

# 사이버범죄 유형별 특징 분석 연구

## Analysis of Cyber Crime and Its Characteristics

이 소 현 (So-Hyun Lee)	연세대학교 정보대학원
강 일 웅 (Ilwoong Kang)	강원경찰청
정 윤 혁 (Yoonhyuk Jung)	고려대학교 미디어학부
김 희 웅 (Hee-Woong Kim)	연세대학교 정보대학원, 교신저자

### 요 약

기존에 오프라인에서만 발생하던 범죄들이 이제 사이버 공간에서도 발생하게 되었다. 특히, 최근 스마트폰 보급에 힘입어 SNS 사용이 증가하면서, 사이버범죄가 증가하게 되었다. 현재 심각한 사회문제로 언급되고 있는 사이버범죄와 그 유형들을 이해하고, 각 사이버범죄의 범죄 관련 요인들을 파악함으로써 사이버범죄를 예방하는 구체적인 방안 제시가 필요하다. 하지만, 사이버범죄 관련 기존 연구들은 대부분 문헌연구 또는 간접적 접근을 통해서 이루어졌다. 그리하여, 본 연구에서는 실제 사이버범죄를 저지른 피의자(범죄자)를 대상으로 인터뷰를 실시하여 범죄 관련 요인들을 파악하고, 이를 기반으로 사이버범죄의 구체적인 예방 및 대응방안을 제시한다. 특히, 다양한 사이버범죄의 유형 중에서 본 연구에서는 최근 급증하며 문제가 되고 있는 정보통신망이용 범죄의 ‘거래’와 ‘금융’, 그리고 불법콘텐츠 범죄의 ‘ 명예훼손·모욕’에 집중하여 조사하고자 한다. 본 연구는 인터뷰를 실시하고, 도출된 주요 요인들 간의 관계를 나타낸 것에 학술적 의의가 있으며 사회적으로는 사이버범죄의 예방 및 대응방안을 제시함으로써 사이버범죄의 피해를 줄이고 이를 해결하는데 기여할 수 있다.

**키워드 :** 사이버 범죄, 사이버 명예훼손·모욕, 사이버 거래, 사이버 금융거래, 인터뷰

## I. 서 론

사이버 공간은 컴퓨터, 인터넷 등 정보통신망을 통한 정보전달 즉, 정보교류에 의하여 형성되며 그 속에서 전자우편(Email), 메신저(Messenger), 소셜 네트워크(Social Network) 등의 서비스를 이용

하여 서로 정보를 주고받는다. 사람들은 사이버공간인 온라인 환경에서 정보교류를 통하여 관계를 형성할 수 있고, 나아가 현실세계의 생활방식을 온라인 환경에 적용할 수 있다. 결국, 현실세계와 사이버 공간이 동일 시 되면서(김연수, 2003) 사람들의 생활이 정보통신망으로 연결된 사이버 공간에서도 이루어지게 되어 기존에 현실세계에서만 발생하던 범죄 현상들이 사이버 공간에서도 발생하게 되었다. 다시 말하면, 정보통신망을 악용하여 사이버 공간을 대상으로 하거나 사이버 공간을

† 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018S1A3A2075114). 이 논문은 연세대학교 바른ICT연구소의 (일부) 지원을 받아 수행된 연구 결과임(2018-22-0003).

이용하여 이루어지는 사이버범죄(Cyber crime)가 발생하고 있으며(곽병선, 2008), 최근 이러한 사이버범죄의 발생률이 증가함으로써 심각한 사회문제로 대두되고 있다. 특히, 소셜미디어 사용의 증가로 사이버범죄와 같은 사회분열 현상들이 증가하고 있다(Kim *et al.*, 2015).

경찰청의 2018년 9월 사이버위협 분석보고서에 따르면, 2018년 한 해 발생한 사이버범죄는 총 10만 8,825건으로 전년 대비 7.1% 증가한 것으로 하루에 약 399건의 사이버범죄가 발생하고 있는 실정이다(김상순, 2018). 또한, 경찰청 사이버안전국의 사이버범죄 발생 검거 현황을 통해 2004년부터 2015년까지 사이버범죄 발생 건수가 지속적으로 증가하고 있는 것을 확인할 수 있었다(이현진, 2017). 사이버범죄는 기존의 오프라인에서의 범죄가 온라인의 사이버공간에서 이루어지는 것도 있지만, 새로운 기술의 발전에 따라 가상통화, 사물인터넷(IoT) 등과 연결된 기존에 볼 수 없었던 새로운 방법을 이용한 범죄도 발생하고 있다. 특히, 익명성과 비대면의 환경에서 발생하는 사이버범죄는 피해자만 남고 피의자는 존재하지 않는 경우가 많아 심각한 사회문제로 나타나고 있다. 사이버범죄 중에서도 거래와 연계된 인터넷 사기가 82,716건으로 전체 사이버범죄의 76%를 차지해 가장 많은 비율을 보였다. 특히, 한국은 스마트폰 보유율이 94%로 전 세계 주요 국가 중 1위를 기록하고 있으며, 개인의 인터넷 이용 및 모바일 쇼핑 이용이 크게 증가함에 따라 인터넷 사기도 증가하고 있는 것으로 볼 수 있다. 다음으로 사이버 명예훼손·모욕이 11,236건(10.3%), 사이버 금융 범죄가 3,786건(3.5%)으로 많이 발생하고 있다(이관주, 2018). 사이버 명예훼손·모욕이 만연하게 된 것 또한 스마트폰의 대중화와 SNS 사용이 증가하면서 시작된 1인 미디어 시대가 끼친 영향이 크다. 이와 관련하여, 온라인에서의 댓글 문화와 1인 방송이 대중화되면서 사이버 명예훼손·모욕이 급증하고 있으며, 온라인에서는 오프라인에 비해 전달하는 콘텐츠의 전파 및 파급력이 크기 때문에 그 문제성 또한 심각하다. 이렇듯 현재

심각한 사회문제로 언급되고 있는 사이버범죄의 세부 유형들을 이해하고, 주요 사이버 범죄의 유형에 대한 범행 관련 요인 분석을 통하여 사이버범죄를 예방할 수 있는 방안 제시가 필요하다.

이와 관련하여 기존 사이버범죄 관련 연구에서는 사이버범죄의 개념 및 특징적 관점(이규안, 2012; 이성식, 2018; 정완, 2009), 법/제도적 관점(Ajaji, 2016; 강동범, 2007; 곽병선, 2008), 피해 요인적 관점(Nasution *et al.*, 2018; Riek *et al.*, 2016; 성용은, 박준호, 2018; 이춘화, 2009)의 연구가 있었으나 대부분이 기존 문헌을 기반으로 조사되어 지거나 일반인을 대상으로 범죄의 원인을 유추하는 간접적인 접근 방법으로 이루어졌다. 하지만, 현재 심각한 사회 문제로 대두되고 있는 사이버범죄 행위에 대한 이해와 정확한 분석을 위해서는 각 사이버범죄 유형의 실제 범행 요인들과 그들 간의 다각적 분석이 요구된다. 그리하여 본 연구에서는 실제 사이버범죄의 피의자들을 대상으로 인터뷰를 실시하여 사이버범죄에 대한 원인 및 방법 등을 파악하고, 이를 기반으로 사이버범죄의 구체적인 예방 및 대응방안을 제시하고자 한다. 본 연구에서는 경찰청 사이버안전국에서 제공하는 사이버범죄 분류 기준에 의거하여 그 유형들을 분류하고, 분류된 사이버범죄 유형의 세부 유형 중에서 최근 그 발생률이 가장 높은 정보통신망이용 범죄의 사이버 거래와 금융, 그리고 정보통신망이용 불법 콘텐츠 범죄의 사이버 명예훼손·모욕에 대하여 조사하였다. 즉, 실제 사이버범죄 피의자들을 대상으로 범행의 동기, 가능이유, 방법, 사용한 미디어 등을 실제 범죄 사실을 기반으로 심층 인터뷰하고 이를 분석하여 각 사이버범죄에 대한 대응방안을 제시한다. 더불어, 인터뷰를 통해 도출된 주요 요인들을 각 질문에 따라 구분하고 그들 간의 연결 관계를 살펴보고 시각화한다. 본 연구는 사이버범죄와 관련하여 실제 범행 피의자를 대상으로 인터뷰를 실시하고 도출된 주요 요인들 간의 관계를 네트워크 분석을 통해 시각화한 것이 방법론 측면에서 학문적 의의가 있으며, 사

회적으로는 사이버범죄의 예방 및 대응방안을 제시함으로써 사이버범죄 피해를 줄이고, 이를 해결하는데 기여할 수 있다.

## II. 개념적 배경

### 2.1 사이버 범죄

사이버범죄는 컴퓨터, 통신, 인터넷 등을 악용하여 사이버 공간에서 행하는 범죄로 컴퓨터 시스템이나 사이버 공간을 이용하여 다른 사람에게 피해를 주고 사이버 문화에 해를 끼치는 행위이다. 이러한 사이버범죄는 기존의 컴퓨터 네트워크망을 기반으로 하며 인터넷의 특성인 익명성과 비대면성을 악용한 사이버 상에서 벌어지는 불법 행위를 말한다(성용은, 박준호, 2018). 즉, 사이버 범죄는 일반 범죄와 달리 빠른 시간 안에 불특정 다수에게 악영향을 끼치며, 전자 정보의 수정 또한 쉽다. 초기 사이버범죄들은 대부분 데스크탑 컴퓨터를 이용하여 인터넷에 접속하는 방법으로 이루어졌으나 모바일 기기를 통한 인터넷 접속이 가능해지면서 다양한 디바이스들을 이용한 새로운 유형의 사이버범죄가 출현하고 있다. 최근 새로운 정보시스템 기술들이 지속적으로 개발 및 사용되어지면서 사이버범죄의 형태가 다양화되어지고 있으며, 그 개념도 관점에 따라 컴퓨터범죄, 하이테크범죄, 인터넷범죄 등 다른 용어들로 사용되어지고 있다(정완, 2007).

기존 연구들에 의하면 사이버범죄는 새로운 생활공간인 가상공간을 이루게 할 수 있는 정보통신망에 대한 불법적인 행위를 포함하여 가상공간에서 일어나는 모든 불법적인 행위라고 정의(정완, 2009)되거나, 가상공간에서 다른 사람의 생명, 신체, 재산, 명예 및 사생활 등 개인을 위협하거나 또는 사회를 위협하는 불법적인 행위라고 정의(조병인 등, 2010)하고 있다. 또 다른 연구에서는 정보통신망을 이용하여 이루어지는 불법적인 거래, 금융 행위, 정보통신망을 이용하여 이루어지는 아

동포르노 유포 행위, 그리고 정보통신망 없이는 할 수 없는 모든 불법적인 행위라고 정의되고 있다(Garg and Camp, 2015). 이를 기반으로, 본 연구에서는 기존 연구들에서 정의된 사이버범죄의 개념을 기반으로 사이버공간에서 정보통신망을 목적으로 하거나, 정보통신망을 수단으로 하는 모든 불법적인 행위를 사이버범죄라고 정의하였다.

### 2.2 사이버 범죄의 유형

사이버범죄는 가상공간의 기반이 되는 정보통신망의 존재를 위협하는 것과 현실공간에서의 전통적인 범죄가 가상공간으로 옮겨져 정보통신망을 수단으로 하는 것으로 크게 구분할 수 있다. 또한, 정보통신망을 통하여 이루어지는 불법적인 금융 행위 유형과 정보통신망을 통하여 이루어지는 불법적인 콘텐츠 게시유포배포의 유형 및 정보통신망 없이는 이루어질 수 없는 모든 불법적인 행위 유형으로 구분하고 있다(Garg and Camp, 2015). 한국의 경찰청 사이버안전국에서는 2014년 7월을 기준으로 기존 해킹/바이러스, 인터넷 사기, 사이버폭력, 불법사이트 운영, 불법 복제판매, 기타의 항목으로 사이버범죄를 분류하던 것에서 정보통신망침해 범죄, 정보통신망이용 범죄, 정보통신망이용 불법 콘텐츠 범죄의 세 가지의 항목으로 구분하기 시작하였다. 그리하여 본 연구에서는 경찰청 사이버안전국의 유형별 사이버범죄 통계자료의 구분 기준을 근거로 정보통신망의 존재를 위협하는 1) 정보통신망침해 범죄, 정보통신망을 주요수단으로 이용하는 2) 정보통신망이용 범죄, 그리고 정보통신망을 통하여 전송되는 데이터(콘텐츠)가 불법인 3) 불법콘텐츠 범죄의 세 가지의 유형으로 크게 구분하였다. 그리고 구분된 세 가지 유형은 다시 세부 유형으로 구분할 수 있다. 즉, 각 유형에 속하는 세부 유형의 범죄로는 정보통신망침해 범죄의 해킹, 정보통신망이용 범죄의 금융, 거래, 저작권 침해, 마지막으로 불법콘텐츠 범죄의 도박, 명예훼손·모욕, 음란물, 스토킹이 있다(<표 1> 참조).

