構（IPA）、アイルランド研究機関IVIと、人材育成のための相互協力協定締結。IPAの人材育成ツール「iコンピテンシディクショナリ」とIVIの「IT-CMF」の相互補完による連携・協力関係を深める。
- エイベックス、不正アクセス被害による約35万人分の個人情報流出を発表。その後、6月公表の調査委員会報告書により、約64万人であったことが判明。

海外

- 台湾鴻海精密工業、シャープの買収契約締結。
- 欧州議会、新たな個人情報保護施策として、「GDPR（一般データ保護規則）」可決。個人データの保護対象範囲の拡大や保護対象となる個人、欧州連合（EU）域外の企業による個人データのEU域外持出しを厳しく規制。
- Microsoft、同社クラウド利用者に無断でメール開示を要求するのは憲法違反として、米司法省を提訴。
- 米最高裁判所、Googleの書籍全文検索サービス「Google Book」が著作権侵害にあたらずとして、米作家協会からの訴えを退ける。
- EU、GoogleのAndroid端末メーカに対するGoogleアプリインストール強要がEU競争法に反するとして異議告知書を送付。
- 米プライバシー擁護団体電子フロンティア財団（EFF）、米司法省に対し、政府が企業に対し顧客データを秘密裏に暗号解読するよう命じたかについて、情報開示義務があるとして提訴。
- 米政府、Appleの支援なしに麻薬密売者のiPhoneロック解除。4月上旬の時点では同社に解除を要請するも、その後、ニューヨーク州の裁判所に支援不要を提出。
- 独Bitkom調査、ドイツ産業界の3分の2以上企業が過去2年間にサイバー犯罪や海外の諜報活動の影響で個人情報の盗難、産業スパイ、破壊工作の被害に。
- 米連邦捜査局（FBI）、技術の脆弱性の確認・開示を判断する米政府方針「Vulnerability Process」に従って、iPhoneとMacのソフトウェアの脆弱性をAppleに通知。
- 先進7か国（G7）情報通信相会合、情報通信技術活用の理念を示す「憲章」と行動計画をまとめた「共同宣言」を採択。経済成長を妨げかねない中国、ロシア政府によるネット規制をけん制し、サイバーセキュリティの向上による国際協調を図る。
- Google、Ford、Uberら、自動運転連合「Self-Driving Coalition for Safer Streets」設立。連邦政府レベルでの自動運転車の安全基準等の整備・実現化を目指す。

