

사이버 범죄의 특성과 대응방안 연구: 저작권 침해, 도박, 음란물 범죄를 중심으로¹⁾

Exploring the Nature of Cybercrime and Countermeasures:
Focusing on Copyright Infringement, Gambling, and Pornography Crimes

강일웅 (Ilwoong Kang)	강원경찰청 ²⁾
김재희 (Jaehui Kim)	연세대학교 정보대학원 ³⁾
이소현 (So-Hyun Lee)	경기대학교 산업경영정보공학과 ⁴⁾
김희웅 (Hee-Woong Kim)	연세대학교 정보대학원 ⁵⁾

〈 국문초록 〉

사이버 공간의 발전과 우리 일상생활과의 상호작용이 증가함에 따라 사이버 범죄는 최근 몇 년 동안 꾸준한 증가세를 보이며 심각한 사회 문제로서 그 양상이 더욱 두드러지고 있다. 특히, '4대 악성 사이버 범죄'로 분류되는 사이버 금융 범죄, 사이버 사기, 사이버 성폭력과 사이버 도박은 주목해야 할 대상 중 하나이다. 심각한 사회문제 중 하나인 사이버 범죄의 피해를 최소화하기 위해 사이버 범죄의 유형 별 특성을 심층적으로 파악하고 원인과 예방 및 대처 방안을 구체적으로 제시할 필요성이 있다. 그러나 기존 사이버 범죄 관련 연구에서는 통계 자료나 피해자, 일반 대중을 대상으로 자료를 수집하는 간접적인 방법을 활용하여 접근해왔다. 따라서 본 연구는 사이버 범죄 중 최근 범행 건수가 급증하며 범죄의 심각성이 강조되는 정보통신망이용 범죄의 '저작권 침해'와 정보통신망이용 불법콘텐츠 범죄의 '도박' 및 '음란물' 유형에 대하여 사이버 범죄 피의자를 대상으로 직접 인터뷰를 실시하고 코딩 분석과 텍스트마이닝을 통해 결과를 분석함으로써 사이버 범죄의 특성과 발생 원인을 밝히고 예방 및 대책 방안을 제시하고자 한다. 본 연구는 범죄 피의자와의 인터뷰를 통해 얻은 결과를 분석하고 주요 요인들 간의 관계를 탐구함으로써, 사이버 범죄에 대한 깊은 이해와 통찰력을 제공한다. 더하여 예방 및 대응 방안을 제안함으로써 심각한 사회 문제인 사이버 범죄의 피해를 최소화하기 위한 제도적 마련에 핵심 자료를 제공했다는 점에서 의의를 가진다.

주제어: 저작권 침해, 사이버 도박, 음란물, 인터뷰 방법론, 텍스트 마이닝

1) 이 논문은 2023년 대한민국 교육부와 한국연구재단의 공동연구지원사업의 지원을 받아 수행된 연구임(NRF-2023S1A5A2A03084147). 이 논문은 2016년 연세대학교 강일웅의 석사학위논문 "사이버범죄 특징분석 및 예방방안을 위한 탐색적 연구"를 기반으로 작성됨.

2) 제1저자, ilwoongkang@gmail.com

3) 공동저자, keemjaehee@yonsei.ac.kr

4) 공동저자, sohyun@kgu.ac.kr

5) 교신저자, kimhw@yonsei.ac.kr

1. 서론

사이버 공간(Cyberspace)이라는 개념이 등장한 이래로 우리는 사이버 공간이라는 가상공간 안에서 삶과 문화를 유기적으로 결합하고 상호 영향을 끼쳐왔다. 최근에는 온라인 쇼핑, 여가 생활은 물론 화상회의를 통한 협업, 재택 근무, 비대면 수업까지 대부분의 일상 생활을 영위할 수 있게 됐고, 이러한 사이버 공간에서의 삶은 코로나19 대유행으로 그 활용과 적응이 더욱 빨라졌다. 하지만 사이버 공간에서 다양한 활동을 수행할 수 있게 되면서 편리함과 더불어 각종 다양한 범죄 또한 온라인과 오프라인을 구분하지 않고 발생하기 시작했다. 이는 코로나19 대유행 이후 비대면 활동이 증가하며 더욱 증가하고 있는 양상이다(이서현 등, 2022). 최근 5년 동안 국내 사이버 범죄의 발생 건수는 2021년을 제외하고 꾸준히 증가했는데, 이는 국내 사이버 범죄의 심각성을 시사하고 있다(김영명, 2023). 실제로 사이버 공간의 활성화에 따라 각종 사회문제에 대응하기 위해 경찰청은 정보통신 디지털 수사 자료나 증거를 다루는 부서를 신설했다(김보라 & 임수진, 2022). 더하여 경찰청은 ‘4대 악성 사이버 범죄’에 사이버 금융범죄, 사이버 사기, 사이버 성폭력 및 사이버 도박을 포함시켜 이에 대한 대응을 강화하고 있다. 이중 사이버 사기 범죄는 금전적인 피해 규모가 큰 편이며, 국민 실생활에 직접적으로 영향을 미치고 있다(김성찬, 2023).

사이버 사기와 더불어 급증하는 유형으로는 ‘저작권 침해’ 문제가 있다. 2023년 경찰청이 발표한 통계자료에 따르면, 지난 2년동안 사이버 저작권 침해는 2,423건에서 3,302건으로 36.3% 증가한 수치를 나타냈다(김영명, 2023). 이러한 사이버 저작권 침해는 최근 한국 드라마, 영화뿐만 아니라 웹툰, 웹소설이 전세계적인 인기를 얻으며 콘텐츠 문화 산업이 급속히 성장하면서, 콘텐츠 불법 유통과 같은 사례가 급증하고 있는 것으로 나타났다(김지현, 2023). 이와 같은 콘텐츠의 불법 유통으로 인해 막심

한 피해가 발생한 대표적인 사례로는 ‘누누티비’가 있다. ‘누누티비’는 해외 서버를 사용하여 다양한 온라인 동영상 서비스(OTT) 및 드라마, 영화 등을 무단으로 배포하는 불법 복제 웹사이트이며, 사용자들은 추가적인 연령 확인이나 회원 가입 절차 없이 고해상도의 영상을 자유롭게 볼 수 있다. 이 영상들은 방송국과 OTT등 저작권자로부터 이용 허락을 받지 않고 영상을 무단 복제 및 게시된 것이며, 총 조회수 약 15억 3,800회, 월간이용자수 1,000만명에 이른다고 밝혀졌다(이영아, 2023). 이러한 불법 스트리밍 사이트로 인해 저작권 침해 피해 규모가 점차 커지자, 일각에서는 저작권 침해행위를 근절하기 위해 저작권법 일부 개정이 필요하다고 주장하고 있다(소장섭, 2023; 김현정, 김범수, 2023; 박민정, 채상미, 2017).

저작권 침해 문제와 함께 주요 사이버 범죄 유형 중 하나인 ‘사이버 성폭력’은 최근 그 위험성이 지속적으로 증가하고 있다. 이는 사이버 공간에서 음란물을 배포, 판매, 또는 전시하는 행위이며, 디지털 기기와 소셜 미디어의 발전으로 인해 그 영향력이 더욱 커지고 있다. 2021년 경찰청 자료에 따르면, 사이버 성폭력·불법촬영 피해 경험이 있는 사람 3390명 가운데 42.2%가 음란물을 전송 받은 적이 있다고 답변했다(오세진, 2021). 이어서 마지막 4대 악성 사이버 범죄 중 ‘사이버 도박’의 경우, 특히 청소년을 중심으로 한 사이버도박이 심각하다. 코로나19의 영향으로 비대면 문화가 일상화되면서 온라인 도박이 성행하게 되었고, 이에 따라 청소년들 사이에서도 온라인 불법 도박이 유행처럼 번져나갔다. 한국도박문제예방치유원의 실태조사에 의하면 2021년 10월 기준 초·중·고등학교에 재학 중인 청소년 398만6천403명 중 약 4.78%가 ‘도박 위험집단’에 해당했다(임순현, 2023).

이러한 사례로 볼 수 있듯이 현재 사이버 범죄는 사회 전반에서 다양한 문제의 근원이 되어 심각한 사회문제로 간주되고 있다. 이에 따라 사이버 범죄의 다양한 유형과 각 유형별 특성을 이해하고, 해당 범죄와 관련된 주요 요

인을 분석하여 예방 및 대처 방안을 모색하는 것이 필요하다. 이 분야에서 선행 연구들이 수행되어 왔으나, 대부분 사례는 간접적인 방법을 사용해 관련 통계 자료나 피해자, 일반 대중을 중심으로 접근했으며 직접적인 피의자 중심의 연구는 많이 이루어지지 않았다. 그러나 사이버 범죄의 근본적인 원인과 구체적인 범행 방법을 분석하고, 이를 토대로 예방 및 대응 방안을 마련하기 위해서는 실제 피의자를 대상으로 데이터를 수집하고 분석하는 접근이 필요하다. 따라서 본 연구는 사이버 범죄 중 ‘저작권 침해’, ‘도박’, ‘음란물’과 관련하여 범죄 피의자를 중심으로 인터뷰를 실시하여 데이터를 수집한 후, 각 유형별 사이버 범죄의 피의자의 개인 환경과 범행 특성을 분석하고 이를 토대로 예방 및 대응 방안을 제안하고자 한다.

본 연구는 다음과 같은 중요한 의미를 지닌다. 첫째로, 현재의 사이버 범죄가 사회 전반에 미치는 영향이 더욱 심각해지고 있는 상황에서, 사이버 범죄의 다양한 유형과 각 유형별 특성을 피의자 중심으로 직접적으로 분석함으로써 사이버공간 사용의 주체 및 정책 입안자와 같은 이해 관계자들에게 핵심 정보와 통찰력을 제공할 수 있다. 둘째로, 본 연구는 사이버 범죄의 원인과 범행 방법을 근본적으로 이해하는 데 기여함으로써 예방 및 대응 방안을 효과적으로 개발하는데 도움이 될 수 있다. 특히, 피의자 중심의 연구 방법을 통해 사이버 범죄의 범행 동기와 특성을 상세하게 파악하여 정부, 경찰, 민간 기업 등 사이버 공간을 사용하는 이해관계자들의 실질적인 대책 마련 과정에 기여할 것으로 기대된다.

2. 개념적 배경

2.1. 사이버 범죄의 개념 및 유형

사이버 범죄의 개념은 학문적으로 명확히 정립되지 않

았으나, 사이버 공간 내에서 이뤄지는 범죄 행위로 보는 것이 일반적인 접근이다. 가장 일반적으로 인용되는 학문적 정의는 ‘불법이거나 특정 당사자에 의해 불법으로 간주되고 글로벌 전자 네트워크를 통해 수행될 수 있는 컴퓨터 매개활동’으로 알려져 있다(Thomas & Loader, 2013). 국내 연구에서는 사이버범죄 행위에 대하여 ‘사이버 공간에 대한 특별한 지식을 이용하는 범죄’, ‘컴퓨터와 전자 네트워크를 매개로 한 불법으로 간주되는 행위 또는 활동’으로 정의하거나, ‘가상공간에서 다른 사람(법인 포함)의 생명, 신체, 재산, 명예 및 사생활 등 개인을 위협하거나 사회를 위협하는 불법적인 행위’로 정의하고 있다(이원상, 채희정, 2010; 조병인, 2000).

사이버 범죄의 개념은 명확한 정의보다는 주로 유형 분류를 통해 이해되며, 이러한 분류 시스템은 연구자와 정책 입안자들에 의해 널리 사용되고 있다. 첫째로, 사이버 범죄를 크게 ‘사이버 기반’ 범죄와 ‘사이버 의존’ 범죄로 분류할 수 있다(Brenner, 2013). 이 분류 시스템은 등장 이래로 다양한 연구와 정책 입안에 지속적으로 활용되고 있으며(Akdemir & Lawless, 2020; McGuire & Dowling, 2013; Paoli et al., 2018; Sarre et al., 2018), 분류 체계와 정의는 다음과 같다. ‘사이버 기반’ 범죄는 사이버 기술이 등장하기 이전부터 존재하던 범죄 유형으로, 사이버 기술을 통해 더 다양해지고 쉽게 저지르게 된 범죄를 의미하며 사이버 사기, 사이버 스토킹, 사이버 폭력 등이 포함된다. 이에 비해 ‘사이버 의존’ 범죄는 사이버 기술의 등장과 함께 나타난 범죄로, 디지털 세계 외부에서는 발생하지 않는 범죄를 의미한다. 이 범주에는 해킹, 랜섬웨어 공격과 같은 사이버 공간에서 주로 발생하는 범죄가 포함된다.