〈표 1〉 사이버범죄의 유형

대분류	중분류	내용
1) 정보통신망 침해범죄	해킹	정보통신망과 같은 자원에 대한 접근제한 정책을 비정상적인 방법으로 우회하거나 무력화시킨 뒤 접근하는 행위
2) 정보통신망 이용범죄	금융	정보통신망을 이용하여 피해자의 계좌로부터 자금을 이체 받거나, 소액결제가 되게 하는 행위
	거래	정보통신망을 통하여, 이용자들에게 물품이나 용역을 제공할 것처럼 기망하여 피해자로부터 금품을 편취하는 행위
	저작권 침해	정보통신망을 통하여, 디지털 자료화된 저작물 또는 컴퓨터프로그램 저작물에 대한 권리를 침해하는 행위
3) 정보통신망 이용 불법 콘텐츠범죄	도박	정보통신망을 통하여, 체육진흥투표권이나 이와 비슷한 매체를 발행하는 시스템을 이용하여 도박을 하거나 하게 하는 행위, 스포츠 경주를 이용하여 도박을 하거나 하게 하는 행위, 또는 이외의 방법으로 영리의 목적으로 도박을 하거나 도박 사이트를 개설하여 도박을 하게 하는 행위
	명예훼손·모욕	정보통신망을 통하여, 다른 사람의 명예를 훼손하는 행위 또는 공연히 사람을 모욕하는 행위
	음란물	정보통신망을 통하여, 일반 보통사람의 성욕을 자극하여 성적 흥분을 유발하고 정상적인 성적 수치심을 해하여 성적 도의 관념에 반하는 내용의 표현물을 배포, 판매, 임대, 전시하는 행위
	스토킹	정보통신망을 통하여, 공포심이나 불안감을 유발하는 부호, 문언, 음향, 화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 행위

\* 위 사이버범죄의 유형은 경찰청 사이버안전국의 사이버범죄 유형 기준에 의거하여 분류함  
(참조: <https://cyber.go.kr/share/sub3.jsp?mid=030300>).

정보통신망침해 범죄는 정당한 접근 권한 없이 또는 허용된 접근 권한을 넘어 정보통신망에 침입하거나 시스템, 데이터 프로그램을 훼손, 멸실 또는 변경하게하거나 정보통신망에 장애를 발생하게 하는 범죄를 말한다. 그 예로 해킹(계정도용, 단순침입, 자료유출, 자료훼손), 서비스거부 공격, 악성프로그램(바이러스) 유포제작이 있다. 정보통신망이용 범죄는 정보통신망을 범죄의 본질적 구성요건에 해당하는 행위를 주요 수단으로 이용하는 범죄를 말한다. 즉, 컴퓨터 시스템을 전통적인 범죄를 행하기 위하여 이용하는 범죄를 말한다. 그 예로 인터넷 사기(직거래 사기, 쇼핑몰 사기, 게임 사기), 사이버금융 범죄(피싱, 파밍, 스미싱, 메모리해킹, 몸캠), 개인위치정보 침해, 저작권 침해, 스팸메일 발송이 있다. 불법콘텐츠 범죄는 정보통신망을 통하여 법률에서 금지하는 재화, 서비스 또는 정보를 배포, 판매, 임대, 전시하는 범죄

즉, 정보통신망을 통하여 유통되는 콘텐츠 자체가 불법적인 범죄를 말한다. 그 예로 음란물, 도박(스포츠, 경마, 경륜, 경정), 명예훼손·모욕, 스토킹이 있다.

사이버범죄를 유형별로 살펴보면, 2018년 9월까지 정보통신망침해 범죄는 2,192건으로 2%, 불법콘텐츠 범죄는 15,527건으로 14.3%, 정보통신망이용 범죄는 91,106건의 83.7%로 가장 높은 발생비율을 차지하였다. 특히, 인터넷 사기가 82,716(76.0%)으로 가장 높은 비율을 차지하였으며, 직거래 사기가 55,734건으로 전년도에 비해 6.1% 증가하였다. 급증한 사이버범죄 비율로는 피싱이 1,195건으로 전년도 392건에 비해 무려 304.8% 급증하였다. 그 밖에, 사이버범죄의 세부 유형 가운데 전년동기 대비 증가한 사이버범죄로는 사이버 명예훼손·모욕이 9,760건에서 11,236건으로 15.1% 증가하였다. 이와 관련한 대표적인 사례로

거래 및 금융 관련하여 특히, 명절 전후에 선물, 승차권 판매 등을 빙자한 인터넷 사기와 명절이나 택배 등을 가장한 스미싱 등의 범죄가 발생하고 있다. 그 밖에, 카카오톡 메시지를 통하여 사용자의 명의를 도용하여 지인인 척 돈을 빌려달라고 하는 카톡피싱도 증가하고 있다.<sup>1)</sup> 또한, 사이버 명예훼손 관련해서는 최근 정준영 동영상 사건을 둘러싸고 근거 없는 여자 연예인들의 이름이 담긴 글이 빠르게 퍼지면서 이름이 언급된 연예인들은 심각한 피해를 받고 있다.<sup>2)</sup> 즉, 확인되지 않은 내용 또는 사실이더라도 개인의 은밀한 사생활과 관련하여 명예를 훼손하는 내용을 인터넷 커뮤니티나 채팅방을 통해 퍼뜨리는 사례가 증가하며 문제가 되고 있다. 그리하여, 본 연구에서는 최근 그 발생율이 급증하고 있는 정보통신망이용 범죄의 금융과 거래를 통한 범죄와 불법콘텐츠 범죄의 명예훼손·모욕의 세 가지 사이버범죄에 집중하여 조사하고자 한다.

### 2.3 사이버 범죄 관련 선행 연구

사이버범죄는 일반적으로 사이버 공간에서 발생하는 범죄를 일컫는다(정완, 2009). 현재 사이버 공간에서는 다양한 유형의 사이버범죄가 발생하고 있으며 이는 기존의 오프라인에서의 범죄 행위가 사이버공간으로 옮겨 행해지거나 사이버공간이라는 새로운 공간의 등장과 함께 새로운 유형의 범죄가 발생하기도 한다. 사이버범죄는 비대면성, 익명성의 특징으로 사이버공간에서 자신의 신분을 노출하지 않고 활동을 하는 것이 가능하므로 범행 행위가 더 과격하고 대범해지고 있다. 게다가, 시간과 공간의 제약 없이 누구든지 쉽게 사이버공간에 접속할 수 있으므로 더 많은 범죄의 기회가 제공될 수 있다. 또한, 정보의 과급력이 큰 사이버

공간에서의 범죄 행위는 일반 범죄에 비해 더 큰 피해를 가져다주면서 최근 심각한 사회문제로 대두되고 있으므로 이를 예방 및 대처할 수 있는 실질적인 방안이 필요하다.

사이버범죄 관련 선행연구는 관점에 따라 개념 및 특징적 관점, 법/제도적 관점, 피해 요인적 관점의 연구로 구분할 수 있었다. 개념 및 특징적 관점의 연구로는 사이버범죄의 개념적 정의를 통하여 유추된 특징을 기반으로 한 사이버범죄의 대응방안(이규안, 2012), 사이버범죄의 원인과 실태를 간단히 살펴보고 이에 따른 정책적 대응책 제시(정완, 2009), 그리고 사이버범죄의 유형을 구분하고 각 유형의 범죄에 대한 원인, 대책, 그리고 차이를 나타낸 연구(이성식, 2018)가 있었다. 그 밖에, 사이버범죄의 유형 중에서 사이버 명예훼손의 원인과 해결책을 제시하고자 온라인 악플과 선플의 원인 및 대응방안(Lee and Kim, 2015)의 연구가 있었다. 법/제도적 관점의 연구로는 사이버범죄의 처벌 범규의 현황과 문제점을 토대로 그 처벌 문제점에 대한 대응방안을 제시한 연구(강동범, 2007; 곽병선, 2008)와 사이버범죄의 법과 정책 마련(Ajayi, 2016)의 연구가 있었다. 마지막으로 피해 요인적 관점의 연구로는 인터넷 채팅에서 청소년의 사이버범죄에 대한 피해요인을 기반으로 그 피해요인에 대한 대응방안(이춘화, 2009)과 SNS를 기반으로 한 사이버범죄의 심각성을 조사하고 이에 대한 문제점과 대응방안(성용은, 박준호, 2018)의 연구가 있었다. 그 밖에 사이버범죄의 영향(Nasution *et al.*, 2018; Riek *et al.*, 2016)에 대한 연구가 있었다. 이와 같은 선행 연구들은 사이버범죄의 개념 및 특징, 법/제도적 문제점 또는 사이버범죄의 피해 요인을 중심으로 그 특징 및 발생원인을 밝혀내고 이를 기반으로 사이버범죄의 대응방안을 제시하였다. 그 밖에, 사이버범죄의 피해가 사이버범죄의 가해에 미치는 영향과 이를 설명하는 이론을 제시한 연구(이성식, 2015), 사이버범죄가 재정적 부문에 미치는 영향과 관련한 연구(Lagazio *et al.*, 2014) 등이 있었다.

1) 울산매일UTV, 2019.02.19., <http://www.iusm.co.kr/news/articleView.html?idxno=835812>.  
 2) 스타투데이, 2019.03.12., <http://star.mk.co.kr/v2/view.php?mc=ST&year=2019&no=148996>.

특히, 기존 사이버범죄 관련 연구들은 사이버범죄의 유형별 또는 문제점에 따른 대응방안들을 제시하고 있었다. 정완(2009)은 사이버범죄의 원인과 문제점을 파악하고, 이를 기반으로 사이버윤리교육 강화, 사이버모욕죄 입법의 필요성, 인터넷 루어링 금지, 인터넷 실명제 실시 등의 대응방안을 제시하였다. 이성식(2018)은 사이버범죄의 유형을 구분하고, 각 사이버범죄 유형별 대책을 나타내었다. 즉, 불법콘텐츠범죄는 낮은 자기통제력의 영향에서 윤리의식이, 정보통신망이용재산범죄는 이득의 영향에서 공식처벌이, 그리고 신종침해범죄는 성적부진의 영향에서 기회제약이 각각 완충작용을 하는 것을 제시하였다. Lee and Kim(2015)은 온라인 댓글문화의 문제점으로 익명성, 책임감 결여, 규율과 처벌 부족 등을 나타내었고, 개선방안으로는 인터넷 교육프로그램 및 캠페인, 실명제 실시, 규율 강화 등을 제시하였다. 강동범(2007)은 사이버범죄의 문제점에 대한 대응방안으로 사이버공간에서의 전통적 범죄와 새로운 범죄에 대한 입법적 대책들을 제시하였다. Ajayi(2016)은 현재 사이버범죄의 문제점들을 해결하는데 노력하고, 보편적인 법 마련에 힘을 쓸 것을 제안하였다. 하지만, 기존 연구들에서 조사한 사이버범죄의 발생원인 및 문제점은 기존문헌을 이용하거나 일반인을 대상으로 사이버범죄의 원인을 유추하는 간접적인 접근방법에 의해 조사되었다. 즉, Lee and Kim(2015)과 이성식(2018)은 일반인을 대상으로 조사하여 그 원인 및 대응방안을 제안하였고, 성용은, 박준호(2018)와 정완(2009)은 관련 사이트 및 선행연구를 이용한 문헌연구의 방법을 이용하였다. 그리하여, 본 연구에서는 사이버범죄의 유형을 세분화하고, 각 유형의 사이버범죄를 저지른 실제 피의자 인터뷰를 통하여 범행의 동기, 방법, 범행대상, 이용매체 등을 조사하여 기존 연구들과 차별화하고자 한다. 더불어, 인터뷰를 통해 도출된 주요 결과 요인들 간의 관계를 분석하여 시각화함으로써 그 해석을 돕는다.

### III. 연구방법론

#### 3.1 정성적 연구: 인터뷰 방법

정성적 연구방법은 현상학적 접근법 또는 해석주의 접근법에 바탕을 둔 접근법으로 현상에 대한 세밀한 기술을 통해 다양한 측면의 관계를 파악함으로써 상황적 이해를 제공한다. 정성적 연구의 특징으로는 연구자의 입장에서 첫째, 경험이 가장 의미 있는 자료라고 믿고 실제 경험 대상자를 인터뷰하는 등 대상자를 연구에 참여시키고자 한다. 둘째, 실제의 본질 또는 그 변화과정에 더 관심이 있다. 셋째, 연구하려는 대상에 대한 완전하고 전체적인 것을 얻으려고 하기 때문에 방대한 자료를 필요로 한다. 넷째, 연구 의도에 있어 대상자가 경험한 의미를 이해하는 것이 중요하다고 생각하기 때문에 각 대상자의 생각인 주관적 자료에 초점을 둔다(백혜주, 정주현, 2013). 정성적 연구는 이러한 특징들을 기반으로 대상자의 행동에 대한 근본적인 이유와 동기에 대한 심층적 정보를 얻을 수 있고, 주제 및 사안에 대하여 심도 있게 이해할 수 있다. 특히, 정성적 연구 방법 중 인터뷰 방법은 조사하고자 하는 주제 및 사안에 대하여 일대일 환경에서 충분히 이해할 수 있어 심층적인 정보를 수집할 수 있다. 특히, 인터뷰 방법은 현상에 대한 충분한 이해와 추론이 가능하여 탐구하고자 하는 현상의 본질을 비교적 자세히 관찰할 수 있는 강점이 있다(Yin, 2013).

