국내외 컴퓨터범죄관련 처벌법규 분석

이대기,김태성,노종혁,진승헌,정교일

한국전자통신연구원

Analysis of the Domestic and International Laws on Computer Crime

Daiki Lee, Taesung Kim, Jonghyuk Roh, Seunghun Jin and Kyoil Chung

Electronics and Telecommunications Rersearch Institute

요 약

본 논문에서는 최근 급격하게 증가하고 있는 해킹, 컴퓨터바이러스 유포 등 각종 전자적 침해행위, 개인정보의 광범위한 수집과 오·남용, 음란·폭력정보의 범람, 익명성·비대면성을 악용한 인권 침해행위 및 신종 사이버범죄 등의 정보화 역기능에 대처하기 위한 국내 컴퓨터범죄관련 처벌법규가 제·개정시 강화되어 어느 정도 효과적으로 대응할 수 있게 되었으나 국내외 컴퓨터범죄관련 처벌법규 체계를 조사·분석하여 관련 법·제도의 개선방향을 제시한다.

I. 서론

최근 인터넷을 이용한 각종 해킹, 컴퓨터바이러스 유포 및 사이버범죄 등이 크게 증가하고 있으며, 수법도 고도화, 지능화되어 가고 있다. 공공기관 비밀번호 파일의 불법 유출, 홈뱅킹 및 폰뱅킹 사고, 국제적 해킹 사고 등 국가 또는 개인정보 누출과 정보화 역기능 현상이 국가사회 전반에 걸쳐서 심각한 문제로 대두되고 있다. 이러한 위협은 지식정보화사회로 진입하게 되면서 전통적으로 분류된 컴퓨터 및 네트워크에 대한 위협에 새로운 형태의 위협이 가미한 형태로 나타나고 있다. 이러한 컴퓨터범죄나 사이버범죄가 급증하고 있으며, 조직화된 사이버테러(Cyber Terror)도 확산되어 가고 있다. 사이버테러는 국경없는 신종 컴퓨터범죄의 일종으로 정보통신망을 통하여 국가사회의 주요 기반시설을 파괴하는 대규모적 범죄행위이다. 이러한 컴퓨터범죄 행위 등을 최소화하기 위하여 정보보호관련 법규의 제·개정시 처벌규정 등이 한층 더 강화되고 있다. 국내외 컴퓨터범죄와 관련한 처벌규정을 종합적으로 파악·분석하고 그에 따른 개선방향을 제시하여 향후 정보보호관련 법규의 재정비에 도움을 주고자 한다.

II. 컴퓨터범죄 개요

1. 컴퓨터범죄의 정의

경제협력개발기구(OECD)에서 컴퓨터범죄를 데이터의 자동처리와 전송을 수반하는 불법적·비윤리적, 권한 없는 행위로 인한 컴퓨터 자료에 대한 비정상적인 행위로 규정했다.

스와이저(James A. Sweizer)는 컴퓨터를 사용하거나 컴퓨터, 단말기, 통신망 등 컴퓨터의 구성요소에 대한 접근을 요소로 하는 범죄로 정의했다. 그리고 맨델(Steven L. Mandel)은 컴퓨터를 사용함으로써 같은 조건에서 컴퓨터를 사용하지 않는 경우보다 큰 위험을 일으킬 비난 가능성이 있는 행위로 규정했고, 돈 파커(Don Parker)는 컴퓨터시스템 내에서 행해진 화이트 칼라의 범죄이고, 상업 범죄의 도구로써 컴퓨터를 사용하는 행위로 정의했다. 따라서 컴퓨터범죄는 불법적이고 비윤리적인 방법으로 권한 없이 컴퓨터에 의해 제어된 자원이나 컴퓨터 사용이 포함하는 단체나 개인에 대한 사기와 오용이라 할 수 있다. 이와 같이 컴퓨터에 대한 일체의 침해행위를 컴퓨터범죄(Computer Crime)라고 할 수 있는데, 최근에는 독립된 컴퓨터 자체에 대한 범죄의 범주를 넘어서서 네트워크를 이용하여 행해지는 컴퓨터범죄를 포괄하기 위하여 사이버범죄(Cyber Crime)라는 용어가 자주 쓰이고 있으며, 이러한 컴퓨터범죄가 인터넷을 통하여 이루어지는 경우 인터넷범죄(InternetCrime)라고 하며,하이테크범죄(High-tech Crime)라고도 한다.

