KIEP 기초자료
21-12

2021년 9월 8일

APEC CBPR 운영 및 논의 동향과 시사점

박은빈 APEC연구컨소시엄사무국 전문연구원 (ebpark@kiep.go.kr, 044-414-1046)
강민지 무역통상실 무역협정팀 전문연구원 (mjkang@kiep.go.kr, 044-414-1196)

KIEP 대외경제정책연구원
Korea Institute for International Economic Policy

Korea Institute for International Economic Policy

APEC CBPR 운영 및 논의 동향과 시사점

요약

▶ APEC은 국경간 전자상거래 활성화로 개인정보의 국외 이전 수요가 증가함에 따라 최소한의 개인정보보호 원칙을 기반으로 개인정보보호 인증 메커니즘인 '국경간 프라이버시 규칙(CBPR)'을 2011년에 마련하였으나, APEC 회원국의 가입률 저조로 최근 CBPR을 非APEC 국가로 확대하려는 움직임이 있음.

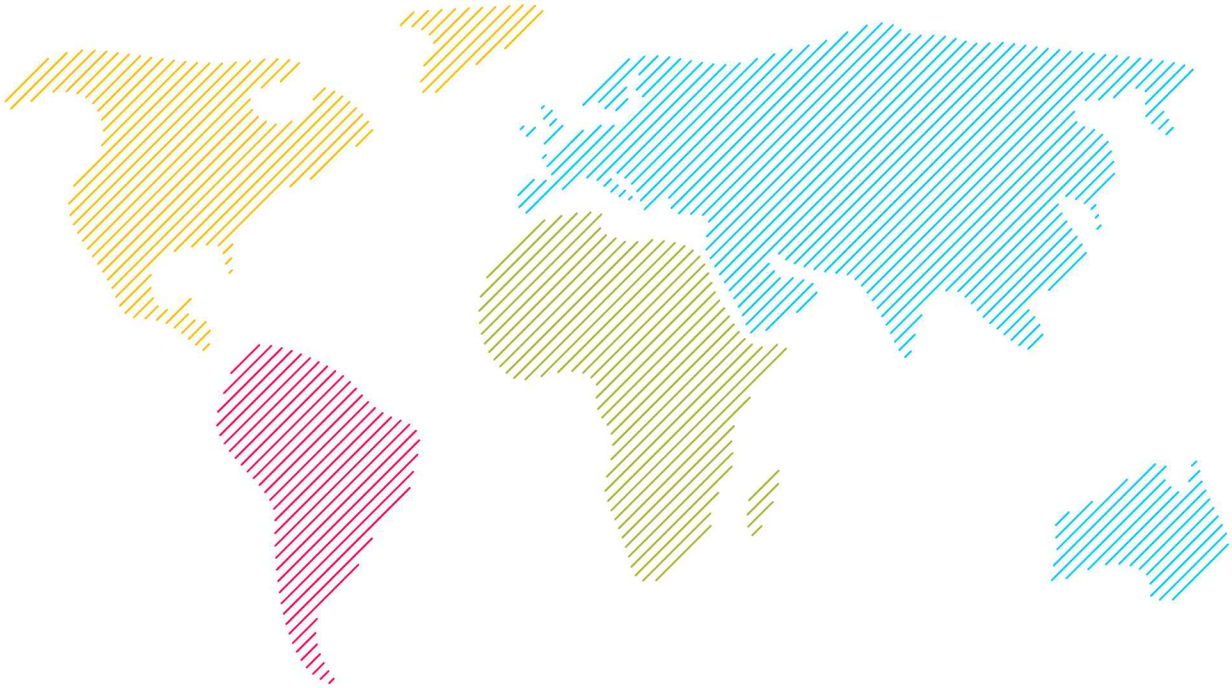
- APEC CBPR은 회원국간 안전하고 자유로운 데이터 활용을 장려하기 위해 자발적 참여를 전제로 개발된 개인정보보호 자율인증 제도로, 이는 2004년 APEC 각료회의에서 승인된 'APEC 프라이버시 프레임워크(APF)'에 포함된 개인정보보호 원칙을 바탕으로 수립됨.
- 창설된 지 10년이 지났으나 2021년 우리나라를 비롯하여 9개국(미국, 멕시코, 일본, 캐나다, 한국, 호주, 싱가포르, 대만, 필리핀)이 APEC CBPR에 가입하였고, 그중 5개국에 인증기관이 설치되었으며, 이 중 3개국만 실제로 운영하고 있어 기업의 인증률이 저조한 편임.
- 현재 APEC 회원국에 한하여 CBPR 가입신청이 가능하고 APEC 심의를 통해 가입이 결정되나, 미국은 CBPR을 APEC으로부터 독립시켜 CBPR 회원국 확대를 모색하고 있음.

▶ 국가마다 개인정보보호를 위한 법제도의 규제 수준이나 보호 범위 등이 상이하여, APEC은 CBPR을 국경간 데이터 이전의 글로벌 메커니즘으로 상호운용성을 높이고자 노력하고 있으며, 최근 CBPR이 국경간 정보 이전에 효과적인 메커니즘임을 인정하는 자유무역협정이 체결되고 있음.

- 한편 GDPR의 경우 국경간 이전과 관련하여 원칙적으로 개인정보보호의 관점에서 적정한 보호 수준을 갖춘 국가·기업으로의 이전만을 제한적으로 허용하는 등 CBPR보다 높은 요건으로 인해 상호운용 논의가 어려운 상황임.
- 최근 체결된 USMCA, SADEA에는 개인정보보호를 위한 법적 체계 개발에 있어 고려해야 할 국제 원칙과 지침으로 APEC CBPR 인증체계가 포함되었으며, 데이터 국외 이전에 효과적인 메커니즘으로 CBPR을 인정하고 있음.

▶ APEC CBPR의 실효성을 강화하고 이를 글로벌 대표 인증체계로 인정받기 위해서는 정부와 APEC 차원의 다양한 부문에서 역할과 노력이 필요할 것으로 보임.

- 우리나라의 CBPR 인증기관인 KISA는 2021년 하반기 중에 CBPR을 정식으로 운영할 계획이며, 일본과 싱가포르는 이미 CBPR을 자국의 「개인정보보호법」과 동등한 수준의 보호체계로 인정하여 그에 상응하는 혜택을 부여하고 있음.
- 현재는 CBPR-BCR의 상호운용성 논의를 위한 APEC 내 비공식회의가 중단된 상태이나, APEC CBPR이 하나의 인증 메커니즘으로 GDPR에서 인정 받기 위해 상호운용 논의를 지속적으로 진행할 필요가 있음.
- 향후 CBPR을 개인정보보호위원회가 지정하는 인증제도 중 하나로 고려해볼 수 있는지 혹은 CBPR에 반영되지 않은 국내 「개인정보보호법」 요소들을 CBPR에 반영할 수 있는지를 검토하고, 국경간 정보 이전에 있어 국내법에 상응하는 혜택을 인증 기업들에 부여하는 방향으로 나아갈 필요가 있음.
- USMCA, SADEA 등에서 개인정보보호를 위한 법적 체계 개발 시 고려해야 할 국제기구의 원칙과 지침 중 하나로 APEC CBPR을 규정하고 있듯, FTA 및 디지털무역협정 등에 APEC CBPR을 포함함으로써 글로벌 대표 인증체계로 발돋움하는 데 기여할 필요가 있음.



차 례

1. 서론

2. APEC CBPR의 주요 내용 및 현황
   가. APEC CBPR의 주요 내용
   나. 가입국별 운영 현황

3. APEC CBPR 발전에 관한 논의 동향
   가. APEC CBPR의 상호운용성(Interoperability) 논의
   나. 자유무역협정 내 APEC CBPR의 인정

4. 시사점

부록: 1. CBPR 인증제도 승인 기업
      2. PRP 인증제도 승인 기업

참고문헌

1. 서론

■ APEC은 2011년에 개인정보를 보호하면서 원활한 데이터 흐름을 보장하기 위해 글로벌 개인정보보호 인증 메커니즘인 '국경간 프라이버시 규칙(CBPR: Cross-Border Privacy Rules)'을 도입하였으나, 실제 회원국의 활용률은 높지 않음.

- APEC은 국경간 전자상거래가 활성화됨에 따라 안전한 개인정보 이전 규칙을 마련하기 위해 2004년 'APEC 프라이버시 프레임워크(APF: APEC Privacy Framework)'를 수립함.
- APF는 '개인정보가 포함된 데이터의 자유로운 흐름을 보장한다'는 관점에서 아태지역의 개인정보보호 체계(국경간 데이터 이전 시 개인정보 처리 원칙 등)에 대한 가이드라인을 제공하기 위한 목적으로 수립됨.
- APEC은 APF를 토대로 국경간 데이터 이전 시 기업의 데이터 보호 수준을 인증하기 위한 메커니즘으로 CBPR을 개발하여 국경간 자유로운 데이터 흐름을 보장하는 환경을 구축하였음.
- APEC 21개 회원국 중 일부 회원국(중국, 베트남 등)은 개인정보보호와 국가 보안 이슈 등의 이유로 국가 차원에서 데이터를 관리하는 데이터 보호주의적 관점에서, 반면 다른 일부 회원국(미국, 일본 등) 디지털무역 활성화를 위해 최소한의 개인정보보호 기준 준수를 조건으로 자유로운 데이터 흐름을 보장하는 관점에서 CBPR 논의에 참여하고 있음.

