

방송통신정책연구

2020-0-01348

신종 보이스피싱 대응을 위한
정책적 · 기술적 방안 연구
A Study of Policy and Technical Measures
against Emerging Voice Phishing

김기범/권현영/박현민/송종화/문현지/윤상필/임지훈/현새롬

2020. 12

연구기관 : 성균관대학교



과학기술정보통신부



정보통신기획평가원

이 보고서는 2020년도 과학기술정보통신부 방송통신발전기금 방송통신정책연구사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 과학기술정보통신부의 공식입장과 다를 수 있습니다.

제 출 문

과학기술정보통신부 장관 귀하

본 보고서를 『신종 보이스피싱 대응을 위한 정책적·
기술적 방안 연구』의 연구결과보고서로 제출합니다.

2020년 12월

연구기관 : 성균관대학교

총괄책임자: 김기범(성균관대학교)

참여연구원: 권현영(고려대학교)

박현민(성균관대학교)

송종화(성균관대학교)

문현지(성균관대학교)

윤상필(고려대학교)

임지훈(고려대학교)

현새롬(고려대학교)

목 차

요약문	xii
제1장 서론	1
제2장 보이스피싱 범죄실태와 신종 유형의 등장	2
제1절 보이스피싱 개념과 특징	2
1. 보이스피싱 개념	2
2. 보이스피싱 유형	6
3. 보이스피싱 특징	9
4. 신종 보이스피싱 등장	12
제2절 보이스피싱 범죄 실태	14
1. 보이스피싱 범죄 현황	14
2. 보이스피싱 피해자 분석	14
3. 대포통장 적발 현황	18
4. 보이스피싱 2차 피해	20
5. COVID-19의 영향	22
제3절 신종 보이스피싱 등장	25
1. 대출사기형 보이스피싱	25
2. 공공기관 사칭형 보이스피싱	26
3. 지인사칭형 메신저 피싱	29
4. 소액결제 사기형 스미싱	31
제4절 미래 보이스피싱 예측	33
1. 딥페이크 기술을 활용한 보이스피싱	33

2. 심스와핑(SIM Swapping)을 통한 모바일 서비스 통제권 탈취	34
3. 스푸핑(Spoofing)을 활용한 사칭	35

제3장 신종 보이스피싱 범행수법과 대응기술 37

제1절 신종 보이스피싱 범죄조직	37
1. 범죄조직 구성 및 기능	37
2. 범죄조직의 언어(은어)	43
제2절 신종 보이스피싱 범행수법	53
1. 개괄	53
2. 선불 유심(USIM) 악용	55
3. IMEI 변조	56
4. 심박스(SIM Box)	58
5. 오토콜	63
6. 악성앱 운영	66
7. 자금세탁	68
제3절 신종 보이스피싱 대응기술	75
1. 개괄	75
2. 발신번호 변작 차단·탐지	76
3. 네트워크 패킷분석	78
4. 통신패턴분석	79
5. 심박스 전파탐지	81
6. 음성인식	85
7. 텍스트추출	89
8. 악성앱 탐지	91
9. 데이터 정보분석	96
제4절 소결	104

제4장 신종 보이스피싱 대응정책 및 평가 106

제1절 개괄	106
제2절 정부부처의 개별대책	116
1. 보이스피싱 10계명 발표 (2007년)	116
2. 외국인 예금계좌 개설시 신원확인 의무화 (2007년)	117
3. 발신번호 표시제도 도입 (2009년)	118
4. 보이스피싱 예방수칙 10계명 배포 (2009년)	119
5. 발신번호변작 방지대책반 구성 (2011년)	120
제3절 정부부처의 종합대책	122
1. 보이스피싱 피해방지 종합대책(2012년)	122
2. 신·변종 전기통신금융사기 피해방지 종합대책(2013년)	125
3. 전기통신금융사기 방지 종합대책(2018년)	128
4. 보이스피싱 척결 종합방안(2020년)	133
제4절 정책평가 및 시사점	147

제5장 신종 보이스피싱 법제 및 쟁점 149

제1절 신종 보이스피싱 법제 분석	149
1. 형법	149
2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률	153
3. 전기통신사업법	155
4. 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법	157
5. 통신비밀보호법	160
6. 범죄수익은닉의 규제 및 처벌 등에 관한 법률	161
7. 특정 금융거래정보의 보고 및 이용 등에 관한 법률	163
8. 전자금융거래법	165
9. 기타 법률	167

제2절 신종 보이스피싱 법제 개정안과 주요쟁점	171
1. 개정법률안 현황	171
2. 개정법률안 주요 내용	171
제3절 신종 보이스피싱 양형기준	176
1. 신종 보이스피싱 양형 실태	176
2. 형법상 사기죄 양형기준	177
3. 전자금융거래법위반 양형기준	179
제4절 법제분석 및 시사점	182

제6장 해외 신종 보이스피싱 대응체계 및 법제 185

제1절 미국의 대응체계 및 법제	185
1. 범죄 동향	185
2. 대응 체계	186
3. 대응 법률	195
제2절 독일의 대응체계 및 법제	227
1. 범죄 동향	227
2. 대응 체계	227
3. 대응 법률	239
제3절 일본의 대응체계 및 법제	253
1. 범죄 동향	253
2. 대응 체계	255
3. 대응 법률	263
4. 대응 정책	273
제4절 중국의 대응체계 및 법제	283
1. 범죄 동향	283
2. 대응 체계	284
3. 대응 법률	285

4. 대응 정책	287
제5절 비교분석 및 시사점	288
1. 미국	288
2. 독일	291
3. 일본	294
4. 중국	296

제7장 신종 보이스피싱 대응 정책적·기술적 개선 방안 298

제1절 입법적 개선방안	298
1. 해외 발신전화 차단에 대한 기술적 조치 의무화	298
2. 금융기관의 보이스피싱에 대한 배상책임 강화	299
3. 통신제한조치 대상에 전기통신금융사기죄 포함	300
4. 상습 전과자 신상정보 공개제도 도입	301
5. 전기통신금융사기 취득객체에 재물 포함	303
제2절 제도적 개선방안	305
1. 보이스피싱 음성·신원 제보자 포상금 확대	305
2. 보이스피싱 피해자 구제 활성화	308
3. 선불·알뜰폰 본인확인 절차 강화	309
4. 인터폴 적색수배에 범죄자 얼굴공개 추진	312
5. 국제기구 편당을 통한 아시아 지역의 수사작전 주도	313
6. 범죄단체조직죄 적용을 통한 강력한 처벌	314
제3절 기술적 개선방안	315
1. 보이스피싱 대응기술 프레임워크 설계	315
2. AI 기반 보이스피싱 음성 활용 연령대별 체험형 홍보활동 전개	316
3. 범죄자 음성 식별기술 및 피해자 감정인식 기술 개발	317
4. 금융기관 보이스피싱 FDS 구축 의무화	318
5. 4G 이용 심박스 탐지기술 개발	318

6. 범죄수익 추적 기술 개발	319
제8장 결론	321
참고문헌	323

표 목 차

<표 2-1> 신종금융사기의 각 행위단계별 적용법조 및 법정형	5
<표 2-2> 전통적인 보이스피싱 범죄의 주요 유형	7
<표 2-3> 최근 연도별 전화금융사기 피해 현황	14
<표 2-4> 유형별 보이스피싱 피해 현황	15
<표 2-5> 분기별 메신저피싱 피해 현황	16
<표 2-6> 연령별·성별 보이스피싱 피해 비율 현황	17
<표 2-7> 일반인 대비 피해 유형별 신용 등급 분포비율 현황	18
<표 2-8> 보이스피싱 관련 대포통장 적발 현황	19
<표 2-9> 대포통장 검거 현황	20
<표 2-10> 최근 메신저 피싱 피해현황	23
<표 3-1> 보이스피싱 총책 역할	39
<표 3-2> 보이스피싱 통장제공책 역할	41
<표 3-3> 보이스피싱 자금세탁책 역할	42
<표 3-4> 보이스피싱 은어 : 조직	44
<표 3-5> 보이스피싱 은어 : 금융	46
<표 3-6> 보이스피싱 은어 : 자금	49
<표 3-7> 보이스피싱 은어 : 범행수법 및 장소	49
<표 3-8> 보이스피싱 은어 : 범행수단	50
<표 3-9> 보이스피싱 은어 : 상태 및 기타	51
<표 3-10> 보이스피싱 범행수법	54
<표 3-11> IMEI 구조와 형식	57
<표 3-12> 보이스피싱 대응기술	75
<표 3-13> C&C 하드코딩 유형	92
<표 3-14> 전화 가로채기 코드 유형	93

<표 3-15> 암호화폐 종류별 블록체인 주소와 형태	101
<표 4-1> 정보보호진흥원, 전화금융사기(보이스피싱) 피해예방 10계명 (2007년)	116
<표 4-2> 지식경제부, 전화금융사기(보이스피싱) 피해예방 수칙 10계명 (2009년)	119
<표 4-3> 방송통신위원회, 보이스피싱 피해 예방을 위한	123
<표 4-4> 관계부처 합동, 전기통신금융사기 방지 종합대책(2018년)	130
<표 4-5> 디지털 경제의 신뢰 기반 조성을 위한 보이스피싱 척결 종합방안(2020년 6월)	134
<표 5-1> 최근 발의된 통신사기피해환급법 개정안의 주요 내용	171
<표 5-3> 사기범죄 양형기준(양형위원회) : 조직적 사기의 경우	177
<표 5-4> 전자금융거래법위반범죄 양형기준(양형위원회)	179
<표 5-2> 통신사기피해환급법 개정안 비교검토	182
<표 6-1> 미국의 신종 금융사기 관련 행위의 유형별 담당 집행기관	187
<표 6-2> 미국의 각 행정구역의 피싱 사기범죄 대응	193
<표 6-3> 독일 연방내무부 기관 구성	228
<표 6-4> 독일 BSI 부서 구성	233
<표 6-5> 독일 연방범죄수사국의 부서 체계	236
<표 6-6> 보이스피싱에 관한 일본 지자체의 단독 조례	258
<표 6-7> ‘특수사기’의 정의 (미에현 쿠와나시 조례 제2조)	260
<표 6-8> 생활안전 조례 개정을 통한 보이스피싱 범죄 대응	262
<표 6-9> 일본의 휴대전화 부정이용 방지법의 주요 내용	271
<표 7-1> 보이스피싱 대응기술 개요	316

그 립 목 차

[그림 2-1] 피해자가 실제로 받은 허위 서류	29
[그림 2-2] 피해사례의 실제 대화(왼), 피해자와 사기범 프로필(오)	30
[그림 3-1] 보이스피싱 조직단체 구성도	38
[그림 3-2] 보이스피싱 범행수법 개요도	53
[그림 3-3] USIM 없는 심박스(VoIP Gateway)	59
[그림 3-4] 차량 내부에 설치된 심박스	60
[그림 3-5] 심박스 사용 모듈	61
[그림 3-6] 심박스 부품	62
[그림 3-7] 오토콜 통화 흐름	64
[그림 3-8] 오토콜 발신번호 설정 및 관리	65
[그림 3-9] 자금세탁을 위한 면세점 대리구매 절차	71
[그림 3-10] 가상통화 환치기 흐름도	73
[그림 3-11] 심박스 패킷	79
[그림 3-12] i2 프로그램의 ELP 모델	97
[그림 3-13] i2 프로그램을 활용한 통화네트워크 분석화면	98
[그림 3-14] 구조적 등이성 원리 활용 분석 사례	98
[그림 3-15] 금융의심거래 정보분석 서비스	99
[그림 3-16] 비트코인 개별 거래(Transaction) 정보	102
[그림 4-1] 「보이스피싱 척결 종합방안」 중 부처별 주요 개선 내용	135
[그림 4-2] 보이스피싱 전기통신수단 신속 예방·차단 전략	136
[그림 4-3] AI, 빅데이터를 활용한 FDS 운영 시스템	139
[그림 6-1] 일본 송금사기구제법에 의한 금융기관의 구제 개요도	256
[그림 6-2] 일본의 AI 카메라 솔루션을 활용한 보이스피싱 대응	282

요 약 문

1. 제 목

- 신종 보이스피싱 대응을 위한 정책적·기술적 방안 연구

2. 연구 목적 및 필요성

- (목 적) 신종 보이스피싱의 현황, 대응 법제와 기술을 살펴보고, 해외 대응체계와 비교분석하여 정책적·기술적 대안 제시
- (필요성) 보이스피싱이 첨단기술과 결합하여 글로벌화·지능화·조직화되면서 피해가 확산, 정책적·기술적 대응방안에 대한 연구 시급

3. 연구의 구성 및 범위

- (2장) 보이스피싱 범죄실태와 신종 유형의 등장
 - 보이스피싱 개념 및 특징
 - 신종 보이스피싱 실태, 유형 및 전망
- (3장) 신종 보이스피싱 범행수법과 대응기술
 - 보이스피싱 범죄조직의 체계와 기능
 - 신종 보이스피싱 범행기술
 - 신종 보이스피싱 대응기술
- (4장) 신종 보이스피싱 대응정책 및 평가
 - 정부부처의 개별대책
 - 정부부처의 종합대책
- (5장) 신종 보이스피싱 법제 및 쟁점
 - 신종 보이스피싱 법제 분석

- 신종 보이스피싱 법제 개정안과 쟁점
- 신종 보이스피싱 양형기준
- (6장) 해외 신종 보이스피싱 대응체계 및 법제
 - 주요국(미국·독일·일본·중국)의 범죄동향
 - 주요국(미국·독일·일본·중국)의 대응체계
 - 주요국(미국·독일·일본·중국)의 대응법률
- (7장) 신종 보이스피싱 대응 정책적·기술적 개선방안
 - 신종 보이스피싱 대응을 위한 입법적 개선방안
 - 신종 보이스피싱 대응을 위한 제도적 개선방안
 - 신종 보이스피싱 대응을 위한 기술적 개선방안

4. 연구 내용 및 결과

- (입법적 개선방안) ① 해외 발신전화 차단에 대한 기술적 조치 의무화, ② 금융기관의 보이스피싱에 대한 배상책임 강화, ③ 통신제한조치 대상에 전기통신금융사기죄 포함, ④ 상습 전과자 신상정보 공개제도 도입, ⑤ 전기통신금융사기 취득객체에 재물 포함 등 제시
- (제도적 개선방안) ① 보이스피싱 음성·신원 제보자 포상금 확대, ② 보이스피싱 피해자 구제 활성화, ③ 선불·알뜰폰 본인확인 절차 강화, ④ 인터폴 적색수배에 범죄자 얼굴공개 추진, ⑤ 국제기구 편당을 통한 아시아 지역의 수사작전 주도, ⑥ 범죄단체조직죄 적용을 통한 강력한 처벌 등 제시
- (기술적 개선방안) ① 보이스피싱 대응기술 프레임워크 설계, ② AI기반 보이스피싱 음성 활용을 통한 연령대별 체험형 홍보활동 전개, ③ 범죄자 음성 식별기술 및 피해자 감정인식 기술 개발, ④ 금융기관 보이스피싱 FDS 구축 의무화, ⑤ 4G이용 심박스 탐지기술 개발, ⑥ 범죄수의 추적기술 개발 등 제시

5. 정책적 활용 내용

- (입법) 통신사기피해환급법 등 관련법률 개정에 필요한 기초자료로 활용
- (정책) 과학기술정보통신부, 금융위원회, 경찰청, 한국인터넷진흥원 등에서 보이스피싱 피해예방, 대응정책 및 범죄수사에 활용
- (기술) 보이스피싱 예방 및 대응을 위한 기술 유형화 및 향후 국가 연구 개발(R&D) 과제 제시

6. 기대효과

- 정부부처의 보이스피싱 피해 예방 및 대응역량 제고 기대
- 수사기관 및 대응기관(한국인터넷진흥원 등)의 단속역량 확대 기대
- 정부부처, 수사기관, 공공기관 및 민간의 보이스피싱에 대한 이해도 증진 및 새로운 법제 및 기술도입에 대한 공감대 확산 기대

SUMMARY

1. Title

- A Study of Policy and Technical Measures against Emerging Voice Phishing

2. Objectives and Importance of Research

- (Objectives)
 - Reviewing the current state, legislative responses, and technologies of emerging voice phishing
 - Suggesting policy and technical measures through comparative analysis between domestic and foreign responses
- (Importance)
 - Damage of voice phishing is increasing as they become more globalized, sophisticated, and organized combined with advanced technologies
 - There is an urgent need for research on policy and technical measures.

3. Contents and Scope of the Research

- (Chapter 2) Actual Situations of Voice Phishing and the Emerging Voice Phishing
 - Concept and Features of Voice Phishing
 - Current Status, Types, and Prospects of Emerging Voice Phishing
- (Chapter 3) Criminal Methods and Response Technologies of

Emerging Voice Phishing

- Criminal Organization and Functions of Emerging Voice Phishing
- Criminal Methods of Emerging Voice Phishing
- Response Technologies of Emerging Voice Phishing

○ (Chapter 4) Government Plan and Evaluation for Emerging Voice Phishing

- Individual Measures by Government Departments
- Comprehensive Measures by Government Departments

○ (Chapter 5) Legislation and Issues for Emerging Voice Phishing

- Analysis of Legislation for Emerging Voice Phishing
- Amendments and Issues of Legislation for Emerging Voice Phishing
- Sentencing Guidelines for Emerging Voice Phishing

○ (Chapter 6) Foreign Countries' Response System and Legislation for Emerging Voice Phishing

- Trends in Major Countries(USA, Germany, Japan, China)
- Response System in Major Countries(USA, Germany, Japan, China)
- Laws in Major Countries(USA, Germany, Japan, China)

○ (Chapter 7) Policy and Technical Measures against Emerging Voice Phishing

- Legislative Measures to Emerging Voice Phishing
- Institutional Measures to Emerging Voice Phishing
- Technical Measures to Emerging Voice Phishing

4. Results of the Research

- (Legislative Measures) We suggest ① to do mandatory technical

actions to block overseas outgoing calls, ② to strengthen the liability of financial institutions to compensate for voice phishing, ③ to add to telecommunications-based financial fraud to the target of communication-restricting measures, ④ to introduce a system to disclose personal information of habitual criminals, ⑤ to include properties to the concept of telecommunications-based financial fraud.

- (Institutional Improvement Plan) We suggest ① to increase rewards for reporting voice of criminals and information about criminals, ② to activate relief for victims of voice phishing, ③ to reinforce of prepaid and affordable phone identification procedures, ④ to promote disclosure of criminals' faces in Interpol Red Notice, ⑤ to lead investigations in Asia through funding with international organizations, ⑥ to strengthen punishment through the application of organization of criminal group crime(Criminal Code Article 114)

- (Technical Improvement Plan) ① to design response technology framework for emerging voice phishing, ② to progress experience-based promotion activities by age group through the use of AI-based voice phishing conversations, ③ to develop criminal voice identification technology and victim's emotion recognition technology, ④ to mandate financial institutions to establish FDS for voice phishing, ⑤ to develop SIM Box detection technology using 4G, ⑥ to develop criminal proceeds tracking technology

5. Policy Suggestions for Practical Use

- (Legislation) Basic data for revision of relevant acts such as Special Act

on the prevention of loss caused by telecommunications-based financial fraud and refund for loss.

- (Policy) Prevention, measures and criminal investigations by the Ministry of Science and ICT, the Financial Services Commission, the National Police Agency, and the Korea Internet & Security Agency.
- (Technology) technical typology of New voice phishing and national R&D projects.

6. Expectations

- Enhancement on prevention and response capabilities of government ministries.
- Expansion of the regulatory capabilities of investigative and response agencies(such as the Korea Internet & Security Agency).
- Increased understanding on voice phishing and consensus on the need for introduction of new legislation and technology among government ministries, investigative agencies, public institutions and the private sectors.

제1장 서론

보이스피싱은 2000년대 중반에 등장한 이래 꾸준히 지능화되면서 피해가 계속되고 있다. 범행수법도 전화 방식에서 악성앱을 포함하는 방식으로 바뀌고, 계좌이체형에서 대면편취형·침입절도형으로 교묘해지고 있다. 기술적으로 URL을 통한 원격 악성코드 유포, 심박스를 활용한 전화번호 변작, 악성앱 설치, 자금세탁에서 암호화폐의 활용 등으로 치밀해지고 있다. 그간 정부는 관련부처가 참여하여 4차례에 걸쳐 종합대책을 수립하여 다양한 대책을 강구하였으나 보이스피싱을 근절하기에는 역부족인 것으로 보인다.

따라서 본 연구는 최근에 등장한 신종 보이스피싱의 유형을 살펴보고, 이를 근절하기 위한 제도적·기술적 개선방안을 모색하고자 한다. 제2장에서는 보이스피싱의 개념과 범죄실태 그리고 신종 보이스피싱의 유형을 살펴본다. 향후에는 어떠한 신종 보이스피싱이 등장할 것인지도 전망하고자 한다. 제3장에서는 보이스피싱 범행수법과 대응기술을 분석한다. 이를 위해 보이스피싱 조직 체계와 역할을 조사하고, 범죄자들의 은어도 수집하고자 한다. 범행수법을 유형화하고, 이에 맞는 대응기술을 도출하여 기술의 수준을 진단하고자 한다. 제4장에서는 신종 보이스피싱에 대한 그간의 정부 정책을 분석하여 긍정적·부정적 평가를 한다. 제5장에서는 신종 보이스피싱에 대한 법률과 쟁점을 분석한다. 보이스피싱과 관련 있는 통신사기피해환급법, 정보통신망법, 전기통신사업법 등 총 11개의 법률을 검토하고 현재 국회에 계류 중인 통신사기피해환급법 관련 5개 법률안도 비교하고자 한다. 제6장에서는 해외 신종 보이스피싱 대응체계 및 법제를 살펴본다. 특히, 미국, 독일, 일본, 중국의 범죄동향, 대응체계, 대응법률 및 추진정책을 조사하여 시사점을 도출하고자 한다. 마지막으로 제7장에서는 신종 보이스피싱 대응을 위한 정책적·기술적 대응방안을 제시한다.

제2장 보이스피싱 범죄실태와 신종 유형의 등장

제1절 보이스피싱 개념과 특징

1. 보이스피싱 개념

보이스피싱(voice phishing)이란 ‘목소리를 통하여 개인정보를 낚아 올린다’는 의미로, 음성이라는 뜻의 ‘보이스(voice)’와 기망행위로 타인의 재산을 편취하는 범죄라는 ‘피싱(phishing)’이 결합된 용어를 말한다.¹⁾ 목소리를 통하여 개인정보를 낚아 올린다’라는 의미에서 만들어졌다.²⁾ 피싱(phishing)은 1990년대 중반 해커들이 AOL 사용자들의 전화를 이용하여 불법적으로 개인정보 또는 금융정보를 빼내어 범죄에 사용하는 행위 즉, “피해자를 기망하여 피해자의 금융 관련 개인정보를 빼내고 이를 이용해 피해자의 계좌에서 일정 금액을 인출하는 행위”를 의미한다.³⁾⁴⁾

-
- 1) 김덕용, “보이스피싱에 대한 경찰의 대응방안에 관한 연구”, 한국디지털콘텐츠학회, 한국디지털콘텐츠학회논문지 19(1), 2018, 193면
 - 2) 이용훈, “보이스피싱의 행위별 죄책에 관한 형법적 연구”, 단국대학교 대학원 석사학위 논문, 2020, 5면
 - 3) 피싱(Phishing)의 어원은 ‘fishing’에서 ‘f’를 해커들의 철자법인 ‘ph’로 표기한 것으로, 원격 통신 시스템 해킹을 의미하는 프리킹(Phreaking)에서 영향을 받은 것으로 추정된다. CSO (2020.9.4.), “What is phishing? How this cyber attack works and how to prevent it”, <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html> (2020.10.23. 최종확인)
 - 4) 임석순, “피싱(phishing)에 대한 형법적 이해와 새로운 구성요건 창설의 필요성”, 안암법학회, 안암법학 48, 2015, 94면

보이스피싱은 기관마다 개념 정의를 달리하고 있지만 전체적인 맥락은 유사하다고 볼 수 있다. 경찰청은 전화를 이용하여 피해자에게 검찰, 경찰 등 형사사법기관을 사칭하는 방법으로 개인정보를 악용하여 비밀번호 등 개인 금융정보를 빼내거나, 돈을 인출하여 송금하도록 유도하거나 환급 등을 명목으로 송금을 받아 가로채는 사기 범죄라고 규정한다.⁵⁾ 한국인터넷진흥원은 피해자에게 전화를 걸어 공공기관, 금융기관, 수사기관, 지인 등을 사칭해 세금환급, 카드대금 연체, 출석요구, 거짓 납치사고 등을 빌미로 송금을 요구하거나 개인정보 및 금융정보를 탈취하는 수법으로 정의하고 있다.⁶⁾ 금융감독원은 피해자에게 전화를 걸어 공공기관 등을 사칭해 세금환급, 연체 및 법원 미출석 등을 빌미로 계좌 보호조치가 필요하다는 등, 은행 자동지급기로 유인해 현금을 편취하는 등 ‘기망행위로 타인의 재산을 편취하는 사기범죄’를 의미한다.⁷⁾ 최근에는 전기통신수단을 이용한 비대면 거래 방식으로 금융분야에서 발생하는 일종의 특수사기 범죄로 정의하고 있다.⁸⁾

정보통신기술의 발달과 함께 보이스피싱의 개념도 변화하고 있다. 유·무선·인터넷 전화 등 통신매체를 이용하여 피해자를 기망한 후, 금원을 제공하도록 유도하여 편취하는 금융사기 수법이라는 개념⁹⁾에서 전화를 이용하여 피해자로부터 금융정보를 취득한 후 범죄자가 금융거래를 시도하여 금원을 편취하는 개념으로 확대되고 있다.¹⁰⁾ 나아가 가짜 웹페이지로 접속을 유도하여 피해자의 계정 정보

5) 윤해성, 곽대경, “보이스피싱의 예방과 대책마련을 위한 연구”, 한국형사정책연구원, 형사정책연구원 연구총서 9(15), 2009, 20면

6) 한국정보보호진흥원 보도자료, “정보통신업계, 전화금융사기 예방 발벗고 나선다!”, 2007.8.1.자

7) 금융감독원 보도자료, “전화금융사기 예방대책 이행실태 점검 및 대국민 홍보 강화”, 2007.4.25.자

8) 금융감독원 홈페이지, 피싱사기 개요 中 피싱사기 정의, <http://phishing-keeper.fss.or.kr/fss/vstop/guide/define.jsp> (2020.10.23. 최종확인)

9) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서 16, 2016, 89면

를 취득하거나 금전을 편취하는 파밍(pharming), 스마트폰에 악성 프로그램을 유포하여 계정정보를 취득하거나 소액결제를 유도하는 스미싱(smishing) 등으로 확대되고 있다.¹¹⁾ 이와 연결하여 이메일해킹 무역사기(Business E-mail Compromise), 랜섬웨어(Ransomware), 섹스토션(Sextortion, 일명 “몸캠피싱”) 범죄까지 발생하고 있다.¹²⁾

영미권에서는 2005년 옥스퍼드 영어사전의 표제어로 ‘phishing’ 이 등재된 이후 일반적으로 피싱이라는 용어를 사용하지만, 우리나라에서는 공공기관이나 일반인을 나누지 않고 보이스피싱이라는 용어를 사용하고 있다.¹³⁾ 이렇게 볼 때 일반적으로 보이스피싱은 넓은 의미에서 기술적 수단을 활용하여 개인정보나 금융정보를 탈취한 후 피해자의 계좌에서 인출하여 재물 또는 재산상 이익을 편취하는 일련의 행위라고 정의할 수 있을 것이다.

초창기에 보이스피싱은 형법상 사기, 공갈, 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 “정보통신망법” 이라 함) 등 다양한 법률에서 규율하였다. 보이스피싱의 형태가 다양해서 어떠한 법률로든 처벌 자체는 가능했다.¹⁴⁾ 하지만 보이스피싱이 갖는 불법성을 표현하는데 한계가 있었고, 전국적으

10) 이 개념에서 보이스피싱은 단순히 현금을 이체 내지 송금하거나 소액을 결제하도록 하는 방식을 벗어나, 피해자를 현금자동지급기 또는 자동입출금기 등으로 유인하여 피해자 계좌에 예치된 금원을 자발적으로 이체하도록 하는 방식도 사용된다. 김동민, “접근매체를 이용하는 전자금융사기의 범위에 관한 소고”, 충남대학교 법학연구소, 법학연구 31(2), 2020, 54면

11) 윤해성, 곽대경, “보이스피싱의 예방과 대책마련을 위한 연구”, 한국형사정책연구원, 형사정책연구원 연구총서 09(15), 2009, 19-20면

12) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구 : 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서 16, 2016, 85면

13) 임석순, “피싱(phishing)에 대한 형법적 이해와 새로운 구성요건 창설의 필요성”, 안암법학회, 안암법학 48, 2016, 95면

14) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한

로 범집행이 통일적으로 이루어지지 않은 문제가 발생하였다.

〈표 2-1〉 신종금융사기의 각 행위단계별 적용법조 및 법정형

행위단계	적용법률	구성요건	법정형 (자유형)
범죄 단체조직	형법	범죄단체조직	목적에 정한 형
개인정보 수집 및 거래	형법	비밀침해	3년 이하
	정보통신망법	정보통신망 침해/비밀침해	5년 이하
		서비스제공자의 개인정보 무단 사용	5년 이하
		속이는 행위에 의한 개인정보 수집	5년 이하
	개인정보보호법	개인정보 부정취득, 제공, 교사, 알선	10년 이하
		정보처리자의 개인정보 무단제공	5년 이하
	정보통신기반보 호법	주요정보통신기반시설 침해	10년 이하
거짓 메일 발송, 거짓 웹사이트 개설	형법	사전자기록 위작/변작	5년 이하
	저작권법	컴퓨터 프로그램 저작권 침해	5년 이하
	상표법	상표권 침해	7년 이하
악성코드 제작, 배포, 발송	형법	컴퓨터 업무방해	5년 이하
	정보통신망법	악성 프로그램 유포	7년 이하
금 융 정 보 사취및이용	정보통신망법	비밀침해	5년 이하
	전자금융거래법	전자금융기반시설 불법 접근	10년 이하
	통 신 사 기 피 해 환급법	전기통신금융사기	10년 이하
이익의 취득	형법	컴퓨터 등 사용사기, 공갈	10년 이하
자금 세탁	범죄수익규제법	범죄수익 등 은닉 및 가장	5년 이하

국형사정책연구원, 형사정책연구원 연구총서 16, 2016, 222-223면

대 포 통 장 모 집	금융실명법	실명거래 위반	5년 이하
	전자금융거래법	접근매체 양도/대여	5년 이하
대포폰 수집/모집	전기통신사업법	전기통신역무 제공	1년 이하

(출처: 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원 연구총서 16, 2016, 222면)

이와 같은 문제를 해결하기 위해 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」(이하 “통신사기피해환급법”이라 함)을 제정하고, 전기통신금융사기라는 용어를 신설하였다. 즉, 통신사기피해환급법에서는 전기통신을 이용하여 타인을 기망(欺罔)·공갈(恐喝) 함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 행위(자금을 송금·이체하도록 하는 행위, 개인정보를 알아내어 지금을 송금·이체하는 행위)라고 정의하였다.(제2조 제2호) 다만, 재화의 공급 또는 용역의 제공 등을 가장한 행위는 제외하고, 대출의 제공·알선·중개를 가장한 행위는 포함하도록 하였다.(제2조 제2호) 통신사기피해환급법에서 정의하는 전기통신금융사기는 모든 통신수단을 포괄하여 그 범위가 넓고, 이용할 수 있는 범죄 수단이나 수법도 다양하다는 점에서 보이스피싱의 다양한 양태를 포괄할 수 있다. 하지만, 새로운 형태의 범죄가 등장하면서 구성요건에 대해서 지속적으로 개정을 해야 하는 상황이 발생하고 있다.

2. 보이스피싱 유형

보이스피싱은 초기에 국세청 등 공공기관에서 세금을 환급해준다고 피해자를 현금지급기로 유도하여 계좌이체 하도록 하는 수법을 활용하였고,¹⁵⁾ 이후 대학

15) 김동민, “접근매체를 이용하는 전자금융사기의 범위에 관한 소고”, 충남대학교 법학연구소, 법학연구 31(2), 2020, 55-56면

등록금 환급이나 경품행사에 당첨되었다는 등의 다양한 형태로 진화하였다.¹⁶⁾ 사전에 피해자의 개인정보를 입수하여 활용하거나, 휴대전화 문자메시지를 대량으로 발송한 후 통화가 연결되면 신용카드를 제3자가 불법으로 사용하였다고 속이는 등 수법과 화법도 다양해졌다. 주말이나 휴무일에 범행하여 은행이나 공공기관 등이 사실관계를 확인하지 못하도록 하였다.¹⁷⁾ 이와 같은 형태를 종합하여 전통적인 보이스피싱의 유형을 정리하면 다음과 같다.

〈표 2-2〉 전통적인 보이스피싱 범죄의 주요 유형

주요 유형	주요 수법
자녀 납치 및 사고를 빙자하여 편취	범행 전에 부모와 자녀의 연락처를 확보한 범인이 부모에게 변조한 자녀의 전화번호로 연락하여 납치나 사고를 당했다는 방식으로 기망하여 계좌이체 등으로 편취
메신저에서 지인을 사칭하여 송금 요구	해킹한 메신저 아이디 등 계정정보에 등록된 피해자의 지인과 메신저로 대화하여 교통사고 등 급하게 돈이 필요하다고 속여서 편취
인터넷 뱅킹을 이용하여 카드로 대금 및 예금 등 편취	피해자가 범죄사건으로 수사받고 있다는 등으로 속여 피싱사이트에 접속하게 한 후, 입력한 정보로 알아낸 피해자의 금융거래 관련 정보를 이용하여 범죄자가 직접 피해자 명의로 대출을 받은 후 금원을 편취
금융회사, 금감원 명의의 허위 긴급공지 문자메시지로 기망, 피싱 사이트로 유도하여 예금 등 편취	은행의 보안등급 향상 등 피싱사이트 링크가 포함된 문자를 발송한 후 피해자가 피싱사이트에 접속하여 입력한 금융거래 관련 정보로 범죄자가 피해자 명의 계좌에 있는 금원을 이체하거나 대출하는 방법으로 편취

16) 윤해성, 곽대경, “보이스피싱의 예방과 대책마련을 위한 연구”, 한국형사정책연구원, 형사정책연구원 연구총서 9(15), 2009, 21면

17) 금융감독원 보도자료, “전화금융사기 예방대책 이행실태 점검 및 대국민 홍보 강화”, 2007.4.25.자

주요 유형	주요 수법
전화통화를 통해 텔레뱅킹 이용정보를 알아내어 금전 편취	고령 피해자를 대상으로 전화하여 피해자 명의 계좌가 범죄에 악용되었다는 등으로 현혹하여 개인정보 및 금융 거래 관련 보안정보를 알아낸 후 피해자 명의 계좌에 있는 금원을 이체하거나 대출하는 방법으로 편취
피해자를 기망하여 자동화기기로 유인 편취	경찰·검찰을 사칭한 범죄자가 피해자에게 전화하여 계좌 등이 범죄에 악용되어 조치가 필요하다는 등으로 속여 범죄자의 계좌로 금원을 이체하게 하거나, 금융기관 직원이 개인정보를 유출하였다고 속여 자동화 기기에서 피해자가 범죄자의 계좌로 금원을 이체하는 방법으로 편취
피해자를 기망하여 피해자에게 자금을 이체토록 하여 편취	경찰·검찰을 사칭하여 수사를 위해 계좌 거래내역을 확인 해야 한다는 등의 이유로 범죄자의 계좌에 이체하게 하 거나, 국세청 직원을 사칭하여 미납 세금을 납부하라고 속여 범죄자의 계좌로 금원을 이체하는 방법으로 편취
신용카드정보 취득 후 ARS를 이용한 카드론 대금 편취	피해자 신용카드 정보를 범죄자가 확보하여 대출을 받은 후 피해자에게 범죄자금의 입금되었다고 속여 다시 범죄자의 계좌로 이체하는 방법으로 편취
기관사칭 상황극 연출에 의한 피해자 기망 편취	피해자에게 경찰 또는 검찰의 수사상황을 들리도록 상황을 연출하여 피해자를 기망한 후, 범죄에 악용된 피해자의 금융정보 확인을 위해 필요하다는 범죄자의 계좌로 자금을 이체하도록 한 후 편취
물품대금 오류송금 빙자로 피해자를 기망하여 편취	피해자에게 물품대금 등 허위 계좌 입금 문자를 발송한 후, 잘못 송금한 금원의 반환을 요구하여 편취

(출처: 이승용, 이주락, “빅데이터와 FDS를 활용한 보이스피싱 피해 예측 방법 연구”,
시큐리티연구 62, 2020, 190-191면)

3. 보이스피싱 특징

가. 초국가성

보이스피싱은 기존의 금융사기 범죄수법에 다양한 형태의 인적·기술적 요소가 결합된 범죄로 초국가성, 조직범죄화, 지능화, 비대칭성의 특징을 갖는다.¹⁸⁾ 먼저 특정 지역과 국가에 한정하여 발생하지 않기 때문에 초국가성을 갖는다. 이 때문에 초국가성을 국제범죄성라고 표현하기도 한다.¹⁹⁾²⁰⁾ 국내에서 발생한 보이스피싱은 대부분 중국이나 필리핀 등 해외에 서버를 구축하고, 우리나라에 거주하는 피해자를 상대로 범행하며 그 범죄수익을 자금세탁하여 다시 국외로 반출하고 있다.²¹⁾ 범죄조직이 중국 현지에서 한국어를 유창하게 사용할 수 있는 조선족을 고용하기도 한다. 이와 관련하여 국제전화가 이루어지는 경로가 복잡하고 다양하여 수사기관이 추적하는데 어려움이 있고, 추적된다 하더라도 해당 국가에서 수사에 협조하지 않으면 검거에 한계가 있다.

18) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서 16, 2016, 86면

19) 「국제범죄대책협의회 규정」(국무총리훈령 제640호)은 제2조에서 국제범죄를 ‘우리나라 국민이 국외에서 저지르거나 외국인의 국내범죄 및 우리나라 국민을 상대로 한 범죄, 국가 간 공조가 필요한 국제질서 법익침해사건’이라고 정의한다. 보이스피싱은 외국인 또는 외국에서 우리나라 국민 또는 우리나라에 거주하는 사람을 대상으로 하는 범죄로, 국가 간 공조가 필요불가결하며, 국제범죄의 특징인 조직범죄로서의 성격을 충분히 갖추고 있다. 정육상, “국제범죄의 새로운 양상과 그 대응방안”, 한국범죄심리학회, 한국범죄심리연구 7(1), 2011, 159-160면

20) 김도윤, “한·중 전기통신금융사기범죄 및 관련 제도의 현황과 시사점”, 한중법학회, 중국법연구 41, 2020, 164면

21) 경향신문 보도 (2014.4.10.), “[개인정보 유출 2차 피해] 피싱 조직 대부분 해외에 서버... 경찰 수사 한계”,
http://m.khan.co.kr/amp/view.html?art_id=201404102217205 (2020.12.13. 최종확인)

나. 조직범죄화

보이스피싱은 초기에는 작은 규모로 시작하였지만 이제는 거대한 조직범죄의 형태를 갖추고 있다. 범죄조직은 총책(주범)을 중심으로 프로그램 개발·제작·유포, 대포통장 모집·공급, 현금 인출·송금, 시스템 운영 등을 담당하는 하부조직으로 나뉘고, 이를 관리하는 간부급 중간조직원까지 두어 형법상 범죄단체의 수준에 이르렀다.²²⁾ 최근에는 보이스피싱, 피싱, 파밍 등 개별적 범죄가 대출사기, 조건만남사기, 섹스토션 등 높은 범죄수익을 가져오는 다양한 범죄와 융합되는 형태를 보이고, 범죄조직의 규모도 기업형으로 변화하고 있다.²³⁾ 범죄자들이 프로그램 개발을 외주형태로 맡겨서 납품을 받는 경우까지 등장하고 있다. 보이스피싱이 조직범죄화되어 수사기관이 주범을 검거하지 못하고 하부조직원만 검거할 경우 주범은 하부조직원을 바꾸면서 계속 범행을 할 수 있어 관련범죄를 근절하기 어려워진다. 소수 혹은 단독 관리자를 중심으로 점조직으로 운영되면서 조직원 간에 서로의 직책이나 직위를 알지 못하는 경우도 많아지고 있다.²⁴⁾ 이처럼 예비·음모 단계부터 기수에 이르기까지 체계적이고 조직적인 편취행위가 이루어지고, 비대면 형태로 프로그램을 이용하면서 죄책감을 감쇄시키는 결과를 가져오고 있다.²⁵⁾

다. 지능화

-
- 22) 서울서부지방법원 2015. 5. 1. 선고 2015노331 판결; 박찬걸, “전기통신금융사기 관련 범죄의 가별성 검토”, 홍익대학교 법학연구소, 홍익법학 21(3), 2020, 372면
- 23) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서 16, 2016, 86면
- 24) 윤해성, 곽대경, “보이스피싱의 예방과 대책마련을 위한 연구”, 한국형사정책연구원, 형사정책연구원 연구총서 09(15), 2009, 28-29면
- 25) 김도윤, “한·중 전기통신금융사기범죄 및 관련 제도의 현황과 시사점”, 한중법학회, 중국법연구 41, 2020, 165면

보이스피싱은 범죄를 계획하고 실행하는 범죄조직이 피해자에게 전화를 걸거나 SMS 등을 보내어 확보한 다른 통장으로 계좌이체를 유도하는 방식은 유사하지만,²⁶⁾ 실행 과정에서 다양한 수법이 등장하면서 지능화되고 있다. 사칭하는 기관은 주기적으로 변경하고, 새로운 모델을 만들어 내며, 시기나 상황을 고려하기도 한다.²⁷⁾ 현금지급기 조작 화면을 영어로 선택하게 하거나, 계좌이체 후에 거래명세표를 파기하라고 지시하는 등 피해사실을 인지하더라도 신고할 수 없거나 수사를 지연시킬 수 있는 다양한 방법을 만들고 있다.²⁸⁾ 이 때문에 보이스피싱에 대한 대책을 만들면 범죄자가 수법을 변경하거나 허점을 노려 정부의 대책을 다시 무력화시키는 현상이 반복되고 있다.²⁹⁾ 범죄자들은 복잡한 정보통신 기술과 금융결제 방식의 취약점을 찾아내거나 여기에 악성 프로그램을 설치하고 있다. 정보보안 업체나 수사기관이 악성 프로그램을 탐지하면 바로 변종 악성 프로그램을 개발하여 유포한다. 금융기관이 범행계좌를 파악하여 지급정지하려 해도 짧은 시간 내에 수많은 금융계좌로 분산 이체하여 빠져 나간다. 환치기 수법, 게임 아이템 구매, 비트코인 환전의 방법으로 범죄수익을 세탁하여 인출하기도 한다.

라. 비대칭성

26) 차영민, 송영시, “보이스피싱 범죄의 실태와 피해자의 손해보전 방법에 관한 소고”, 조선대학교 법학연구원, 법학논총 21(2), 2014, 537면

27) 특정 기관을 사칭하는 수법은 지속해서 사칭기관이 다양하게 변화한다. 기존 우체국, 검찰, 국세청 등 기관을 사칭하던 보이스피싱 범죄 수법이 일반시민들에게 많이 알려지자 최근에는 성매매를 미끼로 한 신종 보이스피싱범죄까지 발생하고 있다. 윤해성, 곽대경, “보이스피싱의 예방과 대책마련을 위한 연구”, 한국형사정책연구원, 형사정책연구원 연구총서 9(15), 2009, 29면

28) 윤해성, 곽대경, “보이스피싱의 예방과 대책마련을 위한 연구”, 한국형사정책연구원, 형사정책연구원 연구총서 9(15), 2009, 29-30면

29) 이기수, “최근 보이스피싱의 범죄수법 동향과 법적 대응방안”, 경찰대학 수사과학연구원, 범죄수사학연구 4(2), 2018, 3-17면

보이스피싱은 범죄자가 범행 주도를 위한 다양한 정보를 가지고 있는 반면, 피해자는 범죄자에 이끌려가기 때문에 상대적으로 정보가 없어 비대칭성이 발생한다. 피해자는 금융이나 행정에 대한 지식과 정보가 부족할 수밖에 없고, 개인정보가 유출되었다고 하면 범죄자가 어디까지 알고 있는지 두려워할 수밖에 없다. 전자는 금융기관 사칭이 대표적인 사례이다. 일반 소비자는 금융회사의 대출이나 금융정책 정보, 이와 관련한 보안정책 등에 취약할 수밖에 없다. 다양한 교육과 홍보를 통해서 어느 정도 해소할 수 있겠으나 범죄가 순식간에 발생하고, 그렇더라도 사회적 약자나 노인들에게는 한계가 발생할 수밖에 없다. 보이스피싱이 서민층에 집중되는 이유이기도 하다.³⁰⁾ 후자는 개인정보 유출이 대표적인 사례이다. 피해자의 대학지원서, 카드정보, 가족 및 인적사항 등 신상정보가 불법으로 거래되고 있기 때문에 이러한 현상이 발생하는 것이다.

4. 신종 보이스피싱 등장

2008년에 악성 프로그램을 이용하여 피싱사이트로 접속을 유도한 후 금원을 편취하는 파밍(pharming)이 발생하였고, 2011년에 악성 프로그램이 포함된 링크를 스마트폰에 발송하여 피해자의 금융정보를 탈취한 후 금원을 편취하는 스미싱(smishing)이 등장하였다.³¹⁾ 나아가 메신저 피싱이나 불법금융사이트 또는 스마트폰 앱을 이용하거나 간편송금 제도와 결합한 보이스피싱이 등장하기도 하였다.³²⁾ 2013년에는 피해자에 대한 기망행위가 없는 상태에서 악성앱 또는 악성코드로 피해자의 컴퓨터나 휴대전화를 감염시켜 금원을 편취하는 메모리해킹(memory

30) 윤해성, 곽대경, “보이스피싱의 예방과 대책마련을 위한 연구”, 한국형사정책연구원, 형사정책연구원 연구총서 9(15), 2009, 31-32면

31) 김동민, “접근매체를 이용하는 전자금융사기의 범위에 관한 소고”, 충남대학교 법학연구소, 법학연구 31(2), 2020, 56면

32) 금융위원회 보도자료, “전기통신금융사기 방지 종합대책”, 2018.12.18.자

hacking),³³⁾ 기업의 이메일 계정을 해킹하여 수출 관련 물품 대금을 편취하는 이메일 해킹(e-mail haking)을 이용한 무역사기도 등장했다.³⁴⁾ 이렇듯 보이스피싱은 새로운 정보통신기술과 서비스의 등장에 맞추어 계속하여 진화하고 있다.³⁵⁾

최근에는 신종 보이스피싱이 등장하고 있다. 선불휴대전화를 사용하거나 외국인 명의의 휴대전화번호를 활용하여 보이스피싱을 한다. 해외발신 전화를 국내 전화번호로 변조하는 심박스(SIM BOX)를 활용하여 범행을 하기도 한다. 악성 앱을 설치하여 전화를 가로채거나, 피해자의 휴대전화에 앱을 설치하는 방법으로 대출 또는 이체를 하기도 한다.³⁶⁾ 신종 보이스피싱은 기존의 전화연결을 시도하거나 ATM기기로 유인하던 일차원적인 수법과 달리 피해자를 기망하는데 고도의 기술을 사용하고, 대응기관의 탐지·차단도 어렵게 하며 수사기관의 추적도 따돌리고 있다.

33) ZD Net Korea 보도(2013.8.23.), “PC메모리에 상주하는 악성코드 주의보”, <https://zdnet.co.kr/view/?no=20130823164250> (2020.12.14. 최종확인)

34) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서 16, 2016, 90면

35) 김동민, “접근매체를 이용하는 전자금융사기의 범위에 관한 소고”, 충남대학교 법학연구소, 법학연구 31(2), 2020, 56-57면

36) 금융위원회 보도자료, “디지털 경제의 신뢰 기반 조성을 위한 보이스피싱 척결 종합방안”, 2020.6.24.자

제2절 보이스피싱 범죄 실태

1. 보이스피싱 범죄 현황

경찰청 통계에 따르면, 보이스피싱은 2006년 이후 꾸준히 증가하다가 2017년을 기점으로 급증하는 추세를 보였다.³⁷⁾ 이어 2017년에는 총 24,259건, 2018년에는 34,132건, 2019년에는 37,667건으로 계속하여 증가하였고, 그 추세도 가파르게 상승하였다. 정부부처와 수사기관에서 다양한 전략을 추진하고 있지만, 보이스피싱은 글로벌화·지능화되면서 정부 당국을 따돌리고 있다.

〈표 2-3〉 최근 연도별 전화금융사기 피해 현황

구분	누적	2006~2016	2017	2018	2019
피해건수(건)	215,537	119,479	24,259	34,132	37,667
피해액(억원)	23,937	11,029	2,470	4,040	6,398

(출처 : 경찰청 보도자료, “경찰, 서민생활 보호에 역량을 집중한다”, 2020.2.17.자)

2. 보이스피싱 피해자 분석

가. 유형별 피해 현황

금융감독원은 보이스피싱 피해 예방을 위해 2017년부터 2020년 1분기까지 보이스피싱 피해구제를 신청한 피해자 135,000명을 대상으로 연령, 성별, 신용등급

37) 경찰청은 불특정 다수의 서민을 대상으로 막대한 피해를 야기하는 보이스피싱을 ‘서민 경제 침해 범죄’로 규정하고, 2020년 2월부터 ‘서민생활 침해 범죄’ 특별 단속을 추진하였다. 보이스피싱 등 전기통신금융사기로 2006년 이후 2019년까지 약 21.5만건이 발생하여 약 23조원 규모의 피해가 발생한 데 따른 조치였다. 경찰청 보도자료, “경찰, 서민생활 보호에 역량을 집중한다”, 2020.2.17.자

등 피해자 특징을 분석하였다.³⁸⁾

〈표 2-4〉 유형별 보이스피싱 피해 현황

(단위: 명, %)

구 분	‘17년	‘18년	‘19년	‘20년 1Q	합계
전체	30,420	48,116	49,597	7,288	135,421
대출빙자	25,036 (82.3)	32,649 (67.9)	38,213 (77.0)	4,990 (68.5)	103,929 (76.7)
사칭형	5,384 (17.7)	12,426 (25.8)	11,384 (23.0)	2,298 (31.5)	31,492 (23.3)
메신저	1,116 (3.7)	8,152 (16.9)	6,687 (13.5)	1,741 (23.9)	17,696 (13.1)

* () 안은 해당연도 전체피해자에서 유형별 피해자가 차지하는 비중
(출처: 금융감독원 보도자료, “보이스피싱 피해자 속성 빅데이터 분석을 통해 금융소비자 맞춤형 예방업무를 추진합니다”, 2020.8.11.자)

보이스피싱 전체 피해자 가운데 피해 유형별 현황을 살펴보면, 대출빙자형 피해자가 전체의 76.7%로 대부분을 차지하였고, 사칭형은 23.3%에 불과하였다. 2016년 이후 전체 피해 가운데 대출빙자형 보이스피싱 피해가 사칭형보다 높게 나타나는 추세가 계속 되었고, 메신저피싱은 2018년 이후 증가하는 양상을 보인 가운데 분기별로는 4분기에 증가하여 계절적 요인의 영향이 일부 있는 것으로 나타났다.

38) 금융감독원 보도자료, “보이스피싱 피해자 속성 빅데이터 분석을 통해 금융소비자 맞춤형 예방업무를 추진합니다.”, 2020.8.11.자

〈표 2-5〉 분기별 메신저피싱 피해 현황

(단위: 명)

구분	1분기	2분기	3분기	4분기
‘17년	151	164	310	491
‘18년	991	1,683	2,113	3,365
‘19년	1,417	1,702	1,654	1,914

(출처 : 금융감독원 보도자료, “보이스피싱 피해자 속성 빅데이터 분석을 통해 금융소비자 맞춤형 예방업무를 추진합니다” , 2020.8.11.자)

나. 연령별·성별 피해 현황

연령별 보이스피싱 피해 현황을 살펴보면, 50대가 32.9%로 가장 취약하고, 그 다음으로 40대(27.3%), 60대(15.6%) 순으로 나타났다. 대출빙자형 보이스피싱은 자녀 학자금이나 주택마련 등으로 자금 수요가 많은 40대와 50대에서 전체의 64.6%를 차지하였고, 사칭형 보이스피싱은 공공기관에 대한 신뢰도가 상대적으로 높은 50대와 60대에서 전체의 56.3%를 차지하였다. 사칭형 보이스피싱 가운데 메신저피싱 피해는 50대 이상이 전체의 74.5%를 차지하였고, 전체적으로 50대가 보이스피싱 피해가 가장 컸다.

최근 3년간 전체 피해자 대비 성별에 따른 보이스피싱 피해현황은 남성과 여성이 비슷한 수준이었고, 대출빙자형 보이스피싱 피해는 남성이 여성보다 조금 높은 수준이었다. 그러나 사칭형 보이스피싱 피해 및 메신저피싱 피해는 남성보다 여성이 더 취약하다는 점을 확인할 수 있었다.

〈표 2-6〉 연령별 · 성별 보이스피싱 피해 비율 현황

(단위: %)

구 분	20대	30대	40대	50대	60대	70대 이상	성별		합계
							남성	여성	
전체	6.7	15.2	27.3	32.9	15.6	2.3	51.6	48.4	100.0
대출빙자	5.0	16.1	31.4	33.2	12.9	1.4	57.8	42.2	100.0
사칭형	12.3	12.2	13.6	32.0	24.3	5.6	31.0	69.0	100.0
메신저	2.4	6.6	16.5	41.6	28.4	4.5	29.4	70.6	100.0

(출처 : 금융감독원 보도자료, “보이스피싱 피해자 속성 빅데이터 분석을 통해 금융 소비자 맞춤형 예방업무를 추진합니다”, 2020.8.11.자)

다. 신용등급별 피해 현황

피해자의 신용등급은 보이스피싱 유형별로 다양한 모습을 보였다.³⁹⁾ 먼저 대출빙자형 피해는 저신용자(58.8%)가 고신용자(4.8%)에 비해서 높게 나타나 신용등급이 낮을수록 취약하였다. 그러나 사칭형은 고신용자가 전체의 65.1%로 절반 이상을 차지한 반면 저신용자는 6.1%에 불과하였다. 즉, 고신용자는 비율로 볼 때 대출빙자형보다 사칭형에서 더 많은 피해가 발생한 것이다.

39) 총 10단계로 구분된 신용등급은 1~3등급은 고신용, 4~6등급은 중신용, 7~10등급은 저신용 등급으로 분류한다.

〈표 2-7〉 일반인 대비 피해 유형별 신용 등급 분포비율 현황

(단위: %)

구 분	1	2	3	4	5	6	7	8	9	10
대출빙자	1.0	1.4	2.4	5.4	11.9	19.0	37.7	15.5	3.3	2.2
사칭형	26.6	21.7	16.8	13.6	9.5	5.8	4.1	1.3	0.4	0.2
일반인	15.7	15.9	18.0	18.6	15.2	7.1	3.9	3.3	1.4	0.9

(출처 : 금융감독원 보도자료, “보이스피싱 피해자 속성 빅데이터 분석을 통해 금융소비자 맞춤형 예방업무를 추진합니다”, 2020.8.11.자)

3. 대포통장 적발 현황

금융당국은 보이스피싱 예방을 위해 2012년부터 대포통장이 발급되지 않도록 다양한 대책을 마련하였고, 2015년부터 ‘대포통장 근절 종합대책’을 시행하여 통장 개설 절차를 강화하였다. 2015년부터 은행 및 상호금융 권역에서 신규 계좌의 개설 심사 및 대포통장 의심거래 모니터링을 강화하여 대포통장 발생 건수를 감소시켜 나갔다.⁴⁰⁾ 그러나 2017년 인터넷전문은행이 등장하면서 대포통장 발생률이 다시 증가하기 시작하였다.⁴¹⁾ 실제로 인터넷은행 카카오뱅크의 경우, 보이스피싱 이용 계좌가 2017년 199건에서 2018년 932건, 2019년 2,153건으로 급격하게 증가한 것으로 확인되었다.⁴²⁾ 여기에는 인터넷상 상거래 목적으로 공개된

40) 금융감독원 보도자료, “2017년 상반기 대포통장 및 보이스피싱 현황 분석”, 2017.8.21.자

41) 금융위원회 및 금융감독원은 인터넷전문은행의 비대면 계좌 개설에 따른 대포통장 발생을 예방하기 위하여 고객 확인 절차 및 고객 금융거래 목적 확인 절차를 강화하는 등 선제적 대응 조치를 시행하였다. 전기통신금융사기 방지 대책협의회, 금융위원회 보도자료, “전기통신금융사기 방지 종합대책”, 2018.12.18.자

42) 연합뉴스 보도(2020.10.12.), “작년 보이스피싱 등 통신금융사기 이용 계좌 7만8천개 '역대최대'”

계좌번호를 활용하여 사기 피해금을 이체한 후 착오송금을 사유로 재이체를 요구하거나, 아르바이트 구직자를 대상으로 구매대행 또는 환전업무라고 속이고 사기 피해금을 이체한 후 현금으로 전달할 것을 요구하여 정상적인 통장을 보이스피싱에 활용하는 사례도 포함된다.⁴³⁾

〈표 2-8〉 보이스피싱 관련 대포통장 적발 현황

(금융감독원, 단위: %)

구분	2015	2016	2017	2018. 10
연간 건수	57,299	46,629	45,495	47,520
월평균	4,775	3,885	3,791	4,752

(출처 : 금융위원회 보도자료, “전기통신금융사기 방지 종합대책”, 2018.12.18.자)

한편, 국회 행정안전위원회 이해식의원(더불어민주당)이 경찰청으로부터 제출받은 자료에 따르면, 2016년부터 올해 8월까지 대포통장 사용으로 검거된 건수가 모두 89,050건으로 2016년 13,429건에서 2019년 25,526건으로 약 2배 가까이 증가한 것으로 나타났다. 다만, 2020년 1-8월까지 검거건수 및 검거인원은 전년 대비 감소한 것으로 나타났는데, 이는 코로나19의 상황과 정부와 금융·통신업체의 주의보 발령 및 전화번호 즉각 차단 등에 의한 결과로 보인다.⁴⁴⁾

<https://www.yna.co.kr/view/AKR20201011066600002?input=1195m> (2020.10.24. 최종확인)

43) 금융감독원 보도자료, “나도 모르게 대포통장(사기이용계좌) 범죄자가 될 수 있으니 조심하세요”, 2020.7.6.자

44) 금융위원회 보도자료, “디지털 경제의 신뢰 기반 조성을 위한 보이스피싱 척결 종합방안”, 2020.6.24.자

〈표 2-9〉 대포통장 검거 현황

(경찰청, 단위: %)

구분	2016	2017	2018	2019	2020. 8.
검거건수	13,429	16,380	21,453	25,526	12,262
검거인원	16,584	20,673	26,024	30,658	14,625

(출처 : 더퍼블릭, “[2020년 국정감사] 이해식 의원, 통장·핸드폰·차량 등 ‘대포 3종 세트’ 5년간 135,958건 검거”, 2020)

4. 보이스피싱 2차 피해

보이스피싱은 경제적 피해를 넘어서 극단적인 선택에 이르게 하는 경우도 많다. 보이스피싱 피해자 가운데 가장 많은 비중을 차지하는 50대는 한 가정의 가장인 경우가 대부분으로 피해를 입은 경우 극단적인 선택하는 경우도 있었다.⁴⁵⁾ 이와 같은 위험에도 보이스피싱으로 인한 자살에 대한 통계는 별도로 관리하지 않아 그 심각성을 파악하는 데 한계가 있다. 언론에 보도된 보이스피싱 관련 자살 사건은 아래와 같다.

① 20대/ 남성/ 취업준비생/ 전북 순창/ 2020년 1월⁴⁶⁾

검사를 사칭하여 “계좌가 대규모 금융사기에 연루되었다” 는 보이스피싱으로 420만원의 피해를 입은 후 신변을 비관하여 자살하였다. 수사결과 피해 현금을 수거한 혐의로 체포된 범죄자는 중국인 부부로, 서울에서 환전소를 운영하며 이른바 ‘환치기’ 수법을 통해 보이스피싱 조직 자금 관리에 개입하고 있는 것으로 확인되었다.

45) 김도윤, “한·중 전기통신금융사기범죄 및 관련 제도의 현황과 시사점”, 한 중법학회, 중국법연구 41, 2020, 163-164면

46) 연합뉴스 보도(2020.8.14.), “청년 극단적 선택 부른 보이스피싱...“순수한 사람도 살 수 있길””, <https://www.yna.co.kr/view/AKR20200814076300055> (2020.10.25. 최종확인)

② 40대/ 여성/ 직장인/ 광주광역시/ 2017년 1월⁴⁷⁾

보이스피싱 사기로 800만원의 피해를 입은 후 신변을 비관하여 자살하였다.

③ 20대/ 여성/ 대학생/ 경남 김해/ 2009년 3월⁴⁸⁾

우체국직원을 사칭하여 “발송되지 않은 신용카드가 우체국에 있다” 며 송금을 요구하는 보이스피싱으로 640만원의 피해를 입은 후 신변을 비관하여 자살하였다. 사건발생 직후 피해 사실을 신고하여 이체 후 30분만에 지급정지를 하였지만, 불과 5분만에 입금액이 모두 출금되었다. 경찰에서 2개월만에 인출책 및 대포통장 모집책 등을 검거하였으나 주범은 검거하지 못했다.⁴⁹⁾

④ 30대/ 남성/ 직장인/ 서울특별시/ 2020년 1월⁵⁰⁾

피해자 개인정보를 도용해 대포통장을 만들고, 가짜 수사서류 및 검찰 신분증까지 만들어 검사를 사칭한 보이스피싱 조직에 속아 약 1주일간 예금·보험금 및 회사 공금까지 약 5억 3천만원의 피해를 입은 후 경찰에 신고하였으나, 피해자 진술을 마친 후 약 3개월만에 자살하였다. 수사 결과, ① 피해사례에서 사용한 보이스피싱 전화의 발신지가 국내 같은 장소라는 사실을 확인했고, 인출책 등은 검거하였으나 총책 등 주범은 해외에 거주하는 것으로 나타났다.

47) 서울경제 보도(2017.7.28.), “ ‘광주 보이스피싱 피해자 자살 ’ 괴로워했다 네티즌 ‘살인죄로 적용해라’ ” ,

<https://www.sedaily.com/NewsView/10INGT62PU> (2020.10.24. 최종확인)

48) 연합뉴스 보도(2009.4.1.), “김해서 ‘보이스피싱’ 피해 여대생 투신 자살” ,

<https://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=001&oid=001&aid=0002583264> (2020.10.25. 최종확인)

49) 경남매일 보도(2009.4.16.), “여대생 자살 물고간 보이스피싱단 검거. 경남매일” ,

<http://www.gnmaeil.com/news/articleView.html?idxno=125331> (2020.10.25. 최종확인)

50) YTN 보도(2020.4.23.), “[단독] 또 ‘검사 사칭’에 속아...대한상의 직원, 극단적 선택” . https://www.ytn.co.kr/_ln/0103_202004230923448971 (2020.10.25.

최종점검)

⑤ 80대/ 남성/ 무직/ 서울특별시/ 2019년 1월⁵¹⁾

금융감독원을 사칭한 보이스피싱에 속아 아파트 앞에서 600만원을 대면 편취당한 후 사기 당했다는 사실을 자책하며 신변을 비관하다 자살하였다.

⑥ 50대/ 여성/ 무직/ 충북 청주/ 2015년 9월⁵²⁾

보이스피싱으로 2,700만원 상당의 피해를 입은 후 약 2개월 만에 자살하였다.

⑦ 60대/ 남성/ 무직/ 경기 성남/ 2011년 12월⁵³⁾

카드론 대출사기형 보이스피싱 조직에 2,700만원 상당의 피해를 당한 후 3일 만에 자살하였다.

5. COVID-19의 영향

COVID-19가 보이스피싱에 미치는 영향은 아직 속단하기 어렵기 때문에 관련된 통계를 소개하는 수준에서 논의하고자 한다. 금융감독원에 접수된 전기통신금융사기 관련 피해구제 접수 내용을 보면 2019년 1월부터 4월까지 약 2,177억원이었던 것에서 2020년 1월부터 4월까지 1,220억원으로 전년도 동기간 대비 약 43%가 감소하였다.⁵⁴⁾ 하지만 금융감독원은 통신사기피해환급법상 전기통신금융

51) 국민일보 보도(2019.1.17.), “[단독] “보이스피싱 당해 자책” … 80대 노인, 아파트서 투신 “,
<http://news.kmib.co.kr/article/view.asp?arcid=0012998679&code=61121211>
 (2020.10.25. 최종확인)

52) 중앙일보 보도(2015.11.29.), “[사회] 보이스피싱 피해 50대 여성 숨진 채 발견”, <https://news.joins.com/article/19155459> (2020.10.25. 최종확인)

53) 경향신문 보도(2011.12.13.), “서민 목숨 앗아간 카드로 보이스피싱”,
http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201112132131125
 (2020.10.25. 최종확인)

54) 금융위원회 보도자료, “디지털 경제의 신뢰 기반 조성을 위한 보이스피싱 척

사기가 아닌 대면편취형 사기가 증가하고 있고, 건당 피해액수는 전년 대비 0.5% 증가하는 등 코로나19 상황이 완화되면 다시 증가할 것으로 전망하고 있다.⁵⁵⁾ 그런데 메신저 피싱은 증가하였다. 2020년 1월부터 9월까지 기간 중 메신저 피싱의 총 피해건수 및 피해금액은 각각 6,799건 및 297억원으로 전년 동기 5,931건 및 237억원에 비하여 각각 14.6% 및 25.3% 증가하였다. 이렇게 볼 때 보이스피싱은 COVID-19로 인하여 해외 출국이 어려워지면서 감소한 것으로 보이고, 메신저 피싱은 고도의 기술이 필요하지 않고, 동시에 여러 명에게 접근할 수 있어 증가한 것으로 보인다.

〈표 2-10〉 최근 메신저 피싱 피해현황

(단위 : 건, 억원, %)

구 분		2018년	2019년	1월~9월(A)	2020년 1월~9월(B)	증감(률) B-A(B/A)	
메신저피싱	피해건수	9,607	8,306	5,931	6,799	868	(14.6)
	피해금액	216	342	237	297	60	(25.3)
카카오톡	피해건수	7,849	7,494	5,309	5,818	509	(9.6)
	피해금액	148	310	214	239	25	(11.7)

(출처 : 금융감독원 보도자료, “금감원, 문자 또는 카카오톡 등 메신저를 통해 가족 또는 친구를 사칭하는 보이스피싱에 유의하세요!” , 2020.11.4.자)

한편, COVID-19의 등장으로 보이스피싱 사기범들은 불안감을 이용하여 사회공학적인 방법을 사용하기 시작하였다. INTERPOL 보고서에 따르면, 기존의 범죄가 가

결 종합방안” , 2020.6.24.자

55) 금융위원회 보도자료, “디지털 경제의 신뢰 기반 조성을 위한 보이스피싱 척결 종합방안” , 2020.6.24.자

짜 약품 광고, COVID-19 관련 소식 업데이트, 금융 패키지 및 긴급 혜택 등으로 변환되어가고 있다고 한다.⁵⁶⁾ 발신번호를 조작하여 피해자가 의심하지 않으면 COVID-19와 관련된 시나리오를 사용하여 사기성 웹사이트에 검색을 유도하여 정보를 수집하고 결과적으로 금원을 편취한다.⁵⁷⁾

56) INTERPOL Report, “CYBERCRIME: COVID-19 IMPACT” , 2020, pp.8-9

57) INTERPOL Report, “CYBERCRIME: COVID-19 IMPACT0” , 2020, pp.8-9

제3절 신종 보이스피싱 등장

1. 대출사기형 보이스피싱

대출사기형 보이스피싱은 저금리나 대환대출 형태의 광고를 스미싱으로 배포하여 금원을 편취하는 수법을 말한다. 즉, 금융기관을 사칭하여 정부지원자금, 대환대출 등 저금리로 대출이 가능하다고 피해자에게 접근한 후, 피해자가 대출 의사가 있다면 대출 진행을 명목으로 악성코드가 포함된 금융앱을 다운로드받도록 유도한다. 이후 IP 주소를 발송하여 악성앱을 설치하게 하고, 보이스피싱을 의심하는 피해자에게는 은행 대표번호로 전화하도록 유도한다. 이때 악성코드에 감염된 피해자의 모바일에서 발신 전화를 탈취, 보이스피싱 조직원이 은행직원을 사칭하여 피해자를 안심시킨 후 피해금을 편취한다.

- ① 사기범은 금융기관을 사칭하여 대출상담을 빙자해 피해자에게 접근하였다. 피해자에게 ‘정부지원자금으로 저금리 대출 최대 3천만원까지 가능’ 하다고 피해자를 기망한 사기범은 대출진행을 위해 금융기관 앱을 다운로드 받아야 한다고 안내한 후 피해자에게 IP 주소를 전송하였다. 피해자가 자신의 말에 따라 IP 주소를 클릭하여 앱(악성코드)을 설치하도록 유도한 사기범은 보이스피싱이 아닌지 의구심을 갖는 피해자에게 은행 대표번호로 전화하도록 하였다. 피해자가 은행 대표번호로 전화하자 사기범은 악성코드를 활용하여 피해자의 발신 전화를 탈취, 은행원을 사칭하여 ‘신용평점 상승을 위한 절차이니 입금해도 된다’ 고 안심시켜 피해자로부터 기존 대출금 상환명목으로 300만원 상당을 편취하였다.⁵⁸⁾

58) 경찰청 보도자료, “대출절차 진행에 필요하다며 금융기관 앱을 다운로드 받도록 하는 수법”, 2018.12.19.자

- ② 2019년 2월 56세 피해자는 ‘1577-xxxx’ 전화번호로 신용캐피탈 대출 팀장이라 사칭하는 사기범의 전화를 받게 되었다. 보이스피싱 사기범은 피해자가 1천만원 전환대출이 가능한 대상으로 선정되었으나, 신용점수가 부족하다는 이유를 설명하며 대출을 발생시켜 갚는 방법으로 신용등급을 올리는 방법을 제시했다. 피해자는 사기범의 지시대로 ‘대출전용 앱’을 설치한 뒤 신용점수를 올리기 위해 카드사로부터 카드론 대출 500만원을 받은 후 다시 대출을 갚기 위해 해당 카드사의 대표번호로 전화를 하였다. 하지만 사기범이 설치를 유도한 대출전용 앱은 피해자의 발신 전화를 가로채는 악성 앱으로 피해자가 카드사 대표번호로 발신한 전화를 가로채 ‘고객님의 카드론 상환을 위해 차명계좌로 입금하라’라는 안내를 하였다. 이후 피해자는 차명계좌로 500만원을 송금하였고 실제 카드사의 대금청구서를 받아 카드론대출이 상환되지 않은 것에 대해 문의하는 과정에서 보이스피싱을 당한 사실을 알게 되었다.⁵⁹⁾

2. 공공기관 사칭형 보이스피싱

공공기관 사칭형 보이스피싱은 대환대출형 보이스피싱과 수법이 비슷하다. 기관의 대표번호로 전화하는 피해자의 발신전화를 탈취하기 위한 악성앱 설치 유도 및 허위 사이트 링크 공유, 허위 공문서를 사용한 신종 범행 수법으로 진화하였다. 주로 “서울중앙지검 수사관”을 사칭하는 경우가 많았고, 피해자에게 연락을 취해 “사기 사건에 연루되어 해당 사건의 피해자들에게 고소된 상태”라며 피해자를 심리적으로 압박한다. 사기행위와 관련된 허위 공문 및 검사 신분증 사본을 보내 피해자를 안심시킨 사기범은 거짓 URL 주소를 피해자에게 보내 사이버안전국 앱으로 위장한 악성앱을 다운로드 하도록 유도한다. 이후 피해자에게 금융감독원 대표번호로 전화하여 사기에 관련한 사항을 확인하라고 지시하는데, 이때 사기범

59) 금융감독원 보도자료, “허위 신용카드 결제 문자 및 원격조종 앱을 통한 피해사례”, 2019.8.21.자

은 악성코드에 감염된 피해자의 모바일에서 해당 전화를 탈취한다. 다른 사기범과 통화를 마친 피해자는 허위 서울중앙지검 홈페이지에 접속하여 사건조회를 위해 개인정보를 입력하게 되는데 이때 개인정보를 탈취 당한다. 사건 조사를 명목으로 계좌에 있는 돈을 금융감독원 담당자에게 입금해야 한다고 요구하거나, 문화상품권을 결제하는 방식으로 통장의 진위 여부를 확인해야 한다며 상품권 구입 PIN번호의 전송을 유도한다. 이때 범죄자는 피싱·스미싱·파밍 등 알려진 사기 수법을 총망라하여 치밀하게 시나리오를 설계한 후 피해자에게 접근한다.

- ① 사기범은 서울중앙지검 수사관을 사칭하여 피해자의 명의를 쇼핑몰 사기에 도용되었고, 피해자들에게 고소된 상태라고 기망하였다. 해당 문제를 해결하기 위해 검사를 연결시켜 준다는 이메일로 가짜 사건공문과 가짜 신분증 사본을 보내 피해자를 안심시키고, 경찰청 사이버안전국 사이트라며 거짓 URL 주소를 보내 악성앱을 다운로드 하도록 유도하였다. 이후 사기범은 금융감독원 1332로 전화하여 피해금액을 확인하라고 지시하였고, 피해자가 금융감독원 번호로 전화하자 악성앱으로 인해 금융감독원 직원을 사칭한 다른 사기범에게 연결되어 사기범 말을 신뢰하게 된다. 그래서 피해자가 가짜 홈페이지 <https://x.x.x.x>에 접속하여 ‘나의 사건조회’ 클릭 후 성명 및 주민번호를 입력하면 사건개요와 함께 위조된 서울중앙지검 공문을 보게된다. 이후 사기범은 피해자가 사건과 관련이 있는지 계좌 조사가 필요하고, 이를 위해 피해자들의 피해금을 금융감독원 팀장 계좌에 입금하면 조사 후 바로 환금된다고 속여 이를 편취하였다.⁶⁰⁾

- ② ‘010’ 으로 시작되는 번호로 전화가 와 계좌가 사기에 활용되었다며 금융감독원에서 연락이 왔다.⁶¹⁾ 우선 보이스포싱을 의심하자 소장.PDF 파일을 카

60) 금융감독원 보도자료, “주요 보이스포싱 피해 유형”, 2018.9.11.자

61) 본 사례는 연구자가 2020년 8월 20일 인터넷 블로그에서 보이스포싱에 대한

카오톡으로 전송받았고, 그 후 소장에 대한 설명과 자신의 경고를 무시했을 때 구속수사가 된다고 안내했다. 자신을 ‘금융감독원 과장’ 이라고 소개한 사기범이 계좌 정지 및 잔고 확인을 위해 인터넷뱅킹 로그인을 유도했고 잔고 화면을 캡처 및 전송하라며 요구했다. 보이스피싱 의심이 가시지 않아 정확한 사실 확인을 위해 업무를 핑계로 다시 통화하기로 하였다. 하지만 스마트폰에 설치된 악성코드로 인해 전화가 먹통이 된 상황이었다. 스마트폰에 설치된 악성코드 종류는 알 수 없었고, 안드로이드 모양의 앱이 생성되었다. 앱을 지워도 여전히 핸드폰이 먹통이라 대리점에 방문하여 휴대폰을 공장 초기화하였다. 사기범들은 이미 내 과거 행적과 농협 통장을 개설한 농협지점 및 지역을 알고 접근하였고, 기본적인 모든 정보를 알고 있었다. 보이스피싱임을 알아차리고 혹시 몰라 거래 금융사에 대출신청 정지를 요청하던 중 사기범들이 대출 시도를 했다는 사실을 알게 되었다. 카카오뱅크 /국민은행에서 대출을 위한 신용정보 조회 안내 카톡을 받게 되어서 알게 되었다. 카카오뱅크의 대출 시도를 확인하고 모든 계좌의 지급 정지를 위해 각 은행과 통화하던 중 국민은행에서 추가 시도가 있다는 것을 알게 되었다. 거래하고 있는 모든 계좌의 입출 및 대출을 정지시켰고 공인인증서 비밀번호를 변경하였다. 사건 후 처리에서 경찰관의 태도가 마음에 들지 않았다. 금전적인 피해를 입지 않았으니 본인이 알아서 처리해야 한다고 말했고, 어떻게 후 처리를 해야 하는지 방법이나 추가 설명이 없어 스스로 해결해야 했다. ‘이강우 검사’ 라는 사람이 실제로 존재하고 ‘이강우 검사’ 라는 이름으로 다른 피해자들이 계속 발생하고 있다는 것을 알게 되었다.

피해사실을 게시한 피해자를 연결하여 전화 인터뷰를 한 것임

[그림 2-1] 피해자가 실제로 받은 허위 서류

[illegible][illegible]

3. 지인사칭형 메신저 피싱

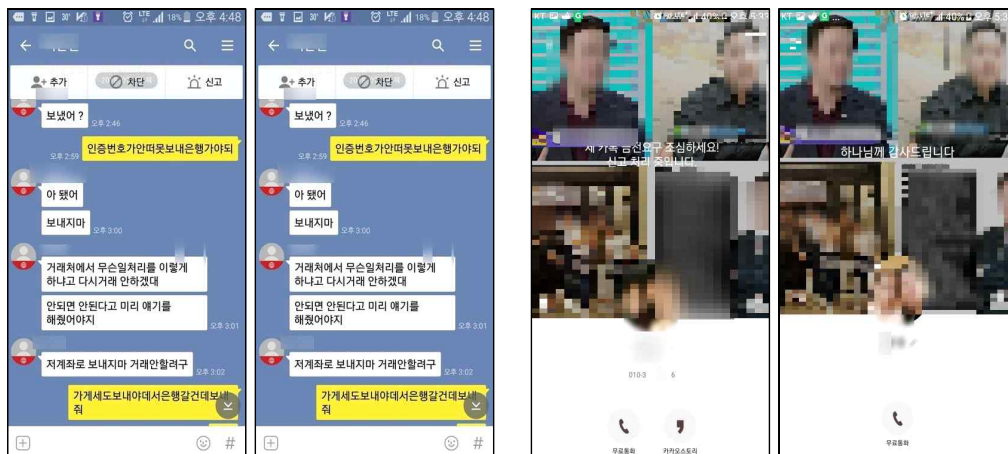
지인사칭형 메신저 피싱은 주소록이나 지인정보에 대해 쉽게 저장하고 확인할 수 있는 서비스가 보급되면서 생긴 신종 수법이다. 범죄조직은 유출된 개인정보 등에서 확인한 피해자의 포털 사이트 계정, 메신저 및 SNS 계정을 해킹하여 접속한다. Naver나 Google등 포털 계정의 경우 피해자의 모바일에 저장된 지인들의 데이터가 존재하는데 이런 데이터들을 수집한 후 피해자의 이름 및 프로필 사진을 도용하여 지인들에게 접근한다. 이때 휴대폰 고장을 핑계로 통화를 회피하고, 부모, 이모, 삼촌 등 호칭을 특정하기 쉬운 사람에게 접근하고, 인증 전 오류 등 송금 불가를 핑계로 소액 송금을 요구한다.⁶²⁾ 소액 송금 부탁을 비교적 잘 들어주는 50, 60대를 겨냥하여 자녀, 조카 등을 사칭하는 경우가 많다.

① 메신저피싱이 일어나기 전, 피해자는 네이버 포털사이트에서 자신의 아이디

62) 경찰청 보도자료, “지인을 사칭한 메신저피싱 주의 당부”, 2018.12.18.자

로 해외 접근이 시도되었다는 메일을 받았다. 그 다음날 피해자의 네이버 포털사이트 내 주소록 서비스 정보를 탈취한 사기범은 피해자의 이름을 도용하여 카카오톡을 새로 설치하였다며 피해자의 지인들에게 접근을 시도했다. 이때 사기범은 피해자의 카카오톡 이름, 배경, 이미지 등을 똑같이 사용하여 카카오톡으로 피해자의 가족들에게 소액을 요구하는 연락을 취했다. 피해자와 똑같은 프로필로 피해자를 사칭하기 때문에 지인들이 사기범을 친구추가하게 되면 사기범과 실제 피해자의 카카오톡 프로필 구분이 어렵게 된다. 이런 수법으로 사기범은 피해자 어머니를 기망하여 송금받은 98만원을 편취하였다.⁶³⁾

[그림 2-2] 피해사례의 실제 대화(왼), 피해자와 사기범 프로필(오)



(출처 : 네이버블로그(2018.7.13.), “카카오톡 피싱 신종보이스피싱 당했다.”)

- ② 독일에서 피해자는 손녀로 사칭한 사기범으로부터 “집을 구매하는데 20,000 유로가 급하게 필요하며, 현금은 손녀의 지인을 보넬테니 그에게 전달해 달라” 는 전화를 받았다. 피해자는 의심 없이 은행으로 가서 돈을 인출 후 사기범에게 현금을 전달했다. 이와 유사한 범죄로는 Lolli로, Lolli라고 알려진

63) 네이버블로그 (2018.7.13.), “카카오톡 피싱 신종보이스피싱 당했다”, <https://blog.naver.com/hanuricu/221318518758> (2020.10.21. 최종확인)

폴란드 범죄자는 2015년 오스트리아에서 개통한 전화를 활용해 Enkeltrick 조직을 만들고 노년층을 대상으로 약 640,000유로의 금전적 이득을 취했다. 결국 Lolli는 사기행각을 했다는 혐의로 독일 함부르크 법정에 섰고, 12년 6개월의 징역형을 선고 받았다.⁶⁴⁾

4. 소액결제 사기형 스미싱

소액결제 사기형 스미싱 수법은 보이스피싱 조직이 피해자에게 피해자가 사용하지 않은 신용카드 결제 확인 문자 메시지를 발송하면서 시작한다. 피해자가 메시지를 받은 후 사실여부를 확인하기 위하여 메시지에 있는 번호로 전화를 하면서 보이스피싱 범죄가 이루어진다. 통화 연결이 된 상담원은 피해자에게 명의도용되었다고 설명하고 경찰을 사칭하는 다른 직원에게 연결시키고, 경찰을 사칭하는 사기범은 피해자의 명의가 사기범죄에 이용되었고 이에 따른 수사협조를 요청하며 피해자의 모바일이나 PC에 원격조종 프로그램을 설치한다. 그 후, 피해자의 공인인증서 비밀번호 및 개인정보를 탈취하여 피해자 계좌의 예금을 편취하는 방식으로 보이스피싱 피해를 야기한다.

- ① 피해자 A씨는 본인이 사용한 적이 없는 결제 문자메시지를 받고 사실 여부를 확인하기 위해 문자메시지에 안내된 번호로 전화하였다. 전화 상담원은 피해자 A씨에게 “명의를 도용된 것 같으니 고객(피해자)를 위해 대신 경찰에 신고해 주겠다”며 피해자를 안심시킨 후, 서울지방경찰청 지능범죄수사대 최 00을 사칭하는 사기범을 연결시켜 주었다. 사기범은 피해자 A씨에게 “당신의 신용카드가 해외에서 발생한 명의도용 사기범죄에 이용되었으니 범죄 수

64) The Local (2018.6.26.), “Duping Oma: what to know about the ‘Enkeltrick’ scam in Germany” ,
<https://www.thelocal.de/20180626/what-to-know-about-the-enkeltrick-scam-in-germany> (2020.10.25. 최종확인)

사에 협조하면 당신에게 직접적인 불이익은 없을 것”이라며 피해자에게 자신의 지시를 따를 것을 요구하였다. 이후 사기범은 피해자 소유의 은행 계좌 해킹 및 바이러스 감염 여부를 점검해준다는 명목으로 피해자 소유 컴퓨터에 원격조종 프로그램을 설치하게 한 후, oo은행 인터넷 뱅킹에 접속하여 피해자에게 이체 비밀번호 및 공인인증서 비밀번호, OTP 생성번호를 직접 입력하게 하여 2천만원 상당의 예금을 편취하였다.⁶⁵⁾

- ② 피해자는 지역 은행 상담원을 사칭한 사기범으로부터 “타 지역에서 발생한 2건의 가짜 결제건이 있어서 해당 카드에 대해 거래정지 처리가 필요하다”라는 전화를 받았다. 사기범은 사전에 입수한 H씨의 카드번호 마지막 4자리 정보를 사용해 피해자의 의심을 피했다. 사기범은 이어 기존 거래 카드정지 후 새로운 카드 발급 여부를 확인했고, 피해자는 이에 응했다. 이 과정에서 다시 피해자의 의심을 피하기 위해 사기범은 사전에 입수한 피해자의 상세주소를 사용했고, 새로운 카드 발급에 필요하다는 명목으로 피해자의 모친 maiden name과 기존 카드 뒷면의 CVV 번호, 그리고 기존 카드의 PIN번호를 요구했다. 피해자는 의심없이 모든 정보를 사기범에게 제공했고, 사기범은 위조된 카드와 피해자의 정보를 이용해 2,900달러를 결제하고 ATM 기기를 통해 500달러를 인출하는 등의 금전적 이득을 취했다.⁶⁶⁾

65) 방송통신위원회 보도자료, “스미싱 문자를 이용한 보이스포싱 피해사례”, 2019.9.5.자

66) Krebs on Security (2018.10.18.) , “Voice Phishing Scams Are Getting More Clever” ,
<https://krebsonsecurity.com/2018/10/voice-phishing-scams-are-getting-more-clever/> (2020.10.25. 최종확인)

제4절 미래 보이스피싱 예측

1. 딥페이크 기술을 활용한 보이스피싱

미래사회에서는 딥페이크를 이용한 보이스피싱이 발생할 수 있다. 인공지능 기술이 발전함에 따라 딥페이크 기술을 활용한 조작된 음성과 영상이 새로운 수단이 될 수 있다.⁶⁷⁾ 인공지능을 이용해 만든 콘텐츠는 범죄 인지와 탐지가 쉽지 않고, 온라인에 배포된 프로그램을 통해 일반인도 접근이 가능하다. 이미 다양한 모바일 앱이 존재하고, 유·무료 서비스도 등장하여 누구나 사용할 수 있게 되었다.

실제로 딥페이크가 보이스피싱에 활용된 사례가 있다. 2019년에 독일에서 인공지능을 이용해 CEO의 음성을 사칭한 보이스피싱이 발생하였다. 독일 모회사 CEO를 사칭한 사기범은 영국에 본사를 둔 에너지 회사의 CEO인 피해자에게 “긴급 요청건으로, 1시간 이내에 헝가리 공급자에게 자금은 보내 달라”고 요구하였고, 피해자는 목소리와 억양 등 모든 것이 독일 CEO와 똑같다고 생각하고 22만 유로를 헝가리 은행 계좌로 이체한 것이다.⁶⁸⁾

향후 보이스피싱 조직원이 딥페이크 기술을 활용하여 지인의 목소리와 억양을 동일하게 구사하면 현재의 예방 및 차단 시스템이 다소 무력화될 수 있고, 그로 인한 피해는 더욱 커질 것으로 보인다.

67) DAWES center for future crime at UCL report, “DAWES CENTER FOR FUTURE CRIME ANNUAL REPORT” , 2020, p.4

68) THE WALL STREET JOURNAL(2019.8.30.), “Fraudsters Used AI to Mimic CEO’ s Voice in Unusual Cybercrime Case” ,
<https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402> (2020.10.23. 최종확인)

2. 심스와핑(SIM Swapping)을 통한 모바일 서비스 통제권 탈취

심 스와핑(SIM Swapping)은 기존의 휴대폰에서 새로운 휴대폰으로 사용하던 서비스를 그대로 전환하여 사용할 수 있는 역할을 지원하는 기능이다. 일반적으로 이 기술은 휴대폰을 분실하거나 도난을 당했을 때 사용된다. 통신서비스 업체가 해당 전화번호를 다른 심(SIM)에 이식할 수 있는 기술을 가지고 있으며, 이를 활용하는 방식이다. 즉, 범죄자는 심 스와핑을 위해서는 통신사 인증이 필요하기 때문에 통신사 직원을 매수하거나, 사전에 충분한 타인의 정보를 확보하여 범행을 시도하게 된다.⁶⁹⁾ 범죄자는 스마트폰 유심(USIM)에 저장되어 있는 타인의 정보를 가로채어 인증 수단으로 활용하여 불법 사용이나 금융자산(암호화폐 등) 탈취에 활용한다.⁷⁰⁾ 대부분의 인증 수단을 스마트폰의 SMS 문자로 실시하기 때문에 비밀번호 분실을 위장하여 계정과 비밀번호를 재지정할 수 있다. 따라서 문자를 기반으로 한 이중 인증장치를 손쉽게 무력화 시킬 수 있다.

심 스와핑을 이용하여 피해자의 전화 서비스 통제권을 탈취한 사례도 있다.⁷¹⁾ 피해자는 심카드가 업데이트되었다는 이동통신사의 SMS를 받고 남편의 휴대전화를 이용해 자신의 휴대전화번호로 전화 연결을 시도했으나, 통화연결음만 갈 뿐 피해자의 휴대전화로는 전화가 걸려오지 않았다. 사기범은 심 스와핑을 통해 피해자의 전화 서비스 통제권을 탈취하였고, 피해자의 남편에게 전화해 피해자의 @Rainbow라는 트위터 계정을 포기할 것을 요구하는 협박을 했다.⁷²⁾ 범죄자는 2

69) 보안뉴스 보도(2020.12.29.), “이탈리아 모바일 통신사 호 모바일 고객 정보 250만 건 유출돼”, <https://www.boannnews.com/media/view.asp?idx=93815> (2020.12.30. 최종확인)

70) EUROPOL, SIM SWAPPING-A MOBILE PHONE SCAM, <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/sim-swapping-%E2%80%93-mobile-phone-scam> (2020.12.30. 최종확인)

71) VICEmedia group (2018.7.17.), “The SIM Hijackers”, https://www.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin (2020.10.25. 최종확인)

차 인증시 필요한 피해자의 전화번호와 각 계정에 연결된 이메일 주소를 통제할 수 있었고, 때문에 피해자의 트위터 계정뿐만 아니라 인스타그램, 아마존, 이베이,페이팔, 넷플릭스, 훌루 등 여러 온라인 계정을 탈취해 금전적 이득을 취했다.⁷³⁾

3. 스푸핑(Spooping)을 활용한 사칭

스푸핑(Spooping)은 보안 취약성을 악용한 것으로 자신의 주소를 속여서 접속하는 공격이다.⁷⁴⁾ 피싱 사기범들은 스푸핑 위장 기술을 사용하여 스마트폰에 부처의 전화번호가 발신자 번호로 뜨도록 조작하여 피해자들을 안심시키고, 실제 공무원의 이름과 직위를 사칭하기도 한다.⁷⁵⁾ 사기는 이메일을 사용하기도 하나, 피해자의 신뢰를 얻기 위해 주로 전화나 메시지를 활용하기도 한다.

