EU一般データ保護規則が改正個人情報保護法に与える影響

[**IT・情報セキュリティ**](https://business.bengo4.com/category3)2017年08月31日 20:10

[渡邉 雅之弁護士 [](https://business.bengo4.com/lawyer/28977)](https://business.bengo4.com/lawyer/28977)

　「EUデータ保護指令」や今後新たに定められる「EU一般データ保護規則」が個人情報保護法の改正にどのような影響を与えるのか教えてください。また、米国がEUとの間で締結していたセーフハーバー協定や新たに締結したEU-US Privacy Shieldについても教えてください。

　EUデータ保護指令は、EU域内から個人データを第三国に移転できる場合を、当該第三国がEUから見て十分な水準の保護措置を確保している場合に限定する「十分性認定」の制度が設けられているため、日本は「十分性の認定」を得る観点から、改正個人情報保護法において、「独立した第三者機関の設置」、「要配慮個人情報の取扱いの規律」、「小規模事業者への保護法の適用」「越境データ移転についての規律」、「開示請求権の適用の明確化」を行いました。もっとも、2018年5月に施行される「EU一般データ保護規則」により、EUにおける個人データの保護の規律は強化され、改正個人情報保護法が「十分性の認定」を得る上で十分かという問題があります。

　他方、米国がEUと締結していたセーフハーバー協定は2015年10月6日に欧州司法裁判所で無効とされました。これにより、米国とEUは2016年2月にEU市民のプライバシー保護を強化したEU-US Privacy Shieldという新たな協定を締結しました。

**解説**

※本QAの凡例は注の通りです[1](https://business.bengo4.com/category3/practice612" \l "fn:1)。

**EUデータ保護指令の「十分性の認定」**

　EUでは、「**個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する1995年10月24日の欧州議会及び理事会の95／46／EC指令**」（Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data）（以下「**EUデータ保護指令**」といいます）により、EU域内から個人データを第三国に移転できる場合を当該第三国がEUから見て十分な水準の保護措置を確保している場合に限定する「**十分性認定**」の制度が設けられています。

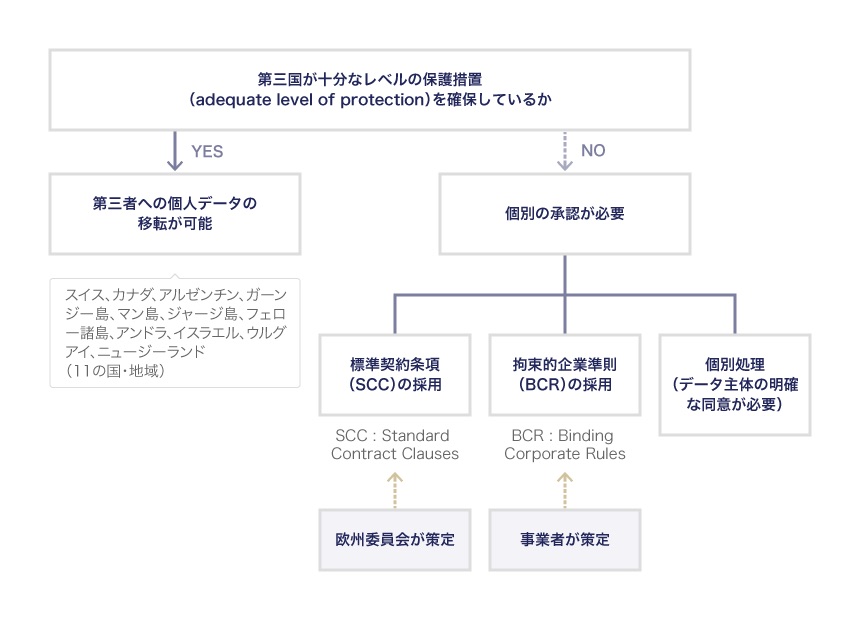
　参照：総務省「**[パーソナルデータの利用・流通に関する研究会（第1回）](http://www.soumu.go.jp/main_sosiki/kenkyu/parsonaldata/64882.html" \o "" \t "_blank)**」