표 1. 글로벌 전자상거래 기업 상품거래액 (GMV: Gross Merchandize Value) 증가 추이

(단위: 10억 달러)

순위	기업명	본사	2018	2019	2020	'18~'20 증가율
1	알리바바	중국	866	945	1,145	32.2%
2	아마존	미국	344	417	575	67.2%
3	JD.com	중국	253	302	379	49.8%
4	Pinduoduo	중국	71	146	242	240.8%
5	Shopify	캐나다	41	61	120	192.7%
6	eBay	미국	90	86	100	11.1%

그림 1. APEC 주요 회원국별 전체 소매 판매 중 전자상거래 비중

(단위: %)

자료: UNCTAD(2021), "Estimates of Global E-Commerce 2019 and Preliminary Assessment of COVID-19 Impact on online retail 2020" 참고하여 저자 재구성.

■ 최근 미국은 CBPR을 APEC 차원에서 논의하는 것이 비효율적[1]이라고 밝히며, CBPR을 APEC으로부터 독립시켜 다른 국가들도 가입할 수 있도록 전담 운영기구를 신설하고자 CBPR 개정안을 제안함.

- 미국의 주도로 추진된 APEC CBPR의 인증체계는 데이터 지역화를 주장하고 있는 중국, 러시아, 베트남 등의 반대로 CBPR 가입국 확장이 어려워졌으며, 그 외 미가입국에서는 아직 개인정보보호의 법적 근거가 마련되어 있지 않고, 기술적으로 앞서가는 선진국과의 국외 이전을 원활화할 경우 당국의 데이터 개인정보보호가 보장되지 않을 것을 우려함.

1) APEC은 의사결정 시 회원국간 컨센서스 형성 필요. 연합뉴스(2020. 8. 21), 「美 국제 데이터 유통서 中 제외 노려...APEC 규칙 개정 제안」 참고.

- CBPR은 창설된 지 10년이 지났으나 회원국간 의견 차로 현재 9개국[2]만 가입한 상황이며, 그중 CBPR의 개인정보보호 기준 준수를 확인하는 인증기관(Accountability Agency)이 마련된 국가는 미국, 일본, 싱가포르, 한국, 대만 등 5개국에 불과함.
  - 인증기관(Accountability Agency)이 마련된 5개국 중 CBPR 인증제도를 실제로 운영하고 있는 국가는 미국, 일본, 싱가포르 3개국뿐이며, CBPR에 인증 받은 기업은 총 42개에 그침.
- 미국은 CBPR을 APEC에서 독립시킬 경우 APEC 회원국이지만 CBPR에 참여하지 않고 있는 중국의 간섭 없이 신설기구의 규칙을 강화하거나 가입국을 확대할 수 있을 것으로 기대함.
  - 다만, 중국이 APEC CBPR과 상반되는 관점(데이터 국외 이전 관리·감독 강화)을 취하고 있는 상황으로 미국의 이러한 움직임은 디지털무역 경쟁력을 제한하려는 시도[3]로 인식할 수 있음.

■ 본고에서는 최근 APEC CBPR 운영 현황, GDPR과의 상호운용 가능성, 지역협정 내 국경간 데이터 이전에 관한 조항 등을 통해 APEC CBPR의 발전 가능성을 살펴보고, 이에 대한 우리나라의 대응방안을 고찰하고자 함.

- 안전한 국경간 데이터 이전과 전자상거래 활성화를 동시에 도모하면서 개인정보보호를 위한 국제적 규범을 형성하고자 하는 상황에서 한국은 미·중 갈등으로 인한 논의 정체에서 벗어나 보다 적극적이고 체계적인 대응이 필요한 시점임.

2. APEC CBPR의 주요 내용 및 현황

가. APEC CBPR의 주요 내용

■ [CBPR 수립 배경 및 인증기준] CBPR은 APEC 회원국간 안전하고 자유로운 데이터 이전을 위해 자발적 참여를 전제로 한 개인정보보호 자율인증 제도이며, APEC 각료회의에서 승인된 'APEC 프라이버시 프레임워크(APF)'에 포함된 9개 원칙을 바탕으로 개발됨.

- APF는 1998년 정상회의 부속서로 채택된 'APEC 전자상거래 행동계획(Blueprint for Action on Electronic Commerce)' 이행을 목적으로, 국경간 자유로운 개인정보 이전을 통한 전자상거래 촉진에 초점을 맞춘 프레임워크임.
  - APF는 1980년에 발표된 OECD 프라이버시 가이드라인[4] 원칙을 참고하여 작성하였으며, 가이드라인이 새롭게 개정됨에 따라 변화된 환경 반영 및 원칙 조화를 위해 APF도 2015년에 개정된 프레임워크를 발표함.

2) 미국, 멕시코, 일본, 캐나다, 한국, 호주, 싱가포르, 대만, 필리핀.
3) 미국이 '5G 클린패스(Clean Path)' 정책(미국 시민 및 기업의 개인정보보호 목적)을 통해 화웨이, ZTE 등 중국의 대표적인 IT 기업들을 글로벌 공급망에서 배제하려는 움직임을 보임.
4) OECD는 안전하고 원활한 개인정보 처리를 위해 적절한 해결방안을 제시하기 위해 1980년 프라이버시 가이드라인(Gudielines on the Protection of Privacy and Transborder Flows of Personal Data)을 제시함. 빅데이터, 클라우딩 서비스와 같은 새로운 ICT 기술의 등장과 발전에 따라 기존 가이드라인을 재검토하여 2013년에 개정 가이드라인(The OECD Privacy Framework)을 발표함. 정보통신산업진흥원(2014. 6. 4), 「개정 OECD 프라이버시 가이드라인 주요 내용 및 향후 전망」 참고.

- APF 수립 이후 미국은 2007년 전자상거래운영그룹(ECSG: E-Commerce Steering Group)[5] 산하 개인정보보호 분과(DPS: Data Privacy Sub-Group)에서 '개인정보보호 관련 선구자 사업(APEC Privacy Pathfinder)'[6]을 제안하여 CBPR의 자가진단 지표, 평가방법, 인증기관 지정 절차 등 운영 기초를 마련함.
- 2011년 11월에 개최한 APEC 각료회의에서 '개인정보보호 관련 선구자 사업'을 통해 마련된 CBPR 운영 기초문서가 승인되어, 같은 해 정상선언문에 APEC CBPR 개발 및 이행을 촉구하는 문구를 포함하여 CBPR 회원국 가입 개시를 알림.
- CBPR은 APF에 수록된 9가지 원칙을 기반으로 50가지 인증 기준을 구성하였으며, 각각의 기준들은 국경간 데이터 이전 시 기업의 개인정보보호 수준을 파악할 수 있는 척도로 활용됨(표 2 참고).

표 2. APEC CBPR 인증제도 수립 배경

연도	내용
1998	정상회의 부속서로 채택된 'APEC 전자상거래 행동계획' 이행의 일환으로 OECD 국경간 개인정보 이전 가이드라인(1980)을 참고하여 APF 수립 작업 개시
2004	APEC 각료회의에서 APF 승인
2011	APF에 포함된 9개 원칙을 바탕으로 CBPR 인증제도 도입
2015	OECD 가이드라인(2013)이 업데이트됨에 따라 APF도 2015년 업데이트하여 발표[7]
2015	APEC은 CBPR 인증제도에 포함되지 않은 정보 프로세서(information processor)의 보호 수준을 평가하는 개인정보보호 프로세서 인증제도(PRP: Privacy Recognition for Processor)[8] 도입

자료: 저자 작성.

표 3. APEC 개인정보보호 규칙에 기반을 둔 CBPR 인증 기준 요구사항

APEC Privacy Framework 9개 원칙	설명	CBPR 인증 기준(50개)
고지 (Notice)	'사전 혹은 동시'에 고지를 제공할 것을 규정하고 있고, 경우에 따라 '사후 고지' 가능	개인정보보호 정책 고지 항목, 고지 방법 등(4개)
수집 제한 (Collection Limitation)	수집 목적에 관련(related)된 정보를 합법적이고 공정하게 수집하고, 적절한 경우 동의를 받아야 함	개인정보 수집 방법, 수집 최소화, 합법적 수집 등(3개)
개인정보 이용 (Uses of Personal Information)	수집 목적과 양립 가능(compatible)하거나 관련(related)된 목적으로 이용	수집 목적 내 이용·위탁·제3자 제공 등(6개)
선택 (Choice)	적절한 경우 정보주체에게 수집·이용·제공에 대한 선택권 부여	정보주체의 수집·이용·제공에 대한 선택권 제공 방법 등(7개)
개인정보의 무결성 (Integrity of Personal Information)	정보의 정확성, 완전성, 최신성 확보	개인정보의 최신·정확·완전성을 위한 정정, 수탁자 통지 등(5개)

5) ECSG는 1998년 채택된 전자상거래 행동계획 이행을 목적으로 설립된 그룹임. 현재는 전자상거래뿐만 아니라 디지털경제의 전반적인 이슈를 다루기 위해 범위를 넓히고, '디지털경제조정그룹(DESG: Digital Economy Steering Group)'으로 명칭을 변경함.

6) 개인정보보호 관련 선구자 사업(시범사업)의 목적은 APEC 회원국간 데이터 이전 시 개인정보를 보호하면서 활발한 이전을 촉진하기 위해 기업이 활용할 수 있는 국경간 데이터 이전 규칙제도를 개발하는 것임. APEC Document(2007/SOM3/ECSG/SEM/023).