이처럼 이분법적 분류 체계 이외에도 사이버 범죄를 세 가지 범주로 구분한 Wall (2007)의 분류 체계가 존재한다. 이는 학술 문헌에서 처음으로 소개되었으며, 등장 이후 관련된 다양한 연구에서 인용되고 있다(Arief et al.,

2015; McGuire, 2017; Phillips et al., 2022; Williams & Levi, 2015). 세 가지 범주로 구분한 분류 체계는 다음과 같다. 먼저, 기계에 대한 범죄(Crimes against the machine)는 사이버 환경 자체를 공격하는 행위를 나타내며, 해킹, 크래킹, DDos 공격 등이 이에 해당한다. 다음으로, 기계를 이용한 범죄(Crimes using the machine)이다. 이는 사이버 공간 및 기술을 이용해 저지르는 행위를 나타내며, 불법 복제와 강도, 사기 등이 해당한다. 마지막으로, 기계 속의 범죄(Crimes in the machine)가 있다. 이는 컴퓨터 콘텐츠 범죄로도 알려져 있으며, 사이버 공간 상에서 사용자 간 발생하는 범죄를 나타낸다. 온라인 상에서의 괴롭힘과 음란물 유포가 이러한 범죄에 해당된다.

한편, Khosla and Dubey (2016)는 사이버 범죄를 다양한 범주로 분류하였으며, 개인 대상의 사이버 폭력, 사이버 스토킹, 기업의 영업비밀 침해, 저작권 침해, 정부를 겨냥한 사이버 테러, 음란물 유포, 도박, 마약 거래 등이 포함된다. 국내 연구에서도 사이버 범죄를 다양한 관점에서 분류한 사례(강석구 등, 2010)가 있으며, 이 경우 범죄 수법 및 피해 기준, 범죄 대상, 범죄자, 범죄근원지를 기준으로 고려하였다.

한편, 경찰청의 사이버범죄 신고시스템(ECRM)은 계속해서 그 유형과 방법이 다양해지고 있는 사이버 범죄에 대응하기 위해, 범죄의 분류 기준을 마련하고 각 분류에 해당되는 범죄 사례들을 명시했다. 먼저 ‘정보통신망 침해 범죄’는 합법적인 접근 권한이 없거나 주어진 접근 권한을 넘어 컴퓨터나 정보통신망(컴퓨터 시스템)에 무단으로 침입하거나, 시스템이나 데이터 프로그램을 손상시키거나 파괴, 변경하는 행위 혹은 정보통신망(컴퓨터 시스템)에 장애(사용불능 및 성능저하)를 유발한 경우를 말한다. 해킹 범죄가 이 사례에 해당된다. 다음으로, ‘정보통신망 이용범죄’는 범죄의 핵심 구성요건에 해당하는 행위를 할 때 정보통신망(컴퓨터 시스템)을 주요한 수단으로 이용하는 경우를 말한다. 사이버 사기, 사이버 금융

범죄, 저작권 침해, 사이버 스팸 메일, 개인·위치정보 침해가 이에 해당한다. 마지막으로, ‘정보통신망 이용 불법 콘텐츠범죄’는 법적으로 금지된 재화, 서비스 또는 정보를 정보통신망(컴퓨터 시스템)을 통해 배포, 판매, 임대, 또는 전시하는 행위를 말한다. 사이버 도박, 사이버 성폭력, 명예훼손·도박, 사이버스토킹이 이 분류에 해당한다.

본 연구에서는 국내·외에서 진행된 연구와 경찰청의 사이버범죄 신고시스템(ECRM)에서 제시한 사이버 범죄 분류 기준을 바탕으로, 사이버범죄를 정보통신망 네트워크 존재 자체를 위협하는 ‘정보통신망 침해범죄’, 정보통신망을 주된 수단으로 활용하는 ‘정보통신망 이용범죄’, 정보통신망 이용범죄 중 정보통신망을 통해 전송되는 데이터(콘텐츠)가 불법인 경우를 구분하여 ‘정보통신망 이용 불법콘텐츠범죄’로 분류하고자 한다.

2.2. 선행 연구

사이버범죄 관련 선행연구로는 사이버 범죄를 유발하는 요인을 연구한 사례, 지속적인 범죄 확산에 따른 대응 방안을 연구한 사례, 사이버 범죄의 피해 저지를 위한 수사 기술을 연구한 사례가 있다. 먼저, 사이버 범죄를 유발하는 요인에 대한 연구에서는 인간의 5단계 욕구에 기반하여 개인의 심리적 특성이 사이버 범죄 발생에 어떤 영향을 미치는지 탐구한 사례가 있었다(임현욱, 2021). 또한, 온라인 네트워크 환경의 발전으로 청년층의 스마트폰 및 인터넷 중독 현상과 개인의 도덕적 태도가 사이버 범죄에 미치는 영향을 조사한 연구도 있었다(김계원, 서진완, 2012; 이성식, 전신현, 2022). 사이버범죄의 대응 방안 측면에서는, 사이버범죄 발생 환경을 분석하고 현재 수사과정의 미비점을 개선하기 위해 범국가적인 공동 수사팀 구축을 제안한 연구(서승모, 권현영, 2022)가 있었다. 이어서 지속적으로 발전하는 사이버환경을 고려하여 경찰뿐만 아니라 모든 관련 주체의 협력과 참여가 필

요한 파트너십 사이버경찰 활동의 필요성을 강조한 연구도 있었다(정태진, 2022). 또한, 현재 형사사법체계의 한계를 지적하며 실체법과 절차법의 개선 및 국제적 협약을 통한 규제방안을 제시한 연구가 있었다(정지혜, 2020). 마지막으로, 사이버 범죄의 수사 기술적 측면에서는 다양한 상황 및 장소에서 발생하는 사이버 범죄를 신속하고 효과적으로 탐지하고 차단할 수 있는 새로운 기술을 제안한 연구(김지은, 우병관, 2022)와 사이버 범죄 수사 및 범인 검거에 있어 더욱 효율적으로 대응할 수 있도록 사이버 범죄 대응 디지털 포렌식 모델을 제안한 연구가 있었다(오세연, 2015).

이와 같은 선행연구들은 사이버 범죄의 발생 요인과 대응방안, 수사기술 중심으로 연구되었으며 이는 사이버 범죄에 대한 이해와 대응능력 향상에 기여한다. 하지만 이와 같이 진행된 사이버 범죄 관련 선행연구들은 모두 통계적 데이터 혹은 피해자와 일반 대중을 중심으로 접근하는 간접적인 방법으로 진행되었고, 피의자를 중심으로 접근하는 직접적인 방법은 관련 연구에서 대중적으로 채택되지 않고 있다.

피의자 중심 인터뷰를 진행하여 직접적인 접근 방법을 활용한 연구의 경우 사이버 거래와 금융, 명예훼손을 저지른 피의자를 중심으로 유형별 특징을 분석한 사례가 있었다(이소현 등, 2019). 하지만 이는 기술적, 문화적 변화에 따라 진화하는 사이버 범죄 수법의 영향을 완벽하게 다루지 못하는 한계가 있다. 예를 들어, 온라인 동영상 서비스(OTT)의 발전과 한국 문화 콘텐츠 영향력의 확대로 인해 콘텐츠 불법 유통 문제가 크게 증가하고 있는데, 이러한 측면에서 관련 분석은 이전 연구에서 제대로 이뤄지지 않았다. 아울러, 모바일 환경이 더욱 익숙한 청소년들 사이에서 최근에 두드러지고 있는 사이버 도박과 음란물 관련 범죄 또한 그 심각성이 두드러지고 있으며, 이러한 범주를 다루는 추가적인 연구가 필요한 상황이다.

따라서 본 연구에서는 선행 연구를 기반으로 사이버

범죄의 개념과 유형을 정의하고, 그 중에서도 ‘저작권 침해’, ‘도박’, ‘음란물’과 같이 심각성이 강조되는 범주에 중점을 두며, 이러한 범죄를 저지른 피의자들의 개인 환경과 범행 특성을 조사함으로써 기존 연구와 차별화하고자 한다. 그리고 각 유형별 사이버 범죄의 특징과 발생원인의 분석결과를 토대로 예방 및 대응방안을 제안함으로써 기존의 사이버 범죄 관련 연구에 기여하고자 한다.

3. 연구방법론

3.1. 인터뷰 방법론

본 연구에서 사용한 인터뷰 방법론은 정성적 연구(Qualitative research)이며, 사회과학의 주류 연구 패러다임인 정량적 연구(Quantitative research)와 대비되는 해석적 연구 패러다임이다(Hammersley & Atkinson, 2019). 정성적 연구는 질적 연구로도 불리며, 숫자에 의한 단순한 양적 비교보다는 숫자로 표현될 수 없는 의미나 통찰적 시각 획득을 목표로 사용된다. 또한 양적 데이터는 코딩 과정에서 소수의 두드러지는 지원자를 제외하고는 각 지원자가 지니는 개별적 특수성이 최소화되는데 반해, 질적 데이터는 학습자에 대한 심층적인 이해가 가능하다는 특징을 지니고 있다(김태영, 2015).

그중 인터뷰 방법론은 사회과학의 한 연구방법인 질적 연구에서 사용하는 자료수집 방식으로서의 인터뷰를 말한다(Patton, 2002). Yin (2014)에 따르면, 인터뷰 방법론은 원하는 현상을 자세하게 관찰하고 현상에 대한 충분한 이해와 추론을 가능하게 함으로써, 탐구하려는 현상의 본질을 파악하는 데 강점을 갖고 있다. 선행 연구에서는 주로 통계 데이터나 피해자를 중심으로 한 간접적인 자료를 사용하였기에, 범행 특성 정보를 파악하기에는 어려움이 있었다. 본 연구에서는 사이버 범죄를 정보통

신망침해 범죄, 정보통신망이용 범죄, 그리고 정보통신망 이용 불법콘텐츠 범죄 세 가지 유형으로 구분한 후, 그 중 최근 발생률이 증가하고 사회적으로 많은 관심을 받는 정보통신망이용 범죄의 저작권 침해와 정보통신망 이용 불법콘텐츠 범죄의 도박 및 음란물 범죄 요인들을 밝혀내는 것을 목적으로 한다. 이를 위하여 범죄 피의자를 중심으로 범행 특성 정보를 수집하고 각 유형에 대한 심층적인 사례분석을 실시하고자 하며, 데이터 수집 방법으로 사이버 범죄를 저지른 피의자를 대상으로 인터뷰를 진행하거나 담당 수사관이 작성한 피의자 사건기록을 참고하는 방법을 채택했다.

3.2. 인터뷰 설계 및 데이터 수집

<표 1>는 피의자 및 담당 수사관을 대상으로 인터뷰를 하거나, 담당 수사관이 조사하며 기록한 사건기록에서 정보를 추출하기 위해 인터뷰 내용을 구성한 것이다. 데이터는 사이버 범죄의 유형 중 정보통신망이용 범죄의 저작권 침해와 정보통신망 이용 불법콘텐츠 범죄의 도박 및 음란물 범죄를 대상으로 수집했다.

사이버 범죄에 대한 피의자 인터뷰 등 자료수집은 경찰서 사이버 범죄 수사팀이 관할하는 강원도 지역에서 발생한 사건을 기준으로, 해당 지역에서 접수되어 기소 의견으로 검찰청에 넘겨진 사건들을 중심으로 자료를 수집했다. 이는 2010년부터 2015년까지의 범죄 사건을 대상으로 하며, 이후 검찰청에서의 기소 여부나 기소 후 법원에서의 판결 여부는 고려하지 않았다. 본 연구에서는 정보통신망이용 범죄의 저작권 침해 33건과 불법콘텐츠 범죄의 도박 22건, 음란물 24건의 총 79건의 사례를 수집했다. 이는 해당 범죄행위를 저지른 피의자 44명과 그 피의자들을 조사한 담당 수사관 4명을 대상으로 인터뷰가 진행되었으며, 해당 담당 수사관이 조사 중에 기록한 피의자 신문조사 79건도 참고했다.

<표 2>는 사이버 범죄의 유형별 사례 수집 현황을 표시한 자료이다. 언급한 바와 같이 사이버 범죄의 각 유형에 해당되는 형법 및 특별법의 죄명을 고려하여 해당 범죄행위를 저지른 피의자를 중심으로, 총 79건의 데이터를 수집했다.

