붙임2 **통신분야 주요 대책(10개) 세부 설명자료(과기정통부)**

◇ 기존 제도를 우회하는 신·변종 수법이 다수 등장함에 따라,

- **제도적 보완**과 함께 **AI·빅데이터** 등을 활용한 **기술적 대응**을 강화함으로써 선제적·예방적 대처에 중점

< 제도적 보완 >

1 대포폰 악용가능성 높은 사망자·폐업법인·외국인 명의 휴대폰 조기 정리

o (현황 및 문제점) 약 5천만 휴대폰 대상 본인확인 전수조사를 연 2회(매 6개월) 실시중이나, 문제회선이 존재할 경우 최장 6개월까지 유지될 수 있고 그간 단기관광 외국인 사용 휴대폰에 대해서는 사후관리가 미흡

* 연 2회 전수조사를 통해 매년 약 40만 회선에 대해 정리중

⇨ **(개선방향) 본인확인 주기를 4개월로 단축하고(20. 하반기부터 연 3회 실시), 법무부(출입국관리소) 등 협조 통해 외국인 단기관광객 출국시에도 정지(즉시)**

* 회선 해지·정지 등을 위해서는 이용자 사전고지 및 일정기간 유예·보장 등이 필수적인 바 4개월이 현실적으로 단축가능한 최단기간에 해당

2 본인확인이 상대적으로 취약한 선불·알뜰폰에 대한 관리·점검 강화

o (현황 및 문제점) 알뜰폰은 비대면·온라인 개통이 일반적으로 특히 선불폰은 일단 개통되면 별도 요금청구 과정 등이 없어 추후 명의도용 여부 확인이 곤란*, 또한 동일인 명의로 통신사를 바꿔가며 대량 개통 사례도 발생**

* 보이스피싱에 사용되어 차단된 전화번호 중 선불폰 전화번호가 80% 이상('19년)

** 그간 통신사별로는 약관을 통해 1인당 3~4회선으로 제한중이나, 통신사를 달리하는 통합 회선수에 대해서는 별도 제한 부재

⇨ **(개선방향) ①비대면 개통시 위조가 용이한 신분증 대신 관련법상 수단(공인인증, 신용카드)에 의해 본인확인할 수 있도록 주의 환기 및 현장점검 강화(즉시)**

②사용기한이 크게 도과된 선불폰부터 주기적 검증 통해 퇴출 유도(즉시)

③단기간에 다회선 개통 관련가이드 마련 및 이통3사 통해 자사 망을 이용중인 알뜰폰에도 적용함으로써 통합 관리(4분기)

3 공공·금융기관 전화번호 사칭 방지 노력 확대

o (현황 및 문제점) 범죄자의 공공·금융기관 전화번호 사칭을 막기 위해 주요 전화번호에 대해서는(112 등) 위·변작 금지 목록(DB)화(KISA(한국인터넷진흥원)) 하여 통신사와 공유중이나, 대표번호 위주로 되어 있어 한계 노출

* 공공·금융기관 사칭 전화번호 차단은 지속 증가 추세 : ('17년) 34 → ('19년) 59백만건

⇨ (개선방향) 해당 공공·금융기관과 협력해 모든 보유번호를 대상으로 위·변작 금지 목록(DB) 추가 지속 확대(계속)

4 해외발신 인터넷전화의 국내전화, 일반전화의 010번호로의 허위표시 단속 강화

o (현황 및 문제점) 회선설비 보유 기간(주요) 통신사를 통한 전화번호 변작(거짓·허위 표시)은 현저히 줄었으나, 회선설비에 연결해 서비스를 제공하거나 회선설비를 임대하는 영세사업자(舊 별정 및 특수부가*)를 통한 변작은 여전

* 주로 대량 문자발송 대행업체로 스미싱(문자(SMS)+피싱)을 통한 보이스피싱과 연계

⇨ (개선방향) ①영세사업자 대상 계도(설명회 등) 및 집중 단속 병행(즉시)
②특수부가사업자의 문자발송 서비스 신청자에 대한 확인의무 강화(고시 개정, 3분기)
③변작 의무 위반 사업자에 대한 과태료 상향(최대 3 → 5천만원)(시행령 개정, 연내)
④특히 국내개통 인터넷전화(국내번호)로 해외에서 발신하는 경우에도 국외발신 표시 추진(주요 사업자부터 단계적 시작, 연내)

5 보이스피싱 등 범죄 이용 전화번호에 대한 신속·철저한 이용중지

o (현황 및 문제점) 경찰청·금감원 등의 요청에 따라 보이스피싱 등 범죄에 이용된 전화번호 이용중지를 시행중이나, 요청에서 이용중지까지 소요기간 과다(평균 3~5일), 타 통신사로 이동시 재사용 가능, 보이스피싱 외 스미싱에는 적용 제한 등의 문제 지적