国　内	海　外
2016年5月	
・IPA、情報セキュリティに対する経営者の関与、組織的取組みについて日・米・欧で比較調査実施。日本はCSIRT設置満足度や担当者の質的充足度が欧米に比べて低い結果に。 ・サイバーエージェント、自社運営の「Ameba」へのリスト型攻撃を受け、5万件の不正ログインが発覚。 ・大阪府警、大阪市教育委員会のサーバにDDos攻撃を仕掛け、市内444校のWebサイトを一時閲覧不能にした高校生（犯行当時中学生）を電子計算機損壊等業務妨害容疑で書類送検。自治体に対するサイバー攻撃での立件は全国初。 ・IDC Japan調査、国内IoT市場規模は約6.2兆円。2020年には13.8兆円に拡大と予測。 ・行政機関個人情報保護法成立。改正法により行政機関が保有する個人情報を匿名加工情報として企業に提供することが可能に。 ・全国17都府県のコンビニATMで、南アフリカの銀行発行のクレジットカード情報が偽造され、14億円の不正引出し被害。 ・科学技術振興機構、文部科学省が開始したAIPプロジェクトの実施機関としてAIPネットワークラボの運営を開始。理化学研究所とも連携。 ・個人情報保護委員会、2015年度年次報告でマイナンバー漏えい事案に関する報告が83件、苦情あっせん相談窓口の受付状況が993件あったと公表。 ・通信傍受法改正。通信傍受対象の犯罪が拡大され、通信内容を自動的に暗号化して保存できる機器があれば、通信事業者の立会いなく、警察施設等での傍受が可能に。 ・資金決済法改正。ビットコインなどの仮想通貨に財産的価値があるとして物品、サービスの対価としての使用が可能に。仮想通貨取引所を登録制として、金融庁の監督下に。 ・トレンドマイクロ調査、2016年第四半期のサイバー攻撃の動向としてランサムウェア脅威が拡大。国内での検出台数は前年同期比9.2倍に。 ・内閣府、AI研究開発、産業利用時の倫理指針、法制度問題検討に向け、有識者による「人工知能と人間社会に関する懇談会」開催。年度内に意見を取りまとめ、科学技術イノベーション総合戦略に反映させる。 ・厚生労働省調査、2015年末に流出した健康保険証番号を含む約10万人分の個人情報について、36都道府県1万8,470人分の番号が5月時点で使用されていることを発表。 ＜JIPDECトピックス＞ ・スターティアの法人向けオンラインストレージとJCAN証明書を利用した電子契約サービス開始。	・MicrosoftとGoogle、世界各国で双方が争っていたすべての訴訟取下げで合意。 ・中国国家工商行政管理局、電子商取引企業に対する監視強化、違反への厳罰、虚偽、違法オンライン広告の取締りのため、5～11月をキャンペーン期間に設定。 ・中国ネット通販大手Alibaba、2016年3月期決算が米小売最大手Wal-Martを抜き、流通総額4,850億ドルで世界一に。 ・Facebook、自社商品ブランド名を「Face book」と商標登録した中国食品業者珠江飲料廠に対する商標侵害訴訟で勝訴。 ・米・中国両政府、サイバー空間での国際安全保障のため、サイバー問題を専門とする外交、国防当局者による初の会合をワシントンで開催。 ・米LinkedIn、2012年にビジネスSNSからユーザのパスワードなど約650万人分が流出した事件で、2016年5月時点で1億1,700万人分にまで影響が拡大している可能性を発表。 ・Google、仏情報処理・自由全国委員会（CNIL）による全世界のドメインでの「忘れられる権利」に基づく情報削除実施命令（2016/3）に対し、仏最高行政裁判所に上告。 ・仏捜査当局、法人税や付加価値税、約16億ユーロの脱税容疑でGoogleパリ支店を家宅捜索。 ・Google、Oracleが提訴したJava関連の著作権侵害訴訟裁判で勝訴。 ・欧州委員会（EC）、Facebook、Twitter、YouTube（Google）、Microsoftが欧州でのヘイトスピーチ対策のための「code of conduct（行動規範）」に署名し、通知から24時間以内のヘイトスピーチの削除・遮断対応に合意したと発表。

