2018.08.08

情報セキュリティニュース ＜号外＞

EU 一般データ保護規則（GDPR）について

【要旨】

■ 本年 5 月 25 日、「EU 一般データ保護規則（General Data Protection Regulation：GDPR）」が施行された。

■ GDPR は、EU を含む欧州経済領域（EEA）域内で取得した個人データの処理および EEA 域外に移転するために満たすべき法的要件を規定しており、EEA 域内に現地法人・支店・駐在員事務所を置く企業・団体・機関だけでなく、EEA 域内に現地法人・支店・駐在員事務所を置かない事業者であっても、インターネット取引などで EEA 域内所在者の個人データのやり取りをする企業・団体・機関が適用対象となり得る。

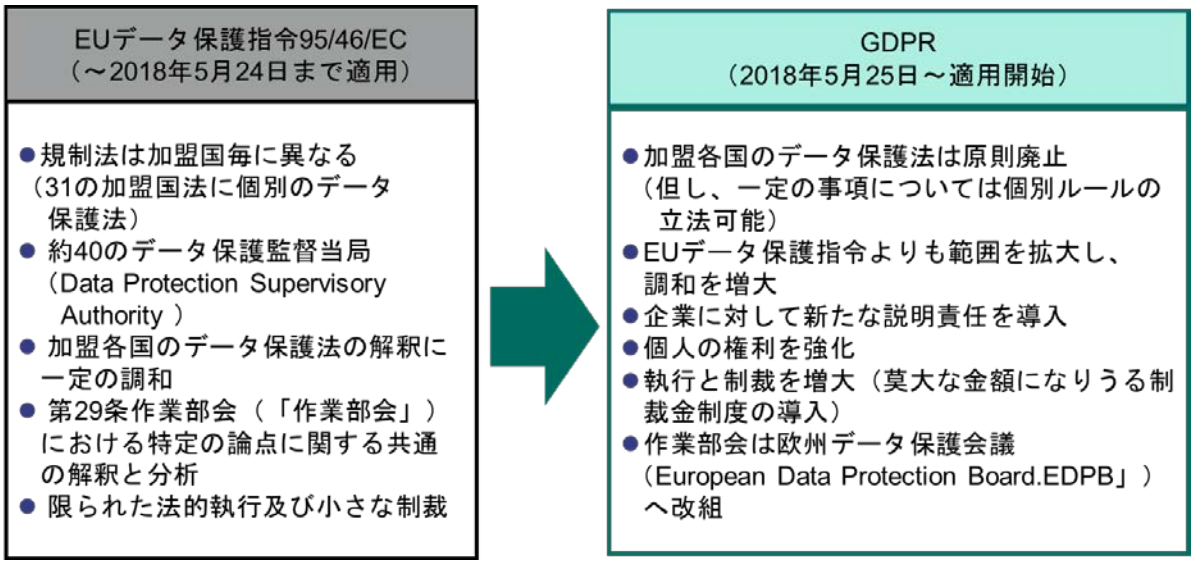
■ GDPR の要求事項は多岐にわたり、違反による制裁が極めて重く、経営に重大なインパクトを与えるおそれがある。企業は各条文の内容の理解にとどまらず自社の置かれている状況を適切に把握した上で実務対応計画を慎重に進めていくことが望ましい。

■ 本レポートでは、GDPR の概要を整理するとともに、最低限実施すべき取組のポイントを解説する。

１．GDPR の概要

EEA域内[1]の個人データ保護を規定する法として、1995 年から現在に至るまで適用されている「EU データ保護指令（Data Protection Directive 95）」に代わり、「EU一般データ保護規則（General Data Protection Regulation：GDPR）」が施行された。

GDPR は個人データやプライバシーの保護に関して、EU データ保護指令より厳格に規定しており、また、EU データ保護指令が EU 加盟国による法制化を要するのに対し、GDPR は EU 加盟国に同一に直接効力を持つ。



