日経産業新聞
NIKKEI BUSINESS DAILY FORUM
フォーラム

「個人情報保護対応におけるリスクマネジメント戦略」
～GDPRおよびPIAによるプライバシー保護の最新動向を踏まえて～

個人情報保護規制強化が世界的な潮流となっている。昨年5月に改正個人情報保護法が日本で施行され、欧州連合（EU）では今年5月に「一般データ保護規則（GDPR）」が導入される。先般行われた日経産業新聞フォーラムでは「個人情報保護対応におけるリスクマネジメント戦略」と題して、GDPRへの対応などの最新情報が提供された。

合法の手段策定へ対応急がれる

基調講演
越境データ移転におけるリスクマネジメントのあり方 ～改正個人情報保護法とGDPRへの対応を中心に～

慶應義塾大学　総合政策学部　教授
新保　史生氏

昨年5月、改正個人情報保護法が全面施行された。改正には5つの狙いがある。1つ目は「個人情報の定義の明確化」、2つ目は「適切な規律の下での個人情報等の有用性確保」、3つ目は「個人情報の保護の強化」である。

4つ目は「個人情報保護委員会の設置」であり、今回の改正の大きなポイントだ。従来、個人情報保護に関するガイドラインは、事業分野ごとに担当省庁が定めてきた。改正後は同委員会のガイドラインへと一元化され、わかりやすく、使い勝手が増した。安定的で統一的な法の執行が今後期待される。

5つ目は「グローバル化への対応」だ。具体的には、国境を越えた個人情報の取り扱いに対する適用範囲に関する規定〈75条〉、外国執行当局への情報提供に関する規定の整備〈78条〉、個人データの外国にある第三者への提供の制限〈24条〉が新設されている。

企業活動に大きく関わるのは24条で、同条では日本で得た個人データを外国の第三者に提供する場合、本人の同意を取るよう求めている。ただし、わが国と同水準の個人情報保護制度を持つ国、あるいは同水準のセキュリティーレベルを持つ第三者への提供などは、同意なしに行える。クラウドの利用など、グローバルでの個人情報のやり取りは、こうした規定を十分に理解し、合法かつコストを抑えて行いたい。

一方、EUで取得した個人情報を日本国内に移転し、利用する企業はさらに大きな注意を払う必要がある。今年5月にGDPRがEUで導入されるからだ。GDPRは個人情報の利用や移転に関するルールで、違反した場合、多額の制裁金が科せられる。EU圏でサービスを展開するなら、日本企業も例外ではなく、その対応が急がれる。

例えば、EUから域外の国へ個人情報を持ち出すには、その国がEUの「十分性認定」を得ていなければならない。認定にはEUと同基準の個人情報保護の法制度を当該国が持つことが条件だが、日本は未承認だ。よって日本へ個人情報を移転するには、企業が個別に認定を受ける必要がある。それが「標準契約条項（SCC）」の締結、あるいは「拘束的企業準則（BCR）」の策定である。今後「行動規範」「認証」という方法も追加されるが、いずれも煩雑な手続きとコストがかかる。日本が国として早急に十分性認定を受けることが望ましい。

国の内外で保護規制に差

セッション1
GDPRから読み解く日本企業のプライバシー・リスクマネジメント

EYアドバイザリー・アンド・コンサルティング
パートナー　公認会計士

梅澤　泉氏

企業は様々なリスクに常にさらされている。その1つが個人データの紛失、毀損、改ざん、漏洩などのプライバシーリスクである。

これらは日本の個人情報保護法でも扱われるが、EUの新たな枠組みであるGDPRには、さらに「個人の権利への不適切な対応」というリスクが含まれる。例えば「同意を得ない個人データの取得、移転」や「個人データに関する同意撤回の仕組みの不十分さ」などがこれに当たる。またGDPRを知るには、プロファイリング規制や消去権といった概念の理解も不可欠だ。

