해킹행위에 의한 게임아이템 불법취득과 형사법적 규제

- 해킹사례를 중심으로 -

강 철 하* 강 승 훈*

차 례

Ⅰ. 서 설

게임 제작기술 발전 및 정보통신망 고도화에 따라 PC 게임, 아케이드 게임, 콘솔게임, 온라인게임 등 다양한 유형의 게임이 온라인·오프라인을 통해 선보이고 있고 남녀노소를 불문하고 그 이용이 확대되고 있다. 그 중 최근 온라인게임인 '다중접속온라인역할수행게임(Massively Mutiplayer Online Role Playing Game, MMORPG)[1]'의 이용이 늘어

* 동국대 경찰행정학과 부교수, 법학박사
* 경찰청 사이버테러대응센터 연구원(법학석사)
** 경찰청 사이버테러대응센터 연구원(컴퓨터공학 박사과정)

1) MMORPG는 다수의 게임 이용자가 동시접속하여 User-ISP간 또는 User-User간의 상호작용을 통해 게임을 진행시킨다는 Hardware적 특성과 안정적 사이버 공간에서 사이버 자아를 성장·발전시키는 등 게임 전개를 개방적으로 설계하는 Software적 특성을 가지고 있다; [이춘수(2007), 인터넷상의 재산권, 과학기술의 발전과 사법의 대응(서울대학교 세미나 자료집), p. 93]. 현재 국내에 운영 중인 MMORPG

나는 가운데 가상의 게임상에서 유통되는 게임아이템[2] 및 게임머니가 실제로 현실 세계에서 거래되고 있는 실정이고, 더욱이 이러한 아이템 현금거래 행위에 수반하여 아이템 사기, 개인정보 도용, 업무방해 등 다양한 형태의 불법행위가 발생하고 있어 사회적 문제를 야기하고 있다.

그런데 이러한 아이템 현금거래를 둘러싸고 발생하고 있는 다양한 범죄에 대처하기 위해서는 명확한 법적 근거가 존재해야 함에도 실제에 있어서 처벌근거가 부존재하거나 존재하더라도 그 해석상의 모호함으로 인해 수사기관이 적절히 대처하지 못하고 있는 실정이다. 다만, 최근 음반·비디오물 및 게임물에 관한 법률의 분법화 과정을 거쳐 '게임산업진흥에 관한 법률'이 제정됨에 따라 그 동안 게임아이템 불법거래행위에 대한 직접적인 규제 장치의 공백을 메우고 있기는 하지만 동 법은 적용범위의 한정성으로 인해 일정한 내재적 한계를 가지고 있다는 점에서 게임아이템 거래를 둘러싸고 발생되는 다양한 범죄에 대처하기 힘들다고 본다.[3]

더욱이 정보화의 진전에 따라 타인의 게임아이템 탈취 유형도 종래의 '게임 아이템 사기' 이외에 '해킹기법을 이용한 게임아이템 취득방식' 등 고도화된 기술을 이용한 범죄사례가 발견되고 있으며 이러한 해킹기법 사용은 부수적으로 정보통신망에 대한 장애를 발생시켜 업무상·재산상 피해를 주고 있기도 하다. 이런 이유로 해킹기법을 이용한 게

로는 리니지, 리니지Ⅱ, 라그나로크, 뮤 등이 있다.

2) 게임 아이템(item)이란, 통상 온라인 게임상의 '가상재산(virtual property)'으로 게임 이용자의 분신인 '아바타'가 사용하는 칼, 방패, 망토 등을 의미한다. 게임아이템의 성질에 관한 자세한 내용은 홍승희, "정보재산권의 형법적 보호", 형사정책연구원(2005년도 춘계 형사정책세미나 자료집), pp. 123-6 참조

3) 예컨대, 게임산업진흥에 관한 법률에서는 '누구든지 게임물의 이용을 통하여 획득한 유·무형의 결과물(점수, 경품, 게임 내에서 사용되는 가상의 화폐로서 대통령령이 정하는 게임머니 및 대통령령이 정하는 이와 유사한 것을 말한다)을 환전 또는 환전 알선하거나 재매입을 업으로 하는 행위'를 금지하면서(동법 제32조 제1항 제7호) 동법 시행령 제18조의3에서 "대통령령이 정하는 게임머니 및 대통령령이 정하는 이와 유사한 것"을 게임물을 이용할 때 베팅 또는 배당의 수단이 되거나 우연적인 방법으로 획득된 게임머니(제1호), 제1호에서 정하는 게임머니의 대체 교환 대상이 된 게임머니 또는 게임아이템 등의 데이터(제2호), 게임제작업자의 컴퓨터프로그램을 복제, 개작, 해킹 등을 하거나 게임물의 비정상적인 이용을 통하여 생산·획득한 게임머니 또는 게임아이템 등의 데이터(제3호)로 한정하였기 때문에 결국 위 시행령 제18조의3 각 호에서 정하는 게임머니나 게임아이템이 아닌 것은 동법으로 처벌할 수 없을 뿐만 아니라 설사 시행령 제18조의3 각 호에 해당한다고 하더라도 동법 제32조 제1항 제7호에 따라 환전업, 환전 알선업 또는 재매입업이 아닌 개인간 거래행위에 대해서는 여전히 처벌할 수 없다는 문제점이 발생한다.

임아이템 불법취득행위에 대한 법적 규제가 필요하다는 목소리가 높아지고 있지만 실제로 그러한 불법행위를 처벌할 법적 근거가 형법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'으로 약칭한다) 등 개별 법률로 산재해 있을 뿐만 아니라 그 구성요건의 '포괄성 및 애매성'으로 인해 구체적인 해킹사례에의 적용이 쉽지 않은 것도 사실이다.

따라서, 본 논문에서는 최근 게임아이템 취득을 위해 사용되고 있는 해킹기법에 대한 실제적인 분석 작업과 함께 각 해킹행위 단계별로 현행 법체계 내에서의 형사 처벌가능성을 구체화하는 한편, 그 과정에서 제기되는 '게임아이템의 법적 성질 문제'를 규명하여 해킹기법을 이용한 게임아이템 불법취득 행위에 대한 형사법적 대응 해법을 제시해 보고자 한다.

Ⅱ. 게임아이템 불법취득 해킹모델

우선 게임 아이템 취득을 위해 동원되는 해킹기법으로는 크게 게임 이용자를 공격하는 방법과 온라인 게임 회사를 공격하는 방법으로 분류할 수 있다. 이 중 빈번하게 일어나는 경우는 이용자를 공격하는 방법으로 악성프로그램의 유포를 통해 이용자의 게임계정 탈취 및 게임아이템을 불법 취득한다는 점에서 그 위험성이 높다고 하겠다. 더욱이 이러한 공격은 불특정 다수를 대상으로 일상적인 인터넷 사용만으로도 계정을 탈취하기 때문에 그 피해 여파는 상당히 광범위하게 나타날 수 있다. 따라서 이하에서는 온라인게임을 이용하는 불특정 다수인을 대상으로 한 해킹기법과 온라인게임 회사를 대상으로 한 해킹기법에 대해 구체적으로 분석해 보고 기타 이와 관련된 최근의 해킹 사례를 검토해 보도록 하겠다.

1. 해킹모델A - 게임 이용자 공격기법

전술한 불특정 다수의 컴퓨터를 해킹하여 아이템을 탈취하는 해킹기법은 우리가 인터

넷을 사용하는 일상적인 활동과 연관되어 있다. 대표적인 사례로 웹사이트를 방문하는 것만으로도 악성프로그램에 감염되는 경우를 들 수 있는데, <그림 2-1>을 보면 공격자는 게임 계정을 탈취하기 위해 우선 포털사이트 등 타인의 웹사이트를 해킹한다. 주로 웹 취약점 공격 및 SQL injection[4] 해킹기법 등을 사용하여 사용자들이 많이 사용하는 포털사이트를 해킹한 후 사용자가 접근하면 자동적으로 악성 프로그램이 설치될 수 있도록 웹 사이트를 조작한다. 이 경우 공격자는 웹사이트에서 사용할 수 있는 iframe[5] 취약점을 이용하거나 사이트의 신뢰성을 기반으로 위장한 ActiveX[6]를 이용하여 악성 프로그램이 설치되게 조작한다. 이 후 불특정 다수의 사용자가 웹 사이트에 접속하게 되면 이용자 개인 컴퓨터에 악성 프로그램이 설치가 됨으로써 컴퓨터의 보안장치가 무력화된다. 나아가 이 처럼 악성 프로그램이 설치된 것만으로 클라이언트 컴퓨터의 보안설정 및 접근제어는 무력화되고 악성 프로그램을 감지하기 위한 백신 프로그램마저 무력화시키기도 한다. 그런데 이용자 컴퓨터에 설치된 악성 프로그램은 온라인게임 이용자가 게임 사이트 등으로 접근하기를 기다리게 되고 이용자가 게임 사이트에 접속하여 아이디와 비밀번호를 입력하게 되면 악성프로그램은 이용자의 컴퓨터에 있는 메모리에서 키보드 입력 정보를 탈취하여 저장한다. 이러한 악성프로그램의 기능을 'Keylogger'라고 하는데 이는 키보드로 입력한 정보가 메모리로 올라가 있는 때에 메모리에서 정보를 탈취하는 기법[7]으로 통상 키보드 정보들을 특정 파일에 기록하여 보관하거나 악성 프로그램의 메모리에 저장하는 형태를 취하고 이렇게 저장된 정보들은 추후 악성프로그램이 이용자

---

4) 웹 클라이언트의 반환 메시지를 이용하여 불법 인증 및 정보를 유출하는 공격. 웹 응용 프로그램에 강제로 구조화 조회 언어(SQL) 구문을 삽입하여 내부 데이터베이스(DB) 서버의 데이터를 유출 및 변조하고 관리자 인증을 우회할 수도 있다. 이 공격은 MS SQL 서버뿐만 아니라 모든 관계형 데이터베이스 관리 시스템(RDBMS)에서 가능하다.

