산업융합연구 제19권 제6호 pp. 37-47, 2021
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2021.19.6.037

불법스팸 방지를 위한 개선방안 : 정책적 제안을 중심으로

손종모[1], 임효창[2*]
[1]서울여자대학교 정보보호학과 조교수, [2]서울여자대학교 경영학과 교수

A Study on the Effective Countermeasure of SPAM : Focused on Policy Suggestion

Jong-Mo Sohn[1], Hyo-Chang Lim[2*]
[1]Assistant Professor, Dept. of Information Security, Seoul Women's University
[2]Professor, Dept. of Business Administration, Seoul Women's University

요 약 오늘날 이메일(E-mail), 스마트폰, SNS 등의 다양한 정보통신 매체는 정보공유 및 의사소통을 위한 필수품이다. 하지만 불법으로 수집한 개인정보와 보안에 취약한 기기를 활용하여 대량으로 불법 스팸을 보내거나, 사기에 이용하기 위한 악의적인 공격에 이용되고 있다. 불법스팸과 스미싱, 사기 메일(SCAM) 등은 기업과 사용자들에게 정신적 피로감 등의 사회적 비용뿐만 아니라 IT인프라 자원의 불필요한 소모와 경제적 손실 등 직간접적으로 많은 피해를 주고 있다. 스팸 관련 법제도가 마련되어 있지만 교묘히 회피하여 여전히 기승을 부리고 있고 피해자가 지속적으로 발생하고 있어 문제점이 없는지 검토가 필요하다. 불법스팸을 차단하고 이로 인한 사기 피해를 예방하기 위해 관련 제도를 개선하는데 기여하는 학술적 연구가 필요한 상황이다. 본 연구는 국내외 법제도와 스팸 관련 대응 활동과 문제점을 도출하고 정책적 개선 방안을 제안하였다.

키워드 : 스팸(SPAM), 문자 스팸, 전화 스팸, 이메일 스팸, 스미싱

Abstract Today, people share information and communicate with others using various information and communication media such as e-mail, smartphones, SNS, etc. However, it is being used in malicious attacks to send a large amount of illegal spam or to use it for fraud by using illegally collected personal information and devices that are vulnerable to security. Illegal spam, smishing, and fraudulent mail(SCAM) cause a lot of direct and indirect damage to companies and users, including not only social costs such as mental fatigue, but also unnecessary consumption of IT infrastructure resources and economic losses. Although there are regulations related to spam, violators of the law are still on the rise by circumventing the law, and victims are constantly occurring, so it is necessary to review what the problem is. This study examined domestic and foreign spam-related regulations and spam-related response activities, identified problems, and suggested improvement countermeasures. Through this study, it was intended to suggest directions for improving spam-related systems in order to block illegal spam and prevent fraudulent damage.

Key Words : SPAM, Text Spam, Voice Spam, E-mail Spam, Smishing

*Corresponding Author : Hyo-Chang Lim(hrm@swu.ac.kr)
Received November 11, 2021 Revised December 16, 2021
Accepted December 20, 2021 Published December 31, 2021

1. 서론

정보통신 기술의 발전은 사람들로 하여금 다양한 방법으로 의사소통을 가능하게 하고 편리함을 제공하지만 역기능으로 인한 피해도 점차 늘어나고 있다. 정보화의 역기능으로 인한 부작용이 얼마나 심각하게 인식되고 있는지를 조사한 결과, 스팸메일, 개인정보유출, 해킹바이러스, 사생활침해, 명예훼손 순으로 나타났다. 또한, 소비자의 82%는 스팸메일을 유해한 것으로 인식하고 있고 전화스팸에 대해서는 79.1%가 해롭다고 생각하고 있는 것으로 나타났다[1].

스팸 발생 유형별로 살펴보면 도박, 불법대출, 금융, 성인 등과 관련된 스팸이 대부분을 차지하고 있어 차단되지 않고 노출될 경우 2차 피해로 이어질 가능성이 높아 효과적인 대책 마련이 필요하다. 한국인터넷진흥원에 의하면, 2020년 하반기에 발생한 음성 스팸의 84.3%는 불법대출 관련 전화이고, 문자 스팸의 35.1%는 도박 관련 내용으로 문자 스팸의 5.6%는 정보유출이나 금융사기 등의 피해를 줄 수 있는 스미싱 공격인 것으로 나타났다. 금융감독원에 따르면, 2020년 보이스피싱으로 인한 피해 금액이 2,353억 원인 것으로 나타났다[2,3].

관련 법제도를 정비하고 시스템 구축 및 전담 조직을 구성하여 대응하고 있지만 매년 문자 스팸과 음성 스팸은 증가 추세에 있고, 정부나 공신력 있는 기관, 가족·지인 등을 사칭한 교묘한 방법으로 이용자들을 현혹하여 금전적인 피해도 급증하고 있다. 불법스팸에 신속히 대응하고 2차 피해를 최소화하기 위해서는 여러 경로로 수집되고 있는 스팸 정보공유와 관련 조직 간의 유기적인 협업이 필요하다.

기존 연구에서는 법제도 측면이나 기술적 측면에서 개선방안을 제시하는 사례는 많이 있으나 현재 스팸 대응에 대한 전반적인 문제 제기와 연구는 많지 않다.

본 연구는 스팸의 정보화 역기능이 심각하여, 기업과 개인에게 커다란 물질적·정신적·시간적 피해를 주는 문제점을 해결하기 위해 정책적 대안을 마련하는 것을 목적으로 이루어졌다. 국내외 스팸 관련 법제도와 기술, 조직 및 시스템, 국제협력 등의 대응 현황 전반에 대해 살펴보고 개선방안을 제시하고자 한다.

2. 이론적 배경

2.1 스팸 정의

스팸이란 정보통신망을 통해 수신자의 명시적인 사전 동의 없이 일방적으로 전송되는 영리목적의 광고성 정보를 말한다. 불법스팸은 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 “정보통신망법”이라 한다) 제50조부터 제50조의8의 규정을 위반하여 전송 또는 게시되는 영리목적의 광고성 정보를 말한다. 정보통신망법 제 50조 1항에서는 ‘누구든지 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려면 그 수신자의 명시적인 사전 동의를 받아야 한다’고 규정하고 있다. 영리 사업을 영위하는 사업자뿐만 아니라 개인, 공공기관, 단체, 비영리법인이라도 영리 목적으로 광고성 정보를 전송하는 경우에는 적용 대상이 되며, 전화, 팩스, 이메일뿐만 아니라 앱, SNS, 블로그, 카페 등의 메시징 기능, IP주소 등의 디지털 식별자도 전자적 전송매체에 해당한다. 명시적인 사전 동의는 광고성 정보의 수신동의 시 추후 광고를 수신할 수 있다는 점과 광고성 정보의 내용을 인지할 수 있도록 이용자에게 분명하게 알린 후에 동의를 받아야 한다는 의미이다[4,5].