プロファイリングとは、オンラインショッピングやGPS（全地球測位システム）などの履歴から、個人の置かれた環境や趣味、嗜好、健康状態などを推測し、より効果的な広告などを表示する手法だ。GDPRではこれに規制がかかる。

一方、消去権は「忘れられる権利」とも呼ばれるもので、ウェブサイト上に載せられた過去の情報の削除を請求する権利である。

こうした「個人の権利への不適切な対応」は、日本の個人情報保護法には規定がなく、EU圏でビジネスを展開する日本企業は、これらを十分に認識し、対応を取る必要がある。

GDPRへの適応には、特定、分析、評価、対応の4つのプロセスで臨みたい。特定では、データマッピングによる現状把握とリスクの洗い出し。分析では、リスクの特質の理解と、そのレベルの決定。評価では、取り組みの優先準位の決定。そして対応では、リスクの排除、軽減、予防の実行に取り組む。

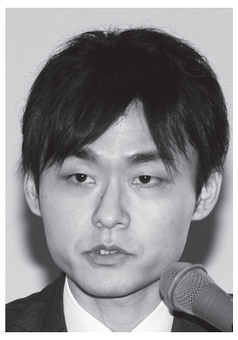
具体的な検討課題は、方針、戦略、実務の3つの階層で考える。方針では「EU域外拠点でのGDPRの影響の試算」「日本本社のカバーすべき範囲の明確化」など。戦略では「どのようなDPOを選任するか」など。実務では「漏洩通知に向けた体制の構築」などがポイントだ。

経営陣がこれらをまず明確に定めれば、現場の実務もスムーズに進むはずだ。

方針、戦略、実務からの検討要

セッション2
GDPRリーガルリスク軽減のためのコンプライアンス体制構築の実務

岩田合同法律事務所　弁護士



佐藤　喬城氏

松田　章良氏

岩田合同法律事務所　弁護士

佐藤氏　いまGDPRが着目されている主な理由は「多額の制裁金規定」と「域外適用範囲の拡大」の2つである。データ保護規制に違反しているかどうかの判断は比較的客観的に可能であると思われ、積極的な制裁の発動も予想される。

そこでまず必要なことは適切なコンプライアンス体制の構築だ。有事に至るリスクの低減かつ制裁金の減免につながる。その大前提として、自社がGDPRの適用を受けるか否かを判定する必要がある。そのために不可欠な実務上の作業として、自社グループにおける個人データの取り扱いの現状を、データマッピングを行って確認することが重要になる。

◇◇◇

松田氏　自社がGDPRの適用対象と確認できた段階で必要なことは、データの処理や移転の規制を順守するための体制づくりである。

処理規制で重要なことは説明責任が義務化されている点。データ保護方針の策定は必須となる。同意の取得はもちろん、侵害の認識から72時間以内の監督当局への通知・報告義務、データ保護責任者の専任義務などへの注意も必要だ。

一方、移転規制への対応には標準データ保護条項あるいは拘束的企業準則が原則になる。EU域内で取得され、日本に移転されたデータはGDPRが要求する措置の対象となるので、日本の個人情報保護法と合わせた対応が欠かせない。

自社データ活用の把握を　佐藤氏
規制順守のための体制づくり　松田氏

セッション3
コンプライアンス対策に迫るデジタル変革の波 ～テクノロジーの欠如はGDPR対応の妨げ

ベリタステクノロジーズ
コンサルティング・マネージャー

若山　光太郎氏

いま企業が保有するデータは爆発的に増大している。近年の特徴は、それらの大半がメールやチャット、画像、動画のような非構造化データとなっていることだ。これらは、アプリケーションによって生成される構造化データと異なり、秩序立てて整理することが非常に難しい。従って、その中にある個人情報を適切に管理するには、テクノロジーを活用しなければならない。非構造化データの分類、分析を行えるテクノロジーによって、データを整理し、それぞれの置き場所を決め、主体的に管理し、記録する。それがGDPR対策につながる。

