디지털 경제의 신뢰 기반 조성을 위한

# 보이스피싱 척결 종합방안

2020. 6.

관 계 부 처 합 동

# 목 차

# Ⅰ. 추진배경

□ 정부는 **'혁신적 포용국가'** 구현을 위해 **디지털 기반 혁신성장**과 함께 **포용금융, 인간안보**(Human security) 등의 **정책**을 추진해 왔음

○ 그러나, 이러한 **정책 추진의 이면**에서 **디지털 신기술**을 악용한 **신종수법**에 따른 **보이스피싱 범죄**의 피해가 **심각**한 상황

- 특히, **스마트폰 사용이 대중화** 되는 등에 따라 **대포폰, 악성앱** 등 **통신서비스 부정사용이 증가**

□ **보이스피싱**은 개인 뿐 아니라 **가족까지도 파괴**하고, 나아가 **금융·통신 인프라**에 대한 **신뢰를 저해**하는 **사회적 문제**

○ **금융회사**는 **디지털금융 리스크 관리** 차원에서, **통신사업자**는 **통신서비스 부정사용 방지 차원**에서 각각 대응 중

○ 정부는 **관계부처가 협력**하여 **피해구제, 금융회사**에 대한 **관리감독** 강화 등으로 **보이스피싱 대책**을 시행 중 ('18.12월~)

□ **민간사업자·정부의 대응 노력, 코로나19 상황** 등으로 **'20년 4월까지는 피해가 감소***하고 있으나 **[참고 1]**

* (전기통신금융사기 피해) ('19.1~4월) 2,177억 → **('20.1~4월) 1,220억원 (43%↓)**
[금감원, 피해구제 접수 기준, 잠정] **[참고 2]**

○ **범죄수법·수단** 등이 **지능화·고도화**됨에 따라, **개별 분야**에 **한정되지 않고 종합적**이고 **지속적인 강력대응**이 필요한 상황

□ **대통령**께서도 **반부패정책협의회**('20.6.22일)에서 **보이스피싱**과 같은 **민생침해 범죄**에 대해 **초기부터 강력하게 대응**하고,

○ **부처 간 공조를 강화**하여 **신속하게 대책**을 마련할 것을 지시

※ **국무총리께서**도 **보이스피싱** 등 민생침해 금융범죄에 대해 **강력대처**할 것을 지시 ('20.1.23, 국정현안점검회의)

## 참고 1 보이스피싱에 대한 관계부처 대응 현황

□ 관계부처 합동*으로 **보이스피싱 종합대책을 마련**하여 **이행 중**

* 금융위, 과기정통부, 법무부, 외교부, 방통위, 경찰청, 방심위, 금감원 등

❶ **(사전 예방) 전화·SMS 및 신종수법** 차단, **금융회사의 책임 강화** 등

(i) **(전화·SMS)** 보이스피싱 **전화번호 이용중지 기간 연장**(90일 → 1~3년), **대포폰 차단**을 위해 **휴대전화 가입자에 대한 전수조사** 실시(~'20.1월) 등

* '19년 휴대전화 가입자 전수조사 결과 : 약 40만개 회선 이용정지·해지 등 후속조치

(ii) **(신종 수법)** 다양한 **신종 수단**에 대해 **맞춤형 대책**으로 대응

- **악성 앱** 모니터링 실시('19.1월, 금보원) → '20.5월까지 약 50,126개 탐지
- **메신저 피싱** 위험메시지 수신시 경고 표시를 개선('19.1월)
- 은행권의 **가상통화 취급업소에 대한 관리 강화**('19.7월~, 지연이체 72시간 등)

(iii) **(금융회사의 책임 강화)** 사기이용계좌에 대한 **금융회사의 관리 책임 강화**

- 현재 **신규계좌**만을 대상으로 하는 **개선계획 제출 명령** 기준을 **'모든 계좌'** 로 확대('19.10월, 시행세칙 규정개정 예고 → '20.1월 시행)
- **사기이용계좌 명의인 정보 공유 기간**을 **1년 → 3년**으로 확대('19.11월, 감독행정)
- **은행 모바일 앱**에 **보이스피싱 방지 기능**을 자율적으로 도입('19.7월~)

❷ **(사후 제재 · 단속)** ①**대포통장 양수도·대여 처벌 강화**(징역 3년→5년), ②**보이스피싱 범죄자 전자금융거래 제한 강화** 입법 완료*

* ①「전자금융거래법」, ②「통신사기피해환급법」 개정안 통과('20.4월, 전해철의원안)

- 경찰은 **전담수사체제 강화 및 보이스피싱 특별단속 실시**('19.5~10월)

❸ **(홍보)** 공익광고, 전국민 문자메시지 등 다양한 채널을 통한 **보이스피싱 홍보 및 교육** 실시

□ 한편, **코로나19 상황**에서 **금융·통신·수사당국의 협업**을 강화하여 보이스피싱에 대응 → **'20.1분기 보이스피싱 피해 감소**

① **과기정통부·금융위·경찰청 공동**으로 **'코로나19 허위문자'**에 대한 **주의보를 발령**, **코로나 피싱 전화번호**에 대해서는 **신고**시 **즉각 차단 실시**('20.2.17, 공동 보도참고)

- **과기정통부는** 한국인터넷진흥원(KISA) 內 **24시간 스미싱 상황반** 설치·운영('20.2월~)

② **금융위 주관 컨퍼런스 콜**을 통해 **"코로나19" 보이스피싱**에 대한 **금융회사**의 상시 모니터링을 강화하고, **관계부처**(과기정통부·경찰청 등)**와 전화번호 차단·수사·단속 관련 협조체계를 강화**하여 대응 ('20.2.28일, 공동 보도자료 배포)

# Ⅱ. 피해 현황

## 1. 최근 보이스피싱 피해 현황 ※ [금감원 통계]

◈ '19년까지 **보이스피싱**(전기통신금융사기) **피해는 지속 증가**하는 추세였으나, **금년**에 **감소 추세**로 전환

* (총피해액) '17년 2,431억(26.4%↑) → '18년 4,440억(82.6%↑) → '19년 6,720억(51.3%↑)

### (1) '20년 1~4월 전기통신금융사기 현황 [금감원, 잠정]

◇ **총피해액 : 1,220억원** → 전년 동기(2,177억원) 대비 약 **43% 감소**

◇ **총 피해건수 : 13,084건** → 전년 동기 (26,053건) 대비 약 **49% 감소**

◇ **건당 피해액 : 932만원** → **전년**(건당 927만원) **대비 0.5% 증가**

□ **금융회사에 접수**된 **전기통신금융사기 피해액**은 전년 대비 **감소**

○ **보이스피싱 종합대책**('18.12월)에 따른 **관계부처 대응 강화**, 금융회사의 **자체 노력*** 등이 있었고,

* 시중은행이 **악성앱** 탐지시 **금융앱이 실행되지 않는** 기능 도입('19.7월~), **대포통장 명의인 정보 3년간 공유**('19.11월~), **사기이용계좌 관리의무 강화**('20.1월, 시행세칙 개정) 등

- **코로나19 상황을 악용한 보이스피싱**에 대해 **관계부처**의 **지속 경보**에 따라 국민의 보이스피싱에 대한 **경각심이 강화**된 바 있으며

