ashurst

英EU企業実務セミナー
データ保護：UK/EU GDPR

岩村浩幸
パートナー弁護士
アシャースト法律事務所

2021年2月29日

自己紹介

- アシャースト法律事務所ロンドンオフィス　コーポレート部門　パートナー
- 資格
  - 2003年米国法弁護士（NY州及びNJ州）
  - 2005年英国法弁護士（英国及びウェールズ）
- 専門
  - 会社法全般（M&A、組織再編、会社清算、一般契約書のレビュー）
  - 紛争解決（海外における訴訟対応）
  - Brexit関連のアドバイス
  - コンプライアンス（GDPR、競争法、贈収賄法、雇用法　等）

ashurst

アジェンダ

- GDPRの基礎
- GDPRの下での域外移転規則の基本
- 新SCCの概要と対策
- Brexitの影響

GDPRの基礎

- GDPRは英国のEU離脱法に基づいて、UK GDPRとして内容がほぼ同じまま英国で適用されている
- 基本的なルールは変わらない
  - 情報処理の際は第5条の6原則の順守
    - 情報処理にあたっては情報主体者への通知、目的外利用の禁止　等
  - 合法性の確保
    - 例：従業員からの同意は無効、CCTVの利用
  - 域外移転にあたっては何らかの施策が必要（十分性認定、SCC、BCR）
  - 漏洩の際の72時間以内の当局への通知
  - 情報処理の記録
  - DPO/Representativeの任命
  - 域外適用
- ただし、英国がEU加盟国で無くなったことにより、注意するべき点がある
  - 個人情報の域外移転
  - Representativeの任命
- プライバシーポリシーなどの修正は行うべき

GDPRの基礎 - 用語の説明

- Controller: natural or legal person which determines the purposes and means of processing of personal data
  情報管理者：個人又は法人で、個人情報の処理の目的や方法を決定する者
- Processor: natural or legal person which processes personal data on behalf of the controller
  情報処理者：個人又は法人で情報管理者のために情報を処理する者
- Data Subject: Individuals whose personal data are being processed
  情報主体者：個人情報が属する個人
- Personal data: any information relating to an identified or identifiable natural person
  個人情報：特定できる自然人に関する全ての情報
  - An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, ID number, location data, online ID, factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.
    特定できる個人とは、名前、認識番号、位置情報、オンラインID、その他身体的・精神的、文化的・社会的な情報に基づいて、直接的又は間接的に識別がされうる個人
- Processing: any operation or set of operations performed on personal data whether or not by automated means
  処理：自動的であるか無いかに関わらず個人情報に対して行われる操作
  - Collection, recording, organisation, structuring, storage, adaptation, alteration…
    収集、記録、整頓、整理、保管、変更、読出、使用、開示、削除…
- Filing System: any structured set of personal data accessible according to specific criteria
  ファイリングシステム：特定の基準に基いてアクセスされうる、整理された個人情報の集合体

