情報の自由な流通とデータプライバシー

ヤフー株式会社　コーポレート統括本部
政策企画本部
望月　健太

本日のアジェンダ

1．データローカライゼーション

－実情と問題点
－国際的な規制：TPPの電子商取引章を例に
－国際的な動向：国際会合等を例に

2．データプライバシー

－EUのGDPRにおける個人データの第三国移転
（正当化事由に関する実務的視点）
－他の国際枠組みとの連携：APEC/CBPR

１．データローカライゼーション

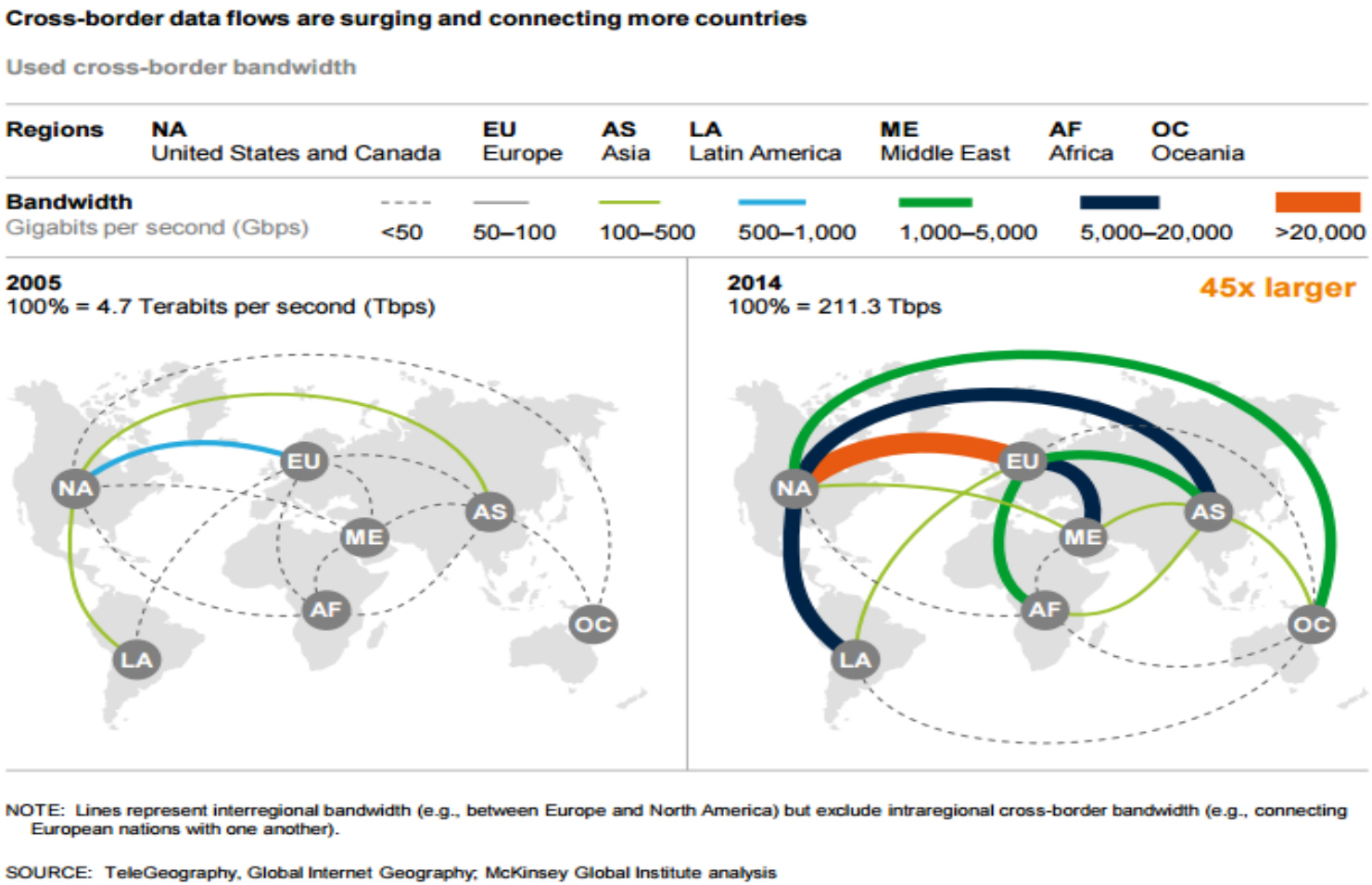
世界のデータ流通の現状

- 世界のデータ流通は格段に増加
- その流通成長率は２００５年比４５倍と、貿易や金融を凌駕

出展: MCKINSEY GLOBAL INSTITUTE, “DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS” (MARCH 2016)

世界のデータ流通の現状

- 越境データ流通量は、米国・EU間が最大



出展：MCKINSEY GLOBAL INSTITUTE, “DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS” (MARCH 2016)

世界のデータ流通の現状

- IoT/ビッグデータの時代においては、情報の自由な流通がイノベーションや経済成長のキー・イネイブラーとなる。したがって、グローバルでオープンであるというインターネットの本質的価値に基づく情報の自由な流通を維持することは非常に重要。

- 他方、情報の自由な流通によって、プライバシーリスクやサイバー脅威が広がっていることも事実（最悪の場合、サイバー空間を越えて物理的なインパクトをもたらす）。これらに対しては、情報の自由な流通を維持しつつ、マルチステークホルダー・アプローチに基づいた適切なプライバシーの保護やサイバーセキュリティに関する措置を実施する必要がある。