* 과기정통부(2. 18), 경찰청(2. 17), 금융위·금감원(3~4월), 지자체(4. 22) 관련 보도자료 등

- **코로나19**로 인한 해외 **보이스피싱 조직 활동 감소** 등도 원인

※ 한편, 금융회사의 피해예방 활동 강화 등에 따라 「통신사기피해환급법」상 **전기통신금융사기가 아닌 대면편취형 사기**는 증가 추세

### (2) 평가 및 시사점

□ 현재 **피해액 둔화 추세**이나, 코로나19 등 **재난상황이 완화**될 경우 **피해 증가** 가능성 → **관계부처 협업을 강화하여 대응**할 필요

## 2. 피해 원인 분석

◈ **보이스피싱 조직의 해외 이전**으로 인해 **검거가 어렵고 국내외 악용**가능한 **대포폰·변작 전화가 활용**되고 있으며, **금융·ICT의 결합**으로 질적으로 달라진 **신종수법** 등이 원인

1 **[보이스피싱 조직의 해외 이전]** 본거지, 콜센터 등이 대부분 국내에서 **해외로 이전** → **수사공조** 등을 통한 **단속에 어려움**

○ 이에 보이스피싱 조직의 **범죄활동 기간**이 길어져 **피해가 증가**

2 **[전화이용 수법 고도화]** 보이스피싱 조직의 **해외 이전** 등에 따라, **국내·외**를 가리지 않고 활용가능한 **대포폰** 및 **전화 변작**이 활용

❶ **(범죄수단 다양화)** 최근 **대포폰 확산**은 명의도용 사실을 인지하기 어려운 **선불폰*·외국인 명의폰****을 **중심**으로 **발생**

* 보이스피싱에 사용되어 차단한 전화번호 중 선불폰 전화번호가 84% 차지('19)
** 외국인 여권·등록증 등을 매입해 대포폰 개통·유통한 일당 검거 사례 매년 발생

- 소위 **'내구제'**(나를 구제하는) **대출**을 조건으로 한 **고의적 명의 대여** 및 다수의 통신사를 이용한 대포폰 **다회선 개통**도 **빈발**

* 통신사 별로 휴대전화 가입 회선수에 제한을 두고 운영 중이나, 한사람의 명의로 통신사를 바꿔가며 휴대전화를 대량 개통하여 악용하는 사례 빈발

- **분실·도난폰** 매입 후 불법·조직적 **개인정보 탈취** 사례도 속출

❷ **(범죄수법 고도화)** 추적이 곤란한 **인터넷전화**와, 해외발신 전화도 국내번호(010)로 변조할 수 있는 **SIM박스*** 등이 보이스피싱에 악용

* SIM박스 : 다른 번호의 유심(USIM)을 최대 256개까지 꽂아 중계장치 등으로 이용

**< SIM 박스 운용 형태 >**

**<참고 : 해외 보이스피싱 조직의 국내 중계소 운영 방식>**


### 3 **[신종 수법 등장]** 금융과 ICT가 결합된 **신종 수법** 등장·확산

**❶ (전화 가로채기)** **악성 앱**을 설치하여 금융회사에 전화를 하더라도 **보이스피싱 조직**으로 **통화가 연결**되는 수법

* 가로채기앱 탐지건수 : 1,825건('17) → 4,223건('18) → 5,855건('19), (KISA)

**❷ (원격제어 앱 악용)** 허위 결제메시지를 전송한 후 **원격제어 앱*을 설치**토록 유도하여 **피해자 휴대폰 금융 앱**에서 **금전 탈취**

* 해당 앱 자체는 PC 등에서 휴대폰에 접속하여 장애해결 등에 이용되는 정품 앱(QuickSupport 등)이나, 동 앱을 범죄조직이 원격제어를 통한 보이스피싱에 악용

- 특히, **휴대폰 원격제어**와 **동시대출이 결합**시 피해가 크게 증가*

* 예) 원격제어앱으로 피해자의 휴대폰을 조작한 후 모바일 금융 앱을 실행하여 다수의 동시대출을 받은 후, 3.2억원의 자금을 탈취 ('19.5월)

**❸ (메신저 피싱)** 카카오톡 등 **메신저 계정을 해킹**하거나 **지인을 사칭**하여 피해자를 속이고 **금전 송금** 등 유도

* (메신저 피싱) ('17) 58억원 → ('18) 216억원 (272%↑) → ('19년) 342억원 (58.2%↑)
→ ('20.1~4월) 128억원 (52.3%↑)

➡ 현재 흐름 지속 시, **국민의 재산상 피해 증가가 지속**되고 **디지털금융과 통신 인프라에 대한 신뢰에 부정적 영향**

- **보이스피싱 피해 방지**를 위한 **근본적 정책방향의 전환과 피해과정 전 단계를** 아우르는 **종합적 대응방안** 마련이 필요

## Ⅲ. 추진 방안

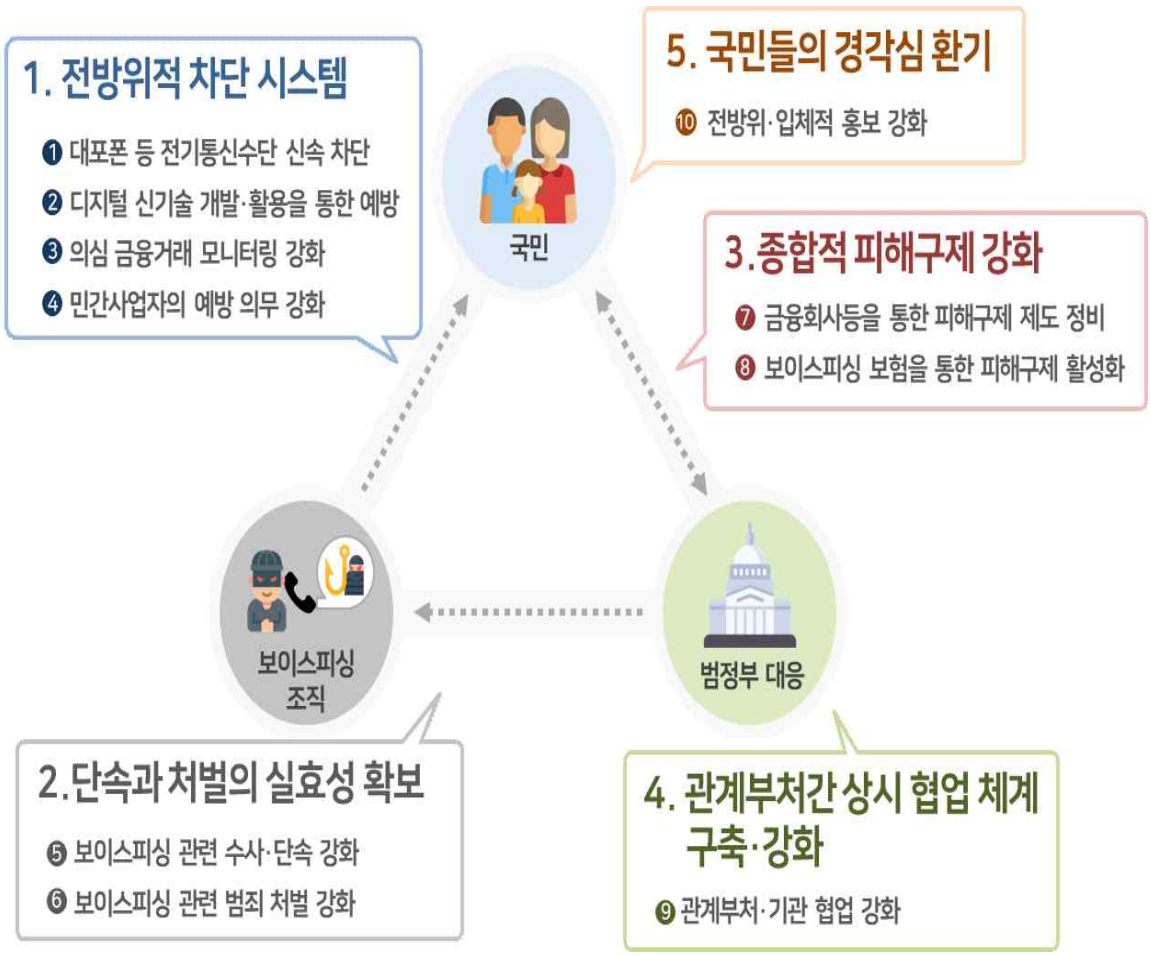
◈ [전략 ❶] 보이스피싱 범죄 시도가 성공하지 못하도록 **전방위적인 예방, 차단 시스템**을 구축

