令和２年度内外一体の経済成長戦略構築にかかる国際経済調査事業
（FTAAPに向けたAPEC内での電子商及び越境データ移転の調査研究）

APECにおけるCBPRの促進策の調査結果報告

株式会社野村総合研究所
コンサルティング事業本部
コーポレートイノベーションコンサルティング部

2021年3月19日

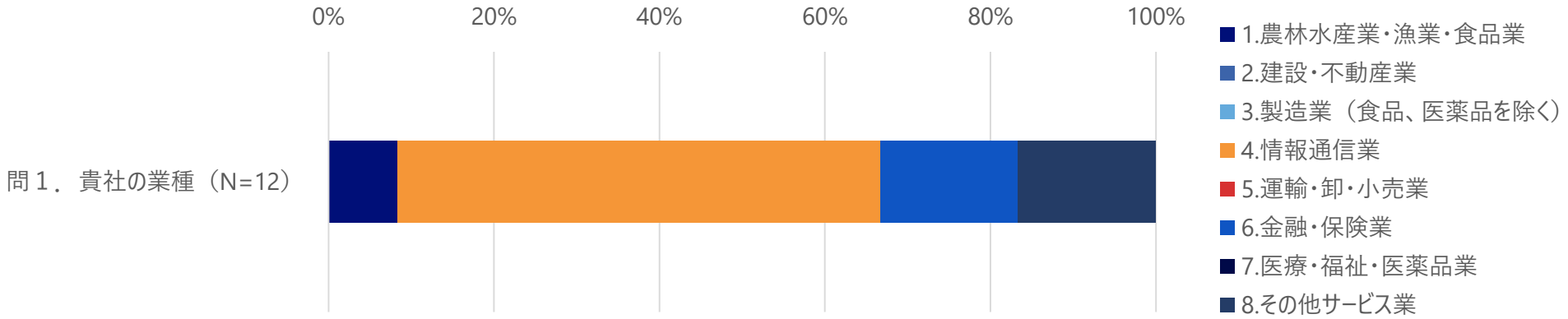
NRI

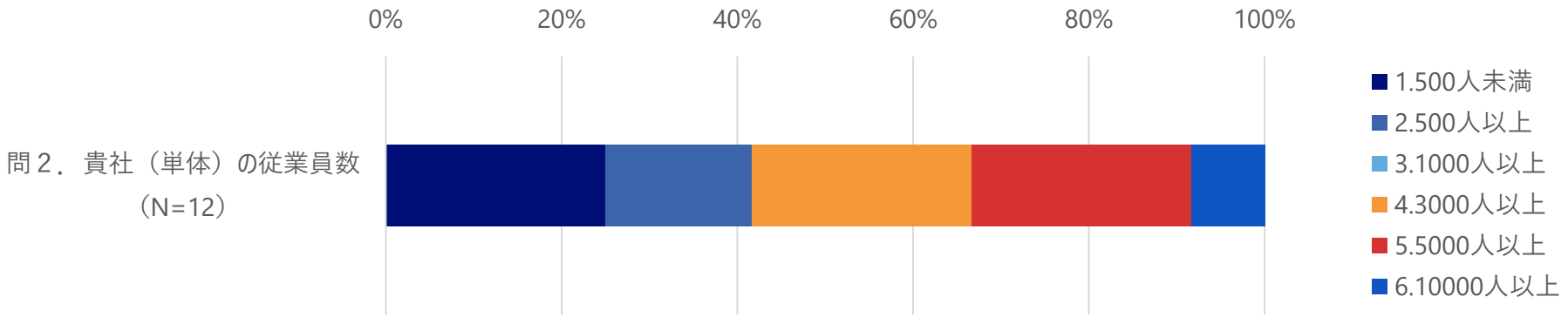
Share the Next Values!

回答企業・組織について

業種及び従業員数

- 61企業・組織に回答を依頼、12社から回答あり
- JISA経由での依頼を中心に実施したため、情報通信業が過半数を占めた



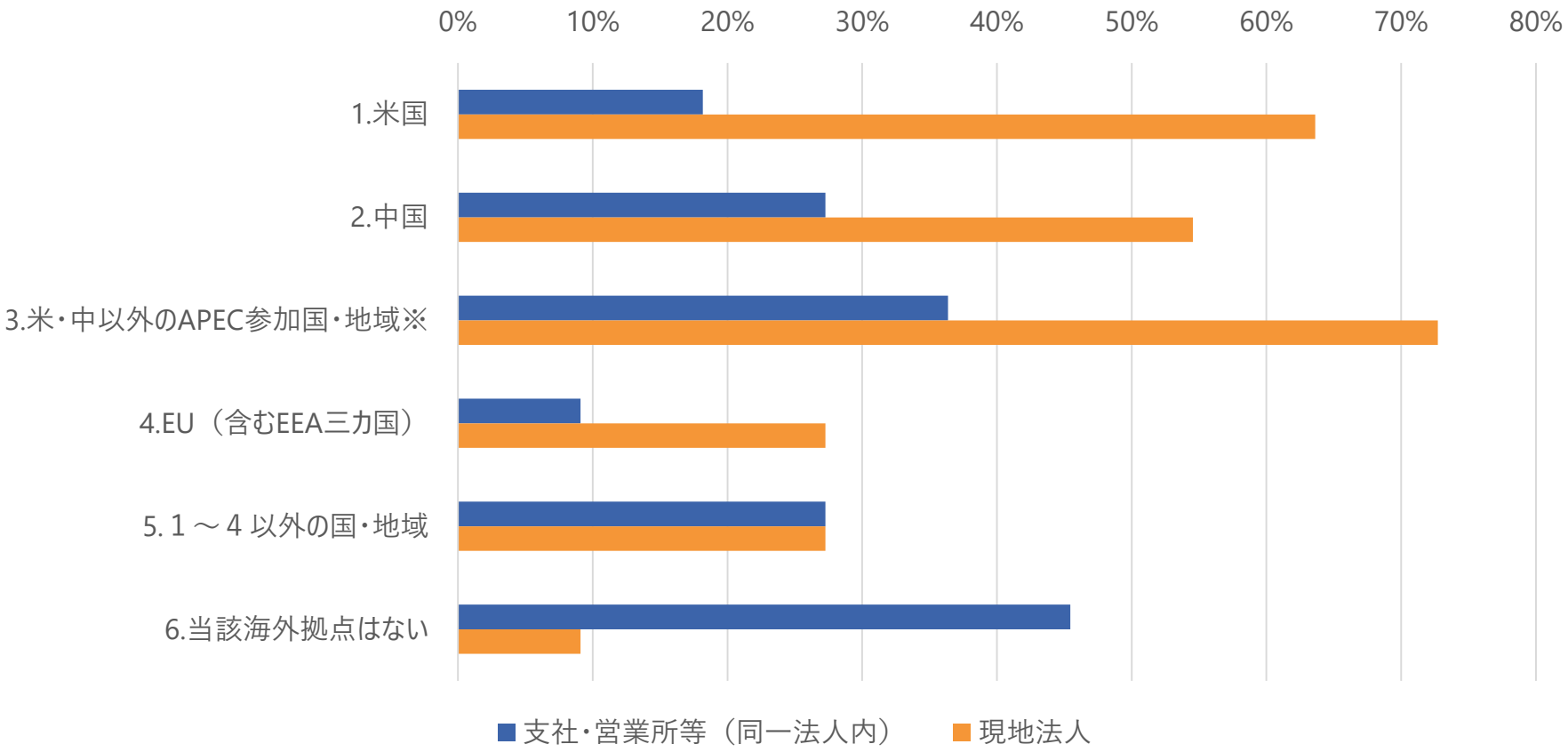


海外拠点の有無

同一法人内の支社・営業所等、及び現地法人の有無とその所在地

■ 同一法人内の支社・営業所等は所在国・地域にばらつきあり。現地法人は米国・中国が安定して多い

問３．系列企業の海外拠点の所在地（複数選択可）（N=12）

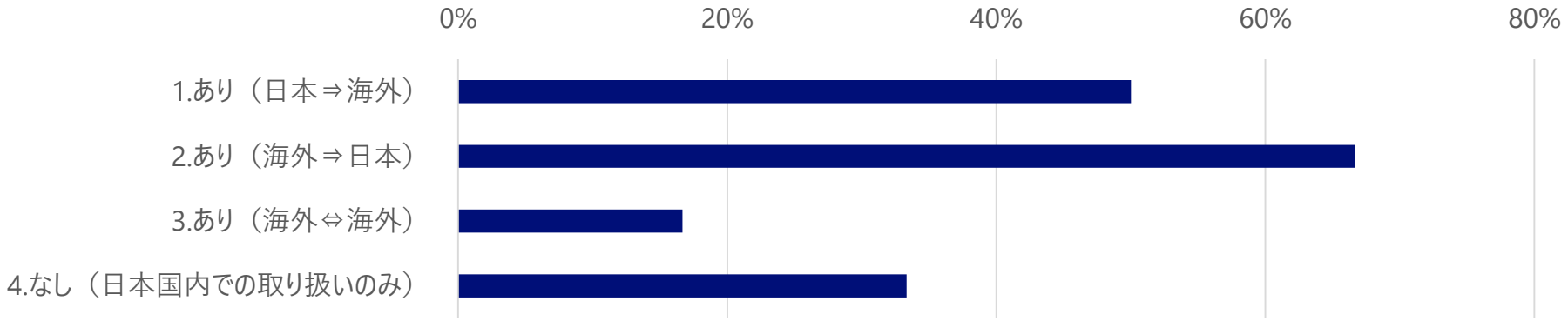


※韓国、台湾、香港、タイ、フィリピン、マレーシア、シンガポール、ブルネイ、インドネシア、パプア・ニューギニア、オーストラリア、ニュー・ジーランド、カナダ、メキシコ、チリ

