GDPRは、日本企業にも影響大！

個人データ保護を強化するEU。多額の制裁金も

EU（欧州連合）における個人情報保護の新たな枠組みが、2018年5月25日より始まります。「EU一般データ保護規則（GDPR）」です。海外の法律ではあるものの、ヨーロッパでビジネスを展開している日本企業にも大きく影響してきます。

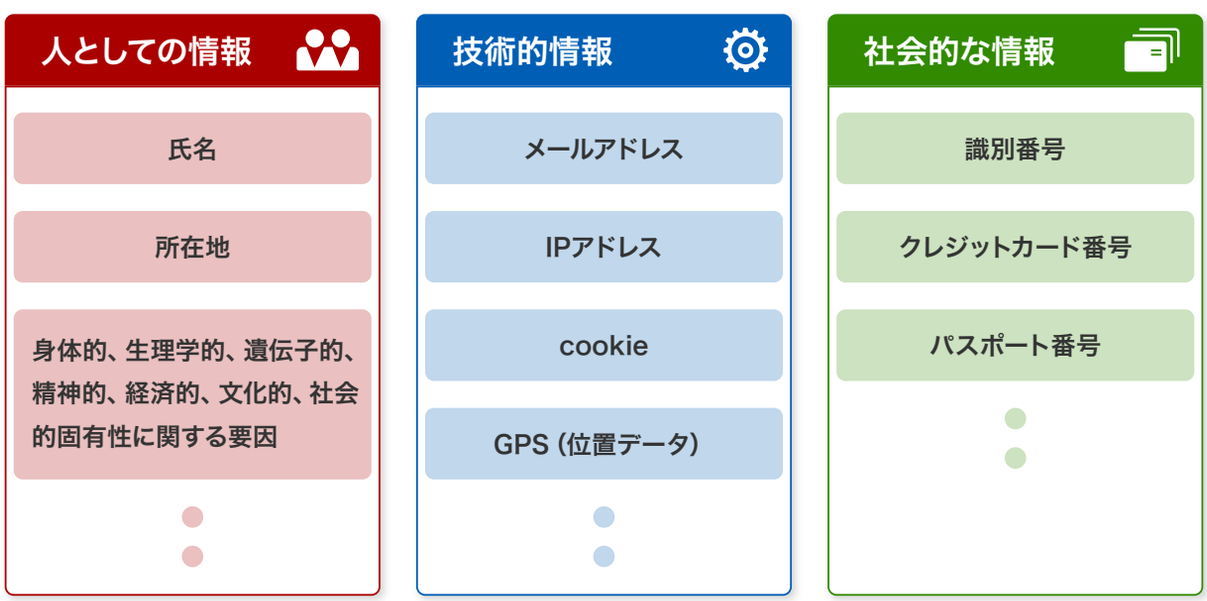
EUが個人データの保護を強化する枠組み「GDPR」を開始

人間の権利は誰にとっても重要なものですが、その考え方は、国や地域、そして個人によって違いがあります。特にヨーロッパは、先駆けて人間の権利に取り組んできた歴史を持っています。

そのEUにおいて、個人情報保護の新たな取り組みが始まります。「EU一般データ保護規則（GDPR）」です。これは個人データの「処理」と「移転」に関するルールを定めた規則で、EUに所在するすべての個人が自分の「個人データ」をコントロールする権利を、基本的人権として保障することを主目的としています。これまでも個人情報保護に関するルールはあったものの、EU内の国によって違いがありました。GDPRは、それを統一しようという動きでもあります。

GDPRでは「個人データ」を、「識別された、または識別され得る自然人に関するすべての情報」と定義しています。なお、「識別された、または識別され得る自然人」は「データ主体」と呼ばれます。個人データに含まれるものを具体的に挙げると、氏名や所在地、識別番号、メールアドレス、IPアドレスやCookie、GPSなどの技術的な情報、クレジットカード情報、パスポート情報などのほか、身体的、生理学的、遺伝子的、精神的、経済的、文化的、社会的固有性に関して「識別され得る情報」も含まれます。

図1：GDPRにおける個人データの例



これらのなかには、Cookieのように、単体のデータでは個人を識別できないものもあります。しかしほかのデータと組み合わせることで個人を識別できると考えられる場合は、そのデータも個人データと見なされるのがポイントです。

GDPRは、日本企業にも影響大！

個人データに国籍は関係なし！ 漏えいすれば72時間以内に報告義務

EUにおける個人データの厳格な取り扱いを定めたGDPRを、「あくまでもEU域内のルールであって、日本企業には関係ない」と考えてしまうのは早計です。日本企業もGDPRの影響を受ける可能性は十分にあります。

GDPRが保護対象としている個人データは、EU加盟国にアイスランド、リヒテンシュタイン、ノルウェーを加えた「欧州経済地域」（EEA）に所在する個人のデータです。ここで着目したいのは「所在する」という部分で、個人の国籍は関係なく、EU内に所在することが重要です。

そして万が一、個人データの情報漏えいが発生した場合は、監督機関に対し72時間以内に報告する義務があるほか、大量のデータを継続的に取り扱う企業などは、データ保護責任者を任命する必要があるとしています。