실제 범죄자는 터키에서 스푸핑 소프트웨어를 사용해 독일의 비상 핫라인인 110 번을 발신번호로 하여 독일의 연금 수급자인 피해자들에게 전화를 하여 경찰을 사칭하면서 “절도범의 타겟이 되었으니, 귀중품을 안전한 곳으로 숨기고 현재 가지고 있는 현금을 다른 계좌로 이체하라” 고 유도한 사건이 있었다.⁷⁶⁾ 그래서 피해자

72) VICEmedia group (2018.7.17.), “The SIM Hijackers” ,
https://www.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin (2020.10.25. 최종확인)

73) VICEmedia group (2018.7.17.), “The SIM Hijackers” ,
https://www.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin (2020.10.25. 최종확인)

74) Deutsche Welle(2019.2.14.), “‘Fake police’ steal hundreds of thousands from Germany’s elderly” ,
<https://www.dw.com/en/fake-police-steal-hundreds-of-thousands-from-germanys-elderly/a-47523341> (2020.10.25. 최종확인)

75) coindesk KOREA(2019.5.7.), “뉴욕경찰 “비트코인 노린 보이스피싱 급증” 경고” , <https://www.coindeskkorea.com/news/articleView.html?idxno=45863> (2020.12.15. 최종확인)

76) Deutsche Welle(2019.2.14.), “‘Fake police’ steal hundreds of thousands from Germany’s elderly” ,

의 현금을 사기범의 대포통장으로 이체하도록 유도하여 약 78만 유로를 편취하였다.⁷⁷⁾

또한, 미국의 국세청(IRS, Internal Revenue Service) 직원을 사칭하는 사례도 발생하였다. 은행이나 국세청에서 전송한 메시지인 것처럼 가장하고, 피해자가 스미싱 내 링크를 눌러 스마트폰이 악성코드에 감염된 다음 메시지 발신번호로 전화하면 사기범이 수신하는 방식인 것이다.⁷⁸⁾ 사기범들은 피해자에게 전화를 걸어 선불카드, 기프트 카드 또는 계좌이체 등의 방법으로 납부하라고 압박하고, 미납된 금액을 즉시 지불하지 않으면 경찰이 체포하거나 기소할 것이라고 위협한다.⁷⁹⁾

<https://www.dw.com/en/fake-police-steal-hundreds-of-thousands-from-germanys-elderly/a-47523341> (2020.10.25. 최종확인)

77) Deutsche Welle(2019.2.14.), “‘Fake police’ steal hundreds of thousands from Germany’s elderly” ,

<https://www.dw.com/en/fake-police-steal-hundreds-of-thousands-from-germanys-elderly/a-47523341> (2020.10.25. 최종확인)

78) Federal Communications Commission, Avoid the Temptation of Smishing Scams, <https://www.fcc.gov/avoid-temptation-smishing-scams> (2020.12.15. 최종확인)

79) Federal Communications Commission, This Tax Season, Don’ t Fall for Spoofed IRS Calls, <https://www.fcc.gov/tax-season-dont-fall-spoofed-irs-calls> (2020.12.15. 최종확인)

제3장 신종 보이스피싱 범행수법과 대응기술

제1절 신종 보이스피싱 범죄조직

1. 범죄조직 구성 및 기능

가. 연구방법

보이스피싱 범죄조직의 체계, 구성과 역할을 살펴보기 위하여 논문, 판결문⁸⁰⁾ 등을 기초로 하여 2020년 6월부터 10월까지 보이스피싱 수사경험이 있는 수사과장·팀장·수사관 등 총 5명, 보이스피싱 탐지 관련 기업 관계자 4명, 이동통신사 관계자 2명 등 총 11명과 대면 또는 전화 인터뷰를 진행하였다.

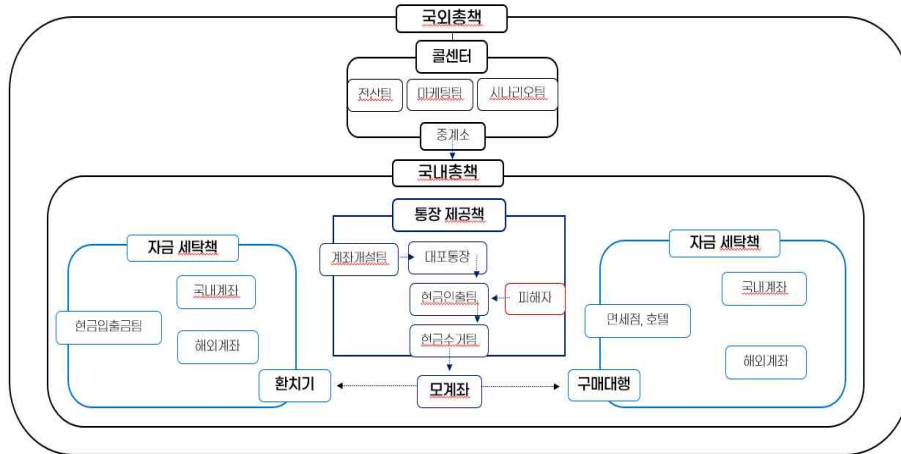
나. 범죄조직 구성도⁸¹⁾

보이스피싱 조직은 크게 총책, 통장제공책, 자금세탁책으로 나눌 수 있다. 총책은 오다집, 통장 제공책은 장집, 자금세탁책은 세탁집으로 불리고 있다. 총책이 통장제공책, 자금세탁책을 모집하는 경우도 있고, 그 반대로 통장제공책과 자금세탁책이 총책을 모집하는 경우도 있다. 조직의 규모에 따라 자금세탁책과 통장제공책이 구분되지 않고, 양자의 역할을 동시에 수행하는 경우도 많다.

80) 대구지방법원 2017.1.19. 선고 2016고단5392 판결; 서울고등법원 2015. 4. 24. 선고 2014노3497 판결; 수원지방법원 안산지원 2016. 12. 16. 선고 2016고합203, 220(병합), 242(병합), 245(병합), 2016초기126, 289, 334 판결

81) 서울강동경찰서 보이스피싱 수사팀장님을 대상으로 2020년 6월 3일에 인터뷰를 실시한 내용을 기재한 것임

[그림 3-1] 보이스피싱 조직단체 구성도



(출처 : 서울강동경찰서 자료 수정 · 보완, 2020년)

다. 범죄조직 기능 및 역할

1) 총책

총책은 주로 각 조직원들의 실적에 따라 범죄수익을 분배하는 조직원들을 총괄 지휘하고, 범행을 지시한다. 국외총책과 국내총책으로 나뉘는데 국외총책은 국외에서 활동하는 조직과 국내 조직을 관리하고, 파밍 사기에 이용하는 악성코드 유포 및 콜센터를 운영하며 송금 및 인출을 위해 통장모집과 전달을 담당한다. 국내총책은 보이스피싱 범죄에 사용할 대포통장의 계좌주를 감시하는 감시책, 감시책으로부터 받은 현금을 전달하는 배달책으로 구성된다. 총책이 관리하는 콜센터는 전산팀, 1차 콜센터(시나리오팀), 2차 콜센터(마케팅팀), 중계소팀 등으로 구성되고 콜센터를 운영하며 피해자에게 전화를 걸고 피해자를 기망하여 각종 금품을 탈취하는 역할을 한다.

〈표 3-1〉 보이스피싱 총책 역할

분류		세부내용
총책	국외총책	<ul style="list-style-type: none"> · 국외 국내 조직 관리 · 콜센터 운영 · 입·출금을 위한 통장 모집 및 전달 지시
	국내총책	<ul style="list-style-type: none"> · 국내 조직원 관리 · 보이스피싱에 사용되는 대포통장 및 계좌주 감시 · 입·출금을 위한 통장 모집 및 전달 지시
콜센터	전산팀	<ul style="list-style-type: none"> · 스미싱을 통한 악성코드 유포 및 악성앱 개발 · 해킹·악성코드 유포를 통해 개인정보 확보 · 피해자들이 접속할 기관사칭 허위사이트 제조 · 허위문서 작성 등
	1차 콜센터 (시나리오팀)	<ul style="list-style-type: none"> · 피해자를 속이기 위한 시나리오 작성(대환대출, 기관사칭, 중고거래, 등) · 피해자들에게 전화하여 개인정보 파악 후 2차 콜센터로 전달
	2차 콜센터 (마케팅팀)	<ul style="list-style-type: none"> · 시나리오를 따라 직접 피해자들에게 전화하여 속인 후 준비한 계좌로 피해금 이체 유도하는 역할
	중계소팀	<ul style="list-style-type: none"> · 인터넷 전화를 010이나 02등 국내 전화로 보이도록 발신 번호를 변작하여 피해자에게 접근

세부적으로 살펴보면 전산팀은 스미싱을 통한 악성코드 유포 및 악성앱 개발, 해킹·악성코드 유포를 통해 개인정보 확보, 피해자들이 접속할 기관사칭 허위사이트 제조 등의 역할을 수행한다. 콜센터는 1차 콜센터와 2차 콜센터로 나뉘는데, 1차 콜센터는 피해자들에게 전화하여 개인정보를 파악한 후 2차 콜센터로 전달하는 역할을 하고, 2차 콜센터는 시나리오를 따라 직접 피해자에게 전화를 걸어 개인정보를 알아내거나, 직접 피해자들을 속여 미리 준비한 대포통장 계좌로 피해금원 이체를 유도하는 역할을 한다.⁸²⁾ 2차 콜센터와 피해자가 전화 연결이 되면

82) 이기수, “최근 보이스피싱의 범죄수법 동향과 법적 대응방안”, 경찰대학 범죄수사연구원, 범죄수사학연구 4(2), 2018, 3-19면

대환대출 서비스 제공이나 검사 사칭, 피해자들의 직계비속을 납치하고 있다는 협박 등 여러 가지 시나리오로 피해자들에게 대포통장 계좌로 현금을 이체시킨다. 국외총책은 1차 콜센터를 관리하면서 상담원들로 하여금 대출희망자들의 인적사항을 파악하게 하고 이를 취합한 내역을 2차 콜센터로 전송해 대출희망자 인적사항을 2차 콜센터 상담원들에게 분배한다. 국내 총책은 한국 내 조직원을 관리하며 송금 및 인출을 위한 통장 모집 및 전달을 지시한다. 이 때 감시책은 ‘국내총책’ 으로부터 대포통장에 피해금이 입금되었다는 연락을 받으면 ‘대포통장 계좌주’ 를 만나 계좌주로 하여금 현금을 이체하게 하고 이를 감시하는 역할을 한다.

이들은 텔레마케터(상담원)를 고용하고 교육시킨 다음 실제 여러 가지 수법을 동원하여 확보한 개인정보를 통해 피해자에게 연락을 한다. 주로 국제전화를 우회할 수 있는 심박스(SIM Box)를 이용하여 인터넷 전화를 010이나 02 등의 국내전화로 보이도록 발신번호를 변작하여 접근한다. 이를 수신한 피해자는 시나리오팀의 시나리오에 따른 다양한 수법으로 기망당해 재산을 탈취당하게 된다. 대표적인 사기유형으로는 저금리 대출 및 마이너스 통장 개설 안내 등의 대환대출 사기, 검찰 등 국가기관을 사칭하는 행위가 있다. 조건만남을 조건으로 하여 성매매대금을 무단으로 취득하거나 거래 중 환불을 요청할 시 추가 입금을 요구하는 사례가 있고, 중고나라 물건 판매 명목으로 편취하는 중고나라 사기, 이성적 관심을 빌미로 자금 등을 편취하는 로맨스 스캠 등도 발생하고 있다. 사회적 이슈가 변화하고 기술이 진화함에 따라 시나리오는 점점 지능화되고 고도화되고 있다.

정리하면 전산팀은 해킹과 악성코드 유포를 통해 개인금융정보를 확보하고, 시나리오팀(1차 콜센터)은 피해자를 속이기 위한 시나리오를 작성한다.⁸³⁾ 마케팅팀(2차 콜센터)은 시나리오에 따라 피해자에게 전화를 걸어 개인정보를 알아내거나 계좌이체를 유도한다.⁸⁴⁾

83) 이기수, “최근 보이스피싱의 범죄수법 동향과 법적 대응방안”, 경찰대학 범죄수사연구원, 범죄수사학연구 4(2), 2018, 3-19면

84) 이기수, “최근 보이스피싱의 범죄수법 동향과 법적 대응방안”, 경찰대학 범죄수사연구원, 범죄수사학연구 4(2), 2018, 3-19면

2) 통장제공책

통장제공책은 대포통장을 개설하는 계좌개설팀과 보이스피싱 피해금을 인출하는 현금인출팀과 수거하여 모계좌로 입금하는 현금수거팀으로 구성된다. 계좌개설팀은 개인계좌, 법인계좌, 인터넷 뱅킹이 가능한 계좌, 달러 이체가 가능한 계좌 등의 대포통장을 개설한다. 보이스피싱 피해자가 해당 계좌로 돈을 입금하거나 현금수거책이 피해자와 대면으로 피해금을 편취하게 된다. 계좌로 입금하였을 경우에는 은행 ATM 인출기를 통해 현금을 인출하여 현금인출책이 현금수거책에게 직접 전달하기도 한다. 이렇게 편취된 범죄수익금은 은행 ATM 무통장 입금을 통해 1차 모계좌로 입금되게 되고 이를 세탁하는 작업을 거치게 된다.

〈표 3-2〉 보이스피싱 통장제공책 역할

분류		세부내용
통장 제공책	계좌개설팀 (통장모집책)	<ul style="list-style-type: none"> 차명계좌를 모집 광고하여 대포통장을 수집 및 개설 작장(개인계좌), 큰장(법인계좌), 인백(인터넷 뱅킹이 가능한 계좌), 달러장(달러 이체가 가능한 계좌) 등의 대포통장을 개설하여 직접 또는 퀵 서비스로 전달하는 역할
	현금인출팀	<ul style="list-style-type: none"> 피해자의 피해금을 현금인출 ATM기에서 인출하는 역할. 주로 조직의 하위 조직원이 행동하며, 고액알바 광고 등으로 일반인들이 가담하는 경우가 많음
	현금수거팀	<ul style="list-style-type: none"> 각 지역 계좌개설팀(통장모집책)이 모집한 통장을 인출책에게 전달하는 역할 대포통장에 입금된 보이스피싱 피해금을 ATM에서 인출 및 피해자에게 대면 수거하여 1차 범죄 모계좌로 무통장 입금

3) 자금세탁책

보이스피싱의 자금세탁책은 모계좌팀, 환치기팀, 환전소팀으로 구성된다. 이 구성원은 피해자들에게 탈취한 범죄수익금을 합법적인 거래 및 환전 등의 유통과정을 거쳐 자금세탁을 한다. 결국 보이스피싱 피해자에게 탈취한 범죄수익금은 통장제공책의 모계좌로 입금된다. 범죄조직은 1차 모계좌로 들어간 범죄수익금을 계좌이체나 비트코인 등의 가상화폐로 교환하거나 문화상품권, 백화점상품권 등으로 교환한다. 직접 전달하여 2차 모계좌로 전송하기도 한다. 통장제공책의 모계좌에서 보이스피싱 피해자에게 탈취한 범죄수익금은 환치기나 구매대행의 형태로 해외에서 자금세탁이 되어 최종적으로 총책에게 들어간다. 그렇기 때문에 범죄수익금을 처리한 특정인을 수사하는 것이 아닌 환전소를 조사해야 한다. 구매대행 또한 실제 물품유통업자가 물품구입을 요청할 때에도 보이스피싱을 통해 취득한 범죄수익금을 사용하고, 그 물품을 해외에 송부하는 방식으로 자금세탁을 한다.

〈표 3-3〉 보이스피싱 자금세탁책 역할

분류		세부내용
자금 세탁책	모계좌팀	· 범죄수익금의 형태를 변환하는 단계이다. 1차 모계좌로 들어간 범죄 수익금을 계좌이체, 가상화폐, 문화상품권, 백화점상품권 등으로 교환하여 자금세탁
	환치기팀	· 수익금을 해외에 송금할 때 은행을 통해 송금하는 것이 아닌 국내계좌와 외국계좌를 모두 가지고 있는 특정인을 통해 적은 수수료로 돈을 송금하는 방식으로 자금세탁. 불법환전소는 환전 요청인이 요청한 금액을 자신의 돈이 아닌 보이스피싱을 통해 취득한 범죄수익금으로 환전거래 진행
	환전소팀	· 실제 물품유통업자가 해외에서 물품구입을 요청하게 되면 이를 국내 면세점에서 보이스피싱을 통해 취득한 범죄수익금으로 해당 물품을 구입 후 그 물품을 해외에 송부하는 방식으로 자금세탁

이처럼 보이스피싱 조직은 국내조직과 해외조직의 이원화로 운영되며 구체적인 역할별로 조직이 세분화 되어있다. 하지만 점조직형태로 구성된 복잡하면서도 느슨한 조직체계로 이루어져 있어 한곳에서 적발되더라도 보이스피싱 조직 전체 파악 및 핵심 인물들의 특징이 어렵다.

2. 범죄조직의 언어(은어)

가. 조사방법

보이스피싱 범죄조직의 구성과 기능을 정확하게 이해하기 위해서는 그들이 사용하는 언어 즉 은어를 이해해야 한다. 보이스피싱 은어는 음성인식이나 텍스트 마이닝을 통해서 탐지 기술을 개발하는 데에도 기초자료로 활용할 수 있을 것이다. 원래 은어란 형식적 규칙을 배제하면서 비교적 참신성이 있고 생명력이 짧으며 유대감을 표시하는 일종의 특수어로서, 한 집단의 유대감이나 동일한 집단의식 형성에도 영향을 미치는 단어를 말한다.⁸⁵⁾

보이스피싱 은어를 조사하기 위해 2020년 10월 20일부터 10월 22일까지 포털사이트, 다크웹, SNS를 검색하고, 보이스피싱 관련 판결문, 보도자료, 피해자 전화인터뷰 등을 종합하여 1차적으로 은어를 도출하였다. 이어 보이스피싱에 대한 수사경험이 있는 경찰관 15명을 임의적으로 선정하여 2020년 10월 22일 부터 10월 26일까지 서면조사와 전화인터뷰를 진행하여 최종적으로 8가지 유형에 84개의 은어를 발굴하였다.

85) 김자영, “러시아 마피아 집단의 특수어 연구 : 은어를 중심으로”, 배재대학교 한국-시베리아센터, 한국시베리아연구 16(2), 2012, 112면

나. 은어의 개념과 종류

보이스피싱 조직에 관한 은어로는, 총책을 의미하는 따거, 선장집, 레이더(다)가 있으며, 콜센터의 경우 오다집, 장집, 검집, 대출집, 배우, 전화기집, 통신책(유심책)이 있다. 통장제공책에는 배차, 출자, 출, 말, 세탁집, 징뱃이 있으며, 모집책으로는 토스실장, 유입책, 차책이 존재하였다. 조직을 뜻하는 은어들은 각 조직의 역할을 설명하고 있었고, 범행수법에 따라 다양한 형태로 결합되는 ‘오다집’과 ‘장집’도 있었다.

<표 3-4> 보이스피싱 은어 : 조직

분 류		은 어	의 미	비 고
전체		보피	보이스피싱 피해자, 보이스피싱	범죄자의 입장에서 피해자는 고객을 뜻한다.
조 직	총 책	따거	사장	
		선장집	총책 중 조직원을 찾는 사람	
		레이더 (다)	현금이 운반되는 과정(현금수거책, 전달책, 송금책, 인출책)을 뒤에서 감시하는 역할	주로 조선족으로 국내 사정에 정통한 사람들을 상대로 일을 시키고 있다.
	콜 센 터	오다집	통장 오더집, 줌비 오더 등등 각 개별적으로 통장 및 계좌 모집 진행	‘오다집’과 ‘장집’은 별개의 조직이자 각자 역할을 총괄하는 콜센터를 의미한다. 규모가 큰 조직에서는 ‘오다집’과 ‘장집’을 동시에 운영하거나, 여러개의 콜센터를 운영하는 경우가 있다.
		장집	· 불법 계좌 개설을 담당 · 범죄수익금의 수거, 전달, 송금, 인출과정을 전담	
		검집	검찰 사칭 콜센터	
		대출집	대출사기형 콜센터	

조 직		배우	피해자에게 직접 전화 걸어 연기하는 과싱책	
		전화기 집	범행이용 인터넷전화를 개통하는 조직	
		통신책 (유심책)	대포폰, 유심 개설 담당	
	통장 제공 책	배차	통장을 가져갈 사람	
		출자	현금을 인출하는 인출책(현금 인 출책)	
		출	현금인출(책)	‘출’ 표현은 인출을 지칭한다. 예) ‘출자’ 는 인출책을 지칭 예) 출기 → 인출하라 구인구직사이트에 ‘출’ 을 모집, 관리하는 팀을 ‘출팀’ 이라고 표현한다.
		말	<ul style="list-style-type: none"> · 현금을 인출하는 국내 인출책, 수거책 · 현금 전달책으로부터 받은 돈을 수거하여 조직 상부에 전달하는 역할 · ‘장집’ 콜센터에서 인출책 및 송 금책에게 카톡 및 위챗 메신 저로 지시를 내리며 장기관의 말처 럼 움직이게 한다고 하여 ‘말’ 이 라 칭함 	
		세탁집	해외에서 환치기 및 구매대행을 수범으로 하여 자금을 세탁하고 국내 오다집에 범죄수익금 전달	
		징벳	<ul style="list-style-type: none"> · ‘징역 베틱’ 의 줄임말 · 검거되어 실형에 처할 것을 각 오하고서 피해금 현금수거 등 역할에 가담하는 것을 의미 	

조 직	모집 책	토스 실장	보이스피싱 등 범행에 사용되는 대포폰(유심)을 개통하기 위해 인 터넷에 광고글을 게시하여 가입자 들을 모집하는 사람	
		유입책	돈을 입금할 피해자를 모집하는 모집책	
		차책	대포차 모집 담당	

또한, 범행에 사용하는 계좌를 의미하는 다양한 은어들이 있다는 것을 확인하였다. 은어의 조어는 일반적으로 계좌를 의미하는 ‘장’이라는 단어에서 파생하였고, 장물량, 장주, 독장, 공장, 개인장, 한도장, 신규·재장, 공상, 앞장, 세차장이라는 단어도 사용하였다. 인출과 관련된 계좌로는 작장, 작은장, 큰장, 의뢰장, 출장이 있고, 세탁과 관련하여 막장, 중간장, 안정장, 뒷장이라는 단어를 사용하였다. 또한, 특수목적용 가진 계좌를 따로 분류하여 인뱅(인벤)장, 코인장, 체크장, 법인장, 쇼핑장, 달러장, 카드장, 중고나라장, 비트장, 보피장, 증권장이라는 단어를 사용하였다. 이를 통해 보이스피싱 조직은 거래목적에 따라 세부적으로 계좌를 나누어 범죄자금의 체계적으로 운영이 되고 있음을 알 수 있다.

〈표 3-5〉 보이스피싱 은어 : 금융

분 류	은 어	의 미	비 고
금 용 계 좌	장	계좌	
	장물량	보유한 통장의 양	
	장주	대포통장의 계좌주	
	독장	사용 이력(이용내역)이 없는 계좌	
	공장	피해금액 인출 뒤 신고 되지 않아 재사용 준비 중인 통장	

금 용	계 좌	개인장	개인 계좌	
		한도장	한도가 있는 계좌	
		신규 /재장	신규 및 다시 사용하는 계좌	
		공상	중국 공상계좌(중국계좌)	
		앞장	피해금을 받는 계좌	
		세차장	입출금 등 테스트가 완료된 범행 계좌	
	인 출	작장	일한도 600만원 이하 현금인출 전용 계좌	
		작은장	<ul style="list-style-type: none"> · 일한도 600만원 이하 현금인출 전용계좌 · 계좌주로부터 계좌번호, 비번, OTP 등을 받고 피해자로부터 계좌에 돈을 송금 받은 후 국내에서 현금을 뽑아서 계좌로 송금하는 사람, 조직 	
		큰장	<ul style="list-style-type: none"> · 장주가 직접 돈을 인출하는 계좌(한도없음) · 장주가 직접 본인 계좌에 입금된 피해금을 피의자들의 계좌로 돈을 송금 	보통 검찰사칭 오다집에서 큰 금액의 피해금을 입금받기 위해 사용하는 대포통장을 의미한다.
		의뢰장	인출 전용 계좌	
		출장, 출금장	현금 입금·출금은 가능하나 다른 계좌로 이체할 수는 없는 통장	
	세 탁	막장	<ul style="list-style-type: none"> · 보이스피싱 피해금을 입금 받을 대포통장 · 개인 명의로 된 통장 중 한번 사용하고 버릴 용도로 개설한 통장 · 장집 콜센터에서 대포통장을 모집하기 위해 계좌 명의자를 속여 계좌정보를 오다집에 제공 	

금 용	세 탁	중간장	피해자가 송금한 계좌에서 중간 유통목적으로 이용되는 통장	
		안정장	범인 통장 등으로 장기적으로 사 용이 가능한 통장 보이스피싱 피해금을 인출하여 환전상들을 통해 중국등으로 보 내기 전에 범죄수익금이 모이는 통장	
		뒷장	피해금액을 입금하는 계좌(환전, 세탁 계좌)	
	특수 목적	인뱅 (인벤)장	인터넷뱅킹 가능 계좌	
		코인장	비트코인으로 피해금을 받는 계좌	
		체크장	체크카드와 연결되어 있는 계좌	
		법인장	법인명의로의 계좌	
		쇼핑장	현물거래시 사용되는 계좌	
		달러장	달러 이체 가능 계좌	
		카드장	카드와 연결되어 있는 계좌	
		중고 나라장	중고나라 거래시 연결되는 계좌	
		비트장	비트코인 거래가 가능한 계좌	
		보피장	보이스피싱 피해금을 이체받을 대포통장	
		증권장	증권 거래를 위한 계좌	

자금을 나타내는 단어로는 장값, 세탁돈, 까만돈, 쿵이라는 단어를 사용하여 자금의 상태와 단위를 별도로 설정하였다.

〈표 3-6〉 보이스피싱 은어 : 자금

분 류	은 어	의 미	비 고
자금	장값	장집에서 판매하는 계좌 1개당 금액	
	세탁돈	피해금을 세탁(여러 계좌로 송금, 비트코인 매입·환전, 토토사이트 충전·환전, 금목걸이 등 현물의 구입·판매 등)하여 수사기관에서 추적하기 곤란하게 만든 돈	
	까만돈	· 세탁되지 않은 돈 · 보이스피싱 피해금 자체	
	쿵	‘만원’을 부르는 단위	

범행 수법을 의미하는 은어로는, 대·검·조·협·사라는 단어로 대환대출, 검찰사칭, 조건만남, 협박, 중고나라 물품사기의 앞글자만 딴 단어를 사용하였다. 또한, 검찰 오다와 같이 범행수법과 조직을 의미하는 단어를 합성하여 사용하였다. 범행장소는 상황실을 뜻하는 오다지와 인출, 수금, 전달 등이 이루어지는 현장을 뜻하는 필드라는 단어를 사용하였다.

〈표 3-7〉 보이스피싱 은어 : 범행수법 및 장소

분 류	은 어	의 미	비 고
범행 수법	대/검/조/협/사	대환대출, 검찰사칭, 조건만남, 협박, 중고나라 물품사기의 앞글자만 딴 것으로 보이스피싱 단체의 범죄수법	

범행 수법	검찰 오다	검찰을 사칭하여 피해자들로부터 금원을 편취하는 수법으로 검사 또는 검찰 수사관을 사칭한 보이 스피싱을 의미	검찰사칭 수법을 사용하는 오 다집 일명 ‘검집’ 이라고도 부른다.
범행장소	오다지	상황실	
	필드	인출, 수금, 전달 등이 이루어지는 현장	

범행 수단은 강수강발, 인바프로그램, 모바일게이트웨이, DB, 막DB, 내구제DB, 멘트지, 통카오, 콜폰, 본폰, 소결의 단어를 사용하였으며, 범죄행위로는 배짱장사, 손배달, 장작업, 덩동, 만세, 세차, 비대개통이 있었다.

〈표 3-8〉 보이스피싱 은어 : 범행수단

분 류	은 어	의 미	비 고
범행 수단	강수강 (강발)	금융기관을 사칭한 악성코드가 설치된 악성 애플리케이션 ‘강발’ 은 강제수신 강제발신의 줄임말	악성앱이 설치되면 피해자가 발신하거나 수신하는 전화를 오다집에서 가로채 받거나 원하는 전화번호로 강제발신 이 가능하다.
	인바 프로그램	<ul style="list-style-type: none"> 인바운드 프로그램 인바운드는 외부에서 걸려오는 전화, 아웃바운드는 직전 전화를 거는 것을 의미 DB를 구입하여 대량의 문자 또는 전화를 뿌린 후 상담을 원하는 피해자를 오다집 상담원 들에게 자동 배당되게 하는 프로그램 	과거엔 피해자들의 DB를 구입하여 직접 전화를 거는 아웃바운드 방식의 수법을 사용했다.
	모바일 게이트 웨이	<ul style="list-style-type: none"> 심박스(유심 중계기) 중국에서 070으로 발신하는 전화번호를 국내에 설치된 심박스를 통해 010의 전화번 	

범행 수단		호로 변작	
	DB (디비)	피해자들의 이름, 연락처 등 개인정보	
	막DB	이름, 전화번호, 주소 정도만 있는 간략한 개인정보	
	내구제 DB	가족사항, 금융정보, 직장사항 등 다양한 개인정보가 있어 활용 도거 높은 고급 개인정보	
	멘트지	보이스피싱 전화 시 피싱책들이 보는 시나리오(대본)	
	통카오	통장 체크카드 OTP카드	
	콜폰	대포 휴대전화	
	본폰	본인 명의로 개통된 실제 사용 휴대전화	
	소결	휴대전화 소액결제	

나아가 특정상태를 설명하는 은어로 휴, 오다방어, .을 사용하였고, 기타 듀넘, 라스, 민짜 등의 용어도 사용한 것을 확인하였다.

<표 3-9> 보이스피싱 은어 : 상태 및 기타

분 류	은 어	의 미	비 고
상태	휴	안전한가	
	.	별일 없다	
	오다방어	지연	
기타	듀넘	듀얼넘버	
	라스	라스트 스코어	
	민짜	미성년자	

이처럼, 범죄조직들은 은밀하게 정보를 공유하고 범죄 수사망을 피하고자 은어를 사용하였다. 언어는 사람의 인식과 행동을 반영하여 발전하게 된다. 따라서 보

이스피싱 범죄조직이 사용하고 있는 은어를 파악하여 범죄행태를 더욱 구체적으로 분석할 수 있을 것이다. 보이스피싱 용의자의 음성이 누적되면 음성을 분석하고 특정 형태로 분류하는 것이 용이해질 것이다. 대검찰청에서 ‘용의자 음성식별을 위한 한국인 음성 데이터베이스 수집 및 음성 자동분석 시스템 개발’⁸⁶⁾, ‘용의자 음성식별을 위한 한국인 표본 데이터베이스 구축’⁸⁷⁾ 등의 과제를 진행한 것으로 보아 음성 데이터베이스에 대한 기초 연구가 어느 정도 진행되었을 것이다. 여기에 보이스피싱 범죄조직이 사용한 은어를 활용하면 음성식별을 위한 텍스트마이닝 기술에 하나의 데이터베이스로 활용할 수 있을 것이다.

86) 신지영, “용의자 음성식별을 위한 한국인 음성 데이터베이스 수집 및 음성 자동분석 시스템 개발”, 대검찰청 용역과제, 2014

87) 신지영, “용의자 음성식별을 위한 한국인 표본 데이터베이스 구축”, 대검찰청 용역과제, 2014

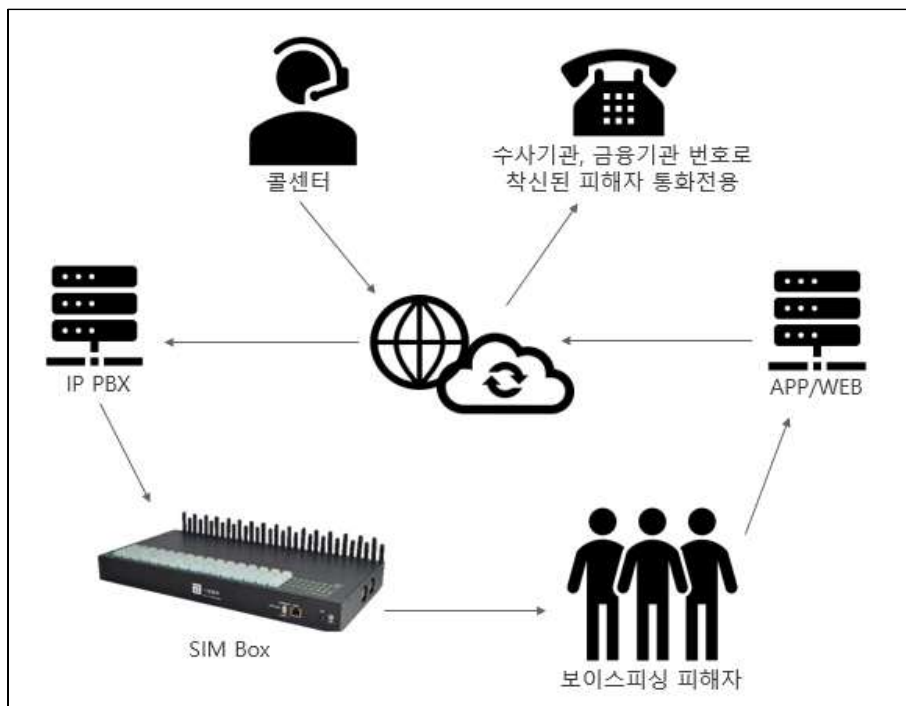
제2절 신종 보이스피싱 범행수법

1. 개괄

보이스피싱 범죄자가 피해자에게 접근하는 수법은 크게 6단계로 나눌 수 있다.

- ① 보이스피싱 콜센터에서 피해자에게 전화 발신
- ② 인터넷 신호로 변환되어 VPN서버를 통해 IP-PBX 주소로 전송
- ③ IP-PBX를 거쳐 연결되어 있는 심박스로 신호 전송
- ④ 국제번호가 국내 '010' 번호로 변작되어 피해자에게 수신
- ⑤ 스미싱이나 사기범의 유도로 악성앱 설치 및 모바일 악성코드 감염
- ⑥ 모바일 감염을 통해 피해자 발신전화를 착취하여 사기범에게 연결

[그림 3-2] 보이스피싱 범행수법 개요도



콜센터가 주어진 개인정보 목록을 바탕으로 피해자에게 전화를 걸면 전화통신의 호가 인터넷 신호로 변환되어 VPN 서버를 거친다. 발신된 국제번호 통신신호는 VPN서버 주소를 포함하여 IP-PBX를 통해 국내에 설치된 심박스로 전달된다. 신호를 받은 심박스는 국제번호를 국내번호로 변작하는 역할을 하고, 해외 발신번호는 심박스를 통해 '010' 번호로 변작되어 피해자의 모바일에 표기된다.

피해자가 보이스피싱 사기범의 전화를 국내번호로 오인하고 수신하면, 사기범은 정해진 시나리오 대로 피해자의 모바일에 악성 앱의 설치를 유도한다. 설치된 악성앱은 국가·금융기관 대표번호로 향하는 발신통신의 호가 보이스피싱 사기범에게 연결되도록 피해자의 모바일을 악성코드에 감염시킨다. 사기범은 피해자에게 상황을 판단하기 위해 국가·금융기관 대표번호로 전화하도록 유도하며, 악성코드에 감염된 모바일을 통해 피해자가 확인전화를 걸면 사기범이 해당 전화를 받는다. 이처럼 보이스피싱에 사용되는 기술은 ① 선불 유심(USIM) 악용, ② IMEI 변조, ③ 심박스, ④ 오토콜, ⑤ 악성앱 운영, ⑥자금세탁 등 6가지로 구분할 수 있다. 보이스피싱에 사용되는 범행수법은 다음과 같다.

<표 3-10> 보이스피싱 범행수법

범행수법		세부내용
① 선불 유심(USIM) 악용		선불 USIM의 개통이 쉽고 간편하다는 점을 악용하여 대량 개통 후 발신번호 변작에 사용
② IMEI 변조		수사 시 IMEI 값으로 추적되는 것을 방지하기 위해 IMEI 값 변조
③ 심박스	네트워크 구성	콜센터 전화신호를 IP-PBX를 통해 인터넷전화 신호로 변환, VPN 서버를 활용하여 국내로 전화신호 전달 및 연결, 3G통신을 4G(LTE) 통신으로 전환하는 4G Router 사용으로 보이스피싱 조직의 범행 기술 고도화
	운영방식	기본적으로 모텔, 고시원 등 특정 장소에 설치하여 운영되며, 최근 이동 차량에 설치하거나 유심 없는 심박스 국내 설치 등 수사를 피하기 위한 운영방식 등장

	토도스	해외 출국자가 국내 유심을 사용하여 국내에서 사용하던 번호를 그대로 사용 가능하도록 지원하는 서비스
④ 오토콜		대량의 번호를 사용하여 수신은 하지 않고 발신에만 사용하는 스팸발신 서비스
⑤ 악성앱 운영	악성앱 설치	스미싱 및 사기 시나리오를 통해 피해자의 모바일에 악성앱 설치를 유도하여 악성코드에 감염되도록 조치
	발신전화 탈취	음성통화로 악성앱을 설치하도록 유도하여 국가기관 대표 번호로 전화하더라도 발신번호가 범죄자에게 가도록 설정
⑥ 자금세탁	현금 인출·수거	보이스피싱 편취금 인출 후 범죄 조직에게 전달
	구매 대행	구매대행 의뢰가 들어오면 편취금으로 물품을 구매하고 구매대행 의뢰인으로부터 합법적인 현금 확보
	면세품	대리 구매자들을 모집하여 면세점에서 사기 편취금으로 면세품 구매를 진행한 후, 구매고객이 원하는 발송지로 국제 발송하는 형태로 자금세탁
	환전소	한국에서 원화를 받으면 환전상이 중국의 위안화를 고객 계좌로 이체시켜주는 방식
	암호화폐	국내 편취금으로 해외에서 발급받은 암호화폐 주소를 활용하여 범행 차명계좌에 송금하는 방식

2. 선불 유심(USIM) 악용

유심은 가입자 식별 정보를 구현한 IC칩으로, 사용자 개인식별번호가 부여되어 가입자 확인을 위해 활용된다. 선불 이동전화서비스 가입자가 사용하는 USIM이 선불 USIM이다. 서비스를 이용하기 전 사용 예정량에 해당하는 만큼의 통신요금을 충전한 후, 사용량만큼 해당 요금을 차감해 가며 이용하는 것을 선불 이동전화 서비스라고 한다.⁸⁸⁾ 이 서비스에서 사용되는 요금제가 선불요금제이고, 기본료가

88) 윤두영, “이동전화 선불요금제 현황 및 시사점”, 정보통신정책연구원, 정보통신방송정책 23(1), 2011, 3면

없거나 저렴하기 때문에 통신 소량 이용자나 국내 체류 외국인이 주로 사용한다. 보이스피싱에 사용되는 선불 USIM의 경우 이런 선불 이동전화 서비스를 이용하기 위해 개통되는 USIM을 말한다. 선불 USIM은 가상 이동 통신망 사업자(MVNO, Mobile Virtual Network Operator)를 거치는데, MVNO는 이동통신 3사(SKT, KT, LG유플러스)의 이동통신망을 임차하여 서비스하는 형태로 국내에선 알뜰폰이라는 명칭으로 불린다. 2020년 10월 기준 알뜰폰 전체 가입자는 약 890만 명이며, 이는 전체 이동통신가입자 7,000만 명 중 12.8%를 차지한다.⁸⁹⁾ 한국알뜰통신사업자협회 자료에 따르면 2019년 5월 기준 알뜰폰 전체 가입자 808만명중 선불폰 가입자는 374만명으로 전체 가입자 절반에 해당하는 규모이다.⁹⁰⁾ 이동통신 3사의 경우 1인당 최대 개통 회선(번호)을 2개로 제한을 하였으나, 알뜰폰의 경우 1인당 최대 4개 회선을 개통할 수 있다. 국내 알뜰폰 통신사만 70여개가 넘어 한 사람이 수십에서 수백 개까지의 번호 개통이 가능하다. 별정통신사를 통해 비교적 개통 절차가 간편한 선불 유심이 범죄에 사용되는 사례는 증가할 수밖에 없다. 개통된 다수의 선불 유심은 보이스피싱 범죄 행위 중 발신번호 변작에 사용된다. 보이스피싱 조직은 010 번호를 부여받은 선불 USIM을 구매하여 콜센터가 발신시 사용하는 국제번호를 국내 ‘010’ 번호로 변작 시키는데에 사용한다.

3. IMEI 변조

IMEI(International Mobile Equipment Identity)는 이동통신 모뎀칩에 부여되는 고유번호로, 전 세계 무선사업자가 운영하는 망에 접속해야 하는 장비 또는 모뎀 칩에 할당된 고유번호이다. 각 이동통신사는 IMEI를 기반으로 장비를 구분할 수 있

89) 스마트 초이스 홈페이지, 이동전화서비스 가입자 현황,
http://www.smartchoice.or.kr/smc/smartreport/service_03_client.do (2020.12.9. 최종확인)

90) 한국알뜰통신사업자 협회 홈페이지, 알뜰폰 현황,
http://www.kmvno.or.kr/info/info_02.php?PHPSESSID=7df05ae6e52a1efc944d39b04e294aa (2020.12.9. 최종확인)

다.⁹¹⁾ IMEI는 제조사가 스마트폰을 공장에서 출고 시에 부여되며 스마트폰의 제조사/국적/모델/스마트폰 일련번호 등의 정보가 포함되어 있어 대부분 스마트폰을 식별하고 스마트폰의 도난을 방지하기 위해 사용한다.⁹²⁾

<표 3-11> IMEI 구조와 형식

구분	자릿수	설명
TAC	AA(2)	IMEI 관리기관에서 TAC의 할당된 발급기관에 대한 고유코드
	BBBBBB(6)	발급기관에서 제조사에게 제공하는 번호로 제조사가 제조하는 ME마다 고유의 번호를 지정해 제공
일련번호	CCCCCC(6)	제조사가 정하여 발급하는 시리얼번호(스마트기기에 할당된 고유번호)
체크 디지털	D(1)	앞의 14자리를 특정한 알고리즘에 따라 확인할 수 있는 번호(주민등록번호와 같이 정상 번호 여부를 확인)

IMEI 값은 발신번호 변작 역할을 하는 심박스의 위치를 추적하는데 중요한 단서가 된다. 경찰은 보이스피싱 신고가 들어오면 이동통신사에 범죄에 사용된 전화번호 정보를 요청하고, 이동통신사는 해당 전화번호에 할당된 정보들 중 IMEI 값을 찾고, 범죄자의 단말기가 접속한 중계기 또는 기지국의 위치를 특정하여 경찰에게 제공한다. 이러한 방식으로 수사가 진행되자 사기범은 통신신호를 발생시킬 때 기지국에 접속할 IMEI값을 변조하여 수사망을 빠져 나간다.

91) 트루네트웍스 전문가를 대상으로 2020년 6월 15일에 인터뷰를 실시하였음.

92) 김선주, “USIM 정보를 활용한 패스워드리스 방식의 개인키 보호 방안”, 한국콘텐츠학회, 한국콘텐츠학회논문지 17(6), 2017, 34면

4. 심박스(SIM Box)

가. 네트워크 구성

보이스피싱 조직이 발신번호를 변작하는 과정을 거칠 때, ‘010’ 번호로 개통된 선불 USIM을 심박스의 슬롯에 최대 256개까지 장착할 수 있다. 심박스는 발신번호를 해외번호를 국내번호로 변작하기 위한 장치이고, 대량으로 모여 하나의 큰 장비를 형성하게 되면 이를 심뱅크(SIM Bank)라고 부른다. 이와 같은 변작을 규제하기 위해서 전기통신사업법은 전화번호를 거짓표시를 할 경우에 형사처벌하도록 규정하고 있다(제95조의2). 일반적으로 사용자의 신청에 의해 전화단말이 정상적으로 개통되었을 때, 개통된 단말로 전화를 발신하면 수신측에는 발신 단말의 전화번호가 표시된다. 수신자가 자신의 단말에 표시된 발신 전화번호로 다시 전화를 걸면 수신자에게 전화 발신을 했던 그 단말에 전화가 걸려야 한다. 하지만 보이스피싱 조직은 국제전화를 사용하거나 070등의 인터넷 전화를 이용하여 자신들의 발신 번호를 변작하여 피해자에게 전화를 한다. 국제전화가 걸려올 경우 보이스피싱이라는 사실을 인식하게 되자 범죄자들은 국내 일반 전화번호인 것처럼 ‘010’ 과 같은 형태로 발신번호 변작하기 시작했다.

이렇듯 발신번호 변작을 위해 콜센터에서 음성통화 신호를 발신할 때에 통신 신호는 VPN, IP-PBX, 4G Router를 거치게 된다. 콜센터에서 음성통화 신호를 발생시키면 VPN과 인터넷을 거쳐 일반신호가 인터넷 신호로 변환된다. VPN은 인터넷 전화를 해외로 보내는 서버이다. 보이스피싱 조직은 사기에 사용하기 위한 VPN서버를 여러 개 개설하여 소유하고 있고, 평균 일주일 단위로 서버를 바꾸기 때문에 피해자가 피해 당한 후 시간이 지나면 통신 시 연결되어 있던 VPN서버의 주소가 바뀌어 추적이 어려워진다. IP-PBX는 보이스피싱 조직이 인터넷 전화를 발신할 때 전화가 들어오고 나갈 수 있는 길을 만들고 삭제하는 유지관리 장치로 심박스의 각 포트에 기기를 연결 및 해지하는 역할을 한다. 4G Router의 경우는 일반 3G 인터넷 신호를 4G(LTE)의 신호로 돌려주는 역할을 한다. 이는 3G 전파신

호를 탐지하여 심박스의 위치를 추적하는 수사기법을 피하기 위한 고도화된 기술이고, 심박스와 Router가 연결되어 있어 심박스에서 신호를 피해자에게 발신할 시 Router를 거쳐 4G로 변환된 신호가 발신된다. 이러한 일련의 과정을 거쳐 보이스 피싱 사기범은 해외에서 음성통화 신호 발신을 해도 한국 유심 사용으로 발신번호를 국내번호로 변경시킨다.

나. 운영방식

심박스는 VoIP Gateway라고도 불리며 모텔, 고시원 등 특정 장소에 설치하여 운영한다. 기존 심박스는 다량의 실물 유심이 심박스에 꼽혀있는 상태로 설치되었으나 최근 심박스가 적발되어 압수 당하자 유심이 있는 심뱅크(SIM Bank)는 해외에 두고, 유심 없이 인터넷전화만 받는 심박스는 국내에 설치하기 시작했다.

아래 그림은 경찰에서 압수한 유심없이 국내에 설치된 VoIP Gateway 장비이고, 초록색으로 LED가 점등된 포트는 통화 중임을 나타낸다. VoIP Gateway는 유심없이 LTE유선 라우터만 연결되어 있는 형태이고, 신속한 수거와 이전이 가능하다.

[그림 3-3] USIM 없는 심박스(VoIP Gateway)



(출처: 부천원미경찰서, 2020)

최근 범죄자들이 경찰의 수사망을 피하기 위해 차량 내부에 심박스를 설치하여 유심을 포함한 다수의 게이트웨이를 이동식으로 운영하는 사례가 적발되었다.⁹³⁾ 심박스는 디스플레이, 프로세서, 키보드, 카메라, 스피커 등 많은 기능을 탑재하는 일반적인 모바일 기기와는 달리 통화 신호와 음성처리를 위한 유심, 안테나, 음성 처리 모듈, 모뎀 등만 갖추고 있다. 그래서 심박스는 디스플레이가 없고, 음성 및 모뎀만을 사용하기 때문에 전력을 적게 소모한다.

[그림 3-4] 차량 내부에 설치된 심박스

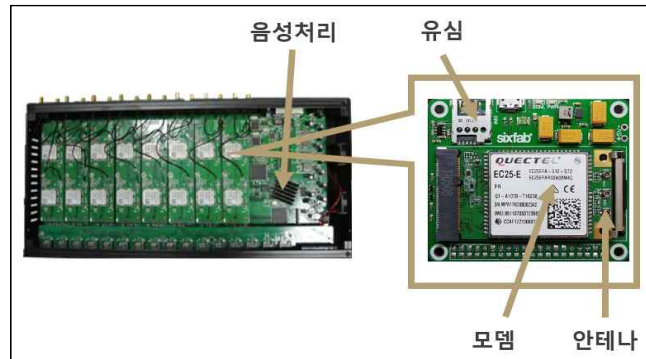


(출처: 부천원미경찰서, 2020)

심박스는 일반 모바일 기기와 달리 전력량 소모가 많지 않기 때문에 상당기간 외부에서 구동할 수 있고, 이동하면서 인근에 있는 와이파이 공유기 중 비밀번호가 설정되어 있지 않은 것을 이용하거나 LTE 라우터 역할을 하는 포켓 와이파이를 이용하여 인터넷을 사용하기도 한다.

93) 부천원미경찰서 보이스피싱 수사과장을 대상으로 2020년 6월 3일 인터뷰를 실시한 내용임

[그림 3-5] 심박스 사용 모듈



(출처: 트루네트웍스, 2020)

심박스 기기는 주로 해외에서 국내로 수입되는데, 밀수하는 형태가 많다. 최근 심박스를 완제품이 아닌 메인보드, 안테나 형태로 분해하여 부품 형태로 밀수하다 적발된 사례도 있다.⁹⁴⁾ 일반인들은 일반적인 기계의 메인보드 및 부품으로 인식할 가능성이 높다. 심박스는 대부분 해외에서 개발하고, 수입대항으로 얼마든지 구매가 가능하며 아직까지 국내 제조자는 확인되지 않았다. 해외직접구매 사이트 중 하나인 AliExpress에서 심박스 제조사인 ‘Wavecome’ 과 ‘SIM Box’, ‘SIM Bank’ 를 검색하였을 때 한 페이지 당 약 70개의 제품이 검색될 정도로 많다.

94) YTN 보도(2020.6.22.), “보이스피싱용 부품 밀수 일당 적발...범죄 원천 차단 나선다”, https://www.ytn.co.kr/_ln/0103_202006220535148350 (2020.10.6. 최종확인)

[그림 3-6] 심박스 부품



(출처: YTN, “보이스피싱용 부품 밀수 일당 적발...범죄 원천 차단 나선다”, 2020)

다. 토도스(Todos)

토도스(Todos)는 정식 정부 등록 통신업체로, 해외에서 앱(어플)을 통하여 국내 번호로 전화통신을 할 수 있도록 하는 서비스를 제공한다. 서비스 이용자가 본인 명의로 개통된 유심 카드를 토도스센터에 맡기면, 인터넷이 연결된 어느 곳에서든 국내에서 사용하던 본인의 전화번호로 추가 요금 없이 무료통화와 SMS(단문)를 이용할 수 있다.⁹⁵⁾ 즉, 이용자가 해외로 출국했을 때에도 로밍과 같은 특별한 절차 없이 인터넷만 연결된다면 앱을 설치하여 국내에서 사용하던 번호를 그대로 사용할 수 있는 서비스를 말한다. 하지만 보이스피싱 범죄조직이 토도스 업체에 대포 유심칩을 대량으로 맡긴 후 해당 서비스를 범죄에 활용하기 시작하였다. 보이스피싱 사기범은 국외에서 토도스 업체에 맡겨진 유심칩에 원격으로 접속해 010번호로 변작한 후 국내의 피해자에게 접근하는 방식을 사용했다.⁹⁶⁾ 따라서, 서비스 제공하던 업체는 보이스피싱에 사용된 유심을 경찰에 전달하였고,⁹⁷⁾ 경찰수사 협조

95) Todos 홈페이지, 고객센터 공지사항,

http://todosdialer.com/board/notice_view.asp?idx=143 (2020.6.8.최종확인)

96) 부천원미경찰서 보이스피싱 수사과장님 대상으로 2020년 6월 3일 인터뷰한 내용임

를 위해 2020년 4월부터 서비스 제공을 잠정 중단하였다. 이후 2020년 8월 iPhone에서 토도스 서비스를 이용 가능 하도록 iOS 앱을 출시하면서 토도스는 기존의 국내번호를 사용한 통화 서비스를 재개하며 현재 정상 서비스 운영 중이다.

5. 오토콜

오토콜이란 SIP⁹⁸⁾ 전화교환기를 개량해서 만든 것으로 입력된 수신전화번호로 자동 전화 다이얼링 할 수 있도록 만든 전화발신전용 프로그램이다. 오토콜은 PDS(Predictive Dialing System)와 ACS(Auto Calling Service)를 사용한다.⁹⁹⁾ PDS란 컴퓨터 프로그램에 전화번호를 넣어 자동으로 연결된 콜을 상담원에게 순차적으로 자동 분배 및 전화 연결해주는 시스템이다. ACS는 정보를 수집하는 시스템으로, 입력된 DB의 전화번호로 자동 콜을 보내 수신자와 연결되면 프로그램에 입력된 ARS멘트를 송출한다. 그 후, 안내되는 멘트에 따라 번호를 눌러 반응을 보인 수신자들의 전화번호나 정보를 수집한다. 오토콜은 발신전용 프로그램이기 때문에 발신전화번호의 경우, 프로그램에 입력한 번호로 수신자에게 표시되는 특징을 가지고 있다.¹⁰⁰⁾ 오토콜은 서버와 이용자 프로그램, 관리자 프로그램으로 구성되어 있다. 서버는 전화개통과 발신 등의 전화교환, 타사 기간통신사와 연동 역할을 하며 서버의 내부에는 이용자·관리자 프로그램에서 입력된 전화번호의 데이터베이스가 구축되어 있다. 이용자(발신자)프로그램의 경우 오토콜 서비스 사용자가

97) Todos 홈페이지, 고객센터 공지사항,

http://todosdialer.com/board/notice_view.asp?idx=143 (2020.6.8. 최종확인)

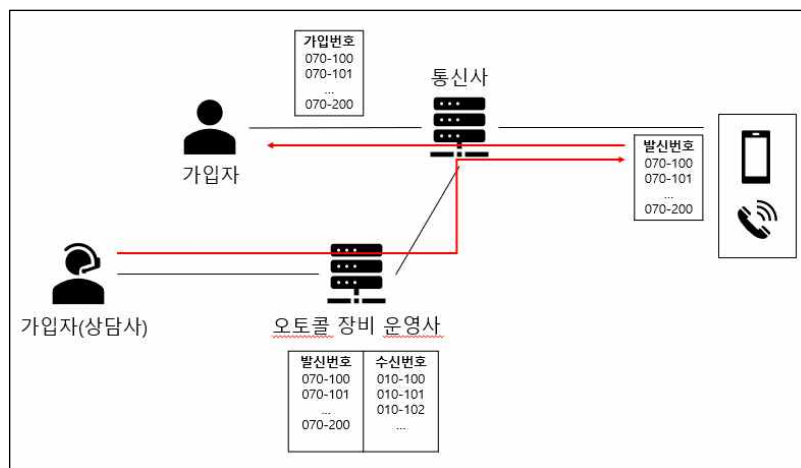
98) 세션개시프로토콜(SIP, Session Initiation Protocol)은 IETF에서 정의한 시그널링 프로토콜로 인터넷 환경에서 전화 통신과 유사한 서비스를 제공한다. Jonathan Rosenberg, “The Session Initiation Protocol: Internet-Centric Signaling”, IEEE, IEEE Communications Magazine 38(10), 2000, p.134

99) 한국인터넷진흥원(KISA) 휴대전화 부정이용 대응 연구반 회의 발표자료, “오토콜 프로그램 발신번호 변작서비스 이슈”, 2020.9.24.

100) 한국인터넷진흥원(KISA) 휴대전화 부정이용 대응 연구반 회의 발표자료, “오토콜 프로그램 발신번호 변작서비스 이슈”, 2020.9.24.

수신전화번호를 입력하고 입력된 번호로 다이얼링하는 기능을 수행한다.¹⁰¹⁾ 관리자(통신사) 프로그램은 개통된 발신전화번호를 서버에 입력하는 기능을 수행하고 통화내역 및 과금자료 등을 확인하는 역할을 한다.¹⁰²⁾ 오토콜 전화 발신 시 발신전화번호는 서버에 입력된 발신번호 중 하나를 지정하거나, 다수를 변경해가며 사용할 수 있다.

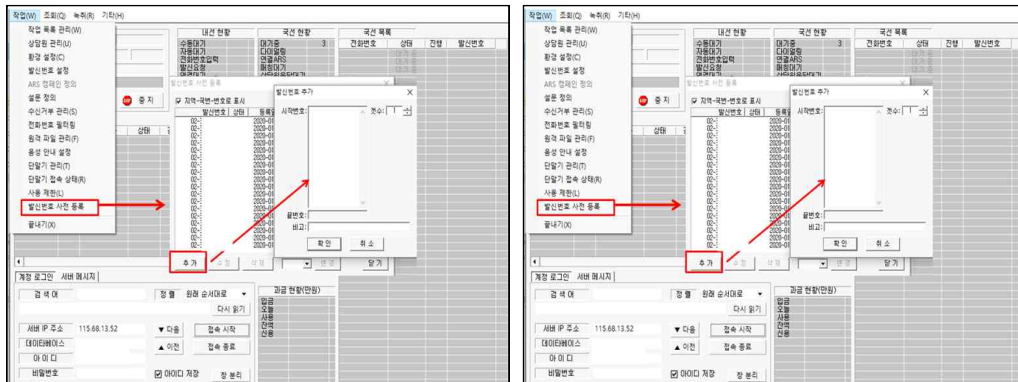
[그림 3-7] 오토콜 통화 흐름



(출처: KISA, “오토콜프로그램 발신번호 변작서비스 이슈”, 2020)

- 101) 한국인터넷진흥원(KISA) 휴대전화 부정이용 대응 연구반 회의 발표자료, “오토콜 프로그램 발신번호 변작서비스 이슈”, 2020.9.24.
- 102) 한국인터넷진흥원(KISA) 휴대전화 부정이용 대응 연구반 회의 발표자료, “오토콜 프로그램 발신번호 변작서비스 이슈”, 2020.9.24.

[그림 3-8] 오토콜 발신번호 설정 및 관리



(출처: KISA, “오토콜프로그램 발신번호 변작서비스 이슈”, 2020)

[그림 3-8]는 오토콜을 통한 발신번호 등록 방법 및 수신에 대한 프로세스를 표현한 것이다. 오토콜 서비스를 사용하는 절차는 다음과 같다.¹⁰³⁾

- ① 통신사는 가입자의 인터넷전화 가입서를 받아 070-100번~070-200번의 번호를 개통해주며, 오토콜발신 전화를 추가로 계약하게 된다.
- ② 통신사는 가입자의 이용 전화번호(070-100-070-200)를 오토콜 전화발신화선에 발신전화번호로 입력 표시한다.
- ③ 가입자(상담사)가 전화 발신을 하면 오토콜 장비 운영사를 통해 번호를 부여받고 통신사를 거쳐 수신자에게 전화를 걸게 된다. 이때 수신자의 핸드폰엔 오토콜 장비에서 부여된 발신번호가 표시된다.
- ④ 만약 수신자가 발신번호로 전화하게 될 경우, 실제 통화를 하였던 상담사는 전화번호가 없기 때문에 상담사와 연결이 불가능하다. (대부분 가입자가 콜백서버를 따로두어 ‘상담원이 통화중입니다.’ 라는 ARS음성안내를 한다.)

즉, 오토콜 전화 발신시 이용자가 입력된 발신전화번호 중 하나를 지정하여 표

103) 한국인터넷진흥원(KISA) 휴대전화 부정이용 대응 연구반 회의 발표자료, “오토콜 프로그램 발신번호 변작서비스 이슈”, 2020.9.24.

시할 수 있고, 입력된 발신번호가 100개이면 로테이션으로 변경해가면서 입력된 발신번호를 표시할 수 있다. 104) 오토콜을 사용한 보이스피싱 전화발신의 경우, 통신사에서 받은 가입서류는 대부분이 가짜이고, 실제 전화이용자의 물리적 위치가 특정되지 않는다. 105) 수신자측에서 모바일에 표시된 수신번호를 차단 및 신고처리를 하여도 오토콜 서비스 이용자는 다른 발신전화번호로 변경하여 해당 수신자에게 재발신이 가능하다. 106) 따라서 수신자의 조치 요청에 따라 발신번호가 차단되더라도 대량의 다른 발신번호로 쉽게 변경이 가능하기 때문에 보이스피싱이나 불법스팸과 같은 불법전화 발신자가 오토콜을 사용한다.

6. 악성앱 운영

가. 악성앱 설치

신종 보이스피싱 수법 중 피해자의 모바일 내 악성앱을 설치하도록 유도하여 모바일을 악성코드에 감염시키는 행위가 빈번하게 발생하고 있다. 악성앱은 스미싱의 악성링크를 통해 설치되거나, 보이스피싱 사기범이 피해자에게 직접 설치하도록 유도하는 방법을 통해 피해자 모바일에 설치된다.

이때 사기범은 금융기관을 사칭하여 대환대출 시 필요한 절차라고 피해자를 속이거나, 수사관을 사칭하며 수사를 위해 관련 앱(APP)을 설치해야 한다며 피해자의 모바일에 악성앱 설치를 유도한다. URL, 도메인, IP주소 등을 알려주면서 관련 앱을 다운로드 받도록 하거나, 원격제어 앱을 설치하도록 한 뒤 사기범이 직접 피

104) 한국인터넷진흥원(KISA) 휴대전화 부정이용 대응 연구반 회의 발표자료, “오토콜 프로그램 발신번호 변작서비스 이슈”, 2020.9.24.

105) 한국인터넷진흥원(KISA) 휴대전화 부정이용 대응 연구반 회의 발표자료, “오토콜 프로그램 발신번호 변작서비스 이슈”, 2020.9.24.

106) 한국인터넷진흥원(KISA) 휴대전화 부정이용 대응 연구반 회의 발표자료, “오토콜 프로그램 발신번호 변작서비스 이슈”, 2020.9.24.

해자 모바일에 악성코드를 설치하는 경우도 있다.¹⁰⁷⁾ 이때 악성코드에 감염된 피해자의 모바일은 보이스피싱 사기범들의 대포폰으로 복제되기도 한다. 이런 경우 피해자의 문자수신함, 피해자 SNS 등으로 사생활을 파악할 수 있으며, 피해자의 상황에 맞춰 더욱 치밀해진 보이스피싱 범죄가 가능하다.¹⁰⁸⁾

사기범이 유포하는 악성앱의 경우 정상적인 금융앱과 같은 디자인으로 설계되어 있으며 피해자가 악성앱에 접속하였을 때 정상적인 금융앱과 다를 바 없는 이미지에 이질감을 느끼지 못하게 된다. 감염된 기기를 통해 은행을 사칭하는 사기범과 통화하여 확인해 보았을 때, 은행 업무시간(09시~16시) 이후에는 대출과 관련해서 상담을 진행하지 않았다.¹⁰⁹⁾ 다음날 오전에 전화를 부탁드린다고 공손히 대응하는 점을 보았을 때 사기범은 피해자를 기만하기 위해 많은 부분을 고려해 범죄활동을 하는 것으로 추정된다.¹¹⁰⁾

나. 발신번호 탈취

메시지로 전송된 악성코드 설치 링크 주소를 누르도록 하거나 음성통화로 악성앱을 설치하도록 유도하여 피해자의 모바일에 설치된 악성앱은 개인정보 및 피해자의 발신전화를 탈취한다. 피해자들이 본인의 모바일에 설치한 악성앱 내의 악성코드는 IMEI, SMS수신 내역 등 모바일 기기의 주요 정보를 악성앱과 연동된 서버

107) 경찰청 보도자료, “「앱(악성코드) 설치」 유도형 보이스피싱 주의 - 악성코드로 신고·확인전화까지 돌려받아 피해자 속여 -”, 2018.12.17.자

108) 충청투데이 보도(2020.9.16.), ““내 정보 너무 잘 알아” 악성앱 피싱으로 진보한 ‘보이스피싱’”,
<https://www.cctoday.co.kr/news/articleView.html?idxno=2094375> (2020.12.16. 최종확인)

109) 금융보안원 보고서, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018, 45면

110) 금융보안원 보고서, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018, 45면

로 유출시킨다.

피해자 모바일에 설치된 악성앱 내부엔 블랙리스트 전화번호가 들어 있으며 전국 금융기관과 금융감독원 등 보이스피싱 조직이 사칭하는 대표기관의 번호가 리스트화 되어 있다. 블랙리스트는 악성 앱이 설치된 이후, 리스트에 있는 대표기관 번호로 피해자에게 전화가 수신될 시 자동적으로 차단하게 된다. 포워드리스트 또한 금융기관과 국가기관 등 대표기관의 번호가 모두 포워드리스트 내에 포함되어 있고, 피해자가 리스트 내의 번호로 전화를 걸면 범죄자가 발신 전화를 가로채는 형태이다. 사기범들은 피해자에게 상황확인을 위해 금감원, 금융기관 등의 대표번호로 전화를 하도록 유도한다. 피해자는 사기범의 유도함에 따라 기관의 대표번호로 발신을 하지만 이미 악성코드에 감염되어있는 모바일로 인해 발신번호가 탈취되어 보이스피싱 내 다른 사기범으로 통화가 연결된다. 이렇게 피해자는 자신도 모르는 사이에 보이스피싱 사기범에게 기망되어 사기범이 요구하는 대로 지시를 따르게 된다.

7. 자금세탁

가. 현금인출 · 수거

보이스피싱은 점조직 형태로 이루어져 있기 때문에 인출책, 수거책들 조차 누가 어떤 역할을 하는지 서로 전혀 모르는 상태이다. 보이스피싱 조직은 현금을 인출 및 이체, 수거하기 위해 주로 단기 고액알바를 광고를 통한 현금인출책 인원을 모집한다. 현금인출 시 계좌주의 계좌개설 설정에 따라 한 계좌에서 현금을 인출하거나 이체하는 경우 범죄예방을 위한 한도금액이 정해져 있는 것이 일반적이다. 따라서 알바 광고를 통해 모집된 일반인들은 보이스피싱의 중간책 지시에 따라 여러 계좌를 사용하여 현금을 이체 및 인출하게 되고, 중간책은 이러한 지시를 위해 카카오톡이 아닌 보안 기능이 접목되어 있는 텔레그램과 위챗을 사용한다. 특히

텔레그램은 외부에서 대화내용의 접근을 방지하기 위해 대화 암호화, 비밀삭제 등 보안성이 강력한 기능들을 소유하고 있다. 이는 경찰이 인출책과 수거책을 검거하여도 대화내용을 보호하는 보안 기술력으로 인해 보이스피싱 사기범들의 관계 및 중심 조직원의 범죄혐의를 입증하기 어려워져 수사에 큰 방해가 된다. 최근, 보이스피싱 범죄에 무분별하게 사용되는 현금인출기(ATM)가 점점 사라지고 있는 추세이다.¹¹¹⁾ 최근 6년간 현금인출기는 1만여 대의 수가 줄었고, 현금인출기 이용자의 감소로 수수료 수익이 급감하여 유지비 충당을 못해 은행의 손실도 커져가고 있다. 그러나 노년층의 이용을 위해 기기수를 줄이지 말라는 정부의 입장으로 전체 철거가 이루어지지 않아 아직까지 보이스피싱 조직이 현금인출기를 이용해 현금 인출이 가능하다. 하지만 추후 전국에서 현금인출기가 사라질 경우 보이스피싱 사기범의 피해금액 탈취가 현금인출이 아닌 또 다른 방식으로 진행될 것에 대해 고려해볼 필요가 있다.

나. 구매대행

해외에서 구매대행을 목적으로 업체에 의뢰가 들어오면 피해금으로 의뢰 물품을 구매하고, 의뢰인에게 물품을 전달하여 이익을 확보하는 방식이다. 따라서 피해금액은 물품 구매비로 소비하고 이익을 취하는 금액은 정식으로 구매대행을 요구한 의뢰자의 합법적인 자금으로 세탁된다. 이 형태는 피해금이 해외로 빠져나가지 않고 국내에서 머무르게 한다.

보이스피싱 조직이 세운 구매대행 업체는 해외송금을 대행할 직원을 모집한다는 광고를 통해 차명 계좌를 확보한다. 고액 아르바이트라는 조건으로 모집된 계좌주에게 보이스피싱 조직원은 자신을 외주사업팀장으로 소개하며 “구매자들로

111) 한국경제 보도(2020.9.5.), “없애고 싶은데...은행 ‘애물단지’ 된 ATM”, https://www.hankyung.com/economy/article/2020090457311?fbclid=IwAR1dFBhT_B3xjyi8P9eCGZhXkUXUbyM5CW6CgHN69fo1XofBTej7CvWjYvs (2020.10.10. 최종확인)

부터 수금한 구매대금을 당신의 계좌로 보내줄 테니 구매 결제를 위해 캄보디아 현지업체로 송금해두면 된다” 라고 설명한다. 계좌주는 송금액의 2%를 주겠다는 말에 현혹되어 자신의 계좌로 입금된 자금을 모바일 뱅킹 애플리케이션을 통해 조 직원에게 송금한다.¹¹²⁾

다. 면세품

보이스피싱에서 구매대행을 위한 중간매체로 면세점에서 면세품을 구매하는 것을 확인 후 검거하였다. 외국인의 경우 국내 시내 면세점에서 물건을 구매할 때 여권과 항공권만 확인하면 곧장 물건을 준다는 점을 노렸다. 중국인 유학생들을 SNS로 모집해 국산 유명 브랜드 화장품을 면세점에서 대리 구매시킬 후 이를 중국으로 밀수출해온 중국인 중간 판매자 2명을 체포했다. 이들은 중국인들이 자주 사용하는 SNS에 국산 화장품 대리구매 알바생을 모집한다고 글을 올리거나 기존에 화장품 구매를 담당하던 중국인 유학생들을 대상으로 삼았다.

112) INFOSTOCK DAILY 보도(2019.11.15.), “'알고보니 보이스피싱 범죄'... 금감원 ‘해외송금 알바’ 소비자 주의 발령”,
<http://www.infostockdaily.co.kr/news/articleView.html?idxno=78356>
 (2020.12.14. 최종확인)

[그림 3-9] 자금세탁을 위한 면세점 대리구매 절차



(출처: KBS 뉴스, “유학생 대리 구매...면세 화장품 中 밀수출”, 2020)

보이스피싱 조직책들은 면세점에서 화장품을 구입한 후 항공권을 취소하는 수법을 사용하였다. 내국인의 경우 시내 면세점에서 물건을 구매한 뒤 공항 출국장에서 받지만, 외국인의 경우 국내 면세점에서 면세품을 구매하면 곧장 물건을 해외 배송지로 발송해 주는 서비스를 애용했다.¹¹³⁾ 일반적으로 면세점 직원은 면세품 구매 고객이 실제로 출국했는지에 대한 사실 여부를 확인한 후 EMS로 면세품을 구매고객이 원하는 발송지로 발송해야 하지만, 보이스피싱 관계자는 비행기 티켓만 구매한 후 출국은 하지 않아도 면세점 측에서 면세품을 해외로 발송한 것이다. 즉, 면세점에서 제대로 확인하지 않고 면세품을 배송하였을 것이라는 예상이 가능하고, 면세품으로 보이스피싱을 통한 불법수익에 대한 자금 세탁을 원활하게 만들 수 있는 환경이 조성된 것이다.

라. 환전소

113) KBS 뉴스 보도(2017.4.28.), “유학생 대리 구매...면세 화장품 中 밀수출”, <http://mn.kbs.co.kr/mobile/news/view.do?ncd=3472162> (2020.12.14. 최종확인)

환전소에서 통화를 교환하듯 중간에서 환전상 역할을 하며 피해금을 해외계좌로 송금하는 사례이다. 한국에서 원화를 받으면 환전상이 중국에 있는 동업자에게 연락해 현지에서 위안화를 고객계좌로 이체시켜주는 방식을 사용한다. 이 방식은 구매대행과 마찬가지로 환전소를 차려 실제 환전업무와 돈세탁 업무를 섞어가며 진행한다. 중국 보이스피싱 조직원은 한국 계좌로 송금한 자금을 중국 계좌로 대신 송금해주면 환전 금액의 1.6%를 수수료로 받기로 했다. 조직원은 총 7회에 걸쳐 1억 6,450만원을 환치기 수법으로 중국 은행에 송금하던 중 추적에 나선 경찰에 덜미가 잡힌 사례가 있다.¹¹⁴⁾ 또한, 관세청에서는 가상통화를 이용한 신종 환치기 수법을 적발하였다. 종전까지 발생한 환치기 사건의 경우 양국 간 환치기계좌에서 거래대금을 상호 상계하는 것을 일반적으로 하였고, 잔액 부족이 발생할 경우 이를 보충할 목적으로 불법적으로 휴대 반출하거나 은행을 통해 송금해왔다. 반면, 관세청에 적발된 가상통화 환치기의 경우 환치기 계좌 잔액이 부족할 경우 가상통화를 송금하거나, 환치기업자가 수수료로 가상통화를 수수하는 사례가 있다. 추가적으로 가상통화 구매를 위해 해외에 페이퍼 컴퍼니를 설립한 후 무역계약을 체결해 송금하는 등 신종 수법이 드러나고 있다.¹¹⁵⁾

114) NEWSIS 보도(2020.3.2.), “보이스피싱 1억6450만원, 환치기로 중국에 빼돌린 20대 실형”, <https://news.v.daum.net/v/20200302111716381> (2020.12.14. 최종확인)

115) 한국세정신문 보도(2018.2.1.), “관세청, 가상통화 이용 신종 환치기 수법 적발”, <https://www.taxtimes.co.kr/news/article.html?no=235453> (2020.12.14. 최종확인)

[그림 3-10] 가상통화 환치기 흐름도



국내 불법 환치기는 보이스피싱 범죄와 연루되면서 그 규모가 더욱 늘어나고 있다. 금융당국의 단속에도 환치기 범죄가 사라지지 않는 이유는 불법 환전소 때문이다. 특히 국내 체류 중인 중국인의 경우 SNS 등을 통해 자유롭게 환전, 송금 등이 이루어진다. 적발 건수에 비해 환치기 규모가 커진 것도 눈에 띄는 대목이다. 환치기 송금 방식은 한국에서 원화를 받으면 환전상이 중국에 있는 동업자에게 연락해 현지에서 위안화를 고객계좌로 이체시켜주는 방식이다. 이 방법은 실질 해외송금이 일어나지 않고 해외송금 효과를 보게 된다. 하지만, 실제 환전이 일어나지 않으므로 거래비용이 없고 유리한 환율을 적용받게 된다. 환치기 송금은 외국 환거래법의 적용을 피하고 외환통계에는 잡히지 않는 불법행위이다. 따라서 외환시장의 음성화를 유발할 수 있고 재산은닉이나 사기 송금, 보이스피싱 송금 등 각종 범죄행위에도 연루될 수 있다.¹¹⁶⁾

116) 뉴데일리경제 보도(2019.3.14.), “불법 환치기 적발건수 2배 증가...규모도 1조3천억원”,
<http://biz.newdaily.co.kr/site/data/html/2019/03/13/2019031300255.html>
 (2020.12.14. 최종확인)

마. 암호화폐

최근 비트코인 등 가상화폐를 악용하여 대포통장 없이도 거액의 피해금을 인출하는 등 보이스피싱 범죄자들의 범죄수법이 진화하고 있다.¹¹⁷⁾ 이처럼 보이스피싱 범죄자들이 자금세탁을 할 경우, 암호화폐와 같은 디지털 자산을 활용하여 수사기관의 추적을 피할 수 있다. 암호화폐는 중앙에 신뢰할 수 있는 기관(TTP: Trusted Third Party)이 없고, 네트워크의 참여자들이 공동으로 원장을 관리하는데 혁신이 있다고 할 수 있다.¹¹⁸⁾ 암호화폐는 중앙 신뢰기관이 없다 보니 수사를 위한 용의자 정보를 확보하는 것이 어렵고, 나아가 지급 정지도 불가능하다. 암호화폐가 등장한 이후 새로운 비즈니스 모델로 암호화폐거래소가 등장하였고, 암호화폐거래소를 이용하는 경우 개인정보, 송금정보, 접속기록 등을 확보하여 거래소 이용자를 추적할 수 있게 되었다. 또한 암호화폐거래소는 수사기관의 요청에 의하여 계좌에 대해 지급정지를 하기 때문에 과거와 달리 자금세탁이 어려워졌다. 하지만 입출금 기능은 없고 이체 기능만 있는 소프트웨어에서 암호화폐 주소를 생성하거나 해외 암호화폐거래소를 이용하여 자금세탁을 하는 경우에는 추적이 어렵다. 암호화폐의 거래내역을 섞는 믹싱(Mixing) 서비스를 이용하는 경우에도 마찬가지다.

117) 방송통신위원회 보도자료, “대출을 권유하는 사기 전화나 문자메시지에 주의하세요”, 2017.9.18.자

118) 자세한 내용은 Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system“, 2008, pp.1-9

제3절 신종 보이스피싱 대응기술

1. 개괄

연구진은 보이스피싱 범행수법을 바탕으로 범행수법을 크게 8가지로 분류하였다. 즉, ① 발신번호변작 차단·탐지, ② 네트워크 패킷분석, ③ 통신패턴분석, ④ 심박스 전파탐지(3G·4G), ⑤ 음성인식(범죄자 음성인식, 피해자 음성·감정인식), ⑥ 텍스트추출, ⑦ 악성앱 탐지(악성앱 분석, 악성링크 탐지), ⑧ 데이터 분석(SNA 분석, 금융계좌분석, 암호화폐추적) 등으로 세분화하였다. 세부 내용은 다음과 같다.

<표 3-12> 보이스피싱 대응기술

대응기술		세부내용
① 발신번호변작 차단·탐지		· 범죄자가 발신번호를 변작하여 통화연결을 시도하는 행위에 대한 탐지·차단 기술
② 네트워크 패킷분석		· 패킷헤더에서 ① 발신을 어디로 했는지에 대한 발신번호(피해자 번호), ② SIM Bank, SIM Box의 IP주소, ③ IP-PBX의 IP주소, ④ 실시간 음성 등을 수집하여 탐지하는 기술
③ 통신패턴분석		· 보이스피싱 범행시 보여지는 통신 특징을 분석 후, 패턴을 모델링하여 탐지하는 기술
④ 심박스 전파탐지	3G 전파탐지	· 전파탐지연구소의 Analyzer, 스펙트럼 분석기로 3G 미세 신호를 확인하여 심박스의 설치장소를 탐지하는 기술 · 차량에 심박스를 싣고 이동하는 범행형태는 탐지 곤란
	4G 전파탐지	· 전파신호 탐지의 길이(거리)가 짧고, 신호 사용자가 많은 4G(LTE) 심박스 탐지에 한계 · 4G(LTE)를 3G로 다운그레이드하여 탐지하는 방식 검토 가능

⑤ 음성인식	범죄자 음성인식	<ul style="list-style-type: none"> · 화자인식 방법을 통해 범죄자의 음성 성문군집을 생성하여 동일인의 음성을 식별하는 기술 · 음성 확보 및 녹음의 어려움, 노이즈가 포함된 음성인식 한계 등
	피해자 음성·감 정인식	<ul style="list-style-type: none"> · 피해자 음성의 감정을 분석하여 보이스피싱을 탐지하는 기술 · 피해자 스스로 설정할 수 있어 범죄자 음성에 비해 사용 용이
⑥ 텍스트추 출	음성에서 텍스트 추출	<ul style="list-style-type: none"> · 범행에 사용되는 전화번호, 계좌번호의 연계데이터를 시각화, 관계분석 등을 통해서 보이스피싱 탐지하는 기술 · IBK피싱스탑, 후후컴퍼니, 피싱아이즈 등에서 활용
⑦ 악성앱 탐지	악성앱 분석	<ul style="list-style-type: none"> · 악성앱의 코드를 분석하여 악성여부를 판단하여 탐지하는 기술
	악성링크 탐지	<ul style="list-style-type: none"> · SMS 분석을 통해서 보이스피싱 여부를 탐지하는 기술
⑧ 데이터 분석	SNA 분석 (i2)	<ul style="list-style-type: none"> · 중심성 원리와 하위집단분석원리를 중심으로 사회연결망 분석(SNA) 알고리즘을 반영한 수사기술
	금융 계좌분석	<ul style="list-style-type: none"> · 금융계좌 분석을 통해서 자금세탁, 범죄수익은닉 등을 찾아내는 기술
	암호화폐 추적	<ul style="list-style-type: none"> · 비트코인, 이더리움 등 암호화폐를 추적·분석하는 기술

2. 발신번호 변작 차단·탐지

보이스피싱에서 사용하는 발신신호는 주로 IP-PBX를 거쳐 이동통신사의 인터넷 전화 서비스를 이용한다. IP-PBX란 인터넷 상에서 음성, 데이터, 멀티미디어 환경을 종합적으로 지원하는 IP(Internet Protocol) 기반의 사설교환기(PBX: Private Branch eXchange)이다.¹¹⁹⁾ IP-PBX는 IP전화 서비스를 제공하는 기업용 음성 통신

119) 조성호, 최성욱, “IP-PBX를 이용한 혼합형 전화통신망과 IP-Phone 망과의 비교연구”, 융복합지식학회, 융복합지식학회논문지 6(2), 2018, 21면

시스템이며, 인터넷 상에서 음성전화뿐만 아니라 데이터 통신 및 멀티미디어 환경을 종합적으로 지원하는 장비이다. IP-PBX를 통한 통신은 일반 사업자의 업무목적 사용 및 서버 데이터 처리 등 여러 가지 이용 목적이 존재한다. 따라서 이동통신사의 입장에서 IP-PBX로 들어오는 신호만으로 통신서비스 부정사용인지 아닌지의 여부를 확인하는 것이 어렵다. 또한 이동통신사에서 기술적으로 IP-PBX를 통한 인터넷 전화 신호를 자체적인 기준을 세워 국가별로 큰 틀을 구분하는 것은 가능하지만, 사용자 정보 및 이용 목적과 같은 통신 내 세부 정보를 특정할 수 있는 신호 데이터를 구분하지는 못한다. 즉, IP-PBX의 신호만으로 보이스피싱 조직이 통신서비스를 부정하게 사용하였는지 명확하게 알 수 없다.

현재, 이동통신 3사와 KISA는 휴대전화 스팸 트랩 시스템(Spam trap system)을 운영하고 있다.¹²⁰⁾ 이 시스템은 개통 이력이 없는 휴대전화 번호가 통신을 시도하는 행위를 잡아내는 것으로, 2006년부터 실행되었다. 이동통신사 측에서는 고객에게 할당(개통)하지 않는 전화번호를 목록화하여 가지고 있다. 만약 이동통신사에서 고객에게 지원하지 않는 번호를 사용하여 누군가 계속 전화나 문제를 발신한다면 해당 번호는 통신 부정사용을 하려는 목적이 있다고 볼 수 있어 차단을 진행한다. 즉, 스팸 트랩 시스템은 개통 이력이 없는 번호라는 덫을 설치하여 통신 행위를 자동으로 저장 및 분석하여 불법스팸을 잡아내는 것이다. 스팸트랩의 전화번호로 불법스팸과 같은 통신을 실행할 경우, 정보통신망법 제50조의 4 제1항 수신자의 사전동의 의무 위반, 정보통신망법 제50조의 5 제2항 영리광고 전송 목적을 위한 전화번호 자동 등록 등의 위법행위를 발생한다. 따라서 관계부처는 스팸 트랩에 탐지되는 발신자를 추적해 번호 정지, 수사의뢰 등의 조치를 취한다.¹²¹⁾ KISA

120) 컴퓨터월드 보도(2014.12.26.), “KISA, 휴대전화 스팸 트랩 번호 대폭확대…불법 스팸 근절”,
<http://www.comworld.co.kr/news/articleView.html?idxno=48640> (2020.12.14. 최종확인)

121) 컴퓨터월드 보도(2014.12.26.), “KISA, 휴대전화 스팸 트랩 번호 대폭확대…불법 스팸 근절”,

불법스팸대응센터의 2015년 하반기 자료에 의하면 2015년 7월에서 12월까지 5개월 동안 한국인터넷진흥원으로 신고되거나 스팸 트랩 시스템에 필터링 된 스팸 메시지는 총 262만 건이었다. 스팸 트랩 시스템은 발신번호변작의 여부 뿐 만 아니라, 짧은 시간 동안 발신을 계속적으로 시도하는 오토콜을 탐지 할 때에도 사용된다.

3. 네트워크 패킷분석

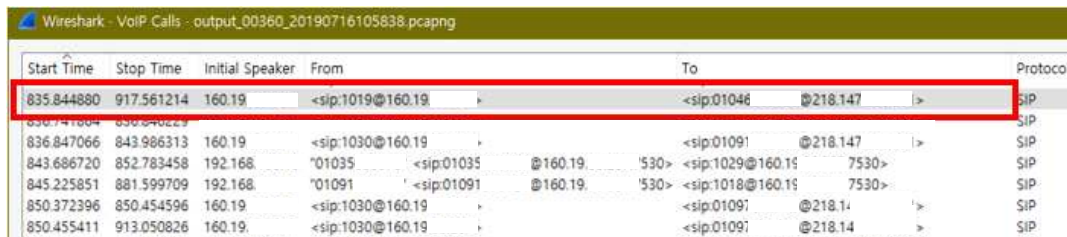
인터넷에서는 정보를 전달하는 기본 단위는 패킷(packet)으로, 패킷은 송신자가 보내고자 하는 데이터와 목적이 주소를 포함하여 네트워크를 통해 목적지까지 전달한다.¹²²⁾ 보이스피싱 사기범이 사용하는 심박스의 경우 인터넷 전화를 사용하기 때문에 음성통화시 네트워크 패킷이 발생한다. 따라서, Wireshark를 이용하여 패킷을 모니터링 할 수 있고, 패킷의 헤더를 분석하면 보이스피싱 범죄자를 특정할 수 있는 데이터를 획득할 수 있다. 네트워크 패킷 분석 시 확인할 수 있는 데이터는 총 4가지이다. 첫 번째로 통화를 통해 오고가는 사기범과 피해자의 음성을 들을 수 있다. 두 번째로 사기범의 발신지 정보와 최종 목적지(피해자)의 010 번호를 알 수 있다. 세 번째로는 심박스와 심뱅크(SIM Bank)의 IP를 알 수 있다. 국외에 설치된 실제 유심이 꽂혀있는 심뱅크와 VoIP Gateway 형태로 유심 없이 국내에 설치된 심박스는 주기적으로 통신하기 때문에 통신기록을 확인하면 신호 발생지인 심뱅크와 신호 수신지인 심박스의 IP를 추정할 수 있다. 마지막으로 IP-PBX의 IP를 알 수 있다. IP-PBX의 경우 다수의 원격 게이트웨이를 관리하고, 보이스피싱 조직원의 전화신호를 심박스와 연동시켜준다. 이때, 자신의 정확한 위치를 알리는

<http://www.comworld.co.kr/news/articleView.html?idxno=48640> (2020.12.14. 최종확인)

122) 우동연, 박세웅, “모바일 기가 통신 : MPTCP 기반 LTE/Wi-Fi 묶음 기술”, 한국통신학회, 정보와 통신 열린강좌 33(12), 2016, 21면

레지스터(Register) 정보를 패킷에 함께 실어 통신하게 된다. 발신(From) 패킷의 형태는 ‘IP-PBX 레지스트리 번호@IP-PBX IP주소’ 이다.

[그림 3-11] 심박스 패킷



Start Time	Stop Time	Initial Speaker	From	To	Protocol
835.844880	917.561214	160.19	<slp:1019@160.19>	<slp:01046 @218.147>	SIP
836.847066	843.986313	160.19	<slp:1030@160.19>	<slp:01091 @218.147>	SIP
843.686720	852.783458	192.168	'01035' <slp:01035 @160.19>	'530' <slp:1029@160.19>	SIP
845.225851	881.599709	192.168	'01091' <slp:01091 @160.19>	'530' <slp:1018@160.19>	SIP
850.372396	850.454596	160.19	<slp:1030@160.19>	<slp:01091 @218.14>	SIP
850.455411	913.050826	160.19	<slp:1030@160.19>	<slp:01091 @218.14>	SIP

(출처 : 트루네트웍스, 2019)

[그림 3-11]의 경우 발신 패킷헤더 주소는 ‘1019@160.19.0000.0000’ 이며 수신지는 ‘01046xxxxxx@218.147.0000.0000’ 이다. 여기서 발신 패킷헤더의 IP-PBX의 레지스트리 번호는 1019이며, IP주소는 160.19.0000.0000이다. 또한 수신주소의 ‘01046xxxxxx’ 은 피해자의 번호가 된다.

하지만 심박스 패킷 분석의 경우 모니터링이 이루어져 심박스의 위치를 추적한 다 할지라도 현재 실제 유심이 꽂혀있는 심뱅크는 국외에 설치되어 있는 경우가 많기 때문에 심뱅크 압수를 위한 국제공조 프로세스가 필요하다. 실시간 패킷의 모니터링은 네트워크 주소뿐만 아니라 주고받는 음성통화 확인이 가능하고, 이는 감청여부의 소지가 있다는 한계가 있어 실제 대응기술로 활용하기에는 많은 한계가 있다.

4. 통신패턴분석

통화내역기록 서비스인 CDR(Call Detail Reporting) 기술은 과금할 목적으로 특정 내선번호나 가입자 그룹에 대한 통화 세부 내역 데이터(발신 번호, 착신 번호, 통화량, 통화 시간 등)를 수집하고 기록하는 서비스이다.¹²³⁾ CDR 기술은 음성 데

123) 정보통신기술용어해설 홈페이지, CDR Call Detail Reporting,

이터에서 통화 세부 내역 데이터를 수집하여 분석할 수 있도록 한다. 현재 해외에서는 CDR 기술을 활용한 기술 연구가 활발히 진행 중이다. 모바일 네트워크에서 국제 음성 트래픽의 통화 내역을 분석에 기간을 선정하여 트래픽 프로파일을 만들 수 있다.¹²⁴⁾ 미국의 GL회사는 통신 회사에서 생성한 많은 통화 데이터(CDR)을 활용하여 통화가 도중에 갑자기 끊어지는 등의 통화 사고를 막기 위해 CDR 분석 시스템을 적용하였다.¹²⁵⁾ GL에서 개발한 CDR 분석 시스템은 TDM, IP 또는 무선 통신과 같은 모든 네트워크 유형에서 통화 중 발생하는 모든 데이터를 수집하도록 설계하였다. 이를 활용할 경우 보이스피싱 뿐만 아니라 실제 통화 중에 있어서도 통화(음성) 데이터를 분석할 수 있을 것이다. 음성 데이터에 대한 정보를 수집하는 기술이 고안되어 있기 때문에 이러한 데이터를 패턴화, 모델링 작업을 거쳐 탐지하는 것이다.¹²⁶⁾ 해당 기술은 행위에 대한 이상징후를 감시하기 위해 행위를 기반하여 탐지하는 시스템에 관한 기술로, 특정 행위를 추출하고 행위에 대해 수치화한 후 패턴화하여 등록한다. 결과적으로는 해당 시스템을 이용하면 들어오는 정보에 대해 분석된 모델로 검토하여 이상징후를 탐지할 수 있기 때문에 이동통신사에 도입하면 음성을 분석하여 패턴을 모델링화하여 차단할 수 있을 것이다.

보이스피싱 의심 번호 발견 시 이동통신사에서 자체적으로 해당 통신을 끊을 수 있으나, 이동통신사가 직접적으로 처리할 경우 법적인 논란이 발생할 수 있다. 보이스피싱 사기범에게 기망 당한 피해자는 피해 내용을 이동통신사가 아닌 경찰에

http://www.ktword.co.kr/abbr_view.php?m_temp1=2567 (2020.10.24.최종확인)

124) Z. Aziz, R. Bestak, “Analysis of Call Detail Records of International Voice Traffic in Mobile Networks“, IEEE, 2018 10th International Conference on Ubiquitous and Future Networks (ICUFN), 2018, 475면

125) GL Communications Inc., Analysis of Call Detail Records(CDR) using Excel Addin, <https://www.gl.com/call-detail-records-analysis-tools.html> (2020.10.24. 최종확인)

126) 최병환, “네트워크 세션 행위 패턴 모델링 탐지방법 및 모델링탐지시스템”, KR20140055762A, 2014.6.20.

