

보이스피싱의 심각성과 통합신고·대응 선호의 관계: 보이스피싱 대처방법의 조절효과를 중심으로

이 재 완*
은 중 환**

국문요약

본 연구는 일반국민들의 보이스피싱 심각성 인식이 보이스피싱 통합신고·대응에 대한 선호에 어떤 영향을 미치는지를 분석하고, 나아가 보이스피싱 대처방법이 이들 간의 관계를 조절하는지를 분석하고자 하였다. 이를 위해 본 연구는 '보이스피싱 범죄 정부합동수사단 출범 관련 여론조사' 데이터를 활용하여 상호작용항을 포함한 다중회귀모형으로 분석하였다. 그 분석결과, 보이스피싱 심각성 인식은 보이스피싱 통합신고·대응 선호에 긍정적인 영향을 미쳤으며, 대처방법 중 기준범주인 '경찰청 등에 신고'에 '비대응', '사칭기관 등에 재확인', '기타'의 경우 보이스피싱 통합신고·대응을 더 선호하는 것으로 나타났다. 보이스피싱 심각성 인식과 대처방법 간의 상호작용항은 '미대응', '사칭기관 등에 재확인', '기타'에서 유의미한 음(-)의 영향을 보여 보이스피싱 심각성 인식과 보이스피싱 통합신고·대응 선호 간의 관계를 약화시키는 것으로 확인되었다. 본 연구는 교육이나 홍보 캠페인을 통해 보이스피싱의 심각성을 강조할 필요가 있으며, 통합신고·대응센터와 같은 원스톱(one-stop) 방식도 중요하지만 일반국민들이 쉽고 간편하게 접근할 수 있도록 사용자 친화적인 온라인 플랫폼이나 모바일 애플리케이션 개발 등도 필요함을 시사한다.

주제어: 보이스피싱, 심각성 인식, 통합신고·대응, 정책 선호, 대처방법

I. 서론

보이스피싱은 디지털 시대에도 만연하고 있는 진화하는 위협으로 개인과 조직 모두에 위협을 초래하고 있다. 사이버 범죄자들이 점점 더 정교한 수법을 사용함에 따라 보이스피싱 사건을 신고하고 대응하는 데 있어 일반국민들의 선호에 영향을 미치는 요인들을 이해하는 것은 효과적인 정책 수립 및 사이버 보안 전략을 위해 중요해졌다. 본 연구는 보이스피싱 통합신고·대응에 대한 선호를 형성하는 복잡한 역학을 조사하고 대중 인식 및 정책개발에 대한 영향을 탐구하고자 하였다. 즉, 최근 우리 정부가 보이스피싱 범죄에 효과적으로 대응하기 위해 통합신고·대응 체계를 마련하였는데, 이에 대해 일반국민들의 선호에 보이스피싱 심각성 인식이 미치는 효과를 분석하고자

* 제1저자

** 교신저자

하였다. 나아가 이 둘 간의 관계를 보이스피싱 대처방법이 조절하는지를 분석하고자 하였다. 이를 위해 법무부와 문화체육관광부가 공동으로 조사한 ‘보이스피싱 범죄 정부합동수사단 출범 관련 여론조사’ 데이터를 활용하였다.

최근 우리나라 보이스피싱 범죄발생 현황을 보면, 2006년 발생한 이래 증가세를 나타내다가 2019년 37,667건으로 최고치를 기록한 후 코로나19로 인해 사기활동이 위축되면서 감소하는 추세로 전화되어 2020년 31,681건, 2021년 30,982건, 2022년 21,832건으로 감소하였다(통계개발원, 2023). 감소추세이기는 하지만 여전히 보이스피싱은 서민들의 경제를 위축시키고 사회 신뢰를 저해하고 있다. 이에 우리 정부는 2008년 보이스피싱 피해예방 10계명을 발표한 이래 다양한 대응책을 내놓았다. 윤석열 정부도 2022년 12월 정부합동수사단을 출범시키고 2023년에는 보이스피싱 통합신고·대응센터를 설치하여 통합신고·대응체계를 구축하였다(국무조정실, 2023). 한편 통합신고·대응체계의 경우 각 주체 간 연계를 효율적이고 지속화시키기 위해서는 이를 제도화할 필요가 있고, 그러한 제도화를 통하여 범죄예방에 필요한 각 주체 간의 의무적 연계를 이끌어낼 수 있도록 노력을 기울여야 할 것이다(박광섭·박행렬, 2007: 192). 그러나 위와 같은 보이스피싱 대응책은 주로 형사사법기관 및 금융감독기관 등을 중심으로 한 공급자 시각에서 접근한 것이다. 보이스피싱을 비롯한 사이버범죄의 경우 시민들과의 파트너십이 중요하다고 알려져 있다(이성식, 2006). 보이스피싱으로부터 위협을 받고 있거나 받을 우려가 있는 일반국민들의 시각을 반영하지 못하고 있다. 이 때문에 여전히 통합신고·대응을 체계적으로 운영할 필요성이 대두되고 있다(고상근, 2023).

따라서 본 연구에서는 보이스피싱 통합신고·대응에 대한 선호에 미치는 영향을 미치는 요인들에 초점을 두고 분석하고자 하였다. 특히 범죄예방책에 중요한 영향을 미친다고 알려진 범죄 심각성 인식이 보이스피싱 통합신고·대응 선호에 미치는 효과를 분석하고자 하였다. 나아가 보이스피싱 심각성 인식과 보이스피싱을 경험한 일반국민들이 선택한 대처방법 간의 상호작용을 분석해 보이스피싱 심각성 인식과 통합신고·대응 선호에 어떻게 영향을 미치는지에 대한 이해를 풍부하게 하여 정책입안자와 사이버 보안 전문가 등에게 실무적인 통찰력을 제공하고자 하였다. 진화하는 사이버 위협 환경에 맞춰 사이버 보안 전략을 수립하는 것이 필수적이라는 점에서 보이스피싱 대응책에 대한 일반국민들의 선호를 이해하는 것은 시의적절할 뿐만 아니라 사이버 보안을 강화하기 위한 기본 단계라 할 수 있다.

II. 논의의 배경

1. 보이스피싱 현황

보이스피싱은 1997년 대만에서 시작되었으며, 우리나라에서는 2006년 5월 18일 ‘국세청 직원 사칭 환급금 사기 사건’이 발생한 이래 증가 추세를 보이고 있다(채문희·박찬혁, 2018). 보이스피싱(Voice Phishing)은 음성(Voice)으로 개인정보(Private data)를 낚는다(Fishing)는 의미를 가지고

있다(홍성삼, 2019). 보이스피싱은 피해자를 속이거나 협박하여 금융거래 정보 또는 개인정보를 요구하거나 금전 이체를 노리는 금융사기범죄의 일종이다(홍성삼, 2019). 보이스피싱 범죄는 주로 국제적인 조직망을 통해 인터넷 국제전화 등 복잡한 발신경로를 거쳐 행해지는데, 최근에는 서버를 해외에 두고 중계기를 국내에 설치하여 피해자에게 접근하여 금품을 수수하고 국내 수금책을 통해 송금하는 등 범죄수법이 다변화되고 있다(홍성삼, 2019).

보이스피싱의 특징은 검찰, 경찰, 금융감독원 등 공공기관이나 금융기관을 사칭하며, 발신번호를 조작해 해당 기관의 전화번호가 발신번호창에 뜨도록 하며, 전화나 문자메시지를 통해 개인정보 유출, 범죄사건 연루, 납치 등 허위사실로 심리적 압박을 가해 피해자의 금융정보를 불법으로 취득하고, 대출 또는 취업 등을 미끼로 획득한 예금통장을 사기에 활용하여 이체하게 하거나 인출한 돈을 수거책에게 건네는 방법 등을 활용한다(단국대 산학협력단, 2013). 피해자는 서민층이나 고령층이 다수를 차지하고 있고, 피해자의 경제 상황에 상당한 영향을 미치며, 민생 경제 전반에 악영향을 미친다(신진, 2012).

최근 우리나라에서 발생하고 있는 보이스피싱의 특징을 보면, 먼저 경찰청 통계에 따르면 보이스피싱 발생 건수 기준으로 대면편취형 비중이 2019년 8.6%에서 2022년 64.3%로 대폭 증가하였다(금융감독원, 2023). 그리고 오픈뱅킹·간편송금을 활용하고 고도화된 악성 앱을 이용하는 등 범죄 수법이 지능화되는 추세이며, 지급정지 제도를 악용한 신종사기 수법 등이 성행하여 선의의 피해자가 발생하고 있으며, 취득한 정보를 토대로 접근하여 피해자 상황에 맞춘 보이스피싱 시나리오의 활용이 증가하고 있다(금융감독원, 2023).

〈표 1〉 우리나라 보이스피싱 유형별 피해 현황

(단위: 명, 건, 억원)

구분		2018년	2019년	2020년	2021년	2022년	2023년 상반기
대출 빙자	피해자수	36,184	38,861	11,207	3,014	1,437	1,161
	피해건수	55,040	56,216	14,686	3,710	1,781	1,266
	피해액	3,095	4,506	1,566	521	311	241
기관 사칭	피해자수	4,226	4,548	1,225	514	899	1,243
	피해건수	5,604	7,966	2,252	912	1,310	2,007
	피해액	1,129	1,872	414	170	213	292
지인 사칭	피해자수	8,355	6,963	5,833	9,685	10,480	2,925
	피해건수	9,607	8,306	8,921	25,287	25,534	7,460
	피해액	216	342	373	991	927	320
합계	피해자수	48,765	50,372	18,265	13,213	12,816	5,329
	피해건수	70,251	72,488	25,859	29,909	28,619	10,733
	피해액	4,440	6,720	2,353	1,682	1,451	853

출처: 동아경제(2023).

보이스피싱의 유형은 '특정인을 대상'으로 하는 유형과 '불특정다수를 대상'으로 하는 유형으로 구분할 수 있다(장주성, 2022). 먼저, '특정인을 대상'으로 하는 유형은 협박형, 지인사칭형, 의무부과형으로 세분할 수 있다. 협박형은 피해자에 대한 신상정보를 알고 있는 상황에서, 가족을 납치했다는 식의 절박한 상황을 연출해 심리적 압박을 가해 협박하고 몸값을 요구한다. 지인사칭형은 메신저를 해킹해 아이디와 패스워드를 알아낸 후, 친구목록에 있는 사람들에게 대화를 걸어 급전이나 합의금 등의 명목으로 돈을 편취하며, 의무부과형은 대학교 추가합격 관련 등록금 납부를 요구하거나 동창회를 사칭해 회비를 요구하는 유형으로, 대인관계를 유지하려는 사람들의 심리를 교묘하게 이용한다(장주성, 2022).

다음으로 '불특정 다수를 대상'으로 하는 유형은 보호형, 보상제공형으로 세분할 수 있다. 보호형은 금융감독원, 검찰, 경찰을 사칭하며 개인금융정보가 유출되어 보호가 필요하다고 접근한 후 개인 정보를 알아내는 방식이다(장주성, 2022). 보상제공형은 보험금, 세금 등의 초과 납부분에 대한 환급 등 공짜로 이익을 얻을 수 있다는 말로 사람의 심리를 교묘하게 이용하는 유형으로, 초기에는 주로 노년층을 대상으로 했지만, 점점 전(全) 연령대에 걸쳐 피해가 발생하고 있다(장주성, 2022).

