네트워크보안의 형사법적 보호

김형만†

요 약

컴퓨터·네트워크의 보급에 의하여 사회경제활동을 비롯한 다양한 활동들이 신속하고 효율적으로 행해지는 한편, 네트워크를 이용한 범죄도 용이하게 되어 사회시스템에 대한 취약성이 증가되고 있다. 범죄도 사회적 존재인 이상 이러한 가상공간에서 발생하는 피해에 대해서도 새롭게 조명하지 않을 수 없게 되었다. 따라서 본고에서는 20세기말부터 현제화하기 시작한 새로운 법적규제 공간으로서 네트워크상의 보안문제를 그 위협의 정도·태양에 따라 구분하여 살펴보고, 형사법적 규제의 필요성에 대해서 고찰하고자 한다. 특히 가상공간의 특수성을 전제로 기존의 법적규제에 대한 수정이 필요한지 여부와 그 근거는 무엇인지도 아울러 고찰하였다.

주제어 : 사이버범죄, 가상공간, 정보보안, 컴퓨터범죄, 부정 액세스

Network security and legal protection of the Criminal

Hyung-Man Kim†

ABSTRACT

The spread of computer and network gets various social and economic activities done quickly and efficiently. As a result, it makes a crime using network easy and increases the vulnerability of a social system. As there is a crime as a social being, we need to give careful consideration to the crime occurring in virtual space. Accordingly, the purpose of this paper is to investigate the regulatory need of the Criminal Procedure concerning the network security issues as the new legal and regulatory space that begins to be realized from the late of 20th century because of the extent of social threat. Above all, we addresses whether the amendment of existing legal regulations is necessary, based on the special characteristics of the virtual space.

Key Words : Cybercrime, Virtualspace, Information Security, Computer Crime, Unauthorized Access

† 광주대학교 경찰법행정학부 부교수
논문접수: 2011년 5월 6일, 1차 수정을 거쳐, 심사완료: 2011년 6월 10일
본 논문은 2011년 광주대학교 교내연구비에 의하여 지원되었음

1.서 론

컴퓨터·네트워크의 보급에 의하여 사회경제활동을 비롯한 다양한 활동들이 신속하고 효율적으로 행해지는 한편, 사회의 컴퓨터 시스템에 대한 의존도가 증가함에 따라 네트워크를 이용한 범죄[1]도 용이하게 되어 사회시스템에 대한 취약성이 증가하고 있는 것이 현실이다. 따라서 가상공간에 있어서도 컴퓨터 통신이라는 전자적 실재성을 가진 사회적 존재인 이상 그 사회를 반영한 형태로 규제할 필요성이 있는지 검토할 필요성이 제기되었다[1].

네트워크상에서의 컴퓨터 남용과 오용의 문제는 1960년대 말 발생하기 시작하여 초기에는 주로 타인의 패스워드를 수집·해독하는 프로그램인 트로이목마[2]를 설치하여 타인의 ID로 컴퓨터를 부정사용하는 위법행위가 대부분이었다. 다만 현재 문제가 되고 있는 컴퓨터바이러스도 컴퓨터 내의 프로그램을 변형하거나 기존 프로그램의 정상적인 작동을 방해하고 다른 컴퓨터를 감염시킨다는 점에서 이 유형에 속한다고 할 수 있다[2].

1970년부터 80년대는 컴퓨터의 성능과 정보통신기술의 급격한 성장을 배경으로 세계적으로는 컴퓨터를 악용한 범죄행위가 급증한 시기였다. 현금카드와 정보처리 시스템을 대상으로 한 은행의 금융시스템이 그 목표였다. 2001년 4월 우리나라에서 발생한 사건으로 어떤 해커가 신용카드정보처리 전문 업체의 시스템을 해킹하여 약 47만명의 주민번호와 신용카드번호 등 중요한 신용정보를 유출하려다 적발된 사건이 등이 바로 그것이다[3]. 이 시기에는 비밀번호의 조합 시스템이 조잡하였을 뿐만 아니라 보안에 관한 의식 수준도 낮아 범행을 조장한 측면도 있었지만, 수법은 그렇게 복잡하지는 않았다.

1990년대에 이르러 컴퓨터 네트워크의 확대와 이용도가 급속히 향상되었다. 제공되는 서비스도 다양하고, 인터넷의 학술적 이용이나 전자상거래 이용, 행정정보의 네트워크에 의한 제공이나 행정절차의 온라인화 등, 사회 구석구석까지 네트워크화 되어 갔다. 이것과 함께 컴퓨터·네트워크의 안전성 그 자체에 대한 위협도 증대되었다. 특히 대량의 데이터를 저렴하고 고속으로 전송할 수 있는 광통신이 일반화되어, 개인 레벨에서의 인터넷 접속이 일반화되자 정부와 기업의 컴퓨터뿐만 아니라 개인의 컴퓨터도 공격의 대상이 되어 피해의 양적확대라는 점에서 심각한 문제가 제기되었다.

본고에서는 20세기말부터 현제화하기 시작한 새로운 법적규제 공간으로서 네트워크상의 보안문제를 그 위협의 정도·태양에 따라 구분하여 살펴보고, 형사법적 규제의 필요성에 대해서 고찰하려고 한다. 특히 가상공간의 특수성을 전제로 기존의 법적규제에 대한 수정이 필요할지 여부와 그 근거는 무엇인지도 아울러 고찰하였다.

