日本企業のベルギー子会社・ベルギー支店が取っておくべきEU一般データ保護規則へのコンプライアンス対応

ベルギー日本人会商工委員会2016年度第3回ビジネスセミナー
（2016年12月12日、ブリュッセル）

ウィルマーヘイル法律事務所
ブリュッセルオフィス
シニアアソシエイト
弁護士　杉本 武重
+ 32 2 285 49 69
Takeshige.Sugimoto@WilmerHale.com

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

目次

I. GDPRコンプライアンス対応における重要論点

I-1. GDPRコンプライアンス対応における重要論点: 基本概念

指令から一般データ保護規則へ

- GDPR（General Data Protection Regulation: 一般データ保護規則）は、**個人データを処理**し、個人データを欧州経済領域(European Economic Area。「**EEA**」(EU加盟国28ヶ国＋アイスランド、リヒテンシュタイン、ノルウェー) から第三国に**移転する**ために満たすべき法的要件を規定している。
- GDPRは「EU基本権憲章」というEU法体系の根幹をなす法において保障されている、個人データの保護に対する権利という基本的人権の保護を目的とした法律である。GDPRは、基本的人権という「EU基本権憲章」上の重要な価値を保障するため、違反に対し厳しい行政罰を定める。

EUデータ保護指令 95/46/EC

(2018年5月24日まで)

▪データ保護法は加盟国毎に大きく異なる。

▪**第29条作業部会**(加盟国各国のデータ保護機関の代表、欧州委員会司法総局データ保護課の代表、欧州データ保護監察機関の代表によって構成される)**(「作業部会」)**は、特定の問題に関して共通の解釈と分析を提供することにより、EU加盟国のデータ保護法の解釈にある程度の調和をもたらす。

- 限られた法的執行及び小さな制裁

GDPR

(2018年5月25日から適用開始)

▪加盟国各国のデータ保護法は廃止（但し、一定の事項（雇用、ジャーナリズム、研究等）については加盟国が個別のルールを立法することができるとされていることに留意が必要）

▪指令よりも範囲を拡大

▪調和を増大させる。

▪企業に対して新たな説明責任を導入する。

▪個人の権利を強化する。

▪制裁と執行を増大させる。

- 作業部会は**欧州データ保護会議** (European Data Protection Board. 「**EDPB**」)へと改組

制裁金の基準（GDPR第83条第4項/5項）(1)

- GDPR違反の場合の制裁金の上限額には、次の2通りの類型がある 。
  - 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%のいずれか高い方
  - 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%のいずれか高い方
- GDPR違反の場合の監督機関による執行としては、行政制裁金の賦課のみならず、開示や監査といった調査、作為または不作為に関する遵守命令、処理の禁止、データ主体に周知させる命令、認証の撤回、および警告があり、常に行政制裁金が課せられるわけではない。

制裁金の基準（GDPR第83条第4項/5項）(2)

制裁金の基準	義務違反の類型
管理者又は処理者が、右記に当てはまる場合、€1000万以下、事業者の場合には、管理者又は処理者の全世界年間売上高の2%以下のいずれか高い方	▪ 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(第8条) ▪ 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、又はそのような措置を実施しない処理者を利用した場合(第25条、第28条) ▪ 義務があるのにEU代理人を選任しない場合(第27条) ▪ 責任に基づいて処理行為の記録を保持しない場合(第30条) ▪ 監督機関に協力しない場合(第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(第32条) ▪ 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(第33条)、データ主体に通知しなかった場合(第34条) ▪ 影響評価を行なわなかった場合(第35条) ▪ 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(第36条) ▪ データ保護責任者を選任しなかった場合、又はその職や役務を尊重しなかった場合 (第37～39条)
管理者又は処理者が、右記に当てはまる場合、€2000万以下、事業者の場合には、企業の全世界年間売上高の4%以下のいずれか高い方	▪ データ処理に関する原則を遵守しなかった場合(第5条) ▪ 適法に個人データを処理しなかった場合(第6条) ▪ 同意の条件を遵守しなかった場合(第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(第9条) ▪ 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(第12-22条) ▪ 個人データの移転の条件に従わなかった場合 (第44-49条) ▪ 監督機関の命令に従わなかった場合 (第58条(1)及び(2))

GDPRを一言で説明すると？＝「個人データ」の「処理」と「移転」に関する法律

- GDPRは、EEA域内で個人データを処理し、個人データをEEAから第三国に移転するために満たすべき法的要件を規定している。

概念	説明	例
個人データ（第4条(1)及び前文第26項から第30項）	**識別された又は識別可能な自然人に関連する全ての情報** **識別可能な自然人**とは、直接又は間接的に識別される人である。個人が識別可能かどうかを判断するには、個人を直接又は間接的に識別するために**管理者**又はそれ以外の者が適切に使用可能な全ての手段を考慮しなければならない。	– 名前 – 識別番号 – 所在地データ – 職業上のE-mailアドレス – オンライン識別子(IPアドレス / クッキー識別子) – 身体的/生理学的/遺伝子的/精神的/経済的/文化的/社会的固有性に関する要因
処理（Processing）（第4条(2)）	GDPRは、処理がEU内で行われるか否かにかかわらず、EU内の**管理者**又は**処理者**の拠点の活動に照らして個人データの処理に適用される（第3条(1); *Google Spain*, C-131/12） 処理とは、**自動的手段で行われるか否かにかかわらず、個人データに対して行われる全ての操作又は組単位の操作**を意味する。	- E-mailアドレスの**収集** – クレジットカードの詳細の**保管** – 顧客の連絡先詳細の**変更** – 顧客の名前の**開示** – 上司の従業員業務評価の**閲覧** – データ主体のオンライン上の識別子の**削除** – 全従業員の名前、社内での職務、事業所の住所及び写真を含む**ディレクトリの作成**
移転（Transfer）	「個人データの移転」の概念は指令とGDPRのいずれにも定義されていない。あえて定義すると、**第三国の第三者に対して個人データを閲覧可能にするためのあらゆる行為**である	個人データを含んだ書面又は電子形式の文書を郵便又はメールを通して送付する

仮名化データと匿名化データ

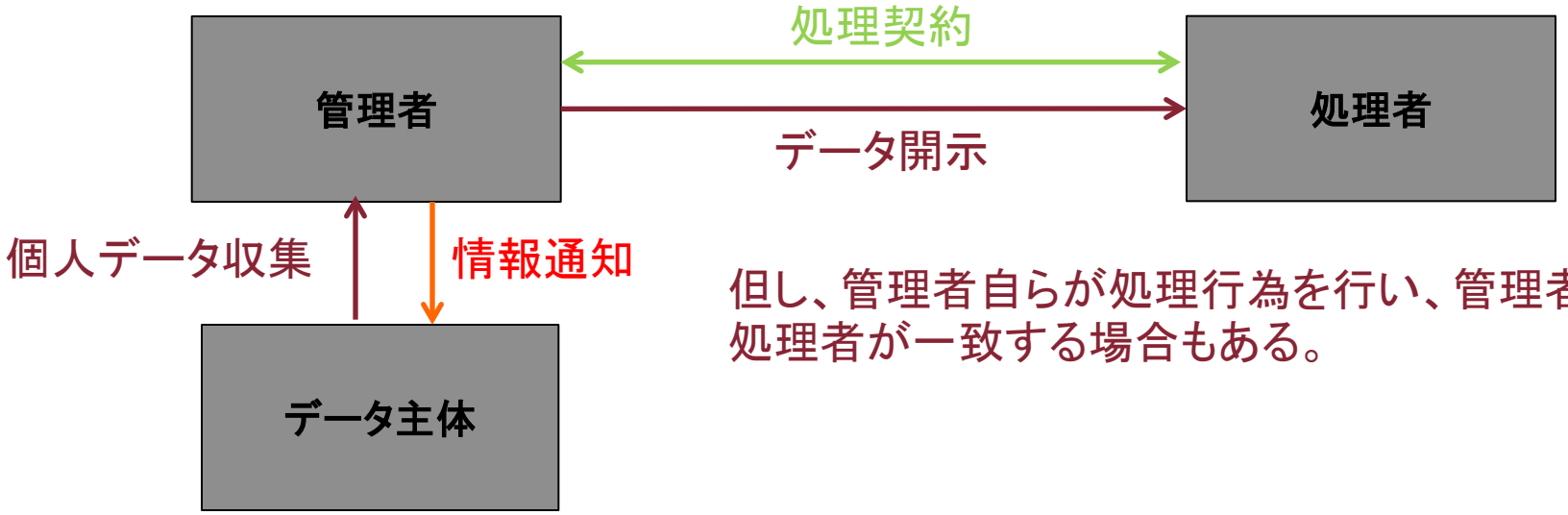
概念	説明	例
仮名化データ（第4条(5)及び前文第26項）	仮名化とは、識別された又は識別可能な個人に属するものではないことを保証するために、追加情報が別途保管され、かつ技術的及び組織的対策の対象となっている限り、**かかる追加情報なしには、データがデータ主体に属するものと分からないように 個人データを処理すること**である。**仮名化データは依然として個人データである**	「チャールズ・スペンサーは1967年4月3日に生まれ、二人の男の子と二人の女の子の4児の家族の父である」という文章は、以下のように仮名化されることができる。「324は二人の男の子と二人の女の子の4児の家族の父である」
匿名化データ（前文第26項、WP216の6頁）	**匿名化は不可逆的に識別を防止するもので、匿名化データは個人データではなく、**またGDPRの範囲内にも入らない。 作業部会は匿名化に不可欠な三つのリスクを検討している。以下の3つのリスクへの解決法(完全な匿名化過程)は、管理者及び第三者が利用する最も可能性が高く合理的な手段によって実行される再特定化に対して堅固である。理想的な解決法は**ケースバイケース**で決めるべきである。 1. **選び出し(Singling out)**: データセット中で個人を特定する一部又は全部の記録を分離する可能性に対応する 2. **照合可能性(Linkability)**: 同一のデータ主体又はデータ主体の組(同一のデータベース中か二つの異なるデータベース中)に関する少なくとも二つの記録を結びつけることのできる能力 3. **推論(Inference)**: 他の属性のセットの値から、ある属性の値を、高度の蓋然性をもって推論することができる可能性	データは暗号化されており、復号キーは既に廃棄されている

特別カテゴリーの個人データ

概念	説明	例
特別カテゴリーの個人データ(センシティブデータ)(第9条(1))	**人種/種族的出身、政治的見解、宗教又は哲学的信念、労働組合の組合員たる地位、遺伝子データ、生体データ、健康又は性生活及び性的嗜好を表す個人データ** 企業はかかるデータを例外を除き処理することができない	ABC社は自社従業員の個人データを処理し、労働組合に加入している者をリストアップする
遺伝子データ(第4条(13)及び前文第34項)	**遺伝を受けた又は後天的な個人の遺伝特性に関連する全ての個人データであり**、個人の生理機能又は健康に関する固有の情報を提供するものであり、問題となる個人の生体試料の分析から明らかになるものである。	ABC社は臨床試験を行い個人のDNAを分析する
生体データ (第4条(14))	個人の固有の識別を可能に又は確定する**特別な技術的処理から得られる個人の身体的、生理的又は行動的特性に関連するあらゆる個人データ**	ABC社は顔画像を認識しそれをABC社のサーバに送信することによって個人を識別するカメラを作った。
健康に関するデータ (第4条(15) 及び前文第35項)	自然人の健康状態を明らかにする、ヘルスケアサービスの提供を含む**自然人の身体的又は精神的健康に関連する個人データ**	発生源とは関係なく病気、障害、疾病リスク、病歴、臨床治療、或いは実際の生理的又は生物医学的状態に関する全ての情報

