

2022 November | Vol. 8

11



# 융합연구리뷰

Convergence Research Review

**팬데믹 시대의 사이버 보안 기술 및 표준화 동향**

이대성(부산가톨릭대학교 컴퓨터공학과 교수)

**개인인증과 보안을 위한 생체인식 센서 기술**

박영삼(한국전자통신연구원 책임연구원)

# CONTENTS

- 01 편집자 주
- 03 팬데믹 시대의 사이버 보안 기술  
및 표준화 동향
- 29 개인인증과 보안을 위한  
생체인식 센서 기술
- 65 국가R&D 현황 분석



융합연구리뷰 | Convergence Research Review  
2022 November vol.8 no.11

**발행일** 2022년 11월 7일

**발행인** 김현우

**발행처** 한국과학기술연구원 융합연구정책센터

02792 서울특별시 성북구 화랑로 14길 5

Tel. 02-958-4977 | <http://crpc.kist.re.kr>

**펴낸곳** 한빛사회적협동조합



### 팬데믹 시대의 사이버 보안 기술 및 표준화 동향

사이버 공격의 유형 중 하나인 랜섬웨어(ransomware)에 감염된 파일 또는 컴퓨터를 복구하기 위한 방법에 대한 내용을 다루는 블로그나 복구업체들의 광고를 인터넷 상에서 쉽게 발견할 수 있다. 랜섬웨어란 몸값을 뜻하는 랜섬(ransom)과 악성코드를 의미하는 말웨어(malware)의 합성어로 사용자의 동의 없이 악성파일을 설치해 컴퓨터를 사용 불가능한 상태로 만들거나 데이터를 암호화해 사용할 수 없도록 한 후, 이를 불모로 금전을 요구하는 악성 프로그램을 일컫는다. 일반적으로 복구업체에서는 잠긴 파일을 해독해서 암호키를 알아낸다고는 하나 고도의 암호로 걸려 있는 경우에는 복구가 어렵기 때문에 백신 프로그램 설치, 최신 버전으로 소프트웨어 업데이트, 출처가 불명확한 이메일과 웹사이트 주소 실행 금지, PC 내 주요 자료 백업 등 사이버 보안을 강화하기 위한 다양한 방법들이 권장되고 있다. 그러나 사이버 공격은 날이 갈수록 빨리 확산될 뿐만 아니라 점차 지능화되고 있어 개인은 물론이고 기업들의 피해 사례도 빈번하게 발생함에 따라 사이버 보안 기술의 중요성이 부각되고 있다.

사이버 보안은 사이버 환경에서 네트워크 운영상의 위험으로부터 조직과 사용자 자산을 보호하기 위해 사용하는 기술적 수단을 의미한다. COVID-19 대유행으로 인한 재택근무 증가에 따라 사이버 보안은 더욱 취약해진 것으로 나타났다. 지디넷코리아 기사(2021년 3월 23일)에 따르면, 글로벌 보안 기업인 트렌드마이크로가 2021년에 탐지한 재택근무자 대상 공격이 전년대비 210% 급증하였고 전체 재택근무자의 15.5%가 사이버 공격을 받은 것으로 나타났다. 본 호 1부에서는 최근의 사이버 위협 및 공격 동향, 사이버 보안 기술 및 표준화 동향에 대해 소개하며 모든 것이 네트워크에 연결되어 있는 초연결 시대에 안전한 사이버 환경을 구축할 수 있기를 기대해 본다.

### 개인인증과 보안을 위한 생체인식 센서 기술

인터넷 시대에 비밀번호는 필수이다. 인터넷 사이트 가입 시 매번 비밀번호를 설정하는 것은 번거로운 일이고 사용하는 계정이 증가함에 따라 복잡한 비밀번호를 기억하는 것은 분명 귀찮은 일임에 틀림없다. 한국인터넷진흥원에서 2020년 2,105명을 대상으로 실시한 '계정관리 보안 실태' 설문조사 결과에 의하면 이용하는 계정의 비밀번호를 모두 동일하게 설정하는 응답자의 비율은 과반이 넘는 58.48%에 달하는 것으로 나타났다. 또한 아이디, 비밀번호를 암기하지 않고 수첩 또는 지갑에 수기로 기재(19.43%)하거나 USB나 스마트 폰 등에 문서로 저장(16.44%), 브라우저에 저장(12.45%), 비밀번호 관리프로그램에 저장(15.82%)하는 응답자의 비율도 64.11%에 이르는 것으로 드러났다. 그러나 이제는 계정에 접속하기 위해 비밀번호를 기억하기 위한 수고를 덜 수 있게 되었다. 우리 몸 자체가 비밀번호가 되는 생체인식 기술 덕분이다.

생체인식 기술이란 사람의 지문, 정맥 패턴, 홍채, 얼굴 등의 신체적 특징과 음성, 걸음걸이 등 행동적 특징을 센서 등을 통해 인식하여 개인을 식별 또는 인증하는 정보 보안 기술이다. 안전성과 편의성으로 인해 최근에는 스마트폰 잠금 해제, ATM 거래, 공항 내 자동출입국 심사 등 활용 분야가 점차 넓어지고 있는 추세이다. 생체인식의 정확도 향상을 위해서는 생체정보를 인식하기 위한 센서의 성능이 특히 중요하기 때문에 이를 위한 연구개발이 활발히 이루어지고 있다. 해킹과 개인정보 유출 방지를 위해 비밀번호를 설정하는 것이 필수인 시대에 본 호 2부에서는 다양한 생체인식 센서 기술 동향을 소개한다.

# 융합연구리뷰

Convergence Research Review 2022 November vol.8 no.11



# 01

## 팬데믹 시대의 사이버 보안 기술 및 표준화 동향

이대성(부산가톨릭대학교 컴퓨터공학과 교수)



# I 팬데믹과 보안 기술 환경변화

현재 사물인터넷(IoT, Internet of Things), 클라우드, 빅데이터, 5G 기술이 기업 업무의 대부분과 생산시설에 활용되면서 산업 전반에 걸쳐 사이버물리시스템(CPS, Cyber Physical System)화가 빠르게 진행되고 있다. 특히 코로나-19 팬데믹(pandemic)의 영향으로 경제·사회 활동도 온·오프 하이브리드 환경으로 전환됨에 따라 클라우드 마이그레이션(Cloud Migration)과 디지털 전환(DT/DX, Digital Transformation)도 급속히 확산되고 있다. 사이버 보안기술도 이러한 사이버 공간의 변화에 대응하여 전통적인 시스템·네트워크보안 영역에서 대체불가 토큰(NFT, Non-Fungible Token), 중앙은행 발행 디지털 화폐(CBDC, Central Bank Digital Currency), 메타버스 등 미래 디지털 경제를 선도하는 영역으로 기술개발 범위를 확대시켜 나가고 있다.

이처럼 팬데믹과 더불어 사이버 공간에 대한 사회·경제활동의 의존도가 급증하면서 해커집단의 사이버 공격 행태도 더욱 전문화·조직화되고 있으며, 이에 대응하기 위한 차세대 사이버 보안 기술의 혁신 노력도 그만큼 더 중요성을 더해 가고 있다.

## 1. 경계 기반 네트워크 보안에서 제로 트러스트 아키텍처(ZTA)로 이행

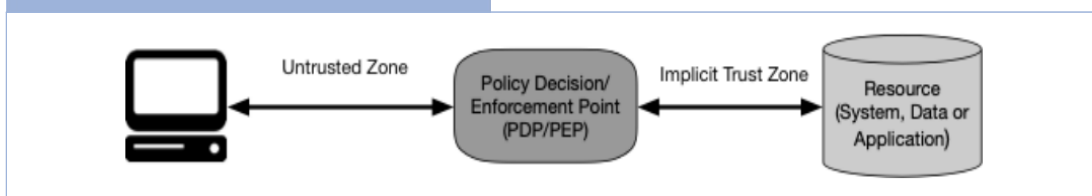
그동안 기업 내 IT 시스템들은 사내 근무 형태의 내부 업무망 이용을 전제로 구축·운영되어 왔기 때문에 방화벽(firewall)이나 침입탐지 시스템(IDS, Intrusion Detection System)과 같은 보안장비를 기준으로 사내와 사외를 경계로 하는 보안 개념이 적용되어 왔다. 하지만 팬데믹 이후 5G 기반의 모바일을 이용한 재택근무, 원격 교육, 멀티 영상회의 등 온택트(ontact) 문화가 일상화되고, 기업 외부에서의 사용자 액세스가 급증하면서 내부 시스템 침입을 시도하는 공격방식도 다양하게 변화되고 있다.

이에 따라 2020년 미국 국립표준기술연구원(NIST, National Institute of Standards and Technology)은 진화되고 있는 사이버 위협과 공격을 신속하게 탐지·방어 조치하고, 보안사고로부터 정상 서비스로 회복하는 사후 조치로 구성되는 새로운 사이버보안 프레임워크인 제로 트러스트 아키텍처(ZTA, Zero Trust Architecture)를 제안하였다. 제로 트러스트란 기업 리소스에 대한 어떠한 액세스 요구도 신뢰하지 않는다는 의미로, 제로

트러스트 아키텍처(ZTA)는 사용자 ID를 계속해서 검증하여 시스템 사용에 대한 리스크를 최소화하는 기술적 개념이다.

제로 트러스트 아키텍처(ZTA)에서는 <그림 1>과 같이 정책 결정 포인트(PDP, Policy Decision Point)와 정책 집행 포인트(PEP, Policy Enforcement Point)를 통해 기업 리소스에 대한 액세스를 허가하기 때문에, 지역적으로 분산되어 있는 그룹 기업이나 업무 이동성이 강한 직원들을 많이 보유한 기업 또는 외부 기업과 협업을 하는 기업들에서 상대적으로 높은 보안 편익을 보장받을 수 있다(NST, 2020; NST, 2021).

그림 1. NIST의 제로 트러스트 액세스



\* 출처: NIST(2020)

미국 국립표준기술연구원(NIST)이 제로 트러스트 기반의 보안체계를 효율적으로 구축하기 위해 제시하고 있는 실행 프로세스의 주요 내용을 요약 정리하면 다음과 같다.

첫째, 제로 트러스트 아키텍처(ZTA)에 참여하는 식별 주체에는 사람과 사물(NPE, Non-Person Entities)이 모두 포함되며, 개발자나 시스템 관리자 등 특수 권한을 가진 사용자에게 속성이나 역할을 할당할 때는 그들이 비즈니스 요구사항을 만족시킬 수 있도록 충분한 유연성을 허용해야 한다. 또한, 로그 및 감사를 통해 액세스 패턴을 식별할 수 있어야 한다.

둘째, 제로 트러스트 아키텍처(ZTA)의 핵심 요구사항 중 하나는 디바이스를 식별하고 관리하는 능력이다. 여기에는 기업이 소유한 네트워크 인프라에 연결되어 있거나 기업 리소스에 액세스하는 디바이스 중에서 기업 소유가 아닌 디바이스를 식별하고 모니터링해야 한다.

기업 자산은 노트북, 스마트폰, IoT 디바이스와 같은 하드웨어 자산(HWAM, Hardware Asset Management)과 사용자 계정, 애플리케이션, 디지털 인증서와 같은 소프트웨어 자산(SWAM, Software Asset Management)으로 구분하여 관리한다. 이러한 자산들을 물리적 위치나 네트워크를 포함해서 항상 설정, 조사, 업데이트할 수 있어야 한다. 또한, 기업 소유 인프라에서 새롭게 발견된 자산을 빠르게 식별, 구분, 액세스하는 능력을 갖추는 것을 고려해야 한다. 이때 기업 자산 데이터베이스를 구분하거나 관리하는 것 외에 설정 관리 및 모니터링도 포함해야 된다.

특히, 기업 소유가 아닌 자산과 기업 소유의 쉐도우 IT(shadow IT, 직원이 IT 부서에서 승인하지 않은 클라우드 애플리케이션 또는 서비스를 구입하고, 이를 IT 관리부서나 책임자가 파악하지 못하는 현상) 자산을 최대한 구분해야 한다. 쉐도우 IT 컴포넌트는 인지되지는 않지만, 네트워크 액세스가 필요하기 때문에 특수한 문제를 발생시킬 수 있으며, 액세스 결정이나 모니터링 및 포렌식(forensic)에도 활용되기 때문이다.

셋째, 핵심 프로세스 식별 및 위험 평가로써 비즈니스 프로세스와 데이터 플로우 그리고 이들의 관계를 식별하고, 성능, 사용자 경험, 워크플로우 취약점 증가 가능성 사이의 균형을 고려하여 우선순위를 부여한다. 클라우드 기반 리소스를 사용하거나 원격 근무자가 사용하는 비즈니스 프로세스는 제로 트러스트 아키텍처(ZTA)를 적용하기에 적합한 경우가 많다. 이런 비즈니스 프로세스는 기업 경계를 클라우드에 옮기거나 클라이언트가 가상 사설망(VPN, Virtual Private Network)을 통해 기업 네트워크를 사용하는 것이 아니라, 기업의 클라이언트가 클라우드 서비스를 직접 요청할 수 있기 때문에 가용성 등을 개선해야 할 여지가 많다.

넷째, 제로 트러스트 아키텍처(ZTA) 후보에 대한 정책을 수립해야 하는데, 후보 서비스나 워크플로우는 프로세스의 중요성, 영향을 받는 주체, 워크플로우에 사용되는 리소스의 현재 상태에 따라 결정한다. 이를 위해 자산이나 워크플로우를 식별한 후, 워크플로우가 사용하거나 영향을 주는 모든 업스트림 리소스(ID 관리 시스템, 데이터베이스, 마이크로서비스), 다운스트림 리소스(로그, 보안 모니터링, 엔티티(주체, 서비스 계정)를 식별해야 한다. 그리고, 기업의 모든 주체에게 필수적인 애플리케이션/서비스(이메일)보다 기업의 일부 주체가 사용하는 애플리케이션이나 서비스(구매 시스템)를 후보로 선호할 것이기 때문에 기업의 관리자는 후보 비즈니스 프로세스가 사용하는 리소스에 대해 기준들을 결정하거나, 중요도에 따른 가중치를 결정해야 한다.

다섯째, 솔루션 후보 식별단계로써 비즈니스 프로세스 후보 목록이 작성되면, 기업 설계자는 아래와 같은 고려 기준에 따라 솔루션 후보 목록을 작성하고 확인해야 한다.

- 솔루션이 기업 소유가 아닌 자산(BYOD(Bring Your Own Device, 직원들이 직장에 개인 소유의 스마트기기 또는 모바일 장비를 가져와 비즈니스 목적으로 사용하는 것) 또는 기관 간 협업 등)을 사용하는 비즈니스 프로세스에는 적용이 제한되므로 클라이언트에 컴포넌트를 설치해야 하는지를 확인한다.
- 후보 비즈니스 프로세스의 리소스 위치는 제로 트러스트 아키텍처(ZTA)와 후보 솔루션에 모두 영향을 미친다. 일부 솔루션은 요청된 리소스가 클라우드에 위치하고 기업 경계 내부에 있지 않다고 가정하기 때문에 솔루션이 비즈니스 프로세스 리소스가 모두 온 프레미스(on-premise, 기업의 서버를 클라우드 같은 원격 환경에서 운영하는 방식이 아닌, 자체적으로 보유한 전산실 서버에 직접 설치해 운영하는 방식)에서도 동작하는지를 확인해야 한다.



- 제로 트러스트의 핵심 컴포넌트는 액세스 결정 시 정책 엔진으로 피드백 되는 프로세스 플로우 관련 데이터를 수집하고 사용하기 때문에 솔루션이 분석에 필요한 로그 상호작용에 대한 방법을 제공하는지 확인이 필요하다.
- 솔루션이 다양한 애플리케이션, 서비스, 프로토콜을 지원한다면, 프로토콜(웹, SSH(Secure Shell, 원격 호스트에 접속하기 위해 사용되는 보안 프로토콜) 등) 및 전송(IPv4, IPv6)을 광범위하게 지원하는 솔루션인지, 웹/이메일처럼 좁은 범위에서만 동작하는 솔루션인지를 확인해야 한다.
- 솔루션이 주체의 행위에 변경을 요구한다면, 특정 워크플로우를 수행하기 위해 기업 주체는 워크플로우의 수행 방법을 바꾸어야 한다.

여섯째, 초기 시행 및 모니터링 단계로써 후보 워크플로우 및 제로 트러스트 아키텍처(ZTA) 컴포넌트를 선택하면, 초기 시행에 들어간다. 기업 관리자는 처음에 중요한 사용자 계정(관리자 계정)이 필요한 리소스에 대한 액세스가 거부되거나, 할당된 액세스 권한이 과도할 수 있기 때문에 모니터링 모드로 운영하기를 원할 수 있다.

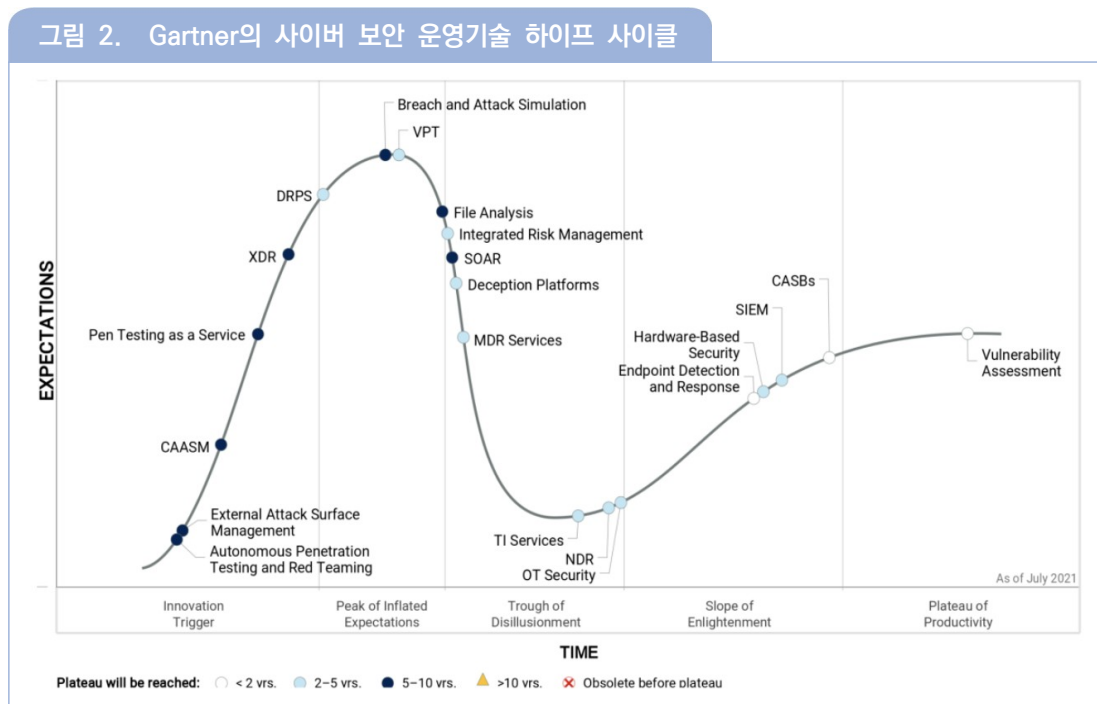
또한, 새로운 제로 트러스트 비즈니스 워크플로우에 대해 정책이 효과적이고 운영 가능한지 확인될 때까지 리포트만 수행하는 모드(reporting-only mode)로 운영할 수도 있다. 이를 통해 기업은 자산·리소스에 대한 액세스 요청·행위·통신 패턴의 베이스라인을 인식할 수 있다. 보고만 수행한다는 것은 대부분의 요청에 대해 액세스를 허가하며, 접속 로그·추적 등 최초 작성된 정책과 비교하는 것을 의미하지만 기본적인 정책(다중 인증에 실패하는 요청, 공격자가 침해한 것으로 알려진 IP 주소 거부 등)을 실행하고 로그를 기록해야 한다.

마지막 단계는 제로 트러스트 아키텍처(ZTA) 확대 단계로써 워크플로우 정책이 개선되었으면, 기업은 정상적인 운영 단계에 진입한다. 네트워크·자산을 지속적으로 모니터링하고, 트래픽을 로그에 기록한다. 이때, 대응 및 정책 변경이 적시에 이루어져야 하며, 주체 및 리소스·프로세스의 이해 관계자는 운영 개선을 위한 피드백 활동을 해야 한다.

이 단계에서 기업 관리자는 제로 트러스트의 다음 단계를 진행할 수 있다. 최초 전개와 마찬가지로 워크플로우 및 솔루션 후보를 식별하고, 초기 정책을 작성할 필요가 있으나, 워크플로우에 변화가 생겼다면, 제로 트러스트 아키텍처(ZTA) 운영에 대한 재평가가 필요하다. 또한, 신규 디바이스, 제로 트러스트 논리 컴포넌트의 중요 업데이트, 조직 구조의 이동과 같은 시스템의 중요한 변화도 워크플로우 또는 정책의 변화를 초래할 수 있으므로, 이때는 전체 프로세스를 다시 검토해야 한다.

## 2. 사이버 보안 운영기술의 하이프 사이클 전망

가트너(Gartner)의 하이프 사이클(Hype Cycle)은 기술 성숙도에 대한 시장 기대의 변화를 경험적으로 예측하는 것으로, 기술의 성숙도를 혁신 단계, 기대정점 단계, 환멸 단계, 계몽 단계, 생산성 안정단계로 구분하여 예측한다. 가트너는 사이버 보안 위협의 진화에 대응하기 위한 차세대 사이버 보안 운영기술에 대해 <그림 2>와 같이 전망한다(Gartner, 2021).



\* 출처: Gartner(2021)

혁신단계(Innovation Trigger)는 잠재 기술이 관심을 받기 시작하는 시기로 상용화 제품은 없고 상업적 가치도 아직 증명되지 않은 상태이다. 디지털 리스크 보호 서비스(DPRS, Digital Risk Protection Service), 탐지대응 강화기술(XDR, Extended Detection and Response), 클라우드에서 제공하는 모의 침투 시험 서비스인 PaaS(Pen Testing as a Service)가 있으며, 데이터 및 보안 솔루션을 하나로 통합해 관리하는 차세대 네트워크 개념의 공격 표면 관리(CAASM, Cyber Asset Attack Surface Management) 기술, 알려졌거나 알려지지 않은 외부 공격에 대한 종합적인 표면관리(EASM, External Attack Surface Management) 기술, 기업 내·외부의 취약성 평가와 사회공학적 공격을 추가하여 침입을 시뮬레이션하는 자동 침입 테스트 및

레드티밍(APTRT, Autonomous Penetration Testing and Red Teaming) 기술이 있다.

기대정점 단계(Peak of Inflated Expectations)는 일부 기업만이 실제 사업에 착수하고, 대부분의 기업들은 관망하는 상태이다. BAS(Breach and Attack Simulation)는 네트워크의 사이버 방어 수준을 측정하기 위해 공격자가 자동화 도구를 사용하여 시뮬레이션 공격을 실행하는 도구 기술이며, VPT(Vulnerability Prioritization Technology)는 위험 관리기반의 자동화된 취약성 관리도구 기술이다.

환멸 단계(Trough of Disillusionment)는 제품 향상에 성공한 일부 기업만이 투자를 계속하며 대부분은 제품화를 포기하는 상태이다. 파일 분석(file analysis), 통합 위험관리(integrated risk management), 다양한 사이버 위협에 대해 대응 수준을 자동으로 분류하고 표준화된 업무 프로세스에 따라 보안 업무 담당자와 솔루션이 유기적으로 협력할 수 있도록 지원하는 SOAR(Security Orchestration, Automation and Response)가 대표적인 기술이다.

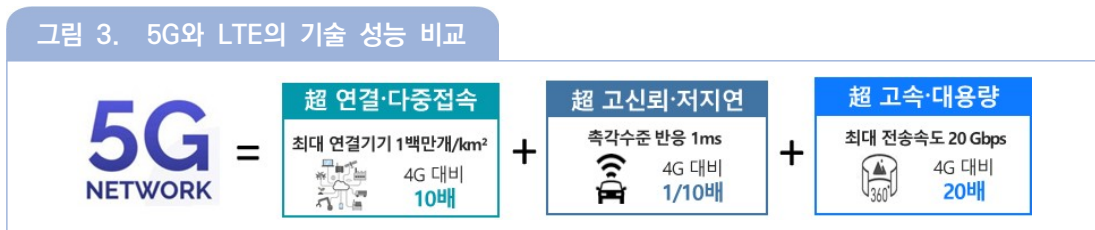
또한, 클라우드나 로컬 네트워크 환경 하에서 기존의 솔루션이 탐지하거나 방어할 수 없는 새로운 유형의 공격이나 정교한 공격을 탐지하는 위장 플랫폼(deception platform) 기술, 보안 이벤트 로그 모니터링과 함께 실시간 대응 및 조치가 가능한 MDR(Managed Detection and Response) 기술, 네트워크와 엔드포인트(endpoint, 컴퓨터 네트워크에 연결하고 컴퓨터 네트워크와 정보를 교환하는 모든 디바이스) 위협정보를 통합해 신·변종 해킹에 선제적으로 대응하는 TI(Threat Intelligence) 기술, IDS/IPS(Intrusion Detection System, 침입탐지 시스템/Intrusion Prevention System, 침입 방지 시스템)와 네트워크 위협 분석(NTA, Network Threat Analysis), 네트워크 포렌식 기술을 통합하여 기존의 트래픽과 사건(incident)들을 역추적 분석이 가능한 NDR(Network Detection and Response, 네트워크 탐지 및 대응) 기술, OT(Operational Technology, 운영 기술) 보안기술 등이 제시된다.

계몽 단계(Slope of Enlightenment)는 기술이 수익을 창출하며 2~3세대 제품들이 출시되는 단계이다. 팬데믹을 계기로 이용이 급증하고 있는 클라우드 서비스의 보안을 강화하기 위한 클라우드 접근 보안 중개(CASB, Cloud Access Security Broker) 기술이 주목을 받고 있으며, 보안 정보 및 이벤트 관리(SIEM, Security Information and Event Management), 하드웨어 기반 보안(hardware-based security), 종단 탐지 및 대응(EDR, Endpoint Detection and Response) 기술 등이 있다.

생산성 안정 단계(Plateau of Productivity)는 기술성고가 구체적으로 나타나면서 시장에서 정착해 가는 단계이다. 보안 취약성 평가(vulnerability assessment) 기술이 대표적이며, 핵심 서버, 유·무선 네트워크, 데이터베이스(DB, Database), 웹의 취약성 평가 등으로 구성된다.

## II 최근의 사이버 위협 및 공격 동향

무선 인프라인 5G/6G가 기술혁신을 거듭하면서 <그림 3>과 같이 LTE에 비해 초연결·다중접속화, 초고신뢰·저지연화, 초고속·대용량화 성능이 획기적으로 향상되었고, 이와 동시에 자율주행 기반의 전기자동차, 드론, 인공지능(AI, Artificial Intelligence) 로봇 등 다양한 첨단 서비스의 개발·보급도 빠르게 확산되고 있다. 특히, 팬데믹 발생 이후, 전 세계적으로 재택근무, 원격 수업 등 비대면 문화가 일상화되었고, 리테일 이커머스 (retail E-commerce), 디지털 헬스케어 분야의 워크로드도 클라우드로 이동하는 추세를 보이고 있다.



\* 출처: 부산가톨릭대학교 융합보안공학센터(2021)

이러한 보안기술의 변화 속에서 사이버 보안 기업인 이글루시큐리티, 시만텍(Semantec), 트렌드 마이크로 (Trend Micro) 등의 전망에 따르면, 공격자들은 AI를 활용한 지능형 지속 공격(APT, Advanced Persistent Threat)과 랜섬웨어 기반의 변종 공격을 강화할 것으로 예상되고 있으며, 방어자 측에서도 사이버 공간에서의 취약점 보안을 위해 AI 기술을 활발하게 도입할 것으로 보고 있다.