5) 하이퍼텍스트 생성 언어 HTML 문서에서 글 중의 임의 위치에 또 다른 HTML 문서를 보여 주는 내부 프레임(inline frame) 태그로 그림 파일을 문서에 포함시키는 것과 유사하며 넷스케이프에서는 동작하지 않는다. 네이버 백과사전(http://terms.naver.com/search.naver?query=iframe, 2007. 10. 22. 방문) 참조.

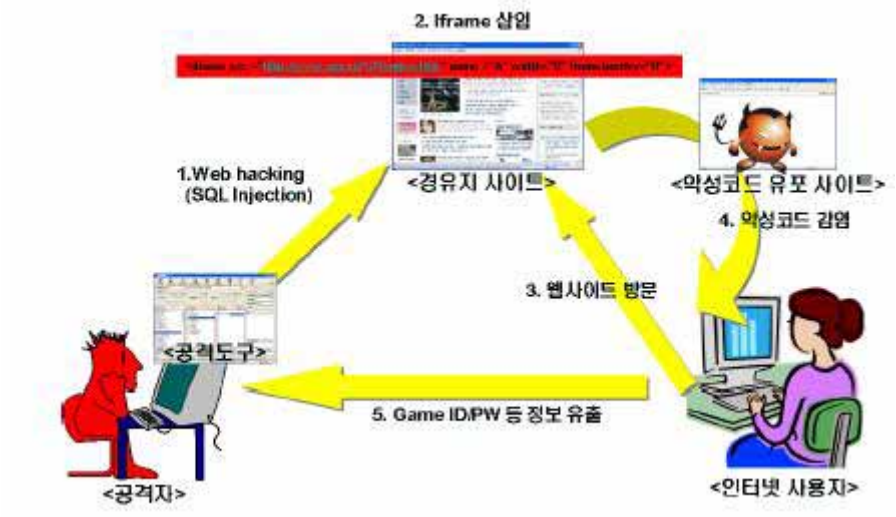
6) 윈도 사용자들이 인터넷을 쉽고 편리하게 이용하도록 마이크로소프트사에서 개발한 것으로, 기존의 응용 프로그램으로 작성된 문서 등을 웹과 연결시켜 그대로 사용할 수 있게 하는 기술.

7) Cormac Herley, Dinei Florencio(2006). How To Login From an Internet Cafe Without Worrying About Keyloggers, The proceedings of Simposium on Usable Privacy and Security.

모르게 공격자에게 이메일로 전송하거나 공격자가 준비해 놓은 사이트로 전송함으로써 공격은 성공한다.

이 후 공격자는 수집된 타인 계정 정보를 이용하여 게임사이트에 접속하고 타인 계정에 등록되어 있는 아이템 등을 공격자가 준비한 다른 계정으로 넘겨줌으로써 아이템을 탈취하게 된다. 또한 공격자는 아이템을 탈취한 후에도 게임아이템을 탈취당한 이용자가 계정을 사용하는 것을 지연하거나 단념케 하기 위해 계정의 비밀번호를 변경하는 등 악의적인 행위를 하기도 한다.

<그림 2-1> 웹사이트를 통한 악성 프로그램 감염



"금융권 사이트, 웹해킹 대비에 사활걸어라!", 보안뉴스 2006. 1. 12.자에서 발췌

2. 해킹모델B - 게임 회사를 대상으로 한 공격기법

인터넷을 매개로 하여 온라인 게임서비스를 제공하기 위해서는 다수의 게임이용자들이 접속할 수 있는 운영 Server가 필요하다. 따라서 게임회사는 이러한 운영 Server를 여러 개 두고 게임 사용자들의 접속을 관리하고 Database Server와 연동하여 계정, 캐릭

터, 지도, 시나리오 등을 관리한다. 물론 게임아이템이나 사이버머니 기록은 여기 Database Server에 위치한다. 그런데 만약 공격자가 운영 Server, Database, 웹 Server, 기타 연동되는 System들의 취약점을 공격하여 침입에 성공한다면 Database에서 계정 정보 등을 탈취하고 특정 계정의 아이템 등을 조작하는 등 다양한 피해를 가할 수 있다.[8] 또한 이러한 공격으로 계정을 탈취할 경우 해당 계정들로 접속하여 아이템들을 탈취할 수 있을 뿐만아니라 직접 아이템을 조작할 경우에는 수많은 아이템을 만들어 낼 수도 있다. 만약 이러한 공격이 운영자가 인식하지 못하도록 은밀히 지속될 경우 게임 회사는 막대한 피해를 입게 될 것이다. 실제로 지난 2006년 국내 범죄조직과 결탁한 중국의 해커 집단은 포커게임 사이트 Server를 직접 해킹하고 그 운영 Server에서 게임머니를 조작하여 전국에 불법 유통시키는 등 59억여원의 부당이득을 취한 바 있다.

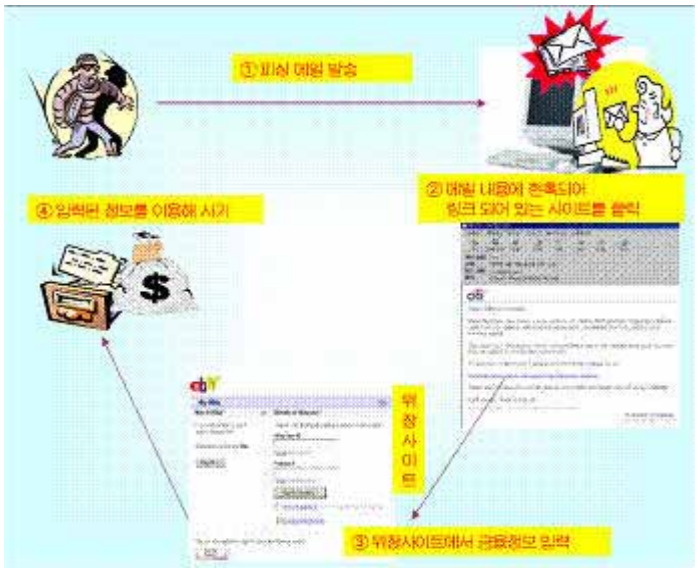
3. 해킹모델C - 피싱(Phishing)행위를 이용한 공격기법

그 동안 금융권에서는 피싱(Phishing)이란 기법이 금융 정보 및 금전을 탈취하기 위해 사용되어 왔다. 피싱은 개인정보를 의미하는 프라이버시(Privacy)와 낚시를 의미하는 피싱(Fishing)의 합성어로써 인터넷을 사용하는 일반 사용자들의 착각을 유발시켜 정보를 탈취하는 방법이다. 최근 이러한 인터넷 해킹 행위가 게임 이용자들을 대상으로 사용됨으로써 상대적으로 계정관리가 취약한 게임 사이트에 접속하는 다수의 이용자들이 자신의 게임계정 및 아이템들을 탈취당한 바 있다. 이러한 피싱(Phishing)행위를 이용한 공격기법을 <그림 2-2>의 순서로 자세히 살펴보면 우선 공격자는 불특정 다수 또는 게임을 사용하는 이용자들에게 이메일 등의 수단으로 게임과 관련된 관심정보를 발송한다. 통상 이러한 정보들은 온라인게임을 운영하는 회사에서 전달하는 이벤트 또는 새로운 뉴스와 같은 정보로 위장되어 발송되며 관심사항에 따라 이용자는 해당 온라인게임사이트로 연결하기 위해 이메일에 링크되어 있는 사이트로 접속하게 되는데 이 경우 실제로 연결된 사이트는 게임사이트가 아니라 공격자가 미리 만들어 놓은 위장사이트가 된다.

8) Meier, J.D.(2006). Web application security engineering, IEEE Security & Privacy Magazine.

그런데 이러한 사실을 모르는 이용자는 평소와 다름없이 그 위장사이트에 온라인게임 사이트 아이디와 비밀번호를 입력하여 접속을 시도하게 되며 이와 같이 접속정보를 입력하면 공격자의 위장사이트는 아이디와 비밀번호를 탈취하게 된다. 또한 이용자에게 접속 에러 메시지 등을 출력하면서 실제 게임회사가 운영하고 있는 사이트로 이동시켜 이용자가 비밀번호를 잘못 입력한 것처럼 착각하게 만든다.[9] 결국 공격자는 이렇게 획득한 게임계정을 이용하여 피해자의 게임아이템들을 앞의 해킹모델A와 같이 공격자 자신이 관리하고 있는 계정으로 넘겨 받게 된다.