3.3. 데이터 분석

데이터 분석 단계에서는 인터뷰를 통해 수집한 데이터를 바탕으로 각 사이버 범죄 유형을 분석하고, 사이버 범죄의 유형별 특징을 바탕으로 예방 및 대응방안을 제안하고자 한다. 본 연구에서는 사이버 범죄 중 정보통신망 이용 범죄의 (1) 저작권 침해 및 정보통신망이용 불법콘텐츠 범죄의 (2) 도박, (3) 음란물에 해당하는 세부 유형에 대하여 분석을 실시했다. 데이터 추출은 두 가지 방식으로 이루어졌는데, 첫 번째 방식은 사전에 설계된 인터뷰 질문을 피의자나 수사관에게 직접 물어보고, 그에 대한 답변을 상세하게 기록한 것이다. 두 번째 방식은 담당 수사관이 조사 과정에서 작성한 기록에서 인터뷰 질문에 대한 답변을 최대한 상세히 추출한 것이다. 데이터 추출 다음으로, 주제나 이름으로 범주화 시킨 뒤 하나의 분석 단위를 생성하여 분석 대상이 될 데이터와 그렇지 않은 데이터를 구분하였다. 이때 분석 대상이 된 데이터는 코딩분석(Coding Analysis) 방법을 통해 내용이나 의미를 개념화시켰다. 또한, 분석 결과에 대한 타당성을 검증하기 위하여 데이터 내에서 핵심 키워드를 추출하는 텍스트 마이닝(text mining) 분석과 사이버 범죄 및 정보시스템 분야 연구자들의 동료 검사(Peer Review)를 통해 이전 단계에서 얻어진 범주를 재검토한 후 최종적으로 사이버 범죄의 주요 요인을 도출하였다. 이러한 본 연구의 전반적인 흐름은 <그림 1>에서 확인할 수 있다.

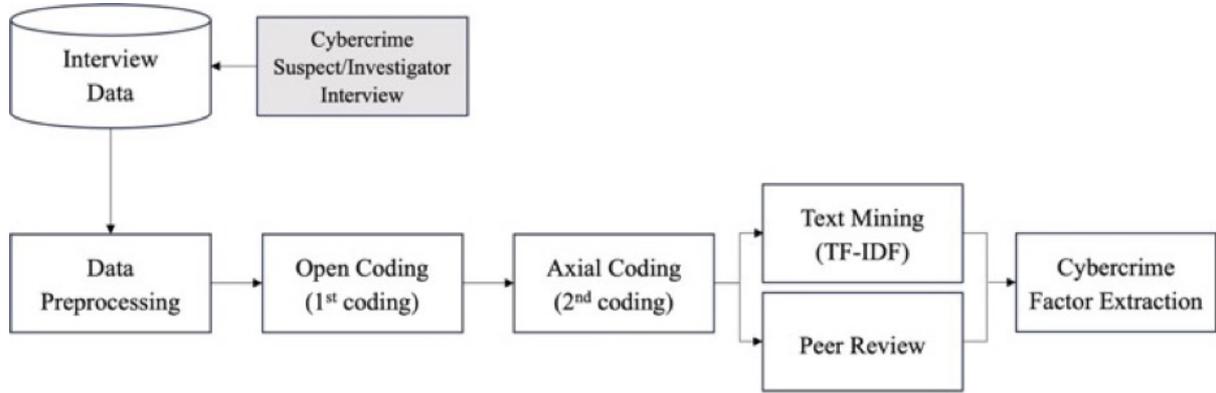
코딩분석이란 질적 연구에서 연구자가 관여하는 기본적인 분석 과정이며, 개방코딩(Open Coding), 축 코딩

〈표 1〉 사이버 범죄(저작권 침해, 도박, 음란물) 인터뷰 문항 구성

범주	인터뷰 질문
개인 환경	성별, 연령, 교육수준, 직업, 소득수준 및 혼인여부
범죄 기록	(과거에) 형사적 처벌을 받은 경험이 있습니까?
피해자관계	범죄의 대상은 누구였습니까?
범행이용매체	어떤 경로(서비스 혹은 매체)를 이용하여 범행했습니까?
범행방법	정보통신망에서 어떤 방법으로 범행했습니까?
범행가능이유	정보통신망에서 범행을 저지를 수 있었던 이유는 무엇입니까?
범행동기	해당 범죄행위를 한 이유는 무엇입니까?

〈표 2〉 사이버범죄 유형별 사례 수집 현황

대분류	중분류	사례수	인터뷰
정보통신망 이용범죄	저작권 침해	33	피의자 인터뷰: 16명 수사관 인터뷰: 4명(중복) 사건기록: 33건
	도박	22	
정보통신망 이용 불법콘텐츠범죄	음란물	24	피의자 인터뷰: 28명 수사관 인터뷰: 4명(중복) 피의자신문조사: 46건
	합계	79	



〈그림 1〉 연구 절차

(Axial Coding), 선택코딩(Selective Coding)의 세 가지 기본적인 코딩 유형이 있다(Corbin & Strauss, 1990). 1차 코딩인 개방코딩(Open Coding)은 데이터를 자세히 검토하고 현상을 명명하거나 같은 현상에 속하는 것처럼 보이는 개념끼리 분류하는 일종의 분석 작업이다. 이후 2차 코딩인 축 코딩(Axial Coding)을 통해 새로운 범주들을 기존의 코드 및 범주들과 의미론적으로 연결하는 데 중

점을 두고 진행한다. 축 코딩은 여러 코드와 범주들을 분류, 대조, 통합, 재구성, 삭제, 이동시키는 작업으로써 추상도 높은 범주들을 생성하고 그 범주들의 특징과 관계를 해명하는 과정으로, 1차 코딩에서 도출된 코드보다 더욱 지시적이고 선택적이며 개념적인 특징을 나타낸다(Glaser, 1978).

본 연구에서는 먼저 초기 코딩분석을 통해 사이버 범

죄 피의자를 중심으로 인터뷰 진행 및 데이터 수집 과정에서 성별, 연령, 소득수준, 학력수준, 직업 및 업종, 가족관계 등과 같은 개인 환경 요인과 더하여 범행동기, 범행가능이유, 범행방법, 범행이용매체, 범행대상 및 범행전과 등과 같은 범행 특성 요인을 사이버 범죄의 요인으로 간주하여 마스터 리스트(Master List)에 기반한 사전 코딩 방식으로 분석을 수행하였다. 이어서, 12개 항목으로 구성된 마스터 리스트 내에서 의미 있는 패턴을 개념화하고, 이 중에서 상호 관련성이 있거나 유사한 요소들을 찾아내어 이들을 범주화하는 개방코딩(Open Coding) 방법으로 분석을 진행했다. 그 다음으로, 개방코딩의 결과인 범주화된 요인들을 바탕으로 요인간 관계를 정리하고 인과관계에 좀 더 부합하는 결합된 요인들로 분류하기 위해 축 코딩(Axial coding) 분석을 실시하였으며, 이 분석 과정을 통해 해당 현상을 깊이 이해하고자 하였다.

추가적으로, 범주화 과정의 신뢰성을 높이기 위해 데이터 내에서 핵심 키워드를 추출하는 텍스트 마이닝 분석을 실시하여 이전 단계에서 도출한 요인과 비교하였다. 텍스트 마이닝(Text Mining)이란 대량의 비정형 텍스트 데이터에서 유용한 정보를 추출하고, 이를 분석하여 패턴, 트렌드, 관계를 발견하는 분석 방법론이다. 그중 TF-IDF(Term Frequency-inverse Document Frequency)는 문서에서 핵심적인 키워드를 추출하는 데 사용되는 방법으로, 단어 빈도수를 기반으로 한 키워드 추출 방식보다 더 정교한 계산 방법을 적용한다(김진솔 외, 2021). 단어 빈도 분석은 한 개의 문서 내에서 자주 나타나는 단어를 중요하게 여기는 반면, TF-IDF는 특정 문서에서만 높은 빈도로 나타나고 다른 문서에서는 드물게 나타나는 단어를 그 문서의 주요 키워드로 도출하는 방식이다. 이전 단계에서 도출한 요인을 재검토하기 위하여 TF-IDF 기법을 통해 최종적으로 분석 대상이 된 데이터를 대상으로 핵심 키워드를 추출하였다. 그리고 이전 단계에서 도출한 요인과 비교 분석함으로써 기존 요인에 대하여 추가

적인 검증을 실시하였다.

마지막으로, 본 연구자 외 세 명의 동료 연구자로부터 피의자 중심으로 추출한 인터뷰 내용, 마스터 리스트의 항목 그리고 개방 코딩을 통해 얻은 범주화된 항목을 재검토하는 동료 검사(Peer Review)를 진행하였다. 해당 단계에서는 잠재적 편향을 피하기 위하여 세 명의 다른 연구자들이 코딩 분석을 수행하였다. 각 코더는 인터뷰 기록을 한 줄씩 검토하며 코드들을 범주 간 합의된 요인(개념)으로 그룹화하였다. 전체 코딩 절차에 대한 평가자 간 신뢰도는 평균 0.77이었으며, Cohen의 Kappa 계수는 평균 0.76으로 평가자 간 신뢰도가 허용 가능한 수준임을 나타내었다.

이와 같이 피해자 인터뷰 자료 분석을 통하여 성별, 연령, 소득수준, 학력수준, 직업 및 업종, 가족관계 등과 같은 개인 환경 요인과 더하여 범행동기, 범행가능이유, 범행방법, 범행이용매체, 범행대상 및 범행전과 등과 같은 범행 특성 요인에 속하는 발생 원인 요인을 식별하여 개념화하고 그 빈도를 측정하였으며, 식별된 요인들이 사이버 범죄의 발생과 어떠한 연관성을 가지는지 분석하였다.

4. 분석 결과

4.1. 정보통신망이용 범죄: 저작권 침해

4.1.1. 개인 환경 분석

다음은 정보통신망 이용범죄(저작권 침해)의 개인 환경 요인 별 비율을 나타낸 자료이다. 정보통신망 침해범죄(저작권 침해) 33건에 대해 성별, 연령, 교육수준, 직업, 소득수준, 혼인 여부와 같이 개인환경 6개 항목을 사이버 범죄의 요인으로 간주하고 분석하였다. 먼저, 성별 요인으로는 남성이 84.85%(28명), 여성이 15.15%(5명)를 차지하였다. 연령 요인으로는 30대가 42.42%(14명), 20대가

27.27%(9명), 40대가 18.18%(6명), 10대가 9.09%(3명), 50대는 3.03%(1명)를 차지하였다. 교육수준 요인으로는 고등학교가 51.52%(17명), 대학교와 대학원이 39.39%(13명), 초·중학교가 9.09%(3명)를 차지하였다. 직업·업종 요인에 있어 무직이 33.33%(11명), 파트타임을 포함한 판매업은 30.3%(10명), 일용직을 포함한 건설업은 12.12%(4명), 학생과 운수업은 각각 6.06%(2명), 공무원, 광고업, 교육업, 제조업은 각각 3.03%(1명)를 차지하였다. 소득수준 요인에 있어 월평균 130만원 이하의 소득 비율은 84.85%(28명), 130만원부터 260만원까지의 소득 비율은 15.15%(5명)를 차지하였다. 혼인 요인에 있어서는 미혼 비율이 72.73%(24명),

기혼 비율이 27.27%(9명)를 차지하였다. 이와 같은 정보통신망 이용범죄(저작권 침해)의 개인 환경 분석 결과를 도식화한 내용은 <표 3>을 통해 확인할 수 있다.

자료를 요약하면, 정보통신망 이용범죄(저작권)를 저지른 피의자들은 대다수가 30대의 미혼 남성이었다. 이들은 대부분 고등학교, 대학교 또는 대학원 수준의 교육을 이수한 학생들이었으며 지금은 취업 준비 중이거나, 이미 일하고 있음에도 소득이 상대적으로 낮은 파트타임 업종 및 일용직을 포함한 건설 관련 일자리에 종사하며 생계를 유지하는 것으로 나타났다.

<표 3> 정보통신망 이용범죄(저작권 침해) 개인 환경 요인별 비율

요인	분류	빈도
성별	남	28 (84.85)
	여	5 (15.15)
연령	10대	3 (9.09)
	20대	9 (27.27)
	30대	14 (42.42)
	40대	6 (18.18)
	50대	1 (3.03)
교육수준	초·중학교	3 (9.09)
	고등학교	17 (51.52)
	대학교·원	13 (39.39)
직업·업종	건설업(일용직 포함)	4 (12.12)
	공무원	1 (3.03)
	광고업	1 (3.03)
	무직	11 (33.33)
	운수업	2 (6.06)
	학생	2 (6.06)
	판매업(파트타임 포함)	10 (30.3)
	교육업	1 (3.03)
	제조업	1 (3.03)
소득수준	130만원~260만원	5 (15.15)
	130만원 이하	28 (84.85)
혼인	기혼	9 (27.27)
	미혼	24 (72.73)
표본 수		33

4.1.2. 범행 특성 분석

<표 4>는 정보통신망 이용범죄(저작권 침해)의 범행 특성 요인 별 분석결과이다. 정보통신망 이용범죄(저작권) 33건의 사례에 대하여 범행 특성 요인에 속하는 6개 항목을 사이버 범죄의 요인으로 간주하여 분석을 실시했다.