게 먼저 신고한다. 신고접수를 받은 경찰은 과학기술정보통신부(이하 과기부)에 이용정지를 요청하며, 이동통신사나 KISA에 보이스피싱에 사용된 번호에 대한 이용정지를 직접 요청하기도 한다. 이러한 과정을 거쳐 최종적으로 이동통신사에서 해당 번호를 정지하게 된다. 위의 절차에서 알 수 있듯이 해외에서 들어오는 일반 전화의 신호 또한 이동통신사의 주관적인 판단으로 통신차단을 진행할 수 없다.

실제 유사한 사례가 실무에서 활용되고 있다. 전화 알림음을 한번 울리고 끊어 부재중전화 알림으로 상대로 하여금 궁금증을 불러일으킨 후 소비자들에게 각종 광고 등으로 유도하는 ‘원링콜’은 대부분 해외전화로 사용된다. 이때 이동통신사가 확인하여 전화번호 1개당 1천 건 이상의 음성 통화를 시도하는 전화번호를 실시간 모니터링 하여 해당 번호가 스팸으로 유도하는 전화일 경우 자동으로 정지시키는 서비스가 실행 중이다.¹²⁷⁾ 결과적으로 스팸이나 보이스피싱에 사용되는 ‘오토콜’ 서비스는 통화연결 유지시간이 짧아 이동통신사 입장에서 보이스피싱에서 발생하는 신호인지를 인지할 수 있을 것으로 보인다.

5. 심박스 전파탐지

가. 3G 전파탐지¹²⁸⁾

수사기관이 3G 통신을 이용하여 심박스의 위치를 추적하는 기술을 이해하기 위해서는 먼저 수사절차에 대한 이해가 필요하다. 수사기관은 중앙전파관리소와 협조하여 보이스피싱에 이용되는 심박스의 전파를 탐지하여 범인을 검거한다. 수사기관은 통신회사로부터 중계기 위치를 확인하고 스펙트럼 분석기(전파탐지기) 등을

127) 베타뉴스 보도(2008.8.18.), “원링콜 차단 정책, 효용정은 ‘글세?’”, <https://news.joins.com/article/3264308> (2020.12.14. 최종확인)

128) 이하의 내용은 이진(투루네트웍스) 경찰수사연수원 강의자료 “보이스피싱 심박스 추적수사”, 2019에서 발췌

활용하여 지속적으로 전파가 발생하고 있는 특정위치를 탐지한다.

이 때, 피해자의 신고를 받아 진행하는 심박스 탐지 과정은 다음과 같다. 심박스 탐지과정은 ① 전화번호를 할당한 통신사 협조로 전화번호에 할당된 IMSI 도출, ② IMSI 또는 TMSI로 해당 단말(ME)의 IMEI 도출, ③ GSMA 또는 국내 통신사에 등록된 IMEI로 단말 종류 추정, ④ 해당 ME가 접속한 중계기 또는 기지국 반경을 중심으로 삼각 측량하여 접속위치 도출, ⑤ 도출된 위치의 건물을 특정 후 휴대용 계측기를 이용한 방향 탐지/탐문수사의 순으로 진행된다.

보이스피싱 피해자가 최초 피해신고 접수 시 경찰은 먼저 범죄에 사용된 전화번호(010)의 통신사를 확인한다. 별정통신사 대상으로 일일이 전화를 걸어 해당 별정통신사의 회선인지 확인한 후에 통신자료제공요청서를 발송하게 된다. 확인된 통신사 대상으로 통신자료제공요청하여 해당전화번호의 가입자를 확인한다. 긴급통신사실확인자료 제공요청을 해야 하기 때문에 사건접수 이후 피해조서를 작성하자마자 통신자료를 회신 받아야 한다. 범행에 사용된 전화번호 가입자를 확인하고 즉시 긴급통신사실확인자료 제공요청을 한다. 범행에 사용된 전화번호의 발신기지국실시간위치추적과 발신통화내역(발신기지국 위치 포함)을 요청한다. 미리 허가를 받지 못한 사유를 작성하며 보이스피싱 범행에 사용된 전화번호는 모두 선불대포폰임을 함께 기재한다. 추가적으로 유심칩으로 요금이 소진되거나 범행에 성공하여 대포폰이 이용정지 상태가 될 경우 추적이 불가능한 긴급한 사유도 기재한다. 발신기지국위치추적 회신기간을 초과할 시에는 청구가 기각된 사례가 있기 때문에 2~3일로 기재한다.

이후 발신지역 범위를 특정하기 위하여 집행 회신 문자를 활용하여 전화번호가 현재 살아 있는지 여부를 파악하고 나서 경찰청의 자체 애플리케이션을 통해 PN 값에 해당하는 지역을 확인하여 실제 중계소 위치를 파악한다. 파악된 거점에 도착하면 전파탐지기를 이용하여 해당 구역 내부를 수색한다. 보이스피싱 조직책들은 대부분 원룸 및 오피스텔을 임차하여 운영하기 때문에 높은 층에서부터 호실별로 일일이 탐방하여 수색해야 하는 어려움이 있다. 현장에서 수사기관은 심박스가

존재할 것으로 예측되는 후보 위치에서 전파가 발생하는 위치를 찾을 때까지 계속 이동해야 한다. 이는 심박스가 3G, 4G(LTE) 별로 통신하는 방식에 따라 탐색하는 면적의 크기가 다르기 때문이다. 전파탐지기는 과학기술정보통신부 산하 중앙전파관리소를 비롯하여 각 지역 전파관리소에서 운용하고 있는 장비이고, 전파관리소 특사경과의 공조 수사도 가능하다. 전파관리소 특사경은 전파법(제71조의 2 제2항)상 출입·조사권을 가지고 있다.

본론으로 들어가서 3G 네트워크는 3GPP(3rd Generation Partnership Project)라는 표준화 기구에서 제정한 UMTS(Universal Mobile Telecommunication System) 표준안을 따르는 네트워크를 의미한다.¹²⁹⁾ 3G의 경우 신호 반경이 100m~3km로 넓어 탐색 반경에 대한 정확도가 낮다는 단점이 있지만 LTE가 보급이 되어 있어 3G 통신의 신호발신지는 쉽게 찾을 수 있다. 전파연구소에서 사용하는 추적기인 Analyzer, 스펙트럼 분석기를 동원하여 후보 위치에서 발생하는 3G 미세신호를 확인할 수 있다. 보이스피싱 단속시 3G(WCDMA) 기반의 심박스(모바일 게이트웨이)가 활용되고 있고, 3G 사용 단말은 상대적으로 소수인데 반해 심박스는 특정 장소에서 다수의 통화가 일어나기 때문에 탐지가 가능하다. 보이스피싱 범죄로 추정되는 신고된 번호 수집하고 통신사 협조를 통해 수집된 번호의 실시간 위치 추적을 진행하고, 발신기지국 확인 후에는 반경을 좁혀 심박스의 3G신호 전파탐지를 한다.

129) NAVER D2 (2012.7.25.), “3G 모바일 네트워크의 이해”,
<https://d2.naver.com/helloworld/111111> (2020.10.24. 최종확인)

나. 4G 전파탐지

4G(4세대) 이동통신은 3세대 이동통신인 IMT-2000의 후속 이동통신서비스를 지칭하는 말로, 3G보다 최대전송속도가 10배 이상 빠른 서비스이다.¹³⁰⁾ 4G LTE는 동시에 ‘변조’ 및 ‘다중화’를 수행하는 전송 기법인 OFDM 방식¹³¹⁾ 사용으로 신호가 불연속적이고 주파수 대역이 넓어 탐지가 쉽지 않다. 보이스피싱 사기범들은 4G Router를 이용하여 4G(LTE) 신호를 사용하는데, 이로 인해 신호 반경이 5m 이내로 탐색 반경에 대한 정확도가 높아진 반면 일반적인 모바일 인터넷 신호 역시 4G(LTE)를 사용하기에 탐지율이 떨어진다.¹³²⁾ 또한, 최근 4G(DFDM) 기반 심박스가 등장하고 가격이 하락하여 보이스피싱에 활용되는 사례가 증가할 것으로 예상된다. 4G 신호기반 심박스 사용 범행이 증가하여도 OFDM 신호의 특성으로 인해 현 기술로는 위협 신호를 탐지할 수 없는 것이 현실이다.¹³³⁾ 이에 따라서 이동통신 표준 규격 분석을 통해 이동통신 기반으로 보이스피싱에 사용되는 4G 신호에 대한 추적기술이 필요하다.

이러한 상황을 극복할 수 있는 방법은 4G를 3G로 다운시켜 심박스의 위치를 추적하는 방법이 있을 것이다. 이러한 방법은 아이디어 상으로만 논의되고 있고 실제 수사현장에서 접목한 적이 없고, 통신사 역시 통신방식을 다운시키는 것이 시스템적으로 가능한지에 대한 검토가 없었다. 만약 4G를 3G로 다운시키는 것이 기술적으로 가능하다면 압수수색 영장 등 법적 근거에 대한 검토를 진행해야 할 것이다.

130) 표학길, “4G에 대비한 정보통신정책”, 한국통신학회, 한국통신학회지(정보와통신) 19(7), 2002, 102면

131) 정보통신기술용어해설 홈페이지, OFDM Orthogonal Frequency Division Multiplexing 직교 주파수 분할 다중화, OFDM 기술, OFDM (2020.08.10.), http://www.ktword.co.kr/abbr_view.php?m_temp1=2163 (2020.10.24.최종확인)

132) 트루네트웍스 소장을 대상으로 2020년 8월 10일에 인터뷰한 내용임

133) 트루네트웍스 소장을 대상으로 2020년 8월 10일에 인터뷰한 내용임

6. 음성인식

가. 범죄자 음성인식 기술

생체 인식을 위해 지문이나 얼굴, 또는 음성 등을 측정하는 다양한 방법이 사용되고 있다. 각각의 방법은 정확성과 사용 방법에 따라 장단점이 존재하지만 음성 인식 분야는 30년 이상의 연구 개발을 통해 풍부한 과학적 기초를 다져왔다. 현재 음성인식 기술의 연구개발은 보이스피싱 범죄자의 음성을 분석하여 검거된 사기범의 추가 여죄를 확인하는 단계까지 진행되었으며, 나아가 음성분석을 통한 화자의 감정 인식 기술로 피해자의 통화 목소리 분석을 통해 보이스피싱 범죄를 사전에 예방할 수 있을 것이다.

국립과학수사연구원(이하 국과수)은 음성 인식 연구를 통해 음성데이터 고유의 값을 구분해 화자를 인식하여 사기범을 탐지하는 화자분석시스템을 개발하였다.¹³⁴⁾ 화자인식은 크게 화자 확인과 화자식별로 나뉘는데, 화자확인 은 발성된 음성이 원하는 화자인지 아닌지를 구분해 내는 것이며 화자인식은 인식대상이 되는 음성의 발성방법에 따라 특정 개인 차이를 구별하는 것이다.¹³⁵⁾ 국과수에서 개발한 화자분석시스템은 화자확인에 해당한다. 국과수는 보이스피싱 사기범들의 목소리를 수집하고 이 음성 파일 중 동일한 사람으로부터 발화된 목소리가 있는지에 대한 법과학적 화자 분석 방법을 이용하는 연구를 하였다.¹³⁶⁾ 그 결과 금융감독원

134) 박남인, 전옥엽, 김태훈, 이중, “보이스피싱 음성 파일에 대한 법과학적 화자 분석 방법의 적용 사례”, 한국디지털포렌식학회, 디지털포렌식연구 13(1), 2019, 35-44면

135) 이한구, 이기성, “강인한 정합과정을 이용한 텍스트 종속 화자인식에 관한 연구”, 대한전기학회, 대한전기학회 학술대회 논문집 25(2), 2002, 605면

136) 국립과학수사연구원 홈페이지, 연구분야 디지털,
<https://www.nfs.go.kr/site/nfs/04/10401000000002017082110.jsp> (2020.12.30. 최종확인)

에서 수집한 2,327개의 보이스피싱 신고 음성파일들을 상호 비교하여 음성 특징이 유사한 것으로 확인되는 화자 군집들을 확인하였다. 화자인식 훈련과정에 사용되는 음성 파일에 대해 무음 구간을 제거하는 전처리 과정을 수행한 후, DB에 저장하며 저장된 파일에서 I-vector를 추출하여 코사인 유사도 행렬 기반으로 개인의 고유한 음성 특징을 비교하여 화자의 군집을 분석한다.¹³⁷⁾ 본 연구에 사용된 음성으로 금융감독원에서 보유한 보이스피싱 음성파일 중 채널과 잡음 특성이 비교적 양호한 1,458점을 선택하였으며, 각 보이스피싱 음성 파일에서 피해자의 음성을 제외한 범죄자들의 목소리만 약 1분 정도 생성하여 DB에 저장하였다. 그 후, 보이스피싱 음성파일에 대한 군집 분석을 위한 보이스피싱 음성 파일 전처리과정을 통해 I-vector의 코사인 유사도 행렬값을 도출하였으며, 그 결과로 여성의 군집·분석 결과 수사기관 사칭과 금융대출 사기가 동일인에 의해 발생하는 것이 확인되었다.¹³⁸⁾

아직 보이스피싱 음성 탐지에 상용화되지 않은 음성 감정 인식 기술과 달리 화자 분석 시스템은 가시적인 성과를 낸 사례가 존재한다. 2017년 충남지방경찰청 지능범죄수사대는 중국 천진에서 보이스피싱 콜센터와 인출책 등 총 34명을 입건하고 이 중 27명을 구속¹³⁹⁾하였으며, 같은 해 필리핀 콘에서 보이스피싱 조직 40명¹⁴⁰⁾을 구속하였다. 구속된 사기범 중 콜센터 직원들의 목소리는 국과수의 화자 분석 시스템을 통해 금융감독원 홈페이지(www.phishing-keeper.fss.or.kr)에 신고

137) 박남인, 전옥엽, 김태훈, 이중, “보이스피싱 음성 파일에 대한 법과학적 화자 분석 방법의 적용 사례”, 한국디지털포렌식학회, 디지털포렌식연구 13(1), 2019, 35-44면

138) 박남인, 전옥엽, 김태훈, 이중, “보이스피싱 음성 파일에 대한 법과학적 화자 분석 방법의 적용 사례”, 한국디지털포렌식학회, 디지털포렌식연구 13(1), 2019, 35-44면

139) 충남지방경찰청 보도자료, “충남청 지능범죄수사대, 관공서 사칭한 해외 보이스피싱 사기단 검거”, 2017.5.22.자

140) 중앙일보 보도(2017.12.15.), “한국판 콘에어...필리핀서 범죄인 47명 전세기 로 수송”, <https://news.joins.com/article/22206459> (2020.12.14. 최종확인)

로 등록된 ‘그 놈 목소리’ 음성파일을 토대로 중국 천진 사기범 중 10명, 필리핀 보이스피싱 사기범 중 17명에 대한 추가 범행을 확인하였다.¹⁴¹⁾ 이를 계기로 검거되지 않았더라도 범행 당시 범인들의 목소리 자료를 축적하여 추후 검거된 사기범의 목소리와 대조하여 추가 과거 범행을 밝혀 처벌의 강도를 높일 수 있게 되었다.

금융감독원은 2015년 7월부터 홈페이지에 보이스피싱 음성 녹음파일 신고제도를 운영하고 있고, 국립과학수사연구원은 지난 2016년 5월 금감원과 ‘보이스피싱 근절을 위한 업무협약’을 맺은 이래로 보이스피싱 사기범의 목소리를 지속적으로 제공받아 체계적인 음성DB를 축적(현재 음성파일:1300여점) 및 업데이트(800여점)하고 있다. 이 음성 DB인 ‘바로 이 목소리’를 토대로 콜센터 피싱책 추가 범행 20건을 특정하는 등의 성과는 음성 분석기술을 통한 보이스피싱 수사를 주요 정책으로 채택하기에 충분하다고 보인다. 하지만 일부 범죄에서는 음성자료를 분석하여도 조건에 따라 성문에서 포먼트(formant)를 측정할 수 없을 수도 있고, 발성된 음성 정보가 많지 않아 분석할 수 없을 때도 있으므로 추가적인 연구 및 기술 발전 또한 병행되어야 한다.

나. 피해자 음성 감정인식 기술

국내에서 음성으로 감정을 인식하는 기술 연구가 활발히 진행되고 있다. 음성은 기본적인 의사소통 수단이어서 다양한 인터페이스에 적용되고 측정하기가 간단하다는 장점을 갖고 있어 감정을 인식하는 도구로 적합하다.¹⁴²⁾ 문화에 따라 감정을 표현하는 제스처(gesture)가 다를 수 있고 성인이 되면 감정을 제어하는 경향을 보이므로 제스처(gesture)와 같은 표정보다 음성에 표현되는 감정의 정보가 더 일관

141) 충남지방경찰청 보도자료, “충남청 기능범죄수사대, 관공서 사칭한 해외 보이스피싱 사기단 검거”, 2017.5.22.자

142) 권철홍, 송승규, 김종열, 김근호, 장준수, “감정 인식을 위한 음성 특징 도출”, 한국음성학회, 말소리와 음성과학 4(2), 2012, 73면

성이 있다.¹⁴³⁾ 여기서 착안한 음성감정 인식 기술은 음성 정보를 분석하여 감정 상태를 확인하는 기술을 의미한다. 음성감정 인식 시스템인 SER(Speech Emotion Recognition System)은 주어지는 음성 신호로부터 특징을 추출하고 감정 모델을 정의하여 학습 및 분류를 진행한다. 감정을 모델링하기 위한 방법으로 과거에는 Hidden Markov Model을 이용한 방법들이 주로 사용되어 왔으나 최근 심층 신경회로망 DNN(Deep neural Network)과 RNN(Recurrent Neutral Network)의 등장으로 감정 인식의 음성신호와 같은 시계열 데이터 처리 시스템의 연구에 괄목할 만한 진전이 이루어지고 있다.¹⁴⁴⁾

하지만, 기존의 감정 발화 음성적 특징을 살핀 연구의 대부분은 특정 한두 가지 감정만을 연구 대상으로 삼거나 감정 발화의 특징을 주로 억양에만 기대어 설명하였다.¹⁴⁵⁾ 하지만 인간은 감정을 두 가지의 분류로 명확히 나누어 느끼지 않으며, 감정의 종류가 두 가지만 존재한다고 말할 수 없다. 인간은 보편적으로 기쁨, 슬픔, 놀람, 공포, 분노, 혐오의 여섯 가지 감정을 지니고 있으며 이런 감정들은 억양뿐만 아니라 발화 속도, 강도 등 다양한 음성적 특질 차이를 만들어 낸다.¹⁴⁶⁾ 즉

143) 김도경, 김윤중, “음성감정데이터베이스의 분석과 프레임 단위 특징과 발음 단위 특징을 통합하는 Attention mechanism을 이용한 음성 감정 인식 시스템의 개발”, 한국정보과학회, 정보과학회논문지 47(5), 2020, 480면

144) 김도경, 김윤중, “음성감정데이터베이스의 분석과 프레임 단위 특징과 발음 단위 특징을 통합하는 Attention mechanism을 이용한 음성 감정 인식 시스템의 개발”, 한국정보과학회, 정보과학회논문지 47(5), 2020, 480면

145) 감정 발화의 연구로는 손남호, 이호영, 황효성, “감정발화의 데이터베이스 구축과 음향 분석”, 사단법인 한국언어학회, 언어학 72, 2015, 175-199면; 윤은경, “방언 간 코드 스위칭으로 인한 감정 발화의 음성적 변화: 예비 한국어 교원을 대상으로”, 한국외국어대학교 언어연구소 언어와언어학 70, 2016, 365-391면; 이서배, “한국어 감정 음성에서 모델로 추출한 피치 곡선 연구”, 한국언어과학회, 언어과학 25(3), 2018, 191-209면; 조성문, 김미희, “남녀 분노 발화의 음성적 특징”, 한국언어문화학회, 한국언어문화 68, 2019, 347-379면; 김진만, 정종수, “명령 발화의 감정별 음성 특징 연구”, 한양대학교 동아시아문화연구소, 동아시아문화연구 81, 2020, 96면 등을 참조.

음성에서 감정에 대한 정보를 담고 있는 것은 억양에서만 나타난다고 보기 어려우며 음성데이터의 다양한, 특히 보이스피싱 사기를 당하는 피해자는 당황, 의문, 다급함 등과 같은 기존의 감정분류와 다른 종류의 세부 감정으로 나뉠 것이라 예상된다. 예상치 못한 사실에 놀라 사기범에게 상황을 되묻는 물음의 억양이나 당황하여 끊기는 말의 공백, 발화 문장의 정확하지 못한 완성도 등 보이스피싱이라는 특수 상황에 대한 정확한 이해와 사기를 당하는 피해자의 감정에 따른 발화 음성의 연구가 충분히 이루어진다면 피해자의 음성만으로 보이스피싱 음성을 탐지할 수 있을 것이다. 현재는 주로 범죄자의 음성을 텍스트로 추출하여 키워드에 대한 빈도분석 등을 할 수 있고 모바일 운영체제에서 관련 음성을 녹음하는 기능을 막을 경우에는 한계가 있지만, 발화자인 피해자의 음성은 해당 스마트폰에서 수집하여 활용할 수 있기 때문에 활용성이 높을 것으로 판단된다.

7. 텍스트추출

통화 중 보이스피싱 여부를 확인하기 위해 인공지능 기술을 사용한 많은 방법이 도입되고 있다. 즉, 보이스피싱 음성을 텍스트로 변환하는 STT(Speech-To-Text) 기술을 사용해 키워드를 탐지하는 것이다.¹⁴⁷⁾ 최근에 보이스피싱의 음성을 분석하여 통화 중에 실시간으로 보이스피싱 여부를 탐지할 수 있는 기술을 개발하고 있다.¹⁴⁸⁾ 텍스트를 이용한 화자 인식 기술은 텍스트나 단어를 바탕으로 텍스트-종속(text-dependent)과 텍스트-독립(text-independent)으로 구분된다.¹⁴⁹⁾ 텍스트 독립

146) 김진만, 정종수, “명령 발화의 감정별 음성 특징 연구”, 한양대학교 동아시아문화연구소, 동아시아문화연구 81, 2020, 96면

147) KT 보도(2016.4.7.), “KT DS, 콜센터 전용 음성인식 솔루션 ‘썬크 투 텍스트’ 출시”, https://corp.kt.com/html/promote/news/report_detail.html?datNo=12275 (2012.12.17. 최종확인)

148) 박형우, 배명진, “목소리 분석을 통한 보이스피싱 예방에 관한 연구”. 인문사회과학기술융합학회, 예술인문사회융합멀티미디어논문지 7(3), 2017, 393-400면

은 훈련과 테스트에 같은 텍스트를 사용하는 반면에 텍스트 독립은 훈련과 테스트에 다른 텍스트를 사용한다. 종속 시스템(text dependent system)은 훈련 단계와 테스트 단계 모두에서 같은 텍스트를 말하는 것을 포함한다. 텍스트 독립 시스템에서는 말해야 할 텍스트에 제한이 없으며 인식률(recognition rate)은 텍스트 독립 시스템보다 텍스트 종속 시스템이 더 좋다.¹⁵⁰⁾

KT 후후애킴퍼니는 2020년 1월 STT 기술을 사용한 보이스피싱 탐지 기술을 상용화하였고, 2020년 12월부터 KT 융합기술원 AI 연구소에서 개발한 ‘성문분석’ 기술을 더해 ‘실시간 보이스피싱 탐지’ 기능을 후후 앱을 통해 제공하고 있다.¹⁵¹⁾ 금융감독원과 한국정보화진흥원 및 IBK기업은행은 인공지능 기술을 활용해 보이스피싱 전화를 실시간으로 차단하는 AI 앱(APP)을 공동 개발하고 2019년 3월 18일부터 시범운행을 실시했다.¹⁵²⁾ 이 앱은 휴대전화 통화내용을 인공지능을 사용한 실시간 분석으로 보이스피싱 사기일 확률이 일정 수준에 도달하면 경고음성과 진동으로 알려준다. 해당 음성은 발신자에게는 들리지 않고 수신자에게만 전달된다. 이 앱은 금융감독원이 수집한 8천여 보이스피싱 사례 속 단어나 발화 패턴, 문맥 등을 머신러닝 방식으로 학습한 내용을 기반으로 보이스피싱 여부를 판단한다.

8. 악성앱 탐지

가. 악성앱 분석

149) 김민서, 문종섭, “STFT와 RNN을 활용한 화자 인증 모델”, 한국정보보호학회, 정보보호학회논문지 29(6), 2019, 1393-1401면

150) Jyoti B. Ramgire, Sumati M.Jagdale, “A Survey on Speaker Recognition With Various Feature Extraction And Classification Techniques”, International Research Journal of Engineering and Technology (IRJET) Vol 03 Issue 04, 2016, pp.709-712

151) 디지털타임스 보도(2020.11.4.), “내 통장 댄으려는 ‘그놈 목소리’ 단 14초만에 잡아낸다”, <https://bit.ly/2JC9amX> (2020.12.17. 최종확인)

152) 금융감독원 보도자료, “보이스피싱 이제 인공지능으로 잡는다.”, 2019.3.18.자

보이스피싱에서 사용되는 악성앱과 악성코드의 역할은 피해자가 기관의 대표번호로 전화를 할 때 기관이 아닌 범죄자에게 전화가 가도록 발신 호를 탈취하는 것이다. 악성앱의 구성 내부를 분석하면 기관 전화번호를 필터링하기 위한 ‘블랙리스트(Blacklist)’와 ‘포워드리스트(Fowardlist)’가 존재한다. 블랙리스트에 목록화되어있는 전화번호는 전국 금융기관과 금감원 등 사칭 사기 시나리오에 사용되는 대표기관의 전화번호로 피해자가 해당 리스트에 적혀있는 대표번호로 전화를 걸면 대표기관이 아닌 보이스피싱 사기범에게 통신 호가 전달된다. 포워드리스트 전화번호 리스트는 블랙리스트와 마찬가지로 사칭 사기 시나리오에 사용되는 대표기관 번호 목록이다. 블랙리스트와는 반대로 대표기관에서 포워드리스트에 목록화된 번호로 피해자에게 전화를 발신할 시 통신호를 피해자 모바일 단에서 차단한다. 결국 악성앱이 피해자의 모바일에 설치되면 대표기관의 통신이 차단되거나 통신 신호가 가로채여 범죄자들에게 연결되어 피해를 입게 된다.

금융보안원은 금융회사를 사칭하는 악성앱을 2018년을 기준으로 평균 하루에 수 십개의 악성 앱을 실시간으로 수집하여 분석하고 있다.¹⁵³⁾ 금융보안원에서 연구한 보이스피싱 악성앱 프로파일링 보고서에 따르면, 악성 앱은 대표적으로 두 가지의 특징을 가지고 있다. 첫째는 C&C 정보가 앱 내부에 하드 코딩되어 있는 것, 둘째는 앱의 가장 주된 기능인 전화 가로채기 코드가 포함되어 있다는 것이다. 대부분 악성코드의 경우 C&C 서버 정보를 담고 있었고 몇 가지 소수 코드의 경우 C&C 서버의 IP 주소도 하드 코딩되어 있는 경우가 있다.¹⁵⁴⁾ 금융보안원의 악성앱 분석 결과, 2번 하드코딩의 경우 사용하는 라이브러리 파일명은 ‘libma숫자sker.so’ 형태이고, 파일명 가운데 포함되어 있는 숫자는 1~3까지 각각 4월, 6월, 10월에 확인되었다. 이는 추가적으로 ‘libma4sker.so’와 같은 세부 유형이 추가 발견될 가능성이 있다는 것을 보여준다. 3번 XHttpRequestUtils 클래스, 4번

153) 금융보안원 보고서, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018.12.20. 13면

154) 금융보안원 보고서, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018.12.20. 13면

ConfigUtils 클래스, 6번 ClientmayServices 클래스는 C&C 서버 IP 주소를 얻어오는 형태를 띄고 있었다.¹⁵⁵⁾

<표 3-13> C&C 하드코딩 유형

번호	C&C 하드코딩 유형	
1	Config 클래스	
2	(1)	libmalsker.so 파일
	(2)	libma2sker.so 파일
	(3)	libma3sker.so 파일
3	XHttpRequestUtils 클래스	
4	ConfigUtils 클래스	
5	MyGlobal 클래스	
6	ClientmayServices 클래스	
7	Constant 클래스	

(출처: 금융보안원, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018)

보이스피싱의 악성앱 특징인 전화 가로채기 코드는 (1) 브로드캐스트리시버를 이용해 발신전화를 가로채기 위한 클래스를 생성하고, (2) 전화 상태가 변경되는 것을 확인하기 위해 클래스 내부에 onReceiver() 메서드를 오버라이드한다.¹⁵⁶⁾ 이후 (3) 전화 발신 상태를 확인, (4) 발신 상태로 확인이 되면 setResultData(“포워딩할 전화번호”)를 사용해 전화를 가로챈다.¹⁵⁷⁾ 악성코드는 이 프로세스를 거쳐 일반적으로 발신전화를 가로챌 수 있고, 금융보안원 보고서는 전화 가로채기 코드

155) 금융보안원 보고서, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018.12.20. 19면

156) 금융보안원 보고서, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018.12.20. 20면

157) 금융보안원 보고서, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018, 20면

유형을 클래스 명 기준으로 총 10가지로 분류하였다.

〈표 3-14〉 전화 가로채기 코드 유형

번호	코드 유형
1	PhoneNewRecevier 클래스
2	NewPhoneCallReceiver 클래스
3	PG_CallRcver 클래스
4	ShowReceiver 클래스
5	My_CallRcver 클래스
6	ScanCallReceiver 클래스
7	Main_CallRcver 클래스
8	CallReceiver 클래스
9	CallHandleReceiver 클래스
10	CalRcver 클래스

(출처: 금융보안원, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018)

클래스 내부에 구현된 코드들을 살펴보면 6번 ScanCallReceiver 클래스만 단일적이고, 나머지 유형들은 비슷한 코드에서 약간의 변화를 보이는 것으로 보아 기존의 클래스 업그레이드 버전으로 추정할 수 있다.¹⁵⁸⁾ 이러한 형식으로 각 클래스의 내부를 살펴보면 각자의 특이사항들을 세부적으로 발견할 수 있다. 금융보안원에서 분석한 악성앱 내의 세부클래스 명, 혹은 코드 유사도 등을 비교해보면 매월 새로운 유형이 발견되는 것을 알 수 있었다. 이는 보이스피싱 사기범이 계속해서 다양한 방법으로 새로운 공격 시도를 하는 것을 예상할 수 있다.

현재 국내에서 악성앱을 탐지하여 가시적인 효과를 내는 서비스는 ‘피싱아이즈’가 대표적이다. ‘인피니그루’는 지난 4월에 이상징후탐지시스템(FDS)과 연동해 사

158) 금융보안원 보고서, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018, 25면

기 피해를 예방하는 보안앱인 ‘피싱아이즈’를 개발하였다. 보이스피싱을 통해 이루어지는 금융거래는 거래 데이터상 피해자가 자발적으로 금융거래를 하는 것처럼 보이기 때문에 금융사의 거래 데이터만으로 피해자가 보이스피싱 사기범에게 당한 행위인지 확인할 수 없다. 이런 한계를 개선하기 위해 피싱아이즈 서비스를 출시하였다.¹⁵⁹⁾ 피싱아이즈는 인공지능(AI) 기술을 활용한 이상징후 탐지인데 머신러닝을 통해 학습한 피싱아이즈는 악성앱 탐지는 물론 문자, 통화 음성에서 보이스피싱 의심 키워드를 스스로 발견하며 변형된 악성 앱을 찾아내고 있다.

휴대폰에서 보이스피싱 데이터를 확보하여 금융사의 FDS 시스템에서 대출실행, 인출시점 직전에 차단시키기 위하여 모바일 App, 사기데이터, 탐지률, 금융사 FDS 연동을 한다. 휴대폰 통화 및 문자 내용상 사기의심 내용, 악성앱 등이 탐지되는 경우 해당 내용을 사용자의 주거래 금융사에 전송하고 인피니그루 협력 금융사의 FDS(이상거래탐지시스템)에서 자금이체 및 대출을 차단하여 선제적으로 대응한다. 허위 금융신청에 대해 확인이 가능하고, 음성인식의 경우 서버를 거쳐 분석하는 것이 아닌 디바이스 자체에서 실시간으로 판단하는 방식이다. 하지만 금융사가 개인정보를 제공할 수 있는지에 대하여 개인정보보호법과 금융실명법에 대한 검토가 필요하다. 보이스피싱 의심사례가 적발되면 통화를 강제로 종료하는 것이 타당한지도 검토해야 한다.

나. 악성링크 탐지

보이스피싱 조직은 금융기관 등에서 광고 및 안내를 목적으로 발송하는 SMS 정보를 입수하여 이와 동일한 방식으로 피해자에게 문자를 보내 악성코드에 모바일을 감염시키는 스미싱 방식을 사용한다. 하지만 피해자를 보다 직관적으로 기망해

159) 피싱아이즈 관계자와 2020. 7. 31. 인터뷰한 결과, 출시 후 두 달간 피싱아이즈를 운영한 결과 보이스피싱 악성 앱 14개를 찾아내는 성과를 냈다고 하였다. 예상보다 훨씬 더 많은 보이스피싱 범죄 시도가 있어 앱을 설치한 고객 1,800명 가운데 24명에게 사기 시도를 했다가 피싱아이즈앱에 적발되었다고 한다.

야 하기 때문에 금융기관 등에서 보내는 문자와 완전히 동일할 수 없다. 따라서 범
 죄자들이 발송하는 SMS 문자를 데이터베이스화하고 패턴을 분석하여 주요 키워드
 를 추출하면 보이스피싱을 예방할 수 있을 것이다. 해외에선 스미싱 탐지(smishing
 Detector)를 위한 모델이 제안되었고, 이 모델의 SMS 텍스트를 통한 스미싱 탐지
 정확도는 96.29%에 이르렀다.¹⁶⁰⁾ smishing Detector 모델의 주요 탐지 모듈은 총 4
 가지로 문자 내 텍스트 데이터를 분석하는 ‘SMS 콘텐츠 분석(SMS Content
 Analyzer)’ , 악성 URL을 필터링 하기위한 ‘URL 필터(URL Filter)’ , SMS 자체의
 ‘소스코드 분석(Source Code Analyzer)’ , 사용자 명령 없이 다운로드 되는 악성
 코드 및 악성 앱 탐지를 위한 ‘APK 다운로드 탐지(APK Download Detector)’ 로
 구성되어 있다. 국내에서도 SMS 문자 메시지 필터링에 대한 연구¹⁶¹⁾가 다양하게
 이루어지고 있어 보이스피싱 악성앱 유포 탐지 활용을 위한 해당 기술을 도입이
 커다란 어려움은 없는 것으로 보인다. 다만, APK Download Detector 모듈에서 다
 운로드한 애플리케이션의 진위성을 보장하기 위한 보안성이 부족하다는 한계가
 있어 기술적 보완 연구가 진행되어야 한다.

160) Sandhya Mishra, Devpriya Soni, “Smishing Detector: A security model to
 detect smishing through SMS content analysis and URL behavior analysis” ,
 Elsevier Science B.V., Amsterdam, Future Generation Computer Systems
 108, 2020, pp.803-815

161) 이현영, 강승식, “워드 임베딩과 딥러닝 기법을 이용한 SMS 문자 메시지 필
 터링” , 한국스마트미디어학회, 스마트미디어저널 7(4), 2018, 13-18면

9. 데이터 정보분석

가. SNA 분석

i2 프로그램은 IBM에서 개발한 데이터 인텔리전스 전환 비주얼 분석 툴로, 데이터에 숨겨진 연결성과 패턴을 효과적으로 식별할 수 있게 도와 준다.¹⁶²⁾ 이 툴은 사이버 및 사기 위협을 효과적으로 식별할 수 있고, 경찰청에 2015년에 도입되어 수사에 활용 중이다. 중심성 원리와 하위집단 분석원리를 중심으로 총 6가지 사회 연결망 분석(SNA) 알고리즘이 반영되어 있다.¹⁶³⁾ 사회연결망은 사람들이 연결되어 있는 관계망을 의미하며, 다양한 행위자들이 상호작용을 하면서 만들어진 관계망을 의미한다.¹⁶⁴⁾ 사회연결망 분석은 사회 행위자들을 연결망의 구조적 변수, 즉 분석 단위인 노드(nodes)로 설정하고 연결망 안에서 행위자들간 연계는 연결관계(link 또는 tie)로 나타낸다.¹⁶⁵⁾ i2 프로그램 또한 관계 데이터를 분석할 시 기본 단위는 노드(node)와 라인(line)으로 구성되는데 여기서 노드는 행위자를 나타내고, 라인은 행위자들의 연결관계인 링크로 표현된다. 관계데이터 분석에는 많은 데이터들을 사용할 수 있으나, 수사 시 분석 대상이 되는 관계데이터는 발신번호와 수신번호로 구성되어 있는 통화내역과 송금계좌와 수신계좌로 연계를 나타낼 수 있는 계좌내역이다. 기존의 분석 방법론으로는 다수 통화자, 다액 거래자 등 양적인

162) IBM, IBM Security i2 Analyst' s Notebook,
<https://www.ibm.com/kr-ko/products/i2-analysts-notebook> (2020.12.15.
 최종확인)

163) 김지온, “사회연결망 분석원리의 범죄 수사상 활용방안에 관한 연구”, 한국디지털포렌식학회, 디지털포렌식연구 13(2), 2019, 89-109면

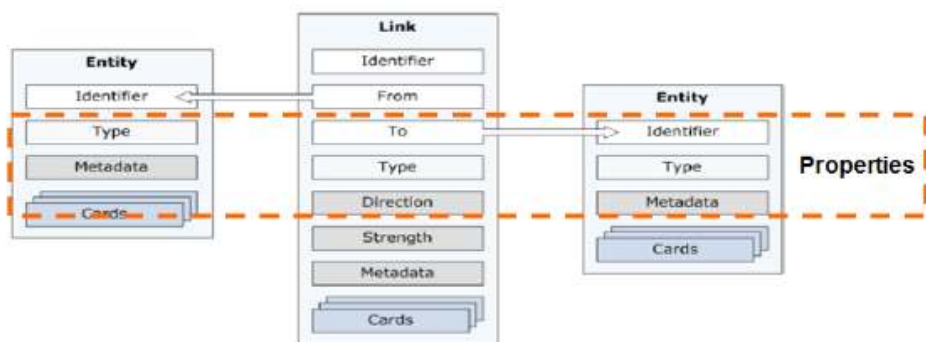
164) 김성희, 장로사, “사회 연결망 분석 연구동향 및 정보학 분야에서의 활용가능성에 대한 연구”, 한국정보관리학회, 정보관리학회지 27(4), 2010, 72면

165) 최영진, 양창훈, “경찰 범죄정보 수집 활동의 관계망 분석:비공식적 사회연결망 분석을 중심으로”, 한국콘텐츠학회, 한국콘텐츠학회논문지 20(1), 2020, 451면

분석에 주로 의존해 왔는데 양적인 분석은 개개인의 자료를 분석할 때 도움이 된다.¹⁶⁶⁾ 하지만 수사대상자가 여러 명인 조직범죄와 같은 사건은 관계데이터를 분석하는데 효과적이지 않기 때문에 관계데이터의 양이 많지 않더라도 수사대상자의 관계도 상 유의미한 형태나 구조적인 패턴이 도출되어야 수사상 의미있는 결과가 도출된다. 통화내역 파일에 있는 여러 컬럼 중에 ‘발신번호’를 왼쪽 노드의 ID로, 오른쪽 노드는 ‘착신번호’로 지정하고 링크의 ID는 통화횟수를 확인하기 위해 ‘발생 횟수’로 지정하면 수사대상자들의 통화네트워크에 대한 사회관계망 분석 모델이 완성된다.

또한, i2 프로그램은 관계분석과 함께 속성 분석도 가능하다. i2의 분석 원리를 ELP 모델이라고 표현하는데 Entity, Link, Properties를 의미하는 것으로 개체와 링크의 속성값을 지정할 수 있다.

[그림 3-12] i2 프로그램의 ELP 모델



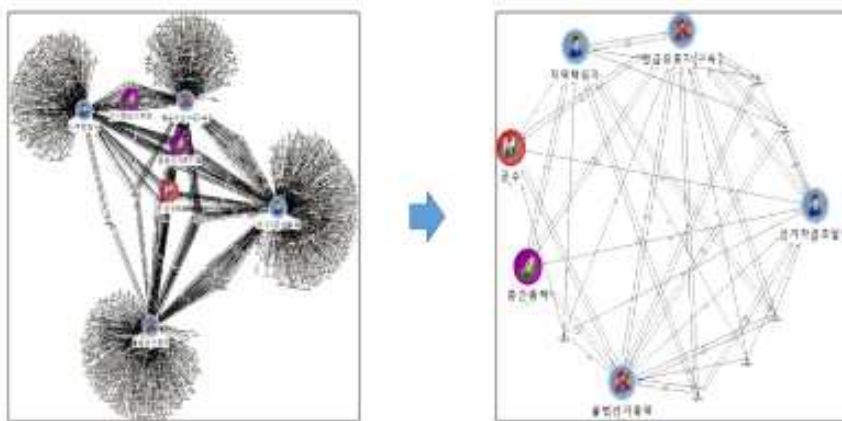
(출처: 김지운, “사회연결망 분석원리의 범죄 수사상 활용방안에 관한 연구”, 디지털포렌식연구, 2019)

통화 네트워크 분석모델에서 링크의 속성값으로 기지국 위치를 넣으면, 모델링

166) 김지운, “사회연결망 분석원리의 범죄 수사상 활용방안에 관한 연구”, 한국디지털포렌식학회, 디지털포렌식연구 13(2), 2019, 93면

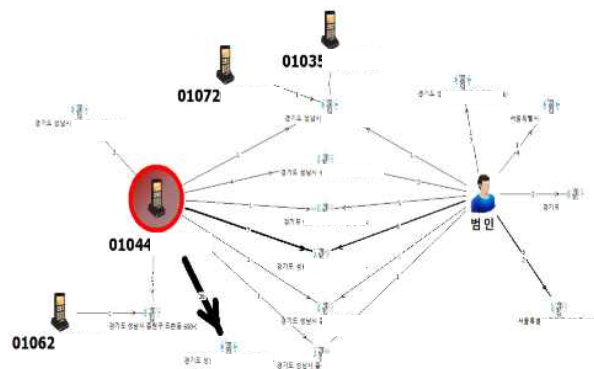
이 가능해진다. 모델링이 끝나면 사건 관계자의 통화내역을 일정한 형태의 레이아웃으로 시각화하는 방식으로 사회연결망 분석(SNA) 알고리즘을 활용하여 분석을 수행한다. [그림 3-13]은 4인의 통화 네트워크를 i2 프로그램을 이용하여 시각화하여 SNA 알고리즘 중 하위집단을 파악하는 ‘클러스터 찾기’ 기능을 활용한 화면이다. 결과적으로는 12명의 하위집단을 식별해 낸 것을 확인할 수 있다.

[그림 3-13] i2 프로그램을 활용한 통화네트워크 분석화면



(출처: 김지은, “사회연결망 분석원리의 범죄 수사상 활용방안에 관한 연구”, 디지털포렌식연구, 2019)

[그림 3-14] 구조적 등이성 원리 활용 분석 사례



(출처: 김지은, “사회연결망 분석원리의 범죄 수사상 활용방안에 관한 연구”, 디지털포렌식연구, 2019)

SNA 분석 원리는 6가지의 알고리즘 외에도 다양하다. 네트워크의 지위와 역할에 대한 위치적(positional) 접근 방법인 역할(Role) 분석과 자료의 형태가 2인 행렬 연결망인 2-mode 네트워크 분석원리는 보이스피싱 조직범죄에 인출총책이나 중간책을 추려낼 때 효과적으로 적용할 수 있는 원리이다.¹⁶⁷⁾

나. 금융계좌분석

금융결제원에서는 금융결제원이 운영하는 금융공동망 데이터 등을 활용 및 분석한 금융사기 의심 계좌 정보를 금융회사에 제공하는 서비스를 운영하고 있다. 머신러닝 방식의 금융 의심 거래정보 분석 서비스로 여러 은행의 ATM을 통해 입출금할 경우 기존 은행별 데이터 분석으로는 적발이 어려웠던 점을 이번 서비스를 통해 ATM 간 연결되는 계좌정보 등을 분석할 수 있도록 하였다.¹⁶⁸⁾ 원거리에서 연속으로 출금할 시에도 금융결제원이 해당 ATM 위치정보를 활용해 의심 계좌를 적발할 수 있다는 점이 특징이다.

[그림 3-15] 금융의심거래 정보분석 서비스



(출처: 금융위원회, “혁신금융서비스 지정 관련 참고자료”, 2019)

167) 김지은, “사회연결망 분석원리의 범죄 수사상 활용방안에 관한 연구”, 한국디지털포렌식학회, 디지털포렌식연구 13(2), 2019, 89-109면

168) 금융위원회 보도자료, “혁신금융서비스 지정 관련 참고자료”, 2019.12.18.자

금융실명법 제4조 제4항에 따르면 거래정보 등을 알게 된 자는 그 정보 등을 타인에게 제공 또는 누설하거나 그 목적 외의 용도로 이용하지 못하도록 금지하고 있다. 하지만, 금융위원회는 금융회사에 제공 가능한 금융거래정보 등의 범위를 금융 회사명, 계좌번호, 예금주(성명), 금융사기 의심 사유 및 관련 금융거래정보로 제한하여 금융결제원이 금융공동망 데이터를 금융사기 방지를 위해 사용하도록 하였다.¹⁶⁹⁾ 아울러 금융거래정보 등을 활용해 분석한 금융사기 정보의 유의성 등을 높이기 위해 1단계 정합성 분석, 2단계 은행에 정보 제공, 3단계 대상 금융회사 확대 등 단계별 실시 등의 단서를 달았다.¹⁷⁰⁾

금융회사는 이상거래탐지시스템(FDS)을 개발해 왔고,¹⁷¹⁾ 2016년 SK증권·한국스마트카드·신한은행 등이 추진한 이상거래탐지시스템 구축¹⁷²⁾에는 인피니그루의 GruDEEP 솔루션이 적용되었다.¹⁷³⁾ A 은행에서 2017년도에 발생한 보안사고 데이터와 시나리오를 기반으로 탐지한 거래 데이터 및 정상 거래 데이터를 이용하고 인공지능 탐지모델 연구를 살펴보면 Deep Learning 기반 지도학습 방식의 CNN(Convolutional Neural Network) 알고리즘을 사용하여 최적의 모델을 찾고 이를 보완하여 시나리오 기반과 인공지능기반이 결합한 탐지모델 개발 Hybrid 형태 최적의 지능화 모델을 제안하였다.¹⁷⁴⁾

169) 금융위원회 보도자료, “혁신금융서비스 지정 관련 참고자료”, 2019.12.18.자

170) 아주경제 보도(2019.11.21.), “혁신금융으로 보이스피싱 잡는다...금융공동데이터 의심 거래 확인에 활용”,

<https://www.ajunews.com/view/20191121112824749> (2020.12.14. 최종확인)

171) 금융위원회 보도자료, “금융위원장, 금융IT보안 강화를 위한 현장간담회 개최”, 2015.2.2.자

172) 금융보안원 보도자료, “머신러닝 기반의 이상거래 탐지시스템 동향”, 2017.8.25.자

173) 인피니크루 관계자 인터뷰(2020.7.31)에 의하면 해당 솔루션에는 딥러닝 기술이 적용되었고, 데이터 거래 패턴을 스스로 분석하는 별도의 룰 엔진이 필요 없이 데이터 거래 패턴을 스스로 학습하기 때문에 시간이 흐를수록 이상 거래 탐지 정확도가 높아진다고 하였다. 따라서 사람이 인지하기 어려운 복잡한 데이터 간 상관관계도 학습을 통해 분류해 낼 수 있다고 답변하였다.

다. 암호화폐 분석

암호화폐 추적은 범죄자들이 사용하는 암호화폐 주소를 찾았을 때 시작된다. 가장 먼저 해당 주소가 비트코인(Bitcoin)인지, 이더리움(Etherum)인지, 대시(Dash)인지 확인해야 한다. 개별 암호화폐에 대한 블록체인에 접속해서 암호화폐의 길이와 형태 등을 기준으로 판단해야 한다. 비트코인의 경우 비트코인 주소와 블록 정보를 알게 되면 최신 거래 내역을 확인할 수 있다. 암호화폐 종류별 블록체인의 주소와 형태는 아래와 같다.

〈표 3-15〉 암호화폐 종류별 블록체인 주소와 형태

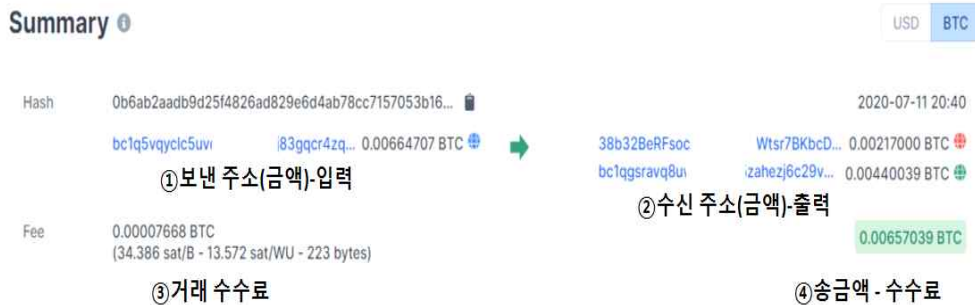
연번	이름	블록체인	주소 형태(예시)
1	비트코인	https://Blockchain.info	liUjpiUjpDwwMzUNQqNkHrbDwpd2uCd2uC
2	이더리움	https://etherscan.io	0610a610a12a0428a89f90ee9139f6432be964e964
3	리플	https://xrpcharts.ripple.com/#/transactions/	rbpdebpddeeFStatyayCWjXYY44YBB4YBB4
4	모네로	https://moneroblocks.info	84a9a4a9add2305295246d06c09e7ab74ad0235c684be14e9754f18cfbe2f2be2 (다양함)

비트코인이라고 확인된 다음에는 블록체인에서 거래내역에 대한 분석을 해야 한다. 일반적으로 비트코인 거래는 아래 그림과 같이 구성되고, 비트코인을 보내는 주소(금액), 이를 수신한 주소(금액) 및 해당 거래의 승인을 위해 블록체인에 등록(채굴)하는 경우 이를 등록한 채굴자가 받는 보상인 거래 수수료로 구성된다.¹⁷⁵⁾

174) Jeong. E, Lim. J, “전기통신금융사기 사고에 대한 이상징후 지능화(AI) 탐지 모델 연구”, 한국정보보호학회, 정보보호학회논문지 29(1), 2019, 149-164면

175) 자세한 내용은 Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system“, 2008, pp.1-9

[그림 3-16] 비트코인 개별 거래(Transaction) 정보



이와 같이 수작업으로 거래내역을 추적한 다음에 비트코인이 최종적으로 모이는 주소를 특정하였다면 해당 주소에 대해서 암호화폐거래소에 일반 압수수색 영장 또는 통신사실확인자료제공요청허가서를 제시하여 개인정보, 거래내역, 접속 정보 등을 확보하여 용의자를 특정한다. 만약 해당 주소가 국내 암호화폐거래소에서 발급된 것이 아닌 경우에는 해외 암호화폐거래소에 국제공조를 요청해야 하는데, 사실상 정보제공을 기대하기는 어려운 실정이다.

한편, 수작업으로 추적하는 방법 외에 경찰청을 비롯하여 전 세계 수사기관에서 사용하는 암호화폐 분석 프로그램인 체인어널리시스(Chainalysis) 회사의 리액터(reactor)가 있다. 리액터(reactor)는 주로 비트코인과 이더리움에 대한 거래내역을 분석·추적하는 기능을 제공하고, 자금세탁 과정을 시각적으로 보여준다. 각 지갑 별로 거래내역 조회가 가능하고 트랜잭션(거래번호), 송신자 지갑 주소, 수신자 지갑 주소별로 조회도 할 수 있다. 그런데 비트코인과 이더리움 등 일부 암호화폐에 대한 분석기능을 제공하고 있어 아직까지 부족한 점이 많다. 따라서 암호화폐 추적에 대한 다양한 기술 연구가 필요하고, 그러한 연구를 바탕으로 자금세탁 추적 역량을 확충하는 것이 필요하다.

제4절 소결

이상에서 보이스피싱의 범죄조직 체계와 범죄자들이 사용하는 범행수법 6가지, 그리고 대응기술 8가지를 대략적으로 살펴보았다. 보이스피싱 범죄조직은 이미 조직범죄로 성장하였다. 국내와 해외로 이원화되어 있지만 콜센터, 인출책, 통장제공책, 자금세탁책 등으로 구성하여 체계적으로 운영하면서 차단과 추적을 따돌리고 있다. 심박스를 이용하여 발신번호를 변작하고, 피해자에게 악성앱을 설치한 후 발신번호를 탈취하는가 하면, 암호화폐를 사용하여 자금세탁을 하는 등 계속하여 지능화되고 있다.

이에 대하여 보이스피싱 대응기술을 ① 발신번호변작 차단·탐지, ② 네트워크 패킷분석, ③ 통신패턴분석, ④ 심박스 전파탐지(3G·4G), ⑤ 음성인식(범죄자 음성인식, 피해자 음성·감정인식), ⑥ 텍스트추출, ⑦ 악성앱 탐지(악성앱 분석, 악성링크 탐지), ⑧ 데이터 분석(SNA 분석, 금융계좌분석, 암호화폐추적) 등 8가지로 분류하여 기술의 원리와 한계를 도출하였다. 발신번호 변작 차단·탐지 기술은 그간 후행적으로 대응하다 보니 한계가 나타나고 있다. 네트워크 패킷분석은 기술적으로 가능하겠지만, 감청 이슈가 있기 때문에 수사기관이 통신제한조치허가서를 발부받아야 사용이 가능하다. 하지만 수사에서는 실익이 있지만 범죄예 방 측면에서는 무의미하다. 통신패턴분석은 이동통신사에서 수행할 경우 상당한 성과를 보일 것으로 예측되는데, 아직까지 가시적인 노력이 보이지 않는다. 심박스 전파탐지는 3G에서는 기술을 개발하여 성과를 내고 있으나 4G는 신호가 불연속적이고 주파수 대역이 넓어 탐지가 어려워 기술 개발이 필요한 상황이다. 음성인식과 텍스트 추출은 일부 기업에서 출시한 서비스에서 사용하고 있으나 이것만으로 완벽한 대응책이 될 수 없고, 기술 개발도 계속 진행해야 할 것이다. 실시간으로 차단하여 예방할 때 사용할 수 있고, 음성의 신원을 특정하여 범죄자를 검거하는 데도 활용할 수 있을 것이다. 아직 많은 기술이 도입되지 않았지만 향후 집중적으로 역량을 투입해야 할 분야로 보인다. 악성앱 탐지는 금융보안원에서 프로파일링을 하

고, 일부 기업에서 서비스를 제공하고 있는데, 서비스 범위와 분야가 다소 한정적이어서 그 효과가 대외적으로 충분히 알려져 있지 않다. 하지만 지금 많은 피해가 악성앱에서 발생하고 있는 만큼 조속한 기술 개발과 서비스 출시가 필요하다. 마지막으로 데이터 분석은 주로 수사기관에서 사용하고 있는데, 현재 자체 시스템과 소프트웨어를 사용하고 있지만, 본질적으로 데이터가 부족할 경우 한계가 있고, 도구 업데이트의 지체, 암호화폐 추적기술의 한계 등으로 어려움이 있어 보인다. 따라서, 향후 범죄자들의 범행수법을 면밀히 분석하고 이에 대응하기 위한 다양한 기술을 개발하는 노력이 필요할 것으로 보인다. 더불어 범죄자들이 고도의 수법을 사용하고, 피해자들이 그 어려운 수법을 이행하면서 피해를 당하고 있는 것을 볼 때 기술적 방법만으로 해결할 수는 없어 보인다. 기술 개발과 더불어 법제도의 개선, 수사역량의 제고, 민간기업의 협력 나아가 시민들의 경각심과 인식 제고가 필요할 것이다.

제4장 신종 보이스피싱 대응정책 및 평가

제1절 개괄

우리나라에서 보이스피싱 피해가 처음 발생한 것은 2006년 6월로 5월 18일 인천 우리은행 간석동 지점에서 발생한 사건으로 피해액은 800만원이었다.¹⁷⁶⁾ 2006년 한 해 동안 약 106억원의 피해가 발생하였지만, 해외에서 범죄가 본격적으로 이루어지기 시작하였던 2009년에는 반기 만에 5,000건에 약 510억원이 넘는 피해가 발생할 정도로 심각해졌다. 이에 2009년에 정부가 국제전화 식별번호 표시제도를 도입하여 일시적으로 감소하였으나 인터넷 전화 등장과 스마트폰 보급으로 2011년에 8,244건에 1,019억원의 피해가 발생하였다.¹⁷⁷⁾ 이후 정부가 스마트 및 인터넷 환경에 대한 대응방안을 마련하면서 2016년까지 다소 감소하였으나 2017년부터 대출빙자형 수법이 등장하고, 간편 송금 서비스의 출시와 금융권의 메신저 사용이 확산되면서 2018년까지 폭발적으로 증가하였다.¹⁷⁸⁾

정보통신부와 정보보호진흥원은 2006년에 ‘보이스피싱 피해방지 10계명’을 시작으로, 2007년 외국인 예금계좌 개설시 신원 확인 의무화, 2009년 발신번호 표시제도 도입, 2011년 발신번호변작 방지대책반 구성 등 다각적인 대응책을 마련하였다. 그럼에도 근절되지 않자 정부는 관련부처를 모두 참여시켜 2012년 ‘금융소

176) 이훈재, “보이스피싱의 피해실태 및 경찰의 대응방안에 관한 연구”, 피해자학연구 17(2), 2009, 217-244면.

177) 정상욱, 김봉식, “국내 보이스피싱(전화금융사기) 현황 및 대응방안 검토-통신 분야 대책을 중심으로”, 정보통신정책연구원, 정보통신방송정책 24(15), 2012, 50-69면.

178) 보안뉴스 보도(2018.5.17.), “다시 고개 든 보이스피싱, 대출사기형 81%”, <https://www.boannews.com/media/view.asp?idx=69499&page=3&kind=2> (2020.10.1. 최종확인)

비자 보호를 위한 보이스피싱 피해방지 종합대책’ , ‘보이스피싱 피해 예방을 위한 발신번호 조작방지 가이드라인’ , 2013년 ‘신·변종 전기통신금융사기 피해방지 종합 대책’ , 2018년 ‘전기통신금융사기 방지 종합대책’ , 그리고 2020년 ‘보이스피싱 척결 종합방안’ 을 마련하였다. 정부차원에서 많은 법제와 기술을 개발하여 보이스피싱에 적극 대응하고 있지만 그 피해가 여전히 줄지 않고 계속되고 있어 시급히 해결해야 할 사회문제가 되고 있다. 이하에서는 시대의 흐름과 기술 발전에 따른 신종 보이스피싱 대응정책의 주요 내용을 살펴보고 이에 대한 평가와 시사점을 도출해 보고자 한다.

제2절 정부부처의 개별대책

1. 보이스피싱 10계명 발표¹⁷⁹⁾ (2007년)

정보보호진흥원(現 한국인터넷진흥원)은 2006년 보이스피싱 사례가 처음 접수된 이후, 국세청, 금융기관 등을 사칭하거나 유괴 등 협박을 통하여 개인정보를 취득하고 금전 등을 탈취하는 전화사기로 인한 피해가 급증하자 ‘전화사기(보이스피싱) 피해방지 10계명’을 발표했다. 정보통신부와 정보보호진흥원은 전화금융사기(보이스피싱)로 인한 피해 예방을 위한 캠페인에 이동통신 3사 및 초고속인터넷 사업자, 주요 포털 사업자와 유관 협회 등을 참여하도록 하였다. 이들은 통신서비스 가입자를 대상으로 요금고지서 내 전화금융사기 주의 권고문을 삽입하고 SMS를 발송하는 등의 방법으로 캠페인에 참여했고, 포털 사업자들은 웹사이트 공지사항을 통해 전화금융사기 주요 수법과 대처 요령을 소개하고, 회원들을 대상으로 이메일을 발송하여 경각심을 제고하기 위해 노력하였다.

<표 4-1> 정보보호진흥원, 전화금융사기(보이스피싱) 피해예방 10계명 (2007년)

-개인정보보호 캠페인- 전화금융사기(보이스피싱) 피해예방 10계명	
1. 미니홈피, 블로그 등 1인 미디어 내에 전화번호 등 자신 및 가족의 개인정보를 게시하지 않습니다.	
2. 종친회, 동창회, 동호회 사이트 등에 주소록 및 비상연락처 파일을 게시하지 않습니다.	
3. 자녀 등 가족에 대한 비상시 연락을 위해 친구나 교사 등의 연락처를 확보합니다.	
4. 전화를 이용하여 계좌번호, 카드번호, 주민번호 등 정보를 요구하는 경우 일체 대응하지 마십시오	

179) 한국정보보호진흥원(現 한국인터넷진흥원) 보도자료, “정보통신업계, 전화금융사기 예방 발벗고 나선다! - KISA, 보이스피싱 예방 10계명 발표”, 2007.7.31.자

-
5. 현금지급기(CD/ATM)를 이용하여 세금 또는 보험료 환급, 등록금 납부 등을 하여 준다는 안내에 일체 대응하지 마십시오.
 6. 동창생 또는 종친회원이라고 하면서 입금을 요구하는 경우 반드시 사실관계를 재확인하시기 바랍니다
 7. 발신자 전화번호를 확인합니다.
 8. 자동응답시스템(ARS)을 이용한 사기 전화를 주의하세요
 9. 휴대폰 문자서비스를 적극 이용하세요
 10. 속아서 전화사기범들 계좌에 자금을 이체했거나, 개인정보를 알려준 경우, 즉시 관계 기관에 신고하세요
-

2. 외국인 예금계좌 개설시 신원확인 의무화¹⁸⁰⁾ (2007년)

금융감독원, 은행연합회 등 금융권은 2007년부터 보이스피싱에 대한 대책을 추진하였다. 2007년 8월 외국인 예금계좌 개설 시 신분확인 절차 강화를 목적으로 여권 외에 사업자등록증, 취업증명서 등 신원확인을 의무화하였다. 2009년 10월 외국인이 예금계좌 개설 시 법무부의 ‘외국인정보인증시스템’에 온라인으로 접속하여 신분증 진위 여부를 확인토록 하였다. 2010년 3월, 2011년 3월 두 차례에 걸쳐 개인 및 법인이 우체국 및 새마을금고를 포함한 전(全) 금융회사에서 단 기간(최근 1개월) 다수(2개 이상)의 요구불 예금계좌(보통·저축예금, 기업자유예금)를 개설하는 경우 거래목적을 확인하고 불분명한 경우 계좌개설을 거절하도록 규제하였다. 입금단계의 대책으로 2007년 7월 CD/ATM기의 거래한도를 축소하고, CD/ATM기에서 계좌이체 시 전화금융사기 주의문구를 화면에 표시토록 하였다. 2009년 6월 금융회사와 공동으로 전화금융사기에 많이 이용되는 유형의 계좌를 모니터링하여 피해자가 피해금 이체 시 송금은행에 피해사실을 확인하고 사기범의 피해금 인출을 제한토록 하였다. 2009년 7월 CD/ATM기에서 계좌이체 시 화

180) 정상욱, 김봉식, “국내 보이스피싱(전화금융사기) 현황 및 대응방안 검토-통신 분야 대책을 중심으로”, 정보통신정책연구원, 정보통신방송정책 24(15), 2012, 50-69면.

면에 전화금융사기 주의문구를 2회 이상 보여주고 음성경고를 실시하도록 하고, 2009년부터는 전화금융사기에 취약한 노인 및 주부 등의 경우 최근 1년간 이체 실적이 없는 계좌에서의 이체한도를 대폭 축소(70만원)하여 보다 구체적인 정책을 추진하였다.¹⁸¹⁾

3. 발신번호 표시제도 도입 (2009년)

2008년 국제적 금융위기에 따라 경제불황이 장기화됨에 따라 경찰청은 생계침해범죄에 대한 강력한 단속체계를 갖추기 위해 대책 추진단을 만들었고, 보이스피싱은 강·절도 및 불법사금융과 함께 중점 단속대상으로 선정되었다.¹⁸²⁾

2009년 4월 15일에는 총리실 국무차장 주관으로 경찰청, 금융감독원, 방송통신위원회 등의 관계자가 참여한 가운데, 보이스피싱 근절을 위한 대책을 마련하였다. 방송통신위원회는 통신사업자들과 공동대책을 수립하고 2009년 5월부터 보이스피싱 피해 예방을 위해 총 26억 원을 투자하여 국제 착신전화에는 대해 국제전화 식별번호를 표시하는 발신번호 표시제도를 도입하였다. 2009년 11월부터 수신하는 이용자에게 “국제전화입니다” 라는 문자안내서비스를 제공하도록 한 것이다.¹⁸³⁾ 국제전화 식별번호 표시제도는 중국 등 해외에서 국제교환망(TDM망)을 통해 국내로 걸려오는 국제전화번호 앞에 001(KT), 002(LGU+), 006(SK텔링크), 00391(별정통신사업자) 등 국제전화를 최초로 접수한 통신사업자의 고유한 국제전화 식별번호를 삽입하여 송출하는 제도이다. 보이스피싱 범죄자들이 해외 콜센터에서 전화를 걸면서 우리나라 금융기관이나 경찰서, 우체국인 것처럼 속이는데, 이때 발신번호를 국내 전화인 것처럼 조작하기 때문에 피해자들이 발신자의 거주지와

181) 감사원, “공직사회 모범선행사례 모음. 제15집”, 2012, 187-188면

182) 보안뉴스 보도(2009.1.6.), “경찰, 생계침해범죄 근절대책 추진”,
<https://www.boannews.com/media/view.asp?idx=13541&page=16&kind=3>
 (2020.10.1. 최종확인)

183) 금융감독원 보도자료, “금융소비자 보호를 위한 보이스피싱 피해방지 종합 대책”, 2012.1.31.자

정체를 파악하지 못하고 손쉽게 사기 행각에 당하게 된다. 국제전화 식별번호 표시제도는 국제전화발신번호 앞에 001, 002 등 식별번호를 표시함으로써 국민들이 국제전화임을 쉽게 인식할 수 있게 하여 보이스피싱에 대한 경각심을 높일 뿐만 아니라, 최초로 국제전화를 접수한 통신사업자가 어느 사업자인지를 신속하게 확인할 수 있어 해외의 어느 통신사업자를 통해 전화가 걸려 왔는지도 확인할 수 있게 해주었다. 이후 도입된 휴대폰 국제전화 문자안내서비스는 휴대폰 사용자가 국제전화를 수신할 경우, 액정화면에 “국제전화입니다” 라는 문자를 표시해줌으로써 수신자가 국제전화임을 확인할 수 있도록 하여 효과를 높여주었다. 전화사기범이 아무리 지능적으로 금융기관 직원이나 공무원을 사칭하더라도, 국민들이 쉽게 인식할 수 있어 범죄예방 효과를 제고할 수 있었다.¹⁸⁴⁾

4. 보이스피싱 예방수칙 10계명 배포 (2009년)

2008년 6월 경북 구미에서 실제 집배원의 실명을 밝히고 보이스피싱을 하는 등 공공기관을 이용한 보이스피싱이 늘어났다.¹⁸⁵⁾ 국세청이나 국민연금관리공단 등을 사칭한 세금 및 보험료 환급 수법에서 우체국 금융 및 택배(등기) 등을 이용한 수법으로 진화한 것이다.¹⁸⁶⁾ 이에 따라 지식경제부 우정사업본부와 수사기관 등은 협력하여 보이스피싱 피해예방 수칙 10계명을 배포하였다.¹⁸⁷⁾

184) 금융감독원 보도자료, “금융소비자 보호를 위한 보이스피싱 피해방지 종합 대책”, 2012.1.31.자

185) 세계일보 보도(2008.6.12.), “집배원 실명 내세운 신종 보이스피싱 등장”, <http://www.segye.com/newsView/20080612001338> (2020.10.1. 최종확인)

186) 아웃소싱타임즈 보도(2009.1.19.), “보이스피싱 피해 예방위한 10대수칙”, <https://www.outsourcing.co.kr/news/articleView.html?idxno=49103> (2020.10.1. 최종확인)

187) 보안뉴스 보도(2009.1.6.), “보이스피싱 피해예방 이렇게 하세요”, <https://www.boannews.com/media/view.asp?idx=13871&page=16&kind=3> (2020.10.1. 최종확인)

〈표 4-2〉 지식경제부, 전화금융사기(보이스피싱) 피해예방 수칙 10계명 (2009년)

-지식경제부 우정사업본부- 전화금융사기(보이스피싱) 피해예방 수칙 10계명	
1. 자동응답시스템(ARS)을 이용한 사기전화에 주의하라.	
2. 전화를 이용한 개인정보 요구에 대응하지 말라.	
3. 현금지급기를 이용해 세금 등을 환급해준다는 안내에 속지말라.	
4. 속아서 전화사기범 계좌에 자금을 이체한 경우, 즉시 거래은행에 지급정지 신청을 하고 가까운 경찰서에 신고하라.	
5. 속아서 개인정보를 알려준 경우, 즉시 은행이나 금융감독원에 신고하라.	
6. 동창생 또는 종친회원이라고 하면서 입금을 요구하는 경우 반드시 사실 관계를 재확인하라.	
7. 법원공무원을 사칭하며 전화를 걸어 ‘당신이 국민 참여재판 배심원으로 선정됐으나, 재판일에 출석하지 않았으므로 과태료를 내야 한다’ 고 할 경우 반드시 사실 관계를 재확인하라.	
8. 자녀를 납치한 것처럼 부모에게 전화해 돈을 송금하도록 할 경우 반드시 사실 관계를 재확인하라.	
9. 발신자 전화번호를 확인하라.	
10. 휴대전화 문자서비스를 적극 이용하라.	

5. 발신번호변작 방지대책반 구성¹⁸⁸⁾ (2011년)

국제전화에 대한 문자서비스 제도가 인터넷 전화와 스마트폰 사용의 보편화로 한계를 보이기 시작하였다. 우체국, 경찰청 등 공공기관의 전화번호를 사칭해 보이스피싱을 시도하는 사례가 늘어났다. 경찰청에 따르면 2009년까지 감소치를 보이던 보이스피싱의 피해규모가 누적 2,600억 원에 이르게 되었다. 방송통신위원회는 보이스피싱 방지 대책을 마련하기 위해 기간통신사업자, 전자통신연구원

188) 보안뉴스 보도(2011.2.27.), “외국발 보이스피싱 막자, 발신번호변작 방지대책반 구성” ,

<https://www.boannews.com/media/view.asp?idx=25049&page=12&kind=3>(2020.10

.1. 최종확인)

(ETRI) 등으로 ‘발신번호변작 방지대책반’을 구성하고 2011년 2월 24일 첫 회의를 개최하여 ETRI를 통해 인터넷 국제전화의 신호전달 경로를 분석하고 변작된 발신번호를 검색해 차단하는 등의 기술적 대책을 마련하고, 통신사업자의 교환시스템 보강, 발신번호 표시제도 개선 등을 추진하였다.

제3절 정부부처의 종합대책

1. 보이스피싱 피해방지 종합대책¹⁸⁹⁾(2012년)

2009년 이후 소강상태를 보이던 보이스피싱이 2011년 들어 다시 증가하기 시작하였다. 2011년에만 신고건수는 8,244건, 피해액은 1,019억원으로 전년대비 신고건수는 2,789건(51.1% 증가), 피해액은 465억원(83.9% 증가)이 증가하였다. 1건당 평균 피해금액도 1,236만원으로 크게 증가하였다.

정부는 금융위원회와 방송통신위원회, 경찰청, 금융감독원, 금융권 등과 합동으로 한 관계기관 TF를 구성하고, 2012년 1월 31일 보이스피싱 피해방지 종합대책(안)을 마련했다. 주요 내용은 개인정보만으로 온라인 통한 재발급이 가능한 공인인증서 재발급을 본인이 지정한 3대의 단말기에서만 허용하도록 하였다. 공인인증서 발급 단말기 외에 재발급 단말기를 추가로 지정하는 경우 대면확인 또는 본인확인 수단(전화인증, 휴대폰 인증 중 1가지와 OTP, 금융IC카드) 중 2가지 방법을 적용해서만 가능하도록 제한하였다. 공인인증서 사용도 지정된 단말기(발급·재발급 단말기)에서만 가능하도록 제한하되, 지정 단말기 외의 제3의 단말기에서 사용하는 경우 이체과정에서 추가 인증방법(휴대폰, OTP 등)을 적용해야 하며 1회 추가 인증을 받은 단말기에서는 사용자 불편 감소를 위해 추후 재인증을 면제했다. 300만원 이상의 계좌 간 이체금액도 계좌이체 후 바로 입금되지 않고 10분 후에 인출되도록 했다. 지연출금에 따른 정상거래자의 불편과 은행 자체 모니터링을 통한 의심계좌 적발에의 소요시간을 고려해 10분으로 정했고, 통상 이체거래의 대부분(91%)이 300만원 미만 소액인데 반해, 피해사례의 경우 총 이체건수의 84%가 300만원 이상의 고액인 상황을 고려하여 설정했다. 300만원 이상의 카드론 대출은 휴대폰 문자메시지로 카드론 승인사실을 안내한 다음 2시간 후에 입금

189) 금융감독원 보도자료, “금융소비자 보호를 위한 보이스피싱 피해방지 종합 대책”, 2012.1.31.자

이 의무화했다. 또한, 카드론에 의한 대출자금은 통장에 기재되는 거래 내역에 카드론임을 알 수 있도록 명확하게 표시하게 했다. 신용카드와 카드론 간 신청절차도 별도로 분리하여 신용카드 신규 발급시 카드론 미이용을 기본으로 설정하고, 카드론 이용 희망자는 별도 서식을 작성하여 신청하도록 했다. ARS를 통한 카드론 원칙적 금지하였으나 소비자의 불편 최소화를 위해 과거 카드론 거래실적 등을 확인해 검증된 경우에 한하여 예외적으로 허용했다. 통신 분야에서는 발신번호가 조작된 전화는 연결 차단 또는 정상번호 송출하도록 했고, 불법정보 유통사이트 및 공공기관 사칭 피싱사이트에 대한 대응을 강화했다. 사후적발을 강화하기 위해 전화금융사기 전담 수사팀을 운영하고 집중 기획수사를 실시하기도 했다.

나아가 방송통신위원회는 2012년 6월 28일 전화번호 조작 사기행위를 사전에 뿌리 뽑기 위한 기술적, 제도적 방안을 담은 가이드라인¹⁹⁰⁾을 채택하고 통신사업자의 적극적인 참여하에 7월 1일부터 단계적으로 시행하였다.

〈표 4-3〉 방송통신위원회, 보이스피싱 피해 예방을 위한
발신번호 조작방지 가이드라인 (2012년)

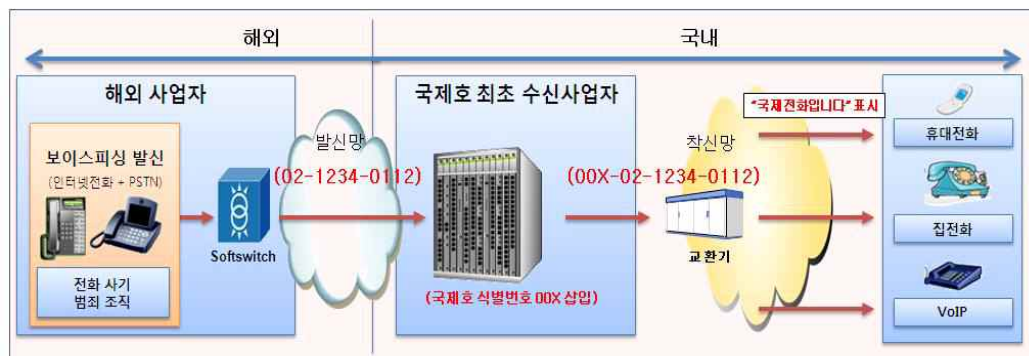
보이스피싱 피해 예방을 위한 발신번호 조작방지 가이드라인	
가. 문자메시지 피싱 대책	
① 휴대전화에서 보내는 문자메시지의 발신번호 변경 제한	
•	휴대폰에서 문자를 보낼 때 발신번호를 변경할 수 없게 했다. 이미 시행 중인 휴대폰을 포함해 10월부터 출시되는 휴대폰은 발신번호 변경을 할 수 없게 되고, 기존에 보급된 스마트폰의 경우는 펌웨어 업그레이드 방식으로 변경할 수 없도록 했다. 발신번호가 변경된 문자메시지를 통신사업자가 전달과정에서 차단하고 그 사실을 문자 발송자에게 고지하는 내용도 포함된다.

190) 방송통신위원회 보도자료, “보이스피싱 피해 예방을 위한 발신번호 조작방지 가이드라인”, 2012.7.31.자

② 인터넷에서 발송되는 피싱 문자 차단

- 문자메시지에 ‘보안등급’ 과 같이 피싱에 자주 인용되는 문구가 들어가면 통신사업자가 이를 차단한다. 금융기관 전화번호 등을 발신번호로 사칭해서 인터넷 웹에서 발송되는 문자메시지를 통신사업자가 사전에 차단한다. 한국인터넷진흥원은 이를 위해 피싱 신고내용을 분석하여 피싱에 사용된 전화번호 및 문구패턴을 분석하고 DB로 만들어 통신사업자에게 제공한다.

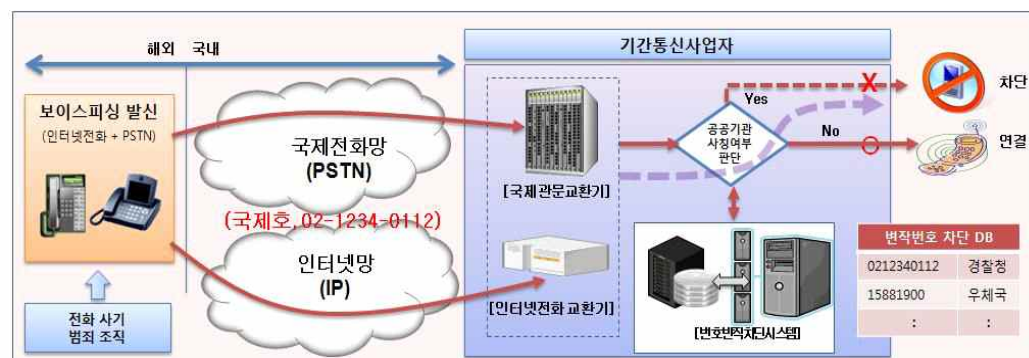
③ 인터넷 발송 문자메시지 식별기호 표시 및 고유번호 부여



- 인터넷 웹상에서 발송된 문자메시지의 본문에 특정 식별기호를 표시하는 제도를 도입한다. 이 식별기호는 그 문자메시지가 휴대폰에서 발송된 것이 아니라 인터넷 웹상에서 발송되었음을 의미한다. 인터넷에서 문자를 보낼 때는 회선 전화번호를 임의로 입력해 인터넷 발송 문자메시지에서 피싱과 문자폭력이 자주 발생한 데 따른 것이다.
- 또한, 피싱에 사용된 인터넷 발송 문자메시지의 전달경로를 쉽게 파악할 수 있도록 눈에 보이지 않는 고유번호를 통신사업자 및 대량 문자발송자에게 부여하고 문자규격으로 적용한다.

나. 보이스피싱 대책

① 공공기관 등 사칭 국제전화번호 차단



- 공공기관, 금융기관 등 보이스피싱에 자주 사칭되는 전화번호를 수집하고 내년 1월부터 외국에서 발신된 국제전화에서 이 번호가 사용되면 수신자가 전화를 받기 전에 통신사업자가 전화교환기에서 사전적으로 차단한다.

② 피싱에 이용된 가입자회선 해지 등 피해확산 차단

- 보이스피싱 전화의 전달경로를 추적하여 국제전화 식별번호를 삽입하지 않거나 해당 전화번호를 차단하지 않는 등 기술적 의무를 위반한 사업자는 행정적 제재를 가하고 피싱에 이용된 가입자회선은 직권 해지한다.

③ 국제전화 알림 및 수신거부 서비스 제공

- 스마트폰의 경우 국제전화가 걸려올 때 “국제전화입니다” 라는 음성 벨소리를 선택할 수 있게 되며, 유선전화단말기 등에 대해서는 관련 규격을 표준화하여 출시를 유도한다. 또한, 신사업자들이 국제전화 차단서비스를 부가서비스로 개발해 이를 신청하는 이용자는 국제전화가 걸려오는 것을 차단한다.

다. 메신저 피싱 및 피싱 사이트 대책

① 메신저 가입인증 강화 및 피싱방지 자가점검 리스트 제공

- 카카오톡 같은 메신저에 가입할 때 타인 명의 도용사례를 줄이기 위해 회원가입 시 문자 발송을 통한 인증과정에서 인증 실패 횟수를 제한하는 방식으로 본인 인증 체계를 강화한다. 또한, 피싱방지를 위한 자가 점검 체크리스트를 제공하여 사업자가 자율적으로 점검하도록 한다.

② 피싱사이트 신고절차 개선 및 차단 강화

- 피싱에 이용된 가짜 인터넷사이트를 차단하는데 걸리는 시간을 현행 2시간에서 1시간으로 줄이기 위해 한국인터넷진흥원과 금융기관과의 핫라인을 가동하고 신고양식을 통일, 간소화한다.

라. 피싱대응센터 설립

- 전기통신망을 악용한 복합적인 피싱범죄 대책을 시행하고 보완할 전담기관으로 ‘피싱대응센터’가 한국인터넷진흥원 내에 설치, 운영한다.

2. 신·변종 전기통신금융사기 피해방지 종합대책¹⁹¹⁾(2013년)

2012년 1월 보이스피싱 피해방지 종합대책 시행 이후 전통적인 보이스피싱 피해는 감소 추세를 보였으나 기존 대책만으로는 방지하기 어려운 메모리해킹·스미싱 등 인터넷 및 스마트폰 기반의 고도화된 기법을 활용한 신·변종 수법이 등장하였다. 정부는 2013년 12월 금융위원회, 미래창조과학부, 법무부, 경찰청, 해양경

191) 금융위원회 보도자료, “신·변종 전기통신금융사기 피해방지 종합대책”, 2013.12.3.자

찰청, 금융감독원 등을 중심으로 전기통신금융사기 방지를 위한 범부처 협의회를 구성하여 「신·변종 전기통신금융사기 피해방지 종합대책」을 발표했다.

종합대책은 피싱·파밍과 관련해서 국내외에서 신규로 생성되는 도메인을 분석하여 수사, 공공, 금융기관과 비슷한 도메인을 사전에 탐지해 차단하는 시스템을 구축하고, 공공·금융기관의 사이트 접속 시도 시 해외로 이동하는 트래픽을 탐지하여 ISP를 통해 해외 파밍사이트로의 이동을 차단하는 시스템을 도입하기로 하였다. 스미싱과 관련해서는 휴대폰 발송 번호변경 문자차단, 웹발신 문자 알림 서비스, 스미싱 차단앱 기본 탑재를 비롯하여 사이버트랩시스템, 지능형 스미싱 대응 시스템을 개발하기로 하였다. 메모리해킹과 관련해서는 은행권의 키보드 보안 프로그램에 메모리해킹 방지기능을 보완하도록 조치하고, 수취계좌번호, 이체금액 입력까지의 단계인 예비거래가 비정상적으로 종료되는 등 메모리해킹이 의심될 경우 SMS 또는 전화를 통한 본인인증을 하도록 인증절차를 강화하였다.

또한 정부는 2014년에 피해금 환급에 치우친 기존의 법을 개정해 전기통신금융사기 범죄에 효과적으로 대응하는 한편, 정부와 금융회사의 피해예방 노력을 강화하기 위해 「전기통신금융사기 피해금 환급에 관한 특별법」을 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」으로 변경하였다. 이를 통해 피해구제대상 확대, 전기통신금융사기죄 신설, 금융회사의 본인확인 의무화, 금융회사 이상 금융거래 탐지 시 지연·일시정지, 사기이용계좌 명의인에 전자금융거래 제한, 과태료 부과, 포상금 지급, 정부의 대응 근거 규정 마련 등을 포함하였다. 금융회사의 본인확인 의무화는 온라인으로 대출 신청 및 저축상품 해지 시 금융회사는 전화인증 또는 휴대폰 SMS인증 등을 통해 본인확인을 해야 하도록 규정했다. 자체 점검인 이상금융거래 탐지시스템을 통해 이용자 계좌가 금융사기에 이용된다고 인정될 경우 이체·송금을 지연 또는 일시 정지 등 ‘임시조치’를 취하게 했다. 뿐만 아니라 금융회사는 보이스피싱 범죄 확산을 방지하기 위해 사기이용계좌인 대포통장 명의인에 대해 인터넷·스마트뱅킹, ATM이체 등 전자금융거래를 제한하도록 했다. 금융위는 사기이용계좌 발생 건수 등을 고려해 금융회사에 필요한 조치를

명할 수 있고, 미이행시 금융회사에 과태료를 부과했다.

통신사기피해환급법은 2016년 7월 26일 한 차례 더 개정되었다. 법인고객이 본인확인 조치를 신청한 경우에만 본인확인 조치를 하도록 하고, 사기이용계좌에 대한 지급정지 조치가 이루어진 이후에는 압류·가압류 등의 강제집행 명령신청을 금지하도록 하였다. 해당 개정을 통해 향후 대포통장 등의 불법 양수·양도 광고 행위를 금지하고 처벌규정을 마련해 불법행위 유인 광고 억제 및 대포통장을 근절하고자 했다. 이와 함께 대포통장 광고 및 보이스피싱에 이용된 전화번호를 중지할 수 있는 근거를 마련해 전자금융사기 피해 예방에 기여하고, 지급 정지된 사기이용계좌에 대해 압류·가압류 등 강제집행을 할 수 없도록 하였다.

그러나 보이스피싱 범죄와 관련하여 정상적인 상거래 대금이라 하더라도 피해자의 계좌로부터 송금·이체된 피해금이라면, 해당 계좌가 사기이용 계좌에 해당되어 계좌명의인의 이의제기를 반려하고 있었고, 이로 인해 소송 등의 일체의 대항을 할 수 없는 문제가 발하였다. 실제 2014년부터 2016년까지 보이스피싱 피해를 이유로 20회 이상 유선을 지급정지를 신청하여 허위 신고자로 의심되는 자가 70여명이나 되었고, 이들의 신청으로 인해 지급정지된 계좌수만 6,900여개에 달했다.

이에 따라 2018년 다시금 통신사기피해환급법을 개정하여 피해자로부터 입금된 금액이 재화나 서비스를 제공하고 받은 금액임을 소명하는 경우 계좌명의자의 이의제기를 할 수 있도록 허용하고, 누구든지 지급정지가 된 사기이용계좌의 채권 전부 또는 일부와 관련하여 손해배상·부당이득반환청구소송 등의 제기를 금지하고 있었던 법률 조항의 개정하여 지급정지 중에도 명의인 또는 피해자는 그 상대방에 대하여 채무부존재확인·부당이득반환청구 소송을 제기할 수 있게 하였다. 또한 허위의 보이스피싱 범죄자를 막기 위해 해당 허위 신청자의 계좌자료를 금융기관이 감독당국에 제공할 수 있는 법적 근거를 마련하였다.

3. 전기통신금융사기 방지 종합대책¹⁹²⁾(2018년)

2014년 이후 보이스피싱 피해가 감소하였으나 2018년부터 신종 수단인 메신저 피싱, 불법사이트·앱 사기로 인한 피해가 증가하여 새로운 국면을 맞이하게 되었다. 간편송금을 이용한 보이스피싱의 피해 규모는 낮은 수준이었지만 간편송금시장의 성장으로 선제적 대응이 필요하다는 의견도 제기되었다. 이에 따라 2018년 금융위원회, 법무부, 과학기술정보통신부, 외교부, 경찰청, 방송통신위원회, 방송통신심의위원회, 금융감독원은 합동으로 「전기통신금융사기 방지 종합대책」을 발표하였다. 주요 내용을 살펴보면 다음과 같다.

〈표 4-4〉 관계부처 합동, 전기통신금융사기 방지 종합대책(2018년)

1. 보이스피싱 수단별 대응 강화		
(1) 신종 보이스피싱 수단에 대한 대응 강화		
① 메신저 피싱 예방 조치 강화	19.上	관계부처
② 불법 금융사이트에 대한 차단 조치 강화	19.上	방통위
③ 보이스피싱에 이용되는 악성 앱 모니터링 강화	19.1월	금융위
④ 선불전자금융업자를 통한 보이스피싱 피해 방지	19.上	금융위
(2) 전화·SMS 등 기존의 보이스피싱 수단에 대한 대응 강화		
① 보이스피싱 등 금융사기 방지를 위한 데이터 활용 체계 구축 방안 마련	19년	금융위
② 전화·SMS 피싱을 차단할 수 있는 AI 기반 App 보급	19년	금감원
③ 보이스피싱 사용 전화번호 이용중지 기간 법정화	19.上	과기정통부
④ 발신번호 변작 다수 신고 통신사업자 현장점검 강화	19년	과기정통부

192) 금융위원회 보도자료, “전기통신금융사기 방지 종합대책”, 2018.12.18.자

⑤ 휴대전화 부정사용 방지를 위한 서비스 제공 의무화 및 휴대전화 가입자에 대한 본인확인 전수조사 실시	19년	과기정통부
-----------------------------------------------------------	-----	-------

2. 대포통장 사전 방지·사후 제재 강화

(1) 사전예방 조치 강화

① 금융회사의 대포통장 발생에 대한 개선 조치 강화	19.上	금융위
② 인터넷전문은행의 비대면 계좌 개설시 고객 확인 절차 강화	19.上	금융위
③ 사기이용·의심계좌 정보 공유 및 모니터링 강화	19.上	금감원
④ 전자금융거래 제한 관련 해제 요건 강화 추진	19.下	금융위

(2) 사후제재 강화

① 대포통장 양수도 처벌 규정 강화 (전자금융거래법 개정)	19년	금융위
② 통장의 매매·대여 권유·중개, 계좌번호 대여·유통행위 처벌 근거 명확화 (관련 법령 개정 등)	19년	금융위
③ 보이스피싱 피해자금 전달 등에 단순 편의 제공 행위에 대한 제재 근거 신설 (전기통신금융사기법 개정)	19년	금융위

3. 보이스피싱 조직 엄정 단속

(1) 전담수사체제 가동, 보이스피싱 조직 단속 강화

① 전담수사체제 강화, 보이스피싱 특별단속 추진	19.上	경찰청
----------------------------	------	-----

(2) 보이스피싱 범죄자·협의자에 대한 여권 제재 강화

① 해외 체류 보이스피싱 범죄·협의자에 대한 여권 제재(발급·재발급 거부) 적극 시행	19.上	외교부
-------------------------------------------------	------	-----

(3) 해외 수사당국 등과의 공조 강화

① 해외 수사당국과의 공조 강화 조치 수행	19년	법무부
-------------------------	-----	-----

② 외국 경찰기관과 국제공조를 통해 해외범 단속·국내 송환 조치 활성화	19년	경찰청
-----------------------------------------	-----	-----

4. 보이스피싱 피해 구제 절차 정비

(1) 보이스피싱 피해구제 강화를 위한 부패재산몰수법 개정

① 전기통신금융사기법상 피해구제가 어려운 경우 사기자의 재산을 몰수하여 환급하는 내용의 부패재산몰수법 개정·시행	19년	법무부
----------------------------------------------------------------	-----	-----

(2) 채권소멸절차 未개시 근거 마련

① 채권소멸·환급절차 진행으로 인한 비용 대비 편익이 낮은 경우 채권소멸절차 未개시 근거 마련(전기통신금융사기법 개정)	19년	금융위
--------------------------------------------------------------------	-----	-----

5. 보이스피싱 방지 홍보·교육 강화

(1) 대국민 밀착형 보이스피싱 피해예방 홍보 추진

① 한국방송광고진흥공사를 통해 보이스피싱 방지 공익광고 추진	19년	관계부처
② 금융협회 등을 통해 고객밀착형 공동 캠페인 실시	19년	금융위·금감원
③ 신·변종 보이스피싱에 대한 소비자경보 발령(문자발송 등)	19년	관계부처

(2) ‘19년 대국민 보이스피싱 피해 방지교육 실시

① 대학 교육과정과 연계하여 보이스피싱 예방교육 실시 유도	19년	금감원
② 금융협회 등을 통해 보이스피싱 교육 콘텐츠 개발·전파	19년	금감원

종합대책에는 처벌 강화와 예방정책이 많이 포함되었고 새로운 기술의 도입과 금융권의 기술대책이 포함되었다. 정부는 대국민 메시지와 공익 광고를 확대하였고,¹⁹³⁾ 인터넷 전문 은행 및 간편송금 업체들과 관련한 대응과 은행권의 인터넷

193) 연합뉴스 보도(2019.5.16.), “보이스피싱 의심되면 바로 끊어야...정부, 전국민에 문자보낸다”,

메신저 사용 빈도의 증가에 대한 대응을 추가로 실시하였다.¹⁹⁴⁾

구체적으로 살펴보면, 신종 보이스피싱 수단별 대응을 강화하였다. 해외에서 발송된 메시지 및 친구등록이 되지 않은 사람에 대한 메시지 수신시 경고 표시를 강화하여 메신저 피싱을 예방하고, 불법 금융사이트에 대해 방송통신심의위에서 정보통신서비스 제공 사업자에 대한 시정요구 조치(삭제·접속차단 등)를 신속 시행하도록 하였다. 새로운 차단 기술의 적극 도입과 SNS 업체에 차단을 요청하는 방안도 병행하였다.