최근 5년간 보이스피싱 유형별 피해 현황을 살펴보면, 먼저 대출빙자형의 경우 피해건수 91,864명, 피해건수 132,699건, 피해금액 1조240억원이었다(동아경제, 2023). 그리고 기관사칭형의 경우 피해자수 12,655명, 20,051건, 피해액 4천90억원이었고, 지인사칭형의 경우 피해자수 44,241건, 피해건수 85,115건, 피해액 3천169억원이었다(동아경제, 2023).

한편 메신저피싱의 경우 문자메시지 등을 활용하여 피해자를 기망하여 금품을 편취하는 방법으로, 그 전달매체인 메신저로 카카오톡, 네이버온, 페이스북, 텔레그램, 기타 등 다양하다. 최근 5년간 우리나라의 메신저피싱 피해 현황을 살펴보면, 피해건수는 총 85,115건, 피해액은 3,168억원이었다(동아경제, 2023). 메신저 종류별로 보면, 먼저 카카오톡의 경우 피해건수 23,680건, 피해금액 755억원이었고, 네이버온은 피해건수 713건, 피해액 53억원이었다. 페이스북은 피해건수 474건, 피해액 6.5억원이었으며, 텔레그램은 피해건수 25건, 피해액 3억원, 기타의 경우 피해건수 60,223건, 피해액 3,168억원이었다(동아경제, 2023).

2. 보이스피싱에 대한 대응

보이스피싱에 대한 대응은 크게 나눠 피해자인 일반국민의 대처요령과 금융기관의 예방 제도로 나눌 수 있다(금융감독원, 2023). 먼저 피해자의 대처요령은 계좌지급 정지, 명의도용 계좌·대출 확인, 개인정보 노출 등록, 휴대폰 명의도용 방지 등이 있다. 계좌지급 정지는 본인 계좌 또는 사기범 계좌의 금융회사나 금융감독원 콜센터로 지체 없이 피해사실을 신고하여 계좌로 지급이 되지 않도록 하는 것이다. 가까운 경찰서에 방문하여 보이스피싱 피해사실에 대한 '사건사고사실 확인원'을 발급받아 3영업일 내에 지급정지 신청한 금융회사에 제출하면 되는데, 신속한 지급정지로 잔액이 남아있는 경우 금융감독원의 피해금 환급절차를 통해 피해구제가 가능하다(금융감독원, 2023). 명의도용 계좌·대출 확인(내계좌 통합관리)은 '계좌정보 통합관리서비스'에서 본인 명

의로 개설된 계좌 또는 대출을 한눈에 확인하여 명의도용 피해가 없는지 확인하는 방법이다. 본인 모르게 개설된 계좌가 있을 경우 '내계좌지급정지' 메뉴에서 일괄 지급정지가 가능하다(금융감독원, 2023). 개인정보 노출 등록은 신분증 사본 등을 사기범에게 제공하였거나, 출처가 불분명한 URL을 클릭하여 개인정보가 노출되었다고 판단한 경우 '개인정보 노출자'로 등록하는 방법이다. 개인정보 노출자로 등록되면 신규 계좌개설, 신용카드 발급 등이 제한되어 추가적인 명의도용 피해 예방이 가능하다(금융감독원, 2023). 휴대폰 명의도용 방지는 '명의도용 방지서비스'를 이용하여 본인 모르게 개통된 이동전화, 인터넷 전화 등 이동통신사 가입현황을 조회하는 것으로, 그 결과 명의도용으로 인한 개통이 확인되면 해당 통신사 등에 연락하여 회선 해지신청 및 명의도용을 신고하면 된다. 피해 이전에 본인 명의 이동전화의 신규 개설을 차단하는 「가입제한 서비스」를 이용하면 휴대폰 명의도용에 따른 피해 예방이 가능하다(금융감독원, 2023).

한편 금융기관은 보이스피싱 또는 개인정보유출에 따른 명의도용으로 발생하는 피해를 방지하기 위해 여러 가지 사전예방 서비스를 운영 중이다(금융감독원, 2023). 사전에 금융소비자가 지정한 방식의 금융거래만 가능하도록 하여, 비정상적 금융거래가 발생하지 않도록 방지할 수 있는데, 금융회사 홈페이지나 모바일앱에서 신청 가능하며, 서비스 해지는 본인확인을 위해 영업점 방문이 필요하다(금융감독원, 2023). 여기에는 ATM 지연인출 제도, 지연이체 서비스, 입금계좌 지정 서비스, 단말기 지정 서비스, 해외 IP 차단 서비스, 카드사의 고령자 지정인 알림서비스 등이 있다. ATM 지연인출 제도는 100만원 이상 현금이 계좌로 입금된 경우 30분간 해당 금액이 자동화기기(ATM/CD기)로 인출·이체되는 것을 정지시켜 피해금 인출을 지연하는 것이다(금융감독원, 2023). 지연이체 서비스는 전자금융거래를 이용한 이체시 본인이 지정한 일정 시간(최소 3시간) 후 수취인 계좌에 입금되도록 지연하는 것이다(금융감독원, 2023). 입금계좌 지정 서비스는 미리 지정한 계좌로 본인의 전자금융 이체 한도 내에서 자유롭게 송금 가능하지만, 미지정 계좌로는 소액 송금만 가능한 것이다(금융감독원, 2023). 단말기 지정 서비스는 본인이 미리 지정한 기기(스마트폰, PC 등)에서만 주요 금융거래가 가능한 서비스로, 미지정 기기에서는 추가 인증을 요구해 제3자에 의한 거래를 차단한다(금융감독원, 2023). 해외 IP 차단 서비스는 해외에서 접속한 IP로 확인된 경우 전자금융거래를 제한하여 이상 접속으로 인한 자금 이체를 차단한다(금융감독원, 2023). 카드사의 고령자 지정인 알림서비스는 만65세 이상 개인 중 본인이 희망한 고객에 한해 본인의 카드대출 이용 내역을 지정인에게 문자로 제공하여 부정대출을 방지하는 것이다(금융감독원, 2023).

우리 정부는 보이스피싱을 중대한 반사회적 민생침해 범죄로 인식하고, 2009년 보이스피싱 문제에 대한 방지대책으로 '국제전화 식별번호 표시'를 기간통신사업자뿐만 아니라 주요 별정통신사업자로 확대 시행하였다(방송통신위원회, 2009). 2011년에는 우체국, 국민은행 등 금융기관이 운영하고 있는 자동응답시스템(ARS)의 메뉴 체계를 개선해 보이스피싱 피해신고에 필요한 시간을 절반으로 단축하였다(방송통신위원회, 2011). 또한 전기통신수단을 이용한 금융사기의 피해자가 소송절차를 거치지 않고 피해금을 신속히 돌려받을 수 있도록 채권 소멸절차와 피해금 환급절차 등을 마련하여 전기통신금융사기 피해자를 구제하기 위한 근거법률로 2011년 「전기통신금융사기 피해금 환급에 관한 특별법」을 제정하였다. 2013년에는 '전자금융사기 예방서비스'를 모든 고객에게 확대

하였으며, 금융위원회, 금융감독원 등 금융당국은 물론 통신, 사법, 경찰 등 관계부처를 총망라해 총력 대응하고 특히 사전예방 강화에 초점을 두는 것으로 전환하였다(금융위원회, 2013). 2019년에는 방송통신위원회와 금융위원회, 금융감독원, 경찰청은 이날 한국정보통신진흥협회, 이동통신 3사 및 알뜰통신사업자 37개사와의 협력을 통해 '전화금융사기 피해예방 문자메시지'를 발송하기 시작하였다(금융위원회, 2019). 2020년에는 보이스피싱 수법과 수단이 지능화 고도화됨에 따라 종합적이고 지속적인 강력 대응이 필요하다는 판단에서 보이스피싱 척결 종합방안을 마련하였다. 보이스피싱 척결 종합방안은 예방·차단·단속·처벌·피해구제-경각심 강화의 4단계에 대한 단계별 대응 강화와 함께 집행의 실효성을 높일 수 있도록 관계부처간 상시 협업체계를 구축·강화하였다(금융위원회, 2020). 2021년에는 금융기관 사칭에 따른 보이스피싱 피해를 막기 위해 문자메시지가 아닌 새로운 형태의 차세대 메시지 서비스를 도입하였다(기획재정부, 2021).

2022년에는 합동수사단을 설치하고, 여러 부처에 분산된 수사·대응업무도 통합신고·대응센터를 만들어 일원화하기로 하였다(국무조정실, 2022). 2023년 전기통신금융사기(보이스피싱) 통합신고·대응센터'를 개소하였으며, 보이스피싱 신고는 국번없이 112번, 인터넷은 '보이스피싱 지킴이' 사이트로 일원화하였다. 이에 보이스피싱 신고절차 및 피해구제가 대폭 간소화돼 한 번의 신고로 사건처리부터 피해구제까지 '원스톱'으로 처리할 수 있게 되었다(국무조정실, 2023). 통합신고대응센터는 국무총리훈령인 「전기통신금융사기 통합신고대응센터 설치 및 운영에 관한 규정」에 의해 설립되었으며, 센터장은 총경이며, 금융감독원과 KISA 직원 및 금융자문관(금융위원회 공무원), 통신자문관(과학기술정보통신부 공무원) 등으로 구성되었다(고상근, 2023). 경찰청은 센터의 운영을 2023년 11억 8백만원, 2024년 48억 5,200만원을 예산을 편성하였다(고상근, 2023).

그런데 우리 정부의 현행 보이스피싱 대응책은 주로 형사사법기관 및 금융감독기관 등 관계당국을 중심으로 한 대책으로 수요자인 일반국민의 입장을 반영하지 못한 한계가 있다. 일반적으로 보이스피싱을 비롯한 사이버범죄의 경우 국가나 정부 중심의 접근방법으로는 범죄예방과 근절에 실효를 거두기 어려우므로 일반시민들과의 파트너십이 중요하다고 알려져 있다(이성식, 2006). 이 때문에 일반국민들의 선호를 반영한 보이스피싱 통합신고·대응 체계를 마련하는 것이 중요하다(고상근, 2023). 이에 본 연구에서는 일반국민들을 대상으로 한 설문 결과를 토대로 보이스피싱 통합신고·대응 체계에 대한 방향성을 모색해보고자 한다.

한편 보이스피싱 대응책에 관한 연구하여 많은 연구들이 수행되었다. 해외연구들은 보이스피싱을 예방하기 위한 기술적 측면에 초점을 두고 있다(권한조·이재완, 2023). Selvan과 Vanitha(2013)는 효과적인 보이스피싱 예방을 위해 Multi Factor Authentication 기술을 제시하였다. Damodaram(2016)은 Antiphish 및 Dom Antiphish 기술, Mail Secure 피싱 방지 모듈, Browser Integrated Tools, Netcraft, ESET 스마트 보안체계 등을 제시하였다. Alkhalil et al.(2021)은 현재 사용자 교육, 기술적 해결책, 법집행 강화라는 세 가지 방법이 보이스피싱에 대한 대책으로 활용되고 있다고 하였다(권한조·이재완, 2023).