【図 1】データ保護指令から GDPR への主な変更点

[1] EEA 域内
EU 加盟国にノルウェー、アイスランド、リヒテンシュタインを加えた自由経済圏。

（１）保護対象となる「個人データ」の範囲

GDPRでは、「識別された自然人[2]または識別可能な自然人（これを「データ主体」という）に関する情報」を「個人データ」と定義されている。個人データの例として、

- 個人に関する属性情報（氏名、住所、生年月日、電話番号、メールアドレスなど）
- 個人の行動に関する情報（位置情報、購買履歴、信用履歴など）
- オンライン識別子（IP アドレス、cookie など）
- その他、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、社会的な固有性に関する要因を識別できるもの

が挙げられる。

日本における個人情報保護法では、位置情報やオンライン識別子（cookie）は保護対象の範囲に含まれておらず、GDPR は保護対象となる個人データの範囲が広く定義されていることがわかる。

（２）GDPR の適用範囲

従来の EU データ保護指令では、EEA 域内に現地法人・支店・駐在員事務所等、物理的な拠点をもつ企業や団体が適用対象であったが、GDPR は以下のとおり規定している。

①その取扱いがEEA域内で行われるものであるか否かを問わず、EEA域内の管理者[3]または処理者[4]の拠点の活動の過程における個人データの取扱い

（例：自社欧州子会社の従業員データ・顧客データを日本で保存する）

②取扱活動が以下と関連する場合、EEA域内に拠点のない管理者または処理者によるEEA域内のデータ主体の個人データの取扱い

・EEA 域内のデータ主体に対して商品またはサービスを提供する場合

・EEA 域内のデータ主体の行動を監視する場合

（例：日本法人が、英語で、ユーロが支払通貨として利用できるようにして日本のサーバで EC サイトを運営し、EEA 域内に在住する顧客から、個人情報を取得する）

（例：欧州に在住する個人から、アプリ等で位置情報を取得したり、ウェブサイト上から cookie で個人情報を取得する）

すなわち、GDPR は、EEA 域内にいるデータ主体の個人情報を取り扱う企業であれば EU 域内外を問わずに適用される。日本国内に拠点を置く企業であっても、EEA 域内の個人に向けてサービスや商品を提供する場合は、GDPR を遵守する必要がある。

２．GDPR において企業が求められる義務

GDPR は 173 項の前文と 99 条の本文で構成され、適用対象となる企業・団体・機関に対して求める主要な事項を以下に示す。

（１）個人データの取扱いと関連する基本原則

個人データを処理するに当たり、管理者は下表 1 の 6 原則を遵守する義務を負っている。これに加えて、管理者はその遵守を個人（データ主体）や監督機関に証明できなければならない（アカウンタビリティ）。

---

[2] 自然人
権利能力が認められる社会的実在としての人間をいう。法人に対する概念であり，単に人ともいう。

[3]管理者
単独または共同で個人データの処理の目的と手段を決定する自然人、法人、公的機関、行政機関またはその他の団体。管理者は、個人データの処理の適法性と GDPR 違反に対する責任を負う。

[4]処理者
管理者を代理して、個人データの処理を行う自然人、法人、公的機関、行政機関またはその他の団体。

【表 1】個人データの処理における原則

原則	内容（第 5 条 1 項）
適法性、公平性および透明性の原則	個人データは、適法、公平かつ透明性のある手段で処理されなければならない。
目的の限定の原則	個人データは、識別された、明確かつ適法な目的のために収集されるものでなければならず、これらと相容れない方法で更なる処理を行ってはならない。
個人データの最小化の原則	個人データは、処理を行う目的の必要性に照らして、適切であり、関連性があり、最小限に限られていなければならない。
正確性の原則	個人データは、正確であり、必要な場合には最新に保たれなければならない。不正確な個人データが確実に、遅滞なく消去または訂正されるように、あらゆる合理的な手段が講じられなければならない。
保管の制限の原則	個人データは、当該個人データの処理の目的に必要な範囲を超えて、データ主体の識別が可能な状態で保管してはならない。
完全性および機密性の原則	個人データは、当該個人データの適切なセキュリティを確保する方法で取り扱われなければならない。当該方法は、無権限の、または違法な処理に対する保護および偶発的な滅失、破壊、または損壊に対する保護も含むものとし、個人データの適切なセキュリティが確保される形で処理されなければならない。

