
국외출장 결과 보고서

- 개인정보보호 규제기관 라운드테이블 등 참석 -

2017. 5.



방송통신위원회

Korea Communications Commission

목 차

I. 출장 개요	2
II. 출장 결과	3
1. 개인정보보호 규제기관 라운드테이블	3
2. APEC CBPR 국제워크숍	7
3. 관계기관 실무회의 내용	9
III. 동향 및 시사점	13

1. 개요

□ 출장 목적

- APEC CBPR 도입·운영 관련 한국의 현황과 정책 발표 및 회원국의 추진 현황과 애로사항 공유 등 CBPR 정착·활성화를 위한 과제 논의
 - APEC CBPR을 도입하여 운영 중인 미국과 일본 정부 및 인증기관(AA, Accountability Agent)과 실무회의를 통해 국내 CBPR 도입 시 활용
- ※ APEC CBPR(Cross-Border Privacy Rules system, 국경 간 프라이버시 규칙) : 기업의 개인정보보호 수준을 평가하여 인증하는 글로벌 인증체계로, APEC이 전자상거래 활성화와 회원국 간 안전한 개인정보 이전을 위해 개발('11년)

□ **출장기간 및 방문국가** : '17. 5. 9.(화)~5. 12.(금) [3박 4일] / 일본 도쿄

□ **출장자 (2명)** : 개인정보보호협력팀 김기석 팀장, 이정수 사무관

□ 주요 일정

일 자	주요 일정
'17. 5. 9(화)	한국(김포) 출발 → 일본(도쿄) 도착
'17. 5. 10(수)	APEC CBPR 규제기관 라운드테이블 참석
'17. 5. 11(목)	APEC CBPR 국제워크숍 참석
'17. 5. 12(금)	APEC CBPR 인증기관(TRUSTe, JIPDEC) 실무회의 진행
	일본(도쿄) 출발 → 한국(김포) 도착

□ 선물수령 관련

- 선물 수령 여부 : X
- 선물 신고 여부 : X

1

개인정보보호 규제기관 라운드테이블

□ 일 정 : '17. 5. 10.(수) 14:00-16:00 / Google Japan

□ 참석자 : 한국(방통위, 행자부, KISA), 미국(상무성, TRUSTe), 일본(경제산업성, 개보위, JIPDEC), 대만(외교부) 등 주요국 규제기관 및 CIPL (행사주관, 글로벌 컨설팅사), 구글, HP, Apple 등 30여명

※ TRUSTe와 JIPDEC은 각각 미국과 일본의 APEC CBPR 인증기관으로, APEC 승인을 받아 CBPR 인증 업무를 수행

□ 주요 논의내용

-
- 각국의 CBPR 도입(준비) 현황을 소개하고 주요 쟁점에 대해 각국 정부 및 이해관계자들의 입장 공유 및 대안 모색
 - 인증 유인 확대, 각국 기존 제도와의 조화, CBPR의 타 인증제도와 상호운용성 등
-

《 주요국 추진현황 공유 》

- (한국) CBPR 신청서 제출('16.12월) 이후 APEC 심사 절차 중에 있으며, CBPR 운영 정책 논의 및 인증기관 신청 준비 현황 소개
- 국내 법규와 CBPR의 조화, 국내 인증제도와의 연계, CPBR 상호운용성 등 주요 쟁점을 제시하고, EU 적정성 평가를 동시에 진행하고 있음을 언급
- (일본) '16.1월 JIPDEC(일본 정보·경제사회추진협회)이 인증기관으로 APEC 승인을 받아, '16.12월 1개 기업(Intasect, 여행자정보처리사) 인증

