情 報 保 護 學 會 誌
第 13 券 第 5 號, 2003. 10

사이버범죄방지협약의 국내법적 수용문제

박 영 우*

요 약

인터넷 이용의 급증과 더불어 컴퓨터바이러스, 해킹 및 프라이버시 침해 등 각종 사이버범죄도 또한 날이 갈수록 크게 증가하고 있다. 또한 인터넷과 같이 글로벌한 네트워크 환경에서 발생하는 범죄는 많은 경우 필연적으로 '국제적' 성격을 띠며, 따라서 개별국가의 노력만으로는 범죄를 충분히 방지하기 어렵다. 따라서 다수 국가가 사이버범죄에 대한 수사와 처벌을 위한 협력의 틀을 마련하기 위해 만든 사이버범죄방지협약(Convention on Cyber-Crime)은 컴퓨터 시스템, 네트워크 또는 데이터를 대상으로 하거나 이를 오용한 다양한 형태의 범죄행위의 방지 및 처벌과 관련하여 실체법적 측면과 절차법적 측면에서 그 중요성이 매우 높다. 이 글에서는 이 사이버범죄방지협약에 대해 그 제정과정 및 주요내용을 살펴보고, 다음으로 우리법과 비교·분석하였다.

Ⅰ. 서 론

인터넷 이용의 급증과 더불어 컴퓨터바이러스, 해킹 및 프라이버시 침해 등 각종 사이버범죄도 또한 날이 갈수록 크게 증가하고 있다. 인터넷과 같이 글로벌한 네트워크 환경에서 발생하는 범죄는 '국제적' 성격을 띠며, 따라서 개별국가의 노력만으로는 범죄를 방지하기 어렵다. 따라서 다수 국가가 사이버범죄에 대한 수사와 처벌을 위해 협력하는 법적 노력의 하나로 만든 것이 사이버범죄방지협약(Convention on Cyber-Crime)이다. 동 협약은 컴퓨터 시스템, 네트워크 또는 데이터를 대상으로 하거나 이를 오용한 다양한 형태의 범죄행위를 실체법적 측면과 절차법적 측면에서 방지·처벌할 수 있도록 제안된 최초의 국제협약(International Treaty)이라 점에서 그 의의가 크다.

Ⅱ. 사이버범죄방지협약의 제정경과

1997년 제41차 유럽평의회 회의에서 악의적 해킹, 컴퓨터바이러스의 작성·유포, 아동포르노의 온라인 유포 및 사기에 관한 사이버범죄에 관한 안건이 상정되었다. 이후 유럽평의회(Council of Europe) 회원국(43개국)이 중심이 되고 미국, 캐나다, 일본, 멕시코, 바티칸이 옵저버로 참여하여 협약안을 작성하였으며 2001년 5월 25일 최종안이 완성되어 2001년 6월 22일 유럽평의회 각료회의의 승인을 받았다. 이때까지 협약안은 모두 27회에 걸쳐 수정이 있었다. 승인된 협약은 2001년 11월 20일부터 서명을 받기 시작하여 2003년 9월 15일 현재 현재 37개국(유럽평의회 회원국 33개국과 캐나다, 일본, 남아프리카, 미국)이 협약에 서명하였으며, 알바니아(2002. 6. 20), 크로아티아(2002. 10. 17), 에스토니아(2003. 5. 12)의 3개국이 비준하였다.

협약은 유럽평의회 회원국 3개국을 포함한 5개국의 서명·비준으로 효력이 발생하도록 되어있으며, 아직 미발효 상태이다. 협약은 발효 후 서명·비준 국가에 한해 동의표시를 한 날부터 3개월이 경과한 다음달 1일에 효력을 발생한다(협약 제36조).