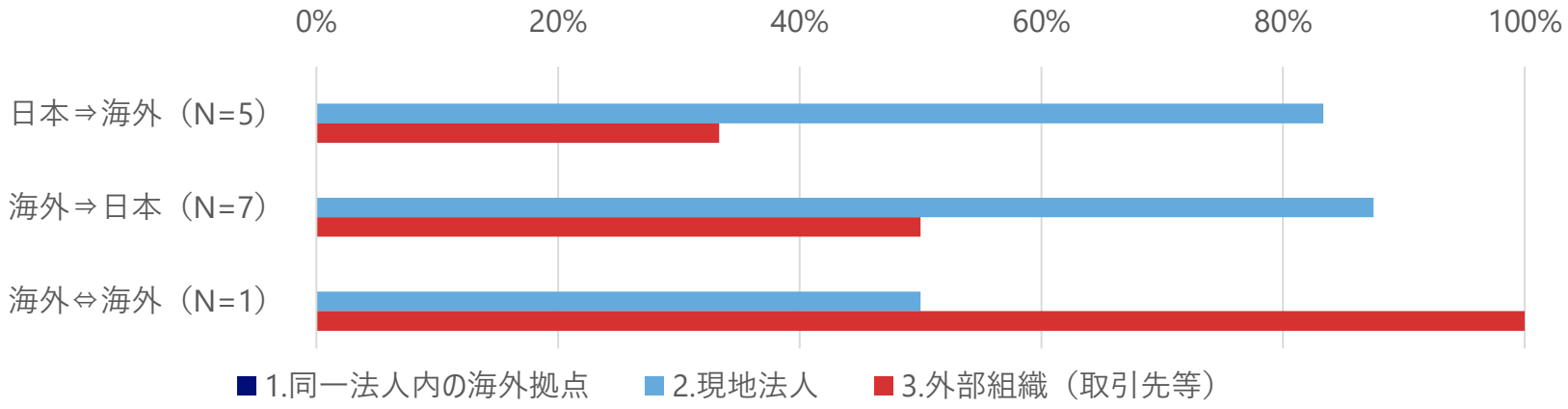
直近1年間で個人データを国・地域間で移転させた実績

- 直近1年間の個人データ移転実績では、海外から日本へのデータ移転が最も多く、移転元は現地法人が多い
- 同一法人内の海外拠点を移転元とする回答は0件であった

問４．直近1年間の個人データの越境移転実績（複数選択可）　（N=12）



問５．直近1年間の個人データの移転元（複数選択可）

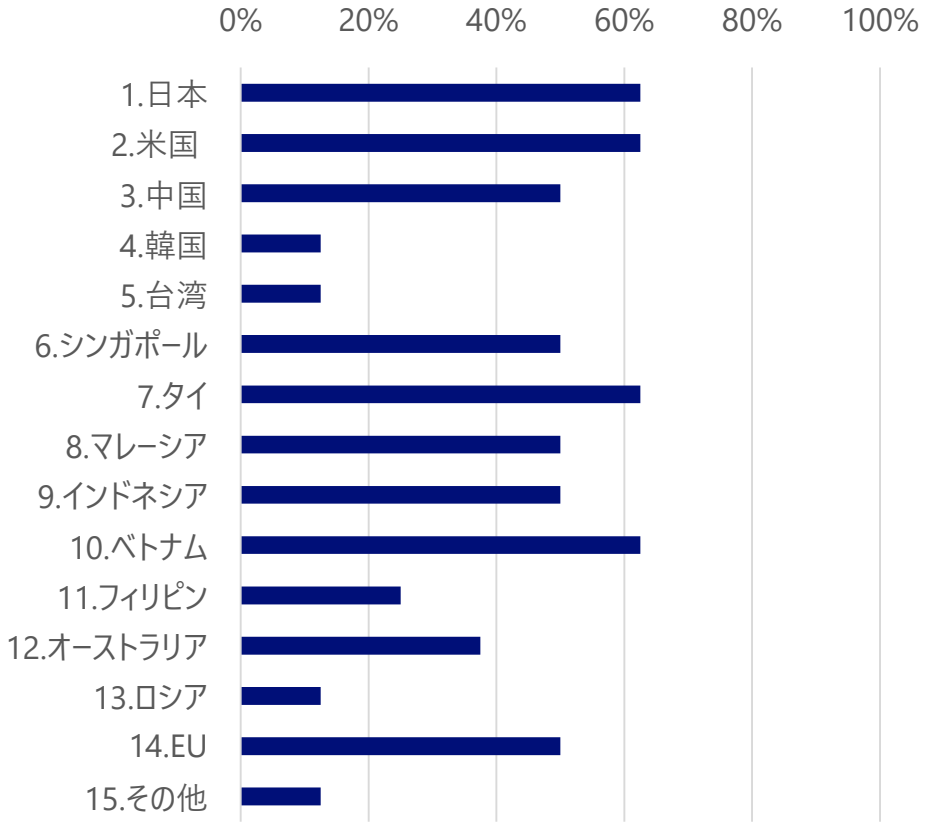


個人データを移転させている国・地域、及び今後データ移転が増加の見込みについて

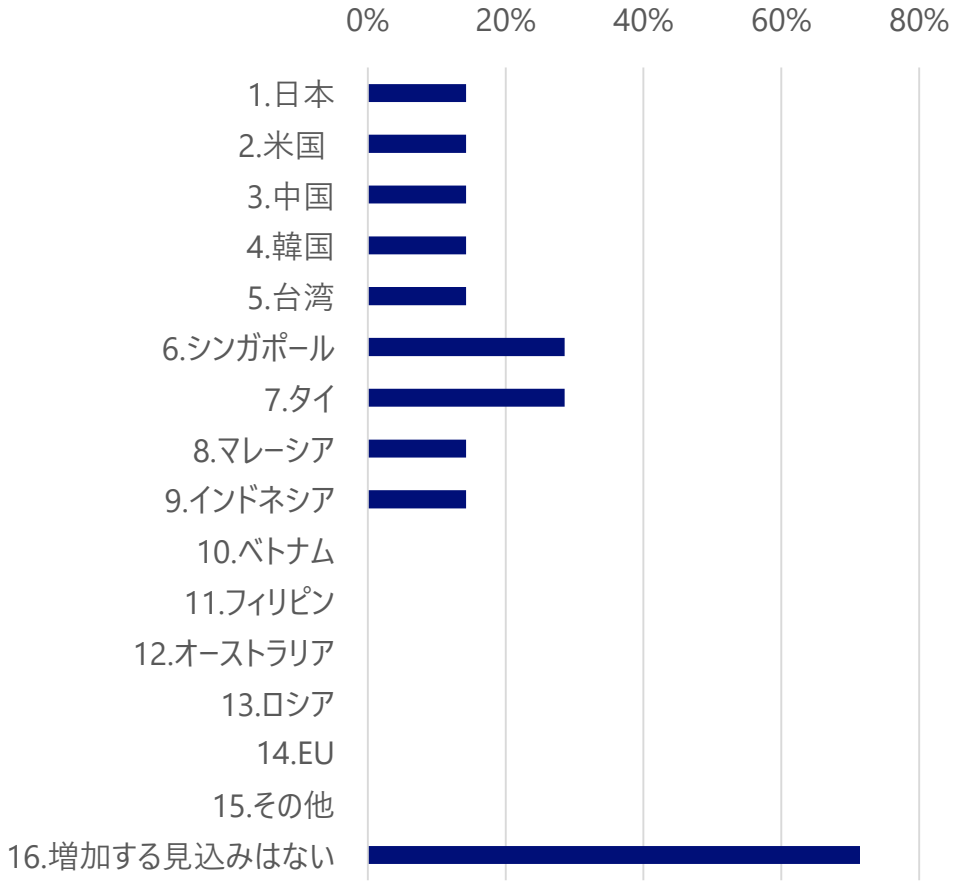
■ 個人データの移転元・移転先となっている国・地域に特筆すべき傾向はない

■ 今後、個人データ移転の増加を見込んでいない企業が大多数であった

問６．現在、個人データを越境移転している国や地域（移転元/移転先）（複数選択可）　（N=8）



問７．今後、個人データの越境移転が増加する見込みの国や地域（複数選択可）　（N=7）

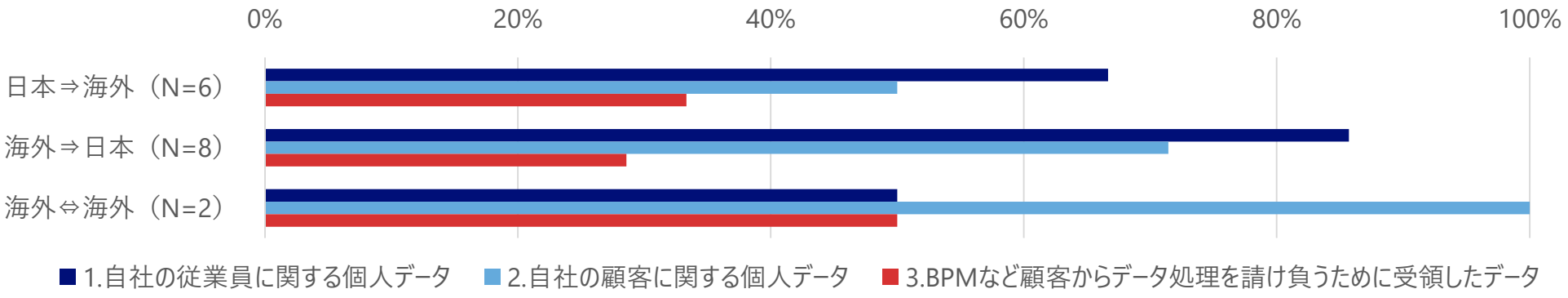


国・地域間で移転した個人データの内容と件数

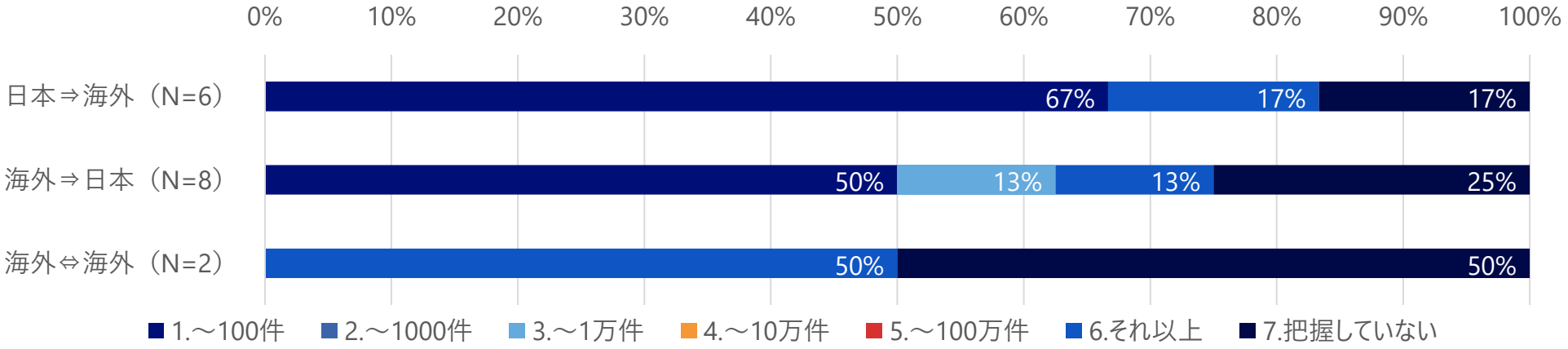
■ 海外から日本へのデータ移転が多く、自社の従業員または自社の顧客に関する個人データの移転が多い

■ 件数は100件未満との回答が最も多く、データフロー問わず把握していないとの回答も一定数あった

問８．どのような個人データを移転しているか（複数選択可）



問９．直近１年間で、およそ何人分（件）個人データを移転したか

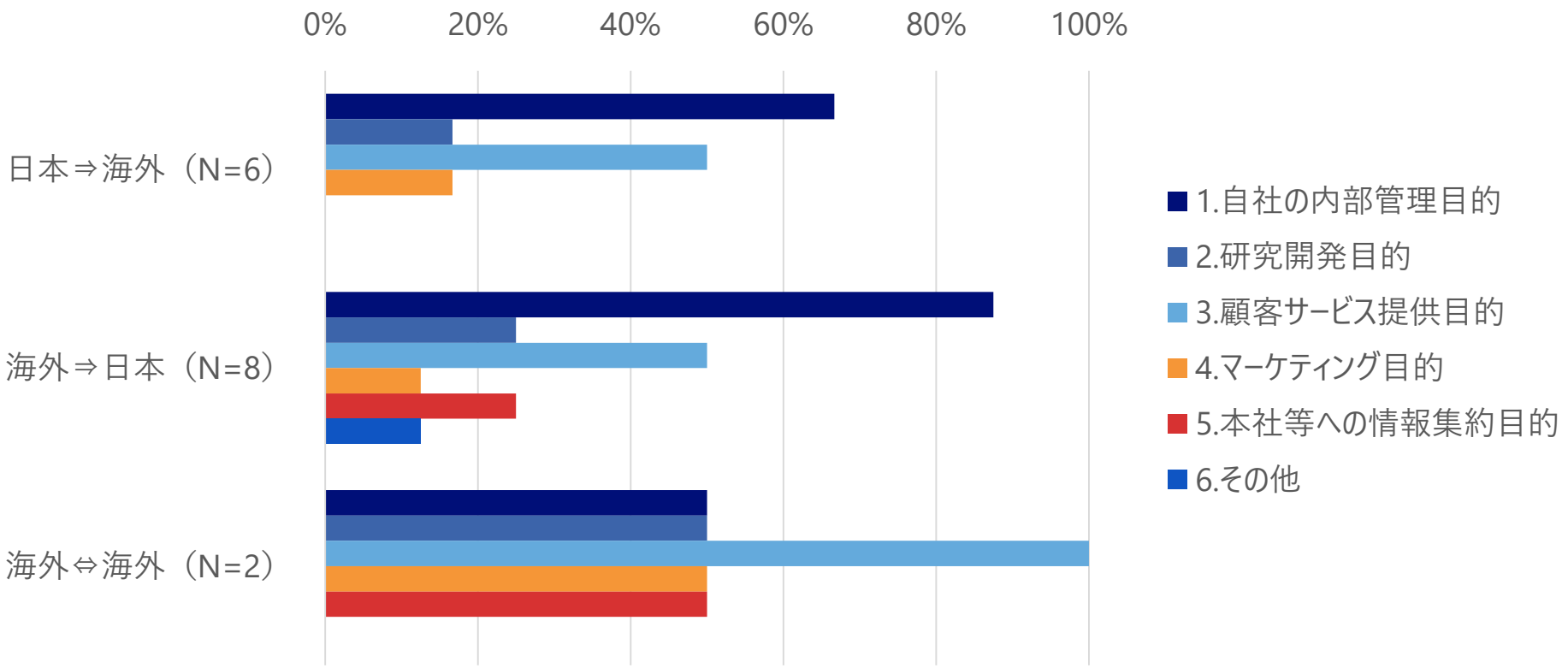


個人データを越境移転した目的

■ 日本を含むデータフローでは、自社の内部管理目的が最多。データフロー問わず、顧客サービス目的が一定数あり

- 海外⇒日本の「その他」には、「出向者のビザ申請書類作成」との回答あり

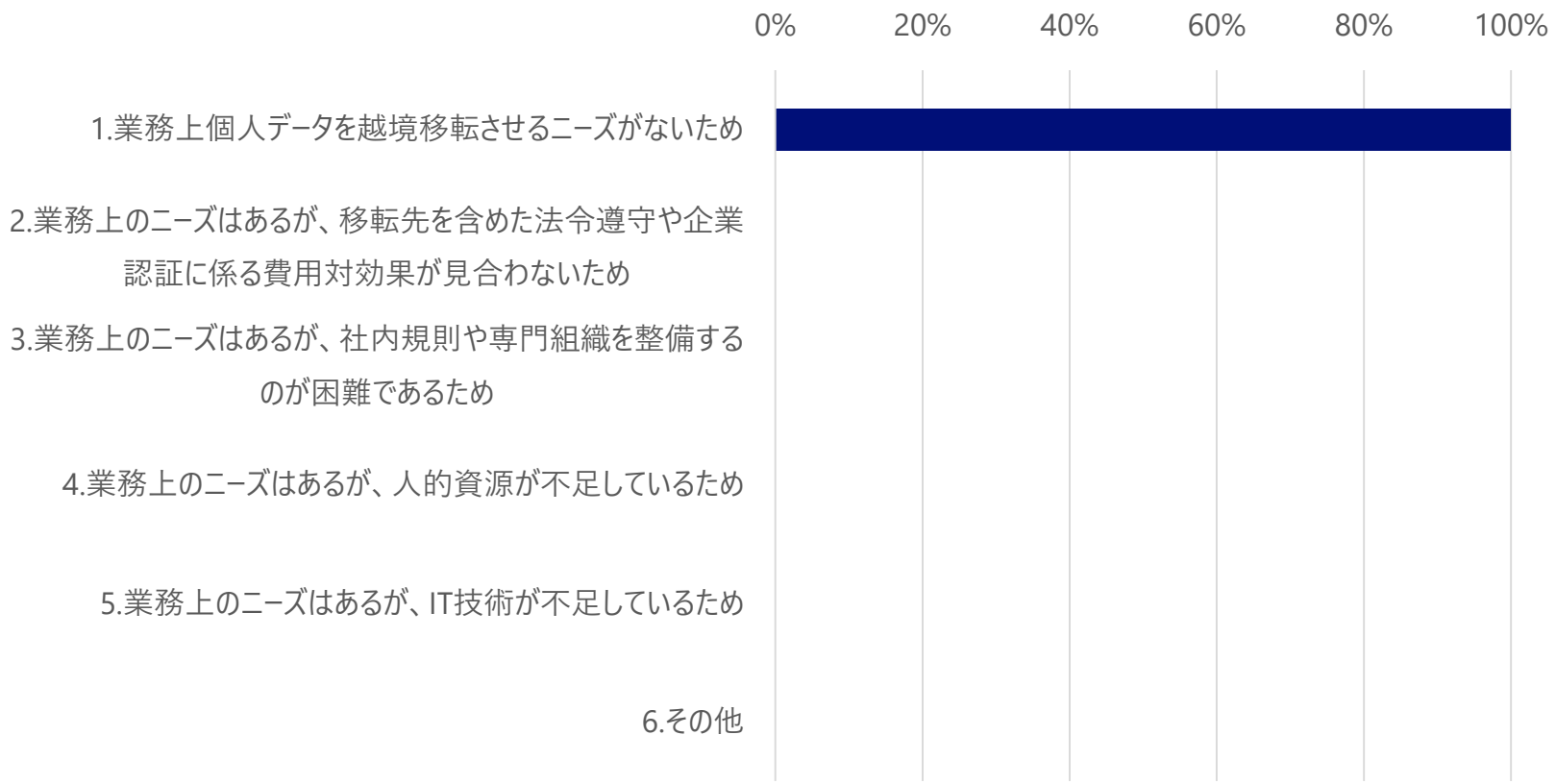
問10．個人データ移転の目的は何か（複数選択可）



直近1年間で個人データの越境移転を実施していない理由

■ 直近1年間で個人データ越境移転の実績がない理由として選択された回答は、すべて「業務上のニーズがないため」

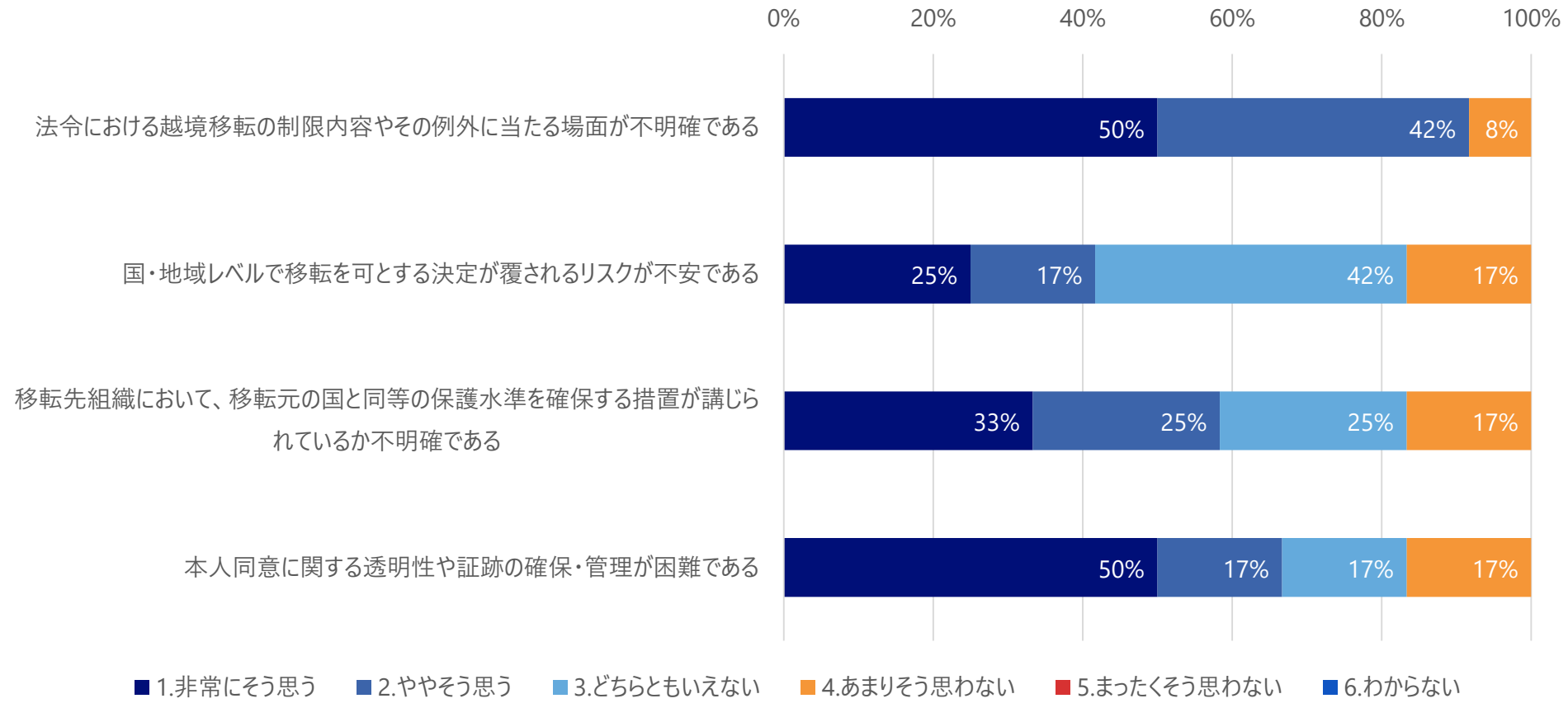
問11．個人データの移転実績がない理由（複数選択可）　（N=3）



個人データの越境移転の法令対応について企業・組織が課題・懸念と認識している事項

■ 個人データの越境移転については、法令の内容が不明確であること、次いで、本人同意の管理に関して懸念、課題としている企業・組織が多い

問12. 個人データの越境移転について、その法令対応に関する課題や懸念について（当てはまるものを選択）（N=12）



その他の課題や懸念事項

■ 問13. 問12の選択肢以外で、企業として懸念している事項、課題としている事項（自由記入）

- 各国の法令により、個人データ移転先となる外国の個人情報保護法制につき、データ輸出者として一定の調査・本人への情報提供が求められる傾向があると理解している（日本個人情報法保護法（令和2年改正）、GDPR（Schrems II判決を受けたEDPBによるRecommendations）等）。そのような外国法令調査等が個々のデータ輸出者である事業者に委ねられるとすると、本人への適切な情報提供が必ずしも担保されず、また、事業者による調査の重複による非効率が生じるのではと懸念している。
- 当社は、個人データの越境移転のためCBPRを取得していますが、Google等のクラウドサービスを通じて、ほとんど全ての会社が個人データの越境を行っているのが現実だと思います。
- 現時点では個人データの越境移転に関する事例はないが、弊社におけるサービス型事業の急速な拡大に伴い個人データの越境移転ニーズが高まることが予測され、GDPR対応を始めとした規定やルールの整備が急務と考えている。また、個人データに対する意識の高まりは世界的な潮流であるため、CBPR等の各国・各地域のルールに関する情報収集等も今後の課題と認識している。
- 各国の国内法に当社のやり方が抵触しないかの確認が専門家でないと難しいと思っています。
- 各社のプライバシーポリシーが、各国の個人情報保護規制を確実に準拠したものになっているか（どうかを懸念している）。
- 制限内容やその例外に当たる場面が不明確」という課題について、不明点は弁護士に聞けばよいが、制限内容が決まっていない場合があって困る。欧州はだいたい決まってきているが、他の国だと、どこまで適用されるか実際のところがわからない場合があり、対処方法を決めるに決められないケースがある。
- 2020年7月16日のSchrems II事件判決のように、十分性認定が覆されるリスクがあるなかで、どこまで織り込んで対応を考えるかが難しい。

