온라인 게임범죄의 사례분석과 대응방안

A Study on Schemes to Case Analysis and Cope with Online Game Crimes

유용봉
한세대학교 경찰행정학과
Yong-Bong Yoo(ybyoo@hansei.ac.kr)

요약

온라인 게임범죄 주요 행위 유형은 타인 명의의 주민등록번호의 도용으로부터 폭행범죄, 사기범죄, 컴퓨터등 사용사기범죄 등에 이르기까지 다양하다. 동 범죄에 대한 법적 대응은 현행 형법을 기본법으로 특별법안들이 마련되어 있으나 다양한 행정부처에 분산되어 있어 효과적인 대응에 문제를 제기하고 있다. 따라서 본 연구는 나날이 다양해져 가고 있는 인터넷상 온라인 게임범죄에 즉시 대처할 수 있는 기본법안을 중심으로 통일적으로 대처할 수 있는 입법적 문제가 선결되어야 함을 강조하고 있다. 자연환경상 또는 인터넷 환경상 범죄에 대한 대응방안은 사전예방이 최선책이라 할 수 있으며, 그 중 가장 중요한 사전예방 조치는 보안이라 할 수 있다. 온라인 게임을 제공하는 포털업체나 개인의 경우 개인정보 유출에 대한 보안에 가장 신경을 곤두세워야 한다. 나아가 인터넷감리제도, 실명확인과정과 온라인 게임에 중독 여부에 관하여 자가 체크등도 이를 사전에 예방책이라 할 수 있다. 온라인 게임범죄의 경우 자신의 행위가 범죄라는 인식조차 없이 범행을 저지르고 자신이 노출되지 않는다고 믿는 의식에서 비롯되기 때문에 동 게임을 이용하는 게이머의 의식변화와 윤리의식 확립도 게임범죄의 사전 예방책이란 점도 밝히고 있다.

■ 중심어 : | 온라인 게임범죄 | 주민등록번호도용 | 해킹 | 비밀침해죄 | 사기죄 | 컴퓨터 등 사용사기죄 |

Abstract

Schemes to case analysis and cope with on-line game crimes net supervision system, a real name confirmation process, and a self-examination system to check by themselves if they are addicted to on-line games with a view to prevent the addiction.

In addition, this study found that general precuations should comprise measures to change the awareness of the users of the internet and to establish their ethical senses because most on-line gamers are not aware that their actions are a crime and believe their crimes are not disclosed to the outsiders.

■ Key Word : | Onlien Game-Crime | Hacking | Using by Stealth a Number of Personal Residence | Secret-Violation | Fraud | Fraud of Computer Using |

접수번호 : #060818-002
접수일자 : 2006년 08월 18일
심사완료일 : 2006년 09월 13일
교신저자 : 유용봉, e-mail : ybyoo@hansei.ac.kr

I. 일반론

1. 서 론

2004년 12월 말 우리나라의 인터넷 이용인구는 약 3,158만 명으로 전체인구의 70.2%에 이르고 있으며, 연령대별로는 20대가 95.3%, 30대가 88.1%를 차지하고 있어 향후 경제활동을 이끌어 갈 연령층의 대부분이 인터넷을 이용하고 있는 실정이며, 특히 10대 이하의 인터넷 이용률은 96.2%를 차지하는 등 머지않은 장래에 우리나라의 인터넷 이용률은 100%에 육박할 것이라 예상할 수 있다. 이는 전국에 산재한 PC(Personal Computer)방에서 저렴한 가격으로 얼마든지 인터넷을 이용할 수 있고 길거리나 자동차, 열차에서 비행기에 이르기 까지 인터넷을 이용할 수 있을 뿐만 아니라 무선인터넷의 이용가능이란 기반과 유비쿼터스 홈네트워크의 기술개발에 힘입어 그 이용자는 계속 증가한다는 점은 부정할 수 없다.

그러나 보안의식의 기대 이하 즉 보안불감증과 관련한 사이버 공간상 문제는 심각하다고 할 수 있다. 특히 브라질, 이라크, 중국 등 세계 각국들로부터 대량의 홈페이지 변조 해킹, 국가전산망 침입 및 자료 유출 등 국제적 사이버테러범죄 피해가 발생하여 국가적인 경각심을 불러일으킨 지난해라 할 수 있다.

한국게임산업개발원에 따르면 2005년 게임산업의 규모는 2004년도에 비해 2배 이상 성장하여 8조6700억 원으로 2004년의 4조 3000억 원 대비 101.1%의 급성장한 것으로 나타났다[1].수출액 또한 같은 기간에 대비 45.6%증가한 5억 6000만 달러로 집계되어 게임산업이 신흥수출의 효자노릇을 하고 있다는 사실을 밝히고 있다. 하지만 이 같은 게임 산업 성장의 이면에는 묘하게도 최근 사행성 문제로 도마 위에 오르고 있는 성인 게임장의 확대를 불러온 아케이드 게임이 자리 잡고 있는 것으로 드러났다. 국내 게임 시장을 이끌고 있는 온라인 게임은 1조 4000억 원의 매출로 40% 정도의 성장률을 보였고 모바일게임(1939억 원)과 비디오게임(2183억 원)도 각각 10%대 성장에 그쳤다. 반면 아케이드 게임의 경우 9655억 원의 매출액으로 무려 329.7%의 성장률을 기록하며 단번에 주류로 뛰어올랐다. 게임 관련 유통업소 역시 아케이드 게임장이 306%의 성장을 보이며 약 3조 7900억 원으로 최대 시장으로 떠올랐고 PC방은 1조 9900여억 원으로 18.8% 성장에 불과했다. 반면 비디오게임장은 358억 원으로 38.6% 감소했다. 전체 수출액은 5억 6466만 달러로 수입액(2억 3292만 달러)에 비해 2배 이상 높은 것으로 집계됐다.

2. 온라인 게임의 참가형태

온라인 게임은 게임을 제공하는 포털업체, 이를 중계하는 PC방과 개인 또는 업체의 PC, 이를 이용하는 온라인 게임 참여자로 구분할 수 있다. 여기에 부수적으로 금융기관 또는 우체국이 관여하게 된다. 온라인 게임에 참여하기 위해서는 게임제공자인 포털업체와 온라인 게임 참여자간에는 양자가 계약의 형태로 약정을 하여야 한다. 약정은 사인간의 계약의 형태로 게임제공업체인 포털사이트는 게임 참여자가 원하는 온라인 게임이란 서비스를 제공하고 동일성을 확정하기 위하여 개인의 이름과 주민등록번호의 입력을 요구하고 서비스대금의 지불처를 확정한다. 전자인 계약은 민법상 성년자에 한하여 단독적인 법률행위를 할 수 있기 때문에 이를 충족하기 위한 요건이며, 후자인 서비스대금은 동 계약이 성립하여 효력을 발생하기 위한 요건이 된다. 따라서 전자는 계약의 일 당사자가 법적으로 유효한 계약성립을 위한 상대방인가 아니면 미성년자의 경우 법정 대리인의 동의가 있었는가를 확인하는 절차라 할 수 있다. 따라서 미성년자가 법정 대리인의 동의가 있는 것처럼 속인다든지, 행위자가 타인 명의의 주민등록번호를 도용하는 경우 사법상의 손해배상에 관한 문제가 발생하게 된다.

