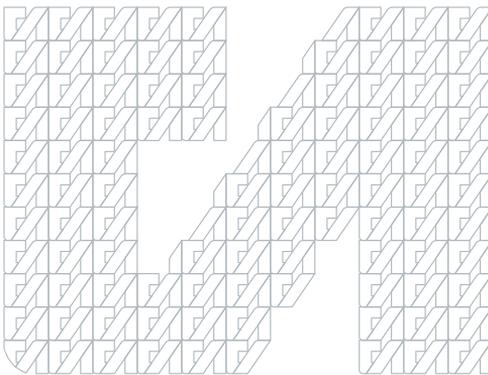


# 시민안전을 위한 전화금융사기 피해 예방에 관한 연구

A Study on Prevention of Voice Phishing Fraud  
for Urban Safety

이 형 복





**연구책임**

• 이형복 / 도시기반연구실 책임연구위원

**비상임연구원**

• 강용길 / 경찰대학교 치안정책연구소 연구관

정책연구 2017-46

## 시민안전을 위한 전화금융사기 피해 예방에 관한 연구

**발행인** 박재묵

**발행일** 2017년 11월

**발행처** 대전세종연구원

34863 대전광역시 중구 중앙로 85(선화동 287-2)

**전화** 042-530-3500 팩스: 042-530-3528

**홈페이지** <http://www.dsi.re.kr>

**인쇄** 대전문화사 TEL 042-252-7208 FAX 042-255-7209

이 보고서의 내용은 연구책임자의 견해로서 대전광역시와 세종특별자치시의 정책적 입장과는 다를 수 있습니다.

출처를 밝히는 한 자유로이 인용할 수 있으나 무단 전재나 복제는 금합니다.



# 차례 | Contents

제 1 장 서론	3
제1절 연구의 배경 및 목적	3
1. 연구의 배경	3
2. 연구의 목적	5
제2절 연구의 범위와 방법	6
1. 연구의 범위	6
2. 연구의 방법	6
제3절 연구결과의 기대효과	8
제 2 장 이론적 고찰	11
제1절 보이스피싱의 개념	11
1. 법률적 정의	11
2. 용어의 정의	13
제2절 보이스피싱 유형 및 특징	15
1. 보이스피싱의 유형	15
2. 보이스피싱의 특징	17
제3절 보이스피싱 범죄 유형별 법률 적용	19
제 3 장 보이스피싱 현황 및 특징	23
제1절 보이스피싱 범죄 관련 현황	23
1. 최근 10년간의 범죄 발생 추이	23
2. 보이스피싱 유형별 피해 추세	31
3. 보이스피싱 피해자 현황	32
4. 지역별 보이스피싱 발생 현황	33
5. 전화금융사기 국제공조수사 현황	35

<b>제2절 최근 보이스피싱 범죄 관련 특징</b>	<b>36</b>
1. 보이스피싱 유형별 피해 특징	36
2. 최근 대포통장 발생 주요 특징	38
3. 2017년도 보이스피싱 범죄 특징	41
<b>제3절 대전광역시 보이스피싱 발생 현황</b>	<b>43</b>
1. 대전광역시 보이스피싱 발생·피해 및 검거 현황	43
2. 대전광역시 보이스피싱 유형별 피해 추세	45
3. 보이스피싱 피해자 현황	46
<b>제 4 장 보이스피싱 예방 및 대응 동향</b>	<b>49</b>
<b>제1절 보이스피싱 주요 수법과 대응방안</b>	<b>49</b>
1. 보이스피싱 범죄 진행과정	49
2. 보이스피싱 주요 수법	54
3. 금융사기 피해자 분석	61
<b>제2절 보이스피싱 피해방지 주요 대책</b>	<b>68</b>
1. 연도별 주요 대책	68
2. 5대 금융약 추방 대책 중 보이스피싱 분야 대책	74
<b>제3절 해외 주요국의 사례</b>	<b>76</b>
1. 주요국 보이스피싱 현황	76
2. 해외 보이스피싱의 특징 및 시사점	78
<b>제4절 국내·외 지자체 대응 동향</b>	<b>82</b>
1. 일본 지자체의 보이스피싱 예방노력	82
2. 국내 지자체 협력 사례	85
<b>제 5 장 대전시 보이스피싱 예방 방안</b>	<b>89</b>
<b>제1절 기본 방향</b>	<b>89</b>
1. 보이스피싱 예방의 중요성	89
2. 지자체 역할의 중요성 인식	90
3. 보이스피싱 예방을 위한 지자체의 대책 방향	91
<b>제2절 보이스피싱 예방 대책 수립</b>	<b>93</b>

1. 문제점 및 대응 방향 .....	93
2. 추진 목표 및 중점과제 도출 .....	94
3. 중점과제 및 분야별 추진 방안 .....	95
<b>제3절 단계별 실행 방안 .....</b>	<b>96</b>
1. 기반구축 단계 .....	96
2. 역량강화 단계.....	98
3. 피해예방 및 대응 단계 .....	99
<b>제 6 장 결론 및 정책제언 .....</b>	<b>107</b>
제1절 결 론.....	107
제2절 정책제언 .....	109
참고문헌 .....	111
<b>부 록 .....</b>	<b>113</b>
부록 1. 일본 지자체의 「보이스피싱 피해방지 조례」.....	113
부록 2. 보이스피싱 교육자료 .....	120
부록 3. 보이스피싱 교육 만족도 조사.....	121
부록 4. 회의록 .....	124

# 표 차례 | Contents

[표 2-1] 전기통신금융사기의 정의	12
[표 2-2] 전기통신금융사기에 대한 대응	13
[표 2-3] 보이스피싱 범죄 유형별 법률 적용	19
[표 3-1] 최근 10년간(2007~2016) 보이스피싱 발생 및 검거현황	30
[표 3-2] 보이스피싱 유형별 피해 추세	31
[표 3-3] 2016년 보이스피싱 피해자 현황	32
[표 3-4] 최근 10년간(2007~2016) 보이스피싱 발생 및 검거현황	34
[표 3-5] 2016년도 전화금융사기 관련 국제공조수사 현황	35
[표 3-6] 보이스피싱 피해 현황	36
[표 3-7] 2016년 정부기관 사칭형 성별·연령별 피해 현황	37
[표 3-8] 2016년 대출빙자형 성별·연령별 피해 현황	38
[표 3-9] 대포통장 발생현황	38
[표 3-10] 신규 계좌 개설 후 기간별 대포통장 이용현황	39
[표 3-11] 2017 상반기 보이스피싱 유형별 피해자의 성별·연령 분포	42
[표 3-12] 최근 8년간(2009~2016) 보이스피싱 발생 및 검거현황	44
[표 3-13] 대전광역시 보이스피싱 유형별 피해 추세	46
[표 3-14] 대전광역시 보이스피싱 피해자 현황(2016)	46
[표 4-1] 보이스피싱 범죄 스크립트	50
[표 4-2] 전자금융사기 유형 및 특징 (2014년)	54
[표 4-3] 대표적인 대출사기 수법(2015년)	55
[표 4-4] 대검찰청 홈페이지를 활용한 신종 보이스피싱(2016년)	56
[표 4-5] 악성코드 유포 사례	57
[표 4-6] 금감원 피해 접수 및 소비자 경보 발생 사례	60
[표 4-7] 금융소비자 당부사항(금융감독원)	60
[표 4-8] 금융사기 발생 현황(2015)	61
[표 4-9] 금융사기 유형별 성별·연령대별 피해현황	62

[표 4-10] 피싱사기 성별 피해 분석 .....	64
[표 4-11] 대출사기 성별 피해 분석 .....	64
[표 4-12] 시간대별 피해 현황 .....	65
[표 4-13] 요일별 피해 현황 .....	66
[표 4-14] 지역별 피해 현황 .....	67
[표 4-15] 일본의 보이스피싱 발생 추이 .....	76
[표 4-16] 중국의 보이스피싱 발생 추이 .....	77
[표 4-17] 일본의 보이스피싱 발생 추이 .....	77
[표 4-18] 쿠마모토현의 보이스피싱 피해방지 조례 .....	84
[표 4-19] 카시와시의 보이스피싱 예방 주요 활동 .....	84
[표 4-20] 강릉시-금감원 업무협약 주요 내용 .....	85
[표 4-21] 강릉시-금감원 업무협약 주요 내용 .....	86
[표 5-1] 지방자치단체 및 사회·시민단체의 역할 강화방안 .....	92
[표 5-2] 대전시 보이스피싱 예방 및 대응 방향 .....	93
[표 5-3] 대전시 보이스피싱 예방 대책 .....	95
[표 5-4] 대전시 보이스피싱 표준모델 구상(안) .....	103

# 그림 차례 | Contents

[그림 1-1] 최근 10년간 보이스피싱 발생·피해 및 검거 현황 .....	3
[그림 1-2] 연구의 진행 흐름도 .....	7
[그림 2-1] 보이스피싱의 종류 .....	14
[그림 3-1] 보이스피싱 피해방지를 위한 단계별 대응방안-2012 .....	26
[그림 3-2] 2013년도 피싱·파밍 범죄발생 추이 .....	27
[그림 3-3] 전화번호 신속이용정지 절차 개요 .....	28
[그림 3-4] 아르바이트 구직자가 대포통장 명의인이 되는 사례 .....	40
[그림 3-5] 보이스피싱 피해자가 대포통장 명의인이 되는 사례 .....	41
[그림 4-1] 텔레뱅킹을 이용한 보이스피싱 흐름(2012년) .....	54
[그림 4-2] 은행을 사칭한 피싱사이트 사례(2012년) .....	55
[그림 4-3] 첨단 보이스피싱 수법 .....	59
[그림 4-4] 중점추진대책(2017) 목표 및 전략 .....	74
[그림 4-5] 일본 쿠마모토현의 보이스피싱 조례 개요 .....	83
[그림 4-6] 국내지자체 협력 사례(업무협약서) .....	86
[그림 5-1] 불법금융 추방 범 금융권 협의체 .....	91
[그림 5-2] 추진목표 및 중점과제 .....	94

# 서론

1. 연구의 배경 및 목적
2. 연구의 범위 및 방법
3. 연구결과의 기대효과

## 1장

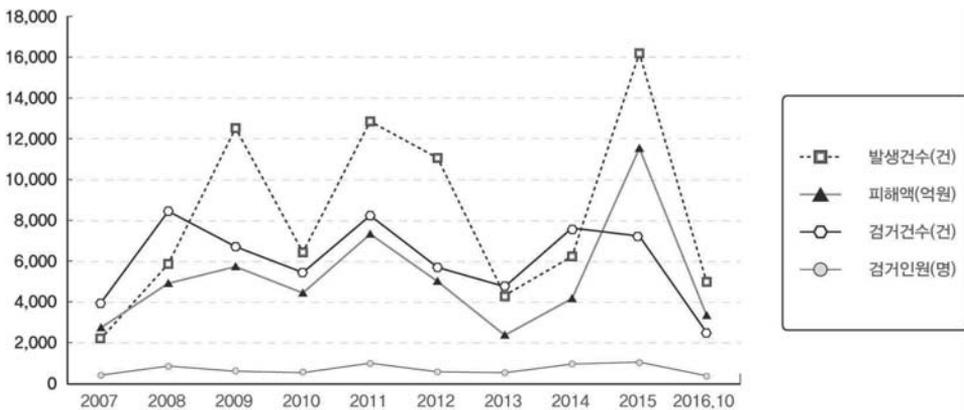


# 제 1 장 서 론

## 제1절 연구의 배경 및 목적

### 1. 연구의 배경

세계경제의 불황과 한국경제의 성장 둔화 속에 부의 양극화가 지속화 되면서, 사회경제 각 분야에서 불법적 범죄수익을 노린 다양한 형태의 지능형 범죄가 늘어나고 있다. 일명 보이스피싱(Voice Phishing)은 전화를 이용하여 개인정보를 불법적으로 알아내고, 예금을 인출해가는 사기수법으로써 국내에서는 2006년 5월에 처음 발생<sup>1)</sup>한 이후 많은 피해사례들이 속출하며 사회문제로 부각되고 있다. 매일같이 수법이 교묘해지고 지능화되고 있는 심각한 민생침해 범죄로 그 피해도 더욱 심각해지고 있다. 2007년부터 2016년 10월까지 10년간 보이스피싱 발생현황을 보면 총 발생 건수는 6만 715건에 피해액은 7,295억 원에 이른 것으로 나타났다(2017 치안전망, 치안정책연구소).



[그림 1-1] 최근 10년간 보이스피싱 발생·피해 및 검거 현황

1) 이진권, 전화금융사기 범죄에 대한 고찰, 한국경찰연구, 제6권, 제2호, 2007

전화금융사기는 금융, 통신 등 사회적 인프라가 잘 갖추어져야 가능한 선진국형 범죄라고 할 수 있다. ICT강국인 우리나라는 정보화 사회가 빠르게 진척되면서 사회적 부작용인 전화금융사기도 급증하였다. 스마트폰의 빠른 보급과 인터넷을 통한 은행업무의 발전은 한층 전화금융사기를 가속화시켰다. 또한 전화금융사기 피해는 그동안 사회적으로 부유한 계층보다 상대적으로 정보에 취약한 가정주부, 노인 등 서민층에 피해가 집중되었다. 그러나 최근, 인터넷뱅킹 등에 능숙하지만 사회경험이 적은 젊은 층에서도 피해가 급증하고 있어 심각한 사회문제가 되고 있다. 더욱이 종전에는 고령층이 피해가 컸으나, 최근에는 30·40대의 금융대출사기 피해가 늘고 있어 전화금융사기 피해는 보다 빠르게 신·변종 수법으로 진화하고 있다고 볼 수 있다.

2016년 기존 5대 금융악 특별대책을 「5대 금융악 및 3유·3불 추방 특별대책」으로 확대 개편(2016년 4월)하고 총력 대응한 결과, 금융사기 피해 감소 등 가시적 성과는 물론 금융 불안 해소 등으로 사회 전반의 공감을 얻고 있다.

그러나 아직도 다양하고 교묘한 불법·부당 금융행위가 성행하고 그에 따른 국민 피해도 여전하다. 소위 대포통장, 대포폰 등의 규제문제가 법적으로 해결되지 않고 있으며 범죄수법은 날로 다양화·고도화됨에 따라 이에 대한 대처요구도 강해지고 있다. 또한, 보이스피싱, 불법사금융, 유사수신의 경우 특히 노인, 서민, 사회초년생 등 취약계층에 깊숙이 침투해 사회 불안을 야기하고 있어 감독당국 및 금융권의 확고한 불법금융 근절 의지 천명과 지속적인 홍보 노력 없이는 대국민 피해예방이 어렵다는데 공감대 형성하고 있다.

전화금융사기는 서민들에게 물질적, 정신적 피해를 야기하는 범죄인만큼 대시민 홍보 및 교육, 관련기관 간 협업방안 등 이에 대한 집중적인 시책과 제도마련이 필요한 상황이다.

## 2. 연구의 목적

본 연구에서는 대전광역시(이하 대전시) 시민의 전화금융사기 피해로부터 보다 안전하게 예방하기 위해 교육 및 홍보, 관련 제도 마련을 위한 정책 방향을 모색을 목적으로 한다. 구체적으로 전화금융사기 피해로부터 대전 시민의 안전을 확보하기 위해 예방대책을 위한 기본구상 및 중점과제 제언을 목적으로 한다.

우선 경찰청과 금융감독원 데이터를 통해서 전화금융사기 피해현황과 현재까지 전국적으로 추진되었던 피해방지 주요대책을 살펴본다. 그리고 중앙정부의 피해방지 주요대책을 기반으로 하여 예방방안으로서는 기반구축, 역량강화, 피해예방의 3부분으로 나누어 조속히 실천 가능한 중점과제를 제안한다. 세부적인 연구의 목적은 다음과 같다.

### 첫째, 전화금융사기 피해 관련 법·제도 및 전국 및 대전시 피해현황 파악

『전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법』의 내용 파악 및 대전시 전화금융사기 피해현황을 전국적인 타시도와 비교분석하며, 범죄 유형별 현황을 파악한다.

### 둘째, 전화금융사기 범죄 동향 및 특징 파악

전화금융사기의 구체적인 특징파악을 위해 보이스피싱 주요수법을 진행 과정으로 살펴보고, 금융사기 피해자 분석을 통해 피해대상에 대해 알아본다. 지금까지 추진되었던 중앙정부의 보이스피싱 피해방지 주요대책을 주요 연도별로 살펴본다. 또한 대안마련을 위해 보이스피싱 예방 및 대응 동향을 국내·외적으로 살펴보고 시사점을 알아본다.

### 셋째, 전화금융사기 피해로부터 시민의 안전을 확보하기 위한 예방대책 기본방향 검토

피해현황 분석의 결과를 토대로 시민안전을 위한 전화금융사기 피해 예방방안을 위한 기본방향 설정과 그에 따른 중점과제를 제시하고, 목표달성을 위한 단계별 실행방안을 구체적으로 제시한다.

## 제2절 연구의 범위와 방법

### 1. 연구의 범위

본 연구의 범위를 시간적 측면에서 살펴보면, 연구범위는 대전시 전화금융사기 피해예방을 위한 정책의 기본방향과 세부전략을 마련하고자 과거 10년간의 전화금융사기 피해 현황 및 자료를 분석하였다. 공간적 측면에서는 대전시를 대상으로 하였지만, 우리나라에서 발생한 전화금융사기 피해현황, 관련 선행연구 및 법·제도를 전반적으로 검토하고, 선진도시의 자료 및 정보를 얻기 위해 일부 전화금융사기 피해예방 정책을 효과적으로 추진하고 있는 국외 선진사례의 내용을 검토하였다.

구체적으로는 첫째, 전화금융사기 피해에 대한 이론적 고찰로서 선행된 연구를 검토 및 분석하고 국내·외 전화금융사기 피해와 관련된 법규를 검토한다. 둘째, 이론적 고찰과 함께 경찰청과 금융감독원의 데이터를 기반으로 전화금융사기 피해의 현황 및 문제점을 분석하여, 전화금융사기 피해예방을 위한 기본방향을 설정하고 추진전략을 제시한다.

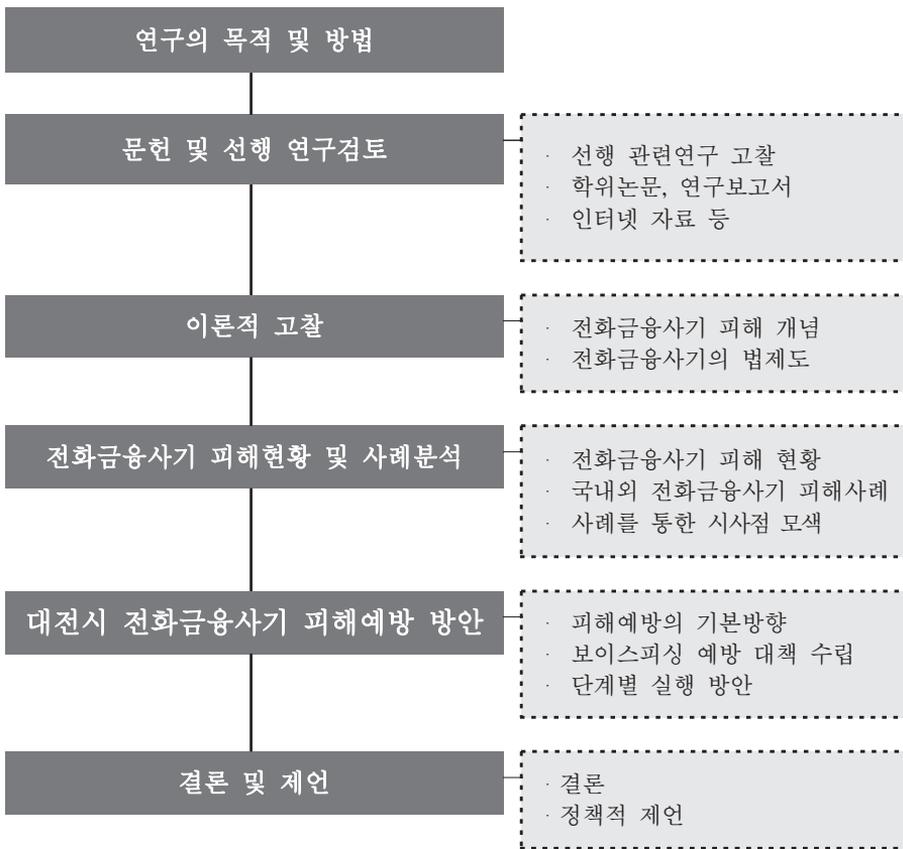
### 2. 연구의 방법

본 연구의 방법은 자료수집 및 전문가 인터뷰(경찰, 교수, 금융전문가, 교육전문가 등)를 기초로 하여 이루어지며, 구체적인 방법은 다음과 같다.

첫째, 자료수집은 보이스피싱 개념 및 용어정의 등의 고찰을 위한 문헌조사 및 선행연구 고찰, 국내·외 보이스피싱 사례조사, 전화금융사기 관련 법규검토, 피해유형에 따른 현황을 살펴보기 위하여 경찰대학 치안정책연구소와 대전지방경찰에 요청하여 관련 현황을 수집 및 분석하였다. 또한, 보이스피싱 예방교육에 있어서는 관련 전문가 및 교육전문가의 콜로키움·

자문 등을 실시하였다.

연구를 체계적으로 수행하기 위해 아래의 [그림 1-2]와 같은 연구 절차에 의하여 진행하였다. 전화금융사기의 개념 정립과 국내·외 관련 법규 검토, 전화금융사기 피해 현황 및 문제점 분석을 분석하고, 전화금융사기 피해 예방을 위한 정책 기본방안 및 구체적인 시책 제시를 통해 정책적 제언을 구하고자 한다.



[그림 1-2] 연구의 진행 흐름도

### 제3절 연구결과의 기대효과

본 연구의 연구결과 활용 및 기대효과는 다음과 같다.

첫째, 전화금융사기와 관련된 문헌연구와 국내·외 사례검토를 통하여 최근에 발생하고 있는 사례의 특징을 알아본다. 앞으로 대전시에서 새로운 금융사기 피해 예방 정책을 마련 시 국내의 시사점을 활용할 수 있다.

둘째, 실증적인 정책방향 설정을 위해서 관련 전문가(경찰, 경찰학 교수, 금융관련 종사자, 전화금융사기 예방교육자 등)의 다양한 의견을 수렴 및 정리하여서 전화금융사기 관련 현장성 있는 내용들을 활용할 수 있다.

셋째, 본 보고서를 전화금융사기 피해예방을 위한 교육 및 홍보 자료를 작성 시 기초적 자료로 활용할 수 있다. 이를 통해 시민안전을 위한 전화금융사기 피해 예방에 기여할 수 있을 것으로 기대해 본다.

끝으로 전화금융사기 피해 예방을 위한 조례를 제정시 대전시가 참조할 수 있는 기초적 자료로서의 역할을 할 수 있을 것으로 기대한다.



## 이론적 고찰

1. 보이스피싱의 개념
2. 보이스피싱 유형 및 특징
3. 보이스피싱 범죄 유형별 법률 적용

## 2장



## 제 2 장 이론적 고찰

### 제1절 보이스피싱의 개념

#### 1. 법률적 정의

##### 1) 전기통신금융사기와 보이스피싱

전화금융사기의 대표격인 보이스피싱은 불법적으로 개인정보를 빼내서 사용하는 신종범죄이다. ‘보이스피싱(voice phishing)’은 음성의 ‘voice’와 개인 정보의 ‘private data’, 낚시의 ‘fishing’을 조합한 용어이다. 전화(휴대폰, 스마트폰) 및 컴퓨터 등 전기통신수단을 이용하여 개인정보를 빼내고 이를 다양한 사기에 이용하여 피해자로부터 자금을 송금(이체)받는 범죄수법이라고 할 수 있다. 이에 따라 보이스피싱 범죄는 그 수단으로서 전기통신을 이용하고 있기 때문에 법적으로 “전기통신금융사기”의 한 종류로 분류되고 있다.

국내법에서 전기통신금융사기에 대한 정의는 “전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법” 제2조에 규정되어 있으며, 이때 수단으로서의 전기통신의 정의는 “전기통신기본법”에서 다루고 있다.

“전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법”에서는 「전기통신기본법」 제2조제1호에 따른 전기통신을 이용하여 타인을 기망(欺罔)·공갈(恐喝)함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 각종 행위를 “전기통신금융사기”로 규정하고 있다. 이 조항은 전기통신을 이용하여 자금을 송금 받는 사기행위를 포괄적으로 규정하고 있으며 여기에는 대출의 제공·알선·중개를 가장한 행위 포함되고, 재화의 공급 또는 용역의 제공 등을 가장한 행위는 제외하고 있다.

## [표 2-1] 전기통신금융사기의 정의

### 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법

제2조 (정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “금융회사”란~(중략)
2. “전기통신금융사기”란 「전기통신기본법」 제2조제1호에 따른 전기통신을 이용하여 타인을 기망(欺罔)·공갈(恐喝)함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 다음 각 목의 행위를 말한다. 다만, 재화의 공급 또는 용역의 제공 등을 가장한 행위는 제외하되, 대출의 제공·알선·중개를 가장한 행위는 포함한다.
  - 가. 자금을 송금·이체하도록 하는 행위
  - 나. 개인정보를 알아내어 자금을 송금·이체하는 행위
- 2의2. “전자금융거래”란 금융회사가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융회사의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.
3. “피해자”란 전기통신금융사기로 인하여 재산상의 피해를 입은 자를 말한다.
4. “사기이용계좌”란 피해자의 자금이 송금·이체된 계좌 및 해당 계좌로부터 자금의 이전에 이용된 계좌를 말한다.
5. “피해금”이란 전기통신금융사기로 인하여 피해자의 계좌에서 사기이용계좌로 송금·이체된 금전을 말한다.
6. “피해환급금”이란 피해금을 환급하기 위하여 제9조에 따라 소멸된 채권을 기초로 하여 제10조에 따라 산정되어 금융회사가 피해자에게 지급하는 금전을 말한다.
7. “이용자”란 금융회사와 체결한 계약에 따라 전자금융거래를 이용하는 자를 말한다.

## 2) 전기통신금융사기에 대한 대응

보이스피싱 등 전기통신금융사기의 피해가 커지고 사회적 문제로 대두됨에 따라 이에 대응하는 각종 조치를 취할 것을 법으로 규정하고 있다. ‘전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법’에서는 전기통신금융사기의 발생에 대비하고 그 피해를 최소화하기 위하여 전기통신금융사기 관련 정보의 수집 및 전파, 예보 및 경보 발령, 그 밖의 대응 조치를 취할 것을 규정하고 있으며, 피해 구제 및 예방업무와 관련하여 금융회사에 대한 유관업무 관리 감독을 금융위원회 또는 금융감독원이 실시할 수 있도록 법적 근거를 마련해 두고 있다.

## [표 2-2] 전기통신금융사기에 대한 대응

### 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법

제2조의2(전기통신금융사기에 대한 대응 등) ① 금융위원회는 전기통신금융사기의 발생에 대비하고 그 피해를 최소화하기 위하여 다음 각 호의 업무를 수행한다.

1. 전기통신금융사기에 관한 정보의 수집·전파
  2. 전기통신금융사기에 대한 예보·경보
  3. 그 밖에 대통령령으로 정하는 전기통신금융사기 대응조치
- ② 금융위원회는 전기통신금융사기의 발생을 방지하기 위하여 필요하다고 인정하는 경우에는 연도별 피해환급금 지급액 및 사기이용계좌 발생건수를 고려하여 금융위원회가 정하는 기준에 해당하는 금융회사나 그 임직원에게 대하여 다음 각 호의 사항을 권고·요구 또는 명령하거나 그 개선계획을 제출할 것을 명할 수 있다.
1. 금융회사 및 임직원에게 대한 주의·경고·견책(譴責) 또는 감봉
  2. 금융회사가 전자금융거래 업무를 수행함에 있어 안전성과 신뢰성을 확보하기 위한 전산인력, 전산시설 및 전자적 장치 등의 개선 또는 보완에 관한 사항
- ③ 금융위원회는 제1항 및 제2항에 따른 업무의 전부 또는 일부를 「금융위원회의 설치 등에 관한 법률」에 따라 설립된 금융감독원의 원장(이하 “금융감독원장”이라 한다)에게 위탁할 수 있다. [본조신설 2014.1.28.]

## 2. 용어의 정의

‘보이스피싱(voice phishing)’은 타인의 재산을 편취하는 사기범죄의 하나로써 전기통신수단을 이용한 비대면 거래를 통해 금융 분야에서 발생하는 일종의 특수 범죄이다. 보이스피싱은 ‘피싱사기’의 진화된 형태로 볼 수 있는데 ‘피싱사기’란 “기망행위로 타인의 재산을 편취하는 사기범죄의 하나로 전기통신수단을 이용한 비대면거래를 통해 금융분야에서 발생하는 일종의 특수사기범죄”로 정의할 수 있다. ‘보이스피싱’이라는 용어와 관련된 다양한 유사용어로서는 스미싱, 파밍, 피싱, 메모리 해킹, 대포통장 등이 있는데 주요 용어를 살펴보면 아래의 [그림 2-1]과 같다. 사기수법의 형태에 따라 분리되며, 직접적인 금융피해가 되기도 하고 타인의 금융피해의 수단으로 활용되기도 한다.

<b>스미싱</b> (Smishing)	<p>문자 메시지(SMS)와 피싱(Phishing)의 합성어. '무료 쿠폰 제공' '돌잔치 초대장' 등 문자 메시지에 포함된 인터넷 주소를 클릭하면 악성코드가 설치되어 피해자가 모르는 사이에 소액결제 피해가 발생하거나 개인·금융정보를 탈취하는 수법. 최근에는 쓰레기 방치 및 투기로 신고가 접수되었다는 스미싱이 유행하고 있다.</p>
<b>파밍</b> (Pharming)	<p>악성코드에 감염된 PC를 조작해 이용자가 정상적인 주소를 입력해도 위조 사이트로 유도된다. 감염된 컴퓨터 혹은 위조 사이트에서 인터넷뱅킹에 접속해 계좌 비밀번호 등을 입력하면 그 정보를 이용해 즉시 돈을 빼가는 수법이다.</p>
<b>피싱</b> (Phishing)	<p>개인정보(Pprivate data)와 낚시(Fishing)의 합성어로 개인정보를 낚는다는 의미. 금융기관 또는 공공기관을 가장해 전화나 이메일로 인터넷 사이트에서 보안카드 일련번호와 코드번호 일부 또는 전체를 입력하도록 요구해 금융 정보를 몰래 빼간다.</p>
<b>메모리 해킹</b>	<p>컴퓨터 메모리에 있는 이용자의 계좌번호, 보안카드 비밀번호를 탈취해 돈을 빼돌리는 새로운 해킹 방식이다. 정상적인 인터넷뱅킹 사이트에 접속해도 이체거래 과정에서 금융거래 정보 등을 실시간 위조·변조한다.</p>
<b>대포통장</b>	<p>통장을 개설한 뒤 돈을 받고 남에게 통째로 넘겨준 통장. 금융 사기범이 빼돌린 돈을 이체하는 데 이용한다. 통장을 타인에게 양도하거나 매매하는 행위는 금융실명제에 따른 전자금융거래법 위반으로 3년 이하의 징역 등에 처한다.</p>

[그림 2-1] 보이스피싱의 종류

자료: 송지혜, “기자도 당했다, 보이스피싱”, <사사인> 2014. 11. 18

## 제2절 보이스피싱 유형 및 특징

### 1. 보이스피싱의 유형

#### 1) 보호형 · 보상제공형 · 협박형 · 의무부과형

금융감독원은 보이스피싱 범죄를 피해자로부터 송금을 유인하는 형태에 따라 크게 네 가지 유형으로 분류하고 있다. ①보호형, ②보상제공형, ③협박형, ④의무부과형으로 분류한다. 보호형은 금융정보의 유출이나 범죄 연루 등으로부터 피해자를 보호해 주겠다고 유인하는 형태이다. 보상제공형은 초과 납부한 연금, 보험금, 세금 등을 환급 해준다거나 경품 등에 당첨되었다고 속여 피해자를 유인하는 형태이다. 협박형은 피해자의 가족을 납치하여 데리고 있다는 등의 방법으로 피해자를 속여 피해금을 편취하는 형태이다. 의무부과형은 동창회비의 납부, 대학의 추가합격 등에 따른 등록금 납부 등과 같은 방법으로 피해자를 유인하는 형태이다.<sup>2)</sup>

#### 2) 공공, 금융기관 사칭형 · 납치 가장형

국가정보원의 국제범죄정보센터에서는 보이스피싱을 크게 공공, 금융기관 사칭형과 납치 가장형으로 구분하고 있다.