（出典：日本貿易振興機構「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編））

（２）取扱いの適法性

管理者または処理者は、下表 2 の適法根拠に基づいた個人データの処理を行わなければならない。

【表 2】個人データの適法な処理の要件

適法根拠	要件
同意	データ主体が 1 つ以上の特定の目的のために自己の個人データの処理に同意を与えた場合
契約	データ主体が当事者となっている契約の履行のために処理が必要な場合、または契約の締結前のデータ主体の求めに応じて手続きを履践するために処理が必要な場合
法的義務	管理者が従うべき法的義務を遵守するために処理が必要な場合
データ主体からの重大な利益	データ主体、または他の自然人の重大な利益を保護するために処理が必要な場合
公共の利益	公共の利益、または管理者に与えられた公的権限の行使のために行われる業務の遂行において処理が必要な場合
正当な利益	管理者または第三者によって追求される正当な利益のために処理が必要な場合。 ただし、データ主体の、特に子どもがデータ主体である場合の個人データの保護を求める基本的権利および自由が、当該利益に優先する場合を除く

（出典：日本貿易振興機構「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）に基づきＭＳ＆ＡＤインターリスク総研が作成）

（３）同意の要件

管理者は、明確かつ平易な文言を用いて、本人から明示的な同意を取得する必要がある。また、本人がいつでも同意を撤回する権利が認められている。

なお、管理者は、個人（データ主体）の同意を取得したことを証明できなければならず、同意の証明には、同意取得方法、取得日時、情報提供内容を記録する必要がある。

（４）特別な種類の個人データの取扱い

以下に関するデータの取扱いは、原則として禁止されている。

【表 3】特別な種類の個人データ

分類	例
特別カテゴリーの個人データ（第 9 条）	･人種的若しくは民族的な出自 ･政治的な意見 ･宗教上若しくは思想上の信条 ･労働組合への加入を明らかにする個人データの取扱い ･遺伝子データ ･自然人を一意に識別することを目的とする生体データ ･健康に関するデータ ･自然人の性生活若しくは性的指向
犯罪関係の個人データ（第 10 条）	･有罪判決に関するデータ ･犯罪歴に関するデータ

なお、特別カテゴリーの個人データについて、例外的に取扱いを許される条件は、

- データ主体が明確な同意を与えた場合
- 雇用及び社会保障並びに社会的保護の法律の分野における管理者またはデータ主体の義務を履行する目的のため
- データ主体が物理的または法的に同意を与えることができない場合で、データ主体またはその他の自然人の生命に関する利益を保護するために取扱いが必要な場合

などに限られている。

（５）透明性のある情報提供、連絡及び書式

従来も本人への利用目的等の通知義務が定められていたが、GDPR は個人データの取り扱いや本人の権利（アクセス、訂正、削除、利用制限、ポータビリティ）について透明かつ明瞭に開示する必要がある。

