EY Advisory

EU一般データ保護規則（GDPR）適用後の日本企業の動向と課題

EYアドバイザリー・アンド・コンサルティング（株）　熊谷真知子

▸ Machiko Kumagai

公認情報システム監査人。EYに入所後15年超にわたり、金融機関、製造業、小売業、サービス業、公的機関等に対し、個人情報保護、情報セキュリティに関する管理体制構築支援、第三者評価業務を実施。近年は、GDPR対応をはじめとするプライバシー案件に対して、海外のEYメンバーと連携し業務を提供している。

Ⅰ　はじめに

2016年4月に欧州連合（EU）地域における新たな個人情報保護法制として採択されたGDPRは、18年5月25日に適用が開始されました。当初から、同規則が日本を含むEU域外国にも影響があること、日本の同種法制より規制が強化されていること、さらに違反時の制裁金が高額であること等から日本でも注目を集めており、多くの企業からその取り組みに苦慮しているという声が聞かれます。本稿では、こうした状況を踏まえ、GDPR適用後の日本企業における対応状況、最近の動向を紹介します。

Ⅱ　18年の5月時点では、多くの企業が対応継続中の様相

大手新聞社が適用開始直前に国内主要企業100社に対し実施した緊急アンケートでは、「対応の必要性があると答えた企業のうち、全て完了と回答した企業は2割にとどまる」との結果が公表されています。5月の適用開始前後には、日本企業の対応の遅れに関する調査レポートや、有識者からの指摘などが報道されていました。

Ⅲ　GDPR違反？適用開始直後から複数発生も

こうした日本の状況をよそに、GDPR違反を疑われる事例も発生しています。5月25日の適用開始当日には、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、GDPR違反を問う苦情申立てをEUのデータ保護機関へ提出しました。同団体は、GDPRにおいて規制が強化されている「個人データ収集時の本人からの同意取得」（第7条）に関して、前記4社が、個人データの取扱いに同意しなければオンラインサービスやアプリを利用できないようにしていることは同意の強制につながる（「自由意思」に基づかない）と主張しています。

同主張が認められた場合、オンラインサービス、アプリを通じてEUの個人データを取り扱う多くの企業に対し影響があると想定され、今後の同事案の行方が注目されます。

また、日本国内の企業が関係する事案としては、EU域内でホテル関連ビジネスを展開するA社（フランス）が運営するホテル予約サイトのサーバーが、18年6月に2回にわたり不正にアクセスされ、同予約サイトを利用する日本国内の企業（複数のホテル）の宿泊者データ（氏名、住所、クレジットカード等）、計12万件超が流出したという事案が発生しています。

この場合、一般的にホテル側は、日本企業であってもGDPR上の管理者（本人から個人データを収集する組織）、予約サイトを運営するA社はGDPR上の処理者（管理者に代わり、個人データの処理を行う組織）

▶表1　2018年5月以降に公表されたガイドライン

	説明	公表時期
①	“Guidelines 2/2018 on derogations of article49 under Regulation” ：第49条（データ移転規制の例外）に関するガイドライン	2018年5月25日（適用）
②	“Guidelines 1/2018 on Certification and identifying certification criteria in accordance with Article 42 and 43 of the regulation 2016/679” ：第42条（認証）、第43条（認証機関）に準拠する認証及び認証基準に関するガイドライン	2018年5月25日（ドラフト版の公表のみ）

と見なされ、管理者はEUの個人情報に関する取扱い業務を委託する場合は、第28条で定める「処理者」としての要求事項を遵守する企業を適切に選択することが求められます。

A社からのデータ漏えいが、適切なセキュリティ対策が講じられなかったことに起因する場合、第28条1項が定める「適切な技術的及び組織的対策を実施することを十分に保証する取扱者のみを利用しなければならない」ことへの対応が管理者であるホテル側で実施できていなかったと見なされ、GDPR違反として、最大で全世界売上高の2%もしくは1,000万ユーロの制裁金が科せられる可能性（第83条）があります。加えて、企業イメージの悪化、風評被害といったリスクにつながる恐れがあります。

Ⅳ　適用開始後のEU、日本政府の動き

1. GDPRガイドラインの公表状況

GDPRの特定の規制については、詳細解説に当たるガイドラインが順次公表されています。5月以降も、EU加盟国各国のデータ保護機関の代表等によって構成される欧州データ保護会議（European Data Protection Board：EDPB）より、ガイドラインの公表が進められています（<表1>参照）。

