새로운 해킹기법과 관련된 형법적용의 흠결과 해결방안

최 호 진*

국문요약

해킹범죄는 최첨단 정보통신기술을 이용해 사회 중추신경인 정보통신망을 안정적인 운영을 방해·파괴하고, 해킹으로 획득한 정보를 불법적 용도로 사용함에 따라 사회안전에 중대한 위협이 되는 대표적인 범죄유형이다. 하지만 해킹기법이 IT 기술의 발전과 궤를 같이 하여 끊임없이 새로운 공격기법이 등장함에도 불구하고 해킹과 관련된 형사법적 대응은 지나치게 단순하여 형사법적 한계를 가진다. 이에 본 논문에서는 해킹과 관련된 현행법규를 분석·적용한 후 형사법적 한계와 흠결을 지적하여 그 해결방안을 도출하고자 한다.

먼저 해킹과 관련된 유형을 정보통신망의 보호조치와 관련하여 형법의 비밀침해죄, 정보통신망법, 전자기록손괴죄의 성립여부, 단순해킹과 관련되어 정보통신망법의 해석을 통한 적용가능성을 논의하였다. 해킹관련법규의 정당한 접근권한의 여부, 권한을 초과한 경우, 보호조치를 침해한 후 침입하는 경우와 보호조치를 침해하지 않고 우회적으로 침입하는 경우로 나누어 각 법규정의 해석과 적용을 해보았다. 또한 악성코드를 유포하는 것이 해킹을 위한 사전적 준비행위에 해당한다는 점, 악성코드와 해킹툴의 구별이 어려워지는 점, 해킹툴과 같이 불법목적으로 가진 프로그램을 제작하는 행위 등과 같이 위험한 예비행위를 처벌할 필요성이 있다. 이에 최근의 독일형법 개정안을 고려하여 우리 형사입법에도 도입할 수 있는지에 대하여 검토하였다.

* 단국대학교 법정대학 법학과 조교수, 법학박사

Ⅰ. 머리말

정보화사회에서 유비쿼터스사회로 넘어가는 과도기에 위치한 우리나라의 IT기술의 발전은 삶의 질을 획기적으로 개선하여, 새로운 IT서비스의 출시와 IT 인프라의 고도화 등 정보서비스환경을 급격히 변화시키고 있지만, 이러한 발전에 따른 역기능으로 새로운 IT 위협 또한 증가하고 있다. 현재 정보시스템은 행정・금융・산업・교통・군사・의료분야 등 국가사회전반에 보급되어 활용되고 있기 때문에 해킹은 최첨단 정보통신기술을 이용해 사회 중추신경인 정보통신망을 안정적인 운영을 방해・파괴하고, 해킹으로 획득한 정보를 불법적 용도로 사용함에 따라 사회의 안전에 중대한 위협이 되고 있다.[1)]

한국정보보호진흥원에서 2006년 해킹과 바이러스 동향을 분석한 결과에 따르면, 해킹시도와 웜・바이러스제작목적이 과거에는 단순한 호기심이나 명예성취에서 행해졌지만, 현재는 특정정보 또는 서비스를 대상으로 하는 금전적 탈취로 변화하고 있다고 한다. 이러한 목적의 변화로 인하여 공격대상 또한 특정화되어, 2005년 대비 해킹・바이러스 전체 피해건수는 감소하였으나 위험도는 더욱 높아지고 있다.[2)] 악성코드는 특정서비스 이용자가 많이 접속할 것으로 예상되거나 일반적으로 인지도가 높은 사이트를 대상으로 해킹하여 초기화면에 게임ID와 비밀번호 등을 탈취하는 악성코드를 은닉하여 일반이용자가 해당 사이트 접속할 때 이용자의 PC를 감염시키는 것으로, 최근에는 정상적인 데이터베이스 내에 악성코드를 삽입하는 등 수법이 고도화, 지능화되고 있다.[3)] 뿐만 아니라 공격기법 또한

---

1) FBI 국가기반구조보호센타 책임자인 Michael Vatis는 미의회 경제위원회에서 사이버 공격에 의한 국가기반구조인 통신, 전기, 수송, 가스와 유류공급, 은행, 금융, 상하수도, 긴급구호서비스, 정보기능에 대한 공격들은 국가안보나 경제에 큰 영향을 줄 수 있으며, 진주만공격에 비교할만한 재앙이 될 수 있다고 증언한바 있다(구상회, 테러학개론, 1999, 252면).

2) 대표적으로 LineageHack 등의 트로이잔은 특정 웹게시판, 자료실에 은닉되어 유포되며, 특정 게임의 ID와 비밀번호를 탈취하여 아이템사기등에 악용되고 있다. 이러한 트로이잔은 지속적으로 발견되고 있으며, 06년 발생한 피해건수는 05년 대비 51.6% 감소하였으나, 이러한 악성코드 유포의 궁극적 목적은 금전적 이익을 취하기 위한 것이기 때문에 그 위험성은 더욱 높아졌다고 할 수 있다(한국정보보호진흥원, 2006 정보시스템 해킹・바이러스 현황 및 대응, 2006.12, 5면).

정보시스템에 직접적으로 침입을 시도하기 보다는 해커는 트로이잔을 감염시키기 위해 해당정보를 소유한 사람이 가장 많이 방문할 만한 온라인 커뮤니티, 자료실, 게시판, 블로그 등을 대상으로 Virut와 같은 악성코드를 은닉한 후 개인PC를 악성 봇(Bot)[4]으로 감염시킨다. 좀비(Zombie)라 불리는 '악성 봇 감염시스템'은 사용자의 의지와 관계없이 해커가 미리 준비해 둔 IRC서버에 접속하여 해커로부터 웜 전파시도 등의 악성행위 명령을 전달받아 수행하게 된다. 최근에는 해킹한 서버를 IRC서버로 설정하여 악용하는 추세이다.[5] 이와 같이 해커의 원격통제가 가능한 악성 봇에 감염된 소위 좀비PC는 해커의 원격명령을 받아 특정사이트에 트래픽공격을 시도하는 DDos 공격은 물론 스팸메일발송 등 사이버범죄에 악용되고 있지만, 더욱 심각한 것은 개인사용자의 입장에서도 자신의 PC가 좀비PC로 이용되고 있다는 사실을 인식하지 못하기 때문에 개인PC안에 있는 개인정보, 금융정보가 유출될 수 있다는 것이다.[6]

이와 같이 해킹공격기법이 IT 기술의 발전과 궤를 같이 하여 끊임없이 새로운 공격기법이 등장함에도 불구하고 해킹과 관련된 형사법적 대응규범은 그 내용이 너무나 단순하다. 즉 해킹에 대한 범죄를 규율하는 정보통신망이용촉진등에관한법률(이하 정보통신망법)[7] 제48조 제1항은 누구

3) 국내 연간 해킹・바이러스 사고통계 및 분석에 대해서는 한국정보보호진흥원, 2006 정보시스템 해킹・바이러스 현황 및 대응, 2006.12, 9면이하 참조.

4) 악성 봇은 IRC Robot에서 유래한 단어로, IRC(Internet Relay Chat)라는 인터넷채팅에서 사용자 로그아웃 이후에도 대화방을 보전하기 위해 홀로 남아 대화방을 지키던 프로그램이 그 기원이다. 이후 IRC Robot에 여러 가지 기능이 추가되고 해커들이 웜・바이러스에 접속시키면서 현재의 악성 봇으로 진화하게 된다.

5) 특히 2006년에 나타난 웜・바이러스의 가장 큰 특징인 웹사이트를 통한 트로이잔 기능을 가진 악성코드이며, 이러한 악성코드의 전파수단으로 가장 보편화된 인터넷 서비스인 웹(WWW)를 활용하는 경향이 매우 두드러진 점이다. 악성코드로 총칭되는 인터넷 웜, 바이러스, 트로이잔 및 애드웨어, 스파이웨어, 악성 봇 들은 그 경계를 짓기가 매우 모호해지고 있다(한국정보보호진흥원, 해킹・바이러스 동향, 38면).

6) 한국정보보호진흥원에 따르면 2006년 전 세계 Bot 감염추정 PC 중 국내 PC가 차지하는 비율이 12.5%에 해당한다고 추정하고 있다.

7) 이외에도 정보의 위작・변작・행사에 관한 특별법으로 '산업기술기반조성에관한법률', '무역업무자동화촉진에관한법률', '화물유통촉진법', '공공기관의개인정보보호에관한법률', '신용정보의이용및보호에관한법률' 등이 있고, 비밀침해・보호조치 침해 및 정보 훼손에 관한 특별법 규정으로 앞의 법률들 외에 '통신비밀보호법', '전기통신사업법' 등에서 그 구성요건과 형벌이 규정되어 있다.

든지 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하여서는 아니된다고 규정하고 있으며, 이를 동법 제63조 제1항에 의해 처벌하고 있을 뿐이다. 종전의 보호조치를 침해하지 않고 정보통신망에 '침입'하는 즉, 보호조치를 우회하는 해킹유형을 처벌하기 위해 동법을 개정하였다. 입법적 연혁을 통해 볼 때 보호조치를 침해하지 않고 침입하는 경우뿐만 아니라 보호조치를 침해한 후 침입하는 경우에도 적용이 가능하다고 생각된다. 따라서 정보통신망에 정당한 접근권한이 없이 침해하는 경우를 보호조치와의 관련성에서 보호조치를 침해한 후 정당한 접근권한 없이 침입하는 경우와 보호조치를 침해하지 않고 정당한 접근권한 없이 침입하는 경우로 나누어 보아야 한다. 현재 해킹기법은 정보통신망에 침입을 한 것으로 볼 수 있는지 의문이 드는 기법이 등장하였기 때문이다(Ⅲ). 논의를 본격적으로 전개하기 위하여 해킹과 관련된 기본개념인 해킹, 정당한 권한없는 침입, 보호조치를 설명한 후(Ⅱ), 현재 해킹과 관련된 현행법규정을 정보통신망의 보호조치와의 관련하여 정당한 접근권한없이 침입하는 경우와 권한을 남용하여 침입하는 경우로 각각 나누어 고찰한다(Ⅲ). 마지막으로 새로이 등장한 특수한 형태의 해킹기법이 현행법해석으로 처벌될 수 있는지를 살펴본 후 형사법적 흠결이 있다면 이를 보완하는 방법을 제시하고자 한다(Ⅳ).[8] 또한 2007년 8월 독일형법개정법 §202 c은 EU의 사이버범죄방지조약[9]의 이행을 위하여 개정되었는데, 개정법 내용 중 컴퓨터해킹에 사용될 수 있는 소프트웨어의 유통을 처벌하고 있다. 이와 대하여 우리의 경우에도 입법적으로 해킹과 관련되어 '위험한 예비행위'를 도입할 수 있는지를 살펴보고자 한다.