2. 네트워크의 안전성에 대한 위협

2.1. 사회의 아킬레스건으로서 네트워크

미국국무성(DOD)은 「Eligible Recever」라고 하는 군사연습을 1997년에 실시하였다. 종래 군사연습과 다른 것은 장소가 사이버공간이었다. 연습에는 30인 정도의 국가안전보장국 컴퓨터 전문가들로 편성되어, 「DOD의 직원으로서 알 수 있었던 지식은 사용하지 않는다」는 조건이 붙었다. 그들의 임무는 미국전역에 있는 전원 및 전화시스템의 차당방법을 발견하는 것과 DOD의 컴퓨터·네트워크에 침입하는 것이었다.

결과는 예상 이상으로 충격적이었다. 팀은 물론 실제로 사회에 충격을 주지는 않았지만, 송전제어 시스템에 침입하고, 시스템 전체를 제어할 수 있는 최상위의 관리자 권한을 취득하였다. DOD의 네트워크를 지배하는 관리권한도 취득하였다. FBI와 DOD는 팀을 추적하였지만 발견한 것은 미국의 본토에 본거지를 둔 1팀뿐이며 다른 3팀은 발견할 수 없었다. 팀의 멤버들은 시내의 가전매장에서 컴퓨터를 구입하여 일반적인 지식만으로도 상용네트워크에 접속하여 인터넷으로부터 다운로드 가능한 소프트웨어를 사용하는

1) 가상공간에서의 불법행위는 그 범죄현상을 어떻게 파악하느냐에 따라 범죄학계에서는 컴퓨터 범죄, 인터넷 범죄, 하이테크 범죄, 네트워크 범죄, 디지털 범죄 등 여러 가지 용어로 설명되고 있다.

2) 겉으로는 아무런 해를 끼치지 안을 것으로 보이지만, 실제로는 바이러스와 같은 위험인자를 내포하고 있는 프로그램으로 시스템 프로그램을 불법 수정하여 배포자가 원하는 기능을 수행할 수 있도록 되어 있다. 주로 이메일이나 인터넷을 통해 다운 받은 소프트웨어에서 발견된다.

등 다양한 전과(戰果)를 올렸다.

이와 같이 네트워크의 비약적인 발전은 범죄와 전쟁의 구별조차 애매하게 만들었다. 겨우 30명이라는 매우 적은 규모의 팀으로도 미국에 대한 전쟁도발을 가능하게 하였다. 이것이 이 연습으로부터 얻은 DOD의 교훈이다.

「Eligible Recever」와 같은 대규모의 사이버테러는 다행이 발생하고 있지 않지만, 위험의 분산과 시스템 전체의 안전성을 유지하기 위해서 네트워크를 형성하고 있으나, 네트워크에 대한 의존도가 높으면 높을수록 반대로 네트워크 그 자체가 전체사회에 대한 아킬레스건이 되어 간다고 하는 사실이다[4].

2.2. 부정 액세스에 의한 공격

전 세계는 2000년을 앞두고 초기의 컴퓨터가 메모리 절약차원에서 연도(年度)표기의 4행중 끝자리 2행을 가지고 처리하는 방식을 택하고 있어 2000년을 1900년으로 인식할 가능성이 있다고 판단하였다. 따라서 지구상의 모든 컴퓨터·네트워크가 연쇄적으로 오작동할 것이라는 우려가 제기되었을 뿐만 아니라, 핵미사일 및 원자력발전소도 제어불능이 될지도 모르기 때문에 미국정부 등은 세계의 모든 미국대사관에 물과 식량을 비축할 것을 명령할 정도였다.

그러나 이른바 「2000년(Y2K)문제」는 기우로 끝났다. 그 직후 1월부터 2월에 거쳐 일본의 과학기술청을 비롯한 11개의 정부기관의 홈페이지가 개찬(改竄)되었다. 경찰은 전자계산기손괴 등 업무방해죄(일본형법제234조의2)등의 용의로 수사를 개시하였다[5].

이 때 복수의 하드디스크에 남아있던 액세스기록을 해독한 결과 다음과 같은 사실이 판명되었다. 즉 확보한 메모리 영역(Buffer)에 대해서 허용량을 초과하는 대량의 데이터를 송출하거나, 프로그램을 폭주시켜 시스템을 다운시켰다는 것이다. 또한 버퍼를 초과한 데이터를 실행시키는 버퍼·오버프로우 공격(Buffer Overflow)[3]에 의하여 백도어[4]가 작성되어, 이것을 이용하여 앞에 지적한 정부부처 홈페이지의 개찬이 이루어졌다.

공격의 대부분은 공격당한 홈페이지에 남경대학살에 대한 비난 문구가 있었던 것으로 보아 중국의 소행으로 추측되었지만, 그 동기가 일본정부에 대해 비판적이라는 점에서 정치성·국제성의 색채를 띠고 있는 특징을 보였다. 다만, 이러한 공격은 정부부처의 홈페이지에 집중되었지만 그 침입의 수법은 비교적 단순한 방법이었다.