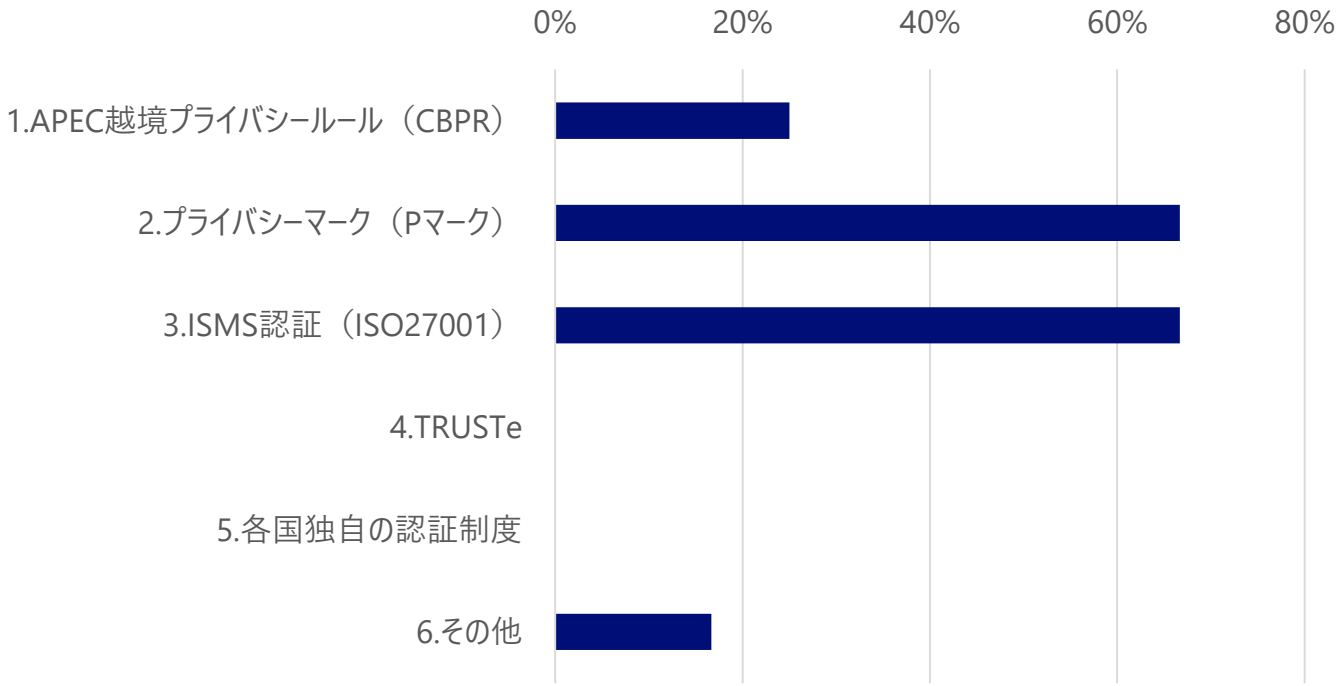
データ保護に関する認証について

回答企業・組織が取得している認証

■ データ保護に関する認証では、やはりプライバシーマークやISO27001を取得している企業・組織が多い

- 「6. その他」の自由記入欄には「PCI DSS」と回答あり

問14. 取得しているデータ保護に関する認証（複数選択可） （N=12）



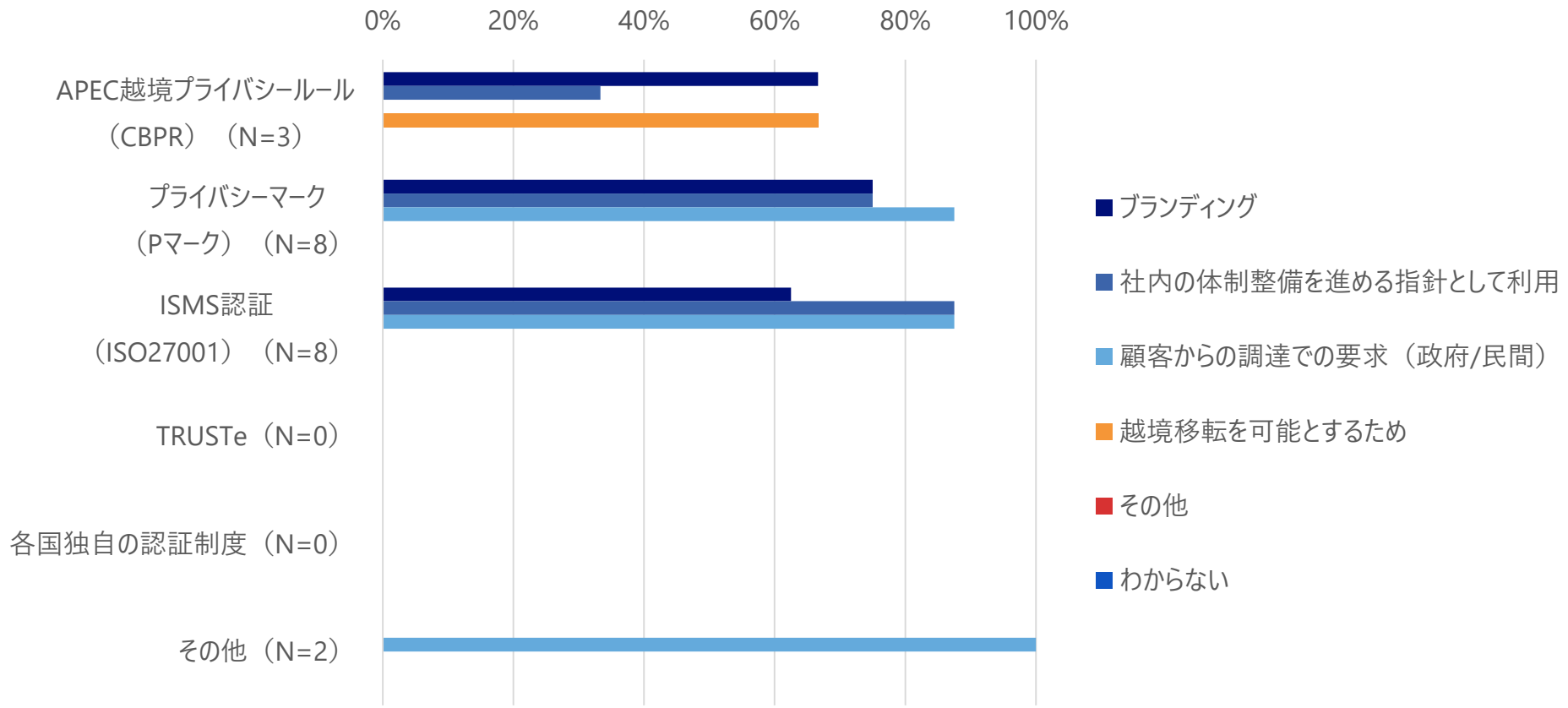
データ保護に関する認証について

回答企業・組織が取得している認証

■ プライバシーマークやISO27001と異なり、CBPRは越境移転を目的として利用されていることがわかる。逆に、Pマークや ISO27001の取得目的として選択されていて、CBPRで選択されていないのは、「顧客からの調達上の要望」であった

- 「その他」は問14の自由記入欄にて「PCI DSS」と回答あり

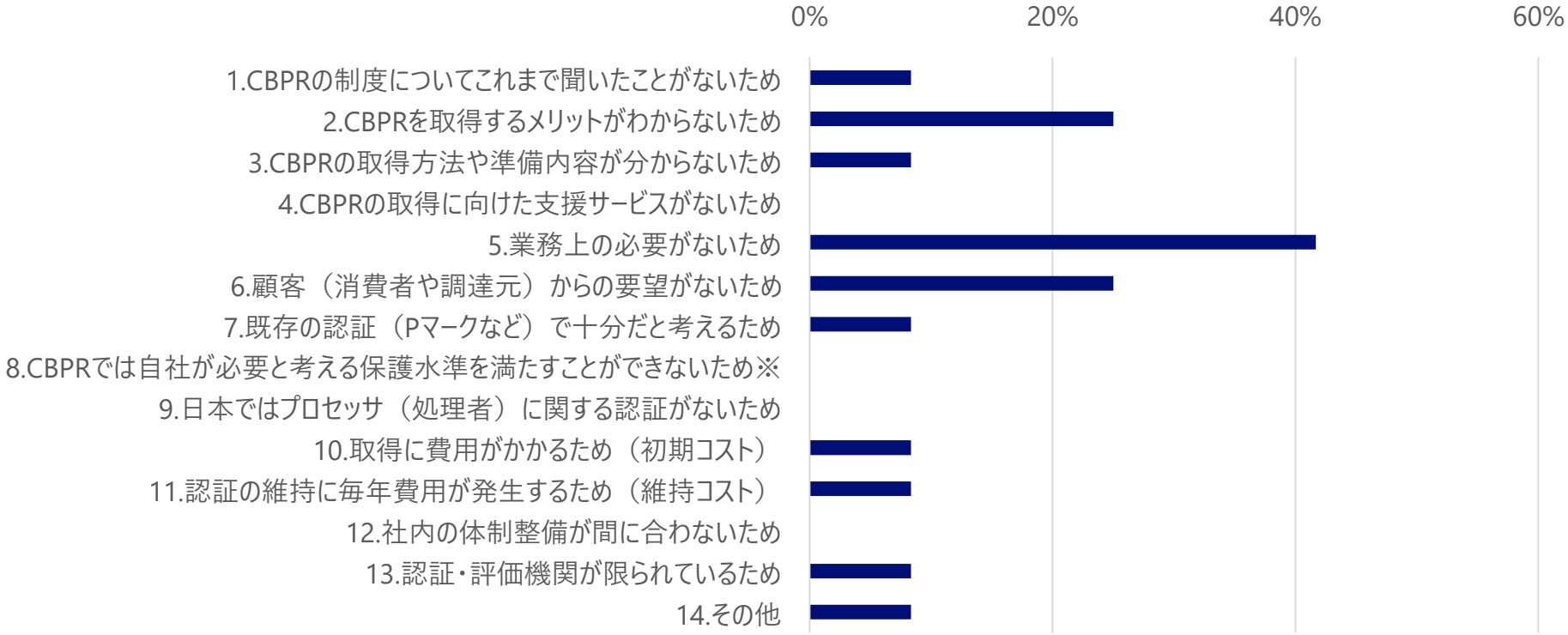
問15. 認証を取得した、あるいは取得しようとしている目的（複数選択可）



APEC越境プライバシールール（CBPR）を取得していない理由

- CBPRを取得していない理由としては、「業務上の必要がない」が最多、次いで「顧客からの要望がない」ことを挙げる企業が多い
- 初期コスト、維持コスト問わず、予算を原因とする回答はごく一部に留まった
- 「その他」の記入欄には「CBPR取得に関してはISO27701の動向も見たうえで検討」との回答あり

問16．CBPRを取得していない理由（複数選択可）　（N=12）



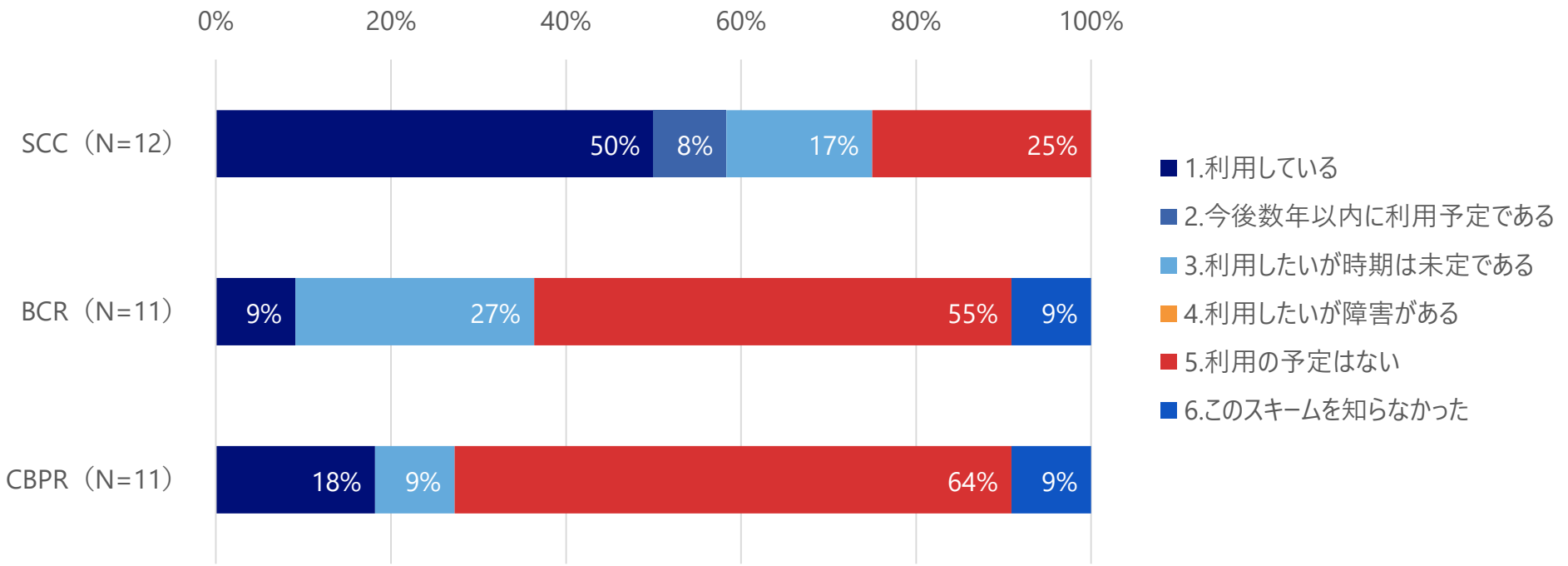
※EU 一般データ保護規則（GDPR）に準拠している場合を含む

今後利用したい個人データ越境移転に係るスキーム（※）

※法令上一般に越境移転が禁止されている場合において、例外的に越境移転が許容されるような仕組みをここでは「スキーム」と呼ぶ。BCRとSCCはEU一般データ保護規則（GDPR）上の、CBPRは日本・個人情報保護法上の「スキーム」となる。

- CBPRについて、今後利用したいと回答した企業は限定的で、「利用の予定はない」という回答が最多
- 一方で、CBPRを「知らなかった」という回答も少なく、利用実績の少なさが認知度の低さによるものとは考えにくい

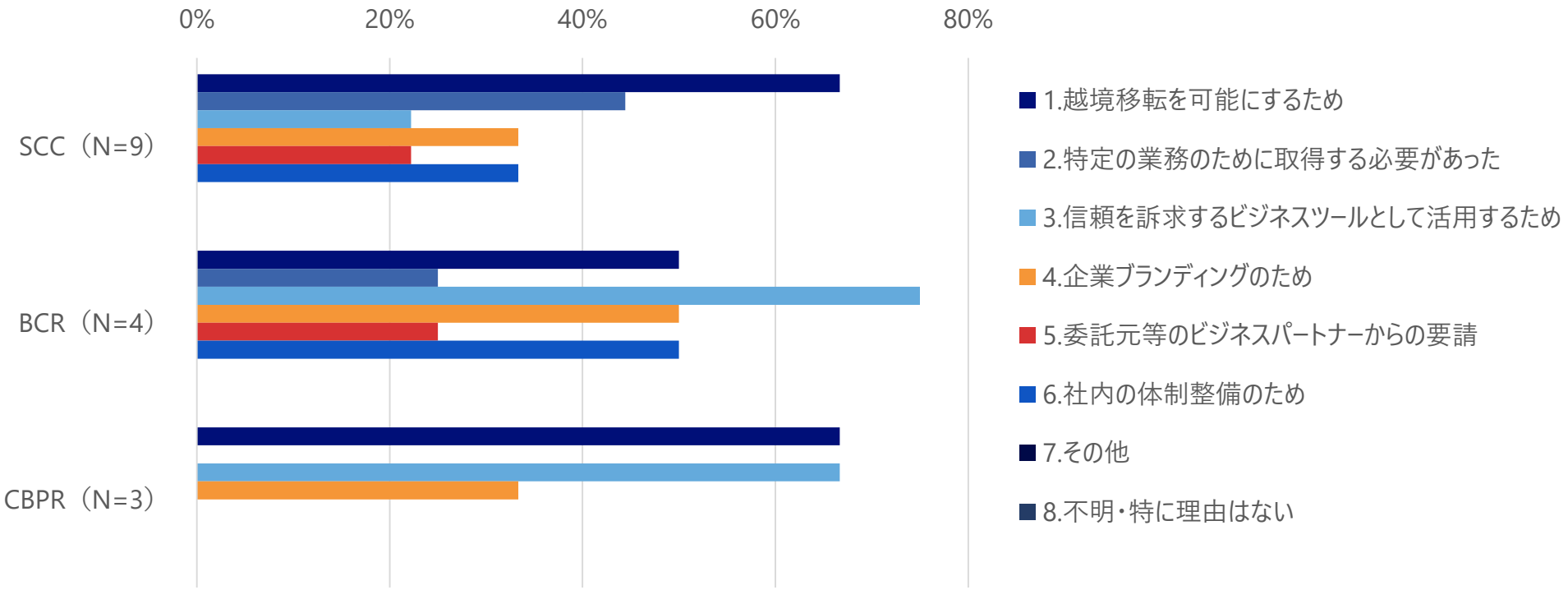
問17．個人データ越境移転に係るスキームについて



今後利用したい個人データ越境移転に係るスキームと、その理由

- 今後、CBPRを利用したい理由は、「越境移転を可能にするため」、「信頼訴求ツールとしての利用のため」が最多で、次いで「企業ブランディングのため」が選択されている
- CBPRを利用する（したい）理由にはなく、SCC、BCRを利用する（したい）理由として選択されているのは、「特定の業務のために取得する必要があった」、「ビジネスパートナーからの要請」、及び「社内の体制整備のため」

問18. 問17で「利用している」「今後数年以内に利用予定」「利用したいが時期は未定」「利用したいが障害がある」と回答したスキームを利用する（利用したい）目的（複数選択可）