しかし・・・

国家によるインターネットの管理を強化する動き。その一つがデータローカライゼーション。

データローカライゼーション

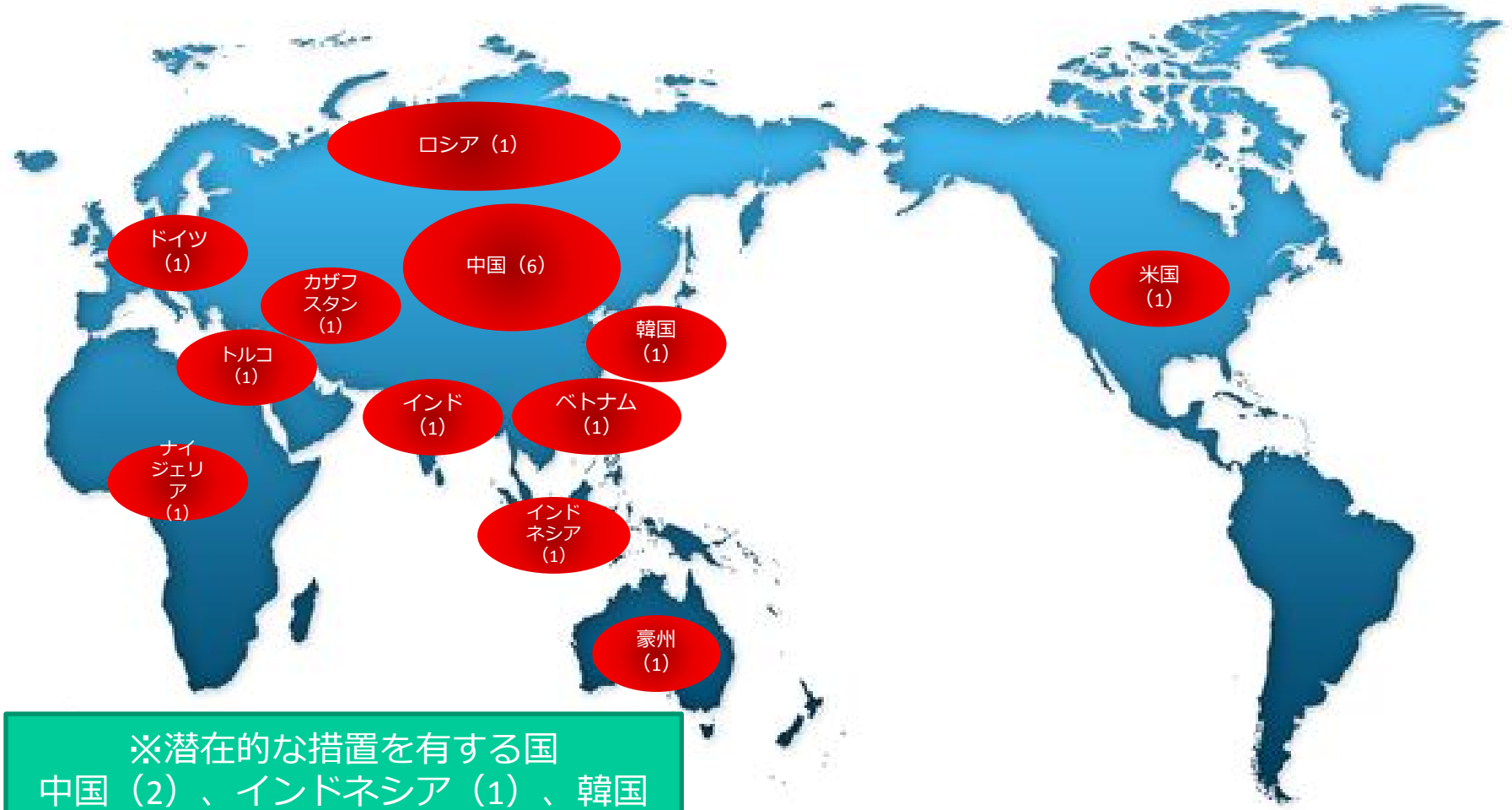
- データローカライゼーションとは、一般的に、 企業等が自国の領域内で事業を行うための条件として、その領域内において コンピュータ関連設備を利用又は設置し、 そこでデータを管理・処理するよう要求すること。

- 新興国がデータローカライゼーションを求める理由としては、自国でプライバシーやセキュリティーを守るため、自国産業を保護し経済成長を促進するためと言われている。

- 他方、国外の企業からすれば、適切なプライバシー保護法制がなく、サイバーセキュリティーが整備されていない国からそのような要求を受けた場合、追加的なコストの可能性を含む過度なビジネス・リスクを抱えたまま、その国に進出せざるを得なくなる（最悪の場合、進出そのものを断念）。

データローカライゼーションの実情

＜データローカライゼーション措置を実施している国＞　※括弧内は法律や規則等の数



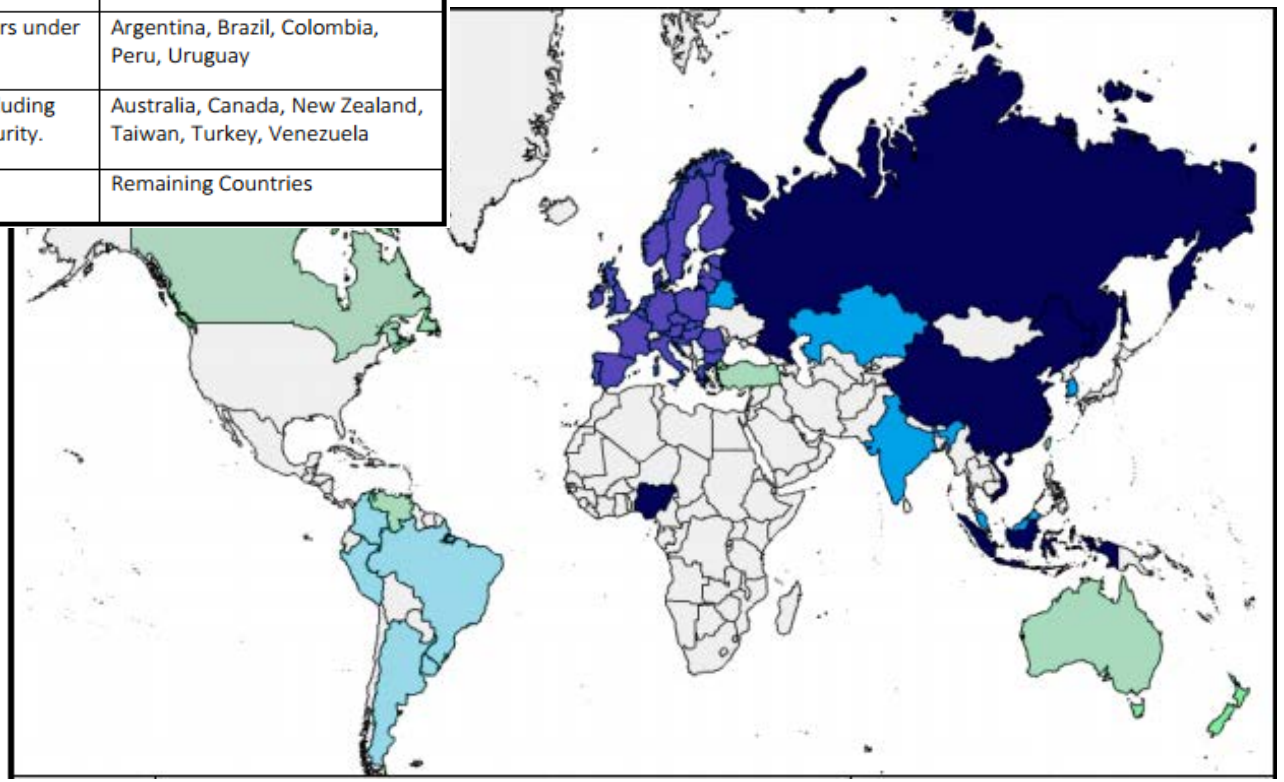
※潜在的な措置を有する国
中国（2）、インドネシア（1）、韓国（1）、サウジアラビア（1）、ベトナム（1）。

※米国情報技術産業協議会（ITI）調べ（2016年9月）

データローカライゼーションの実情

COLOR	STRENGH OF MEASURES	COUNTRIES
	Strong: Explicit requirements that data must be stored on servers within the country.	Brunei, China, Indonesia, Nigeria, Russia, Vietnam
	De Facto: Laws that create such large barriers to the transfer of data across borders that they effectively act as data localization requirements.	European Union
	Partial: Wide range of measures, including regulations applying only to certain domain names and regulations requiring the consent of an individual before data about them is transferred internationally.	Belarus, India, Kazakhstan, Malaysia, South Korea
	Mild: Restrictions on international data transfers under certain conditions.	Argentina, Brazil, Colombia, Peru, Uruguay
	Sector-specific: Tailored to specific sectors, including healthcare, telecom, finance, and national security.	Australia, Canada, New Zealand, Taiwan, Turkey, Venezuela
	None: No known data localization laws.	Remaining Countries