공공, 금융기관 사칭형도 크게 두가지 형태로 세분될 수 있다. ①국세청, 국민연금관리공단, 우체국 등의 직원을 사칭하여 세금이나 보험금을 돌려준다며 현금지급기를 조작하도록 유인하여 현금을 사취하는 유형, ②법원 · 검찰 · 경찰직원 등으로 가장하여 피해자 명의의 계좌가 범죄에 연루되었다며 예금보호를 위해 현금인출기에서 일정한 숫자를 누르도록 유도하여 최종적으로는 계좌이체를 통해 현금을 사취하는 유형을 말한다.

납치 가장형은 ‘가족을 납치했으니 몸값을 입금하라’ 는 등의 위급한

2) 오영근 · 정정원(2012), 보이스피싱 근절을 위한 입법적 대응방안 연구, 법무부 연구용역

상황을 내세워 피해자를 심리적으로 불안한 상태로 만들어 협박하는 유형을 말한다. 특히 부모와 연락이 쉽게 닿지 않는 여행객이나 유학생 자녀를 납치했다고 위협하면서 신변의 안전을 위해서는 거액을 요구한다.

### 3) 안전계좌 송금형 · 특정명령 입력형 · 납치 빙자형

보이스피싱 범죄를 안전계좌 송금형 · 특정명령 입력형 · 납치 빙자형으로 분류하기도 한다. 이 유형은 세금 및 의료보험료 등을 환급하여 주겠다고 현금인출기 앞으로 유인하고 보안코드 변경 등으로 보안 조치를 해주겠다고 속여 특정한 명령을 입력하게 하는 특정명령 유도형, 피해자의 명의가 도용되었다는 등의 명목으로 현금인출기 앞으로 유인하고 피해금을 안전계좌로 이체하도록 유인하는 안전계좌 유도형, 피해자의 가족 등이 납치되었다는 등 해악을 고지하고 피해금을 갈취하는 납치빙자형으로 분류하고 있다(허성욱 · 정세종, 2008).

### 4) 보호기망형 · 협박형

보이스피싱 범죄의 수법에 따라 보호기망형과 협박형으로 분류할 수 있다. 우선 보호기망형은 예금의 안전한 보호나 세금환급 등으로 기망하는 유형이다. 협박형은 자녀의 납치나 가족의 채무 등을 이유로 송금을 요구하는 유형을 말한다. 그 세부적인 기망수법에 따라 공공기관인 국세청 및 국민연금관리공단 등을 사칭하여 현금지급기로 세금을 환급하겠다고 유혹하는 환급유형, 금융기관인 카드사, 은행, 채권추심단 등을 사칭하여 카드요금 연체 또는 명의가 도용되었다며 피해자의 계좌번호나 카드번호의 입력을 요구하는 카드연체 및 카드도용의 유형, 검찰, 경찰 등의 수사기관 등을 사칭하여 당사자가 범죄에 연루되었다며 개인정보를 요구하는 범죄연루유형, 지인 등을 사칭하여 자녀의 납치 및 사고를 당하였다고 거짓정보를 흘린 후, 사고처리나 수습의 대가로 부모에게 돈을 요구하는 거짓납치 및 사고유형으로 유형화될 수 있다고 한다(홍승희, 2009).

## 2. 보이스피싱의 특징

금융감독원, 경찰청, 한국인터넷진흥원에서 공동으로 운영하는 보이스피싱 지킴이 홈페이지<sup>3)</sup>에 따르면 ‘보이스피싱’ 범죄수법은 다음과 같은 몇 가지 특징을 보이고 있다.

첫째, ‘보이스피싱’의 수법이 전화나 통신을 통한 비대면 접촉방식을 활용한다는 점이다. ‘보이스피싱’을 시도하는 범죄자가 피해자에게 일방적으로 접촉을 시도함으로써 피해자의 인적 정보 및 관련 내용에 대한 주요 정보들도 범죄자에 의해 일방적으로 제공된다는 점에서 사실상 범죄자에 대한 정보를 최소화한다는 점이다.

둘째, 가장 일반적으로 많이 사용된 수법은 기관을 사칭하는 것이다. 범죄자는 일반인들에게는 정보가 부족하고, 쉽게 접근하기 어려운 금융감독원, 검찰, 경찰 등 금융기관 및 공공기관을 번갈아 사칭하여 정보의 신뢰성을 최대화하고자 한다. 특히 최근에는 사칭하는 기관의 가짜 전화번호, 홈페이지 등을 제작하여 피해자들에게 확인하도록 유도하거나, 발신번호를 조작하는 등 기술적으로 진화하고 있는 추세이다. 이는 ‘보이스피싱’ 수법이 점차 조직화, 기술화, 체계화되고 있음을 의미한다.

셋째, 피해자의 개인정보노출, 범죄사건 연루, 가족의 안전(교통사고, 병원입원 등) 등 피해자 또는 가족과 직접 관계되며, 급박한 위협에 관한 거짓정보를 제공함으로써 합리적이고 이성적으로 사안을 판단할 수 있는 여지를 최소화함과 동시에 심리적으로 피해자를 압박하는 수법을 활용한다.

넷째, 범죄증거를 남기지 않기 위해 피해자의 금융거래정보인 계좌 및 카드번호와 비밀번호, 인터넷 뱅킹 정보, 텔레뱅킹 정보 등을 제공받아 범죄자가 직접 인출하는 수법이 증가하고 있다. 기존 피해자에 의한 이체 등의 방식에서 ‘고객보호를 위한 상시모니터링 활동의 강화’, ‘피해사실 통보에 따른 지급정지’, ‘이체 후 일정시간 경과 후의 인출시스템 보완’ 등

3) <http://phishing-keeper.fss.or.kr/fss/vstop/main.jsp>

보이스피싱 예방대책이 강화되면서 직접 인출방식으로 수법을 전환한 것으로 보인다.

다섯째, ‘보이스피싱’ 범죄에 활용되는 전화, 이체 통장 등은 노숙자 또는 대학생, 취업준비생, 구직자 등 대출이나 취업을 희망하는 사람들에게 금전을 제공하고 취득한 일명 ‘대포통장’, ‘대포전화’로 수사나 추적을 따돌리는 방법을 사용하는 것이 특징이다.

위와 같이 ‘보이스피싱’은 예방대책이 계속 보완되고 있음에도 불구하고 그 기술과 수법이 진화되고 있으며, 초기의 개별적이고 적은 피해수준에 비해 최근에는 조직적이고 피해자의 수와 금액도 기하급수적으로 증가하고 있는 점을 고려하면, 더 이상 개인적 범죄가 아닌 사회적 범죄로 인식되어야 할 것이다. 이러한 차원에서 이제는 개별적 피해예방의 단계에서 사회적 피해예방으로 제도적이고 정책적인 대응이 요구된다.

## 제3절 보이스피싱 범죄 유형별 법률 적용

[표 2-3] 보이스피싱 범죄 유형별 법률 적용

범죄 유형	적용 여부	법률 적용
사기죄	●	<ul style="list-style-type: none"> <li>사기죄가 성립하기 위해서는 피기망자가 착오에 빠진 상태에서 그의 의사에 의하여 처분행위를 하여야 함</li> <li>처분의사는 피해자의 자신의 재산의 이전에 대한 인식과 의사라고 볼 것이므로 보이스피싱의 경우 피해자가 최소한 자신의 예금계좌에서 다른 계좌로 예금이 이전한다는 사실에 대한 인식을 가지고 예금을 보호할 의사로 계좌이체의 행위를 한 것이므로 피해자의 처분의사를 인정할 수 있음</li> </ul>
공갈죄	●	<ul style="list-style-type: none"> <li>실제 피해자의 가족을 납치하지 않았음에도 불구하고 허위로 납치하였다고 피해자를 공갈하는 것과 같은 경우에는 가족 납치라는 허위의 사실이 피해자에게 공포심을 유발시켜 재물의 교부나 재산상의 이익을 취하였다면 공갈죄가 성립될 수 있음</li> </ul>
컴퓨터 등 사용 사기죄	●	<ul style="list-style-type: none"> <li>피해자 스스로 착오 또는 공포심으로 인하여 자신의 금융정보를 직접 입력한 후 계좌이체행위를 하는 경우에는 범죄자에게 책임을 묻기에 한계가 있으나 타인의 대포통장의 현금카드를 이용하여 현금자동인출기에서 출금하는 행위는 권한없이 정보를 입력하는 행위로 컴퓨터 등 사용 사기죄가 성립됨</li> <li>각종 개인정보 및 금융정보를 취득한 후 이를 이용하여 피해자의 금융계좌에 접속하여 피해자의 명의로 대출을 받은 뒤 피해자 예금계좌에 입금된 금원을 다른 계좌로 이체하는 유형의 카드로 보이스피싱 등의 경우에 권한 없는 정보의 입력행위로 컴퓨터 등 사용 사기죄가 성립됨</li> </ul>
경범죄처벌법상 관명사칭	▲	<ul style="list-style-type: none"> <li>검찰공무원이나 경찰공무원을 사칭하여 예금계좌를 보호해주겠다고 하는 것과 같은 행위는 사칭한 공무원의 직권에 해당하지 않는 행위이기 때문에 성립이 어렵다는 것이 일반적인 견해임</li> <li>다만, 직권을 행사하지 않고 공무원의 자격을 사칭한 경우에는 경범죄 처벌법 제3조 제1항 제7호(관명사칭 등)를 위반한 것임</li> </ul>

범죄 유형	적용 여부	법률 적용
전자금융 거래법 위반	●	<ul style="list-style-type: none"> <li>타인의 명의로 개설되어진 차명계좌의 예금통장, 현금카드 등을 사용하는 경우 계좌의 양도인과 양수인 그리고 이를 알선하는 자는 모두 전자금융거래법 위반죄에 해당</li> </ul>
정보통신 망 이용촉진 및 정보보호 등에 관한 법률 위반	●	<ul style="list-style-type: none"> <li>보이스피싱범죄를 위하여 정보통신망을 통하여 속이는 행위로 타인의 계좌번호, 전화번호, 주소 등의 개인정보를 수집하는 행위는 동법상 금지되는 속이는 행위에 의한 개인정보의 수집금지 행위에 해당하게 되어 처벌받게 됨</li> </ul>
범죄수익 은닉의 규제 및 처벌 등에 관한 법률 위반	●	<ul style="list-style-type: none"> <li>차명계좌의 양도인, 양수인 및 해당 계좌의 양도·양수를 알선한 자의 경우 각각의 행위가 범죄수익은닉의 규제 및 처벌 등에 관한 법률에 위반됨</li> <li>범죄수익은닉의 규제 및 처벌 등에 관한 법률은 특정범죄와 관련된 범죄수익의 취득 등에 관한 사실을 가장하거나 특정범죄를 조장할 목적 또는 적법하게 취득한 재산으로 가장할 목적으로 범죄수익을 은닉하는 행위를 규제하고 있음</li> </ul>

자료 : 정정원(2013), ‘보이스피싱범죄의 형사법적 검토 및 대응방안’, 가천법학 제6권 제2호의 내용을 참고하여 재구성

## 보이스피싱 현황 및 특징

1. 보이스피싱 범죄 관련 현황
2. 최근 보이스피싱 범죄 관련 특징
3. 대전광역시 보이스피싱 발생 현황

# 3장



## 제 3 장 보이스피싱 현황 및 특징

### 제1절 보이스피싱 범죄 관련 현황

보이스피싱 범죄는 2000년대 초반 대만에서 시작되어 중국, 일본, 싱가포르 등 아시아 지역으로 넓게 확산되었다. 보이스피싱 범죄조직은 해외에 범죄단 본부 및 콜센터를 운영하고 국내에는 인출팀, 환전·송금팀, 계좌모집팀 등이 네트워크를 이루고 있다. 국내에서는 2006년부터 보이스피싱 범죄가 사회적 문제로 대두되기 시작하였다(금융감독원, 2012).

#### 1. 최근 10년간의 범죄 발생 추이

최근 10년간(2007년~2016년) 보이스피싱은 총 117,991건이 발생하였고, 총 피해액은 1조 923억 원에 이른다. 지난 10년 동안 발생건수가 급격히 증가하는 시점은 2008년과 2013년 등 두 번의 변곡점을 확인할 수 있다. 2007년에 비해 2배 이상의 증가를 보인 2008년부터 2012년까지 소폭의 증감을 반복하였으나, 2013년에 21,634건으로 급격하게 증가하기 시작하여 2014년을 정점으로 이후 소폭 감소하는 추세이다.

연도별 추세를 살펴보면 다음과 같다. 2007년도 보이스피싱 발생 건수는 총 3,981건이었고, 피해액은 434억 원이었다. 이 중 2,757건에 2,221명을 검거하여, 발생대비 검거비율은 69.3%이다. 초창기 보이스피싱은 주로 검찰, 국세청, 금융감독원 등의 공공기관이나 은행을 사칭하는 수법이 대부분이었다. 주로 “국세청 직원이다. 세금을 환급해줄 테니 현금인출기로 가서 지시하는 대로 번호를 입력하라”거나 “당신 신상 정보가 유출돼 돈이 빠져 나갈 위험이 있다. 즉시 우리가 불러주는 안전한 계좌로 돈을 옮겨라”는 식이었다.

2008년에는 8,454건이 발생하여 총 피해액 877억 원으로 전년 대비 2배 이상 폭증하였다. 이 발생 건수 중 4,927건에 5,878명을 검거하여 검거비율은 58.3%로 전년 대비 11.0%가 감소하였다. 이후 2007년 하반기부터는 한 단계 진화된 수법이 등장하게 된다. 교묘하게 피해자의 금융 정보를 빼내던 방법에서 자식이나 가족을 납치했다는 방식으로 상대를 협박하는 수법을 사용하게 된다. 또한 사전에 대상자의 신상 정보 및 가족관계까지 파악하는 식의 ‘표적 범죄’가 늘었다. 당시 대선과 총선시기에 여론조사를 빙자해 “설문에 응하면 답례로 돈을 입금시켜줄 테니 계좌와 비밀번호를 알려 달라”는 방식 등으로 범죄를 실행하기도 하였다.

2009년도 발생건수는 6,720건이고 피해액은 621억으로 전년도에 비해 소폭 감소하였다. 검거건수는 5,742건에 1만 2,523명을 검거하여 검거율 85.4%로 매우 많이 증가하였다. 2009년은 검거실적에서 보여주듯 경찰의 지속적 단속과 함께 이루어진 휴대폰 국제전화 표시 서비스 시행,<sup>4)</sup> 피해 예방 광고홍보, 대포통장 개설방지 시스템구축 등 피해 예방노력으로 2009년에 감소세로 돌아섰다.

2010년에는 발생 건수가 5,455건으로 2008년의 발생건수의 65%에 해당되었으며, 피해액은 553억 원으로 역시 63% 수준으로 대폭 감소하였다. 그러나 이러한 대응 노력에도 불구하고 공공기관 사칭 및 카드로 사기수법, 인터넷 전화상의 발신번호 변작수법 등 진화된 사기 수법에 의한 보이스피싱은 여전히 계속되었다. 발신번호 변작수법의 경우 해외에서 인터넷폰으로 번호 조작해서 경찰청 민원 안내실 등 관공서 전화번호로 입력하여 경찰청에서 전화한 것처럼 기망하는 방식이다.

2011년도 보이스피싱의 발생건수는 8,244건으로 전년도 대비 51.1%가 증가하였으며 피해액도 1,019억 원으로 무려 84.3%가 증가하였으며, 한 건당 평균 피해금액도 1,236만원으로 증가하였다. 이처럼 피해가 크게 증가하게

---

4) 2009. 5. 1부터 국제전화를 최초 접수한 통신업체 식별번호(001,005 등)가 표시되고 있으며, 2009. 10. 1부터 국제전화가 올 경우 휴대전화 화면에 “국제전화입니다”라는 문구를 표시 중이다.

된 계기는 카드론 또는 공공기관을 사칭한 피싱사이트 등 신종수법의 등장이라 할 수 있다. 2011년 초에 처음으로 피해가 발생한 카드론 보이스피싱 범죄는 2011년 11월까지 1,999건, 약 202억 원에 이르는 것으로 나타났다. 이는 2011년 한해동안 발생한 보이스피싱 총 피해건수의 약 27.6%를 차지하였다.

보이스피싱 발생건수 및 피해금액이 급격히 증가함에 따라 2011년 8월 16일부터 서울지방경찰청에서는 112센터를 통해 보이스피싱 피해금 지급정지 신청제도를 시행하여 10월말까지 2개월 보름동안 약 7억원의 피해금액을 지급정지하는 성과를 거두었다. 그리고 11월 30일부터는 ‘경찰청 112 센터를 통한 보이스피싱 피해금 지급정지 신청제도’<sup>5)</sup> 실시지역을 전국으로 확대하였다. 이를 통해 사기범이 피해금액을 인출하는데 소요되는 시간은 약 5~15분인데 비해 기존 금융기관별로 지급정지신청을 할 경우 지급정지에 소요되는 시간이 약 7분이었으나, 이후 2~3분으로 단축하게 된 것이다.

한편, 2011년 9월 30일에 「전기통신금융사기피해금환급에관한특별법」을 제정하여 시행함으로써 피해지원에 관한 법률적 근거도 마련되었다.

2012년에는 보이스피싱 발생건수가 5,709건으로 전년대비 30.7%가 감소하였고, 피해액은 595억 원으로 41.6%가 감소하였다. 정부에서 2012년 1월에 경찰청, 금융감독원, 금융위원회, 방송통신위원회, 금융권 합동으로 관계기관 TF를 구성하고 ‘보이스피싱 피해방지를 위한 종합대책’을 마련하여 강력한 대응을 실시한 결과인 것으로 평가된다. 이 대책은 보이스피싱 범죄의 단계별 대응방안을 마련하여 체계적이고 유기적인 공조시스템을 구축하는데 중점을 두었다.

---

5) 보이스피싱 피해자의 신속한 피해금 지급정지를 위해, 피해자가 경찰청 112에 전화를 하면 경찰청과 금융회사간 구축된 핫라인을 통해 지급정지 신청이 가능토록 한 제도



**[그림 3-1] 보이스포싱 피해방지를 위한 단계별 대응방안-2012**

자료: 금융감독원(2012a), 금융소비자 보호를 위한 보이스포싱 피해방지 종합대책, 보도자료

2012년도는 위와 같이 정부차원에서의 적극적인 대응으로 보이스포싱 범죄가 대폭 감소하였으나 하반기에 접어들면서 텔레뱅킹(전화 금융거래)을 이용한 보이스포싱과 가짜홈페이지를 이용한 피싱사이트 범죄가 점차 증가하였다.

2013년의 보이스포싱 범죄 발생건수는 21,634건으로 전년 대비 약 3.8배가 증가하였고, 피해액도 1,429억 원으로 전년 대비 약 2.4배가 증가하였다. 이는 2013년도부터 대출사기도 보이스포싱의 한 유형으로 통합하여 통계를 관리하였기 때문이다. 2013년 이후에는 피싱사이트, 파밍 등 인터넷 기반의 신·변종 수법의 비중이 전체 범죄건수의 절반 이상을 차지하였다. 2013년 1분기 비중은 58.7%이고, 2분기에는 57.9%, 3분기 63.0%, 4분기에는 53.3%를 차지하였다. 또한, 금융회사, 검·경 등 주요 공공기관을 사칭한 피싱사기 비중이 큰 폭으로 상승하였다.



**[그림 3-2] 2013년도 피싱·파밍 범죄발생 추이**

자료: 금융감독원(2014), 피싱사기 피해 구제현황 및 소비자 유의사항, 보도자료

위와 같이 피싱사기가 증가함에 따라 2013년 9월 26일에 ‘전자금융사기 예방서비스’를 전면 시행하였으며, 이후에는 피싱사기 피해가 다소 감소한 반면, 스마트폰 बैं킹을 이용한 파밍 피해가 증가하였다. 주로 스마트폰을 통한 스미싱, SMS 탈취 등 새로운 사기수법이 증가하였다. 이에 따라 스마트폰을 이용한 금융사기 피해예방을 위해 2013년 11월에 SMS탈취 의심거래에 대한 ARS인증 지도와 2014년 1월에 스마트폰 बैं킹에 대해서도 전자금융사기예방서비스를 각각 시행하였다.

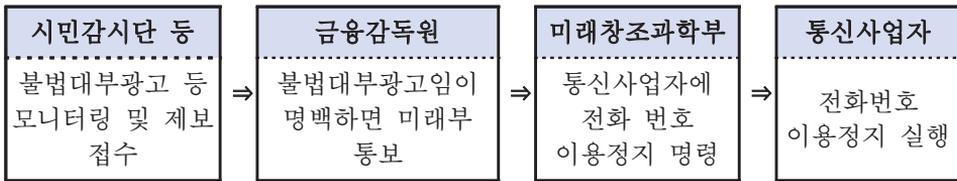
2014년도의 보이스피싱 발생건수는 22,205건으로 전년 대비 2.6%가 증가하였고, 피해액은 1,887억 원으로 전년 대비 32.1%가 증가하였다. 정부당국은 2012년부터 보이스피싱을 비롯한 금융사기에 대한 근절대책을 꾸준히 추진하였다. 2014년 5월에는 ‘대포통장 의심거래자에 대한 예금계좌 개설 절차 강화’ 방안을 시행하였다.

그럼에도 금융사기 피해는 줄어들지 않고 지속적으로 증가하는 추세를 보였다. 피싱사기의 피해액은 12년에 1,154 → 13년에는 1,365 → 14년도는 2,165억 원으로 증가하였고, 대출사기 피해상담 건수도 22,537 → 32,567 → 33,410로 증가하였으며, 피싱사기를 기준으로 하는 대포통장 건수도 33,496 → 38,437 → 44,705로 각각 증가하는 추세를 보였다.

또한 파밍과 같은 기술형 범죄수법에 대한 예방대책이 강화되면서 사기

수법이 진화된 보이스피싱의 비중이 12년도 66.2%에서 13년도 41.7%로 감소하였다가 14년에 46.8%로 증가하였다. 금융권의 예금계좌 개설 절차가 강화되면서 기존에 정상 발급된 예금통장이 불법매매 등을 통해 대포통장으로 유통·활용되는 사례도 증가하였다.<sup>6)</sup>

2014년 7월 29일 ‘전기통신금융사기 특별법’을 개정하여 대포통장 과다 발급 금융회사에 대한 개선계획 제출명령 및 제재 근거를 마련하였다. 그리고 ’ 14.12월 정부합동 ‘전기통신금융사기 방지대책’에서 대포통장 광고 및 금융사기에 이용된 전화번호를 신속하게 정지 조치할 수 있도록 관련법규인 ‘전자금융거래법 등’에 이용정지 근거를 마련하기로 하였다(금융감독원, 2015a).



**[그림 3-3] 전화번호 신속이용정지 절차 개요**

자료: 금융감독원(2015a), 보이스피싱 등 금융사기 척결 특별대책[「민생침해 5대 금융악 척결 특별대책」 세부 대책①], 보도자료

2015년의 보이스피싱 발생건수는 18,549건으로 전년 대비 소폭 감소하였으나 피해액은 2,040억원으로 소폭 증가하였다. 그러나 검거건수는 총 15,887건으로 전년 대비 2.8배가 증가하였고, 검거인원은 약 2.6배 증가하였다. 이는 경찰청이 2015년을 전화금융사기 척결의 원년으로 삼아 본청에 전화금융사기 대응 T/F 설치 및 각 지방경찰청 지능범죄수사대에 보이스피싱 전담 수사팀을 편성하여 적극 운영한 결과이다. 이를 바탕으로 서민들의 피해가 큰 전화금융사기·중소상공인 대상 사기·노인 대상 사기를 ‘3대 악성 사기’로 선정하여 연중 상시단속한 점도 검거건수를 늘리는데 기여한

6) 금융감독원(2015). “보이스피싱 등 금융사기 척결 특별대책”, 보도자료(4월 13일자)

것으로 나타났다. 2015년 9월부터 자연인출제도를 확대 시행하고, 2015년 10월부터 자연이체제도를 시행한 점도 보이스피싱 피해발생을 줄이는데 기여한 것으로 보인다(치안전망, 2016).

2016년에도 2015년에 이어 ‘3대 악성사기’ 인 전화금융사기에 대해 연중 상시단속(2015. 11~2016. 10)을 실시한 결과,<sup>7)</sup> 2016년에는 보이스피싱 범죄의 발생 건수가 17,040건으로 8.1%가 감소하였고 피해액은 1,468억 원으로 28%가 감소하였다. 경찰청과 금융감독원은 ‘2016년도 금융범죄 척결 중점 협력사항에 대한 업무협약’을 체결하여 ‘보이스피싱 112신고 및 현장예방·검거 체계’를 구축<sup>8)</sup>(2016. 3. 15)하여 현장 검거를 강화하는 등 적극적으로 대응하고자 노력하였다.

‘전기통신금융사기 피해방지 및 피해환급에 관한 특별법’ 및 ‘전자금융거래법’ 시행으로 보이스피싱에 사용되거나 대포통장의 양수 및 양도에 사용된 전화번호의 이용을 중지할 수 있는 제도를 도입하였다. 경찰청장, 검찰총장 또는 금융감독원장이 전화금융사기에 이용된 전화번호를 확인한 때에 미래창조과학부 장관에게 해당 전화번호에 대한 이용중지 요청을 할 수 있어 피해발생을 감소시킬 것으로 기대된다.

또한 피해신고 활성화 방안으로 금융기관에서 피해 접수 시, 보이스피싱 범죄에 이용된 전화번호를 신고하도록 하는 제도를 마련하였다. 그동안 송금내역 등 피해사실만 확인하였으나, 피해자가 수신한 보이스피싱 전화번호를 적극 신고토록 한 것이다. 그 외에도 금융감독원은 SK, KT 등 이동통신사와 협조하여 신고를 활성화하고 있다. ‘T전화’ 앱을 이용하여 보이스피싱 전화를 수신시 즉시 사기범 목소리와 전화번호를 금융감독원으로 신고할 수 있도록 협조체계를 구축하였다. KT 자회사이자 악성 전화번호 차단 서비스 전문회사인 ‘후후앤컴퍼니<sup>9)</sup>’ 와도 업무협약을 체결(2016. 11.

7) 경찰청은 ‘3대 악성사기범 근절’ 등 10개 과제에 대해 6개 분야로 그룹화하여 기획수사(2015. 11. 1~2016. 10. 31)를 하였으며, 전화금융사기, 대출사기, 중소기업인 노인 대상사기 등 3대 악성사기 외에 부정부패 비리단속, 보험사기, 유사수신다단계 사범, 3대 대포물건 등 10개 과제에 대한 기획수사를 진행하였다.

8) 시행 75일 간(3.15~6.30) 성과로 총 49억 원(217건)피해를 예방하고, 인출액 54명을 현장 검거. 정부 3.0 국민체감 성과점검회의(7.22)에서 협업 우수사례로 선정되었다.

18)하여 보이톡피싱을 시도하는 전화나 문자메시지를 원천적으로 차단하도록 한 것이다.

한편, 금융감독원은 국립과학수사연구원과 ‘전화금융사기 근절을 위한 업무협약’을 체결(2016. 5. 19)하고 전화 사기범의 실제 목소리를 과학적으로 분석하고 관리할 수 있도록 사기범의 목소리 DB를 구축하고 공개하였고, 수사기관에 참고자료로 제공하고 있다. 첨단 과학수사기법인 인공지능(AI) 성문분석<sup>10)</sup>을 통하여 구축한 프로그램으로 ‘바로 이 목소리’라는 이름으로 공개하고 있다. 이는 보이톡피싱 지킴이 홈페이지를 통해 운영하고 있다.

**[표 3-1] 최근 10년간(2007~2016) 보이톡피싱 발생 및 검거현황**

구 분	발생건수(건)	피해액(억 원)	검거건수(건)	검거율
2007	3,981	434	2,757	69.3%
2008	8,454	877	4,927	58.3%
2009	6,720	621	5,742	85.4%
2010	5,455	553	4,454	81.6%
2011	8,244	1,019	7,336	89.0%
2012	5,709	595	5,023	88.0%
2013	21,634	1,429	8,143	37.6%
2014	22,205	1,887	8,170	36.8%
2015	18,549	2,040	15,887	85.6%
2016	17,040	1,468	11,386	66.8%
계	117,991	10,923	73,825	62.6%

주 : 2013년부터 대출사기 통계 관리, 대출사기도 보이톡피싱의 한 유형으로 통계 합산  
 자료: 경찰청(2017) 내부자료 발췌하여 편집함

9) KT로부터 독립한 자회사로, 보이톡피싱 전화, 스팸 전화 등의 차단 기능을 제공하는 ‘후후’ 어플리케이션을 운영 중인 회사이다.

10) 다수 국민들에게 걸려온 사기범의 전화목소리를 인공지능(AI)을 활용한 기계학습(machine learning)으로 분석하여 음성 정보에 기록된 특징을 추출하여 비교 분석하는 방법이다.

## 2. 보이스피싱 유형별 피해 추세

범정부적인 보이스피싱 예방대책의 시행 및 홍보강화로 정부기관을 사칭하는 보이스피싱에 대한 대처능력이 강화되자, 보이스피싱 범죄는 급전이 필요한 서민들을 대상으로 대출사기를 행하는 수법으로 전환되고 있는 것으로 나타났다.

대출사기는 대출 진행을 위해서 보증료, 신용등급 상향비 등을 요구하고 이를 편취하는 전형적인 수법에서, 고금리 대출을 받으면 저금리 대출로 바꿔준다는 고금리 대출을 먼저 받게 하고 상환 명목으로 대출금을 편취하는 신종 수법으로 진화하고 있다. 사기 수법이 지능화되고 고도화되면서 1인당 피해금액도 높아지고 있다.

실제로 아래 표와 같이 기관사칭형 보이스피싱의 발생건수는 2015년도에 7,239건으로 전체 보이스피싱 범죄의 39%를 차지하였고, 대출사기형은 11,310건으로 61%였다. 2016년도에는 기관사칭형이 3,384건으로 전년 대비 절반 이상이 줄었으며 이는 전체 보이스피싱 범죄의 19.9%의 비중으로 전년 대비하여 발생건수 및 비율이 대폭 감소하였다. 이에 반해 대출사기형의 경우 2016년에 총 13,658건으로 소폭 상승하였으나, 비중은 전체의 80.2%로 대폭 상승하였다.

[표 3-2] 보이스피싱 유형별 피해 추세

구 분		2015상	2015하	2016상	2016하
발생 건수 (건)	기관사칭형	4,800	2,439	1,398	1,986
	대출사기형	6,621	4,689	6,522	7,134
	합계	11,421	7,128	7,920	9,120
피해 금액 (억원)	기관사칭형	688	382	226	318
	대출사기형	410	560	401	523
	합계	1,098	942	627	841

자료 : 경찰청(2017) 내부자료

### 3. 보이스피싱 피해자 현황

2016년 현재 보이스피싱 범죄의 피해자 성별 현황을 살펴보면, 보이스피싱의 유형 중 기관사칭형의 경우 여성의 피해가 남성에 비해 3배 이상인 것으로 확인되었다. 이는 남성보다 수사기관 등 공공기관의 절차에 대해 잘 알지 못하고 쉽게 당황하거나 타인의 말에 공감하는 경향 때문인 것으로 보인다. 반면, 대출사기형의 경우는 남성이 여성보다 많은 피해를 당하였다. 통상적으로 남성의 금융과 관련된 활동이 여성에 비해 많다는 점에서 대출사기에 많이 노출되어 있기 때문인 것으로 판단된다.