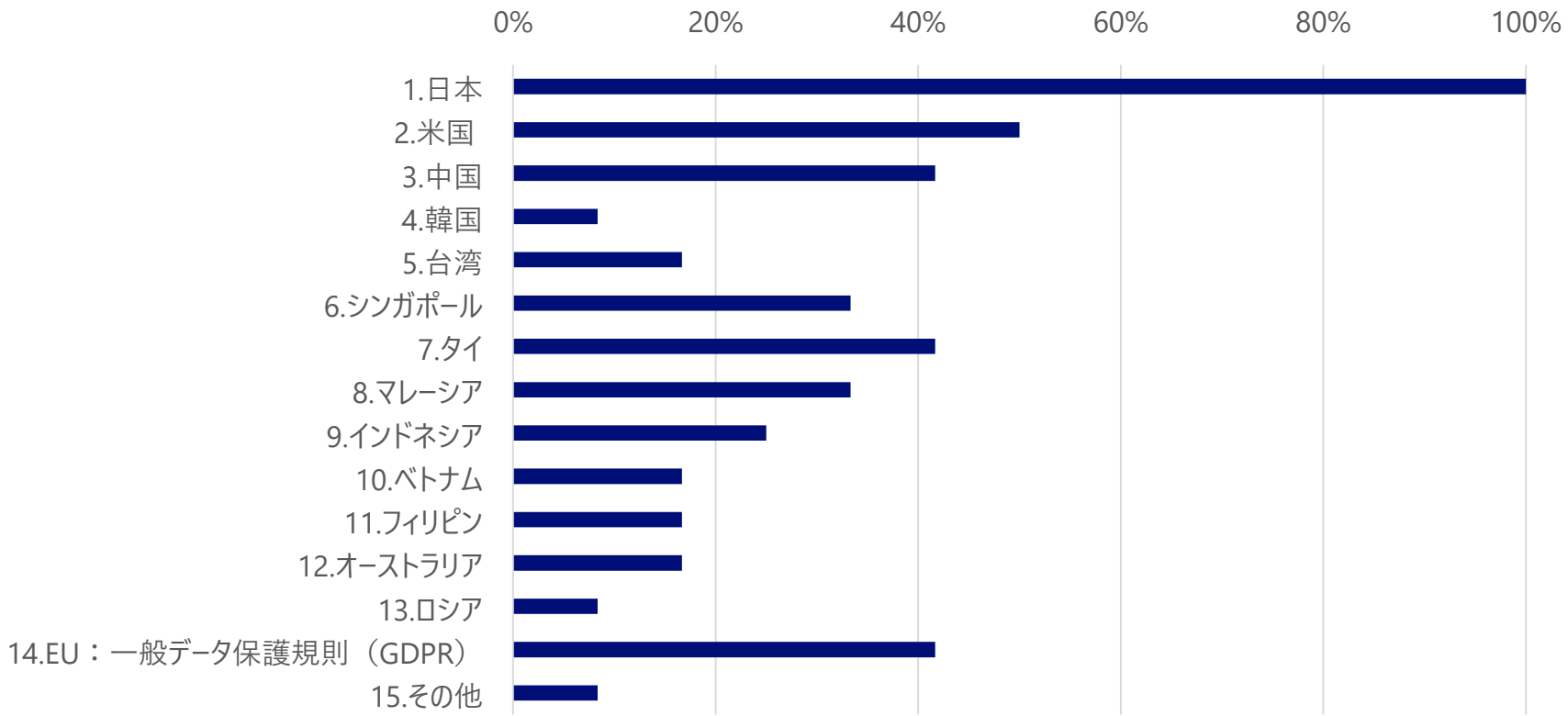


準拠している個人情報保護法令（※）

※個人情報保護を直接の目的としているもののほか、個人情報保護に関連する規定を含む法令などを含む。
インドネシアやベトナムなど、包括的な個人情報保護法は制定されていないが、電子商取引に関連する法令などの個別分野の業法などに個人情報の保護や情報の移転に関する規制が含まれる場合を意味する。

■ 日本以外では、米国の個人情報保護法令に準拠している企業が最多。次に中国・タイ・EU（GDPR）が多い

問18．準拠している国内外の個人情報保護法令（グループ会社を含む）（複数選択可）　（N=12）



アンケート調査結果のまとめ：CBPR検討の方向性

越境移転対応のメリットは認知されている。他方、日本企業における競合先はISMSやPマークであり、想定ニーズについてこれら認証との差別化・すみわけを検討する必要がある

■ 本アンケートから得られた示唆

状態	CBPRの想定ニーズ	アンケートでの検証結果	得られた示唆
越境移転あり	越境移転	• CBPRの越境移転対応としてのメリットは明確に認識されている	• 企業には越境移転ツールとして認知されている • しかし、CBPRを越境移転スキームとして認めているのは実質日本のみであり、この点APEC地域で越境移転スキームとしてのCBPR受け入れ拡大が必要
	社内体制整備	• 社内体制整備については、PマークやISMSが用いられることが多い（Q15） • ローカルな認証との競合は確認できなかった（同）	• 社内の体制整備に用いる場合、PマークやISMSとCBPRの差別化を図っていくことが必要
	調達対応	• 体制整備同様、調達対応についてもPマークやISMSに比べて要求事例が少ない（Q15)	• 政府調達や民間での調達基準としての活用が進めば、CBPRも拡大が進む可能性がある • そのためには、ISMSやPマークとの比較（コストとの兼ね合い）が必要
	ブランディング	• ブランディング目的での取得はすでに行われている	• ブランディングを目指すには、知名度の向上とともに、CBPR取得がPマークやISMSと比べてどのように高い水準を持っているかの検討が必要
越境移転なし		• -	• 越境移転を前提としない活用（体制整備、調達対応等）についても、さらなる検討が必要


Share the Next Values!

Provisional report on Work Plan on Digital Trade and E-Commerce

Mid-term Report

(Final Report will be completed by MRT, 2021)

March, 2021

CONTENTS

Executive summary 3
Introduction of the project 4
Chapter 1: Take stock of digital trade / e-commerce elements in FTAs/RTAs, assess convergence and divergence, and examine current situations and new trends. 7
1.1 The legal control on electronic commerce in RTA 7
1.2 CHAPTER ON ELECTRONIC COMMERCE IN EPAS/FTAS 10
1.3 REGULATIONS CONCERNING DATA LOCALIZATION 27
1.4. Recent Legislative Activities among APEC Economies 31
1.5. Overall analysis on stocktaking 36
Chapter 2: Assess digital trade and e-commerce related initiatives in APEC (CTI, DESG, TEL, including the APEC Internet and Digital Economy Roadmap, APEC Cross-Border E-Commerce Facilitation Framework, etc.) and initiatives in other international fora including the WTO. 39
2.1 e-commerce related initiatives in APEC 39
2.2 DISCUSSIONS WITHIN MAJOR INTERNATIONAL ORGANIZATIONS 40
Chapter 3: Consider next steps on the issues related to the eventual realization of FTAAP taking into account the above-mentioned assessments and capacity building activities. 49
3.1 Capacity building for legal and operational framework for facilitating e-commerc 49
3.2 Promotion of CBPR as a foundational framework for APEC's privacy protection and maintaining interoperability with privacy frameworks with other regions 51
3.3. Common Understanding on Data Free Flow with Trust that facilitates e-commerce and domestic reforms 52

Executive summary

The purpose of this report is to propose possible further action planes, such as rule-makings and capacity building activities of APEC for the expansion of digital trade and e-commerce.

To this end, in the Chapter 1, this report examined stocks of digital trade / e-commerce related provision of existing major RTA/FTA/EPAs and domestic regulations on data, such as data localization requirements. The outcome here is that APEC economies have entered numerous trade agreements with other economies that contains digital trade/e-commerce chapters. This survey also revealed that among these chapters, while basic articles, such as privacy protection, consumer protection and electronic signature gained wide acceptance, other articles especially those on international data flows gained substantial acceptance (10-50% of the total).

We can also point out that while FTAs/EPAs with e-commerce related articles, National legislations that may restrict international data flows are also widespread.

Chapter 2 examined digital trade and e-commerce related initiatives in APEC and other international organizations. This includes capacity building for legal and operational framework for facilitating e-commerce and privacy protection initiatives in the APEC, especially on CBPR including. In addition, this Chapter also covers relevant discussions in the international organizations, OECD and UNCITRAL. This contains privacy protection, online dispute resolution and model laws on electronic transactions.

Chapter 3 is dedicated to the analysis on possible future steps for APEC concerning digital trade and e-commerce related initiatives, which eventually leads to FTAAP. This analysis covers capacity buildings for legal and operational framework for facilitating e-commerce, promotion of CBPR as a foundational framework for APEC's privacy protection and domestic reforms for realizing Data Free Flow with Trust that facilitates digital trade and e-commerce.

Introduction of the project

The recent developments in information and communications technology, as exemplified by the Internet, have profound positive impacts to spur innovation in the mostly all the sectors, and dramatically reduced the cost of international trade. The growth of the Internet has, since its birth in the 20th century, accelerated and demonstrated the importance of cross-border data flows, transformed R&D, production, delivery and consumption process of goods and services and created numerous business opportunities, particularly for MSMEs in the Asia-Pacific region.

As a result, trade opportunities have been created for a broader range of people, businesses and enterprises especially for those traditionally outside of global value chains due to the lack of appropriate infrastructure, efficient logistics or access to suitable markets. In addition, recent Regional Trade Agreement, Free Trade Agreement, and Economic Partnership Agreement (here in after referred to as "RTA", "FTA", and "EPA") have included provisions or independent/dedicated chapters or articles to address digital trade and e-commerce related issues.

Keep up with these changing landscapes of digital economy, APEC has conducted various activities on digital trade / e-commerce. In 2009 the Study on Identifying Convergences and Divergences in APEC RTAs/FTAs analyzed the similarities and differences of Electronic Commerce provisions. In the Pathways to FTAAP (2010) Leaders affirmed "APEC should contribute to the pursuit of an FTAAP by continuing and further developing its work on sectoral initiatives in such areas as investment, services, e-commerce, rules of origin, trade facilitation including supply chain connectivity and Authorized Economic Operator (AEO) programs, and environmental goods and services (EGS)", and subsequently the Beijing Roadmap for APEC's Contribution to the Realization of the FTAAP (2014) agreed to accelerate works including "advancing initiatives in areas such as investment, services, e-commerce, rules of origin, global value chain, supply chain connectivity, customs cooperation, environmental goods and services, good regulatory practices, as well as next generation trade and investment issues that the FTAAP should contain".

Furthermore, in 2015, APEC agreed on the Work Plan for Advancing "Facilitating Digital Trade for Inclusive Growth" as a Potential Next Generation

Trade and Investment Issue. Based on Leaders' instruction included in their 2015 Declaration, it was implemented in the following year. In 2016, the Collective Strategic Study on Issues Related to the Realization of the FTAAP (CSS) included digital trade as a potential next generation trade and investment (NGeTI) issue, while without prejudice to possible future work on FTAAP. In 2017, the APEC Capacity Building Needs Initiative (CBNI) Seminar on Electronic Commerce Chapter of the RTAs/FTAs took place with the aim of sharing experiences among economies, understand business needs, increase capacity and explore possible policy implications.

Business expectations are also high. APEC Business Advisory Council (ABAC) has continuously included recommendations on digital trade / e-commerce in its annual Report to APEC Economic Leaders in recent years.

For the eventual realization of FTAAP, digital trade / e-commerce elements are indispensable and should address the business needs and the latest trends of international trade and the global economy.

In 2020, most of the countries in the world is facing the unprecedented challenges posed by the COVID-19 pandemic. On 5th May, the APEC Ministers Responsible for Trade had issued the statement on COVID-19 calling for the member economies to collaborate at all levels and across the region to hasten our fight against COVID-19 to mitigate its impacts on international trade and investment. While imposing limitation of international movement of people, utilization of digital technologies are fundamental aspects to achieving secure distribution of goods and service and supply chain resilience. On 25th July, the Ministers responsible for Trade Meeting was held virtually and adopted minister's statement on COVID-19. The statement stated that "We(ministers) encourage Economies to collaborate and adopt digital solutions that will strengthen supply chain resilience as well as enable seamless cross-border business, including through e-commerce. In harnessing the opportunities of digital economy, the ministers acknowledge the importance of cooperation on facilitating the flow of data and strengthening consumer and business trust in digital transactions."

In that context, the member economies should be required further facilitation of Data Free Flow with Trust and support the international rule-making on e-commerce not only in the WTO, but also individual RTA.

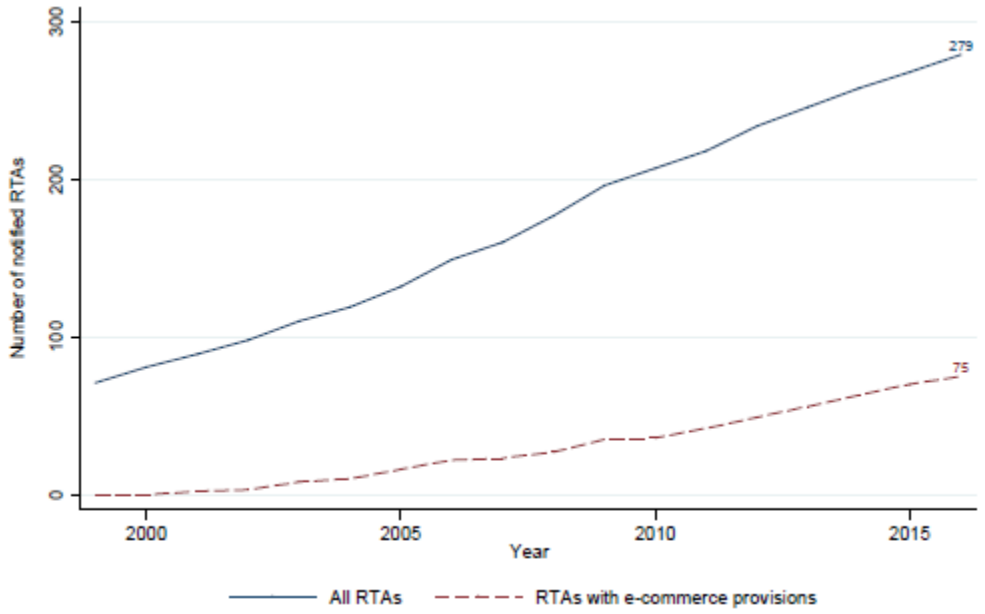
Based on aforementioned background, this report consisted by 3 chapters. Firstly, implementation of a take stock on digital trade / e-commerce elements in FTAs/RTAs to assess convergence and divergence of the current situations and new trends in e-commerce chapter. Secondary, the report assess digital trade and e-commerce related initiatives in APEC (CTI, DESG, TEL, including the APEC Internet and Digital Economy Roadmap, APEC Cross-Border E-Commerce Facilitation Framework, etc.) and initiatives in other international fora including the WTO. Finally, the report concludes the study including a consideration of next steps on the issues related to the eventual realization of FTAAP taking into account the assessments and capacity building activities. The report conducted a survey to member economies and received answers from 11 economies.

Chapter 1: Take stock of digital trade / e-commerce elements in FTAs/RTAs, assess convergence and divergence, and examine current situations and new trends.

1.1 The legal control on electronic commerce in RTA

José-Antonio Monteiro and Robert Teh (2017) noted that increasing number of RTAs with e-commerce provisions is in line with the growing discussions on the role of e-commerce and digital economy in the policy agenda of many regional and multilateral forums and organizations(Figure 1).Updating the figure with Regional Trade Agreements Database provided by World Trade Organization, there are 342 RTAs in the world of which 86 RTAs, representing 28% of all the RTAs notified to the WTO and currently in force as of March 2021. The trend on the e-commerce elements in RTA has been continuing.

Figure 1: Evolution of RTA's with e-commerce provisions



Source: José-Antonio Monteiro and Robert Teh(2017)

Although discussions on e-commerce under the international frameworks have not reached conclusions, establishment of effective legal control within EPAs/FTAs has progressed since the chapter on electronic commerce was included in the Australia-Singapore FTA (signed in February 2003). The legal control on electronic commerce have been mainly discussed following contents

as the “concept of electronic commerce”,“classification of digital contents”, and “custom duties”.

(1) THE DEFINITIONS AND OUTLINE OF ELECTRONIC COMMERCE

The concept of electronic commerce is either not defined or used in individual terms and definitions in existing international agreements. In the “chapter on electronic commerce” in EPAs/FTAs, “electronic commerce” is not defined, but characteristics that constitute electronic commerce are set out as follows.

(a) TECHNOLOGICAL NEUTRALITY

Although electronic commerce and traditional commerce have differences in methods and technology, other elements are technologically neutral.

We can see this concept applied to, for example, the method to declare the commercial intention (paper-based document or E-mail), the method to supply services across the border (postal mail, fax. telephone or E-mail) and the method to deliver the intangible products including software (trade in tangible medium like CD/DVD or communication with electromagnetic wave for broadcasting or Internet).

(b) ECONOMIC GROWTH AND OPPORTUNITY

This is a concept that seeks to grasp the true nature of electronic commerce, based on the principle that there should be a proper awareness of the advantages of multiple international transactions specific to electronic commerce and that internationally consistent initiatives aimed at the maintenance and further development of these advantages should be promoted in order to maintain this trend and aim for further growth.

(c) ENVIRONMENT OF TRUST AND CONFIDENCE

This is a concept that seeks to grasp the essence of electronic commerce, focusing on the risks, such as increased opportunities for fraud or the leakage of information, based on the principle that there should be a proper recognition of the nature of such risks and that internationally consistent initiatives/framework should be promoted in order to avoid or reduce such risks.

(2) THE CLASSIFICATION OF DIGITAL CONTENTS

When the digital contents are purchased, the applicable WTO rules are found in either GATT, GATS or TRIPS depending on whether the issue that arises out of marketing digital contents is the purchase price of goods, payment for a service, or royalty for intellectual property rights, respectively. Among countries that have concluded EPAs/FTAs including “chapters on electronic commerce”, the United States, Australia and Japan have continued to take neutral positions with respect to classification or distinction of them. These countries maintain their neutral stance in discussions within the WTO and this is frequently cited in the chapters on electronic commerce in the form of an annotation.

(3) NOT IMPOSING CUSTOMS DUTIES

Custom Duties are not imposed on software that is downloaded from another country from websites through the Internet. One of the reasons is that electronic transmissions cannot be captured by modern technology and so imposition of customs duties is practically not possible. However, it is also internationally agreed at present that customs duties should not be imposed on electronic transmissions.

Regarding bilateral EPAs/FTAs, the non-imposition of custom duties is stipulated as a permanent legal obligation in the chapter on electronic commerce of the FTAs concluded by the United States and Australia.

The modalities for custom duties on carrier media including software were discussed at the GATT Committee on Customs Valuation before the creation of the WTO. The Committee decided that "If the software is transmittable through a wired channel or a satellite, there are no issues of custom duties"; this is a circumstance to be considered for custom valuation of software.

If electronic transmissions can be technologically captured in the future, the Moratorium on Customs Duties will end and some WTO member countries may start imposing customs duties on electronic transmissions. The objective of having a provision on electronic commerce within bilateral FTAs is to prepare for these risks.