Ⅲ. 사이버범죄방지협약의 구성과 주요내용

1. 사이버범죄방지협약의 구성

사이버범죄방지협약은 전문과 4장 및 48개 조문으

* 한국정보보호진흥원 선임연구원

로 구성되어 있다. 제1장은 동 협약에서 사용하는 용어의 정의를 규정하한다. 제2장의 제1절은 컴퓨터 범죄 또는 컴퓨터 관련 범죄로서 범죄화해야 할 실체법적 규정을 담고 있다. 이에는 컴퓨터 데이터 및 시스템의 기밀성, 무결성 및 가용성에 대한 범죄 등 9개의 행위를 범죄로 규정하고 동 범죄행위에 대한 종범의 책임과 처벌을 규정하고 있다. 제2장의 제2절은 컴퓨터 시스템을 이용해서 행해진 범죄행위와 전자 증거에 관한 절차법 조항을 규정하고 있다. 제3장은 현행 국제법상의 국제공조 및 컴퓨터 범죄 관련 공조와 인도에 관한 규정을 두고 있는데 이에는 양 당사국간에 조약 등이 존재하지 않는 경우와 조약 등이 체결되어 있는 경우 동 협약에 의한 공조 등을 포함하고 있다. 컴퓨터 범죄 및 컴퓨터 관련 범죄에 관한 특별한 공조는 범죄인 인도를 포함하여 2가지 상황을 모두 포괄한다. 또한, 공조를 필요로 하지 않지만 저장된 컴퓨터 자료의 초국경적 접근 등 특별한 형태에 대한 관련 규정도 포함하고 있으며 당사국들 간의 24시간 공조체제 확보를 규정하고 있다. 제4장은 유럽평의회 협약의 표준 규정을 최종 규정으로 반복하여 규정하고 있다.

2. 사이버범죄방지협약의 주요내용

(1) 사이버범죄의 규정 및 처벌

협약 가입국은 국내법에 사이버범죄 처벌 규정을 마련하여야 한다. 즉 컴퓨터 데이터와 컴퓨터 시스템의 비밀성, 무결성 및 가용성을 침해하는 행위, 컴퓨터 관련 위조 및 사기, 아동포르노 관련 범죄, 저작권 및 관련권리 침해 관련 범죄와 그 종범(從犯)을 국내법상 범죄행위로서 규정하여야 한다.

협약은 사이버범죄의 유형을 첫째 컴퓨터데이터와 시스템의 기밀성, 무결성 및 유용성에 대한 범죄(Offences against the confidentiality, integrity and availability of computer data and systems), 둘째 컴퓨터관련 범죄(Computer-related offences), 셋째 컨텐츠관련 범죄(Content-related offences), 넷째 저작권 및 저작인접권 침해에 관한 범죄(Offences related to infringements of Copyright and related rights) 등 네 가지로 구분하고 동 범죄에 가담한 종범의 책임과 처벌에 대하여 규정하고 있다.

가) 컴퓨터데이터와 시스템의 기밀성, 무결성 및 유용성에 대한 범죄

협약은 컴퓨터데이터와 시스템의 기밀성, 무결성 및 유용성에 대한 범죄를 불법접속, 불법감청, 데이터손괴, 시스템손괴, 장치의 오용 등 다섯 가지 유형으로 분류하고, 이를 국내법상의 형사법에 규정하여 범죄로서 처벌하고 이에 수반되는 조치를 취하도록 요구하고 있다. 이 부분은 우리가 종래 해킹 및 바이러스 유포행위로 총칭하던 내용이라 할 수 있다.

먼저 권한없이(without right) 컴퓨터시스템의 일부 또는 전체에 고의적으로(intentionally) 접속하는 행위를 '불법접속'(Illegal Access)으로 규정하고 동 행위를 국내법상 범죄로 규정하는데 필요한 입법 및 그에 부수되는 조치를 취하도록 요구하고 있다(협약 제2조). 동 협약의 당사국은 컴퓨터데이터의 획득이나 기타 부정한 의도로(dishonest intent) 또는 당해 컴퓨터시스템과 다른 컴퓨터시스템을 연결하기 위하여 컴퓨터시스템 보안장치를 손상시키는 것을 불법접속 범죄의 요건으로 정할 수 있다.

둘째, 전자 마그네틱(electromagnetic) 등 컴퓨터데이터를 컴퓨터시스템 내에서 처리하거나 다른 컴퓨터시스템으로 동 데이터를 비공개(non-public) 전송하는 것을 기술적 방법을 통하여 가로채는 행위를 '불법감청'(Illegal Interception)으로 규정하고 각 당사국으로 하여금 이를 처벌하도록 규정하고 있다(협약 제3조). 동 범죄에 관하여 각 당사국은 부정한 의도로 또는 당해 컴퓨터시스템과 다른 컴퓨터시스템을 연결하는 행위를 구성요건으로 할 수 있다.