7) 개정된 프레임워크에는 PRP 개념이 추가되었고, 9가지 원칙은 2004년에 발표된 그대로이며 원칙의 해설(commentary)과 시행(implementation) 부문에 Privacy management program, Security breach notification, education and awareness, global interoperability 항목 등이 추가됨.

8) APEC PRP 인증제도는 정보 프로세서(information processors, e.g. 본사의 개인정보보호 규정에 따라 정보를 처리하는 현지 법인)가 개인정보 처리와 관련해 정보 컨트롤러(information controllers, e.g. 해외 법인의 개인정보 수집 목적 및 수단을 규정하는 본사)의 개인정보보호 준수 의무를 효과적으로 이행하기 위한 능력을 입증하도록 한 것임. PRP 인증제도는 정보 컨트롤러가 자격과 책임이 있는 정보 프로세서를 판별하는 데 도움을 주고, 중소 규모 정보 프로세서의 보호 준수 정도를 파악하여 신뢰성을 입증할 수 있음. 2020년 7월 12일 기준 APEC PRP에 가입한 국가는 미국, 일본, 싱가포르 3개국이며, 미국은 3개, 싱가포르는 2개의 기업이 PRP 인증을 받음.

APEC Privacy Framework 9개 원칙	설명	CBPR 인증 기준(50개)
보안조치 (Security afeguards)	위험 발생 가능성과 심각성, 정보의 민감성에 비례하여 적절히 조치 * 구체적 보호조치 기준 없음	개인정보의 민감성, 침해 가능성 및 침해의 심각성에 비례한 보호조치, 보호조치에 대한 평가 등 (10개)
열람·정정 (Access and Correction)	정보주체의 요청이 있을 시 개인정보의 열람·정정 등이 가능하나, 과도한 비용이 수반되거나 상업적 비밀로 보호되어야 하는 경우 제외	정보주체의 열람·정정·삭제 요청에 대한 절차 등 (3개)
책임성 (Accountability)	개인정보를 이전하는 경우, 동의를 받거나 개인정보를 이전받는 기관(개인)의 보호 수준을 실사하고 합리적 조치 이행	책임자 지정, 민원처리 및 피해구체 절차, 수탁자 및 제3자에 대한 관리·감독 방법 등(12개)
피해 구제 (Preventing Harm)	구제조치는 피해의 개연성과 심각성에 비례하여 취해져야 함	(책임성 등 다른 항목에 '피해 구제'에 대한 사항 내포)

자료: 한국인터넷진흥원 APEC CBPR 인증제도 페이지(https://www.kisa.or.kr/business/infor/main_sub11.jsp).

■ [CBPR 가입 절차] CBPR 인증제도를 운영하기 위해 APEC은 회원국간 개인정보보호 관련 정보 공유 및 공동조사 등의 법집행 협력을 목적으로 하는 '국경간 프라이버시법 집행약정(CPEA: Cross-border Privacy Enforcement Arrangement)'을 마련하였으며, CPEA에 가입해야만 CBPR 가입 신청이 가능함.

- CBPR 가입 심의 및 의결은 APEC 디지털경제조정그룹(DESG: Digital Economy Steering Group) 산하 개인정보보호 분과(DPS: Data Privacy Sub-Group)에서 맡아서 진행하고 있음.
  - ○ DESG-DPS에서 공동감독 패널(JOP: Joint Oversight Panel)[9]을 선출하며, JOP는 CPEA 가입을 결정하고, CBPR 가입 심사, 인증기관(Accountability Agent) 승인[10] 등 CBPR 가입 심사 및 행정 관리 업무를 수행함.
- 인증제도 가입 및 인증 절차는 [표 5]와 같음.

표 4. CBPR 인증제도 가입(회원국) 및 인증(기업) 절차

구분	APEC 회원국 CBPR 가입 절차	기업의 CBPR 인증 절차
1단계: 자가진단/구비서류 제출	국경간 프라이버시집행약정(CPEA) 가입 확인서 및 최소 1개의 법 집행기관 선정	인증기관(Accountability Agent) 선정
	APEC 승인을 받은 인증기관을 사용하겠다는 의도 확인	APF 9가지 원칙 준수에 대한 자가진단
	개인정보보호 국내법과 이를 집행할 수 있는 메커니즘 유무 확인	APEC CBPR 자체진단 설문지 제출[11]
2단계: 규정 준수/리뷰	제출 서류에 대한 DESG-DPS 의장 및 Joint Oversight Panel(JOP)의 CBPR 합치성 평가	인증기관(Accountability Agent)의 평가
3단계: 승인	DESG 의장 승인	승인 시 규정 준수 기업 명단에 신청 기업 추가[12]
4단계: 시행/법 집행	회원국의 규정 준수 여부에 따라 JOP에서 CBPR 참여를 종료하거나 중단할 수 있음.	프라이버시법 집행기관 및 인증기관의 감독 아래 규정 준수

자료: APEC Document Database(2011/SOM3/CTI/023b) 참고하여 저자 작성.

9) DESG-DPS 내에서 CBPR 가입 협의, 인증기관 승인, 권고 작성 등을 수행하기 위해 3명의 공동감독 패널(JOP: Joint Oversight Panel)을 선출함. (APEC Document Database(2011/SOM3/CTI/023b)).

10) JOP는 APEC 회원국의 CBPR 가입 의사에 관한 JOP 조사결과보고서(Findings Report)를 작성하고, 가입 후 승인을 요청하는 인증기관에 대한 승인 가능 여부를 확인하기 위한 권고보고서(Recommendations)를 작성하여 DESG-DPS에 제출함.

11) APEC CBPR Intake Questionnaire, https://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-Intake-Questionnaire.pdf.

12) 인증기관이 선정한 모든 회원국의 CBPR 및 PRP 인증 유효기간은 1년이며, 인증기간 만료 전 재인증을 신청하여 유효기간을 갱신할 수 있도록 안내함.

■ **[CBPR 최근 논의 현황]** 미국은 2020년 제2차 고위관리회의 기간 동안 DPS에서 'CBPR을 APEC 차원에서 논의하는 것이 비효율적이라고 밝히며, 非APEC 국가들도 가입할 수 있도록 하면서 전담 운영기구 신설 필요성을 제안함.

- APEC의 디지털 이슈는 국경간 데이터 이전 촉진을 찬성하는 입장인 미국 주도로 진행되고 있으나, 국가 주도로 데이터를 관리하는 중국과의 이견으로 인해 논의가 정체되고 있음.
  - ○ 디지털 이슈에 관한 역내 갈등으로는 개인정보를 자국 내에서만 저장하고 처리하도록 한 '데이터 지역화' 금지에 대한 이견 등이 있으며, 역외적으로도 디지털통상, 특히 글로벌 데이터 거버넌스를 수립하는 과정에서 미·중 간 갈등이 지속되고 있음.
  - ○ 지난 10년간 21개 회원국 중 9개 회원국만 CBPR에 가입한 상황이며, 이들 중 미국, 일본, 싱가포르, 한국, 대만 등 5개국을 제외한 나머지 4개국은 인증기관이 부재하여 기업의 인증률도 저조한 상황임.
- APEC CBPR을 APEC으로부터 독립시켜 운영하게 될 경우 APEC의 의사결정 방식인 회원국간 컨센서스 형성[13] 없이도 운영 절차를 개선하거나 불필요한 인증 기준을 제외하는 것이 가능하여 인증제도의 실효성 부문을 강화하는데 보다 용이하게 운영할 수 있음.

나. 가입국별 운영 현황

■ **APEC CBPR에 가입한 회원국은 미국, 멕시코, 일본, 캐나다, 한국, 호주, 싱가포르, 대만, 필리핀(가입순) 총 9개국이며, 이 중 인증기관이 마련된 미국, 일본, 싱가포르, 한국, 대만의 운영 현황만 분석함.**

표 6. APEC 회원국별 CBPR 가입 및 운영 현황(2021. 8. 12 기준)

가입국	가입 연도	프라이버시법 집행기관 (Privacy Enforcement Authority)	인증기관 (Accountability Agent)
미국	2012	연방거래위원회 (FTC: Federal Trade Commission)	Schellman
			Truste/TrustArc
			NCC Group
			HITRUST
			BBB National Program
멕시코	2013	정보·데이터보호접근연방기관 (Federal Institute for Access to Information and Data Protection of Mexico)	없음.
일본	2014	일본 개인정보보호위원회	JIPDEC
캐나다	2015	캐나다 개인정보보호위원회(OPCC: Office of the Privacy Commissioner of Canada)	없음. * 인증기관 모색 중이며, 미국의 인증기관인 TrustArc을 지정하는 방식도 고려 중
한국	2017	개인정보보호위원회	한국인터넷진흥원 (Korea Internet & Security Agency)
호주	2018	호주 연방정보위원회(OAIC: Office of the Australian Information Commissioner) 빅토리아주 정보위원회(OVIC: Office of the Victorian Information Commissioner)	없음.

13) 현재는 CBPR 가입국이 아닌 APEC 회원국도 CBPR 운영 등 위임사항(Terms of Reference) 의사결정에 참여하고 있음.

가입국	가입 연도	프라이버시법 집행기관 (Privacy Enforcement Authority)	인증기관 (Accountability Agent)
싱가포르	2018	개인정보보호위원회 (Personal Data Protection Commission)	정보통신미디어개발청(Info-communications Media Development Authority)
대만	2018	개인정보보호청 (Personal Data Protection Office)	정보산업진흥원 (Institute for Information Industry)
필리핀	2020	국가 개인정보보호위원회 (National Privacy Commission)	없음.