「データ主体」、「管理者」、「処理者」

概念	説明	例
データ主体	個人データが関連する当該個人	ABC社は自社従業員の個人データを処理している。この個人データが関連するABC社の従業員個人がデータ主体である。
管理者 (第4条(7))	**単独又は共同で個人データ処理の目的と手段を決定する。**管理者はデータ処理の適法性の責任を負いGDPR違反に対する責任を負う。	ABC社は自社従業員の個人データを処理している。雇用者としての義務を遂行するために処理を行っているため管理者に相当する。
処理者 (第4条(8))	処理者は**自然人又は法人であり、管理者を代理して、個人データの処理を行う。**	ABC社は他社のマーケティングツールの管理のためのデータ処理を専門業としている。この機能においてはABCは処理者であり、管理者を代理して処理を行う。



但し、管理者自らが処理行為を行い、管理者と処理者が一致する場合もある。

GDPRの適用範囲(第2条及び第3条)

- GDPRは、管理者又は処理者がEEA内で行う処理に対して適用される。
- GDPRは、管理者又は処理者がEEA内に拠点を有しない場合であっても、以下のいずれかの場合には適用される。
  - EEAのデータ主体に対し**商品又はサービスを提供**し、又は
  - EEAのデータ主体の**行動を監視**する場合
- 日本本社のウェブサイトでEEA所在者に対し商品・サービス(鉄道切符、航空券、パッケージ旅行等)を販売する企業は本社に対しGDPRの直接適用があり得ることに注意が必要である。

概念	説明	例
行動監視(前文第24項)	特に個人の意思決定を収集するため、若しくは個人の嗜好、行動及び態度を分析又は予測するために**インターネット上で自然人を追跡し、プロファイリングすること**	以下の目的で顧客をプロファイリングする。 – 自社のマーケティングの狙いを定める – 詐欺を防ぐ – 自社サービスの誤用を防ぐ – 顧客の居住地、購買習慣又は社会的交際範囲に関する情報の信憑性を確認
プロファイリング(第4条(4))	自然人に関連する特定の個人的側面を評価するために、特に当該自然人の職務遂行、経済的状況、健康、個人的嗜好、趣味、信頼性、態度、所在地又は行動に関する特定の個人的な側面を評価するための当該個人データの使用により構成される個人データの自動処理のあらゆる形態	以下の目的で顧客をプロファイリングする。 – 自社のマーケティングの狙いを定める – 詐欺を防ぐ – 自社サービスの誤用を防ぐ

GDPRの適用範囲に入らないものは何か?

- **個人データがファイリングシステムに含まれておらず、又は含まれることが意図されていなかった場合の手動の処理、並びに特定の基準に従って構造化されていないファイル、ファイルのセット及びそれらの表紙は、**GDPRの適用範囲外である (第2条(1)及び前文第15項)。
- GDPR は**純粋に個人的な又は家庭活動であり(第2条(2)(c))、**専門的又は商業的活動に関連しない**自然人の個人データの処理**には適用されない。純粋に個人的な又は家庭活動には、個人及び家庭活動の関連内で行われる通信や住所の保有、又はソーシャルネットワーキングやオンラインでの活動が含まれ得る。しかし、かかる個人又は家庭活動のための個人データを処理する手段を提供するような管理者又は処理者にはGDPRが適用される(前文第18項)。

保護対象となる「個人データ」の範囲

- GDPRの保護対象となる「個人データ」とは、EEA域内に所在する個人(国籍や居住地などを問わない)の個人データ
  - 短期出張や短期旅行でEEA域内に所在する日本人の個人データを日本に移転する場合を含む
- 日本企業から現地に出向した従業員の情報(元は日本からEEA域内に移転した情報)についても、第三国への移転の制限を受ける個人データに含まれる。
  - 移転のルールは「処理を実行中、又は第三国への移転後に処理が予定されている個人データのいかなる移転」にも適用される(第44条)。
  - 日本からEEA域内に一旦個人データが送付されると、EUの基準に沿ってEEA域内において処理されなければならない。当該個人データが日本へ移転される場合、EUの基準を遵守しなければならない。

GDPR遵守への第一ステップとしてのデータマッピング

- GDPRを遵守するためには、質問票を本社、子会社、支店等の全ての拠点に送付し、フォローアップのインタビューを行い、個人データの処理や移転について調査を行う。これは、ベルギー子会社が法務部を有しない場合、ベルギー子会社・支店ではなく、本社が行うべきこと。
- 本社/子会社/支店がEEA内に所在する個人（国籍や居住地を問わない）の個人データを処理するかどうかを調査する。以下の事項を特定する。
  - 処理の目的
  - 個人データの種類と量
  - 特別カテゴリーの個人データを処理するかどうか
  - EEAデータをデータ輸入者（EEA域外の拠点）に対して送付するデータ輸出者（EEA域内の拠点）
  - 企業グループ内のデータ輸出者/データ輸入者の役割（管理者又は処理者）
  - EEA域外の拠点が収集し、EEA域内に所在する個人から受領する個人データを特定し、どのメディアを通じて受領するかを特定する
  - EEA所在者の個人データを保管するサーバを特定する
- ベルギー子会社・支店が行うべき対応は、本社より質問票を受け取り次第、適切な「個人データ」の概念の理解に基づき、回答を行うことである。

I-2. GDPRコンプライアンス対応における重要論点: データ処理

データ処理の要件

- ベルギー子会社・支店は以下の事項への対応を本社と連携を取りながら進める必要がある。

説明責任 (GDPR第5条第2項)	遵守を実証する方法の実行(GDPR第24条-第30条、第35条-39条)	データセキュリティに関係する義務 (GDPR第32条-34条)	データ主体の権利の尊重 (GDPR第12条-22条)

▪ 以下の原則を遵守する
  ▪ 適法性、公正性及び透明性。例えば、有効な方法でデータ主体の同意を取得する
  ▪ 目的の限定
  ▪ データ最小化
  ▪ 正確性
  ▪ 保管の限定
  ▪ 完全性・機密性
▪ 管理者は遵守を実証できなければならない
	▪ データ保護方針の制定・施行
	▪ 認証の取得
	▪ 仮名化
	▪ 処理行為の記録保持義務の履行
	▪ GDPRを遵守する処理者の使用
	▪ 設計・初期設定におけるデータ保護
	▪ データ保護影響評価/事前相談
	▪ データ保護責任者の選任
		▪ 適切なセキュリティ対策の実施
		▪ 監督機関及びデータ主体に対する個人データ侵害の通知とそれに伴う内部手続きの構築
			▪ データ主体の権利の尊重とその行使の促進、情報権、アクセス権、訂正権、削除権（忘れられる権利）、制限権、異議権、データポータビリティの権利、及び自動的な個人の意思決定に関する権利
			▪ 適切な申請書の策定と内部の遵法の手続きの策定

説明責任
(GDPR第5条第2項)

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

説明責任(第5条(2))

- 管理者は、個人データ処理の原則の遵守に責任を負い、その遵守を実証できる必要がある。

原則	個人データの取扱い
適法性、公平性及び透明性	適法、公平かつ透明性のある方法で処理すること(第5条(a))
目的の限定	特定的で、明確、かつ正当な理由のために収集され、それらの目的にそぐわない方法でそれ以上の処理を行なわないこと(第5条(b))
データの限定	処理を行なう目的に関し、十分で関連性があり必要最小限に限定されていること(第5条(c))
正確性	正確で、必要であれば常に最新状態に更新しておくこと。不正確な個人データは遅滞なく削除又は訂正する こと(第5条(d))
保管の限定	処理の目的に必要な期間以上、データ主体の識別可能な状態で保管をしないこと(第5条(e))
完全性と機密性	不正又は違法な処理からの保護、不慮の損失、破壊、損失からの保護を含み、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すること(第5条(f))

処理の適法性(第6条)

- 管理者/処理者は以下のいずれかの要件を満たす場合に個人データの処理を行うことができる。
  - 1. データ主体が一又は一以上の個別の目的のため、自己の個人データの処理に**同意**を与えた場合(第6条(1)(a))
  - 2.-5. 以下のいずれかの処理が必要とされる場合(第6条(1)(b)-(e))
    - 2. データ主体が当事者である契約の実行のため、又は、データ主体の要請により契約締結前に段階を踏むため
    - 3. 管理者が負う法的義務を遵守するため
    - 4. データ主体又は他の自然人の重大な利益を保護するため
    - 5. 公共の利益あるいは管理者に属する公式な権限の行使として実行する作業の履行のため
  - 6. データ処理は管理者あるいは第三者が追及する**正当な利益**の為に必要である場合。但し、例外として、データ主体が子供であった場合のように、そのような利益が個人データの保護として、データ主体の利益又は基本的人権及び自由に優先される場合は除く(第6条(1)(f))。この点において、データを収集する時点でのデータ主体の合理的な予測が考慮されるべきである(前文第47項)
    - 指令第7条の管理者の正当な利益の考え方に関する作業部会の意見書(WP217)参照

処理の適法性：データ主体の同意の要件

- **データ主体の同意**とは、**自由に与えられた、個別の、情報に基づく、不明瞭ではないデータ主体の意思表示によって、データ主体が発言又は明快な肯定的行動により合意を示すこと**を意味する(第4条(11))。
  - **同意が情報に基づくもの**と認められるためには、データ主体は少なくとも管理者の身元と個人データが処理される目的について知っている必要がある (前文第42項。第13条・第14条参照)。
  - **同意が自由に与えられたか否か**を検討する際、契約の履行としてデータ処理への同意が条件とされているかについて最大の注意が払われなければならない(第7条(4) 、前文第43項)。
    - データ主体に実質的な選択の自由がなく、不利益を被ること無しに同意を撤回することが不可能な場合、同意は自由に与えられたものとみなされない(前文第42項)。
      - 監督機関は管理者が従業員から取得する同意については任意性について疑いを持っている。
      - 従って、「個人データの処理の適法性」の「2. データ主体が当事者である契約の実行のため処理が必要な場合」の要件に依拠して、処理の適法性を担保するのが慎重な対応である(例、労務契約の実行のために必要な範囲で従業員のデータ処理を行う)。
  - **同意が書面による声明として求められた場合**、他の項目が問題となる。同意の依頼は、他の項目から明確に識別できる形で表記され、分かりやすい言葉で明瞭かつ簡潔に書かれていなければならない。声明の一部がGDPRに違反する場合、データ主体の同意に拘束力はない(第7条(2))
  - **データ処理の目的が複数である場合**、同意を**全ての処理目的について取得するべき**(前文第32項)
  - データ主体はその**同意をいつでも撤回する権利**を有する。同意の撤回は、撤回前のデータ処理の適法性に影響を与えるものではない。これらの点は、同意を行う前にデータ主体に知らされなければならない。同意の撤回は同意を行うときと同様に簡単でなくてはならない(第7条(3))
  - **データ処理の対象が16歳未満の子供の場合**、同意は子供に対し親の責任を有する者によって承認されなければならない(第8条(1))
    - 加盟国はこの年齢を法律により13歳未満とならない範囲でより低い年齢を規定することができる(第8条(1))
    - 管理者は、平均的な技術を考慮し、同意が子供に対し親の責任を有する者によって承認されたことを確認するために合理的な努力をする必要がある(第8条(2))

特別カテゴリーの個人データの処理の適法性(第9条)