■ 措置の程度によって色分け。
ブルネイ、中国、インドネシア、ナイジェリア、ロシア、ベトナムが最も強いとの事（2015年9月現在）。



※出展：ALBRIGHT STONEBRIDGE GROUP, “DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION” (September 2015)

データローカライゼーションの問題点

- 本来、世界中の誰もが自由に接続ができ、意見や情報を発信できるグローバルで共通な環境がインターネットであり、情報の自由な流通こそがインターネットの本質的価値。

  ⇔データローカライゼーションはローカルな措置であり、グローバルな情報の流通を阻害する；インターネットの本質的価値を損ね、断片化を引き起こす。

- 大規模な個人データの漏洩事案やサイバーセキュリティの脆弱性を前に、世界中の人々の懸念が高まっており、データの物理的管理のためのデータローカライゼーションを主張する傾向がある。

  ⇔国外の企業からすれば、適切な個人情報保護制度がなく、サイバーセキュリティーが整備されていない国からそのような要求を受けた場合、追加的なコストや事業の非効率性を含む過度なビジネス・リスクを抱えたまま、その国に進出せざるを得なくなる（最悪の場合、進出そのものを断念）。

- 自国産業の保護を理由に、データローカライゼーションを主張する傾向がある。

  ⇔自国産業の保護という短期的な経済成長を目的として、自国領域内のコンピューター関連設備の利用や設置を国外の企業に対し要求することによって、長期的には外国投資の減少を引き起こしうる。

国際的な規制：TPPの電子商取引章を例に

- データローカライゼーションの国際的な規制の例としては、日モンゴル経済連携協定（2015年2月署名）、そして環太平洋パートナーシップ（ＴＰＰ）協定（2016年2月署名）が挙げられる。

（参考）日モンゴル経済連携協定第9.10条（第9章　電子商取引）

1. Neither Party shall require: (a) a service supplier of the other Party; (b) an investor of the other Party; or (c) an investment of an investor of the other Party in the Area of the former Party, **as a condition for conducting its business in the Area of the former Party, to use or locate computing facilities in that Area.**
2. Notwithstanding paragraph 1, nothing in this Article shall be construed to prevent a Party from adopting or maintaining measures affecting the use or location of computing facilities **necessary to achieve a legitimate public policy objective**, provided that **such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade**.

国際的な規制：TPPの電子商取引章を例に

- 環太平洋パートナーシップ（ＴＰＰ）協定第14.13条（第14章　電子商取引）

1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
2. **No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory**.
   ⇒データローカライゼーションの禁止規定。
1. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 **to achieve a legitimate public policy objective**, provided that the measure: (a) **is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade**; and (b) **does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective**.
   ⇒例外規定。①「正当な公共政策目的を達成」、②「恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと」、③「目的の達成のために必要である以上にコンピュータ関連設備の利用又は設置に制限を課するものではないこと」が鍵。

国際的な規制：TPPの電子商取引章を例に

- 環太平洋パートナーシップ（ＴＰＰ）協定第14.1条

「コンピュータ関連設備（computing facilities）」の定義

computing facilities means computer servers and storage devices for processing or storing information for commercial use.

⇒商業上の利用のために情報を処理し、又は保存するためのコンピュータ・サーバー及び記憶装置をいう。

- なお、第14.1条の「対象者」の定義において、「金融機関又は国境を越えて金融サービスを提供する締約国のサービス提供者」は電子商取引章の「対象者」に含まれないとしているため、こうした事業者によるデータローカライゼーションは、「公共政策目的例外」を満たすまでもなく許容されることになる。

国際的な規制：TPPの電子商取引章を例に

■ 論点

（１）例外規定にある「正当な公共政策目的」とは何か？

⇒世界貿易機関（WTO）・サービスの貿易に関する一般協定（GATS）にはデータローカライゼーションに関する規定はなく、また一般的例外（第14条）にもこうした「公共政策目的」例外はない。**どのような「公共政策目的」が「正当」と判断されるのか、解釈の余地が大きい。**

（２）「目的の達成のために必要である以上にコンピュータ関連設備の利用又は設置に制限を課するものではないこと」はどのように解釈されるか？

⇒WTO貿易の技術的障害に関する協定（TBT協定）第2条2項の文言「このため、強制規格は、正当な目的が達成できないことによって生ずる危険性を考慮した上で、正当な目的の達成のために必要である以上に貿易制限的であってはならない」に類似。

●この点、WTO紛争解決手続で積み重ねられたTBT協定に関する過去の判例によれば、「正当な目的を達成するか」と「必要以上に貿易制限的か」の**2ステップ・テスト**が採用。後者についてはさらに、（通常の場合）①より制限的でない代替措置があるか、②当該代替措置は同程度に正当な目的を達成するか、③代替措置が合理的に利用可能か、の**3ステップ・テスト**にしたがって審査。

☆TPPのような例外規定についても、3ステップ・テストが採用？

国際的な規制：TPPの電子商取引章を例に

■ 論点

（３） 「恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと」はどのように解釈されるか？

⇒「サービスの貿易に関する一般協定（GATS）」の第14条の文言「ただし、それらの措置を、同様の条件の下にある国の間において恣意的若しくは不当な差別の手段となるような態様で又はサービスの貿易に対する偽装した制限となるような態様で適用しないことを条件とする」に類似（一般的に「**柱書**」と呼ばれる）。

●米国－国境を越えた賭博サービスの及ぼす影響に係る措置（DS285）において、パネル（第一審）は、類似の文言が規定されている「関税及び貿易に関する一般協定（GATT）」第20条柱書に関し蓄積された判例に基づく解釈原則がGATS第14条の柱書の解釈に用いることができると判断。その上で、特定の措置の適用が「恣意的若しくは不当な差別」となるかについては、措置の**一貫性の欠如（the absence of consistency）**が指針となるとした（上級委員会（第二審）もこの「一貫性基準」を支持）。

☆TPPのような例外規定（柱書）について、こうした解釈原則に基づいて判断？。

国際的な動向の最新例（１）：APEC TEL 54

- **APEC第54回電気通信・情報作業部会（APEC TEL 54）：[LSG] Industry / Regulatory Roundtable on Free Flow of Data**

（１）日時：2016年11月1日　9:30～12:30

（２）場所：京都府・関西文化学術研究都市（けいはんな学研都市）

（３）登壇者：

①Industry Session: AT&TのJake Jennings氏がモデレーター、パネリストはNational Center for APEC（米国）、Rebright Partners（シンガポール），SONYおよびYahoo! JAPAN（日本）