2. 컴퓨터범죄의 특징

컴퓨터범죄는 여러가지면에서 전통적인 범죄와 구분되는 특징을 가지고 있다.

첫째로 컴퓨터범죄는 연속적으로, 반복적으로 이루어지는 경우가 많다. 컴퓨터 부정조작이나 시스템 침입 등은 단발성 범죄로 그치기보다는 빈

번하게 반복되는 경우가 훨씬 많다. 이는 컴퓨터 시스템에서 그 진행과정이 매우 규칙적으로 구성되어 있어서 행위자가 일단 조작방법을 터득하기만 하면 이를 임의로 쉽게 이용할 수 있기 때문이다.

둘째로 범행의 자동성과 광역성을 가지고 있다. 즉, 프로그램 조작에 의하여 발생하는 컴퓨터범죄는 행위자가 어떤 다른 행위를 하지 않더라도 일단 불법 변경된 고정자료를 호출하거나 불법 프로그램을 삽입할 때마다 자동적으로 범죄행위가 유발된다. 또한, 현재의 컴퓨터는 대부분이 통신기능을 보유하고 있고, 원격지에 있는 단말기를 통신회선에 연결하여 정보의 전달과 처리를 하도록 통신시스템에 접속되어 있기 때문에 범죄자는 이러한 통신시스템을 이용하여 원격지에 범행할 수 있게 되어 범죄가 광역화되고 있다.

셋째로 컴퓨터범죄의 적발과 증명은 대단히 곤란하다. 컴퓨터조작은 단시간에 처리되는 양이 대단히 많기 때문에 부정조작의 경우 이를 사후에 자세히 검토하여 잘못을 가려낸다는 것이 사실상 어렵거나 경제적으로 막대한 비용이 드는 경우가 많다. 또한, 저장장치가 폐쇄성과 은닉성을 갖기 때문에 그 적발과 증명이 매우 곤란하다.

넷째로 컴퓨터범죄의 고의성 입증이 어렵다. 비록 컴퓨터상에 오류가 발견된다고 하더라도 행위자가 범죄의사가 명확하게 표현되었을 때에는 문제가 없지만 단순히 자료의 변경, 손실 등의 형태에 불과할 경우에는 범행 의사가 없이 외부관리의 소홀 등의 실수로 발생한 것처럼 말소될 때에 입증이 곤란한 경우가 허다하다.

3. 국내 컴퓨터범죄관련 법규

컴퓨터의 보급확대와 정보통신망의 이용 확대에따라 정보화의 역기능에 대처하기 위하여 국내 컴퓨터범죄관련 법규 제·개정시 컴퓨터범죄의 처벌규정이 더욱 강화되고 있다.

우리나라의 법령 총 건수는 3,624건(2002.9.30./법제처 자료)이며, 그 내용은 헌법 1건, 법률 1,019건, 대통령령 1,360건, 총리령 22건 및 부령 1,222건이다.

국내 컴퓨터범죄관련 처벌에 정보통신망이용촉진및정보보호등에관한법률, 통신비밀보호법, 형법 등 24건 정도의 법률이 적용되고 있다.

III. 컴퓨터범죄의 유형별 처벌법규

컴퓨터범죄의 유형과 범위를 정확하게 설정하는 것은 어려운 일이지만 컴퓨터와 범죄의 상관관계를 통해 그에 대한 개략적인 기준은 설정할 수 있다고 본다.

첫째로 컴퓨터는 범죄적인 측면에서 공격의 대상으로 파악된다. 컴퓨터나 정보통신망 자체 또는 그 안에 저장된 데이터가 침입행위나 파괴행위의 대상이 되는 경우로써 해킹이나 바이러스 유포, 서비스공격행위 등이 여기에 해당된다.

