クラウドコンピューティングにおける個人情報保護
～越境データ移転を中心に～

2017年12月7日

（株）国際社会経済研究所
主幹研究員　小泉 雄介
y-koizumi@pd.jp.nec.com

報告者の略歴

〇小泉　雄介
株式会社 国際社会経済研究所　主幹研究員　http://www-i-ise-com.onenec.net/jp/about/researcher/koizumi.html

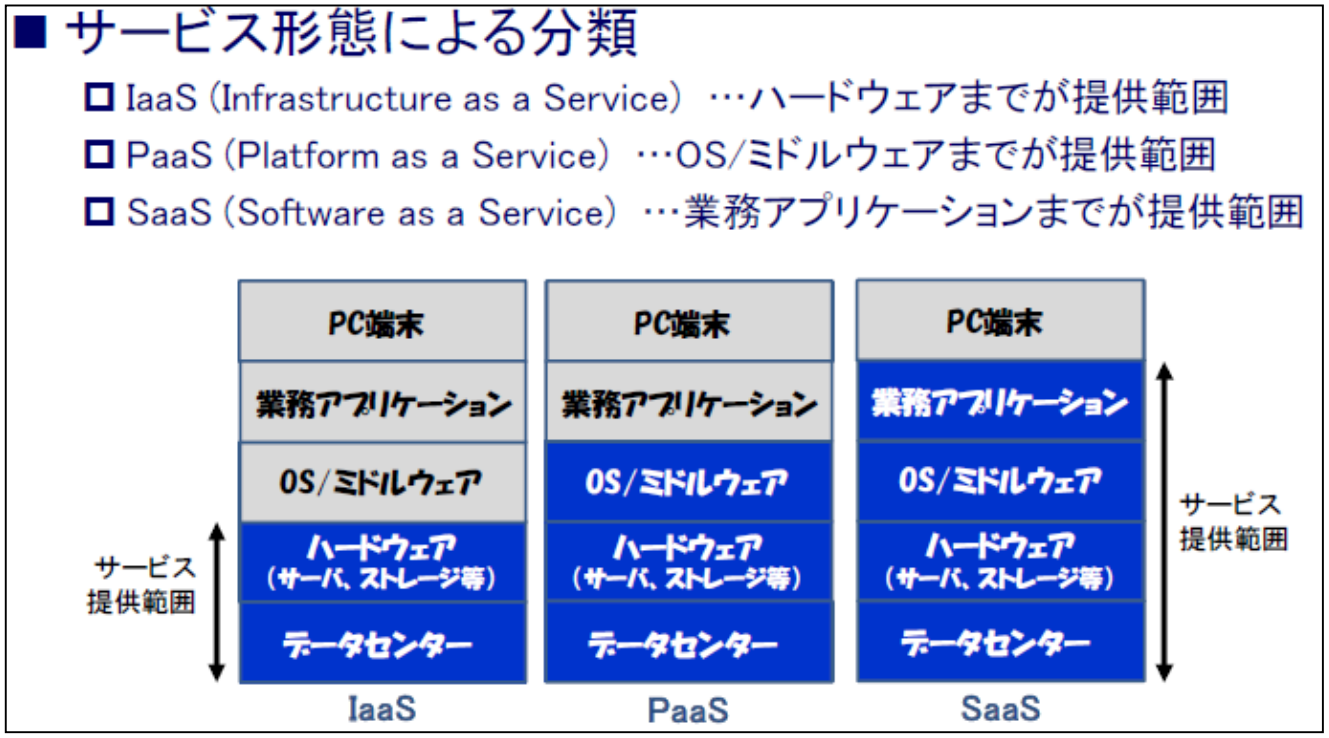
- 専門領域:
  - 個人情報保護/プライバシー、監視社会、電子政府（国民ID/マイナンバー制度）、途上国市場調査
- 略歴:
  - 1998年　（株）NEC総研入社
  - 2008年7月　日本電気（株）パブリックサービス推進本部に出向
  - 2010年7月　（株）国際社会経済研究所（旧NEC総研）に復帰
- 主な著書
  - 『国民ID　導入に向けた取り組み』（共著、NTT出版、2009年）
  - 『ブログ・SNS利用者の実像』（共著、NEC総研、2006年）
  - 『現代人のプライバシー』（共著、NEC総研、2005年）
  - 『経営戦略としての個人情報保護と対策』（共著、工業調査会、2002年）
- 主な論文・解説
  - 「ICT世界の潮流パートⅤ：諸外国における国民IDカードとeID」（日刊工業新聞2017年6月）
  - 「英国における監視カメラと顔認識の動向」（『画像ラボ』2017年3月号）
  - 「プライバシー影響評価（PIA）の海外動向と日本への応用」（『日本データ通信』2017年3月号）
  - 「EUデータ保護規則案の動向と個人データ越境移転」（『ITUジャーナル』2015年11月号）
  - 「マイナンバー制度とは」（日本経済新聞2013年4月7日「今を読み解く」に掲載）
  - 「EUデータ保護指令の改定と日本企業への影響」(『CIAJ Journal』2012年6月号)
  - 「国民ID制度の概要と海外の最新事情」（共著、『CIAJ Journal』2011年1月号）
  - 「オーストリアの電子IDカードと市民カード」（共著、『情報化研究』情報産業振興議員連盟、2008年）　等

1．クラウドコンピューティングにおける個人情報保護： 概要

クラウドサービスの分類

- IaaS（Infrastructure as a Service）:
  - CPU、メモリ、ストレージ、ネットワークなどのハードウェア資産をサービスとして提供するクラウドサービス。
- PaaS（Platform as a Service）:
  - オペレーティングシステムや実行環境をサービスとして提供するクラウドサービス。
- SaaS（Software as a Service）:
  - アプリケーションやデータベースをサービスとして提供するクラウドサービス。