3. 온라인 게임범죄의 현황

한편 사이버 공간상 역기능의 일종인 사이버 범죄는 2004년도 총 77,099건으로 2001년 대비 132%가 증가하였고, 온라인 게임산업의 발달과 함께 온라인 게임범죄(아이템관련범죄)는 35,162건으로 전체 사이버범죄의 약 46%를 차지하고 있고, 해킹, 바이러스에 의한 범죄는 15,390건이 발생하였고, PC방을 이용한 범죄가 36,148건으로 전체 사이버범죄의 절반 가량을 차지하고 있는 점도 주목해야 할 부분이다[2].

1.1 명의도용행위

명의도용등 개인정보침해행위는 2003년 2,863건이 발생하여 2,015건이 검거되고, 2004년 3,137건이 발생하여 2,065건이 검거되고 있는 실정이다[2]. 명의도용행위는 예를 들어 현 대통령의 주민등록번호와 신상정보가 인터넷망에 노출되어 지금껏 416회나 사용되었고, 그 중 280회가 성인인증용도로 사용되었고, 한국무총리와 타 국무위원들의 주민등록번호 역시 예외는 아니었고, 나아가 지방자치단체 118개 중 84개단체에서 수십 만개의 주민등록번호가 노출되어 있어 지방자치단체의 주민등록번호의 관리 또한 문제를 제기한다[8][9].

1.2 사기행위

사기범죄 중 온라인 사기행위는 2003년도에 통신 및 게임사기가 37,453건인데 비해 2004년도에 동 사기는 40,283건으로 2003년도에 비해 거의 30%가량 늘어났다. 온라인 게임관련 범죄에서 사기는 주로 아이템 거래와 관련 35,162건으로 전체 사이버범죄의 약 46%에 해당하며 그 밖에 계정 거래에서 약정한 내용을 이행하지 않는 것으로 게임관련 범죄의 90%에 해당한다[1]. 이와 관련하여 경찰청사이버테러대응센터에서는 이용자들이 조심해야 할 사기유형으로 다음과 같은 유형을 제시하고 주의를 요한다.

첫 번째 피해가 가장 심각한 유형으로 인터넷 게시판을 통해 게임 아이템이나 사이버머니를 판매하겠다고 알린 다음, 상대방으로부터 게임아이템이나 돈을 받은 다음, 잠적하는 수법이다. 이러한 수법은 한 건당 수십명에서 많게는 100명이상 피해를 입을 수 있어 파괴력이 크다. 인터넷 게시판을 통해 빠르게 노출되기 때문에 동시범죄가 가능하다.

두 번째로 ID나 아이템을 속이는 행위로 이용자들의 각별한 주의를 요구한다. 게임이용자들의 대화를 엿들은 다음, 고의로 다가가서 게임아이템이나 사이버머니를 요구하는 수법이다. 특히 친한 사람과 유사한 아이디를 만들고 접근하는 교활함을 보이며 당초 주기로 했던 아이템과 비슷한 모양으로 생긴 저렴한 가격의 아이템을 주는 수법도 있다. 이는 온라인게임 아이템의 모양이 서로 비슷한 점에서 착안한 범죄수법이다.

세 번째로 최근 이용자들이 속수무책으로 당하는 수법으로 이용자들끼리 온라인에서 아이템을 현금이나 사이버머니로 거래한 다음, 상대방이 자신의 계정을 해킹했다며 게임업체에 신고하는 수법이다. 이 수법은 온라인게임 아이템의 현물거래가 대부분의 게임업체들의 약정에서 금지돼 있다는 점을 활용하고 있다.

온라인 게임은 동 게임을 제공하는 포털업체에 이용료를 지불하여야 하고, 아이템 등을 사용할 경우 별도로 아이템 구입비를 지불해야 하며 이는 전화통신망에 의한 결제도 가능하다. 예를 들어 하나로통신사에 웹젠사의 '뮤'라는 온라인 게임을 이용시 자신의 아이디와 비밀번호(PW: Pass Word)의 입력에 전화로 결제한다는 의사표시를 통하여 결제가 가능하다. 그러나 최근에는 게임업체간의 경쟁과 무분별한 영업 이익을 높이기 위한 결제수단의 간소화에 따라 아이디만으로 결제가 가능한 경우가 허다하며, 이는 모두 게임이용자들에게 피해를 전가하고 있는 실정이다[8][9]. 이는 온라인 게임상 접속수단인 개인의 아이디와 비밀번호라는 수단에 의한 동일성 확인과 포털사이트와 접속한 전화번호로 결제한다는 의사표시의 하자와 보안상 배려가 없다는 경우이다.

1.3 해킹행위

해킹은 일반계정의 해킹과 게임계정의 해킹으로 나누어 볼 수 있고, 사이버테러형 해킹과 일반사이버공간상 해킹으로 구분할 수 있으며, 2003년에 14,159건에서 2004년 15,348건이 발생하였고, 검거는 2003년도 8,891건에서 2004년 10,993건으로 계속 증가하는 추세이다[2].

일반계정의 해킹은 2001년 2,661건, 2002년에는 2,588건으로 줄어든데 비해 게임계정의 해킹은 5,973건에서 8,878건으로 증가하는 추세이다. 그리고 온라인 게임에서의 해킹 목적은 궁극적으로 아이템이나 사이버머니를 취득하기 위한 경우가 대부분이며, 사기와는 달리 거래가 아닌 타인 계정과 타인 비밀번호 등을 알아내어 게임에 접속한 뒤 목적한 아이템이나 사이버머니를 행위자 자신이 원하는 계정으로 빼돌리는 경우를 말한다. 이 경우 행위자는 타인 계정을 불법적으로 접근할 뿐만 아니라 타인의 개인정보까지 함께 유출될 가능성이 많아 그 피해가 개인정보침해 및 훼손, 변경 등으로 이어

지기도 한다.

1.4 폭력행위

온라인 게임에서 제공되는 폭력은 게임 참여자간 쌍방이 게임을 하는 과정에서 발생하는 온라인상 언어폭력, 협박 등과 같이 정신적인 피해를 비롯하여 게임상의 전투패배나 게이머를 죽이는 PK(Player Killing)로부터 과격한 분노로 표출되어 오프라인(off-line)인 게임방 등에서 폭력사건으로 나타나며, 인터넷 공간상의 폭력이 자연공간상 폭력인 실제 폭력으로 진행되는 경우를 말한다. 예를 들어 온라인 게임상 거래되는 아이템이나 사이버머니를 자연공간상 거래하는 과정상 실제로 청소년들의 금품을 빼앗거나 협박하는 행위 등 학교폭력과도 연관성이 높은 것으로 분석되고 있다. 따라서 온라인 게임에 참여할 경우 자연환경상 스포츠게임(sports- game)과 동일하게 페어플레이(fairplay)정신이 요구되며, 특히 게이머 간에 상호간 예의를 지켜야 한다. 나아가 게임의 참여자는 장시간의 게임중독으로 인하여 온라인 게임이란 인터넷 환경과 자연환경이란 현실간의 혼동이 생기지 않도록 하는 조절능력이 있어야 하며 온라인상 또는 실제상 폭력사건의 가·피해자가 되지 않도록 하여야 할 필요가 있다.

1.5 불법복제행위

온라인 게임과 관련하여 온라인상 불법복제 및 판매행위는 2003년 664건에서 2004년 1064건으로 증가하였고[2], 최근 도박사이트에서 주로 발생하는 범죄로써 게임용 사이버머니나 고가의 아이템을 복제하여 판매하는 것을 말한다. 유형은 게임회사의 서버를 해킹하여 사이버머니를 복제한 후 목적한 계정에 할당하여 판매하는 방식과 게임회사의 서버에서 관련기술을 알아낸 후 직접 사이버머니를 생성할 수 있는 프로그램을 제작하여 실행함으로써 수천 경이라는 천문학적인 사이버머니를 복제하기도 한다. 이 경우 다른 게임관련 범죄와는 달리 행위자가 컴퓨터와 게임프로그램에 상당한 지식을 가지고 있는 전문가일 수가 있다.