2016年6月

国内

- 産業競争力会議、成長戦略「日本再興戦略2016」で名目国内総生産（GDP）600兆円に向けた成長戦略として「官民戦略プロジェクト10」を創設。IoT、ビッグデータ、AI、ロボットなどで創出する市場を30兆円規模に育て、第4次産業革命の実現を目指す。
- IoT推進コンソーシアム、IoT事業を手掛ける中小企業への支援を開始。傘下のIoT推進ラボが自治体や企業のマッチングイベント開催。
- 経済産業省、「電子商取引及び情報財取引等に関する準則」改訂。電子商取引や情報財取引等の実務、関連技術動向、国内外のルール整備の状況を踏まえ、既存項目の一部改訂と、データ消失時の顧客に対する法的責任を追加。
- 日・米・欧・中・韓による5大特許庁長官会合開催。IoT、人工知能等新技術に対応した知的財産制度推進等を目指す「五庁共同声明2016（東京声明）」合意。
- 日立製作所、大量の日本語記事を分析・判断し、意見を日本語で提示できる人工知能の基礎技術開発。
- 情報通信研究機構（NICT）サイバーセキュリティ研究所、格子暗号評価アルゴリズムのC++言語の実装コード公開。
- 人工知能学会倫理委員会、人工知能研究者が守るべき倫理綱領の素案発表。
- 電気通信大学、不正アクセスを受け、学外約280万件のアドレス宛フィッシングメール送信の踏み台に。
- 特許庁、わが国初の海外での知的財産訴訟費用を賄う保険制度創設。
- JTB、3月に受けた標的型メール攻撃により、最大約679万人分の顧客情報流出の可能性を発表。
- サイバーセキュリティ戦略本部報告、2015年度の日本政府機関へのサイバー攻撃件数が前年度比約1.5倍の613万件で、過去最高に。
- 松山市、過去の健診対象者名簿約14万人分のデータを外部に持ち出した元職員が、市の個人情報保護条例違反容疑で逮捕。
- 警視庁、有料放送を無料視聴できるプログラム開発で不正アクセス不正競争防止法違反容疑で逮捕された少年が、佐賀県の教育情報システムに侵入し、個人情報を含む約21万件のファイルを盗み取ったとして、不正アクセス禁止法違反容疑で再逮捕。
- 個人情報保護委員会、アジア太平洋地域の執行機関が協力関係構築、情報交換を行う「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。

＜JIPDECトピックス＞

- メールドメイン認証DMARCをサポートするEasy Solutions社のDMARC Compassを日本で初導入。

海外

- LINE、2015年8-9月に期間限定で行った公式アプリの脆弱性発見者に対する報奨金制度「LINE Bug Bounty Program」を常設化。脆弱性の新規度、重要度にあわせた報奨金額を設定。
- 米最高裁判所、Googleの広告プログラム「AdWords」を利用した広告主による集団訴訟を不服としたGoogleの上訴を棄却。広告主らは訴訟手続きが可能に。
- Facebook、Google等IT企業、FBIが令状なしに電子通信処理記録を閲覧できる権限を付与できる「米電子通信プライバシー法改正案」への反対書簡に署名。
- 加カルガリー大学、大学関係者が10日間にわたりメール機能を停止され、サイバー攻撃を仕掛けたハッカーに2万ドル支払い。
- 米司法省、AppleとSamsungによるスマホの特許紛争について最高裁判所に巡回控訴裁への審理差戻しを求める意見書提出。
- 米民主党全国委員会、ロシア政府指揮下のハッカー集団のハッキングにより内部情報が閲覧されていたと発表。ロシア側は政府機関の関与否定。
- 米連邦巡回控訴裁判所、米連邦通信委員会が定めた「ネット中立性」規則を承認する判決。
- IBM調査、データ漏えいによる企業の損害額は平均400万ドル。セキュリティ障害の発見遅れがコスト増大にも影響。
- 台湾Acer、サイバー攻撃により、クレジットカード情報など34,500件のデータ流出。
- スパコン計算速度世界ランキング「Top500」、純中国製、中国国立研究所の「神威太湖之光」が首位。計測速度は「京」の9倍。
- 米国防総省、バグ発見者への報奨金プログラム「Hack the Pentagon」の拡大計画発表。
- 経済協力開発機構（OECD）、デジタル経済相会合をメキシコで開催。IoTの可能性を最大限に活かすため、越境データの自由な流通の促進などを内容とする閣僚宣言採択。
- 米連邦航空局（FAA）、ドローン規制緩和を発表。2年ごとの筆記試験に合格した操縦証明書取得者はパイロット免許やFAAの飛行許可が不要に。ドローンを使った宅配サービス、農業、監視などへの応用拡大へ。
- 独ダイムラー他、欧・米・日・韓11社、自動運転車に不可欠な地図・位置情報をクラウド管理するデータ形式の標準化推進で合意。日本からはパイオニアとアイシン・エイ・ダブリュが参加。
- ベルギープライバシー委員会、Facebookがユーザ以外の者に対するネット利用状況の監視がEU法令に違反するとした訴訟で敗訴。ブリュッセル上訴裁判所が委員会が監視をやめさせる権限はないと判定。