또한, 비대면 환경이 빠르게 확장되면서 표적 공격이나 악성코드 침투가 쉬워지고, 다크웹(dark web, 일반 웹브라우저가 아닌 특수한 프로그램으로만 접속할 수 있는 온라인 공간) 활성화 등 공격자에 유리한 환경이 만들어지고 있는데, 현재 진행 중인 사이버 보안 위협과 공격의 특징적 추세는 기존 공격 패턴의 지능적 진화, 산업 스마트화에 따른 사이버 공간과 공격대상의 확대, 팬데믹에 의한 비대면 플랫폼 이용 및 공격 유발 유인의 급증으로 요약할 수 있다.

## 1. 사이버 공격기술의 지속 진화

### 1.1. 사이버 공격 기법의 AI 활용

그 동안 AI와 빅데이터 분석기술은 일부 기업이나 사용자들에 의해 제한적으로 연구되어 왔으나, 캐글(Kaggle)이나 깃허브(GitHub)와 같은 데이터 전문가 커뮤니티의 활성화와 오픈소스 공유 플랫폼의 이용이 확산되고, 이 분야의 연구에 전문가들이 자유롭게 참여할 수 있게 되면서 기술발전 속도도 빨라지고 있다.

반면, 이러한 개방적인 AI 연구 환경에 사이버 공격자들도 참여하기 시작하면서 수작업으로 만들던 악성코드를 첨부한 이메일의 대량 자동 생성, 실시간 메가급 사이버 공격, 딥페이크(deepfake) 기술을 활용한 정보 조작, 위장 사이트의 성공률도 동시에 높아질 것으로 우려된다.

실제로 공격자들은 머신러닝(ML, Machine Learning) 알고리즘을 사용하여 공격의 효율성을 높이고, 머신러닝 학습에 사용되는 데이터 셋(data set)을 조작해 방어자들의 공격패턴 분류의 정확성을 낮추기 위한 데이터 포이즈닝(data poisoning)이 보고되고 있다.

따라서 AI를 활용한 이미지나 영상정보의 위변조 공격, AI 학습변조, AI 기반의 해킹 자동화 도구 개발 등 최근 사이버 공격기술의 지능화에 대응하기 위해서는 방어자 측에서도 AI 기반의 데이터 위변조에 대한 실시간 자동 탐지 및 분석기술 개발, 사이버 공격 발생원인 분석까지도 가능한 XAI(Explainable AI, 설명가능 인공지능) 기술 개발의 필요성이 강조되고 있다(KISTEP & IITP, 2022; IITP, 2020; ICF, 2020).

### 1.2. 랜섬웨어(ransomware) 공격의 변종 확산

2012년 레벤톤(Reveton)을 시작으로 알려지기 시작한 랜섬웨어는 초기에는 암호화된 데이터를 복호화해 주는 대가로 금전을 요구하였으나, 최근에는 데이터 복호 외에 주요 데이터를 탈취하여 공개하겠다는 협박으로 변화되고 있다. 2017년에 처음 출현한 워너크라이(Wanna Cry)는 MS 서버 메시지 블록(SMB, Server Message Block) 프로토콜의 취약점을 악용하여 74개국에서 시스템의 감염피해를 발생시킨 대표적인 사례이다. 2021년에도 미국 CNA Financial, Colonial Pipeline, JBS Foods 등에 대한 랜섬웨어 공격으로 서비스 중단이 보고되었다.

랜섬웨어 공격은 제조, 유통 등 특정기업 분야를 대상으로 하고 있으며, 해킹 메일 등을 이용하여 내부 직원 PC를 장악하여 중앙 관리시스템(active directory)의 관리자 계정을 탈취하려는 APT 형태로 진화되고 있다. 또한, 디도스(DDoS, Distributed Denial of Service attack) 공격과 랜섬웨어가 결합된 랜섬 디도스(RDDoS, Ransom DDoS) 공격도 증가하고 있으며, 정보를 탈취하고 암호복구 대금을 요구하는 이중 협박형

랜섬웨어나 공격기술 초보자들에게 랜섬웨어를 제작해서 제공해 주는 서비스형 랜섬웨어(RaaS, Ransomware as a Service)도 등장하고 있다.

현재 랜섬웨어는 사이버 공격 전체의 35% 이상을 차지하고 있으며, 피해 규모를 가장 크게 유발시킬 수 있다는 점에서 공격자들은 앞으로도 공격 패턴을 계속 지능적으로 진화시켜 나갈 것으로 보인다(이글루시큐리티, 2022a; 이글루시큐리티, 2022b; ICF, 2023)

### 1.3. 제로데이 공격대상의 확대

제로데이 공격(zero-day attack)은 우수한 기술력을 갖춘 해커들이 소프트웨어 제작자나 개발자가 발견하지 못한 취약점을 보안 패치가 배포되기 전에 시간적인 갭(gap)을 이용하여 빠르게 공격하는 고도의 사이버 공격기법이며, 아직까지 뚜렷한 보안대책이 제시되지 못하고 있어 피해가 확산되고 있다.

최근의 제로데이 공격 수법은 해커가 공격 대상자의 이메일이나 SNS 등에서 보안 취약점을 찾아낸 후, 악성 URL 등을 첨부한 해킹 메일을 이용하여 필요한 정보를 탈취하기 때문에, 제로데이 공격에 대한 보안대책은 주로 사용자가 클릭한 URL의 악성여부를 실시간으로 대응하는 등 악성코드 시그니처(signature)와 URL 평판에 의존하고 있으며, 공격 패킷의 특징 분석을 통해 제로데이 공격을 차단하기 위한 연구 등이 진행되고 있다.

이제까지 보안 취약점을 이용한 제로데이 공격은 가상화폐 거래소의 내부에 침투하여 가상화폐나 기업정보를 탈취하거나, 소프트웨어 개발자의 PC를 장악하여 소스코드 접근 권한 탈취에 집중되어 왔으나, 팬데믹을 계기로 코로나-19 백신 및 치료제 개발정보 탈취를 위해 백신 연구와 밀접히 연관된 학계 및 제약업계로 확대되는 추세를 보이고 있다.

2021년에는 프로그램 동작 과정에서 생성되는 로그기록을 남기는 오픈소스 프로그램인 자바 기반의 Log4j 취약점 공격이 발생하여 공급망 보안의 중요성이 입증되었고, 이미 발견된 제로데이 취약점을 패치하지 않은 미국 내 3만 개 이상의 기업과 정부기관들의 MS Exchange Server가 공격을 받았다. 또한, 국내에서는 특정업체의 VPN 취약점을 이용한 메일시스템과 인증서버에 대한 해킹사고가 발생하였다(KISTEP&ITTP, 2022; 이글루시큐리티, 2022b; 이대성, 2019).



## 2. 산업기반시설의 CPS화에 따른 공급망 리스크 증가

과거 유비쿼터스 센서 네트워크(USN, Ubiquitus Sensor Network)의 개념으로 시작된 IoT는 IPv6을 기반으로 하여 IoT 센서와 장비, 소프트웨어 등을 통합하는 무선 플랫폼으로 본격적인 성장을 계속하고 있다. 이러한 배경에는 IoT 인프라를 구축하여 생산 효율성을 높이고 산업생산 리스크를 감소시킬 수 있다는 점이 강조된 것으로 평가할 수 있다.

전력, 교통, 수자원 등 중요 정보통신 기반 시설들은 오랜 기간 폐쇄망으로 운용되어 왔기 때문에 원격 액세스 권한을 확보하기 위한 공격자들의 해킹 시도는 거의 불가능했다. 특히, ICS(Industrial Control System)/OT(Operation Technology) 환경은 보안 위협이나 취약점이 발견되더라도 가용성을 우선시 해왔기 때문에 보안패치 및 시스템 재부팅 등이 거의 불가능했으며, 폐쇄망 구성이라는 인프라 구성방식을 채택하였기 때문에 상대적으로 사용자의 보안 인식이 결여되어 있는 것으로 지적되어 왔다.

이러한 기존의 ICS/OT 환경에서의 사이버 공격기법으로는 ICS/OT를 구성하고 있는 소프트웨어나 장비를 표적으로 스텍스넷(Stuxnet)이나 트라이톤(Triton)과 같이 전용 악성코드가 주로 사용되었다. 하지만 ICS/OT 환경이 운영 효율성과 자동화 등의 목적으로 클라우드, 액티브 디렉토리(active directory) 등의 IT 기술과 연동되고, 또한 IoT 디바이스의 경우에는 상당 부분이 보안 경계 밖에 위치해 있기 때문에 IoT 망을 경유하여 ICS/OT에 접근할 수 있는 액세스 접점이 크게 늘어남으로써 공격 도구의 보편화, 공격 파급력 확대 역량을 갖춘 사이버 위협도 그만큼 더 증가할 것으로 예상된다. 실제로 랜섬웨어나 원격접속 프로그램 등 공개된 소프트웨어나 오픈소스를 활용한 공격사태가 최근 급증하고 있다(KISTEP & ITTP, 2022; 이글루시큐리티, 2022a; 이글루시큐리티, 2022b).

한편, ICS/OT 환경에서 발생하는 사이버 공격들이 국가지원을 기반으로 한 해킹그룹들의 활동이 두드러지면서 이에 따른 보안위협 영향도가 커지고 있다. 러시아 해커조직 다크사이드(DarkSide)가 수행한 것으로 추정되는 미국 송유관 해킹 공격으로 세계 경제에 막대한 영향을 끼쳤으며, 북한 해커조직도 국가 기반 시설과 주요 인원들 대상으로 사이버 공격을 수행하고 있기 때문에 ICS/OT 보안은 날로 중요성을 더하고 있다.

주요 공격 사례로는 2010년 이란 대규모 산업 시설 제어 시스템의 오작동을 유발한 스텍스넷(Stuxnet)을 시작으로 2015년 블랙에너지(Black Energy), 2016년 크래쉬 오버라이드(Crash Override), 2017년 트라이톤(Triton), 2018년 TSMC(Taiwan Semiconductor Manufacturing Co.) 워너크라이 랜섬웨어, 2019년 노르스크 하이드로 록커고가(NorskHydro LockerGoga), 2021년 플로리다 수도인프라 공격 등이 보고되었다.

ICS/OT에 대한 사이버 공격 행위는 해당 국가는 물론 전 세계 경제활동에도 치명적인 피해를 초래할 수 있는 만큼 사이버물리시스템(CPS), 오픈소스 코드, 클라우드, 디지털 공급망, 소셜 미디어 등 광범위한 디지털 자산을 통제 관리할 수 있도록 초고속 대용량으로 유입되는 악성 패킷을 실시간 모니터링하고 분석·차단할 수 있는 차세대 보안 리스크 관리체계의 구축이 요구된다.

### 3. 온라인서비스 플랫폼에 대한 보안 위협 증대

코로나-19의 전 세계 확산에 따른 팬데믹을 계기로 VPN을 경유하여 사내 인트라넷 플랫폼을 이용하는 재택근무, 줌(Zoom)이나 웹엑스(WebEX) 등을 이용한 영상회의, SNS를 이용한 주문배달 등 비대면 온라인 생활문화가 일상화되면서 보안이 취약한 홈 네트워크와 개인 디바이스에 대한 해킹 시도가 증가하고 있다.

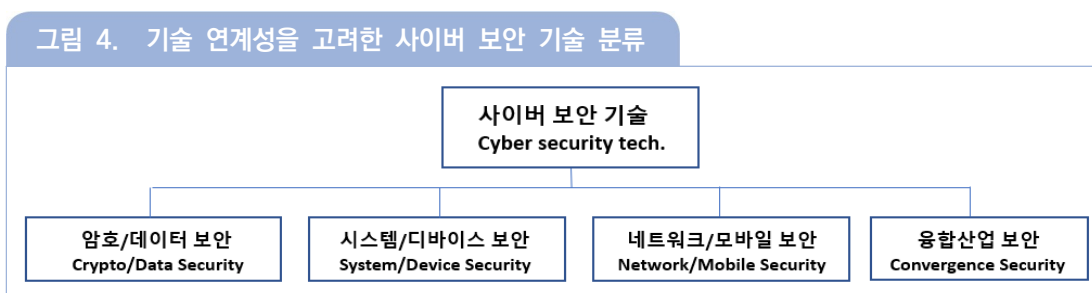
특히, 사실 진위 여부를 밝히기 힘든 가짜 데이터를 생성하는 딥페이크 공격이나 다크웹을 통해 탈취된 사용자 계정 정보와 내부 정보 탈취, 취약점 공격인 익스플로잇(exploit)으로 비대면 애플리케이션을 장악하는 등의 공격이 증가하여 이에 대한 보안대책이 마련되어야 하며, 시스템 비인가자들이 영상수업이나 회의를 방해하는 사례가 빈발하여 온라인 접근통제를 강화하기 위해서는 신뢰할 수 있는 원격 제어가 가능한 제로 트러스트와 같은 새로운 개념의 개인 인증체계 적용이 필요하다.

한편, MS365, Google Workspace, AWS, GCP, Azure 등 클라우드 시스템에 대한 사용자들의 의존도가 높아짐에 따라 단순 사고가 대규모 접속장애 및 정보유출로 이어지고, 클라우드 시스템만 전문적으로 공격하는 사례도 늘고 있다. 현재 주요 선진국에서는 금융기관이나 공공기관들이 전통적인 온 프레미스(on-premise) 방식에서 온 프레미스(on-premise)와 퍼블릭 클라우드를 조합한 하이브리드 클라우드로 전환하는 추세를 보이고 있으며, 이에 따라 보안 설정 및 접속 관리는 물론 인프라, 플랫폼, 소프트웨어 등 서비스별 통합 보안 체계의 재정립을 위한 클라우드 보안 가이드라인이 개발되어 보급되고 있다(KISTEP & ITTP, 2022; IITP, 2020; 이글루시큐리티, 2022b).

### III 사이버 보안 기술 개발 동향

사이버 공간에서의 ICT 기술 환경은 초연결·초고속·초저지연화를 목표로 빠르게 진화하고 있다. 이에 따라 사이버 보안 기술분야에서도 다양한 사이버 보안 위협에 실시간 대응하기 위해 사용자 디바이스, 네트워크, 정보시스템의 전 구간을 대상으로 안전·신뢰성을 보장하고 사이버 복원력(cyber resilience)을 구현하는 초신뢰화 기술과 통합적 사이버 위험관리(cyber risk management) 인프라 구축에 필요한 요소기술의 개발이 진행되고 있다.

사이버 복원력은 IT 시스템과 리소스에 대한 공격과 손실을 예상하여 사이버 공격과 위협을 예측(anticipate), 대응(withstand), 복구(recover), 적응(adapt)하는 4단계 방어로 구성된 차세대 보안 기술 개념을 구현하는 것을 목적으로 한다. 이하에서는 사이버 보안 기술을 기술 간의 연계성을 고려하여 <그림 4>와 같이 4개 기술 영역으로 구분하여 기술개발 동향을 살펴보기로 한다.



\* 출처: 부산가톨릭대학교 융합보안공학센터(2021)

## 1. 암호/데이터 보안 기술

차세대 암호기술에서는 대량의 암호화 데이터를 수집하고 활용하기 위해 복호화하지 않고도 데이터 자체를 연산할 수 있는 동형 암호기술, 함수 암호기술 등이 연구되고 있으며, 초신뢰 데이터 보안을 구현하기 위해 양자 암호통신(QKD, Quantum Key Distribution), 양자내성 암호 알고리즘(PQC, Post Quantum Cryptography), AI 기반의 암호 안전성 분석에 대한 연구가 추진되고 있다.

특히, 개인 데이터의 활용성을 높이면서 동시에 데이터 오남용을 차단하여 사용자의 프라이버시를 보장할 수 있는 동형 암호, 함수 암호 등 4세대 암호 기술과 IoT 기기에 적용할 수 있는 환경 적합형 경량 암호기술 개발도 활발하게 연구되고 있다(IITP, 2020).

인증기술 분야에서는 모바일 디바이스와 소셜 비즈니스의 이용 확산으로 다양한 서비스를 지원할 수 있는 개인인증 보안기술의 수요가 팬데믹을 계기로 급속하게 증대되면서 세션이 진행되는 동안 사용자의 행위적 요소 등을 통해 지속적으로 인증하는 보안 기능을 강화하며, 비접촉 방식의 바이오 인식 보안 솔루션 개발과 스마트 뇌파, 심전도, 뼈, 근육, 혈액 등 스마트 디바이스 기반의 새로운 바이오 인증 수단의 개발이 진행 중이다.

AI를 이용한 데이터 공격과 방어기술 분야에서는 적대적 기계학습을 이용한 AI 역기능 유발공격에 대한 자동화 대응, AI 시스템의 오작동이나 이상행위 등을 판단·예측하여 대응할 수 있는 고신뢰 AI 서비스 기술 등이 연구되고 있다(과학기술정보통신부, 2021).

블록체인은 네트워크 내의 참여자가 중개자 없이 신뢰를 확보할 수 있는 차세대 보안 기술이며, 1세대 기술인 분산장부 공유, 2세대 기술인 스마트 컨트랙트(smart contract)를 거쳐 현재는 블록체인 데이터 전송 최적화 및 프라이버시 확보, IoT 등 다중 데이터 연동 처리, 블록체인 간 상호운용성, 산업 및 실생활 블록체인 적용 문제 해결에 연구가 집중되고 있다.

블록체인의 범용성을 확보하기 위해 I/OAT(I/O Acceleration Technology), 해시그래프(Hashgraph) 등 DAG(Directed Acyclic Graph, 비순환 방향 그래프) 알고리즘 방식의 기술 개발이 진행 중이며, 아마존, 구글, 애플과 같은 글로벌 플랫폼 기업들은 개인키 분실이나 해킹을 차단하기 위해 전자지갑 기술, 개인키 분실 대응과 거래소 서버의 보안성 강화 기술 등을 개발 중이다(IITP, 2020).

## 2. 시스템/디바이스 보안 기술

악성 코드 대응에서는 PC, 모바일 디바이스, 서버 등 단말에서 급속하게 증가하고 있는 변종 악성 코드를 실시간 탐지·분석하고, 공격 패턴의 시공간적 상관관계를 부호화하여 대응하는 종단 탐지 및 대응(EDR)에 백신 기능을 탑재하여 신종 공격에 취약한 기존 안티 바이러스 제품들을 빠르게 대체해 갈 것으로 예상된다. 특히, AI를 이용하여 알려지지 않은 새로운 악성코드나 문서형 악성코드를 탐지·분석하는 AI 백신기술이 중점적으로 개발되고 있다.

취약점 분석에서도 자동 해킹 도구를 이용한 제로데이 공격에 효과적으로 대응하기 위해 딥러닝을 기반으로 악성코드를 탐지하고 유사도를 자동 측정하는 기술과 외부 공격을 스스로 인식하고, 소프트웨어(SW)나 하드웨어(HW)에 내재된 보안 취약점을 스스로 제거하여 정상상태로 되돌리는 자기학습형 사이버 면역기능을 갖는 지능형 사이버위협 대응기술(CTI, Cyber Threat Intelligence)이 개발 중이다. 이러한 기술에는 SW/HW 보안 취약점 분석 자동화기술, 임베디드 펌웨어(firmware) 및 HW 백도어(backdoor, 시스템에 접근하기 위해 정상적인 인증 절차를 무효화하는 악성 코드의 유형) 탐지기술 등이 있다.

또한, 공급망(supply-chain)을 통해 개별기업으로부터 조달되는 일련의 HW나 SW 공급 과정도 다양한 해킹 및 보안 위협에 노출되고 있다. HW를 통한 백도어 형태의 공격은 소프트웨어의 취약성에 비해 분석과 탐지가 매우 어려운데 공급망 보안에서는 ICT 공급망 제품 및 서비스의 위험평가 프로세스 기준과 관련 도구 개발과 함께 IC(Integrated Circuit, 집적 회로) 칩, PCB(Printed Circuit Board, 인쇄 회로 기판), 펌웨어를 대상으로 보안 분석 및 취약점 자동 탐지 기술과 신뢰중심(trust hub) 기술을 중심으로 연구되고 있다(IITP, 2020; 김대원 외, 2020).

디바이스 보안영역에서는 SW 취약점 분석, 부채널 분석 대응, 보안 알고리즘/프로토콜 경량화, 모바일 장치 관리(MDM, Mobile Device Management)를 중심으로 기술 개발이 추진되었으나, 미국 등에서는 기존의 시그니처를 기계학습을 통해 모바일 네트워크와 모바일 엔드포인트를 보호하는 기술들도 개발되고 있다.

IoT 인프라 보호기술은 응용 범위가 스마트 그리드, 스마트 팩토리, 스마트 카, 스마트 의료, 스마트 홈 등으로 계속 확장됨에 따라 차세대 보안에서도 가장 주목받는 영역이다. 차세대 IoT 인프라 보호에 필요한 주요 기술로는 사물 지능 통신(M2M, Machine to Machine) 기기 인증 및 신뢰통신 보안 서비스 제공기술과 이를 내장한 임베디드 SIM(Subscriber Identity Module, 가입자 식별 모듈)이 개발 중이며, 경량 IoT 보안 게이트웨이와 초연결 디바이스에 대한 무인원격 보안관리서버 기술, HW 제약·성능 등이 서로 다른 이기종

디바이스를 위한 맞춤형 보안 운영체제와 경량/저전력 디바이스에 특화된 보안 HW 모듈 등 IoT 디바이스의 고가용성 보장을 위한 보안 기술이 개발되고 있다(이대성, 2019).

클라우드 보안 기술은 가상화, 클라우드, 소프트웨어 정의 네트워킹(SDN, Software Defined Network) 등의 환경에서 사용자 데이터 및 기업 데이터를 안전하게 공유·활용하는 방법들이 연구되고 있다. 세부적으로는 클라우드 자체를 보호하기 위해 SecaaS(Security as a Service) 및 가상화 기반에 보안기능을 제공하여 보안 서비스의 유연성 확보, 클라우드 환경에서의 보안기능 지능화, 보안 기능의 동적 구성이 가능한 고성능 보안 가상화 플랫폼 기술 개발이 추진되고 있다. 또한, 사이버 공격의 최종 목표인 관리자 계정의 보호를 위해 클라우드 기반에서의 권한 접근 관리(PAM, Privileged Access Management) 기술, 피싱에 대응하는 비즈니스 이메일 컴프로마이즈 기술, 안티 프로드(anti-fraud, 사기방지 프로그램) 및 ID 관리기술도 중점적으로 연구될 것으로 보인다.

특히, 소프트웨어 정의 보안(SDsec, Software Defined Security) 및 네트워크 기능 가상화(NFV, Network Function Virtualization) 환경에서 보안기능의 동적 재구성, 고성능 제어, 가시성을 확보하기 위해 네트워크 하이퍼바이저(hypervisor), 컴퓨팅과 네트워킹이 결합된 서버-스위치 등 고성능 클라우드 보안 플랫폼 기술 개발이 진행 중이다(IITP, 2020; 박인상 외, 2020).

### 3. 네트워크/모바일 보안 기술

모빌리티 수요와 클라우드 이용이 급증함에 따라 네트워크 아키텍처의 개념이 소프트웨어 정의 네트워킹(SDN) 과 스위치, 방화벽(firewall), 로드 밸런싱(load balancing, 네트워크 또는 서버에 가해지는 부하를 분산해주는 기술), 암호화 등을 소프트웨어적으로 가상 구동할 수 있는 네트워크 기능 가상화(NFV)의 구현으로 이동함에 따라 차세대 네트워크 보안의 개념도 이동성과 클라우드 컴퓨팅을 지원하고 사이버 위협의 동적 변화환경에 대응하는 방향으로 변화될 것이 예상된다.

SDN/NFV 플랫폼 보안에 필요한 기술로는 사이버 복원력을 중심으로 사이버 공격에 사전 예방적으로 대응할 수 있는 가상화 기반 지능형 네트워크 보안기술, 소프트웨어 정의 네트워킹(SDN) 기반 보안 언어, SDsec 컨트롤러 등이 개발 중이며, 네트워크 가상화와 안전한 5G 서비스 제공을 보장하기 위한 유무선 네트워크 및 장비 보안 원천기술 개발, 스마트 IoT 서비스 네트워크 보호를 위한 사이버공격 대응 원천기술 개발, 초연결 네트워크 보안기술이 중점 기술개발 영역이 될 것으로 보인다.



모바일 네트워크 보안에서는 모바일 사용자들이 5G 서비스를 안전하게 이용할 수 있도록 5G 코어망, 다중접속 엣지컴퓨팅(MEC, Multi-access Edge Computing), 이기종 5G 디바이스 등에 대한 전체적인 사이버 위협에 대처할 수 있는 보안 기술 개발이 이루어지고 있다. 주요 기술로는 5G 시그널링 방화벽 및 엣지 보안, 5G 서비스 플랫폼과 Massive Device 보안위협 탐지·차단기술, 이기종 IoT 무선 네트워크 보안을 위한 원격 신뢰 접속 제어 Secure GW 기술 등이 있다.

또한, 5G 보다 50배나 빠른 6G는 2030년을 기술 상용화 목표로 하고 있으며, 자율주행이나 스마트 진료에 필수적인 차세대 모바일 기술이다. 이에 따라 미국과 중국을 중심으로 6G 사이버 위협에 선제 대응하기 위해 설계 초기 단계부터 보안기능을 내재화하고, 6G 보안 QoS 보장, 6G 기밀성 제공을 위한 양자 안전성 보안기술, 해상, 공중, 위성을 포함한 초공간·초입체적 모바일 보안기술 등 6G 핵심원천 기술을 선점하기 위한 연구가 이루어질 전망이다(IITP, 2020; 최동진, 2019).

보안관제 기술은 탐지의 개념에서 사전·사후 대응의 개념으로 빠르게 변화되고 있다(최동진, 2019). 이를 위해 네트워크, 서버, 엔드포인트 전 구간에서 발생하는 사이버 공격 위협을 실시간 모니터링하며, 빅데이터 기술과 결합하여 공격을 탐지하는 정보 보안과 이벤트 관리(SIEM, Security Information and Event Management), 머신러닝(ML)을 기반으로 엔드포인트에서 내부자들의 행위기반으로 자동 감지 및 대응하는 사용자 및 개체 행동 분석(UEBA, User and Entity Behavior Analytics)과 같은 기술 솔루션들이 출시되고 있다. 최근에는 SIEM과 UEBA의 확장 개념으로 알려지지 않은 위협에도 대응할 수 있는 종단 탐지 및 대응(EDR)이 차세대 보안관제 기술로 주목받고 있다.

한편, 보안 오케스트레이션, 자동화 및 대응(SOAR, Security Orchestration, Automation and Response)도 AI 기술을 활용한 사이버 공격 자동화 도구에 대응하여 사이버 위협 수준을 자동으로 분류하고, 분석하여 사이버 테러를 예방하는 보안 관제 플랫폼 기술로서의 인프라 기능을 고도화시켜 나가고 있다(오영택 외 2019).

#### 4. 융합산업 보안 기술

IoT, 클라우드, 빅데이터, 5G 등 4차 산업혁명 선도형 핵심 기술들이 전통적 산업들과 기술적으로 융합되면서 융합산업 보안기술은 국가 경제와 국민의 생활안전과 직결되는 국가 안보 영역에 속하는 기술로 인식되고 있다.