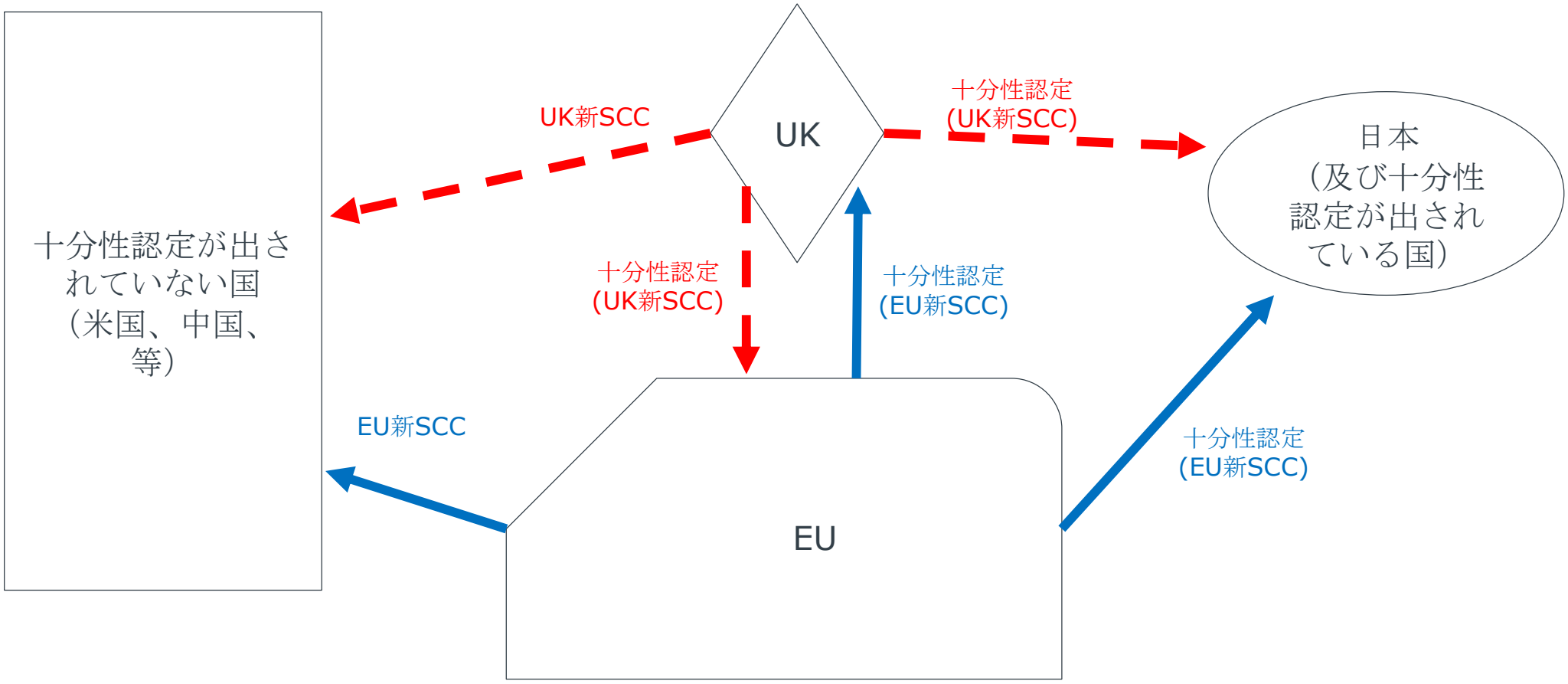
ashurst

GDPRにおける域外移転の禁止概要

- GDPR 第44条ではEU域外の第三国への個人情報の移転が原則禁止されている
- この「原則」を回避するために、企業に与えられている一般的な手段は以下の通り:
  - 十分性認定に依拠した個人情報の移転:
    - EU域外の第三国による個人情報保護法制度が十分であるとの欧州委員会による認定
    - 日本とUKを含む13か国に十分性認定が出されている
    - 米国や中国、東南アジアのほとんどの国に対しては十分性認定は出されていない
    - 日系企業が海外の子会社・兄弟会社間で情報共有を行う際には十分性認定だけに頼ることは困難
    - 国によっては補完的なルールに従うことを求められる場合もある(日本)
    - 期限が決められている場合もある(英国)
  - グループ企業間が結ぶ社内ポリシーに従って行われる個人情報の移転(Binding Corporate Rules、以下「BCR」という。)
    - ポリシーの文言の内容を比較的自由に当事者が決定することができる
    - 文言はEU加盟国の個人情報保護当局により承認されなければならず、一般的に承認手続きには十数か月から数年かかる(すなわちコストが莫大にかかる)
    - 様々な当局からかなり細かい文言に対するチェックが入るために、自社が最初に提案した文言でポリシーが作成できることはない
    - 後日ポリシーの内容を変更する際にも当局からの承認が必要となるため、継続的にコストが発生する
  - 域内の情報の移転元(以下「Exporter」という。)と域外の移転先(以下「Importer」という。)の間で欧州委員会が認めた文言に基づいて結ばれた契約(以下「SCC」という。)に従った個人情報の移転
    - 情報の移転に関してGDPRに準ずる、SCCに記載されている義務を守ることが求められる
    - 域内の情報主体者は、被害を被った際にImporterとExporterに対して域内の機関や裁判所を通じて救済を求めることができる
    - SCCの締結には当局からの承認は必要なく、コストと時間は主にSCC導入のために必要となる情報収集に関するもの
- 企業などの移転において同意に基づいて行われることはあくまでも例外(第49条)