첫 번째, 범행동기 요인을 구체적으로 분석했을 때, 아 이템에 해당하는 피의자는 다운로드를 위한 포인트 획득을 위해서라고 답변했으며 비율은 45.45%(15건)으로 나타났다. 충동심이라고 대답한 피의자는 지루해서, 합법으로 여겨서, 호기심이 생겨서라고 답변했으며 그 비율은 39.39%(13건)으로 나타났다. 부탁에 해당하는 피의자의 경우 온라인에서 알게 된 지인의 부탁을 받아서라고 답변했고 그 비율은 9.09%(3건)으로 나타났다. 정보이용에 속하는 피의자는 상업적으로 이용하기 위해서라고 답변했고, 정보공유에 관련된 피의자는 음악을 타인에게 알려주기 위해서라고 답변했다. 실제로 인터뷰 동안 범행동기를 질문했을 때, 일부 피의자는 ‘저작권법 위반에 해당될 줄은 알았지만 정말 이렇게 범죄 행위가 될 줄 몰랐다’, ‘회사를 운영하고 있는데 소비자에게 광고를 하려고 했다’라고 답변했다.

두 번째, 범행가능이유 요인으로는 제재없음의 비율이

〈표 4〉 정보통신망 이용범죄(저작권 침해) 범행 특성 요인별 비율

요인	구분	내용	빈도 (%)
범행동기	아이템	포인트 사용 (다운로드)	15 (45.45)
	충동심	무료함, 합법으로 생각, 호기심	13 (39.39)
	부탁	타인	3 (9.09)
	정보이용	상업적 이용	1 (3.03)
	정보공유	알리기 위함 (단순 공유)	1 (3.03)
범행가능이유	제재없음	업로드 가능 (제재 없음), 자동업로드	33 (100)
범행방법	유포	드라마, 소설, 영화 업로드	30 (90.91)
	이용	서체, 프로그램 사용	3 (9.09)
범행이용매체	웹하드		24 (72.73)
	공유 소프트웨어		5 (15.15)
	직접	직접 이용, 직접 판매	2 (6.06)
	SNS	네이버 블로그	1 (3.03)
	사이트	무료폰트새날	1 (3.03)
범행대상	무관		33 (100)
범행전과/동일전과포함	0		14 / 0 (42.42)
	1		11 / 7 (33.33)
	2~5		5 / 0 (15.15)
	6~9		2 / 1(6.06)
	10~19		1 / 1 (3.03)

100%(33건)를 차지했다. 범행가능이유에 대하여 세부적으로 분석했을 때, 피의자는 아무 제재 없이 파일 업로드가 가능해서, 파일이 자동으로 업로드 되어서라고 답변하였다. 일부 피의자는 실제로 인터뷰 동안 범행가능요인을 묻는 질문에 ‘컴퓨터에 저장하고 있었던 것을 올렸으며, 올릴 때 별 어려움이 없었다’, ‘무료폰트 사이트가 있는데 여러 서체를 무료로 다운 받을 수 있도록 게시되어 있다’라고 답변했다.

세 번째로, 범행방법 요인과 관련하여 유포의 비율은 90.91%(30건), 이용의 비율은 9.09%(3건)를 차지했다. 범행방법에 대하여 세부요인을 확인했을 때, 유포에 해당하는 피의자는 드라마, 영화, 소설 등을 웹하드 등에 업로드 하였다고 답변했다. 이용에 해당하는 피의자는 타인이 만든 서체 프로그램을 사용했다고 답변했다. 일부 피의자는 실제로 인터뷰 동안 범행방법을 묻는 질문

에 ‘웹하드 사이트에서 다운로드 받아서 컴퓨터에 저장했던 것을 올린 것이다’, ‘DX 새날 폰트를 무료로 받아 광고를 만들고 홈페이지에 게시했다’라고 답변했다.

네 번째로, 범행이용매체 요인과 관련하여 웹하드 비율은 72.73%(24건), 공유 소프트웨어 비율은 15.15%(5건), 직접의 비율은 6.06%(2건), SNS, 사이트의 비율이 각각 3.03%(1건)를 차지했다. 범행이용매체를 구체적으로 분석한 결과, 웹하드에 속하는 피의자는 애플파일, 엠파일 등 웹하드를 이용했다고 답변했다. 공유 소프트웨어에 속하는 피의자는 유토렌트나 비트토렌트와 같이 P2P 방식의 공유프로그램을 이용했다고 답변했다. SNS에 속하는 피의자는 네이버 블로그를 이용했다고 답변했다. 사이트에 속하는 피의자는 무료폰트새날 사이트의 서비스를 이용했다고 답변했다.

다섯번째로, 범행대상 요인과 관련하여 무관이 100%

(33건)를 차지했다. 여섯 번째로, 범행전과 요인으로는 전과없음이 42.42%(14건), 전과 1범이 33.33(11건), 전과 2~5범이 15.15(5건), 전과 6~9범이 6.06%(2건), 전과 10~19범이 3.03%(1건)를 차지했다. 또한 범행전과가 있는 피의자 중 동일한 전과를 가지고 있는 피의자는 1범 11건 중 7건, 6~9범 2건 중 1건, 10~19범 1건 중 1건을 차지했다.

다음은 인터뷰 결과 중 피의자가 세부적으로 응답한 항목인 범행동기 요인과 범행방법 요인에 대하여 키워드 분석을 실시한 결과이다. 각 응답에서 정규 표현식을 통해 단어만 추출한 후, 단어의 빈도 수를 계산하여 가장 빈번하게 등장한 단어를 추출하였고 이를 코딩 분석의 결과와 비교하였다. 먼저, 범행 동기 요인에 대해서는 ‘영화’(13건), ‘포인트’(13건), ‘받기 위험’(12건), ‘드라마’(4건), ‘다운로드’(4건)가 가장 빈번히 등장했다. 다음으로 범행방법 요인에서는 ‘허락없이’(32건), ‘다운로드’(31건), ‘인터넷을 통한’(30건), ‘유포’(25건), ‘웹하드 업체’(20건)가 가장 빈번하게 등장한 것으로 나타났다. 기존의 분석 결과와 키워드 분석의 결과를 비교하였을 때, 가장 빈번하게 등장한 단어가 직접 실행한 코딩 분석 결과와 유사함을 확인하였다.

범행동기 요인과 관련하여 그 비율의 합이 50% 이상을 차지하고 있는 아이템과 충동심이 다른 요인들과 갖는 관계를 분석한 결과는 다음과 같다. 먼저 범행가능이유 요인에 대하여 분석했을 때, 아이템 15건과 충동심 13건 전부 제재없음으로 확인되었다. 범행방법 요인으로는 아이템 15건 전부 유포였으며, 충동심 13건 중 10건이 유포, 3건은 이용으로 확인되었다. 범행이용매체 요인에 대하여 분석한 결과, 아이템 15건 중 14건은 웹하드, 1건은 토렌트로 확인되었고, 충동심 13건 중 6건은 웹하드, 4건은 공유 소프트웨어, 2건은 직접, 1건은 사이트로 확인되었다.

4.2. 정보통신망이용 불법콘텐츠 범죄: 도박

4.2.1. 개인 환경 분석

다음은 정보통신망 이용 불법콘텐츠 범죄(도박)의 개인 환경 요인 별 비율을 나타낸 자료이다. 정보통신망 이용 불법콘텐츠 범죄(도박) 22건에 대해 성별, 연령, 교육 수준, 직업, 소득수준, 혼인 여부와 같이 개인환경 6개 항목을 사이버범죄의 요인으로 간주하고 분석하였다. 먼저 성별 요인으로는 남성이 100%(22명)를 차지하였다. 연령 요인으로는 30대가 40.91%(9명), 20대가 36.36%(8명), 40대가 18.18%(4명), 50대는 4.55%(1명)를 차지한 것으로 나타났다. 교육수준 요인으로는 고등학교가 50%(11명), 대학교와 대학원이 36.36%(8명), 초·중학교가 13.64%(3명)를 차지하였다. 직업·업종 요인과 관련하여 파트타임을 포함한 판매업은 27.27%(6명), 일용직을 포함한 건설업과 무직이 각각 13.64%(3건), 운수업, 유흥업, 조선업이 각각 9.09%(2건), 공무원, 학생, 교육업, 제조업이 각각 4.55%(1건)를 차지하였다. 소득수준 요인과 관련하여 월평균 130만원 이하의 소득 비율은 50%(11명), 130만원부터 260만원까지의 소득 비율은 27.27%(6명), 260만원 이상 소득 비율이 22.73%(5명)를 차지하였다. 혼인과 관련하여 미혼 비율은 72.73%(16명), 기혼 비율은 27.27%(6명)를 차지하였다. 이와 같은 정보통신망 이용 불법콘텐츠 범죄(도박)의 개인 환경 분석 결과를 도식화한 내용은 <표 5>를 통해 확인할 수 있다.

정보통신망 이용 불법콘텐츠범죄(도박)를 저지른 피의자들은 대다수가 20대 및 30대 미혼 남성으로 나타났다. 이들은 고등학교, 대학교 또는 대학원 수준의 교육을 받은 학생들로 구성되어 있으며, 현재 취업 준비 중이거나 일용직 건설업, 운수업, 유흥업, 파트타임 판매업, 조선업, 교육업 등 다양한 일자리에 종사하며 낮은 소득으로 생계를 유지하는 것으로 보인다.

특히, 사이버 도박의 경우 다른 범죄와 달리 피의자가

〈표 5〉 정보통신망 이용 불법콘텐츠 범죄(도박) 개인 환경 요인별 비율

요인	분류	빈도
성별	남	22 (100)
연령	20대	8 (36.36)
	30대	9 (40.91)
	40대	4 (18.18)
	50대	1 (4.55)
교육수준	초·중학교	3 (13.64)
	고등학교	11 (50)
	대학교·원	8 (36.36)
직업·업종	건설업(일용직 포함)	3 (13.64)
	공무원	1 (4.55)
	무직	3 (13.64)
	운수업	2 (9.09)
	유흥업	2 (9.09)
	학생	1 (4.55)
	판매업 (파트타임 포함)	6 (27.27)
	조선업	2 (9.09)
	교육업	1 (4.55)
	제조업	1 (4.55)
	소득수준	260만원 이상
130만원~260만원		6 (27.27)
130만원 이하		11 (50)
혼인	기혼	6 (27.27)
	미혼	16 (72.73)
표본 수	22	

다양한 직업과 업종에서 나타나며, 이는 사이버 도박이 유선 네트워크 연결 시대에서 모바일 인터넷 시대로 진화함에 따라, 이제는 장소에 제약 받지 않고 언제든지 어디서든 접속하고 참여할 수 있게 되었기 때문으로 분석된다.

4.2.2. 범행 특성 분석

〈표 6〉는 정보통신망 이용 불법콘텐츠 범죄(도박)의 범행 특성 요인 별 분석결과이다. 정보통신망 이용 불법콘텐츠 범죄(도박) 22건의 사례에 대하여 범행 특성 요인에 속하는 6개 항목을 사이버 범죄의 요인으로 간주하여

분석을 실시했다.

첫째로 범행동기 요인을 구체적으로 분석했을 때, 충동심에 해당하는 피의자는 무료함을 없애기 위해서, 합법으로 생각해서, 호기심이 생겨서라고 답변했으며 가장 빈번한 수치인 54.55%(12건) 비율로 나타났다. 금전에 속하는 피의자는 고수익을 챙기기 위해, 생활비 마련을 위해라고 답변했으며, 그 비율은 22.73%(5건)로 나타났다. 부탁에 해당하는 피의자는 사회후배나 지인, 친구 등의 부탁을 받아서라고 답변했으며, 그 비율은 18.18%(4건)으로 나타났다. 편리에 속하는 피의자는 규제가 많은 합법적 절차보다 편리해서라고 답변했다. 실제로 인터뷰 동안 범행동기를 질문했을 때, 일부 피의자는 ‘최근 스포츠도 도박 사이트가 흔하게 운영되고 있고 수입도 꽤 괜찮다고 전해듣기도 해서 직접 운영해 보기 위해 사이트를 만들었다’, ‘호기심으로 시작했는데 어느새 이렇게 도박을 많이 하게 된 것 같다’라고 답변했다.

두 번째인 범행가능이유 요인으로는 제재없음에 해당하는 비율이 81.82%(18건), 구매가능에 해당하는 비율이 13.64%(3건), 권유의 비율이 4.55%(1건)를 차지했다. 범행가능이유에 대하여 세부적으로 분석했을 때, 제재없음에 해당하는 피의자는 아무 제재 없이 파일 업로드가 가능해서 또는 사이트에 접속이 가능해서라고 답변했다. 구매가능에 해당하는 피의자는 도박 프로그램 구매가 가능해서라고 답변했다. 권유에 해당하는 피의자는 지인이 동업을 제안해서라고 답변했다. 실제로 인터뷰 중에 범행동기에 대해 물었을 때, 일부 피의자는 ‘온라인에서 알게 된 도박 사이트 제작 프로그래머에게 요청하여 제작한 도박 사이트를 운영해도 문제가 없었다’, ‘인터넷 검색으로 우연히 도박 사이트의 광고를 보고 그 사이트에 접속했다’, ‘페이스북에 홍보 게시물을 올려도 처벌 받지 않을 것이라는 친구의 말을 듣고 실제로 페이스북에 직접 홍보를 하였으며 아무런 문제 없었다’라고 답변했다.

