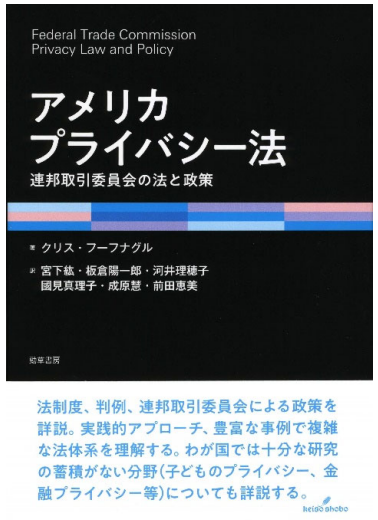
越境プライバシールール（CBPR）の展開と展望

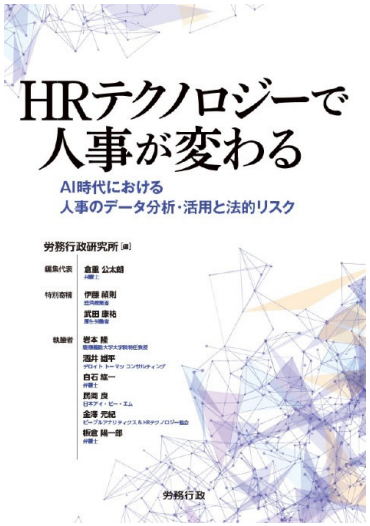
弁護士・ひかり総合法律事務所
理化学研究所革新知能統合研究センター客員主管研究員
国立情報学研究所客員教授
大阪大学社会技術共創研究センター招へい教授
板倉陽一郎

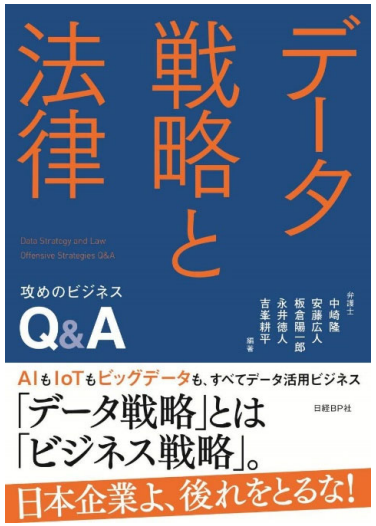
自己紹介

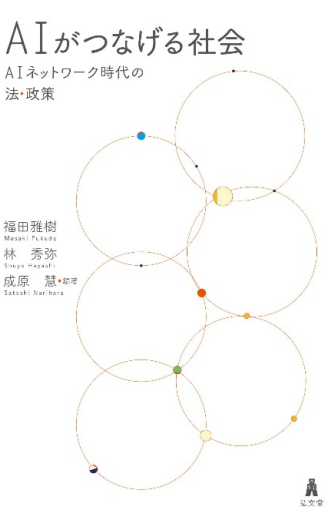
- 2002年慶應義塾大学総合政策学部卒，2004年京都大学大学院情報学研究科社会情報学専攻修士課程修了，2007年慶應義塾大学法務研究科（法科大学院）修了。2008年弁護士（ひかり総合法律事務所）。2016年4月よりパートナー弁護士。
- 2010年4月より2012年12月まで消費者庁に出向（消費者制度課個人情報保護推進室（現・個人情報保護委員会事務局）政策企画専門官）。2017年4月より理化学研究所革新知能統合研究センター社会における人工知能研究グループ客員主管研究員，2018年5月より国立情報学研究所客員教授。2020年5月より大阪大学社会技術共創研究センター招へい教授。2021年4月より国立がん研究センター研究所医療AI研究開発分野客員研究員。
- 消費者庁・デジタル・プラットフォーム企業が介在する消費者取引における環境整備等に関する検討会委員、総務省・情報通信法学研究会構成員、IoT推進コンソーシアム・データ流通促進ＷＧ委員等。
- 日弁連消費者問題対策委員会副委員長（電子商取引・通信ネットワーク部会長），法とコンピュータ学会理事、日本メディカルＡＩ学会監事、一般社団法人データ社会推進協議会監事等。

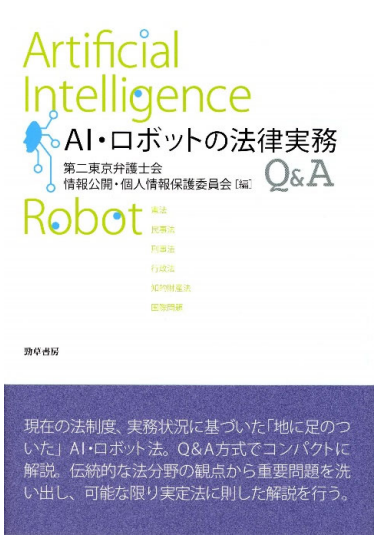
近著


Federal Trade Commission
Privacy Law and Policy
アメリカ
プライバシー法
連邦取引委員会の法と政策
クリス・フーフナグル
宮下紘・板倉陽一郎・河井理穂子
國見真理子・成原慧・前田恵美
法制度、判例、連邦取引委員会による政策を詳説。実践的アプローチ、豊富な事例で複雑な法体系を理解する。わが国では十分な研究の蓄積がない分野(子どものプライバシー、金融プライバシー等)についても詳説する。

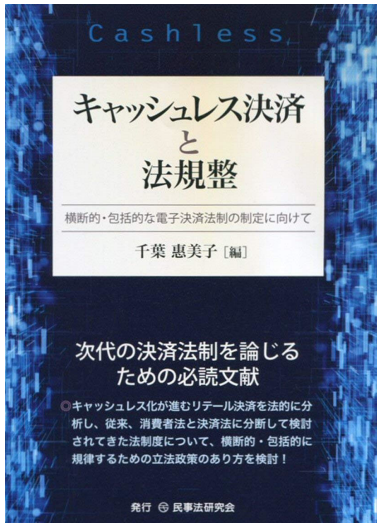

HRテクノロジーで
人事が変わる
AI時代における
人事のデータ分析・活用と法的リスク
労務行政研究所 [編]
労務行政


データ
戦略と
法律
Data Strategy and Law
Offensive Strategies Q&A
攻めのビジネス
Q&A
中崎隆
安藤広人
板倉陽一郎
永井徳人
吉峯耕平
AIもIoTもビッグデータも、すべてデータ活用ビジネス
「データ戦略」とは
「ビジネス戦略」。
日経BP社
日本企業よ、後れをとるな!


AIがつなげる社会
AIネットワーク時代の
法・政策
福田雅樹
林 秀弥
成原 慧


Artificial
Intelligence
Robot
AI・ロボットの法律実務
第二東京弁護士会
情報公開・個人情報保護委員会 [編]
Q&A
勁草書房
現在の法制度、実務状況に基づいた「地に足のついた」AI・ロボット法。Q&A方式でコンパクトに解説。伝統的な法分野の観点から重要問題を洗い出し、可能な限り実定法に則した解説を行う。

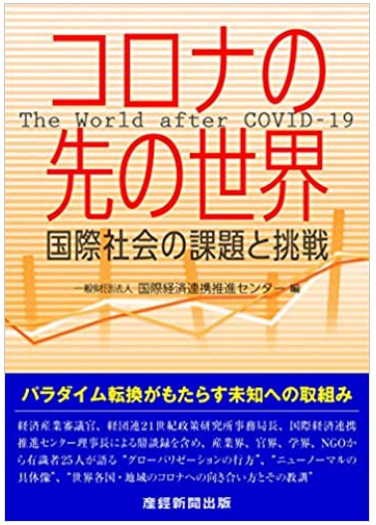

これだけで
わかる!
医療
AI
井川房夫
藤田広志
AI知らずに大丈夫!?
AIは既に、医療者誰しもが無視できないツールです。
医療現場に必要なAIの基本的知識から実際の活用方法まで、やさしく解説しました。
何から手をつけていいかわからない人、まずは本書を開いてみてください。
このまま知らないふり,できますか?
中外医学社


Cashless
キャッシュレス決済
と
法規整
横断的・包括的な電子決済法制の制定に向けて
千葉 惠美子 [編]
次代の決済法制を論じるための必読文献
キャッシュレス化が進むリテール決済を法的に分析し、従来、消費者法と決済法に分断して検討されてきた法制度について、横断的・包括的に規律するための立法政策のあり方を検討!
発行 民事法研究会


個人情報保護法
コンメンタール
石井夏生利 曽我部真裕 森亮二 編著
勁草書房
最新の理論水準と実務の知見を盛り込み、各条項にEU法・アメリカ法の解説も加えた、「立体的な」コンメンタール誕生。
令和2年改正法ベースの逐条解説
行政機関個人情報保護法も論述形式で全体を詳説。

+一


消費者法講義
第5版
日本弁護士連合会 編
日本評論社


コロナの
The World after COVID-19
先の世界
国際社会の課題と挑戦
一般財団法人 国際経済連携推進センター編
パラダイム転換がもたらす未知への取組み
経済産業審議官、経団連21世紀政策研究所事務局長、国際経済連携推進センター理事長による鼎談録を含め、産業界、官界、学界、NGOから有識者25人が語る"グローバリゼーションの行方"、"ニューノーマルの具体像"、"世界各国・地域のコロナへの向き合い方とその教訓"
産経新聞出版

序　APEC-CBPRとの因縁

- アジア太平洋経済協力（APEC）電子商取引推進グループ（ECSG, 現・デジタル経済推進グループ・Digital Economy Steering Group (DESG)）及びデータプライバシーサブグループ（DPS）日本代表団（2010年9月～2012年5月）
- 消費者庁　アジア太平洋地域等における個人情報保護制度の実態調査検討委員会 オブザーバ（2013年1月～3月）
- 経済産業省　平成25年度我が国経済社会の情報化・サービス化に係る基盤整備（経済産業分野を対象とする個人情報保護に係る制度整備等調査研究）平成25年度認定個人情報保護団体の在り方に関する検討委員会 委員（2014年1月～2月）
- 石井夏生利・曽我部真裕・森亮二編著『個人情報保護法コンメンタール』（勁草書房，2021年）47条担当

APECにおける個人情報保護の枠組み①

- 2004年　APECプライバシーフレームワーク
  - ①損害の回避，②通知，③収集制限，④個人情報の利用等，⑤選択，⑥個人情報の完全性，⑦安全保護措置，⑧アクセス及び訂正，⑨責任
- 2009年　越境プライバシー執行協定（CPEA：Cross Border Privacy Enforcement Arrangement)，2010年開始
  - プライバシー執行機関（データ保護機関）単位で加入する。
    - オーストラリア連邦情報コミッショナー事務局，オーストラリアビクトリア州情報コミッショナー事務局，米国連邦取引委員会，香港プライバシー・コミッショナー事務局，カナダ連邦プライバシー・コミッショナー事務局，韓国個人情報保護委員会，メキシコ連邦情報公開データ保護機関，シンガポール個人データ保護委員会，日本・個人情報保護委員会，フィリピン国家プライバシー委員会，台湾・公正取引委員会等15省庁（合計26機関）

APECにおける個人情報保護の枠組み②

- 2011年　APEC越境プライバシールール（CBPR：Cross Border Privacy Rules），2013年認証開始
  - エコノミー（国・地域）単位で加入する。
    - 米国，メキシコ，日本，カナダ，シンガポール，韓国，オーストラリア，台湾，フィリピン（9エコノミー）
  - アカウンタビリティ・エージェント（AA）が認証する。
    - 日本：JIPDEC
    - 韓国：韓国インターネット振興院（KISA）
    - シンガポール：情報メディア振興庁
    - 米国：Schellman，Truste，NCC Group，HITRUST，BBB
- 2015年　PRP（Ther Privacy Recognition for Processors）
  - 日本は未加盟

CBPRs
CROSS BORDER PRIVACY RULES SYSTEM

Search here..

Documents News & Events Privacy in APEC Region

CONSUMERS BUSINESS GOVERNMENT ABOUT CBPRS COMPLIANCE DIRECTORY

Participation in the APEC Cross-Border Privacy Rules (CBPR) System affords Asia-Pacific Economic Cooperation members a unique opportunity to work

with their counterparts throughout the region to facilitate cross-border trade with privacy standards that meet or exceed those set out in the APEC Privacy Framework.

The APEC CBPR System uses appropriately qualified Accountability Agents that have been recognised by participating economies to certify that participating organisations' privacy policies and practices comply with the APEC CBPR System requirements. Accountability Agents (public or private) are also responsible for ensuring any non-compliance is remedied in a timely fashion and, in appropriate cases, reported to the relevant enforcement authorities.

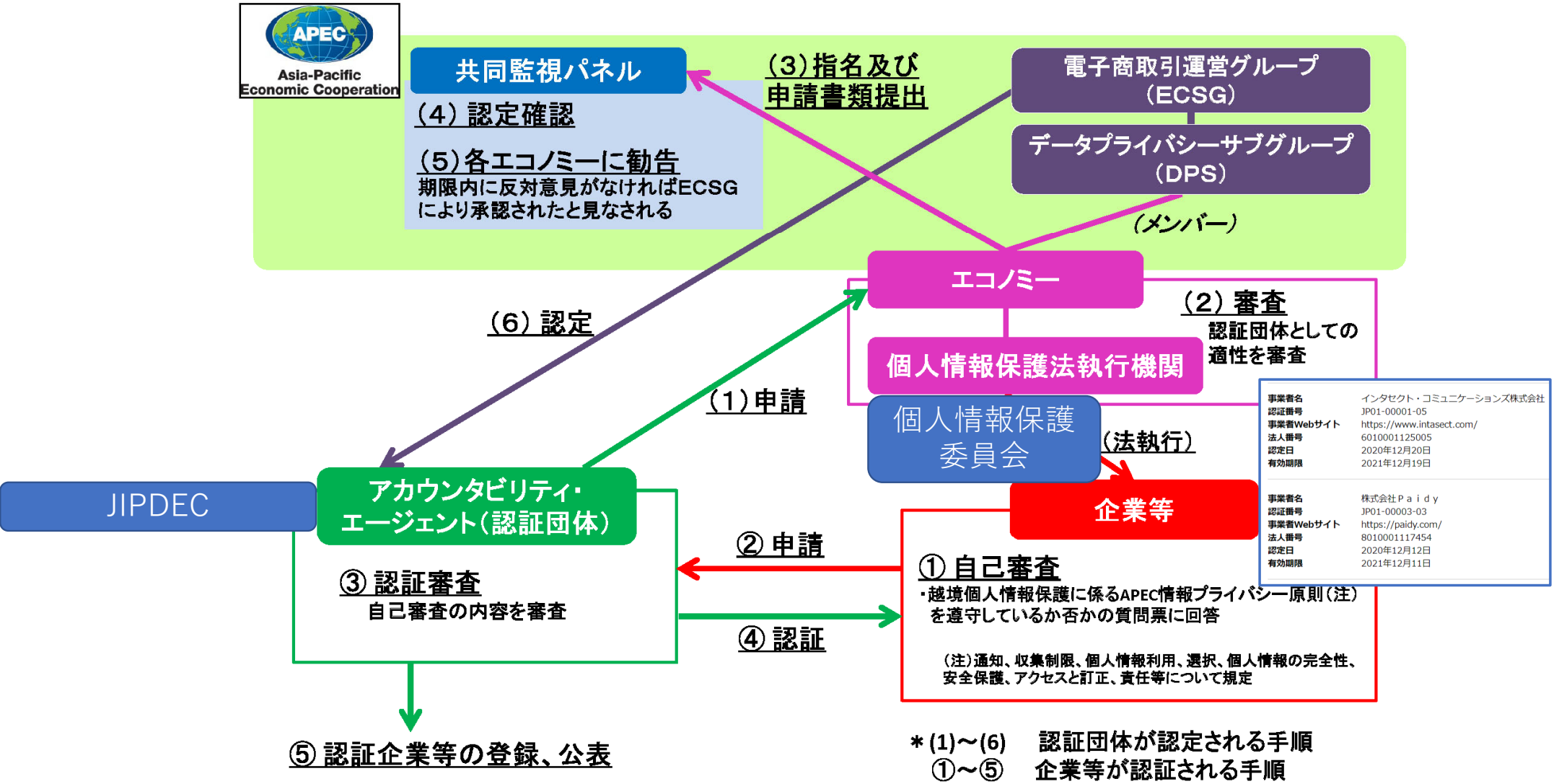
One of the goals of the APEC CBPR System is to lift the overall standard of privacy protection throughout the region through these voluntary, yet enforceable, standards.

THERE ARE CURRENTLY NINE PARTICIPATING ECONOMIES:

USA	**Mexico**	**Japan**
Canada	**Singapore**	**Republic of Korea**
Australia	**Chinese Taipei**	**Philippines**

経済産業省資料を筆者改変

APEC/CBPR システムの概念図



＊(1)～(6)　認証団体が認定される手順
①～⑤　企業等が認証される手順

APEC CBPRのアカウンタビリティ・エージェントに係る業務について

APEC CBPRシステムとは、事業者のAPECプライバシーフレームワークへの適合性を国際的に認証する制度です。CBPRシステムの詳細については、こちらをご覧ください。

認定個人情報保護団体とアカウンタビリティ・エージェントとの関係

APECからアカウンタビリティ・エージェントとして承認されるためには、アカウンタビリティ・エージェントに対し日本の国内法上の執行権が及ぶ必要があります。

日本においては、アカウンタビリティ・エージェントに係る業務は法第47条第1項第3号業務として整理されているため、アカウンタビリティ・エージェントになるには、認定個人情報保護団体であることが要件となります。

アカウンタビリティ・エージェントになるまでの流れ

アカウンタビリティ・エージェントになるには、次のステップを踏む必要があります。

① アカウンタビリティ・エージェントに係る業務は認定に係る業務であるため、その申請にあたっては、CBPRで求められる必要書類に加えて、認定に係る業務として認められるための書類（業務の実施の方法に係る書類、業務を適正かつ確実に実施するための能力・知識並びに経理的基礎を有することを明らかにする書類など）を提出する必要があります。

② 認定個人情報保護団体あるいはその申請をした団体が、必要書類を個人情報保護委員会に提出したのち、個人情報保護委員会は、申請をした団体がアカウンタビリティ・エージェントに係る業務を実施するために必要な知識・能力・経理的基礎を有しているかの審査を行います。

③ 当委員会での審査が終了後、当委員会は、必要書類をAPECに転送します。APECでは、必要書類を審査し、承認されると、当該団体は、アカウンタビリティ・エージェントとしての活動を行うことができるようになります。

アカウンタビリティ・エージェントの認定に必要な書類はこちら (PDF：153KB) 。

AAの役割

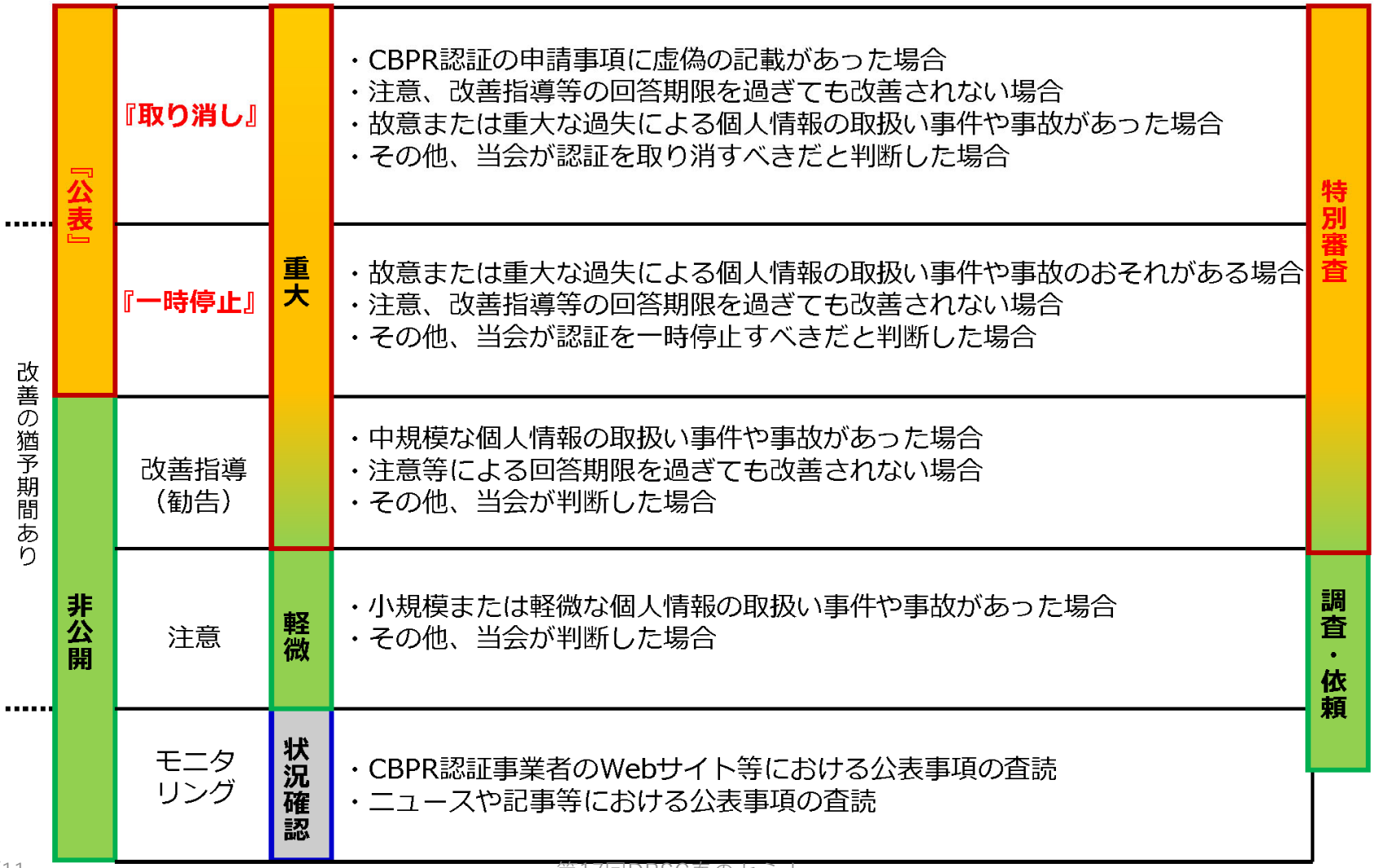
データ通信協会　情報法制研究会　第4回シンポジウム（2016年6月12日）坂下哲也「APEC／CBPRシステムの概要」

- アカウンタビリティエージェント（日本の場合、JIPDEC）は、CBPRシステムの認証プロセスである自己評価の審査に対して責任もち、実施する。
  - 申請する組織は、自身のプライバシーポリシー及び手順の策定に責任を負い、関係するアカウンタビリティエージェントによって、そのポリシー及び手順がCBPRシステムの要件を遵守していると認証された場合にのみ、CBPRシステムに参加することができる。
  - 随時、認証を受けた事業者の**モニタリング**を行い、取り扱う個人情報等の変更などがないか確認を行う。（変更届による対応も有。）

- **苦情処理**を行い、また匿名での事例記録及び苦情に関する統計資料をAPECへ提出する。

- なお、モニタリングや苦情処理の結果によっては、追加の調査依頼や認証の一時停止、取り消しなどを行う場合がある。**（ペナルティ）**

ペナルティ



『赤太文字』：AAの義務　　※この他に、関係監督官庁への通知（連携）。

申請から登録までの流れ

データ通信協会　情報法制研究会　第4回シンポジウム（2016年6月12日）坂下哲也「APEC／CBPRシステムの概要」

- AAである認定個人情報保護団体の対象事業者となる。
- 申請から登録までの流れ
  - 手順として、**①申請、②審査（文書・現地）、③審査会、④登録**を設定。