자료: APEC DESG - DPS Document Database 및 CBPR 홈페이지(http://cbprs.org/) 참고하여 저자 작성.

■ [미국] 미국은 APEC CBPR 체제를 주도적으로 이끌고 있는 회원국으로, 2012년에 가입하여 현재 5개[14]의 인증기관을 두고 있으며, 현재(2021. 9. 1 기준)까지 CBPR은 36개, PRP는 23개의 기업이 인증을 획득함(부록 1, 2 참고).

- 미국 연방정부는 개인정보 처리 행위를 규율하는 「프라이버시법(The Privacy Act of 1974)」을 1974년에 개정하였으나, 미국의 개인정보보호 체계는 기본적으로 시장자율 규율(self-regulation) 방식을 취하고 있음.[15]
- 미국에서 CBPR 인증을 초반에 받은 기업으로 Apple, HP, IBM 등 주요 테크 제조업 기업이 있으며, 그 이후에는 디지털 기술을 활용한 서비스업에 참여하는 기업들(Cisco, Mastercard, PGA Tour, BitSight Technologies 등)도 인증을 받음.

■ [일본] 일본은 2013년 가입신청서를 제출하여 2014년에 가입이 승인되었으며, 일본정보경제사회추진협회(JIPDEC: Japan Institute for Promotion of Digital Economy and Community)에서 CBPR 및 PRP 인증을 돕는 인증기관을 맡고 있고, 2개의 디지털 기술 관련 기업이 CBPR 인증을 획득함(부록 1, 2 참고).

- CBPR 인증제도 가입 당시에는 경제산업성이 개인정보보호 업무를 담당하였으나, 2015년 「개인정보보호법」 개정 이후 2016년에 설치된 개인정보보호위원회에서 집행을 담당하고 있음.
- 일본은 최근(2020년) 개정된 「개인정보보호법」을 통해 개인정보의 국외 이전이 가능한 기준(적합한 체제를 정비하고 있는 경우)을 규정하고 있으며, APEC CBPR 인증을 획득한 기업의 경우 동 기준을 충족한 것으로 간주
  - CBPR 가입이 승인된 기업은 Intasect Communications(IT 솔루션, 온라인 결제 등)와 Paidy(온라인 결제)이며, 2021년 상반기까지는 GMO GlobalSign(IoT용 ID 및 보안 솔루션) 기업도 CBPR 승인 기업이었으나 현재는 CBPR 승인 목록(directory)에서 빠져 있는 상태

■ [싱가포르] 싱가포르는 2017년 CBPR 및 PRP 인증제도에 가입하였으며, CBPR 및 PRP 인증을 받은 기업은 싱가포르 「개인정보보호법」과 비슷한 수준의 보호를 제공하는 것으로 간주됨.[16]

- 싱가포르는 자국의 데이터 보호 신뢰마크(DPTM: Data Protection Trustmark)[17] 표준을 APEC CBPR 및 PRP 인증제도에 맞추었으며, 이에 따라 DPTM 인증을 받은 기업들은 CBPR 및 PRP 인증 획득이 용이해짐.[18]

14) Schellman, Truste(TrustArc), NCC Group, HITRUST, BBB National Program.
15) 개인정보보호위원회 개인정보보호 국제협력센터 웹페이지, https://www.privacy.go.kr/pic/nation_usa.do.
16) IMDA-APEC CBPR 소개 페이지에 언급된 CBPR 및 PRP 인증기관으로의 데이터 전송에 대한 샘플 조항, https://www.pdpc.gov.sg/help-and-resources/2020/06/sample-clause-for-data-transfers-to-apec-cbpr-and-prp-certified-organisations.
17) DPTM은 책임 있는 데이터 보호 관행을 입증하기 위한 자발적인 인증제도임. DPTM에 인증을 받음으로써 기업의 경쟁우위를 강화하고 소비자 및 이해관계자들과의 신뢰를 구축함. Hunton Andrews Kurth, Privacy & Information Security Law Blog(2017. 7. 28), "Singpore Submits Notice of Intent to Join the APEC CBPR and PRP System" 참고.

- 싱가포르는 정보통신미디어개발청(IMDA: Info-communications Media Development Authority)을 CBPR 및 PRP 제도의 인증기관으로 선정하였고, 최근 4개 기업의 CBPR, 2개의 기업의 PRP 인증을 완료함(부록 1, 2 참고).
- IMDA는 기업의 인증 획득을 장려하기 위해 기업발전기금(Enterprise Development Grant)을 운영하여 상담서비스 비용 지원, 중소기업 인증신청 수수료 감면정책을 추진하고 있음.
  - CBPR과 PRP의 인증을 받은 기업으로는 디지털 기술을 활용하여 데이터를 관리하고 솔루션을 제공하는 알리바바 클라우드, TRS 포렌식 등이 있으며, CBPR 인증만 받은 기업으로는 전자정부 서비스를 운영하는 크림슨로직과 보험회사인 그레이트 이스턴 등이 있음.

■ **[한국] 한국은 2017년에 CBPR 가입 승인이 이루어졌으며, 데이터 3법 개정으로 인해 개인정보보호위원회가 한국을 대표하는 개인정보보호법 집행기관[19]의 자격을 갖춤에 따라 2020년 10월 CPEA에 가입하였고, 2021년 3월 DESG-DPS 회의를 통해 2개의 기관(행정안전부, 방송통신위원회)에서 하나로 통일된 법 집행기관인 개인정보보호위원회로 승인됨.**

- 2019년 12월 한국인터넷진흥원(KISA: Korea Internet & Security Agency)이 CBPR 인증 기관으로 선정됨.
- KISA는 CBPR 인증의 본격 시행 전 제도 운영 절차에 대한 검증을 위해 국내 기업 2곳을 대상으로 CBPR 모의심사를 진행하였고, 이 과정에서 발견된 개선 필요 부분들을 보완해 완성도 높은 CBPR 인증제도의 운영 준비를 마무리함.[20]
  - KISA에서 운영하는 CBPR 인증심사 절차는 준비, 심사, 인증, 유지관리 등 4단계로 진행되며, 인증서가 발급되기까지는 기업에 따라 3~5개월 정도 소요됨.
  - 첫 번째 준비단계에서 준비해야 할 인증신청 제출 서류로는 APEC CBPR 인증신청서, 명세서, 인증 기준에 대한 자가평가지 등이 있으며, 제출한 서류를 토대로 인증범위 및 인증준비 상태 점검 등의 예비 점검을 진행함.
  - 두 번째 심사단계에서는 인증심사를 위해 심사팀을 구성하고, 심사를 통해 확인된 결함사항을 기업에 공유하여 보완조치 내역서를 제출할 수 있도록 함.
  - 세 번째 인증단계에서는 인증기관에서 심사결과보고서를 작성하고 인증위원회를 개최하여 인증 여부를 결정하고, 인증이 확인되면 기업에 인증서를 발급함.
  - 마지막 갱신심사는 인증서의 유효기간이 1년임에 따라 매년 한 차례씩 진행하며, 최초 인증심사와 동일과정을 거침.
- KISA는 CBPR 제도의 정식 운영을 위해 2021년도 하반기 중에 CBPR 가이드라인을 제공할 예정이며, 동 인증제도의 초기 정착을 위해 인증신청을 한 기업들을 대상[21]으로 인증수수료를 면제할 계획임.
- 또한 KISA는 국내 인증제도에 이미 가입한 기업이 쉽게 인증을 획득할 수 있는 환경을 제공하기 위해 정보보호 및 개인정보보호 관리체계(ISMS-P)[22] 인증 취득 기업은 CBPR 인증체계에 따른 운영 사전 준비사항을 생략할 수 있도록 함.

---

18) 싱가포르 IMDA, "APEC CBPR and PRP System Certification," Fact Sheet, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/PDP-Seminar-2019/2019-07-17-Fact-Sheet-for-CBPR-PRP-FINAL.pdf?la=en.

19) CBPR 가입 전제조건인 CPEA 가입은 행정안전부가 2011년, 방송통신위원회가 2014년에 가입하였고, 2016년에 행정자치부와 방송통신위원회가 공동으로 CBPR 인증제도 가입신청서를 제출함.

20) KISA CBPR 인증제도 담당자와 전화인터뷰 진행(2021. 8. 18).

21) 신용정보, 의료정보 등 다른 법률을 적용받는 기관들은 인증 대상에서 제외함.

22) ISMS-P는 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증 기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도임.

■ [대만] 대만은 2018년에 CBPR에 가입하였으며, 2021년 3월 DESG DPS 회의에서 정보산업진흥원(Institute for Information Industry)을 인증기관으로 승인하였고, CBPR 인증을 받은 기업은 아직 없음.[23)]

- 대만은 「개인정보보호법」 산하의 독립적인 규제 감독기관이 없어서 국가발전위원회(NDC: National Development Council)가 이를 관장하였으나, GDPR 등 해외 개인정보보호 체계에 대응하기 위해 2018년 7월부터 개인정보보호청(Personal Data Protection Office)을 독립적인 개인정보보호법 집행기관으로 설립함.
- 대만은 최근 CBPR 인증기관을 수립하여 인증 절차를 수립해 나가고 있음.