---

8) 단순한 해킹행위 그 자체에 그치는 것이 아니라, 해킹을 통한 새로운 법익침해유형에 대해서는 살펴볼 필요는 있다. 즉 해킹을 통한 비밀침해, 해킹을 통한 자료삭제 및 자료변경, 해킹에 의한 재산취득 등이 있을 수 있다.

9) 유럽이사회의 사이버범죄방지조약(ETS-Nummer 185)은 2001년 11월 회원국에 의해 서명되고, 2004년 7월 1일부로 발효되었다. 또한 유럽연합의 정보시스템의 공격에 대한 기본결정(ABI, EU Nr. L 69 S.67)은 유럽연합 계약 IV의 규정에 근거하여 2005년 2월 24일 마련되었다. 이에 따라 독일은 컴퓨터범좌와 관련된 형법규정을 개정하게 되었고, 이 개정법은 연방의회의 의결을 거쳐 2007년 8월 11일부터 발효되었다. 독일 형법개정과 관련된 입법이유에 대한 자세한 분석과 평가에 대해서는 박희영, 독일의 컴퓨터범죄방지에 관한 개정형법의 분석 및 평가, 인터넷법률, 제40호, 2007.10, 77면이하 참조.

Ⅱ. 해킹과 관련된 기본개념

1. 해킹과 정당한 권한없는 침입

해킹이라는 용어는 광범위하게 사용됨에도 불구하고 아직 법적으로 확립된 개념이라고 볼 수 없다.[10] 더욱이 단순해킹의 개념에 대한 국내문헌의 정의는 아주 다양한 방면으로 전개되고 있다. 즉 타인의 컴퓨터시스템에 무단으로 침입하여 수록된 정보를 빼내거나 시스템을 파괴하는 행위로 보는 견해[11], 시스템에 침입하는 순간 해킹된 시스템에 저장되어 있는 데이터가 강제적으로 해커의 모니터에 보여진다는 점에서 단순히 침입하는 것과 데이터의 인식을 구별하는 것이 기술적으로 불가능하다는 관점에서 권한없이 타인의 컴퓨터시스템에 접근하여 그곳에 저장된 프로그램이나 데이터를 해커의 모니터상에 불러내어 보는 것이라고 보는 견해[12], 전산망이나 컴퓨터시스템의 보호장치나 안전장치를 기술적 수단을 이용하여 훼손하고 비밀번호의 해독프로그램 등을 이용하여 무단접속하여 권한없이 시스템에 수록된 정보를 탐지하는 행위로서 전산망의 보호조치를 침해하고 단순히 데이터를 탐지하는 것 이외에는 별도의 침해적인 행위를 하지 않는 경우라고 정의하는 견해[13]등이 있다. 또한 컴퓨터를 이용하여 다른 사람의 정보처리장치 또는 정보처리조직에 침입하거나 기술적인 방법으로 다른 사람의 정보처리장치가 수행하는 기능이나 전자기록에 함부로 간섭하는 일체의 행위로 파악하는 견해[14], 컴퓨터에 단순히 침입하는 행위와

---

10) 이상돈, 해킹의 범죄화, 윤리경영과 형법, 2005. 326면; 이상돈교수는 해킹이 사회학적으로 아노미적 상징체계속에 있는 한, 해킹의 의미를 법률적 개념으로 세련화하는 데에는 한계가 있다고 한다. 특히 죄형법정주의가 요구하는 수준의 명확성을 충족시키기는 힘들다고 강조한다.

11) 강동범, 사이버범죄와 형사법적 대책, 80면; 최영호, 정보범죄의 현황과 제도적 대처방안, 형사정책연구원, 1998, 61면.

12) 박희영, 단순해킹의 가벌성에 관한 비교법적 연구, 인터넷법률 통권 제34호, 2006.3, 24면; Jan Vetter, Gesetzeslücken bei der Internetkiminalität, Diss. 2002, S. 122ff.

13) 전지연, 전자적 정보의 형사법적 보호에 관한 연구, 한림법학 FORUM 제8권, 1999, 58면; 강동욱, 정보통신망이용에 있어서 개인정보보호를 위한 형사법적 대응방안에 대한 고찰, 인권과 정의, 1999.12, 36면.

14) 백광훈, 사이버테러리즘에 관한 연구, 형사정책연구원, 2001, 184면.

그 이후 추가적으로 이어지는 행위를 구분하여 타인의 컴퓨터에 단순히 침입하는 행위로 보는 견해[15] 등이 있다.

독일에서의 해킹개념은 컴퓨터체계 또는 컴퓨터전산망에 대한 침입 또는 전자자료의 부당한 인지뿐만 아니라, 컴퓨터체제의 조작을 동일시하고 있다.[16] 제2차 경제범죄처벌에관한법률(WiKG) 당시의 해킹은 타인의 컴퓨터시스템의 단순한 침입을 의미하며, 그 정도를 넘어 타인의 전자자료를 무단으로 절취하거나 컴퓨터시스템에 별도의 침해를 수반하는 것은 제외하였다. 당시의 입법자료에 의하면 해킹의 적용대상이 될 수 있는 형법 202조a는 데이터의 탐지를 내용으로 하기 때문에 단순해킹은 202조a의 적용대상이 아님을 분명히 하였으며, 학설 또한 단순해킹은 202조a의 구성요건해당성이 없다고 하였다.

해킹의 최종적인 목적은 시스템에 수록된 데이터에 대한 침해일수 있지만, 해킹의 유형에는 데이터를 삭제하는 것뿐만 아니라 정보통신망의 관리자체를 침해하는 유형의 해킹도 있을 수 있다. 형법상 처벌을 위한 해킹유형을 개념화함에 있어서 지나치게 넓은 의미로 정의할 수 없다.[17] 해킹개념에 대한 논의에 있어서 공통적으로 사용하는 개념표지는 '정보통신망'과 '침입'개념이며, 정보통신망침입이후에 추가적으로 이어지는 행위의 유형을 구별하는 것이 타당하다. 해킹에 대한 대응법규인 정보통신망법 제48조 규정에 대응하여 해킹의 개념정의를 해보면, 컴퓨터등 정보처리장치를 이용하여 정당한 접근권한이 없는 자 또는 접근권한이 있는 자가 그 권한을 남용하여 정보통신망에 침입하는 행위를 의미한다.[18]

---

15) 김일수/배종대/이상돈, 정보화사회에 대비한 형사법적 대응, 비교형사법연구 제3권 제2호, 42면; 류석준, 해킹에 대한 규제법규에 관한 연구, 비교형사법연구 제6권 제2호, 191면.

16) Lackner, StGB Kommentar §202a Rn. 5.

17) 유인모, 정보형법의 과제와 전망, 형사정책 제12권 제1호, 2000.6, 71면.

18) 단순해킹을 처벌할 수 없다는 입장에서 단순한 침입은 기존의 형법적 법익의 침해를 수반하지 않는 침해의 전단계로서 행위유형에 해당하기 때문에 단순해킹은 비범죄화되어야 한다고 하지만, 대법원판례에 따르면 단순해킹 또한 정보통신망 자체의 안정성과 그 정보의 신뢰성을 보호법익으로 파악하고 있으므로, 단순해킹의 경우에도 법익침해를 수반하는 범죄유형이라고 볼 수 있다(대법원 2005.11.25, 2005도870판결 참조).

2. 보호조치

전통적으로 시스템에 대한 보호조치는 권한을 가진 사용자만이 시스템 사용 권한을 가질 수 있도록 하는 운영체제 측면에서의 보호조치이다. 따라서 파일이나 디렉토리 등에 대한 접근이 정당한지를 판별하기 위한 접근제어(Access Control), 권한 있는 사용자의 접근 여부를 판별하기 위한 인증절차(Authentication), 접근결과를 감사추적하기 위한 감사(Audit trail) 등이 있다.

그러나 최근에는 네트워크의 의존도가 높아짐에 따라 단순히 개별시스템보호에 그치는 것이 아니라 네트워크 환경에서의 시스템적 보호로 발전하고 있다. 네트워크 보안 기술은 개별 제품의 형태에서 복합 형태로 발전하게 되고[19], 정보보호 서비스의 필요성이 증가함에 따라서 보안 관제 서비스가 확대되며[20], 이를 통해서 해커들의 침입에 대한 기존의 모니터링을 통한 수동적인 방어에서 탈피하여 침입자 경로를 역추적하여 계속적인 침입을 막기 위한 능동적이고 지능적인 정보보호 기술로 발전하고 있다.[21]

침입차단·탐지시스템의 경우 방화벽(Firewall)이라고 알려진 침입차단 시스템의 제한적인 시스템 보호능력의 한계를 극복하기 위해 침입탐지 시스템(Intrusion Detection System: IDS)으로 발전하고 있다. 이는 인가되지 않은 사용자의 침입을 사전에 탐지하여 시스템 자원을 효과적으로 보호하기 위한 시스템이다.[22] 침입에는 침입으로 여겨지는 행위나 성공하지 못한 침입 시도, 침입을 위한 준비 행위 등은 포함되지 않는다. 이를 위해 알려진 공격에 대한 제한적인 차단(IP, 포트별 접근차단)뿐만 아니라 이미

---

19) 이렇게 복잡한 보안 시스템을 통합 관리하기 위해서 IETF(Internet Engineering Task Force)나 DMTF(Distributed Management Task Force) 등에서는 표준화를 추진하고 있으며, 다른 기종 보안제품들을 상호연동하기 위해서 OPSEC(Open Platform for SECurity), IDMEF(Intrusion Detection Message Exchage Format)와 같은 프로토콜이 개발되고 있다.

20) 보안관제업체가 제공하는 서비스는 크게 네트워크 자체의 보안을 관리 및 유지해주는 네트워크 보안 서비스, 해당 기업 전산 시스템의 해킹 관제 서비스, 해킹된 시스템의 실시간 복구 서비스, 시스템의 이중화를 통한 데이터 저장 서비스 등이 있다.