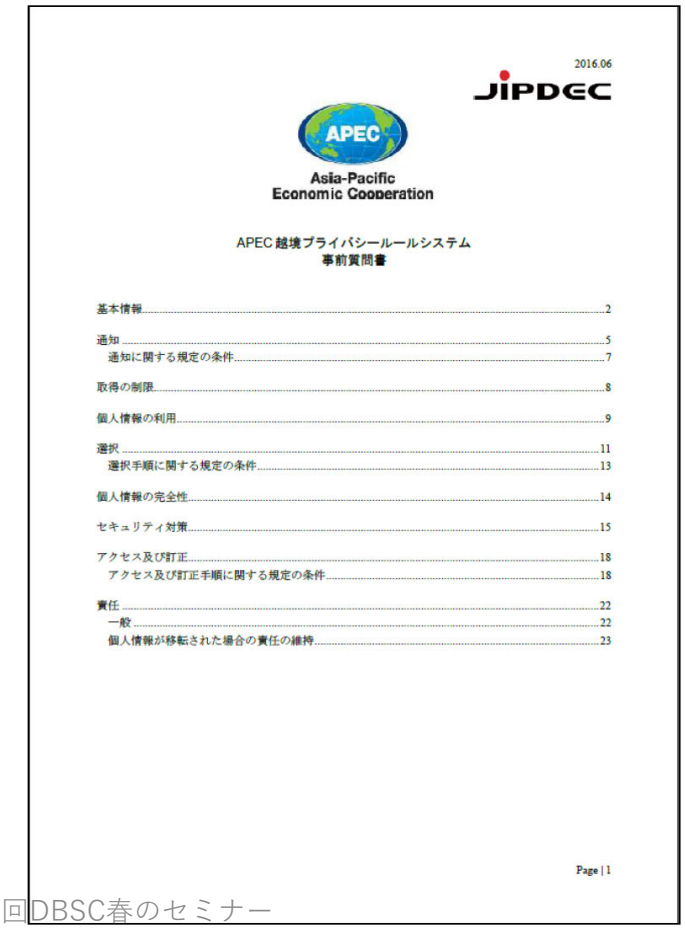
手順	申請者の主な提出物	認定個人情報保護団体事務局の対応
申請	1．**事前質問書** 2．申請書	1．書類の確認 2．CBPR規程の順守に関する確認 3．審査料の請求 4．申請申込書受理
審査（文書）	1．規定類（和・英文） 2．対外公表文書（和・英文） 3．審査に必要な内規他（和文）	1．ヒアリング（全体の聞き取り） 2．文書審査
審査（現地）	（立ち合いと説明）	1．申請事業者の運用状況を現地で確認（主に、セキュリティ等の確認）
審査会		1．審査会を開催し、認証可否を決定 2．認証管理料の請求
登録		1．認証管理料の払い込み確認 2．認証書の発行 3．名称の登録・HP公表

事前質問書の内容（１）

データ通信協会　情報法制研究会　第4回シンポジウム（2016年6月12日）坂下哲也「APEC／CBPRシステムの概要」

■ 事前質問書は、**APECの原則に照らし**個人情報の取扱いに関する50の質問に対する回答を申請者が記載するもの。
（根拠書類等も必要）

- 質問項目の内容は、国内法と整合性を取るため調整を政府において実施。
  - 国内法の認証ではないがこのスキームに則れば結果的に違法な取扱いはしないという考え。



2016.06

JIPDEC

APEC

Asia-Pacific
Economic Cooperation

APEC越境プライバシールールシステム
事前質問書

Page | 1

事前質問書の内容（2）

データ通信協会　情報法制研究会　第4回シンポジウム（2016年6月12日）坂下哲也「APEC／CBPRシステムの概要」

項目	記載内容
基本情報	・組織名称、対象となる組織が管理する組織の一覧、連絡窓口 ・対象となる個人情報の種類（顧客・見込み客、従業員・採用予定者、その他） ・個人情報を取得するエコノミー（APECに参加する国と地域） ・個人情報を移転するエコノミー（同上）

項目	確認する内容
通知	APEC原則（以下、原則）に照らし、①取得される個人情報、移転先、及び利用目的に関する貴社のポリシーを本人に必ず理解してもらっているか、②必要最低限の取得になっていることを条件として、本人の個人情報が取得されるタイミング、移転先、及び利用目的を本人に必ず通知しているか。
取得の制限	APEC取得原則に照らし、個人情報の取得がその取得のために表明した目的に確実に限定されているか。
個人情報の利用	APEC利用原則に照らし、個人情報の利用が取得目的及びこれに適合又は関連するその他の目的を達成することに限定されているか。
選択	選択手順に関する規定の条件に照らし、個人情報の取得、利用及び開示に関して本人が必ず選択できるようになっているか。
個人情報の完全性	記録について正確性及び完全性を維持させ、並びに最新化についても維持しているか。
セキュリティ対策	個人がその個人情報を組織に預けるときに、個人情報の紛失、不正なアクセス、不正な破壊、利用、変更若しくは開示、又はその他の不正使用を防ぐために、その個人情報が合理的なセキュリティ対策によって確実に保護されているか。
アクセス及び訂正	本人がその個人情報にアクセスして、訂正することができることを保証しているか。
説明責任	実施方法を遵守することについて確実に説明責任を果たしているか、また、移転後に原則に従って個人情報を確実に保護するための合理的な措置を用意しているか。

認証ロゴ

横型

縦型

CBPR認証企業

- 日本
  - JIPDEC：インタセクト・コミュニケーションズ，Paidy
- アメリカ
  - TRUSTe：[24]7.ai, Inc.，**Apple Inc.**，Assurant, Inc.，BitSight Technologies, Inc.，**Box, Inc.**，**Cisco Systems, Inc.**，Crowley Webb & Associates, Inc.，Electronic Arts, General Electric Company，**Hewlett Packard Enterprise Company**，**HP Inc.**，IBM, Infor，Kobre & Kim LLP，LogMeIn, Inc.，Mastercard International, Inc.，Merck & Co., Inc., Kenilworth, NJ. USA，Organon & Co.，PGA Tour，Rackspace，Reltio Inc.，Rimini Street, Inc.，The Ultimate Software Group，Virgin Pulse, Inc.，Workday, Inc., World Wrestling Entertainment, Inc.，Yodlee, Inc.，Ziff Davis, LLC
  - Schellman & Company, LLC：ServiceNow, Inc.，**Slack Technologies, Inc**.,
  - NCC Group Security Services, Inc.：Talkdesk, Inc.
- シンガポール
  - 情報メディア振興庁：**Alibaba Cloud (Singapore) Private Limited**，CrimsonLogic Pte Ltd，The Great Eastern Life Assurance Company Limited，TRS Forensics Pte Ltd

APEC CROSS BORDER PRIVACY RULES SYSTEM SINGAPORE

The APEC CBPR System was developed by APEC economies to build consumer, business, and regulator trust in cross-border flows of personal data. The APEC CBPR System requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework and helps to bridge differing national privacy laws within the APEC region, reducing barriers to the flow of information for global trade.

The CBPR System applies to organizations (data controllers) that control the collection, holding, processing, or use of personal data and enables certified organizations across APEC economies to exchange personal data more seamlessly.

The APEC CBPR certification is based on the APEC Privacy Framework which features nine privacy principles: Accountability, Prevent Harm, Notice, Choice, Collection Limitation, Use of Personal Information, Integrity of Personal Information, Security Safeguards and Access and Correction. The framework was endorsed by 21 APEC economies to promote accountable and responsible transfers of personal information between the APEC economies.

Singapore recognizes the APEC CBPR and PRP certifications for overseas transfers of personal data under the PDPA. This means that organizations in Singapore can easily transfer personal data to the overseas certified recipient without meeting additional requireme

Compliance Directory for CBPR can be found here

個人情報保護委員会「APEC CBPRシステムへの参加をご検討下さい」（広報用資料）

APEC CBPRシステムへの参加をご検討下さい

○日本から外国の第三者への個人データの提供

【改正個人情報保護法第24条の内容】
以下のいずれかによって、国内と同様に外国の第三者への個人データの提供が可能。

① 外国にある第三者へ提供することについて、本人の同意を得る。

② 外国にある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。
⇒委託契約やグループ企業の内規・プライバシーポリシー、提供元又は提供先の個人情報取扱事業者がAPECの越境プライバシールール（CBPR）システムの認証を取得している場合等

③ 外国にある第三者が個人情報保護委員会が認めた国に所在する。

個人情報保護委員会

個人情報保護委員会「APEC CBPRシステムへの参加をご検討下さい」（広報用資料）

APEC CBPRシステムとは？

⇒ **APEC域内における個人データ越境移転を円滑にする仕組み**

- 事業者が、自社の越境個人情報保護に関するルール、体制等に対して自己審査を行い、その内容について、予めAPECから認定された認証団体（アカウンタビリティ・エージェント）から審査を受け、認証を得る。認証を受けた事業者は、APEC域内で個人データ越境移転を円滑に行うことができる。
- 日本は平成26年4月にCBPRシステムに参加し、平成28年1月には、APEC CBPRシステムの認証団体として我が国で初めて一般財団法人日本情報経済社会推進協会（JIPDEC）が認定された。

個人情報保護委員会は、国内外におけるワークショップの開催などを通じて、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に積極的に取り組んでいます。

個人情報保護委員会「APEC CBPRシステムへの参加をご検討下さい」（広報用資料）

企業のメリットは？

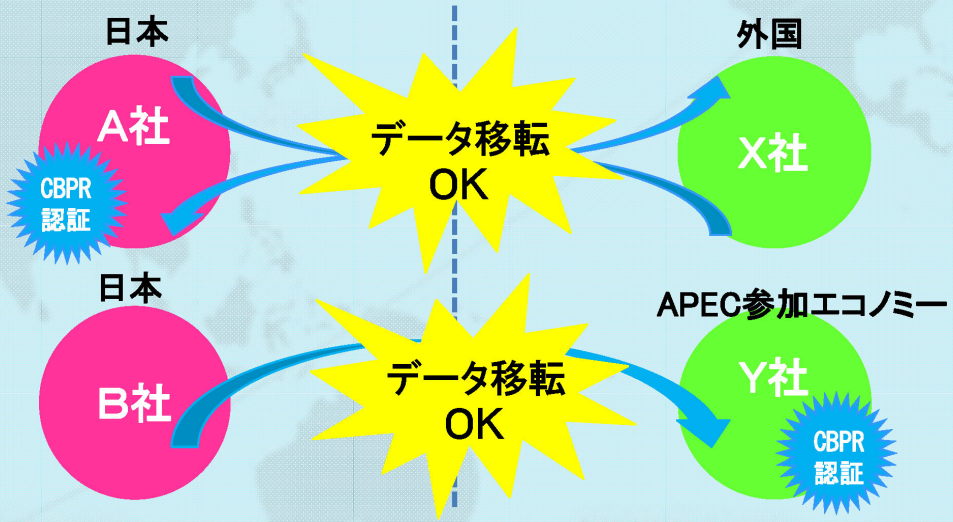
⇒　その１　**日本から外国（APEC域内に限らない）への個人データの移転がスムーズに！**

- 改正個人情報保護法においては、外国への個人データの移転が認められる例として、**出し手**（注）または**受け手**による**CBPRシステムの認証の取得**を、ガイドラインの中で明記。

⇒　その２　**APEC域内から日本への個人データの移転がスムーズに！**

⇒　その３　**国内外の消費者へのアピールポイントに！**

取引先としてのブランド力ＵＰ！



（注）APEC CBPRシステムの認証を取得している事業者は、その取得要件として、当該事業者に代わって第三者に個人情報を取り扱わせる場合においても、当該事業者が本人に対して負う義務が同様に履行されることを確保する措置を当該第三者との間で整備している必要があることとされている。

令和2年改正法概要資料

個人情報の保護に関する法律等の一部を改正する法律（概要）

■ 平成27年改正個人情報保護法に設けられた「**いわゆる３年ごと見直し**」に関する規定（附則第12条）に基づき、個人情報保護委員会において、関係団体・有識者からのヒアリング等を行い、実態把握や論点整理等を実施。

■ 自身の個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、越境データの流通増大に伴う新たなリスクへの対応等の観点から、**今般、個人情報保護法の改正を行い、以下の措置を講ずる**こととしたもの。

改正法の内容

１．個人の権利の在り方

1-1 ● **利用停止・消去等の個人の請求権**について、不正取得等の一部の法違反の場合に加えて、**個人の権利又は正当な利益が害されるおそれがある場合にも要件を緩和**する。

1-2 ● **保有個人データの開示方法**（※）について、**電磁的記録の提供を含め、本人が指示できる**ようにする。

（※）現行は、原則として、書面の交付による方法とされている。

1-3 ● 個人データの授受に関する**第三者提供記録**について、**本人が開示請求できる**ようにする。

1-4 ● ６ヶ月以内に消去する**短期保存データ**について、保有個人データに含めることとし、**開示、利用停止等の対象**とする。

1-5 ● オプトアウト規定（※）により第三者に提供できる個人データの範囲を限定し、**①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外**とする。

（※）本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

２．事業者の守るべき責務の在り方

2-1 ● 漏えい等が発生し、個人の権利利益を害するおそれがある場合（※）に、**委員会への報告及び本人への通知を義務化**する。

（※）一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。

2-2 ● **違法又は不当な行為を助長する**等の**不適正な方法**により個人情報を利用してはならない旨を明確化する。

３．事業者による自主的な取組を促す仕組みの在り方

3-1 ● 認定団体制度について、現行制度（※）に加え、**企業の特定分野(部門)を対象とする団体を認定できるようにする。**

（※）現行の認定団体は、対象事業者のすべての分野（部門）を対象とする。

４．データ利活用に関する施策の在り方

4-1 ● イノベーションを促進する観点から、氏名等を削除した**「仮名加工情報」を創設**し、内部分析に限定する等を条件に、**開示・利用停止請求への対応等の義務を緩和**する。

4-2 ● 提供元では個人データに該当しないものの、**提供先において個人データとなることが想定される情報の第三者提供**について、**本人同意が得られていること等の確認を義務**付ける。

５．ペナルティの在り方

5-1 ● 委員会による命令違反・委員会に対する虚偽報告等の**法定刑を引き上げる**。

（※）命令違反：6月以下の懲役又は30万円以下の罰金
→ 1年以下の懲役又は100万円以下の罰金

虚偽報告等：30万円以下の罰金 → 50万円以下の罰金

5-2 ● データベース等不正提供罪、委員会による命令違反の罰金について、法人と個人の資力格差等を勘案して、**法人に対しては行為者よりも罰金刑の最高額を引き上げる**（法人重科）。

（※）個人と同額の罰金（50万円又は30万円以下の罰金） → 1億円以下の罰金

６．法の域外適用・越境移転の在り方

6-1 ● 日本国内にある者に係る個人情報等を取り扱う外国事業者を、**罰則によって担保された報告徴収・命令の対象**とする。

6-2 ● 外国にある第三者への個人データの提供時に、**移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等**を求める。

7-1 ※ その他、本改正に伴い、「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」及び「医療分野の研究開発に資するための匿名加工医療情報に関する法律」においても、一括法として所要の措置（漏えい等報告、法定刑の引上げ等）を講ずる。

6.　法の域外適用・越境移転の在り方
6-2外国にある第三者への個人データの提供制限の強化

旧第24条

個人情報取扱事業者は、外国（本邦の域外にある国又は地域をいう。以下同じ。）（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規則で定めるものを除く。以下この条において同じ。）にある第三者（個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして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者を除く。以下この条において同じ。）に個人データを提供する場合には、前条第一項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。

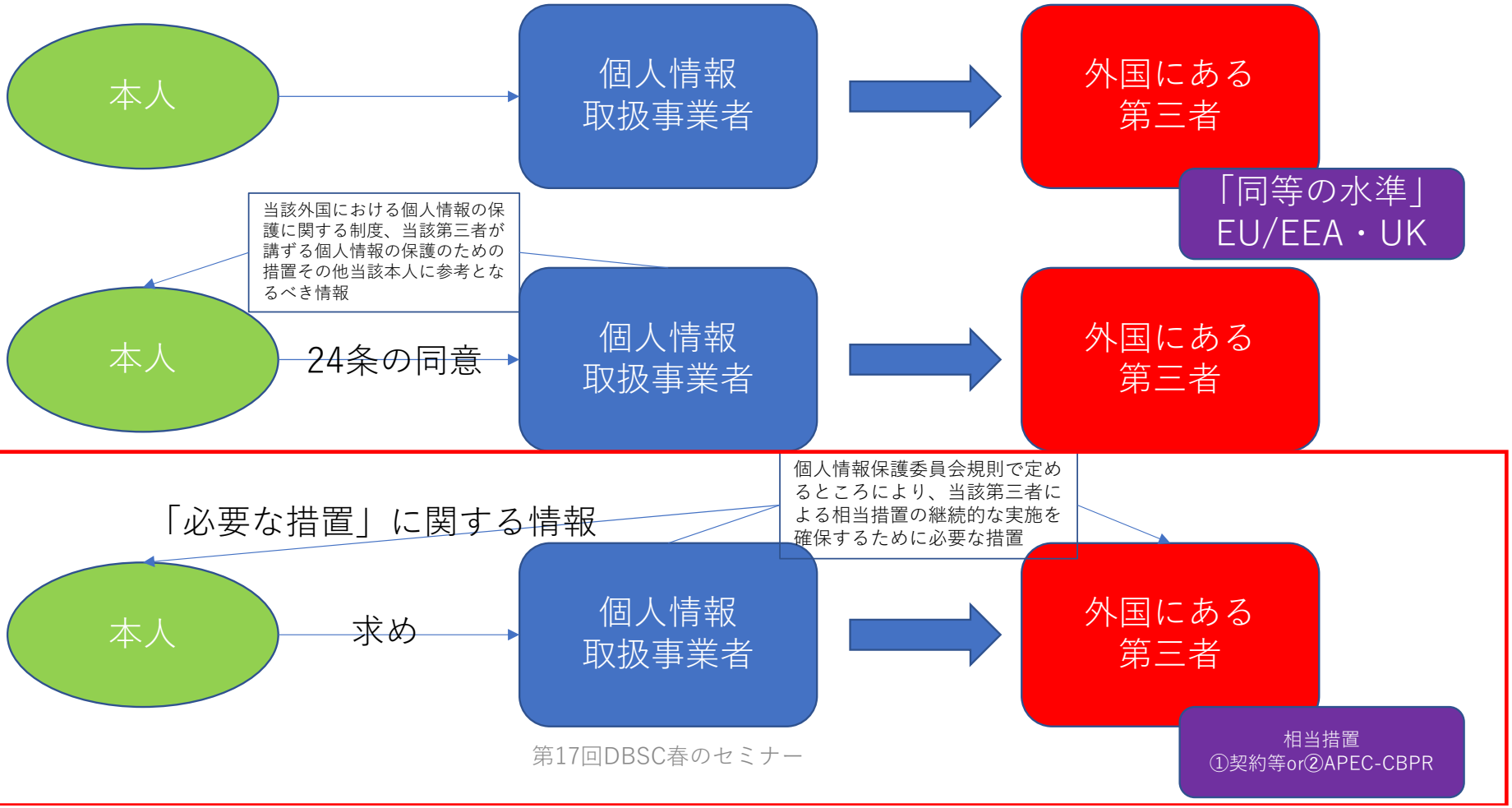
新第24条（令和3年改正後28条）

個人情報取扱事業者は、外国（本邦の域外にある国又は地域をいう。以下同じ。）（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規則で定めるものを除く。以下この条及び第26条の2第1項第2号において同じ。）にある第三者（個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置（**第三項において「相当措置」という**。）を継続的に講ずるために必要なものとして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者を除く。以下この項及び次項並びに同号において同じ。）に個人データを提供する場合には、前条第1項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。

2　個人情報取扱事業者は、**前項の規定により本人の同意を得ようとする場合には、個人情報保護委員会規則で定めるところにより、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供しなければならない**。

3　個人情報取扱事業者は、**個人データを外国にある第三者（第一項に規定する体制を整備している者に限る。）に提供した場合には、個人情報保護委員会規則で定めるところにより、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供しなければならない**。

24条の行為規制


本人
個人情報
取扱事業者
外国にある
第三者
「同等の水準」
EU/EEA・UK
当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報
本人
24条の同意
個人情報
取扱事業者
外国にある
第三者
個人情報保護委員会規則で定めるところにより、当該第三者による相当措置の継続的な実施を確保するために必要な措置
「必要な措置」に関する情報
本人
求め
個人情報
取扱事業者
外国にある
第三者
相当措置
①契約等or②APEC-CBPR

6.　法の域外適用・越境移転の在り方
6-2外国にある第三者への個人データの提供制限の強化

（外国にある第三者への提供に係る同意取得時の情報提供）
新規則第11条の3
法第二十四条第二項又は法第二十六条の二第一項第二号の規定により情報を提供する方法は、電磁的記録の提供による方法、書面の交付による方法その他の適切な方法とする。
2　法第二十四条第二項又は法第二十六条の二第一項第二号の規定による情報の提供は、次に掲げる事項について行うものとする。
一　当該外国の名称
二　適切かつ合理的な方法により得られた当該外国における個人情報の保護に関する制度に関する情報
三　当該第三者が講ずる個人情報の保護のための措置に関する情報
3　前項の規定にかかわらず、個人情報取扱事業者は、法第二十四条第一項の規定により本人の同意を得ようとする時点において、前項第一号に定める事項が特定できない場合には、同号及び同項第二号に定める事項に代えて、次に掲げる事項について情報提供しなければならない。
一　前項第一号に定める事項が特定できない旨及びその理由
二　前項第一号に定める事項に代わる本人に参考となるべき情報がある場合には、当該情報
4　第二項の規定にかかわらず、個人情報取扱事業者は、法第二十四条第一項の規定により本人の同意を得ようとする時点において、第二項第三号に定める事項について情報提供できない場合には、同号に定める事項に代えて、その旨及びその理由について情報提供しなければならない。

（外国にある第三者による相当措置の継続的な実施を確保するために必要な措置等）
新規則第11条の4
法第二十四条第三項（法第二十六条の二第二項において読み替えて準用する場合を含む。）の規定による外国にある第三者による相当措置の継続的な実施を確保するために必要な措置は、次に掲げる措置とする。
一　当該第三者による相当措置の実施状況並びに当該相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその内容を、適切かつ合理的な方法により、定期的に確認すること。
二　当該第三者による相当措置の実施に支障が生じたときは、必要かつ適切な措置を講ずるとともに、当該相当措置の継続的な実施の確保が困難となったときは、個人データ（第二十六条の二第二項において読み替えて準用する場合にあっては、個人関連情報）の当該第三者への提供を停止すること。
2　法第二十四条第三項の規定により情報を提供する方法は、電磁的記録の提供による方法、書面の交付による方法その他の適切な方法とする。
3　個人情報取扱事業者は、法第二十四条第三項の規定による求めを受けたときは、本人に対し、遅滞なく、次に掲げる事項について情報提供しなければならない。ただし、情報提供することにより当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合は、その全部又は一部を提供しないことができる。
一　当該第三者による法第二十四条第一項に規定する体制の整備の方法
二　当該第三者が実施する相当措置の概要
三　第一項第一号の規定による確認の頻度及び方法
四　当該外国の名称
五　当該第三者による相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその概要
六　当該第三者による相当措置の実施に関する支障の有無及びその概要
七　前号の支障に関して第一項第二号の規定により当該個人情報取扱事業者が講ずる措置の概要
4　個人情報取扱事業者は、法第二十四条第三項の規定による求めに係る情報の全部又は一部について提供しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。
5　個人情報取扱事業者は、前項の規定により、本人から求められた情報の全部又は一部について提供しない旨を通知する場合には、本人に対し、その理由を説明するよう努めなければならない。