ashurst

EU/英国からの域外移転の施策



ashurst

欧州委員会が発表した新たなSCC

- 以前は、1995年のData Protection Directive（情報保護指令、以下「DPD」という。）に基づいて発表されたSCCが二種類存在した：
  - 2001年：コントローラーからコントローラーへの移転に利用するもの
  - 2010年：コントローラーからプロセッサーへの移転に利用するもの
    （以下まとめて「旧SCC」という。）
- DPDがGDPRへと改正されて以来、旧SCCの改正が近々なされることが予想されていた
- 2020年7月の欧州司法裁判所によるSchrems II事件の判決
  - 旧SCCの基本的な有効性自体は否定しない
  - 特定の国への個人情報の移転は、当該国の公的機関による情報の傍受や不当な開示命令などにより、個人情報が適切に取り扱われないという危険が存在する
  - 旧SCC（及びBCR）を利用してそのようなリスクが存在する第三国に対して個人情報を移転する際には、特別の施策を設けることが望ましい
- 新SCCの条文は、Schrems II事件の判決及びその後にEU全体の個人情報管轄機関であるEuropean Data Protection Board（以下「EDPB」という。）の意見を反映したもの

旧SCCを利用している日系企業は新SCCに基づいた再締結が求められる

ashurst

新SCCの特徴 (1/3)

- 複数の当事者間で結ぶことが想定されている
- 当事者の役割ごとに異なったモジュールが含まれており、それに対応したモジュールを選択する形となっている

	Exporter	Importer	使用例
モジュール1	コントローラー	コントローラー	グループ会社間の従業員・顧客情報の共有
モジュール2	コントローラー	プロセッサー	域外のサービスプロバイダー、クラウド業者等との契約
モジュール3	プロセッサー	プロセッサー	域内のサービスプロバイダーから域外のサブプロセッサーへの情報移転
モジュール4	プロセッサー	コントローラー	日本の会社が域内の会社に情報収集を求める場合（EUでの治験等）

- 契約当事者の義務はGDPRに含まれているものから抜粋されたもの
  - 例：コントローラーであるImporterの義務（モジュール1）
    - 目的内利用 (purpose limitation)
    - 情報主体者への情報提供 (transparency)
    - 正確性の担保と必要な情報のみの入手 (accuracy and data minimisation)
    - 適切な技術的・組織的な施策 (security of processing)
    - 処理の記録と要請に応じた開示 (documentation and compliance)
    - 情報主体者からの要求への迅速な対応 (data subject rights) 等

ashurst

新SCCの特徴 (2/3)

- 基本的にはEU域外に設立されているImporterもEUの当局または裁判所の管轄、およびEU加盟国の準拠法に同意することが求められる
  - コストを引き受けることでそれ以外の紛争解決機関での問題解決を情報主体者に申し出ることもできる
- 第三国の公的機関により、個人情報の適切な処理が妨げられると信じる理由がないことを当事者が補償することが求めらている
  - 対象国の法律や慣行、処理の目的などを検討して判断を行い、その判断を書面に残すことが求められる
- 2022年12月27日までに新SCCに移行することが求められている
  - 2021年6月4日：決定の発表・OJEUに掲載
  - 2021年6月27日：発行日（JEEU掲載から20日後）
  - 2021年9月27日：旧SCCが撤廃（発行から3か月後）（新規に結ぶことは認められないが既存の仕組みは継続して利用が可能）
  - 2022年12月27日：新SCCへの置き換えの期限（旧SCC撤廃から15か月後）

ashurst

新SCCの特徴 (3/3)