国　内	海　外
2016年7月	
・経済産業省と総務省、IoT機器、システム、サービス提供者、利用者を対象とする「IoTセキュリティガイドラインVer.1.0」策定。 ・東京動物園協会、不正アクセスによりメルマガ登録アドレス等約22,000件流出。 ・三菱東京UFJ銀行、仮想通貨取引所最大手coinbaseと資本業務提携。 ・観光庁、旅行業界における大量個人情報流出事件を受け、再発防止マニュアル策定に向けた「旅行業界情報流出事案検討会」設置。 ・外務省、サイバー空間における安全確保、各国との連携強化に向け、サイバー安全保障政策室設置。 ・東京高裁、過去の犯罪記事のGoogle表示に対し、「忘れられる権利」を認めて削除命令を下したさいたま地裁の決定を取消し。 ・東京地裁、Googleの検索結果が人格侵害に当たるとした削除命令の仮処分決定に対し、同社からの削除命令取消しを求める保全異議申立てを受け、原告の身元について本人同意のもと公になっていたことを認め、約60件の削除命令を取消し。 ・LINE、東京証券取引所とニューヨーク証券取引所（NYSE）に上場。NYSEでの初値は42ドル。IT企業では今年世界最大の上場案件。 ・富士通研究所、匿名加工情報から特定されるリスクの自動評価技術開発。最も個人を特定しやすい属性の組合せと容易度（特定しやすさ）を現実的な時間内で自動的に探索する技術の開発は業界初。 ・ソフトバンクグループ、英半導体設計大手ARMホールディングス買収を表明。3.3兆円投資額発表の影響でソフトバンク株が急落し、ARM株が急騰。9月に子会社化完了。 ・任天堂、Pokémon GOの国内配信開始。 ・日本IT団体連盟発足。53の業界団体、ヤフー、GoogleなどIT関連企業約5,000社が加盟。IT人材育成、教育の推進や団体間連携を図る。 ・東芝、64層積層プロセスを用いた3次元フラッシュメモリ「BiCS FLASH™」を開発。サンプル出荷開始は世界初と発表。 ＜JIPDECトピックス＞ ・コモドジャパンと連携し、「JCAN証明書/CMD」発行開始。	・ブラジルの裁判所、麻薬捜査に関し、Facebookが「WhatsApp」のメッセージ開示を求める連邦政府命令を無視し続けたと判断し、同社の資産約607万ドルを凍結。 ・Google、HTTPSに使用されるセキュリティプロトコルを破る恐れのある大規模量子計算機開発に備え、「Chrome」に量子暗号を搭載して技術実験開始。 ・EC、Googleに対し、欧州でのインターネット検索市場の独占的立場乱用が欧州競争法に違反するとして異議告知書送付。 ・アイルランド高等法院、Facebookが欧米間のデータ移転で被告となっている訴訟で、米国当局による意見陳述や証言での参加を認める。 ・CNIL、Microsoftに対し、Windows10の初期設定によるユーザの同意なしの過剰なデータ収集およびユーザのブラウジング追跡を停止するよう通告。 ・蘭Delft University of Technology、銅原子1個に1ビット情報を記録する技術を開発。1平方インチに約62.5TBの情報の記録が可能に。 ・Facebook、太陽光を利用したドローンの試験飛行成功。アリゾナ州上空1,000フィートを96分間飛行。 ・スロバキアESET、人気モバイルゲーム「Clash of Kings」の公式フォーラムへのハッカー不正侵入により、約160万件のアカウントが流出したと発表。 ・eMarketer調査、Twitterの世界利用者数が2億8,630万人、前年比10.9％増に。2020年には3億6,880万人に達すると予測。 ・Amazon、ドローン用ドッキングステーションの米国特許取得。 ・EFF、デジタルミレニアム著作権法が表現の自由を抑圧し、憲法に違反するとして米国政府を提訴。 ・Yahoo!、Web事業を米携帯電話サービス最大手のVerizonに約48億3,000万ドルで売却することで合意。 ・Amazon、英国運輸省民間航空局と連携し、ドローン配送システム「Amazon Prime Air」の飛行実験実施を発表。 ・Amazon、2016年上半期に米政府から受けた顧客データの個別開示要請件数は1,803件、前年比の2倍。 ・国連経済社会局、世界電子政府ランキング発表。1位英国、2位オーストラリア。3期連続トップだった韓国は3位、日本は6位から11位に後退。