[표 3-3] 2016년 보이스피싱 피해자 현황

(단위 : 건, %)

기관사칭형									
발생 건수 (합계)	성별		연령별						
	남	여	20대	30대	40대	50대	60대	70대 이상	미상
	810	2,574	1,531	591	261	290	387	321	3
100%	23.9%	76.1%	45.2%	17.5%	7.7%	8.6%	11.4%	9.5%	0.1%
대출사기형									
	7,850	5,806	1,675	3,144	4,281	3,544	874	138	-
100%	57%	43%	12%	23%	31%	26%	6%	1%	-

자료: 경찰청(2017) 내부자료

피해자의 연령별 현황을 살펴보면, 기관사칭형의 경우 20대의 비율이 45.2%로 가장 많고, 다음은 30대가 17.5%를 차지하여, 20~30대 젊은 층에

피해가 집중되고 있다. 이는 사회경험이 많지 않고, 인터넷 및 모바일 뱅킹 등 사이버환경에 익숙하여 최근의 기술적 보이스피싱 수단에 쉽게 노출되어 있기 때문으로 추정된다. 그리고 60대와 70대 이상의 연령층에서도 각각 11.4%와 9.5%로 높은 비율을 보이고 있다. 이는 보이스피싱 관련 정보에 취약하고 온라인 뱅킹보다 창구거래에 익숙하며 공공기관에 대한 신뢰도가 높기 때문으로 판단된다. 한편 대출사기형의 경우에는 금융활동이 가장 활발한 30 ~ 50대의 연령층에서 피해가 많이 발생하였다. 이는 성별에서 남성의 피해가 높은 것과는 연관되며, 주로 가정의 가장으로서 각종 생활자금, 사업자금 등이 필요한 시점에서 쉬운 방법으로 대출을 받을 수 있다는 사기행위에 유혹될 가능성이 높기 때문이다.

#### 4. 지역별 보이스피싱 발생 현황

2012년부터 2016년까지 최근 5년간의 지역별 보이스피싱 발생 현황을 살펴보면, 대체로 지역경제 수준이 상대적으로 높고 금융과 교통·통신 인프라가 잘 갖추어진 수도권 및 대도시 지역에서 보이스피싱이 많이 발생하는 것을 알 수 있다.

지역별 발생 건수를 보면 서울이 최근 5년 동안 1만 133건으로 연평균 2,027건이 발생하여 전국 발생 건수의 36%를 차지하였다. 다음으로 경기도가 4,672건으로 연평균 934건이 발생하여 전국 발생 건수의 17%에 해당하였다. 부산은 1,975건으로 연평균 395건이 발생하였으며, 대구는 1,659건에 연평균 332건, 인천은 1,459건에 연평균 292건이 발생하였다. 서울과 수도권 지역에서 전국의 53%에 해당하는 보이스피싱 범죄가 발생하였고, 부산, 인천, 대전광역시 등 대도시 지역에서 집중적으로 발생하였다.

[표 3-4] 최근 10년간(2007~2016) 보이스피싱 발생 및 검거현황

(단위 : 건)

구분	2012	2013	2014	2015	2016
서울	1934	4392	7324	5675	5593
부산	571	2036	1296	993	848
인천	358	1191	1220	874	651
<b>대전</b>	<b>347</b>	<b>1732</b>	<b>1011</b>	<b>1316</b>	<b>1138</b>
대구	52	255	387	322	194
울산	260	591	358	520	514
광주	193	663	908	490	502
경기	521	5793	5829	4212	3279
충북	84	468	539	626	448
충남	196	900	532	507	498
강원	330	694	436	766	744
전북	76	568	576	492	567
전남	145	347	493	376	370
경북	280	667	527	611	1085
경남	262	1096	568	433	307
제주	100	241	201	336	302

자료: 경찰청(2017) 내부자료



## 5. 전화금융사기 국제공조수사 현황

2016년 현재 경찰청은 2016년 11월 22일부터 이틀간 국제공조 강화의 일환으로 ‘제2차 한·일·중 경찰협력회의’를 인천 송도에서 개최하여, 국제범죄 공동대응과 동북아 역내 안전 확보를 위한 치안협력 방안을 논의하였다. 특히 해외도피사범 송환을 비롯, 보이스피싱·사이버·마약 등 국제성범죄 정보공유와 합동대응 방안이 집중 논의되었다.<sup>11)</sup>

2016년 한 해 동안 전화금융사기 범죄와 관련하여 국제공조수사를 실시한 현황을 보면 필리핀이 4건에 19명으로 가장 많고, 다음은 중국이 4건에 11명이 검거되었으며, 태국이 2건에 3명을 검거하는 등 총 10건에 33명을 검거하였다. 이 중 범죄자에 대한 국내 송환인원은 중국이 8명, 태국이 3명, 필리핀이 2명으로 태국의 경우 검거된 모든 범죄자가 국내에 송환되었으나 중국과 필리핀은 검거인원에 비해 국내 송환인원의 비율은 기대에 미치지 못하는 수준이다. 향후 보이스피싱 등의 범죄자가 해외로 도피하는 경우 보다 적극적인 국제공조를 통해 국내 송환비율을 향상시킬 필요가 있을 것이다.

[표 3-5] 2016년도 전화금융사기 관련 국제공조수사 현황

(단위 : 건 / 명)

국가	검거건수	검거인원	국내 송환인원
중국	4	11	8
필리핀	4	19	2
태국	2	3	3
계	10	33	13

자료: 경찰청(2017) 내부자료

11) 경찰청(2016). “경찰청, 「제2차 한·일·중 경찰협력회의」 개최”, 보도자료(11. 21 자)

## 제2절 최근 보이스피싱 범죄 관련 특징

### 1. 보이스피싱 유형별 피해 특징

보이스피싱을 민생침해 5대 금융악으로 규정(2015년4월8일)한 이후 사기범 목소리 공개 등 전방위적인 홍보 대책 등에 힘입어 2016년 발생한 보이스피싱 피해규모는 1,468억원(총 17,040건)으로, 전년 대비 28% 감소하였다. 유형별로는 정부기관 사칭형이 전체 피해금액의 37.1%로 전년 대비 53.3% 감소하였으며, 대출빙자형은 전체 피해금액의 62.9%를 차지하였고, 전년 대비 20.7% 증가하였다.

앞서 10년간의 보이스피싱 유형별 피해 추세에서 살펴본 바와 같이 보이스피싱 범죄는 발생건수 측면에서 전반적으로 감소세를 보이고 있으나, 대출빙자형의 경우 증가함을 파악할 수 있다.

[표 3-6] 보이스피싱 피해 현황

(단위: 건, 억원, %)

구 분		2015년		2016년		
		건수/금액	비중	건수/금액	비중	증감
피해 건수	정부기관 사칭형	7,239	39.1%	3,384	19.9%	(△53.3%)
	대출빙자형	11,310	60.9%	13,656	80.1%	(+20.7%)
	합 계	18,549	100.0%	17,040	100.0%	(△8.1%)
피해 금액	정부기관 사칭형	1,070	52.5%	544	37.1%	(△49.2%)
	대출빙자형	970	47.5%	924	62.9%	(△4.7%)
	합 계	2,040	100.0%	1,468	100.0%	(△28.0%)

주 : ( )내는 ' 15년 대비 증감률

최근 검찰·경찰·금감원 등 정부기관을 사칭하는 수법에 대한 홍보 강화로 국민들의 대처능력이 강화되자, 금융회사의 대출 광고전화로 가장하여 급전이 필요한 서민들을 대상으로 돈을 편취하는 대출빙자형으로 전환되고 있다.

행정기관을 사칭형태의 보이스피싱은 20대, 30대 여성이 피해자의 38%를 차지하고 있다. 피해자들이 대부분 사회경험이 적고 황급한 상황을 연출하는 고압적인 협박에 심적으로 위축될 가능성이 높아 주요 대상이 되고 있다.

**[표 3-7] 2016년 정부기관 사칭형 성별·연령별 피해 현황**

(단위: 건, %)

구 분	남성		여성	
	피해건수	비중	피해건수	비중
10대 이하	4	0.1%	4	0.1%
20·30대	1,061	31.2%	3,214	63.8%
40·50대	1,360	40.0%	1,227	24.4%
60대 이상	977	28.7%	592	11.8%
합 계	3,402	100.0%	5,037	100.0%

대출빙자형의 경우에는 경제둔화에 따른 서민들의 대출 수요 증가 및 사기수법의 정교화와 지능화로 실제 대출광고와 구별하기가 어려워 피해가 증가하고 있으며 더욱이 대출 수요가 많은 40·50대가 피해자의 절반 이상인 58.6%를 차지하고 있다.

[표 3-8] 2016년 대출빙자형 성별·연령별 피해 현황

(단위: 건, %)

구 분	남성		여성	
	피해건수	비중	피해건수	비중
10대 이하	32	0.2%	28	0.2%
20·30대	5,961	28.9%	5,732	35.4%
40·50대	12,323	59.7%	9,249	57.1%
60대 이상	2,323	11.3%	1,190	7.3%
합 계	20,639	100.0%	16,199	100.0%

## 2. 최근 대포통장 발생 주요 특징

대포통장 근절대책에 힘입어 2016년 대포통장은 46,351개로, 전년 대비 19.1% 감소하였다. 특히 은행에서 의심거래 모니터링 강화와 신규계좌 개설 심사강화 등 추진에 의해 큰 폭으로 감소(△10,955건)한 것으로 나타났다.

[표 3-9] 대포통장 발생현황

(단위: 건, %)

구 분	2015년		2016년		
	건수	비중	건수(증감률)		비중
은행	44,385	77.5%	33,430	(△24.7%)	72.1%
상호금융	6,814	11.9%	6,896	(+1.2%)	14.9%
새마을금고	3,383	5.9%	3,161	(△6.6%)	6.8%
우체국·증권 ·저축은행 등	2,701	4.7%	2,864	(+6.2%)	6.2%
합 계	57,283	100.0%	46,351	(△19.1%)	100.0%

주 : ( )내는 '15년 대비 증감률

① 신규 계좌 대신 정상적으로 사용하는 계좌가 대포통장으로 이용  
 대포통장 중 신규 계좌의 비중(4.2%)이 전년(11.4%) 대비 감소(△7.2%p)한 반면, 정상적으로 사용하고 있는 계좌가 68.3%를 차지하였다. 이는 신규 계좌 발급이 어려워지자 급전이 필요한 서민들이 기존 사용 계좌를 대포통장으로 매매함에 따라 발생한 것으로 분석된다.

**[표 3-10] 신규 계좌 개설 후 기간별 대포통장 이용현황**

구 분	' 13년	' 14년	' 15년	' 16년(증감)	
5일 이내	34.8%	15.7%	11.4%	4.2%	(△7.2%p)
1개월 이내	18.5%	8.8%	10.4%	8.3%	(△2.1%p)
6개월 이내	6.5%	6.4%	11.0%	11.3%	(+0.2%p)
1년 이내	3.6%	5.1%	7.8%	7.9%	(+0.1%p)
1년 초과	36.5%	64.0%	59.4%	68.3%	(+8.9%p)

주 : ( )내는 ' 15년 대비 증감

② 개인 대포통장 명의인 수는 감소하였으나, 법인 명의인은 증가  
 2016년 대포통장 명의인으로 등록된 인원은 27,411명으로 전년(37,280명) 대비 26.5% 감소한 반면, 법인인 명의인은 1,300개로 전기(1,001개) 대비 30.0% 증가하였다. 이는 계좌개설 관련규제를 피하기 위해 거짓으로 법인을 설립 후 법인통장을 개설하여 대포통장으로 이용하는 사례가 급증하였기 때문으로 분석된다.

③ 구직·대출신청 과정에서 대포통장 명의인이 되는 사례 증가  
 아르바이트·대출 과정 등으로 오인하여, 타인의 피해금을 사기범에게 전달하여 대포통장 명의인이 되는 사례가 증가하고 있다.

### 아르바이트 구직자가 대포통장 명의인이 되는 사례

- ① 사기범은 인터넷 구직사이트에 인터넷 쇼핑몰 자금 관리 아르바이트를 모집한다고 광고
- ② 구직자(A씨)가 지원을 하자, 사기범은 구직자(A씨)에게 “구매자로부터 판매대금을 입금 받아 회사가 지정한 계좌로 이체하는 업무” 라고 설명
- ③ 사기범은 다른 피해자에게 보이스피싱을 통해 A씨 계좌로 피해금을 이체토록 함
- ④ 구직자(A씨)는 입금된 금액을 판매대금으로 생각하고 사기범이 지정한 계좌로 이체

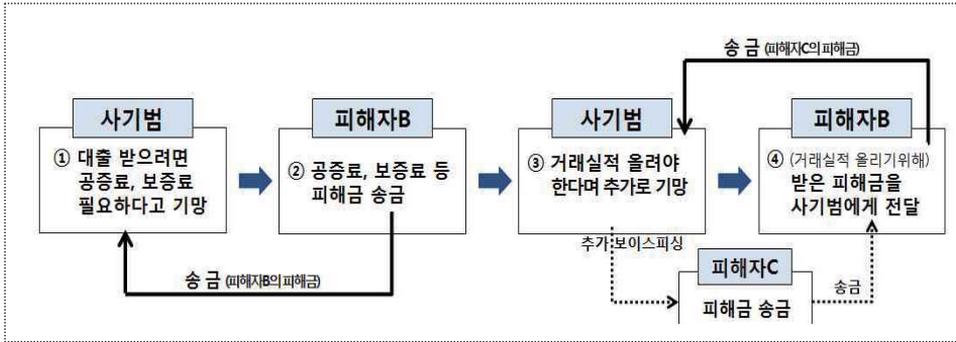


[그림 3-4] 아르바이트 구직자가 대포통장 명의인이 되는 사례

#### ④ 보이스피싱 피해자 명의의 대포통장 활용 사례 증가

### 보이스피싱 피해자가 대포통장 명의인이 되는 사례

- ① 사기범은 피해자B에게 금융회사 직원을 사칭하며 전화한 뒤 저금리로 2,000만원까지 대출을 해주겠다고 권유
- ② 사기범은 대출을 받으려면 공증수수료, 보증서 발급 등을 위해 돈이 필요하다고 피해자B를 기망하여 총 910만원을 이체 받음
- ③ 910만원을 이체 받은 후에도 사기범은 피해자B의 거래실적이 부족하여 대출이 불가하니, 거래실적을 직접 만들어주겠다고 하며 향후 입금되는 금액을 사기범에게 보내도록 유도
- ④ 사기범은 다른 피해자C에게 보이스피싱을 통해 피해자B 계좌로 피해금을 이체토록 한 뒤, 거래실적을 위해 입금된 것으로 오인한 피해자B는 피해금을 사기범에게 전달



[그림 3-5] 보이스피싱 피해자가 대표통장 명의인이 되는 사례

### 3. 2017년도 보이스피싱 범죄 특징

2017년도 상반기의 보이스피싱 주요특징은 보이스피싱에 사용되는 대표통장의 발생건수가 월평균 3,497건으로 2015년 이후 지속적으로 감소하는 추세에 있다. 대표통장 발생건수는 2016년과 대비하여 10.0%가 감소하였다. 보이스피싱의 피해 건수도 월평균 3,674건으로 2015년 월평균 4,808건, 2016년 월평균 3,827건에 비해 감소하였으나, 피해액은 월평균 173억원으로 2016년 대비 8.1%가 증가한 것으로 확인되었다. 이는 보이스피싱의 수법이 기관사칭형에서 주로 저금리 대환대출을 빙자하여 기존 대출금 상환을 사기범의 통장으로 유도하는 대출사기형으로 전환되면서 건당 피해 규모가 크게 증가하였기 때문으로 추정된다.

대표통장 경우는 은행 및 상호금융 권역은 신규계좌 개설심사 및 의심거래 모니터링 강화 등에 힘입어 월평균 대표통장 발생 건수가 2016년 대비하여 은행은 12.7%가 감소하였다. 상호금융은 13.1%가 감소하는 등 큰 폭으로 감소하였으나, 제2금융권 중 새마을금고(7.1%↑)·우체국(10.9%↑)에서 대표통장 발생 건수가 증가하고 있으므로 이에 대한 주의가 요망된다.

최근에는 대표통장 확보가 어려워짐에 따라, 피해금을 비트코인 거래소 계좌로 송금하게 하여 현금화하는 신종 사례까지 발생하고 있다. 보이스피

싱 범죄자들은 피해금으로 온라인 사이트에서 상품권을 구매한 후 이를 현금화하는 기존 수법에 대한 홍보가 강화되자, 비트코인으로 진화하고 있다 (금융감독원, 2017b).

보이스피싱의 경우 대출사기형 보이스피싱의 피해가 지속적으로 증가하였다. 대출사기형의 경우 발신번호 변작, Auto call을 통한 무차별적인 문자 메시지 발송을 통해 대출모집인의 전화 영업방식과 구별이 어려울 정도로 정교화·지능화되는 추세이다. 대출사기형 보이스피싱의 비중은 2015년에 42.7%에서 2016년에는 69.9%, 2017년 상반기에는 71.3%로 증가하였다. 특히 서민층을 위한 햇살론 등 정부지원자금 대출을 많이 사칭하고 있다. 또한, 피해 건수 감소세에도 불구하고 건당 피해 규모는 12.7%가 증가하였다. 이는 대출빙자형의 증가와 더불어 기존의 수수료 편취에서 저금리 대환대출을 빙자하며, 대출금 상환을 사기범의 통장으로 유도하는 수법으로 진화하고 있기 때문이다.

**[표 3-11] 2017 상반기 보이스피싱 유형별 피해자의 성별·연령 분포**

(단위 : 건, %)

구 분	정부기관 사칭형			대출빙자형		
	남성(비중)	여성(비중)	계(비중)	남성(비중)	여성(비중)	계(비중)
10대 이하	- (-)	1 (0.0)	1 (0.0)	11 (0.1)	4 (0.0)	15 (0.1)
20·30대	365 (9.5)	2,002 (51.9)	2,367 (61.4)	2,655 (14.8)	2,379 (13.3)	5,034 (28.0)
40·50대	475 (12.3)	517 (13.4)	992 (25.7)	6,007 (33.5)	4,879 (27.2)	10,886 (60.7)
60대 이상	354 (9.2)	144 (3.7)	498 (12.9)	1,276 (7.1)	728 (4.1)	2,004 (11.2)
합 계	1,194 (30.9)	2,664 (69.1)	3,858 (100.0)	9,949 (55.5)	7,990 (44.5)	17,939 (100.0)

자료: 금융감독원(2017c), '17년 상반기 대포통장 및 보이스피싱 현황 분석, 보도자료

## 제3절 대전광역시 보이스피싱 발생 현황

### 1. 대전광역시 보이스피싱 발생·피해 및 검거 현황

대전시의 보이스피싱 발생 현황은 2009년 이후에 관련 통계가 집계되었다. 2009년에는 총 225건이 발생하였고, 피해액은 19억 원이었으며, 이 중 검거 건수는 108건으로 검거율은 48%이며, 이는 전국 검거율 85.4%에 비해 매우 낮은 수준이다. 2010년에는 발생건수 147건으로 34.7%가 감소하였고, 피해액도 14억 원으로 감소하였다. 검거율은 23.8%로 다시 큰 폭으로 감소하였다. 2011년에는 발생건수가 283건으로 전년 대비 약 2배 증가하였으며, 피해액도 35억 원으로 2.5배 증가하였다. 그러나 검거율은 84.5%로 큰 폭으로 증가하였다. 2012년에는 가장 큰 폭의 증가세를 보이고 있다. 발생건수가 924건으로 전년 대비 3.27배가 증가하였으나 피해액은 42억 원으로 1.2배 증가에 그쳐 소액의 피해발생이 많았음을 알 수 있다. 검거율은 다시 25% 수준으로 대폭 감소하였다. 2013년에는 다시 588건으로 대폭 발생건수가 감소하였으며, 피해액도 34억 원으로 감소하였다. 검거율은 17.9%로 계속 감소추세를 보이고 있다. 2014년에도 358건으로 발생건수는 대폭 감소하였으며, 피해액도 28억 원으로 감소추세를 보였다. 검거율은 36%로 전년 대비 2배가 상승하였다. 2015년에는 528건이 발생하여 증가하였으며, 피해액도 48억 원으로 대폭 상승하였다. 검거율은 26.1%로 하락하였다. 2016년에는 517건이 발생하여 전년 대비 소폭 감소하였으며, 피해액도 43억 원으로 감소하였다. 검거율은 33.7%로 상승하였다.

특이한 점은 전국 단위의 보이스피싱 발생추세와 비교하여 대전시의 보이스피싱 발생추세는 유사한 패턴을 보이지 않는다. 이는 예상컨대, 수집하여 집계한 통계자료가 서로 다를 가능성이 있어 보인다. 예를 들어 앞서 살펴본 전국 지역별 보이스피싱의 최근 발생 현황자료에서 대전시의 보이스피싱 건수와 대전지방경찰청의 집계 건수가 서로 일치하지 않는데, 전국

단위에서는 2013년 이후 대출사기의 통계를 통합하여 집계함으로써 발생건수가 증가한 반면, 대전의 통계자료는 2012년에 급격히 발생건수가 증가한 것을 제외하면 연도별 증가추세를 고려할 때 집계방식에 보이스피싱의 발생건수만 포함시켰을 가능성이 높은 것으로 판단된다. 그러므로 대전시의 보이스피싱 발생현황에 대한 분석은 전국 단위의 분석결과와 비교하기에는 적절하지 않은 것으로 생각되며, 대전의 연도별 증감추세를 중심으로 살펴 보아야 할 것이다.

대전의 경우 2012년을 기준으로 보이스피싱 범죄의 발생건수가 대폭 증가하였고, 피해액도 증가하였음을 알 수 있다. 검거건수의 경우에는 발생건수의 증가에 비해 상대적으로 증가하지 않아 검거율이 매우 저조한 수준임을 알 수 있다. 이는 보이스피싱에 대한 경찰의 보다 적극적인 관심이 필요한 부분이다.

**[표 3-12] 최근 8년간(2009~2016) 보이스피싱 발생 및 검거현황**

구분	발생 건수	피해액(억원)	검거 건수	검거율
2009	225	19	108	42.4%
2010	147	14	35	23.8%
2011	283	35	239	84.5%
2012	924	42	231	25.0%
2013	588	34	105	17.9%
2014	358	28	129	36.0%
2015	528	48	138	26.1%
2016	517	43	174	33.7%

출처: 대전지방경찰청(2017) 내부자료를 편집 인용

## 2. 대전광역시 보이스피싱 유형별 피해 추세

대전시의 2015년과 2016년도의 보이스피싱 유형별 피해 추세의 분석방법은 2015년과 2016년도를 각각 상반기와 하반기로 구분하여 전화금융사기의 대표적인 유형인 기관사칭형과 대출사기형에 따른 월평균 피해액과 피해자수를 통해 추세를 살펴보았다.

먼저 피해액의 추세는 정부기관을 사칭한 금융사기의 경우 2015년도 상반기에 월평균 2억 3천만 원에서 하반기에는 1억 6천만 원으로 약 40%가 감소하였다. 2016년 상반기에는 1억 9천만 원에서 하반기에 1억 7천만 원으로 소폭 감소하였다. 연도별로는 2015년에 비해 2016년에 월평균 피해액이 감소한 것으로 확인되었다. 반면, 대출사기형의 경우는 2015년에는 상반기에 비해 하반기에 소폭 감소하였으나 2016년에는 다시 증가추세로 전환되었고, 피해액의 규모도 대폭 증가하였다. 전반적으로는 2015년의 경우 기관사칭형의 피해액이 대출사기형에 비해 피해액이 많으며, 2016년도 상반기까지 이러한 추세는 이어지다가 2016년도 하반기에 대출사기형의 기관사칭형보다 많은 것으로 확인되었다. 이는 전국단위에서 2015년 하반기 이후에 대출사기형의 피해액이 기관사칭형보다 많아진 이후 피해액의 간격이 크지고 있는 것과 비교할 때 대전광역시의 경우 기관사칭에 의한 보이스피싱의 비중이 상대적으로 높다는 것과 2016년 하반기부터는 대출사기형 보이스피싱이 급증하고 있음을 의미한다. 전체 피해액의 경우에도 2015년은 전반적으로 감소하는 추세였다가 2016년에 다시 큰 폭으로 증가하는 추세로 전환되었다.

피해자의 수에 있어서도 기관사칭형의 경우 꾸준히 피해자의 수가 감소하는 추세이고, 대출사기형은 월평균 피해자의 수가 소폭 감소하고 있으나 일정 숫자가 유지되고 있음을 알 수 있다. 전체 피해자수의 추세는 2015년에 비해 2016년에 감소하였다. 이를 통해 대전광역시의 경우 보이스피싱 피해자의 숫자는 꾸준히 감소하는 추세이나 피해액은 증가하는 추세로 1인당 피해금액이 상승하고 있음을 알 수 있다.

**[표 3-13] 대전광역시 보이스피싱 유형별 피해 추세**

구분 (월평균)		2015상	2015하	2016상	2016하
피해액	정부기관 사칭형	2억3천	1억6천	1억9천	1억7천
	대출 빙자형	1억4천	1억	1억6천	2억6천
	합 계	3억7천	2억6천	3억5천	4억3천
피해자수	정부기관 사칭형	66.2	13.5	10.2	10.7
	대출 빙자형	24	24.2	23.5	23.2
	합 계	90.2	37.7	33.7	33.9

출처: 대전지방경찰청(2017) 내부자료

### 3. 보이스피싱 피해자 현황

2016년도 대전시에서 발생한 보이스피싱 범죄피해자의 성별·연령별 현황을 살펴보면, 총 발생건수 517건 중 여성이 267명에 51.6%이고, 남성이 250명에 48.4%로 여성이 남성보다 조금 많이 피해를 당했으나 거의 유사한 수준이다. 연령별로는 40대가 26.1%로 가장 많고, 다음은 30대 23.6%, 50대가 21.1%의 순서로 많았다. 이는 2015년에 비해 2016년에 대출사기형 보이스피싱이 증가하면서 금융활동의 접근성이 높은 30대에서 50대의 피해자가 많은 것으로 추정된다.

**[표 3-14] 대전광역시 보이스피싱 피해자 현황(2016)**

발생건수	성별		연령별					
	남성	여성	20대	30대	40대	50대	60대	70대 이상
517	250	267	85	122	135	109	52	14
100%	48.4%	51.6%	16.4	23.6	26.1	21.1	10.1	2.7

출처: 대전지방경찰청(2017) 내부자료

## 보이스피싱 예방 및 대응 동향

1. 보이스피싱 주요 수법과 대응방안
2. 보이스피싱 피해방지 주요 대책
3. 해외 주요국의 사례
4. 국내 · 외 지자체 대응 동향

## 4장



# 제 4 장 보이스피싱 예방 및 대응 동향

## 제1절 보이스피싱 주요 수법과 대응방안

### 1. 보이스피싱 범죄 진행과정

#### 1) 범죄 진행 과정

범죄조직은 보이스피싱의 성공률을 높이기 위해 불법 취득한 개인정보를 바탕으로 매우 치밀한 범죄스크립트를 구성하여 이용한다. 또한, 범죄의 특성상 피해자로부터 편취(송금/이체)한 자금을 현금화하여 세탁하는 단계를 거치기 때문에 그 과정도 다소 복잡하다고 할 수 있다.

효과적인 범죄 예방 및 대응을 위해서는 이러한 범죄과정들을 세밀하게 분석할 필요가 있는데, 최관·김민지 등은 ‘한국 보이스피싱 범죄의 진행 과정에 관한 연구(KCI\_FI002032912. 2015.09.21.)’를 통해 국내 최초로 범죄스크립트 기법을 활용하여 보이스피싱 범죄 과정을 분석하고 그 결과 Voice Phishing 범죄 스크립트를 ‘준비’, ‘범행’, ‘범행 후’의 세 가지 단계로 분류하였다. 준비단계는 피싱준비, 텔레마케터 모집, 시나리오 작성으로 구분이 가능하며 주로 Voice Phishing범죄 실행을 위한 구축단계이다. 범행단계는 국제전화 및 인터넷전화를 통해 특정 및 불특정 다수 피해자들에게 전화를 걸고 피싱을 시도하는 단계인 것으로 파악이 되었으며, 범행 후 단계는 피해자들로부터 피해액을 입금 받고 이를 출금하고 다시 송금하는 단계인 것으로 확인되었다. 논문의 분석결과들을 종합하여 스크립트화하면 다음과 같다.

**[표 4-1] 보이스피싱 범죄 스크립트**

프로세스	내용
보이스피싱 준비	<ul style="list-style-type: none"> <li>- 해외총책(주로 대만인)이 보이스피싱 범죄준비</li> <li>- 중간보스(중국한족 혹은 범죄경력 있는 한국인)</li> <li>- 아지트로 아파트 3-4채 빌림</li> <li>- 조직구성(전산팀, 텔레마케터, 시나리오, 통장모집팀, 현금인출팀, 송금, 휴대전화팀)</li> <li>- 각팀별 맡은 역할 수행 시작</li> <li>- 한국총책 구성(피해금 송금역할)</li> </ul>
텔레마케터 모집	<ul style="list-style-type: none"> <li>- 한국어에 능통한 직원 모집 및 아지트에서 숙식을 하며 직무교육 실시</li> <li>- 조직배신에 대한 보복교육 실시</li> <li>- 기본급(3000-4000위안)에 인센티브 있음</li> <li>- 1개조 8-10여명의 텔레마케팅 팀으로 구성</li> </ul>
시나리오 작성	<ul style="list-style-type: none"> <li>- 피해자 유형(보호형, 보상제공형, 협박형, 지인사칭형, 의무부과형)별 30가지 이상의 시나리오 작성</li> <li>- 의심 및 거절에 대비한 긴급대응시나리오 역시 작성</li> </ul>
전화하기	<ul style="list-style-type: none"> <li>- 전산팀이 구축한 자동통화 프로그램에 의해 한국의 특징인 혹은 불특정 다수인 대상 전화시작</li> <li>- 수신경로는 역추적이 어려운 국제전화 사업자 방법 혹은 인터넷전화 사업 자방법을 주로 사용</li> <li>- 특히 인터넷전화는 VoIP(Voice over Internet Protocol)서비스가 보안기술이 미적용상태이며, 자동화 장비에 의해 짧은 시간에 발신조작을 통한 무작위 발송이 가능함.</li> </ul>
전 화	<ul style="list-style-type: none"> <li>- 전산팀은 자동통화 프로그램에 의해 피해자가 전화를 받을 경우, 버튼을 눌러 상담원에게 넘기고 통화 시작.</li> <li>- 상담원을 피해자를 속이고 ATM으로 유도하여 금액결제를 유도</li> </ul>
피해액입금	<ul style="list-style-type: none"> <li>- 통장모집팀에 의해 만들어진 대포통장계좌로 피해액이 입금됨</li> </ul>
출 금	<ul style="list-style-type: none"> <li>- 해외 텔레마케터가 인출관리팀장에게 피해자정보를 알림</li> <li>- 인출관리팀장이 관련정보를 다시 현금인출팀에 알리고 출금 지시</li> <li>- 현금인출팀이 하루에 17-18번씩 대포통장계좌를 확인, 입금액 확인 및 인출</li> <li>- 인출과정은 보안을 위해 대포폰을 사용하며 매번 다른 장소, 방법 등을 달리함</li> <li>- 인출된 돈은 직접전달 혹은 조직원을 통하여 송금팀에 전달됨</li> <li>- 인출된 금액이 클 경우 인출팀장이 직접 전달</li> </ul>
송 금	<ul style="list-style-type: none"> <li>- 인출팀이 피해금을 인출해서 송금팀에 넘기면 이를 중국/대만으로 송금.</li> <li>- 전통적으로 송금팀은 주로 관광객으로 위장하여 입국하면서 피해금을 송금.</li> <li>- 현대에는 환치기 수법을 통해 피해금을 송금.</li> <li>- 특히 계좌상 흔적이 남지 않아 환치기 수법이 주로 사용되고 있음</li> <li>- 한국사채업자를 조직원으로 두고 피해금의 일정수수료를 제외하고 보이스 피싱 사기단에 위안화로 전달.</li> </ul>

자료 : 한국 보이스피싱 범죄의 진행과정에 관한 연구((KCI\_FI002032912, 최관 · 김민지)

## 2) 한국 보이스피싱 범죄의 특징

앞서 살펴본 ‘한국 보이스피싱 범죄의 진행과정에 관한 연구(최관·김민지)’에서는 한국 보이스피싱 범죄의 특징을 다음과 같이 5개 항목으로 제시하였다.