②Regulatory Session: 野村総研の横澤誠氏がモデレーター、パネリストは経団連、経産省、AT&T（米国）、総務省

（４）成果文書（勧告部分）

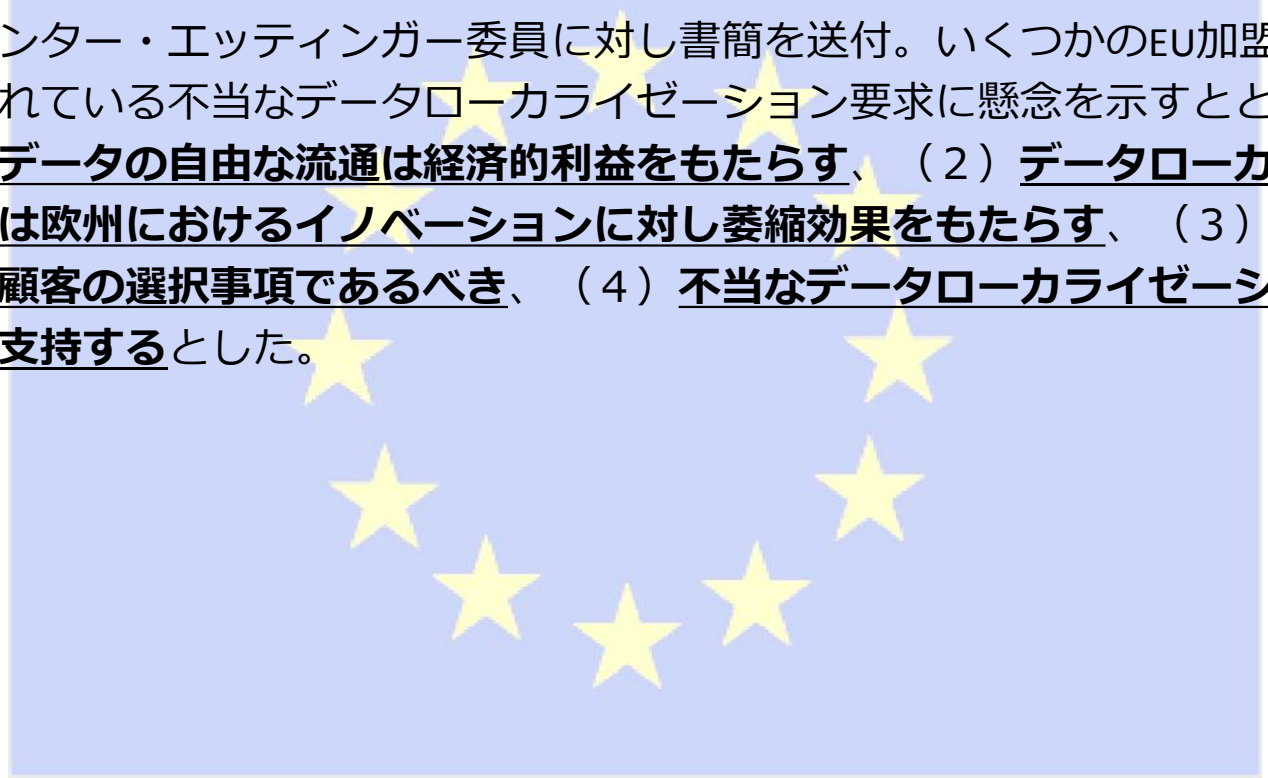
①**情報の自由な流通は、APEC地域のみならず地球規模の包摂的な経済成長において必要不可欠である**

②**知的財産の保護、データおよびプライバシーの保護、そしてサイバーセキュリティーに関する適用可能な枠組みを尊重しつつ、「国際的に受け入れられるような機能するルール（globally accepted operational rules）」を定める政策的・規制的進展が望まれる**

国際的な動向の最新例（２）：欧州の動向

■ 欧州委員会に対する書簡

⇒2016年11月15日、欧州産業界（日本企業のグループを含む）は、欧州委員会・デジタル単一市場担当のアンドルス・アンシプ副委員長および同デジタル経済・社会担当のギュンター・エッティンガー委員に対し書簡を送付。いくつかのEU加盟国において実施されている不当なデータローカライゼーション要求に懸念を示すとともに、（１）**データの自由な流通は経済的利益をもたらす**、（２）**データローカライゼーションは欧州におけるイノベーションに対し萎縮効果をもたらす**、（３）**データの保存先は顧客の選択事項であるべき**、（４）**不当なデータローカライゼーションの禁止を広く支持する**とした。



2．データプライバシー
－EU一般データ保護規則（GDPR）－

EUの個人情報保護制度

- **データ保護指令（Data Protection Directive（95/46/EC））**

  ⇒1995年10月24日採択、1998年10月25日発効。EU法上、「指令（directive）」はEU加盟国に直接適用されないため、各EU加盟国がデータ保護指令に沿った国内法を個別に制定。

  ※データ保護指令の実施に関し各国法毎に差異が発生。法的安定性を損なっていた。

- **一般データ保護規則（General Data Protection Regulation（GDPR））**

  ⇒2016年4月27日採択、2年後の2018年5月25日から施行（より具体的には、GDPR第99条に従い、発効日は2016年5月24日、適用開始日が2018年5月25日）。GDPRは全てのEU加盟国に直接適用される。

  ※「規則（regulation）」は加盟国の法律を統一するために制定されるもので直接適用されるため、原則、GDPRに規定された規範は全てのEU加盟国において直接かつ一律に適用される（もっとも、GDPRの下で各EU加盟国に一定程度の立法裁量が付与）。

☆2018年5月24日まではデータ保護指令が適用、同25日からGDPR適用開始。

EU一般データ保護規則（GDPR）

■ データ保護指令からの変更点

⇒EU加盟国間で一貫した高いレベルの保護を確保し、各国国内法の差異によって生じていた個人データの流通の妨げとなるものを取り除くため、データ保護指令からGDPRに移行。

【主な改正ポイント】

（１）適用範囲の拡大：GDPRの域外適用の可能性
（２）データ管理者のみならず、データ処理者にも直接的な法的義務を課すことに
（３）データ主体の権利が拡大・強化
（４）それに伴い、データ管理者およびデータ処理者に対するGDPR適用も厳格化
（５）遵守確保の強化：個人データ漏えい時の通報義務や、執行および制裁に関する新たな規定等が追加

☆日本企業の観点からは、①適用範囲の拡大に伴う域外適用の可能性、②執行および制裁の強化、そして③個人データのEU域外への移転に関する選択肢、の3つがとりわけ重要！

