KPMG

KPMG Insight

KPMG Newsletter

Vol.29

March 2018

【特集③】

施行直前！
GDPR対応プロジェクト最終チェック

kpmg.com/jp

施行直前！ GDPR対応プロジェクト最終チェック

KPMG コンサルティング株式会社
サイバーセキュリティアドバイザリー
ディレクター　大洞　健治郎
ディレクター　万仲　隆之

大洞　健治郎
おおぼら　けんじろう

万仲　隆之
まんちゅう　たかゆき

2018年5月に、欧州連合（以下「EU」という）で「一般データ保護規則（General Data Protection Regulation：以下「GDPR」という」が施行されます。GDPRはEUに所在する人の個人情報データを保護するための法令要件です。これは、たとえEUに拠点がなくても、EU域内の顧客や取引先、協力会社などを有する企業は適用対象になり得ることを意味しています。つまり、GDPR対応は、EU域内の子会社のみならず、グループ企業全体として取り組むべきプロジェクトです。

施行まであと2ヵ月。皆さんの会社でも、GDPR対応は進んでいることでしょう。

本稿では、最終確認として、KPMGが考えるGDPR対応において最低限対策が必要となる16の項目を確認するためのチェックリストを紹介し、またGDPRの法令要件を満たすためにどのような管理体制を整備し、どのような対応が必要となるのかについて解説します。

なお、本文中の意見に関する部分については、筆者の私見であることをあらかじめお断りいたします。

図表1　GDPR対応における主な実施事項

① ガバナンス態勢構築	● 個人データ管理体制の構築 ● データ保護オフィサー／代理人の設置 ● プライバシーリスク影響評価の実施 ● データ保護方針の策定 ● 国際データ移転における保護措置の実施
①-1 インシデント対応	● 当局への72時間以内報告 ● データ主体への連絡・説明 ● 個人データ侵害の記録
①-2 取引先管理	● 適切な委託先の選定 ● 委託先／共同管理先との契約締結
② プロセス整備	● 適切な同意取得 ● 取扱いの記録・保管 ● データ主体の権利への対応 ● 個人データ取扱原則の遵守
③ システム対応	● リスクに応じた技術的安全管理措置

point 1

GDPR対応要件の確認

5月施行のGDPR対応に最低限必要となる16項目について、簡易診断チェックリストで確認してみましょう。

point 2

GDPR対応は本社主導で

GDPR対応プロジェクトは、本社がリードし、組織横断的にしっかりと対応することが肝要です。

I. 5月施行のGDPR。企業は何をしなければならないのか？

1. GDPRはEUの個人情報保護法

GDPRは、EUの個人情報保護法です。つまり、EUに住む人の個人情報を取得する場合に、本人へ伝達すべき事項や同意条件、データの管理方法などを定めた法令要件のことです。この法令が、2018年5月に施行されます。

この法令要件の対象となる企業は、データ保護責任者（Data Protection Officer、以下「DPO」という）を設置したり、社内ルールを作成したりするなどの対応を行う必要があります。また、GDPR対応はEUに子会社や支店がなくても必要になることもあります。たとえば、インターネットでEUの消費者に商品を販売しているようなケースでも、EUに所在する消費者の個人情報を集めることになり、GDPRの対象となります。

2. GDPR対応プロジェクトは3つの領域に分かれる

GDPR対応は、大きく次の3つの領域での対応が必要となります（**図表1**参照）。

（1）ガバナンス態勢の構築

「個人データ管理体制の構築」「DPOの設置」「インシデント対応体制の構築」「取引先管理体制の構築」などが含まれます。

（2）プロセス整備

「本人同意取得プロセスの見直し」「取扱い記録・保管」など、個々のデータを取り扱うプロセスに関連するものです。

（3）システム対応

ITセキュリティと、ITサービスを使うなかで生じる意図しない国際間データ移転リスクへの対応などが該当します。

各領域での対応は多岐にわたります。施行まで残り2ヵ月。皆さんの会社でも、GDPR対応プロジェクトはかなり進行していることでしょう。プロジェクトに不備や漏れがないか、プロジェクト運営上で問題がないかを、KPMGの簡易診断チェックリストで確認することをお奨めします（**図表2**参照）。