Nevertheless, even for an electronic transmission from a contracting country to an FTA, it is difficult to determine whether or not the source of the transmission was the contracting country. In other words, a policy of a non-imposition of custom duties that is restricted between two contracting countries is likely to be impossible.

So, it is possible to understand that the objective of this discipline is, through the increase of EPAs/FTAs with this discipline, to actually establish 'non-imposition community' which can remain even when electronic transmissions can be captured. In other words, contracting parties of FTAs that stipulates Moratorium on Customs Duties will remain this position for all electronic transmissions, regardless of their imported countries.

1.2 CHAPTER ON ELECTRONIC COMMERCE IN EPAS/FTAS

1.2.1 General Assessment on CHAPTER ON ELECTRONIC COMMERCE IN recent EPAS/FTAS

In terms of elements in e-commerce provisions, our survey on 11 economies observed following trends:

- Elements of e-commerce used to be defined within other chapters' provisions rather separated chapters at the present.
- Moved beyond cooperation in the traditional sense to more comprehensive, focus on higher standard and ambitious provisions such as fast changing and emerging technologies like Artificial intelligence.
- Latest agreement include trust (e.g. online consumer protection, unsolicited commercial electronic messages, protection of data privacy, and protection of intellectual property rights), facilitation (e.g. electronic authentication and signatures and paperless trade) and liberalization provisions to enhancing protection of consumers and ensuring market access.

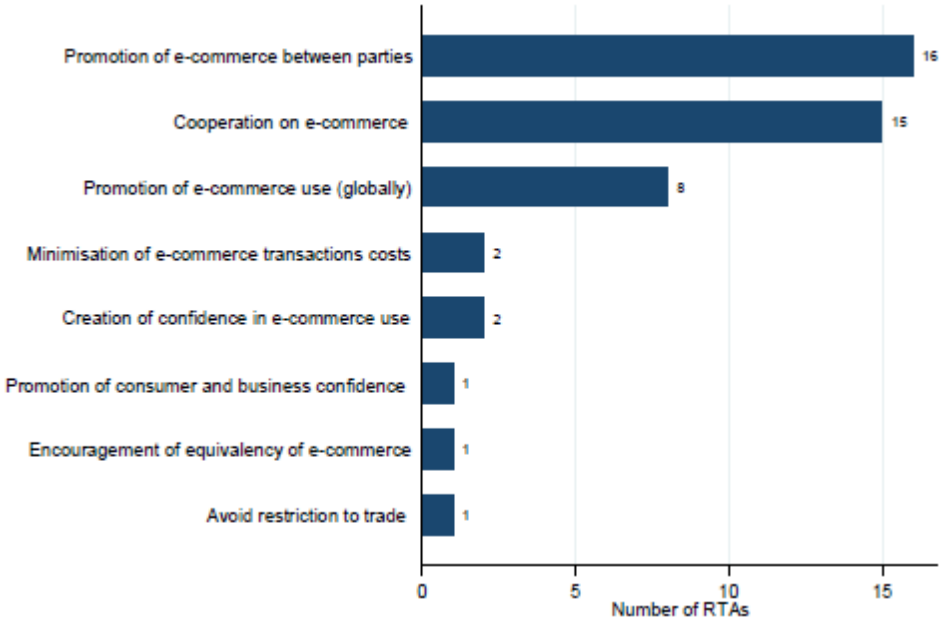
On the other hand, some member economies noted that gaps in terms of competitiveness and level of readiness and different domestic regulation are issues can be addressed since level differences on e-commerce development has still been existing among member economies. Also the survey noted that e-commerce rules should create a level-playing field, consider the extent to which the new provision helps to reduce barriers to trade, and response to the needs of the business community. Even such gaps are existing among member economies, it is interesting that UNCTAD 2019 refer to a research and said that "a growing number of preferential trade agreements (PTAs) include provisions related to digital trade, touching on issues relevant to AI, such as data flows, disclosure of source code and algorithms and data localization. These provisions

can be found in well-known treaties, such as the CPTPP and USMCA, but it is interesting to see that developing countries are also increasingly adopting similar language in their own agreements, even those without a developed digital industry. This shows that the challenge of countries to better understand their own interests when negotiating these digital provisions". It means that there is a question whether economies should be considered the gaps of digital development whenever setting up domestic and/or international rules on e-commerce.

This story seems to be linked with convergence and divergence, rapidly evolving digital technology and its use has clearly made a change the way of business and people's lives, and expanded digital gaps among economies whether how much the economy accommodate the technologies. Each economy legislate their domestic regulations with their own circumstances while international legislation on e-commerce should be unified. We need to take into account the balance between diversifying domestic legislation and convergence of international legislation.

José-Antonio Monteiro and Robert The (2017) analyzed the objectives of e-commerce chapter as shown figure 2, they noted that objectives are not only promote e-commerce between the parties, cooperation and the wider use of e-commerce globally, but also creating an environment of trust and confidence in the use of e-commerce.

Figure 2: Types of objectives of the RTA's chapter on e-commerce



Source: José-Antonio Monteiro and Robert The (2017)

As reference of the "Data Age 2025" published by Seagate 2018, the report predicts that the Global Data which created and corrected in the world will grow from 33 Zettabytes (ZB) in 2018 to 175 ZB by 2025. The development of data utilization in various businesses with tremendous increase of data volume has been being nature of business profit. However, such expansion of digital economy raise an issue of necessity of enhancement of e-commerce chapter in terms of "free data flow", "Data protection" and "Encouragement of smooth digital trade". In that context, the concept of the "Data Free Flow with Trust" has been shared in 2019 in the occasion of World Economic Forum and OSAKA G20 summit.

Figure " " shows contents of e-commerce provisions in recent FTAs such as Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States-Mexico-Canada Agreement (USMCA), EU-Japan Economic Partnership Agreement, U.S.-Japan Digital Trade Agreement, and ASEAN E-Commerce Agreement, elements which includes trust elements. It means that importance of trust provisions are more increasing in the FTAs/RTAs.

Figure 3: Contents of e-commerce chapter in recent FTAs

Elements	CPTPP	USMCA	EU Japan	US Japan	ASEAN
Electronic signatures and authentication	●	●	●	●	●
Paperless trading	●	●			●
Electronic Payment					●
Non-imposition of customs duties on electronic transmissions	●	●	●	●	
Principle on access and use of the Internet	●	●			
Non-discriminatory treatment of digital products	●	●		●	
Cross-border transfer of information	●	●		●	●
Location of computing facilities	●	●		●	●
Online consumer protection	●	●	●	●	●
Unsolicited commercial electronic messages	●	●	●	●	
Protection of personal information	●	●	●	●	●
Source code	●	●	●	●	
Cooperation	●	●	●		●

Source) Each e-commerce chapters in the FTAs

The chapter starts with a brief review of the scope, non-imposition of customs duties and non-discriminatory treatment of digital products, electronic signature and certification, and consumer protection in e-commerce chapter in current FTAs/RTAs to be emphasize the differences of each FTAs/RTAs.

(1) SCOPE

(a) Technological neutrality in services provided electronically

Based on the principle of technological neutrality, the regulations concerning trade in services should be neutral about the technical methods to provide the service. With regard to electronic commerce, this provision confirms that regulation of trade in services shall be equally applicable to services provided electronically and non-electronically.

(b) Clearly stipulating items exempt from the application of the regulation

Sensitive items can exempt either from the whole chapter on electronic commerce or from individual regulations. Such exemptions may include domestic taxation, subsidies and government procurement, broadcasting and audiovisual services, general exceptions and exceptional measures relating to security in GATT and GATS, and measures concerning regulatory inconsistencies in investment services (so-called “non-conforming” measures).

(2) PROVISIONS CONCERNING CONSISTENCY WITH OTHER REGULATIONS

Adjustments are made in the form of "do not apply to the extent of inconsistency with..." when other chapters, such as chapters of trade in goods, trade in services, investment and intellectual property rights, are applicable.

(3) NON-DISCRIMINATORY TREATMENT OF DIGITAL PRODUCTS

The classification of digital content in the WTO has become deadlocked, however, the EPAs/FTAs define digital content as “digital products” and set forth the details of national treatment and most-favoured-nation treatment in relation to such products.

(a) The definition of digital products

Digital products were defined in the US-Singapore FTA as “computer programs, text, video, images, sound recordings and other products that are digitally encoded”. This definition is applied in most of the EPAs/FTAs defining digital products.

However, some definitions say “regardless of whether they are fixed on a carrier medium or transmitted electronically”, and others say “not including ones that are fixed on a carrier medium”.

(b) National treatment

This is the stipulation that there will be no discrimination between domestic and foreign with regard to the country of origin or nationality of the manufacturer, etc. of digital products; this is the same concept as the national treatment concept in trade in goods and services.

(c) Most-favoured-nation treatment

This is the same concept as the most-favoured-nation treatment concept in trade in goods and services, and stipulates that there will be no discrimination against non-signatory countries with regard to the country of origin or nationality of the manufacturer, etc. of digital products.

(4) CUSTOMS

The moratorium on the imposition of customs duties has continued since the 2nd WTO Ministerial Meeting in 1998, right up to the present day; this is given substance in bilateral agreements as a permanent regulation that is legally binding.

However, with regard to the fine points of the provision, there are two models: the United States model, which states that “apart from domestic taxes, tariffs, fees or other levies” shall not be imposed “in relation to the import or export of digital products”, regardless of whether data is fixed on CD, DVD, or other media, or transmitted electronically; and the Australian model, which adopts the WTO moratorium wording and states that “the Parties shall maintain the current practice of not imposing custom duties on electronic transmissions between the Parties.”

(5) SOURCE CODE

In the past, measures requiring access to the source code of the software embedded in devices had been adopted/discussed in China and India. There have been requests by other countries at the WTO to review these measures.

While protectionist policies were observed in some countries, such regulations may possibly be implemented by some country in the future under domestic industry promotion policies and other economic policies, etc. This situation can be a potential concern for ICT device manufacturers, service providers, and investors in the area. In order to prevent such requirements from being made, source code provisions require the government not to request transfer and disclosure of source code as a condition for import or sale of software or devices with embedded software. This provision was provided for the first time among EPAs concluded by Japan in in the Japan-Mongolia EPA (in the chapter on Electronic Commerce) and TPP, CPTPP and Japan-EUEPA also contains similar provision.

(6) PROHIBITION ON REQUIREMENT CONCERNING THE LOCATION OF COMPUTINGFACILITIES

For businesses providing so-called cloud computing services, requirements to locate their servers and data centers in that country can be a disrupting factor for the optimal global deployment of their facilities. In addition, companies using these services and seeking overseas business development with global service providers as partners must bear unnecessary costs if they are required to use domestic servers from the overseas sites. This provision prohibits, in principle, contracting parties from making such requirements. In consideration of the electronic commerce market that has been rapidly developing and expanding in recent years and the needs for creating new rules, this provision was provided for the first time among EPAs concluded by Japan in the Japan-Mongolia EPA (in the chapter on Electronic Commerce) and TPP and CPTPP also contains similar provision.

Additionally, the Japan-Mongolia EPA and the TPP and CPTPP provide that it shall be permitted to adopt and maintain an inconsistent measure under certain circumstances in order to achieve a legitimate public policy objective.

(7) CROSS-BORDER TRANSFER OF INFORMATION VIA ELECTRONIC MEANS

This rule states that each contracting party shall allow cross-border transfer of information (including personal information) by electronic means if such transfer is for business purposes.

Inclusion of this rule in the TPP was the first time in any EPA signed by Japan.

Additionally, the TPP and CPTPP provides that a contracting party shall be permitted to adopt and maintain an inconsistent measure under certain circumstances in order to achieve a legitimate public policy objective.

(8) DOMESTIC REGULATIONS

This provision clearly stipulates the basic principle of industry-led development of electronic commerce and minimization of regulatory burdens, and adopts wording similar to the UNCITRAL model law on electronic commerce, the APEC model measures, and clauses on national regulations in GATS Article VI.

(9) ELECTRONIC SIGNATURES AND AUTHENTICATION SERVICES

In general, this provision includes the pursuit of interoperability with regard to electronic certificates that use Public Key Infrastructure (PKI), mutual recognition

between signatories of electronic certificates, particularly those issued by governments in relation to administrative services, guarantee of equivalence between conventional signature and electronic signature, assurance of technological neutrality on the choice of means of signature, and the prevention of legislation that hinders the opportunity for a party to an agreement to testify in court regarding the compliance of electronic commerce with the law.

Bilateral discussions on interoperability and mutual recognition tend to be difficult when the two countries have different definitions of electronic signature under their own domestic laws.

(10) PAPERLESS TRADE ADMINISTRATION

These regulations stipulate that trade administration documents, from certificates of origin to documents for customs, quarantine, and entry, should be in a form that can be used publicly in an electronic format, and that governments should accept trade administration documents submitted electronically as being legally equivalent to those submitted as paper documents.

In some cases, these provisions are set forth as a legal obligation which does not apply where there are requirements under existing domestic or international laws, or cases in which computerization would actually decrease the efficiency of trade administration.

(11) ONLINE CONSUMER PROTECTION

This provision reflects the principle regarding the adoption and maintenance by each country of measures relating to consumer protection set out in the 1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce. Some agreements also advocate cooperation between consumer protection groups, and contain measures against unsolicited E-mail and protection of privacy.

With regard to privacy, the two main documents are the 2005 APEC Privacy Framework and its forerunner, the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data; the main provisions in bilateral agreements advocate the necessity of protection and give consideration to international standards.

(12) PRIVATE SECTOR PARTICIPATION

This was originally formulated as a separate clause by Australia after summarizing the section that incorporated into bilateral agreements the principle that industry should take the initiative, which is contained in the Domestic Regulatory Framework in the APEC model measures.

In the Japan-Switzerland EPA, the provision advocating self-regulation by the private sector that was summarized as “cooperation” in the APEC model measures is contained in this clause.

(13) COOPERATION

This provision relates to the promotion of electronic commerce by small and medium-sized enterprises, the sharing of information concerning advanced technologies and business practices, and active participation in discussions in international forums that are incorporated into the APEC Blueprint for Action on Electronic Commerce.

1.2.2 Assessment on CHAPTER ON ELECTRONIC COMMERCE IN bilateral trade agreements among APEC economies

We overviewed the relevant provisions of e-commerce in major FTAs / EPAs above. Here, in order to analyze how the above general global trends are introduced in the APEC region, we investigated the main provisions of the bilateral agreements within the APEC region, which have been concluded since the 2000s. According to our research, 26 bilateral agreements including the e-commerce chapter have been signed within the APEC region until 2020. The contents of the e-commerce chapter are very wide, and we divide these e-commerce provisions into following three parts, rules that have received general understanding which are widely accepted within the APEC region and thus a starting point for future regional rules (mainly covered by 50% or more agreements), rules that have received a certain degree of acceptance (10 to 50%), and rules that only a small number of agreements prescribed (less than 10%).

Widely Accepted Rules (covered by 50% or more agreements)

（1）Paperless Trading

It is a provision prescribing that each Contracting Party shall endeavor to make

trade administration documents paperless and cooperate in trade transactions in electronic form. This provision is included in all FTAs / EPAs that Australia, Canada, China, Taiwan and Thailand have concluded with the APEC economy, and in these countries this provision seems to be the core rule of e-commerce.

Other countries have different regulations depending on the other party, and there seems to be no tendency.

（2）Customs Duties

It is a Provision prescribing that each Contracting Party shall not impose customs duties on electronic transmissions. This provision is included in all FTAs / EPAs that Canada, China, Taiwan and Thailand have concluded with the APEC economy, and in these countries this provision seems to be the core rule of e-commerce. Other countries have different regulations depending on the other party, and there seems to be no tendency.

（3）Personal Information Protection

It is a Provision prescribing that each Contracting Party shall protect the personal information of individuals engaged or involved in digital trade. This provision is included in all FTAs / EPAs that Canada, China and Thailand have concluded with the APEC economy, and in these countries this provision seems to be the core rule of e-commerce. Other countries have different regulations depending on the other party, and there seems to be no tendency.

（4）Online Consumer Protection

It is a provision prescribing that each Contracting Party shall protect consumers in electronic commerce.

The provisions included in agreements signed by Australia are often more detailed than those concluded by other countries.

This provision is included in all FTAs / EPAs that Australia, Canada and Thailand have concluded with the APEC economy, and in these countries this provision seems to be the core rule of e-commerce. Other countries have different regulations depending on the other party, and there seems to be no tendency.

（5）Electronic Authentication and Electronic Signatures

It is a provision prescribing that each Contracting Party shall not deny the legal validity of electronic authentication and signatures, and stipulating the legal

validity of electronic authentication and signatures, which are the basis of electronic commerce.

This provision is included in all FTAs / EPAs that Australia and China have concluded with the APEC economy, but other countries are unlikely to have any particular tendencies.

Rules with Certain degree of acceptance (10 to 50%)

（6）Domestic Electronic Transactions Framework

It is a provision prescribing that each Contracting Party shall maintain domestic legal framework governing the electronic transactions consistent with the principles of such as the UNCITRAL Model Law on Electronic Commerce 1996, not impose excessive burdens on e-commerce, and support the technological development of e-commerce.

This provision is included in most of the agreements signed by Australia, but not included in any of the agreements signed by the United States (not included in the Australia-US FTA). There are three agreements including this provision which Australia is not a party : NZ / Thailand CEPA, South Korea / Vietnam FTA, and China / Singapore FTA. The United States may be critical of this provision, as it has the effect of constraining the regulatory powers of each country.

（7）Non-Discriminatory Treatment of Digital Products

It is a provision prescribing that No Party shall accord less favorable treatment to digital products produced in the territory of the other party.

Countries that have a large export of digital products, such as Australia, the United States, Taiwan, and Singapore, signed agreements that include this provision.

（8）Cross-Border Transfer of Information by Electronic Means

This is a provision prescribing that each Contracting Party shall not prohibit the cross-border transfer of information, including personal information, by electronic means. This provision is included in some of the agreements signed by Australia, and is included in the US-Korea FTA in agreements where Australia is not a party. Australia has signed agreements including this provision with Singapore and Hong Kong, which appear to be strong in the digital field, but also includes Indonesia

and Peru (the Peru-Australia FTA was signed in 2020 and is the newest agreement). After 2011, there has been no increase in the number of agreements including this provision.