21) 한국정보보호학회, 차세대 네트워크 보안기술, 한국정보보호진흥원, 2002, 41-43면.

22) 침입(Intrusion)이란 컴퓨터시스템 자원에 대한 무결성(Integrity), 기밀성(Confidentiality) 또는 가용성(Availability)등을 침해하는 일련의 행위를 말하며, 컴퓨터 시스템의 보안 정책을 파괴하는 모든 행위를 말한다(한국정보보호학회, 앞의 책, 217면).

알려져 있는 공격 신호를 감시하면서 수상한 네트워크 활동을 찾는 탐지 과정을 수행한다. 탐지과정 중 수상한 네트워크 활동을 찾아냈을 경우 보안관리자에게 경고 메시지를 보내고 침입의 진전 상황을 보고함으로써 좀 더 효과적인 시스템 보호를 위한 자료를 제공한다.[23] 그러나 네트워크 침입탐지 시스템은 실시간으로 공격을 막을 수 없다는 단점이 있다. 이는 네트워크상에 있는 비정상적 패킷흐름에 대한 감지만 하고, 차단하지 못하기 때문이며 대부분 패킷은 네트워크 침입탐지 시스템이 파악하기 전에 이미 지나쳐 공격하고자 한 목적지에 도달하여 결과적으로 네트워크 침입탐지 시스템이 판별하기 전에 침입에 성공하게 된다.

침입방지 시스템(Intrusion Prevention System : IPS)은 다양한 침입 기술을 다양한 방법의 보안 기술을 이용하여 침입이 일어나기 전에 실시간으로 침입을 막고, 만일 알려지지 않은 방식의 침입이 있다면 이로부터 네트워크와 호스트를 보호할 수 있는 시스템을 말한다. 스니퍼(Sniffer)[24]를 기반으로 탄생한 침입탐지 시스템이 외부의 공격을 정확하게 탐지하는데 그 목적이 있는 반면에 이 시스템은 방화벽(Firewall)과 침입탐지 시스템(IDS), 시큐어(Secure) OS 등의 보안 기술에 기반 두고 외부의 공격탐지와 함께 그 공격이 일어나는 것을 근본적으로 방어하는 것을 목적으로 한다. 침입방지 시스템과 침입탐지 시스템의 결정적인 차이점은 외부의 침입에 대한 대처방법에 있다. 침입탐지 시스템은 침입이 발생하였을 때 그 침입에 대해서 즉각적으로 대처하지는 못하지만, 침입방지 시스템의 경우 공격 신호를 찾아내고 네트워크의 트래픽을 관찰해서 수상한 활동을 하는 패킷에 대해서 즉각적으로 대처할 수 있다. 또한, 만일 서버가 비정상적인 행동을 할 경우에는 자동으로 실행을 중단할 수도 있다.[25] 이런 점에서 침입방지 시스템은 침입탐지 시스템에 비해 보다 적극적인 대응 시스템이다.

그러나 보호조치에 직접 대응하지 않고 이러한 보호조치를 우회하여 접근하는 경우에는 이러한 단계별 고찰이 무의미하다. 종래에는 웜 · 바이러

---

23) 정보홍외 2명, 침입방지 시스템의 기술 및 전망, 한국정보보호산업협회, 2003, (kidbs.itfind.or.kr:8888/WZIN/jugidong/1098/109801.htm) 참조.

24) 스니퍼(Sniffer)는 네트워크 트래픽을 감시하고 분석하는 프로그램으로서 병목현상 등과 같은 문제점을 발견해낸다. 이러한 정보들을 이용하면 네트워크 관리자는 트래픽의 동향을 효율적으로 유지할 수 있다.

25) 정보홍외 2명, 앞의 논문 참조.

스와 해킹기능의 상호연관성이 없었지만, 현재는 양자의 기능결합으로 복합화(Blended), 악성화된 사이버공격의 증가와 사이버공격의 초고속화가 진행되고 있다. 즉 시스템에 대한 취약점을 자동으로 검색하며, 감염된 좀비 PC의 원격제어를 통한 공격 등 공격기법이 점차 자동화되고 있으며, 다양한 변종을 양산하여 방어체계를 무력화시키는 등 지능화되고 있다. 따라서 정보통신망의 보호조치를 침해하지 않으면서도 침입할 수 있는 새로운 형태의 공격기법이 등장함에 따라서 정보통신망법 또한 종래 보호조치를 침해하지 않고 침입할 수 있는 것을 예정하여 법률을 개정한 것이다.

Ⅲ. 해킹에 대한 법적용 가능성 검토

1. 문제제기

정보통신망법 제48조 제1항은 구 전산망보급확장과이용촉진등에관한법률 제22조 제2항 및 구 정보통신망이용촉진등에관한법률 제19조 제3항과 달리 정보통신망에 대한 보호조치를 침해하거나 훼손할 것을 구성요건으로 하지 않고, 단지 '정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입'하는 행위를 금지하고 있다. 이는 정보통신망의 보호조치를 침해하지 않으면서도 침입할 수 있는 새로운 형태의 공격기법이 등장함에 따라서 종래 보호조치를 침해하지 않고 침입할 수 있는 것을 예정하여 법률을 개정한 것이다. 하지만, 입법적 연혁을 통해 고찰해볼 때 보호조치를 침해하지 않고 침입하는 경우뿐만 아니라 행위자가 정보통신서비스제공자의 보호조치를 침해한 후 침입하는 경우에도 적용이 가능하다고 생각된다. 따라서 정보통신망에 정당한 접근권한이 없이 침입하는 경우를 정보통신망의 보호조치와의 관계에서 보호조치를 침해한 후 정당한 접근권한이 없이 침입하는 경우와 보호조치를 침해하지 않고 정당한 접근권한이 없이 침입하는 경우로 나누어 볼 수 있다. 허용된 접근권한을 초과하여 정보통신망에 침입하는 경우 역시 보호조치 침해여부에 따라 양자로 나누어 살펴볼 필요가 있다.

2. 정당한 접근권한없이 침입하는 경우

가. 정당한 접근권한

정보통신망법 제48조 제1항의 보호법익은 사인간의 신뢰를 보호하기 위한 것이 아니라 정보통신망의 안정성 확보를 위한 것이다.[26] 즉 정보통신망법은 정보통신서비스제공자로 하여금 정보통신망의 안정성 및 정보의 신뢰성확보를 위한 보호조치를 하도록 하고 있다. 하지만 보호조치를 침해하지 않는 새로운 형태의 해킹공격기법에 대응하기 위하여 종전의 보호조치의 침해를 전제로 한 규정에서 정당한 권한없이 또는 권한을 초과하여 침입하는 행위를 금지하는 규정으로 개정한 것이므로 동법의 입법의도는 해킹행위의 방지에 있는 것은 분명하다. 따라서 위 조항에서 정당한 권한 없이 또는 허용된 권한을 초과에서 접근권한을 부여하거나 허용하는 주체는 원칙적으로 정보통신서비스제공자라고 볼 수 있으며, 접근권한이 정당한지, 허용된 범위내의 접근인지 여부는 원칙적으로 서비스제공자의 입장에서 판단해야 한다. 즉 정보통신망에 대한 접근권한을 서비스제공자로부터 획득한 것이 아니라 추정에 의한 무차별대입에 의해 접근권한을 획득하거나, 패스워드 크래킹 등과 같이 부정한 방법으로 취득하여 접속한 제3자는 정당한 접근권한이 없는 경우이다. 뿐만 아니라 과거 직무상 알게 된 아이디와 비밀번호로 퇴직 후 접속한 경우[27], 우연히 알게 된 타인의 아이디와 비밀번호로 이용자의 승낙없이 접속한 경우[28]등의 경우에도 정당한 접근권한이 없는 경우라고 할 수 있다.

문제는 서비스제공자로부터 접속에 관한 권한을 부여받은 이용자가 다시 제3자에게 사용하도록 승낙할 수 있는지 여부이다.[29] 이에 대하여 대

---

26) 대법원 2005.11.25. 선고 2005도870 판결.

27) 서울지법 2003. 2. 17. 선고 2002고단9232 판결; 서울지법 2003. 10. 10. 선고 2003고단7734 판결; 서울중앙지법 2004. 3. 18. 선고 2004고정164 판결; 전주지법 2004. 12. 10. 선고 2004고정935 판결(이에 대한 간단한 소개로는 이범균, 대법원 2005. 11. 25. 선고 2005도870 판결, 대법원판례해설, 제59호, 616면-617면 참조)

28) 서울동부지법 2004. 6. 8. 선고 2003고단4200 판결; 수원지법 2004. 8. 16. 선고 2004고정1082 판결; 안산지원 2005. 3. 15. 선고 2004고정1843 판결

29) 이에 대하여 승낙이 불가능하다는 입장, 승낙이 가능하다는 입장의 예상되는 논거와 각 견해의 적용에 따른 결과와 이에 대하여 예상되는 문제점에 대한 자세한 분석으로

법원 2005.11.25. 선고 2005도870 판결에서는 업무상 알게 된 직속상관의 아이디와 비밀번호를 이용하여 직속상관이 모르는 사이에 군 내부전산망 등에 접속하여 직속상관의 명의로 군사령관에게 이메일을 보낸 사안에서, 정보통신망법 제48조 제1항에 규정한 정당한 접근권한 없이 정보통신망에 침입하는 행위에 해당하는지에 대하여 "접근권한을 부여하거나 허용되는 범위를 설정하는 주체는 서비스제공자라 할 것이고, 따라서 서비스제공자로부터 권한을 부여받은 이용자가 아닌 제3자가 정보통신망에 접속한 경우 그에게 접근권한이 있는지 여부는 서비스제공자가 부여한 접근권한을 기준으로 판단"하므로, 원칙적으로 서비스제공자로부터 권한부여를 받지 않은 제3자에게는 정당한 접근권한이 없다고 한다. 그러나 예외적으로 ① 그 제3자의 사용이 이용자의 사자(使者) 내지 사실행위를 대행하는 자에 불과할 뿐 이용자의 의도에 따라 이용자의 이익을 위하여 사용되는 경우와 같이 사회통념상 이용자가 직접 사용하는 것에 불과하거나, ② 서비스제공자가 이용자에게 제3자로 하여금 사용할 수 있도록 승낙하는 권한을 부여하였다고 볼 수 있거나 또는 서비스제공자에게 제3자로 하여금 사용하도록 한 사정을 고지하였다면 서비스제공자도 동의하였으리라고 추인되는 경우에는 정당한 접근권한이 있다고 판단하고 있다.