チェックリストに挙げた16項目は、KPMGが最低限GDPR対応プロジェクトでカバーされるべきと考える事項です。施行までの時間の制約から、まずは規程の整備のみを目標としている企業もあることでしょう。しかし、実際に守るべきものが守れない状態では意味がありません。施行日以降での実現になるとしても、チェックリストの各要件が実質的に充足される管理体制を構築すべきです。

図表2　GDPR対応プロジェクト簡易診断チェックリスト

	診断項目
	Ⅰ. GDPR対応プロジェクトの運営状況
1	貴社のグループ内で収集、処理、保存されているEU在住者の個人データ を網羅的に把握できていますか。
2	GDPR対応プロジェクトの責任部署の役割が定められ、IT部門等の関連部署との協力体制や経営陣への報告体制が整備されていますか。
3	2018年5月のGDPRの施行に向けて、課題・タスク・対応部署が網羅的に洗い出され、課題等に対応するためのスケジュールが設定されていますか。
	Ⅱ. 管理組織と業務プロセスの整備状況
4	EU在住者の個人データを取得する際の同意取得に係るルール・手順を定め、確実に実施していますか。
5	EU在住者本人から様々な要求があった場合に、適切に対応できる体制とルール・手順を整備していますか。
6	貴社におけるEU在住者の個人データの取扱いについて、その記録を作成・保存し、必要に応じて監督機関へ提示できる状態としていますか。
7	データ保護責任者（DPO：Data Protection Officer）の設置要否を判定し、設置する場合にその役割・責任を定めていますか。
8	EU在住者の個人データを新たに取り扱う場合のデータ保護影響評価（DPIA：Data Protection Impact Assessment）を実施するルール・手順 を定めていますか。
9	EU在住者の個人データを複数事業者で共同管理する場合、その責任分担等を契約の締結により取り決めていますか。
	Ⅲ. 安全管理対策の導入状況
10	取り扱う個人データのリスクレベルに応じて、暗号化や仮名化、物理的安全管理措置、データ侵害を阻止するためのシステムセキュリティ対策、障害発生時の復旧対策などを講じていますか。
11	EU在住者の個人データの取扱いを外部に委託する際の方針やルール等を定め、方針等に則った契約を締結していますか。
12	EU在住者の個人データ漏洩などの事故が発生した場合、事故を認識してから72時間以内に監督当局へ報告できるよう、報告基準、報告者等のレポートライン等の具体的な報告手順を定めていますか。
	Ⅳ. 個人データ国際間移転に係る対応状況
13	EU在住者の個人データをEU域外へ移転する場合のルール・手順を定め、運用を開始していますか。
14	グローバルで利用されるITシステムにおいて、意図せずにEU在住者の個人データが国際間移転してしまうリスクの評価とその対策は十分に行われていますか。
	Ⅴ. ルールの浸透・点検活動の状況
15	上記設問のような個人データの取扱いルールを社内規程等として文書化し、従業員に周知・教育していますか。
16	貴社グループ内におけるEU在住者の個人データの取扱いについて、GDPRの要件を遵守していることが証明できるよう、定期的に適切な点検・監査を実施する計画を定めていますか。

詳細はウェブページをご参照ください。
GDPR（EU 一般データ保護規則）対応プロジェクト簡易診断
https://home.kpmg.com/jp/ja/home/insights/2018/01/gdpr-checklist.html

3. なぜ、GDPR対応プロジェクトが進まないのか？

企業におけるGDPR対応プロジェクトでよく目にするのが、プロジェクトチームは発足し、現状調査までは行っているのに、そこから先へ進まない、というケースです。この問題の原因として、管理体制のゴールイメージが明確になっていない、ということが挙げられます。どのようなプロジェクトでもそうですが、具体的な目標がなければ作業は進みません。

ゴールイメージとは、たとえば「社内の個人情報取扱い規程を作る」「事故が起こった場合のインシデント対応の手順書を作る」「DPOの職務規定を作る」などが挙げられます。このようにゴールを定義すると、計画が立てやすくなります。