　「十分性認定」の制度においては、EU域内から個人データを第三国に移転できる場合を当該第三国が十分な水準で個人情報の保護を確保するために必要な措置が取られている場合に限定しています（EUデータ保護指令25条）。  
　これまでに11の国と地域（スイス、カナダ、アルゼンチン、ガーンジー島、マン島、ジャージ島、フェロー諸島、アンドラ、イスラエル、ウルグアイ、ニュージーランド）がEUから十分な水準の保護措置を確保している旨の認定を得ています（参照：個⼈情報保護委員会「[**個⼈情報保護委員会の国際的な取組について**](http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/4th_sangyokakumei_dai2/siryou3.pdf)」）。

　「十分性の認定」を得ないEU域外の国・地域には、①EU域内のデータ主体（本人）から明確な同意を取得するか、②欧州委員会が策定した標準契約条項（Standard Contract Clause）を採用するか（当局の承認が必要）、③事業者が策定した拘束的企業準則（Binding Corporate Rules）を採用（当局の承認が必要）しなければ、個人データの移転が認められません。

　日本政府は、改正前の個人情報保護法ではEUから「十分性の認定」を得ることは困難と考え、改正個人情報保護法により、EUから不十分である指摘されることが推測される、「独立した第三者機関の設置」、「要配慮個人情報の取扱いの規律の設置」、「小規模事業者への保護法の適用」「越境データ移転についての規律の設置」、「開示請求権の適用の明確化」を行いました（参照：「**[個人情報保護法改正の背景と概要](https://business.bengo4.com/category3/practice611" \o "" \t "_blank)**」）。

**【EUから第三国への個人データの移転】**



出典：内閣官房資料

**EU一般データ保護規則**

**EU一般データ保護規則（General Data Protection Rules）**は、欧州議会において、2016年4月27日に制定され、2018年5月25日に施行されます。  
　同規則の施行により、EUデータ保護指令は廃止されます。  
　EU一般データ保護規則は、EUデータ保護指令と異なり、各加盟国での立法化は不要でそのまま効力を有することになります。

　EU一般データ保護規則は、以下の各点においてEUデータ保護指令よりも強化されています。

* 透明で適切なプライバシーポリシーの提供
* 明示的な同意の取得
* 忘れられる権利
* データ・ポータビリティの権利
* プロファイリングの拒否
* 16歳以下の利用者について保護者の同意
* データ違反時の報告・連絡（「可能な限り72時間以内」）
* データ保護影響評価
* 監督機関による高額の制裁金（下表を参照）

　「**十分性の認定**」の制度は維持されます（EU一般データ保護規則45条）。  
　「**標準契約条項**」については、同条項を第三国移転の二当事者間で用いれば、監督機関による更なる承認手続は不要となります（EU一般データ保護規則46条）。  
　「**拘束的企業準則**」は、EU加盟国の1つの監督機関で承認を得れば、EUの他の監督機関は一括でその結果を追認することになります（EU一般データ保護規則47条）。

|  |  |
| --- | --- |
| **制裁金の上限額の基準** | **義務違反の類型（根拠条文はEU一般データ保護規則）** |
| 企業の全世界年間売上高の2％、または、1,000 万ユーロのいずれか高い方（83条） | * 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（8条） * 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（25条、28条） * EU 代理人を選任する義務を怠った場合（27条） * 処理活動の記録を保持しない場合（30条） * 監督機関に協力しない場合（31条） * 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（32条） * セキュリティ違反を監督機関に通知する義務を怠った場合（33条） * データ主体に通知しなかった場合（34条） * データ保護影響評価を行なわなかった場合（35条） * データ保護影響評価によってリスクが示されていたにも関わらず、処理の前に監督機関に相談しなかった場合（36条） * データ保護責任者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（37～39条） |
| 企業の全世界年間売上高の4％、または、2,000 万ユーロのいずれか高い方（83条） | * 個人データの処理に関する原則を遵守しなかった場合（5条） * 適法に個人データを処理しなかった場合（6条） * 同意の条件を遵守しなかった場合（7条） * 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（9条） * データ主体の権利およびその行使の手順を尊重しなかった場合（12〜22条） * 個人データの移転の条件に従わなかった場合（44〜49条） * 監督機関の命令に従わなかった場合（58 条） |