본 연구에서는 사이버범죄를 정보통신망침해범죄, 정보통신망이용 범죄 및 정보통신망 이용불법콘텐츠 범죄의 세 가지 유형으로 구분하고, 그 중에서 최근 그 발생율이 급증하고 있는 정보통신망이용 범죄의 사이버 거래와 금융, 그리고 불법콘텐츠 범죄의 사이버 명예훼손·모욕의 범죄 요인들을 밝혀내고자 한다. 이를 위하여 본 연구에서는 해당 실제 피의자들을 대상으로 인터뷰를 실시하여 관련 범행 요인들의 심층적 정보를 얻고자 하였다. 즉, 사이버범죄의 해당 유형별

사례에 대하여 실제 범행 피의자 또는 담당 수사관을 상대로 인터뷰하고, 추가적으로 담당 수사관이 피의자를 조사하며 작성한 조사기록을 참고자료로 이용한다. 그리하여, 인터뷰 결과 및 조사기록의 자료를 통하여 실제 사이버범죄 피의자들의 개인 및 범행 환경을 분석하여 유형별 사이버범죄에 따른 예방 및 대응방안을 제안할 수 있다.

### 3.2 연구 설계 및 자료 수집

자료의 수집은 사이버범죄의 유형 중, 정보통신망이용 범죄의 사이버 거래와 금융과 정보통신망이용 불법콘텐츠 범죄의 사이버 명예훼손·모욕에 해당하는 것으로 하였다. <표 2>는 본 연구에서 인터뷰를 위한 질문 내용을 나타낸 것이다.

구성된 인터뷰 내용을 바탕으로 해당 범죄를 저지른 피의자 또는 수사관을 인터뷰하거나, 해당 담당 수사관이 조사하며 기록한 조사기록을 참고하는 방법으로 진행하였다.

사이버범죄에 대한 피의자 인터뷰 등 자료수집은 2010년부터 2015년까지 강원도 지역을 관할하는 경찰서 사이버범죄 수사팀에 접수되어 기소의견을 검찰청에 송치된 사건들을 기준으로 하였다. 본 연구에서는 정보통신망이용 범죄의 금융 19건, 거래 14건의 총 33건의 사례를 수집하고, 불법콘텐츠 범죄의 명예훼손·모욕은 41건의 사례를 수집하였다. 자료 수집은 해당 범죄행위를 한 피의자 42명과 그 피해자들을 조사한 담당 수사관 4명을 인터뷰하였고, 해당 담당 수사관이 조사를 하며 기록한 피의자신문조서 74건을 참고하였다.

<표 2> 인터뷰 질문 내용 구성

구분	질문내용
개인 환경	성별, 연령, 교육수준, 직업·업종, 소득수준, 혼인관계
범행여부	(정보통신망이용 범죄의 사이버 거래와 금융) 다른 사람을 속이거나 다른 사람의 개인정보를 권한 없이 이용하여 재산상 이익을 얻은 적이 있습니까? (불법콘텐츠 범죄의 사이버 명예훼손·모욕) 다른 사람의 명예를 훼손 및 모욕한 적이 있습니까?
범행전과	과거에 형사적 처벌을 받은 적이 있습니까?
범행대상	해당 범죄행위는 누구를 대상으로 하였습니까?
범행이용매체	어떤 경로(서비스 또는 매체)를 이용하였습니까?
범행방법	어떤 방법을 이용하였습니까?
범행가능이유	그 (범죄)행위를 할 수 있었던 이유(가능한 이유)는 무엇입니까?
범행동기	그 (범죄)행위를 한 이유 및 동기가 무엇입니까?

<표 3> 사이버범죄의 유형별 사례 수집

대분류	중분류	사례수	인터뷰
정보통신망 이용범죄	금융	19	피의자 인터뷰: 17명 수사관 인터뷰: 4명(중복) 피의자신문조서: 33건
	거래	14	
정보통신망 이용 불법콘텐츠범죄	명예훼손·모욕	41	피의자 인터뷰: 25명 수사관 인터뷰: 4명(중복) 피의자신문조서: 41건
합계		74	

### 3.3 자료 분석 방법

자료 분석은 인터뷰를 통해 수집한 자료를 사이버범죄 유형별로 구분하여 분석하고, 유형별로 구분된 사이버범죄의 특징을 바탕으로 각 사이버범죄의 예방 및 대응방안을 제안하고자 한다. 본 연구에서는 정보통신망이용 범죄의 사이버 (1) 거래와 (2) 금융, 그리고 정보통신망이용 불법콘텐츠 범죄의 사이버 (3) 명예훼손·모욕의 세부 유형의 사이버범죄에 대하여 분석을 진행하였다. 자료 분석은 설계된 인터뷰 내용을 피의자 또는 피의자를 조사한 담당 수사관에게 질문하고, 질문에 대한 답변을 최대한 상세하게 기록하여 추출하거나 또는 해당 담당 수사관이 기록한 조사기록의 내용에서 인터뷰 내용 구성에 따른 질문에 대한 답변을 최대한 상세하게 추출하였다. 추출된 내용의 문자열들을 바탕으로 특정 주제나 이름으로 범주화시켜 하나의 분석 단위를 생성함으로써 분석 대상이 될 자료와 그렇지 않은 자료를 구분하였다. 분석 대상의 자료는 코딩분석 방법을 통하여 그 내용이나 의미를 개념화시켰다.

초기 코딩분석은 사이버범죄의 발생원인을 밝혀내기 위하여 인터뷰를 진행할 때, 성별, 연령, 소득수준, 학력수준, 직업·업종, 가족관계의 개인 환경 요인과 범행동기, 범행가능이유, 범행방법, 범행이용매체, 범행대상 및 범행전과의 범행 환경 요인의 12개 항목을 요인으로 보고 진행하였으므로 이를 마스터 리스트(Master List)로 한 사전 코드분석 방법으로 진행하였다. 이후 코딩분석을 위하여 인터뷰로 도출된 데이터 중 12개 항목의 마스터 리스트 범주 내에서 의미 있는 현상을 개념화하여 이들 중 유사하거나 관련성 있는 것들을 범주화하는 개방코딩(Open coding)분석을 시행하였다. 다음으로 개방코딩으로 범주화된 요인들 간의 관계를 정렬해 인과관계에 맞는 좀 더 결속된 요인들로 범주화하는 축코딩(Axial coding)분석을 진행하여 해당 현상에 대한 심도 있는 이해를 하고자 하였다(Corbin and Strauss, 1998).

마지막으로 이와 같은 범주화 작업에 신뢰도를 향상시키기 위해서 본 연구자 이외에 다른 연구자 두 명의 도움을 받아, 추출한 인터뷰 내용과 마스터 리스트 항목 및 개방코딩을 통하여 얻어진 범주화 항목을 재확인하는 동료 검사(Peer review)를 진행하였다. 이와 같은 피의자의 인터뷰 등 자료 분석으로 성별, 연령, 교육수준, 직업·업종, 소득수준, 혼인여부의 6개 항목의 개인 환경 요인과 범행동기, 범행가능이유, 범행방법, 범행이용매체(서비스), 범행대상, 범행전과의 6개 항목의 범행 환경 요인에 해당하는 발생원인의 요인을 개념화하여 도출하고 그 빈도수를 측정하여 사이버범죄의 발생과 어떤 관계가 있는지 분석하였다.

## IV. 분석결과

### 4.1 정보통신망이용 범죄: 거래

#### 4.1.1 개인 환경 분석

앞의 인터뷰 및 조사기록을 통하여 정보통신망이용 범죄의 사이버 거래는 19건의 사례에 대하여 성별, 연령대, 교육수준, 직업, 소득수준 및 혼인여부의 개인 환경에 해당하는 항목들을 나타내었다. 분석 결과, 남성이 89.47%(17명), 여성이 10.53%(2명)으로 남성이 높은 비율을 차지하였다. 연령대는 20대의 비율이 57.89%(11명)로 가장 높았고, 10대(26.32%), 30대(10.53%), 50대(5.26%)의 순으로 나타났다. 교육수준은 고등학교가 47.37%(9명), 대학교 또는 대학원이 31.58%(6명)로 높았으며, 직업은 무직이 47.37%(9명)로 가장 높은 비율을 나타내었다. 소득 수준은 130만 원 이하가 73.68%(14명)로 많았고, 미혼 비율이 94.74%(18명)로 높았다. 이를 통하여 사이버 거래의 범죄를 행한 피의자들은 대부분 20대의 미혼 남성인 것을 확인하였다. 이들은 고등학교나 대학교 또는 대학원에 진학하여 비교적 높은 수준의 교육을 받았다. 하지만, 현재 재학 및 휴학 중인 학생이거나 교육을 받은 후에 특별한 직업 없이 취업을 준비 중이거나, 취업을 하였더라도

판매업 등 낮은 소득의 파트타임 업무에 종사하여 부모에 의존하며 생활한 것으로 보였다.

#### 4.1.2 범행환경 분석

<표 4-1>과 <표 4-2>는 정보통신망 이용범죄, 사이버 거래의 범행환경 요인별 비율을 나타낸 것이다. 사이버 거래 관련 범죄행위 19건의 사례에 대하여 범행동기, 범행가능이유, 범행방법, 범행이용매체, 범행대상, 범행전과의 범행환경에 해당하는 6개 항목을 사이버범죄의 요인으로 보고 분석하였다. 첫 번째, 범행동기 요인에 있어 ‘금전’이 68.42%(13건)로 가장 높은 비율을 차지하였다. 범행동기 요인에 대하여 세부요인을 분석한 결과, ‘금전’에 해당하는 피의자는 대출금 상환을 위해서, 생활비 마련을 위해서, 용돈 마련을 위해서, 유흥비 마련을 위해서 범행을 저질렀다고 답변하였다. ‘부채’에 해당하는 피의자는 공급 부족으로 물건이 없어서, 구매자에 대한 정보가 삭제되어서, 다른 구매자에게 이미 판매가 되어서라고 답변하였다. ‘아이템’에 해당하는 피의자는 자신에게 없는 게임의 아이템을 획득하기 위해서라고 답변하였다. ‘편리’에 해당하는 피의자는 합법적으로 하는 방법보다 절차 등에 있어 편리해서라고 답변하였다. ‘충동심’에 해당하는 피의자는 자신의 아이템을 판매하는 과정에서 돈을 받고 막상 주려니 아까워서 라고 답변하였다.

실제로 인터뷰에서 범행동기를 묻는 질문에 다

음과 같이 답변하였다.

- [1] “처음부터 계정을 판매할 생각이 없었습니다. 상품권만 받을 생각이었습니다.”
- [2] “막상 돈을 입금 받으니 원래 팔기로 한 계정을 주는 게 싫었습니다.”

두 번째, 범행가능이유 요인에 있어 ‘익명/비대면’의 비율이 89.47%(17건), ‘제재없음’의 비율이 10.53%(2건)를 차지하였다. 범행가능이유 요인에 대하여 세부요인을 분석한 결과, ‘익명/비대면’에 해당하는 피의자는 상대방과 얼굴을 보지 않거나 만난 적이 없는 사람이라서 라고 답변하였다. 다음으로, ‘제재없음’에 해당하는 피의자는 상대방에게 판매한 계정이 자신의 명의로 언제든지 다시 회수할 수 있어서라고 답변하였다.

실제로 인터뷰에서 범행가능이유를 묻는 질문에 다음과 같이 답변하였다.

- [1] “물건을 받고 나면 계정 비밀번호를 변경할 생각이었습니다.”
- [2] “제가 누군지 모르기 때문에 일방적으로 연락을 받지 않았습니다.”