표 7. APEC CBPR 및 PRP 인증 기업 수(2021. 9. 1 기준)

구분	미국	싱가포르	일본	한국	대만
CBPR 인증 기업	36개	4개	2개	-	-
PRP 인증 기업	23개	2개	-	-	-

자료: 저자 작성.

3. APEC CBPR 발전에 관한 논의 동향

가. APEC CBPR의 상호운용성(Interoperability) 논의

■ [EU GDPR 적정성 결정] EU는 개인정보의 역외 이전이 가능하도록 GDPR(General Data Protection Regulation)[24)]에 적정성 평가(adequacy decision)[25)]를 하나의 법적 근거로 제시하였으며, APEC은 적정성평가와 CBPR 인증제도의 상호운용성의 논의가 지속되고는 있으나, CBPR의 개인정보보호 규제의 정도와 범위가 EU보다 낮고 협소하다는 평가[26)]를 받고 있음.

- APEC 회원국 중 일본, 캐나다, 뉴질랜드가 2021년 5월에 개최한 APEC 디지털무역정책대화(Digital Trade Policy Dialogue)[27)]에서 CBPR과 GDPR 적정성(adequacy)이 상호 배타적이지 않다고 언급되었으며, CBPR 인

23) APEC Document Database(2021/SOM1/CTI/028).

24) 유럽연합(EU) 「개인정보보호법(GDPR: General Data Protection Regulation)」은 EU 모든 회원국에 직접적으로 적용되는 개인정보보호법으로, 2018년5월 25일부터 발효됨. GDPR은 상설(Recital) 총 173개 조, 본문 총 11장 및 99개 조로 구성되어 있으며, 자연인에 대한 개인정보보호권을 담보하고(제1조 제2항), EU 역내에서 개인정보의 자유로운 이동을 보장(제1조 제3항)하는 것을 목적으로 함. GDPR은 EU 역내에 거주하는 자연인의 개인정보를 필요로 하는 모든 기업을 대상으로 하며, 무엇보다 규정 위반에 따른 벌금규모가 크다는 점이 특징임. 오태현, 강민지(2018), 「EU 개인정보보호법(GDPR) 발효: 평가 및 대응방안」, KIEP 오늘의 세계경제, Vol. 18, No. 19.

25) EU 개인정보의 국외 이전을 가능하도록 하는 법적 근거 중 하나임. GDPR에 언급된 국외 이전 가능한 법적 근거로는 적정성 평가, 구속력 있는 기업규칙(BCR), 기업간 계약체결을 통한 국외이전조치, 승인된 행동규약, 승인된 인증메커니즘 등이 있음.

26) Hunton Andrews Kurth, Privacy & Information Security Law Blog(2017. 8. 25), "APEC and EU Discuss Interoperability Between Data Transfer Mechanisms."

27) 미국이 2016 제3차 무역투자위원회 본회의에서 디지털무역 이슈를 논의하기 위한 무역정책대화를 캐나다, 호주와 함께 공동 제안함. 2018년부터 2021년까지 총 5회 개최하였으며, 주로 국경간 데이터 이전, 디지털 격차, 신기술에 관한 전문가 의견을 듣고 회원국간 토론을 진행함.

증제도에 가입한 일본이 2018년 GDPR이 발효된 이후 처음으로 적정성 결정(adequacy decision)[28]을 받았다고 밝힘.[29]

- ○ APEC 회원국 중 일본, 캐나다, 뉴질랜드가 EU GDPR 적정성 결정을 받았으며, 한국은 적정성 평가 절차를 밟고 있는 가운데 적정성 결정 최종 승인을 남겨두고 있음.

- 그러나 여전히 APEC 회원국 중 소수의 국가만이 GDPR 적정성 결정을 받았다는 점은 EU 역외 국가의 유럽 데이터 보호장벽이 높다는 것을 보여줌.
- 또한 2020년 7월 유럽사법재판소(CJEU)가 'EU-미국이 체결한 프라이버시 실드 프레임워크는 무효'라고 판결[30]함에 따라 미국 주도로 개발된 CBPR과 GDPR의 상호운용 가능성이 더욱 불투명해진 상황임.

■ [EU BCR] EU가 인증한 인증제도와 CBPR과의 상호운용에 대한 APEC-EU간 논의가 이루어진 바 있으나, 2019년 2월을 마지막으로 중단된 상태임.

- APEC ESEG-DPS는 2017년 8월 EU 집행위와 회의를 열어, EU GDPR의 구속력 있는 기업규칙(BCR: Binding Corporate Rules)[31]과 CBPR 준수 및 인증 요건을 비교하고 CBPR-BCR 상호운용성을 논의한 바 있음.[32]
- EU가 2019년 2월 발표한 개인정보보호 인증 메커니즘에 관한 연구보고서[33]는 CBPR이 개인정보보호 수준을 파악하는 인증 및 감독 메커니즘으로서의 좋은 예(good example)이나 GDPR 인증 표준(GDPR 제42조 인증 및 제43조 인증기관에 관한 규정)과 일치하지 않는다는 결론을 내림.
- GDPR은 원칙적으로 국경간 이전과 관련하여 개인정보보호의 관점에서 적정한 보호 수준을 갖춘 국가·기업으로의 이전만을 제한적으로 허용하고 있어,[34] CBPR 인증제도보다 더 높은 수준을 요건으로 하여 상호인증은 어려운 상황임.
  - ○ APEC CBPR은 개인정보를 수집하는 시점에 정보주체에게 개인정보의 위탁처리 또는 제3자에게 위탁하여 처리 또는 제공될 수 있음을 '고지'하는지(opt out 방식)를 인증 기준의 하나로 정하고 있으나, GDPR의 BCR은 승인을 위한 요건에서 원칙적으로 개인정보 이용 정보주체의 사전 동의(opt in 방식)를 필요로 하는 등 더 엄격한 요건 충족을 요구하는바 상호 인증이 어려울 것으로 보임.

28) 적정성 결정: EU 일반 「개인정보보호법(GDPR)」이 요구하는 수준과 동등한 수준의 개인정보 관련 법제를 보유하고 있는지를 확인하고 승인해주는 제도임. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#relatedlinks (검색일: 2021. 7. 29).

29) Digital Trade Policy Dialogue(2021. 5. 18), 중 미국 국제무역청 크리스토퍼 호프(Christopher Hoff) 부차관보 발표 내용.

30) 막스 슈렘스가 페이스북의 정보보호법 위반을 근거로 제기한 소송에 유럽재판소가 세이프하버 협정(Safe Havor Agreement) 무효화(슈렘스 I 판결)를 결정하자 프라이버시 쉴드 및 표준 개인정보보호 조항(Standard Contractual Clauses) 유효성 논란이 이어졌으며, 이에 2020년 7월 16일 CJEU는 프라이버시 실드를 통한 미국으로의 데이터 이전은 EU 법률의 요구 수준을 충족하지 못하므로 효력이 없는 것으로 판결함. 이를 슈렘스 II 판결(The Schrems II Decision)이라고 함. KISA(2020. 7), 「유럽사법재판소의 프라이버시 쉴드 무효 판결 분석」.

31) EU BCR은 구속력 있는 기업규칙으로 해당 국가가 GDPR 적정성 평가를 받지 않았을 때 EU 시민의 개인정보를 국외 이전할 수 있는 방법 중 하나로 다국적 기업이 EU 개인정보보호 규정에 부합하는 법적 구속력을 갖춘 내부 규칙을 수립하고 EU 회원국 감독기구(DPA)의 승인을 받을 경우 개인정보의 국외 이전을 허용함.

32) APEC Document(2017/SOM3/ECSG/DPS-EU/002), http://mddb.apec.org/Documents/2017/ECSG/DPS-EU/17_ecsg_dps-eu_002.pdf; APEC Document(2017/SOM3/ECSG/DPS-EU/004), http://mddb.apec.org/Documents/2017/ECSG/DPS-EU/17_ecsg_dps-eu_004.pdf; APEC Document(2017/SOM3/ECSG/DPS-EU/005), http://mddb.apec.org/Documents/2017/ECSG/DPS-EU/17_ecsg_dps-eu_005.pdf.

33) https://ec.europa.eu/info/sites/default/files/data_protection_certification_mechanisms_study_publish_0.pdf.

34) 적정성 평가(adequacy decision), 구속력 있는 기업규칙, 표준계약서, 인증(Certificate) 등을 통한 역외 이전이 가능한데(GDPR 제5장), 2021년 6월 16일 유럽연합(EU) 집행위원회는 적정성 평가 결정서 초기결정이 채택되었음을 공식 발표함. 연합뉴스(2021. 6. 17), 「EU, 한국 개인정보보호 적정성 평가 초안 발표…연내 최종결정」.