또 다른 수법으로 온라인게임의 시스템에 오류가 있다는 것을 이미 알고 이를 이용해 아이템을 복제하여 온라인 게임 중 게이머들을 대상으로 불법 복제한 아이템을 판매광고를 이용하여 가격을 실제가격보다 낮춰서 판매한다.

이외에 조직적인 범죄도 등장하고 있어 10대들을 위주로 발생되는 온라인게임과 관련한 사이버범죄에 성인들이 개입함으로 조직적인 범죄도 최근 서서히 등장하고 있는 것으로 드러났다. 온라인게임 시장의 규모가 커지면서 일반인들이 청소년들을 대상으로 사이버범죄를 저지르는 범죄가 발생하고 있으며, 과거의 컴퓨터 전문가가 직접 범행을 행하기보다는 중국 등 외국의 전문해커를 고용하여 범행에 전문해커를 고용하는 형태로 바뀌고 있는 실정이다.

4. 인터넷 환경상 온라인 게임범죄의 정의

게임관련범죄란 다수의 게임 참가자(게이머: gamer)가 오프라인(off-line) 또는 온라인(on-line)을 통해서 함께 게임을 행하는 과정에서 발생하는 범죄의 총체를 말한다. 전자의 경우 아케이드게임 등 자연환경상의 게임과 텔레비전수상기 또는 게임기를 통하여 진행하는 게임과 성인 PC(Personal Computer)방 등에서 컴퓨터를 매개체로 하여 행하는 게임을 의미한다. 후자는 인터넷 망에서 게임포털제공업체가 제공하는 게임에 참가하는 게임류를 의미하며, 그 진행내용이 저장되는 게임에서 주로 발생한다. 따라서 온라인 게임범죄란 불특정 다수가 인터넷 환경상 게임서비스를 제공하는 영상화면이란 온라인 공간을 통해서 또는 매개하여 함께 게임을 하는 과정상 또는 직후 게임과 관련한 범죄의 총체를 말한다.

대부분의 온라인 게임관련 범죄는 미션(전투에서의 승리 또는 문제의 해결)을 통과하는 것으로 발생되는 능력이나 아이템을 게이머 간에 거래하는 것과 도박 게임에서 화폐(사이버 머니)를 비정상적으로 거래하는 과정에서 빈발하고 있다.

온라인 게임범죄와 관련한 범죄행위는 타인명의의 도용행위, 사기행위, 해킹행위, 폭력행위, 불법복제행위 등으로 크게 나눌 수 있고 그 피해는 수십억에서 몇 천원까지 다양하며, 이러한 온라인게임과 관련된 범죄들이 날로 증가하고 있고 수법도 교묘하며 치밀해지고 있다.

II. 온라인 게임범죄의 행위 유형

1. 온라인 게임범죄의 행위 유형

온라인 게임범죄의 행위는 크게 온라인 게임상 온라인 게임을 제공하는 포털 사이트의 프로그램이나 데이터 등 자체를 삭제하여 그 기능을 발휘할 수 없게 하는 경우와 온라인 게임과 관련하여 온라인 상 또는 오프라인상 아이템 또는 사이버머니(Cyber- money) 등을 습득하여 온라인 게임상 거래 수단으로 부정이용하는 경우로 구분할 수 있다. 여기에서 오프라인은 전통적으로 자연환경을 말하며, 반면 온라인은 컴퓨터 또는 휴대폰을 매개수단으로 사용하는 인터넷환경을 의미한다.

인터넷 환경상 온라인 게임범죄는 크게 게임대상인 사람이 전제하느냐에 따라 대인간의 부정이용범죄행위와 인터넷 환경상 자동적으로 작동하는 기계간의 부정이용범죄행위로 구분할 수 있다.

전자의 경우란 의사표시가 가능한 두 사람 이상의 온라인 게임 참가자가 온라인 게임을 행하는 과정에서 발생하는 범죄를 말한다. 한편 온라인 게임의 자동기간 부정이용 범죄란 온라인 게임의 대상이 자연인 즉 사람이 개입하지 않고 게임포털업체가 제공하는 프로그램상 게임 즉 리지니 등과 같은 게임을 온라인상 행하는 과정에서 발생하는 범죄를 말한다. 따라서 양 경우의 차이는 인터넷 환경상 온라인 게임의 대상 즉 온라인 게임의 상대방이 전제하여 게임상 아이템이나 사이버머니를 거래수단으로 수취하는 과정에 의사표시가 가능한 사람이 전제하느냐 아니면 자동적으로 작동하는 온라인 게임기가 의사표시를 대신하느냐 라는 형식의 범죄로 구분할 수 있다.

온라인 게임범죄의 대인간 부정이용행위의 경우나 자동기간 부정이용행위의 경우 동일하게 온라인 게임은 형법상 규제의 객체로서 또는 규범의 적용대상으로서 부정이용은 다음의 3가지 유형인 온라인 게임의 무권한 이용행위, 온라인 게임의 권한남용행위, 온라인 게임의 불법이용행위로 나누어 볼 수 있다. 통상 온라인 게임을 이용하기 위하여 필요로 하는 아이디 등록은 먼저 자신의 주민등록번호를 입력하고 자신의 동일성을 대신할 수 있는 영문 약자 등을 입력하여 동 게임을 이용하기도 한다.

온라인 게임의 무권한 이용행위란 게이머가 권한 없이 타인 명의의 아이디(ID: Identifikationsnummer)와 비밀번호(PIN: Persoenliches Identifikations-nummer)를 이용하여 온라인 게임을 이용하는 경우를 말한다. 이 때 행위자는 동 게임상 거래수단인 아이템이나 사이버머니를 타인명의의 인식번호인 ID나 비밀번호를 이용하여 온라인 게임을 통하여 입수하여 행위자 자신의 계정으로 이체하는 경우를 말한다. 이 경우 온라인 게임상 아이템이나 사이버머니를 자신의 계정 또는 제3자의 계정으로 이체하여 종국적으로 타인인 온라인 게임의 명의인의 계정에서 대가를 지불하게 하는 경우이다.

온라인 게임의 권한 남용행위란 타인 명의의 아이디나 비밀번호를 온라인 게임상 이용할 권한이 있는 행위자가 동 온라인 게임상 아이템이나 사이버머니를 자신의 이익을 위하여 이용하는 경우를 말한다. 예를 들어 인터넷 환경상 온라인 게임을 제공하는 포털업체에서 아이템이나 사이버머니를 관리하는 회사원이 동 게임상 아이템이나 사이버머니를 자신들의 용도로 이용하여 회사에 불이익을 야기하는 경우를 온라인 게임의 권한을 남용하여 이용한 경우라 할 수 있다.

온라인 게임의 불법이용행위란 타인 명의의 아이디와 비밀번호를 위작 또는 변작하여 온라인 게임을 이용하거나 온라인 게임상 아이템이나 사이버머니를 불법적으로 위작 또는 변작하여 이용하는 경우를 말한다.

