

신기술해설

컴퓨터범죄와 보안문제

정진섭[†]

❖ 목 차 ❖

- 1. “빼꾸기기의 알”
- 2. 해커란 무엇인가?

- 3. 국내에서 벌어진 해킹 사례
- 4. 마무리

1. “빼꾸기기의 알” - 소설같은 실제사건

금년초 미국 법무부의 컴퓨터통신 보안실에 방문해서 그들의 보안대책 현황을 견학한 적이 있다. 그곳에서 책임자들과 대화를 하다가 재미있는 컴퓨터범죄 이야기를 들었다.

바로 1988년 독일 하노버에 사는 해커 5명이 저지른 “빼꾸기의 알(The Cuckoo's Egg)”이라는 사건이다. 사건 내용은 독일의 대학생들이 브레멘 대학교의 인터넷 계정을 이용하여 미국의 어느 방위산업체 전산망에 침투한 다음 군사비밀에 해당하는 각종정보를 입수하여 소련 KGB에 넘겨주고 그 대가로 코카인등 마약을 받아왔다는 것이다. 1년반 이상 은밀하게 진행되던 이 해킹범행은 침투당한 방위산업체에 근무하는 클리프 스톨(Cliff Stoll)이라는 한 천문학자의 집요한 추적으로 적발되고 말았다. 필자는 컴퓨터보안 내지 유닉스 전문가가 아니라서 추적 경위를 정확히 이해하지는 못하고 있지만, 스톨이 쓴 책자에 소개된 추적내용을 간단히 소개하면 다음

과 같다.

천문학자인 스톨은 자신이 근무하는 연구소에서 사용한 컴퓨터의 사용요금을 계산하는 과정에서 각 사용자의 이용시간을 합산한 금액이 컴퓨터가 계산한 금액과 75센트 차이가 나는 원인을 찾다가 영국으로 이민간 사람의 인터넷 계정이 사용된 사실을 발견했다. 그는 자신의 연구소에서 LAN이나 다이얼 업으로 연결된 일반 ID이라면 “tly”로 시작하여야 하는데, 외부 컴퓨터에서 접속해오는 경우에는 “nl”로 시작되는 점에 착안하여, 외부에서 접속해오는 인터넷 계정을 사용하는 내용은 모두 자기의 단말기와 프린터에 출력되도록 소스코드를 고쳐 놓고 기다렸다.

얼마후 스톨은 누군가가 연구소의 컴퓨터에서 정상작동되는 시스템에 침입하여 해킹을 하기 위한 프로그램인 “빼꾸기기의 알(The Cuckoo's Egg)”을 일반 사용자들이 아무나 사용할 수 있는 디렉토리에 숨어 놓은 사실을 확인하였다. 해커들은 유닉스 시스템을 이용해서 인공위성을 타고 미국내 방위산업체 컴퓨터에 침입하여 주요 군사시설의 IP 주소를 알아낸 다음, 트로이 목마를 각 컴퓨터마다 숨어놓

† 정 회 원: 대검찰청 전산관리담당원(부장검사)

고 군사정보를 빼내어 갔던 것이다. 전화회사의 추적결과, 결국 해커들은 9,000km 이상 떨어진 독일 하노버에서 AT&T 전화선으로 인공위성 또는 해저 광케이블에 연결된 통신회선을 통하여 2년간 가까이 이러한 스파이 행위를 계속해 온 사실이 적발되었다.

소설보다 더 흥미진진한 스파이 첩보전을 방불케 한 이 사건은 미국 전역을 강타하였고, 무명의 천문 학자에 불과하던 스톨은 순식간에 미국의 영웅으로 부각되었다. 한편, 이 사건으로 미국 군사정보망의 주축을 이루고 있는 ARPANET, MILNET과 그에 연결된 수많은 단말기의 보안체계에 엄청난 구멍이 뚫려 있다는 사실이 적나라하게 노출되었다.

지금 우리 지구촌에는 전세계를 연결하는 인터넷 통신망이 하루가 다르게 확산됨에 따라 “빠꾸기 알” 사건과 유사한 사건이 얼마든지 재발할 수 있는 상황이다. 이러한 우려는 점점 높아지고 있으며, 컴퓨터 보안에 관한 관심과 기술투자도 그에 비례해서 점차 늘어가고 있다.