세 번째로, 범행방법 요인으로는 이용이 100%(22건)

〈표 6〉 정보통신망 이용 불법콘텐츠 범죄(도박) 범행 특성 요인별 비율

요인	구분	내용	빈도 (%)
범행동기	충동심	무료함, 합법으로 생각, 호기심	12 (54.55)
	금전	고수익, 생활비 마련	5 (22.73)
	부탁	사회후배, 지인, 친구	4 (18.18)
	편리	합법보다 편리	1 (4.55)
범행가능이유	제재없음	업로드 가능, 접속 가능	18 (81.82)
	구매가능	도박 프로그램	3 (13.64)
	권유	지인의 동업 권유	1 (4.55)
범행방법	이용	도박 사이트 운영, 도박 사이트 참여, 도박사이트 홍보	22 (100)
범행이용매체	사이트	24-cap, au-hol, cocobet, code-ba, kim-79, jk528, wowo1004	20 (90.91)
	SNS	페이스북	2 (9.09)
범행대상		무관	22 (100)
범행전과/동일전과포함		1	8 / 1 (36.36)
		2~5	7 / 4 (31.82)
		0	4 / 0 (18.18)
		6~9	1 / 0 (4.55)
		10~19	1 / 0 (4.55)
		20~29	1 / 0 (4.55)

를 차지했으며 범행방법에 대하여 세부적으로 분석했을 때, 이용이라 답한 피의자는 도박 사이트를 운영하거나 또는 도박 사이트에 참여하거나, 도박 사이트를 홍보하였다고 답변했다. 실제 인터뷰에서 피의자는 범행방법을 묻는 질문에 ‘경기도 의정부에 있는 아파트에 사무실을 만들어 서버를 운영했다’, ‘스마트폰을 이용하여 주소를 입력하고 접속했다’, ‘다른 사람이 준 문구를 페이스북에 올렸다’라고 답변했다.

네 번째로, 범행이용매체 요인에 있어 사이트는 90.91% (20건), SNS는 9.09%(2건)의 비율을 차지했다. 범행이용매체에 대하여 세부요인을 확인했을 때, 사이트에 속하는 피의자는 해외 지역에 서버를 갖고 있는 도박 사이트에 접속했다고 답변했다. SNS에 속하는 피의자는 페이스북 서비스를 이용했다고 답변했다.

다섯번째로, 범행대상 요인과 관련하여 도박은 특별

한 피해자가 없어 무관이 100%(22건)를 차지했다. 여섯 번째로, 범행전과 요인의 경우 전과 1범이 36.36%(8건), 전과 2~5범이 31.82%(7건), 전과없음이 18.18%(4건), 전과 6~9범, 전과 10~19범, 전과 20~29범이 각각 4.55% (1건)를 차지했다. 또한 범행전과를 가진 피의자 중 동일한 전과를 가지고 있는 피의자는 1범 8건 중 1건, 2~5범 7건 중 4건을 차지했다.

다음은 인터뷰 결과 중 피의자가 세부적으로 응답한 항목인 범행동기 요인과 범행방법 요인에 대하여 키워드 분석을 실시한 결과이다. 각 응답에서 정규 표현식을 통해 단어만 추출한 후, 단어의 빈도 수를 계산하여 가장 빈번하게 등장한 단어를 추출하였고 이를 코딩 분석의 결과와 비교하였다. 먼저, 범행 동기 요인에 대해서는 ‘호기심에’(7건), ‘수입’(7건), ‘게임’(5건), ‘심심해서’(5건), ‘홍보’(4건)이 가장 빈번히 등장했다. 다음으로 범행방법

요인에서는 ‘온라인 사이트’(33건), ‘스포츠 경기’(33건), ‘국외’(26건), ‘배팅’(12건), ‘계좌입금’(5건)이 가장 빈번하게 등장한 것으로 나타났다. 기존의 분석 결과와 키워드 분석의 결과를 비교하였을 때, 가장 빈번하게 등장한 단어가 직접 실행한 코딩 분석 결과와 유사함을 확인하였다.

범행동기 요인과 관련하여 50% 이상의 비율을 차지하는 충동심을 증점적으로 다른 요인들과의 관계를 분석했다. 범행가능이유 요인의 경우, 충동심 12건 전부 제외없음으로 확인되었다. 범행방법 요인은 12건 전부 이용(도박 사이트에 접속하여 이용)으로 확인되었다. 마지막으로 범행이용매체 요인에 대하여 분석한 결과, 12건 전부 사이트(도박 사이트)로 확인되었다. 또한, 정보통신망 이용 불법콘텐츠범죄(도박)는 대부분 범행전과 1범부터 5범의 이력을 가진 피의자들에 의해 발생했다. 전과 1범부터 5범까지 이력이 있는 피의자의 경우, 동일 범행을 저지른 비율이 33.33%(15건 중 5건)로 상대적으로 높았다. 범행동기는 주로 무료함, 호기심 등 충동심 해소였으며, 범행이 가능했던 주된 이유는 휴대폰 문자 메시지를 통해 이루어진 불법 도박 사이트 광고 때문에 원치 않게 광고를 접하게 되고, 포함된 도박 사이트 링크를 클릭했을 때 접속에 제한이 없었기 때문으로 보인다.

4.3. 정보통신망이용 불법콘텐츠 범죄: 음란물

4.3.1. 개인 환경 분석

다음은 정보통신망 이용 불법콘텐츠 범죄(음란물)의 개인환경 요인 별 비율을 나타낸 자료이다. 정보통신망 이용 불법콘텐츠 범죄(음란물) 24건에 대해 성별, 연령, 교육수준, 직업, 소득수준, 혼인 여부와 같이 개인환경 6개 항목을 사이버범죄의 요인으로 간주하고 분석하였다. 먼저 성별 요인으로는 남성이 91.67%(22명), 여성이 8.33%(2명)를 차지했다. 연령 요인으로는 20대가 33.33%(8명), 30

대가 29.17%(7명), 10대가 20.83%(5명) 40대와 50대는 각각 8.33%(2명)를 차지한 것으로 나타났다. 교육수준 요인으로는 고등학교가 54.17%(13명), 대학교와 대학원이 33.33%(8명), 초·중학교는 12.5%(3명)를 차지했다. 직업·업종 요인으로는 파트타임을 포함한 판매업이 29.17%(7명), 무직이 25%(6명), 학생이 20.83%(5명), 공무원과 숙박업이 각각 8.33%(2명), 운수업과 교육업이 각각 4.17%(1명)를 차지했다. 소득수준 요인에 있어서 월 평균 130만원 이하의 소득 비율은 83.33%(20명), 130만원 부터 260만원까지의 소득 비율은 12.5%(3명), 260만원 이상 소득의 비율이 4.17%(1명)를 차지했다. 혼인과 관

〈표 7〉 정보통신망 이용 불법콘텐츠 범죄(음란물) 개인 환경 요인별 비율

요인	분류	빈도
성별	남	22 (91.67)
	여	2 (8.33)
연령	10대	5 (20.83)
	20대	8 (33.33)
	30대	7 (29.17)
	40대	2 (8.33)
	50대	2 (8.33)
교육수준	초·중학교	3 (12.5)
	고등학교	13 (54.17)
	대학교·원	8 (33.33)
직업·업종	공무원	2 (8.33)
	무직	6 (25)
	숙박업	2 (8.33)
	운수업	1 (4.17)
	학생	5 (20.83)
	판매업 (파트타임 포함)	7 (29.17)
	교육업	1 (4.17)
소득수준	260만원 이상	1 (4.17)
	130만원~260만원	3 (12.5)
	130만원 이하	20 (83.33)
혼인	기혼	3 (12.5)
	미혼	21 (87.5)
표본 수		24

련하여 미혼 비율은 87.5%(21명), 기혼 비율은 12.5%(3명)를 차지하였다. 이와 같은 정보통신망 이용 불법콘텐츠 범죄(음란물)의 개인 환경 분석 결과를 도식화한 내용은 <표 7>을 통해 확인할 수 있다.

해당 내용을 종합하면, 정보통신망 이용 불법콘텐츠범죄(음란물)를 저지른 피의자들은 대다수가 20대 및 30대 미혼 남성인 것으로 나타났다. 이들은 대부분이 고등학교 진학으로 비교적 중간정도의 교육 수준을 갖고 있으며, 현재 학생이거나 이후에 일을 하고 있음에도 판매업 등 상대적으로 소득이 낮은 파트타임 일자리에 종사하여 생계를 유지하는 것으로 보인다.

4.3.2. 범행 특성 분석

<표 8>은 정보통신망 이용 불법콘텐츠 범죄(음란물)의 범행 특성 요인 별 분석결과이다. 정보통신망 이용 불법콘텐츠 범죄(음란물) 24건의 사례에 대하여 범행 특성 요인에 속하는 6개 항목을 사이버 범죄의 요인으로 간주하여 분석을 실시했다.

첫 번째로 범행동기 요인을 구체적으로 분석했을 때, 아이템 비율은 66.67%(16건), 충동심 비율은 25%(6건), 폭로, 정보공유 비율은 각각 4.17%(1건)를 차지했다. 이를 세부적으로 살펴봤을 때, 아이템에 해당하는 피의자는 포인트로 다른 파일을 다운로드 하기 위해서, 포인트를 얻어 현금화하기 위해서라고 답변했다. 충동심에 해당하

<표 8> 정보통신망 이용 불법콘텐츠 범죄(음란물) 범행 특성 요인별 비율

요인	구분	내용	빈도 (%)
범행동기	아이템	포인트 사용(다운로드), 포인트 사용(환전)	16 (66.67)
	충동심	성적 욕구 충족, 동조, 화물이(상대방 언행)	6 (25)
	폭로	알리기 위함(상대방 언행)	1 (4.17)
	정보공유	알리기 위함(자존심)	1 (4.17)
범행가능이유	제재없음	업로드 가능	18 (75)
	개인정보 인지가능	무작위, 알고 있는 전화번호	6 (25)
범행방법	유포	음란한 동영상 업로드, 음란한 영상 제작 또는 업로드	18 (75)
	전송	음란한 동영상·문자·영상 전송	6 (25)
범행이용매체	웹하드	파일조, 파일독, 본디스크, 수디스크 등	16 (66.367)
	문자	문자(sms)	3 (12.5)
	SNS	페이스북, 네이버 블로그	2 (8.33)
	메신저	카카오톡	2 (8.33)
	통화	영상통화	1 (4.17)
범행대상	무관		20 (83.33)
	선후배		2 (8.33)
	친구		1 (4.17)
	가족		1 (4.17)
범행전과/동일전과포함	0		13 / 0 (54.17)
	2~5		5 / 0 (20.83)
	1		3 / 0 (12.5)
	10~19		2 / 2 (8.33)
	6~9		1 / 0 (4.17)

는 피의자는 성적 욕구를 충족하려고, 동조하기 위해, 상대방의 말과 행동에 화풀이를 하고 싶어서라고 답변했다. 폭로에 해당 하는 피의자는 타인의 말과 행동을 알리기 위한 목적이라고 답변했다. 정보공유에 속하는 피의자는 자존심을 알리기 위해서라고 답변했다. 실제로 인터뷰 중에 범행동기에 관해 물었을 때, 일부 피의자는 ‘동영상을 업로드하면 조회 수에 비례해 받는 포인트로 다른 동영상을 다운로드하는 데 사용했다’, ‘왜 그랬는지 모르겠다. 그냥 그렇게 보내면 성적으로 기분이 좋았다’, ‘아내가 나와 다른 사람이 부적절한 관계를 가지고 있다고 오해하였고, 아내 또한 외도를 하고 있었기에 가족들도 이를 알고 있어야 된다는 생각에 전송했다’라고 답변했다.

두 번째로, 범행가능이유 요인으로는 제재없음 비율이 75%(18건), 개인정보 인지가능 비율이 25%(6건)를 차지했다. 범행가능이유에 대하여 세부요인을 확인했을 때, 제재없음에 해당하는 피의자는 아무런 제재가 없었고 바로 업로드가 가능해서라고 답변했다. 개인정보 인지가능에 해당하는 피의자는 전화번호를 임의로 고르거나, 주변인이나 인터넷을 통해 이미 상대방의 전화번호를 알고 있었다고 답변했다. 실제로 인터뷰 동안 범행가능이유를 질문했을 때, 일부 피의자는 ‘다른 사람이 다 올렸을 때 아무런 이상이 없어서 올렸다’, ‘같은 회사에 다녀 전화번호를 알고 있었다’, ‘가족들이라 전화번호는 다 알고 있었다’라고 답변했다.