EU一般データ保護規則（GDPR）

■ 概観（※一部のポイントのみ抜粋）

項　目	具体的なポイント
1. 個人情報の範囲	認定基準が低く、個人を識別しうるものはほぼ全て個人データ。IPアドレス、クッキー、web閲覧履歴、RFIDタグ等も含む。ビッグデータも個人を識別できる場合には個人データと認定されうる。
2. 適用範囲の拡大	EU域内に「拠点（establishments）」を有する事業者のみならず、EU域内に拠点を有していない事業者であっても、その個人データの処理活動が①EUのデータ主体へのサービス提供・物品販売に関連する場合、又は②データ主体のEU域内における行動の監視に関連する場合には適用対象。
3. データ処理者の義務	データ管理者のために個人データを処理する者も直接の適用対象となり、データ管理義務、適切な保安基準の実施、保護影響評価の定期的な実施、データ保護担当者の指名等の義務を有する。
4. 同意の厳格化	指令下の「自由意思（freely given）」「特定性（specific）」「十分な理解（informed）」の3要件に、「明確性（unambiguous）」「外形性（statement/clear affirmative action）」の2要件が追加。包括的同意は十分であるとはみなされず、同意はデータ主体によっていつでも撤回可能。
5. データ主体の権利拡大・強化	指令下の「最低限の情報を受取る権利」「アクセス権」「拒否権」「修正権」に加え、「忘れられる権利」「データポータビリティ権」等が追加。
6. データ保護担当者の指名	データ管理者/処理者は、その主たる活動が大規模な定期的かつ体系的なデータ主体の監視である場合や特殊な個人データの大規模な処理からなる場合にデータ保護担当者を指名する義務がある。多国籍企業グループの場合は同一人物でも良く、EU域外のデータ管理者/処理者の場合、EU域内の代表者（representative）を書面で任命する必要。
7. データ漏えい時の通報義務	個人データの漏えい時、データ管理者の場合は遅滞なく72時間以内に、データ処理者の場合は遅滞なく通報する義務があり、漏えいの性質やその影響、影響を軽減する対策等を通知する必要有。
8. ワンストップ・ショップ	EU域内に複数の拠点がある場合、主要なデータ処理活動を実施している「主たる拠点」が存在するEU加盟国の監視当局（主たる当局（lead authority））とやりとりすれば良い（窓口の一本化）。
9. 違反に対する救済	GDPRに違反して個人データが処理された場合、そのデータ主体は、監視当局やデータ管理者/処理者に対する効果的な司法的救済の権利を有し、権利侵害に係る損害賠償請求権を有する。
10. 違反に対する制裁	違反の類型に応じて、①2,000万ユーロ又は前会計年度の年間売上高の4%のいずれか高い金額、又は②1,000万ユーロ又は前会計年度の年間売上高の2%のいずれか高い金額、を上限として課徴金有。

EU一般データ保護規則（GDPR）

■ 適用範囲の拡大：域外適用の可能性（GDPR第3条）

（１）第3条1項：拠点（establishment）がある場合

1. This Regulation applies to the processing of personal data in the context of the activities of an **establishment** of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

⇒この規定はデータ保護指令にもあったが、GDPRでは「処理者」が追加されている。

※拠点（**establishment**）については、データ保護指令前文(19)、そしてGDPR前文(22)において「確固たる取り決め（stable arrangements）を通じて実効的かつ実質的な活動を行っていること」を意味するとされている。

（参考１）データ保護指令に関する第29条作業部会の意見

（Opinion 8/2010 on applicable law (WP179), 16/12/2010)

・EU機能条約第50条（開業の自由）に関する欧州司法裁判所（ECJ）の解釈「確固たる拠点（a stable establishment）には、恒常的に利用可能な特定のサービス提供にとって必要な人的・技術的資源が求められる」を引用し、前文(19)がそれを反映しているとした。その上で、前文(19)の要件を満たせば、法律事務所や1人の事務所であっても「拠点」に該当しうる一方、サーバーやコンピュータのみではおそらく「拠点」にあたらないと例示。

・処理が拠点の活動に「関連して（in the context of）」いれば良い点も注意（適用法の問題）。

EU一般データ保護規則（GDPR）

■ 適用範囲の拡大：域外適用の可能性（GDPR第3条）

（１）第3条1項：拠点（establishment）がある場合

（参考２）欧州司法裁判所判決（C-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014 (“GOOGLE”)）

・本件において、Google Spainはデータの処理を行っておらず（米国のGoogle Inc.が排他的に実施）、スペイン国内のおける広告業務（advertising）を行っていたのみであった。

・これに関し、欧州司法裁判所は、データ保護指令第4条1項（a）は、当該データの処理が拠点（establishment）に「よって（by）」実施されることを求めておらず、拠点の「活動に関連して（in the context of the activities）」いれば良いとしていると指摘。

・その上で、広告スペースに関する活動は、検索エンジンが経済的な利益を上げる手段となり、そのエンジンはそれらの活動が行われることを可能とする手段であることから、検索エンジンの活動とEU加盟国に所在する拠点の活動は密接不可分に関連していると判断。

☆結果として、Google Spainはデータ保護指令第4条1項（a）の拠点に該当すると判断。

EU一般データ保護規則（GDPR）

■ 適用範囲の拡大：域外適用の可能性（GDPR第3条）

（２）第3条2項：拠点（establishment）がない場合

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

   a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

   b. the monitoring of their behaviour as far as their behaviour takes place within the Union.

⇒GDPRから**新たに追加**された規定。これにより、（a）又は（b）に関連してEU域内に所在する主体の個人データの処理活動がなされた場合、**EU域内と何ら物理的紐帯（＝拠点（establishment））がなくとも**GDPRが適用されうる。

（参考）GDPR前文（23） および（24）

・上記（a）項に関し前文（23）は、物品やサービスの注文を可能とするような形で、1又はそれ以上のEU加盟国で使用されている言語や通貨を使用していることや、EU域内の顧客やユーザーに言及していれば、「EU域内のデータ主体に物品やサービスを提供することを想定している」とみなしうるとしている。

・上記(b)に関し前文（24）は、例として、（行動分析等を目的とし）自然人のプロファイリングのためにインターネット上でトラッキングを行う場合、この規定に該当しうるとしている。

EU一般データ保護規則（GDPR）

■ 執行および制裁の強化（GDPR第58条、第83条）

（１）データ保護当局による執行権限の強化（第58条）

⇒データ保護指令（第28条）の下では、各国国内法の下、最低限の権限しかデータ保護当局に付与されていなかった。

☆GDPRの下では、第83条に従い、以下のような非常に広範な権限が監視当局（旧称データ保護当局）に付与。

（1項）**捜査権限**（データ保護監査、違反の通知、情報収集、現地捜査等）

（2項）**是正権限**（警告・懲戒・命令の発出、処理制限、課徴金の賦課等）

（3項）**認可・監督権限**（各種意見表明、認証関連の権限、契約条項（SCC）・行政協定・拘束的企業準則（BCR）の認可等）

（その他）司法機関との連携、法的手続への付託等。各EU加盟国は、法律によって監視当局に対し追加の権限を付与することができる。

EU一般データ保護規則（GDPR）

■ 執行および制裁の強化（GDPR第58条、第83条）

（２）制裁の強化（第83条）

⇒データ保護指令（第24条）の下では、具体的な規定がなく、各国国内法によって制裁内容にばらつきがあった。

☆GDPRでは、第83条に従い、違反の類型に応じて以下のような2種類の課徴金の上限が設けられた。

（4項） **1,000万ユーロ又は前会計年度の年間売上高の2%**のいずれか高い金額。

●具体的な違反類型：データ管理者/処理者に課せられた各種義務の違反、認証機関の義務違反、行動規範に関する監視機関の義務違反。

（5項）**2,000万ユーロ又は前会計年度の年間売上高の4%**のいずれか高い金額。

●具体的な違反類型：「同意」の条件を含むデータ処理に関する基本原則の違反、データ主体が有する権利の侵害、第三国又は国際機関への個人データの移転に係る違反、第9章の下採択される各国国内法によって定められる義務の違反、データ処理に関する命令等や監視当局の指示の不遵守、監視当局の捜査権限の妨害等。