셋째, 컴퓨터데이터를 고의적으로 손상(damaging)·삭제(deletion)·파괴(deterioration)·변경(alteration) 또는 은닉(suppression)하는 행위를 '데이터손괴'(Data Interference)로 규정하고 각 당사국으로 하여금 국내법으로 처벌하도록 규정하고 있다(협약 제4조).

넷째, 권한없이 고의적으로 컴퓨터데이터를 입력(inputting)·전송(transmitting)·손상·삭제·파괴·변경 또는 은닉하여 컴퓨터시스템의 작동을 심각할 정도로 방해하는 것을 '시스템손괴'(System Interference)로 규정하고 이를 국내법상 범죄로 처벌하도록 요구하고 있다(협약 제5조).

다섯째, 제2조 내지 제5조의 범죄에 사용할 의도로써 컴퓨터프로그램 등의 장치나, 컴퓨터비밀번호(computer password), 접속코드(access code) 등의 데이터를 생산, 판매, 이용을 위한 조달(procurement for use), 수입(import), 배포(distribution), 이용 및 소유하는 것을 '장치의 오용'(Misuse of Devices)이라 하여 국내법상 범죄로 처벌하도록 규정하고 있다(협약

제6조). 물론 컴퓨터프로그램이나 컴퓨터비밀번호, 접속코드 등이 컴퓨터시스템의 보호나 합법적인 시험을 위한 것으로 동 협약 제2조 내지 제5조의 범죄를 행할 목적이 아닌 경우에는 형사책임이 부과되지 아니한다.

나) 컴퓨터관련 범죄

협약은 컴퓨터와 관련된 범죄를 컴퓨터데이터의 위조와 컴퓨터데이터 및 시스템상의 불법행위를 통한 사기 등 두 종류로 구분하고 있다. 즉 컴퓨터데이터의 진정성에 흠결이 있는(inauthentic) 데이터를 마치 진정한(authentic) 것처럼 합법적으로 인식되도록 하거나 행사할 목적으로 권한없이 고의적으로 컴퓨터데이터를 입력·변경·삭제 또는 은폐하는 행위를 '컴퓨터관련 위조'(Computer-related Forgery) 범죄로서 국내법으로 입법하도록 요구하고 있다. 동 범죄를 처벌하기 위하여 각 당사국은 사기를 범할 의도 또는 이에 준하는 부정한 의도를 규정할 수 있다(협약 제7조).

'컴퓨터관련 사기'(Computer-related Fraud) 범죄는 컴퓨터데이터를 입력·변경·삭제 및 은폐하거나 컴퓨터 또는 컴퓨터시스템의 정상적 작동을 방해함으로써 타인의 재산에 손실을 입히거나 자신 또는 타인의 경제적 이익을 획득하고자 하는 행위로서 동 범죄에 대하여도 제7조의 절차와 요건을 고려하여 당사국이 처벌할 수 있도록 입법 및 그에 부수되는 조치를 취해야 한다(협약 제8조).

다) 컨텐츠관련 범죄

협약은 현재 컨텐츠관련 범죄를 아동포르노 범죄에 한정하고 있지만 향후 협의를 거쳐 그 적용대상을 확대할 것으로 추정된다. 즉 '사이버공간에서의 범죄에 관한 전문가회의'는 당초 아동포르노 범죄 이외에 컴퓨터시스템을 이용하여 인종차별주의를 선전·배포하는 것을 컨텐츠관련 범죄에 포함시키는 것을 검토하였었다. 그러나 세부사항에 대한 논의 시간이 절대적으로 부족하여 동 협약에 반영되지 못하였다. 이에 전문가회의는 이러한 사항을 가능한 한 시급히 실행할 수 있도록 하기 위하여 동 협약에 추가의정서(an additional Protocol)를 통하여 보완하는 방안을 유럽 형사문제위원회에 제안하기로 합의한 바 있다.

아동포르노관련 범죄(Offences related to child pornography)라 함은 컴퓨터 시스템을 통하여 아동포르노(child pornography)를 배포(distribution)할 목적으로 이를 제작하는 행위, 컴퓨터시스템을 통하여 아동포르노를 이용하도록 하거나 제공하는 행위, 컴퓨터시스템을 통하여 아동포르노를 전송 또는 배포하는 행위, 본인이나 타인을 위해 컴퓨터시스템을 통하여 아동포르노를 획득(procuring)하는 행위, 컴퓨터데이터 저장매체 또는 컴퓨터시스템 내에 아동포르노를 소유(possessing)하는 행위를 권한없이(without right) 고의적으로 범하는 것을 말한다(협약 제9조).