세 번째, 범행방법 요인에 있어 ‘빙자’의 비율이 100%(19건)를 차지하였다. 범행방법 요인에 대하여 세부요인을 분석한 결과, ‘빙자’에 해당하는 피의자는 게임이나 포털 등의 계정을 판매한다고 빙자하거나, 서점이나 쇼핑몰 등에서 사용할 수 있는

<표 4-1> ‘정보통신망이용 범죄: 거래’의 범행환경 요인별 비율

순위	범행동기			범행가능이유		
	구분	내용	빈도(%)	구분	내용	빈도(%)
1	금전	대출금 상환, 생활비 마련, 용돈 마련, 유흥비 마련	13(68.42)	익명/비대면	익명/비대면	(89.47)
2	부채	공급 부족, 구매자 정보, 판매 물건	3(15.79)	제재없음	회수 가능(자신 명의)	(10.53)
3	아이템	아이템 획득	1(5.26)			
4	편리	합법보다 편리	1(5.26)			
5	충동심	아까워서(아이템)	1(5.26)			

사이버머니를 판매한다고 빙자하거나, 청소년들을 대상으로 연예인에 대한 관람티켓을 판매한다고 빙자하였다고 답변하였다.

실제로 인터뷰에서 범행방법을 묻는 질문에 다음과 같이 답변하였다.

- [1] “제가 사이버머니 1억 원을 현금 85,000원으로 바꾸자고 채팅으로 이야기했습니다.”
- [2] “계정을 판매할 생각이 없었습니다. 물건을 받으면 계정 비밀번호를 변경할 생각이었습니다.”

네 번째, 범행이용매체 요인에 있어 ‘사이트’가 89.47%(17건), ‘메신저’의 비율이 10.53%(2건)를 차지하였다. 범행이용매체에 대하여 세부요인을 분석한 결과, ‘사이트’에 해당하는 피의자는 네이버 중고나라, 스마트폰 앱 번개장터 등 중고물품 거래사이트 서비스를 이용하거나, 바람의 나라, 쇼프메거진 등 게임사이트 서비스를 이용하거나, 아이템매니아 등 게임 아이템 거래사이트 서비스를 이용하였다고 답변하였다.

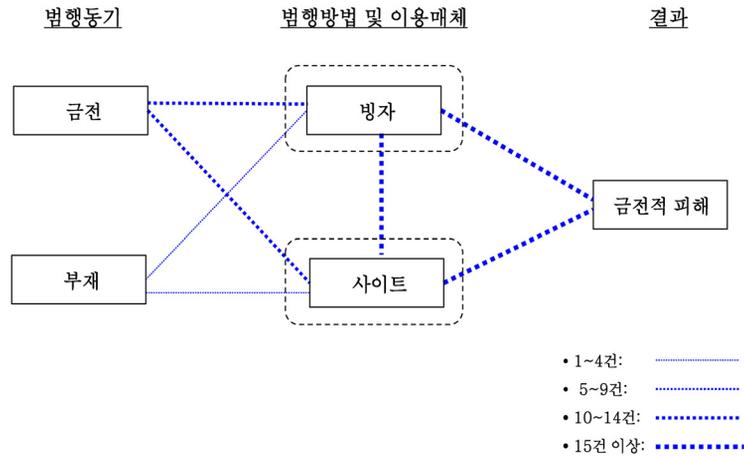
다섯 번째, 범행대상 요인에 있어 ‘무관’의 비율이 100%(9건)를 차지하였다. 여섯 번째, 범죄전과 요인에 있어 ‘전과없음’과 ‘전과 2~5범’의 비율이 각각 26.32%(5건), ‘전과 1범’의 비율이 21.05%(4건), ‘전과 6~9범’의 비율이 15.79%(3건), ‘전과 10~19범’의 비율이 10.53%(2건)를 차지하였다. 또한 범행전과가 있는 피의자 중 동일전과를 보유하고 있는 피의자는 2~5범 5건 중 3건, 1범 4건 중

3건, 6~9범 3건 중 1건, 10~19범 2건 중 2건을 차지하였다.

범행동기 요인에 있어 합이 50% 이상의 비율을 차지하고 있는 ‘금전’에 대하여 다른 요인들과 관계를 분석하였다. 범행가능이유 요인에 대하여 분석한 결과, 범행동기 요인이 ‘금전’인 13건의 사건 모두 ‘익명성/비대면성’으로 확인되었다. 범행방법 요인에 대하여 분석한 결과, 13건 사건 모두 ‘빙자’로 확인되었다. 마지막으로 범행이용매체 요인에 대하여 분석한 결과, 모두 ‘사이트’로 확인되었다. 또한, 정보통신망 이용범죄(사이버 거래)는 대부분 범죄전과 초범부터 5범까지인 전과가 있는 피의자에 의해서 일어났으며 전과 1범부터 5범까지의 경우 동일 범행의 비율이 66.67%(9건 중 6건)로 매우 높았다. 더불어 네트워크 분석을 통하여 범행환경의 주요 요인들 간의 관계를 살펴본 결과, ‘금전 또는 부재-빙자-메신저-금전적 피해’의 요인들 간의 관계를 확인할 수 있었다. 즉, 범행동기로 대출금이나 생활비 등의 금전적인 문제가 많았으며 이를 해결하기 위하여 해당 범죄를 저지를 경우에 의류, 전자제품 등의 물품, 사이버머니, 게임이나 포털 계정 등을 판매한다고 빙자하여 사이트에 게시한 후 다른 소비자들과 메신저로 소통하여 금전을 지불하게 한다는 것이다. 관련 실제 사례 중에는 숙박권 사기의 형태로 호텔이나 펜션 등의 사용권을 저렴하게 판매한다고 중고거래 게시판에 글을 올린 후 메신저 연락을 통해 금액만 받고 연락을 끊는 수법이 있었다.

〈표 4-2〉 ‘정보통신망이용 범죄: 거래’의 범행환경 요인별 비율

순위	범행방법			범행이용매체		
	구분	내용	빈도(%)	구분	내용	빈도(%)
1	빙자	계정 판매 빙자, 사이버머니 판매 빙자, 의류 판매 빙자, 잡화 판매 빙자, 전자제품 판매 빙자, 조건만남 빙자, 티켓 판매 빙자	19(100)	사이트	네이버 중고나라, 바람의 나라, 번개장터, 쇼프메거진, 아이템매니아	17(89.47)
2				메신저	카카오톡, 틱톡	2(10.53)



〈그림 1〉 ‘정보통신망이용 범죄: 거래’의 범행환경 주요 요인들 간의 관계

## 4.2 정보통신망이용 범죄: 금융

### 4.2.1 개인 환경 분석

정보통신망 이용범죄의 사이버 금융과 관련된 범죄행위 14건의 사례에 대하여 성별, 연령대, 교육수준, 직업, 소득수준 및 혼인여부의 개인 환경에 해당하는 항목들을 나타내었다. 분석 결과, 남성의 비율이 100%(14명)를 차지하였으며, 연령대는 20대가50%(7명)로 가장 높았고 10대(42.86%), 30대(7.14%)순이었다. 교육수준은 고등학교가 64.29%(9명)로 가장 높았으며, 직업은 학생(50%)과 판매업(35.71%)이 가장 많았다. 소득은 월평균 130만원 이하가 71.43%(10명)로 가장 높은 비율을 보였으며, 미혼이 92.86%(13명)로 대부분이었다. 이를 통하여 정보통신망이용 범죄의 금융 부분도 거래 부분과 유사하게 피의자들 대부분이 10대와 20대의 미혼 남성들인 것으로 나타났다. 이들 또한 현재 직업이 학생이거나 파트타임을 포함한 판매업이 대부분인 것으로 나타났다.

### 4.2.2 범행환경 분석

<표 5-1>과 <표 5-2>은 정보통신망 이용범죄의 사이버 금융의 범행환경 요인별 비율을 나타낸 것이다. 정보통신망 이용범죄의 사이버 금융과 관련

된 범죄행위 14건의 사례에 대하여 범행동기, 범행가능이유, 범행방법, 범행이용매체, 범행대상, 범행전과의 범행환경에 해당하는 6개 항목을 사이버범죄의 요인으로 보고 분석하였다. 첫 번째, 범행동기 요인에 있어 ‘아이템’의 비율이 42.86%(6건), ‘충동심’의 비율이 35.71%(5건), ‘금전’의 비율이 21.43%(3건)를 차지하였다. 범행동기 요인에 대하여 세부요인을 분석한 결과, ‘아이템’에 해당하는 피의자는 아이템 획득을 위해서라고 답변하였다. ‘충동심’에 해당하는 피의자는 복수하고 싶은 마음에 충동적으로, 호기심이 생겨서라고 답변하였다. ‘금전’에 해당하는 피의자는 생활비 마련을 위해서, 유흥비 마련을 위해서라고 답변하였다.

실제로 인터뷰에서 범행동기를 묻는 질문에 다음과 같이 답변하였다.

- [1] “저녁에 술을 한 잔 마시고 게임을 하다가 게임아이템인 루비가 모자라 구입을 하려는데 제 핸드폰으로 소액결제가 안되었습니다. 그래서 000의 핸드폰으로 접속을 했습니다.”
- [2] “000의 휴대폰으로 게임을 하다가 아이템이 필요해서 별생각 없이 결제하였습니다.”

두 번째, 범행가능이유 요인에 있어 ‘익명/비

대면'의 비율이 50%(7건), '제재없음'의 비율이 50%(7건)를 차지하였다. 범행가능이유에 대하여 세부요인을 분석한 결과, '익명/비대면'에 해당하는 피의자는 상대방과 얼굴을 보지 않거나 만난 적이 없는 사람이라서 라고 답변하였다. '제재없음'에 해당하는 피의자는 비밀번호 등 잠금장치가 설정되지 않아 언제든지 접근할 수 있어서라고 답변하였다.

실제로 인터뷰에서 범행가능이유를 묻는 질문에 다음과 같이 답변하였다.

- [1] “제가 위병소 근무라 들어가는 사람이 휴대폰을 저한테 맡기고 가야했고, 그 사람의 휴대폰에 비밀번호가 설정되어 있지 않았습다.”
- [2] “그때 000과 사귀고 있었기 때문에 자유롭게 휴대폰을 이용할 수 있었습니다.”

세 번째, 범행방법 요인에 있어 '결제'의 비율이 100%(14건)를 차지하였다. 범행방법에 대하여 세부요인을 분석한 결과, '결제'에 해당하는 피의자는

개인정보를 이용하여 계정을 해킹하고 아이템을 결제하거나, 전화번호/인증번호를 알아내어 아이템을 결제하였다고 답변하였다.

실제로 인터뷰에서 범행방법을 묻는 질문에 다음과 같이 답변하였다.

- [1] “000이 소유하고 있는 핸드폰을 이용하여 아이템을 결제했습니다.”
- [2] “000의 핸드폰을 이용하여 게임 사이트에서 인증을 받아 소액결제를 했습니다.”

네 번째, 범행이용매체 요인에 있어 '사이트'의 비율이 92.86%(13건), '메신저'의 비율이 7.14%(1건)를 차지하였다. 범행이용매체에 대하여 세부요인을 분석한 결과, '사이트'에 해당하는 피의자는 아이템 거래 사이트, 게임 사이트 서비스 또는 아이템 중계 사이트 서비스를 이용하였다고 답변하였다. '메신저'에 해당하는 피의자는 카카오톡 서비스를 이용한다고 답변하였다.

다섯 번째, 범행대상 요인에 있어 무관인 경우가 57.14%(8건), 연인, 이웃, 친구, 선후배, 거래,

〈표 5-1〉 '정보통신망이용 범죄: 금융'의 범행환경 요인별 비율

순위	범행동기			범행가능이유		
	구분	내용	빈도(%)	구분	내용	빈도(%)
1	아이템	아이템 획득	6(42.86)	익명/비대면	익명/비대면	7(50)
2	충동심	복수심, 동조, 합법으로 생각, 호기심	5(35.71)	제재없음	비밀번호 미설정	7(50)
3	금전	생활비 마련, 유흥비 마련	3(21.43)			

〈표 5-2〉 '정보통신망이용 범죄: 금융'의 범행환경 요인별 비율

순위	범행방법			범행이용매체		
	구분	내용	빈도(%)	구분	내용	빈도(%)
1	결제	계정 해킹하여 아이템 결제, 전화번호/인증번호 알아내어 아이템 결제, 휴대폰 이용 상품권 결제, 휴대폰 이용 아이템 결제	14(100)	사이트	sk플래닛, 구글플레이스토어, 넥슨, 아이템매니아, 아이템베이, 엔씨소프트, 엠게임, 티스토어, 한게임	13(92.86)
2				메신저	카카오톡	1(7.14)

가족의 비율이 각각 7.14%(1건)를 차지하였다. 여섯 번째, 범죄전과 요인에 있어 전과없음과 전과 1범의 비율이 42.86%(6건), 전과없음의 비율이 35.71%(5건), 전과 10~19범의 비율이 14.29%(2건), 전과 2~5범의 비율이 7.14%(1건)를 차지하였다. 또한 범행전과가 있는 피의자 중 동일전과를 보유하고 있는 피의자는 1범 6건 중 2건, 10~19범 2건 중 2건을 차지하였다.