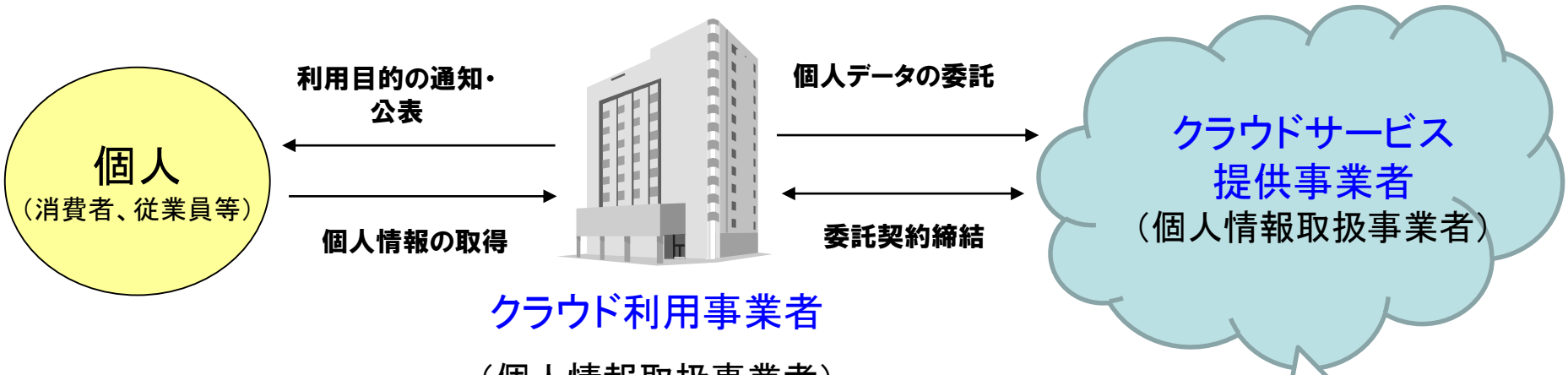
出典：経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」



出典：総務省資料

クラウドサービスにおける個人情報保護

※ 下記は、クラウドサービスの利用が個人情報保護法上の「委託」に当たる場合



【クラウド利用事業者の義務】
- 利用目的の特定
- 目的外利用の制限
- 適正な取得
- 利用目的の通知・公表
- 安全管理措置
- 委託先の監督
- 第三者提供の制限/外国の第三者への提供制限
- 開示/訂正/利用停止等
- 保有個人データに関する事項の公表　等

【クラウドサービス提供事業者の義務】
- 利用目的の特定
- 目的外利用の制限
- 適正な取得
- 利用目的の通知・公表
- 安全管理措置
- 委託先の監督（再委託をする場合）
- 第三者提供の制限　等

改正個人情報保護法との関連(1/2)

- 個人情報保護法ガイドライン・Q&Aでは第三者提供・委託の文脈でクラウドに関する言及がなされている。

① クラウドサービスの利用が、第三者提供にも委託にも当たらない場合

- クラウドサービス提供事業者において個人データを取り扱わないこととなっている場合、個人データの第三者提供や委託には該当しない。(個情法Q&A 5-33)
- 「クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合」とは、契約条項に当該事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等。(個情法Q&A 5-33)
  - ただし、クラウド利用事業者は、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある。(個情法Q&A 5-34)

② クラウドサービスの利用が、委託に当たる場合

- クラウドサービス提供事業者が(顧客企業の利用目的の達成に必要な範囲内で)個人データを取り扱う場合。
- 委託元企業には「委託先監督義務」が発生。
  - 適切な委託先の選定　・委託契約の締結　・委託先における個人データ取扱状況の把握
- なお、委託に当たっては「第三者提供時の確認義務」は適用されない。

③ (委託ではない)第三者提供に当たる場合

- クラウドサービス提供事業者が(顧客企業の利用目的の達成に必要な範囲を超えて)独自の利用目的で利用する場合。
- 「本人の同意」「第三者提供時の確認」等の義務が発生。

【ご参考】

- 個人情報保護法ガイドライン通則編
  - 「「個人データの取扱いの委託」とは、契約の形態・種類を問わず、個人情報取扱事業者が他の者に個人データの取扱いを行わせることをいう。具体的には、個人データの入力（本人からの取得を含む）、編集、分析、出力等の処理を行うことを委託すること等が想定される。」
- 個人情報保護法ガイドラインQ&A
  - （Q&A 5-33）「クラウドサービスには多種多様な形態がありますが、クラウドサービスの利用が、本人の同意が必要な第三者提供（法第23 条第1項）又は委託（法第23 条第5項第1号）に該当するかどうかは、保存している電子データに個人データが含まれているかどうかではなく、クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかどうかが判断の基準となります。当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合には、当該個人情報取扱事業者は個人データを提供したことにはならないため、「本人の同意」を得る必要はありません。また、上述の場合は、個人データを提供したことにならないため、「個人データの取扱いの全部又は一部を委託することに伴って・・・提供される場合」（法第23 条第5項第1号）にも該当せず、法第22 条に基づきクラウドサービス事業者を監督する義務はありません。・・・当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合とは、契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等が考えられます。」
  - （Q&A 5-34）「クラウドサービスの利用が、法第23 条の「提供」に該当しない場合、法第22 条に基づく委託先の監督義務は課されませんが（Q5-33 参照）、クラウドサービスを利用する事業者は、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要があります。」

改正個人情報保護法との関連(2/2)

- 匿名加工情報との関係
  - (1) クラウドサービス提供事業者Bが、クラウド利用事業者Aの委託を受けて、匿名加工情報を作成する場合
    - 匿名加工情報の作成はAとBが共同で行っていると解される。そのため、保護法第36条(匿名加工情報の作成等)の規定はAとBの双方に課される。(個情法Q&A 11-20)
    - 改正個人情報保護法第36条
      - 基準に従った適正な加工　ー加工方法等漏洩の防止　ー作成時の公表
      - 提供時の公表・明示　ー識別禁止　ー安全管理措置等(努力義務)
  - (2) クラウドサービス提供事業者Bが、クラウド利用事業者Aの委託を受けて、匿名加工情報の分析を行う場合
    - 匿名加工情報の第三者提供については「委託」等の例外規定がない。
    - 上記の場合、Aには匿名加工情報の「第三者提供時」の義務が発生？　それとも、(Q&A 11-20からの類推で)匿名加工情報の分析をAとBが共同で行っていると解される？
  - (3) クラウドサービス提供事業者Bが、クラウド利用事業者Aから預かった個人データを元に、自ら匿名加工情報を作成する場合
    - クラウド提供事業者Bによる独自目的での利用のため、事業者AからBへの移動は個人データの第三者提供に当たる。そのため、Aにおける本人同意等が必要と考えられる。