둘째로 컴퓨터는 범죄에 있어 부수적인 역할을 할 수 있다. 예컨데 마약밀매자가 자신의 마약거래에 관한 자료를 컴퓨터에 저장하는 경우가 이에 해당된다. 여기에서 컴퓨터는 마약거래라는 범죄와 관련하여 그 증거자료에 해당하는 데이터를 저장하는 부수적인 기능을 수행한다고 볼 수 있다.

셋째로 컴퓨터가 범죄의 직접적인 수단으로 이용되는 경우이다. 예컨데 컴퓨터나 인터넷을 이용한 전자상거래상의 사기행위나 인터넷을 통한 전문약품의 불법판매, 도박, 음란물 배포행위와 같은 것이다. 이중 둘째와 셋째의 경우는 컴퓨터가 범죄행위의 직접적이거니 보조적인 수단으로 사용된다는 점에서 공통점이 있으므로 양자를 하나로 묶는다면 컴퓨터와 범죄의 관계는 컴퓨터가 범죄행위의 대상이 되는 경우와 컴퓨터가 범죄행위의 수단으로 사용되는 경우 두가지로 구분할 수 있다.

국내의 컴퓨터범죄 건수(경찰청 자료)는 1999년에 1,709건, 2000년에 2,444건, 2001년에 33,289건, 2002년 8월에 39,482건으로 날로 급격히 증가하고 있는 추세를 나타내고 있다.

컴퓨터범죄는 해킹, 컴퓨터바이러스 유포, 전자우편, 개인비밀침해, 음란, 명예훼손, 몰래카메라, 컴퓨터사용사기 등의 유형(대검찰청 자료)으로 구분하여 처벌규정을 적용하고 있다.

1. 국내 컴퓨터범죄 처벌법규

1) 데이터의 부정조작·변조 범죄

전자매체를 이용한 데이터의 부정조작·변조는 자료나 정보의 조작, 프로그램 조작으로 전문적인 해커뿐만 아니라 시스템이나 정보통신망과 관련된 일반인들도 얼마든지 범행이 가능하다. 자료나 정보를 조작 또는 변조하는 목적은 경제적인 이익을 취하기 위한 것이 대부분이나 일부 호기심으로 하는 경우도 있지만 위조나 변조할 수 있는 첨단 복사장비의 보급이나 통신망 사용의 일반화도 중요한 요인으로 작용한다. 데이터의 부정조작·변조범죄는 공공기관의개인정보보호에관한법률 제11조(개인정보취급자의 의무)에서 공공기관의 개인정보처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경 또는 말소한 자는 10년 이하의 징역에 처하도록 규정하고 있다. 무역업무자동화촉진에관한법률 제18조(전자문서 및 무역정보에 관한 보안)제1항에서 컴퓨터파일에 기록된 전자문서 또는 데이터베이스에 입력된 무역정보를 위조 또는 변조하거나 이를 행사한 자는 1년 이상 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 규정하고 있으며, 산업기술기반조성에관한법률 제8조(산업정보의 안전관리 등)제4항에서 사업시행자의 컴퓨터파일에 기록된 전자문서 또는 데이터베이스에 입력된