### ① 첫째, 국제적인 범죄

국제적인 범죄형태를 보이는 보이스피싱은 범죄조직의 두목급은 대만인 혹은 중국인, 부두목급은 중국인, 대만인, 한국인이고 실제 보이스피싱을 실행하는 사람은 조선족과 중국인 유학생, 대만인 송금액, 한국인 계좌모집책 등으로 구성된다. 다양한 국가의 국민들이 참여하는 경우가 많기 때문이었다. 이처럼 보이스피싱 범죄조직은 단일 국가의 국민으로 범죄집단이 구성되는 보통의 범죄와는 다른 극동아시아의 여러 국가의 국민으로 다양하게 구성되어 있으며, 범죄의 특성상 중국 혹은 대만 등지에서 한국 혹은 일본에 전화를 걸어 범죄를 저지르는 경우가 대부분인 것으로 밝혀졌다.

### ② 둘째, 복잡한 발신경로를 통해 보이스피싱 범죄가 실행

보이스피싱은 특정한 국제전화망을 주로 사용했는데, 국제전화와 인터넷 전화가 복잡한 경로로 수신되기 때문에 피해자가 받은 전화를 수사기관에서 역추적하는 것이 쉽지 않다는 문제점이 있었다. 또한 국내 통신회사나 인터넷회사를 통해 이용된 회선이나 IP를 추적하더라도 중국의 특정 통신회사에서 발신되었다는 정보만 알 수 있을 뿐이기 때문에 중국공안당국이 중국의 통신회사를 통해 해당 전화의 발신자를 추적하지 않는 한 한국에서 콜센터에 걸려오는 전화를 막을 수도 없고 추적할 수도 없게 되어 있다는 것이었다.

### ③ 셋째, 보이스피싱 범죄조직의 구성원들이 점조직화

보이스피싱 조직의 구성원들은 형사사법기관의 추적과 검거를 피하기 위해 가입이 쉽고 추적이 어려운 선불폰을 범죄에 사용하고 있는 것으로 밝

혀졌다. 그리고 범죄조직은 철저한 점조직 형태로 구성되어 현금인출책, 계좌모집책 등 조직의 말단 구성원들이 검거되더라도상부 조직에 대한 정보를 갖고 있지 않기 때문에 상부조직은 계속해서 수사기관의 추적을 피할 수 있다는 점이 발생하게 된다. 또한 직속 상부조직원들 경우 역시 서로 별명을 부르고 있고, 접선할 경우에도 택배 혹은 퀵서비스를 이용하고 있어 이름이나 주거지 정보 등에서 조차 서로 간에 일체 알지 못한다는 특징이 확인되었다.

#### ④ 넷째, 보이스피싱 관련 범죄수법이 다양하게 진화 및 변화

보이스피싱 범죄는 사칭기관이 다양화되면서 범죄의 수법도 지속적으로 변화되고 있다. 특정 기관들을 일정 기간 동안 사칭하다가 사람들에게 많이 알려져 있다고 판단되면 새로운 기관으로 사칭하고 있으며, 피해자들이 계좌이체를 통해 돈이 이체된다는 사실을 알지 못하게 하기 위해 현금지급기의 조작 화면을 영어로 선택하게 하기도 하는 것으로 조사되었다. 또한 피해자에게 계좌이체 즉시 거래명세표를 찢어 버리고, 24시간 내에는 절대 금융거래를 하지 못하게 하며, 은행 등 금융기관이나 직원들이 범죄단에 관련된 경우가 많으므로 금융기관에는 절대 알리지 못하도록 전화통화시 피해자들에게 단속하는 것으로 조사되었다. 따라서 피해자들이 자신이 속았다는 사실을 바로 알지 못하기 때문에 현금지급정지 혹은 수사기관에 대한 신고가 지연되도록 하는 등의 방식으로 범죄피해에 대한 신속하고 효율적인 대응을 방해하는 것으로 나타났다.

#### ⑤ 다섯째, 대부분의 보이스피싱 범죄자가 죄의식이 결여

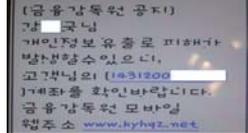
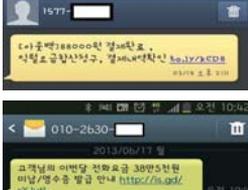
본 연구 결과 보이스피싱은 중국의 콜센터에서 국내의 불특정 다수의 피해자들에게 전화를 걸어 속이기 때문에 비대면성, 익명성이 보장되고 있으며 검거 가능성이 적어서 범죄인들의 죄의식이 다른 사기사건에 비해 낮은 편이었다. 이 때문에 콜센터에서 전화를 거는 조선족 및 중국인들의 경우 전화를 받은 사람들이 속지 않으면 농담을 하거나 아예 욕을 하는 여유까

지 보이고 있는 것으로 분석결과 나타났다. 심지어 몇몇의 사례들에서는 피해금을 인출하는 조직원들도 대부분 자신들이 인출하는 돈이 한국의 피해자들에게서 전화사기를 통해 편취한 피해금이라는 사실을 잘 모르는 경우도 있었다. 중국의 범죄조직에서는 부패한 관료들의 불법적인 돈을 자금 세탁하기 위해 인출한다고 설명하기 때문에 해당 조직원들도 보이스피싱 범행에 대한 죄의식이 낮은 특성이 있는 것으로 나타났다.

## 2. 보이스피싱 주요 수법

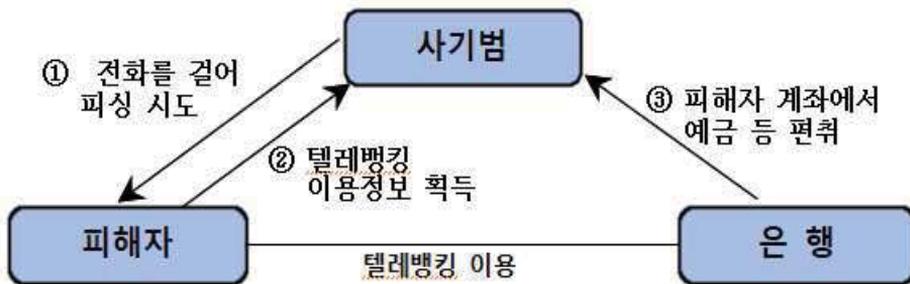
### 1) 주요 유형

[표 4-2] 전자금융사기 유형 및 특징 (2014년)

유형	특징	
피싱사이트	금융정보편취용 가짜 홈페이지로 이동	
파밍	정상적인 경로로 특정 홈페이지에 접속하여도 악의적으로 만들어 놓은 금융정보편취용 가짜 홈페이지로 이동	
스미싱	SMS 등으로 소액결제를 유도하거나, 스마트폰 악성코드를 유포하여 소액결제정보 편취	

자료 : 금융감독원(2014), 피싱사기 피해 구체현황 및 소비자 유의사항, 보도자료 발취

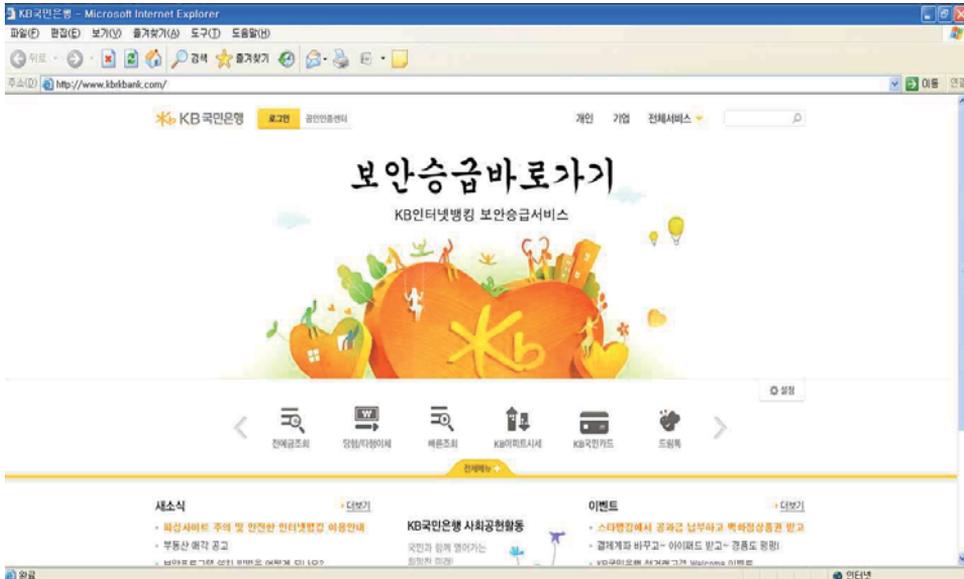
### 2) 텔레뱅킹을 이용한 보이스 피싱



[그림 4-1] 텔레뱅킹을 이용한 보이스피싱 흐름(2012년)

자료: 금융감독원(2012b), 최근 보이스피싱 현황 및 관련 유의사항, 보도자료

## 2) 은행 사칭 피싱 사이트 개설



[그림 4-2] 은행을 사칭한 피싱사이트 사례(2012년)

자료: 금융감독원(2012b), 최근 보이스피싱 현황 및 관련 유의사항, 보도자료

## 4) 대출 빙자 사기

[표 4-3] 대표적인 대출사기 수법(2015년)

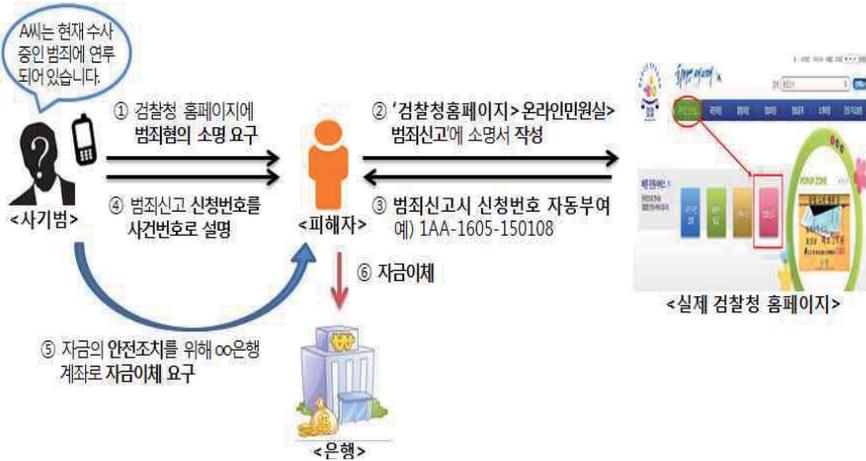
- 신용등급이 낮아 대출이 어려우니 대출을 받기 위해 보증금, 보증보험료를 보증금 환급용 계좌로 송금해라
- 신용조회기록 삭제 또는 신용등급 상향조정에 필요한 금액을 송금해라
- 저금리로 대환하기 위해서는 일정기간의 이자를 선납해라
- 저금리로 대환하기 위해서는 본인 명의의 기존 대출을 사기범이 알려주는 계좌로 갚아라

자료: 금융감독원(2015c), 2015년 하반기부터 금융사기 피해 현저히 감소, 보도자료

## 5) 공공기관 사칭

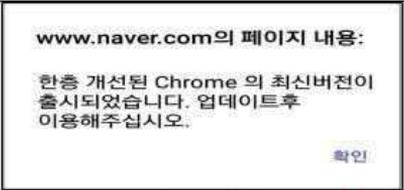
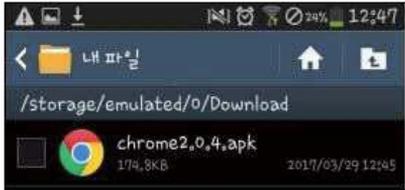
[표 4-4] 대검찰청 홈페이지를 활용한 신종 보이스피싱(2016년)

- ① 보이스피싱 사기범은 서울중앙지방검찰청 수사관을 사칭, 피해자에게 현재 조사 중인 사건 범죄에 연루되어 있으니 형사처벌을 면하기 위해서는 대검찰청 홈페이지에 접속하여 소명할 것을 요구
- ② 피해자는 공식 “대검찰청 홈페이지(www.spo.go.kr) > 온라인민원실 > 범죄신고”에 접속하여, 범죄에 연루되지 않았다는 내용으로 신고함
- ③ 범죄신고 홈페이지에 범죄신고시 민원신청번호가 자동으로 부여되어 피해자에게 문자로 전송됨  
예) 1AA(인터넷, 서면, 방문접수 등 구분)-1605(신고날짜)-150108(일련번호)
- ④ 사기범은 민원신청번호에 앞에 3자리는 특별사건 번호이고, 1605는 범죄신고 일자, 마지막 번호들은 피해자 사건번호라고 거짓 설명하여 피해자들로 하여금 자신을 검찰공무원임을 믿게 함
- ⑤ 사기범은 피해자 명의 계좌에 있는 돈이 위험에 노출되어 있으니, 사건이 끝날 때까지 00은행 계좌에 보관하여 안전조치를 하겠다며 자금이체를 요구
- ⑥ 사기범은 해당 사건은 철저히 비밀리 조사하고 있으니 은행 또는 경찰에 절대 누설해서는 안되며, 누설할 경우 또 다른 피해자가 발생할 뿐만 아니라 비밀누설죄로 처벌될 수 있다며 피해자를 기망



## 6) 악성코드 유포

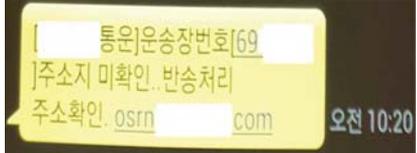
[표 4-5] 악성코드 유포 사례

<p>청계천-성북천 이용자 대상 보이스피싱 유발 악성코드 유포, 주의요망</p>	
<p><b>&lt; 개요 &gt;</b></p>	
<p>▶발견일시 : 2017. 3. 29. 12:45경</p> <p>▶발견장소 : 서울 동대문구 청계천로7길 4 인근(청계천-성북천 접경 둔치)</p> <p>▶요약정보 : 위 장소 이용자 대상 Chrome 업데이트 유도하여, 문자메시지 대량발송 및 금융정보 탈취 등 사이버범죄에 악용되는 악성코드 유포 중</p>	
<p>○ 악성코드 설치 과정</p>	
 <p>① 'anygate' 명칭으로 보안 설정되지 않은 와이파이 식별자 확인</p>	 <p>www.naver.com의 페이지 내용: 한층 개선된 Chrome 의 최신버전이 출시되었습니다. 업데이트후 이용해주십시오.</p> <p>확인</p> <p>② 인터넷 실행 시 '크롬(chrome) 업데이트' 빙자 악성코드 설치 유도</p>
 <p>③ 악성코드 설치 상태</p>	 <p>악성코드 유포지점 (성북천교 개방화장실 인근) 안내</p>
<p>○ 발생 우려되는 사이버범죄 피해</p> <ul style="list-style-type: none"> <li>○ 문자메시지 대량 전송 및 전화번호, 은행계좌 등 개인정보 유출</li> <li>○ 악성코드로 인해 파밍, 보이스피싱 등 사이버범죄 피해 발생 가능</li> </ul>	
<p>○ 당부사항(안드로이드 스마트폰 사용자 대상)</p> <ul style="list-style-type: none"> <li>○ 보안 설정되지 않은 와이파이 접속 차제</li> <li>○ 악성코드로 인한 피해 예방을 위한 백신 설치 / 사용</li> <li>○ 출처를 알 수 없는 앱 설치 금지</li> </ul>	

자료: 정부24(<http://www.gov.kr>).서울특별시 동대문구 보도자료

## 6) 신종 보이스피싱 수법

최근에 나타난 신종 보이스피싱 수법은 금융회사를 사칭하며 대출을 해 줄 것처럼 속인 뒤 돈을 편취하는 사기방식은 기존과 동일하나, 사기과정 및 피해금 인출과정에서 첨단 수법을 사용하고 있다. 이러한 신종 보이스피싱 수법은 아래와 같은 3단계로 진행된다.

① 피해자 물색 단계 ⇒ 악성코드 유포	
<ul style="list-style-type: none"> <li>○ 사기범은 택배 배송 등을 사칭하며 악성코드 URL이 포함된 문자메시지를 불특정 다수에게 발송</li> </ul>	
<ul style="list-style-type: none"> <li>○ 택배 문자로 오인한 피해자가 URL을 클릭하면 스마트폰에 악성코드가 설치되고 피해자의 휴대폰 번호가 사기범에게 전송</li> </ul>	
② 보이스피싱 시도 단계 ⇒ 전화번호 변작	
<ul style="list-style-type: none"> <li>○ 사기범은 전화번호를 확보한 피해자의 스마트폰에 금감원 콜센터번호(☎1332) 및 금융회사 대표전화번호가 표시*되게끔 발신 전화번호를 변작하여 전화</li> <li>* 악성코드 감염으로 인해 피해자가 '1332' 및 금융회사 대표번호로 전화(Return Call)하여도 사기범에게 연결</li> <li>○ 금감원 직원 등을 사칭하며 보이스피싱 시도</li> </ul>	

③ 피해금 인출 단계 ⇒ 가상화폐 악용	
<ul style="list-style-type: none"> <li>○ 사기범은 가상화폐 매매에 필요한 거래소 가상계좌로 피해금을 입금*</li> <li>* 피해자로 하여금 가상화폐 거래소 가상계좌로 직접 입금토록 하거나, 혹은 피해자가 대포통장으로 입금하면 사기범이 거래소 가상계좌로 입금</li> </ul>	
<ul style="list-style-type: none"> <li>○ 피해금으로 가상화폐를 구입하고 가상화폐 전자지갑을 이용하여 거액의 현금을 손쉽게 인출*</li> <li>* 휴대폰번호 및 이메일만으로 가상화폐 거래소 회원 가입이 가능하며, 인출한도에 제한이 없음(금융회사 자동화기기 일일 인출한도는 600만원)</li> </ul>	
<p>④ 금감원(또는 금융회사)으로 연락했으나, 악성코드로 사기범에게 연결</p> <p>② URL 등 클릭 → 악성코드 설치</p>	
 <p>① 악성코드 URL 스팸문자 발송 (피해자 → 사기범)          ② URL 등 클릭 → 악성코드 설치 (피해자)          ③ 금감원(또는 금융회사) 전화번호로 변작 후 보이스피싱 (사기범 → 피해자)          ④ 금감원(또는 금융회사)으로 연락했으나, 악성코드로 사기범에게 연결 (피해자)          ⑤ 피해금 입금 (피해자 → 대포통장)          ⑥ 피해금 이체 (대포통장 → 거래소 가상계좌)          ⑦ 가상화폐 구매 (거래소 가상계좌 → 가상화폐 거래소)          ⑧ 가상화폐를 전자지갑으로 송금 (가상화폐 거래소 → 사기범 전자지갑)          ⑨ 가상화폐 현금화 (사기범 전자지갑 → 사기범)</p>	

[그림 4-3] 첨단 보이스피싱 수법

이러한 보이스피싱 수법은 악성코드 유포, 전화번호 변작 및 가상화폐 악용 등 첨단 수법을 동원하고, 특히 스마트폰을 통해 이루어지는 경우가 많아 금융소비자의 각별한 주의가 요망되고 있으며, 금융감독원은 금년 10월 소비자정보를 발령하기도 하였다.

[표 4-6] 금감원 피해 접수 및 소비자 경보 발생 사례

금감원 피해(상담) 접수 사례	<ul style="list-style-type: none"> <li>○ '17.7월~9.20일 기간 중 악성코드 설치에 따른 금감원 전화(☎1332) 사칭 상담건수 총 18건</li> <li>○ ' 17.1월~8월 기간 중 보이스피싱 전화번호 1,652건 중 48%가 발신번호 변작 등 불법이용</li> <li>○ ' 17.7월~8월 가상화폐를 악용하여 피해금이 인출된 사례 총 50건(피해금 35억원)</li> </ul>									
소비자 경보 발령 사례	<table border="1" style="width: 100%;"> <tr> <th colspan="2" style="background-color: #ffff00;">■ 소비자경보 2017-8호</th> </tr> <tr> <td style="text-align: center;">등급</td> <td style="text-align: center;"> <table border="1" style="display: inline-table;"> <tr> <td style="background-color: #ff8c00;">주의</td> <td style="border: 1px solid red;">경고</td> <td style="border: 1px solid red;">위험</td> </tr> </table> </td> </tr> <tr> <td style="text-align: center;">대상</td> <td style="text-align: center;">스마트폰 이용자</td> </tr> </table>	■ 소비자경보 2017-8호		등급	<table border="1" style="display: inline-table;"> <tr> <td style="background-color: #ff8c00;">주의</td> <td style="border: 1px solid red;">경고</td> <td style="border: 1px solid red;">위험</td> </tr> </table>	주의	경고	위험	대상	스마트폰 이용자
■ 소비자경보 2017-8호										
등급	<table border="1" style="display: inline-table;"> <tr> <td style="background-color: #ff8c00;">주의</td> <td style="border: 1px solid red;">경고</td> <td style="border: 1px solid red;">위험</td> </tr> </table>	주의	경고	위험						
주의	경고	위험								
대상	스마트폰 이용자									

자료: 금융감독원 보도자료, 불법금융대응단, 첨단 수법으로 무장한 신종 보이스피싱 유의, 소비자경보 발령! 2017.10.10

[표 4-7] 금융소비자 당부사항(금융감독원)

구분	대응 방법
악성코드 감염 유의	<ul style="list-style-type: none"> <li>○ 출처가 불분명하거나 잘 알지 못하는 앱 또는 문자메시지는 악성코드일 수 있으므로 보는 즉시 바로 삭제</li> <li>- 특히, 택배 배송을 사칭하는 문자메시지에 유의하고, 악성코드 감염을 방지하기 위해 보안 앱을 이용할 것을 권장</li> </ul>
변작된 전화번호 유의	<ul style="list-style-type: none"> <li>○ 발신 전화번호는 변작되어 금감원과 금융회사 등의 전화번호로 허위 표시 될 수 있음</li> <li>- 이러한 전화를 받은 경우 악성코드 감염 우려가 없는 유선전화 등으로 해당 기관에 직접 전화하여 사실여부를 확인 할 것</li> </ul>
가상화폐 거래 유의	<ul style="list-style-type: none"> <li>○ 금감원 및 금융회사 등은 어떠한 경우에도 가상화폐 거래소 가상계좌로 금전을 송금·이체하도록 요구하지 않음</li> <li>- 이를 요구하는 경우 보이스피싱 등 불법거래일 가능성이 높으므로 절대 응하지 말 것</li> </ul>

### 3. 금융사기 피해자 분석<sup>12)</sup>

#### 1) 분석 개요

금융감독원은 2015년 10월 「전기통신금융사기 특별법」<sup>13)</sup>에 따라 금융감독원에 피해구제를 신청한 피싱사기와 대출사기 피해자현황을 분석하고 ‘금융사기 피해자 분석결과 및 대응방향’을 발표하였다. 이 자료는 2015년 1~8월 기간 중 발생한 금융사기 총 44,619건을 대상으로 다양한 피해자 유형을 분석하였다. 동 기간 중 금융사기 피해금액은 1,946억원으로 이중 피싱사기는 1,202억원, 대출사기는 744억원으로 나타났다.

[표 4-8] 금융사기 발생 현황(2015)

피해발생 건수 기준 (단위 : 건, %)		
구분	건수	비중
피싱사기	18,263	40.9
보이스피싱	8,167	18.3
파밍·피싱사이트	10,096	22.6
대출사기	26,356	59.1
합계	44,619	100.0

피해 금액 기준 (단위 : 건, %)		
구분	피해금액	비중
피싱사기	1,202	61.8
보이스피싱	564	29.0
파밍·피싱사이트	637	32.8
대출사기	744	38.2
합계	1,946	100.0

주 : 2015년 1~8월 기간 중 발생한 금융사기를 대상으로 함

12) 금융감독원(<http://www.fss.or.kr>)이 제작·배포한 ‘금융사기 피해자 분석결과 및 대응방향 보도자료(2015.10.02.)’의 주요 내용을 인용·재가공

13) 「전기통신금융사기 특별법」 개정시행으로 대출사기 피해신고가 '14.7.29일부터 가능해짐 - 이에 따라 '15년도 이전의 금융사기 사기유형별 연간비교는 어려움

## 2) 연령별 피해 현황

금융사기에 취약한 연령대는 40대 남성과 30대 여성으로 나타났다. 전체 피해건수의 연령대별 피해자 점유율은 40대 남성이 남성 중 28.9%, 30대 여성이 여성 중 29.1%로 가장 높은 점유율을 보여 이들 연령대가 보이스피싱 범죄에 취약한 것으로 나타났다.

[표 4-9] 금융사기 유형별 성별·연령대별 피해현황

(단위 : 건, %)

구분	피싱(a)				대출사기(b)				계(a+b)			
	남성		여성		남성		여성		남성		여성	
	건수	비중	건수	비중	건수	비중	건수	비중	건수	비중	건수	비중
0~9세	0	0.0	3	0.0	2	0.0	6	0.1	2	0.0	9	0.0
10~19세	3	0.0	10	0.1	7	0.0	5	0.0	10	0.0	15	0.1
20~24세	224	3.3	383	3.4	222	1.4	348	3.2	446	2.0	731	3.3
25~29세	634	9.2	2,980	26.5	820	5.3	699	6.4	1,454	6.5	3,679	16.5
30~39세	1,486	21.6	3,707	32.9	3,057	19.9	2,753	25.1	4,543	20.5	6,460	29.1
40~49세	1,465	21.3	1,975	17.5	4,955	32.3	3,892	35.5	6,420	28.9	5,867	26.4
50~59세	1,404	20.4	1,202	10.7	4,404	28.7	2,522	23.0	5,808	26.1	3,724	16.8
60세~	1,659	24.1	1,006	8.9	1,873	12.2	739	6.7	3,532	15.9	1,745	7.8
총합계	6,875	100.0	11,266	100.0	15,340	100.0	10,964	100.0	22,215	100.0	22,230	100.0

주) 피해발생 건수 기준

### 3) 유형별 피해

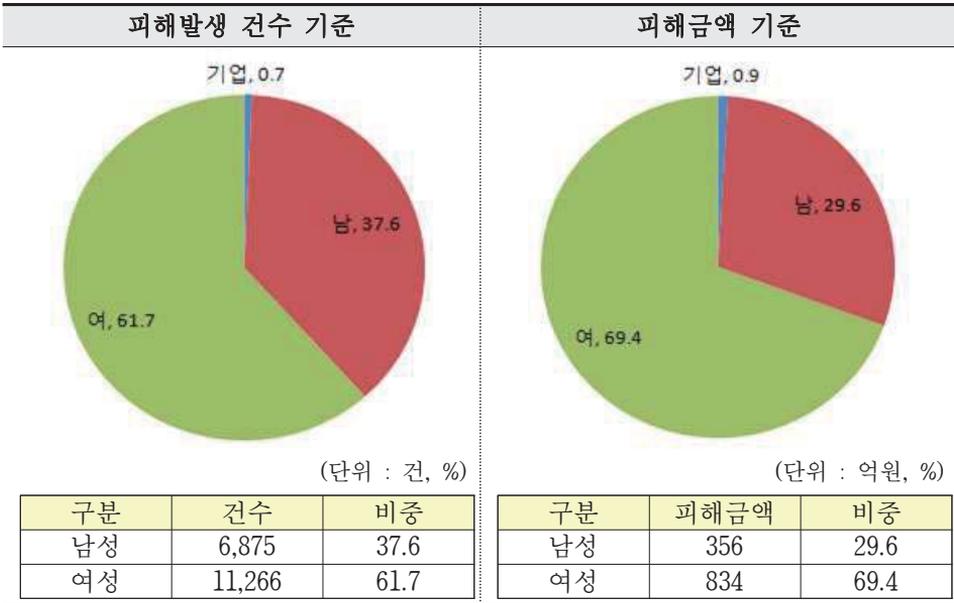
금융사기 유형별로는 피싱사기에 취약한 여성의 연령별 발생비중은 20대 ~ 40대에 80.3%가 집중되어 있고, 그중 30대의 비중이 32.9%로 가장 높았는데 이는 30대의 여성층이 사회경험 부족 등으로 사기범의 심리적 압박에 잘 속아 넘어가기 때문인 것으로 추정된다.

대출사기에 상대적으로 취약한 남성의 연령별 발생비중은 30대~50대에 83.6%가 집중되어 있고, 그중 40대의 비중이 32.3%로 가장 높게 나타났으며 이는 가장으로서 자금수요가 높은 40대 남성에게 대한 접근이 많았을 것으로 추정된다. 특히, 남성중에서는 60대 이상 연령층의 건수 점유율이 24.1%를 나타내어 피싱사기 피해를 가장 많이 당하고 있는 것으로 분석되었는데, 금융사기 수법이 지능화, 교묘화 되어감에 따라 금융사기에 신속히 대응하기에 상대적으로 곤란한 고령층의 피해가 커진 것으로 판단된다.

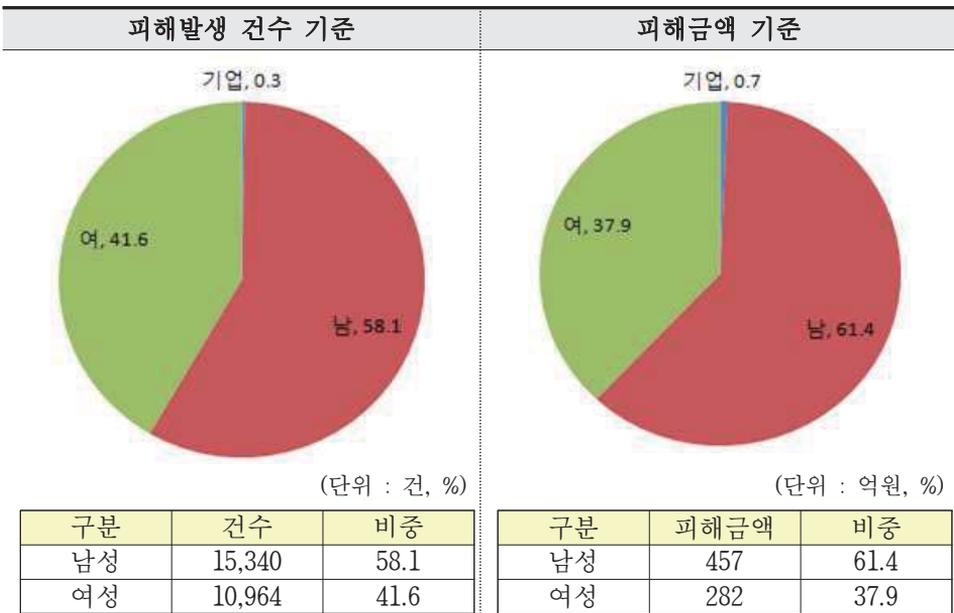
### 4) 성별 피해

피싱사기는 30대 여성, 대출사기는 40대 남성이 취약한 것으로 나타났다. 금융사기의 성별 발생비중은 피해발생 건수 기준으로 남성·여성이 49.8%로 같으나 피해금액 기준으로는 여성이 57.4%로 남성보다 다소 높은 것으로 나타났고, 사기유형별로는 피싱사기에는 여성이 남성보다 취약하여 전체의 61.7%(금액기준 69.4%)를 차지하고 있는 반면, 대출사기의 경우에는 남성이 상대적으로 취약하여 전체의 58.1% (금액기준 61.4%)에 달하는 것으로 분석되었다.