표 8. APEC CBPR과 EU BCR 접근방식 비교

구분	APEC CBPR	EU BCR
수립 목적	- 데이터의 자유로운 이전을 보장하여 전자상거래 활성화를 도모하기 위해 수립된 인증체계 - 기업의 개인정보보호 수준을 파악하기 위함. - 미국의 시장중심적인 관점에서 개발된 인증체계로 인증 기업이 자율적으로 개인정보를 보호하도록 함.	- 국경간 데이터 유통을 촉진하기 위해 개인정보를 역외 이전하려는 기업이 준수해야 할 사항(안전조치)을 적절한 수준으로 보호하고 있음을 선언하기 위함. - CBPR보다 정보주체의 권리와 기업의 책임성을 강화하고 있음. - 유럽 시민의 기본권을 보장하는 차원에서 개인정보보호 문제 접근
심사 방식	기업은 APEC CBPR 인증 기준에 대한 자체 평가지 등을 통한 자율규제(self-regulated) 방식을 통해 인증 절차 진행	EU GDPR의 법규 준수 여부를 심사
인증 기준	APEC 프라이버시 프레임워크(APF)에 포함된 9개 원칙을 바탕으로 만든 50가지 인증 기준에 대한 자체 평가지(intake questionnaire)[35]에 응답한 것을 토대로 심사	- EU BCR은 GDPR 제47조 제1항에서 법적 구속력이 있음을 명시 - 제47조 제2항의 14개 요건(반드시 BCR에 기재해야 하는 사항)을 충족할 것을 명시
피해 구제	- 기업이 획득한 인증 자격 박탈 - 인증기관에 대한 업무 정지	정보주체의 권리를 침해당했을 경우 법적인 청구권 인정[36]

자료: 저자 작성.

■ [ISMS-P] 우리나라의 정보보호 및 개인정보보호 관리체계 인증(ISMS-P: Personal information & Information Security Management System)[37]과 비교할 경우 CBPR의 필수인증 기준이 낮아 ISMS-P 인증을 받은 우리나라 기업은 CBPR의 인증을 받기 용이할 것으로 생각됨.

- ISMS-P는 주요 정보자산 유출을 사전에 예방하기 위해 조직이 자체적으로 운영하고 있는 정보보호 및 개인정보보호 시스템이 적합한지 인증하는 제도로, 정보보호 관리체계 수립 및 운영, 정보보호대책 요구사항, 개인정보 처리 단계별 요구사항 등 3개 분야의 102개 항목을 심사해 인증을 발급함.

※ ISMS 인증은 △정보통신망 서비스 사업자(ISP) △ 정보통신시설 사업자(IDC) △연간매출액 또는 세입이 1,500억 원 이상인 상급종합병원 및 재학생 수 1만 명 이상인 학교 △정보통신 서비스 매출액 100억 원 이상인 자 △정보통신 서비스 일평균 이용자 수가 100만 명 이상인 자,[38] ISMS-P는 선택으로, 2020년 말 기준 ISMS-P 인증서는 총 466건 발급됐으며, 464건이 유지되었고 ISMS 인증은 349건이 유지됨.

35) CBPR 홈페이지>문서>intake questionnaire, http://cbprs.org/documents/.
36) 기업규칙이 민사소송의 근거가 될 수 있음을 관련법규에 명시.
37) '개인정보보호 관리체계 인증(PIMS)'과 '정보보호 관리체계 인증(ISMS)'으로 개별 운영되던 인증체계를 하나로 통합한 '통합인증제도'로, 2018년 11월 7일부터 시행됨. KISA(한국인터넷진흥원) 'ISMS-P' 홈페이지, https://www.kisa.or.kr/business/infor/inforcert_2.jsp.
38) 의무대상자가 ISMS 인증 미이행 시 3,000만 원 이하의 과태료를 부과할 수 있음(「정보통신망법」 제76조).

표 9. ISMS-P 인증항목

인증		구분	인증 기준 (해당 분야 개수)	
ISMS-P (102)	ISMS (80)	관리체계 수립 및 운영(16)	1.1 관리체계 기반 마련(6)	1.2 위험관리(4)
			1.3. 관리체계 운영(3)	1.4 관리체계 점검 및 개선(3)
		보호대책 요구사항 (64)	2.1 정책, 조직, 자산 관리(3)	2.2 인적보안(6)
			2.3 외부자 보안(4)	2.4 물리보안(7)
			2.5 인증 및 권한 관리(6)	2.6 접근통제(7)
			2.7 암호화 적용(2)	2.8 정보시스템 도입 및 개발 보안(6)
			2.9 시스템 및 서비스 운영관리(7)	2.10 시스템 및 서비스 보안관리(9)
			2.11 사고 예방 및 대응(5)	2.12 재해복구(2)
	-	개인정보 처리단계별 요구사항(22)	3.1 개인정보 수집 시 보호조치(7)	3.2 개인정보 보유 및 이용 시 보호조치(5)
			3.3 개인정보 제공 시 보호조치(4)	3.4 개인정보 파기 시 보호조치(3)
			3.5 정보주체 권리보호(3)	

자료: KISA(한국인터넷진흥원), 'ISMS-P 제도소개' 홈페이지, https://isms-p.kisa.or.kr/main/ispims/intro/.

나. 자유무역협정 내 APEC CBPR의 인정

■ [USMCA] USMCA (United States-Mexico-Canada Agreement)은 개인정보보호 법적 체계를 마련함에 있어서 고려할 수 있는 국제 원칙과 지침으로 APF를 예시하고 있으며, APEC CBPR이 국경간 정보 이전 촉진에 효과적인 메커니즘임을 인정하고 있음.

- USMCA는 개인정보보호를 위한 법적 체계 개발에 있어 고려해야 하는 국제 원칙 및 기준의 예로 'APEC 프라이버시 프레임워크(APF)' 및 'OECD의 프라이버시 보호 및 국경간 개인정보의 이전에 대한 가이드라인(2013)' 등을 구체적으로 예시함.[39]
  - ○ TPP (Trans-Pacific Strategic Economic Partnership)는 개인정보보호를 위한 법적 체계 채택 또는 유지를 규정하며, 개인정보보호 법적 체계 개발에 있어 관련 국제기구의 원칙과 지침을 고려할 것을 규정하고 있으나,[40] USMCA에서는 고려해야 하는 원칙 및 지침을 예를 들고 있으며 여기에 APEC APF가 포함됨.
- USMCA는 'APEC CBPR'이 개인정보를 보호하면서 국경간 정보 이전을 확대하는 데 유효한 메커니즘임을 인정한다는 내용을 명시함.[41]
  - ○ TPP 및 USMCA는 각 당사국이 국가별로 개인정보의 보호를 위한 법적 접근이 다를 수 있다는 점을 인정하며, 이러한 다른 체제간 상호운용성을 증진하기 위한 메커니즘을 개발하는 것을 장려하고 있으며, 각국이 당사국의 메커니즘 정보를 교환하려는 노력과 상호운용성 증진하기 위한 방안을 강구하기 위해 노력할 필요성을 규정함.[42]

39) USMCA 제19.8조(개인정보보호) 제2항.
40) TPP 제14.8조(개인정보보호) 제2항.
41) USMCA 제19.8조(개인정보보호) 제6항.
42) TPP 제14.8조(개인정보보호) 제5항 및 USMCA 제19.8조(개인정보보호) 제6항.

■ [DEA] 싱가포르-호주 디지털경제협정(SADEA: The Singapore-Australia Digital Economy Agreement)에도 USMCA와 유사한 조항이 포함되어 있음.

- USMCA와 유사하게, 개인정보보호를 위한 법적 체계 개발 시 고려해야 할 국제기구의 원칙과 지침으로 'APEC CBPR' 시스템과 'OECD의 프라이버시 보호 및 국경간 개인정보의 이전에 대한 가이드라인(2013)' 등을 규정하고 있음.[43]
  - ○ USMCA에서는 개인정보보호를 위한 법적 체계 개발 시 고려해야 할 원칙 및 지침으로 APEC APF를 예시하였으나, DEA에서는 APEC APF를 바탕으로 개발된 APEC CBPR 시스템을 구체적으로 명시하고 있음.
- 또한 DEA는 CBPR 시스템이 개인정보를 보호하는 동시에 국경간 정보 이전을 용이하게 하는 유효한 메커니즘이라는 것을 규정하고 있음.[44]
  - ○ 단 CBPR 시스템이 개인정보보호에 관한 당사국의 법률과 규정을 대체하거나 변경하지 않음을 인정한다고 규정함으로써, CBPR 시스템이 도입되더라도 국내 「개인정보보호법」이 유지됨을 명확히 함.[45]
- 추가적으로 SADEA는 당사국이 산업별 CBPR 시스템에 대한 인식 개선과 참여를 목적으로 CBPR 시스템을 공동으로 홍보하기 위해 노력할 것을 규정함.[46]

4. 시사점

■ APEC CBPR은 자율적 참여를 기반으로 운영되는 인증체제로, APEC 회원국 정보의 국외 이전에 대한 입장차로 인해 제도 확산이 늦어지고 있으며, 특히 미국 주도로 APEC 회원국 이외 다른 국가로 확대하는 방안에 대한 논의가 진행되고 있음.