2. 해커란 무엇인가? - 그 양면성과 폐해

“해커(hacker)”라는 말은 컴퓨터 분야에서 그 평가가 극단적으로 엇갈리는 용어라고 하겠다. 일부에서는 컴퓨터에 관한 한 고도의 전문지식을 갖추었다는 점에서 “영웅”으로 대접하는 반면에, 일부에서는 해커를 현대문명을 파괴하는 “지능범인”의 일종으로 취급하기도 한다. 이런 극단적인 평가는 모두 일면의 타당성을 갖고 있다. 예컨대, 세계적인 컴퓨터왕 빌 게이츠, 워즈니악 등이 모두 젊은 시절 컴퓨터 해커로 명성을 떨친 사람이었다. 이처럼 밝은 면이 있는 반면에, 위의 “빠꾸기 알” 사건에서도 보듯이 악질 해커들의 무분별한 통신망 침해나 이를 이용한 사기행각 등이 날로 심각해 지고 있기 때문이다.

이런 해커 문제가 더욱 심각해 진 것은 1980년대 이후 컴퓨터 네트워크가 발전해 온 것과 궤를 같이 한다. 인터넷의 확산에 따라 전세계의 공공기관 통신망에 침입하여 정보를 손괴, 변경하는 네트워크 접속 해킹행위는 질적, 양적으로 날로 심각해 지고 있다. 컴퓨터 바이러스를 만들어 유포하는 해커도 통

신망의 발전에 따라 더욱 위력을 발휘하게 되었다.

그런데, 컴퓨터 해커의 정확한 의미나 개념은 정립하기가 쉽지 않다. 일반적으로 다른 사람의 컴퓨터에 무단 접근하여 그 컴퓨터에 축적된 자료나 프로그램을 훔쳐내거나 고치는 사람을 의미한다. 그러나, 오늘날 해킹 기법은 하도 다양하고, 발전속도가 너무나 빠르기 때문에 그 종류나 유형을 일률적으로 말하기 어렵다.

따라서, 해커의 유형을 몇가지 분류해 보면 첫째, 시스템 해킹이 있다. 이것은 주로 통신망 회선을 이용해서 이루어 지며, 다른 사람의 시스템을 몰래 쓰거나 그 정보, 자료를 제멋대로 손괴하는 것으로서, 해킹의 가장 대표적 유형으로 간주된다. 둘째, 프로그램 무단 개작(改作)이 있다.

원제작자의 허락없이 자신의 목적대로 프로그램을 고치는 것으로서, 세어웨어 프로그램을 제마음대로 수정을 가해서 상업용 비전으로 판매하거나, 타인의 상업용 프로그램의 암호를 풀어내는 행위, 불법복제 방지를 위한 락을 풀어내는 등이 바로 그것이다. 셋째, 바이러스 제작유포 행위이다. 바이러스 프로그램이 무분별하게 유통되면 컴퓨터지식이 부족한 일반 사용자들이 본의 아니게 시스템 다운되거나, 소중한 자료들을 일시에 날려버리는 경우가 허다하다는 점에서 매우 부도덕한 행위라고 하겠다.

사회에서 실제 벌어지는 해킹수법은 이외에도 여러가지가 있겠으나 이를 유형화해서 일일이 열거하는 것은 결코 쉬운 일이 아니다. 따라서, “해킹은 범법인가?”하는 질문은 꼭 필요한 질문이면서도, 실제 답변하기는 대단히 어려운 우둔(愚問)이기도 하다. 이를 요약해서 말한다면, 해커라는 용어는 법률적 개념이 아니고 컴퓨터 분야에서 통용되는 사실적 개념에 불과하므로, 법률상 “해커” 자체를 처벌하는 규정은 존재하지 않는다. 다만, 해킹 행위라고 분류되는 여러가지 행위 중에서 법률상 “범죄”라고 평가되는 행위 단을 선별적으로 처벌할 수 있을 뿐이다. 법률적으로 어떤 행위를 형사처벌하려면 이른바 “범죄 구성요건”을 충족시켜야 한다. 해킹 행위 중에는 도덕적으로 별 문제가 되지 않는 경우도 적지 않지만, 경우에 따라서는 부도덕하거나, 또는 불법적인

경우가 많으므로 그러한 불법적 행위에 대해서 형사 처벌이 가해지는 것이라는 의미이다.