미국은 스팸메일을 원하지 않는 또는 수신을 요청하지 않은 상업적 전자메일(Unwanted/Unsolicited Commercial Electronic Mail)로 정의하고 있고, EU에서는 원하지 않는 통신으로 정의하고 있다. 스팸의 규제 방식으로는 수신자의 사전 동의 없이는 광고를 전송할 수 없는 옵트인(Opt-in) 방식과 광고성 정보를 전송하는 것을 허용하되 수신자가 수신거부를 하면 더 이상 보낼 수 없도록 하는 옵트아웃(Opt-out) 방식이 있다[6].

2.2 국내 스팸 발생 현황

2020년 국내 전체 스팸 발송량은 7,722만 건으로 2018년 11,627만 건 대비 전체적으로는 감소하였으나 음성과 문자를 통한 발송량은 매년 지속적으로 증가 추세에 있다. 이메일을 통한 스팸은 약 48.4% 줄어든 반면, 문자 스팸은 약 5.3%, 음성 스팸은 약 17.8% 각각 증가하였다.

스팸의 발송경로와 광고유형별로 살펴보면, 음성 스팸의 경우, 유선전화를 통한 스팸 발송이 46.2%로 가장 많고 다음으로 인터넷전화, 휴대전화 순으로 발생하였으며, 광고 유형으로는 불법대출이 84.3%로 가장 많고

통신가입, 성인, 도박 순인 것으로 나타났다. 문자 스팸의 경우, 이동통신사의 무선통신망을 이용하여 대량 문자 발송서비스를 통한 스팸 발송이 87.7%로 가장 많고 휴대전화, 유선·인터넷전화 순으로 발생하였으며, 광고 유형으로는 도박, 금융, 불법대출, 성인 순으로 차지하고 있는 것으로 나타났다.

국외에서 발송된 이메일 스팸은 2020년 4,487만건으로 전체 이메일 스팸의 약 99%를 차지하고 있으며, 국가별로는 중국, 미국, 러시아 순이며 상위 5개국이 전체의 78.4%를 차지하고 있다. 또한 발송경로 확인이 안 되는 국외에서 발송된 문자 스팸은 2020년 278만건으로 2019년 약 60만건에 비해 4배 이상 증가하였으며 전체 문자 스팸의 18.1%를 차지하고 있다. 국외에 20여개의 문자 발송 사이트가 있는 것으로 추정하고 있으며 이중에 180만건은 국내 대량문자 발송서비스 업체를 경유하여 국내에 유입된 것으로 확인되었다[2].

문자 스팸 중에 악성 앱 설치를 유도하여 정보유출, 금품갈취 등의 피해를 줄 수 있는 스미싱 문자는 2018년 24만 여건으로 전체의 약 2%를 차지하였으며 2020년에는 약 5.6%인 것으로 나타났다.

방송통신위원회에서 불법스팸으로 확인되어 검찰이송 및 행정처분으로 처리한 건수는 2020년 993건으로 2017년부터 매년 천여 건의 불법스팸을 적발하여 조치를 하고 있다[7].

2.3 주요 피해 현황 및 사례

최근 확산되고 있는 보이스피싱 및 스미싱의 유형은 정부를 사칭하고 금융 기관의 상호를 그대로 사용하여 정부 및 공신력 있는 기관에서 발송한 문자메시지인 것처럼 오인하도록 유도하고 있다. 2020년 보이스피싱의 피해금액은 2,353억 원으로 전년대비 65% 감소한 반면, 가족·지인 등을 사칭한 메신저피싱에 의한 피해금액은 9.1% 증가하였고 2021년 상반기에만 466억 원으로 이미 작년 피해액을 초과할 만큼 급격히 증가하고 있다. 반면 기관사칭형이나 대출빙자형은 감소 추세에 있다. 피해 연령별로는 대출빙자형에서는 40·50대의 비중이 65%로 가장 높았으며, 사칭형은 60대 이상의 비중이 48.3%로 가장 높은 것으로 나타났다[3].

WSJ의 피해사례는 인공지능을 이용한 사기(scam)가 기업의 새로운 도전임을 말해주고 있다. 2019년 유럽의 에너지 기업의 영국 지사장은 독일에 있는 모기업 대표의 전화를 받고 헝가리 거래처로 22만 유로를 송금한 후에 범죄자들이 인공지능 기반 소프트웨어를 사용하여 CEO의 목소리를 가장하고 사기성 송금을 요구한 사실을 알게 되었다. 국내에서도 보이스피싱이 기승을 부리고 있는 가운데 어눌한 조선족 말투를 쓰거나 금융·수사 기관을 사칭하는 전화에도 많은 피해가 발생하였는데 가족이나 친구처럼 가까운 지인의 목소리를 복제하여 흉내 낼 경우 피해 가능성이 더 커질 우려가 있다[8,9].

한편, 이메일을 통해서 대량의 광고 메시지를 전달하는 스팸 공격에서 최근 거래처를 사칭하여 금전이나 민감한 정보를 탈취하는 BEC(Business Email Compromise) 공격으로 진화하고 있다.

FBI의 발표에 따르면, 미국에서 발생한 BEC 공격에 의한 피해액은 2019년 약 18억 달러로 2017년 6억 달러에 비해 그 피해 규모가 약 3배 가까이 급격히 증가하고 있다. BEC 공격으로 피해를 본 기업만 구글과 페이스북 등을 포함하여 23,000개에 이르며 매년 신고 접수 건수도 증가하고 있다. 국내에서도 BEC 공격으로 2014년 LG화학 240억, 2018년 한국에너지기술연구소 1억, 2020년 미래에셋 홍콩법인이 60억의 피해를 본 것으로 나타났다[10].

3. 국내외 스팸 대응 현황

3.1 외국의 스팸 대응 정책

미국, EU 등 해외 주요국에서는 1990년도 초부터 관련 법제도의 제·개정을 통하여 스팸규제를 하고 있고 강화하는 추세에 있다. 명시적인 사전 동의 제도 도입과 수신동의 철회, 수신거부 시 전송금지, 발신번호 조작금지 등의 제도를 적용하고 있다. 관련 조직에서는 스팸 신고 접수를 위한 웹사이트 운영과 수신거부리스트를 운영관리하고 불법스팸 발송자에 대한 적발 활동을 통해 피해를 최소화하는 한편, 통신사업자와 협업을 통하여 불법스팸을 사전에 차단하는 등의 노력을 기울이고 있다.