- **特別カテゴリーの個人データ**は、要保護性が高いため、監督機関による制裁金賦課やデータ主体による損害賠償請求を受けないようにするため、特に処理の適法性に留意する必要がある。個人データ処理の多くの場合に適法性の根拠として依拠することになる「正当な利益」を使えないため違法となるケースが多い
- 特別カテゴリーの個人データの処理は、以下の場合を除き、認められない。
  1. データ主体が**明示的同意**をしている(第9条(2)(a))
     - 「**明示的同意**」は「個人が個人データの個別の使用又は開示に対し同意するか又は同意しないかという提案を示され、かつ当該個人が積極的に口頭又は書面により質問に回答する全ての状況」を含む。
     - 通常、明示的同意は、手書きの署名付きの書面により与えられるが、これは必ずしも必要ではなく、口頭で与えることもできる(WP187の25頁)。
  2. 以下のいずれかの場合に処理が必要である。(「正当な利益」による処理が適法でない点が「個人データ」と異なる)
     - 法や労働協約で認められている場合の、雇用や社会保障における義務の履行又は権利の行使目的の場合(b)
     - データ主体の重大な利益を保護する場合(c)
     - 処理が、政治的、哲学的、宗教的又は労働組合の目的を有する非営利団体によって適切な保護措置を伴う適法な活動において実行され、当該処理が当該団体の(前の)構成員又は当該目的との関係で当該団体と頻繁に接触していた者にのみ関係するものであること、及び当該個人データが当該データ主体の同意なしに当該団体の外へ開示されないことを条件とする場合(d)
     - データがデータ主体により、明確な形で公開されている場合(e)
     - 法的請求の立証、行使又は防御のため (f)
     - 処理が、追求する目的に比例的であり、データ保護に対する権利の核心を尊重し、かつデータ主体の基本的人権及び利益を保護するための適切かつ具体的な措置を規定する、EU法及び加盟国法に基づいて、重要な公的利益のために必要である場合 (g)
     - 健康上の目的の場合(h)
     - 科学上の目的でデータが匿名化されているかそれが可能でない場合、仮名化されている場合(i)
     - 第89条(1)による公共の利益でのアーカイブの目的、科学的又は歴史調査目的、若しくは統計目的で必要な場合 (j)

遵守を実証する方法の実行
(GDPR第24条-第30条、第35条-39条)

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

データ保護方針の制定・施行(GDPR第24条第2項)

- GDPRに対応したデータ保護方針を制定・施行することは、管理者/処理者に課せられた法的義務である。
  - データ保護方針は管理者の処理及び移転並びにデータ主体の権利について効果的にデータ主体に情報を与えるものでなければならない(第13条、第14条)
- EEA域内の拠点（子会社、支店及び駐在員事務所）では、EEA所在者の個人データを処理する場合、データ保護方針を制定・施行する必要がある。
  - ベルギー子会社は、独自にGDPR対応の個人情報保護要領やプライバシーポリシーを持つことになるが、本社のものをベースに作成すること、または本社とほぼ同じものを作成することも可能。本社とコミュニケーションを取る必要がある。
- 日本本社でGDPRに対応したデータ保護方針を制定・施行
  - 日本の個人情報保護規程とは別に、GDPR対応のデータ保護方針を作成し、EEA所在者の個人データの処理についてのみ適用する。
  - 日本企業のEEA域内の支店や駐在員事務所では、日本本社のGDPR対応のデータ保護方針を策定しておく必要がある。
    - ベルギー支店・駐在員事務所は、本社に対して、GDPR対応の個人情報保護要領やプライバシーポリシーが策定されるのか否かについて確認する。

認証の取得 (GDPR第42条-第43条)

- データ保護認証メカニズムが利用可能になった場合には、利用を検討する。
- 第29条作業部会において認証に関するガイドラインを議論している。2017年第1回の作業部会において認証に関するガイドラインを発表する方向で作業している（当初の2016年末までのスケジュールに遅れが生じている模様）。
- 残された論点（作業部会で検討中の論点）
  - 認証はGDPRの遵守のみを義務付けるべきか、それ以上にすべきか
  - 単一の欧州レベルの認証とすべきか、それともセクター毎に異なったマークやシールを使った複数の認証を認めるべきか。基本的には、均一の欧州レベルの認証に利益があるという議論
  - 認証機関による認定の主な基準
    - 一般的な認定手続
    - 認証機関の役割と義務

      認定機関（第43条第1項第(b)号）はデータ保護に関する適切なレベルの専門性を評価するための深い知識の証拠を提供する義務あり

      第55条又は第56条による管轄監督機関による追加的義務の策定の必要性。データ保護及びプライバシーに関する高水準の知識の保持義務
    - 認定手続における監督機関の役割
    - 各国の認定機関と監督機関の関係の明確化の必要性
  - 監督機関が、認証機関の認定と認証の双方を行なうべきか。利益相反が障害となる。
  - 認証取得者は管轄監督機関に通知をするべきか
  - 認証プロジェクトが失敗した場合の手続
  - データ保護シール上の文言に従わない場合、シールの取消に止まらず、制裁金賦課につなげるべきか

管理者による処理行為の記録保持義務（第30条第1項）

- 各管理者及び、該当する場合、管理者の代理人は、管理下にある処理行為の記録を保持しなければならない。記録は次に掲げる情報のすべてを含む（第30条第1項）。
  - 管理者の名前と連絡先の詳細。該当する場合、共同管理者、管理者の代理人及びデータ保護責任者を含む
  - 処理の目的
  - データ主体の種類と個人データの種類の概要
  - 第三国又は国際機関における取得者を含め、個人データが開示される又は開示され得る取得者の種類
  - 該当する場合、第三国又は国際機関を特定した形式による第三国又は国際機関への個人データ移転、及び、第49条第1項後段で定める移転の場合、適切な保護措置に関する文書
  - 可能であれば、データ種類ごとの削除までの予測される期限
  - 可能であれば、第32条第1項で定める技術的及び組織的安全保護措置の概要
- 記録保持義務は、250名未満の人を雇用する企業/組織には適用されない。
  - 当該処理がデータ主体の権利及び自由を危険にさらす可能性があり、処理が偶発的ではなく、又は特別カテゴリーのデータ又は有罪判決及び犯罪行為に関する個人データの処理を含む場合は、250名未満の人を雇用する企業／組織にも適用される。
    - ベルギー子会社・支店は特別カテゴリーの個人データを処理するのかについて特に検討が必要
- 記録保持義務がGDPR上の義務ではない企業であっても、GDPRが管理者に対して求める記録保持を行っておくことが、監督機関による調査への備えとしては望ましいと考える。
  - 日本本社が管理者となるEEAデータの処理についてはGDPR上の記録保持義務を負う企業がほとんど
  - GDPR違反がなかったことを証明するためには処理行為の記録を監督機関に提出することが効果的と考えられる

処理者による処理行為の記録保持義務（第30条第2項）

- 各処理者及び、該当する場合、処理者の代理人は管理者に代わって行うすべての種類の処理行為に関する記録について、次に掲げる事項を含め、保持しなければならない。
  - 処理者又は複数処理者及び処理者が代わりに実施している各管理者並びに、該当する場合、管理者又は処理者の代理人及びデータ保護責任者の名前と連絡先の詳細。
  - 各管理者の代わりに実施している処理の種類。
  - 該当する場合、第三国又は国際機関を特定した形式によるその第三国又は国際機関への個人データ移転及び、第49条第1項後段で定める移転の場合、適切な保護措置に関する文書。
  - 可能であれば、第32条第1項で定める技術的及び組織的安全保護措置の概要。
- 記録保持義務は、250名未満の人を雇用する企業/組織には適用されない。
  - 当該処理がデータ主体の権利及び自由を危険にさらす可能性があり、処理が偶発的ではなく、又は特別カテゴリーのデータ又は有罪判決及び犯罪行為に関する個人データの処理を含む場合は、250名未満の人を雇用する企業／組織にも適用される。
    - ベルギー子会社・支店は特別カテゴリーの個人データを処理するのかについて特に検討が必要

管理者による処理行為の記録保持義務（第30条第1項）：台帳による管理（例）

- 第30条第1項(a)–(f)の事項は、基本的には台帳を作成し、記録・管理すればよい。
  - 管理者の名前と連絡先の詳細。該当する場合、共同管理者、管理者の代理人及びデータ保護責任者を含む
  - 処理の目的
    - IT運営／サービス管理、製造、人事管理、調達、営業、サービス／メンテナンス、その他
  - データ主体の種類と個人データの種類の概要
    - 従業員データ、顧客データ、サプライヤデータ、その他
    - 特別カテゴリの個人データ（はい・いいえ）、人種・民族的出身、政治的見解、宗教・哲学的信条、健康データ、組合加入状況、性的指向に関するデータ、有罪判決及び犯罪に係る個人データ等
  - 第三国又は国際機関における取得者を含め、個人データが開示される又は開示され得る取得者の種類
    - はい・いいえ、受信側アプリケーション・プロセスの名称、データ処理の目的、受信者の詳細、データの移転先
  - 該当する場合、第三国又は国際機関を特定した形式による第三国又は国際機関への個人データ移転、及び、第49条第1項後段で定める移転の場合、適切な保護措置に関する文書。
    - 移転先の法域の十分性の有無、適切な保護措置（標準契約条項、拘束的企業準則等）
  - 可能であれば、データ種類ごとの削除までの予測される期限。
    - 削除と保管に関する方針の有無、削除期間の実行の有無、当該方針に準拠したデータの自動削除の有無、保持期間の根拠と規定された保持期限
- 「第30条第1項(g)の事項は、技術的保護措置としてログ取得を実装した内容を台帳に記載する必要あり。昨今のITシステムはID/Passwordでアカウント管理が行われる。IDに紐づいて各種情報システムの操作権限が与えられる。誰が何の操作をしたのかという点については各種情報システムで利用しているパッケージの機能に依存する。自社で独自に開発された情報システムの場合、ログ取得のところは実装次第。出来の悪いプログラムでログがきちんと取れない場合には開発から手を入れる必要がある。」（GDPRのITソリューションを専門の一つとする、IIJ Europe Director 小川晋平氏のコメント）
- 可能であれば、第32条第1項で定める技術的及び組織的安全保護措置の概要
  - アクセスコントロール（サーバ所在ビル／部屋、システム、データ）、開示・移転コントロール、入力コントロール、契約コントロール、可用性コントロール、データ分離、ITセキュリティ
- ベルギー子会社、支店及び駐在員事務所は、自社が使っているITベンダーに対しGDPRのIT面での対応が十分かを問い合わせることが望ましい。

GDPRを遵守する処理者の使用(第28条)

- 管理者は、GDPRの要件を満たす技術的、組織的な措置の実行を十分に保障できる処理者以外は使用してはならない(第28条第1項)
  - GDPRを遵守していないクラウドコンピューティングサーバのプロバイダーを利用することのリスク
- GDPRを遵守する処理者を使用することを確保するため、以下の事項を含む契約を締結する
  - 管理者から処理者への処理行為の委託は契約若しくはEU法又は加盟国法(管理者に関する処理者を拘束し、処理の対象事項及び期間、処理の性質及び目的、個人データの種類及びデータ主体の種類並びに管理者の義務及び権利を定める法)に基づく法律行為に基づかなければならない(第28条第3項)。
    - 処理者が従うべきEU法又は加盟国の国内法によって処理の実施が要求されていない限り、第三国又は国際機関への個人データの移転に関することを含め、管理者からの文書化された指示においてのみ個人データを処理すること。当該法律によって処理の実施が要求されている場合、処理者は、当該法律が重要な公共の利益に基づき当該通知を禁止していないならば、処理する前に当該法的要件について管理者に通知しなければならない。
    - 個人データを処理することを許可された個人が機密保持を確約するか、又は適切な法的機密保持義務下に置かれることを保証すること。
    - 第32 条(処理のセキュリティ)により要求されているすべての対策をとること。
    - 他の処理者を従事させることに関して第2項及び第4項で定める条件を遵守すること。
    - 処理の性質を考慮し、可能な限り、管理者が第3章に定められたデータ主体の権利行使の要求に応じる義務を履行するため、適切な技術的及び組織的対策によって管理者を支援すること。
    - 処理の性質及び処理者の利用可能な情報を考慮し、第32条から第36条による義務の遵守を確実にすることにおいて管理者を支援すること。
    - 管理者の選択により、処理に関連したサービスの提供終了後にすべての個人データを消去又は管理者に返却すること及び、EU法又は加盟国の国内法が個人データの保存を要求しない場合に限り、存在する複製物を消去すること。
    - 本条項に定められた義務の遵守を証明するとともに、管理者又は管理者により委任された他の監査人によって実施される調査を含めた監査への準備及び寄与を行うために必要なすべての情報を管理者が入手可能にすること。

