국제기구의 정보보호 논의 동향

김 성 웅*

1. 개 요

우리나라는 2013년에 사이버공간에서의 범죄, 안전, 혜택, 국제안보 등을 논의하는 '사이버공간회의'를 개최하기로 하였다. 2011년 10월 런던회의, 2012년 10월 헝가리 부다페스트 회의에 이어 세 번째로 열리는 것이다. 우리나라의 사이버공간회의 개최는 유럽의 사이버보안 논의를 선도하는 영국, 사이버범죄조약[1]을 이끈 헝가리에 이어 정보보호 분야에서 우리나라가 국제적으로 의제를 설정하고, 위상을 제고할 수 있다는 데 그 의의를 찾을 수 있다.

사이버보안 및 정보보호에 대한 인식은 인터넷 기술의 발달 및 소비자 수요 증가에 따라 자연스럽게 증가해왔고, 사실상 해킹, 사이버테러 등의 문제점들이 확대되면서 그 중요성에 대한 논의가 더욱 활발해졌다고 볼 수 있다. 특히 2000년대 후반에 들어서는 정보보호 및 사이버보안 관련 문제가 국내적인 문제에서 국제적인 문제로 확대되면서 국가 간의 협력 이슈가 주요 의제로 설정되어 왔다.

* 정보통신정책연구원 국제협력연구실 연구원, (02)570-4436, woongnice@kisdi.re.kr

1) 사이버범죄조약(convention on cybercrime)은 '부다페스트조약'이라고도 하며, 인터넷을 이용한 범죄행위에 대하여 상세 규정을 두고 처벌하도록 한 최초의 국제조약이다. 이는 2011년 11월 헝가리 부타페스트 사이버범죄 국제회의에서 서명·발효되었고, 2011년 말 기준 45개국이 가입 중이며 우리나라는 미가입국이다.《디지털데일리》(2011. 7. 11)

이러한 점에서 본고에서는 ITU, OECD, APEC 등 주요 국제기구에서의 최근 정보보호 및 사이버보안 이슈 논의 동향을 정리해 보고자 한다.

2. 주요 국제기구의 정보보호 논의 동향

(1) OECD(경제협력개발기구)

선진경제국 간 회원체 기구인 OECD에서의 정보보호 논의는 25개 분과위원회 중 정보통신정책위원회(ICCP, Committee for Information, Computer and Communications Policy) 산하 작업반인 정보보호작업반(WPISP, Working Party on Information Security and Privacy)에서 주로 진행된다. 최근에는 사이버보안에 관한 국가별 전략을 비교하는 작업이 이뤄지고 있으며, 2002년 만들어진 정보보호 가이드라인에 대한 검토가 진행 중에 있다.

OECD 사무국은 2009년 이후 회원국들이 추진한 사이버보안전략(Cyber Security Strategy)의 배경, 접근방법, 대응전략 등에 있어 국가 간의 공통점 및 차이점에 대한 비교분석을 추진하고 있다. 참여한 몇 개 국가들의 사례를 보면 주요 정보통신 기반시설 보호에 대한 관심 증가, 온라인 위협에 대한 실시간 인지능력 향상, 국제공조에 대한 강조 등이 담겨져 있다.[2] OECD 정보보호 가이드라인에 대해서는 현재 개정 여부가 검토되고 있다. 5년마다 점검하기로 한 동 가이드라인은 2007년에는 원안 그대로 유지하기로 하였으나, 최근의 사이버보안 환경의 변화를 고려하여 회원국 간에 개정 논의가 진행되고 있다. 특히 2002년에는 원칙만을 제시하고 담지 못했던 원칙의 '이행' 문제, '비회원국으로의 확대' 문제 등이 가이드라인에 포함되어야 하는지 등이 논의되고 있다.[3]

한편, OECD는 지난해 인터넷 경제에 관한 고위급회의(High Level Meeting on

2) OECD(2012a), pp.4~7.
3) OECD(2012b), pp.12~16.

Internet Economy)에서 회원국들이 합의한 정책선언문인 '커뮤니케(Communique)'를 통해 인터넷 정책결정 원칙을 천명하였다. 특히 정보보호 이슈의 중요성을 강조하였는데, 개인정보 보호의 일관성 및 효율성 강화(Strengthen consistency and effectiveness in privacy protection: 원칙9), 인터넷 보안 증진을 위한 협력 장려(Encourage Co-operate to promote Internet security: 원칙13)에서 동 이슈를 다루고 있다. 원칙9는 개인정보의 강력한 보호가 인터넷의 사회적, 경제적 잠재력의 실현에 결정적인 요소이며, 개인의 공적, 사적 영역의 인터넷 비중이 확대됨에 따라 개인들은 자신의 정보사용에 대한 주도권을 보유해야 하고 동시에 정보사용이 공정하게 이뤄지고 있다는 확신을 가질 수 있도록 국가와 정부가 노력해야 한다는 점을 강조하고 있다. 원칙13은 인터넷의 지속적인 활성화에 있어 보안에의 위협요소 해결 및 취약성 감소 정책이 중요한 요소이며, 온라인 보호 증진을 위해 국제적으로 인식되고 합의된 보안 관련 표준 및 최적사례의 이행이 장려되어야 한다고 강조하고 있다. 또한 온라인 보안에 대한 개선정책은 사회발전 및 경제성장에 기여하는 인터넷의 개방성을 해쳐서는 안 되며, 자국 보호주의의 구실로 사용되어서는 안 된다는 점을 역설하고 있다.[4)]