미국은 1991년부터 전화소비자 보호법(Telephone Consumer Protection Act, TCPA)에서 수신자의 사전 동의 없이 자동발신시스템 등을 이용하여 유·무선 전화로 텔레마케팅을 하거나 팩스를 이용한 광고성 정보를 전송하는 행위를 제한하고 있다. 이메일에 대해서는 2004년부터 스팸방지법(The Controlling the Assault of Non-Solicited Pornography and Marketing Act,

CAN-SPAM Act 2003) 제정을 통해 광고 표기 및 수신거부방법을 제공하도록 의무화하고, 수신자가 사후적으로 수신거부 의사를 전달하면 이후의 재전송 행위를 금지하고 있다. 휴대전화에 대해서는 옵트인(Opt-in) 방식을 채택해 사전에 동의를 받지 않은 수신자에게 광고 메시지를 송신하지 못하도록 하고 있다. 발신자표시법(Truth in Caller ID Act, TICIDA)에서는 통화 시 발신자 번호를 표시하도록 하여 소비자들이 원하지 않는 스팸전화를 피할 수 있도록 하고, 사기 또는 부당이득을 취하기 위해 발신자 ID 정보를 부정확하게 전송하는 행위를 금지하고 있다. 텔레마케터 또는 텔레마케팅 위탁 판매자에 대해서는 수신거부 이행법(Do-Not-Call Implementation Act)에서 수신거부리스트에 등록된 사람에게 전화를 걸지 못하도록 제한하고, 1개월마다 수신거부리스트를 확인하여 등재된 번호를 자신의 텔레마케팅 리스트에서 삭제하도록 하고 있다[5,12].

음성스팸, 특히 로보콜(Robocall)을 강력히 규제하기 위해 기존의 전화소비자 보호법(TCPA) 등의 내용을 보완, 강화하는 것을 골자로 로보콜 남용 범죄 단속 및 규제에 관한 법률(Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, TRACED Act)을 2019년 12월부터 시행하고 있다. 유·무선 전화로 고의적으로 부정확한 발신자 정보를 제공하거나 전화소비자 보호법(TCPA)을 위반하여 로보콜을 발신하는 경우 연방통신위원회(Federal Communications Commission, FCC)에서 1만 달러 벌금을 부과할 수 있도록 강화하고, 발신자 인증이 되지 않거나 부정 의심이 되는 전화인 경우 통신사업자가 사전 동의를 얻어서 수신자에게 수신되기 전에 차단할 수 있도록 하고, 가입자가 원하지 않는 통화나 문자를 수신하지 않도록 보호하고 있다. 그리고 정책효과를 평가할 수 있는 법무부 주도하에 FCC, 연방거래위원회(Federal Trade Commission, FTC), 상무부, 국무부, 국토안보부, 소비자 금융 보호국 등 관련 기관이 참여하는 워킹그룹을 운영하도록 하고 있다[13].

EU는 1997년 유럽 원격판매 지침에서 전화와 팩스를 이용한 광고성 정보 전송 시 소비자의 동의를 얻도록 요구하였고, 2002년 이메일에 대해서도 전자통신부문의 개인정보처리와 프라이버시 보호에 관한 지침(The Directive on Privacy and Electronic Communications, Directive 2002/58/EC)에서 스팸에 대해 옵트인(Opt-in) 관련 사항을 규정하고 EU 회원국이 자국 입법 시 반영하도록 하고 있다. 다이렉트마케팅(DM) 목적으로 수신자의 사전 동의 없이 ARS 자동전화, FAX, 이메일 등 전자적 전송매체를 이용하는 행위를 금지하고 수신동의를 철회할 수 있는 방법을 명시하도록 의무화하고 있다. 스팸 처리의 실무는 EU 회원국별로 이 지침을 활용한 자국의 법규에 의거하여 담당 기관이 수행하고 있다[13].

ITU-T에서는 스팸을 차단하기 위한 기술표준을 개발하고 있다. 다양한 종류의 스팸을 효과적으로 차단하기 위한 스팸 차단 기술 전략과 스팸 유형별 이메일 스팸 차단 기술, IP 멀티미디어 스팸 차단 기술, 메시징 스팸 차단 기술 표준화를 각각 진행하고 있다. 또한 다양한 종류의 스팸이 네트워크를 통해 전달되는 것을 차단하기 위한 발신자와 수신자간의 상호작용 게이트웨이 시스템에 대해 정의하고 있다. 그리고 효과적인 규제, 기술, 서비스 이용자 및 사업자에 대한 교육 등 스팸 차단을 위한 활동들도 함께 다루고 있다[14].

3.2 국내 스팸 대응 정책

3.2.1 법·제도 관점의 정책

국내에서는 1999년 정보통신망법 개정으로 전자적 전송매체를 이용한 광고성 정보 전송을 규제하기 시작하였으며, 2004년 전화스팸에 대한 옵트인(Opt-in) 제도 도입과 2005년 불법스팸에 대한 처벌 규정 신설, 2014년 이메일을 포함한 모든 광고성 정보에 대한 옵트인(Opt-in) 적용 등 불법스팸방지를 위한 법·제도 개선과 스팸 대응을 위한 사업자 협조 강화, 국외 스팸방지를 위한 국제협력 노력, 대국민 스팸 인식 제고 등의 정책을 추진하고 있다[5,15].

스팸과 관련해서 정보통신망법 이외 전자상거래 등에서의 소비자보호에 관한 법률, 방문판매 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률, 전자문서 및 전자거래 기본법, 전기통신사업법 등에서 적용 범위와 기준, 절차, 위반 시 벌칙 등에 대해 각각 규정하고 있다.

정보통신망법에서는 제50조부터 제50조의8, 제64조, 제74조, 제76조에서 스팸의 개념, 적용범위, 전송 및 게시 제한, 광고성 프로그램 설치, 전송차단 소프트웨어 보급, 전송금지, 자료의 열람이나 제출 요청, 벌칙 등 스팸에 대한 전반적인 내용을 다루고 있다.