각 당사국은 제9조에 규정된 아동포르노에 성적으로 노골적인 행위를 실연하는 미성년자(a minor), 미성년자가 성적으로 노골적인 행위를 실연한다고 표시하는 성인, 성적으로 노골적인 행위를 미성년자가 실연한다는 것을 표시하는 사실적인 영상(images)을 시각적으로 묘사하는 포르노물(pornographic material)을 포함시켜야 한다.

라) 저작권 및 저작인접권 침해에 관한 범죄

협약은 컴퓨터시스템을 이용하여 저작권 및 저작인접권을 침해하는 것을 범죄로 규정하고 있다. 각 당사국은 문예저작물의 보호에 관한 베른협약(Bern Convention for the Protection of Literary and Artistic Works)의 파리개정협약과 지적재산권협약 및 세계지적소유권기구 저작권협약(WIPO Copyright Treaty)에 따라 동 협약이 부여한 인격권(moral rights)을 제외하고는 악의(wilfully)로 상업적 목적(commercial scale)에서 컴퓨터시스템을 이용하여 저작권을 침해하는 행위를 국내법상의 범죄로 규정하여 처벌할 의무로 부과함과 동시에, 실연가, 레코드제작자, 방송사업자 보호를 위한 국제협약(로마협약), 지적재산권협약, 세계지적소유권기구 실연 및 음반 협약(WIPO Performances and Phonograms Treaty)에 따라 동 협약이 부여한 인격권(moral rights)를 제외하고는 악의(wilfully)로 상업적 목적에서 컴퓨터시스템을 이용하여 저작인접권을 침해하는 행위를 처벌하도록 의무지우고 있다(협약 제10조).

마) 종범의 책임과 처벌

협약은 제2조 내지 제10조의 행위를 범죄로 규정한 이외에 동 범죄에 가담한 종범의 책임과 처벌(Ancillary liability and sanctions)에 관해서도 별도로 규정하고 있다.

첫째, 협약 제2조 내지 제10조의 범죄를 방조 또는 교사하는 행위, 동 협약 제3조 내지 제5조, 제7조, 제8조, 제9조 1.(a) 및 제9조 1.(c)의 범죄의 미수를 미수, 방조 또는 교사(Attempt and aiding or abetting)하는 행위를 국내법상 처벌해야 한다(협약

제11조).

둘째, 법인을 대표하는 권한, 법인을 위하여 의사결정을 하는 권한 또는 법인을 감독할 수 있는 지위에 있는 자연인(natural person)이 개인의 이익을 위해서 동 협약에 규정된 범죄를 행한 경우에 법인이 책임(Corporate liability)질 수 있도록 각 당사국은 국내법상의 입법 및 그에 부수되는 조치를 취해야 한다(협약 제12조). 나아가 동 협약은 제12조 제1항의 지위에 있는 자의 관리 및 감독 태만으로 인하여 당해 법인의 자연인이 법인의 이익을 위해 동 협약의 범죄를 행한 경우에도 당해 법인이 책임을 질 수 있도록 하는데 필요한 조치를 취해야 한다. 또한 당사국은 형사·민사 또는 행정책임을 국내법에 따라 부과할 수 있으며 법인에 대한 책임은 자연인의 형사책임과 별도로 부과되도록 하여야 한다.

셋째, 동 협약은 제2조 내지 제11조에 규정된 범죄를 효과적으로 그리고 적정하게 처벌하여 범죄를 방지할 목적으로 자유를 박탈하는 형벌을 부과할 수 있으며 법인의 책임도 벌금형 이외에 형사상 또는 행정적 제재나 조치를 부과할 수 있도록 입법하여야 한다(협약 제13조).

(2) 수사절차 정비

협약은 제2조 내지 제11조에 규정된 범죄의 효과적 처벌과 방지를 위하여 제14조 내지 제21조에 걸쳐 절차규정을 두고 있다. 아울러 초국경적 범죄인 사이버범죄의 관할권을 제22조에 명시하여 전통 국제법상의 주권과 조화를 도모하고 있다.