日本企業がGDPRの影響を受けるケースは？

では具体的には、どのような日本企業が規則の対象となるでしょうか。まず挙げられるのは、子会社や支店、営業所などの拠点がEEA域内にある企業です。そこでは、EUに所在する従業員の個人データを扱うことになるからです。あわせて、日本本社から現地に駐在している、現地子会社に出向している日本人従業員の個人データも保護対象です。

また、日本からEEAに商品やサービスを提供している企業であれば、EEA域内に子会社や営業所がなかったとしても対象となります。そしてEEAから個人データの処理を委託されている企業も含まれます。これにはデータセンターやクラウド事業者などが、当てはまる可能性が高いとされています。

例えば、フランス人が自国から、日本の化粧品ブランドのECサイトで商品を購入した場合、サイトに入力した個人データはGDPRの保護対象となります。逆にフランス人が日本に旅行に来て、土産物店でクレジットカードを使ったとき、入力したカード情報はGDPRの適用外となります。

日本企業がEEA域内での国際見本市に出展したり、自社製品の展示会を開催して、そこで収集した来場者の情報を国内へ持ち帰ることもデータの「移転」に該当する可能性が高いとされています。EEA域内の子会社（支店も含む）が収集した顧客のメールアドレスをリスト化して、日本の親会社へ送信するのも同様です。このような顧客リストに、日本の親会社からアクセスする行為も「移転」と見なされます。

さらには、海外からの旅行予約やホテル宿泊予約などを受け付けているサイトの運営事業社、旅行会社、ホテル事業者、レンタカー事業者なども対象となる可能性が高いとされています。外国人観光客向けの事業者も、日本国内での予約ではなく、EEA域内の自国から日本に直接、インターネットで予約が入った場合は、その個人データは保護対象となります。

「約27億円」という多大な制裁金、企業によっては倒産の危機も

このようにGDPR施行によって、EEA域内に拠点を持たない日本企業でも大きな影響を受けることが想定されます。そのインパクトをさらに大きなものにしているのが、違反した際に科せられる多額の制裁金です。

GDPRは、日本企業にも影響大！

制裁金の上限額には、前年度の全世界における売上高の4%、または2000万ユーロ（1ユーロ＝約133円計算で約27億円）のいずれか高いほう、前年度の全世界における売上高の2%、または1000万ユーロ（同、約14億円）のいずれか高いほうと2種類があり、どちらが適用されるかは違反内容で決まります。「全世界の売上高」というのもポイントで、GDPRに違反した会社は全世界のグループ会社全体に制裁が科されます。

例えば全世界年間売上高が500億円の企業では、売上高の4%は20億円ですが、2000万ユーロ（約27億円）のほうが高いので、制裁金の上限は2000万ユーロとなります。

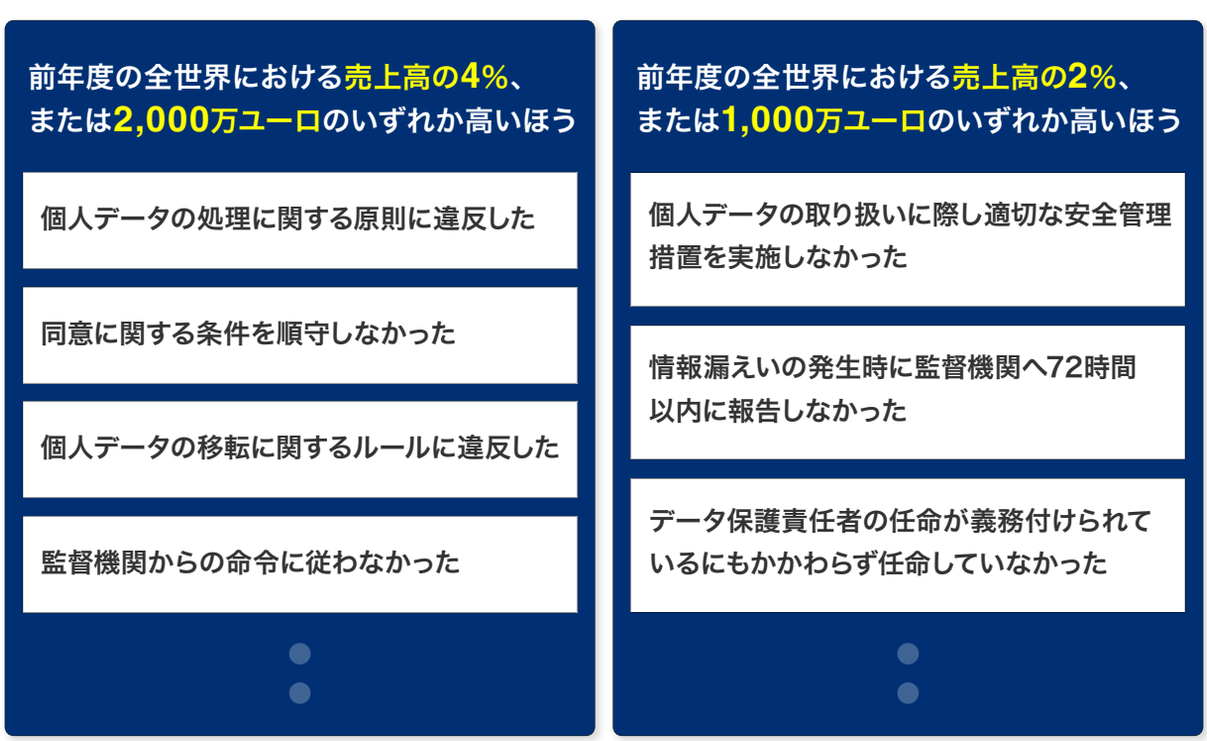
この約27億円という制裁金のインパクトを考えてみます。中小企業庁によると2010年以降、国内の中堅・中小企業の売上高経常利益率は平均約2.5%で推移しています。仮に年商500億円の企業なら経常利益は約12億5000万円です。そこに約27億円の制裁金が科せられれば、倒産しかねません。