Table 1. Main regulations of spam-related laws

Laws	Prior Consent	Withd- rawal Of Consent	Refusal To Receive Infor-mation	Perusal or Sub-mission of Materials
Information and Communications Network Act(ICNA)	○	○	○	○
Act On The Consumer Protection In Electronic Commerce, Etc.	Compliance with ICNA			△
Act On Door-To- Door Sales, Etc.	Exception when notifying the source of collection by phone		○	×
Credit Information Use And Protection Act	Application mutatis mutandis of article 50 of ICNA	○	○	○
Framework Act On Electronic Documents And Transactions	Prohibition of sending advertisements			○
Telecomm-unications Business Act	Prohibition against false display of caller ID			○

주요 내용을 살펴보면, 영리목적의 광고성 정보를 전송하려면 그 수신자의 명시적인 사전 동의를 받아야 하며, 수신자가 수신거부의사를 표시하거나 사전 동의를 철회한 경우에는 영리목적의 광고성 정보를 전송할 수 없다. 이용자가 광고성 정보의 수신을 원하지 아니하는 경우 정보통신서비스 제공자는 차단 조치를 할 수 있으며, 불법행위를 위한 광고성 정보 전송을 금지하고 있다. 정보통신서비스 제공자에게 법을 위반하여 영리목적 광고성 정보를 전송한 자에 대한 자료의 열람이나 제출을 요청할 수 있고, 법 위반 사실과 관련한 관계인의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사할 수 있다.

전기통신사업법은 제84조의2에서 누구든지 영리를 목적으로 송신인의 전화번호를 변작하는 등 거짓으로 표시할 수 있는 서비스를 제공하지 못하도록 규정하고 있다. 거짓 전화 발신을 차단하거나 정상적인 전화번호로 정정 조치하여야 하며, 국외에서 발신된 전화에 대한 국외발신 안내 등의 조치를 하여야 한다. 또한 조치의 이행 여부를 확인하거나 이용자의 피해가 확산되는 것을 방지하기 위하여 전기통신사업자에게 자료의 열람·제출을 요청하거나 필요한 검사를 할 수 있도록 하고 있다.

3.2.2 기술 관점의 정책

불법스팸을 효율적으로 차단하고 관리하기 위해 관련 기관과 서비스 제공업체에서는 스팸 수집, 신고·접수, 차단, 조치 등을 위한 대응체계를 구축하여 운영하고 있다.

방송통신위원회는 한국인터넷진흥원(KISA) 불법스팸대응센터를 통해서 불법스팸 수집, 스팸 신고·접수 및 스팸차단리스트 관리를 하고, 스팸차단리스트 공유를 통해 스팸을 차단할 수 있도록 지원하고 있다. 또한 방송통신위원회 내 방송통신사무소(서울, 부산, 광주, 대전)에서는 불법스팸대응센터와 수집 및 신고·접수된 스팸 정보에 대한 조사를 통해 밝혀진 불법스팸에 대한 수사 및 행정처분 조치를 수행하고 있다.

KISA 불법스팸대응센터에서는 이를 위해 음성스팸 실시간차단시스템, 휴대전화 스팸트랩시스템, 이메일 스팸트랩시스템, 인터넷 게시글 실시간 차단서비스, KISA-RBL, BLOCK 25 등의 시스템 운영과 서비스를 제공하고 있다[16].

금융위원회는 이용자가 효과적으로 금융기관에 대해 스팸 수신거부를 할 수 있도록 연락중지청구시스템(두낫콜; Do-not-call)을 운영하고 있으며, 보이스피싱에 의한 2차 피해방지를 위해 금융보안원을 통해 범금융권 보이스피싱 사기정보 공유시스템을 운영하고 있다.

공정거래위원회에서는 방문판매법에 의거하여 전화권유판매 수신거부의사 등록시스템을 운영하고 있다. 소비자는 본인의 휴대전화번호 등록을 통하여 수신거부의사를 표명하게 되고, 전화권유판매 사업자는 전화권유판매 전에 수신거부대조를 통하여 영업대상목록에서 제외하도록 하고 있다.

과학기술정보통신부에서는 전기통신금융사기에 의한 피해 방지를 위해 산하 중앙전파관리소를 통해 불법 사용번호 정지 시스템(Unlawful Numbering Management System, UNMS)을 운영하고 있고, 한국인터넷진흥원을 통해서는 발신번호 거짓표시 신고 시스템과 음성전화 차단관리시스템, 문자발송 차단관리시스템을 각각 운영하고 있다.

불법 사용번호 정지 시스템은 경찰청, 검찰청, 금감원으로부터 전기통신금융사기 범죄에 이용된 전화번호 이용중지 요청을 받으면 전기통신사업자가 이용중지 조치할 수 있도록 운영되고 있다.

한국인터넷진흥원에서는 발신번호 변작 의심 신고를 위한 발신번호 거짓표시 신고 시스템을 운영하고 있다. 전기통신금융사기 범죄에 이용된 전화번호는 거짓일 가능성이 높으므로 불법 사용번호 정지 시스템으로 이용중지

요청하기 전에 먼저 거짓인지 여부를 확인할 필요가 있다. 또한, 공공·금융기관의 전화번호를 사칭한 보이스피싱을 사전에 차단하는 음성전화 차단 관리 서비스와 공공·금융기관, 기업 및 개인이 등록한 전화번호를 문자중계사업자에게 제공함으로써, 해당 전화번호를 사칭한 인터넷발송 문자메시지를 차단하는 문자 발송 차단 관리 서비스를 운영하고 있다.

이동통신 사업자에서는 지능형 스팸차단서비스, 음성스팸 실시간차단시스템, 스팸전화 차단 앱, 스팸문자 필터링 서비스, 이미지 스팸 차단 서비스, 간편 신고 서비스, 번호도용 문자차단 서비스 등으로 음성 스팸과 문자 스팸을 차단할 수 있도록 서비스를 제공하고 있다. 이동통신사의 평균 문자스팸 차단 율은 2018년 88.1%에서 2020년 93.5%, 2021년 상반기 95.8%로 향상되고 있다[2].

포털사이트에서는 이메일스팸 신고 서비스를 제공하고 있다. 원치 않는 메일이나 불법스팸 메일을 수신한 경우, 이용자가 스팸신고를 통해 메일을 차단할 수 있고, 이용자가 차단할 메일주소, 도메인으로 수신차단 목록을 등록하거나 대출, 광고 등 특정 키워드를 등록하여 차단할 수도 있다.