<그림 2-2> 위조된 웹사이트를 이용한 피싱 기법



"피싱(Phishing) 위협 및 대응 방안", 정보통신연구진흥원 주간기술동향 1237호에서 발췌

9) Rachna Dhamija, J.D. Tygar, Marti Hearst(2006). Why phishing works, The proceedings of the Conference on Human Factors in Computing System (CHI2006).

Ⅲ. 형사법적 규제 가능성

전술한 해킹모델 유형에서 검토한 바와 같이 최근 게임아이템 불법취득을 위해 동원되는 해킹기법은 날로 지능화되어 가고 있고 이용자의 입장에서도 그 피해를 쉽게 인식할 수 없도록 그 수법도 교묘해지고 있다. 더욱이 이러한 해킹행위는 개인적 차원의 피해를 넘어 정보통신서비스의 안정적 제공을 저해·위협한다는 측면에서 법적 규제의 필요성이 제기된다. 다만, 본 연구에서는 법률검토 작업의 중복을 피하고 동시에 복잡한 법률문제를 내포하고 있으며 그 침해 위험성이 높은 '해킹모델A'를 중심으로 법적 검토를 진전시켜 보도록 하겠다.

따라서 이하에서는 '해킹모델A를 이용한 게임아이템 취득'과 관련된 일련의 과정, 즉 ⅰ) 포털사이트를 해킹한 후 이용자가 접근하면 자동적으로 악성프로그램을 설치하도록 조작한 행위 ⅱ) 이러한 해킹을 통해 획득한 아이디·비밀번호로 온라인게임사이트에 접속한 행위 ⅲ) 게임사이트에 접속한 후 타인의 게임계정에 속해 있는 아이템을 자신의 계정으로 이전한 행위 및 ⅳ) 타인의 아이템을 취득한 후 비밀번호를 변경하는 등 온라인게임사이트 이용자의 접속정보를 변경한 행위에 대한 형사법적 규제가능성을 단계적으로 검토해 보고자 한다.

1. 포털사이트를 해킹한 후 이용자가 접근하면 자동적으로 악성프로그램을 설치하도록 조작한 행위

해킹모델A에서와 같이 게임아이템 취득을 위한 전단계로서 인터넷 포털사이트를 공격하여 포털사이트 이용자가 당해 웹사이트에 접속할 경우 자동적으로 그 이용자의 컴퓨터에 악성프로그램이 설치되도록 한 행위에 대하여 현행법 체계 내에서 어떠한 형사법적 규제가 가능한지 문제된다. 즉 포털사이트를 사용하는 이용자의 컴퓨터로 악성프로그램을 설치하도록 조작한 행위가 포털사이트와의 관계에서 '컴퓨터업무방해'에 해당하는지 여부와 이용자의 컴퓨터로 악성프로그램을 유포한 행위가 정보통신망법 제62조 제4호

위반죄(악성프로그램 전달・유포죄)에 해당되는지 문제된다.

가. 컴퓨터 업무방해죄 성립여부

(1) 컴퓨터 업무방해죄는 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해함으로써 성립하는 범죄이다(형법 제314조 제2항).[10] 그런데 여기서 '정보처리장치'란 정보의 저장・검색 등 정보처리능력을 '독자적으로 갖고 있는 시스템'을 의미한다고 해석하는 것이 바람직하고 이런 점에서 정보처리장치에 Hard ware 이외에 Soft ware를 포함하는 견해[11]는 타당하지 않은 것으로 보이며 오히려 Soft ware는 정보처리장치가 아니라 '전자기록 등 특수매체기록'에 해당된다고 해석된다.[12] 또한 본 죄의 '전자기록'은 전기적 또는 자기적 방식에 의해 저정된 기록을 의미하므로 컴퓨터 하드디스크, 램, IC카드 속의 기록은 전기적 방식을, 플로피디스크, 자기테이프 등에 의한 기록은 자기적 방식에 의한 것으로 이해할 수 있고 '특수매체기록'은 광기술을 이용한 기록(CD)으로 볼 수 있다.[13] 더불어, 본 죄가 성립하기 위해서는 이러한 ① 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 ② 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 ③ 기타 방법으로 정보처리에 장애를 발생하는 행위가 있어야 하며 ①의 행위를 '물리적 가해'라고 한다면 ②의 행위를 '논리적 가해'라고 이해할 수 있다. 또한 컴퓨터업무방해죄는 정보처리

10) 컴퓨터 업무방해죄는 컴퓨터사보타주를 규정한 것으로 이와 관련하여 최근 독일 형법 개정안에서는 제303조의b(Computersabotage)를 개정하면서 ⅰ) 일반적인 경우 제303조의a(Datenveränderung) 제1항의 범죄행위(컴퓨터 데이터를 위법하게 소거, 은닉, 사용불능케하거나 변작하는 행위) 또는 정보처리장치 또는 전산자료가 입력된 물체를 파괴, 손상, 사용불능, 제거 또는 변작하는 행위를 통해 타인의 중요한 정보처리를 현저히 방해한 자를 3년 이하의 징역 또는 벌금형에 처하도록 하였으며(제1항), ⅱ) 타인의 영업, 기업 또는 관청에 대하여 중요한 의미를 가지는 정보처리를 방해한 경우에는 5년 이하의 징역 또는 벌금에 처하는 기존의 제1항 규정을 제2항으로 옮겨 놓았다.

11) 배종대(2007), 형법각론, 홍문사, p. 305.

12) 같은 취지의 견해로 박상기(2002), 형법각론, 박영사, p. 213 참조.

13) 배종대, 앞의 책, p. 305.

에 장애를 발생하게 할 것을 필요로 하는 '결과범'이면서 업무라고 하는 법익에 대하여 침해의 위험이 있음으로 족한 '추상적 위험범'에 속한다.[14]

(2) 그런데 해킹모델A와 같이 포털사이트를 해킹한 후 이를 조작하여 인터넷 이용자가 당해 웹사이트를 방문하는 것만으로도 악성프로그램을 이용자의 컴퓨터에 자동설치되도록 한 행위는 ⅰ) 포털사이트의 정보처리장치에 진실에 반하는 정보를 입력하거나 주어서는 안 될 프로그램을 입력한 행위로 평가할 수 있으므로 본 죄에서 말하는 '허위의 정보 또는 부정한 명령을 입력'한 경우에 해당된다고 판단되고, ⅱ) 또한 당해 정보처리장치의 정상적인 기능을 수행하지 못하도록 조작하여 '정보처리장치에 장애를 발생'함과 동시에 ⅲ) 악성프로그램의 전달 등 기능조작을 통해 포털사이트로 하여금 이용자의 컴퓨터로 악성프로그램을 전달케 하여 포털사이트의 '안전성과 신뢰성'을 실추시키고 정상적인 서비스 제공 업무를 방해하였다는 점에서 해킹모델A의 행위자를 형법 제314조 제2항 컴퓨터 업무방해죄로 의율할 수 있을 것으로 판단된다.

나. 정보통신망법 제62조 제4호 위반죄 성립여부

(1) 최근 정보화의 진전에 따라 그 역기능으로 바이러스, 스파이웨어 등 악성프로그램이 인터넷 등 정보통신망을 통해 유포되거나 이용자의 컴퓨터에 은밀히 설치되는 등 민간부문, 공공부문을 막론하고 다양한 피해를 야기하고 있다.[15] 이에 따라 우리의 경우 형법, 정보통신망법 및 정보통신기반보호법상의 개별처벌규정을 통해 악성프로그램 유포 등 전자적 침해행위에 대한 입법적 대처를 하고 있다. 특히 현행 정보통신망법 제48조 제2항은 '정당한 사유없이 정보통신시스템, 데이터 또는

14) 임웅(2007), 형법각론, 법문사, p. 221.

15) 지금보다도 기능면에서 열악한 1988년 최초의 웜으로 알려져 있는 '모리스 웜(Morris Worm)'사건만 보더라도 악성프로그램의 파괴력과 그 위험성을 쉽게 이해할 수 있다. 예컨대 컴퓨터 공학 전공의 대학원생이었던 모리스가 인터넷 보안의 결함을 알리기 위해 자신이 고안한 웜을 배포하였는데 그 웜은 모리스 본인이 예상했던 것 보다도 훨씬 빠른 속도로 다른 컴퓨터를 감염시키고 대학, 군 관련 사이트, 의료연구기관 등 6,200개의 컴퓨터에 피해를 주었으며 그 수리비만 해도 9천 8백만 달러가 넘어가게 되어 결국 모리스는 유죄선고를 받게 되었다. Gerald R. Ferrera 외(2001), CyberLaw(Text and Cases), South-Western College Publishing(a division of Thomson Learning), pp. 297-8 참조.

프로그램 등을 훼손·멸실·변경·위조 또는 그 운용을 방해할 수 있는 프로그램을 전달 또는 유포하는 행위'를 금지하고 있는데 따라서 여기서의 '악성프로그램'이란 결국 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조 또는 그 운용을 방해할 수 있는 프로그램을 의미하는 것으로 이해할 수 있고 바이러스, 스파이웨어, 트로이목마, 웜 등이 이에 해당된다고 볼 것이다.