2.3. 부정 액세스와 바이러스의 경계

그러나 2월 7일부터 2주간에 미국에서 발생한 사이버공격은 매우 심각한 것이었다. YAHOO, Amazon 등 미국의 유명 웹사이트가 연속으로 서비스 방해공격(Denial of Service : Dos공격)을 받았다. 이 Dos공격은 타깃이 된 컴퓨터에 대량의 데이터 및 불량 패킷(packet)을 송신하여 당해 시스템을 다운시키거나 예외적으로 처리시키는 전형적인 사이버 공격의 하나이다. 특히 이 사건에서는 Dos공격 중에서도 분산형 Dos공격(Distributed Denial of Service)이라는 수법이 이용되었다. 이것은 부정 액세스에 의하여 복수의 제3자 컴퓨터(좀비PC)에 원격으로 조종이 가능한 공격프로그램(악성코드)을 미리 설치하여 이것이 설치된 다수의 좀비PC로부터 타깃이 된 컴퓨터에 대해 대량의 데이터를 동시에 송신하는 공격수법이다. 공격하는 좀비PC가 여러 대이기 때문에 타깃이 된 컴퓨터가 한 대인 경우, 그 표적이 된 컴퓨터에 걸리는 부하가 매우 클 수밖에 없었다. 현실적으로 보아 DDos공격[5]은 적어도 타깃이 되면 그것을 완전히 방어할 방법이 없어 인터넷의 근간 그 자체에 대한 위협이 된다. 더구나 Dos공격이나 DDos공격을 간단히 실행할 수 있는 방법이 인터넷에 떠돌고 있는 것도 문제를 심각성을 더하게 하고 있다.

DDos공격을 위한 좀비PC는 다음의 「LOVE 바이러스 사건」에서 사용된 수법에 의해서 만들어졌다.

---

3) 다양한 어플리케이션소프트에 공통한 대표적인 시큐리티 중의 하나로서 이것을 악용하여 원격지의 컴퓨터에 침입하는 것을 말한다.

4) 프로그래머들이 프로그램이나 시스템을 관리하기 위해 만들어 놓은 비밀통로

5) 사상 최대 규모의 사이버테러 사건으로 기록된 사이버 테러도 DDos공격에 의한 것으로, 전 세계 인테넷을 연결하는 기본서버(root server) 13대 중 9대가 다운되었다(2001.10). 특히 DDos공격의 문제점으로 지적되고 있는 것은 다수의 사이트를 대상으로 하고 있어 추적이 어렵고, 공격의 근원지인 악성코드 감영경로나 공격대상 목록 및 그 변환과정을 파악하기 쉽지 않다고 하는 점이다.

이에 의하여 바이러스와 부정 액세스의 경계가 애매하게 된 것도 현실이다.

2.4. 웜바이러스에 의한 네트워크의 파괴

초기의 컴퓨터 바이러스는 플로피디스크 및 문서파일 등에 기생하여 전염되는 타입이었지만, 1999년경부터 메일을 이용하여 확산되는 자기증식형 부정프로그램이 급증하였다. 이것은 네트워크로 연결된 컴퓨터 사이를 자기 스스로 복제되어 증식하는 악성프로그램이다. 이것을 웜(Worm)이라고 부르며 네트워크에 영향을 미치지 않는 바이러스와 달리 네트워크에 손상은 물론 대역폭을 잠식한다는 점에서 그것과 구별된다. 특히 단시간에 확산된 과부하에 의해서 시스템 전체가 다운되어 버리는 것이 특징이다[6].

2000년 5월에 세계로 확산된 「I LOVE YOU」라고 하는 타이틀을 가진 메일은 그 첨부된 파일을 더블 클릭하는 순간 하드디스크에 있던 「vbs」「jpg」「mp3」 등의 확장자를 가진 파일이 다른 코드를 가진 파일로 변환되며 파일명도 변경된다. 본래의 데이터는 완전히 파괴되며 더구나 사용자가 마이크소트프 아웃룩을 사용하고 있으면 그 주소록에 등록되어 있던 모든 사람에 대해서 자신이 받은 「I LOVE YOU」라는 똑같은 내용의 메일이 자동적으로 송신되었다. 또한 2003년 1월 25일에 우리나라에서 발생한 "인터넷 대란"도 미국과 호주 등에서 유입된 슬래머 웜 바이러스가 15분 만에 전세계적으로 대규모 트래픽을 발생시켜 국내 인터넷을 대부분 마비시키는 사회적 혼란을 몰고 왔다. 이외에도 국내·외의 사이버 범죄 현황을 보면 아래 <표 1>과 같다.

<표 1> 국외 사이버범죄 현황

연 도	내 용
1986	소련, 미국 미사일 방어체계 정보입수를 위해 관련 연구소 침입시도
1990	미국. 이라크로 수출하는 프린터 장치에 컴퓨터 바이러스 이식 이후 1991년 걸프전 당시 이라크 방공망 완전마비
2002.5	미 정보기관인 CIA 웹사이트가 해커의 공격을 받아 접속불능상태에 빠짐
2001	국내 전문신용카드정보처리업체의 시스템이 해킹당하여 47만명의 신용정보가 유출
2001	미국 정찰기와 중국 전투기가 충돌한 사건 이후 미·중의 해킹전을 시작으로 백악관 사이트가 일시 마비
2001.7	전세계 370,000 - 380,000여 대의 서버가 코드레드란 웜바이러스에 감염, 국내는 37,000여 대의 서버가 감염되어 피해액이 수십억 달러에 이름
2004	중국 해커들의 한국 국장연구소, 원자력연구소, 외교부, 주요언론사 웹사이트 집중공격
2005	일본 방위청, 경찰청 컴퓨터 해킹 흔적 발견
2007	러시아 해커들이 에스토니아정부, 언론, 방송, 은행 전산망 일제공격
2008	그루지야 러시아 해커들이 정부, 은행 DDoS 공격
2009	키르키스탄 러시아 해커 공격으로 정부 전산망 불통
2009	"7.7 DDoS대란" 한국 주요사이트 및 미국 사이트DDoS공격

