GDPRの適用開始に向けた動向

EYロンドン事務所　公認情報システム監査人（CISA）　橋本聡子

▸ Satoko Hashimoto

2006年から11年まで当法人にて金融のIT監査業務に従事。11年にEYロンドン事務所に転籍。IT監査業務に加え、日系および現地の金融、商社、テレコム、製薬、石油など、さまざまな業種の企業にITリスクとコントロールの観点から内部統制をはじめとする数々のアドバイザリーサービスを提供。

Ⅰ　はじめに

2018年5月25日のEU一般データ保護規則（以下、GDPR）の企業への発効まで、およそあと1年となりました。16年5月の施行当時に比べ、私どもでもGDPRについての問い合わせを受けることが多くなり、対策を始めている企業がかなり増えてきたように感じます。割合としては、顧客を対象にビジネスを行っている企業が多いですが、BtoBのようなビジネス形態の企業でも、対策に取り掛かっています。

GDPRでは、欧州連合（EU）に拠点のある企業はもとより、EUに拠点を持たない企業でも、EU市民の個人データを扱う企業は対象となります。EUに子会社を持っているか否かにかかわらず、例えば日本本社でEU市民のデータを直接扱っている場合、日本本社側での対応も必要になってきます。

Ⅱ　最近の動向

1. Brexitの手続き開始

先日EU基本条約第50条が発動され、英国のEU離脱（Brexit）の手続きが開始されました。BrexitのGDPRへの影響については、英国に拠点を置く企業の懸念事項の一つかと思いますが、次の理由から影響は少ないと考えられています。

- 離脱は19年3月の予定であり、GDPRには離脱前の18年5月25日までに対応する必要がある。
- 離脱後もGDPRと同じような法律が英国に制定されることは英国政府からすでに発表されている。

よって、英国居住者のデータを扱う企業は、Brexitに関係なくGDPRを遵守することが求められます。

2. ガイドラインの公布

現在までのところ、第29条作業部会により次のトピックについてガイドラインが出されています。

- データポータビリティ
- リード監督機関
- データ保護責任者（DPO）

また、以下のトピックについても、17年度中にガイドラインが出されることが公表されています。

- 同意
- 透明性
- プロファイリング
- ハイリスクなデータ処理
- 認定（Certification）
- 罰金
- データ漏洩（ろうえい）の際の報告
- データの移転

同意については、英国の監督機関である情報コミッショナーオフィス（ICO）がガイダンスの草案を近頃発表しましたが、これらのガイダンスが出されることでGDPRの要求事項が明確になり、企業は対策を講じやすくなると期待されています。

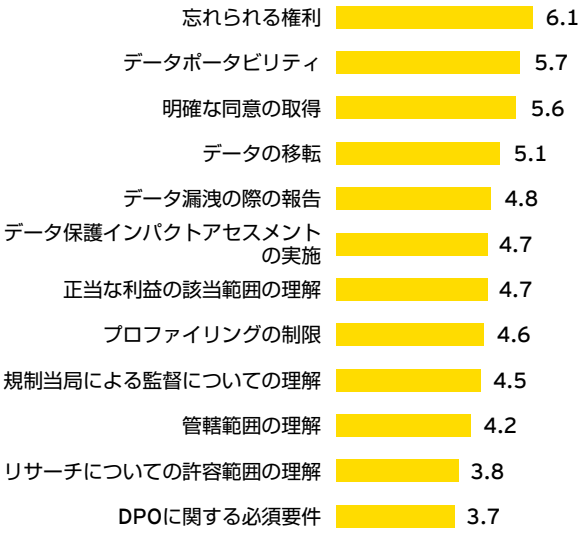
Ⅲ　GDPRへの対応

1. 企業の反応

EYと国際プライバシープロフェッショナル協会（IAPP）が各企業のプライバシー専門家を対象に共同で実施したサーベイの結果、GDPRの要求事項で企業にとって対応が最も難しいと考えられているのは、1位から3位の順に、忘れられる権利※1への対応、データポータビリティ※2への対応、明確な同意の取得※3となっています（＜図1＞参照）。

忘れられる権利への対応として、まず、バックアップも含め、個人データがどこにどのように保持されているのか把握し、要求があった場合に適宜データの削除ができる状態にしておくことが重要となります。

▶図1　対応が難しいGDPRの要件（サーベイ結果*）



＊　GDPRにおける法的義務への対応の難しさについての評価（0：全く難しくない、10：非常に難しい）を集計

出典：https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2016/

2. データの移転

＜図1＞の4位に上げられているデータの移転に関しては、日系企業の最も大きな懸念事項の一つかと思います。GDPRでは業務の形態にかかわらず、欧州経済地域（EEA）外に個人データを移転することは以下の例外事項を除き、原則として禁止されています。これには、例えばEUに拠点を置く子会社から日本本社へ従業員に関わる個人データを送る行為も含まれます。

- ▶ 十分な保護対策を講じている国への移転（日本はこれに含まれていない）
- ▶ データ主体者の明確な同意がある場合
- ▶ 法的要求のために必要な場合（訴えの提起など）
- ▶ 公共の利益のために必要な場合
- ▶ 生命に関わる場合
- ▶ 契約の履行に必要な場合
- ▶ 標準契約条項（SCC）を締結している場合または拘束的企業準則（BCR）を策定している場合

GDPRではデータの処理と移転に関し、前記のような法的根拠を確立することが必要になりますが、それには「同意」以外の方法を用いた方がよいとされています。これは、例えば企業が社員の個人データを処理・移転する際に用いられる「同意」が、本当に本人の自由意志で得られたものかを判断するのが難しいためです。

Ⅳ　おわりに

企業が対策を始める場合、ギャップアナリシスやマチュリティーアセスメントなど、現状分析から行っているところが多く見られます。現状分析の結果を元にGDPRの要求事項とのギャップを割り出し、対策を講じていくやり方が効率的かと思います。18年5月までに対応を済ませて運用を開始できるよう、早めに準備をスタートさせることをお勧めします。

お問い合わせ先
EYロンドン事務所
UK&Iサイバーセキュリティー、プライバシーアンドレジリエンス
E-mail：Shashimoto@uk.ey.com

※1　個人データの保有の必要性がなくなったなどの事由がある場合、データ主体者は情報管理者に対し、本人に関する情報の遅滞なき削除を要求することができる権利
※2　本人が事業者など、ある主体に個人データを提供した場合、その主体が有するその個人についての情報を、他の主体に移転することを要求できる権利
※3　データの処理・移転に関し、目的を特定し明確な説明の下、データの主体者である本人の自由意志で同意を得ることが求められる。また、同意を取得したことの証拠となる記録を残す必要があり、同意を要求する文言は分かりやすいものにしなければならない。