2016年8月

国内

- IoT推進ラボ、「第2回Lab Selection」でDeNAの買い物代行サービスなど13件を選定。あわせて札幌市など29の自治体を「地方IoT推進ラボ」に認定。
- 内閣サイバーセキュリティセンター、企業経営者向け「サイバーセキュリティの考え方」策定。サイバーセキュリティ対策を投資と位置づけ、企業の責任と捉えて取り組むことを期待。
- 経済産業省、業界団体や企業、認定個人情報保護団体がガイドライン作成時の参考となる匿名加工情報作成マニュアル公表。
- 東京地裁、ヤフーの検索結果削除を命じた仮処分決定に対する同社の保全異議申立てについて、検索結果すべてを削除対象とし、一部の違法な記載部分のみを削除するとしたヤフーの自主基準を否定。
- 経済産業省、改正個人情報保護法対応に向け、「匿名加工情報作成マニュアル」公表。
- 楽天、フィンテックやEC分野でのブロックチェーン技術に特化した研究機関「楽天ブロックチェーン・ラボ」を英国に開設。技術の応用可能性を研究。
- 日銀、フィンテック普及に向け専門家会議開催。フィンテック発展のカギとなる情報セキュリティ対策の重要性を強調。
- 軒先パーキング、不正アクセスにより利用者のクレジット情報や会員情報最大15万件流出。
- 熊谷署、マイナンバーカードを親族になりすまして詐取した容疑者を逮捕。マイナンバーカード詐欺では全国初。

＜JIPDECトピックス＞

- ISMSクラウドセキュリティ認証開始。
- 東京商工リサーチと連携し ROBINSによる企業情報の提供開始。

海外

- 香港ビットコイン取引所最大手Bitfinex、ハッキングにより顧客口座から約12万BTC(7,200万米ドル相当)盗難被害。取戻しのために懸賞金6,000BTC(3.6万米ドル)を設定。
- Apple、セキュリティバグ発見開発者に最大20万ドルの報奨金制度導入。
- 米国防総省高等研究計画局、世界初の自律的なソフトウェアのみのハッキング大会開催。優勝したカーネギーメロン大学が賞金200万ドル獲得。
- 台湾鴻海精密工業、出資金3,888億円でシャープの買収完了。
- 米Lookout、LinuxカーネルのTCP脆弱性の影響がAndroid約14億台に影響すると発表。
- 中国酒泉衛星発射センター、量子暗号技術構築のための実験衛星「墨子号」打上げ。
- 米司法省、POS端末にマルウェアを仕掛けてクレジットカード番号を詐取したロシア人に有罪評決。転売による不正利用で、金融機関3,700社の被害総額は1億6,900万ドルに。2014年拘束時にはPCに170万件以上のカード番号発見。
- 流出情報監視サイトLeakedSource、露インターネット企業Mail.Ruが運営するフォーラムから2,500万件超のアカウント情報の盗難被害を発表。
- Pokémon GO、全世界での配信開始1か月のダウンロード数約1.3億万回で、ギネス世界記録認定。
- Twitter、いじめやテロ行為助長アカウントを半年間で約23.5万件凍結。
- イスラエル軍、無人の完全自動運転軍用車の実戦配備を開始。
- EU、アイルランドがAppleの法人税率を低く設定していたとして、Appleに対する130億ユーロの追徴課税を要求。