設計・初期設定におけるデータ保護(第25条)

- 設計におけるデータ保護 (第25条第1項)
  - プロジェクトの初期段階及び当該プロジェクト完了までの間、GDPRの要件を満たすために、必要な保護措置を処理に統合するための適切な技術的・組織的対策（仮名化等）の実施方法を検討
  - この目的を達成するため、企業は、プロジェクトによって提起されるデータ保護の論点を特定し適切な方法を採るため、個人データの処理に関するプロジェクト（例えば、新しいITシステムを構築する又はデータ保護に影響するポリシー/戦略を発展させる）の初期段階でデータ保護影響評価をどのように実行するかを検討
- 初期設定におけるデータ保護 (第25条第2項)
  - 特定の処理目的のために必要なEEAデータのみを処理することを確実にするため、初期設定のための選択肢を検討

データ保護影響評価/事前相談（第35条-36条）

- **データ保護影響評価**とは、データ処理に先立つ個人データ保護のための影響評価のことをいい、データ処理の種類(とりわけ新しい技術)が個人の権利や自由に対して危険性の高い場合に管理者が行うことを義務付けられている（第35条）。
  - 個人の権利や自由に対しての危険性は、たとえば業務内容の査定や予測により個人的な態度がデータ処理により評価された結果としてもたらされる経済的あるいは社会的損失につながる恐れがある(前文第75項)
- 以下の状況においては特に影響評価が必要とされる。
  - プロファイリングを含む自動処理に基づいて自然人に関する個人的側面を体系的かつ広範囲に評価され、その評価に基づいて決定がなされ、その決定が自然人に関する法的効果を生じさせるか又は自然人に重大な評価を与える場合
  - 特別カテゴリーの個人データ並びに、有罪判決及び犯罪行為に関する個人データの大規模な処理
  - 誰でも立ち入ることが出来る場所において大規模な体系的監視を行う場合
- 評価には少なくとも以下に掲げる事項を含む。
  - 予想された処理作業及び処理の目的の体系的記述。該当する場合、管理者によって追求される正当な利益を含む。
  - 目的に関する処理作業の必要性及び比例性の評価。
  - データ主体の権利及び自由に関するリスクの評価。
  - リスクに対処するために予定された対策。データ主体及び関連する他者の権利及び正当な利益を考慮し、個人データの保護を確実にし、GDPRの遵守を証明するための保護措置、安全対策及び安全メカニズムを含む。
- 監督機関は、**データ保護影響評価が必要となる処理業務のリスト**及び**データ保護影響評価が必要とならない処理業務のリスト**をそれぞれ作成し、欧州データ保護会議も当該リストの整合性を保証する。
  - 作業部会は2017年初めにリスクの高い処理およびデータ保護影響評価に関するガイドラインを出すと発表している。
- **事前相談**：管理者によるリスクを軽減するための措置がないために、処理によって高いリスクが起こり得ることを影響評価が示している場合、管理者は**処理前に**監督機関に相談する必要がある（第36条）。

データ保護責任者(DPO): 第37条-39条(1)

- DPOについては2016年末までに作業部会がガイドラインを出すと発表している。
- 次のいずれかの要件を満たす場合にはDPOの選任義務あり
  - 処理が公的機関又は団体によって行われる場合（ただし、司法権に基づく裁判所の行為を除く）
  - 管理者又は処理者の中心的業務が、その性質、適用範囲及び/又は目的によって、大規模にデータ主体の定期的かつ系統的な監視を必要とする処理作業である場合。
    - 「中心的業務」：管理者又は処理者の目的を達成するための主要な業務の実行。例えば、人事データ処理は、DPOの選任義務の根拠とならないが、企業が運送会社のためのトラックの追跡に代表される、位置情報システムのようなシステムを開発した場合はDPOの選任義務あり。
  - 管理者又は処理者の中心的業務が、特別カテゴリーの個人データ並びに有罪判決及び犯罪に関する個人データを大規模に処理する場合、又は
    - 「大規模に」：定量的基準に基づくべきでなく、個別に対処すべき
  - EU又は加盟国の法律でDPOの選任が義務付けられている。
- **DPOの任務**
  - 少なくとも以下の業務を行うこととする。
    - 管理者又は処理者及び処理を実施する従業員にGDPR及びその他EU 又は加盟国のデータ保護規定による義務を通知及び勧告すること。
    - GDPR、その他EU 又は加盟国のデータ保護法、及び個人データの保護に関して管理者又は処理者が設定した個人データ保護方針の遵守の監視。責任の分担、処理作業にかかわる職員の意識の向上及び訓練、並びに関連する監査を含む。
    - 要請があれば、データ保護影響評価に関する助言の提供及びその遂行の監視。
    - 監督機関との協働。
    - 処理に関する問題について監督機関との問い合わせ先となること。事前協議、適切な場合その他事項に関連する協議を含む。

データ保護責任者(DPO): 第37条-39条(2)

- DPOの選任
  - 専門家としての質、特にデータ保護法及びその実務の専門知識並びに任務を遂行する技量に基づいて選任されるものとする。管理者又は処理者の従業員、または業務委託契約に基づいて任務を遂行するものでもよい（第37条第5項）。
  - 残された論点（作業部会で検討中の論点）
    - 非常勤DPOの指名は許容できるが、利益相反および効率的な人員配置のリスクに対する細心の注意を払う
    - 個人又はチームとしてのDPOの指名。個人（自然人）ではなく、法人組織としてのDPO指名（外部法律事務所等）
    - データ保護専門での勤続年数、語学力、DPOの指名に必要な訓練に関する専門知識（十分な知識と解釈）
    - 外部DPOを指名するための標準的な契約条項を検討する必要性
    - DPOの責任の性質：民事又は刑事。加盟国法によって判断
- 利益相反
  - 管理者又は処理者は、そのような任務や義務が利益相反にならないよう確実にしなければならない。
    - 利益相反：データ処理の判断（目的および手段）に関与しないこと。肩書きのみではなく配置や役割が重要
- 管理者・処理者の主な義務
  - DPOの独立性の保証
    - DPOが個人データ保護に関する一切の事柄について適切、適時に取り組むことを確保。
    - 業務遂行においてDPOを支援しなければならず、その支援は、当該業務の実行、個人データ及び処理作業へのアクセス、及びDPOの専門知識を維持するのに必要な資源を提供することによってなされるものとする（第38条第2項）
    - 管理者・処理者は、DPOが任務の遂行に係わる指示を一切受けないことを確実にしなければならない。DPOは、当該任務の遂行について管理者・処理者から解雇又は処罰を課されないものとする。
    - DPOは、管理者又は処理者の最高経営レベルに直接報告を行なうものとする。
    - 明確で透明性のあるミッションステートメント及び年次報告を作成
  - 残された論点：管理者・処理者の追加的責務（作業部会で検討中の論点）
    - 継続した専門性を保持するために、DPOに対し、各職務に関連した資源へのアクセス（ITツール、法律知識、法科大学院や大学におけるその他の学部の授業、特定の専門計画等）を含む定期的で効果的な研修会並びに専門能力開発プログラムを提供
    - DPOの役割が警察官とならないことを保証する。DPOの役割は信頼に基づくべきであり、その目的は解決策を考え出すことである。DPOは処分を行ったり、監督機関への報告をすべきではなく（機密・利益相反）、最高経営幹部への報告を行い、適切な処置を決定すべき

データセキュリティに関する義務
（第32条-第34条）

WILMERHALE

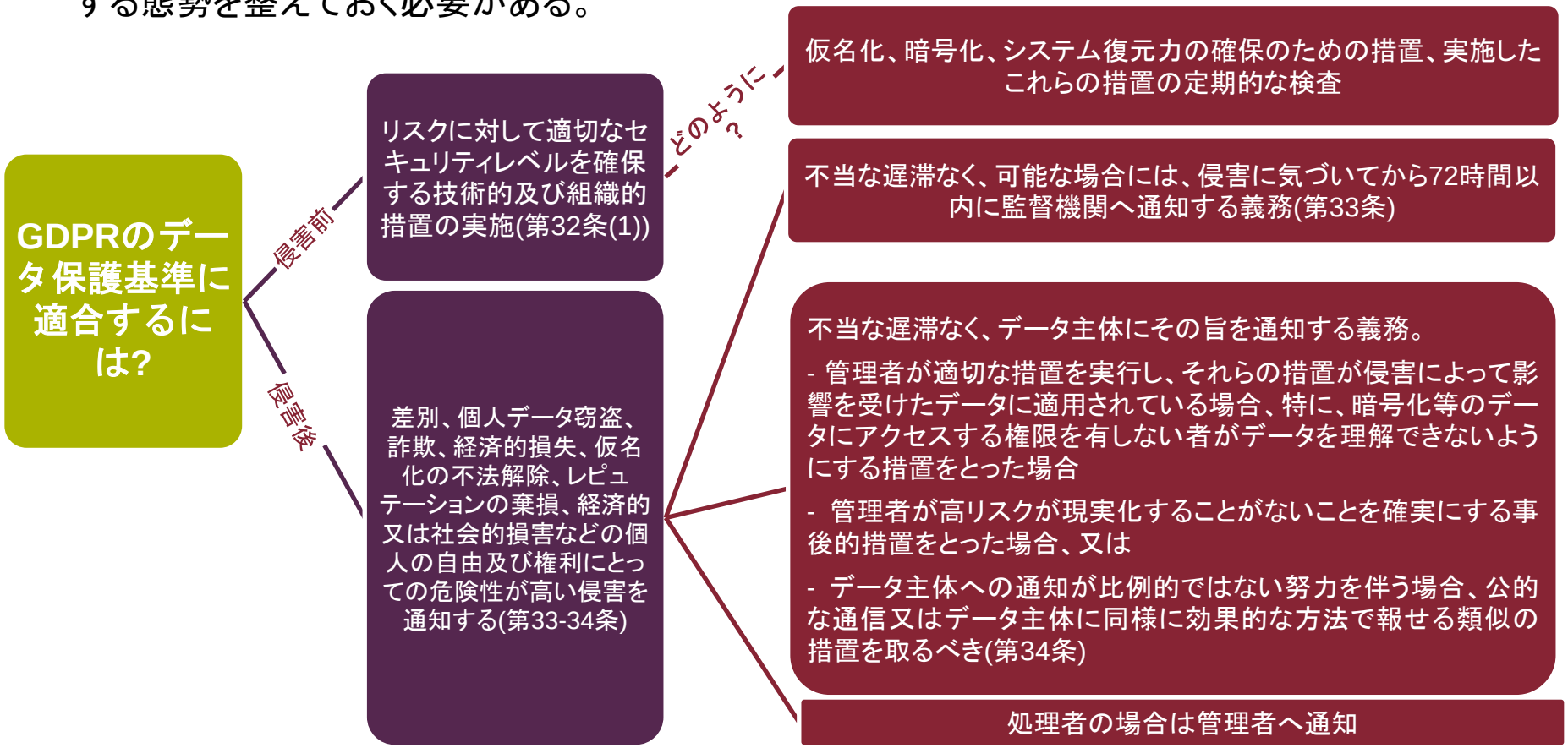
WILMER CUTLER PICKERING HALE AND DORR LLP

適切なセキュリティ対策の実施(第32条第1項-第34条)(1)

- リスクに対して適切なセキュリティレベルを確保するため、適切な技術的・組織的対策の実施の方法を検討
  - 検討される選択肢
    - 仮名化
    - 暗号化
    - システムの復元力を確保する方法
    - ISO 27000
  - 実施する方法のテストを頻繁に行う
- 個人データ侵害を検知し、適時に監督機関に対して通知するための内部手続の構築
  - 従業員をトレーニングし、当該企業内での意識向上
  - 法務、IT及び他の関連する部署のコーディネーション