☆課徴金の賦課については**監視当局に一定程度の裁量権有**。判断基準は2項に列挙。課徴金の賦課は「効果的かつ均衡性のとれたもので、違反を思いとどまらせるもの（effective, proportionate and dissuasive）」でなければならない。⇔Q.「均衡性」がキャップ？懲罰的な課徴金は禁止？

EU一般データ保護規則（GDPR）

■ 個人データの域外移転

（１）**二段階テスト**：GDPRでも変更なし（GDPR前文（101））

1. （第一段階：EU域内）データ処理に関するGDPR上の一般的な要件を満たすこと。また、データ処理者が関わる場合にはその要件を満たすこと（第28条）。
2. （第二段階：EU域外）EU域外の第三国（又は国際機関）への移転に必要となる要件を満たすこと（第45条+α.）。

（２）**十分性認定**（第45条1項）

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
   ⇒欧州委員会が（個人データの域外移転に関し）十分な保護のレベルを有するとみなした国（又は国際機関）以外への個人データの域外移転を原則禁止（十分性認定）。
   ⇔逆に、EUの十分性認定を受けた国への個人データの越境移転は可能。

【十分性認定を受けている国】

アルゼンチン、アンドラ、イスラエル、ウルグアイ、カナダ、ガーンジー島（英国）、ジャージー島（英国）、スイス、ニュージーランド、フェロー諸島（デンマーク）、マン島（英国）

EU一般データ保護規則（GDPR）

■ 個人データの域外移転

（２）**十分性認定**（第45条）：その他のポイント

・十分性認定を行う際の判断基準は、第45条2項（a）～（c）に規定。データ保護指令（第25条2項）から**大幅に詳細化**。

・GDPRの下、今後実施規則が定められる予定（3項）。その中には、**少なくとも4年毎の定期レビューに関するメカニズム**が規定される予定。

⇔データ保護指令にはそのような規定無。もっとも、各国の十分性認定本文に、定期レビューではなくモニタリングに関する規定はあった。

・データ保護指令に基づく十分性認定は、今後の欧州委員会決定によって修正、差し替え又は廃止されるまで有効（9項）。

※他方、GDPRに規定された十分性認定の要件の方が幅広く詳細なため，今後GDPR適用開始後に新たに十分性認定を受ける国が出てくるかや、現在十分性認定を受けている国がそのステータスを維持できるかは不明。

（参考）なお、2000年に締結され、2015年10月6日の欧州司法裁判所（ECJ）判決で無効と判断された「EU-USセーフハーバー協定」に置き換わるものである「EU-USプライバシー・シールド」も、十分性認定を受けたもの。2016年7月12日に欧州委員会がその十分性認定を採択。なお、この十分性認定も現行のデータ保護指令に基づくもの。

EU一般データ保護規則（GDPR）

■ 個人データの域外移転：十分性認定を受けていない国への移転は？

（１）適切な保護措置（第46条）：以下のものがあれば、十分性認定を受けていない国（又は国際機関）への個人データの域外移転が可能。

（a）公の当局又は団体間の法的拘束力かつ執行力のある文書

（b）**拘束的企業準則（BCR）** ☆GDPRから明記

（c）**標準契約条項（SCC）**

（d）**行動規範（Code of Conduct）** ☆GDPRから新たに追加

（e）**認証（Certification）** ☆GDPRから新たに追加

※なお、データ保護指令第26条2項に基づくEU加盟国又は監視当局の認可（authorizations）、そして同4項に基づく欧州委員会の決定（decisions）は、監視当局によって修正、差し替え又は廃止されるまで有効。

したがって、データ保護指令の下承認を得た拘束的企業準則（BCR）や標準的契約条項（SCC）はGDPR適用後も原則有効。もっとも、GDPRによって規制が強化されたため、今後レビューや更新の可能性有（データ保護指令に従ってセットしたからといって安泰ではない！）。

EU一般データ保護規則（GDPR）

■ 個人データの域外移転：十分性認定を受けていない国への移転は？

（２）**拘束的企業準則（BCR）**（第47条）

⇒同一企業グループ内での個人データの移転に関する社内規則。主に多くの海外拠点を有する多国籍企業グループで使用されることが多い。

【メリット】

・多くの海外拠点を有する多国籍企業グループ内の個人データの移転については、これ一本を主たる当局（lead authority）に承認のため提出すれば良い（グループ会社への個人データの移転毎に個別に契約を結ばなくて済む）。

・データ保護指令の下ではBCR自体明記されていなかったが、GDPRからBCRとその承認要件が詳細に規定。

【デメリット】

・同一企業グループ外の第三者への移転の場合には適用されない。

・データ保護指令の下では、BCRの承認要件や解釈が各国によって異なる上、標準契約条項（SCC）のようにテンプレートがある訳でもないため、手続に時間と費用がかかる（※EU協力手続と相互承認（現在19か国））。

⇔GDPRではBCR承認要件が一律化され、「一貫性メカニズム（Consistency Mechanism）」の採用により大幅に改善される見込み。

EU一般データ保護規則（GDPR）

■ 個人データの域外移転：十分性認定を受けていない国への移転は？

（２）**拘束的企業準則（BCR）**（第47条）

（参考）一貫性メカニズム：関連する監視当局は、BCRが以下の要件を満たす場合、原則としてそのBCRを承認しなければならないとするもの。

（a）個人データをやりとりする全てのグループ内企業とその従業員を法的に拘束し、かつ執行力を有すること

（b）データ主体に明示的に執行権限を付与していること

（c）GDPRに規定された要件を満たしていること

【BCRに関する実務的視点】

①どこの国の監視当局を主たる当局（lead authority）に設定するか？

②GDPRの域外適用のケース（第3条2項）の場合、EU域内の代理人を書面で指定しなければならないが（第27条）、その場合の主たる当局（lead authority）は代理人所在地の監視当局となるのか（第56条）？（物品販売・サービス提供の態様と第27条・第56条間の解釈整合性の問題）

③どこの法律事務所に依頼するか？

④どのタイミングで申請するか（現時点でもGDPR対応のBCRを提出可）？

EU一般データ保護規則（GDPR）

■ 個人データの域外移転：十分性認定を受けていない国への移転は？

（３）**標準契約条項（SCC）**（第46条）

⇒個人データの域外移転時に使用される個別の契約（条項）。主に海外拠点が多くない企業や個人データの移転が限定的な場合に使用される。

【メリット】

・同一企業グループ外の第三者への移転の場合に使用（⇔BCR）。

・欧州委員会が承認した以下3種類の標準契約条項のテンプレート有：

（i）EU域内のデータ管理者からEU域外の同管理者への移転の場合に使用（2種類）

（ii）EU域内のデータ管理者からEU域外の同処理者への移転の場合に使用（1種類）

※第29条作業部会が処理者から処理者への案を出したが、欧州委員会未承認。

・必ずしもテンプレートを使う必要はなく、より範囲の広い契約に含めることも可。

【デメリット】

・個別具体的な契約を結ぶ必要があるため、拠点が多く個人データの移転も多様な事業者には適さない。

・テンプレートの規定内容を自由に改変できない（柔軟性の欠如）。

・データ保護指令の下では、国によってはデータ保護当局へのSCCの通知（提出）や承認を求めることがある。

⇔GDPRの下では、そうした国においても事前の承認は不要に。

EU一般データ保護規則（GDPR）

■ 個人データの域外移転：十分性認定を受けていない国への移転は？

（３）**標準契約条項（SCC）**（第46条）

【SCCに関する実務的視点】

・GDPRでは、実は2パターンのSCCが規定されている：

（i） 欧州委員会によって採択された標準データ保護条項（2項（c））

（ii）監視当局によって採択され、欧州委員会によって承認された標準データ保護条項（2項（d））

⇒（i）については、データ保護指令下で作成された3種類のテンプレートが今後GDPRの要件にしたがって更新されるのか？（ii）については、これがどのように運用されるのか？