협약은 일반규정으로서 절차 규정의 적용범위(Scope of Procedural Provision), 조건과 보호(Conditions and Safeguards), 저장된 컴퓨터데이터의 신속한 보존(Expedited preservation of stored computer data), 전송데이터의 신속한 보존 및 일부공표(Expedited preservation and partial disclosure of traffic data), 제출명령(Production Order), 저장된 컴퓨터데이터의 압수수색(Search and Seizure of Stored Computer Data), 전송데이터의 실시간 수집(Real-time collection of traffic data), 컨텐츠데이터의 감청(Interception of content data), 관할권(Jurisdiction)을 명시하고 있다.

이에 따라 협약 가입국은 저장된 컴퓨터 데이터의 신속한 보전, 수색 및 압수와 통신 기록의 신속한 보전 및 부분공개, 제출명령, 실시간 수집, 통신내용 감청, 재판권 등 가입국의 수사 및 재판과 관련한 권한 및 절차를 정비하여야 한다.

(3) 국제공조체계 확립

협약은 사이버범죄의 특성이 네트워크를 이용하여 전 세계 어느 곳에서나 발생할 수 있다는 점을 주목하고, 동 범죄의 처벌을 위해서는 범죄인인도와 형사사법공조가 특히 필요하다는 점을 인식하여 제3장에서 국제공조(international cooperation)를 규정하고 있다.

협약은 당사국들이 서로 가능한 한 넓은 범위의 국제공조를 행하도록 하고 있다. 이 원칙은 협약의 당사국들이 서로에게 폭넓은 공조를 제공하여 정보나 범죄증거가 국제적으로 급속하게 이동하는 것을 최소화하자는 것이라 할 수 있다. 국제공조의 범위 또한 범죄에 사용되는 전자증거의 수집뿐 아니라 동 협약 제14조 제2항이 규정한 바와 같이 컴퓨터시스템과 컴퓨터데이터와 관련된 모든 범죄로 한다. 즉 컴퓨터시스템을 이용하여 행해진 범죄와, 살인과 같이 컴퓨터시스템을 이용한 범죄가 아니더라도 그 증거가 전자증거와 관련이 있는 경우를 포괄하는 것이다.

또한 공조는 형사사건의 국제공조와 관련 있는 국제합의의 적용, 상호입법이나 형평에 기초하여 합의한 협정(arrangements) 및 국내법에 따라 제3장의 규정에 일치되도록 행사될 것을 요구하고 있다. 따라서 이는 일반적인 원칙으로 당사국들간에 유효한 국제형사사법공조협약이나 국제공조를 규정한 국내법상의 관련규정을 파기하는 것이 아니다. 이러한 원칙에 기초하여 동 협약은 제24조 내지 제34조에 걸쳐 국제공조에 관한 상세한 내용을 열거하고 있다.

따라서 협약 가입국은 범죄인 인도, ISP의 사용자 발신처 및 통신기록 보존·제출, 통신기록 제공, 국가간 상시협력창구 등 사이버범죄에 대응하기 위한 국제공조수사체제를 확립하여야 한다.

Ⅳ. 국내법과의 비교분석

1. 개 요

우리나라는 1995년 이후 형법 개정(1995), 정보통신망이용촉진및정보보호등에관한법률 제·개정(1995, 1998, 2000), 정보통신기반보호법 제정(2001), 통신비밀보호법 개정(2001) 등 각종 입법을 통하여 사이버시큐리티 및 사이버범죄에 대한 규정을 상당히 체계적으로 정비하고 있다. 특히 2001년 1월 제정된 정보통신기반보호법은 주요 정보통신인프라를 보호하기

위한 조직 및 체계를 마련하고 이를 침해하는 행위를 엄중처벌하는 규정을 두고 있다. 다음에서는 사이버범죄방지협약의 주요 내용을 우리 법과 비교, 분석한다.

2. 사이버범죄의 처벌

사이버범죄방지협약과 국내법의 규정내용을 비교하면 협약에서 규정하는 4가지 유형의 사이버범죄가 국내법에서도 범죄로 규정 및 처벌되나 다음과 같은 차이가 있다.