外国にある第三者への個人データの提供

国会

第201回国会参・内閣委員会第13号（令和2年6月4日）

○山田太郎君　ありがとうございました。
（前略）　今回、外国にある第三者への制限ということで、改正法の二十四条に当たる部分でありますが、新設されまして、外国にある第三者に個人データを提供する場合に本人からの同意を得る際、本人への参考となるべき情報の提供義務が課されたということなんですが、これも具体的にどのような参考情報の提供義務が発生するか、非常に不明だと思うんですね。
本人に提供しなければならない参考情報の基準とか具体例ですとか提供の方法、それから外国の個人情報保護法の条文を伝えるだけで足りるのかどうかとか、一律に日本語での情報提供でなければならないのか。例えば、被害を受けた人は母国語が英語とかフランス語だった場合に、その人たちに対しては、相手が分かるようにというふうなことがありますので、英語やフランス語で伝えなければならないのか。
企業実務としては非常に問題は大きいと思いますが、この辺り教えていただければと思います。

○政府参考人（其田真理君）　**外国にある第三者への個人データの提供を認める旨の本人の同意を得ようとするときには、個人情報取扱事業者が当該本人に提供しなければならない情報や提供の方法については委員会規則で定めることとしておりますけれども、現時点では、例えば提供すべき情報としては、第三者の所在する外国の国名、それから個人情報保護制度などを想定しております**。
また、**提供の方法につきましては、電磁的な記録の提供や書面の交付による方法、基本的には日本語又は本人が内容を理解できる言語というふうに考えておりますけれども、こういった方法を想定をしてございます**。

○山田太郎君　もう一つ、外国における個人情報保護制度を情報提供する件については、その事業者が独自に外国における個人情報の保護に関する制度等の情報を調査して提供しなきゃいけないとなっているんですけど、これもまた企業にとっては大変重たい状況だと思います。
これらの情報については、多分、できれば個人情報保護委員会さんが外国の制度を調査してウエブで例えば公表すると、その公表されたものを各事業者として、委員会が公表したからということでその情報を提供するというような、少し便宜というか図ってあげないと、個社が個々の外国法制に対して全て調べていくということはほぼ難しいし、同じようなことを社会でもってみんながそれぞれ調べ合うというのもどうかと思いますので、その辺りの便宜ということは図っていただけないでしょうか。

○政府参考人（其田真理君）　**今回の改正は、越境移転を行う事業者において移転先の環境を認識していただくという趣旨もございまして、企業が自らの取組をお願いしたいというのが基本でございますけれども、委員会といたしましても、外国の個人情報保護制度につきまして、参考となる情報を提供してまいりたいと考えております**

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

改正法に関連する政令・規則等の整備に向けた論点について
（越境移転に係る情報提供の充実等）

令和２年11月４日

１．改正法における個人データの越境移転に係る制限の概要

- **<u>本人同意を根拠とする個人データの越境移転</u>**
  移転元の事業者に対し、本人同意の取得時に、移転先の第三者における個人データの取扱い等についての本人への情報提供の充実を求める（改正法第24条第２項）。

- **<u>移転先の第三者の基準適合体制を根拠とする個人データの越境移転</u>**
  移転元の事業者に対して、移転先の第三者による相当措置（法に基づき個人データの取扱いについて我が国の個人情報取扱事業者に求められる措置と同等の措置）の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報の提供を求める（改正法第24条第３項）。

- 同意取得時に本人に提供すべき情報、移転元の事業者が講ずべき「必要な措置」、及び本人の求めがあった場合に提供すべき「必要な措置に関する情報」等については、委員会規則で定めることとしている。

１．改正法における個人データの越境移転に係る制限の概要

改正後の個人情報の保護に関する法律（平成15年法律第57号）

（外国にある第三者への提供の制限）

第24条　個人情報取扱事業者は、外国（本邦の域外にある国又は地域をいう。以下同じ。）（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規則で定めるものを除く。以下この条及び第26条の２第１項第２号において同じ。）にある第三者（個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置（第３項において「相当措置」という。）を継続的に講ずるために必要なものとして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者を除く。以下この項及び次項並びに同号において同じ。）に個人データを提供する場合には、前条第１項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。

２　個人情報取扱事業者は、前項の規定により本人の同意を得ようとする場合には、個人情報保護委員会規則で定めるところにより、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供しなければならない。

３　個人情報取扱事業者は、個人データを外国にある第三者（第１項に規定する体制を整備している者に限る。）に提供した場合には、個人情報保護委員会規則で定めるところにより、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供しなければならない。

２．検討すべき主な論点

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

- 改正法第24条第２項の趣旨は、移転先の外国における個人情報の保護に関する制度や移転先の第三者による個人情報の取扱いを含む移転先の状況の多様性等に起因する、個人データの越境移転に伴うリスクについて、本人の予測可能性を高めることにある。

- 改正法第24条第3項の趣旨は、個人データの越境移転後において、移転先の第三者による相当措置の継続的な実施を確保するとともに、本人が自己の個人データの移転先の第三者における相当措置の実施状況について把握できるようにすることにある。

▶ こうした制度趣旨を踏まえ、以下の事項の内容を検討する。

① 同意取得時に本人に提供すべき情報

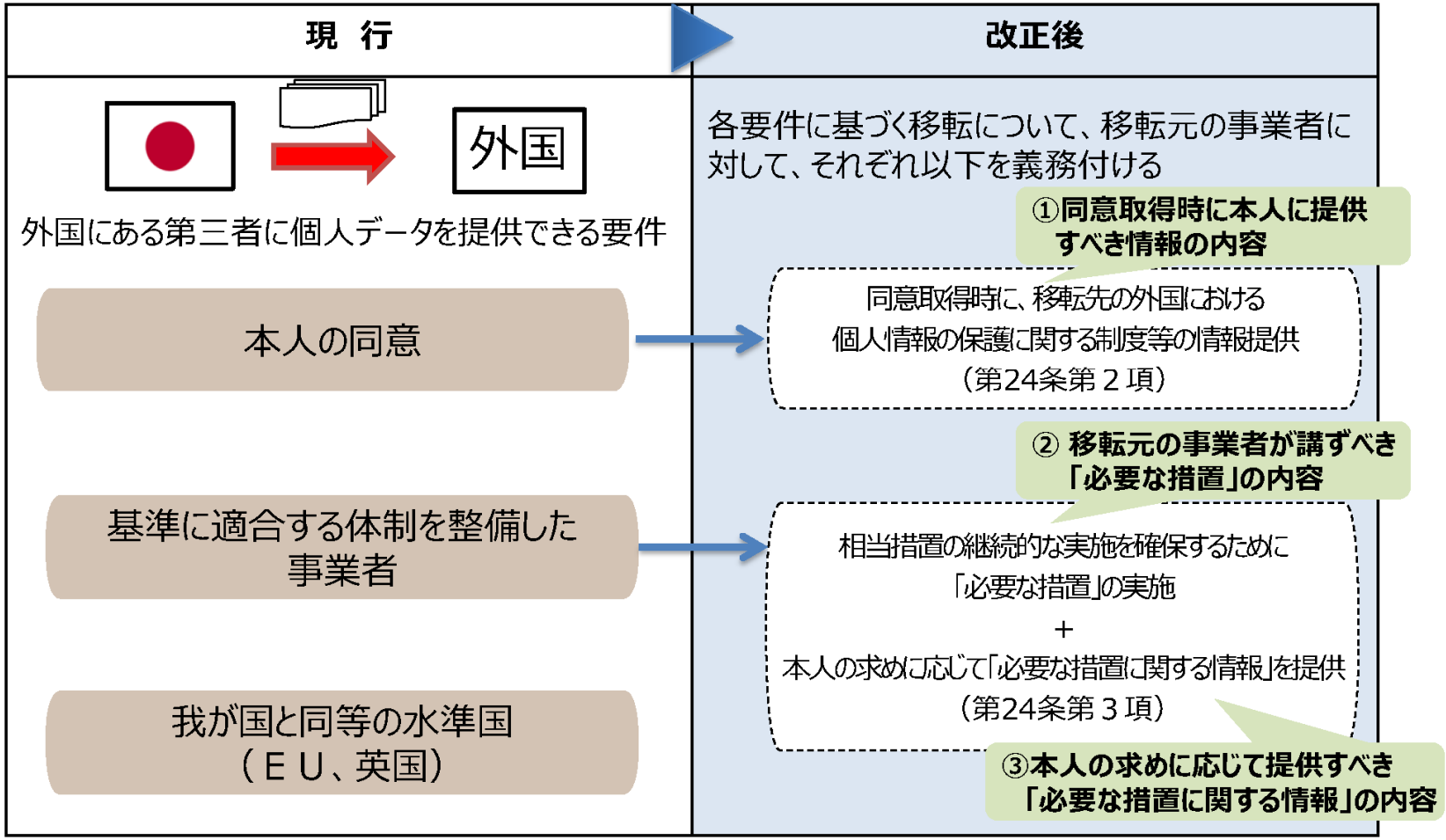
② 移転元の事業者が講ずべき「必要な措置」

③ 本人の求めに応じて提供すべき「必要な措置に関する情報」

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

２．検討すべき主な論点

（イメージ）



※この他、「法令に基づく場合」等の例外要件あり。

３．①同意取得時に本人に提供すべき情報

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

（１）基本的考え方

- 改正法においては、「**当該外国における個人情報の保護に関する制度**」、「**当該第三者が講ずる個人情報の保護のための措置**」、「**その他当該本人に参考となるべき情報**」を個人データの越境移転に係る同意取得時に本人に提供すべき情報としている。

- 本人の予測可能性の向上という制度趣旨を踏まえると、提供すべき情報は、**自己の個人データの越境移転に伴うリスクについて本人が適切に認識できるもの**である必要がある。

- 他方、情報提供義務がその制度趣旨を超えて**事業者の過度の負担とならないよう配意する**必要がある。制度改正大綱の意見募集においても、事業者の負担を懸念する意見や、同意取得時において移転先が未確定であること等により事前の情報提供が実務上困難な場合があることへの配慮を求める意見があった。

▶ 以上を踏まえ、同意取得時に本人への提供を義務付ける情報の内容・粒度は、**本人が自己の個人データの越境移転に伴うリスクを認識できる範囲のもの**としてはどうか。

3．①同意取得時に本人に提供すべき情報

（参考）「個人情報保護法 いわゆる３年ごと見直し 制度改正大綱」に関する意見募集結果（抜粋）

「移転元となる個人情報取扱事業者に対して本人の同意を根拠に移転する場合は、移転先国の名称や個人情報の保護に関する制度の有無を含む移転先事業者における個人情報の取扱いに関する本人への情報提供の充実を求める。」との点については、ベンチャー企業、中小企業において、国外での事業活動や国外事業者との連携が著しく困難になる可能性がある。
そもそも、個別企業において、どこまで海外の制度を把握できているか（国によっては州によって個なる（原文ママ）法制を採る場合もある）という問題があり、そもそも情報提供の範囲を極めて限定するか、もしくは個人情報保護委員会において各国の必要な法制の情報を開示する等の対応がされなければ、事業活動に対して非常に悪影響を及ぼす可能性があると考える。【一般社団法人　Fintech協会】

改正大綱第3章第6節 3.「外国にある第三者への個人データの提供制限の強化」において、データ・ローカリゼーションやガバメント・アクセスといった立法例がみられる中で、（外国に所在する）「移転先となる個人情報取扱事業者に対して本人の同意を根拠に移転する場合は、移転先国の名称や個人情報の保護に関する制度の有無を含む移転先事業者における個人情報の取扱いに関する本人への情報提供の充実を求める」との記述があるが、たとえ国際的にネットワークを有する法律事務所であっても、随時政治情勢によっても変わり得る各国の個人情報保護制度を正確に把握することには相当の時間と労力と費用を要し、ましてや法律の専門家ではない一民間事業者にとって、かかる要求に応えることには経済的にも技術的にも相当な負担となることは明白であるから、他方で「今後、事業者の負担や実務に十分配慮した上で、過重な負担とならないように、提供する情報の内容や提供の方法等について具体的に検討する」との記述があるところ、この点に関する個人情報保護委員会からの積極的な情報提供、並びに、事業者の義務が社会的・経済的にも合理的な範囲内に留まるよう是非適正かつ公平なご検討をお願いしたい。【日本医療機器産業連合会】

（意見）
P30-31に記載のある通り、事業者の負担や実務に十分配慮いただき、過度な負担とならないようにして頂きたい。
（理由）
医薬品等の研究開発においては、日本で取得したデータを海外の審査当局等に移転するケースが一般的に存在する。しかしながら、被験者への同意説明および同意取得を行う時点では、どの国に承認申請するかは未確定であり、詳細な説明は不可能である。また、氏名、住所、電話番号など、本人に直接連絡可能な情報を企業は保有していないため、追加の同意取得も不可能である。【日本製薬工業協会　産業政策委員会】

３．①同意取得時に本人に提供すべき情報

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

（２）方向性

ア　当該外国における個人情報の保護に関する制度

- 本人の適切なリスク認識の観点からは、**本人にとって分かりやすい情報が提供されることが重要**であり、移転先の外国における個人情報の保護に関する制度全体についての網羅的な情報まで求める必要はないと考えられる。

▶ そこで、提供すべき情報は、**我が国の個人情報保護法との間の本質的な差異を認識できる程度の内容・粒度で足りるという方向**とし、委員会規則において「当該外国における個人情報の保護に関する制度」について情報提供を求める旨を定めた上で、**ガイドラインにおいて、適切な内容・粒度を示してはどうか**。

上記の本質的な差異の判断における考慮要素としては、例えば、以下のようなものが考えられる。

a. 個人情報の保護に関する制度の有無

b. 当該外国の個人情報の保護に関する制度についての一定の指標の存在
（例：APEC越境移転プライバシールール（CBPR）の加盟国である、GDPR第45条に基づく十分性認定の取得国である　等）

c. OECDプライバシー・ガイドライン８原則に対応する事業者の義務又は本人の権利の不存在
（例：目的外利用の制限がない、第三者提供の制限がない　等）

d. その他本人の権利利益に重大な影響を及ぼす可能性のある制度の存在
（例：本人の権利利益に重大な影響を及ぼす可能性のあるデータ・ローカライゼーションに係る規制やガバメントアクセスに関する制度の存在　等）

３．①同意取得時に本人に提供すべき情報

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

（２）方向性

ア　当該外国における個人情報の保護に関する制度

- なお、随時更新され得る外国の制度について常に正確かつ完全な情報を提供することを求めた場合、実務上の対応が困難と想定され、事業者にとって過度の負担を負わせるものとなる。

▶ そこで、委員会規則は、**事業者が「適切かつ合理的な方法」により一般的な注意力をもって調査・確認を行って得た情報を提供すれば足りる**という方向で検討してはどうか。

（「適切かつ合理的な方法」の例：
移転先の第三者に照会することや、我が国又は外国の行政機関等が公表している情報を参照すること　等）

- なお、委員会においても、外国の個人情報の保護に関する制度を調査した上で、事業者の参考になる一定の情報を取りまとめて公表することを予定している。

３．①同意取得時に本人に提供すべき情報

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

（２）方向性

イ　当該第三者が講ずる個人情報の保護のための措置

- 本人の適切なリスク認識の観点からは、**本人にとって分かりやすい情報が提供されることが重要**であり、移転先の第三者における個人情報の保護のための措置全体についての網羅的な情報まで求める必要はないと考えられる。

- 一方で、個人データの取扱いについて我が国の個人情報取扱事業者に求められる措置との間に差異が存在する場合には、本人に対し、当該差異が明確に示されている必要がある。

- また、移転先の第三者が講ずる個人情報の保護のための措置は、移転先ごとに様々であると考えられる。

▶ そこで、提供すべき情報は、**個人データの取扱いについて我が国の個人情報取扱事業者に求められる措置との間の本質的な差異を認識できるようにする方向**で、委員会規則においては、「当該第三者が講ずる個人情報の保護のための措置」について情報提供を求める旨を定めた上で、提供すべき情報の内容については、**ガイドラインにおいて、適切な内容・粒度を示してはどうか**。

３．①同意取得時に本人に提供すべき情報

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

（２）方向性

イ　当該第三者が講ずる個人情報の保護のための措置

「当該第三者が講ずる個人情報の保護のための措置」に関する情報提供の例

- 移転先の第三者において、個人データの取扱いについて我が国の個人情報取扱事業者に求められる措置の一部（例：利用目的の通知・公表）を講じていない場合

  「提供先は、利用目的の通知・公表を行っていないものの、それ以外の点については、個人データの取扱いについて我が国の個人情報取扱事業者に求められる措置と同水準の措置を講じています。」

３．①同意取得時に本人に提供すべき情報

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

（２）方向性

ウ　その他当該本人に参考となるべき情報

- 移転先の第三者が所在する外国の名称は、個人データの越境移転に関する基本的な事項である一方、かかる情報の提供を求めたとしても、事業者に過度の追加的な負担が発生するものではないと考えられる。
- また、外国の名称について情報提供がなされることで、本人が、必要に応じて、事業者から提供を受けた当該外国における個人情報の保護に関する制度についての情報の検証を行うことができるようになること等により、本人のリスク認識が促進されることが期待される。

▶ したがって、委員会規則において、「その他当該本人に参考となるべき情報」として、**移転先の第三者が所在する外国の名称**の提供を求めることとしてはどうか。

３．①同意取得時に本人に提供すべき情報

（３）同意取得時に移転先が特定できない場合等の取扱い

- 同意取得時に移転先の外国が特定できない場合や、同意取得時に第三者が講ずる個人情報の保護のための措置についての情報提供が困難な場合でも、その旨及びその理由についての情報提供がなされることで、本人は、自己の個人データの越境移転について一定のリスクが存在することを認識できると考えられる。

▶ そこで、同意取得時に移転先の外国が特定できない場合や、同意取得時に第三者が講ずる個人情報の保護のための措置についての情報提供が困難な場合は、**その旨及びその理由について情報提供を求める**こととしてはどうか。

- また、同意取得時に移転先の外国が特定できないものの、移転先の外国の範囲は定まっている場合、当該範囲についての情報提供がなされれば、本人のリスク認識に資する。

▶ そこで、移転先の外国が特定できないとしても、**移転先の外国の名称に代わる本人に参考となるべき情報**（例：移転先の外国の範囲）**の情報提供ができる場合には、当該情報の提供を求める**こととしてはどうか。

- なお、本人のリスク認識の観点からは、事後的に移転先の外国が特定できた場合や、第三者が講ずる個人情報の保護のための措置についての情報提供が可能となった場合には、本人の求めに応じて情報提供を行うことが望ましい。

４．②移転元の事業者が講ずべき「必要な措置」

（１）基本的考え方

- 現行法上、外国にある第三者が基準適合体制（法に基づき個人データの取扱いについて我が国の個人情報取扱事業者に求められる措置と同等の措置を継続的に講ずるために必要なものとして委員会規則で定める基準に適合する体制）を整備している場合、越境移転に関する本人同意を得ることなく、当該第三者に対して個人データを提供することが許容されている。

- 改正法では、移転先の第三者が基準適合体制を整備していることを根拠に、個人データの越境移転を行った場合、移転元の事業者は、移転先の第三者による相当措置の継続的な実施を確保するために必要な措置を講じなければならないとしている。

- これは、本人の権利利益の保護の観点から、個人データの越境移転後においても、移転元の事業者に、移転先の第三者による個人データの適正な取扱いを継続的に確保する責務があることを明確化するものである。

４．②移転元の事業者が講ずべき「必要な措置」

（２）方向性

ア　定期的な確認の実施

- 移転先の第三者による個人データの適正な取扱いを継続的に確保するためには、移転元の事業者において、移転先の第三者による相当措置の実施状況を適切に把握することが重要である。

- また、移転先の第三者による個人データの取扱いは、移転先の第三者が所在する外国の制度の影響を受ける可能性がある。

▶ そこで、移転元の事業者が講ずべき「必要な措置」として、
- **移転先の第三者による相当措置の実施状況**
- **移転先の第三者の所在する外国における相当措置の実施に影響を及ぼすおそれのある制度の有無**

を定期的に確認することを求めてはどうか。

- なお、定期的な確認の頻度については、移転元と移転先との関係が様々であることや事業者の負担等を踏まえ、**ガイドラインにおいて、例えば、年１回程度といった目安を示してはどうか**。

４．②移転元の事業者が講ずべき「必要な措置」

（２）方向性

イ　支障時の対応

- 移転元の事業者が、移転先の第三者による個人データの取扱いに問題があることを認識した場合、本人の権利利益の保護の観点から、**当該支障の改善・解消のため、必要かつ適切な措置**を講ずるべきである。

（必要かつ適切な措置としては、例えば、移転先の第三者との間で委託契約を締結している場合で、移転先の第三者が契約上の義務に違反して個人データを取り扱っている場合に、これを是正するよう要請すること等が考えられる。）

- また、移転先の第三者による相当措置の継続的な実施の確保が困難となった場合、当該第三者は、実質的に、**基準適合体制を整備しているとはいえないと考えられる**ことから、**それ以降、当該第三者への個人データの提供を停止する**必要がある。

▶ したがって、移転先の第三者による相当措置の実施に支障が生じた場合には、**当該支障の解消のために必要かつ適切な措置を講ずること**とともに、当該第三者による相当措置の継続的な実施の確保が困難になった場合は、**当該第三者に対する個人データの提供を停止すること**を求めるべきではないか。

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

５．③本人の求めに応じて提供すべき「必要な措置に関する情報」

（１）基本的考え方

- 改正法では、移転元の事業者に対して、本人の求めに応じて、「必要な措置に関する情報」の提供を求めることとしている。

- この趣旨は、**本人が移転先の第三者における自己の個人データの取扱状況について把握できるようにする**ことで、**必要な場合に、本人が自己の権利利益を保護するための措置を講じられるようにする**ことにある。

▶ したがって、「必要な措置」の内容のうち、移転先の第三者における自己の個人データの取扱状況について把握できるようにする観点から、以下の情報の提供を求めてはどうか。
- **定期的に実施する確認の対象、頻度及び方法**
- **移転先の第三者による相当措置の実施に関する支障及び当該支障への対応等**

第157回個人情報保護委員会（令和２年11月4日）
改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）

５．③本人の求めに応じて提供すべき「必要な措置に関する情報」

（２）方向性

ア　定期的に実施する確認の対象、頻度及び方法

- **<u>確認の対象に関する情報</u>**として、以下の情報の提供を求めてはどうか。
  - 移転先の第三者による相当措置の実施状況を確認する観点
    - ✓ 基準適合体制の整備の方法（例：移転先との間の契約、移転元と移転先に共通して適用される内規・プライバシーポリシー　等）
    - ✓ 基準適合体制に基づいて第三者が講ずる相当措置の概要
  - 移転先の第三者の所在する外国における相当措置の実施に影響を及ぼすおそれのある制度の有無を確認する観点
    - ✓ 移転先の第三者が所在する外国の名称
    - ✓ 当該外国における相当措置の実施に影響を及ぼすおそれのある制度の有無及び概要
- **<u>確認の頻度及び方法に関する情報</u>**として、以下の情報の提供を求めてはどうか。
    - ✓ 移転元の事業者が上記の確認を行う頻度及び方法

第157回個人情報保護委員会（令和２年11月4日）
越境移転に係る規則案の概要及び論点について（越境移転に係る情報提供の充実等）

５．③本人の求めに応じて提供すべき「必要な措置に関する情報」

（２）方向性

イ　移転先の第三者による相当措置の実施に支障が生じた場合の対応等

- **移転先の第三者による相当措置の実施に支障が生じた場合の対応等に関する情報**として、以下の情報の提供を求めてはどうか。
  - ✓ 移転先の第三者による相当措置の実施に関する支障の有無及びその概要
  - ✓ 当該支障に対して移転元の事業者が講じた措置の概要