当社では、GDPRだけでなく、コンプライアンス全般への対策として、まず情報ガバナンスの整備を提唱する。情報の生成から活用、蓄積、廃棄までのプロセスにおいて、統合的なフレームワークモデルに基づいて、情報システムのソリューションを活用していくのだ。

当社のデータ管理ソリューションは、個人情報を含むデータのガバナンスを徹底させるため、情報のライフサイクルに則したモデルに当てはめて考えられている。そこに戦略、組織、技術、データ漏洩と保護、ポリシーとプロセスの5つの分野で対策を行うアドバイザリーサービスを加えることで、対策を完結させる。

これから情報ガバナンスの体制を整理していくには、まず現状を把握し、課題や取り組むべきリスクを示してロードマップを策定していく。例えば、現状のリスクを把握するには、ウェブ上で公開されている「リスクアナライザー」試用版で体験可能だ。どこに個人情報が含まれているか、そこにどれだけのリスクがあるか、検索して、分析リポートを生成してくれる。

半日から1日のアドバイザリーワークショップで、GDPRや情報ガバナンスに関する説明や事例のディスカッションを行うプログラムも用意している。企業の情報ガバナンス能力を強化するために、テクノロジーをぜひ活用してほしい。

リスクを分析し対策を提案

クロージング特別講演
ITを活用したGDPR対策／セキュリティ投資状況について

アイ・ティ・アール　シニア・アナリスト
大杉　豊氏

企業の情報セキュリティー対策費用は年々増加している一方で、国内企業のGDPR対策や改正個人情報法体制のIT（情報技術）システム対応は十分には進んでいない状況にある。

日本情報経済社会推進協会（JIPDEC）と共同で調査した「企業IT利活用動向調査2017」では、「重視する経営課題」の質問で経営が好調・不調の企業で違いが見られた。業務プロセスの効率化や情報セキュリティーの強化など上位項目に大きな差異はないが、それ以外では経営が不調な企業では「社内体制・組織の再構築」「システム更新への対応」「システムダウンへの対応」と内向きの課題が挙がっている。好調企業では「法令への対応」「企業間の情報連携」「マイナンバー対応」「ビッグデータ活用」を重視している。

現在の企業経営には、信頼、安全、セキュリティーが求められる。プライバシー・バイ・デザインを考慮するだけでなく、一歩進めてセキュリティー・バイ・デザインの考えを取り入れることを勧めたい。ビジネスの創世記からセキュリティーを考慮して、デザインしていく。AI（人工知能）やIoT、クラウドへのビジネス対応といった技術的変化、セキュリティーコントロールなどの環境変化、法令・ガバナンス的変化に早期に対応するためだ。クラウドや仮想化、オープン化といったサイバー空間の活用が広がり、データ駆動型ビジネスへと移行している。こうした変化に対応していかなければならない。

GDPR対策では、データ保護責任者（DPO）の設置の必要性が指摘される。同時にデジタルオーナーの役割も重要だ。法令・ガバナンスの順守が求められる社会で、デジタルオーナーが中心となって個人情報、デジタルデータのライフサイクルを管理する。

当社で毎年行っているIT投資動向調査では、17年には半数以上の企業が海外進出を考えていると回答した。しかし海外進出にあたって、グローバルIT予算を把握しているのは約6割で、4割は把握していない状況だ。EUのプライバシー規制への対応も、「規制にのっとったかたちで適正に個人情報の転移を行っている」とした企業はわずか18・5%にとどまる。具体的な対応策では、「多国籍企業向けのルール、BCRを適用している」企業は11・4%に過ぎない。国境を越えたデータ移転について、モニタリングを確実に行われなければならない。

変化に見合ったＩＴ投資を

広告
企画・制作＝
日本経済新聞社クロスメディア営業局

EY Building a better working world

岩田合同法律事務所
IWATA GODO
Established 1902

VERITAS
The truth in information.