세 번째로, 범행방법 요인에 있어 유포 비율이 75%(18건), 전송 비율이 25%(6건)를 차지했으며 범행방법에 대해 세부적으로 분석했을 때 답변은 다음과 같다. 유포에 해당하는 피의자는 음란한 동영상이나 사진을 업로드하거나, 음란한 사진을 제작한 뒤 업로드했다고 답변했고, 전송에 해당하는 피의자는 음란한 사진이나 동영상, 문자를 전송했다고 답변했다. 실제 인터뷰에서 피의자는 범행방법을 묻는 질문에 ‘집에서 개인용 PC를 이용해 일평균 4-5개 정도를 일주일간 업로드했다’, ‘발신번호를 보이지

않게 한 뒤 성적인 문자를 보냈다’, ‘카카오톡을 통해 여자위키구가 촬영된 사진을 전송했다’라고 답변했다.

네 번째로, 범행이용매체 요인에 있어 웹하드는 그 비율이 66.67%(16건), 문자는 12.5%(3건), SNS와 메신저는 각각 8.33%(2건), 통화는 4.17%(1건)를 차지했다. 범행이용매체에 있어 세부요인으로는, 가장 높은 비율을 차지한 웹하드의 경우 해당 피의자는 파일조, 파일독, 본디스크 등 웹하드 서비스를 이용했다고 답변했다. 이어서 문자에 해당하는 피의자는 기본 문자(SMS)를 이용했다고 답변했고, SNS에 해당하는 피의자는 블로그, 페이스북 서비스를 이용하였다고 답변했다. 마지막으로 메신저라고 응답한 피의자는 카카오톡을 이용하였다고 대답했으며, 통화라고 응답한 피의자는 영상통화를 이용하였다고 답변했다.

다섯번째로, 범행대상 요인과 관련하여 무관의 비율이 83.33%(20건), 선후배의 비율이 8.33%(2건), 친구와 가족의 비율이 각각 4.17%(1건)를 차지했다. 여섯번째로, 범행전과 요인과 관련하여 전과없음이 54.17%(13건), 전과 2~5범이 20.83%(5건), 전과 1범이 12.5%(3건), 전과 10~19범이 9.33%(2 건), 전과 6~9범이 4.17%(1건)를 차지했다. 또한 범행전과가 있는 피의자 중 동일한 전과를 가진 피의자는 10~19범의 2건 중 2건 전부를 차지했다.

다음은 인터뷰 결과 중 피의자가 세부적으로 응답한 항목인 범행동기 요인과 범행방법 요인에 대하여 키워드 분석을 실시한 결과이다. 각 응답에서 정규 표현식을 통해 단어만 추출한 후, 단어의 빈도 수를 계산하여 가장 빈번하게 등장한 단어를 추출하였고 이를 코딩 분석의 결과와 비교하였다. 먼저, 범행 동기 요인에 대해서는 ‘포인트’(16건), ‘환전’(13건), ‘사람들이 받아서’(13건), ‘성적욕구 충족’(5건), ‘화가나서’(4건)이 가장 빈번히 등장했다. 다음으로 범행방법 요인에서는 ‘게시’(18건), ‘사이트’(15건), ‘동영상 전송’(11건), ‘메신저’(3건), ‘전화’(1건)이 가장 빈번하게 등장한 것으로 나타났다. 기존의 분석

결과와 키워드 분석의 결과를 비교하였을 때, 가장 빈번하게 등장한 단어가 직접 실행한 코딩 분석 결과와 유사함을 확인하였다.

범행동기 요인과 관련하여 50% 이상의 비율을 차지하는 아이템을 중점적으로 다른 요인들과의 관계를 분석하였다. 먼저 범행가능이유 요인과의 관계 분석 결과, 아이템 16건이 전부 제재없음으로 확인되었다. 범행방법 요인과의 관계에서는 아이템 16건 전부 유포(인터넷을 통해 업로드)로 확인되었다. 범행이용매체 요인으로는 아이템 16건 전부 웹하드로 확인되었다.

이와 같이, 정보통신망을 통한 음란물의 불법 유통은 대부분 범죄 경력이 없거나 최초 범행부터 5범까지인 피의자들에 의해 수행되었으며 동일 범행은 나타나지 않았다. 이러한 범행 동기는 정보통신망 이용범죄(저작권)와 유사하게 영화, 드라마 등의 저작물을 웹하드 사이트에서 다운로드 하기 위해 필요한 포인트(사이버머니)나 기타 아이템을 획득하기 위한 욕구에서 비롯된 것으로 보인다. 특히, 음란물의 경우 일반 저작물과는 달리 선정적이고 자극적인 특성을 가지고 있어 더 큰 호기심과 다운로드 행동을 일으키며, 이는 더 많은 포인트 적립이 가능하다. 따라서 피의자들은 이러한 특성을 이용하여 더 많은 포인트를 축적하고 현금으로 환전하기 위해서 범행을 저지른 것으로 보인다. 이어서 범행이 가능했던 이유로는 웹하드 사이트에서 음란물 다운로드에 대한 제재가 없었으며, 또한 이를 다시 웹하드 사이트에 업로드 할 때 도 특별한 제재가 없었기 때문으로 보인다.

5. 결론

5.1. 연구 결과 토의

본 연구는 사이버범죄의 유형을 경찰청 사이버안전국

사이버범죄 범죄통계자료 작성의 구분 기준을 참고하여 정보통신망 침해 범죄, 정보통신망이용 범죄, 정보통신망 이용 불법콘텐츠 범죄의 세 가지 유형으로 분류하고 그중 정보통신망이용 범죄의 ‘저작권 침해’와 정보통신망 이용 불법콘텐츠 범죄의 ‘도박’, ‘음란물’을 중심으로 범죄 피의자의 인터뷰 결과를 분석하였다. 데이터 수집 방법으로는 피의자 인터뷰 및 수사관 인터뷰, 피의자 신문조사를 이용했으며 ‘저작권 침해’는 33건, ‘도박’은 22건, ‘음란물’은 24건으로 총 79건의 사례를 수집하였다. 수집된 데이터를 바탕으로 성별, 연령, 소득수준, 학력수준, 직업 및 업종, 가족관계 등 개인 환경 요인과 범행동기, 범행가능이유, 범행방법, 범행이용매체, 범행대상 및 범행전과 등 범행 특성 요인으로 분류하여 분석했고 이를 사이버 범죄의 요인으로 간주하여 세 개의 사이버 범죄 유형별 요인별 분석 결과를 토의하고자 한다.

먼저, 개인 환경에 대한 분석결과는 다음과 같다. ‘도박’의 경우 성별이 전원 남성이었으며, ‘저작권 침해’와 ‘음란물’의 경우 남성이 각각 84%와 91%로 다수를 차지했다. 연령별로는 30대와 20대가 모든 범죄 유형에서 가장 높은 비율을 보였으며, 특히 ‘저작권 침해’에서 이 두 연령대의 합이 69%를 상회했고, ‘도박’은 두 연령대 합이 77%를 넘었으며, ‘음란물’은 두 연령대의 합이 62%를 넘는 것으로 나타났다. 교육수준으로는 모든 유형에 있어 고등학교 졸업이 가장 많았고, 대학교나 대학원을 재학중이거나 졸업한 비율이 그 뒤를 이었다. 직업 및 업종에서는 ‘도박’과 ‘음란물’의 경우 파트타임을 포함한 판매업 종사자가, ‘저작권 침해’는 무직이 가장 많았다. 소득수준으로는 ‘저작권 침해’와 ‘음란물’에서 80% 이상이 130만원 이하였으며, ‘도박’의 경우 50%가 130만원 이하이고 130만원부터 260만원까지의 비율이 27%를 상회하며 그 뒤를 이었다. 미혼자의 비율은 모든 유형에서 70% 이상으로 나타났다. 즉 세 유형의 사이버 범죄에 대하여 개인 환경 요인을 요약했을 때, 주로 고등학교 이상

의 교육을 받고, 판매직을 포함한 파트타임 직업이거나 무직인 20대와 30대의 미혼 남성에게 의해 주로 발생했다.

그 다음으로 범행 특성의 분석 결과 비교이다. 첫째, 범행동기에서는 세 유형의 사이버 범죄에서 공통적으로 나타난 항목은 ‘충동심’이었다. 그중 ‘도박’에서 충동심이 차지하는 비율은 절반 이상을 상회하는 것으로 나타났다. 실제로 충동심으로 도박 범죄를 행한 피의자 중 일부는 무료함을 없애기 위해서였거나 호기심이 생겨서 또는 합법이라고 생각해서 범행을 저질렀다고 밝혔으며, 실제 인터뷰 사례 중 일부는 도박을 게임의 한 종류로 인식하여 행한 것으로 나타났다. ‘저작권 침해’의 경우, 가장 높은 비율을 차지한 ‘아이템’에서 피의자는 다른 파일을 다운받기 위해 포인트가 필요해서라고 답했으며, 실제 인터뷰 사례 중 다른 영화나 드라마를 다운받기 위해 저질렀다고 답변한 사례가 있었다. ‘음란물’에서 가장 높은 비율을 차지한 ‘아이템’의 경우 포인트가 필요해서라고 답했으며, 실제 인터뷰에서 일부 피의자들은 포인트를 받고 실제 현금으로 환전하기 위해서라고 답변했다. 즉, 사이버 범죄의 세 가지 유형에서 피의자들은 충동적이거나 상업적 의도를 가지고 범죄를 저지른 것으로 해석할 수 있다.

둘째, 범행가능이유인 경우 세 유형의 사이버 범죄에서 공통적으로 나타난 항목은 ‘제재 없음’이었다. 특히 ‘저작권 침해’에서 제재 없음이 100%를 차지했으며, 해당 이유로 피의자들이 범죄를 저지르기 용이했음을 보여준다. 이는 현재 불법 콘텐츠 공유가 만연해지며 문화 산업 전반에서 피해 사례가 속출하는 현재 상황을 빗대어 해석할 수 있다. 최근에 폐쇄된 대규모 불법 콘텐츠 공유 사이트 ‘누누티비’ 사례에서 볼 수 있듯, 사용자는 별도의 회원 가입이나 연령 인증 없이도 쉽게 콘텐츠를 이용할 수 있었다. 이와 같이 불법 복제 사이트의 수와 사용자가 증가하는 현상에 대해, 불법 복제행위를 긍정적으로 보고 누군가가 복제 콘텐츠를 올려주기를 기다리는

일종의 사회적 수요가 있다고 해석할 수 있다(박경자, 2016). 그리고 ‘도박’과 ‘음란물’의 경우, ‘제재없음’이 각각 약 81%, 75%를 차지하며 각 유형 별 범행가능 이유에서 가장 높은 수치를 나타냈다. 이는 두 범죄 유형에서도 피의자들이 별 다른 제재 없이 자유롭게 범죄를 행할 수 있었음을 나타낸다.

셋째, 범행 방법의 경우 ‘저작권 침해’와 ‘음란물’에서 가장 높은 비율을 보인 항목은 ‘유포’였다. ‘저작권 침해’에서 유포의 비율은 90%를 상회했으며, ‘음란물’에서는 75%가 유포 관련이고 나머지 25%는 ‘이용’이 차지했다. ‘도박’과 관련해서는 사이트를 직접 운영하거나 참여 또는 홍보한 경우인 ‘이용’이 100%를 차지했다. 인터뷰 결과에 따르면 많은 피의자들이 불법 도박 사이트 이용이 금전적으로 도움이 된다는 주변인의 말을 듣고 직접 사용해보거나 운영한 것으로 나타났다. 특히, 주변 사람들의 영향을 받아 범죄에 손을 대는 경우가 많아, 피의자들은 평소 사이버 범죄에 쉽게 노출될 환경에 있었던 것으로 보인다. 이는 최근 불법 도박이 청소년들 사이에서도 유행하고 있는 현상과 비교할 수 있다. 스마트폰과 SNS의 보편화로 인해 청소년들이 사이버 도박에 쉽게 접근할 수 있는 환경이 조성되었으며, 최근 보도에 따르면 2022년에는 도박 중독으로 병원 치료를 받은 청소년의 수가 크게 증가했다(연합뉴스, 2023). 이러한 현상은 사이버 도박이 대중적으로 널리 퍼져 있고 접근하기 쉽다는 문제점을 갖고 있음을 나타낸다.