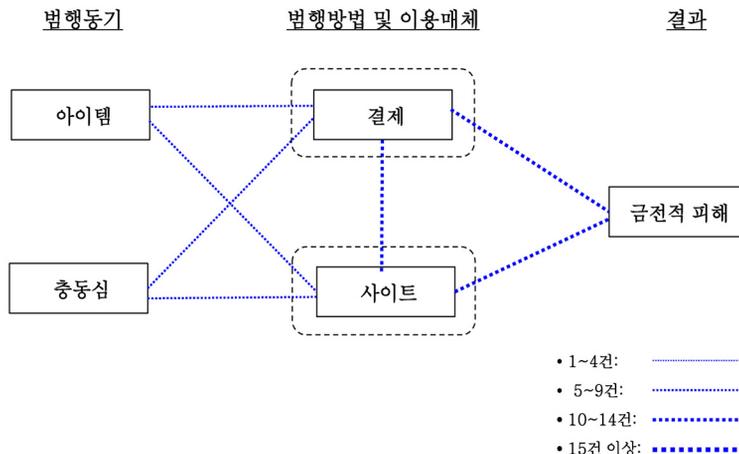
범행동기 요인에 있어 합이 50% 이상의 비율을 차지하고 있는 ‘아이템’, ‘충동심’에 대하여 다른 요인들과 관계를 분석하였다. 정보통신망 이용범죄의 금융 관련 범죄행위는 대부분 범죄전과 초범과 1범인 피의자에 의해서 일어났으며 전과 1범의 경우 동일 전과의 비율이 33.33%(6건 중 2건)로 다소 높았다. 범행동기는 인터넷 게임의 캐릭터 장비 등 아이템을 획득 및 사용하기 위한 것이 대부분이었으며, 범행이 가능했던 이유는 정보통신망 이용범죄의 거래부분과 같이 익명·비대면으로 상대방이 피의자를 알 수 없다고 생각하기 때문이거나, 피해자의 휴대폰을 이용하여 범행을 할 때 휴대폰에 비밀번호가 설정되지 않는 등 제재를 당하지 않았기 때문으로 보였다. 더불어 네트워크 분석을 통하여 범행환경의 주요 요인들 간의 관계를 살펴본 결과, ‘아이템 또는 충동심-결제-사이트

-금전적 피해’의 범행 요인들 간의 관계를 확인할 수 있었다. 즉, 인터넷 게임의 캐릭터장비 또는 아이템을 얻거나 호기심의 이유로 타인의 휴대폰이나 아이디를 통해 게임사이트 등에 접속하여 결제하여 금전을 갈취하는 방법이다. 관련 실제 사례 중에는 인터넷 게임의 아이템을 얻기 위해서 다른 사람의 휴대폰 또는 아이디를 도용하여 게임 사이트에 접속한 후 결제하는 수법이다.

### 4.3 정보통신망이용 불법콘텐츠 범죄: 명예훼손·모욕

#### 4.3.1 개인 환경 분석

정보통신망 이용 불법콘텐츠범죄의 사이버 명예훼손·모욕 관련 범죄행위 41건의 사례에 대하여 성별, 연령대, 교육수준, 직업, 소득수준 및 혼인여부의 개인 환경에 해당하는 항목들을 나타내었다. 분석 결과, 남성의 비율이 70.73%(29명)로 대부분 차지하였으며, 연령대는 20대의 비율이 36.59%(15명)로 가장 높았으며 30대, 40대는 각각 24.39%(10명)였다. 교육수준은 대학교 또는 대학원이 51.22%(22명), 고등학교가 43.9%(18명)를 차지하였다. 직업은 파트타임을 포함한 판매업이 39.02%(16명)로 가장 많았고 다음으로 학생의 비율이 24.39%(10명)를



〈그림 2〉 ‘정보통신망이용 범죄: 금융’의 범행환경 주요 요인들 간의 관계

차지하였다. 마지막으로 소득수준은 월평균 130만 원 이하가 60.98%(25명)로 가장 많았으며 미혼의 비율이 78.05%(32명)로 높았다.

4.3.2 범행환경 분석

<표 6-1>과 <표 6-2>는 불법콘텐츠범죄, 사이버 명예훼손·모욕의 범행환경 요인별 비율을 나타낸 것이다. 불법콘텐츠범죄의 사이버 명예훼손·모욕의 41건의 사례에 대하여 범행동기, 범행가능이유, 범행방법, 범행이용매체, 범행대상, 범행진과의 범행환경에 해당하는 6개 항목을 사이버범죄의 요인으로 보고 분석하였다. 첫 번째, 범행동기 요인에 있어 ‘충동심’의 비율이 87.8%(36건), ‘폭로’의 비율이 12.2%(5건)를 차지하였다. 범행동기 요인에 대하여 세부요인을 분석한 결과, ‘충동심’에 해당하는 피의자는 지루해서, 게시글을 보고 조롱하고 싶어서, 게시글을 보고 짜증나서, 게시글을 보고 충고하고 싶어서, 게시글을 보고 화나서, 상대방의 언행에 짜증나서 답변하였다. ‘폭로’에 해당하는 피의자는 들은 내용을 알리기 위해서, 상대방의 언행을 알리기 위해서라고 답변하였다.

실제로 인터뷰에서 범행동기를 묻는 질문에 다음과 같이 답변하였다.

- [1] “제 전화를 받지 않고, 문자에도 응답을 해주지 않아 화가 나서 해당 댓글을 남겼습니다.”
- [2] “치아가 잘못 치료 되었는데 의사가 진료에

대하여 반성하는 모습이 느껴지지 않아서 화나고 다른 사람들이 그 의사에게 당할까 봐 글을 올리게 되었습니다.”

두 번째, 범행가능이유 요인에 있어 ‘제재없음’의 비율이 100%(41건)를 차지하였다. 범행가능이유에 대하여 세부요인을 분석한 결과, ‘제재없음’에 해당하는 피의자는 아무런 제재 없이 자신의 생각을 표현하여 글을 쓸 수 있고 또한 신분을 밝히지 않고 글을 쓸 수 있어서라고 답변하였다. 실제로 인터뷰에서 범행가능이유를 묻는 질문에 다음과 같이 답변하였다.

- [1] “제 계정으로 글을 남기는 데 별다른 어려움 점이 없습니다.”
- [2] “제 블로그라 글을 쓰는 건 제 마음입니다.”

세 번째, 범행방법 요인에 있어 ‘유포’의 비율이 100%(41건)를 차지하였다. 범행방법에 대하여 세부요인을 분석한 결과, ‘유포’에 해당하는 피의자는 사실을 유포하거나 허위 사실을 유포하였다고 답변하였다.

실제로 인터뷰에서 범행방법을 묻는 질문에 다음과 같이 답변하였다.

- [1] “OOO이 홍보를 위해서 작성한 글에 댓글로 해당 내용을 썼습니다.”
- [2] “제 블로그에 엄마가 O치료에서 치료를 받았던 내용을 글로 썼습니다.”

<표 6-1> ‘정보통신망이용 불법콘텐츠 범죄: 명예훼손·모욕’의 범행환경 요인별 비율

순위	범행동기			범행가능이유		
	구분	내용	빈도(%)	구분	내용	빈도(%)
1	충동심	무료함, 조롱심(게시글 보고), 짜증남(게시글 보고), 충고(게시글 보고), 동조, 측은해서(게시글 보고), 화풀이(게시글 보고), 화풀이(상대방 언행), 짜증남(상대방 언행), 화풀이(타인 언행), 억울함(상대방 언행)	36(87.8)	제재없음	업로드 가능	41(100)
2	폭로	알리기 위함(들은 내용), 알리기 위함(상대방 언행), 알리기 위함(타인 언행)	5(12.2)			

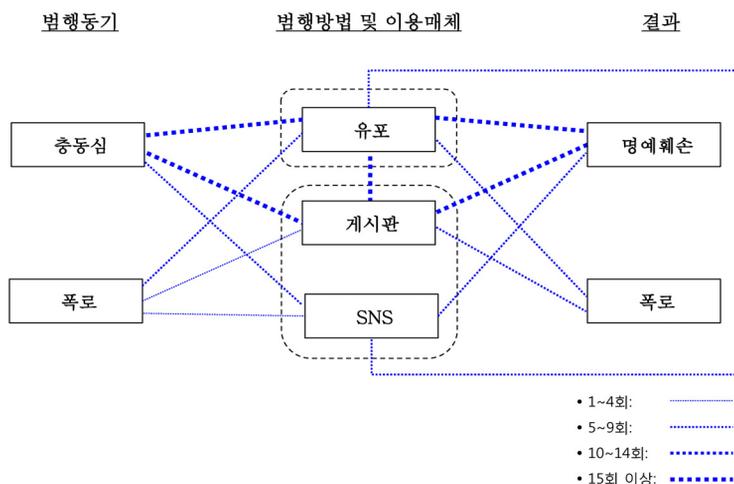
〈표 6-2〉 '정보통신망이용 불법콘텐츠 범죄: 명예훼손·모욕'의 범행환경 요인별 비율

순위	범행방법			범행이용매체		
	구분	내용	빈도(%)	구분	내용	빈도(%)
1	유포	사실 유포, 허위사실 유포	41(100)	게시판	강원대학교, 네이버, 다음, 바람 놀이터, 서울대학교, 춘천강변 코아루 춘천시, 테니스클럽연합회, 한림대학교, 한서중학교	34(82.93)
2				SNS	네이버 블로그, 밴드, 카카오토리, 페이스북	7(17.07)

네 번째, 범행이용매체 요인에 있어 '게시판'의 비율이 82.93%(34건), 'SNS'의 비율이 17.7%(7건)를 차지하였다. 범행이용매체에 대하여 세부요인을 분석한 결과, '게시판'에 해당하는 피의자들은 학교 게시판, 포털 사이트, 게임 게시판, 공공집단 게시판 등 다양한 게시판을 이용하여 해당 범죄를 저질렀다. 'SNS'에 해당하는 피의자는 네이버 블로그, 밴드, 카카오토리, 페이스북 등을 이용하였다고 답변하였다. 다섯 번째, 범행대상 요인에 있어 무관의 비율은 70.73%(29건), 거래의 비율은 9.76%(4건), 고용의 비율은 7.32%(3건), 동호회원, 선후배의 비율은 각각 4.88%(2건), 연인의 비율은 2.44%(1건)를 차지하였다. 여섯 번째, 범죄전과 요

인에 있어 전과없음의 비율은 56.1%(23건), 전과 1범의 비율이 19.51%(8건), 전과 2~5범은 12.2%(5건), 전과 6~9범, 전과 10~19범의 비율은 각각 4.88%(2건), 전과 20~29범의 비율은 2.44%(1건)를 차지하였다. 또한 범행전과가 있는 피의자 중 동일전과를 보유하고 있는 피의자는 1범 8건 중 3건을 차지하였다.

범행동기 요인에 있어 합이 50% 이상의 비율을 차지하고 있는 '충동심', '폭로'에 대하여 다른 요인들과 관계를 분석하였다. 범행가능이유 요인에 대하여 분석한 결과, '충동심' 36건과 '폭로' 12건 모두 '제재없음'으로 확인되었다. 범행방법 요인에 대하여 분석한 결과, '충동심' 36건과 '폭로' 12



〈그림 3〉 '정보통신망이용 불법콘텐츠 범죄: 명예훼손·모욕'의 범행환경 주요 요인들 간의 관계

건 모두 ‘유포’로 확인되었다. 범행이용매체 요인에 대하여 분석한 결과, ‘충동심’ 36건 중 31건은 ‘게시판’, 5건은 ‘SNS’로 확인되었고, 다음으로 ‘폭로’ 5건 중 3건은 ‘게시판’ 2건은 ‘SNS’로 확인되었다. 더불어 네트워크 분석을 통하여 범행환경의 주요 요인들 간의 관계를 살펴본 결과, ‘충동심-유포-게시판-명예훼손 또는 모욕’, ‘폭로-유포-게시판 또는 SNS-명예훼손 또는 모욕’의 요인들 간의 관계를 확인할 수 있었다. 즉, 온라인 게시판을 보다가 특정 게시글에 짜증이 나서 충동적으로 악의적인 글을 남겨 유포함으로써 누군가를 모욕하거나 명예훼손을 하는 것이다. 다른 동기로는 특정 누군가의 행동이나 언행을 의도적으로 다른 사람들에게 폭로하고자 게시판이나 SNS에 유포하여 그 사람에게 모욕을 주거나 명예훼손을 하는 것이다. 관련 실제 사례 중에는 피의자는 자신과의 개인적인 일로 불만을 품고, 충동적으로 피해자가 재직하고 있는 직장의 게시판에 피해자에 대한 악의적인 내용의 글을 게재하여 유포함으로써 피해자의 명예를 훼손한 사건이 있었다.

