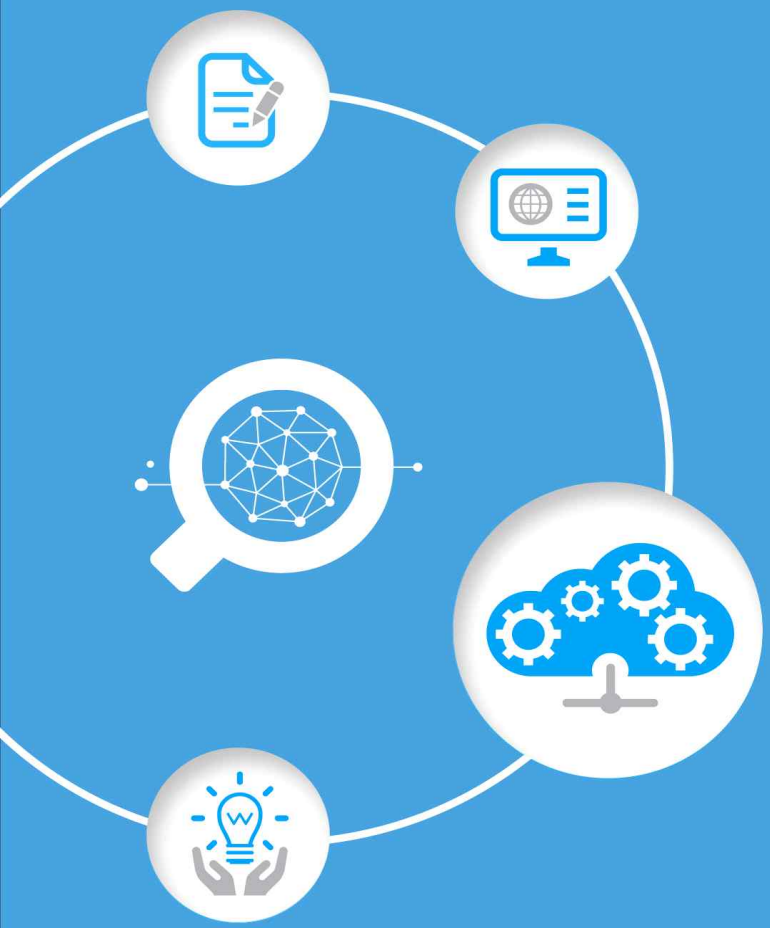
# Ⅲ

# 정보보호

## 차세대보안



# 목차

## 차세대보안

# Ⅰ. 표준화 개요

## 1.1. 기술 개요

차세대보안 기술은 제4차 산업혁명 시대의 초지능, 초연결, 초실감, 초신뢰 ICT 환경에서 전달, 저장되는 정보를 위/변조, 유출, 해킹, 서비스거부 등을 비롯한 각종 불법 행위로부터 안전하게 보호하고, 물리적 공간에서의 보안 침해사고 방지하며, 타 산업과의 융합 시스템에서의 보안을 제공하기 위한 기술로, 차세대 암호기술, 인증서 및 바이오인식 기반 인증 기술, 능동형 사이버 보안기술, 시험평가 기준 및 관리를 위한 보안관리/평가 기술, 헬스케어 및 자동차 보안 등을 위한 융합보안 기술로 구분


<차세대보안 기술의 개요도>

- (차세대 암호기술) 암호기술은 사이버 환경에서 정보의 안전한 관리(저장, 송수신 등)를 위한 기술로 정보보호의 근간을 형성함. 기존에는 보호 대상 정보에 대한 안전성(비밀성, 무결성 등 보장)을 우선적으로 고려한 기술 개발이 주로 이루어진 반면, 최근에는 서비스 가용성을 동시에 고려하여, 특히 클라우드/빅데이터 데이터 보안을 위한 데이터처리(DBMS) 적합형 암호(형태보존 암호 등), 암호문 연산이 가능한 동형 암호나 사물인터넷(IoT) 보안을 위한 경량 암호, 양자 컴퓨터에 대비한 양자 키 분배 등으로 개발 범위를 확장하고 있음

- (PKI 기반 인증 및 응용기술) PKI 기반의 인증기술은 다양한 사용자 인증기술이 발전함에 따라서 서비스기관의 위험정도에 따라 여러 가지 방법이 적용되고 있음. 특히 비밀번호를 대신하는 FIDO 기반의 바이오 인증기술이 지문센서, 홍채센서를 탑재한 스마트폰이 일반화

되면서 다양한 분야에 적용되고 있음. PKI 기반 인증기술도 FIDO 기반의 바이오인증과 결합하여 편리성과 안전성이 강화된 바이오기반 공인인증서 서비스가 금융권에 적용하는 추세에 있음

- (범용인증기술) 범용인증기술은 사이버 환경에서 적법한 사용자나 기기를 식별하고 유통되는 정보의 신뢰성과 부인방지 특성 등을 제공하는 기존의 인증기술 및 미래의 인증기술을 포괄하는 개념으로, 각 인증기술의 특성을 유지하면서 다양한 상황에서 적용 가능한 인증 프레임워크를 제공함. 공인인증서와 같은 사용자 본인확인 기술에서부터 단말기의 진위 여부를 확인하기 위한 디바이스 인증기술, 사용자 익명성을 보장하는 익명인증기술, 일회용 비밀번호를 사용하는 OTP(One Time Password) 인증기술 등을 포함하며, 최근에는 핀테크 분야에서 지식기반(패스워드 등) 인증 대신 소유기반(HW토큰 등), 바이오기반(지문, 얼굴 등) 인증 기술을 적용하는 추세에 있음

- (바이오인식 응용 서비스) 바이오인식 응용서비스는 최근에 스마트폰 등 모바일기기에서 지문·얼굴·홍채·정맥인식 등 바이오인식기술을 적용하여 모바일 지급결제서비스, 인터넷전문은행 등 핀테크분야에서 비대면 인증수단으로 널리 활용하고 있는 추세임. 이러한 모바일 바이오인식기술과 더불어 유무선에서 바이오인식 응용기술을 활용하는 텔레바이오인식기술, 바이오정보 보호기술, 바이오인식 시험기술도 이에 포함될 수 있음도 이에 포함될 수 있음

- (생체신호기반 텔레바이오 인식기술) 기존의 바이오인식기술의 위변조에 대한 위협이 국내외적으로 증대됨에 따라, 최근 미국·캐나다·영국 등 주요선진국에서는 심전도·뇌파 등 생체신호를 이용한 텔레바이오인식 기술개발에 박차를 가하고 있는 추세임. 특히 생체신호 인증기술은 위변조에 강인하고 지속인증 등의 장점이 있어 차세대 바이오인식기술로 각광을 받고 있음

- (바이오인식기반 CCTV보안기술) 최근에 지능형 CCTV 영상보안기술에서 물체와 사람을 우선적으로 구별하고, 사람에 대한 얼굴인식·홍채인식·걸음걸이인식 등의 바이오인식기술을 결합함으로서 국제공항·지하철 등 군집되어 있는 공공시설에서의 대테러 보안 등에 활용하는 융합보안기술이 각광을 받고 있음

- (보안 솔루션 위협정보 공유 및 연동 프레임워크) 사이버 위협이 고도화됨에 따라 사용자는 복잡한 방어체계를 구축하여 대응하고 있으나, 보안솔루션 제품간 다양한 형식의 보안이벤트 및 각각의 상이한 연동 프로토콜을 가지고 있어, 이기종 제품간의 이벤트 정보 연동/공유가 어렵고, 그에 따라 자동화된 위협 대응이 어려움. 따라서 사이버 위협정보를 정형화된 방식으로 표현하고 공유하는 위협정보 공유 및 연동 프레임워크 표준화를 진행하며, 표준화된 방식에 맞는 기술 개발을 함으로써 급속도로 증가되는 사이버위협을 신속하게 분석 · 공유함으로써 국가적인 사이버 위협 빠르게 대응할 수 있는 체계 구축이 가능해짐

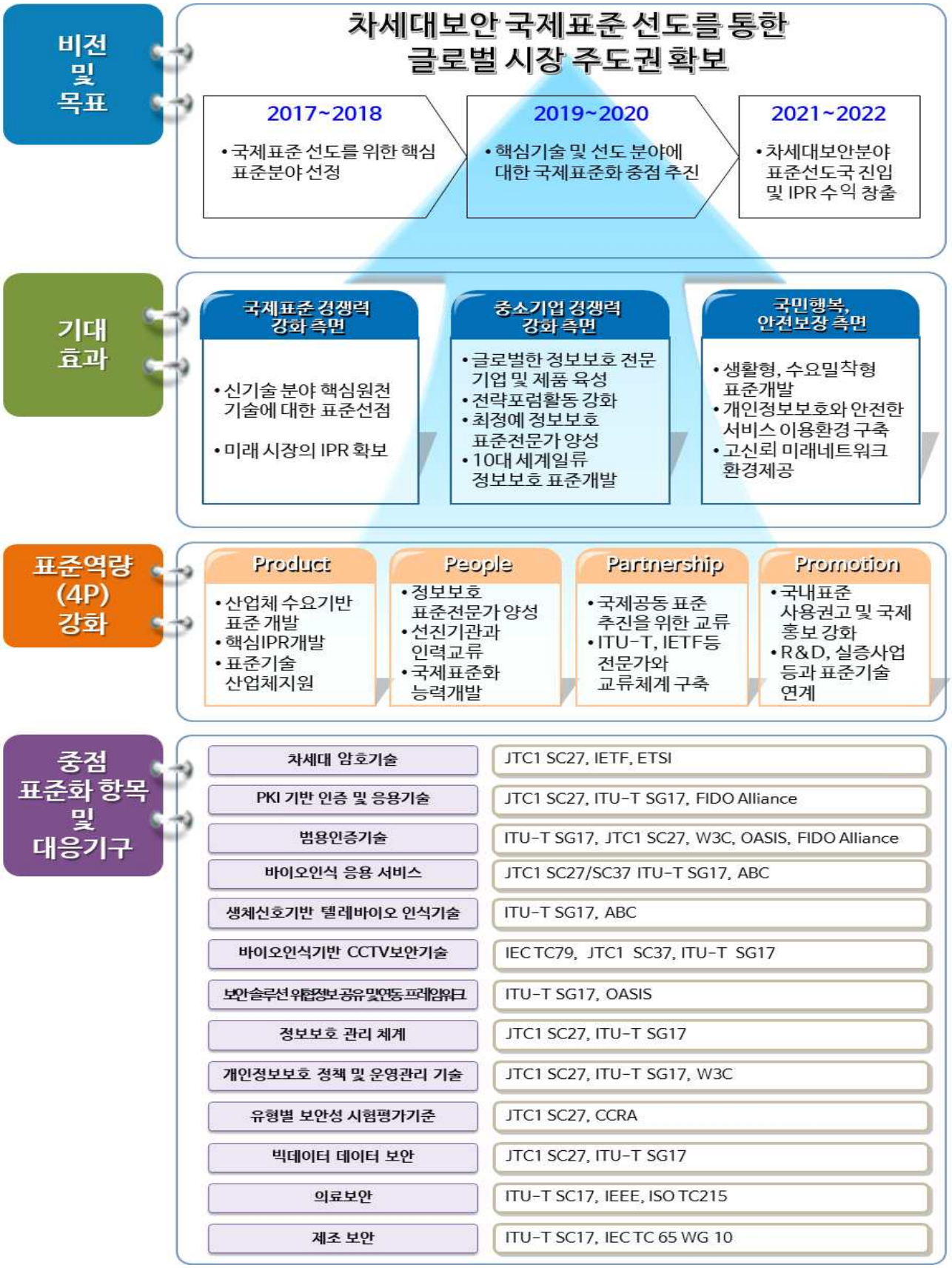
- (유형별 보안성 시험평가기준) 보안성 평가는 정보통신망에서 소통되는 중요 정보를

보호하기 위해 사용되는 정보보호시스템 또는 암호모듈의 보안성을 평가하는 활동으로서 공통평가기준 또는 암호모듈 검증기준이 적용되고 있으며, 시험평가 대상의 유형에 따라 요구사항 기준과 평가방법론이 제공

- (정보보호 관리체계) 정보보호 관리체계는 조직 내외의 모든 활동에서 정보를 안전하게 보호하기 위한 경영체계의 수립을 지원하기 위한 기준 및 지침, 그리고 이를 인증하기 위한 기준 및 지침을 제공함. 또한 금융, 통신, 클라우드, 에너지, 의료 등 산업 분야별 특성을 반영하여 정보보호의 효과성과 효율성을 제고할 수 있는 구체적인 활동 지침과 함께 이러한 업무를 수행하기 위한 전문가에 대한 인증 자격 기준을 제공
- (개인정보보호 정책 및 운영관리 기술) 개인정보보호는 개인정보의 수집, 저장, 이용 및 제공, 관리, 파기 등에 이르는 생명주기에 걸쳐 개인정보 법률을 준수하고, 정보주체에게 자기결정권을 제공함으로써 이용자의 개인정보를 보호하는 기술로서 개인정보가 저장 및 관리되는 데이터베이스뿐만 아니라, 인프라, 네트워크, 디바이스 등 개인정보가 이용되는 모든 과정에서 개인정보를 합법적인 방법으로 사용하도록 보장
- (빅데이터 데이터 보안) 빅데이터는 다양한 정보를 가공, 분석하여 필요한 정보를 획득하는 일련의 과정을 시스템화 하는 기술로 다양한 소스의 데이터를 연결 및 가공하는 것이 필수적인 과정임. 빅데이터 데이터 보안은 이 과정에서 발생할 수 있는 데이터 가공의 오용과 개인정보 침해 가능성을 방지하고 시스템적으로 방지하는 기술을 제공
- (의료보안) 의료기관에서 사용되는 각종 의료정보시스템(HIS, EHR, EMR, PACS, OCS 등), 의료기기 및 개인건강기기 제조업체 및 사용자 등을 기반으로 하는 보안 및 개인정보보호를 위한 기술
- (제조보안) 인터넷 기반의 제조 분야 주요 기기 보안 인증 기술 및 제조 정보보호관리체계 인증 기술

## 1.2. 표준화 비전 및 기대효과

○ 표준화 비전



○ 표준화 목표

- 차세대 보안 분야 국제 표준화 선도 및 글로벌 시장 주도권 확보를 위하여 다음과 같은 표준화 목표를 설정

  · 단기적으로 (2018년경까지), 신규 분야의 국제표준 선도를 위한 핵심원천 기술에 대한 표준 선점 및 시장 주도권 확보를 위한 IPR 확보에 기여
  · 중기적으로 (2020년경까지), 핵심기술 및 선도가능 분야에 대한 국제 표준화를 중점 추진하고, 글로벌 정보보호 전문 기업 육성 및 제품 개발, 표준 전문가 양성 및 10대 글로벌 정보보호 표준 개발을 통해 국내 기업의 국제 경쟁력 강화에 기여
  · 장기적으로 (2022년경까지), 차세대보안 분야 표준 선도국 진입 및 IPR 수익 창출에 기여하고 국민이 안전하고 신뢰할 수 있는 미래 네트워크 및 서비스 이용환경을 제공

○ 표준화 기대효과

- 국제표준 경쟁력 강화 측면

  · 첨단 ICT 환경의 정보보호 핵심 원천기술인 경량, 고속 암호기술과 미래 암호기술인 양자 암호기술 표준 개발 주도
  · 신규 ICT 환경에 적합한 보안 평가기술 국제표준 발굴
  · 세계최초로 개발중인 지문·심전도·심박수 등 다중 생체신호를 이용한 텔레바이오 인식기술을 차세대 바이오인식기술로 발전시켜 국제표준화를 선도
  · 빅데이터 참조모델에서의 보안 및 프라이버시 측면 국제표준 개발

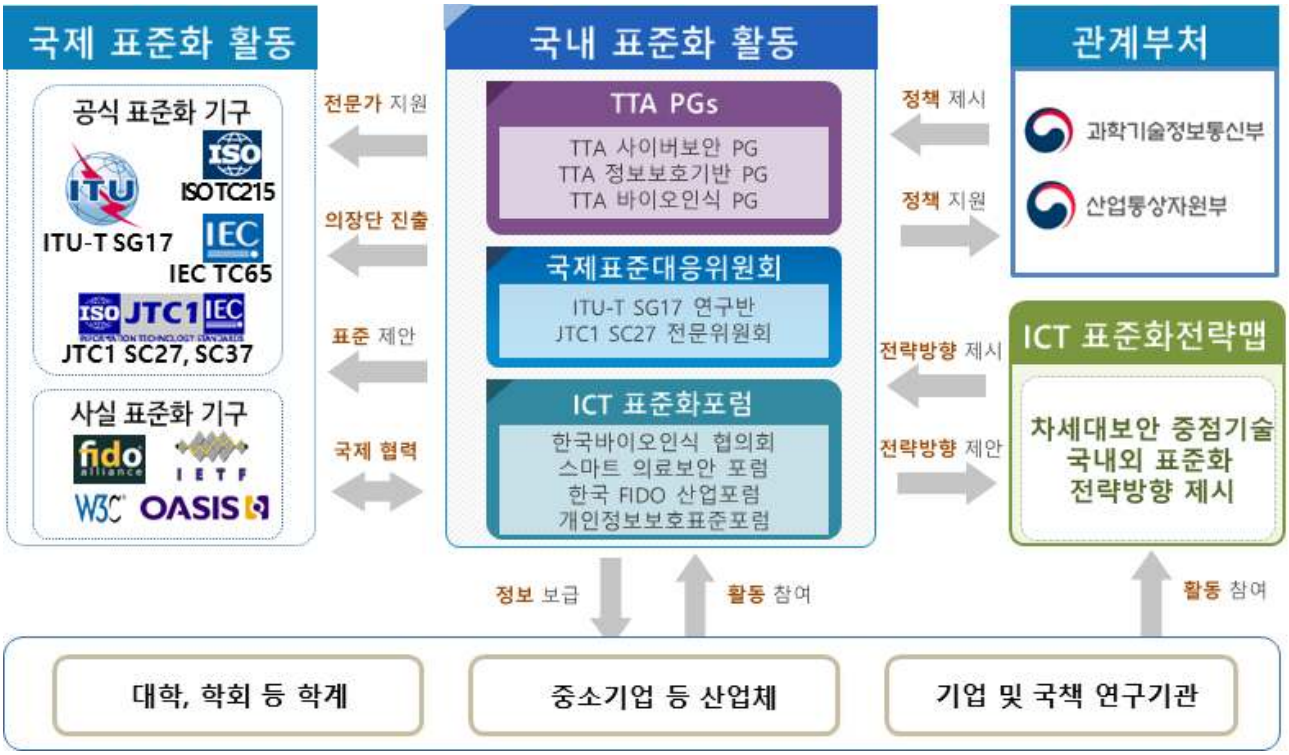
- 중소기업 경쟁력 강화 측면

  · 우수 성능의 차세대 암호기술 사전 적용을 통한 국산 암호제품 시장 경쟁력 확보
  · 다양한 인증기술을 비대면 전자거래에 적용하여 전자거래 전 분야의 서비스 활성화에 기여
  · 중소기업의  환경을 고려한 체계화된 정보보호 활동의 기준을 수립함으로써 정보보호 활동의 사각지대를 최소화하고 균형 성장 기반을 마련하며, 보안평가 관련 국제표준 개발에 적극 참여하여 국내 보안정책 및 보안 산업계의 의견을 반영함으로써 보안산업의 국제 경쟁력 확보
  · 스마트폰에 지문·얼굴·홍채·정맥인식기술 등 바이오인식 응용서비스기술이 확산·보급됨과 동시에 바이오정보 위변조 위협이 급증함에 따라 성능시험 및 제시형 공격 탐지시험 등 바이오인식제품의 시험인증서비스 기반을 조성하여 바이오인식산업의 안전·신뢰성 확보

- 국민행복·안전보장 측면

  · 차세대 암호기술을 기반으로 안전성이 담보된 첨단 ICT 환경의 조기 구축 기여
  · PKI 기반 인증기술과 FIDO 기반의 바이오인증과 결합하여 편리성과 안전성이 강화된 공인인증서 이용 환경 제공
  · 국제공항, 지하철 등 대중 공공장소에 사생활 보호 및 범법자·테러리스트 검색강화를 위하여 바이오인식기반 지능형 CCTV 및 안전신뢰성이 보장된 바이오인식제품 설치·운영
  · 사물인터넷 기기 중 의료·제조 분야 인증제도 및 서비스를 발굴하고 기기·설비들의 안전성·보안성을 제공기 위한 기기 간 상호 보안 인증 기술 국제표준화와 관련 요소 기술 특허 확보 및 선점을 통한 시장 경쟁력 확보

## 1.3. 표준화 추진체계




○ ICT 표준화전략맵

- 표준화전략맵의 표준화 전략방향에 따라 국내 한국바이오인식협의회, 스마트 의료보안 포럼, 한국 FIDO산업포럼, 개인정보보호표준포럼에서 관련 포럼표준을 제정하고, TTA PG501(정보보호기반), PG502(개인정보보호/ID관리, 블록체인 보안), PG503(사이버보안), PG505(바이오인식)를 통해 단체표준을 개발과 ITU-T SG17 연구반 및 JTC1 SC27 등의 국제 표준화 전략 방향을 제시

○ 국내 표준화 활동 체계

- 국내 한국바이오인식협의회, 스마트 의료보안 포럼, 한국 FIDO산업포럼, 개인정보보호 표준포럼에서 산학연 의견수렴하여 포럼 표준을 제정하고, 관련 TTA PG를 통해 단체표준을 개발

○ 국제 표준화 활동 체계

- ITU-T SG17와 ISO/IEC JTC1 SC27 중심으로 국제표준화를 주도하여 표준 개발
- 사실표준화기구인 IETF 및 FIDO Alliance 를 통해 적극 대응

## 1.4. 중점 표준화 항목

○ 중점 표준화 항목 범위의 설정

- 암호 기술은 차세대 암호기술 1개 항목을 중점 표준화 항목으로 설정
- 인증 기술은 PKI 기반 인증 및 응용기술, 범용인증기술,바이오인식 응용 서비스, 생체신호 기반 텔레바이오 인식기술, 바이오인식기반 CCTV보안기술 5개 항목을 중점 표준화 항목으로 설정
- 능동형 사이버보안 기술은 보안 솔루션 위협정보 공유 및 연동 프레임워크 1개 항목을 중점 표준화 항목으로 설정
- 보안 관리/보안 평가 기술은 정보보호 관리체계, 개인정보보호 정책 및 운영관리 기술, 유형별 보안성 시험평가기준 3개 항목을 중점 표준화 항목으로 설정
- 융합보안 기술은 빅데이터 데이터 보안, 의료보안, 제조보안 3개 항목을 중점 표준화 항목으로 설정

| 중점 표준화 항목 | | 표준화 내용 | Target SDOs | 전략 목표 |
|---|---|---|---|---|
| 암호 기술 | 차세대 암호기술 | - IoT/M2M, 클라우드, 빅데이터, 스마트기기, DBMS 등 신규 ICT 환경 정보보호에 적합한 차세대 암호 알고리즘 규격 제시<br>- 양자 암호 키 분배 기술 규격, 안전성 기준 제시 | JTC1 SC27, IETF, ETSI | 차세대 공략 |
| 인증 기술 | PKI 기반 인증 및 응용기술 | - 기기나 사람에 대한 식별 인증하는 기기인증, 공인인증, 서버인증, 차량인증 등의 다양한 PKI 기반의 인증기술<br>- 스마트폰 환경에서 공인인증서의 비밀번호를 바이오인증(FIDO)과 결합하여 대체하기 위한 바이오공인인증서비스 기술<br>- FIDO 2.0에 기반한 O2O 차세대 바이오 인증으로 스마트폰/App, PC/웹브라우저, 그 외 확장된 Device /응용솔루션의 규격 및 기준제시 | JTC1 SC27, ITU-T SG17, FIDO Alliance, W3C | 다각화 협력 |
| | 범용인증기술 | - 행위, 상황, 바이오, 토큰 기반의 다양한 인증기술<br>- ICカード, TrustZone, TPM 등 HW 기반 인증기술<br>- 핀테크, O2O, IoT, SNS 등 서비스 환경에 적합한 인증기술을 지원하고 신뢰된 기관을 통해 ID 통합관리 서비스를 제공하기 위한 기반 및 응용기술 표준화<br>- 대면 인증을 요구했던 기존 오프라인 서비스를 대상으로, 동일한 보안 수준의 비대면 본인확인을 제공하는 인증 서비스의 기반 및 응용기술 표준화 | ITU-T SG17, JTC1 SC27, W3C, FIDO Alliance, OASIS | 적극 공략 |
| | 바이오인식 응용 서비스 | - ICカード, PKI 기술, 스마트 의료정보 보안기술 등 바이오인식기반 융합기술<br>- 모바일 바이오인식 응용기술 및 성능시험기술<br>- 위변조 방지 등 바이오정보 보호기술 | JTC1 SC37, ITU-T SG17, ABC | 적극 공략 |

| 중점 표준화 항목 | | 표준화 내용 | Target SDOs | 전략목표 |
|---|---|---|---|---|
| | 생체신호기반 텔레바이오 인식기술 | - 심박수·심전도 등 생체신호정보 데이터 호환규격, 생체신호 인증메커니즘<br>- 생체신호정보 보호기술<br>- 생체신호 인증알고리즘 성능시험기준 | ISO TC215, ITU-T SG17, ABC | 적극공략 |
| | 바이오인식기반 CCTV보안기술 | - 지능형 CCTV 보안기술<br>- 얼굴인식 등 바이오인식과 결합되는 지능형 CCTV 융합보안 기술 | JTC1 SC37, IEC TC79 | 적극공략 |
| 능동형 사이버 보안 | 보안 솔루션 위협정보 공유 및 연동 프레임워크 | - STIX/TAXII 기반의 사이버 위협분석 정보 표현 규격<br>- STIX/TAXII 기반 사이버 위협분석 정보 연동 프레임워크 | ITU-T SG17, OASIS | 차세대공략 |
| 보안관리/보안평가 | 정보보호 관리체계 | - 정보보호 활동에 대한 체계화되고 통인된 교정활동의 표준을 마련하기 위한 기준 제시<br>- 제조 분야 정보보호 경영시스템 인증기준<br>- 정보보호 경영전문가 자격 기준<br>- 중소기업 정보보호 관리체계 | JTC1 SC27, ITU-T SG17 | 적극공략 |
| | 개인정보보호 정책 및 운영관리 기술 | - 개인정보보호 정책 관리<br>- 개인정보보호 운영 관리 | JTC1 SC27, ITU-T SG17 | 적극공략 |
| | 유형별 보안성 시험평가기준 | - IT제품 보안성 평가기준 표준화<br>- 암호모듈 시험기준 표준화<br>- CC 평가자 및 암호모듈 시험자 자격기준 표준화 | JTC1 SC27, CCRA, CCUF | 적극공략 |
| 융합보안 | 빅데이터 데이터 보안 | - 개인정보 유출 방지를 위한 참조 모니터 기술<br>- 인공지능/빅데이터 분석을 위한 비식별화 기술<br>- 모바일 환경에서 빅데이터 보호 기술 | JTC1 SC27, ITU-T SG17, ODCA, CSA | 차세대공략 |
| | 의료보안 | - 의료정보시스템(HIS, EMR, EHR, PHR 등), 의료영상처리시스템(PACS), 처방전달시스템(OCS), 의료정보 및 교류, 개인건강정보 등 보건의료 분야에서 필요한 정보보호 기술<br>- 사이버공격이 집중되고 취약점이 발견된 약물주입펌프, 인슐린펌프, 심장박동기 등 의료기기 안전 및 정보보호 관련 기술<br>- 헬스케어 응용서비스의 생체신호기반 텔레바이오 인증기술 | ITU-T SG17, ISO TC215 | 차세대공략 |
| | 제조 보안 | - 인터넷 기반의 제조 분야 주요 기기 보안 인증 기술 및 제조 정보보호관리체계 인증 기술 | IEC TC65, ITU-T SG17 | 차세대공략 |

○ 추진경과

- Ver.2016(2015년)에서는 공통기반보안, 네트워크/디바이스보안, 서비스/융합보안 분야로 구분하여 중점 기술 및 표준화 항목을 각각 선정하였음. 공통기반보안 분야는 암호기술, 인증기술, 보안관리/보안평가, 개인정보보호 그룹으로, 네트워크/디바이스보안 분야는 SDN/NFV보안, IoT보안, 사이버보안, 스마트폰보안 그룹으로, 서비스/융합보안 분야는 클라우드/빅데이터보안, 웹보안, 콘텐츠보안, 금융보안, 휴먼/바이오인식, 산업제어 시스템보안, 헬스케어보안 그룹으로 나누어 표준화 항목을 선정함

- Ver.2017(2016년)에서는 Ver.2016과 동일하게 3개 분야(공통기반보안, 네트워크/디바이스보안, 서비스/융합보안)로 구분하였으며, 공통기반보안 분야에서는 차세대 다중요소 인증기술 항목 및 Identity 관리 기반 기술을 타 항목으로 통합 또는 삭제하였으며, 네트워크/디바이스보안 분야는 IoT 게이트웨이 보안 프레임워크, 사이버 공격 대응을 위한 빅데이터 분석 요구사항, 악성코드 통합 대응 기능 및 구조, 스마트폰 스팸 대응을 위한 보안 요구사항을 타 항목과 통합 또는 삭제하였으며, IoT 디바이스 보안, 스마트폰 기반의 봇넷 대응을 위한 보안 요구사항 항목을 새로 추가하였음

- Ver.2018(2017년)에서는 이전의 3개 분야(공통기반보안, 네트워크/디바이스보안, 서비스/융합보안)를 하나로 통합하였으며, 암호기술, 인증기술, 능동형사이버보안, 보안관리/보안평가, 융합보안 그룹으로 나누어 각 그룹 별 표준화 항목을 선정하였음

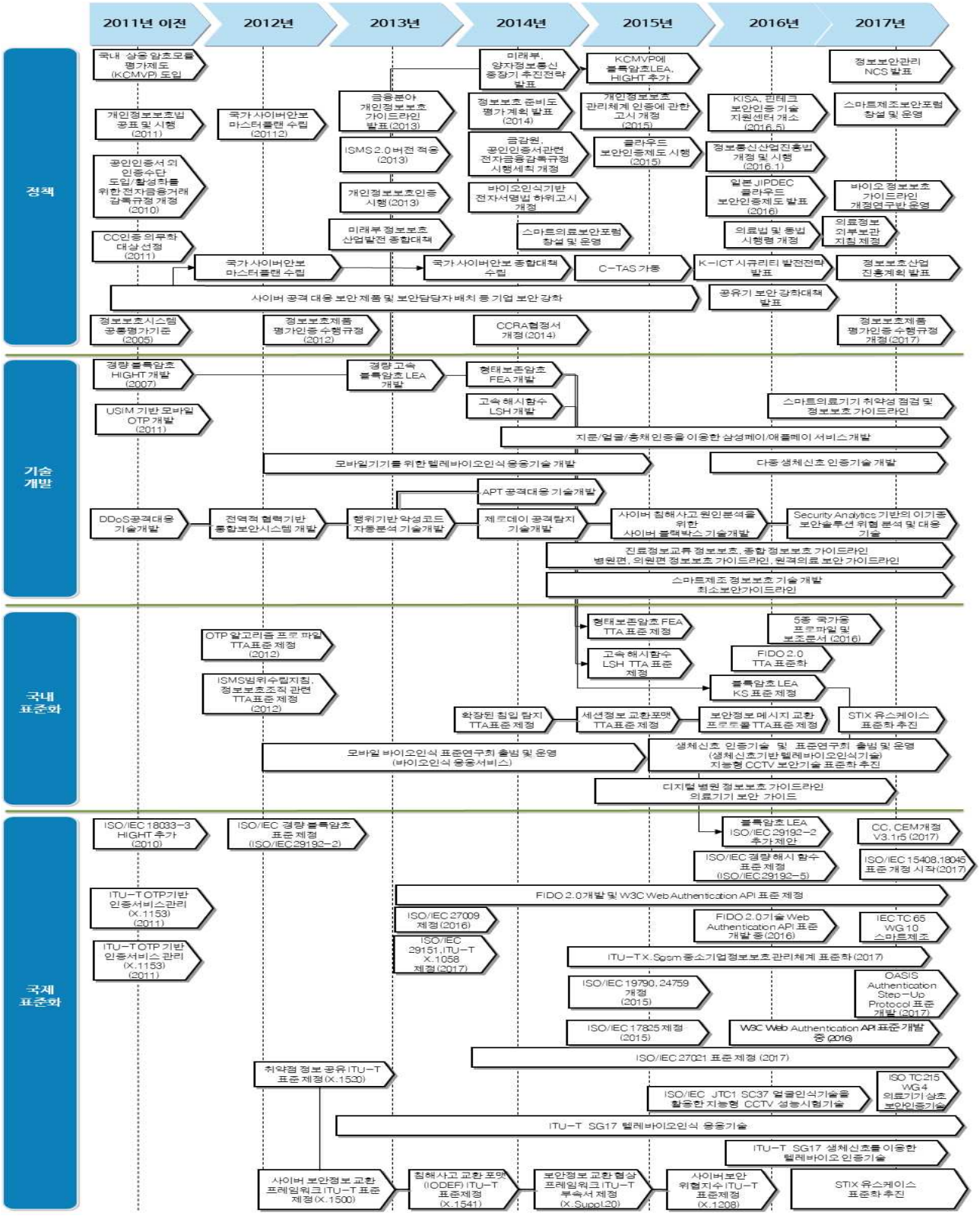
<버전별 표준화 항목 비교표>

| 구분 | Ver.2016 | Ver.2017 | Ver.2018 |
|---|---|---|---|
| 공통기반 | 차세대 암호 및 적용 | 차세대 암호 및 적용 | 차세대 암호기술 |
| | PKI 기반 인증 및 응용기술 | PKI 기반 인증 및 응용기술 | PKI 기반 인증 및 응용기술 |
| | 범용 인증체계 | 범용인증기술 | 범용인증기술 |
| | 차세대 다중요소 인증기술 | - | - |
| | 유형별 보안성 시험평가기준 | 유형별 보안성 시험평가기준 | 유형별 보안성 시험평가기준 |
| | 정보보호 경영전문가 자격 기준 | 정보보호 경영전문가 자격 기준 | 정보보호관리체계 |
| | 정보보호 감사관리 지침 | 정보보호 감사관리 지침 | |
| | 분야별 정보보호 관리체계 및 인증 | 분야별 정보보호 관리체계 및 인증 | |
| | Identity 관리 기반 기술 | - | - |
| | 모바일 결제 기술 | 모바일 결제·인증 기술 | - |
| | 개인정보보호 정책 및 운영관리 기술 | 개인정보보호 정책 및 운영관리 기술 | 개인정보보호 정책 및 운영관리 기술 |
| 네트워크/디바이스 | IoT 통신 인프라 보호 프레임워크 | IoT 네트워크 및 플랫폼 보안 프레임워크 | - |
| | IoT 게이트웨이 보안 프레임워크 | - | - |
| | IoT 서비스 보호 프레임워크 | IoT 정보보호 프레임워크 | - |
| | | IoT 디바이스 보안 | - |
| | SDN/NFV 보안 프레임워크와 메커니즘 | SDN/NFV 보안 프레임워크와 메커니즘 | - |
| | SDN/NFV 보안 응용 및 서비스 | SDN/NFV 보안 응용 및 서비스 | - |

| 구분 | Ver.2016 | Ver.2017 | Ver.2018 |
|---|---|---|---|
| | 사이버 공격 대응을 위한 빅데이터 분석 요구사항 | - | - |
| | 보안정보공유 및 통합제어 프레임워크 | 보안정보공유 및 연동 프레임워크 | 보안 솔루션 위협정보 공유 및 연동 프레임워크 |
| | 악성코드 통합 대응 기능 및 구조 | - | - |
| | 악성코드 분석 및 보고 형식 | 악성코드 분석 및 보고 형식 | - |
| | 침해사고 분석을 위한 네트워크 증거 보존 요구사항 | 침해사고 분석을 위한 네트워크 포렌식 도구 요구사항 | - |
| | 스마트폰 스팸 대응을 위한 보안 요구사항 | - | - |
| | 스마트폰 환경에서의 저장장치 보안 프레임워크 | 스마트폰 환경에서의 저장장치 보안 프레임워크 | - |
| | - | 스마트폰 기반의 봇넷 대응을 위한 보안 요구사항 | - |
| 서비스/융합 | 클라우드 컴퓨팅 서비스에서의 개인정보 국외교환 프레임워크 | 클라우드 컴퓨팅 서비스에서의 개인정보 국외교환 프레임워크 | - |
| | 클라우드 컴퓨팅 서비스 보안 요구사항 | 클라우드 컴퓨팅 서비스 보안 요구사항 | - |
| | 클라우드 인증 및 접근제어 보안 프레임워크 | 클라우드 인증 및 접근제어 보안 프레임워크 | - |
| | 신뢰 클라우드 연동 보안 | 신뢰 클라우드 연동 보안 | - |
| | 빅데이터의 데이터 보안 | 내용기반 빅데이터 접근제어 | 빅데이터 데이터 보안 |
| | 차세대 웹 보안<br>모바일 웹 보안<br>웹 프라이버시 보호<br>SOA 보안 | 웹 매쉬업 보안 | - |
| | 유해정보 차단 정책 및 기술 | 유해정보 차단 정책 및 기술 | - |
| | 콘텐츠 접근 제어를 위한 연령 검증 프로토콜 | 융합서비스 환경에서의 속성기반 접근제어 | - |
| | 핀테크 서비스 보안 기술 | 핀테크 서비스 보안 기술 | |
| | 금융거래 이상 징후 방지 기술 | 금융거래 이상 징후 방지 기술 | - |
| | 바이오인식 응용 서비스 모발 바이오 인증 | 바이오인식 응용 서비스 | 바이오인식 응용 서비스 |
| | 생체신호기반 텔레바이오인식 기술 | 생체신호기반 텔레바이오인식 기술 | 생체신호기반 텔레바이오인식 기술 |
| | - | 바이오인식기반 CCTV보안기술 | 바이오인식기반 CCTV보안기술 |
| | - | - | 제조보안 |
| | 스마트그리드 보안 기능 구조 | 스마트그리드 보안 기능 구조 | - |
| | - | 안전한 단방향 데이터통신 | - |
| | 스마트그리드 보안 기능구조 | 스마트그리드 보안 기능구조 | - |
| | 스마트그리드 보안관리 | 스마트그리드 보안관리 | - |
| | 스마트그리드 기기 보안 | 스마트그리드 기기 보안 | - |
| | V2X 통신 보안 프레임워크 | V2X 통신 보안 프레임워크 | - |
| | 전자건강기록(EHR) 보안 프레임워크 기술 | 전자건강기록(EHR) 보안 프레임워크 기술 | 의료보안 |
| | 개인건강기록(PHR) 서비스 보안 | 개인건강기록(PHR) 서비스 보안 | |