[표 4-10] 피싱사기 성별 피해 분석



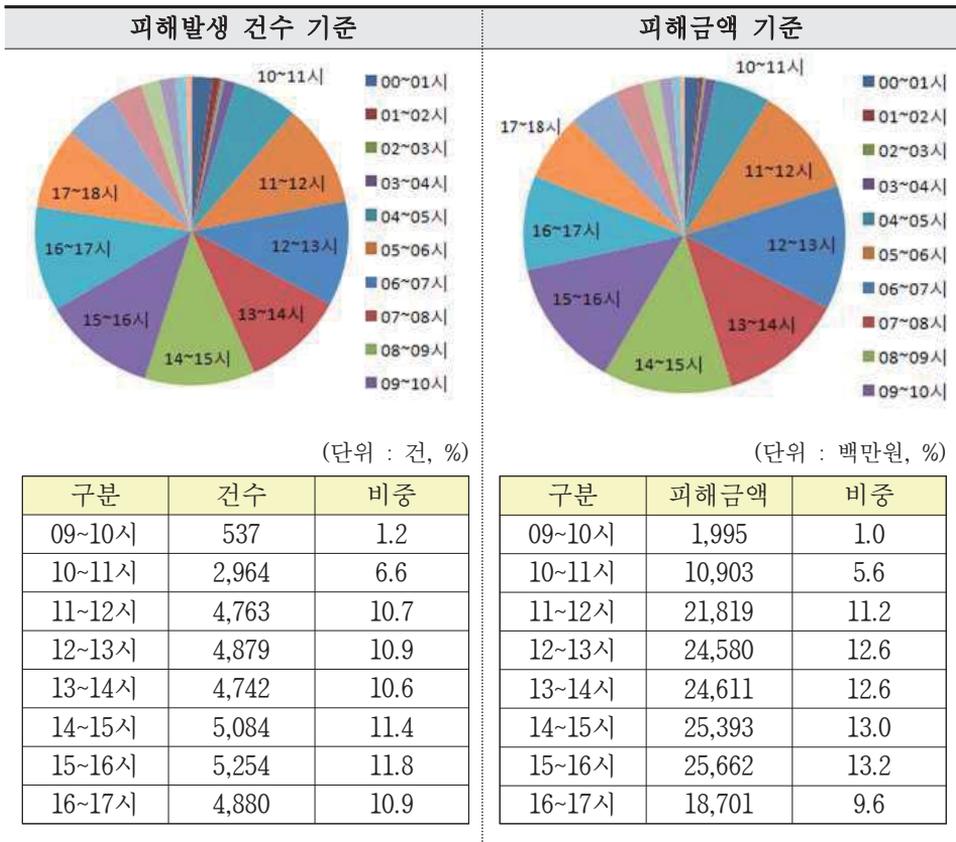
[표 4-11] 대출사기 성별 피해 분석



### 5) 시간대별 · 요일별 분석

보이스피싱 범죄가 주로 발생하는 시간은 금융회사 영업시간대중에서 11시~17시 중에 집중되나(피해발생 건수 기준 66.3%, 금액 기준 72.2%), 영업시간외에도 피해가 발생(피해발생 건수 기준 25.7%, 금액 기준 20.9%)하고 있다.

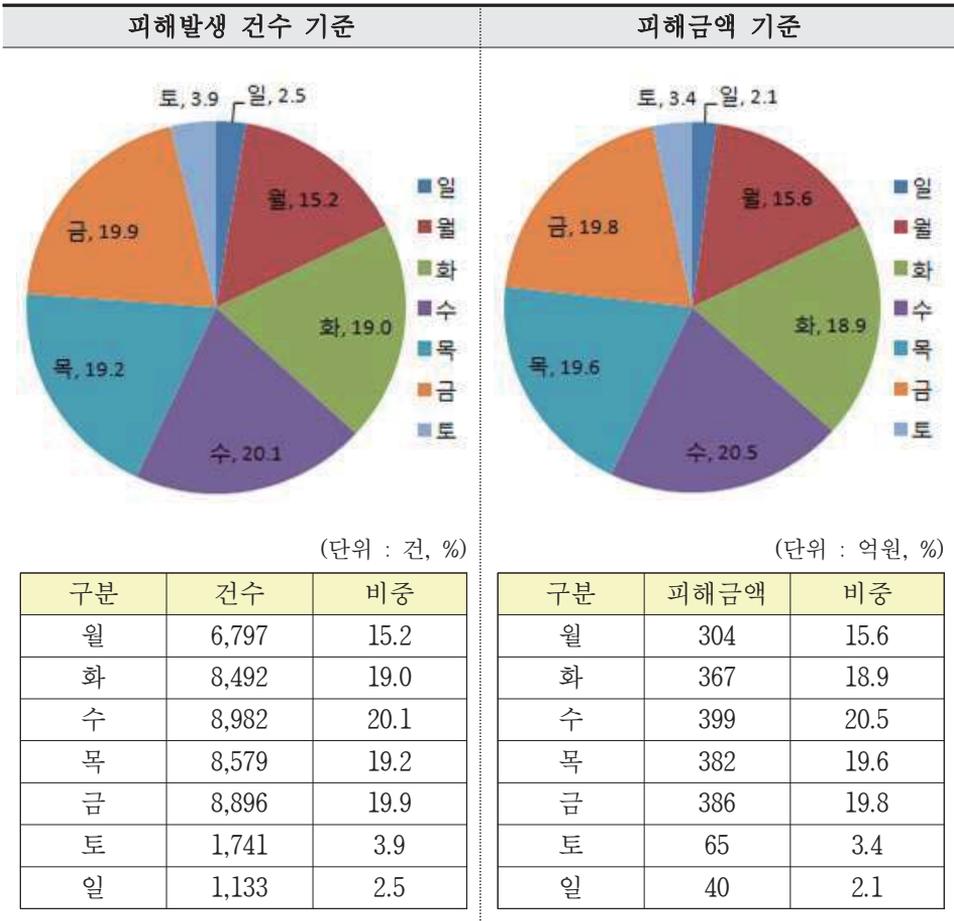
[표 4-12] 시간대별 피해 현황



요일별로는 평일(화~금요일)에 피해가 집중되나(피해발생 건수 기준 78.2%, 금액 기준 78.8%), 휴일에도 피해가 발생(피해발생 건수 기준 6.4%, 금액 기준 5.5%)하고 있다. 이는 보이스피싱을 통해 창구나 CD/ATM기로

유도하는 것과 달리 피싱사이트로 유도하는 파밍 등의 수법은 영업시간이 아니더라도 범행이 가능하기 때문인 것으로 보여 진다.

[표 4-13] 요일별 피해 현황

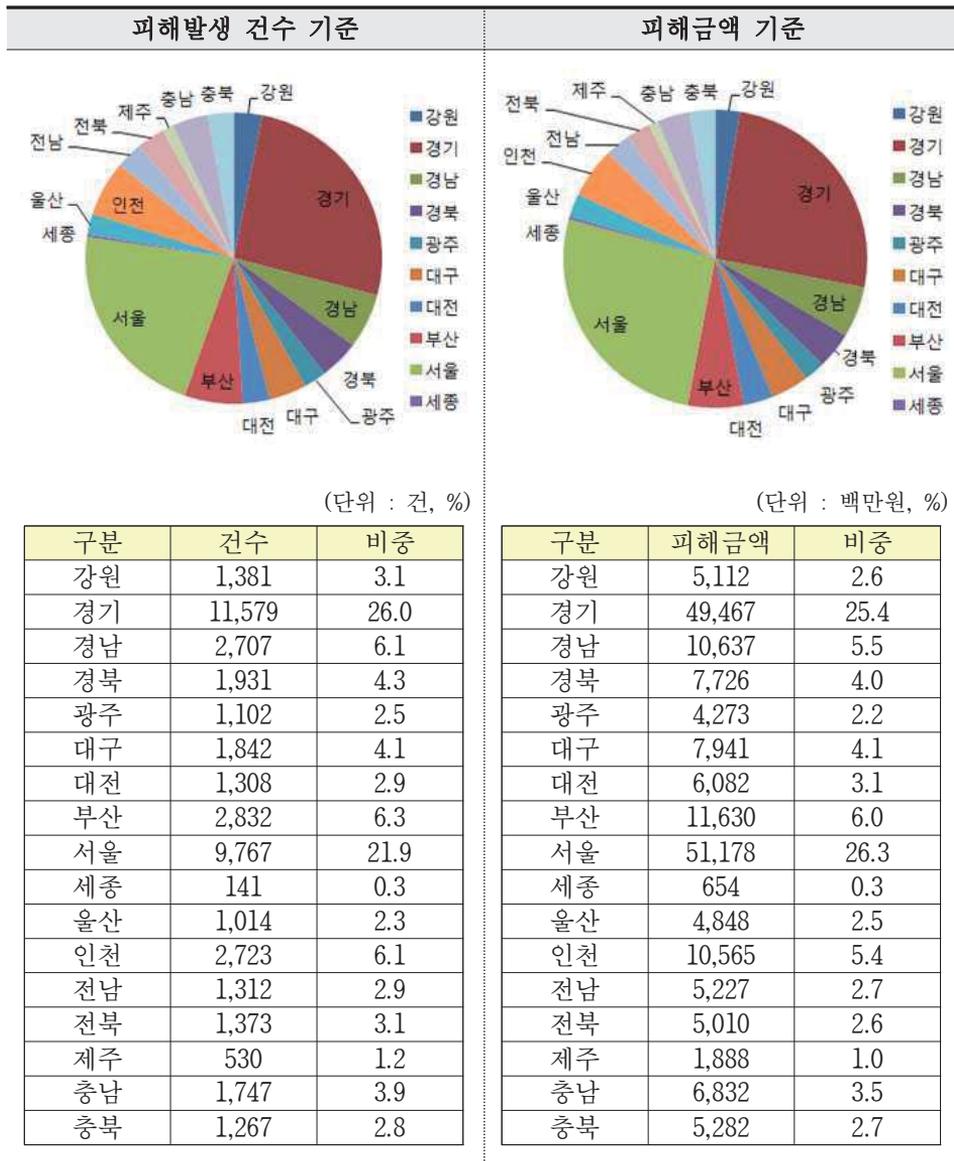


## 6) 지역별 피해 분석

지역별로는 경기, 서울, 인천 등 수도권에 피해가 집중(54.0%)된 것으로 나타났다. 인천·경기(피해발생 건수기준 32.1%, 금액 기준 30.9%), 서울(피해발생 건수기준 21.9%, 금액기준 26.3%) 등 수도권 비중이 전체의 54.0%에

달하며, 부산(피해발생 건수 기준 6.3%, 금액기준 6.0%), 경남(피해발생 건수 기준 6.1%, 금액 기준 5.5%) 順으로 대체로 거주인구수와 비례하여 발생하였다.

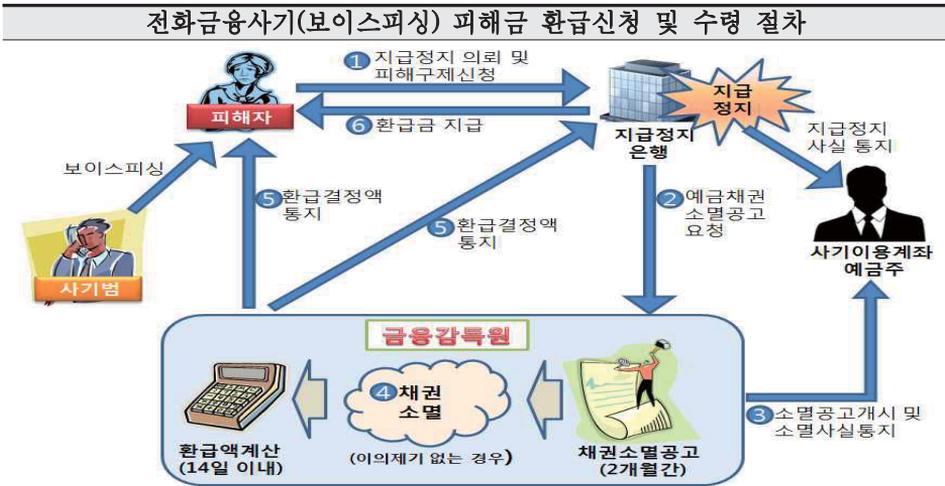
[표 4-14] 지역별 피해 현황



## 제2절 보이스피싱 피해방지 주요대책

### 1. 연도별 주요 대책

#### 1) 2011년도 주요 대책



자료: 금융감독원(2011), '11.9.30일부터 전화금융사기(보이스피싱) 피해금 환급제도 시행, 보도자료

#### 경찰 112센터를 통한 피해금 지급정지 처리절차 마련

- ① (전화금융사기 피해자) 피해사실 인지 후 112로 피해금 지급정지 신청
- ② (경찰청 112센터) 피해자 전화를 사기계좌 보유은행으로 연결 → 피해자가 피해금이 입금된 계좌와 은행을 알고 있는 경우
- ③ (경찰청 112센터) 피해자 전화를 피해자 거래은행으로 연결 → 피해자가 피해금이 입금된 계좌와 은행을 모르는 경우
- ④ (피해자 거래은행) 피해자의 피해금이 송금된 내역을 조회하여 금융회사간 전용라인을 통해 사기계좌 보유은행에 지급정지 의뢰



자료: 금융감독원·경찰청(2011), 경찰청 112센터를 통한 '보이스피싱 피해금 지급정지 신청제도' 실시지역 전국 확대, 보도자료 발췌

## 2) 2012년도 주요 대책

---

### 2012년도 보이스피싱 피해방지 주요 대책

---

#### 1. 보이스피싱 정책 협의회 구성

- 금융위, 방통위, 경찰청, 금감원 등으로 구성하여 매분기 정례회의를 개최하고, 보이스피싱 관련 정책을 총괄·조정하는 기능을 담당
- 협의회 참여기관 및 관련 민간기관 실무자급으로 「정책실무협의회」를 구성하여, 수립된 정책의 효과적 집행을 지원

#### 2. 대포통장 관련 통합관리시스템 구축

- 각 은행별 대포통장 의심계좌 정보와 모니터링 시나리오를 공유하여, 불법거래 의심계좌를 실시간 감시
- 보이스피싱 전담 수사팀을 운영하여 대포통장 매매를 단속하고, 적발 시 업징 제재

#### 3. 공인인증서 발급 및 사용절차 강화

- 공인인증서 재발급 및 1일 누적 기준 300만원이상 인터넷뱅킹을 통한 자금이체시 본인 확인절차를 강화

#### 4. 이체금액 인출제한

- 계좌간 이체금액이 300만원 이상인 경우, 입금된지 10분후에 인출을 허용

#### 5. 카드론 취급 강화

- 카드론 대출 승인시, 휴대폰 SMS로 본인에게 대출승인을 안내하고 이후 2시간 후에 입금
- 카드론 대출은 통장 입금내역에 카드론임을 명기
- 신용카드·카드론간 신청절차 별도 분리
- ARS를 통한 카드론 원칙적 금지

#### 6. 발신번호 변작 제한

- 발신번호가 조작된 전화를 차단하고, 국제전화 여부에 대한 표시를 의무화
- 공공기관의 전화번호 DB를 구축하고, 해외 유입전화에 대한 필터링을 통해 발신번호가 공공기관으로 변작된 경우는 차단

#### 7. 보이스피싱 전담수사팀 구성

- 「전화금융사기 전담수사팀」 설치·운영
- 한·중 경찰간 핫라인을 구축하여 해외 소재 사기범 검거를 위해 피의자 정보를 공유하는 등 공조수사 체계 마련
- 국내 수사 과정에서 드러난 해외 조직에 대해서는 중국 공안·대만 경찰의 강력한 수사 및 검거활동 요청

#### 8. 피해자 지원

- 「전기통신사기 피해금 환급에 관한 특별법」 개정을 통해 피싱 사기 방지를 위한 금융회사의 책임을 강화
- 보이스피싱 피해 관련 대출·연체로 인한 개인신용평점 산정 등 금융거래상의 불이익 최소화

#### 9. 교육 및 홍보 강화

- 공중파 TV 등 취약계층에의 노출 빈도가 높은 매체를 활용하여 피해예방 요령, 구제 방법 등을 집중 홍보
- 납치·사고를 가장한 사기피해가 빈발하는 학생·군인 및 부모를 대상으로 주기적인 사례교육을 실시
- 보이스피싱 포털사이트(가칭: Phishing Stop)를 구축하여, 주요 피해유형 및 대처방안 등의 정보에 대한 접근성 제고

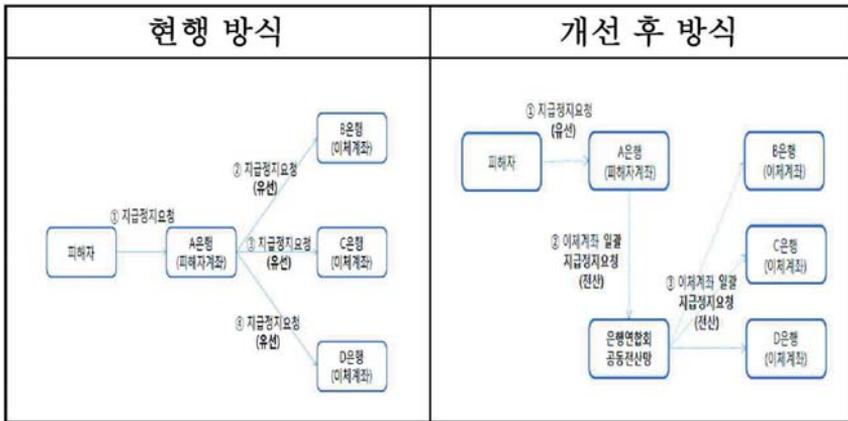
---

자료: 금융감독원(2012a), 금융소비자 보호를 위한 보이스피싱 피해방지 종합대책, 보도자료

### 3) 2015년도 주요 대책

#### 2015년도 보이스피싱 등 금융사기 척결 특별대책

1. 대포통장 근절을 통한 범죄자금 이동루트 선제적 차단
  - 금융권의 예금계좌 발급절차가 강화되면서 기존 정상발급된 예금계좌가 대포통장으로 불법 유통·활용되는 사례 증가
  - 장기 미사용 계좌의 비대면 거래(텔레뱅킹, 인터넷뱅킹 등) 제한(고객의 요청시 해제)을 확대
2. 대포통장 신고 포상금 제도 시행
  - ‘전자통신금융사기 특별법’ 개정(' 14.7월)에 따라 금융사기 의심계좌 신고 포상금 제도(건당 10~50만원)를 도입
  - 보험회사들도 자사 고객들의 예금계좌가 대포통장으로 활용되는 것을 방지하기 위하여 자율적으로 포상금 제도를 운영토록 유도
3. 대포통장 발급·유통 협조자에 대한 처벌 강화
  - 연 2회 이상 대포통장 명의자로 은행연합회에 등록되거나 대포통장임을 알고도 중개·알선 하는 등 대포통장 발급·유통에 협조한 자를 수사기관에 통보하고, 금융질서 문란자로 등록
  - 대포통장 광고 이용 전화번호 신속 정지제도 도입 추진
  - 통장개설 사실 통지 의무화
4. 금융회사간 피해자금 신속지급정지제도 시행



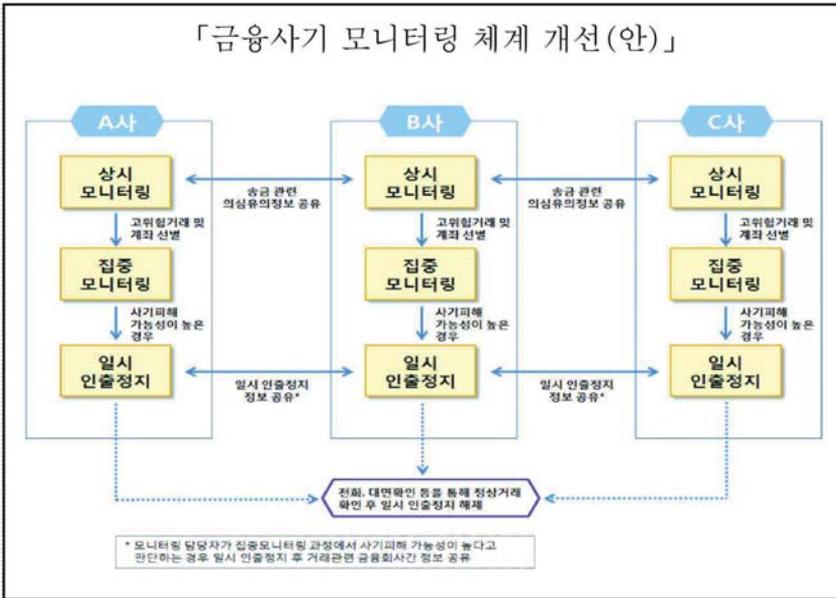
5. 지연 이체·인출 제도의 실효성 제고
  - 지연인출 시간을 확대(현행 3백만원 이상 이체시 10분)하고 일정금액 이상 인출시에도 추가 본인 인증을 적용
  - ‘新계좌지정서비스(안심통장서비스)’ 를 활성화
  - \* 新계좌지정서비스(안심통장서비스) : 고객이 사전에 지정한 계좌에 대해서는 사전에 정한 이체한도 범위내에서 자유로운 이체가 가능하고, 미지정 계좌에 대해서는 최대 1백만원(1일 누적기준) 한도 내에서만 이체가 가능
  - 지연이체 신청제도 시행: 고객이 원할 경우 이체의 효력을 일정시간 지연할 수 있는 제도로 전자금융거래법(제13조) 개정에 따라 ' 15.10.16 시행

6. 본인확인을 위한 전화번호 등록·변경 절차 강화

7. 텔레뱅킹 채널 보안성 강화

- 텔레뱅킹의 특수성을 반영한 「텔레뱅킹 전자금융사기예방서비스 가이드라인」 마련·시행:  
 ①전화 계좌잔액조회 서비스에 대해 OTP 등의 추가 인증, ②텔레뱅킹 거래시 인증수단(OTP 등)의 안전성 수준에 따라 이체 한도 차등 적용 유도 등

8. 금융회사간 의심거래 정보 상호 공유 추진



5. 지연 이체·인출 제도의 실효성 제고

- 지연인출 시간을 확대(현행 3백만원 이상 이체시 10분)하고 일정금액 이상 인출시에도 추가 본인 인증을 적용
- ‘新계좌지정서비스(안심통장서비스)’ 를 활성화
- \* 新계좌지정서비스(안심통장서비스) : 고객이 사전에 지정한 계좌에 대해서는 사전에 정한 이체한도 범위내에서 자유로운 이체가 가능하고, 미지정 계좌에 대해서는 최대 1백만원(1일 누적기준) 한도 내에서만 이체가 가능
- 지연이체 신청제도 시행: 고객이 원할 경우 이체의 효력을 일정시간 지연할 수 있는 제도로 전자금융거래법(제13조) 개정에 따라’ 15.10.16 시행

자료: 금융감독원(2015a), 보이스피싱 등 금융사기 척결 특별대책, 보도자료

#### 4) 2016년도 주요 대책

대책명	시기	추진 내용
금융질서문란행위자 제도 시행	16.3	대포통장을 거래하거나 대출사기 등을 저지르면 금융질서문란행위자로 등록(최장 12년간 금융거래불이익)
경찰청 등과 금융범죄 척결 업무협약(MOU) 체결	16.3	경찰청 및 금융권과 금융범죄 척결을 위한 업무협약 체결
“바로 이 목소리” 공개	16.5	국립과학수사연구원과 협업을 통해 반복 신고된 사기범의 “바로 이 목소리” 공개
안심금융생활 국민네트워크 출범	16.6	각계각층을 대표하는 10개 단체와 함께 불법금융 척결을 위한 “안심금융생활 국민네트워크 출범”
드라마 “38 사기동대” 와 함께 보이스포싱 피해예방 활동 전개	16.6	제3화(' 16.6.24.)에서 보이스포싱 사례를 소재로 방영하고, 드라마 홈페이지에 우리원 “보이스포싱 지킴이” 홈페이지 배너를 게재
전화번호 이용중지제도 시행	16.7	보이스포싱 및 대포통장 매매에 사용된 전화번호를 다양한 채널로 신고 받아, 미래부를 통해 원천 차단
보이스포싱 피해예방 10계명 홍보	16.8	보이스포싱 피해예방을 위한 10계명을 포스터, 스티커 등으로 제작하여 지자체, 국방부, 교육청 등 주요기관 및 시민단체에 배포
'남아 그 말을 믿지 마오' 보이스포싱 예방 연극 공연	16.9	수도권 노인복지관 등에서 총 15회에 걸쳐 노년층이 많이 당하는 보이스포싱 피해사례를 연극 형식으로 흥미 있게 전달하여 예방요령을 자연스럽게 습득하도록 유도
금융회사 피해예방 기여 우수직원 감사장 수여	16.10	2016 상반기중 보이스포싱 피해예방에 기여한 금융회사 우수직원(12명)에 감사장 수여
YTN라디오와 금융사기 피해예방 업무협약(MOU) 체결	16.10	·보이스포싱 등 금융사기 피해예방 홍보강화를 위해 YTN라디오와 업무협약을 체결하고 공동캠페인 실시

대책명	시기	추진 내용
보이스피싱 피해예방 10계명 은행 현금봉투 배포	16.10	보이스피싱 피해예방 10계명을 은행권 현금봉투에 인쇄하여 영업점에 배포
후후앤컴퍼니와 보이스피싱 예방 업무협약(MOU) 체결	16.11	후후앤컴퍼니와 보이스피싱 예방 공동 추진을 위한 업무협약 체결
햇살론 사칭 대출사기 피해예방 강화	16.11	최근 햇살론 등 서민정책자금을 사칭한 보이스피싱이 증가하고 있어, 각 금융회사 등 송금채널, 서민금융통합지원센터 등을 통해 피해사례를 전파하고, 유의사항 안내 강화
“보이스피싱 안 속는다 전해라~” 캠페인 송 배포	16.11	가요 “백세인생” (가수: 이해란)을 개사한 보이스피싱 예방 캠페인 송 “보이스피싱 안 속는다 전해라” 를 제작·공개
보이스피싱 피해예방 문자메시지 발송	16.5,9,12	방통위 및 이동통신사와 협력하여 보이스피싱 피해 예방을 위한 문자메시지를 대국민 발송
강릉시와 금융사기 예방 업무협약 체결	16.12	강릉시 업무협약을 체결하고 강릉시민의 금융사기 예방을 위한 상시 협력체계를 구축

자료: 금융감독원(2017a), '16년 보이스피싱 및 대포통장 큰 폭 감소, 보도자료 발췌

## 2. 5대 금융악 추방 대책 중 보이스포싱 분야 대책

### 1) 2017년도 중점 추진 특별대책<sup>14)</sup> 추진 목표



[그림 4-4] 중점추진대책(2017) 목표 및 전략

14) 금융감독원(2017), 민생보호 및 금융질서 확립을 위한 「5대 금융악 및 3유·3불 추방」 특별대책 관련 분야별 세부 이행과제

## 2) 보이스피싱 분야 세부 이행과제

관리코드	세부 이행 과제명	추진 시기
1-①	사기예방에 노력하는 금융회사 직원 등에 대한 인센티브 강화	
1-①-①	금융회사 영업점 직원 등 피해예방을 위해 기여한 직원 등을 포상	연중
1-②	선의의 사기이용계좌 명의인에 대한 구제절차 강화	
1-②-①	선의의 사기이용계좌 명의인 보호를 위한 ‘전기통신금융사기특별법’ 개정 추진	2/4 분기
1-③	금융회사의 사기피해 예방관련 시스템 구축	
1-③-①	피싱 조기경보시스템 구축	2/4 분기
1-④	한도계좌 보급 활성화 및 신규통장개설 관련 소비자 불편해소	
1-④-①	일정한 범위내에서 금융거래를 하는 한도제한계좌의 보급을 활성화하여 계좌개설 불편 해소 및 대포통장으로의 유용을 방지	연중
1-④-②	한도계좌 개설 이후 일정 기준에 맞는 경우 일반계좌로 전환해 주는 방안 등 강구	2/4 분기
1-⑤	사기의심거래에 대한 모니터링 능력 지속 강화	
1-⑤-①	금융회사간 정보공유를 활성화하여 피해자금의 인출을 신속히 차단	연중
1-⑤-②	FDS 정보공유시스템 등을 통한 상시모니터링	연중
1-⑥	대포통장 광고 전화번호 이용중지제도 운영방안 마련	
1-⑥-①	대포통장 광고 이용 전화번호 이용중지 요청	연중
1-⑦	대포통장 근절을 위한 점검 강화	
1-⑦-①	대포통장 과다발생 금융회사에 대한 이행실태 점검 강화	연중
1-⑦-②	대포통장 거래시 금융질서문란자로 등록되어 금융거래상 불이익을 받음을 적극 홍보	연중
1-⑧	사이버 도박자금 회수 목적 등 허위 신고자에 대한 조치 강화	
1-⑧-①	금융회사에서 모니터링 및 수사의뢰 등 허위신고자에 대한 강력조치	2/4 분기

주 : 본 과제의 주관부서는 불법금융대응단이며, 1-5-2 과제만 IT·금융정보보호단이 주관함

## 제3절 해외 주요국의 사례

### 1. 주요국 보이스피싱 현황

금융감독원에서 발간하고 있는 보고서에 따르면 일본·중국·미국은 대규모 개인정보 유출 사태가 없었음에도 보이스피싱 등 금융사기 피해가 증가하는 추세를 보이고 있다고 한다. IT기술의 발전, 비대면 거래 증가 등과 함께 범죄가 지능화·조직화 되면서 전세계적으로 금융사기 피해가 확대되고 있으며 우리나라도 그 영향권 내에 있는 것으로 보인다. 본 절에서는 금융감독원에서 내놓은 주요국 피해현황 자료를 정리하여 본다.

#### 1) 일본

일본은 '04년 보이스피싱이 처음 발생한 후 '08년 정점에 이른 후 '11년까지 감소했으나 '12년부터 다시 증가세로 전환되었다. 특히, '14년 피해규모(11,257건, 376억엔)는 전년(9,204건, 259억엔) 대비 크게 증가(건수기준 22.3%↑, 금액기준 45.2%↑)하였다.

[표 4-15] 일본의 보이스피싱 발생 추이

(단위 : 건, 억엔)

2008년		2011년		2012년		2013년		2014년	
건수	금액	건수	금액	건수	금액	건수	금액	건수	금액
20,481	276	6,233	127	6,384	160	9,204	259	11,257	376

자료: 일본 경찰청(보이스피싱 기준)

## 2) 중국

중국은 공안당국 추정에 의하면 '14년 피해규모(51만건, 212억위안)가 전년(30만건, 100억위안) 대비 크게 증가(건수기준 70%, 금액기준 112%)한 것으로 나타났다.

**[표 4-16] 중국의 보이스피싱 발생 추이**

(단위 : 건, 억엔)

2011		2012		2013		2014	
건수	금액	건수	금액	건수	금액	건수	금액
10	40	17	80	30	100	51	212

자료: 중국 공안부(2014년은 추정자료)

## 3) 미국

미국은 금융 신원도용(Identity Fraud)<sup>15)</sup>으로 인한 피해가 지속되고 있으며 매 2초마다 새로운 피해자가 발행하고 미국 가정의 7.5%가 피해를 입고 있다는 조사결과가 있다.

**[표 4-17] 일본의 보이스피싱 발생 추이**

(단위 : 만명, 억달러)

2010		2011		2012		2013		2014	
피해자	피해액								
1,020	200	1,160	180	1,260	209	1,310	180	1,270	160

자료: Javelin Strategy and Research, 2015 IDENTITY FRAUD REPORT

15) 타인의 신원을 도용하여 대출, 신용카드 등 새로운 계정을 생성하는 신규계정사기(New Account Fraud)와 타인 명의 기존 계정을 탈취하여 자금이체·현금 인출 등을 수행하는 계정탈취사기(Account Takeover Fraud)가 많음(피싱사기와 유사)

## 2. 해외 보이스포싱의 특징 및 시사점

### 1) 일본·중국의 피해유형은 우리나라와 유사

2003년 대만에서 큰 사회적 물의를 일으킨 보이스포싱 범죄는 2004년 일본에서 발생한 후 2006년 우리나라에서 처음 발생하였다. 같은 아시아권 국가인 일본·중국은 국가기관 등을 사칭하여 돈을 편취하는 등 피해유형이 우리나라와 거의 유사한 것으로 파악된다.