(2) ITU(국제전기통신연합)

정보통신 분야의 단일 국제기구로는 가장 많은 회원국을 보유하고 있는 ITU에서도 일찍이 2000년대 초반부터 정보보호 이슈와 관련한 논의가 활발하게 이루어졌다. ITU는 2003년, 2005년 두 차례의 WSIS(정보사회정상회의) 개최를 통해 원칙선언문과 실천계획을 도출하였고, 선언문 원칙 5(ICT 활용에서의 신뢰와 보안)에서는 정보 및 네트워크 보안의 신뢰성 강화, 프라이버시 및 고객보호, 범죄와 테러 목적의 사용 예방, 스팸 대응 등을 핵심 내용으로 포함시킨 바 있다.[5)]

또한 ITU의 연간활동 전반을 계획하고 승인하는 ITU 이사회의 최근 논의 의제는

4) OECD(2011a), pp.5~6.
5) 김은규, pp.52~56.

다음과 같다. '사이버공간에서의 공격에 대한 대처에 있어 ICT 규제자의 역할'을 주제로 사이버범죄에 대한 인식을 제고하고, 규제자와 정책결정자에게 요구되는 역할, 관련 활동 및 조치 등에 대하여 논의하는 등 사이버공간에서의 도전과 위협에 대응하기 위해 ITU는 범세계적 노력을 조정하도록 위임받아 적극적인 활동을 수행하고 있다. ITU는 구체적으로 사이버보안에 대한 ITU의 역할에 우선순위를 부여하고, ITU 전체적인 차원의 사이버보안 전략인 글로벌 사이버보안 의제(GCA, Global Cyber-security Agenda)를 추진하고 있다. 이는 보안수준의 제고를 위해 사이버 위협에 대한 법적 대응기반 조성, 모바일데이터 및 웹서비스에 대한 보안 필요요건 등 기술적 연구의 추진, 국가들의 필수적인 사이버보안 대응능력 제고 촉진, 국제 협력 강화 등의 전략적 방안을 담고 있다.[6)]

특히 사이버보안 이슈는 회원국 간의 의견 차이가 커 강하게 대립하고 있기 때문에, ITU를 통해 사이버보안 활동 영역을 확대하려는 개발도상국과 중복성을 고려하여 ITU의 역할을 ITU 전문 부문으로 한정하려는 선진국 간의 대립은 당분간 계속될 것으로 보인다.[7)]

(3) APEC(아시아태평양경제협력체)

아시아태평양 지역 경제협력체인 APEC에서의 정보보호 이슈는 11개 실무그룹 중 정보통신실무그룹(TEL) 내의 보안 및 번영 운영그룹(SPSG, Security and Prosperity Steering Group)에서 논의가 주로 이뤄지고 있다. 최근의 논의 의제는 사이버보안 인식 제고, 스팸 대응에 초점을 맞추고 있다. 특히 사이버공간의 정보보호 및 보안과 관련하여 이미 2007년부터 사이버보안 인식 제고 활동 관련 프로젝트, 테러공격으로부터 사이버공간의 보호 등의 이슈에 대해 심도 있는 논의 및 작업과 함께, 국가 간의 협력을 제고하기 위해 많은 노력을 기울여 왔다. 회원국들은 사이버보안 인식 제고

6) ITU(2012), pp.2~5.
7) 박민정, pp.22~23.

주간 선정 등 캠페인 활동, 각국의 인터넷 보안침해 사례 공유 등을 통해 사이버보안 이슈를 국제적으로 인식하고, 해결하기 위한 논의의 장을 만들어왔다. 우리나라는 ICT 선도국으로서 미국, 호주 등과 함께 동 분야의 의제를 선도하고, 2011년 APEC-CTTF[8] 사이버범죄 세미나 개최, 2010년 서울-멜버른 다자간 스팸 대응 양해각서 체결 등의 국제협력 활동에 기여하였다.[9]

한편, APEC은 OECD 등 다른 국제기구와도 공동작업 등의 협력활동을 전개하고 있다. 2009년에는 어린이를 위한 안전한 인터넷 환경 조성을 위한 APEC-OECD 공동 심포지엄을 통해 어린이를 인터넷 이용자로서 인식하고, 이들을 보호하기 위한 인식 제고, 국제협력, 민간·정부 협력 강화 등에 대한 중요성을 강조하였고, 2012년에는 OECD 정보보호작업반(WPISP)과의 공동작업을 통해 사이버보안 전략 비교, 사이버보안 지표 관련 공동 프로젝트 등 연대 및 협력을 추진하고 있다.[10]

