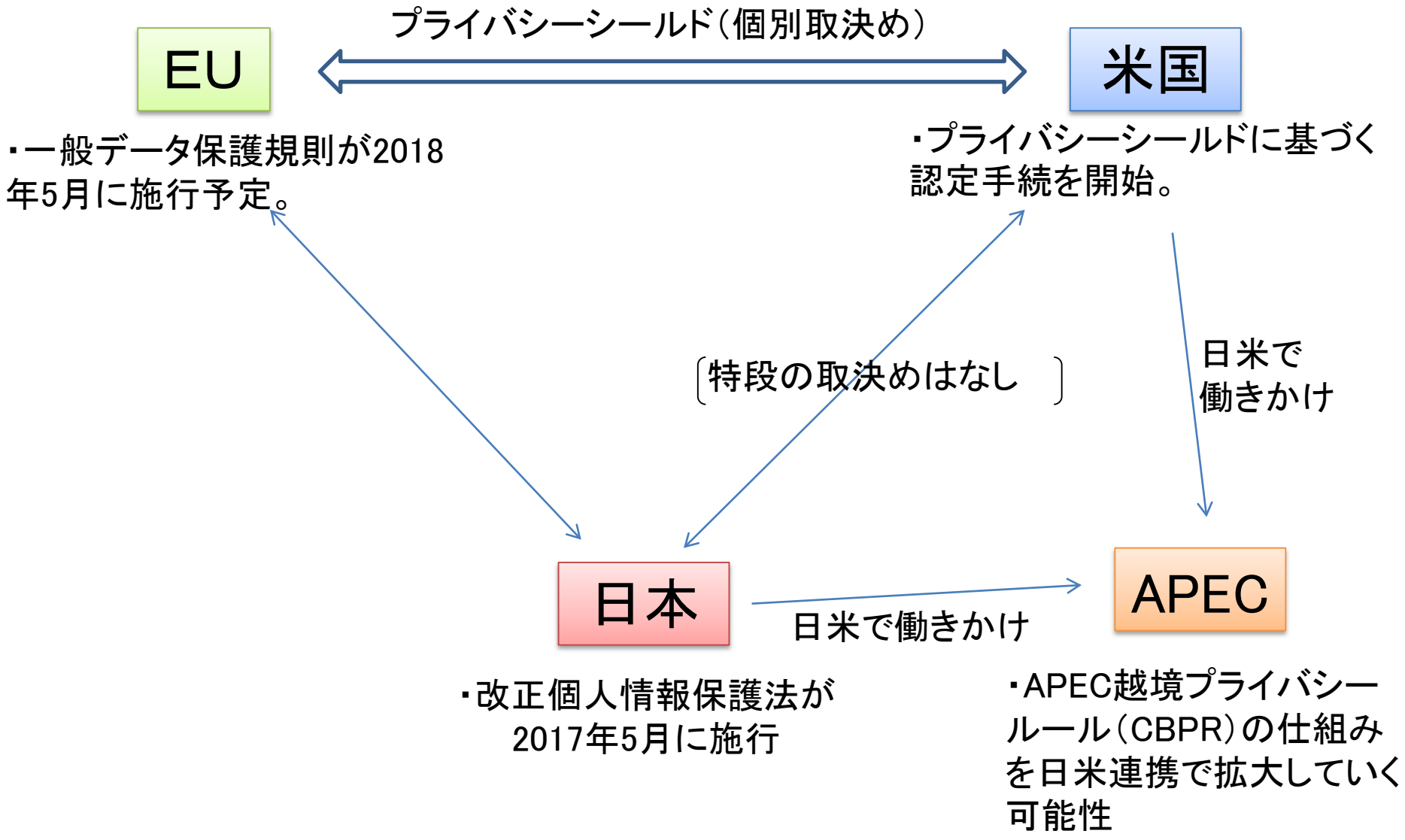
EU一般データ保護規則（GDPR）と
改正個人情報保護法について

平成29年9月27日

目次

- 個人データの越境流通に関する動向
- EU一般データ保護規則（GDPR）について
- 改正個人情報保護法について
- 日EU間の相互の円滑な個人データ移転の確保に向けた取組

個人データの越境流通に関する動向



EU一般データ保護規則（GDPR）について

EU一般データ保護規則の経緯

■ 2012年、ＥＵ（欧州連合）は約20年ぶりとなる個人データ保護基本法の見直しに着手。

■ EU法は、欧州委員会（執行機関）が原案を提案し、欧州議会（立法機関）・欧州理事会（立法機関：加盟国の集まり）が必要に応じて修正した上で合意する必要があり、2015年12月に三者協議を経て合意。2016年4月14日にＥＵ域内で適用されるデータ保護の統一ルールとして、ＥＵデータ保護指令に代わって採択され、同年5月4日に公布された。施行は2018年5月25日を予定している。