Table 2. Spam response systems and services

Provider	Systems and Services
Korea Communications Commission	Voice Spam Real-Time Blocking System
	Cell Phone Spam Trap System
	Email Spam Trap System
	Internet Posting Real-Time Blocking Service (Open API provided)
	KISA-RBL
	BLOCK 25
Financial Services Commission	Contact Suspension Request System (Do-Not-Call)
Financial Security Institute	Pan-Financial Voice Phishing Fraud Information Sharing System
Korea Fair Trade Commission	Telephone Solicitation Sales Refusal Registration System
Ministry of Science and ICT	Unlawful Numbering Management System
	False Caller ID Reporting System
	Voice Call Blocking Management System
	Text Message Blocking Management System
Mobile Telecommunication Service Provider	Intelligent Anti-Spam Service
	Voice Spam Real-Time Blocking System
	Voice Spam Blocking App
	Text Spam Filtering Service
	Image Spam Blocking Service
	Simple Spam Reporting Service
	Stolen Caller ID Text Blocking Service
Portal Service Provider	Email Spam Reporting Service
Mobile Messenger App Provider	Mobile Messenger App Spam Reporting Service
Anti-Spam App Provider	Voice Spam Blocking App
Email Anti- Spam Provider	Email Spam Blocking System

또한 사칭 메일, 외국어 메일, 받는 사람에 내 메일 주소가 없는 메일 등을 스팸으로 미리 설정하여 스팸 메일로 분류 및 차단할 수도 있다. 또한, 메일서버 등록제(Sender Policy Framework, SPF)를 시행하여 발송자 정보를 위변조하는 불법 스팸메일과 피싱메일 등을 사전에 차단하고 있다.

모바일 메신저앱 사업자는 자사의 모바일 신고 서비스를 통해 이용자가 신고할 메시지를 선택하여 스팸 신고 및 차단을 할 수 있도록 기능을 제공하고 있다. 모르는 사람으로부터 스팸 메시지를 수신한 경우 대화 화면에서 해당 메시지를 발송한 사용자를 차단하거나 스팸신고 기능을 이용하여 메시지 차단이 가능하다[17].

스팸전화 차단 앱은 KISA 불법스팸대응센터의 음성스팸차단리스트 연동 등을 통해 스팸전화번호 DB를 지원하여 전화 수신 시 발신번호가 스팸인지 정보를 제공하고, 차단여부와 메모 기능을 제공한다. 수집된 스팸전화번호 정보는 공유되도록 공유기능을 제공하고 있다.

대부분의 기관과 기업에서는 이메일스팸방지 사업자가 제공하는 이메일스팸 차단 시스템을 도입하여 운영 중에 있다. 자체 보안 정책과 KISA-RBL의 실시간 스팸차단리스트 등의 정보를 이용하여 수신되는 모든 이메일의 발송IP 등을 확인하여 스팸여부를 판단하고 즉각 차단하고 있다.

3.2.3 조직 및 시스템 관점의 정책

방송통신위원회에서는 불법스팸 차단 시스템 고도화와 불법스팸 전송자에 대한 제재 강화를 통해 2017년에서 2020년까지 3,927건의 불법스팸을 적발하였다. 연간 1억 2,000만 건(2018년 기준)의 스팸 빅데이터를 구축하여 도박사이트, 불법대출번호, 스팸관여 주식종목 등의 불법스팸 신고데이터를 마사회, 금감원, 한국거래소 등 관련 기관에 제공하여 도박, 주식, 불법대출 사기 등으로 인한 국민의 피해를 예방하였다. 또한 불법스팸 차단을 위한 AI기반 스팸 빅데이터 분석시스템 구축과 도박, 대출 사기 등의 2차 피해를 최소화하기 위해 스팸데이터 개방을 추진하고 있다. 한편 개인정보보호위원회와 합동으로 한국인터넷진흥원의 스팸 신고정보와 SK텔레콤의 고객정보를 결합하여 빅데이터 분석한 결과('20년 1년간 SKT 이용자 신고 1,377만건), 스팸 유형에서 남성은 여성에 비해 도박, 주식정보 스팸, 여성은 남성에 비해 불법대출, 대출카드 스팸 비율이 상대적으로 높았으며, 연령

대별로는 남녀 모두 50대 비중이 가장 높은 것으로 나타났다. 특히 주식정보 스팸의 경우 40대 남성, 의약품 스팸의 경우 60대 남성의 비중이 가장 높게 나왔다. 분석결과는 향후 맞춤형 스팸예방 교육과 인식제고에 활용할 계획으로 있다[18,19].

공정거래위원회 산하 한국소비자원에 등록된 전화권유판매 수신거부의사 소비자는 2015년 기준으로 132,295명으로 2014년 시스템 개통이후 완만한 증가 추세로 큰 변화가 없는 상태이다. 수신거부의사를 등록한 소비자에 대한 전화권유판매 등 법위반 신고 202건(2015년 9월 기준 누적건수) 중에 16건(7.9%)만 처리되었고, 미처리된 186건의 대부분(99.4%)은 사업자의 신원이 불분명한 미등록업체인 것으로 나타났다[20].

과학기술정보통신부에서는 알뜰폰 이용자 보호를 위한 가이드라인 준수여부를 점검하기 위해서 음성전화를 제공하는 주요 15개 사업자에 대한 현장 점검에서 허위과장 광고 금지, 불법 텔레마케팅 금지, 명의도용 및 부당영업 금지 등 29개 항목에 대해 알뜰폰 이용자 보호 실태 점검 결과를 실시하였다. 대부분의 사업자가 자체 업무지침을 마련하고 이용자 보호 전담기구 운영, 임직원 교육 등 가이드라인 준수 상태가 양호한 것으로 나타났다. 하지만 알뜰폰 가입자가 945만 명('21.4월 기준)으로 이동전화 시장의 13.2%를 차지하고 있으나 이용자 보호에 대한 만족도는 낮은 수준으로, 공인전자서명 제도 폐지에 따른 민간 전자서명을 통한 본인확인을 반영하는 등 가이드라인 개정을 통하여 이용자들이 안심하고 사용할 수 있도록 이용자 보호에 보다 신경을 써야 할 것으로 보인다[21].