<表1>の①のガイドラインは、GDPR以前の法制から原則禁止とされていたEU域内から域外への個人データ移転規制に関し、第49条の具体的な解釈、データ移転が適法とされるケースの詳細が紹介されています。

また②のガイドラインは、第42条に規定されている認証制度について解説しています。同制度は、認証機関による第三者評価を受けることで、GDPR遵守状況を証明する仕組みとして推奨されており、同制度を活用することで、透明性が高く客観的にGDPR遵守をアピールできるとして、EU域内外を問わず、EUの顧客企業データを多数取り扱う企業から注目されています。

2. 日本とEU間の「十分性認定」の行方

「十分性認定」とは、データ移転規制の対応策の一つとして第45条に規定されており、欧州委員会が、データ移転先であるEU域外の国や地域における個人データ保護レベルが十分なレベルに達していると見なすことによる国家間の合意で形成されるものです。日本が同認定を受けることにより、EUから日本への個人データ移転は合法と見なされ、データ移転規制に対しては、対策（例：「SCC」の締結※）は不要となります。

18年7月、日本の個人情報保護監督機関である個人情報保護委員会より、EUから日本へのデータ移転に関して、18年の秋までに十分性認定に係る手続きの完了を目指す旨が公表され、同年9月には年内までに正式承認される見通しであることが欧州委員会より公表されました。同年8月には、日本が十分性認定を受けた場合にEU域内から日本に移転された個人データの取扱いに関するガイドライン「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」も公表されています。

Ⅴ　日本企業における適用開始後の取り組み状況と課題

5月の適用開始から数カ月が経過した現在では、日本企業においても影響調査がひととおり完了し、実務的な対応を検討する段階にシフトする企業が増え始めています。

※　EU域内のデータ移転元組織とEU域外のデータ移転先組織の間で、欧州委員会が公表する所定の様式（Standard Contractual Clauses：標準モデル契約条項）に基づき、EU個人データの適切な取扱いを合意する行為

1. GDPR対応を継続的な運用として定着させる準備

GDPR対応の一環として、今回初めて、個人情報の洗い出しやリスク評価を実施した企業では、継続的な運用につなげるための体制整備までは目が行き届かないケースも見受けられます。各取り組みに対する所管部署、責任者の決定、運用の評価をどのように実施するか等、継続運用を見据えた具体的手順の整備が必要です。

2. GDPR遵守のPDCAサイクルの検討

BtoBビジネスであっても、EU域内の取引先企業から、GDPRの遵守状況に関する調査、監査要請を受ける等の機会が5月以降急増しているとの声がよく聞かれます。運用開始後の遵守状況のモニタリングや第三者評価、前述の認証制度の活用等、GDPR対応後の運用維持のための施策を検討する必要があります。

3. EU域外の法規制への対応

EU域外、特にアジア地域でビジネス展開を行う企業では、シンガポールやマレーシアのデータ移転規制や、中国をはじめとして整備が進むデータローカライゼーション規制等に対し、ポストGDPRとして取り組みを始めています。実際に違反時の摘発が行われているケースもあり、グローバルにビジネスを展開する企業は、GDPR対応にとどまらず、他国の法規制にも目を向ける時期が来たと考えるべきでしょう。

Ⅵ　おわりに

GDPRは、EUにおける法規制でありながら、EUの個人データを取り扱う日本企業にも影響があります。違反時には高額な制裁金のリスクがあり、そのためEU企業や個人の関心も高く、日本企業といえども対応が不十分な場合は高額な制裁金のリスクに加え、EUとのビジネスに支障が生じる懸念があります。

個人情報保護の観点から規制強化を進めるGDPRは、プライバシーのグローバルスタンダードとして位置付けられており、こうした動きは、EUに限らず世界的なトレンドとして進行しています。今後のグローバルビジネスの推進において、プライバシーの観点では、まずGDPRの理解と遵守がポイントになってくるでしょう。

グローバル企業においては、GDPR及びその他ビジネス地域の法規制対応を見据えた中長期的な視点で、個人情報保護管理体制の構築や運用を考えることをお勧めします。

お問い合わせ先
EYアドバイザリー・アンド・コンサルティング（株）
E-mail：Machiko.Kumagai@jp.ey.com