# Ⅱ. 국내외 현황분석

## 2.1. 연도별 주요 현황 및 이슈



## 2.2. 정책 현황 및 전망

| 구분 | 주요 현황 |
|---|---|
| 한국 | - 과학기술정보통신부 고시 제2017-7호, 정보보호시스템 평가인증지침 고시 [2017]<br>- 방송통신위원회, 개인정보보호 관리체계(ISMS) 인증 등에 관한 고시(방송통신위원회 고시 제2015-29호) [2016]<br>- 정보통신망법 개정에 따라서 연간 매출액 또는 세입 등이 1,500억 이상인 자 중 대통령령으로 정하는 기준을 해당하는 기관 중 「의료법」제 3조의 4에 따라 상급 종합병원 43개 모두 정보보호관리체계(ISMS) 인증이 의무화됨 [2016.6]<br>- 행정자치부, 개인정보 비식별 조치 가이드라인 고시 [2016]<br>- 미래부 사이버 위협정보 공유 확대 계획 등 'K-ICT 시큐리티 2020' 발표[2016,6]<br>- 금융위원회, 금융감독위원회공고 제2015-7호, 전자금융거래감독규정 [2015]<br>- 미래부, 사물인터넷 기본계획, 정보보호 로드맵 수립에 이어 로드맵 시행계획 마련을 통해 사물인터넷 제품과 서비스의 보안 내재화 및 경량·저전력 암호기술 등의 핵심 원천기술 개발 추진 [2014, 2015]<br>- 미래부, 양자 정보통신 중장기 추진전략을 수립하고 단계별로 수도권과 대전권 연결 양자 암호통신 시험망 구축 추진 [2014]<br>- 미래부, 양자 암호 등 정보보호 신시장 창출 및 양자 정보통신 지원 확대를 포함하는 2017년 업무계획 발표 [2017]<br>- 원자력안전법에 따라 규제기관인 KINS(원자력안전기술원)에서 KINS/RG-N08_22(디지털 계측 및 제어장치의 사이버보안)가 개정되어 실무적으로 활용 [2014.11]<br>- 「원자력시설 등의 방호 및 방사능 방재 대책법」법률에 "전자적 침해 행위", "원자력 시설 컴퓨터 및 정보 시스템"의 정의를 신설하고, 정부 및 원자력사업자가 각각 원자력시설 컴퓨터 및 정보시스템 보안을 강화하기 위한 시책 및 규정을 마련 [2015.12.1.]<br>- 바이오인식기반 전자서명법 하위고시 개정 [2014]<br>- 지문인증을 이용한 삼성페이 서비스 개발 [2015]<br>- 바이오정보보호 가이드라인 2차 개정 연구반 운영중[2017]<br>- 미래창조과학부고시 제2013-51호, 정보보호시스템 공통평가기준[2013]<br>- IT보안인증사무국은 8종의 국가용 보호프로파일 및 보조문서를 개발하여 공개<br>국가용 침입방지시스템 보호프로파일 및 보조문서 개발 (2017)<br>국가용 호스트 자료유출 방지 보호프로파일 및 보조문서 개발 (2017)<br>국가용 네트워크 자료유출 방지 보호프로파일 및 보조문서 개발 (2017)<br>국가용 가상사설망 보호프로파일 및 보조문서 개발 (2016)<br>국가용 네트워크 장비 보호프로파일 및 보조문서 개발 (2016)<br>국가용 무선랜 인증 보호프로파일 및 보조문서 개발 (2016)<br>국가용 인터넷 전화 방화벽 보호프로파일 및 보조문서 개발 (2016)<br>국가용 침입차단시스템 보호프로파일 및 보조문서 개발 (2016)<br>- 의료법 시행규칙 제16조 개정('16. 2. 5)으로 전자의무기록의 의료기관 내부 또는 외부보관이 가능해지고 보관장소(의료기관 내부 또는 외부)별 시설과 장비에 관한 구체적인 세부기준을 마련함에 따라 관련 기술의 개발 보급이 확산 |

| 구분 | 주요 현황 |
|---|---|
| | 될 것임<br>- 제조업의 창조경제 구현을 목표로 4대 추진방향, 13대 세부 추진과제를 중심으로 제조업 혁신 3.0 전략을 수립하여 시행 중<br>- 산업통상자원부와 스마트공장추진단 주관하에 스마트공장 보급확산 사업을 펼치고 있으며, 2017년 현재 2,800여개 중소기업에 스마트공장 기술 접목<br>- '22년까지 스마트공장 2만개 확산을 통해 중소·중견기업 공장(20인 이상)의 약 1/3을 IT기반 생산관리 이상 수준으로 스마트화<br>- 행정자치부는 2016년 6월 "개인정보 비식별 조치 가이드라인"을 발표하고 공공 데이터 공개 가이드라인으로 활용<br>- 2017년 1월 한국산업인력공단에서 정보보호관리·운영 국가직무능력표준 발표 |
| 미국 | - NIST, 경량 환경 전용 암호 표준의 필요성을 확인하고 표준화 절차를 확립하기 위한 Lightweight Cryptography Project 시작 [2013]<br>- NIST, 미국 연방정부 사용 공개키 암호를 양자 내성을 가지는 알고리즘으로 변경하기 위한 Post-Quantum Cryptography 표준화 작업 시작 [2016]<br>- 2016년 3월, 미국 국토방위부(DHS)는 자동화 지표 공유(Automated Indicator Sharing, AIS)시스템을 발표 및 적용. 사이버 위협 첩보를 민간 및 공공 부문 보안 담당자들의 원활한 공유 목적<br>- 미국 법무부(DOJ)와 연방거래위원회(FTC)는 사이버 위협 정보를 상호 공유할 수 있도록 하는 공동 선언문(Antitrust Policy Statement on Sharing Cybersecurity Information) 발표<br>- NIAP은 2016부터 응용 소프트웨어, 인증, 암호화 저장, IDS/IPS, 모바일, 네트워크 디바이스, 네트워크 암호화, 운영시스템, 원격접속, VPN, 가상화, VoIP, 무선랜 부문의 보호프로파일 개발하여 공개(2017)<br>- NIST는 산업제어시스템 정보보호 지침(Guide to Industrial Control Systems(ICS) Security, NIST SP 800-82 Rev.2) 개정 2판을 발행 [2015.5]<br>- NIST는 데스크톱/노트북용 BIOS 보안 표준(BIOS Protection Guidelines, NIST SP 800-147)을 발행 [2011.4]<br>- NIST는 서버 컴퓨터의 BIOS 보안 표준(BIOS Protection Guidelines, NIST SP 800-147B)을 발행 [2011.8]<br>- NIST는 비식별 처리 관련 가이드라인 "De-Identification of Personal Information" 발표 [2015.12]<br>- 스마트워치 등 웨어러블디바이스에서 심장박동 등 생체신호를 이용한 개인식별기술 등장 [2015]<br>- 지문인증을 이용한 애플페이 서비스 개발 [2015]<br>- 바이오인식 위변조 탐지기술 개발 및 국제표준화(PAD, biometric Presentation Attack) 추진 [2016]<br>- NIST, 최신기술의 도입과 더불어 사용 운영체제, 데이터베이스의 패치는 헬스케어 운영진들이 직접 제어하지 못하는 문제점이 있어서 병원의 사이버 보안을 강화하기 위한 새로운 지침(TACIT)을 발표<br>- 의료 산업에서 모바일 장치의 정보 보안은 데이터의 기밀성과, 공급자 조직에서 개인 장치 반입이 증가함에 따라 NIST, NCCoE은 직원의 모바일 장치에 저장된 기밀정보를 유지할 수 있는 초안 가이드를 발표함<br>- FDA, ONC, FCC는 ONC 협조를 통해 각종 행위와 민간 영역의 역량에 기반한 위험 관리 기반의 IT 규제 프레임워크를 만들 것을 제안 |

| 구분 | 주요 현황 |
|---|---|
| | - 2009년부터 'Remaking America'를 슬로건으로 국가 첨단 제조방식 전략계획(2012년 2월) 등 제조업 부흥정책을 강력히 추진<br>- 특히, 정보보호와 관련해서 ISA-99에서 산업 자동 제어 시스템의 전자적 보호를 위한 구현에 절차를 정의하는 표준을 정하고 있으며, 기술보고서와 연계된 정보 포함<br>- 스마트공장의 안전 및 보안을 위하여, 산업 제어 시스템 사이버 대응팀(ICS-CERT: Industrial Control Systems Cyber Emergency Response Team)을 독자적으로 운영<br>- 국토안보부의 사이버 보안 및 통신부서 (DHS CS & C: Department of Homeland Security Cyber Security and Communications)의 한 부문으로 국가 사이버 보안 및 통합 센터(NCCIC: National Cyber-security & Communications Integration Center) 내에서 새로운 사이버 위협에 대한 제어 시스템 환경의 방어를 위한 집중 운영 기능 제공 |
| 일본 | - IPA(일본 정보보안관련 전문기관)는 사이버 공격에 대한 대응을 위해 5대 산업, 45개 참여기업의 정보공유 체계인 J-CSIP(Initiative for Cyber Security Information sharing Partnership of Japan)를 2011.10.25부터 발족하여 운영<br>- 영국 Halifax 은행에서 심장박동을 통하여 금융거래자에 대한 신원확인을 해 주는 시범서비스기술 등장 [2014]<br>- 바이오인식 위변조 탐지기술 개발 및 PAD 시험인증 법제화 추진중 [2016]<br>- 바이오인식시스템의 보안성 평가를 위한 기준과 방법에 대한 국제표준 ISO/IEC19989 진행 [2016]<br>- 기존 신성장전략, 일본재생전략에 이은 세 번째 성장전략의 구체적인 정책으로서 「일본재흥전략(日本再興戰略 JAPAN is BACK)」을 수립하여 발표[2013] |
| 유럽 | - EU, Horizon 2020 R&D 프로그램을 통해 ICT 핵심기술 확보를 위한 다수의 차세대 암호기술 개발 프로젝트 출범 [2014]<br>- '주요 정보 기반 시설 보호(CIIP)' 협력을 통해 사이버 보안에 관련된 14개의 법을 시행함으로써, EU 차원에서 각국의 ICT 인프라를 보호하기 위한 대비책 및 회복 역량을 확보하는 등 보안 수준을 강화<br>- EU 역내 국민의 개인정보보호를 위한 기본법인 GDPR 적용 예정 [2018.5.25.]<br>- 영국은 비식별화 사례를 구현하기 위해 민간조직 UKAN을 설립하고 "익명화 프레임워크" 가이드라인 발표 [2016]<br>- EU의 유럽 연합 대응기구인 ENISA에서 빅데이터 프라이버시 보호 가이드라인 발표 [2015]<br>- 영국 Halifax 은행에서 심장박동을 통하여 금융거래자에 대한 신원확인을 해 주는 시범서비스기술 등장 [2014]<br>- 바이오인식 위변조 탐지기술 개발 및 PAD 시험인증 법제화 추진중 [2016] |
| 중국 | - 2015년 5월 18일에 2025년까지 제조 강국에 진입하는 것을 목표로 하는 '중국 제조 2025'를 발표<br>- 향후 30년간 3단계로 나누어 산업구조 고도화 계획 |

## 2.4. 기술개발 현황 및 전망

| 기술개발 수준 | 국내 | □기초연구 ↦ □실험 ↦ □시작품 ↦ ■제품화 ↦ □사업화 | 국내외 격차 | 3년 |
|---|---|---|---|---|
| | 국외 | □기초연구 ↦ □실험 ↦ □시작품 ↦ □제품화 ↦ ■사업화 | | |

### 2.4.1. 국내 기술개발 현황 및 전망

○ **(차세대 암호기술)** 국가보안기술연구소(NSR)와 ETRI를 중심으로 경량, 고속 암호기술, DBMS 적합형 암호기술 등 주요 차세대 암호기술을 개발하였으며, SKT는 양자 키 분배 장비 개발 및 시험 망 운영 중

- (NSR) IoT/M2M, 스마트기기, 클라우드, 빅데이터, DBMS 등 신규 ICT 환경을 위한 핵심 암호기술을 개발하였으며, 양자 키 분배 안전성 시험기술 개발 중
  · 신규 ICT 환경에 적합한 세계 최고 수준의 경량·고속 블록 암호 LEA, 고속 데이터 처리에 적합한 해시 함수 LSH, 그리고 주민번호 등의 DB 저장 개인정보 보호에 적합한 세계 최고 수준의 형태보존 암호 FEA 개발
  · 양자 암호 시험망, 양자 암호화 장비를 대상으로 양자 키 분배 안전성 실증기술을 개발 중
- (ETRI) 형태보존/순서보존/검색가능 암호 등 다수의 DBMS 환경용 암호기술을 개발함
- (서울대학교) 정수환 기반의 동형 암호 알고리즘을 개발하고 다양한 응용서비스 적용 기술을 개발 중
- (SKT) 양자 키 분배 장치 및 전용 중계장치를 개발, 양자 암호 시험망에 적용 및 시험 중

○ **(PKI 기반 인증 및 응용기술)** 바이오인증기술(FIDO)과 공인인증기술(PKI)이 접목되어 안전하고 편리한 생체기반공인인증서비스가 금융권에 제공되고 있고, 기존 신용카드에 지문센서를 부착한 지문카드가 상용화되어 출시되었고 자율주행을 위한 차량인증체계 연구도 진행중임

- (삼성전자) 삼성 갤럭시 S8에 공인인증서와 바이오인증(FIDO 기술)과 결합한 삼성패스(Samsung PASS)를 탑재하여 은행, 증권 등에 생체기반공인인증서비스를 제공함.
- (한국정보인증 등 공인인증기관) 삼성, LG, 아이폰에의 지문센서를 이용한 FIDO 기술과 결합하여 생체기반 공인인증서 솔루션(K-FIDO)을 개발하여 금융권에 제공 중
- (한국스마트아이디, 코나아이, 라이온 등) IC칩에 지문인식 센서를 부착하여 바이오 인증을 제공하는 지문카드가 상용화 되어 출시되었고 공인인증서도 보관이 가능하여 스마트폰과 함께 많은 응용서비스에 사용 예정
- (한국인터넷진흥원/한국도로공사) 자율주행을 위한 C-ITS 보안인증체계(V-PKI) 구축을 위한 정책 연구가 진행 중이며 향후 차량단말(On-Board Unit), 노변기기(Road Side Unit) 등에 인증서를 발급하여 차량의 프라이버시 보호를 진행할 예정임

○ **(범용인증기술)** 다양한 인증기술이 통합하여 이용할 수 있는 범용 인증서비스 체계를 ETRI 중심으로 연구가 진행 중이며, 인증기술 별로 고도화되고 새로운 타입의 인증 기술이 개발될 것으로 예상됨. 최근 스마트폰에서 제공하는 지문인식 기반의 FIDO 표준과 공인인증서와 결합하여 편리성과 안전성을 제공하기 위한 기술 개발 및 국내 표준화를 중점 진행 중. 향후에는 기존 PC환경에서의 단일 인증수단에서 벗어나 스마트폰/웨어러블/IoT 등 다양한 환경에서의 멀티팩터 인증을 수행하기 위해 비밀정보/소지정보/바이오정보 각각의 인증수단에 대한 보안강도 정의 및 인증수단의 조합에 따른 보안강도의 향상을 반영하고, 전자거래의 해킹사고가 점차 정교해짐에 따라 금융권역 등에서 사용자의 보안성 및 편의성 향상에 중점을 둔 다중요소 인증기술과 다양한 인증기술을 통합 관리하는 기능을 제공하여 인증체계 간 상호운용성과 보안성을 강화하는 범용인증체계 표준화 진행 중

- (ETRI) 순천향대학교와의 공동연구를 통해 개체보증 레벨을 보안수준에 따라 4등급으로 분류하는 가이드라인을 개발하고 인증 메커니즘에 따라 세부적으로 등급별 인증수단을 제시하는 연구를 수행 중
- (ETRI) 국내 최초로 FIDO Alliance의 UAF(Universal Authentication Framework) 기술을 개발하여 상용화하였으며 국제 상호운용성 시험을 통과
- (삼성전자) 갤럭시폰의 지문장치를 활용한 FIDO 인증 장치를 개발하여 삼성페이, 페이팔, 알리페이의 결제서비스에서 사용자 인증을 제공하고, 최근에는 지문·홍채·얼굴 등의 생체 인식을 통한 사용자 인증을 온라인 서비스를 대상으로 제공함
- (금융권/과학기술정보통신부) 금융권역의 OTP 통합인증센터, 과학기술정보통신부의 공인인증체계 등 OTP와 PKI가 일부 특정 인증기술에 국한되어 통합 사용 중
- (금융권) 스마트기기의 발달과 함께 모바일기기를 활용하여 보안성을 강화할 수 있는 다중채널, 다중요소를 포함한 차세대 다중 인증기술의 중요성이 점차 부각됨. 이에 따라, IC카드와 모바일기기 등을 이용하여 위변조 및 복제에 대응하고 동시에 공인인증서를 관리하거나, OTP 생성, 2채널인증, 바이오 인증 등의 인증기술이 개발되어, 일부 기술은 이미 시범서비스가 추진 중
- (금융권) 핀테크(FinTech, Financial과 Technology의 합성어) 활성화 정책과 더불어 기존 전자거래 과정의 최소화 및 간편화 요구 증대와 기술적용에 따라 상대적으로 취약할 수 있는 전자거래 전반의 안정적 서비스를 위해 다중요소 인증기술의 수요는 점차 증가할 것으로 전망

○ **(바이오인식 응용 서비스)** KISA, 한국바이오인식협의회를 중심으로 바이오정보 위변조 탐지기술 및 성능시험 기술개발, 방통위·행자부 등 바이오정보보호 가이드라인 개정작업을 추진중, 삼성전자·LG 전자 등 스마트폰 개발업체를 중심으로 모바일 바이오인식 응용기술을 개발 중

- (방통위, 행자부) 바이오정보 보호정책의 일환으로 바이오정보보호 가이드라인 개정작업 추진과 함께 PKI, 바이오인식을 연동한 융합기술인 PKI 2.0을 보급 중이며, 삼성페이와 같은 스마트폰상의 모바일 지급결제서비스, 인터넷전문은행 등 비대면 인증기술로 활용되는 모바일 바이오인증 서비스가 특히 핀테크 분야에서 더욱 급증할 전망임

- (삼성·LG전자 등 주요 스마트폰 개발업체) 지문·얼굴·홍채·음성인식기술을 탑재한 스마트폰을 출시함과 동시에 스마트폰의 터치스크린에 지문인식센서 탑재 등 박막형 지문인식센서를 활발히 개발 중

- (KISA, 한국바이오인식협의회) 모바일 바이오인식제품의 성능시험기술, 바이오인식 제시형 공격 탐지기술 개발 중

○ **(생체신호기반 텔레바이오 인식기술)** KISA를 중심으로 지문·심전도·심박수 등 생체신호를 이용한 텔레바이오인식기술을 국제공동연구로 개발중이며, 삼성전자·LG 전자 등이 생체신호센서를 개발 중

- (삼성·LG전자 등 웨어러블 개발업체) 일부 대기업을 중심으로 심전도·심박수 등 생체신호센서용 MoC IC칩을 상용화하여 출시하고 있으며, 심박수 측정기능을 갖고있는 스마트밴드, 스마트워치 등의 웨어러블 디바이스 제품화 및 생체신호 인증기술 개발에 박차를 가하고 있는 추세임

- (KISA) 2016년 7월부터 심박수·심전도 등 생체신호를 이용한 텔레바이오인식 인증기술 개발과 관련기술에 대한 ITU-T SG17 국제표준화를 추진하고자 KISA 주관하에 글로벌 프로젝트를 착수하여, 스페인 마드리드대학교와 미국의 Telebiometrics 민간기업 연구소와 국제공동연구를 통하여 심전도·지문 등 다중 생체신호 인증메커니즘, 생체신호센서용 웨어러블 디바이스, 생체신호정보 통신메커니즘 등으로 구성되는 다중 생체신호 인증플랫폼을 개발 중

○ **(바이오인식기반 CCTV보안기술)** KISA, 인하대학교를 중심으로 바이오인식기반의 지능형 CCTV 성능시험 기술개발중

- (KISA, 인하대학교) 지능형 CCTV 영상품질에 대한 성능시험기술, 지능형 CCTV에서의 얼굴영상 획득방법, 지능형 CCTV에서의 개인영상 정보보호지침 등 바이오인식기술을 활용한 지능형 CCTV 보안 응용기술 개발 및 표준화를 추진하여 바이오인식과 지능형 CCTV를 융합한 새로운 물리보안 시장창출이 기대됨

○ **(보안 솔루션 위협정보 공유 및 연동 프레임워크)** ETRI, KISA를 중심으로 보안 정보공유 및 연동 기술 개발 중

- (ETRI) 유관기관간의 보안정보 공유를 통해 전체 공격상황을 직관적으로 파악하고 제어하려는 보안상황 통합보안제어 기술을 개발

- (KISA) KISA를 중심으로 주요 민간 보안업체들이 참여한 위협정보 분석/공유 시스템인 C-TAS(Cyber Threat Analysis System)이 운영 중이며, 표현 규격으로 C-TEX 사용

- (기타) 2016년 6월, 미래부 사이버 위협정보 공유 확대 계획 등 'K-ICT 시큐리티 2020'발표

  · 사이버위협정보 공유에 관한 법적 근거 마련 등 새로운 ICT 환경을 반영한 정보보호 법제도개선을 지속 추진할 계획

○ **(정보보호 관리체계)** 정보보호 관리체계는 정보통신망법에 의해서 정보보호 관리체계 인증이 의무화된 영역과 자율인증 영역으로 나누어져 있음. 정보보호 관리체계(ISMS)가 정부 규제를 중심으로 운영되고 있으나 제도의 중복성 개선과 자발적인 참여에 의한 성숙이 필요함. 2015년 개정된 정보통신망법에 따라 2016년 6월부터 정보보호 관리체계(ISMS)의 의무대상 기관이 상급종합병원과 재학생 수 1만 명 이상인 학교로 확대 적용되었으나, 자발적인 참여 수준이 미흡함. 또한 중소 규모의 조직에 대한 정보보호 수준 개선을 위한 지원 및 활동이 미흡함

- (KISA) 2001년부터 정보보호관리체계(ISMS) 인증제도를 개발하여 시행중에 있으며, 2017.4월 현재 500여개 기관이 인증 받았음

<정보보호 관리체계 인증 및 심사기관 지정 현황>

| 지정시기 | 기관명 | 인증업무의 범위 |
|---|---|---|
| 2014년 4월 | 한국정보통신진흥협회 (KAIT) | 「정보보호관리체계 인증 등에 관한 고시 (과학기술정보통신부고시 제2016-59호)」 제2조에 따른 “인증심사” |
| 2015년 2월 | 한국정보통신기술협회 (TTA) | 「정보보호관리체계 인증 등에 관한 고시 (과학기술정보통신부고시 제2016-59호)」 제2조에 따른 “인증심사” |
| 2015년 7월 | 금융보안원 | 「정보보호관리체계 인증 등에 관한 고시 (과학기술정보통신부고시 제2016-59호)」 제2조에 따른 “인증” 및 “인증심사” |

○ **(개인정보보호 정책 및 운영관리 기술)** 개인정보보호 관리체계(PIMS)와 개인정보보호 인증제(PIPL)는 2016년 1월부터 개인정보보호관리체계(PIMS)로 통합되었으며, 정보보호 관리체계(ISMS)와의 통합도 지속적으로 논의 중에 있음. 개인정보보호 활동은 법률에 근거한 의무 사항을 기준으로 자율에 의한 관리 활동이 이루고지고 있음

○ **(유형별 보안성 시험평가기준)** 국가보안기술연구소를 중심으로 암호모듈 개발 및 CC평가 수행 중

- (국가보안기술연구소 IT보안인증사무국) 정보보호시스템 CC 평가시 CCRA에서 제정한 CC, CEM을 적용하고 있으며, 정보보호제품 유형별 PP를 개발하여 CC평가를 수행 중
- (국가보안기술연구소 KCMVP) 암호모듈 검증시 ISO/IEC JTC1에서 제정한 암호모듈 검증 및 시험기준을 적용하고 있으며, 개발업체는 이 기준을 만족하는 암호모듈을 개발 중. ISO/IEC JTC1에서 제정한 하드웨어 암호모듈 물리적 비침투 공격 방어에 대한 시험기준을 고등급 하드웨어 암호모듈 검증에 적용할 예정

○ **(빅데이터 데이터 보안)** 비식별화 기술을 중심으로 개발 중

- (한국전자통신연구원) 영상 데이터의 비식별화 및 정형 데이터 비식별화 방법에 대한 연구가 진행되고 있고, 광주과학기술원에서 비디오 영상 관제 시스템의 사생활 보호를 위한 비식별화 기술을 개발 중

- (금융보안기술연구원 및 한국인터넷진흥원) 금융정보에 대한 비식별화 가이드라인 개발을 진행하고 있으며, 국제 표준화 대응을 위한 전담반을 동시에 운영 중

○ **(의료보안)** 국내에 85,000여 의료기관에 다양한 직종의 의료종사자들이 활동하고 있으며, 상급종합병원을 중심으로 의료정보시스템과 의료기기들이 사용되고 있으나, 관련된 보안 기술 적용은 일부 대형병원 중심으로만 이루어지고 나머지 대부분은 미 적용 상황

- (보건복지부) 의료법 시행규칙 제16조 개정('16. 2. 5)으로 전자의무기록의 의료기관 내부 또는 외부보관이 가능해지고 보관장소(의료기관 내부 또는 외부)별 시설과 장비에 관한 구체적인 정보보호 관련 세부기준을 마련함에 따라 관련 기술의 개발 보급이 확산 예상
- (과기정통부)정보통신망법 개정에 따라서 의무 대상이 연간 매출액 또는 세입 등이 1,500억 이상인 자 중 대통령령으로 정하는 기준을 해당하는 자로 인증대상을 확대함. 그 중 「의료법」제 3조의 4에 따라 상급 종합병원 43개 모두 정보보호관리체계(ISMS) 인증이 의무화됨
- ISMS 의무 인증 범위 기준은 의료정보시스템과 서비스 제공을 위해 필요한 서버, 네트워크, 시설 등을 반드시 포함해야함. 병원의 경우, EMR 또는 OCS 시스템, 병원 홈페이지 등이 인증범위에 포함됨에 따라 관련 분야에 대한 요소기술 개발 및 서비스 활성화가 이루어질 것임
- (보건산업진흥원) 보건의료정보화추진단을 구성하여 보건의료 정보교류와 이에 따른 보안 가이드라인 개발 및 의료기관·의료종사자 대상 보안인식 교육 강화 등의 사업을 중점적으로 추진하고 있음
- (KISA) 스마트의료기기 취약성 분석 및 보안 가이드라인 개발 작업을 진행하고 있으며, 심전도·뇌파 등 생체신호를 이용한 헬스케어 모니터링 분석을 위한 연구 추진 예정

○ **(제조보안)** '15. 8월에 스마트제조산업협회가 설립되었으며, 이를 통해 산업계 자발적인 표준 개발 및 활용이 촉진될 수 있는 여건을 마련하고, 민관합동 스마트공장추진단과 함께 '스마트공장 공급기업연합'을 구성하여 약 200개의 스마트공장 기술 공급 기업들을 통해서 중소제조기업의 스마트공장화를 추진하고 있으나, 보안 기술을 적용하지 못한 상태에서 보급활동에 주력하고 있는 중임

- (산업통상자원부) 스마트공장 보급확산 사업을 통해서 '16년말까지 2,800여개 중소기업을 대상으로 매칭펀드 방식으로 ICT기술을 접목시켰고, 2022년까지 30,000개 공장을 대상으로 보급 사업을 추진하고 있으나, 보안 기술 및 대책 적용이 시급한 상황임
- (기타) 스마트공장추진단에서 스마트공장 최소보안 가이드라인을 개발하여 보급중에 있음

<국내 주요 사업자 서비스 동향>

| 사업자 | 주요 현황 |
|---|---|
| SKT | - 16년 2월, 국가 양자 암호 시험망 서비스 개시 |
| 윈스 | - 국내 IPS 네트워크 보안 분야의 1위 업체로 자체 CERT 조직을 보유하고 있으며, 지속적인 위협정보를 수집/분석/대응 체계를 가짐<br>- 자사 및 타사의 보안제품을 통합 관리하는 제품(TMS-Plus) 보유 |
| 비트컴퓨터 | - 의료정보시스템, 의료영상처리시스템 등을 개발하여 공급 중 |
| 인성정보 | - 의료정보시스템 등을 개발하여 공급 중 |
| 삼성메디슨 | - 초음파 의료기기 개발하여 국내외 시판 중 |
| 인피니트 | - CT, MRI 의료기기 등 개발하여 국내외 시판 중 |
| 광림 | - 위 내시경, 수술용 내시경 등 장비 개발하여 시판 중 |
| LS산전 | - PLC 제품 약 33%의 국내 시장 점유율 확보 |
| ㈜ACS | - 현대기아자동차, 포스코 등 국내외 1,200여 업체에 관련 솔루션을 시스템 통합 형태로 구축<br>- 자동차 부품 제조업 및 전기전자 부품 제조업 분야에 적합한 공통 팩키지 기능을 ANSI S-95, IEC 62264와 미국 MESA (Manufacturing Enterprise Solution Associates) 모델에서 제시하는 표준 기능으로 개발 |
| ㈜유노믹 | - 2011년부터 국내 공작기계 제조사와 함께 모바일 기반의 공작기계 제어 소프트웨어를 개발<br>- 2013년부터 북미 표준 제조 기술규격인 MTConnect 및 OPC UA를 중심으로 공작기계 모니터링 시스템을 개발<br>- 50여가지 제조 공정 모니터링 및 제어를 위한 소프트웨어를 제공 |
| ㈜엔엔에스피 | - 산업제어시스템 보안기술, 스마트 그리드 보안기술 등을 개발하는 회사<br>- KC, GS, CC 인증 등을 획득한 하드웨어 기반의 물리적 단방향 보안 게이트웨이, 산업용 네트워크 포트 이중화 장비 등을 자체 개발하여 국내외 판매 |
| 펜타시큐리티 | - 펜타 스마트 팩토리 시큐리티(Penta Smart Factory Security) 솔루션을 적용, 스마트공장 운영 과정에서 발생할 수 있는 보안 위협을 최소화<br>- 데이터 수집부터 모니터링, 프로세스 제어까지 가능하도록 안전한 스마트팩토리 환경 구축 |