3.2.4 국제협력 관점의 정책

최근 들어 이메일스팸 중에 국외에서 발송되는 스팸의 비중이 크게 증가하고 있어 이에 대한 관련 국가와의 적극적인 협력 활동이 요구되고 있다. 해외에서 발송되는 이메일 스팸 비중이 2017년 75.2%에서 2020년 98.9%로 매년 급증하고 있고 2021년 상반기 해외 유입 문자스팸은 전체의 약 13%를 차지하고 있다. 방송통신위원회는 국가 간의 불법스팸 방지 및 공조체계를 강화하기 위해 2016년 국제 스팸대응협의체인 UCENet(Unsolicited Communications Enforcement Network)과 M3AAWG(Messaging, Malware, Mobile Abuse Working Group)에 회원국으로 가입하여 국가 간의 불법스팸 전송자에 대한 조치와 다양한 이슈들에 적극 대응하고 있다. UCENet는 미국, 영국, 캐나다 등 31개국의 공공기관이 참여하고 있는 공공영역 스팸대응협의체로 우리나라는 이 중에 8개국과 MOU를 체결하고 정보 공유를 추진하고 있다. M3AAWG는 페이스북, 구글, 통신사 등 글로벌 기업이 주도하여 운영하는 민간과 공공이 함께 참여하는 스팸대응협의체이다. 2018년에는 우리나라, 호주, 일본, 뉴질랜드, 대만 등 5개국이 참여하는 아시아 스팸대응협의체(UCENet Asia-Pacific)를 발족하여 아시아 국가 간 원스톱 연락체계를 구성하여 아시아 지역 내 대량으로 유통되는 불법스팸과 각종 사이버 사기에 대응하고 있으며 중국과 아세안 10개국으로 대상국을 점차 확대해 나갈 예정이다.

4. 정책 제안

4.1 현행 정책의 문제점

국내 스팸 및 보이스피싱 대응은 방송통신위원회, 금융위원회, 공정거래위원회, 과학기술정보통신부에서 관련 법령에 따라 각각 대응하고 있다. 스팸 신고는 방송통신위원회의 위임을 받아 KISA 불법스팸대응센터에서 접수하여 관리하며, 수신거부의사 표시는 금융위원회와 공정거래위원회에서 각각 접수하여 관리하고 있다. 번호도용 문자차단 요청은 과학기술정보통신부의 위임을 받아 한국인터넷진흥원에서 관리하고 있다. 이용자 입장에서는 스팸신고, 수신거부, 번호도용차단 신청 등 사안에 따라 해당 부처에서 운영하고 있는 시스템에 별도로 접속하여 각각 신고해야 하므로 접근하기에 불편함이 있고 활용도도 낮은 것으로 나타났다.

2019년도 금융 관련 음성, 문자스팸 건수 대비 연락중지청구시스템(두낫콜)의 등록 건수 비율은 26.7%로 금융위원회에서 운영하고 있는 연락중지청구서비스에 대한 활용도는 매우 낮은 것으로 나타났다. 전화권유판매 수신거부의사 등록시스템에 등록된 건수는 2015년 9월 기준으로 132,295명으로 전화권유판매업자는 전화권유판매 시 수신거부의사 등록 전화번호를 대조하여 확인하게 되어 있으나 영업 중인 사업자의 20%만이 대조 수행한 이력이 있는 것으로 나타났다[20,22].

관련 부처별로 보유하고 있는 스팸 및 보이스피싱 관련 정보를 살펴보면 방송통신위원회에서는 스팸 정보, 금융위원회에서는 보이스피싱 정보, 과학기술정보통신부에서는 전기통신금융사기 정보를 각각 관리하고 있다. 하

지만 부처 간에 보유하고 있는 정보가 제대로 공유되지 않아 피해가 발생하고 있다. KISA 불법스팸대응센터에 신고·접수된 불법대출광고와 허위결제 문자 메시지 정보가 경찰청과 금감원에 전달되어 차단되지 않아 불법대출광고 전화번호 203개와 허위결제 문자 메시지 전송에 사용된 전화번호 82개가 신고 이후에 전기통신금융사기에 이용되어 불법대출광고 피해자 282명에게 28억여 원, 허위결제 피해자 109명에게 31억여 원의 피해가 발생하였다[23].

공공·금융기관을 사칭한 보이스피싱이나 인터넷발송 문자메시지를 차단하기 위해 음성전화 차단관리 시스템과 문자발송 차단관리 시스템에서 공공·금융기관의 전화번호를 등록하여 관리하고 있으나 수작업으로 처리하고 있어 전화번호가 누락되거나 부정확한 상태로 관리 중에 있다. 5개 은행에 대해 확인한 결과, 대표전화번호의 68.5%, 일반전화번호의 77.1%가 등록되지 않은 것으로 나타났으며 등록되지 않은 3개 은행의 5개 대표전화번호가 변작·이용되어 5천만 원의 피해가 발생하였다[23].

공정거래위원회 및 산하 한국소비자원의 경우 전자상거래법 및 방문판매법에 의거하여 불법스팸에 대해 대응하고 있으나 방문판매법 위반자의 경우 신원 확인이 안 되어서 대응 조치가 미흡하다. 전자상거래법에는 공정거래위원회에서 위반자 확인을 위해 방송통신위원회에 자료요청 할 수 있도록 되어 있으나, 방문판매법은 법위반 사업자를 확인하기 위해 정보통신사업자에 대한 자료 열람·제출 권한을 규정하고 있지 않아, 발신번호를 변작한 불법 전화권유판매에 대해 실질적인 대응조치가 이루어지지 못하고 있는 실정이다[20].

미국의 경우 로보콜(Robocall)을 강력히 규제하고 있다. 발신자 인증이 되지 않거나 부정 의심 전화의 경우 통신사업자가 사전 동의를 얻어서 수신자에게 수신되기 전에 차단할 수 있도록 하고 있다. 12개 통신사업자와 50개 주 정부가 협약을 체결하고 부가 서비스로 로보콜에 대해 사전 차단 서비스를 제공하고 있다. 방송통신위원회에서는 매년 상하반기에 스팸 현황을 발표하고 있으나 로보콜에 대해서는 아직 정확한 현황 파악이 되어 있지 않다. 국내도 음성스팸의 상당수는 로보콜에 의한 대량 발신으로 추정하고 있다[12].

국외에서 발송된 이메일 스팸은 전체 이메일 스팸의 약 99%를 차지하고 있고, 중국 등 상위 5개국이 전체의 78.4%를 차지하고 있다. 또한 발송경로 확인이 안 되는 국외에서 발송된 문자 스팸은 전체 문자 스팸의 18.1%를 차지하고 있으며 급격한 증가 추세에 있다. 국외에 20여개의 문자 발송 사이트가 있는 것으로 추정하고 있으며 이중에 일부는 국내 대량문자 발송서비스 업체를 경유하여 국내에 유입된 것으로 확인되었다. 방송통신위원회에서 발표하는 스팸 현황에는 국외 발송 문자 스팸은 포함되어 있지 않고 또한, 국제 문자 발송 사이트에 대한 확인이 어려워서 실제로 조치까지는 이루어지지 않고 있는 문제가 있다.