- 현재 APEC CBPR 가입국은 우리나라를 비롯하여 미국, 멕시코, 일본, 캐나다, 한국, 호주, 싱가포르, 대만, 필리핀 등 9개국으로, APEC 회원국에 한하여 CBPR 가입을 신청할 수 있으며, APEC 심의를 통해 가입이 결정됨.
  - ○ APEC 회원국인 중국은 최근 「데이터보안법」을 통과하여 '주무부서의 승인을 거치지 않을 경우 중국 내 조직이나 개인이 외국의 사법 또는 법 집행기구에 중화인민공화국 국경 내에 보존된 데이터를 제공하지 못하도록 한 바,[47] 자유로운 정보의 국외 이전을 위한 APEC CBPR로의 가입에 대해 현재로서는 관심이 적을 것으로 보임.
    - ※ 비록 중국은 RCEP에서 국경간 정보 이전 및 데이터설비의 위치에 대한 규정을 받아들였으나, 해당 조항은 자기 결정 예외조항으로 인해 당사국의 재량이 상당히 크게 작용할 것으로 보여 중국이 자유로운 국경간 정보 이전을 지지하는 방향으로 선회했다고 보기 어려움.[48]

43) SADEA 제17조(개인정보보호) 제2항.
44) SADEA 제17조(개인정보보호) 제8항.
45) SADEA 각주12.
46) SADEA 제17조(개인정보보호) 제9항.
47) 「데이터보안법」 제36조(중국은 2021년 6월 12일 「데이터보안법」을 통과시키고 2021년 9월부터 시행할 방침).
2017년 6월부터 시행한 「사이버보안법」 제37조에 따르면 핵심정보기초시설의 운영자는 중화인민공화국 경내에서 운영 중에 수집 또는 생산한 개인정보와 중요 데이터를 경내에 보존해야 하고, 업무상 경외 제공이 명백히 필요한 경우에는 국가 인터넷 정보부서와 국무원 관련 부서가 제정한 방법에 따라 보안평가를 실시하는 한편 법률, 행정법규에 별도의 규정이 있는 경우에는 그 규정에 따라야 할 것을 규정하나, 2021년 9월부터 시행될 예정인 「데이터보안법」은 모든 데이터의 수집, 저장, 사용, 가공, 전송, 제공, 공개 등에 대해 당국이 개입할 수 있는 통로를 마련하였으며, 국가와 관련한 핵심정보를 잘못 취급하거나 국가안보상 민감한 데이터를 국외로 유출한 기업의 경우 면허 박탈, 최대 160만 달러의 과태료 부과가 가능하고 중국정부의 승인 과정을 거치지 않고 외국 사법당국에 디지털 정보를 제공한 경우 최고 500만 위안의 벌금 부과 또는 영업정지도 가능함.

- 미국은 CBPR을 APEC으로부터 독립시켜 CBPR 회원국 확대를 모색하고 있으나 중국, 러시아 등의 반대가 예상되는바(APEC 의사결정 방식: 컨센서스 형성), CBPR의 독립 운영기구화는 어려울 것으로 예상됨.
  - 다만 APEC CBPR이 가입국을 확장하여 인도, 중남미, 아프리카연합 등으로 확장할 경우 CBPR 인증의 효용이 커질 수 있음.[49]

■ **우리나라의 인증기관인 KISA는 2021년 하반기 중에 CBPR을 정식 운영할 계획으로, 글로벌 인증 획득을 통한 대외 신뢰도 제고를 추구하는 기업[50]은 CBPR 신청을 고려할 필요가 있음.**

- 아태지역을 비롯한 국외에 개인정보를 이전하거나 이전 받아 처리하는 기업 및 아태지역에 계열사, 자회사 등이 위치하는 기업, 글로벌 공동인증 기준인 CBPR을 전 사에 적용하여 통일된 정책 수립을 추구하는 기업 등의 경우 APEC CBPR을 통해 글로벌 기준의 개인보호 체계를 수립한 것으로 인정받을 수 있으며, 글로벌 인증 획득을 통해 대외 신뢰도를 제고할 수 있을 것으로 보임.
- 또한 CBPR을 국가 공인 인증으로 승인한 국가들이 있어, CBPR 가입 시 이러한 국가에 있어서는 정보주체의 동의 등 별도의 추가적인 절차 없이 개인정보를 이전 받아 처리할 수 있음.
  - 일본,[51] 싱가포르[52] 등은 CBPR을 자국의 「개인정보보호법」과 동등한 수준의 보호체계로 인정하여 이를 법에 반영하였고, CBPR 인증 기업은 정보주체 동의 등 추가적인 절차 없이 개인정보의 국경간 이전이 가능하도록 하고 있음.
- 우리나라의 인증기관인 KISA는 2021년 하반기 중에 CBPR을 정식 운영할 방침으로, 제도의 초기 정착을 위해 인증 신청 수수료를 면제해주고, ISMS-P/ISMS 인증을 받은 기업에 대해서는 CBPR 인증 절차를 간소화할 예정임.
  - 특히 ISMS 인증 의무대상자들은 추가적으로 CBPR 가입에 부담이 낮을 것으로 예상됨.

■ **궁극적으로 APEC CBPR의 발전을 위해서는 다른 인증제도와의 상호운용성 증대로 인한 실효성 강화 및 국가공인 인증 및 글로벌 대표 인증체계로 인정받기 위한 노력 등 정부의 지속적인 노력이 필요할 것으로 보임.**

- 현재는 CBPR-BCR의 상호운용성 논의를 위한 APEC 내 비공식 회의가 중단된 상태이나, APEC CBPR을 GDPR에서 인정하는 하나의 인증 메커니즘이 되도록 상호운용 논의를 지속적으로 진행할 필요가 있음.
  - GDPR 제42조에서 개인정보보호 인증 메커니즘, 인장 또는 마크의 수립을 장려해야 한다고 명시하고 있으나 CBPR과 GDPR의 상호운용 논의는 설립목적(관점), 인증 기준, 법적 구속력 여부 등의 차이와 최근 EU와 미국이 체결한 프라이버시 실드 프레임워크에 대한 유럽사법재판소의 무효 판결 등으로 인해 불투명해진 상태임.
  - 그러나 안전한 개인정보보호장치 아래 데이터 유통을 촉진한다는 취지는 유사하므로, 상호운용을 위한 틀을 구축하기 위한 추가적인 노력이 더해져야 할 것으로 보임.

---

48) RCEP 제12.15조 제2항은 전자적 수단에 의한 정보의 국경간 이전이 적용대상인의 사업을 수행하기 위한 것인 경우 그러한 행위를 금지하지 않도록 규정하고 있으나, 동조 제3항에서 정당한 공공정책 목표를 달성하기 위하여 당사국이 필요하다고 간주하는 제2항과 불합치하는 모든 조치 및 당사자의 필수적인 안보이익 보호를 위하여 그 '당사자가 필요하다고 간주하는' 모든 조치를 채택하거나 유지할 수 있도록 하여 예외의 판단에서 당사국의 재량을 넓혀 예외 인정이 용이하도록 하였음. 또한 RCEP의 전자상거래 챕터는 19장의 분쟁해결을 이용할 수 없음.

49) 박노형(2020)에 따르면 CBPR 가입 예상 국가 중 우리나라의 전자상거래 수출·수입 대상국가 상위 50개국에 포함된 국가(베트남, 태국, 캄보디아, 인도, 브라질, 남아프리카공화국, 튀니지 등)가 독립된 CBPR에 가입하게 될 경우 전자상거래 분야에 있는 우리 기업에도 긍정적일 것으로 보임.

50) 우리나라의 CBPR 가입 근거 법률인 「개인정보보호법」 적용 대상 기관만 APEC CBPR 인증 신청이 가능함.

51) https://www.ppc.go.jp/files/pdf/CBPR_lets_think_about_it.pdf.

52) Singapore Now Recognises APEC CBPR and PRP Certifications Under PDPA, https://www.pdpc.gov.sg/news-and-events/announcements/2020/06/singapore-now-recognises-apec-cbpr-and-prp-certifications-under-pdpa.

- 향후 CBPR을 개인정보보호위원회가 지정하는 인증제도 중 하나로 고려해볼 수 있는지 혹은 CBPR에 반영되지 않은 국내 「개인정보보호법」 요소들을 CBPR에 반영할 수 있는지를 검토하고, 국경간 정보 이전에 있어 국내법에 상응하는 혜택을 인증 기업들에 부여하는 방향으로 나아갈 필요가 있음.
  - 우리나라는 「개인정보보호법」 개정안에 제28조의8(개인정보 국외 이전) 제2항에서 '4. 개인정보를 국외 이전 받는 자가 제32조의2에 따른 개인정보보호 인증 등 보호위원회가 지정하는 인증을 받은 경우, 정보주체로부터 별도의 동의를 받은 경우가 아니라도 개인정보를 국외 이전할 수 있도록' 하고 있는데, 향후 적절할 경우 CBPR을 보호위원회가 지정하는 인증 중 하나로 고려해볼 수 있을 것임.
  - CBPR을 우리나라의 「개인정보보호법」과 동등한 수준의 인증체계로 인정하는 데 무리가 있다면, 국내 법제 중 CBPR에 반영되지 않은 요소들을 식별하여 CBPR 인증 기준 중 필수항목에 포함할 수 있도록 목소리를 내어, CBPR 인증 기업이 개인정보 국경간 이전에 이점을 얻을 수 있는 방향으로 나아갈 필요가 있음.
- USMCA, SADEA 등에서 개인정보보호를 위한 법적 체계 개발 시 고려해야 할 국제기구의 원칙과 지침 중 하나로 규정하고 있듯, FTA 및 디지털무역협정 등에 APEC CBPR을 포함하여 글로벌 대표 인증체계로 발돋움하는 데 기여할 필요가 있음.
  - 한국은 디지털경제에 선제적으로 대응하기 위해 싱가포르와 디지털동반자협정을 연내 체결할 방침으로,[53] DEA 내용 고려 시 CBPR 시스템이 개인정보를 보호하는 동시에 국경간 정보 이전을 용이하게 하는 유효한 메커니즘이라는 것을 인정하고, CBPR 시스템에 대한 인식 개선과 참여를 목적으로 CBPR 시스템을 공동으로 홍보하기 위해 노력해야 한다는 등의 내용을 포함할 필요가 있음.