- CBPR 홍보를 위해 미국과 공동 국제워크숍 및 세미나('16.10월)를 개최했으며 기업관계자 등 200여 명이 참여함
- 개정 개보법 시행('17.5.30)을 앞두고 하위 법령 준비 등으로 EU 적정성 추진을 적극적으로 추진하지 못하고 있는 상황
- o (대만) 대만은 개인정보보호기관이 아닌 외교부가 CBPR 도입을 추진하고 있으며, 국내 세미나에 이어 '17.10월에 APEC 편딩을 받아 국제워크숍을 개최하여 적극적으로 제도 홍보를 할 예정
- 대만 역시 기존 국내법과 인증제도 등과 CBPR의 조화를 모색할 수 있는 방법을 논의중이며, 기업 참여를 높일 수 있는 방법을 찾는 것이 중요하다고 언급
- o (미국) TRUSTe는 Apple, HP 등 20개 기업에 인증을 발급했으며, 현재 10개 기업이 인증 절차 중에 있음
- 미국은 PRP(Privacy Recognition for Processor, 수탁사 개인정보보호인증)* 신청서를 지난 2월에 제출하여 APEC 심사 중에 있음
- * CBPR은 정보관리자(controller)를 대상으로, PRP는 정보관리자로부터 정보를 수탁받아 처리하는 수탁처리자(processor)를 대상으로 개인정보보호수준 인증
- 제도 확산을 위해 여러 홍보 전략을 고민중이며, 다른 인증제도와 상호운용성(interoperability) 측면에서 CBPR을 GDPR 상 '공인된 인증'으로 인정할 수 있을지 EU 집행위원회와 논의 중임
- ※ GDPR(General Data Protection Regulation) : '16.5월 통과된 ('18.5월 발효) 유럽 개인정보보호법으로, 기존의 규칙(directive)보다 구속력과 보호수준이 강한 것으로 평가되며, 개인정보 역외이전 허용 조건으로 '공인된 인증 획득' 추가

《 자유토론 내용 요지 》

□ 기업 참여 유인(benefit, incentive) 확대

- Apple, HP, CISCO 등 CBPR 인증기업들은 ①상호운용성 ②고객 신뢰 확보 ③계열사 간 통일된 규범·원칙 확립 ④규제기관에 대한 기업 책임성 확보 ⑤규범 준수 비용 절감 등의 참여유인 소개

※ 구글은 CBPR 인증신청을 긍정적으로 검토 중이라고 밝혔고, CBPR에 대한 인지도가 아직 낮아 미국 정부는 적극적인 홍보의 필요성 공감

- 대부분 하나의 회사가 정보관리자(controller)이면서 수탁처리자(processor)로서 두 가지 역할을 맡는 경우가 많기 때문에, CBPR 인증을 받으면 기업 간 신뢰도 확보에도 큰 도움이 될 수 있음

□ 각국 기존 법규 및 인증제도와와의 조화

- 글로벌 사업자들은 각국 (사전)동의 원칙을 인정하나, 이용자 인지가 명확한 경우 동의가 불필요하다는 입장 표명

- HP는 멕시코가 CBPR에 국내 법규 반영을 추진중인 것으로 알고 있으며, CBPR에 국내법의 모든 요구사항을 반영하는 것을 반대

- 일본 JIPDEC은 기존의 P-Mark*와 CBPR은 서로 다른 목적을 지닌 별개의 제도로 추진한다고 밝힘

* P-Mark : '98.4월부터 시행된 일본의 개인정보보호 자율 인증제도이며 현재 까지 총 21,307개 기업이 인증마크를 획득함(수행기관 JIPDEC)

- 미국은 CBPR과 Privacy Shield(EU-미국 개인정보 국외이전 허용 협정에 따른 인증)가 유사하므로, 이미 Privacy shield에 등록된 2,000여 기업이 손쉽게 CBPR을 취득할 수 있을 것이라고 발언