국내 연구의 경우 효과적으로 보이스피싱을 예방하고 피해구제를 할 수 있는 대응책으로 기존의 형사사법기관의 대응력 강화, 법률 개정 및 제도 개선, 그리고 종합적인 접근을 강조하는 연구

들이 있다. 먼저 형사사법기관인 경찰의 대응력 강화를 주장하는 연구들이 존재 한다. 이훈재(2009)는 전담수사기구 및 전담센터 설치, 국제공조시스템의 강화 및 유관기관과의 긴밀한 협조체제 구축, 범행계좌에 대한 경찰의 신속한 접근 허용, 효율적인 홍보활동, 피해지원팀을 통한 피해자금 지원, 정신과 상담 및 법률상담 등을 제안하였다. 이동임(2010)은 형사사법기관인 법원, 검찰, 경찰, 금융기관이 협의체를 구성하여 범죄피해가 명확하다면 돌려받는 절차를 간소화하여야 한다고 주장하였다. 조호대(2012)는 경찰 단속활동 강화, 인터폴 등 관련기관 및 국제공조협력 강화를 제시하였고, 김덕용(2018)은 순찰활동 강화, 단일화된 국가기관 신설, 해외발신번호 변작행위 근절, 선별적인 홍보, 전담센터의 설치 등을 제안하였다. 정웅(2020)은 보이스피싱 수사 인력 확충, 전담부서의 정식 직제화, 국외 추적수사 및 외국 현지 경찰과의 공조, 유관기관·업계와의 정보협력 강화 등을 제시하였다. 김시윤·이범주·이용걸(2022)은 보이스피싱 담당 경찰관 관점에서 범죄예방 측면의 음성 인터넷 프로토콜 게이트웨이와 가상 사설망, SIM 박스, 부정가입 방지, 메신저 피싱에 대해 전반적인 대응, 추가 피해 확산 방지 측면의 이용증지 관련 현황 분석 및 전반적인 개선, 이용증지 대상 확대, 이용증지 관련 법적 개선, 효율적인 수사를 위해 수사 전담 기관의 조직 체계 개선을 제안하였다. 손현종·문광선(2022)은 자치경찰제에서 광역성을 가진 보이스피싱 범죄에 대해 영국 런던시경의 국가사기정보국(NFIB)의 형태처럼 국가경찰에서 최신의 범죄 트렌드와 전반적 예방방안, 시도 자치경찰위원회에서 참고해야 할 사안 등을 공유할 것을 제안하였다. 신성원(2022)은 유관 기업과의 협조 강화, 범정부적 대응체계 구축, 방지제도 홍보 강화, 지연인출제도 강화, 국제공조 강화, 취약계층 교육 및 홍보 강화, 범죄자 및 대국민 대상 홍보 강화, 피해회복 지원 강화를 제시하였다.

다음으로 법률 개정 및 제도 개선을 통한 보이스피싱 대응을 주장하는 연구들이 존재한다. 이기수(2018)는 「범죄수익 은닉의 규제 및 처벌 등에 관한 법률」상 몰수대상으로 규정한 '중대범죄'의 범위에 보이스피싱을 포함시키고 「전자금융거래법」상 대표통장의 대여 및 매매 행위를 보다 중하게 처벌하는 법개정을 제안하였다. 황석진(2021)은 새로운 법률안 제정을 통한 사기범죄의 세분화, 경찰청 주관부서 지정을 통한 대응 및 예방활동 강화, 현실적인 피해자 구제 방안 마련, 사기방지 예방교육의 의무화, 지속적인 피해자 치유 등을 제안하였다. 정제용·염윤호(2023)는 사전 예방 및 차단 중요성, 국제 공조수사의 확대, 범국가적 규제방식 확대, 관련 법률 제·개정 추진, 빅데이터 활용 등을 통한 사전 적발 모델 개발 필요 등을 제시하였다.

그리고 개별적인 접근의 한계를 극복하고 종합적인 접근을 주장하는 연구들이 일찍부터 존재해 왔다. 광대경(2011)은 부정계좌 지급정지제도의 법률적 근거 강화, 국제 보이스피싱 처벌 특별법 제정, 전담수사기구 개편, 홍보와 교육 강화 및 국제범죄 예방·수사 공조 강화, 정보보안 기술의 개발 등을 제안하였다. 채문희·박찬혁(2018)은 모니터링제도의 실효성 확보, 역량 강화, 수사기관의 적극적인 협력과 공조, 전담팀과 인력증원 및 핫라인 활용, 포상금 차등화, 징벌적 배상제도 도입, 금융기관 간의 정보공유와 처벌 강화, 고객에 대한 홍보를 주장하였다. 장주성(2022)은 금융소비자 보호를 위해 긴급전화의 콜 리다이렉션 금지, 보호이체 서비스 출시, 원스탑 신고 시스템 구축, 피싱보험 판매 활성화 등을 제시하였다. 정영호·하형준(2022)은 메신저피싱 범죄에 대한 대응방안으로 수사기

관·민간기업의 협업체계 구축, 수사기관의 추적 개선, 맞춤형 예방홍보 등을 제시하였다. 김대호·한지혜·장광호(2023)는 보이스피싱 피해구제를 위해 수사기관-금융기관-지자체 간의 네트워크 구축, 보이스피싱 통합구제 전담 연구부서 구축, ICT기술 활용 시스템을 주장하였다.

이와 같이 선행연구들은 과거 법개정이나 제도 개선을 통한 처벌 강화에 초점을 두었던 것에서 최근에는 개별적인 접근을 한계를 인식하고 다양한 형사사법기관 및 금융기관 등 관련기관의 협력을 통한 대응을 강조하고 있으며, 보이스피싱 서버의 해외 이전 및 조직의 국제화 등을 인해 국제수사기구 및 해외 형사사법기관들과의 국제공조를 강조하고 있다. 그러나 이러한 주장들은 보이스피싱으로부터 위협을 받고 있는 피해자 내지 피해를 받을 우려가 있는 일반국민들의 선호를 반영한 대응책을 모색하는 단계에 이르지 못한 한계를 갖고 있다.

3. 범죄대책 선호에 관한 선행연구

범죄대책 선호에 대한 선행연구들은 일찍부터 이루어져 왔다. 선행연구들이 제시한 범죄대책 선호에 영향을 미치는 요인은 크게 사회심리적 요인과 인구통계학적 요인으로 구분할 수 있다 (Butter, Hermanns & Menger, 2013). 다시 사회심리적 요인에는 개인의 가치, 지식이나 관심, 범죄 심각성 인식, 범죄의 유형, 범죄에 대한 두려움과 피해, 정치적 관심 등이 있으며, 인구통계학적 요인에는 성별, 연령, 혼인상태, 자녀 유무, 경제불안정성 및 소득, 사회계층 등이 있다.

먼저 사회심리적 요인 중 개인의 가치는 종교성이나 세계관을 의미하는데, Finamore와 Carlson(1987)은 미국 대학생들을 조사한 결과 종교성 및 세계관이 범죄에 대한 처벌과 형사정책에 영향을 미친다고 하였으며, Grasmick과 McGill(1994)도 높은 종교성을 가질수록 그에 상응하는 처벌을 내리는 정책을 선호한다고 하였다. Samra-Grewal과 Roesch(2000)는 캐나다 대학생들을 대상으로 한 연구에서 범죄 이슈에 대한 지식과 관심의 정도가 높을수록 가석방 정책에 대한 선호가 높다고 하였다. Roberts(1992)는 형사적 정의를 실현하기 위한 대책에 대한 대중들의 선호에 범죄 심각성, 범죄 지식이 영향을 미친다고 하였다. Simpson et al.(2023)은 화이트칼라 범죄의 유형과 특징이 범죄대책 선호에 영향을 미친다고 하였다. Hartnagel과 Templeton(2012)은 범죄 피해경험과 경제적 불안정성이 범죄대책 선호에 영향을 미친다고 하였다. Galvin et al.(2018)은 화이트칼라 범죄의 경우 피해경험이 원상회복 프로그램 선호에 중요한 영향을 미친다고 하였다. Nagin et al.(2006)은 청소년 범죄의 경우 피해경험이 범죄대책 선호에 영향을 미친다고 하였다. Pearson-Merkowitz와 Dyck(2017)은 미국 총기범죄 대책에 대한 선호에 정치적 관심이 중요한 영향을 미친다고 하였다.

다음으로 인구통계학적 요인 중 성별의 경우 Matisson과 Mirrless-Black(2000)은 1998년 영국 범죄 서베이(1998 British Crime Survey)를 분석한 결과, 범죄대책 선호에 대해 성별 간에 중요한 차이가 있다고 하였다. Langworthy와 Whitehead(1986)는 미국 ABC의 여론조사를 분석하여 고연령층일수록 강력한 범죄대책을 선호한다고 하였다. Schwartz, Guo와 Kerbs(1993)는 청소년 범죄에 대한 대책에 연령, 인종과 종족, 혼인상태, 자녀 유무 등 인구통계학적 변수들이 영향을 미친다고

하였다. Toch와 Maguire(2014)는 성, 연령, 학력, 혼인 상태 등 인구통계학적 요인들이 범죄 정책에 대한 선호에 영향을 미친다고 하였다. Hough와 Moxon(1985)는 영국의 경우 사회계층에 따라 범죄대책 및 처벌에 대한 선호가 다르다고 하였다. Hogan, Chiricos와 Gertz(2005)는 경제적 불안정성이 범죄대책에 대한 선호에 영향을 미친다고 하였다. Weinrath, Young과 Kohm(2012)은 캐나다 Winnipeg시 주민들을 대상으로 한 설문데이터를 분석하여 범죄대책에 대한 선호에 연령, 성별, 혼인상태, 교육, 소득, 인종 등이 영향을 미친다고 하였다.

한편 보이스피싱 대책에 대한 선호에 영향을 미치는 요인들에 대한 연구들은 매우 드문 실정이다. 앞서 살펴본 바와 같이 해외 연구들은 주로 보이스피싱을 예방하기 위한 기술개발과 적용에 초점을 두고 있다. 국내 연구들은 주로 해외사례의 소개나 규범적 접근을 통한 대응책 제시에 초점을 두고 있으며, 최근 기술개발을 위한 연구들이 진행되었고, 보이스피싱 대책에 대한 인식과 선호를 분석한 연구들이 등장하고 있다. 보이스피싱에 대한 인식을 연구한 정제용·염운호(2023)는 보이스피싱 범죄사건을 수사하거나 연구한 전문가들을 대상으로 초점집단면접을 통해 범국가적 규제방식의 확대가 필요하다고 주장하였다. 한편 권한조·이재완(2023)은 일반국민들을 대상으로 한 설문데이터를 분석하여 보이스피싱 근절정책에 대한 선호에 본인의 피해경험, 보이스피싱 인지도, 성별, 연령, 혼인상태 등이 영향을 미친다고 하였다.

그러나 선행연구들은 일반적인 범죄대책에 대한 선호에 영향을 미치는 요인들을 중점으로 분석하였으며, 최근 등장하고 있는 보이스피싱 범죄대책에 대한 선호를 분석한 연구의 경우 여러 대안들 간의 선택문제를 다루는 것을 뿐, 형사사법절차나 처벌 등과 관련된 범죄대책을 본격적으로 다룬 것이라 보기에는 한계가 있다. 이에 본 연구에서는 보이스피싱 범죄대책인 통합신고·대응에 대한 선호에 영향을 미치는 요인들을 탐색적으로 분석하고자 하였다.