◈ [전략 ❷] 금융범죄의 유인 자체를 없앨 수 있도록 **단속과 처벌의 실효성을 확보**

◈ [전략 ❸] 이미 발생한 피해에 대해 **종합적 피해구제 강화**

◈ [전략 ❹] 집행의 실효성을 높일 수 있도록 **관계부처간 상시 협업 체계를 구축·강화**

◈ [전략 ❺] 보이스피싱에 대한 홍보 강화를 통해 **국민들의 경각심**을 환기



# 1 전방위적 예방, 차단 시스템 구축

## (1) 보이스피싱에 이용되는 전기통신수단 신속 예방·차단

□ **(추진방향)** 통신수단의 **부정사용 자체**를 **방지**하는 한편, **보이스피싱에 이용된 수단**은 **신속·철저히 중지 가능**한 체계를 구축


1 스마트폰 등 **통신수단 부정사용** 자체를 **사전에 방지**하기 위해 **"개통-이용-중지" 단계**에 걸쳐 **신속·종합적 대응체계** 구축

❶ 보이스피싱에 대표적으로 이용되는 범죄 수단인 **대포폰**에 대해 **개통-이용 단계**에서의 **관리감독 강화** (선불폰·외국인 명의폰 중심)

(i) **사용기한 도과 선불폰, 사망자·출국 외국인·폐업법인**의 **未이용회선**을 **정기적으로 일제히 대폭 정리**하고, **정리 주기도 단축**

(ii) **외국인 단기관광객 출국**시 **휴대전화 신속정지**

(iii) 휴대폰 **단기 다회선 개통**시 **가이드 마련** 등을 통해 다회선 개통 억제

❷ 공공기관·금융기관 등을 사칭하는 **전화번호 거짓표시**(변작)를 **사전에 방지**할 수 있도록 차단 체계 구축

(i) 공공·금융기관의 주요 전화번호 **화이트리스트***(변작 차단 목록) **탑재 대폭 확대**(기관 확대 및 현재 대표번호 위주 → 모든 보유번호 단계적 확대)

(ii) **대량 문자발송 대행업체** 등의 신청자 전화번호 확인(위·변조 여부) **절차**를 **강화**하고 **빈도**도 **확대** (최초1회 인증→ 주기적 인증 도입)

(iii) 발신번호 거짓표시(변작) 관련 의무 위반시 과태료 상향(3→5천만원)

* **화이트리스트** : 과기정통부(KISA)에 등록된 전화번호로서, 해당 전화번호로 거짓표시하는 것을 **물리적으로 차단** → 화이트리스트 확대시 사칭전화를 사전에 방지 가능

❸ 보이스피싱에 이용될 가능성이 높은 SIM 박스에 대해서는 **관계부처 협업** 등을 통해 사전에 제거

(i) **SIM박스 밀수** 등 단속을 강화하여 범죄이용을 방지 (관세청 등 협업)

(ii) 국내에 반입된 **SIM박스**에 대해서는 **최신기술 등을 활용**하여 **철저히 단속**(수사기관), **탐지를 고도화**하기 위한 기술도 지속 개발(과기정통부 등)

❹ 휴대폰 등 통신수단이 부정하게 사용되는 것을 방지하기 위한 **대응기반 강화** 및 **건전한 이용 문화 조성**

(i) 휴대전화 도난 방지기능(**Kill Switch**※) 활용 지원을 위해, 휴대전화 개통시, 분실·도난 신고시 이용방법·기능 필수 안내 및 적용 지원

(ii) **국제공조***로 국내 뿐 아니라 **해외**에서도 **분실·도난 휴대전화 원격차단 강화**

* 세계이동통신사업자협회(GSMA)와의 협약(MOU) 통해 분실·도난폰 정보 공유

※ Kill Switch : 스마트폰 운영체제(OS)에 도난관리 SW를 탑재해 분실·도난시 타인의 단말기 사용을 원격으로 무력화(잠금) → 도난폰의 불법사용 방지 가능

## 2 다양한 통신수단(전화번호, 악성앱, 피싱사이트 등)이 보이스피싱 등에 이용된 경우, 신속하게 이용중지·차단하도록 개선

❶ **보이스피싱 피해 신고 후 지체없이 전화번호 이용중지가 가능**하도록 개선 [통상 4~5일(최대 14~15일) → **2일 이내 완료** 목표]

(i) 현행 **피해구제신청서**에 **전화번호 이용중지 신고서식 포함** (금융위)

(ii) **충분한 전화번호 정보 신고**시 보다 신속히 이용중지 조치 (KISA-금감원)

(iii) **스팸 전화번호**(방통위), **전화가로채기 앱 전화번호**(KISA)도 **차단 등 조치** 강화

❷ **이용중지된 전화번호**는 재사용될 수 없도록 보다 **철저하게 차단**

(i) 이용중지된 동일 전화번호는 **타 통신사로 이동하더라도 사용불가** 조치

(ii) **이용중지 기간**도 대폭 확대 (현행 1년 → 1년6개월 이상)

❸ 보이스피싱에 이용되는 전화번호 外 **악성앱·피싱사이트** 등 **신종수단**을 **신속·철저히 차단**할 수 있도록 제도 개선

(i) KISA는 「정보통신망법」 체계·절차에 따른 **악성앱, 피싱·해킹사이트 접속 차단 요청**이 있을 경우 **신속하게 요청 수행**

(ii) **KISA - 금융보안원** 간 **보이스피싱 신종수단 정보 공유 체계 강화**

## (2) 보이스피싱 예방을 위한 디지털 신기술 개발·활용 촉진

□ **(현행) 그간 보이스피싱 예방 기술·서비스** 등은 **개별 기관별**로 보이스피싱 등에 이용되어 **신고된 전화번호**를 **차단**하는 **수준**