□ 중소기업을 위한 제도적 장치

- APEC은 경제공동체로서 중소기업 간 교역확대를 강조하고 있으며, 그 일환으로 중소기업이 CPBR에 참여할 수 있는 방법 강구 중
 - 필리핀은 중소기업을 위한 개인정보보호 인증(SME certifier) 시스템 도입을 고려하고 있음
 - 중소기업 참여진작의 관점에서 CBPR 인증기준에 개별 국가기준을 추가하는 것은 비용부담을 발생시키므로 지양해야 한다는 주장
- 미국 상무성은 개인정보보호 수준 향상을 위해 중소기업이 사용할 수 있는 개인정보보호 기술을 제공하는 방안을 고려중임

□ 인증제도 간 국제적 상호운용

- EU는 '17.1월 집행위원회(EC) 브리핑을 통해 BCR* 등 EU가 인정하는 인증제도와 CBPR과의 상호 운용에 대해 공식적으로 관심을 표명하였고, 향후 상호운용 관련 추진에 대해 긍정적으로 전망

* BCR(Binding Corporate Rules, 구속적 기업규칙) : 개인정보 보호체계에 대한 EU의 인증제도로, 글로벌 기업이 구속력 있는 개인정보보호체계를 구축하여 EU 승인을 받으면 해당 기업은 EU 시민의 개인정보를 역외이전할 수 있음

- CIPL, 미 상무성 등은 한국·일본의 EU 적정성평가 추진에 대하여 개인정보 국외이전의 방법이 여러 가지가 있음을 고려해야 하며 국가단위의 인정보다 기업의 실질적 규범준수가 중요하다고 주장하며 EU 적정성평가가 최선의 방향이 아닐 수 있다고 강조

※ 실질적으로 과거 EU 적정성평가를 받은 국가의 수가 얼마 되지 않았으며, 이미 적정성평가를 받은 국가도 재평가를 받아야한다는 점을 들어서 적정성평가 제도의 실효성에 의문을 제기함

- 일 정 : '17. 5. 11.(목) 10:00-17:00 / 일본 국회의사당
- 참석자 : 한국, 일본, 미국, 대만 정부 및 산학연 전문가 등 50여명
- 주요 논의내용

-
- 일본의 개인정보보호법 개정 내용 및 APEC CBPR 도입에 따른 변화 논의
 - 빅데이터·머신러닝·인공지능 등 신규 기술과 익명가공정보 및 익명화 조치 등 개인정보보호 규제의 조화 방안 논의
-

《 Session1 : 일본 개보법과 국경 간 정보이전 》

- (일본 개보법 개정 내용) '15년 개보법 개정을 통해 독립 위원회 설립 근거 마련, 개인정보 개념 명확화, 개인정보 활용을 위한 익명화 규정 및 국외 이전 규정 신설, 개인정보 제3자 제공에 대한 기록관리, 개인정보 유출 통지 신설 등 마련
 - 개정법 세부 이행 지침을 위해 개보위 시행명령(PPC order, '16.10월), 가이드라인(PPC guideline, '16.11월) 등을 마련함
- (기업의 개인정보 보호·활용) 빅데이터 환경에서 기업은 다양한 개인정보 활용의 기회를 가지는 동시에 단순 프라이버시 법규 준수 이상의 책임감을 가지고 있으며, 정보 이용에 대한 이용자 투명성 확보를 위한 노력을 기울이고 있음
 - 일본의 로펌들도 개정 일본 개보법 및 GDPR 등 글로벌 프라이버시에 대해 사업자 인지를 제고하기 위해 PPC와 협업 중