欧州議会案（2014）	欧州理事会案（2015）
１．域内統合	
● **ＥＵ法を各国に直接適用** （現行法は各国の国内法制化が必要）	● ＥＵ法を直接適用するが、各国の上乗せ規制を許容
２．個人の権利	
● 現行法上の権利を明確化。 ● **「忘れられる権利」**を創設。削除要求を受けた事業者は、自ら削除することに加え、**データが複製された先の第三者に対して通知し、当該第三者も削除を義務づけ**。 ● 個人データの漏えい時の**本人・当局への通知を義務づけ（「遅滞ない通知」）**	● 現行法上の権利を明確化。 ● 「忘れられる権利」については、削除要求を受けた事業者は、**費用対効果を勘案し、第三者に対して通知すればよい（第三者の削除義務は免除）**。 ● 漏えい時の通知については、**深刻なケースに限定し、当局へは72時間以内で可**。
３．事業者の義務	
● データ保護監督者の設置義務。 ● 法違反に対し、最大**1億ユーロ**か**世界売上の5%相当**（どちらか高額な方）の課徴金。	● データ保護監督者の設置義務。 ● 課徴金は、**100万ユーロ**か**世界売上の2%相当**。
４．グローバル対応	
● 域内向けにサービスを提供する場合、域外事業者に法適用することを明確化。 ● **既存の十分性認定はいったん失効**。 ● **第三国の判決等による情報開示を禁止**。	● 域外事業者のうち、**データを頻繁に取り扱わない者等に対する法適用を免除**。 ● **既存の十分性認定は維持。（認定のない第三国からの転送要求は拒否可能）**

【三者合意を受けた最終テキスト】

- **ＥＵ法を直接適用するが、各国の上乗せ規制を許容**

- **現行法上の権利を明確化。**
- **「忘れられる権利」を創設。削除要求を受けた事業者は、費用対効果・技術的可能性を勘案しつつ、第三者に対して通知しなければならない。**
- **漏えい時の通知については、深刻なケースに限定し、当局に72時間以内で通知しなければならない。**

- **データ保護監督者の設置義務。**
- **最大2,000万ユーロか世界売上の4%相当の制裁金（認証メカニズム、データ保護といった規則に違反する場合は最大1,000万ユーロか世界売り上げの2%相当）**

- **域外事業者のうち、データを頻繁に取り扱わない者等に対する法適用を免除。**
- **既存の十分性認定は維持するが、最低４年ごとの見直しを行う。**

ＥＵ一般データ保護規則（GDPR）

規則の概要

（１）　ＥＵ域内における規制の単一化・簡素化

① ＥＵ法令が全加盟国に同一に直接適用されるよう、国内法制化の不要な「規則」に変更。

② 複数の加盟国にまたがる事業者や事案を取り扱う場合、一の監督機関が主管として対処する制度の導入（ただし、他関係国の監督機関も意見を述べることが可能であり、意見が分かれた場合には各加盟国の監督機関の長で構成される欧州データ保護ボードにより決定。）

（２）　より強固な個人データ保護ルールの整備

① 「忘れられる権利」に関する規定の導入（第17条）（データ管理者は、ネット上での個人データへのリンクやコピー・複製された個人データについて、当該個人から削除要求があった場合、当該要求を（それらデータを扱う）第三者に対して通知しなければならない。）

② 「データ持ち運びの権利」を規定（第20条）（自らのデータをあるアプリケーションから別のアプリケーションに移転させることができる等の権利）

③ 「プライバシー・バイ・デザイン」原則の導入（第25条）（データ管理者は漏えいリスクに応じ、仮名化等の適切な技術的・組織的な措置を講じなければならない。）

④ データ漏えい時の通知義務（第33条）（監督機関に対しては72時間以内に通知、個人に対しては深刻な権利侵害を及ぼす可能性がある場合に遅滞なく通知）

⑤ 「データ保護職員」の任命義務（第37条）（データ管理者の主な事業が、「大規模な」個人データの定期的かつ体系的な監視を要する処理から構成される場合（＝データ処理事業者を除く中小事業者は免除）等）

⑥ 制裁金の引き上げ（第83条）（最大2,000万ユーロまたは全世界年間売上高の４％の制裁金（特定の規則に違反する場合は最大1,000万ユーロか世界売り上げの2%相当））

（３）　グローバルな課題への対応

① 域外事業者への適用（第3条）（ＥＵ域内の居住者に物品・サービスの提供またはＥＵ域内の居住者の行動の監視（monitoring）を行う域外事業者にも適用。また一定要件を満たす域外事業者はＥＵ域内に代理人を置くべき旨の規定（第27条）を導入）

② 十分性認定見直しメカニズムの導入（第45条）（既存の十分性認定について最低４年ごとの定期的な見直し）

データ保護規則に基づく主な越境データ移転の手段

十分性認定（第45条）

- 欧州委員会が認定するに当たり、法の支配、司法的救済、独立したデータ保護機関の存在等を考慮要素とする
- 既存の十分性認定について最低４年ごとの見直し

→ 国・地域全体の十分性認定

→ 特定分野の十分性認定

十分性認定がない場合
↓
適切な安全管理措置（第46条）

拘束的企業準則（第43条）(BCR)

- 整合性メカニズムに基づき監督機関から承認された拘束的企業準則（ＢＣＲ）に基づくデータ移転

標準契約条項(SCC)

- 欧州委員会が採択した標準契約条項に基づくデータ移転

行為規範（Code of Conduct）

- 拘束的かつ強制的なコミットメントが付与された、第41条に基づき監督機関より承認された行為規範に基づくデータ移転

認証メカニズム

- 拘束的かつ強制的なコミットメントが付与された、第42条に規定するＥＵ域内の認証機関によって運用されるデータ保護認証メカニズムに基づくデータ移転

適切な安全管理措置がない場合
↓
例外規定（第48条）

- データ主体からの同意取得
- データ主体との契約履行に必要な場合
- 公共の利益
- データ主体の重大な利益の保護　等