５．③本人の求めに応じて提供すべき「必要な措置に関する情報」

（３）具体例

○ **「必要な措置に関する情報」の例**

（A国に所在する第三者に対する委託に伴う個人データの提供の場合）

- **基準適合体制の整備の方法：**
  移転先との間の委託契約
- **移転先が講ずる相当措置の概要：**
  委託契約において、特定した利用目的の範囲内で個人データを取り扱う旨、必要かつ適切な安全管理措置を講ずる旨、従業者に対する必要かつ適切な監督を行う旨、再委託の禁止、個人データの第三者提供の禁止等を定めている
- **移転先が所在する外国の名称：**
  A国
- **移転先による相当措置の実施に影響を及ぼすおそれのある当該外国の制度：**
  特段の制限なく、政府による民間事業者が保有する個人情報へのアクセスが認められている
- **確認の頻度及び方法：**
  毎年、移転先から書面による報告を受ける形で確認している
- **移転先による相当措置の実施に支障が生じた場合の対応等：**
  移転先が、契約上の義務を遵守せず、相当措置の継続的な実施の確保が困難であるため、個人データの提供を停止した

個人情報保護委員会
Personal Information Protection Commission

個人情報の保護に関する法律に基づく行政上の対応について

令和３年４月 23 日
個人情報保護委員会

個人情報保護委員会は、ＬＩＮＥ株式会社（以下「ＬＩＮＥ社」という。）等に対し、令和３年３月 19 日に個人情報の保護に関する法律（以下「法」という。）第 40 条第１項に基づく報告徴収を行うとともに、同年３月 31 日より立入検査を実施している。

立入検査は継続中であるところ、今般、一定の確認が終了した。

ＬＩＮＥ社が委託等した個人データは秘匿性が高く、数量も多いことから、不適切な取扱いが生じた場合の影響も大きい。ＬＩＮＥ社には、それに応じた高い安全管理措置が必要であり、この観点から改善を要する事項が認められ、法第 41 条に基づく指導を行った。

指導の内容及び現在の確認の状況は以下のとおり。

１．法第 41 条に基づく指導の内容

(1) 個人データの取扱いを委託する場合には、法第 22 条に基づき委託先に対する必要かつ適切な監督を行う義務があるところ、法第 20 条に基づき自らが講ずべき安全管理措置と同等の措置が講じられるよう、例えば次のような手法により必要かつ適切な監督を行うこと。

○委託先（再委託先を含む。以下同じ。）のシステム開発者に個人データへのアクセス権限を付与する場合には、その必要性及び権限付与の範囲を組織的に検討した上、必要な技術的安全管理措置を講ずること。

○委託先のシステム開発者に個人データへのアクセス権限を付与する場合には、不正閲覧等を防止するため、アクセスしたデータの適切な検証を可能とするログの保存・分析など組織的安全管理措置を検討した上、必要な措置を講ずること。

○委託先における個人データの取扱状況を把握するため、定期的に監査を行うなど、委託契約の実施状況を調査した上で、委託内容等の見直しの検討を含め、適切に評価する措置を講ずること。

(2) LINE サービスの提供に関してメッセージ等の個人情報を取得する場合には、取得する個人情報の範囲を分かりやすく通知するとともに、通知内容が適切に表示されているか確認する体制を整備すること。

２．現在の確認の状況

(1) 法第 22 条の委託先の監督については、上記１．(1)のとおり一部改善を要する事項があり、改善を求めた。

(2) 法第 24 条の外国にある第三者への提供の制限

○「基準適合体制」については、一部改善を要する事項はあるものの、基準適合体制を整備するための措置が概ね講じられていた。

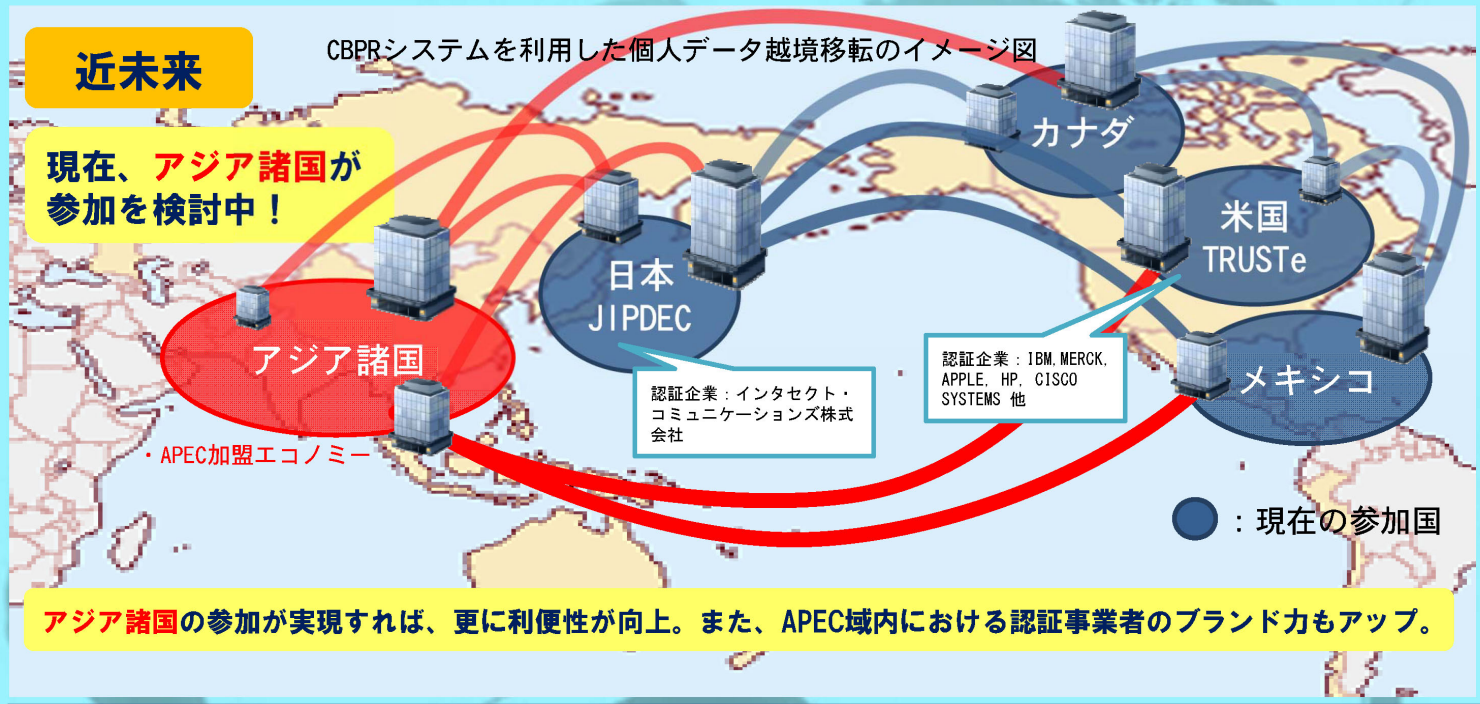
○「本人の同意」については、プライバシーポリシーにおいて、利用者の個人情報の利用目的（サービスの提供・改善、コンテンツの開発・改善、不正利用防止等）及び業務委託先の外国の第三者へ提供することが明記されており、利用者にとって外国にある第三者に提供する場面を特定できなかったとは言い難い。

（以　上）

【連絡先】
個人情報保護委員会事務局
電話番号：03-6457-9685

個人情報保護委員会「APEC CBPRシステムへの参加をご検討下さい」（広報用資料）

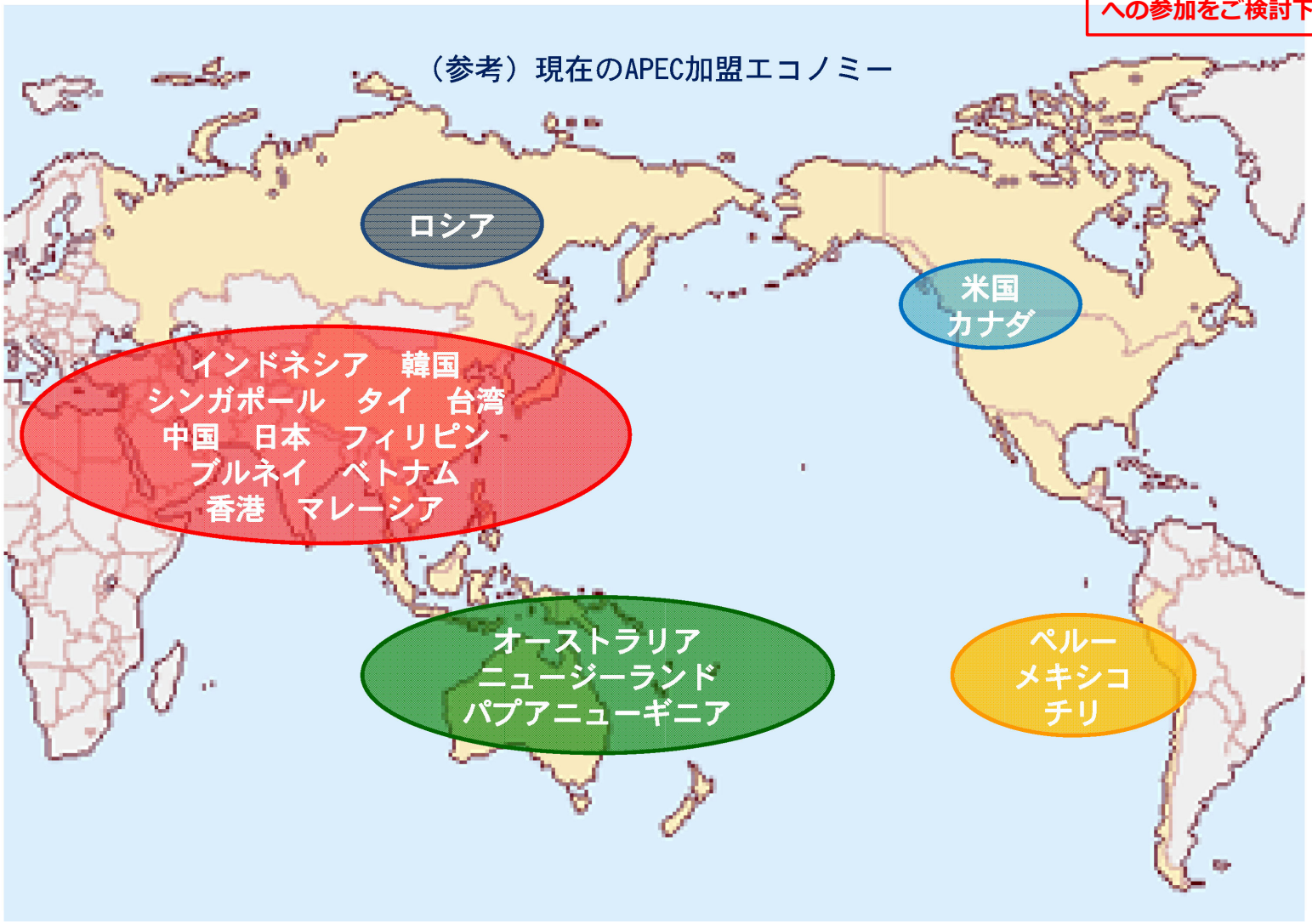
APEC CBPRシステムの未来予想図



さらに未来　EUの個人データ越境移転の制度との相互運用への道も

（注）地図の出典：外務省ホームページ

個人情報保護委員会「APEC CBPRシステムへの参加をご検討下さい」（広報用資料）



（注）地図の出典：外務省ホームページ

Ｖ－３．デジタル（各国の積極対応がもたらす新たな課題）

第8回 産業構造審議会 通商・貿易分科会（2021年5月24日）【資料2】通商政策局・貿易経済協力局「対外経済政策を巡る最近の動向」（2021年5月）

- コロナ危機への対応として、**各国でデジタル化やデータ戦略強化の動きが顕著に。**
- 将来産業を生み出す**データを囲い込み、独占的にAI開発をする動き**も顕在化。様々な優遇政策と相まって育成された国策テック企業による市場総取り、特定企業の下でのビジネス強要等、**デジタル時代における新しい問題**が発生。

日本

- データの利活用を通じたイノベーションを加速するためには、**国境を越えたデータの自由な流通を確保**することが重要として、2019年1月**「データ・フリー・フロー・ウィズ・トラスト（ＤＦＦＴ）」**の理念をダボス会議で提唱。
- **行政のデジタル化、社会全体のデジタル・トランスフォーメーション**を目指し、2021年9月に**デジタル庁を新設**予定。

アメリカ

- デジタル保護主義への対抗措置として、「**2021年戦略的競争法案**」を外交委で可決、本会議にも進む予定（2021年4月）。
- シンクタンクの有識者から、国内ガバナンスが必要として、**連邦プライバシー法、省庁横断体制、包括的な国際デジタル戦略の必要性**を提言。

ＥＵ

- **欧州域内のクラウドサービスの統合**を図るために「**GAIA-X**」を正式発足（2020年6月）。
- **デジタル主権確保**に向け、「**デジタルコンパス2030**」を戦略的な羅針盤として発表（2021年3月）。
- **ＡＩ活用促進と人間中心のデジタル社会実現**のため、**ＡＩ規制法案**を策定（2021年4月）。

インド

- **非個人データのガバナンスに関する議論**を目的とする**専門家委員会を創設**（2019年9月）。
- **「非個人データのガバナンス・フレームワーク」に関するレポート**を公表（2020年7月）。
- 規制検討の背景として、**国民や組織の主権確保**の必要性を強調。

ベトナム

- 公安省がサイバーセキュリティ法等に基づく「**個人情報保護に関する政令案**」を公表（2021年2月）。
- 広範な域外適用の可能性、国内保存義務と組み合わされた**厳しい越境移転規制、センシティブデータの登録義務、政府によるデータへのアクセス**が含まれる。

中国

- サイバーセキュリティ法等においては、**政府によるデータへのアクセス、中国国内でのデータ保管義務、越境移転規制等**が含まれる。
- 「グローバル・データセキュリティ・イニシアチブ」において、**主権、 司法管轄権、データ管理権の尊重**を主張（2020年9月）

Ｖ－４．デジタル（「信頼」できるデジタル経済の構築）

第8回 産業構造審議会 通商・貿易分科会（2021年5月24日）【資料2】通商政策局・貿易経済協力局「対外経済政策を巡る最近の動向」（2021年5月）

- 今後加速するデジタル社会で、安心・安全なデータ流通・デジタル技術の活用を図るためには、データの適切な保護など、取引における**「信頼」が重要な判断要素**に。
- 既存産業やサプライチェーン事業そのものを覆しうる「デジタル化」があらゆる業態・ビジネスで進むなか、有志国とともに共通の価値軸となる**「信頼」を可視化**していくことが必要。

具体的な取組課題

→「データ戦略」を基に「信頼性のある自由なデータ流通（DFFT）」の具体化を推進。

「データ流通」の国際約束

- ✓ 日本は、近年、有志国とともに、多くの**ハイレベルなデジタル通商ルール**に合意・締結（※）

※CPTPP、日米デジタル貿易協定、日英EPA、RCEPにおいて、データの自由な流通・ローカライゼーション要求の禁止を約束。

- ✓ WTO電子商取引交渉や日EU・EPAやAPEC CBPRの見直しを通じた、**自由なデータ流通圏の拡大**を目指している。

「個人データ」の取り扱いに関する協力

- ✓ 日EU間で、**相互の円滑な個人データ移転を図る枠組みを**構築済み。
- ✓ OECDプライバシーガイドライン（各国の個人情報保護法のモデル）のレビュープロセスにおいて、**政府による民間データへのアクセスに関する共通原則について議論**を進めている。

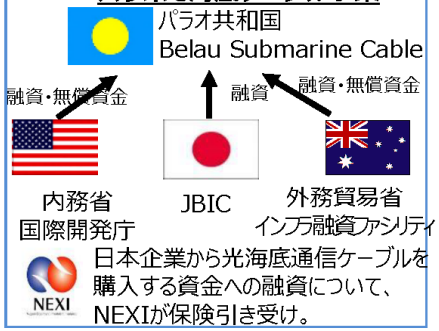
新たな分野における連携（ＡＩなど）

- ✓ **責任あるAIの開発と使用**について議論する「**AIに関するグローバルパートナーシップ（GPAI）**」を有志国と設立。
- ✓ **データ関連の国際標準化**のプロセスにおける**有志国連携**（5G、AI、スマートシティ）。

信頼できるデジタルインフラの構築

- ✓ **海底ケーブルやモバイル通信ネットワーク等**の構築について、**有志国との連携を強化**。

パラオ光海底ケーブル事業



日本企業から光海底通信ケーブルを購入する資金への融資について、NEXIが保険引き受け。

国際枠組みを通じた連携強化

本年のG7デジタル・技術大臣会合で開催に合意した「Future Tech Forum」や、日米欧三極等を通じた連携強化。

GDPRにおける越境移転制限

- 欧州一般データ保護規則（GDPR）上，欧州（EU/EEA）域外への移転は原則禁止されており，GDPR44条以下の要件を満たした場合にのみ許される.
- GDPR45条（十分性認定）は，最も原則的な移転手段であり，国又は地域が，個人データの保護について十分なレベルの保護措置を確保している場合に十分性について，欧州委員会が決定を下すのが基本である
  - 例えば，日本について”Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance) C/2019/304/”

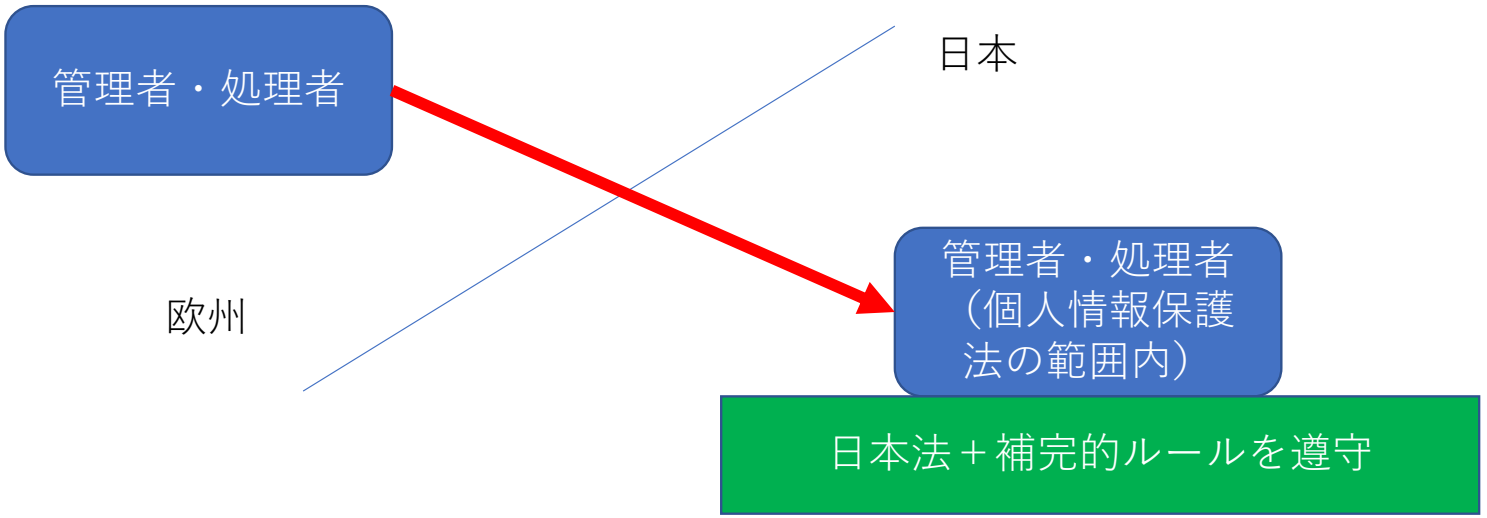
GDPRにおける十分性認定

- 十分性認定とは，欧州一般データ保護規則（GDPR）において，個人データの欧州（EU加盟国及びEEA3カ国）からの移転が原則禁止されているところ，十分なデータ保護の制度を備えている国又は地域として認定されることで，移転が可能となる制度である（ただし，GDPRは個人データの処理も原則禁止しており，処理の適法化事由が不要となるわけではないことに注意が必要である）。具体的には，GDPR第44条及び45条がこれを定める）。
- 十分性判定がなされたのは，
  - アンドラ，アルゼンチン，カナダ（民間部門），フェロー諸島，ガーンジー島，イスラエル，マン島，ジャージー島，ニュージーランド，スイス，ウルグアイ（7カ国4地域），**日本**
  - ~~**EU-USプライバシーシールドスキーム**~~

例外事由

- 適切な安全性確保措置
  - 監督機関の個別承認不要
    - 従来からの方法
      - 標準データ保護約款（GDPR46条2項(c)(d)）
      - 拘束的企業準則（BCR）（GDPR46条(b)）
    - GDPRでの新規導入
      - **行動準則（GDPR40条ないし41条）**
      - **認証（GDPR42条ないし43条）**
  - 監督機関の個別承認
    - 詳細はまだ不明
- 特別の状況における特例
  - 同意が含まれるが，「大量，構造的，反復的な移転には適用されない」との指摘

日本の十分性認定
Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance) C/2019/304/



日EU間の相互の円滑な個人データ移転を図る枠組み発効（2019年1月23日）

- 日EU間の相互の円滑な個人データ移転を図る枠組みが、平成31年１月23日に発効しました。
- 本枠組みの構築に関しては、日EU双方の経済界の要望等も受け個人情報保護委員会と欧州委員会との間で交渉を重ね、平成30年７月、個人情報保護委員会が個人情報保護法第24条に基づく指定をEUに対して行い、欧州委員会がGDPR第45条に基づく十分性認定を我が国に対して行う方針について合意に至りました。この合意を踏まえて、我が国においては、第85回個人情報保護委員会において、上記のEU指定を１月23日付けにて行うことを決定しました（※）。また、欧州委員会においても、上記の我が国の十分性認定を同23日付けにて行うことを決定しました。

熊澤春陽個人情報保護委員会委員、ベラ・ヨウロバー欧州委員会委員（司法・消費者・男女平等担当）による共同プレス・ステートメント（2019 年 1 月 23 日 ）

- 熊澤春陽委員とベラ・ヨウロバー委員は、本日、個人情報保護委員会と欧州委員会による、お互いの個人データの保護レベルが同等だとする決定の採択を歓迎する。
- 相互に十分性を見出すことを通じて、データが安全に流通する世界最大の地域が創出される。これは、特に包括的なプライバシーの法律、中核となる一連の個人の権利の核心、及び独立したデータ保護機関による執行に支えられる、両国の制度の高いレベルの類似性に基づくものである。データ・プライバシー及びセキュリティが消費者の信頼の中心的要素となった今、このような強い法律と確固たる執行に基づく類似性こそが、ますます増大するデータ駆動型経済の持続可能性を確保し、通商の流れを促進することができる。
- 日 EU の市民は、個人データの移転における強固な保護を享受する一方、日 EU の全ての企業は、お互いの経済圏への自由なデータ移転による便益を享受する。このように、本日の決定は、日 EU 経済連携協定から得られる利益を補完し拡大することとなり、日 EU 間の戦略的なパートナーシップにも寄与する。
- 相互に十分性を見出すことによって、日 EU は、プライバシーに関する価値観の共有及び高いレベルの個人データの保護に基づく世界標準の形成に向けた協力の強化へのコミットメントを再確認する。