《 Session2 : 국경 간 정보이전과 APEC CBPR 》

- (CBPR 활성화 현황 공유) 일본 JIPDEC은 미국 TRUSTe에 이어 '16.1월 인증기관 승인을 받고 현재 1개 기업에 대해 인증을 발급 ('16.12월)했으며 기업 홍보를 위해 워크숍, 세미나 개최 추진 중
 - 국제적으로는 '2016년 APEC 정상선언'을 통해 회원국의 CBPR 이행을 독려한 바 있으며, '17년 하반기에 회원국의 CBPR 역량 제고를 위해 예정된 다양한 행사*들에 많은 참여를 독려함
- * CBPR 세미나(APEC 내 고위관리회의인 SOM3에 부대행사 마련, 8월, 베트남), EU-APEC CBPR 상호 운용 관련 논의 라운드테이블(ICDPPC 개최에 맞춰 부대행사 마련, 9월, 홍콩), CBPR 워크숍(10월, 대만/ 12월, 필리핀) 등
- (일본의 개인정보 국외이전 정책) 개정 개인정보보호법을 통해 개인정보 국외이전 조항을 신설하고, ①이용자 동의 ②개인정보 보호위원회(PPC)가 지정한, 일본과 동등한 수준의 개인정보보호 체도를 갖춘 국가 또는 ③ 보호 체계를 갖춘 자에게 이전 허용
 - 개정법 완전 시행('17.5.30)을 앞두고 구체적 이행 지침 마련을 위한 하위법령(cabinet rule, PPC rule 등) 작업 중
 - 또한 제75조(적용 범위), 제78조(외국 집행당국에 대한 정보제공)에 규정 신설을 통해 국외에서 처리되는 개인정보에 대한 집행력 및 국외 기관과의 협력을 강화하였음
 - 일본은 EU 적정성 평가를 추진 중이며, 이를 위해 'EC-PPC Dialogue' 개최('17.3월) 등 다양한 채널로 EC 관계자와 협의 중
 - 한국도 현재 한국의 개인정보보호 체계와 CBPR 도입 추진 현황 및 도입 관련 국내 논의 중인 이슈를 공유함

《 Session3 : 빅데이터, 머신러닝, 인공지능에의 신규 규제 적용 》

- (일본 개인정보 비식별화 정책) 개정 개보법에 개인정보 익명화 규정 신설에 이어 개보위(PPC)는 사업자가 이를 적용하기 위한 필요한 최소한의 조치 기준 마련
 - 또 개보위(PPC)는 익명화처리 정보에 대한 보고서를 발간('17.2월) 하여 익명화 처리 정의, 익명화 처리 방법 및 적용 사례를 소개
- (AI 가이드라인) 국제기구에서 논의 중인 AI 가이드라인(안)의 AI 원칙(①상호협력, ②투명성, ③통제가능성, ④보안, ⑤안전성, ⑥프라이버시, ⑦윤리, ⑧이용자 지원, ⑨책임성)을 소개

3

관계기관 실무회의 내용

□ TRUSTe (미국 CBPR 인증기관) 실무회의

- 일 시 : '17.5.11.(목), 17:30 ~ 19:30
- 장 소 : 오쿠라 호텔
- 참석자 : TRUSTe(Josh Harris외 2명), 방통위(김기석 팀장, 이정수 사무관), KISA (권현준 단장, 박정필 선임)

- (인증기관 간 협력) 인증기관 별 제도 운영의 균형 유지, 회원국 내 제도 확산 및 기업의 자율 규제 지원 등 제도 신뢰 확보라는 공동 목적 달성을 위해 인증기관 간 상호 협업 필요

<인증기관 간 협력 사안>

- ① 제도 활성화(공동 워크숍 개최, 공동 홈페이지, seal, 통합 일련번호 개발)
- ② 분쟁, 민원 처리 공조(정보 공유, 분쟁처리 협업, 공동 처리 절차 개발),
- ③ 인증기관 간 균형 유지(인증 방법, 세부 인증기준 등 정보 공유, 통일화)
- ④ 제도 개선(타 권역과의 상호운용 방안 등 공동 연구, 케이스 스터디 등을 통한 상호 벤치마킹 등)