정보통신 분야 최고 합의체인 장관회의에서도 정보보호 이슈의 중요성을 인식하여 주로 '안전하고 신뢰할 만한 ICT 환경'이라는 주제 아래 선언문이 합의되었다. 2008년 방콕선언문에서는 디지털 번영을 위한 안전하고 신뢰할 만한 ICT 환경 증진, 사이버보안에 대한 대외활동 강화 등을 주제로 논의가 이뤄졌다. 그리고 2010년 오키나와 선언문에서는 안전하고 신뢰 가능한 사회 및 ICT 환경이라는 주제로 통신인프라와 서비스의 안전과 보안 및 신뢰성 확보, 사이버범죄와 공격 등에 대한 효과적인 개인정보 보호 정책과 네트워크 기술 안전 증진 등 보다 강화된 소비자보호 조치의 필요성, 아동과 청소년 등 온라인 위협에 취약한 그룹 보호의 중요성 등에 대한 문구를 선언문에 포함시켰다.[11] 이는 APEC TEL의 중기 계획인 2010~15 전략행동계획의 세부목표에 따른 것으로, 5개 행동계획 중 3번째 계획인 안전하고 신뢰 가능한 ICT 환경촉진(Promote a Safe and Trusted ICT Environment)에 정확히 부합하기도 한다.[12] 이

8) CTTF(Couterterrorism Task Force) 대테러 대책반
9) APEC TEL37~44 SPSG 의제 결과
10) APEC TEL45 SPSG 의제 결과
11) APEC(2010a) p.3.
12) APEC(2010b) p.4.

러한 측면에서 2012년 8월에 개최될 장관회의의 결과물인 페테르부르그선언문에서는 아예 선언문 제목을 'ICT 활용에 있어 경제성장과 번영 촉진을 위한 신뢰 및 보안 구축'으로 설정하는 등 최근의 정보보호 및 보안 문제에 대한 국제적 관심을 보여주고 있다.

3. 결 어

우리나라는 2007년 7월과 2011년 3월에 발생한 대규모 DDos 공격 등 전 세계적으로 유래 없는 대규모 사이버공간 인터넷 침해사고를 경험하였다. 이에 따라 정부는 민간 사업자와의 협업을 통해 피해를 최소화하고, 예방 및 대응체계를 갖추기 위해 노력을 기울였고, 해외 기관과의 협력도 추진하고 있다. 인터넷 개방성을 통해 인터넷 경제가 활성화되고 기술이 급속히 발전함에 따라 발생하는 이와 같은 문제는 대내적으로 적절하고 효율적인 대처뿐만 아니라, 대외적으로 정보와 인식 공유 및 국가 간 협력활동이 필수적이다.

앞서 살펴보았듯이 정보통신 관련 국제기구 내에서의 최근 논의는 안전한 인터넷 환경에 대한 강조, 특히 사이버보안 문제에 초점이 맞춰져 있다. 이러한 정보보호 이슈 및 논의는 국가들 간에 의제를 공유하고 이슈화하여 합의를 이끌어내고, 나아가 각국의 국내 정책에 영향을 미치는 의제 설정 및 선도라는 국제기구의 중요한 기능에 의해 다뤄져야 한다는 국가들의 인식이 확산된 결과라고 할 수 있다. 이와 관련하여 우리나라는 브로드밴드 인프라, 모바일 기술 등 ICT 분야 선도국으로서의 위상을 유지·제고하기 위해서 정보보호 분야에 대한 논의에 적극 참여하여 협력활동을 주도하고, 동시에 국내정책 반영 및 국내정책의 대외 홍보 등의 선순환 효과를 극대화할 필요가 있다.

참고문헌

김은규 (2006), "21세기 국제정보질서의 새로운 패러다임? -정보사회세계정상회의의 역사적 맥락과 의제 검토", 《한국언론정보학보》, 통권 34호, 한국언론정보학회.

《디지털데일리》 (2011. 7. 11), '부다페스트 사이버범죄 조약을 아시나요?'.

박민정 (2011. 2. 16), "ITU의 정책이슈 및 향후 추진방향: PP-10과 GSR-10 결과를 중심으로", 《방송통신정책》, 제 23 권 3호 통권 502호, 정보통신정책연구원.

APEC (2010a). Okinawa Declaration "ICT as an Engine for New Socio-economic Growth". The 8th APEC Ministerial Meeting on the Telecommunications and Information Industry(TELMIN8). 2010. 10.

_____ (2010b). "APEC TEL Strategic Action Plan: 2010~2015". 2010. 10.

ITU (2012). "ITU Activities on Strengthening the Role of ITU in Building Confidence and Security in the Use of Information and Communication Technologies". [Document C12/29-E].

OECD (2011). "OECD High-level Meeting on the Internet Economy: Generation Innovation and Growth Communique on Principles for Internet Policy Making". [DSTI/ICCP(2011)6/FINAL].

_____ (2012a). "Draft Comparative Analysis of National Cybersecurity Strategies". [DSTI/ICCP/REG(2011)12/REV1].

_____ (2012b). "Draft Plan for the Second Review of the 2002 Security Guidelines". [DSTI/ICCP/REG(2012)1].