대포통장에 대한 사전예방·사후제재도 강화하였다. 금융회사의 대포통장 발생에 대한 개선 조치를 강화하여 자율적인 예방을 유도하도록 하고, 인터넷전문은행의 비대면 계좌 개설시 고객 확인절차를 강화하였다. 또한, 초고위험 고객군을 별도로 관리하여 더욱 강화된 고객 금융거래 목적 확인절차를 적용시켰다. 대포통장에 대한 사후제재 방안으로는 전자금융거래법 개정을 통해 대포통장 양수에 대한 처벌을 징역 3년 이하에서 5년 이하로 강화하고 대포통장 조직에 대해 범죄단체죄 적용을 통해 엄벌하고, 범죄수익의 환수를 추진하도록 하였다. 대가를 전제로 통장의 매매·대여를 권유·중개하는 행위를 처벌하고, 계좌번호 등을 보이스피싱 조직원 등에게 대여하는 등 보이스피싱 피해자금을 전달하는 행위도 처벌하도록 하여 처벌 대상을 확대시켰다.

보이스피싱 피해 구제 절차와 관련하여서는 부패재산몰수법을 개정하여 전기통신금융사기법상 피해구제가 어려운 경우 사기자의 재산을 몰수하여 환급할 수 있도록 보이스피싱 범죄수익을 ‘범죄피해재산’으로 규정하는 방안을 추진하도록 하였다. 전자통신금융사기법을 개정하여 채권소멸·환급절차 진행 등으로 인한 사회적 비용 대비 편익이 낮은 경우 채권소멸절차를 선개시할 수 있는 근거도 마련하기로

<https://www.yna.co.kr/view/AKR20190516055300002?input=1195m> (2020.10.1. 최종확인)

194) 전자신문 보도(2018.12.18.), “금융당국, 유관부처와 ‘메신저 피싱’ 차단 나서... 종합대책 발표”, <https://www.etnews.com/20181218000187> (2020.10.1. 최종확인)

하였다.

보이스피싱 대응을 위한 기술개발도 강화하였다. 신종 보이스피싱은 SMS 등을 이용하는 스미싱(Smishing)을 통해 악성 앱을 설치하도록 유도한 후, 피해자가 금융회사 대표번호로 발신하는 확인 전화를 가로채 전자금융사기 거래를 유도하는 방식으로 기존과는 다른 대처가 필요했다. 이에 금융보안원에서는 「전기통신금융사기 방지 종합대책」의 일환으로 보이스피싱 악성 앱을 탐지하기 위한 기법을 개발해 피해예방을 강화하였다. 금융보안원은 안드로이드 앱 분석 과정에서 처음 보이스피싱 악성 앱을 확인한 이후 약 1년여에 걸쳐 지속해서 추적해 악성 앱 유포방식, 주요 기능, 유형 분류 및 유포지 정보 등을 종합 분석해 인텔리전스 보고서로 발간했다.¹⁹⁵⁾

보이스피싱 악성 앱 유포지는 생명주기가 상당히 짧아 살아있는 유포지를 확보하는 것이 어렵지만, 금융보안원은 수 개월간 추적 끝에 다양한 금융회사를 사칭하는 악성 앱을 실시간으로 수집하였다. 그 결과 약 3,000 여개의 악성 앱을 확보하였고, 평균적으로 하루에 수십 개의 악성 앱을 수집하고 있다. 수천 개의 악성 앱을 확보한 이후 동일한 악성 앱 또는 유사성 등을 확인하기 위해 악성 앱 분류가 반드시 필요했다. 악성 앱은 공통적으로 C&C 정보가 앱 내부에 하드 코딩되어 있는 것, 그리고 앱의 가장 주된 기능인 전화 가로채기 코드를 특징으로 하는데, 이 두 가지 기능은 반드시 필요한 코어 기능들이기 때문에 변종이 발생하더라도 코드 상의 변화가 크지 않고, 코어 기능이기 때문에 개발자가 다른 경우 기능은 유사하더라도 구현 방식은 상이하기 힘들기 때문에 악성 앱 분류에 가장 적합한 특징이라고 판단했다. 해당 보고서에는 C&C 하드코딩 유형은 세부 유형까지 포함해 총 9가지 형태로 나누었고, 전화 가로채기 코드 유형은 클래스명을 기준으로 총 10가지 형태로 나누었다.

보이스피싱 악성 앱에 대한 모니터링을 강화하기 위해 자체적으로 개발한 악성

195) 금융보안원 보고서, “2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링]”, 2018

앱 탐지기법은 금융보안원 피싱탐지시스템에 추가되어 운영된다. 금융보안원 피싱탐지시스템은 금융회사, 경찰청, 검찰, 각종 포털 등으로 속이는 피싱사이트를 24시간 365일 탐지하는 자체 개발 시스템으로 2018년도 약 1만5천여 건의 피싱사이트를 탐지해 차단시켰다.

4. 보이스피싱 척결 종합방안¹⁹⁶⁾(2020년)

가. 추진배경

전 세계적 코로나 사태 이후 2008년 서브프라임 모기지발 금융위기의 대응과 유사하게 개별 민생 범죄에 대한 대응이 중시되어 이에 따라 대통령이 반부패정책협의회(2020.6.22일)에서 보이스피싱과 같은 민생침해 범죄에 대해 초기부터 강력하게 대응하고, 부처 간 공조를 강화하여 신속하게 대책을 마련할 것을 지시했으며 국무총리도 보이스피싱 등 민생침해 금융범죄에 대해 강력히 대처할 것을 지시했다. (2020.1.23, 국정현안점검회의)

2018년 전기통신금융사기 종합대책 이후 관계부처 합동으로 보이스피싱에 대해 종합적으로 대응한 결과, 2019년도 상반기 보이스피싱 피해에 비하여 2020년도 상반기 피해는 감소하였으나 코로나 재난 상황이 전 세계적 상황이기에 해외 조직으로 대부분 구성된 보이스 피싱 조직의 활동성 감소와 관련이 있다고 판단되어 재난 상황 완화 이후의 피해 증가 가능성은 무시할 수 없었다. 이에 각 관계부처는 아래의 5가지 추진 전략을 바탕으로 세부 계획을 발표하였다.

추진전략은 크게 (1) 전방위적인 예방, 차단 시스템 구축, (2) 단속과 처벌의 실효성 확보, (3) 발생한 피해에 대해 종합적 피해구제 강화, (4) 관계부처간 상시 협업 체계를 구축·강화, (5) 홍보 강화를 통해 국민들의 경각심 환기로 나뉘며 각 전략마다 구체적인 세부 전략을 통해 개별 부처의 협업 목표와 추진 방안을 제시하였다.

196) 과학기술정보통신부 보도자료, “디지털 경제의 신뢰 기반 조성을 위한 보이스피싱 척결 종합방안”, 2020.6.24.자

〈표 4-5〉 디지털 경제의 신뢰 기반 조성을 위한 보이스피싱 척결

종합방안(2020년 6월)

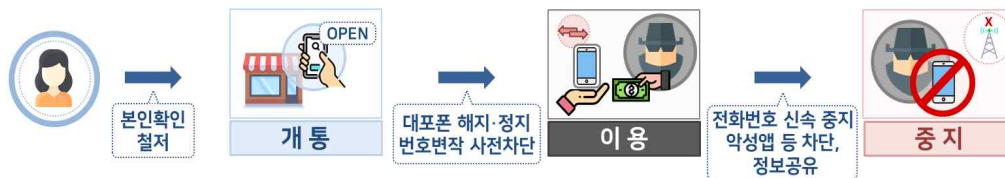
(전략 1) 보이스피싱 범죄 시도가 성공하지 못하도록 전방위적인 예방, 차단 시스템을 구축	
세부 전략	(1) 보이스피싱에 이용되는 전기통신수단 신속 예방·차단 ① 스마트폰 등 통신수단 부정사용 자체를 사전에 방지하기 위해 “개통-이용-중지” 단계에 걸쳐 신속·종합적 대응체계 구축 ② 다양한 통신수단(전화번호, 악성앱, 피싱사이트 등)이 보이스피싱 등에 이용된 경우, 신속하게 이용중지·차단하도록 개선
	(2) 보이스피싱 예방을 위한 디지털 신기술 개발·활용 촉진 ① 통신사업자 등이 각종 빅데이터·AI 연계 시범사업 등을 활용하여 보이스피싱 탐지·대응 기술·서비스 고도화할 수 있도록 지원 ② 보이스피싱 유형별로 능동적·선제적 예방 기술 확보 위해 R&D 과제 기획 수행 및 과제화 추진
	(3) 보이스피싱 의심 금융거래 모니터링 강화 ① (법제도) 빅데이터·AI 등 신기술을 활용하여 금융회사 이상금융거래 탐지시스템(FDS)을 적극 개선토록 법제도 정비를 추진 ② (인프라) 금융분야 데이터 관련 유관기관의 의심거래 모니터링 지원을 위한 금융사기 방지 인프라 고도화 ③ (대응체계) 금융권 공동 컨소시엄을 先구축하고, 금융·통신·유통 등 다분야 사기정보 컨소시엄 구축 추진
	(4) 민간사업자의 예방 의무 강화 ① 금융회사의 보이스피싱 예방을 위한 의무를 강화 ② 통신사업자 자체 모니터링·제재 등 보이스피싱 예방노력 강화
(전략 2) 금융범죄의 유인 자체를 없앨 수 있도록 단속과 처벌의 실효성을 확보	
세부 전략	(5) 보이스피싱 관련 수사·단속 강화 ① (범죄 수사·단속) 보이스피싱 관련 범죄에 대해 엄정한 단속이 이루어질 수 있도록 일제 수사 등 법집행 강화 ② (유관업체 점검) 일제단속기간 중 통신사업자 등 점검 강화
	(6) 보이스피싱 관련 범죄 처벌 강화 ① 보이스피싱의 통로인 대포통장 범죄 처벌을 대폭 강화 ② 보이스피싱 조력 행위에 대해서도 처벌 규정 신설 ③ 보이스피싱 범죄 자체에 대한 처벌도 대폭 강화

나. 전방위적인 예방, 차단 시스템 구축

1) 보이즈피싱에 이용되는 전기통신수단 신속 예방·차단

첫 번째 추진 방안은 전방위적인 예방, 차단 시스템을 구축하는 것이다. 통신수단의 부정사용 자체를 방지하는 한편, 보이즈피싱에 이용된 수단은 신속·철저히 중지 가능한 체계를 구축하기로 하였다.

[그림 4-2] 보이즈피싱 전기통신수단 신속 예방·차단 전략



이를 위해 보이즈피싱에 대표적으로 이용되는 범죄 수단인 대포폰, 특히 선불폰·외국인 명의폰 중심으로 개통-이용 단계에서의 관리감독을 강화하기로 하였다. 사용기한 도과한 선불폰과 사망자·출국 외국인·폐업법인의 未이용회선을 정기적으로 정리하고, 그 주기도 단축하기로 하였다. 외국인 단기관광객 출국시 휴대전화 신속정지를 추진하고, 휴대폰 단기 다회선 개통시 가이드을 마련하여 다회선 개통 억제하고, 공공기관·금융기관 등을 사칭하는 전화번호 거짓표시(변작)를 사전에 방지할 수 있도록 차단 체계를 구축하기로 하였다. 공공금융기관의 주요 전화번호 화이트리스트(변작 차단 목록) 탑재를 확대하고 기존 기관 확대 및 현재 대표번호 위주에서 리스트 대상을 모든 보유번호 단계적으로 확대하는가 하면, 대량 문자발송 대행업체 등의 신청자 전화번호 확인(위·변조 여부) 절차를 강화하고 빈도도 최초 1회 인증에서 주기적 인증으로 확대하기로 하였다. 발신번호 거짓표시나 변작 관련 의무 위반시 과태료를 3천 만원에서 5천 만원으로 상향하기로 하

였다.

보이스피싱에 이용될 가능성이 높은 심박스에 대해서는 관계부처 협업 등을 통해 사전에 제거하도록 하고, 관세청과 협업하여 밀수 등 단속을 강화하여 범죄이용을 방지하며, 국내에 반입된 심박스에 대해서는 수사기관을 중심으로 단속하기로 하였다. 아울러 과학기술정보통신부는 심박스 탐지를 고도화하기 위한 기술의 지속 개발을 추진기로 협의하였다. 무엇보다 중요한 것은 휴대폰 등 통신수단이 부정하게 사용되는 것을 방지하기 위한 대응기반 강화 및 건전한 이용 문화 조성이었다. 스마트폰 운영체제(OS)에 도난관리 SW를 탑재해 분실·도난시 타인의 단말기 사용을 원격으로 무력화(잠금)시키는 휴대전화 도난 방지기능(Kill Switch 기능 활용 지원을 위해, 휴대전화 개통시, 분실·도난 신고시 이용방법·기능 필수로 안내하고 적용을 지원하기로 하였다. 세계이동통신사업자협회(GSMA)와의 협약(MOU) 통해 분실·도난폰 정보 공유를 추진하는 등 국제공조를 통해 국내 뿐 아니라 해외에서도 분실·도난 휴대전화 원격차단을 강화해 나가로 계획을 수립하였다.

다양한 통신수단(전화번호, 악성앱, 피싱사이트 등)이 보이스피싱 등에 이용된 경우, 신속하게 이용중지·차단하도록 개선하는 것도 필요하다고 보았다. 정부는 보이스피싱 피해 신고 후 기준 통상 4~5일에서 최대 14~15일까지 걸리던 전화번호 이용중지에 대해 2일 이내 완료되도록 하였다. 각 부처별로는 금융위원회는 현행 피해구제신청서에 전화번호 이용중지 신고서식 포함하는 방안을, 한국인터넷진흥원과 금융감독원은 충분한 전화번호 정보 신고시 보다 신속히 이용중지 조치를, 방송통신위원회와 한국인터넷진흥원은 스팸 전화번호 및 전화가로채기 앱 전화번호 차단 조치를 강화하도록 협력하기로 하였다.

보이스피싱 등과 관련하여 이용중지된 전화번호는 재사용될 수 없도록 차단하고, 이용중지된 동일 전화번호는 타 통신사로 이동하더라도 사용하지 못하도록 조치하는가 하면 이용중지 기간도 1년에서 1년 6개월 이상으로 대폭 확대하기로 결정했다. 보이스피싱에 이용되는 전화번호 외 악성앱·피싱사이트 등 신종수단을 신

속·철저히 차단할 수 있도록 제도 개선 작업도 병행하기로 했다. 한국인터넷진흥원은 정보통신망법 체계·절차에 따른 악성앱, 피싱·해킹사이트 접속차단 요청이 있을 경우 신속하게 요청을 수행하고, 한국인터넷진흥원·금융보안원 간 보이스피싱 신종수단 정보 공유 체계를 강화하도록 하였다.

2) 보이스피싱 예방을 위한 디지털 신기술 개발·활용 촉진

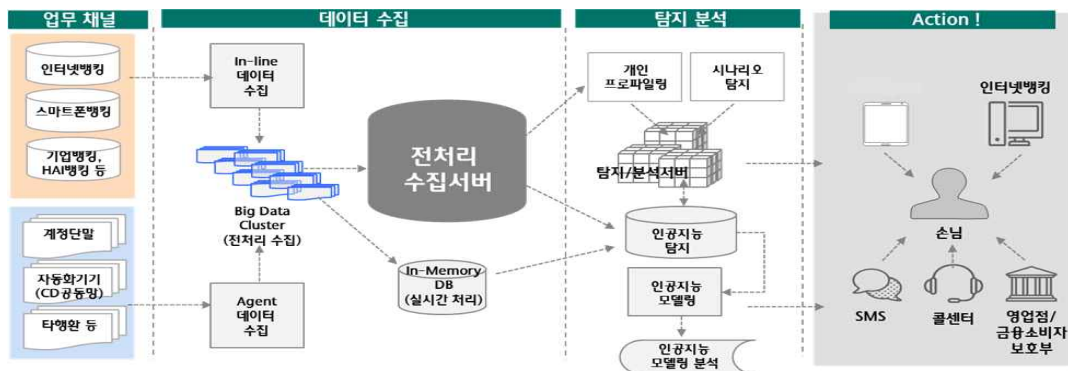
보이스피싱 예방을 위한 기술이 부족하다는 문제와 관련하여서는 보이스피싱 예방을 위한 디지털 신기술 개발·활용을 본격 지원하는 구체적 대안들을 마련하였다. 우선 통신사업자 등이 각종 빅데이터·AI 연계 시범사업 등을 활용하여 보이스피싱 탐지·대응 기술·서비스 고도화할 수 있도록 지원하기로 하였다. 통신사·금융권 등의 정보를 통합 활용하는 한편, 보이스피싱 음성(voice)·문맥(context)에 대한 머신러닝 기법 적용 등으로 지속적·자율적 고도화를 지원하고 보이스피싱 위험이 탐지된 경우 실제로 은행의 이상금융거래탐지시스템(FDS) 등과도 연계해 실질적 피해 예방 기여하도록 하였다. 통신사가 가지고 있는 통신정보와 및 CB사가 가지고 있는 금융정보를 결합·활용해 보이스피싱을 판별·예방할 수 있는 서비스 신규 출시도 지원하고, 관련 R&D 과제 투자에도 지원을 아끼지 않기로 하였다. 보이스피싱 유형별로 능동적·선제적 예방 기술 확보 위해 R&D 과제 기획 수행 및 과제화 추진하며 2020년 중 신종수법(인터넷전화, 심박스 등) 및 해외 동향 등을 반영해 R&D 과제 기획 및 요소기술 구체화하도록 할 계획을 세웠다. 2021년부터는 다 부처 협업으로 사회문제 해결형 R&D 과제화하고 법·규정 등에 저촉 없이 예방 및 조기 단속이 될 수 있도록 신속한 법제화를 추진하기로 결정했다.

3) 보이스피싱 의심 금융거래 모니터링 강화

금융회사나 일정한 전자금융업은 스스로 금융사기·사고 등을 탐지하기 위한 이상금융거래 탐지 시스템(FDS; Fraud Detection System)을 구축하여 보이스피싱 등 금융사기나 부정결제 사고 등 의심거래를 모니터링·차단 중이나, 금융관련 법

령상 금융회사등의 FDS 구축 등에 대해 별도의 법제도가 마련되어 있지 않고, 관련 인프라·대응체계도 효율적으로 활용되지 못하고 있다. 이에 따라 금융회사가 의심 금융거래를 모니터링하고 차단 가능하도록 법제도·인프라·대응체계를 구축하도록 지원하도록 하였다.

[그림 4-3] AI, 빅데이터를 활용한 FDS 운영 시스템



법제도 측면에서는 빅데이터·AI 등 신기술을 활용하여 금융회사 이상금융거래 탐지시스템(FDS)을 개선토록 법제도 정비를 추진하고, 금융회사가 FDS 개선 시 빅데이터·AI 등 신기술을 활용하기 위한 법적 불확실성을 해소하기로 하였다. 2020년 8월 5일부터 시행되는 개정 신용정보법은 금융회사등·CB사의 FDS 개발·분석을 위한 가명정보·빅데이터 활용을 활성화하고, 통신사기피해환급법 개정을 통해 빅데이터 기술을 통한 사기의심계좌 모니터링 업무 지원 서비스 제도화를 추진하기로 하였다. 나아가 통신사기피해환급법령의 개정을 통해 신기술 등을 활용한 의심거래 차단 수행에 대해 금융회사 및 그 임직원의 고의·중과실이 없는 한 면책할 수 있는 근거를 마련하기로 하였다.

인프라 측면에서는 금융분야 데이터 관련 유관기관의 의심거래 모니터링 지원을 위한 금융사기 방지 인프라를 고도화하는 것을 목표로 설정하였다. 2020년 1월부터 금융감독원이 은행권, 한국인터넷진흥원 등과 협업하여 은행권 전화번호 DB를 공유하고, 해당 DB에 없는 전화번호는 신고시 차단하도록 한 것을 모범 사

례로 들 수 있다. 인프라 고도화도 각 기관별로 구체적 추진 방안을 제시하고 있는데, 신용정보원은 신용정보 집중·활용 강화를 통해 보이스피싱 방지하고 금융결제원은 빅데이터 기술을 통한 은행의 사기의심계좌 모니터링 업무 지원을 위한 혁신금융서비스를 고도화하기로 하였다. 금융보안원은 금융분야 정보공유·분석센터(Information Sharing & Analysis Center) 기능을 강화하여 FDS 고도화를 지원하고, 신종 사기수단 분석·차단을 위한 기관 간 정보공유를 강화하기로 하였다. 신용조회회사는 다양한 신용정보를 기반으로 개인·기업의 금융사기(Fraud) 가능성을 평가하는 Fraud Scoring 시스템을 통한 금융회사에 대한 금융사기 방지 업무 지원 기능(Fraud CB)을 대폭 강화하기로 하였다.

대응체계와 관련해서 보이스피싱 위협 거래 탐지 시나리오 개발, 모바일 앱에 보이스피싱 차단 기능 탑재하는 등 금융회사 FDS 고도화를 위한 협업·기술공유 인센티브가 부족하다고 보았다. 이에 따라 금융권 공동 컨소시엄을 먼저 구축하고, 금융·통신·유통 등 다분야 사기정보 컨소시엄 구축을 추진하기로 하였다. 은행·금보원 등의 운영지원을 통해 금융회사 간 공동으로 신종수법 사례 분석, 모니터링 기법·차단기술 공유 등을 추진하고 금융분야 외 통신·유통 등 다양한 사기정보를 활용하여 보이스피싱을 방지할 수 있도록 다분야 사기정보 컨소시엄 구축을 지원하기로 하였다. 동 제도운영 관련, 선의의 피해자가 발생하지 않도록 컨소시엄 내 사기 혐의자의 권리 보호를 위한 장치도 검토하기로 하였다.

4) 민간사업자의 예방 의무 강화

정부, 공공기관의 노력만으로는 보이스피싱 예방·대응을 빈틈없이 수행하는 것이 불가능하다. 이에 실제 보이스피싱 범죄 수행 과정에서 이루어지는 금융 거래와 통신을 일선에서 통제할 수 있는 민간사업자의 예방 의무를 강화하고 민관협업을 추진하기로 하였다. 금융회사와 통신사업자를 민간사업자의 주요 주체로 삼고 각각의 예방 의무를 강화하기로 하였다. 금융회사는 보이스피싱 의심계좌에 대해 자체점검을 통한 임시조치 의무가 있으나, 이를 준수하도록 유도하는 규율이 부재

한 것이 문제점으로 지적되어 왔다. 특히 금융회사는 통신사기피해환급법 제2조의 5에 의하여 자체 점검을 통한 보이스피싱 피해의심 계좌에 대해 지연이체, 임시 지급정지 등 조치를 하여야 하나 위반시 불이익이 없어 강제력이 없었다. 이에 금융회사가 의심계좌 지급정지 등 보이스피싱 예방을 위해 필요한 의무를 강화하고, 이에 통신사기피해환급법 등 개정을 통해 금융회사에 대한 주의·경고, 과태료 부과 등을 하기로 하였다. 일정한 금융회사에 대해 이상금융거래탐지시스템(FDS)의 구축을 의무화하고, 의심계좌에 대한 자체 임시조치 의무 확대를 추진하며 FDS 시스템 구축이 미흡하여 피해가 크거나 자체 임시조치 의무 이행이 미흡 시 시정·제재 조치를 강화하기로 하였다.

통신사업자 자체 모니터링·제재 등 보이스피싱 예방 의무도 강화했다. 현재 통신사는 전기통신사업법상에 전화번호 변작 금지, 휴대폰 명의도용·부정가입 방지 시스템 구축 등 다양한 통신수단 부정사용 방지에 관한 의무가 규정되어 있으나, 보이스피싱 예방을 위한 자체 조치는 부족한 측면이 있다. 이에 종합대책에서는 통신 유통망에 대한 자체 모니터링·제재 및 수범사례 공유 등을 통한 통신사업자의 자율정화 노력 확대를 유도하기로 하였다. 수범사례는 과거 사례 추적·분석 통해 발신 전화번호에 보이스피싱 의심표시를 제공한 사례, 이상징후(단기 다회선 개통, 발신번호 집중 변경 등) 체크리스트 운용, 관련 지침 배포 및 미준수에 대한 패널티 부과(대리점 계약서 반영) 등이 있다.

다. 단속과 처벌의 실효성 확보

1) 보이스피싱 단속 강화

수사기관은 그간 보이스피싱에 대한 단속을 강화해왔으나, 계속되는 인출책의 등장과 해외 범죄조직에 대한 마땅한 대책을 마련하지 못했다. 이에 종합대책은 관계부처 합동으로 보이스피싱 관련 범죄 일제 단속을 위한 구체적 대안을 마련하였다.

첫 번째로, 보이스피싱 관련 범죄에 대해 엄정한 단속이 이루어질 수 있도록 일제 수사 등 법집행을 강화하기로 하였다. 대책 발표와 함께, 연말까지 보이스피싱 등에 대해 경찰 지능범죄수사대·광역수사대, 금융감독원 불법금융단속전담팀 등 불법금융행위 유관기관이 일제히 집중단속을 실시하고, 국내·외 기관과 연계·협업을 통한 보이스피싱 범죄를 단속하기로 하였다. 경찰청과 대검찰청은 보이스피싱 조직이 주로 본거지를 두고 있는 해외에 대한 국제 수사 공조체계를 강화하고, 해외 국가와 MOU를 체결하는 등 핫라인을 강화하기로 하였다. 경찰청 및 지방경찰청 소속 보이스피싱 전담인력을 확대하고, 금융회사와 연계하여 집중단속을 실시하기로 하였다. 또한 심박스 등 밀수 단속도 강화하기로 하였다. 불법행위에 대해서는 법조항을 엄격히 적용하여 허용 가능한 최대수준으로 처벌하기로 방침을 정했다.

두 번째로, 일제 단속기간 중 통신사업자 등 유관업체 점검을 강화하기로 하였다. 과학기술정보통신부는 금융사기 등에 악용될 수 있는 대량문자 발송 대행업체 및 일부 설비임대 통신사(舊 별정통신사)를 집중 점검하고, 위법사항 적발 시 엄중하게 제재하기로 하였다. 문자 발송 의뢰자에 대한 본인확인 의무 및 전화번호 거짓표시(공공·금융기관 등 사칭) 방지를 위한 기술적 조치 의무 위반 여부 등에 대한 단속·제재를 실시하기로 협의하였다.

2) 보이스피싱 관련 범죄 처벌 강화

보이스피싱 범죄가 디지털 금융·통신 인프라에 대한 신뢰를 저해하는 등 일반 사기범죄에 비해 중대한 범죄임을 감안하여 보이스피싱 및 이와 관련된 범죄를 보다 무겁게 처벌하여 경각심을 제고하도록 하였다. 우선 보이스피싱의 통로인 대포통장 범죄 처벌을 대폭 강화하기로 하였다. 전자금융거래법이 2020년 4월 말 국회를 통과하여, 2020년 8월 20일부터 시행된 바 있다. 대포통장 양수도·대여 등의 행위에 대한 처벌(법정형)을 강화하여 기존 징역 3년, 벌금 2천만원의 처벌을 징역 5년, 벌금 3천만원으로 상향하였다. 범죄(보이스피싱 등)에 이용될 것을 알

면서 계좌 관련 정보를 제공·보관·전달·유통하는 행위도 대포통장 범죄 수준으로 처벌하도록 하였다.

보이스피싱 조력 행위에 대해서도 처벌 규정을 신설할 계획이다. 보이스피싱 단순 조력 행위에 대한 처벌 규정을 신설하여 다수의 국내 송금·인출책 범죄에 대한 경각심 강화한다. 해당 규정이 신설되면 범죄에 이용할 목적으로 또는 범죄에 이용될 것을 알면서, 전자금융거래를 통해 타인으로부터 자금을 교부 받아 전달한 자 또는 해당 행위를 도운 자에 대해서도 처벌이 가능해진다. 동시에 보이스피싱 범죄 자체에 대한 처벌도 대폭 강화한다. 관계부처와 협의하여 보이스피싱 및 유사 금융사기 범죄의 범정형을 대폭 강화하는 방안도 검토하며, 대포통장 등 보이스피싱 관련 범죄행위를 일관되게 규율할 수 있도록 통신사기피해환급법 개정하는 방안을 검토·추진하기로 하였다.

라. 발생한 피해에 대해 종합적 피해구제 강화

1) 금융회사 등을 통한 피해구제 제도 정비

형사처벌과 동시에 국민 피해에 대한 구제제도를 잘 정비하여야 국민이 체감하도록 추진하기로 하였다. 현재는 보이스피싱 발생시 피해자의 피해구제신청을 거쳐 사기이용계좌를 신속히 지급정지하여 피해금 환급이 가능하나 지급정지 제도에 사각지대가 존재할 뿐만 아니라, 피해금 환급을 넘어 금융회사등이 직접 배상 책임을 지는지 여부도 불분명하다. 이에 지급정지제도 및 피해배상 제도를 개선하여 금융소비자를 두텁게 보호하는 방안을 마련하고자 하였다.

우선 금융회사등이 사기이용계좌에 대해 충분한 지급정지 조치를 시행·유지할 수 있도록 제도를 정비한다. 현행 법률에 의하면 금융회사가 보이스피싱 의심계좌에 대해 자체 지급정지를 하여도, ‘본인이 자금이체 한 것이 확인’ 시 지급정지를 해제하여야 한다. 보이스피싱 의심계좌에 대해 금융회사가 자체 판단으로 지급정지를 지속할 수 있는 근거를 명확히 하도록 하였다. 간편송금업자 등 전자금융업

자 또한 지급정지와 관련한 보이스피싱 방지 의무가 없고, 이에 따라 금융회사와 사기이용계좌 관련 정보를 공유하는데 한계가 있어 왔다. 이에 통신사기피해환급법 개정을 통해 간편송금업자 등에 대해서도 지급정지 등과 관련하여 일정한 보이스피싱 방지 의무를 부과하고, 금융회사와 사기이용계좌 관련 정보의 공유를 허용하도록 하였다.

이번 대책의 가장 핵심이 되는 내용 중 하나는 금융회사등의 보이스피싱에 대한 책임을 강화하는 것이다. 현행법은 금융거래시 본인확인을 하지 않은 경우나, 수사기관·금감원의 정보제공 또는 정당한 피해구제신청이 있었음에도 지급정지 선이행 시에만 금융기관이 배상책임을 지는 구조로 되어 있어 배상책임 인정 사례가 거의 없었다. 보이스피싱의 통로로 이용되는 금융회사등이 금융인프라 운영기관으로서 책임을 다하도록 제도 개선이 필요하다. 이에 종합대책에서는 보이스피싱에도 이용자의 고의·중과실이 없는 한 금융회사등이 원칙적으로 배상책임을 지는 방안을 추진하도록 하였다. 피해자가 ‘사기·강박’에 의해 거래를 허용하게 된 점, FDS 구축 등으로 사전예방 노력을 강화하도록 할 필요성 등을 고려하여 배상책임의 요건과 범위를 조정해갈 예정이며 금융회사등과 이용자 간에 보이스피싱 관련 피해액이 합리적으로 분담될 수 있도록 기준을 마련할 예정이다. 이와 관련한 연구용역 결과를 바탕으로 금융회사 등의 의견을 충분히 수렴하여 향후 통신사기피해환급법등의 개정을 추진한다

2) 보이스피싱 보험을 통한 피해구제 활성화

보이스피싱 피해를 보상해 주는 여러 보험상품이 판매 중이나, 보장 금액이 제한적이고 이용도가 낮아 피해 구제에는 실질적인 한계가 있었다. 대부분의 보험이 최대 보장한도 1천만원 이내, 보장한도액 5백만원 기준으로 피해 금액에 비해 보장 금액이 낮으며 보험 가입의 동인도 거의 없었다. 이에 보이스피싱 피해 구제 지원을 위한 보험상품의 보장 범위를 확대하고 판매채널 등도 확대할 수 있도록 추진한다는 계획을 발표하였다. 특히 기존 보험 판매 채널(보험설계사) 뿐 아니라

통신대리점, 은행 등 금융회사 창구 등에서 다양하게 해당 상품을 안내하도록 하여 보험 상품의 홍보를 강화하기로 하였다.

마. 관계부처간 상시 협업체계를 구축·강화

보이스피싱 수법이 다양한 ICT 기술을 바탕으로 기존의 금융분야를 넘어 복잡·교묘해지고 있으나, 현재 각 기관 소관법령에 근거한 개별 대응 시스템으로는 진화하는 수법에 맞는 신속하고 유연한 대응이 곤란한 측면이 있다. 반면, 해외의 경우 관계부처 간 통합적인 대응체계를 구축하여 민생을 침해하는 금융범죄에 효과적으로 대응하고 있다. 예를 들어 대만은 反사기부서통합 조정회의 및 反사기연합 방지회의를 구성하여 산하에 전담 통합신고센터 등을 운영하여 금융사기에 종합적으로 대응하고 있다. 정부도 유관부처간 상시 협업이 가능한 시스템 구축 검토하고 구체적 협업체계를 가동하도록 하였다.

우선 금융·통신·수사당국, 민간사업자 공동 대응체계를 강화하기로 하였다. 정부는 2020년 6월말부터 금융위, 과기정통부, 방통위, 법무부, 대검찰청, 경찰청, 금감원, 민간업자 등이 포함된 보이스피싱 관계부처 전담 TF를 구성·운영하고 있다. 관련 기관 간 중점협약사항 도출 및 MOU 체결도 추진하여 실질적인 협업체계를 강화하도록 하였다. 두 번째로 공동 대응체계 구축을 기반으로 민간업자 간 협업을 적극 지원하고, 정부·민간업자 협업을 강화하기로 하였다. 금융·통신당국은 해외 발신, 변작 전화번호 등을 사전에 차단하는 서비스 제공 등을 위한 금융·통신사 협업을 적극 지원하여 금융·통신 新기술을 이용한 신종수법에 효과적·선제적으로 대응한다. 통신당국은 KISA·금감원·수사기관·통신사 간 핫라인을 구축한다. 과학기술정보통신부·KISA 간 정례적 기술협의회를 기술정책협의회로 확대 개편하고, 유관기관의 참여도 적극 유도한다. 수사당국은 금융당국, 금융회사와의 협업으로 보이스피싱 피해 구제를 가장한 악의적인 피해 신고 방지를 위해 허위 피해구제 의심 사건 수사를 신속히 처리하기로 하였다.

바. 홍보 강화를 통해 국민의 경각심 환기

보이스피싱 방지 홍보 노력은 금융부문 중심으로 한정되어 진행되어 왔다. 이 때문에 금융소비자의 보이스피싱 이해도가 낮을 뿐 아니라, 현행보다 적극적인 홍보가 필요하다는 의견도 다수 개진되어 온 것이 사실이다. 이에 대국민 접촉이 많은 관계부처, 지자체 등을 통해 전방위적인 대국민 홍보를 연중 실시하기로 하였다. 우선 방송, 광고, 캠페인 등을 통한 입체적인 대국민 홍보가 절실하다고 보았다. 대국민 접점이 많은 곳(휴대폰 대리점, 대중교통, 은행창구 등)에서 보이스피싱 방지 십계명 및 신종수법 사례 배포, 길거리 캠페인 실시, 공익광고 송출 등을 수행하도록 하였다. 경찰청 홍보예산 등을 활용하여 공중파 TV, 유튜브 광고 등 홍보를 강화하고, 금융감독원은 보이스피싱 수법을 알리기 위한 유튜브를 운영하기로 하였다. 공영방송사와 협업하여 보이스피싱 수법 소개 등을 위한 별도 방송편성을 통해 대국민 이해도를 높이는 것도 필요하다고 보았다.

국민 체감형 경각심 강화 프로그램도 운영하기로 하였다. 금융감독원, 통신당국, 통신사 등이 협업하여 신종수법 출현·피해증가 우려시 소비자경보 발령 및 경고문자 발송 체계를 구축하는 한편 행정안전부는 전 국민 대상 문자를 긴급재난문자처럼 발송하여 경각심을 강화하는 방안도 추진하기로 하였다. 현재 보이스피싱 방지 전국민 대상 문자는 통신사 협조를 통해 SMS(40자)로만 발송함에 따라 개략적인 내용만 알릴 수 있었지만 긴급재난문자를 활용하면 장문의 내용을 신속하게 보낼 수 있다. 금융회사도 피해 예방 십계명, 지연인출제도·지연이체서비스 등에 대한 홍보를 다양한 채널을 통해 홍보할 것을 장려하기로 하였다.

제4절 정책평가 및 시사점

정부는 2006년에 보이스피싱이 발생한 이래 지난 15년간 다양한 대책을 수립하여 피해 예방을 위해 노력하여 왔다. 하지만, 보이스피싱이 글로벌화·지능화·조직화되고, 온라인·비대면으로 의사소통, 경제활동 및 금융거래가 활발해지면서 여전히 계속되고 있다. 무엇보다도 범죄조직들이 해외에 소재하고 있어 검거가 어렵고, 신종에 대해 선제적으로 대응하지 못하기 때문으로 해석된다.¹⁹⁷⁾

그간 정부정책을 평가해보면 부처의 개별대책을 넘어서 발 빠르게 범정부 차원의 종합대책을 수립하였다는 점이다. 초기에는 개별 부처에서 이슈에 따라 산발적으로 대책을 발표하였으나 최근에는 금융위원회, 방송통신위원회, 방송통신심의위원회, 과학기술정보통신부, 법무부, 외교부, 경찰청, 금융감독원, 한국인터넷진흥원 등 모든 부처가 참여하여 대책을 수립하고 있다. 그 결과 2012년 보이스피싱 피해방지 종합대책, 2013년 신·변종 전기통신금융사기 피해방지 종합대책, 2018년 전기통신금융사기 방지 종합대책, 2020년 보이스피싱 척결 종합방안 등을 굵직굵직한 대책을 신속하게 마련하여 시의성 있게 대응하였다. 정부가 통신사기피해환급법이라는 특별법을 제정한 것도 높게 평가할 수 있다. 특별법에서 전기통신금융사기죄를 신설하여 가중처벌하고, 피해금 환급절차까지 규정하여 수사, 예방 및 피해구제에 기여하였다. 나아가 국가·공공기관뿐만 아니라 이동통신사, 금융기관, 통신사업자 등 민간의 참여를 적극 추진하였다는 점이다. 반드시 필요한 사안에 대해서는 법률에서 의무규정을 신설하고 협의가 필요한 부분에 대해서는 함께 협의해 나가는 방식은 긍정적으로 평가할 수 있을 것이다. 마지막으로 법제·수사뿐만 아니라 기술을 포함하여 포괄적인 대책을 마련하였다는 점이다. 그간의 범죄 대책은 주로 법제나 수사역량을 강화하는데 방점을 두었으나, 종합대책은 탐지·추적기술을 개발하여 부처와 수사기관의 예방과 단속활동을 뒷받침하였다. 이러한

197) 이기수, “최근 보이스피싱의 범죄수법 동향과 법적 대응방안”, 경찰대학 범죄수사연구원, 범죄수사학연구 4(2), 2018, 3-19면

과정에서 금융·통신·정보보호 등 민간의 참여를 이끌어 냈다는 점도 긍정적으로 평가할 수 있을 것이다.

하지만 정부의 종합대책에 아쉬운 점도 있다. 새로운 종합대책을 수립할 때 기존의 종합대책에 대한 평가가 없다. 종합대책 수립의 시급성은 이해가 되지만, 기존 종합대책에 대한 평가가 없으면 개별정책 중에서 어떠한 시책이 효과가 있었는지를 판단할 수가 없다. 그래서 확대 시행해야 할 정책과 폐기해야 할 정책을 결정하기 어렵다. 예산집행의 우선순위를 결정하는 것도 어렵게 된다. 종합대책 수립 당시의 현상적인 문제에만 천착하여 미래 범죄를 예측하여 선제적으로 대응하지 못한 것도 아쉬운 점이다. 앞으로는 미래의 보이스피싱 기술을 충분히 예측하여 거기에 맞는 법제도와 기술을 미리 준비하는 전략을 수립해야 할 것이다. 정부정책의 방향성도 다소 부족해 보인다. 국가와 민간의 책임과 역할을 어떻게 구분할 것인지, 법제 대응과 기술 대응에서 어디에 방점을 둘 것인지, 예방과 검거에 대한 예산투입 비율을 어떻게 결정할 것인지에 대한 고민이 필요하다. 나아가 보이스피싱에 대한 거버넌스 체계도 미흡하다. 부처 간, 부처와 수사기관 간, 부처와 민간 간의 협력체제가 중요하다. 마지막으로 보이스피싱 수사분야에 대한 정책개발이 부족하다. 정부부처는 다양한 정책을 개발하였으나 범죄수사에 대한 정책개발이 다소 부족하다. 수사인력 확충, 국제공조수사 강화 등 일반적인 대책을 넘어서 수사권한 확대를 포함하여 다양한 대책을 발굴해야 할 것이다. 특히, 아시아지역 주요국과의 국제공조수사 역량 강화를 위한 대책발굴이 시급하다.

제5장 신종 보이스피싱 법제 및 쟁점

제1절 신종 보이스피싱 법제 분석

1. 형법

가. 주요 내용

신종 보이스피싱은 형법에서 제347조 사기, 제347조의 2 컴퓨터등 사용사기, 제350조 공갈, 제114조 범죄단체조직 등으로 처벌할 수 있다. 제347조의 사기죄가 적용되기 위해서는 기망행위가 있어야 하고, 피기망자가 착오를 일으켜 재산처분 행위를 해야 하며, 재산상 손해가 발생한 다음에 기망자가 재산상의 이익을 취득해야 한다. 피해자가 스스로 돈을 직접 이체하거나 송금하기 때문에 기망자의 기망행위와 재산처분 행위 사이에 직접성이 인정되어 사기죄로 처벌할 수 있다.¹⁹⁸⁾

형법 제350조에서 명시하고 있는 공갈죄는 재물을 교부받거나 재산상 이익을 취득하기 위해 폭행·협박으로 상대방에게 공포심을 일으키게 하는 일체의 행위¹⁹⁹⁾를 의미한다. 다만, 공갈죄에서의 폭행·협박은 강도죄에서와 같이 피해자의 반항을 억압할 정도의 강한 수준이 아닌, 객관적으로 공포심을 야기하기에 충분하여 피해자의 의사를 제한하는 정도로 충분하다.²⁰⁰⁾ 보이스피싱 범죄에서는 폭행이

198) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서, 2016, 270면

199) 배종대, 「형법각론 제7전정판」, 2011, 74/4

200) 대법원 1961.5.12. 선고 4294형상101 판결; 배종대, 형법각론 제7전정판, 2011, 74/4, 74/9

아닌, 협박을 통해 범죄가 이루어질 수 있으며, 협박은 상대방에게 공포심을 갖게 할 목적으로 해악을 고지하는 일체의 행위를 의미하고, 여기에서 언급하는 해악의 내용에는 제한이 없다.²⁰¹⁾ 대법원은 공갈죄에 해당하는 해악의 고지는 반드시 명시적인 방법이 아니더라도 말이나 행동을 통해서 상대방으로 하여금 어떠한 해악에 이르게 할 것이라는 인식을 하게 하면 족하고, 피공갈자 이외의 제 3자를 통해 간접적으로도 할 수 있으며, 행위자가 그의 직업, 지위 등에 기하여 불법한 위세를 이용하여 재물의 교부나 재산상이 이익을 요구하고 상대방으로 하여금 그 요구에 응하지 않을 때는 부당한 불이익을 당할 위험이 있다는 의구심을 일으키게 하는 경우에도 인정된다고 명시하고 있다.²⁰²⁾ 따라서 기망행위가 아닌, 일정한 해악을 예고하여 피해자로부터 직접 재물의 교부를 받거나 재산상의 이익을 취득하는 방식의 보이스포싱의 경우에는 공갈죄에 해당한다고 할 수 있다.

또한, 신종 보이스포싱 범죄에 적용가능한 형법 조문으로는 제114조의 범죄단체조직죄가 있다. 해당 조문은 사형, 무기 또는 장기 4년 이상의 징역에 해당하는 형법 및 특별형법에 규정되어 있는 범죄를 목적으로 하는 단체 또는 집단을 조직하거나 가입 또는 그 구성원으로 활동한 자를 처벌한다. 원칙적으로 범죄 목적으로 단체를 조직하거나 가입하는 것은 일종의 예비·음모 행위에 지나지 않으나, 점점 증가하고 있는 조직범죄의 높은 위험성을 고려하여 형법에서는 특별규정으로 해당 범죄단체조직죄를 두고 있다.²⁰³⁾ 판례는 범죄단체를 주도하는 최소한의 통솔체제를 갖춘 조직성과 어느 정도의 시간적 계속성을 가지고 있어야 한다고 명시하여 일시적인 범죄 공모 및 분담만으로는 처벌할 수 없다고 해석하고 있다.²⁰⁴⁾

201) 배종대, 「형법각론 제7전정판」, 2011, 74/60-7

202) 대법원 2005.7.15. 선고 2004도1565판결; 2013.4.11. 선고 2010도13774 판결

203) 배종대, 「형법각론 제6전정판」, 2007, 93/2

204) 대법원 1981.11.24. 선고 81도2608 판결; 대법원 1985.10.8. 선고 85도1515 판결

나. 법적 쟁점

보이스피싱 범죄를 사기죄로 적용함에 있어, 피해자인 피기망자가 자신의 계좌에서 범인의 계좌로 금원이 이체되고 있다는 사실을 인식하고 있는 경우에 그 계좌이체를 예금의 점유이전으로 파악하여 ‘재물의 교부’로 보아 사기취재죄에 해당하는 것으로 볼 것인지, 예금채권이라는 이익의 이전으로 파악하여 ‘재산상의 이익의 취득’, 즉 사기이득죄에 해당하는지를 구분할 필요가 있다.²⁰⁵⁾ 공공기관을 사칭하여 피해자를 현금인출기로 유인한 이후, 피해자가 사기범이 불러주는 계좌번호와 이체액수에 대하여 해당 기관의 인증코드 및 보안코드라 속여 직접 입력을 진행하는 경우, 처분행위성을 인정할 수 없어 사기죄를 적용하기 어렵다. 이러한 경우에는 제347조의2인 컴퓨터등 사용사기죄의 적용을 고려해볼 수 있다. 컴퓨터등 사용사기죄는 일반 사기죄와는 달리 피해자를 직접 속이지 않고 허위정보나 권한 없이 정보를 정보처리장치에 입력하여 이익을 취하는 등 정보화 사회의 신종 범죄를 처벌하기 위해 1995년 처음 형법에 도입되었는데 스미싱 사기 등 휴대폰 해킹, 파밍 등 컴퓨터 바이러스를 이용한 사기 등이 해당 범죄에 해당될 수 있다. 이와 관련하여 위와 같은 공공기관 사칭의 경우 사기범은 피해자를 일종의 도구로 이용하여 현금자동인출기에서 예금 이체에 관하여 권한 없이 정보를 입력하게 함으로써 예금채권을 취득한다고 볼 수 있고, 이에 따라 해당 사기범을 컴퓨터등 사용사기죄의 간접정범으로 인정할 여지가 있다. 이는 사기범 즉, 이용자가 피이용자인 피해자의 행위 내지 동작을 자신의 의사에 의해 지배하여 소기의 목적을 실현한다는 점에서 사기범을 컴퓨터등 사용사기죄의 정범으로 인정할 수 있기 때문이다.²⁰⁶⁾

범죄단체조직죄와 관련하여서는 보이스피싱을 위한 범죄단체에 가입하여 이를

205) 윤해성, 김유근, “보이스피싱 피해유형별 구체적 예방방안에 관한 연구”, 대검찰청 보고서, 2017, 32-35면

206) 윤해성, 김유근, “보이스피싱 피해유형별 구체적 예방방안에 관한 연구”, 대검찰청 보고서, 2017, 32-35면

위한 행위에 가담하지만, 실질적으로는 법률의 한계로 인해 처벌하지 못하는 경우가 존재하는데 이러한 처벌 공백을 해소하기 위해 보이스피싱의 범죄단체조직죄 적용이 필요하다. 현재 판례에서는 보이스피싱 범죄단체에 대하여 보이스피싱이라는 사기범죄를 목적으로 구성된 다수인의 계속적인 결합체로서, 최소한의 통솔 체계를 갖춘 형법상의 ‘범죄단체’에 해당하고, 보이스피싱 조직의 업무를 수행한 피고인들에게 범죄단체 가입 및 활동에 대한 고의가 인정된다면, 보이스피싱 조직에 의한 사기범죄 행위가 범죄단체에 해당한다고 보고 있다.²⁰⁷⁾ 범죄단체 가입 행위 또는 활동행위와 사기 행위는 각각 별개의 범죄구성요건을 충족하는 독립된 행위이고 서로 보호범의도 달라, 범조경합 관계로서 목적 범죄인 사기죄만 성립한다고 볼 수 없다고 명시하고 있고, 1개의 행위에 대한 수 죄의 성립을 인정하여 상상적 경합 관계에 있다고 보고 있다. 그러므로 이러한 범죄단체 등의 조직죄는 보이스피싱을 위한 범죄단체에 가입하여 보이스피싱 범죄를 모의하고 준비한 자에 대해서 적용할 수 있을 것으로 보인다.

만일, 보이스피싱과 관련된 다수 행위자들이 형법 제114조의 범죄단체에 해당하지 않을 경우 범죄집단으로 처벌하는 방법도 있다. 판례는 범죄집단을 인정하기 위해서는 범죄단체와 동일하게 범죄의 실행을 공동의 목적으로 한 다수인의 결합체라는 구성요건을 필요로 하나, 그 결합이 계속적일 필요가 없고, 다수가 동시에 동일장소에 집합되어 있으며 그 조직의 형태가 수괴, 간부, 가입자를 구분할 수 있을 정도로만 결합체를 이루고 있으면 된다고 판시하고 있다.²⁰⁸⁾ 범죄집단을 인정하는 경우에는 범죄단체보다 계속성을 요구하지 않고, 더 낮은 수준의 조직성으로도 충분하다는 것이다. 최근 대법원에서 중고차량 판매와 관련하여 범죄단체조직죄보다 입증이 보다 완화된 범죄집단조직죄를 인정한 사례도 있다.²⁰⁹⁾ 다만, 해당

207) 서울고등법원 2017. 5. 19. 선고 2017노209 판결, 대법원 2017. 10. 26. 선고 2017도8600 판결

208) 대법원 1976. 12. 14. 선고 76도3267 판결 참조; 대법원 1987. 3. 24. 선고 87도157 판결; 대법원 1991. 1. 15. 선고 90도2301 판결; 대법원 1991. 5. 28. 선고 91도739 판결; 대법원 1991. 12. 24. 선고 91도2397 판결

판례는 형법 제114조에 대해 실시한 판례가 아니라, 해당 조항과 동일하게 범죄단체와 범죄집단으로 구분하고 있는 폭력행위 등 처벌에 관한 법률(이하 “폭처법”이라 함)의 관련 조항에 대해 실시한 것으로, 이후 형법 제114조의 범죄집단 여부를 판단함에 있어 이와 동일한 판단기준을 적용할지 확인할 수는 없다. 하지만 두 법에서 언급하고 있는 범죄단체와 범죄집단이 동일한 용어로 명시되어 있고, 동일한 맥락을 가지고 있다는 점에서 동일하게 적용할 수 있을 것이다.

2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

가. 주요 내용

정보통신망법에서 신종 보이스피싱에 적용할 수 있는 법조문은 제48조 정보통신망 침해행위 등의 금지, 제49조의 2 속이는 행위에 의한 정보의 수집금지 등 및 이에 따른 벌칙 조항이다. 정보통신망법 제48조에서는 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하는 것을 금지하고 있고, 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 악성프로그램의 전달, 유포를 금지하고 있다. 악성 프로그램은 최근 보이스피싱 범죄를 위해 피해자의 스마트폰에 설치를 유도하고 각종 사기와 협박을 위한 정보를 빼내는데 상당히 사용되고 있기에 범죄 예방 및 수사를 위해 해당 조항의 적용 대상과 범위를 면밀히 검토할 필요가 있다.

정보통신망법 제49조의2인 속이는 행위에 의한 정보의 수집금지 등 조항에서 보이스피싱 범죄와 같이 정보통신망을 사용하여 타인의 정보를 불법적으로 수집하거나, 타인의 정보를 제공하도록 유인해서는 안 된다고 규정하고 있다. 해당 조문에 따라서 보이스피싱 범죄를 위해 타인의 정보를 제공하도록 유인한 자는 제72조 제1항 제2호에 따라 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 되어 있고, 해당 범죄와 관련하여 취득한 금품이나 그 밖의 이익에 대해서는 제75

209) 대법원 2020.8.20. 선고 2019도16263 판결

조의 2에 따라 몰수할 수 있고, 만약 몰수할 수 없을 경우에는 그 가액을 추징할 수 있도록 규정하고 있다.

나. 법적 쟁점

정보통신망법 제49조의2는 보이스피싱에 악용될 수 있는 악성 프로그램에 대한 전달·유포죄만 규정하고 있을 뿐 제조·소지죄에 대한 처벌규정은 두고 있지 않다. 이 때문에 조직적으로 움직이는 보이스피싱 기획자들을 처벌하기가 힘든 측면이 있고, 범죄수단을 지속적으로 제작하고 소지하고 있는 자에 대해 죄를 묻기 힘들다는 문제가 있다. 그러나 악성 프로그램의 제작 행위를 형사처벌하는 것은 정보통신망의 안정성을 침해하는 행위에 훨씬 앞서 있는 단지 잠재적인 위험을 처벌하는 것으로서 법익침해의 전단계의 범죄화한 것이라는 비판도 존재한다.²¹⁰⁾ 하지만, 악성 프로그램의 제조·소지죄에 대한 처벌 규정은 유럽평의회 사이버범죄방지협약에 포함되어 있기 때문에 “범죄를 목적으로” 혹은 “영리 또는 부정한 목적으로” 등의 구성요건을 추가하여 입법화하는 것을 검토할 수 있을 것이다.²¹¹⁾ 꼭 보이스피싱을 위해서가 아니라 일반적인 정보통신망침해범죄를 단속하기 위해서 필요한 규정이기도 하다. 나아가 전기통신금융사기는 통신사기피해환급법에 따라 금융위원회가 예방대응조치 의무를 가지고, 침해사고는 정보통신망법에 따라 과학기술정보통신부에게 예방대응조치를 부여하고 있어 대응 주체가 이원화되어 있는 문제도 있다.

210) 김일수, 배종대, 이상돈, “정보화사회에 대비한 형사법적 대응”, 한국비교형사법학회, 비교형사법연구 3(2), 2001, 46-47면

211) 김대근, “기술적 수단을 사용한 사이버 금융사기범죄의 실태와 형사정책적 대응방안”, 한국형사정책연구원, KIC ISSUE PAPER 14, 2016, 16-17면

3. 전기통신사업법

가. 주요 내용

전기통신사업법에서 신종 보이스피싱 범죄를 저지른 자에게 적용할 수 있는 법 조문은 제32조의4 이동통신단말장치 부정이용 방지 등과 제84조의2 전화번호의 거짓표시 금지 및 이용자 보호 및 이에 따른 벌칙 조항이다. 이 외에 신종 보이스 피싱 범죄 예방을 위해 제32조의3 전기통신역무제공의 제한 및 제32조의 5 부정 가입방지시스템 구축과 제84조의2 전화번호의 거짓표시 금지 및 이용자 보호 내 제3항 이하의 조문을 두고 있다. 전기통신사업법에서는 발신자의 전화번호의 변조 및 조작과 관련하여 고의로 공공기관 혹은 타인의 번호로 오인하도록 번호를 조작하는 경우, 전화번호의 변조를 실행한 자에 대하여 전기통신사업법 제84조의 2 제1항에 따라 동법 제95조의 2 제4호에 의해 3년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 되어 있다.

나. 법적 쟁점 및 검토

발신자의 전화번호의 변조 및 조작에 해당하는 전화번호는 이미 전기통신사업자와의 계약을 통해 존재하고 있는 전화번호뿐만 아니라 아예 존재하지 않아 수신자가 해당 발신 번호로 다시 전화를 하였을 때 없는 번호라고 나오는 전화번호까지 포함된다. 실제 전화개통이 되지 않은 070 전화번호를 오토콜 시스템에 입력하여 발신번호로 변작 표시하여 전화발신 역무를 제공한 경우 전기통신사업법 위반으로 처벌하기도 하였다.²¹²⁾ 존재하지 않는 번호로 발신자의 전화번호를 변작한 자는 제84조의 2 제1항의 적용을 받아 동법 제95조의 2 제4호에 의해 3년 이하의 징역 또는 1억원 이하의 벌금형에 처하게 된다. 변작을 가능하게 하는 영리 서비스를 제공한 자도 전기통신사업법 제84조의 2 제2항에 따라 동법 제95조의2 제5호에 의해 3년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 되어 있다. 자금을

212) 인천지방법원 2019. 11. 28. 선고 2019고단5751 판결

제공 또는 유통해주는 조건으로 타인의 명의로 이동통신단말장치를 개통하여 이용하거나 해당 자금의 회수에 이용하는 행위를 금지하고(제32조의4) 이를 동법 제95조의2 제2호에 의해 3년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

보이스피싱 범죄와 관련하여 전기통신사업자는 전화번호 변작을 통한 보이스피싱 등으로 인한 피해를 막기 위해 제84조의 2 제3항에 따른 조치를 하여야 하고, 과학기술정보통신부장관은 전기통신사업자가 해당 조항에 따른 조치의 이행 여부를 확인하기 위해 이에 필요한 자료의 열람·제출 요청 및 검사를 할 수 있다. 또한 보이스피싱을 방지하기 위해서 전기통신사업법에서는 과학기술정보통신부장관에게 이전에 보이스피싱에 사용되었던 전화번호에 대한 전기통신역무 제공을 중지하는 명령을 내릴 수 있는 권한을 부여하고 있고(제32조의3), 과학기술정보통신부장관은 부정한 방법을 통한 전기통신역무 제공계약 체결 방지를 위해 가입자 본인 확인에 필요한 시스템인 부정가입방지시스템을 구축하고 이동통신단말장치와 관련한 전기통신역무 제공에 관한 계약을 체결을 하는 전기통신사업자가 해당 시스템을 이용할 수 있도록 해야 한다(제32조의5).

또 하나의 이슈는 전화번호를 속이기 위해 사망자의 전화번호를 도용하는 경우다. 이는 전기통신사업법 제84조의 2 제1항에서 언급하는 송신인의 전화번호를 변작하는 경우에 해당한다고 볼 수 있다. 하지만 동법 제32조의 4 제2항에 따라 전기통신역무 제공에 관한 계약, 즉 전화번호의 개설에 대한 계약을 체결하는 경우에는 동법 제32조의 5 제1항에 따른 부정가입방지시스템을 통해 본인 여부를 확인할 수 있기에 사망자 여부를 확인할 수 있다. 그에 반해 이미 전화번호가 개설되어 있는 자가 사망한 경우에는 현행법상 이를 확인할 수 있는 근거가 없다. 전기통신사업자나 관련 국가기관이 임의적으로 사망자의 명의를 전달받거나 확인받는 것은 개인정보보호법상 문제가 될 수 있다. 이러한 이유로 사망자 명의 도용을 통한 보이스피싱에 대한 수사는 제대로 이루어지지 않았는데, 이러한 문제와 관련하여 사망자는 민법 제3조에 따라 더 이상 권리와 의무의 주체가 되지 않아 개인정보보호법상 권리의 주체가 되지 않으므로 사망자의 명의를 전달받거나 확

인받는 것은 법적 문제가 없는 것으로 보인다. 따라서 사망자 명의를 확인시켜 줄 수 있는 행정안전부로부터 주민등록법 제35조 제2호 및 주민등록법 시행령 제58조 제3항에 따라 전기통신사업자 혹은 관련 국가기관이 사망자 명의를 확인받을 수 있도록 하여 전기통신사업법 제84조의 2 제1항에 해당하는 사망자 명의를 사용한 보이스피싱에 대한 수사를 강화해야 할 것이다.

4. 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법

가. 주요 내용

통신사기피해환급법은 보이스피싱 즉, 전기통신금융사기에 대하여 사후 피해금 환급에 중점을 두고 있는 법으로 2011년에 제정되었다. 통신사기피해환급법에서 신종 보이스피싱을 저지른 자에게 적용할 수 있는 법조문은 제15조의2 벌칙 조항이고, 신종 보이스피싱과 관련하여 발생한 피해금에 대한 환급을 위해 적용할 수 있는 법조문은 제3조 피해구제의 신청부터 제13조 소멸채권 환급 청구까지이다. 또한 해당 보이스피싱으로 또 다른 피해자가 나오지 않도록 하기 위한 사후조치로 제13조의2인 사기이용계좌의 명의인에 대한 전자금융거래 제한 및 제13조의 3인 전기통신금융사기에 이용된 전화번호의 이용중지 등이 있다.

우선, 전기통신금융사기란 전기통신기본법의 전기통신(제2조 제1호)을 이용하여 타인을 기망·공갈함으로써 자금을 송금·이체하도록 하거나 개인정보를 알아내어 자금을 송금·이체하여 기망·공갈자나 제3자가 ‘재산상 이익’을 취하는 행위를 말하는데, 여기에 대출의 제공·알선·중개를 가장한 행위는 포함되지만, 재화의 공급이나 용역의 제공 등을 가장한 행위는 제외된다.

보이스피싱 범죄를 저지르기 위해서 타인으로 하여금 컴퓨터 등 정보처리장치에 정보 또는 명령을 입력하게 하거나 취득한 타인의 정보를 이용하여 컴퓨터 등 정보처리장치에 정보 또는 명령을 입력하는 행위를 한 자에 대해서는 제15조의2 벌칙 조항을 통해 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. 해당 행위의 미수범도 처벌하도록 하고 있고, 상습범에 대해서는 가중처벌 조항도 두고

있다. 해당 법은 피해자에 대해서도 제3조부터 제11조까지의 조항을 통해 피해금을 송금 및 이체한 계좌를 관리하는 금융회사 또는 사기이용계좌를 관리하는 금융회사에게 피해구제 및 지급정지를 신청하여 피해환급금을 지급받을 수 있게 한다. 피해구제 신청 및 지급정지와 관련된 절차와 관련 채권에 대한 처리에 관하여는 제3조부터 제9조까지에 명시하고 있고, 피해환급금과 관련하여 결정 및 지급에 대해서는 제10조에, 피해환급금을 지급받을 수 없는 자에 대하여는 제11조에 명시하고 있다. 또한 해당 법률로 인해 발생하는 채권의 변동사항에 대해서는 제12조(손해배상청구권과의 관계)와 제13조(소멸채권 환급 청구)에서 명시하고 있다.

해당 법률은 보이스피싱 가해자·피해자에 대한 직접적인 사후조치뿐만 아니라 피해자가 발생하지 않도록 금융감독원 및 금융회사에 대하여 사기이용계좌의 명의인에 대한 전자금융거래를 제한할 수 있게 하는 규정(제13조의2)과 수사를 담당하는 기관(검찰 및 경찰)과 금융감독원이 보이스피싱에 이용된 전화번호를 사용하지 못하도록 하는 중지 요청을 과학기술정보통신부장관에게 할 수 있도록 하는 규정(제13조의3)을 포함하고 있다. 특히, 보이스피싱에 이용된 전화번호의 이용중지와 관련하여 해당 법률을 통해 요청받은 과학기술정보통신부장관은 전기통신사업법 제32조의3에 따라 이를 전기통신사업자에게 명할 수 있도록 되어 있다.

나. 법적 쟁점 및 검토

정부는 2020년 디지털 경제의 신뢰 기반 조성을 위한 보이스피싱 척결 종합방안”에서 통신사기피해환급법의 개정 계획을 발표하였다. 우선 보이스피싱 관련 범죄 및 유사금융사기 범죄에 대한 처벌 형량을 대폭 강화하고, 관련 범죄행위를 일관되게 규율할 수 있도록 법을 개정하겠다고 발표하였다. 이러한 방향은 통신사기 피해환급법 제15조의 2 벌칙 조항의 법정형을 현재보다 높이는 형태로 이루어질 가능성이 높다.

또한 법정형의 형량을 높이는 대처 방안 이외에 보이스피싱 피해자들의 피해 구제 제도를 정비하는 방안도 제시하고 있다. 세부적으로는 현재의 통신사기피해환

금법 제4조 지급정지 제도를 정비하여 금융회사가 보이스피싱 의심계좌에 대해 자체적으로 지급정지를 한 경우에 대해 본인의 자금이체가 확인이 되어도 일정한 요건에 해당되는 경우에는 지급정지를 해제하지 않는 것이나, 이러한 지급정지 의무를 전자금융업자에게도 부여하는 것이다. 현재의 지급정지 미이행 시에만 인정하고 있는 금융회사의 배상책임의 범위를 넓혀 이용자의 고의 및 중과실이 없는 금융회사등이 원칙적으로 배상책임을 지도록 하려는 것이다. 또한 통신사기피해 환급법에 보이스피싱 의심 금융거래를 모니터링하기 위해서 금융회사 이상금융거래 탐지시스템(FDS)을 의무적으로 구축하도록 하고, 빅데이터·AI 등 신기술을 활용하여 개선하도록 하고 있다.

추가 쟁점으로 통신사기피해환급법상 전기통신금융사기의 요건에는 취득객체에 재산상 이득만 포함하고 있어, 재물을 취득한 경우를 처벌하지 못하고 있다. 통신사기피해환급법은 전기통신금융사기를 목적으로 타인으로 하여금 컴퓨터등정보처리장치에 정보·명령을 입력하게 하거나 취득한 타인의 정보를 이용하여 컴퓨터등정보처리장치에 정보·명령을 입력하는 경우 10년 이하 징역이나 1억원 이하 벌금으로 처벌한다.(제15조의2) 전기통신금융사기란 전기통신기본법의 전기통신(제2조 제1호)을 이용하여 타인을 기망·공갈함으로써 자금을 송금·이체하도록 하거나 개인정보를 알아내어 자금을 송금·이체하여 기망·공갈자나 제3자가 ‘재산상 이익’을 취하는 행위를 말한다. 하지만 최근에는 직접 만나서 금원을 편취하는 즉, “재물”을 편취하는 사례가 많아지면서 처벌의 공백이 발생하고 있다. 이에 통신사기피해환급법 제2조 제2호의 전기통신금융사기의 취득객체에 재산상 이익 외에 “재물”을 추가하여 처벌의 공백을 메울 필요가 있다.²¹³⁾

213) 윤동호, “통신사기피해환급법의 정보·명령입력죄의 구성요건적 의미와 한계”, 한국형사정책학회, 형사정책 32(1), 2020, 223-243면

5. 통신비밀보호법

가. 주요 내용

통신비밀보호법에서 신종 보이스피싱 범죄에 적용할 수 있는 법조문은 제13조 범죄수사를 위한 통신사실확인자료제공의 절차이다. 통신비밀보호법 제13조 제1항은 검사 또는 사법 경찰관에게 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자에게 통신사실확인자료의 열람이나 제출을 요청할 수 있다고 명시하고 있다. 나아가 통신비밀보호법에서는 통신제한조치 제도에 대해서도 규정하고 있는데 통신사기피해환급법은 통신제한조치 대상 범죄에 해당하지 않아서 수사현장에서 활용되지 못하고 있다.

나. 법적 쟁점

보이스피싱을 수사하는데 강력한 수사권한이 필요하지만 감청대상 범죄에 보이스피싱은 포함되어 있지 않다. 수사현장에서는 범죄단체조직죄, 범죄수익은닉죄 등을 의율하여 통신제한조치허가서를 발부받아 집행하는 경우가 종종 있지만 범죄단체의 증명 자체가 쉽지 않고, 범죄수익은닉 규명도 어려워 활용성은 낮다. 나아가 통신비밀보호법 제5조 제1항에 수사 목적으로 감청을 사용할 수 있는 범죄에 대해서 명시되어 있는데 여기에는 형법 제39장 사기와 공갈의 죄 중 제350조, 제350조의 2, 제351조(제350조, 제350조의 2의 상습범에 한정한다)가 포함되어 있다. 공갈죄, 특수 공갈죄, 공갈죄의 상습범은 수사 목적으로 감청할 수 있다. 하지만 이러한 죄명들은 보이스피싱을 처벌하는 주된 법률이라고 보기 어려워 현장에서는 적용하는데 주저할 수밖에 없다.

6. 범죄수익은닉의 규제 및 처벌 등에 관한 법률

가. 주요 내용

범죄수익은닉규제법은 범죄수익을 은닉하는 행위를 규제하고, 특정범죄와 관련된 범죄수익의 몰수 및 추징에 관한 특례를 규정함으로써 특정범죄를 조장하는 경제적 요인을 제거하여 사회질서를 유지하는데 목적이 있다. 범죄수익은닉규제법 제2조 제2호에 따르면 해당 법률이 적용되는 범죄수익은 중대범죄에 해당하는 범죄행위에 의하여 생긴 재산 또는 그 범죄행위의 보수(報酬)로 얻은 재산 또는 성매매알선처벌법, 폭력행위 등 처벌에 관한 법률 등 해당 법률 제2호 나목에 열거된 죄와 관련된 자금이나 재산을 의미한다. 여기서 가목에서 언급하는 중대범죄로 명시되어 있는 별표에 규정된 죄목에는 형법 제347조 사기죄와 제347조의2 컴퓨터 등 사용사기죄, 제350조 공갈죄 및 그 미수가 포함된다. 보이스피싱은 앞에서 살펴보았듯이 사기죄, 컴퓨터등 사용사기죄 및 공갈죄가 적용되고, 그러므로 해당 범죄로부터 얻은 수익은 범죄수익은닉규제법의 적용 대상이 된다. 이러한 이유로 해당 법률에서 신종 보이스피싱 범죄에 적용할 수 있는 법조문은 제3조 범죄수익 등의 은닉 및 가장, 제4조 범죄수익등의 수수와 해당 범죄수익에 대한 몰수 및 추징 조항이다.

범죄수익은닉규제법 제3조 제1항에 의하면 범죄수익등의 취득 또는 처분에 관한 사실 또는 범죄수익의 발생 원인에 관한 사실을 가장하거나 특정범죄를 조장하거나 적법하게 취득한 재산으로 가장할 목적으로 범죄수익등을 은닉한 자는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처하며, 미수범 및 예비·음모한 자도 동 조 제2항 및 제3항에 따라 처벌하도록 규정되어 있다. 또한 동 법 제4조에 의하면 그 정황을 알면서 범죄수익등을 수수한 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처하도록 명시되어 있다. 다만 제8조 제3항에서 제1항 각호의 재산이 범죄피해재산인 경우에는 몰수할 수 없도록 명시하고 있다. 또한 제10조 제2항에서도 범죄피해재산에 대해서는 추징할 수 없도록 명시하고 있다. 범죄피해재산은 사기죄를 포함하는 재산에 관한 죄에 해당하는 범죄에 의해 피해자로부터 취득한

재산 또는 그 재산의 보유·처분에 의하여 얻은 재산을 의미하므로 사기죄 및 컴퓨터등 사용사기죄로 규율되는 보이스피싱 범죄를 통해 얻은 범죄수익은 몰수 및 추징될 수 없다. 다만, 판례에서는 보이스피싱 범죄에 의해 얻은 범죄수익에 대하여 사기죄가 아닌 형법 제114조 범죄단체조직죄에 따라 몰수 및 추징할 수 있도록 하고 있다.²¹⁴⁾

나. 법적 쟁점

범죄수익은닉규제법에 의해 몰수할 수 있는 범죄수익에는 암호화폐 혹은 가상화폐도 포함된다. 범죄수익은닉규제법은 범죄수익을 몰수, 추징하기 위하여 몰수의 대상을 ‘물건’으로 한정한 형법보다 넓게 ‘재산’으로 규정하면서 재산의 범위를 현금, 예금, 주식, 그 밖에 재산적 가치가 있는 유형, 무형의 재산(동법 시행령 제2조 제2항)으로 정의하여 반사회적 범죄를 사전에 예방하고 범죄를 조장하는 경제적 요인을 효과적으로 제거할 수 있도록 하고 있다.²¹⁵⁾ 대법원은 암호화폐의 일종인 비트코인에 대한 몰수와 관련하여 비트코인은 재산적 가치가 있는 무형의 재산이라고 보아야 하고, 몰수의 대상인 비트코인이 특정되어 있기 때문에 범죄수익은닉규제법에 의해 몰수할 수 있다고 판시하였다.²¹⁶⁾

또한, 범죄수익은닉규제법에 의해 몰수 혹은 추징될 수 있는 보이스피싱에 의한 범죄수익은 동법 제12조에 의해 기소 전에도 몰수보전 및 추정보전이 가능하다. 범죄수익은닉규제법 제12조는 동법에 따른 몰수 및 추징과 국제 공조에 관해서는 「마약류 불법거래 방지에 관한 특례법」 제19조부터 제63조까지, 제64조제2항 및 제65조부터 제78조까지의 규정을 준용하도록 되어있다. 마약류 불법거래 방지

214) 서울고등법원 2017. 5. 19. 선고 2017노209 판결, 대법원 2017. 10. 26. 선고 2017도8600 판결

215) 김현서, 송문호, “가상화폐의 몰수 - 대법원 2018. 5. 30. 선고 2018도3619 판결 -”, 전북대학교 동북아법연구소, 동북아법연구 12(2), 2018, 408면

216) 대법원 2018. 5. 30. 선고 2018도3619 판결

에 관한 특례법 제34조와 제53조를 살펴보면 제34조에는 기소 전 몰수보전명령을, 제53조에는 기소 전 추정보전명령을 할 수 있도록 규정되어 있다. 이러한 기소 전 몰수보전명령과 기소 전 추정보전명령은 해당 재산이 법령에 따라 몰수할 수 있는 재산에 해당한다고 판단할만한 상당한 이유가 있고, 필요하다고 인정되는 등의 경우에는 검사가 지방법원판사에게 청구하여 몰수보전명령처분 혹은 추정보전명령처분을 받아 실행할 수 있다. 사범경찰관도 동 조항에 따라 검사에게 신청하여 검사의 청구로 해당 처분을 받을 수 있다.

따라서 수사현장에서는 보이스피싱 용의자들이 자금세탁하는 암호화폐를 적극적으로 몰수하여야 할 것이다. 기소전 몰수 보전 또는 기소전 추정 보전 제도도 적극 활용할 필요가 있다.

7. 특정 금융거래정보의 보고 및 이용 등에 관한 법률

가. 주요 내용

특정금융정보법은 각종 자금세탁과 관련된 행위를 파악하고 수사기관에 정보를 제공할 수 있도록 하는 법률이다. 해당 법률의 대상이 되는 제2조 제3호에서 언급하고 있는 불법재산은 범죄수익은닉규제법에서 명시하고 있는 범죄수익을 포함하고 있어 보이스피싱을 얻은 범죄수익도 해당한다. 신종 보이스피싱에 적용할 수 있는 법조문은 제4조 불법재산 등으로 의심되는 거래의 보고 등, 제5조의2 금융회사등의 고객 확인의무, 제7조 수사기관 등에 대한 정보 제공이며, 이에 대한 벌칙 및 과태료 조항을 두고 있다. 특정금융정보법 제4조 및 제5조의2는 금융회사에게 자금세탁행위와 관련된 거래행위를 파악할 수 있도록 하고 있다. 제4조 제1항은 불법재산 등으로 의심되는 거래에 대해 불법재산이라고 의심되는 합당한 근거가 있는 경우이거나 자금세탁행위나 공중협박자금조달행위를 하고 있다고 의심되는 합당한 근거가 있는 경우에 한해 대통령령으로 정하는 바에 따라 금융정보분석원장에게 보고해야 한다. 동 법 제5조의2는 금융거래를 이용한 자금세탁행위 및 공중협박자금조달행위를 방지하기 위한 합당한 주의의무를 이행하기 위해 계좌 신

설이나 각종 거래에 있어 고객이 실제 소유자인지 여부가 의심되는 등 고객이 자금세탁행위나 공중협박자금조달행위를 할 우려가 있는 경우에 고객을 확인할 의무를 부여하고 있다. 금융회사의 의무와 관련하여 제14조 벌칙 조항에서는 제4조의 보고를 거짓으로 한 자와 보고한 내용을 누설한 자에 대해 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하고 있고, 제17조 과태료 조항에서는 제5조의2에 의한 확인의무를 해태한 자에 대해 최대 1억원 이하의 과태료를 부과하고 있다. 따라서 금융회사가 보이스포싱 범죄를 통해 얻은 범죄수익과 관련된 거래행위를 파악하고도 각 조항에 따른 보고의무와 확인의무를 이행하지 않은 경우에는 형사처벌될 수 있다.

또한, 금융정보분석원장은 동 법 제7조 제1항 및 제2항에 따라 불법재산·자금세탁행위 또는 공중협박자금조달행위와 관련하여 수사에 필요하다고 인정되는 경우에는 동 조 각 호에 명시되어 있는 특정금융거래정보를 수사기관에 제공해야 한다. 수사기관이 특정형사사건의 수사등을 위하여 필요하다고 인정하는 경우에는 대통령령으로 정하는 바에 따라 금융정보분석원장에게 특정금융거래정보를 요구할 수 있다.

나. 법적 쟁점

2020년 3월 24일 개정되고 2021년 3월 25일부터 시행될 개정 특정금융정보법에는 제6조부터 제8조까지 가상자산사업자에 대해 규제를 신설하였다. 가상자산사업자는 개정법률 제2조 제1호 하목에서 가상자산과 관련하여 1) 가상자산을 매도, 매수하는 행위, 2) 가상자산을 다른 가상자산과 교환하는 행위, 3) 가상자산을 이전하는 행위 중 대통령령으로 정하는 행위, 4) 가상자산을 보관 또는 관리하는 행위, 5) 1) 및 2)의 행위를 중개, 알선하거나 대행하는 행위, 6) 그 밖에 가상자산과 관련하여 자금세탁행위와 공중협박자금조달행위에 이용될 가능성이 높은 것으로서 대통령령으로 정하는 행위를 영업으로 하는 자로 정의하고 있다. 가상자산에 대해서는 개정법률 제2조 제3호에서 경제적 가치를 지닌 것으로서 전자적으

로 거래 또는 이전될 수 있는 전자적 증표(그에 관한 일체의 권리를 포함한다)라고 명시하고 있다. 따라서 해당 법의 개정으로 인해 흔히 암호화폐 혹은 가상화폐라고 명칭하는 재산은 해당 개정 법률의 가상자산에 해당하고, 이와 관련하여 영업을 하는 자는 특정금융정보법의 규율을 받게 되었다.

개정 특정금융정보법은 제7조에서 영업을 위한 신고를 하도록 되어 있고, 제8조에서는 제4조제1항 및 제4조의2에 따른 보고의무 이행을 위하여 고객별 거래내역을 분리하여 관리하는 등 대통령령으로 정하는 조치를 하여야 한다. 기존의 금융회사등이 가지고 있던 제4조 제1항 및 제4조의 2에 따른 보고의무도 당연히 지는 것으로 명시하고 있다. 따라서 암호화폐 등의 가상자산으로 영업하는 가상자산사업자는 법재산 등으로 의심되는 거래에 대해 불법재산이라고 의심되는 합당한 근거가 있는 경우이거나 자금세탁행위나 공중협박자금조달행위를 하고 있다고 의심되는 합당한 근거가 있는 경우에는 지체 없이 금융정보분석원장에게 보고하여야 한다.

8. 전자금융거래법

가. 주요 내용

전자금융거래법에서 신종 보이스피싱에 적용할 수 있는 조항은 제6조 접근매체의 선정과 사용 및 관리와 이에 따른 벌칙 조항이다. 전자금융거래법 제6조의3에 의하면 누구든지 범죄에 이용할 목적으로 또는 범죄에 이용될 것을 알면서 계좌와 관련된 정보를 제공받거나 제공하는 행위 또는 보관·전달·유통하는 행위를 해서는 안된다고 명시하고 있다. 대포통장 모집 및 거래와 관련하여 대포통장 계좌의 양도인과 양수인, 그리고 이와 관련된 자 모두를 포괄하고 있다. 대포통장 계좌의 양도인과 양수인을 포함한 대포통장 모집 및 거래와 관련된 모든 자들은 제6조의3에 따라 금지된 행위를 한 것으로 볼 수 있고, 벌칙 조항인 제49조 제4항 제5호에 따라 5년 이하의 징역 또는 3천만원 이하의 벌금에 처해지게 된다.

전자금융거래법 제6조 제3항 제1호에 따르면 누구든지 접근매체를 사용 및 관

리함에 있어서 다른 법률에 특별한 규정이 없는 한 접근매체를 양도하거나 양수하는 행위를 해서는 안된다. 동조 제3항 제2호 및 제3호에 의하면 대가를 수수(授受)·요구 또는 약속하면서 접근매체를 대여 받거나 대여하는 행위 또는 보관·전달·유통하는 행위 및 범죄에 이용할 목적으로 또는 범죄에 이용될 것을 알면서 접근매체를 대여 받거나 대여하는 행위 또는 보관·전달·유통하는 행위도 금지하고 있다. 여기에서 접근매체란 전자금융거래법 제2조 제10호에 따라 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 전자식 카드 및 이에 준하는 전자적 정보, 전자서명법 제2조제4호의 전자서명생성정보 및 같은 조 제7호의 인증서, 금융회사 또는 전자금융업자에 등록된 이용자번호, 이용자의 생체정보, 전자식 카드 및 이에 준하는 전자적 정보 또는 전자서명법 제2조제4호의 전자서명생성정보 및 같은 조 제7호의 인증서의 수단이나 정보를 사용하는데 필요한 비밀번호 중 어느 하나에 해당하는 수단 또는 정보를 의미한다. 보이스피싱 범죄에서 대포통장 모집 및 거래와 관련하여 양수인 및 명의차용은 대포통장과 함께 현금카드, 비밀번호, 양도인 및 명의대여인의 주민등록번호까지 양도받으므로, 전자금융거래법상의 접근매체를 양도 및 대여하게 된다.²¹⁷⁾ 따라서 양도인 및 명의대여자는 제6조 제3항 제1항, 제2항 또는 제3항에 따라 금지된 행위를 한 것이고, 벌칙 조항인 제49조 제4항 제1호 또는 제2호에 따라 5년 이하의 징역 또는 3천만원 이하의 벌금에 처해지게 된다.

나. 법적 쟁점

2020년 6월 16일 발의된 박용진위원의 전자금융거래법 일부개정법률안을 살펴보면 가상통화를 취급하고자 하는 사업자는 인가를 받도록 하고 있다. 제46조의 8에 의하면 누구든지 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제2조 제3호에 따른 불법재산의 은닉, 같은 조 제4호에 따른 자금세탁행위 또는 같은 조

217) 윤해성, 김유근, “보이스피싱 피해유형별 구체적 예방방안에 관한 연구”, 대검찰청 보고서, 2017, 37면

제5호에 따른 공중협박자금조달행위 및 강제집행의 면탈, 그 밖에 탈법행위를 목적으로 가상통화의 매매·중개·교환·발행·관리를 하여서는 아니 된다. 이러한 의무를 위반한 자에 대해서는 제49조 제4항 제4호에 따라 5년 이하의 징역 또는 3천만원 이하의 벌금에 처할 수 있도록 하고 있다. 즉, 보이스피싱을 통해 얻은 수익을 암호화폐 혹은 가상화폐를 통해 자금세탁할 수 없도록 규정하고 있다. 해당 법률안이 통과되면 가상화폐를 통한 자금세탁행위를 보다 강력하게 처벌할 수 있을 것이다.

또한, 관계부처 TF는 올해 6월 보이스피싱 척결 종합방안에서 대포통장을 양도·양수, 대여하는 행위에 대한 처벌을 징역 5년, 벌금 3천만원으로 상향하여 범죄단체조직죄로 처벌하고자 하였다. 이는 2020년 5월 19일 곧바로 개정되어 현실화되었고, 이제는 범죄단체조직죄로 처벌할 수 있게 되었다.

9. 기타 법률

가. 금융실명거래 및 비밀보장에 관한 법률

금융실명법은 타인 명의의 대포통장을 범죄에 사용하는 보이스피싱을 규율할 수 있는 법률이다. 해당 법률에서 신종 보이스피싱에 적용할 수 있는 법조문은 제3조 금융실명거래가 있고, 이에 대한 벌칙 및 과태료 조항이 있다. 금융실명법 제3조 제3항에서는 누구든지 특정금융정보법 제2조 제3호에 따른 불법재산의 은닉, 같은 조 제4호에 따른 자금세탁행위 또는 같은 조 제5호에 따른 공중협박자금조달행위 및 강제집행의 면탈, 그 밖에 탈법행위를 목적으로 타인의 실명으로 금융거래를 하면 안된다고 명시하고 있고, 동 조 제4항에서는 금융회사에 종사하는 자에게 이러한 금융거래의 알선이나 중개를 금지하고 있다. 동 법 제6조 벌칙 조항에서는 타인의 명의로 금융거래를 하거나 이를 알선하거나 중개한 금융회사에 종사한 자에게 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 하고 있고, 동 법 제7조 과태료 조항에서는 이를 위반한 금융회사등의 임원 또는 직원에게 3

천만원 이하의 과태료를 부과하도록 규정하고 있다. 제10조에서는 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제6조 또는 제7조에 따라 처벌 혹은 과태료 처분을 받는 경우, 해당 행위자 뿐만 아니라 이러한 위반행위 방지를 위한 주의와 감독을 게을리 한 법인 혹은 개인에 대해서 제6조 또는 제7조에 따른 처벌 혹은 과태료를 부과하도록 하고 있다. 따라서 보이스포싱을 통한 범죄수익을 타인의 대포통장을 통해 거래한 자 혹은 이러한 거래를 알선하거나 중개한 금융회사에 종사하는 자를 처벌할 수 있다.

나. 특정경제범죄 가중처벌 등에 관한 법률

특정경제범죄법은 특정재산범죄에 대하여 가중처벌하는 법률로 보이스포싱을 보다 높은 형량으로 처벌할 수 있게 하고 있다. 해당 법률에서 보이스포싱에 적용할 수 있는 법조문은 제3조(특정재산범죄의 가중처벌) 조항이다. 제3조의 경우 기존에는 형법 제347조(사기), 제350조(공갈), 제350조의2(특수공갈) 등의 죄를 범한 사람이 그 범죄행위로 인하여 취득하거나 제3자로 하여금 취득하게 한 이득액이 5억원 이상일 때에는 법정 이득액 구간에 따라 가중 처벌하도록 하고 있었다. 그러나 컴퓨터등 정보처리장치에 허위의 정보 등의 입력으로 재산상의 이익을 취득하는 컴퓨터등 사용사기죄의 경우에는 그 가중처벌 대상에서 제외되어 있어 신종 보이스포싱에 대한 가중처벌이 불가능하였다. 이에 특정재산범죄의 가중처벌 대상에 형법 제347조의2의 컴퓨터등 사용사기죄를 포함시켜야 한다는 지적이 나왔고, 2018년에 이를 반영하여 법률을 개정하였다.

다. 부패재산의 몰수 및 회복에 관한 특별법

부패재산몰수법은 국제연합부패방지협약 및 그 밖의 관련 국제협약을 효율적으로 이행하기 위하여 부패재산의 몰수 및 추징, 환수 등에 관한 특례를 규정함으로써 부패범죄를 조장하는 경제적 요인을 근원적으로 제거하여 부패범죄를 효과적으로 방지·척결하고 청렴하기 위한 법률이다. 2008년 제정된 동법은 부패재산의 몰수 및 추징, 몰수 및 추징 보전절차, 몰수재판 및 추징재판의 집행과 보전에 관한 국제공조절차, 부패재산의 회복에 관한 특례 및 절차 등을 규정하고 있다. 부패재산몰수법은 불법 또는 부당한 방법으로 물질적·사회적 이득을 얻거나 다른 사람으로 하여금 얻도록 도울 목적으로 범한 죄인 “부패범죄”의 범죄행위에 의하여 생긴 재산 또는 그 범죄행위의 보수로서 얻은 재산인 “부패재산”(제2조)을 몰수하는 것(제3조)을 주된 내용으로 한다. 다만 제6조(범죄피해재산의 특례)를 통해 범죄피해자가 범죄피해재산에 관하여 범인에 대한 재산반환청구권 또는 손해배상청구권 등을 행사할 수 없는 등 피해회복이 심히 곤란하다고 인정되는 경우 몰수·추징할 수 있도록 하고 있다. 여기서 “범죄피해재산”은 원래 제2조제1호의 부패범죄 중 형법 제2편제40장 횡령과 배임의 죄 중 제355조, 제356조 및 제359조의 죄와 특정경제범죄가중처벌 등에 관한 법률 제3조 중 형법 제355조 및 제356조에 해당하는 죄의 범죄행위에 의하여 그 피해자로부터 취득한 재산 또는 그 재산의 보유·처분에 의하여 얻은 재산을 의미한다. 그런데 사기죄에 속하는 보이스피싱은 범죄피해재산으로 포함되지 않아 국가가 범인으로부터 재산을 몰수·추징할 수 없다는 문제가 있었다.

이러한 문제를 해결하기 위하여 2019년 보이스피싱, 다단계, 유사수신행위 등 사기범죄로 인한 범죄피해재산을 국가가 범인으로부터 몰수추징하여 피해자에게 돌려줄 수 있도록 하는 부패재산몰수법 일부개정법률안이 국회 본회의를 통과하였다. 따라서 사기죄 중 범죄단체를 조직하여 범행한 경우, 유사수신행위 또는 다단계판매의 방법으로 기망하여 범행한 경우, 전기통신금융사기 등의 경우를 부패

범죄로 규정하고, 해당 범죄로 인한 피해재산을 범죄피해재산의 범위에 포함시킴으로써, 유사수신행위·다단계판매사기, 전기통신금융사기 등 사건의 수사 중에 범죄피해재산을 발견하면 몰수·추징한 후 피해자에게 돌려줄 수 있게 하였다.

더불어 보이스피싱 범죄로 인한 피해재산이 범죄피해재산으로 인정되면서, 보이스피싱 범죄수익에 대한 몰수 및 추징, 이를 위한 국제공조도 제8조(마약류 불법거래방지에 관한 특례법)에 따라 마약류 범죄의 진압과 예방에 해당하는 마약거래방지법의 수준에 해당하는 규정을 준용할 수 있게 된 것에 큰 의의가 있다.