　上記各点に相当する規律は、改正個人情報保護法においても定められていないため、EU一般データ保護規則が施行された場合、今回の改正個人情報保護法により、「十分性の認定」を得る上で十分かという問題が生じます。

**【忘れられる権利】**  
　さいたま地裁は、平成27年12月22日、インターネットの検索エンジンで住所と氏名を入力して検索すると三年余り前の女子高校生に対する児童買春の罪での逮捕歴が検索結果として表示され、更生を妨げられない利益が侵害されるとして検索エンジンの管理者に検索結果の削除を求めた仮処分命令の申立てについて、「忘れられる権利」に基づき認容されたとの決定を出しました（**さいたま地裁平成27年12月22日決定・判時2282号78頁**）。  
  
　しかしながら、同決定は、平成28年7月12日、東京高裁において取り消されました（**東京高裁平成28年7月12日決定・判時2318号24頁**）。同決定は、忘れられる権利は「法律で定められたものではなく要件や効果が明確でない」としました。忘れられる権利については本質的には名誉毀損やプライバシー侵害にもとづく申し立てと変わらず「独立して判断する必要はない」と判断されました。平成29年１月31日の最高裁第3小法廷判決においても同判断は維持されました（**[最高裁平成29年1月31日決定](http://www.courts.go.jp/app/hanrei_jp/detail2?id=86482" \t "_blank)**

[**無料会員登録・ログイン**](https://business.bengo4.com/login)**することで、本文中の法令・判例からe-gov、裁判所のサイトにリンクします。**

**・判時2328号10頁**）。

**米国のセーフハーバー協定と新たな協定（EU-US Privacy Shield）**

　米国とEUとの間では、2000年に、EU域内から米国に移転される個人データについてプライバシーに関するセーフハーバー原則に適合していると米国商務省が認定した米国企業に対してのみ、その情報の移転を認める「セーフハーバー協定」が結ばれていました。

　しかしながら、セーフハーバー協定は、2015年10月6日に欧州司法裁判所により当該協定が無効と判断されました。  
　これは、元CIAのスノーデン氏が、CIA等の米国の国家安全保障当局がFacebookなどのSNSから無差別・大量の個人情報を取得していると暴露をしたことを契機に、EU市民がEU域内のFacebookの現地法人に対して提起した訴訟です。

　この司法判断を受けて、米国とEUは、従前のセーフハーバー協定に代わる新たな枠組みとして、2016年2月にPrivacy Shieldを締結しました。  
　**Privacy Shield**は、モニタリングや執行に関して、EUの監督機関に対して厳格にすることを要求すると共に、米国の政府当局によるデータへのアクセスに関する規律についてはじめて書面化されたものです。

　Privacy Shieldの規律の特徴は以下のとおりです。

1. 民間事業者の義務の強化
   * 義務の強化および執行の厳格化
   * 透明性の強化
   * 事業者が本ルールを遵守していることを監督するメカニズムの導入
   * 遵守しない事業者への罰則・除外