그런데, 해킹모델A와 같이 특정 웹사이트 접속시 '악성프로그램'이 이용자의 컴퓨터에 자동적으로 설치되도록 한 행위는 범죄의사가 없는 포털사업자의 웹사이트를 통해 이루어지고 있다는 점에서 '악성프로그램 전달·유포'의 결과를 해킹 행위자의 작품으로 평가할 수 있는지 문제된다. 그러나, 설사 악성프로그램 전달·유포의 결과가 이와 같이 포털사업자의 웹사이트를 통해 이루어지고 있다고 하더라도 이는 당해 포털사이트를 해킹한 행위자가 동 사이트를 자신의 지배영역 내에 둠으로써 마치 '도구'와 같이 사용하는 경우로 이해할 수 있으므로 결국 위 행위자 자신이 정보통신망법 제48조 제2항에서 말하는 '악성프로그램의 전달 또는 유포행위'를 하였다고 평가할 수 있다고 본다. 따라서 위 행위자는 정보통신망법 제62조 제4호 위반죄(악성프로그램 전달·유포죄)로 처벌될 것으로 판단된다.

(2) 그런데 위와 같은 정보통신망법 규정은 악성프로그램의 '전달 또는 유포하는 행위'만을 처벌할 뿐 그 이전 단계인 '악성프로그램의 제작행위'에 대한 어떠한 처벌 규정도 두지 않고 있다는 점에서 '악성프로그램 제작행위'에 대한 법적 평가를 어떻게 해야할지 문제된다. 이와 관련하여 최근 독일 형법 개정안 제202c조에서는 "데이터 탐지 및 탈취에 대한 준비(Vorbereiten des Aussphens und Abfangens von Date)"라는 제목으로 제202a조 또는 제202b조에 의한 범행을 위해 ⅰ) 정보에 접근을 가능하게 해 주는 비밀번호, 기타의 비밀코드 및 ⅱ) 이와같은 범행을 수행하기 위해 고안된 컴퓨터프로그램을 제작하거나 이를 자신 또는 타인을 위해 조달·판매하거나 또는 타인에게 전달시킨 자는 1년 이하의 징역 또는 벌금형에 처하도록 하고 있다. 물론, 우리의 경우 현 시점에서 악성프로그램의 제작행위에 관한 법적 처벌근거를 찾기 힘들기 때문에 현실적인 처벌은 어렵겠지만 ⅰ) 통상 제작된 바이러스, 웜 등 악성프로그램의 경우 엄청난 속도로 컴퓨터 시스템을 감염시키고

그 피해 또한 걷잡을 수 없이 확산된다는 점, ii) 일종의 예비단계로써 '악성프로그램을 제작하는 행위' 자체를 처벌하는 것이 과잉형벌에 해당할 수 있다는 발생가능한 비판은 독일의 경우와 같이 '범죄목적으로 제작한 경우'라는 일정한 제한을 통해 해소할 수 있다는 점에서 우리의 경우에도 '범죄목적으로 악성프로그램을 제작하는 행위'에 대한 처벌규정을 신설할 필요가 있다고 본다.

(3) 더불어 앞서 검토한 컴퓨터 업무방해죄와 악성프로그램 전달·유포죄와의 관계에 있어서도 형벌체계상의 개선이 필요하다고 본다. 왜냐하면 법무부 형법개정법률안 제안이유서에서 보면 컴퓨터 업무방해죄 구성요건의 '부정한 명령의 입력'에 '컴퓨터 바이러스' 등 악성프로그램 입력도 포함된다고 보면서 '부정한 명령의 입력'을 넘어 정보처리에 장애를 발생시키고 타인의 업무를 방해한 컴퓨터 업무방해죄의 경우 그 법정형이 '5년 이하의 징역 또는 1천500만원 이하의 벌금'인데 반해 정보통신망법상 악성프로그램 전달·유포죄의 경우 '5년 이하의 징역 또는 5천만원 이하의 벌금'으로 오히려 높게 규정되어 있어 형벌체계상의 혼란을 야기하고 있기 때문이다.

2. 획득한 타인의 아이디·비밀번호로 온라인게임사이트에 접속한 행위

다음으로 전술한 바와 같은 해킹기법을 이용하여 피해자의 온라인게임사이트 아이디·비밀번호 정보를 취득[16]하고 그 정보를 입력하여 온라인게임사이트에 접속한 행위를 어떻게 처벌할 수 있는지 문제된다. 그런데 이러한 행위는 '타인의 정당한 접근권한을 도용한 정보통신망 침입'이라는 점에서 현행 정보통신망법 제63조 제1항 제1호 위반죄(정보통신망 침입죄) 성립여부와 관련된다.

16) 다만, 주의할 것은 해킹모델A와 같이 'Keylogger'기법에 의해 수집한 아이디·비밀번호 정보도 실제로 컴퓨터의 기억장치 중 하나인 램(RAM, Random Access Memory)에 올려진 기록으로 '전자기록 등 특수매체기록'에 해당하는 것으로 판단되고, 더불어 당해 정보를 수집함에 있어서 악성프로그램 설치 및 Keylogger기법 등 '기술적 수단을 이용'하였다는 점에서 형법 제316조 제2항(기술적 수단 이용 비밀침해죄) 위반의 소지도 있다. RAM에 올려진 전자기록이 형법 제232조의2의 타인의 전자기록 등 특수매체기록에 해당한다고 본 판결로 대법원 2003. 10. 9. 선고 2000도4993 판결 참조

(1) 현행 정보통신망법 제48조 제1항은 '보호조치의 해제[17]' 여부를 불문하고 '정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입'하는 행위를 처벌하고 있다.[18] 그런데 본 죄의 구성요건 해석과 관련하여 몇가지 의문점이 제기되는데 우선 우리의 경우 독일과 달리 본죄의 미수범을 처벌하면서 독일형법 제202a조와 같이 '정보를...취득한 자'라는 문구 없이 단순히 정보통신망에 침입한 것만으로 기수책임을 인정하고 있다는 점에서 과연 어느 단계를 미수로 볼 것인지가 문제된다. 또한 독일 형법 제205조와 같이 제202a조(데이터탐지)나 제202b조(데이터탈취) 등의 경우 친고죄로 규정한 것과 달리 우리의 경우 본 죄를 비친고죄로 규정하고 있는데 이러한 조처가 과연 타당한 것인지도 의문이다.

그런데 안타깝게도 현행 정보통신망법 제63조 제1항 제1호 위반죄의 미수에 관한 국내 연구논문을 찾아보긴 힘들지만 어떻든 현행 정보통신망법이 미수범을 처벌하고 있다는 점에서 이에 관한 면밀한 법적 분석작업은 긴요하다고 하겠다. 그런데, 미수범이란 범죄의 실행에 착수하여 행위를 종료하지 못하였거나 결과가 발생하지 아니한 때(형법 제25조 제1항)를 의미하고 '실행에 착수하였다는 점'에서 예비와 구별되기 때문에 현행 정보통신망법 제63조 제1항 제1호 위반죄의 미수문제는 결국 '실행의 착수 시점을 어디에 둘 것인가의 문제'로 귀결된다고 본다.

그런데 일반적으로 실행의 착수시기는 당해 구성요건에 해당하는 행위를 하거나 그 구성요건 실현을 위한 직접적 행위가 있을 때 인정될 수 있다. 예컨대, 강도죄나 강간죄의 경우 '폭행 또는 협박행위시'를 실행의 착수시기로 보는 것은 전자에 해당하고, 절도죄와 같이 타인의 물건을 절취할 목적으로 타인의 주거에 침입하여 절취할 재물을 물색

17) 과거 정보통신망법의 전신인 '전산망보급확장과이용촉진에관한법률'에서는 전산망의 보호조치를 침해 또는 훼손하는 행위를 처벌하였다.

18) 미국의 경우에도 우리와 유사한 규정을 두고 있는데 예컨대 "접근권한 없는 의도적 접근(intentionally accesses without authorization a facility through which an electronic communication service is provided)"과 "권한을 초과한 접근(intentionally exceeds an authorization to access that facility)"이 그것이다(18 USC Sec. 2701). 반면 일본의 경우에는 헤세이 11년 8월 13일에 공포되고, 헤세이 12년 2월 13일 시행된 '부정액세스 행위의 금지등에 관한 법률(不正アクセス行爲の禁止等に關する法律)' 제3조 제2항 각 호를 통해 부정액세스 행위를 규정하고 있다.

할 때[19]를 실행의 착수시기로 보는 것은 후자의 예에 해당된다고 판단된다. 다만, 여기서 '직접적 행위'란 당해 구성요건 실현에 대한 직접적 행위로서 구성요건적 행위와 시간적·장소적으로 근접한 경우[20]를 의미하고 이 경우에도 당해 구성요건을 직접 실현하는 행위가 있는지 여부는 행위자의 '범죄목적 또는 범죄계획'에 의하여 결정되어야 한다.