- 添付資料には以下のような情報を含めることが求められている
  - Annex 1：それぞれの移転に関して情報が明らかに区別することができ、かつ当事者のそれぞれの役割が明確にされなければならない。
    - A:当事者の情報
      - Exporter及びImporterそれぞれに関して、名前、住所、コンタクトパーソンの名前・役職・連絡先、転送される情報に関わる活動、署名・日時
    - B:移転の詳細
      - 個人情報が移転される情報主体者の種類
      - 移転される情報の種類
      - 移転される特別な情報とそれに関わり設けられる制限・施策
      - 移転の頻度
      - 処理の特性
      - 移転の目的と、さらなる処理
      - 個人情報が保持される期間又は期間を決定するために利用される基準
      - プロセッサー・サブプロセッサーへの移転に関しては、処理の主題、特質及び期間
    - C:適切な管轄機関（モジュール１～３のみ）
  - Annex 2:技術的・組織的な施策（情報のセキュリティーを確保するためのものも含む）（モジュール１～３のみ）
    - 具体的（一般的でなく）な技術的・組織的施策の説明が求められる上に、それぞれの移転にどの施策が利用されているかを明らかに示さなければならない。
    - Importerにより、適切なレベルのセキュリティーを確保するために設けられている技術的・組織的な施策の説明（匿名化の施策、秘匿性を確保するための施策、事故の際に速やかに個人情報へのアクセスを復帰することを確実にするための施策等）
    - プロセッサー・サブプロセッサーへの移転に関しては、プロセッサー・サブプロセッサーがExporterへとアシスタンスを提供するための特定の技術的・組織的な施策の記載
  - Annex 3: サブプロセッサーのリスト（モジュール2・3で、サブプロセッサーの利用に関して特定の承認を求めることになっている際のみ使用）

ashurst

Brexitの影響

- Brexitの結果、UKからの個人情報の域外移転の施策として新SCCを利用することはできない
- 英国からEU加盟国への情報移転については英国がEU加盟国に対して出している十分性認定に依拠して行うことができる
  - 欧州委員会が既に他の12か国（日本含む）に対して出している十分性認定は英国政府により引き継がれている
- EU加盟国から英国への情報移転についても欧州委員会が発表した英国に対する十分性認定に基づいて行うことができる
  - 4年後に自動的に効力が切れるために、欧州委員会が再度認定のプロセスを行わなければならない（sunset clause)
- 英国の情報保護当局であるInformation Commissioner's Office (ICO)はUK独自のSCCを検討中であり、夏には発表したいと述べている
- それまでは旧SCCを継続して利用できることができる（EUが定めた期限は関係ない）

ashurst

新SCC締結に向けた対応策

1. 英国とEU加盟国に居住する情報主体者（従業員、顧客など）の個人情報を処理している会社の洗い出し
2. 移転されている情報の分析
   - 新SCCのAnnexに基づいて分析
3. 情報処理に関わる当事者の役割の分析
   - プロセッサーかコントローラーか？ImporterかExporterか？外部か内部か？
4. 当事者と情報の組み合わせに基づいて、適切な新SCCにおけるモジュールの検討
5. 新SCCで求められている義務・役割の各当事者への説明と、必要に応じた体制の構築
6. 新SCCの締結
   - Annex 1にすべてのImporterとExporterを列挙
   - それぞれの権限を有する者がAnnex 1のコピーにサイン

まとめ

- 旧SCCを新SCCに置き換える期限は2022年末であるために、時間的な余裕はある
- ただし、情報収集や特定の国での展開（Works councilがあるような国）では時間がかかる可能性があるために、時間に余裕をもって準備を行うことが推奨される
- 日本及び英国への移転については十分性認定に基づいて行うことができるが、それぞれのデメリットも理解するべき
  - 日本：補完的ルールの順守
  - 英国：4年後に自動的に切れるというリスク
    - ただし新SCCの下で課せられるImporterとしての義務を鑑みるに、新SCCに従うほうがコンプライアンスの負担は大きいと思われる
- GDPRの施行から5年、適用開始から3年たった今、全体的なコンプライアンスの状況の監査と絡めてBrexit対応と新SCCの準備を行うことが推奨される

ashurst

ご視聴有難うございました

岩村浩幸（英国・米国弁護士）

アシャースト法律事務所
E-mail: hiroyuki.iwamura@ashurst.com
電話番号：+44 (0)207-859-3244
携帯：+44 (0)780-920-0318

ashurst

aQ Legal and Business Skills 35120886

7_1

ashurst