- KISA는 인증기관 협의회(Association) 구성·운영을 통해 지속적인 협업 기반 마련과 장기적으로는 독립조직 설립 추진을 제안했고,
 - TRUSTe는 협의회 구성에 적극 지원 의사를 밝혔으며, 이에 추가하여 인증기관 협의회 규정(인증기관 신청 시 자동으로 협의회에 참여하는 강제 규정 등)을 마련하고 APEC ECSG DPS에 공식적으로 제안하고 지지를 받는 등의 아이디어를 제안함
 - 방통위가 TRUSTe와 개인정보보호 감독기구의 협력방식에 대해 문의하자, 인증기관이 감독기구에 기업의 관련 규율 위반 사항을 매번 보고하는 것은 아니지만 협조 요청이 있는 경우 자료 제공 등 필요한 도움을 적극적으로 제공하고 있다고 답변
- (관련 EU 규범 동향) '18년 시행되는 EU GDPR에 국외 이전 허용 요건으로 '공인 인증 매커니즘'이 신규로 포함되었으며, '17.1월 EC 브리핑에 인증 매커니즘 활성화 계획이 포함
- APEC DPS는 EU-APEC 합동팀을 구성하여 BCR과 CBPR 상호 운용을 위해 연구, BCR-CBPR 공통질문지(안)을 개발('14년)한 바 있으며, 최근 GDPR 시행을 앞두고 다시 상호간 논의가 활발해짐
 - TRUSTe는 APEC DPS 또는 TRUSTe 자체 채널을 통해 EC 등과 소통 중이며, EC는 회원국 공동의 인증제도 운영 경험이 없는 관계로, 축적된 노하우가 있는 CBPR('11년 개발)에 많은 관심을 보이고 있으며, 향후 전망이 긍정적이라고 언급함
- (TRUSTe 조직 및 인증방법) CBPR 및 TRUSTe 자체 개발 인증을 포함한 각종 인증제도의 평가 인력 30여명 및 영업·컨설팅 인력 30여명으로 구성(CBPR 전담팀은 없음)

- 인증 방법은 제출된 문서 검토를 통해 평가하며(현장실사 없음), 심사 수수료는 신청기업 규모, 인증범위 등에 따라 산정(3천~5천 USD, 문서화된 수수료 지급 기준 없으며 매번 계약에 따름)
- ※ TRUSTe 자체 인증마크와 CBPR 간 구체적 상호운용 체계는 없으나 복수의 인증을 획득하는 경우 인증수수료 할인 등의 비공식적 절감 혜택이 있음. 향후 여러 인증제도가 글로벌 인증으로서 획득 유인이 많은 CBPR 쪽으로 통합되어 운영될 가능성이 있음.
- 인증 기간은 일반적으로 4주 정도 소요(최초로 CBPR 인증을 받은 IBM의 경우 '13.6월에 신청서를 제출하여 '13.8월 인증을 받음)
- 수년간 축적된 TRUSTe 자체 인증 수행 경험을 바탕으로 구성된 세부 인증 가이드가 있으며, 현재 시스템으로 구축되어 평가에 활용되고 있음 (SW기반으로 체계적으로 운영됨)
- o (인증수행 현황) TRUSTe의 CBPR 인증기업은 20개이며, 현재 인증 신청 검토* 중인 기업이 10개 있음
 - TRUSTe의 CBPR 인증 개시 시점('12년)에는 기업들의 CBPR에 대한 인지도가 낮아 확산에 어려움이 있었으나 더 많은 국가 및 인증기관들이 참여한다면 활성화에 훨씬 유리하다고 평가
 - * 인증 신청을 희망하나 아직 개인정보보호에 대한 기본적 체계정립이 필요한 기업의 경우 사전 컨설팅 과정이 필요하여 신청서 제출까지 시간 다소 소요
 - 현재 회계법인, 보안업체 등이 신규 인증기관으로 신청을 검토 중이며, 이들이 참여하면 기업 규모별로 인증 시장이 형성되어 점차 확대될 것으로 전망
 - ※ TRUSTe는 인력과 자원의 한계로 구글이나 페이스북 등 초대형 기업에 대한 인증이 어려우나(중견기업 대상 인증), 향후 대형 및 소형기업(앱 개발사, 스타트업)을 대상으로 하는 인증기관도 생길 것으로 예상