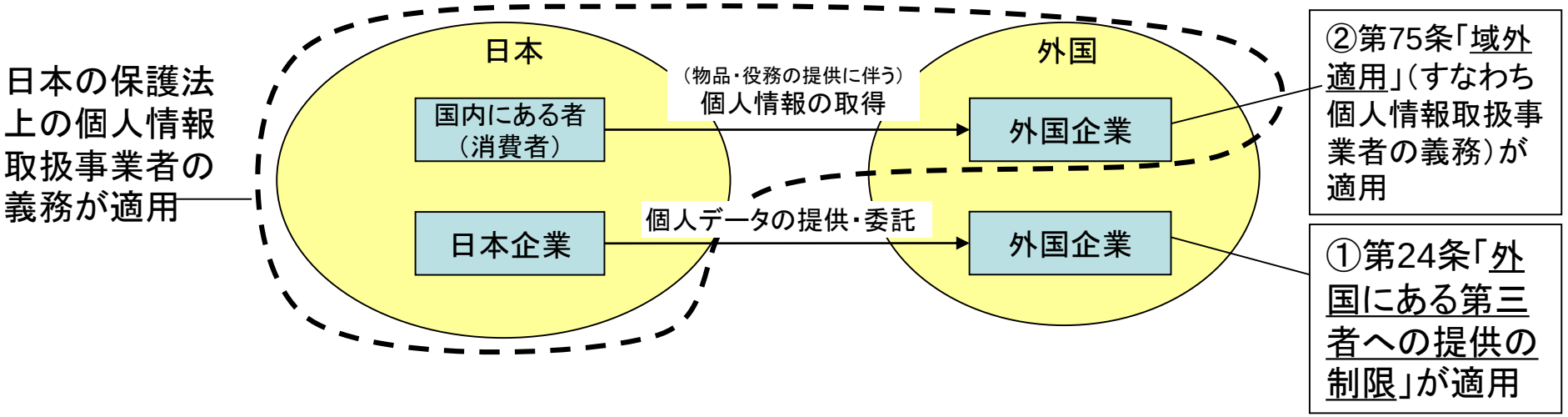
【ご参考】個人情報保護法ガイドラインQ&A

- 「(Q&A 11-20)個人情報を提供して匿名加工情報の作成を委託した場合には、匿名加工情報の作成は委託先事業者において行われることになりますが、匿名加工情報の作成は委託元事業者と委託先事業者が共同で行っているものと解されますので、法第36 条の規定は委託元事業者と委託先事業者の双方に課せられると考えられます。」

２．日本から諸外国への越境データ移転

日本から外国への個人データ移転

- 諸外国へのデータ移転に関連し、改正個人情報保護法で新設された条項は下記3つ
  - 外国にある第三者への提供の制限（第24条）①
  - 域外適用（第75条）②
  - 外国執行当局への情報提供（第78条）



外国にある第三者への提供の制限

- 個人情報取扱事業者が外国の第三者に個人データを提供（オプトアウト、委託、事業承継、共同利用を含む）できるのは、以下の場合に限られる。（第24条）

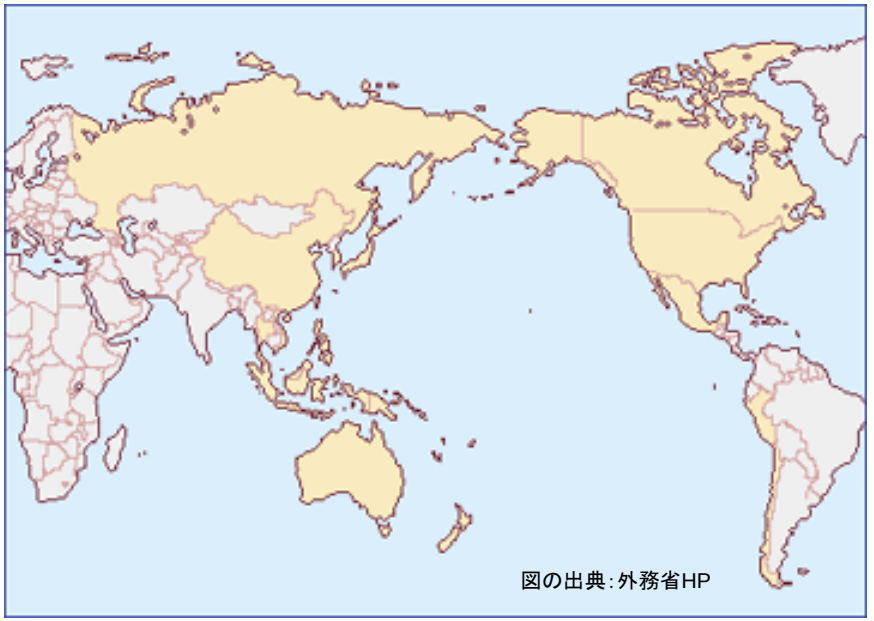
  - （1）当該国が、個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として、個人情報保護委員会の規則で定める国の場合

  - （2）第三者が、個人情報保護委員会の規則で定める基準に適合する体制を整備している場合
    - 事例1）外国にある事業者に個人データの取扱いを委託するケース
      → 委託元と委託先の間で適切な契約、確認書、覚書等を取り交わしていること　又は、
      → 委託元の日本企業がAPECの越境プライバシールール（CBPR）の認証を得ていること　又は、
      → 委託先の外国事業者がAPECの越境プライバシールール（CBPR）の認証を得ていること
    - 事例2）同一の企業グループ内で個人データを移転するケース
      → 提供元及び提供先に共通して適用される内規、プライバシーポリシーが適切であること　等

  - （3）外国にある第三者への提供を認める旨の本人同意があるか、以下の場合
    - 法令に基づく場合
    - 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき
    - 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき
    - 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき

【ご参考】 APEC越境プライバシールール（CBPR）

- 越境プライバシールール（CBPR）
  - **APEC内で、企業・組織が国境を越えて個人データを移転するためのルール**。
  - 2013年6月に日本が参加申請し、2014年4月に承認（米国、メキシコに続き3カ国目）。15年4月にカナダ承認。17年6月に韓国承認。現時点で米・メ・日・加・韓の5か国。
  - 検討経緯
    - 2006年からAPECのECSG（電子商取引運営グループ）において検討を開始。2007年に閣僚会合の承認によって設置された「APECデータプライバシー・パスファインダー」において、開発が進められた。
    - 2011年11月のAPEC閣僚会合及び首脳会議において取りまとめられ、公表された。