(참고자료 : 사이버테러와 국가안보)

3. 부정 액세스법의 시행

3.1. 부정 액세스법의 제정 경위

앞에서 서술한 것처럼 특히 1990년대 후반부터 인터넷의 폭발적인 보급에 의하여 타인의 ID나 패스워드 등을 부정하게 사용하여 컴퓨터·네트워크를 권한 없이 침입하거나 권한을 초과한 부정 액세스가 증가하게 되어 경제협력개발기구(OECD)는 1986년에 각국에 이에 대한 범죄화 검토를 적극 권장하였다[8]. 이러한 배경에는 특정한 사용자에게 암호를 이용하여 외부로부터 격리된 컴퓨터 시스템을 이용하는 경우에는 그 인정시스템 자체가 법적인 보호의 대상이 될 수 있을 뿐만 아니라 이것은 네트워크의 안정성 및 신뢰성이라는 관점에서도 매우 필요성이 인정되었기 때문이다. 예를 들면 주거자의 의사에 반하여 타인이 지배하고 있는 물리적 영역을 침해하는 것이 현실사회에 있어서 주거침입죄라고 한다면, 가상의 세계에 있어서는 권한 없는 자가 전자적으로 부정한 액세스

(네트워크 범죄)에 의하여 통제된 시스템을 침해하는 행위가 바로 여기에 해당한다고 할 수 있다. 즉 현실사회에서 타당한 사회적 룰(규칙)은 기본적으로 네트워크상의 가상세계에 있어서도 타당하다는 점을 전제하고 있다고 할 수 있다[9].

이와 같은 관점에서 유럽과 미국 등에서는 1980년대부터 네트워크상의 범죄에 대하여 적극적으로 범죄화를 진행시켜 왔지만, 일본(1987년)과 우리나라(1995년)[6]에서는 형법의 일부개정으로 네트워크에 침입한 후, 파일의 개찬이나 제거 등을 행하는 크래킹(Cracking)은 전자기록부정작출죄(일본형법제161조의2/한국형법제227조의2와 제232조의2)나 전자계산기손괴 등 업무방해죄(형법제234조의2/ 314조2항) 등 컴퓨터 범죄규정이 도입되었다. 다만 단순히 네트워크에 침입만하는 해킹에 대해서는 부정 액세스가 이러한 행위의 예비적 수단에 불과하기 때문에 컴퓨터 무단사용이나 타인의 데이터를 단순히 훔쳐보는 것 그 자체로는 범죄가 성립되지 않는다고 하였다. 따라서 부정 액세스법은 이른바 해킹이라고 불리는 행위 가운데 i)네트워크나 시스템에 부정하게 침입(액세스)만 하는 행위와 ii)부정침입 후, 시스템을 변개하거나 데이터를 파괴하고, iii)데이터를 부정 입수하는 등의 행위(크레킹)와 구별하여 부정침입 그 자체를 처벌하려고 하는 것이다. 다시 말하면 기존의 형법상 컴퓨터범죄로서 처벌되는 ii)와 iii)의 행위에 의한 결과발생 이전의 행위, 즉 그 「수법」이 되는 부정 액세스 그 자체를 처벌대상으로 하고 있다[10].

또한 부정 액섹스 행위는 1990년대 후반부터 인터넷이 폭발적으로 보급되어 정보통신은 지금까지의 폐쇄된 네트워크로부터 일반사회에 개방되고 오픈된 글로벌 네트워크로 극적으로 변모하였다. 이것에 의하여 국경을 초월하여 발생하는 네트워크 범죄의 위험성이 높아져서, 중요한 데이터를 훔치거나, 중요한 컴퓨터에 허위의 데이터를 입력하여 오작동을 시키는 등의 범죄로부터 사이버테러의 발생까지도 우려되고 있는 것이 현실이다[11]. 그러나 외국으로부터 부정하게 국내 네트워크를 경유하여 외국에서 범죄를 범한 경우 국내에 처벌규정이 없으면, 국내 경찰은 해외로부터 수사협력요청에 응할 수 없다(쌍벌주의). 따라서 우리나라가 외국의 시스템에 침입거점이 될 수 있을 뿐 만 아니라, 외국의 표적이 될 우려도 있다. 이에 따라 1985년에 개최된 버밍햄서미트에서는 하이테크 범죄대책이 주요의제의 하나로서 채택되어 구체적인 행동계획의 책정과 실시가 과제가 되었다[12].

이와 같은 국제적인 움직임을 배경으로 일본은 1999년에 「부정 액세스 행위의 금지행위에 관한 법률」이 성립되어, 그 다음 해 2월부터 실시되었다.