2015年9月

国内

- LINEモバイル、MVNO(仮想移動体通信事業者)事業参入発表。月額500円(税抜)でトーク、無料通話が使い放題に。
- 電気通信事業者協会と携帯電話事業者、10月から迷惑メール情報の相互提供実施を発表。
- 政府、第4次産業革命など将来的に成長が見込まれる分野への投資拡大に向けた成長戦略と構造改革の加速化を図る「未来投資会議」第1回会合開催。
- 日経Automotiveと独ETAS、日本初、自動車をハッキングする技術を競う「自動車セキュリティハッカソン」開催。
- 警察庁調査、2016年度上半期のサイバー犯罪検挙数、相談件数ともに増加。逆にインターネットバンキングの不正送金被害額はウイルス感染機器の早期検知等対策により、9億円、前期比6.3億円減少。
- 京都大学大学院情報学研究所　梅野健教授、大容量データを高速に暗号化できる技術を開発。
- アドプリント、不正アクセスにより、顧客情報約15,000件流出の可能性。
- アカマイテクノロジーズ日本法人調査、全世界での2016年4～6月のDDos攻撃数が前年同期比129%増加。
- 富士通研究所、ディープラーニング学習に使うメモリの使用量を削減できる技術を開発。
- 宮城県警、不正入手によるID/パスワードで買い物サイトにアクセスした高校生2名を不正アクセス禁止法違反の疑いで書類送検。

＜JIPDECトピックス＞

- JIPDEC 全WebサイトへのEV証明書導入。

海外

- Mozilla、Appleら4社、個人情報にアクセスしたことを企業が顧客に知らせないよう命じたとして、米司法省に対し情報開示要請を行ったMicrosoftを支持し、訴訟当事者ではない第三者が提出する意見陳述書「アミカスクリエ意見書」を裁判所に提出。
- Google、Androidの脆弱性情報を募るハッキングコンテスト「Project Zero Prize」開始。2017年3月まで受け付け、優勝賞金は20万ドル。
- Microsoft、ネットワーク障害の影響により世界規模で「Azure」サービスの一部で障害発生。
- 米消費者製品安全委員会、Samsungの新型スマホ「Galaxy Note 7」のバッテリー過熱事故を受けリコール。対象約100万台。
- AP通信らメディア3社、2015年のカリフォルニア銃乱射事件捜査に係るiPhoneロック解除ツール提供業者との取引内容開示を求め、FBIを提訴。
- 米連邦地裁、ビットコインを通貨と判断。無認可取引所運営者が主張する「資金に当たらず」とする抗議を却下。
- 米運輸省、自動運転技術の安全性確保と技術革新に向け、自動運転車に関する連邦指針発表。
- IBM、マサチューセッツ工科大学とAIの中核的側面を担う「マシンビジョン」の共同科学研究で複数年提携を発表。
- Yahoo!、2014年に5億人分のユーザ情報流出被害があったと発表。
- 米情報サイトKrebs on Security、大規模なDDos攻撃の影響でWebサイトがダウン。攻撃の規模は最大級の665Gbps。
- Mozilla、中国最大手認証局WoSignの偽証明書発行問題で、FirefoxでWosignの証明書をブロック。10月の無効化を通告。
- Intel、BMWらドイツ大手自動車メーカ3社、モバイル技術関連企業による連合体「5G Automotive Association(5GAA)」結成。
- Amazon、Facebook、Google、IBM、Microsoft、AIの研究開発で提携、非営利組織「Partnership on AI」設立。

JIPDEC IT-Report 2016 Winter
2016年12月15日発行（通巻第8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12階
TEL：03-5860-7555　FAX：03-5573-0561
制　作　開成堂印刷株式会社