제2절 신종 보이스피싱 법제 개정안과 주요쟁점

1. 개정법률안 현황

신종 보이스피싱에 대응하기 위한 통신사기피해환급법 개정법률안이 연이어 발의되고 있다. 2020년 9월 통신사기피해환급법과 관련하여 이주환 의원, 한병도 의원, 강민국 의원, 김민철 의원, 송재호 의원이 대표발의한 개정법률안 5건이 국회에 계류 중이다.

<표 5-1> 최근 발의된 통신사기피해환급법 개정안의 주요 내용

제안일	대표 제안 의원	주요 내용
20.09.07.	이주환 의원 (국민의 힘)	직접 대면 수법도 전기통신금융사기에 포함
20.09.08.	한병도 의원 (더불어민주당)	금융위원회 전기통신금융사기대응위원회 설치, 금융회사 규정 위반 시 과태료 상향
20.09.11.	강민국 의원 (국민의 힘)	금융회사가 금융거래 목적 확인할 수 있도록 법률로 규정
20.09.14.	김민철 의원 (더불어민주당)	전기통신금융사기에 대해 무기 징역 이 가능하도록 벌칙 상향
20.09.18.	송재호 의원 (더불어민주당)	금융회사 및 간편송금서비스업체 피해의심거래계좌 발견 위한 상시 자체점검 의무화

(출처 : 국회 의안정보시스템 내용 취합; 강진규, Digital Today(2018))

2. 개정법률안 주요 내용

가. 이주환 의원 대표발의안 (의안번호 3570, 2020. 9. 7.)

이주환 의원(국민의힘) 등 14인이 발의한 개정법률안은 전기통신금융사기 범위를 확대하는 내용을 담고 있다. 현행법이 전기통신금융사기를 “전기통신을 이용해

타인을 기망, 공갈함으로써 자금을 송금, 이체하도록 하거나 타인의 개인정보를 알아내어 자금을 송금, 이체하는 방법으로 재산상의 이익을 얻는 행위”로 규정하고 있어 전화로 피해자에게 접근해 계좌의 예금을 인출하도록 한 뒤 피해자를 직접 만나 자금을 건네받는 수법을 처벌하지 못하는 문제를 해소하고자 하였다. 더불어 전자통신금융사기의 개념을 확장하여 범죄에 이용된 전화번호에 대한 제재를 못하는 문제도 해결하고자 하였다.²¹⁸⁾

전자금융거래법 개정으로 대포통장 개설 및 양도가 점점 어려워져 대면 편취형 또는 침입 절도형 보이스피싱²¹⁹⁾이 증가할 것으로 보인다. 대면 편취형과 침입 절도형 보이스피싱은 올해 7월 말까지 8,937건이나 발생하였고, 같은 기간 발생한 보이스피싱 범죄 중 47.7%의 비율을 차지하고 있다. 2019년 7월 감사원이 발표한 ‘금융 전기통신금융사기 방지대책 추진실태’ 보고서에 따르면 경찰청은 송금·이체행위가 없는 대면편취·절도형 등에 사용된 전화번호도 이용중지할 수 있도록 법률 개정이 필요하다고 지적하고 있다.²²⁰⁾ 이에 대면 편취형 보이스피싱 범죄도 통신사기피해환급법상 전기통신금융사기에 포함시켜 형사처벌의 사각지대를 없애는 입법이 필요해 보인다.

218) 이주환의원 등 14인 발의, “전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 일부개정법률안”, 3570, (2020. 9. 7.) [계류 중]

219) 침입 절취형 보이스피싱은 범죄자들이 경찰관 등을 사칭하여 피해자의 개인정보가 유출됐으니 예·적금을 인출해서 집에 보관해두고, 아파트의 비밀번호를 알려주면 경찰관을 보내서 보관할 수 있도록 하겠다고 기망하여 해당 재물을 편취하는 보이스피싱의 유형을 말한다.

220) 해럴드 경제 보도(2020.9.7.), “직접 만나 돈 뺏는 보이스피싱 피해↑…이주환, 법안 발의”,
<http://news.heraldcorp.com/view.php?ud=20200907000364> (2020.10.1. 최종확인)

나. 한병도 의원 대표발의안 (의안번호 3584, 2020. 9. 8.)

한병도 의원(더불어민주당) 등 13인이 발의한 개정법률안은 금융당국의 역할을 강화하는 내용을 담고 있다.²²¹⁾ 현행법은 금융위원회로 하여금 전기통신금융사기 대응 관련 업무를 수행하도록 하고 있으나, 최근 전기통신금융사기 수법이 지능화·고도화되고 있어 금융당국에서 범죄 예방 및 피해자 구제 등의 업무를 모두 대응하기에 한계가 있다. 개정법률안은 정부로 하여금 금융위원회, 과학기술정보통신부, 법무부, 외교부 및 경찰청 등 관계 기관 간 협업체계를 구축하도록 하고, 전기통신금융사기 대응 관련 정책의 수립 및 관계 기관 간 업무 협의를 위하여 금융위원회에 전기통신금융사기대응위원회를 설치하도록 한다.

또한 현행법은 피해구제 관련 각종 절차를 수행하지 아니한 금융회사에게 1천만원 또는 500만원 이하의 과태료를 부과하고 있으나 과태료가 낮아 금융회사의 책임을 담보하기에 부족하다는 문제가 있었다. 개정법률안은 금융회사에 대한 과태료 부과 수준을 현행 ‘1천만원 또는 500만원 이하’의 과태료를 ‘3천만원 이하’의 과태료로 상향 조정하도록 하였다.

다. 강민국 의원 대표발의안 (의안번호 3800, 2020. 9. 11.)

강민국 의원(국민의힘) 등 11인이 발의한 개정법률안은 금융회사가 계좌를 개설하는 고객에게 금융거래 목적을 확인할 수 있도록 하는 내용을 담고 있다.²²²⁾ 최근 은행 등 금융회사들은 대포통장 개설을 막기 위해 신규 계좌를 만드는 고객들에게 금융거래 목적을 확인하기 위한 서류를 요구하고 있는데, 이는 특정금융정보법에 근거를 두고 있다. 금융회사는 이를 통해 고객의 금융거래 목적을 확인할 수 있으며, 확인이 불가능한 경우에는 계좌 개설을 거절할 수 있는 것이다.

221) 한병도의원 등 13인 발의, “전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 일부개정법률안”, 3584, (2020. 9. 8.) [계류 중]

222) 강민국의원 등 11인 발의, “전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 일부개정법률안”, 3800, (2020. 9. 11.) [계류 중]

그러나 현행법에서는 자금세탁행위 및 공중협박자금조달행위를 방지하기 위한 경우를 제외하고는 금융회사가 금융거래의 목적을 확인할 수 있다는 규정을 두고 있지 않아 은행창구 현장에서 고객들의 불만 및 민원이 발생하고 있다. 특히 은행 창구 직원이 금융거래업무를 도와줌에 있어 고객이 보이스피싱에 연루되어 현금을 인출하는 등 수상한 낌새를 느끼어 이를 확인하고 싶을 때도 고객들이 항의를 하고 금융거래 목적 확인에 응하지 않으면 금융회사 측에서는 거래 목적을 확인하고 개입할 수 있는 법적 근거가 없어 보이스피싱 예방이나 선제적 대응이 불가능하다. 개정법률안은 대통령령으로 정하는 고객이 전자금융거래를 위한 계좌의 개설을 신청하는 경우 금융회사가 그 금융거래의 목적을 확인하도록 법률에 규정하고, 그 목적이 전기통신금융사기와 관련되어 있거나 고객이 정보 제공을 거부하여 확인을 할 수 없는 경우에는 그 계좌 개설을 제한할 수 있도록 하였다. 다만, 모든 고객들이 금융거래 목적을 금융회사에 알려야만 계좌를 개설할 수 있도록 하는 것은 과도한 규제에 해당할 수도 있어 시행령 제정 시 면밀한 검토가 필요하다.

라. 김민철 의원 대표발의안 (의안번호 3851, 2020. 9. 14.)

김민철 의원(더불어민주당) 등 14인이 발의한 개정법률안은 전기통신금융사기 처벌을 강화하는 내용을 담고 있다.²²³⁾ 개정법률안은 전기통신금융사기에 대한 벌칙을 ‘10년 이하의 징역 또는 1억원 이하의 벌금’에서 ‘무기 또는 10년 이상의 징역’으로 상향하는 것을 골자로 하고 있다. 또한 ‘해당 범죄행위로 인하여 취득하거나 제3자로 하여금 취득하게 한 재물 또는 재산상 이익의 가액’의 2배 이상 10배 이하에 상당하는 벌금을 반드시 병과하도록 함으로써 보이스피싱 범죄자에 대한 위하효과를 제고하고 국민의 불안을 경감시키고자 한다. 해당 범죄의 미수범 또한 같은 수준으로 처벌하도록 하였다.

223) 김민철의원 등 14인 발의, “전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 일부개정법률안”, 3851, (2020. 9. 14.) [계류 중]

마. 송재호 의원 대표발의안 (의안번호 4027, 2020. 9. 18.)

송재호 의원(더불어민주당) 등 13인이 발의한 개정법률안은 피해의심거래계좌를 선제적으로 대응하도록 하는 내용을 담고 있다.²²⁴⁾ 현행법은 금융회사로 하여금 이용자의 계좌가 피해의심거래계좌로 이용되는 것으로 추정할 만한 사정이 있다고 인정되면 해당 계좌의 이체 또는 송금을 지연시키거나 일시 정지하는 임시조치를 하도록 규정하고 있다. 그러나 현행법은 피해의심거래계좌를 선제적으로 발견하도록 하는 의무를 금융회사에 부여하고 있지 않고, 이에 대한 처벌 규정도 마련하고 있지 않아 금융회사가 전기통신금융사기에 소극적으로 대처한다는 지적이 있다. 최근 간편송금서비스를 이용한 전기통신금융사기가 증가하고 있음에도 간편송금서비스를 제공하는 사업자에 대한 의무가 현행법에 규정되어 있지 않아 법률 규정의 사각지대가 존재하고 피해자의 구제도 어려운 실정이다.

이에 개정법률안은 금융회사 및 간편송금서비스를 제공하는 사업자로 하여금 피해의심거래계좌를 발견하기 위하여 상시적으로 자체점검을 실시하도록 규정하였다. 금융감독원이 전자금융거래제한대상자를 지정한 경우 그 사기이용계좌 및 거래내역에 관한 사항을 법무부, 경찰청 등에 통지하도록 하여 금융범죄로 인한 피해 방지를 위하여 금융회사 및 관계 기관의 적극적 조치 의무를 명시하였다. 금융회사에 상시 자체점검 실시 의무화 규정을 두고 규제 대상에 간편송금서비스 사업자를 포함시키는 것은 보이스피싱 예방의 주요 이해 당사자로서 보다 적극적인 금융회사의 대처를 이끌어 낼 수 있을 것으로 보인다.

224) 송재호의원 등 13인 발의, “전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 일부개정법률안”, 4027, (2020. 9. 18.) [계류 중]

제3절 신종 보이스피싱 양형기준

1. 신종 보이스피싱 양형 실태

양형기준은 법관이 형을 정함에 있어 참고할 수 있는 기준으로, 법관이 각 범죄에 대응하여 법률에 규정되어 있는 법정형 중에서 선고할 형의 종류를 선택하고 법률에 규정된 바에 따라 형의 가중·감경, 집행유예 여부 등을 결정하는 기준이 된다. 원칙적으로 구속력은 없으나, 법관이 양형기준을 이탈하는 경우 판결문에 양형이유를 기재해야 하므로 합리적 사유 없이 양형기준을 위반할 수는 없다.

보이스피싱은 불특정 다수를 대상으로 금전적, 정신적 측면에서 막대한 피해를 주고, 대부분 사회적 취약계층을 대상으로 이루어지는 악질적인 범죄 중 하나이다. 그럼에도 보이스피싱 범죄자들은 1~3년의 비교적 낮은 징역형을 선고받는 경우가 많고, 집행유예가 선고되는 사례도 있다.

2019년 7월, 서울동부지방법원은 보이스피싱 조직에 가담해 금융위원회 위원장 명의로 문서 7장을 위조하고 피해자에게 갈취한 돈을 송금하는 등 범죄에 적극 가담한 피고인에 대해 판결했으나, 법원은 피고인이 고등학생이라는 점을 참작해 징역 장기 10월, 단기 8월을 선고했다.²²⁵⁾ 부산지방법원은 2019년 11월, 직접 전화로 16명의 피해자를 기망해 9,500만원을 편취한 보이스피싱 조직의 콜센터 상담원에 대해 보이스피싱에 직접 가담해 엄벌이 불가피하다며 선고한 형량이 징역 3년이다.²²⁶⁾ 올해 2월, 보이스피싱 피해로 인해 20대 청년이 스스로 목숨을 끊은 사건이

225) Law Leader 보도(2019.7.29.), “권덕진 판사, 보이스피싱 조직에 고용된 고등학생 실형 선고 왜?”,
<http://www.lawleader.co.kr/news/articleView.html?idxno=2863>(2020.10.1.
 최종확인)

226) Digital Today 보도(2020.6.25.), “보이스피싱과 전쟁 선포했지만... 솜방망이 처벌에 실효성 의문”,
<http://www.digitaltoday.co.kr/news/articleView.html?idxno=238861>(2020.10.1.
 최종확인)

발생할 정도로 피해자에게 극심한 피해를 주는 보이스피싱 범죄의 중대성과 국가적인 손실에 비해 보이스피싱 범죄에 대한 처벌은 너무나 가벼운 것이 현실이다. 특히 반복적, 계획적으로 이뤄지고 조직적인 체계를 가지고 행해지는 보이스피싱 범죄, 피해액이 큰 보이스피싱에 대해서는 이에 비례하여 더욱 무겁게 처벌하는 가중 처벌 규정을 통해 피해에 합당한 처벌을 내릴 필요가 있다.

2. 형법상 사기죄 양형기준

보이스피싱은 형법상 사기 범죄의 일종으로 사기 중에서도 개인이 수행하는 일반적인 사기 범죄가 아닌 범죄 조직을 구성하고 기능별로 역할을 담당하여 이루어지는 조직적 사기로 분류할 수 있다. 일반적으로 조직적 사기는 다수인이 역할을 나누어서 사기 범행을 저지르고 피해의 규모도 커지기 때문에 일반범죄보다 중한 범죄로 본다. 이와 관련하여 적용되는 양형위원회의 사기범죄 양형기준(조직적 사기의 경우)은 다음과 같다. 여기서 기준이 되는 이득액은 범죄행위로 인하여 취득하거나 제3자로 하여금 취득하게 한 재물 또는 재산상 이익의 가액을 의미한다.

〈표 5-3〉 사기범죄 양형기준(양형위원회) : 조직적 사기의 경우

유형	구분	감경	기본	가중
1	1억 원 미만	1년 ~ 2년6월	1년6월 ~ 3년	2년6월 ~ 4년
2	1억 원 이상, 5억 원 미만	1년6월 ~ 3년	2년 ~ 5년	4년 ~ 7년
3	5억 원 이상, 50억 원 미만	2년 ~ 5년	4년 ~ 7년	6년 ~ 9년
4	50억 원 이상, 300억 원 미만	4년 ~ 7년	6년 ~ 9년	8년 ~ 11년
5	300억 원 이상	6년 ~ 10년	8년 ~ 13년	11년 이상

구분		감경요소	가중요소
특별 양형 인자	행위	<ul style="list-style-type: none"> · 기망행위의 정도가 약한 경우 · 손해발생의 위험이 크게 현실화되지 아니한 경우 · 사실상 압력 등에 의한 소극적 범행 가담 · 단순 가담 · 피해자에게도 범행의 발생 또는 피해의 확대에 상당한 책임이 있는 경우 	<ul style="list-style-type: none"> · 사기범행을 주도적으로 계획하거나 그 실행을 지휘한 경우 · 불특정 또는 다수의 피해자를 대상으로 하거나 상당한 기간에 걸쳐 반복적으로 범행한 경우 · 피해자에게 심각한 피해를 야기한 경우 · 범죄수익을 의도적으로 은닉한 경우 · 피지휘자에 대한 교사
	행위자 /기타	<ul style="list-style-type: none"> · 농아자 · 심신미약(본인 책임 없음) · 자수, 내부비리 고발 또는 사기범행의 전모에 관한 완전하고 자발적인 개시 · 처벌불원 또는 상당부분 피해 회복된 경우 	<ul style="list-style-type: none"> · 상습범인 경우 · 동종 누범
일반 양형 인자	행위	<ul style="list-style-type: none"> · 기본적 생계치료비 등의 목적이 있는 경우 · 범죄수익의 대부분을 소비하지 못하고 보유하지도 못한 경우 · 소극 가담 	<ul style="list-style-type: none"> · 비난할 만한 범행동기 · 범행에 취약한 피해자 · 인적 신뢰관계 이용
	행위자 /기타	<ul style="list-style-type: none"> · 심신미약(본인 책임 있음) · 진지한 반성 · 형사처벌 전력 없음 · 피해 회복을 위한 진지한 노력 	<ul style="list-style-type: none"> · 범행 후 증거은폐 또는 은폐 시도 · 이종 누범, 누범에 해당하지 않는 동종 및 횡령배임범죄 실행전과 (집행종료 후 10년 미만)

형량은 피해액 기준으로 1억 원 미만, 1억 원 이상 5억 원 미만, 5억 원 이상 50억 원 미만, 50억 원 이상 300억 원 미만, 300억 원 이상 등 제1유형에서 제5유형까지 나눌 수 있으며 사안에 따라 1년에서 11년 이상까지 선고가 가능하다. 재판부가 감경요소 및 가중요소를 고려하여 감형을 할 수도 가중을 할 수도 있으며 선

처를 받으면 집행유예 선고도 가능하다. 형의 가중 요소는 사기범행을 주도적으로 계획하거나 그 실행을 지휘한 경우, 불특정 또는 다수의 피해자를 대상으로 하거나 상당한 기간에 걸쳐 반복적으로 범행한 경우, 피해자에게 심각한 피해를 입힌 경우, 상습범이거나 동종 범죄의 누범인 경우, 범죄수익을 의도적으로 은닉한 경우 등이 있다. 반면 사기 범행인지 모르고 단순가담한 경우, 손해발생 위험이 크게 현실화되지 아니한 경우, 피해자와 합의한 경우, 사실상 압력 등에 의해 소극적으로 가담한 경우 등에는 감형이 가능하다.

3. 전자금융거래법위반 양형기준

양형위원회는 최근 사기범죄의 양형기준 뿐만 아니라 전자금융거래법위반범죄에 대한 양형기준도 마련해두고 있다. 2019년 7월 1일부터 시행된 전자금융거래법위반범죄 양형기준은 다음과 같다.

〈표 5-4〉 전자금융거래법위반범죄 양형기준(양형위원회)

유형	구분	감경	기본	가중
1	일반적 범행	~ 6월	4월 ~ 10월	6월 ~ 1년2월
2	영업적·조직적·범죄이용 목적 범행	~ 8월	6년 ~ 1년6월	10월 ~ 2년6월

구분		감경요소	가중요소
특별 양형 인자	행위	<ul style="list-style-type: none"> 범행가담 또는 범행동기에 특히 참작할 사유가 있는 경우 단순 가담 	<ul style="list-style-type: none"> 범행을 주도적으로 계획하거나 그 실행을 지휘한 경우(2유형 중 조직적 범행) 접근매체의 수가 다량인 경우 또는 범죄로 인한 수익이 매우 큰 경우 피지휘자에 대한 교사

특별 양형 인자	행위자/ 기타	<ul style="list-style-type: none"> · 농아자 · 심신미약(본인 책임 없음) · 자수, 내부고발 또는 범행(2유형 중 조직적 범행)의 전모에 관한 완전하고 자발적인 개시 · 자발적 거래정지·분실 신고 등으로 후속범죄 위험이 현실화되지 않은 경우 	<ul style="list-style-type: none"> · 동종 누범
일반 양형 인자	행위	<ul style="list-style-type: none"> · 소극가담 · 생계형 범죄 · 실제 이득액이 없거나 경미한 경우 	<ul style="list-style-type: none"> · 비난할 만한 범행동기 · 후속범죄로 인하여 중대한 피해가 야기된 경우
	행위자/ 기타	<ul style="list-style-type: none"> · 진지한 반성 · 형사처벌 전력 없음 · 일반적 수사협조 	<ul style="list-style-type: none"> · 범행후 증거은폐 또는 은폐 시도 · 이종 누범, 누범에 해당하지 않는 동종 실행전과(집행 종료 후 10년 미만)

전자금융거래법위반범죄 양형기준은 보이스피싱 수단으로 이용되고 있는 통장 매매행위 등에 대한 양형기준을 설정하고 일반적 범행과 영업적·조직적·범죄이용 목적 범행을 구분하여 후자를 가중처벌하기 위해 만들어졌다. 적용법조는 전자금융거래법 제49조 제4항 제1호를 위반하여 접근매체를 양도하거나 양수한 자, 제2호 또는 제3호를 위반하여 접근매체를 대여 받거나 대여한 자 또는 보관·전달·유통한 자, 제4조를 위반한 질권설정자 또는 질권자, 제5호를 위반하여 알선하거나 광고하는 행위를 한 자를 구성요건으로 하고 법정형은 5년 이하의 징역 또는 3천만 원 이하의 벌금형이다. 영업적·조직적·범죄이용목적 범행의 경우 가중영역 상한을 징역 2년6월로 설정하여 비난가능성이 큰 사안에서는 특별가중으로 법정최고형인 징역 5년까지 선고가능하다(사기죄 등이 병합될 경우 추가 형량 상향). 가중처벌이 가능한 경우는 조직적 범행을 주도적으로 계획하거나 그 실행을 지휘한 경우, 접근매체의 수가 다량인 경우, 동종 누범, 피지휘자에 대한 교사 등의 경우

이며 특별가중인자로 반영하여 가중처벌한다. 반면 범행가담 또는 범행동기에 특히 참작할 사유가 있는 경우, 단순가담, 자발적 거래정지·분실신고 등으로 후속범죄 위험이 현실화되지 않은 경우 등은 특별감경인자로 형을 감경한다.

특히 최근 전자금융거래법은 법률 개정(2020.05.19.)을 통해 대포통장을 양도·양수, 대여하는 행위에 대한 처벌을 ‘징역 3년, 벌금 2천만원’에서 ‘징역 5년, 벌금 3천만원’으로 상향하였고 현행 처벌대상인 알선·광고 외에 대포통장을 중개하거나 대가를 전제로 권유하는 행위도 처벌하기로 하였다. 보이스피싱에 이용될 것을 알면서도 계좌 관련 정보를 제공·보관·전달·유통하는 행위도 처벌한다. 대포통장 범죄의 형량을 5년 이하로 상향한 것은 대포통장조직에 범죄단체조직죄를 적용할 수 있게 되었다는 것에 큰 의의가 있고, 이에 따라 대포통장조직에도 대포통장 및 범죄단체조직죄를 동시 적용하여 경합범으로 가중처벌할 수 있고, 범죄단체조직죄는 범죄수익은닉규제법상 중대범죄에 해당하므로 범죄수익 환수까지 가능하다.

제4절 법제분석 및 시사점

보이스피싱과 관련하여 다양한 입법적 논의가 있으나 우선 국회에 계류 중인 통신사기피해환급법 개정법률안의 내용을 비교·검토해 보고자 한다. 현재 계류중인 법률에 대해서 각각 목적, 주요 개정 내용, 개정 조항을 정리하면 다음과 같다.

〈표 5-2〉 통신사기피해환급법 개정안 비교검토

구분	이주환의원 대표 발의안	한병도 의원 대표 발의안	강민국 의원 대표 발의안	김민철 의원 대표 발의안	송재호 의원 대표 발의안
목적	<ul style="list-style-type: none"> 대면 편취형, 침입 절도형 등 신종 보이스피싱 범죄 대응수단 마련 	<ul style="list-style-type: none"> 보이스피싱 대응에 대한 금융당국의 역할 강화 전기통신금융사기에 대한 금융회사의 대응 의무 강화 	<ul style="list-style-type: none"> 금융회사에 고객 금융거래 목적 확인 권한부여를 통한 대포통장 개설 방지 	<ul style="list-style-type: none"> 전기통신금융사기에 대한 처벌 및 벌금 대폭 강화 	<ul style="list-style-type: none"> 금융회사 및 간편송금서비스업체의 상시자점점 및 보고 의무 강화
주요 개정 내용	<ul style="list-style-type: none"> ‘전기통신금융사기’의 범위에 “직접 대면하여 자금을 건네받는 행위” 포함 	<ul style="list-style-type: none"> 보이스피싱 대응을 위한 관계기관 협업체계 구축 의무 부여 전기통신금융사기대응위원회 설치 금융회사의 피해구제 의무 해태에 대한 과태료 상향 	<ul style="list-style-type: none"> 고객의 대포통장 개설 의심시 금융회사에 금융거래 목적 확인 권한 부여 미 확인시 계좌 개설거절가능 	<ul style="list-style-type: none"> 전기통신금융사기에 대한 벌칙을 ‘10년 이하의 징역 또는 1억원 이하의 벌금’에서 ‘무기 또는 10년 이상의 징역’으로 대폭 상향 범죄 수익의 2~10배 상당의 벌금 병과 	<ul style="list-style-type: none"> 금융회사 및 간편송금서비스사업자에 피해의심거래좌 발견을 위한 상시 자체 점검 의무 부여 관련 내용 인지도 향상 수사당국에 통지 및 적극적인 조치 의무 명시
개정 조항	<ul style="list-style-type: none"> 제2조(정의) 개정 제명중 “전기통신금융사기”를 “전기통신사기”로 개정 	<ul style="list-style-type: none"> 제2조의3(상호협력체계) 제2호 신설 제2조의4(전기통신금융사기대응위원회) 신설 과태료 규정 개정 	<ul style="list-style-type: none"> 제2조의6(금융거래의 목적 확인) 신설 금융거래의 목적을 확인하지 아니한 금융회사에 과태료 부과 	<ul style="list-style-type: none"> 제15조의2(벌칙) 개정 법정형 및 벌금 강화 	<ul style="list-style-type: none"> 제2조의5(이용자계좌에 대한 임시조치) 개정 제4조(지급정지) 개정 제13조의2(사기이용계좌의 명의인에 대한 전자금융거래 제한) 개정

이주환 의원 대표발의안은 대면 편취형, 침입절도형 등 신종 보이스피싱에 대응하기 위해 전기통신금융사기의 범위에 “직접 대면하여 자금을 건네받는 행위”를 포함하자는 내용이다. 대포통장에 대한 규제가 강화되어 범죄자들이 대면 편취형과 침입 절도형으로 이동하고 있기 때문에 이러한 불법행위를 차단하기 위해 법률 개정을 조속히 추진할 필요가 있다. 다만, 구성요건을 “재물”을 삼입하는 형태로 할 것인지, “직접 대면하여 자금을 건네받는 행위”를 추가할 것인지에 대해서는 추가적인 고민이 필요해 보인다. 입법이 되면 대면 편취형, 침입절도형 등 신종 보이스피싱에 사용된 전화번호에 대한 이용중지 조치도 가능해 질 것이다.

한병도 의원 대표발의안은 보이스피싱 대응을 위한 관계기관의 협업체계를 구축하고, 전기통신금융사기대응위원회를 설치하여 지속가능한 협의체를 운영하자는 내용이다. 그간 정부에서 부처간 협력체계를 운영하여 대응하여 왔지만, 새롭게 등장하는 보이스피싱에 대응하는데 한계를 보인 것도 사실이다. 따라서 정책의 책임성을 확보하고 일관성 있게 추진해 나가기 위해 거버넌스 체계를 구축하고 법적 근거를 마련하는 것도 필요하다고 보여 진다.

장민국 의원 대표 발의안은 대포통장 개설 의심 시 금융회사가 고객에게 금융거래 목적을 확인할 수 있도록 하고 관련 증빙 자료를 요청할 수 있도록 하자는 내용이다. 보이스피싱에 대해 금융회사가 적극 개입하여 예방할 수 있다는 측면에서 긍정적이지만 금융거래자에게 다소간의 불편함을 줄 수 있을 것으로 보인다. 이러한 마찰을 해소하면서 대포통장 개설을 차단할 수 있는 방안에 대한 논의가 병행되어야 할 것으로 보인다.

김민철 의원 대표발의안은 전기통신금융사기에 대한 벌칙을 ‘무기 또는 10년 이상의 징역’으로 상향하고 범죄 수익의 2~10배 상당의 벌금을 병과하자는 내용이다. 범죄자에 대한 강력한 위하효과가 있다는 측면에서는 긍정적이지만, 전기통신금융사기가 다양한 태양을 포함하고 있기 때문에 “무기징역 또는 10년 이상의 징역”으로 규정하는 것이 타당한지 검토가 필요하다. 나아가 다른 불법행위의 법정 형과 비교하여야 할 것이다.

송재호 의원 대표 발의안은 금융회사 및 간편송금서비스를 제공하는 사업자로 하여금 피해의심거래계좌를 발견하기 위하여 상시적으로 자체 점검을 실시하자는 내용이다. 보이스피싱 대응 당사자로 간편송금사업자를 포함시키고, 금융회사의 적극적인 대처를 요구한다는 측면에서 긍정적이지만, 금융권의 부담이 커지므로 수용 가능한 수준에서 규제 방식을 택할 필요가 있을 것이다.

한편, 법률에서 보이스피싱에 대해서 법정형을 상향하는 등 강력하게 규제 하고 있음에도 실제 선고형량은 약하다는 비판이 있다. 보이스피싱에 대한 양형기준을 마련하고 가중처벌 요소를 고려하여 선고한다지만 판결에서는 다양한 감경요소가 고려되기 때문에 솜방망이 처벌에 그치는 경우가 많다는 것이다. 범죄자들이 범죄 수익금으로 일부 피해자와 합의하여 형량을 낮추려는 시도도 많이 일어나고 있다. 따라서 보이스피싱의 계획성, 조직적 운영, 반복성, 피해액의 규모, 범죄수익의 은닉 여부 등을 고려하여 가중처벌 요소를 적극 고려하여 보다 강력하게 처벌하는 것이 필요하다.

제6장 해외 신종 보이스피싱 대응체계 및 법제

제1절 미국의 대응체계 및 법제

1. 범죄 동향

미국에서 보이스피싱은 Voice와 Phishing의 결합어로 Vishing이라고 불리고 사람이 직접하기도 하지만 AI나 컴퓨터 프로그램을 통해서 하는 보이스피싱도 대두되고 있다. 보이스피싱 범죄의 주된 목적은 신용카드정보, 개인정보, 개인계좌, 비밀번호 등을 얻어내는 것이다.²²⁷⁾ 미국에서 행해진 보이스피싱의 한 사례로 무작위로 전화를 걸어 수신자에게 ‘제 목소리가 들리세요?(Can you hear me?)’ 라고 묻고 수신자가 ‘예(Yes, Sure, Ok)’라고 대답하면 금융사기에 걸려드는 사기가 성행했다. 사기범은 수신자의 대답을 녹음하여 각종 물건 구매에 사용하고 소비자가 구매에 동의했다는 증거로 녹음한 음성을 활용하는 수법을 이용했다. 정부기관을 사칭해 배심원에 선정되었다고 전화하여 사회 보장 번호와 인적사항 등 개인정보를 탈취하기도 하였다.²²⁸⁾ FBI 인터넷 범죄 민원센터(IC3)의 보고에 의하면 2018년 및 2019년 1년 동안 총 사이버 범죄 피해액 \$3.5 billion 중²²⁹⁾ 보이스피싱 범죄를 포함하는 피싱 범죄로 \$57 million 이상의 손해가 발생하였다. 2019년의 경우

227) FBI , Internet Fraud,

<https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud> (2020.12.15.최종확인)

228) 이은진, “전기통신금융사기 피해자 구제에 관한 연구”, 고려대학교 법무대학원 석사학위논문, 2018, 37면

229) FBI (2020.2.11.), “FBI Releases the Internet Crime Complaint Center 2019 Internet Crime Report” ,
<https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2019-internet-crime-report> (2020.12.15.최종확인)

114,702건의 피싱 범죄가 발생하여 다른 유형의 범죄 통계보다 두 배 이상으로 보이스피싱을 포함한 각종 피싱 범죄가 미국에서 횡행하고 있음을 보여준다.²³⁰⁾

2. 대응 체계

가. 사이버 범죄 대응을 위한 각종 조직

미국은 사이버 기술의 증가로 인한 상호 연결성 증가와 그에 따른 도난, 사기의 위험 증가에 대해 강조하며 기업 보안 침해, 스피어 피싱, 소셜 미디어 사기 같은 다양한 형태의 사이버 공격의 취약성을 인지하고 이에 대한 다각적인 보호를 통해 대응하고 있다.²³¹⁾ 미국에서 인터넷과 관련한 국내 범죄를 조사하는 법집행기관으로는 연방수사국(the Federal Bureau of Investigation, FBI)과 비밀경호국(the United States Secret Service), 이민세관집행국(the United States Immigration and Customs Enforcement, ICE), 우편검열국(the United States Postal Inspection Service), 주류, 담배, 화기단속국(the Bureau of Alcohol, Tobacco and Firearms, ATF)이 있다. 이들 기관은 주별로 사무소를 두고 있고, 모두 워싱턴 D.C.에 본부를 두고 있다. 이 가운데 신종금융사기와 관련한 행위의 유형별로 담당 집행기관을 도표로 나타내면 아래의 표와 같다.²³²⁾

230) FBI IC3 Report, “2019 Internet Crime Report”, 2019

231) CISA, Combating Cyber Crime, <https://www.cisa.gov/combating-cyber-crime> (2020.12.15. 최종확인)

232) DOJ, REPORTING COMPUTERT, INTERNET-RELATED, OR INTELLECTUAL PROPERTY CRIME, <https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime> (2020.12.15. 최종확인)

〈표 6-1〉 미국의 신종 금융사기 관련 행위의 유형별 담당 집행기관

범죄유형	담당 법집행기관
컴퓨터 침입 (예: 해킹)	· FBI 지역사무소 · 비밀경호국 · 인터넷범죄 신고센터(IC3)
비밀번호 밀매	· FBI 지역사무소 · 비밀경호국 · 인터넷범죄 신고센터(IC3)
화폐위조	· 비밀 경호국
아동 포르노 및 착취	· FBI 지역사무소 · 수입시, 이민세관집행국(ICE) · 인터넷범죄 신고센터(IC3)
우편과 연관성 있는 아동 착취 와 인터넷 사기 행위	· 우편검열국 · 인터넷범죄 신고센터(IC3)
인터넷 사기 및 SPAM	· FBI 지역사무소 · 비밀경호국 · 연방무역위원회(FTC) · 보안관련 사기 및 투자 SPAM은 증권거래위원회(SEC) · 인터넷범죄 신고센터(IC3)
인터넷을 이용한 괴롭힘	· FBI 지역사무소
인터넷을 이용한 폭과 위협	· FBI 지역사무소 · 주류,담배,화기 단속국(ATF) 지역사무소
인터넷을 통한 폭발, 방화 장치 및 총기 밀매	· FBI 지역사무소 · 주류,담배,화기 단속국(ATF) 지역사무소
저작권 침해	· FBI 지역사무소 · 이민세관집행국(ICE) · 인터넷범죄 신고센터(IC3)
상표위조	· FBI 지역사무소 · 이민세관집행국(ICE) · 인터넷범죄 신고센터(IC3)

영업 비밀 탈취 및 경제 첩보	· FBI 지역사무소
기타 범죄 보고 및 정보 공유 기관 · 인터넷범죄 신고센터(IC3) · 국토안보부 사이버보안 및 기반시설보호청(CISA)내 국가기반시설협력처(NICC) · 국토안보부 사이버보안 및 기반시설보호청(CISA)내 컴퓨터 긴급 대응팀(US-CERT)	

나. 법무부 및 산하 연방수사국(FBI)

법무부는 2014년 12월 컴퓨터범죄 및 지식재산부(Computer Crime and Intellectual Property Section, CCIPS)에 사이버보안 부처를 신설해 사이버 공간에서의 범죄감시와 컴퓨터사기 및 남용이 사이버보안에 어떤 영향을 미치는지에 대한 전문가 자문과 법률지도의 중심 거점 역할을 하게 하였다. 해당 부처의 목표는 사범 당국이 사이버 관련 범죄자들을 효과적으로 처벌할 수 있도록 기능하도록 함과 동시에 미국인들의 프라이버시를 보호하는 것이다. 이뿐만 아니라 CCIPS는 사이버 공격으로부터 미국의 컴퓨터 네트워크와 개인들을 보호하기 위한 사이버보안 법안을 만드는 데 일조한다. CCIPS는 합법적인 사이버보안 관행을 촉진하기 위하여 민간에 대한 광범위한 홍보 활동도 병행하고 있다.²³³⁾

연방수사국(FBI)은 법무부 소속 수사기관이자 정보기관으로 통상 연방 형법 적용사건, 연방정부의 이해관계가 걸린 사안에 대해 수사를 진행하며 테러공격, 정보공작 및 간첩, 사이버 범죄, 공공부패 등과 같이 미국 사회에 대한 위협과 지방정부의 권한만으로는 다루기 어려운 사건들을 취급한다. 따라서 연방 형법이 적용되는 보이스피싱 범죄에 대해서는 연방수사국이 수사관할권을 갖는다. 이러한 연방수사국의 수사는 행위지, 피해발생지 등에 따라 각 지역사무소가 담당하게 된

233) DOJ, CTBERSECURITY UNIT,

<https://www.justice.gov/criminal-ccips/cybersecurity-unit> (2020.12.15.

최종확인)

다. 연방수사국 내에서 보이스피싱에 대한 직접적인 대응체계를 구축하고 있는 곳은 인터넷범죄 신고센터(IC3)로 2000년 이후부터 설립하여 운영하고 있다. 해당 센터의 최초 명칭은 인터넷 사기 신고센터(Internet Fraud Complaint Center)였으며 2000년 이후로 온라인 사기에서부터 지적재산권 침해, 컴퓨터 침입, 산업스파이, 국제자금세탁, 신원절도 등 사이버범죄에 대한 신고를 본격적이고 광범위하게 관리하기 시작하면서 IC3로 개명하였다. 이러한 IC3의 임무는 대중에게 신뢰할 수 있고 편리한 신고 메커니즘을 제공하고, 인터넷을 통한 범죄행위와 관련된 정보를 연방수사국(FBI)에 제출하며, 법 집행기관 및 업계 파트너와 제휴를 맺어 신고된 정보를 수사 및 대중 및 산업 파트너의 인식을 위해 분석 및 전파하는 허브의 역할을 수행하는 것이다.²³⁴⁾

이러한 IC3 내에서도 2019년에 창설된 복구 및 조사 개발(RaID)팀은 금융 기관 및 법 집행 기관과 제휴하여 관련 금융 범죄들을 조사하고 수사하고 있다. 해당 팀은 RAT(Recovery Asset Team)와 MMT(Money Mule Team)의 두 팀으로 구성되어 있다. RAT가 주로 재정 회복에 초점을 맞추고 있는 반면, MMT는 새로운 범죄에 대한 수사의 일환으로 이전에 알려지지 않았던 범죄에 대한 상세한 분석과 연구를 수행한다. 이러한 RaID의 두 팀은 서로 협력하여 사이버 보안 전문가와 금융 및 법 집행 파트너의 자원을 활용하여 끊임없이 변화하고 증가하는 사이버사기 문제를 해결하는데 도움을 주고 있다. 또한 RaID는 공개 사례 연구를 지원하고 사기 자금의 흐름을 막기 위해 필요한 모든 법적 절차를 지원하는 데 필요한 정보 공유를 촉진하기 위해 금융 및 법집행기관 수사관 간의 허브 역할을 수행하고 있다.

234) FBI IC3 Report, “2019 Internet Crime Report”, 2019

다. 국토안보부 산하 비밀경호국, 이민세관집행국(ICE), 사이버 범죄센터(C3)

비밀경호국은 애초에 요인 경호 등을 목적으로 설립되었으나, 2003년 재무부에서 국토안보국으로 소속이 바뀌면서 국가원수 경호뿐만 아니라 미국의 재정인프라 및 주요 인프라 보호 등 국토안보국이 수행하는 미국민 보호라는 보편적 임무에 기여하고 있다. 미국 비밀경호국은 전자범죄 테스크포스팀을 운영하고 있는데, 이 팀은 사이버 침입, 은행 사기, 데이터 침해, 기타 컴퓨터 관련 범죄와 관련된 국제적인 사이버 범죄자들을 식별하고 위치시키는 데 초점을 맞추고 있다. 비밀경호국은 특히 접근장치사기나 신원절도, 은행사기를 비롯해 그 외 복잡한 사이버 범죄를 수사할 권한을 가지고 있다.²³⁵⁾ 또한, 비밀경호국은 국가 컴퓨터 법의학 연구소를 운영하여 법 집행관, 검사, 판사들에게 사이버 범죄와 관련된 정보를 제공하고 있다.

이민세관집행국은 사이버범죄에 있어 국제적인 무역거래 상의 문제나 지적재산권이나 상표권의 침해에 대하여 타국가의 기관들과 국토안보부내 관세국경보호국(CBP), 법무부 및 IC3와 긴밀히 협력하여 컴퓨터 기반 기술 서비스를 제공하는 등의 대응을 취하고 있다. 또한 이러한 이민세관집행국 내부의 IPR센터는 FBI내부의 지적재산권 부대를 감독하여 사이버 범죄와 관련되어 있는 경제적인 침해에 대응하고 있다.²³⁶⁾

사이버범죄센터(C3)는 사이버범죄수사대, 아동착취수사대, 컴퓨터포렌식대로 구성되어 있고, 연방, 주, 지방 및 국제 사법 기관에 사이버 범죄 지원과 훈련을 제공하고 있다. 또한 C3는 디지털 증거회복을 전문으로 하는 완비된 컴퓨터 포렌식 연구소를 운영하고 있으며 컴퓨터 조사 및 법의학 기술 교육을 실시하고 있다.

235) CISA, Combating Cyber Crime, <https://www.cisa.gov/combating-cyber-crime> (2020.12.15. 최종확인)

236) ICE 보도(2011.5.24.), “National Intellectual Property Rights Coordination Center”, <https://www.ice.gov/factsheets/ipr> (2020.12.15. 최종확인)

라. 국토안보부 산하 사이버정보 공유 및 기반시설보호청(CISA)

정보공유는 국토안보부가 수행하는 임무 중 가장 중요한 것 중의 하나로, 이를 통해 악의적 사이버 활동에 대한 상황적 인식을 공유할 수 있도록 한다. 사이버공간을 보호하는 것은 국가의 중요 인프라와 핵심 자원을 탄력적이면서도 안정적으로 운용하는 데에 필수적이라는 인식에서 출발하여 국토안보부는 산하 국가방위·프로그램국(National Protection & Programs Directorate)에 국가 사이버 보안·통신 통합센터(National Cybersecurity and Communication Integration Center, NCCIC)를 설치하였다. 이후, 국토안보부는 '사이버보안 및 기반시설보호를 위한 전문기관 설립법'을 통해 국토안보부(DHS) 내의 국가방위·프로그램국(National Protection & Programs Directorate)을 격상하고 NCCIC를 포함하여 사이버보안을 총괄적으로 담당하는 새로운 조직, 사이버보안 기반시설보호청(Cybersecurity and Infrastructure Security Agency, CISA)을 설립하였다. 이를 통해 국토안보부는 사이버보안에 대한 국토안보부의 리더십을 강화하고, 법안 개정을 통해 사이버보안 기반시설보호청 연방기관으로서 권한을 부여받아 더 많은 정책자금을 운용할 수 있게 되었다. 이를 통해 국토안보부는 관련 정부조직에 업무지시를 적극적으로 요청할 수 있게 되었다. 이와 함께 사이버보안 기반시설보호청이 적극적으로 정부기관 민간조직·기업과의 조정을 담당하게 되어 결과적으로 미국의 국가 사이버보안을 국토안보부가 담당하는 통합적인 거버넌스 체계를 갖추게 되었다.²³⁷⁾

NCCIC는 사이버 상황인식과 사고대응 및 관리 행위를 하는 중심기관으로서 기능하며고 있으며, ① NCCIC 운영 및 통합(NO&I), ② 컴퓨터 비상대응팀(US-CERT), ③ 산업제어 시스템 사이버 비상대응팀(ICS-CERT), ④ 국가통신 조정센터(NCC)의 네 가지 분과로 구성되어 있다. NCCIC는 통합적이며 연방의 총괄적 차원에서 사이버보안과 통신 이슈를 해결하는 데에 필요한 권한과 기능,

237) 김근혜, “트럼프 행정부의 주요기반시설 사이버보안 정책분석에 관한 연구”, 한국정보보호학회, 정보보호학회지 29(4), 2019, 907-918면

협력을 제공한다. 해당 센터는 사이버보안 평가(Cybersecurity Assessments)를 하고 있으며, 이러한 평가 중 피싱 상황 평가(PCA)는 다양성을 지닌 피싱 형태에 대한 조직의 민감성과 반응을 평가하고 있다. 이를 통해 다양한 유형의 피싱에 대한 조직의 반응성이 평가되고, 피싱 공격의 피해자 성향과 관련된 지표를 요약한 평가 보고서를 받게 된다.²³⁸⁾

국토안보부의 비밀경호국²³⁹⁾과 같은 기관과 부서 및 신설 국토안보부 산하 사이버보안 기반시설보호청은 전체적으로 미국의 피싱사기에 대한 수사에 있어 독자적 특정한 범위에 있어 수사권 이외에도 정보를 취합하고 분석하는데 도움을 주며 그러한 정보를 제공하고 전문 인력을 수사기관에 제공 혹은 태스크포스를 구성하게 하고 감사한다.

마. 연방 거래 위원회(Federal Trade Commission, FTC)²⁴⁰⁾

연방거래 위원회는 1914년 기업의 불공정거래 관행으로부터 사업의 영위를 보호하는 것을 목적으로 설립된 미국의 대표적인 경쟁규제기관이다. FTC는 다양한 소비자들의 불만을 접수받아 데이터를 구축하여 법 집행기관들(FBI 등)이 수사시 참고자료 등으로 사용할 수 있도록 지원하고 있다. 이 일환으로 연방거래위원회는 보이스피싱에 대해 정의내리고 권고조치를 하는 등 연방 시민들의 피싱에 대해 보고를 받는 체계와 데이터를 가지고 있고, 그 정보를 관리하여 대응하도록 도움을

238) 김학범, “미국의 사이버보안 및 사회기반시설 보안기관법에 관한 연구”, 한국사회안전범죄정보학회, 한국정보범죄연구 5(1), 2019, 13-39면

239) CNBC 보도(2020.4.2.), “US Secret Service warns that coronavirus email scams are on the rise”,
<https://www.cnn.com/2020/04/02/us-secret-service-warns-that-coronavirus-email-scams-are-on-the-rise.html> (2020.10.1. 최종확인)

240) FTC, How to Recognize and Avoid Phishing Scams,
<https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>
 (2020.12.15. 최종확인)

주고 있다.²⁴¹⁾ FTC는 피싱에 대하여 개인정보(비밀번호, 계좌번호, 사회보장번호 등)와 관련된 각종 공격 형태에 대해 개인에게 경고하고 있다. 피싱 범죄를 당한 피해자들에 대하여 대처 방안을 안내하기도 한다.

<표 6-2> 미국의 각 행정구역의 피싱 사기범죄 대응

주(State)	관련 조항
알래스카	Alaska Stat. § § 45.45.792 et seq., 45.50.471(51)
애리조나	Ariz. Rev. Stat. § § 18.501 et seq.
알칸소	Ark. Code § § 4-111-101 to-105, § 19-6-301, § 19-6-804
캘리포니아	Cal. Bus. & Prof. Code § § 22947 to 22947.6
조지아	Ga. Code § § 16-9-152 et seq.
하와이	Hawaii Rev. Stat. § 708.890, 708.891, 708.891.5, 708.891.6
일리노이	720 ILCS 5/17-52, 720 ILCS 5/12-7.5(3)(a-4), ILCS 5/12-7.5(2)(2.2)
인디애나	Ind. Code § § 24-4.8-1et seq.
아이오와	Iowa Code § § 715.1to 715.8
루이지애나	La. Rev. Stat. § § 51:2006 to 51:2014
네바다	Nev. Rev. Stat. § 205.4737
뉴햄프셔	N.H. Rev. Stat. § § 359-H:1 to 359-H:6
뉴욕(州)	N.Y. Penal Law § 156.00
펜실베이니아	73 P.S. 2330.1et seq.
로드아일랜드	R.I. Gen. Laws § § 11-52.2-2,-3,-4,-5,-6,-7

241) FTC, How to Recognize and Avoid Phishing Scams,
<https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>
 (2020.12.15. 최종확인)

텍사스	Tex. Bus. & Comm. Code § § 324.001 to 324.102
유타	Utah Code § § 13-40-301to -303,13-40-402
버지니아	Va. Code § 18.2-152.4
워싱턴(州)	Wash. Rev. Code § § 19.270.101 to 19.270.900
와이오밍	Wyo. Stat. § 6-3-506
괌	9 GCA 46.601 to .602
푸에르토리코	10 L.P.R.A. § § 2181et seq.

바. 각 주(State)별 피싱 사기범죄 대응 현황

미국의 23개의 주와 괌에서는 온라인 피싱(phishing)사기를 특정 범죄로 취급하고 이를 엄격히 금지하고 발생한 범죄를 처벌하도록 하고 있다.²⁴²⁾ 인터넷 웹사이트, 전자우편, 기타 수단을 이용하여 해당 사업자의 권한 또는 승인 없이 사업자로 사칭하여 개인신원확인정보를 요청하거나 타인으로 하여금 이를 제공하도록 유도하는 행위를 불법으로 규정하고 있는 ‘피싱사기방지법(Anti-phishing Act)’은 캘리포니아 외 7개 주에서 명시적으로 입법화하였고, 그 외의 주에서는 ‘사기범죄’ 또는 ‘컴퓨터범죄’ 관련 규정을 통해 연방제라는 독특한 국가 구성방식 내에서의 세부 행정체계를 통해 대응하고 있다.

242) NCSL 보도(2020.2.23.), “State Laws Addressing “Phishing” ”, <https://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx> (2020.12.15. 최종확인)

3. 대응 법률

가. 개인정보 및 금융정보 보호에 관한 법제

1) 연방정보보안현대화법(FISMA)²⁴³⁾

미연방법전 제44편 제35장은 9.11 테러사건을 계기로 제정된 2002년 연방정보보안관리법(Federal Information Security Management Act of 2002, FISMA 2012)에 의해 삽입·시행된 부분이다. 이는 모든 연방기관에 대해 정보보안을 위한 범기관적 프로그램을 개발하고 기록하며 시행할 것을 요구한다. 본 편은 다시 2014년도에 연방정보보안현대화법(Federal Information Security Modernization Act of 2014, FISMA 2014)에 의해 개정되었는데, 이로써 종전의 제2절과 제3절이 삭제되고, 새로 제2절이 삽입되었다. 이렇게 개정된 미연방법전 제44편 제35장은 연방의 정보정책(Federal Information Policy)을 규정하고 있는 제1절(Subchapter I, § § 3501~3531)과 정보보안(Information Security)을 규정하고 있는 제2절(Subchapter II, § § 3551~3558)로 구성되어 있다. 해당 법률은 국토안보부 장관, 관리예산국 국장(Director of the Office of Management and Budget) 등의 권한과 기능, 연방정부 기관의 보고 및 통지의무 등을 규정하고 있으며, 다만 정보침해나 의무위반 등에 대한 형사제재에 관한 내용은 두고 있지 않다.

2014년에 개정된 FISMA에 따르면, 본 법은 정보보안의 효율성 제고를 위한 포괄적 거버넌스를 제시하고, 연방의 정보 및 정보시스템을 보호하기 위해 필요한 최소한의 통제체계 개발과 유지를 지원하며, 연방기관의 정보보안 프로그램을 보다 효과적으로 개선하기 위한 메커니즘을 제공하는 것을 목적으로 한다. 이러한 목적을 위해 관리예산국 국장에게는 모든 연방기관의 정보보안정책과 실무를 감독할 권한을 부여하였다. 또한, 국토안보부 장관에게는 관리예산국 국장을 지원하며 연방정부의 정보시스템에 대한 기관의 정보보호 활동 이행을 관리할 권한이 부

243) Pub.L. 113-283, Stat. 2521

여하고, 타 기관의 네트워크에 대해 국토안보부의 기술적 지원 및 기술 부서 인원 배치를 승인할 수 있게 하였다. 그리고 국토안보부 산하에 정보보안사고센터(US-SERT)를 배치하였다. 해당 법률에 의하면 연방정부의 각 기관은 매년 의회에 기관보고를 할 때 통상적인 주요정책보고 및 회계정보보고에 더해 보안요구사항과 보안위협, 보안사고 등에 관한 사항까지 보고해야 한다. 또한, 연방정부 기관들은 정보침해에 대한 통지정책과 지침을 정기적으로 갱신해야 하며, 침해사고가 발생한 경우 신속하게 의회에 통지해야 한다. 이뿐만 아니라 개인에 대한 통지정책도 개정되었다. 관리예산국 국장은 비효율적 보고체계를 없애고 정보보호 담당자가 정보시스템 보호를 위해 많은 자원을 활용할 수 있도록 법 개정 이후 1년 이내에 관리예산규칙(Budget Circular A-130)을 개정하도록 하였다. 해당 법은 거버넌스 체계의 수정으로 FISMA 관련 보고를 간소화하여 주요 정보보안 사고에 대한 새로운 보고 요구사항을 추가하는 동시에 비효율적이고 낭비적인 보고를 제거하려 하는 것이다.²⁴⁴⁾

2) 신원절도 및 사기에 관한 미연방법전 제18편

미연방법전 제18편은 범죄와 형사절차에 관한 규정이다. 제18편은 크게 (1) 범죄, (2) 형사소송, (3) 교도소와 수형자, (4) 청소년 범죄자 교정, (5) 증인의 면책이라는 다섯 개의 부(Part)으로 구성되어 있다. 신종금융사기와 관련해 살펴볼 만한 것은 제1조부터 제2725조로 이루어진 제1부 “범죄(Crimes)”이며, 제1부는 총 123개의 장으로 구성된다. 그 가운데에서도 신종금융사기와 관련해 특히 살펴볼 만한 것은 제47장 사기와 허위진술(Chapter 47 Fraud and False Statements)과 제63장 우편 사기 및 다른 사기 범죄(Chapter 63 Mail Fraud and Other Fraud Offenses)이다. 제47장의 경우, 1984년 포괄적 범죄규제법(Comprehensive

244) CISA, FEDERAL INFORMATION SECURITY MODERNIZATION ACT,
<https://www.cisa.gov/federal-information-security-modernization-act>
 (2020.12.15. 최종확인)

Crime Control Act of 1984)의 제정을 통해 컴퓨터와 네트워크에 대한 권한 없는 접근 및 이용에 대한 규정이 추가되었다. 또한, 1986년 컴퓨터 관련 범죄를 일괄적으로 규정한 컴퓨터사기 및 남용법(Computer Fraud and Abuse Act of 1986, CFAA)의 제정을 통해 컴퓨터 정보처리에 대한 범죄적 행위를 규제하는 방향으로 연방법전 제18편 제1030조 제a항의 범죄구성요건이 수정되었다. 제47장의 40개 조문 가운데 신종 보이스피싱 범죄에 적용할 수 있는 조문은 제1028조 및 제1028조A 신원절도와 제1029조 접근장치 사기, 제1030조 컴퓨터 사기가 있다. 그리고 제63장은 1872년 Postal Act를 재성문화 하는 과정에서 우편사기죄(Mail fraud)를 규율할 수 있도록 신설되었으며, 이후 몇 차례 관련 사항에 대한 제정 및 개정을 통해 현재에 이르게 되었다. 제63장에서 신종 보이스피싱 범죄에 적용할 수 있는 조문은 제1343조 통신, 라디오, 텔레비전 사기(Fraud by wire, radio, or television)이다.

가) 신원절도 및 사기죄(18 U.S.C. § 1028, § 1028A)

미연방법전 제1028조는 식별 문서, 인증 기능 및 정보와 관련된 사기 및 관련 행위(Fraud and related activity in connection with identification documents, authentication features, and information)을 규정하고 있으며, 제1028A조는 가중 신원사기(Aggravated identity theft)를 규정하고 있다. 이 두 조항을 통칭하여 신원절도 및 사기죄로 표기한다. 해당 조항들의 내용은 다음과 같다.

- 18 U.S. Code § 1028. 식별 문서, 인증 기능 및 정보와 관련된 사기 및 관련 행위
- (a) 누구든지, 본 조 (c)항에 명시된 상황에서
- (1) 고의로 정당한 권한 없이 식별 문서나 인증서, 허위의 식별 문서를 제작하거나
 - (2) 고의로 식별 문서나 인증서, 허위의 식별 문서를 그것이 절취되었거나 정당한 권한 없이 제작되었음을 알고 전송하거나
 - (3) 고의로 다섯 개 이상의 식별 문서(소지자의 사용을 위해 적법하게 발행된 경우는 제외)나 인증서, 허위의 식별 문서를 위법하게 사용하거나 전송할 목적으로 소유하거나
 - (4) 고의로 식별 문서(소지자의 사용을 위해 적법하게 발행된 경우는 제외)나 인

- 증서, 허위의 식별 문서를 미국인을 대상으로 사취하기 위한 용도로 소유하거나
- (5) 고의로 허위 식별 문서, 사용할 문서 작성 도구 또는 인증서 작성에 사용할 목적으로 문서 작성 도구 또는 인증서를 제작, 이전, 보유하거나
- (6) 고의로 식별 문서나 인증서가 절취되거나 적법한 권한 없이 작성된 것을 알면서도 미국 혹은 국가적으로 중요한 특별 이벤트로 지정된 행사의 후원 주체를 표시하는 식별 문서 또는 인증서로 보이는 식별 문서 또는 인증서를 소유하거나
- (7) 고의로 연방법에 반하거나 해당 주 혹은 지방 법률에 따라 중범죄가 성립되는 불법행위를 저지르거나 원조하거나 방조하려는 의도로 타인의 식별 수단을 적법한 권한 없이 이전, 소유 혹은 사용하거나
- (8) 고의로 허위의 식별 문서, 문서 작성 도구 또는 식별 수단에 사용하기 위해 허위 혹은 실제 인증서를 거래하는 경우
- 본 조 제(b)항에 명시된 처벌을 받게 된다.
- (b) 본 조 (a)항에 명시된 범죄에 대한 처벌은 다음과 같다.
- (1) 제3호와 제4호에 명시된 바를 제외하고, 다음과 같은 범죄에 대하여 본 조에 따른 벌금 또는 15년 이하의 징역, 혹은 벌금 및 징역형에 처한다.
- (A) 다음과 같은 식별 문서, 인증서 또는 허위의 식별 문서의 생산 또는 전달
- (i) 미국 또는 미국의 권한에 의해 발행된 신분 증명서 또는 인증서
- (ii) 출생 증명서, 운전 면허증 또는 개인 신분증
- (B) 5개 이상의 식별 문서, 인증서 또는 허위의 식별 문서의 생산 또는 전달
- (C) (a)항 제5호에 따른 위반행위 또는
- (D) (a)항 제7호에 따른 위반행위의 결과로 해당 위반행위를 한 개인이 1년 동안 1,000달러 이상의 가치를 획득하는 경우, 1개 이상의 식별 수단의 전달, 소유, 또는 사용과 관련된 본 항 제7호에 따른 위반행위
- (2) 제3호와 제4호에 명시된 바를 제외하고, 다음과 같은 범죄에 대하여 본 조에 따른 벌금 또는 5년 이하의 징역, 혹은 벌금 및 징역형에 처한다.
- (A) 식별 수단, 식별 문서, 인증서 또는 허위의 식별 문서의 기타 생산, 전달 또는 사용
- (B) (a)항의 제3호 또는 제7호에 따른 위반행위
- (3) 다음과 같은 범죄에 대하여 본 조에 따른 벌금 또는 20년 이하의 징역, 혹은 벌금 및 징역형에 처한다.
- (A) 마약 밀매 범죄를 용이하게 하는 범죄(제929조 (a)(2))
- (B) 강력 범죄와 관련된 경우(제924조 (c)(3))
- (C) 본 조에 따른 유죄판결 이후 범죄가 이루어지는 경우
- (4) 위반행위가 국내 테러 행위(제2331조 (5)) 또는 국제 테러 행위(제2331조 (1))를 용이하게 하기 위해 이루어진 경우, 해당 범죄에 대하여 본 조에 따른 벌금 또는 30년 이하의 징역, 혹은 벌금 및 징역형에 처한다.
- (5) 본 조 (a)항에 명시된 범죄의 경우, 범죄를 저지르기 위해 사용되거나 사용되

도록 의도된 모든 개인 재산은 미국에 몰수된다.

(6) 그 이외의 경우, 본 조에 따른 벌금 또는 1년 이하의 징역, 혹은 벌금 및 징역 형에 처한다.

(c) 본 조 (a)항에 명시된 상황이란

(1) 식별 문서, 인증서 또는 허위의 식별 문서는 미국의 기관 또는 국가적으로 중요한 특별 이벤트로 지정된 행사의 후원 주체가 발행한 것이며, 문서 작성 도구는 식별 문서, 인증서 또는 허위의 신분 증명서를 만들기 위해 고안되거나 적합한 것 이어야 한다.

(2) 위법행위는 본 조 (a)항 제4호에 명시된 위법행위이거나,

(3)

(A) 본 조에서 금지한 생산, 전달, 보유 또는 사용이 전자적 수단에 의한 문서 전달을 포함하여 국내 혹은 국외 상거래에 존재하거나 영향을 미치는 경우이거나

(B) 식별 수단, 식별 문서, 허위의 식별 문서 또는 문서 작성 도구가 본 조에서 금지한 생산, 전달, 보유 또는 사용의 과정에서 우편으로 전달되는 경우

(d) 본 조와 제1028A조에서

(1) 인증 표식은 해당 식별 문서, 문서 작성 도구 또는 식별 도구가 위조, 변경 또는 변조되었는지를 확인하기 위해 기관에서 사용하는 홀로그램, 워터마크, 인증, 기호, 코드, 이미지, 숫자 또는 문자 일련번호 또는 기타 방식을 의미한다.

(2) 문서 작성 도구는 식별 문서, 허위의 식별 문서 또는 그 외의 문서 작성 도구에 특별히 구성되거나 주로 사용되는 모든 도구, 표현, 템플릿, 컴퓨터 파일, 컴퓨터 디스트, 전자장치 또는 컴퓨터 하드웨어 혹은 소프트웨어를 의미한다.

(3) 식별문서란 미국 정부, 주(州), 주의 정치적 분과 국가적으로 중요한 특별 이벤트로 지정된 행사의 후원 주체, 외국 정부, 외국 정부의 정치적 분과, 국제 정부 또는 국제 준정부 기구의 권한에 의해 발행되거나 만든 특정 개인에 관한 정보가 완비되었을 때, 개인 식별을 목적으로 의도되거나 이를 일반적으로 목적으로 받아들이는 유형의 문서를 의미한다.

(4) 허위의 식별 문서란 다음과 같은 개인 식별을 목적으로 의도되거나 이를 일반적으로 목적으로 받아들이는 유형의 문서를 의미한다.

(A) 정부 기관 또는 정부 기관의 권한에 의해 발행되지 않거나 정부 기관의 권한에 따라 발행되었으나 이후 기망의 목적으로 변경된 경우

(B) 미국 정부, 주(州), 주의 정치적 분과 국가적으로 중요한 특별 이벤트로 지정된 행사의 후원 주체, 외국 정부, 외국 정부의 정치적 분과, 국제 정부 또는 국제 준정부 기구 혹은 그의 권한에 의해 발행된 것으로 보이는 경우

(5) 허위 인증 표식이란 다음과 같은 인증 표식을 의미한다.

(A) 진정한 표식이나, 발행기관의 허가 없이 기망의 목적으로 변조되었거나 변경된 것

(B) 진정한 표식이나, 발행기관의 허가 없이 그리고 합법적으로 만들어진 식별 문

서, 문서 작성 도구 또는 식별 수단과 각 발행기관에 의해 부착되거나 들어 있도록 하는 의도의 해당 인증 표식 사이의 관계없이 배포되었거나 배포를 목적으로 하는 것

(C) 진정한 표식으로 보이거나 아닌 것

(6) 발행기관이란

(A) 식별 문서, 식별 수단 또는 인증 표식을 발행할 권한을 가지는 모든 정부 주체 혹은 기관을 의미한다. 그리고

(B) 미국 정부, 주(州), 주의 정치적 분과 국가적으로 중요한 특별 이벤트로 지정된 행사의 후원 주체, 외국 정부, 외국 정부의 정치적 분과, 국제 정부 또는 국제 준정부 기구를 포함한다.

(7) 식별 수단이란 다음을 포함하는 특정 개인을 식별하기 위해 단독으로 또는 다른 정보와 함께 사용할 수 있는 이름 또는 번호를 의미한다.

(A) 이름, 사회보장번호, 생년월일, 주 또는 정부가 발급한 운전면허 또는 신분증 번호, 외국인 등록번호, 정부 여권 번호, 고용주 또는 납세자 식별 번호

(B) 지문, 성문, 각막 또는 홍채 이미지 혹은 기타 고유한 신체적 정보와 같은 고유의 생체정보

(C) 고유의 전자적 식별 번호, 주소, 또는 라우팅 코드

(D) 통신 식별 정보 또는 접근 기기(제1029(e))

(8) 개인 식별 카드란 주 또는 지방 정부 단독으로 식별 목적으로 발행한 식별 문서를 의미한다.

(9) 생산이란 용어는 변경, 인증, 집합을 포함한다.

(10) 전달은 식별 문서, 허위의 식별 문서 또는 문서 작성 도구의 선택과 다른 사람이 이용할 수 있는 온라인 위치에 해당 식별 문서, 허위의 식별 문서 또는 문서 작성 도구를 배치하거나 배치를 지시하는 것을 포함한다.

(11) 주는 미국 내의 모든 주, 워싱턴 특별 자치구, 푸에르토리코, 그 외 모든 미국 영토 및 정치적으로 세분화된 모든 구역, 부, 지역 단체 등을 의미한다.

(12) 거래(traffic)는 다음을 의미한다.

(A) 가치 있는 것에 대한 대가로서 다른 사람에게 운반, 양도 또는 처분하는 것

(B) 운송, 양도 또는 처분할 목적으로 통제하려 하거나 통제하는 것

(e) 본 조는 미연방, 주, 주의 정치적 분과 또는 정보기관의 합법적으로 허가된 조사, 보호 또는 정보 활동이나 본 절의 224장에 따른 허가된 활동을 금지하지 않는다.

(f) 시도 및 모의

본조에 따른 범죄를 저지르기 위한 시도나 모의를 한 자는 그 시

(g) 몰수 절차

재산의 압류 및 처분과 관련된 모든 사법적 또는 행정적 절차를 포함하는 이 조에 따른 재산 몰수는 1970년 포괄적 약물 남용 방지 및 관리에 따른 법률(21 U.S.C.

853) 제413조(해당 조항의 제d항 제외)의 규정에 따른다.

(h) 몰수; 처분

법원은 제a항의 위반으로 규죄판결을 받은 자가 있는 경우, 모든 불법 인증 표식, 식별 문서, 문서 작성 도구 또는 식별 도구의 몰수·파괴 또는 그 밖의 처분에 관하여 규정한 벌칙과 별도로 명령하여야 한다.

(i) 해석 규칙

본 조 제a항 제7호의 목적상, 1개 이상의 식별 수단을 포함하는 단일 식별 문서 또는 허위의 식별 문서는 1개의 식별 수단으로 해석되어야 한다.

제1028조는 제a항에서 각종 구성요건을 열거적으로 규정하고 있으며, 처벌에 관한 내용은 제b항에 별도로 두고 있다. 해당 조항 중에서 보이스피싱 범죄에 적용할 수 있는 구성요건은 제a항 제7호에서 명시하고 있는 고의로 연방법에 반하거나 해당 주 혹은 지방 법률에 따라 중범죄가 성립되는 불법행위를 저지르거나 원조하거나 방조하려는 의도로 타인의 식별 수단을 적법한 권한 없이 이전, 소유 혹은 사용하는 것이다. 제a항에서 열거하고 있는 대부분의 구성 요건들이 식별 문서나 인증서, 허위의 식별 문서의 제작이나 전송, 소유하는 행위이기 때문에 통신을 통해 피해자를 기망하는 방식으로 진행되는 보이스피싱의 경우에는 적용하기 어렵다. 그러나 제a항 제7호는 연방법에 반하거나 해당 주 혹은 지방 법률에 따라 중범죄가 성립되는 불법행위를 위해 이름이나 생년월일과 같은 타인의 식별 수단을 적법한 권한 없이 이전받거나 소유 혹은 사용하는 것을 구성요건으로 하므로, 의사소통 과정에서 타인을 기망행위로 속여 사취하기 위한 보이스피싱 범죄에 있어 충분히 일어날 수 있는 요건이므로 보이스피싱 범죄에 적용할 수 있다. 물론 그 외의 구성요건들도 신중 보이스피싱 범죄에 있어 해당 요건이 만족되는 경우에는 충분히 적용 가능하다.

이러한 제1028조의 적용을 받는 보이스피싱 범죄는 행위 유형에 따라 최대 15년의 징역형을 부과할 수 있다. 특히, 앞에서 살펴본 제a항 제7호에 해당하는 보이스피싱 범죄로 인해 그 결과로 해당 위반행위를 한 개인이 1년 동안 1,000달러 이상의 가치를 획득하는 경우, 벌금 또는 15년 이하의 징역 및 양벌규정이 병과될 수 있다. 제1028조에 해당하는 보이스피싱에 대해서는 미수나 모의에 대해서도 처벌

하고 있으며 형량은 기수범과 같다.(제f항) 또한 더 나아가 해당 범죄로 인해 취득한 재산이나 이익은 포괄적 마약남용방지 및 통제법(Comprehensive Drug Abuse Prevention and Control Act of 1970)에 따라 몰수하도록 하고 있다(제g항 및 제h항).

18 U.S. Code § 1028A. 가중 신원사기

(a) 범죄

(1) 일반조항

누구든지, 제c항에 열거된 중범죄를 위반하거나 그와 관련하여 합법적인 권한 없이 고의로 타인의 식별 수단을 이전, 소유 또는 사용하는 자는 그러한 중범죄에 규정된 처벌 이외에 2년의 징역형을 선고받는다.

(2) 테러 범죄

누구든지, 제2332b조 제g항 제5호 제B목에 열거된 중범죄 위반하거나 그와 관련하여 합법적인 권한 없이 고의로 타인의 식별 수단 또는 허위의 식별 문서를 이전, 소유 또는 사용하는 자는 그러한 중범죄에 규정된 처벌 이외에 5년의 징역형을 선고받는다.

(b) 형벌제도 - 다른 법률 조항에도 불구하고 -

(1) 법원은 본 조의 위반으로 유죄 판결을 받은 자를 집행유예하여 보호관찰하지 않는다.

(2) 제4호를 제외하고, 본 조에 따라 부과된 형기는 식별 수단의 이전, 소유 또는 사용된 중범죄에 대하여 부과된 형기를 포함하여 다른 법률 조항에 따라 부과된 형기와 동시에 실행될 수 없다.

(3) 법원은 식별 수단이 이전, 소유 또는 사용된 중범죄에 대해 부과할 형기를 결정함에 있어, 본 조항을 위반하여 부과되거나 부과될 별도의 형기를 보충·감안하여 해당 범죄에 부과될 형기를 감경하지 않도록 하여야 한다.

(4) 본 조를 위반하여 부과된 징역형은 재판부의 재량으로 전체 또는 일부에 대해 재판부가 본 조의 추가 위반에 대하여 동시에 그 자에게 동시에 부과하는 다른 징역형과 동시에 집행될 수 있으며, 그러한 재량은 제28절 제994조에 따라 연방양형위원회의 관련 지침·정책 보고서에 부합해야 한다.

(c) 정의 -본 조의 목적상, 제c항에 열거된 중범죄는 다음과 같은 중범죄를 의미한다 -

(1) 제641조(공적 자금·재산 보상 관련 범죄), 제656조(은행 임직원의 절도·횡령·유용범죄) 또는 제664조(직원의 근로자복지기금 절도범죄)

(2) 제911조(시민권 관련 허위사칭범죄)

(3) 제922조 제a항 제6호(총기취득 관련 허위진술범죄)

(4) 본 장에 포함된 모든 조항(사기 및 허위 진술 관련 범죄)

(5) 제63장에 포함된 모든 조항(우편, 은행 그리고 통신 사기 관련 범죄)

- (6) 제69장에 포함된 모든 조항(국적과 시민권 관련 범죄)
- (7) 제75장에 포함된 모든 조항(여권과 사권 관련 범죄)
- (8) Gramm-Leach-Bliley Act 제523조(15 U.S.C. 6823)(허위사칭에 의한 고객 정보 취득범죄)
- (9) 이민 및 국적법 제243조 또는 제266조(8 U.S.C. 1253 and 1306)(국외추방 이후 출국하지 않고 외국인등록증을 고의로 위조한 범죄)
- (10) 이민 및 국적법 제2절 제8장에 포함된 모든 조항(8 U.S.C. 1321 et seq.)(다양한 이민 관련 범죄)
- (11) 사회보장법 제208조, 제811조, 제1107조 제b항, 제1128조 제a항, 제1632조(42 U.S.C. 408, 1011, 1307(b), 1320a-7b(a), 1383a)(해당 법에 따른 프로그램 관련 허위진술범죄)

제1028조에 이어서 제1028조A는 가중적 신원절도 범죄를 규정하고 있다. 해당 조항은 동 조 제 c항에 명시된 중범죄 및 테러와 관련된 중범죄와 관련하여 합법적인 권한 없이 고의로 타인의 식별 수단(테러와 관련된 중범죄의 경우, 허위의 식별 문서도 포함)을 이전, 소유 또는 사용하는 자에 대하여 별도로 2년의 징역형(테러와 관련된 중범죄의 경우, 5년)을 부과한다. 해당 조항에서 언급되는 중범죄 중에는 보이스피싱 범죄에 적용될 수 있는 제1028조 등이 포함되어 있는 제47장과 제1343조 통신사기죄가 포함되어 있는 제63장의 모든 조항들이 포함되어 있어, 해당 조항을 적용하는 보이스피싱 범죄의 경우에는 가중 처벌된다는 것을 확인할 수 있다. 또한 해당 조항을 위반한 자에 대해서는 집행유예가 적용되지 않으며, 해당 조항으로 부과된 형기는 다른 법률의 위반으로 부과된 형기와 동시에 집행되지 않고, 이에 더하여 해당 조항이 적용되었다고 해서 중범죄로 인해 부과되는 형기가 감경되지도 않는다. 즉, 보이스피싱 범죄를 저지른 자에게 제1028A조를 통해 부과되는 2년의 형기는 반드시 집행되어야 하며, 보이스피싱 범죄로 인해 부과 받은 형기를 마친 이후 순차적으로 집행되고, 2년의 형기의 별도 부과가 보이스피싱 범죄로 인해 부과받는 형기에 절대 영향을 미쳐서는 안된다는 것으로 해당 조항을 통해 보이스피싱 범죄에 대해 가중처벌이 가능하다는 것을 확인할 수 있다.

나) 접근장치 사기(18 U.S.C. § 1029)

미연방법전 제1029조는 이른바 접근장치 사기(Fraud and related activity in connection with access devices)를 규정하고 있으며 United States v. Bailey, 444 U.S. 394, 404 (1976), United States v. Jewell, 532 F.2d 697, 700 n. 7 (9th Cir.), cert. denied, 426 U.S. 951 (1976)의 의도, 알고 있는 상황에 대한 판결에 근거해 입법되었다.²⁴⁵⁾ 1994년 9월 13일, 1994년 Pub. L. 103-322, § 250007, 108 Stat. 1796의 강력 범죄 통제 및 법 집행법의 일부로서 § 1029의 (a)(7)항이 추가되었다. 해당 조항을 살펴보면 다음과 같다.

18 U.S. Code § 1029. 접근장치와 관련된 사기 및 관련 행위

(a) 누구든지 다음의 행위를 한 자는 해당 범죄가 국내 혹은 국제 상거래에 영향을 미치는 경우, 본조 제c항에 명시된 바에 따라 처벌된다.

(1) 사취할 의사를 가지고 고의로 하나 이상의 위조 접근장치를 생산, 사용 또는 거래하는 경우

(2) 사취할 의사를 가지고 고의로 1년이라는 기간 동안 하나 이상의 허가받지 않은 접근장치를 거래하거나 사용하고 그러한 행위를 통해 해당 기간 동안 1,000달러 가치 이상을 얻은 경우

(3) 사취할 의사를 가지고 고의로 15개 이상의 위조 또는 허가받지 않은 접근장치를 소유하는 경우

(4) 사취할 의사를 가지고 고의로 기기 제조 장비를 생산, 판매, 통제 또는 보관 혹은 소유하는 경우

(5) 사취할 의사를 가지고 고의로 1년 동안 총 가치가 1,000달러 이상의 금액 또는 기타 가치를 받기 위해 다른 사람 혹은 사람들에게 1개 이상의 접근장치를 발급하여 거래에 영향을 미친 경우

(6) 접근장치 발행자의 허가 없이, 사취할 의사를 가지고 고의로 다음과 같은 목적을 위해 간청하는 경우

(A) 접근장치의 제공

(B) 접근장치와 관련된 정보 혹은 접근장치를 획득하기 위한 신청서의 판매

(7) 사취할 의사를 가지고 고의로 전기통신서비스의 허가받지 않은 사용을 위해 수정 또는 변경한 통신 장비의 사용, 생산, 거래, 통제, 보관 또는 소유하는 경우

(8) 사취할 의사를 가지고 고의로 스캐닝 수신기의 사용, 생산, 거래, 통제, 보관 또는 소유하는 경우

245) DOJ, FRAUDULENT PRODUCTION, USE OR TRAFFICKING/COUNTERFEIT, <https://www.justice.gov/archives/jm/criminal-resource-manual-1024-fraudulent-production-use-or-trafficking-counterfeit-or> (2020.12.15. 최종확인)

- (9) 고의로 전기통신 기기와 관련되거나 포함된 식별 정보를 허가 없이 전기통신 서비스를 얻는데 사용할 수 있도록 전기통신 기기와 관련된 정보를 삽입하거나 수정하도록 하려는 것을 알고 하드웨어 또는 소프트웨어를 사용, 생산, 거래, 통제, 보관 또는 소유하는 경우
- (10) 신용카드 시스템 직원이나 그 대리인의 허가 없이, 사취할 의사를 가지고 고의로 접근장치에 의한 거래에 관한 하나 이상의 증거 또는 기록을 직원이나 그 대리인에게 제공하도록 타인을 야기하거나 주선하는 행위
- (b)
- (1) 누구든지 본 조 제a항에 따른 범죄를 저지르기 위해 시도하는 자는 시도의 대상이 된 범죄에 대해 규정된 것과 동일한 처벌을 받아야 한다.
- (2) 당사자 중 어느 한 사람이 그러한 죄를 범하기 위해 어떤 행위에 관여하는 경우, 누구든지 본 조 제a항에 따른 범죄를 저지르기 위해 두 사람 이상의 사람들과 모의한 자는 본 조 제c항에 따라 그러한 범죄에 대해 최대 벌금형으로 언급된 금액 이하의 벌금 또는 본 조 제c항에 따라 최대 징역형으로 규정된 기간의 반에 해당하는 기간 동안의 징역형, 또는 양벌을 병과하여 부과한다.
- (c) 처벌조항
- (1) 일반조항 - 본 조 제a항에 따른 범죄에 대한 처벌은 다음과 같다.
- (A) 본 조에 따른 다른 범죄에 대한 유죄판결 이후 발생하지 않은 범죄의 경우
- (i) 제a항의 제1호, 제2호, 제3호, 제6호, 제7호 또는 제10호에 대한 범죄의 경우, 본 조에 따른 벌금 또는 10년 이하의 징역에 처하거나, 양벌을 병과하여 부과한다.
- (ii) 제a항의 제4호, 제5호, 제8호 또는 제9호에 대한 범죄의 경우, 본 조에 따른 벌금 또는 15년 이하의 징역에 처하거나, 양벌을 병과하여 부과한다.
- (B) 본 조에 따른 다른 범죄에 대한 유죄 판결 이후 발생한 범죄의 경우, 본 조에 따른 벌금 또는 20년 이하의 징역에 처하거나, 양벌을 병과하여 부과한다.
- (C) 모든 경우, 범죄를 저지르기 위해 사용되거나 사용되도록 의도된 개인 재산에 대하여 미국 정부가 몰수한다.
- (2) 몰수 절차 - 재산의 압류 및 처분과 관련된 모든 사법적 또는 행정적 절차를 포함하는 이 조에 따른 재산 몰수는 본 조의 제d항을 제외하고, 통제 물질법 제413조에 따른다. (이하 생략)

제1029조에서 언급하는 접근장치²⁴⁶⁾란 단독으로 또는 다른 접근장치와 결합하여 자금이나 재화, 서비스 등을 제공받기 위한 계정에 접속할 수 있는 카드나 판, 코드, 계정번호, 전자적 일련번호, 모바일 신원확인 번호 등을 말한다(제e항 제1~7호). 이에 따라 해당 조문들을 판단해보면 보이스피싱 범죄의 피해자에게서 기망

246) 18 U.S.C. § 1029

행위를 통해 계정에 접속할 수 있는 번호나 모바일 신원확인 번호 등의 제공을 요청하는 경우에는 제a항 제6호의 적용을 받을 수 있을 것이다. 이에 더불어 해당 행위를 통해 얻은 접근장치를 사용하여 피해자의 계좌로부터 자금을 탈취하는 행위 등을 하는 경우에는 제a항 제2호 및 제a항 제3호의 적용을 받을 수 있을 것이다. 해당 조항을 적용할 수 있는 보이스피싱 범죄를 저지른 경우에는 벌금형 혹은 10년 이하의 징역형이 부과될 수 있으며, 양벌규정을 병과할 수 있다(제c항 제1호 제A목).

이뿐만 아니라, 제a항 제7호와 제a항 제9호에서는 전기통신서비스 혹은 전기통신 기기와 관련된 행위를 규율하고 있다. 해당 조항은 사취를 목적으로 전기통신 서비스의 허가받지 않은 사용을 위해 통신 장비를 사용, 생산, 거래, 통제, 보관 또는 소유하거나(제a항 제7호), 전기통신서비스의 허가받지 않은 사용을 위해 전기통신 기기와 관련된 정보를 삽입하거나 수정하기 위한 하드웨어 또는 소프트웨어를 사용, 생산, 거래, 통제, 보관 또는 소유하는 경우(제a항 제9호)를 규제한다. 그러므로 해당 조항을 통해 보이스피싱 범죄를 위해 전화번호 변작과 같은 각종 신종 보이스피싱 범죄에 적용되는 기술적 행위를 규율할 수 있을 것이다. 해당 조항을 적용할 수 있는 보이스피싱 범죄를 저지른 경우, 벌금형 혹은 10년 이하(제a항 제7호)나 15년 이하의 징역에 처해 질 수 있으며, 양벌규정을 병과할 수 있다.

다) 컴퓨터 사기(18 U.S.C. § 1030)

미연방법전 제1030조는 컴퓨터 사기에 대한 죄책을 명시하고 있으며, Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030)로 인해 대폭 개정된 것으로 해킹규제를 주 목적으로 제정되었다. 제1030조는 총 10개 항으로 이루어져 있으며, 구성요건 내용을 규정한 제a항은 다시 7개의 유형으로 구분되어 있다. 구성요건을 명시하고 있는 제a항을 내용적으로 살펴보면 해당 조문 내에는 국가적 법익을 보호하는 규정과 개인적 법익을 보호하는 규정이 혼재되어 있음을 확인

할 수 있다. 제a항은 국가 보안 정보에 대한 첩보행위(제1호), 컴퓨터에 대한 액세스 및 정보 획득(제2호), 정부의 컴퓨터에 대한 침입(Trespass in Government Cyberspace)(제3호), 경제적 이득을 위한 컴퓨터 액세스(제4호), 고의적인 불법 접근에 의한 손상과 의도(제5호), 암호의 밀매(제6호), 컴퓨터와 관련한 기타 강탈(제7호)에 대한 것을 처벌하는 규정으로 구성되어 있다.²⁴⁷⁾ 이러한 제1030조에서 보이스포싱과 관련되어 있는 내용들을 살펴보면 다음과 같다.

18 U.S. Code § 1030. 컴퓨터와 관련된 사기 또는 관련 행위

(a) 누구든지 다음의 행위를 한 자는 본조 제c항에 명시된 바에 따라 처벌된다.
(중략)

(2) 의도적으로 허가 없이 컴퓨터에 접속하거나 허가된 접근을 초과하여 결과적으로 다음을 얻은 경우

(A) 금융기관 또는 제15절 제1602조 제n항에 정의된 카드 발급자의 재무기록에 포함된 정보 또는 공정 신용 보고 법에서 정의한 용어에 따른 소비자에 대한 소비자 관련 보고 기관의 파일에 포함된 정보(15 U.S.C. 1681 et seq.)

(B) 미국 기관 또는 부서로부터의 정보

(C) 보호받는 컴퓨터로부터의 정보
(중략)

(4) 사기의 대상과 해당 행위를 통해 획득한 가치가 오직 컴퓨터의 사용만이며, 그러한 사용의 가치가 1년 동안 5,000달러 이하인 경우가 아닌 경우에 한하여, 사취할 의사를 가지고 고의로 허가 없이 보호받는 컴퓨터에 접속하거나 허가된 접근을 초과하여 이러한 행위를 통해 의도한 사기행위를 하고, 가치를 획득한 경우
(중략)

(b) 누구든지 본 조 제a항에 따른 범죄를 저지르기 위해 시도하는 자는 제c항에 명시된 대로 처벌받아야 한다.

(c) 본 조의 제a항 또는 제b항에 따른 범죄에 대한 처벌은 다음과 같다.
(중략)

(2)

(A) 제B호에 명시된 바를 제외하고, 본 조의 제a항 제2호, 제a항 제3호, 제a항 제6호에 따른 범죄에 대하여 본 조에 따른 다른 범죄에 대한 유죄판결 또는 본 조에 따라 처벌할 수 있는 범죄에 대한 시도 후에 일어나지 않은 경우에는 본 절에 따른 벌금 혹은 1년 이하의 징역 혹은 양벌이 병과된다.

(B) 다음 호와 같이 제a항 제2호에 따른 범죄를 저지르거나 시도하는 경우에는 본 절에 따른 벌금 혹은 5년 이하의 징역 혹은 양벌이 병과된다.

247) DOJ CCIPS Criminal Division, “Prosecuting Computer Crimes”, 2017

- (i) 해당 범죄를 상업적인 이익이나 사적인 금전상의 목적으로 저지른 경우
 - (ii) 해당 범죄를 미국이나 혹은 타국가의 헌법 또는 법률을 위반하는 범죄나 고문 행위를 위해 저지른 경우
 - (iii) 얻은 정보의 가치가 5,000달러 이상인 경우
- (C) 본 조의 제a항 제2호, 제a항 제3호, 제a항 제6호에 따른 범죄에 대하여 본 조에 따른 다른 범죄에 대한 유죄판결 또는 본 조에 따라 처벌할 수 있는 범죄에 대한 시도 후에 일어난 경우에는 본 절에 따른 벌금 혹은 10년 이하의 징역 혹은 양벌이 병과된다.
- (3)
- (A) 제B호에 명시된 바를 제외하고, 본 조의 제a항 제4호, 제a항 제7호에 따른 범죄에 대하여 본 조에 따른 다른 범죄에 대한 유죄판결 또는 본 조에 따라 처벌할 수 있는 범죄에 대한 시도 후에 일어나지 않은 경우에는 본 절에 따른 벌금 혹은 5년 이하의 징역 혹은 양벌이 병과된다.
- (B) 본 조의 본 조의 제a항 제4호, 제a항 제7호에 따른 범죄에 대하여 본 조에 따른 다른 범죄에 대한 유죄판결 또는 본 조에 따라 처벌할 수 있는 범죄에 대한 시도 후에 일어난 경우에는 본 절에 따른 벌금 혹은 10년 이하의 징역 혹은 양벌이 병과된다.
- (중략)
- (d)
- (1) 미국 비밀 경호국(The United States Secret Service)은 이러한 권한을 가진 다른 기관 외에 본 조에 따른 범죄를 조사할 권한을 가진다.
- (2) 연방 수사국(The Federal Bureau of Investigation)은 본 절의 제3056조 네a항에 따라 미국 비밀 경호국의 직무에 영향을 미치는 범죄를 제외하고, 제a항 제1호에 따른 첩보, 외국 방첩, 국방 또는 대외관계의 이유로 허가받지 않은 공개로부터 보호되는 정보 또는 제한된 자료(1954년 원자력 에너지 법 제11조 제y항(42 U.S.C. 2014(y))와 관련된 모든 사건을 조사할 수 있는 일차적인 권한을 가지고 있다.
- (3) 해당 권한은 재무장관과 법무장관이 체결하는 협약에 따라 행사되어야 한다.
- (중략)
- (i)
- (1) 법원은 본 조의 위반 또는 모의로 유죄판결을 받은 자에게 형을 부과할 때, 주법의 조항과는 관계없이 부과된 다른 형벌에 추가하여 그 자가 미국 정부에 다음을 몰수되도록 명령해야 한다.
- (A) 해당 위반 행위를 저지르거나, 이를 용이하도록 하기 위해 사용되거나 사용되도록 의도된 개인 재산에 있어서 그 자의 이익
- (B) 해당 위반의 결과로 직접 또는 간접적으로 취득한 수익금, 실제 혹은 개인적인 또는 구성 혹은 파생된 모든 재산
- (2) 재산의 압류 및 처분과 관련된 모든 사법적 절차를 포함하는 이 조에 따른 재산 몰수는 1970년 포괄적 약물 남용 방지 및 관리에 따른 법률(21 U.S.C. 853)

제413조(해당 조항의 제d항 제외)의 규정에 따른다.

(j) 제i항의 목적상, 다음과 같은 사항은 미국 정부에 몰수될 수 있으며, 해당 사항에는 재산권이 인정되지 않는다.

(1) 본 조의 위반 또는 모의를 저지르거나 이를 용이하게 하기 위해 사용되거나 사용되도록 의도된 모든 개인 재산

(2) 본 조의 위반 또는 모의를 추적할 수 있는, 혹은 추적이 가능한 수익금, 실제 혹은 개인적인 재산

제1030조에서 언급하는 컴퓨터란 논리, 산술 또는 저장기능을 수행하는 전자, 자기, 광학, 전기화학 또는 그 밖의 고속 데이터 처리 장치를 의미하며, 이러한 장치와 직접 관련되거나 연계하여 작동하는 데이터 저장 시설 또는 통신 시설을 포함하나, 자동 타자기 또는 식자기 혹은 휴대용 계산기나 그 이외의 유사 장치는 포함되지 않는다.²⁴⁸⁾ 이에 따라 해당 조문들을 판단해보면 보이스피싱을 위해 허가 없이 특정한 개인의 정보를 알아내는 행동을 한 경우에는 해당 개인의 정보가 들어있는 보호받는 컴퓨터로부터의 정보를 탈취한 것으로 볼 수 있어 제a항 제2호의 적용을 받을 수 있다. 해당 조항이 적용되는 보이스피싱을 저지른 자에 대해서는 벌금형 혹은 최대 10년 이하의 징역형이 처해질 수 있고 양벌규정을 병과할 수 있다.