⇨ (개선방향) ①절차 간소화·자동화 통해 처리기간 단축(1일* 이내 목표)
(주요 사업자부터 단계적 시작, 연내)
②이용중지된 전화번호는 타사로 번호이동시에도 이용 불가 조치(지침 개정, 즉시) 및 이용중지 기간도 확대(약관 반영, 1년→1년 6개월 이상)(3분기)**
③KISA(한국인터넷진흥원)(스미싱 탐지)·금감원(이용중지 요청) 등과 협력 통해 스미싱에 이용된 전화번호도 이용중지 실시(즉시)

* 법령에 따른 이용중지 전 이용자 고지절차 등을 감안

** 통신사에 의한 전화번호 이용중지 전 이용자 스스로 정지 후 번호이동하는 경우도 제한

< 기술적 대응 강화 >

⑹ 각종 시범·확산 사업 활용 보이스피싱 탐지서비스 고도화 및 확산 지원

o (현황 및 문제점) 그간 보이스피싱 방지 앱 등은 **개별 기관별**로 보유한 정보를 활용하는 단계(피싱·스미싱 등에 이용된 것으로 신고된 전화번호 차단 등)

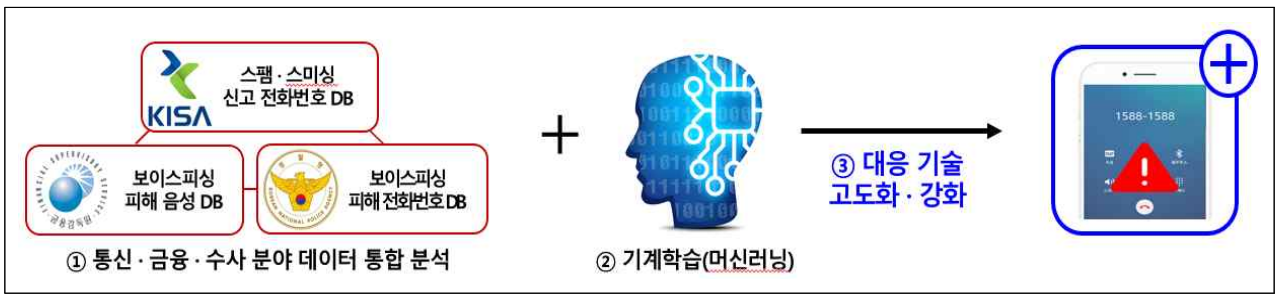
⇨ **(개선방향) ①과기정통부 예산사업 등을 활용해 통신사·금융권 등의 정보를 통합 분석하는 한편, 피싱 음성·문맥 에 대한 기계학습(머신러닝) 기법 적용으로 지속적·자율적 고도화 지원(연내)**

②이를 통해 보이스피싱 위험이 탐지된 경우에는 실제로 은행의 이상금융거래 탐지시스템(FDS) 등과도 연계해 실질적 피해 예방 기여(연내)

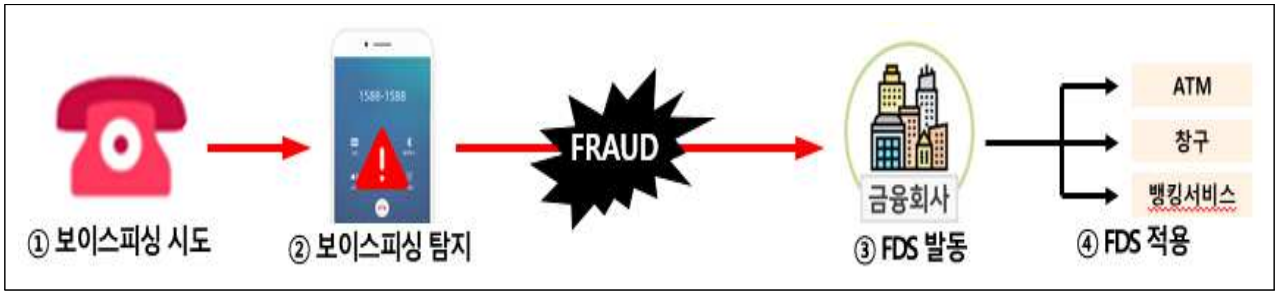
③정부 사업으로 개발된 관련 기술·알고리즘 등은 일반에도 공개해 조기 확산 유도 병행(계속)

* 금년도 “다분야 데이터 결합 통한 빅데이터·AI 기반 실시간 보이스피싱·스미싱 방지 서비스” 개발중(총 예산 : 7.5억원)

< 다분야 데이터 결합·활용 통한 대응 기술 고도화 >



< 은행 이상금융거래시스템(FDS) 연계 방안 >



⑦ 보이스피싱 유형별로 능동적·선제적 예방 기술(R&D) 확보

o (현황 및 문제점) 글로벌을 기반으로 추적 등이 곤란한 인터넷전화, SIM 박스, 악성 앱 등을 활용하는 등 보이스피싱 수법이 날로 지능화·고도화하고 있어 법제도 보완과 함께 기술적 대처를 통한 예방노력 확대가 시급