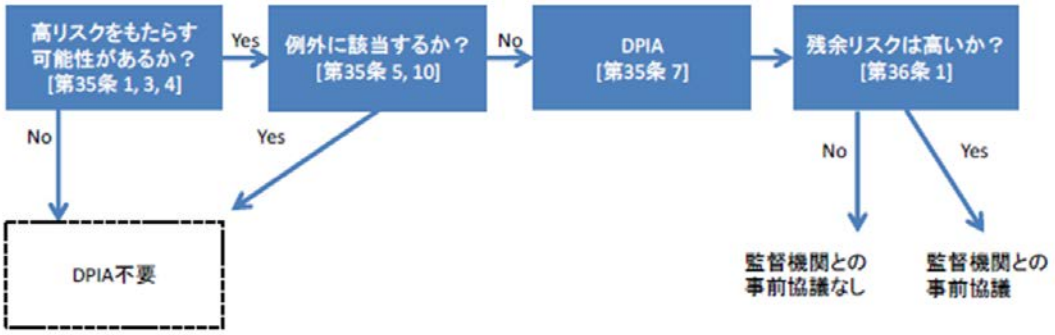
（６）データ保護影響評価

取扱いの性質、範囲、過程及び目的を考慮に入れた上で、個人データの処理が自然人の権利および自由に対する高いリスクを発生させるおそれがある場合、管理者は、データ保護影響評価（DPIA）を行わなければならない。

データ保護影響評価は少なくとも以下の事項を含めなければならない。

- 想定されるデータ処理業務の内容及びその目的
- 目的に対するデータ処理業務の必要性及び比例性
- データ主体の権利及び自由に対するリスクの程度
- 上記リスクに対処するために予定される対策

データ保護影響評価（DPIA）実施判断基準および実施方法は以下の図 2 のとおり。



【図 2】データ保護影響評価実施の判断フロー

（７）データ保護オフィサー（DPO）の指名

管理者及び処理者は、以下の場合において、データ保護オフィサー（Data Protection Officer、DPO）を指名しなければならない。

- 公的機関または公的組織によって個人データ処理が行われる場合
- 管理者または処理者の中心的業務が、その取扱いの性質、範囲及びまたは目的のゆえに、データ主体の定期的かつ系統的な監視を大規模に要する取扱業務によって構成される場合
- 管理者または処理者の中心的業務が、第 9 条による特別な種類のデータ及び第 10 条で定める有罪判決及び犯罪行為と関連する個人データの大規模な取扱いによって構成される場合

（８）EEA 域外への個人データ移転禁止の原則

EEA 域外にある第三国への個人データの移転は、原則として次のいずれかの措置が必要となる。

- 十分性認定
  移転先の所在国が十分な保護措置を講じている国として EU 監督機関から認定を受ける。日本は十分性認定を受けていない（ただし、個人情報保護員会発表（7/17）「日 EU 間の相互 の円滑な個人データ移転を図る枠組み構築に係る最終合意」のとおり、2018 年の秋までに十分性 認定の発効を実現できる見込み）。
- 拘束的企業準則（Binding Corporate Rules、BCR）
  企業グループ内でのデータ移転に関する行動規範である BCR を策定し、EU 監督機関の承認を得る。
- 標準契約条項（Standard Contractual Clauses、SCC）
  データ授受当事者企業間で、SCC（EU が定めた標準契約でありデータ保護措置の必要事項を定めたもの）を締結する。当事者企業において、各々、SCC に定められたデータ保護要件を充たす態勢を整備する必要がある。
- 特別な例外
  個人（データ主体）の明示的な同意がある場合など。

（９）記録保持義務

個人データの管理者と処理者は、各 EU 加盟国に設置されているデータ保護監督機関から求められた場合、いつでも個人データ処理記録を提出しなければならない。

記録する必要がある項目は下表 4 のとおり。

【表 4】管理者、処理者の記録保持義務

管理者の処理記録	処理者の処理記録
･管理者、データ保護責任者の名前および連絡先 ･取扱いの目的 ･データ主体の類型（顧客、従業員など） ･（想定される）個人データの開示先 ･第三国移転がある場合の移転先国 ･第 49 条[5]の例外による第三国移転を行う場合、保護措置の内容 ･（可能なときは）個人データの保持期限 ･（可能なときは）組織的・技術的安全管理措置の概要	･処理者、管理者の名前および連絡先 ･処理者、管理者それぞれの代理人、データ保護責任者の名前および連絡先 ･管理者の代わりに行われる取扱いの種類 ･第三国移転がある場合の移転先国 ･第 49 条の例外による第三国移転を行う場合、保護措置の内容 ･（可能なときは）組織的・技術的安全管理措置の概要