3. 국내에서 벌어진 해킹 사례 - 어떻게 처벌되나?

얼마전 국내 신문지상에 크게 보도되었던 청와대 방자 컴퓨터통신 사기사건을 예로 들어보자. 당시 범인은 자신의 미국 유학자금을 마련하기 위하여 국내 천리안 통신망을 이용하여 금융기관의 휴면계좌를 자기 구좌로 모으려는 사기행각을 시도하다가 검찰의 추적에 의해 검거되었다. 이 범인은 "TRY AND ERROR"라는 원시적인 해킹수법으로 청와대, 국세심판소 등 공공기관의 천리안 ID와 비밀번호를 알아낸 다음, 여러 금융기관을 상대로 청와대 정권인수팀 명의로 휴면계좌에 관한 자료제출을 요구하던 도중에 적발된 것이다. 이 범인에게 적용된 죄명은 "사기미수"이다. 해킹행위 자체가 형사처벌의 대상이 되었다기 보다, 그 해킹 수법이 "남을 속여서 재산상 이익을 취득하려는 행위"에 해당되기 때문에 형사처벌을 받았던 것이다.

또, 얼마전 사회적으로 엄청난 관심을 끌었던 한글2.5 암호해독 프로그램 공개사건의 경우는 컴퓨터 프로그램보호법상의 저작권 침해여부가 문제되었던 사건이다. 현행 컴퓨터프로그램보호법은 프로그램 원저작자의 허락없이 "공표, 복제, 개작, 번역, 배포 또는 발행"하는 경우 저작권 침해로 간주 처벌하도록 하고 있다. 문제된 한글2.5 암호해독 사건의 경우 원프로그램을 수정했는지 여부를 확인하지 못해서 무단개작에 해당여부가 불분명하지만, 만일 한글 프로그램의 일부에 수정을 가한 사항이 있다면, 컴퓨터프로그램보호법상의 "개작", "공표"에 의한 저작권침해가 성립된다고 해석된다. 다만, 저작권 침해의 경우, 이른바 친고죄(親告罪)에 해당되므로 피해자인 한글과 컴퓨터사에서 고소를 하여야만 형사처벌이 될 수 있는데, 어떤 일인지 한컴사에서는 고소권을 쉽게 포기하고 말았다.

바이러스 제작행위도 그 행위를 곧바로 처벌할 수 없기는 마찬가지이다. 바이러스 프로그램의 제작행

위 자체가 형사처벌되는 것이 아니라, 그 행위로 인해서 타인의 시스템을 손괴하거나 업무수행을 방해했을 때 비로소 형사처벌이 된다고 해석할 수 있다. 지난해 과학기술처에서 컴퓨터프로그램보호법 개정작업을 진행하면서 컴퓨터바이러스 제작유통 행위를 직접 형사처벌하는 규정을 두려는 움직임이 있기는 하였으나, 형사처벌을 위한 "구성요건"의 특징이 곤란하다는 등의 이유로 입법이 보류된 바 있다.

이처럼 컴퓨터 해킹수법을 이용해서 물건을 훔친다면 절도죄로, 공금횡령을 한다면 횡령죄로, 남의 업무를 방해한다면 업무방해죄로, 저작권을 침해한다면 저작권법 또는 컴퓨터프로그램보호법위반으로 각각 처벌되는 것이다. 또, 컴퓨터의 발전에 따라 새로이 형사처벌할 필요성은 높지만 이런 현행법으로 처벌하기 곤란한 유형의 행위에 대해서는 형법개정 등의 방법으로 새로운 처벌규정을 마련중에 있다. 예컨대, 컴퓨터 파일을 일반 문서와 동일하게 인정하여 그 위조, 변조행위를 처벌하기 위한 "전자적기록 위·변조죄"나, "컴퓨터를 이용한 배임, 재물손괴" 등 재산범죄 규정을 신설하는 내용 등이 포함된 형법개정안이 현재 국회에 상정 중에 있다.