  - **企業の越境個人データに係るプライバシーポリシーとプライバシー・プラクティスに対して、APECが認定した各国の責任団体（Accountability Agent：AA）が第三者認証を行う**。
    - 責任団体（AA）は公的機関でも民間団体でも良い。
    - 現時点でAAの認定を受けているのは米国のTRUSTeと、日本のJIPDEC。
  - **ポリシーに対するコミットメントに違反した企業に対しては、各国のプライバシー執行機関（いわゆるDPA）が法執行を行う**。このプライバシー執行機関はCBPRの要件と整合的な国内法令の下で法執行を行う能力が必要。また、参加国のプライバシー執行機関の少なくとも1つは、下記のCPEAに参加していることが必要。
- 越境プライバシー執行のための協力取決め（CPEA）（2010年発効）
  - APEC内で、各国のプライバシー執行機関のネットワークを通じて、プライバシー法令の国境を越えた執行協力を行うための取決め。
  - これまで、オーストラリア、カナダ、中国香港、ニュージーランド、米国、日本の執行機関が参加。

域外適用、外国執行当局への情報提供

- 個人情報保護法改正法案 第75条（適用範囲）
  - 「第15条（※利用目的の特定）、第16条（※利用目的による制限）、第18条（※取得に際しての利用目的の通知等）（第二項を除く。）、第19条から第25条まで（※データ内容の正確性の確保等、安全管理措置、従業者の監督、委託先の監督、第三者提供の制限、外国にある第三者への提供の制限、第三者提供に係る記録の作成等）、第27条から第36条まで、第41条、第42条第1項、第43条及び次条の規定は、国内にある者に対する物品又は役務の提供に関連してその者を本人とする個人情報を取得した個人情報取扱事業者が、外国において当該個人情報又は当該個人情報を用いて作成した匿名加工情報を取り扱う場合についても、適用する。」

- 個人情報保護法改正法案 第78条（外国執行当局への情報提供）
  - 「委員会は、この法律に相当する外国の法令を執行する外国の当局（以下この条において「外国執行当局」という。）に対し、その職務（この法律に規定する委員会の職務に相当するものに限る。次項において同じ。）の遂行に資すると認める情報の提供を行うことができる。
  - ２ 前項の規定による情報の提供については、当該情報が当該外国執行当局の職務の遂行以外に使用されず、かつ、次項の規定による同意がなければ外国の刑事事件の捜査（その対象たる犯罪事実が特定された後のものに限る。）又は審判（同項において「捜査等」という。）に使用されないよう適切な措置がとられなければならない。
  - ３（略） ４（略）」

外国の事業者への個人データ移転について（1/2）

- 事例：
  - ある日本企業Aが外国企業Bのクラウドサービスに、個人データを含むデータの分析等を委託。外国企業Bは日本国外で個人情報を取り扱う場合。
- この場合、日本企業から外国企業への個人データの取扱いの委託に当たるため、第24条の「外国にある第三者への提供の制限」が適用される。
  - 日本企業A（委託元）には「委託先監督義務」が発生。
    - 適切な委託先の選定
    - 委託契約の締結
    - 委託先における個人データ取扱状況の把握
  - 外国企業B（委託先）は第24条（外国にある第三者への提供の制限）の要件を満たす必要。
    - 個人情報保護委員会規則で定める国にある企業　or
    - 個人情報保護委員会規則で定める基準に適合する体制を整備している企業　等
- 国外にデータがある限り、外国企業Bには、（第24条を除き）日本の個人情報保護法は適用されない。
  - もし外国企業Bが利用規約で、準拠法を外国法と規定していて、Bが（日本の個人情報保護法違反には当たるが）外国法の違反には当たらない行為を行った場合、Bを個人情報保護法で罰することはできない。

※ なお、前述のように、外国企業Bにおいて個人データを取り扱わないこととなっている場合には、委託（や提供）に当たらず、第24条は適用されない。

外国の事業者への個人データ移転について(2/2)

- 事例:
  - 日本の消費者Cが外国企業Dのソーシャルネットサービスの会員となり、個人情報を提供。外国企業Dは日本国外で個人情報を取り扱う場合。

- この場合、外国企業は日本の消費者から個人情報を直接取得しているため、(第24条ではなく)第75条の域外適用が適用される。
  - 外国企業Dには、第75条に挙げられた個人情報取扱事業者の義務が発生。
- なお、消費者Cと外国企業Dの間で係争が起こった場合の準拠法は、外国企業Dの設定する利用規約に依存する(例えばカリフォルニア州法など)。
  - ただし、個人情報保護法違反に当たる場合(適切な安全管理措置を講じていない場合等)には、個人情報保護委員会がDに対して助言、勧告等を行うことができる。
  - 助言や勧告で改善が図られずに更なる強制力を行使をする必要性が生じた場合には、外国の執行当局に情報提供(第78条)を行い、執行協力を求める。

日本国内へのデータ保存が要求されるケース

- 強制力はないが、ガイドラインや政府報告書等において、国内へのコンピュータ設備設置が要求されているケースがある。

- 医療情報：
  - 「医療情報を受託管理する情報処理事業者向けガイドライン」（経済産業省、2012年）
    - 医療情報を受託管理する情報処理事業者を対象に、安全管理上の要求事項を記述したもの。
    - 「法令により作成や保存が定められている文書を含む場合には、医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実とすることが必要である。」
      - 診療録は医師法により5年間の保存義務あり。
- 自治体関連情報：
  - 「自治体クラウド推進本部 有識者懇談会とりまとめ」（総務省、2011年）
    - 「・・・SLA等を確実に担保するためには、契約の規定でデータセンターの設置場所やアクセス区域を国内に限定する必要がある。また、民事裁判管轄・準拠法についてもサービス提供契約に特約が置かれることが一般的であるが、国内でなければ事実上の限界が生じる場合がある。」
  - 「自治体クラウド開発実証に係る標準仕様書」（地方自治情報センター、2010年度）
    - 「自治体クラウドのサービスを提供する場合、サービス提供者は、その取り扱う情報の重要性・機密性から日本国内法が適用される国内にデータセンターを設置する必要がある。」