앞서 말한 바와 같이 온라인 게임범죄에서 행위자는 타인 명의의 주민등록번호를 도용하여 타인 명의로 온라인 게임에 참여하기 위한 아이디나 비밀번호를 생성하고, 동 게임의 비용을 지불하고 아이템을 구입하거나 사이버머니 등을 자신의 계정으로 이체하여 부당한 이익을 취하는 성격이 있다. 이 경우 타인 명의의 주민등록번호를 도용하여 아이디나 비밀번호를 생성하는 행위는 형법상 사전행위에 해당하며, 행위자는 이를 이용하여 온라인 게임상 요구되는 비용이나 아이템 구입비용 또는 사이버머니를 행위자 자신의 계정으로 이체하기 위한 목적으로 이용한다는 점에서 이를 사후행위라고 할 수 있다. 이 후자인 사후행위가 인터넷 환경상 온라인 게임범죄의 주류를 이르고, 행위자는 종국적으로 후

자의 목적으로 부당한 이익을 취하기 위하여 사전 행위를 행한다는 특성을 갖고 있다.

2. 온라인 게임범죄의 법익 침해 유형

공법인 형사법이 범죄로부터 개인, 사회 나아가 국가를 보호해야한다는 차원에서 개인적 법익, 사회적 법익, 국가적 법익으로 구분할 수 있으며[3-7], 별도로 국가간의 공조를 요하는 인터넷 테러범죄의 경우 국제적으로 보호해야 할 국제적 법익으로 구분할 수 있다. 온라인 게임범죄와 관련하여 개인이 보호하는 법익은 개인이 관리하거나 개인에게 귀속된 권리가 침해될 경우 개인적 법익, 사회적으로 보호해야할 이익이 있을 경우 사회적 법익, 나아가 국가적으로 보호해야할 이익이 있는 경우 국가적 법익으로 구분할 수 있으며, 본 연구는 한정된 지면관계로 인하여 게임사와 관련한 범죄는 차후로 미루고 개인적 법익과 관련한 연구에 한정함을 밝힌다.

III. 문제제기

앞서 언급한 바와 같이 2004년 10대들이 주로 즐기는 온라인게임의 범죄율이 급증함에 따라 10대 청소년들의 범죄율이 높아져 10대 전과자들이 양산되고 있어 동 범죄에서 청소년 보호 또한 시급하다고 할 수 있다.

나아가 온라인 게임의 경우 인터넷의 보급과 연령계층의 확산으로 인하여 각계각층에서 이용되어지고 있는 실정이며, 그로 인한 범죄가 증가하고 있는 실정이다. 예를 들어 현재 인터넷 가입자 10명 가운데 6명 이상의 개인정보가 시중에 불법으로 유출된 것으로 밝혀졌으며, 특히 771만 명의 이름에서 가족관계에 이르기까지 개인정보가 건당 1원에 거래되고 있는 실정이며, 이 경우 동 게임에 명의를 도용할 수 있는 문제를 제기한다.

현대사회에 이르러 컴퓨터설비기인 정보처리장치와 통신망의 발달은 자연환경과 대비되는 인터넷환경이란 공간을 제공하였고, 동 공간은 자신을 드러내지 않아도 되는 익명성과 그 밖의 개방성, 초공간성, 동시성과 유동성적 특성[8][9]과 높은 파급효과로 인하여 불특정 또는 특정다수에게 정보를 전달할 수 있는 환경으로 발전하였다. 더욱이 앞으로 컴퓨터나 휴대폰 등의 계속적인 증가와 네티즌의 수의 급증은 그 만큼 인터넷 온라인 게임범죄 발생의 암수성을 내포하며 사회적으로 동 범죄의 예방 등 대응방안의 시급함이 주요 문제로 제기된다. 문제는 게이머들이 동 범죄에 대한 인식이 부족하여 자신이 범죄를 저지르고도 그것이 범죄라는 것을 인식하지 못하거나, 알면서도 사회에서 보통 통용되는 것이기 때문에 처벌받지 않을 것이라고 쉽게 치부해 버리는 점도 큰 문제라 할 수 있다.

IV. 온라인 게임범죄의 사례와 형법적·특별법적 방지대책

앞서 언급한 바와 같이 온라인 게임범죄는 크게 사전범죄행위와 사후범죄행위로 구분할 수 있다. 전자는 행위주체가 타인 명의의 주민등록번호의 도용하여 회원으로 가입하거나 해킹범죄행위를 통하여 게임용 타인 명의의 아이디와 비밀번호를 해킹하는 행위를 말한다. 한편 후자는 행위주체가 사전범죄행위에 의하여 얻어진 타인의 주민등록번호나 타인의 아이디 등을 이용하여 종국적으로 재산상의 이익을 자신이 취하는 범죄행위로 구분할 수 있다. 재산범죄와 관련한 사후행위의 경우 사이버환경과 자연환경상 행위가 결합한 경우가 많으며, 반대로 사이버환경에서만 이루어지는 경우도 가능하다.

1. 사전행위로써 타인 명의의 주민등록번호 도용범죄

앞서 말한 바와 같이 온라인 게임을 이용하기 위한 참여자는 온라인 게임을 제공하는 포털업체에 회원가입을 해야 하며, 원칙적으로 자신의 동일성을 확인할 수 있는 이름과 주민등록번호를 입력하여야 한다. 이 때 회원은 게임제공업자가 제공하는 약관을 숙지한다고 동의를 하여야 하며 이가 바로 양자 간의 계약이 성립하는 경우라 할 수 있다. 앞서 언급한 바와 같이 약정은 사인간의 계약의 형태로 게임제공업체인 포털사이트는 게임 참여자가 원하는 온라인 게임이란 서비스를 제공하고 게임서비스이용대금의 지불처를 확정한다.

회원가입 후 게임참여자는 자신의 사이버머니나 아이템을 관리할 수 있는 계정을 개설하여야 한다. 타인 명의의 주민등록번호를 게임포털업체에 회원가입을 위하여 도용한 경우는 사전행위이며, 회원가입 후 타인 명의로 게임이란 서비스를 이용했을 경우는 사후행위로써 온라인 게임을 이용할 목적성이 제기되고 형법상 사기죄가 성립할 가능성이 있다. 이때에도 행위자가 조우하는 대상이 자연환경 속에서 자연인일 경우 형법 제347조상 사기죄가 성립할 수 있고, 반대로 자동적으로 작동하는 인터넷환경상 온라인 게임컴퓨터와 조우할 경우 동법 제347조의2상 컴퓨터 등 사용사기죄가 성립할 수 있다.

타인의 주민등록번호를 자기 또는 타인의 재물이나 재산상의 이익을 위하여 부정 사용한 경우 주민등록법 제21조 제2항 9호상 벌칙규정에 해당하며, 허위의 주민등록번호를 생성하여 자기 또는 타인의 재물이나 재산상의 이익을 위해 사용한 경우, 동법상 벌칙규정 제21조 제2항 제3호에 허위의 주민등록번호를 생성하여 자기 또는 다른 사람의 재물이나 재산상의 이익을 위할 경우 또는 허위의 주민등록번호를 생성하는 프로그램을 다른 사람에게 전달하거나 유포한 경우 동법상 벌칙규정 제21조 제2항 4호에 규정하여 모두 3년 이하의 징역 또는 1천만 원 이하의 벌금형에 처하게 된다.