이상 설명한와 같이, 해커 또는 해킹행위 자체는 법률적 개념이 아닌 관재로 이를 직접적으로 형사처벌하는 규정은 존재하지 않지만, 그렇다고 해서 자신의 뛰어난 컴퓨터지식을 악용해서 불법적인 행위를 하는 악한 "해커"들을 방치해 두는 것은 전혀 아니다. 지적하고 싶은 점은, 사회에 해독을 끼치는 악한은 결국 처벌되게 마련이라는 것이다.

4. 마무리 - 정의의 해커를 기다린다.

오늘날 날로 심각해져 가는 컴퓨터 해킹범죄를 확실하게 색출 진압하려면 클리프 스톨과 같이 높은 윤리의식과 탁월한 컴퓨터 지식을 겸비한 엘리트 인물이 절실히 요구된다. 그러나, 안타깝게도 지금 우리나라에는 해커의 동기나 사회적 과장을 생각치 않고 컴퓨터 지식만 높이 평가해서 영웅시하는 분위기가 혹시 있지 않은가 생각하게 된다. 특히 희귀한 해킹사건이 발생하면 대다수 언론이 들뜬 분위기에서

선정적 보드를 거듭함으로써 다수인의 “공익”이 무시되는 장면이 간혹 벌어지고 있다. 이런 분위기로 인하여 우리나라에서는 맵스컴 지향적 또는 악의적인 저질 해커들은 수없이 명멸하고 있으면서도, 막상 진정한 사명감을 가진 “좋은 해커”는 나타나지 않고 있는 게 아닌가 하는 적정도 든다.

필자는 지난 2월 한달동안 미국 대법원, 검찰청, FBI 등 공공기관의 컴퓨터시스템과 정보통신망을 시찰할 기회를 가졌었는데, 컴퓨터 선진국인 미국도 역시 해커문제로 골치를 썩고 있기는 마찬가지였다. 그런데 인상적인 것은 미국 법무부 전산보안팀 내에 엄청난 컴퓨터 실력자가 근무하면서 못된 해커들 추적하고 있다는 점이었다. 머리가 덩수룩하고 조용하게 생긴 그는 “해커잡는 해커”로서, 일종의 “반-해커” 아니면, “정의의 해커”라고 말할 수 있겠다. 이처럼 해커의 칼날을 바로 양날이다. 다수의 공익을 생각하는 “정의의 해커”가 더욱 많이 탄생하기를 진심으로 기대한다.



정진섭

- 경희대학교 법과대학 및 동대학원 졸업(법학박사)
- 학위논문: 국제지적소유권제도의 현황 및 발전방향 연구
- 제21회 사법시험 합격 및 사법연수원 제11기 수료
- 프랑스 국립사법관학교(ENM) 국제부 수료

- 연세대학교 특허법무대학원 고위자 과정 제1기 수료
- 서울지검 남부지청, 청주지검 영동지청, 법무부 검찰제4과, 검찰제2과, 서울지검 검사, 부산지검 검사, 영월지청장, 대검검찰연구원
- 특허청 특허심판제도 연구위원회 위원, 특허청 영업비밀 입법추진위원회 위원, 법무부 형법개정특별심의회위원회 전문위원, 서울시 소청심사위원회 위원 등 역임
- 한국 지적소유권학회 이사, 한국 국제법학회 평의원
- 저서: 국제지적재산권법 (1995. 육법사), 주권식 형법총론 (1990.탁영사)
- 주요논문: 지적소유권관련 대외통상협상현황, 지적소유권 보호를 위한 형사정책, 지적재산권 산업재산권 용어에 대한 이견, 사적 이용을 위한 복제의 허용한계, 저작물 제호의 법적 보호, 프랑스의 특허제도, 형사사건으로 본 저작권침해사례, 전자문서 출현과 EDI의 법적문제등 다수

1996년 국제 컨퍼런스

한국정보처리학회에서는 우리나라 정보산업 발전과 국제 경쟁력 강화에 필수불가결한 “21세기 정보기술”에 관한 국제 컨퍼런스를 다음과 같이 개최합니다.

- 디 옴 -

1. 주 제 : 기업의 경쟁력 향상과 21세기 정보기술
Industrial Survival Strategy for next Generation S/W Technology
2. 일 시 : 1996. 6. 12~13(2일간)
3. 장 소 : 롯데호텔(잠실)
4. 내 용 : - Next Generation Software
- Internet을 활용한 Business Opportunity
- Object Oriented Technology
- Data Warehousing