ゴールを明確に定義することで、たとえば「何月の経営会議で、その文書の正式承認を得る」「そのためには付議資料をいつまでに用意する」「資料の内容を固めるために関係部署との打ち合わせをセットする」というように、逆算でプロジェクト計画を立てることが可能になります。

4. 2ヵ月間でゴールに到達するための現実的なアプローチ

一般的には、GDPR対応プロジェクトは「法令要件の整理」から始まり、「現状の実態調査」「法令要件とのギャップ分析」「対応方針の検討」「対応計画の策定」と進めていき、「対策の実施・改善」までを行います。しかし、3月時点で、簡易診断チェックリストで不備や抜け漏れが見つかった場合、セオリーどおりに進めていては間に合いません。

施行までの2ヵ月間でゴールに到達するためには、「管理態勢の構築」と「現状調査に基づく対応」の2つのタスクを同時に進めなければならないでしょう（**図表3**参照）。

「管理態勢の構築」では、まずGDPRに対応すべき項目を整理・文書化し、基準となるグループ共通ポリシーを本社で策定します。次に、そのグループ共通ポリシーをグループ各社に展開し、各子会社でルールを導入するよう指示します。

一方「現状調査に基づく対応」では、EU在住者データの調査を実施し、それを基に国際間データ移転にかかる契約締結等の措置と、処理の記録義務に対応する台帳を作成します。

II. GDPRプロジェクトを成功させるための3つのポイント

1. 本社と子会社の役割分担を明確にする

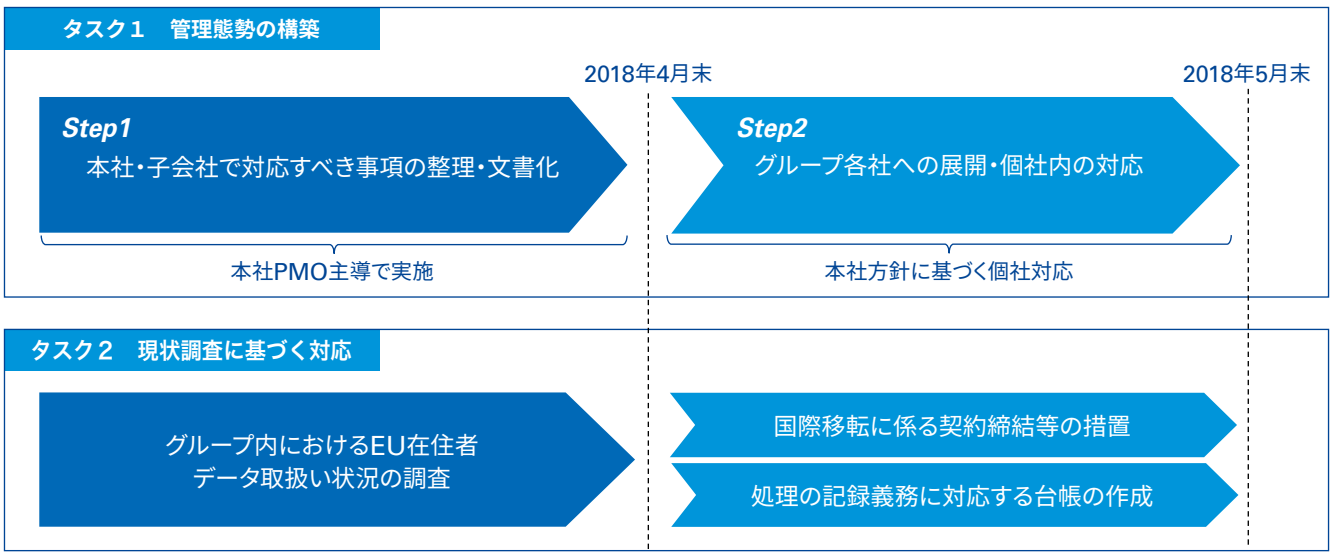
GDPRプロジェクトを成功に導くために最も重要となるのが、本社と子会社の役割分担の明確化です。あるべき姿は、本社が主導してグローバル共通ポリシーを策定し、プロジェクトを推進することです。子会社がそれぞれで基準を作ってしまうと、グループ全体の整合性が取れなくなってしまうことから、グループ全体の方針や基準は本社で決めることが重要です。