2. 사후행위로써 사기범죄

청소년층에서 가장 즐기고 있는 게임관련 범죄가 약 63%이고, 그 중에서 금원을 편취하는 게임사기가 약 81%에 달하고 있으며, 그 유형의 대부분은 아이템이나 사이버머니를 거래 또는 교환하면서 돈만 받고 주기로 약속한 아이템이나 사이버머니를 주지 않는 행위는 형법상 사기죄가 성립하며, 동법 제347조 제1항상 10년 이하의 징역 또는 2천만원이하의 벌금형이란 처벌성이 제기된다. 또한 상호간에 아이템이나 사이버머니를 교환하자고 하여 자신의 아이디와 비밀번호를 허위로 알려준 후 상대방이 알려준 계정에 접속하여 아이템이나 사이버머니를 빼가는 해킹행위는 사전행위로써 정보통신망이용촉진및정보보호등에관한법률 제63조 위반죄가 성립하며, 이는 장시간 많은 노력과 시간을 투자하여 얻어낼 수 있는 아이템과 사이버머니가 게임 마니아들에게 현실에서 느낄 수 없는 대리만족을 주고 있어 인기가 높은데, 그러한 과정을 중시하지 않고 지나치게 성과물인 아이템이나 사이버머니에 집착하여 과도한 경쟁이나 수단과 방법을 가리지 않는 소유욕이 범죄로 이어지고 있다.

온라인 게임상에서 아이템이나 사이버머니는 형법상 재물로 인정되지 않고 있으므로 현금이나 사이버머니로 아이템을 구입하기로 하고 약속을 지키지 않는 행위, 빌려 사용한 아이템을 돌려주지 않는 행위 등에 대하여 동법상 영득범죄 성립이 인정되지 않는다[8][9]. 나아가 정당한 권한 없이 또는 부여된 권한을 초과하여 정보통신망에 침입한 행위인 부정접속행위 또는 이름, 주민등록번호 등 정보통신망에 의해 처리·보관되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용·누설하는 비밀침해행위에 해당하는 경우 정보통신망이용촉진및정보보호등에관한법률 제48조 제1항상 정보통신망 침해행위 등의 금지위반죄에 해당하며, 벌칙으로 동법 제63조 제1호에 따라 3년 이하의 징역 또는 3천만원이하의 벌금형에, 동법 48조 제2항상 제62조 제6호상 는 5년 이하의 징역 또는 5천만 원 이하의 벌금형에 처하게 된다.

형법 제347조상 사기죄의 경우 2001년 5월부터2003년 6월까지 진해와 거제지역의 PC방에서 인터넷 '리지니' 게임의 사이버머니인 '아데나'를 판매한다고 속여 40명으로부터 1,500만원을 교부 받아 편취한 10대 상습 피의자의 행위에 직접 적용되며, 동 행위는 10년 이하의 징역 또는 2천만원이하의 벌금형이란 처벌성이 제기된다. 이 경우 행위자는 인터넷 공간상 행위대상들에게 대인간 의사표시에 의한 기망행위가 전제되고, 인과관계의 직접성이 제시되어 사기죄의 직접적용이 가능하다.

3. 사전행위로써 해킹범죄와 사후행위로써 컴퓨터 등 사용사기죄의 경합형태

온라인 게임과 관련하여 다른 사람의 주민등록번호와 개인의 비밀번호 또는 계정을 해킹하는 경우, 해킹행위 자체는 사전행위로써 정보통신망이용촉진및정보보호등에관한법률 제48조, 제63조상 정보통신망 무단침입죄에 해당되고, 해킹에 의해 비밀이 침해(타인 이메일 무단접

속 후 내용물 열람)되면 형법 제316조 제2항상 비밀침해죄가 성립하여 3년 이하의 징역이나 500만 원 이하의 벌금형이 부과되며, 특별법인 정보통신망이용촉진및정보보호등에관한법률 제49조상 비밀 등의 보호위반죄에 해당하며, 벌칙규정으로 동법 제62조 제6호상 5년 이하의 징역 또는 5천만 원 이하의 벌금형을 부과할 수 있고(정보통신망비밀침해죄), 통신비밀보호법 제16조 제1호상 통신비밀무단감청죄가 성립한다.

나아가 해킹 후 자료를 변경하면 개인적 법익과 관련하여 제232조의2상 사전자기록위작·변작죄에 해당되어 5년 이하의 징역 또는 1천만원이하의 벌금형이 부과되며, 국가적 법익과 관련하여 형법 제227조의2상 공전자기록위작·변작죄가 성립하며 10년 이하의 징역형이 부과된다. 이 양자 중 후자의 형은 국익과 관련한 법익이기 때문에 전자보다 무거운 형이 부과되는 특성이 있다. 법익과 관련하여 통상 국가 사회의 주요정보통신기반시설에 해킹을 하는 경우 정보통신기반보호법 제12조 제1호에 위반하여, 동법의 벌칙규정 제28조상 주요정보통신기반시설침해죄에 해당하며 10년 이하의 징역 또는 1억 원 이하의 형벌이 부과된다.

예를 들어 2002년 2월 1일부터 2003년 말 까지 인터넷 사용자의 컴퓨터 비밀번호를 알아내는 해킹프로그램을 이용한 공범자 11명이 500여명의 ID와 비밀번호 등을 알아낸 경우 사전행위로써 해킹범죄가 성립하며, 500여명의 명의로 인터넷 '리지니' 게임에 접속하여 게임 아이템을 되파는 방법으로 1,000만원의 부당이득을 취한 행위는 형법 제347조의2상 컴퓨터사용사기죄의 직접 적용은 배제된다.

위에서 행위자는 타인 명의로 온라인 게임을 이용할 경우 온라인 게임을 제공하는 컴퓨터라는 기계에 타인 명의권한을 기망하여 온라인상 제공하는 게임서비스를 제공받았고, 온라인 게임상 그러한 이익은 동조 제1항이 요구하는 재산상의 이익이라는 점에 있어 문제가 제기되지 않는다[10][11]. 단지 기망의 대상인 온라인 게임을 제공하는 포털업체는 타인 명의인의 명의로 동 게임 서비스대가를 보장받기 때문에 온라인 게임의 대가에 대한 손해를 전혀 받지 않는다. 여기에서 재산상의 손해는 첫째로 명의인의 온라인 계정으로부터 포털업체에 제공하는 정보처리장치인 컴퓨터의 매개로 전자적인 대금의 자동이체과정을 포털업체의 계정으로 이전되며 포털업체는 이를 현금으로 추심할 수 있으며, 이로 인하여 명의인의 온라인 계정상에는 전자적인 대금이 전자적인 방식으로 감액 기록된다. 이 전자적인 기록은 명의인에게 재산상의 손해를 야기한다[12]. 이러한 재산 처분은 행위자가 어떠한 변제가 없이 타인의 명의권한을 이용하여 포털업체가 제공하는 사이트를 통하여 명의인 계정에 부담을 주는 것이다. 따라서 그 부담은 온라인 게임을 제공하는 포털업체에 손해가 발생하는 것이 아닌 제3자인 명의인의 온라인 계정상의 부담이란 측면에서 제3자의 손해 발생을 야기하는 컴퓨터삼각사기의 문제가 제기된다.

컴퓨터삼각사기는 전통적인 규범으로서 삼각사기[13-15]와 같이 행위자, 착오로 인한 재산처분자, 손해자라는 3당사자가 참가한 형태라는 특징을 갖는다. 그러한 일반적 요건에 해당하는 3당사자로써는 여기에서 행위자로써 타인 명의의 개인 인식번호(ID)와 비밀번호를 무권한 사용한 행위자, 제3자의 재산을 처분하는 온라인 게임을 제공하는 포털업체의 정보처리장치인 컴퓨터, 제3자로써 동 게임상 인식번호와 비밀번호의 명의인인 손해자의 형태라고 할 수 있다. 전통적 규범으로서 삼각사기는 피기망자와 처분자는 동일하여야 할 것을 요구하고, 피기망자와 재산상의 손해자는 동일하지 않아도 된다는 기본 원칙이 요구된다[16].