The Australian-style provisions include such statement that each Contracting Parties can impose restrictions on the transfer of information by electronic means, but the US-Korea FTA prescribes that each Contracting Party "shall endeavor to refrain from imposing or maintaining unnecessary regulations".

（9）Location of Computing Facilities

It is a provision prescribing that each Contracting Party shall not require covered person to locate computing facilities in that Party's territory, and prohibiting so-called localization measures. We will discuss about this provision in detail in 1.3.

This provision is included in some of the agreements signed by Australia (with Singapore, Hong Kong, Indonesia, Peru).

（１０）Cybersecurity Cooperation

It is a provision prescribing that each Contracting Party recognizes the importance of cyber security and maintains a cooperative system. It is included in the Singapore-Australia FTA (2003), Singapore-Taiwan EPA (2014), and Australia-Peru FTA (2020). Since the number of agreements that include this provision is small, it cannot be said that the number of agreements that include this provision has increased after 2011.

（１１）Unsolicited Commercial Electronic Messages

It is a provision prescribing that each Contracting Party shall adopt and maintain measures to deal with unsolicited commercial electronic messages in order to protect consumers from unsolicited commercial electronic messages. This provision is included in the agreements signed by Australia of which the partner countries are Singapore, Hong Kong, Malaysia, South Korea, Indonesia and Peru.

（１２）Principles on Access to and Use of the Internet

It is a provision prescribing that each Contracting Party shall allow consumers in their own territory to access necessary information, devices, and the Internet, etc.

This provision is included in the Singapore-Australia FTA, the US-Korea FTA, and the Australia-Peru FTA.

（１３）Objectives

It is a provision concerning the purpose of the agreement. The content of the purpose depends on the agreement, but the purpose of promoting electronic commerce is always included. It is included in the Malaysia-Australia FTA, NZ-Taiwan EPA, Korea-Australia FTA, and Australia-China FTA.

（１４）Consultations

This is a provision prescribing that Contracting Parties will consult when problems arise with electronic commerce or at the request of the Contracting Parties. It is included in the Australia-Chile FTA, NZ-Hong Kong CEPA, and NZ-Taiwan EPA.

（１５）Cooperation

It is a provision on what should be cooperated between the Parties. The content of cooperation depends on the agreement. It is included in some of the agreements signed by Australia and all of the FTAs and EPAs signed by Thailand, Canada and China with APEC economy.

（１６）Source Code

It is a provision that each Contracting Parties shall not require the transfer of or access to the source code of software owned by a person of another Party as a condition for the import or use of software or products.

（１７）Non-application of Dispute Settlement Provisions

It is a provision prescribing that the provisions of the Dispute Settlement Chapter do not apply to the provisions of the Electronic Commerce Chapter. This provision is included in some of the agreement signed by China and all of the FTAs and EPAs that Thailand and NZ have signed with APEC economy.

（１８）Electronic Supply of Services

It is a provision prescribing that the Parties recognize that the supply of a service using electronic means falls within the scope of the obligations contained in the relevant provisions of the other Chapters (such as Investment, Cross-Border Trade in Services, Telecommunication, and Financial Services). This provision is included in all FTAs and EPAs that the United States has signed with

APEC economy, some of the agreements that South Korea and Australia have signed, and the Singapore-Taiwan EPA.

（１９）Transparency

It is a Provision prescribing that each Contracting Party shall ensure transparency in matters covered by the Electronic Commerce Chapter. There is no national trend.

（２０）Relation to Other Chapters

It is a provision prescribing that in the event of an inconsistency between this Chapter and another Chapter, the other Chapter shall prevail to the extent of the inconsistency. This provision is included in some of the agreements that Canada, South Korea and Peru have signed with other APEC economy.

（２１）Digital Products

This provision has the similar content to Customs Duties provision prescribing that each Contracting Party shall not impose customs duties on digital products. There is no Customs Duties provision in agreements which has this provision. This Provision is included in some of the agreement signed by South Korea and the United States.

Rules only a small number of agreements prescribed (less than 10%)

（２２）Electronic Invoicing

It is a provision prescribing that each Contracting Party recognizes the benefit of electronic invoicing and promotes its use. This provision is included only in Singapore-Australia FTA.

（２３）Express Shipments

This is a provision prescribing that each Contracting Party provides for accelerated customary procedures to facilitate express shipments. This provision is included only in Singapore-Australia FTA.

（２４）Electronic Payments

This is a provision prescribing that each Contracting Party supports the

promotion of electronic payments. This provision is included only in Singapore-Australia FTA.

（２５）Information and Communication Technology Products that Use Cryptography

This is provision prescribing that a Party shall not require a manufacturer or supplier of a commercial ICT product that uses cryptography, as a condition of the manufacture, sale, distribution, import or use of the commercial

ICT product, to transfer or provide access to any technological information, partner or otherwise cooperate with a person in the territory of that Party, and use or integrate a particular cryptographic algorithm or cipher. This provision is included only in Singapore-Australia FTA.

（２６）Digital Identities

This is a provision prescribing that each Contracting Party shall endeavor to align policies on digital identity with the other Party. This provision is included only in Singapore-Australia FTA.

（２７）Artificial Intelligence

This is a provision prescribing that each Contracting Party cooperates in using Artificial Intelligence technology in accordance with its own policy. This provision is included only in Singapore-Australia FTA.

（２８）Cooperation on Competition Policy

This is a provision prescribing that each Contracting Party cooperates with the other Party on competition policy. This provision is included only in Singapore-Australia FTA.

（２９）Data Innovation

This is a provision prescribing that a Party supports Data Innovations. This provision is included only in Singapore-Australia FTA.

（３０）Open Government Data

This is a provision prescribing that to the extent that a Party chooses to make government information available to the public, it shall endeavor to ensure that

the government information is in a machine-readable and open format and the Parties shall endeavor to cooperate to identify ways in which each Party can expand access to and use of government information that the Party has made public. This provision is included only in Singapore-Australia FTA.

（３１）Small and Medium Enterprises

This is a provision prescribing that the Parties recognize the fundamental role of SMEs in competitiveness in the digital economy, and with a view towards enhancing trade and investment opportunities for SMEs in the digital economy, the Parties shall endeavor to make information publicly available and cooperate with other Parties. This provision is included only in Singapore-Australia FTA.

（３２）Internet Interconnection Charge Sharing

This is a provision prescribing that each Party recognizes that a supplier seeking international Internet connection should be able to negotiate with suppliers of the other Party on a commercial basis. This provision is included only in Singapore-Australia FTA.

（３３）Location of Financial Service Computing Facilities for Covered Financial Service Suppliers

This is a provision prescribing that neither Party shall require a covered financial person to use or locate computing facilities in the Party’s territory as a condition for conducting business in that territory. This provision is included in Singapore-Australia FTA and Australia-Hong Kong FTA. There are differences in whether or not the terms are defined, but the specific obligations are the same.

（３４）Disclosure of Information

This is a provision prescribing that nothing in this Chapter shall require a Party to furnish or allow access to confidential information, the disclosure of which would be contrary to its law, impede law enforcement, or otherwise be contrary to the public interest, or which would prejudice legitimate commercial interests of particular enterprises, public or private. This provision is included only in Singapore-Australia FTA.

（３５）Creating a Safe Online Environment

This is a provision prescribing that the Parties shall create and promote a safe

online environment where users are protected from harmful content, and work together and within international fora to create a safe online environment. This provision is included only in Singapore-Australia FTA.

（３６）Submarine Telecommunications Cable Systems

This is a provision prescribing that each Party shall endeavor to ensure that, to the extent possible, a person of the other Party who operates, owns or controls submarine telecommunications cable systems has flexibility to choose suppliers of installation, maintenance or repair services, and specifying the conditions when a person from either Party or a non-Party operates these services, and in case of a problem, the Parties shall consult. This provision is included only in Singapore-Australia FTA.

（３７）Standards and Conformity Assessment for Digital Trade

This is a provision prescribing that where it is appropriate, the Parties should actively participate in the work of relevant regional and international bodies relating to the development and adoption of standards that support digital trade and endeavor to share experience and views. This provision is included only in Singapore-Australia FTA.

（３８）FinTech and RegTech Cooperation

This is a provision prescribing that the Parties shall cooperate in FinTech and RegTech. This provision is included only in Singapore-Australia FTA.

（３９）Stakeholder Engagement

This is a provision prescribing that the Parties shall seek opportunities to convene a Digital Economy Dialogue (the “Dialogue”) at times agreeable to the Parties, to promote the benefits of the digital economy, and where appropriate, and as may be agreed by the Parties, the Dialogue may include participation from other interested stakeholders, such as researchers, academics, industry and other stakeholders. This provision is included only in Singapore-Australia FTA.

（４０）Capacity Building

This is a provision prescribing that the Parties shall cooperate in capacity building. This provision is included only in Singapore-Australia FTA.

（４１）Review

This is a provision prescribing that in any review of this Agreement, conducted in accordance with Article 17.7 (Final Provisions), the Parties shall consider discussing appropriate amendments to this Chapter. This provision is included only in Singapore-Australia FTA.

（４２）Promotion of E-Commerce

This is a provision prescribing that the Parties shall cooperate in promoting the use of E-Commerce, promoting the efficient functioning of E-Commerce in its own country and the international community, and establishing a predictable and simple legal environment for E-Commerce. This provision is included in the NZ-Hong Kong CEPA and the NZ-Taiwan EPA.

（４３）E-Government Initiatives

This is a provision prescribing what the E-governmental initiatives shall persue. This provision is included only in NZ-Hong Kong CEPA.

（４４）Protection from Fraudulent and Deceptive Commercial Practices

This is a provision confirming the importance of maintaining and adopting transparent and effective means to protect consumers from malicious commercial practices when engaging in e-commerce. This provision is included only in Peru-Singapore FTA.

1.3 REGULATIONS CONCERNING DATA LOCALIZATION

In recent years, the principle of free cross-border information transfer has been confirmed in various EPAs/FTAs and at various international forums to promote global economic growth. On the other hand, some countries have introduced regulations to retain personal information and data important to the state within its territory (“data localization”) from the viewpoints of protection of individual human rights, protection of domestic industries, and national security.

In May 2020, Sidewalk, Google-affiliate urban innovation company, announced withdrawal of a smart city project in Toronto Canada and their statement stated that “unprecedented economic uncertainty has set in around the world and in the Toronto real estate market. We concluded that it no longer made sense to proceed with the Quayside project”. However, a news source named “Nypost” said that “the project has proved controversial for number of reasons including

the fact Sidewalk wanted to put data-collecting sensors around the city that it would oversee. The data collecting proposal was rejected". The project has been objected to the company's approach to privacy and intellectual property which collected by the project even there is no requirement of Data Localization in Canada.

This chapter compares and gives an overview of the cross-sectoral, general data regulations concerning data localization in the EU, China, Viet Nam, Indonesia, and Russia. Note that data localization regulations are also sometimes included in industry regulations, although these are not covered in this Column.

(1)COMPARISON OF REGULATIONS

As stated above, this Chapter compares the following data protection regulations as major examples and gives an overview of their purpose and content: [1] Regulation (EU) of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as the General Data Protection Regulation or GDPR); [2] Cybersecurity Law of China; [3] Cybersecurity Law of Viet Nam; [4] Republic of Indonesia Minister of Communications and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (hereinafter referred to as the "Personal Data Protection Regulation"); and [5] Russian Federal Law on Personal Data.

These data protection regulations will be compared in terms of the following two aspects: [i] restrictions on cross-border transfers of data existing in the country's territory; and [ii] obligation to retain data necessary to conduct business within the country's territory (data localization obligation).

Below, this Chapter summarizes the above regulations in terms of whether they impose restrictions on international data transfers and data localization obligations, and if applicable, the content of such restrictions.

(a) REGULATION ON CROSS-BORDER DATA TRANSFERS

The EU, China, Indonesia, and Russia all restrict the international transfer of personal information, etc. The differences among the regulations are summarized below. The cybersecurity law in China regulate a wider scope for cybersecurity purposes.

A.Basic Content of Regulation

While the EU GDPR guarantees the freedom of the transfer of personal information within the EU territory, it restricts transfer of such information to a third country.9 However, the purpose of such restriction by the EU is to protect personal information vis-à-vis a third country; thus, the GDPR provides that personal information can be transferred to a third country if said third country fulfills certain criteria, such the protection level of personal information.

The Chinese Cybersecurity Law is aimed at ensuring national security. In addition to personal information, it protects data closely related to national security, economic development, and social public interests. 10 This law includes restrictive measures against the provision of personal information and important data to a foreign third party, such as compulsory security assessment on cross-border data transfers.

B.Scope of Information Subject to Regulation

The scope of regulation in the EU, Indonesia, and Russia is limited to personal information.

Meanwhile, China also regulates the transfer of “important data,” in addition to personal information. “Important data” subject to the regulation in China is defined as data closely related to national security, economic development, or social public interests.11 Annex A of the Guidelines for Cross-Border Data Transfer Security Assessment (Draft) shows examples of important data in 27 sectors, including “oil and natural gas” and “communications.” These examples include an extensive range of items, from shipping slip data of post corporations to sampling information of mass-produced processed food products. Moreover, the law includes a bucket clause, which provides that important data is not limited to said 27 sectors but could also be data in other sectors. There is a concern that the transparency of the application of the law may not always be maintained.

C.Regulated Entities

Under the regulations in the EU, Indonesia, and Russia, persons managing personal information are subject to regulation.

Meanwhile, China regulates a wide scope of entities from the viewpoint of national security. The Chinese Cybersecurity Law includes persons

managing personal information as well as operators of critical information infrastructures, such as communications, financial, and medical institutions, in the scope of regulation. In addition, the draft Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data adds network operators in the scope as well.

However, the definition of “network operator” is not clearly stated. Such ambiguity raises a concern as to what kind of business operators are included into the scope.

D.Other Regulations

Generally, cross-border data transfer is allowed when one of the following grounds is met: [1] the individual concerned consents to the data transfer, or [2] the requirements of safety management measures are fulfilled. The latter case (requirements of safety management measures) is judged based on either the legal system of the transfer destination state or the attributes, etc. of the entity receiving the data. In addition to the above conditions, the Russian authority requires prior notification of cross-border data transfers scheduled, while the Indonesian authority imposes a reporting obligation. In addition to notification and reporting obligations, the Chinese Cybersecurity Law also imposes on network operators the obligation to provide technical support and cooperation for national security and crime investigations conducted by the national security authorities.

(b) DATA LOCALIZATION OBLIGATION

The regulations in China, Viet Nam, Indonesia and Russia include provisions concerning the obligation to store data within the territory of the nation (localization obligation), while the EU GDPR does not have such a provision. If a less advantageous treatment is accorded to foreign companies compared to domestic companies due to the localization requirement, it may constitute a violation against the principle of national treatment. In the course of formation of international rules on e-commerce, Japan has attached importance to securing the free transfer of information in principle and advocated for the observation of the non-discrimination principle, which is the fundamental principle of the WTO. In the context of data localization

obligations, it is also necessary to pay close attention to avoid excessive localization obligations from being introduced.

A.Scope of Subject Information

As with cross-border data transfer, Russia limits the scope of data localization obligation to personal information. Meanwhile, China, Indonesia, and Viet Nam also include certain data that is important to the nation in the scope of the data localization obligation, in addition to personal information.

B.Regulated Entities

While Russia regulates persons managing personal information, China, Indonesia, and Viet Nam regulate system providers managing important data. However, the scope of such system providers differs among countries: such providers are referred to as “operators of important information infrastructures” (China), “a company that provides services on communication networks, the Internet and additional services in cyberspace” (Viet Nam), and “electronic system providers for public services” (Indonesia). However, none of the scopes of these terms is clearly defined.

C.Other Regulations

China, Viet Nam, Indonesia and Russia impose obligations of domestic data storage regardless of whether the business operator is domestic or overseas. For overseas business operators, there might be some additional responsibilities associated with domestic data storage. These measures could result in a risk that the overseas business operators being treated at a substantial disadvantage over domestic operators.

1.4. Recent Legislative Activities among APEC Economies

In this part, with respect to laws or regulations in 1.3, we will analyze laws or regulations that will have a huge influence on cross-border data flows. Our study will focus on China, Russia and Vietnam respectively.

1.4.1 China

China's National Information Law broadly stipulates government activities (policy objectives) that allow government access, as well as government access authority and criminal penalties for non-cooperation.

Article 14 The state intelligence work organization shall carry out intelligence work according to law, and may require relevant organs, organizations and citizens to provide necessary support, assistance and cooperation.
Article 28 Whoever violates the provisions of this Law and obstructs the state intelligence work organization and its staff from carrying out intelligence work according to law shall be recommended by the state intelligence work agency to be dismissed by the relevant units or be warned by the state security organs or public security organs or below fifteen days. Detained; if it constitutes a crime, criminal responsibility shall be investigated according to law.

Article 2: National intelligence work adheres to the overall national security concept, provides intelligence reference for major national decisionmaking, provides intelligence support for preventing and defusing risks that endanger national security, and safeguards state power, sovereignty, unity and territorial integrity, people's well−being, and economic and social Sustainable development and other important national interests.

In addition, China's draft of the Personal Information Protection Law contains many provisions that affect cross-border data distribution, such as extraterritorial application and regulations on cross-border relocation.

Extraterritorial Application
Article 3: This Law applies to organizations and individuals' handling personal information activities of natural persons within the borders of the People's Republic of China.
Where one of the following circumstances is present in handling activities outside the borders of the People's Republic of China of personal information of natural persons within the borders of the People's Republic of China, this Law applies as well:
1. Where the purpose is to provide products or services to natural persons inside the borders;

2. Where conducting analysis or assessment of activities of natural persons inside the borders;
3. Other circumstances provided in laws or administrative regulations.