먼저, 산업제어시스템(ICS, Industrial Control System)은 국가 중요 기반시설(critical infrastructure) 및 제조 산업의 작업 공정을 감시하고 제어하는 시스템이며, SCADA(Supervisory Control And Data Acquisition, 감시 제어 및 데이터 취득), DCS(Distributed Control System, 분산 제어 시스템), PLC(Programmable Logic Control, 프로그램 가능 논리 제어기), SIS(Safety Instrumented System, 안전계장시스템) 등이 있다. 이러한 시스템들은 그동안 인터넷과 분리되어 제조사의 독자적인 운영체제와 프로토콜(vendor proprietary protocol)을 사용하여 왔다. 하지만 산업제어설비들이 초연결화 되어 감에 따라 사이버 공격의 위협 범위도 운영 기술(OT) 영역으로 확장되고 있다.

산업제어시스템에 대한 공격은 주로 보안 통제가 미흡한 엔드포인트를 경유하거나 공급망에서 취약한 기기나 협력업체에 개방된 네트워크를 경유하여 이루어지고 있다. 따라서 산업제어시스템에 대한 실시간 모니터링과 AI 기반의 이상행위 사전 탐지 및 식별기술이 개발 중이며, 주로 제어시스템에 대한 감사기록 추적 및 모니터링 기술, 산업제어시스템 연계구간별 보안을 위해 망의 완전한 분리를 구현하는 교차 영역 솔루션(CDS, Cross Domain Solution) 기술이 중점 개발되고 있다(이건희, 2019).

스마트그리드(smart grid, 전기 및 정보통신 기술을 활용하여 전력망을 지능화·고도화함으로써 고품질의 전력서비스를 제공하고 에너지 이용효율을 극대화하는 전력망) 보안기술은 신재생에너지원과 친환경 관리를 위해 다양한 IoT들이 인터넷을 이용해 복합적으로 연계되어 있기 때문에 보안 리스크의 범위가 계속 늘어나고 있다. 폐쇄망 내에 위치한 제어시스템은 HW나 SW의 유지보수 및 패치 설치에서 취약점 평가가 이루어져 비교적 안전하다는 평가를 받고 있으나, 여전히 네트워크 공격의 핵심 목표가 되고 있으며, 지능형 검침 인프라(AMI, Advanced Metering Infrastructure) 해킹이나 스마트 그리드 참여자의 과도한 정보 수집으로 인한 개인정보보호 노출 문제도 당면 과제로 부각되고 있다.

특히 스마트그리드나 마이크로그리드(microgrid, 신재생 에너지뿐만 아니라 다양한 분산 에너지원을 경제적으로 조합하여 필요 에너지를 경제적으로 공급하는 지역적 전력망)에 Windows나 Linux와 같은 범용 소프트웨어가 사용되고, 네트워크 표준 프로토콜이 채택되면서 최종적으로 제어계 시스템(OT)을 목표로 하는 사이버 공격기법이 고도화되고 공격 횟수도 크게 증가할 것으로 예상된다. 따라서 화이트리스트(whitelist, 블랙리스트와

반대되는 개념으로 신뢰되는 정보 목록)를 우회하여 침입하는 Black energy나 WannaCry와 같이 기반시설을 공격목표로 하는 악성코드에 대한 보호대책이 요구된다(이대성, 2021).

스마트시티 보안 기술은 스마트시티 인프라 상에서의 데이터 흐름을 안정적으로 유지하고 신뢰성을 확보하기 위해 보안경계 외부에 위치하는 스마트 장비의 펌웨어 불법 조작 방지나 DDoS 등의 사이버 공격을 탐지하고 사전 대응하는 기술이다. 스마트시티 구역 안에서 사용되는 기기종 디바이스간의 상호 인증을 위한 암호화 및 디지털 서명에 의한 무결성 기술, 카메라 및 스마트 장치에서 수집한 데이터의 도청, 차단 및 수정을 방지하기 위한 스마트시티 플랫폼 공격탐지 및 침해차단 기술, 스마트홈 다중 디바이스 보안관리 및 디바이스 취약점 자동 진단기술, IoT를 활용한 생활 안전, 재난 모니터링 예측, 재난 대응 로봇 기술 등이 개발되고 있다(엄익채, 2019).

자율주행차, 드론 등 무인 이동체 보안은 전용 운영 체제(OS, Operating System)를 갖춘 IT 플랫폼이 외부 네트워크에 연결되기 때문에 대형 참사가 예상되는 사이버 위협이 항상 존재하기 때문에 해킹의 진입점인 전자제어장치(ECU, Electronic Control Unit) 접근제어 무력화, 차량/개인정보 보호, 안티 멀웨어(anti-malware, 악성 소프트웨어를 대처하는 소프트웨어) 유입 차단, 블록체인 기반 키 관리, 코드 난독화, 고속 서명 등의 보안기술이 중점 개발될 전망이다.

자율주행 차량의 경우, 차량 간 차량사물통신(V2X, Vehicle-to-Everything) 메시지의 고속 처리를 위한 차량 간 메시지 서명의 고속화 검증기술, 차량 안에서의 다양한 지능형 서비스 이용을 위한 이더넷 보안 및 취약점 분석 기술, 차량 내부 네트워크의 트래픽을 학습(ML)하여 차량의 이상 징후를 탐지하는 알고리즘 개발 등이 진행되고 있다(한국자동차공학회, 2020).

드론 기술과 관련해서는 드론 내에 잠재된 보안 취약점을 사전에 파악하여 취약점을 기반으로 한 공격을 방어하기 위해 인증·드론식별 모듈 개발과 도심 상공에서 사람이나 화물을 운송할 수 있는 차세대 교통체계인 도심용 공중 모빌리티(UAM, Urban Air Mobility)의 안전성 확보를 위한 보안기술이 연구되고 있다.

팬데믹으로 인해 비대면 진료의 필요성이 강조되고 있는 의료보안 영역에서는 의료네트워크, 의료정보시스템, 의료기기의 보안 게이트를 우회하는 해킹을 차단하고, 개인의 바이오 정보, 개인식별 정보 등 민감정보에 대한 비식별화 기술의 개발이 진행되고 있으며, AI 이상 징후 분석기반의 병원 네트워크 침입탐지 및 랜섬웨어 대응, 바이오 정보 기반의 보안통신 등도 연구되고 있다.

## IV 보안 표준화 동향

IoT, 클라우드 컴퓨팅, 빅데이터, 5G 등 4차 산업형 핵심기술들이 전통산업 분야와 스마트 기반의 융합화를 이루면서 새로운 사이버물리시스템(CPS)을 창출하고 있다. 이러한 기술변화 추세에 맞추어 최근 사이버 보안과 관련된 국제 표준활동도 기존의 정보보안 표준기술과 산업별 융합보안 표준기술로 나뉘어 활발하게 연구되고 있다.

보안표준과 관련된 국제기구 중에서 ISO/IEC JTC1, IUT-T는 암호, 보안아키텍처, 보안관리, ID관리, 프라이버시 보호, 스팸 대응 등 사이버 보안 전반에 걸쳐 표준화를 주도하고 있다. 네트워크 보안 표준화와 관련해서는 IEEE802(LAN/MAN 프로토콜 및 보안), 국제 인터넷 표준화 기구(IETF, Internet Engineering Task Force - 인터넷 프로토콜 보안), 유럽 전기통신 표준기구(ETSI, European Telecommunications Standards Institute - 사이버 보안, 모바일 보안), 3GPP(모바일 보안 프로토콜, 서비스 기능), GSMA(모바일 가이드라인, 취약성 대책) 등이 활동하고 있다. 인증/인가 표준에서는 OASIS(Organization for the Advancement of Structured Information Standards, 개방형 데이터 포맷 인증 표준), FIDO(복수 인증, 패스워드 인증), Open ID Foundation(Open ID 인증인가 규격), W3C(웹 인증, 어플리케이션 보안, 프라이버시 보호) 등이 대표적으로 활동하고 있다(IITP, 2020; TTA, 2021).

그림 5. 사이버 보안 관련 국제표준화 기구

보안 표준 전반	■ ISO/IEC JTC1, ITU-T
인증/인가 표준	■ OASIS, FIDO, Open ID Foundation, W3C
유·무선 보안 프로토콜	■ IEEE802, IETF, ETSI, 3GPP, GSMA
정보보호관리체계	■ ISO/IEC JTC1 SC27, ITU-T SG17
개인정보보호 표준	■ OneM2M, ITU-T SG17, ISO/IEC JTC1 SC27

\* 출처: 부산가톨릭대학교 융합보안공학센터(2022)

## 1. 정보보안 표준화 동향

정보보안기술 분야별 표준화 동향을 살펴보면, 암호기술의 표준화는 미국 국립표준기술연구원(NIST), ISO/IEC JTC1 SC27, 국제 인터넷 표준화 기구(IETF, Internet Engineering Task Force)가 중심이 되어 양자 컴퓨터 암호의 안전성 확보를 목표로 연구 중이며, ISO/IEC 양자컴퓨터 알고리즘, ITU-T는 양자 암호통신의 표준, 국제 인터넷 표준화 기구(IETF)는 암호 인증 프로토콜에 암호 알고리즘 적용 표준을 준비 중이다(TTA, 2021).

인증/인가 표준은 사이버 공격 기법의 진화와 서비스 발전 추세에 대응하기 위해 3GPP, W3C, FIDO 등 포럼 단체들이 중심이 되어 새로운 암호·인증 모듈 개발과 연계하여 공개 키 기반구조(PKI, Public Key Infrastructure) 기반의 기기 인증과 비대면 인증기술의 표준화를 추진하고 있다.

프로토콜 보안 표준은 인터넷이나 통신시스템의 안전성 확보를 위해 도메인 네임 시스템(DNS, Domain Name System), 경계 경로 프로토콜(BGP, Border Gateway Protocol) 보호대책 등을 프로토콜별로 보안 기능에 추가하는 것으로, 보안 프로토콜은 SSL/TLS, IPsec 등이 표준화되어 하이퍼텍스트 전송 프로토콜(HTTP, Hypertext Transfer Protocol, 인터넷상에서 데이터를 주고받기 위한 서버/클라이언트 모델을 따르는 프로토콜), 이메일 통신의 암호화에 적용되어 사용 중이며, 5G, 6G 등 타 분야 표준화 전문가들과의 연구교류가 활발하게 이루어지고 있다.

보안관리 표준은 ISO/IEC JTC1 SC27가 중심이 되어 정보보호관리체계(ISMS, Information Security Management System), 정보보안관리, IT 보안성 평가기준 등을 검토하고 있으며, ITU-T SG17은 통신사업자용을 제정하고 있다. 먼저, 공통평가기준(CC, Common Criteria)으로 불리우는 ISO 15408은 국가별로 정보보호 시스템들의 보안성을 평가하고 보안등급별로 인증한 회원국의 CC 인증서를 다른 회원국들도 인정해 주는 국제 평가기준이다. JTC1 SC27와 협력하여 3개 파트로 구성된 15408 버전에 2개 파트가 추가되었으며, ICT 환경 변화에 따른 새로운 기능을 제공하는 제품 평가를 위해 관련 보호 프로파일(PP, Protection Profile)을 계속해서 개발 중이다.

ISO/IEC 27000 계열은 정보보호관리체계 인증 표준 전반에 대한 원칙과 용어, 인증 요구사항을 다루고 있으며, 특히 ISO/IEC 27002를 토대로 퍼블릭 클라우드 상의 개인식별정보(PII, Personally Identifiable Information)를 보호하기 위한 ISO 27018, 네트워크 보안을 위한 ISO 27033, 의료 정보보호관리체계를 위한 ISO 27799가 표준으로 보급되고 있다. 특히, ISO/IEC 27017는 클라우드 서비스를 제공하거나 사용하기 위해 37개의 통제항목과 고객의 가상 환경 보호 및 분리, 가상 머신(VM, Virtual Machine)의 구성, 클라우드

환경과 관련된 관리 작업 및 절차 등 7개 신규 클라우드 통제 항목으로 구성되어 있다(박인상 외, 2020).

또한, ITU-T에서 취약성 정보 공유를 위해 관련 단체 간 표준을 제정하여 취약성 관리, DDoS 대응, 스팸 대응에 활용하기 위해 사이버 보안대책을 마련하고 있는데, ITU-T SG17은 사이버 위협 대응을 위한 악성코드 분석 공유 포맷 표준을 개발하고 있으며, IEEE-SA는 악성코드 교환 포맷의 표준화를 진행 중이다.

이 밖에 개인 데이터의 안전한 유통을 위한 프라이버시 보호(PPM, Privacy Preference Manager)를 위해 oneM2M, ITU-T SG17, ISO/IEC JTC1 SC27에서는 개인의 정보사용 동의 여부 및 동의 내용에 기반 한 데이터 전송 제어 표준이 제정 중이다(TTA, 2021; 국제표준화기구 보안 사이트).

## 2. 융합산업 보안표준화 동향

융합산업 보안표준은 해당 산업 제품 및 서비스의 고유 기능에 본안의 안전성과 신뢰성이 기술적으로 융합되는 영역이기 때문에 차세대 보안 표준 활동이 활발하게 진행 중이다. 특히, 소프트웨어 정의 네트워킹(SDN), 네트워크 기능 가상화(NFV)와 같은 가상화 기술들이 차세대 IT 인프라에 적용됨에 따라 이에 대응하기 위한 보안 표준이나, 초연결 인프라를 구성하는 플랫폼의 안전·신뢰성에 대한 공급망 보안, SW/HW 보안성 평가, 취약성 관리 표준 등이 강조되고 있다(한국자동차공학회, 2020).

또한, 자율주행차나 드론 보안, 스마트 헬스 보안, 스마트 시티 보안, AI 엔진 신뢰성 등과 같이 차세대 융합보안 기술의 보안 우수성을 확보하기 위한 표준화 노력도 함께 추진되고 있다.

ISO/IEC 21827은 ISO 제어 목표의 성숙도를 측정할 수 있는 시스템 보안 엔지니어링 능력 성숙모델(SSE-CMM)을 기반으로 하는 국제 표준이며, IEC 62443 사이버 보안 표준은 산업 자동화 및 제어 시스템(IACS, Industrial Automation and Control Systems)에 대한 프로세스, 기술 및 요구 사항을 정의하고 있다(최동진, 2019).

융합산업 생산 인프라의 백본망(backbone network)이라 할 수 있는 5G 보안은 3GPP, ITU-T SG 17, ETSI 등이 비공용 네트워크(NPN, Non Public Network)에서 초신뢰·지연통신(URLLC, Ultra-Reliable Low-Latency Communication)을 지원하는 버티컬 서비스(vertical service, 한 부분의 기능만을 집중적으로 제공하는 서비스)에 필요한 보안요구 사항을 표준화하고 있다.

자율주행차 보안 표준은 ITU-T SG17과 ISO TC204/TC22, 스마트 시티 보안 표준은 ITU-T SG17/SG20, oneM2M, AI 엔진 신뢰성은 ISO/IEC JTC1 SC42, 전기전자공학자협회(IEEE, Institute of Electrical and



Electronics Engineers)가 중심이 되어 활동하고 있다. ISO/SAE 21434는 차량의 개발 수명 주기에 대한 사이버 보안 조치에 관한 표준이며, 자율주행 인간공학, 정밀지도, 기능 안전 및 사이버 보안, 차량제어 등의 분야로 나뉘어 표준 활동이 진행되고 있다(한국자동차공학회, 2020).

IoT 보안 표준은 ITU-T, ISO/IEC, IETF, ETSI, GSMA, CITS 등 많은 표준단체들이 참여하고 있으며, ETSI EN 303 645는 IoT에서 발생이 우려되는 데이터의 도난과 조작을 차단하는데 필요한 IoT 개발자나 제작업체를 위한 기술 제어 및 조직 정책 표준으로 활용된다. 다만, IoT 보안 표준은 보안 문제의 심각성에도 불구하고 아직까지 충분한 표준안이 마련되지 못한 상태이다. IoT, 5G, AI 등을 활용하는 스마트시티 표준화도 ITU-T SG20, ISO TC268, JTC1 WG 11 등이 주요 가이드라인, 평가지표, 플랫폼 관련된 표준화를 진행 중이다(TTA, 2021).

스마트그리드 보안 표준화는 IEC SG 3(Strategic Group 3)의 28개 기술위원회가 100개 이상의 국제표준 작업을 진행 중이다. SG3은 스마트그리드를 11개 분야로 나누어 표준을 개발하고 있는데, 특히 배전망 관리, 수요가 에너지 관리, E-mobility 표준화에 주력하고 있다. 국제 인터넷 표준화 기구(IETF)도 대규모로 설치되고 있는 수많은 노드들이 네트워크를 통해 연결되는 스마트 미터링(계량기에 지능정보기술이 융합되어 에너지 계량정보가 에너지 공급자와 수요자 간에 쌍방향으로 원격에서 실시간으로 활용이 가능하도록 하는 디지털 플랫폼) 보안을 위해 기존의 확장 가능한 인증 프로토콜(EAP, Extensible Authentication Protocol)을 사용해 네트워크에서 디바이스 인증을 구현하는 IP 기반 프로토콜 PANA(Protocol for Carrying Authentication for Network Access)를 정의했다(이대성, 2021).

의료기기 보안 표준화는 환자의 안전을 중시하여 리스크 관리에 중점을 두고 진행되고 있으며, 의료기기의 설계와 개발뿐 아니라 기존 의료기기에 새로 적용되는 소프트웨어의 보안 패치(patch) 운용 등을 중심으로 진행되고 있다. IEC 62304는 의료기기 소프트웨어, IEC 62304는 헬스케어 소프트웨어, IEC 82304-1은 헬스케어 소프트웨어 제품 영역을 각각 다루고 있다(국제표준화기구 보안 사이트).

이 밖에 해양 선박과 관련된 표준화는 국제해사기구인 IMO(International Maritime Organization)를 비롯하여 ISO, IEC, ITU 등 국제표준기구에서 선박 원격 관제 및 제어, 선박통신 및 네트워크 기술, 자율운항시스템을 중심으로 표준화가 진행되고 있다.

## V 맺음말

코로나-19 팬데믹 이후 재택근무, 원격교육, 영상회의 등 비대면 문화가 일상화되고, 보안경계 외부로부터의 트래픽 유입이 급증하면서 조직의 내부와 외부를 경계로 하는 기존의 보안경계 개념이 빠르게 무너지고 있다. 그리고 스마트 시티, 스마트 팩토리, 스마트 팜 등 산업 생산 시설과 사회 인프라의 스마트화가 진전되고, 사이버 공격자들의 자동화 도구를 이용한 실시간 메가 공격이 예상됨에 따라 초연결·초저지연·초고속 사이버 공간과 물리적 공간을 동시에 보호하기 위한 제로 트러스트의 도입 등 차세대 보안기술의 혁신이 요구되고 있다.

이를 위해 기밀성, 무결성, 가용성 보장이라는 기존 사이버 보안기술의 영역을 벗어나 데이터, 시스템, 네트워크, 디바이스 전 구간과 물리적 보안 공간에서 발생하는 초대용량의 위협정보를 실시간 수집, 분석할 수 있는 AI 기반의 보안관제 및 실시간 사고대응 체계와 같은 보다 고도화된 보안 프레임워크가 구현되어 나갈 것으로 예상된다.

또한 개인 데이터의 익명화 및 가명화 등 사이버 공격자의 빅데이터 분석 능력을 차단하기 위한 개인정보보호 기술의 확보 노력과 함께 서비스 복원력(service resilience)과 실시간 오류 대응이 가능한 카오스 엔지니어링(chaos engineering), 사이트 신뢰성 공학(SRE, Site Reliability Engineering)의 활용 등 보다 확장된 영역의 기술개발도 활발하게 연구될 것으로 전망된다.

### 저자\_ 이대성(Daesung Lee)

#### • 학력

인하대학교 컴퓨터정보공학 박사  
 인하대학교 전자계산공학 석사  
 인하대학교 전자계산공학 학사

#### • 경력

現) 부산가톨릭대학교 컴퓨터공학과 교수  
 現) 국가사이버안보센터 정보보안관리실태 평가위원

## 참고문헌

### 〈국내문헌〉

- 1) 과학기술정보통신부. (2021.02). 데이터보호 핵심기술 개발 전략, 1~6.
- 2) 김대원, 강동욱, 최용제 외. (2020). 공급망 보안기술 동향. 전자통신동향분석, 35권 제4호, 한국전자통신연구원
- 3) 박인상, 이호형, 조수연. (2020). 클라우드 보안기술 및 표준동향. Weekly ICT Trend 주간기술동향, 제 1977호, 정보통신기획평가원.
- 4) 오영택, 조인준. (2019). 인공지능 기술기반의 통합보안관제 서비스모델 개발방안. 한국콘텐츠학회, Vol.19 No.1, 108~116.
- 5) 엄익채. (2019). 스마트시티 보안 이슈와 대응기술 동향. Weekly ICT Trend 주간기술동향, 1923호, 정보통신기획평가원.
- 6) 이건희. (2019). ITU-T 사이버물리시스템(CPS) 보안 표준화 동향. 정보보호학회지, 29(2).
- 7) 이대성. (2019). 차세대 사이버 보안기술 동향. Weekly ICT Trend 주간기술동향, 제 1916호, 정보통신기획평가원.
- 8) 이대성. (2021). 지능형 전력망의 안전성과 신뢰성 확보를 위한 보안위협과 정책 분석. 한국정보통신학회논문지, Vol. 25 No.10, 1381~1390.
- 9) 이윤수, 문형우, 박건량 외. (2021). 코로나19에 따른 사이버위협 및 대응기술 동향(보안과제와 침해대응 서비스를 중심으로). 정보보호학회지, 31(5).
- 10) 정보통신기획평가원(IITP). (2020.12). ICT R&D 기술 로드맵 2025 - 차세대 보안·블록체인, 7~27.
- 11) 정부 합동. (2020.06). 제2차 정보보호산업 진흥계획(2021~2025), 14~29, 42~46.
- 12) 최동진. (2019). 5G 시대의 차세대 IoT 보안. Weekly ICT Trend 주간기술동향, 제 1914호, 정보통신기획평가원.
- 13) 한국과학기술기획평가원(KISTEP) & 정보통신기획평가원(IITP). (2021). 2022년 기술트렌드 분석과 시사점. 과학기술 & ICT 정책·기술동향, No. 206, 1~7.
- 14) 한국자동차공학회. (2020.01). 자율주행차 표준화 전략 로드맵, 4~5.
- 15) 한국정보통신기술협회(TTA). (2021.12). 차세대 보안, ICT 표준화 전략맵, 331~385.

### 〈국외문헌〉

- 16) Gartner. (2021.06). 2021 Gartner Hype Cycle for Security Operations.
- 17) ICF. (2020). The Impact of COVID on the Cybersecurity Sector. ICF White paper.
- 18) Ross. R., Pillitteri, V., Graubat. R., Bodeau. D., Mcquaid. R. (2021.12). Developing Cyber Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, Vol. 2, 7~22.
- 19) Rose. S., Borchert. O., Mitchell. S., Connelly, S. (2020.08). Zero Trust Architecture, NIST Special Publication 800-207, 36~42.

〈기타문헌〉

- 20) 과학기술정보통신부 보도자료. (2022.04). 최근 사이버 위협동향 및 대응방안. e-브리핑시스템.
- 21) 국제표준화기구 보안 관련 사이트(ISO, ITU-T, IETF)
- 22) 이글루시큐리티. (2022.01.05.) 2021년 보안위협 분석을 통한 2022년 보안위협 및 보안기술 전망. <https://www.igloo.co.kr/security-information/2021%EB%85%84-%EB%B3%B4%EC%95%88%EC%9C%84%ED%98%91-%EB%B6%84%EC%84%9D%EC%9D%84-%ED%86%B5%ED%95%9C-2022%EB%85%84-%EB%B3%B4%EC%95%88%EC%9C%84%ED%98%91-%EB%B0%8F-%EB%B3%B4%EC%95%88%EA%B8%B0%EC%88%A0/>
- 23) 이글루시큐리티. (2022.01.06). 2021 사이버 위협 동향. <https://www.igloo.co.kr/security-information/2021%EB%85%84-%EC%82%AC%EC%9D%B4%EB%B2%84-%EC%9C%84%ED%98%91-%EB%8F%99%ED%96%A5/>



# 02

## 개인인증과 보안을 위한 생체인식 센서 기술

박영삼(한국전자통신연구원 책임연구원)

# I 생체인식 기술

## 1. 생체인식 기술의 개요

‘생체’란 살아있는 생명체의 몸이며, ‘센서’란 소리와 빛, 온도와 압력 등의 물리량을 검출하는 소자 또는 그 소자를 갖춘 기계장치로 정의된다(네이버 사전). 본 고에서 ‘생체인식 센서’는 살아있는 사람의 고유한 신체 특징 혹은 행동 특징의 정보를 검출하는 소자 또는 그 소자를 갖춘 기계장치로 정의하고자 한다.

생체인식 기술은 개인인증과 보안을 위한 목적으로 다양한 산업에서 활용이 가능하다. 개인인증과 보안을 위해 기존에 사용되어 오던 비밀번호 또는 공인인증서의 경우, 잊어버리거나 잃어버릴 시 새로 발급받아야 하는 불편함이 있으며, 다른 사람이 도용하여 사용할 수 있다는 우려가 있다. 하지만, 생체인식 기술을 사용한다면 그 불편함과 우려를 줄일 수 있다.

생체인식 기술로 활용되기 위한 생체의 대표적인 특징은 다음의 여섯 가지이다(김도현, 2021). 1) 보편성: 모든 사람이 가지고 있어야 한다, 2) 유일성: 개인마다 구별될 수 있는 특징이어야 한다, 3) 영구성: 변화하거나 변경되지 않아야 한다, 4) 획득성: 생체특성 정보를 추출하고 정량화하는 데 어려움이 없어야 한다, 5) 정확성: 생체특성 정보는 정확하고 빠르게 얻어야 하고 언제 정보를 얻더라도 항상 같은 값을 얻어야 한다, 6) 접근성: 생체정보 특성 추출 방법에 대한 사용자의 거부감이 없어야 한다, 6) 기만성: 부정사용으로부터 안전하여야 한다.

## 2. 생체인식 기술의 종류와 특징 그리고 응용 분야

생체인식으로 활용되는 신체의 특정 부분으로는 지문, 정맥, 홍채, 얼굴 등이 있는데, 여기에는 대부분 각 개인의 선천적 요인으로 생성된 특징이 있다. 한편 행동학적 특징의 예로는 음성, 걸음걸이, 서명인식 등이 있는데, 이들 대부분은 후천적인 요인으로 생성된 특징이다(Bouchrika, 2018). 생체인식 기술은 스마트폰과 노트북 같은 모바일 기기 분야, 은행 입출금 등의 금융 분야, 차량 문을 열고 시동을 켜는 등의 자동차 분야, 시스템과 데이터에 대한 접근과 인증제어 등의 보안과 국방 분야, 동사무소 서류 발급 등의 공공분야 등에서



폭넓게 사용되고 있다. 이중, 스마트폰 시장은 생체인식 기술의 가장 큰 시장 중의 하나로서, 지문인식 뿐만 아니라 얼굴인식 등 다양한 기술들이 소비자의 선택을 받기 위해 서로 경쟁 중이다.



\* 출처: Bouchrika(2018)

아래의 <표 1>은 각각의 신체적 특성과 행동적 특징을 이용한 생체기술에 대한 종류와 특징을 정리한 표이다. 지문인식 기술은 스마트폰 잠금 해제와 모바일 결제 등을 통해 대중에게 가장 널리 알려진 생체인식 기술 중 하나로서, <표 1>에 제시된 기술 중 현재 가장 수요가 큰 기술이다.