「個人情報の保護に関する法律に係るＥＵ及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」

- 個人情報保護委員会は、日ＥＵ間で相互の円滑な個人データ移転を図るため、法第 24 条に基づき、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ＥＵを指定し、これにあわせて、欧州委員会は、ＧＤＰＲ第 45 条に基づき、日本が個人データについて十分な保護水準を確保していると決定した。
- これにより、日ＥＵ間で、個人の権利利益を高い水準で保護した上で相互に十分性認定により移転が図られることとなる。日ＥＵ双方の制度は極めて類似しているものの、いくつかの関連する相違点が存在するため、ＥＵ域内から移転を受けた個人情報の取扱いについて、個人情報保護委員会は補完的ルール（以下「本ルール」という。）を策定した。

- 人厳定関条をて、個り規機２義いとたよをる第定つこれ、限す法るにるとる、権管びすいすの回る所及関扱定合上ずを報に取策整し講法情）のを に完を護人むタル的補置保個含一一際を措報慮をデル国容の情配め人的り内他人要定個完図るの個るるた補る。をめそ、めすけたい護定置は定関受して保で措会ににを定しの令の員項間転規有層法上委３期移をを一、制護第有り護限るら法保条保よ保権すかな報２（にのる関点要情第タ定準すに観必人法一認水定報るう個、デ性い策情すよ、い人分高を人築るて、従個十り律個構れっに有らよ規は、をらが条保かのいは度けた６る内益し条制設し第め域利厳６るを。法定Ｕ利り第係律る。、にＥ権よ法に規いて項、のに報なてし７め人り特情格しと第含個よ
- ーす権とにすデ守く定務完人遵づ規義補個を基のびりるれに法及よれこルる利にさはーす権律る。転者ル完る規き移業本補めなでり事、り定細がよ扱りよに詳とに取あにルりこ定報で律一よる認情律規ルで得性人規な本格を分個る細。厳済十、す詳るり救らし有りなよもか束をよとがら内拘力で象ルか域を束格対一所Ｕ者拘厳行ル判Ｅ業的り執本裁は、事法よのは扱はが会は、人ル取ルル員合本ール報ーー委場ル情ルル護たに、本人本本保っ様き、個。、報あ同きるるは情がとづすあ務人害定基領が義個侵規に受要びにるのれを必及様す法こタる利同対る

- 個人情報保護委員会による執行に関しては、個人情報取扱事業者が本ルールに定める一つ以上の義務を遵守しない場合、個人情報保護委員会は法第 42 条に基づく措置を講ずる権限を有する。一般的に、ＥＵ域内から十分性認定により移転を受けた個人情報について、法第 42 条第 1 項の規定による勧告を受けた個人情報取扱事業者が正当な理由（※２）がなくその勧告に係る措置をとらなかった場合は、法第 42 条第 2 項に定める「個人の権利利益の重大な侵害が切迫している」と認められる。
- なお、本ルールは、ＥＵから英国が離脱した後、英国域内から十分性認定により移転を受けた個人データの取扱いについても同様に対象とする。

- （※１）法第 4 条、第 6 条、第 8 条、第 24 条、第 60 条及び第 78 条、並びに規則第 11 条
- （※２）正当な理由とは、個人情報取扱事業者にとって合理的に予測できない不可抗力のできごと（たとえば自然災害）による場合や、個人情報取扱事業者が違反を完全に是正する代替的措置をとったことにより法第 42 条第 1 項に基づく個人情報保護委員会による勧告に係る措置を講じる必要性が失われた場合が考えられる。

(4) 外国にある第三者への提供の制限（法第 24 条・規則第 11 条の 2 関係）

- 個人情報取扱事業者は、ＥＵ又は英国域内から十分性認定に基づき提供を受けた個人データを外国にある第三者へ提供するに当たっては、法第 24 条に従い、次の①から③までのいずれかに該当する場合を除き、本人が同意に係る判断を行うために必要な移転先の状況についての情報を提供した上で、あらかじめ外国にある第三者への個人データの提供を認める旨の本人の同意を得ることとする。
- ① 当該第三者が、個人の権利利益の保護に関して、我が国と同等の水準にあると認められる個人情報保護制度を有している国として規則で定める国にある場合
- ② 個人情報取扱事業者と個人データの提供を受ける第三者との間で、当該第三者による個人データの取扱いについて、適切かつ合理的な方法（契約、その他の形式の拘束力のある取決め又は企業グループにおける拘束力のある取扱い）により、本ルールを含め法と同等水準の個人情報の保護に関する措置を連携して実施している場合
- ③ 法第 23 条第 1 項各号に該当する場合

APEC-CBPRだけ名指しで省かれているのでは？①

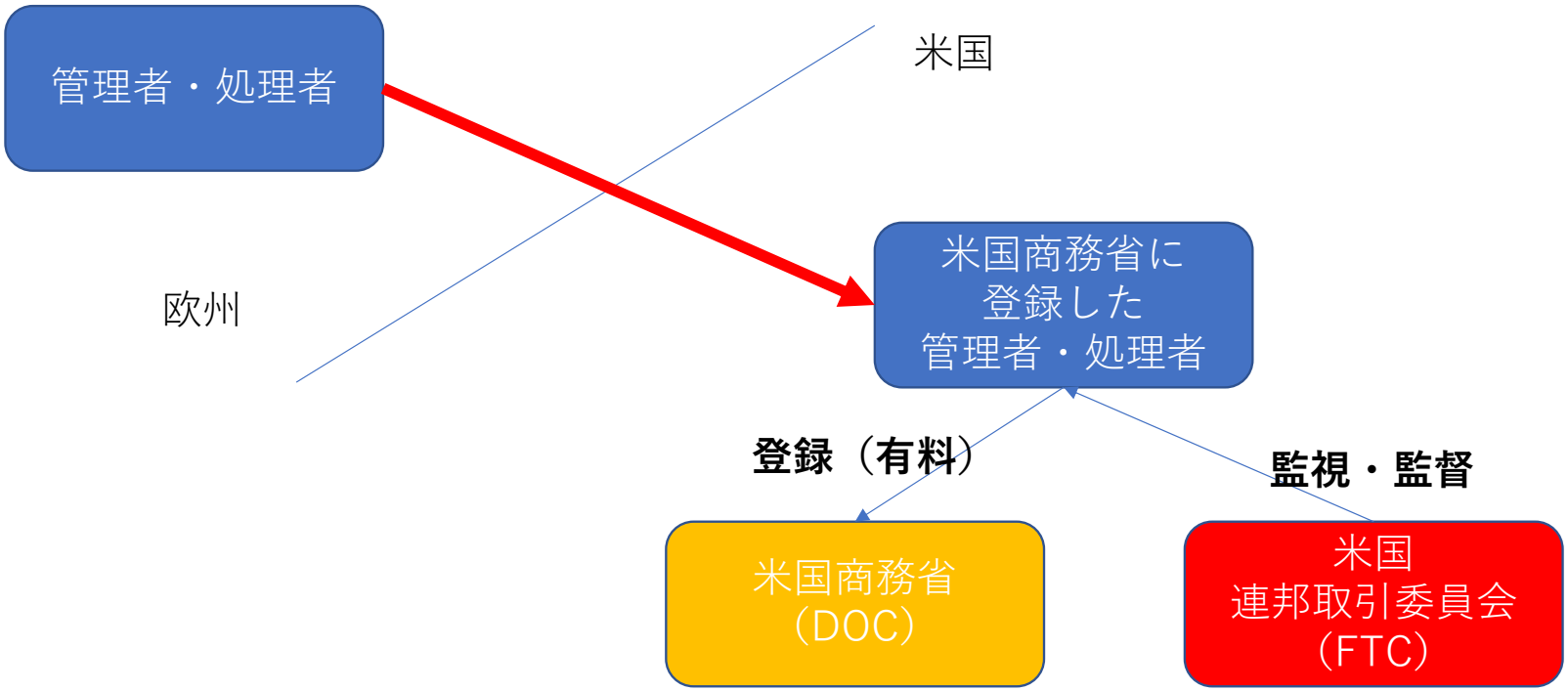
	外国第三者提供GL（パブコメ中）	補完的ルール
同意	「法第 24 条第 1 項において求められる本人の同意を得ようとする場合には、本人に対し、**法第 24 条第 2 項に基づく情報提供を行わなければならない**。同意取得時に本人に提供すべき情報については、5（同意取得時の情報提供）を参照のこと。」（2-1）	**本人が同意に係る判断を行うために必要な移転先の状況についての情報を提供した上で**、あらかじめ外国にある第三者への個人データの提供を認める旨の本人の同意を得る
同等性	「外国（本邦の域外にある国又は地域をいう。以下同じ。）（**個人の権利利益を保護する上で我が国と同等の水準にあると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規則で定めるもの**を除く。以下この条において同じ。）」（法24条1項）	① **当該第三者が、個人の権利利益の保護に関して、我が国と同等の水準にあると認められる個人情報保護制度を有している国として規則で定める国にある場合**
適切かつ合理的な方法	「個人情報取扱事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、法第4章第1節の規定の趣旨に沿った措置の実施が確保されていること。」（規則11条の2第1号）「前条第1項各号に掲げる場合を除くほか」（法24条1項）**「適切かつ合理的な方法」は、個々の事例ごとに判断されるべきであるが、個人データの提供先である外国にある第三者が、我が国の個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずることを担保することができる方法である必要がある**。例えば、次の事例が該当する。 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場合 **提供元及び提供先間の契約、確認書、覚書等** 事例2）同一の企業グループ内で個人データを移転する場合 **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等**	② 個人情報取扱事業者と個人データの提供を受ける第三者との間で、当該第三者による個人データの取扱いについて、**適切かつ合理的な方法（契約、その他の形式の拘束力のある取決め又は企業グループにおける拘束力のある取扱い）により、本ルールを含め法と同等水準の個人情報の保護に関する措置を連携して実施している**場合
提供元がCBPR	また、アジア太平洋経済協力（APEC）の越境プライバシールール（CBPR）システム（※）の認証を取得している事業者は、その取得要件として、当該事業者に代わって第三者に個人情報を取り扱わせる場合においても、当該事業者が本人に対して負う義務が同様に履行されることを確保する措置を当該第三者との間で整備している必要があることとされている。 したがって、**提供元の個人情報取扱事業者がCBPRの認証を取得しており、提供先の「外国にある第三者」が当該個人情報取扱事業者に代わって個人情報を取り扱う者である場合には、当該個人情報取扱事業者がCBPRの認証の取得要件を充たすことも、「適切かつ合理的な方法」の一つであると解される**。なお、提供先の「外国にある第三者」がCBPRの認証を取得している場合については、本ガイドライン4-3（個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること（規則第11条の2第2号関係）)を参照のこと。	**対応なし**

APEC-CBPRだけ名指しで省かれているのでは？②

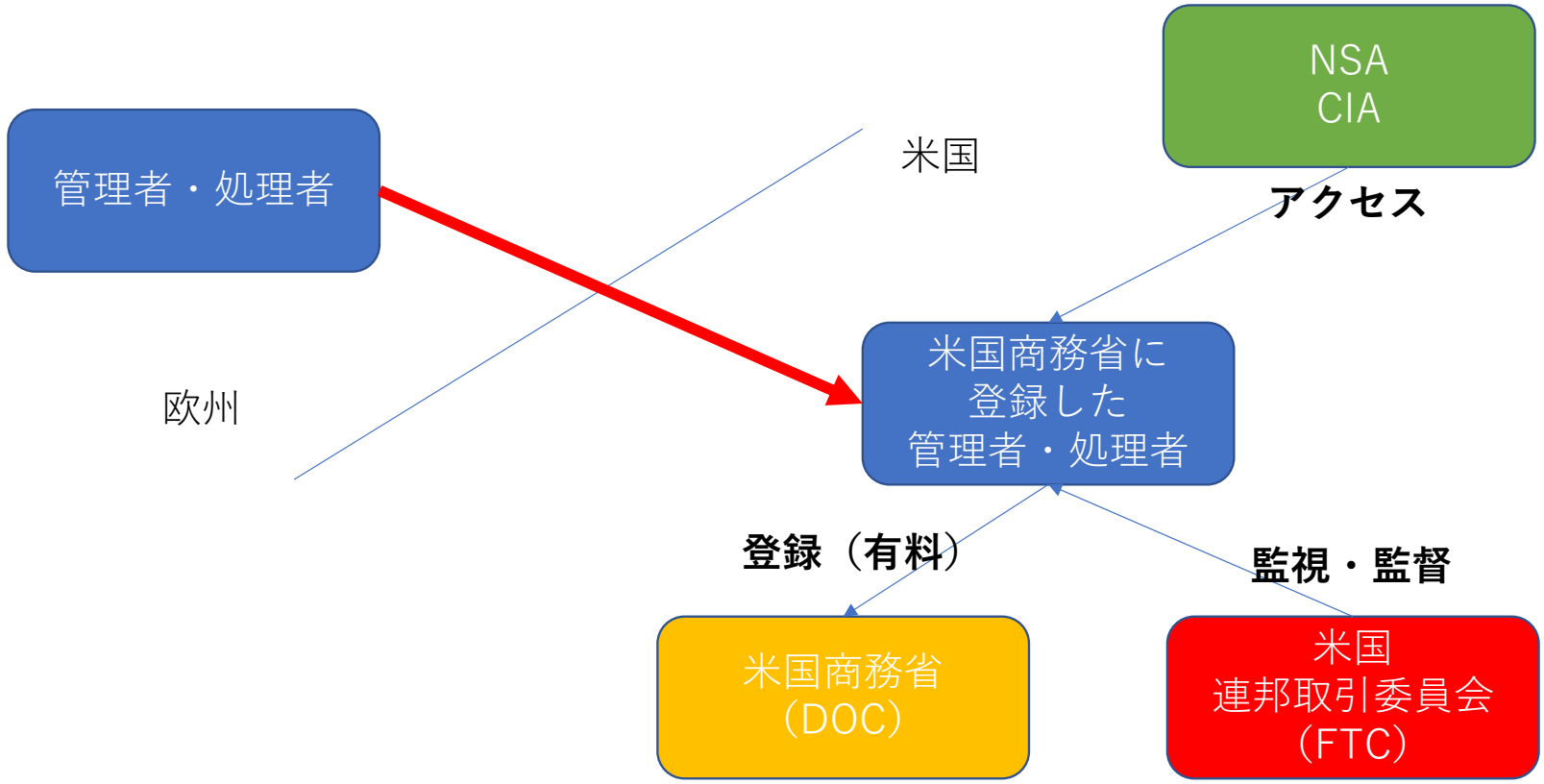
	外国第三者提供GL（パブコメ中）	補完的ルール
適用除外	「前条第1項各号に掲げる場合を除く」（法24条1項）	③ **法第 23 条第 1 項各号に該当する場合**
国際的な枠組みに基づく認定	「個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること。」（規則11条の2第2号） 「個人情報の取扱いに係る国際的な枠組みに基づく認定」とは、国際機関等において合意された規律に基づき権限のある認証機関等が認定するものをいい、当該枠組みは、個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずることのできるものである必要がある。**これには、提供先の外国にある第三者が、APECのCBPRシステムの認証を取得していることが該当する**。なお、個人データを提供する者がCBPRの認証を取得している場合については、本ガイドライン4-1（適切かつ合理的な方法（規則第11条の2第1号関係））を参照のこと。」（4-3）	**対応なし**

4-2　法第 4 章第 1 節の規定の趣旨に沿った措置（規則第 11 条の 2 第 1 号関係） 法第 24 条第 1 項の「この節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置」に該当するものとして規則第 11 条の 2 第 1 号に「法第 4 章第 1 節の規定の趣旨に沿った措置」と規定されている。 「法第 4 章第 1 節の規定の趣旨に沿った措置」については、外国にある第三者により個人データが取り扱われる場合においても、我が国の個人情報取扱事業者により個人データが取り扱われる場合に相当する程度の本人の権利利益の保護を図るという観点に加え、経済協力開発機構（OECD）におけるプライバシーガイドラインや APEC におけるプライバシーフレームワークといった国際的な枠組みの基準も踏まえた国際的な整合性も勘案する。	4-2　法第 4 章第 1 節の規定の趣旨に沿った措置（規則第 11 条の 2 第 1 号関係） 法第 24 条の「この節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置」に該当するものとして規則第 11 条の 2 第 1 号に「法第 4 章第 1 節の規定の趣旨に沿った措置」と規定されている。 具体的には、国際的な整合性を勘案して別表 2（※1）のとおりとなる。なお、国際的な整合性の判断は、経済協力開発機構（OECD）におけるプライバシーガイドラインや APEC におけるプライバシーフレームワークといった国際的な枠組みの基準に準拠している。

欧米プライバシーシールドの十分性認定
Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) C/2016/4176



個人データへの公的機関のアクセス



Maximillian Schrems v Data Protection Commissioner(C-362/14)（SchremsI決定）

(interpretation of Directive Art.25-26)

- …**in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union**

- …the term **‘adequate level of protection’ must be** understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, **a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.**

The Charter of Fundamental Rights of the European Union

- ***Article 7***
- Respect for private and family life
  - Everyone has **the right to respect for his or her private** and family life, home and communications.
- ***Article 8***
- Protection of personal data
  - 1. Everyone has **the right to the protection of personal data concerning him or her.**
  - 2. Such data must be processed fairly for specified purposes and on the basis of the consent of theperson concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
  - 3. Compliance with these rules shall be subject to control by an independent authori

SchremsII決定

- SchremsII決定では，”Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield is invalid.”，つまり，欧米プライバシーシールドについての十分性決定が無効とされた.
- その主たる理由は，移転先である米国におけるパブリック・アクセス，就中，**米国が安全保障のために執行している諜報法分野における措置が，欧州連合基本権憲章が求める権利の保障のレベルに達していない**ということにある.
- 特に問題である点として，
  - ①**米国の諜報法体系の下で，非米国人である（欧州市民を含む）データ主体が，米国当局に対して訴訟可能な権利を与えられていない**こと，
  - ②**米国の諜報機関を拘束するための権限を有するはずのオンブズパーソンの独立性が確保されていない**こと

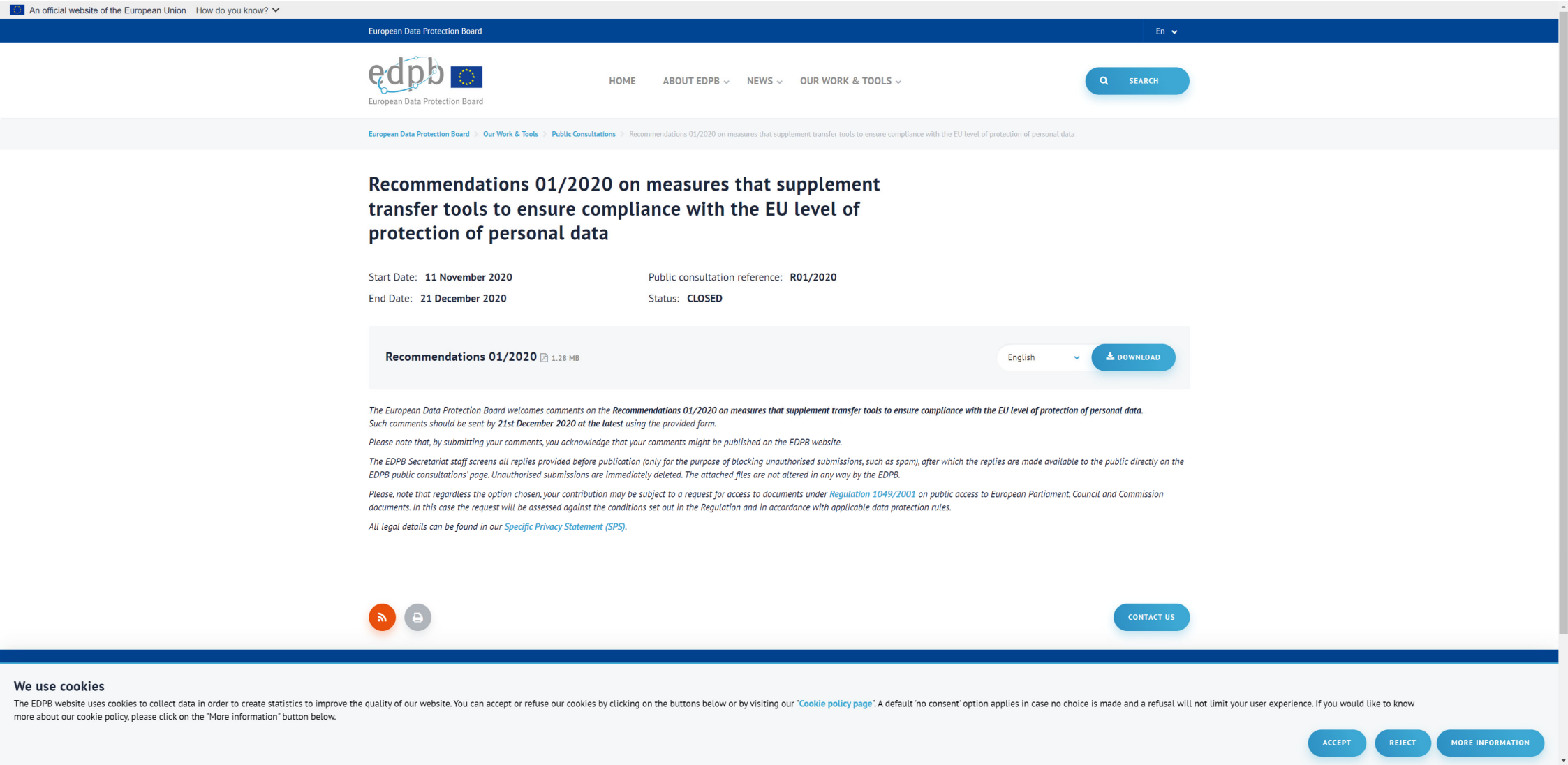
- 133 It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.
- 133 GDPR46 条(2)(c)に基づいて欧州委員会が採択した標準的なデータ保護約款は，EU に設立された管理者及び処理者に対して，すべての第三国で一律に適用される契約上の保証を提供することのみを目的としており，その結果，各第三国で保証されている保護レベルとは無関係である．これらの標準的なデータ保護条項は，その性質上，EU 法の下で要求される保護レベルへの準拠を保証するための契約上の義務を超える保証を提供することができない限りにおいて，特定の第三国の実勢に応じて，その保護レベルへの準拠を保証するために，管理者が追加的な措置を採用することを要求する場合がある．

- Schrems II決定は，プライバシーシールドについての十分性認定を無効であるとし，その主たる理由は，米国の諜報法分野におけるデータ主体の保護の薄弱さであった．ここで問題となっているのは移転先国たる米国における個人データの保護のレベルなのであるから，標準データ保護条項ないし標準契約約款（Standard Contractual Clauses）に基づく移転もできなくなるのではないかというのが，産業界の当然の懸念．
- 欧州連合司法裁判所は，「追加的な措置」が必要な場合があるとし，他方で，当該措置が必要な場合があることを前提に，標準データ保護約款による移転すべてを無効とはしなかった．
- この「追加的な措置」は，SchremsII決定が初出ではなく，一般データ保護規則（GDPR）前文109においても「追加的な保護措置」（additional safeguards）という語は現れていた．しかしながら，文脈的には，SDPCないしSCCを契約や約款の一部とすることは許され，より強い保護は奨励される，というものであり，追加的な措置が必要的な場合があるということを読み取ることは困難であった．

- GDPR前文(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. **Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses**.
- (109) 欧州委員会又は監督機関によって採択された標準データ保護約款を管理者又は処理者が利用することができるということは，欧州委員会又は監督機関によって採択された標準契約条項と直接又は間接に矛盾せず，かつ，データ主体の基本的な権利及び自由を妨げるものではない限り，管理者又は処理者が，処理者と別の処理者との間の契約のような，より広範囲の契約の中に標準データ保護条項を含めることを妨げるものではなく，また，その約款の中に別の条項や保護措置を追加することを妨げるものでもない。**管理者及び処理者は，標準データ保護条項を補完する契約上の約定を介して，追加的な保護措置を提供することが奨励されなければならない**.