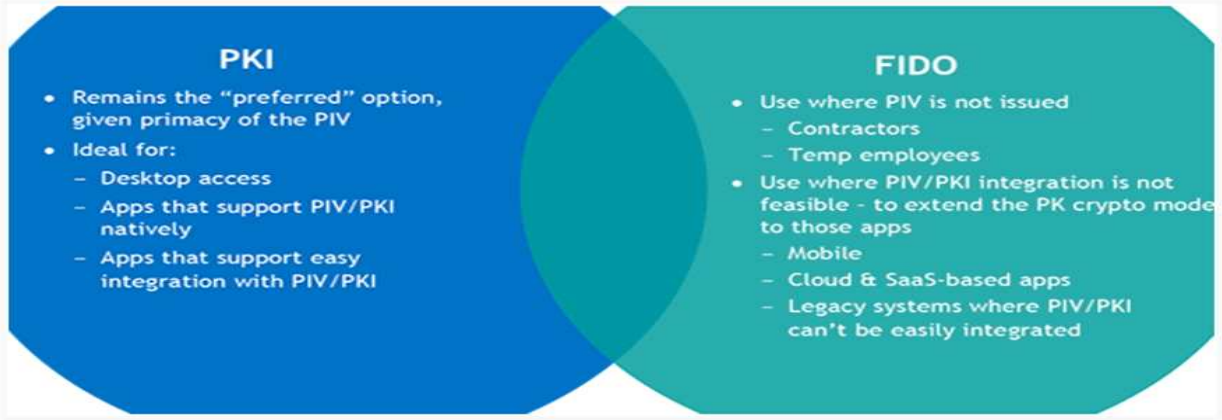
### 2.4.2. 국외 기술개발 현황 및 전망

○ **(차세대 암호기술)** 미국과 유럽은 각각 국가 기관과 학계를 중심으로 차세대 암호 알고리즘의 개발 및 국제표준화를 통한 시장 주도권 선점을 추진 중

- (미국 NSA) 경량 환경을 위한 블록 암호 SIMON/SPECK을 개발함
- (스위스 STMicroelectronics) 미국 NIST가 연방정부 사용을 승인(NIST FIPS 202)한 SHA-3 해시 함수 Keccak을 개발함
- (미국 HPE Security) 미국 NIST가 연방정부 사용을 승인(NIST SP 800-38G)한 형태보존 블록 암호 운영 모드 FFX를 개발함
- (벨기에 COSIC) 경량 메시지 인증 코드 알고리즘 Chaskey와 LightMAC을 개발함
- (미국 IBM, Microsoft 등) 다수의 (완전) 동형 암호 알고리즘을 개발하고 의료 분야 등 다양한 응용서비스 적용 기술을 개발 중
- (스위스 IDQ, 미국 MagicQ, 중국 QuantumCTek 등) 시험용 양자 키 분배 장치 판매 중
  · 중국은 세계 최초 양자통신 실험위성을 쏘아 올린데 이어 1,200km 통신에 성공함
  · 일본은 중국에 이어 두 번째로 우주-지상 양자 키 분배에 성공함

○ **(PKI 기반 인증 및 응용기술)** 바이오인증 표준인 FIDO 2.0이 출시 예정이고 PDF 및 클라우드 환경에서의 인증 기술이 적용되고 있으며, 자율주행관련 PKI기반 인증이 미국, 유럽 등에서 실증 프로젝트가 진행 중

- (FIDO Alliance) FIDO기술의 플랫폼을 PC영역으로 확대한 FIDO2.0 표준화가 진행 중이고 W3C에서 Web API관련 표준화도 진행 중이고 이 표준이 확정되면 Microsoft, Google 등의 브라우저 업체가 반영하여 제공 예정
- (구글, 페이스북, 인스타그램 등) 2FA(2nd Factor Authentication)을 지원하고 있음. 또한 유럽은행당국 (European Banking Authority)에서 새로운 결제표준으로 2FA를 권고하고 있으며 PSD2 (Payment Services Directive) Regulation에서 모바일 바이오인증 솔루션을 요구함으로써 이를 반영한 결제서비스 지침이 2018년부터 시행될 예정으로 FIDO 표준의 영향력이 증가할 것으로 예상
- (전자문서 업체) 전자문서형식인 PDF에 대한 전자서명 기술로 어도비사의 echoSign, 구글의 DocuSign, 헬로사인의 HelloSign 등이 서비스 중
- (Connected Car 실증)미국, 유럽 등에서 PKI 기반의 자율주행 등 다양한 연구 및 실증이 추진 중
- (FIDO) FIDO 차원에서 최근 FIDO 기술과 PIV(Personal Identity Verification)간 효과적인 통합 가능한 모델을 제안하고 있음. PIV에서 New derived credentials이 카드리더기 없이 네트워크를 통해 Challenge가 이뤄질 수 있으나, 이 경우 어떤 application이나 서비스는 PKI가 enable되어야 함. 이를 효과적으로 대신할 Light FIDO asymmetric key pair가 모바일 디바이스상에서의 다양하고 많은 application단에서 인증에 활용이 가능해질 것으로 기대. 이는 기존 PIV에 FIDO를 통합시 강한 인증체계를 갖출 수 있음을 보여주는 예가 될 수 있음




<FIDO표준과 PKI 보안모델 간 Leverage>

- (FIDO) 미국NIST의 CSF (CyberSecurity Frame), 유럽의 PSD2 (EU의 Payment와 digital Banking을 규정)와 eIDAS (EU의 새로운 전자서명 규정), 아시아의 APKIC(아시아 PKI 컨소시엄)등과 글로벌표준 및 협업전개 중

- (두바이 공항) 바이오인식기술을 활용하여 여객들을 스크리닝할 계획으로 일명 'Gate-less border'을 구현할 준비를 갖추고 있음. 또한 최근 Biometric airport screening은 미국 공항의 TSA나 CBP (Customs & Border Protection) 같은 정부산하기관들 지원하에 추진중임 (미국 애틀란타공항, 덴버공항)

○ **(범용인증기술)** OATH와 FIDO Alliance에서 발표된 표준을 기반으로 정부차원 및 기업차원에서 통합인증 체계를 개발 및 서비스 중

- (OATH) VeriSign, Entrust, Gemalto 등 다양한 보안업체의 연합인 OATH(Open AuTHentication)는 모든 네트워크, 디바이스, 사용자에게 적용 가능한 범용 강화 인증 아키텍처를 제공

- (FIDO) ARM社, Bank of America, Google, PayPal, RSA社, 삼성SDS 등의 연합인 FIDO(Fast IDentity Online) Alliance는 클라이언트 인증 수단과 원격인증 프로토콜을 분리함으로써 서버 변경 없이 다양한 인증 수단의 활용이 가능한 개발한 범용인증서비스 프레임워크를 개발. 현재는 W3C를 통해 웹브라우저에 기본 탑재를 추진 중으로, 급격한 서비스 활성화가 예상(IBM)

- (OAuth) OpenAPI로 개발된 표준 인증 방식으로, 사용자가 접근 허가 인증이나 자신의 전체 데이터를 공유하지 않은 상태에서도 다른 서비스 제공업체에 저장된 자신의 정보에 대한 제3사이트 접근이 가능하도록 함. Google과 Facebook, Naver 등 메이저 서비스 제공자가 활발하게 활용 중

- (Apple) 2014년 NFC와 지문인식 기술에 보안칩을 이용하여 사용자의 지문정보와 카드정보를 관리하는 스마트카드 기반의 결제시스템인 애플페이를 출시하여 미국에서 빠르게 사용자를 확보 중

- (Gemalto) 다양한 인증 수단 및 디바이스 호환, 컨텍스트 주도 ID 관리, 하드웨어 기반의 보안 플랫폼, 클라우드 구축을 지원하는 SafeNet 인증 솔루션을 개발

- (NIST) 전자인증 가이드라인(SP 800-63-1)은 4 레벨의 인증 보증 레벨에 대해 기술적인 요구사항(인증 토큰, 토큰 및 인증정보의 관리 메커니즘, 인증 메커니즘 프로토콜, 원격인증 결과 보증 메커니즘)을 명세

- (싱가포르/노르웨이) 국가인증체계(NAF, National Authentication Framework)를 통해 전 국민을 대상으로 공공·금융·민간을 통합하는 인증서비스를 제공하고 있으며, 노르웨이는 BankID를 통해 금융권역의 범용 인증서비스를 제공 중

- (미국/싱가포르/유럽) 미국, 싱가포르 등에서는 고위험거래 시 멀티팩터 인증의 사용을 적극 권고하고 있으며, 영국을 중심으로 유럽 전반에서는 EMV의 CAP을 지원하는 IC카드 단말기를 통해 일회용 비밀번호를 생성하는 등 다중요소 인증기술이 널리 이용되고 있으며, 독일 일부 은행에서는 IC카드가 내장된 전용 단말기로 PKI 방식의 전자서명을 생성하는 기술이 사용 중

- (미국) 2012년부터 시작된 미국의 NSTIC 프로젝트는 온라인 거래의 안전성을 높이기 위해 소비자가 인터넷 거래를 할 때 사용할 수 있는 인증 ID(인터넷 신분증)를 제공하기 위하여 매년 700만 달러 규모의 파일럿 프로젝트를 수행

○ **(바이오인식 응용 서비스)** 미국 NIST, 유엔난민기구 등에서는 스마트카드에 바이오정보를 탑재한 ID카드를 개발보급중이며, 미국 애플社, 일본 NTT 등 스마트폰에서 박막형 지문인식센서를 개발하고 미국 NIST, 유럽 등에서는 바이오인식 제시형 공격 탐지기술을 개발 중

- (미국 NIST, UN 난민기구) 스마트카드와 연동기술인 바이오인식기반의 MOC(Match-On-Card) 카드형태의 미국 연방정부의 PIV 카드, 유엔 지문스마트카드·난민식별카드 등 상용제품이 널리 보급되고 있으며, 인터넷전문은행, ATM 기기, 스마트폰 등 바이오인식 기반의 비대면 인증기술이 핀테크 분야에서 특히 널리 보급되고 있음

- (미국의 애플사, 일본 NTT 도코모사 등 주요 스마트폰 개발업체) 지문·얼굴·정맥·음성인식기술을 탑재한 스마트폰을 출시함과 동시에 스마트폰의 터치스크린에 지문인식센서 탑재 등 박막형 지문인식센서를 활발히 개발 중

- (미국 NIST, 유럽 핀테크 금융업체) 특히 독일 CCC 해커스그룹에서 스마트폰에 탑재된 지문·홍채인식에 대한 위변조 해킹시도가 있었으며, 지난 2016년 12월, JTC1 SC37에서 미국 NIST가 개발하여 ISO/IEC 30107 국제표준(Biometric Presentation Attack Detection, PAD)으로 제정됨에 따라, 미국·유럽 등 주요 선진국 금융권에서는 비대면 본인확인에 활용되는 바이오인식제품을 도입시에 PAD 국제표준 적합성 시험인증기술을 활발히 개발중에 있으며 시험·인증서비스에 대한 법제도 정비를 서두르고 있는 추세임

○ **(생체신호기반 텔레바이오 인식기술)** 미국 TI社, 워싱턴 대학교 등에서는 생체신호센서 및 뇌파 인증기술을 개발 중이며, 영국 및 캐나다 주요은행에서는 생체신호를 이용한 인증서비스 기술개발 중

- (미국 TI社, 미국 워싱턴대학교) 뇌파·심전도·심박수·근전도 등 생체신호 측정용 의료장비 및 웨어러블 디바이스, 생체신호센서용 MoC IC칩 등 미국 TI(Texas Instrument)사를 중심으로 활발히 제품화가 진행중에 있으며, 미국의 워싱턴 대학 등 대학교를 중심으로 뇌파·심전도·심박수 등 생체신호 개인식별기술에 대한 연구가 활발히 진행중에 있음
- (영국 Halipax 은행, 캐나다 Bionym社) 영국의 Halipax 은행, 캐나다 왕립은행 등 주요선진국 금융권에서는 시범사업으로 캐나다 Bionym社rk 개발한 심박수 측정용 웨어러블 디바이스를 통하여 생체신호를 이용한 고객통장의 개인식별서비스를 시행 중

○ **(바이오인식기반 CCTV보안기술)** 영국 South Hampton 대학교를 중심으로 바이오인식기반 지능형 CCTV 융합기술을 개발 중

- (영국 내무부) 영국을 중심으로 ISO/IEC JTC1 SC37에서는 지능형 CCTV에서의 바이오인식 적용방안(파트1: 설계 및 사양, 파트2: 성능시험방법론)에 대한 국제표준을 개발중에 있음
- (영국 South Hampton대학교) 영국 South Hampton 대학교 등 주요 선진국 대학교에서는 걸음걸이·얼굴인식 등 다양한 다중 바이오인식기술과 결합한 지능형 CCTV 응용기술에 대한 제품화에 박차를 가하고 있는 추세임

○ **(보안 솔루션 위협정보 공유 및 연동 프레임워크)** 미국 MITRE와 일본 NICT는 네트워크 전체를 보안 제어 영역으로 확장하여 서로 다른 기관간의 보안정보 공유를 통한 협력기반의 연동 프레임워크 기술에 대한 연구를 활발히 진행 중

- (미국) 미국 국토안보부는 MITRE 프로젝트에서 개발된 사이버 위협정보를 공유하는 자동화된 표준 운용기술 결과물을 오픈소스로 발표함(Cybox, STIX, TAXII)
  - · 미국은 사이버 위협 정보의 개념을 표준화하고 구조화하여 사이버 위협에 대한 일관된 분석과 자동화된 해석이 가능하게 하는 정보 표현 규격을 제정하고, 정보공유체계의 핵심요소인 STIX는 8 가지 구성요소 (Observable, Indicator, Incident, TTP, ThreatActor, Campaign, ExploitTarget, COA)로 사이버 위협정보를 구조화 함
  - · 2016년 3월, 마이크로소프트(MS)가 미국내에 사이버보안센터 구축완료, 사이버위협 및 분석 정보를 정부와 공유하는 민관협력 창구로 활용할 계획
- (일본) 일본의 IPA(일본 정보보안관련 전문기관)는 사이버 공격에 대한 대응을 위해 5대 산업, 45개 참여기업의 정보공유 체계인 J-CSIP(Initiative for Cyber Security Information sharing Partnership of Japan)를 2011.10.25부터 발족하여 운영
- (유럽) 유럽에서도 '주요 정보 기반 시설 보호(CIIP)' 협력을 통해 사이버 보안에 관련된 14개의 법을 시행함으로써, EU 차원에서 각국의 ICT 인프라를 보호하기 위한 대비책 및 회복 역량을 확보하는 등 보안 수준을 강화

○ **(유형별 보안성 시험평가기준)** CCRA와 JTC1 중심으로 유형별 보안성 시험평가 개발 중

- (CCRA) ICT 기술 환경의 변화에 따라 평가 기술 개선과 IT제품의 보안성 평가시 cPP 적용 등 평가기준 변경에 대한 CC 및 CEM 개정을 추진하고 있으며, 본 개정작업에 국가보안기술연구소 IT보안인증사무국이 주도적으로 참여
- (ISO/IEC JTC1) CCRA와 협력하여 보안성 평가기준과 평가방법론을 개정하고 있으며, 국가보안기술연구소와 한국의 KCCUF 전문가들이 주도적으로 참여하고 있음.
- (ISO/IEC JTC1) 암호모듈 검증 및 시험기준을 국가보안기술연구소 KCMVP 주도적 참여로 2015년 개정하였으며 클라우드 서비스, 사물인터넷(IoT), 스마트 기기 등 신규 ICT 환경 변경에 따른 추가 개정이 예정
- I(SO/IEC JTC1) 암호모듈 공격기술 발달에 따라 암호모듈 물리적 비침투 공격 방어에 대한 시험기준을 2015년 개정하였고 고등급 하드웨어 암호모듈 검증시 적용될 예정

○ **(정보보호 관리체계)** ISO27001을 기반으로 개발되어 오던 정보보호 관리체계에 대한 표준이 2013년 ISO/IEC 27001:2013과 ISO/IEC 27002:2013으로 재개정 됨에 따라, 국내 정보보호 관리체계에 대한 국제 표준과의 호환성 논의와 검토가 활발해 진행되고 있음

- (금융, 통신, 클라우드, 에너지, 의료분야등) 정보보호 경영시스템(ISO27001)은 ISO27009를 기반으로 산업분야별로 금융, 통신, 클라우드, 에너지, 의료분야에 대한 보안 통제 항목 및 구현가이드 등이 정립되고 있음
- (중소기업 정보보호 관리체계) 기존의 정보보호 관리체계의 요구사항 및 통제 항목이 규모에 의존적이지 않도록 구성되어 있음에도 불구하고 정보보호 관리체계는 투자와 관심의 여력이 있는 조직에 한해 운영되고 있으며, 중소 조직의 정보보호 활동을 지원하기 위한 가이드라인의 국제 표준이 개발되고 있음. 특히 통신분야에 있어 ITU-T SG17을 중심으로 중소 규모의 통신 조직 환경과 운영의 특성을 반영한 중소 조직을 위한 정보보호 관리활동 기준 가이드라인 표준(X.Sgsm)이 개발되고 있으며, 2017년 하반기에 최종 승인 될 예정에 있음

○ **(개인정보보호 정책 및 운영관리 기술)** 개인정보보호 관리체계에 대한 표준이 2017년 ISO/IEC 29151의 개인정보보호대책 지침과 ITU-T에서 통신조직의 개인정보 관리가이드 X.1058로 공동 개발 승인이 이루어졌으며, 개인정보보호 가이드에 대한 활용을 지원하기 위한 부속서 등의 개발이 추가적으로 진행되고 있음. 개인정보보호 관리체계에 대한 프로세스를 마련하기 위해 ISO/IEC 29522 개발이 진행되고 있음

○ **(빅데이터 데이터 보안)** 빅데이터 데이터 보안 분야는 데이터의 내용 분석에 따른 개인정보 유출 및 침해에 대한 연구가 진행되고 있음

- (ISO/IEC) ISO/IEC WD 20889 비식별 기술 표준 - ISO/IEC 29100(Privacy Framework)에서 프라이버시 강화를 위한 방법으로 비식별 기술을 제시하고 있음. 개별화, 연결 가능성, 추론 가능성 분별 가능성에 따른 위험을 분류
  - 비식별화 기술로는 마스킹, 가명화, K-익명성, l-다양성, t-유사성, 샘플링 총계 등의 다양한 비식별 기술이 연계되어 있어, 각각을 비교하고 있음
- (미국 NIST) 미국 상무부 산하의 표준화 기구인 NIST에서 20년간의 비식별화에 대한 논의를 정리하여 "개인 식별 정보의 비식별 처리"에 대한 가이드를 발표 (2015년 10월)
  - 2016년 12월 "공공데이터에 대한 비식별 처리" 가이드를 추가로 발간하고, 공공정보 분야에서의 비식별화에 대한 연구를 진행하고 있음
  - 2012년부터 5년간 20여명의 보안 전문가들이 참여하여 비식별 처리를 위한 방법을 논의하고 그결과를 집대성한 보고서
  - 비식별 방법을 정형 비식별화, 보장형 비식별화, 통계적 비식별화, 기능적 비식별화의 4가지로 분류하였고, 비식별 처리에 따른 위험과 정보 유용성 관점에서 정리함

○ **(의료보안)** '17년초부터 의료기기에 대한 보안 취약성이 집중적으로 거론되고 있고 사이버공격과 해커들에 의한 공격이 증가하고 의료기관을 대상으로 한 랜섬웨어 공격 등이 활발해짐에 따라서, 유럽 주요 국가들과 특히 미국 FDA를 중심으로 의료정보시스템과 의료기기들에 대한 보안 표준화 작업이 활발히 전개되고 있음

○ **(제조 보안)** 독일에서 제조업 기반으로 플랫폼 인더스트리 4.0을 전개하면서 국제표준화 작업을 리드해 가고 있으며, 미국, 일본 등이 이에 앞서 가고자 경쟁적으로 작업을 진행하고 있으나, 보안 분야에 대한 투자는 세계적인 다국적 기업을 제외하고 거의 적용되지 못하고 있음

- (독일) 독일의 인더스트리 4.0은 2011년 11월에 독일연방정부의 "미래 프로젝트" 가운데 하나로 추진 중인 하이테크 전략 2020 실행 계획(Action Plan)의 일환으로 추진, 독일의 제조업 경쟁력 향상을 위한 인더스트리 4.0 추진 전략을 참조하여 산업통상자원부에서는 2015년 3월에 제조업 혁신 3.0 전략을 수립하여 대응하면서 스마트공장 및 스마트제조에 대한 기술개발, 보급·확산, 인력양성, 표준화 등의 활동을 본격적으로 전개
- (미국) 상무부 산하 NIST 와 국토안보부 산하 ICS CERT를 중심으로 산업제어시스템, SCADA 등에 대한 보안 취약점을 찾아서 대책을 마련하고 관련된 정보들을 제공하고 있음
- 산업 제어시스템 계통설비의 시스템 및 네트워크에 대한 프로파일링 및 제어 프로세스의 미반영으로 수동적으로 공격 위협을 탐지하는 수준

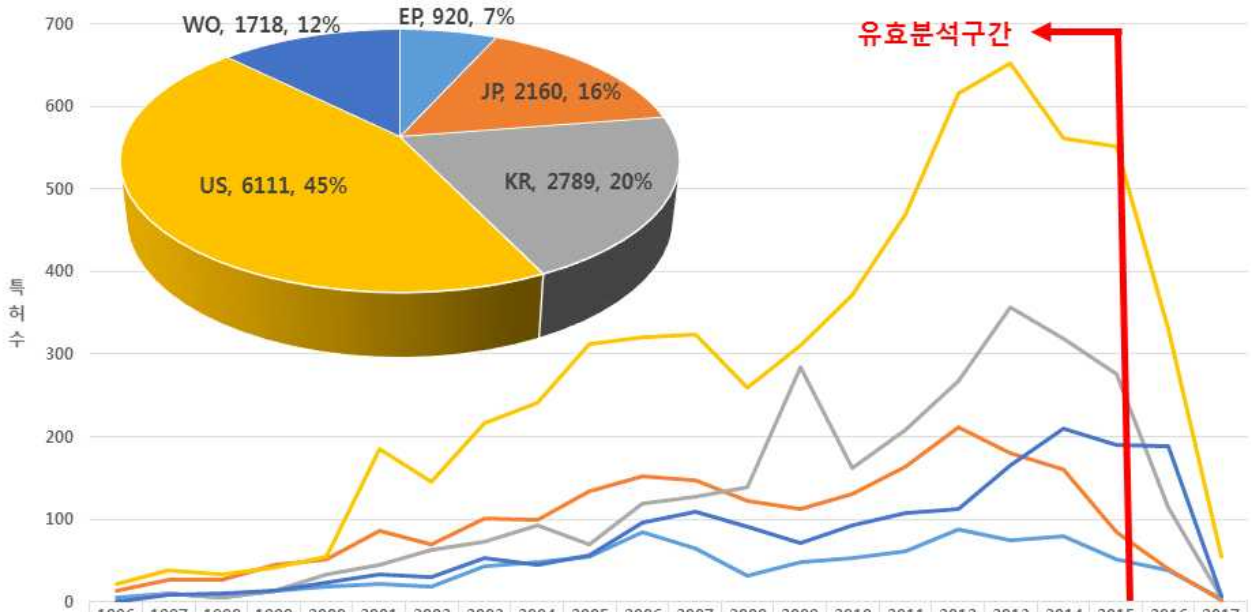
- 의도적인 침해사고를 방지하기 위하여 제어프로세스 트랜잭션 추적기반의 능동적 공격 위협 탐지 기술에 대한 연구개발이 필요할 것으로 예상
- 신뢰성 보장을 위한 업무 프로세스별 보안 모니터링을 위해 설비장비의 시스템 및 네트워크 상태 분석에 대한 연구개발이 필요할 것으로 예상
- 산업 제어시스템 보안제품 수요 및 추가 기술개발의 요구 증가
- 도입기에 있는 산업 제어시스템 보안 기술은 침해사례 발생으로 제품 수요가 급격하게 증가하고 있으며, 이에 따른 추가적인 기술개발의 요구가 증가하고 있어 기술의 성숙정도는 당분간 급격한 성장의 추세를 보일 것으로 전망
- 9·11 테러 이후, 미국의 경우에는 주요 기반시설에서의 보안성 강화에 지속적으로 관심이 높아지고 있으며, 특히 세계 산업 제어시스템 제조업체들이 직면하는 중요한 도전은 사이버 보안 위험에 대처하는 것이며, 전 세계적으로 사이버보안을 강화하기 위한 인증제도 부상
- ISCI(ISA Security Compliance Institute)의 SCADA 보안 검사에 대한 공식화와 ISA99 WG4에서 정한 표준은 이전의 산업 검사와 인증 제도를 대체할 것으로 예상
- SCADA 시스템에서 통신프로토콜로 주로 사용되고 있는 Modbus와 DNP3는 암호와 인증/인가 기능을 추가한 프로토콜 상의 보안을 고려하였으나, 가용성 관점의 서비스거부 공격에 대한 보안사항은 고려하지 않고 있음
- 최근 공격목표와 공격 형태를 기준으로 제어시스템 표준 프로토콜(DNP3, Modbus) 환경에서 발생하는 공격을 분류하고, 이에 대한 방어를 위해 연구 진행

## 2.5. IPR 현황 및 전망

○ 특허분석 개요

- 차세대 보안 분야에 있어서, 2017년 8월 현재까지 한국, 미국, 일본, 유럽, 국제 공개(등록)된 특허들을 대상으로 앞서 제시된 표준화 항목에 따라 검색/추출된 총 13,698건의 특허를 대상으로 분석을 수행함

○ 특허 출원년도별 특허공보별 동향




| | 1996 | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| EP | 5 | 10 | 5 | 14 | 19 | 22 | 19 | 44 | 49 | 55 | 84 | 64 | 32 | 48 | 53 | 61 | 88 | 74 | 80 | 51 | 39 | 4 |
| JP | 13 | 26 | 26 | 45 | 51 | 86 | 69 | 101 | 99 | 134 | 153 | 148 | 123 | 113 | 130 | 163 | 212 | 181 | 161 | 84 | 40 | 2 |
| KR | 1 | 10 | 6 | 14 | 33 | 45 | 63 | 73 | 93 | 69 | 119 | 128 | 139 | 285 | 162 | 209 | 267 | 357 | 319 | 276 | 115 | 6 |
| US | 21 | 38 | 34 | 41 | 55 | 185 | 145 | 217 | 241 | 312 | 320 | 324 | 259 | 310 | 371 | 469 | 616 | 653 | 562 | 552 | 331 | 55 |
| WO | 1 | 8 | 10 | 13 | 23 | 33 | 30 | 54 | 45 | 57 | 96 | 110 | 91 | 72 | 92 | 108 | 113 | 166 | 210 | 191 | 188 | 7 |

* 특허 분석구간(1996년~2017년) : 출원일 기준으로 분석하며, 일반적으로 특허출원 후 18개월이 경과된 때에 출원관련정보를 대중에게 공개하고 있음. 따라서 아직 미공개 상태의 데이터가 존재하는 2016년 이후 자료의 경우 미공개분이 존재함을 고려해야함

- 연도별 출원 동향을 살펴보면, 2000년대 중반까지 꾸준한 증가세를 유지하다가 2000년대 후반부터 다소 큰 폭의 증가세를 보이고 있으며, 특히 미국(US), 한국(KR), 국제(WO) 특허들의 출원양이 늘어나고 있는 것으로 나타남
- 한국(KR)을 비롯하여 미국(US), 국제(WO) 특허 출원양이 최근(2013년, 2014년)에 가장 많은 것으로 보아 차세대 보안 기술 분야에 대한 관심도가 높고 연구개발이 활발한 것으로 판단됨
- 국적별로는 미국(US) 특허가 6111건(45%)으로 가장 많은 출원양을 나타내고 있으며, 한국(KR)이 2789건(20%)으로 그 뒤를 잇고 있음
- 의료, 제조를 비롯한 다양한 분야에서 보안에 대한 중요성이 커지고, 바이오 인식 등을 통한 차세대 보안 기술이 개발됨에 따라 특허 출원이 지속적으로 증가할 것으로 예상됨

○ 각 표준화 항목에 대한 연도별 출원 동향

| 표준화 항목 / 출원 년도 | PKI 기반 인증 | 바이오 인식 | 범용 인증 기술 | 보안 관리 평가 | 보안정보 공유 및 연동 | 빅데이터 보안 | 의료 보안 | 제조 보안 | 차세대 암호 기술 |
|---|---|---|---|---|---|---|---|---|---|
| 1996 | 2 | 1 | 9 | 0 | 0 | 0 | 13 | 1 | 15 |
| 1997 | 15 | 0 | 16 | 2 | 0 | 0 | 25 | 11 | 23 |
| 1998 | 10 | 0 | 22 | 0 | 1 | 1 | 21 | 5 | 21 |
| 1999 | 24 | 5 | 29 | 2 | 3 | 2 | 26 | 4 | 32 |
| 2000 | 28 | 10 | 45 | 3 | 2 | 1 | 53 | 20 | 19 |
| 2001 | 55 | 13 | 67 | 8 | 3 | 0 | 152 | 17 | 56 |
| 2002 | 59 | 13 | 69 | 7 | 5 | 5 | 90 | 28 | 50 |
| 2003 | 69 | 21 | 126 | 11 | 9 | 8 | 133 | 32 | 80 |
| 2004 | 108 | 25 | 93 | 19 | 8 | 7 | 126 | 41 | 100 |
| 2005 | 106 | 32 | 129 | 7 | 5 | 3 | 149 | 61 | 135 |
| 2006 | 138 | 26 | 197 | 16 | 2 | 8 | 166 | 83 | 136 |
| 2007 | 165 | 42 | 218 | 16 | 6 | 2 | 156 | 58 | 111 |
| 2008 | 130 | 57 | 176 | 18 | 3 | 5 | 126 | 49 | 80 |
| 2009 | 107 | 93 | 318 | 10 | 3 | 5 | 135 | 45 | 112 |
| 2010 | 141 | 92 | 219 | 12 | 4 | 7 | 174 | 45 | 114 |
| 2011 | 174 | 126 | 322 | 19 | 6 | 13 | 208 | 41 | 101 |
| 2012 | 192 | 241 | 351 | 20 | 3 | 29 | 282 | 58 | 120 |
| 2013 | 174 | 254 | 395 | 37 | 1 | 49 | 330 | 72 | 119 |
| 2014 | 173 | 236 | 369 | 33 | 2 | 36 | 255 | 88 | 140 |
| 2015 | 153 | 181 | 264 | 30 | 2 | 62 | 214 | 103 | 145 |
| 2016 | 85 | 90 | 85 | 24 | 6 | 38 | 203 | 66 | 116 |
| 2017 | 11 | 11 | 9 | 3 | 0 | 12 | 15 | 7 | 6 |
| 합계 | 2119 | 1569 | 3528 | 297 | 74 | 293 | 3052 | 935 | 1831 |

- 차세대 보안 분야의 특허출원은 2000년대 들어서서 출원양이 증가하고 있으며, 특히 PKI 기반인증, 바이오인식, 범용인증기술, 의료보안, 제조보안 등에 대한 출원양이 다소 큰 폭으로 증가하는 것으로 보아 해당 기술에 대한 관심도가 높은 것으로 판단됨

○ 각 표준화 항목에 대한 특허공보별 출원 동향

| 표준화 항목 / 출원 국가 | PKI 기반 인증 | 바이오 인식 | 범용 인증 기술 | 보안 관리 평가 | 보안 정보 공유 및 연동 | 빅데이터 보안 | 의료 보안 | 제조 보안 | 차세대 암호 기술 | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| 한국특허 | 431 | 444 | 1059 | 104 | 5 | 64 | 345 | 135 | 202 | 2789 |
| 미국특허 | 509 | 735 | 1283 | 108 | 52 | 161 | 2063 | 454 | 746 | 6111 |
| 일본특허 | 782 | 236 | 220 | 41 | 1 | 22 | 376 | 49 | 433 | 2160 |
| 유럽특허 | 143 | 42 | 260 | 8 | 5 | 15 | 103 | 165 | 179 | 920 |
| 국제특허 | 254 | 112 | 706 | 36 | 11 | 31 | 165 | 132 | 271 | 1718 |

- 범용인증기술 및 차세대 암호기술에 대한 출원은 각 국별 공통적으로 많은 출원이 이루어지고 있으며, 일본의 경우 PKI 기반 인증 및 의료보안, 유럽은 제조보안, 한국은 바이오인식 분야에 대한 특허출원이 활발한 것으로 나타남
- 어느 한 분야의 표준화 항목에 치우치지 않고 모든 표준화 항목에서 고른 분포를 보임

○ 한국특허에서의 주요 출원인별 출원 현황 (KR)

| 표준화 항목 / 출원인 | PKI 기반 인증 | 바이오 인식 | 범용 인증 기술 | 보안 관리 평가 | 보안 정보 공유 및 연동 | 빅데이터 보안 | 의료 보안 | 제조 보안 | 차세대 암호 기술 | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| 비즈모델라인 | 15 | 40 | 179 | 0 | 0 | 1 | 1 | 0 | 0 | 236 |
| ETRI | 24 | 10 | 53 | 10 | 2 | 3 | 4 | 4 | 41 | 151 |
| 삼성전자 | 26 | 22 | 16 | 2 | 0 | 2 | 17 | 2 | 13 | 100 |
| KT | 21 | 3 | 37 | 3 | 0 | 1 | 5 | 2 | 1 | 73 |
| SK텔레콤 | 11 | 1 | 10 | 5 | 1 | 0 | 6 | 0 | 14 | 48 |
| Qualcomm | 15 | 7 | 3 | 0 | 0 | 0 | 2 | 1 | 3 | 31 |
| LG전자 | 13 | 13 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 29 |
| 고려대학교 | 10 | 1 | 6 | 0 | 0 | 0 | 1 | 0 | 9 | 27 |
| 경북대학교 | 2 | 3 | 2 | 0 | 0 | 1 | 17 | 1 | 1 | 27 |
| SK플래닛 | 3 | 1 | 18 | 1 | 0 | 0 | 2 | 0 | 0 | 25 |