이 법률은 네트워크범죄를 방지하고, 전기통신의 질서를 유지하여 고도의 정보통신사회에 있어서 건전한 발전에 기여할 것을 목적으로 하고(제1조), 전기통신회선에 접속하고, 또한 액세스 제어기능(ID나 패스워드 등에 의하여, 각 사용자에 대해서 미리 허가된 이외의 액세스를 금지하기 위한 기술적 조치)이 장착되어 있는 컴퓨터에 대한 침입행위를 부정 액세스로 정의하였다(제3조). 법정형은 1년 이하의 징역 또는 50만엔 이하의 벌금이며(제8조), 또한 타인의 식별부호를 제3자에게 제공하는 부정 액세스조장행위(ID나 패스워드 등)도 금지하고 있고, 이 위반행위에 대해서는 30만엔 이하의 벌금을 규정하고 있다(제9)[13].

3.2. 부정 액세스의 유형과 제재의 필요성

본 법률은 부정 액세스에 대해 2개의 유형을 규정하고 있다. 첫째, 타인의 식별부호를 이용하여 부정하게 네트워크에 액세스하는 「식별부호도용형」이고(제3조1항1호), 둘째, 씨큐리티의 약점을 뚫고 부정하게 액세스하는 「시큐리티·홀 공격형」이 그것이

6) 우리나라에서는 1995년 형법을 개정하여 사이버범죄에 자체에 대한 처벌규정으로 "공용서류등무효죄(제141조1항)""공전자기록위작·변작죄(제227조의2)","사전자기록위작·변작죄(제232조의2)", "컴퓨터 업무방해죄(제314조2항)", "기술적 수단에 의한 비밀침해죄(제316조2항)", "손괴죄(제366)"등을 규정하여 해킹이나 바이러스 유포를 통해 당해 기록의 효용을 해하거나 그 내용을 변경시키는 등 타인의 업무처리를 방해하는 행위를 처벌할 수 있게 되었다. 그러나 1995년은 인터넷 등 네트워크가 발전하기 전이어서 그후 인터넷환경의 비약적인 발전으로 사이버범죄의 종류가 다양해 졌을 뿐만 아니라, 그 발생건수도 매년 폭증하고 있다. 따라서 우리나라는 기본법인 형법의 개정을 통해서 대응하는 것이 아니라 정보통신망법(제71조, 제72조), 정보통신기반보호법(제8조1항) 그리고 통신비밀보호법 등을 통하여 대응하고 있다. 그러나 그 결과 다양한 법률에 사이버범죄의 대응에 관한 규정이 10여개 산재하게 되었다. 그 가장 큰 문제점으로 지적되고 있는 것은 다양한 법률에 그 처벌규정이 산재되어 있어 형사처벌에 관한 체계적 파악이 곤란할 뿐만 아니라, 구성요건적 행위에 따른 법정형의 균형이 이루어 지지 않은 부작용등이 지적되고 있다.

다.(제2호 및 3호)[14].

ID나 패스워드 등의 식별부호는, 네트워크 공간에서 액세스 권한이 있는 본인임을 식별·인증하는 가장 일반적인 수단이다. 따라서 해킹에 성공하면 이른바 타인의 지문을 남기며 당당하게 범죄를 할 수 있기 때문에 실제로는 해킹이 각종 범죄행위의 출발점이 될 우려가 있다. 이 식별부호도용형의 유형에서는 패스워드 등의 관리에 대해 이른바 인간의 심리적인 약점을 이용하여 행해진다. 이러한 의미에서 이 침입유형은 기술적인 시큐리티만으로 대항할 수 있는 것은 아니고 규범적인 규제가 필요하다. 이것에 대해서 시큐리티·홀 공격형은 프로그램버그(Bug) 등의 시큐리티상 논리적 취약성이 부정 액세스의 수단으로 이용된다는 점에서 식별부호도용형과 구별된다. 따라서 이 유형에서는 형법적 예방보다도 기술적인 시큐리티를 강화하는 것이야 말로 유효한 대책이 된다.

3.3. 부정 액세스법의 형사법적 규제

부정 액세스에 대한 형사법적 규제는 가장 기본적이고 매우 유용한 대응방법이다. 이것은 형사법적 규제가 일반범죄에 대한 국가의 대응체계로서 장기간 걸쳐 발달해 온 규제방식으로서 다른 법률에 비하여 정비가 잘되어 있기 때문이다. 다만, 부정 액세스에 대한 형사법적 규제를 고려할 때, 그 당벌성과 처벌근거에 관해 기본적으로 두 가지 관점에서 생각하지 않으면 안 된다. i)해킹의 미수죄 또는 예비죄적 행위로서 고려하든지, ii)네트워크에 있어서 사회적·경제적 안정성이나 신뢰성을 침해한다고 하는 독자의 당벌성(當罰性)을 가진 행위로 고려하든지 하는 것이다. 크래킹은 해킹의 발전단계이기 때문에 해킹의 단계까지 처벌시기를 앞당기는 것에 대해서는 일정한 부분에서 합리성이 인정될 수 있을 것이다. 그러나 모든 해킹이 크래킹을 의도하고 그것에 연동되는 것이 아니며 또한 일본에서는 서비스나 정보의 부정입수 일반이 범죄로 되어 있지 않는 이상, 해킹을 미수죄 내지는 그 예비죄적인 성격을 가진 것으로서 구성하는 것에 대해서는 무리가 있다[15]. 여기서 해킹 자체에 당벌성이 인정되는지 문제가 된다. 컴퓨터 네트워크의 사회적·경제적인 중요성이 점점 증대하는 이상, 폐쇄적인 시스템 자체에 법적보호를 하는 것이 필요하고, 부정 액세스를 이른바 전자적 불법침입죄로서 구성하는 것은 가능할 것이다. 앞에서 지적하였지만, 주거침입죄에서는 물리적인 침해가 그 요건으로 되어 있지만, 가상세계에서는 일정의 액세스 제어 시스템을 침해하는 것이 이것에 해당한다고 할 수 있다. 법률도 이와 같은 취지로 보호의 대상을 액세스 제어가 실시된 네트워크·시스템에 한정하고, 이 액세스 제어의 부정한 해제를 그 요건으로 하고 있다.