4.2 불법스팸 방지 개선방안

본 연구에서는 국내외 관련 법제도와 기술, 대응 조직, 국제협력 등의 현황 분석을 통해서 불법스팸을 방지하고 2차 피해를 예방하기 위해 다음과 같은 개선방안을 제시한다.

첫째, 스팸 관련 시스템의 활용도를 개선하기 위한 창구 일원화가 필요하다. 스팸 관련 신고접수 창구를 일원화하여 이용자의 접근이 편리하게 하고 각 부처별로 개별 관리하고 있는 스팸 관련 정보들을 통합 관리하여 정보의 활용도를 높일 수 있도록 개선이 필요하다. 범죄이용 전화번호, 보이스피싱 정보 및 불법스팸 정보는 서로 관련성이 매우 높은 정보로 방송통신위원회, 금융위원회, 과학기술정보통신부 등 관련 부처 간의 정보공유를 통해 추가 피해가 발생하지 않도록 신속히 대처하는 것이 필요하다.

둘째, 공공·금융기관 전화번호의 변작차단 목록의 자동화 및 현행화가 필요하다. 음성전화 차단관리 시스템과 문자발송 차단관리 시스템에서 수작업으로 등록 관리하고 있어 전화번호 누락 및 부정확한 상태로 관리 중이나 자동화하여 주기적으로 업데이트하여 최신 정보로 관리할 수 있도록 개선이 필요하다.

셋째, 방문판매법 위반자의 신원을 확인할 수 있도록 제도적인 보완이 필요하다. 방문판매법에서는 방문판매업자 또는 전화권유판매업자에 대해 신고를 하도록 되어 있고, 변경사항이 있을 경우에 관련 서류를 제출받아서 신고증을 발급하도록 되어 있으나 전화권유판매법 위반 신고 건 중에 미처리된 건의 대부분은 미 등록 업체인 것으로 나타나 조치를 하지 못하고 있다. 방문판매법에 공정거래위원회에서 위반자 확인이 불가한 경우에 방송통신위원회에 요청하여 위반자 신원을 확인할 수 있도록 자료 열람요청 조항 반영 등의 제도적

인 보완이 필요하다.

넷째, 국내 로보콜에 대한 현황 파악과 대책 마련이 필요하다. 미국과 마찬가지로 국내에서도 로보콜에 의한 스팸이 많이 발생하고 있는 것으로 추정되고 있다. 정보통신망법 제50조의4에는 정보통신사업자로 하여금 서비스를 차단할 수 있는 근거가 마련되어 있고 KISA 불법스팸대응센터의 음성스팸실시간차단시스템에서 제공하는 음성스팸차단리스트에 대해서는 이동통신사업자가 사전차단 조치를 하고 있다. 또한 전기통신금융사기에 이용된 전화번호에 대해 경찰청, 검찰청, 금감원의 신고 시 발신번호 거짓 여부를 확인하여 정보통신사업자가 차단하고 있다. 로보콜에 대해서 발신자 인증이 되지 않거나 부정 의심 전화의 경우 통신사업자가 이용자의 사전 동의를 얻어서 전화가 수신되기 전에 차단할 수 있도록 제도 개선이 필요하다.

다섯째, 국외 스팸에 대한 현황 파악 및 대책 마련이 필요하다. 우리나라는 국제 스팸대응협의체인 UCENet과 M3AAWG, 그리고 아시아 스팸대응협의체(UCENet Asia-Pacific)의 회원국으로 가입되어 있어 매년 정기적인 행사를 통해 각 국의 스팸 대응 현황과 이슈에 대해 정보 교류를 하고 있다. 회원국들과 정보 공유 및 협력을 통해 스팸 현안에 대한 해결방안 마련이 필요하다. 각 국의 스팸 정책과 효과적인 대응 방안에 대한 정보 공유뿐만 아니라 실무 차원의 협업 활동을 통한 대응 조치가 될 수 있도록 상시적인 대응체계를 구축할 필요가 있다. 국외 유입 스팸에 대해 관련 국가와의 공조를 통한 보다 적극적인 대처가 요구된다.

여섯째, 관련 기관이 참여하는 스팸 대응협의체 구성이 필요하다. 스팸과 관련하여 여러 기관에서 대응하고 있으나 협업을 통한 대응이 필요하다. 방송통신위원회, 금융위원회, 공정거래위원회, 과학기술정보통신부, 금융감독원, 한국소비자원, 한국인터넷진흥원, 경찰청 등 관련 기관이 참여하는 스팸 대응협의체 구성을 통해 스팸 관련 현안 이슈들을 공유하고, 정기적인 합동 점검을 통해 문제점을 파악하여 제도를 개선해 나가는 것이 필요하다.

5. 결론

오늘날 사람들은 다양한 정보통신 수단을 활용하여 편리하게 의사소통을 하고 있다. 하지만 이를 악용하여 불법으로 취득한 개인정보를 이용하여 수신자의 동의 없이 불법으로 광고성 정보를 대량으로 전송하거나 스미싱이나 보이스피싱 등으로 정보유출이나 금융사기와 같은 2차 피해에 활용함으로써 사회적으로 물의를 일으키고 있다. 이러한 피해를 방지하기 위해 법제도를 정비하고 관련 시스템을 구축하여 단속 활동을 하고 있지만, 단속을 교묘히 피하거나 공권력이 미치지 못하는 국외에서 지속적으로 불법스팸을 발송하고 있다.

스팸 해결에는 단일 묘책이 없으며, 종합적이고 지속적인 대응책이 필요한 만큼 법적·자율적 규제, 기술적 조치, 이용자 인식제고, 국제협력 등 다각적인 방법으로 접근이 필요하고, 관련 민·관 및 국가 간의 공조체제를 구축하여 협력을 강화해 나가는 것이 요구된다[24].

본 연구에서는 스팸 관련 법제도와 기술적 조치 사항, 관련 기관과 사업자에서 대응하고 있는 현황, 국제협력 등에 대해 살펴보았으며, 이를 종합적으로 분석하였다. 분석결과를 바탕으로 개선이 필요한 부분에 대해 대책을 제시하였으며, 앞으로 스팸 개선 방안을 수립하는데 참고가 될 수 있을 것이다. 특히 스팸 관련 정부부처의 역할과 책임에 대한 정책 제안을 하였는데 향후 정부의 스팸정책 개선에 기여할 수 있을 것으로 기대한다. 현행 법제도 하에서 개선이 가능한 스팸 신고 창구의 일원화, 음성전화 차단관리 시스템과 문자발송 차단관리 시스템에서 전화번호의 변작차단 목록의 자동화 및 현행화, 로보콜의 차단 등은 실무적으로 검토하여 추진할 수 있을 것이다.