➡ **(개선) 신종수법**에 효과적·선제적 대응을 위해, **빅데이터·AI** 등을 **활용**한 대응 기술·서비스 개발 **R&D** 강화

### 1 통신사업자 등이 각종 빅데이터·AI 연계 시범사업 등을 활용하여 보이스피싱 탐지·대응 기술·서비스 고도화할 수 있도록 지원

❶ **빅데이터·AI 기술**을 활용하여 **기존 보이스피싱 방지 기술·서비스 지속적·자율적 고도화** 지원

(i) **통신사·금융권 등의 정보를 통합 활용**하는 한편, **보이스피싱 음성(voice)·문맥(context)에 대한 머신러닝** 기법 적용 등으로 지속적·자율적 고도화 지원

(ii) 보이스피싱 위험이 탐지된 경우 실제로 **은행의 이상금융거래탐지시스템(FDS) 등과도 연계**해 실질적 피해 예방 기여

❷ **통신정보***(통신사) 및 **금융정보****(CB사 등)를 **결합·활용**해 **보이스피싱**을 **판별·예방**할 수 있는 서비스 **신규 출시** 지원

* (통신정보) 로밍, 휴대전화 개통 주소지 정보 등 ** (금융정보) 금융질서문란정보 등

### 2 보이스피싱 유형별로 능동적·선제적 예방 기술 확보 위해 R&D 과제 기획 수행 및 과제화 추진

❶ **금년 중 신종수법**(인터넷전화, SIM박스 등) 및 **해외 동향** 등을 반영해 **R&D 과제 기획** 및 **요소기술 구체화**

❷ 내년 이후 **다부처 협업**으로 **사회문제 해결형 R&D 과제화** → 법·규정 등에 저촉 없이 예방 및 조기 단속 추진

**※ 주요 기술**(예시)

(i) 전통적 통신사업자 경유 대신 글로벌 인터넷 플랫폼 기반으로 사이버 침해 등과 연계된 신·변종 보이스피싱에 대한 능동 대응 기술

(ii) IP 추적 등의 염려 없이 인터넷전화의 해외발신 여부 자동 탐지·고지 기술

(iii) 패턴 분석 등을 통해 SIM 박스 등을 이용한 보이스피싱 추적 기술 등

## (3) 보이스피싱 의심 금융거래 모니터링 강화

□ **(현행) 금융회사나 일정한 전자금융업자**(이하, **'금융회사등'**)는 스스로 **FDS***를 구축하여, **[참고 2]**

* **FDS**(Fraud Detection System) : 금융사기·사고 등을 탐지하기 위한 "이상금융거래 탐지 시스템"

○ 보이스피싱 등 **금융사기나 부정결제 사고** 등 **의심거래를 모니터링·차단 중**

○ 그러나, 현재 금융관련 법령상 **금융회사등의 FDS 구축** 등에 대해 **별도의 법제도**가 **마련되어 있지 않아,**

- **법적 불확실성**이 있을 뿐 아니라, 관련 **인프라·대응체계**도 효율적으로 활용되지 못하는 실정

➡ **(개선) 금융회사**가 **의심 금융거래를 적극 모니터링**하고 **차단 가능**하도록 **법제도·인프라·대응체계**를 구축

---

1 **(법제도)** 빅데이터·AI 등 **신기술을 활용**하여 금융회사 **이상금융거래 탐지시스템**(FDS)을 적극 개선토록 **법제도 정비**를 추진

---

○ **금융회사가 FDS 개선 시 빅데이터·AI 등 신기술을 적극 활용**하기 위한 **법적 불확실성을 해소하고 유인도 부여**

(i) **(데이터 규제 개선) 금융회사등 · CB사**의 **FDS 개발·분석**을 위한 **가명정보***·**빅데이터 활용** 활성화 (개정「신용정보법」 8.5일 시행)

* 추가정보의 사용 없이는 특정 개인을 알아볼 수 없도록 조치된 정보 → '연구' 목적 해당

(ii) **(의심정보 분석 허용)** 빅데이터 기술을 통한 **사기의심계좌 모니터링 업무 지원 서비스**(금결원 혁신서비스 등 포함) **제도화** 추진 (「통신사기피해환급법」 개정)

(iii) **(면책)** 신기술 등을 활용한 **적극적인 의심거래 차단 수행**에 대해 금융회사등 및 그 임직원의 **고의·중과실이 없는 한 면책** (「통신사기피해환급법령」 등 개정)

## 2 **(인프라)** 금융분야 데이터 관련 유관기관의 의심거래 모니터링 지원을 위한 금융사기 방지 인프라 고도화

* (사례) **금융감독원** → 은행권, 한국인터넷진흥원 등과 협업하여 은행권 전화번호 DB를 공유하고, 해당 DB에 없는 전화번호는 신고시 차단('20.1월 시행)

❶ **(신용정보원) 신용정보 집중·활용 강화**를 통해 보이스피싱 방지*

* **신용질서문란자 등록** 제도 개선 / **동시대출의 보이스피싱 악용 방지** 등

❷ **(금융결제원) 빅데이터 기술**을 통한 은행의 **사기의심계좌 모니터링 업무 지원 혁신금융서비스** 지속 고도화 추진 ('19.11월 지정 / '20.5월 시행)

❸ **(금융보안원) 금융분야 ISAC*** 기능을 강화하여 **FDS 고도화 지원, 신종 사기수단 분석·차단**을 위한 **기관 간 정보공유 강화**

* 정보공유·분석센터 (Information Sharing & Analysis Center) → 192개 금융회사 참여

❹ **(신용조회회사) Fraud Scoring* 시스템을 통한 금융회사에 대한 금융사기 방지 업무 지원 기능(Fraud CB)**을 대폭 강화**

* 다양한 신용정보를 기반으로 개인·기업의 금융사기(Fraud) 가능성을 평가
** 예) 가맹점 거래정보를 풍부하게 보유한 **신용카드회사 등**의 **개인사업자 CB 겸업을 허용**(개정 「신용정보법」 旣 반영) → **효율적인 사기방지 서비스** 기대

## 3 **(대응체계)** 현재 금융회사 FDS 고도화*를 위한 협업·기술공유 인센티브 부족** → ❶금융권 공동 컨소시엄을 先구축하고, ❷금융·통신·유통 등 다분야 사기정보 컨소시엄 구축도 추진

* 예) 보이스피싱 위험 거래 탐지 시나리오 개발, 모바일 앱 上 보이스피싱 차단 기능 탑재 등
** 기술·시스템 개발에 기여하는 바 없이 他 금융회사가 개발한 기술 등을 이용할 유인

❶ **FDS 고도화**를 위한 **금융권 공동 컨소시엄**을 **우선 구축**

- **은행연·금보원** 등의 **운영지원**을 통해 **금융회사 간 공동으로 신종수법 사례 분석, 모니터링 기법·차단기술 공유** 등 추진

❷ 금융분야 外 **통신·유통** 등 **다양한 사기정보**를 활용하여 **보이스피싱을 방지**할 수 있도록 **다분야 사기정보 컨소시엄 구축**

- 한편, 동 제도운영 관련, **선의의 피해자가 발생**하지 않도록 컨소시엄 내 **사기 혐의자의 권리 보호를 위한 장치**도 검토

※ **진행중인 연구용역 결과**('19.12월~)를 반영, **「통신사기피해환급법」** 등 **개정 추진**

## 참고 2 이상금융거래탐지시스템 (FDS)

□ FDS(Fraud Detection System)란, 금융거래 과정에서 **금융회사가 수집**하는 다양한 **데이터**를 바탕으로 **이상금융거래를 탐지**하는 시스템