追加的措置についての動き

- EDPB（欧州データ保護ボード）
  - 2020年11月11日には，"Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"（EUの個人データ保護のレベルの遵守を確実にするための移転ツールに追加する措置に関する勧告，「追加的措置勧告」）を公表し，2020年12月21日までパブリックコメントに付した
    - 締切までには178件の意見が提出されている.
- 欧州委員会
  - 2020年11月12日に第三国への個人データの移転に関する標準契約約款である"IMPLEMENTING DECISION (EU) …/… of XXX on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council"のドラフトを公表し，2020年12月10日までパブリックコメントに付した.
    - 締め切りまでには149件の意見が提出されている.
- EDPB及びEDPS（欧州データ保護観察官）
  - 新SCC案に2021年1月14日に合同で意見を述べている
    - EDPB - EDPS Joint Opinion 1/2021 on the European Commission’s Implementing Decision on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725.


An official website of the European Union How do you know?
European Data Protection Board
En
edpb
European Data Protection Board
HOME
ABOUT EDPB
NEWS
OUR WORK & TOOLS
SEARCH
European Data Protection Board > Our Work & Tools > Public Consultations > Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
Start Date: 11 November 2020
End Date: 21 December 2020
Public consultation reference: R01/2020
Status: CLOSED
Recommendations 01/2020 1.28 MB
English
DOWNLOAD
The European Data Protection Board welcomes comments on the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Such comments should be sent by 21st December 2020 at the latest using the provided form.
Please note that, by submitting your comments, you acknowledge that your comments might be published on the EDPB website.
The EDPB Secretariat staff screens all replies provided before publication (only for the purpose of blocking unauthorised submissions, such as spam), after which the replies are made available to the public directly on the EDPB public consultations' page. Unauthorised submissions are immediately deleted. The attached files are not altered in any way by the EDPB.
Please, note that regardless the option chosen, your contribution may be subject to a request for access to documents under Regulation 1049/2001 on public access to European Parliament, Council and Commission documents. In this case the request will be assessed against the conditions set out in the Regulation and in accordance with applicable data protection rules.
All legal details can be found in our Specific Privacy Statement (SPS).
CONTACT US
We use cookies
The EDPB website uses cookies to collect data in order to create statistics to improve the quality of our website. You can accept or refuse our cookies by clicking on the buttons below or by visiting our "Cookie policy page". A default 'no consent' option applies in case no choice is made and a refusal will not limit your user experience. If you would like to know more about our cookie policy, please click on the "More information" button below.
ACCEPT
REJECT
MORE INFORMATION

Data protection - standard contractual clauses for transferring personal data to non-EU countries (implementing act)

Draft act

Feedback period

12 November 2020 - 10 December 2020

FEEDBACK: CLOSED

UPCOMING

Commission adoption

About this initiative

Topic	Justice and fundamental rights
Type of act	Implementing decision
Committee	C49000

Draft act

FEEDBACK: CLOSED

Type

Draft implementing decision

More about draft acts

Feedback period

12 November 2020 - 10 December 2020 (midnight Brussels time)

View feedback received >

Draft implementing decision - Ares(2020)6654686
English (284.2 KB - PDF - 9 pages) — Download

Annex - Ares(2020)6654686
English (514.7 KB - PDF - 29 pages) — Download

Feedback (148)

10 December 2020

Anonymous

The EORTC welcomes the updates in the EU SCC, especially since they were at the center of many legal uncertainties linked to data transfer in light of Brexit and Schrems II case law. This issue has been especially challenging for stakeholders involved in conducting health research (legal sponsors, academic universities, investigators). Our main observations are: - The title is very misleading for the contracts departments in clinical...

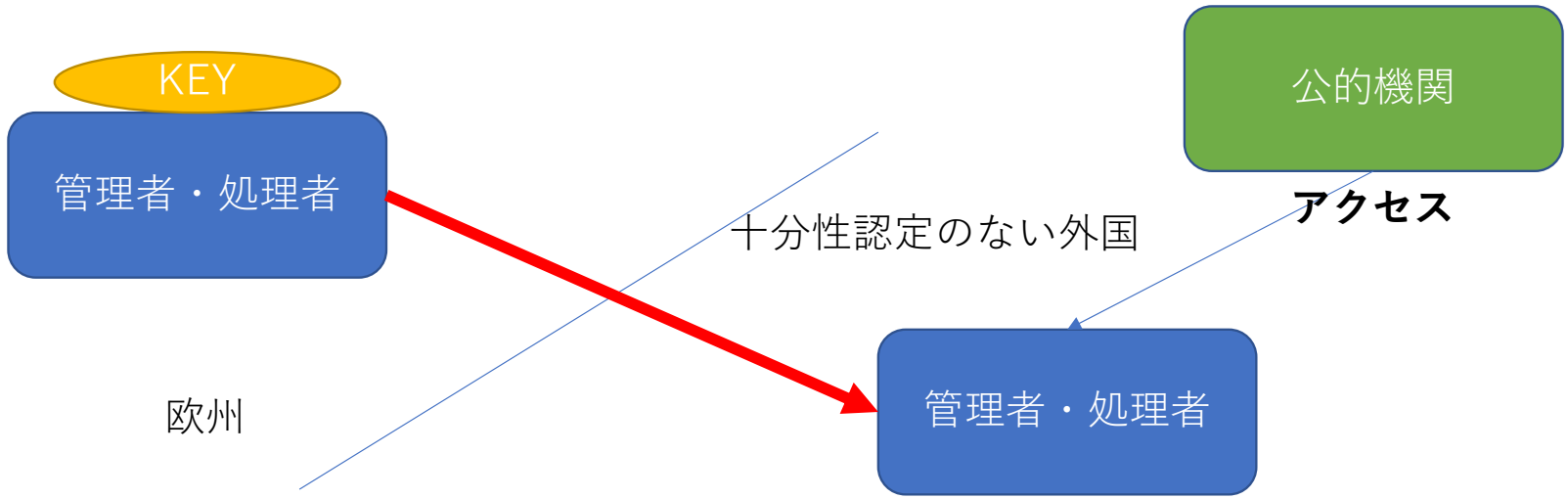
2. "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data“（EUの個人データ保護のレベルの遵守を確実にするための移転ツールに追加する措置に関する勧告，「追加的措置勧告」）

- **ステップ1　移転の認知**
  - すべての移転を認知し，マッピングすることを求めており，GDPR30条も根拠となる（8項，9項）．越境のリモートアクセスや海外のクラウドの利用も含まれる（13項）．
- **ステップ2　移転ツール（越境移転に関する適法化事由）の特定**
  - 十分性認定，SCC，BCR，行動規範，認証メカニズム，GDPR49条の例外事由のいずれを根拠として移転しているかを確認する（14項以下）．
- **ステップ3　移転ツールの有効性**
  - 輸入者と協力して，第三国の法律や慣行が移転ツールの有効性に影響を及ぼすかを評価しなければならない（30項）．複雑なスキームの場合は評価も複雑となる（31項）．移転の文脈が影響する，処理目的，処理に関与する機関の種類（公的，私的，管理者，処理者），分野（金融，通信，広告等），第三国に保存されるものか，アクセスするだけか，移転されるデータがプレーンテキストか，暗号化されているか，再移転があるか等（33項），アクセス権等が移転先国の法令等により妨げられないか（34項），パブリックアクセス及び，その際のデータ主体の救済の権利は特記されている（35項）．これは，SchremsIIにおいてプライバシーシールドの十分性認定が無効となった一因である．刑事法の執行，国家安全保障目的の規制にも特別に注意せよとされている（36項）．この際，EDPBのEEG勧告（Recommendations 02/2020 on the European Essential Guarantees for surveillance measures）の諸要素が参考になるとされている（39項），評価は公開されている法例を中心とし，文書化される必要がある（42項）．SchremsII決定で問題となったのは，米国FISAの702条であり，比例原則を満たさないとした．この場合，追加的な措置により，米国の諜報機関からのアクセスが不可能又は非効率となる必要がある．
- **ステップ4　追加的な措置の採用**
  - 追加的な措置には，契約的，技術的，組織的なものが含まれ，それらの組み合わせも推奨される（47項，48項）．技術的な措置はパブリックアクセスを阻害できるということが前提になっている．具体的なリストは別紙2.
- **ステップ5　有効な追加的な措置を確認した場合の手続**
  - データ保護機関の確認は不要（56項），SCCと矛盾する場合は，（SCCではなくなるため）個別の移転の承認が必要になる（57項），GDPR46条2.の適法化根拠は，第三国の公的機関を拘束しない（58項）．BCRについてはEDPBも検討中である（59項）．アドホックな契約（GDPR46条3.）もEDPBは検討中である（61項）．
- **ステップ6　再評価**
  - 継続的な再評価の必要性を述べる（62～63項）．

追加的措置

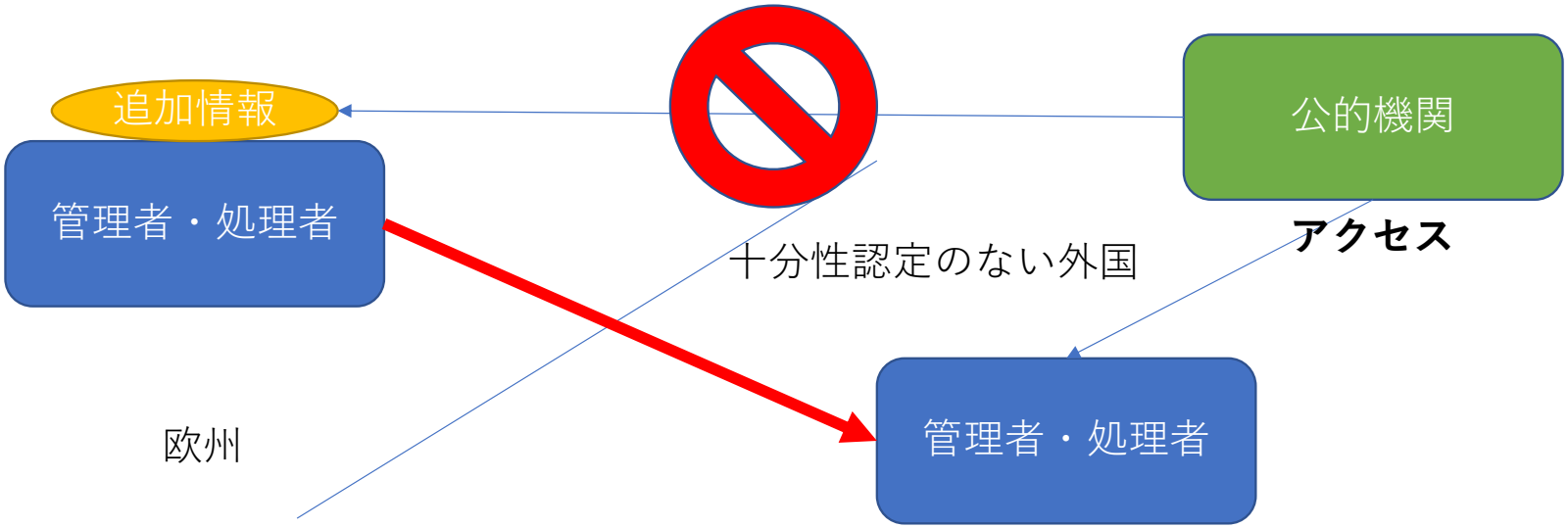
- 技術的な追加的な措置
  - 有効なユースケースと無効なユースケースを列挙している．有効なユースケースとしては，
    - ①強力な暗号化がなされている場合の第三国におけるバックアップ，
    - ②適切な仮名化がなされている場合の移転，
    - ③エンドツーエンド暗号化がなされている場合の，第三国の通過，
    - ④暗号化がなされている場合の，特に保護された輸入者への移転，
    - ⑤秘密計算の利用が挙げられている．
  - 他方，無効なユースケースとして，
    - ⑥クラウドサービスを利用した場合，当該サービスにパブリックアクセスが行われる場合，
    - ⑦ビジネス目的でリモートアクセスを行うが，パブリックアクセスが行われる場合，が挙げられている．
  - いずれも詳細には要件が挙げられており，あくまで例示ではあるが，クラウドサービスを利用した場合のパブリックアクセスについては（米国を意識してか）特に厳しい見解ではないかと思われる．

Use Case 1: Data storage for backup and other purposes that do not require access to data in the clear



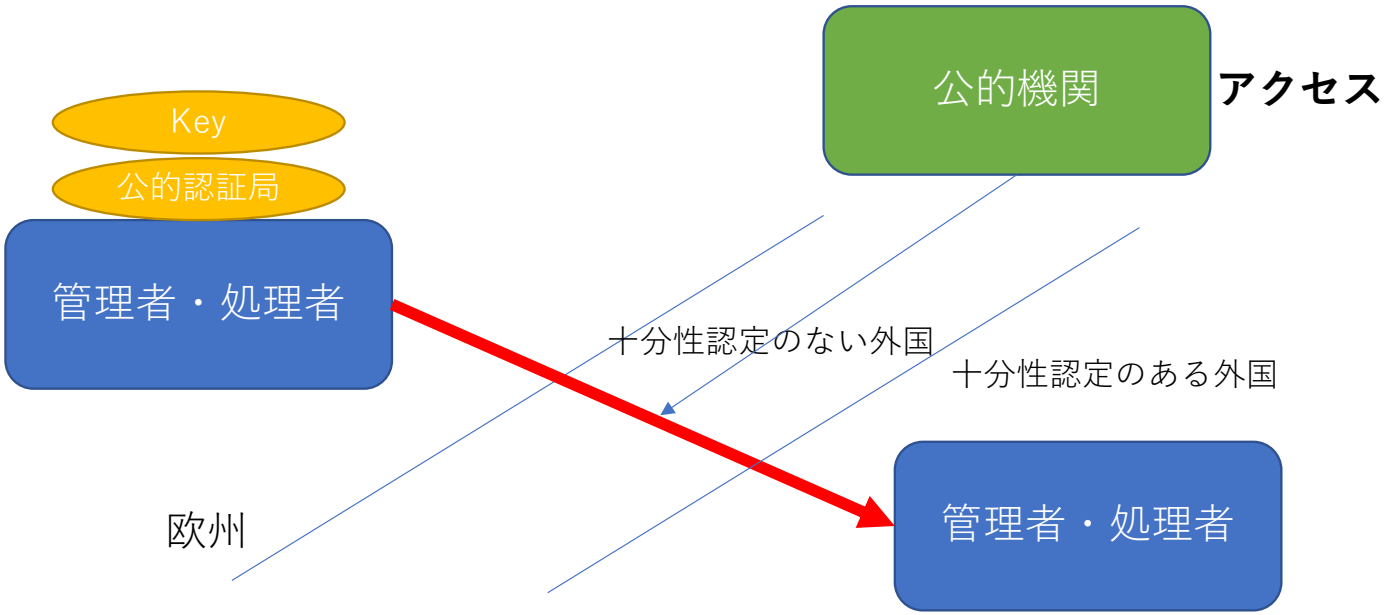
1. the personal data is processed using **strong encryption** before transmission,
2. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered **robust against cryptanalysis performed by the public authorities** in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,
3. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved
4. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, **e.g., by certification**,
5. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and
6. **the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured**,

Use Case 2: Transfer of pseudonymised Data



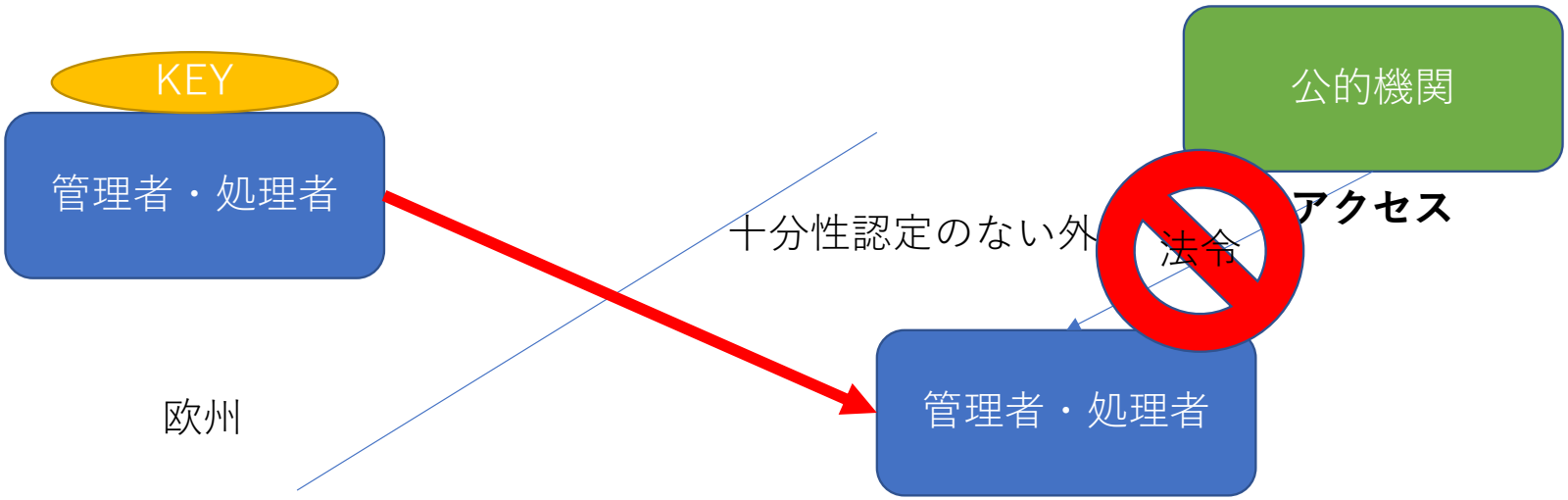
1. a data exporter transfers personal data processed in such a manner that **the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information**,
2. **that additional information is held exclusively** by the data exporter and kept separately in a Member State or in a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured,
3. **disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards**, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information, and
4. the controller has established by means of a thorough analysis of the data in question taking into account any information that the public authorities of the recipient country may possess **that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information**,

Use Case 3: Encrypted data merely transiting third countries



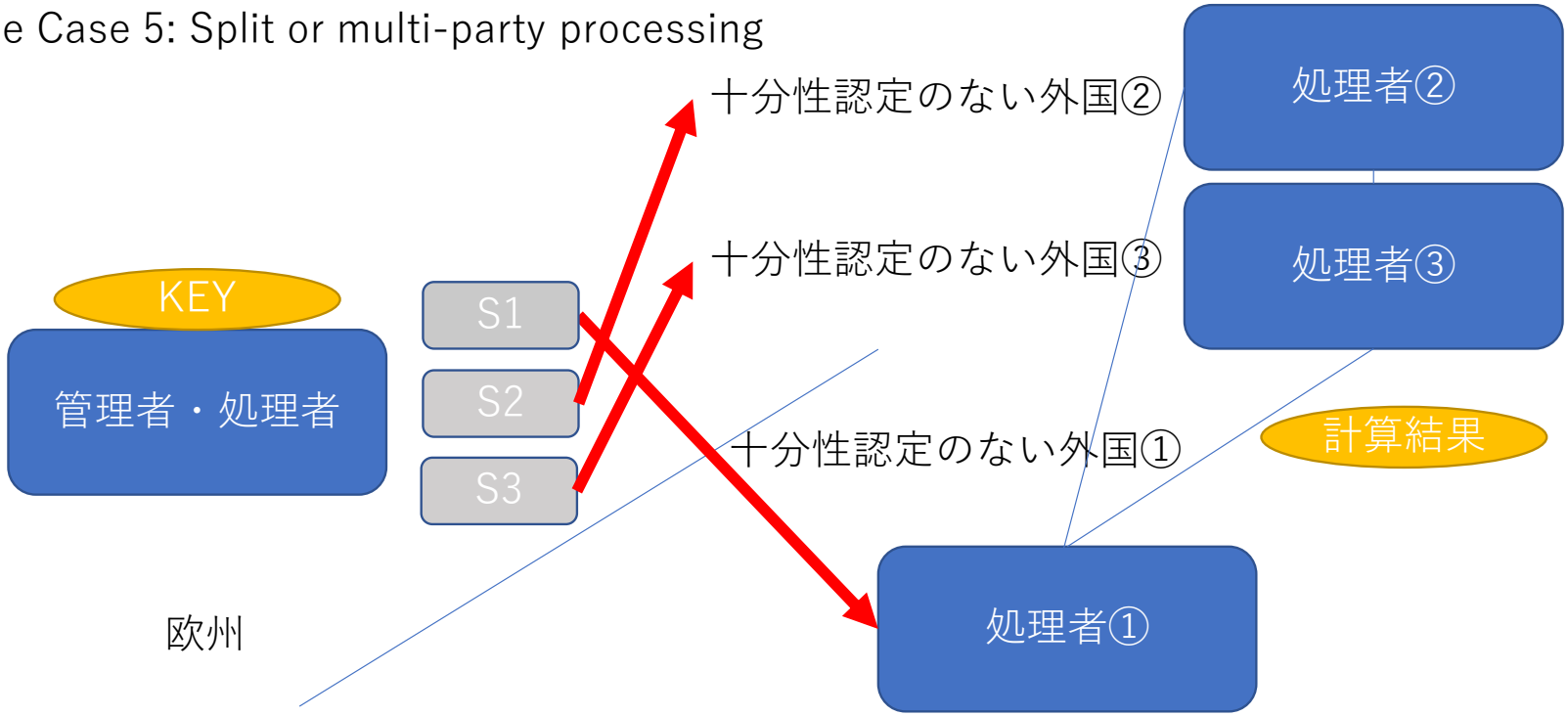
1. a data exporter transfers personal data to a data importer in a jurisdiction ensuring adequate protection, the data is transported over the internet, and **the data may be geographically routed through a third country not providing an essentially equivalent level of protection,**
2. **transport encryption is used** for which it is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of the third country,
3. decryption is only possible outside the third country in question,
4. the parties involved in the communication agree on **a trustworthy public-key certification authority or infrastructure**,
5. specific protective and state-of-the-art measures are used against active and passive attacks on transport-encrypted,
6. in case the transport encryption does not provide appropriate security by itself due to experience with vulnerabilities of the infrastructure or the software used, personal data is also encrypted end-to-end on the application layer using state-of-the-art encryption methods,
7. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the transiting country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,
8. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,
9. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,
10. the existence of backdoors (in hardware or software) has been ruled out,
11. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of the intended recipient, and revoked), by the exporter or by an entity trusted by the exporter
12. under a jurisdiction offering an essentially equivalent level of protection