- 한국특허 다수 출원인은 비즈모델라인, ETRI, 삼성전자, KT, SK텔레콤 등의 순임
- Qualcomm, Intel, Microsoft, SONY, Thomson Licensing, Panasonic(Matsushita Electric), Apple, Interdigital, Mitsubishi electric, Philips 등의 외국기업이 한국에 출원하고 있음

○ 해외특허에서의 주요 출원인별 출원 현황 (US, JP, EP, WO 모두 포함)

| 표준화 항목 / 출원인 | PKI 기반 인증 | 바이오 인식 | 범용 인증 기술 | 보안 관리 평가 | 보안 정보 공유 및 연동 | 빅데이터 보안 | 의료 보안 | 제조 보안 | 차세대 암호 기술 | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| NEC | 66 | 13 | 24 | 2 | 0 | 3 | 14 | 1 | 142 | 265 |
| Rcokwell Automation | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 234 | 0 | 238 |
| IBM | 20 | 5 | 90 | 2 | 0 | 3 | 34 | 1 | 35 | 190 |
| TOSHIBA | 45 | 5 | 7 | 2 | 1 | 0 | 53 | 0 | 56 | 169 |
| Microsoft | 22 | 19 | 76 | 3 | 4 | 3 | 13 | 0 | 26 | 166 |
| NTT | 75 | 9 | 14 | 1 | 0 | 0 | 7 | 0 | 54 | 160 |
| SONY | 89 | 13 | 8 | 0 | 0 | 3 | 8 | 0 | 28 | 149 |
| FUJITSU | 56 | 18 | 12 | 2 | 2 | 0 | 8 | 0 | 43 | 141 |
| 삼성전자 | 36 | 17 | 38 | 0 | 0 | 1 | 24 | 3 | 20 | 139 |
| Qualcomm | 64 | 34 | 21 | 0 | 0 | 0 | 6 | 4 | 6 | 135 |

- 해외특허 다수 출원인은 NEC, Rockwell Automation, IBM, Toshiba, Microsoft 등의 순이며, 주로 일본 국적의 기업들이 다출원인 상위권에 많은 비중을 차지하고 있는 것으로 나타남
- 주요 출원인들은 주로 통신, 전자제품, 소프트웨어 등에 관련된 기업이며, 특히 PKI 기반 인증 및 차세대암호기술에 집중하여 특허를 출원 하고 있는 것으로 나타남
- 삼성전자는 해외에도 활발한 특허출원을 하고 있으며, ETRI, SK텔레콤, LG전자, SK플래닛, 삼성SDS 등과 같은 한국기업이 해외에도 출원하고 있음

## 2.6. 표준화 현황 및 전망

| 표준화 수준 | | | 표준화 격차/특성 | |
|---|---|---|---|---|
| | 국내 | □기획↦□항목승인↦□개발/검토↦■최종검토↦□제/개정 | | 1년 |
| | 국제 | □기획↦□항목승인↦□개발/검토↦□최종검토↦■제/개정 | | 후행 |
| * 표준화 특성: 선행(선표준화 후기술개발) - 병행(표준화 & 기술개발 동시추진) - 후행(선기술개발 후표준화) | | | | |

| 구분 | 표준화 기구 | | 표준화 현황 |
|---|---|---|---|
| 국제 (공적) | ISO/IEC JTC1 | SC27 | **(정보보호 전 분야)** 시스템, 네트워크, 데이터 보안 등 전 분야에 대한 보안 이슈 표준화 작업 진행 중<br>**(차세대 암호기술)** ICT 정보보호를 위한 핵심 암호기술 및 이용 가이드라인에 대한 표준화 추진 중<br>CCRA에서 개정 추진 중인 CC 및 CEM은 ISO/IEC JTC1에서 국제표준으로 개정 예정이며, 한/미/일 공동으로 19790(암호모듈 검증기준) 및 ISO/IEC 24759(암호모듈 시험기준) 표준 2018년 개정 예정<br>바이오인식 응용서비스) 바이오정보 보호지침, 바이오인식기반 하드웨어 보안토큰 등을 개발완료<br>**(정보보호 관리체계)** ISO/IEC 27021 정보보호 경영시스템 전문가 자격 기준 국제표준 제정 추진 중<br>ITU-T X.1051\|ISO/IEC 27011 통신분야 정보보호 통제 지침 국제표준 제정 완료(2016)<br>ISO/IEC 20547-4 Big data reference architecture - Part 4 : Security and privacy fabric 개발 중<br>ISO/IEC JTC1은 CCRA와 협력하여 ISO/IEC15408과 ISO/IEC18045를 2020년 개정할 예정이며, 한/미/일 공동으로 19790(암호모듈 검증기준) 및 ISO/IEC 24759(암호모듈 시험기준) 표준 2018년 개정 예정 |
| | | SC37 | **(바이오인식 응용서비스)** 손금인식을 위한 데이터 호환규격, C++기반의 바이오인식 호환규격 적합성 시험규격 개정안을 개발완료하였고 ISO/IEC 30106-1AMD1, 30106-4 등 객체지향형 바이오인식 호환규격 적합성 시험기술을 개발중<br>**(지능형 CCTV 보안기술)** 얼굴인식을 결합한 지능형 CCTV 성능시험기술을 개발중 |
| | ISO | TC215 | **(IoT 기반 스마트의료기기 보안인증 표준 개발)**<br>보안 인증을 통한 IoT 의료기기 안전성·보안성 확보 및 민감한 개인건강정보의 개인정보보호를 보장하기 위한 스마트 의료기기 보안인증기술 표준화 |
| | IEC | TC65 WG10 | **(제조 표준화)** 산업 공정에 대한 측정, 제어, 자동화 (Industrial-process measurement, control and automation) 관련 표준을 개발 중이며, 공정 제어기기, 공정 조절밸브 등에 대한 표준을 개발하고 있고, 최근 스마트 공장 실현을 위한 요소기술 표준화<br>**(제조 보안)** 미국 ISA99 표준안을 그대로 국제표준으로 전환 |
| | ITU-T | SG17 Q3 | **(정보보호 관리체계: (Telecommunication information security management)** ITU-T X.1051\|ISO/IEC 27011 통신분야 정보보호 통제 지침 국제표준 제정 완료(2016) |
| | | SG17 Q4 | (Cybersecurity: STIX 유스케이스) 다양한 보안업체들의 보안 이벤트 간의 연동을 위해 구조화된 위협정보 표현 규격(STIX)에 대한 유스케이스 표준 개발 진행 중 |

| 구분 | 표준화 기구 | | 표준화 현황 |
|---|---|---|---|
| | | SG17 Q8 | **(Cloud computing security: 빅데이터 보안)** 서비스로서의 빅데이터 보안 가이드라인 |
| | | SG17 Q9 (Telebio metrics) | **(바이오인식 응용서비스)** 모바일기기를 위한 텔레바이오인식 보호지침, 바이오인식기반 하드웨어 보안토큰을 개발완료하였으며, 스마트 ID카드를 이용한 원격 바이오 접근제어 등을 개발중<br>**(생체신호기반 텔레바이오인식기술)** 생체신호를 이용한 텔레바이오인식 인증기술을 개발 중으로 추후 생체신호 인증기반 헬스케어 보안기술 표준화 연구기획 중<br>ITU-T X.1051\|ISO/IEC 27011 통신분야 정보보호 통제 지침 국제표준 제정 완료(2016) |
| | IETF | SEC (Security Area) | **(차세대 암호기술)** 정보보호 서비스 제공을 위한 주요 암호 프로토콜 및 이를 뒷받침하기 위한 핵심 암호기술과 적용 가이드라인에 대한 표준화 추진 중 |
| | ETSI | | **(차세대 암호기술)** ICT 네트워크에 양자 암호를 적용하기 위해 기본이 되는 양자 키 분배 기술부터 표준화를 진행하며, 양자 키 분배를 위한 시스템 및 환경에 대한 규격 개발 추진 중 |
| 국제 (사실상) | FIDO | | 온라인과 오프라인상 FIDO솔루션의 확산을 위해 W3C, EMVCo와 협업함과 동시에 FIDO 2.0 (모바일+웹, PC운영체제)로의 업그레이드 및 이와관련된 표준화 추진 중<br>국가/정부차원의 표준화전개 활동의 일환으로 NIST의 CSF (미국 Cyber Security Frame), PSD2 (EU의 Payment 및 Digital Banking 규정), eIDAS (EU의 새로운 전자서명 규정), APKIC (아시아PKI) 부분과의 표준화 연계 협업 중 |
| | CCRA | | 공통평가기준(CC)와 평가방법론(CEM) 개정, CCRA내 국제기술커뮤니티(iTC)를 통해 cPP와 cPP SD문서 지속 개발 진행중 |
| | 미국 ISA 99 | | **(제조 보안)** 제조 분야 전반에 대한 보안 기술 표준화 진행 |
| 지역 표준화 협의체 | CJK IT Standard Meeting | | - CJK IT Standard Meeting 안에 정보보호 작업반(WG)에서 한중일 전문가들의 의견 공유 및 지역 표준화 개발<br>- 블록체인의 국제표준화 활동을 위해 한중일 3국 간 협력을 제안하였으며, 정보보호 작업반(WG) 산하에 블록체인 임시그룹(Adhoc Group)을 신설('17.8)하기로 결정 |
| 국내 | TTA | PG501 | **(차세대 암호기술)** 주요 차세대 암호기술 표준화 완료 및 양자 키 분배 시스템 규격 표준화 추진 중<br>ISO 17024에서 규정하는 요구사항을 만족하는 인증기관 및 ISO 27021의 요건을 만족하는 인증 스킴에 대한 표준화 준비 중 |
| | | PG502 | **(범용인증 프레임워크)** 신원확인 관리지침, 차세대 네트워크를 위한 아이덴터티 관리 메커니즘, 상호 호환성 및 신뢰를 위한 글로벌 ID 관리 시스템 요구 사항, 개체 인증에 대한 보증 프레임워크, 바이오 정보에 기반한 본인확인 관리방법을 개발하였으며, 최근에는 FIDO UAF, U2F 등을 표준 제정<br>**(개인정보 보호)** 개인정보 영향평가 보고서 작성을 위한 지침, 개인정보 영향 평가를 위한 프라이버시 리스크 관리 프레임워크 개인 정보 관리를 위한 프라이버시 보호 원칙, 개인정보보호 수준 정의를 위한 공통 항목, 개인정보보호를 위한 DB 보안감사 로그, 프라이버시 강화형 |

| 구분 | 표준화 기구 | | 표준화 현황 |
|---|---|---|---|
| | | | 역할기반 접근제어 생성언어 등을 개발함<br>**(지불결제)** 모바일 지불결제, 상호운영성 시험 표준, 대면거래에서의 전자서명 규격, 모바일 어플리케이션 보안지침 등을 개발함<br>**(블록체인 보안)** 블록체인 기반 사물인터넷 디바이스 및 자원 검색 프레임워크 표준을 개발 중 |
| | | PG503 | **(STIX 기술 표준화)** 구조화된 위협 정보 표현 규격(STIX)에 대한 시리즈 표준을 개발 중 |
| | | PG504 | **(응용 보안 평가 인증)** 응용 보안 평가 인증 부문 정보통신단체 표준 제·개정 |
| | | PG505 | **(바이오인식 응용서비스)** 일회용 ID기반 바이오 인증기술, 모바일 바이오인식제품 위조샘플 탐지를 위한 시험평가지침, 바이오인식과 IC카드를 이용한 접근제어용 개인확인시스템, IC카드 기반의 MOC 지문인식 응용 프레임워크 등을 개발중<br>**(생체신호기반 텔레바이오인식기술)** 생체신호 인증알고리즘 성능시험기준, 생체진호정보 프라이버시 보호지침, 개인인증용 생체신호 데이터포맷 등을 개발중<br>**(지능형 CCTV 보안기술)** 지능형 CCTV의 성능 평가용 주석 데이터 교환 포맷 등을 개발완료함<br>**(의료보안)** 디지털 병원 정보보호 요구사항, 전자건강기록 보안기술 등에 관한 표준개발중 |
| | 퀀텀포럼 | | **(차세대 암호기술)** 유럽 ETSI에서 진행하는 양자 키 분배 시스템 관련 표준 규격의 국내 도입 추진 중 |
| | JTC1 SC27 전문위원회 | | 한국/미국/일본 공동으로 ISO/IEC 19790, ISO/IEC 24759 표준을 2018년 개정 후, KS X 표준 2019년 개정 예정 |
| | 국립전파연구원 (SC37-Korea) | | **(바이오인식 응용서비스)** 바이오인식 정보의 보호를 위한 기술적 관리적 지침(TTA 단체표준), 바이오인식 제시형 공격 탐지기술(ISO/IEC 30107-1) 등 KS 국가표준을 개발 중 |
| | 국가기술표준원 | | 공통평가기준, 공통평가방법론, 한국암호모듈검증제도의 암호모듈 보안 요구사항과 시험 요구사항 제·개정 |
| | 스마트의료보안포럼 | | 디지털 병원 정보보호 요구사항<br>모바일 디바이스에서 전자기록의 보안- 보안실무자 가이드<br>모바일 디바이스에서 전자기록의 보안- 보안표준 및 특성 비교<br>스마트의료 서비스 보안위협 |
| | 개인정보보호포럼 | | 개인정보보안 기술 관련 국내/국제 표준 개발 및 제·개정<br>스마트그리드, 클라우드, 스마트 폰 보안, 암호알고리즘 등 보안 및 개인정보보호 기술 국내외 표준 개발 |
| | 한국FIDO산업포럼 | | FIDO UAF 1.1, U2F 1.2, FIDO 2.0에 대한 Spec 공유<br>FIDO 신규보안평가 시스템의 국내 공유 및 가이드<br>국내표준을 FIDO의 글로벌 표준에 반영추진 |

### 2.6.1. 국내 표준화 현황 및 전망

○ **(차세대 암호기술)** TTA를 중심으로 신규 ICT 정보보호를 위한 핵심 암호기술 규격의 표준화를 완료하였고, 현재 양자 키 분배 시스템 표준화를 진행 중

- (TTA 정보보호기반 PG(PG501)) ARIA, SEED, LEA, HIGHT 등 국내에서 개발한 블록 암호 알고리즘의 규격 및 운영 방식(운영 모드, 키 유도 함수, 의사 난수 발생기 등)에 대한 표준화를 진행하였으며, 양자 암호 시스템 규격에 대한 표준화를 시작함
- (국립전파연구원 방송통신표준심의회) 신규 ICT 정보보호를 위한 경량 블록 암호 LEA 규격 표준화 완료
- (NSR) 현재 양자 암호통신 기술에 대한 국내 표준화는 미비한 실정이며, NSR은 양자 암호통신 중 안전성과 관련된 양자 암호기술에 대한 표준화 추진을 제안하였고, 세종대 및 퀀텀포럼은 ETSI의 양자 암호통신 표준 도입을 추진 중임. 또한 SKT 등 통신업체를 중심으로 양자 암호 시스템 개발이 진행 중이며, 이와 관련한 기술 표준화에 대한 관심도가 높아지고 있는 상황임

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA PG501 | TTAK.KO-12.0040/R1, 64비트 블록암호 HIGHT | 2008 | 경량 암호 알고리즘 규격 |
| | TTAK.KO-12.0189/R1, 결정론적 난수발생기 - 제1부- 블록암호 기반 난수발생기 | 2015 | 범용 암호기술 규격 |
| | TTAK.KO-12.0272/0273/0274, 블록암호/HMAC/패스워드 기반 키 유도 함수 | 2015 | 범용 암호기술 규격 |
| | TTAK.KO-12.0275, 형태 보존 암호 FEA | 2015 | 차세대 암호기술 규격 |
| | TTAK.KO-12.0276, 해시 함수 LSH | 2015 | 차세대 암호기술 규격 |
| | TTAK.KO-12.0015/R3, 부가형 전자서명 방식 표준 - 제3부: 타원곡선을 이용한 한국형 인증서 기반 전자서명 알고리즘(EC-KCDSA) | 2016 | 범용 암호기술 규격 |
| | TTAK.KO-12.0001/R4, 부가형 전자서명 방식 표준 - 제2부: 한국형 인증서 기반 전자서명 알고리즘(KCDSA) | 2016 | 범용 암호기술 규격 |
| RRA | KS X 3246, 128 비트 블록 암호 LEA | 2016 | 경량 암호 알고리즘 규격 |
| | KS X 3254, n비트 블록 암호 운영 모드 - 제1부 일반 | 2016 | 범용 암호기술 규격 |

○ **(PKI 기반 인증 및 응용기술)** KISA 주도로 PKI 기반 인증 및 응용기술에 대한 표준화가 진행 중

- (KISA) 스마트폰내에서 안전한 공인인증서 이용을 위한 가이드라인 제공, 간편 공인인증서 인터페이스 가이드라인(2016.8), 바이오정보 연계 등 스마트폰 환경에서 공인인증서 안전 이용 구현 가이드라인(2016.9) 제정함

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA | TTAK.KO-12.0054/R1 i-PIN 서비스 프레임워크 | 2011 | PKI 기반 인증 및 응용기술 |
| | TTAK.KO-12.0001/R3 부가형 전자서명 방식 표준 – 제2부: 한국형 인증서 기반 전자서명 알고리즘(KCDSA) | 2014 | |
| | TTAK.KO-12.0015/R2 부가형 전자서명 방식 표준 – 제3부: 타원곡선을 이용한 한국형 인증서 기반 전자서명 알고리즘(EC-KCDSA) | 2014 | |
| | TTAK.KO-12.0250 대면거래에서의 전자서명 규격 | 2014 | |
| | TTAK.KO-12.0259 HTML5 로컬 스토리지에 저장되는 데이터의 암복호화 프레임워크 | 2014 | |
| KISA | KCAC.TS.KP 전자서명키 보호기술 규격 | 2009 | |
| | KCAC.TS.ACUG 전자서명인증체계 공인인증서 갱신 규격 | 2009 | |
| | KCAC.TS.CT 무선단말기와 PC간 공인인증서 전송을 위한 기술규격 | 2012 | |
| | KCAC.TS.CM 무선단말기에서의 공인인증서 저장 및 이용 기술규격 | 2015 | |
| | KCAC.TS.CMP 공인인증서 관리 프로토콜 규격 | 2015 | |
| | KCAC.TS.UI 공인인증기관간 상호연동을 위한 사용자 인터페이스 기술규격 | 2015 | |
| | KCAC.TS.HSMS 보안토큰 기반 공인인증서 저장형식 기술규격 | 2016 | |
| | KCAC.TS.HSMU 보안토큰 기반 공인인증서 이용기술 규격 | 2016 | |

○ **(범용인증기술)** TTA를 중심으로 ID관리 및 인증기술에서 바이오 인증 기술로 표준화가 진행 중이며, 특히 금융서비스에 특화하여 산업계 요구사항을 수용한 표준화가 추진될 전망

- (TTA 정보보호기반 PG) 2009년부터 OTP로부터 최근 OPT 기술이외의 다양한 인증기술을 개방적으로 수용하여 범용인증 서비스를 제공하기 위한 보안관리 요구사항 등이 개발되고 있으며, 이용자가 소지한 스마트기기와 IC카드 기반 기술을 연계한 멀티팩터 인증기술의 표준화를 진행
- (국가기술표준원) 2012년 모바일 카드, 대면 거래, 비대면 거래에 대한 표준이 제정됨
- (TTA 개인정보보호/ID관리, 블록체인 보안 PG) i-PIN, ID 관리 등에 대한 표준화가 진행되어 왔으며, 2015년 이후에는 FIDO 유니버셜 인증 프레임워크 표준을 제정하였음. 향후 개인정보 유출 확산 방지, O2O 환경에서 주민번호 대체, 보안성이 강화된 새로운 결제 방식에서의 인증 등 현안 문제 해결을 위한 기술 개발 및 표준화 활동이 전망
- (기타) 바이오인식 기능이 탑재된 스마트기기의 보급이 증가하면서 편의성과 보안성을 제공하는 멀티팩터 인증기술 개발에 대한 요구가 증대됨에 따라 국내 표준기구에서 관련 표준화가 추진될 전망

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA PG501 | TTAK.KO-12.0128, 일회용 패스워드(OTP) 통합인증 서비스 프레임워크 | 2009 | 범용인증기술 |
| | TTAK.KO-12.0168, 일회용 패스워드(OTP) 기반 통합인증 서비스 관리 프로토콜 | 2011 | |
| | TTAK.KO-12.0192, IC칩 기반 보안 매체를 활용한 통합형 사용자 인증 서비스 프레임워크 | 2012 | |
| | TTAK.KO-12.0194, 통합인증 기반 부인방지 서비스 프레임워크 | 2012 | |
| | TTAK.KO-12.0218, 모바일기기에 적합한 IC 칩 기반 인증 모듈용 API | 2013 | |
| | TTAK.KO-12.0218/R1, 일회용 패스워드(OTP) 통합인증 서비스 프레임워크(개정) | 2013 | |
| | TTAK.KO-12.0219, IC칩 기반 인증 모듈 보안 요구 사항 | 2013 | |
| | TTAK.KO-12.0221, 모바일 기기를 이용한 다중 요소 인증 메커니즘 | 2013 | |
| | TTAK.KO-12.0244, 전자거래 단계별 위험수준에 대한 인증서비스 지침 | 2014 | |
| | TTAK.KO-12.0245, 신뢰기관을 이용한 통합인증서비스 보안 요구사항 | 2014 | |
| | TTAK.KO-12.0247, 전자거래 보증 수준별 인증방법 요구사항 | 2014 | |
| | TTAK.KO-12.0248, 국내 환경에 적합한 실체 인증 보증 프레임워크 | 2014 | |
| TTA PG502 | TTAK.KO-12.0038/R2, i-PIN 서비스 중복 가입 확인 정보 | 2011 | |
| | TTAK.KO-12.0054/R1, i-PIN 서비스 프레임워크 | 2011 | |
| | TTAK.KO-12.0198, IC 칩 기반 모바일 결제 보안 요구 사항 | 2012 | |
| | TTAK.KO-12.0196, 모바일 환경의 사용자 중심 개인화 서비스를 위한 사용자 데이터 처리 구조 | 2012 | |
| | TTAE.IT-Y.2722, 차세대 네트워크를 위한 아이덴터티 관리 메커니즘 | 2012 | |
| | TTAE.IT-Y.2721, 차세대 네트워크를 위한 아이덴터티 관리 요구 사항 및 사용 시나리오 | 2012 | |
| | TTAE.IT-Y.2720, 차세대 네트워크를 위한 아이덴터티 관리 프레임워크 | 2012 | |
| | TTAK.KO-12.0200, 개인 정보 관리를 위한 프라이버시 보호 원칙 | 2012 | |
| | TTAE.IT-X.1250, 상호 호환성 및 신뢰를 위한 글로벌 ID 관리 시스템 요구 사항 | 2012 | |
| | TTAK.KO-12.0250, 대면거래에서의 전자서명 규격 | 2014 | |
| | TTAE.OT-12.0017-Part1~11, FIDO 유니버셜 인증 프레임워크(UAF) | 2015 | |
| | TTAE.OT-12.0018-Part1-7, FIDO 유니버셜 이중인증(U2F) | 2016 | |
| | TTAI.OT-12.0019, 웹 인증: 크리덴셜 접근을 위한 웹 API | 2016 | |
| | TTAK.KO-12.0250, 대면거래에서의 전자서명 규격 | 2014 | |
| | TTAK.KO-12.0252, 모바일 결제를 위한 어플리케이션 보안 지침 | 2014 | |
| RRA | KCS.KO-05.0048 모바일 터치 서비스 동글 인터페이스 규격 | 2012 | |
| | KCS.KO-05.0047 모바일 터치 서비스 애플릿 규격 | 2012 | |
| 국가기술표준원 | KS X 6928-1, 모바일 카드 | 2012 | |
| | KS X 6928-2, 대면 거래 | 2012 | |
| | KS X 6928-3, 비대면 거래 | 2012 | |
| PG505 | TTAR-12.0021, 핀테크 환경에서 텔레바이오인식을 이용한 비대면 인증(기술보고서) | 2016 | |

○ **(바이오인식 응용 서비스)** 국내 표준은 TTA PG505, KISA, 인하대학교, 충북대학교, 경인여대를 중심으로 개발되어 왔으며, 바이오정보 보호기술·시험기술, 텔레바이오인식 응용기술은 JTC1 SC27·SC37, ITU-T SG17 등 국제표준화 기구에서 제정한 표준을 국내 상황에 맞게 수정한 상태로 준용되었음

- (TTA PG505, 인하대, 충북대, 경인여대) 금융보안 관련 바이오인식 운영지침, 핀테크 환경의 텔레바이오인식 적용, 지문입력기의 취약점 분석기술 등에 관하여 표준개발 완료
- (TTA PG505, 인하대, 충북대, 경인여대) 모바일 기기를 이용한 원격 바이오인증 서비스가 급증함에 따라, 모바일 바이오인식제품 위조샘플 탐지를 위한 시험기술, IC카드기반의 MOC 바이오인식 융합기술, 텔레바이오인식 응용기술에 대한 표준을 활발히 개발 중

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA PG505 | TTAK.KO-12.0302, 금융보안을 위한 바이오인식 운영 지침 | 2016 | 바이오인식 응용 서비스 |
| | TTAR-12.0021, 핀테크 환경에서 텔레바이오인식을 이용한 비대면 인증(기술보고서) | | |
| | TTAR-12.0004/R1, [개정] 지문인식 시스템의 안전성 확보를 위한 지문입력기의 취약점 분석(기술보고서) | | |
| | 2017-415, 일회용 ID기반 바이오 인증기술 | 진행중 (2017) | |
| | 2017-050, 모바일 바이오인식 제품의 위조샘플 탐지를 위한 시험 평가 지침 | | |
| | 2017-049, 바이오인식과 IC 카드를 이용한 접근제어용 개인 확인시스템 | | |
| | 2016-1902, 바이오인식 보안토큰을 이용한 원격 바이오인증 프레임워크 | | |
| | 2016-1901, 모바일 디바이스에서의 텔레바이오인식 보안지침 | | |
| | 2016-098, IC 카드 기반의 Match-on-card 지문인식 응용 Framework | | |

○ **(생체신호기반 텔레바이오 인식기술)** 국내 표준은 한국정보통신기술협회(TTA) PG505, 한국인터넷진흥원(KISA), 서울의과대학교를 중심으로 텔레바이오인식기술 표준을 개발 중

- (TTA PG505, KISA, 서울의과대학교) KISA 모바일 생체신호 인증기술 표준연구회를 중심으로 심박수·심전도 등의 생체신호에 대한 개인식별 기술개발과 표준화 연구를 착수하였으며, TTA PG505를 통하여 생체신호센서 인터페이스, 생체신호 개인식별 및 보호기술, 생체신호 시험기술 등의 표준을 개발 중

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA PG505 | TTAK.KO-12.0304, 개인인증용 생체신호센서 요구사항 | 2016 | 생체신호기반 텔레바이오 인식기술 |
| | TTAK.KO-12.0303, 개인인증을 위한 생체신호 정보 시험용 DB 구축지침 | | |
| | 2017-414, 생체신호 인증알고리즘 성능시험기준 | 진행중 (2017) | |
| | 2016-1904, 생체신호 정보 프라이버시 보호지침 | | |
| | 2016-1903, 개인인증용 생체신호 데이터 포맷 | | |

○ **(바이오인식기반 CCTV보안기술) TTA** PG505를 중심으로 표준 개발 중

- (TTA PG505) 지능형 CCTV 시험기술, 얼굴인식과 결합한 지능형 CCTV 융합보안기술 등의 표준화를 추진 중

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA PG505 | TTAK.KO-12.0159, 얼굴 영역 검출을 이용한 CCTV 영상정보 프라이버시 보호를 위한 보안 요구 사항 | 2010 | 바이오인식기반 CCTV 보안기술 |
| | TTAK.KO-12.0216, 영상감시 시스템에서의 개인 영상정보 보호 지침 | 2012 | |
| | TTAK.KO-12.0207, 네트워크 영상감시시스템에서 증거영상 수집을 위한 지침 | | |
| | TTAK.KO-12.0291, 지능형 CCTV의 성능 평가용 주석 데이터 교환 포맷 | 진행중 (2018) | |

○ **(보안 솔루션 위협정보 공유 및 연동 프레임워크)** 국내 표준은 TTA, ETRI, KISA를 중심으로 개발되어 왔으며, 사이버보안 정보공유 프레임워크와 정보공유 프로토콜은 ITU-T와 IETF 등 국제표준화 기구에서 제정한 표준을 국내 상황에 맞게 준용되었음

- (TTA 사이버보안 PG(PG503)) 침해사고 정보 전달 포맷 및 프로토콜에 대한 표준이 제정되었으며, 사이버 공격대응 통합관리 솔루션 연동 기술에 대한 표준 추진 예정

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA PG503 | (TTA) TTAK.KO-12.0145, 분산서비스거부 공격의 탐지 및 대응 메시지 교환 포맷 | 2010 | 보안 솔루션 위협정보 공유 및 연동 프레임워크 |
| | (TTA) TTAK.KO-12.0061/R1, 네트워크 공격에 대한 시그니처 교환 프로토콜 | 2010 | |
| | (TTA) TTAK.KO-12.0172, 사이버보안 정보공유 협상 절차 | 2011 | |
| | (TTA) TTAE.IT-X.1570, 사이버보안 정보 교환에서의 탐색 메커니즘 | 2012 | |
| | (TTA) TTAK.KO-12.0229, 확장된 침입 탐지 메시지 교환 포맷 | 2013 | |
| | (TTA) TTAK.KO-12.0242, 세션 정보 메시지 교환 포맷(SIMEF) | 2014 | |
| | (TTA) TTAK.KO-12.0256, 보안 관제를 위한 시스템 메시지 교환 포맷 | 2014 | |
| | (TTA) TTAK.KO-12.0279, 보안 정보 메시지 교환 프로토콜 | 2015 | |
| | (TTA) TTAE.IF-RFC4766, 침입 탐지 메시지 교환 요구사항 | 2015 | |
| | (TTA) TTAK.KO-12.0282, 침입탐지시스템을 위한 보안 정책 메시지 및 배포 프로토콜 | 2015 | |
| | (TTA) TTAK.KO-12.0283, Snort 기반 침입탐지시스템 탐지 규칙 요구사항 | 2015 | |
| | (TTA) TTAI.OT-12.0020-part1, 구조화된 위협 정보 표현 규격(STIX) 제1부: 개요 | 2016 | |
| | (TTA) TTAI.OT-12.0020-part2, 구조화된 위협 정보 표현 규격(STIX) 제2부: 공통 | 2016 | |
| | (TTA) TTAI.OT-12.0020-part3, 구조화된 위협 정보 표현 규격(STIX) 제3부: 코어 | 2016 | |

○ **(유형별 보안성 시험평가기준)** 정책기관, 인증기관, 평가기관, 정보보호시스템 개발업체 간의 협업(사용자 포럼 등)을 통한 기술별 평가 기준 개발 및 국내 표준화(TTA 등) 추진

- (국가기술표준원) 2009년 12월 공통평가기준 국제표준과 일치하는 국내 표준 KS X ISO/IEC 15408-1, 15408-2, 15408-3을 개정하였으며, 2010년 12월 공통평가방법론 국제표준과 일치하는 국내 표준 KS X ISO/IEC 18045를 개정하였음. 한국암호모듈검증제도의 암호모듈 보안 요구사항과 시험 요구사항은 2007년 각각 KS X ISO/IEC 19790과 KS X ISO/IEC 24759로 제정되었으며, 2015년 개정

- (국가보안기술연구소 IT보안인증사무국) CCRA에서 제정한 CC 및 CEM을 홈페이지에 게시하고 있으며, 제품 유형별 보호프로파일을 개발하여 공개하고 있음.