생각건대, 정당한 접근권한에 대한 판단은 제공되는 정보서비스의 성격에 따라 개별적·구체적으로 판단해볼 필요가 있다. 대부분 정보통신서비스제공자의 정보통신망의 이용에 따른 약관을 살펴보면 이용자는 서비스의 이용권한을 타인에게 양도, 증여할 수 없다고 정하고 있다.[30] 이는 실제공간과는 달리 익명성이 통용되어 실제 행위자가 누구인지를 명확하게 확인하기 어려운 가상공간에서 아이디와 비밀번호 등 식별부호는 그 행위자의 인격을 표상하는 것으로, 그러한 신뢰가 무너지면 정보통신망의 안정성 및 그 정보통신망 안에 있는 정보의 신뢰성이 깨어진다고 할 수 있기 때문이다.[31]

는 이범균, 앞의 논문, 620면 이하 참조.

30) 포탈사이트중의 하나인 nate.com의 이용자약관 제20조 (회원 ID(고유번호)와 Password (비밀번호) 관리에 대한 의무와 책임) 제3항에서는 본인의 ID(고유번호) 및 Password(비밀번호)를 제3자에게 이용하게 해서는 안된다고 정하고 있으며, 제25조에서는 회원은 서비스의 이용권한, 기타 이용 계약상 지위를 타인에게 양도, 증여할 수 없으며, 이를 위반한 경우 손해배상을 청구할 수 있다고 규정하고 있다.

이 경우 정당한 접근권한에 대하여 이용자가 서비스제공자의 승낙여부와는 상관없이 제3자에게 양도하거나 일시사용하게 할 수 있는가 여부는 정보통신서비스제공자가 접근권한을 일률적으로 정할 것이 아니라 제공되는 정보통신서비스의 구체적 성격에 따라 개별적으로 판단할 필요가 있다고 생각된다. 예를 들면 인터넷동영상강좌를 제공하는 사이트와 같이 인터넷콘텐츠를 제공하는 대가로 이용자에게 일정한 비용을 지불하게 한 후 개인별로 식별부호를 부여하는 경우에는 서비스제공자가 허락한 경우를 제외하고는 이용자는 제3자에게 자신의 접근권한을 양도 또는 일시사용하게 할 수 없다고 보아야 한다. 하지만 서비스제공자의 입장에서 이용자 자신이 사용하든 타인으로 하여금 사용하게 하든 서비스제공자가 이용자에게 부여한 권한의 범위 내에서 발생한 것이라면 서비스제공자의 입장에서는 차이가 없는 경우에는 달리 살펴볼 필요가 있다. 게임전용 정보통신망와 같이 정보제공보다는 아이디별로 사용해온 실적과 아이템을 기준으로 게임에 이기기 쉬운 더 많은 능력을 사용할 수 있도록 하는 게임서비스를 제공하는 정보통신망의 경우, 이메일서비스나 기업이나 법률등과 같은 고급유료정보를 제공하는 서비스제공과 달리 실제공간의 주체가 누구인지는 문제되지 않기 때문에 이용자가 제3자에게 양도한 경우 명시적 제한이 없는 한 서비스제공자가 양도를 승낙할 가능성이 있기 때문이다. 따라서 이 경우에는 제3자의 접근은 원칙적으로 접근권한이 있다고 볼 수 있다.

대법원 판례에서 나타난 육군웹메일이나 핸드오피스 시스템의 경우와 같이 이메일서비스뿐만 아니라 전자결제기능을 부가하고 있는 시스템의 경우 정보서비스제공자가 이용자의 특성에 따라 사용권한의 유무와 권한범위를 정해놓은 경우이기 때문에 원칙적으로 이용자가 제3자에게 권한을 양도할 수 없으며, 제3자가 접근한 경우에는 정당한 접근권한 없이 침입한 경우에 해당한다. 그러나 게임서버의 경우에는 이용자의 특성에 따라 사용권한과 권한의 범위를 정해놓은 것이 아니기 때문에 이용자가 권한을 양도한 제3자가 접근한 경우에는 정당한 접근권한이 있는 경우라고 볼 수 있다.[32] 참고로 일본의 부정액세스행위금지등에관한법률[33] 제3조에서는

31) 이범균, 앞의 논문, 621면.

32) 실제로 가족, 친구, 직장동료 등 가까운 사이에서 아이디를 공유하는 등으로 사용을 승낙하는 경우가 많은데, 이를 원칙적으로 정보통신망법 위반으로 보는 것은 잠재적 범

부정액세스행위에서 당해 액세스제어기능을 부가한 액세스관리자가 하는 경우 또는 당해 액세스관리자 또는 당해 식별부호에 관계된 이용권자의 승낙을 얻어 액세스하는 경우에는 부정액세스라고 보지 않는다.

나. 정당한 접근권한없이 보호조치를 침해한 후 침입하는 경우

1) 형법 제316조 제2항 비밀침해죄의 적용가능성

타인이 설치한 보안장치를 단순히 푸는 행위만 하고 타인의 비밀을 탐지하지 않는 유형의 해킹의 경우에도 형법 제316조 제2항의 비밀침해죄가 적용될 수 있는가에 해당하는 가에 대하여 부정하는 견해는[34] 본죄를 침해

죄자를 양산하는 셈이 되어 현실과 동떨어진 결론이 될 수 있으며, 정보통신망의 목적이 정보통신망의 안정에 있다고 본다면 이용자의 승낙을 얻어 접근한 경우에 정보통신망의 교란이나 훼손이 있다고 볼 수 없기 때문에 이용자의 승낙을 얻어 접속한 경우까지 처벌대상으로 하는 것은 입법목적을 넘어선 새로운 구성요건을 만드는 경우가 될 수 있다(이범균, 앞의 논문, 629면).

33) 동법의 목적은 컴퓨터관련범죄나 전자통신방법에 의한 범죄를 방지하고 접근통제를 이용하여 설치되어 있는 전자통신에 관한 질서의 유지에 있다(제1조). 즉 컴퓨터네트워크의 보호자체와 컴퓨터사기 또는 컴퓨터업무방해를 그 전단계에서 미리 금지하는데 중점이 있다. 동법 제3조에 따르면 부정액세스행위를 금지하고 있는데, 부정액세스행위란 ① 액세스제어기능을 가지는 특정컴퓨터에 통신망을 통하여 당해 액세스제어기능에 관계된 타인의 식별부호를 입력하여 특정컴퓨터를 작동시키고, 액세스제어기능에 의하여 제한되고 있는 특정이용을 할 수 있는 상태가 되게 하는 행위(접근통제장치가 되어 있는 컴퓨터에 타인의 ID를 무단히 입력하는 행위), ② 액세스제어기능을 가지는 특정컴퓨터에 통신망을 통하여 액세스제어기능에 의하여 제한되고 있는 특정이용의 제한을 면할 수 있는 정보 또는 명령을 입력하여 특정컴퓨터를 작동시키고, 그 제한되어 있는 특정이용을 할 수 있는 상태가 되게 하는 행위(컴퓨터에 접근제한을 회피하는 정보나 명령(ID제외)을 입력하는 행위), ③ 전기통신회선을 매개로 하여 접속된 다른 컴퓨터가 가지고 있는 액세스제어기능에 의하여 특정이용을 제한하고 있는 컴퓨터에 전기통신회선을 통하여 그 제한을 면하게 할 수 있는 정보 또는 명령을 입력하여 당해 특정컴퓨터를 작동시키고, 그 제한되어 있는 특정이용을 할 수 있는 상태가 되는 행위(다른 인증서버에 의하여 접근이 통제되는 컴퓨터에 정보나 명령을 입력하는 행위)를 말한다. 이외에도 동법 제4조에서는 타인의 ID를 무단히 공개함으로써 부정한 접근을 조장하는 행위를 처벌하고 있다.

34) 김일수/서보학, 형법각론, 제6판, 2004, 228면; 이재상, 형법각론, 222면; 배종대, 형법각론, 295면; 정성근/박광민, 형법각론, 216면; 임웅, 형법각론, 229면; 백광훈, 해킹범죄와 그 처벌법규 및 문제점, 2000.12.6 제4회 해킹방지워크샵 발표문; 박희영, 단순해킹의 가벌성에 관한 비교법적 연구, 인터넷법률 제34호, 2006.3, 36면.

범으로 해석하기 때문에 봉함 또는 비밀장치한 특수매체기록을 단지 개봉한 것만으로는 아직 그 내용을 공개할 수 있는 상태에 둔 것은 아니므로,[35] 단지 타인의 시스템에 침입만 하고 그 내용을 알아내지 못한 행위에 대해서는 형법상 처벌규정이 없다고 한다.[36] 이에 대하여 본죄를 추상적 위험범으로 해석하여 내용을 지득하지 못한 경우에도 기수가 된다고 하여 긍정하는 견해가 있다.[37] 본죄의 '그 내용을 알아낸다'는 의미에 대하여 그 내용을 인식하는 것으로 족하고, 그 의미까지 이해할 필요는 없다고 한다. 이에 따르면 화면에 출력된 내용을 보았더라도 그 내용을 이해하지 못하고 이에 따라 비밀이 침해되지 않더라도 본죄가 성립한다고 한다.

생각건대 형법의 비밀침해죄는 정보통신망 자체의 안정성과 그 정보의 신뢰성을 보호하기 위한 것이 아니라 개인의 사생활 즉 프라이버시를 보호하기 위한 법이다. 따라서 개인의 사생활과 관련되지 않은 영역은 본죄의 보호범위에 속하지 않는다고 보아야 한다. 그렇다면 정보통신망에 연결되어 있지 않는 개인의 비밀에 대하여 침해를 한 경우에 본죄의 적용이 문제될 수 있지만, 정보통신망에 연결되어 있는 경우에는 본죄의 적용은 문제되지 않는다고 보아야 한다. 따라서 해킹행위 자체에 대한 가벌성여부는 정보통신망에 연결되어 있는지에 따라 검토되어야 한다.

2) 정보통신망법 제48조 제1항, 제63조

정보통신망법 제48조 제1항에서는 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하여서는 아니된다고 규정하면서 동법 제63조 제1항을 통하여 이를 위반하는 자를 처벌하고 있으며 제2항에 미수범처벌규정을 두고 있다.