4. 선행연구와의 차별성과 본 연구의 가설

기존 선행연구들의 경향을 보면, 해외 연구들의 경우 보이스피싱에 대한 기술적 해결책에 초점을 두고 있으며, 국내 연구들의 경우 해외사례의 소개 및 법·제도적 개선에 초점을 두고 있다. 특히 국내 선행연구들은 보이스피싱 범죄의 실태와 문제점을 분석하고 그에 대한 대응책을 제시하는 규범적·처방적 연구가 주를 이루고 있다. 그러나 이러한 연구들은 보이스피싱 전담경찰관 또는 컴퓨터공학자, 법학, 범죄학 및 경찰학과 형사정책 전문가들의 시각에서 접근한 것들이다. 따라서 기존 연구들은 주로 공급자 중심의 시각에서 보이스피싱 대응책을 논의해 왔다고 할 수 있다. 일반국민들이 선호하는 대응 프로그램이 무엇인지에 대한 체계적인 분석 없이 전문가나 범죄 예방 관련 기관에 의해 보이스피싱 대응책이 제시되어 왔던 것이다. 이로 인해 실제 일반국민들이 체감하는 보이스피싱 문제해결에 한계가 있었으며, 정부가 새롭게 내놓은 대응책의 효과성에도 의문을 제기하였다고 할 것이다.

따라서 본 연구에서는 일반국민이라는 수요자 입장에서 보이스피싱의 심각성 인식이 보이스피싱 통합신고·대응에 대한 선호에 어떤 영향을 미치는지를 실증 분석하고자 하였다. 특히 다음과

같은 점에서 본 연구는 선행연구들과 차별성을 갖는다. 첫째, 우리 정부에서 최근 도입한 보이스피싱 통합신고·대응 체계에 대한 선호를 분석하고 있다. 선행연구들은 통합신고·대응책보다는 개별적인 범죄대책에 대한 선호를 분석하고 있으나, 본 연구는 통합적인 대책을 분석하고자 하였다. 둘째, 최근 증가 추세에 있는 보이스피싱 범죄의 심각성에 초점을 두고 그것이 범죄대책 선호에 미치는 영향을 분석하고자 하였다. 일반적인 범죄대책 선호에 대한 연구들에서는 범죄의 심각성을 독립변수로 다룬 연구들이 있으나, 보이스피싱 대책의 경우는 거의 없다. 셋째, 보이스피싱에 대해 어떻게 대처해 왔는지에 따라 보이스피싱의 심각성과 보이스피싱 대책에 대한 선호가 다를 수 있으므로 조절변수를 설정하여 분석하였다. 선행연구들은 조절변수로 인구통계학적 변인을 설정한 것들이 있었지만, 범죄에 대한 대처방법을 조절변수로 설정한 연구는 거의 없었다. 이와 같은 점들에 초점을 두고 본 연구를 진행하였다.

본 연구에서는 보이스피싱 심각성을 독립변수로 설정하고자 하였다. 범죄학 및 형사정책에 있어서 범죄 심각성 인식은 형사정책에 대한 태도에 중요한 영향을 미친다고 알려져 왔다(O'Connell & Whelan, 1996; Michel et al., 2014). Simpson et al.(2023)에 의하면 화이트칼라 범죄에 대한 심각성 인식은 범죄 예방책에 대한 선호에 중요한 영향을 미친다고 하였다. 따라서 본 연구에서는 보이스피싱 대응책과 관련된 상황 중 보이스피싱의 심각성을 일반국민들이 어떻게 인식하는지에 초점을 두고 분석하고자 하였다. 이와 같은 보이스피싱 심각성 인식이 최근 우리 정부가 추진하고 있는 보이스피싱 통합신고·대응 선호에 어떤 영향을 미치는지를 분석하기 위해 다음과 같은 가설을 설정하였다.

가설 1: 보이스피싱 심각성 인식은 보이스피싱 통합신고·대응 선호에 긍정적 영향을 미칠 것이다.

한편 본 연구에서의 조절변수인 범죄에 대한 대처방법은 범죄 심각성과 범죄대책 선호에 영향을 미칠 수 있다. Botchkovar, Tittle과 Antonaccio(2013)에 따르면, 긴장에 대한 대처방법은 회피, 알콜 의존, 범죄행동 등이 있으며, 처음 선택한 대처방법은 후속 긴장 대책에 영향을 미치며, 대처방법과 긴장의 강도는 상호작용을 통해 후속 긴장 대책에 영향을 미친다고 한다. 이와 마찬가지로 개인이 보이스피싱을 당한 경우 어떻게 대처하는지에 따라 보이스피싱 심각성 인식과 보이스피싱 통합신고·대응 선호 간의 관계에 차이가 있을 것이다. 보이스피싱의 피해자가 되지 않는 방법에 대해 전문가들은 3단계 행동 원칙을 숙지할 것을 강조한다(부산일보, 2016). 첫째는 '의심하라'이다. 국내 공공기관 관계자들이 일반국민에게 전화를 걸어 현금 인출 등을 안내하는 경우는 전혀 없으며, 상식에서 벗어난 엄청난 수익률을 제공하는 경우도 있을 수 없다. 이런 경우는 의심부터 해보아야 한다. 둘째는 '확인하라'이다. 해당 기관에 확인하면 진위를 알 수 있다. 셋째는 '신고하라'이다. 각 금융기관 콜센터, 경찰(112), 금융감독원(1332) 등에 최대한 빨리 신고해 도움을 받으면 된다(부산일보, 2016). 이러한 행동 원칙을 일반국민들이 숙지하고 있다면 보이스피싱 범죄는 발생하기 어려울 것이다. 그러나 현실적으로 이러한 행동 원칙, 즉 대처방법을 제대로 숙지하지 못하고 있거나 심리적 압박으로 당황하여 생각이 나지 않아 보이스피싱의 피해자로 전락하는 것이

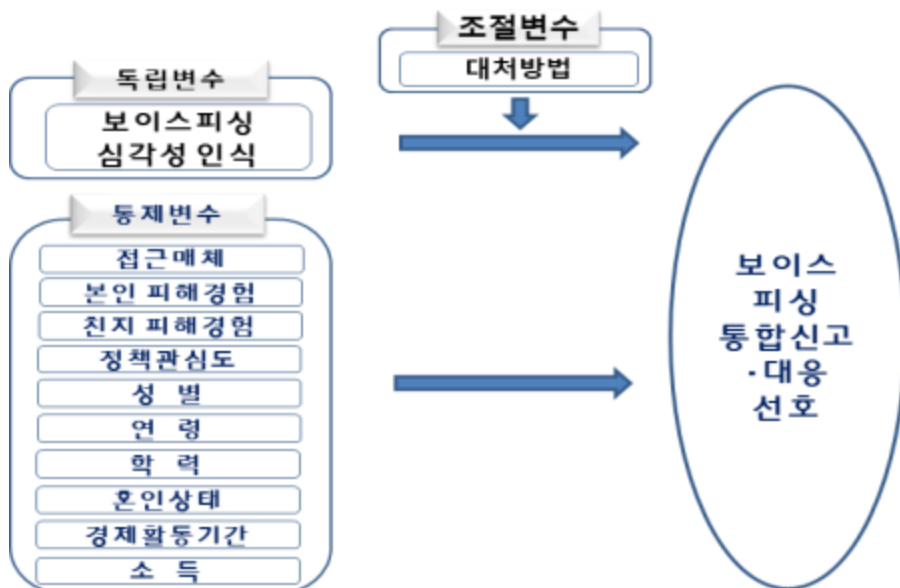
다. 따라서 보이스피싱을 당하고도 대처방법을 몰라서 제대로 대처하지 못한 경우와 그렇지 않은 경우에는 보이스피싱 대응책에 대한 반응이 다를 것이다(윤해성 외, 2023). 특히 최근 정부가 개선한 보이스피싱 통합신고·대응의 경우 몰라서 또는 번거로워서 신고를 하지 못하는 것을 방지하고자 하는 의도가 작용할 것이다. 따라서 보이스피싱 대처방법에 따라 그 선호에 큰 차이가 있을 것이다. 몰라서 대처하지 못한 경우는 손쉽게 신고할 수 있는 통합신고·대응에 대한 선호가 높을 것이라 예상할 수 있다. 반면 기존 대처방법에 대해 잘 알고 대처한 경우는 상대적으로 보이스피싱 통합신고·대응을 중복적인 것으로 인식하여 그다지 선호하지 않을 가능성이 존재한다. 또한 최근 피해자 휴대전화에 악성 앱이 깔려 112로 전화를 걸어도 다시 범죄조직원에게 연결되는 사건도 발생한 바 있다(중앙일보, 2023). 이렇게 되면 통합신고·대응을 위한 단일한 신고 전화번호인 112에 대한 선호가 낮아질 우려도 존재한다. 따라서 본 연구에서는 대처방법에 따른 차이를 검증하기 위해 다음과 같은 가설을 설정하였다.

가설 2: 보이스피싱 대처방법에 따라 보이스피싱 심각성 인식과 보이스피싱 통합신고·대응 선호의 관계에 차이가 있을 것이다.

Ⅲ. 연구방법

1. 연구의 모형과 방법

〈그림 1〉 본 연구의 분석틀



본 연구에서는 일반국민의 보이스피싱 심각성 인식이 보이스피싱 통합신고·대응 선호에 미치는 효과를 분석하기 위해 <그림 1>과 같은 분석틀을 설정하였다. 본 연구의 종속변수는 보이스피싱 통합신고·대응 선호이며, 독립변수는 보이스피싱 심각성 인식(Simpson et al., 2023), 그리고 조절변수는 보이스피싱 대처방법(Botchkovar, Tittle & Antonaccio, 2013)으로 설정하였다. 그리고 본 연구에서는 통제변수로 보이스피싱 통합신고·대응 선호에 영향을 미칠 수 있는 보이스피싱 관련된 요인들인 보이스피싱 접근매체(Simpson et al., 2023), 보이스피싱 본인 피해경험(Galvin et al., 2018) 및 친지 피해경험(Nagin et al., 2006), 정책관심도(Pearson-Merkowitz & Dyck, 2017)를 설정하고, 인구통계학적 변인으로 성별(Matison & Mirrless-Black, 2000), 연령(Langworthy & Whitehead, 1986), 학력(Toch & Maguire, 2014), 혼인상태(Weinrath, Young & Kohm, 2012), 경제활동기간(Hogan, Chiricos & Gertz, 2005) 및 소득(Hough & Moxon, 1985)을 포함하였다.

보이스피싱 통합신고·대응에 대한 선호에 영향을 미치는 다른 요소들을 통제하고, 보이스피싱 심각성 인식이 보이스피싱 통합신고·대응 선호에 미치는 영향을 분석하고, 보이스피싱 대처방법이 이들 간의 관계에 조절효과를 가지고 있는지를 살펴보기 위해 통상최소자승(OLS) 추정법으로 다중회귀모형(multiple regression model)을 활용하였다.