또한, 보이스피싱을 통해 특정한 개인에게 그의 계좌나 특정 금융 관련 정보를 알아내어 이를 기반으로 현금자동인출기나 인터넷 뱅킹을 통해 금전을 탈취한 경우에는 제a항 제4호의 적용을 받을 수 있을 것이다. 다만, 이러한 경우에 해당 조항이 적용되기 위해서는 해당 범죄를 통해 획득한 가치가 5,000달러를 초과해야만 한다. 해당 조항이 적용되는 보이스피싱을 저지른 자에 대해서는 벌금형 혹은 10년 이하의 징역형이 처해질 수 있고 양벌은 병과하여 부과될 수 있다. 그리고 이러한 제1030조에 규율되는 보이스피싱 범죄를 저지르기 위해 시도한 자는 시도한 범죄의 종류에 따라 기수범과 동일하게 처벌받게 된다. 그리고 이러한 범죄로 얻은 이익뿐만 아니라 해당 범죄에 사용되거나 사용될 의도가 있었던 재산에 대해서 몰

248) 18 U.S.C. § 1030.

수를 할 수 있도록 명하고 있다(제i조 및 제j조).

라) 통신, 라디오, 텔레비전 사기(18 U.S.C. § 1343)

통신, 라디오, 텔레비전 사기(Fraud by wire, radio, or television)를 규율하고 있는 18 U.S.C. § 1343은 같은 제63장에 규정되어 있는 우편사기죄를 규율하고 있는 18 U.S.C. § 1341을 모델로 하여 1952년에 제정된 조항으로 법문의 구조나 적용 이론 등이 매우 유사하다. 해당 조항은 다음과 같다.

18 U.S. Code § 1343. 통신, 라디오, 텔레비전 사기
 사취할 책략 또는 허위 또는 부정한 주장·표시·약속이란 수단을 통해 현금이나 재산을 취득하려는 책략을 고안하거나 고안하려 의도한 자가, 그와 같은 책략을 실행하거나 실행하려고 시도할 목적으로, 주간(州間) 또는 외국과의 상행위에서 통신, 라디오, 또는 텔레비전 통신의 수단을 통해 문서, 기호, 신호, 그림 또는 음향을 전송하거나 전송되도록 원인을 제공한 경우 벌금형에 처하거나 20년 이하의 징역형에 처하며, 두 형벌은 병과될 수 있다. 위반이 인가, 운송, 전송, 전달, 지출 또는 이와 관련하여 대통령령으로 선언되는 중대 재난이나 긴급한 상황(Robert T. Stafford 재해 구호 및 긴급 지원법(42 U.S.C. 5122) 제102조)과 관련하여 지급되는 편익에 대해 발생 혹은 관련되거나 경제 기관에 영향을 미친 경우, 그러한 자는 1,000,000달러 이하의 벌금 또는 30년 이하의 징역에 처하거나, 양벌을 병과하여 부과한다.

해당 조항은 사취할 책략 또는 허위 또는 부정한 주장·표시·약속이란 수단을 통해 현금이나 재산을 취득하려는 책략을 고안하거나 고안하려 의도한 자가 이를 실행하기 위해 통신을 사용하는 것을 규율하는 조문으로 해당 통신 수단을 통해 음향을 전송하는 것을 포함하므로 이는 보이스피싱 범죄의 수단과 맞닿아 있다고 할 수 있다. 하지만 해당 조문이 적극적으로 모든 보이스피싱 범죄에 적용되기 힘든 점은 해당 통신수단을 통해 사취할 책략 등을 실행하는 대상이 ‘주간(州間) 또는 외국과의 상행위’에서라는 점이다. 그러므로 해당 조항을 보이스피싱 범죄에 적용하기 위해서는 특정 거래행위로 보일 수 있는 상황을 연출한 상황에서 보이스피싱

범죄가 이루어져야 할 것이다. 하지만 해당 조항이 보이스피싱 범죄의 적용에 있어 특이한 점은 제1349조 시도 및 음모에서 제1343조가 있는 제63장에 있는 범죄를 시도하거나 음모를 꾸민 자에 대하여 그 범죄의 시도 또는 음모의 대상이었던 범죄에 대하여 규정된 것과 동일한 처벌을 받도록 하고 있다는 점이다. 즉, 제1343조가 적용될 수 있는 보이스피싱 범죄에 대하여 해당 범죄를 시도하거나 음모를 한 자에 대해서 해당 범죄가 기수가 되지 않고, 또한 실제로 실행하지 않더라도 처벌이 가능하다는 점이다.

3) 통신감청지원법(CALEA)

미국은 1994년 통신사업자로 하여금 법집행기관의 감청업무에 협조할 의무를 부과하는 통신감청지원법(Communications Assistance for Law Enforcement Act of 1994)²⁴⁹⁾을 제정하였다. 동법은 당시 디지털 전송기술과 무선 전송기술이 발달함에 따라 법집행기관이 사인의 통신을 감청하는 것이 점차 어려워지고 있던 현상을 반영한 것으로 통신회사가 감청에 필요한 설비를 갖추어 법집행기관이 필요한 정보를 요청하는 경우 이를 제공할 수 있도록 하는데 목적을 두고 있다.

동법의 주요 내용을 살펴보면 다음과 같다. 먼저 통신사업자는 감청 장비, 시설, 서비스 등을 갖추고 법원의 명령 또는 기타 합법적인 승인 절차에 따라 수사기관이 감청을 요청할 경우 감청을 수행하여 그 결과물을 수사기관에 전달해야 한다. 또한 수사기관이 합법적 허가를 얻어 통신사실확인자료(call identifying information)를 요청할 경우 합리적으로 취득할 수 있는 통신사실확인자료를 수사기관에 제공해야 한다.²⁵⁰⁾ 다만 정부는 전기통신사업자에게 특정 설비를 갖추도록 요구할 수는 없고 서비스의 제공이나 개인 간의 통신을 목적으로 구축된 사설 네트워크에 대해서는 이러한 의무를 부여할 수 없다.²⁵¹⁾ 또한 통신사업자는 보유하

249) 47 U.S.C. § 1001- § 1010

250) 47 U.S.C. § 1002(a)

251) 47 U.S.C. § 1002(b)

고 있는 통신설비시스템을 통해 감청할 수 있는 최대 건수 등을 일정 기간 내에 보고하여야 하며 법무부 장관은 해당 보고서를 검토한 후 감청설비를 구축하기 위해 필요한 직접 경비를 보상할 수 있다.²⁵²⁾ 나아가 통신사업자는 시스템의 보안성과 무결성을 보장하여 통신의 감청이나 통신사실확인자료에 대한 접근은 합법적 권한을 보유한 정부기관이나 직원에 의해서만 이루어지도록 해야 하며,²⁵³⁾ 전송 교환 장비의 제조업체나 통신지원서비스 제공 사업자 등은 통신사업자가 수사기관의 합법적 요청에 따른 감청을 적시에 수행할 수 있도록 협력하여야 한다.²⁵⁴⁾ 법무부 장관은 산업계를 포함한 표준단체 또는 협회, 연방, 주 및 지역 법집행기관 등과 협의하여 기술적 요구사항을 정의할 수 있으며 산업계는 주도적으로 관련 표준을 정립할 수 있다. 만약 산업계에서 자율적으로 기술적 요구사항이나 표준을 정의하지 못하는 경우 연방통신위원회(Federal Communications Commission, FCC)는 비용효율적인 방식에 의한 통신감청 협조역량 확보, 통신의 비밀 보호, 이 법에 따른 의무 준수를 위한 비용의 최소화, 신기술 및 서비스의 채택 및 제공, 감청협조를 위해 필요한 합리적인 시간과 요건 등을 고려한 기술적 요구사항, 표준 등을 포함하는 규칙을 제정할 권한을 갖는다.²⁵⁵⁾ 감청명령을 발부한 법원은 통신사업자나 설비 제조업체 등이 감청에 필요한 설비를 갖추지 않았거나 감청 내용을 제공하지 않는 경우 이를 수행하도록 명령할 수 있다.²⁵⁶⁾ 또한 법무부 장관은 통신사업자 등이 동법에 규정된 감청설비를 갖추도록 요구하는 민사소송을 제기할 수 있으며,²⁵⁷⁾ 법원은 통신사업자 또는 통신설비 제조업체에 대하여 해당 설비를 갖추도록 명령하면 특정일을 정하지 않은 이상 그 명령이 있는 날의 익일부터 매일 \$10,000의 민사제재금(Civil monetary penalty)이 부과할 수 있다.²⁵⁸⁾

252) 47 U.S.C. § 1003

253) 47 U.S.C. § 1004

254) 47 U.S.C. § 1005

255) 47 U.S.C. § 1006

256) 47 U.S.C. § 1007(a); 18 U.S.C. § 2522(a)

257) 18 U.S.C. § 2522(b)

은밀하고 조직적으로 이루어지는 보이스피싱 범죄의 수사를 위해서는 통신사업자의 협조가 필수적이라고 할 수 있다. 따라서 CALEA에서 규정하는 통신사업자의 감청설비 설치 및 협조의무는 우리 통신수사 법체계에도 필요할 수 있다. 관련하여 우리 환경에 적용할 수 있는 부분을 분석하여 전기통신사업자의 협조의무 등을 효율적이고 합리적으로 개선하는데 활용할 수 있을 것이다.

나. 조직범죄 관련 법제

조직범죄법(Racketeer Influenced and Corrupt Organizations Act:: RICO, 18 U.S.C. § 1961-1968)은 불법행위에 연관된 자들에게 형사책임과 민사책임을 부여하는 법으로 1970년에 제정되었으며, 조직범죄관리법(Organized Crime Control Act (OCCA) of 1970) 제9장에 수록되었다.²⁵⁹⁾ 해당 법률은 고도로 정교하고 다양한 활동들로 구성된 미국 내 범죄조직의 라케티어링 행위(racketeering activity)로 인하여 미국 경제의 수조 달러가 흘러나가고 있고, 범죄조직이 도박, 사채업, 절도와 장물, 마약류의 수입과 유통 기타 라케티어링 행위로 취득한 금전을 통하여 권력을 얻고 있으며, 이러한 금전과 권력이 합법적인 기업과 노동조합에 침투하여 이들을 부패시키고 민주주의적 절차를 전복시키고 부패시키고 있고, 이러한 조직범죄행위로 말미암아 국가적 경제의 안정성을 약화시키고 선량한 투자자와 경쟁조직들을 위협함으로써 내수 경제의 안정을 위협하고 국가와 시민의 안녕을 약화시키고 있는데, 증거 수집의 어려움으로 인하여 조직범죄가 더욱 더 기승을 부리고 있는 현실을 타개하기 위한 목적으로 조직범죄법을 제정하였다. 이러한 조직범죄법은 마피아와 같은 조직범죄집단을 규제하고자 제정되었으나 점차, 공무원들의 뇌물 수수, 기업이 불법적으로 경제적 이익을 취득한 행위 등 광범위한 화이트칼라 범죄에 관하여 규제하게 되었다. 이러한 조직범죄법은 제1961조에서 정의,

258) 18 U.S.C. § 2522(c)

259) Pub. L. No. 91-452, 84 Stat. 922, 941, (1970)

제1962조에서 금지되는 행위를 규정하고 있으며, 제1963조에서 형사처벌을 규정하고 있고, 제1964조에서는 민사 구제책을 규정하고 있다. 이러한 조직범죄법의 조문은 다음과 같다.

18 U.S. Code § 1961. 정의

본 장에서의

(1) 라케티어링 행위는

(A) 살인, 납치, 도박, 방화, 강도, 뇌물 수수, 부당취득, 음란물을 다루거나 규제물질 또는 규제물질법 제102조에서 정의하고 있는 열거된 화학

물질을 다루는 행위 또는 이러한 행위가 포함된 협박행위를 의미하는 것으로써 주법에 따라 1년 이상의 금고형에 처해질 수 있는 행위를 의미하며,

(B) 연방범죄가 열거된 연방형법(U.S. Code 제18장)의 다음 조항 중 하나에 따라 기소할 수 있는 모든 행위: 뇌물수수관련조항(18 U.S.C. § 201), 스포츠뇌물수수 관련조항 (18 U.S.C. § 224), 위조 관련 조항 (18 U.S.C. § 471, 472, 473), 만약 기소된 행위가 제659조에 따라 중범죄인 경우에 내수무역의 절도관련 행위 (18 U.S.C. § 659), 연금복지펀드의 횡령과 관련된 행위(18 U.S.C. § 664), 신용거래의 부당취득에 관한 행위(18 U.S.C. § 891-894), 신원위조서류와 관련된 사기행위 등에 관한 행위(18 U.S.C. § 1028), 기기 접근과 관련된 사기행위(18 U.S.C. § 1029), 도박정보송출과 관련된 행위(18 U.S.C. § 1084), 우편사기 관련 행위(18 U.S.C. § 1341), 전선사기관련 행위(18 U.S.C. § 1343), 금융기관사기관련 행위(18 U.S.C. § 1344), 외국노동계약사기관련 행위(18 U.S.C. § 1351), 불법국적취득관련 행위(18 U.S.C. § 1452), 음란물관련행위(18 U.S.C. § 1461-1465), 재판방해관련 행위(18 U.S.C. § 1503), 형사조사방해행위(18 U.S.C. § 1510), 주 또는 지역 법집행방해관련 행위(18 U.S.C. § 1511), 증인, 피해자 또는 정보원 부정매수행위(18 U.S.C. § 1512), 증인, 피해자 또는 정보원에게 보복행위(18 U.S.C. § 1513), 여권 사용과 신청 부정행위(18 U.S.C. § 1543), 여권의 부정사용과 위조 관련 행위(18 U.S.C. § 1543), 여권의 남용행위(18 U.S.C. § 1544), 비자, 허가증 기타 서류의 남용과 사기관련 행위(18 U.S.C. § 1546), 인신매매관련 행위(18 U.S.C. § 1581-1592), 강도 또는 부당취득을 통한 상업방해(18 U.S.C. § 1951), 라케티어링과 관련된 행위(18 U.S.C. § 1952), 도박용품 등의 내수간의 운송관련 행위(18 U.S.C. § 1953), 불법 복지펀드 결제와 관련된 행위(18 U.S.C. § 1954), 불법 도박

사업관련 행위(18 U.S.C. § 1955), 금전 불법세탁관련 행위(18 U.S.C. § 1956), 특정불법행위로 인하여 취득한 부동산의 금전거래에 연루된 행위(18 U.S.C. § 1956), 청탁살인과 관련하여 내수경제시설을 사용과 관련된 행위(18 U.S.C. § 1958), 금전의 불법송금행위(18 U.S.C.A. § 1960), 아동성적착취관련 행위(18 U.S.C. § 2251, 2251A, 2252, 2260), 도난된 자동차를 이용하여 내수 간 운송관련 행위(18 U.S.C. § 2312, 2313), 도난된 물품의 내간 운송관련 행위(18 U.S.C. § 2314, 2315), 포르노기록, 컴퓨터 프로그램 또는 컴퓨터프로그램 서류 또는 패키지 및 동영상 사본 또는 기타 시청각 자료의 표지위반관련 행위(18 U.S.C. § 2318), 형사적인 상표권침해행위(18 U.S.C. § 2319), 허가 없이 라이브 뮤지컬 등의 동영상 또는 사운드 녹음 관련 밀거래 행위(18 U.S.C. § 2319A), 위조된 상표로 상품 또는 서비스의 밀거래 행위(18 U.S.C. § 2320), 특정 자동차 또는 자동차 부품을 밀거래 행위(18 U.S.C. § 2321), 밀수된 담배의 밀거래 행위(18 U.S.C. § 2341-2346), 노예밀거래관련 행위(18 U.S.C. § 2421-24), 생화학적 무기 관련 행위(18 U.S.C. § 175-178), 화학 무기 관련 행위(18 U.S.C. § 229-229F), 핵물질 관련 행위(18 U.S.C. § 831)

(C) U.S. Code 제29장의 노동조합의 대출과 지불제한을 다루는 행위(29 U.S.C.A. § 186) 또는 조합편드의 횡령과 관련된 행위(29 U.S.C.A. § 501(c))에 따라 기소할 수 있는 모든 행위

(D) 파산사기와 관련된 사기(본 장 제157조에 따른 경우를 제외하고), 유가증권 판매사기, 중범죄에 해당하는 제조, 수입, 장물, 은닉, 구매, 판매 또는 기타 규제 물질이나 열거된 화학물질(통제 물질법 제102조)을 다루는 경우, 기타 미국 법에 따라 처벌 가능한 범죄 행위와 연관된 모든 범죄 행위

(E) 외국화폐거래보고법에 따라 기소할 수 있는 행위

(F) 국적과 이민법에 따라 기소할 수 있는 행위, 특정 외국인 은닉과 밀항관련 (§ 274), 특정 외국인 밀항 방조관련 (§ 277) 또는 불법적인 목적으로 외국인 밀수 행위 (§ 278)와 같이 이러한 법률 규정에 따라 기소할 수 있는 행위가 금전적 이익을 얻기 위한 목적으로 행해진 행위

(G) 2332(g)(5)(B)에 열거된 범죄행위

(2) 주는 미국 내의 모든 주, 워싱턴 특별 자치구, 푸에르토리코, 그 외 모든 미국 영토 및 정치적으로 세분화된 모든 구역, 부, 지역 단체 등을 의미한다.

(3) 사람은 재산에 대한 법적 또는 유익한 지분을 보유할 수 있는 개인 또는 개체를 포함한다.

(4) 단체는 개인, 파트너십, 기업, 조합 기타 법인과 조합, 또는 법인이 아니더라도

도 사실상의 단체(association-in-fact) 등을 의미한다.

(5) 라케티어링 행위의 패턴은 최소한 두개 이상의 라케티어링 행위와 하나의 라케티어링 행위가 이전의 라케티어링 행위를 저지른 후로부터 10년 이내의 기간(수감 기간 제외)에 일어나는 것을 요구한다.

(6) 불법적인 채권은

(A) 미연방, 주, 또는 정치적 분파의 법률에 위배되는 도박 행위로 일어나거나 계약된 채권이면서

(B) 이는 미연방, 주, 또는 정치적 분파의 법률에 위반되는 도박 사업 또는 주 또는 연방법에 따라 불법적인 요율로 금전이나 물건을 빌려주는 사업과 관련하여 발생한 채권을 의미하며, 여기서의 불법적인 요율은 최소 집행 가능한 금액의 2배 이상을 의미한다.

(7) 라케티어링 조서관은 법무장관이 지명하고 이 장의 실행 또는 시행의 의무가 부과되는 모든 변호사 또는 조서관을 의미한다.

(8) 라케티어링 조사는 본 장 또는 미국 법원의 최종 명령, 판결 또는 결정을 위반한 자가 있는지를 확인하기 위해 본 장에 따라 발생하는 모든 경우와 과정에 있어 적절하게 라케티어링 조서관이 시행하는 조사를 의미한다.

(9) 문서는 모든 책, 보고서, 문서, 기록, 기록물, 또는 기타 물질을 포함한다.

(10) 법무장관은 미연방 법무장관, 미연방 법무차관, 미연방 법무부 차관보, 미연방 법무부의 직원 또는 법무장관이 본 장에 의해 법무장관에게 부여된 권한을 수행하기 위해 지정한 미국 연방의 모든 부서 또는 기관의 직원을 포함한다. 지정된 모든 부서 또는 기관은 본 장의 조사 규정 또는 해당 부서 혹은 기관이 달리 법률로 부여한 수사 권한을 본 장에서 승인한 조사에 사용할 수 있다.

18 U.S. Code § 1962. 금지행위

(a) 이익을 획득하기 위하여 또는 관련된 단체의 설립, 운영 또는 내수 경제 또는 외국과의 경제활동에 영향을 주는 행위로서 라케티어링 행위의 패턴(pattern of racketeering activity) 또는 U.S. Code title 18 section 2의 의미 내의 자로써 불법적인 채권추심을 통하여(collection of an unlawful debt) 소득을 얻은 자가 이러한 소득 또는 소득의 수익금을 투자 또는 사용하는 행위에 직접 또는 간접적으로 참여하는 것은 위법하다. 구매자, 직계 가족의 구성원, 그리고 그 또는 그들의 공범자들이 해당 구매 이후 라케티어링 행위의 패턴이나 불법적인 채권추심에 대해 보유하고 있는 발행자의 유가증권이 총액으로 1개 등급의 미결 유가증권의 1 퍼센트에 달하지 않으며, 법률상 또는 사실상 한명 이상의 발행자의 이사를 선출

할 수 있는 권한을 부여하지 않는다면, 발행자의 유가증권투자의 목적으로, 그리고 발행자의 조정의 통제 또는 참여하거나 다른 사람이 그렇게 하도록 도울 의도 없이, 공개된 시장에서의 유가증권을 매입하는 것은 해당 조항에 따른 위법한 행위가 아니다.

(b) 라케티어링 행위의 패턴 또는 단체의 이익 또는 통제권을 획득 또는 유지하기 위하여 직접적 또는 간접적으로 행하여진 불법채권추심행위가 내수경제 또는 외국과의 경제에 영향을 주는 행위는 금지된다.

(c) 단체에 고용되었거나 또는 관련된 자가 내수 경제 또는 외국과의 경제에 영향을 주는 행위로서 라케티어링 행위의 패턴 또는 불법채권추심을 통하여 단체의 업무에 직접 또는 간접적으로 행위 또는 참여하는 것은 금지된다.

(d) 본 조 제a항, 제b항, 제c항의 위반규정을 모의하는 행위는 금지된다.

18 U.S. Code § 1963. 형사처벌

(a) 본 장의 제1962조를 위반한 자는 누구든지 본 장에 따른 벌금 또는 20년 이하의 징역(또는 최대 형량이 무기징역을 포함하는 라케티어링 행위에 기초한 위반인 경우에는 무기징역) 또는 벌금 및 징역형을 부과하고, 주범의 모든 조항과 관계없이 미국 연방에 다음이 몰수된다.

(1) 동법 제1962조 위반으로 취득 또는 유지한 이익

(2) 동법 제1962조 위반으로 설립, 운영, 통제, 실행, 참가한 단체가 얻은 모든

(A) 이익

(B) 유가증권

(C) 권리

(D) 영향력의 근원인 모든 종류의 재산 또는 계약상 권리

(3) 동법 제1962조 위반인 라케티어링 행위 또는 불법적인 채권추심으로 직접적 또는 간접적으로 얻은 획득한 수익금 또는 이로 인한 재산

법원은 이러한 자에게 형량을 부과함에 있어 본 조에 따라 부과된 다른 형법 이외에 본 조에 기술된 모든 재산을 미국 연방에 몰수할 것을 명령해야 한다. 본 조에서 달리 허가한 벌금 대신, 범죄로부터 이익 또는 기타 수익을 얻은 자에게는 총 이익 또는 기타 수익의 2배 이하의 벌금을 부과할 수 있다.

(b) 본 조에 따른 형사적 몰수의 대상이 되는 재산은 다음을 포함한다.

(1) 부동산과 해당 부동산에서 자란 작물, 부속물, 발견물

(2) 권리, 특허, 이익, 유가증권을 포함한 개인소유의 유형, 무형의 재산

(c) 제a항에 기술된 재산에 대한 모든 권리, 소유권 및 이익은 본 조항에 따른

몰수 조항의 명령에 따라 미국 연방에 귀속된다. 피고가 아닌 자에게 양도되는 재산은 특별 몰수 판결의 대상이 될 수 있으며, 양수인이 제1항에 따른 심리에서 구입 당시 해당 재산이 본조에 따른 몰수의 대상이라고 믿을만한 이유가 전혀 없는 해당 재산의 가치에 대한 선의의 구매자임을 입증하지 않는 한, 미 연방에 몰수된다.

(이하 생략)

18 U.S. Code § 1964. 민사적 구제

(a) 미국의 지방법원은 다음을 포함하되 이에 국한되지 않은 적절한 명령을 내려 본 장 제1962조의 위반을 방지하고 제지할 수 있는 관할권을 가진다: 모든 단체에 있어 직접적이든 간접적이든 모든 이익을 박탈하도록 명령하는 것; 단체의 활동과 동일한 유형의 노력에 참여하는 것을 금지하고, 그 활동이 국내 또는 국외 상거래에 영향을 미치는 것을 포함하되 이에 국한되지 않은 개인의 미래 활동 또는 투자에 대해 합리적인 제한을 가하는 것; 모든 단체의 해산 또는 조직 개편을 명령하고 무고한 사람들의 권리에 대한 적절한 조항을 제정하는 것

(b) 법무장관은 본 조에 따라 절차를 시행할 수 있다. 법원은 최종결정을 내릴 때까지 언제든지 금지 명령을 내리거나 이행보증서의 수용을 포함한 기타 조치를 취할 수 있다.

(c) 본 장 제1962조의 위반으로 자신의 사업 또는 재산에 손해를 입은 자는 적절한 미국 지방법원에 소송을 제기할 수 있으며, 그가 입은 손해의 3배와 합리적인 변호사 비용을 포함한 소송비용을 배상받을 수 있다. 단, 제1962조의 위반을 성립시키기 위해 유가증권의 구입 또는 판매에 있어 사기로 행동할 수 있는 행위를 한 자는 제외한다. 사기 사건과 관련하여 형사적으로 유죄판결을 받은 사람에 대한 소송에 있어서는 앞의 문장에 포함된 예외조항이 적용되지 않으며, 이 경우 유죄 판결이 확정되는 날짜에 공소시효가 개시된다.

(d) 본 장에 따라 미국 정부가 제기한 모든 형사소송에서 미국 정부에게 유리한 최종 판결 또는 결정은 미국 정부가 제기한 후속 민사 소송에서 피고가 형사 범죄의 본질적인 혐의를 부인하는 것을 금지한다.

조직범죄법 제1962조는 이익을 획득하기 위하여 또는 관련된 단체의 설립, 운영 또는 내수 경제 또는 외국과의 경제활동에 영향을 주는 행위로서 라케티어링 행위의 패턴 또는 불법적인 채권추심을 통하여 소득을 얻은 자가 이러한 소득 또는 소득의 수익금을 투자 또는 사용하는 행위에 직접 또는 간접적으로 참여하는 것을 금지하고 있으며, 라케티어링 행위의 패턴 또는 단체의 이익 또는 통제권을 획득 또는 유지하기 위하여 직접적 또는 간접적으로 행하여진 불법채권추심행위가 내수경제 또는 외국과의 경제에 영향을 주는 행위를 금지하고, 단체에 고용되었거나 또는 관련된 자가 내수 경제 또는 외국과의 경제에 영향을 주는 행위로서 라케티어링 행위의 패턴 또는 불법채권추심을 통하여 단체의 업무에 직접 또는 간접적으로 행위 또는 참여하는 것을 금지하고, 이러한 세 가지의 금지 행위를 모의하는 행위 역시 금지하고 있다. 이러한 조직범죄법 제1962조의 구성요건을 만족시키기 위해서는 라케티어링 행위가 있어야 하며, 라케티어링 행위의 패턴이 존재해야 하고, 단체와 관련되어 있으야 하며, 라케티어링 활동이 내수와 외국과의 경제행위에 영향을 주는 것이어야 한다. 해당 구성요건 행위를 보이스피싱과 관련하여 자세히 살펴보면 다음과 같다.

금지되는 라케티어링 행위란 특정범죄의 행위 또는 위협을 구성하는 행위로 이에 대하여 제1961조 제1호에서 규정하고 있다. 이러한 라케티어링 행위를 구성하고 있는 다양한 주범 및 연방 형법에 기술된 범죄행위 중 보이스피싱 범죄에 적용되는 미연방법전 제1028조 신원절도 및 사기죄와 제1029조 접근장치 사기죄, 그리고 제1343조 통신사기죄가 명시되어 있다. 그러므로 미연방형법 제1028조, 제1029조, 제1343조에 의해 처벌할 수 있는 신종 보이스피싱 범죄의 경우에는 당연히 해당 법의 적용 대상이 될 수 있다. 또한 제1961조 제5호에 의하면 라케티어링 행위의 패턴이 형성되기 위해서는 최소한 두 개 이상의 라케티어링 행위가 이전의 라케티어링 행위를 저지른 후로부터 10년 이내의 기간에 일어나야 한다. 즉, 조직범죄법 제1961조 제5호에서 언급하는 범죄활동의 패턴은 최소한 두 개 이상의 범죄행위가 필요하고, 이러한 범죄행위는 해당 조직범죄법의 효력이 발생된 1970년 10

월 15일 이후에 발생되어야 하며, 첫 범죄행위가 행해진 이후로 1년 이내에 다른 행위가 행해졌어야 할 것을 요구하고 있다.²⁶⁰⁾ 이러한 범죄행위는 단순히 다수의 범죄행위가 행해졌다는 것을 넘어(계속성), 가해자가 조직화된 범죄에 포함되어 있거나 기능적으로 동일하게 행한 경우에만 패턴을 형성하였다고 인정되며 각 범죄활동들 간에 관련성이 있어야 하고 해당 단체와도 관련이 있어야 인정된다.(관련성)²⁶¹⁾ 조직적인 보이스피싱 범죄 활동에 있어 조직 내에서 각자가 맡은 행위를 분담하여 사기 범죄를 벌이므로 동일한 보이스피싱 범죄 행위가 계속성과 관련성을 만족시켜 패턴을 이루고 있다고 보아도 무방하다.

그리고 조직범죄법에서 인정되는 라케티어링 행위는 단체 혹은 단체와 어떠한 방식으로든 연관되어 있는 개인이 한 활동이어야 하며, 여기서 언급되는 단체는 제1961조 제4호에서 언급하는 개인, 파트너십, 기업, 조합 기타 법인과 조합, 또는 법인이 아니더라도 사실상의 단체(association-in-fact) 등을 의미한다. 이러한 단체는 공동의 목적을 위해 일련의 행위를 하고자 현재의 목적을 지닌 개인들이 함께 결합된 실체이며, 여기서 언급되는 단체는 합법적인 단체와 불법적인 단체를 모두 포함한다.²⁶²⁾ 이 역시 보이스피싱 범죄를 위해 조직된 단체의 경우, 일부 범죄에 대한 의도 없이 특정 행위를 위해 모집된 자를 제외하고 보이스피싱 범죄라는 공동의 목적을 위해 일련의 행위를 하고자 하는 개인들이 모인 불법적인 단체로 보아 조직범죄법에서 언급하고 있는 단체에 해당한다고 할 수 있다.

조직범죄법에서 언급하는 라케티어링 활동은 내수와 외국과의 경제 행위에 영향을 주는 것이어야 하는데, 현재 이에 관련하여 미국 판례는 열거된 범죄행위가 내수경제에 최소한으로 영향을 주는 경우에는 장래의 영향력의 입증으로 입증하면 된다고 명시하고 있다.²⁶³⁾ 이는 조직범죄법에 해당하는 단체가 그 활동으로 인

260) HJ Inc. v. Northwestern Bell Telephone Company, 492 U.S. 229. (1989)

261) United States v. Louis Daidone, 471F. 3d 371. (2006)

262) United States v. Turkette, 452 U.S. 576. (1981)

263) Richard L. Bourgeois, Jr./S. P. Hennessey/Jon Moore/Michael E. Tschupp, "Racketeer Influenced and Corrupt Organizations", American Criminal

해 내수 경제에 영향을 미치며, 해당 단체와 내수경제 간의 최소한의 관련성만 입증하면 된다. 그러므로 이를 보이스피싱 범죄에 적용하면 보이스피싱 범죄를 위해 조직되고 활동하고 있는 단체는 보이스피싱을 통해 금전적 피해를 피해자들에게 주기에 내수경제와 연결되어 있고, 또한 보이스피싱 범죄를 통해 얻은 범죄수익은 자금세탁 행위를 통해 해외로 빠져나가는데 이는 국내의 자금이 해외로 반출되는 경우로 보아 역시 내수경제와 연결되어 있다고 볼 수 있다. 따라서 이러한 구성요건들을 만족함을 볼 때 보이스피싱도 조직범죄법의 규제 대상이라고 볼 수 있다.

이렇게 보이스피싱 범죄가 조직범죄법의 규제 대상임에 따라 조직범죄법 제 1962조 제d항에 따라 보이스피싱 범죄의 모의행위도 처벌의 대상이 된다. 또한 해당 법에 반하여 보이스피싱 범죄를 저지른 자는 제1963조에 따라 벌금 및 20년 이하의 징역형을 선고받을 수 있으며, 국가는 피고가 조직범죄법 범죄를 행함으로 인하여 취득한 이익, 조직범죄법 위반을 통해 설립하거나 운영한 단체가 얻은 이익, 그리고 조직범죄법을 위반함으로써 습득한 금전에 대해 몰수할 수 있다. 또한 보이스피싱에 대한 조직범죄법 상의 민사 구제책으로는 제1964조에 따라 라케티어링 행위로 야기된 손해에 대하여 피해자가 3배 손해배상을 청구할 수 있다.

다. 자금세탁에 관한 법제

1) 개요

미국은 자금세탁 방지를 위한 법체계를 크게 두 가지 측면에서 구성하고 있다. 하나는 자금세탁을 범죄화하여 통제하기 위한 법률로서 자금세탁규제법(Money Laundering Control Act, 18 U.S.C. § 1956, § 1957)이며, 다른 하나는 금융기관에 대한 통제장치를 마련함으로써 자금세탁을 예방하려는 은행비밀보호법(The Currency and Foreign Transaction Reporting Act, 31 U.S.C.)이다. 한편 2001년

9.11 테러사건을 계기로 제정된 USA PATRIOT 법을 통해 자금세탁 규제를 강화하는 방향으로 은행비밀법 개정이 이루어졌다.²⁶⁴⁾

2) 은행비밀보호법

은행비밀보호법은 통화와 해외거래를 보고하도록 한 법률로 1970년 제정되었다. 제202조에 따르면 통화와 해외거래 보고규정의 목적은 범죄나 조세, 또는 일반적인 수사나 소송에서 특히 활용할 만한 보고나 기록이 존재하는 경우 그러한 보고나 기록을 요구하도록 하기 위함이라고 한다. 은행비밀보호법은 조직범죄와 화이트칼라 범죄, 마약범죄, 탈세, 부정부패 등을 규제하기 위해 자금원의 출처와 규모, 이동 등을 확인하기 위해 제정된 법률이라고 할 수 있다.

본 법률에 따르면 금융기관에는 두 가지 의무가 부과된다. 우선 금융기관은 재무 장관이 범죄나 조세, 기타 규제와 관련해 필요하다고 결정한 거래자의 이름, 수표나 기타 증서의 사본, 수취인의 이름 등을 5년간 보존해야 한다. 또한 10,000 달러 이상의 자금이 이체되거나 신용제공된 경우 금융기관은 이에 대한 기록을 보관하고 15일 이내에 국세청에 보고해야 한다. 특히 이 두 번째 의무를 이행하지 않을 경우에는 이나 벌금형을 부과할 수 있다.

은행비밀법은 1992년 Annunzio-Wylie 자금세탁방지법(The Annunzio-Wylie Anti-Money Laundering Act of 1992)과 1994년 자금세탁억제법(The Money Laundering Suppression Act of 1994)에 의해 개정되었는데, 이로써 자금세탁을 관할하는 재무부(장관)의 권한이 강해지고, 혐의거래보고절차의 간소화 등 자금세탁 통제기능이 강화되었다.

3) 자금세탁규제법

264) 이진국, 이윤제, 박정수, “미국 FinCEN의 자금세탁 방지제도 운영실태 연구”, 금융위원회 연구보고서, 2008, 4면

자금세탁규제법은 자금세탁을 범죄화하고 은행비밀법상 현금거래보고의무를 강화하기 위해 1986년 도입되었다. 본 법률은 우선 “통화수단세탁(Laundering of monetary instruments)”을 규정하고 있다. 그에 따르면 “특정 불법활동(specified unlawful activity)으로부터 생긴 수익임을 알면서 그와 관련한 금융거래를 하거나 행하려고 시도한 자는 ① 특정 불법활동의 실행을 조장할 의도가 있거나, ② 거래의 전부 또는 일부가 (i) 특정 불법활동으로부터 얻은 수익의 성질이나 장소, 출처, 소유, 운영을 은폐하거나 위장하기 위한 것이라거나 (ii) 주나 연방의 법률에 의한 거래보고의무를 회피하기 위한 것이라는 점을 알고 있었을 때” 20년 이하의 이나 50만 달러 또는 관련자금의 2배액 중 다액 이하의 벌금형에 처하도록 하고 있으며, 모두 부과할 수도 있다. “특정 불법활동”에 대해서는 제1956조 제a항 제7호에 열거적으로 규정하고 있다. 여기에는 이른바 RICO법이 규정하고 있는 위법 행위도 포함되는데,²⁶⁵⁾ RICO법 제1961조 제1호 제A목은 1년 이상의 을 부과할 수 있는 모든 행위를 중대범죄(racketeering activity)로 포섭하고 있기 때문에, 자금세탁의 전제범죄 범위는 매우 넓어지게 된다. 요컨대 수익이 발생할 수 있는 대부분의 범죄가 자금세탁의 전제범죄에 포함한다고 볼 수 있다. 한편 본 법률은 국제적 자금세탁도 규율하고 있는데, (B)의 요건에서 해당 자금이나 펀드가 특정 불법활동에 기인한 것임을 알았을 것을 추가적으로 요한다는 점을 제외하고는 제1956조 제a항 제1호의 국내 자금세탁과 동일하다.

본 법률은 자금세탁행위를 처벌하기 위한 수사당국의 입증책임을 일정 부분에서 상당히 완화하였다. 즉 10,000 달러를 넘는 범죄적 자금거래행위에 대해서는 단지 그 자금이 특정 불법활동에 근거한 것임을 알고 있었다는 점을 입증할 필요가 없다. 그 밖에 고액현금거래 신고의무를 회피하기 위해 10,000 달러 이하로 분할하여 금융거래를 하는 행위(Structuring transactions)도 처벌하도록 하고 있다.

265) 이진국, 이윤제, 박정수, “미국 FinCEN의 자금세탁 방지제도 운영실태 연구”, 금융위원회 연구보고서, 2008, 4-5면

4) USA PATRIOT법

2001년 9.11 테러 이후 미국 의회는 테러와의 전쟁을 위해 국가기관에게 보다 강력한 법적 권한을 부여하기 위한 작업에 착수하였다. 그 결과 제정된 것이 USA PATRIOT 법이다. 이 법률 제3장에서는 자금세탁에 대한 강력한 규제를 그 내용으로 담고 있다. 즉 자금세탁과 테러자금 조달을 억제하기 위해 미국금융시스템을 이용하는 외국은행과 단체, 개인에게 매우 높은 수준의 주의의무와 기록보존 및 보고의무를 부과하고 있다. 또한 이를 위해 은행비밀법과 자금세탁규제법을 개정하기에 이르렀다.

자금세탁 규제강화를 위한 USA PATRIOT 법의 주요 내용을 살펴보면, 우선 외국은행과 거래하는 미국은행에 대해 주의의무를 강화하였다. 이를 위해 재무부 장관은 금융기관에게 기록보존을 요구하고, 미국 관할 밖에서 자금세탁의 우려가 있는 국제거래와 관련해 금융기관에 특정거래의 기록유지와 보고, 미국은행 내 특정 계좌의 외국인수익자 신원확인 등의 특별조치를 취할 수 있게 되었다. 미국인이 아닌 자를 위한 은행간 외환거래계좌나 사설은행계좌에 대한 정밀조사를 요구할 수 있게 되었으며, 외국의 위장은행(shell bank)과 외환거래 계좌를 개설하는 것을 금지하였다. 그 밖에 연방사법당국과 금융기관으로 하여금 자금세탁방지를 위한 정보를 공유하도록 하였으며, 집중계좌(concentration accounts)를 이용한 국제적 거액송금이 익명으로 이루어지는 것을 방지하기 위해 재무부 장관에게 집중계좌 관리에 관한 규제발동권을 부여하였다. 금융기관에게는 자금세탁방지 프로그램(anti-money laundering program)을 작성하도록 규정하였고, 미국의 금융범죄 단속 네트워크(FinCEN)를 재무부 조직으로 구성하여 자금세탁분석과 함께 테러자금분석도 수행할 수 있도록 하였다.

라. 범죄피해 환급 관련 법제

1) 신원사기 집행, 원상복구법

미국의회는 2008년에 신원사기 집행·원상복구법(Identity Theft Enforcement and Restitution Act)을 입법화하였다. 이에 따라 새로운 조항으로 ‘미국연방법전 제18편 제3663조의 (b)(6)’이 추가되었다. 조항은 피싱사기 피해자를 피싱사기가 발생한 이전의 원상태로 완전히 복구할 수 있도록 하는 실질적인 근거 규정이 되었다.²⁶⁶⁾

이 조항에 따라 법원은 피싱사기 피해자가 입은 예정된 또는 실제의 피해를 개선하기 위해 ‘합리적으로 사용한 시간의 금전적 가치’를 부담하도록 피싱 사기 범에게 명할 수 있게 되었다. 피싱사기로 인해 무고한 피해자가 입은 직접적인 피해액뿐만 아니라 기타 개인적 신용의 원상복구비용 등과 같은 간접적인 피해의 금전적인 배상이 가능하도록 한 것이다. 간접적인 피해의 손해배상액에 대한 구체적인 증거를 제시하지 못하는 경우에도 피싱사기 피해자가 당해 피싱사기로 인해 입은 것으로 예상되는 합리적인 피해액을 시간의 가치로 환산하여 주장하고 법원이 이를 인정하게 되면, 피해자는 이 금액을 원상복구금액의 명목으로 피싱 사기범에게서 지급받을 수 있다.

2) 경제성장 규제완화 및 소비자 보호법

도널드 트럼프 대통령은 2018년 5월 경제 성장, 규제 완화 및 소비자 보호법(Economic Growth, Regulatory Relief, and Consumer Protection Act, 2018)에 서명하였다. Dodd-Frank Act에 대한 미국 은행 규제의 완화가 주요 골자이나 사이버 환경에서 피싱 등의 소비자 피해에 대한 보호조항을 포함하고 있다.²⁶⁷⁾ 이 조

266) 최창수, “미국의 온라인 피싱사기방지법과 시사점”, 법조협회, 法曹 63(10), 2014, 121-164면

항으로 피싱사기가 의심되는 정황이 있는 금융소비자들이 자신들의 신용을 동결시킬 수 있도록 허용한다. 금융소비자는 소비자 신용정보기관에 서면으로 요청함으로써 자신의 신용정보에 대해 보안 동결을 할 수 있다. 즉, ‘보안 동결(security freeze)’은 소비자의 요청에 따라 본인의 신용 정보에 접근하는 것을 중단함으로써 채권자나 금융회사에서 신용정보를 획득하거나 이를 통해 신규 계좌를 개설하는 것을 막게 된다. 이렇게 되면 보안 동결을 요청한 소비자의 신용정보는 본인의 사전 허가 없이 제3자에게 공개되지 않으며 다시 신용거래의 재개를 신청하면 정상적인 신용, 서비스 사용을 위해 개인 식별번호로 해당 보안동결 조치를 일시적으로 해제하도록 허용하고 있다.

267) Public Law No: 115-174, (2018)

제2절 독일의 대응체계 및 법제

1. 범죄 동향

독일에서는 보이스피싱 범죄에 대해 voice phishing, 혹은 해당 언어의 줄임말인 vishing, 혹은 VOIP-phishing, Call Center-Betrug, call scamming, Betrug mit der Telefon 등으로 매우 다양하게 언급하고 있다. 이러한 독일 내의 보이스피싱 범죄에 대해서 명확하게 확인된 통계는 없으나, 독일 연방범죄수사국에 의하면 보이스피싱 사건을 포함하여 독일 형법 제 263조a를 적용하는 컴퓨터사용사기사건은 2017년 473건, 2018년 644건으로 36.2%가 증가하였다고 한다.²⁶⁸⁾ 독일 연방범죄수사국 홈페이지에서 전형적인 보이스피싱 범죄인 '콜센터 사기'를 관할 범죄로 명시하고 있는 등, 독일 내에서 보이스피싱 범죄는 독일 사회 내에서 꽤 비중있는 범죄로 자리잡고 있다. 이러한 독일 내의 보이스피싱 범죄에 대한 독일의 대응 기관 및 관련 법제, 그리고 대응 정책에 대하여 확인하고자 한다.

2. 대응 체계

가. 연방내무부(Bundesministerium des Innern, für Bau und Heimat, BMI)

1) 개괄

연방내무부는 독일 내 안보를 담당하는 주관부처로 주요기반보호, 정보통신기반보호 및 각종 IT 사이버 정보보안 정책 등을 입안하고 결정하는 역할을 수행한다. 그러므로 이러한 연방 내무부는 재난 발생 시 일어날 수 있는 각종 물리적 피해를 포함한 각종 피해로부터 국민들을 보호하는 역할을 한다. 그러므로 해당 기관은 기반보호, 범죄 예방 및 대책, 테러 방지 등과 같이 국가 내부 안전의 보장이

268) Bundeskriminalamts, "Cybercrime Bundeslagebild", 2018

라는 목표를 달성할 수 있는 광범위한 업무 범위를 가진다.²⁶⁹⁾

연방내무부의 구성은 크게 내각과 의회 담당 및 국제 담당 비서진, 언론 보도 대변인, 편집 사무실 등으로 이루어진 장관실과 총 15개의 부처로 구성되어 있으며, 각 부처들은 다음과 같다.²⁷⁰⁾

〈표 6-3〉 독일 연방내무부 기관 구성

부서명	부서 설명
Z 부서	연방내무부 내 예산 및 조직 관리 등 전반적인 관리업무를 수행하는 중심 부처
EU 부서	연방내무부 내의 유럽연합 관련 정책의 개발, 형성 및 조정을 담당하는 부처
ÖS 부서	경찰 업무, 연방 범죄 등을 포함한 공공 안전 분야 업무를 수행하는 부처
B 부서	연방경찰의 활동에 대하여 다면적으로 협조하고 조정하는 업무를 수행하는 부처
M 부서	이민, 통합, 난민, 유럽의 조화 등에 대한 연방정부의 정책과 관련된 업무를 수행하는 부처
KM 부서	각 연방기관들의 국가적 위기관리에 관련한 업무와 시민 보호 및 연방차원에서의 재난 관리 업무를 수행하는 부처
V 부서	헌법, 행정법, EU법, 국제법과 관련된 의무, 초안 작성 및 입안 등과 관련된 업무를 수행하는 부처
D 부서	공공 서비스 및 공공 서비스 직원 고용과 관련된 법적 기반에 대한 업무를 수행하는 부처
DG 부서	효과성, 대응성, 효율성, 투명성의 요건을 충족할 수 있도록 하는 공공 행정의 디지털 전환과 현대화를 추진하는 부처
DG 부서	OZG 과제를 통합하고 관리 조직 및 현대화에 관한 주제를 보완하는 부

269) 한국인터넷진흥원 보고서, “미국, 영국 독일 기반보호법 체계에 관한 연구”, 2010, 226-234면

270) BMI,

<https://www.bmi.bund.de/DE/ministerium/das-bmi/abteilungen-und-aufgaben/abteilungen-und-aufgaben-node.html> (2020.12.10.최종확인)

	서. 2020년 6월 1일 신설 됨
CI 부서	국민, 기업, 정부의 사이버 및 정보 보안을 위한 정책 개발, 기술 개발 감독 및 입법 등과 관련된 업무를 수행하는 부처
H 부서	독일 전역의 도시와 농촌의 사회적 응집력을 강화하고 동등한 생활여건을 조성할 수 있도록 지역사회 건설 등과 관련된 업무를 수행하는 부처
SP 부서	우수한 스포츠의 증진에 대한 국가 차원의 정책과 스포츠 정의와 관련된 업무를 수행하는 부처
G 부서	독일 국내 정책 모든 분야에 관한 정책 기획과 전략적 소통과 관련된 업무를 수행하는 부처
SW 부서	도시개발과 주택개발에 관한 업무를 수행하는 부처. 2020년 현재, 연방환경부에서 연방내무부로 업무 이관 중에 있음
BW 부서	독일 및 유럽 차원에서 건축 및 건설 분야의 경제적, 법적, 기술적 측면 업무를 수행하는 부처. 2020년 현재, 연방환경부에서 연방내무부로 업무 이관 중에 있음

2) 보이스피싱 관련 부서

광범위한 업무 영역을 지니고 있는 독일의 연방내무부에서 보이스피싱 범죄와 관련된 업무를 담당하고 있는 부서는 CI 부처이다. CI 부서는 IT 보안 부서로, 해당 부서는 정부와 비즈니스 등 많은 작업들이 IT에 의존하고 있으며, 독일인의 4분의 3이 인터넷을 사용함과 동시에 점차 생활이 디지털화되어 가고 있는 환경에서 일어날 수 있는 사이버 범죄로 인한 위협을 줄이기 위하여 만들어졌다. 당해 부서는 BSI(Federal Office for Information Security) 및 각종 기관들과 협력하여 적절한 IT 보안을 제공하는 것을 목표로 한다. 당해 부서를 위시한 연방 내무부의 사이버 보안과 관련된 정책의 방향성은 2016년 11월 9일에 채택된 '독일 사이버 보안 전략 2016'에 명시되어 있다. 그리고 해당 전략에는 사이버공간 내 보안을 강화하기 위한 30가지 이상의 전략 목표와 조치가 포함되어 있다.²⁷¹⁾

271) BMI, Cyber-Sicherheitsstrategie für Deutschland,

나. 연방정보기술보안청(Bundesamt für Sicherheit in der Informationstechnik, BSI)

1) 개괄

연방정보기술보안청은 1991년 설립되었으며, 독일의 IT 보안의 개선을 목표로 하는 기관이다. 이러한 목표를 위해 정보기술 적용 시의 보안 위험을 조사하고, 구체적인 보안대책을 개발한다. BSI는 정보기술과 그 사용에 따른 위험에 대하여 정보를 제공하고 구체적인 문제의 해결을 지원한다. 이는 여러 업체들과의 협력을 기반으로 하는 IT 시스템을 개발과 해당 시스템에 대한 보안의 심사 및 평가로 나눌 수 있다. BSI는 위험을 최소화하거나 완전히 배제하기 위해 정보기술의 제조자, 운영자 및 사용자에게 정보를 제공하고 정보기술의 발전과 동향을 분석한다. 또한 이미 독일 연방정부의 컴퓨터긴급대응팀(CERT-Bund)에서 새로운 취약점 및 위험에 대한 광범위한 정보를 제공하는 것과 별개로 BSI 포털에서는 민간 IT 이용자들에게 정보 및 자문 서비스를 제공한다.²⁷²⁾²⁷³⁾ 이러한 BSI의 업무와 관련하여 BSI 법(BSI Act) 제 3조에서 다음과 같이 나열하고 있다.²⁷⁴⁾

- 연방 정보 기술 보안에 대한 위협 방지
- 보안 위험 및 보안 유의사항에 대한 정보를 수집 및 분석하고, 해당 결과를

<https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html>
(2020.12.15. 최종확인)

272) 한국인터넷진흥원 보고서, “미국, 영국 독일 기반보호법 체계에 관한 연구”, 2010, 240면

273) BSI, Functions,
https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.html
(2020.12.15. 최종확인)

274) Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) § 3 Aufgaben des Bundesamtes

업무 목적을 달성하기 위해 필요한 기관이나 보안 이익을 보존하기 위해 필요한 제 3자에게 제공

- 연방에서 법률적으로 위임된 작업의 일부로서 연구를 포함하여 직무를 수행하는 데 필요한 경우, 정보기술 사용과 관련된 보안 위협의 연구와 특히 정보 기술 보안을 위한 정보 기술 프로세스 및 장치를 포함한 보안 유의사항의 개발
- 정보 기술 시스템 또는 구성 요소의 보안을 테스트 및 평가하고 IT 보안 표준 준수를 테스트 및 평가하는 기준, 절차, 도구 개발
- 정보 기술 시스템 또는 구성요소의 보안 시험 및 평가, 보안 인증서 발급
- 정보 기술 시스템 및 구성 요소 테스트 및 연방 사무국의 기술 지침에 정의된 IT 보안 표준 준수 확인
- 연방지역 또는 연방계약의 맥락에서 기업이 연방보안관리확인법(SWG) 제4조에 따라 공무상 비밀정보를 처리하거나 송수신하는 데 사용할 정보기술 시스템이나 구성요소의 시험, 평가, 승인
- 당국의 요청에 따라 공식 기밀 또는 기타 영역에서 기밀을 보호하기 위해 사용되는 연방 정보 보안 시스템을 위한 핵심 데이터 생산 및 암호 및 보안 관리 시스템 운영
- 조직 및 기술 보안 조치에 대한 지원 및 자문 제공 및 보안관리 확인법 제4조에 따라 기밀 공무 정보를 보호하기 위한 기술 시험 수행
- 연방 정보 기술 및 보호가 특별히 필요한 정보 기술 계약자의 적합성을 위한 기술 보안 표준 개발
- 연방 기관이 IT 보안 제품을 사용할 수 있도록 설정
- 특히 이들 기구가 자문 또는 감독 업무를 수행하는 경우, 정보 기술의 보안을 책임지는 연방 기구에 대한 지원 제공. 이에 대하여 연방정보보호청 정보보호청장에 대한 지원이 우선되어야 하며, 연방청장이 직무를 수행할 때 자치권한에 따라 제공되어야 한다.
- 다음과 같은 지원은 정보기술의 보안에 반하는 활동이나 정보기술을 이용하

여 실시하는 활동을 예방하거나 조사하기 위하여 필요한 경우에 한하여 지원할 수 있다. 연방 사무소는 지원 요청의 기록을 보관해야 한다.

- a) 법적으로 위임된 업무를 수행하는 경찰과 검찰 당국에 대한 지원 제공,
- b) 헌법 및 군사정보국의 검찰 당국은 연방 및 주법과 군사정보보호법에 의해 승인된 테러활동 또는 정보활동으로부터 도출된 정보의 분석 및 평가에 대한 지원 제공
- c) 법적으로 위임된 업무를 수행하는 연방정보국에 대한 지원 제공
 - Länder 관할 기구의 요청에 따라, 정보기술의 보안에 대한 위협의 예방과 관련하여 이들 기구를 지원 및 Länder 관할 기구의 요청에 따라, 정보기술의 보안에 대한 위협의 예방과 관련하여 이들 기관을 지원
 - 보안 주의사항의 결여 또는 불충분한 보안 주의사항의 잠재적 결과를 유념하고, 이러한 정보 기술의 귀중함에 관한 생산자, 유통자 및 사용자뿐만 아니라 연방 및 Länder 기관 및 Länder 기관에게 조언 및 경고한다.
 - 초기 단계의 위기를 인식하고, 대응 및 관리하며, 민간 산업과 비협조적인 중요 인프라의 정보 기술 보안을 보호하기 위한 노력을 조정하기 위한 적절한 통신 구조 구축
 - 타 기관의 특수한 역량에 대한 편견 없이, 외국 경쟁 기관과의 협력에 관한 정보 기술 보안의 중심 기관으로서의 업무
 - 중요 인프라 및 디지털 서비스의 정보 기술 보안을 위한 중심 기관으로서 제 8a절부터 제 8c절까지에 따른 업무
 - 제 5a절에 따른 정보 기술 시스템의 보안 또는 기능 회복에 대한 지원 제공

이러한 BSI의 구성은 기관장 및 기관장 산하 관리 부서 3개와 그 외의 8개 부서로 이루어져 있으며, 각 부서들은 다음과 같다.²⁷⁵⁾

275) BSI, Aufgaben,

https://www.bsi.bund.de/DE/DasBSI/Aufgaben/aufgaben_node.html (2020.12.15.)

〈표 6-4〉 독일 BSI 부서 구성

부서명	부서 설명
BL 부서	연방, 주 및 지방 정부에 IT 보안과 관련된 자문을 제공하고, 정보 보호와 관련된 법률 검토와 연방 통합 데이터 센터 및 네트워크의 보안과 관련된 업무를 수행하는 부서
DI 부서	안전한 전자 신원 솔루션에 대한 기술적 구현 및 사이버 연방 정부의 디지털화 프로젝트 내에서 보안 관련 업무를 담당하는 부서
KM 부서	전자식 분류 정보(VS) 및 IT 보안 시스템의 승인 및 제공과 암호화, VS 및 IT 보안 시스템의 사양과 개발 및 테스트 등의 업무를 수행하는 부서
OC 부서	취약점 발견과 같은 보안 관련 이벤트들을 신속하고 안정적으로 감지하고, 이러한 이벤트가 개인 및 조직에 영향을 미치는 경우 적절한 대처를 할 수 있도록 하는 부서
SZ 부서	IT 보안 서비스 제공 업체의 인증 원칙 설정, 표준화 활동 및 인증 절차의 기술적 구현 등의 업무를 수행하는 부서
TK 부서	정보 보안의 맥락에서 다가오는 기술 변화를 조기에 감지하고 디지털화된 환경에서 보안을 보장할 수 있는 적절한 솔루션의 개발 업무를 수행하는 부서
WG 부서	중요 인프라와 경제 사회 내 인프라에 대한 보안을 목적으로 관련 협력과 홍보 등 다양한 업무를 수행하는 부서
Z 부서	BSI 내 예산 및 조직 관리 등 전반적인 관리업무를 수행하는 중심부처

2) 포이스피싱 관련 부서

정보 보안과 관련된 다양한 업무를 하고 있는 연방정보기술보안청 내 부서 중에서 보이스 피싱 범죄와 관련된 부서는 OC 부서와 BL 부서, WG 부서이다. 이 세 부서들은 각기 담당하고 있는 업무가 다르며, 그로 인하여 보이스 피싱 범죄를 대하는 방향에 차이가 존재한다. 우선 OC 부서는 기본적으로 사이버 보안과 관련된 이벤트를 탐지하고 이에 대한 대응을 담당하는 부서이다. 그러므로 OC부서는 보이스 피싱 범죄와 관련하여 각종 취약점에 대한 탐지나 혹은 정보 탈취 사건 등이

최종확인)

발생한 경우의 대응 등, 직간접적인 방식으로 보이스 피싱 범죄 사건에 대하여 대응하는 역할을 맡게 된다.²⁷⁶⁾ 그에 반하여 BL 부서는 기본적으로는 정보 보안과 관련하여 연방, 주 및 지방 정부에 자문 등을 제공하는 업무를 주로 하고 있으나, 사이버 보안과 관련하여 국제 관계 업무도 함께 맡고 있다. 따라서 BL부서는 해외에서 범죄가 이루어지는 보이스 피싱 범죄와 관련된 업무도 관할한다고 판단할 수 있다.²⁷⁷⁾ 이 외에도 WG 부서는 중요 인프라와 관련된 보안 업무와 함께 경제 사회 내 인프라에 대한 전반적인 사이버 보안과 관련된 업무도 담당하고 있으며, 이러한 업무에는 시민들에 대한 사이버 보안 및 홍보의 업무가 포함되어 있어 보이스 피싱 범죄와 관련된 보안 수칙 등의 홍보 업무를 관할한다고 판단할 수 있다.²⁷⁸⁾

다. 연방범죄수사국(Bundeskriminalamts, BKA)

1) 개괄

독일 내의 범죄의 수사와 소추는 원칙적으로는 각 주의 경찰에게 관할권이 있다. 하지만 국제범죄 및 중범죄에 대해서는 연방범죄수사국이 관할권을 가진다. 이는 해당 범죄 자체가 각 주의 경계를 넘어 전 독일에 걸쳐 이루어지거나 더 나아가 범죄의 행위가 국제적으로 분산되어 이루어져 개별 주만을 관할로 하는 주

276) BSI, Abteilung OC - Operative Cyber-Sicherheit,
https://www.bsi.bund.de/DE/DasBSI/Aufgaben/AbteilungOC/AbteilungOC_node.html (2020.12.15. 최종확인)

277) BSI, Abteilung WG - Cyber-Sicherheit für Wirtschaft und Gesellschaft,
https://www.bsi.bund.de/DE/DasBSI/Aufgaben/AbteilungWG/AbteilungWG_node.html (2020.12.15. 최종확인)

278) BSI, Abteilung WG - Cyber-Sicherheit für Wirtschaft und Gesellschaft,
https://www.bsi.bund.de/DE/DasBSI/Aufgaben/AbteilungWG/AbteilungWG_node.html (2020.12.15. 최종확인)

경찰의 수사 역량으로는 면밀한 수사가 어렵기 때문이다.²⁷⁹⁾ 이러한 연방범죄수사국이 관할권을 가진다고 명시하고 있는 범죄 영역은 크게 4가지로, 다음과 같다.

- 국제적으로 조직화되어 이루어지는 무기, 탄약, 폭발물, 마약, 의약품 등의 불법거래
- 국제적으로 조직화되어 이루어지는 위조지폐의 제작 및 유포, 자금세탁 등과 관련된 범죄 행위
- 국제적으로 조직되는 테러
- 간첩 활동 및 불법 기술 이전과 같이 컴퓨터 업무 방해 등의 중대한 사례

이러한 연방범죄수사국은 청장과 부청장 이하, 다음과 같이 11개 부서로 이루어져 있다.²⁸⁰⁾

279) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 한국형사정책연구원, 형사정책연구원 연구총서, 2016, 253-270면.

280) BKA, Fachabteilungen,
https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/fachabteilungen_node.html (2020.12.15. 최종확인)

〈표 6-5〉 독일 연방범죄수사국의 부서 체계

부서명	부서 설명
ST 부서	정치적 동기 범죄
TE 부서	이슬람 동기 테러 및 극단주의 범죄
SO 부서	중범죄 및 조직범죄
CC 부서	사이버 범죄
SG 부서	연방 헌법 기관 및 해외 순방 귀빈 안전 및 보호 업무 담당 부서
ZI 부서	범죄 및 식별 정보와 관련된 중앙 정보 관리 및 검색 관련 업무 담당 부서
OE 부서	운영, 배포 및 조사 지원 업무 담당 부서
IZ 부서	국제 조정, 교육 및 연구 센터 업무 담당 부서
KT 부서	법의학 연구소
IT 부서	경찰과 BKA의 정보 교환을 위한 정보 기술 업무 담당 부서
ZV 부서	BKA 내 중앙 행정 관리 부서

2) 보이스피싱 관련 부서

연방범죄수사국 내에서 보이스피싱 범죄와 관련된 부서는 CC부서와 SO부서, KT부서로 총 3곳이다. CC 부서는 좁은 의미의 사이버 범죄를 대상으로 하는 부서로, 여기서 언급하는 좁은 의미의 사이버 범죄란 인터넷, 데이터 네트워크, 정보 기술 시스템 또는 그 데이터에 대한 범죄를 의미한다. 이러한 사이버 범죄는 1990년 중반까지 OA부서의 업무 중 하나였으며, 이후 그 비중이 증가함에 따라 SO부서에서 담당하게 되었다. 하지만 사이버 범죄의 특성상 관련 IT 전문가 등의 인원이 필요하고 점차 증가함에 따라 IT 부서에 사이버 범죄 관련 그룹이 생기게 되었다. 그 이후, 사이버 범죄의 범행이 다양해지고 그 수도 증가함에 따라 국제 공조 등의 필요성이 증가하여 이를 관장할 새로운 부서의 필요성을 절감하게 되었다. 이에 따라 연방내무부는 연방범죄수사국 내에 사이버 범죄를 전담하는 부서를 만

들 것을 명령하였으며, 2020년 4월 1일부터 사이버 범죄를 전담하는 CC 부서가 신설되었다. 이러한 CC 부서에서는 사이버 공간에서 활동 중인 범죄자에 대한 조사를 수행하고, 매우 복잡한 사이버 기술 분야의 조사를 위해 관련 정보의 수집, 처리 및 분석을 하며, 좁은 의미의 사이버 범죄와 관련된 범죄 정책 문제에 대해 연방 형사 경찰국에 조언을 하는 등의 업무를 진행한다. 이러한 CC 부서의 업무 내용에는 피싱, 사회 공학을 통한 데이터 도난 등이 포함되어 있어, 보이스피싱 범죄에 대한 수사 등을 진행하는 부서로 볼 수 있다.²⁸¹⁾

또한 사이버 범죄를 다루는 CC 부서와 별개로 중범죄 및 조직 범죄를 다루는 SO 부서는 아동 포르노 유포, 아동 및 청소년을 대상으로 하는 성적 학대, 무기와 마약, 위조화폐의 불법 거래 등을 대상으로 하고 있다. 해당 부서는 범죄 행위 결과 취득한 불법 재산을 추적하고 몰수하는 것도 업무로 하고 있으며, 이 외에도 마피아와 같은 고전적 조직범죄와 일상생활 영역에서 발생하는 조직적 범죄도 관할하고 있다. 그리고 이러한 일상생활 영역에서 발생하는 조직적 범죄 중 하나가 바로 노인들을 대상으로 하는 '콜센터 사기'²⁸²⁾로, 이는 전화를 이용한 사기 범죄로써 전형적인 보이스피싱에 해당한다.²⁸³⁾

이렇게 직접적으로 사이버 범죄를 다루는 CC부서나 일부 보이스피싱에 대해 다루고 있는 SO부서와는 별개로 KT부서는 보이스피싱과 관련된 증거를 확보하고

281) BSI, Ab- teilung "Cyber- crime" (CC),
https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/cybercrime_node.html (2020.12.15. 최종확인)

282) BSI, Be- trü- ge- ri- sche Gewinn- versprechen am Telefon,
https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/BetruegerischeGewinnversprechen/betruegerischegewinnversprechen_node.html (2020.12.15. 최종확인)

283) BSI, Ab- teilung "Schwe- re und Organi- sierte Krimi- nalität" (SO),
https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/SchwereOrganisierteKriminalitaet/schwereorganisiertekriminalitaet_node.html (2020.12.15. 최종확인)

조사 및 평가하는 부서로 존재하고 있다. KT부서는 거의 모든 법의학 조사 영역에 걸쳐 광범위하고 학제 간으로 분산되어 구성되어 있다. 이러한 KT부서는 크게 사례 관련 업무, 연구 및 개발, 법의학 수집 및 정보 시스템의 유지 관리, 국내 및 국제 교육 및 조안에 대한 업무를 맡고 있다. 이러한 KT부서는 보이스피싱과 관련된 디지털 증거들에 대한 포렌식 업무를 맡고 있다는 점에서 보이스피싱과 직접적으로 관련이 있는 부서라고 할 수 있다.²⁸⁴⁾

라. 관세청 내 금융거래조사부(Finanztransaktionsuntersuchungen, FIU)

중앙 금융거래 조사국은 연방재무부 산하 관세청 내에 존재하는 기관으로 자금 세탁 또는 테러 자금 조달과 관련하여 의심스러운 금융거래에 대한 보고서를 접수, 수집 및 평가하는 기관이다. FIU는 자금세탁법 제2조에 따라 의무 당사자가 보낸 의심스러운 활동 보고서에 대한 분석을 수행하고, 분석 결과에 따라 범죄의 징후가 있는 경우에는 검찰청을 포함한 관련 법집행기관과 세금 관련 기관 등에 이를 이관한다. 이뿐만 아니라 자금세탁 방법을 식별하고, 이러한 과정을 통해 얻은 지식을 자금세탁 및 테러 자금 조달을 방지하기 위해 관련 의무 당사자, 협력 기관 등에 제공한다. FIU는 표적 분석을 통해 자금세탁 및 테러 자금 조달을 미연에 방지하려 한다. 따라서 FIU는 이를 위해 감독 당국과 정기적으로 연락하고 금융 및 비재무 부문에서 자금세탁 회의를 조직하며, 국내 및 국제 실무 그룹 회의에 참여하여 연례 활동 보고서를 게시한다. 이러한 자금세탁 및 테러 자금 조달 방지를 위해 다양한 역할을 하는 FIU는 2017년 6월 26일부터 관세형사청의 일반 관세국 내에 있으며, 독립적인 결정 권한이 존재한다.²⁸⁵⁾

284) BSI, Ab- tei- lung “Kri- mi- nal- tech- ni- sches Institut“ (KT),
https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/KriminaltechnischesInstitut/kriminaltechnischesinstitut_node.html (2020.12.15.
 최종확인)

285) ZOLL,

3. 대응 법률

독일 법제에서 보이스피싱 범죄에 대해서 해당 범죄 행위 과정에서 행한 정보의 탈취와 같이 보이스피싱 범죄를 위한 수단으로서의 행위와 보이스피싱 범죄의 결과인 금융 사기에 대하여 별도로 구분하여 판단하고 있다. 그리고 이러한 판단에 있어서 기준이 되는 법은 형법이다. 2006년 9월 20일, 독일 연방법무부에서는 기존의 형법으로 보이스피싱을 포함한 피싱 범죄가 충분히 판단될 수 있다고 보았다. 따라서 다음은 보이스피싱 범죄에 대해서 실질적으로 적용을 하고 있거나, 혹은 적용을 할 수 있는 법률이다.

가. 범죄단체조직과 관련된 죄

독일 형법 제 129조와 제 129조의 b는 범죄단체조직죄에 대하여 규정하고 있다. 해당 규정의 내용은 다음과 같다.

제 129조 범죄단체조직

- ① 범죄를 그 목적이나 활동의 대상으로 하는 단체를 조직한 자, 그 단체에 구성원으로 가입한 자, 그 단체를 위한 구성원이나 후원자를 모집한 자 또는 그 단체를 원조한 자는 5년 이하의 자유형 또는 벌금형에 처한다.
- ② 제1항은 다음 각호의 1에 해당하는 경우 이를 적용하지 아니한다.
 1. 제1항의 단체가 연방헌법재판소에 의하여 위헌으로 선언된 정당이 아닌 경우
 2. 범죄의 수행이 그 단체의 목적이나 활동 중 종속적 의미에 불과한 경우
 3. 단체의 목적이나 활동이 제84조 내지 제87조의 범죄와 관련이 있는 경우
- ③ 제1항의 단체조직행위의 미수는 처벌한다.
- ④ 행위자가 제1항의 단체의 수괴나 배후조정자인 경우 또는 기타 특히 중한 경우에는 6월 이상 5년 이하의 자유형에 처한다. 범죄단체의 목적이나 활동이 형사소송법 제100조c 제2항 제1호 a, b, c, d, e와 제239조a나 제239조 b의 범죄행위

https://www.zoll.de/DE/Der-Zoll/Struktur/Generalzolldirektion/Zentralstelle-FIU/zentralstelle-fiu_node.html (2020.10.13. 최종확인)

를 제외한 g, h 내지 m, 제2호 내지 제5호, 제7호에서 제시된 범죄행위인 경우에는 6월 이상 10년 이하의 자유형에 처한다.

⑤ 법원은 그 책임이 경미하고 가담정도가 종속적 의미에 불과한 단순 관여자에 대하여 제1항 및 제3항의 형을 면제할 수 있다.

⑥ 법원은 다음 각호의 1에 해당하는 경우에는 동조에 의한 형을 작량하여 감경(제49조 제2항)하거나 면제할 수 있다.

1. 행위자가 자의로 단체의 존속 또는 그 목적에 속하는 범죄의 실행을 방지하기 위하여 진지하게 노력한 경우

2. 행위자가 자의로 계획을 알고 있는 그 범행이 제지될 수 있을 만큼 적시에 자신이 알고 있는 사실을 관청에 진술한 경우

행위자가 단체의 존속을 저지하기 위한 목적을 달성하였거나 그의 관여 없이도 그러한 목적이 실현된 경우에는 처벌하지 아니한다.

제 129조b 외국에서의 범죄단체와 테러단체, 확장적 박탈과 몰수

① 제 129조와 제 129조a의 규정은 외국에서의 단체에 대해서도 적용된다. 범죄행위가 유럽연합 소속국 이외의 단체와 관련된 경우라면 이는 이 법의 장소적 적용범위 내에서 실현된 활동을 통하여 범해지거나 행위자나 피해자가 독일인이거나 독일 내에 있는 경우에 한하여 적용된다. 제2문의 행위는 독일연방 법무부의 수권이 있는 경우에만 형사소추된다. 수권은 개별적 행위를 위해서 또는 일반적으로 특정한 단체와 관련된 장래의 행위에 대한 소추를 위해서도 부여될 수 있다. 수권에 대하여 결정할 경우 법무부는 '단체의 목적이 인간존엄을 존중하는 국가질서의 근본가치나 국민의 평화로운 공존에 배치되는지' 그리고 '모든 상황을 비교할 때 비난가능하게 보여지는지'를 고려하여야 한다.

② 제129조 및 제129조a의 경우 및 각각 제1항과 관련하여서도 제73조d 및 제74조a를 준용한다.

해당 범죄는 우리나라 형법 제 114조인 범죄단체 등의 조직죄와 동일한 맥락을 가진 법으로 공공질서의 평온이라는 사회적 법익을 해친 자에 대하여 처벌하는 조항들이다. 보이스피싱은 연방범죄수사국의 수사 맥락이나 실제 보이스피싱 범죄의 실현 과정에 의하면 사이버 범죄이기도 하지만, 그와 동시에 조직범죄이기도 하다. 제129조에서는 범죄단체조직의 대상이 되지 않는 경우만을 한정하고 있을 뿐, 범죄단체조직의 대상이 되는 범죄에 대해서 명시적으로 특정하고 있지 않으

며, 보이스피싱은 범죄단체조직의 대상이 되지 않는 범죄에 대하여 언급하고 있는 독일 형법 제 129조 2항 3호의 위헌정당유지죄나 군사적 사보티지 목적의 스파이 활동죄와 내용적으로 다르다. 그러므로 자신이 보이스피싱 범죄와 관련된 각종 범죄 행위를 목적으로 하거나 활동의 대상으로 하는 단체를 조직하거나, 가입, 원조하는 것을 알면서도 이를 행한 자의 경우에는 제 129조에 의한 처벌이 가능하다. 또한 보이스피싱 범죄 단체가 독일 및 유럽연합 이외의 국가에 근거지를 두고 있는 경우에도 해당 단체의 보이스피싱 행위로 인해 독일인에게 피해를 준다면 해당 단체를 조직, 가입 및 원조한 자에 대하여 제 129조b 1항에 의해 제 129조를 적용할 수 있게 된다.

이러한 제129조는 해당 범죄의 구성요건에 해당하는 자에 대하여 별도의 형을 부여하는 형식이기에 동일한 행위에 대하여 타법의 적용을 받는 경우에는 상상적 경합의 대상이 되어 더 중한 죄의 형으로 처벌받게 되며, 단순 가담자와 일반 가담자 및 범죄단체의 수괴나 배후조정자 사이에 형의 차별을 두고 있어 더 중한 범죄를 저지른 자에게 더 중한 형을 가하도록 하는 가중 처벌을 가능하도록 되어 있다. 뿐만 아니라 미수범 처벌 조항이 존재하여 보이스피싱 범죄와 관련하여 범죄단체조직의 미수가 발생한 경우에도 처벌이 가능하다. 그리고 제 129조b의 제 2항은 위법행위를 위한 또는 그로 인한 물건을 박탈하도록 하는 제73조d(확장적 박탈)와 중과실로 범죄의 대상이 되거나 부당한 방법으로 취득한 물건에 대하여 해당 물건을 몰수하도록 하는 제74조a(몰수의 확장적 조건)를 준용한다. 그러므로 이를 통해 제 129조와 제 129조b에 해당하는 범죄조직에 대한 박탈과 몰수를 이행할 수 있다. 이는 보이스피싱 범죄 조직이 얻은 불법수익을 박탈 및 몰수할 수 있도록 하는 조항으로 적용할 수 있다.

나. 정보탐지의 죄

독일 형법 제 202조a에서는 정보탐지죄에 대하여 규정하고 있다. 해당 죄의 보호법익은 정보의 정신적 내용에 대한 개인의 권리로부터 파생한 형식적 처분권한으로, 개인적 법익에 해당한다. 해당 규정의 내용은 다음과 같다.

제202조a 정보탐지(Ausspähen von Daten)

- ① 접근차단장치를 해제하여 자신에게 알려지지 않았으며 부정한 접근으로부터 특별히 보호되고 있는 정보에 권한 없이 접근하거나 제3자로 하여금 접근하도록 한 자는 3년 이하의 자유형 또는 벌금형에 처한다.
- ② 제1항의 정보는 오로지 전기적으로, 자기적으로 또는 기타 직접 인식할 수 없도록 저장되거나 전송되는 정보만을 의미한다.

해당 규정에서 정보(Daten)란 “알려지거나 위임된 협약에 근거하여 신호나 지속적인 기능을 통해 표현되는 것으로서 처리를 목적으로 코드화되거나 정보처리 결과로 나타난 정보(Information)”를 의미한다. 따라서 이메일주소, 인터넷뱅킹을 위한 접근정보를 비롯해 오늘날 대부분 전자적으로 기록되고 보관되는 모든 유형의 개인정보와 금융정보는 네트워크를 통한 커뮤니케이션, 신원확인, 업무 등을 위해 코드화된 것이기 때문에 본 규정의 정보개념에 포섭된다.²⁸⁶⁾ 이러한 정보는 직접 인식할 수 없는 형태로 저장되거나 전송되는 것이어야 한다. 그러므로 이메일주소나 인터넷뱅킹을 위한 접근정보, 계좌정보 등도 서비스제공자의 서버에 전자기적 형태로 저장되어 전자기적 처리를 통해서만 볼 수 있어 이에 해당한다. 이러한 정보는 행위자에게 알려지지 않을 것을 요건으로 한다. 이러한 요건은 정보에 대한 형식적 처분권자의 의사에 따라 정보가 범죄행위 당시에 행위자의 지배영역에 있어서는 안 될 경우에 만족한다.²⁸⁷⁾ 그러므로 이에 의하면 정보 주체가

286) Im, Strafbarkeit und Strafverfolgung von grenzüberschreitendem organisiertem Phishing, 2015, S. 80

공개를 결정하지 않은 개인정보나 금융정보는 이러한 요건을 만족하며, 인터넷 뱅킹과 관련된 정보를 포함한다. 그리고 이러한 정보는 부정한 접근으로부터 특별히 보호되는 것이어야 한다. 이는 권리가 없는 자의 접근을 방해하거나 적어도 어렵게 하는 차단장치가 있음을 의미한다. 그리고 이를 만족하기 위해서는 암호화 프로그램과 같은 비밀보호를 위한 기술적·기계적 보안조치를 필요로 한다.

이러한 정보에 접근하기 위하여 행위자는 접근차단장치를 해제하는 행위를 해야 한다. 여기서 언급하는 해제는 기술적·기계적 보안조치를 끄기 위한 모든 행위를 의미한다.²⁸⁸⁾ 보이스피싱의 경우, 해당 요건의 만족과 관련하여 논쟁이 존재한다. 보이스피싱에 해당 조항을 적용할 수 없다는 의견에 의하면 피해자가 스스로 자신의 개인정보 및 금융정보를 행위자에게 교부하는 경우에는 접근차단장치 해제행위가 존재하지 않는다고 본다. 하지만 해당 조항을 적용할 수 있다는 의견에서는 피해자가 보이스피싱을 통해 스스로 정보를 교부한 시점에 접근차단장치 해제행위가 있다고 보고 있다. 이는 결국 접근차단장치 해제행위에 대하여 해당 접근차단장치에 대한 적극적이고 직접적인 해제행위가 존재하여야 하는지, 혹은 비밀번호를 교부받는 것과 같이 간접적인 방식의 해제행위를 인정해야 하는지의 문제로, 이에 대해서는 아직도 논쟁이 있다.²⁸⁹⁾

287) Kargl, NK-StGB, § 202a Rn. 7

288) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서, 2016, 257면

289) Christoph Stammer, 「Einblick in die Cybercrime am Beispiel des Phishing」, 2014, p.32

다. 형법상 증거가치 있는 정보의 위작죄

독일형법 제 269조에서는 형법상 증거가치 있는 정보의 위작죄에 대하여 규정하고 있으며, 해당 규정의 보호법익은 법률관계의 안전과 신뢰이다. 조문의 내용은 다음과 같다.

제269조 증거가치 있는 정보의 위작(Falschung beweiserheblicher Daten)

- ① 법률관계에서 기망을 목적으로 증거가치 있는 정보를 저장하거나 변경하여 그 정보를 판별하는 과정에서 위조 또는 변조된 문서가 존재하는 것으로 보이도록 하거나, 그렇게 저장되거나 변경된 정보를 사용한 자는 3년 이하의 자유형 또는 벌금형에 처한다.
- ② 미수는 처벌한다.
- ③ 제267조 제3항 및 제4항은 준용한다.

해당 규정에서 언급하는 정보의 개념은 제 202조a 제 2항을 준용하는 것으로 보아야 한다. 그리고 한편 증거가치가 있다는 것은 법률관계에서 법적으로 중요한 사실을 증빙하기 위한 증거로 이용될 수 있다는 것을 의미한다. 즉, 권리의무의 발생과 유지, 변경, 양도, 종료에 영향을 미칠 수 있는 사실을 증빙하기 위한 증거를 의미한다. 다만, “위조 또는 변조된 문서의 존재”는 가정적 행위 결과에 불과하기 때문에 해당 사실이 실제로 존재할 필요는 없다.²⁹⁰⁾

해당 규정은 보이스피싱을 통해 얻은 개인정보를 이용한 온라인 banking 과정에 적용될 수 있다. 독일 형법 제 270조²⁹¹⁾에 의하면 허위 사실에 의하여 법적 거래 시의 정보처리과정에 영향을 미치는 행위는 법적 거래 시의 기망으로 보며, 이를

290) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서, 2016, 261면

291) 제270조 정보처리과정에서의 법적 거래의 기망허위 사실에 의하여 법적 거래 시의 정보처리과정에 영향을 미치는 행위는 법적 거래 시의 기망으로 본다.

통해 온라인 뱅킹 과정에서 권한 없는자가 마치 권한이 있는 것과 같이 은행 데이터 처리 프로그램을 속이는 것도 기망으로 판단될 수 있다. 그러므로 보이스피싱을 통해 얻은 개인정보를 해당 정보주체가 아닌 자가 정보주체인 것처럼 온라인 뱅킹에 입력하는 것은 은행 거래와 관련된 권리의무에 영향을 미치는 사실을 증빙하기 위함이며, 이를 통해 은행 데이터베이스에는 로그인 기록이 남아 저장되고, 이를 바탕으로 계좌 이체 등의 은행 업무를 진행하는 법적 거래가 이루어지므로 해당 규정이 적용될 수 있다.²⁹²⁾

라. 형법상 컴퓨터사용사기죄

독일형법 제 263조a에서는 컴퓨터사용사기죄에 대하여 규정하고 있으며, 해당 조문의 내용은 다음과 같다.

제263조a 컴퓨터사기

- ① 위법한 재산상의 이익을 자신이 취득하거나 제3자로 하여금 취득하게 할 의사로 프로그램의 부정확한 구성, 부정확하거나 불충분한 정보의 사용, 정보의 권한 없는 사용, 기타 (정보처리) 과정에 대한 권한 없는 작용에 의하여 정보처리의 결과에 영향을 줌으로써 타인의 재산에 손해를 가한 자는 5년 이하의 자유형 또는 벌금형에 처한다.
- ② 제263조 제2항 내지 제7항은 동일하게 적용된다.
- ③ 당해 행위의 수행을 목적으로 하는 컴퓨터프로그램을 만들거나, 자신이 또는 제3자로 하여금 취득하게 하거나, 팔려고 내놓거나, 보존하거나 또는 타인에게 양도함으로써 제1항에 의한 범죄행위를 예비한 자는 3년 이하의 자유형 또는 벌금형에 처한다.
- ④ 제3항의 경우에 제149조 제2항 및 제3항은 동일하게 적용된다.

해당 조항에 의하면 보이스피싱을 통해 피해자를 기망 또는 협박하여 개인정보 및 금융정보를 교부받고, 피해자의 인터넷 뱅킹 사이트 등에 접속하여 피해자의

292) Christoph Stammer, 「Einblick in die Cybercrime am Beispiel des Phishing」, 2014, p.33

개인정보 및 금융정보를 기입한 행위는 “정보의 권한 없는 사용” 또는 “기타 정보 처리과정에 대한 권한 없는 작용”을 통해 정보처리결과에 영향을 준 행위에 해당한다. 그러므로 보이스피싱 범죄에 해당 조항이 적용된다.²⁹³⁾

마. 형법상 강요죄 및 공갈죄

독일 형법 제 240조와 제 253조에서는 강요죄와 공갈죄에 대하여 규정하고 있으며, 해당 조문의 내용은 다음과 같다.

제240조 강요

- ① 폭행 또는 상당한 해악을 고지한 협박에 의해 타인에게 작위, 수인 또는 부작위를 강요한 자는 3년 이하의 자유형 또는 벌금형에 처한다.
- ② 의도한 목적을 위하여 폭행을 사용하거나 해악을 고지한 행위가 비난받아야 할 것으로 인정되는 경우에 그 행위는 위법하다.
- ③ 미수범은 처벌한다.
- ④ 특히 중한 경우에 6월 이상 5년 이하의 자유형에 처한다. 특히 중한 경우란 특별한 사정이 없는 한, 행위자가 다음 각호의 1에 해당하는 경우이다.
 1. 타인에게 성적 행동 또는 부부관계를 강요하는 경우
 2. 임신부에게 낙태를 강요하는 경우
 3. 공무원으로서 권한 또는 지위를 남용하는 경우

제253조 공갈

- ① 자기 또는 제3자의 불법한 영리를 위하여 폭행 또는 상당한 해악을 고지한 협박에 의하여 타인에 대하여 위법하게 작위, 수인 또는 부작위를 강요하고 그로 인하여 피강요자 또는 타인의 재산에 손해를 가한 자는 5년 이하의 자유형 또는 벌금형에 처한다.
- ② 의도된 목적을 위하여 폭행을 가하거나 또는 해악을 고지한 행위가 비난받아야 할 것으로 인정된 경우에 그 행위는 위법하다.
- ③ 미수범은 처벌한다.
- ④ 특히 중한 경우에 1년 이상의 자유형에 처한다. 특히 중한 경우란 특별한 사정

293) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서, 2016, 264면

이 없는 한, 행위자가 직업적으로 또는 공갈의 계속적 수행을 목적으로 조직된 범죄조직의 구성원으로서 행위한 경우를 말한다.

제 240조의 강요죄와 제 253조의 공갈죄에서 언급하는 해악은 실제로 실현할 의사를 요하지 않으며, 실현 가능할 필요도 없다.²⁹⁴⁾ 그러므로 친인척에 대한 납치 등의 해악을 고지하고 그에 따라 입금을 요구하는 '콜센터 사기' 방식의 보이스피싱의 경우, 그러한 행위의 실현만으로도 제 240조의 강요죄가 성립되며, 이후 입금이 이루어져 재산상의 이익을 취득한 경우에는 제 253조의 공갈죄가 성립된다. 또한 입금을 요구하지 않더라도 피해자의 개인정보나 금융정보를 갈취하는 것만으로도 충분히 제 240조의 강요죄가 성립된다. 그리고 보이스피싱의 경우, 조직범죄에 해당하므로 제 253조의 공갈죄가 성립되는 경우 제 253조 제 3항이 적용되어 1년 이상의 자유형에 처해지게 된다.

바. 형법상 자금세탁, 불법적으로 획득한 재산가치의 은닉죄

독일형법 제 261조에는 자금세탁, 불법적으로 획득한 재산가치의 은닉죄가 규정되어 있으며, 조문의 내용은 다음과 같다.

제261조 자금세탁, 불법적으로 획득한 재산가치의 은닉

① 제2문에 언급된 위법행위로 인하여 생긴 대상물을 은닉하거나 그 출처를 위장하거나 출처의 수사, 그 대상물의 발견, 추정, 몰수 또는 압류를 방해하거나 위태롭게 한 자는 3월 이상 5년 이하의 자유형에 처한다. 제1문에 의한 위법행위란 다음 각호의 죄를 말한다.

1. 중죄

2. 다음에 해당하는 경죄

a) 제332조 제1항, 제3항 및 제334조

b) 향정신성의약품법(Betäubungsmittelgesetz) 제29조 제1항 제1호 및 원료 감독

294) Toepel, NK-StGB, § 240 Rn. 99; Fischer, StGB, § 240 Rn. 97

법(Grundstoffüberwachungsgesetz) 제29조 제1항 제1호

3. 조세규정(Abgabenordnung) 제373조 및 제374조 제2항에 의한 경죄(25), 모든 경우에 공동시장조직 및 직접변제의 수행에 관한 법률(Gesetz zur Durchführung der Gemeinsamen Marktorganisationen und der Direktzahlungen) 제12조 제1항과 연계

4. 다음 각 해당 경죄를 영업적 또는 당해 행위의 계속적 수행을 목적으로 조직된 범죄조직의 구성원으로 행한 경우

a) 제152조a, 제181조a, 제232조 제1항 및 제2항, 제233조 제1항 및 제2항, 제233조a, 제242조, 제246조, 제253조, 제259조, 제263조 내지 제264조, 제266조, 제267조, 제269조, 제284조, 제326조 제1항, 제2항 및 제4항, 제328조 제1항, 제2항 및 제4항

b) 체류법(Aufenthaltsgesetz) 제96조, 망명절차법(Asylverfahrensgesetz) 제84조 및 조세규정 제370조

5. 제129조 및 제129조a 제3항 및 제5항에 의한 경죄, 모든 경우에 제129조b 제1항과 범죄조직 또는 테러조직의 구성원으로서(제129조, 제129조a, 각각의 경우 제129조b 제1항과 연계) 범한 경죄

조세규정(Abgabenordnung) 제370조에 의한 영업적 또는 조직범죄적 탈세의 경우에 탈세를 통해 절약된 비용 및 불법하게 취득한 조세상환액 및 조세변상액에 대하여 더 나아가 제2문 제3호의 경우에 당해 조세에 관하여 탈세한 대상물에 대하여 제1문은 적용된다.

② 제1항에 규정된 대상물에 대하여 다음 각호의 1에 해당하는 행위를 한 자도 전항과 동일하게 처벌한다.

1. 자신이 취득하거나 제3자로 하여금 취득하게 하는 행위

2. 취득 당시 그 대상물의 출처를 알면서도 이를 보관하거나 자기 또는 제3자를 위하여 처분하는 행위

③ 미수범은 처벌한다.

④ 특히 중한 경우에는 6월 이상 10년 이하의 자유형에 처한다. 특히 중한 경우란 특별한 사정이 없는 한, 행위자가 영업적으로 또는 자금 세탁의 계속적 수행을 목적으로 조직된 범죄조직의 구성원으로서 행위한 경우를 말한다.

⑤ 제1항 또는 제2항의 경우에 그 대상물이 제1항에 언급된 위법행위로 부터 유래한다는 사실을 중과실로 인식하지 못한 자는 2년 이하의 자유형 또는 벌금형에 처한다.

⑥ 당해 범죄를 범하지 아니하고 사전에 제3자가 대상물을 취득한 경우에 그 행위는 제2항에 의하여 처벌되지 아니한다.

⑦ 자금세탁범죄와 관련 있는 대상물은 이를 몰수 할 수 있다. 제74조a는 준용된다. 제43조a, 제73조d는 행위자가 자금세탁의 계속적 수행을 목적으로 조직된 범죄조직의 구성원으로서 행위한 경우에 이를 준용한다. 제73조d는 행위자가 영업적으로 행위한 경우에도 준용하여야 한다.

⑧ 당해 행위가 행위지에서도 처벌되는 경우에 제1항에 규정된 유형으로 국외에서

발생한 범죄에서 유래한 대상물은 제1항, 제2항 및 제5항에 규정된 대상물과 동일하게 본다.

⑨ 다음 각호의 모두에 해당하는 자는 제1항 내지 제5항에 따라 처벌되지 아니한다.

1. 신고 당시 자금세탁행위의 전부 또는 일부가 발각되지 아니하였고 행위자가 이러한 사실을 인식하거나 상황에 대한 상식적 평가를 통하여 이를 기대할 수 있었던 경우에 자의로 관할관청에 (자금세탁)행위를 신고하거나 또는 신고하게 한 자
2. 제1항 또는 제2항의 경우에 제1호에 언급된 조건하에서 범죄행위와 관련 있는 대상물을 보전한 자

그 밖에 본범의 참가를 이유로 처벌되는 자도 제1항 내지 제5항에 따라 처벌되지 아니한다.

⑩ 법원은 제1항 내지 제5항의 경우에 행위자가 자의로 자기가 알고 있는 사실을 진술하여 자신이 가담한 범죄행위 또는 제1항에 기재된 타인의 위법행위를 적발할 수 있도록 하는 데에 결정적으로 기여한 경우에는 작량 하여 그 형을 감경하거나 (제49조 제2항) 또는 면제할 수 있다.