현행 정보통신망법 개정이전에는 정보통신서비스 제공자의 보호조치의무를 전제로 하여 서비스제공자가 강구한 보호조치를 침해 또는 훼손하는

35) 김일수/서보학, 형법각론, 229면.
36) 이 견해에 따르면 단순해킹의 경우 처벌흠결은 특별법인 정보통신망법 제48조, 제63조에 의해서 메워질 수 있다.
37) 박상기, 형법각론, 225면; 오영근, 형법각론, 293면; 이정원, 형법각론, 246면; 이형국, 형법각론, 346면; 류석준, 해킹에 대한 규제법규에 관한 연구, 비교형사법연구 제6권 제2호, 199면.

행위만을 처벌대상으로 규정하였으나, 현행 정보통신망법은 그러한 보호조치의 침해 또는 훼손행위를 요건으로 하고 있지 않으며 단지 정당한 접근권한이 없거나 허용된 접근권한을 초과하여 정보통신망에 침입하는 행위를 처벌대상으로 규정하고 있다. 이는 해킹기술의 발전으로 보호조치를 침해하지 않고도 보호조치를 우회하는 방법을 통하여 정보통신망에 침입할 수 있는 방법이 가능해짐에 따라 발생할 수 있는 형벌의 공백을 예상하여 이루어진 입법이다.[38] 따라서 본죄는 정보통신망에 대한 보호조치를 침해하거나 훼손할 것을 요구하지 않으며, 단지 '정당한 접근권한 없이 또는 허용된 접근권한을 초과'하여 정보통신망에 침입하면 성립한다. 하지만, 입법적 연혁을 통해 고찰해볼 때 보호조치를 침해하지 않고 침입하는 경우뿐만 아니라 행위자가 정보통신서비스제공자의 보호조치를 침해한 후 침입하는 경우에도 적용가능하다.

3) 전자기록 손괴죄의 적용여부

해킹과정에서 무력화시키는 대상이 되는 정보통신망의 보호조치[39] 중 기술적 보호조치[40]의 경우 정보보호시스템 중 침입탐지시스템, 침입차단시스템, 인증시스템, 보안관제시스템, 바이러스 월과 같은 경우는 컴퓨터 프로그램인 경우가 대부분이다. 이에 따라 형법 제366조의 전자기록손괴죄가 성립한다는 견해가 있다. 이 견해에 따르면[41] 보안프로그램은 컴퓨터내부

38) 류석준, 해킹에 대한 규제법규에 관한 연구, 191면; 박희영, 단순해킹의 가벌성에 관한 비교법적 연구, 34면.

39) 정보통신망법 제45조 제1항에 따르면 정보통신서비스제공자는 정보통신서비스제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 마련하여야 한다. 이에 따라 정보통신부장관은 제1항의 규정에 따른 보호조치의 구체적 내용을 정한 '정보보호조치 및 안전진단방법·절차·수수료에 관한 지침'을 정하여 고시하고 있다.

40) 보호조치는 구체적으로 관리적 보호조치, 기술적 보호조치, 물리적 보호조치로 나눌 수 있다. 관리적 보호조치는 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련계획을 수립하는 것을 말하며, 정보보호조직의 구성과 운영, 정보보호계획 등의 수립 등을 말한다. 물리적 보호조치는 정보통신시설의 출입·접근·통제 등과 같이 비인가자가 출입할 수 없도록 잠금장치를 설치하는 경우를 말한다.

41) 류석준, 해킹에 대한 규제법규에 관한 연구, 192면; 원혜욱, 인터넷범죄의 특징과 범죄유형별 처벌조항, 형사정책연구 제11권 제42호, 2000, 100면.

의 전자적 기억장치에 컴퓨터언어로 기록된 일단의 컴퓨터명령체계로서 이는 전자기록에 해당하므로 이러한 보안프로그램의 침해 및 무력화는 원래 프로그램기능의 효용을 해하는 행위에 해당한다고 볼 수 있으므로 보호조치를 침해하는 행위는 형법상 전자기록손괴죄에 해당할 수 있다고 한다.

그러나 보안프로그램을 전자'기록'이라고 할 수 있는지에 대하여 의문이 있다. 전자기록 등 특수매체기록이란 사람의 지각에 의하여 인식이 불가능한 방식으로 작성되어 정보처리장치에 의한 정보처리를 위하여 제공된 '기록'을 말하므로, 보안프로그램과 같은 컴퓨터'프로그램'[42]의 경우에는 전자기록이 아니라 전자기록관리 또는 보호장치라고 해석하는 것이 타당하다고 생각된다.[43] 뿐만 아니라 보호조치에는 파일이나 디렉토리 등에 대한 접근이 정당한지를 판별하기 위한 접근제어(Access Control), 권한있는 사용자의 접근 여부를 판별하기 위한 인증절차(Authentication), 접근결과를 감사추적하기 위한 감사(Audit trail) 등이 있다. 대표적인 보호조치인 침입탐지시스템의 경우 공격에 대한 제한적인 차단(IP, 포트별 접근차단)뿐만 아니라 이미 알려져 있는 공격 신호를 감시하면서 수상한 네트워크 활동을 찾는 탐지과정을 수행 중 수상한 네트워크 활동을 찾아냈을 경우 보안관리자에게 경고 메시지를 보내고 침입의 진전 상황을 보고함으로써 좀 더 효과적인 시스템 보호를 위한 자료를 제공하는 역할을 수행하기 때문에, 이와 같이 해킹프로그램에 의하여 보호조치 프로그램이 손괴되는 것이 아니라고 볼 수 있다.[44] 예를 들면 경보장치가 되어 있는 주거에 침입하는 경우, 경보장치에 대하여 직접적으로 손괴하는 것이 아니라 단지 경보장치가 없는 곳 또는 경보체계가 미약한 곳을 찾아서 주거

---

42) 컴퓨터프로그램보호법 제2조에 따라면 "컴퓨터프로그램저작물"이라 함은 특정한 결과를 얻기 위하여 컴퓨터 등 정보처리능력을 가진 장치(이하 "컴퓨터"라 한다)안에서 직접 또는 간접으로 사용되는 일련의 지시·명령으로 표현된 창작물을 말한다고 한다.

43) 형법 제314조의 컴퓨터업무방해죄의 경우 프로그램을 포함하는 개념인 '컴퓨터 등 정보처리장치'와 전자기록 등 특수매체기록을 구분하여 정의를 하고 있으며, 제366조의 전자기록손괴죄의 경우 컴퓨터 등 정보처리장치개념이 없이 전자기록만을 규정하고 있는 것을 보면 양자의 개념은 구별된다고 볼 수 있다.

44) 만약 해킹프로그램등을 통하여 전산망의 안정적인 운영을 방해한 결과가 발생하였다면 손괴죄와 정보통신망법 제62조 제4항의 상상적 경합으로 처벌될 수 있을 것이지만, 단순침입만으로는 손괴의 결과가 발생하였다고 평가하기는 어렵다(임웅, 형법각론, 495면 참조).

에 침입하는 것과 같은 논리이다. 전자기록 등 특수매체기록에 대한 손괴는 기억매체의 파손이나 정보의 소거를 말하여, 기록 그 자체를 소거 또는 변경하는 경우뿐만 아니라 기록매체를 파손하는 경우를 말한다고 보아야 한다. 따라서 형법 제366조의 성립을 부정하는 것이 타당하다.

다. 정당한 접근권한없이 보호조치를 침해하지 않고 침입하는 경우

정보통신망은 무권한자의 접근 내지 침입을 방지하기 위해서 보호조치가 강구되어 있음에도 불구하고, 이러한 보호조치를 해제하거나 우회하여 정보통신망을 권한없이 접근하는 행위를 이른바 단순해킹이라고 불러왔다.[45)46)] 정보통신망에 침입하기 위해서 타인에게 부여된 사용자계정과 비밀번호를 권한자의 동의 없이 사용하는 것 즉 타인의 식별부호 즉 아이디와 패스워드를 무단히 입력하여 정보통신망을 통하여 컴퓨터를 이용하는 행위와 같은 아이디 절도 또는 아이디도용[47)]과 같은 경우, 액서스 제어기능에 따른 이용의 제한을 면하게 하는 것을 가능하게 하는 정보 또는 명령을 입력하여 이용하는 행위(시큐리티 홀 공격 또는 시스템 침입형)같은 경우에는 정당한 접근권한이 없이 보호조치를 침해하지 않고 침입하는 경우라고 볼 수 있다. 이외에도 과거 직무상 알게 된 아이디와 비밀번호를 퇴직 후 접속한 경우, 우연하게 알게 된 타인의 아이디와 비밀번호로 이용자의 승낙없이 접속한 경우 등이 있다.

형법 제316조 제2항의 적용가능성에 대하여 동조의 해석을 통하여 단순해킹의 가벌성을 인정할 수 있다는 견해[48)]가 있지만, 이미 상술한 바와

45) 박희영, 단순해킹의 가벌성에 관한 비교법적 연구, 인터넷법률 통권 제34호, 2006.3, 21면.
46) 개정된 독일형법 제202조a는 본인 또는 타인을 위하여 권한없이, 본인 또는 타인에게 특정되어 있지 아니하고 부당한 접근에 대하여 특별히 보안이 되어 있는 데이터에 '접근보호조치의 극복을 통하여 접근'한 자는 3년이하의 징역 또는 벌금형에 처한다고 하였다. 데이터탐지죄의 개정의 입법이유의 분석에 대해서는 박희영, 독일의 컴퓨터범죄 방지에 관한 개정 형법의 분석 및 평가, 77면 이하.
47) 개념상으로만 보면 단순침입의 한 가지 유형에 해당하지만 사용자 도용이 차지하는 부분이 많아 별도로 구분하고 있다(경찰청 사이버범죄 대응센터).
48) 원혜욱, 인터넷범죄의 특징과 범죄유형별 처벌조항, 형사정책연구 제11권 제2호, 2000. 여름, 100면; 류석준, 해킹에 대한 규제법규에 관한 연구, 비교형사법연구 제6권 제2호, 196면.

같이 형법의 비밀침해죄는 정보통신망 자체의 안정성과 그 정보의 신뢰성을 보호하기 위한 것이 아니라 개인의 사생활 즉 프라이버시를 보호하기 위한 법이므로 개인의 사생활과 관련되지 않은 영역은 본죄의 보호범위에 속하지 않는다고 보아야 한다. 따라서 단순해킹행위에 대한 형법상 처벌규정은 없으며 특별법인 정보통신망법에 의하여 처벌될 수 있을 뿐이다.