適切なセキュリティ対策の実施(第32条第1項-第34条)(2)

- EEAデータに関し個人データ侵害を探知し監督機関へ適時に通知できるように、適切な保護措置及び社内手続を実行する。具体的には、EEAデータが保管されているサーバの場所を特定し、当該サーバにサイバーアタックがあった際に、監督機関への通知の要否を適時に判断し、通知する態勢を整えておく必要がある。



データ主体の権利の尊重
（第12条-第22条）

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

データ主体の権利への対応(第12条第1項-第22条)(1)

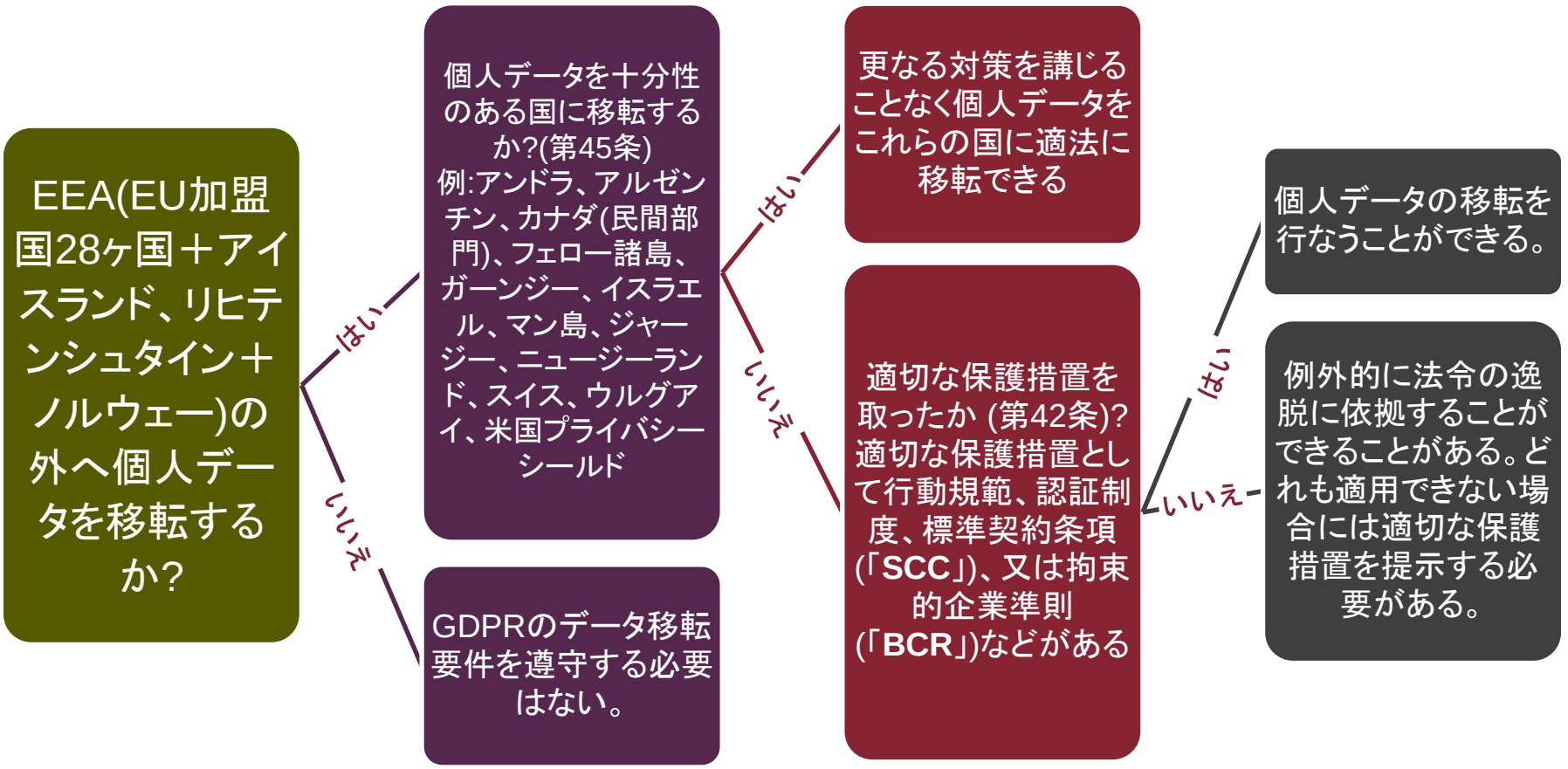
- データ主体の権利（情報権、アクセス権、訂正権、削除権、データポータビリティの権利、異議権）の行使を可能にする申請書の準備
  - 管理者は、データ主体の権利を尊重する義務があるため、データ主体の権利行使のための管理者における連絡先を個人データ保護方針等で明らかにしておく必要がある。
  - 遅くとも依頼を受け取ってから1ヶ月以内、必要であれば3ヶ月以内に不当な遅滞なく返答しなければならない。
  - 管理者は企業グループ内でデータ主体の権利行使があった場合に適切に対応するメカニズムを作る必要あり
- データ主体の苦情に対応することができるように内部の苦情手続の構築

データ主体の権利への対応(第12条第1項-第22条)(2)

データ主体の権利	内容
情報権(第13条、第14条)	管理者はデータ主体から個人データを収集する場合に、個人データ入手時に、データ主体に一定の情報を提供しなければならない。
アクセス権(第15条)	管理者はデータ主体から処理が行われている個人データへのアクセスの請求があればそのコピーを提供しなければならない
訂正の権利 (第16条)	不正確な自己の個人データに関する訂正を管理者に求める権利を有する
削除権(第17条(1))	一定の場合、データ主体は自分に関する個人データの削除を遅滞なく管理者から得る権利を有する。
制限権(第18条)	データ主体は管理者に対して一定の場合に個人データ処理を制限する権利を有する。
データポータビリティの権利(第20条)	データ主体は自分に係わる個人データを、構造化され、一般的に使用され、機械によって読み取り可能な形式で受け取る権利を有する。
異議権(第21条)	データ主体は管理者又は第三者によって追求される適法な利益の目的のための処理の必要性に基づく自己の個人データの処理に異議を唱える権利を有する。
自動化された個人の判断に関する権利(第22条)	データ主体は、自分に対する法的影響を生じ得たり、自分に対する多大な影響を生じ得るような、プロファイリングを含む自動処理のみに基づいた判断の対象にならない権利を有する(例、人が介入しないオンライン上での借入申込やインターネットでの採用活動–前文第71項)。

I-3. GDPRコンプライアンス対応における重要論点: データ移転

個人データの移転(第45条-49条)



データ移転のツールの概要

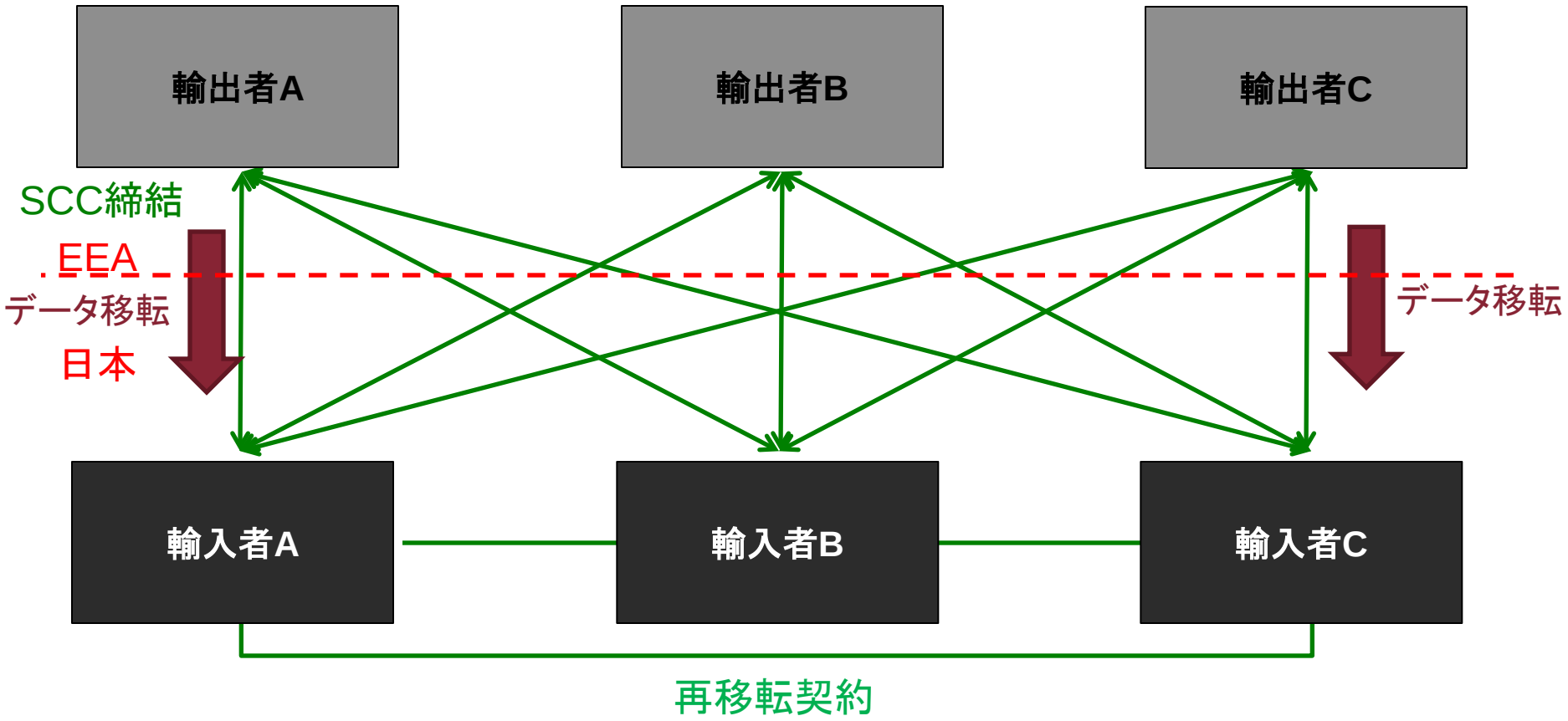
法的根拠	説明
SCC(標準契約条項)	欧州に法務部を持つかなりの数の日本企業がSCCを締結している。それ以外の多くの日本企業が指令に基づく又はGDPRを見据えてSCC対応を行っている。
BCR(拘束的企業準則)	少なくとも2社の日本企業（楽天株式会社、株式会社インターネットイニシアティブ（IIJ）（実際の申請者はIIJ Europe））がBCRの申請を行った。BCRの承認を取得した日本企業はまだ一社もない。指令におけるSCC対応よりも、BCR対応（＋企業グループ外との関係でSCC対応）の方が執行リスクを減らす点でも費用対効果の点でも望ましいと思われる日本企業の数は多いと考える。
同意/必要性の例外	同意は非常に制限的な例外であるが、個人データを移転するために依拠することが必要な場合も依然としてある。必要性に基づいて認められる例外も法定されているが利用可能な場合は限定的
プライバシー・シールド	プライバシー・シールドは、EUから米国へのデータ移転のみに利用可能である。プライバシー・シールドの有効性についてEU裁判所で争われている。
十分性認定の取得	**日本企業は、GDPR施行前の日本国としての十分性の取得に期待すべきではない。**日本は正式に十分性に関する申請を未だ行っておらず、取得するには日本が正式に十分性認定の申請を行った後、過去の実例を踏まえると、少なくとも4年前後は要する見込みである。韓国や英国による十分性認定の申請への動きによっては、欧州委員会における十分性認定の審査のためのリソースが先に取られてしまい、日本の申請の審査が後回しになる懸念もある。
認証	認証制度は、日本企業が日本で取得した認証が、EUの認証制度との**相互認証**を得られるような場合に特に興味深い。しかしながら、何らのガイダンスも出されていない。
行動規範	行動規範を取得する活動に加わることによりコンプライアンス関連のコストを削減することができる可能性があることから興味深い。しかしながら、何らのガイダンスも出されていない。