今後の移転に関する条件の厳格化

1. EUのデータ主体（本人）の救済手段の強化  
   複数の救済手段が可能となります。
   * 会社への直接請求  
     会社は45日以内に請求に対して回答が必要。
   * ADR（調停）  
     ADRは無料で利用可能。
   * EUのデータ保護に関する監督機関  
     米国の商務省、連邦商取引委員会と連携し、EU市民の未解決の申請を解決。
   * Privacy Shield Panel  
     最終的な手段として、仲裁手続によることを認める。
2. 明確な保護施策・透明な義務
   * はじめて、米国政府が文書により、当局による個人データへのアクセスは、明確な制限、保護施策、監査のメカニズムにしたがって行わなければならないことを保証。
   * 米国の政府当局が無差別・大量の調査をしないことを保証。
   * 事業者は、請求のあったアクセスのおおよその数を報告することが可能。
   * 独立性のあるオンブズマン制度の導入。
3. モニタリング
   * 毎年、EUと米国は協力してモニタリングを行うメカニズムを構築。
   * 法執行・国家安全保障の目的によるアクセスを含む検証。
   * 欧州委員会・米国商務省が、米国とEUのデータ保護当局の国家による調査の専門家の協力の下に行う。
   * NGOその他のステークホルダーは、米国のプライバシー法およびその影響に関するプライバシーサミットを毎年行う。
   * 欧州委員会は、毎年のモニタリングの結果を欧州議会その他の関連当局に報告。

　米国企業への影響は以下のとおりです。

* Privacy Shieldの要件にあっているか毎年、自己確認が必要となる。
* ウェブサイトにプライバシーポリシーを公表する。
* 個人からの救済に関する申請に対して迅速に回答する必要がある。
* 人材に関する個人データを扱っている場合には、EUのデータ保護当局に協力することが求められる。

　EU市民への影響は以下のとおりです。

* セーフハーバー協定より透明性の高い個人データの米国への移転のためのルールの創設。
* 簡易で廉価な救済手段の創設：米国企業に直接または自分が住んでいるEU加盟国のデータ保護当局への申請が可能となる。

**日本政府が模索している方向性**

　日本政府は、EUとの間での個人データの域外への移転を認めることを模索し、交渉をしています。  
　個人情報保護委員会は、平成28年7月29日、「**[個人データの円滑な国際的流通の確保のための取組について](http://www.ppc.go.jp/enforcement/cooperation/initiatives/" \o "" \t "_blank)**」（個人情報保護委員会決定）と題する以下の文書を公表しました。

　経済・社会活動のグローバル化及び情報通信技術の進展に伴い、個人情報を含む大量のデータの国境を越えた流通が増大しており、OECD、APEC等において、個人情報の保護に関する情報交換や越境執行協力等を目的とした国際的な枠組みが構築されてきている。また、個人情報保護委員会の設置により、国際的な執行協力の枠組みであるGPEN（グローバルプライバシー執行ネットワーク）、APPA（アジア太平洋プライバシー機関フォーラム）においては、我が国が正式参加国として認められたところである。  
  
　これらの国際的な動向を踏まえて、個人情報保護法に基づく「[**個人情報の保護に関する基本方針**](https://www.ppc.go.jp/files/pdf/kihonhousin.pdf)」の変更に向けては、同方針案に「個人情報保護委員会において、個人情報の保護を図りつつ、国際的なデータ流通が円滑に行われるための環境を整備するため、国際的な協力の枠組みへの参加、各国執行当局との協力関係の構築等に積極的に取り組む」との趣旨を盛り込むこととし、国際的な取組を一層推進することとする。  
  
　具体的には、当面、以下の方針により取組を進めることとする。  
  
　個人情報保護委員会において、個人情報の保護を図りつつ、その円滑な越境移転を図るため諸外国との協調を進めることとし、当面、これまでに一定の対話を行ってきている米国、EU（英国のEU離脱の影響についてその動向を注視。）については、相互の円滑なデータ移転を図る枠組みの構築を視野に定期会合を立ち上げる方向で調整する。

　平成28年11月8日の「**[国際的な取組について](http://www.ppc.go.jp/enforcement/cooperation/initiatives/" \o "" \t "_blank)**」（個人情報保護委員会決定）においても同方針は維持されています。