행위자가 타인 명의의 개인 비밀번호와 인식번호를 온라인 게임을 제공하는 정보처리장치인 컴퓨터에 입력하여 명의인의 계정으로부터 온라인 게임을 제공하는 포털업체의 계정상에 전자적인 방식으로 대금이체가 완료된 상태에 이르러 전자대금 양도의 상대방으로써 확실한 체결자를 확보하고 동시에 법률행위상 요구되는 합치의사가 전제된다. 이에 따라 동 포털업체는 전자대금을 현금이란 액면가에 대한 청구권을 보장받는다. 따라서 포털업체의 정보처리장치인 컴퓨터는 타인의 재산을 처리할 수 있는 권한을 합치의사 즉 법률행위의 결과로서 취득한다. 결국 포털업체의 정보처리장치는 행위자와 전자대금의 이체에 관한 합치의사에 따른 법률행위에 의하여 타인인 명의인의 재산에 손해를 가하는 권

한을 갖고 있다고 할 수 있다[17][18]. 여기에서 결국 포털업체의 정보처리장치는 제3자인 명의인의 재산인 전자대금에 직접 영향을 미치는 법률행위상의 당사자이며 그 결과로서 타인인 명의인의 재산을 처분할 수 있는 권한을 법적인 권한설에 의하여 부여받았다[19][20]고 할 수 있으며, 컴퓨터등 사용사기죄상 재산처분자라 할 수 있으며 형법 제347조의2상 컴퓨터등 사용사기죄가 성립할 수 있으며, 행위자는 10년 이하의 징역형이나 2천만원 이하의 벌금형에 처하게 된다.

4. 사후행위로써 사기죄 또는 컴퓨터등 사용사기죄

유명 인터넷 게임회사 (주) A정보통신 사이트에서 운영하는 126대의 게임서버 대부분을 해킹한 후 6,270경원에 달하는 사이버머니를 위조하고 이를 판매하여 약 15억원의 부당이득을 취한 피의자 3명을 검거하여 2명은 구속하고 1명은 불구속 입건하였다. 이들이 해킹에 성공한 서버의 규모나 위조한 사이버머니 및 부당이득의 규모는 사상최대이며 아예 사이버머니 생산장을 완전히 장악해 마음대로 사이버머니를 찍어내 부당이득을 취했다. 위의 피의자는 앞서 언급한 바와 같이 해킹행위는 사전행위로써 처벌성이 제기되고, 단지 사이버머니를 위작한 경우 형법 제232조의2상 사전자기록위작죄에 해당하여 5년 이하의 징역 또는 1천만원이하의 벌금형에 처하게 된다. 여기에서 주의하여야 할 점은 사이버머니는 앞서 말한 바와 같이 형체성이 없는 데이터 또는 정보자료이기 때문에 위조라는 표현을 하지 않는 다는 것이다. 이렇게 위작한 사이버머니를 인터넷 공간에서 의사표시가 가능한 대인간에 판매한 경우 동 행위는 사후행위로써 형법 제347조상 사기죄가 직접 적용되고, 행위자는 10년 이하의 징역형이나 2천만원이하의 벌금형에 처하게 된다. 반면 행위자가 사이버공간에서 자동적으로 작동하는 컴퓨터상 사이버머니를 판매했을 경우, 동 행위는 형법 제347조의2상 컴퓨터등 사용사기죄의 직접적용이 가능하며, 행위자는 10년 이하의 징역형이나 2천만원이하의 벌금형에 처하게 된다. 반면 행위자가 타인 명의의 아이디 등을 이용하여 사이버머니를 위작하였을 경우 그 부담은 온라인 게임을 제공하는 포털업체에 손해가 발생하는 것이 아닌 제3자인 명의인의 온라인 계정상의 부담이란 측면에서 제3자의 손해 발생을 야기하는 컴퓨터삼각사기의 문제가 제기될 수 있다.

V. 온라인 게임범죄의 일반적 대응방안

1. 형사법적 대응 방안

앞서 검토한 바와 같이 인터넷 범죄는 현행 실정법보다 훨씬 앞서 발생하는 범죄다. 현재 형법을 기준으로 온라인게임과 관련한 사이버 범죄에 대해 대처할 수 있는 법안들이 마련되고 있으나 다양한 행정부처에 분산되어 있어 대처방안으로 효율성이 부족하다고 할 수 있다. 따라서 나날이 다양해져 가고 있는 인터넷상 온라인 범죄에 즉시 대응하기 위하여 동 범죄와 관련한 기본법안을 중심으로 각 행정부처에 산재되어 있는 음반비디오물게임물에관한법률, 저작권법, 컴퓨터프로그램보호법, 통신망이용촉진및정보보호등에관한법률 등 관련법규의 정비 또는 통합이라는 입법론적 문제가 선결되어야 하며 동 범죄에 효율적인 대응을 할 수 있다고 본다.

2. 개인정보의 유출 방지 대책

개인정보 도용 사건이 빈번한 이유는 인터넷 환경에서 그만큼 개인정보를 쉽게 구할 수 있기 때문이다. 흔히 도용되는 개인정보는 주민등록번호, 전화번호, 신용카드 번호, 웹사이트 가입 비밀번호 등이다.

그렇다면 개인정보를 온라인 게임 등에 도용하는 사람들은 이 같은 정보를 어떻게 얻을까?

가장 기본적인 방법은 인터넷 검색이다. 일부 인터넷 업체 및 정부 기관은 회원들의 개인 정보를 서버에 일반 문서 형태로 보관한다. 인터넷 포털 업체들의 검색 프로그램은 인터넷을 돌아다니며 각종 정보를 자동으로 모아 오는데 이때 이런 명단 및 개인정보가 섞이게 되는 것이다. 실제 인터넷 검색 사이트에서 '명단' 또는 '주민등록번호'라는 키워드를 검색하면 상당히 자세한 개인정보가 담긴 명단들이 쏟아져 나온다. 실제로 세계 최대 검색 사이트인 G포털업체를 통해 90만 명 이상의 개인 주민등록번호가 인터넷상 나돌고 있고, 외국포털업체인 M사의 검색사이트는 개인정보보호를 위한 방어장치를 하

지 않아 개인정보의 노출이 심각한 수준이라 할 수 있다.

또한 온라인 게임의 '리지니'게임의 명의 도용 피해신고가 20만 건에 이르고 있으며 동 게임의 이용자가 200만 명이란 점을 감안하면 동 게임상 개인 명의도용은 더 극심한 암수성이 있다고 할 수 있다[21].