2. 자료수집 및 변수의 측정

1) 데이터의 출처

본 연구에서는 법무부와 문화체육관광부가 공동 의뢰해 마크로밀 엠브레인이 조사한 「보이스피싱 범죄 정부 합동수사단 출범 관련 여론조사」 데이터를 활용하였다. 이 조사는 보이스피싱 합동수사단 및 보이스피싱 통합신고·대응센터의 필요성 및 효과에 대한 객관적인 여론을 파악하고, 향후 운영 방향 수립을 위한 기초자료를 수집하고자 진행되었다(마크로밀 엠브레인, 2022). 조사 기간은 2022년 10월 27일에서 11월 8일까지이며, 조사방법은 온라인조사였다(마크로밀 엠브레인, 2022). 조사대상은 전국 만18세 이상 일반국민이며, 행정안전부의 2022년 9월 주민등록인구를 기준으로 성·연령·지역별 비례할당으로 1,500명을 추출하였으며, 표본오차는 95% 신뢰수준에서 최대허용오차 $\pm 2.53\%$ 이다(마크로밀 엠브레인, 2022).

본 연구에서는 보이스피싱 관련 문자 및 전화 등을 받아본 경험이 없는 사람을 제외한 1,208명의 응답을 분석에 활용하였다.

2) 변수의 조작적 정의와 측정

본 연구의 분석모형에 포함될 주요 변수의 조작적 정의와 측정은 다음과 같다. 먼저 종속변수인 ‘보이스피싱 통합신고·대응 선호’는 “귀하께서는 보이스피싱 통합신고 및 대응이 얼마나 필요하다고 생각하십니까?”라는 질문으로 “①전혀 필요하지 않다, ②별로 필요하지 않다, ③다소 필요하다, ④매우 필요하다” 등의 4점 척도로 측정하였다.

그리고 독립변수인 ‘보이스피싱 심각성 인식’은 “귀하께서는 보이스피싱이 우리 사회에 얼마나 심각하다고 생각하십니까?”라고 질문하여 “①전혀 심각하지 않다, ②심각하지 않다, ③심각하다, ④매우 심각하다”의 4점 척도로 측정하였다.

조절변수인 ‘보이스피싱 대처방법’은 “귀하께서는 보이스피싱을 당했을 때 주로 어떻게 대처하셨습니다?”라는 질문을 통해 “①몰라서 아무 대응하지 않았다(무대응), ②경찰청, 금융감독원, 인터넷진흥원, 경찰민원콜센터 등에 신고하였다(신고), ③사칭을 한 금융기관, 사법기관, 지인 등에게 재확인했다(재확인), ④기타”로 구분하여 측정하였다.

통제변수에 해당하는 ‘접근 매체’는 “귀하께서 당한 보이스피싱은 주로 어떤 매체를 통해 접근한 피싱이었습니까?”라는 질문으로 “①전화, ②문자, ③기타”로 구분하여 측정하였다. 보이스피싱으로 인한 ‘본인 피해경험’은 “귀하께서는 보이스피싱으로 인해 지금까지 금전적 피해를 입은 적이 있습니까?”라는 질문으로, ‘친지 피해경험’은 “귀하의 가족 및 지인(친지)이 보이스피싱으로 인해 금전적 피해를 입은 적이 있습니까?”라는 질문으로 “①금전적 피해를 입은 적이 있다, ②금전적 피해를 입은 적은 없다”로 측정하였다. ‘정책관심도’는 “귀하께서는 평소 정부정책이나 국정과제에 대해 얼마나 관심을 가지고 계십니까?”라는 질문으로 “①관심이 전혀 없다, ②관심이 별로 없는 편이다, ③관심을 가지고 있는 편이다, ④매우 관심을 가지고 있다”의 4점 척도로 측정하였다.

성별은 “귀하의 성별은 무엇입니까?”라는 질문으로 남성을 기준으로 더미변수로 측정하였으며, 연령은 응답자의 출생연도를 기준으로 만 나이를 산정하여 연속형으로 측정하였다. 학력은 “귀하의 학력은 어떻게 되십니까?”라고 질문하여 “①중학교 졸업 이하, ②고등학교 졸업, ③대학교 재학/졸업(2년제·3년제 포함), ④대학원 재학/졸업”으로 측정하였다. 혼인상태는 “귀하의 현재 혼인상태는 어디에 해당하십니까?”라는 질문으로 “①미혼(=기준), ②기혼, ③기타”로 구분하여 더미변수로 측정하였다. 경제활동 기간은 “귀하께서 경제활동을 한지는 얼마나 되었습니까?”라고 질문하여 “①경제활동을 하지 않는다, ②3년 미만, ③3년~5년 미만, ④5년~10년 미만, ⑤10년~20년 미만, ⑥20년 이상”으로 구분하여 측정하였다. 소득은 응답자가 속한 가구의 월평균 합산 세전 소득으로 “①200만원 미만, ②200~300만원 미만, ③300~400만원 미만, ④400~500만원 미만, ⑤500~600만원 미만, ⑥600~700만원 미만, ⑦700~800만원 미만, ⑧800만원~900만원 미만, ⑨900만원~1,000만원 미만, ⑩1,000만원 이상”으로 구분하여 측정하였다. 본 연구의 주요 변수들의 조작적 정의와 측정을 정리하면 <표 2>와 같다.

〈표 2〉 주요 변수의 측정

영역	변수	설문문항	측 정
종속 변수	보이스피싱 통합신고·대응센터 선호	귀하께서는 보이스피싱 통합신고 및 대응이 얼마나 필요하다고 생각하십니까?	①전혀 필요하지 않다, ②별로 필요하지 않다, ③다소 필요하다, ④매우 필요하다
독립 변수	보이스피싱 심각성 인식	귀하께서는 보이스피싱이 우리 사회에 얼마나 심각하다고 생각하십니까?	①전혀 심각하지 않다, ②심각하지 않다, ③심각하다, ④매우 심각하다

영역	변수	설문문항	측 정
조절 변수	보이스피싱 대처방법	귀하께서는 보이스피싱을 당했을 때 주로 어떻게 대처하셨습니다?	①몰라서 아무 대응하지 않았다(무대응), ②경찰청, 금융감독원, 인터넷진흥원, 경찰민원콜센터 등에 신고했다(신고), ③사칭을 한 금융기관, 사법기관, 지인 등에게 재확인했다(재확인), ④기타
통제 변수	접근 매체	귀하께서 당한 보이스피싱은 주로 어떤 매체를 통해 접근한 피싱이었습니까?	①전화, ②문자, ③기타
	본인 피해경험	귀하께서는 보이스피싱으로 인해 지금까지 금전적 피해를 입은 적이 있습니까?	①금전적 피해를 입은 적이 있다, ②금전적 피해를 입은 적은 없다(=기준)
	친지 피해경험	귀하의 가족 및 지인이 보이스피싱으로 인해 금전적 피해를 입은 적이 있습니까?	
	정책관심도	귀하께서는 평소 정부정책이나 국정과제에 대해 얼마나 관심을 가지고 계십니까?	①관심이 전혀 없다, ②관심이 별로 없는 편이다, ③관심을 가지고 있는 편이다, ④매우 관심을 가지고 있다
	성별	귀하의 성별은 무엇입니까?	①남성(=기준), ②여성
	연령	응답자의 만 나이	만 나이(단위:세)
	학력	귀하의 학력은 어떻게 되십니까?	①중학교 졸업 이하, ②고등학교 졸업, ③대학교 재학/졸업(2년제·3년제 포함), ④대학원 재학/졸업
	혼인상태	귀하의 현재 혼인상태는 어디에 해당하십니까?	①미혼(=기준), ②기혼, ③기타
	경제활동 기간	귀하께서 경제활동을 한지는 얼마나 되었습니까?	①경제활동을 하지 않는다, ②3년 미만, ③3년~5년 미만, ④5년~10년 미만, ⑤10년~20년 미만, ⑥20년 이상
	소득	귀댁의 한 달 평균 가구 수입은 얼마나 되십니까? (부수입, 보너스 등 모두 포함, 세전 소득 기준)	①200만원 미만, ②200~300만원 미만, ③300~400만원 미만, ④400~500만원 미만, ⑤500~600만원 미만, ⑥600~700만원 미만, ⑦700~800만원 미만, ⑧800만원~900만원 미만, ⑨900만원~1,000만원 미만, ⑩1,000만원 이상

IV. 분석 결과

1. 주요 변수의 기술통계

1) 데이터의 출처

〈표 3〉 응답자의 주요 특성별 분포

변 수		빈도	비율(%)	변 수		빈도	비율(%)
성별	남성	578	47.85	본인 피해경험	있음	78	6.46
	여성	630	52.15		없음	1,130	93.54
혼인 상태	미혼	375	31.04	친지 피해경험	있음	222	18.38
	기혼	797	65.98		없음	986	81.62
	기타	36	2.98	대처방법	미대응	523	43.29
접근 매체	전화	496	41.06		신고	170	14.07
	문자	641	53.06		재확인	291	24.09
	기타	71	5.88		기타	224	18.54

응답자의 인구통계학적 특성을 살펴보면, 성별의 경우 여성이 52.15%로 과반을 차지하였으며, 남성은 47.85%였다. 혼인상태의 경우 기혼이 65.98%로 가장 많았고, 미혼이 31.04%, 기타가 2.98% 순이었다.

그리고 보이스피싱 접근 매체의 경우 문자가 53.06%로 가장 많았으며, 전화가 41.06%, 기타가 5.88% 순이었다. 보이스피싱으로 인한 본인 피해경험의 경우 ‘없음’이 93.54%를 차지하고 ‘있음’은 6.46%였다. 친지 피해경험의 경우 ‘없음’이 81.62%였으며 ‘있음’이 18.38%였다. 보이스피싱 대처방법의 경우 ‘미대응’이 43.29%로 가장 많았으며, ‘재확인’이 24.09%, ‘기타’가 18.54%, ‘신고’가 14.07% 순이었다.

2) 주요 변수의 기술통계량

본 연구의 분석모형에 포함된 주요 변수들의 기술통계량은 〈표 4〉와 같다. 먼저 보이스피싱 통합신고·대응 선호의 평균은 4점 만점에 3.734점으로 나타났다. 다음 보이스피싱 심각성 인식의 평균은 4점 만점에 1.300점이었으며, 정책관심도의 평균은 4점 만점에 2.960점이었다. 그리고 연령의 경우 평균 48.036세였으며 최소값은 만18세, 최대값은 만80세였다. 학력의 평균은 4점 만점에 2.906점이었고, 소득의 평균은 10점 만점에 4.190점이었다.

〈표 4〉 주요 변수들의 기술통계량

변수명	관측치	평균	표준편차	최소값	최대값
통합신고·대응 선호	1,208	3.734	0.478	1	4
심각성 인식	1,208	1.300	0.478	1	3
정책관심도	1,208	2.960	0.642	1	4
연 령	1,208	48.036	14.542	18	80
경제활동 기간	1,208	3.619	2.078	1	6
학 령	1,208	2.906	0.657	1	4
소 득	1,208	4.190	2.390	1	10

2. 1. 보이스피싱 통합신고·대응 선호에 대한 분석 결과

1) 집단간 보이스피싱 통합신고·대응 선호의 차이

〈표 5〉 보이스피싱 대처방법과 보이스피싱 통합신고·대응 선호

구분		빈도	평균	표준편차	F값 (p-value)
대처 방법	미대응	523	3.734	0.476	0.630 (0.594)
	신고	170	3.735	0.517	
	재확인	291	3.759	0.444	
	기타	224	3.701	0.496	

먼저 보이스피싱 대처방법과 보이스피싱 통합신고·대응 선호에 차이가 있는지를 ANOVA 분석을 통해 알아보았다. 그 결과, 보이스피싱 통합신고·대응 선호에 대한 대응방법별 차이는 통계적으로 유의미하지 않았다.