2. リスクコントロールの観点から管理ルールを策定する

GDPR対応として、単純に法令条文をそのまま規程・ルール化するだけでは意味がありません。実際に適切な取扱いが行われるようにするには、法令違反の生じるリスクを特定し、そのリスクに対して誰が何をするかという具体的な管理ルールを決めておく必要があります。

たとえば、個人情報漏洩事故が起きた場合、GDPRでは72時間以

図表3　最短でゴールに到達するための現実的アプローチ案



内に監督当局に報告する義務が定められています。しかし、社内規定に「72時間以内に報告すること」と記載するだけでは、実際に72時間以内に監督当局に報告することは難しいでしょう。なぜならば、インシデントの報告基準が曖昧だったり、誰が監督当局に報告をするのかが決まっていなかったとしたら、どのようなアクションを取ればよいのかがわからないからです。

3. DPOに最適な連携体制を設計する

GDPRでは、一定の条件下においてDPOの設置が求められており、一般的には、DPOの実務的な支援を行うサポートチームも設けられます。GDPRでは、DPOはグループ企業内の複数企業を兼務することも許容されているため、グループ内のどこにDPOを設置し、その責任範囲をどのように設定するか、といった点について、慎重に設計することが重要です。

DPOの責任範囲が適切に設定されていないと、監督当局や対象となる個人情報のデータ主体とのコミュニケーションが適時に行えなかったり、データ保護影響評価のコンサルテーションや、法令遵守状況のモニタリングなどの手続きが複雑になったりするなど、実運用上での問題が生じる可能性があります。逆に、グループ全体で適切な体制が設計できていれば、様々な管理業務の効率化が期待できます。

III. データを守るための セキュリティ対策

1. セキュリティ対策は多層防御で

GDPRのDはデータのことです。つまり、GDPRはデータを保護するための法令ということです。そのため、GDPR対応プロジェクトにおけるIT部門の役割は広範囲にわたり、しかも極めて重要です。「システム対応」の領域はもちろんのこと、「ガバナンス態勢構築」や「プロセス整備」の領域でも、IT部門が関与する要件は多々あります。

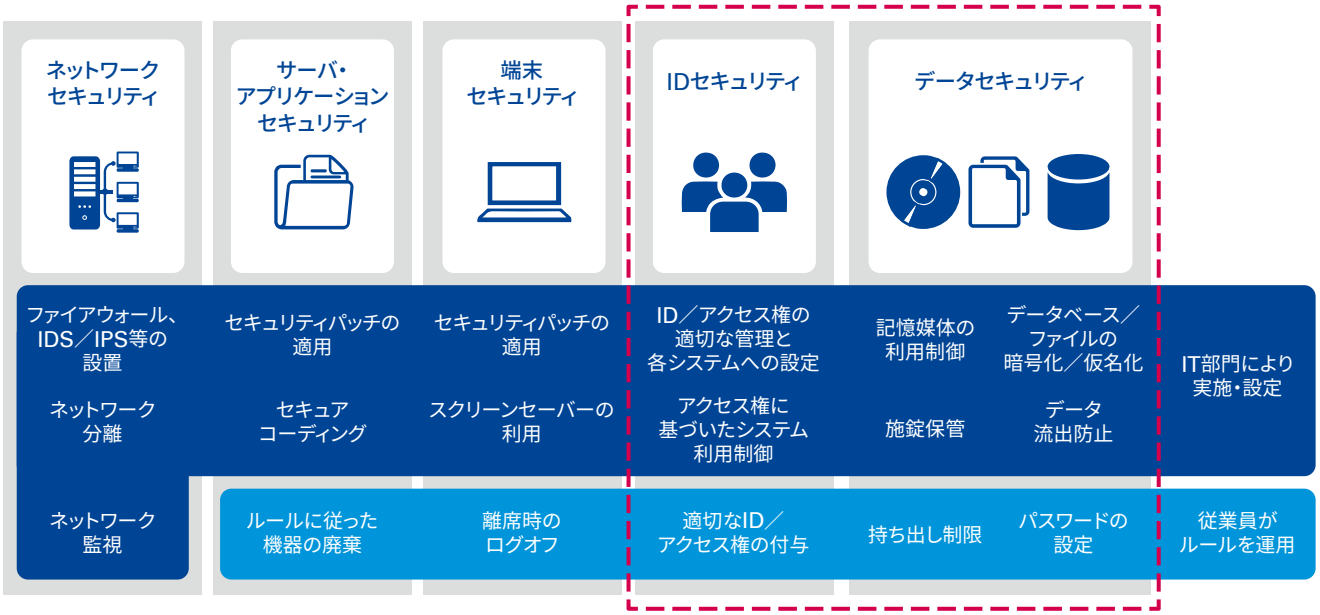
また、IT部門が導入する技術的セキュリティ対策には、ファイアウォールの設置や認証システムの構築、データの暗号化などがありますが、これらの対策には多くの時間と多大な費用がかかります。