다만 정보통신망법 제48조에 따르면 단순해킹에 대한 구성요건표지로 '침입'을 규정하고 있다. 이 규정은 단순해킹을 처벌할 수 있는 규정으로 구법과는 달리 구성요건에서 보호조치 침해를 요건으로 하고 있지 않고 침입하는 행위만 있으면 처벌되기 때문에 보호조치를 침해하지 않고 우회하는 해킹행위도 처벌할 수 있게 된다. 이에 대하여 구성요건적 행위가 침입이라고 규정되어 있다는 점에서 예를 들면 안테나 등 기계장치를 이용하여 모니터의 전자파를 감지함으로써 시스템에 접근하는 경우와 같이 정보통신망에 대한 침입행위가 아닌 외부에서의 부정접근행위는 처벌할 수 없다는 견해가 있다.[49]

생각건대 해킹기법중의 하나인 Ping Scan[50]이나 Port Scan의 경우에는 해커가 특정 호스트를 공격대상으로 삼았을 때 해커는 그 호스트의 약점이 무엇이 있는지 우선 알아내기 위해 Scan을 이용하여 어떤 서비스가 제공되는지 알아낸 후 공격을 시도하는 것이다. 이러한 해킹기법은 '침입'하는 행위라기보다는 '침입을 시도하는' 행위라고 볼 수 있기 때문에 침입을 구성요건으로 하는 정보통신망법 제48조에 따라 기수범으로 처벌하기 어렵다. 구성요건적 행위로서 '침입'은 행위자가 해당 정보통신망의 자원을 사용하기 위해서 거쳐야 하는 인증절차를 거치지 않거나 비정상적인 방법을 사용하여 해당 정보통신망의 접근권한을 획득하는 것으로, 정보통신망의 자원을 임의대로 사용할 수 있는 상태가 되었을 때 침입이 이루어진 것이라고 할 수 있기 때문이다.[51]

---

49) 박희영, 앞의 논문, 39면.

50) ping은 목표물이 현재 작동되고 있는지 확인할 때 사용되는 네트워크진단도구로서 네트워크 매핑을 하는데 유용하다. 즉, 어떤 네트워크에서 사용되는 IP를 알아내기 위해서 네트워크 전체에 걸쳐 ping을 보내고 그 응답을 봄으로서 그 네트워크에서 사용중인 IP를 알아내는 것으로 이 방법은 매우 느리고 오래된 방법은 대부분의 IDS는 이런 형태의 공격을 대개 탐지해낸다.

51) 침입을 시도하는 Ping Scan이나 Port Scan의 경우에 침입죄에 대한 실행의 착수로 인

3. 허용된 접근권한을 초과한 경우

서비스제공자가 허용한 접근권한을 초과하여 접근한 경우를 의미한다. 예를 들면 서비스제공자가 A, B의 서비스를 제공하면서 일반회원에게는 A서비스만을 제공하고, 특별회원에게는 A, B 서비스를 모두 제공하는 경우, 일반회원인 이용자에게 허용된 접근권한은 A서비스뿐이므로 일반회원인 이용자가 B서비스에 접근하는 것은 허용한 접근권한을 초과하는 것이 된다.[52] 이용자로부터 특정범위의 사용승낙을 받은 후 제3자가 그 범위를 넘어 사용한 경우도 이에 해당한다. 하지만, 이용자가 제3자에게 자신의 아이디와 비밀번호를 알려주며 사용을 승낙하여 정보통신망을 사용하도록 한 경우라 하더라도, 제3자의 사용이 이용자의 의도에 따라 이용자의 이익을 위하여 사용되는 경우와 같이 사회통념상 이용자가 직접 사용하는 것이라고 볼 수 있는 경우 등을 제외하고는 원칙적으로 제3자에게는 정당한 접근권한이 없다고 보는 것이 상당하다.[53] 이에 따라 대법원 2007.10.12, 선고 2007도4450 판결에 따르면 갑이 A와 교제하면서 A에게 갑의 아이디와 비밀번호를 알려주면서 메일 등에 접속하여 갑이 A에게 남긴 이메일을 읽어 볼 수 있도록 하였으나, A가 때때로 갑이 자신에게 남긴 이메일이 아니라 제3자에게 보낸 이메일까지 함부로 읽어 보았고, 이 때문에 갑과 다툰 후 아이디와 비밀번호를 변경하여 A의 접속을 막아 이메일을 볼 수 없게 하였지만, 갑의 비밀번호가 변경되었음에도 불구하고 우연히 조합하여 알게 된 비밀번호로 메일에 접속하여 갑의 이메일을 읽어 본 사안에 대하여 A의 행위는 정보통신망법 제48조 제1항이 규정하고 있는 정당한 접근권한없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하는 행위에 해당된다고 하였다.[54] 이외에도 동사무소에서 상근예비역으로 근무하는 피고인이 예비군 관리업무를 담당하면서 담당직원의

정하여 미수범으로 처벌할 수 있는지, 아니면 예비행위에 해당하는지에 대한 논의가 필요하다.

52) 이범균, 앞의 논문, 622면.

53) 대법원 2005.11.25, 2005도870 판결 참고

54) 대법원 2007년 10월 12일, 2007도4450; 이 사건은 갑이 A를 정보통신망법위반으로 고소를 한 것에 대하여 A가 무고죄로 다시 고소한 것이다. 법원은 A의 행위를 정보통신망법위반으로 파악함에 따라 갑의 행위는 무고죄의 성립을 부정하였다.

아이디와 비밀번호로 행정자치부 주민전산망시스템에 접속할 수 있음을 기화로, 함부로 접속하여 청소년성범죄자들의 주민등록번호와 주소를 알아낸 경우,[55] 이용자로부터 아이디를 사용하여 게임을 하는 것만을 승낙받고는 그 허락범위를 넘어 당해 게임아이템을 임의로 자신의 캐릭터로 옮긴 경우[56] 등이 권한을 남용한 경우에 해당한다.

Ⅳ. 특수형태의 해킹기법에 대한 형법적용의 한계

1. IP 스푸핑 (IP Spoofing)

IP스푸핑은 해커가 악용하고자 하는 호스트의 IP어드레스를 바꾸어서 이를 통해 해킹을 하는 것을 말한다. 정보통신시스템에서 상호 신뢰관계에 있는 A, B 두 시스템간에는 A시스템의 어카우트를 가지고 B시스템에 엑서스할 수 있다. 이는 네트워크에서 신뢰관계를 형성하는 서비스가 네트워크 주소에 기반하여 이를 인증하기 때문이다. 이때 IP스푸핑은 신뢰관계에 있는 두 시스템사이에서 해커의 호스트를 마치 하나의 신뢰관계에 있는 호스트인 것처럼 속이는 것이다. TCP와 UDP서비스는 호스트의 IP주소가 유효하다고 가정하고 주소를 신뢰한다. 이때 해커의 호스트는 IP소스 라우팅을 사용하여 신뢰받는 호스트나 클라이언트로 변장할 수 있다. 해커는 목적지의 길을 지정할 수 있으며, 원래 위치로 돌아오는 길도 지정할 수 있다. 결국 해커는 진짜 호스트로 갈 패킷을 만나지 않고도 전송을 가로채거나 수정할 수 있다.

이와 같이 IP스푸핑의 경우 특정서버에 '침입' 또는 '침입시도'할 것을 전제로 한 현행법의 적용을 피할 가능성이 높다. 위에서 살펴본 바와 같이 IP스푸핑의 경우 외부에서 특정서버로 침입하는 것이 아니며, 일종의 전송되는 정보를 중간에 가로채기에 해당하기 때문이다. 또한 클라이언트 스푸핑의 경우 내부사람만이 보호된 네트워크내의 종료된 컴퓨터가 어떤

55) 서울지법 2003.4.4. 선고 2002고단12011 판결(이범균, 앞의 논문, 619면에서 재인용).
56) 부산지법 2004.8.24, 선고 2004고단3011 판결(이범균, 앞의 논문, 619면에서 재인용).

것인지를 알 것이기 때문에 공격은 외부로부터의 공격이 아니라 '내부'공격이라고도 볼 수 있기 때문이다. 따라서 현행법상 스푸핑의 경우 예비죄 처벌규정이 없는 한 불가벌적 행위에 해당한다.

2. 스니핑 (Sniffing)

냄새를 맡다라는 Sniff의 단어의미에서 알 수 있듯이 스니퍼는 컴퓨터 네트워크상에 흘러 다니는 트래픽을 엿듣는 도청장치를 말하며, 스니핑은 이러한 스니퍼를 이용하여 네트워크상의 데어터를 도청하는 행위를 말한다. 이러한 스니핑 공격은 웹호스팅, 인터넷데이터센터(IDC) 등과 같이 여러 업체가 같은 네트워크를 공유하는 환경에서는 매우 위협적인 공격기법이다. 하나의 시스템이 공격당하게 되면 그 시스템을 이용하여 네트워크를 도청하게 되고, 다른 시스템의 이용자의 ID와 Password를 알 수 있기 때문이다.[57] 패킷이 송수신되는 과정에서 여러 라우터를 거쳐 가게 되는데, 중간 ISP 라우터에 접근권한을 가진 사람이라면 암호화되지 않은 패킷을 쉽게 잡아낼 수 있다.

스니핑 역시 스푸핑과 마찬가지로 외부에서 침입이라고 보기 어렵다. 이는 전화에 비유를 한다면 전화중계기에 도청장치를 설치하는 것을 의미하며, 이 경우 직접 해당 서버에 침입하는 것은 아니기 때문이다. 따라서 침입을 전제로 하는 정보통신망법의 적용을 피할 가능성이 높기 때문에 처벌하지 못하는 흠결이 있을 수 있다.[58] 하지만 패킷이 송수신되는 과정에서 중간 라우터에 접근권한을 가진 사람이 스니핑을 하는 경우에는 정당한 접근권한을 가진 경우에 해당하지만, 접근권한을 남용한 경우에 해당한다고 볼 수 있다.