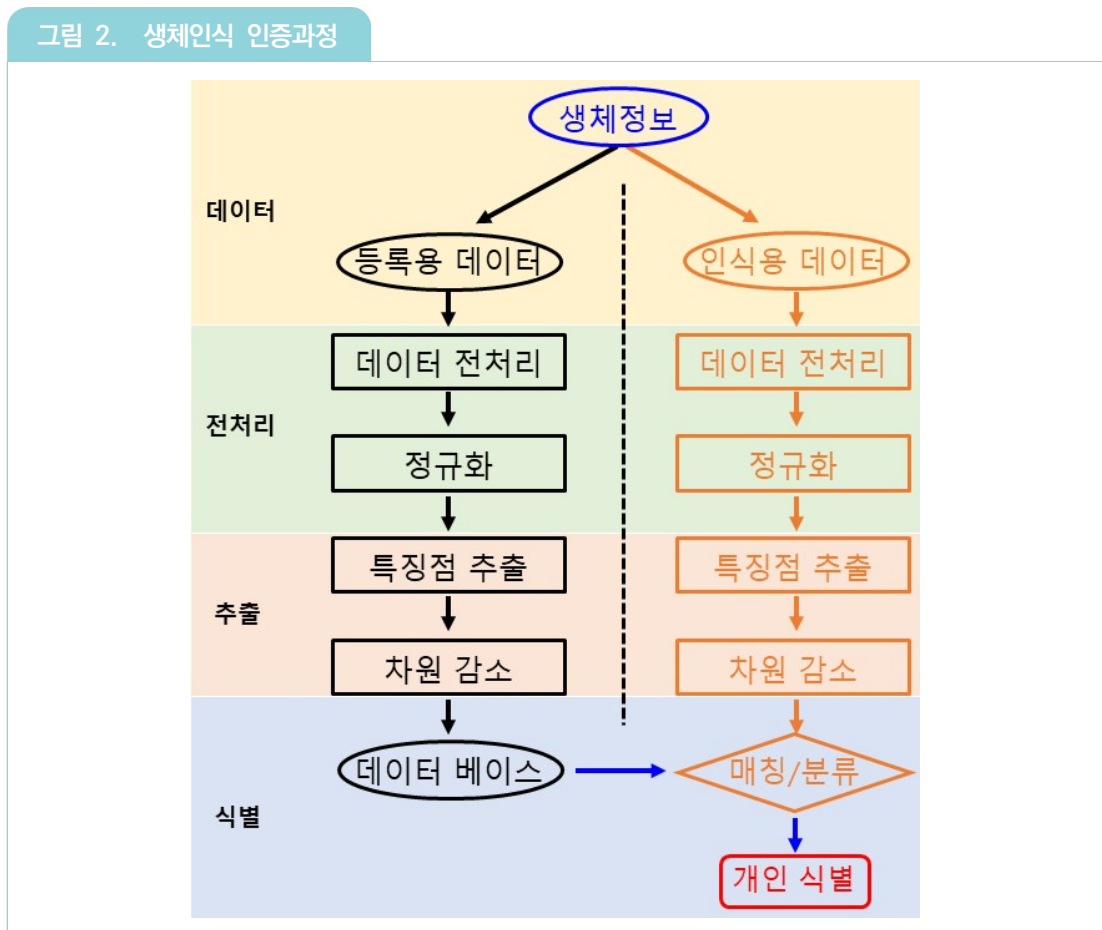
표 1. 신체 특징과 행동 특징을 이용한 생체인식 기술의 종류와 특징

종류	특징
지문 인식	<ul style="list-style-type: none"> <li>• 개요: 지문의 디지털영상을 획득하여 사용자를 인식하는 기술임</li> <li>• 장점: 낮은 에러율과 비교적 높은 인식을 및 빠른 검증 속도라는 장점 외에도 다른 생체인식 기술과 비교하여 사용자의 적은 부담감과 소형화의 장점 가짐</li> <li>• 단점: 지문이 손상되거나 없어진 경우, 잘리거나 메마른 피부, 붕대를 감았거나 피부가 굳은 손가락은 지문인식에 어려움이 있음</li> </ul>
정맥 인식	<ul style="list-style-type: none"> <li>• 개요: 육안으로는 보이지 않으나 정맥 패턴이 사람마다 다르다는 점에서 착안한 것으로, 적외선을 사용하여 혈관을 투시한 후 그 영상 이미지를 이용하여 신분을 확인하는 기술임</li> <li>• 장점: 정맥은 인체 내부에 있어 외상이나 노화로 인한 변형 가능성이 작고 복제가 거의 불가능함</li> <li>• 단점: 손등의 피부 배경으로부터 정맥이 분포한 부분을 추출하기가 쉽지 않아 하드웨어 구성이 복잡하고 소형화가 어려워 시스템 크기도 크고 시스템 구축 비용이 큼</li> </ul>
홍채 인식	<ul style="list-style-type: none"> <li>• 개요: 사람의 눈에서 중앙의 검은 동공과 흰자 사이에 존재하는 도넛 모양의 홍채를 이용하여 사용자를 인증하는 기술임</li> <li>• 장점: 사람의 홍채는 쌍둥이조차 서로 다른 패턴들을 가지고 있어 통계학적으로 DNA 분석보다 정확하다고 알려져 있음. 홍채는 복제가 거의 불가능하고, 외상 또는 아주 드문 질병을 제외하고는 평생 변화하지 않으며, 콘택트렌즈나 안경을 착용하더라도 인식 가능함</li> <li>• 단점: 인식 방법에 따라 거부감이 생길 수 있고, 시스템 구축 비용이 고가임</li> </ul>
얼굴 인식	<ul style="list-style-type: none"> <li>• 개요: 얼굴 전체보다는 코와 입, 눈썹, 턱 등 얼굴 골격이 변하는 주요 부위 50여 곳을 분석하여 인식함</li> <li>• 장점: 사용자의 거부감이 적으며, 사용자의 판독을 위해 제출된 사진이 남기 때문에 사용자의 사후 추적이 가능함</li> <li>• 단점: 조명, 환경과 영상의 각도에 민감하며, 변장, 세월이 흐르면서 생기는 얼굴 변화, 성형수술, 쌍둥이의 유사한 얼굴 특징 등을 구분하는 데 어려움 있음</li> </ul>
음성 인식	<ul style="list-style-type: none"> <li>• 개요: 음성으로부터 추출한 독특한 특성을 이용하는 인식기술로써 음성 경로, 비강과 구강의 모양 등에 의한 음성학적 특성을 이용</li> <li>• 장점: 음성인식은 인간에게 친숙한 정보 전달 방법이기 때문에 별도의 학습이나 훈련 없이도 기기를 손쉽게 사용할 수 있으며, 손과 발이 자유롭지 못한 상황에서도 정보를 입력할 수 있음</li> <li>• 단점: 사용자에 따른 인식을 차이, 주변잡음, 인식대상 어휘 제한 등에서 한계를 보임</li> </ul>
걸음 걸이	<ul style="list-style-type: none"> <li>• 개요: 걸음걸이 특성을 분석하여 인식하는 기술임</li> <li>• 장점: 다른 기술에 비해 장거리에서도 등록 및 인증 가능하며, 한꺼번에 인증해야 할 경우 인증 시간이 많이 단축될 수 있음</li> <li>• 단점: 사용자 옷, 바닥 표면, 신발, 부상 여부, 가방과 우산 등 외부 영향을 많이 받으며 시스템을 소형화하기가 어려움</li> </ul>
서명 인식	<ul style="list-style-type: none"> <li>• 개요: 필체 역학을 이용하여 압력이나 속도를 분석하여 인증하는 방법임</li> <li>• 장점: 사용이 쉽고, 언어라서 자유로우며, 빠른 인증 속도와 작은 저장 공간이 사용되는 장점이 있음</li> <li>• 단점: 변조가 쉽고, 인증 시 측정범위와 식별 기준을 잡기 어려우며, 수전증 등 지병이 있는 경우 사용하기 어려움</li> </ul>

\* 출처: 박범근(2016) 문헌을 참고하여 재구성

### 3. 생체인식 인증과정

생체인식을 위해서는 등록과 인식 과정이 있어야 한다(김도현, 2021). 등록과 인증과정은 다음의 세 가지 단계, 즉 데이터 단계, 신호처리를 기반으로 한 전처리 단계, 생체 특징점 추출 단계를 차례로 거친다. 그 후 최종 단계에서 등록 과정의 경우 각 개인을 대표하는 생체 특징점을 데이터베이스에 저장하는 단계, 인식 과정의 경우 새롭게 들어온 생체 특징점과 기존 데이터베이스에 저장되어 있던 생체 특징점들을 비교 분석하여 개인을 식별하는 단계를 거친다.



\* 출처: 김도현(2021)

## II 지문인식 센서 기술

### 1. 개인 식별을 위한 지문의 특징점

지문에는 약 40개 정도의 개인별 특징점이 있는데, 그중 융선과 골이 있다(백영현, 2018). 융선은 빙빙 돌아가는 선이며, 골은 융선과 융선 사이의 공간이다. 분기점은 융선이 흐르다가 갈라지는 부분, 끝점은 융선이 흐르다가 끊어지는 부분이다. 중심점은 융선의 굴곡이 위쪽으로 큰 곳이며, 삼각주는 융선 흐름이 세 방향으로 모이는 지점이다.

그림 3. 지문의 특징점



\* 출처: 백영현(2018)

## 2. 벌크형 vs 필름형 지문인식 센서

지문인식 센서는 두께에 따라 벌크형(bulk-type)과 필름형(film-type), 두 가지로 분류할 수 있다. 아래 <그림 4>의 왼쪽 사진은 두께가 두꺼운 벌크형 센서이고 오른쪽 사진은 스마트 폰에 사용되는 두께가 작은 필름형 센서이다.

그림 4. (좌) 벌크형 센서, (우) 필름형 센서



\* 출처: 삼성디스플레이 뉴스룸(2019)

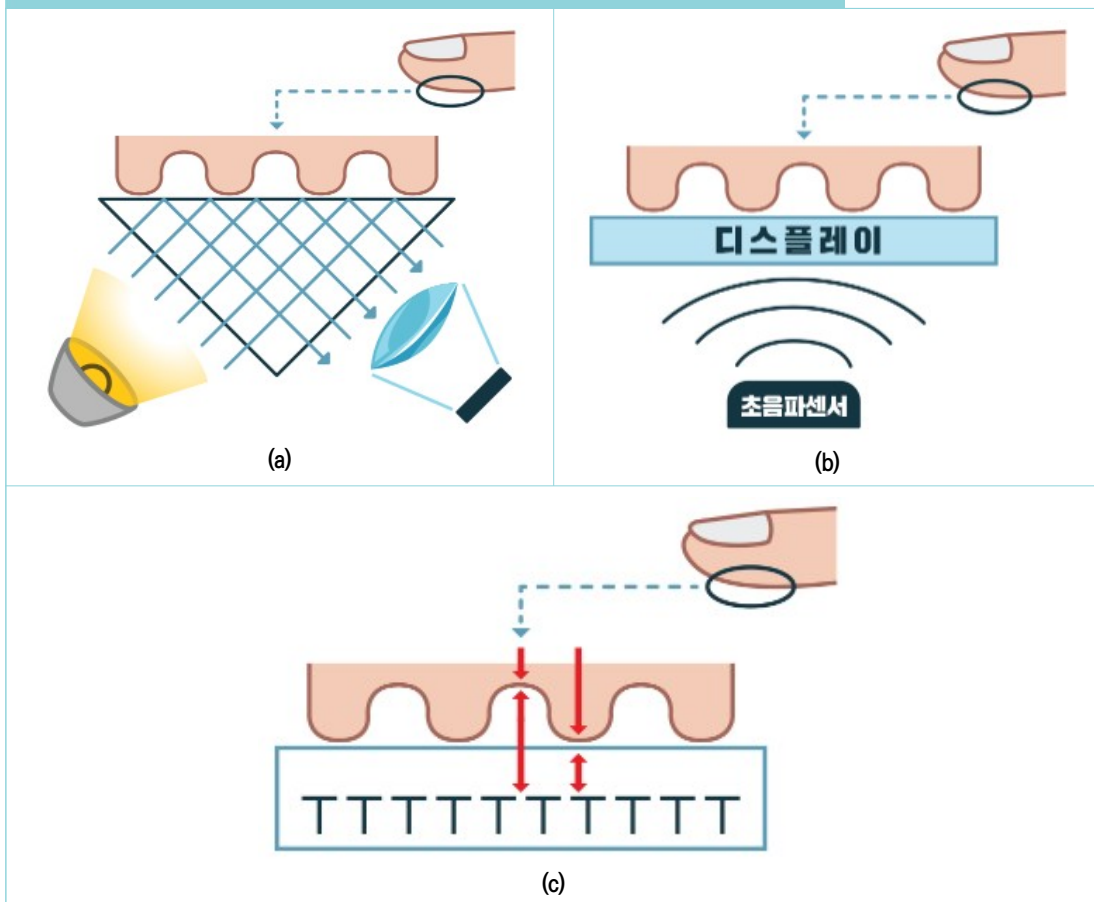
## 3. 광학방식 vs 초음파방식 vs 정전용량방식 지문인식 기술

필름형 센서의 주요 활용처 중 하나인 스마트폰에 활용되는 지문인식 방법으로 <그림 5>와 같이 광학방식, 초음파방식과 정전용량방식, 세 가지가 있다. 광학방식(<그림 5a>)은 카메라로 지문 사진을 찍는 방법으로, 광원을 지문으로 쏘면 빛은 지문에서 반사된 후 되돌아오는데 용선과 골에서 빛의 밝기 차이가 생기는 것을 활용하여 지문 이미지를 확보한다. 2020년 광학방식 점유율이 60%로써 대세인 것으로 보도되었다(디지털데일리, 2020).

초음파방식(<그림 5b>)은 초음파 센서에서 발사된 초음파가 용선과 골을 맞고 되돌아오는 시간이 서로 다른 것을 활용한다. 발사된 초음파는 유리와 플라스틱 등의 스마트폰 패널 물질 종류와 상관없이 투과할 수 있으므로 초음파방식은 패널 구조로부터 설계가 자유롭고 지문인식 정확도가 세 가지 방식 중 가장 높다는 장점이 있다. 그러나 높은 가격이 가장 큰 단점이다. 광학방식과 초음파방식은 디스플레이 내장형 지문센서(FoD, Fingerprint on Display) 구현이 가능한 기술이다.

정전용량방식(그림 5c)은 용선과 골의 경우 정전용량 값(capacitance value) 차이가 난다는 원리를 활용한다. 단점으로는, 지문인식 센서와 손가락 지문 사이의 거리가 0.3mm를 넘으면 제대로 인식되지 않을 수 있다는 점이다. 스마트폰 커버글라스 두께가 대부분 0.45~0.7mm 정도이기 때문에 정전용량방식 지문인식 센서는 스마트폰 옆면 혹은 후면에 위치하는 경우가 많다.

그림 5. (a) 광학방식, (b) 초음파방식, (c) 정전용량방식 지문인식 기술



\* 출처: 삼성디스플레이 뉴스룸(2019)

지문인식 센서 기업으로는 크루셜텍, 이지스텍, 구덕스, 쉘컴 등이 있다. 크루셜텍은 정전용량방식 업체로써 광학방식 지문인식 센서도 양산하고 있다. 이지스텍과 구덕스는 광학방식에 주력하고 있으며 쉘컴은 초음파방식에 강점이 있다(디지털데일리, 2019).

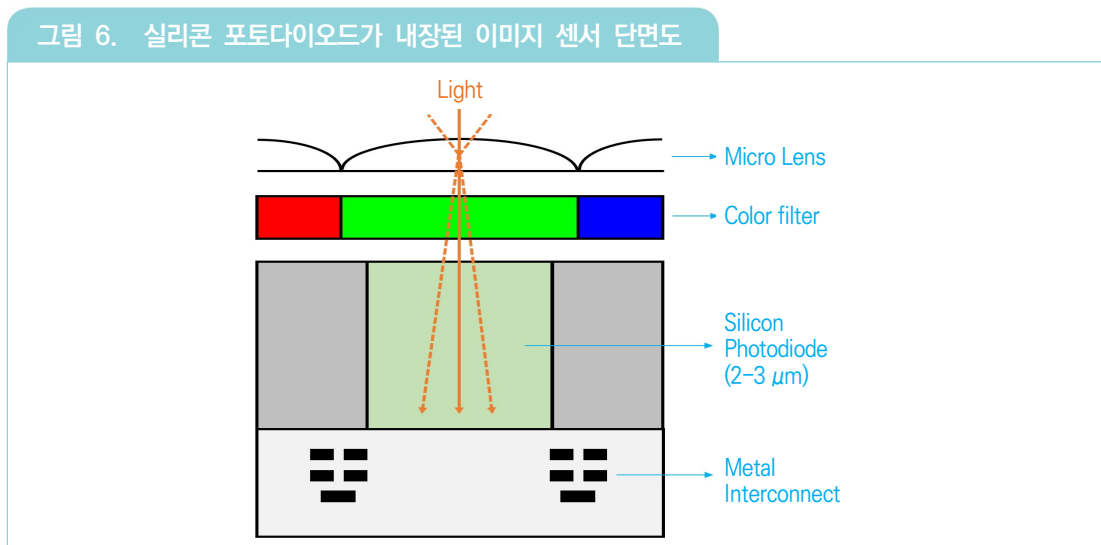


#### 4. 광학방식 지문인식 센서 기술

광학방식, 초음파방식과 정전용량방식 중 대체로 자리를 잡은 광학방식 기술(디지털데일리, 2020)은 이미지 센서(image sensor) 기술을 활용한다(AZoSensors, 2014). 이미지 센서는 빛을 흡수하고 이를 디지털(digital) 신호로 변환한 후 영상으로 보여주는 반도체 소자(semiconductor device)이다.

이미지 센서 기술은 시모스(CMOS, Complementary Metal Oxide Semiconductor)와 시시디(CCD, Charge Coupled Device), 두 가지 기술로 분류될 수 있는데, 이미지 센서 시장에서 CMOS 기술이 우위를 차지하고 있다. CMOS 기술은 빛 에너지에 의해 발생한 전하를 각 픽셀에서 바로 전기신호로 변환하는 방식으로써, CMOS 반도체 표준 공정을 사용하기 때문에 이미지 센서와 주변 회로를 하나의 칩 안에 집적화시킬 수 있고, 가격 경쟁력이 높고 소형화가 가능하며 전력 소비량이 적다는 장점이 있다. CCD 기술은 빛 에너지의 양에 따라 전하의 생성되는 양이 달라지는데, 생성된 전하를 축적한 후 이를 전기신호로 변환하는 방법을 사용한다. CMOS 기술과 비교해 CCD 기술은 전력 소비량은 많지만 노이즈가 적고 해상도가 높다는 장점이 있다.

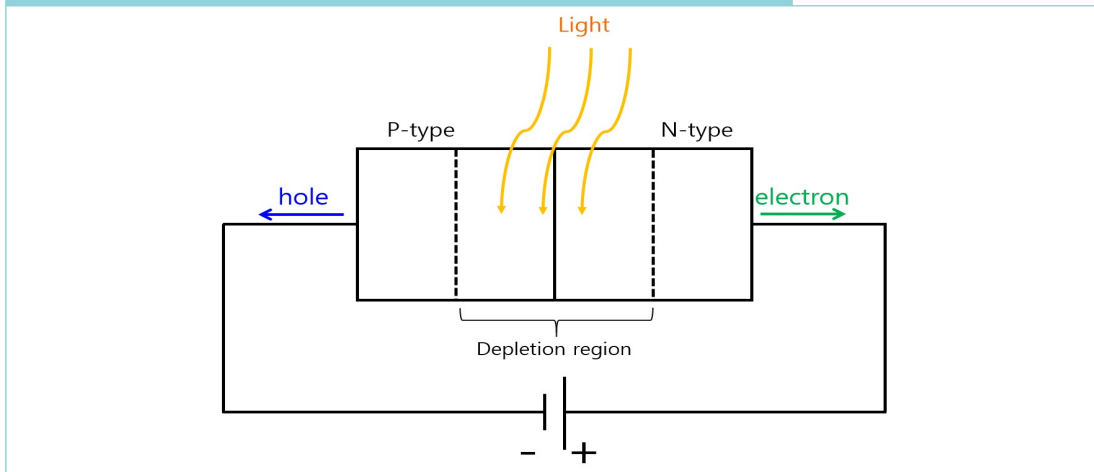
〈그림 6〉은 실리콘 포토다이오드(silicon photodiode)가 내장된 이미지 센서의 단면도 그림이다. 빛은 마이크로 렌즈(micro lens), 칼라필터(color filter), 실리콘 포토다이오드를 차례로 거치며 이동한다. 마이크로 렌즈는 더욱 많은 빛을 칼라필터로 보내주고, 칼라필터는 적색(red), 녹색(green), 청색(blue) 중 희망하는 빛의 파장을 선택하고, 실리콘 포토다이오드는 빛을 흡수한 후 이를 전기신호로 바꾸는 역할을 한다.



\* 출처: Panasonic Holdings Corporation(2016)

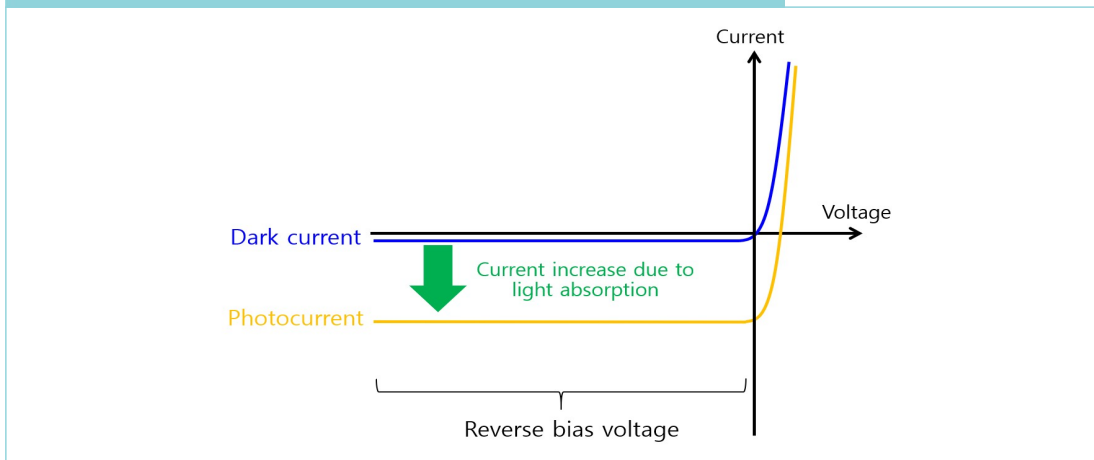
〈그림 7〉은 역방향 전압(reverse bias voltage)이 걸린 상태에서 pn 접합(pn junction)을 이용한 포토다이오드의 동작을 나타낸 그림이다. 빛을 차단한 상황에서 역방향 전압을 걸어놓으면 전류가 거의 흐르지 않는다. 이때의 전류를 암전류(dark current)라고 한다(〈그림 8〉 참고). 하지만, 포토다이오드가 빛을 받으면 〈그림 8〉와 같이 암전류보다 매우 큰 광전류(photocurrent) 값이 측정되는데, 이는 빛 에너지 흡수로 인해 전자(electron)와 홀(hole)이 생성되고 이들이 〈그림 7〉과 같은 방향으로 각각 이동하기 때문이다.

그림 7. 역방향 바이어스 상태에서 빛을 흡수한 포토다이오드 동작



\* 출처: Nalwa(2001)

그림 8. 역방향 바이어스 상태에서 빛의 흡수에 따른 광전류 발생



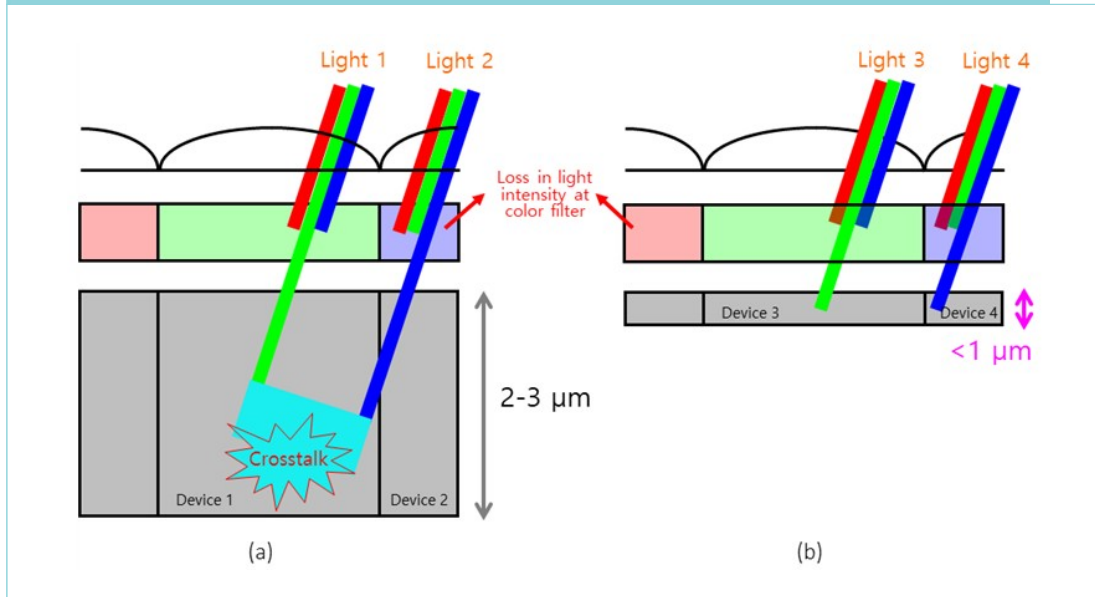
\* 출처: Nalwa(2001)

파나소닉은 2~3 $\mu\text{m}$  두께의 실리콘 포토다이오드를 0.5 $\mu\text{m}$  두께의 유기물질로 바꾸면, 이미지 센서의 감도를 높이고(high sensitivity), 다양한 각도에서 더 많은 빛을 흡수(wide incident angle)할 수 있음을 발표하였다(Panasonic Holdings Corporation, 2016).

실리콘은 물질 자체의 광흡수계수(light absorption coefficient, 빛을 흡수하는 정도를 나타내는 상수)가 낮기 때문에 일정량 이상의 빛을 흡수하기 위해서는 적어도 수 마이크로미터의 두께가 반드시 필요하지만 이로 인해 포토다이오드 소자들 간의 빛 간섭(crosstalk)이 발생한다(정대성, 2017). 또한 실리콘은 빛을 팬크로매틱(다파장) 흡수(panchromatic absorption)하는 특성을 가지므로 적색, 녹색, 청색 파장을 선택한 후 흡수하기 위해서는 칼라필터가 필요하다. 하지만 이를 광흡수계수가 큰 유기물로 대체하면 유기물 두께를 낮출 수 있으므로 소자들 간의 빛 간섭을 줄일 수 있다. 또한 적색, 녹색, 청색 파장을 선택하여 흡수할 수 있는 유기물을 개발한다면 칼라필터 없이도 포토다이오드를 제작할 수 있다(정대성, 2017).