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| 국가표준기술원 | KS X ISO/IEC 15408-1, 정보기술보안 평가기준 - 제1부 : 개요와 일반모델 | 2009 | 정보보호제품 평가 |
| | KS X ISO/IEC 15408-2, 정보기술보안 평가기준－제2부 : 보안기능 컴포넌트 | 2009 | |
| | KS X ISO/IEC 15408-3, 정보기술보안 평가기준－제3부 : 보안보증 컴포넌트 | 2009 | |
| | KS X ISO/IEC 18045, 정보 기술 보안 평가 방법론 | 2010 | |
| | KS X ISO/IEC 19790, 정보 기술 - 보안 기술 - 암호모듈 보안 요구사항 | 2015 | 암호모듈 검증 |
| | KS X ISO/IEC 24759, 정보 기술 - 보안 기술 - 암호모듈 시험 요구사항 | 2015 | |
| IT보안인증사무국 | KECS-PP-0714-2016, 국가용 네트워크 장비 보호프로파일 | 2016 | 정보보호제품 평가 |
| | KECS-PP-0715-2016, 국가용 침입차단시스템 보호프로파일 | 2016 | |
| | KECS-PP-0716-2016, 국가용 가상사설망 보호프로파일 | 2016 | |
| | KECS-PP-0717-2016, 국가용 인터넷전화방화벽 보호프로파일 | 2016 | |
| | KECS-PP-0718-2016, 국가용 무선랜 인증 보호프로파일 | 2016 | |
| | KECS-PP-0822-2017, 국가용 통합인증 보호프로파일 | 2017 | |
| | KECS-PP-0820-2017, 국가용 문서 암호화 보호프로파일 | 2017 | |
| | KECS-PP-0822-2017, 국가용 데이터베이스 암호화 보호프로파일 | 2017 | |
| | KECS-PP-0819-2017, 국가용 무선침입방지시스템 보호프로파일 | 2017 | |
| | KECS-PP-0803-2017, 국가용 침입방지시스템 보호프로파일 | 2017 | |
| | KECS-PP-0804-2017, 국가용 네트워크 자료유출방지 보호프로파일 | 2017 | |
| | KECS-PP-0805-2017, 국가용 네트워크 자료유출방지 보호프로파일 | 2017 | |
| TTA | TTAK.KO-12.0293, 암호모듈 현장시험 지침 | 2016 | 암호모듈 검증 |
| | TTAK.KO-12.0289, DB 암호화 제품 보안성 평가를 위한 보안 요구 사항 | 2015 | 정보보호 제품 평가 |

○ **(정보보호 관리체계)** 국가 차원의 규제를 바탕으로 정보보호 관리체계가 발전하고 있으나 규제와 제도의 중복으로 표준화를 통한 효율적인 관리가 필요하며 특히 관리체계의 효과적인 유지를 위한 표준화가 필요. 정보보호 관리체계 중에서 산업 분야별 정보보호 관리체계 인증기준은 ISO 27001 ISMS 요구사항을 기반으로 산업 분야별로 금융, 통신, 클라우드, 에너지, 의료 분야에 대한 보안 통제 항목 및 구현 가이드 등이 지속적으로 개발되고 있으나, 제조 분야에 대해서는 정의된 기준이 없음

- 정보보호 활동에 대한 사각지대를 최소화하고 기업비지니스 활동을 지원하기 위하여 효과적인 정보보호 활동에 대한 기준 제시와 유효성을 지원할 수 있는 제도가 개발되었으나 실제 업무 환경에 적용되기 위해서는 더욱 명확한 활동의 표준 가이드의 제시가 필요

- (미래부/KISA) ISMS 인증제도를 개발하여 시행중에 있음, 정보보호 관리과정 12개 항목과 정보보호대책 항목 92개 항목으로 총 104개 인증기준을 기반으로 인증제도 운영 중

- (금융위/금융보안원) 금융 ISMS 인증제도를 개발하여 시행 하고 있음 금융기관의 특성을 고려하여 KISA에서 운영중인 인증제도보다 강화된 인증기준을 개발

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA PG501 | TTAS.KO-12.0036, 정보보호관리체계 수립 지침 | 2006 | 정보보호 관리체계 |

○ **(개인정보보호 정책 및 운영관리 기술)** 개인정보 관리체계에 대한 통합이 PIMS를 중심으로 이루어져 적응과정을 거치고 있으며, 개인정보와 정보보호 관리체계의 통합 및 ISO27001과의 상호 인증에 대해서도 지속적인 논의를 추진함으로써 개인정보보호에 대한 효과적인 활동이 이루어 질 수 있는 방안에 대한 방향제시가 필요

- (TTA 개인정보보호/ID관리, 블록체인 보안 PG(PG502))개인정보관리를 위한 프라이버시 보호 원칙에 대한 표준을 수립하였으며, 정부에서는 국내외 표준과 국내 개인정보보호 관련 법률을 고려하여 “개인정보보호 관리체계 인증제도”를 운영 중. 현재 국내 표준화 전문가의 주도로 국내의 개인정보보호 관리체계지침을 기반으로 한 국제 표준화가 수행되고 있으므로, 국제 표준 수립 후 이를 반영하여 국내 표준으로 재정립하는 활동이 필요

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA PG502 (개인정보보호/ID 관리, 블록체인 보안 PG) | TTAR-06.0013, RFID 프라이버시 보호 가이드라인 | 2006 | 개인정보보호 정책 및 운영관리 기술 |
| | TTAS.KO-12.0053, 개인정보 생명주기별 보안 관리 모델 | 2007 | |
| | TTAS.KO-12.0051, 개인정보보호정책 설정 및 협상 규격 | 2007 | |

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| | TTAK.KO-12.0055/R2, i-PIN 서비스 전달 메시지 형식 | 2011 | |
| | TTAK.KO-12.0054/R1, i-PIN 서비스 프레임워크 | 2011 | |
| | TTAK.KO-12.0072, 개인정보 DB 관리 기술의 보안요구사항 | 2008 | |
| | TTAK.KO-12.0073, 프라이버시 강화형 역할기반 접근제어 생성언어 | 2008 | |
| | TTAK.KO-10.0302, 라이프로그 데이터 운영상의 프라이버시 보존 | 2008 | |
| | TTAK.KO-06.0185, 모바일 RFID 사용자 프라이버시 보호 서비스-시스템 요구사항 | 2008 | |
| | TTAK.KO-12.0038/R2, i-PIN 서비스 중복가입 확인정보 | 2011 | |
| | TTAK.KO-12.0103, 개인정보보호 수준 정의를 위한 공통 항목 | 2009 | |
| | TTAK.KO-12.0103, 개인정보보호 수준 정의를 위한 공통 항목 | 2009 | |
| | TTAK.KO-12.0105, 개인정보보호를 위한 DB 보안감사 로그 | 2009 | |
| | TTAK.KO-12.0142, 보조기억매체의 안전한 이용 방안 | 2010 | |
| | TTAK.KO-12.0159, 얼굴 영역 검출을 이용한 CCTV 영상 정보 프라이버시 보호를 위한 보안 요구 사항 | 2010 | |
| | TTAK.KO-06.0146/R1, 모바일 RFID 사용자 프라이버시 보호 프레임워크 | 2010 | |
| | TTAE.OT-12.0015, 공공 클라우드 컴퓨팅의 보안 및 프라이버시 보호 지침 | 2011 | |
| | TTAE.IT-X.1275, RFID 응용에서의 개인 정보 보호 지침 | 2011 | |
| | TTAK.OT-10.0336, 모바일 웹 애플리케이션을 위한 단말 API 정책 및 개인 정보 보호 요구 사항 | 2012 | |
| | TTAK.KO-12.0200, 개인 정보 관리를 위한 프라이버시 보호 원칙 | 2012 | |
| | TTAK.KO-10.0616, 퍼스널 클라우드 개인정보보호 참조모델 | 2012 | |
| | TTAK.KO-12.0233, 스마트폰 단말기에서 모바일뱅킹을 위한 개인정보보호 지침 | 2013 | |
| | TTAK.KO-12.0226,개인 정보 영향 평가를 위한 프라이버시 리스크 관리 프레임워크 | 2013 | |
| | TTAK.KO-12.0288,호스트 컴퓨터 개인 정보 보호 제품 보안성 평가를 위한 보안 요구 사항 | 2015 | |
| | TTAK.KO-12.0277, 개인 정보 영향 평가 보고서 작성을 위한 지침 | 2015 | |
| | TTAK.KO-10.0834, 건강라이프로그 서비스를 위한 프라이버시 및 보안 분류 지침 | 2015 | |

○ **(빅데이터 데이터 보안)** 정부의 공공정보 공개 방침에 따라, 다양한 공공정보가 공개되고 있으나 일부 개인정보 및 개인정보 유출 가능성이 있는 데이터의 공개로 인해 비식별 및 오용/남용 탐지를 위한 참조 모니터 기술의 표준화가 시급함

- (행정자치부) 2016년 정부 가이드라인 형태로 개발되어 정형 데이터의 비식별화 기술과 공공정보 공개에서 어떤 비식별화 기술을 사용하는 것이 좋은지를 권고하고 있음. 2017년 영상 정보에 대한 비식별화 기술에 대한 가이드라인을 추진하고 있음
- (금융보안원/KISA) 금융정보의 비식별화 기술 및 가이드라인을 개발하고 있으며, 서로 다른 데이터를 결합하는 서비스에서 개인정보 유출에 대한 다양한 가이드라인 개발 중

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| 금융보안원/ KISA | 금융정보의 비식별화 기술 및 가이드라인 | 추진 중 (2020) | 빅데이터 데이터 보안 |

○ **(의료보안)** '17년초부터 인체에 삽입된 의료기기에 대한 해킹공격이 발생함에 따라, 시판전후의 전과정에서 나타날 수 있는 보안 취약성과 대응방안을 사전에 마련토록 하고 있음

- (TTA PG505, 스마트의료보안포럼) 디지털 병원 보안 요구사항, 스마트 의료서비스 참조모델의 보안위협, 모바일 디바이스에서의 전자건강기록의 보안기술에 대한 기술보고서를 개발완료하였으며, 생체신호를 이용한 헬스케어 모니터링기술 등 표준화를 추진할 전망임

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA PG505, 스마트의료 보안포럼 | TTAK.KO-12.0305, 디지털 병원 정보보호 요구사항 | 2016 | 의료보안 |
| | TTAR-12.0022, 모바일 디바이스에서 전자건강기록의 보안 - Part I :요약(기술보고서) | | |
| | TTAR-12.0023, 모바일 디바이스에서 전자건강기록의 보안 - Part II:개인정보(PHI) 보호체계(기술보고서) | | |
| | 2016-1760, 스마트의료 서비스 참조 모델의 보안위협 | 진행중 (2017) | |
| | 2017-047, 모바일 디바이스에서 전자기록의 보안-엔지니어 가이드 | | |
| | 2017-048, 모바일 디바이스에서 전자건강기록의 보안 PART Ⅳ 보안표준 및 특성 비교 | | |

○ **(제조 보안)** 국내에서는 주로 제조 분야에 대한 일반적인 표준이 주로 마련되고 있고, 스마트 제조 보안 분야에 대한 표준화 작업이 미미함

- (TTA PG609) 사물인터넷, 클라우드, 빅데이터, 모바일 등과 같은 ICT 기술을 기반으로 스마트공장에 적용하는 목적으로 관련 스마트공장 표준을 개발

< 국내 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| TTA PG609 | TTAK.KO-11.0207, 스마트팩토리 용어 | ~2017 | 제조 보안 |
| | TTAK.KO-11.0199, ICT 제조 융합 스마트 팩토리 참조 모델 | | |
| | TTAK.KO-11.0200, ICT 제조 융합 전개 모델 | | |
| | TTAK.KO-11.0205, 스마트 팩토리를 위한 생산현장의 스마트화 요구사항 | | |
| | TTAK.KO-11.0198, 사이버-물리 생산 시스템(CPPS) 연동 미들웨어의 인터페이스 요구사항 | | |
| | TTAK.KO-11.0202, 사이버-물리 생산 시스템 연동 미들웨어의 명세 언어 정의 | | |
| | TTAK.KO-11.0208, 사이버-물리 생산 시스템 서비스 디렉토리 인터페이스 명세 | | |
| | TTAK.KO-11.0209, 사이버-물리 생산 시스템 게이트웨이 실행 모듈 인터페이스 정의 | | |
| | TTAK.KO-11.0210, 사이버-물리 생산 시스템 연동 미들웨어에서의 설비 제어서비스 제공 규격 | | |
| | TTAK.KO-11.0211, 사이버-물리 생산 시스템 연동 미들웨어 사용자 인터페이스 | | |
| | TTAK.KO-11.0116, CPS 시스템을 위한 메타모델링 언어 개발 지침 | | |
| | TTAK.KO-11.0117, CPS 시스템의 모델 검사기 참조 모델 | | |
| | TTAK.KO-11.0118, CPS 시스템의 연동 시뮬레이션을 위한 객체 모델 지침 | | |

### 2.6.2. 국외 표준화 현황 및 전망

○ **(차세대 암호기술)** ISO와 IETF를 중심으로 한 암호 알고리즘 규격 및 적용 가이드라인의 표준화와, ETSI를 중심으로 한 양자 키 분배 시스템 규격 표준화가 활발히 진행 중임

- (ISO) 경량 환경을 위한 암호 알고리즘 및 기능성 차세대 암호기술 규격에 대한 표준화가 활발히 진행 중
  - · 미국 NSA가 개발한 SIMON/SPECK 및 한국의 LEA를 경량 블록 암호 알고리즘 표준(29192-2)에 포함시키기 위한 표준화 작업이 진행 중
  - · 벨기에 COSIC에서 개발한 Chasky와 LightMAC을 경량 메시지 인증 코드 알고리즘 표준(29192-6)으로 제정하기 위한 표준화 작업이 진행 중
  - · 동형 암호를 범용 암호화 알고리즘 표준(18033-6)에 포함시키기 위한 표준화 작업이 진행 중. 동형 암호 분야에서는 최근 학계에서 연구되고 있는 완전 동형 암호(Fully Homomorphic Encryption)가 아닌 부분 동형 암호(Somewhat Homomorphic Encryption) 알고리즘 2종에 대한 표준화가 진행 중임. 이러한 추세는 산업계의 기술 소요에 대응하여 개발된 암호 알고리즘에 대한 선 표준화 후 활용의 추진 체계를 통해 시장 주도권을 선점하기 위한 전략임
  - · 2015년 미국 연방정부 사용이 승인된 신규 해시 함수 SHA-3를 전용 해시 함수 알고리즘 표준(10118-3)에 포함시키기 위한 표준화 작업이 진행 중
- (IETF) 경량 환경에 적합한 암호 프로토콜 규격 및 프로토콜 적용을 위한 핵심 암호기술에 대한 표준화가 활발하게 진행 중
  - · 특히 (D)TLS는 IoT 연결 플랫폼 개발을 위한 오픈소스 프로젝트(IoTivity, openM2M, Thread 등)를 비롯하여 경량 환경에서의 정보보호를 위한 핵심 프로토콜로 채택되고 있음
  - · TLS의 안전성 강화를 위한 새로운 규격 개발(TLS 1.3) 및 관련 신규 암호기술의 표준화가 진행 중
  - · 해시 함수 SHA-3의 암호 프로토콜 적용을 위한 표준화가 진행될 것으로 전망됨
- (ITU-T) 경량 암호 기술과 관련하여, ITU-T SC17은 ICT 전반의 정보보호를 위해 ISO에서 표준화하고 있는 다양한 암호 알고리즘을 활용하는 측면에서 ISO 표준안의 공동 검토 등의 협력 체계를 구축하고 있음
- (ETSI) 양자 암호는 ETSI를 중심으로 도시바, IDQ 등 양자 암호 선도업체 중심의 표준화가 진행되고 있음. ETSI의 표준화는 2010년 전후로 다소 주춤하였으나, 최근의 양자 정보통신에 대한 국제적 관심이 증대됨에 따라 2016년부터 다시 본격적으로 표준화에 대한 논의가 활발하게 진행 중
  - · 차세대 암호기술 중 양자 암호기술의 표준화는 ETSI가 주도하고 있으며, 보안 관점이 아닌 시스템 구축 측면으로 진행 중임. 이는 아직 산업화 기반이 약한 양자 암호의 조기 상용화를 위해 산업계의 주도로 진행되기 때문으로 볼 수 있으며, 관련 업계의 구현기술 보편화를 위한 일반화 가능한 영역부터 표준화를 시도하는 추세임
  - ·

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ISO SC27 | ISO/IEC 9797, Message Authentication Codes (MACs)<br>- Part 1: Mechanisms using a block cipher<br>- Part 2: Mechanisms using a dedicated hash-function<br>- Part 3: Mechanisms using a universal hash-function | 2011 | 범용 암호기술 규격 |
| | ISO/IEC 10116, Modes of operation for an n-bit block cipher | 2006 | 범용 암호기술 규격 |
| | ISO/IEC 10118, Hash-functions<br>- Part 2: Hash-functions using an n-bit block cipher<br>- Part 3: Dedicated hash-functions | 2010<br>2004 | 범용 암호기술 규격 |
| | ISO/IEC 14888, Digital signatures with appendix<br>- Part 2: Integer factorization based mechanisms<br>- Part 3: Discrete logarithm based mechanisms | 2008<br>2016 | 범용 암호기술 규격 |
| | ISO/IEC 18031, Random bit generation | 2011 | 범용 암호기술 규격 |
| | ISO/IEC 18033, Encryption algorithms<br>- Part 2: Asymmetric ciphers<br>- Part 3: Block Ciphers<br>- Part 4: Stream Ciphers<br>- Part 5: Identity-based ciphers | <br>2006<br>2010<br>2011<br>2016 | 범용 암호기술 규격 |
| | - Part 6(CD): Homomorphic encryption | 진행중 (2018) | 차세대 암호기술 규격 |
| | ISO/IEC 19772, Authenticated encryption | 2009 | 범용 암호기술 규격 |
| | ISO/IEC 29192, Lightweight cryptography<br>- Part 2: Block ciphers<br>- Amendment 1 to Part 2 - SIMON/SPECK<br>- Amendment 2 to Part 2 - LEA<br>- Part 3: Stream ciphers<br>- Part 4: Mechanisms using asymmetric techniques<br>- Part 5: Hash-functions<br>- Part 6(WD): Message authentication codes (MACs) | <br>2012<br>진행중 (2019)<br>2013<br>2016<br>2016<br>진행중 (2018) | 차세대 암호기술 규격 |
| IETF | RFC 7008, A description of the KCipher-2 Encryption Algorithm | 2013 | 범용 암호기술 규격 |
| | RFC 7253, The OCB Authenticated-Encryption Algorithm | 2014 | 범용 암호기술 규격 |
| | RFC 7539, ChaCha20 and Poly1305 for IETF Protocols | 2015 | 범용 암호기술 규격 |
| | RFC 7634, ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec | 2015 | 암호 알고리즘 프로토콜 적용 규격 |
| | RFC 7693, The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC) | 2015 | 암호 알고리즘 프로토콜 적용 규격 |
| | RFC 7748, Elliptic Curves for Security | 2016 | 범용 암호기술 규격 |
| | RFC 7801, GOST R 34.12-2015: Block Cipher "Kuznyechik" | 2016 | 범용 암호기술 규격 |

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| | RFC 7905, ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS) | 2016 | 암호 알고리즘 프로토콜 적용 규격 |
| | RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2 | 2016 | 암호 알고리즘 프로토콜 적용 규격 |
| | RFC 8018, PKCS #5: Password-Based Cryptography Specification Version 2.1 | 2017 | 암호 알고리즘 프로토콜 적용 규격 |
| | RFC 8031, Curve25519 and Curve448 for the Internet Key Exchange Protocol Version 2 (IKEv2) Key Agreement | 2016 | 암호 알고리즘 프로토콜 적용 규격 |
| | RFC 8032, Edwards-Curve Digital Signature Algorithm (EdDSA) | 2017 | 범용 암호기술 규격 |
| | RFC 8080, Edwards-Curve Digital Signature Algorithm (EdDSA) for DNSSEC | 2017 | 암호 알고리즘 프로토콜 적용 규격 |
| | RFC 8103, Using ChaCha20-Poly1305 Authenticated Encryption in the Cryptographic Message Syntax (CMS) | 2017 | 암호 알고리즘 프로토콜 적용 규격 |
| | RFC 8133, The Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) Protocol | 2017 | 암호 알고리즘 프로토콜 적용 규격 |
| | draft-ietf-tls-tls13-20, The Transport Layer Security (TLS) Protocol Version 1.3 | 진행중 (2017) | 암호 알고리즘 프로토콜 적용 규격 |
| | draft-ietf-tls-dtls13-00, The Datagram Transport Layer Security (DTLS) Protocol Version 1.3 | 진행중 (2018) | 암호 알고리즘 프로토콜 적용 규격 |
| ETSI | GS-QKD-002, Quantum Key Distribution(QKD); Use Cases | 2010 | QKD 시스템 규격 |
| | GS-QKD-003, Quantum Key Distribution(QKD); Components and Internal Interfaces | 갱신중 (2018) | QKD 시스템 규격 |
| | GS-QKD-004, Quantum Key Distribution(QKD); Application Interface | 2010 | QKD 시스템 규격 |
| | GS-QKD-005, Quantum Key Distribution(QKD); Security Proofs | 2010 | QKD 시스템 규격 |
| | GS-QKD-008, Quantum Key Distribution(QKD); QKD Module Security Specification | 2010 | QKD 시스템 규격 |
| | GS-QKD-011, Quantum Key Distribution(QKD); Component characterization: characterizing optical components for QKD systems | 2016 | QKD 시스템 규격 |
| | GS-QKD-007, Quantum Key Distribution(QKD); Ontology, vocabulary and terms of reference | 진행중 (2018) | QKD 시스템 규격 |
| | GS-QKD-010, Quantum Key Distribution(QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems | 진행중 (2018) | QKD 시스템 규격 |
| | GS-QKD-012, Quantum Key Distribution(QKD); Device and Communication Channel Parameters for QKD Deployment | 진행중 (2018) | QKD 시스템 규격 |
| | GS-QKD-013, Quantum Key Distribution(QKD); Characterisation of Optical Output of QKD transmitter modules | 진행중 (2018) | QKD 시스템 규격 |

○ **(PKI 기반 인증 및 응용기술)** IETF에서 PKI 표준화가 종료되었으며 사용자 인증 강화를 위한 FIDO에 PKI 연계방안 등 PKI 응용 표준화가 진행 중

- (IETF) PKI 관련 국제표준의 경우 IETF의 표준화(pkix) 표준화 종료
- (W3C) W3C의 FIDO 2.0의 Web API 표준화 진행 중
- (FIDO Alliance) 사용자 인증을 강화하기 위한 표준 프레임워크를 제공하기 위한 표준단체를 통하여 서버환경의 변경 없이 다양한 인증수단(Bio 정보, 보안토큰 등)을 지원할 수 있는 표준 규격FIDO 1.X이 제정되었고 FIDO 2.0 및 사용자 인증강화를 위한 표준프레임웍 표준화가 진행 중이며, FIDO와 PKI 연계 방안에 대한 표준화 추진 중임
- (IEEE) 자율주행 차량을 위한 WAVE (Wireless Access for Vehicle Environment) 국제표준이 2013년 처음 만들어 지고 2016년에 추가 개정되어 사용 중이며 실증프로젝트의 결과를 반영하여 향후 추가 개정될 예정임

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| IETF | RFC 6664 S/MIME Capabilities for Public Key Definitions | 2012 | PKI 기반 인증 및 응용기술 |
| | RFC 6712 Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP) | 2012 | |
| | RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile | 2013 | |
| | RFC 6844 DNS Certification Authority Authorization (CAA) Resource Record | 2013 | |
| | RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP | 2013 | |
| | RFC 7030 Enrollment over Secure Transport | 2013 | |
| ISO/IEC JTC1 SC2 | ISO/IEC 18014-1 Time stamping services and protocols- Part 1 : Framework | 2014 | |
| | ISO/IEC 18014-4 Time-stamping services - Part 4: Traceability of time sources | 2015 | |
| | ISO/IEC 9594-1 The Directory -- Part 1: Overview of concepts, models and services | 2014 | |
| | ISO/IEC 9594-8 The Directory -- Part 8: Public-key and attribute certificate frameworks | 2014 | |
| IEEE | IEEE Std. 1609.2-2016, Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages | 2016 | |
| FIDO Alliance | FIDO Universal Authentication Framework(UAF) v1.1 Specifications | 2017 | |
| | FIDO Universal 2nd Factor (U2F) v1.2 Specifications | 2017 | |

○ **(범용인증기술)** 웹인증, 핀테크 인증 등을 위한 다양한 표준화가 진행 중이며, 향후 해당 기술의 표준화는 다수의 글로벌기업 주도로 ISO/IEC, ITU-T, IETF 등에서 활발히 이루어질 전망

- (ITU-T SG17) 2012년 통합인증 서비스 프레임워크를 제안하여 2014년 X.1159로 표준화되었으며, 2012년 한국 주도로 스마트 환경의 보안성 향상을 위한 국제 표준안을 제안하여 2014년 X.1158이 완료되었으며, 서로 다른 도메인(민간-공공)간 인증 및 정보공유를 위한 클라우드 ID 관리 시스템 등 기술 개발 및 표준화 활동이 전망
- (ISO/IEC JTC1 SC27) 2013년 "Entity authentication assurance framework"가 제정되었으며, 전통적인 IC카드 표준이 접촉식은 ISO7816로 비접촉식은 ISO14443로 표준화가 진행
- (FIDO Alliance, W3C) 2014년 FIDO Universal Authentication Framework 표준안을 제정한 후, 현재 FIDO 2.0 표준안을 W3C에 제안하여 2017년 현재 W3C에서 "Web Authentication: An API for accessing Public Key Credentials" 표준화가 진행
- (OASIS) 2000년대 서버간 도메인간 인증내역을 공유하는 SAML, WS-Federation, Identity Metasystem가 표준화되었으며, 2017년은 인증 크리덴셜의 신뢰 강도를 향상하는 방법에 대한 표준화를 추진

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ITU-T SG17 | ITU-T X.1141, 'Security Assertion Markup Language (SAML 2.0) | 2006 | 범용인증기술 |
| | ITU-T X.1250, Baseline capabilities for enhanced global identity management and interoperability | 2009 | |
| | ITU-T X.1251, A framework for user control of digital identity | 2009 | |
| | ITU-T X.1252, Baseline identity management terms and definitions | 2010 | |
| | ITU-T X.1253, Security guidelines for identity management systems | 2011 | |
| | ITU-T X.1254, Entity authentication assurance framework | 2012 | |
| | ITU-T X1158, Multi-factor authentication mechanisms using a mobile device | 2014 | |
| | ITU-T X.1159, Delegated non-repudiation architecture based on X.813 | 2014 | |
| ISO/IEC | ISO/IEC 10181-4:1997, Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework | 1997 | |
| | ISO/IEC 7816-5 Identification cards - Integrated circuit cards - Part 5: Registration of application providers | 2004 | |
| | ISO/IEC 21481 Information technology - Telecommunications and information exchange between systems - Near Field Communication Interface and Protocol -2 (NFCIP-2) | 2005 | |
| | ISO/IEC 7816-3 Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols | 2006 | |
| | ISO/IEC 7816-2 Identification cards - Integrated circuit cards - Part 2: Cards with contacts - Dimensions and location of the contacts | 2007 | |
| | ISO/IEC 14443-1 Identification cards - Contactless integrated circuit cards - Proximity cards - Part 1: Physical characteristics | 2008 | |
| | ISO/IEC 14443-4 Identification cards - Contactless integrated | 2008 | |

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| | circuit(s) cards - Proximity cards - Part 4: Transmission protoco | | |
| | ISO/IEC 13888-1:2009, Information technology - Security techniques - Non-repudiation - Part 1: General | 2009 | |
| | ISO/IEC 13888-3:2009, Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques | 2009 | |
| | ISO/IEC 14443-2 Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 2: Radio frequency power and signal interface | 2010 | |
| | ISO/IEC 13157-2 Information technology - telecommunications and information exchange between systems — NFC Security - Part 2: NFC-SEC cryptography standard using ECDH and AES | 2010 | |
| | ISO/IEC 13888-2:2010, Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques | 2010 | |
| | ISO/IEC 7816-1, Identification cards - Integrated circuit cards - Part 1: Cards with contacts - Physical characteristics | 2011 | |
| | ISO/IEC 14443-3, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anticollision | 2011 | |
| | ISO/IEC 7816-4, Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange | 2013 | |
| | ISO/IEC 18092, Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1) | 2013 | |
| | ISO/IEC 29115, Information technology — Security techniques — Entity authentication assurance framework | 2013 | |
| | ISO/IEC:29115, Information technology - Security techniques - Entity authentication assurance framework | 2013 | |
| | ISO/IEC 13157-1, Information technology - Telecommunications and information exchange between systems — NFC Security — Part 1: NFC-SEC NFCIP-1 security services and protocol(Revisions) | 2014 | |
| EMV | EMV 1.1, PayPass - ISO/IEC 14443, Implementation Specification | 2006 | |
| | EMV 4.3, Book1 - Application Independent ICC to Terminal Interface Requirements | 2011 | |
| | EMV 4.3, Book2 - Security and Key Management | 2011 | |
| | EMV 4.3, Book3 - Application Specification | 2011 | |
| | EMV 4.3, Book4 - Cardholder, Attendant, and Acquirer Interface Requirements | 2011 | |
| | EMV 2.6, Book D: Contactless Communication Protocol | 2016 | |
| FIDO | FIDO-UAF-V1.1, FIDO Universal Authentication Framework (UAF) V1.1 | 2017 | |
| W3C | W3C webauthn, Web Authentication: An API for accessing Public Key Credentials | 2017 | |
| OASIS | xri-syntax-v2.0, Extensible Resource Identifier(XRI) Syntax V2.0 | 2005 | |
| | saml-core-2.0, Security Assertion Markup Language | 2006 | |
| | identity-1.0, Identity Metasystem Interoperability | 2009 | |
| | ws-federation-1.2, WS-Federation V1.2 | 2009 | |
| | trust-el-protocol-v1.0, Authentication Step-Up Protocol and Metadata | 2017 | |
| IETF | RFC 4422, Simple Authentication and Security Layer (SASL) | 2006 | |

○ **(바이오인식 응용 서비스)** 바이오정보 보호기술은 JTC1 SC27에서, 바이오인식 시험기술은 JTC1 SC37에서 개발중이며, 텔레바이오인식 응용기술은 ITU-T SG17 Q9에서 개발 중

- (ISO/IEC SC27) ITU-T SG17과 공동으로 바이오인식기반 하드웨어 보안토큰은 개발완료
- (ISO/IEC SC37) C++기반의 바이오인식 호환규격 적합성 시험기술 개정작업은 완료됨. C#, JAVA 등 객체지향형 바이오인식 호환규격 적합성 시험기술을 개발 중
- (ITU-T SG 17 Q.9) 모바일기기용 텔레바이오인식 응용기술, 바이오인식기반 하드웨어 보안토큰은 개발완료. 스마트 ID카드를 이용한 원격 바이오 접근제어기술을 개발 중

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ITU-T SG17 | X.1087, A guideline to technical and operational countermeasures for telebiometric applications using mobile devices(X.tam) | 2017 | 바이오인식 응용 서비스 |
| | X.1085 \| ISO/IEC 17922, Telebiometric authentication framework using biometric hardware security module | | |
| | X.tac, Telebiometric Access Control with smart ID | 진행중 (2017) | |
| ISO/IEC JTC1 SC37 | 24709-1R1, Conformance Test for BioAPI Part1 revision | 2017 | |
| | 19794-15, Biometric data interchange format - Part 15: Palm crease image data | 2017 | |
| | 30106-1AMD1, Object oriented BioAPI -- Part 1: Architecture -- Amendment 1: Additional specifications and conformance statements | 진행중 (2017) | |
| | 30106-4, Information technology -- Object oriented BioAPI -- Part 4: C++ Implementation | | |
| ISO/IEC JTC1 SC27 | ITU-T X.1085 \| ISO/IEC 17922, Telebiometric authentication framework using biometric hardware security module | 2017 | 바이오인식 응용 서비스 |

○ **(생체신호기반 텔레바이오 인식기술)** 생체신호기반의 텔레바이오인식 인증기술은 ITU-T SG17 Q9(Telebiometrics)에서 개발 중

- (ITU-T SG17 Q9) 스마트워치 등 웨어러블 디바이스에서 생체신호 인증기술에 대한 상용화와 연구개발은 활발히 진행중이나, 생체신호 인증기술관련 표준화는 전무한 상태임. 이에 따라 KISA에서 ITU-T SG17 Q9을 통하여 표준화를 추진 중

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ITU-T SG17 | ITU-T X.tab, Telebiometric authentication using bio-signals | 진행중 (2017) | 생체신호기반 텔레바이오 인식기술 |

○ **(바이오인식기반 CCTV보안기술)** 바이오인식기반 CCTV 보안기술은 ISO/IEC JTC1 SC37에서 개발 중

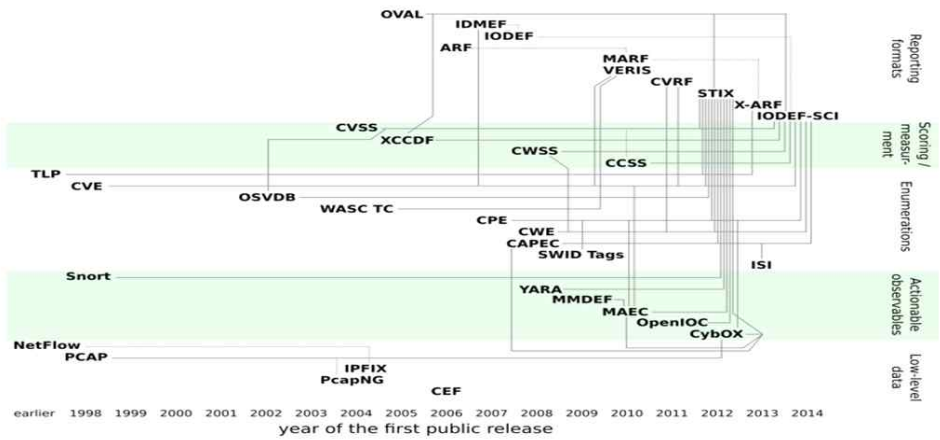
- (JTC1 SC37) 인하대에서 바이오인식기술을 이용한 지능형 CCTV 시험기술에 대한 국제표준 개발 중

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ISO/IEC JTC1 SC37 | ISO/IEC 30137-2, Use of biometrics in video surveillance systems -- Part 2: Performance testing and reporting | 진행중 (2017) | 바이오인식기반 CCTV 보안기술 |

○ **(보안 솔루션 위협정보 공유 및 연동 프레임워크)** 국외 표준은 ITU-T, IETF, OASIS를 중심으로 개발되어 왔으며, MITRE에서 개발한 사이버 위협 정보 전송 규격(TAXII)과 사이버 위협 표현 규격(STIX)에 대한 표준화 작업은 OASIS의 CTI(Cyber Threat Intelligence) 기술 위원회에서 진행 중

- (IETF) 침해사고 데이터형식인 IODEF(Incident Object Description Exchange Format)와 침해사고 추적 프로토콜인 RID(Real-time Inter-network Defense)를 표준화 진행 중
- (ITU-T SG17) 사이버보안에 대한 정보공유 프레임워크(CYBEX)에 대한 표준이 제정되었으며, 관련 메커니즘에 대한 표준화 작업이 지속적으로 진행 중. 침해사고 세션정보 교환 포맷에 대한 국제표준을 한국주도로 진행 중
- (OASIS) 2016년 사이버위협에 대응하기 위한 유관기관간의 침해사고 정보공유 포맷 및 협업형 통합제어 프레임워크 정의되고 있음
  · 사이버 위협정보 표현방식은 지속적으로 발전/통합되고 있으며, 또한 다른 위협정보의 내용과 연동성을 제공하는 기능들을 제공하는 방식으로 발전되고 있음




< 사이버 위협정보 표현방식 표준화 이력 >

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ITU-T SG17 | X.1209, Capabilities and their context scenarios for cybersecurity information sharing and exchange | 2010 | 보안 솔루션 위협정보 공유 및 연동 프레임워크 |
| | X.1500, Overview of cybersecurity information exchange (CYBEX) | 2011 | |
| | X.1500.1, Procedures for the registration of arcs under the | 2012 | |