標準契約条項（SCC）

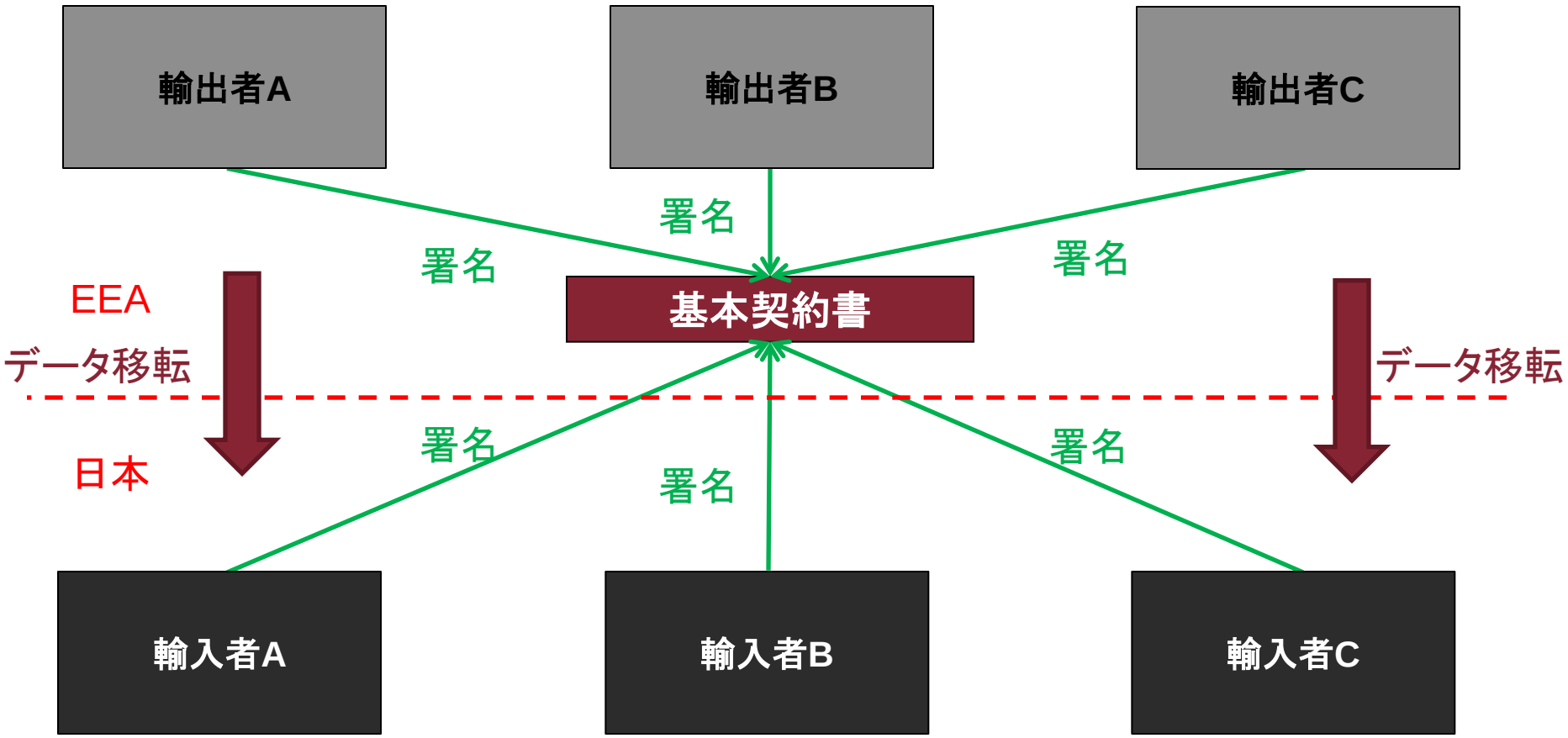
- SCCとは、欧州委員会によって決定された契約書の雛形であり、二当事者間でこの雛形を使ってデータ移転契約を締結することで適切な保護措置を提供し、適法なデータ移転を行うものである。現時点で利用可能なSCCは管理者-管理者SCCが2つ、管理者-処理者SCCが1つの計3つある。
- SCCは、単に署名をしさえすれば後は保管しておけば良いという性質のものではなく、SCC中のデータ輸出者とデータ輸入者の義務をそれぞれ履行できる体制を整えることが肝要である。当該義務の違反は制裁金の対象となる可能性がある。
- 処理者-復処理者のSCCはまだ存在しない（作業部会が提案したSCC案のみ）

輸出者	輸入者	状況	現在のSCCのセット
管理者	管理者	個人データがEU内の管理者からEU外の管理者へ移転される場合	2セットのSCCがある ▪ **2001年SCC**(EC Decision 2001/497/EC) ▪ **2004年SCC**(EC Decision 2004/915/EC)
管理者	処理者	個人データがEU内の管理者からEU外の処理者へ移転される場合	▪ **2010年SCC**(EC Decision 2001/87/EC)
処理者	復処理者	個人データが、まずEU内で管理者から処理者へ移転され、その後、その処理者からEU外にいる復処理者へ移転される場合	作業部会は2014年3月、**処理者-復処理者SCC案**を提案した(WP214)。しかし、欧州委員会はこれをまだ承認していない。