주요 피해유형을 살펴보면 ① 국가기관(전화국, 수사기관, 국세청 등)이나 친·인척 등 지인을 사칭하여 금융범죄 연루, 자녀납치, 교통사고 합의금 등을 명목으로 돈을 이체시켜 편취하는 사기, ② 대출을 빙자하여 보증금 등의 명목으로 돈을 이체시켜 편취하는 사기, ③ 국세청 등을 사칭하여 환급금 등에 필요한 절차를 가장하거나 가공의 요금 청구를 구실로 돈을 편취하는 사기 등이 있다. (이 중 일본에서 발생하는 ①번 유형의 사기를 ‘오레오레 사기’(オレオレ)로 칭하는 데, 손자나 아들의 교통사고 합의금 등이 필요하다는 전화를 걸 때 부모들 속이기 위해 사기꾼이 “オレオレ(저예요!)”라는 말로 전화를 시작하는 것에서 유래하였다.)

### 2) 직접 찾아가 현금을 건네받는 현금수취형 피해 급증

최근 일본의 경우 피해자금 편취방식이 돈을 대포통장으로 돈을 이체시켜 인출하는 ‘이체형’ 대신, 피해자를 직접 찾아가 돈 또는 현금카드를 건네받는 ‘현금수취형’<sup>16)</sup>이 최근 급증하고 있다.

이는 대포통장에 대한 단속 강화, ATM 인출한도 하향, 금융회사의 피해 예방 노력 등으로 인한 풍선효과로 추정되고 있다.

---

16) 현금수취형(‘오레오레 사기’ 기준) : (‘11년) 48% → (‘14년) 90%

## 일본의 현금수취형 피해사례

### □ 집을 찾아가 직접 현금을 받아온 사례

- ▶ 전화번호부, 졸업생 명부 등 각종 명부를 기초로 자녀 또는 친척을 가장하여 부모님이나 형제자매에게 전화를 걸어 “휴대전화 번호가 바꿨다”, “회사 휴대전화이니 등록해 두어라” 라고 말하고 사기범 조직의 연락처로 전화를 유도함
- ▶ 이 후 “지하철에서 회사돈이 든 가방을 잃어버렸다”, “여자친구를 임신시켰다”, “회사돈을 사용해 버렸다”, “감사에 걸려 해고당했다”, “친구에게 보증을 섰다”, “주식투자에 실패했다” 등 어려움을 당하고 있다고 호소함
- ▶ 그리고 “집까지 받으러 갈테니 돈을 준비해 달라. 자신을 갈 수 없으니 동료를 보내겠다” 라고 말하고 현금수취 역할의 조직원을 보내 돈을 직접 받아옴

우리나라도 최근 대포통장 단속, ATM 인출한도 하향 등 대응조치가 강화되어 현금수취형(방문형) 피해사례<sup>17)</sup>가 심화될 가능성이 높으므로 국민들의 인식수준 제고를 위한 대국민 홍보활동 등 선제적 대응이 필요한 것으로 판단된다.

### 3) 보다 안전한 금융거래 환경 조성에 노력

해외 주요국은 계좌개설시 철저한 신원확인 뿐만 아니라 운전면허증 등 신분증에 기재된 주소와 현거주지가 다른 경우 거주지 증명서류(전기·가스요금 고지서 등)를 요구(미국·영국·일본·홍콩)하고 있다.

현금카드의 경우 1~2주일 후 자택으로 우편발송(일본) 또는 약 2주간 사용 가능한 임시 직불카드와 임시수표가 발행되고 7~10일 후 우편으로 정식

17) (최근 피해사례) ①독거노인 등을 대상으로 금감원 직원을 사칭하여 “계좌정보가 노출되어 안전조치가 필요하다” 며 현금을 직접 찾아오도록 하여 편취. ② 보이스피싱 우려가 있다며 속여 돈을 장롱·냉장고 또는 지하철 물품보관함 등에 보관하게 한 뒤 편취

직불카드와 수표가 배송(미국)되는 경우가 있으며 계좌에 일정금액 이상 잔액을 유지하지 않으면 ‘계좌유지 수수료’가 부과(미국·홍콩)되기도 하고, 계좌개설을 위해 사전 인터뷰 예약을 해야 하고 인터뷰까지 평균 1주일 대기(영국)하는 등 관련 절차가 매우 까다롭다.

〈일본 미쓰이스미토모은행의 계좌개설 신청 고객에 대한 안내문(발췌)〉

- 일본 내 주재중인 개인 고객에 한해 개설이 가능합니다.
- 예금계좌가 범죄에 이용되는 사태가 사회문제화되어 있기 때문에 가족 계좌를 포함하여 단기간에 복수의 계좌를 신청하는 등 당 행 소정의 조건에 해당되는 경우 계좌 개설을 거절하는 경우가 있습니다
- 계좌 개설 희망지점은 원칙적으로 자택 또는 근무지와 가까운 지점을 택해 주십시오. 소재지와 먼 지점을 희망하는 경우에는 이용목적을 여쭙볼 수 있습니다. 경우에 따라서는 계좌 개설을 거절할 수 있으니 주의해 주십시오.

또한, 타행이체시 당일 이체되지 않거나(미국·독일) 평일 15시 이전에 이체한 경우에 한해 당일 이체가 가능(일본)하는 등 자금이체가 실시간을 기반으로 하지 않는 사례가 많다.

우리나라는 상대적으로 IT의 발전이 빨라서 신속·편리함 중심으로 금융 거래환경이 형성·발전하였고, 금융서비스에 있어서 국민들이 신속함을 요구하고 있어 금융사기에 상대적으로 취약한 측면이 있다.

국민들 누구나 금융사기 피해자가 될 수 있다는 생각으로 다소간의 불편함을 감수하더라도 신속·편리함과 금융안전 간 조화로운 균형점을 찾기 위한 사회적 공감대 확산이 필요한 시점이다.

#### 4) 대포폰 등 주요 범죄수단 신속 차단

해외에서도 금융사기범의 주요 범죄수단인 대포통장, 대포폰 등에 대해 민관이 협력하여 공동 대응하고 있다.

특히, 일본은 대포통장 뿐만 아니라 대포폰에 대해서도 강력대응하고 있는데 일본경찰청은 보이스피싱 신고를 받은 대포폰의 동일번호가 다시 보이스피싱에 사용되는 것을 방지하기 위해 이동 통신사업자에게 계약자 확인을 요청하고 이동통신사업자는 계약자에게 본인 확인을 요구하여 해당 계약자가 이에 응하지 아니하면 서비스 제공을 거절한다.

이러한 사례에서 시사하는 바는 휴대전화 발급 시 본인확인 절차를 보다 강화하고 금융사기에 이용된 대포폰의 신속정지 체계 구축이 요구된다.

## 5) 범정부 차원 공동대응 및 민간부문 적극 참여

미국·일본·중국은 수사당국(경찰청 등) 주도하에 금융당국 등 범정부 차원에서 공동대응하고 있다. 또한 민간부문은 은행 등 금융회사 이외에도 인터넷포탈사업자, 이동통신사업자, 민간보안회사, 대학연구소 등이 피해예방 홍보활동에 적극 참여하고 있다.

우리나라에서는 민간부문의 경우 주로 금융회사를 중심으로 협력하고 있어서, 인터넷포탈(네이버 등), 이동통신사업자(SKT 등) 등 여타 민간부문의 참여 확대를 유도할 필요가 있다.

## 6) 금융소비자도 피해예방에 스스로 노력할 책임 부담

미국·일본 등은 본인이 제3자에게 접근매체(통장, 현금카드, 공인인증서 등)를 제공하는 등 금융소비자에게 고의·중과실이 있는 경우 피해보상 시 금융회사의 책임을 면책(전부 또는 일부)하고 있다. 다만, 해외에서는 신속한 배상절차 진행을 제도화하고 금융회사에게 고객의 고의·중과실을 입증토록 하는 등 소비자 보호장치를 두고 있다.

우리나라 금융이용자들도 금융사기로부터 자신의 금융재산을 보호하기 위해 스스로 안전조치를 강화하는 한편, 금융사기에 반사적으로 저항할 수 있는 인식 수준 제고가 필요하다.

## 제4절 국내 · 외 지자체 대응 동향

### 1. 일본 지자체의 보이스피싱 예방노력

일본의 보이스피싱 단속활동은 경찰청이 주관하고 있으나 각 지자체도 지역 내 경찰서, 금융회사, 시민단체 등과 협력하여 지역주민 대상 피해예방 홍보활동을 적극 운영하고 있다.<sup>18)</sup>

일본 경찰청에서는 피해발생현황과 사기유형별 정보제공을 하고 있다. 물론 예방을 위해서도 관련 다양한 정보를 제공하고 있다. 전화금융사기 순서에 따른 내용들과 실제 과거범인들의 목소리를 들을 수 있도록 HP에 탑재하고 있다.

상담창구도 각 현경찰본부에 직접 메일을 통해 할 수도 있게 하고, 전화상담은 전국공통의 #9110<sup>19)</sup>으로 통일시켜 놓고 있기도 하고 각 경찰본부 별로도 상담전화를 운영하고 있다. 또한 지능범죄(사기담당) 담당부서와 폭력단 담당부서의 연계수사를 통해 범죄조직 척결 차원에서의 강력한 보이스피싱 단속활동을 실시중이며, 2016년 4월 보이스피싱 등 특수사기 척결을 위해 지방경찰관 약 160명을 증원하였다.

일본의 보이스피싱 단속활동은 경찰청이 주관하고 있으나 각 지자체도 지역내 경찰서, 금융회사, 시민단체 등과 협력하여 지역주민을 대상으로 한 피해예방 홍보활동을 적극 운영중에 있다.

특히, 전체 47개 도도부현(광역지자체) 중 3개현에서는 「보이스피싱 피해방지 조례」를 제정하여 시행중인데 쿠마모토현(2009.4.1. 시행), 오카야마현(2010.4.1. 시행), 토쿠시마현(2014.4.1. 시행) 등이 이에 해당하고, 또한, 기초지자체 중에서도 카시와市(치바현)가 전국 최초로 조례를 제정하여 시행(2016.4.1.)하고 있다.

18) 금융감독원, 일본의 보이스피싱 예방노력 및 시사점

19) 우리나라 110 정부민원안내콜센터와 유사

# 현민을 보이스피싱 피해로부터 지켜주는 조력자의 개토

## < 목 적 >

보이스피싱 사기 피해를 급증하여 사회문제가 됨에 따라 보이스피싱 피해 방지를 위해서 현·현민 및 사업자의 책무를 명확히 하는 보이스피싱 사기 방지조치를 강구하여 현민의 재산을 보호함을 목적으로 한다.

## 구미모토 현

경찰본부

지사무국(행정담당국)

- 통보
- ① 피해를 당했거나 피해를 우려가 있는 사람을 발견한 경우
  - ② 본인이나 친족이 의심스러운 전화, 우편물 등을 받은 경우

- 보이스피싱 피해 방지에 관한 종합적인 시책의 추진
- 현민의 관심을 높이고 이해체고를 위한 홍보 활동 및 계몽 활동
- 피해 방지에 관한 자주적인 활동을 촉진하기 위한 인제 육성
- 현민 등 상호간에 정보와 의견 교환을 할 수 있는 기회의 설치
- 시정촌에 대한 발생현황 및 기타 피해방지에 유용한 정보 제공
- 피해 방지에 관한 자주적인 활동을 지원하기 위한 정보제공, 조언 및 기타 조치
- 현민 등으로부터 피해통보를 받은 경우의 조치

- 통보
- ① 현민에서 피해통보를 받은 경우
  - ② 보이스피싱 피해를 당했거나 피해를 우려가 있는, 또는 사기 행위를 하고 있다고 의심이 되는자를 발견 한 경우

### 현민

"본인이나 친족이 피해를 당하지 않도록 노력할 것"  
 "현이 실시하는 피해 방지 노력에 협력 할 수 있도록 노력할 것"

### ATM 이용시 유의사항

- 변경하는 등 고의로 이용자가 판별되지 않도록 하여 ATM을 조작하는 것
- ATM의 조작에 있어 타인의 지시 또는 연막을 기다리는 등 장시간에 걸쳐 ATM을 정거하는 것
- 다수의 저축 통장 또는 현금 카드를 사용하여 장기간 또는 반복하여 ATM을 조작하는 것
- 휴대전화 및 기타 휴대용 무선 통신기를 사용하면서 ATM을 조작하는 것



(운영상 유의사항) 현민과 현 체류자의 자유와 권리를 부당하게 제한하지 않도록 유의

### 사업자

- 은행, 신용 금고 등의 금융 기관 · 백화점 등
- ATM을 설치하고 있는 편의점 · 배화점 등
- 태배 등 운송사업을 영위하는 사람
- 휴대전화 판매사업자, 임대업자 등
- 기타 보이스피싱 사기 범행행태에 비추어 보이스피싱 피해방지에 긴급히 조치가 필요하다고 공안위원회가 정하는 것

※ 시행 후 3년 후 검토한 다음 필요한 조치를 취한다.

[그림 4-5] 일본 구미모토현의 보이스피싱 조례 개요

## [표 4-18] 쿠마모토현의 보이스피싱 피해방지 조례

피해방지 조례 주요 내용(쿠마모토현)
<ul style="list-style-type: none"><li>• 기초지자체가 보이스피싱 사기 예방대책을 시행하는 경우 협력·지원</li><li>• 보이스피싱 피해방지를 위한 홍보활동</li><li>• 정상거래시 보이스피싱 사기의심을 피하기 위한 유의사항 등의 정보 제공</li><li>• 경찰의 보이스피싱 발생상황, 사기방지 체크리스트 등 제공</li></ul>

## [표 4-19] 카시와시의 보이스피싱 예방 주요 활동

카시와시의 보이스피싱 예방 주요 활동
<ul style="list-style-type: none"><li>• 보이스피싱 대책검토회의, 대책본부 및 피해자 지원종합창구 설치<ul style="list-style-type: none"><li>- 보이스피싱 피해자의 정신적 충격 조기회복을 위한 보건의료·복지서비스 제공</li></ul></li><li>• 카시와시, 시민 및 사업자에게 보이스피싱 예방 의무 부과</li><li>• 보이스피싱 예방전화기 구입비 지원 : 65세 이상, 50% 보조(최대 1만엔)</li><li>• 민관협력 홍보활동<ul style="list-style-type: none"><li>- 마을회관, 금융회사 객장에 홍보포스터 부착 및 예방강좌 실시</li><li>- 시민단체 공동 예방교육 및 홍보 실시</li><li>- 사기발생지역 신속한 순찰 및 마을별 보이스피싱 발생지도 작성·배포 등</li></ul></li></ul>

일본의 보이스피싱 예방의 시사점을 살펴보면 ①금융범죄의 숙주중 하나인 대포폰에 대한 강력한 단속, ②지역내 택배, 편의점, 부동산중개업자 등의 예방활동 협력, ③금융청 및 전국은행협회 등 금융부문도 예방활동 적극 동참, ④국민들과 가장 접점에 있는 지자체의 활발한 예방활동, ⑤피해자의 정신적 충격까지 살피는 세심한 지원 대책, ⑥정보취약계층 대상 맞춤형 대책을 마련하고 있다는 것이다.

우리나라도 보이스피싱 피해예방을 위해서는 민·관의 다양한 조직이 적극 참여해야 하며, 앞으로는 주민의 생활에 밀접하게 관여하고 있는 지자체의 관심(조례제정, 맞춤형 대책 등)이 더욱 요구되어 진다고 할 수 있다.

## 2. 국내 지자체 협력 사례

### 1) 강릉시 금감원 업무협약 체결 사례

강릉시와 금융감독원은 2016년 12월 업무협약을 체결하고 강릉시민의 금융사기 예방을 위한 상시 협력체계를 구축하였다. 업무협약의 주요 내용을 살펴보면, 강릉시 홈페이지를 활용한 예방콘텐츠 게시, 신·변종 사기수법의 신속한 전파, 지역금융회사 등과의 협업을 통한 정보취약계층 대상 맞춤형 홍보, 조례제정 등으로 구성되어 있다.

#### [표 4-20] 강릉시-금감원 업무협약 주요 내용

강릉시-금감원 업무협약 주요 내용
제2조(협력사항) 본 협약에 의하여 상호 수행해야 할 업무범위는 다음과 같다.
1. 홈페이지 상호 연계를 통해 강릉시민에 대한 신·변종 피해사례 및 예방법, 구제신청절차 등 홍보
2. 신·변종 사기수법 발생시 지역주민센터, 마을이장, 아파트관리사무소 등을 통한 신속 전파
3. 지역금융회사 등과 협업하여 고령층 등 정보취약계층 대상 맞춤형 홍보 실시
4. (가칭)「강릉시민의 금융사기 예방을 위한 조례」의 제정을 위한 공동 노력

한편, 강릉시는 전국 226개 기초지자체의 협력단체인 ‘전국시장군수구청장협의회’ 회장지자체로서 향후 강릉시의 모범사례를 여타 지자체로도 확산하여 예방 홍보체계를 전국적으로 확충해 나갈 예정으로 알려졌다.

### 2) 서울시, 금감원 및 시중은행과 업무협약 체결

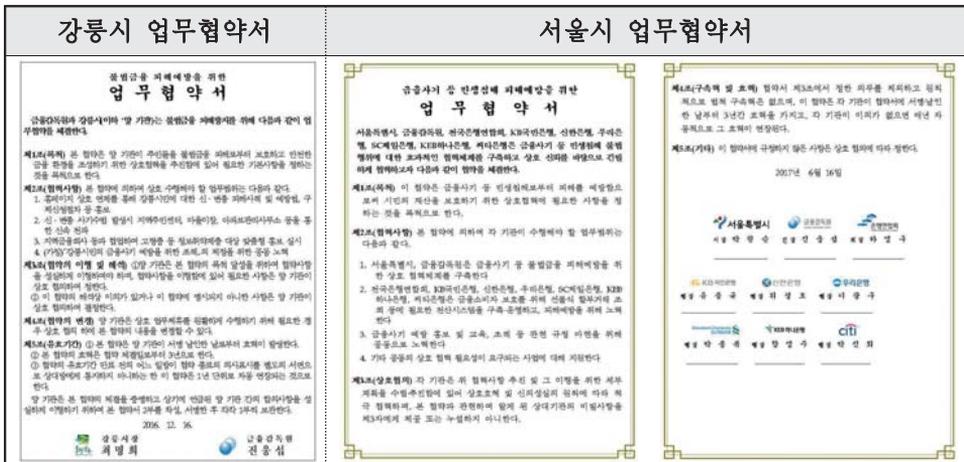
서울시는 금융감독원 및 6개 주요 시중은행(KB국민, 신한, 우리, SC제일, KEB하나, 씨티은행)과 「금융사기 등 민생침해 피해예방을 위한 업무협약」을 체결하고, 힘을 모아 불법 사금융, 보이스 피싱 등 금융사기 피해예방을 추진하

고 있다. 그 간 서울시는 금융감독원은 경찰청과 공동으로 ‘보이스피싱지킴이’ 사업 등을 추진해왔으나, 각 기관의 노력에도 불구하고 금융피해가 끊이지 않자, 서울시와 금융감독원, 시중 주요 은행이 함께 힘을 모으게 되었다.

업무협약의 주요 내용을 살펴보면 ‘보이스피싱 등 금융사기 피해예방을 위한 공조체제를 구축하여 적극 대응하고, 이를 위해 서울시·금융감독원·6대 시중은행이 각각 협력할 필요가 있다’ 라고 기술하고 있다. 또한 유관 사업 추진 근거 마련을 위한 조례제정을 위해 노력한다는 것을 골자로 하고 있다.

[표 4-21] 강릉시-금감원 업무협약 주요 내용

서울시 업무협약 주요 내용	
제2조(협력사항) 본 협약에 의하여 각 기관이 수행해야 할 업무범위는 다음과 같다.	
1. 서울특별시, 금융감독원은 금융사기 등 불법금융 피해예방을 위한 상호 협력체제를 구축한다.	
2. 전국은행연합회, KB국민은행, 신한은행, 우리은행, SC제일은행, KEB하나은행, 씨티은행은 금융소비자 보호를 위해 선불식 할부거래 조회 등에 필요한 전산시스템을 구축·운영하고, 피해예방을 위해 노력한다.	
3. 금융사기 예방 홍보 및 교육, 조례 등 관련 규정 마련을 위해 공동으로 노력한다.	
4. 기타 공동의 상호 협력 필요성이 요구되는 사업에 대해 지원한다.	



[그림 4-6] 국내지자체 협력 사례(업무협약서)

# 대전시 보이스피싱 예방 방안

1. 기본 방향
2. 보이스피싱 예방 대책 수립
3. 단계별 실행 방안

## 5장



# 제 5 장 대전시 보이스피싱 예방 방안

## 제1절 기본 방향

### 1. 보이스피싱 예방의 중요성

보이스피싱·불법사금융·유사수신 등 불법금융으로 인한 피해규모는 우리나라 GDP의 1.6%인 연간 27조원 수준으로 민생경제 및 지역사회에 심각한 피해를 끼치고 있다. 대전시의 보이스피싱 범죄는 연간 약 5백건 이상 발생(2014년 528건/2015년 517건)하고 있으며, 피해액은 처음으로 통계가 집계된 2009년에 15억원 수준에서 2016년 43억원으로 그 규모가 크게 확대되고 있다.

이러한 보이스피싱 피해는 미국·중국·일본 등 전세계적으로도 확대되는 추세이고, 특히 한국의 경우는 자금이체(송금) 환경이 매우 편리하여 보이스피싱이 범죄가 비교적 용이한 편이다. 또한, 최근 보이스피싱 수법이 첨단화·지능화됨에 따라 피해자는 부지불식간에 범죄의 표적이 되고 있는데, 보이스피싱은 개인정보를 필수적으로 탈취(도용)하기 때문에 한번 범죄의 표적이 되면 본인도 모르게 부가적인 금융사기에 휘말릴 가능성이 크다.

최근의 보이스피싱은 그 대상을 가리지 않고 오히려 사회적 약자의 약점을 이용하는 방법으로 악랄해지고 있다. 과거에는 공공기관을 사칭하여 노인을 대상으로 하는 유형의 범죄가 많았으나, 최근에는 돈이 필요한 서민에게 대출을 가장하여 범죄를 저지르고, 취업을 미끼로 청년들에게 접근하여 대포통장개설 및 금융사기를 시도하는 경향이 높아지고 있다. 특히, 보이스피싱 범죄조직은 중국 등 해외에서 저임금의 조직원(아르바이트)를 고용하여 범죄에 동원하기 때문에 이들은 별다른 죄의식 없이 범죄를 지속적으로 이어나간다.

이와 같이 보이스피싱 범죄는 단순히 일회성에 사기에 따른 피해자의 금전적 손실뿐만 아니라 개인정보 유출에 따른 후속범죄의 우려와 정신적 피해를 함께 유발하고 있어 심각한 범죄이며, 점조직으로 해외에서 운영되는 사례가 많아 근절이 어렵기 때문에 그 예방이 매우 중요하다.

## 2. 지자체 역할의 중요성 인식

보이스피싱 범죄는 전기통신수단을 사용하고, 비대면 특성을 가지고 있어 특정 지역에서 발생하지는 않는다. 그러나 그 피해는 피해자의 가정과 이웃 및 지역으로 귀속된다. 이에 따라 최근 보이스피싱 범죄 예방을 위한 지역사회 노력의 강화되고 있는 추세다.

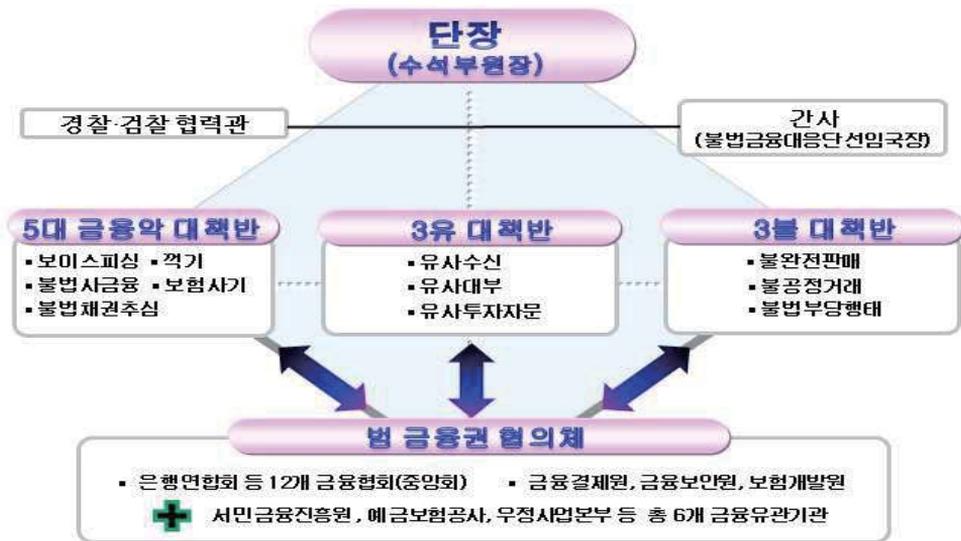
일본에서는 구마모토현, 오카야마현, 도쿠시마현 등 3개의 광역지자체가 보이스피싱 피해방지 조례를 제정해 주민과 지역민 상인의 자발적 예방 활동을 유도하고 있으며, 택배 사업자, 금융회사, 노인단체, 시민단체, 금융회사, 노인단체 등과 함께 민관합동으로 홍보 활동을 강화하고 있다.

우리나라에서도 지난해 12월 강릉시와 금감원이 “불법금융 피해예방을 위한 업무협약”을 체결하였고, 서울특별시도 금년 6월 금감원 및 시중6대 은행과 “금융사기 등 민생침해 피해예방을 위한 업무협약”을 체결하여 협약기관간 공조협력과 함께 조례제정을 추진하는 등 자체적인 보이스피싱 예방활동을 적극적으로 수행하고 있다.

대전시도 보이스피싱 피해예방을 위해 민·관을 망라한 다양한 부문의 적극적인 동참이 필요하며 특히 지역 주민과 가장 접점에 있는 지차체가 주민 보호에 주도적으로 나설 필요가 있다.

### 3. 보이сп피싱 예방을 위한 지자체의 대책 방향

국내의 보이сп피싱과 관련한 예방활동은 주로 금융감독원이 담당하고 그 대응은 주로 경찰 등 수사당국이 담당하고 있다. 또한, 금융당국은 민생침해 5대 금융악 척결 및 3유·3불 추방 범 금융권 협의체(불법금융 추방 범 금융권 협의체)를 구성·운영하고 있으며, 보이сп피싱 부문은 5대 금융악 분야에 해당하여 동 협의체에서 다양한 예방 대책을 추진하고 있다.



[그림 5-1] 불법금융 추방 범 금융권 협의체

보이сп피싱 관련 주무기관인 금융감독원은 2016년 4월 발표한 「5대 금융악 및 3유·3불 추방 특별대책」<sup>20)</sup>에서 공동대책의 일환으로 ‘지방자치단체 및 사회·시민단체의 역할 강화방안 마련’ 과제를 추진하고 있으며, 국민들과 최접점에 있는 지자체 및 사회·시민단체들이 불법금융 근절 및 피해예방 홍보에 주도적으로 참여하도록 유도하겠다는 대책을 수립하였다.

20) 금융감독원은 2016년 4월 기준 ‘5대 금융악 특별대책’을 「5대 금융악 및 3유·3불 추방 특별대책」으로 확대 개편

## [표 5-1] 지방자치단체 및 사회·시민단체의 역할 강화방안

---

- ① 지방자치단체의 보이스포싱 등 금융사기 예방을 위한 조례제정 유도
  - 서울시와 협력하여 조례제정을 유도하고 다른 지자체에도 확산
- ② 전국 지자체와 업무협약 체결 추진
  - 금감원과 강릉시 간 업무협약\* 모범사례를 전국 226개의 기초자치단체로 확산
  - \* 강릉시 홈페이지에 금융사기 예방 콘텐츠 게재, 신·변종 사기수법 확인시 주민안내방송을 통한 신속 전파, 지역금융회사 등과 협업하여 고령층 등 정보취약계층 대상 맞춤형 홍보활동 협력 등
- ③ 「안심금융생활 국민네트워크」 '17년 협업과제 선정·추진
  - 시민단체별 특성에 맞는 중점 교육·홍보사업 등을 마련·추진

※ (참고) '16년도 주요 협업 사업

- ▶ 대한노인회 : 맞춤형 교육 및 전국 경로당(6만여개)에 예방 스티커 부착 캠페인
  - ▶ 바르게살기운동중앙협의회 : 불법금융 신고모니터단 위촉활동 등
  - ▶ 한국여성단체협의회 : 전국여성대회( '16.11월)시 여성층 대상 집중홍보 실시
  - ▶ 중소기업중앙회 : 국내기업의 국제금융사기 피해예방 공동캠페인 실시
- 

대전시의 보이스포싱 예방 대책은 이러한 상급기관의 정책과 동조하고, 지역특성을 반영한 민관 협력 공조체계를 구성하여 유관정책을 수립해 나아가야 할 것이다.

## 제2절 보이스피싱 예방 대책 수립

### 1. 문제점 및 대응 방향

대전광역시가 효과적으로 보이스피싱을 예방하기 위한 분야별 주요이슈의 문제점과 필요성을 살펴보고, 이에 따른 대응방향은 다음의 [표 5-2]와 같이 정리할 수 있다.

[표 5-2] 대전시 보이스피싱 예방 및 대응 방향

주요 이슈	문제점 및 필요성	대응 방향
보이스피싱 대책 추진 근거 부재	<ul style="list-style-type: none"> <li>• 법 제도적 추진 근거 부재</li> <li>• 지자체(대전시) 주도적 대책 추진을 위한 조례 제정 필요</li> </ul>	<ul style="list-style-type: none"> <li>• 대전광역시 보이스피싱 및 금융사기 피해 감소를 위한 조례(가칭) 제정 추진</li> </ul>
	<ul style="list-style-type: none"> <li>• 민관 협력 협의 기구 부재</li> <li>• 보이스피싱 관련 유관기관 및 시민이 참여하는 협의체 구성 필요</li> </ul>	<ul style="list-style-type: none"> <li>• 유관 정책(예방 및 대응 정책) 기획·조정·의결 기능의 민관협의체 구성 및 운영</li> </ul>
	<ul style="list-style-type: none"> <li>• 중장기계획 부재</li> <li>• 체계적인 사업 추진을 위한 중장기계획 수립 필요</li> </ul>	<ul style="list-style-type: none"> <li>• 대전시 지역특성을 반영한 맞춤형 중장기계획 수립 및 시행</li> </ul>
실무 대응 역량 미흡	<ul style="list-style-type: none"> <li>• 신변중 보이스 피싱 발생에 대한 신속한 대응 필요</li> </ul>	<ul style="list-style-type: none"> <li>• 모니터링 및 신속한 상황 전파 체계 확립</li> </ul>
	<ul style="list-style-type: none"> <li>• 민간 자율 활동 지원 및 활성화 필요</li> </ul>	<ul style="list-style-type: none"> <li>• 금융기관 및 민간단체 실무대응 활동 지원 방안 마련</li> </ul>
	<ul style="list-style-type: none"> <li>• 금융사기 대응 유관기관 간 공조 협력체계 구축 필요</li> </ul>	<ul style="list-style-type: none"> <li>• 금감원 업무협약 추진 등 관계기관 협업 및 공조 강화</li> </ul>
실행 방안 마련 필요	<ul style="list-style-type: none"> <li>• 보이스피싱 원인 제거 및 출구 봉쇄를 통한 사전 예방 대책 필요</li> </ul>	<ul style="list-style-type: none"> <li>• 개인정보보호 및 대포통장 근절 대책 수립 및 시행</li> </ul>
	<ul style="list-style-type: none"> <li>• 정부당국 및 산하기관의 개별적 산발적인 교육·홍보로 예방 효과를 저하</li> </ul>	<ul style="list-style-type: none"> <li>• 연령별/계층별 맞춤형 교육·홍보를 확대하고, 유관기관 공조·연계 사업 확대</li> </ul>
	<ul style="list-style-type: none"> <li>• 시민참여 증진을 통한 예방 능력 강화 및 사업 확산을 위한 다양한 대책 강구 필요</li> </ul>	<ul style="list-style-type: none"> <li>• 시민 참여 증진 및 범업을 위한 단계별 예방활동 지원 대책 마련 및 시행</li> </ul>

## 2. 추진 목표 및 중점과제 도출

효과적이고 체계적으로 보이스피싱을 예방하기 위해서는 보이스피싱 및 금융사기 예방을 위한 조례제정 등 추진 기반을 구축하고, 유관기관과의 공조 협력을 강화하는 등 실무역량을 강화해야 하며, 교육 홍보 및 시민참여 증진을 위한 다양한 단계별 대책을 수립하고 시행하여야 한다.