네 번째로, 범행이용매체 측면에서 ‘저작권 침해’와 ‘음란물’ 범주에서 가장 높은 비율을 보인 것은 ‘웹하드’였다. ‘저작권 침해’의 경우, 웹하드가 전체 비중의 72.73%를 차지하며, ‘음란물’의 경우 66.36%로, 둘 다 절반 이상의 비율을 나타냈다. 실제로 경찰은 2018년 8월부터 2019년 5월까지 ‘웹하드 카르텔’을 대상으로 집중 단속을 실시하여 불법 촬영 및 음란물 게시자 647명을 체포하고 그 중 25명을 구속시키는 등 웹하드를 통한 사

이러한 범죄 단속에 주력하고 있다(정환봉, 2019). ‘도박’ 범주에서 가장 높은 수치를 기록한 범행이용매체는 ‘사이트’였으며, 그 비중은 90.91%를 기록했다. 또한, 세 가지 사이버 범죄에서 공통적으로 나타난 범행이용매체는 ‘SNS’였다. 각 범주에서 SNS가 차지하는 비중은 ‘저작권 침해’에서 3.03%, ‘도박’에서 9.09%, ‘음란물’에서 8.33%로 나타났다. 이는 비교적 낮은 수치로 해석될 수 있으나, 최근 모바일 및 SNS의 발전이 급속하게 이루어지는 점으로 보아 범행이용매체로서의 SNS 비중은 지속적인 주목을 받아야 할 것으로 보인다.

다섯째로, 범행대상 측면에서는 세 유형의 사이버 범죄 전부 ‘무관’이 가장 높은 비율을 보였다. ‘저작권 침해’와 ‘도박’의 경우 무관이 100%를 차지했으며 음란물’의 경우는 그 비중이 83.33%를 차지했고 뒤이어 선후배와 친구, 가족 순으로 나타났다. 실제 인터뷰에서 대부분의 피의자들은 어떠한 관계도 없는 사람이거나 연락처에 저장되어있다는 이유만으로 범죄를 저질렀다고 답변했다.

마지막으로, 범행전과요인과 관련하여 한번이라도 범행을 저지른 적 있는 피의자에 의해 범죄가 발생하는 비율은 ‘저작권 침해’는 57.58%, ‘도박’은 81.82%, ‘음란물’은 81.82%로 나타났다. 특히, ‘저작권 침해’의 경우 한 번의 범행 전과가 있는 피의자 중 50% 이상이 동일 전과를 갖고 있는 것으로 나타났다. 이는 다른 사이버범죄 유형들에 비해 저작권 침해의 경우 동일한 전과를 가진 범죄자들의 해당 범죄율이 높은 것을 확인할 수 있다. 더불어, 범행전과 요인의 경우, 다른 요인보다 더 세부적으로 분석될 필요가 있다. 범행 동기를 비롯하여 피의자의 행동 양식이 범행 전과 유무에 따라 확연한 차이를 보일 수 있기 때문이다. 먼저 ‘저작권 침해’의 경우, 범행전과가 없는 초범 피의자의 범행동기는 충동심이 57.14%를 차지하였는데, 재범 피의자의 경우 범행동기 중 ‘충동심’은 26.32% 정도에 그쳤으며 ‘아이템’ 취득 목적이 52.63%, ‘부탁’이 15.79%에 달하는 것으로 나타나 큰 차이를 보

였다. ‘도박’ 범죄의 경우, 초범인 피의자는 범행동기 중 ‘고수익’이 50%를 보였으나 재범인 피의자의 경우 ‘고수익’은 11.11% 정도만 차지하였고 생활비 마련과 주변 사람들의 부탁으로 인한 범행 건수가 33.33% 정도로 더 많은 것으로 나타났다. ‘음란물’의 경우, 초범 피의자의 경우 범행동기 중 현금화가 목적인 ‘아이템’이 46.15%를 차지하였고 그 뒤로 충동심이 38.46%, 폭로가 15.38%를 차지하였다. 반면 재범 피의자의 경우, ‘아이템’이 90.91%를 차지하며 충동심과 폭로와 같은 개인의 정서가 담긴 목적보다 금전적 이익을 취하려는 목적이 더욱 뚜렷하게 나타남을 확인하였다.

지금까지 살펴본 사이버 범죄의 세 가지(정보통신망이용 범죄의 저작권 침해, 정보통신망이용 불법콘텐츠 범죄의 도박과 음란물) 유형에 대하여 개인 환경과 범행 특성 측면에서의 분석 결과를 바탕으로 아래의 <표 9>에서 각 범죄 유형별 예방 및 대응방안을 제안하고자 한다.

5.2. 한계점 및 향후 연구

본 연구는 다음과 같은 한계점이 존재한다. 첫째로, 본 연구는 사이버 범죄 중 정보통신망이용 범죄의 저작권 침해와 정보통신망이용 불법콘텐츠 범죄의 도박, 음란물에 대하여 각각의 사례에 따라 개별적으로 데이터를 수집했다. 최근 불법 저작물 사이트에서는 다른 유형의 여러 불법사이트 광고를 게시하는 등 각 불법사이트 간 공생관계가 복잡한 범죄 네트워크를 형성하고 있다. 따라서 사이트나 SNS를 통해 저작권 침해 범죄를 저지른 피의자는 도박, 음란물 범죄를 함께 저질렀을 가능성도 존재한다. 본 연구에서는 각 범죄 유형 별 피의자를 개별 사건으로 구분하여 조사함으로써 이러한 범죄 간 연결 가능성을 고려하지 않았다. 따라서 여러 유형에 동시다발적으로 해당되는 범죄 사례에 대하여 피의자를 추가적으로 조사함으로써 새로운 분석 결과를 도출해낼 수 있

〈표 9〉 사이버 범죄 유형별 예방 및 대응방안 제안

구분	정보통신망이용 범죄 (저작권 침해)	정보통신망이용 불법콘텐츠 범죄(도박)	정보통신망이용 불법콘텐츠 범죄(음란물)
기술적 측면	<ul style="list-style-type: none"> 지능화된 범죄 대응을 위한 인공지능 기반 탐지 시스템 마련 다크웹 대응 기술 개발 	<ul style="list-style-type: none"> 텔레그램, 카카오톡 오픈채팅 등 휘발성 채팅 기능 내용 탐지 시스템 구축 암호화폐 활용에 따른 대응 기술 마련 	<ul style="list-style-type: none"> 딥페이크 등 인공지능 기반 범죄 탐지를 위한 허위동영상판정도구 개발 콘텐츠 내 전자서명 포함 기술 개발
	<ul style="list-style-type: none"> 콘텐츠 제공 소프트웨어 내 보안 시스템 구축 콘텐츠 메타데이터 포함(디지털 워터마크) 		
관리적 측면	<ul style="list-style-type: none"> 관련된 지자체 및 기관과 경찰청의 합동수사체계 구축 경찰 외 사이버공간 이용자가 참여가능한 파트너십 사이버경찰 활동 마련 합법적 사행성 사이트 및 연령 인증 운영 		
	<ul style="list-style-type: none"> 저작권 침해 전문 경찰 육성 웹사이트 및 플랫폼 감시 체제 강화 신속한 콘텐츠 삭제 및 사용자 제재 절차 강화 	<ul style="list-style-type: none"> 온라인 도박 사이트 모니터링 및 단속 강화 텔레그램, 카카오톡 오픈채팅 등 휘발성 채팅 모니터링 시스템 구축 	<ul style="list-style-type: none"> 유관기관의 처리 권한 확대 신고된 게시물 검토 및 처리 체계 간소화
제도적 측면	<ul style="list-style-type: none"> 저작권 법률 컨설팅과 소송 지원 제도 마련 주요 국가별 저작권 침해 사이트 정보 수집 경찰 인력의 디지털포렌식 기술 활용 역량 강화 	<ul style="list-style-type: none"> 운영 및 이용자 양측 처벌 수위 강화 불법 사이트 운영자에게 신속 조치 사이버 수사 체계 정비 	<ul style="list-style-type: none"> 음란물 신고 보상 제도 마련 개인인증 절차 다단계화 음란물 범죄 담당 수사관의 의무 조치 강화
교육적 측면	<ul style="list-style-type: none"> 저작권 윤리 교육 강화 	<ul style="list-style-type: none"> 도박 행위 예방 교육 강화 재범예방 및 치유 프로그램 마련 선도조건부 훈방 프로그램 운영 강화 	<ul style="list-style-type: none"> 온라인 인권피해 교육 강화 사이버 공간 사용 에티켓 교육 강화 체험형 교육 실시

을 것이다.

둘째로, 본 연구의 인터뷰는 2010년부터 2015년까지 강원도 지역에서 발생한 사이버 범죄 피의자들을 대상으로 진행됐다. 피의자를 중심으로 데이터를 수집함으로써 기존 연구보다 심층적인 요인 분석이 가능했으나, 사이버 범죄는 장소에 제한되지 않는 점과 각 범죄 유형에서 활용하고 있는 정보기술이 빠르게 발전하는 점을 바탕으로 인터뷰 대상을 확장하여 향후 연구를 진행할 필요가 있다. 향후 연구에서는 기존의 강원도 지역을 넘어 전국에서의 사이버 범죄 사건을 대상으로, 기술 및 온라인 서비스의 발달 흐름에 따라 변화하는 사이버 범죄 유형의 특성을 파악하는 것을 추가적으로 고려할 수 있을 것이다.

셋째로, 본 연구는 사이버범죄의 요인 도출을 위해 수행된 인터뷰 자료를 바탕으로 개인 환경 요인과 범행 특성 요인으로 구분하여 분석을 진행하였다. 이때 본 연구

에서 고려된 6개의 범행 특성 요인 외에도 추가적인 중요 요인들이 존재할 수 있다. 특히 사이버범죄의 범행 특성 요인 중 ‘범행전과/동일전과’ 항목에 대하여 세부적인 데이터를 수집함으로써 새로운 요인들을 도출해낼 수 있는 기회가 있을 것으로 생각된다. 이러한 접근 방식을 통해 향후 추가적인 연구를 진행한다면, 사이버범죄 예방 및 대응 전략을 수립하는 데 있어 이해관계자들에게 보다 명확한 시사점을 제시할 수 있을 것이라 생각한다.

5.3. 학술적 시사점

앞서 제시한 연구의 한계점에도 불구하고, 본 연구는 다음과 같은 학술적 시사점을 갖는다. 첫째, 본 연구는 사이버 범죄의 명확한 분류 체계를 활용함으로써 각 유형의 사이버 범죄의 특징과 요인을 분석하여 결과를 제시했

다. 학계에서의 사이버 범죄의 유형 분류는 아직까지 한 개의 확립된 체계가 없어 데이터 수집, 분석 및 결과 해석 과정에서 어려움이 발생할 수 있다. 따라서 본 연구는 경찰청 사이버안전국 사이버범죄에서 제시한 분류 기준을 활용하여 사이버 범죄의 각 유형에 대한 데이터를 수집하고 분석함으로써 분류 체계의 명확성을 확보했으며, 이를 통해 사이버 범죄의 분류 기준 확립의 중요성을 강조하고 향후 분류 기준 정립 과정에 기여할 수 있다. 둘째, 사이버 범죄의 실제 피의자를 대상으로 정성적 연구방법 중 인터뷰 방법을 활용하여 사이버 범죄 요인들을 밝혀냈다. 사이버 범죄 분야에서 다양한 선행 연구들이 수행되어 왔으나 대부분은 관련 통계 자료나 피해자, 일반 대중을 중심으로 한 간접적인 방법을 채택했다. 이에 본 연구는 사이버 범죄 피의자를 중심으로 인터뷰를 통해 요인 별 분석 결과를 도출하여 사이버 범죄에 대해 보다 심층적인 접근법을 제안했다. 셋째, 사이버 범죄를 저지른 피의자의 범행 특성 요인을 세부적으로 분석하고 결과를 도출함으로써 향후 사이버 범죄 관련 연구에서 활용 가능한 분석 기준을 제시했다. 본 연구는 사이버 범죄 피의자의 범행동기, 범행가능이유, 범행방법, 범행이용매체, 범행대상, 범행전과 총 6개의 범행 특성 요인을 기반으로 인터뷰 설계부터 진행, 결과 분석까지 일관된 기준을 제시했다. 이 기준은 사이버 범죄 관련 선행 연구에서 자주 활용되지 않았으며, 따라서 향후 연구의 방법론적 방향을 확장시킬 수 있는 근거가 될 수 있다.