Article 52: Personal information handlers outside the borders of the People's Republic of China as provided in Article 3 Paragraph II of this Law shall establish a dedicated entity or appoint a representative within the borders of the People's Republic of China, to be responsible for matters related to the personal information they handle, and will report the name of the relevant entity or the name and contact method, etc., of the representative to the departments fulfilling personal information protection duties and responsibilities.

Chapter III: Regulations on the Cross-Border Provision of Personal Information
Article 38: Where personal information handlers need to provide personal information outside the borders of the People's Republic of China for business or other such requirements, they shall meet at least one of the following conditions:
1. Pass a security assessment organized by the State cybersecurity and informatization department according to Article 40 of this Law;
2. Undergo personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department;
3. Conclude an agreement with a foreign receiving party, agreeing on both sides' rights and obligations, and supervising their personal information handling activities' satisfaction of the personal information protection standards provided in this Law;
4. Other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department.
Article 39: Where personal information handlers provide personal information outside of the borders of the People's Republic of China, they shall notify the individual about the foreign receiving side's identity, contact method, handling purpose, handling methods, and personal information categories, as well as ways for individuals to exercise the rights provided in this Law with the foreign receiving side, and other such matters, and obtain individuals' separate consent.
Article 40: Critical information infrastructure operators and personal information handlers handling personal information reaching quantities provided by the State cybersecurity and informatization department shall store personal information

collected and produced within the borders of the People's Republic of China domestically. Where they need to provide it abroad, they shall pass a security assessment organized by the State cybersecurity and informatization department; where laws or administrative regulations and State cybersecurity and informatization department provisions permit that security assessment not be conducted, those provisions are followed.
Article 41: Where it is necessary to provide personal information outside of the borders of the People's Republic of China for international judicial assistance or administrative law enforcement assistance, an application shall be filed with the relevant competent department for approval according to the law.
Where the People's Republic of China has concluded or participates in international treaties or agreements that contain provisions concerning providing personal information outside of the borders of the People's Republic of China, those provisions are followed.
Article 42: Where foreign organizations or individuals engage in personal information handling acts harming personal information rights and interests of citizens of the People's Republic of China, or harming the national security or public interest of the People's Republic of China, the State cybersecurity and informatization department may put them on a list limiting or prohibiting personal information provision, issue a warning, and adopt measures such as limiting or prohibiting the provision of personal information to them, etc.

Article 43: Where any country or region adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China in the area of personal information protection, the People's Republic of China may adopt retaliatory measures against said country or region on the basis of actual circumstances.

1.4.2 Russia

In Russia, amendments to the Personal Information Protection Law require that the personal data of Russian citizens be stored domestically (so-called localization measures, but it is possible to store them in parallel on overseas servers). And for the breach of this duty, this law stipulate sanctions including blocking the offender from the Russian Internet.

The Sovereign Internet Law was enacted in November 2019. Under the law, in Russia, it is obligatory for ISPs and others to install equipment that assists

government censorship, and all packets are subject to government surveillance, that is, GA.

Under this law, it is obligatory to install facilities that enable DPI (Deep Packet Inspection), which allows all Russian ISPs to obtain information including the contents of packets for traffic monitoring on the Internet by the government in order to protect the security of the Internet.

This law also allows the government to limit the points at which Russian ISPs connect to the international Internet, and it enables blocking the Russian Internet from the global Internet (although its effectiveness is questionable).

The above-mentioned obligation to localize under the Russian Personal Information Protection Law includes a penalty for blocking the Internet connection, and in fact (although it was the case before the enactment of the law), the US SNS site LinkedIn has had its website blocked for violating the obligation.

The Kremlin says it has access to all the information on the Internet obtained by DPI and can block the access to the Internet in Russia from abroad if the Internet is at risk.

In this way, it can be pointed out that the law may function as a basis for information activities in Russia. Internet traffic is analyzed through this law, which may be used to implement the various listed GAs.

1.4.3 Vietnam

In Vietnam, there is no general privacy law applicable to every industrial sector and privacy protections are stipulated in regulations or other detailed guidelines stipulated by each Ministry. However, on December of 2019, first general privacy regulation in Vietnam, Summary of Draft Decree on Personal Data Protection was published. On February 2021, the text of the draft decree officially published by Ministry of Public Security for public consultation.

This draft decree have wide range of articles on privacy protection, such as definition of personal data, legal basis for personal data processing and establishment of Personal Data Protection Committee, it is worth noted that it contains restriction of transfer of personal data to outside of Vietnam. Namely, Art. 21 (1) of the draft decree stipulates that requirements for cross-border data transfer include;

(i) the consent of the data subject;

(ii) the original data is stored in Vietnam;
(iii) there is written evidence that the jurisdiction where the data is received offers the same or higher level of data protection compared to Vietnam; and
(iv) the Personal Data Protection Committee has issued a written approval for the transfer.

Requirement (ii) is especially important as original data must be stored in Vietnam and this is clearly a new localization measure. Compare to GDPR and Personal Information Protection Act of Japan, that do not require original data storage in their territories, it might be considered excessive requirement especially for foreign countries doing business in Vietnam.

1.5. Overall analysis on stocktaking

From the above analysis, we will analyze the implications for rule formation in the field of Electronic Commerce in APEC. In particular, we analyze how many rules have already been accepted in each APEC economy, and on the other hand, what are necessary for the future rules formation in the APEC region, using advanced rules as benchmarks, although they are not sufficiently widespread.

1.5.1 Provisions that widely accepted among APEC economies

First, in the APEC region, it can be said that there are widespread acceptance on two rules, especially (1) provisions that facilitate trade in electronic goods and services, and (2) provisions related to institutional development aimed at revitalizing domestic electronic commerce. This specifically refers to the following five rules.

Paperless Trading stipulates that trade in goods by electronic means, and Customs Duties stipulates that no customs duties shall be imposed on the electronic exchange of digital products and services, that is, trade in services. Through these provisions, electronic trades in services and goods are facilitated, and trade costs can be further reduced.

- Paperless Trading
- Customs Duties

Next, Electronic Authentication and Electronic Signatures provide institutional infrastructure such as legal validity regarding the usefulness of electronic contracts

within Contracting Parties, and Personal Information Protection and Online Consumer Protection provide consumer privacy and contract protection in online transactions. It can be said that these provisions establishes a foundation that enables the activation of electronic commerce.

It can be analyzed that such provisions aim to expand the e-commerce market itself by establishing an institutional foundation for establishing the e-commerce market in the partner country of the agreement.

- Electronic Authentication and Electronic Signatures
- Personal Information Protection
- Online Consumer Protection

1.5.2 Provisions accepted to some extent in agreements between APEC economies

As regulations that have been accepted to some extent among the APEC economies, the ones that are particularly important for cross-border data distributions are (1) prohibition of location of computing facilities requests, (2) prohibition of source code disclosure requests, and (3) free flow of data. These are stipulated in the CPTPP, USMCA, etc., and are also included in multiple bilateral agreements concluded by CPTPP member countries. For example, Indonesia, which is not a CPTPP member country, accepts the free flow of data.

In addition, there is the Domestic Electronic Transactions Framework as a provision that is classified into the institutional foundation described in 1.5.1. It promises to adopt domestic regulations on e-commerce in accordance with international rules such as UNCITRAL Model Law on Electronic Commerce 1996, not to impose an excessive burden on e-commerce, and to support the technological development of e-commerce. It is a regulation that forms an important institutional foundation for electronic commerce.

1.5.3 Sprouting provisions in agreements among APEC economies

The characteristic features of the sprouting provisions are that they are concerning cooperation to promote the digital economy rather than legal obligations, and especially the Singapore-Australia FTA includes many advanced provisions that are also adopted by the DEPA.

This is, for example, a provision that stipulates cooperation on digital identity, Fintech / Regtech, AI, etc., and since agreements that include these provisions have been concluded in recent years, not necessarily a specific progress in digital economy has been made by these provisions. However, such basic cooperative relationships are important for the expansion of cross-border digital transactions and the expansion of the digital economy based on them, and it is considered important to promote such cooperation agreements and the organizational foundations for promoting them (for example, the establishment of committees) as the basis for advancing the movement toward policy coordination and harmonization of standards and regulations.

In addition, the promotion of open data is a sprouting regulation, which is included in the USMCA and the Singapore-Australia FTA. Private use of government-owned data is extremely important in data use, and discrimination in data provision to foreign companies can occur, so it is necessary to stipulate non-discrimination inside and outside the country.

Chapter 2: Assess digital trade and e-commerce related initiatives in APEC (CTI, DESG, TEL, including the APEC Internet and Digital Economy Roadmap, APEC Cross-Border E-Commerce Facilitation Framework, etc.) and initiatives in other international fora including the WTO.

2.1 E-commerce related initiatives in APEC

The Leader's Declaration as "A Vision for the 21st Century" (1997) and the "Blueprint for Action on Electronic Commerce (1998)" recognized the large potential and importance of electronic commerce. In 1999, the ECSG (Electronic Commerce Steering Group) was established as an APEC Senior Officials' Special Task Force. Data privacy and paperless trade have been discussed and a model of electronic commerce chapter has been formulated for EPA/FTAs. Going forward, it has been decided that the ESCG was reorganized into the Digital Economy Steering Group (DESG).

(a) Data privacy

With the aim of promoting consistent information privacy protection measures in APEC member countries, in order to prevent flows of information relating to trade between member countries being hindered unnecessarily, the APEC Privacy Framework was adopted at the APEC Leaders' Summit held in November 2005. This framework itself acknowledged that it is fundamentally consistent with the 1980 OECD Guidelines, with new provisions to prevent tangible harms to individuals. Furthermore, based on the Framework, the development of the Cross-border Privacy Rules (CBPRs) proceeded as a rule for organizations handling personal information across borders.

Based on the APEC Data Privacy Pathfinder adopted in 2007 by both the APEC Ministers' Meeting and the APEC Leaders' Summit, the Pathfinder project, which began in 2008, involves discussions aimed at the formulation of documents such as self-assessment guidelines for businesses and the Cross-border Privacy Enforcement Agreement (CPEA).

The main document of the CBPR was approved at the Ministerial Meeting held in November 2011. In January 2014, the Common Referential for the Structure of the EU System of Binding Corporate Rules and APEC Cross Border Privacy Rules System was completed. Its objective was promoting interoperability of information distribution systems between APEC and the EU. Moreover, the updating of the APEC Privacy Framework was promoted. At the

Ministerial Meeting in November 2016, the APEC Privacy Framework 2015 was approved.

As of July 2020, the CBPR system is participated in by United States, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Chinese Taipei, and the Philippines. Accountability Agents review companies' cross-border data protection systems and certify their compliance with the APEC Data Privacy Pathfinder. So far, 4 institutions in United States, each one institution in Japan, The Republic of Korea and Singapore have been recognized by the ECSG and started their service as Accountability Agents. These institutions have given certification to 35 companies, respectively.

Although CBPR is a voluntary, accountability based system, number of participated economies and certificated companies seems not enough to achieve objectives of CBPR to facilitate cross boarder flow of personal information. Most of economies who answered the survey recognized that the CBPR system is an important framework for cross boarder data flow while there are currently no global rules to facilitate cross boarder data flow.

(b) Paperless trade

Based on the Strategies and Actions toward a Cross-border Paperless Trading Environment approved at the sixteenth APEC Ministerial Meeting (November 2004), work that will facilitate the electronic transmission of trade-related information (electronic certificate of origin, electronic invoice, electronic documents and electronic trade financing) within the APEC region by 2020 is underway.

2.2 Discussion Within Major International Organizations

There have been ongoing discussions on e-commerce at the WTO since the formulation of a Work Programme in 1998. With the fourth industrial revolution and technological advancement and expansion of cross-border business, the awareness for the necessity of international rules on e-commerce has been particularly heightened in recent years. Rules on e-commerce listed below are also being discussed under various international frameworks other than the WTO, such as G7, G20 and OECD as follows.

Figure 4: Rules on e-commerce

Category	Elements
Facilitation	Electronic signatures and authentications
	Electronic documentation of trade documents (paperless trading)
	Electronic Payment
Liberalization	Non-imposition of customs duties on electronic transmissions
	Principle on access and use of the Internet
	Non-discriminatory treatment of digital products
	Cross-border transfer of information by electronic means
	Location of computing facilities
Trust	Online consumer protection
	Unsolicited commercial e-mail (spam)
	Protection of personal information (privacy)
	Protection of important information such as trade secrets, including source codes
Cooperation	Publication and exchange of information on regulatory measures and procedures
	Technical assistance and capacity building

(1) WTO

E-commerce has prompted WTO discussions regarding its relationship with existing WTO agreements because it is a new form of trade that frequently involves cross-border transactions.

Specific areas being discussed with respect to e-commerce are as follows.

(a)DIGITAL CONTENT UNDER CURRENT WTO AGREEMENTS

Agreements E-commerce has brought substantial changes to the distribution structures for goods and services, but consensus has not been reached yet as to the concept of e-commerce and how to regulate this type of transaction within the context of the WTO.

The issue of classification of digital contents has been discussed for years. Depending on whether consideration for exchanged digital contents are classified, whether as goods prices, services fees, or fees relating intellectual property rights, the rules that apply regulating the digital contents differ. It also has been pointed out that trade distorting effects may occur if there is discriminatory treatment between physical distribution and network distribution.

The EU asserts that provision of digital contents is a service activity and should be disciplined only by the GATS. It also asserts that, from the standpoint of technical neutrality, digital contents should not be treated differently depending on whether they are provided through broadcasting services or through electronic commerce.

Japan's position is that where recording and cross-border transactions of digital contents through carrier media, fall within the coverage of GATT disciplines, it is appropriate that the same digital contents transmitted through the Internet should also be granted unconditional application of MFN and national treatment as under the GATT. The U.S. similarly argues that the discussion regarding digital contents should not be limited to discussions on whether digital contents should be regulated under the GATT or the GATS. Rather, it is essential to keep in mind that the discussion contributes to develop electronic commerce and that the disciplines on digital content should not reduce the level of market access currently enjoyed.

Although the concepts of digital contents still need to be examined, it is essential to assure basic WTO principles, such as most-favoured-nation and national treatment, to apply to digital contents in order to foster the growth of e-commerce.

(b)CUSTOM DUTIES ON ELECTRONIC TRANSMISSIONS

Digital content that used to be delivered physically, for example on floppy disks and CD-ROMs, is increasingly being delivered on-line. The main problem in attempting to tax these transactions is that it is almost impossible for customs agencies to capture them. If one attempts to tax electronic transmission of digital contents (for example, capturing the transmission log) as a substitute, one runs the risk of imposing taxes far in excess of or short of the value of the content because the value of digital content itself is not always proportionate to the transmission volume.

In addition to these technical difficulties in collecting customs duties on electronic transmissions, there is also the need to ensure a free trading environment to foster the growth of e-commerce. This has led many to support the establishment of an international agreement not to impose customs duties on on-line transactions.

At the Second WTO Ministerial Conference in 1998, Members agreed to a "Ministerial Declaration on Global Electronic Commerce" that promised to maintain the current practice of not imposing customs duties on electronic transmissions until the next Ministerial Conference (1999) (moratorium on payment of customs duties). However, when physical goods are moved along with e-commerce transactions, tariffs apply as with ordinary transactions.

The impasse at the Third Ministerial Conference in 1999 delayed agreement on the handling of the moratorium on payment of customs duties. The Fourth Ministerial Conference in Doha, Qatar in November 2001, however, officially announced that the moratorium would be extended until the Fifth Ministerial Conference. Although the September, 2003 Fifth Ministerial Conference in Cancun collapsed and the taxation moratorium was not extended, Members agreed in the General Council at the end of July 2004 that the moratorium would be extended until the Ministerial Conference in Hong Kong scheduled for the end of 2005. Afterward, Members agreed to extend the moratorium until the next Ministerial Conference, at the Sixth WTO Ministerial Conference in Hong Kong (December 2005), the Seventh Ministerial Conference (December 2009), the Eighth Ministerial Conference (December 2011), the Ninth Ministerial Conference (December 2013), the Tenth Ministerial Conference (December 2015) and the 11th Ministerial Conference (December 2017).

(c) FISCAL IMPLICATIONS OF E-COMMERCE

It is difficult in electronic commerce to identify where production and consummation were undertaken. This raises the question of how to harmonize the traditional concept of state taxation and its practices. Developing countries have expressed concern that the expansion of e- commerce will lead to a reduction in state tax revenues. In order to convince developing countries otherwise, it is necessary to study the positive effects that the promotion of e-commerce will have on national economies as a whole and on the negative impacts that may be seen in state tax revenues.

(2) OECD

The OECD guidelines have been incorporated into EPAs/FTAs. The OECD Action Plan for Electronic Commerce was adopted in the OECD Ministerial Conference on Electronic Commerce (October 1998). It contains the four principles mentioned below.

(a) Building trust with users and consumers

The main activities that are derived from this principle are consumer protection, privacy protection, and information security and authentication. In particular, with regard to consumer protection, the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce was published (1999; amended in 2016). This document sets forth eight principles: “transparent, effective consumer protection”; “fair sales, advertising and marketing behavior”; “online information disclosure”; “verification processes”; “payment”; “conflict resolution and redress”; “privacy protection”; and “education and publicity”. In addition to the aforementioned eight basic principles, the OECD is recommending and proposing the implementation of guidelines and global cooperation. In particular, in 2003, the OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practice Across Borders were established, giving more concrete form to part of the aforementioned principle of “fair sales, advertising and marketing behavior”.

At the same time, the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, which was enacted in September 1980, is the cornerstone of privacy protection, and, through their implementation, the OECD is promoting activities such as the technological verification of improved privacy protection and increased user awareness. The Guidelines were revised in 2013.

In the ongoing discussion on the revision of the privacy guidelines, the Committee on Digital Economy Policy (CDEP) and DGP's Trusted Government Access (TGA) have been discussed since 2020 under the leadership of the Government of Japan. A drafting committee is expected to be established in 2021.

The DGP states that discussions on TGA require urgent international discussion for the following reasons: DGP regards unconstrained and disproportionate government access to personal data as an important issue

for data governance and privacy, and a potential barrier to reliable and free data flow.