산업기술정보기록을 위조·변조하거나 위조·변조된 전자문서 또는 산업정보기록을 행사한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 규정하고 있으며, 신용정보의이용및보호에관한법률 제32조(벌칙)제11항에서 권한 없이 신용정보를 검색·복제 기타의 방법으로 이용한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 규정하고 있고, 정보통신기반보호법 제12조(주요정보통신기반시설 침해행위 등의 금지)에서 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 규정하고 있으며, 정보통신망이용촉진및정보보호등에관한법률 제48조(정보통신망 침해행위 등의 금지)에서 정당한 사유없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 규정되어 있으며, 화물유통촉진법 제48조의7(전자문서 및 무역정보의 보안)제1항에서 물류전산망에 의한 전자문서를 위작 또는 변작하거나 그 사정을 알면서 위작 도는 변작된 전자문서를 행사한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 규정하고 있으며, 형법 제227조의2(공전자기록 위작·변작)에서 사무처리를 그르치게 할 목적으로 공무원 또는 공무소의 전산기록 등 특수매체기록을 위작 또는 변작한 자는 10년 이하의 징역에 처하도록 규정하고 있으며,제228조(공정증서원본 등의 부실기재)에서 공무원에 대하여 허위신고를 하여 공정증서원본 또는 이와 동일한 전자기록 등 특수매체기록에 부실의 사실을 기재 또는 기록하게 한 자는 5년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 규정하고 있으며, 제232조의2(사전자기록 위작·변작)에서 사무처리를 그르치게 할 목적으로 권리·의무 또는 사실증명에 관한 타인의 전자기록 등 특수매체기록을 위작 또는 변작한 자는 5년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 규정하고 있다.

2) 비밀침해에 관한 범죄

비밀침해에 관한 범죄는 주로 자료나 정보의 무단유출 등으로 컴퓨터통신이나 정보통신망을 통하여 다른 컴퓨터나 시스템에 함부로 침입하여 파일을 출력하거나 전송하는 방법, 혹은 무단으로 자료나 정보를 복사하는 방법, 정보통신망의 통신회선이나 무선을 이용한 통신망의 전송정보를 도청하는 행위, 정보통신망에의 전자적 침해 행위 등에 관한 범죄를 말한다. 정보통신망의 전자적 침해행위에 관한 범죄는 정보통신기반보호법 제12조(주요정보통신기반시설 침해행위 등의 금지)에서 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 하였다.

비밀침해에 관한 범죄는 공공기관의개인정보보호에관한법률 제11조(개인정보취급자의 의무)에서 개인정보를 누실 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적으로 사용한 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 규정하고 있으며, 반도체집적회로의배치설계에관한법률 제44조(비밀유지의무)에서 직무상 알게된 비밀을 다른 사람에게 누설한 자는 2년 이하의 징역 또는 500만원 이하의 벌금에 처하도록 규정하고 있다. 부정경쟁방지및영업비밀보호에관한법률 제18조(벌칙)에서 기업의 임원 또는 직원으로서 그 기업에 유용한 기술상의 영업비밀을 이유없이 외국에서 사용하거나 외국에서 사용될 것임을 알고 제3자에게 누설한 자는 7년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 규정하고 있으며, 무역업무자동화촉진에관한법률 제18조(전자문서 및 무역정보에 관한 보안) 제2항에서 지정사업자·무역업자·무역유관기관 및 대행처리사업자의 컴퓨터화일에 기록된 전자문서 또는 데이터베이스에 입력한 무역정보를 훼손하거나 그 비밀을 침해한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 규정하고 있다. 산업기술기반조성에관한법률 제8조(산업정보의 안전관리 등)제3항에서 사업시행자의 컴퓨터화일에 기록된 전자문서 또는 데이터베이스에 입력된 산업정보기록을 훼손하거나 그 산업정보의 비밀을 침해한 자 또는 그 업무상 알게 된 산업정보에 관한 비밀을 누설하거나 이를 도용한 사업시행자의 임원·직원이거나 임원·직원이었던 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 규정하고 있으며, 신용정보의이용및보호에관한법률 제 27조(업무목적외 누설금지 등)제1항 및 제2항에서 업무상 알게 된 타인의 신용정보 및 사생활 등 개인적 비밀을 업무목적외로 누설 또는 이용한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 규정하고 있다. 전기통신사업법 제54조(통신비밀의 보호)제1항에서 전기통신사업자가 취급 중에 있는 통신의 비밀을 침해하거나 누설한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 규정하고 있다. 정보통신망이용촉진및정보보호등에관한법률 제49조(비밀 등의 보호)에서 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자는 5년 이하의 징역 도는 5천만원 이하의 벌금에 처하도록 규정하고 있으며, 통신비밀보호법 제3조(통신 및 대화비밀의 보호)에서 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취한 자는 10년 이하의 징역과 5년 이하의 자격정지에 처하도록 규정하고 있으며, 화물유통촉진법 제48조의7(전자문서 및 물류정보의 보안)제2항과 제5항에서 물류전산망에 의하여 처리·보관 또는 전송되는 물류정보를 훼손하거나 그 비밀을 침해·도용 또는 누설한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 규정하고 있으며, 형법 제140조(공무상 비밀표시 무효)에서 공무원이 그 직무에 관하여 봉함 기타 비밀장치한 문서·도화 또는 전자기록 등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아 낸 자는 5년 이하의 징역 또는 700만원 이하의 벌금에 처하도