３．諸外国から日本への越境データ移転

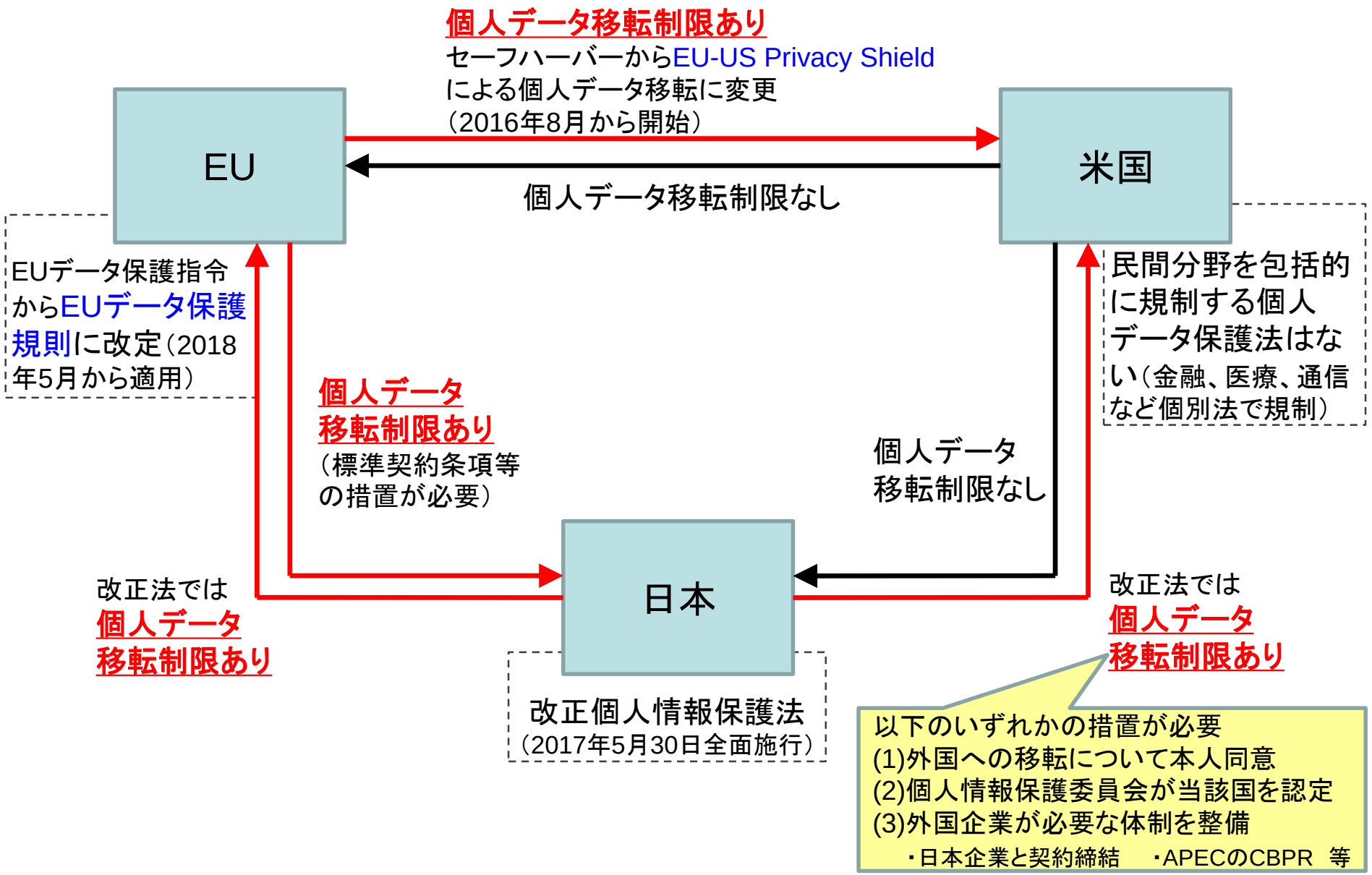
第三国(外国)への個人データ移転制限のある諸国

- EU
  - EUデータ保護指令／一般データ保護規則(GDPR)における第三国移転条項

- アジア諸国(EUと同様な第三国移転条項がある国)
  - シンガポール、マレーシア、台湾、香港　等
  - 日本(改正個人情報保護法)

- データローカライゼーション(相手国の個人情報保護レベルに関わらず移転を禁じる)
  - **ロシア**:2014年7月成立(2016年9月施行)の法律(No.242-FZ)においてロシア市民の個人データはロシア国内のデータベースに保存することが義務付けられた。
  - **中国**:2016年11月成立(2017年6月施行)のサイバーセキュリティ法において、ネットワーク運営者に対して国内で取得された個人情報と重要データの国内保存義務を規定。これらのデータを国外に持ち出す場合には、本人同意およびセキュリティ評価が必要。
  - **ブラジル**:NSAスノーデン事件を受けて同様な条項を含む法案を審議していたが、2014年4月に可決された法案ではこの条項は削除された。
  - EU加盟国でもイタリア、ギリシャはデータローカライゼーション政策を取っているという。

日米欧データ移転の全体像



EU一般データ保護規則(GDPR)の主要スケジュール

● これまでの経緯と今後のスケジュール

- (1995年10月　EUデータ保護指令の採択)
- 2012年1月　欧州委員会による**EUデータ保護規則案の公表**
- 2016年4月14日　**欧州議会で正式採択**　・同年5月4日　EU官報で公布
- 2016年～17年:　準備期間
  - 諮問機関(EU指令第29条作業部会)によるガイドラインの作成
  - 既に採択されたガイドライン
    - データポータビリティの権利に関するガイドライン(WP242)(2017年4月5日)
    - データ保護オフィサー(DPO)に関するガイドライン(WP243)(2017年4月5日)
    - 主たる監督機関に関するガイドライン(WP244)(2017年4月5日)
    - DPIA(データ保護影響評価)に関するガイドライン(WP248)(2017年10月4日)
    - 課徴金に関するガイドライン(WP253)(2017年10月3日)
  - パブコメに付されている(11/28まで)ガイドライン案
    - データ侵害通知に関するガイドライン案(WP250)
    - 自動化された意思決定とプロファイリングに関するガイドライン案(WP251)
  - 今後予定されているガイドライン
    - 同意、透明性、認証、データ移転に関するガイドライン
- 2018年5月25日:　**新規則のEU加盟国(+EEA加盟国)への直接適用**(application)