다음 보이스피싱 접근 매체와 보이스피싱 통합신고·대응 선호에 차이가 있는지에 대해 ANOVA 분석을 하였다. 접근 매체가 기타인 집단의 보이스피싱 통합신고·대응 선호의 평균이 3.775점으로 가장 높았고, 문자인 집단의 경우 평균은 3.760점, 전화인 집단의 평균은 3.696점 순이었다. 보이스피싱 통합신고·대응 선호에 대한 접근 매체별로 통계적으로 유의미한 차이가 있었는데, 가장 보수적인 Scheffe 사후검정 결과 '전화'의 경우가 나머지 접근 매체와 다른 집단으로 묶였다.

〈표 6〉 보이스피싱 접근매체와 보이스피싱 통합신고·대응 선호

구분		빈도	평균	표준편차	F값 (p-value)
접근 매체	전화	496	3.696 ^{a)}	0.507	2.800 (0.061)
	문자	641	3.760 ^{b)}	0.449	
	기타	71	3.775 ^{b)}	0.513	

주: Scheffe 사후검정 a < b.

그러나 이러한 결과는 다른 혼란변인들을 통제하지 않은 단순한 집단 간 차이에 불과하다. 따라서 혼란변인들을 통제한 다중회귀모형으로 분석할 필요가 있다.

2) 주요 연속형 변수들의 상관관계

본 연구의 분석모형에 포함된 주요 연속형 변수들 간의 상관관계를 분석한 결과는 〈표 7〉과 같다. 먼저 종속변수인 보이스피싱 통합신고·대응 선호와 보이스피싱 심각성 인식은 -0.340으로 낮은 음(-)의 상관관계를 나타냈고, 정책관심도 및 연령은 낮은 양(+의 상관관계를 나타냈다. 통제 변수들 간의 상관관계도 낮은 상관관계를 나타냈다.

〈표 7〉 주요 연속형 변수들의 상관관계

구 분	1.	2.	3.	4.	5.	6.
1.통합신고·대응 선호	1.000					
2.심각성 인식	-0.340***	1.000				
3.정책관심도	0.235***	-0.139***	1.000			
4.연령	0.127***	-0.072**	0.124***	1.000		
5.경제활동 기간	0.042	-0.042	0.115***	0.161***	1.000	
6.학력	0.042	0.031	0.137***	-0.123***	0.111***	1.000
7.소득	0.031	-0.033	0.065**	-0.023	0.157***	0.209***

주: * p<0.1, ** p<0.05, *** p<0.01

다중공선성을 검토하기 위해 분산팽창지수(VIF: Variance Inflation Factor)를 추정하였는데, 모형 I 을 기준으로 평균 VIF는 1.433으로 나타났다.¹⁾ 전체적으로 분석모형에 대한 다중공선성의 우려는 없는 것으로 나타났다.

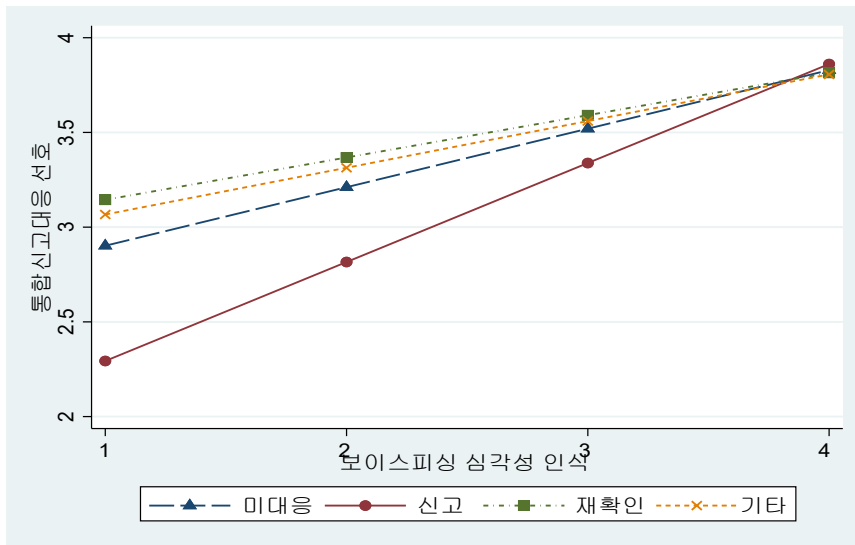
3) 다중회귀분석 결과

일반국민들의 보이스포싱 심각성 인식이 보이스포싱 통합신고·대응 선호에 미치는 영향을 분석하기 위한 모형 I 과, 보이스포싱 심각성 인식과 보이스포싱 통합신고·대응 선호 간의 관계를 보이스포싱 대처방법이 조절하는지를 분석하기 위한 모형 II와 같은 다중회귀모형을 설정하였다. 그 분석 결과는 <표 8>과 같다.

독립변수인 보이스포싱 심각성 인식은 모형 I 과 II 모두에서 보이스포싱 통합신고·대응 선호에 통계적으로 유의미한 양(+)의 영향을 나타냈다. 이는 보이스포싱을 더 심각하게 인식할수록 일반국민들이 통합신고·대응에 대한 선호도가 높아진다는 것을 의미한다. 이는 Roberts(1992) 및 Simpson et al.(2023)의 결과와 유사한 것으로 범주의 심각성 인식이 범죄대책 선호에 영향을 미친다는 것이다. 형사정책적인 맥락에서 보면, 정부나 관련 기관이 효과적인 대응 및 예방책을 마련하고 보이스포싱의 심각성을 공공에 인식시키는 노력은 일반국민들이 보이스포싱 통합신고·대응에 대한 긍정적인 태도를 갖게 하는 데 중요하다고 해석할 수 있다.

조절변수의 경우 모형 II에서 기준범주인 '경찰청 등에 신고'에 비해 '미대응', '사칭기관 등에 재확인', '기타' 모두가 보이스포싱 통합신고·대응에 대한 선호가 높은 것으로 나타났다. 이러한 결과로부터 기존 경찰청 등에 신고하는 것을 복잡하거나 어려운 것으로 인식하여 보다 손쉽고 간편한 다른 대응방법에 대한 선호도가 높은 것으로 추정할 수 있다.

〈그림 2〉 조절효과



1) 다중회귀모형에 상호작용항을 포함한 경우 다중공선성이 나타날 가능성이 높다. 이 경우 평균중심화(mean-centering)로 다중공선성을 줄일 수 있다는 주장과 이러한 작업이 무익하다는 주장이 존재한다(이학식, 2012: 58-59). 이와 같이 변수를 변환한 경우 다중공선성을 무시할 수 있다는 것이 일반적이다(Allison, 2012).

모형 II에서 보이스피싱 심각성 인식과 대처방법의 상호작용항의 경우 '미대응', '사칭기관 등에 재확인', '기타' 모두가 유의미한 음(-)의 영향을 미치는 것으로 나타났다. 이러한 결과는 긴장 대처방법에 관한 Botchkovar, Tittle과 Antonaccio(2013)의 연구와 유사한 것이다. 기존에 선택한 대처방법이 무엇인지에 따라 새로 발생한 긴장의 심각성과 후속 대책 간의 관계에 영향을 미치는 것과 같이, 보이스피싱에 대한 대처방법이 보이스피싱의 심각성 인식과 보이스피싱 통합신고·대응 선호의 관계에 영향을 미치는 것이다. 조절효과와 결과를 그림으로 나타내면 아래 <그림 2>와 같다. 그림과 같이, 보이스피싱 대처방법 중 기준범주인 '경찰청 등에 신고'는 보이스피싱 통합신고·대응 선호와 우상향하는 관계를 가지고 있으며 그 기울기가 비교적 가파른 것으로 나타났다. 즉 '경찰청 등에 신고'의 경우 보이스피싱 심각성 인식이 높아질수록 보이스피싱 통합신고·대응 선호가 높아지며 더 정도가 가파르게 증가하였다. 한편 보이스피싱 대처방법 중 '미대응', '사칭기관 등에 재확인', '기타' 등은 보이스피싱 통합신고·대응 선호와 우상향하는 관계를 가지고 있으나, 그 기울기는 상대적으로 완만하였다.

〈표 8〉 다중회귀분석 결과

구 분		모형 I	모형 II
		Coef. Std. Err.	Coef. Std. Err.
심각성(A)		0.309*** (0.027)	0.522*** (0.068)
대처 방법 (기준=신고)	무대응(B)	0.027 (0.040)	0.822*** (0.297)
	재확인(C)	0.034 (0.043)	1.150*** (0.334)
	기타(D)	0.028 (0.046)	1.049*** (0.330)
상호작용항	A×B		-0.213*** (0.079)
	A×C		-0.299*** (0.089)
	A×D		-0.276*** (0.089)
접근 매체 (기준=전화)	문자	0.055** (0.027)	0.054** (0.027)
	기타	0.036 (0.057)	0.038 (0.056)
본인 피해경험 (기준=없음)		0.075 (0.054)	0.074 (0.054)
친지 피해경험 (기준=없음)		-0.075** (0.034)	-0.077** (0.034)
정책관심도		0.136*** (0.020)	0.136*** (0.020)

구 분		모형 I	모형 II
		Coef. Std. Err.	Coef. Std. Err.
성별(기준=남성)		0.038 (0.027)	0.032 (0.027)
연 령		0.003** (0.001)	0.002** (0.001)
혼인상태 (기준=미혼)	기 혼	0.012 (0.038)	0.012 (0.037)
	기 타	-0.031 (0.082)	-0.036 (0.082)
경제활동 기간		1.691e-4 (0.007)	-0.001 (0.007)
학 령		0.038* (0.020)	0.038* (0.020)
소 득		-0.001 (0.006)	-0.001 (0.006)
절 편		1.884*** (0.136)	1.103*** (0.266)
관측치		1,208	1,208
F값		15.14***	13.56***
R^2 (Adjusted R^2)		0.169 (0.158)	0.178 (0.165)

주: * p<0.1, ** p<0.05, *** p<0.01

그리고 통제변수들 중 접근매체의 경우 모형 I 과 II 모두에서 기준범주인 '전화'에 비해 '문자'가 보이스피싱 통합신고·대응 선호에 통계적으로 유의미한 양(+)의 영향을 나타냈다. 이는 Simpson et al.(2023)이 주장한 바와 같이 범죄의 특성과 유형이 범죄대책 선호에 영향을 미치는 것이다. 이러한 결과로부터 문자 메시지를 통해 보이스피싱 시도를 받은 개인이 전화를 통해 보이스피싱 시도를 받은 개인에 비해 통합신고·대응에 대한 선호를 더 많이 표현한다는 것을 알 수 있다. 정책적 측면에서 이러한 결과는 보이스피싱을 퇴치하는 맥락에서 개인이 전화 통화보다는 문자 메시지를 통한 피싱 시도를 접할 때 통합신고·대응을 선호할 수 있음을 시사한다. 전화보다는 문자 메시지의 경우 내용을 읽고 이해하는 데 보다 긴 시간이 소요되고 그 과정에서 진위에 대한 판단이 어느 정도 가능해서 신고나 대응을 할 가능성이 높고, 가급적 원스톱으로 대응하기를 원하기 때문인 것으로 추정된다.