따라서 어느 범죄를 범하려는 자신의 표상에 따라 그 범죄의 구성요건 실현을 위해 직접 착수한 자는 그 범죄의 미수를 범한 것으로 판단되고, 이런 점에서 범행결의를 현실화하는 모든 임의적 착수로 충분한 것은 아니지만 당해 행위가 구성요건에 해당되지 않는다고 하더라도 행위자의 전체계획에 따르면 구성요건적 실행행위와 밀접하게 결부되어 있어서 행위진행에 방해가 따르지 않는 한, 그 범죄구성요건 전부를 직접 실현케 할 결과를 가져오게 하는 그런 행위만으로도 충분하다고 본다[21].

그런데 현행 정보통신망법은 '보호조치의 훼손'이나 '데이터의 취득'여부를 불문하고 '정보통신망 침입행위 자체'를 처벌하고 있으므로 해킹모델A와 같이 '아이디·비밀번호 등 타인의 접속정보을 통해 정보통신망에 접근하는 경우'에는 결국 정보통신망 침입 전단계로써 '아이디·비밀번호를 입력하고 웹사이트 로그인 배너를 클릭하는 등 접근명령을 실행한 때'에 실행의 착수가 있다고 볼 수 있고, 따라서 접근명령을 실행하였으나 당해 정보통신망의 장애 등으로 인해 결과적으로 타인의 정보통신망에 침입할 수 없게 되었다면 장애미수로 처리할 수 있을 것으로 판단된다.[22]

---

19) 대법원 1966. 9. 20. 선고 66도1108 판결 이 외에도 자동차 안에 있는 밍크코트를 발견하고 이를 절취할 생각으로 차 오른쪽 앞문을 열려고 앞문손잡이를 잡아당기다가 피해자에게 발각된 경우(대법원 1986. 12. 23. 선고 86도2256 판결), 주간에 절도목적으로 방안까지 들어갔다가 절취할 재물을 찾지 못하여 거실로 나온 경우(대법원 2003. 6. 24. 선고 2003도1985 판결)도 물색행위를 하면서 재물에 대한 피해자의 사실상 지배를 침해하는 '밀접한 행위'를 한 것으로서 실행의 착수를 인정할 수 있다.

20) 이재상(2001), 형법총론, 박영사, p. 352 참조

21) Johannes Wessels(1997). Strafrecht Allgemeiner Teil(C.F.Müller Juristischer Verlag GmbH, Heidelberg). 허일태/역(1998), 독일형법총론, 세종출판사, pp. 286-7 참조

22) 다만, 정보통신망법 제63조 제1항 제1호 위반죄의 실행의 착수시기를 위와 같이 '접근명령을 실행한 때'로 파악하게 된다면 컴퓨터의 정보처리 능력향상과 정보처리 속도의 신속성을 감안할 때 이러한 접근명령과 거의 동시에 정보통신망 침입이라는 결과가 발생된다는 점에서 정보통신망 장애로 인해 침입이 좌절되는 등 장애미수로 되는 것은 별론으로 하고 중지미수가 성립될 여지는 거의 없게 된다. 이런 이유로 그 실행의 착수시기를 '아이디·비밀번호 입력시'로 앞당겨 이해할 경우, 법이론상 중지미수의 성립여지는 높겠지만 이러한 해석은 오히려 피고인에게 불리한 해석이라는 점, 더불어 지나친

한편, 독일 형법 제205조와 같이 제202a조(데이터탐지)나 제202b조(데이터탈취) 등의 범죄행위에 대해 피해자의 처벌희망의 의사표시가 있을 때에만 수사 및 공소를 제기하는 것이 과연 타당한지 여부를 살피건대, ⅰ) 실제로 인터넷 등 정보통신망을 통해 전송되는 정보를 중간에서 가로채는 해킹의 경우 그 증거는 이른바 휘발성 증거(Volatile evidence)로서 컴퓨터 종료와 함께 사라지기 일쑤라는 점, ⅱ) 한편 하드디스크에 범죄혐의 입증에 필요한 정보가 존재하더라도 이용자가 실수로 '덮어쓰기'를 할 경우 기존의 데이터를 복구하기는 거의 불가능에 가깝다는 점에서 사이버범죄 행위자의 검거를 위해서는 전문적인 수사기관의 신속한 초동수사가 무엇보다도 절실할 것인데, 독일 형법과 같이 친고죄로 규정할 경우 피해자의 고소권 행사만을 기다려 상당한 시간을 허비하게 되고 그 후 피해자가 고소한다 하여도 범죄 혐의입증에 필요한 증거확보가 어렵게 되어 범죄자 검거가 곤란하게 된다는 점, ⅲ) 더욱이 독일의 경우 위 규정은 그 보호법익이 '개인의 비밀의 자유'에 있는 것으로 해석되지만[23] 우리 정보통신망법 규정의 보호법익은 오히려 '정보통신망 자체의 안정성과 그 정보의 신뢰성'에 있다고 해석된다는 점에서 독일과 달리 비친고죄로 하고 있는 우리 정보통신망법의 태도가 타당하다고 본다.

(2) 그런데 정보통신망법 제63조 제1항 제1호 위반여부와 관련하여 해킹모델A와 같이 타인의 컴퓨터 시스템을 해킹하여 획득한 타인의 아이디·비밀번호를 이용해 온라인게임사이트에 접속한 행위가 앞에서 검토한 '정보통신망의 침입'에 해당된다는 점에는 의문의 여지가 없다는 점에서 결국 그 행위자에게 정당한 접근권한이 존재하는지 여부에 따라 본 죄의 위반여부를 확인할 수 있을 것이다. 그런데 본 죄에서 말하는 '접근권한의 존재여부에 관한 판단'은 대법원이 적절히 지적한 바[24]와 같이 본 죄가 이용자의 신뢰 내지 그의 이익을 보호하기 위한 규정이 아니라 '정보통신망 자체의 안정성과 그 정보의 신뢰성을 보호하기 위한 것'이라는 점에서 접근권한을 부여하거나 허용되는 범위를 설정하는 주체는 결국 '서비스제공자'라 할 것이고, 따라서 서비스제공자로부터 권한을 부여

범죄화로 인해 범죄자 양산의 우려가 있다는 점에서 타당하지 않다고 본다.

23) 일반적으로 친고죄는 피해자의 명예보호나 침해법익의 경미성을 감안하여 규정된다. 친고죄의 본질과 유형에 대한 자세한 내용은 정웅석(2006), 형사소송법, 대명출판사, pp. 138-9 참조

24) 대법원 2005.11.25. 선고 2005도870 판결 참조

받은 이용자가 아닌 제3자가 정보통신망에 접속한 경우에는 그에게 접근권한이 있는지 여부는 서비스제공자가 부여한 접근권한을 기준으로 판단하여야 한다고 해석된다. 따라서, 위 해킹모델A에서와 같이 온라인게임사업자와 서비스이용계약 체결을 통해 정당한 접근권한을 가지고 있는 자의 컴퓨터를 해킹하여 획득한 아이디·비밀번호를 이용해 온라인게임사이트에 접속한 행위자는 결국 '온라인게임사업자의 입장'에서 보면 무권한자이기 때문에 정보통신망법 제48조 제1항에서 말하는 '정당한 접근권한 없이 정보통신망에 침입한 자'에 해당되어 본 죄의 기수책임을 지게 될 것이다.

3. 게임사이트 접속 후 타인의 게임아이템 탈취행위

앞서 접근권한 없는 자가 타인의 정보통신망에 접근한 경우 현행 정보통신망법 제63조 제1항 제1호(정보통신망 침입죄)[25]의 구성요건에 해당함을 확인할 수 있었다. 다만, 해킹모델A와 같이 해킹행위자가 타인의 아이디·비밀번호로 온라인게임사이트에 접속하여 타인 계정의 게임아이템을 자신의 계정으로 옮긴 경우 이를 어떻게 형사처벌할 수 있는지 문제된다. 즉 '타인 계정의 게임아이템을 자신의 계정으로 옮기는 행위'와 관련하여 형법상 컴퓨터 등 사용사기죄(형법 제347조의2)를 인정할 수 있는지 여부가 문제되는데, 본 죄에 해당하기 위해서는 '컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득'하여야 한다. 위의 해킹모델A의 경우 ⅰ) 무권한자가 정보통신망에 침입한 후 컴퓨터등 정보처리장치에 '권한 없이 일정한 정보를 입력'하였다는 점, 그리고 ⅱ) 이러한 정보 입력행위에 따라 게임 아이템이 타인의 계정에서 해킹 행위자의 계정으로 이동되도록 '정보처리'가 실제 이루어 졌다는 점은 수긍할 수 있다. 그러나 본 죄는 이득죄로서 본 죄가 성립하기 위해서는 이러한 행위를 통해 해킹 행위자가 '재산상 이익'을 취득하거나 제3자로 하여금 취득케 해야 하는데, 이는 결국 해킹행위자가 취득한 '게임아이템의 법적 성질'이 무엇인지에 대한 판단 여하에 따라 그 법적 취급을 달리하게 된다고 하

25) 정보통신망법 제48조 (정보통신망 침해행위 등의 금지) ①누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하여서는 아니된다.