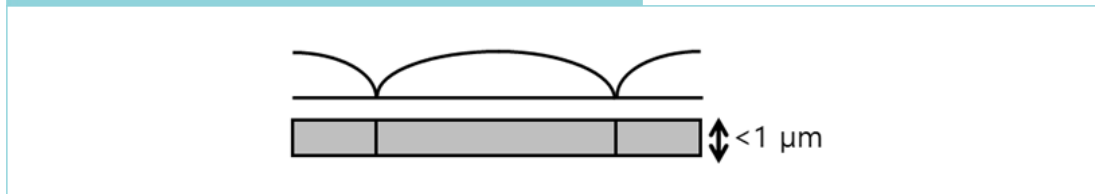
빛은 광원으로부터 360도 모든 각도로 방사된다. 따라서 이미지 센서는 수직 방향으로 들어오는 빛뿐만 아니라 비스듬한 방향으로 들어오는 빛까지 흡수하게 된다. <그림 9>는 빛이 비스듬하게 입사하는 경우 포토다이오드 소자의 광흡수층 두께가 감소함에 따라 빛 간섭이 줄어드는 것을 설명해주는 그림이다. <그림 9a>에서 보이는 바와 같이 Light 1은 녹색 칼라필터를 거친 후 녹색광이 Device 1에 도달한다. 한편 Light 2의 경우에는 청색 칼라필터를 거친 후 청색광이 Device 1에 도달한다. Device 1의 경우 상단에 녹색 칼라필터가 배치되어 있으므로, 녹색광만 흡수하는 것이 바람직한 것으로 설계되어 있지만, 실제로는 녹색광뿐만 아니라 청색광도 도달하기 때문에 빛 간섭이 발생한다. <그림 9b>와 같이 포토다이오드 소자의 광흡수층 두께가 1 $\mu\text{m}$  이하로 감소하면 Device 3에는 희망하는 녹색광만 도달하고 희망하지 않는 청색광은 도달하지 않는다. 그러나 <그림 9a>와 <그림 9b>에서와 같이 칼라필터가 배치되어 있으면, 칼라필터를 통과할 때 빛의 손실(loss in light intensity)이 발생하기 때문에 <그림 10>과 같이 유기물 등을 활용하여 칼라필터가 없는 포토다이오드를 구현하기 위한 노력이 진행 중이다.

그림 9. 칼라필터가 장착되고 포토다이오드의 광흡수층 두께가 (a) 두꺼운 소자와 (b) 얇은 소자



\* 출처: 정대성(2017)

그림 10. 칼라필터 없고 광흡수층 두께가 얇은 소자



\* 출처: 정대성(2017)

## 5. 기관별 동향

### 5.1. 한국전자통신연구원(ETRI)

한국전자통신연구원은 FIDO(Fast Identity Online) 연합 회원으로, 2015년부터 국제인증을 받은 FIDO 기술을 21개 핀테크와 보안 기업에 기술을 이전하였으며, 이전된 기술들은 간편 결제와 스마트뱅킹 등 핀테크 서비스에 적용되어 사업화 중이다. FIDO는 삼성전자, 구글, 마이크로소프트, 비자, 페이팔 등 190개 글로벌 기업이 회원으로 참여 중인 생체인증 국제표준 단체이다.

한국전자통신연구원은 울산과학기술원(UNIST), 크루셜텍과의 협업으로 정전용량방식의 지문인식 센서를 개발하였다(그림 11) 참고).

그림 11. ETRI-UNIST-크루셜텍 공동개발 정전용량방식 지문인식 센서기술로 얻은 지문 이미지

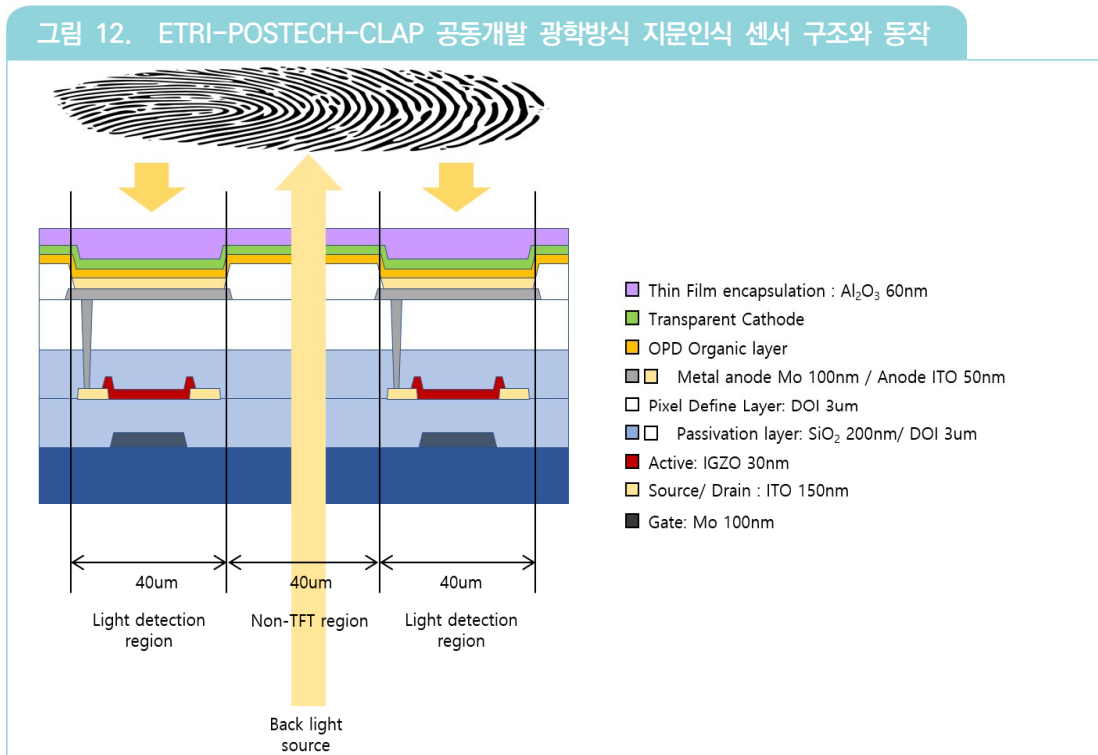


\* 출처: Seo et al.(2018)

또한, 한국전자통신연구원은 포항공과대학교(POSTECH) 정대성 교수와 클랩(CLAP)과 협업으로 광학 방식을 활용하여 핸드폰 화면 일부가 아닌 전면에 도입될 수 있는 프린팅 기반의 필름형 지문인식 센서 기술을 개발하였다(Kim et al, 2021; 전자신문, 2021). 주요 핵심기술은 다음의 세 가지다. 첫째, 지문센서를 구성하는 포토다이오드의 광 흡수 물질로 비스플루로페닐 아자이드(Bis(Fluorophenyl azide))가 도핑된 유기물을 사용하였다. 실리콘 대신 광흡수계수가 높은 유기물을 도입함으로써 실리콘보다 작은 두께의 광흡수층(light absorption layer) 구현이 가능하며 이로 인한 빛 간섭 억제에 장점을 확보하는 동시에, 비스플루로페닐 아자이드 도핑을 통해 반도체 분자 간의 정전기적 인력을 강화함으로써 포토다이오드의 외부양자효율(EQE, External Quantum

Efficiency, 외부광원 흡수로 인해 얼마나 많은 전자와 정공이 생성되어 광전류를 형성시키는지(이를 나타내는 인자임)를 비약적으로 향상시키고, 반도체 분자 간의 공유결합 가교를 유도함으로써 포토다이오드 안정성을 개선하였다. 둘째, 빛을 위로부터 흡수하는 형태인 상부입광형(빛을 위에서 흡수) 포토다이오드 개발을 위해 투명 저저항 3중층 상부 전극을 개발하였고, 이로써 하부입광형(빛을 아래로부터 흡수) 포토다이오드가 갖는 단점인, 하부 기판의 불투명성으로 인한 수광량 감소 문제를 해결하였다. 셋째, 산업현장에서 쉽게 적용할 수 있는, 양산화가 가능한 제조공정인 산화물 박막 트랜지스터 어레이(oxide thin film transistor array) 공정을 활용하여 지문인식 센서를 제작하였다.

〈그림 12〉와 같이 지문인식 센서는 유기 포토다이오드(OPD, Organic PhotoDiode)와 산화물 박막 트랜지스터 어레이로 구성된다. 하부 광원(back light source)에서 출발한 빛은 지문에 도달한 후 유기 포토다이오드에서 흡수되고 유기 포토다이오드는 흡수한 빛 에너지를 전기에너지로 바꾼다. 산화물 박막 트랜지스터 어레이는 그 전기에너지를 활용하여 지문 이미지를 구현하는데 기여한다.



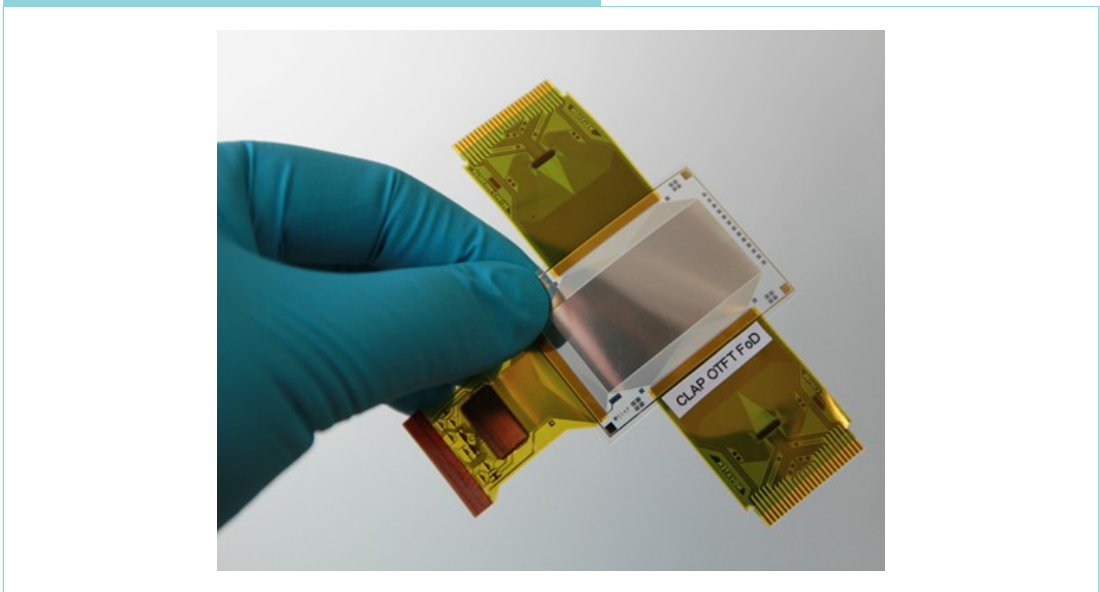
\* 출처: Kim et al.(2021)



## 5.2. 클랩(CLAP)

광학방식 지문인식 센서 개발에 집중하고 있는 클랩은 OLED(Organic Light Emitting Diode, 유기발광다이오드) 광원을 갖는 스마트폰 하단에 장착되는 대면적 필름형 지문인식 센서(크기: 가로 5cm, 세로 2.5cm, 두께 0.1mm 이하)를 개발하였다(〈그림 13〉 참고). 해상도는 500ppi(ppi, pixel per inch)이며 저온 공정으로 제작된 유기물 박막 트랜지스터(OTFT, Organic Thin Film Transistor)를 활용하였으며, 누설 전류(leakage current)를 낮춤으로써 낮은 소비전력을 구현하였다(에이빙, 2022).

그림 13. 클랩이 개발한 광학방식 지문인식 센서



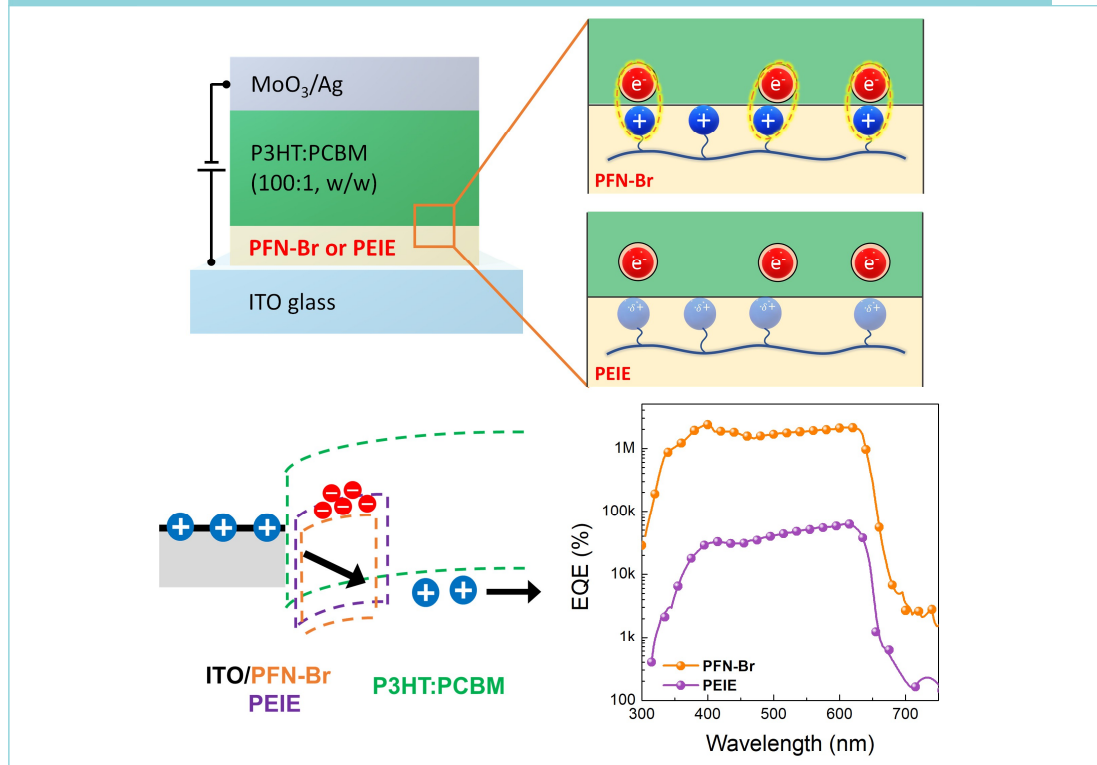
\* 출처: 클랩 제공

## 5.3. 포항공대(POSTECH)

포항공대 정대성 교수 그룹은 유기 포토다이오드 분야에서 가장 활발한 연구를 수행하는 연구그룹 중 하나이다. 연구진은 꾸준히 광전류 증폭을 위한 유기 포토다이오드 소재 및 소자 구조 개선을 통하여 양자효율을 증가시킨 결과를 발표해오고 있다. 2021년에는 광흡수층과 전극 계면에 전기이중층(electric double layer)을 삽입하여 외부양자효율을 1,000,000% 이상으로 향상시킨 바 있으며(〈그림 14〉 참고), 후속 연구로써 광흡수층을 구성하는 유기 반도체 구조를 제어하여 전자주개(electron doner, 전자를 주기 쉬운 원자, 이온 또는 분자)와 전자받개

(electron acceptor, 전자를 받기 쉬운 원자, 이온 또는 분자) 간의 섞임성을 최적화하여 광전류 증폭 상태의 안정성을 비약적으로 향상시킨 바 있다(Lee et al., 2022).

그림 14. 포항공대가 발표한 광전류 증폭형 유기 포토다이오드의 설계 개념도 및 양자효율



\* 출처: Kim et al.(2021)

최근에는 분자 스위치를 이용하여 사용자의 필요에 따라 일반적인 포토다이오드에서 광전류 증폭 포토다이오드로 동작을 스위칭할 수 있는 지능형 포토다이오드를 보고한 바 있다(Kang et al., 2022). 광전류 증폭형 유기 포토다이오드의 지속적인 성능 개선은 향후 유기 포토다이오드의 생체인식 센서로의 응용을 가속화시킬 것으로 보인다.

#### 5.4. 삼성전자

스마트폰의 지문인식 기술 트렌드를 선도하는 기업이다. 2015년 갤럭시 S6에 지문인식 기능을 탑재했으며 모바일 결제 서비스인 삼성페이를 선보였다. 갤럭시 S 모델들은 대부분 스크린에 손가락을 대면 잠금을 해제할 수 있지만, 갤럭시 Z폴드4는 지문인식 센서가 측면 전원 버튼에 탑재되어 전원 버튼에 손가락을 스캔하면 화면 잠금을 풀 수 있다. 삼성전자는 광학방식과 초음파방식 지문인식 센서를 모두 채택하여 스마트폰에 적용하고 있다. 초음파방식은 고가 제품에, 광학방식은 중저가 제품 위주에서 조금씩 고가 제품으로도 확장되고 있다.

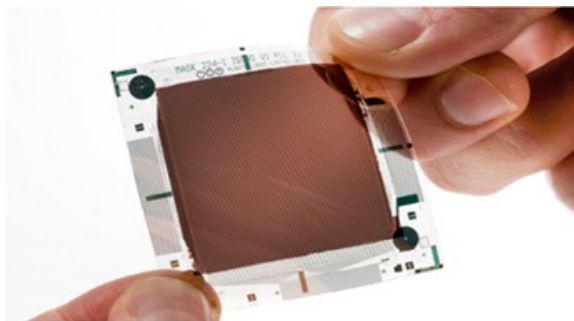
#### 5.5. 애플

스마트폰 기업인 애플(Apple)은 2012년 지문인식 솔루션 업체인 어센텍(AuthenTec)을 인수하였다. 2013년 손가락 하나로 본인 확인이 가능한 지문인식 센서(touch ID)를 탑재한 아이폰 5S를 출시하였고, 아이폰 6에서는 지문인식 센서와 근거리 무선 통신(NFC, Near Field Communication)을 활용한 모바일 결제 시스템인 애플페이(Apple Pay)를 공개하였다. 2017년 아이폰 X에서 지문인식 센서가 사라지고 대신 얼굴인식 기술(face ID)이 등장하고 있다.

#### 5.6. ISORG

프랑스 기업인 ISORG는 대면적 유기 포토다이오드 지문인식 센서 개발의 선두그룹 중 하나이다. 2021년 ISORG의 FAP(Fingerprint Acquisition Profile) 10은 유기 포토다이오드 기반 광학방식 지문센서 중 세계 최초로 미국 연방수사국(FBI, Federal Bureau of Investigation) 인증을 획득하였는데, 이는 최고 수준의 보안이 필요한 공항뿐만 아니라 다양한 보안 응용제품에 사용될 것으로 기대된다(Printed Electronics World 사이트).

그림 15. ISORG가 FlexEnable과 협업하여 개발한 대면적 지문/정맥인식 센서



※ 센서 유효(active) 면적: 가로 8.6cm, 세로 8.6cm

\* 출처: FlexEnable 사이트

## 5.7. 현대자동차

스마트폰을 통해 대중과 친숙해진 생체인식 기술은 자동차 산업에도 적용되고 있다. 자동차 산업에서 생체인식 기술의 적용이 활발히 검토되고 있는 이유는, 첫째, 운전자의 안전 운전을 보조할 수 있는 안전 수단이고, 둘째, 자동차 키 보관의 불편함과 분실 위험성 등을 해소하기 위한 운전자의 편리성 증대 수단으로 인식되기 때문이다. 안전 수단의 예로는, 운전자의 눈과 시선 처리 그리고 얼굴 포즈를 감지하는 운전자 상태 모니터링(driver status monitoring)이 될 수 있는데(Ji et al., 2002), 운전자의 졸음을 감지하게 되면 시트를 진동시키거나 에어컨을 켜서 안전 운전을 유도할 수 있다. 또 다른 예로 운전대에 심장 박동수 측정 센서를 탑재해 운전자의 건강 상태를 측정할 수 있는 시스템 역시 개발되었다.

현대자동차는 제네시스 GV60에 지문인식 기술을 도입하였다(〈그림 16〉 참고). 차량 출입에는 얼굴인식 기술인 페이스 커넥트(face connect)를 적용하고 시동을 거는 것에 정전용량방식의 지문인식 기술을 적용하는 등 2중의 보안성을 확보함으로써, 미등록 운전자가 차량을 운행하는 것은 사실상 불가능하다. 또한 등록된 운전자는 열쇠가 없어도 차량의 출입부터 운행까지 가능하다. GV60에 탑재된 지문인증 시스템은 차량 내에서 카페이 결제 승인 등의 인증 기능을 수행한다.

그림 16. 현대자동차 제네시스에 적용된 지문인식 기술



\* 출처: 현대자동차 사이트

## 5.8. 기아자동차

기아자동차는 뉴 K9 모델에 지문인증 기술을 적용하였다. 핸들 왼쪽 하단에 위치한 지문인식 스크린을 통해 스마트키가 없어도 시동을 걸 수 있다. 또한 사용자가 저장해 놓은 지문을 통해 미리 설정해 둔 좌석 위치, 아웃사이드 미러, 공조, 클러스터 등이 자동으로 실행되는 개인화 프로필을 이용할 수 있으며, 제휴된 주유소나 주차장에서 별도 카드 없이 지문인식을 통해 결제할 수 있다(뉴스1코리아, 2021).

그림 17. 기아자동차 뉴 K9에 적용된 지문인식 기술



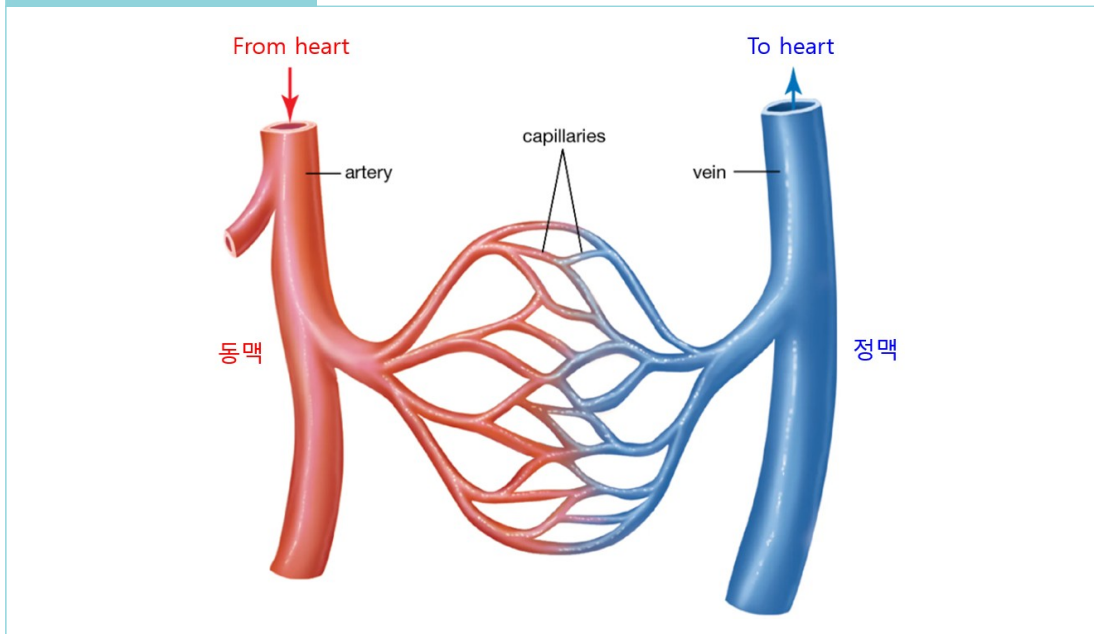
\* 출처: 기아자동차 사이트

### III 정맥인식 센서 기술

#### 1. 정맥 개요

정맥(vein)은 심장으로 들어가는 혈액이 흐르는 혈관으로써, 동맥(artery)과 비교할 때 피부에 더 가까이 분포한다. 동맥보다 정맥에서의 혈압이 낮아서 혈관 벽이 더 얇다. 동맥은 심장에서부터 나가는 혈액이 흐르는 혈관으로 정맥보다 몸속 깊은 곳에 분포한다. 동맥은 심실의 수축 때문에 생기는 높은 혈압을 견뎌야 하므로 정맥보다 혈관 벽이 두껍다.

그림 18. 정맥과 동맥

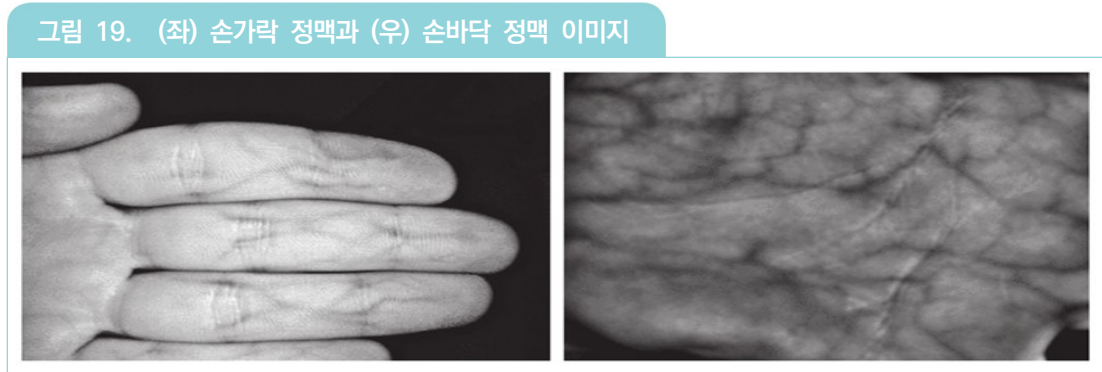


\* 출처: 브리태니커 백과사전



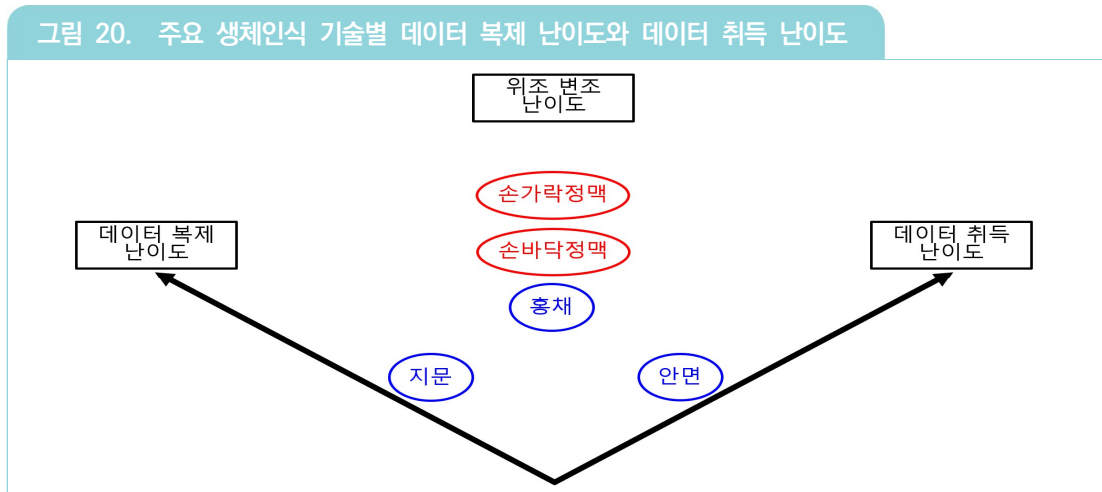
## 2. 손가락 정맥인식과 손바닥 정맥인식

손가락 정맥과 손바닥 정맥이 정맥인식 기술에 주로 사용된다. <그림 19>는 정맥인식 센서를 활용하여 획득한 손가락 정맥과 손바닥 정맥 이미지다.



\* 출처: Sierro et al.(2015)

정맥인식 기술은 지문인식이나 얼굴인식 혹은 홍채인식과 비교하여 데이터 복제 난이도와 데이터 취득 난이도 측면에서 기술적으로 가장 우위에 있기 때문에 복제하거나 다른 사람이 임의로 취득하기에 가장 어려운 것으로 보고되고 있다(<그림 20> 참고). 손가락 정맥인식 기술은 손바닥 정맥인식 기술보다 위조 변조 난이도가 더욱 높다.