나아가 인터넷 가입자의 개인정보가 신규 업체 마케팅에 악용되는 사례가 발생하고 있어 우리사회에 충격을 주고 있다. 2006년 4월 3일 국내 인터넷 가입자 1240만 명의 62.2%에 해당하는 771만 명의 개인정보가 시중에 불법 유출된 사실이 경찰에 적발됐다. 경북지방경찰청 사이버수사대는 3일 가입자 정보를 불법 유통시킨 혐의로 텔레마케팅회사 대표 김모씨 등 3명에 대해 구속영장을 신청하고 박모씨 등 9명을 불구속 입건했다. 경찰에 따르면 김씨는 지난 1월 초 PC방에서 텔레마케팅회사 대표인 장모씨로부터 476만 명의 인터넷 서비스업체 가입자 정보가 담긴 CD 2장을 270만원에 구입하는 등 771만 건의 가입자정보를 확보, 건당 1원 전후의 가격으로 판매했고, 적발된 불법 유통정보는 KT, 하나로통신, 두루넷, 온세통신 등 국내 4대 인터넷 서비스업체의 가입자 정보였으며 이 정보를 구매한 업자 대부분은 지난해 신규 시장에 진출한 파워콤과 관련된 고객유치 영업을 담당하는 텔레마케팅 회사 관계자 등인 것으로 파악됐다[22].

이처럼 개인의 불법정보는 사이버 공간상 넘쳐나 자연환경상 덤핑거래의 대상이 되고 있으며, 유출된 정보는 고객 이름과 주소, 주민등록번호, 전화번호, 아이디뿐 아니라 일부의 경우 고객 가족관계 정보까지 포함돼 있는 것으로 밝혀졌다. 개인정보가 인터넷 공간 등을 통해 무차별적으로 거래되면서 거래단가도 대폭 하락한 것으로 나타났다. 불법 개인정보 유출을 막기 위해서는 각종 인터넷 관련 가입 시 이름 등 최소정보만 제공하는 것이 지금으로선 최선의 방법[22]이라 할 수 있다.

1.1 개인적 대응 방안

네티즌들의 경우 온라인 게임회원으로 가입하기 위한 주민등록번호나 가입 비밀번호는 개인정보 도용을 위해 반드시 알아내야 하는 정보자료이기 때문에 개인 자신이 직접 관리를 하여야 한다. 개인의 경우 인터넷 환경에서 직접 자신의 정보를 키워드로 검색해 본 뒤 문제가 생긴 웹사이트 운영자에게 주의를 주어야 하는 등 개별적인 관리를 요한다.

특히 인터넷 전문가들은 의외로 PC방 등 외부 컴퓨터에 개인의 로그인 정보를 남겨 두는 사람들이 적지 않다고 지적하며, 외부 컴퓨터에 남겨놓은 개인 정보는 많은 도용 사건의 원인이 되고 있다는 점을 주의하여 반드시 로그아웃을(logout) 해야 한다. 또한 개인의 비밀번호의 경우도 숫자와 문자를 섞어 사용해야 하며, 생일이나 주소 등 숫자는 피하여야 한다.

또한 외부 컴퓨터를 사용할 때는 높은 버전의 웹브라우저를 써야 하며, 좋은 웹브라우저는 온라인으로 교환되는 정보를 엄격히 암호화하기 때문에 해커들이 중간에서 정보를 가로 막는 역할을 한다. 나아가 웹브라우저를 모두 사용한 후에는 브라우저 내 '인터넷 옵션'으로 들어가 파일과 암호 자동완성 기능 등을 반드시 지워야 한다.

현재 전자 상거래나 전자금융거래가 확산되면서 신용카드의 정보 등이 인터넷 환경을 통하여 전송 또는 입력하여야 하는 개인 금융정보도 크게 늘어났다. 따라서 신용카드와 관련한 정보 등도 온라인 게임상 지불수단으로 또는 매개수단으로 사용할 경우 온라인 정보 암호화 프로그램을 반드시 설치하여야 하며, 공인 전자 서명도 꼭 받아 둬야 할 필요가 있다. 전자서명이란 금융결제원, 증권전산, 한국정보인증, 한국전자인증, 무역정보통신 등 6개 공인인증기관에서 전자상거래의 본인 여부를 인증 받는 것으로 인터넷 환경에서에서 인감증명의 역할을 담당한다. 이는 개인의 아이디나 비밀번호를 입력할 필요 없이 한번 만들어진 전자서명만 온라인으로 전송하면 되며, 전자서명은 고도화된 암호코드로 이뤄져 있기 때문에 자신의 개인정보 보안상 기대효과가 크다고 할 수 있다.

1.2 법적 대응 방안

앞서 언급한 바와 같이 온라인 게임 '리지니'의 경우 이용자가 200만 명 정도란 점을 감안하면 그 밖의 포털사이트가 제공하는 서비스에 방문하는 네티즌은 그 수가 어마어마하다고 할 수 있다. 정부와 여당은 인터넷상

1일 방문자 수가 포털사이트에 30만 명, 미디어에 20만 명 이상인 사이트에 한하여 인터넷 실명제를 내년 상반기 중에 시행하기 위한 제한적 대책으로 정보통신망이용촉진및정보보호등에관한법률을 개정하기로 한 점은 고무적이라 할 수 있다[23].

1.3 민사상 배상책임

온라인 게임범죄의 피해자는 가해자를 대상으로 앞서 언급한 형사법적 대처 외에 민사법적 피해배상을 청구할 수 있다. 이를 민법 제750조 이하 규정에 따른 불법행위에 따른 손해배상청구권이라 하며 형사법적으로 범죄 즉 가해자의 행위를 법원이 판단하여 불법행위가 성립될 경우 피해자는 그 불법행위를 원인으로 자신의 손해액을 법원에 소를 제기하여 청구할 수 있는 대처방안도 있다.

최근에 특히 아이템 현금거래 계정압류 취소 판결 "내 계정도 내놔라" 라는 집단소송도 예상되고 있으며, 서울고등법원은 2006년 6월 15일 온라인게임 '리니지' 개발사측(대표 김00)에 '리니지'에서 게임 아이템을 현금으로 거래하다 적발된 이용자에 대해 계정(아이디와 비밀번호)을 영구 압류한 조치를 취소하라는 조정을 내렸다. 이날 법원의 조정은 '리니지' 이용자 차모씨가 지난해 7월 다른 리니지 이용자로부터 남의 계정에서 훔친 아이템을 자신의 계정으로 넘겨받는 대가로 현금 44만원을 지급했고, 다른 이용자로부터 넘겨받은 계정에서 아이템을 현금 거래로 시도하다 적발돼 두 개의 계정 모두 영구 압류 조치를 당했다면서 낸 소송의 최종 판결이다. 차씨의 경우 아이템 현금 거래를 했다고 1000만원 상당의 아이템이 들어 있는 게임 계정을 영구 압류 한 것은 지나치다며 게임사를 상대로 1000만원의 손해배상 청구 소송을 제기했으나 동 법원은 15일 계정 압류 조치를 취소한다는 조정이 성립됐다고 밝혔다. 그동안 우리 법원은 아이템 현금거래가 사기, 절도 등 각종 범죄를 유발하고 있어 계정 압류 조치는 문제가 없다는 입장이었다. 같은 사안을 놓고도 지난해 1심 법원은 게임사가 현금거래가 적발되면 계정을 압류한다는 공고를 했고 약관에도 현금거래를 금지하고 있어, 계정압류 조치는 지나치지 않다고 판결했다. 그러나 차씨는 이 같은 1심 법원의 판결에 불복해 항소했고, 항소심인 서울고법의 이 같은 판결에 따라 아이템 현금거래로 계정이 압류된 사람들의 집단 소송이 예상된다. 그동안 계정 압류를 당한 이용자들이 이번 소송 결과에 촉각을 곤두세웠던 만큼 향후 이와 비슷한 소송에서 어떤 판결이 내려질지 주목된다. 또한 리지니 게임사는 지난 4월28일 온라인 게임 '리니지'게임에서 개인정보가 유출된 게임 이용자들에게 1인당 50만원씩을 지급하라는 법원(서울중앙지법 민사 43단독 허00성욱 판사) 판결도 받은 바 있다. 이는 개인정보를 유출당한 게임 이용자들이 게임회사를 상대로 승소한 첫 판결이며 민사상 배상책임을 인정한 경우라 할 수 있다. 한편, 공정거래위원회는 지난해 10월 아이템 현금거래 행위로 적발된 경우 계정을 압류하게 한 조항 등이 위법이라며 국내 11개게임 업체에 이용약관을 수정하도록 시정조치[24]를 하였고, 이는 불공정한 약관에 대한 게임업체의 책임소재를 가늠할 수 있는 규제라 할 수 있다.