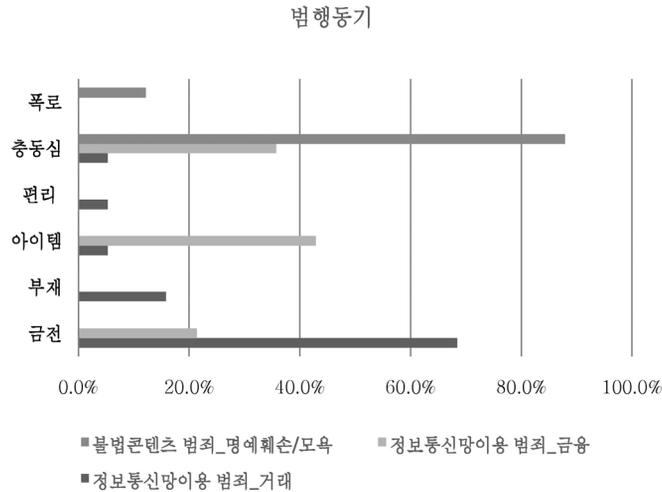
## V. 연구결과 토의 및 시사점

### 5.1 연구결과 토의

본 연구에서는 사이버범죄의 유형과 유형별 특징 및 대응방안을 마련하기 위하여 사이버범죄의 유형을 크게 정보통신망침해 범죄, 정보통신망이용 범죄, 정보통신망이용 불법콘텐츠 범죄의 세 가지로 분류하고, 각 유형에 속하는 세부 사이버범죄의 유형 중 최근 급증하고 있는 정보통신망이용 범죄의 ‘거래’와 ‘금융’, 그리고 정보통신망이용 불법콘텐츠 범죄의 ‘명예훼손·모욕’에 대하여 조사하였다. 각 세부 유형의 사이버범죄에 대하여 실제 범죄 피의자 및 수사관의 인터뷰를 통하여 정보통신망이용 범죄의 거래 14건, 금융 19건, 불법콘텐츠 범죄의 명예훼손·모욕 41건의 사례를 수집하여 분석하였다. 인터뷰 또는 조사기록을 통

해 수집된 사건들은 해당 범죄를 저지른 피의자의 성별, 연령대, 교육수준, 직업, 소득수준과 혼인여부의 개인 환경 요인과 범행동기, 범행가능이유, 범행방법, 범행이용매체, 범행대상 및 범행전과의 범행환경 요인을 포함한다. 즉, 본 연구에서는 사이버범죄의 세부 유형에 대한 환경 및 범죄 요인들을 실제 피의자 인터뷰를 실시하여 그 결과를 분석하고, 이를 기반으로 각 사이버범죄의 대응방안을 제시하였다.

우선, 본 연구에서 조사한 정보통신망이용 범죄의 ‘거래’와 ‘금융’, 불법콘텐츠 범죄의 ‘명예훼손·모욕’의 세 가지 사이버범죄의 범행환경 요인별 분석 결과를 비교 및 분석하였다. 첫째, 범행환경 요인의 범행동기에서 세 가지의 사이버범죄가 모두 포함되어 있는 동기요인은 ‘충동심’이었다. 그 중에서도 명예훼손·모욕에서 대부분의 피의자들이 충동적인 마음에 해당 범죄를 저지르는 것을 확인할 수 있었다. 이와 관련한 명예훼손·모욕의 실제 사례 중에는 특정 유명인에 대한 인격모독성 비방글을 올려 고소당한 사건이 있었고, 이에 피의자는 해당 피해자가 받을 정신적 피해에 대해 심각하게 여기지 않고 단순 유희나 충동으로 저지른 것으로 언급하였다. 즉, 사이버공간이 커뮤니케이션의 개념을 바꾸어 놓으면서 인터넷 공간에서의 무분별한 악성 댓글들이 난무하면서 사회적으로도 심각한 문제가 되고 있다(Pegg *et al.*, 2018; 정승민, 2007). 그 밖에, 정보통신망이용 범죄의 거래와 관련해서는 온라인 환경에서 자신의 아이템을 다른 사람에게 판매하는 과정에서 돈을 먼저 받고 막상 아이템을 주려니 아까운 마음이 들어서 충동적으로 저지른 일이라고 답변하였다. 정보통신망이용 범죄의 금융에서는 다른 사람의 휴대폰을 잠깐 맡고 있는 상황에서 충동적으로 한 행동이지만 법적으로 크게 문제가 있을 거라고 인지하지 못했다고 답변하였다. 즉, 명예훼손·모욕의 사이버범죄에서 ‘충동심’의 동기요인이 가장 많이 나타났고, 충동심으로 범행을 저지른 때 대부분의 피의자들은 그 행동이 법적으로 큰 문제가



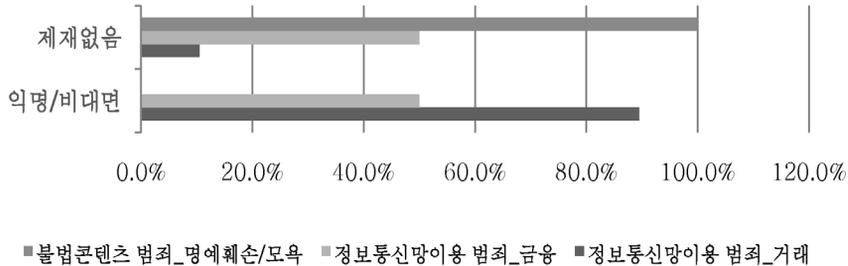
〈그림 4〉 주요 사이버범죄의 동기요인 비교

될 것임을 인지하지 못하고 있는 것으로 나타났다. 정보통신망이용 범죄의 거래에서는 대부분의 피의자들이 ‘금전’의 요인 때문에 해당 범죄를 저지르는 것으로 나타났다. 즉, 대부분의 피의자들은 이와 관련하여 생활비나 용돈을 마련하기 위해서, 대출금 때문에, 유흥비를 마련하기 위해서 해당 범죄를 저질렀다고 답변하였다. 범행 동기요인 중에서 ‘아이템’은 정보통신망이용 범죄의 금융에서 범행의 주요 요인으로 나타났다. 이는 온라인 게임, 온라인 쇼핑과 같은 온라인 환경에서의 다양한 활동과 기능이 발달하면서 새로운 유형의 가상머니 또는 아이템과 온라인 결제가 가능하게 되었다. 특히, 스마트폰을 이용한 소액결제는 본인 인증의 절차 없이 쉽게 결제가 가능하므로 인터넷 게임의 아이템 구매에 이러한 범행을 저지르는 것으로 나타났다.

둘째, 범행환경 요인의 범행가능 이유로는 세 가지의 사이버범죄 모두 ‘익명/비대면성’과 ‘제재없음’의 이유로 해당 범죄를 저지를 수 있는 것으로 나타났다. 범행가능 이유 중 ‘제재없음’은 명예훼손과 금융 부문에서 해당 이유로 범죄를 더 쉽게 저지를 수 있는 것으로 나타났다. 명예훼손·모욕과 관련해서는 피의자가 온라인 게시판이나

SNS에 특정인을 대상으로 악의적인 글이나 상대의 명예를 훼손시킬 수 있는 내용을 작성하는 것에 대한 특별한 제재가 없다는 것을 나타낸다. 최근 관련 사례로 2018년 10월, ‘맘카페’라는 커뮤니티에 도를 넘은 악성댓글로 보육교사가 스스로 목숨을 끊는 사건이 있었다. 해당 보육교사는 아동학대를 하지 않았지만 특정 누군가의 확인되지 않은 제보로 무차별한 언어폭력을 당하고 이에 극단적인 선택을 한 사건이었다. 즉, 누구나 특정 제재 없이 온라인 커뮤니티나 게시판에 타인을 비방하는 글을 남길 수 있는 것이 이와 같은 비극적인 사건의 원인이 될 수 있다는 것을 보여준다. 금융과 관련해서는 피의자들은 다른 사람의 스마트폰에 잠금장치가 설정되어 있지 않아서 쉽게 접근할 수 있었다고 인터뷰에서 답변하였다. 다음으로 ‘익명/비대면’은 정보통신망이용 범죄인 거래와 금융에서 해당 이유로 범행이 가능한 것으로 나타났다. 실제 인터뷰에서도 피의자는 본인의 신분을 정확히 상대방에게 밝힐 필요가 없고 대면하지 않아도 되기 때문에 해당 범죄를 저지를 수 있었다고 언급하였다. 수사관 인터뷰에서도 인터넷 거래에서 일어나는 사기는 범인이 익명성을 보장받으면 서 비교적 쉽게 범행을 저지를 수 있기 때문에 급증

범행가능 이유



〈그림 5〉 주요 사이버범죄의 범행가능 이유 비교

하고 있는 것으로 답변하였다. 즉, 온라인 상에서의 비대면성과 익명성은 자유로운 의사소통이 가능하다는 이점도 있지만, 반대로 사이버범죄가 가능한 주요 요인이 되기도 한다(유인창, 2012).

셋째, 범행방법으로는 세 가지 유형의 사이버범죄 각기 다른 방법으로 범행을 저지르는 것을 확인할 수 있었다. 정보통신망이용 범죄의 거래는 ‘빙자’, 금융은 ‘결제’, 그리고 불법콘텐츠 범죄의 명예훼손·모욕은 ‘유포’의 방법을 통하여 해당 범행을 저질렀다. 우선 ‘빙자’의 방법으로 범행을 저지르는 정보통신망이용 범죄의 거래와 관련해서는 인터넷 사이트 계정이나 사이버머니 등의 판매 빙자, 의류 잡화 등 물품 판매 빙자, 조건 만남 등의 빙자를 통해 접근하는 방법으로 범행을 저질렀다. 실제 인터넷 거래의 사기 범죄에서 처음부터 판매할 물품 없이 거짓으로 물건을 싸게 판매한다는 글을 올려 범행을 저지르는 사건을 종종 볼 수 있다. 한 사례로 인터넷 중고물품 사이트에서 카메라 등의 물품을 판매한다는 허위 글을 올린 다음 돈만 받고 물품은 전달하지 않는 방식으로 2천만 원을 갈취한 사건이 있었다. 정보통신망이용 범죄의 금융에서는 인터넷 사이트의 계정을 해킹하여 아이템을 결제하거나, 전화번호/인증번호를 알아내어 아이템을 결제하거나, 다른 사람의 휴대폰을 이용하는 등의 ‘결제’의 방법을 사용하였다. 즉, 해당 범죄에서 ‘결제’가 가능한 것은 다

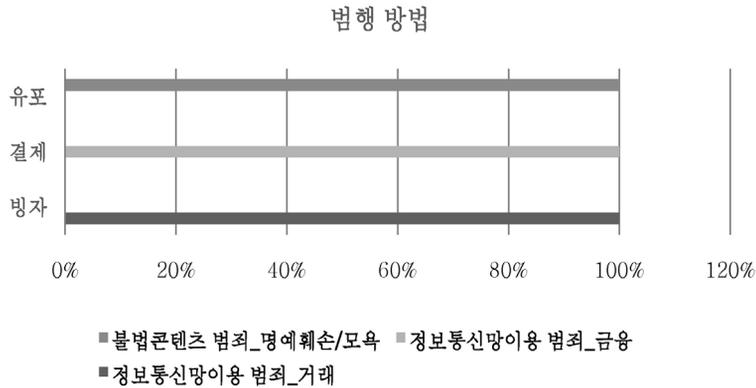
른 사람의 아이디를 해킹하거나 휴대폰을 이용한 것으로, 특히 스마트폰의 사용으로 보안 문제와 같은 비용이 증가한 것이다(Kleijnen et al., 2007; 신하정, 남기환, 2018) 정보통신망이용 불법콘텐츠 범죄의 명예훼손·모욕은 ‘유포’의 방법을 통하여 해당 범행을 저질렀다. 온라인 환경에 게시되는 글, 이미지, 동영상 등의 콘텐츠는 매우 빠르게 확산되는 특성을 가진다. 즉, 오프라인 환경에서는 누군가의 비도덕적인 언행이나 행동을 다른 사람들에게 알리고자 할 때 시간과 거리의 한계가 존재하지만, 모바일 기기를 통한 온라인 환경에서는 오늘 한 이야기가 단 몇 분 만에 전 세계로 확산되는 시간과 공간을 초월하는 특성을 가진다(손명원 등, 2016). 이러한 특성으로 온라인에서의 유포의 방법을 이용한 명예훼손·모욕에 대한 범죄는 더 심각한 상황으로까지 치닫하게 하는 심각한 사회문제로 언급되고 있다.