EU一般データ保護規則(GDPR)の概要

個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州連合理事会規則(GDPR)
(2016年4月採択、2018年5月適用)

EU+EEA加盟国に直接適用

●EU加盟国(2017年12月現在)
- ベルギー
- ドイツ
- フランス
- イタリア
- ルクセンブルク
- オランダ
- デンマーク
- イギリス
- アイルランド
- ギリシャ
- スペイン
- ポルトガル
- オーストリア
- フィンランド
- スウェーデン
- キプロス
- チェコ
- エストニア
- ハンガリー
- ラトビア
- リトアニア
- マルタ
- ポーランド
- スロバキア
- スロベニア
- ブルガリア
- ルーマニア
- クロアチア

計28カ国

●EEA加盟国
(2017年12月現在、EU加盟国以外)
- アイスランド
- リヒテンシュタイン
- ノルウェー

合計31カ国

EU+EEA

A国

- 公正かつ適法な利用
- 利用目的の明確化
- 個人データの正確性
- 本人同意の上での取得・利用
- 特定カテゴリーの個人データの利用制限
- セキュリティ対策
- その他

公共機関・民間企業

以下の事項を本人に通知
- 管理者、データ保護オフィサー
- 個人データの利用目的
- 個人データの提供先
- 保存期間
- アクセス権、訂正・消去権
- その他

- 独立的な監督機関の設置
- 課徴金

監督機関

- 個人データへのアクセス権、訂正・消去する権利等の保証

個人

域内での個人データの自由な移転は認める

B国

C国

○第三国移転条項

第三国等が個人データに関する十分なレベルの保護を保証する場合に移転を許可(第45条)

その他、適切な安全管理措置に従った移転(第46条)や例外規定(第49条)あり

日本

米国

(出典:国際社会経済研究所)

GDPRの日本企業への影響

日本企業への影響は、以下に分類できる。

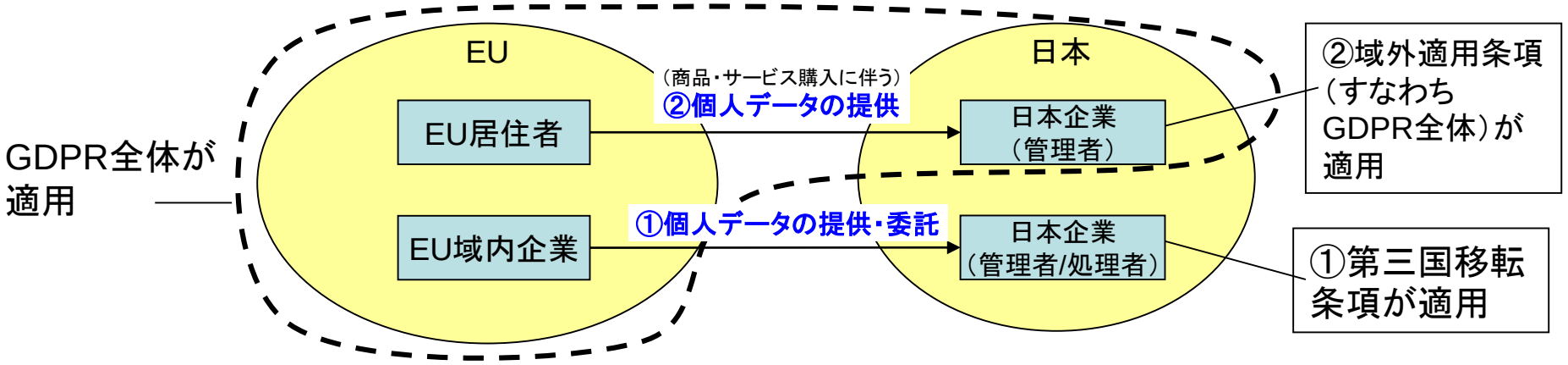
（1）EU域外企業（日本企業等）に対する影響

①EUからのデータ移転　→（GDPRの）第三国移転条項が適用される

②EU域外企業への域外適用　→GDPR全体が適用される（課徴金含む）

（2）EU域内企業（日本企業の現地法人等）に対する影響

→GDPR全体が適用される（課徴金含む）



EUから第三国への個人データ移転方法（GDPR）

- 下記の場合に**EU域内の管理者から第三国の管理者（又は処理者）へのデータ移転**が可能。

① **十分性認定**：欧州委員会が十分なレベルの個人データ保護を保証していると認定した国や地域等

- スイス、カナダ、アルゼンチン、イスラエル、アンドラ、ガーンジー、マン島、ジャージー（左記3つは英国の王室属領）、フェロー諸島（デンマークの自治領）、ウルグアイ、ニュージーランド。
- 認定に当たっては「個人データの第三国移転：EUデータ保護指令第25条及び第26条の適用（WP12 5025/98）」に基づいて評価。

② 米国については特例として、**セーフハーバー・スキーム（2015年に無効判決、2016年よりPrivacy Shield）**

- セーフハーバー7原則を遵守すると自己宣言する米国企業については、欧州域内からの個人データ移転を認めるもの（セーフハーバー決定）。
  - 形式上は「十分性認定」の1つとされている。
- 2015年に欧州司法裁判所により無効判決を受け、2016年より後継のPrivacy Shieldが開始。