・さらに、データ管理者又は処理者と、管理者又は処理者あるいはデータを受領する第三者（第三国/国際機関）との間の契約条項についても、監視当局の承認（authorization）があれば使用可能となっている（3項（a））。

⇒テンプレートを用いないSCCについて明記したのみ？

EU一般データ保護規則（GDPR）

■ 個人データの域外移転：十分性認定を受けていない国への移転は？

（４）**行動規範（Code of Conduct）**（第40条）

⇒業界団体等（associations and other bodies）がGDPRの遵守を目的とした行動規範を作成、監視当局に承認された場合、その業界団体等に所属している事業者が契約又はその他の法的拘束力ある文書で行動規範にコミットした場合、GDPRの要件を満たしているとみなされるもの。EU域外の事業者が承認された行動規範を遵守しているとみなされる場合、それがEU域外への適切なデータ移転の根拠となる（3項）。

（５）**認証（Certification）**（第42条）

⇒各国が認定した認証機関、監視当局、又は欧州データ保護会議（EDPB：第29条作業部会の後継）によって発行された認証を取得することができた事業者は、GDPRの要件を満たしているとみなされるもの。認証がEDPBによって承認された基準に基づいて発行される場合には、欧州データ保護シール（共通認証）とすることができる。認証の期限は3年、認証要件を引き続き満たしていれば更新可。認証についても、EU域外の事業者が取得した場合、それがEU域外への適切なデータ移転の根拠となる（2項）。

※いずれも更なる詳細については実施規則が定められる予定。

EU一般データ保護規則（GDPR）

■ 個人データの域外移転：十分性認定もその他の保護措置もない場合

（１）**逸脱条項**（第49条）：以下いずれかの条件を満たす限りにおいて域外移転可能。

（a）可能性のあるリスクを十分に理解した上で、データ主体が同意した場合

（b）データ主体・管理者間の契約の履行に必要な場合、又はデータ主体の求めに応じ、契約締結前に何らかの措置を実施する必要がある場合

（c）データ主体の利益のために、管理者と他の主体との間で契約を締結又は履行するために必要な場合

（d）公益上の重要な理由で必要な場合

（e）法的手続（establishment, exercise or defence of legal claims）に必要な場合

（f）データ主体が物理的・法的に同意することができない場合において、同人又は第三者の重要な利益を守るために必要な場合

（g）公的機関（register）がEUや各国法に従って情報公開等を行う際に移転がなされる場合

※上記逸脱条項は、データ保護指令から存在するが、あくまでも十分性認定やその他の保護措置がない場合に限って使用可能なものであり、非常に限定的な状況下でしか使用できない点に注意。

EU一般データ保護規則（GDPR）

■ 個人データの域外移転：十分性認定もその他の保護措置もない場合

（２）**逸脱条項**（第49条）：**同意**（1項（a））

⇒第4条（11）は、同意の定義について以下のように規定。

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

☆つまり、「自由意思（freely given）」、「特定性（specific）」、「十分な理解（informed）」の3要件に加え、「明確性（unambiguous）」と「外形性（a statement or a clear affirmative action」が必要。

※データ保護指令では、前者3要件のみであったため、GDPRから同意の要件が厳しくなった。

※第7条には、同意の条件について詳細に規定されている。

EU一般データ保護規則（GDPR）

■ 個人データの域外移転：十分性認定もその他の保護措置もない場合

（２）**逸脱条項**（第49条）：**同意**（1項（a））

【同意に関する実務的視点】

・かなり限定的に解釈されるため、例えば雇用関係（従業員データの移転等）において同意に依拠することはリスキー（特に雇用の条件として同意が求められる場合、自由意思に基づくものではないと判断される）。

・包括同意は無効。データ主体に対し十分な説明を行った上で、個別具体的に同意を取得する必要がある。

・適切な同意の立証責任は事業者側。そのため、同意に依拠する場合には、GDPRの5要件をしっかりと立証できるように準備する必要。

・同意はデータ主体によっていつでも撤回可能であり、その事実を事前にデータ主体に説明する必要があるとともに、同意の撤回は容易でなければならない（第7条3項）。

・データ保護指令からGDPRになることによって同意の要件が厳しくなっているため、これまで同意で処理していた場合は、レビューの必要性有。

☆同意の解釈については、データ保護指令に関する第29条作業部会の意見（Opinion 15/2011 on the definition of consent (WP187), 13/07/2011 ）も参考になる。

EU一般データ保護規則（GDPR）

■ 個人データの域外移転：十分性認定もその他の保護措置もない場合

（３）**逸脱条項**（第49条）：**契約の履行に必要な場合**（1項（b））

⇒the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request

☆ここでは、「necessary」という文言が限定的に解釈される。

【実務的視点】

・雇用契約に基づいて従業員データの域外移転を行うことは可能か？

A. データ保護指令に関する第29条作業部会の作業文書（Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995 (WP114), 25/11/2005）

・多国籍企業グループが人事関連業務の本社集約のために、従業員データを（EU域内の）子会社から（EU域外の）親会社に移転する場合、これを雇用契約の履行に「必要」な措置とみなすのは困難とのこと（雇用契約の範囲を超えているとの事）。

EU一般データ保護規則（GDPR）：日本企業の視点

- 事業者は、まず自らの事業活動と個人データの越境移転の態様を詳細に確認した上で、GDPRの適用対象となるかを確認する必要（そのためにも、積極的に国内外で情報収集とネットワーキングを行うべき）。

- 適用対象となる場合、日本はEUから十分性認定を受けた国ではないため、GDPRに基づく正当化事由（拘束的企業準則（BCR）、標準契約条項（SCC）。今後は行動規範（Code of Conduct）、認証（Certification）も選択肢に？）のどれを使うかを検討する必要。逸脱条項（同意や契約の履行に必要等）の利用は最後の手段とすべき。

- 実際に正当化事由を使う場合には、この分野に精通した法律事務所を使う必要。但し、どのような事業活動を行っているかは事業者自身が一番良く分かっている訳であり、丸投げしない。