록 규정하고 있다. 제316조(비밀침해)에서 봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록 등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자는 3년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처하도록 규정하고 있다.

3) 업무방해에 관한 범죄

업무방해에 관한 범죄는 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록에 손상을 주거나 유·무선 통신을 통해 허위 정보 또는 부정한 정보를 정보시스템에 입력하거나 장애를 유발하도록 하여 고유의 정보처리 업무를 방해하는 범죄로 정보통신망이용촉진및정보보호등에관한법률 제48조(정보통신망 침해행위 등의 금지) 제2항에서 악성프로그램을 전달 또는 유포한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 규정하고 있으며, 형법 제314조(업무방해)제2항에서 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자는 5년 이하의 징역 또는 1천500만원 이하의 벌금에 처하도록 규정하고 있다.

4) 재물손괴·은닉 등에 관한 범죄

재물손괴·은닉 등에 관한 범죄는 공공기관이나 민간기관의 컴퓨터 시스템에 저장된 전자기록(데이터)이나 저장장치(하드디스크, 테이프 등) 등에 있는 데이터를 손상하거나 은닉 또는 본래의 정보가치를 해하는 경우와 타인의 정보를 손상 또는 은닉하여 그 효용을 해하는 범죄로 형법 제141조(공용서류 등의 무효,공용물의 파괴)제1항에서 공무소에서 사용하는 서류 기타 물건 또는 전자기록 등 특수매체기록을 손상 또는 은닉하거나 기타 방법으로 그 효용을 해한 자는 7년 이하의 징역 또는 1천만원 이하의 벌금에 처하고, 제366조(재물손괴 등)에서 타인의 재물, 문서 또는 전자기록 등 특수매체기록을 손괴 또는 은닉 기타 방법으로 그 효용을 해한 자는 3년 이하의 징역 또는 700만원 이하의 벌금에 처하도록 규정하고 있다.

5) 컴퓨터사기에 관한 범죄

컴퓨터사기에 관한 범죄는 컴퓨터 보급확대와 그 기능이 커짐에 따라 컴퓨터를 이용한 범죄가 증가하고 있음에도 컴퓨터를 이용하여 타인의 허락없이 재산적 이익을 취득한 경우 등에 적용되는 범죄로 형법 제 347조의2(컴퓨터 등 사용사기)에서 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처하도록 규정하고 있다.

2. 국외 컴퓨터범죄 처벌법규

1) 해킹 범죄

미국은 국가 중요 컴퓨터시스템의 비밀성, 무결성 및 안전성 보호증진을 위해 국가정보기반보호법(National Information Infrastructure Protection Act)을 1996.10.11.입법하였다. 이 법에서 7가지 컴퓨터범죄행위 즉, 1)비밀지정 국가정보의 침해, 2)재정,국가 및 기타 컴퓨터정보의 침해, 3)국가컴퓨터시스템의 침해, 4)중요한 컴퓨터의 무권한 사용, 5)컴퓨터에 대한 손상, 6)부정거래에 의한 사취, 7)컴퓨터에 대한 직접적인 협박 등을 범죄행위로 규정하고 있으며, 위반시에는 10년 이하의 징역에 처하도록 규정하고 있다. 또한, 최근에 컴퓨터보안과 관련하여 미 정부의 포괄적인 역할을 규정하고 미국 국립표준기술연구소(NIST)의 위상를 강화하고 사이버 보안표준을 마련,개선하는 내용을 골자로하는 연방정보보안관리법안(Federal Information Security Management Act)이 미 상원통상위원회에 제출되었다.