이에 따라 대전 시민 모두가 보이스피싱의 피해 걱정 없이 살 수 있는 안전한 사회구현을 본 대책의 비전으로 설정하고, 보이스피싱 근절 대책 수립 및 시행을 추진 목표로 설정하였다.

또한 중점 추진과제는 단계별로 수립 시행하며 앞서 살펴본 문제점 및 대응방향의 주요 내용을 구조화 하여 다음의 그림과 같이 3대 분야 12개의 과제를 도출 하였다.



[그림 5-2] 추진목표 및 중점과제

### 3. 중점과제 및 분야별 추진 방안

앞서 도출된 3대 분야 12대 중점추진과제별로 세부적인 추진 방안은 다음과 같이 요약할 수 있다.

[표 5-3] 대전시 보이스피싱 예방 대책

추진단계	중점 과제	추진 방안	추진 시기
기반 구축	조례제정	<ul style="list-style-type: none"> <li>지자체 주도 실무 추진 법적 근거 마련</li> <li>지자체 예방활동 범위 및 의무사항 규정</li> <li>사업추진 예산 및 조직 관련 사항 규정</li> </ul>	초기 ~ 중기
	민관협의체 구성	<ul style="list-style-type: none"> <li>예방 및 대응 정책 기획·조정·의결</li> <li>대전시·금감원 및 금융기관·경찰 및 유관 사법기관·시민단체 등으로 구성</li> <li>정기/비정기 회의 개최, 수시 활동</li> </ul>	초기
	증장기계획 수립	<ul style="list-style-type: none"> <li>범죄 현황 분석 및 지역 환경 분석</li> <li>지역특성을 반영한 범죄예방 전략 수립</li> <li>부문별/연차별 증장기 세부 계획 마련</li> </ul>	초기
역량 강화	모니터링 및 전파 체계 확립	<ul style="list-style-type: none"> <li>모니터링 전담 조직/예산/시스템 마련</li> <li>신종 범죄수법 정보수집 및 신속 전파</li> <li>보이스피싱 범죄 DB구축 및 사후 활용</li> </ul>	중기
	실무대응 지원 방안 마련	<ul style="list-style-type: none"> <li>예방 실무 지원(전문가 교육/홍보)</li> <li>금융창구 실무 지원(예방지원도구 등)</li> <li>민간 자율 예방활동 지원</li> </ul>	중기
	관계기관 협업 강화	<ul style="list-style-type: none"> <li>금감원 업무협약 추진</li> <li>대전시 유관기관 협의회 구성/운영</li> <li>지자체-경찰-금융기관 실무 공조 강화</li> </ul>	초기
예방 및 대응	개인정보보호 및 대포통장 근절	<ul style="list-style-type: none"> <li>개인정보보호 및 도용 예방 대책 수립</li> <li>대포통장 개설·대여(판매) 근절 대책 마련</li> <li>상위 정책 연계, 효율화 방안 마련</li> </ul>	전기간
	맞춤형 교육·홍보 확대	<ul style="list-style-type: none"> <li>광역 홍보 신설 및 확대</li> <li>기관 간 홍보 공조·연계 사업 확대</li> <li>연령별/계층별 맞춤형 교육 실시</li> <li>민간 활동 독려 및 지원 방안 마련</li> </ul>	전기간
	시민 참여 증진	<ul style="list-style-type: none"> <li>신고 독려 및 보상 체계 마련</li> <li>피해 구제 및 사후 지원 방안 마련</li> <li>관내 피해 사례 및 대응 우수사례 전파</li> <li>금융사기 예방 캠페인/이벤트 전개</li> </ul>	전기간

## 제3절 단계별 실행 방안

### 1. 기반구축 단계

#### 1) 조례 제정

##### ○ 추진배경 및 필요성

- 지자체와 지역민 중심의 보이스피싱 예방 대책 수립 및 시행을 위한 법제도적 근거 마련 필요
- 일본의 구마모토현, 카시와시 선진 사례 등과 국내의 강릉시, 서울시 등의 추진 경과를 벤치마킹하고 대전시 지역여건에 맞는 조례 제정

##### ○ (실행방안) 보이스피싱 예방을 위한 대전광역시 조례 제정

- 대전광역시 보이스피싱 예방 대책 수립 및 실무 추진을 위한 조례를 제정하고, 유관 사업을 추진
- 보이스피싱 예방을 위한 지자체의 책임 및 의무 규정 마련
- 사업 추진 동력 확보를 위한 예산과 조직 관련 사항 규정 마련
- 유관기관 간 협력을 위한 업무협약 및 협력체계 구축 사항 포함

#### 2) 민관협력 협의체 구성 및 운영

##### ○ 추진배경 및 필요성

- 보이스피싱 예방 및 대응활동 전반에 대한 기획 활동을 추진하고, 사안별 논의 및 의결을 위한 심의·조정 기능의 컨트롤타워 구성 및 운영 필요
- 사업별 실무 추진을 위한 실무 협의회 구성 필요

##### ○ (실행방안) 보이스피싱 예방 및 대응 주체 간 협의체 구성

- 대전광역시·금융감독원 및 대전소재 금융기관 지점·지역 경찰 및

유관 사법기관·시민단체 및 민간기구·기타 일반인 및 유관기관 대표자 등으로 구성된 “대전시 보이스피싱 대책 위원회(가칭)” 또는 “대전시 금융사기 예방을 위한 민관협력협의회(가칭)” 등을 조직·운영

- 정기/비정기 회의 개최 및 각종 사안 심의·의결·평가(위원회)
- 금융사기 및 보이스피싱 예방을 위한 목적 사업 추진(협의회)

### 3) 중장기계획 수립 및 시행

#### ○ 추진배경 및 필요성

- 지역의 금융사기 및 보이스피싱 예방을 위한 체계적이고 효율적인 대책 수립 및 중장기 실행계획 마련 필요
- 민관 전문가가 참여하는 전문기관의 연구용역을 통해 5년 단위로 중장기 계획을 수립하고, 지역특성에 맞는 맞춤형 실행 방안 수립

#### ○ (실행방안) 보이스피싱 피해 예방 및 근절을 위한 중장기 계획 수립

- 국내외 보이스피싱 현황 및 동향 분석
- 대전시 보이스피싱 관련 환경 분석 및 특성 도출
- 대전시 보이스피싱 발생 현황 및 피해현황 분석
- 국내외 주요 지자체의 보이스피싱 예방 우수사례 분석
- 대전시 지역특성을 반영한 보이스피싱 예방 전략 체계 수립
- 단계별/연차별 세부 실행 계획 수립
- 기대효과 도출

## 2. 역량강화 단계

### 1) 모니터링 및 전파 체계 확립

#### ○ 추진배경 및 필요성

- 보이스포싱 수법이 지속적으로 변화하고 지능화·첨단화가 가속되어 신·변종 보이스포싱에 대한 지역의 대응 역량이 미흡
- 금융당국 및 경찰 등과 네트워크를 구축하여 신·변종 범죄 및 첨단 범죄 발생에 대한 상시 모니터링체계를 마련하고, 이를 통해 확보한 정보를 신속하게 지역에 전파

#### ○ (실행방안) 보이스포싱 현황 모니터링 및 상황 전파 체계 확립

- 관내 보이스포싱 발생에 대한 상시 모니터링 체계 구축
- 금융감독원 또는 경찰청, 언론, 지역금융기관 등에서 발생하는 보이스포싱 관련 사항 모니터링
- 전국 보이스포싱 예방경보 발생 및 신종 보이스포싱 수법 발생 인지 시 신속한 상황 전파(금융기관 및 유관기관 전파, 일반 시민 전파)
- 기타 보이스포싱 및 불법금융 관련 사항 모니터링
- 단기적으로는 경찰, 금감원 등 유관기관 자원 활용, 중장기적으로는 대전시 자체 모니터링 요원 배치
- 신속한 모니터링 및 체계적 상황전파를 위한 전용 시스템 구축

### 2) 실무 대응 지원 방안 마련

#### ○ 추진배경 및 필요성

- 보이스포싱 대응 정책이 금융당국 및 경찰 주도로 시행되고 있어 지자체 단위에서 자체 추진할 수 있는 개별 정책 및 지원 사업 부재
- 대전시 관내 보이스포싱 유관기관의 범죄예방 및 대응 실무 지원 사

업과 민간의 자율적인 예방활동 지원 사업 추진을 통해 지역의 역량 강화 및 활성화를 도모

- (실행방안) 보이스포싱 예방 및 대응 실무 지원 정책 수립/시행
  - 보이스포싱 전문가 교육 지원 사업 추진(관내 유관기관의 실무자를 대상으로 전문 교육을 지원)
  - 관내 금융기관 및 금융창구 실무자를 대상으로 한 범죄예방활동 지원 사업 추진(홍보물 지원, 대민서비스 우수사례 포상 및 홍보 등)
  - 민간 자율 예방활동 지원(지역별, 단체별 자생 민간조직이 자율적인 보이스포싱 예방활동을 수행할 경우 홍보물 및 행사 지원 등)

### 3) 관계기관 협업 강화

- 추진배경 및 필요성
  - 보이스포싱 및 금융사기 대응 유관기관 간 네트워크를 구축하고, 유사 업무간 협력 사업 및 지자체 추진사업 공조·협업을 통해 관내 범죄예방 활동의 효율 제고 및 실효성 향상을 도모
- (실행방안) 보이스포싱 유관기관간 공조·협업 체계 구축
  - 금융감독원 업무협약 추진(금융사기 대응 주관기관인 금융감독원과 대전광역시 간 공동협력을 위한 업무협약 추진 및 협력 사업 발굴)
  - 대전시 보이스포싱 유관기관 실무 협의회 구성 및 운영(지자체-경찰-금융기관 실무 공조 및 협력사업 추진)

## 3. 피해예방 및 대응 단계

### 1) 개인정보보호 및 대포통장 근절

- 추진배경 및 필요성
  - 보이스포싱 및 전기통신금융사기 범죄는 개인 신상정보를 도용하여

범죄 성공률을 높이므로 피해예방을 위해서는 개인정보 유출을 방지하는 것이 최우선 과제 인식되며 지역민에게 지속적인 홍보 필요

- 범죄활동의 최종 단계에서 반드시 대포통장이 활용되므로, 대포통장 근절은 범죄 예방 및 대응을 위한 가장 효과적인 수단 중 하나로 인식되어 관내 대포통장 개설 및 매매 근절 정책 지속 추진 필요

○ (실행방안) 개인정보보호 및 대포통장 근절 대책 수립/시행

- 개인정보보호 및 도용 예방 대책 수립/시행(행안부 및 경찰청사이버 안전국에서 추진하는 주요 개인정보보호 정책과 공조하여 지역민 대상 교육·홍보활동 강화)
- 대포통장 개설·대여(판매) 근절 대책 마련(금감원 및 관내 금융기관과 업무협약을 통한 통장개설 절차 강화 및 의심사례 신고체계 구축, 개인 간 통장 대여 및 매매 금지에 대한 홍보 강화 등)
- 상위 정책 연계, 효율화 방안 마련(정부 및 산하기관 등 유관업무 주무기관과의 정책공조를 통한 효율 제고)

## 2) 시민 참여 증진

○ 추진배경 및 필요성

- 보이스피싱 신고 활성화, 피해자 구제 및 사후지원 체계 수립, 금융사기 예방 이벤트/캠페인 개최 등을 통해 시민의 참여를 증진하고 생활 속 보이스피싱 예방의 활성화 유도 필요

○ (실행방안) 시민참여 증진 사업 추진

- 금융사기 신고 독려 및 보상체계 마련(보이스피싱 및 대포통장 관련 신고 시 신고자 보상 제도 홍보 강화, 대전시 자체적으로 추가 보상방안 마련 등, 타인 의심사례 신고 시 신고자 보호 및 보상 방안 마련 등)
- 보이스피싱 피해자 구제 및 지원 방안 마련(‘전기통신금융사기 피

- 해 방지 및 피해금 환급에 관한 특별법' 상의 피해자 구제 제도 홍보 강화, 신속한 피해자 구제를 위한 대전시 지원 체계 마련 등)
- 보이스피싱 피해 및 대응 우수 사례 전파 및 포상(관내에서 발생한 보이스 피싱 피해사례의 신속 전파, 보이스피싱 대응 우수사례에 대한 포상 제도 도입 등)
  - 보이스피싱 예방 캠페인 및 이벤트 추진(민관이 참여하는 대전시 보이스피싱 예방 캠페인 상시 추진, 지역축제/행사와 연계한 이벤트 추진, 대전시 및 유관기관 홈페이지를 활용한 보이스피싱 예방 온라인 이벤트 추진 등)

### 3) 연령별/계층별 맞춤형 교육·홍보 확대

보이스피싱 예방을 위한 금융감독원을 중심으로 한 국가기관 및 경찰청, 지방자치단체 등 관련 단체에서 국민들을 대상으로 다양한 금융사기 예방 교육이 실시되고 있다. 그러나 기관별 자료제작 및 교육전문가 부족, 고령자 중심의 교육 등으로 실질적이고 교육방법에는 효과가 미미한 상태이다.

보이스피싱 범치는 원격지에서 전기통신수단을 통해 은밀하게 이루어지고, 개개인의 정보수준과 상황대처 역량에 따라 피해 여부 및 그 규모가 결정되기 때문에 지역민에 대한 교육·홍보의 강화가 필요하다.

앞서 연령대별로 피해를 알아본 바와 같이 취약계층을 중심으로 우선적으로 연령별 및 계층별 교육·홍보사업 추진이 필요하다. 즉 범죄수법에 따라 유형별 보이스피싱 취약계층(노인, 취업준비생, 여성 등)을 대상으로 특성화된 교육·홍보사업의 추진이다.

첫째로 각 기관별로 추진되고 있는 예방교육에 있어 유치원에서 성인에 이르는 세대별, 연령대별 대상에 맞는 세부적 맞춤형 교육 표준안을 마련하여 체계적 예방교육을 해야 한다. 가능하다면 시의 적극적인 지원하에 관련 기관의 담당자로 구성되는 보이스피싱 예방교육 자료작성팀(안)을 구성하여 표준안 개발을 추진하는 것도 효과적이라 판단된다.

예를 들어 보이스피싱 유형별 특성교육은 크게 의미 이해, 세대별 피해 건수 및 금액, 년도별 피해 건수 및 피해 금액, 피해 사례 소개, 창의적 체험(실습)을 통한 역할 놀이 후 역할체험에 대한 각자 의견을 제시하여 토론하는 방식을 모색할 수 있다.

둘째로 현재 부족한 전문강사를 양성하여 교육장소에 강사를 파견하는 것이다. 표준안이 마련되면 전문강사를 양성하여 표준 교안안을 토대로 교육이 이루어지도록 추진한다. 전문강사를 양성하기 위해서는 금융감독원, 경찰청, 대전준법지원센터 등 관련기관의 담당자들로부터 수범과 범죄특성 등을 교육받도록 하며, 강의방식에 대해서는 강의 경험이 풍부한 강사로부터 강의수법을 교육받도록 한다. 즉 교육특성에 따라 세대별 통합교육, 재연 체험(실습) 활동 등의 형태로 금융사기피해 예방교육을 마련해야 한다. 갈수록 다양해지고 교묘해지는 금융사기에 대한 발 빠른 대처 요령에 대한 교육은 정기적으로 업그레이드도 되어야 한다.

홍보방안도 효율적인 예방홍보가 되려면 연령별/계층별 맞춤형 교육 및 홍보사업이 추진되어야 한다. 첫째로 홍보계획 수립을 마련한다. 기본의 팜플렛 자료를 통한 홍보에서부터 홍보효과가 큰 매스미디어(TV, 라디오 등)를 활용하는 방법, 대전시가 보유하고 있는 미디어(홈페이지, 전광판, 스카이로드 등)를 활용한 홍보매체를 활용한 다각도 홍보계획 수립이다. 전문가들의 지적에 의하면 TV광고를 통한 홍보효과가 가장 크므로 TV방송국과의 연중캠페인을 검토한다. 각 기관별로 비용을 분담한다면 예산 측면에서도 절감할 수 있는 효과가 있을 수 있다고 기대된다.

둘째로 관련기관 간 홍보공조 및 연계사업 확대이다. 관내 유관기관별로 추진하고 있는 홍보사업의 공유 및 업무조정 등을 통해 예방홍보사업의 효율성 증진, 유사사업의 공동 협력 추진을 통한 성과제고 방안 마련 등이다.

셋째로 민간활동 독려 및 지원방안 마련이다. 민간(관련 시민단체)이 자율적으로 추진하는 교육 및 홍보사업에 대해 홍보물 지원 등 다양한 지원책을 강구한다. 이러한 민간지원에 대한 예산도 홍보계획에 구체적으로 포함되어야 한다.

끝으로 스마트폰, 인터넷가입, PC판매 등 전기통신관련 사업자(사업장)의 소비자 안내 활성화이다. 상품 구매 및 서비스 가입단계에서 보이스피싱 예방 안내 및 피해보상 제도 홍보를 통해 시민들이 금융사기피해예방에 대한 인식제고가 선행될 수 있도록 유도한다.

**[표 5-4] 대전시 보이스피싱 표준모델 구상(안)**

보이스피싱 예방교육 표준모델 구상(안)
▶ 금융사기 예방 교육 필요성 및 청강자 동기부여
▶ 경험자의 이야기 나누기
▶ 금융사기 피해 유형별 개념 및 개념에 따른 실제 피해 사례 소개 <ul style="list-style-type: none"> <li>- 눈 뜨고도 당하는 금융사기(알면서도 당하고 조심해도 당함)</li> <li>- 누구나 표적이 된다.(어느 누구도 예외 없음)</li> <li>- 장기간 집 비울 시 열쇠는 우편함에 보관하지 말 것</li> <li>- 과거와 현재 변화된 보이스 피싱 수법 및 유형별 실제 피해 사례</li> </ul>
▶ 금융사기 피해자의 특성을 극복하기 위한 이론 교육 <ul style="list-style-type: none"> <li><input type="checkbox"/> 무경험에 대한 예방 교육               <ul style="list-style-type: none"> <li>- 실제 상황(녹취 파일 들려주거나 동영상 보여줌)</li> </ul> </li> <li><input type="checkbox"/> 불감증(평소 나는 아닐거야, 무대책) 해소</li> <li><input type="checkbox"/> 무의식(친절함, 자존심, 급한 성격으로 인한 사기 피해 노출)</li> <li><input type="checkbox"/> 순간 착각(부정적 사실 인식 없이 현실 그대로 받아줌)</li> <li><input type="checkbox"/> 무방비, 무대응 (가족 위험 시, 간절할 때)으로 침착성 결여</li> <li><input type="checkbox"/> 상호 경험 사례 등을 교환하여 간접적인 교육 습득</li> </ul>
▶ 체험(실습) 역할 놀이 <ul style="list-style-type: none"> <li><input type="checkbox"/> 실제 사례별 녹취 파일을 시나리오 형식(ppt교안)으로 변환</li> <li><input type="checkbox"/> 교구(전화기 준비) 사용 2인 1조 편성하여 실제상황 재연</li> </ul>
▶ 금융사기 피해 예방법
▶ 금융사기 대처법
▶ 금융사기 피해 인식 후 후속 조치요령



## 결론 및 정책제언

1. 결론
2. 정책제언



## 제 6 장 결론 및 정책제언

### 제1절 결 론

2006년 5월 국내에서는 처음 보이스피싱 사기가 발생한 이후 많은 피해 사례들이 속출하며 사회문제로 부각되고 있다. 매일같이 수법이 교묘해지고 지능화되고 있어 심각한 민생침해 범죄로 그 피해도 더욱 증가되고 있다. 더욱이 피해자가 고령층에서 사회초년생들에게 까지 확대됨에 따라 심각한 사회문제로 번지고 있다.

최근 전화금융사기는 스크립트 능력과 침단기술을 활용하는 복합적인 지능형 범죄로 성장하고 있다. 사전에 피해자 정보를 정확하게 파악하여 피해자 상황에 적절한 맞춤형 스크립트를 작성·이용하며, 전화번호 변작, 가상화폐 이용 등 다양한 침단기술을 동원한다. 또한, 기술의 발전과 함께 이들의 범죄수법도 지속적으로 진화하고 있어서 단속기관의 어려움이 계속되고 있다. 전화금융사기로 인해 시민들의 금융적 피해도 날로 커져가고 있지만, 또 다른 한편에서는 지자체 및 경찰청 등의 행정업무를 비롯해 대시민 서비스의 행정행위 등에 까지 영향을 미치고 있다. 이처럼 여러 국면에서 날로 심각해져가는 전화금융사기의 피해방지를 위해 현황파악과 시민들의 피해예방 및 인식제고를 위한 방안검토를 목적으로 했다.

본 연구에서는 첫째로 전화금융사기 피해 관련 법·제도 및 전국 및 대전시 피해현황을 파악하였다. 둘째로 전화금융사기 범죄 동향 및 특징을 파악하였다. 특성을 파악 후 전화금융사기 피해로부터 시민의 안전을 확보하기 위한 예방대책 기본방향을 검토하였다.

현황파악에 있어서는 경찰청, 대전지방경찰청, 금융감독원의 통계를 활용하여 지역별, 유형별, 연령별 등 다양하게 알아보아 현재의 사기피해 특징을 살펴보았다.

대전시의 시민안전을 위한 전화금융사기 예방을 위해 『시민 모두가 보이스피싱의 피해 걱정 없이 살 수 있는 안전한 사회구현』을 본 대책의 비전으로 설정하고, 보이스피싱 근절 대책 수립 및 시행을 추진 목표로 설정하였다. 추진목표 달성을 위한 중점 추진과제는 단계별로 수립 시행하며 3대 분야 12개의 과제를 도출하여 제시하였다.

우선 기반구축 단계에서는 조례제정, 민관협의체 구성, 중장기계획 수립을 제시하였다. 역량강화 단계에서는 모니터링 및 전파체계 확립, 실무대응 지원 방안 마련, 관계기관 협업강화를 제시하였다. 예방 및 대응 단계에서는 개인정보보호 및 대포통장 근절, 맞춤형 교육·홍보 확대, 시민 참여 증진을 제시하였다.

단계별 실행방안에서는 앞서 제시한 12개 과제가 다루어야 할 주요내용들을 간략하게 제시하였다. 추진배경 및 필요성, 실행방안으로 알기 쉽게 개조식으로 내용을 제시하였다. 다만 교육 및 홍보는 본 연구의 목적에서 제일 중요하므로 다소 심도 있게 내용을 다루었다. 관련기관의 전문가들의 조언에 따라 40분 정도의 예방교육에 사용할 수 있는 표준교육모델(안)을 제시하기도 하였다. 가장 중요한 것은 시민들이 피해를 입지 않도록 보이스피싱 예방안내 및 피해보상 제도 홍보를 통해 시민들이 금융사기 피해예방에 대한 인식제고가 선행될 수 있도록 유도해야 한다는 것에 공감한다.

최근의 전화금융사기의 5가지 유형은 크게 첫째로 환급금 빙자유형, 둘째로 예금보호조치 빙자유형, 셋째로 납치협박 빙자유형, 넷째로 합의금 등록금 요구유형, 다섯째로 가짜사이트 결합유형으로 구분되어지고 있다. 이에 유형별 대응할 수 있는 다양한 시책이 관련기관과 협업하여 만들어야만 시너지효과가 발생할 수 있다. 관련기관의 협업이 피해를 최대한 줄일 수 있는 묘책이라 할 수 있다. 좀 더 국가적 차원으로 확대하면 보이스피싱 조직이 국제화되어 감에 따라 아직도 중국 등을 거점으로 하는 범죄조직이 한자문화권인 한·중·일 등을 보이스피싱 대상지역으로 삼고 있을 가능성이 높아 3국간 협력체계 구축을 통해 적극적인 공동 대응이 필요하다.

## 제2절 정책제언

날이 갈수록 전화금융사기 범죄는 그 수법이 교묘해지고 지능화 되고 있다. 피해자 역시 고령자에서 대출을 미끼로 30대·40대가 주요 타겟군으로 옮겨가고 있으며, 심지어 취업난에 허덕이는 젊은 청년들까지 대상이 되고 있다. 전화금융사기가 증가함에 따라 국내에서도 금융위원회, 금융감독원, 경찰청 등이 다양한 방법을 동원해 적극적으로 대처하고 있다. 그러나 중복적인 추진시책과 교육·홍보를 받지 못하는 그룹이 생김에 따라 시민의 안전을 전반적으로 책임지는 지자체의 역할이 더욱 제고된다고 할 수 있다.

이에 대전시의 시민안전을 위한 보이스포싱 예방을 위해 『시민 모두가 보이스포싱의 피해 걱정 없이 살 수 있는 안전한 사회구현』이라는 목표설정을 제안한다. 또한 이 목표를 달성하기 위해서 관련기관이 함께하는 3대 분야 9개 과제를 구체적으로 제안한다.

이러한 과제를 실천하기 위해서 다음과 같은 시급한 정책을 제언으로 하고자 한다.

첫째, 금융사기피해에 대한 시민들의 인식제고이다. 경제적으로 어려움이 지속되고 있는 현 시점에서 금융사기피해를 겪는다면 본인은 물론이요 가족들까지도 심리적 상처는 크게 된다. 특히 고령자의 경우는 자신의 단순한 행동으로 인해 자식들까지도 피해를 입었다는 생각으로 인해 트라우마에서 벗어나지 못해 사회생활 전반이 원활하지 못하게 되는 경우도 종종 발생한다. 금융사기피해가 한 개인의 생활의 전부를 붕괴시킬 수 있다는 점을 시민 스스로 모두가 인식하는 것이 중요하다고 판단된다.

둘째, 앞서 제시한 3대 분야 12개 과제에 대한 전략적 로드맵을 관련기관에서 심도있는 검토를 제안한다. 더불어 성공적인 전화금융사기 예방 사례를 지속적으로 발굴하여 12개 과제에 대한 내용적 업그레이드가 필요하다고 판단된다. 전화금융사기 예방을 위한 과제발굴에 있어서는 선행되어야 할 것이 관련기관의 협조체계 구축이라는 것을 잊지 말아야 한다.

셋째. 적극적인 홍보와 교육이라고 할 수 있다. 한정된 경찰력으로 지능화 되어가는 보이스피싱을 막는다는 것은 현실적으로 불가능하다. 사후관리가 아닌 선도적인 예방방안이 보이스피싱 전체에 대한 피해를 줄일 수 있는 최선의 방안이 될 것이다. 이를 위해서는 각종 언론매체를 활용한 지속적인 홍보를 검토해야 할 것이다. 또한 병행되어야 하는 것이 대시민 교육이 절대적이라 생각한다. 연구과정에서 준비한 보이스피싱예방 교육을 받은 시민들에게 설문조사를 한 결과, 교육의 만족도와 유사교육을 받고자 하는 의지가 큰 만큼 행정에서는 관련기관과 협업하여 다양한 교육프로그램을 만들어야 할 것이다.

넷째. 기관과의 협업이다. 피해현황을 위한 통계분석에서 알 수 있듯이 기관별도 통계데이터가 다소 일치하고 있지 않다. 범죄라는 차원에서 현장을 담당하는 경찰과 피해구제를 위해 담당하는 금융감독원의 분석시점과 기타 이유로 인해 차이를 발생하고 있다고 생각된다. 통계를 넘어 예방차원에서도 기관과의 협업을 통해 중복되는 업무를 방지하고, 효율적인 홍보·교육에서 시너지 효과를 만들 수 있고 예산을 절감도 가능하다.

끝으로 『시민 모두가 보이스피싱의 피해 걱정 없이 살 수 있는 안전한 사회구현』의 비전을 달성하려면 제도적 마련이 필요하다. 즉 일본의 경우처럼 예방을 위한 교육에 있어서는 행정이 우선적으로 책임을 가질 수 있도록 제도를 마련해야 할 것이다. 시민과 가장 접점에 있는 대전시가 시민 보호에 주도적으로 나설 필요가 있다. 이러한 실천을 위해서는 구체적인 계획과 예산이 마련되도록 조례 제정을 검토 할 필요가 있다.

본 연구에서는 단순한 통계데이터와 관련 기관의 자료를 검토하여 정리하는 것으로 진행되었다. 향후과제는 보다 효과적인 연구성과를 얻기 위해서 전문가들이 모여 피해사례를 중심으로 분석하여, 유형별 대책을 마련하는 심도있는 작업이 병행되어야 한다고 판단된다.

지금까지 살펴 본 바와 같이 시민안전을 위한 전화금융사기 피해 예방을 위해 전략적으로 실천과제를 우리모두가 실천한다면 전화금융사기로부터 피해를 줄일 수 있다고 확신한다.

## 참고문헌

- 법제처(2017), 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법  
법제처(2017), 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 시행령  
법제처(2017) [법령] 전기통신기본법  
경찰청(2016). “경찰청, 「제2차 한·일·중 경찰협력회의」 개최”, 보도자료(11. 21)  
경찰청(2017), 전화금융사기 현황자료  
금융감독원(2011), ‘11.9.30일부터 전화금융사기(보이스피싱) 피해금 환급제도 시행,  
보도자료(9. 29)  
금융감독원·경찰청(2011), 경찰청 112센타를 통한 ‘보이스피싱 피해금 지급정지  
신청제도’ 실시지역 전국 확대, 보도자료(11. 30)  
금융감독원(2012a), 금융소비자 보호를 위한 보이스피싱 피해방지 종합대책, 보도자료(2. 1)  
금융감독원(2012b), 최근 보이스피싱 현황 및 관련 유의사항, 보도자료(9. 25)  
금융감독원(2014), 피싱사기 피해 구제현황 및 소비자 유의사항, 보도자료(2. 25)  
금융감독원(2015a), 보이스피싱 등 금융사기 척결 특별대책[「민생침해 5대 금융악  
척결 특별대책」세부 대책①], 보도자료(4. 13)  
금융감독원(2015b), SK텔레콤 PR2팀, “금융감독원, SK텔레콤과 손잡고 보이스피싱  
사기 척결”, 보도자료(11. 2)  
금융감독원(2015c), 2015년 하반기부터 금융사기 피해 현저히 감소!, 보도자료(11. 18)  
금융감독원(2016a), “2016년도 상반기 불법금융 척결 추진성과 및 향후대응”, 보  
도자료(7. 22)  
금융감독원(2016b), “보이스피싱 전화번호 적극 신고하세요”, 보도자료(10. 28)  
금융감독원(2016c), “스마트폰으로 보이스피싱 목소리 및 전화번호를 신고하세요”,  
보도자료(11. 18)  
금융감독원(2016d), 대검찰청 공식 홈페이지를 악용한 신종 보이스피싱 발생, 보도  
자료(6. 2)  
금융감독원(2017a), 2016년 보이스피싱 및 대포통장 큰 폭 감소, 보도자료(2. 17)  
금융감독원(2017b), “비트코인을 요구하는 대출사기에 주의!”, 보도자료(4. 14)  
금융감독원(2017c), 2017년 상반기 대포통장 및 보이스피싱 현황 분석, 보도자료(8. 21)  
금융감독원(2017d), 첨단 수법으로 무장한 신종 보이스피싱 유의, 소비자경보 발령!,  
보도자료(10. 10)

금융감독원, 일본의 보이스피싱 피해실태와 예방노력 및 시사점(2017.09.23) (보도자료)  
 대전지방경찰청(2017), 대전광역시 전화금융사기 현황자료  
 이진권(2007), 전화금융사기 범죄에 대한 고찰, 한국경찰연구, 제6권, 제2호  
 이창운(2015), “전자자금이체에 관한 연구”, 금융법연구, 제12권 제1호  
 오영근·정정원(2012), 보이스피싱 근절을 위한 입법적 대응방안 연구, 법무부 연구  
     구용역과제  
 정정원(2013), ‘보이스피싱범죄의 형사법적 검토 및 대응방안’, 가천법학 제6권 제2호  
 정진연(2011), “국제전화금융사기에 대한 형사법적 쟁점”, 『법학연구』 제41집  
 치안정책연구소(2016), 2017 치안전망  
 허성욱/정세종(2008), “국제전화금융사기에 관한 법적 고찰”, 『한국경찰연구』 제7권  
     제2호: 125-126면  
 홍승희(2009), “차명계좌를 중심으로 한 전화금융사기의 법적 쟁점”, 『비교형사  
     법연구』 제11권 제2호: 30-31면  
 서울특별시(2017), 서울시 금감원 6개 주요은행, 손잡고 금융사기 예방 나선다(보도자료)  
[http://spp.seoul.go.kr/main/news/news\\_report.jsp#view/209832?tr\\_code=snews](http://spp.seoul.go.kr/main/news/news_report.jsp#view/209832?tr_code=snews)  
<http://blog.daum.net/ujkim100/5953239>  
<http://phishing-keeper.fss.or.kr>

## 부 록

### [1] 일본 지자체의 「보이스피싱 피해방지 조례」

#### 1. (광역지자체) 쿠마모토縣의 현 주민을 보이스피싱으로부터 지키는 조례

##### 1. 목적

- 보이스피싱 사기 피해가 급증하여 사회문제화되고 있어 보이스피싱 사기의 피해방지를 위해 현, 현 주민 및 사업자의 책무를 명확하게 함은 물론 보이스피싱 사기에 대한 피해방지 조치를 강구하여 현 주민의 재산을 지킨다.