3. 게임참여자의 의식 변화

인터넷 기술은 앞으로도 계속적인 발달을 보일 것이고 그로 인한 범죄는 나날이 새롭게 나타날 것이다. 이러한 범죄에 효과적으로 대응하기 위해서는 일시적 대책이 아닌 미래 대안적인 방법을 강구할 필요가 있다.

사이버 공간을 이용하는 참여자들의 대부분은 익명성을 이용하여 자신의 행위가 범죄라는 인식조차 없이 범행을 저지르는 경우가 많다. 이는 자신이 노출되지 않는다고 믿는 것에서 나타나는 것으로서 그렇기 때문에 인터넷을 사용하는 사용자 대상의 의식변화와 윤리의식 확립이다. 경우에 따라 사이버범죄의 경우 자신의 능력을 과신하여 남보다 우월한 기술을 자랑하고자 하는 자만심과 게임과 실재를 구분하지 못하고 연관시켜 생각함으로써 나타나기 때문에 그를 막는 방법으로서 윤리의식의 확립과 의식의 변화는 꼭 필요하다 하겠다.

4. 게임중독여부의 자가 체크

각국은 범죄에 관하여 형사정책상 일반예방적인 성격을 갖는 사전예방을 원칙으로 하며, 부수적으로 범죄행위자의 범죄책임을 전제하여 행위자 자신에게 형벌을

과하는 특별예방의 효과를 기대하고 있다.

따라서 온라인 게임범죄의 경우도 사전 예방조치로 온라인 게임에 중독 여부에 관하여 자가 체크를 하여 게임을 즐기는 게이머 스스로가 이를 사전에 예방할 수도 있다.

5. 사전 예방 대책

인터넷 환경상 개인정보 유출을 막기 위하여 웹사이트제작과정상 인터넷감리제도를 법제화하여 웹사이트 설계단계부터 제3자의 감시를 해야 한다는 주장이 제기된다[24]. 또한 개인정보 노출 여부를 검증할 수 있는 '방문객 검색엔진 시뮬레이션 감리'도 필요하다. 이미 미국 등에서는 감리를 통해 홈페이지의 설계과정에서부터 개입하여 개인정보 노출을 차단하고 있으며, 미 국방성의 경우도 군사비밀보호를 위하여 2000여 산하 웹사이트에 '시뮬레이션 감리' 방안을 채택하고 있다. 그 밖에 포천지 선정 500대 기업 대부분도 검색엔진 마케팅과 개인 또는 기업정보보호 간의 정보딜레마를 해결하기 위한 시뮬레이션 감리를 도입하고 있는 실정이다[24].

VI. 결 론

앞서 검토한 바와 같이 온라인 게임범죄와 관련하여 동 범죄의 주요 유형은 타인 명의의 주민등록번호의 도용으로부터 폭행범죄, 사기범죄 등에 이르기까지 다양하다. 이에 대하여 법적으로 현재 형법을 기준으로 온라인게임과 관련한 사이버 범죄에 대해 대처할 수 있는 법안들이 마련되고 있으나 다양한 행정부처에 분산되어 있어 대처방안으로 효율성이 부족하다고 할 수 있다. 따라서 나날이 다양해져 가고 있는 인터넷상 사이버 범죄에 즉시 대처할 수 있는 기본법안을 중심으로 통일적으로 대처할 수 있는 입법적 문제가 선결되어야 한다.

나아가 가장 중요한 사전예방조치는 보안이라 할 수 있으며, 온라인 게임을 제공하는 포털업체나 개인의 경우 보안 개인정보 유출에 대한 보안에 가장 신경을 곤두세워야 한다. 다음으로 인터넷감리제도, 실명확인과정과 온라인 게임에 중독 여부에 관하여 자가 체크를 하여 게임을 즐기는 게이머 스스로가 이를 사전에 예방할 수도 있다.

온라인 게임범죄의 경우 자신의 행위가 범죄라는 인식조차 없이 범행을 저지르는 경우가 많다. 이는 자신이 노출되지 않는다고 믿는 것에서 나타나는 것으로서 그렇기 때문에 인터넷을 사용하는 사용자 대상의 의식변화와 윤리의식 확립이 선결문제이기도 하다.

참 고 문 헌

[1] Focus, p.38, 2006(7.18).

[2] 경찰청, *2005 경찰백서*, p.160, 2005(7.20).

[3] 이재상, *형법각론*, p.5, 2004.

[4] 강구진, *형법강의 각론 I*, p.8, 1983.

[5] 김종원 외 6, *신고 형법각론*, p.51, 1986.

[6] 정영석, *형법각론*, 1983.

[7] 황산덕, *형법각론*(5정판), p.51, 1983.

[8] 원혜욱, "인터넷범죄의 특징과 범죄유형별 처벌조항", 형사정책연구, 제42호, p.95, 2000.

[9] 백광훈, "인터넷범죄의 규제법규에 관한 연구", 형사정책연구, 40호, p.39, 2000.

[10] 이재상, *형법각론*(제5판), p.249, 2004.

[11] 김일수, *형법각론*(III), p.528, 1997.

[12] Vgl. Schoenke/ Schroeder-Cramer, *Strafgesetzbuch Kommentar*, §263 Rn. 28.

[13] 이재상, *형법각론*, 339, 2005.

[14] 박상기, *형법각론*: p.317, 2004,

[15] 안경옥, "신용카드의 부정취득·사용행위에 대한 형법적 고찰1", p.248, 1999.

[16] RGSt 73, 384; BGHSt 18, 223; Hamburg HESt 2, 317.

[17] Erich Samson, *Systematischer Kommenter zum Straggesetzbuch Besonderer Teil Band II*(§§80-358), 4. Aufl., 29. Lfg.), §263 Rn. 98, 1991.

[18] W. Joecks, *Zur Vermoegensverfuegung beim Betrug*, S. 132, 133 f., 1982.

[19] Samson, *Systematischer Kommenter zum Straggesetzbuch Besonderer Teil Band II*(§§80-358), 4. Aufl., 29. Lfg.), §263 Rn. 78 f., 1991.
[20] 대판 1981.7.28, 81도529.
[21] 조선일보, p.A4, 2006(2.20).
[22] metro, p.2, 2006(4.4).
[23] 조선일보, p.A1, 2006(7.29).
[24] Focus, p.52, 2006(6.19).

저 자 소 개

유 용 봉(Yong-Bong Yoo) 정회원

- 1980년 2월 : 국민대학교 정치학사
- 1992년 2월 : 국민대학교 법학석사
- 1995년 9월 : Kiel University in Germany 법학석사
- 1996년 12월 : Kiel University in Germany 법학박사
- 2001년 3월~현재 : 한세대학교 경찰행정학과 교수

<관심분야> : 형법, 형사소송법, 인터넷범죄, 컴퓨터범죄