□ JIPDEC (일본 CBPR 인증기관) 실무회의

- 일 시 : '17.5.12.(금), 13:30 ~ 15:00
 - 장 소 : JIPDEC 회의실
 - 참석자 : JIPDEC(Tetsuya Gunji, Hirumu Yamada), 방통위(김기석 팀장, 이정수 사무관), KISA (권현준 단장, 박정필 선임)
-

○ (현황) 현재 JIPDEC은 100여 명 규모이고 그 중 50여 명이 일본의 기존 개인정보보호 인증제도인 P-Mark를 수행하고 있는 인력이며, CBPR 담당 업무는 6~7명이 맡고 있음

- P-Mark는 OECD 8원칙 및 EU 프라이버시 지침을 반영하여 설계 ('99년)한 일본 산업 기준(JIS Q 15001:2006)으로, 120개 인증 기준으로 구성되었으며, 기업의 기술적·관리적 보호 조치 평가에 중점

※ P-Mark 인증 기준은 일본의 개인정보보호 법규 보다 엄격하며 향후 개정 ('15년)된 개보법 반영을 하여 P-Mark도 개정 예정

- CBPR은 하나의 인증에 3명(JIPDEC 인력 1, 외부 심사원 2명)으로 팀을 구성하고, 심사는 현장실사(1~2일)을 포함하며, 사례가 1개 밖에 없어 소요 기간을 일반화하기 어려움(최초 인증사례는 4주 소요)

○ (상호운용) P-Mark와 CBPR은 각각 평가 목적에 따라 국내 사업을 기반을 둔 사업자와 해외진출 희망사업자 대상으로 구분하여 운영하고 있으며, 아직 구체적인 상호 운용에 대한 계획은 없음

- 그러나 향후에는 제도 운영의 효율성 등을 위해 두 제도를 상호 운용하는 방안도 검토가 필요할 것이라고 언급

□ 주요 활동사진

APEC CBPR 워크숍 사진	APEC CPBR 워크숍 참석 사진
	
JIPDEC 관계자 인터뷰 사진	JIPDEC 관계자 인터뷰 사진
	

Ⅲ. 동향 및 시사점

□ 주요 동향

- (제도 확산) CBPR 가입국가 및 인증기업 수 증가에 따라 기업의 CBPR 신청 유인 및 국제적 인지도가 증가할 것으로 예상됨
- (상호운용성) CBPR과 EU GDPR이 인정하는 인증 간 상호운용성 확보를 통해 CBPR 가입 및 인증신청 유인 확대노력 추진 중
- (인증기관 간 협조강화) CBPR 인증기업에 대한 통일적 규범 적용을 위해 인증기관 간 협조강화 및 협의체 구성 논의가 진행되고 있음

□ 시사점

- CBPR 제도상, 글로벌 기업이더라도 본사(headquarter)가 위치하고 있는 국가의 인증기관에서만 인증을 받도록 되어 있으며, 인증의 효과는 CBPR에 가입된 모든 국가에 똑같이 적용됨
 - 한국만 보호수준이 높은 CBPR 기준(한국형 등)을 적용하는 것의 실효성이 낮고 한국에 본사를 둔 기업에 대한 차별이 될 수 있으므로, **CBPR 50가지 표준 질문지를 활용**하는 방법을 고려할 필요 (TRUSTe와 JIPDEC 모두 표준 질문지를 기준으로 인증심사 실시 중)
- TRUSTe는 SW기반 CBPR 심사 시스템을 구축하고 있음(심사원이 각 심사를 진행하면서 시스템에 관련 사례 및 노하우를 추가하는 방식으로 심사 방식을 점차 체계화할 수 있도록 함)
 - 인증 용이성을 위한 무리한 PIMS 연계보다, **SW 기반 CBPR 인증 시스템 구축** 등의 방법을 통해 인증 효율성을 확보할 수 있음