Use Case 4: Protected recipient



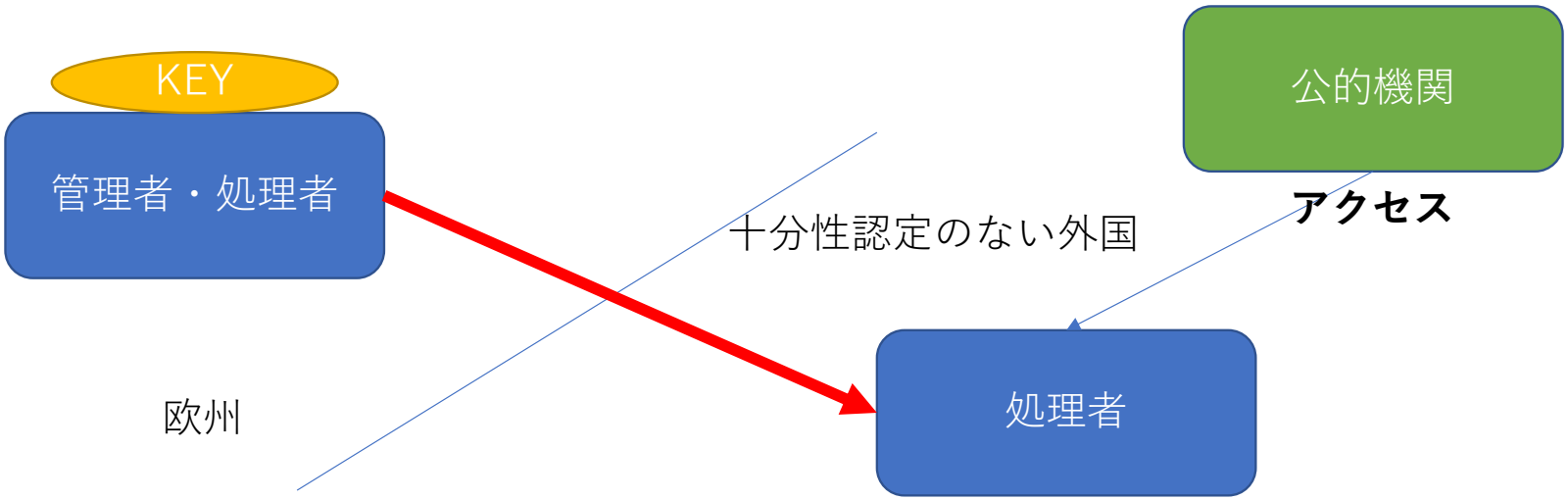
1. the law of a third country **exempts a resident data importer from potentially infringing access to data held by that recipient for the given purpose, e.g. by virtue of a duty to professional secrecy applying to the data importer**,
2. that exemption extends to all information in the possession of the data importer that may be used to circumvent the protection of privileged information (cryptographic keys, passwords, other credentials, etc.),
3. the data importer does not employ the services of a processor in a way that allows the public authorities to access the data while held by the processor, nor does the data importer forward the data to another entity that is not protected, on the basis of Article 46 GDPR transfer tools,
4. the personal data is encrypted before it is transmitted with a method conforming to the state of the art guaranteeing that decryption will not be possible without knowledge of the decryption key (end-to-end encryption) for the whole length of time the data needs to be protected,
5. the decryption key is in the sole custody of the protected data importer, and appropriately secured against unauthorised use or disclosure by technical and organisational measures conforming to the state of the art, and
6. the data exporter has reliably established that the encryption key it intends to use corresponds to the decryption key held by the recipient,

Use Case 5: Split or multi-party processing



1. a data exporter processes personal data **in such a manner that it is split into two or more parts each of which can no longer be interpreted or attributed to a specific data subject without the use of additional information**,
2. **each of the pieces is transferred to a separate processor located in a different jurisdiction**,
3. the processors optionally process the data jointly, e.g. using secure multi-party computation, in a way that no information is revealed to any of them that they do not possess prior to the computation,
4. the algorithm used for the shared computation is secure against active adversaries,
5. **there is no evidence of collaboration between the public authorities located in the respective jurisdictions where each of the processors are located**, which would allow them access to all sets of personal data held by the processors and enable them to reconstitute and exploit the content of the personal data in a clear form in circumstances where such exploitation would not respect the essence of the fundamental rights and freedoms of the data subjects. Similarly, public authorities of either country should not have the authority to access personal data held by processors in all jurisdictions concerned.
6. the controller has established by means of a thorough analysis of the data in question, taking into account any information that the public authorities of the recipient countries may possess, that the pieces of personal data it transmits to the processors cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,

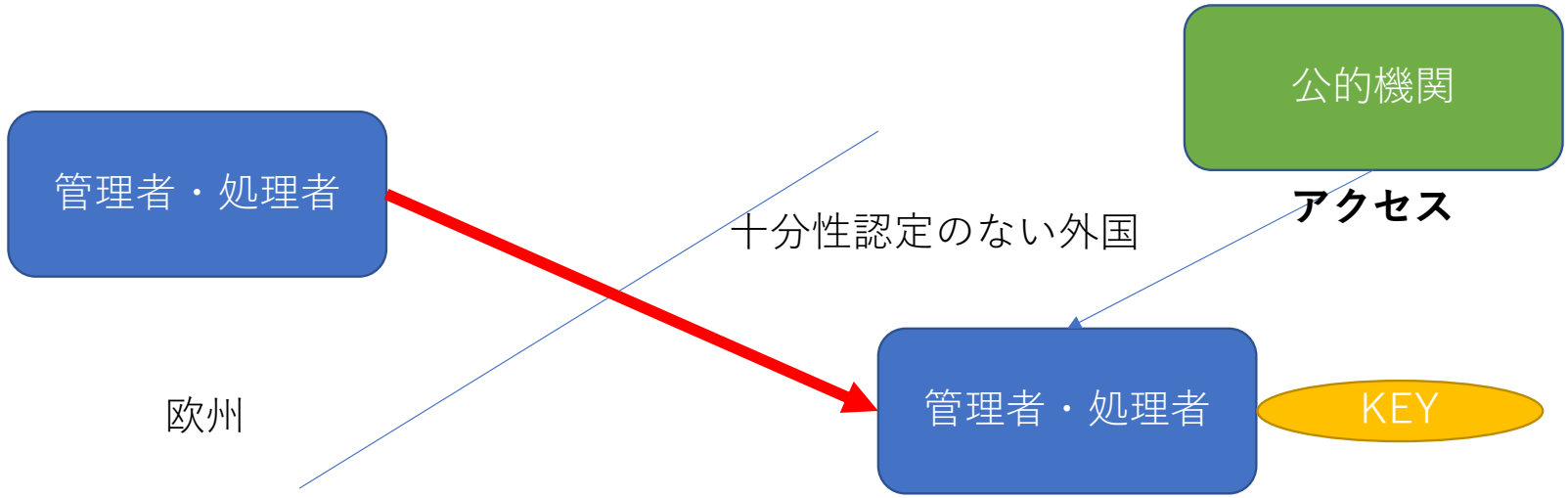
Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear



1. a controller transfers data to a cloud service provider or other processor,
2. the cloud service provider or other processor needs access to the data **in the clear in order to execute the task assigned**, and
3. **the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society**

then the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear.
89. In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.

Use Case 7: Remote access to data for business purposes



1. a data exporter transfers personal data to a data importer in a third country by making it available in a commonly used information system in a way that allows the importer direct access of data of its own choice, or by transferring it directly, individually or in bulk, through use of a communication service,
2. the importer uses the data in the clear for its own purposes,
3. **the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,**

then the EDPB is incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights.

91. In the given scenarios, **where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys**.

契約的な追加的な措置

- 契約的な追加的な措置はナンバリングされていない．第三国の当局は拘束できないことが前提とされ（93項），他の技術的又は組織的な措置を組み合わせることが推奨される（同）．例として，以下が挙げられている．
  - 特定の技術的手段を使用する義務
  - 透明性義務（パブリックアクセスについての根拠法令の列挙等）
  - 具体的な行動を取る義務（開示命令への異議申し立て等）
  - データ主体への権利付与（データ主体の同意を前提としたアクセス等）
  - 特にグループ企業間の移転に関する内部統制
  - 透明性およびアカウンタビリティの義務（パブリックアクセスについての文書の記録とデータ輸出者への開示等）
  - 組織的手法及びデータ最小化措置（アクセス権限等についての限定）
  - 標準やベストプラクティスの受容（ISO等）
  - その他（内部監査，再移転禁止）

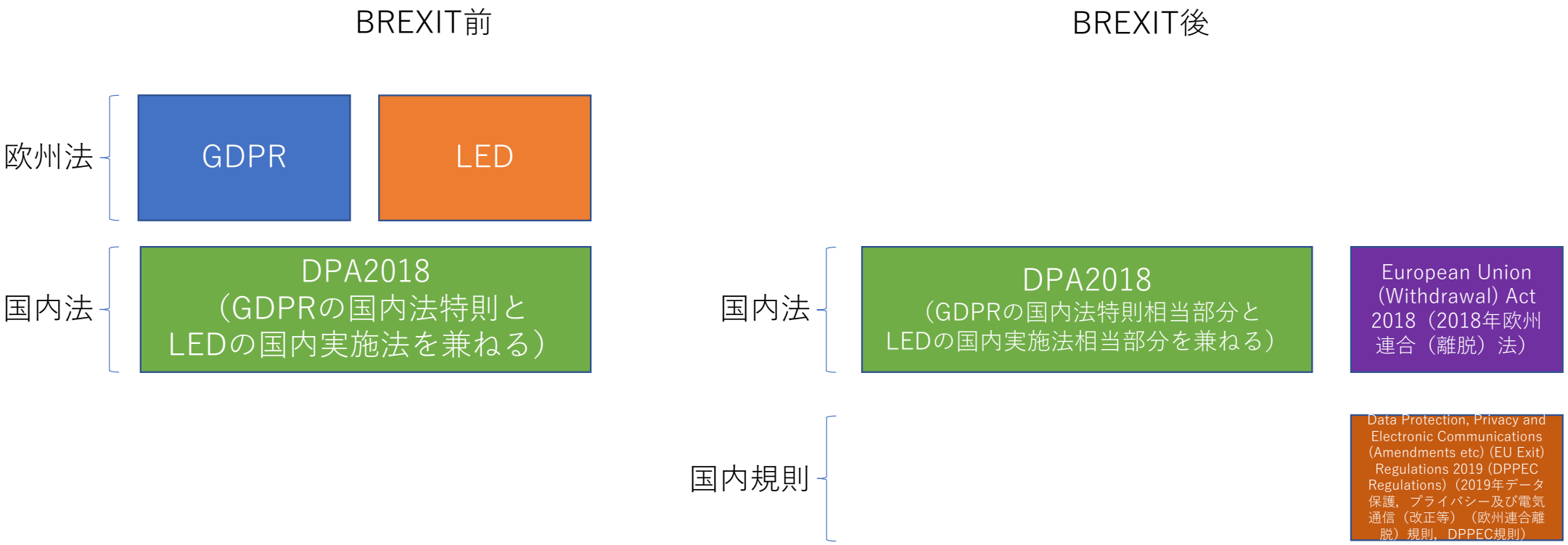
英国の十分性認定手続

- GDPR全面適用後に認定されたのは日本（個人情報保護法の適用範囲）のみ.
- 2021年2月19日に，いわゆるブレグジットにより欧州連合を離脱した英国のデータ保護制度について，欧州委員会が一般データ保護規則（GDPR)及び法執行指令（LED）上の十分性認定のドラフトを公開した（以下，それぞれ「GDPRドラフト」，「LEDドラフト」という．）
  - GDPR上の十分性認定手続が開始した国として，英国は日本に注いで二例目ということになる.

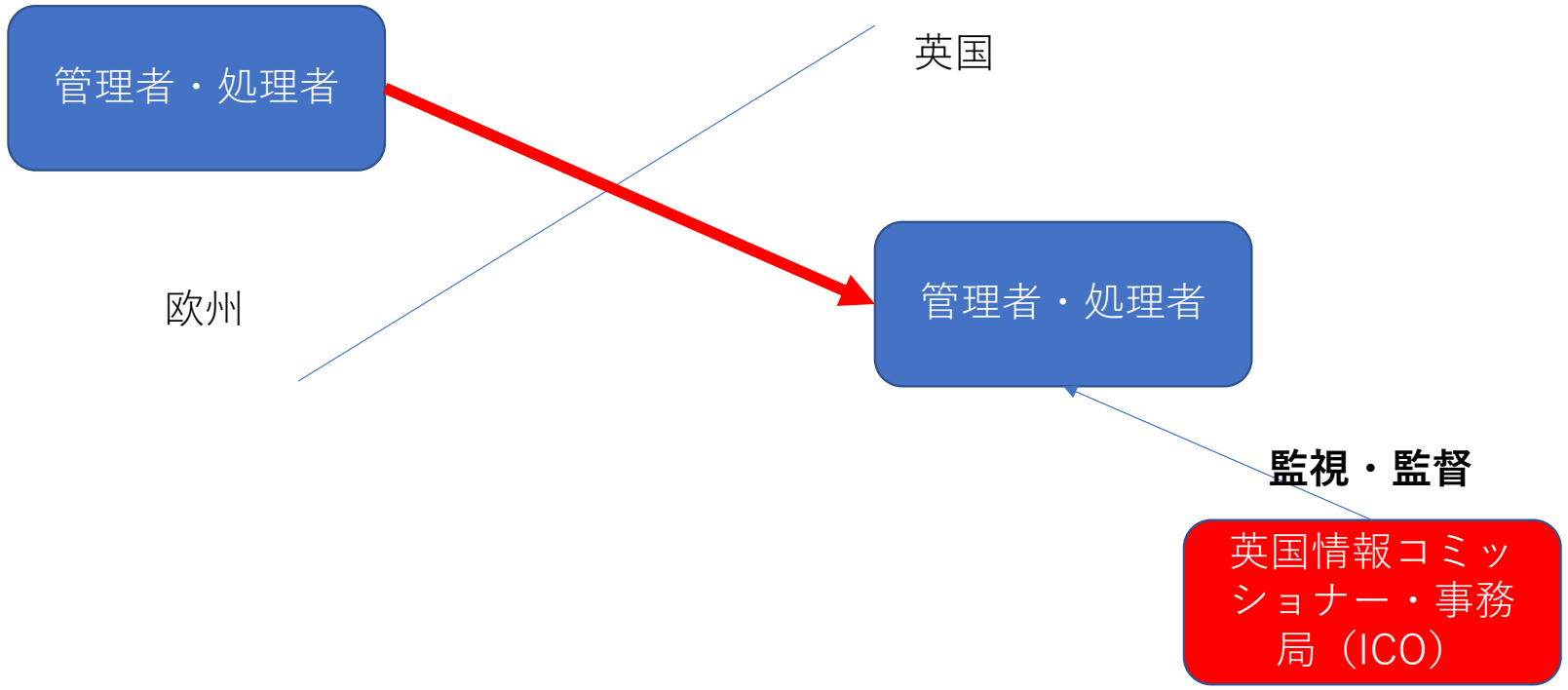
英国のデータ保護制度

- 英国では，GDPRを国内法化したUK GDPRと，Data Protection Act 2018（2018年データ保護法，DPA2018）がデータ保護制度の中心を構成しているが，その構造はやや複雑
- 英国は欧州連合から離脱したので，GDPRは直接適用されないが，**European Union (Withdrawal) Act 2018（2018年欧州連合（離脱）法）の二次法であるData Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019（DPPEC Regulations）（2019年データ保護，プライバシー及び電気通信（改正等）（欧州連合離脱）規則，DPPEC規則）により，GDPRをほぼそのまま，法律の二次法としての規則として採用することにした（UK GDPR）**
- 本家GDPRは各国の国内法化を待たずして執行され得る欧州法上の「規則」であったが，UK GDPRは，形式的には英国の法律の二次法である「規則」であり，法律レベルでの根拠は2018年欧州連合（離脱）法である。
- 同じ「規則」であるが，このようにGDPRとUK GDPRの位置付けは異なるので注意
- **DPA2018はブレグジットまではGDPR及びLEDの国内実施法の役割を有していたが，ブレグジット後は，UK GDPRの例外規定部分及び，LEDの適用範囲である法執行機関（警察，検察等）及び情報機関（いわゆる諜報機関）についてのデータ保護を定める法律としての役割を担うことになった**.
- DPA2018の3章が法執行機関のデータ保護を，4章が情報機関のデータ保護をそれぞれ定めている.

英国のデータ保護制度


BREXIT前
BREXIT後
欧州法
GDPR
LED
国内法
DPA2018
（GDPRの国内法特則と
LEDの国内実施法を兼ねる）
国内法
DPA2018
（GDPRの国内法特則相当部分と
LEDの国内実施法相当部分を兼ねる）
European Union (Withdrawal) Act 2018（2018年欧州連合（離脱）法）
国内規則
Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (DPPEC Regulations)（2019年データ保護，プライバシー及び電気通信（改正等）（欧州連合離脱）規則，DPPEC規則）

英国へのデータ移転（GDPR）

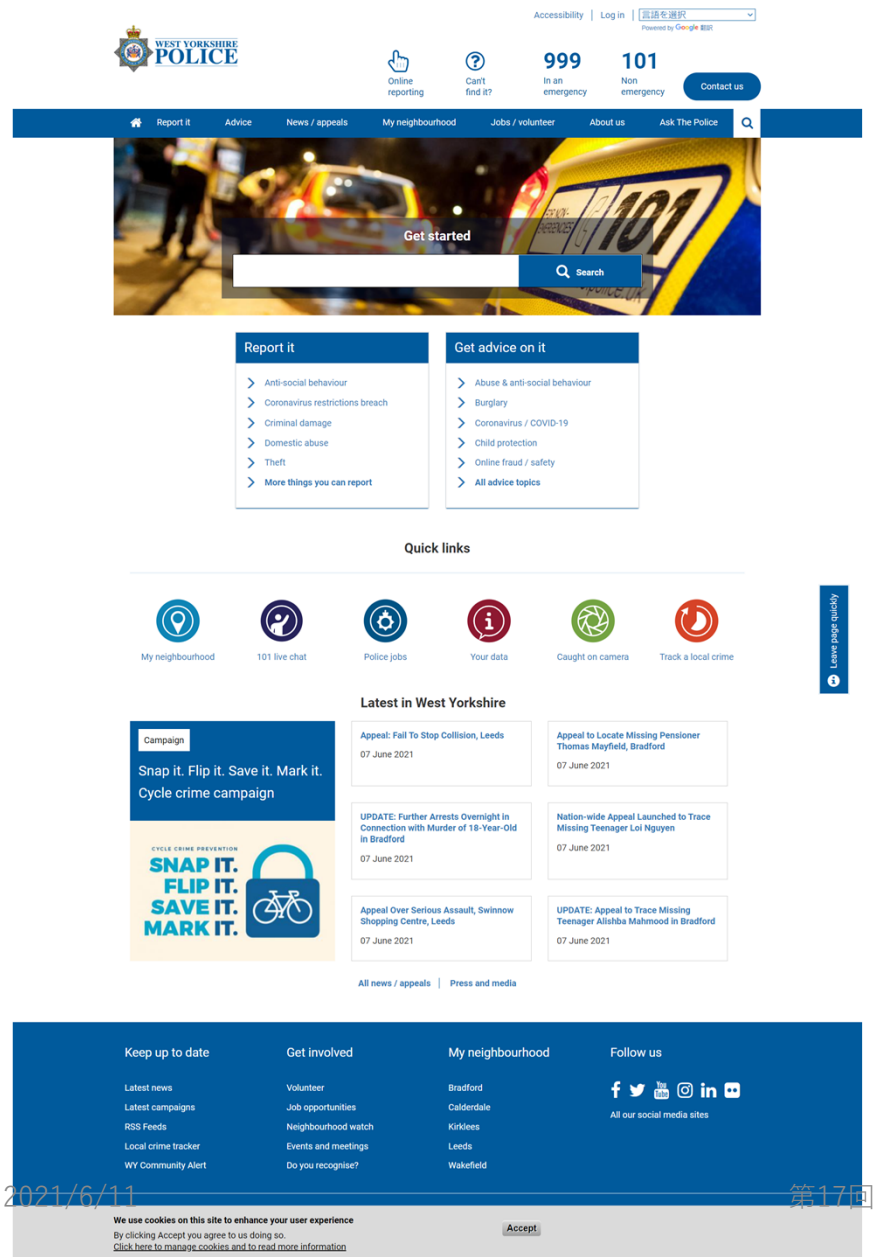


GDPRドラフト2章
データ保護に適用されるルール

- 通常のデータ保護についての検討部分（UK GDPRの適用範囲）
  - UK GDPRはGDPRをほぼ引き写しているため，欧州委員会としてはその部分はそのまま受け入れている（当然であるが）．
  - 例えば，GDPRの中心的な条項である6条（処理の適法化事由）や7条（同意の要件）等はほぼ同じであることがあっさり書かれている（GDPRドラフト24～25項）．
- DPA2018による例外規定の具体化部分
  - 機微情報の処理が許される「実質的な公益」についてのDPA2018附則1第2章（GDPRドラフト30項以下）
  - 個人の権利の制限についてのDPA2018附則2ないし4（特定性と機密性原理，GDPRドラフト55項以下）
  - 報道，芸術，学術及び文学並びにアーカイブ及び研究についての例外（DPA2018附則2第5章）（GDPRドラフト70項以下）
- 監督機関
  - 英国情報コミッショナー：同事務局（ICO）は2020年3月段階で768人の常勤職員を擁する．英国は，データ管理者の登録料を継続している極めて稀な国であり，予算の85～90％は登録料からなる．7年任期，再選不可（GDPRドラフト85～91項）．

GDPRドラフト3章
欧州連合から移転された個人データの，英国の公的機関によるアクセスと利用

- DPA2018の3章が法執行機関の，4章が情報機関のデータ保護を定めている
  - 4章には「国家安全保障」のための制限規定が存在するが，この制限規定を利用するためには，閣僚か，検事総長の署名を付した承認が必要である．期間は5年を超えず，対象も制限される（GDPRドラフト126及び127項）．
  - 承認について，上級審判所への異議申立ても可能である（同128項）．



https://www.westyorkshire.police.uk/about-us/our-departments/mounted-section/mounted-section

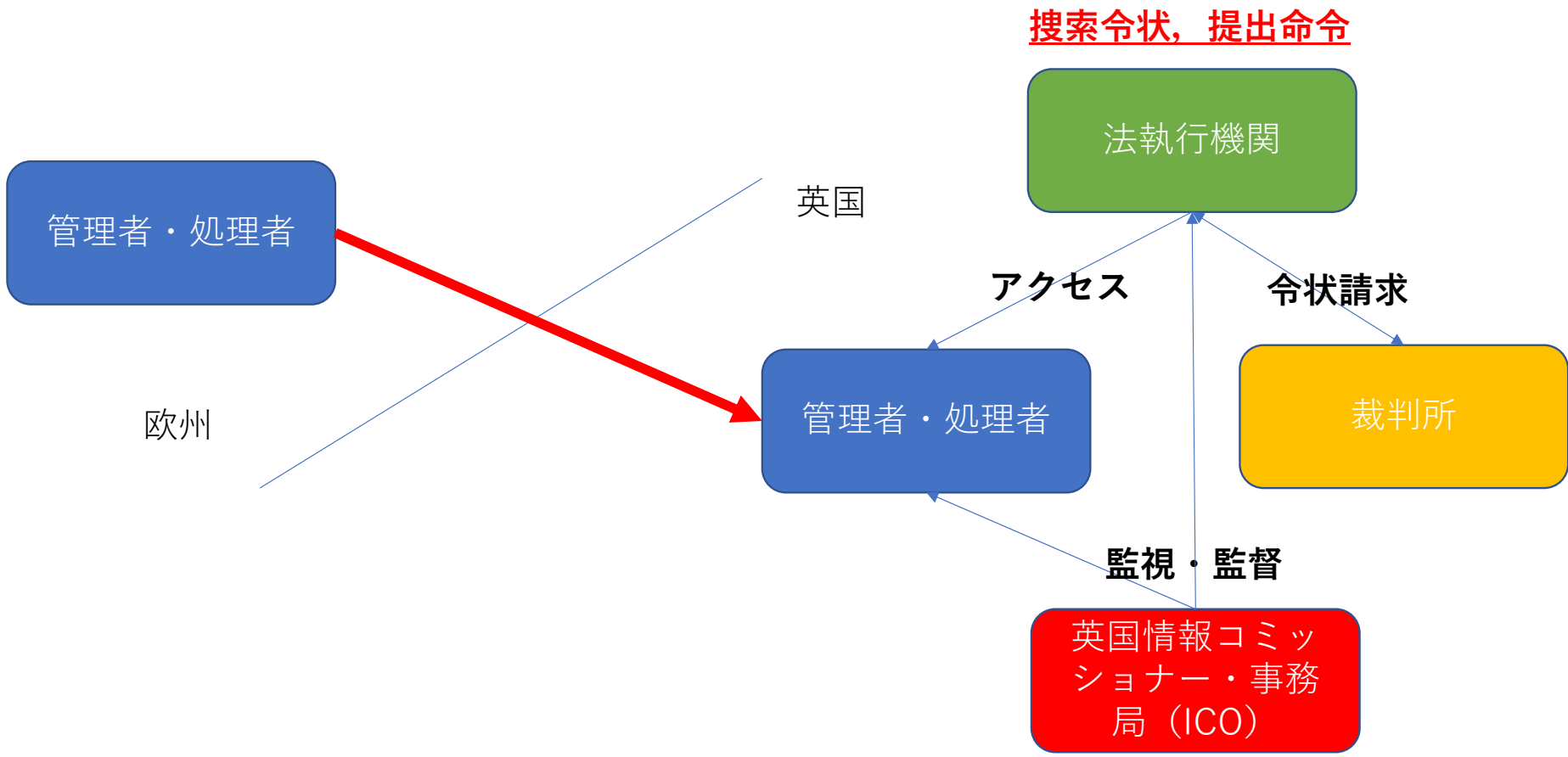
法執行機関のアクセス

- 法執行機関のアクセス
  - 根拠は，**捜索令状と提出命令であり，いずれも裁判所の審査を経由する**（GDPRドラフト134項）．
  - 重大犯罪の防止等のためには，**標的型傍受（2016年捜査権限法（IPA2016）第2章），通信データの取得（IPA2016第3章），通信データの保持（IPA2016第4章），標的型機器干渉（IPA2016第5章）等が可能**であるが，「一括捜査」は不可能である（情報機関は可能）．
  - これらの情報収集手段は，主務官庁が請求し，独立した司法委員が許諾した令状による必要がある（「二重鍵」手続と呼ばれている）（GDPRドラフト139項）．

「再共有」

- 一般の管理者等に「再移転」の問題があるように，法執行機関には，「再共有」の問題がある．
- 法執行機関が，非・法執行機関と個人データを共有する場合や，法執行機関が情報機関と共有する場合などが想定され，根拠法が定められている（GDPRドラフト140項以下）．
- 米国クラウド法の下で締結された英米協定については，欧米アンブレラ協定で提供されている保護と同等の保護が提供されていると評価されている（GDPRドラフト151項以下）．
- 法執行機関への監督は，英国情報コミッショナーが行う他，IPA2016で設置された捜査権限コミッショナー事務局（IPCO），生体情報コミッショナー，監視カメラコミッショナーが複合的に行っているとされる（GDPRドラフト155項以下，162項以下は議会による監視も記述）．

個人データへの公的機関のアクセス（通常令状）



IPCO
Investigatory Powers Commissioner's Office

Who we are | What we do | Investigatory Powers | Publications | News | Contact us

Home > Who we are

Who we are

Overseen by the Investigatory Powers Commissioner, Sir Brian Leveson, the Investigatory Powers Commissioner's Office (more commonly known as IPCO) currently employs approximately 50 people, including Inspectors, lawyers and policy officials.