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| | object identifier arc for cybersecurity information exchange | | |
| | X.1570, Discovery mechanisms in the exchange of CYBEX | 2011 | |
| | X.1520, Common vulnerabilities and exposures | 2011 | |
| | X.1541, Incident object description exchange format | 2012 | |
| | X.1580, Real-time inter-network defence | 2012 | |
| | X.1581, Transport of real-time inter-network defence messages | 2012 | |
| | X.1526, Open vulnerability and assessment language | 2013 | |
| | X.Suppl.18, ITU-T X.1205 - Supplement on guidelines for abnormal traffic detection and control on IP-based telecommunication networks | 2013 | |
| | X Suppl.20, ITU-T X.1205 - Supplement on framework of security information sharing negotiation | 2013 | |
| | X.1582, Transport protocols supporting cybersecurity information exchange | 2014 | |
| | X.1525, Common weakness scoring system | 2015 | |
| | X.1500 Appendix I - X.1500 (2011) Amendment 7, Overview of cybersecurity information exchange (CYBEX) | 2015 | |

○ **(유형별 보안성 시험평가기준)** JTC1 및 CCRA를 중심으로 IT 제품의 보안성 평가기준, 평가방법론, 암호모듈 시험기준, CC평가자 및 암호모듈 시험자 자격기준의 표준화가 진행 중

- (JTC1 SC27, CCRA) CCRA에서 개정 추진 중인 CC 및 CEM은 ISO/IEC JTC1과 협력하여 ISO/IEC 15408, ISO/IEC 18045로 개정 중이고 기존의 ISO/IEC 15408 part1/2/3에 part4/5를 추가하여 확장됨. 보호프로파일을 모듈화 적용하여 제품을 평가할 수 있도록 하고 평가방법과 활동 명세에 대한 프레임워크와 평가보증등급(EAL)과 같이 기존에 정의된 패키지에 대한 부분으로 세분화함. 기존 버전에서 개정된 버전으로 전환을 위한 가이드가 표준화로 진행중, CCRA에서는 CCRA 상호인정 효력이 실제적으로 작용되어 중복 평가에 따른 업체 부담을 축소해야 한다는 공통 입장을 고려하여 cPP와 cPP SD를 지속적으로 개발 추진 중에 있고, ISO/IEC JTC1 SC27에서는 ISO/IEC 19896-3 CC평가자 자격기준 국제표준화가 진행 중

- (JTC1 SC27, NIST) 암호모듈 시험 국제표준은 1994년에 NIST에서 발표한 FIPS 140-1에 뿌리를 두고 있으며, 현재는 2001년에 발표된 FIPS 140-2를 기반으로 하고 있음. 국제표준화는 보안 요구사항이 2006년 ISO/IEC 19790으로 제정되었으며, 2012년 개정됨. 암호모듈 시험 요구사항은 2008년 ISO/IEC 24759로 제정되었으며, 2014년 개정되고, 한국의 보완사항을 반영하여 2015년 ISO/IEC 19790/24759가 다시 개정됨. 현재 2015년 ISO/IEC 19790/24759 개정판이 미국 NIST CMVP의 FIPS 140-3으로 사용되기 위해 검토 중. ISO/IEC JTC1 SC27에서 ISO/IEC 20540 암호모듈 현장시험 가이드가 한국 주도로 표준화 진행 중에 있고 ISO/IEC 20543 난수발생기 시험방법, ISO/IEC 17825 물리적 비침투 공격 방어 시험기준, ISO/IEC 18367 암호알고리즘 구현 적합성 시험방법, ISO/IEC 19896-2 암호모듈 시험자 자격요건, ISO/IEC 20897 물리적 복제 불가기능 시험방법 등이 국제적 관심 속에서 제정되었거나 표준화 진행 중

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ISO/IEC | ISO/IEC 15408-1, Evaluation criteria for IT security Part1: Introduction and general model | 개정 진행중 (2021) | 정보보호제품 평가 |
| | ISO/IEC 15408-2, Evaluation criteria for IT security Part2: Security functional components | | |
| | ISO/IEC 15408-3, Evaluation criteria for IT security Part3: Security assurance components | | |
| | ISO/IEC 15408-4, Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities | 진행중 (2021) | |
| | ISO/IEC 15408-5, Evaluation criteria for IT security - Part 5: Pre-defined packages of security requirements | | |
| | ISO/IEC 18045, Methodology for IT security evaluation | 개정 진행중 | |
| | TBD, Introductory guidance on Evaluation for IT security | 진행중 (2021) | |
| | ISO/IEC 19790, Security requirements for cryptographic modules | 2015 개정 | 암호모듈 검증 |
| | ISO/IEC 24759, Test requirements for cryptographic modules | | |
| | ISO/IEC 20540, Guidelines for testing cryptographic modules in their operational environment | 진행중 (2019) | |
| | ISO/IEC 20543, Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408 | | |
| | ISO/IEC 19896-1, Competence requirements for information security testers and evaluators | | 시험 및 평가자 자격 |
| | ISO/IEC 19896-2, Competence requirements for information security testers and evaluators- Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers | | |
| | ISO/IEC 19896-3, Competence requirements for information security testers and evaluators-Part 3: Knowledge, skills and effectiveness requirements for CC evaluators | | |
| | ISO/IEC 18367, Cryptographic algorithms and security mechanisms conformance testing | | 암호모듈 검증 |
| | ISO/IEC 17825, Testing methods for the mitigation of non-invasive attack classes against cryptographic modules | 2015 | 암호모듈 검증 |
| | ISO/IEC 15446, Guide for the production of Protection Profiles and Security Targets | 개정 진행중 (2019) | 정보보호제품 평가 |
| | ISO/IEC 20897, Security requirements, test and evaluation methods for physically unclonable functions for generating non-stored security parameters | | 암호모듈 검증 |
| CCRA | Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5 | 2017 개정 | 정보보호제품 평가 |
| | Common Methodology for Information Technology Security Evaluation, Version 3.1, revision 5 | | |
| | collaborative Protection Profile for Stateful Traffic Filter Firewalls v1.0 | 2015 | |
| | collaborative Protection Profile for Full Drive Encryption - Encryption Engine v2.0 | 2016 | |
| | collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition v2.0 | 2016 | |
| | collaborative Protection Profile for Network Devices v2.0 | 2017 | |
| NIST | FIPS 140-2, Security Requirements for Cryptographic Modules | 2001 | 암호모듈 검증 |

○ **(정보보호 관리체계)** 법률에 의한 규제와 함께 ISO/IEC JTC1 SC27을 중심으로 하는 민간의 표준화 활동이 활발히 이루어지고 있으며, 에너지, 항공교통 등 중요 인프라 공격, 비즈니스 환경의 다각화에 따른 분야별 보안통제 실무지침의 인증기준 표준화 진행 중

- (ITU-T SG17) 적용 범위에 제약을 두지 않고 하나의 정보보호 관리체계의 표준에 대해 다양한 비즈니스 환경을 고려한 영역별로 특수한 환경 등 고려한 표준을 개발하고자 하는 움직임의 결과로 ISO/IEC JTC 1과 공동으로 통신(X.1051), 클라우드 서비스(X.1631) 분야를 위한 보안통제 실무지침을 개발하였으며, 중소 통신 조직의 환경을 고려한 정보보호 관리체계의 표준(X.sgsm)을 만들고자 하는 활동이 일본과 한국의 주도로 진행 중

- (ISO/IEC JTC1 SC27) ISMS Family를 표준 개발하고 있음. ISO/IEC 27002에 기초하여 통신(27011), 금융(27015), 클라우드 서비스(27017), 퍼블릭 클라우드 개인정보보호(27018), 에너지(27019), 의료(27799) 등 분야별 보안통제 실무지침 시리즈가 개발되었거나 작업 중. 2016년 ISO/IEC 27009 분야별 정보보호 경영체계 인증 요구사항 표준을 제정함. 이에 따라 클라우드, 통신조직 등 기존의 분야별 보안통제 실무지침을 ISO/IEC 27009의 요구사항에 따라 분야별 정보보호 경영체계 인증을 위한 표준으로 만들기 위한 연구(Study period)를 지속하고 있음

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ISACA | COBIT(Control Objectives for Information and related Technology) | 1996 | 정보보호 관리체계 |
| | (NSA) SSE-CMM(System Security Engineering capability maturity Model) | 1996 | |
| NIST | Security Self assurance Guide for IT system | 2001 | |
| ISO/IEC | ISO 27001, Information security management | 2013 | |
| | ISO 27002, Information technology - Security techniques - Code of practice for information security management | 2013 | |
| | ISO27007, Guidelines for information security management systems auditing (focused on the management system) | 진행중 (2020) | |
| | ISO27008, Guidance for auditors on ISMS controls (focused on the information security controls) | 진행중 (2020) | |
| | SO27009, Sector-specific application of ISO/IEC 27001-Requirements | 2016 | |
| ISO, ITU-T | ITU-T X.1051\|ISO/IEC 27011, - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organization | 2016 | |
| ITU-T | X.Sgsm - Information security management guidelines for small and medium-sized telecommunication organizations | 진행중 (2017.10) | |

○ **(개인정보보호 정책 및 운영관리 기술)** 개인정보보호 이슈로 인해 산업 분야별 특성을 반영한 제3자 인증의 필요성이 높아지고 있으며 ISO/IEC 29151과 ITU-T X.1058의 개인정보보호 관리체계 가이드가 2016년 표준으로 제정되고 이를 이용한 기존 분야별 보안통제 실무지침과 부속서의 개발이 진행 중

- (JTC1 SC27) 국내 표준전문가가 주도하여 개인정보보호 관리체계 표준인 “섹터기반 제3자

인증을 위한 27001의 이용 및 적용(ISO/IEC 27009)"와 "개인정보보호 지침(ISO/IEC 29151)" 등을 개발하여 2017년에 표준이 최종 승인되어 공개됨. 2014년 4월 홍콩 SC27회의에서 "통신조직을 위한 개인정보보호 지침"인 ITU-T X.gpim과 "개인정보보호지침"인 ISO/IEC 29151을 통합한 공통표준(ITU-T X.gpim | ISO/IEC 29151)의 개발 합의를 시작으로 ISO/IEC27009에 근거해 "개인정보보호 관리체계를 위한 추가적인 요구사항"에 대해 프랑스, 한국, 독일, 인도 등이 신규 워크아이템으로 제안하여 2016년 4월 미국 템파 SC27 회의에서 확정하고, 2017년 개발을 완료함. 개인정보 측면에서 개인정보보호 통제의 구현 가이던스인 부속서 등이 추가 개발되고 있음. 개인정보보호에 대한 통제 구현에 대한 권고가 마련되어 있었으나, 개인정보보호 활동의 특징을 반영한 프로세스에 대한 권고(ISO/IEC 27522)에 대한 개발이 추가로 필요함.

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ISO/IEC | ISO 13335, Information technology - Guidelines for the management of IT Security | 2008 | 개인정보보호 정책 및 운영 관리 기술 |
| | ISO 27001, Information security management | 2013 | |
| | ISO 27002, Code of practice for information security management | 2013 | |
| | SO/IEC 29151 Code of practice for personally identifiable information protection | 2017 | |
| | ISO/IEC 29134 Guidelines for privacy impact assessment | 2017 | |
| | ISO/IEC 29100 Privacy Framwork | 2011 | |
| | ISO/IEC CD 20889 Privacy enhancing data de-identification techniques | 진행중 (2018) | |
| | ISO/IEC 29190 privacy capability assessment model | 2015 | |
| | ISO/IEC 29101 privacy architecture framework | 2013 | |
| | IOS/IEC 29176 Consumer privacy-protection protocol for Mobile RFID services | 2011 | |
| | ISO/IEC 27550 Privacy engineering | 진행중 (2019) | |
| | ISO/IEC 27552 Enhancement to ISO/IEC 27001 for privacy management | 진행중 (2019) | |
| W3C | P3P(Platform for Privacy Preferences) 1.0 | 2002 | |
| | P3P(Platform for Privacy Preferences) 1.1 | 2006 | |
| OASIS | XACML(eXtensible Access Control Markup Language) 2.0 | 2005 | |
| | XACML(eXtensible Access Control Markup Language) 3.0 | 2013 | |
| ITU-T | X.1058 Code of practice for personally identifiable information protection | 2017 | |
| | X.sup-gpim Code of practice for personally identifiable information protection based on ITU-T X.1058 for telecommunications organizations | 2017 | |

○ **(빅데이터 데이터 보안)** 국제 표준화는 ISO/IEC JTC1에서 개발하고 있는 ISO/IEC WD 20889 표준과 NIST의 비식별 가이드라인이 활용되고 있으며, 최근 비정형 데이터의 비식별화 기술 및 온라인으로 오남용을 감지하는 참조 모니터 기술이 ITU-T를 중심으로 추진 중

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ISO/IEC | ISO/IEC CD 20889, Privacy enhancing data de-identification techniques | 진행중 (2018) | 빅데이터 데이터 보안 |
| NIST | NISTIR 8053, De-identification of Personally Identifiable Information | 2015 | |
| | Draft NIST SP 800-188, De-identifying Government Datasets | 2016 | |
| ITU-T | ITU-T X.fdip, Framework of de-identification Processing service for telecommunication service providers | 진행중 (2019) | |
| | ITU-T X.srfb, Security Requirements and Framework for Big Data Analytics in mobile Internet services | 진행중 (2018) | |

○ **(의료보안)** 국제 표준화는 ISO TC 215에서 중점적으로 개발 중

- (ISO TC215) '17년 5월 표준 총회에서 보건의료 개인정보 비식별화인 ISO 25237에 대한 작업과 의료 정보보호관리체계인 ISO 27799에 대한 개정되었으며, IoT 기반 스마트의료기기 보안인증 NP 제안 중
- (IEC SC27) 최근 의료기기에 대한 보안 취약성이 제기되고 있음에 따라 국내에서 의료기기 상호보안인증과 관련한 NP를 IEC 80001 Series에 제안하여 추진 중

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| ISO | IoT 기반 스마트의료기기 보안인증 (NP 제안 중) | 진행 중 (2020) | 의료보안 |
| | ISO 13485, Medical devices - Quality management systems - Requirements for regulatory purposes | 2016 | |
| | ISO 14971:2007 specifies a process for a manufacturer to identify the hazards associated with medical devices | 2007 | |
| IEC | IEC 80001-1, 네트워크에 연결된 개별 의료기기를 직접적으로 관리하기 어려운 환경에서 안전한 형태로 시스템을 관리하기 위한 요구사항 정의 | 2010 | |
| | IEC 62304, 안전한 의료기기를 위한 소프트웨어 개발관련 프로세스를 정의 | 2006 | |
| | IEC 60601-1, Medical electrical equipment - Part 1: General requirements for basic safety and essential performance | 2005 | |
| | IEC 62366-1, Medical devices — Part 1: Application of usability engineering to medical devices | 2015 | |

○ **(제조 보안)** 제조 분야 국제 표준화는 미국이 중심이 되어 추진되어 왔으나, 최근 독일을 중심으로 플랫폼 인더스트리 4.0과 RAMI 4.0을 내세우며 적극적으로 추진하고 있어 양대 세력이 앞장서고 있는 추세임

- IEC TC 65에서 보안과 관련된 주요 표준 문서는 IEC 61508 Functional Safety 전기/전자/프로그램 가능한 전자 안전 관리 시스템의 기능 안전과 IEC 62439 High Availability Automation Network 을 기본으로 살펴볼 수 있음
- 미국에서는 ISA-99/IEC 62443 국제표준을 통해 산업 자동 제어 시스템의 정보보호를 위한 구현 절차를 정의하는 표준, 기술보고서와 연계된 정보를 보급하고 있으며, 이 지침서는 사용자, 시스템 통합자, 안전점검자와 제어 시스템을 제작하는 기업에서 산업용 자동화 시스템에 대한 제조, 설계 구현과 관리를 위한 것으로서 산업제어시스템의 다양한 보안 표준들 가운데 가장 일반적인 표준으로 주목을 받고 있음
- 미국 국립표준기술원(NIST)에서는 SP(Special Publication) 800-82를 통해서 ICS(Industrial Control System) 기본개념 및 구성요소에 대해 정의하고, 이들에 대한 정보보호 개념을 IT 정보보호 기술과 비교하면서 IT 전문가들이 ICS를 이해할 수 있도록 가이드를 제시하고 있음
- SP800-82에는 정보보호 관리체계 구축에 필요한 정보보호 대책을 정의한 NIST SP 800-53을 ICS 관점에서 정리한 해설을 담고 있음. SP800-53 제정 당시에는 ICS를 고려하지 않았으나, 북미전기안전협회(NERC, North American Electric Reliability Corporation)가 제정한 CIP(Critical Infrastructure Protection) 시리즈를 참고하여 ICS 관점에서 정보보호대책을 SP 800-53 Rev 4(2015)에 규정
- 또한, 2010년 8월에 NIST IR(Interagency Report) 7628 Guidelines for Smart Grid Cyber Security를 발표하고, 이외에도 NERC CIP v5와 NIST IR 7628을 비교·분석하여 기술문서로 발표

< 국제 표준화 현황 >

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| IEC TC 65 | IEC 62443-1 Series 1 : 개념 모델, 용어 등 일반적인 사항 규정<br>- IEC 62443-1-1, 용어, 개념과 모델 정의<br>- IEC TR 62443-1-2, 사용하는 용어와 약어의 마스터 용어 정의<br>- IEC 62443-1-3, 내부 회계관리제도 보안을 위한 규정 준수 지표의 집합 식별<br>- IEC TR 62443-1-4, 내부 회계관리제도 보안 라이프사이클을 정의하고 사례 설명 | <br>2009.7<br>2009.7<br>2013.8<br>2013.8 | 제조보안 |
| | IEC 62443-2 Series 2 : 산업제어시스템을 보유하는 조직의 보안 정책과 관리시스템에 대해 규정<br>- IEC 62443-2-1, IACS(Industrial Automation and Control Systems) 보안 프로그램을 설정하는 방법 정의<br>- IEC TR 62443-2-2, IACS 보안 프로그램을 동작하는 방법 정의<br>- IEC TR 62443-2-3, 내부 회계관리제도의 환경에서 패치 관리를 위한 요구사항 | 2010.11<br>2010.11<br>2015.6<br>2015.6 | |

| 개발기구 | 표준(안)명 | 개발연도 | 관련 표준화항목 |
|---|---|---|---|
| | - IEC 62443-2-4, 내부 회계관리제도 공급 업체의 보안 정책과 관행의 인증 정의 | | |
| | IEC 62443-3 Series 3 : 시스템 통합을 위한 산업제어시스템에 대한 보안기능 요구사항을 규정하고 있는데, 요구사항으로는 식별, 인증(FR1), 사용제어(FR2), 시스템 무결성(FR3), 데이터 기밀성(FR4), 데이터 제한성(FR5), 응답성(FR6), 자원가용성(FR7)의 7가지 항목이 있으며, 산업제어시스템의 위험을 줄이기 위해 필요한 강도를 가진 요구사항(FR1 ~ FR7)을 선택하여 설계 및 구현 실시<br>- IEC TR 62443-3-1, 내부 회계 관리 제도의 보안에 적합한 기술에 관한 분석 보고서<br>- IEC 62443-3-2, 보안 보증 수준을 정의하는 방법을 다룸<br>- IEC 62443-3-3, 내부 회계 관리 제도의 보안에 대한 자세한 기술 요구 사항 정의 | 2009.7<br>2015.8<br>2013.8 | |
| | IEC 62443-4 Series 4 : 산업제어시스템을 구성하는 제어기기, 장비, 애플리케이션의 보안을 취급하는 장비 업체를 위한 보증 요구사항과 기능 요구사항이 규정될 예정이며, 현재 표준화 진행 중<br>- IEC 62443-4-1, 보안 내부 회계 관리 제도 제품 및 솔루션의 개발에 대한 요구 사항 정의<br>- IEC 62443-4-2, 시리즈 주소 자세한 기술 요구 사항 | 2016.6<br>2017.1 | |

## 2.7. 오픈소스 현황 및 전망

○ OpenSSL

- OpenSSL은 암호화 통신을 위한 대표적인 오픈소스 라이브러리로 TLS(Transport Layer Security) 및 SSL(Secure Sockets Layer)에 대한 높은 수준의 툴킷 및 범용 암호 라이브러리를 제공함. 1998년 12월 OpenSSL 프로젝트가 공식적으로 시작되었으며, 보안 취약점 보완 등 코드 개선 및 업그레이드를 진행하고 있음. 현재 1.1.0 시리즈가 배포되고 있음. 2006년 오픈소스 중 최초로 1.0버전에 대한 FIPS 140-2 검증을 받았으며, 2016년 7월 OpenSSL 1.1에 대한 FIPS 140-2 검증을 시작

○ OpenSSH

- SSH 터널을 통해 두 지점 사이의 트래픽을 암호화된 채널을 통해 안전하게 이동할 수 있도록 지원함. 윈도우즈에서는 putty와 winscp를 주로 사용하고 리눅스에서는 ssh와 scp 명령어를 통해 사용함. OpenSSH는 SSH 프로토콜 관련 다양한 명세서(specifications)를 구현하고 있으며, 2017년 3월 OpenSSH 7.5 버전이 출시

○ OWASP(The Open Web Application Security Project, OWASP)

- OWASP는 오픈소스 웹 애플리케이션 보안 프로젝트 임. 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며, 10대 웹 애플리케이션의 취약점 (OWASP TOP 10)을 발표 함. OWASP TOP 10은 웹 애플리케이션 취약점 중에서 빈도가 많이 발생하고, 보안상 영향을 크게 줄 수 있는 것들 10가지를 선정하여 2004년, 2007년, 2010년, 2013년을 기준으로 발표되었고, 문서를 공개

○ 기타 오픈소스 보안 툴

| 오픈소스 보안툴 | 설 명 |
|---|---|
| Nmap | 가장 널리 알려진 네트워크와 포트를 스캐닝 하는 툴임. Nmap은 네트워크 서비스에 관한 취약성, 잘못된 구성 및 보안 관련 정보를 탐지할 수 있는 NSE 스크립트를 제공함. |
| OpenVAS | Nessus가 사용화 될 때 엔진을 복제하여 만들어져 오픈소스 취약점 스캐닝 툴임. 웹기반의 대쉬보드를 통해 보안 취약점을 관리할 수 있음. |
| OSSEC | 호스트 기반의 침입탐지시스템으로 설치 및 구성이 쉬우며, 누구나 쉽게 사용할 수 있음 |
| Security Onion | 네트워크 보안모니터링 툴로 설치 및 구성이 쉬움. 최소한의 노력으로 APT를 포함한 네트워크 기반의 이상행위를 탐지할 수 있음 |
| Metasploit Framework | 공격자의 관점에서 보안의 수준을 테스트할 수 있음. 침투테스트 도구로 익스플로잇과 스캐닝 그리고 감사기능을 포함하고 있음 |

| 오픈소스 보안툴 | 설 명 |
|---|---|
| Wireshark | 트래픽을 캡쳐하여 분석할 수 있는 기능을 제공해 주는 오픈 소스툴로 다양한 OS 환경을 지원함 |
| Kali Linux | Back Track Linux 기반으로 만들어 졌으며, 데비안 기반의 보안 테스트를 위한 리눅스용 배포임. |
| Nikto | 10년이 넘은 웹서버 테스트 툴, 알려진 취약한 스크립트, 구성실수 및 관련 보안 문제를 찾기 위해 웹 서버에서 실행하기에 적합함 |
| Truecrypt | TrueCrypt는 2014년이후 유지관리가 되고 있지 않으나, 두 개의 새로운 보안 도구인 CipherShed와 VeraCrypt가 복제되어 모든 것을 암호화 할 수 있는 툴로 이용됨 |
| Moloch | 패킷캡쳐 분석 툴로 pcap으로부터 빠른 검색이 가능함. 캡쳐된 패킷의 디코딩을 지원하며 트래픽 분석에 유용한 툴임 |
| Bro IDS | 시그니처기반의 전통적인 IDS의 기능을 넘어 프로토콜을 디코딩 하고 트래픽 내에서의 특이점을 탐지할 수 있음 |
| Snort | 실시간 트래픽 분석 및 패킷 로깅 도구로서 전통적인 IDS와 유사하게 동작함. Suricata 시스템이 snort엔진에서 복제 되었음 |
| OSQuery | Facebook Security Team에서 시작한 크로스플랫폼으로 시스템에 에이전트 기반으로 동작하면서 이상 행위와 보안관련된 이벤트를 모니터링 할 수 있음 |
| GRR | Google 신속 대응 툴로 구글에 의해 보안 사고를 대응하기 위해 만들어진 툴로 파이썬 에이전트와 서버의 조합을 통해 사고 대응을 원격에서 수행할 수 있음 |

# Ⅲ. 국내외 표준화 추진전략

## 3.1. 표준화 SWOT 분석

<table>
<tr><th colspan="3">국내역량요인 / 국외환경요인</th><th colspan="2">강 점 요 인 (S)</th><th colspan="2">약 점 요 인 (W)</th></tr>
<tr><td colspan="3" rowspan="3"></td><td>시장</td><td>- 각종 보안 이슈 대응을 위해 기업 및 기관의 침해사고 대응장비 구매 증가<br>- 보안 필요성에 대한 높은 범사회적 인식</td><td>시장</td><td>- 세계 시장 대비 상대적으로 국내 보안시장 규모 협소<br>- 국내개발 암호기술의 제품 적용사례 미흡</td></tr>
<tr><td>기술</td><td>- 국제 경쟁력을 갖춘 범용 및 신규 ICT용 암호 기반기술 및 인증 응용기술 다수 확보<br>- 침해사고 대응체계 및 풍부한 경험 보유</td><td>기술</td><td>- 차세대 암호·인증 기술, 정보보호 관리체계 구축 등 관련 고급 개발인력 부족<br>- 의료, 제조 분야 등 융합보안 분야에서 보안기술 적용 미흡</td></tr>
<tr><td>표준</td><td>- 보안 분야에서 국내 전문가의 국제표준화 기여도 높음<br>- 국내 및 국제표준화 경험을 토대로 신규 표준화 활동 용이</td><td>표준</td><td>- 학계와 KISA, ETRI 등 정부기관 중심으로 표준화 진행하며, 산업체의 참여 미흡<br>- 표준화 전문인력 부족으로 다양한 표준화 기구를 통한 표준화 추진이 어려움</td></tr>
<tr><td rowspan="3">기회요인 (O)</td><td>시장</td><td>- 신규 ICT 환경에 기반한 범용/바이오 인증 서비스 시장 규모 확장</td><td colspan="3" rowspan="3">【SO전략】<br><br>-(시장)범용/바이오 인증 등 시장 확대 예상 분야에서 기존 인프라와의 결합을 통한 선점 효과 극대화<br>-(기술)국내 개발 차세대 암호·인증기술을 다양한 신규 ICT 보안에 활용하여 응용 측면의 융합보안 기술 확보<br>-(표준)ISO/IEC, ITU-T에서 활동 중인 국제 표준 전문가를 활용한 국제표준화 추진, 양자암호 암호안전성 기준 조기 수립 및 국내 표준화를 통한 관련 국제 표준화 주도</td><td colspan="2" rowspan="3">【WO전략】<br><br>-(시장)정보보호 관리체계 조기 구축을 통한 정보보호 관리영역 확대 및 클라우드, 빅데이터, 의료 등의 개인정보보호 제품 적용 분야 확대 추진<br>-(기술)국내 산업계의 요구사항을 반영한 소요기술 개발 및 제품 즉기 적용을 통한 제품 경쟁력 향상<br>-(표준)융합보안 관련 분과와 협력하여 보안기술 적용 표준 도출</td></tr>
<tr><td>기술</td><td>- 웹2.0, 클라우드, 빅데이터 등의 활성화에 따른 개인정보보호에 대한 지속적 수요<br>- 해킹기술의 고도화 등으로 정보보호 강화 요구 증가<br>- 적용환경 변화 및 취약요소 증가로 이에 적합한 새로운 암호 기술 개발소요 확대</td></tr>
<tr><td>표준</td><td>- ISO/IEC JTC1, ITU-T 등 국제표준화 기구에서 논의 초기단계인 양자암호 표준화 선도</td></tr>
<tr><td rowspan="3">위협요인 (T)</td><td>시장</td><td>- 다양한 보안 분야에서 글로벌 기업의 독점 우려<br>- 상호운용성 확보 및 개발 규모를 이유로 국내개발 암호기술의 제품 적용 기피</td><td colspan="3" rowspan="3">【ST전략】<br><br>-(시장)국내 환경 선적용을 통해 제품 인지도와 완성도를 제고하여 해외 시장 경쟁력 확보<br>-(기술)신규 ICT 서비스 중심의 암호·인증 원천기술 및 융합보안 기술 개발을 통한 국제 경쟁력 확보<br>-(표준)개발 기술의 적용 검험을 바탕으로 도출된 다양한 Use Case를 기반으로 표준화 초기 단계에서 주도권 확보 추진</td><td colspan="2" rowspan="3">【WT전략】<br><br>-(시장)국내 산·학·연 연계를 통한 기술 개발 및 활용의 선순환 체계 구축<br>-(기술)국책 연구개발 과제를 통한 IPR 획득 및 이를 통한 기술 및 서비스 제공<br>-(표준)활용성이 담보된 표준 개발을 통한 산업계 참여 확대 및 산업계 표준화 소요 조기 대응</td></tr>
<tr><td>기술</td><td>- 국가 차원의 보안 원천기술 확보 경쟁 심화<br>- 일부 국가와 기업에서 보안 핵심 원천기술 확보</td></tr>
<tr><td>표준</td><td>- 북미, 유럽 표준화 단체 중심의 국제 표준화 추진</td></tr>
<tr><td colspan="7">표준화 추진상의 문제점 및 현안 사항</td></tr>
<tr><td colspan="7">- 차세대보안 원천기술의 국내 산업경쟁력이 선진국대비 격차가 존재하나, 차세대 암호기술, 바이오 - 인증 기술 등 국제표준화에 적극적인 대응 추진<br>- 최신 비식별화 기술은 정보를 압축하거나 변형하여 필요한 경우 복원할 수 있는 기술이며, 제4차 산업혁명에 필요한 국가적 차원의 최신 비식별화 기술 확보 및 관련 특허 및 IPR의 선행적 확보 추진 필요</td></tr>
</table>

## 3.2. 중점 표준화 항목별 국내외 추진전략

○ 선행(선표준화 후기술개발), ◑ 병행(표준화&기술개발 병행추진), ● 후행(선기술개발 후표준화)

<table>
<tr><td rowspan="2">High<br><br>전략적 중요도<br>(IPR 확보 가능성, 시장/기술적 파급 효과, 정책 부합성 등)<br><br>Low</td><td>< 차세대공략 항목(신규제안) ><br><br>● 차세대 암호기술<br>◑ 보안 솔루션 위협정보 공유 및 연동 프레임워크<br>◑ 빅데이터 데이터 보안<br>◑ 의료보안<br>◑ 제조 보안</td><td>< 적극공략 항목(선도경쟁) ><br><br>◑ 범용인증기술<br>◑ 바이오인식 응용 서비스<br>◑ 생체신호기반 텔레바이오 인식기술<br>◑ 바이오인식기반 CCTV보안기술<br>◑ 유형별 보안성 시험평가기준<br>◑ 정보보호 관리체계<br>○ 개인정보보호 정책 및 운영관리 기술</td></tr>
<tr><td>< 전략적수용 항목(수용/적용) ></td><td>< 다각화협력 항목(부분협력) ><br><br>● PKI 기반 인증 및 응용기술</td></tr>
<tr><td></td><td colspan="2">Low 국내 역량 (표준화/기술개발 수준, 국제 표준화에 국내 기여도 등) High</td></tr>
</table>

○ 영역별 특징 및 대응전략

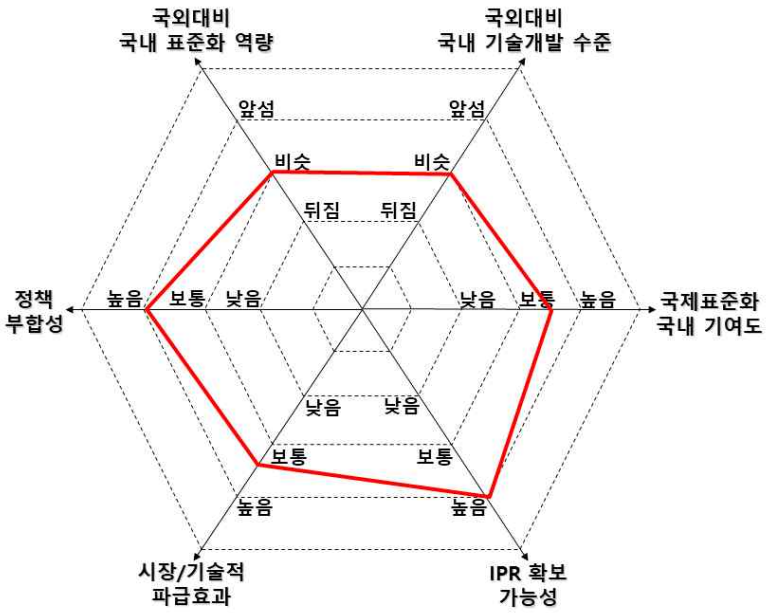
- **차세대공략 항목(신규제안)** : 미래 핵심기술 및 유망서비스 관련 선행적 표준화 분야
  : 국제표준 기획단계부터 주도적 참여를 통해 국제표준화 선도기반 확보
  : 기술 및 특허 반영을 위한 원천기술 개발 병행 (기술개발-표준화 연계 강화)

- **적극공략 항목(선도경쟁)** : 아직 국제표준 완성도가 낮아 국제표준 선도경쟁이 치열한 분야
  : 국내 기술의 국제표준 반영을 위한 표준화 활동 강화
  : 전략적 대외협력 강화 및 제휴를 통한 기술/표준의 Catch-up 전략 추진