Given the globally interdependent nature of the digital economy, the DGP fears that access to unrestricted, irrational or non-proportional government-enforced access to privately-owned personal data will undermine credibility and data flow, and says that it can have an economic impact due to the restrictions on the data flow.

As DGP's response to the above problems, it takes an approach to first understand the current TGA practices of OECD countries and then explore high-level principles and policy guidance. Here, the aim is to harmonize national security and rights protection, and in particular, safeguards on the following matters are discussed;

Legal basis; justification, necessity or proportion, transparency, prior permission or restriction; Restrictions on the handling of personal data obtained (including restrictions on confidentiality, integrity, availability); Independent Audits and effective remedies

For the above purposes, CDEP has agreed to set up a drafting committee consisted of government representatives and experts, including law enforcement and intelligence agencies. The Drafting Committee will be active in early 2021 and will work with other OECD related committees to formulate recommendations for the CDEP.

Finally, with regard to information security and authentication, the OECD Guidelines on Security of Information Systems were formulated in 1992, while in 1997, the Guidelines on Cryptography Policy were enacted. The former were revised in 2002 as the Guideline for the Security of Information Systems and Networks, and then further revised in September 2015 as the Digital Security Risk Management for Economic and Social Prosperity.

(b) Setting the basic rules for digital markets

As a result of the Turku Conference, which was held in 1997, conditions concerning the basic framework for the taxation of electronic commerce were enacted at the OECD Ministerial Conference on Electronic Commerce (October 1998). The basic principles of the tax system proposed that the principles of neutrality, efficiency, clarity and certainty, effectiveness and fairness, and flexibility are necessary. The tax system framework for implementing these principles specifies that the elements covered are services for taxpayers, tax

administration (administration of information about individual taxpayers and authentication of taxpayers), the collection of taxes, consumption tax, and cooperation with the international tax system.

In December 2000, the OECD submitted a report with an analysis of a table showing each country's GATS commitments from the particular perspective of the provision of online services.

(c) Strengthening information infrastructure for electronic commerce

With regard to access to and use of information infrastructure, consideration has primarily been given to market trends and policy implications with regard to communications technology, such as approaches to network service prices, telecommunications regulations and interconnectivity between businesses. In particular, with regard to the relationship with electronic commerce, a report entitled Local Access Pricing and E-Commerce was published in 2000, which appealed for an awareness of the "international digital divide" brought about by differences in the degree to which international networks have become pervasive.

With regard to Internet management and the domain names system (DNS), a report providing statistical information to the Working Group on Internet Governance was submitted in May 2005, which was formed under the auspices of the United Nations.

(d) Maximizing the benefits brought about by electronic commerce

The main activities arising from this principle relate to the impact on the economy and society, electronic government, small and medium-sized enterprises, education and skills, remote area development and information and communications technology, cooperation in development, and global participation. In order to develop highly consistent international statistics, the OECD has published various reports that scrutinize various private sector surveys, while proposing a definition of electronic commerce and various relevant indicators.

(3) UNCITRAL

A model law related to electronic commerce and electronic signature has been adopted in United Nations Commission on International Trade Law (UNCITRAL), which was established in 1966 as a committee under the direct control of the United Nations General Assembly.

(a) Model Law on Electronic Commerce

This was adopted by UNCITRAL in 1996, and was adopted as an international resolution of the General Assembly in January 1997. Its objective is to provide a model law which can apply to use of electronic means, instead of paper-based means, for communication and information storage.

The main relevant provisions include “the legal weight, effectiveness or enforceability of information must not be denied on the grounds that it takes the form of a data message (Article 5)”, and “in relation to the completion of contracts, as long as there is no particular agreement between the parties, it is possible to display applications and consent to applications by means of data messages (Article 11)”. (This model law was revised in 1998.)

(b) Model Law on Electronic Signature

Based on Article 7 of the Model Law on Electronic Commerce, concerning electronic signature, this model law was adopted by UNCITRAL in 2001, reflecting the latest technological developments relating to electronic signatures. This model law specified the establishment of standards relating to technological reliability in order to certify the equivalence of electronic signatures with written signatures, and the guaranteeing of technological neutrality to ensure that no legal advantage is given to a particular technological product used for electronic signatures.

(c) Technical Notes on Online Dispute Resolution (ODR)

ODR is an indispensable component of e-commerce. When a person conducted cross-border e-commerce and a dispute arises from that commerce, it needs a lot of cost and burden for that user to raise a litigation. This is because he/she may have to raise that litigation in the exporter’s country, namely in a foreign country for him/her, and legal issues such as governing law and enforcement arises. This is caused by judicial system is operated under a country specific regime.

In this regard, online dispute resolution can contribute for solving these challenges and mitigating cost and burden.

In this regard, APEC economies have actively engaged in cooperation on ODR. APEC established APEC ODR Collaborative Framework in August 2019, which

supports international commercial dispute resolution among businesses in the APEC. Several APEC economies already participated in this framework.

APEC keeps updating this framework and upheld implantation action plan of it March 2021.

While APEC has already conducted extensive discussion on ODR, UNCITRAL also has been dealing with ODR and published “Technical Notes on Online Dispute Resolution” in 2016. This document is a reference material for ODR schemes.

(d) Notes on the Main Issues of Cloud Computing Contracts

In the UNICTRAL, initiatives on cloud computing contracts are also discussed. This document was published in 2019 and provides practical check list for user companies to review their contracts with cloud service providers.

In this document, various aspects of risks emerged from data localization requirements and government access to stored data are explained for the review of the cloud using contract. These include signer obligated for data localization requirement, data breach notification and response to data access request from government institutions, etc.

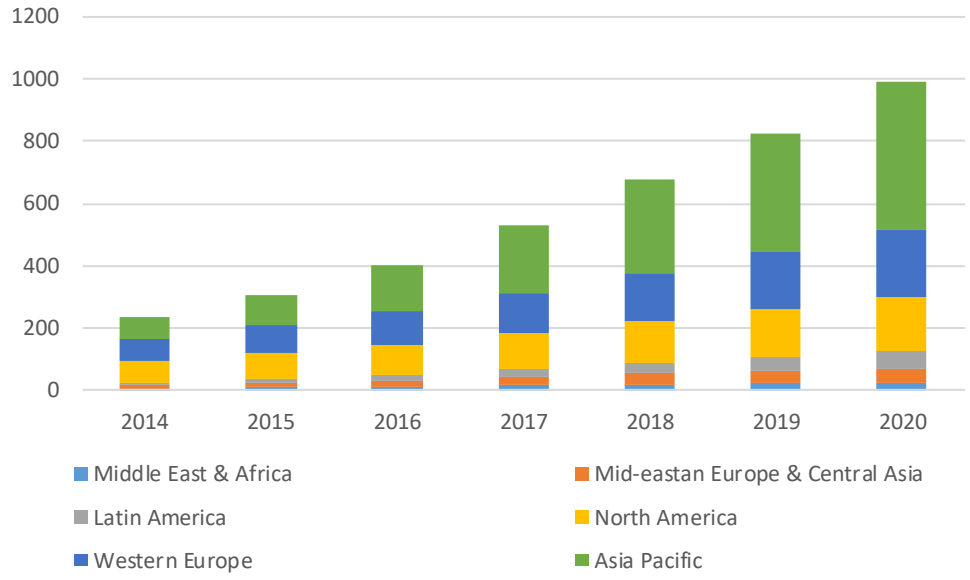
In general, utilization of cloud services will lead to the reduction of implementation and operational costs of IT systems, they are important for digitalization of companies, especially for MSMEs. Localization requirements makes cloud contracts more burdensome for companies and utilization of cloud services might be obstructed.

Chapter 3: Consider next steps on the issues related to the eventual realization of FTAAP taking into account the above-mentioned assessments and capacity building activities.

3.1 Capacity building for legal and operational framework for facilitating e-commerce

B2C cross border e-commerce market in the world has been rapidly growing from 236 billion US$ in 2014 to 994 billion US$ in 2020, of which Asia Pacific is 71 billion US$ to 476 billion US$ at the same period. Although, ratio of world e-commerce to retail trade is only 11.9% in 2018, digitalization will lead healthy growth of e-commerce.

Figure 5: Cross border e-commerce



Source) Ministry of Economy, Trade and Industry[1]

according to the “Summary of Adoption of E-Commerce Legislation Worldwide compiled by UNCTAD”, which provide the state of e-commerce legislation covered by 194 UNCTAD member state. In terms of e-transaction law, 145 countries (85%) are already adopted, of which 104 countries are developing or transition economies. And four out of five countries are in Asia and Latin America. Regarding the data protection and privacy legislation, 107 countries (of

[1] https://www.meti.go.jp/press/2019/05/20190516002/20190516002-1.pdf

which 66 were developing or transition economies) have put in place legislation to secure the protection of data and privacy.

Figure 6 shows the adoption of e-commerce legislation in APEC economies belonging with UNCTAD, all of economies has already been adopted E-transactions law, and most of all of the economies have also been adopted Consumer Protection law, Data protection & Privacy law and cybercrime law.

Figure 6: adoption of E-Commerce Legislation in APEC economies

	E-Transactions Laws	Consumer Protection Laws	Data Protection & Privacy Laws	Cybercrime Laws
Australia	✔	✔	✔	✔
Brunei Darussalam	✔	No Legislation	No Legislation	✔
Canada	✔	✔	✔	✔
Chile	✔	✔	✔	✔
China	✔	✔	✔	✔
Indonesia	✔	✔	✔	✔
Japan	✔	✔	✔	✔
Malaysia	✔	✔	✔	✔
Mexico	✔	✔	✔	✔
New Zealand	✔	✔	✔	✔
Peru	✔	✔	✔	✔
Philippines	✔	✔	✔	✔
Republic of Korea	✔	✔	✔	✔
Russian Federation	✔	Draft Legislation	Draft Legislation	No data
Singapore	✔	✔	✔	✔
Thailand	✔	✔	✔	✔
United States of America	✔	✔	✔	✔
Viet Nam	✔	✔	✔	✔

Source: UNCTAD

OECD (2010) concerned that against the backdrop of WTO stalemate, an increasing number of RTAs adopted specific provisions and rules for e-commerce. While these provisions increase the tradability of e-commerce, they also risk the creation of an e-commerce spaghetti bowl that will undermine the prospects for future WTO consensus in this area. Weber (2015) recognized that the adoption of WTO law is a very promising way, however, progress has not been made and law itself does not seem fit to meet the realities of Today's online society. And he noted that the situation at the multilateral level is characterized by legal gaps, so Government, investors, traders as well as consumers needed solutions within bilateral and regional trade agreement.

In addition to the above-mentioned legislation, the trainings on government's enforcement system that actually uses the system, private experts (business persons, lawyers, etc.) and organizations (certificate authorities that perform electronic certification) relating to electronic commerce are also required. Such a development on enforcement system and specialists are not always successful from a short-term perspective, and some long-term efforts are required through cooperative relationships between nations. APEC should function as a forum for forming such partnerships.

3.2 Promotion of CBPR as a foundational framework for APEC's privacy protection and maintaining interoperability with privacy frameworks with other regions

According to our survey on 11 economies of APEC, economies mostly agree that CBPR can be utilized as a practical guidance of institutional framework that facilitates trust in the Digital Economy, which is necessary for expansion of digital trade and e-commerce.

This survey also revealed that CBPR can play a role as harmonization of domestic legal systems of privacy protection among APEC economies.

Despite this wide recognition of CBPR's importance for the expansion of digital trade and e-commerce in the APEC region, as we discussed in 2.1, some contries express worries about the fact that the number of current CBPR participating economies and certified companies are not so huge at this moment.

Some economies pointed out that one possible reason is the lack of understanding of CBPR, especially the merits of it. If this is the truth, we have to conduct a cost-benefit analysis on CBPR certification, especially comparison with international standards that compete with CBPR, such as ISMS. Also, some developing economies state that not only merits of multinational companies based in advanced economies, but also that of MSMEs in the developing economies have to be made clear.

Some economies also stated that in the course of figuring out of these merits, we have to create clear merits of CBPR, such as exceptions for cross-border transfer of personal data in the domestic laws.

According to the survey, we also found that while economies recognize importance of CBPR, they are now conducting implementation of domestic legal system for CBPR. For example, an economy has not yet established Data Privacy Agency, while

other economy has accomplished it, but is now searching suitable domestic organization for the Accountability Agent.

APEC needs to facilitate sharing of experiences from economies already operating CBPR as a domestic system to economies on the way to that status. Also, in case of there is such a need, APEC needs to facilitate capacity building activities, such as organizational developments and training of legal systems development for the domestic implementation of CBPR.

Lastly, some economies stated the importance of CBPR to have an interoperability with other internationally recognized privacy frameworks, such as GDPR and regional frameworks among APEC economies like ASEAN or Pacific Alliance. In this regard, APEC has conducted interoperability study between CBPR and BCR and been in a discussion with EU for further study.

In addition to these possible improvement suggestions based on current CBPR system, economies also proposed possible future developments of CBPR.

Some economies pointed out that under current CBPR system, certified companies have to make a yearly payment for renewal of certification and it is a heavy burden for companies with CBPR certifications. We should take note that possible cost reduction is also important for CBPR expansion.

Economies also proposed further development of privacy protection beyond current CBPR. Taking recent international developments of privacy protection, such as right of data portability stipulated in the GDPR into account, APEC should promote further discussion of new themes of privacy protection related to CBPR.

3.3. Common Understanding on Data Free Flow with Trust that facilitates e-commerce and domestic reforms

As mentioned in 1., the concept of DFFT mentioned in the G7 Leaders' Statement, etc., promotes further data flow by increasing confidence in data flow, and by rotating this positive cycle, the data economy will be expanded as a whole. The institutional foundations for trust mentioned in 3.1., for example, the legal system for electronic commerce, the system for privacy protection and consumer protection, etc. are important for securing such trusts. The APEC economy should start discussions on such an internationally agreed and common starting point for data flow, and involve all stakeholders, including governments, private sectors, and

consumer representatives to promote such basic understanding sharing among economies.
In fact, according to our survey on 11 economies, it is widely accepted that such trust is important for the development of digital trade and e-commerce. Among other, debate on privacy protection must be enhanced based on existing regime such as CBPR.

On the other hand, legal systems that are not necessarily tied to such trusts, such as excessive localization and unlimited government access, rather impair the trust and impede the free flow of data. Such a system should be rigorously reviewed from the view point of whether it serves the purpose of legitimate public policy and, if necessary, necessary changes should be added to more embody the DFFT philosophy.

At the same time, according to our survey on 11 economies, economies agrees that some localization requirements and government access have legitimate purposes for public policy. APEC take care that these debate respect legitimate regulatory powers of APEC member economies within their territories.

Economies with a wealth of know-how on data-related policies should proactively provide the necessary technical advice and capacity building for such domestic reforms implemented by other economies.

APEC should also provide technical support for reforms required by various economies, by sharing best practices for domestic reforms.

According to our survey on 11 economies, developing economies expressed a clear need for such kinds of capacity building. Such capacity building activities include dispatch of experts and training of officials and sharing of best practices for domestic reforms.

The survey also revealed that APEC economies are highly interested in the cooperation related articles contained high-standard agreements such as DEPA. In this regard, if what kinds of actual cooperation activities done and the contribution of these activities for the development of digital economies is shared, that is a very important input for APEC's further discussion on digital trade and e-commerce. APEC should facilitate these activities and parties of high-standard agreements are requested to share these precious experiences with other economies.

3.3. Multilateral rule-making in the APEC

Finally, APEC should promote the formation of multilateral rules regarding e-commerce in APEC in order to promote the above-mentioned cooperative relations and domestic reforms regarding e-commerce between APEC economies. As a basis for such rules, APEC should refer to agreements already agreed by the APEC economy, such as agreements with advanced rules on e-commerce such as CPTPP, USMCA and DEPA.

On the other hand, it is difficult for the APEC economy to agree on all the provisions of the above agreement, so as analyzed in 1. of this report, it is possible to include provisions that have broad agreements among the economies as a starting point, promote domestic reforms while building capacity for e-commerce and to form higher-level rules. Even when taking such options, we must not forget that the ultimate goal is to form high-dimensional rules, and the basic idea is to proceed from the rules that have already been agreed upon as an intermediate stage to aim this goal.

Finally, it is also important to connect the above-mentioned rule formation in APEC to the formation of multilateral rules regarding global electronic commerce. In this regard, it is conceivable that APEC will make positive proposals to the meeting while referring to the discussions at the Volunteer State Meeting on Electronic Commerce held at the WTO. APEC once played an important role in WO's negotiations on ITA, and we should also be aware of the importance of APEC playing an active role in the formation of multilateral rules regarding electronic commerce.

WTO’s JSI (Joint Statement Initiative on e-commerce) was established from an initiative of Australia, Japan and Singapore, all of which are APEC economies and therefore has a deep relationship with APEC. While many economies of APEC already participated in the JSI, APEC can play a further role as facilitating more economies’ participation as well as providing necessary information and consultation with economies considering its participation towards JSI.

In fact, our survey on 11 economies revealed AEPC economies widely recognize the importance of APEC’s active engagement to JSI.

APEC is characterized by being a unique and huge forum in which developing and developed countries cooperate in forming non-binding rules, and has played its role in global rule formation more than ever before. With this in mind, APEC should play an active role in the formation of digital-related rules, which will become increasingly important in the future.

Through the above mentioned initiatives including achieving digital economy based on “Data Free Flow with Trust” and becoming a world leader both in rule-making and economic development, APEC should further contribute to the development of world economy.

Annex I References

- José-Antonio Monteiro and Robert The, “Provisions on Electronic Commerce in Regional Trade Agreements”, WTO Working Paper ERSD-2017-11 (https://www.wto.org/english/res_e/reser_e/ersd201711_e.pdf)
- Seatgate “Data Age 2025” (https://www.seagate.com/jp/ja/our-story/data-age-2025/)
- Rolf H. Weber, “Digital Trade and E-Commerce: Challenges and Opportunities of the Asia-Pacific Regionalism”, *Asian Journal of WTO & International Health Law and Policy,* Vol. 10, No. 2, pp. 321-348, September 2015