The team supports the Investigatory Powers Commissioner and Judicial Commissioners in fulfilling their duties under the Investigatory Powers Act 2016.

Before this legislation came into force, three precursor organisations were merged to form IPCO in September 2017. The previous organisations were the Office of Surveillance Commissioners (OSC), the Interception of Communications Commissioner's Office (IOCCO) and the Intelligence Service Commissioner's Office (ISComm).

Under the terms of the Investigatory Powers Act 2016, funding for IPCO is provided by the Home Secretary. However, IPCO carries out its functions independently of the Government and is not part of the Home Office.

Investigatory Powers Commissioner

The Investigatory Powers Commissioner, Sir Brian Leveson, has responsibility for reviewing the use of investigatory powers by public authorities, such as intelligence agencies, police and local authorities. He is supported by a team of Judicial Commissioners.

Read more >

Judicial Commissioners

A Judicial Commissioner is a serving or retired member of the senior judiciary in the UK. Judicial Commissioners support the Investigatory Powers Commissioner in his oversight duties by providing independent authorisation of applications for the use of certain investigatory powers. These powers are used by public authorities.

Read more >

Organisations we oversee

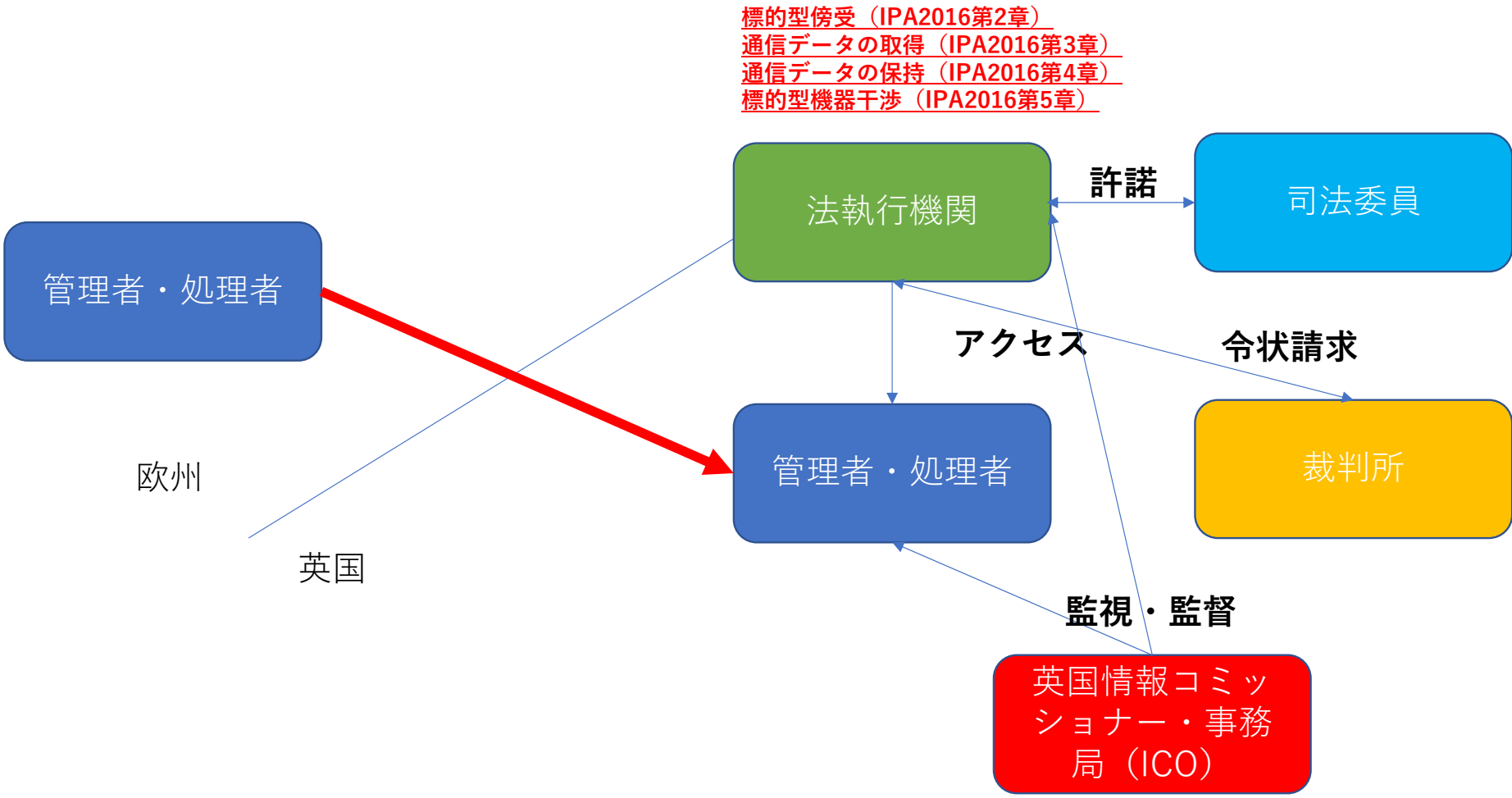
We oversee the use of covert powers by over 600 public authorities. The organisations can broadly be categorised into six groups:

- Intelligence agencies
- Police and law enforcement agencies
- Local authorities
- Prisons
- Warrant granting departments
- Others

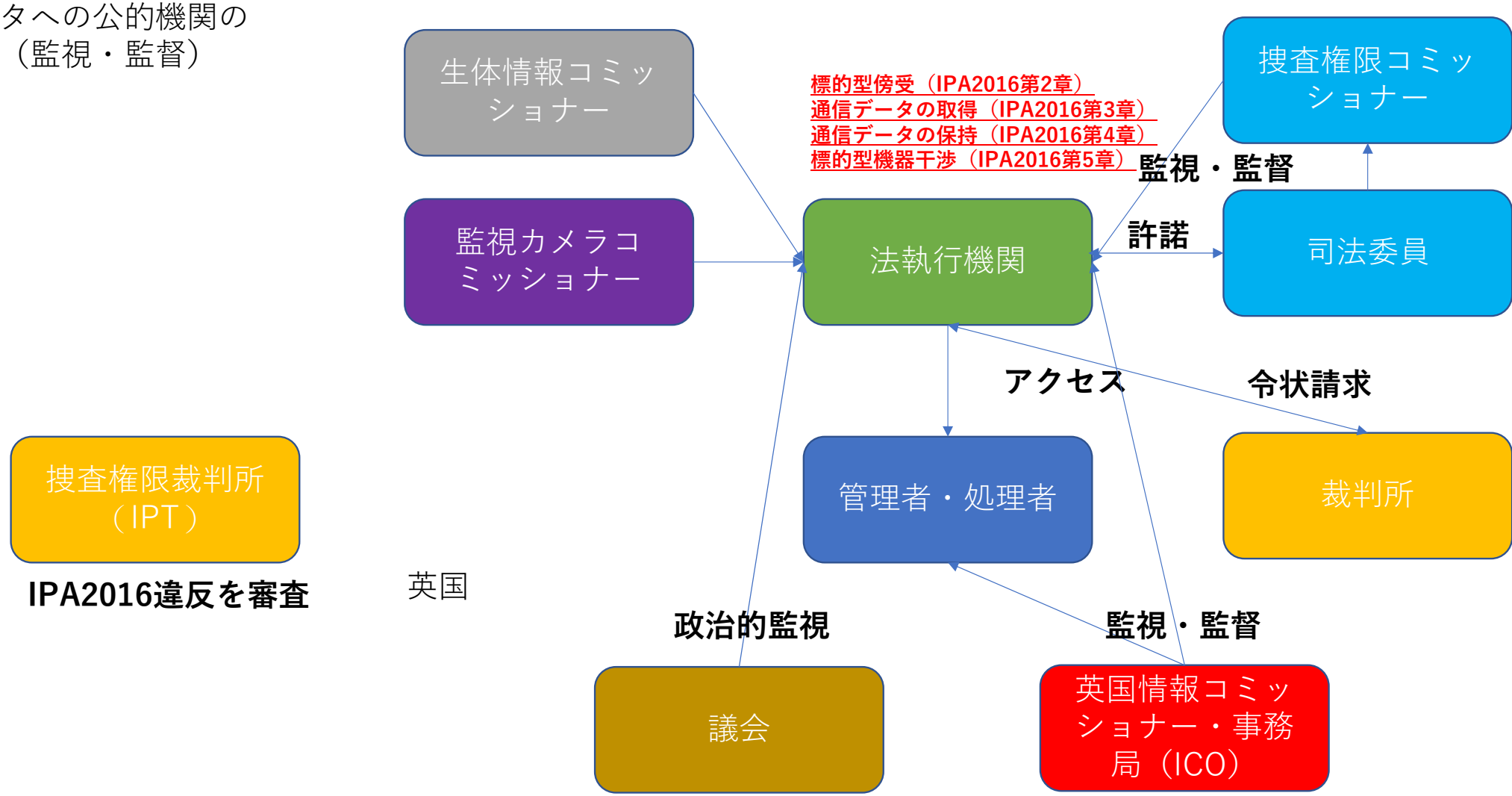
The Powers	Judicial Commissioner Approval Required	Details
Bulk Communications Data	Yes	Judicial Commissioner approval is required in all cases.
Targeted Communications Data	No*	Judicial Commissioner approval **only** required to identify or confirm journalistic sources. Applications for law enforcement are approved by the Office for Communications Data Authorisations.
Bulk Equipment Interference	Yes	Judicial Commissioner approval is required in all cases.
Targeted Equipment Interference	Yes	Judicial Commissioner approval is required, except in **urgent** cases.
Bulk Interception	Yes	Judicial Commissioner approval is required in all cases.
Targeted Interception	Yes	Judicial Commissioner approval is required, except in **urgent** cases.
Bulk Personal Datasets	Yes	Judicial Commissioner approval is required in all cases.
Covert Human Intelligence Sources	No*	Judicial Commissioner approval is required to deploy an undercover officer for more than 12 months only. Approval must be given in advance.
Intrusive Surveillance	Yes	Judicial Commissioner approval is required, except in **urgent** cases.
Property Interference	No*	Judicial Commissioner approval is required for law enforcement to use this power in intrusive settings only (e.g. a private residence or office). Judicial Commissioner approval is required if the applicant seeks to acquire confidential material. Judicial Commissioner approval is not required in **urgent** cases.

Although approval is not generally required, there are exceptions to this as explained in the "Details" column.

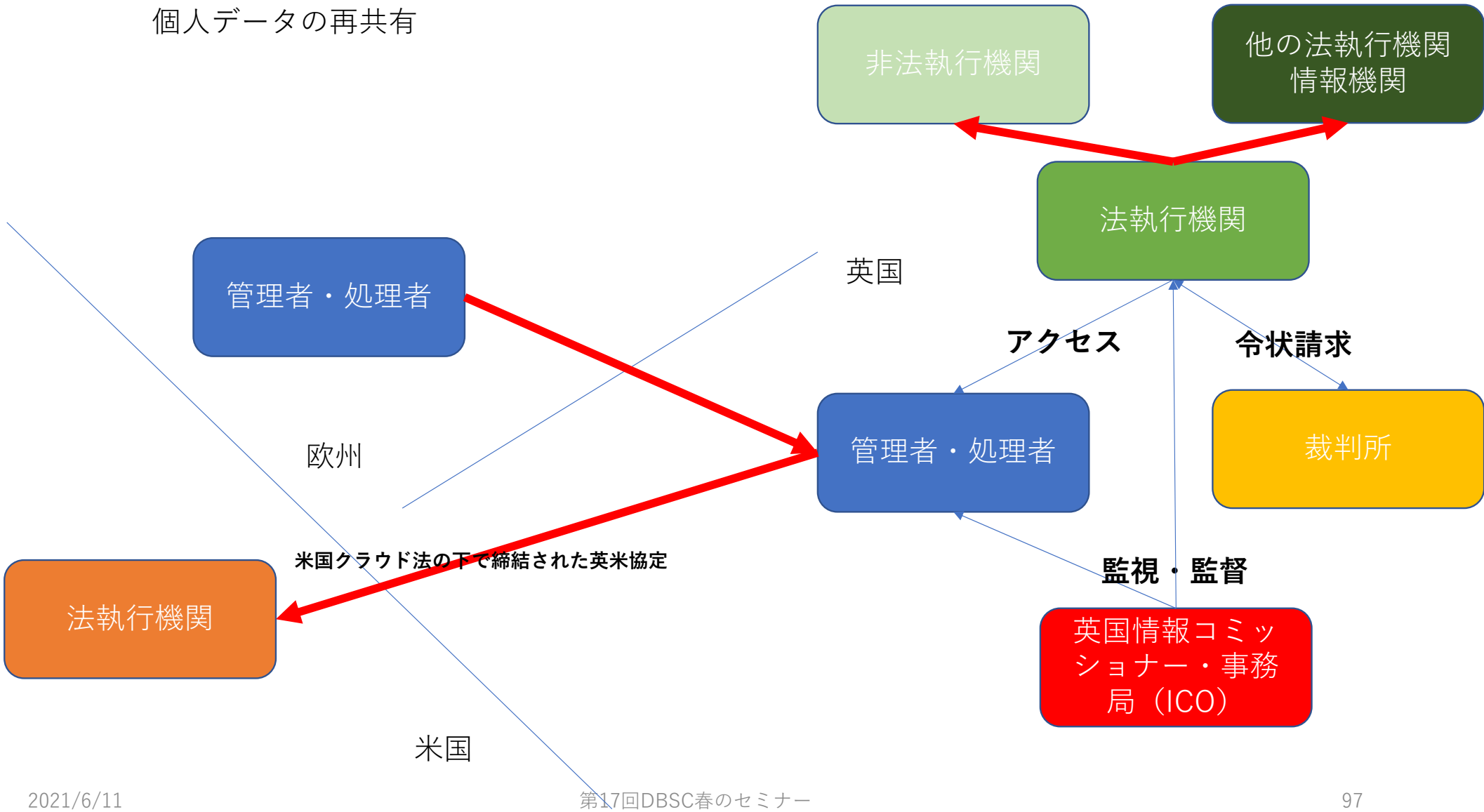
個人データへの公的機関のアクセス（傍受令状等）



個人データへの公的機関の
アクセス（監視・監督）



個人データの再共有


非法執行機関
他の法執行機関
情報機関
法執行機関
英国
管理者・処理者
アクセス
令状請求
管理者・処理者
裁判所
欧州
米国クラウド法の下で締結された英米協定
監視・監督
法執行機関
英国情報コミッショナー・事務局（ICO）
米国

ARTICLE 29 DATA PROTECTION WORKING PARTY

538/14/EN
WP 212

Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents

Adopted on 27 February 2014

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

2. Scope of an Organization's Personal Data Protection and Privacy Rules

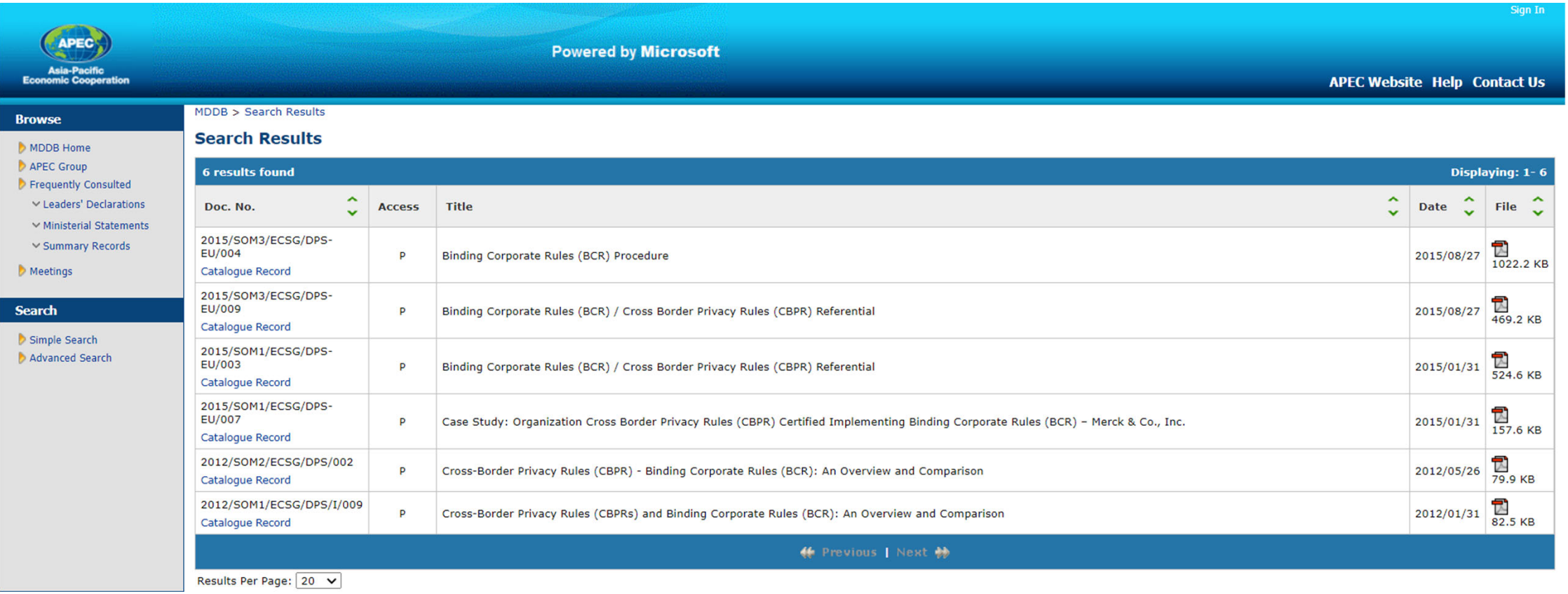
Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules should include a description of its scope of application including:

- The geographical scope (see sections 4 and 15 of this referential) [10];
- The material scope (i.e. nature of data, customers/prospective customers, employees/prospective employees, suppliers…) [11];
- The list of the entities bound by the organization's personal data protection and privacy rules [12]; and
- The purposes of the transfer and/or processing [13].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
The processing of personal data that is publicly available is subject to the requirements of EU data protection law and is not exempted from the BCR. Organizations that choose to participate in the BCR System shall implement privacy policies and practices consistently with the BCR program requirements for all personal data that is transferred within the Group outside of the European Union. While not required for BCR approval, participating organizations may apply the same privacy policies and procedures to all personal data that are processed within the Group globally, provided that compliance with EU data protection law is ensured where personal data is processed in the EU.	N/A
Clarification of the Scope of BCR N/A	**Clarification of the Scope of CBPR** In some instances, the organization's personal data protection and privacy rules may not apply to publicly available information [14]. Organizations that choose to participate in the CBPR System should implement privacy policies and practices consistently with the CBPR program requirements for all personal information that they have collected or received that is subject to cross-border transfer to other participating APEC

BCRとCBPRの基準の対照表（両方取得している例はある）



EDPB Plenary - adopted documents

28 May 2021 **EDPB**

During its May plenary, the EDPB adopted the following documents:

- Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe
- Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE)
- Statement on the Data Governance Act in light of legislative developments
- Recommendations on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions
- Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the LT SA (Article 28(8) GDPR)
- Response to Mr. de Serpa Soares, Under-Secretary-General for Legal Affairs and UN Legal Counsel
- Response to Access Now on the process to identify a controller's main establishment under the GDPR
- Letter to the European Commission on the protection of personal data in the AML-CFT legislative proposals

Latest news

Luxembourg's supervisory authority CNPD has published 18 decisions on the outcome of investigations

9 June 2021 **Luxembourg**

Dutch DPA: CP&A receives fine for violating privacy of sick employees

9 June 2021 **EDPB**

EDPB Annual Report 2020: Ensuring data protection rights in a changing world

2 June 2021 **EDPB**

EDPB Plenary - adopted documents

28 May 2021 **EDPB**

Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe

Adopted on 19 May 2021

Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE)

Adopted on 19 May 2021

まとめ

- ①CBPRが一定の保護レベルを示す認証であることは間違いなく，これを推進していくこと自体は正しい。企業の取引コストも下がる。
- ②APEC域内で，日本においてCBPR認証を得ている企業への移転がスムースになるように積極的に働きかけていくことも正しい（DFFTにも資する）。
- ③他方で，APEC域内を超えてDFFTの前面に出していくには欧州に嫌われすぎている。BCRとの相互運用についても数年間動きがない。EDPBの「追加的措置」勧告や行動規範の認定の動向の調査が欠かせない。
- ④CBPRに「追加的措置」に相当するものを加えたうえで，欧州のどこかの国の行動規範との相互互換が得られる，というあたりが最大成果ではないか？