同様に中小企業庁によると大企業の経常利益率は2010年以降、平均で約4.5%です。年商5000億円の企業であれば、経常利益は225億円です。約27億円の制裁金で、経常利益は10%以上のマイナスとなってしまいます。もちろん、違反による影響は制裁金だけではありません。企業ブランドと評判の失墜も考えられます。

GDPR施行目前、対応へ向けて日本企業は何をすべきか

違反例を挙げると、売上高の4%、または2000万ユーロが適用されるのは、「個人データの処理に関する原則に違反した」「監督機関からの命令に従わなかった」などのケースです。売上高の2%、または1000万ユーロが適用されるのは、「情報漏えいの発生時に監督機関へ72時間以内に報告しなかった」「データ保護責任者の任命が義務付けられているにもかかわらず任命していなかった」などのケースです。

図2：2種類の制裁金と違反ケース



GDPRは、日本企業にも影響大！

では、GDPRに適切に対応し、違反と見なされないためには何を実行すべきでしょうか。まずデータの「移転」に関しては、上述したとおりデータの物理的な移転だけでなく、EU内の個人データへ日本からアクセスできるケースも含まれるので、日本国内でも注意が必要です。

GDPRで個人データの移転が許されているのは、十分にデータ保護を実施していると認められる国や地域のみに限定されています。日本には個人情報保護法があり、個人情報保護は強化されていますが、残念ながら現時点ではGDPRにおいて「十分なデータ保護を実施している国」とは認められていません。

そのため日本へ個人データを移転するには、「拘束的企業準則（BCR）」を整備するか、もしくは「標準契約条項（SCC）」を締結する方法が一般的です。BCRは、自社グループ内の企業間で個人データを移転する際のルールです。これを運用することで、グループ内での個人データ移転は自由に行えます。ただしグループ外の企業とのデータ移転は行えません。

一方のSCCは、個人データの移転元と移転先の企業間において締結するデータ保護に関する取り決めです。これを結べば、グループ外へのデータ移転も行えますが、移転の目的と対象の個人データを契約書に明記する必要があるため、追加や変更のたびに見直しが求められます。

また2018年2月には、個人情報保護委員会が「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ガイドラインの方向性について」を公表しました（※）。ここでは、「要配慮個人情報の範囲」「保有個人データの範囲」「利用目的の特定」「日本から外国への個人データの再移転」「匿名加工情報」の5項目について、日本の現行法令とGDPRの異なる点を明示しています。今後、この方向性を踏まえてガイドラインが策定されれば、日本企業がEU内から個人データの移転を受けるために、このガイドラインに沿った対応が必要になると推測されます。

次のポイントとして注意したいのは、データ取得時の同意です。取得と利用目的について、データ主体から有効な同意が明確に示される必要があります。つまり、Webサイトなどにプライバシーポリシーや利用規約を掲載し、「同意」を意味するチェックボックスにあらかじめチェックが入った状態で、ユーザーによる操作を必要とせずに次へ進めるような仕組みを用意して、「暗黙の同意を得た」という運用では、「有効な同意」とは認められないことになります。また、一度得た同意をデータ主体がいつでも取り消すことができる仕組みも要件として必要です。

このようなポイントを踏まえた上で、企業の各拠点においてどのような個人データを保有し、どのように扱っているか調査、把握し、データ保護の責任者や役割分担を明確にして、GDPR対応計画を構築、運用することが対策として求められます。

EU域内でビジネスを展開している日本企業は少なくありません。企業のグローバル化が進むなか、GDPRが定める規則を順守することはもちろんですが、個人データの保護というGDPR本来の目的を理解し、日本企業全体で個人データ保護の文化を浸透させることが重要といえるでしょう。

※個人情報保護委員会：「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ガイドラインの方向性について」
https://www.ppc.go.jp/files/pdf/300209_siryou1.pdf（2018 年 4 月現在）

【 制作／コンテンツブレイン 】

NTT コムウェア株式会社
URL：http://www.nttcom.co.jp/
WEB 掲載：2018.4