データ移転毎にSCCを締結する

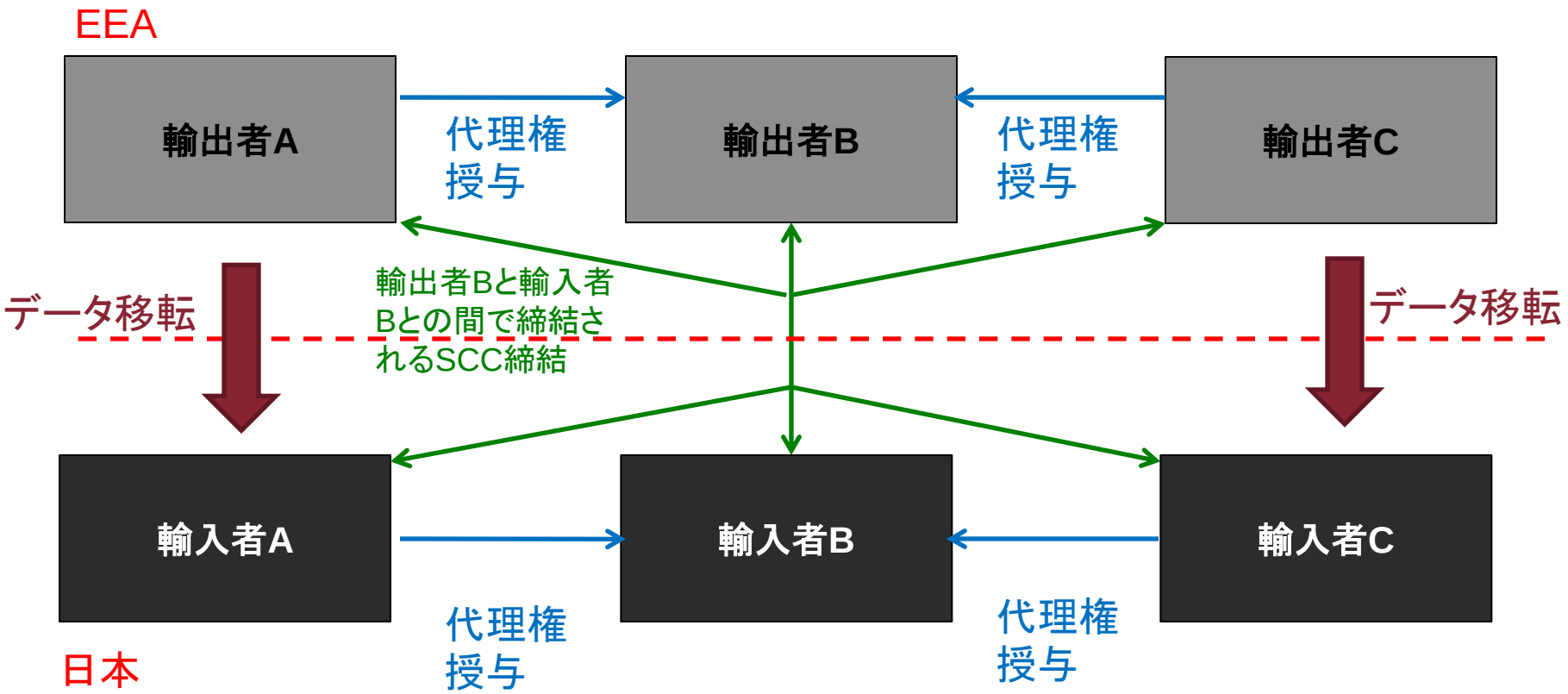


SCCによる複数当事者間のデータ移転：タイプA

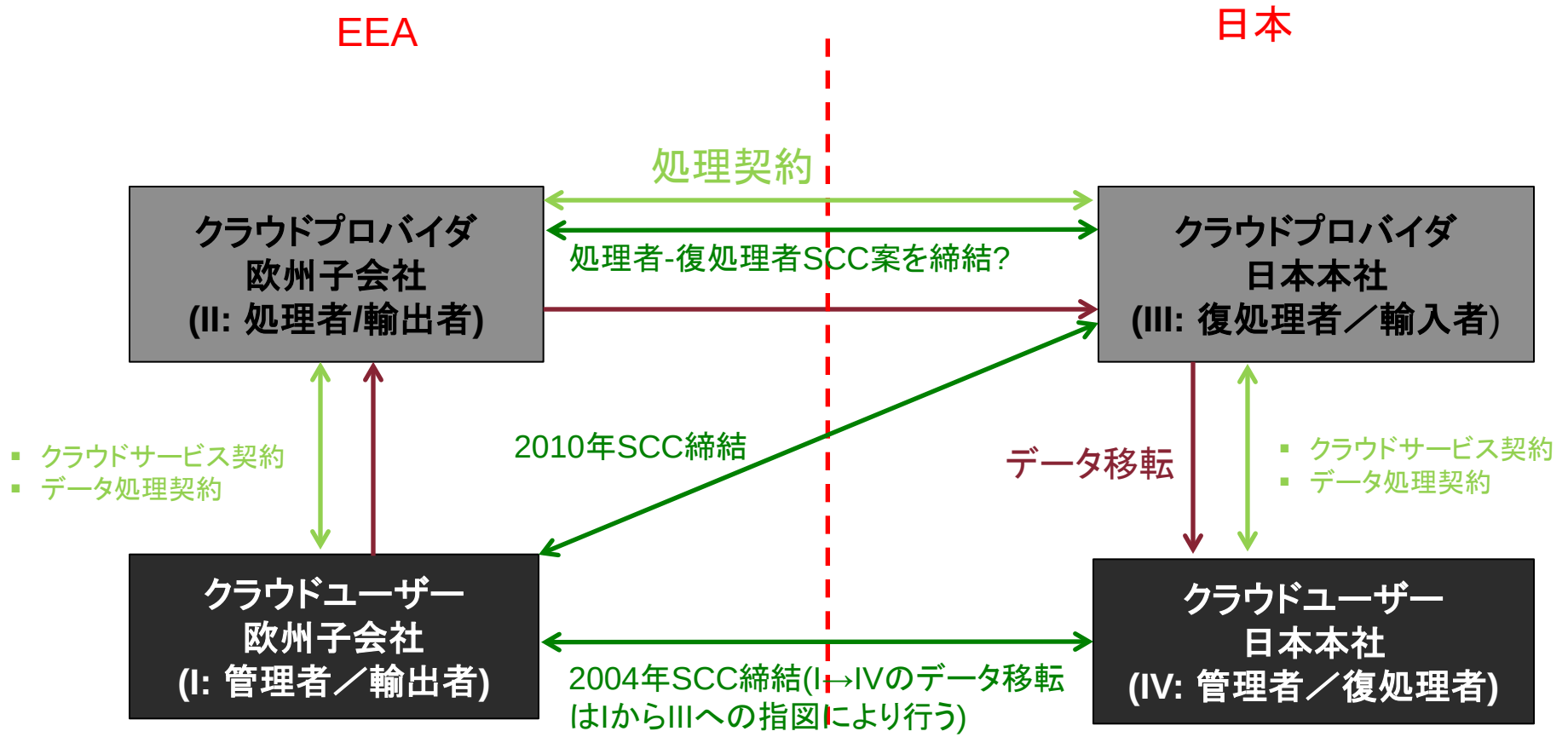


EEAからデータを送る者を輸出者、EEAからデータを受け取る者を輸入者とするのが簡便

SCCによる複数当事者間のデータ移転：タイプB

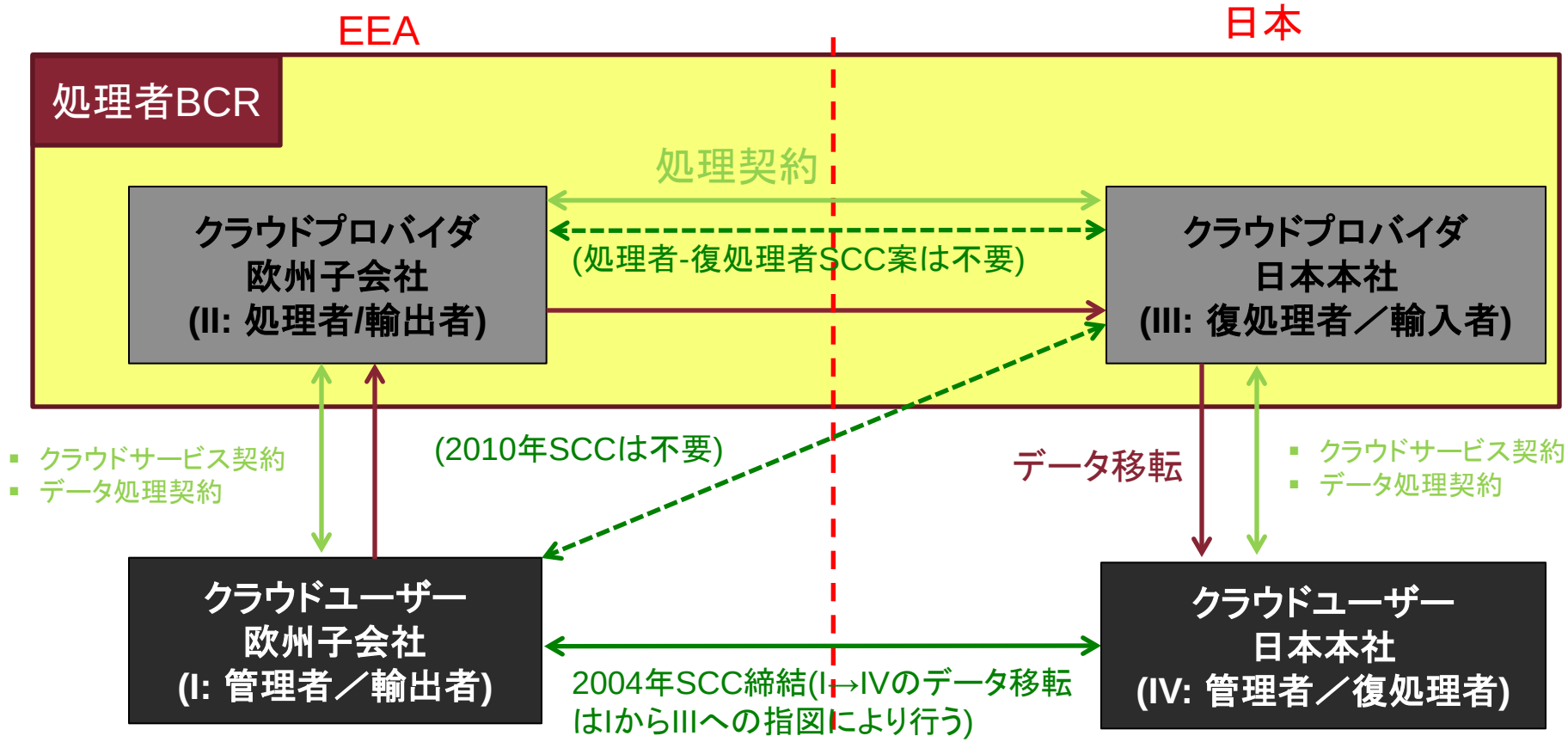


クラウドサービスプロバイダを通じてデータ移転を行う場合(処理者BCRなし)



クラウドサービスプロバイダを通じてデータ移転を行う場合(処理者BCRあり)

- 監督機関の視点からはBCRを取得し高いデータ保護基準を満たすクラウドプロバイダにGDPRを執行するのは比較的困難。執行リスクの点で処理者BCRを取得したクラウドを使うメリットは大きい（GDPRを遵守した処理者を使用するメリット）



SCC: 処理行為の登録

- フランス、ベルギー、オランダ等の加盟国においては、企業は監督機関に対し処理行為の登録を行う必要がある。処理行為の監督機関への登録がなされていない段階で、SCCを監督機関に通知するか、SCCを個人データの移転のために使用することへの監督機関の承認を求めることは、監督機関が処理行為を調査することにつながり得、執行リスクを増大させる。
- 但し、処理行為の監督機関への登録の制度はGDPRでは廃止される見込みであるため、指令の下での多少の執行リスクを取れるのであれば、処理行為の登録を行わない選択肢も一応ありうる。

フランス	オランダ	ベルギー
オンラインで、フランス語で届け出る データ処理の目的毎に一つの通知が必要だが、監督機関は、一般的なデータ処理の数カテゴリーに簡略化された基準を作成している。企業がこの基準に遵守すれば、コンプライアンス認証に署名し監督機関に送付するだけで良い。 書類はオンライン登録する。監督機関は最終版の申告書の提出直後に電子受領書を発行する。 監督機関は遅くとも完成したファイルの受領から1週間以内に問題なしとのシグナルを送る センシティブデータについては事前承認が必要。その場合、監督機関は4ヶ月以内に決定を行う	オランダ語のオンラインフォームを届け出る 顧客データベース、調査、人事などに関する様々な処理について通知義務が免除されている。 このプロセスには6週間から10週間かかる	フランス語/オランダ語/ドイツ語のオンラインフォームを届け出る ある処理行為は、例えば、顧客データベースや人事との関係で、さらなる要件に服するが、通知義務を免除される 監督機関は21日以内に通知のコピーを送付する

SCC: SCC使用の監督機関への事前通知

- ベルギーのような幾つかの加盟国ではSCCの使用に先立って監督機関への通知が必要である
- その結果、企業は各加盟国における要件をチェックし、EEA域外へ個人データを移転させる前に全ての関連する監督機関（義務がある場合）に対しSCCを通知する必要がある
- 例えば、ベルギーにおける手続は以下のようなものである
  - SCCはベルギーの監督機関にEメールで送らなければならない
  - SCCが修正されなかった場合、ベルギーの監督機関は自動的にSCCが要件を満たしたものと結論付ける
    - 監督機関は企業に対しSCCが欧州委員会に採択されたものに一致したことを確認するために企業に通知する
    - 当該通知の日から移転は許可されるものと考えられる
    - 当該レターのコピーが法務省に送付される
  - ベルギーの監督機関は手続の長さに関して何の情報も提供していないが、SCCが変更されている場合に60日以内に監督機関が意見を出すことを考慮すると、当該手続は迅速であるはず。

SCC: SCC使用の事前承認取得

- フランスのような加盟国では監督機関のSCC使用に関する事前承認を取得する必要がある
- その結果、企業は加盟国における要件をチェックし、EEA外に個人データを移転させる前に関連する監督機関からのSCCへの承認を取得する必要がある
- 例えば、フランスの事前承認手続は以下のようなものである
  - データ処理を登録するとき、データ管理者は、SCCによって移転が法的に正当化されることを述べるボックスにチェックする短いデータ移転の別紙の記入をする必要がある
  - 実際のSCCは監督機関に提出する必要はないが、個別の要請があった場合に監督機関に提出する
  - 監督機関は完成したファイルを受領したときから決定を行うまで2ヶ月間(一度2ヶ月間の更新が可能)かけることができる
  - 監督機関から何の連絡もない場合は承認申請の拒否とみなされる

BCRの取得

- より多くの企業がBCRを申請し、申請を検討している
  - SCCの加盟国毎の要件を回避するための一つの方法
  - 仮に、世界中のグループ内で大量の個人データの移転を行っていることがデータマッピングの結果明らかになった場合には、複数のSCCに替えてBCRの取得を検討することができる
  - 厳密には、現行指令の下では、EEA内の21の国（オーストリア、ベルギー、ブルガリア、キプロス、チェコ共和国、エストニア、フランス、ドイツ、アイスランド、アイルランド、イタリア、ラトビア、リヒテンシュタイン、ルクセンブルグ、マルタ、オランダ、ノルウェー、スロバキア、スロベニア、スペインおよび英国）がBCRの相互認証手続（Mutual Recognition Procedure）に加盟しており、これらの国の監督機関のいずれかを主要監督機関として承認を受けたBCRの取得企業グループ内では、上記21の国々からEEA域外への個人データ移転をBCRによって適法に行うことができることになる。BCRの取得企業が、上記21の国々以外のEEA加盟国からEEA域外への個人データ移転を当該BCRによって行う場合、当該EEA加盟国の監督機関から個別に当該BCRの審査を受け承認を受ける必要がある。
- デュッセルドルフ、英国、オランダの監督機関はBCRの審査を合理的なファーストドラフトの提出から1年以内に完了させる立場である。
  - しかし、実際には、GDPRの効力発生が近づくにつれ、監督機関におけるBCRの審査のリソースは不足気味になっているように見受けられる。
- 英国の監督機関に対しBCRの承認を申請するかどうかを現在検討している英国における企業は、英国に欧州統括拠点を有する企業のBCR申請（すなわち、他の監督機関の中での協力手続をハンドルする監督機関）をレビューするにあたっての英国の監督機関による「主要当局」としての役割について不確実性があることを念頭におくべきである。仮に、当該承認が英国がEUを離脱する前に与えられなかった場合、当該「主要当局」の役割は異なる監督機関に移転される必要がありうる。これらの論点は英国の監督機関及び他の関連する監督機関と議論するべきである

GDPR下でのSCCやBCR

- SCC
  - GDPRでは、処理行為の登録の制度は廃止され、これに代わり、管理者・処理者が処理行為の記録を残す義務（第30条）が課せられるようになると説明されている。
  - SCCの事前通知・事前承認取得の手続も廃止される。
    - 但し、データ保護影響評価（第35条）の高リスクの一類型として、SCCによる越境データ移転が規定されないかは要注意。規定された場合、データ保護影響評価の結果が高リスクの場合、監督機関への事前協議（第36条）が必要となる
- BCR
  - GDPR適用開始後は、相互認証手続への加盟の有無にかかわらずEEA域内のどの国からの個人データ移転もBCR取得企業グループ内ではBCRに基づいて適法に行うことができることになる

同意によって従業員データを移転させる

- 多くの会社は従業員の同意に基づきEEA外へ従業員の個人データを移転させることを求める
  - データ主体の同意は自由に与えられ、個別の、情報に基づく、不明瞭ではないものであり、さらに明示的である必要がある
  - 同意は個別になされなければならないため、長く複雑な就業規則において個人データの移転に対する従業員の同意を得ることは同意の要件を満たさない可能性が高い
  - 従業員の同意の取得にあたっては、区別された別個のフォームを使うことが薦められる
  - 同意は非常に制限的である
    - データ主体がいつでも同意を撤回できる。
    - 企業は関係する全ての人から同意を取得する必要がある
    - 繰り返し行なわれ、大量で、かつ構造的であると認められる可能性がある個人データの移転は、可能であればSCCやBCRのような適切な保護措置の下で行なわれるべきである(WP114. p.9参照)