③ 十分性認定がない場合は、以下の「適切な安全管理措置」が必要

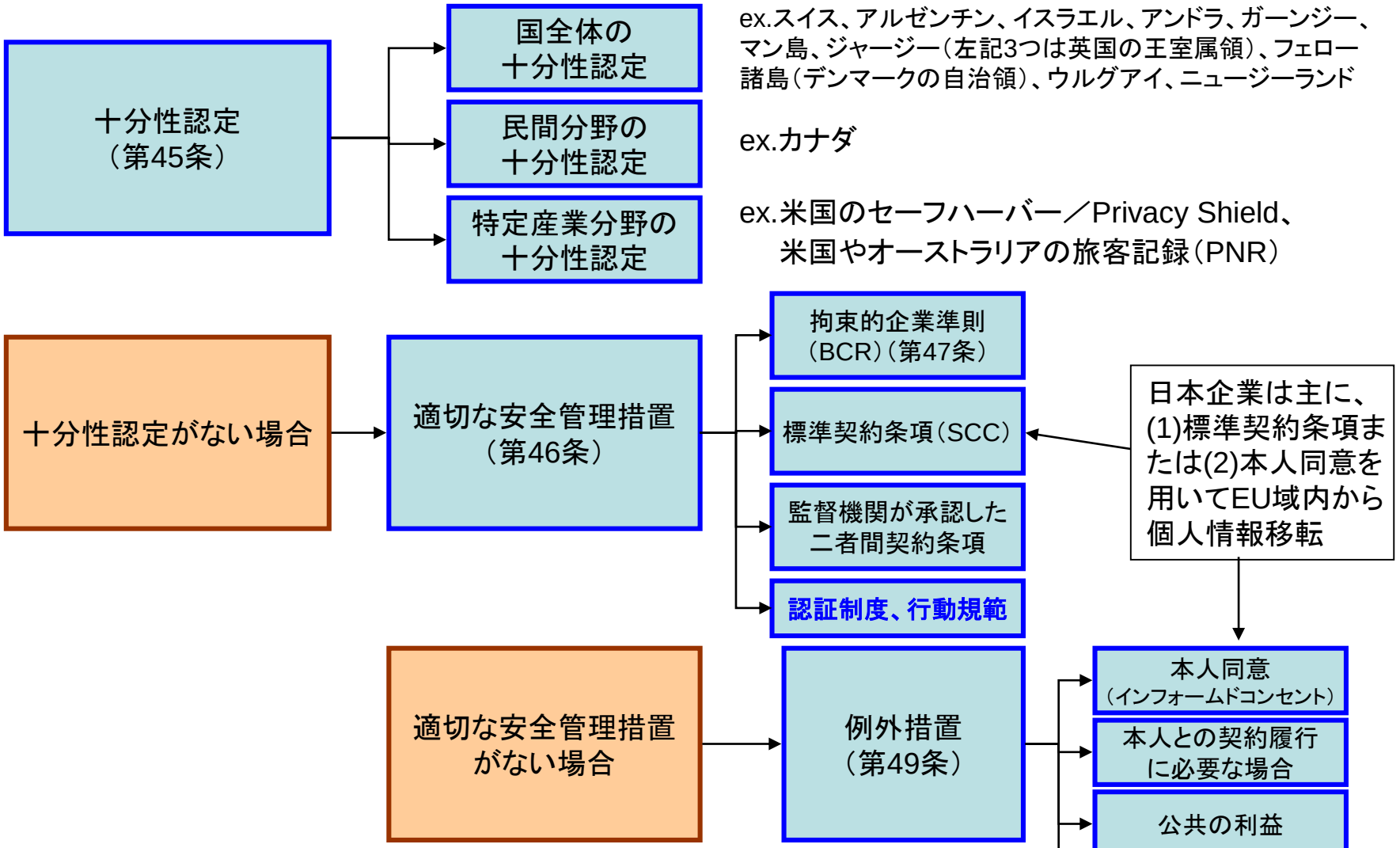
- **標準契約条項（Standard Contractual Clauses：SCC）**（第26条第4項）：
  欧州委員会が策定。2001年様式、2004年様式、2010年様式がある。
- **拘束的企業準則（Binding Corporate Rules：BCR）**（第26条第2項）：
  多国籍企業、企業グループ内部での個人データ移転を対象。監督機関が承認。
- さらにGDPRでは、「認証制度」、「行動規範」による移転手段が追加された。

④十分性認定も、適切な安全管理措置もない場合には、以下の例外措置がある

- **本人が明確な同意を与えている場合**や、データ主体及び管理者間の契約の履行のために必要な場合等（第26条第1項）

→日本企業は主に、(1)標準契約条項または(2)本人同意を用いてEU域内から個人情報移転

EUから第三国への個人データ移転方法（GDPR）



(1)標準契約条項の問題点：　相手企業ごと・案件ごとに締結が必要、弁護士費用等のコスト、監督機関の承認に時間がかかる、EU企業に日本企業側のデータ取扱いに関する責任発生など

(2)本人同意の問題点：　消費者全員の同意取得は困難、従業員データでも国により労組の同意が必要

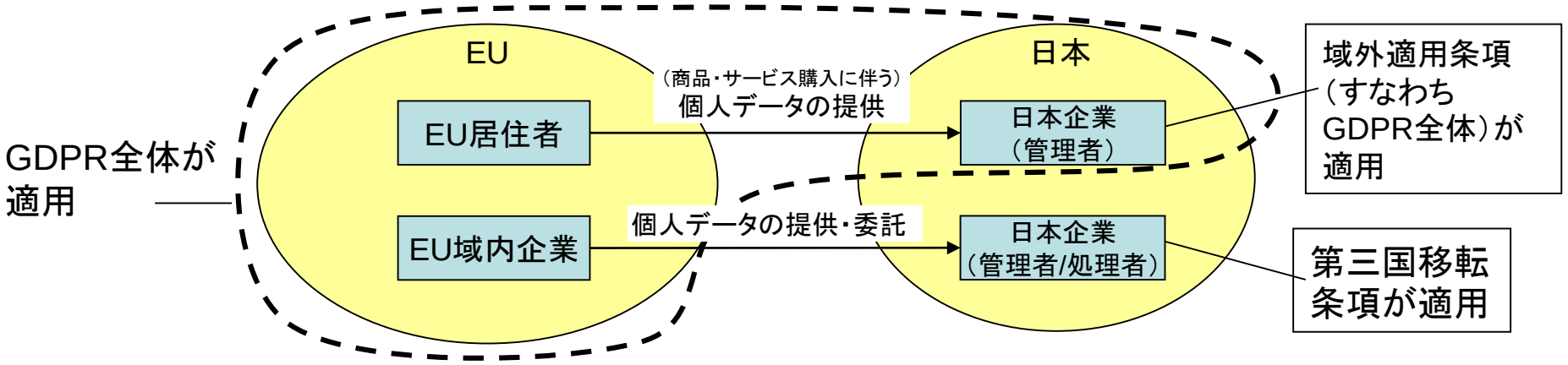
GDPRの域外適用

○ EUデータ保護指令の規定

- 管理者がEU域内に事業所を持つか、EU域内の設備でデータ処理を行う場合のみEU指令の対象となる。

○ GDPRでの改定内容

- **EU域外企業であっても、以下の場合、EU居住者のデータを取扱う管理者に対してはGDPRが適用される**（第3条第2項）。
  - ① EU居住者に商品やサービスを提供している場合
  - ② EU居住者の個人の行動をモニターしている場合
- 具体的には、国内のオンラインサービス事業者、パーソナルクラウド事業者、オンライン広告事業者、スマートフォンアプリ事業者等が対象になりうる。