이에 대하여 독일형법 제202조b 데이터불법취득죄를 신설하여, 비공개 데이터전송으로부터 또는 데이터처리장치에서 방출되는 전자파로부터 행

57) 네트워크 설정을 통하여 스니핑을 어렵게 하는 여러 가지 방법중에 가장 좋은 방법은 데이터를 암호화하는 것이다. 데이터를 암호화하게 되면 스니핑을 하더라도 그 내용을 볼 수 없기 때문이다. SSL, PGP 등 인터넷ㅂ안을 위한 많은 암호화 프로토콜이 존재한다(참고 http://www.modssl.org).

58) Klaus Malek, Strafsachen im Internet. Rn. 163; Daniel Schnabl, Strafbarkeit des Hacking - Begriff und Meinungsstand, wistra 2004, 211,212.

위자에게 특정되지 아니한 데이터를 기술적 수단을 사용하여 권한없이 취득하거나 다른 사람으로 하여금 취득하게 한 경우에도 처벌한다. 이와 같은 입법규정은 형법상 전화대화의 도청과 녹음에 대응하는 규정이라고 볼 수 있는데, 우리 형법의 경우에도 도입의 필요성이 있다고 생각된다.

3. 서비스 거부공격(Denial of Service Attack; DoS) 또는 분산서비스공격(Distributed Denial of Service; DDoS)

서비스 거부공격(DoS)이란 일반적으로 공격자의 컴퓨터로부터 표적시스템과 그 시스템이 속한 네트워크의 과다한 데이터를 보냄으로써 시스템과 네트워크의 성능을 급격히 저하시켜 표적시스템에서 제공하는 서비스들을 인터넷 사용자들이 이를 이용하지 못하도록 하는 기법을 말한다.[59] 최근에 급격히 증가한 분산서비스공격(DDoS)은 주로 보안이 취약하고 유동IP를 사용하는 개인PC, 이른바 좀비PC를 숙주로 이용하는 특징이 있다.[60] 즉, 해커는 악성코드유포를 통해 개인PC중 보안장치가 허술한 해킹 경유지를 확보한 후 이른바 좀비PC를 통해 공격목표인 정보통신망에 공격명령을 내려 해당 공격 목표서버를 마비시킬뿐만 아니라 소속 기관의 내부 스위치, 라우터 등 네트워크 장비를 마비시킴으로써 각급 기관의 업무장애와 서비스마비 등을 초래한다.

서비스거부공격은 해킹의 한 기법으로 소개되고 있지만, 그 공격기술 내용을 살펴볼 경우에는 해킹관련범죄라기 보다는 형법 제314조 제2항의 컴퓨터업무방해죄를 적용하는 것이 타당하다고 생각된다. 서비스거부공격은 시스템이나 네트워크를 교란시켜 자원에 대한 정상서비스제공을 방해하거나 파괴시키는 것이기 때문이다. 일반적으로 해킹이라고 하면 권한획득을 위해 시스템에 침입하여 중요한 데이터를 가져가거나 시스템을 못쓰게 만드는 것을 의미하지만, 서비스거부공격은 시스템에 침입하지 않고 비정상적인 데이터를 지속적으로 보내 시스템자원을 고갈[61]시키거나 시

59) DoS공격에는 공격방법에 따라 SYN flooder attack, UDP flooder attack, ICMP flooder attack, Mail attack 등이 있다.

60) 최근 성인· 도박· 화상채팅 사이트를 대상으로 분산서비스거부(DDoS)라는 방법으로 돈을 요구하고 해킹 공격을 하는 사례가 잇따르고 있다고 한다.

스템을 파괴시키는 것을 의미하기 때문이다.

또한 정보통신망법 제48조 제3항, 제62조에 따르면 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내는 행위를 처벌하고 있는데, DoS공격 또는 DDoS공격[62]에 대한 직접적용이 가능한 법규정이라고 판단된다. 다만 소위 좀비PC로 이용되는 개인PC이용자의 경우에는 구성요건적 고의를 인정할 수 없기 때문에 처벌할 수 없으므로 이를 이용한 해커는 간접정범의 형태로 본죄를 범한 것으로 볼 수 있다.

4. Port Scan과 트로이목마

해커의 공격은 여러 단계에 걸쳐 이루어지는데 일반적으로 처음 행해지는 단계는 Port Scan이다. 해커는 정보통신망을 통해 자신이 공격하고자 하는 서버에 연속적으로 액세스하며, 보안상의 약점(세큐리티홀)을 찾는 Port Scan을 한다.[63] 포트스캔은 이 포트에 순차적으로 액서스하여 서버내에서 작동하고 있는 어플리케이션 소프트와 OS의 종류를 조사하여, 침입로가 될 수 있는 취약한 포트가 있는지를 조사하는 것이다. 포트스캔 결과, 세큐리티홀이 발견되면 침입용 프로그램을 사용해서 부정 침입이 이루어지는 경우가 많다.[64] 해커의 포트스캔행위는 정보통신망에 칩입하는 행위로 볼 수 없으며, 단지 공격서버에 침입을 하기 위하여 시도를 준비하는 예비행위에 해당한다. 해킹의 실행의 착수시점 또한 포트스캔의 결과 보안의 취약점이 발견된 후 침입용 프로그램을 설치하는 것을 실행의 착수시점으로 보아야 한다. 이에 대하여 예비죄를 처벌하는 규정이 없는 이상 현행법상 불가벌적 행위에 해당한다.[65] 트로이 목마[66]의 경우[67]에도 특정서버에

---

61) 이 공격은 cpu 사용율, 메모리나 파일시스템사용량 또는 프로세스와 같은 시스템자원을 고갈시켜 서비스를 못하도록 하는 방법이다.

62) DDoS 공격에 대한 독일형법의 적용에 대하여 분석한 문헌으로는 Jan Vetter, Gesetzeslücken bei der Internetkiminalität, S. 56ff.

63) 인터넷상에서 공개 된 서버 컴퓨터는 TCP/IP라고 하는 통신 규약(프로토콜)에 따라서 작동하고 있으며, 보통 포트라 불리는 접속 창구를 다수 준비하여 이용자로부터의 접속을 기다린다.

64) Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht, Rn. 688.

65) Rinker, MMR 2002, 663(665).

66) 트로이 목마(trojan horse)는 정상적인 기능을 할 것처럼 보이나 실제로 다른 기능을

대한 이용자의 접근권한에 대한 정당한 정보를 획득한 후 침입을 시도하기 때문에 침입을 위한 전단계에 해당하는 행위로서 침입에 해당하는 행위로 보기는 어려우며 예비행위에 해당한다고 볼 수 있다.[68]

5. 위험한 예비행위의 처벌필요성

2007년 8월 독일형법개정안은 EU의 사이버범죄방지조약[69]의 이행을 위하여 개정되었다. 개정안은 종전에는 처벌하지 않았던 컴퓨터관련범죄를 범죄화하고 있다. 주요내용은 추가적인 법익침해가 없는 단순해킹에 대하여 처벌할 수 있도록 종래의 제202조a를 개정하였으며, 데이터불법취득죄(제202조b)를 신설하여, 비공개 데이터의 전송으로부터 또는 데이터처리장치에서 방출되는 전자파로부터 행위자에게 특정되지 아니한 데이터를 기술적 수단을 사용하여 권한없이 취득한 경우와 다른 사람에게 취득한 경우에 처벌하고 있다. DoS공격과 같은 컴퓨터업무방해를 종전에는 기업이나 공공기관에 대한 침해만 처벌하였는데(제303조b), 뿐만 아니라 개인의 컴퓨터에도 적용하여 처벌하도록 함으로써 적용범위를 넓혀 개인의 데이터를 보호하고자 하였으며, 더 나아가 제202조c 데이터탐지및취득

하는 프로그램을 말하고 백도어(backdoor)는 시스템에 비인가된 접근을 가능하게 하는 프로그램을 말하는 것으로써, 트로이목마가 시스템의 불법적인 침입을 위한 백도어로 사용되기도 한다.

67) 공격자는 정상적인 login 기능을 하는 것 같은 패스워드 수집기(Password grabber)프로그램을 작성한다. 의심없는 사용자가 로그인 프롬프트(login :)를 보면 로그인하려고 하고, 프로그램은 정상적인 로그인 순서로 사용자가 평범한 방법으로 로그인하고 있다고 생각하게 한다. 하지만 트로이 목마를 가진 그 프로그램은 로그인 ID와 패스워드를 받으면 이 정보를 공격자 소유의 파일에 복사하거나 메일로 공격자에게 전송한다. 그리고 "login incorrect"라는 오류 메시지를 보낸다. 사용자는 자신이 잘못 입력하였다고 생각하고 로그인 ID와 패스워드를 다시 친다. 그 동안 트로이 목마를 가진 프로그램은 빠져 나오고 실제 login 프로그램에게 제어권을 넘겨 준다. 다음에 사용자는 성공적으로 로그인하게 되고 자신의 로그인 ID와 패스워드 정보가 유출되었다는 사실을 전혀 의심치 않는다.

68) Klaus Malek, Strafsachen im internet, Rn. 158.

69) 유럽이사회의 사이버범죄방지조약(ETS-Nummer 185)은 2001년 11월 회원국에 의해 서명되고, 2004년 7월 1일부로 발효되었다. 또한 유럽연합의 정보시스템의 공격에 대한 기본결정(ABI, EU Nr. L 69 S.67)은 유럽연합 계약 IV의 규정에 근거하여 2005년 2월 24일 마련되었다. 이에 따라 독일은 컴퓨터범좌와 관련된 형법규정을 개정하게 되었고, 이 개정법은 연방의회의 의결을 거쳐 2007년 8월 11일부터 발효되었다.

의 예비죄를 신설하여, 이러한 IT범죄에 대한 위험한 예비행위라고 볼 수 있는 해킹툴과 같은 디바이스의 남용을 형사처벌하고 있다. 특히 범죄행위에 사용가능한 보안도구의 유통, 판매, 소유 모두 불법으로 간주하고 있는 점을 주목할 수 있다. 제202조c는 데이터의 접근을 가능하게 하는 패스워드 또는 보안코드, 컴퓨터프로그램에 해당하는 것을 제작・취득하거나, 타인으로 하여금 취득하게 하거나, 판매・양도・유포・접근가능하게 한 경우 처벌한다.[70]

이에 비하여 우리나라는 정보통신망법 제63조 제1항 제1호에서 정보통신망에 침입함으로써 성립하는 기수범을 처벌하고 있으며, 동조 제2항에서는 이에 대한 미수범만을 처벌하고 있을 뿐이다. 또한 동법 제62조 제4호에서는 악성프로그램을 전달 또는 유포한 자만을 처벌하고 있으며, 이에 대한 미수범처벌규정이 존재하지 않는다.