セーフハーバー/プライバシー・シールドとは？

- 欧州委員会は、2000年のセーフハーバー決定において、米国商務省により提供される「セーフハーバー・プライバシー原則」が、EUから米国に拠点を置く組織に移転される個人データに対して、当該組織が当該条件を満たすことを前提に、十分なレベルの保護を確保すると判断した。
- 2015年10月6日、**Schrems判決において欧州連合司法裁判所(European Court of Justice. "ECJ")はセーフハーバーを無効とした。**
- 2016年2月2日、EUと米国は「**EU-米国間のプライバシー・シールド**」と呼ばれるセーフハーバー決定の後継についての政治的合意に至った。
- 2016年4月13日、第29条作業部会はプライバシー・シールドについての意見を発表し、商業的な面と移転されたデータへの公共のアクセスの両方に強い懸念を示した(WP238)
- 2016年5月26日、欧州議会はプライバシー・シールドについて再度検討するよう欧州委員会に命じた。
- 同年6月8日、欧州データ保護監視官局はプライバシー・シールドは十分堅固でないと発言した。欧州委員会は、プライバシー・シールドに監督機関からのレコメンデーションを含める形で、内容の修正を行った。
- 2016年7月12日、欧州委員会が**EU-米国間のプライバシーシールドの十分性決定**を採択、同年8月1日利用開始
  - プライバシーシールドにより米国企業はEUから米国への個人データ移転を一定の条件の下で自由に行うことができることになった。
  - しかし、Schrems判決においてECJがセーフハーバーを無効とする理由として指摘した米国政府の諜報機関等が民間企業からの国家安全保障を図る目的で個人データを大規模取得することを可能とする米国の法制は特に改正されていない。
  - プライバシーシールドによるデータ移転の有効性が監督機関の調査の対象となり、さらにECJにおいてプライバシーシールド自体の有効性について判断が下される。
  - したがって、日本企業は、プライバシーシールド以外の他の適切な保護措置(SCCやBCR)を使用してEUから米国へのデータ移転を行うことが望ましい。

十分性認定の取得

- 当面の間、日本企業・日本の事業者団体・公的機関は十分性の認定の取得という選択肢を頼りにすべきではない。
  - 日本はまだ欧州委員会による十分性決定を受けていない。
    - 日本政府は、欧州委員会と非公式な予備的接触を始めており、精力的に情報交換を行っている。在ブリュッセルの欧州連合日本政府代表部と欧州委員会の各担当者との関係は良好であるように見える。
  - 日本はまだ欧州委員会に対し十分性審査の申請を行っていない。
  - 日本は、EU法である指令及びGDPR並びに過去の欧州委員会の十分性決定の実例を踏まえて、日本の個人情報保護制度を分析し、その分析結果に基づいて、欧州委員会から十分性認定の決定を受けられるよう、必要な法改正を行うべきである。
  - 国会での可決に向けた法案の内容が固まると同時に、欧州委員会に対し当該法案の説明を非公式な接触の中で行い、先方の感触を探り、その後、正式な申請(特段の様式はない)を行う。最近の例では決定が出るまで3年半から4年かかっている。

II. 最近のEUデータ保護法分野での執行動向

ハンブルグ監督機関によるデータ移転規制違反に基づく制裁金賦課の実例（2016年6月）

- 2016年6月6日、ハンブルグの監督機関は、米国-EU間のセーフハーバー決定が無効となった後に、早期に代替手段となる法的手法を取らず、**違法に米国へ従業員及び顧客に関する個人データを移転した**として、Adobe Systems、Punica (フルーツジュースメーカー。PepsiCo Inc.の関連会社)、Unileverにそれぞれ€8000、€9000、€11000の**制裁金を課した。**
  - ハンブルグ監督機関は、上記セーフハーバーが無効となった後、米国親会社を持ち、かつ北部ドイツ州に拠点のある企業によるデータ移転の実務について調査を行っていた。調査の結果、これらの企業のうち圧倒的多数の企業が、上記セーフハーバーが無効となった後の6ヶ月間の経過期間の間に、データ移転の実務をSCCに基づくものに変えていたことが分かった。
- 日本企業は、現段階において何らの適切な保護措置を取らずにEEA域内から日本へ個人データ移転を行うことには、現行法に基づき、監督機関によって制裁金が課されるリスクがあることを十分に認識する必要がある。
  - 現行法下では、制裁金の額は少額に留まると思われるが、執行を受けた場合には全世界のメディアで広く報道されることが予想される(風評リスク)。
  - 現行法下で執行を受けた場合には、GDPR適用開始後に再度、監督機関による調査の対象になるおそれ(風評リスク＋調査対応のコスト)。

10のドイツのデータ保護機関による越境データ移転への連携された書面監査・評価（2016年11月）

- 2016年11月3日付けバイエルン州のデータ保護機関のプレスリリースによれば、
  - 10のドイツのデータ保護機関が、越境データ移転、すなわち非EU加盟国への移転に関する連携された書面監査・評価を開始した。
  - 500社のドイツ企業は、当該企業によるEU域外の国への個人データの越境移転の詳細に関する包括的な質問状に回答することを要請されることになる。

バイエルン州の監督機関による当該監査の動機の一つはクラウドコンピューティングサービスによる個人データの越境移転への懸念である。

- 「近年、私企業における個人データの越境移転の数が大幅に増大した。こうした展開の理由の一つは、経済のグローバル化といわゆるクラウドコンピューティングというサービスおよび商品の継続的な普及である。ドイツにおける中小企業でさえも、（例えば、顧客、従業員または応募者の）個人データの移転のため多くのクラウドコンピューティングに関する外部サービスを使用している。」
- 「しかしながら、こうしたクラウドコンピューティングサービスの多くは、米国企業によって提供されている。従って、通常、当該サービスは個人データの米国および/または非EU加盟国への越境移転を必要とする。ドイツのデータ保護機関の経験は、これまでのところ、企業はそうした商品の使用により個人データの非EU加盟国への越境移転が生じているという事実に常に気がついているわけではないことを示している。」

バイエルンデータ保護コミッショナーの声明

- 「中小企業にとってさえもEU域外の国への個人データの移転は、特に増大する市場におけるクラウドコンピューティングソリューションに鑑みれば、通常業務の一部である。しかしながら、企業は個別のデータ保護に関連する要件を遵守しなければならないことに気がつく必要がある。10のドイツのデータ保護機関による現在の連携された監査の目的の一つは、企業によるこの分野での認知度を高めることにある。質問状への回答によっては、バイエルン監督機関は必要な場合にはより詳細な評価を実行する。」

質問状への対応は慎重に

- 質問状を受け取った企業は当該質問状を真剣に処理する必要がある。
- 質問状への誤った回答はより包括的なかつ完全なデータ保護機関による調査につながる可能性がある。
- ドイツのデータ保護法（Bundesdatenschutzgesetz – BDSG）の条項の違反がデータ保護機関に検知された場合、300,000ユーロ以下の制裁金の賦課につながる可能性がある。

III. 結論

日本企業のベルギー子会社・ベルギー支店が取っておくべきEU一般データ保護規則へのコンプライアンス対応

- 本社からGDPR対応に関して連絡がない場合、本社に対して対応を促す。
- 本社と連携して以下の事項に対応することが望ましい
  - データマッピングの質問票への回答
  - データ保護方針の制定・施行、そして遵守
  - 現在使用している委託先（クラウドコンピューティングサービスを含む）がGDPRを遵守しているか否かのチェック
  - 処理行為の記録保持の方法の検討
    - 特別カテゴリーの個人データの処理を行っている場合
  - データ保護責任者の選任義務がないかについてウォッチ
    - 2016年中に公表される作業部会のガイドラインに注目
  - データ保護影響評価が必要な場合がないかについてウォッチ
    - 2017年初めに公表される作業部会のガイドラインに注目
  - 事業所のITセキュリティがGDPRの基準を満たしているかのアセスメント
    - IIJ Europe等の日系企業がGDPRのITソリューションを提供しており必要に応じて使用する
  - 事業所で処理する個人データが漏洩した場合に監督機関へ通知する体制を整える。
  - データ主体の苦情に対応することができるように内部の苦情対応手続の確認
  - 本社との標準契約条項の締結
    - ベルギーのデータ保護監督当局へのSCCの事前届出、処理行為の登録も行う

結論：制裁金の算定基準を踏まえるとGDPRへの遵守努力は制裁金減免のため重要

- GDPRコンプライアンスは日本企業にとって短期的にはコストであるが、中長期的には、制裁金の減免を得ることにつながる、何億円、何十億円という利益が制裁金支払いによって消えてしまわないように先手を打つという積極的な投資である。
  - 制裁金を課すかどうか、またその金額についての判断を行なう場合には以下を十分に考慮すること(第83条第2項)
    - 侵害の性質、重大さ及び期間
    - 違反の故意性又は過失性
    - データ主体の被った損害を緩和するために講じた措置
    - 実施された技術的・組織的対策
    - 関連する以前の違反
    - 違反を救済するための監督機関との協力の程度
    - 違反によって影響を受けた個人データのカテゴリー
    - 監督機関が違反を知ることになった経緯
    - 監督機関から警告を受けていたかどうか
    - 承認された行動規範・認証の遵守
    - その他の悪化又は緩和要因

講師紹介

ウィルマーヘイル法律事務所ブリュッセルオフィス・シニアアソシエイト

弁護士　杉本　武重　(ブリュッセル(準会員)、日本国、米国NY州)

略歴：2004年3月慶應義塾大学法学部法律学科卒業、2006年10月長島・大野・常松法律事務所入所。2012年6月シカゴ大学ロースクール法学修士課程卒業(LL.M)、2013年7月オックスフォード大学法学部法学修士課程卒業(Magister Juris)、2013年8月ウィルマーヘイル法律事務所入所、同事務所ブリュッセルオフィス・アソシエイト。2015年1月から同オフィス・シニアアソシエイト、デュッセルドルフ日本商工会議所法務委員会専門委員就任(2016年度のEUの一般データ保護規則のセミナーを担当)

主な取扱分野：EUデータ保護法(日本企業向けの一般データ保護規則のコンプライアンス対応等)、EUカルテル規制(国際カルテル事件における日本企業を代理した欧州委員会対応等)、EU企業結合規制及び標準必須特許問題を含むEU競争法全般

最近の主要講演：

- 日本貿易振興機構（ジェトロ）主催セミナー「EU・英国最新経済動向セミナー－ジェトロ事務所長による現地事情報告を中心に－」において「日本企業のEU一般データ保護規則への対応」と題する講演（東京・2016年12月7日）
- 日本経済団体連合会情報通信企画部会にて「EU一般データ保護規則が企業に与える影響」と題する講演（東京・2016年7月26日）
- 在英日本商工会議所主催「JCCI法務セミナー」にて「EUの一般データ保護規則」に関する講演(ロンドン・2016年7月7日)
- 在蘭日本商工会議所、ジェトロ・アムステルダム事務所、当事務所共催「EUの一般データ保護規則」に関するセミナーにて講演(アムステルダム・2016年6月29日)
- 在仏日本商工会議所主催「実務セミナー」にて「EUの一般データ保護規則」に関する講演(パリ・2016年6月15日)
- 日本貿易振興機構(ジェトロ)ロンドン事務所主催セミナーにおいて「EUのデータ保護法について」と題する講演(ロンドン・2016年5月4日)
- デュッセルドルフ日本商工会議所法務委員会主催セミナーにて「EUの一般データ保護規則」と題する講演(デュッセルドルフ・2016年4月15日)