겠다.[26]

가. 게임아이템의 법적성질

(1) 게임아이템이 '재물(財物)'에 해당하는지 여부

통상 온라인 게임상에서 가상재산으로 유통되는 게임아이템이 재물에 해당되는지 문제되는데 이는 절도죄, 횡령죄, 장물죄 등 재물죄의 성립과 관련하여서도 주요한 쟁점이 된다. 그런데 이와 관련하여 현행 형법은 재물에 대한 구체적인 정의 없이 오로지 제346조를 통하여 '관리할 수 있는 동력은 재물로 간주한다'고만 규정하고 있어 형법상 재물개념을 둘러싸고 학설이 대립하고 있다. 예컨대, 관리가능성설과 유체성설의 대립이 그것인데 여기서 관리가능성설은 형법상 재물의 개념을 민법 제98조[27]의 물건과 동일한 개념으로 파악하면서 형법 제346조의 규정은 단순한 주의규정으로 이해하는 입장이며 이와 달리 유체성설은 형법상의 재물은 원칙적으로 유체물에 한정되지만 형법 제346조에 따라 '관리할 수 있는 동력'도 예외적으로 재물로 간주된다고 이해하는 입장이다. 결국, 이러한 학설 대립은 형법 제346조의 '관리할 수 있는 동력'을 민법 제98조의 '전기 기타 관리할 수 있는 자연력'과 동일하게 볼 것인지 아니면, 형법 제346조의 '관리할 수 있는 동력'을 민법 제98조의 '전기 기타 관리할 수 있는 자연력'보다 좁게 보아 형법상의 재물개념의 범위를 축소하여 이해할 것인지의 문제로 귀결된다.

그러나, 유체물이 원칙적으로 재물개념의 본질을 이루지만 무체물이라고 하더라도 관리가 가능하고 또한 형법적 보호의 필요성이 존재한다면 그것이 '관리할 수 있는 동력'이건 '전기 기타 관리할 수 있는 자연력'이건 실제에 있어서 형법의 보호를 달리해야할 본질적인 차이점을 발견할 수 없고, 또한 형법이 재물개념에 관해 적극적으로 정의하지 않고 단순히 제346조의 규정을 두어 '관리할 수 있는 동력'을 재물개념에 포함시키고 있다

26) 이와 같이 게임아이템의 법적성질 규명은 게임아이템 거래에 있어서 아이템 구매자가 판매자와 정상적인 아이템 거래를 가장하고 판매자로부터 아이템을 넘겨 받은 후 그 판매대금을 지불하지 않는 통상의 '아이템 사기'의 경우에도 마찬가지의 법적 의미를 가지고 있다.

27) 민법 제98조 (물건의 정의) 본법에서 물건이라 함은 유체물 및 전기 기타 관리할 수 있는 자연력을 말한다.

는 점에서 위 제346조의 규정을 일종의 '주의규정'으로 이해하는 것이 타당하다고 본다.[28]

그런데, 이러한 관리가능성설의 입장에서 볼 때에도 '게임아이템'은 ⅰ) 현실세계에서 일정한 공간을 차지하고 있는 유체물이 아님은 분명하고, ⅱ) 다만, '관리가능한 동력' 또는 '전기 기타 관리가능한 자연력'에 해당하는지와 관련하여 검토해 보건대 '게임아이템'은 특정 게임 프로그램에 의해 연산되어 게임플랫폼을 통해 시청각적으로 표현된 디지털 데이터라는 점에서 무체정보이고, 이러한 무체정보 또한 컴퓨터 기술 발전 및 IT기술 고도화에 따라 현실적으로 '물리적 관리[29]'가 가능하다고 볼 수도 있을 것이다. 그러나, 이러한 무체정보는 적어도 여기서의 '자연력' 또는 '동력'으로 볼 수 없다는 점에서 무체정보로서 게임아이템은 형법상 재물에 해당된다고 볼 수 없다.

(2) 게임아이템이 '재산상 이익'에 해당하는지 여부

최근 온라인 게임(특히, MMORPG)이용의 증가에 따라 게임 내에서 사용되는 게임 아이템이 게임 이용자 사이에서 현금거래 되는 사례가 비일비재할 뿐만아니라 실제 이러한 게임아이템 거래를 중개해 주는 사업자도 곳곳에서 발견되고 있다.[30] 따라서 이와 같이 아이템 현금거래라는 경제적 측면에서 볼 때 게임아이템의 법적 성질을 '재산상 이익'

---

28) 마찬가지로 "관리가 가능하여 관리하는 자연력이라면 인위적으로 만든 동력과 전혀 차이가 없으며, 형법 제346조의 '동력'이 관리하는 자연력을 배제할 이유가 없다"고 하면서 "민법 제98조의 '전기 기타 관리가능한 자연력'과 형법 제346조의 '관리가능한 동력'은 동일한 의미로 이해해야 한다"는 견해로 이정원, "가상공간에서의 Cyber 물체에 대한 침해행위와 형법적 평가", 중앙법학 제6집 제1호, p. 131 참조.

29) 대법원은 타인의 전화기를 무단사용한 것이 절도죄에 해당하는지 여부에 대한 판단에서 '타인의 전화기를 무단으로 사용하여 전화통화를 하는 행위는 전기통신사업자가 그가 갖추고 있는 통신선로, 전화교환기 등 전기통신설비를 이용하고 전기의 성질을 과학적으로 응용한 기술을 사용하여 전화가입자에게 음향의 송수신이 가능하도록 하여 줌으로써 상대방과의 통신을 매개하여 주는 역무, 즉 전기통신사업자에 의하여 가능하게 된 전화기의 음향송수신기능을 부당하게 이용하는 것으로, 이러한 내용의 역무는 무형적인 이익에 불과하고 물리적 관리의 대상이 될 수 없어 재물이 아니라고 할 것이므로 절도죄의 객체가 되지 아니한다'고 판시하여 '물리적 관리가능성'을 재물성 인정을 위한 요건으로 제시한 바 있다. 이에 대한 자세한 내용은 대법원 1998. 6. 23. 선고 98도700 판결 참조.

30) 대표적인 게임아이템 중개사이트로 아이템베이(www.itembay.com)와 아이템매니아(www.itemmania.co.kr)를 들 수 있으며 일부 통계에 따르면 아이템거래 시장규모가 연간 1조원에 육박한다고 한다.

으로 이해할 수 있는지 문제되는데 이와 관련하여 형법상 '재산개념(財産槪念)'을 둘러싸고 학설은 크게 법률적 재산설, 경제적 재산설, 절충설(법률적·경제적 재산개념)로 대립되고 있다.

여기서 ⅰ) 법률적 재산설은 '민법(재산법)상' 인정되는 개인의 권리만을 재산개념으로 파악하는 견해로 법률적으로 인정되지는 않았지만 경제적인 이익이 있는 경우를 배제한다는 측면에서 재산개념을 좁게 이해하는 입장이다. 이와 달리 ⅱ) 대법원이 취하고 있는 경제적 재산설[31]은 형법상의 재산개념을 경제적 관점에서 접근하여 경제적 교환가치만 있으면 법률상 허용되지 않는 경제적 이익의 경우에도 재산으로 취급하는 입장이다. 그러나, 이 학설의 경우에는 불법한 이익의 경우에도 여기서의 '재산상 이익'으로 평가하기 때문에 법의 통일성을 해친다는 비판이 있다. ⅲ) 절충설(법률적·경제적 재산개념)은 경제적인 가치가 있는 것 중에서 법질서가 승인하는 재화를 재산개념으로 이해하는 견해로 경제적 이익을 '법질서의 통일성'이라는 척도로 일정부분 제한을 가하는 이론이다.

생각건대 법률적 재산설은 아무런 경제적 가치를 가지지 못하는 경우에도 사법상 권리의 대상이 된 경우에는 '재산상 이익'으로 평가해야 하는 것은 부당하다는 점, 또한 재산개념의 해석은 우선적으로 '경제적 관점'에서 출발해야 한다는 점에서 볼 때 타당하지 않고, 절충설의 경우에도 '형법적 보호가치'와 '사법적 권리보호'와의 관계를 혼동한 것으로서 사법적 권리로서 보호되지 못하는 불법재산이라고 하더라도 형법적 견지에서 보호가치가 있고 그 침해행위에 대한 처벌의 필요성이 있는 경우라면 형법상의 재산개념에 포함시켜야 할 것으로 본다. 따라서, 현재 우리 대법원이 취하고 있는 경제적 재산설이 타당하고, 이런 관점에서 볼 때 '게임아이템'의 경우 ⅰ) 실제로 온라인게임 이용자들 사이에서 빈번히 현금거래가 이루어지고 있다는 점, ⅱ) 더욱이 이러한 아이템거래 중개를 사업모델로 하는 아이템중개사이트를 통해 일정한 거래가격이 형성되고 있으며[32] 그 거

31) 예컨대, 금품등을 받을 것을 전제로 성행위를 하는 부녀를 기망하여 성행위 대가의 지급을 면한 사건에서 대법원은 "부녀가 상대방으로부터 금품이나 재산상 이익을 받을 것을 약속하고 성행위를 하는 약속 자체는 선량한 풍속 기타 사회질서에 위반한 사항을 내용으로 하는 법률행위로서 무효이나, 사기죄의 객체가 되는 재산상의 이익이 반드시 사법(私法)상 보호되는 경제적 이익만을 의미하지 아니하고, 부녀가 금품 등을 받을 것을 전제로 성행위를 하는 경우 그 행위의 대가는 사기죄의 객체인 경제적 이익에 해당"한다고 판시한 바 있다(대법원 2001. 10. 23. 선고 2001도2991 판결).