3.4. 주요국가의 형사법적 규제와 그 한계

미국은 1984년 컴퓨터사기 및 오용방지법을 제정한 후, 1996년 이를 대폭 수정하여 컴퓨터 사기 및 오용 방지법을 「국가정보기반구조보호법(National Information Infrastructure Protection Act)」으로 개정하였다.

이 법이 처벌대상으로 하고 있는 행위는 i)권한 없이 또는 권한을 초과하여 고의적으로 컴퓨터에 접속하는 행위를 하거나, 권한을 초과한 접속으로 법령상 공개가 제한되어 있는 자료를 획득하는 행위 등, ii)권한 없이 또는 권한을 초과하여 고의적으로 컴퓨터에 접속하여 금융기록이 포함된 정보 또는 소비자 보호기관의 소비자 관련 파일이 포함된 정보 등을 획득하는 행위, iii)권한 없이 고의적으로 국가기관의 업무용 컴퓨터에 접속하는 행위 등, iv)고의적으로 그리고 사기를 행할 목적으로 권한 없이 또는 권한을 초과하여 보호가 필요한 컴퓨터에 접속하는 행위, v)고의적으로 프로그램, 정보, 부호 또는 명령을 전송하여 의도적으로 보호가 필요한 컴퓨터를 권한 없이 손상시키는 행위, vi)고의적으로 그리고 사기를 행할 목적으로 컴퓨터에 권한 없는 접속을 가능하게 하는 패스워드 또는 이와 유사한 정보를 거래하여 주(州)간 통상 또는 국제통상에 영향을 주는 행위, vii)개인, 기업, 단체, 각종 기관으로부터 재화나 정보 등을 강탈할 목적으로 보호가 필요한 컴퓨터를 손상시킬 것이라고 위협하는 등이다. 이처럼 미국은 대부분의 주에 있어서 부정 액세스를 처벌하고 있다.

특히 미국은 9·11 테러 이후 사이버테러에 대응하여 여러 법안을 통과시켰는데 그 중 대표적인 법이 2002년 국토보안법의 수정법안으로 통과된 사이버보

안증진법(Cyber Security Enhancement Act)이다[16].

영국은 1990년에 컴퓨터오용금지법(Computer Misuse ACT)을 제정하여 사이버범죄를 본격적으로 규제하기 시작하였다. 이 법에 따르면 컴퓨터처리기록에 권한 없이 다음과 같이 액세스한 행위를 한 때에는 처벌하였다. 즉 컴퓨터를 작동시킬 시점에서 액세스 권한이 없다는 것을 알면서 타인의 컴퓨터에 축적된 프로그램 또는 데이터에 액세스할 의도를 가지고 컴퓨터를 작동시키는 행위에 대하여는 약식기소에 의하여 6개월이하의 징역형 또는 표준수준의 5이하의 벌금형 또는 이 형벌들을 병과할 수 있도록 하였다.

그 후 2006년에 경찰 및 사법절차에 관한 법률과 2008년에 컴퓨터오용금지법 자체를 개정하여 처벌규정을 강화하였다. 이 법의 특징은 바이러스 유포행위와 관련하여 피해자의 실질적 손해와 그에 대한 가해자의 고의를 요구하지 않고 바이러스 유포 및 제조자체를 처벌하고 있다는 점이다. 컴퓨터오용금지법은 ⅰ)컴퓨터자료에 대한 모든 접근, ⅱ)위법행위를 조장하거나 범죄를 목적으로 하는 무단 접근, ⅲ)컴퓨터자료에 대한 무단 수정 등을 사이버범죄로 규정하고 있다[17].

독일은 정보통신기술의 남용행위에 대한 범죄화 및 유럽의회의 사이버방지조약을 국내법으로 전환하기 위하여 2007년 8월에 발효되었던 제41차 형법개정법 중 컴퓨터범죄관련 형법을 제·개정하였다. 즉 컴퓨터범죄 방지를 위한 형법 개정법은 컴퓨터 범죄의 핵심에 해당하는 형법구성요건을 개정하거나 새롭게 입법하였다. 즉 개정한 것으로는 데이터 불법탐지죄(제202조a), 데이터불법취득죄(제202조b), 데이터 변경죄(제303조a), 컴퓨터사보타지죄(제303조b) 등이 있고 새로 규정한 것으로는 컴퓨터범죄의 예비죄(제202조c)가 있다.