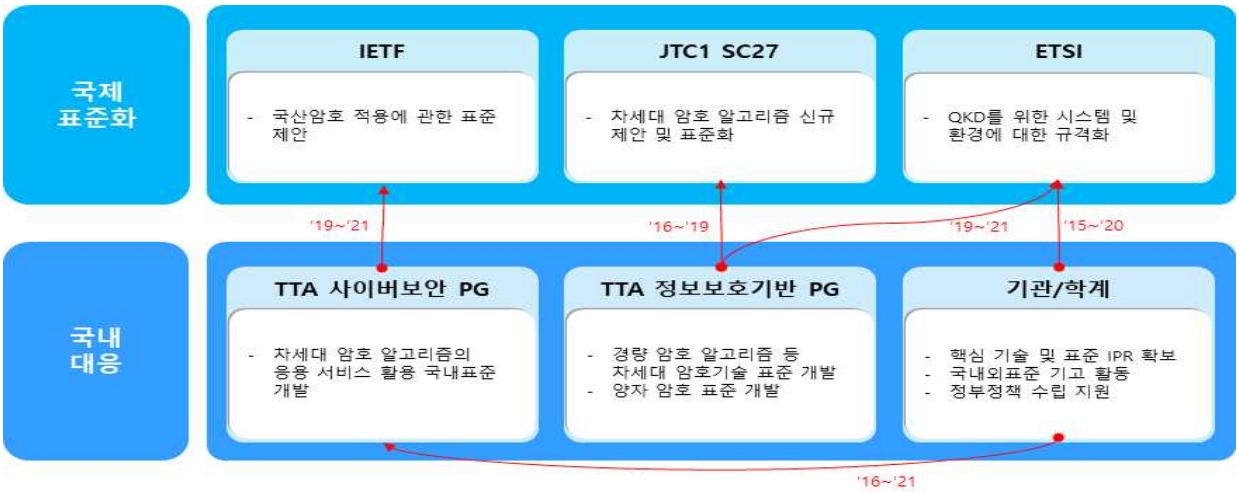
- **다각화협력 항목(부분협력)** : 시장에서의 기술/상용화 경쟁이 치열한 분야로 포럼/컨소시엄 위주의 표준화가 진행되는 분야
  : 세계 사실표준화기구 대응 및 국내 포럼 활동 강화
  : 사실표준화기구와 공식표준화기구에 다각적인 대응 모색

- **전략적수용 항목(수용/적용)** : 기술개발 및 국제표준화가 거의 완료단계이고, 서비스/시장 확산을 위한 후속 표준화가 필요한 분야
  : 국제표준의 수용/적용을 통한 국제 호환성 확보 및 국내 시장 확산
  : 킬러 애플리케이션/서비스 개발과 병행하여 틈새표준 발굴, 표준화 추진

## (차세대공략 | 후행) 차세대 암호기술

<table>
<tr><td rowspan="3">전략적 중요도 / 국내 역량</td><td colspan="2" rowspan="3"> 
</td><td rowspan="3">표준화 기구/ 단체</td><td>국내</td><td>TTA 정보보호 기반 PG, 사이버보안 PG</td></tr>
<tr><td>국제</td><td>JTC1 SC27, IETF, ETSI</td></tr>
<tr><td>국내 참여 업체/ 기관</td><td>NSR, KISA, ETRI</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="2">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td><td>기술 수준</td><td>90% (선도국가대비)</td></tr>
<tr><td>국외</td><td colspan="2">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td><td>기술 격차</td><td>1년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국/NSR, 일본/NTT, 벨기에/COSIC, 미국/NSA, 스위스/IDQ</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="2">□과제기획↦□과제승인↦■개발↦□검토↦□표준채택</td><td>표준 수준</td><td>95% (선도국가대비)</td></tr>
<tr><td>국제</td><td colspan="2">□과제기획↦□과제승인↦□개발↦■검토↦□표준채택</td><td>표준 격차</td><td>0.5년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">미국/NIST, 일본/Sony, 벨기에/COSIC</td></tr>
</table>

- Trace Tracking : 차세대공략(Ver.2017) → 차세대공략(Ver.2018)
  차세대 암호기술의 경우 블록 암호 LEA, 형태보존 암호 FEA를 제외하고 확보된 기술이 없기 때문에 신규 기술개발을 통한 확보가 필요한 상황이며, 현재 미국 등의 자국 암호기술 위주 표준화 추세에 대응하고 표준화 리더십을 확보하기 위하여, 암호기술 활용성 강화와 국제 협력 추진이 우선 필요하다고 판단되어, Ver.2018에서도 “차세대공략” 항목으로 분류

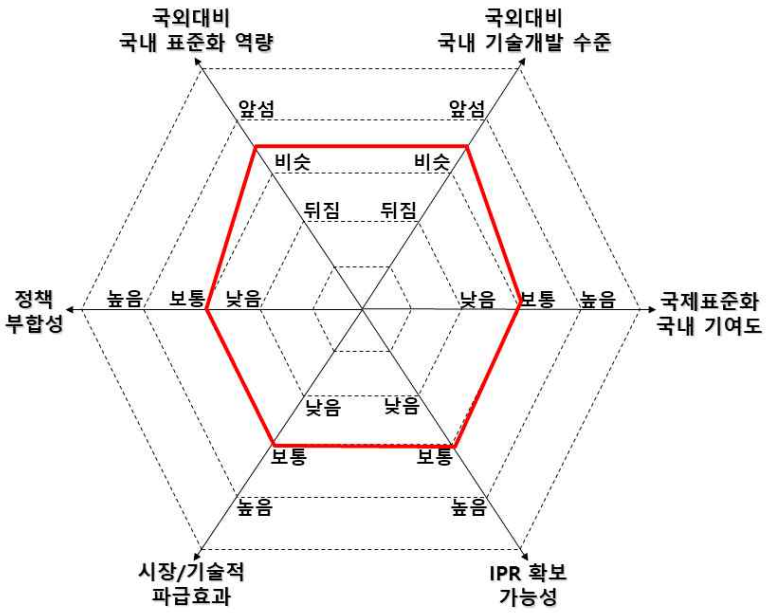



**<국제표준화 대응체계>**

| | |
|---|---|
| **국제 표준화 대응 방안** | **<현황>**<br>- 차세대 암호기술 중 경량 암호와 동형 암호는 ISO/IEC JTC1 SC27을 통해서 표준화가 추진 중<br>- 양자 암호는 ETSI를 중심으로 도시바, IDQ 등 양자 암호 선도업체 중심의 표준화가 진행 중<br>**<경쟁표준/기구의 전략>**<br>- 차세대 암호기술 중 경량, 고속 암호기술과 관련하여 ISO 수준으로 알고리즘 규격에 대한 표준화를 진행하는 기구는 없음<br>- 암호기술의 표준화는 ETSI가 주도하고 있으며, 시스템 구축 측면으로 진행 중<br>**<대응방안>**<br>- (국제표준화기구 신규 과제 제안) 현재 NSR은 블록 암호 LEA를 JTC1 SC27의 경량 블록 암호 표준(29192-2)에 포함시키는 것을 제안하여 WD 단계를 진행 중. Editor 수임을 비롯한 JTC1 SC27 WG2 에서 정부 기관 및 국내 학계와의 공조 체계를 구축하고, 미국, 중국, 러시아 등 타국과 협력 체계 구축(상호지지 등)을 통해 표준화 주도<br>- (기타) 현재 퀀텀포럼이 ETSI 양자 암호 표준화에 참여하고 있으나, 국내 양자 암호통신 기술기반 미흡으로 관련 논의를 주도하지는 못하는 상황임. 따라서 먼저 정부 기관, 국내 학계, 퀀텀포럼 간 공조체계를 갖추어 국제표준화에 기여하는 것이 필요 |
| **국내 표준화 추진 계획** | **<현황>**<br>- 경량 블록 암호, 형태보존 암호 등 일부 상용화 가능한 차세대 암호기술에 대한 국내 표준화는 이미 완료됨<br>- NSR은 양자 암호통신 중 안전성과 관련된 양자 암호기술에 대한 표준화 추진을 제안하였고, 세종대 및 퀀텀포럼은 ETSI의 양자 암호통신 표준 도입을 추진 중<br>**<추진계획>**<br>- 연구개발 표준화 연계 개발<br>- (세부전략 - 차세대 암호기술) 원천기술 개발을 시작으로 JTC1 SC27 WG2에서 추진 중인 국제표준화 대응하고, 기 확보 기술을 학계나 기업과의 협력을 통해 프로토콜 적용 규격 개발을 통한 활용성 강화와 TTA 정보보호기반 PG, 사이버보안 PG를 통한 국내 표준화를 선제 추진<br>- (세부전략 - 양자 암호기술) 국내 산업체의 양자 암호 시스템화 연구개발을 바탕으로 선제적 표준화 기반 마련 추진. 특히 양자 암호의 상용화 지원을 위한 시스템 요소와 개발 장비의 안전성 보장을 위한 암호 안전성 요소를 분리하여 표준화를 추진 |
| **표준 특허 전략** | **- 표준 및 R&D 중후기 전략 : 특허 권리범위 보완전략**<br>- (세부전략) 최적 구현 기술의 개발을 통해, 표준을 적용하는 제품 개발 시 제품의 성능 향상에 영향을 줄 수 있는 특허를 확보하고 상황에 변화에 따라 추후 권리범위를 보안 |
| **기술개발 -표준화 -IPR 연계 방안** | - 기술개발 후속 표준화<br>- (세부전략 - 차세대 암호기술) 우수 성능의 암호기술을 개발을 기반으로 응용서비스에 최적화된 암호 알고리즘 구현기술에 대한 특허를 확보함. 이와 동시에 신규 서비스에서의 시장선도 및 다양한 응용서비스에서의 상호 운용성 확보를 위한 암호기술 규격의 표준화를 추진<br>- (세부전략 - 양자 암호기술) 안전성 검증과 연계된 양자 암호기술, 양자 암호시스템과 현대암호 연동기술 관련 특허를 확보함. 또한 이를 활용한 시스템화 기술 표준화 |

## (다각화협력 | 후행) PKI 기반 인증 및 응용기술

**전략적 중요도 / 국내 역량**




**표준화 기구/단체**

| | |
|---|---|
| 국내 | TTA 정보보호 기반 PG |
| 국제 | JTC1 SC27, ITU-T SG17, FIDO Alliance, W3C |
| 국내 참여 업체/기관 | KISA, 공인인증기관, 기기인증기관, PKI 포럼, 보안업체 등 |

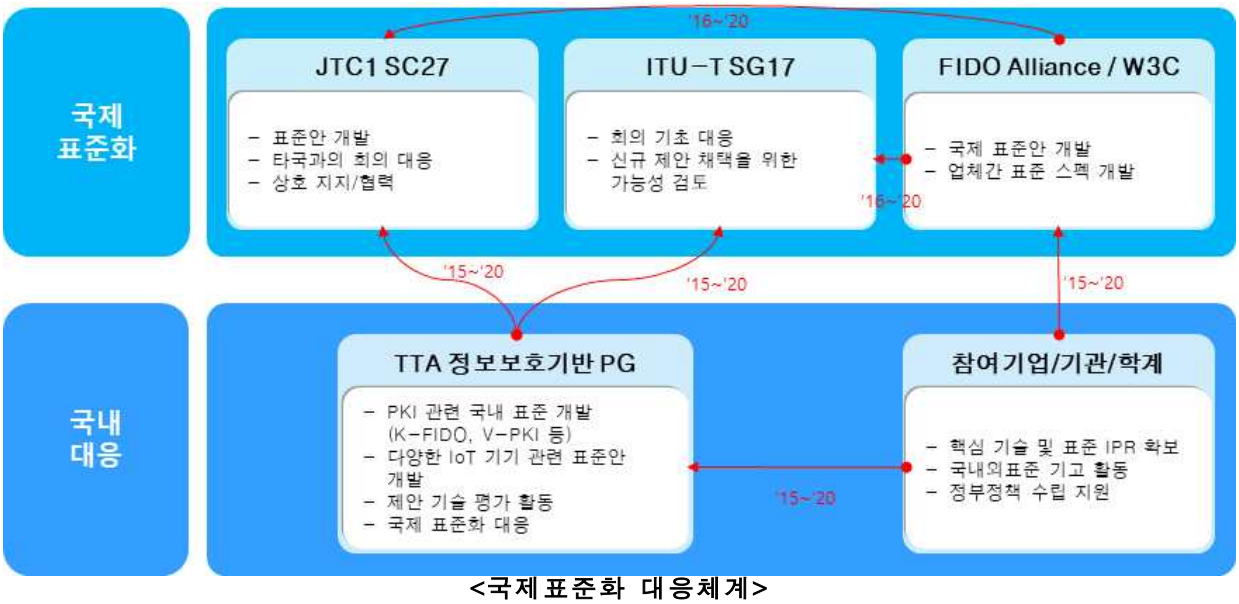
**기술 개발 단계**

| | | | |
|---|---|---|---|
| 국내 | □기초연구↦□실험↦□시작품↦□제품화↦■사업화 | **기술 수준** | 95% (선도국가대비) |
| 국외 | □기초연구↦□실험↦□시작품↦□제품화↦■사업화 | **기술 격차** | 0.5년 |
| 선도국가/기업 | 한국/ ETRI, KISA(공인인증기관 포함), PKI보안업체, 기기인증업체, 바이오인증 업체<br>미국 / Symantec, Qualcomm, RSA, NokNok Labs | | |

**표준화 단계**

| | | | |
|---|---|---|---|
| 국내 | □과제기획↦□과제승인↦■개발↦□검토↦□표준채택 | **표준 수준** | 95% (선도국가대비) |
| 국제 | □과제기획↦□과제승인↦□개발↦■검토↦□표준채택 | **표준 격차** | 0.5년 |
| 선도국가/기업 | 한국/ ETRI, KISA, TTA<br>미국 / Symantec, Qualcomm, RSA, FIDO Alliance, Google, Microsoft | | |

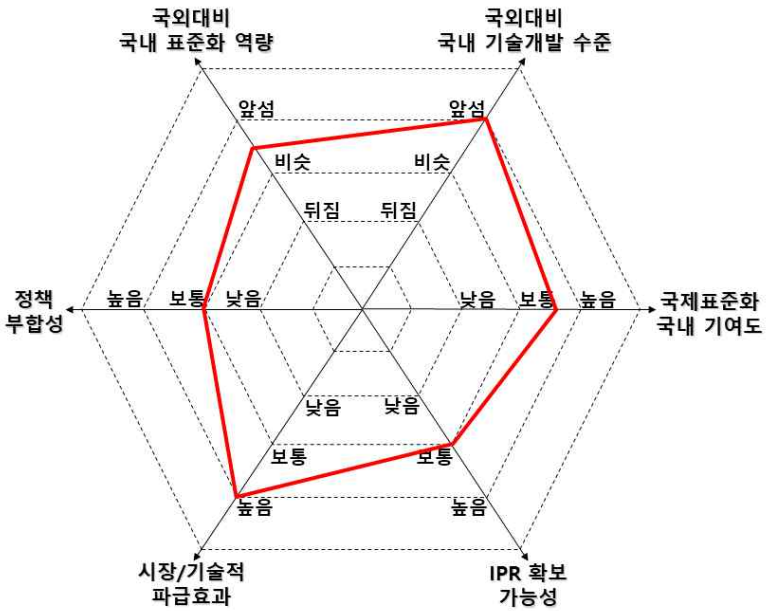
- **Trace Tracking** : 다각화협력(Ver.2017) → 다각화협력(Ver.2018)
  상황인지 기반의 사용자 인증 방식과 다양한 IoT 기기에 대한 인증의 수요가 증가하고 있음, 특히 FIDO 기반 바이오 인증 분야에서는 기존 인증 인프라와 결합하여 우리나라가 주도 가능하며 부가가치가 높은 항목으로 판단되나, 표준개발은 FIDO Alliance의 미국 기업 중심으로 주도하고 있기 때문에 "다각화협력"으로 분류



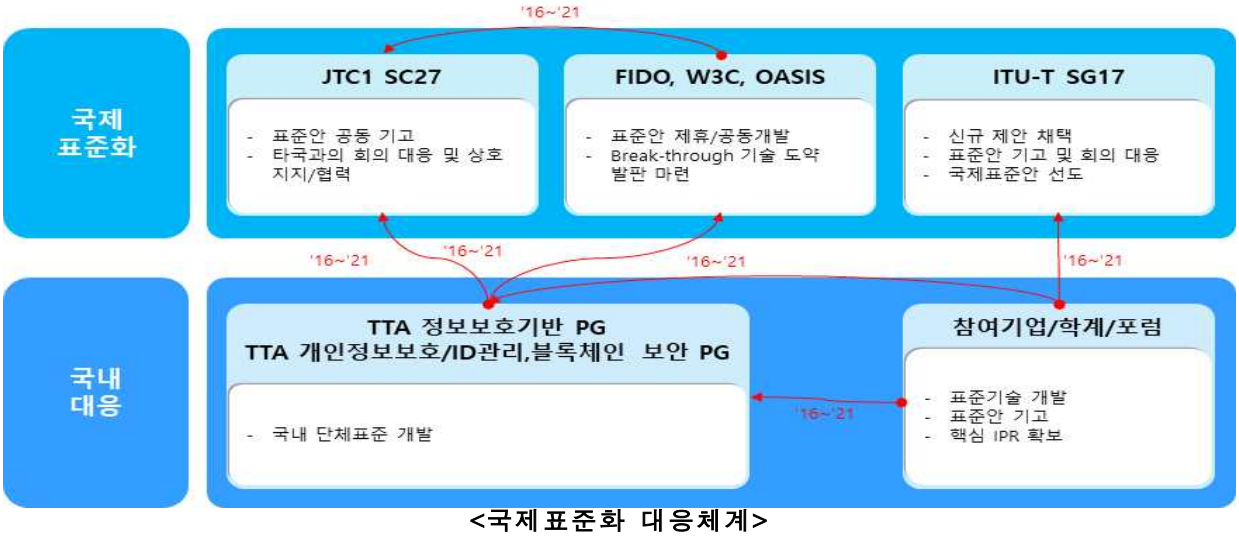

**<국제표준화 대응체계>**

| | |
|---|---|
| 국제 표준화 대응 방안 | **<현황>**<br>- ITU-T SG17, ISO/IEC JTC1 SC27 등에서 IPTV, CCTV, Smart Grid 등 다양한 디바이스에 대하여 국제표준화가 활발히 추진 중이고 FIDO Alliance와 W3C를 통하여 FIDO 2.0 표준화가 진행 중이고 향후 스마프폰에서 PC로 바이오인증 분야의 확산에 기여할 것임<br>**<경쟁표준/기구의 전략>**<br>- 산업계 표준단체인 FIDO Alliance 워킹그룹의 적극 참여를 통해 사용자 인증강화를 위한 표준프레임웍 표준화 지원 및 FIDO와 PKI 연계 방안에 대한 표준화 추진 예정<br>**<대응방안>**<br>- (사실표준화기구 활동) 국내 공인인증서의 비밀번호를 FIDO와 결합한 기술개발을 경험을 바탕으로 FIDO Alliance의 산업표준에 포함하는 방안 추진 |
| 국내 표준화 추진 계획 | **<현황>**<br>- KISA를 중심으로 바이오정보 연계 등 스마트폰 환경에서 공인인증서 안전 이용 구현, 간편 공인인증서 인터페이스 가이드라인, 공인인증서와 FIDO와 결합하여 편리성과 안전성이 강화된 공인인증서 등에 대한 국내 표준화 추진<br>**<추진계획>**<br>- (표준화 포럼 활동) KISA, TTA 등 국내 표준화 인프라를 활용하여 다양한 바이오 인증기술에 대한 표준 주도하여 국내 주도권 확보하고 FIDO Alliance내 한국 WG을 창설통한 효율적이고 적극적인 국내표준화 추진하는 전략이 요구됨, 또한 국내 공인인증서의 비밀번호를 FIDO와 결합한 생체기반 공인인증서 기술의 국내 표준화 진행 |
| 표준 특허 전략 | - **표준 및 R&D 중후기 전략 : 특허 권리범위 보완전략**<br>- (세부전략) 사용자 인증의 강화로 멀티팩터 인증의 증가하매 따라 바이오인증 방법의 증가하고 있고 다양한 기기에서 출현 및 사용 증가에 따른 IoT 기기인증 분야의 중요성이 높아짐에 따라서 인증에 대한 필수 기술을 특허화 하고 상황에 변화에 따라 추후 권리범위를 보안 |
| 기술개발 -표준화 -IPR 연계 방안 | - 기술개발 후속 표준화<br>- 금융권에서 OTP의 대체방안으로 바이오인증을 제공 중이고 PKI 분야에서도 FIDO기반의 바이오인증과 결합한 생체기반 공인인증서 기술개발되어 서비스 중<br>- 자율주행을 위한 프라이버시 보호형 차량인증체계(Vehicular PKI)의 연구개발이 진행 중이고 이를 통해 국제표준화, IPR 확보를 추진 필요<br>- 인터넷전화, 셋탑박스, IPTV, CCTV, Smart Grid, 자율주행차 등의 사물인터넷(IoT) 분야에서도 다양한 기기간의 인증을 위한 인증체계와 연계된 기술개발 추진 |

## (적극공략 | 병행) 범용인증기술

<table>
<tr><td rowspan="3">전략적 중요도 / 국내 역량</td><td colspan="2" rowspan="3"> 
</td><td rowspan="3">표준화 기구/ 단체</td><td>국내</td><td>TTA 정보보호 기반 PG, 개인정보보호 및 ID관리 PG,</td></tr>
<tr><td>국제</td><td>ITU-T SG17, JTC1 SC27, W3C, FIDO Alliance, OASIS</td></tr>
<tr><td>국내 참여 업체/ 기관</td><td>공인인증기관, TTA, ETRI</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="2">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td><td>기술 수준</td><td>100% (선도국가대비)</td></tr>
<tr><td>국외</td><td colspan="2">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td><td>기술 격차</td><td>0년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국 / 공인인증기관, ETRI<br>미국 / VeriSign, EMV, IBM, VISA, Google, Microsoft</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="2">□과제기획↦□과제승인↦□개발↦■검토↦□표준채택</td><td>표준 수준</td><td>95% (선도국가대비)</td></tr>
<tr><td>국제</td><td colspan="2">□과제기획↦□과제승인↦□개발↦■검토↦□표준채택</td><td>표준 격차</td><td>0.5년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">미국 / IBM, VISA, Google, Microsoft<br>유럽 / EMV<br>한국 / 공인인증기관, ETRI, 금융결제원</td></tr>
</table>

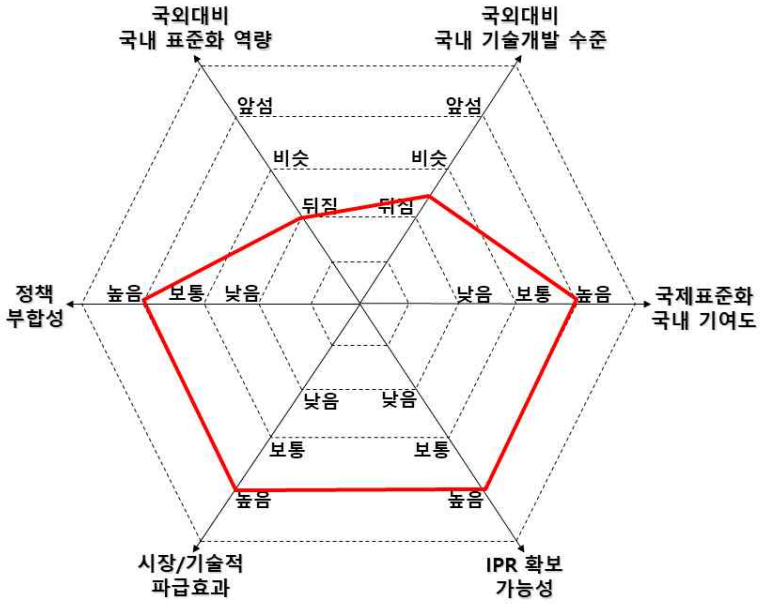
- **Trace Tracking** : 적극공략(Ver.2017) → 적극공략(Ver.2018)
  범용인증기술은 금융분야에서부터 통합인증서비스를 시작하였으며, 2011년 ITU-T에서 OTP기술을 기반으로 한 통합인증 표준인 X.1153이 완료되었음. 또한 I-PIN, ID 관리, 금융IC카드에 대한 표준화가 진행되어 왔으며, 2015년 핀테크 인증기술인 FIDO 유니버셜 인증 프레임워크 표준을 제정. 이처럼, 한국 주도로 개발되는 통합인증 표준은 향후 타 국가에서의 활용 가능성과 관련 산업의 부가가치가 높은 항목으로 판단되며, 글로벌 기업이 참여하는 FIDO Alliance 등의 활발한 표준화가 진행될 것으로 예상되어 Ver.2017과 마찬가지로 적극공략으로 분류




<국제표준화 대응체계>

| | |
|---|---|
| 국제 표준화 대응 방안 | **<현황>**<br>- ITU-T SG17을 통해 통합인증 서비스 프레임워크가 표준화되었으며 한국 주도로 스마트 환경의 보안성 향상을 위한 국제 표준안이 완료됨<br>- ISO/IEC JTC1 SC27는 개체 인증 보증 프레임워크를 제정하였으며, 전통적인 IC카드 표준이 접촉식은 ISO7816로 비접촉식은 ISO14443로 표준화가 진행됨<br>- FIDO Alliance는 FIDO Universal Authentication Framework 표준안을 제정한 후, 현재 FIDO 2.0 표준안을 W3C에 제안하여 2017년 현재 W3C에서 "Web Authentication: An API for accessing Public Key Credentials" 표준화가 진행 중<br>- OASIS는 서버간 도메인간 인증내역을 공유하는 SAML, WS-Federation, Identity Metasystem가 표준화되었으며, 인증 크리덴셜의 강도를 향상시키는 프로토콜에 대한 표준화를 추진 중<br>**<경쟁표준/기구의 전략>**<br>- ITU-T SG17의 통합인증 서비스 프레임워크와 ISO/IEC JTC1 SC27차 개체 인증 보증 프레임워크, FIDO Alliance와 W3C의 FIDO 2.0 표준화, OASIS의 인증 크리덴셜 강도를 향상시키는 프로토콜 표준화를 통해 각 기구별로 범용인증기술을 플랫폼 수준으로 표준화 진행 중<br>**<대응방안>**<br>- (국제표준화기구 신규 과제 제안) 현재 ETRI는 에디터로서 ISO/IEC JTC1 SC 27에서 인증키 관리 메커니즘에 대한 표준화를 진행 중이며, ITU-T SG17에서 클라이언트-서버 모델에서 hybrid 인증 및 키 관리 메커니즘에 대한 가이드라인 표준화를 진행 중. 또한 PKI, 바이오, OTP 등의 다양한 인증기술을 통합하여 제공 가능한 범용 인증체계를 개발하고 ISO, ITU-T, FIDO Alliance 등의 국제표준화기구에서의 기초대응을 수행 중 |
| 국내 표준화 추진 계획 | **<현황>**<br>- 인증기관, 인증서비스 기관, 인증기술 개발업체 간의 협의를 통하여 시장 변화에 따른 범용 인증체계 관련 표준 아이템 개발 및 국외 표준화(ITU-T, ISO, W3C, OASIS 등)의 준용을 추진하는 상황이나, 환경/상황정보 등에 기반한 차세대 인증요소 기술에 대한 표준화는 진행되지 않음<br>**<추진계획>**<br>- (표준화위원회 PG 활동) TTA PG501에서 차세대 인증요소 기술규격을 제정하고, TTA PG502에서 FIDO와 공인인증서를 결합하여 안전한 전자서명 이용환경을 제공하기 위한 기술규격 및 개인정보 유출 확산 방지, O2O 환경에서의 주민번호 대체 등 현안 문제 해결을 위한 범용인증기술 표준 제정 예정 |
| 표준 특허 전략 | - **표준 및 R&D 중후기 전략 : 특허 권리범위 보완전략**<br>- (세부전략) 공인인증서, OTP, 바이오인식(지문, 홍채, 음성, 행동) 기술 등의 다수의 인증기술과 쉽게 연계할 수 있는 IC카드와 스마트기기와 연계한 다중요소 인증기술이 IPR 확보 가능 분야이며, 산·학·연의 긴밀한 연계 및 공통 작업을 통해 IPR 확보를 추진하고 상황에 변화에 따라 추후 권리범위를 보안 |
| 기술개발 -표준화 -IPR 연계 방안 | - 표준화-기술개발 병행추진<br>- (세부전략) FIDO 인증 기술과 같이 범용인증기술은 산업에 즉시 활용될 수 있으므로 기술 개발과 동시에 표준화를 병행 추진함으로써 기술의 파급효과를 높이며 더 많은 부가가치를 창출하는 IPR을 확보함 |

## (적극공략 | 병행) 바이오인식 응용 서비스

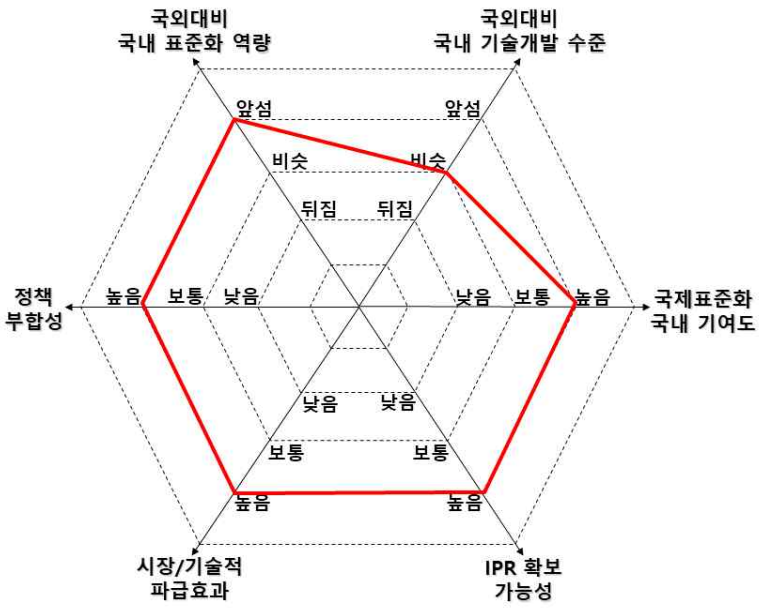
<table>
<tr><td rowspan="3">전략적 중요도 / 국내 역량</td><td colspan="2" rowspan="3"> 
</td><td rowspan="3">표준화 기구/ 단체</td><td>국내</td><td>TTA<br>바이오인식 PG,<br>KBID</td></tr>
<tr><td>국제</td><td>JTC1 SC37,<br>ITU-T SG17,<br>ABC</td></tr>
<tr><td>국내 참여 업체/ 기관</td><td>KISA, ETRI,<br>인하대, 충북대,<br>경인여대,<br>슈프리마,<br>유니온 커뮤니티</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="2">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td><td>기술 수준</td><td>85%<br>(선도국가대비)</td></tr>
<tr><td>국외</td><td colspan="2">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td><td>기술 격차</td><td>1년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국/삼성전자<br>미국/애플<br>일본/NEC</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="2">□과제기획↦□과제승인↦■개발↦□검토↦□표준채택</td><td>표준 수준</td><td>80%<br>(선도국가대비)</td></tr>
<tr><td>국제</td><td colspan="2">□과제기획↦□과제승인↦■개발↦□검토↦□표준채택</td><td>표준 격차</td><td>2년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국/KISA<br>미국/NIST<br>영국/NPL<br>프랑스/Sagem Morpho<br>중국/알리바바<br>일본/NTT 도코모</td></tr>
</table>

- **Trace Tracking** : 다각화협력(Ver.2017) → 적극공략(Ver.2018)
  모바일 바이오인식기술, 바이오인식 융합기술 등의 내용을 포함하여 헬스케어, 핀테크, 스마트카 등 다양한 IoT 환경분야에서 비대면 인증수단으로 바이오인식 국산기술을 널리 활용함에 따라 Ver2018에서도 적극공략으로 분류


| | |
|---|---|
| 국제 표준화 대응 방안 | **<현황>**<br>- ITU-T SG17 Q9(Telebiometrics)와 ISO/IEC JTC1 SC37간 Liaison officer를 한국(KISA)에서 담당하고 있으므로, 바이오인식분야 공적표준화 활동에 주도적인 역할을 수행하는 중임<br>**<경쟁표준/기구의 전략>**<br>- 미국 NIST, 유럽 EAB(협의회) 등에서 ISO/IEC 30107(PAD) 등 바이오인식 위변조 탐지기술, 표준적합성 시험기술과 연계하여 국제협력체계 구축<br>**<대응방안>**<br>- (국제표준화기구 의장단 수임) ABC(아시아지역 바이오인식 협력체)와 협력하고 ISO/IEC JTC1 SC37, ITU-T SG17/Q9에서 관련표준의 에디터쉽을 확보하여 ISO/IEC 30106-1AMD1, 30106-4, ITU-T X.tac 등에 대한 국제표준화를 진행 중 |
| 국내 표준화 추진 계획 | **<현황>**<br>- TTA PG505, KBID, KISA 표준연구회를 중심으로 활발히 바이오인식분야 국내표준 및 국제표준 개발에 박차를 가하고 있음<br>**<추진계획>**<br>- (연구개발 표준화 연계 개발) KISA가 추진중인 IITP “텔레바이오인식기술 표준개발” 과제의 일환으로 바이오인식 시험기술, 텔레바이오인식 응용기술 등에 관한 표준개발을 추진 중<br>- (국내 표준화 활동기반 마련) KISA 텔레바이오인식기술 표준연구회에서 산학연 전문가그룹과 협력을 통하여 바이오인식 응용서비스에 대한 국내표준화 추진 중 |
| 표준특허 전략 | - **표준 초중기 및 R&D 중후기 전략: 표준 필수특허 설계전략**<br>- (세부전략) ISO/IEC 30106-1AMD1, 30106-4 등 바이오인식 시험기술관련 개발중인 국제표준에 대한 필수특허 출원 추진 예정 |
| 기술개발-표준화-IPR 연계 방안 | - 표준화-기술개발 병행추진<br>- (세부전략) KISA 바이오인식 표준적합성 시험기술 개발과 병행하여 ISO/IEC JTC1 SC37 국제표준화 추진 중 |

## (적극공략 | 병행) 생체신호기반 텔레바이오 인식기술

**전략적 중요도 / 국내 역량**




**표준화 기구/단체**

| | |
|---|---|
| 국내 | TTA 바이오인식 PG, KBID, 스마트헬스표준포럼 |
| 국제 | ISO TC215, ITU-T SG17, ABC |
| 국내 참여 업체/기관 | KISA, 서울의과대학, 충북대, 경인여대, 유파인스, 유니온커뮤니티, 삼성전자, LG전자 |

**기술 개발 단계**

| | |
|---|---|
| 국내 | □기초연구↦■실험↦□시작품↦□제품화↦□사업화 |
| 국외 | □기초연구↦□실험↦■시작품↦□제품화↦□사업화 |
| 선도국가/기업 | 한국/삼성전자, LG전자, SK텔레콤, KISA<br>미국/애플사, TI사<br>영국/Halipax 은행<br>캐나다/Bio-Nym사, 왕립은행 |