32) 예컨대, 아이템거래 중개사이트인 아이템매니아를 통해 리니지Ⅱ 게임의 '마법사용 갑옷(+6메이저아르

래규모 또한 천문학적인 숫자에 이른다는 점에서 게임아이템의 '경제적 교환가치'를 인정할 수 있고 따라서, '게임아이템'도 형법상 '재산상 이익'에 포함된다고 본다.[33]

나. 컴퓨터 등 사용사기죄 성립여부

결국 위의 분석과 같이 게임아이템의 법적 성질을 경제적 재산설의 입장에 따라 형법상 '재산상 이익'으로 파악할 경우 타인의 아이디·비밀번호를 이용하여 온라인게임사이트에 접속한 후 타인 계정에 속해 있는 게임아이템을 자신의 계정으로 옮긴 행위는 ⅰ) 정당한 접근권한 없이 타인의 정보통신망에 침입하여 컴퓨터등 정보처리장치에 '권한 없이 정보를 입력'하였다는 점, ⅱ) 또한 이러한 입력행위로 인해 타인 계정의 게임아이템이 행위자의 계정으로 이전하는 정보처리가 이루어 졌다는 점, ⅲ) 행위자의 게임 계정으로 피해자의 게임아이템이 이전됨으로써 앞에서 검토한 바와 같이 본 죄의 '재산상 이익'을 취득하였다는 점에서 형법 제347조의2의 구성요건해당성을 인정할 수 있고 그 밖의 위법성조각사유, 책임조각사유가 존재하지 않는 한 행위자는 형법 제347조의2(컴퓨터등 사용사기)의 죄로 처벌받게 된다.

4. 게임아이템 취득한 후 이용자의 아이디·비밀번호를 변경한 행위

(1) 해킹모델A와 같이 통상 해킹 행위자는 게임아이템 취득에 성공한 후 그 침해사실에 대해 정당한 온라인게임사이트 이용자가 쉽게 인식하지 못하게 하거나 당해 이용자의 계정사용을 지연·단념케 하는 등 악의적인 목적으로 이용자의 계정정보(아이디·비밀번호)를 변경하기도 한다. 이 경우 그러한 정보변경 행위를 어떻게

키나로브)'의 거래가격이 100만원, 검의 일종인 소드 오브 미라클-아큐맨(+11)이 250만원에 거래되고 있음을 확인할 수 있다. (www.itemmania.co.kr, 2007. 10. 24 방문).

33) 물론 대법원을 통해 '게임아이템'의 법적 성질이 규명된 사례는 찾기 힘들지만 일부 하급심 판결을 통해 게임아이템이 '재산상 이익'에 해당된다는 취지의 판단이 시도되고 있다. 이에 대한 자세한 내용은 서울지법 서부지원 2000. 11. 8. 선고 2000고단1366 판결; 부산지법 동부지원 2002. 2. 7. 선고 2002고단108 판결; 부산지법 2004. 10. 7. 선고 2004고단3425, 4613(병합) 판결 참조.

처벌할 수 있는지 문제된다. 이와 관련하여 최근 대법원은 대학의 컴퓨터시스템 서버를 관리하던 직원이 전보발령을 받아 더 이상 웹서버를 관리 운영할 권한이 없는 상태에서, 웹서버에 접속하여 홈페이지 관리자의 아이디와 비밀번호를 무단으로 변경 사건에 대해 '정보처리장치를 관리 운영할 권한이 없는 자가 그 정보처리장치에 입력되어 있던 관리자의 아이디와 비밀번호를 무단으로 변경하는 행위는 정보처리장치에 부정한 명령을 입력하여 정당한 아이디와 비밀번호로 정보처리장치에 접속할 수 없게 만드는 행위로서 정보처리에 장애를 현실적으로 발생시킬 뿐 아니라 이로 인하여 업무방해의 위험을 초래할 수 있으므로, 컴퓨터 등 장애 업무방해죄를 구성한다'고 판단[34]한 바 있다.

(2) 그런데 위 대법원 판결에 대해서는 몇가지 의문점이 제기된다.

첫째, 권한없는 자의 정보 입력행위를 '정보처리장치에 부정한 명령을 입력한 행위'로 파악할 수 있는지 여부이다. 실제로 형법 제314조 제2항(컴퓨터 업무방해죄)의 구성요건에는 형법 제347조의2(컴퓨터 등 사용사기죄)와 달리 '권한없이 정보를 입력·변경하여'라는 규정이 명문화되어 있지 않다.[35] 따라서, 형법 제314조 제2항과 형법 제347조의2 모두 '부정한 명령을 입력'이라는 구성요건을 동일하게 규정하고 있으면서 형법 제347조의2 해석과 달리 형법 제314조 제2항 '부정한 명령을 입력'하는 것에 '권한없이 정보를 입력·변경'하는 것이 포함된다고 해석하는 것은 죄형법정주의에 반하는 법해석(유추해석)이라는 지적이 있을 수 있다. 그러나 2001년 형법 개정 전 컴퓨터 등 사용사기죄의 '부정한 명령 입력'에 '권한없는 정보 입력'이 포함된다는 이전의 대법원 판결(대법원 2003. 1. 10. 선고 2002도2363 판결)의 취지를 차용하여 컴퓨터 업무방해죄의 경우에도 '부정한 명령 입력'에 '권한없는 정보 입력'을 포함시킬 수 있을 것으로 생각된다. 예컨대 위 판결에서는 "ⅰ) 구 형법(2001. 12. 29. 법률 제6543호로 개정되기 전의 것) 제347조의2 규정의 입법취지와 목적은 프로그램 자체는 변경(조작)함이 없이 명령을 입력(사용)할 권

34) 대법원 2006. 3. 10. 선고 2005도382 판결.

35) 컴퓨터 등 사용사기죄의 경우 2001년 형법 개정 전에는 무권한 입력행위가 '부정한 명령'에 해당하는지에 대한 학설상의 논란이 있었으나 2001년 형법을 개정하여 '권한없이 정보를 입력·변경'을 추가함에 따라 이러한 논란은 무의미해지게 되었다.

한 없는 자가 명령을 입력하는 것도 부정한 명령을 입력하는 행위에 포함한다고 보아, 진실한 자료의 권한 없는 사용에 의한 재산상 이익 취득행위도 처벌대상으로 삼으려는 것이었음을 알 수 있고, ii) 오히려 그러한 범죄유형이 프로그램을 구성하는 개개의 명령을 부정하게 변경, 삭제, 추가하는 방법에 의한 재산상 이익 취득의 범죄 유형보다 훨씬 손쉽게 또 더 자주 저질러질 것임도 충분히 예상되었던 점에 비추어 이러한 입법취지와 목적은 충분히 수긍할 수 있으며 iii) 권한 없는 자에 의한 명령 입력행위를 '명령을 부정하게 입력하는 행위' 또는 '부정한 명령을 입력하는 행위'에 포함된다고 해석하는 것이 그 문언의 통상적인 의미를 벗어나는 것이라고 할 수도 없고, iv) 구 형법상으로는 그와 같은 권한 없는 자가 명령을 입력하는 방법에 의한 재산상 이익 취득행위가 처벌대상에서 제외되어 있었다고 볼 수는 없는바, 이러한 해석이 죄형법정주의에 의하여 금지되는 유추적용에 해당한다고 할 수도 없다"는 취지의 판단을 내린 바 있다.

둘째, 설사 권한없는 자의 정보 입력행위를 '정보처리장치에 부정한 명령을 입력한 행위'로 파악할 수 있다고 하더라도 본 죄가 성립하기 위해서는 '정보처리에 장애가 발생'해야 되는데[36] 아이디·비밀번호를 변경하는 행위만으로 '정보처리에 장애가 발생'한 것으로 평가할 수 있는지 문제된다. 생각건대 i) 본 죄에서 말하는 '정보처리의 장애'란 정보처리장치의 입력, 출력, 검색, 연산 등의 작동장애나 정보처리기능 장애로 이해할 수 있고, 이런 점에서 '아이디·비밀번호를 변경하는 행위'만으로 프로그램화 되어 있는 정보처리 방식에 어떠한 변경을 가져 오는 것도 아닐 뿐만 아니라 과부하에 의해 서버가 다운되는 등 현실적인 장애가 발생되는 것도 아니라는 점, ii) 대법원의 견해처럼 '정당한 아이디·비밀번호로 정보처리장치에 접속할 수 없게 만든 것'을 정보처리 장애로 이해하는 것은 접속방해와 정보처리 장애를 혼동한 것이라는 점[37]에서 단순히 '아이디·비밀번호를 변경하는

36) 물론 본 죄의 경우 '기타 방법'에 의한 경우에만 정보처리의 장애가 요하고 그 밖의 '허위의 정보 또는 부정한 명령을 입력하는 경우'에는 정보처리의 장애 발생이 필요없다는 일부 견해가 있지만(오영근, p. 281 참조), 본 죄에 있어서 '정보처리의 장애 발생'은 업무방해 위험을 판단하는 기본적인 척도이고, 더불어 컴퓨터 등 사용사기죄, 전자기록위변작죄 등과의 구별을 위해서도 본 죄 성립에 필요한 요건이라고 볼 것이다.