보이스피싱으로 인한 친지 피해경험이 있는 경우는 모형 I 과 II 모두에서 보이스피싱 통합신고·대응 선호에 통계적으로 유의미한 음(-)의 영향을 나타냈다. 즉 보이스피싱 피해를 입은 친지가 있는 경우 보이스피싱 통합신고·대응에 대한 선호도가 낮아졌다. 이러한 결과는 Nagin et al.(2006) 및 Galvin et al.(2018)의 연구결과와 일맥상통하는 것으로, 보이스피싱에 대한 개인적인 경험이 보이스피싱 대응정책에 대한 개인의 태도 및 선호도에 미치는 영향을 미칠 수 있다는 점을 보여준다.

보다 심도 있는 논의를 위해서는 부정적인 영향 뒤에 있는 이유에 대한 추가 조사를 통해 보이스피싱에 대응하는 개인의 의사결정 프로세스에 대한 더 깊은 통찰을 요구한다고 할 수 있다.

다음으로 정책관심도는 모형 I 과 II 모두에서 보이스피싱 통합신고·대응 선호에 통계적으로 유의미한 양(+)의 영향을 나타냈다. 즉 정책에 대한 적극적인 관심이 보이스피싱 통합신고·대응 선호에 긍정적인 영향을 미쳤다. 이러한 결과는 Pearson-Merkowitz와 Dyck(2017)의 연구와 동일한 것으로, 정책에 대한 대중의 인식과 관심이 높아지면 보이스피싱 통합신고·대응 선호가 높아지는 것과 관련이 있을 수 있음을 나타낸다. 추가적인 분석을 통해 개인의 공감을 불러일으키고 보이 피싱 사건에 대한 통합신고·대응 선호에 기여하는 정책 관심의 특정 측면을 탐색할 필요가 있다.

인구통계학적 변인 중 연령은 모형 I 과 II 모두에서 보이스피싱 통합신고·대응 선호에 통계적으로 유의미한 양(+)의 영향을 나타냈다. 이러한 결과는 Schwartz, Guo와 Kerbs(1993)의 결과와 동일한 것으로, 연령이 많아질수록 보이스피싱 통합신고·대응에 대한 선호가 증가하였다. 그리고 학력도 모형 I 과 II 모두에서 보이스피싱 통합신고·대응 선호에 통계적으로 유의미한 양(+)의 영향을 나타냈다. 이는 Weinrath, Young과 Kohm(2012)과 같은 결과로, 고학력일수록 보이스피싱 통합신고·대응에 대한 선호가 높았다.

III. 결론

본 연구에서는 보이스피싱 심각성 인식이 보이스피싱 통합신고·대응 선호에 미치는 효과 및 이들 간의 관계를 보이스피싱 대처방법이 조절하는지를 다중회귀모형으로 분석하였다. 분석결과, 보이스피싱 심각성 인식은 보이스피싱 통합신고·대응 선호에 긍정적인 영향을 미쳤다. 이는 정책적 맥락에서 보이스피싱 심각성 인식 캠페인은 보이스피싱 통합신고·대응에 대해 긍정적인 태도를 조성할 수 있다는 것을 의미한다. 또한 대처방법 중 기준범주인 '경찰청 등에 신고'에 '비대응', '사칭기관 등에 재확인', '기타'의 경우 보이스피싱 통합신고·대응을 더 선호하는 것으로 나타났다. 이러한 결과는 법집행기관에의 신고가 복잡하다는 인식으로 인한 것으로 추정된다.

한편 보이스피싱 심각성 인식과 대응방법 간의 상호작용항은 '미대응', '사칭기관 등에 재확인', '기타'에서 유의미한 음(-)의 영향을 보여 보이스피싱 심각성 인식과 보이스피싱 통합신고·대응 선호 간의 관계를 약화시키는 것으로 확인되었다. 즉, 보이스피싱 심각성 인식이 증가할수록 보이스피싱 통합신고·대응 선호가 증가하지만, 그 기울기는 '경찰청 등에 신고'에 비해 작은 것으로 나타났다.

접근매체의 경우 '문자'가 보이스피싱 통합신고·대응 선호에 양(+)의 영향을 미치는 것으로 나타나 문자메시지를 통해 보이스피싱 시도를 받은 개인은 전화로 당한 경우보다 보이스피싱 통합신고·대응을 더 선호하는 것으로 나타났다. 또한 친지가 보이스피싱 피해를 입은 경우 보이스피싱 통합신고·대응 선호에 음(-)의 영향을 미쳤다. 정책관심도는 보이스피싱 통합신고·대응 선호에

긍정적인 영향을 미쳤으며, 연령과 학력 모두 보이스피싱 통합신고·대응 선호에 긍정적 영향을 미치는 것으로 나타났다.

본 연구는 보이스피싱 예방과 통합신고·대응 활성화에 있어 여러 가지 정책적 시사점을 갖고 있으며 이를 제시하면 다음과 같다. 첫째, 교육과 캠페인 등을 통한 보이스피싱에 대한 인식 제고가 필요하다. 본 연구의 결과는 보이스피싱의 심각성에 대한 인식과 통합신고·대응에 대한 선호 사이의 긍정적인 인과관계를 있음을 보여준다. 이러한 관계를 활용하기 위해 정책 당국은 보이스피싱의 심각성을 강조하는 포괄적인 교육과 캠페인을 시작할 필요가 있다. 이러한 캠페인은 잠재적인 위험과 결과에 관한 정보를 전파하여 통합신고·대응 노력에 적극적으로 참여하기 위한 일반국민들의 이해와 동기를 높여줄 것이다. 보이스피싱 퇴치의 중요성에 대한 집단적 인식을 심어주기 위해서는 교육 계획, 지원 프로그램, 커뮤니케이션 전략에 대한 투자가 무엇보다 중요하다. 둘째, 신고채널의 다양화가 필요하다. 본 연구는 단순히 형사 및 수사기관에 신고하는 것 이상의 대응방법을 선호한다는 사실을 보여주며, 다양하고 접근 가능한 신고 채널이 필요함을 시사한다. 통합신고·대응센터의 설립을 옹호하는 동시에, 정책입안자들은 일반국민들을 위해 다양하고 편리한 신고 경로를 보장할 것을 제안한다. 보이스피싱 신고에 맞춰진 사용자 친화적인 온라인 플랫폼과 모바일 애플리케이션의 개발은 광범위하고 간편한 참여를 독려하는 데 중요한 역할을 할 것이다. 셋째, 인구통계학적 특성에 부합하는 전략을 마련할 필요가 있다. 통합신고·대응 선호에 대한 연령과 교육의 긍정적인 영향을 인식하여 정책 당국은 다양한 인구통계학적 특성에 맞게 공감할 수 있는 목표 전략을 수립하도록 해야 할 것이다. 특히 보이스피싱 취약계층에 해당하는 연령층 및 교육적 배경을 가진 사람들의 선호와 특성에 맞게 인식 캠페인을 맞춤화하는 것이 필수적이라고 할 수 있다. 이러한 맞춤형 접근 방식은 커뮤니케이션 노력의 효율성을 높여 보이스피싱에 대한 경각심을 다양한 계층의 사람들에게 전파되고 공감하도록 할 것이다.

그러나 본 연구는 다음과 같은 한계를 지니고 있다. 첫째, 보이스피싱 심각성에 대한 주관적 인식을 조사하였지만, 객관적인 심각성을 조사하지 못하였다는 점이다. 보이스피싱의 객관적 상황과 주관적 인식이 차이가 있을 수 있으므로, 추후 객관적 상황에 대한 조사를 통해 통합적 접근을 할 필요가 있다. 둘째, 본 연구는 자기기입식 설문 데이터에 근거하고 있으므로 사회적 소망성 편향 또는 회상 편향과 부정확성의 영향력을 완전히 배제하지 못하였다. 셋째, 보이스피싱 통합신고·대응과 관련된 대중의 태도와 선호에 영향을 미칠 수 있는 언론 보도, 정치적 수사, 기술 발전, 사이버범죄 수법의 진화 등 외부 영향을 광범위하게 포함하지 못한 한계가 있다. 이러한 문제로 누락변수 편이가 개입될 위험이 존재한다고 할 수 있다. 추후 연구에서는 보다 정교한 설문구성과 자료수집을 통해 추가적인 분석이 요구된다.

참고문헌

- 경찰청 수사국. (2016). 「보이스피싱, 누구도 예외일 수 없습니다」, 서울: 미래의 창.
- 고상근. (2023). 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 일부개정법률안 검토 보고. 국회 정부위원회.
- 곽대경. (2021). 보이스피싱의 실태와 대책에 관한 연구. 「형사사법연구」, 1(1): 9-52.
- 권한조 · 이재완. (2023). 보이스피싱 근절정책 선호에 관한 연구. 「한국사회와 행정연구」, 34(2): 257-278.
- 국무조정실. (2022). 보이스피싱 정부합수단 설치…신고·대응도 일원화 추진. 보도자료. 06.23.
- 국무조정실. (2023). 이제 보이스피싱 신고는 ‘112’로…피해구제까지 원스톱 처리. 보도자료. 09.27.
- 금융감독원. (2023). 알아두면 든든한 보이스피싱 대처법: 보이스피싱 예방을 위한 제도 및 대응 방법에 대한 종합 지침서. 보도자료. 6.23.
- 금융위원회. (2013). 전자금융사기 예방서비스 전면 시행. 보도자료. 09.26.
- 금융위원회. (2019). 정부, 전 국민에 ‘보이스피싱 경보’ 문자메시지 보낸다. 보도자료. 05.16.
- 금융위원회. (2020). 보이스피싱 뿌리 뽑는다…처벌 수준 높이고 금융사 배상책임 강화. 보도자료. 06.24.
- 기획재정부. (2021). ‘보이스피싱 차단’ 신형 메시지 도입…통합신고시스템도 구축. 보도자료. 12.02.
- 김대호·한지혜·장광호. (2023). 스마트치안을 통한 보이스피싱 피해구제 연구. 「한국경찰학연구」, 22(1): 27-52.
- 김덕용. (2018). 보이스피싱에 대한 경찰의 대응방안에 관한 연구. 「한국디지털콘텐츠학회 논문지」, 19(1): 193-198.
- 김세령·박정선(2021). 성향점수매칭 분석을 통한 청소년의 구체적 범죄두려움에 대한 설명요인 검증: 성별 및 학년별 중심으로. 「한국범죄학」, 15(3): 37-74.
- 김시윤 · 이범주 · 이용걸. (2022). 전기통신금융사기 대응 방안에 관한 연구: 보이스피싱 담당 경찰관의 관점으로. 「치안정책연구」, 36(1): 343-378.
- 단국대 산학협력단. (2013). 유선 및 인터넷 전화 단말에서 국제전화 알림 및 거부 방안 연구. 한국 인터넷진흥원. 연구보고서 KISA-WP-2013-0025.
- 마크로밀 엠브레인. (2022). 보이스피싱 범죄 정부합동수사단 출범 관련 여론조사 보고서.
- 박광섭·박행렬. (2007). 「범죄이론과 정책」, 대전: 충남대학교출판부.
- 방송통신위원회. (2009). ‘보이스피싱 예방’…국제전화 식별번호 표시 확대. 보도자료. 06.05.
- 방송통신위원회. (2011). 보이스피싱 피해신고 빨라진다. 보도자료. 07.20.
- 손현종 · 문광선. (2022). 자치경찰제에서 광역범죄 예방정책에 관한 연구: 보이스피싱 범죄분석 중심으로. 「한국경찰학연구」, 21(3): 77-100.
- 신성원. (2022). 보이스피싱의 실태 및 대응방안에 관한 연구. 「한국치안행정논집」, 19(4): 165-185.