협약 제2조의 불법접근(해킹)과 제4조의 데이터 손괴는 우리법에서도 범죄로 규정하여 처벌되고 있으며, 특히 범죄의 대상 내지 그 결과에 따라 처벌을 달리하는 합리적인 입장을 취하고 있다. 다만, 협약 제11조가 불법접근(해킹)과 데이터 손괴의 미수범을 처벌하도록 하고 있으나, 우리법은 정보통신기반보호법(제28조제2항)의 경우를 제외하고는 미수범을 처벌하지 않는다. (정보통신기반보호법도 "해킹 등에 의한 주요정보통신기반시설의 교란·마비 또는 파괴" 및 "저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위에 의한 주요정보통신기반시설의 교란·마비 또는 파괴" 행위의 미수를 처벌한다고 하여 해킹 및 데이터를 조작·파괴·은닉 또는 유출 자체의 미수를 포함하는지 의문의 여지가 있다.)

다음으로 협약 제6조 장치의 오용에 해당하는 규정이 우리법에는 없다. 현재 해킹, 컴퓨터바이러스 등에 관한 일반법의 역할을 하는 법이 정보통신망이용촉진및정보보호등에관한법률이므로 이에 해당조항을 신설하는 방안을 검토할 수 있을 것이다.

협약에서는 컴퓨터바이러스 유포와 관련하여 제작·유포하는 것뿐만 아니라 소지(possession)하는 행위 자체도 처벌대상이 된다고 규정하나(협약 제6조 제1항 b), 국내법은 소지행위를 처벌하지 않는다.

협약 제9조의 아동포르노 관련 범죄와 관련하여 협약이 필수 입법사항으로 정하는 ① 컴퓨터 시스템을 통하여 아동포르노의 제작, 제공, 게시, 배포하는 자, ② 아동이 성행위에 등장, ③ 18세 미만을 포함하는 것과 관련하여 청소년의성보호에관한법률은 협약상의 필수 입법사항을 모두 만족하고 있으며, 연령에 대하여는 19세 미만이라고 하여 보호하는 청소년의 범위가 협약보다 넓다.

협약에서는 미수범을 처벌하도록 규정하나, 국내법은 협약 제2조의 불법 접근, 제4조 및 제5조의 데이터 또는 시스템 손괴와 관련한 정보통신기반보호법, 협약 제7조 및 제8조와 관련한 위조 또는 사기에 대한 형법 그리고 협약 제9조와 관련한 청소년이용 음란물의 경우 외에는 미수범 처벌규정 없다. 한편, 방조 및 교사는 형법상 공범으로 처벌받으며(형법 제31조, 제32조), 이는 형법 제8조에 의하여 다른 법령의 범죄 및 벌칙에도 적용된다. 따라서 방조 및 교사에 대해서는 우리법으로 충분히 규율되고 있다고 할 수 있다.

협약에서는 법인의 책임도 인정하나(협약 제12조), 국내법에는 불법 접속(해킹), 데이터 손괴 및 아동포르노와 관련한 범죄에 대해서만 법인에 대한 양벌규정이 있고 다른 범죄에 대해서는 양벌규정이 없다.

3. 수사절차

절차법 규정에 있어서 사이버범죄방지협약은 저장된 컴퓨터 데이터의 신속한 보존과 압수·수색(협약 제16조, 제19조), 트래픽 데이터의 신속한 보존 및 일부 공개와 실시간 수집(협약 제17조, 제20조), 컨텐츠 데이터의 감청(협약 제21조)에 대해 상세히 규정하고 있으나, 국내법은 이에 대한 세부적인 규정이 미흡하다.

4. 국제공조

끝으로 국제공조에 있어서 사이버범죄방지협약은 매우 상세한 규정을 두고 있으나(협약 제23조 내지 제35조), 국내법에는 이에 관한 세부적인 규정이 미흡한 실정이다.

Ⅴ. 사이버범죄방지협약의 수용 움직임

사이버범죄방지협약의 수용과 관련하여서는 협약의 서명 및 비준과 별도로 UN, OECD, APEC 및 기타 지역기구나 개별국가에서 다양한 입법노력이 이루어졌다.