다만, 독일은 ⅰ)형법제202조a에 규정된 데이터 불법탐지죄에 있어서 기존에 논란이 되었던 단순해킹의 가벌성 문제를 입법으로 해결하였으며, ⅱ)제202조b는 특별히 보안이 되어 있지 않은 데이터를 전송 중에 취득하는 행위를 처벌할 뿐만 아니라, 종래 처벌되지 않던 데이터 처리장치에서 방출되는 전자파로부터 데이터를 취득하는 행위도 처벌함으로써 구성요건을 확대하였다. ⅲ)특히 제202조c는 컴퓨터 형법의 영역에서 위험성이 큰 특정한 예비행위를 처벌하기 위한 조항이다. 이를 통하여 데이터에의 접근, 비밀번호의 유포, 해커의 툴 제작과 같은 행위가 위 규정을 통하여 처벌이 가능해 졌다.

위에서 고찰한 것처럼 부정 액세스에 대한 각국의 규정들은 단순히 부정하게 네트워크에 침입하는 것으로부터 침입 후, 데이터의 부정입수 및 변개와 파괴에 이르기까지 다양한 형태가 규정되어 있고, 대부분 형사법적 대응을 하고 있다. 그러나 부정 액세스 는 이러한 형사법적 대응에도 불구하고 그 성격상 일정한 한계를 초래하여 국제협력에 의존하지 않을 수 없다는 문제점이 제기되었다[18]. 그것은 첫째, 형사법적 대응은 본질적으로 사후적 조치이고, 그 대응속도 또한 매우 느리기 때문에 사이버범죄에 대한 효과를 발휘하는데 근본적인 한계가 있다. 둘째, 많은 국가들이 자국에 있는 사이버공격자를 타국에 인도하거나 타국을 위해 기소하는 것을 기피하고 있다는 점이다. 특히 당해 국가가 사이버범죄를 형사법적으로 제도화하고 있지 않거나, 공격대상 국가가 여러 가지 사정으로 이를 묵인하는 경우에도 한계가 있을 수밖에 없다는 점이다. 즉 이러한 경우 외교적 역량과 노력에 따라 사이버범죄자의 처벌이 결정되거나, 해당국가간 관련협약이 이루어져 있지 않은 경우 처벌이 불가능하다. 또한 범죄인인도조약이 체결되어 있다고 하더라도 국제형사사법공조법에 의한 공조절차는 너무 복잡하여 신속한 처리가 요구되는 사이버범죄의 해결에 지장을 초래할 가능성이 매우 높다.

4. 국제협력의 동향

이러한 문제점과 더불어 1990년대 중반부터 세계적으로 네트워크가 구축되면서 부정 액세스 위반행위의 이외에도 각종의 사이버범죄가 국내외를 불문하고 급증하고 있다. 국내의 사이버테러의 발생 및 검거건수를 살펴보면 다음<표 2>와 같다.

다만 이러한 사이버 상에서 행해지는 범죄는 한 국가의 노력에 의해서 해결될 수 없는 문제임에도 불구하고 관할권이나 국제법상 원칙 등 아직도 명확하지 않은 부분이 많다. 따라서 종래에는 사이버범죄의 특성상 국제조약의 체결에 의한 해결이 현실적으로 어렵다고 생각하는 견해가 지배적이었다.

<표 2> 유형별 사이버 범죄발생· 검거현황

(단위 : 건수)

		사이버테러형범죄		
		소계	해킹	바이러스
발생	'09년도	16,601	16,558	43
	'08년도	20,077	19,950	127
	'07년도	17,671	17,593	78
	'06년도	20,186	20,119	67
	'05년도	21,389	21,336	53
검거	'09년도	13,151	13,124	28
	'08년도	16,953	16,854	99
	'07년도	14,037	13,988	49
	'06년도	15,979	15,934	45
	'05년도	15,874	15,831	43

(참고자료 : 경찰백서2010)

유럽의회는(Council of Europe)는 사이버범죄의 컴퓨터시스템에 대한 남용을 억제하고자 1996년 11월 컴퓨터전문가위원회(Committee of Experts on Crime in Cyberspace)를 창설하여 사이버 범죄에 대한 형사법적 문제점을 가능한 한 해소할 것을 검토하여 왔다. 이 조약의 제정목적은 ⅰ)사이버범죄의 유형화, ⅱ)정보기술에 대한 법적보호, ⅲ)사이버범죄에 대한 국제공조와 효과적인 대응책 마련, ⅳ)형사공조조약의 보완 및 전자증거수집 지원 등이며 미국, 일본 등 총 29개국이 서명하였으며, 2004년 7월 1일 발효되었다. 특히 이 조약은 사이버범죄에 관한 최초의 국제조약으로 사이버범죄방지를 위한 국제협력 및 조약체결의 가능성을 보여주었다는 점에서 그 의의가 있다.

1997년 1월 리용그룹 전체회의에서는 사이버공간에서 발생하는 범죄에 대한 대응은 한 국가만으로 한계가 있으며 각국의 상호연대가 필요하다는 인식 하에 국제하이테크범죄대책을 검토하는 하위그룹이 설치되었다. 또한 G8 법무·내무장관회의에서는 리용그룹의 검토결과를 토대로 각국은 컴퓨터 등 하이테크 범죄에 대한 국제사법공조체제의 강화를 목표로 국제협력 관계의 기본원칙과 이를 이행하기 위한 실천방안을 결의하였다[19].