넷째, 범행에 이용하는 매체로는 사이트, 메신저, 게시판, SNS가 사용되었고 그 중에서 정보통신이용 범죄의 거래와 금융은 사이트와 메신저, 불법콘텐츠 범죄의 명예훼손·모욕은 게시판과 SNS가 범행에 사용되었다. 금융과 거래의 정보통신망이용 범죄는 범행 이용매체로 사이트와 메신저를 사용하였지만, 대부분 사이트를 이용하여 범행을 저질렀다. 즉, 정보통신망이용 범죄의 거래는 중고나라 거래 사이트 등과 같은 사이트를 통하여

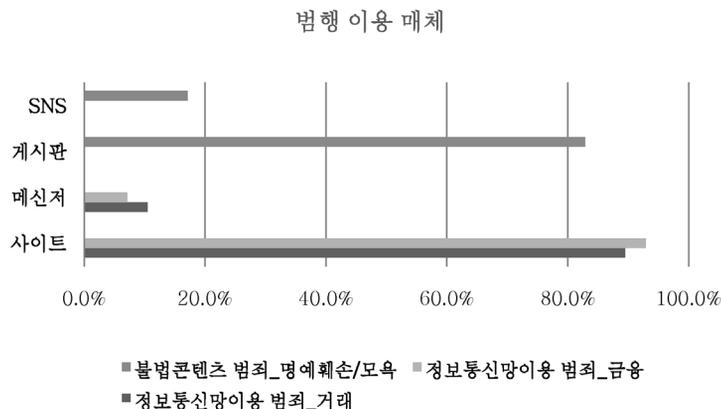
범행이 이루어지고 추가로 메신저를 이용하기도 하였다. 정보통신망이용 불법콘텐츠 범죄의 명예훼손·모욕은 게시판과 SNS를 범행 이용매체로 사용하였는데 이것은 범죄의 특성상 게시글을 올릴 수 있어야하고, 많은 사람들에게 해당 내용을 전달하고자 하므로 게시판과 SNS를 사용하는 것으로 나타낼 수 있다. 그래서, 명예훼손·모욕의 범죄 피의자들은 네이버와 같은 포털사이트의 게시판을 이용하거나 게시하고자 하는 내용과 상황에 따라 학교 게시판, 아파트 게시판 등을 이용하였다. 더불어, 최근 SNS 사용의 급증과 그 속에서 자유롭게 글을 작성할 수 있는 특성으로 페이스북

과 블로그 등이 명예훼손·모욕의 범행의 이용매체로 이용되어지고 있다(Jabee and Afshar, 2016).

다섯째, 범행대상 요인에 있어서는 대부분 온라인 환경에서 처음 접촉하는 본인과 관계가 없는 사람들을 범행 대상으로 선택하였다. 하지만, 범행을 저지른 이유에 따라 친구, 연인, 선후배 관계에서도 발생하였고 심지어 가족까지도 범행의 대상으로 선택되기도 하였다. 한편 사이버범죄의 유형에 따라 다소 차이가 있었는데, 정보통신망이용 범죄의 거래에서는 인터뷰했던 모든 해당 사건의 피의자들이 본인과 관계가 없는 사람들을 대상으로 선택한 것으로 나타났다. 하지만, 정보통신망이용 범



〈그림 6〉 주요 사이버범죄의 범행 방법 비교



〈그림 7〉 주요 사이버범죄의 범행 이용 매체 비교

죄의 금융과 정보통신망이용 불법콘텐츠 범죄의 명예훼손·모욕도 관계가 없는 사람들을 범행 대상으로 선택하는 것이 가장 많았지만, 그 밖에 연인, 이웃, 친구, 선후배, 가족, 거래 및 고용관계 등이 있었다. 즉, 대부분 본인과 관계가 없는 사람들을 대상으로 해당 범죄를 저지르지만 상황에 따라서는 가족, 연인, 친구, 선후배 등 본인과 가까운 관계에 있는 사람들에게도 범행을 저지르기도 하였다.

마지막으로 범행전과 요인에 있어서는 한번이라도 범행을 저지른 경험이 있는 피의자에 의해서

범죄가 일어나는 비율이 55%이고, 전과가 없는 피의자에 의해서 범죄가 일어나는 비율이 45%였다. 특히, 범행 전과가 있는 피의자 중에서 사이버범죄에 대한 동일 전과가 있는 상태에서 다시 동일한 범죄를 저지르는 경우가 많았다. 지금까지 조사한 사이버범죄의 세 가지(정보통신망이용 범죄의 금융, 정보통신망이용 범죄의 거래, 정보통신망이용 불법콘텐츠 범죄의 명예훼손·모욕) 유형에 따른 범행환경 요인 분석을 기반으로 각 사이버범죄에 대한 대응방안을 다음과 같이 제시한다(<표 7> 참조).

<표 7> 사이버범죄 유형별 대응방안 제안

구분	정보통신망이용 범죄_금융	정보통신망이용 범죄_거래	정보통신망이용 불법콘텐츠 범죄_명예훼손·모욕
기술적 측면	<ul style="list-style-type: none"> <li>본인 인증/등록 시스템 강화</li> <li>- 사이트 접속 시(로그인), 엄격한 본인인증 시스템</li> <li>- 결제 시 거래당사자가 관리할 수 있는 인증/등록 시스템 및 안전거래시스템</li> </ul>		<ul style="list-style-type: none"> <li>콘텐츠 필터링 서비스</li> <li>- 악의적인 글, 이미지에 대한 필터링을 통한 차단</li> <li>최초 배포자(seed) 탐지 시스템</li> <li>- 악의적인 콘텐츠를 최초 배포한 사람의 추적</li> </ul>
관리적 측면	<ul style="list-style-type: none"> <li>정기적 사이트 관리 및 모니터링</li> <li>- 거래 및 거래자 관리를 통한 부정 거래 방지</li> <li>사이버범죄 발생에 따른 즉각적 대응책 마련</li> <li>- 범죄 발생 시 2차 피해 방지를 위한 계정 및 콘텐츠 차단 등을 통한 즉각적인 대응 활동 마련</li> </ul>		<ul style="list-style-type: none"> <li>프로그램 및 콘텐츠 관리</li> <li>- 악의적인 프로그램, 게시글, 이미지에 대한 정기적인 모니터링</li> </ul>
치료 및 교육적 측면	<ul style="list-style-type: none"> <li>심리치료</li> <li>- 스트레스 및 분노 조절 심리치료</li> <li>- 온라인 게임 중독 및 욕구 조절 심리치료</li> </ul>	<ul style="list-style-type: none"> <li>인터넷 교육 및 사이버범죄의 심각성 인지를 위한 캠페인 활동</li> <li>- 사이버범죄의 심각성 및 처벌에 대한 인식 교육 및 캠페인</li> <li>- 연령대별 인터넷 맞춤형 교육</li> <li>- 인터넷 윤리교육 및 사이버범죄 체험교육(피해 상황을 부여함으로써 심각성 인지)</li> <li>사이버범죄 전과자에 대한 지속적인 관리 및 교육</li> <li>- 재범의 발생율을 줄이기 위한 전과자 지속적 관리 요구</li> </ul>	
정책 및 제도적 측면	<ul style="list-style-type: none"> <li>사이버범죄 예방을 위한 기업의 책임 강화</li> <li>- 기업의 기술적/관리적 조치의 제도 마련</li> <li>- 아이템 중개 사이트에 민사적 책임 부과</li> </ul>		<ul style="list-style-type: none"> <li>불법 콘텐츠 신고 보상 제도</li> <li>- 악의적인 댓글을 접할 경우 신고를 통한 보상</li> </ul>
	<ul style="list-style-type: none"> <li>온라인 활동 시, 사용자 정보 인증 제도 강화</li> <li>- 사이트, 게시판, SNS 접속 시(로그인), 사용자 본인 인증 강화</li> <li>- 사이트 특성에 따른 인터넷 실명제 실시</li> <li>사이버범죄에 대한 처벌 강화</li> <li>- 각 사이버범죄 유형에 따른 엄격하고 철저한 처벌을 위한 법률 마련</li> </ul>		

## 5.2 연구의 한계 및 향후 연구방향

본 연구는 다음과 같은 한계점이 있으며 이를 보완한 향후 연구 방향은 다음과 같다. 첫째, 본 연구에서는 사이버범죄의 유형을 구분하고 유형에 따른 범죄 요인들을 파악하여 사이버범죄 예방을 위한 대응방안을 제시하였다. 특히, 본 연구는 정보통신망이용 범죄의 사이버 거래와 금융, 그리고 정보통신망이용 불법콘텐츠 범죄의 사이버 명예훼손·모욕의 사이버범죄에 중점을 두고 연구를 진행하였다. 하지만, 본 연구에서 조사한 사이버범죄의 유형 뿐만 아니라 최근 새로운 기술 및 서비스를 이용한 새로운 형태의 신종 사이버범죄들이 출현하고 있다. 즉, 사이버범죄의 유형 중에서 현재 그 발생율이 급증하여 문제가 되고 있는 사이버범죄들에 집중하여 조사한 것도 의미가 있지만, 정보기술을 이용하는 사이버범죄의 특성상 기술 및 온라인 서비스 변화의 흐름에 따른 범죄의 유형을 구분하여 조사하는 것도 고려할 수 있다. 이는 정보기술의 발달과 함께 시간의 흐름에 따라 변화하는 사이버범죄의 유형 및 특성을 파악할 수 있다.

둘째, 본 연구에서 수행한 피의자 및 수사관 인터뷰, 그리고 피의자 조사기록이 모두 강원도 지역을 관할하는 경찰서에서만 수집되었다는 것이다. 이는 사이버범죄의 특성상 특정 지역의 피의자가 전국에 있는 사람들을 대상으로 범행을 저지를 수 있지만, 그 지역의 특성 및 환경적인 요인으로 인해 피의자들의 범죄 행위에 차이가 날 수 있다. 그러므로, 향후 연구에서는 전국 각 지역을 대상으로 인터뷰하거나 조사자료의 수집을 통하여 사이버범죄의 현상 및 유형의 특성을 일반화할 수 있을 뿐만 아니라 수집된 자료에 대한 신뢰를 높일 수 있다.

셋째, 본 연구는 실제 사이버범죄를 저지른 경험에 있는 피의자를 대상으로 한 인터뷰 기반 연구이다. 실제 사이버범죄를 저지른 피의자를 대상으로 해당 범죄를 저지른 동기, 가능이유, 방법,

사용매체 등을 인터뷰하고 그 결과를 분석하여 실질적인 대응방안을 제시한 것도 의미가 있지만, 향후 연구에서는 사이버범죄를 통해 피해를 입은 피해자를 대상으로 한 연구도 가능할 것이다. 사이버범죄의 피해자 인터뷰를 통하여 관련 정책 및 제도를 개선하는 것뿐만 아니라 범행이 일어난 후의 대처 방안 제시에 기여할 수 있다. 즉, 사이버범죄의 피해자 측면에서 사이버범죄의 심각성을 정확히 파악함으로써 사이버범죄에 대한 처벌이나 제도를 구축하는 기초자료로 사용될 수 있다. 또한, 범죄가 발생된 이후에 피해자 및 관련 기관들이 어떻게 대처해야하는지에 대한 구체적인 방안 마련에 기여할 수 있다.

## 5.3 연구의 학술적/실무적 의의

본 연구의 학술적 시사점은 다음과 같다. 첫째, 본 연구는 사이버범죄의 예방 및 대응방안을 제시하는데 있어서 실제 해당 범죄를 저지른 피의자들을 대상으로 인터뷰한 것에 의의가 있다. 기존 사이버범죄 관련 연구에는 사이버범죄의 개념 및 특징적 관점(이규안, 2012; 이성식, 2018; 정완, 2009), 법/제도적 관점(Ajayi, 2016; 강동범, 2007; 광병선, 2008), 그리고 피해 요인적 관점(Nasution *et al.*, 2018; Riek *et al.*, 2016; 성용은, 박준호, 2018; 이춘화, 2009)의 연구들이 있었지만, 대부분 기존 문헌을 이용하거나 일반인을 대상으로 사이버범죄의 원인을 유추하는 간접적인 접근방식으로 이루어졌다. 본 연구에서는 실제 사이버범죄를 저지른 피의자와 그 피의자를 조사한 담당 수사관을 대상으로 범행 관련 요인들을 인터뷰하고, 인터뷰 결과를 분석하여 사이버범죄 대응방안을 제시한 것에 본 연구의 차별성이 있다. 둘째, 본 연구에서는 실제 피의자를 대상으로 사이버범죄 관련 요인들을 인터뷰하여 분석한 것뿐만 아니라 인터뷰를 통해 도출된 주요 요인들 간의 관계를 나타내었다. 즉, 인터뷰 질문에 따라 응답한 내용의 주요 요인들의 관계를 빈도수가 높은 요인들을 기반으

로 연결하여 시각화하여 나타내었다. 이는 범행 관련 요인들 간의 연결 관계를 파악하여 시각화함으로써 관련 내용을 더 직관적으로 이해할 수 있게 하였다.