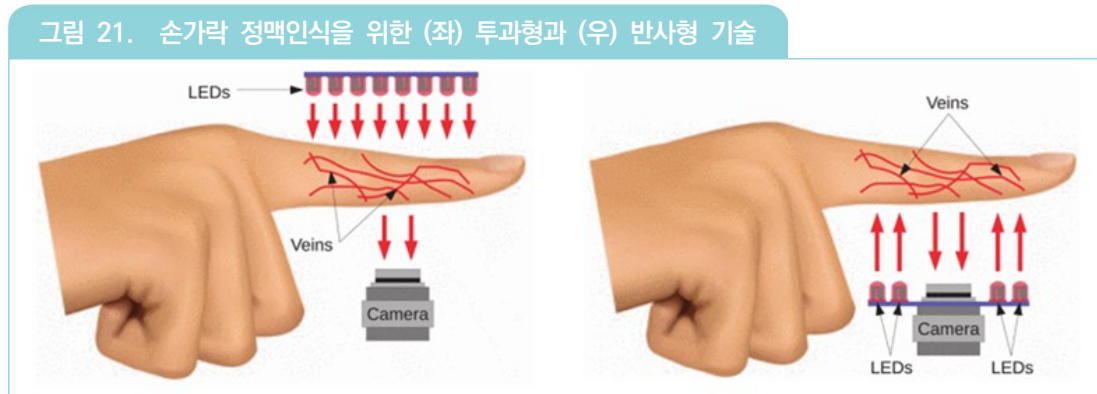


\* 출처: LG히다찌 사이트

### 3. 광학방식 정맥인식 센서 기술

지문인식을 위하여 앞에서 언급한 바와 같이 광학방식, 초음파방식, 정전용량방식의 세 가지 기술이 사용되는 반면, 정맥인식을 위하여 광학방식 기술이 주로 사용된다.

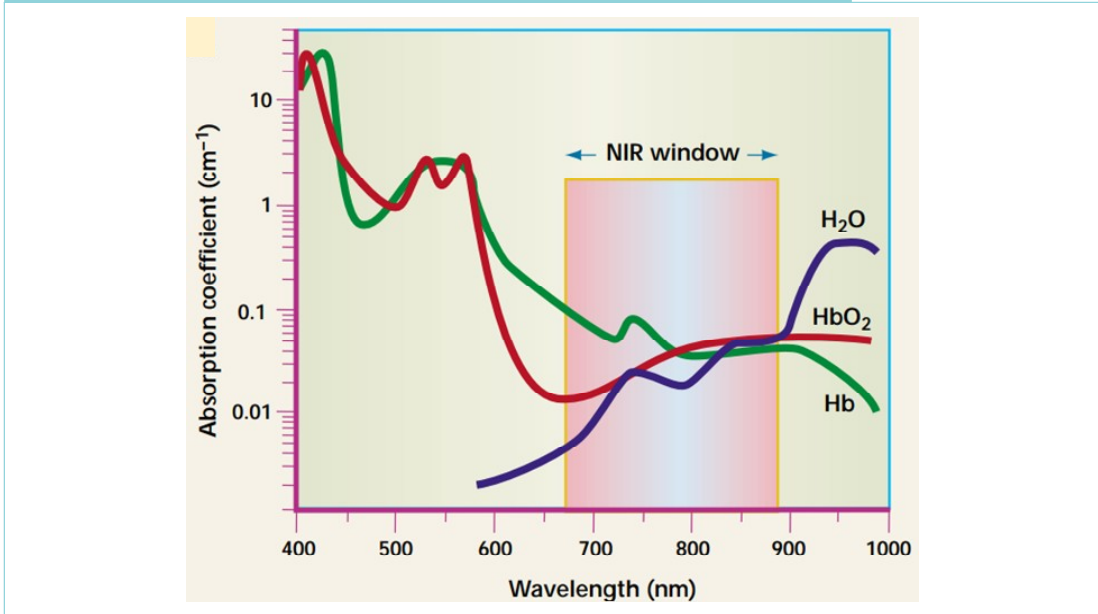
정맥인식 센서는 투과형과 반사형 기술, 두 가지를 사용한다(〈그림 21〉 참고). 투과형의 경우 손가락을 기준으로 한쪽에는 광원, 다른 한쪽에는 카메라가 위치한다. 반사형의 경우 광원과 카메라는 손가락을 기준으로 같은 쪽에 존재한다. 〈그림 21〉은 손가락 정맥인식 과정을 예로 설명한 그림이지만, 손바닥 정맥 역시 동일한 장치와 인식 과정을 거친다.



\* 출처: Sierra et al.(2015)

광원으로는 발광 다이오드(LED, Light Emitting Diode)가 주로 사용되며, 근적외선(NIR, Near Infrared) 파장의 빛을 주로 사용한다. 그 이유는 〈그림 22〉로부터 알 수 있다. 사람 몸속에 존재하는 혈관인 정맥에는 혈액이 흐르는데, 혈액은 혈장(물이 대부분을 차지함), 적혈구, 백혈구와 혈소판으로 구성된다. 물과 헤모글로빈( $H_2O$ , Hb와  $HbO_2$ )에 대한 흡수 실험 결과(〈그림 22〉 참고)에서 확인할 수 있는 바와 같이, 물과 헤모글로빈은 근적외선 영역 파장의 빛에 대한 흡수계수가 가장 작기 때문이다.

그림 22. 빛 파장에 따른 물과 헤모글로빈(H<sub>2</sub>O, Hb와 HbO<sub>2</sub>) 흡수계수



\* 출처: Weissleder(2001)

## 4. 기관별 동향

### 4.1. 한국전자통신연구원

300ppi급 256 by 256 유기 포토다이오드 기반 센서 어레이를 설계하였으며, 산화물 반도체 기반의 백플레인 (back plane)에 유기 포토다이오드를 집적화한 정맥인식 센서 기술을 개발하였다.

### 4.2. 롯데카드

손바닥 정맥으로 결제하는 ‘핸드페이(hand pay)’ 서비스를 세븐일레븐, 오크밸리 등 160여 곳에 설치한 바 있다(EBN 산업경제, 2021).

### 4.3. 히다찌

히다찌는 손가락 정맥인증 시스템을 국내 금융기관 등에 공급하였다. BNK 부산은행과 경남은행은 디지털브랜치(Digital Branch)에 손가락 정맥인증 시스템을 도입함으로써 직원들의 단말 접속뿐 아니라 고객들도 손가락 정맥인증과 지능형 순번 시스템이 결합된 디지털 컨시어지(Concierge)를 이용한 본인 인증을 통해 맞춤형 서비스를 받으며, 신한과 새마을금고도 직원들의 시스템 로그인에 히다찌 시스템을 이용한 바 있다(디지털타임즈, 2020). 일본 내 금융기관 자동입출금기의 80% 이상에 히다찌 손가락 정맥인증 시스템이 도입되어 있다.

그림 23. 손가락 정맥인증 시스템



\* 출처: IT Chosun(2017)

### 4.4. 후지쯔

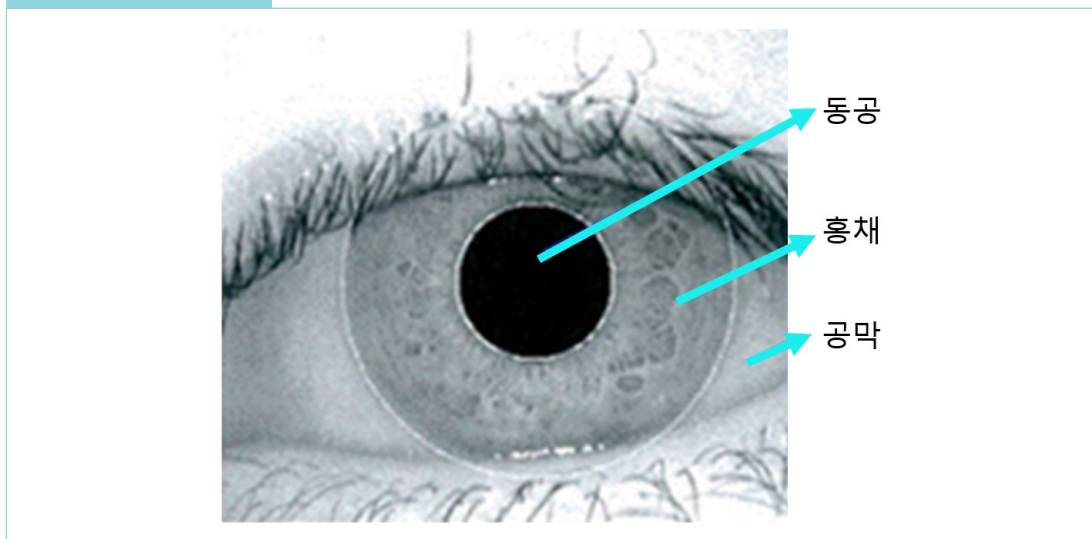
후지쯔는 2019년 전국 14개 공항의 국내선 탑승 절차 서비스에 손바닥 정맥인증 기술을 제공하였다(인사이트코리아, 2019). 탑승 절차 때 육안으로 신분증을 확인하는 절차가 생략되고, 전용 게이트에 손바닥만 대면 곧바로 본인 인증이 되기 때문에 탑승 수속이 간편해졌으며, 신분증을 휴대하지 않더라도 탑승할 수 있어 편리해졌다.

## IV 홍채인식 센서 기술

### 1. 눈 구조와 홍채인식

〈그림 24〉는 눈의 구조를 설명하는 그림이다. 홍채인식을 위해서는 광학방식 센서 기술을 활용한다. 적외선 파장의 광원을 활용하여 홍채 영상을 획득하고, 이로부터 동공, 홍채 경계, 속눈썹, 눈꺼풀 등의 데이터를 확보한다(백영현, 2018). 홍채는 266개의 고유 패턴이 존재하기 때문에 40개 정도의 식별 특징을 갖는 지문보다 훨씬 복잡하고 정교하므로 안정성이 높다(박범근, 2016).

그림 24. 눈 구조



\* 출처: 백영현(2018)

## 2. 기관별 동향

### 2.1. 삼성전자

‘갤럭시 언팩 2016’에서 발표한 갤럭시 노트 7에 스마트폰 최초로 홍채인식 센서가 탑재되어 스마트폰 잠금 해제와 사용자 본인 인증 수단으로 사용되었지만, 2019년 갤럭시 10과 갤럭시 폴드에서는 홍채인식 기술이 제외되었다(산업일보, 2019). 제외된 이유로는, 첫째, 홍채인식을 위해서는 눈을 뜨고 행동을 멈춘 채 화면을 바라봐야 하는데 이때 사용자로 하여금 심리적 불안감을 느끼게 했다는 분석과, 둘째, 최소한의 베젤(bezel, 스마트폰에서 화면이 나오는 부분을 제외한 테두리 영역)만 남겨두는 베젤리스 스마트폰이 새로운 트렌드로 부상함에 따라 홍채인식용 카메라의 공간 확보에 어려움이 생겨 해당 기능을 삭제했다는 분석도 있다(산업일보, 2019).

### 2.2. 유니온커뮤니티

유니온커뮤니티에서는 지문인식, 얼굴인식(최대 1m 거리까지 가능)과 홍채인식(최대 45cm 거리까지 가능)을 통합한 트리플 모달형 바이오 인식시스템을 2022년 출시하였다(전자신문, 2022). 이 시스템은 모바일 출입 카드, 패스워드 및 신용카드 인증 등에 사용할 수 있다.

### 2.3. 아이리시아이디

국내뿐만 아니라 캐나다와 미국, 멕시코, 인도 등 해외 시장에 홍채인식 솔루션을 공급하였다. 인도에서는 10억 명의 홍채를 등록하였으며, 이를 취업, 사회복지, 운전면허, 여권 발급, 은행 계좌 등에 활용하였다(전자신문, 2016).

### 2.4. 아이리텍

아이리텍-블록체인기술연구소 합작사는 2022년 인도와 기술검증 계약을 체결하였다(한국경제티브이, 2022). 이 계약을 통해 홍채인식 기술을 활용하여 인도 국민이 행정과 금융거래 등을 할 때 필요한 가상지갑을 제공한다.

### 2.5. 이리언스

이리언스는 연간 5조 원 규모의 중국 생체인증 시장을 선점하기 위해 중국인 홍채 데이터베이스 구축사업에 착수한다고 2021년 밝혔다(중부일보, 2021). 이리언스는 우리은행을 비롯한 대형 금융기관과 보훈병원 등 의료기관, 에콰도르 등 전 세계 30여 개 국가에서 금융거래, 연금지급, 개인인증, 출입자인증시스템을 공급한 바 있다.

# V 얼굴인식 센서 기술

## 1. 얼굴 특징 정보 추출과 데이터베이스

광원에서 발사된 빛은 얼굴에 도달한 후 이미지 센서로 향하며, 이미지 센서는 그 빛을 흡수하여 영상화한다. 앞의 1장에서 언급한 바와 같이(〈그림 2〉 참고), 영상화된 얼굴 이미지로부터 얼굴 특징 정보를 추출하고 이를 데이터 베이스와 매칭/분류한 후 개인을 식별한다.

얼굴 특징 정보를 추출하는 방법은 다음의 네 가지로 분류되며 이들의 대표적인 특징은 다음과 같다(Yang et al, 2002). 첫째, 지식 기반 탑다운 방법(knowledge-based top-down method, 사람 얼굴에 대한 지식으로부터 얻어진 규칙을 활용), 둘째, 바텀업 특징 기반 방법(bottom-up feature-based method, 지식 기반 탑다운 방법과는 달리 얼굴의 고유한 특징을 찾아서 활용), 셋째, 템플리트 매칭 방법(template matching method, 사전에 미리 설정된 표준화된 얼굴 패턴을 활용), 넷째, 외형 기반 방법(appearance-based method, 얼굴 패턴을 미리 설정하는 템플리트 매칭 방법과 달리 획득한 이미지를 활용하여 얼굴 패턴을 획득).

데이터베이스 종류로는 MIT database, FERET database, UMIST database 등이 있으며, 조명에 의한 밝기 변화, 얼굴 방향과 포즈, 얼굴 찌푸림과 안경 유무, 헤어스타일 변화 등에 영향을 받지 않고 높은 인식률을 갖는 기술개발이 진행되고 있다(Yang et al, 2002).

## 2. 기관별 동향

### 2.1. 한국전자통신연구원

한국전자통신연구원은 인공지능(AI, Artificial Intelligence)을 활용하여 얼굴이 포함된 사진이나 동영상을 입력하면 특정 영상에서 해당 인물이 출연하는 구간을 검색하는 기술인 AI 얼굴인식 기술을 개발하였으며 이를 2022년 독일 국제가전박람회(IFA, Internationale Funkausstellung Berlin)에서 홍보하였다(뉴시스, 2022). 이 기술은 지능형 미디어 정보 검색 서비스, 유해 영상 차단 서비스, 출입자 인증 및 식별 등에 활용될 수 있다.



## 2.2. 삼성전자

갤럭시 S8과 S9, 노트 9와 10등에서 얼굴인식 센서 기술을 적용하였다. 2019년 S10 시리즈에는 얼굴인식과 지문인식 기술을 함께 사용하였다.

## 2.3. 신한카드

신한카드는 2020년 한양대학교 구매 식당에서 국내 최초 얼굴인식 결제 서비스인 '신한 페이스페이(face pay)'의 상용화에 성공하였다(EBN 산업경제, 2021). GS25 편의점과 홈플러스 등의 대형마트에도 도입되어 신용카드나 스마트폰 없이 결제가 진행되고 있다(메가경제, 2021).

## 2.4. 애플

애플은 2017년 아이폰 X 출시부터는 지문인식을 없애고 얼굴인식 센서인 페이스 ID를 적용하고 있으며, 2022년 아이폰 14 맥스와 아이폰 14 프로 등에도 페이스 ID를 장착한다고 발표하였다(뉴시스, 2022).

## 2.5. 알리바바

알리바바에서는 얼굴인식 기술을 활용한 결제 시스템인 알리페이(Alipay)를 개발하였다. 알리페이는 중국 모바일 결제시장에서 점유율 54%를 차지하고 있으며, 롯데면세점은 2019년 알리페이를 도입하였다(스포츠투데이, 2019).

## 2.6. 슈프리마

AI 기반 얼굴인식 솔루션 '페이스스테이션(face station) F2'와 스마트폰으로 출입 인증을 하는 모바일 출입 카드 등 다양한 비접촉 출입 인증 솔루션을 보유하고 있다(아이티데일리, 2022).

## VI 생체인식 기술 시장

### 1. 세계 시장

시장 조사기관마다 연도별 생체인식 기술 시장규모와 연평균 성장률에는 다소 차이가 있지만, 시장규모가 매년 큰 폭으로 성장한다는 것에는 이견이 없다. 마켓스앤마켓스(MarketsandMarkets)에 따르면, 글로벌 생체인식 기술 시장은 2020년 366억 달러에서 연평균 13% 성장하여 2025년 686억 달러에 달할 것으로 전망되는데, 사물인터넷(IoT, Internet of Things) 기술의 발달과 각 정부의 투자 확대 그리고 지능형 자동차 기술개발로 인해 시장이 크게 성장할 것으로 분석된다(김도현, 2021). 한편 프로스트앤설리번(Frost & Sullivan)은 '2024 글로벌 생체인식 시장 분석 보고서'에서 2024년까지 세계 생체인식 기술 시장규모는 연평균 19.6%로 성장하여 459억 달러 수준에 달할 것으로 전망하였다(보안뉴스, 2020).

세계 시장 기준 각 생체인식 기술이 차지하는 점유율은 지문인식(52%), 얼굴인식(23%), 홍채인식(12%), 정맥인식(5%), 음성인식(4%) 및 기타(4%)의 순이다(보안뉴스, 2021). 2021년 대비 2022년 각 생체인식 기술의 시장 성장률은 홍채인식, 정맥인식과 음성인식은 20~22% 수준이고 지문인식과 얼굴인식은 16~18%로 예측된다(보안뉴스, 2021).

### 2. 국내 시장

과학기술정보통신부와 한국정보보호산업협회가 공동으로 발표한 '2022년 국내 정보보호산업 실태조사' 결과, 국내 생체인식 보안시스템 시장은 2022년 4,789억 원으로 전년 대비 46.9% 급성장하였는데, 이는 코로나-19로 인한 근무환경 변화로 비대면 출입 통제 시장이 급성장하였고 새로운 무인 사업 등장 등으로 시장이 확대되었기 때문으로 분석된다(전자신문, 2022).

## VII 생체인식 기술 정책 동향

### 1. 해외

2020년 UN(국제연합) 인권이사회는 평화적 시위 보장을 위해 얼굴인식 기술 사용을 규탄하는 결의안을 채택하고 얼굴인식 기술에 의한 인권 위협을 경고하였다.

유럽연합(EU)은 2021년 얼굴인식을 포함한 AI 기술 전반에 관한 규제 법안을 발표하였는데, 이는 얼굴인식이 편리한 기술이나, 국가가 개인을 감시하는 데 악용될 가능성이 크다는 인식이 확산되었기 때문이다(아주경제, 2022). 법안의 주요 내용은 공공장소에서 얼굴인식 기술 사용을 원칙적으로 금지하고, 행방불명 아동 수색, 테러 위협 방지와 중대한 범죄 피의자 검거 등 극히 예외적인 경우에만 사용을 허용한다는 것이다.

미국의 경우 샌프란시스코 등 일부 도시는 공공장소에서의 얼굴인식 기술 사용을 금지하였고, 캘리포니아 등 일부 주(state) 에서 얼굴인식 기술을 탑재한 경찰의 보디캠 사용을 제한하였으며, 얼굴인식 기술 사용에 대한 지침과 제한에 관한 내용을 담은 연방법 제정을 위한 논의를 진행 중이다(아주경제, 2022).

중국과 러시아는 얼굴인식 기술을 가장 적극적으로 활용하는 국가이다(아주경제, 2022). 특히, 중국 정부는 다중이용시설에서 신원 확인, 범죄 예방, 전자상거래 결제 승인, 도서 대출 모니터링, 위구르족 감시 등 다양한 영역에서 얼굴인식 기술을 활발히 활용하고 있다.

### 2. 한국

개인정보보호위원회는 지문, 얼굴, 정맥, 홍채 등 생체정보의 보호와 안전한 활용을 위한 생체정보 보호 가이드라인을 2022년 개정하였는데, 이를 통해 생체인식 정보를 안전하게 이용할 수 있는 환경 조성에 도움이 될 것으로 기대된다. 가이드라인 적용 대상을 기존 정보통신서비스 제공자 등에서 개인정보처리자, 생체정보 처리기기와 시스템 및 서비스를 개발 혹은 운영하는 제조사로도 확대하였으며, 2021년 개정된 개인정보 보호법 시행령에 따라 민감 정보로 규정된 생체인식 정보의 수집과 이용 시 별도 동의가 필요하다(이데일리, 2021).

## VIII 맺음말

정보의 디지털화가 빠르게 진행됨에 따라 개인인증과 보안을 위한 생체인식 기술에 대한 수요는 더욱 커지고, 빅데이터와 AI 인공지능 기술과 결합되어 새로운 시장이 계속 창출할 것으로 기대된다.

생체인식 센서 기술은 단독으로 사용되지 않고 다른 생체인식 센서 기술과 함께 복합화되어 사용되기도 한다. 예를 들어 지문인식 기술과 정맥인식 기술을 함께 활용하는 손가락 스캐너가 개발되어 보안성을 더욱 극대화하기도 하고, 자동차 분야에서는 지문인식과 얼굴인식 기술이 함께 사용된 차량이 등장하고 있다. 이러한 복합화 경향이 앞으로도 계속 나타날 것으로 예상된다.

생체인식 기술이 시장에 살아남기 위해서는 사용자의 거부감을 해소하고, 생체정보의 위조나 변조 그리고 유출 등에 대한 사용자의 불안감을 해소해야 한다. 또한 거대 기업 등에 의한 생체정보 독점과 임의의 사용을 방지할 수 있는 사회안전망 구축에 대한 노력이 앞으로도 계속 진행되어야 한다.

저자\_ 박영삼(Young-Sam Park)

### • 학력

한국과학기술원 재료공학 박사  
한국과학기술원 재료공학 석사  
한국과학기술원 재료공학 학사

### • 경력

現) 한국전자통신연구원 ICT창의연구소 책임연구원  
前) 삼성전자 반도체총괄 책임연구원

## 참고문헌

### 〈국내문헌〉

- 1) 김도현. (2021). 최근 생체인식 산업 동향과 시사점. S&T GPS 이슈분석 188호, 한국과학기술기획평가원.
- 2) 박범근. (2016). 생체인식 기술 및 시장동향. S&T Market Report, Vol. 39, 연구성과실용화진흥원.

### 〈국외문헌〉

- 3) Bouchrika, I. (2018). Chapter 1: A survey of using biometrics for smart visual surveillance: gait recognition, in book (entitled) Surveillance in Action: Technologies for Civilian, Military and Cyber Surveillance, P. Karampelas, and T. Bourlai (edited by), Springer.
- 4) Ji, Q. & Yang, X. (2002). Real-Time Eye, Gaze, and Face Pose Tracking for Monitoring Driver Vigilance. Real-Time Imaging, Vol. 8, 357.
- 5) Kang, M., Hassan, S. Z., Ko, S. M., Choi, C., Kim, J., Parumala, S. K. R., Kim, Y. H., Jang, Y., H., Yoon, J., Jee, D. W., Chung, D. S. (2022). A Molecular-Switch-Embedded Organic Photodiode for Capturing Images Against Strong Backlight. Advanced Materials, Vol. 34, Issue. 17, 2200526
- 6) Kim, J., Joo, C. W., Hassan, S. Z., Yu, S. H., Kang, M., Pi, J. E., Kang, S. Y., Park, Y. S., Chung, D. S. (2021). Synergetic Contribution of Fluorinated Azide for High EQE and Operational Stability of Top-Illuminated, Semitransparent, Photomultiplication-Type Organic Photodiodes. Materials Horizons, Vol. 8, 3141.
- 7) Kim, J., Kang, M., Lee, S., So, C., Chung, D. S. (2021). Interfacial Electrostatic-Interaction-Enhanced Photomultiplication for Ultrahigh External Quantum Efficiency of Organic Photodiodes, Advanced Materials, Vol. 33, 2104689.
- 8) Lee, S., Lee, G. S., Kang, M., Ha, Y. H., Kim, Y. H., Chung, D. S. (2022). High-Performance and High-Stability All-Polymer Photomultiplication-Type Organic Photodiode Using an NDI-Based Polymer Acceptor with Precisely Controlled Backbone Planarity. Advanced Functional Materials, Vol. 32, Issue. 36, 2204383.
- 9) Nalwa, H. S. (edited by), Photodetectors and Fiber Optics, Academic Press (2001)
- 10) Seo, W., Pi, J. E., Cho, S. H., Kang, S. Y., Ahn, S. D., Hwang, C. S., Jeon, H. S., Kim, J. U., and Lee, M. (2018). Transparent Fingerprint Sensor System for Large Flat Panel Display. Sensors, Vol. 18, 293.
- 11) Sierra, A., Ferrez, P., Roudit, P. (2015). Contact-Less Palm/Finger Vein Biometrics, 2015 International Conference of the Biometrics Special Interest Group(BIOSIG), 145

- 12) Weissleder, R. (2001). A Clearer Vision for In Vivo Imaging. Nature Biotechnology, Vol. 19, 316-317.
- 13) Yang, M. H., Kriegman, D. J., Ahuja, N. (2002). Detecting Faces in Images: A survey. IEEE Transactions on Pattern Analysis Machine Intelligence, Vol. 24 No. 1, 34.