- なお、英国に主要な拠点を有する事業者は、Brexit（英国のEU離脱）に関する最新動向もしっかりと把握しておく必要。

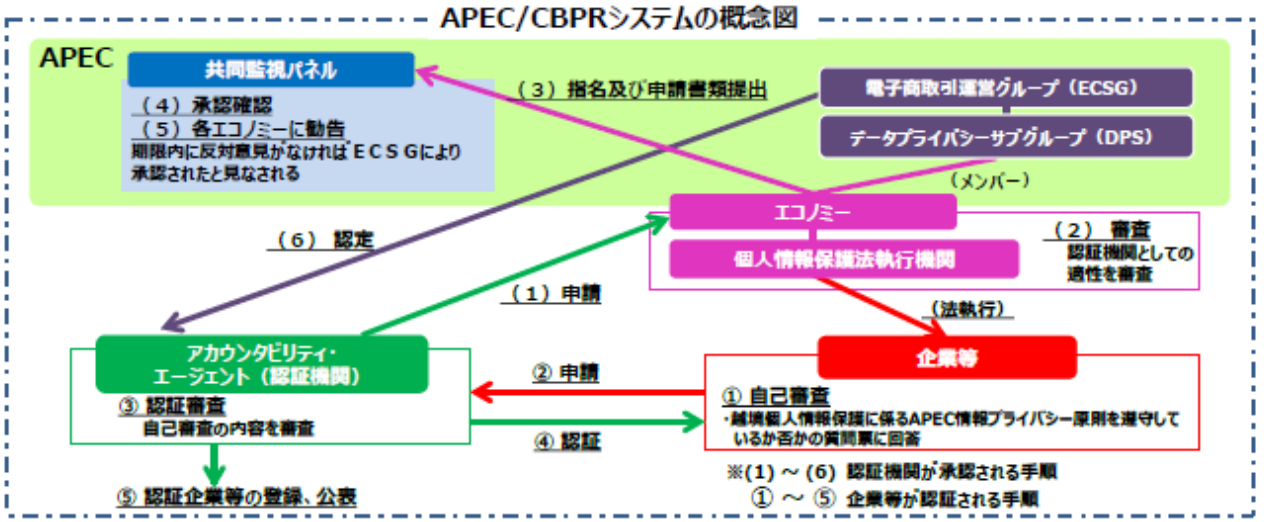
- フランスの動向についても注意が必要：GDPRの範囲を超えて、さらに貿易協定で規制を強めようとするフランス大臣の発言等。

EU一般データ保護規則（GDPR）：相互運用性の議論

- 現在、EUの拘束的企業準則（BCR）とAPECの越境プライバシールール（CBPR）システムとの相互運用性について議論が継続中。
- APEC/CBPRとは？

⇒企業等の越境個人情報保護に係る取組みに関し、APEC情報プライバシー原則への適合性を認証する制度。申請企業等は、自社の越境個人情報保護に関するルール、体制等に関して自己審査を行い、その内容についてあらかじめ認定された中立的な認証機関（アカウンタビリティ・エージェント:民間団体又は政府機関）から認証審査を受ける。2016年10月現在、米国、メキシコ、日本、カナダ（全てTPP署名国）がエコノミーとして参加。認証機関としては米国のTRUSTeと日本のJIPDECが認定を取得。

GDPRの適用以降は明示的に認証制度も始まるため、BCRとの相互運用性が進まないのであれば、認証制度とAPEC/CBPRとの相互運用性を目指すべきでは？



出展：経済産業省（2016年10月）

（参考）APEC/CBPRへの参加国拡大に向けて

- **APEC/CBPRの参加国拡大を求める各国産業界の共同文書**

  ⇒米国の情報技術産業協議会（ITI）、日本の電子情報技術産業協会（JEITA）、米国商工会議所（U.S. Chamber of Commerce）、米国国際ビジネス評議会（USCIB）の連名で、APEC/CBPR参加国の拡大を求める共同文書が展開中。その中では、全てのAPEC加盟国に対し、2017年にベトナムで開催される次回貿易担当大臣会合までにCBPRシステムに参加することをコミットするよう求めている。

  ※今後、経団連と情報サービス産業協会も共同文書に参加する予定。

参考資料（順不同）

- 藤井康次郎・河合優子（西村あさひ法律事務所）「Web解説TPP協定「14 電子商取引」」（経済産業研究所（RIETI），2016）
- 経済産業省『2016年版不公正貿易報告書』（2016）
- 庄司克宏『新EU法　基礎篇』（岩波書店，2013）
- セミナー資料「欧州とドイツにおけるデータの取扱い－新EUデータ保護規制への対応」（ARQUIS Foreign Law Office Foreign Law Joint Enterprise with TMI Associates, 2016）
- セミナー資料「経営法友会月例会　欧州個人情報保護法の改正動向と日本企業の実務対応」（アシャースト法律事務所, 2016）
- セミナー資料「データ保護・プライバシーセミナー」（ベーカー＆マッケンジー法律事務所（外国法共同事業），2016）
- Peter Van den Bossche & Werner Zdouc, The Law and Policy of the World Trade Organization (3rd ed.) (Cambridge U.P., 2013)
- Hunton & Williams LLP, THE EU GENERAL DATA PROTECTION REGULATION: A guide for in-house lawyers（2016）
- Albright Stonebridge Group, DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION (2015)
- MCKINSEY GLOBAL INSTITUTE, DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS (2016)
- White & Case LLP, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law (2016)
- Information Technology Industry Council (ITI), Data Localization Snapshot as of September 15th 2016 (2016)

※その他、EUや経済産業省のウェブページに掲載されている公式文書を適宜使用。

越境データ移転に関するシンポジウム
―EUからのデータ移転と日本がとりうる選択肢を考える―

- **日時：2016年12月21日(水) 14:00～17:00**
- **場所：紀尾井カンファレンス(東京ガーデンテラス紀尾井町4F)**
- **プログラム（無料：お申込みは**http://passmarket.yahoo.co.jp/event/show/detail/013dg8yih38e.html**へ）**

（１）講演（14:00－15:25）

①其田真理　個人情報保護委員会事務局長
「（仮）個人情報保護委員会の国際的な取り組みについて」

②藤井康次郎　西村あさひ法律事務所　パートナー弁護士
「国際通商交渉・紛争の観点からみた越境データ移転問題」

③三膳孝通　株式会社インターネットイニシアティブ　技術主幹
「（仮）新しい個人データ保護への対応について」

④別所直哉　ヤフー株式会社　執行役員
「産業界の視点で考えるEUからのデータ移転」

（２）パネルディスカッション（15:40－17:00）

「EUからのデータ移転と日本がとりうる選択肢を考える」

モデーレータ：藤井康次郎　西村あさひ法律事務所　パートナー弁護士
パネリスト　：青野慶久　サイボウズ株式会社　代表取締役社長
石井夏生利　筑波大学図書館情報メディア系　准教授
中島洋　全国ソフトウェア協同組合連合会　会長
中村美華　株式会社セブン＆アイ・ホールディングス　法務シニアオフィサー
別所直哉　ヤフー株式会社　執行役員

Thank you for your kind attention.

Kenta Mochizuki, Attorney at Law (New York)

Public Policy & Corporate Governance

Corporate Management Group

Yahoo Japan Corporation

Kioi Tower, Tokyo Garden Terrace Kioicho,

1-3 Kioicho, Chiyoda-ku, Tokyo, 102-8282 Japan

kemochiz@yahoo-corp.jp