보이스피싱의 경우, 해당 조항에서 해당될 수 있는 죄목은 제 261조 제 1항 제 4호의 제 253조 공갈죄, 제 269조의 증거가치 있는 정보의 위작, 제 261조 제 1항 제 5호의 제 129조 범죄단체조직죄가 있다. 그러므로 이러한 죄목에 해당하는 범죄 행위와 관련하여 사전행위에 대한 보답이나 보수, 범죄의 산물 내지 관련대상물의 경우 모두 자금세탁죄가 적용되는 대상이라고 할 수 있다.²⁹⁵⁾

자금세탁죄의 행위자는 이러한 대상물을 은닉하거나, 대상물의 출처를 위장하거나 출처의 수사 또는 그러한 대상물의 발견이나 추정, 몰수, 압류를 방해하거나 위태롭게 해야 한다. 또는 대상물을 스스로 취득하거나 제3자로 하여금 취득하게 한 경우, 대상물을 취득할 당시 그 출처를 알면서 보관하거나 자기 또는 제3자를 위해 사용한 경우에도 마찬가지로 처벌할 수 있다. 그리고 이러한 행위들은 모두 구체적인 위험 발생을 요구한다.²⁹⁶⁾ 보이스피싱 범죄에서 사용되는 대포통장에 대한 제공행위는 자금의 흐름을 은닉하기 위한 행위로서 대상물의 발견이나 추정,

295) Fischer, StGB, § 261 Rn. 7

296) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서, 2016, 268-269면

몰수, 압류를 방해하거나 위태롭게 하는 행위에 해당할 수 있다. 하지만 해당 제공 행위만으로는 행위 객체인 대상물이 존재하지 않아 구체적 위험에 이르지 못하였다고 보고 있다. 그러므로 대포통장에 입금된 피해금액을 인출하여 다른 계좌로 이체 내지 송금하는 경우에 비로소 행위객체인 대상물이 생성된 것이며, 또한 대상물 발견이나 추징, 몰수, 압류를 방해하거나 구체적으로 위태롭게 한 것이 된다고 본다.²⁹⁷⁾ 또한 대포통장 인출책 및 송금책 임무를 수행하는 자들은 인출과 송금행위 사이에 상당 시간 동안 피해금액을 보관하게 되어 제261조 제2항 제2호를 적용할 수 있으며, 즉시 송금하는 경우 제3자로 하여금 취득하게 하는 행위로 제261조 제2항 제1호를 적용하게 된다.

사. 전자금융 사기피해 구제 관련 법제

독일 민법에 의하면 자금이체는 다음과 같이 이루어진다. 금융기관이 자금이체를 요청받은 경우에 자신의 자산으로 먼저 이체를 진행하고, 그 지출액에 대하여 고객에게 상환을 받는다. 그리고 만약 계좌의 진정한 소유자가 자금이체를 지시한 것이 아니라 권한이 없는 자가 자금이체를 지시하여 자금이 이체된 경우, 금융기관은 해당 지출액에 대하여 고객으로부터 상환받을 권리를 가지지 못하게 되어 있다. 그럼에도 불구하고 금융기관이 지출액에 대해 고객의 계좌에서 자금을 인출해 간 경우 고객은 해당 액수를 상환 청구할 수 있다.

이러한 과정에서 금융기관은 고객과의 예금계약에 포함된 기본적 권리에 의존하여 면책을 주장할 수 없다. 다만 고객이 주의의무를 위반한 것이 금융기관에 의하여 명확하게 증명될 수 있다면, 지출액에 대해 청구할 수 있는 권리를 가지게 되며, 고객의 중과실을 입증할 경우 금융기관은 지출액 전액에 대해 청구할 수 있

297) 김대근, 임석순, 강상욱, 김기범, “신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로”, 한국형사정책연구원, 형사정책연구원 연구총서, 2016, 268-269면

고 이를 이용해 고객의 환불청구에 대해 대항할 수 있다.²⁹⁸⁾ 그리고 여기서 언급하는 고객의 주의의무는 컴퓨터 등에 백신 설치의무, 제3자의 수상한 행동을 분간할 의무, 제3자에게 PIN, TAN 번호 등 정보를 제공하지 않은 의무 등이다. 그러므로 이에 의하면 보이스피싱에 의하여 개인정보 및 금융정보를 교부한 경우에는 고객으로서의 주의의무를 다한 것으로 볼 수 없어 사기 피해에 대한 구제를 받기 어렵다고 볼 수 있다.

독일에 직접적으로 적용되는 법률은 아니나, 유럽 전역에 해당 법률의 내용을 따를 것을 명시하는 지침의 일종인 지급서비스지침(Payment Services Directive) 제 69조에 의하면, 지급서비스 이용자는 무권한 자금이체가 이루어진 경우 그 사실을 지체 없이 지급서비스 제공자에게 통보할 의무를 가진다.²⁹⁹⁾ 그리고 그 기간은 71조에 따라서 최장 13개월 이내로 규정된다.³⁰⁰⁾ 이러한 통보가 적시에 이루어진 경우, 그 이후의 무권한 자금 이체에 대해서 지급 서비스 이용자는 일절 책임지지 않는다. 또한, 통보가 이루어지기 전에 행해진 무권한 자금 이체에 대해서는 지급 서비스 이용자가 중과실을 범하거나 사기적으로 행동하지 않았다면 최대 50유로의 범위 내에서만 책임을 진다. 여기서 언급하는 중과실 판단 여부도 위의 독일 민법에서와 같이 고객의 주의의무를 다하는 경우로 본다. 하지만 만약 13개월 이내에 신고가 이루어지지 않았다면, 지급 서비스 이용자의 무권한 이체에 대한 책임은 제한되지 않는다.³⁰¹⁾ 그러므로 이에 의하면 보이스피싱에 의하여 무권한 자

298) 박진성, “주요국의 전자금융 사기피해 구제제도에 대한 비교 연구: 범경제학적 접근”, 한국무역연구원, 무역연구 11(5), 2015, 546면

299) DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, Article 69 Obligations of the payment service user in relation to payment instruments and personalised security credentials

300) DIRECTIVE (EU) 2015/2366, Article 71 Notification and rectification of unauthorised or incorrectly executed payment transactions

금이체가 일어난 경우, 피해자가 통보를 적시에 한 경우에 한하여 그 이후에 일어나는 무권한 자금이체에 대해서는 피해를 입지 않게 된다. 하지만 통보 이전의 무권한 자금이체에 대해서는 보이스피싱에 의하여 개인정보 및 금융정보를 교부하여 고객으로서의 주의의무를 다한 것으로 보기 어려워 이에 대한 피해에 대하여 피해자가 온전히 감수해야 한다.

301) DIRECTIVE (EU) 2015/2366, Article 74 Payer's liability for unauthorised payment transactions

제3절 일본의 대응체계 및 법제

1. 범죄 동향

일본어로 예금 계좌에 돈을 입금 또는 송금하는 것을 ‘후리코미’ 라고 하며, 전화나 엽서 등을 이용한 사기 또는 공갈 행위로 현금을 지정하는 계좌에 이체(후리코미)시키는 수법을 ‘계좌이체사기’ 또는 ‘후리코메사기(振り込め詐欺)’ 라고 부른다. 2004년 11월까지 이러한 종류의 범죄는 모두 보이스포싱 이라고 했지만, 수법의 다양화에 이름과 실태가 맞지 않고 특수사기 중의 4가지 유형 (스푸핑 사기, 가공 청구사기, 융자보증금사기, 환급 금 등의 사기)를 총칭하여 2004년 12월 경찰청에 의해 통일 명칭으로 후리코메사기(振り込め詐欺)’ 라고 부르는 것이 결정되었다.³⁰²⁾ 이러한 전화를 이용한 사기 사건 자체는 ‘오레오레(俺俺·나야 나) 사기’ 이나 ‘후리코메사기’ 라는 말이 등장하기 이전부터 존재하였으나, 일본 내에서 첫 보이스포싱으로 드러난 것은 1999년 8월부터 2002년 12월 사이에 전화를 통해 가족의 목소리를 가장하여 11명에게 은행계좌 이체를 시킨 사건으로 기록되고 있다. 2003년 2월 범인을 검거한 토토리현 경찰은 해당 수법에 대해 처음으로 ‘오레오레사기(보이스포싱)’ 이라는 용어를 사용하기 시작하였다.

2018년도의 일본 보이스포싱 인지건수는 16,315건으로 전년대비 8.9% 감소하여 7년만에 감소세로 돌아섰고 피해액 또한 전년대비 7.7% 감소한 349억엔이 발생하였다. 하지만 여전히 일본 경찰청은 심각한 수준으로 판단하고 있으며, 지자체가 아닌 수도권에서의 피해 비율이 증가하고 있다. 도쿄도내 사건 인지 건수만 3913건으로 과거 역대 최대를 기록하였으며, 최신기술의 활용 및 수법이 교묘해지고 있는 것이다.

일본에서는 전형적으로 ‘오레오레(俺俺·나야 나)’ 사기가 여전히 가장 많은 피해

302) 毎日新聞, “総称は「振り込め詐欺」 実態に即し 警察庁決定 今年被害220億円に”, 2014, 31면

를 낳고 있으며, 가공청구 사기, 환급금 사기, 대출보증금 사기 순으로 피해를 받고 있다. ‘오레오레’ 사기 및 가공청구사기의 2가지 사기가 전체 보이스피싱의 대부분(건수:85.7%, 금액 91.7%)을 차지할 정도로 두가지 유형의 사기가 가장 심각하다. 피해자로부터 금전을 수취하는 방법으로는 ‘오레오레’ 사기의 경우 직접 현금을 전달하는 방식으로 많은 피해를 보는 반면, 융자보증금 및 환급금 사기의 경우에는 이체 방식이 이용되고 있다.³⁰³⁾

일본의 보이스피싱 사기 그룹은 각각 역할분담을 통해 조직적으로 운영된다. 돈을 요구하는 전화를 걸어 속이는 역할의 인간을 ‘카케코「掛け子(架け子)」’라 하며, 입금시킨 금융계좌로부터 현금을 인출하는 역할의 인간을 ‘다시코「出し子」’라 한다.³⁰⁴⁾ 또한, 금융 계좌를 사용하지 않고 직접 접촉해 현금을 받는 역할의 인간을 ‘우케코「受け子」’ 등의 속칭으로 부르고 있다.³⁰⁵⁾ ‘카케코’가 제대로 전화를 하고 있는지 감시하고 관리하는 우두머리격의 ‘반토우「番頭」’가 있으며, ‘다시코’와 ‘우케코’가 수령한 금전을 몰래 밀반출한 것을 방지하기 위해 ‘감시 역「見張り役」’이 있다. 이 밖에 현금을 수령 하는 현장을 담당하게 되는 ‘다시코’와 ‘우케코’를 선발하기 위한 ‘리크루터「リクルーター」’가 있는 것이 확인되었다.³⁰⁶⁾

303) 이종호, “[조사자료] 2018년 일본의 보이스피싱 동향 및 대응현황”, 금융감독원 업무자료, 2019

304) The Sankei News(2019.11.11.), “バイト感覚で詐欺の片棒受け子・出し子の哀れな末路”,
<https://www.sankei.com/premium/news/191111/prm1911110003-n1.html>
(2020.12.14. 최종확인)

305) 松村明[監修], 「大辞泉」(第2版), 小学館, 2012

306) 毎日新聞(2013.02.21.), “振り込め詐欺:「受け子」リクルーター? 71歳、容疑で逮捕/静岡”,
<http://mainichi.jp/area/shizuoka/news/20130221ddlk22040212000c.html>
(2020.12.14. 최종확인)

2. 대응 체계

가. 경찰청

경찰청은 2004년 전국 최초로 부 총감을 본부장으로 하는 보이스피싱 대책본부를 설치하였으며 그 후, 각 토도부현(일본의 행정구역) 본부에도 이와 같은 대책본부를 설치하고 전문 수사반, 기술반을 편성 공식 웹 사이트에서도 시민들에게 주의를 호소하고 있다.

경찰청 홈페이지는 전화나 문서를 이용해 상대방을 속이거나 금융 기관 등을 사칭해 돈을 빼내는 금융 사기를 의미하는 후리코메사기(振り込め詐欺)를 특수사기의 한 종류로 분류하고 이 특수사기 대책에 포함시켜서 보이스피싱 대책을 게재하고 있다. 특수사기에는 오레오레사기(オレオレ詐欺, 나야 나 사기), 가공청구사기, 용자보증금사기, 환부금등사기, 금융상품등 거래명목 사기, 도박필승정보제공명목 사기, 이성과의 교제알선명목사기 등이 포함되고 있으며 이러한 보이스피싱을 포함한 특수사기에 대한 대책으로 수법 및 특징, 주의사항, 관련기관 등에 대한 정보를 제공하고 있으며 만화로도 예방대책을 홍보 중이다.³⁰⁷⁾

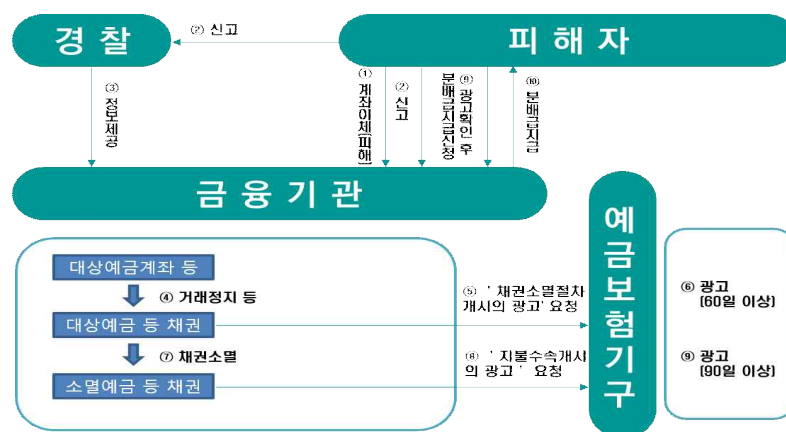
또한, 일본 경찰청은 2008년 6월에 법무성과 공동으로 “보이스피싱 척결액션플랜”을 발표하였으며, 일본 경찰청 산하에 보이스피싱 대책실(실장 경찰청 차장)을 설치하고 각 지방경찰에 대책반을 구성하여 대대적인 단속을 하였다. 보이스피싱에 관해서는 지능범죄 사기담당부서와 폭력단 담당부서가 연계수사를 하여 지속적으로 단속하며 2016년 4월에는 해당 부서에 약 160명의 경찰관을 증원하여 수사를 강화하고 있다.

307) 警察庁, “ストップ・オレオレ詐欺 47 家族の絆作戦”,
https://www.npa.go.jp/safetylife/seianki31/1_hurikome.htm (2020.12.15.
 최종확인)

나. 금융청

금융청은 홈페이지를 통해 보이스피싱 사기 주의사항 홍보를 하고 있으며, “금융서비스이용자상담실”에서 상담전화를 받아 상담을 해주고 있다. 또한 송금사기 구제법(犯罪利用預金口座等に係る資金による被害回復分配金の支払等に関する法律)에 따라 보이스피싱 사기 구제업무를 담당하고 있다. 보이스피싱 피해자가 금융청을 통해 구제를 받기 위해서는 피해사실을 즉시 송금 금융기관에 연락해야 하며, 피해복구 분배금 지급을 받기 위한 신청이 필요하다. 단, 범인이 계좌에서 이미 현금을 인출하거나, 입금 절차에 의하지 않는 사기(예를들어 범인에게 직접 현금을 전달한 경우, 우편이나 소포 등으로 현금을 동봉하여 범인이 지정한 대상에게 우송한 경우)는 송금사기구제법에 의해 구제적용을 받지 못한다.³⁰⁸⁾

[그림 6-1] 일본 송금사기구제법에 의한 금융기관의 구제 개요도



(출처: 預金保険機構, “犯罪利用預金口座等に係る資金による被害回復分配金の支払等に関する法律の概要図“)

308) 金融庁, “振り込め詐欺等の被害にあわれた方へ”,
<https://www.fsa.go.jp/policy/kyuusai/furikome/index.html> (2020.12.15.
 최종확인)

다. 전국은행협회

전국은행협회는 홈페이지³⁰⁹⁾에 금융범죄의 수법을 게재하고 신종 사기 수법의 전파와 예방 홍보를 하고 2005년부터 매년 10월 보이스피싱 근절 강화 추진 기간으로 지정하여 다채로운 행사를 하고 있다. 2014년에는 도쿄 중심가에서 금융범죄 방지 이벤트로 “가족이 함께 방지하자! 금융범죄”를 개최하였고, 2013년 도쿄 치요다구 방송회관에서 “금융범죄 방지 계몽 심포지움-당신을 노리는 금융범죄! 속지 않기 위하여”를 개최하였다. 2016년에는 스포대회 지방 순회 경기 관람객 대상 보이스피싱 예방 캠페인을 실시하였으며, 연극단을 결성하여 사기예방 순회 공연을 하기도 하였다. 2016년 5월부터는 고등학생을 대상으로 지역 내 보이스피싱 예방 계몽 활동 지원 사업을 실시하는 등 다양한 활동을 추진하고 있다.³¹⁰⁾

또한, 최근 은행 협회 직원을 사칭하여 신종 코로나 바이러스와, 도쿄올림픽 등을 명목으로 한 현금카드를 가로채는 등의 신종 보이스피싱 등이 성행하고 있어 이와 관련한 범죄 수법의 사례를 홈페이지에 공개하고 범죄 예방을 위해 취할 수 있는 대응 절차를 홍보, 교육하고 있다.³¹¹⁾

라. 지자체

면식이 없는 불특정한 인원에 대해 전화 및 기타 통신수단을 이용하여 예저금계좌로의 송금 및 기타 방법으로 현금 등을 가로채는 특수사기는 보이스피싱(오레

309) 全国銀行協会, 振り込め詐欺, <https://www.zenginkyo.or.jp/hanzai/5404/> (2020.12.14. 최종확인)

310) 홍성삼, “피싱 사기범죄에 대한 인터폴 및 국가별 대응정책 비교연구”, 원광대학교 경찰학연구소, 경찰학논총 14(1), 2019, 116-117면

311) 全国銀行協会, “銀行協会職員を騙る詐欺(新型コロナウイルスやオリンピック等を名目にしてキャッシュカードをだまし取る手口)”, <https://www.zenginkyo.or.jp/hanzai/7320/> (2020.12.15. 최종확인)

오래 사기, 가공 청구 사기, 융자보증금 사기 및 환급금 등 사기) 및 보이스피싱 이외의 특수 사기(예를 들면, 금융상품 등 거래 명목, 도박 필승법 정보 제공 명목 등의 사기)가 있으며, 각 지자체는 이러한 특수사기에 대해 조례를 통해 대응하고 있다. 특수사기에 대한 조례는 크게 2가지의 형태로 구분할 수 있는데, 먼저 특수 사기로 인한 피해를 방지하기 위한 단독 조례와 기존 생활 안전조례 등을 개정하여 특수사기에 의한 피해를 방지하기 위한 규정을 두는 것이다.³¹²⁾

1) 특수사기 관련 단독조례 제정

2020년 4월 기준 특수사기에 관하여 단독조례를 제정하고, 그 피해방지대책 등을 규정하고 있는 지자체는 아래와 같다.

〈표 6-6〉 보이스피싱에 관한 일본 지자체의 단독 조례

구분	조례명칭	공표	시행
쿠마모토 현	현민의 입금 사기 피해로부터 보호하는 조례	2009년 3월 27일	2009년 4월 1일
오카야마 현	오카야마 현 특수 사기 피해 방지 조례	2010년 3월 17일	2010년 4월 1일 (2014년 3월 20일 개정 시행)
도쿠시마 현	도쿠시마 현 입금 사기 등의 피해 방지에 관한 조례	2014년 3월 20일	2014년 4월 1일
치바현 카시와시	카시와시 입금 사기 등 피해 방지 등 조례	2016년 3월 23일	2016년 4월 1일
아이치현	한다시 입금 사기 등 피해	2017년 7월 12일	2017년 7월 12일

312) 地方自治研究機構, “特殊詐欺に関する条例”,
http://www.rilg.or.jp/htdocs/img/reiki/010_specialfraud.htm (2020.12.15.
 최종확인)

한도시	방지에 관한 조례		
사이타마현 미사토시	미사토시 입금 사기 등의 피해 방지에 관한 조례	2018년 3월 27일	2018년 4월 1일
사이타마현	사이타마 현 특수 사기 근절 조례	2018년 3월 19일	2018년 3월 19일
미에현 쿠와나시	쿠와나시 특수 사기 근절 조례	2019년 7월 2일	2019년 7월 2일
오이타현	오이타현 특수 사기 등 피해 방지 조례	2019년 12월 23일	2020년 4월 1일
야마나시현	야마나시현 전화 사기 등 피해 근절에 관한 조례	2020년 3월 30일	2020년 3월 30일

이중 구마모토현 조례는 보이스피싱만을 대상으로 하고 있다. 오카야마현 조례의 경우 2010년 제정 당시의 조례명은 ‘오카야마현 송금 사기 피해 방지 조례’였는데, 2014년 3월에 개정되어 넓은 범위의 특수사기를 대상으로 하여 현재의 조례명으로 개정하였다. 전국의 시정촌(市町村)에서 최초로 송금 사기 등에 관한 조례를 제정한 것은 카시와시다. 카시와시는 전국 평균에 비해 보이스 피싱 사기 피해 건수가 많아 큰 사회적 문제로 다루어졌으며³¹³⁾ 도시 차원에서 보이스피싱 사기에 대항하기 위해 사업자와 시민을 포함한 입금 사기에 관련되는 사안을 정한 조례를 처음으로 제정하게 되었다.³¹⁴⁾

대부분의 조례에서 ‘특수사기’는 ‘보이스피싱’ 및 ‘보이스피싱 유사행위’로 정의하고, ‘보이스피싱’이란 ‘오레오레 사기’, ‘가공청구 사기’, ‘대출보증금 사기 및 환급금 등 사기’로 정의하고 있다. 예를 들면 쿠와나시 조례 제2조에서는 ‘오레오레 사기’, ‘가공청구 사기’, ‘융자 보증금 사기’, ‘환급금 등 사기’ 및 ‘송금 사기 유사 행위’를 각각 다음과 같이 규정하고 있다.

313) 岩津圭介, “柏市振り込め詐欺等被害防止等条例”, 自治体法務研究 No.46 2016年 秋号, 2016

314) 総務部 防災安全課, “柏市振り込め詐欺等被害防止等条例の制定の経緯等について”, 2016

〈표 6-7〉 ‘특수사기’의 정의 (미에현 쿠와나시 조례 제2조)

구분	특수사기의 정의
오래오래 사기	친족 등을 가장하여 전화를 걸어 허위 명목으로 즉시 현금이 필요하다고 믿게 하고, 지정한 예금계좌에 현금을 입금하게 하는 수법, 기타 이와 유사한 방법에 의한 사기(형법 제246조 또는 제246조의2의 죄에 해당하는 행위를 말함)
가공 청구사기	가짜로 만들어 낸 사실을 구실로 금품을 요구하는 문서 등을 송부하여 지정한 예금계좌에 현금을 입금하게 하는 수법 및 기타 이와 유사한 방법에 의한 사기
대출보증금 사기	대출을 받기 위한 보증금 등의 명목으로 지정한 예금 계좌로 현금을 입금하게 하는 수법, 기타 이와 유사한 방법에 의한 사기
환급금 등의 사기	국가 또는 지방공공단체의 직원 등을 가장하여 의료비, 세금, 연금에 관한 보험료 등의 환급 등에 필요한 절차라고 말하고, 현금자동입출기를 조작시켜 예금계좌 간의 송금으로 현금을 입금하게 하는 수법, 기타 이와 유사한 방법에 의한 사기
보이스피싱 유사사기	금융상품의 거래, 복권 당첨번호 등의 제공, 이성과의 교제 알선 및 기타 명목으로 허위 정보를 제공하는 등 지정한 예저금계좌에 현금을 입금시키는 수법 및 기타 이와 유사한 방법으로 이루어지는 사기(보이스피싱 제외)

한편, 야마나시현 조례에서는 ‘전화사기’라는 용어를 사용하고 있다. 이는 ‘오래오래 사기’나 ‘가공청구 사기’ 등 대부분의 특수사기에서 거의 모든 범행에 전화가 사용됨에 따라 ‘특수사기’를 ‘전화사기’로 명명하며 보이스피싱에 대응하고 있다.

조례의 내용에 대해서는 대부분의 경우, 현(시)의 책무, 현(시)민의 역할, 사업자의 역할, 보급 계발, 정보의 제공, 통보 등의 규정을 두고 있으며, 추가적으로 ATM 이용 시의 유의 사항(쿠마모토현 조례 10조), 피해방지에 관한 유의사항(오카야마현 조례10조, 한다시 조례7조) 피해자에 대한 지원(카시와시 조례 8조, 미사토시 조례 8조, 오이타현 조례 14조), 특수사기 경계 선언(쿠와나시 조례 8조 2항) 등의 규정을 두는 경우도 있다. 이러한 이념적인 규정과 더불어, 오이타현 조

례는 범죄거점(아지트)대책 및 연락처 리스트(명부)대책에 관한 규정을 두고 있다.

우선, 범죄 거점(아지트) 대책으로서 건물의 대출에 관한 규제 등이나 여관 영업자등의 영업에 관련되는 규제 등의 규정을 두고 있다. 즉, 누구나 자신이 대출을 하려는 현 내에 소재하는 건물이 특수사기 등의 용도로 제공될 우려가 있음을 알면서 해당 건물을 대출해서는 안 되며(15조), 건물을 대출하려는 자는 해당 대출과 관련된 계약의 체결 전에 해당 계약의 상대방에 대해 해당 건물을 특수사기 등의 용도로 제공하는 것이 아님을 서면으로 확인하도록 노력할 필요가 있다(16조 1항). 물건을 대출하는 대리 또는 매개하는 자는 해당 대리 또는 매개와 관련된 건물이 특수사기 등에 제공될 우려가 있음을 알면서 해당 대출과 관련된 계약을 대리하거나 매개해서는 안 되며(17조 1항), 「여관업법」 제2조 제1항에 규정된 주택숙박사업을 영위하는 자는 숙박하고자 하는 자에 의해 여관업 등을 영위하는 시설이 특수사기 등의 용도로 제공될 우려가 있음을 알면서 해당 시설에 숙박하게 해서는 안 된다(18조 1항)고 규정하고 있다.

다음으로 연락처 리스트(명부) 대책으로서 개인정보의 제공 등과 관련되는 규제 등의 규정을 두고 있다. 즉, 누구든지 특수사기 등의 용도로 제공될 우려가 있음을 알면서도 개인정보(개인정보보호에 관한 법률 제2조 제1항 제1호에 규정된 개인정보 중 성명, 생년월일, 주소, 전화번호 등 또는 이들의 조합으로 특수사기 등의 용도로 제공될 우려가 있는 것에 한 함)을 제삼자에게 제공해서는 안 된다.(19조 1항)

또한, 개인정보 취급사업자(법 제2조 제5항에 규정된 개인정보 취급사업자를 말한다.)는 개인정보(동조 제6항에 규정된 개인 데이터 중 성명, 생년월일, 주소, 전화번호 등 또는 이들 조합으로 특수사기 등의 용도로 제공될 우려가 있는 것에 한함)를 제3자(동조 제5항 각 호에 열거된 자는 제외)에게 제공할 때 법 제25조 제1항의 기록을 작성하는 경우에는 운전면허증을 제시받는 방법, 기타 규칙으로 정하는 방법에 따라 성명 또는 명칭, 기타 규칙으로 정하는 사항을 확인해야 한다

(20조제1항 본문)고 규정하고 있다.

2) 기존의 생활안전 조례 개정

특수사기에 대해 단독 조례로 제정하는 것이 아닌 기존의 생활 안전조례 등에서 관련된 규정을 두고, 그 피해방지대책 등을 규정하고 있는 지자체로는 다음과 같은 지역이 있다.

〈표 6-8〉 생활안전 조례 개정을 통한 보이스피싱 범죄 대응

구분	조례 명칭	공포	개정
시가현	‘없애자 범죄’ 시가의 안전한 마을 만들기 조례	2003년 3월 20일	2003년 4월 1일 (2015년 4월 1일 개정 시행)
도쿄도	도쿄도 안전 안심 마을 만들기 조례	2003년 7월 16일	2003년 10월 1일 (2015년 9월 1일 개정 시행)
오사카 부	오사카 안전한 마을 만들기 조례	2002년 3월 29일	2002년 4월 1일 (2019년 6월 1일 개정 시행)

위 지역 모두 조례 개정에 따라 특수사기에 관한 규정이 생겼다. ‘특수사기’의 정의에 대해서는 ‘사기(형법 제246조의 2의 죄를 말함) 또는 컴퓨터 사용 사기(형법 제246조의 2의 죄를 말함) 중 면식이 없는 불특정인을 전화나 기타 통신수단을 이용하여 대면하지 않고 속이고 불법으로 조달한 가공 또는 타인 명의의 예금계좌에 입금하거나 기타의 방법으로 해당자에게 재물을 교부하게 하거나 재산상 불법의 이익을 얻거나 타인에게 이를 얻게 하는 것(도쿄도 조례3조제1항)으로 규정하고 있다. 도쿄도 조례에는 범죄 거점(아지트) 대책에 관한 규정(33조)이 있으며, 오사카부 조례에는 범죄 거점(아지트) 대책 및 연락처리리스트(명부) 대책에 관한 규정(22조~25조)이 마련되어 있다.

3. 대응 법률

가. 형법

1) 보이스피싱에 해당하는 사기죄

보이스피싱의 처벌에 관해서는 형법에서 규정하는 사기죄를 중심으로 다루어지고 있다. 사기죄는 형법 246조에 규정되어 있으며, 그 성립에는 ①기피행위 ②착오 ③처분행위 ④속취라는 독특한 인과관계가 필요하다. 사기죄는, 「교부죄」라고 불리는 범죄로 ‘교부’가 필요하다는 점에서 마찬가지로 점유를 빼앗는 범죄인 절도죄·강도죄와는 구별된다. 절도죄·강도죄는 남의 물건을 빼앗아 버리는 범죄이지만, 사기죄의 경우는 사람이 스스로 재물을 넘기는 범죄인 것이다. 그런 점에서 공갈죄와 비슷한 유형의 범죄 유형이라고 할 수 있다.

사기죄는 객체에 따라 1항 사기와 2항 사기로 갈린다. 각각 246조 1항과 동조 2항으로 나누어 규정되어 있는 것이 그 명칭의 유래이다. 1항 사기는 재물, 2항 사기는 재산상의 이익이 객체가 된다. 재물이란 타인이 점유하는 타인의 재물을 말하며, 재산상의 이익이란 재물 이외의 모든 이익이 해당 된다. 여기에는 적극적 이익(예를 들면, 채권의 취득, 서비스의 제공 등) 외에 소극적 이익(예를 들면, 지불해야 할 채무를 면하는 등)도 포함된다.

사기죄는 사람에 대해서만 성립한다. ①기피행위→②착오→③처분행위→④속취라는 인과관계가 필요하기 때문에, 착오에 빠지지 않는 사람에 대해서 사기죄는 성립할 수 없는 것이다. 즉, 기계에 대한 사기는 성립하지 않고, 절도죄를 구성하는 것에 지나지 않는다. 예를 들면, 주운 현금카드로 타인의 계좌로부터 금전을 인출하는 행위는, 절도죄라고 하는 것이 돼. 처분행위에 의해 피해자가 재물 또는 재산상의 이익을 상실하고, 사기행위자가 그것을 자유롭게 처분할 수 있는 지위를 획득함으로써 사기죄는 기수가 된다. 그리고 사기죄는 개별 재산에 대한 죄므로 피해자는 재산상의 손해가 발생해야만 한다.

해당 사기 범죄를 행한 자에 대해 일본 형법 제246조의2에서는 246조 1항과 2항에서 규정하는 사항과 더불어, 사람의 사무처리에 사용하는 컴퓨터에 허위의 정보 또는 부정한 지령을 하여 재산권의 득실 또는 변경과 관련된 부실한 전자적 기록을 작성하거나 재산권의 득실 또는 변경과 관련된 허위의 전자적 기록을 사람의 사무처리용으로 제공하여 재산상 불법의 이익을 얻거나 타인에게 이를 얻게 한 자는 10년 이하의 징역에 처한다고 규정하고 있다.

또한 해당 범죄로 획득한 것은 몰수(형법 19 조) 또는 추징(형법 20 조)되며, 범죄행위가 조직적으로 행해진 경우는 조직적범죄처벌법(組織的な犯罪の処罰及び犯罪収益の規制等に関する法律)에 의해 1년 이상의 유기 징역과 죄가 무거워진다(조직적범죄처벌법 3조 제1항 제13호). 또한, 사기죄에 대해서는 미수도 처벌되며(형법 250조) 또한 미성년자 등 지식과 사려가 부족하거나 상황 판단 능력이 불충분 한 자에 대하여 기망에 준한 행위로 인하여 재물의 교부 또는 재산상의 이익을 취하면 준 사기죄(형법 248 조)로 10년 이하의 징역에 처하게 된다.

2) 카케코「掛け子(架け子)」의 형사 책임

송금 사기의 실행범은, 피해자에게 전화를 걸어 기망하고, 착오에 빠지게 하여 계좌에 금전을 입금시킨다. 이러한 ‘보이스피싱’의 실행범은, ‘카케코’라고 불린다. 이들의 행위는 형법의 사기죄에 해당함은 틀림없으나 1항 사기와 2항 사기 중 어느 쪽에 해당하는 지에 대해서는 의견 대립이 존재한다.

1항 사기와 2항 사기의 차이는 객체가 물건인가(246조 1항) 재산상의 이익인가(동조 2항)이라는 점에 있다. 1항 사기로 보는 견해는 계좌에 입금되면 계좌 명의인은 그 금전을 자유롭게 처분할 수 있으므로 재물인 금전의 교부가 있었던 것이 된다고 논하고, 2항 사기로 보는 견해는 계좌에 입금되어도 그것만으로는 예금채권이라는 재산상의 이익을 취득했다는 것에 지나지 않는다고 논한다.

1항 사기설에는 계좌에 입금되어도 예금을 되찾을 때까지는 금전을 자유롭게 처분할 수 있는 것은 아니라는 비판이 쏠린다. 그러나 ATM기나 인터넷·뱅킹 등이

보급되어 있는 현재는, 금전이 계좌에 입금되면, 이것을 즉시 자재로 처분할 수 있다. 오히려 2항 사기설에 있어서 예금채권의 획득이라는 이론은 이론적으로는 명쾌하다고는 해도 감각적으로는 부자연스러운 측면이 있다. 예를 들어, 통신 판매에서의 결제를 생각하면, 송금이 종료된 단계에서, 자신은 금전을 지불하고, 가게는 금전을 취득했다고 느끼는 것이 자연스러울 것이다. 그렇다면, 예금 상태로 존재하는 금전이 ‘현물’에 해당하는가 하는 난점이 있지만, 1항 사기설은 충분히 설득력이 있다고 말할 수 있으며 최근 이와 관련한 실무에서도 1항 사기에 의한 처리가 많다고 여겨진다. 이와 같이 ‘카케코’에는 1항 사기죄가 성립한다고 생각할 수 있다.³¹⁵⁾

3) 다시코「出し子」의 형사 책임

송금 사기는, 금전이 계좌에 입금된 단계에서, 기수에 도달한다. 즉, 사기 기수죄가 성립해, 그 이후에 새롭게 관여한 사람에 대해서는, 사기죄를 물을 수 없다. 그러나 현실에는 실행범의 부탁을 받아 은행의 ATM기에서, 입금된 금전을 인출하는 사람이 존재한다. 이러한 인출책을 ‘다시코’라고 한다. 실행범이 수사기관에 잡히지 않도록 하는 것을 목적으로 하여 말단의 사람에게 행하게 하는 경우가 많다.

만일 ‘카케코’와 ‘다시코’가 사전의 의사를 교환하는 연락이 있으면, ‘다시코’는 사기죄의 공범, 공모 공동 정범이 된다. 문제는 그러한 사정이 없는 경우이다. 이러한 경우 구체적으로는 은행이 점유하는 현금을 대상으로 한 절도죄(형법 235조)의 성패가 문제가 된다.

최초로 검토해야 하는 것은 예금채권 취급이다. 예금채권이 무효라면 절도죄가 성립하는 것에는 문제가 없다. 그러나 민법상으로는 예금채권이 유효하게 성립되어 있다고 여겨지기 때문에, 이 점을 어떻게 생각할지가 문제가 되는 것이다. 여기

315) 松澤伸, “振込め詐欺を巡る諸問題”, 早稲田大学社会安全政策研究所紀要 5, 2012, 12-13면

에서는 이른바 오입금 사건 판결(최고재판소 2003·3·12 형집 57권 3호 322페이지)에 따르면 오입금을 원인으로 하는 입금일 경우에도 예금채권은 유효하게 성립하지만, 은행에는 반송 등의 조치를 취하는 방법이 있었으므로, 수취인은 오입금이 있었던 것에 대해 신의칙상 고지의무가 있으며, 고지의무를 위반한 부작위 사기죄가 성립한다고 판시하였다.

우선, 여기에서는 단순한 고지의무 위반을 가지고 사기죄의 성립이 인정되고 있는 것은 아님에 주의할 필요가 있다. 그렇지 않으면 고지의무 위반의 존재하지 않는 ATM 절도죄는, 일체 성립할 수 없게 될 것이기 때문이다. 본질적 문제는 고지의무 위반이 아니라 은행의 점유에 보호성이 인정될 것인가 어떤가이며, 2003년 결정도 그러한 관점에서 이해할 수 있다. 즉, 오입금이 발생한 은행에서는 오입금을 한 송금 의뢰인으로부터의 신청이 있으면, 수취인의 예금계좌로의 입금 처리가 완료된 경우라도 수취인의 승낙을 얻어 송금 의뢰 전의 상태로 되돌리는 반송이라는 조치를 취할 수 있지만, 여기에 수취인에게 대항할 수 있는 은행의 이익이 있으며, 따라서 은행의 점유에는 보호성이 인정된다고 할 수 있다. 이러한 이유로부터 2003년 판례는 사기죄의 성립을 긍정하고 있어, ATM에서 인출하는 경우에는, 절도죄가 성립하게 된다.

사기죄나 절도죄는 형법상 보호해야 할 점유의 침해가 있어야만 발생하는 것이며, 오히려 은행의 점유에 어떤 이익이 있는지가 결정적인 사정일 것이다. 이러한 점에서 은행의 점유에 이익이 있는 경우를 어느 한도에서 인정해야 할지가 중요한 문제가 된다. 보이스피싱에 대해서는 인출되는 금전이 「범죄 이용 예금 계좌 등과 관련한 자금에 의한 피해 회복 분배금의 지불 등에 관한 법률」, 이른바 「보이스피싱 사기 구제법」의 ‘이체 이용 범죄 행위’의 피해금에 해당하는 경우, 은행에 이익이 있다고 생각된다. 동법에 의하면, 송금 사기로 인해 입금된 금전에 대해서는, 은행이 피해자에 대해서 피해 회복을 실시할 의무를 지게 되지만, 그 반면, 은행의 점유가 보호되어야 한다.

덧붙여 ‘다시코’가 은행 창구에서 금전을 받았을 경우는, 상기의 이론을 전제로,

1항 사기죄가 성립하고, 또, 타인의 은행 계좌로 이체 송금했을 경우는, ‘컴퓨터 사용 사기죄’가 성립한다고 생각할 수 있다. 해당 행위가 피해자와의 관계에서 장물 등 운반죄(256조) 2항이 되지 않는지 문제가 될 수 있다. 기존에 거의 논의되지 않았으나 갑의 행위가 1항 사기로 구성된다면, 피해 금전은 ‘도난품 기타 재산에 대한 죄에 해당하는 행위에 의해 영득된 물건’이며, 장물 등 운반죄의 고의가 있는 한, 그 성립을 부정할 이유는 없다. 보이스피싱의 구성에 대해서 1항 사기와 2항 사기는 법정형에 있어서 차이는 없고, 어느 처리에서도 큰 지장은 없다고 말하기도 하지만, 여기에서는 큰 차이가 생길 수 있다.³¹⁶⁾

4) 우케코「受け子」의 형사 책임

최근의 일본의 송금 사기 사건에서는, 이른바 ‘우케코(수령책)’를 이용하는 경우가 증가하고 있다. 이것은, 은행 계좌를 개설하는 것이 점점 어려워지고 있는 점과 은행 ATM에 방범 카메라가 설치되어 있어, 붙잡힐 가능성이 높아지고 있는 것이 원인이라고 여겨진다. 이러한 수령책을 이용하는 방식은 은행계좌를 이용하는 것과는 달리 ‘우케코’가 금전을 받을 때까지는 사기죄는 기수에 이르지 않았다. 따라서 ‘우케코’에 대해서는 사기죄의 공범(공동정범)의 성립 가능성이 검토될 수 있다. 이른바 승계적 공범의 논란이다.

범죄 공동설을 철저히 한 경우(완전 범죄 공동설)나, 공동 의사 주체설에 의한 경우, 승계적 공동 정범의 성립이 긍정되기 쉽다. 완전범죄 공동설은 죄명의 완전한 일치를 요구하기 때문에, 후행자에 대해서도 선행자와 동일한 죄명으로 처벌한다. ‘카케코(연락책)’의 기만행위에 의해 피해자는 착오에 빠져 최종적으로 금전을 교부하고 있으므로, ‘카케코’에게는 사기죄의 공동 정범이 성립하는 것은 물론, 이것에 의사를 통해서 가담한 ‘우케코’에 대해서도, 같은 죄명, 즉 사기죄의 공동 정범이 성립한다고 하는 것이다. 공동 의사 주체설은 공범 현상을 공동 의사 주체에

316) 松澤伸, “振込め詐欺を巡る諸問題”, 早稲田大学社会安全政策研究所紀要 5, 2012, 14-17면

의한 범행이라고 생각함에 따라 중간부터 공동 의사 주체에 가담한 ‘우케코’에 대해서도 공동 의사 주체가 지는 사기죄의 공동 정범의 죄책이 추궁당하게 된다.

그러나 이러한 견해는 ‘우케코’가 스스로 영향력을 끼치지 않은 행위에 대해 책임을 묻는 것을 인정하기 때문에 책임주의에 반한다. 또는 연대 책임을 인정하는 것으로 비판받을 가능성이 있다. 순수하게 ‘우케코’의 행위만을 보면, 사기죄의 실행 행위의 일부를 담당하고 있다고는 해도, 기만행위는 행하지 않았기에 결국 점유이탈물 횡령죄가 성립하는 것이 아닌가하는 의견이 있다. 이러한 결론은, 이른바 인과적 공범론에 의해서 증명된다. 인과적 공범론은 어디까지나 갑이 스스로 영향력을 미치고 있는 행위에 대해서만 책임을 지운다는 생각에 기초하지만, 이를 철저히 하고, 승계적 공동 정범을 일체 부정한다는 결론에 이를 수 있다. 즉, 인과적 공범론에 따르면, 공범이 일부의 실행밖에 분담하지 않았음에도 불구하고 전부 책임을 지는 것은 다른 공범자에게 인과적인 영향력을 미치고 있기 때문으로, 그러한 인과적인 영향력이 미치지 않은 행위로부터 발생한 결과에 대해서는 책임을 질 필요가 없다고 해석된다. 그리고 인과성은 시간을 역행하는 일은 없으므로, ‘우케코’가 인과성을 가지고 영향력을 미칠 수 있는 것은 어디까지나 ‘우케코’가 가담한 후의 공범 행위에 한한다. 그러면, ‘우케코’는, ‘카케코’가 행한 기만행위, 피해자가 빠진 착오에 대해 책임을 지지 않는다. 즉, 승계적 공동 정범은 부정되어 ‘우케코’에게 사기죄는 인정되지 않고, 기껏해야 점유 이탈물 횡령죄가 인정되는 것에 지나지 않게 되는 것이다. 행위 무가치론에 서든, 결과 무가치론에 서든, 법익 침해(또는 그 위험)를 일으키지 않는 한, 범죄가 성립한다고 해석해서는 안 된다. 그렇다면, 인과적 공범론에 근거한 승계적 공동 정범 부정설에는, 지극히 설득력이 있다. 그러나 이러한 결론은 사회적 인식으로 볼때 불편한 점이 있으며 대다수가 ‘우케코’에 대해서는 사기죄를 긍정하는 것이 타당하다고 생각한다.

이러한 가치 판단으로부터, 중간설이 주장되고 있다. 강도죄 등의 결합범, 혹은 사기죄 등의 결합범과 비슷한 유형의 범죄의 경우나, 결과적 가중범의 경우, 예를 들어 선행자가 폭행을 가해 후행자는 재물 탈취의 단계부터 가담했을 경우, 혹은

선행자가 기만행위를 하고 피해자가 착오에 빠진 후에, 후행자가 가담하여 재물을 가로챘을 경우 등에 있어서는 후행자는 선행자의 행위를 적극적으로 이용하고 있는 것으로 이러한 경우에게까지 승계적 공동 정범을 부정하는 것은 결론으로서 타당하지 않다고 여겨진다.

다만, 이 견해의 문제점은 승계적 공동 정범이 인정되는 기준이 명확하지 않다는 데 있다. 이에 대해서는 구성요건의 일부에 개입해 범죄를 실현했을 때, 혹은 행위의 특성상 선행자의 행위의 일부를 전제로 하여 스스로의 행위를 행했을 때 등의 기준이 마련되고 있어 이를 바탕으로 참고해 나갈 수 있다. 이처럼 보이스포싱의 송금 사기에서 ‘우케코’의 형사 책임에 대해 여러 견해가 있지만, 결론적으로는 상기 어느 기준에 의해서도, ‘우케코’의 사기죄의 성립을 긍정해야 한다는 것이 일반적으로 받아들여지고 있다.³¹⁷⁾

5) 조직범죄처벌법의 적용

보이스피싱 사기범죄는 일본 형법상 사기죄에 해당하며 일반적으로 형법 246조에 의해 10년 이하의 징역에 부과된다(복수 행위가 기소되어 병합죄로 가중되는 경우 상한은 징역 15년). 그러나 대부분의 보이스포싱이 조직적으로 이루어진다는 점에서 일본에서는 오랜 기간 보이스포싱의 조직범죄처벌법의 적용이 논의되어 왔다. 범죄를 조직적으로 행했을 경우에는 일본에서는 조직범죄처벌법을 적용하여 더욱 무거운 형벌(징역 20년 이하)을 선고한다. 보이스포싱에 대해 조직범죄처벌법이 적용된 사례에서는, 주범에 대해 징역 20년의 판결이 내려진 사례가 있으며(도쿄 지방 법원 2010년). 해당 사례에서는 피해액이 약 1억 4,600만엔으로 그 규모가 상당하였다. 조직적으로 이루어진 보이스포싱으로 인해 피해액이 1,000만엔 정도일 경우 주범격에 해당하면 징역 9년 6개월을 선고받는 사례가 있으며(오사카 고등법원 2017년), 조직범죄처벌법이 적용되는 경우 주범격은 가벼워도

317) 松澤伸, “振込め詐欺を巡る諸問題”, 早稲田大学社会安全政策研究所紀要 5, 2012, 17-19면

징역 6년 이상은 선고받는다. 범행이 미수에 끝난 경우에도 징역 2년 정도가 형량되며, 단순 말단 준비역이나 관여자의 경우에도 통상적으로 징역 1년 6개월에서 2년의 실형에 처한다.³¹⁸⁾

나. 범죄수익 이전 방지법

종래 일본의 자금세탁 대책의 핵심이 되는 법률은 「본인확인법」과 「조직적범죄처벌법」 두 가지였다. 그러나 2003년에 개정된 돈·세탁(돈세탁) 대책에 있어서 국제 협력을 추진하기 위해 설립된 정부 간기구 FATF의 ‘The 40 Recommendations on Money Laundering’에서 금융기관뿐만 아니라 비금융업자(부동산·귀금속·보석 등 취급업자 등), 직업 전문가(변호사·공인회계사 등)도 ‘규제해야 할 대상’으로 추가됨에 따라 일본 정부의 국제조직범죄 등 국제테러대책추진본부는 「본인확인법」과 「조직적범죄처벌법」 제5장을 일원화하고 대상업종을 확대하는 법안을 작성하고 FIU를 금융청에서 국가공안위원회로 이관하는 등의 결정을 하였다.

이로 인해 2007년 4월 1일 일부 시행되고 이듬해 3월 1일 전면 시행된 「범죄수익이전방지법(犯罪による収益の移転防止に関する法律)」은 범죄로 인한 수익이 조직적인 범죄를 조장하기 위하여 사용됨과 동시에 범죄로 인한 수익이 이전되어 사업활동에 이용됨으로써 건전한 경제활동에 중대한 악영향을 미치고 범죄수익의 이전이 그 박탈이나 피해회복에 충당함을 곤란하게 함에 따라 범죄로 인한 수익의 이전을 방지하여 국민 생활의 안전과 평온을 확보함과 동시에 경제활동의 건전한 발전에 기여함을 목적으로 하고 있다.³¹⁹⁾

318) 弁護士法人中村国際刑事法律事務所, 「刑事法のひろば」に関する刑事弁護コラム, <https://www.t-nakamura-law.com/column/> (2020.12.15. 최종확인)

319) 警察庁刑事局組織犯罪対策部組織犯罪対策企画課犯罪収益移転防止対策室, “犯罪収益移転防止法の概要”, 2020.04.01.

동 법이 금융기관 등의 거래 시 확인 및 거래 기록 보존 및 혐의 거래 신고 등의 의무를 정하고 있기 때문에 은행은 고객에게 거래하실 때 본인임을 확인 등의 확인이 의무화되었다. 또한, 동 법에 따라 보이스피싱과 같은 특수 사기사건 등에 타인 명의의 예금계좌 등이 악용되어 그 부정이용을 방지하며, 계좌를 양도하는 행위, 계좌를 양수하는 행위, 또는 이를 권유하는 등의 행위는 1년 이하의 징역 또는 100만엔 이하의 벌금 또는 병과된다. 또한, 양도 행위 등을 업으로 한 경우에는 3년 이하의 징역 또는 500만 엔 이하의 벌금 또는 병과 하고 있다.

다. 휴대전화 부정이용 방지법

2005년 제정된 「휴대전화 부정이용 방지법 (携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律)」은 이른바 보이스 피싱 사기 등의 휴대 전화의 부정 이용을 방지하기 위해 휴대전화 계약 시 본인확인 의무 나 휴대전화의 무단 양도의 금지 등을 내용으로 하는 법률이다.

휴대 전화의 부정 이용 방지를 목적으로 하는 「휴대 전화 부정 이용 방지법」의 개요는 다음과 같다.

〈표 6-9〉 일본의 휴대전화 부정이용 방지법의 주요 내용

연번	주요 내용
1	· 휴대 음성 통신 사업자 (이동 통신사 및 PHS 사업자)에게 휴대 전화 등 (휴대 전화 및 PHS) 계약 체결 시 및 양도 시 계약자의 본인확인을 의무화
2	· 휴대폰 대여업자에 대해서도 운전면허증 등의 신분증을 확인하는 것에 의한 계약자의 본인확인을 의무화
3	· SIM 카드에 대해서도 통화 가능 단말 설비와 동일한 규율을 부과
4	· 계약자가 본인확인 시에 허위의 이름 등을 신고하는 것을 처벌의 대상으로 함

5	· 휴대 음성통신 사업자에게 무단으로 업으로서 유상으로 통화 가능한 휴대폰 등을 양도하는 것을 처벌의 대상으로 함
6	· 자기가 계약자가되어 있지 않은 통화 가능한 휴대폰 등을 양도하는 경우 처벌의 대상으로 함
7	· 상대방의 이름 등을 확인하지 않고 업으로서 유상으로 통화 가능한 휴대폰 등을 대여하는 것을 처벌의 대상으로 함
8	· 통화 가능한 휴대폰 등이 일정한 범죄에 이용된 경우 등에서 경찰서장으로부터의 요구를 받고 휴대 음성통신 사업자가 가입자 확인을 할 수 있음
9	· 휴대 음성통신 사업자는 가입자가 본인확인에 응하지 않는 경우 등에는 역무의 제공을 거부할 수 있음
10	· 국가 공안위원회는 휴대전화 사업자에 대한 정보의 제공과 입금 사기 대책에 대한 국민의 이해를 얻기위해 필요한 조치를 강구해야 함

이처럼 용역 제공 계약에 관한 통신 가능한 단말 설비 등 (통화 가능한 휴대폰 등)를 타인에게 양도하고자하는 경우에는 친족 또는 생계를 같이하고있는 자에게 양도하는 경우를 제외하고는 미리 휴대 음성 통신사업자 (통신사)의 동의를 얻어야 하며, 업으로서 유상으로 통화 가능 단말 설비 등을 양도 한자는 2년 이하의 징역 또는 300만엔 이하의 벌금 또는 병과 한다.

라. 송금사기구제법

「범죄 이용 예금 계좌 등에 관한 자금에 의한 피해 회복 분배금의 지급 등에 관한 법률(犯罪利用預金口座等に係る資金による被害回復分配金の支払等に関する法律)」 통칭 「송금사기구제법」은 2007년 제정되어 송금 사기를 비롯한 특수 사기 등의 피해자의 신속한 피해회복을 도모하기 위해서, 범죄 이용 예금 계좌 등과 관련되는 자금에 의한 피해회복 분배금의 지급 등에 관한 법률로 2008년 6월부터 시행되었다. 일반적으로 대상이 되는 범죄 행위로는 보이스피싱, 가공 청구 사기 대출 보증금 사기, 환급금 등 사기 외에도 사채업자와 미공개 주식 매입에 따른 사기 등이 해당한다. 피해를 입은 사람은 법에서 정한 절차를 거쳐 실권한

입금 계좌의 잔액을 한도로 피해회복 분배금의 지급받는 방법으로 피해 회복을 받을 수 있다.

4. 대응 정책

가. 범죄대책각료회의 보이스피싱 대책 플랜

일본은 2003년 9월 2일 각료회의를 통해 ‘세계에서 가장 안전한 나라, 일본『世界一安全な国 `日本』’ 을 목표로 관계 추진본부 및 관계 행정기관의 긴밀한 연계를 확보함과 동시에 효과적이고 적절한 대책을 종합적이고 적극적으로 추진하기 위해 ‘범죄대책 각료회의’ 를 수시로 개최할 것을 정하였다. 해당 회의는 전 각료로 구성되며 필요에 따라 기타 관계자의 출석을 요구하고 있으며, 내각총리대신 주재로 이루어진다. 특히 총기대책추진회의, 약물남용대책추진회의, 인신거래대책추진회의 및 재범방지대책추진회의를 수시로 개최하고 있다.³²⁰⁾ 특히 2018년의 특수사기 인지 건수는 약 1만 6,500건, 피해액은 약 364억 엔으로 높은 수준으로 추이하고 있어 여전히 심각한 상황에 있는 특수사기 피해 전체에서 고령자가 차지하는 비율이 78.1%를 기록하고, 특히 ‘보이스피싱(오레오레 사기)’ 는 96.9%에 이르는 등 고령자의 피해방지가 매우 중요한 과제로 떠오르고 있다. 최근에는 노인에게서 전화로 자산상황을 알아낸 뒤 범행에 이르는 수법의 강도사건도 잇따라 발생함에 따라 2019년 6월 25일 범죄대책각료회의에서 ‘보이스피싱(오레오레 사기) 대책 플랜’ ³²¹⁾을 발표하게 되었다.

1) 피해방지대책의 추진

320) 首相官邸, 犯罪対策閣僚会議, <http://www.kantei.go.jp/jp/singi/hanzai/> (2020.12.15. 최종확인)

321) 犯罪対策閣僚会議, “オレオレ詐欺等対策プラン”, 2019.06.25.

가) 전 부처에서의 홍보활동 강화

① 가족 간의 유대감의 중요성 등을 호소하는 홍보계발 활동의 전개

특수사기 피해를 당하기 쉬운 고령자뿐 아니라, 저 연령층 세대에 대한 활동도 강화하고, 가족의 유대감을 강화하여, 가족 간에 평소부터 서로 연락함으로써 피해를 방지해 나가려는 사회적 분위기 형성 등을 목표로, 폭넓은 세대에 대해 높은 발신력을 가진 저명한 인사를 통해, 각 지방공공단체 등의 모든 공적 기관은 물론, 경제단체를 비롯한 사회의 모든 분야와 관련한 각종 단체, 민간 사업자 등의 폭넓은 협력을 얻어 다양한 매체를 활용하여 특수사기 피해 방지에 임하도록 홍보계발 활동을 전개한다.

② 모든 기관·단체·사업자 등의 웹사이트, SNS 등에 의한 주의 환기

2012년도부터 내각부 대신관방 정부홍보실이 경찰청, 금융청 및 소비자청과 제휴해 각 기관에서 실시하고 있는 특수사기 피해방지의 정부 홍보와 함께 경찰청, 금융청, 소비자청, 법무성 등 각 부처나 각 지방 공공단체를 비롯한 모든 공적기관은 물론, 각종 단체나 민간 사업자 등과 관련한 웹사이트나 SNS에 의한 각종 사기피해 방지에 관한 주의 환기를 추진한다.

③ 고령자와 접할 기회가 많은 단체·사업자 등에 의한 주의 환기

각 지방공공단체는 물론, 민생위원, 노인정 등의 복지 관련 단체 등이나 간호서비스사업자, 보험사업자, 택배 사업자, 기타 소매사업자, 버스·택시업자 등의 고령자가 일상생활에서 접점을 갖는 모든 기관·단체·사업자 등과도 연계하여 주의 환기를 추진한다. 또한, ‘소비자안전확보지역협의회’를 활용해, 관계 기관이 제휴해 주의 환기·홍보 계발을 추진하는 것과 동시에, 특수사기와 관련한다고 생각되는 정보의 공유 등을 통해, 소비 생활 센터와 경찰의 제휴 강화를 도모한다.

④ 아동이나 손자 세대를 대상으로 한 직장이나 학교에서의 홍보계발 추진

가족 간 피해방지의식을 높이기 위해 각 직장에서의 교육, 연수 등과 함께 학교 등에서의 방법 지도 등 주로 자녀나 손자 세대를 대상으로 한 모든 교육, 연수 기회를 통해 특수 사기피해 방지 홍보계발을 추진한다.

나) 자동 응답 전화 기능의 활용 등의 촉진 (경찰청, 소비자청)

① 부재중 전화 기능의 활용 등에 관한 홍보 추진

범인으로부터의 전화를 직접 받는 것을 방지하기 위해 고령자 집의 고정전화를 항상 자동 응답전화로 설정하는 것이나, 스팸 전화 방지 기능을 가지는 기기의 활용의 유효성에 대해서 홍보계발을 추진한다.

② ‘우량 스팸 전화 방지 기기 권장 사업’ 을 통한 기기 보급 촉진

「우량 스팸 전화 방지 기기 권장 사업」을 실시하고 있는 공익재단법인 ‘전국방범협회연합회’와 제휴하여, 스팸 전화 방지 기능을 가지는 기기의 보급을 촉진한다.

다) 금융기관과 연계한 피해 미연 방지 (경찰청, 금융청)

① 금융기관 창구의 전달 등의 추진

고액의 환급 등을 신청한 고령의 고객에 대한 금융기관의 요청을 통해 피해를 미연에 방지하기 위해, 고객 대응시의 체크리스트를 금융기관에 제공하며, 금융기관 등의 직원과 공동으로 실시하는 훈련 등에 의해 대응을 추진한다. 또한, 금융기관 창구에서의 안내와 함께 각 금융기관이 정한 일정한 기준(고객의 연령, 환급금액 등)에 근거하여 경찰에 전건 통보하는 대응을 추진한다.

② ATM 이용 제한 등의 추진

금융기관과 연계하여 일정연수 이상에 걸쳐 ATM에서의 이체실적이 없는 고령

자의 ATM 이체한도액을 0엔 또는 극히 적은 금액으로 하는 대응(ATM 이체제한) 및 고령자의 ATM 인출한도액을 소액으로 하는 대응(ATM 인출제한)을 추진하고 금융기관의 예금계좌 모니터링을 강화한다.

라) 편의점 등과 연계한 피해 미연 방지 (경찰청, 금융청, 소비자청, 경제산업성)

① 편의점에서의 피해 방지 추진

전자화폐형이나 수납대행 이용 수법에 대한 대책으로서 일반사단법인 ‘일본 프랜차이즈 체인협회’, ‘각 편의점 사업자’ 와 제휴하여 전자화폐 구입 희망자나 수납대행 이용자에게 보이스피싱 관련 사안을 안내하며, 점포 판매 선반이나 계산대·단말기 화면을 통한 주의 환기 표시 등의 대응을 추진한다.

② 전자화폐 발행 사업자 등의 피해 방지 추진

일반사단법인 ‘일본자금결제업협회’, ‘전자화폐 발행사업자’, ‘수납대행사업자’ 등과 연계하여 고객에 대한 주의 환기를 비롯한 피해방지와 관련된 대응을 추진한다.

마) 택배사업자와 연계한 피해 미연방지 (경찰청)

① 피해금 배송지 리스트를 활용한 피해 방지 추진

택배 사업자와 제휴해, 과거에 범행에 사용된 피해금 송부처의 리스트를 활용하고, 수상한 택배의 발견이나 경찰에의 신고라고 하는 대응을 추진한다.

② 수화물 수령 시 주의 환기

택배 사업자가 고객으로부터 수화물을 받을 때, 운송약관에 근거한 취급할 수 없는 현금이 택배에 재중하고 있지 않은지의 말 등을 통해 주의 환기를 추진한다.

바) 압수명부를 활용한 주의 환기 (경찰청)

특수 사기 등의 수사 과정에서 입수한 명부의 등재자에 대해, 경찰관에 의한 호별 방문이나 경찰이 민간 위탁한 콜 센터로부터의 전화 연락 등을 실시해, 주의 환기나 구체적인 예방 대책 등의 주지를 도모하는 등의 대응을 추진한다.

2) 범행도구에 대한 대책

가) 전화 전송 서비스를 통한 고정 전화번호 악용을 위한 대책 (경찰청, 총무성)

특수사기의 범행에서는, 전화 전송의 구조를 악용해, 상대방에게 고정 전화 번호를 표시시켜 전화를 걸거나, 관공서를 가장한 전화번호를 통해 전화를 걸거나 문자 등을 보내는 수법이 많이 사용되고 있다. 이것에 대응하기 위해, 특수사기에 이용된 고정 전화번호의 이용 정지를 비롯한 실효성이 있는 대책을 강구 한다.

나) 전화 전송 서비스사업자에 대한 지도 감독 강화 (경찰청, 총무성)

특수사기에 이용되는 전화 전송 서비스를 제공하는 사업자에 대해서는 범죄에 의한 수익의 이전 방지에 관한 법률(1997년 법률 제22호, 이하 ‘범수법’) 제2조 제2항에 규정하는 특정 사업자로서 거래 시 확인 등의 의무 이행이 요구되고 있다. 지금까지도 해당 의무의 적절한 이행을 확보하기 위해 범수법에 근거한 특정 사업자에 대한 보고 징수 등을 하고 있지만, 의무 위반이 인정되는 특정 사업자에 대해 시정 명령을 실시하는 등 특수사기 범행에 이용되는 전화 전송 서비스사업자에 대한 지도 감독을 강화한다.

다) 범행에 이용되는 휴대전화에 대한 대책 (경찰청, 총무성)

특수사기의 범행에 이용되는 MVNO 등의 휴대전화(알뜰폰)에 대해서 휴대 음성통신 사업자에 의한 계약자 등의 본인확인 및 휴대 음성통신 역무의 부정한 이용의 방지에 관한 법률(2005년 법률 제 31호)에 근거한 계약자 확인의 요구, 역무 제공 거부에 관한 경찰로부터 사업자에 대한 정보 제공을 추진하는 것 외에 사업자와 제휴해, 특수사기에 이용된 휴대전화의 서비스를 정지하는 대응을 추진한다.

라) 경고 전화 사업 추진 (경찰청)

범행에 이용된 전화에 대해서, 반복해 전화를 걸어 메시지를 흘림으로써, 전화를 사실상 사용할 수 없게 하는 경고 전화 사업을 실시한다.

마) 범행에 이용된 예금계좌 동결 등 (경찰청, 금융청)

특수사기 범행에 이용된 예금계좌에 대해 금융기관에 대한 신속한 계좌 동결 의뢰를 실시하고, 동결된 예금계좌 명의자 명단을 경찰청이 작성해 일반사단법인 ‘전국은행협회’ 등에 제공함으로써 불법계좌 개설 방지를 추진한다.

3) 효과적인 단속 등의 추진

가) 범죄자 그룹 등에 대한 다각적·전략적 단속 추진 (경찰청)

특수사기 사건의 배후에 있다고 생각되는 폭력단, 준 폭력단, 불량 외국인, 폭주족, 불량소년그룹 등의 범죄자 조직 등을 약화시키고 특수사기 억제를 도모하기 위해 각 부문에서 다각적인 단속을 추진함과 동시에 적극적인 정보 수집을 실시하는 등, 그 활동 실태나 특수사기에 대한 관여 상황 등을 해명한다.

나) 범행거점의 적발 등에 의한 실행범 검거 및 수사 조직에 의한 중추 피의자 검거 추진 (경찰청)

모든 정보를 활용하여 범행거점의 발견에 힘쓰고 범행거점의 적발을 통해 관계자 등을 검거하는 동시에 현장 설정이나 피해 발생 전후의 초동수사를 철저히 하여 ‘우케코(수령자)’, ‘다시코(출납자)’ 등을 검거한다. 또한, 추가 수사의 강화를 통해 중추 피의자 등의 검거를 추진한다.

다) 예금계좌나 휴대전화의 부정매매와 같은 특수사기를 조장하는 범죄 검거 등의 추진 (경찰청)

예금 계좌나 휴대전화의 부정매매와 같은 특수사기를 조장하는 범죄 검거나 악질적인 범행 톨 제공 사업자 등에 대한 단속을 추진한다.

라) 특수사기에 가담한 소년의 재비행 방지를 위한 대처 추진 (경찰청, 법무성)

소년원 등 관계 기관과 연계하여 비행 방지 교실을 개최하는 등 소년의 재비행 방지를 위한 대응을 추진한다.

나. 우량 스팸 전화 방지 장치 권장 사업

‘전국방범협회연합회’에서는 특수사기 등 피해방지를 위해 2017년 4월부터 ‘우량 스팸 전화 방지기기 권장사업’을 시작하였다.³²²⁾ 대부분의 사람들이 특수사기와 악질 상법의 종류 및 수법을 알고 있음에도 전화를 받음으로써 속는 경우

322) 全国防犯協会連合会, “公益財団法人全国防犯協会連合会推奨「優良迷惑電話防止機器」(優良防犯電話)について”, <http://www.bohan.or.jp/suishou/denwa.html> (2020.12.15. 최종확인)

가 많다. 지금까지 경찰, 행정, 매스미디어 및 방범협회 등의 자원봉사자가 특수 사기 박멸을 위한 다양한 대책을 추진해 왔지만 여전히 인지 건수, 피해액 모두 높은 수준으로 드러났으며, 이러한 현실을 보면 특수 사기 피해를 방지하기 위한 방범 홍보 및 계몽 활동의 효과에는 한계점이 있다는 것이 드러났다. 이에 따라 보이스피싱 피해를 방지하기 위해 전화의 착신 시 경고 음성을 발하는 기능과 통화 중 자동으로 녹음 기능 등을 갖는 장치인 스팸 전화 방지 장치를 노인 주택에 설치하는 방안이 대두되었으며, 이런 가운데 공익 재단법인 전국방범협회연합회는 2017년부터 우량 스팸 전화 방지 장치 권장사업을 전개하고 스팸 전화 방지 기기의 보급 촉진에 노력하고 있다.

우량 스팸 전화 방지기기 권장 규정(優良迷惑電話防止機器推奨規程)에 따르면 우선 전화기 또는 휴대전화에 쉽게 장착할 수 있는 외장 기기로서 전화 수신 시 전화 상대방에게 경고 음성을 발하는 기능을 가지며, 통화 중 자동으로 통화 내용을 녹음하는 기능을 가지거나 스팸 전화 번호 데이터베이스(경찰, 지자체 등으로부터 제공되는 스팸 전화번호 데이터베이스이며, 수신 거부를 판별하기 위한 전화번호 정보가 순차적으로 축적되는 DB)에 등록된 정보를 통해 스팸 전화번호를 자동 판별하여 수신 거부 또는 수신 램프 등으로 경고하는 기능이 포함되어야 한다. 또한, 기기의 내구성이 보장되어야 하며, 고령자 등이 사용함에 있어 조작이 용이해야 한다.³²³⁾ 이러한 기준에 충족하는 기기에 대해서는 연합회 홈페이지를 통해 업데이트되어 공표되고 있다.

323) 島田 重夫, “特殊詐欺等対策優良迷惑電話防止機器(優良防犯電話)”, 日防設ジャーナル 2018年爽秋号, 2015, 1-5면.

다. AI 기술을 활용한 보이스피싱 경고

NTT, NTT동일본, NTT서일본, NTT커뮤니케이션의 4개사는 2019년 8월 29일 보이스피싱 등의 특수 사기 전화를 해석하는 AI의 데모를 매스컴 대상으로 실현하였다. 전화의 음성을 클라우드 상의 AI가 실시간으로 해석하여, 사기의 혐의가 있으면 본인이나 친족에게 주의를 환기시키는 메시지를 보내는 구조이다. 도쿄도 내 실증 실험을 거쳐 2020년 가을까지 실용화를 추진할 계획이다. 가정에서 사용되고 있는 전화기에, 대화를 녹음해 클라우드에 송신하는 ‘특수 사기 대책 어댑터’를 접속하여 전화를 발신할 때에는 대화를 녹음한다는 내용을 전하는 안내 문구를 내보낸 후 음성 데이터를 클라우드 상의 음성인식 엔진으로 전송하게 된다. AI의 해석·판정에 대해서는 경찰과 제휴하여 특수 사기범이 자주 사용하는 최신의 용어를 사용해 학습시켜 정확도를 높이고 있다. 녹음된 데이터는 이용자 전화에 설치하는 어댑터 내부에 보존되어 경찰의 수사에도 도움을 줄 것으로 기대된다.

해당 실증 실험을 통해 현재 이용자 및 행정 기관의 요구사항을 모집하고 있으며, 서비스 내용에 반영시키는 것 외에 어댑터 설치나 설치 후의 애프터 서비스 등 운용 면의 개선도 실시 중에 있다. 실제 상용화 단계에서는 미리 전화번호부에 등록되어 있는 사람과의 전화는 녹음하지 않도록 하는 등 운용면의 개선이 예상된다.³²⁴⁾

이처럼 전화음성을 AI를통해 분석하는 대응 기술 이외에도 은행의 ATM 카메라 솔루션에 AI를 탑재하여 보이스피싱 사기에 대응하는 실증 연구가 진행되고 있다.

324) 坪田弘樹(2019.8.29.),

“「その電話、詐欺かも」AIが警告、NTTが2020年に実用化へ”,

<https://businessnetwork.jp/Detail/tabid/65/artid/6918/Default.aspx> (2020.12.15.

최종확인)

[그림 6-2] 일본의 AI 카메라 솔루션을 활용한 보이스피싱 대응



2020년 7월 13일 주식회사 비즈라이트 테크놀로지는 주식회사 J. VC켄우드와 공동개발을 진행중인 엡지AI카메라의 프로토타입을 활용하여 호쿠요 은행의 일부 지점에서 보이스피싱을 미연에 방지하는 솔루션 실증을 개시하였다. 해당 솔루션은 ATM앞에서 전화를 걸고있는 자세를 골격 추정으로 검출하여 은행 내 직원에게 경고하고 직원이 상황에 따라 적절한 대응을 통해 보이스피싱을 통한 계좌이체를 미연에 방지하기 위한 것이다.

특히 본 실증에서 사용하는 엡지AI 카메라는 고객의 프라이버시를 고려하여 영상녹화 및 음성녹음을 일절 하지 않은채 엡지AI에 의한 딥러닝 처리를 실시간 진행한다. 문제가 검출되었을 경우 구내직원에게 대한 통지는 서브기가대를 이용한 무선으로 실시하므로 은행측에서는 별도의 배선 공사가 불필요하며, 은행의 기존 네트워크도 이용하지 않으므로 기존의 보안 수준을 취약하게 만들지도 않는다는 장점이 있다. 향후에는 무인ATM 코너나 편의점 등의 ATM에서의 검출, 통지에 대해 검증을 진행하는 동시에, 구내직원에게 의한 말을 거는 방법 등 현장에 있어서의 방법 시책에 대하고 검토를 진행시켜 본격 도입을 추진할 계획에 있다.³²⁵⁾

325) 株式会社ビズライト・テクノロジー(2020.7.1.),

제4절 중국의 대응체계 및 법제

1. 범죄 동향

중국에서 전화를 이용해 현금이체를 시키는 범죄를 ‘전화사편(电话诈骗: 디엔화짜피엔)’이라고 한다. 중국에서 전화금융사기 피해는 주로 여성이 70% 정도라고 하며 정보에 취약한 사람들이 많이 당한다고 한다. 2014년 중국 전역에서 발생한 전화금융사기는 51만 건, 피해액은 3조 6,094억 원 정도로 추정되고 있다.³²⁶⁾ 중국은 전화금융사기를 형법 제266조의 재산침범 사기죄 혹은 제192조의 금융사기죄를 적용해 처벌한다. 중국은 주로 예방대책 홍보강화 정책을 쓰고 있다. 하나의 예로써 광둥성 중산시가 추진하는 전화사편(电话诈骗: 디엔화짜피엔) 예방대책을 보면 다음과 같다. 대대적인 선전활동을 통하여 시민의 방법의식을 강화, 비밀보호의식을 강화하고 정보유출을 방지, 안전감독관리를 강화하고 상호협력하여 전화금융사기를 적발, 그리고 과학기술수단을 적극 이용하여 수사와 처벌을 강화하여 억제하는 것 등이다.³²⁷⁾

특히, 2020년 들어 중국의 공안기관들은 허위 대출 앱을 조작해 수수료, 보증금을 대신 내준다는 이유로 대출 의향이 있는 계층에 대해 통신 사기를 자행한 사례를 다수 적발하였다. 공안부는 이를 중시해 공작반을 별도로 편성해 이 같은 불법 범죄 활동에 대한 전투를 벌이고 특별 수사를 실시고 있다. 2020년 5월 7일 베이

“AIで振り込め詐欺を検出、通知するカメラソリューションの実証を北洋銀行の店舗で7月13日から開始”,

https://bizright.co.jp/pdf/2020/press_release_20200701.pdf (2020.12.15.

최종확인)

326) 금융감독원 보도자료, “일본의 보이스피싱 피해실태와 예방노력 및 시사점”, 2016.9.22.자

327) 홍성삼, “피싱 사기범죄에 대한 인터폴 및 국가별 대응정책 비교연구”, 원광대학교 경찰학연구소, 경찰학논총 14(1), 2019, 118-119면

징(北京), 허베이(等北), 상하이(上海), 장쑤(江苏) 등 15개 성시(省市) 공안기관이 일제히 집중 수사에 나섰으며, 대부업체의 인터넷 사기 단속을 위한 불법 문자 메시지 플랫폼 57개를 적발하였고, 798명을 검거해 휴대전화와 은행 카드, 컴퓨터 등 사기 범행에 사용된 물건을 압수하는 등 대대적인 수사를 펼치고 있다.³²⁸⁾

2. 대응 체계

유일한 전국 공안기관인 공안부는 통신 네트워크의 신종 위법 범죄를 단속하는 임무를 수행하고 있다. 이와 관련하여 특히 베이징시 공안당국에서는 전국 최고로 반(反)사기 센터를 설립하였으며, 2017년 4만 건의 사기 피해를 막고 19억 8000만 위안의 피해를 막아 보이스피싱 사기 등의 피해를 5년 만에 가장 낮은 수준으로 만들었다. 베이징시 공안국 형사총대 반(反)사기 센터에는, 당일의 통신 사기 차단 주의보가 실시간으로 표시되고, 경찰의 접수현황 등이 기록된다. 해당 센터의 사건 정보처리 대응실에서는, 수십 명의 근무자가 플랫폼에 따라 실시간으로 검사하여, 속고 있는 것으로 의심되는 피해자에게 전화를 걸어 송금 등의 행위를 만류하고 있다. 피해자 중 일부가 해당 센터의 조언을 듣지 않으면 직원은 관할 구역의 경찰서에 연락하여 협력을 요청하고 있다. 또한, 8개 은행과 협력관계를 구축하고 기업과 제휴하여 보호망을 형성하고 있다.

반(反)사기 센터에서 사기를 당하는 사람에게 주의를 촉구하는 한편, 사기범의 계좌를 동결하고 사기당한 사람의 송금을 제한하는 등의 조치에 더욱 집중하고 있다. 시 공안국은, 시 은행 규제국과의 커뮤니케이션 제휴를 계속해서 강화하고 있으며, 2017년말에는, 중국 은행, 북경 은행 등 8개 은행과 함께 반(反)사기 센터에 정착하여 보이스피싱 범죄 퇴치의 새로운 돌파구가 열렸다.

이와 같은 은행과 연동 외에도, 베이징시 반(反)사기센터는 차이나모바일, 차이

328) 新华社(2020.5.7.), “公安部打击贷款类电信网络诈骗犯罪集群战役抓获犯罪嫌疑人798名”, http://www.gov.cn/xinwen/2020-05/07/content_5509605.html (2020.12.20. 최종확인)

나유니콤, 차이나텔레콤과 직접적인 연계를 맺고 있어, 보이스피싱 사기범의 통신 흐름을 직접 차단할 수 있다. 베이징시 공안국은 우선적으로 경찰과의 합작을 실시하고, 텐센트·아리·바이두·360 등의 기업을 센터에 입주시킴으로써, 그들과 합작하여 시스템을 개발, 베이징시에 촘촘한 보호망을 형성하고 있다. 2017년 베이징시 공안국은 통신 및 네트워크 사기 범죄를 단속하여, 베이징과 전국 전기 통신 인터넷 사기 사건 및 범죄 사건을 해결하고 있다. 범인 검거는 2016년 대비 각각 50%, 30%씩 상승해 3년 연속 사건 해결, 범인 검거, 사건 발생, 군중 피해 감소라는 '2상승, 2하락'이라는 작업 목표를 달성하였다.³²⁹⁾

3. 대응 법률

중국에서 사기 범죄는 불법 소유, 가상의 사실을 꾸며내거나 진실을 은닉하기 위해 대량의 공공 및 사유 재산을 기만하는 행위를 말한다. 특히 중화인민공화국 형법 제 266조는 일반적인 재산의 편취에 대해 다루고 있으며, 공공과 개인의 재물을 편취한 경우, 액수가 비교적 큰 경우에는 3년 이하의 유기징역, 구역 또는 관제에 처하고, 벌금을 병과하거나 또는 벌금에만 처한다. 액수가 매우 크거나 기타 사안이 엄중한 경우에는 3년 이상 10년 이하의 유기징역에 처하고, 벌금을 병과한다. 액수가 특별히 매우 크거나 기타 사안이 특별히 엄중한 경우에는 10년 이상의 유기징역 또는 무기징역에 처하고, 벌금 또는 재산몰수를 병과하고 있다. 또한, 제 192조는 특별히 금융 사기죄를 규정하고 있으며, 불법점유를 목적으로 사기의 방법에 의하여 불법으로 자금을 조달한 경우, 액수가 비교적 큰 경우에는 5년 이하의 유기징역 또는 구역에 처하고, 2만위안 이상 20만위안 이하의 벌금을 병과한다. 액수가 매우 크거나 또는 사안이 엄중한 경우에는 5년 이상 10년 이하의 유기징역에 처하고, 5만위안 이상 50만위안 이하의 벌금을 병과한다. 액수가 특별히

329) 北京市公安局, “北京电信诈骗发案量5年最低”,
http://gaj.beijing.gov.cn/xxfb/fjjx/201912/t20191220_1371973.html (2020.12.15.
 최종확인)

매우 크거나 또는 사안이 특별히 엄중한 경우에는 10년 이상의 유기징역 또는 무기징역에 처하고, 5만원 이상 50만원 이하의 벌금 또는 재산몰수를 병과한다.

또한, 이러한 사기범죄행위에 대해 제199조에 의해 액수가 특별히 매우 크고 국가와 인민의 이익에 특별히 중대한 손실을 초래한 경우에는 무기징역 또는 사형에 처하고, 재산몰수를 병과하고 있다.

법에서 규정하고 있는 범죄 피해액의 규모에 대해서는 각 지역별로 별도의 상세 기준을 가지며 1998년 7월에 베이징시 인민 검찰원과 베이징시 공공 보안국에 의해 공동으로 발행된 기준에 따르면 베이징시는 도난, 사기, 횡령, 강도 및 기타 8가지 유형의 재산 침해 범죄의 범죄 양에 대해 사기 금액 (RMB로 계산)을 결정하는 기준과 관련하여 금액이 3,000위안을 초과하는 경우, 50,000위안을 초과하는 경우, 200,000위안을 초과하는 경우로 구분하여 규정하고 있다. 또한, 이와 같은 금액은 재산 침해의 범죄를 결정하는 중요한 기준으로 작용하지만, 유일한 기준은 아니며 재산 침해의 양에 더하여, 죄의 고백과 죄의식의 태도뿐만 아니라 기타 특정 상황에 기초하여 포괄적인 분석이 수행되어 결정된다.

허난성의 경우 사기 신고 기준을 5,000위안, 50,000위안, 500,000위안을 기준으로 하여 달리 적용하고 있다. 상하이의 경우 최고인민법원, 상하이사찰국, 상하이공안국, 상하이사법국이 1997년 4월 24일 대법원의 관련 규정에 따라 “사기 재판에 관한 법률 적용에 관한 사법적 해석”을 발표하면서 상하이의 사기 범죄에 대한 구체적인 금액 기준을 제시하여 4,000위안, 50,000위안, 100,000위안, 30,0000위안에 대해 그 기준을 달리하고 있다. 이 밖에 형법 제 287조 금융사기, 도난, 횡령, 공공 자금 횡령, 또는 기타 범죄를 저지르기 위해 컴퓨터를 사용하는 경우 관련 동 규정에 따라 유죄 판결을 받게 된다.

4. 대응 정책

가. 베이징시 안티 텔레콤 네트워크 사기 빅 데이터 플랫폼 구축

베이징시 보안국은 안티 텔레콤 네트워크 사기에 관한 빅 데이터 플랫폼 정보화 구축을 베이징시 당국의 빅 데이터 정책 수립의 핵심 건설 프로젝트로 간주하고, 시 당국의 빅 데이터 구축의 전반적인 아이디어와 프레임워크 하에서 형사 조사팀은 국내 첨단 기술 기업과 협업하고 있다. 기술의 도움으로 은행 계좌 조사 및 통제, 자본 흐름 조회 및 통신 네트워크 사기 사건 정보 분석 등과 같은 절차를 개발하고 비정상적인 카드 개설 직원 정보 데이터베이스와 은행 계좌개설 직원 정보 데이터베이스를 설정하였다. 또한, 정보 기술을 사용하여 도난당한 자금을 쫓는 병목 현상을 해결하고 수사를 지원하는 것과 동시에, 통신 네트워크 사기 정보 플랫폼의 대책 및 차단 기능을 최대한 활용하여 해외 발신의 사기 통신에서 얻은 사기 정보를 방지하고 피해의 확산을 억제하기 위해 단속 방지 작업을 적극적으로 수행하고 있다.³³⁰⁾

나. AI 안티 보이스피싱 사기 탐지기술 개발

공공 보안부 형사 조사국과 인터넷 회사가 공식적으로 발표 한 “Qiandun Anti-fraud Robot”은 발신자 번호 및 AI 음성 상호 작용 기술을 통해 잠재적인 피해자를 사기 트랩에서 안내하거나 잠재적인 통신 네트워크 사기 피해자에게 전화를 걸고, 알림을 보내 사기방지를 강화하도록 하여 차단 성공률을 높이고 있다. 2019년 11월 15일에 일부 지역에서 시험 운행한 이래 하루 평균 3,000명 이상에게 알림 권고를 보내고 있으며, 성공률은 96%를 넘는 것으로 나타났다.³³¹⁾

330) 北京市公安局, “北京市公安局: 三记重拳 从源头遏制电信网络诈骗”, http://gaj.beijing.gov.cn/xxfb/jwbd/201912/t20191220_1366654.html (2020.12.15. 최종확인)

제5절 비교분석 및 시사점

1. 미국

미국의 보이스피싱과 관련하여 강력한 가중적 처벌 규정을 가지고 있다는 점이다. 가중적 신원절도 범죄(제1028A조)는 보이스피싱에 적용할 수 있는 조항인 제1028조와 제1343조를 해당 조항의 적용 대상에 포함시키고 있으며, 해당 범죄를 위해 합법적인 권한 없이 고의로 타인의 식별 수단을 이전, 소유 또는 사용하는 자에 대하여 별도로 2년의 징역형을 부과하고 있다. 해당 조항을 통해 부과되는 2년의 징역형은 집행유예가 적용되지 않으며, 다른 범죄로 부여받은 형기가 끝난 이후에 순차적으로 집행되며, 해당 형기를 받았다고 타 범죄에 대한 형기에 영향을 전혀 주지 않도록 법문에 명시되어 있다. 즉, 해당 조항에 적용이 되는 보이스피싱을 저지른 자에 대해서는 반드시 집행되어야만 하는 2년형의 추가 형기가 부여된다는 것이다. 이는 실질적으로 제1028조와 제1343조의 구성요건을 만족하는 경우에는 제1028A조가 대부분 적용된다는 점에서 해당 조항들이 적용되는 보이스피싱에 대하여 강력한 가중적 처벌 규정으로 해당 범죄를 규율하고 있다는 것을 확인할 수 있다.

또한 보이스피싱에 있어 실제 범죄 실행행위라고 볼 수 있는 전화 통신을 통한 사취행위에 대하여 사기죄를 기준으로 해당 사취행위를 어떠한 수단을 취하였는지에 여부에 따라 적용 조항을 다르게 적용할 수 있도록 다양한 조항을 사기죄에 집중하여 마련해놓고 있다. 이는 보이스피싱에 적용할 수 있는 조항을 쉽게 인식할 수 있도록 하는 효과가 존재한다. 신원절도 및 사기죄(제1028조)와 통신사기죄(제1343조)에 대해서는 시도 및 음모죄에 대해서도 처벌 조항을 마련해 놓는 등, 개별 조항에 최대한 해당 범죄행위에 대하여 필요한 처벌이 있다면 해당 조항에

331) 新华社(2020.1.19.), “电信网络诈骗花样翻新, 警方教你这样守好「钱袋子」”, http://www.gov.cn/xinwen/2020-01/19/content_5470759.htm (2020.12.15. 최종확인)

정확하게 명시하여 해당 범죄 안에서 철저한 처벌이 가능하도록 하고 있기도 하다.

나아가 보이스피싱을 조직범죄로 처벌할 수 있는 조직범죄법을 두고 있었다. 해당 법은 전반적인 조직범죄에 대하여 전천후로 적용할 수 있는 법으로 조직범죄법 제1962조의 4가지의 구성요건을 만족하고 제1028조, 제1029조, 제1343조를 적용하는 보이스피싱에 대해 벌금 또는 20년 이하의 징역형이나 양벌을 병과 부과하도록 하며, 모의행위를 처벌할 수 있게 하고 있다. 해당 법에 의하면 조직범죄를 행함으로써 인하여 취득한 이익, 조직범죄법 위반을 통해 설립하거나 운영한 단체가 얻은 이익, 그리고 조직범죄법을 위반함으로써 습득한 금전을 몰수할 수 있게 하고 있다. 이러한 조직범죄법을 보이스피싱에 적용하는 경우, 보이스피싱에 적용하는 제1028조, 제1029조에서 상습범에 대한 가중적 처벌과 동일한 형인 20년 이하의 징역형을 부과한다는 점과 명확한 몰수 규정을 통해 조직적인 보이스피싱을 엄하게 규율하고 있다는 것을 확인할 수 있다.

뿐만 아니라, 보이스피싱에서는 해당 범죄에 의해 입은 피해의 손해배상을 명문화하고 있으며, 피해자가 보이스피싱으로 인한 피해액만 배상받을 수 있는 것이 아니라 징벌적 손해배상과 흡사하게 3배의 손해배상액을 배상받을 수 있도록 하고 있다. 조직범죄법에 의하면 해당 법에 의해 처벌되는 자에 대하여 해당 범죄로 인해 얻은 이익에 대하여 몰수를 하는 것은 당연하며, 이에 더하여 원고가 사실관계, 인과관계, 손해의 정도를 입증하면 의무적, 자동적으로 손해배상을 할 수 있도록 법으로 명시해두었다. 조직범죄법에 의해 이루어지는 손해배상은 손해액의 3배로 명확하게 지정되어 있으며, 이러한 3배의 손해배상금 책정에 있어 배심원이나 법원의 재량이 부과될 여지가 없어 손해배상액의 다툼이 있을 수 있는 일반적인 징벌적 손해배상과 달리 피해자의 구제에 초점을 맞추고 있다. 이러한 3배의 손해배상금 책정은 피해자에게 적극적으로 보이스피싱 사기를 적발하고 기소하는 것을 독려하고, 측정하기 어려운 정신적 손해에 대한 보상을 가능하게 해준다는 점³³²⁾에서 주목할 만하다.

한편 국제적, 조직적으로 이뤄지고 있는 신종금융 사기 대응 행정체계에 있어 트럼프 행정부에 들어 많은 변화가 일어난 점도 주목할 만한 점이다. 사이버 공간의 보호에 있어서 정책추진 체계이자 보좌하는 감독기관으로서 백악관의 역할이 약해지고 국토안보부의 기능이 매우 강해졌으며 그들은 감독과 지원을 담당해 사이버 안보 및 범죄의 환경에 있어서도 형사적인 부분과는 별도의 지원에 있어 중앙집권적인 체계를 갖추게 되었다. 물론 법무부의 각 사이버 범죄, 금융 범죄등의 담당 기관은 세분화 되어 있고 분산되어 있지만 지원기관으로서의 국토안보부 그리고 그 휘하 사이버안보 기반시설보호청의 분산화된 설립으로 기능이 강화되어 정보를 공유하고 사용하는데 있어서는 어느 정도 통일적인 체계를 가지게 되었다.

이러한 보이스피싱에 대한 대처를 통해 우리나라에 줄 수 있는 시사점으로는 3가지가 있다. 첫째, 보이스피싱에 적용할 수 있는 법률 조항들의 간결성이다. 미국의 보이스피싱에 적용할 수 있는 조항은 신원절도 및 사기죄(18 U.S.C. § 1028, § 1028A), 접근장치 사기죄(18 U.S.C. § 1029), 컴퓨터 사기죄(18 U.S.C. § 1030), 통신, 라디오, 텔레비전 사기죄(18 U.S.C. § 1343)로 모두 사기죄라는 항목 안에 존재하는 세부 조항들이다. 물론 조직범죄법(RICO, 18 U.S.C. § 1961-1968)이 있으나, 해당 법은 앞에서 언급한 보이스피싱 관련 사기죄를 준용하여 적용하는 방식으로 이루어져 있으므로 실질적으로 보이스피싱 행위자에게 직접적으로 적용되는 조문은 위의 다섯 조항에 불과하다. 그에 반해 우리나라의 경우에는 많은 법률에 관련 처벌 조항이 산재하여 있어 적용과 관련된 어려움이 있는 것이 사실이다.