5. 결 론

인터넷 및 컴퓨터 시스템의 급속한 확대로 인하여 고도의 정보화 사회로 들어섰다. 정보화 사회는 역사적으로 말하면 농업혁명, 산업혁명에 이은 제3의 혁명인 정보혁명에 의해서 초래된 사회이다. 이러한 혁명이 사회경제적으로 커다란 변화를 가져온 것도 사실이며, 이것은 기존의 법질서에 대한 새로운 변화를 촉구하고 있다고 할 수 있다.

네트워크상의 범죄는 초기의 컴퓨터 남용과 오용의 문제와는 달리 정보기술의 발달과 그 범죄가 가진 특성[20]인 ⅰ)익명성, ⅱ)불특정 다수성, ⅲ)시간적·지리적 무한정성, ⅳ)무흔적성에 의하여 단순히 네트워크에 침입하는 해킹을 비롯하여 국가의 기반시설을 오작동하게하거나 파괴시켜 사회혼란을 초래한 것은 물론 국가의 안보까지 위협하는 행위로까지 발전하여 현대사회에 새로운 형사규제의 대상으로 된지 오래되었다. 다만 사이버상의 범죄는 앞에서 지적한 것처럼 「규범으로서 규제해야 할 문제」와 「기술로서 규제해야 할 문제」에 대한 구별의 전제하에 규범으로서 규제해야 할 문제라고 생각한다면, 이것은 가상세계의 행위라 할지라도 현실사회의 구성요소로서 (전자적)실재성을 가진 행위로써 기본적으로는 현실사회의 법적규제에 따라야 한다. 즉 현실사회에서 위법이라면 원칙적으로 가상세계에 있어서도 위법한 행위가 되어야 한다. 이것은 인간이 정보화혁명을 추진하고 그 혁명에 의하여 실현된 (가상)사회도 인간사회의 일부이기 때문이다. 다만 네트워크공간의 특수성으로 인하여 기존의 법적규제에 수정을 가하게 될 수는 있을 것이다. 이 문제에 관해서는 별도로 논할 필요가 있을 것이다.

참 고 문 헌

[1] 島崎俊隆(1998), ハイテク犯罪の現狀と今後の對應, 信學技報, 8면.
[2] 園田壽(2011), 情報社會と刑法, 成文堂, 16면.
[3] 문종식·이임영(2010), 사이버테러 동향과 대응방안, 정보보안학회지제20권4호, 24면.
[4] 園田壽(2011), 전게서, 17-18면.
[5] 後藤啓二(2000), ハイテク犯罪の現狀と對策,

53卷8号, 1면.
[6] 宮協磊介(2000), サイバーセキュリティについて, 法律のひろば53卷6号, 36면.
[7] 문종식・이임영(2010), 전게논문, 24면.
[8] 石井壯治(2001), 不正アクセス行爲の禁止等に關する法律違反事件の搜査處理について, 搜査研究595号, 17면.
[9] 石井孝(2000), ハイテク犯罪に對する國際的取り組み, 警察時報55卷8号, 21면
[10]加藤敏幸(2001), 不正アクセスに, 刑法雜誌41卷1号, 79면,
[11] 金澤正和(2000), 不正アクセス行爲等の取り締り狀況及び今後の課題, 警察學論集53卷8号, 22면.
[12] 園田壽 외(2000), ハッカ vs. 不正アクセス禁止法, 日本評論社, 162면.
[13] 園田壽 외(2000), 전게서, 183면 이하, 葛原宏高(2000), 不正アクセスに關する制度の現狀と課題, 新聞經營152号, 80면.
[14] 園田壽(2011), 전게서, 22면, 中田光一(2002), サイバーテロ對策の現狀と取組み法律のひろば55卷3号, 21면, 檜恒重臣(2001), ネットワクを利用ハイテク犯罪對策について, 警察時報53卷6号, 67면, 關聰司(2000), ハイテク犯罪の現狀と對策, 法律のひろば53卷6号, 4면, 渡邊國佳(2001), ハイテク犯罪の檢擧狀況について, 警察時報56卷6号, 11면, 後藤啓二(2000), ハイテク犯罪の現狀と對策, 53卷8号, 1면.
[15] 이정훈(2005), Cyber범죄조약에 대한 실체법적 대응모색 -최근 일본의 하이테크범죄에 대한 입법동향을 검토하며-, 중앙법학제7집1호, 227면.
[16] 김흥석(2010), 사이버테러와 국가안보, 제7회 법률가대회발표논문, 18면이하.
[17] 宗像明(2001), 日本におけるサイバーテロ對策の存り方を考える, 警察學論集54卷5号, 98면,
[18] 정완(2007), 사이버범죄의 방지를 위한 국제협력방안, 형사정책연구 제18권2호, 117면이하, 檜恒重臣(2001), 이창수(2009), 초국가적 사이버범죄에 대한 국제공조 활성화 방안과 그 선결과제, 형사법의 신동향제21호, 104면.
[19] 정완(2007), 전게논문, 122면.
[20] 박윤해(2006), 컴퓨터범죄에 관한 연구, 법학논총제16집, 251면.

김 형 만

1986 숭실대학교 법학과 (법학사)
1988 일본명치(明治)대학원 법학과(법학석사)
1995 일본 명치대학원 법학과 (법학 박사)
1996.9~2008.2 대불대학교 경찰행정학과 부교수
2008.3~현재 광주대학교 경찰법행정학부 부교수
관심분야: 사실인정, 오판, 피해자소송참여
E-Mail: hmkim57@gwangju.ac