- 윤해성·전영실·이정민·김계환. (2023). 「보이스피싱 범행단계별 대응방안 연구」, 한국형사법무정책연구원.
- 이기수. (2018). 최근 보이스피싱의 범죄수법 동향과 법적 대응방안. 「범죄수사연구」, 7: 3-19.
- 이동임. (2010). 보이스피싱범죄 대응 및 피해회복 방안. 「피해자학연구」, 18(2): 263-284.
- 이성식. (2006). 사이버범죄와 시민의 역할. 「정보화정책」, 13(3): 69-86.
- 이학식. (2012). 「사회과학을 연구할 위한 회귀분석」. 서울: 집현재.
- 이훈재. (2009). 보이스피싱의 피해실태 및 경찰의 대응방안에 관한 연구. 「피해자학연구」, 17(2): 217-244.
- 장주성. (2022). 금융소비자 보호를 위한 보이스피싱 대응방안 연구: 통신사, 제조사, 금융사, 플랫폼 사업자와의 협업을 통한 단계별 대응방안 제안. 「금융감독연구」, 9(1): 125-155.
- 정영호 · 하형준. (2022). 메신저피싱 범죄의 실태와 대응방안에 관한 연구. 「범죄수사연구」, 14: 31-54.
- 정웅. (2020). 보이스피싱 범죄추세와 수사 대응체제의 발전방향. 「한국공안행정학회보」, 81: 461-484.
- 정제용·염윤호. (2023). 보이스피싱 추세분석을 통한 문제점 파악과 대응방안 도출. 「범죄수사학연구」, 9(2): 153-175.
- 조호대. (2012). 보이스피싱 발생 및 대응방안. 「한국콘텐츠학회논문집」, 12(7): 176-182.
- 채문희 · 박찬혁. (2018). 전화금융사기 범죄에 대한 대응방안 연구. 「한국공안행정학회보」, 71: 417-448.
- 홍성삼. (2019). 피싱 사기범죄에 대한 인터폴 및 국가별 대응정책 비교연구. 「경찰학논총」, 14(1): 101-130.
- 황석진. (2021). 전기통신금융사기 근절을 위한 고찰: 보이스 피싱을 중심으로. 「경찰학연구」, 21(1): 91-123.
- 대한뉴스방송. 최근 5년간(2018~2023년 상반기) 보이스피싱 피해금액 1조7천499억원. 2023.09.29.
- 동아경제. 보이스피싱 5년새 1.7조 피해... "카톡 통해 최다". 2023.12.18.
- 부산일보. 조선족 어투 버린 금융사기 말쑥한 전문가로 돌아왔다. 2016.7.11.
- 아주경제. 보이스피싱 대면편취, 3년 새 8.6%→64.3%... "사전 예방, 신속 대응 필요". 2023.6.22.
- 연합뉴스. 국정원, 해외 보이스피싱 조직 36개 적발...3년간 183명 붙잡아. 2022.4.16.
- 중앙일보. 침착하게 건 112도 '가짜'...서울대 교수 10억 뜯어간 피싱 수법. 2023.11.01.
- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 3: 1-22.
- Allison, P. (2012). When Can You Safely Ignore Multicollinearity? (<http://statisticalhorizons.com/multicollinearity>). 검색일 2023.12.20.)
- Botchkovar, E. V., Tittle, C. R., & Antonaccio, O. (2013). Strain, coping, and socioeconomic

- status: Coping histories and present choices. *Journal of Quantitative Criminology*, 29: 217-250.
- Bowers, K. J., Johnson, S. D., & Hirschfield, A. (2004). The measurement of crime prevention intensity and its impact on levels of crime. *British Journal of Criminology*, 44(3): 419-440.
- Butter, R., Hermanns, J., & Menger, A. (2013). Simultaneous prediction of punitive and rehabilitation-oriented attitudes towards probation: An ecological approach. *Probation Journal*, 60(1): 24-39.
- Damodaram, R. (2016). Study on Phishing Attacks and Antiphishing Tools. *International Research Journal of Engineering and Technology*, 3(1): 700-705.
- Finamore, F., & Carlson, J. M. (1987). Religiosity, belief in a just world and crime control attitudes. *Psychological Reports*, 61(1): 135-138.
- Galvin, M. A., Loughran, T. A., Simpson, S. S., & Cohen, M. A. (2018). Victim compensation policy and white-collar crime: Public preferences in a national willingness-to-pay survey. *Criminology & Public Policy*, 17(3): 553-594.
- Grasmick, H. G., & McGill, A. L. (1994). Religion, attribution style, and punitiveness toward juvenile offenders. *Criminology*, 32(1): 23-46.
- Hartnagel, T. F., & Templeton, L. J. (2012). Emotions about crime and attitudes to punishment. *Punishment & Society*, 14(4): 452-474.
- Hogan, M. J., Chiricos, T., & Gertz, M. (2005). Economic insecurity, blame, and punitive attitudes. *Justice Quarterly*, 22(3): 392-412.
- Hough, M., & Moxon, D. (1985). Dealing with Offenders: Popular Opinion and the Views of Victims: Findings from the British Crime Survey. *The Howard Journal of Criminal Justice*, 24(3): 160-175.
- Langworthy, R. H., & Whitehead, J. T. (1986). Liberalism and fear as explanations of punitiveness. *Criminology*, 24(3): 575-591.
- Mattison, J., & Mirrlees-Black, C. (2000). Attitudes to crime and criminal justice: Findings from the 1998 British Crime Survey. London. HMSO.
- Michel, C., Heide, K., & Cochran, J. K. (2014). The Consequences of Knowledge About Elite Deviance. *American Journal of Criminal Justice*, 39(4): 1-24.
- Nagin, D. S., Piquero, A. R., Scott, E. S., & Steinberg, L. (2006). Public preferences for rehabilitation versus incarceration of juvenile offenders: Evidence from a contingent valuation survey. *Criminology & Public Policy*, 5(4): 627-651.
- O'Connell, M., & Whelan, A. (1996). Taking Wrongs Seriously Public Perceptions of Crime Seriousness. *British Journal of Criminology*, 36: 299-319.
- Pearson-Merkowitz, S., & Dyck, J. J. (2017). Crime and partisanship: How party ID muddles reality, perception, and policy attitudes on crime and guns. *Social Science Quarterly*,

98(2): 443-454.

- Roberts, J. V. (1992). Public opinion, crime, and criminal justice. *Crime and justice*, 16: 99-180.
- Samra-Grewal, J., & Roesch, R. (2000). The Parole Attitudes Scale (PAS): Development of a 15-item scale to assess attitudes toward conditional release. *Canadian Journal of Criminology*, 42(2): 157-175.
- Schwartz, I. M., Guo, S., & Kerbs, J. J. (1993). The impact of demographic variables on public opinion regarding juvenile justice: Implications for public policy. *Crime & Delinquency*, 39(1): 5-28.
- Selvan, K., & Vanitha, M. (2013). An Enhanced Countermeasure Technique for Deceptive Phishing Attack. *International Journal of Science and Research*, 4(9): 802-806.
- Simpson, S. S., Galvin, M. A., Loughran, T. A., & Cohen, M. A. (2023). Perceptions of white-collar crime seriousness: Unpacking and translating attitudes into policy preferences. *Journal of Research in Crime and Delinquency*, 60(5): 582-622.
- Toch, H., & Maguire, K. (2014). Public opinion regarding crime, criminal justice, and related topics: A retrospect. *Journal of Research in Crime and Delinquency*, 51(4): 424-444.
- Weinrath, M., Young, J., & Kohm, S. (2012). Attitudes toward the criminal justice system in a high crime Canadian community. *Canadian Journal of Urban Research*, 21(2): 112-131.

이재완(李在完): 서울대학교 행정대학원에서 행정학 박사학위(논문: 지방정부의 행정정보공개에 관한 연구, 2013)를 받고, 호서대학교 법경찰행정학과 교수로 재직 중이다. 주요 관심분야는 정보공개, 정책수단, 정책평가, 범죄정책 등이다. 주요 논문으로 “거주지역의 범죄위험 인식과 범죄예방 프로그램 선호에 관한 연구”(2022), “퇴직공무원의 전문성 활용 필요성과 취업제한 기간에 대한 선호”(2021) 등이 있다(noso791@gmail.com).

은종환(殷鍾煥): 서울대학교 행정대학원에서 정책학 박사학위를 받고, 경상국립대 행정학과에서 교수로 재직 중이다. 주요 관심분야는 디지털정부, 정책의사결정, 조직행태 등이다. 주요 저서로 “디지털플랫폼정부의 미래”(공저, 2024), 주요 논문으로 “공정성 인식과 직무스트레스 관계에 관한연구: 세대의 조절효과를 중심으로”(2022) 등이 있다(eunjh327@gnu.ac.kr)

Abstract

The Seriousness of Voice Phishing and Preference for Integrated Reporting and Response: Focusing on the Moderating Effect of Voice Phishing Response Methods

Lee, Jae-Wan
Eun, Jonghwan

This study sought to analyze how the severity of voice phishing affects the general public's preference for integrated reporting and response to voice phishing, and furthermore, to analyze whether voice phishing response methods moderate the relationship between them. To this end, this study analyzed it with a multiple regression model including an interaction term using data from the 'Public Opinion Survey on the Launch of the Government Joint Investigation Team for Voice Phishing Crime.' As a result of the analysis, the perception of the seriousness of voice phishing had a positive effect on the preference for integrated reporting and response to voice phishing. Among the response methods, the standard categories of 'report to the National Police Agency, etc.' were shown to be more preferred in the case of 'non-response', 'reconfirmation to impersonation agencies, etc.', and 'other'. Integrated reporting and response to voice phishing was preferred. The interaction term between response method and 'non-response', 'reconfirmation with imposter organizations, etc.', and 'other' showed a significant negative effect, weakening the relationship between voice phishing seriousness awareness and voice phishing integrated reporting/response preference. This study found that there is a need to emphasize the seriousness of voice phishing through education and promotional campaigns, and that a one-stop method such as an integrated reporting and response center is important, but it is also important to provide easy and convenient access for the general public. Please translate "This suggests that there is a need to develop user-friendly online platforms and mobile applications.

Key Words: Voice Phishing, Perception of Seriousness, Integrated Reporting and Response, Policy Preference, Response Method