행위'는 본 죄의 '정보처리에 장애가 발생한 경우'로 볼 수 없다고 판단된다.

(3) 따라서, 해킹모델A와 같이 온라인게임사이트의 정당한 이용자로 하여금 계정사용을 지연·단념케 하기 위하여 이용자의 아이디·비밀번호를 변경한 행위는 권한없는 자의 정보 입력행위로써 '정보처리장치에 부정한 명령을 입력한 행위'로 이해할 수 있는 있으나 본 죄는 정보처리에 장애가 발생해야 하는 결과범이라는 점에서 단순히 '아이디·비밀번호를 변경하는 행위'만으로 정보처리상의 장애가 발생하였다고 볼 수 없으므로 결국 당해 행위자를 형법 제314조 제2항 위반죄로 처벌할 수 없다고 본다.

Ⅳ. 결 론

지금까지 타인의 게임아이템을 불법취득 하기 위해 최근 사용되고 있는 해킹기법을 분석해 보고 각 해킹행위 단계별로 현행법 체계 내에서 형사법적 규제 가능성을 검토해 보았다.

(1) 우선 이번 연구를 통해 게임아이템 취득에 사용되거나 동원 가능한 해킹기법으로 ⅰ) 불특정 다수인이 사용하는 포털사이트 등 타인의 웹사이트를 공격하여 그 이용자에게 악성프로그램을 전달·유포한 후 이를 이용하여 게임아이템을 취득하는 기법(해킹모델A), ⅱ) 직접 온라인게임 사업자를 공격하고 그 소유의 운영 Server를 조작하여 게임아이템을 취득하는 기법(해킹모델B) ⅲ) 피싱(Phishing)행위를 이용하여 게임아이템을 취득하는 기법(해킹모델C) 등 다양한 공격기법이 있음을 확인할 수 있었고 다만, 해킹모델A의 경우 타인의 웹사이트를 공격하여 다수의 이용자에게 악성프로그램을 확산시킨다는 점에서 높은 위험성이 존재함을 알 수 있었다.

37) 접속방해와 정보처리 장애를 구별하는 견해에 의하면 정보처리 장애는 어떠한 정보를 입력함으로 인하여 정보처리장치의 작동을 못하게 하거나 원래 예정되어 있는 프로그램의 실행과는 다른 명령을 수행하도록 만드는 것인데 반해, 접속방해는 접속권한 있는 자 내지 업무자로 하여금 정보처리장치에 접근할 수 있는 가능성을 차단하는데 불과하다고 한다. 이에 대한 자세한 내용은 이정훈(2006), "컴퓨터등장애업무방해죄의 성립 요건", 비교형사법연구 제8권 제1호, pp. 404-5 참조.

(2) 따라서, 해킹기법을 이용한 이러한 게임아이템 불법취득 행위에 대처하고 피해 방지를 위해 위의 '해킹모델A를 중심으로' 형사법적 규제 가능성을 검토한 결과, 전술한 바와 같이 형법, 정보통신망법 등 개별규정의 구성요건에 대한 구체적 법해석을 통해 정보통신망 침입행위, 악성프로그램 전달·유포행위, 게임아이템 취득행위 등에 대한 형사법적 규제가 가능함을 확인할 수 있었다.

(3) 다만, 현행 정보통신망법상의 악성프로그램 전달·유포죄의 경우 악성프로그램의 전달·유포행위 외에 그 제작행위는 처벌하고 있지 않지만 ⅰ) 바이러스, 웜 등 악성프로그램의 경우 높은 전파성으로 인해 광범위하게 컴퓨터 시스템을 감염시키고 그 피해 또한 순식간에 확산된다는 점, 또한 ⅱ) 예비단계로써 '악성프로그램을 제작하는 행위'를 처벌하더라도 독일과 같이 '범죄목적으로 제작한 경우'라는 일정한 제한을 가할 경우 과잉형벌의 여지는 상당히 축소된다는 점에서 우리의 경우에도 '범죄목적으로 악성프로그램을 제작하는 행위'에 대한 처벌규정을 신설할 필요가 있다고 본다. 나아가 컴퓨터 업무방해죄와 악성프로그램 전달·유포죄와의 관계에 있어서도 형벌체계상의 문제가 존재함을 발견할 수 있었고 이 부분도 개선이 필요하다고 본다.

(4) 또한 이와 더불어 컴퓨터 등 사용사기죄 성립여부와 관련하여 '게임아이템의 법적 성질'에 대한 규명작업을 수행한 결과, ⅰ) 게임아이템은 유체물이 아닌 무체정보로서 IT기술 고도화에 따라 물리적 관리가 가능하더라도 '자연력' 또는 '동력'으로 볼 수 없기 때문에 관리가능성설, 유체성설을 불문하고 형법상 재물로 보기 어렵다는 점 다만, ⅱ) 형법상 재산개념은 '경제적 재산설'의 입장에서 파악하는 것이 타당하고 이런 관점에서 볼 때 게임아이템이 실제로 온라인게임 이용자들 사이에서 빈번히 현금거래되고 있으며 아이템거래 중개사이트를 통해 일정한 거래가격이 형성되어 있다는 점에서 그 '경제적 교환가치'를 인정할 수 있고 따라서 게임아이템이 형법상 '재산상 이익'에 해당함을 확인할 수 있었다.

(5) 최근 해킹행위를 포함하여 빠르게 진화해 가는 IT기술을 접목한 새로운 유형의 범죄가 출현하고 있고 실제로 그 피해 또한 앞에서 검토한 바처럼 광범위하게 나타나고 있다. 그러나 기술발전 속도에 비하여 그 역기능 방지를 위한 법·제도는 대

부분 엄청난 피해를 경험한 후에야 마련되기 때문에 관련 법제도가 항상 기술에 뒤떨어져 등장하는 것은 어쩌면 숙명적인 일일지도 모른다. 따라서 새로운 기술을 악용한 범죄에 대처하기 위해 관련 법·제도를 마련하는 작업도 물론 필요하겠지만 '죄형법정주의의 틀 안에서' 현행법에 대한 부단한 법해석 작업을 통해 발생가능한 범죄에 대처하는 일도 무엇보다 중요하며 이런 관점에서 금번 연구의 의미를 찾을 수 있지 않을까 한다.

참 고 문 헌

Ⅰ. 단행본

구모영(2000), 신형법강의, 법률행정연구원

박상기(2002), 형법각론, 박영사

배종대(2007), 형법각론, 홍문사

이재상(2001), 형법총론, 박영사

임 웅(2007), 형법각론, 법문사

정웅석(2006), 형사소송법, 대명출판사

Gerald R. Ferrera 외(2001), CyberLaw(Text and Cases), South-Western College Publishing(a division of Thomson Learning)

Johannes Wessels(1997). Strafrecht Allgemeiner Teil(C.F.Müller Juristischer Verlag GmbH, Heidelberg). 허일태/역(1998), 독일형법총론, 세종출판사

Ⅱ. 논 문

강철하(2007), “사용자제작컨텐츠 이용확산에 따른 사회적 유해성 예측 및 법·제도적 대응방안 연구”, 경찰학연구 제7권 제2호, p. 98

이정원(2004), “가상공간에서의 Cyber 물체에 대한 침해행위와 형법적 평가”, 중앙법학 제6집 제1호, p. 131

이정훈(2006), “컴퓨터등장애업무방해죄의 성립 요건”, 비교형사법연구 제8권 제1호, pp. 404-5

이춘수(2007), “인터넷상의 재산권”, 과학기술의 발전과 사법의 대응(서울 대학교 세미나 자료집), p. 93

홍승희(2005), “정보재산권의 형법적 보호”, 형사정책연구원(2005년도 춘계 형사정책세미나 자료집), pp. 123-6

Cormac Herley, Dinei Florencio(2006). How To Login From an Internet Cafe Without Worrying About Keyloggers, The proceedings of Simposium on Usable Privacy and Security

Meier, J.D.(2006). Web application security engineering, IEEE Security & Privacy Magazine

Rachna Dhamija, J.D. Tygar, Marti Hearst(2006). Why phishing works, The proceedings of the Conference on Human Factors in Computing System (CHI2006)

Ⅲ. 기 타

“금융권 사이트, 웹해킹 대비에 사활걸어라!”, 보안뉴스 2006.1.12.자

네이버 백과사전(http://terms.naver.com/search.naver?query=iframe, 2007. 10. 22. 방문)

아이템매니아 홈페이지(www.itemmania.co.kr, 2007. 10. 24. 방문)

아이템베이 홈페이지(www.itembay.com, 2007. 10. 24. 방문)

한국정보통신기술협회 TTA용어사전(http://word.tta.or.kr/index.jsp, 2007. 10. 22. 방문)

“피싱(Phishing) 위협 및 대응 방안”, 정보통신연구진흥원 주간기술동향 1237호