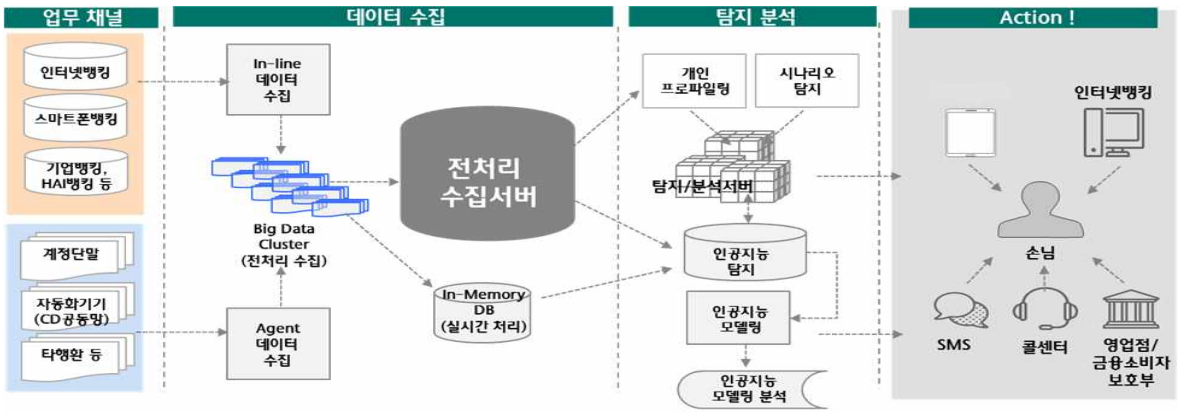
○ 보이스피싱에서는 **거래 단계별로 모니터링**하여 **의심거래를 중지 또는 지연**하는 데 활용

□ 이러한 **FDS 시스템을 강화**할 경우 **보이스피싱 등 금융사기** 뿐만 아니라 **전자금융사고·정보유출 등을 사전에 방지**할 수 있는 확률이 높아지며

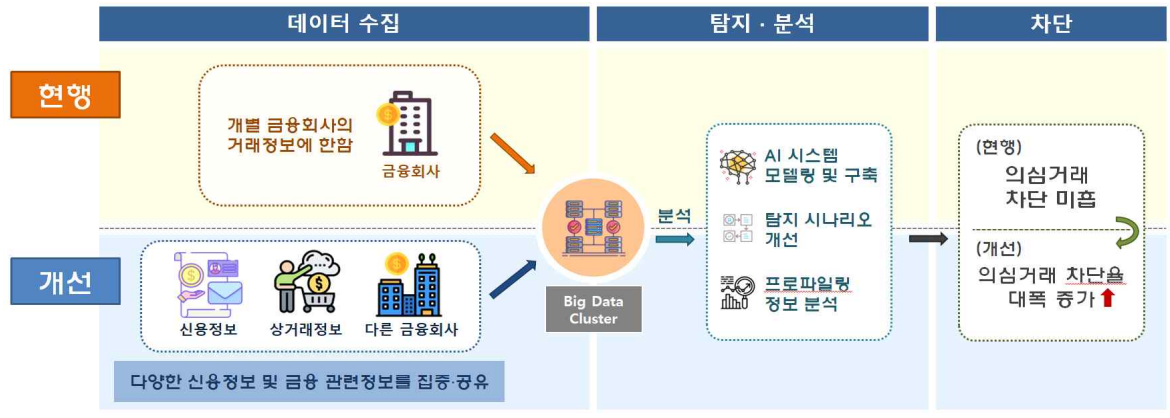
○ **다양하고 정확한 정보**가 집중되고 **기술이 발전**할수록 시스템 정교화를 통해 보이스피싱 의심거래 차단률 증가

→ **빅데이터·AI 활용을 통한 FDS 개발·분석 활성화 추진**

**< 참고 1 : AI, 빅데이터를 활용한 FDS 운영 시스템>**




**< 참고 2 : FDS 개선 방향 및 기대효과>**



## (4) 민간사업자의 예방 의무 강화

### 1 금융회사의 보이스피싱 예방을 위한 의무를 강화

○ **(현행)** 금융회사는 **보이스피싱 의심계좌**에 대해 **자체점검**을 통한 **임시조치** 의무가 있으나, 이를 **준수하도록 유도**하는 **규율이 부재***

* 금융회사는 자체점검을 통한 보이스피싱 피해의심 계좌에 대해 **지연이체, 임시 지급정지 등 조치**를 하여야 함(「통신사기피해환급법」 제2조의5) → **위반시 불이익 없음**

➡ **(개선)** 금융회사가 의심계좌 지급정지 등 **보이스피싱 예방**을 위해 **필요한 의무를 강화**하고, 이에 대한 **법집행도 강화**

❶ **(의무 강화)** 일정한 금융회사에 대해 **이상금융거래탐지시스템(FDS)** 등 **구축 의무화,** 의심계좌에 대한 **자체 임시조치 의무**도 확대

❷ **(법집행 강화) FDS 시스템 구축이 미흡**하여 **보이스피싱 피해**가 크거나 자체 **임시조치 의무 이행**이 미흡 시 **시정·제재*** **조치**

* 금융회사에 대한 주의·경고, 과태료 부과 등

※ **「통신사기피해환급법」 등 개정**을 통해 추진

### 2 통신사업자 자체 모니터링·제재 등 보이스피싱 예방노력 강화

○ **(현행)** 통신사의 다양한 **통신수단 부정사용 방지 의무***는 규정되어 있으나, 보이스피싱 예방을 위한 **자체 조치**는 **부족**한 측면

* (전기통신사업법) 전화번호 변작 금지, 휴대폰 명의도용·부정가입 방지시스템 구축 등

➡ **(개선)** 통신 유통망에 대한 **자체 모니터링·제재** 및 **수범사례 공유** 등을 통한 **통신사업자의 자율정화 노력 확대 유도**

**※ 주요 수범사례**

(i) 과거 케이스 축적·분석 통해 발신 전화번호에 보이스피싱 의심표시 제공
(ii) 이상징후(단기 다회선 개통, 발신번호 집중 변경 등) 체크리스트 운용
(iii) 관련 지침 배포 및 미준수점에 대한 패널티 부과(대리점 계약서 반영) 등

※ **통신사업자 약관 반영, 필요시 관련법령 개정** 등 검토 (관계부처 추가 협의)

## 2 단속과 처벌의 실효성 확보

### (5) 보이스피싱 관련 수사·단속 강화

□ **(현행) 수사기관은** 보이스피싱 범죄 관련 **단속을 지속 강화**하고 있으나, **범부처 일제 수사 및 단속**은 아직 미흡한 상황

➡ **(개선) 관계부처 합동으로 보이스피싱 관련 범죄 일제 단속**

1 **(범죄 수사·단속)** 보이스피싱 관련 범죄에 대해 **엄정한 단속**이 이루어질 수 있도록 **일제 수사** 등 **법집행 강화**

❶ 대책 발표와 함께, **연말까지 보이스피싱 등 불법금융행위 유관기관***이 **일제히 집중단속** 실시

* (경찰) 지능범죄수사대(688명), 광역수사대(624명) 등 / (금감원) 불법금융 단속전담팀 운영

❷ **국내·외 기관**과 **연계·협업**을 통한 **보이스피싱 범죄 단속 강화**

(i) 보이스피싱 조직이 주로 **본거지**를 두고 있는 **해외**에 대한 **국제 수사 공조체계 구축·강화** (대검찰청·경찰청)