■ **APEC은 앞으로도 소비자들이 신뢰할 수 있고, 기업들에 큰 부담이 없으면서도, 안전하고 자유로운 국경간 데이터 이전에 대한 다자 차원의 통일된 규칙을 수립하기 위한 환경을 구축하기 위해 정부, 업계, 학계 등이 함께 참여하는 다중이해관계자간 토론의 장을 지속해서 제공할 필요가 있음.**

- 다른 국제회의에서도 데이터 국외 이전과 관련해 구체적인 성과를 거두지 못하고 있는 상황에서 아이디어 인큐베이터 역할[54]을 하고 있는 APEC에서 정책토론의 자리를 마련하여 의견을 수렴하고, 역량개발 사업을 통해 개발도상 회원국의 「개인정보보호법」 체계 구축 조화 등의 지원이 요구됨.
- APEC은 APEC만의 비구속적(non-binding) 특징을 살려, WTO 등 글로벌 차원에서 디지털무역 제약 이슈(데이터 국외 이전 등)와 관련된 구속적인 규정을 협상하는 와중에 동일한 주제로 APEC 회기 내 토론의 장을 제공하여 회원국간 이견이 있는 접근방식을 조화시켜 나갈 필요가 있음. KIEP

53) 서울경제(2021. 6. 14), 「'디지털통상' 영토도 넓힌다… 싱가포르와 연내 협정 체결」, https://www.sedaily.com/NewsVIew/22NMV4H3F7.
54) 예를 들면 APEC은 해외출장이 잦은 기업인들을 위해 비자 면제, 공항 내 전용 수속레인을 통해 신속한 출입국을 보장해주는 제도(ABTC: APEC Business Travel Card)에 대한 아이디어를 제안하여 제도를 도입하였으며, 이를 통해 APEC 회원국간 경제교류를 활성화함.

부록 1. CBPR 인증제도 승인 기업

국가	no.	신청 기업	책임 기관	승인 날짜
미국	1	7.ai, Inc.	TRUSTe(TrustArc)	12/2018
	2	Apple Inc.		09/2014
	3	Assurant, Inc.		04/2020
	4	Asurion, LLC.		03/2017
	5	BitSight Technologies, Inc.		05/2021
	6	Box, Inc.		07/2014
	7	Cisco Systems, Inc.		07/2016
	8	Credly, Inc.		02/2020
	9	Crowley Webb &Associates, Inc.		10/2018
	10	DoubleVerify, Inc.		06/2021
	11	Electronic Arts		04/2017
	12	General Electric Company		12/2018
	13	Hewlett Packard Enterprise Company		11/2015
	14	HP Inc.		10/2014
	15	IBM		08/2013
	16	Infor		06/2019
	17	Johnson Controls, Inc.		12/2020
	18	Kobre &Kim LLP		09/2017
	19	LogMeIn, Inc.		04/2020
	20	Mastercard International, Inc.		05/2019
	21	Merck &Co., Inc., Kenilworth, NJ. USA		10/2013
	22	Organon & Co.		05/2021
	23	PGA Tour		05/2018
	24	Rackspace		01/2017
	25	Reltio Inc.		02/2019
	26	Rimini Street, Inc.		10/2014
	27	The Ultimate Software Group		09/2016
	28	Virgin Pulse, Inc.		08/2019
	29	Workday, Inc.		03/2014
	30	World Wrestling Entertainment, Inc.		12/2017
	31	Yodlee, Inc.		12/2013
	32	Ziff Davis, LLC		08/2014
	33	ServiceNow, Inc.	Schellman & Company, LLC	8/14/2020
	34	Slack Technologies, Inc.		12/2019
	35	Talkdesk, Inc.	NCC Group Security Services, Inc.	05/2021
	36	Herbalife Nutrition	BBB National Programs	07/2021
싱가포르	1	Alibaba Cloud (Singapore) Private Limited	Infocomm Media Development Authority (IMDA)	04/2021
	2	CrimsonLogic Pte Ltd		04/2020
	3	The Great Eastern Life Assurance Company Limited		09/2020
	4	TRS Forensics Pte Ltd		05/2021
일본	1	Intasect Communications, Inc.	JIPDEC	12/2016
	2	Paidy inc.		12/2018

자료: http://cbprs.org/ 참고하여 저자 작성.

부록 2. PRP 인증제도 승인 기업

국가	no.	신청 기업	책임 기관	승인 날짜
미국	1	Adobe Inc.	TRUSTe(TrustArc)	11/2019
	2	Apple Inc.		10/2019
	3	Asurion, LLC.		10/2019
	4	BitSight Technologies, Inc.		05/2021
	5	Box, Inc.		09/2018
	6	DoubleVerify, Inc.		06/2021
	7	Epiq System, Inc.		07/2020
	8	General Electric Company		12/2018
	9	Johnson Controls, Inc.		
	10	Lineal Services		02/2021
	11	LogMeIn, Inc.		04/2020
	12	Mastercard International, Inc.		05/2019
	13	MD Connect, Inc.		10/2018
	14	Salesforce.com Inc. and its Affiliates		11/2019
	15	Virgin Pulse, Inc.		08/2019
	16	Workday, Inc.		09/2018
	17	Yodlee, Inc.		09/2018
	18	Zycus, Inc.		03/2021
	19	Cisco Systems, Inc.	BBB National Programs	08/2019
	20	DocuSign Inc.	Schellman & Company, LLC	9/09/2020
	21	Okta, Inc.		7/23/2020
	22	Slack Technologies, Inc.		12/2019
	23	Talkdesk, Inc.	NCC Group Security Services, Inc.	05/2021
싱가포르	1	Alibaba Cloud (Sigapore) Private Limited	Infocomm Media Development Authority (IMDA)	04/2021
	2	TRS Forensics Pte Ltd		05/2021

자료: http://cbprs.org/ 참고하여 저자 작성.

참고문헌

[국문자료]

김현수, 강민지, 이정은, 이용규. 2019.『주요국의 혁신성장 정책과 제도: 미국, 유럽, 일본을 중심으로/제2편 주요국의 혁신성장 제도』. 연구보고서 19-15-2.

박노형. 2020.「APEC 개인정보보호 인증체계(CBPR) 현황 점검 및 非 APEC 국가로 CBPR 확대시 한국에 미치는 영향 검토」. 외교부.

오태현, 강민지. 2018.「EU 개인정보보호법(GDPR) 발효: 평가 및 대응방안」. KIEP 오늘의 세계경제, Vol. 18, No. 19.

이규엽, 강민지. 2021.「WTO 전자상거래 협상 전망과 한국의 과제」. KIEP 오늘의 세계경제, Vol. 21, No. 3.

개인정보보호위원회. 2020.『2020 개인정보보호 연차보고서』.

한국인터넷진흥원. 2020.『2020 EU 일반개인정보보호법 가이드북』.

한국정보화진흥원. 2014.『국제기구의 개인정보보호 인증제도간 인증항목 비교(번역본)』.

[영문자료]

IMDA. “APEC CBPR and PRP System Certification.” Fact Sheet. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/PDP-Seminar-2019/2019-07-17-Fact-Sheet-for-CBPR-PRP-FINAL.pdf?la=en.

UNCTAD. 2021. “Joint Statement Initiative on E-Commerce (JSI): Economic and Fiscal Implications for the South.” UNCTAD Research Paper No. 58. https://unctad.org/system/files/official-document/ser-rp-2021d1_en.pdf.

UNCTAD. 2021. Estimates of Global E-Commerce 2019 and Preliminary Assessment of COVID-19 Impact on online retail 2020.

USTR. 2019. “FACT SHEET on U.S.-Japan Trade Agreement.” https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/september/fact-sheet-us-japan-trade-agreement.

WTO. 2021. 5. 20. JOINT STATEMENT ON E-COMMERCE, E-commerce negotiations advance, delve deeper into data issues. https://www.wto.org/english/news_e/news21_e/jsec_20may21_e.htm.

[온라인 자료]

개인정보보호위원회 개인정보보호 국제협력센터 웹페이지. https://www.privacy.go.kr/pic/nation_usa.do.

서울경제. 2021. 6. 14.「‘디지털통상’ 영토도 넓힌다… 싱가포르와 연내 협정 체결」. https://www.sedaily.com/NewsVIew/22NMV4H3F7.

연합뉴스. 2020. 8. 21.「美 국제 데이터 유통서 中 제외 노려…APEC 규칙 개정 제안」. https://www.yna.co.kr/view/AKR20200821058900073.

연합뉴스. 2021. 6. 17.「EU, 한국 개인정보보호 적정성 평가 초안 발표…연내 최종결정」. https://www.yna.co.kr/view/AKR20210617071500530.

APEC Document Database. http://mddb.apec.org/Pages/default.aspx.

CBPR 홈페이지. http://cbprs.org/.

IMDA- APEC CBPR 소개 웹페이지. https://www.imda.gov.sg/cbpr.
KISA(한국인터넷진흥원). “ISMS-P 제도소개” 홈페이지. https://isms-p.kisa.or.kr/main/ispims/intro/.
KISA(한국인터넷진흥원). “ISMS-P” 홈페이지. https://www.kisa.or.kr/business/infor/inforcert_2.jsp.

[협정문]

SADEA(싱가포르 호주간 디지털 경제 협정, Digital Economy Agreement)
TPP(환태평양 경제동반자 협정, Trans-Pacific Strategic Economic Partnership)
RCEP(역내 포괄적 경제 동반자 협정, Regional Comprehensive Economic Partnership)
USMCA(미국·멕시코·캐나다 협정, United States-Mexico-Canada Trade Agreement)