영국은 컴퓨터자료에 대한 무책임 등의 범죄의 구성요건과 처벌 등을 규정하고, 범죄의 소추에 따른 관할 문제 등을 규정하기 위하여 컴퓨터오용방지법(Computer Misuse Act)을 1990.6.29.입법하였다. 이 법에서는 컴퓨터자료에 대한 무단침입 행위시에는 약식판결에 의하여 6개월 이하의 금고 또는 표준등급 5등급 이하의 벌금이나 이를 병과하여 처벌하며 컴퓨터내용의 무단변경행위시에는 6개월 이하의 금고 또는 법정최고 이하의 벌금이나 이를 병과하고, 정식기소에 따른 판결에서는 5년 이하의 금고 또는 벌금에 처하도록 규정하고 있다.

EU(유럽연합)는 회원국 내 정보시스템에 대한 조직화된 공격이 자행되고 있는 데에서 사이버공격에 대한 우려가 점증하는 가운데 보다 안전한 정보사회구현을 위해 유럽위원회(EC)가 2002.4.23.사이버범죄에 대한 회원국들의 대응기준을 제시할 법안초안을 발표하였으며,이 기준안 초안(Proposal for a Council Framework Decision on attacks against systems)은 정보시스템에 대한 범죄행위의 중요 유형인 해킹(Hacking), 컴퓨터바이러스(Computer Virus) 유포 및 웹사이트 훼손 등의 행위에 대해 회원국별로 가이드라인이 될 범죄행위의 유형 및 정의, 처벌기준 등을 마련할 수 있도록 하였다. 또한, 사이버범죄협약을 2001.11월에 제정하여 사이버 공간에서 발생할 각종 범죄들을 처벌할 수 있도록 각국의 국내법을 정비하도록하고 다양한 국제공조절차를 따르도록 함으로써 국제사회의 사이버범죄에 효율적으로 대처하도록 하였다.

캐나다는 컴퓨터시스템을 권한 없이 이용하거나 시스템을 파괴하는 것을 처벌할 수 있도록 1985년 형법(Criminal Code)을 개정하였다. 이 법상에 권한 없이 부정한 방법으로 컴퓨터서비스를 획득하거나 가로채는 행위자는 10년 이하의 징역

에 처하고 고의적인 데이터 파괴, 변경, 업무방해를 금지하며 이를 위규시에는 손괴죄를 적용하여 처벌하도록 규정하고 있다.

프랑스는 데이터자동처리시스템에 불법 액세스한 자는 1년 이하의 징역 또는 100,000프랑의 벌금에 처하고, 데이터자동처리시스템의 기능을 방해한 자는 3년 이하의 징역 또는 300,000프랑의 벌금에 처하고, 데이터자동처리시스템에 부정데이터 삽입 및 무단내용 변경한 자는 3년 이하의 징역 또는 300,000프랑의 벌금에 처하도록 규정하고 있다.

일본은 부정액세스행위의금지등에관한법률(법률제128호1999.8.13.)을 제정하여 2000.2.13.부터 시행 중에 있으며 부정액세스(Acccss) 행위자는 1년 이하의 징역 또는 50만엔 이하의 벌금에 처하고, 부정액세스 행위를 조장하는 자는 30만엔의 벌금에 처하도록 규정하고 있다.

호주는 컴퓨터범죄법을 제정하여 고의로 연방컴퓨터 혹은 연방을 위한 컴퓨터에의 부정액세스를 금지하고 있으며 위반시에는 6개월 이하의 징역에 처하도록 하고, 연방 데이터 파괴금지를 위반시에는 10년 이하의 징역에 처하도록 하였다.