これら技術的セキュリティ対策は、大きく分けると「ネットワーク」「サーバー・アプリケーション」「端末」「ID」「データ」の5つに分類できます。そのなかでも個人データ保護という意味では、データそのものを保護する「データセキュリティ」と、誰がそのデータにアクセスできるかを設定する「IDセキュリティ」が特に重要となります（**図表4**参照）。

2. コンプライアンスツールを利用する

個人データの処理をIT部門や外部組織に委託する場合、コンプライアンス上の必要性から、そこで実施されているセキュリティ対策を調査票などで確認することがあります。こうした確認は、依頼元となる様々な部署が、それぞれの都合でばらばらに行うため、委託

図表4 「取扱いの保護」における実施対象と内容（一例）



を受けている側では、同じような項目を何度も確認されることになり、負担が大きくなります。

こうした非効率を解消することを目的に、欧米では各組織でのコンプライアンス状況を一元管理・共有できるGRC（Governance, Risk & Compliance）ソリューションの導入が進んでいます。GRCソリューションとは、ガバナンス、リスク、コンプライアンスにかかる「リスク」「統制目標」「実施状況」「確認結果」等の情報をデータベースに一元管理することで、態勢の高度化・効率化を図るITツールです。

GRCソリューションでは、個人データの台帳を一元的に管理することも可能で、これを活用することによって、データ主体や監督当局からの要請にも速やかに対応することが可能になると期待されています。

IV. 本社主導で組織横断的に対応する

ネットワークが世界中に張り巡らされ、様々なSNSで情報が拡散する現代社会において、個人情報漏洩やプライバシー侵害を起こすと、その企業は高額な罰則金の支払いや営業停止命令、ライセンスのはく奪といった行政処分を受けることになります。事後対応が長引けば、企業ブランドも毀損しかねず、経営にも影響を与えます。つまり、GDPRをはじめとしたプライバシーリスク対応は経営の最重要課題の1つと言え、その対策には本社主導でグループ各社と密にコミュニケーションを取り、組織横断的に対応することが重要です。

GDPR　コンテンツ

ウェブサイトでは、GDPR（EU一般データ保護規則、General Data Protection Regulation）の概要をはじめとする解説や最新情報、企業における対応の進め方のポイント、簡易診断ツールなどを提供しています。また、KPMGが提供するサービスやセミナーもご紹介します。
www.kpmg.com/jp/gdpr

本稿に関するご質問等は、以下の担当者までお願いいたします。

KPMG コンサルティング株式会社
サイバーセキュリティアドバイザリー
TEL：03-3548-5111（代表電話）

ディレクター　大洞　健治郎
kenjiro.obora@jp.kpmg.com

ディレクター　万仲　隆之
takayuki.manchu@jp.kpmg.com

KPMGジャパン

marketing@jp.kpmg.com
www.kpmg.com/jp