* 해외 국가와 MOU 체결 등을 통해 보이스피싱 수사기관간 핫라인 구축, 수사자료 및 정보 제공

(ii) 경찰청·지방경찰청 소속 **보이스피싱 범죄 전담 인력을 지속 확대**하고, 금융회사와 연계하여 보이스피싱 범죄 **집중단속** 실시 (경찰청)

(iii) 최근 증가하는 **메신저 피싱에 대해 집중 수사**를 실시하고, **SIM박스** 등 밀수 단속 등도 강화 (관세청 협업 등)

→ **단속·적발된 각종 불법혐의**는 불법행위별 관련된 법조항*을 **엄격히 적용**, 허용가능한 **최대수준**으로 **처벌·처리할 방침**

* (보이스피싱 관련) 통신사기피해환급법, 전자금융법, 전기통신법, 정통망법 등

2 **(유관업체 점검)** 일제단속기간 중 **통신사업자 등 점검 강화**

○ **과기정통부**는 금융사기 등에 악용될 수 있는 **대량문자 발송 대행업체** 및 일부 **설비임대 통신사**(舊 별정통신사) **집중 점검**

→ **위법사항 적발 시 엄중하게 제재** 예정

* 문자 발송 의뢰자에 대한 본인확인 의무 및 전화번호 거짓표시(공공·금융기관 등 사칭) 방지 위한 기술적 조치 의무 위반 여부 등에 대한 단속·제재

## (6) 보이스피싱 관련 범죄 처벌 강화

□ 보이스피싱 범죄가 **디지털 금융·통신 인프라에 대한 신뢰를 저해**하는 등 일반 사기범죄에 비해 **중대한 범죄**임을 감안,

○ **보이스피싱 및 이와 관련된 범죄**를 보다 **무겁게 처벌**하여 **경각심**을 높이도록 추진

### 1 보이스피싱의 통로인 대포통장 범죄 처벌을 대폭 강화

○ 관련 내용의 「전자금융거래법」이 '20.4월말 국회를 통과하여, **'20.8.20일부터 시행** 예정

(i) **대포통장 양수도·대여** 등의 행위에 대한 **처벌(법정형) 강화** :
'징역 3년, 벌금 2천만원' → **'징역 5년, 벌금 3천만원'** 으로 상향

(ii) **범죄**(보이스피싱 등)**에 이용될 것을** 알면서 **계좌 관련 정보**를 **제공·보관·전달·유통**하는 행위도 **대포통장 범죄 수준으로 처벌**

### 2 보이스피싱 조력 행위에 대해서도 처벌 규정 신설

○ **보이스피싱 단순 조력 행위에 대한 처벌 규정을 신설**하여, **다수의 국내 송금·인출책 범죄**에 **대한 경각심 강화**

* 예)범죄에 이용할 목적으로 또는 범죄에 이용될 것을 알면서, 전자금융거래를 통해 타인으로부터 자금을 교부받아 전달한 자 또는 해당 행위를 도운 자

### 3 보이스피싱 범죄 자체에 대한 처벌도 대폭 강화

○ 관계부처와 협의하여 **보이스피싱 및 유사 금융사기 범죄**의 **법정형을 대폭 강화**하는 방안도 검토

※ 그 밖에 **대포통장 등 보이스피싱 관련 범죄행위를 일관되게 규율**할 수 있도록 **「통신사기피해환급법」 개정**하는 방안을 검토· 추진

## 3 발생한 피해에 대해 종합적 피해구제 강화

### (7) 금융회사등을 통한 피해구제 제도 정비

□ **(현행)** 보이스피싱 발생시 피해자의 **피해구제신청**을 거쳐 **사기이용계좌를 신속히 지급정지**하여 **피해금 환급**이 가능 **[참고 3]**

○ 이러한 지급정지 제도에 **일정한 사각지대**가 있을 뿐만 아니라,

○ **피해금 환급**을 넘어 **금융회사등이 직접 배상책임**을 지는지 **여부가 불분명**함

➡ **(개선) 지급정지제도 및 피해배상 제도를 개선**하여 **금융소비자를 두텁게 보호**

1 **(지급정지제도 정비)** 금융회사등이 **사기이용계좌**에 대해 **충분한 지급정지 조치**를 **시행·유지**할 수 있도록 제도를 정비

❶ 금융회사가 **보이스피싱 의심계좌**에 대해 **자체 지급정지**를 하여도, **'본인이 자금이체 한 것이 확인'** 시 **지급정지를** 해제하여야 함

→ 보이스피싱 의심계좌에 대해 **금융회사가 자체 판단**으로 **지급정지를 지속**할 수 있는 **근거를 명확화**

❷ **간편송금업자** 등 전자금융업자는 금융회사와 달리 **지급정지**와 관련한 **보이스피싱 방지 의무**가 **없으며,**

- 이에 따라 금융회사와 **사기이용계좌 관련 정보**를 **공유**하는데 **한계**

→ **간편송금업자** 등에 대해서도 지급정지 등과 관련하여 일정한 **보이스피싱 방지 의무**를 부과하고, 금융회사와 **사기이용계좌 관련 정보의 공유**를 허용

※ **「통신사기피해환급법」 등 개정**을 통해 추진

### 2 **(배상책임 강화)** 금융회사등의 **보이스피싱**에 대한 **책임**을 강화

○ **(현행)** ①**금융거래시 본인확인을 하지 않은** 경우, ②**수사기관·금감원**의 **정보제공** 또는 **정당한 피해구제신청**이 있었음에도 **지급정지 未이행** 시에만 **배상책임** (→ 인정 사례 거의 없음)

- **보이스피싱의 통로**로 이용되는 **금융회사등**이 **금융인프라 운영기관**으로서 **책임**을 다하도록 개선할 필요

➡ **(개선)** 앞으로는 **보이스피싱**에도 이용자의 **고의·중과실이 없는** 한 **금융회사등이 원칙적으로 배상책임**을 지는 방안을 추진

○ ①피해자가 **'사기·강박'** 에 의해 **거래를 허용**하게 된 점, ②**FDS 구축** 등으로 **사전예방노력**을 **강화**하도록 할 **필요성** 등 고려

- 다만, **금융회사등과 이용자** 간에 **보이스피싱 관련 피해액이 합리적으로 분담**될 수 있도록 기준 마련

* 예) 이용자의 도덕적 해이 방지를 위한 고의·중과실 범위, 손해의 공평한 분담이라는 민사상 기본 원칙 등

※ 현재 진행중인 연구용역 결과('19.12월~)를 바탕으로, 「통신사기피해환급법」 등 개정 추진 (입법예고 과정에서 **금융회사**등의 **의견을 충분히 수렴**)

## (8) 보이스피싱 보험을 통한 피해구제 활성화

□ **(현행)** 보이스피싱 피해를 보상해 주는 **보험상품이 판매 중**이나, **보장 금액이 제한적***이고 **이용도가 낮아** 피해 구제에는 한계