### 〈기타문헌〉

- 14) 강일용. (2022.02.06). 12조원 시장 규모 예상되는 얼굴인식...중국·러시아는 적극적, EU·미국은 규제 나서. 아주경제, <https://www.ajunews.com/view/20220206073356456>.
- 15) 권오철. (2019.10.29). 롯데면세점, 알리페이 안면인식 결제시스템 도입. 스포츠서울, <https://www.sportsseoul.com/news/read/840520>.
- 16) 기아 자동차 사이트, <https://www.kia.com/kr/vehicles/thenewk9/features.html>
- 17) 김남규. (20217.06.07). 신협중앙회, 지정맥인증 기반 업무통제 시스템 구축. IT Chosun, [https://it.chosun.com/site/data/html\\_dir/2017/06/07/2017060785037.html](https://it.chosun.com/site/data/html_dir/2017/06/07/2017060785037.html)
- 18) 김도현. (2019.10.25). '정전식→광학식→초음파' 지문인식 센서, 방식별 장단점은?. 디지털데일리, <https://www.ddaily.co.kr/news/article/?no=187377>
- 19) 김도현. (2020.03.11). 지문인식 '광학식' 대세 된다 ... 쿨컴 '초음파'는 아직. 디지털데일리, <https://www.ddaily.co.kr/news/article/?no=192862>
- 20) 김명철. (2021.12.14). 흥채기업 '이리언스', 중국 5조 생체인증시장 공략 본격화. 중부일보, <https://www.joongboo.com/news/articleView.html?idxno=363516734>
- 21) 김양수. (2022.09.01). ETRI, 독일 국제가전박람회(IFA)서 AI얼굴인식 등 핵심기술 공개. 뉴시스, [https://newsis.com/view/?id=NISX20220901\\_0001998975&cID=10807&pID=10800](https://newsis.com/view/?id=NISX20220901_0001998975&cID=10807&pID=10800).
- 22) 김영준. (2021.11.30). ETRI 등, 고성능 지문인식 센서 개발...빠른 상용화 기대. 전자신문, <https://www.etnews.com/20211130000098>
- 23) 김인순. (2016.05.04). 아이리시아이디, 인도 국가 주민증 사업 10억명 흥채 등록. 전자신문, <https://www.etnews.com/20160504000035>
- 24) 네이버 사전, <https://dict.naver.com/>
- 25) 백영현. (2018.07). 생체인식 기술연구 및 기술동향, 생체인식 최신기술 분석 및 시장 확대 방안. 한국미래기술 교육연구원(KECFT) 세미나 교재.
- 26) 박승원. (2022.08.01). 아이리텍-블록체인기술연구소 합작사, 인도 국민 대상 기술검증 돌입. 한국경제티브이, <https://www.wowtv.co.kr/NewsCenter/News/Read?articleId=A202208010227&t=NN>
- 27) 신진주. (2021.06.18). 휴대폰 밖으로 나온 신용카드 '생체인식'. EBN 산업경제, <https://www.ebn.co.kr/news/view/1488251/?sc=Naver>
- 28) 설명환. (2019.02.28). 스마트폰 풀기능, 지문인식 기술의 종류와 원리가 궁금하다면?. 삼성디스플레이 뉴스룸, <https://news.samsungdisplay.com/18221>

- 29) 안경애. (2020.12.16). LG히다찌, 지문·홍채보다 보안성 뛰어나... 위변조 불가. 디지털타임스, [http://www.dt.co.kr/contents.html?article\\_no=2020121702101731650001](http://www.dt.co.kr/contents.html?article_no=2020121702101731650001)
- 30) 안수민. (2022.05.04). 유니온커뮤니티, 지문·얼굴·홍채 3가지 바이오인증 통합단말 '유바이오 엑스트리플' 출시. 전자신문, <https://www.etnews.com/20220504000040>
- 31) 엄호식. (2020.12.01). 출입통제·생체인식 시장, 2020년 핫 키워드. 보안뉴스, <https://www.boannews.com/media/view.asp?id=92989&kind=>
- 32) 엄호식. (2021.08.14). 러시아 생체인식시장, 30% 성장세... 주목하는 방식은?, 보안뉴스, <https://www.boannews.com/media/view.asp?id=99787&kind=>
- 33) 오현주. (2022.08.25). 애플, 9월 8일 '아이폰 14' 공개... "1주일 앞당겨 신제품 발표". 뉴시스, <https://www.news1.kr/articles/4782889>
- 34) 이균진. (2021.06.02). 기아 '더 뉴 K9' 내일부터 사전계약... "모든 역량 집약해 개발". 뉴스1코리아, <https://www.news1.kr/articles/?4325692>
- 35) 이후섭. (2021.09.08). 개인정보위, 지문·얼굴 등 '생체정보 안전한 활용' 지침서. 이데일리, <https://www.edaily.co.kr/news/read?newsId=02692886629178152&mediaCodeNo=257&OutLnkChk=Y>
- 36) 정대성. (2017). Thin Film Color-Selective Photodiodes for High Resolution Image Sensor Applications. 한국전자통신연구원 기술세미나 발표자료.
- 37) 정종길. (2022.09.01). 슈프리마, 4년 연속 '코스닥 라이징스타' 선정. 아이티데일리, <https://www.itdaily.kr/news/articleView.html?idxno=209903>
- 38) 최수린. (2019.05.17). 스마트폰 홍채 인식 기술 '주춤' ... "심리적 불안감 큰 탓". 산업일보, <https://www.kidd.co.kr/news/208919>
- 39) 최예원. (2022.08.30). 클랩, K-Display 2022서 유기물 반도체 박막기판 & 국산 OLED 디스플레이 위상차 필름 알린다. 에이빙, <https://kr.aving.net/news/articleView.html?idxno=1770410>
- 40) 최호. (2022.09.13). 정보보호산업 매출 13.4% ↑ · 수출 8.5% ↑, 전자신문, <https://www.etnews.com/20220913000154>
- 41) 한민철. (2019.03.29). 한국후지쯔, 세계 최초 손바닥 정맥 기술 국내 공항 국내선 도입. 인사이트코리아, <https://www.insightkorea.co.kr//news/articleView.html?idxno=35201>
- 42) 황동현. (2021.12.02). 신한카드XGS리테일, 안면인식 결제 '신한 페이스페이' 선보여. 메가경제, <https://www.megaeconomy.co.kr/news/newsview.php?ncode=1065572333950263>
- 43) AZoSensors. (2014.02.03). CMOS Image Sensors in Biometrics. <https://www.azosensors.com/article.aspx?ArticleID=448>.
- 44) HMG 저널 운영팀. (2021.10.15). 운전자와의 교감을 완성하다, GV60의 생체 인식 시스템. 현대자동차 사이트, <https://www.hyundai.co.kr/story/CONT0000000000002541>
- 45) Encyclopedia Britannica, <https://www.britannica.com/>



- 46) FlexEnable 사이트, <https://www.flexenable.com/newsroom/press-release-flexenable-and-isorg-reveal-first-large-area-fingerprint-and-vein-sensor-on-plastic/>
- 47) LG히다찌 사이트. (2016.03). 지정맥 인증 솔루션 소개(Finger vein identification security solutions), <https://www.hitachi.co.kr/products/biometrics/vein/index.html>
- 48) Panasonic Holdings Corporation. (2016.02.03). Panasonic Develops Industry-First\*1 123dB Simultaneous-Capture Wide-Dynamic-Range Technology using Organic-Photoconductive-Film CMOS Image Sensor. <https://news.panasonic.com/global/press/en160203-5>
- 49) Printed Electronics World 사이트, <https://www.printedelectronicsworld.com/articles/23293/fbi-certification-for-first-organic-photodiode-fingerprint-scanner>



융합연구리뷰

Convergence Research Review 2022 November vol.8 no.11



# 03

## 국가R&D 현황 분석

융합연구리뷰 11월호에서 다룬 2개의 주제(차세대 사이버 보안 기술 및 보안을 위한 생체인식 센서 기술)에 대한 각각의 국가R&D 현황을 살펴보기 위해 국가연구개발 과제 분석을 수행하였다. 연구비를 기준으로 연구비 규모별 과제수, 연구수행주체, 연구수준, 연구분야(국가과학기술표준분류, 미래유망신기술분류) 등 여러 측면에서의 분석 결과를 제시한다.

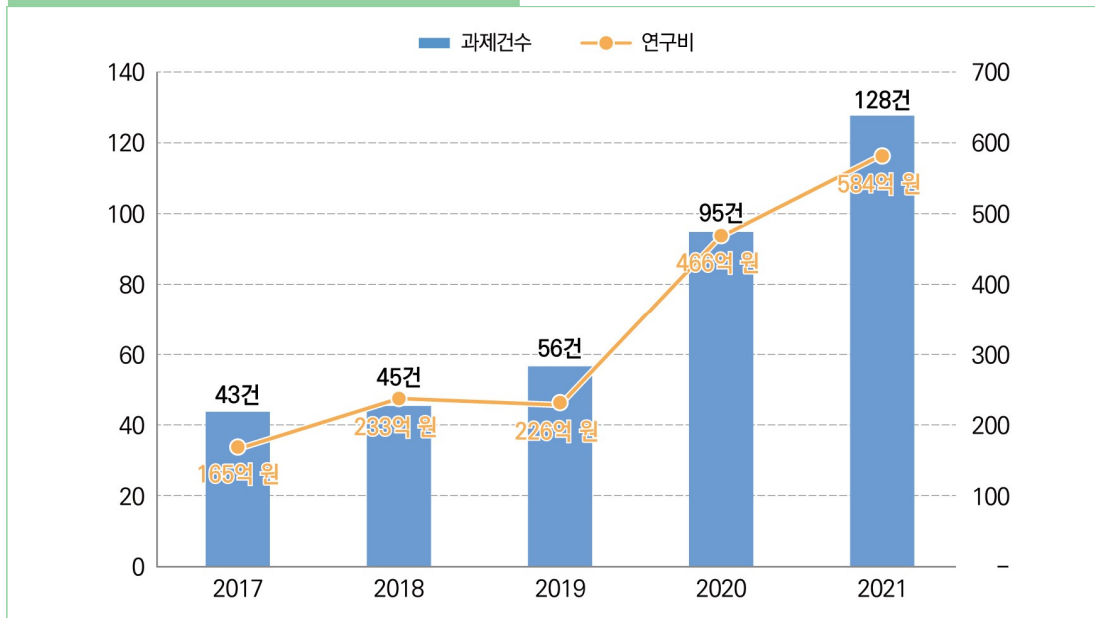
## I 차세대 사이버 보안 기술

□ (총괄) 최근 5년간('17~'21) 총 367건의 과제에 대해 1,674억 원의 연구비가 투자됨

※ 국가과학기술지식정보서비스(NTIS) 플랫폼을 기반으로 관련 국가 연구개발 과제 분석 수행 : 원고의 핵심 키워드를 고려하여 검색 실시

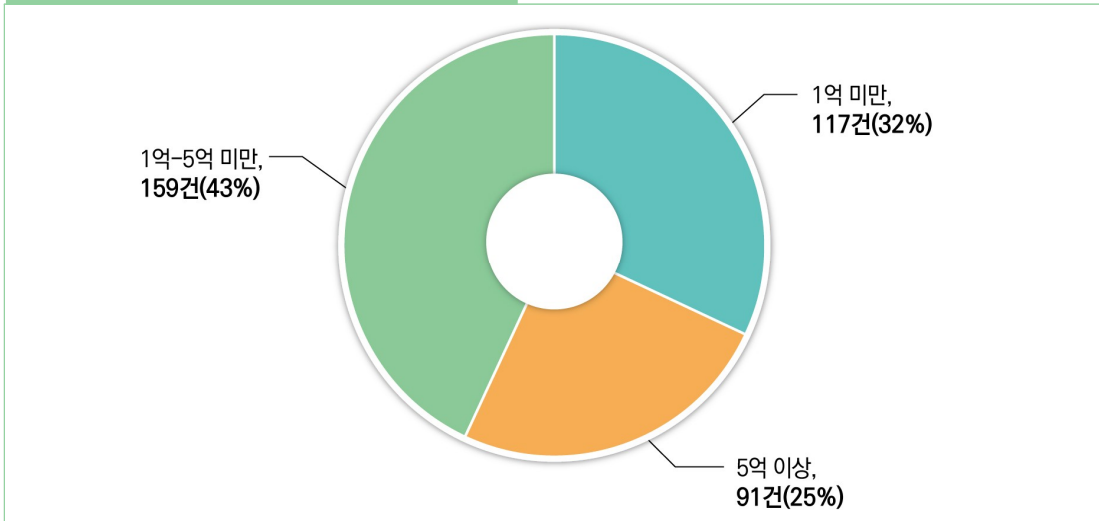
\* (사이버 보안) and (암호 or 데이터 or 시스템 or 디바이스 or 네트워크 or 모바일 or 융합산업)

그림 1. 연도별 연구과제 건수 및 연구비



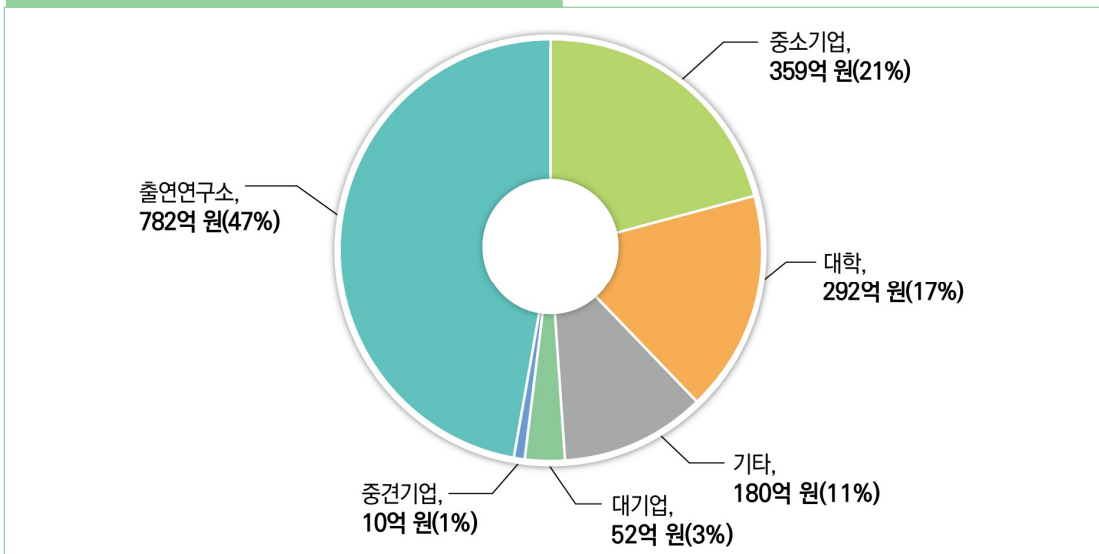
□ (연구비 규모별 과제 수) 연구비가 1억 원 이상 5억 원 미만인 과제(43%, 159건), 1억 원 미만인 과제(32%, 117건), 5억 원 이상인 과제(25%, 91건) 순으로 연구비 비중이 큰 것으로 나타남

그림 2. 연구비 규모별 과제 수 및 비율



□ (연구수행주체) 연구수행주체 별 지원받는 연구비 비중은 출연연구소(47%, 782억 원)가 가장 크고, 중소기업이 21%(359억 원) 그 다음으로 큰 것으로 드러남

그림 3. 연구수행주체별 연구비 규모 및 비율



□ (연구수준) 차세대 사이버 보안 기술은 개발연구 단계에 있으며 기술수명주기는 도입기 단계인 것으로 확인됨

- (연구개발단계 분석 결과) 개발연구에 투자되는 연구비 비중이 55%(832억 원)로 차세대 사이버 보안 기술 관련 전체 연구비의 절반 이상을 차지하는 것으로 드러났으며, 응용연구에 투자되는 비중은 25%(373억 원), 기초연구에 투자되는 비중은 20%(302억 원)로 나타남
- (연구개발성격 분석 결과) 제품 또는 공정개발 관련 연구에 투자되는 연구비의 비중이 50%(358억 원)로 가장 크고 아이디어개발의 연구비 비중과 시작품개발의 연구비 비중은 각각 25%(181억 원), 24%(173억 원)로 거의 유사한 것으로 확인됨
- (기술수명주기 분석 결과) 도입기에 투자되는 연구비 비중은 56%(585억 원), 성장기에 투자되는 연구비 비중은 42%(433억 원)인 반면, 성숙기에 투자되는 연구비 비중은 2%(18억 원)에 불과한 것으로 드러남

그림 4. 연구개발단계별 연구비 규모 및 비율

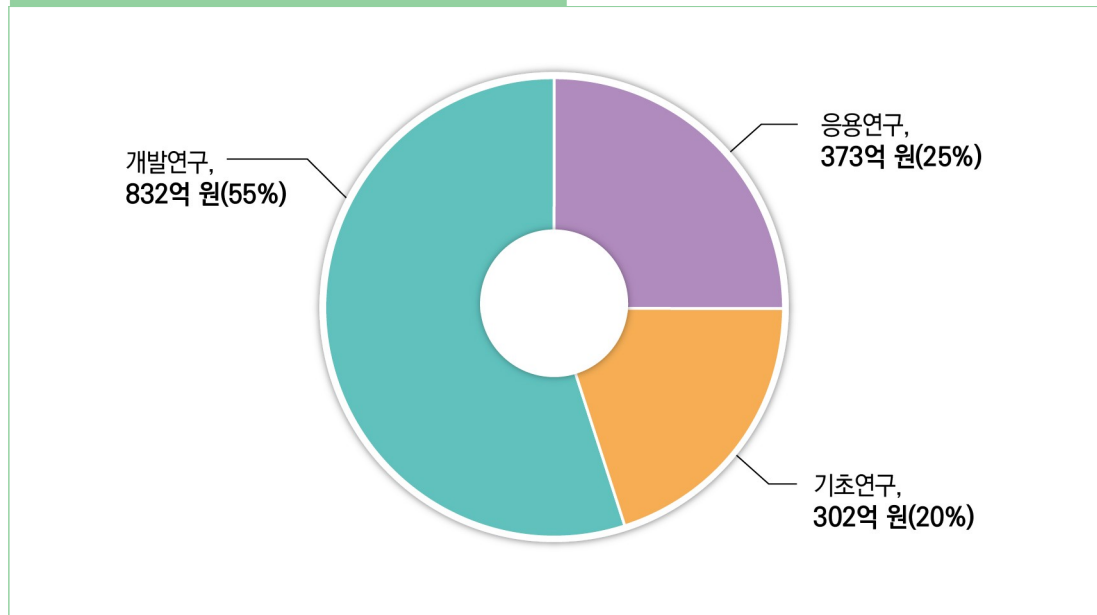


그림 5. 연구개발성격별 연구비 규모 및 비율

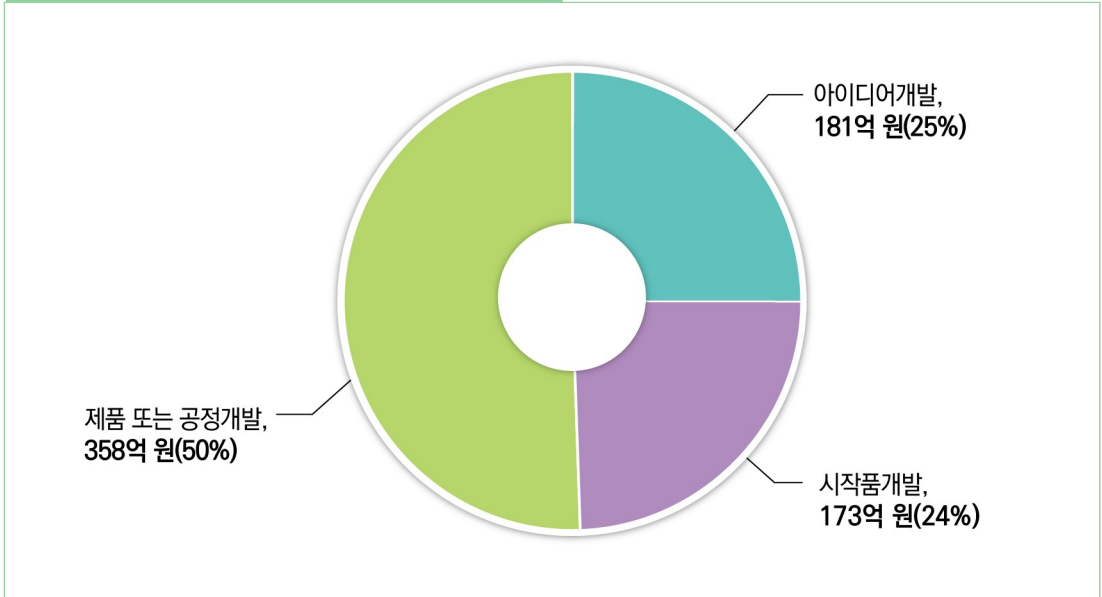
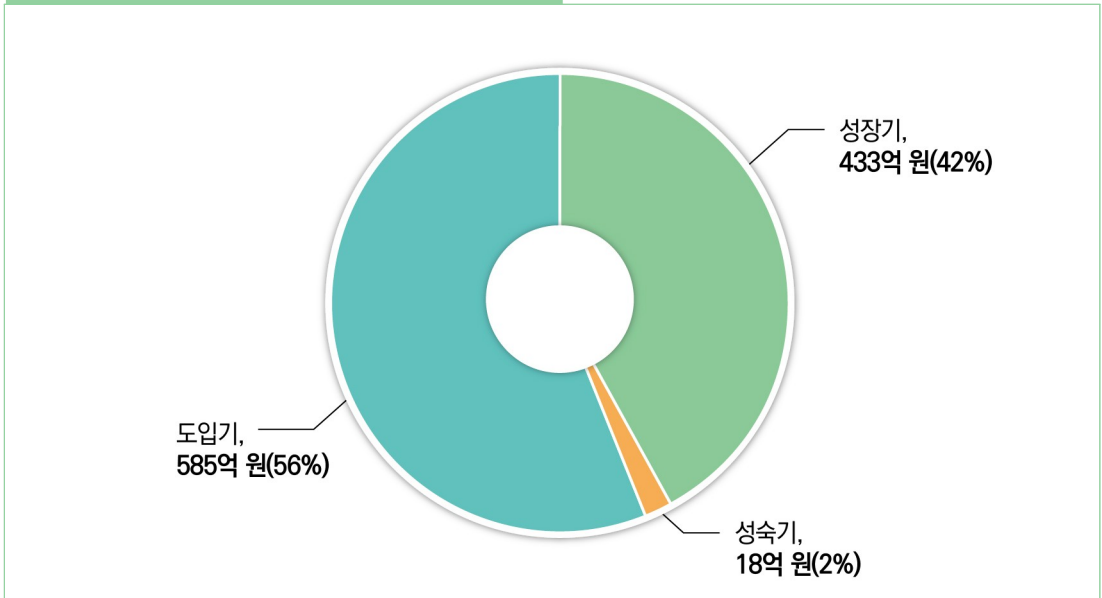


그림 6. 기술수명주기별 연구비 규모 및 비율





□ (연구분야) 국가과학기술표준분류와 미래유망신기술분류(6T) 분석 결과, 정보통신기술(IT) 분야를 중심으로 차세대 사이버 보안 기술 연구가 이루어짐

- (국가과학기술표준분류 분석 결과) 정보/통신 분야에 대한 연구비 비중(57%, 958억 원)이 가장 큰 것으로 확인됨
  - ※ 연구책임자가 최대 3개까지 지정한 국가과학기술표준분류의 대분류에 대한 각 가중치를 고려한 결과임
  - 융합과제에 지원된 연구비 비중은 차세대 사이버 보안 기술 연구에 투자된 전체 연구비의 15%를 차지하며 약 237억 원이 지원됨
  - ※ 융합과제란 연구책임자가 지정한 국가과학기술표준분류의 대분류가 두 개 이상의 분류에 해당하는 과제를 의미함
- (미래유망신기술분류(6T) 결과) IT 관련 연구에 대한 연구비 비중이 68%(1,134억 원)로 가장 큰 것으로 드러남

그림 7. 국가과학기술표준분류별 연구비 규모 및 비율

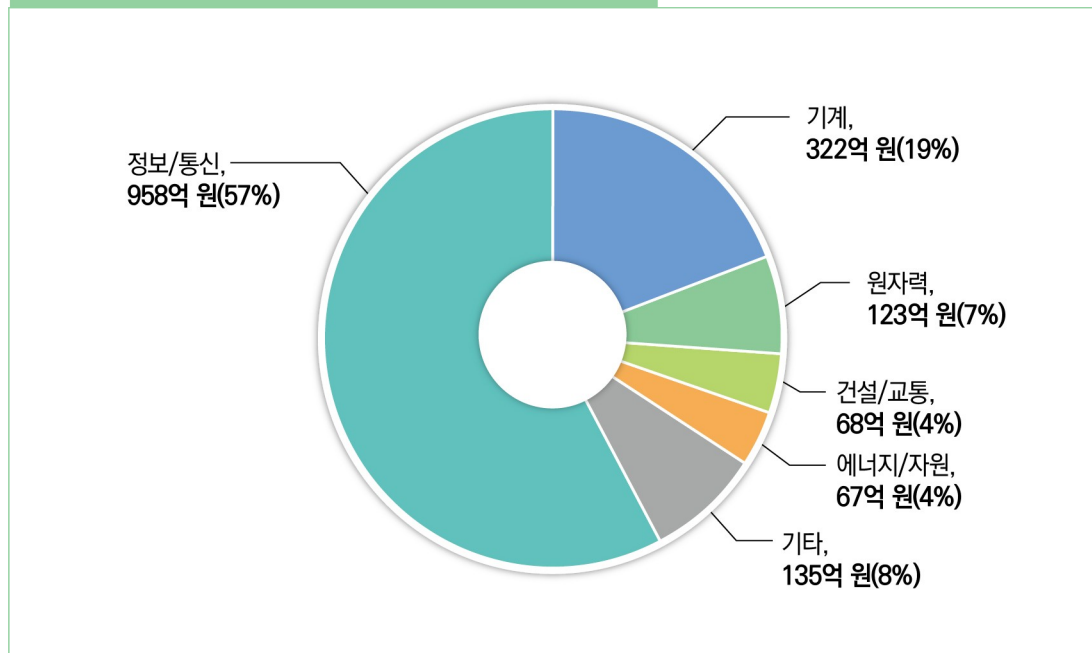


그림 8. 융합 R&D 과제 연구비 규모 및 비율

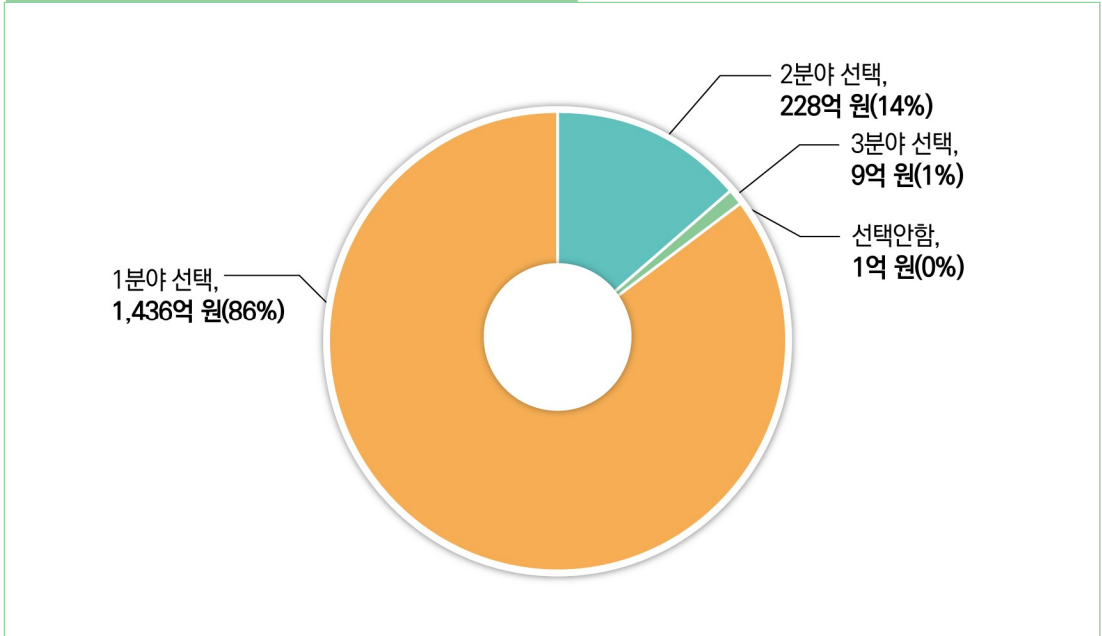
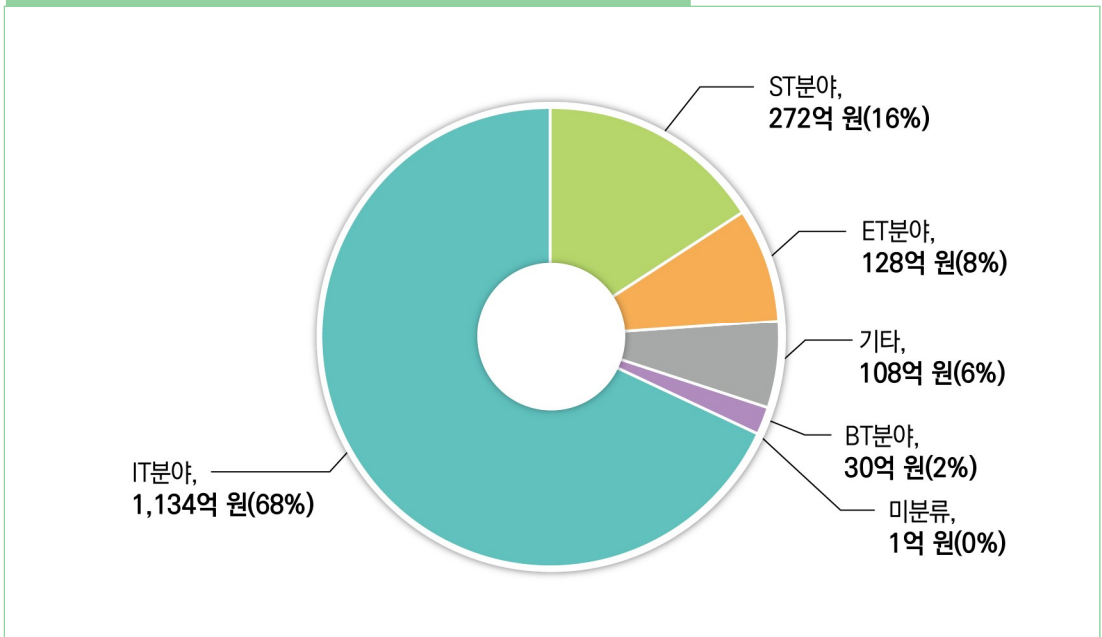