스위스는 데이터 무단 삭제, 변경, 침해한 자는 3년 이하의 징역 또는 40,000스위스프랑의 벌금에 처하고, 데이터 무단 삭제, 변경, 침해를 목적으로 한 프로그램 작성, 수입, 선전, 게시, 회람한 자는 3년 이하의 징역 또는 40,000스위스프랑의 벌금에 처하고, 이익을 목적으로 한 행위자는 5년 이하의 징역에 처하도록 규정하고 있다.

말레이시아는 컴퓨터범죄법을 제정하여 사기목적의 부정액세스를 한 자는 150,000링기드의 벌금 또는 10년 이하의 징역 혹은 양벌에 처하도록 하고, 컴퓨터컨텐츠의 무단변경시에는 100,000링기드의 벌금 또는 7년 이하의 징역 혹은 양벌에 처하도록 하고 있으며 형법의 재산죄의 목적으로 행하여 졌을 경우에는 150,000링기드의 벌금 또는 10년 이하의 징역 혹은 양벌에 처할 수 있도록 규정하고 있다. 타인의 패스워드 부정사용시에는 25,000링기드의 벌금 또는 3년 이하의 징역 혹은 양벌에 처할 수 있도록 하였다.

2) 컴퓨터바이러스 등 유포 범죄

미국은 국가정보기반보호법에 고의적으로 보호대상 컴퓨터에 프로그램, 정보, 암호(Codc) 또는 명령을 전송하거나 그 행위 결과 권한 없이 의도적으로 손상시킨 자는 형사처벌할 수 있도록 규정하고 있다. 미 상원통상위원회는 사용자 동의없이 무차별적으로 발송되는 전자메일을 제재하는 스팸메일방지법을 2002.5월에 통과시켰으며, 발송자가 전자메일이나 실제 주소를 속이는 등 법을 위반시에는 벌금이나 징역형이 부과된다. 벌금은 최대 150만달러까지 매길 수 있도록 하고 주검찰이 스패머들을 체포할 수 있도록 규정하고 있다.

네덜란드는 형법에 누구든지 고의로 컴퓨터에 작동시키면 복제과정을 일으켜 컴퓨터에 위해를 일으키는 정보를 유포하거나 이러한 정보를 사용할 수 있게 한 자는 4년 이하의 징역 또는 100,000길더 이하의 벌금에 처하도록 규정하고 있다.

스위스는 형법에 함부로 전자적 자료를 소거·수정·파괴하는 자 또는 어떤 방법으로 든지 불문하고 이러한 행위를 할 수 있는 수단을 제조·배포·전파하거나 사용할 수 있게 한 자는 3년 이하의 징역이나 벌금에 처하고, 이로 인하여 중대한 피해를 야기한 때에는 징역 5년에 처하도록 규정하고 있다.

이탈리아는 형법에 프로그램을 직접 제작하지 않아도 제3자가 제작한 프로그램을 악의의 목적으로 유통하여 시스템 운용을 중단시키는 행위를 처벌하도록 규정하고 있다.

중국은 컴퓨터정보체계의 안전을 보호하기 위하여 안전보호등급제도의 실시와 공안기관의 안전 감독에 대한 권한 등에 관한 사항을 규정한 컴퓨터정보체계안전보호령을 1994. 2월에 제정하였다. 이 령에서 고의로 컴퓨터바이러스 및 그 밖의 유해한 데이터를 입력하여 컴퓨터정보체계의 안전을 위해하거나 허가받지 않고 컴퓨터정보체계 안전전용 제품을 판매한 경우에는 공안기관이 경고하거나 개인에 대해서는 5천위안 이하의 벌금을 부과하고 단체에 대해서는 1만5천위안 이하의 벌금을 부과하고 불법소득이 있는 경우에는 이를 몰수하는 외에 불법소득의 1배 내지 3배의 벌금을 부과하도록 규정하고 있다.