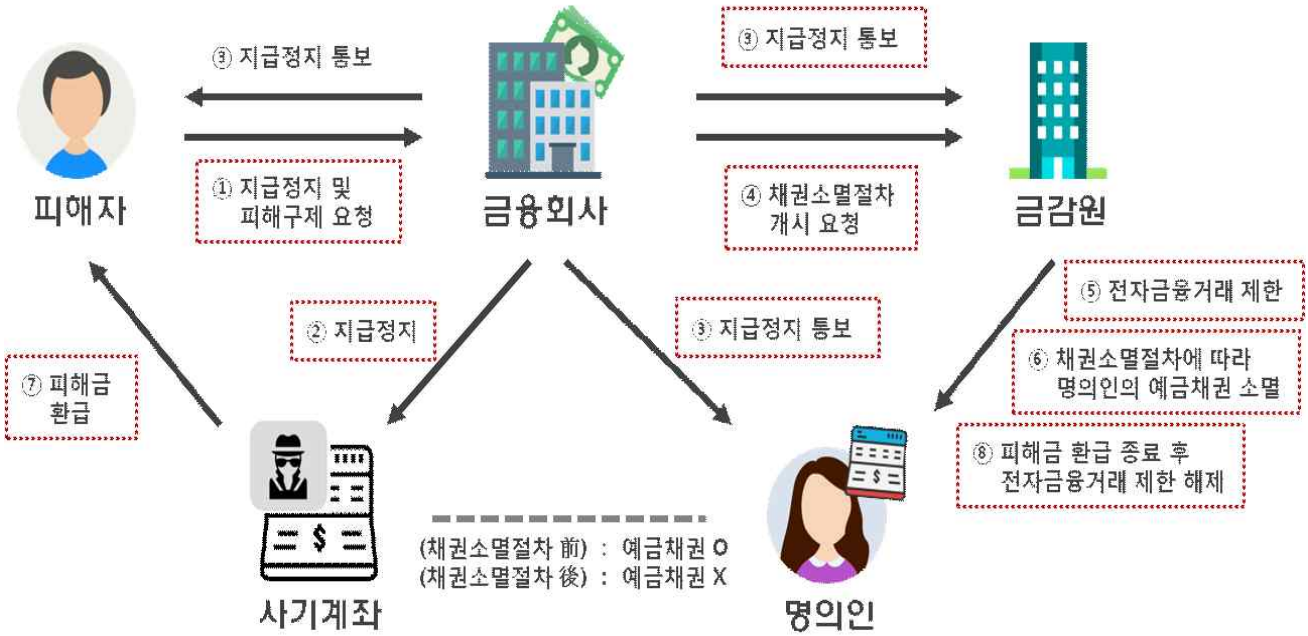
* 현재 최대 보장한도 1천만원 이내 / 보장한도액 5백만원 기준, 월 보험료 300~500원

➡ **(개선)** 보이스피싱 피해 구제 지원을 위한 **보험상품의 보장 범위를 확대**하고 **판매채널 등도 확대**할 수 있도록 추진

- 특히 기존 보험 판매 채널(보험설계사) 뿐 아니라 **통신대리점, 은행 등 금융회사 창구** 등에서 다양하게 해당 상품을 안내

## 참고 3 금융회사의 보이스피싱 피해 구제 절차

※ **지급정지**(금융회사) → **채권소멸절차**(금감원·금융회사) → **전자금융거래 제한 및 피해금 환급**(금감원)




| 절차 | 내용 | 근거법령 |
|---|---|---|
| ① **지급정지 및 피해구제 요청** | 보이스피싱 피해자가 사기범에게 자금을 이체한 계좌(사기계좌)에 대한 지급정지(입출금·이체 금지) 요청 및 피해구제 신청 | 통신사기피해환급법(이하 '법') §3① |
| ② **지급정지** | 금융회사가 보이스피싱 사기이용계좌에 대한 지급정지 실시(입출금·이체 금지) | 법 §4① |
| ③ **지급정지 통보** | 금융회사가 금감원, 명의인, 피해자 등에게 지급정지 사실을 통보 | 법 §4② |
| ④ **채권소멸절차 개시 요청** | 금융회사가 금감원에 사기이용계좌 명의인의 예금채권을 소멸하기 위한 절차 개시 공고 요청 | 법 §5① |
| ⑤ **전자금융거래 제한** | 금감원이 ③에 따라 통보받은 명의인을 전자금융거래 제한 대상자로 지정 | 법 §13의2 |
| ⑥ **채권소멸절차** | ④의 요청에 따라, 금감원이 채권소멸절차가 개시된 사실을 공고 | 법 §5② |
| | (이의제기 등 없을시) 2개월 후 예금채권 소멸 | 법 §9① |
| ⑦ **피해금 환급** | 채권소멸 후 금감원이 14일 내 피해환급금을 산정하여 피해금 환급 결정 → 금융회사를 통해 피해금 환급 | 법 §10① |
| ⑧ **전자금융거래 제한 종료** | 피해금 환급 지급이 종료된 경우 전자금융거래 제한 종료 | 법 §8① |

# 4 관계부처간 상시 협업체계를 구축 · 강화

## (9) 관계부처·기관 협업 강화

□ (현행) **보이스피싱** 수법이 다양한 **ICT 기술**을 바탕으로 **기존의 금융분야**를 넘어 **복잡·교묘**해지고 있으나,

○ 현재 각 기관 소관법령에 근거한 **개별 대응 시스템**으로는 **진화하는 수법**에 맞는 **신속하고 유연한 대응**이 **곤란**한 측면

○ 반면, **해외***의 경우 **관계부처 간 통합적인 대응체계**를 구축하여 **민생을 침해하는 금융범죄**에 **효과적으로 대응**하고 있음

* 예) **대만** → **"反詐欺部署統合 調整會議 및 反詐欺連合防止會議"**를 구성, 산하에 **전담 통합신고센터 등을 운영**하여 금융사기에 종합적으로 대응

➡ (개선) 유관부처간 상시 협업이 가능한 시스템 구축 검토 추진

### 1 금융·통신·수사당국, 민간사업자 공동 대응체계 구축

○ **6월말**부터 **보이스피싱 관계부처 전담 TF**를 **구성·운영**

* 금융위, 과기정통부, 방통위, 법무부, 대검찰청, 경찰청, 금감원, 민간업자 등

- **관련 기관** 간 **중점협약사항 도출** 및 **MOU 체결**도 추진 (3분기 중)

### 2 공동 대응체계 구축을 기반으로 민간업자 간 협업을 적극 지원하고, 정부-민간업자 협업도 강화

❶ **금융·통신당국 : 해외 발신, 변작 전화번호** 등을 사전에 차단하는 서비스 제공* 등을 위한 **금융·통신사 협업을 적극 지원**

* **전기통신사업자는 변작 전화 차단 및 해외 발신 전화번호 안내** 조치의무가 있음 (전기통신사업법 §84의2③) → **해당 조치를 협업 등으로 적극 수행**할 필요

→ **금융·통신 新기술**을 이용한 **신종수법에 효과적·선제적 대응**

❷ **통신당국 :** KISA-금감원-수사기관-통신사 간 **핫라인** 구축

- 과기정통부-KISA 간 정례적 기술협의회를 **기술·정책협의회로 확대개편**하고, **유관기관의 참여**도 적극 유도

❸ **수사당국 :** 보이스피싱 **피해 구제를 가장한 악의적인 피해 신고 방지**를 위해 **허위 피해구제 의심 사건*** 수사를 신속히 처리