　本年7月29日の個人情報保護委員会において、「**[個人データの円滑な国際的流通の確保のための取組について](http://www.ppc.go.jp/enforcement/cooperation/initiatives/" \t "_blank)**」を決定し、その中で、「個人情報保護委員会において、個人情報の保護を図りつつ、その円滑な越境移転を図るため諸外国との協調を進めることとし、当面、これまでに一定の対話を行ってきている米国、EU（英国のEU離脱の影響についてその動向を注視。）については、相互の円滑なデータ移転を図る枠組みの構築を視野に定期会合を立ち上げる方向で調整する」とした。これを踏まえ、米国及びEUと対話を行ってきているところである。  
  
　なお、個人情報の保護に関する法律第7条の規定に基づき、10月14日の個人情報保護委員会において作成し、10月28日に閣議決定された、**[個人情報の保護に関する基本方針](https://www.ppc.go.jp/files/pdf/kihonhousin.pdf" \t "_blank)**においては、「個人情報保護委員会において、個人情報の保護を図りつつ、国際的なデータ流通が円滑に行われるための環境を整備するため、国際的な協力の枠組みへの参加、各国執行当局との協力関係の構築等に積極的に取り組むものとする」とされている。

* **米国**  
  　定期的な会合を続けていくこと及び緊密に連携することの重要性について認識を共有した。加えて、自国のステークホルダーと共に、APEC越境プライバシールール（CBPR）システムに関する周知活動及び、APEC加盟エコノミーに対する参加促進を協力して行っていくことで一致している。   
  ⇒引き続き、グローバルな展開を念頭に、個人データ移転の枠組みであるAPEC越境プライバシールール（CBPR）システムの活性化等の取組を進める。
* **EU**  
  　日EU間で個人データの保護を図りながら越境移転を促進することが重要であることを強調し、その目標に向かって、日EU間で協力対話を続けていくことで一致している。  
  ⇒引き続き、グローバルな個人データ移転の枠組みとの連携も視野に置きつつ、以下の点を踏まえた議論を推進する。
  + 日EU間での個人データ移転は、改正個人情報保護法（独立機関である個人情報保護委員会の設置など）を前提として相互の個人データ流通が可能となる枠組みを想定するものとする。
  + また、EUにおいては、本年採択されたEU一般データ保護規則（GDPR）が平成30年5月に適用されることから、その運用に向けた動きも注視していく必要がある。

　さらに、平成29年7月4日の「**[日EU間の相互の円滑な個人データ移転について](http://www.ppc.go.jp/enforcement/cooperation/initiatives/" \t "_blank)**」（個人情報保護委員会決定）においては、EUから日本への個人データの移転については、EU一般データ保護規則に基づく十分性の認定を、日本からEUへの個人データの移転については、平成30年（2018年）前半を目標に、個人情報保護法24条に基づくEU加盟国の指定を行うことを視野に、個人情報保護法施行規則の改正を進めていくことを明らかにしました。

　個人情報保護委員会は、昨年来、個人情報保護法を前提として、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を視野に、欧州委員会司法総局と累次の対話を重ねてきており、相互の制度に関する理解は相当程度進んできた。  
  
　本年7月3日には、熊澤個人情報保護委員会委員はヨウロバー欧州委員と会談を実施し、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の具体的方策等について確認したところである。  
　この会談を踏まえ、個人情報保護委員会としては、今後、欧州委員会の日本に対する十分性認定に係る作業の進捗に併せて、来年前半を目標に個人情報保護法第24条に基づくEU加盟国の指定を行う可能性を視野に、本年6月16日に個人情報保護委員会において決定した「**[個人情報保護法第24条に係る委員会規則の方向性について](https://www.ppc.go.jp/files/pdf/290616_siryou1.pdf" \t "_blank)**」に基づき、今後委員会規則の改正手続を進めていくこととする。  
  
　また、EU加盟国については、EUの個人情報保護制度のみならず、その制度の遵守態勢、執行態勢並びに相互の理解、連携及び協力の可能性等について確認していく必要があることから、引き続き、情報収集・調査を行うとともにEU加盟国の各データ保護機関等との対話を引き続き精力的に行っていくこととする。

* + 個人情報保護法、改正個人情報保護法：個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成27年9月9日法律第65号）に基づく改正後の個人情報保護法