##### 2. 정의

- 보이스피싱 사기의 정의 : 오레오레 사기, 가공청구 사기, 용자보증금 사기, 환급금 등 사기
- 사업자의 정의
  - . 금융기관(은행, 신용금고 등)
  - . 금융기관이 ATM을 설치한 편의점, 백화점 등
  - . 운송사업을 영위하는 자, 우체국, 기타 타인의 요청으로 유상으로 운송하는 자
  - . 휴대폰음성통신사업자, 중개사업자 및 대여업자

##### 3. 현의 책무

- 1의 목적을 달성하기 위해 보이스피싱 사기의 피해방지에 관한 시책을 종합적으로 추진한다.

##### 4. 현 주민의 책무

- 본인 및 친척이 보이스피싱 사기를 당하지 않도록 노력한다.
- 현이 시행하는 보이스피싱 사기의 피해방지를 위한 대책에 협력한다.

##### 5. 사업자의 책무

- 보이스피싱 사기의 피해방지에 관한 관심과 이해를 높이고 현이 시행하는 보이스피싱 사기의 피해방지를 위한 대책에 협력하도록 노력한다.

## 6. 시읍면과의 연계

- 현은 시군구가 보이스피싱 사기의 피해방지에 관한 시책을 실시하는 경우에는 필요한 협력 및 지원을 실시한다.

## 7. 홍보활동 및 계몽활동

- 현은 보이스피싱 사기의 피해방지에 관한 현 주민의 관심과 이해를 제고하기 위해 보이스피싱 피해방지에 관한 홍보활동 및 계몽활동을 실시한다.

## 8. 현 주민 등의 자주적인 활동의 지원

- 현은 현 주민, 사업자 및 그 밖의 자가 조직하는 단체(이하 현 주민 등이라고 한다)에 의한 보이스피싱 사기 방지대책과 관련된 자주적 활동을 촉진하기 위하여 해당 활동을 담당하는 인재육성에 노력한다.
- 현은 보이스피싱 사기의 피해방지를 위한 대책을 추진하기 위해 현 주민 등과의 사이에 있어 또는 현 주민 등 상호간에서 정보 및 의견을 교환하는 기회를 만든다.

## 9. 정보의 제공

- 경찰본부장은 필요가 있다고 인정되는 경우 시군구에 대하여 보이스피싱 사기 발생현황, 기타 피해방지에 유용한 정보를 제공한다.
- 경찰본부장은 현 주민 등에 의한 보이스피싱 사기 피해방지에 관한 자주적 활동을 지원하기 위해 정보제공, 조언 기타 필요한 조치를 취한다.

## 10. ATM이용시의 유의사항

- 다음의 행위는 보이스피싱 사기의 전형적인 형태인 바, ATM을 이용하고자 하는 자는 정당한 이유가 있는 경우를 제외하고 다음의 행위를 피하도록 노력한다.
  - . 변장을 하는 등 특이한 이용자라고 판별되지 않도록 하여 ATM을 조작
  - . ATM 조작과 관련된 타인부터의 지시 등의 연락을 기다리기 위해 장기간에 걸쳐 ATM을 점유
  - . 다수의 저축통장 또는 현금카드를 사용하여 장기간에 걸쳐 또는 반복적으로 ATM을 조작
  - . 휴대전화, 기타 휴대용 무선통신장치를 사용하면서 ATM을 조작

### **11. 통보(현 주민)**

- 현 주민은 다음 각각에 해당할 때는 경찰관 또는 사업자에게 통보하거나 기타 적절한 조치를 강구하도록 노력한다.
- . 그 언행으로부터 보이스피싱 피해를 당하고 있는 것으로 우려되는 사람을 발견한 경우
- . 본인 또는 친척이 보이스피싱 사기의 의심이 있는 전화, 우편물 등을 받은 경우

### **12. 통보(사업자)**

- 사업자는 11의 통보를 받거나 사업을 행하면서 보이스피싱 사기피해에 노출되어 있는 자 또는 보이스피싱 사기에 관한 행위를 하고 있는 의심이 되는 자를 발견한 때에는 경찰관에게 통보하는 등 적절한 조치를 강구하도록 노력한다.

### **13. 조치**

- 경찰관은 11 또는 12의 통보를 받은 때에는 해당 통보에 관한 조사를 행하는 등 적절한 처리를 한다.

### **14. 운용상의 유의사항**

- 그 조례의 운용에 있어서는 현 주민 및 현 체류자의 자유와 권리를 부당하게 제한하지 않도록 유의한다.

### **15. 보고**

- 公安위원회는 보이스피싱 사기 범행의 형태를 거울삼아 보이스피싱 사기피해방지에 긴급하게 노력할 필요가 있는 사업자를 지정할 때는 그 취지를 의회에 보고한다.

### **16. 기타**

- 이 조례는 시행후 3년이 지나면 검토하여 필요한 조치를 강구한다.

## 2. (기초지자체) 카시와市の 보이스피싱 피해방지 조례

### (목적)

**제1조** 이 조례는 보이스피싱 등 피해가 시민생활에 악영향을 미치고 있는 현상을 보고 보이스피싱 등 피해방지(이하 “피해방지”라 한다) 및 피해자의 지원에 관한 본 시와 시민 및 사업자의 책무를 명확하게 함은 물론 유용한 정보의 제공과 이에 필요한 사항을 정함으로써 보이스피싱 등의 피해를 방지하고 해당 피해자를 지원하고 나아가 안심하고 안전한 시민생활의 확보에 기여하는 것을 목적으로 한다.

### (정의)

**제2조** 이 조례에서 다음 각호에 의한 용어의 정의는 각각 해당 각호에 정하는 것에 의한다

- (1) 보이스피싱 등이란 보이스피싱 및 보이스피싱 유사사기를 말한다.
- (2) 보이스피싱은 오레오레 사기, 가공청구 사기, 대출보증금 사기 및 환급금 등 사기를 말한다.
- (3) 오레오레 사기란 친족을 가장한 전화를 걸어 해당 친족이 그 근무처의 물건을 횡령하여 보상을 위해 직접 현금이 필요하다고 기망하고 지정한 예금계좌 또는 저금계좌(이하 “저축금계좌”라고 한다)에 현금을 송금시키는 수법이나 이와 유사한 방법의 사기(형법 제246조의 죄에 해당하는 행위를 말한다. 이하 같다)를 말한다.
- (4) 가공청구 사기란 웹사이트를 사용한 사실이 있는 것처럼 해당 이용에 관한 요금을 청구한 문서를 송부하고 지정하는 저축금계좌에 현금을 송금시키는 수법이나 이와 유사한 방법의 사기를 말한다.
- (5) 대출보증금 사기란 용자를 해 줄 의사가 없음에도 불구하고 해당 용자의 신청을 유도하고 해당 용자를 신청한 자에게 대해 먼저 해당 용자를 받기 위한 조건으로 금전을 납부하도록 요구하여 지정한 저축금계좌에 현금을 송금시키는 수법이나 이와 유사한 방법의 사기를 말한다.
- (6) 환급금 등 사기란 국가 또는 지방자치단체의 직원이나 기타 법령에 의거 공무에 종사하는 직원을 사칭하여 의료비, 세금, 연금에 관한 보험료 등의 환급금 또는 기타의 급부금이 있는 것처럼 가장하여 그 수령절차에 관련하여 현금자동인출기를 작동시켜서 저축금계좌간 송금에 의해 현금을 송금시

- 키는 수법이나 이와 유사한 방법의 사기를 말한다.
- (7) 보이스피싱 유사사기란 금융상품의 거래, 당첨금부증방법(当せん金付証票法) 제2조 제2항에 규정한 가산형 당첨금부 증표의 당첨에 관한 수자의 제공, 이성과의 교제에 관한 알선, 기타 대면하지 않는 사람을 기만하고 허위의 정보를 제공한 다음에 현금을 편취하는 사기를 말한다.
- (8) 시민 등이란 시 안에 거주, 체제 또는 근무하거나 통학하는 자를 말한다.
- (9) 사업자란 다음에 같은 자로서 시 안에서 사업활동을 하는 자를 말한다.
- 1) 범죄이용 예금계좌에 관한 자금에 의한 피해회복 분배금의 지불 등에 관한 법률 제2조제1항에서 규정하는 금융기관
  - 2) 자기가 소유하고 또는 관리하는 토지 또는 건물에 현금자동인출기를 설치하고 있는 자
  - 3) 화물자동차운송사업법 제39조제1호에 규정된 화물자동차운송사업자
  - 4) 휴대음성통신사업자에 의한 계약자 등의 본인확인 등 및 휴대음성통신역무의 부당한 이용의 방지에 관한 법률 제2조제3항에 규정하는 휴대음성통신사업자, 동법 제6조제1항에서 규정한 중개업자 및 동법 제10조제1항에서 규정한 대여업자
  - 5) 주택건물거래법 제2조제3호에서 규정한 주택건물거래업자(주택 또는 건물의 매매, 교환 또는 임대차 대리 또는 중개 행위를 업으로 하는 자에 한한다.)
  - 6) 1)부터 5)까지 언급한 자 이외에 보이스피싱 등의 범행과 관련하여 해당 범행수단으로 이용되거나 이용될 우려가 있는 상품 등의 유통 및 역무의 제공을 업으로 행하는 자

**(운용상의 주의)**

**제3조** 이 조례의 운용에 있어서는 시민 등 및 사업자의 권리를 부당하게 침해하지 않도록 유의해야 한다.

**(카시와시의 책무)**

**제4조** 카시와시는 피해방지에 관한 시책을 종합적으로 책정하여 실시한다.

2. 카시와시는 시민 등, 사업자 및 그 밖의 자가 조직한 단체(이하 단체 등 이라고 한다)에 대하여 보이스피싱 등의 발생상황과 피해방지에 관한 유용한 정보를 제공한다.

3. 카시와시는 피해예방에 관한 단체 등의 관심 및 이해를 심화하기 위해 효과적인 홍보 및 계몽활동을 실시하고 단체 등이 행한 피해방지에 관한 자주적인 활동을 지원한다.

#### (시민 등의 책무)

**제5조** 시민 등은 전조 제2항의 정보 및 피해방지를 위한 학습의 기회를 주체적이고 적극적으로 활용하여 자립적인 소비자로서 피해방지에 스스로 노력한다.

2. 시민 등은 카시와시가 실시하는 피해방지에 관한 시책에 협력함은 물론 사업자가 시민 등에 대해 피해방지에 관한 주의를 환기한 때에는 이에 대한 적절한 행동을 하도록 노력한다.

#### (사업자의 책무)

**제6조** 사업자는 피해방지에 관심 및 이해를 심화하고 나아가 카시와시가 실시하는 피해방지에 관한 시책 및 시민 등이 행한 피해방지에 관한 자주적인 활동에 협력하도록 노력한다.

2. 사업자는 상품 등의 유통 및 역무의 제공을 할 때 보이스피싱 등의 수단에 이용되지 않도록 수단을 강구하고 나아가 피해방지에 관한 시민 등의 주의환기 및 홍보를 행하도록 노력한다.

#### (통보 등)

**제7조** 시민 등은 다음 각호(시내에 근무처 또는 통학처가 있는 것에는 제1호)에 해당할 때에는 경찰관 또는 사업자에의 통보와 그 밖에 적절한 조치를 강구하도록 노력한다.

- (1) 그 말과 행동으로부터 보이스피싱 등에 의한 피해를 받을 수 있다라고 의심되는 자를 발견한 때
- (2) 자기 또는 자기와 동일한 세대에 속하는 자가 보이스피싱 등으로 의심되는 전화 또는 우편물 등을 받은 때
2. 사업자는 전항의 통보를 받은 때 또는 상품 등의 유통 혹은 역무의 제공을 할 때 보이스피싱 등에 관한 피해를 받는 것으로 의심되는 자 또는 보이스피싱 등에 관한 행동을 하고 있다고 의심되는 자를 발견한 때는 법령의 범위내에서 경찰관에게 통보, 그 밖에 적절한 조치를 강구하도록 노력한다.

**(피해자에의 지원)**

**제8조** 카시와시는 보이시피싱 등에 의한 피해(시외에서 받은 피해를 포함한다)를 받거나 받은 것 같은 시민이 그 범죄에 의해 심신이 받은 중대한 영향으로부터 조기에 회복할 수 있도록 하기 위해 그 심신 상황 등에 대응한 적절한 보건의료서비스 또는 복지서비스가 제공되도록 또는 사법수단 등에서 그 권리를 원활히 행사할 수 있도록 필요한 조치를 강구한다.

**(치바현과의 협력)**

**제9조** 카시와시는 치바현이 실시하는 피해방지에 관한 시책에 대해 필요한 협력을 실시한다.

**(경찰과의 연대)**

**제10조** 카시와시는 제4조제2항의 규정에 의한 정보의 제공 혹은 동조제3항의 규정에 의한 지원을 행하거나 제8조의 규정에 의한 조치를 강구함에 있어서는 치바현경찰본부 및 카시와시 구역을 관할하는 경찰서(이하 치바현경찰본부 등이라 한다)와의 연대를 도모한다.

2. 카시와시는 치바현경찰본부 등이 실시하는 피해방지에 관한 시책에 있어서 필요한 협력을 행하는 것과 함께 치바현경찰본부 등과의 연대를 도모한다.

**(위임)**

**제11조** 이 조례의 시행에 관한 필요한 사항은 시장이 별도로 정한다.

**부 칙**

**(시행기일)**

1. 이 조례는 2016년 4월 1일부터 시행한다.
2. 시장은 이 조례의 시행후 5년을 경과한 경우에 이 조례의 시행상황에 대해 검토하여 필요한 것이 있다고 인정되는 때는 그 결과에 기초하여 소요조치를 강구한다.

## [2] 보이스피싱 교육자료

### 피싱사기 피해 예방교육 - 배점호 소장 (안양준법지원센터)

일시 : 2017.11.28

장소 : 대전세종연구원 2층 대회의실

## 피싱 사기 피해 예방교육

법무부 안양준법지원센터  
소장 배점호

### 보이스피싱으로 인한 피해



### 피싱이란 무엇일까?

◆ 피싱(Phishing)

**개인정보(Private Data)**  
**낚시(Fishing)를 합친 합성어**

금융계좌번호, 계좌비밀번호, 보안카드숫자 같은 중요한 개인정보를 훔치기 위해 속이는 행동

### 피싱사기의 주요유형



3. 공공기관을 사칭하여 문자메시지 보낸 후 가짜사이트로 유도하여 예금 등 가로챌

### 피싱사기 구체적 사례

◆ 사례3: 자녀의 납치 및 사고 방자 편취

Y씨(40대, 여)는 오후 1시경 자녀의 이름과 학교를 대면서 "지금 당장 아이를 납치하였다. 하룻 수천하며 죽여버린다. 1,000만원을 불러주는 계좌로 송금해라"는 전화를 받고 보유하고 있던 300만원을 사기범 계좌로 이체하여 피해를 봄

K씨(50대, 여)는 오전에 사기범으로부터 "학교 행정실인데 아이가 머리를 다쳐서 치료를 해야 하니 1,000만원을 입금 하라"는 전화를 받고 800만원을 입금하여 피해를 봄. 사기범은 자녀 이름, 휴대전화 번호, 학교이름을 정확히 알고 있었음

### 피싱사기 막아봅시다!

- ◆ 금융거래정보 요구는 절대 응대하지 마세요.
- ◆ 현금지급기로 유인하면 100% 보이스피싱
- ◆ 자녀납치 보이스피싱에 미리 대비
- ◆ 개인·금융거래정보를 미리 알고 접근하는 경우에도 내용의 진위를 확인하고 피해를 당한 경우 신속히 지급정지를 요청

### 피싱사기를 당했다면

◆ 사기이용 계좌의 지급정지

송금계좌의 금융기관이나 사기계좌의 금융기관에 피싱사기 직접 피해구제신청

또는 수사기관(112콜센터)이나 금융감독원(1332번)에 피해사실을 신고하면 수사기관이나 금융감독원이 사기이용계좌의 금융기관에 지급정지 요청

### 끝마치며

- ◆ 첫째도 예방!! 둘째도 예방!! 셋째도 예방!!
- ◆ 절대 당황하지 마세요!!
- ◆ 혹시라도 송금한 뒤엔 최대한 빠르게 도움 요청!!

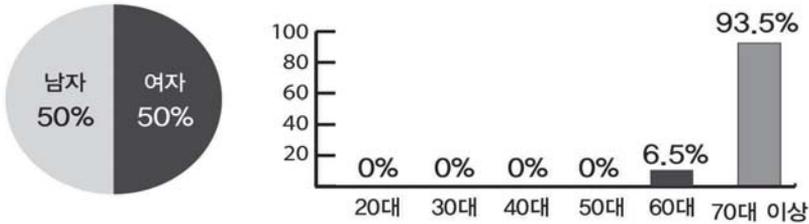
### [3] 보이스피싱 교육 만족도 조사

#### 1. 설문 개요

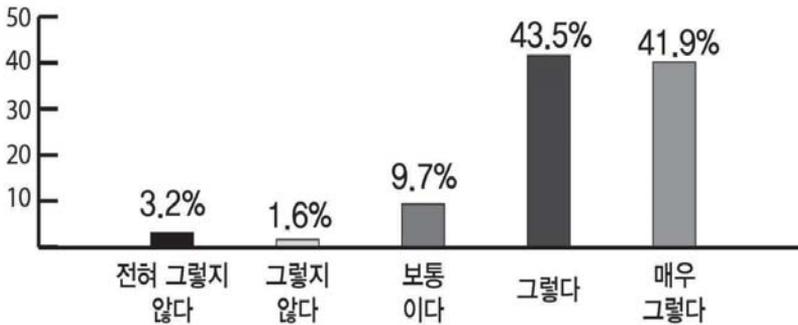
- (조사목적) 새로운 유형의 금융사기 증가로 추가적인 피해를 막고자 전화금융사기피해 예방을 목적으로 교육을 실시하였고 효과적인 교육 커리큘럼 반영을 위한 교육 대상자에게 만족도 설문조사를 실시
- (조사기간) 2017년 11월 22일부터 30일 까지 실시
- (표본 수) 62부
- (설문항목) 보이스피싱 교육의 전반적 만족도, 교육의 집중만족도, 교육시간의 적정성, 보이스피싱 범죄유형에 대한 인식, 보이스피싱에 대한 대처 방안 등

#### 2. 설문 분석

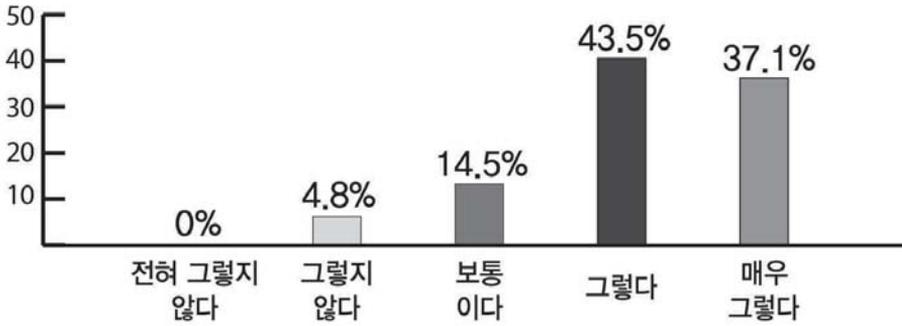
[성별 및 연령대]



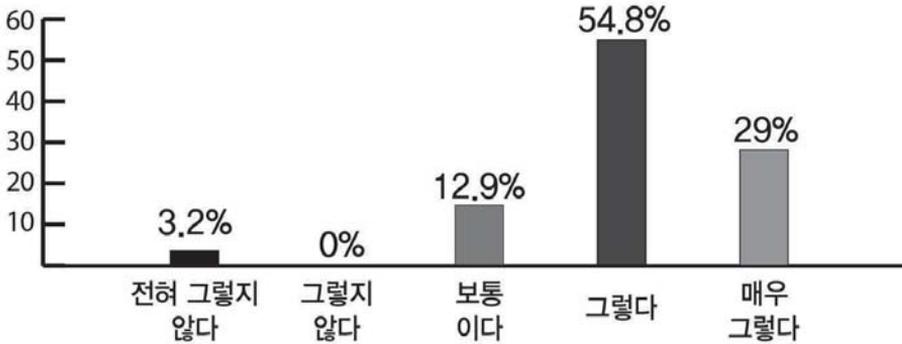
[교육은 전반적으로 만족스러웠다]



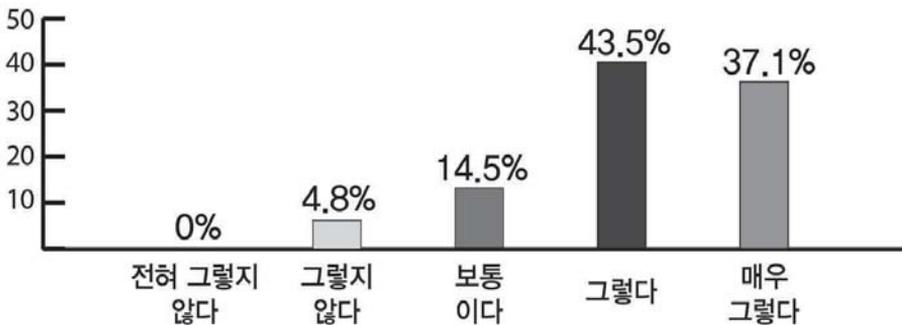
[교육은 전반적으로 재미있었다]



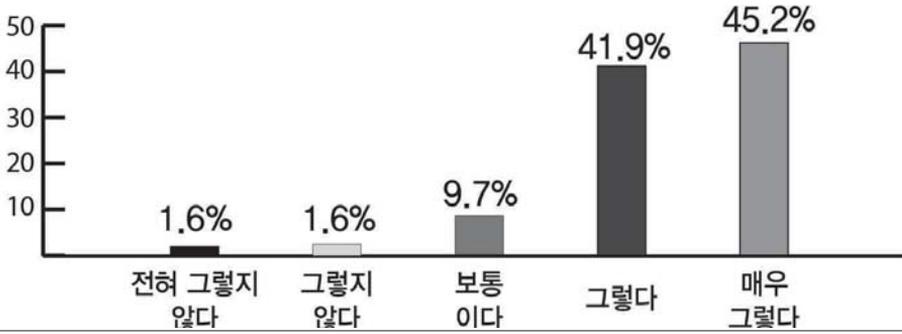
[교육시간이 적절하였다]



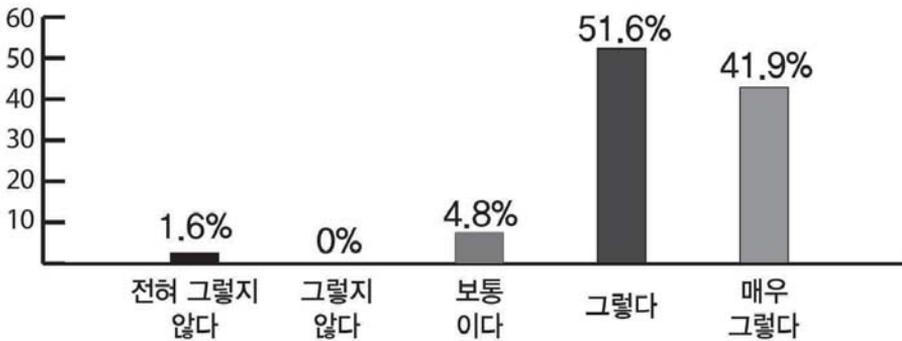
[교육을 다른 사람들에게 추천하고 싶다]



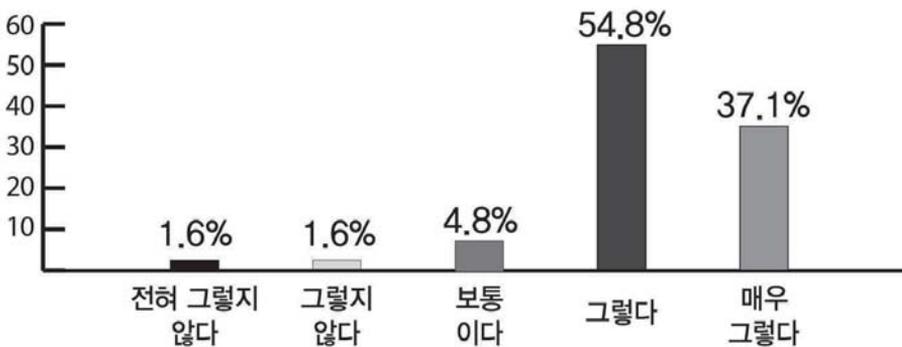
[교육을 통해 보이스피싱의 대처 방안을 알게 되었다]



[나도 보이스피싱의 피해자가 될 수 있다는 것을 알았다]



[향후 관련 유사교육에도 참여의사가 있다]



#### [4] 회의록

제 목	시민안전을 위한 전화금융사기피해 예방 전문가 콜로키움
일 시	2017년 11월 20일(월) 14:00~16:00 / 대전준법지원센터 5층 대회의실
참석자	<ul style="list-style-type: none"> <li>▶ 대전광역시의회 김동섭 의원</li> <li>▶ 대전준법지원센터(2)             <ul style="list-style-type: none"> <li>- 대전준법지원센터 성우제 소장 외 1명</li> </ul> </li> <li>▶ 대전세종연구원(3)             <ul style="list-style-type: none"> <li>- 이형복 책임연구위원 외 2명</li> </ul> </li> <li>▶ 발표 및 토론(6)             <ul style="list-style-type: none"> <li>- 대전대학교 임창호 교수 / 한국금융범죄예방연구센터 이기동 소장</li> <li>- 치안정책연구소 강용길 교수 / (주)인사이트코리아 박경식 이사</li> <li>- 대전중부경찰서 CPO 심국보 팀장 / 대전지방경찰청 김수환 경감</li> </ul> </li> </ul>
회의 내용	<ul style="list-style-type: none"> <li>○ 대전대학교 경찰학과 임창호 교수             <ul style="list-style-type: none"> <li>- 지자체의 예산 및 제도적 지원을 통한 교육환경의 구축이 필요</li> <li>- 효율적인 보이스피싱 범죄피해를 막기 위해서는 예방·홍보활동을 지속적으로 실시하되 맞춤형 교육(연령·계층·성별 등)의 콘텐츠를 세분화 하여 실시할 필요가 있음</li> </ul> </li> <li>○ 한국금융범죄예방연구센터 이기동 소장             <ul style="list-style-type: none"> <li>- 보이스피싱 범죄의 핵심 수단인 대포통장 및 대포폰을 적극차단 할 수 있는 법적 처벌 및 단속체계의 수위를 높여야함</li> <li>- ‘발신번호 조작기술’에 대한 제도적 방지 기술과 법적 규범을 재정립할 필요가 있음</li> </ul> </li> <li>○ 대전지방경찰청 수사과 김수환 경감             <ul style="list-style-type: none"> <li>- 보이스피싱은 전반적으로 사회취약군을 대상으로 범죄가 증가하고 있으며 이에 대한 대전을 중심으로 피해상황의 자료를 취합하여 범죄 패턴을 분석하고 있음</li> <li>- 현재 보이스피싱 현행범으로 검거되는 범죄자들은 송금액·전달책이 대다수이며 이 중에서도 본인이 범죄에 가담한 사실조차 모르는 피해자들이 속출하고 있음(보안인식 및 범죄유형 파악 필요)</li> </ul> </li> <li>○ 대전중부경찰서 CPO 심국보 팀장             <ul style="list-style-type: none"> <li>- 제1·2금융권과 경찰의 협력체계를 구축하여 사기피해로 인한 예금거래시 중간에서 신속한 차단이 필요하며, 현재 개인정보유출이라는 명분으로 금융권의 협조가 미약함(조례를 통한 제도적 기반이 필요)</li> </ul> </li> </ul>
증빙 자료	

제 목	보이스피싱 교육전문가 발표 및 간담회
일 시	2017년 11월 28일(화) 10:00~12:00 / 대전세종연구원 4층 회의실
참석자	<ul style="list-style-type: none"> <li>▶ 대전세종연구원(3) <ul style="list-style-type: none"> <li>- 이형복 책임연구위원 외 2명</li> </ul> </li> <li>▶ 자문위원(3) <ul style="list-style-type: none"> <li>- 수원준법지원센터 배점호 소장</li> <li>- 대전준법지원센터 임성숙 계장</li> <li>- 국민생활안전교육원 김종학 원장</li> </ul> </li> </ul>
회의 내용	<ul style="list-style-type: none"> <li>○ 수원준법지원센터 배점호 소장 <ul style="list-style-type: none"> <li>- 행정적 차원에서의 효율적 보이스피싱 교육 방안으로는 각 계층에 맞는 범죄 유형의 인과관계 패턴을 면밀히 분석하여 보편적인 교육 자료를 제작하여 적극 반영해야 됨</li> <li>- 시민 및 지자체의 전반적인 의견들을 반영하여 보이스피싱 관련 조례를 만들고, 조례를 통해 컨트롤 타워의 역할을 수행하여 균형있는 활동의 기틀을 만들어야 됨</li> <li>- 보이스피싱 교육 및 홍보에 있어 넓은 타겟에 초점을 맞추어 포괄적 범위를 설정하는 것 보다는 ‘정보소외계층’에 초점을 맞추어 헌법적 차원에서의 ‘시민의 알 권리 충족’을 적극 실현해야 됨</li> <li>- 시민의 역할에 있어서 교육 참여에 적극적인 태도로 임하여 민관이 더욱 상호 보완할 수 있는 네트워크를 유지해야 됨</li> </ul> </li> <li>○ 대전준법지원센터 임성숙 계장 <ul style="list-style-type: none"> <li>- 보이스피싱 범죄의 근본적인 취약요소(개인정보, 통장개설, 취약한 보안인식)를 보완할 수 있는 교육 내용이 중점이 되는 자료를 통해 사전에 예방할 수 있는 공익광고 방영을 통해 효율성을 극대화 할 수 있음</li> <li>- 범죄에 쉽게 노출될 수 있고, 자주적 판단이 미숙한 청소년들을 위한 보안의식 교육프로그램을 개발하여 보이스피싱 범죄로부터 올바른 판단력을 갖도록 증진시킬 필요가 있음</li> </ul> </li> <li>○ 국민생활안전교육원 김종학 원장 <ul style="list-style-type: none"> <li>- 고령자를 위한 교육도 중요하지만 금융대출을 많이 하고 있는 30대~40대를 대상으로 하는 교육도 필요함</li> <li>- 짧은 시간에 인팩트 있는 교육을 하는 것이 중요. 교육은 즐거움!</li> </ul> </li> </ul>
증빙 자료	