그리고 두 번째로는 조직범죄에 해당하는 보이스피싱이나 상습범의 경우에는 우리나라에 비해 더 강력하게 처벌하고 있다는 점이다. 미국은 RICO에 의해 제 1028조, 제1029조, 제1343조를 적용하는 보이스피싱에 대해 벌금 또는 최대 20년의 법정형을 부과할 수 있도록 되어 있으며, 제1028조와 제1029조의 상습범인 경우에도 벌금 또는 최대 20년의 법정형을 부과할 수 있다. 이는 실질적으로 근래의 보이스피싱 범죄가 조직적으로 이루어지며, 상습사기에 해당한다는 점에서 보이

332) 18 U.S.C. § 1964(c)

스피싱 범죄자에 대한 기본 법정형이 20년 이하라고 해도 무방할 것이다. 하지만 우리나라의 경우에는 관련 법률들에서 최대 10년 이하의 법정형을 두고 있어 미국에 비한다면 법정형이 낮은 편에 속한다. 따라서 우리나라도 보이스피싱에 더욱 강력하게 대처하기 위해 미국의 입법과 같이 법정형을 더 높일 필요가 있을 것이다.

마지막으로는 보이스피싱 피해자들에 대한 손해배상제도가 있다. 미국은 RICO에 의해 규율되는 보이스피싱 범죄자에 대해 3배의 손해배상을 하도록 명문화하고 있다. 이러한 손해배상제도는 일반적인 불법행위에 의한 손해배상제도와는 다르게 피해자가 받은 손해보다 더 많은 손해배상을 명한다는 점에서 징벌적 손해배상과 흡사해 보인다. 하지만 이러한 손해배상은 일단 손해배상이 결정된 이후에는 징벌적 손해배상과 같이 손해배상액의 다툼 없이 명시적으로 손해액의 3배를 손해배상액으로 명시하고 있다. 이러한 점은 결국 피해자들이 보이스피싱에 대해 적극적으로 수사를 할 수 있도록 돕고, 자신이 입은 정신적 손해까지 별도의 다툼 없이 배상받을 수 있다는 점에서 긍정적인 영향을 미친다. 현재 우리나라는 보이스피싱 범죄 피해자의 손해배상과 관련하여 금융회사의 책임을 기반으로 한 손해배상 외에는 일반적인 불법행위에 의한 손해배상만 가능하다. 그러므로 이러한 미국의 손해배상제도를 참고하여 보이스피싱 피해자들이 적극적으로 수사에 협력하고 자신의 피해를 온전하게 회복할 수 있는 기회의 범위를 넓힐 필요가 있을 것이다.

2. 독일

독일 보이스피싱과 관련된 기관 및 관련 법제, 정책에서 보이는 특징 중 하나는 보이스피싱에 대하여 조직범죄로 규정하고 있으며, 이에 대응할 수 있는 조치들이 마련되어 있다는 점이다. 수사 단계부터 ‘콜센터 사기’와 같은 전형적인 보이스피싱에 대해 조직 범죄로 규정하여 금전 세탁 등의 조직 범죄를 전담하는 연방범죄수사국 내 SO 부서가 수사를 전담하고 있으며, 이 외에도 사이버 범죄를 전담하는 CC 부서에서도 보이스피싱과 관련된 죄목인 독일형법 제263조a 컴퓨터사용사

기죄와 관련된 수사를 하도록 하고 있다.

관련 법제에서도 다음과 같이 조직적인 보이스피싱에 대하여 강력하게 대응하고 있다. 형법 제192조 범죄단체조직죄의 경우 해당 범죄의 구성요건에 해당하는 자에 대하여 별도의 형을 부여하는 형식이기에 동일한 행위에 대하여 타법의 적용을 받는 경우에는 상상적 경합의 대상이 되어 더 중한 죄의 형으로 처벌받게 되며, 단순 가담자와 일반 가담자 및 범죄단체의 수괴나 배후조정자 사이에 형의 차별을 두고 있어 더 중한 범죄를 저지른 자에게 더 중한 형을 가하도록 하는 가중 처벌이 가능하도록 규정하고 있다. 또한 이러한 범죄단체조직죄에 해당하는 경우에는 범죄조직에 대한 박탈과 몰수를 이행할 수 있어 보이스피싱 범죄 조직이 얻은 범죄수익에 대한 형법적인 처분 규제도 이루어지도록 하고 있다. 제253조 공갈죄에서 특히 중한 경우라고 하여 행위자가 직업적으로 또는 공갈의 계속적 수행을 목적으로 조직된 범죄조직의 구성원으로서 행위한 경우에는 기본적으로 5년 이하의 자유형을 처했던 공갈죄의 형에 대하여 1년 이상의 자유형에 처하게 하는 등 조직적으로 이루어진 범죄에 대한 처벌 혹은 가중 처벌을 규정하고 있다.

뿐만 아니라 제261조 자금세탁, 불법적으로 획득한 재산가치의 은닉죄에서도 조직 범죄로 행한 관련 범죄에 대하여 처벌 및 불법적으로 얻은 대상물에 대한 박탈 및 몰수를 명하는 등, 조직 범죄로서의 보이스피싱을 가중하여 처벌할 수 있는 법 규정을 마련해두고 있다. 이처럼 보이스피싱을 조직적 범죄로 규정하고 수사 및 처벌하는 것은 보이스피싱에 대한 구조적이고 세밀한 수사를 가능하게 하고, 관련 범죄를 저지른 자에 대한 철저한 처벌을 가능하게 할 수 있다.

이 외에도 독일 보이스피싱 범죄와 관련하여 확인할 수 있는 특징은 전자금융사기피해 구제제도이다. 우리나라의 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법과 같이 별도의 사기 피해 구제제도를 만드는 것이 아니라, 기존의 민법과 유럽연합 지급 서비스 지침에 규정되어 있는 자금이체와 관련된 부분을 활용하여 전자금융사기에 피해자가 구제를 받을 수 있는 방안을 마련하였다. 또한 모든 전자금융사기 피해자에게 구제를 가능하도록 하는 것이 아니라 고객으로서

의 통보 의무, 주의의무를 다하였을 때에 해당 구제제도를 활용할 수 있도록 하고 있다. 이는 은행 서비스를 사용하고 있는 고객들에게 컴퓨터 등에 백신을 설치하거나, 제3자의 수상한 행동을 분간하거나 제 3자에게 자신의 PIN, TAN 번호 등 개인정보 및 금융정보를 제공하지 않도록 하는 등 최소한의 주의의무를 부여하여 자신의 행동에 책임을 지게하고, 은행 등 금융사들이 해당 범죄와 관련된 너무 많은 금전적 부담을 지지 않도록 하는 것으로 보인다.

이러한 독일의 보이스피싱에 대한 대처를 통해 우리나라에 줄 수 있는 시사점으로는 2가지가 있다. 우선, 독일의 보이스피싱 범죄에 적용할 수 있는 법률의 일원화이다. 독일의 보이스피싱에 적용할 수 있는 처벌 관련 조항은 모두 독일 형법 내에 포함되어 있다. 그러므로 다양하게 많은 특별법들에 관련 조문들이 퍼져있는 우리나라와는 다르게 독일의 경우에는 보이스피싱에 대해 규율하기 위해서는 형법만 살펴보면 된다는 장점이 있다. 즉, 어떤 법률을 적용해야 하는지에 대해 명확히 알지 못해 제대로 법률을 적용하지 못하는 문제는 발생하지 않을 수 있다. 따라서 우리나라도 이러한 독일과 같이 관련 법률을 일원화하지는 못하더라도 적용 조항들의 간결화를 위해 대안을 제시할 필요성이 있을 것이다.

그리고 마지막으로 전자금융 사기피해 구제 관련 법제에 있어 금융기관의 책임과 관련하여 고객의 주의의무와 관련된 사안이다. 독일 민법에 의하면 금융기관의 자금이체는 요청 받은 즉시 금융기관의 자산으로 이체를 진행하고 그 지출액에 대해 고객에게 상환을 받는 방식으로 이루어지고 있다. 그러므로 만약 권한이 없는 자가 자금이체 지시를 하여 이체가 일어난 경우, 금융기관이 고객의 고의 또는 중과실을 입증하여야만 고객에게서 해당 액수를 상환할 수 있도록 되어 있다. 그런데 해당 금융기관이 고객의 주의의무를 입증함에 있어 판단 기준은 컴퓨터 등에 백신을 설치하거나, 제3자의 수상한 행동을 분간하거나 제 3자에게 자신의 PIN, TAN 번호 등 개인정보 및 금융정보를 제공하지 않도록 하는 등으로 보이스피싱 수법을 통해 살펴보면 해당 범죄로 인해 피해를 입은 피해자들이 주의의무를 다하지 않았다고 볼 수밖에 없다. 따라서 이러한 주의의무 기준은 실질적으로 피해자

들이 보이스피싱에 대한 피해 구제를 받지 못하게 하는 걸림돌로 작용하고 있다.

그런데 2020년 6월에 발표된 종합방안에서 언급된 우리나라의 통신사기피해환급법 개정 방향을 살펴보면 이용자의 고의 및 중과실이 없는 경우에 한해 금융회사의 손해배상책임을 강화한다고 명시하고 있다. 물론 이용자들의 최소한의 주의의무를 판단하여 이용자의 심대한 과실이 있는 경우에만 그로 인한 손해를 배상해줄 필요는 없다. 하지만 이러한 고의 및 중과실을 판단함에 있어 독일의 사례와 같이 실질적으로 보이스피싱 범죄로 인해 피해를 입은 피해자들이 법에 의한 구제를 받지 못하도록 하지는 않아야 한다. 이는 해당 법을 유명무실화하게 만드는 것으로 법을 신설하는 목적에 부합하지 않기 때문이다. 따라서 우리나라의 경우, 독일의 고의 및 중과실 판단 기준을 살피고 현실적으로 이용자의 도덕적 해이 방지를 위한 적절한 기준을 세울 필요가 있을 것이다.

3. 일본

앞서 살펴본 일본의 보이스피싱 범죄의 형태와 이에 대한 대응은 우리나라의 보이스피싱 대응 상황에 대해 크게 조직범죄로서의 대응, 범정부차원의 대응, AI기술을 활용한 대응이라는 3가지 측면에서 시사점을 안겨준다.

첫 번째, 수사 단계에서부터 보이스피싱 범죄에 대해 조직적 범죄로 인식하고 이에 맞는 수사 대응 체계를 구축하여야 한다. 일본의 보이스피싱 사기의 형태가 총책부터 단순 현금수령 혹은 피싱전담 등 말단 조직원까지 대규모의 조직적으로 운영된다는 점에서 그 구조가 우리나라의 보이스피싱 범죄단체의 구성과 매우 흡사한 면이 있다. 이처럼 보이스피싱 범죄의 형태가 조직적으로 일어난다는 점에서 일본의 경찰청은 보이스피싱 범죄를 단순히 지능범죄팀의 수사로 진행하는 것이 아니라, 조직폭력단 담당부서와의 긴밀한 연계를 통해 수사를 펼치고 있다는 점에서 보이스피싱 범죄가 대규모 조직으로 운영됨을 명확히 인식하고 이에 적절한 수사 대응을 하고 있다. 이처럼 우리나라에서도 보이스피싱 범죄를 지능범죄수사 대응 부서와 조직범죄수사 전담 부서의 전문인력으로 구성된 조직적 보이스피싱 범

죄에 대응하기 위한 TF팀의 구성이 필요하다.

두 번째, 보이스피싱 대응을 위한 협력적 거버넌스 체계를 구축해야 한다. 일본은 2019년 범죄대책각료회의를 통해 보이스피싱을 주요 화제로 선정하고 범정부 차원의 ‘보이스피싱(오레오레 사기) 대책 플랜’을 발표하여 전 관계 부처 및 기관의 대책을 촉구하고, 갈수록 고도화 되고 심화되는 보이스피싱 사기에 대한 전 국가 차원의 대응을 추진해나가고 있다. 특히 해당 계획에서는 단순히 정부만의 대응이라기보다 통신사, 택배 사업자, 편의점 사업자 등 보이스피싱 범죄와 연계될 수 있는 민간 사업자와 정부 기관의 연계 방안을 제시하고 있다는 점에서 보이스피싱 대응의 민관협력대응 구조의 실현을 꾀하고 있다. 물론 우리나라의 경우에도 올해 6월 22일 문재인 대통령이 반부패정책협의회에서 보이스피싱과 같은 민생침해 범죄에 대해 초기부터 강력하게 대응하고, 부처 간 공조를 강화해 신속하게 대책을 마련할 것을 지시한 바 있으며, 6월 24일 금융위·과기정통부·경찰청 등 관계 부처에서 금융-통신-수사 전 분야에서의 협력을 강화하고 보이스피싱 척결 종합 방안을 마련하는 등 노력하고 있지만 앞으로 이러한 협력을 보다 견고히 하고 무엇보다 민간과의 연계방안을 마련하여 보이스피싱 범죄에 대한 협력적 대응 거버넌스 체계를 강화하여야 할 필요가 있다.

마지막으로, 첨단 AI 기술을 활용한 보이스피싱 대응을 보다 적극적으로 추진할 필요가 있다. 일본은 보이스피싱 피해방지를 위해 AI기술을 적극적으로 활용하고 있다. 물론 우리나라에서도 AI를 활용한 보이스피싱 차단 앱 등이 개발되어 왔으며 앞으로도 이와 같은 AI기술을 활용한 대응이 기대되고 있으나 일본의 경우 우리나라와 달리 좀 더 이용자 중심에 대응이 고려되고 있다는 점에서 배울 점이 있다. 예를 들어 일본의 보이스피싱 피해자가 대부분 고령자에 집중되어 있다는 점에서 일본의 통신기기에 적용하는 AI 음성분석 솔루션은 보이스피싱 의심 전화로 분류되는 통화에 대해 통화 당사자뿐만 아니라 해당 서비스 이용자의 자녀나 보호자 등 주변에서 적절한 대응을 취해줄 수 있는 제3자에게도 경고가 가는 등 실제 보이스피싱 피해 가능성이 높은 집단에 대한 배려가 고안되고 있다는 점이 특징이

다. 또한, AI를 통한 음성분석 솔루션의 경우 결국 모든 통화음성을 녹음하고 이를 분석하여야 하는데, 이때 발생할 수 있는 여러 법적 문제에 대비하기 위해 해당 서비스 이용자가 통화를 개시할 때 AI보이스피싱 대책 솔루션 이용자임을 밝히며 해당 통화가 녹음된다는 안내음성이 나오도록 하는 등의 방안을 마련하고 있다. 이러한 안내는 보이스피싱을 하려고 했던 사기범들에게도 충분한 경각심을 심어줄 수 있으며, 범행을 단념하도록 하는 추가적인 효과 또한 기대된다. 이러한 장치들은 우리나라의 AI를 활용한 보이스피싱 음성분석 솔루션을 개발 도입하는 데 있어 충분히 적용해볼 수 있을 것이다. 다만 일본의 보이스피싱 대책은 우리나라가 휴대전화(스마트폰)에서 보이스피싱 대응(앱 등을 통한 솔루션)을 추진하는 것과 달리 주로 가정집에 설치되어 있는 고정전화에 대한 대응이 주를 이루고 있다는 점에서 우리나라와 차이점을 보인다. 따라서 일본의 대응에 대한 장점을 흡수하면서도 우리나라의 실정에 맞는 방안의 구상을 고안할 필요가 있을 것이다. 이밖에도 은행에서의 대응으로 ATM 카메라에 AI 기술을 탑재하여 ATM기기 앞에서 휴대전화를 사용하는 경우 보이스피싱으로 의심하여 은행직원을 통한 적절한 확인이 이루어질 수 있도록 하는 등의 조치는 은행 측에서도 큰 부담 없이 보이스피싱 피해를 미연에 방지할 수 있다는 점에서 우리나라의 은행들에서도 충분히 도입 가능할 것으로 예상되며, 적은 투자비용 대비 보이스피싱 피해 방지 효과를 누릴 수 있을 것이다.

4. 중국

중국의 보이스피싱 범죄에 대한 대응은 우리나라의 보이스피싱 대응방안을 고려함에 있어 엄중한 양형기준 마련과 민관의 유기적인 대응기구의 설립이라는 두 가지 측면에서 시사점을 준다.

첫째, 법률에 의해 보이스피싱에 대해 보다 엄격한 양형 부과를 검토해야 한다. 중국의 경우 보이스피싱에 대해 그 규모에 따라 양형을 구분하고 있으며, 사안이 엄중한 경우에는 10년 이상의 유기징역 또는 무기징역에 처하도록 하고 있다. 특

히 그 액수가 매우 크고 국가와 인민의 이익에 특별히 중대한 손실을 초래하는 경우에는 무기징역 또는 사형에 처하고, 재산몰수를 병과하는 등 상당히 엄격한 양형을 부과하고 있는 것을 알 수 있다. 보이스피싱의 규모나 심각성이 나날이 커지고 있는 우리나라의 보이스피싱에 대한 양형 기준에 관한 검토가 요구된다. 물론 중국처럼 사형이라는 극단적인 양형까지는 아니더라도 사안의 엄중함과 규모에 따라 무기징역 등에 대한 검토도 있을 수 있다. 또한, 법률에서 보이스피싱의 규모나 영향력에 따라 양형 수준을 구분하고 있다는 점에서도 우리 양형 기준을 검토하고 보다 엄중하고 구체적인 양형 기준을 설정해야 할 것이다.

둘째로, 보이스피싱과 관련한 모든 관련 기관 및 민간조직이 참여하는 보이스피싱 전담 대응조직을 설립하여 보이스피싱 대응의 실효성을 높여야 한다. 이와 관련한 중국의 보이스피싱에 대한 대응으로는 베이징시 등 대도시 지역을 중심으로 하는 공안기관의 대처가 있다. 특히 베이징시의 경우 공안기관을 중심으로 신종 피싱 사기 등에 대응하기 위해 반(反)사기 센터를 설립하여 운영하는 등 보이스피싱에 대응체계를 확립하고 있는 것이 특징적이다. 해당 센터는 베이징시의 주요 은행 및 통신사가 포함되어 있어 실질적으로 보이스피싱에 관계되는 모든 기관 및 사업자가 연계하여 대응할 수 있는 구조를 구축하고 있다. 이는 보이스피싱 범죄의 경우 무엇보다 신속한 범행 계좌의 동결이나, 통신관련 기록의 확인 등 범인 색출이 이루어져야 하는데 이러한 신속한 대응에 효과적이고 실효적으로 대처할 수 있다는 장점이 있다. 이와 같은 중국의 보이스피싱 대응 협력체계는 중국에서 공안기관이 갖는 권한과 영향력을 고려할 때 여러 기관이나 민간 사업자의 합동 대응 및 즉각적인 대응을 보다 용이하게 구축할 수 있다는 점에서 우리나라와는 분명 다른 환경조건을 갖는다. 그러나 보이스피싱에 대한 대응이 무엇보다도 신속하고 유기적으로 진행되어야 함을 고려한다면 중국만큼의 강한 통제는 아니더라도 베이징시에서 운영하는 반(反)사기 센터와 같이 보이스피싱 대응과 관련된 모든 관계 부처 및 조직이 정보 공유 및 협업할 수 있는 인프라를 구축할 필요가 있다.

제7장 신종 보이스피싱 대응 정책적·기술적 개선 방안

제1절 입법적 개선방안

1. 해외 발신전화 차단에 대한 기술적 조치 의무화

이동통신사가 해외 보이스피싱 발신전화의 패턴을 분석하여 신속하게 차단하여 추가적인 피해를 예방할 수 있도록 기술적 조치를 의무화할 필요가 있다. 통신내용에 대한 패킷을 열람하여 차단하자는 것이 아니라 보이스피싱 발신전화의 패턴을 분석하여 차단하는 방식이다. 이동통신사는 통화가 완료된 보이스피싱 발신전화에 대한 통화시간, 빈도수, 트래픽정보, IP 주소, MAC 주소, VPN 등 다양한 정보를 가지고 있고, 이러한 정보를 분석할 경우 보이스피싱 전화를 식별할 수 있을 것이다. 검찰총장, 경찰청장 또는 금융감독원장이 사건발생 후 사후적으로 발신번호에 대한 차단조치를 요구할 것이 아니라 전기통신사업자가 선제적으로 기술적 조치를 취하는 방식이다.

보이스피싱에 대한 기술적 조치와 유사한 제도로 전기통신금융사기에 이용된 전화번호에 대한 전기통신역무 제공중지 제도가 있다. 검찰총장, 경찰청장 또는 금융감독원장은 전기통신금융사기에 이용된 전화번호를 확인하면 과학기술정보통신부장관에게 전기통신역무 제공의 중지를 요청할 수 있고(통신사기피해환급법 제13조의3 제1항), 과학기술정보통신부장관은 요청을 받아 1년 이상 3년 이내의 기간을 정하여 전기통신사업자에게 전기통신역무 제공의 중지를 명할 수 있다(전기통신사업법 제32조의3). 이를 통해서 보이스피싱에 이용된 전화번호를 차단할 수 있는데, 인터넷이나 가상사설망(VPN)을 사용하는 경우에는 해당 통신만 차단하는데 한계가 있고, 사후적 차단으로 피해예방에도 한계를 보이고 있다. 또한, 특수유형부가통신사업자에게 송신인의 전화번호 변작 등 거짓표시를 방지하기 위한

기술적 조치 실시계획을 과학기술정보통신부장관에게 등록하도록 의무화하고 있고(전기통신사업법 제22조 제2항 1의2), 금융위원회는 전기통신금융사기 대응에 있어서 금융회사나 임직원에게 개선계획 등을 제출하도록 하는 규정을 두고 있다.

이와 같은 기술적 조치는 보이스피싱 외에 다른 범죄의 대응에서도 활용하고 있다. 개인정보보호법에서 기술적·관리적 보호조치(제29조), 전기통신사업법에서 불법촬영물등 기술적 조치(제22조의3, 제22조의5) 등 사전적 조치가 있고, 정보통신망법에서 사생활침해에 대한 임시조치(제44조의2 제6항), 저작권법에서 불법복제물 삭제명령(제103조 제5항) 등 사후적 기술적 조치가 있다.

따라서 이와 같은 다양한 기술적 조치를 벤치마킹하여 이동통신사가 이행할 수 있는 범위, 방법과 절차에 대한 세부절차를 논의할 필요가 있다. 이때 이동통신사가 해외 보이스피싱 발신전화를 차단한 경우 법률에서 정해진 절차에 따라 이행하였고, 고의·중과실이 없는 경우 책임을 감면할 수 있는 규정도 마련해야 한다. 실제 정보통신망법상 임시조치, 저작권법상 복제·전송 중단 등에서도 법률에서 정해진 절차에 따라서 이행할 경우 책임을 감면하는 규정을 두고 있다.

2. 금융기관의 보이스피싱에 대한 배상책임 강화

금융기관이 보이스피싱 피해자의 고의·중과실이 없는 경우 원칙적으로 배상책임을 지도록 통신사기피해환급법을 개정할 필요가 있다. 통신사기피해환급법(제4조)에서는 금융회사가 금융거래 시 본인확인을 하지 않았거나, 수사기관, 금융감독원의 정보제공 또는 정당한 피해구제 신청이 있었음에도 지급정지를 하지 않은 경우에 한하여 배상책임을 지도록 하고 있어 피해자가 배상을 받는 경우가 거의 없다. 결국 피해자들은 민법 제750조 불법행위에 기한 손해배상 조항에 따라서 손해배상 소송을 제기해야 하는데, 범죄자가 특정되지 않은 경우가 많아 사실상 곤란하다. 기업이 자발적으로 금융소비자에 대한 보상제도를 운영하는 경우도 있다. 핀테크 업체인 토스는 부정결제나 보이스피싱 피해가 발생했을 경우 피해금액을 자체적으로 보상하는 제도를 도입하여 금융소비자가 30일 이내에 신고하면 피해

금액을 보상하고 있다.³³³⁾ 한편, 박재호의원은 “다중사기범죄의 피해 방지 및 구제에 관한 법률안”을 발의하여 다중사기범죄 혐의자에게 징벌적 손해배상제도의 도입을 촉구하였다(안 제31조).³³⁴⁾

3. 통신제한조치 대상에 전기통신금융사기죄 포함

수사기관이 전기통신금융사기를 수사할 경우 통신제한조치(전기통신감청)를 할 수 있도록 통신비밀보호법을 개정하여야 한다. 현재는 통신제한조치의 대상범죄에 통신사기피해환급법상 전기통신금융사기가 포함되어 있지 않아 전기통신감청 제도를 활용할 수 없다. 일부 수사관서에서 전기통신금융사기를 형법상 범죄단체 조직죄(제114조) 또는 특정경제범죄법상 특정재산범죄(제3조, 사기죄 5억 이상)로 의율하여 집행하는 경우가 있지만 범죄단체조직죄는 범인을 특정해 가는 과정에서 단체를 입증하기 어렵고, 특정재산범죄 역시 개별사건의 이득액이 5억 이상이어야 하기 때문에 대상범죄에 해당되기 어렵다. 전기통신금융사기는 10년 이하의 징역 또는 1억원 이하의 벌금으로 법정형이 높고, 수사기관이 각종 수단을 강구해도 관련범죄가 줄고 있지 않고 피해가 계속되고 있기 때문에 강력한 법집행 권한을 부여할 필요성이 있다. 나아가 통신제한조치는 전기통신사업자의 협조의무가 있음에도 절차, 방법 및 대상에 대한 구체적인 내용이 마련되지 않아 협조가 쉽지 않은 만큼 세부절차를 마련하고, 협조의무를 담보할 수 있는 제재수단도 검토해야 할 것이다.

333) 한국경제 보도(2020.07.06.), “카카오 이어 토스도 부정결제 피해 先보상”, (2020.10.03. 최종확인)

334) 박재호 의원 대표발의(의안번호 제3080호), “다중사기범죄의 피해 방지 및 구제에 관한 법률안” (2020. 8. 20)

4. 상습 전과자 신상정보 공개제도 도입

보이스피싱 상습 전과자에 대하여 관련범죄를 선제적으로 예방하고, 범죄자에게 경각심을 심어주기 위해 확정판결에 따라 신상정보를 공개하는 제도를 도입할 필요가 있다. 신상정보 공개제도는 예비 범죄자들에게 심리적 압박을 주어 범죄예방에 대한 효과를 가져 올 수 있다.³³⁵⁾ 보이스피싱은 경제와 금융 영역에서 다수가 기능적으로 역할을 분담하여 불특정 다수에게 피해를 준다는 측면에서 형법상 사기범죄가 상정했을 때의 상황과는 질적으로 다르다.³³⁶⁾ 기존의 규범체계에서 포섭할 경우 가벌성에 대한 평가가 적절하지 않고, 범죄수익과 피해에 한참 밑도는 처벌을 할 경우 일방예방 내지 특별예방의 효과도 달성하기 어렵다.³³⁷⁾ 이미 “다중사기범죄 등 규제 기본법안”에 대한 논의가 이루어지고 있고,³³⁸⁾ 박재호 의원은 “다중사기범죄의 피해 방지 및 구제에 관한 법률안”을 발의하여 전기통신금융사기 등의 상습범에 대하여 신상정보를 공개하자고 제안하면서 유죄판결을 받을 경우 10년 이상 30년 이하의 범위에서 신상정보를 공개하자고 주장하고 있다.³³⁹⁾ 신상정보 공개제도가 범죄예방에 효과가 있을지 의문을 제기하고,³⁴⁰⁾ 범죄

335) 오영근, “한국의 청소년대상 성범죄자의 신상공개제도”, 송실대학교 법학연구소, 법학논총 23(3), 2006, 158면

336) 김대근, “다중사기범죄의 현상에 대한 비판적 고찰과 규범적 대안 : 다중사기범죄 등 규제 기본법의 법제화를 위한 시론”, 한국형사정책연구원, 형사정책연구 29(3), 2018, 131면

337) 김대근, “다중사기범죄의 현상에 대한 비판적 고찰과 규범적 대안 : 다중사기범죄 등 규제 기본법의 법제화를 위한 시론”, 한국형사정책연구원, 형사정책연구 29(3), 2018, 131면

338) 김대근, “다중사기범죄의 현상에 대한 비판적 고찰과 규범적 대안다중사기범죄 등 규제 기본법의 법제화를 위한 시론”, 한국형사정책연구원, 형사정책연구 29(3), 2018, 133면

339) 박재호 의원 대표발의(의안번호 제3080호), “다중사기범죄의 피해 방지 및 구제에 관한 법률안” (2020. 8. 20)

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

2. “다중사기범죄”란 다음 각 목의 어느 하나에 해당하는 행위를 통하여 다중

자의 재사회화에 대한 우려와 이중처벌 금지원칙에 어긋난다는 견해³⁴¹⁾가 있지만

을 상대로 이득을 편취하는 행위를 말한다.

가. 전기통신금융사기

나. 유사수신행위

다. 무인가, 무허가, 미등록, 미신고 등 금융업 영위행위

제46조(벌칙) ① 제3조를 위반하여 다중사기범죄 행위를 한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

② 제1항의 위반행위로 취득한 금품이나 그 밖의 재산상 이익의 가액(이하 이 조에서 “이득액”이라 한다)이 5억원 이상일 때에는 다음 각 호의 구분에 따라 가중처벌한다.

1. 이득액이 50억원 이상일 때: 무기 또는 5년 이상의 징역

2. 이득액이 5억원 이상 50억원 미만일 때: 3년 이상의 유기징역

③ 제2항의 경우 이득액 이하에 상당하는 벌금을 병과(併科)할 수 있다.

제51조(신상정보 등의 공개명령) ① 법원은 제46조제1항의 죄로 유죄판결을 선고하는 경우에 그 유죄판결을 선고받는 자가 다음 각 호의 어느 하나에 해당하면 제5항의 공개정보를 10년 이상 30년 이하의 범위에서 공개기간을 정하여 정보통신망을 이용하여 공개하도록 하는 명령(이하 “공개명령”이라 한다)을 유죄판결과 동시에 선고하여야 한다. 다만, 피고인이 아동·청소년인 경우, 그 밖에 신상정보를 공개하여서는 아니 될 특별한 사정이 있다고 판단하는 경우에는 그러하지 아니하다.

1. 상습으로 제46조제1항의 위반행위를 한 자

2. 제46조제1항의 위반행위로 인한 이득액이 50억원 이상인 자 (중략)

제52조(공개명령의 집행) ① 공개명령은 금융위원회가 정보통신망을 이용하여 집행한다.

② 법원은 공개명령의 판결이 확정되면 판결문 등본을 판결이 확정된 날부터 14일 이내에 법무부장관에게 송달하여야 하며, 법무부장관은 제51조제1항에 따른 공개기간 동안 공개명령이 집행될 수 있도록 제51조제5항 각 호에 따른 공개정보를 지체 없이 금융위원회에 송부하여야 한다.

③ 공개명령의 집행·공개절차·관리 등에 관한 세부사항은 대통령령으로 정한다.

340) 이경재, “성범죄자 신상정보공개제도의 문제점과 개선방안”, 강원대학교 비교법학연구소, 강원법학 33, 2011, 362면

341) 김혜정, “성범죄자 정보등록·열람제도에 관한 검토”, 한국형사정책연구원, 형사정책연구 18(3), 2007, 865면

보이스피싱이 상습적으로 이루어지고, 전 국민을 대상으로 수많은 피해를 양산하고 있어 보다 강력한 조치가 불가피해 보인다.

5. 전기통신금융사기 취득객체에 재물 포함

전기통신금융사기의 취득객체에 재산상 이익 외에 재물을 추가하여 처벌의 공백을 메꾸어야 한다.³⁴²⁾ 전기통신금융사기는 전기통신을 이용하여 타인을 기망·공갈함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하는 행위를 처벌하고 있어 재물은 제외되어 있다(제2조 2호). 그렇다면 보이스피싱 피해자들이 은행창구, ATM 또는 인터넷뱅킹으로 송금하지 않고, 현금을 수거책에게 직접 전달하는 경우는 통신사기피해환급법으로 처벌하지 못하는 경우가 발생한다. 형법상 사기죄로 처벌할 수 있지만 특별법으로 강력하게 처벌하지 못한다. 결국 대면편취형 보이스피싱은 전기통신금융사기에 포함되지 않기 때문에 검찰총장, 경찰청장 또는 금융감독원장이 과학기술정보통신부장관에게 해당 전화번호에 대한 전기통신역무 제공의 중지요청도 할 수 없다(제13조의3).³⁴³⁾

한편, 전기통신금융사기에서 타인의 개념에 대해 기망·공갈을 당한 사람만을 의미하는지, 전기통신금융사기에 이용된 대포통장계좌의 명의인도 포함되는지 논란이 있다.³⁴⁴⁾ 전기통신금융사기를 통해서 피해자 자금을 대포통장계좌로 송금·이

342) 윤동호, “통신사기피해환급법의 정보·명령입력죄의 구성요건적 의미와 한계”, 한국형사정책학회, 형사정책 32(1), 2020, 236면

343) 과학기술정보통신부장관은 관계 행정기관의 장으로부터 「대부업 등의 등록 및 금융이용자 보호에 관한 법률」 제9조의6에 따른 불법 대부광고에 사용된 전화번호의 이용중지, 「전자금융거래법」 제6조의2에 따른 불법 광고에 이용된 전화번호의 이용중지에 이어 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」 제13조의3에 따른 전기통신금융사기에 이용된 전화번호의 이용중지를 요청받은 경우 전기통신사업자에게 1년 이상 3년 이내의 기간을 정하여 전기통신역무 제공의 중지를 명할 수 있는 것이다.(전기통신사업법 제32조의3)

344) 윤동호, “통신사기피해환급법의 정보·명령입력죄의 구성요건적 의미와 한

체되도록 한 후 현금인출기에 그 계좌 명의인의 체크카드를 넣고 비밀번호를 입력하는 행위에 대한 정보·명령입력죄의 성부가 달라진다.³⁴⁵⁾ 대법원 판결에서 다수의견은 전자의 입장으로 기망·공갈하여 취득한 피기망·공갈자의 정보만 해당한다고 보아 정보·명령입력죄의 성립을 부정하지만, 반대의견은 후자의 입장으로 죄의 성립을 인정하였다.³⁴⁶⁾ 따라서 피해자의 자금 인출책도 정보·명령입력죄로 처벌할 필요가 있다면 전기통신금융사기 개념에 범죄자 쪽의 계좌에 입금된 피해자의 자금을 인출하거나 송금·이체하는 행위도 포함시켜야 할 것이다.³⁴⁷⁾ 정보통신기술과 전자금융 기술을 이용한 신종 보이스피싱에 적절히 대응하기 위해서는 전기통신금융사기의 개념을 정교하게 규정해 나가야 사각지대를 없앨 수 있을 것이다.

계”, 한국형사정책학회, 형사정책 32(1), 2020.4, 224면

345) 윤동호, “통신사기피해환급법의 정보·명령입력죄의 구성요건적 의미와 한계”, 한국형사정책학회, 형사정책 32(1), 2020.4, 224면

346) 윤동호, “통신사기피해환급법의 정보·명령입력죄의 구성요건적 의미와 한계”, 한국형사정책학회, 형사정책 32(1), 2020.4, 224면; 대법원 2016. 2. 19. 선고 2015도15101 전원합의체 판결

347) 윤동호, “통신사기피해환급법의 정보·명령입력죄의 구성요건적 의미와 한계”, 한국형사정책학회, 형사정책 32(1), 2020.4, 231~233면

제2절 제도적 개선방안

1. 보이스피싱 음성·신원 제보자 포상금 확대

보이스피싱 음성 제보자에게 소정의 신고포상금을 지급하고, 보이스피싱 음성 에 대한 신원제보자에게는 범죄의 규모에 따라 최대 1억원까지 신고포상금을 지급하도록 하여 시민들의 적극적인 참여를 유도할 필요가 있다. 피해자가 자신이 직접 통화한 보이스피싱 음성을 신고할 경우에는 자신의 음성을 비식별화할 수 있는 기술적 조치가 있어야 한다.³⁴⁸⁾ 신고포상금 확대는 범죄자를 특정하는 효과도 있지만, 국민들에게 보이스피싱에 대한 경각심을 불러일으키고 피해를 예방하는 효과도 있다. 무엇보다도 범죄자들에게 자신들의 음성이 공개되어 신원이 특정될 수 있다는 두려움을 주어 범죄를 억제하는 효과도 기대할 수 있다.

현재 금융감독원과 국립과학수사연구원은 시민으로부터 제보 받은 보이스피싱 사기범의 목소리를 성분 분석하여 4회 이상 신고된 사기범의 목소리를 추출한 뒤 보이스피싱지킴이 사이트의 “바로 이 목소리” 코너를 통해 공개하고, 신원을 제보할 경우 최대 2천만원의 신고포상금을 지급하고,³⁴⁹⁾ 경찰청은 2015년부터 “범죄 신고자 등 보호 및 보상에 관한 규칙”에 따라 보이스피싱 신고보상금을 100만원에서 최고 1억원까지 올려 지급하고 있다. 하지만, 양 제도 모두 보이스피싱 음성을 제보하는 경우에 대한 신고포상금 제도가 없어 음성분석을 통해서 신원을 확보하기 위해 필요한 음성을 충분히 확보하는데 한계가 있다. 금융감독원과 경찰청의 신고포상금이 차이가 나는 것도 문제다.

이를 위해서는 먼저 보이스피싱이 개인정보에 해당하는지를 검토가 필요하다.

348) 전영균, 김현경, “AI 스피커 음성정보의 합리적 규제 방안에 대한 연구”, 미국헌법학회, 미국헌법연구 31(1), 2020.4, 170-171면

349) 금융감독원에서는 2017년 5월 현재 총 2,349건의 음성파일을 확보하였다. 보이스피싱지킴이 홈페이지,
http://phishing-keeper.fss.or.kr/fss/vstop/avoid/this_voice_1.jsp#,
(2020.10.03. 최종확인)

피해자 음성은 정보주체가 동의하는 절차를 만들거나 비식별화할 경우 문제가 없을 것인데, 범죄자의 음성이 논란이 될 수 있다. 음성파일은 목소리, 음색, 어조, 말투 등을 포함하고 있고, 대화 속에 나오는 부가적인 정보를 이용할 경우 개인을 식별할 수 있어 개인정보라고 해석할 여지도 있다. 하지만 통신사기피해환급법에서 금융위원회는 전기통신금융사기에 대한 대응조치(제3호)를 수행해야 하고, 업무의 일부를 금융감독원장에게 위탁할 수 있도록 명시하고 있어 금융감독원의 수집·이용은 개인정보보호법 제15조 제1항 제3호에 따라 ‘공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우’로 해석할 수 있다.³⁵⁰⁾

350) 금융감독원은 보이스피싱 의심 녹취파일 정보를 정보주체의 동의 없이 제3자에게 제공하거나 공개할 수 있을까? 우선 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」(이하 ‘통신사기피해환급법’) 제2조의2(전기통신금융사기에 대한 대응 등) 제1항에 따르면 금융위원회는 전기통신금융사기의 발생에 대응하고 그 피해를 최소화하기 위하여 전기통신금융사기에 관한 정보의 수집·전파(제1호), 전기통신금융사기에 대한 예보·경보(제2호), 그 밖에 대통령령으로 정하는 전기통신금융사기 대응조치(제3호)를 수행한다고 규정하고 있으며, 같은 조 3항은 위 제1항에 따른 업무의 일부를 금융감독원장에게 위탁할 수 있다고 명시하고 있다. 금융위원회의 업무를 위탁받은 금융감독원은 개인정보보호법 제15조 제1항 제3호에 따라 ‘공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우’ 개인정보를 수집할 수 있으며 그 수집 목적에서 이용할 수 있다. 따라서 금융감독원이 수사기관 등을 통해 제공받거나 신고자의 제보를 받아 수집한 보이스피싱 의심 녹취파일 정보를 보이스피싱 지킴이 홈페이지에 공개하는 것은 「개인정보보호법」 제15조 제1항 제3호에 따라 수집한 목적 범위에서 이를 제공하는 경우로서 동법 제17조(개인정보의 제공) 제1항 제2호에 따라 허용된다고 볼 수 있다. 민간 사업자에게 녹취파일을 제공하는 것도 금융감독원의 소관 업무를 민간 사업자를 통해 수행하고자 하는 것으로, 「개인정보보호법」 제26조에 따른 개인정보 처리업무 위탁의 방법에 의하면 문제 없이 가능한 것으로 사료된다. 뿐만 아니라 금융감독원이 보이스피싱 지킴이 사이트에서 보이스파일 의심 녹취파일을 신고받을 때는 개인정보 수집·이용 및 제공 동의서에 의해 명확한 동의 하에 신고인의 전화번호, 통신사, 발신번호, 수신시각, 이메일주소, 녹취파일 등을 수집·제공하고 있어 기관이 수집한 개인정보에 대한 기술적·관리적 보호조치만 충실히 이행한다면 「개인정보

하지만, 보이스피싱 음성에 대해서는 의심 녹취파일 수집, 음성정보 학습을 위한 통화 데이터 수집 등에 있어서 사안별 대책과 가이드라인을 마련해야 할 것이다. 음성정보는 저장·전송시 암호화하여 저장하여야 하고, 방송통신위원회가 발표한 ‘바이오정보 보호 가이드라인’도 준수하여야 한다.³⁵¹⁾

스마트폰 중 안드로이드 계열은 녹음 기능이 있지만 아이폰은 녹음기능이 없어 보이스피싱 음성을 녹음하는데 한계가 있다. 하지만 아이폰 AppStore에 통화 녹음 어플리케이션을 활용하면 녹음할 수 있기 때문에 원천적으로 불가능한 것은 아니다.³⁵²⁾ 범죄자 음성에 대한 동일성 확인 기술이 정확한지도 검토해야 한다. 앞서 살펴본 바와 같이 국립과학수사연구원은 2016년 이후 범죄자의 음성을 이용하여 금융감독원의 음성 데이터베이스를 분석하여 동일범을 찾아 여죄를 특정한 사례가 2건이 있어 실무적으로 증명이 되었다고 판단된다.³⁵³⁾ 그렇다고 100% 정확한

보호법」상 제기될 만한 이슈는 해소하고 있는 것으로 보인다.

351) 제1원칙(비례성 원칙), 제2원칙(수집·이용 제한의 원칙), 제3원칙(목적 제한의 원칙), 제4원칙(통제권 보장의 원칙), 제5원칙(투명성 원칙), 제6원칙(바이오정보 보호 중심 설계 및 운영의 원칙)

352) KT소식(2016.11), “‘보이스피싱 신고’ 기능 통해 피해 예방! 후후X금융감독원 ‘보이스피싱 예방 캠페인’ 진행”, <https://blog.kt.com/683>, (2020.10.20. 최종확인); 보이스피싱 예방 앱인 후후에 비슷한 기능이 있다. 안드로이드 버전에 한하여 보이스피싱 신고 메뉴가 존재하는데, 자동 녹음 설정을 해 놓고 통화를 하면 자동으로 통화 내용이 녹음되며 통화 녹음 목록에서 선택하여 신고 버튼을 누른다. 신고 버튼을 누르게 되면 연동된 이메일에 자동으로 메일 및 녹음 파일이 작성되고 전송 버튼을 누르면 신고가 완료된다. 후후에서 개발된 기능은 안드로이드에서만 가능하다는 단점이 있으며, 자동 녹음 설정, 통화녹음 목록에 들어가서 직접 신고 버튼을 눌러야 한다. 그리고 무엇보다 신고 방식이 이메일로 금융감독원에 메일을 보내는 형태이다 보니 스마트폰에 익숙치 않은 디지털 소외계층의 경우 이메일 설정이 되어 있지 않은 경우가 많으므로 신고가 어렵고 번거로울 수 있다. 제안한 앱의 자동신고 기능은 앱에서 보이스피싱 여부를 판단한 후 자동으로 용의자의 음성만을 추출하여 데이터베이스 서버로 전송하는 것이므로 실시간 대응으로 인한 신고 시간이 단축되고, 디지털 소외계층도 번거로운 절차 없이 신고가 가능하다.

것은 아니기 때문에 지속적으로 기술개발을 해야 할 것이다. 범죄자들이 음성에 노이즈를 포함하거나 AI를 이용하여 범행을 할 경우에도 대비해야 한다. 노이즈를 포함할 경우에는 시민들이 범죄로 인식할 가능성이 높아 오히려 예방에 기여할지도 모르겠다. 시민의 제보가 틀렸다 하더라도 수사기관 등에서 출입국관리기록을 확인하여 전화를 한 시점에 해외 체류사실을 확인하면 기술적 한계를 보완할 수 있다. 시민들의 참여가 결정적인데, 지금보다 신고포상금을 대폭 상향하여 지급하고, 용의자를 검거하거나 포상금을 지급하는 사례를 적극적으로 홍보하면 높은 수준의 참여를 이끌어 낼 수 있을 것이다. 마지막으로 시민들에게 통화 녹음을 조장하여 감시사회에 대한 우려가 있을 수 있으나 보이스피싱 범죄예방을 위한 국민들이 집단적 노력이라는 측면에서 설득할 수 있을 것이다.

2. 보이스피싱 피해자 구제 활성화

가. 보이스피싱 피해 보험제도 마련

보이스피싱 피해자의 대부분은 사회적 취약계층이 대부분으로 피해 발생 시 보험제도 통해 피해를 구제할 수 있는 제도를 만들어야 한다. 정부도 2020년 「보이스피싱 척결 종합방안」에서 보이스피싱 보험을 통한 피해구제를 활성화하겠다고 밝혔다. 현재 보험상품은 보장한도액 500만원을 기준으로 월 보험료는 300~500원 수준이고, 최대 보장금액이 1천만원으로 피해금액과 비교하면 턱없이 미흡하다. 삼성화재는 토스 서비스와 연동하여 연간 보험료 5,600원으로 최대 300만원을 보상해주는 보이스피싱 보험을 운영하고, 보험 선물하기 기능을 이용하여 부모, 노인층에게 확산되도록 마케팅하고 있다. 농협은행도 스마트피싱보호 서비스에서 보이스피싱이 발생하면 최대 300만원까지 보상을 해주는 보험서비스를 제공

353) 2016년 이후 충남경찰청에서 용의자를 검거한 후에 해당음성을 국립과학수사연구원에 의뢰하여 금융감독원의 데이터베이스에 있는 음성 중 동일한 20건을 추가로 확인하였고, 서울경찰청에서도 동일한 방법으로 17명에 대한 24건의 여죄를 추가로 확인하여 성과를 거두었다.

하고 있다. 보험상품이 출시되고 있으나 보장 금액이 제한적이고 이용도가 낮아 실질적인 피해 구제에 한계가 있다. 따라서 다양한 보험상품을 개발하고, 보장범위를 확대하는가 하면 판매채널도 통신대리점, 은행 등 금융회사 창구까지 확대하여 가입이 활성화될 수 있도록 해야 한다.³⁵⁴⁾

나. 금융기관 책임보험 제도 도입

보이스피싱에 대한 금융기관의 책임보험 제도를 도입하는 방안을 검토할 수 있다. 앞서 설명한 바와 같이 통신사기피해환급법에는 금융회사가 본인확인을 하지 않았거나, 정당한 피해구제 신청이 있었는데도 지급정지를 하지 않은 경우에만 배상 책임을 지도록 규정(제4조)하고 있어 피해자에게 배상되는 경우가 거의 없다. 보이스피싱 특성상 피해자가 부주의하였거나 과실이 있을 가능성이 높고, 금융회사와 과실 공방을 하더라도 유리한 위치에 서기 어렵다. 이러한 문제를 해결하기 위해 금융기관의 책임보험 제도를 검토할 필요가 있다. 책임보험 제도는 자동차손해배상책임보험, 원자력손해배상책임보험, 근로자재해보상보험, 재난배상책임보험, 개인정보 손해배상책임 보장제도 등 다양한 사례가 있다. 영국은 바클레이즈, HSBC, 로이드뱅크그룹, 스코틀랜드왕립은행(RBC)를 비롯하여 대형 은행 등 9개사가 보이스피싱 피해고객에 중과실이 없다면 은행이 전액을 보상해주는 파격적인 형태의 “사기피해 환불제도” 까지 도입하고 있다.

3. 선불·알뜰폰 본인확인 절차 강화

선불·알뜰폰 개통시 본인확인 절차를 강화하여야 한다. 대부분 비대면과 온라인을 통해 개통되는 만큼 본인확인에 취약하고 선불폰은 개통되면 명의도용 여부에 대한 확인이 어렵다. 알뜰폰 사업자들은 가입자로부터 신분증 등 진위여부 증서를

354) 과학기술정보통신부 보도자료, “디지털 경제의 신뢰 기반 조성을 위한 보이스피싱 척결 종합방안”, 2020.6.24.자

제시받아 육안으로 본인 여부를 확인한 후, 전기통신사업법 제32조의5에 규정된 부정가입방지시스템을 통해 부정가입을 차단하고 있으나 여전히 우회하는 방안이 존재한다. 비대면 개통시 공인인증, 신용카드, 화상통화 등을 활용하는 방안을 고려할 필요가 있다. 인터넷전문은행의 비대면 계좌 개설시 고객확인에 준하는 수준의 확인절차가 필요하다. 알뜰폰은 신분증 사진, 신분증과 얼굴이 함께 나온 사진 전송으로 개통³⁵⁵⁾이 가능하기 때문에, 정부에서 신분증의 위·변조를 식별할 수 있는 기술을 보급하는 것도 필요하다. 실제 2020년 관계부처가 합동으로 발표한 “보이스피싱 척결 종합방안”에서도 선불·알뜰폰 비대면 개통 시 본인확인 수단을 위조가 용이한 신분증 대신 공인인증이나 신용카드를 통해 진행하고, 사용기간이 경과한 선불폰은 즉시 퇴출하는 방안이 포함되어 있다. 단기간에 다 회선을 개통하지 못하도록 가이드라인을 마련하고, 선불·알뜰폰의 본인확인 횟수를 늘리기 위해 2020년 하반기부터 조사 주기를 6개월에서 4개월로 단축할 계획도 가지고 있다.

알뜰폰 사업자 스스로의 책임의식도 중요하다. 2020년 한국알뜰통신사업자협회에서 알뜰통신(MNVO)사업자들과 함께 유통망 점검을 강화하고 다회선 선불 개통에 따른 부정사용 방지·차단을 위해 자율규제를 전개하겠다는 선언은 의미가 있다.³⁵⁶⁾ 신규 판매점과 거래 계약을 체결할 때 부정판매점 이력을 확인한 후 안전하게 계약을 체결할 수 있도록 절차를 강화하고, 정부부처 및 수사기관 등으로부터 부정사용 회선을 접수받았을 경우 신속하게 조치하겠다는 것이다.

355) 머니투데이 보도(2020.6.16.), “위조신분증 한 장으로 대포폰 ‘뚝딱’ ...사진은 확인도 안했다”,
<https://news.mt.co.kr/mtview.php?no=2020061517082522711> (2020.12.30. 최종확인)

356) 아이뉴스24 보도(2020.6.30.), “알뜰폰협회, 보이스피싱 예방 가이드라인 마련”, 아이뉴스24, <http://www.inews24.com/view/1277682> (2020.12.30. 최종확인)

4. 인터폴 적색수배에 범죄자 얼굴공개 추진

보이스피싱 범죄자에 대한 온라인 공개수배를 활성화하고, 인터폴 적색수배를 하는 경우 얼굴 공개하는 것도 필요하다. 국내 수배자들은 자신의 일상 활동 중에 경찰에 의해서 검거될 가능성이 있는 반면, 해외 수배자들은 검거될 가능성이 전혀 없다. 따라서 온라인공개수배와 인터폴 적색수배(얼굴공개)를 통해서 보이스피싱 범죄자의 얼굴이 공개되어 해외에서도 현지 경찰이나 교민들의 제보할 수 있게 하여야 한다. 보이스피싱 범죄자들이 해외에서 활동하는데도 상당한 위축을 가져다 줄 것이다.

먼저 공개수배할 때 강력범죄뿐만 아니라 보이스피싱 범죄자도 대상에 포함되도록 하여야 한다. 경찰청의 종합 공개수배 제도는 경찰청의 “지명수배 등에 관한 규칙” 제9조에 따라 매년 상·하반기로 나눠 공개수배위원회를 열어 20명씩을 선정하고, 공개수배지 3만장을 인쇄하여 게시하고 있고, 인터넷 홈페이지나 스마트 국민제보 어플리케이션 ‘목격자를 찾습니다’를 통해서 게시한다.³⁵⁷⁾ 2010년 국가인권위원회는 인터넷상의 공개수배가 유·무죄 확정 이후에도 개인정보가 사이버 공간에 남는다는 이유로 인권 침해 소지가 있다고 제도 개선을 권고³⁵⁸⁾하여 지명수배 등에 관한 규칙을 만들어 엄격한 기준에 따라 공개수배 대상을 정하고 온

357) 이해환, 이동희, “언론을 활용한 긴급 공개수배의 범인 검거의 효과 분석(공개수배 포스터 상의 정보와 언론 노출빈도를 중심으로)”, 경찰대학 범죄수사연구원, 범죄수사학연구 6(1), 2020, 158면

358) 국가인권위원회는 경찰청의 온라인 공개수배 제도와 관련하여 법무부장관에게 「형사소송법」에 공개수배의 요건과 절차 등에 관한 근거를 마련하고, 인터넷 공개수배의 근거 규정을 신설할 것을 권고하고, 경찰청장에게 공개수배와 관련하여, 공개수배의 요건 및 절차 등에 관한 규정을 준수할 것, 인터넷 홈페이지에 게시된 공개수배자의 사진을 피의자 검거 후 즉시 삭제할 것, 인터넷 홈페이지에 게시된 공개수배자의 사진을 복제·유포할 수 없도록 기술적 보안장치를 마련하고 경고 문구를 삽입할 것, 그리고 공개수배 대상자 선정위원회에 외부인사를 포함시킬 것 등을 권고하였다.

라인상 수배내용의 유포를 차단하고 있다. 하지만, 2017년 이후 현재까지 종합 공개수배 대상에 특정범위반 범죄자는 다수 있는데 여기에 보이스피싱 범죄가 포함되어 있는지는 알 수 없다. 다만, 통신사기피해환급범위반인 범죄자는 포함되어 있지 않았다.

나아가 인터폴에 적색수배를 요청하는 경우 수배자의 얼굴까지 공개되도록 해야 한다. 적색수배서는 인터폴이 가지고 있는 가장 특색 있고 유용한 제도의 수배서로 국제지명수배서(International Wanted Notice)를 말한다. 적색수배서는 사전 구속영장 또는 체포영장이 발부된 자 중에서 ① 살인·강도·강간 등 강력범죄 사범, ② 폭력조직 중간보스 이상의 조직폭력 사범, ③ 50억 원 이상의 경제사범, ④ 기타 수사관서에서 특별히 적색수배를 요청하는 중요 사범에 대하여 범죄인인도를 목적으로 하는 경우에 발행한다.³⁵⁹⁾ ④항에 보이스피싱이 포함된다고 해석할 수 있기 때문에 근거도 분명하다. 미국 연방수사국(FBI)은 홈페이지 ‘Fugitives’ 중 Cyber 코너에서 이메일해킹 무역사기(Business Email Compromise)로 6백만불을 편취한 범죄자를 수배하고,³⁶⁰⁾ 80대 노인을 상대로 4만 5천불을 편취한 보이스피싱 범죄자를 공개수배하고 있다.³⁶¹⁾ 얼굴공개로 인한 프라이버시 침해에 대한 우려가 있지만,³⁶²⁾ 이미 국내에서 얼굴공개를 하고 있고, 보이스피싱 범죄가 수배 상태에

359) 김재덕, “인터폴을 통한 국제공조수사의 개선방안”, 원광대학교 법학연구소, 원광법학 27(3), 2011, 52~54면; 적색수배자는 발견국과 요청국 간에 범죄인 인도조약이 체결된 경우 발견국은 수배자를 체포하고 사무총국과 수배 요청국에 그 사실을 통보한다. 그후 범죄인은 범죄인인도조약에 따라 외교채널을 통해 요청국에 인도한다. 만약 체결되지 않았다면 발견국은 수배자를 발견 즉시 사무총국과 수배 요청국에 그 사실을 통보하고 수배자의 자국 내 동향을 감시한다. 그 후 범죄인은 외교채널을 통한 강제추방 등 국제관례에 따라 처리한다.

360) FBI, FBI Most Wanted Fugitives,
<https://www.fbi.gov/wanted/cyber/alex-afolabi-ogunshakin> (2020.12.30. 최종확인)

361) 한국일보 보도(2018.12.6.), “80대 노인상대 사기 용의자 공개수배”,
<http://dc.koreatimes.com/article/20181206/1218644> (2020.12.30. 최종확인)

362) 연합뉴스 보도(2020.1.28.), “적색수배에도 인터폴 사이트엔

서도 계속되는 경우가 많아서 죄질이 불량하고, 해외 범죄자에 대해서는 체포수단이 많지 않기 때문에 관련제도의 도입을 적극 논의하여야 할 것이다.

5. 국제기구 편당을 통한 아시아 지역의 수사작전 주도

인터폴 편당을 통해 아시아 지역의 보이스피싱 조직에 대한 수사작전(Investigation Operation)을 주도할 필요가 있다. 무엇보다도 보이스피싱에 대해서 짧은 시간에 강력한 효과를 거둘 수 있는 방법은 해외 콜센터 조직을 검거하는 것이다. 우리나라가 관련국과 국제공조하여 검거하는 방법도 있겠지만, 인터폴에 편당을 하여 인터폴의 이름으로 아시아 국가와 함께 보이스피싱에 대한 특별단속을 전개하는 것도 방법이다.

경찰청에서 2020년 3월부터 2023년 2월까지 총 3년 동안 사이버경제범죄와 온라인성착취물 단속을 위하여 인터폴에 편당하기로 결정하고, 2020년도에 총 15.32억원을 확보하여 사이버경제범죄(5.72억원)와 온라인 성착취물(9.6억원)의 단속에 지원하기로 하였다.³⁶³⁾ 주요국과 공조하고 전문가 그룹을 통한 수사기법을 공유하는가 하면 캄보디아, 필리핀의 콜센터 소재지 등 해외 거점 조직에 대한 단속을 전개할 계획이다.³⁶⁴⁾ 인터폴은 보이스피싱을 비롯한 사이버경제범죄를 대상으로 ① 개별국 수사역량 강화 및 수사활동 지원 ② 광범위한 범죄정보 수집과 과학적 분석 ③ 회원국 합동검거 기획·시행을 시행할 것이다.³⁶⁵⁾ 하지만, 연간 5.72

‘전무’…이유는?” , <https://www.yna.co.kr/view/MYH20200128002700038>
(2020.10.20. 최종확인)

363) 경찰청 내부자료(2020).

364) 아시아경제 보도(2020.02.11.), “ ‘아동포르노·보이스피싱’ 근절 맞손…첫 편당사업” , <https://www.asiae.co.kr/article/2020021114193232576> (2020.10.03. 최종확인)

365) 인터폴 회원국이 ① 범죄정보 및 회원국 요구사항 수집, ② 세계 사이버경제범죄 현황진단, ③ 회원국별 제한사항 도출, ④ 회원국과 컨설팅을 통한 해결책 제시, ⑤ 사업 참여국 전체회의 개최, ⑥ 연 1회 이상 합동검거 시행, ⑥ 성과보고 및 환류 등의 순으로 진행하여 성과를 거양할 방침이다.

역원을 편당하여 아시아지역의 보이스피싱 조직을 소탕할 수 없기 때문에 과감한 편당을 통하여 주변국의 참여를 이끌어 내야 할 것이다.

6. 범죄단체조직죄 적용을 통한 강력한 처벌

보이스피싱은 대부분 조직범죄의 형태를 가지고 있기 때문에 형법 제114조에 범죄단체조직죄로 강력하게 처벌해야 한다. 최소한의 통솔체계를 갖춘 형법상의 ‘범죄단체’에 해당하고 보이스피싱 조직의 업무를 수행한 피고인들에게 범죄단체 가입 및 활동에 대한 고의가 인정된다면 처벌이 가능하다. 범죄단체가 안된다면 범죄집단으로 의율할 수 있다. 사기에 직접 가담하진 않았지만 범죄 목적을 달성 하는데 기여한 경우에 처벌할 수 있고, 목적 범죄에 대한 실행의 착수까지는 이르지 못한 예비·음모도 처벌이 가능하다.³⁶⁶⁾³⁶⁷⁾

한편, 대포통장 양수·양도 행위에 대해서 범죄단체·범죄조직죄를 적용하여 엄벌해야 한다. 전자금융거래법을 개정하여 대포통장 양수·양도 등의 행위에 대한 법정형을 5년이하 징역 또는 3천만원 이하의 벌금으로 상향시켜 형법상 범죄단체조직죄의 대상이 되었다. 그간 대포통장의 불법행위에 다소 관대하였으나 보이스피싱이 계속되는 이유가 대포통장의 공급이라고 할 때 마냥 가벼운 범죄로 인식할 수 없는 것이다.

366) 하담미, “보이스피싱 조직의 범죄단체 의율에 관한 제문제”, 대검찰청, 형사법의 신동향 58, 2018, 342-343면

367) 대법원 2009.9.10. 선고 2008도10177 판결

제3절 기술적 개선방안

1. 보이스피싱 대응기술 프레임워크 설계

보이스피싱 대응기술을 ① 발신번호변작 차단·탐지, ② 네트워크 패킷분석, ③ 통신패턴분석 ④ 심박스 전파탐지, ⑤ 음성인식, ⑥ 텍스트추출, ⑦ 악성앱탐지, ⑧ 데이터분석 등 8가지로 구분하였다. 향후 보이스피싱 대응기술 프레임워크를 중심으로 우리나라의 보이스피싱 대응기술의 수준을 진단하고, 연구개발사업의 기획의 기초자료로 활용할 수 있을 것이다. 이와 같은 기술개발을 통해 입법적·제도적 다양한 정책들을 뒷받침할 수 있을 것이다.

<표 7-1> 보이스피싱 대응기술 개요

분류		세부내용
① 발신번호 변작 차단·탐지		· 범죄자가 발신번호를 변작하여 통화하는 행위를 차단·탐지하는 기술
② 네트워크 패킷분석		· 패킷헤더에서 ① 발신을 어디로 했는지에 대한 발신번호(피해자 번호), ② SIM Bank, SIM Box의 IP주소, ③ IP-PBX의 IP주소, ④ 실시간 음성 등을 수집하여 탐지하는 기술(감청이슈 발생)
③ 통신패턴분석		· 보이스피싱 통화를 분석하여 패턴을 모델링하여 탐지하는 기술
④ 심박 스 전파 탐지	3G 전파탐지	· 전파탐지연구소의 Analyzer, 스펙트럼 분석기로 3G 미세신호를 확인하여 심박스의 설치장소를 탐지하는 기술 · 차량에 심박스를 싣고 이동하는 범행형태는 탐지 곤란
	4G 전파탐지	· 전파신호 탐지의 길이(거리)가 짧고, 신호 사용자가 많은 4G(LTE) 심박스 탐지에 한계 · 4G(LTE)를 3G로 다운그레이드하여 탐지하는 방식 검토
⑤ 음성 인식	범죄자 음성인식	· 화자인식 방법을 통해 범죄자의 음성 성문군집을 생성하여 동일인의 음성을 식별하는 기술 · 음성확보 및 녹음 어려움, 노이즈가 포함된 음성인식 한계

	피해자 음성·감정인식	<ul style="list-style-type: none"> · 피해자 음성의 감정을 분석하여 보이스피싱 탐지하는 기술 · 피해자 스스로 설정할 수 있어 범죄자 음성에 비해 사용 용이
⑥ 텍스트 추출	음성에서 텍스트 추출	<ul style="list-style-type: none"> · 범행에 사용되는 전화번호, 계좌번호의 연계데이터를 시각화, 관계분석 등을 통해서 보이스피싱 탐지하는 기술 · IBK피싱스탐, 후후컴퍼니, 피싱아이즈 등에서 활용
⑦ 악성 앱 탐지	악성앱 분석	<ul style="list-style-type: none"> · 악성앱의 코드를 분석하여 악성여부를 판단하여 탐지하는 기술
	악성링크 탐지	<ul style="list-style-type: none"> · SMS 분석을 통해서 보이스피싱 여부를 탐지하는 기술
⑧ 데이터분석	SNA분석(i2)	<ul style="list-style-type: none"> · 중심성 원리와 하위집단분석원리를 중심으로 사회연결망 분석(SNA) 알고리즘을 반영한 수사기술
	금융계좌분석	<ul style="list-style-type: none"> · 금융계좌 분석을 통해서 자금세탁, 범죄수익은닉 등을 찾아내는 기술
	암호화폐 추적	<ul style="list-style-type: none"> · 비트코인, 이더리움 등 암호화폐를 추적·분석하는 기술

2. AI 기반 보이스피싱 음성 활용 연령대별 체험형 홍보활동 전개

AI 기반으로 범죄자의 보이스피싱 음성을 활용하고, 연령대별로 가장 많은 피해를 당하는 시나리오를 채택하여 국민들이 직접 듣고 체험할 수 있는 서비스를 보급할 필요가 있다. 금융감독원에서 “보이스피싱 체험관”을 운영하여 전화금융사기 범의 음성통화내역을 청취하는 단계를 넘어 직접 대화하는 형태로 보이스피싱을 체험하는 것이다. 국가, 지방자치단체, 수사기관 및 민간에서 공익광고에서 유튜브 광고까지 다양한 예방활동을 하지만 강의, 문자, 영상 등의 전달 방식으로는 한계가 있을 수 밖에 없다. 실제 음성으로 실제 사례를 활용하여 대화하는 방식으로 직접 체험을 해보는 것이다. 범죄자들이 사용했던 시나리오, 수법, 음성을 최대한 활용하고, 20대는 취업, 30~40대는 대출 등으로 연령대별로 주제를 선정하여 효

과를 극대화할 수 있을 것이다. 사전에 보이스피싱 예방 캠페인이라는 사실을 명확히 알려주고, 발신전화 번호도 하나로 통일하여 혼선이 발생하여 신고하거나, 신고가 되더라도 즉시 상담이 가능한 체계를 만들어야 할 것이다. 범죄자들이 사용하는 최신의 내용으로 실시간으로 업데이트 하여 운영하면 더욱 효과가 좋을 것이다.

3. 범죄자 음성 식별기술 및 피해자 감정인식 기술 개발

금융감독원에서 수집한 보이스피싱 범죄자의 음성을 분석하고, 상습범을 특정하기 위해 음성인식 기술을 고도화해야 한다.³⁶⁸⁾ 보이스피싱에 대한 범죄자들의 은어도 확보하고 해석해야 한다. 보이스피싱 방지 앱, 이상행위 모니터링 시스템 등에 연계하여 알고리즘을 발전시키는데도 활용할 수 있다. 앞서 살펴본 바와 같은 국립과학수사연구원은 데이터베이스에 저장된 음성 파일에 대한 i-vector를 획득한 후, 전체 음성파일에 대한 i-vector의 코사인 유사도 행렬을 생성하였으며, 상호 유사도가 높은 후보군들에 대해 군집 구성을 통해 용의자의 여죄를 추가로 밝혀냈다.³⁶⁹⁾ 대검찰청도 “용의자 음성식별을 위한 한국인 음성 데이터베이스 수집 및 음성 자동분석 시스템 개발”, “용의자 음성식별을 위한 한국인 표본 데이터베이스 구축” 등의 과제를 수행하여 연구성과를 가지고 있다.³⁷⁰⁾ 하지만, 대용량의 음성 DB에서 동일한 음성을 선별하거나 특정 용의자의 음성과 동일한 음성

368) 보이스피싱 단체 내 공범의 데이터를 사기 시나리오에서 사칭 시 사용하였던 담당 이름(예를 들어, 00지점의 00점사, 00은행의 000대리), 피의자 성별, 범행 이용 전화번호 등에 대해서 1차 필터링 후, 텍스트 유사도가 높은 음성 파일을 추려 그룹핑이 이루어진다면, 검거된 피의자 뿐만 아니라 피의자가 속한 조직의 공범을 간접적으로 확인할 수 있다.

369) 박남인, 전옥엽, 김태훈, 이중, “보이스피싱 음성 파일에 대한 법과학적 화자 분석 방법의 적용 사례”, 한국디지털포렌식학회, 디지털포렌식연구 13(1), 2019, 35-44면

370) 신지영, “한국인 표준 음성 DB 구축(II)”, 한국음성학회, 말소리와 음성과학 9(2), 2017, 9면

을 자동분석하는 기술은 쉽지 않기 때문에 연구가 필요하다. 나아가 음성 비식별화 기술³⁷¹⁾과 음악, 소음 등 노이즈 제거 기술도 함께 병행해야 할 것이다.

한편, 보이스피싱 피해자 음성에 대한 감정인식 기술의 개발도 필요하다. 보이스피싱 대응기술 개발은 주로 범죄자 음성을 중심으로 이루어졌으나 피해자는 일반적으로 지시를 받기 때문에 “예”와 같은 단어가 많고, 놀람, 당혹, 다급 등 감정 표출이 많아 식별 가능성이 높을 수 있다. 자신의 스마트폰에 탐지기능을 내장할 경우 개인정보 이슈 등 복잡한 절차 없이 활용할 수 있을 것이다.

4. 금융기관 보이스피싱 FDS 구축 의무화

보이스피싱과 같은 이상금융거래를 모니터링 할 수 있는 FDS(Fraud Detection System)를 구축할 필요가 있다. 전자금융거래법 보다 구체적으로 전자금융감독규정에 FDS에 관한 내용을 포함하여 정책화해야 한다. 나아가 통신사기피해환급법(제2조의5)에 따라 피해의심거래계좌에 대한 임시조치 의무를 해태한 금융회사에 대한 주의·경고, 과태료 부과도 필요할 것이다. FDS는 일반적으로 ① 금융거래 이용자의 금융거래 정보수집 및 가공 단계, ② 금융거래 정보와 이상금융거래 유형 정보를 머신러닝으로 분석하는 이상거래 탐지 단계, ③ 이상거래로 탐지된 거래에 대해 추가 인증하거나 차단하는 단계로 이루어져 왔다.³⁷²⁾

5. 4G 이용 심박스 탐지기능 개발

보이스피싱 범죄자들이 4G 기반으로 심박스를 이용하는 경우 해당 전파를 탐지할 수 있는 기술을 개발하여야 한다. 국내 LTE 주파수를 모두 지원하면서 통신사 협조를 통해 제공받은 기지국정보, IMSI, TMSI 정보를 활용하여 발신 위치를 탐

371) 전영균, 김현경, “AI 스피커 음성정보의 합리적 규제 방안에 대한 연구”, 미국헌법학회, 미국헌법연구 31(1), 2020, 170-171면

372) 이승용·이주락, “빅데이터와 FDS를 활용한 보이스피싱 피해 예측 방법 연구”, 한국경호경비학회, 시큐리티연구 62, 2020, 195-196면

지할 수 있는 장비도 개발해야 한다. 3G를 이용하는 경우 통신사와 공조를 통해 발신기지국, 중계기 위치 등을 협조 받아 심박스 의심 설치장소를 특정하고 전파 탐지기를 통하여 추적할 수 있다. 하지만, 다수의 사용자가 이용하는 LTE 전파를 이용하는 심박스는 추적하기 어렵다. 국내 LTE는 LTE-A방식으로 전체 주파수를 항상 사용하면서 주파수를 분할해서 각 사용자 단말기와 연결되며 셀 중첩에 의한 간섭 최소화를 위해 CoMP(Coordinated MultiPoint), eICIC(enhanced Inter Cell Interference Coordination)의 기술을 사용하기 때문에 통신 시에만 전파를 전송하는 3G 탐지 장치로는 추적할 수 없다. 심박스 추적은 신고된 전화번호를 바탕으로 하여 해당 단말기의 IMEI값을 도출한 후 해당 IMEI가 접속한 중계기 또는 기지국을 반경을 중심으로 삼각측량하는 방법으로 접속위치를 알아낸다. 휴대용 전파탐지기(스펙트럼 분석기)를 통해 일일이 방문 수색하는 방식으로 IMEI 변조에 대응하거나 심박스와 안테나를 분리하여 연결한 장비를 추적하기도 한다.

나아가 국내 LTE 주파수를 모두 지원하면서 LTE Signaling Process를 이용하여 탐지기로부터 발신 단말기의 방향과 위치를 알 수 있도록 추적장비가 필요하다.³⁷³⁾ 수사기관이 압수수색 영장을 발부받아서 범죄자들이 사용하는 4G 통신을 3G로 다운그레이드 할 수 있는 기술도 필요하다. 수사기관은 보이스피싱 범죄자들이 사용하는 심박스 위치가 어느 정도 좁혀질 경우에 해당 지역에 이동통신사가 유선 인터넷망 서비스를 위하여 할당한 IP주소의 정보를 바탕으로 용의자를 추적해 볼 수 있을 것이다.

6. 범죄수의 추적 기술 개발

수사기관, 국세청, 금융정보분석원 등이 통합하여 보이스피싱 범죄자의 범죄수익을 추적할 수 있도록 관련기술을 개발하여야 한다. 수사기관은 국세청에 계좌정보를 제공하여 누적·관리하면서 추적할 수 있도록 하고, 금융정보분석원에서는 관

373) 2020년 8월 10일 트루네트웍스 소장을 인터뷰하여 장리한 것임.

런계좌를 확인하였을 경우 수사기관에게 통보하여 주어야 한다. 암호화폐를 이용하여 자금세탁하는 경우에 이를 분석할 수 있는 기술도 필요하다. 그래야 불법수익을 몰수·추징할 수 있다.

한편, 금융기관과 FIU에서 자금추적·분석을 강화할 수 있도록 허용해야 한다. 피의자의 통화내역, 금융거래를 중심으로 분석하고 용의자를 검거하였을 때 금융거래 패턴을 분석하여 보이스피싱 총책이 자금세탁하는 패턴까지 탐지해서 분석해야 한다.

제8장 결론

보이스피싱은 악성앱 설치, URL을 통한 원격 악성코드 유포, 심박스를 활용한 전화번호 변작, 암호화폐 이용 자금세탁 등 지금 이 순간에도 진화하고 있다. 보이스피싱의 유형이 재빠르게 바뀌고, 피해가 커지면서 사후적·단속적 대응은 한계를 보여 사전적·예방적 대응이 강하게 요구되고 있다.

이에 본 연구는 신종 보이스피싱 유형에 대한 범행수법과 대응기술을 살펴보고 제도적·기술적 개선방안을 제시하고자 노력하였다. 제2장에서는 보이스피싱의 개념과 범죄실태 그리고 신종 보이스피싱의 유형에 대해서 살펴보았다. 제3장에서는 보이스피싱 범행수법과 대응기술을 분석하였다. 문헌연구 및 수사관 인터뷰를 통해서 보이스피싱 조직 체계와 역할을 조사하였고, 범죄조직을 이해하기 위해 범죄자들이 사용하는 은어도 84개 수집하여 분석하였다. 범행수법을 6가지로 유형화하고, 이에 맞는 대응기술 8가지를 도출하여 기술진단을 실시하였다. 제4장에서는 신종 보이스피싱에 대한 정부의 대응정책을 분석하고 평가하였다. 정부가 종합 대책을 수립하고, 통신사기피해환급법과 같은 특별법을 제정하는가 하면 법제와 기술을 병행한 정책을 추진하였다는 측면에서 긍정적으로 보았다. 하지만, 기존 정책에 대한 비판 없이 새로운 정책을 계속하여 수립하고, 다수의 대안들이 현재의 문제해결에만 천착하고 있어 미래범죄에 대한 예측과 중장기적인 법제·기술 준비는 부족한 것으로 보았다. 제5장에서는 신종 보이스피싱에 대한 법률과 쟁점을 분석하였다. 보이스피싱과 관련 있는 통신사기피해환급법, 정보통신망법, 전기통신사업법 등 총 11개의 법률을 검토하고 쟁점을 도출하여 대안을 제시하였다. 현재 국회에 계류 중인 통신사기피해환급법 관련 5개 법률안을 비교분석을 하였다. 법률안 내용 중에서 전기통신금융사기에 재물을 포함하는 법안, 보이스피싱 거버넌스 체계를 마련하는 법안에 대해서는 긍정적으로 해석하였고, 전기통신금융사기의 법정형을 무기징역 또는 10년 이상의 징역으로 하자는 법안에 대해서는 부

정적으로 판단하였다. 제6장에서는 해외 신종 보이스피싱 대응체계 및 법제를 살펴보았다. 미국, 독일, 일본, 중국의 범죄동향, 대응체계, 대응법률 및 추진정책을 조사하였다. 각국마다 범죄현상이 상이하고, 대응체계와 법률마다 상이하여 단순 비교는 어렵지만, 우리나라에 의미 있는 시사점을 제시하여 주었다.

마지막으로 제7장에서는 신종 보이스피싱 대응을 위한 정책적·기술적 개선방안으로 입법적, 제도적, 기술적으로 분류하여 총 17개를 제시하였다. 입법적 개선방안은 ① 해외 발신전화 차단에 대한 기술적 조치 의무화, ② 금융기관의 보이스피싱에 대한 배상책임 강화, ③ 통신제한조치 대상에 전기통신금융사기죄 포함, ④ 상습 전과자 신상정보 공개제도 도입, ⑤ 전기통신금융사기 취득객체에 재물 포함 등을 제시하였다. 제도적 개선방안은 ① 보이스피싱 음성·신원 제보자 포상금 확대, ② 보이스피싱 피해자 구제 활성화, ③ 선불·알뜰폰 본인확인 절차 강화, ④ 인터폴 적색수배에 범죄자 얼굴공개 추진, ⑤ 국제기구 펀딩을 통한 아시아 지역의 수사작전 주도, ⑥ 범죄단체조직죄 적용을 통한 강력한 처벌을 주장하였다. 마지막으로 기술적 개선방안은 ① 보이스피싱 대응기술 프레임워크 설계, ② AI기반 보이스피싱 음성 활용을 통한 연령대별 체험형 홍보활동 전개, ③ 범죄자 음성 식별기술 및 피해자 감정인식 기술 개발, ④ 금융기관 보이스피싱 FDS 구축 의무화, ⑤ 4G이용 심박스 탐지기술 개발, ⑥ 범죄수익 추적기술 개발 등을 제시하였다.

본 연구에서 제시한 다양한 개선방안들이 정부의 정책과 입법의 기초자료로 활용되어 우리나라를 비롯하여 전 세계의 보이스피싱 해결에 기여할 수 있기를 바란다.

참 고 문 헌

□ 국내 문헌

○ 저서

배종대, 형법각론 제6전정판, 홍문사, 2007

_____, 형법각론 제7전정판, 홍문사, 2011

○ 논문

권철홍 · 송승규 · 김종열 · 김근호 · 장준수, 감정 인식을 위한 음성 특징 도출,
한국음성학회, 말소리와 음성과학 4(2), 2012

김근혜, 트럼프 행정부의 주요기반시설 사이버보안 정책분석에 관한 연구, 한
국정보보호학회, 정보보호학회지 29(4), 2019

김대근, 기술적 수단을 사용한 사이버 금융사기범죄의 실태와 형사정책적 대
응방안, 한국형사정책연구원, KIC ISSUE PAPER 14, 2016

_____, 다중사기범죄의 현상에 대한 비판적 고찰과 규범적 대안 : 다중사기
범죄 등 규제 기본법의 법제화를 위한 시론, 한국형사정책연구원,
형사정책연구 29(3), 2018

김대근 · 임석순 · 강상욱 · 김기범, 신종금융사기범죄의 실태 분석과 형사정책
적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심
으로, 한국형사정책연구원, 형사정책연구원 연구총서 16, 2016

김덕용, 보이스피싱에 대한 경찰의 대응방안에 관한 연구, 한국디지털콘텐츠
학회, 한국디지털콘텐츠학회논문지 19(1), 2018

김도경 · 김윤중, 음성감정데이터베이스의 분석과 프레임 단위 특징과 발음단

- 위 특징을 통합하는 Attention mechanism을 이용한 음성 감정 인식 시스템의 개발, 한국정보과학회, 정보과학회논문지 47(5), 2020
- 김도윤, 한·중 전기통신금융사기범죄 및 관련 제도의 현황과 시사점, 한중법학회, 중국법연구 41, 2020
- 김동민, 접근매체를 이용하는 전자금융사기의 범위에 관한 소고, 충남대학교 법학연구소, 법학연구 31(2), 2020
- 김민서·문종섭, STFT와 RNN을 활용한 화자 인증 모델, 한국정보보호학회, 정보보호학회논문지 29(6), 2019
- 김선주, USIM 정보를 활용한 패스워드리스 방식의 개인키 보호 방안, 한국콘텐츠학회, 한국콘텐츠학회논문지 17(6), 2017
- 김성희·장로사, 사회 연결망 분석 연구동향 및 정보학 분야에서의 활용가능성에 대한 연구, 한국정보관리학회, 정보관리학회지 27(4), 2010
- 김일수·배종대·이상돈, 정보화사회에 대비한 형사법적 대응, 한국비교형사법학회, 비교형사법연구 3(2), 2001
- 김자영, 러시아 마피아 집단의 특수어 연구 : 은어를 중심으로, 배제대학교 한국-시베리아센터, 한국시베리아연구 16(2), 2012
- 김재덕, 인터폴을 통한 국제공조수사의 개선방안, 원광대학교 법학연구소, 원광법학 27(3), 2011
- 김지온, 사회연결망 분석원리의 범죄 수사상 활용방안에 관한 연구, 한국디지털포렌식학회, 디지털포렌식연구 13(2), 2019
- 김진만·정종수, 명령 발화의 감정별 음성 특징 연구, 한양대학교 동아시아문화연구소, 동아시아문화연구 81, 2020
- 김학범, 미국의 사이버보안 및 사회기반시설 보안기관법에 관한 연구, 한국사회안전범죄정보학회, 한국정보범죄연구 5(1), 2019
- 김현서·송문호, 가상화폐의 몰수 - 대법원 2018. 5. 30. 선고 2018도3619 판결 -, 전북대학교 동북아법연구소, 동북아법연구 12(2), 2018

- 김혜정, 성범죄자 정보등록열람제도에 관한 검토, 한국형사정책연구원, 형사정책연구 18(3), 2007
- 박남인·전옥엽·김태훈, 이중, 보이스피싱 음성 파일에 대한 법과학적 화자 분석 방법의 적용 사례, 한국디지털포렌식학회, 디지털포렌식연구 13(1), 2019
- 박진성, 주요국의 전자금융 사기피해 구제제도에 대한 비교 연구: 범경제학적 접근, 한국무역연구원, 무역연구 11(5), 2015
- 박찬걸, 전기통신금융사기 관련 범죄의 가벌성 검토, 홍익대학교 법학연구소, 홍익법학 21(3), 2020
- 박형우·배명진, 목소리 분석을 통한 보이스피싱 예방에 관한 연구, 인문사회과학기술융합학회, 예술인문사회융합멀티미디어논문지 7(3), 2017
- 손남호·이호영·황효성, 감정발화의 데이터베이스 구축과 음향 분석, 사단법인 한국언어학회, 언어학 72, 2015
- 신지영, 한국인 표준 음성 DB 구축(II), 한국음성학회, 말소리와 음성과학 9(2), 2017
- 우동연·박세웅, 모바일 기가 통신 : MPTCP 기반 LTE/Wi-Fi 묶음 기술, 한국통신학회, 정보와 통신 열린강좌 33(12), 2016
- 윤동호, 통신사기피해환급법의 정보·명령입력죄의 구성요건적 의미와 한계, 한국형사정책학회, 형사정책 32(1), 2020
- 윤두영, 이동전화 선불요금제 현황 및 시사점, 정보통신정책연구원, 정보통신방송정책 23(1), 2011
- 윤은경, 방언 간 코드 스위칭으로 인한 감정 발화의 음성적 변화: 예비 한국어 교원을 대상으로, 한국외국어대학교 언어연구소 언어와언어학 70, 2016
- 이경재, 성범죄자 신상정보공개제도의 문제점과 개선방안, 강원대학교 비교법학연구소, 강원법학 33, 2011

- 이기수, 최근 보이스피싱의 범죄수법 동향과 법적 대응방안, 경찰대학 범죄수사연구원, 범죄수사학연구 4(2), 2018
- 이서배, 한국어 감정 음성에서 모델로 추출한 피치 곡선 연구, 한국언어과학회, 언어과학 25(3), 2018
- 이승용 · 이주락, 빅데이터와 FDS를 활용한 보이스피싱 피해 예측 방법 연구, 한국경호경비학회, 시큐리티연구 62, 2020
- 이용훈, 보이스피싱의 행위별 죄책에 관한 형법적 연구, 단국대학교 대학원, 석사학위 논문, 2020
- 이은진, 전기통신금융사기 피해자 구제에 관한 연구, 고려대학교 법무대학원 석사학위논문, 2018
- 이한구 · 이기성, 강인한 정합과정을 이용한 텍스트 종속 화자인식에 관한 연구, 대한전기학회, 대한전기학회 학술대회 논문집 25(2), 2002
- 이현영 · 강승식, 워드 임베딩과 딥러닝 기법을 이용한 SMS 문자 메시지 필터링, 한국스마트미디어학회, 스마트미디어저널 7(4), 2018
- 이혜환 · 이동희, 언론을 활용한 긴급 공개수배의 범인 검거의 효과 분석(공개수배 포스터 상의 정보와 언론 노출빈도를 중심으로), 경찰대학 범죄수사연구원, 범죄수사학연구 6(1), 2020
- 임석순, 피싱(phishing)에 대한 형법적 이해와 새로운 구성요건 창설의 필요성, 안암법학회, 안암법학 48, 2016
- 전영균 · 김현경, AI 스피커 음성정보의 합리적 규제 방안에 대한 연구, 미국헌법학회, 미국헌법연구 31(1), 2020
- 정육상, 국제범죄의 새로운 양상과 그 대응방안, 한국범죄심리학회, 한국범죄심리연구 7(1), 2011
- 정의석 · 임종인, 전기통신금융사기 사고에 대한 이상징후 지능화(AI) 탐지 모델 연구, 한국정보보호학회, 정보보호학회논문지 29(1), 2019
- 조성문 · 김미희, 남녀 분노 발화의 음성적 특징, 한국언어문화학회, 한국언어

문화 68, 2019

조성호 · 최성욱, IP-PBX를 이용한 혼합형 전화통신망과 IP-Phone 망과의 비교연구, 융복합지식학회, 융복합지식학회논문지 6(2), 2018

차영민 · 송영시, 보이스피싱 범죄의 실태와 피해자의 손해보전 방법에 관한 소고, 조선대학교 법학연구원, 법학논총 21(2), 2014

최영진 · 양창훈, 경찰 범죄정보 수집 활동의 관계망 분석:비공식적 사회연결망 분석을 중심으로, 한국콘텐츠학회, 한국콘텐츠학회논문지 20(1), 2020

최창수, 미국의 온라인 피싱사기방지법과 시사점, 법조협회, 法曹 63(10), 2014

표학길, 4G에 대비한 정보통신정책, 한국통신학회, 한국통신학회지(정보와통신) 19(7), 2002

하담미, 보이스피싱 조직의 범죄단체 의율에 관한 제문제, 대검찰청, 형사법의 신동향 58, 2018

홍성삼, 피싱 사기범죄에 대한 인터폴 및 국가별 대응정책 비교연구, 원광대학교 경찰학연구소, 경찰학논총 14(1), 2019

○ 보고서

금융보안원, 2018 사이버 위협 인텔리전스 보고서 [보이스피싱 악성 앱 프로파일링], 금융보안원 보고서, 2018

신지영, 용의자 음성식별을 위한 한국인 음성 데이터베이스 수집 및 음성 자동분석 시스템 개발, 대검찰청 연구과제, 2014

_____, 용의자 음성식별을 위한 한국인 표본 데이터베이스 구축, 대검찰청 연구과제, 2014

윤해성 · 곽대경, 보이스피싱의 예방과 대책마련을 위한 연구, 한국형사정책연구원, 형사정책연구원 연구총서 9(15), 2009

윤해성·김유근, 보이스피싱 피해유형별 구체적 예방방안에 관한 연구, 대검
찰청 보고서, 2017

이진국·이운제·박정수, 미국 FinCEN의 자금세탁 방지제도 운영실태 연구,
금융위원회 연구보고서, 2008

한국인터넷진흥원, 미국, 영국, 독일 기반보호법 체계에 관한 연구, 한국인터
넷진흥원 보고서, 2010

○ 판례

대법원 1961.5.12. 선고 4294형상101 판결

대법원 1976. 12. 14. 선고 76도3267 판결

대법원 1981.11.24. 선고 81도2608 판결

대법원 1985.10.8. 선고 85도1515 판결

대법원 1987. 3. 24. 선고 87도157 판결

대법원 1991. 1. 15. 선고 90도2301 판결

대법원 1991. 12. 24. 선고 91도2397 판결

대법원 1991. 5. 28. 선고 91도739 판결

대법원 2005.7.15. 선고 2004도1565판결

대법원 2009.9.10. 선고 2008도10177 판결

대법원 2013.4.11. 선고 2010도13774 판결

대법원 2016. 2. 19. 선고 2015도15101 전원합의체 판결

대법원 2017. 10. 26. 선고 2017도8600 판결

대법원 2017. 10. 26. 선고 2017도8600 판결

대법원 2018. 5. 30. 선고 2018도3619 판결

서울고등법원 2015. 4. 24. 선고 2014노3497 판결

서울고등법원 2017. 5. 19. 선고 2017노209 판결

서울고등법원 2017. 5. 19. 선고 2017노209 판결

대구지방법원 2017.1.19. 선고 2016고단5392 판결

서울서부지방법원 2015. 5. 1. 선고 2015노331 판결

수원지방법원 안산지원 2016. 12. 16. 선고 2016고합203, 220(병합), 242
(병합), 245(병합), 2016초기126, 289, 334 판결

인천지방법원 2019. 11. 28. 선고 2019고단5751 판결

□ 해외 문헌

○ 논문

Astrid Brandt, “Zur Strafbarkeit des Phishing-Gesetzgebung vs. Technologie“,
Kovac, Dr.Verlag 1, 2010

Bundeskriminalamt, “Bundeslagebild Cybercrime 2018“, 2019

Christoph Stamme, “Einblick in die Cybercrime am Beispiel des Phishing“,
Hochschulbibliothek HWR Berlin 4, 2014

DAWES centre for future crime at UCL, “DAWES CENTRE FOR FUTURE
CRIME ANNUAL REPORT 2020”, 2020

FBI IC3, “2019 Internet Crime Report”, 2019

U.s. Department of Justice (COR), “Prosecuting Computer Crimes”,
CreatespaceIndependentPub, 2017

INTERPOL, CYBERCRIME: COVID-19 IMPACT, 2020

Jonathan Rosenberg, The Session Initiation Protocol:Internet-Centric
Signaling, IEEE Communications Magazine 38(10), 2000

Jyoti B. Ramgire, Sumati M.Jagdale, A Survey on Speaker Recognition
With Various Feature Extraction And Classification Techniques,
International Reserch Journal of Engineering and Technology
(IRJET) Vol 03 Issue 04, 2016

Richard L. Bourgeois, Jr./S. P. Hennessey/Jon Moore/Michael E. Tschupp,
Racketeer Influenced and Corrupt Organizations, American
Criminal Law Review 37, 2000

Sandhya Mishra, Devpriya Soni, Smishing Detector: A security model to
detect smishing through SMS content analysis and URL behavior
analysis, Future Generation Computer Systems 108, 2020

Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Bitcoin,
2008

Z. Aziz · R. Bestak, Analysis of Call Detail Records of International Voice
Traffic in Mobile Networks, 2018 10th International Conference on
Ubiquitous and Future Networks (ICUFN), 2018

松村明, 大辞泉」(第2版), 小学館, 2012

島田 重夫, 特殊詐欺等対策優良迷惑電話防止機器(優良防犯電話), 日防設
ジャーナル 2018年爽秋号, 2015

松澤伸, 振込め詐欺を巡る諸問題, 早稲田大学社会安全政策研究所紀要 5, 2012

岩津圭介, 柏市振り込め詐欺等被害防止等条例, 自治体法務研究 46, 2016

○ 판례

United States v. Louis Daidone, 471F. 3d 371., 2006

United States v. Turkette, 452 U.S. 576., 1981