본 연구는 정책 제안 연구로서 스팸 관련 국내외 현황과 문제점을 제시하고 정책대안을 제시함에 있어서 과학적 연구방법론을 사용하지 않았다는 연구한계를 가지고 있다. 스팸 관련 변수간 인과관계를 검증하기 위한 모델 도출 및 실증연구가 이루어질 필요가 있다. 서베이 및 서베이 결과의 통계적 분석 결과를 가지고 개선이 필요한 부분에 대해 객관적 증명을 통해 대책을 제시하거나 서베이 및 서베이 결과의 통계적 분석 결과를 가지고 앞으로 객관적 증거라료를 이용해 개선 방안을 제시하는 실증연구가 이루어질 필요가 있다. 정책에 초점을 맞춘 후속 연구를 진행할 경우라고 하더라도 국내외 전문가에 대한 인터뷰를 통해서 보다 깊이있고 다양한 정책 제안이 가능할 것이다. 향후에는 스팸 정책의 효과성이나 스팸 피해의 원인 등에 대해 데이터 기반 과학적 연구방법론에 의한 연구가 이루어질 필요가 있다.

본 연구가 국내외 스팸의 현황과 정책대안에 초점을 맞춘 반면 기업이나 행정기관 등 개별 조직 차원에서 스

팸으로 인한 경영성과 및 경영효율성 측면을 고려하지 않았다는 연구한계를 가지고 있다. 개별 조직 단위를 연구 범위로 하는 사례연구 혹은 실증연구가 후속연구로 이어지기를 기대한다.

ACKNOWLEDGMENTS

This work was supported by a research grant from Seoul Women's University(2021).

REFERENCES

[1] K. H. Lee. (2008). A Study on the effective consumer policies against spam in Korea. *Journal of Consumer Policy Studies*, *33*, 93-121.

[2] KISA. (2021). *Spam distribution status in the second half of 2020*. Naju : Korea Internet & Security Agency.

[3] FSS. (2021). *Analysis of Voice Phishing Status in 2020*. Seoul : Financial Supervisory Service.

[4] KISA. (2020). *Information and Communications Network Act Guide for Prevention of Illegal Spam*. [Brochure]. Naju : Korea Internet & Security Agency.

[5] C. B. Lee. (2021. Feb). *2021 KISA REPORT, Review of KISA, 2*, 55-67.

[6] S. J. Kim. (2010). Analysis on Spam-related Regulations of EU·Germany. *Zeitschrift der Koreanisch-Deutschen Gesellschaft für Sozialwissenschaften*, 20(3), 137-158.

[7] KCC. (2021). *Cases of illegal spam investigation and administrative disposition*. Gwacheon : Korea Communications Commission.

[8] C. Stupp. (2019). *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*. The Wall Street Journal(Online). Retrieved from https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

[9] J. S. Kim. (2021). *It was the same as our boss... I called and sent money to the customer*. Yonhapnews(Online). Retrieved from https://www.yna.co.kr/view/AKR20210720055500797?input=feed_daum.

[10] D. K. Lee, G. S. Jang & K. H. Lee. (2020). A Study on the Effective Countermeasure of Business Email Compromise (BEC) Attack by AI. *Journal of The Korea Institute of Information Security & Cryptology*, *30(5)*, 835-846. DOI : 10.13089/JKIISC.2020.30.5.835

[11] KISA. (2019). *Analysis of overseas personal information protection trends in 2018*. Naju : Korea Internet & Security Agency.

[12] H. O. Kwon. (2020. Aug). *2020 KISA REPORT, Review of KISA, 8*, 44-50.

[13] KISA. (2017). *Analysis of overseas personal information protection trends in 2016*. Naju : Korea Internet & Security Agency.

[14] S. Y. Park & S. K. Kang. (2011). International Standardization Trend of ITU-T Spam Response Technology. *The Korea Institute of Information Security & Cryptology*, 21(2), 47-52.

[15] Y. C. Baek. (2007). A Study on Spam Regulation. *Journal of Information Management*, 38(4), 48-67.

[16] S. S. Shin. (2013. Aug). *KISA Internet & Security Focus, Review of KISA, 4*, 72-90.

[17] J. H. Baek & Y. J. Kim. (2014. Nov). *KISA Internet & Security Focus, Review of KISA, 2*, 18-38.

[18] KCC. (2021). *Report on the work plan for 2021 of the Korea Communications Commission*. Gwacheon : Korea Communications Commission.

[19] KCC. (2021). *A Pilot Case of Combining Pseudonymisation Information for SPAM Analysis*. Gwacheon : Korea Communications Commission.

[20] KCA. (2015). *Investigation Report : Investigation of the Situation of Unfair Sales of Telephone Solicitation*. Chungbuk Innovation City : Korea Consumer Agency.

[21] MSIT. (2021). *Result of Inspection on the Protection of MVNO's Resale Phone Users*. Sejong : Ministry of Science and ICT.

[22] FSC. (2021). *Comprehensive Audit Results for the Korea Federation of Banks*. Seoul : Financial Services Commission.

[23] BAI. (2020). *Audit Report : Status of Implementation of Telecommunication Financial Fraud Prevention Measures*. Seoul : THE Board of Audit and Inspection of KOREA.

[24] K. K. Kim. (2004. Sep). *OECD Focus, Review of OECD, 3(5)*, 16-23.

손 종 모(Jong-Mo Sohn) [정회원]

· 1984년 2월 : 서강대학교 수학과 (이학사)
· 1987년 2월 : 서강대학교 수학과 (이학석사)
· 2016년 10월~현재 : 서울여자대학교 정보보호학과 조교수

· 관심분야 : 개인정보보호, 빅데이터
· E-Mail : jmsohn@swu.ac.kr

임 효 창(Hyo-Chang Lim) [정회원]

· 1991년 2월 : 서강대학교 경영학과 (경영학사)
· 1993년 2월 : 서강대학교 경영학과 (경영석사)
· 1999년 2월 : 서강대학교 경영학과 (경영박사)

· 2007년 3월~현재 : 서울여자대학교 경영학과 교수
· 관심분야 : 인적자원관리, 기업보안, 성과관리
· E-Mail : hrm@swu.ac.kr