なお、従業員 250 名以下の企業はこれらの処理記録を保持する義務はないが、以下に該当する場合は処理記録を保持しなければならない。

- 当該処理がデータ主体にリスクを及ぼす可能性が高い場合
- 当該処理が 1 回限りではない場合
- 特別カテゴリーの個人データ（第 9 条）もしくは犯罪に関する個人データ（第 10 条）を処理する場合。

（10）監督機関に対する個人データ侵害の通知

管理者は、個人データの侵害を認識してから 72 時間以内に担当するデータ保護監督機関へ届出しなければならない。また、72 時間以内に届け出ることができない場合、その理由を明らかにする必要がある。

なお、管理者は、いかなる個人データ侵害についても、その内容、影響、講じられた救済措置に関する事実を記載した文書を作成しなければならない。

また、本人の権利、自由を脅かす高いリスクがある場合には、本人に対しても遅滞なく通知する必要がある。

３．監督処分と制裁金

EU の各加盟国は GDPR の施行を監視するために、データ保護監督機関を設置することが義務付けられており、データ保護監督機関は管理者や処理者に対する情報提出命令、監査、管理者・処理者が処理する個人データの閲覧、立ち入り調査、警告、データ主体に周知させるよう指示する命令、作為・不作為に関する遵守命令、処理の禁止命令、制裁金賦課などの権限を行使する。

GDPR 違反の場合の制裁金の上限額には、次の 2 とおりの類型がある。

[5] GDPR 第 49 条
十分性認定を得ておらず、適切な安全管理措置を講じていない場合には、以下の特別の状況にある場合のみ EEA 域外の第三国への個人データの移転が認められている。
- リスクについて情報提供を受けた後の明示的な同意
- 契約の履行のため必要な場合
- 重要な公共の利益のため

【表 5】GDPR 違反に対する制裁金の上限額

2,000 万ユーロ、または、事業者の場合には前会計年度の全世界年間売上高の 4%のいずれか高い金額	
	・データ処理に関する原則を遵守しなかった場合 ・適法に個人データを処理しなかった場合 ・同意の条件を遵守しなかった場合 ・特別カテゴリーの個人データ処理の条件を遵守しなかった場合 ・データ主体の権利及びその行使の手順を尊重しなかった場合 ・個人データの移転の条件に従わなかった場合 ・監督機関の命令に従わなかった場合
1,000 万ユーロ、または、事業者の場合には前会計年度の全世界年間売上高の 2%のいずれか高い金額	
	・16 歳未満の子どもに対する直接的な情報社会サービスの提供に関する個人データの処理には、子に対する保護責任を持つ者による同意または許可が必要という条件に従わなかった場合 ・GDPR 要件を満たすために適切な技術的・組織的な対策を実施しなかった、またはそのような措置を実施しない処理者を利用した場合 ・義務があるのにEU代理人[6]を選任しない場合 ・責任に基づいて処理行為の記録を保持しない場合 ・監督機関に協力しない場合 ・リスクに対する適切なセキュリティレベルを保証する適切な技術的・組織的な対策を実施しなかった場合 ・個人データ侵害を義務があるのに監督機関に通知しなかった場合、データ主体に通知しなかった場合 ・影響評価を行なわなかった場合 ・影響評価によって示されていたにも係わらず処理の前に監督機関に助言を求めなかった場合 ・データ保護オフィサーを選任しなかった場合、またはその職や役務を尊重しなかった場合

[6] EU 代理人
EEA 域内に拠点を持たない企業は代理人を選定しなければならない可能性があり、EU 代理人を個人データが処理されるデータ主体が居住する加盟国のうちの一つに設置する必要がある。