특히 APEC에서 미국은 지난 2002년 8월 20일과 21일 멕시코 아카풀코에서 개최된 제3차 고위관리회의(SOM III)에서 2001년 APEC 정상회의(중국 베이징)에서 채택된 반테러 성명의 이행을 위한 별도의 성명을 마련하여 2002년 10월 26일과 27일 멕시코 로스·카보스에서 열리는 정상회의에서 채택하였다. 이 성명에서는 2003년말까지 사이버범죄방지협약 수준의 포괄적인 사이버시큐리티 및 사이버범죄 관련법률을 입법할 것과 2003년 10월까지 사이버범죄를 담

당하는 국가기관 및 국제고급기술 연락기관을 정할 것을 내용으로 하고 있다.

한편 각국 정부와 달리 기업단체 및 시민단체들은 사이버범죄방지협약이 인터넷 사업발전을 저해할 가능성 및 프라이버시 침해우려가 있다는 부정적인 입장이 우세하다. 또, 인터넷서비스제공자들은 협약에 따라 정보 보존 및 공개를 위한 대폭적인 시스템변경 및 확장에 고비용 지출을 우려하고 있다.

Ⅵ. 결 론

해킹, 컴퓨터바이러스 등 사이버범죄는 대체로 국내법상 처벌이 가능한 국내범죄이지만, 국경이 따로 없는 이른바 '신종 국제범죄'로서 개별국가의 노력만으로는 충분하게 대응할 수 없다. 현재까지 사이버범죄에 대해 효과적인 대응이 이루어지지 않은 이유는 각국이 사이버범죄를 국내법상의 실체적 범죄로 규정하고 있을 뿐, 이에 대한 효과적 수사, 압수, 수색, 기소 및 판결을 위한 국제협약이나 메카니즘이 마련되지 않았기 때문이다. 따라서 국제적인 사이버범죄에 제대로 대응하기 위해서는 기술적 측면에서의 사전예방 및 사후대응 공동협력만으로는 충분하지 않으며, 이들 범죄의 수사 및 처벌을 위한 공동협력이 필수적이다.

이러한 점에서 실체법적, 절차법적 규정 뿐만 아니라 형사사법공조에 대한 규정을 모두 담고 있는 사이버범죄방지협약은 향후 국제적인 사이버범죄에 대한 대응에 있어서 가장 중요한 규범적 기초가 될 것이며, 21세기 지식정보사회 강국을 지향하는 우리나라의 입장에서 협약 가입의 필요성은 크다고 할 수 있다.

그러나 우리나라는 협약의 제정에 참여한 국가가 아니어서 우리나라의 참가의사 표시만으로 협약에 가입할 수 있는 것이 아니며, 협약의 발효 후 유럽평의회 각료회의가 체약국의 만장일치 동의를 얻어 참가요청(invite to accede)을 하는 경우 이에 응하는 형태로 가입할 수밖에 없다. 하지만 최근 UN, OECD, APEC 등 국제기구에서 사이버범죄방지협약의 수용확대가 논의되고 있으므로 조만간 우리나라에도 협약 가입의 문제가 현실화될 것이다.

이러한 상황에서 우리나라가 취할 수 있는 것은 UN, APEC 등 국제적 합의에 따라 우리나라의 실체법과 절차법 그리고 사이버범죄 수사체계를 사이버범죄방지협약 수준으로 정비하는 일이다. 그리고 우리 법체계와 국가이익의 관점에서 협약을 면밀히 분석하고 우리가 취할 입장을 정리하는 것이다.

참 고 문 헌

[1] 한국사이버감시단 편, 2001 한국사이버범죄백서, 전자신문사, pp. 00-00, Dec. 2001.

[2] 금봉수, *사이버범죄 방지를 위한 국제공조방안 연구*, 경희대 박사학위논문, 2001.

[3] サイバー刑事法研究會, 「歐州評議會サイバー犯罪條約と我が國の對應について」, 經濟産業省, 2002年4月.

[4] CONVENTION ON CYBERCRIME, Budapest, 23.XI.2001

〈著者紹介〉

박 영 우 (Young-Woo Park)

1985년 2월 : 고려대학교 법과대학 법학과 졸업(법학사)
1988년 8월 : 고려대학교 대학원 법학과 석사과정 졸업(법학석사)
1995년 8월 : 고려대학교 대학원 법학과 박사과정 졸업(법학박사)
1995년 1월~1998년 6월 : 법무부 법무자문위원회 연구위원
1998년 7월~현재 : 한국정보보호진흥원 선임연구원
관심분야 : 전자상거래 및 정보보호 관련 정책 및 법제도