5.4. 실무적 시사점

이어서 본 연구는 다음과 같은 실무적 시사점을 가질 수 있다. 첫째, 본 연구는 사이버 범죄의 다양한 유형 중에서도 저작권 침해, 도박, 음란물 범죄에 대한 심리적 및 인구통계학적 자료를 분석함으로써, 정책 입안과 기

술 개발 등 해결 방안의 근거가 될 수 있는 핵심 정보를 제공하였다. 이러한 범죄는 단순히 사이버 공간에서 일어나는 문제를 넘어 현실 세계의 다양한 사회적 문제로 이어질 수 있다. 예를 들어, 저작권 침해는 불법 복제와 유통으로 작품들이 무단으로 이용됨에 따라 관련 수익이 감소하는 등 문화 산업과 창작자에게 심각한 피해를 입히고 있다. 이로써 문화 산업의 성장이 저해되며, 창작자들은 정당한 보상을 받지 못할 수 있다. 도박 범죄의 경우 인터넷을 통해 언제 어디서나 불법 도박 게임에 접근할 수 있으며, 특히 모바일 기기를 통하여 도박 앱이 무수히 많이 제공됨에 따라 청소년 세대까지 쉽게 노출될 수 있다. 이에 청소년 도박 중독 문제라는 사회적 문제가 대두되었으며, 그 심각성은 더욱 커지고 있다. 음란물 범죄의 경우 성적 차별과 성폭력 문제를 촉진할 수 있다. 부적절한 이미지나 비디오 유포로 인해 사이버 공간 이용자들은 성적 차별과 폭력에 노출될 수 있으며, 이는 특히 어린 미성년자에게 큰 피해를 줄 수 있다. 따라서 이러한 범죄에 대하여 사회 전방면에서의 적극적인 해결 방안 모색이 요구된다. 본 연구는 이 세 가지 유형의 사이버 범죄에 대하여 피의자 중심 인터뷰와 그에 따른 결과 분석을 통하여, 각 범죄 유형 별 핵심 특성 정보를 제공함으로써 범죄의 심각성을 부각시키며 예방 및 대응방안에 대한 새로운 접근 방식을 제공할 수 있을 것이다.

둘째, 피의자 중심의 연구방법을 통해 사이버 범죄의 범행 동기, 범행 전과/동일전과 포함과 같은 범행 특성을 분석하고 결과를 도출함으로써 관련 사이버 범죄를 예방하고 대응할 수 있는 방안을 제시하였다. 특히, 범행 전과 유무에 따라 범행 동기와 같이 피의자 행동 심리에 차이가 존재할 수 있음을 구체적으로 밝혀냈다. 이는 범죄 예방과 대응을 위한 정부의 노력뿐만 아니라 사이버 공간 이용 주체인 민간에서의 사이버 범죄 근절 노력에도 보다 세부적으로 예방 및 대책을 마련하는 데 도움을 줄 수 있을 것이라 기대된다.

마지막으로, 본 연구에서는 피의자 중심 인터뷰 결과를 기반으로 한 기술적, 관리적, 제도적, 교육적 측면에서 사이버 범죄 유형 별 구체적인 방안을 제시하였다. 이러한 방안들은 다양한 이해 관계자들이 협력하여 구현할 수 있도록 설계되었으며, 이를 통해 사이버 범죄의 다양한 측면을 고려하여 종합적이고 실질적인 해결책을 제시할 수 있다. 이에 따라 우리 사회는 보다 안전하고 안정적인 사이버 환경을 조성하고 사이버 범죄로부터 대중들을 보호하는데 더 많은 도움을 얻을 수 있을 것으로 기대할 수 있다.

〈참고문헌〉

[국내 문헌]

1. 강석구, 윤해성, 박영우, 김민호, 권현영, 김도승, 김기범 (2010). **사이버안전체계 구축에 관한 연구**. 서울: 한국형사정책연구원.
2. 김계원, 서진완 (2012). 청소년의 인터넷 중독 수준과 사이버범죄의 상관관계 분석. **한국치안행정논집**, 9(2), 23-43.
3. 김보라, 임수진 (2022). 사이버성폭력수사관 정신건강 실태조사에 근거한 심리지원제도 개선 방향에 관한 연구. **지식경영연구**, 23(4), 43-67.
4. 김지은, 우병관 (2022). 사이버 범죄 탐지 및 분석기술에 대한 탐색적 연구. **한국치안행정논집**, 19(3), 57-76.
5. 김진술, 신동훈, 김희웅 (2021). 비정형 빅데이터를 이용한 COVID-19 주요 이슈 분석. **지식경영연구**, 22(2), 145-165.
6. 김태영 (2015). 질적 연구 방법을 사용한 자료 수집, 분석 및 논문 작성의 실제-인터뷰 방법을 중심으로. **한국언어문화교육학회 학술대회**, 9-14.
7. 김현정, 김범수 (2023). 스마트기기 활용역량과 프라이버시 우려: 온라인 사회참여 활동과 정보 사실성 판단 능력의 매개효과 및 프라이버시의 조절효과. **지식경영연구**, 24(1), 51-72.
8. 박경자 (2016). 디지털콘텐츠 불법 파일공유에 관한 사회문화적 접근. **지식경영연구**, 17(1), 113-133.
9. 박민정, 채상미 (2017). 빅데이터 환경 형성에 따른 데이터 감시 위협과 온라인 프라이버시 보호 활동의 관계에 대한 연구. **지식경영연구**, 18(3), 63-80.
10. 서승모, 권현영 (2022). 사이버범죄 대응을 위한 국가 간 공동수사팀 구성 모델. **한국경찰학회보**, 24(6), 57-86.
11. 오세연 (2015). 사이버범죄의 대응강화를 위한 디지털 포렌식 수사 활용방안. **디지털융복합연구**, 13(4), 81-87.
12. 이서현, 이새롬, 곽동현 (2022). When do i protect myself? Avoidance motivation toward online sexual harassment on social media: A study based on threat avoidance theory. **지식경영연구**, 23(3), 45-64.
13. 이성식, 전신현 (2022). 대학생의 스마트폰중독의 사이버범죄에 대한 영향과 그 완충요인에 관한 연구. **한국중독범죄학회보**, 12(3), 45-62.
14. 이소현, 강일웅, 정운혁, 김희웅 (2019). 사이버범죄 유형별 특징 분석 연구. **Information Systems Review**, 21(3), 1-26.
15. 이원상, 채희정 (2010). **사이버범죄의 새로운 유형과 형사정책적 대안연구**. 한국형사정책연구원 (연구총서 10-16-03).
16. 임현욱 (2021). 사이버범죄를 유발하는 심리적으로인 분석. **The Journal of the Convergence on Culture Technology (JCCT)**, 7(2), 157-163.
17. 정지혜 (2020). 사이버범죄 특성에 적합화된수사 및 처벌을 위한 형사법적 규제방안 연구. **입법학연구**, 17(2), 139-164.
18. 정태진 (2022). 사이버평화 구축을 위한 사이버범죄대응방안. **한국경찰연구**, 21(4), 243-256.
19. 조병인 (2000). **사이버경찰에 관한 연구: 사이버범죄의 규제를 중심으로**. 형사정책연구원 연구총서, 11-195.

[국외 문헌]

20. Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. **Internet Research**, 30(6), 1665-1687.
21. Arief, B., Adzmi, M. A. B., & Gross, T. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 1-Attackers. **IEEE Security & Privacy**, 13(1), 71-76.
22. Brenner, S. W. (2013). Cybercrime: Re-thinking crime control strategies. In **Crime online** (pp. 12-28). United States of America: Willan.
23. Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. **Qualitative Sociology**, 13(1), 3-21.
24. Glaser, B. (1978). **Theoretical sensitivity: Advances in the methodology of grounded theory procedures and techniques**. Sage Publications, CA, USA.
25. Hammersley, M., & Atkinson, P. (2019). **Ethnography: Principles in practice** (4th ed). London, UK: New York: Routledge.
26. Khosla, P., & Dubey, P. (2016). Survey paper on cyber crime: A threat to national security. **IITM Journal of Management and IT**, 7(1), 62-65.
27. McGuire, M. (2017). Cons, constructions misconceptions of computer related crime: From a digital syntax to a social semantics. **Journal of Qualitative Criminal Justice & Criminology**, 6(2).

28. McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. *Home Office Research Report, 75*, 1-35.
29. Paoli, L., Visschers, J., Verstraete, C., & Van Hellemont, E. (2018). *The impact of cybercrime on Belgian businesses* (Vol 5). UK: Intersentia.
30. Patton, M. Q. (2002). *Qualitative evaluation and research methods* (3rd ed). Newbury Park, CA: SAGE Publications, inc.
31. Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences, 2*(2), 379-398.
32. Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: Current trends. *Police Practice and Research, 19*(6), 515-518.
33. Thomas, D., & Loader, B. D. (2013). Introduction: Cybercrime: Law enforcement, security and surveillance in the information age. In *Cybercrime* (pp. 1-14). London, UK: Routledge.
34. Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol 4). Cambridge, UK: Polity.
35. Williams, M., & Levi, M. (2015). Perceptions of the eCrime controllers: Modelling the influence of cooperation and data source factors. *Security Journal, 28*, 252-271.
36. Yin, R. K. (2014). *Case study research: Design and methods*. Thousand Oaks, CA: Sage.
42. 신동섭 (2023). <https://www.ksilbo.co.kr/news/articleView.html?idxno=961493>
43. 연합뉴스 (2023). <https://m.yonhapnewstv.co.kr/news/MYH20230705011600641>
44. 오세진 (2021). <https://www.seoul.co.kr/news/newsView.php?id=20210118009027>
45. 이영아 (2023). <https://www.techm.kr/news/articleView.html?idxno=108071>
46. 임순현 (2023). <https://www.yna.co.kr/view/AKR20230926048900004>
47. 정환봉 (2019). https://www.hani.co.kr/arti/society/society_general/897783.htm

[URL]

37. 김성찬 (2023). <https://www.gnnews.co.kr/news/articleView.html?idxno=524832>
38. 김영명 (2023). <https://www.boannews.com/media/view.asp?idx=115507>
39. 김지현 (2023). <https://www.eachj.co.kr/news/articleView.html?idxno=10735>
40. 박광하 (2022). <https://www.koit.co.kr/news/articleView.html?idxno=102906>
41. 소장섭 (2023). <https://www.ibabynews.com/news/articleView.html?idxno=112019>

● 저 자 소 개 ●



강 일 응 (Ilwoong Kang)

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



김 재 희 (Jaehui Kim)

현재 연세대학교 정보대학원에서 비즈니스 빅데이터 분석 트랙 석사과정이다. 포항공과대학교 인공지능연구원에서 연구인턴으로 재직했으며, 관심 분야는 Natural Language Processing in Deep Learning, Time Series Analysis, Large Language Model이다.



이 소 현 (So-Hyun Lee)

Xi'an Jiaotong University 경영대학에서 근무한 후, 현재 경기대학교 산업경영정보공학과 조교수로 근무 중이다. 주요 연구분야는 디지털 비즈니스, 데이터 애널리틱스 등이다. 관련 연구들은 Information Systems Research, Communications of ACM, Information and Management, International Journal of Information management, Internet Research 등에 논문이 게재되었다.



김 희 응 (Hee-Woong Kim)

National University of Singapore 정보시스템학과에서 근무한 후, 현재 연세대학교 정보대학원 교수로 근무 중이다. 주요 연구분야는 디지털 비즈니스, 정보시스템 관리 및 활용 등이다. 관련 연구들은 MIS Quarterly, Information Systems Research, Journal of Management Information Systems 등에 60여 편의 논문이 게재되었다. MIS Quarterly, JAIS, IEEE TEM의 편집위원과 KrAIS회장으로 활동했고, 현재 한국경영정보학회장을 역임하고 있다.

〈 Abstract 〉

Exploring the Nature of Cybercrime and Countermeasures: Focusing on Copyright Infringement, Gambling, and Pornography Crimes

Ilwoong Kang^{*}, Jaehui Kim^{**}, So-Hyun Lee^{***}, Hee-Woong Kim^{****}

With the development of cyberspace and its increasing interaction with our daily lives, cybercrime has been steadily increasing in recent years and has become more prominent as a serious social problem. Notably, the “four major malicious cybercrimes” - cyber fraud, cyber financial crime, cyber sexual violence, and cyber gambling - have drawn significant attention. In order to minimize the damage of cybercrime, it's crucial to delve into the specifics of each crime and develop targeted prevention and intervention strategies. Yet, most existing research relies on indirect data sources like statistics, victim testimonials, and public opinion. This study seeks to uncover the characteristics and factors of cybercrime by directly interviewing suspects involved in 'copyright infringement', 'gambling' related to illicit online content, and 'pornography crime'. Through coding analysis and text mining, the study aims to offer a more in-depth understanding of cybercrime dynamics. Furthermore, by suggesting preventative and remedial measures, the research aims to equip policymakers with vital information to reduce the repercussions of this escalating digital threat.

Key words: Copyright infringement, Cyber gambling, Pornography crime, Interview analysis, Text mining

* Gangwon Provincial Police Agency

** Graduate School of Information, Yonsei University

*** Department of Industrial and Management Engineering, Kyonggi University

**** Graduate School of Information, Yonsei University