４．最低限実施すべき取組のポイント

日本において GDPR の影響を受けるのは、「EEA 域内に子会社、支店、営業所を有している企業」「日本から EEA 域内に商品やサービスを提供している企業」「EEA 域内から個人データの処理について委託を受けている企業」となる。

GDPR の要求事項は多岐にわたり、違反による制裁が極めて重く、経営に重大なインパクトを与えるおそれがある。企業は各条文の内容の理解にとどまらず自社の置かれている状況を適切に把握した上で、次のような実務対応計画を慎重に進めていくことが望ましい。

（１）現状把握

まず取り組むべき優先事項としては、自社内における個人データの現状把握が挙げられる。業務で扱う個人データを大別すると、以下の 3 種類となる。

・ 一般消費者（顧客）の個人データ
・ 従業員の個人データ
・ 取引先（法人顧客、仕入れ先）の個人データ

これらの個人データの自社における管理・処理・移転の方法および個人（データ主体）との関係を整理すべく、企業グループの本社、子会社、支店などにおいて処理される EEA 域内で取得した個人データの処理の目的、種類(特別カテゴリーの個人データ、犯罪関係の個人データの有無)および量と内容を、各々の本社、子会社、支店などに質問票を送付・回収すること、またはフォローアップのヒアリングを行うことで把握する。

次に、当該処理行為が GDPR で求められている個人データ処理その他の法的要件を満たしているかどうか、GDPR の規定および各種ガイドラインと照合し、GDPR の要求に十分に応えられていない部分を洗い出す。

（２）管理体制の構築

現状把握の結果に基づき、GDPR 対応として求められる個人データ保護の管理体制を構築する。具体的には個人データの管理を担当する部署、個人データを取り扱う部門、個人情報保護に関する法規定をアドバイスする部門などからなる組織横断的なプロジェクトとして、プロジェクトをまとめる事務局、プロジェクトの責任者の選任等が必要である。

また、現状把握の結果課題が洗い出された個人データの処理に対して、対策の優先順位などを社内で検討していく。同時に、こうした作業の過程をとりまとめ、監督当局から照会を受けた際には、自社が適切に対応できる体制をとっていることを説明できるよう準備をしておく。

（３）対策の実行

GDPR 対応のプライバシーポリシーの策定を行い、社内への展開と外部向けに自社のホームページで公開する準備を行う。

併せて個人データの取扱い手順等を定めるデータ保護方針、規程類、マニュアルを策定する。新たに制定した規程類やルールにのっとって適切に運用が行われているかどうかを評価し、必要に応じて規程等の見直しまたは運用の改善を実施する。

（４）その他

GDPR は、一定の事項に関して、EU 加盟国が各国法により独自に定めることを認めている。EU 加盟各国が規定することができる項目の中には、欧州ビジネスを行う日本企業に影響を及ぼすものもあるため、実際の GDPR 対応においては、ビジネスを展開する EU 加盟国の個人データ保護関連法の確認も必要となってくる。

前述のとおり GDPR の適用となる企業にとって実施すべき対策事項は多岐にわたり、GDPR 違反した場合の影響は金銭面のみならずレピュテーションリスクにおいても甚大である。本稿にて、対策が不十分な企業において最低限実施しておくべきことを解説したが、これらはあくまでも暫定的な対策にすぎないことに留意いただきたい。

GDPR 対応においては、本規制のみならず、企業が活動する EU 加盟国における関連法についての法的観点からのアドバイスは不可欠である。個人情報取扱いの契約文書（BCR や SCC）の作成や文言のリーガルチェックなど、法律家へ支援・協力をすることをおすすめする。

GDPR のリスクを正しく理解いただき、経営陣によるリーダーシップの下、グローバルな情報管理体制の構築および強靭化をすすめていただきたい。

ＭＳ＆ＡＤインターリスク総研㈱　リスクマネジメント第四部
マネジャー・上席コンサルタント　岡田　智之