⇨ **(개선방향) ①금년중 보이스피싱 신종 수법 및 해외 동향 등을 반영해 R&D 과제 기획 수행(연내),**

②최신 기법 대응에 초점을 맞춰 요소기술 구체화(유관부처·기관 대상 수요조사 병행) 및 다부처 협업 사회문제 해결형 R&D 과제 성립 통해 조기 예방 및 차단 지원(내년 이후)

* "ICT 신·변종 수법을 활용한 피싱 등에 대한 AI 기반 대응기술 기획" 과제 발주
  AI 및 머신러닝 알고리즘 등은 세계적으로 피싱 등의 자동 필터에 효과 기대

* 주요 기술(예시)
  - 전통적 통신사업자 경유 대신 글로벌 인터넷 플랫폼 기반으로 사이버 침해 등과 연계된 신·변종 보이스피싱에 대한 능동 대응 기술
  - IP 추적 등의 염려 없이 인터넷전화의 해외발신 여부 자동 탐지·고지 기술
  - 패턴 분석 등을 통해 SIM 박스 등을 이용한 보이스피싱 추적 기술 등

< 기타 >

⑧ 통신과금 서비스(휴대폰 소액결제) 부정이용(일명 '휴대폰 깡', '내구제 대출' 등)* 방지노력 확대

* 급전 필요 청년층·저소득층으로 하여금 휴대폰이나 기타 물품을 구입해 업자에게 넘기고 돈을 빌리는 방식, 업자는 원가보다 싸게 구매 후 중고로 되팔아 수익화

o (현황 및 문제점) 통신과금 서비스를 이용한 부정거래는 결제방식이 정상거래와 동일하고 피해자도 불분명해 적발에 한계가 있는데다, 이렇게 개통된 휴대전화는 대포폰에 악용될 소지가 높음

⇨ **(개선방향) 통신사 및 결제대행사(PG사) 별로 운영중인 고객이력관리 시스템을 연계함으로써 부정이용자에 대한 정보 공유를 강화하고, 저신용자미납이력자의 경우 이용한도(현재 월 100만원) 하향 · 제한 조치(3분기)**

⑨ 휴대전화 도난방지기술(Kill Switch)* 이용 활성화 및 분실·도난폰에 대한 국제공조 강화

* 휴대폰 분실시 관련 사이트(myaccount.google.com/find-your-phone, www.icloud.com/#find)를 직접 방문해 원격제어(데이터 삭제·위치 확인 등) 가능 (안드로이드 계열은 Factory Reset Protect(FRP), iOS 계열은 Activation Lock)으로 명명되며, 설정 → 내 기기 찾기에서 확인 가능)

o (현황 및 문제점) 주요 스마트폰 제조업체는 동 Kill Switch를 기본값으로 설정해 놓고 있으나 홍보 부족으로 이용이 여전히 미흡한 측면, 또한 국내에서는 분실·도난폰으로 가입이 곤란하나 해외에서는 가능한 한계

⇨ **(개선방향) 가입 및 분실신고 시 통신사(유통망) 또는 KAIT (한국정보통신진흥협회) 등을 통해 Kill Switch 기능 및 이용법에 대한 안내를 강화하고(8월), GSMA(세계이동통신사업자협회) 등과 협력해 분실·도난폰의 해외사용 금지 지속 확대(계속)**

* Global System for Mobile Communication Association : 전세계 휴대전화의 IMEI(International Mobile Equipment Identity) : 국제모바일기기식별코드) 생성·부여 단체, 미국·유럽 등과 IMEI 차단목록 공유중, 우리와도 차단목록 공유 업무협약 체결('19. 11월)

⑩ 보이스피싱 유관기관 간 기술적 협력 강화 및 정보·시스템 연계·통합

o (현황 및 문제점) 그간 과기정통부, 통신사, KISA(한국인터넷진흥원) 중심으로 보이스피싱 대응 기술협의회를 운영해 왔으나, 타 부처·기관과의 유기적 연계는 부족한 측면

⇨ **(개선방향) 동 기술협의회를 관계 부처·기관에 개방하는 한편(즉시), 유관기관별로 분산 보유중인 정보·시스템을 연계·통합(연내 착수)함으로써 전반적 보이스피싱 대응역량 확충**

* 예 : 과기정통부(KAIT)가 명의도용 여부를 확인할 수 있도록 운영중인 명의도용 방지시스템(www.msafer.or.kr)을 금융서비스와 연동할 경우, 계좌 개설 또는 대출 시 금융기관에 사전 등록된 휴대폰 및 동일 명의의 모든 휴대폰에 관련 사실 통보 가능 등