셋째, 본 연구는 법학 또는 심리학 분야에서 주로 다루어 온 범죄 관련 연구에 대하여 최근 인터넷과 다양한 디바이스 사용으로 사이버범죄가 출현하면서 정보기술 관련 지식이나 정보의 필요성으로 정보기술 분야와의 융복합적 연구라고 볼 수 있다. 즉, 단순히 오프라인의 범죄행위가 온라인 환경으로 옮겨지는 것뿐만 아니라 최신 기술을 이용한 새로운 유형의 사이버범죄들이 증가하고 있다. 이는 범행을 저지르고자 하는 범행 환경이나 범죄자의 범행 심리를 넘어 정보기술에 대한 정보 및 전문 지식이 추가로 요구된다(박창욱, 2008). 본 연구는 주로 법학이나 심리학 분야에서 개념적으로 연구되어져왔던 주제를 정보시스템 분야의 지식을 기반으로 분석함으로써 학문 분야의 융복합적 관점에서 실질적인 제안을 제시한 것에 의의가 있다.

다음으로 본 연구의 실무적 시사점은 다음과 같다. 우선, 본 연구에서는 사이버범죄의 유형에 따라 각 범죄를 예방할 수 있는 방안을 제시하였다. 최근 사이버공간에서의 범죄행위가 심각한 사회문제로 대두되고 있으며, 이는 오프라인에서의 범죄와 다른 특성을 가지므로 사이버범죄의 유형과 특성을 파악하고 범행 관련 요인들을 분석하는 것이 필요하다. 그리하여, 본 연구에서는 먼저 사이버범죄의 유형을 분류하고, 각 유형의 사이버범죄의 특성을 나타내었다. 더불어, 세 가지 사이버범죄(정보통신망이용 범죄의 거래와 금융, 불법콘텐츠 범죄의 명예훼손·모욕)에 관하여 실제 피의자들을 대상으로 인터뷰를 실시함으로써 범행 요인들을 분석하여 사이버범죄의 실질적인 예방 및 대응방안을 제안하였다. 즉, 사이버범죄 유형에 따른 특성을 파악하고 인터뷰한 후, 이를 기반으로 사이버범죄 유형 별 대응방안을 제시하였다.

마지막으로, 본 연구에서는 사이버범죄의 예방

및 대응방안을 제시하는데 있어서 기술적 측면, 관리적 측면, 치료 및 교육적 측면, 그리고 정책 및 제도적 측면에서 고려해야 할 구체적인 방안을 제시하였다. 특히, 사이버범죄는 특성상 기술적인 부분과 온라인 사이트 및 서비스의 관리적인 부분의 조치가 필요하다. 또한, 새로운 정보기술과 디바이스의 사용으로 오프라인 범죄와는 다른 새로운 유형의 범죄들이 출현과 동시에 발생하고 있으므로, 이에 대한 구체적인 정책 및 제도가 요구된다. 그 밖에, 범죄자들의 근본적인 범행 동기 및 원인을 근절하기 위한 사이버범죄에 대한 인식 및 교육이 강화되어야 한다. 그리하여, 본 연구에서는 심각한 사회문제로 언급되고 있는 사이버범죄를 예방하고, 이에 대응하기 위하여 본 연구를 통해 도출된 범행 요인들을 기반으로 실질적인 대응방안을 기술적, 관리적, 치료 및 교육적, 그리고 정책 및 제도적 측면으로 구분하여 제시하였다.

## 참 고 문 헌

- [1] 강동범, “사이버범죄 처벌규정의 문제점과 대책”, *형사정책*, 제19권, 제2호, 2007, pp. 33-54.
- [2] 곽병선, “사이버범죄 예방을 위한 법제도적 해결방안”, *원광법학*, 제24권, 제3호, 2008, pp. 115-141.
- [3] 김상순, “경찰청 2018년 3분기 사이버위협 분석보고서 발간”, 대한민국 정책브리핑, 2018. 10. 30., Available at <http://www.korea.kr/briefing/pressReleaseView.do?newsId=156301269>.
- [4] 김연수, “사이버와 사이버범죄의본질 및 특징에 대한 분석”, *계간 사상*, 제56호, 2003, pp. 158-187.
- [5] 박창욱, “경찰의 사이버범죄에 대한 효율적 대응방안에 관한 연구”, *한국컴퓨터정보학회 논문지*, 제13권, 제3호, 2008, pp. 189-196.
- [6] 백혜주, 정주현, “노인 도시락 봉사활동을 위한 디자인 제안-정성적 조사 방법을 중심으로

- 로”, *기초조형학연구*, 제14권, 제1호, 2013, pp. 257-265.
- [7] 성용은, 박준호, “SNS(Social Network Service) 기반 사이버범죄 피해 연구”, *한국민간경비학회보*, 제17권, 제3호, 2018, pp. 109-142.
- [8] 손명원, 권순동, 김용영, “스마트폰 이용자의 정서적 소진과 학습 성과에 영향을 주는 인지·감성 성향과 사용 경험에 관한 연구”, *Information Systems Review*, 제18권, 제4호, 2016, pp. 69-88.
- [9] 신하정, 남기환, “디바이스 유형을 고려한 온라인 멀티 채널 마케팅 효과”, *Information Sysmes Review*, 제20권, 제4호, 2018, pp. 59-78.
- [10] 유인창, “사이버 명예훼손행위와 형사법적 대응방안”, *한국컴퓨터정보학회논문지*, 제17권, 제5호, 2012, pp. 177-183.
- [11] 이관주, “올해 사이버범죄 최대 유형은 ‘인터넷 사기’...피싱 범죄 3배 증가”, *아시아경제*, 2018.10.30., Available at <http://view.asiae.co.kr/news/view.htm?idxno=2018103010472922544>.
- [12] 이규안, “사이버범죄의 새로운 양상과 대처방안 연구”, *한국전자통신학회 춘계학술지*, 제6권, 제1호, 2012, pp. 224-226.
- [13] 이성식, “사이버범죄에서 피해의 가해에의 영향의 매개과정 연구: 세 이론의 검증”, *피해자학연구*, 제23권, 제3호, 2015, pp. 99-120.
- [14] 이성식, “사이버범죄의 세 유형별 원인과 대책요인의 상호작용효과 분석”, *한국치안행정논집*, 제15권, 제1호, 2018, pp. 209-234.
- [15] 이춘화, “청소년의 사이버범죄 피해요인에 관한 연구”, *피해자학연구*, 제17권, 제1호, 2009, pp. 267-289.
- [16] 이현진, “사이버범죄 10년새 90% 증가...예방 위한 단일 법령 만든다”, *한국경제*, 2017.04.20., Available at <http://news.hankyung.com/article/2017042057541?nv=o>.
- [17] 정 완, “사이버범죄의 실태와 동향 및 대응책”, *홍익법학*, 제10권, 제1호, 2009, pp. 195-224.
- [18] 정 완, “사이버범죄의 현상”, *형사정책*, 제19권, 제2호, 2007, pp. 9-32.
- [19] 정승민, “악성댓글의 문제점과 대응방안”, *한국공안행정학회보*, 제16권, 제2호, 2007, pp. 171-201.
- [20] Ajayi, E. F. G., “Challenges to enforcement of cyber-crimes laws and policy”, *Journal of Internet and Information Systems*, Vol.6, No.1, 2016, pp. 1-12.
- [21] 조병인, 박광민, 최응렬, 김종오, *국내거주 외국인의 조직범죄 실태와 대책 연구*, 한국형사정책연구원 연구총서 10-03, 2010
- [22] Corbin, J. and A. Strauss, “Basic considerations in basics of qualitative research”, *Techniques and procedures for developing grounded theory* (3rd ed.), Sage, 1998.
- [23] Garg, V. and L. J. Camp, “Why cybercrime?”, *ACM SIGCAS Computers and Society*, Vol.45, No.2, 2015, pp. 20-28.
- [24] Jabee, R. and M. Afshar, “Issues and challenges of cyber security for social networking sites (Facebook)”, *International Journal of Computer Applications*, Vol.144, No.3, 2016, pp. 36-40.
- [25] Kim, H. W., H. C. Chan, and S. Gupta, “Social media for business and society”, *Asia Pacific Journal of Information Systems*, Vol.25, No.2, 2015, pp. 211-233.
- [26] Kleijnen, M., K. De Ruyter, and M. Wetzels, “An assessment of value creation in mobile service delivery and the moderating role of time consciousness”, *Journal of Retailing*, Vol.83, No.1, 2007, pp. 33-46.
- [27] Lagazio, M., N. Sherif, and M. Cushman, “A multi-level approach to understanding the impact of cyber crime on the financial sector”, *Computers & Security*, Vol.45, 2014, pp. 58-74.
- [28] Lee, S. H. and H. W. Kim, “Why people post

- benevolent and malicious comments online”, *Communications of the ACM*, Vol.58, No.11, 2015, pp. 74-79.
- [29] Nasution, M. D. T. P., Y. Rossanty, A. P. U. Siahaan, and S. Aryza, “The phenomenon of cyber-crime and fraud victimization in online shop”, *International Journal of Civil Engineering and Technology*, Vol.9, No.6, 2018, pp. 1583-1592.
- [30] Pegg, K. J., A. W. O’Donnell, G. Lala, and B. L. Barber, “The role of online social identity in the relationship between alcohol-related content on social networking sites and adolescent alcohol use”, *Cyberpsychology, Behavior, and Social Networking*, Vol.21, No.1, 2018, pp. 50-55.
- [31] Riek, M., R. Bohme, and T. Moore, “Measuring the influence of perceived cybercrime risk on online service avoidance”, *IEEE Transactions on Dependable and Secure Computing*, Vol.13, No.2, 2016, pp. 261-273.
- [32] Yin, R. K., *Case study research: Design and methods* (5th ed.), Sage publications, Los Angeles, 2013.

## Analysis of Cyber Crime and Its Characteristics

So-Hyun Lee\* · Ilwoong Kang\*\* · Yoonhyuk Jung\*\*\* · Hee-Woong Kim\*\*\*\*

### Abstract

Now we are facing with a possibility of having crimes, which have been only possible offline, in cyber spaces as well. Especially, a recent growth in the use of SNS, promoted by popularization of smart phones, also has led an abrupt increase in cyber crime. It would be important to have a understanding of cyber crime and its characteristics by type as well as factors associated with each type of cyber crime in order to devise appropriate preventive measures against cyber crime. However, most of the previous studies on cyber crimesolely made through literature review or indirect approaches. Therefore, this study has been designed to conduct the interview with actual suspects(criminals) of cyber crime to address factors of cyber crime and to devise specific preventive measures and countermeasures against cyber crime. Especially, among various types of cyber crime, this study aims at addressing the ‘trades’ and ‘financial transaction’ of crimes committed using the information and communication network and the ‘cyber libel/insult’of crimes committed using unlicensed contents, which have been soared recently and become significant issues. The findings of this study could be beneficial for the society since it has managed to conduct the interview and reveal relationships among major factors of cyber crime. The findings of this study could be used for devising and developing proper preventive and countermeasures against cyber crime, in turn reducing and preventing its damage.

**Keywords:** *Cyber Crime, Cyber Libel/Insult, Cyber Trades, Cyber Financial Transaction, Interview*

---

\* Graduate School of Information, Yonsei University

\*\* Gangwon Provincial Police Agency

\*\*\* School of Media and Communication, Korea University

\*\*\*\* Corresponding Author, Graduate School of Information, Yonsei University

## ◎ 저 자 소 개 ◎



**이 소 현 (sohyun1010@yonsei.ac.kr)**

연세대학교 정보대학원에서 정보시스템학 박사학위 취득 후, 현재 연세대학교 정보대학원에서 연구교수로 근무 중이다. 주요 연구분야는 디지털 비즈니스, 소셜미디어, 온라인 마케팅 등이다. 관련 연구들은 Information Systems Research, Communications of ACM, Information and Management, International Journal of Information Management 등에 논문이 게재되었다.



**강 일 웅 (ilwoongkang@gmail.com)**

연세대학교 정보대학원에서 석사학위 취득 후, 현재 강원경찰청에 근무 중이다. 주요 관심분야는 디지털 포렌식, 사이버범죄이다.



**정 윤 혁 (beyond@korea.ac.kr)**

울산과학기술원 경영학부에서 근무 후, 현재 고려대학교 미디어학부 교수로 근무 중이다. 주요 연구분야는 뉴미디어 산업 및 기술, 정보기술 사용자 등이다. 관련 연구들은 International Journal of Information Management, Journal of Computer-Mediated Communication, Computers in Human Behavior, New Media & Society 등에 논문이 게재되었다.



**김 희 웅 (kimhw@yonsei.ac.kr)**

National University of Singapore 정보시스템학과에서 근무 후, 현재 연세대학교 정보대학원 교수로 근무 중이다. 주요 연구분야는 디지털 비즈니스, 정보시스템 관리 및 활용 등이다. 관련 연구들은 MIS Quarterly, Information Systems Research 등 IS 저널에 50여 편의 논문이 게재되었다.

논문접수일 : 2019년 03월 20일

게재확정일 : 2019년 05월 07일

1차 수정일 : 2019년 04월 29일