（出典：国際社会経済研究所）

GDPR／EU指令におけるクラウドサービスの位置付け（１/２）

- GDPR／EU指令では、欧州企業Aがクラウドサービス提供事業者Bに、個人データを単に預ける行為も、個人データ処理の委託とみなされる

（GDPR／EU指令の用語で言うと、クラウド提供事業者Bは「処理者」に当たる）。

- 欧州企業（日本企業の欧州現地法人等）が取得した個人データを、EU域外のクラウドサービス提供事業者に預ける場合、個人データ処理の委託とみなされ、EU域外事業者への「移転」に該当するため、SCC締結・BCR承認など第三国移転のために必要な措置を取らないといけない。

GDPR／EU指令におけるクラウドサービスの位置付け（2/2）

- EU指令第29条作業部会「クラウドコンピューティングに関する意見書」（2012年）（WP196）
  - 「クラウド提供事業者が顧客企業のためにアクトし（act on behalf of）、手段とプラットフォームを提供しているならば、当該クラウド提供事業者は「処理者」とみなされる。」
  - また、クラウドサービスにおける「処理者」の類型として、「SaaS/PaaS/IaaS」が挙げられている。

- GDPR第4条2項（EUデータ保護指令でも同様の規定となっている）
  - 「処理者」（processor）とは、管理者のために（on behalf of）個人データの処理（processing）を行う自然人、法人、公的機関、行政機関又はその他の団体をいう。
  - 「処理」（processing）とは、自動的な手段であるか否かにかかわらず、個人データ又は個人データの集合に対して行われるあらゆる作業又は一連の作業をいう。この作業は、取得、記録、編集、構造化、保存（storage）、修正又は変更、復旧、参照、利用、移転による開示、周知又はその他周知を可能なものにすること、整列又は結合、制限、消去又は破壊することをいう。

※ EU指令第29条作業部会「管理者と処理者の概念に関する意見書」（2010年）（WP169）
  - 事例16で、Webホスティングサービス事業者を「原則として個人データの処理者である」としている。

EU・日本間の越境データ移転： 最近の状況

- EUから日本への個人データ移転について、現状では不自由な状況にあるが、日本政府は日EU間の「相互の円滑なデータ移転を図る枠組みの構築」を目指して2016年からEU側と協力対話を続けている。
- 2017年7月3日には、個人情報保護委員会と欧州委員会が協力対話を行い、日EU間の相互の円滑な個人データ移転を図る枠組みとして、相互に双方の保護水準が十分であることを認める相互認証を目指し、2018年の早い時期に成果を出すことを目標にお互い努力していくことについて確認。
- 2017年10月末～11月初めには欧州議会LIBE（市民の自由・司法・内務委員会）の議員団8名が来日し、日本の産業界等における個人情報保護の実態についてヒアリング調査を実施。

【ご参考】EU-US Privacy Shield

- 2013年6月にNSA元職員スノーデン氏の証言により米国PRISMの存在が発覚し、セーフハーバーの有効性が揺らぐ。
  - PRISM：米国政府による米国インターネット企業からの個人データ収集プログラム。FISA（外国情報監視法）の授権範囲を越えてデータ収集していた疑い。
- 2015年10月の欧州司法裁判所による「米欧セーフハーバー無効判決」を受け、米欧間で新たな枠組みを交渉。2016年2月にPrivacy Shieldに大筋合意。同年8月から運用開始（商務省サイトで受付）。

- 「EU-US Privacy Shield」では、セーフハーバーと同等な内容に加え、以下の3点が追加。

  ①米国企業に対する執行強化
  - 商務省が企業の遵守状況を定期的にモニター

  ②米国政府に対する規制強化
  - 米国政府はEUから移転された個人データに対する無差別な大量監視を行わない
  - 米国政府による国家安全保障目的でのデータアクセスに対するオンブズパーソン新設
  - 米国政府に対する米欧共同での年次レビュー

  ③EU市民に対する有効な権利保護
  - 米国企業のEU市民からの苦情への一定期間内の回答義務
  - EU市民による自国DPA（データ保護監督機関）への苦情申立、DPAから米国機関への苦情照会 等

- 2017年9月に第1回共同レビュー実施。
  - 欧州委員会は米国政府に対し、FISA（外国情報監視法）におけるプライバシー保護強化、商務省による能動的モニター、正式なオンブズパーソン指名などを要求。

【ご参考】マイクロソフト vs. 米国司法省

- 2016年7月の米国連邦第2巡回区控訴裁判所の判決
  - 「米国の連邦または州の法執行機関が従来の捜査令状を使用して米国外のデータセンターに保存されている外国人の電子メールを取得することはできない」とするマイクロソフト社の主張を認める。
  - 「クラウドコンピューティングなどが登場する数十年前に制定された法律である電子通信プライバシー法 (ECPA) は、国境を越えて他国の中に及ぶことは意図していなかった」とマイクロソフト社は主張。
- これに対し、2017年10月に連邦最高裁は司法省の上訴を受理。
- マイクロソフト社の考え方
  - 1. 米国の法令を国境を越えて他国に適用するには、その法律を通過させたときの議会がそのことを意図していたことを明確にする必要がある、という基本的な前提を満たしていない。
  - 2. 捜査令状を支持する政府の主張の前提となっている、顧客の電子メールは顧客ではなくプロバイダーの所有物であるとする考え方には同意できない。そのように考えると、人々はオンラインのものについて権利がないことになる。
  - 3. ヨーロッパやその他世界各国の法律と矛盾する。各国の法律は、プライバシーの権利を保護することを目的とし、個人データの第三国への開示や移動を制限している。
  - 4. あらゆる人の電子メールを危険にさらすことになる。米国政府が米国外の電子メールを取得する令状を一方的に使用するのであれば、外国政府が米国内の電子メールを一方的に取得しようとする場合、それを阻止できるだろうか。各国が外国政府によるハッキングを深刻に懸念するなか、司法省の解釈はそのようなことを許す入り口を作ることになる。
- （出典：日本マイクロソフト https://www.microsoft.com/ja-jp/mscorp/legal/issues-ja20171016.aspx）