이미 설명한바와 같이 해킹프로그램은 그 자체로서 악성프로그램의 성격을 가지고 있으며, 해킹프로그램과 악성프로그램이 결합화・복합화되는 현상으로 인하여 구별이 어려워지고 있으며, 해킹프로그램이 반드시 정보통신망에 직접적으로 사용되지 않을 수 있으며, 해킹프로그램과 웜 또는 바이러스 등이 결합된 새로운 형태의 기법이 등장한다는 점을 고려한다면 이에 대한 해킹관련프로그램을 제작하는 행위 또한 형사정책적 관점에서 처벌할 필요성이 있다고 생각한다. 해킹툴은 그 제작방식에 따라 이미 불법목적에 기여할 것을 목표로 하고 있다는 점도 고려되어야 할 것이다. 다만 정보통신망을 운영하는 보안전문가들이 관련프로그램을 제작, 사용할 수 있기 때문에 범죄에 이용할 목적이라는 목적범 형태로 입법하는 것이 타당하다고 판단된다. 또한 포트스캔등과 같은 침입을 시도하는 행위를 통하여 획득한 특정서버에 대한 보안취약성이나 버그를 의도적으로 유출하는 행위 또한 위험한 예비행위로 처벌할 필요성이 있다.

---

70) 사이버범죄방지조약 제6조 제1항 a Nr. ii에 따르면 각 회원국은 최소한 컴퓨터패스워드, 접속코드, 그 밖의 컴퓨터시스템 전체 또는 그 시스템의 일부에 접근할 수 있는 데이터를 제조・판매・사용목적의 취득・수입・유포 기타 그 밖의 처분행위를 범죄로 해야 한다고 규정하고 있다. 이에 따라 독일형법이 개정된 것이다.

Ⅴ. 결 론

IT기술의 발전에 따라 새로운 해킹기법의 등장은 형사법영역에서도 새로운 과제를 안겨 준다. 해킹과 같은 정보통신망침입범죄나 바이러스와 같은 악성프로그램을 유포하는 대표적인 사이버범죄들에 대해서 형사법규범은 어느 정도 존재하고 있지만, 그 범죄구성요건을 살펴볼 때 IT기술의 발전에 따라 등장하는 새로운 형태의 해킹기법이 출현하고 있음에도 불구하고 형사법의 도그마틱은 이러한 변화에 적절히 대응하지 못하고 있다. 따라서 IT기술의 발전에 따라 새로이 등장한 해킹공격기법에 대하여 형사법규범이 적절하게 대응하고 있는지를 살펴볼 필요가 있다. 특히 해킹행위와 바이러스유포행위의 경계선이 모호해지고 결합되어 가는 것에 대하여 규범적 적응가능성에 대한 논의가 필요할 것이다.

먼저 해킹과 관련된 형법의 비밀침해죄, 정보통신망법, 전자기록손괴죄의 성립여부, 단순해킹과 관련되어 정보통신망법의 해석을 통한 적용가능성을 논의한 결과, 비교적 단순한 형태의 해킹기법에 대해서는 처벌가능성이 인정될 수 있지만, IP스푸핑, 스니핑, 서비스거부공격, Port Scan과 트로이목마와 같은 특수한 형태의 해킹기법에 대해서는 형법적용의 한계가 있다는 점이 발견된다. IP스푸핑과 스니핑의 경우 특정서버를 침입할 것을 전제로 한 현행법의 적용을 피할 가능성이 높으며, 예비죄 처벌규정이 없는 한 불가벌적 행위라고 볼 수 밖에 없다. 또한 서비스분산거부공격의 경우 해킹관련범죄라기보다는 공격의 특성상 컴퓨터업무방해죄로 파악하는 것이 타당하다.

최근 독일형법 제202조c에서 데이터탐지및취득의 예비죄를 신설하여, 이러한 IT범죄에 대한 위험한 예비행위라고 볼 수 있는 해킹툴과 같은 디바이스의 남용을 형사처벌하고 있다. 제202조c는 데이터의 접근을 가능하게 하는 패스워드 또는 보안코드, 이러한 범죄목적을 가진 컴퓨터프로그램에 해당하는 것을 제작 · 취득하거나, 타인으로 하여금 취득하게 하거나, 판매 · 양도 · 유포 · 접근가능하게 한 경우 처벌한다. 해킹툴을 제작하는 행위와 같이 일정한 범죄를 목적으로 하는 행위는 단순한 제작에 그치는 것이 아니라 인터넷을 통한 유포의 가능성, 실행가능성을 고려한다면

이는 위험한 예비행위에 해당할 수 있다. 뿐만 아니라 악성코드를 유포하는 것이 해킹을 위한 사전적 준비행위에 해당한다는 점, 악성코드와 해킹툴의 구별이 어려워지는 점을 고려한다면 해킹관련 범죄에 대하여 예비죄처벌의 필요성을 더욱 커진다. 법규범의 적용가능성을 해석을 통하여 점검해보는 것은 너무나 당연한 작업일 것이지만, 이러한 법규범의 적용가능성이 불가능하다면 새로운 입법을 통해서 해결하는 것이 옳다고 판단된다. 이에 최근에 개정된 독일형법에서 해킹관련범죄에 대한 예비죄신설은 우리 형사입법에서도 고려될 필요성이 있다고 판단된다.

이제 정보화사회에서 유비쿼터스사회로 넘어가는 시점에 있는 우리나라의 경우 새로운 형태의 사이버범죄가 등장할 것이라는 예상은 충분히 할 수 있다. 정보화시대의 진전을 뒷받침하는 IT기술의 급속한 성장·발전 속도에 따라 형사법규범 또한 다양화・전략화를 모색해야 한다.

참고문헌

이상돈, 해킹의 범죄화, 윤리경영과 형법, 2005.

강동범, 사이버범죄와 형사법적 대책, 형사정책연구 제11권 제2호(통권 제42호, 2000? 여름호).

강동욱, 정보통신망이용에 있어서 개인정보보호를 위한 형사법적 대응방안에 대한 고찰, 인권과 정의, 1999.12.

김일수/배종대/이상돈, 정보화사회에 대비한 형사법적 대응, 비교형사법연구 제3권 제2호. 2001.12.

류석준, 해킹에 대한 규제법규에 관한 연구, 비교형사법연구 제6권 제2호. 2004.12.

박희영, 단순해킹의 가벌성에 관한 비교법적 연구, 인터넷법률 통권 제34호, 2006.3.

박희형, 독일의 컴퓨터범죄방지에 관한 개정 형법의 분석 및 평가, 인터넷법률 통권 제40호, 2007.10.

백광훈, 해킹범죄와 그 처벌법규 및 문제점, 2000.12.6 제4회 해킹방지워크샵 발표문.

백광훈, 사이버테러리즘에 관한 연구, 형사정책연구원, 2001.
백광훈, 인터넷을 이용한 범죄의 유형과 처벌법규, 범죄방지포럼, 2003.
이범균, 대법원 2005. 11. 25. 선고 2005도870 판결, 대법원판례해설, 제59호.
유인모, 정보형법의 과제와 전망, 형사정책 제12권 제1호, 2000.6.
유용봉, 인터넷범죄와 형법, 21세기사, 2005.
전지연, 전자적 정보의 형사법적 보호에 관한 연구, 한림법학 FORUM 제8권, 1999.
정보홍외 2명, 『침입방지 시스템의 기술 및 전망』, 한국정보보호산업협회, 2003, (kidbs.itfind.or.kr:8888/WZIN/jugidong/1098/109801.htm).
최영호, 정보범죄의 현황과 제도적 대처방안, 형사정책연구원, 1998.
한국정보보호학회, 『차세대 네트워크 보안기술』, 한국정보보호진흥원, 2002.
한국정보보호진흥원, 2006 정보시스템 해킹 · 바이러스 현황 및 대응, 2006.12.
Annette Marberth-Kubicki, Computer- und Internetstrafrecht, C.H.Beck, 2004.
David S. Wall, Crime ahd the Internet, Routledge, 2001.
Daniel Schnabl, Strafbarkeit des Hacking - Begriff und Meinungsstand, wistra 2004.
Eric Hilgendorf, Die Neuen Medien und das Strafrecht, ZStW, 2001, S. 650.
Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht, Springer, 2005.
Jan Vetter, Gesetzeslücken bei der Internetkiminalität, Diss. Stuttgart. 2002
Klaus Malek, Strafsachen im internet, C.F.Müller, 2005.
Kindhäuser/Neumann/Paeffgen, Nomos Kommentar StGB, 2.Aufl.

Loopholes in Criminal Law to New Types of Hacking Attacks

Choi, Hojin
(Professor, Department of Law, Dankook University,
Ph. D. in Law)

Computer and the Internet make many activities easier for us. They also make illegal activities easier for criminals. Hacking, or intentional unauthorized access to computer systems, is a whole new category that includes a wide range of illegal activities from harmless pranks to huge thefts and shutdown of important services. In this paper, the problem related Hacking through the interpretation theory of criminal law are discussed. Argue about many aspects of hacking is important because hacking is the principal part of cyber crimes.

Unauthorized access to especially secure data is to be a crime not only security measures were cracked but also security measures were not cracked. Almost major Web sites were shut down by denial-of-service. Denial-of-service attacks are also now a crime. in this kind of attack, hakers overload target site with requests for Web pages and other information. The procurement of data from data transmissions or electromagnetic radiation emmitted from data processing system is punishalbe by Law. Furthermore, there is need to criminalize that especially dangerous preparations for such IT crimes are also punishable by law. In particular, creating, propagating, and procuring hacker tools designed to perform a legal actions now falls like Section 202c of the revised German Penal Code. There is need to criminalize that the somebody disclosure security vulnerabilities intentionally. Criminal Law have to cover the modern threats and up to a certain degree they are open for new technical developments. Law

are more technologically up-to-date.

주제어 : 해킹, 사이버범죄, 스푸핑, 스니핑, 서비스 거부공격, 무권한접근, 보호조치, 인터넷범죄, 데이터탐지죄, 컴퓨터업무방해

Keywords : Hacking, Cyber Crimes, Sniffing, Denial of Service Attack; DoS, Unauthorized access, Security measures. Internet Crimes, Computer sabotage