그림 9. 미래유망 신기술분류(6T)별 연구비 규모 및 비율



□ (주요 과제) 원고의 주요 내용 및 키워드 등을 기준으로 선정함

과제명 (사업명, 부처명)	수행기관, 총 연구기간, 연구비 규모	과제 주요 내용
자율주행차량의 차세대 내부 네트워크의 보안 및 초고속 무결성 부여 기술 개발 (자율주행기술개발혁신사업, 과학기술정보통신부)	한국전자기술연구원, 2021-2024년, 14억 원('21)	차량 내부 네트워크 침입공격에 대응하고, 내부 이종 네트워크의 지연 최소화를 위한 초고속 연동, 데이터 무결성 및 실시간 V2X 연동을 위한 보안 통신 핵심 기술 개발
(KGSS) 네트워크 경로, 서버 은닉기술을 활용한 보이지 않는 스텔스 차세대 네트워크 보안 통합솔루션 프로젝트 (정보보호핵심원천기술개발, 과학기술정보통신부)	주식회사 스텔스솔루션, 2019-2020년, 2억 원('20)	네트워크 주소를 동적으로 변경하는 기술과 네트워크의 주요 경로를 보이지 않게 하는 기술을 적용하여, 주요 서버를 보호하고 보안이 강화된 폐쇄 업무망들을 구축해주는 '스텔스 네트워크' 솔루션 개발
차세대 보안 모니터링을 위한 자가 조절형 스트리밍 알고리즘 (개인기초연구, 과학기술정보통신부)	국민대학교, 2016-2019년, 0.3억 원('19)	어떠한 IT환경에 설치되더라도 보안 전문가의 별도 개입 없이 플러그앤플레이 형태로 보안 모니터링을 가능하게 하는 신개념의 자가 조절형 스트리밍 알고리즘 핵심기술 연구 및 소프트웨어 개발

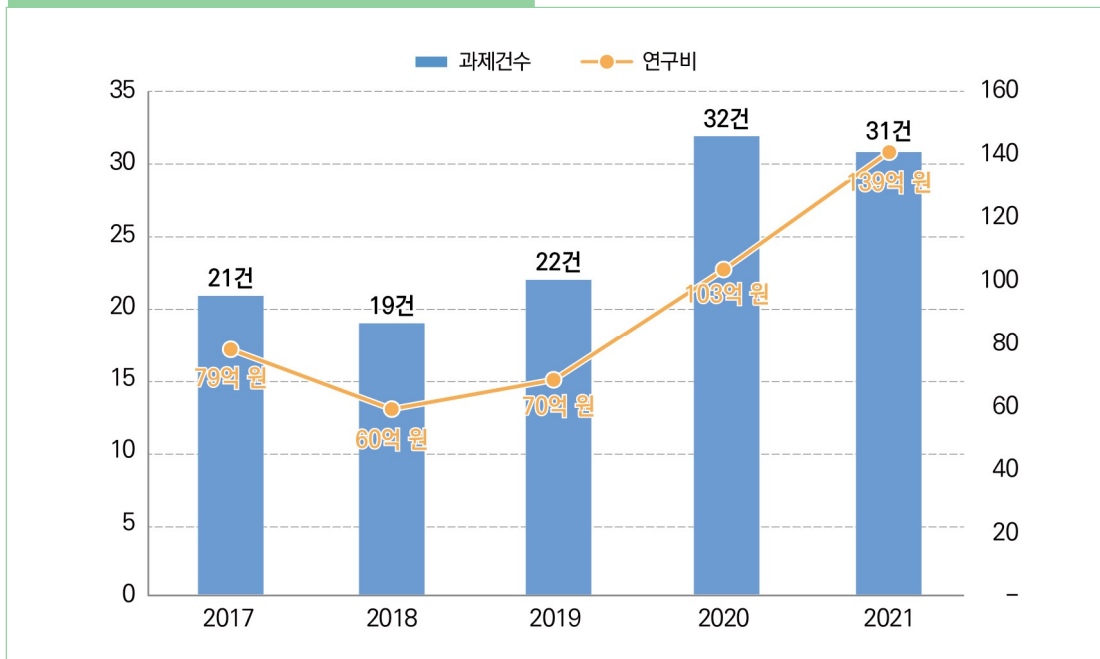
## II 보안을 위한 생체인식 센서 기술

□ (총괄) 최근 5년간('17~'21) 총 125건의 과제에 대해 450억 원의 연구비가 투자됨

※ 국가과학기술지식정보서비스(NTIS) 플랫폼을 기반으로 관련 국가 연구개발 과제 분석 수행 : 원고의 핵심 키워드를 고려하여 검색 실시

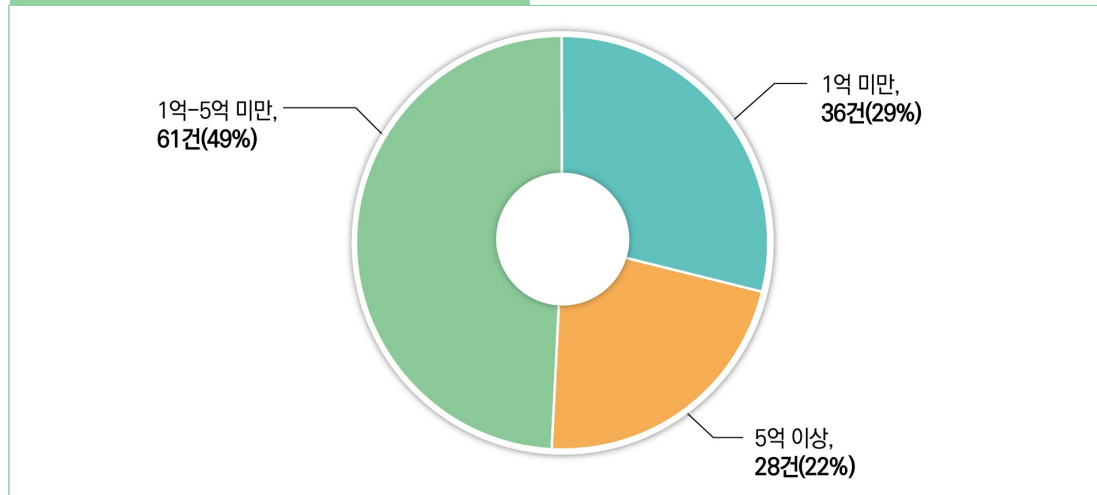
\* (지문 or 정맥 or 홍채 or 얼굴 or 생체) and 인식 and (인증 or 보안) and 센서

그림 10. 연도별 연구과제 건수 및 연구비



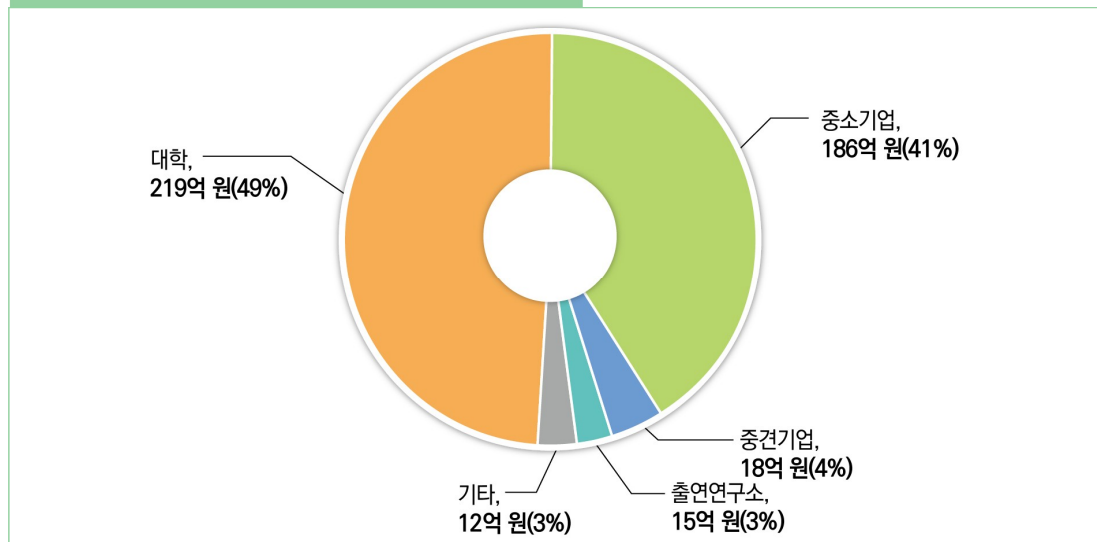
□ (연구비 규모별 과제 수) 1억 원 이상 5억 원 미만인 과제 연구비가 보안을 위한 생체인식 센서 기술 관련 전체 연구비의 거의 절반(49%, 61건)의 비중을 차지하고, 1억 원 미만의 과제 연구비는 29%(36건), 5억 원 이상인 과제인 연구비는 22%(28건)의 비중을 차지하는 것으로 확인됨

그림 11. 연구비 규모별 과제 수 및 비율



□ (연구수행주체) 대학(49%, 219억 원), 중소기업(41%, 186억 원), 중견기업(4%, 18억 원) 순으로 지원받는 연구비의 비중이 큰 것으로 드러남

그림 12. 연구수행주체별 연구비 규모 및 비율



- **(연구수준)** 연구수준을 분석한 결과, 보안을 위한 생체인식 센서 기술 관련 연구는 성장기이며 개발연구 단계인 것으로 나타남
- **(연구개발단계 분석 결과)** 개발연구에 대한 연구비는 보안을 위한 생체인식 센서 기술 관련 전체 연구비의 62%(269억 원)의 비중을 차지하고, 응용연구와 기초연구의 연구비 비중은 각각 19%(84억 원), 18%(78억 원)로 거의 유사한 것으로 확인됨
  - **(연구개발성격 분석 결과)** 제품 또는 공정개발 관련 연구의 연구비 비중(65%, 133억 원)이 월등히 큰 것으로 확인되었으며, 그 다음으로 시작품개발 관련 연구(21%, 42억 원), 아이디어개발 관련 연구(15%, 31억 원) 순으로 연구비 비중이 큰 것으로 드러남
  - **(기술수명주기 분석 결과)** 성장기에 대한 연구비 비중(49%, 144억 원)과 도입기에 대한 연구비 비중(48%, 142억 원)이 유사한 것으로 확인됨

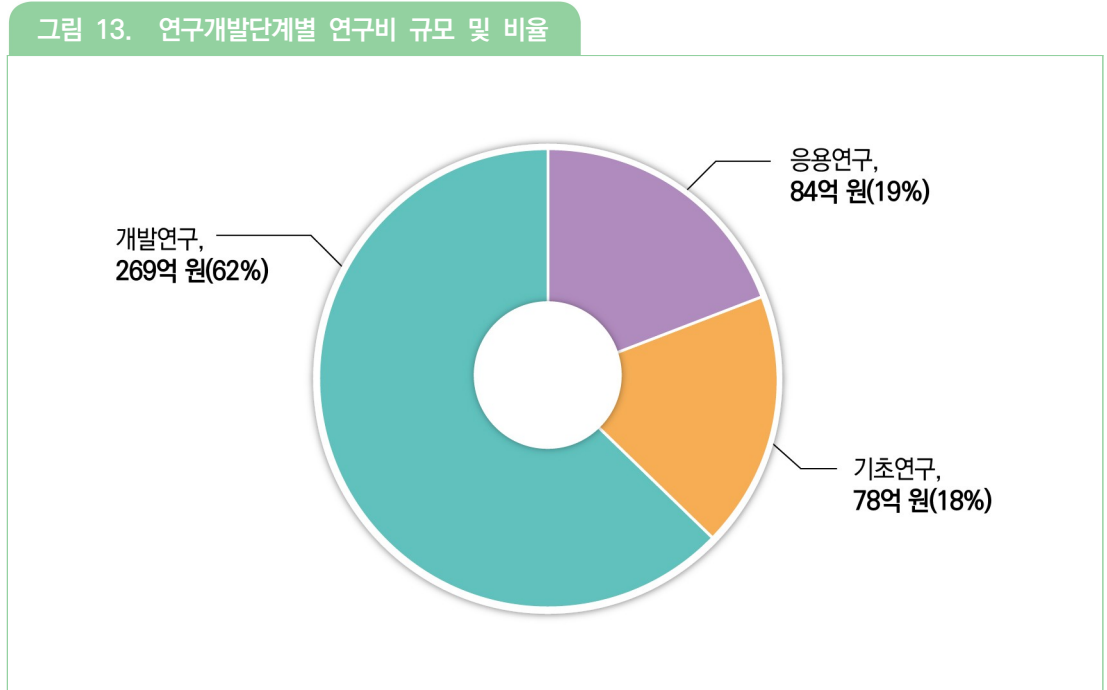


그림 14. 연구개발성격별 연구비 규모 및 비율

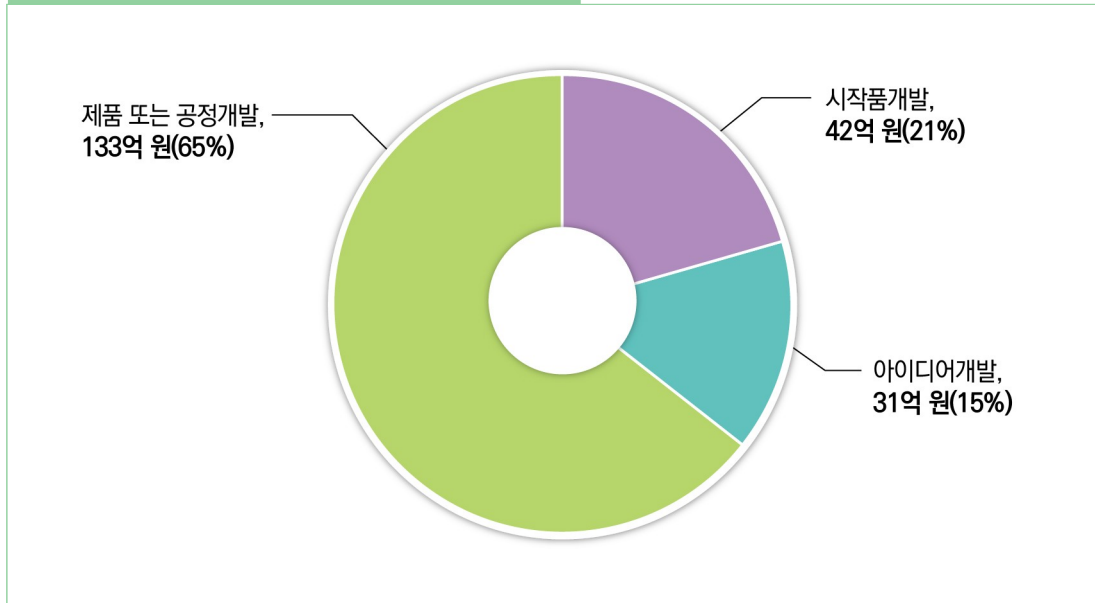
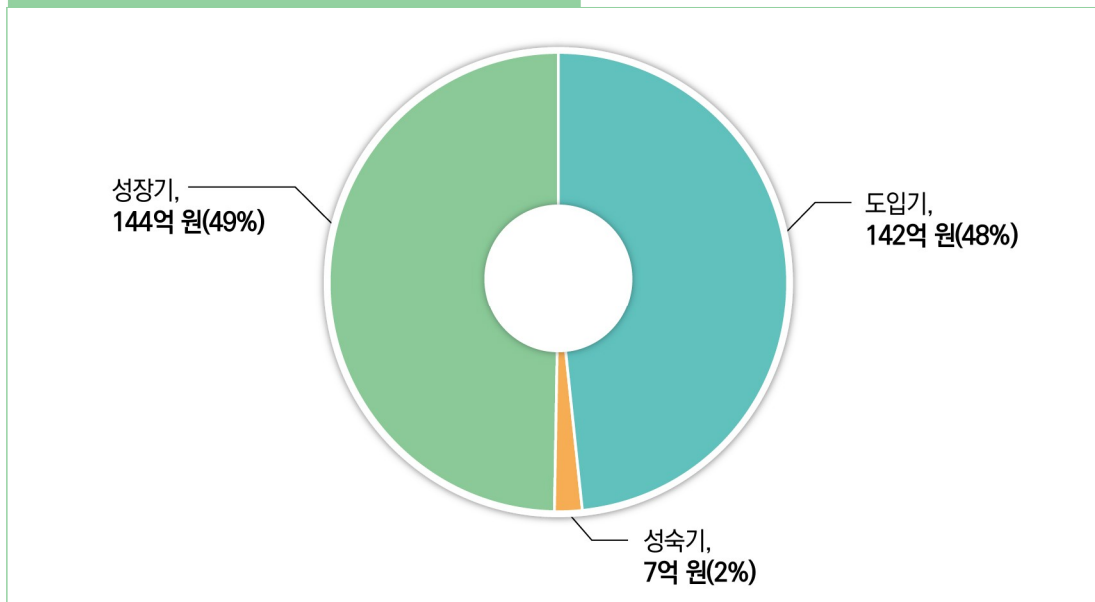


그림 15. 기술수명주기별 연구비 규모 및 비율





- **(연구분야)** 국가과학기술표준분류와 미래유망신기술분류(6T) 분석 결과, 보안을 위한 생체인식 센서 기술에 대한 연구비 투자는 정보/통신 기술(IT) 및 전기/전자 분야를 위주로 이루어짐
- **(국가과학기술표준분류 분석 결과)** 국가과학기술표준분류 중 전기/전자 분야에 대한 연구비 비중이 36%(160억 원)로 가장 높고 정보/통신(35%, 160억 원) 분야가 그 다음으로 큰 것으로 드러남
    - ※ 연구책임자가 최대 3개까지 지정한 국가과학기술표준분류의 대분류에 대한 각 가중치를 고려한 결과임
  - 보안을 위한 생체인식 센서 기술과 관련하여 융합과제에 지원된 연구비 비중은 16%(69억 원)인 것으로 나타남
    - ※ 융합과제란 연구책임자가 지정한 국가과학기술표준분류의 대분류가 두 개 이상의 분류에 해당하는 과제를 의미함
  - **(미래유망신기술분류(6T) 결과)** 정보통신 기술(IT) 관련 연구에 대한 투자 비중이 86%(389억 원)로 보안을 위한 생체인식 센서 기술 전체 연구비 중 가장 큰 비중을 차지함

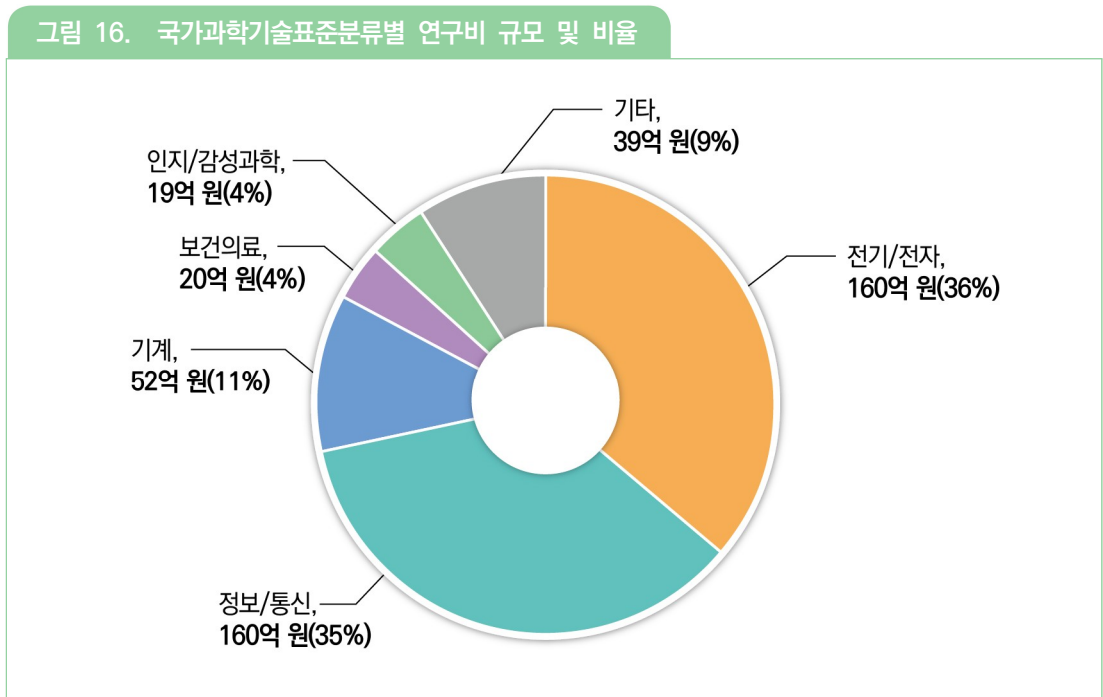


그림 17. 융합 R&D 과제 연구비 규모 및 비율

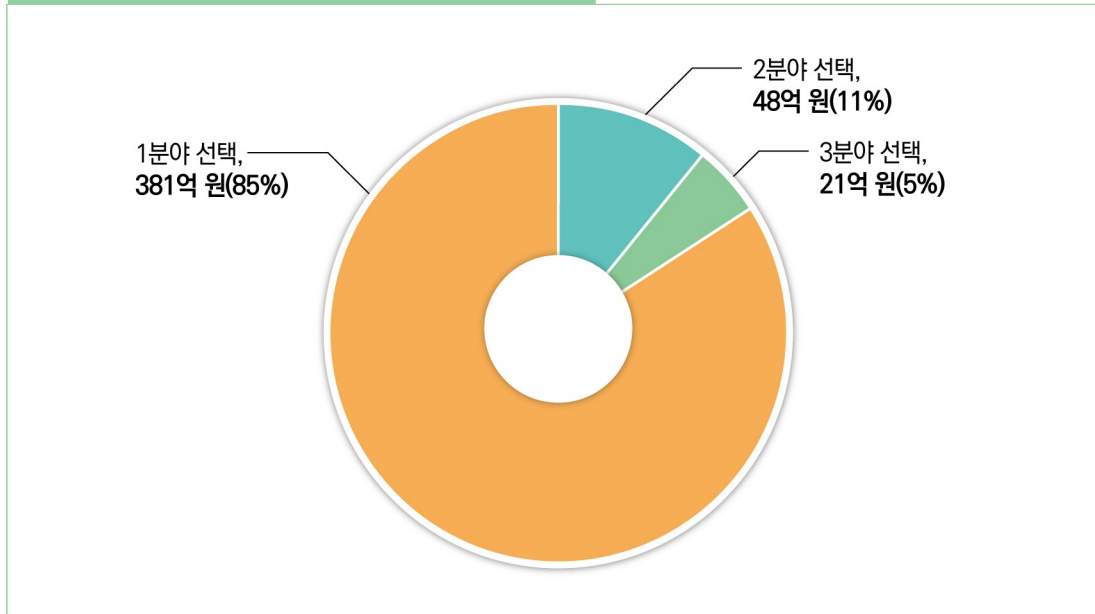
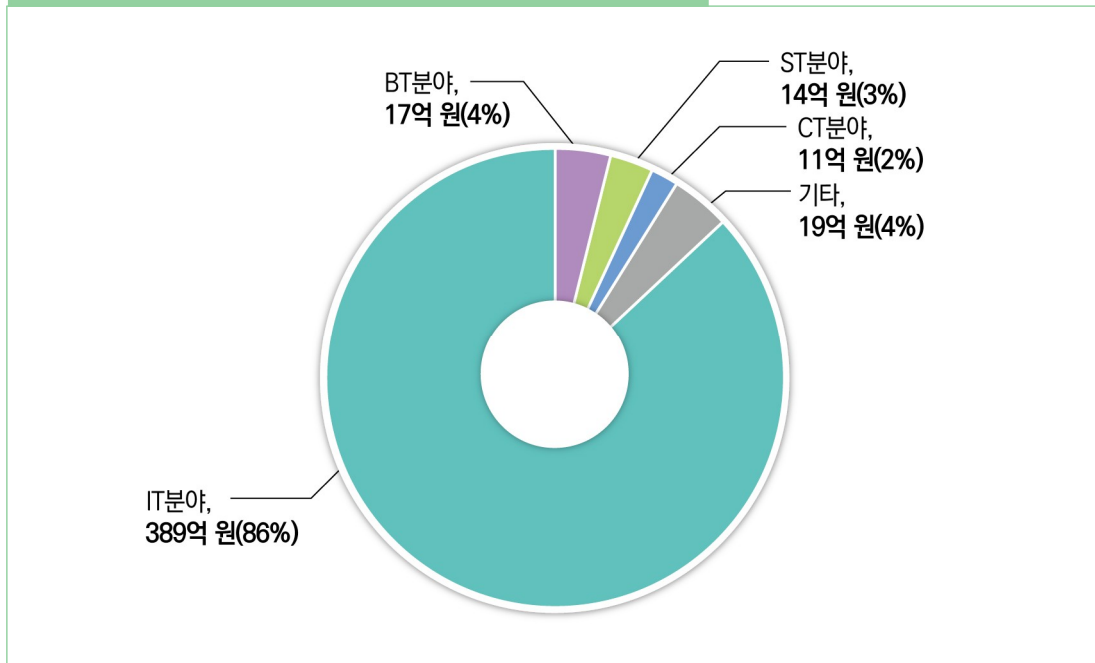


그림 18. 미래유망 신기술분류(6T)별 연구비 규모 및 비율



□ (주요 과제) 원고의 주요 내용 및 키워드 등을 기준으로 선정함

과제명 (사업명, 부처명)	수행기관, 총 연구기간, 연구비 규모	과제 주요 내용
웨어러블 디바이스 기반 다중생체 신호를 이용한 사용자 인증 기술 (이공학학술연구기반구축, 교육부)	조선대학교, 2017-2026년, 5억 원('17)	일상생활 중 웨어러블 디바이스를 통해 다중 생체신호를 취득하고, 이를 이용하여 사용자를 인증할 수 있는 정보통신기술(IT)과 생명공학기술(BT)이 융합된 기술 개발
비접촉 2단계인증을 이용한 신원확인 시스템 개발 (중소기업기술혁신개발, 중소벤처기업부)	에코스올루션(주), 2020-2022년, 2억 원('21)	얼굴인식 알고리즘 개발 및 딥 러닝(deep learning)을 이용한 인식을 및 안정성 향상
향상된 보안과 정보보호를 위한 걸음걸이신호로부터 키 자동 생성 (개인기초연구, 교육부)	전남대학교, 2017-2020년, 0.1억 원('20)	걸음걸이신호(gait biometrics)로부터 암호화시스템에서 사용 할 수 있는 암호화 키(key)를 생성하여 기존 암호화 시스템과 융합

# 융합연구리뷰

Convergence Research Review 2022 November vol.8 no.11

이 보고서는 2022년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 사업임

(No. NRF-2012M3C1A1050726)