* 예) 지급정지를 요청하고 나서 3영업일 내에 피해구제를 신청하지 않은 경우, 소액이 이체된 다수의 계좌에 대해 지급정지를 신청한 경우 등

→ 금융회사의 의심계좌 모니터링 등을 **실제 피해구제·방지에 집중**

# 5 홍보 강화를 통해 국민의 경각심 환기

## (10) 전방위·입체적 홍보 강화

□ **(현행)** 보이스피싱 방지 **홍보 노력**은 **금융부문 중심**으로 한정

○ 이에 따라 ①**금융소비자의 보이스피싱 이해도가 낮을** 뿐 아니라, ②현행보다 **적극적인 홍보**가 필요하다는 의견도 다수*

* ① "검찰·금감원은 돈을 안전하게 보관해준다(35.2%)"는 등 잘못된 인식 ('18.9월, 금감원)
② 보이스피싱 등을 막기 위해 **적극적 홍보**(29.3%) 필요 ('20.1월, 금융소비자보호 인식조사)

➡ **(개선) 대국민 접촉이 많은 관계부처, 지자체** 등을 통해 **전방위적이고 입체적인 대국민 홍보**를 연중 실시

### 1 방송, 광고, 캠페인 등을 통한 입체적인 대국민 홍보 실시

❶ **대국민 접점이 많은 곳**(휴대폰 대리점, 대중교통, 은행창구 등)에서 **보이스피싱 방지 십계명 및 신종수법 사례** 배포, **길거리 캠페인** 실시, **공익광고 송출** 등

❷ **경찰청 홍보예산**(약 7억) 등을 활용하여 **공중파 TV, 유튜브 광고** 등 홍보 강화

- 보이스피싱 수법을 알리기 위한 별도 **유튜브** 등도 운영(금감원 등)

❸ **보이스피싱 수법 소개** 등을 위한 별도 **방송 편성** 등을 통해 **대국민 관심 및 이해도** 제고 추진 (공영방송사 등 협의)

❹ 코리아핀테크위크 「보이스피싱 체험관」(5.28~)을 **연말까지 지속 운영**

### 2 신종수법 수시 경보 발령, 방지 서비스 안내 등을 통한 국민 경각심 강화

❶ **신종수법 출현·피해증가 우려**시 **소비자경보 발령** 및 **경고문자 발송을 위한 체계 구축** (금감원, 통신당국, 통신사 등 협업)

❷ 한편, **보이스피싱 방지 전국민 대상 문자**를 **긴급재난문자처럼 발송*** 하여 경각심을 강화하는 방안도 추진 (행안부)

* (현행) 통신사 협조를 통해 SMS(40자)로만 발송함에 따라 개략적인 내용만 알릴 수 있음 → (개선) 장문의 내용을 재난문자로 보낼 수 있어 경각심 강화

❸ **금융회사**등은 **보이스피싱 피해 예방 십계명, 지연인출제도·지연이체서비스** 등에 대한 홍보도 다양한 채널을 통해 **지속적으로 강화**

* 은행창구, 모바일뱅킹 앱, 홈페이지 등 활용

## Ⅳ. 향후 계획

□ 이상의 **"보이스피싱 척결 종합방안"을 반영**하여 「**통신사기피해환급법**」의 **개정을 추진**

○ 대책 **발표** 후 관계부처 의견 수렴 등을 거쳐 **정부입법**으로 **추진 → '20.3분기 중 입법예고 실시***

*** '20년 말까지 국회 제출** 목표

○ **법 개정 이전**이라도 하위 법규 개정, 법집행 강화 등으로 추진 가능한 과제는 대책 발표와 함께 **우선 추진** ('20.하반기 중)

**<참고 : 「통신사기피해환급법」 개정 필요성>**

□ 「통신사기피해환급법」은 **피해자의 신속한 재산상의 피해회복**이라는 **"이미 발생한 개인의 권리구제"**에 관한 특별법으로 제정('11.3월)

○ 해당 법률에 **"앞으로의 피해 방지에 관한 규율"**을 **단편적으로 추가**함에 따라, **체계적인 피해 방지에 한계**

□ **금융분야의 사후적인 피해구제 위주의** 현행 「통신사기피해환급법」을 **사전예방**과 **통신분야도 규율**함과 동시에, **형사처벌도 강화**하도록 개정

→ **국민의 보이스피싱 피해를 보다 체계적으로 예방 가능**

## 별첨 보이스피싱의 개념과 유형

### 1. 보이스피싱 [ "전기통신금융사기" ] (「통신사기피해환급법」 §2 ⅱ )

□ ①**전기통신***을 통해 ②**타인을 기망·공갈**함으로써 ③**자금을 송금·이체**하도록 하거나, 개인정보를 알아내어 자금을 송금·이체하도록 함으로써 ④**재산상의 이익을 편취**하는 사기·공갈행위

* 유선·무선·광선 및 기타의 전자적 방식에 의하여 부호·문헌·음향 또는 영상을 송·수신하는 것 (전화, SMS, 메신저, 인터넷사이트 등) (「전기통신기본법」 §2 ⅰ )

### 2. 보이스피싱의 유형

□ **(범죄 수단)** 전화통화, 스미싱*(SMS), 파밍**(악성코드), 불법사이트, 악성 앱 등을 이용한 사기 수단이 존재

* 스미싱(SMS+phishing) : SMS(문자메시지)발송을 통해 특정 사이트로 이동 또는 악성코드·악성 앱을 설치하도록 유도하거나, 대출권유 등을 통한 사기행위

** 파밍(Pharming) : PC·모바일 기기 등을 악성코드에 감염시켜 해킹자가 만든 사이트로 강제 이동하도록 하여 개인정보·인증수단을 유출, 금전 편취

○ 다만, 최근에는 여러 수단이 결합된 사기사례*가 다수 발생하여 **범죄 수단이 중복**되는 경향

* 예) SMS 문자 발송을 통해 악성코드에 감염시켜 불법사이트로 이동시키고, 개인정보를 탈취하여 보이스피싱 → 스미싱+파밍+불법사이트 등의 수단이 결합

□ **(범죄 수법)** ①**대출사기형**·②**非대출사기형**으로 분류되며, **보이스피싱 통계**도 범죄 수단 보다는 **범죄 수법에 따라 집계**

* ① **(대출사기형) 전화·SMS** 등을 통해 **대출 상담·알선을 가장**하여, 대출수수료 입금 등의 명목으로 금전을 요구하여 가로채는 수법
② **(非대출사기형)** (i)**사건연루조사**(정부기관 사칭), (ii)**메신저 피싱**(지인 사칭), (iii)**납치협박**(범죄 사칭) 등의 수법이 사용됨

○ 대출사기형은 대출을 빙자하여 **수수료·선이자 등을 요구**하는 행위로 **건당 피해액이 비교적 적은** 경향(건당 피해액 약 784만원)

○ 반면, 非대출사기형은 **피해자를 사기·협박하여 금전을 편취**하는 행위로, **건당 피해액이 높은** 경향(건당 피해액 약 1,360만원)