IV. 결론

인터넷으로 상징되는 전자커뮤니케이션 네트워크가 국가와 국경을 초월하여 구성되어 있는 것을 감안할 때 이를 통해 전개되는 사이버범죄를 효과적으로 차단하기 위해서는 국가와 국경을 초월한 공동의 노력 즉, 글로벌화된 사이버 공격, 불건전정보 유통에 대한 효과적 대응을 위해 국제공조체제 구축이 필요하겠다. 선진국에서는 정보화의 역기능방지 대책의 일환으로 고도의 암호기술 연구는 물론 정보산업 육성, 정보보호 전문인력 양성에 노력하고 있으며 개인정보보호 법제, 비밀수준관계 법제, 컴퓨터범죄방지 법제, 지식정보사회촉진 법제 등에서도 사이버공간에 대한 패러다임전환에 부합되는 괄목할만한 진전을 이룩하고 있다.

또한, 세계 각국은 정보시스템에 대한 범죄행위의 중요 유형인 해킹, 컴퓨터바이러스 유포 및 웹사이트 훼손 등의 행위에 대해 범죄행위의 유형 및 정의, 처벌기준 등을 명확히 규정하고 있으며 처벌규정도 강화하고 있다. 처벌규정은 사이버범죄를 예방하기에 충분할 만큼 효과적이고 균형잡힌 것으로 하며, 특히 조직적이거나 사회의 안정에 심각한 영향을 미치는 사이버범죄의 경우 가중처벌하는 경향이 두드리지고 있다. 미국을 비롯한 일부 국가에서는 범죄의 재범시에는 법에 의거 가중 처벌하도록 규정하고 있다.

국내의 해킹 건수(한국정보보호진흥원 자료)는

1999년에 572건(미국9,859건, 영국1,712건), 2000년에 1,943건(미국21,756건, 영국4,783건), 2001년에 5,333건(미국52,658건, 영국40,274건), 2002년8월에 4,677건(2002년9월에 미국73,359건, 영국74,754건)으로 급증세를 나타내고 있으며, 앞으로의 해킹·바이러스 공격은 에이전트화, 분산화, 자동화, 은닉화되는 등 더욱 지능화·고도화되고 있으며, 복합적인 형태로 악성화 될 것으로 예상되고 있다. 주요기반시설의 정보통신시스템이 상호연계됨으로써 사이버위협도 상호연계·공유되고 있으며, 고도화된 정보인프라는 국제해커들의 공격목표가 되고 있으므로 고도의 해킹방지 기술개발, 컴퓨터 범죄관련 법규의 정비 강화, 국가 해킹사고 예방 보안 활동 강화, 기관별 보안전문인력 양성 강화, 기관별 해킹사고처리체계 구축 등 범 정부적 대책이 지속적으로 강구되어야 하겠으며, 정보의 무권한적 침해에 대한 단일 법제연구도 적극적으로 검토되어야 하겠다.

참고문헌

[1] 최영호, "컴퓨터와 범죄현상", 컴퓨터출판사, 1996.7.

[2] 한국정보보호센터, "국내외 정보보호관련 법제도 현황", 1996.12.

[3] 정완, "하이테크범죄대책에 관한 국제 동향", 형사정책연구, 1999.9.

[4] 이정현, "사이버범죄협약에 대한 소고", 한국정보보호진흥원, 2001.7.

[5] 최양서, 서동일, 손승원, "네트워크 보안평가를 위한 해커 및 해킹기법 수준 분류,"한국정보보호학회지, 2001.10.

[6] 한국정보보호진흥원, "2001년 정보화역기능 실태조사 보고서", 2001.12.

[7] 김병준, "EC,사이버범죄에 대한 기준안 초안 검토서", 정보통신정책연구원, 2002.5.

[8] 정보통신부, "중장기 정보보호기본계획",2002.8.

[9] 이대기, 조영섭, 진승헌, 정교일, "국내 정보보호관련법규 분석",한국정보보호학회지, 2002.8.

[10] http://www.moleg.go.kr

[11] http://icic.sppo.go.kr

[12] http://www.certcc.or.kr

[13] http://www.cert.org

[14] http://www.cybercrime.gov

[15] http://www.ja.net/cert

[16] http://europa.eu.int