**기술 수준**: 90% (선도국가대비)

**기술 격차**: 0.5년

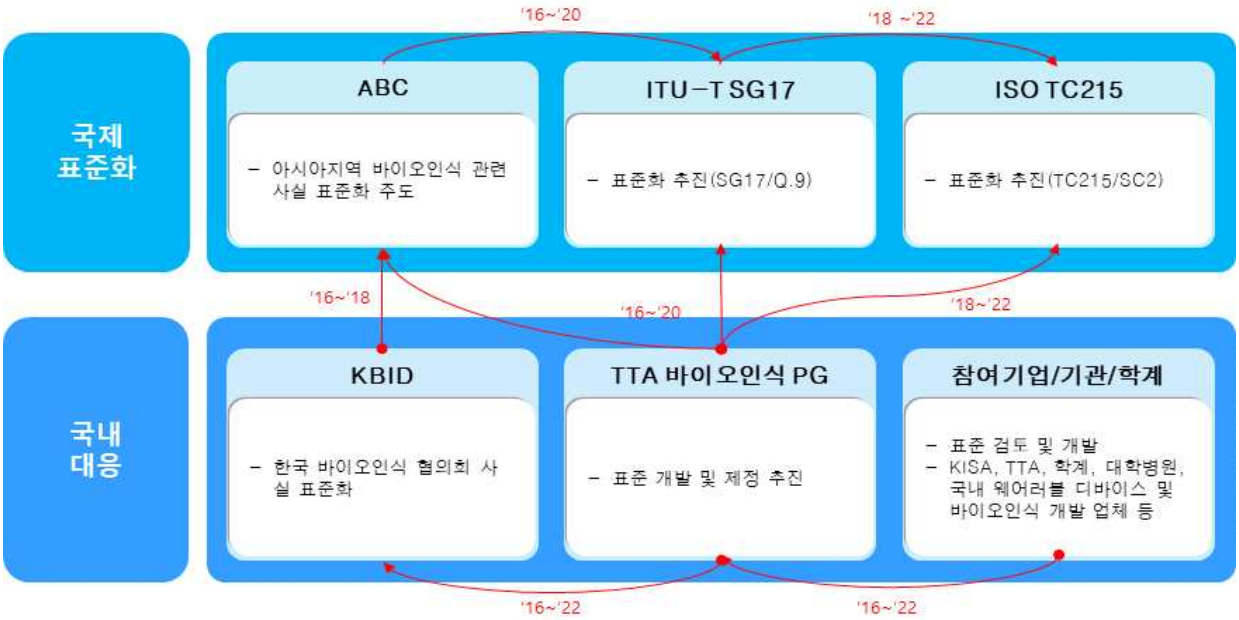
**표준화 단계**

| | |
|---|---|
| 국내 | □과제기획↦□과제승인↦■개발↦□검토↦□표준채택 |
| 국제 | ■과제기획↦□과제승인↦□개발↦□검토↦□표준채택 |
| 선도국가/기업 | 한국/KISA<br>미국/Telebiometrics 민간연구소, TI사<br>스페인/Carlos-3세 마드리드대학교 |

**표준 수준**: 100% (선도국가대비)

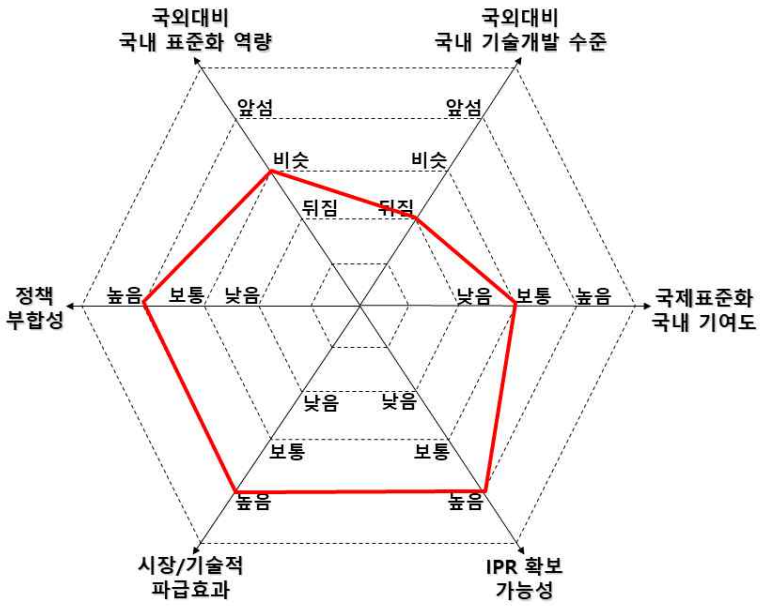
**표준 격차**: 0년

- **Trace Tracking** : 차세대공략(Ver.2017) → 적극공략(Ver.2018)
  KISA에서 Ver2017을 통해 생체신호를 이용한 텔레바이오인식 인증기술 개발 및 국내외 표준화를 착수함에 따라, 주요선진국에서 이에 대한 관심과 적극적인 기술개발이 활발히 진행하여 ITU-T SG17 국제표준을 2017년도부터 국제표준화 선도를 위해 개발 중이므로 적극공략으로 분류

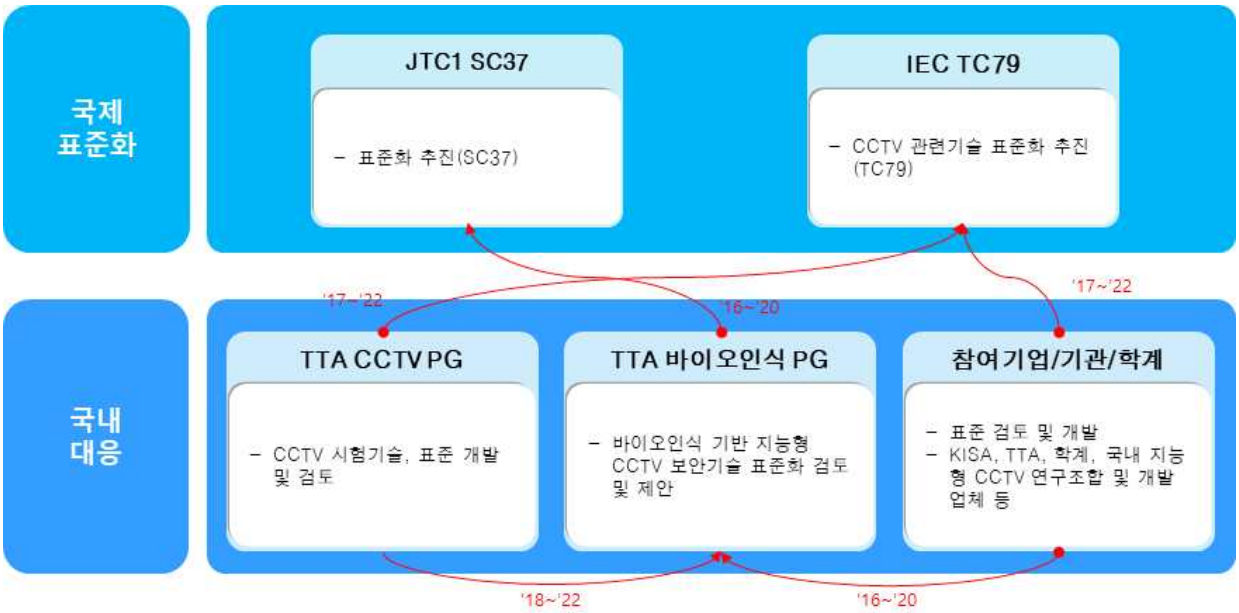



| | |
|---|---|
| 국제 표준화 대응 방안 | **<현황>**<br>- ITU-T SG17 Q9(Telebiometrics)에서 X.tab(Telebiometric authentication using bio-signals) 국제표준화를 선점함에 따라 향후 이를 발전시키어 헬스케어 보안기술로 ISO TC215에 연계 추진할 필요가 있음<br>**<경쟁표준/기구의 전략>**<br>- 미국 Telebiometrics 민간연구소, 스페인 마드리드대학교 등과 국제공동연구를 KISA가 주도하여 ITU-T SG17을 통한 국제표준화에 국제협력체계 강화 추진 중<br>**<대응방안>**<br>- (국제표준화기구 의장단 수임) ITU-T SG17/Q9에서 관련표준의 에디터쉽을 확보하여 ITU-T X.tab 등에 대한 국제표준화를 진행 중 |
| 국내 표준화 추진 계획 | **<현황>**<br>- TTA PG505, KBID, KISA 표준연구회를 중심으로 활발히 생체신호기반 텔레바이오인식 분야에서 국내표준 및 국제표준 개발에 박차를 가하고 있음<br>**<추진계획>**<br>- (연구개발 표준화 연계 개발) KISA가 추진 중인 IITP "심전도를 이용한 텔레바이오인식 인증기술개발" 국제공동연구 일환으로 스페인, 미국 등과 관련기술개발 및 국내표준화를 병행하여 추진 중<br>- (국내 표준화 활동기반 마련) KISA 생체신호인증 기술연구회에서 산학연 전문가그룹과 협력하여 국제표준화와 병행해서 TTA 바이오인식 PG를 통해 바이오인식 응용서비스에 대한 국내표준화 추진 |
| 표준특허 전략 | - **표준 및 R&D 초중기 전략 : 특허를 통한 표준 아이템 도출 전략**<br>- (세부전략) ITU-T SG17 X.tab 등 생체신호 인증기술관련 개발중인 국제표준에 대한 필수 특허 출원 추진예정 |
| 기술개발-표준화-IPR 연계 방안 | - 표준화-기술개발 병행추진<br>- (세부전략) KISA 다중 생체신호 인증기술 개발과 병행하여 ITU-T SG17 국제표준화 추진 중 |

## (적극공략 | 병행) 바이오인식기반 CCTV 보안기술

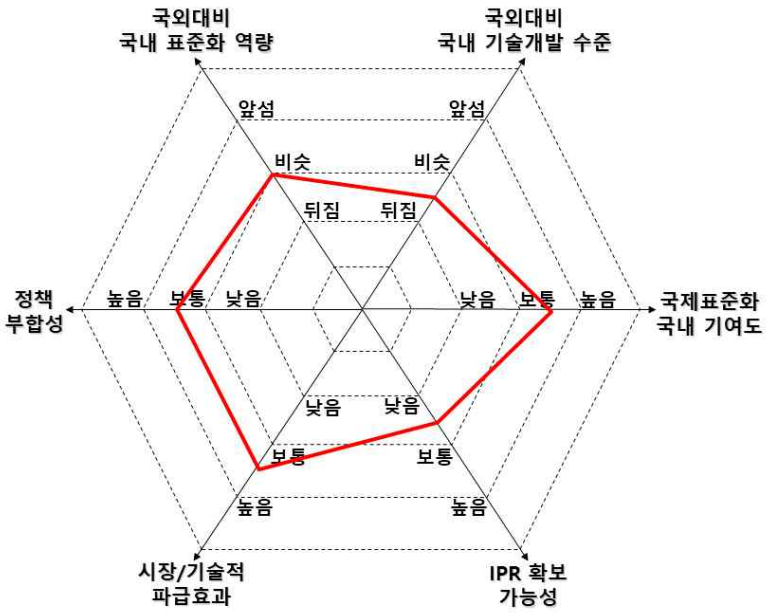
<table>
<tr><td rowspan="3">전략적 중요도 / 국내 역량</td><td colspan="2" rowspan="3"> 
</td><td rowspan="3">표준화 기구/ 단체</td><td>국내</td><td>TTA 바이오인식 PG, CCTV PG, KBID</td></tr>
<tr><td>국제</td><td>JTC1 SC37, IEC TC79</td></tr>
<tr><td>국내 참여 업체/ 기관</td><td>KISA, ETRI, TTA, 인하대, 한국디지털CCTV 연구조합, 테크윈, 에스원, UDP, 아이브스 테크놀로지</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="2">□기초연구↦□실험↦■시작품↦□제품화↦□사업화</td><td>기술 수준</td><td>80% (선도국가대비)</td></tr>
<tr><td>국외</td><td colspan="2">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td><td>기술 격차</td><td>2년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국/에스원, UDP, 테크윈<br>영국/내무부 I-LIDS<br>중국/하이크비전</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="2">□과제기획↦□과제승인↦■개발↦□검토↦□표준채택</td><td>표준 수준</td><td>90% (선도국가대비)</td></tr>
<tr><td>국제</td><td colspan="2">□과제기획↦□과제승인↦■개발↦□검토↦□표준채택</td><td>표준 격차</td><td>1년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국/KISA, TTA<br>영국/내무부<br>중국/알리바바</td></tr>
</table>

- **Trace Tracking** : 차세대공략(Ver.2017) → 적극공략(Ver.2018)
  Ver2017에서는 미래 핵심기술 및 유망서비스 관련 선행적 표준화 분야로 선정되었으며, TTA PG505 국내표준화 추진과 함께, ISO/IEC SC37, IEC TC79 등 국제표준화 선도경쟁이 치열해질 것으로 예상되어, 전략적 대외협력 강화 및 제휴를 위한 적극공략으로 분류

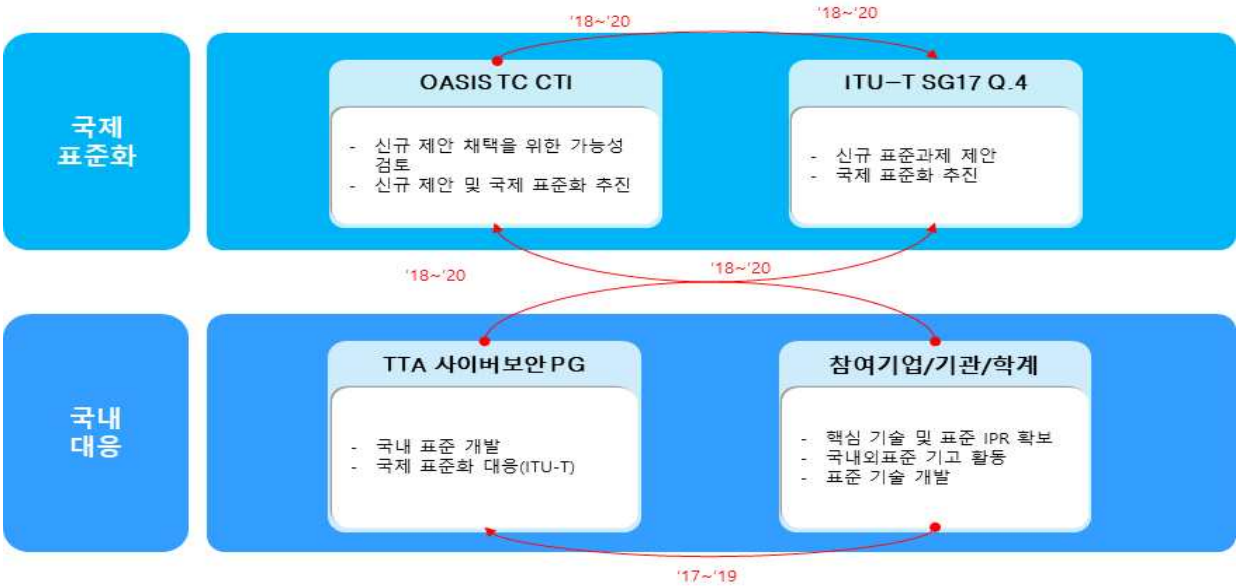



| | |
|---|---|
| 국제 표준화 대응 방안 | **<현황>**<br>- ISO/IEC JTC1 SC37은 바이오인식기술을 결합한 지능형 CCTV 보안기술을, IEC TC79는 CCTV 관련표준화가 진행중으로 상호 협력체계 구축 필요<br>**<경쟁표준/기구의 전략>**<br>- 영국 NPL, South Hamton 대학교 등과 국제협력을 통한 걸음걸이 등 바이오인식기술과 지능형 CCTV 융합 보안기술에 대한 공동연구 추진 필요<br>**<대응방안>**<br>- (국제표준화기구 의장단 수임) KISA 표준연구회, KBID, TTA, 한국디지털CCTV 연구조합 등과 협력체계를 구축하여 지능형 CCTV 보안기술에 대한 기술개발 및 표준화 대응 필요 |
| 국내 표준화 추진 계획 | **<현황>**<br>- TTA PG505에서는 바이오인식기반 지능형 CCTV 보안기술 국내 표준화, TTA PG427에서는 CCTV 장비기술 국내 표준화를 추진하고 있음<br>**<추진계획>**<br>- (PG간 협업을 통한 산업표준 개발) 지능형 CCTV 성능시험기술 등 TTA PG505와 PG427간의 협력체계 구축 필요 |
| 표준특허 전략 | - **표준 초중기 및 R&D 중후기 전략: 표준 필수특허 설계전략**<br>- (세부전략) 바이오인식기반 지능형 CCTV 성능시험기술 등 한국디지털CCTV 연구조합, 학계, KISA, TTA와 긴밀한 연계를 통해 표준특허 아이템 발굴 및 특허출원 추진 |
| 기술개발-표준화-IPR 연계 방안 | - 표준화-기술개발 병행추진<br>- (세부전략) TTA PG505를 중심으로 바이오인식기반 지능형 CCTV 보안기술에 대한 수요를 조사하고, 표준항목 도출 및 관련기술의 IPR 확보 노력 필요 |

## (차세대공략 | 병행) 보안 솔루션 위협정보 공유 및 연동 프레임워크

<table>
<tr><td rowspan="3">전략적 중요도 / 국내 역량</td><td colspan="2" rowspan="3"> 
</td><td rowspan="3">표준화 기구/ 단체</td><td>국내</td><td>TTA 사이버보안 PG</td></tr>
<tr><td>국제</td><td>ITU-T SG17, OASIS</td></tr>
<tr><td>국내 참여 업체/ 기관</td><td>ETRI, KISA, 윈스</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="2">□기초연구↦□실험↦■시작품↦□제품화↦□사업화</td><td>기술 수준</td><td>85% (선도국가대비)</td></tr>
<tr><td>국외</td><td colspan="2">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td><td>기술 격차</td><td>1년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국 / 한국전자통신연구원(ETRI), 한국인터넷진흥원(KISA), 윈스<br>미국 / MITRE(정보보안 관련 연구소)</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="2">□과제기획↦■과제승인↦□개발↦□검토↦□표준채택</td><td>표준 수준</td><td>90% (선도국가대비)</td></tr>
<tr><td>국제</td><td colspan="2">□과제기획↦□과제승인↦■개발↦□검토↦□표준채택</td><td>표준 격차</td><td>1년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국 / 한국전자통신연구원(ETRI), 한국인터넷진흥원(KISA), 윈스<br>미국 / MITRE(정보보안 관련 연구소)</td></tr>
</table>

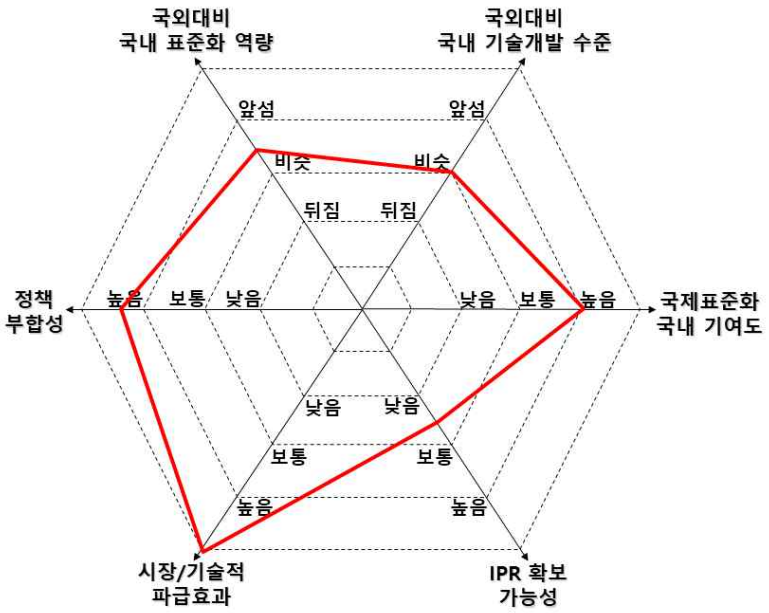
- **Trace Tracking** : 다각화 협력(Ver.2017) → 차세대공략(Ver.2018)
  Ver.2017에서는 다각화협력 항목으로 분류되었으며 현재시점에서 사실표준화기구와 공식표준화기구에 다각적인 대응 모색이 필요하고, 세계 사실표준화기구 대응 및 국내 포럼 활동이 강화되어야 하므로 차세대공략 항목으로 분류



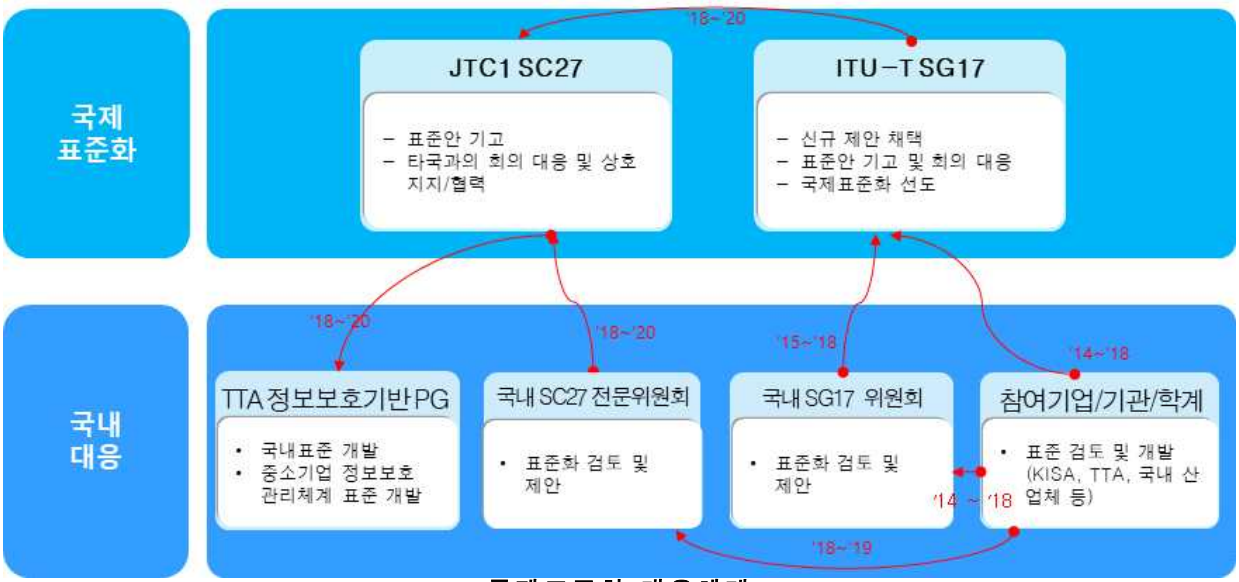

**<국제표준화 대응체계>**

| | |
|---|---|
| 국제 표준화 대응 방안 | **<현황>**<br>- OASIS TC CTI 에서 사이버 위협 정보의 개념을 표준화하고 구조화하여 사이버 위협에 대한 일관된 분석과 자동화된 해석이 가능하게 하는 정보 표현 규격을 제정하고, 정보공유체계의 핵심요소인 STIX는 8 가지 구성요소 (Observable, Indicator, Incident, TTP, ThreatActor, Campaign, ExploitTarget, COA)로 사이버 위협정보를 구조화 함<br>**<경쟁표준/기구의 전략>**<br>- 위협정보 공유 관련 국제 표준은 ITU-T, IETF, OASIS를 중심으로 개발되어 왔으며, MITRE에서 개발한 사이버 위협 정보 전송 규격(TAXII)과 사이버 위협 표현 규격(STIX)에 대한 표준화 작업은 OASIS의 CTI(Cyber Threat Intelligence) 기술 위원회에서 진행 중<br>- ITU-T SG17 에서는 사이버보안에 대한 정보공유 프레임워크(X.cybex)'에 대한 표준이 제정 되었으며, 관련 메커니즘에 대한 표준화 작업이 지속적으로 진행 중<br>**<대응방안>**<br>- (국제표준화기구 신규 과제 제안) 2017년 3월 ITU-T SG17 회의에서 한국 주도로 신규 표준 아이템(X.ucstix, STIX의 유스케이스)을 제안하여 채택되었고, STIX 표준 개발을 주도하고 있는 OASIS TC측과 협력하여 ITU-T SG17 권고안(X.ucstix) 개발 중 |
| 국내 표준화 추진 계획 | **<현황>**<br>- 국내 표준은 TTA, ETRI. KISA를 중심으로 개발되어 왔으며, 사이버보안 정보공유 프레임워크와 정보공유 프로토콜은 ITU-T와 IETF 등 국제표준화 기구에서 제정한 표준을 국내 상황에 맞게 수정한 상태로 준용됨<br>- 2016년부터 구조화된 위협정보 표현규격(STIX)에 대한 시리즈 표준을 개발하기 시작<br>**<추진계획>**<br>- (표준화위원회 PG 활동) TTA 사이버보안 PG(PG503) 에서 OASIS의 구조화된 위협정보 표현 규격(STIX)에 대한 준용 표준 개발과 동시에, ITU-T SG17에서 진행하고 있는 X.ucstix (STIX의 유스케이스)에 대한 국제표준을 개발을 진행하기 위하여 국내업체에서 개발하고 있는 보안 솔루션 위협정보 공유 기술에 대한 국내 고유표준 개발 추진 |
| 표준 특허 전략 | **- 표준 초중기 및 R&D 중후기 전략: 표준 필수특허 설계전략**<br>- (세부전략) 보안 솔루션 위협정보 공유 및 연동 프레임워크 분야는 국제 기여도가 매우 높으며, 또한 IPR 확보 가능성 및 국제표준의 다각화 협력 가능성이 높음. 따라서 보안 솔루션 위협정보 공유 및 연동 프레임워크에 대한 국내외 IPR 적극적 확보 |
| 기술개발 -표준화 -IPR 연계 방안 | - 표준화-기술개발 병행추진<br>- (세부전략) 보안 솔루션 위협정보 공유 및 연동 프레임워크 분야는 국제 기여도가 매우 높은 상태이므로, 실용적인 기술 개발 및 검증과 함께 현재 미흡한 IPR확보에 역점을 두어 관련 국제 표준특허에 협력/경쟁 구도로 추진 |

## (적극공략 | 병행) 정보보호 관리체계

<table>
<tr><td rowspan="3">전략적 중요도 / 국내 역량</td><td colspan="2" rowspan="3"> 
</td><td rowspan="3">표준화 기구/ 단체</td><td>국내</td><td>TTA 정보보호 기반 PG, ITU-T SG17 연구위원회, 국가기술표준원 SC27전문위원회</td></tr>
<tr><td>국제</td><td>JTC1 SC27, ITU-T SG17</td></tr>
<tr><td>국내 참여 업체/ 기관</td><td>KISA, TTA</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="2">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td><td>기술 수준</td><td>90% (선도국가대비)</td></tr>
<tr><td>국외</td><td colspan="2">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td><td>기술 격차</td><td>1년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">미국 / KPMG, 영국/BSI, 한국 / TTA, KISA</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="2">□과제기획↦□과제승인↦■개발↦□검토↦□표준채택</td><td>표준 수준</td><td>95% (선도국가대비)</td></tr>
<tr><td>국제</td><td colspan="2">□과제기획↦□과제승인↦□개발↦■검토↦□표준채택</td><td>표준 격차</td><td>0.5년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">미국/NIST, 일본/NEC, 한국/TTA,KISA</td></tr>
</table>

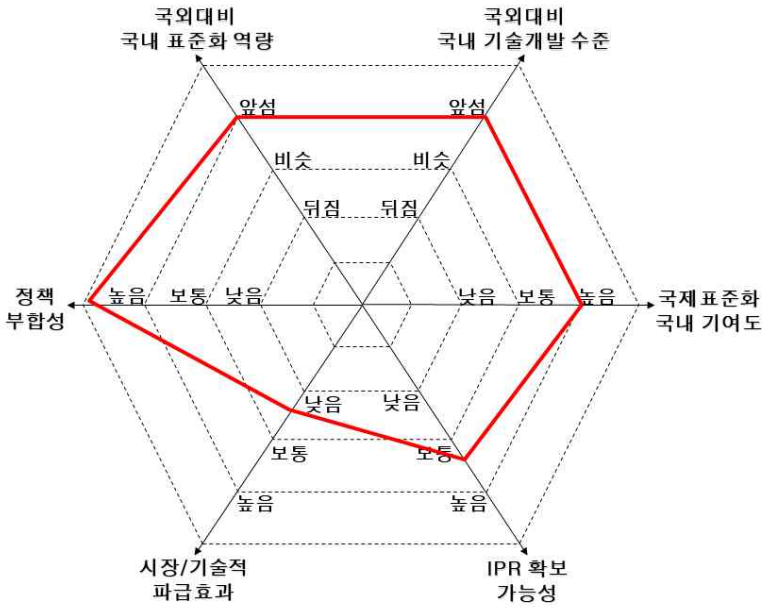
- Trace Tracking : 차세대공략(Ver.2017) → 적극공략(Ver.2018)
  국내의 개인정보 유출 사고 등 사회적 이슈와 맞물려 사회적 관심이 높은 분야로서 국제적으로는 관리체계에 대한 수립 및 표준화에 대한 성장이 많이 이루어져 있으나 국내의 경우 짧은 경험에 의한 체계 수립이 불완전한 상태로써 학계와 산업계의 지속적인 연구 개발을 기반으로 차별적 선택과 통합을 통해 국내 환경에 적합한 표준화를 개발할 수 있도록 적극공략으로 분류



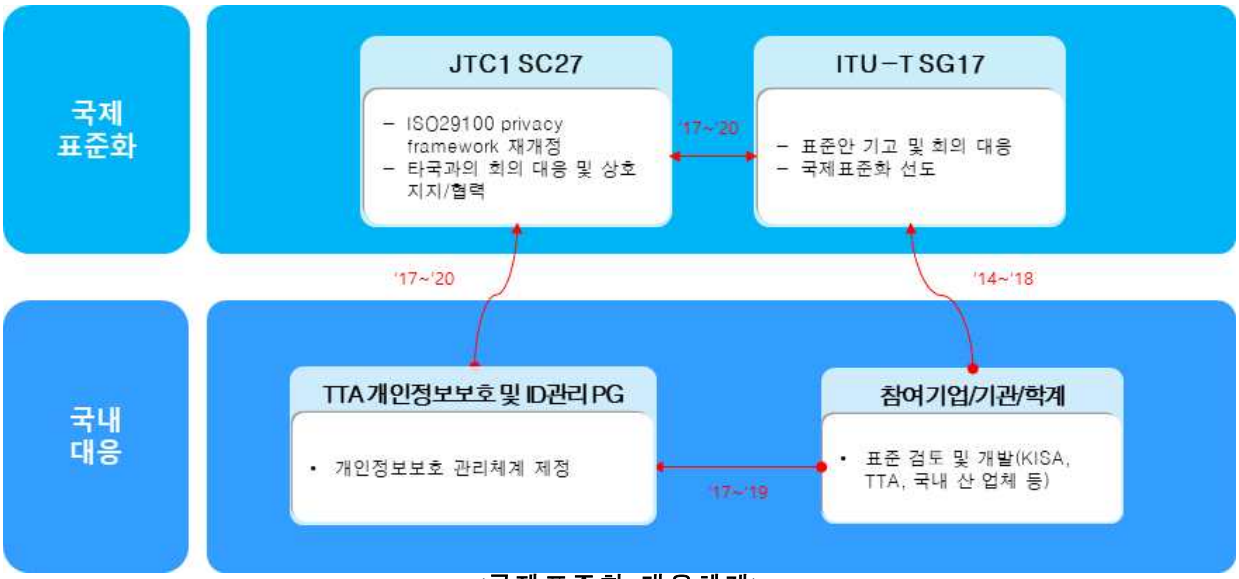

**<국제표준화 대응체계>**

| | |
|---|---|
| **국제 표준화 대응 방안** | **<현황>**<br>- 정보보호 관리체계는 ISO/IEC에서 표준화된 부분도 있으나 일부 개발이 진행되고 있는 부분도 있어 국제 표준 재개정 작업에 활발히 참여함으로써 프로세스 및 요건을 표준화하고 국내 지침을 국제 표준에 반영하기 위한 활동이 지속되어야 함<br>- TTA를 중심으로 중소기업의 정보보호 관리체계의 표준이 진행되고 있으며 과학기술정보통신부의 후원과 함께 중소기업의 정보보호 관리수준을 측정할 수 있는 준비도 평가의 시장 정착을 위해 중소기업의 정보보호 수준을 객관적으로 평가할 수 있는 표준화 가이드라인이 필요함. 국내 에디터십을 통해 중소규모조직을 위한 정보보호 관리기준 수립에 국내 실무를 반영하기 위해 추진 중에 있으며, 국제 표준 수립 후 TTA PG를 통한 국내 표준 수립을 통한 시장 공급을 진행 중<br>**<경쟁표준/기구의 전략>**<br>- IOS/IEC에서는 ISO/IEC 27001과 ISO/IEC27002가 조직의 규모에 관계없이 모든 조직에 적용 가능한 정보보호 관리를 위한 가이드임을 주장하고 있어, 중소 규모의 보안 활동에 대한 현실적 상황의 직시를 통한 실용적 가이드의 표준 필요성 주장 필요<br>**<대응방안>**<br>- (국제표준화기구 신규 과제 제안) 현재 중소규모의 조직을 위한 정보보호 관리체계를 ITU-T의 표준으로 채택하기 위한 노력이 진행 중. ITU-T에서의 한국이 X.sgsm(제목) 에디터쉽을 확보해 국제 표준화 이후 통신 조직이외의 일반 중소 규모의 조직으로의 적용을 확대 하기 위해 국내 표준의 추진 및 ISO/IEC JTC1 SC27에 신규 표준의 제안 예정('18) |
| **국내 표준화 추진 계획** | **<현황>**<br>- 정보보호 관리체계는 ISMS 인증제도를 통하여 국내에 보급되고 있으나, 정보보호 활동의 사각지대에 있는 중소 규모의 조직을 위한 활동 가이드에 대한 표준은 미 수립<br>**<추진계획>**<br>- (학계나 기업과의 협력을 통해 프로토콜 적용 규격 개발) ITU-T에서 추진되고 있는 중소조직을 위한 정보보호 관리체계의 국제 표준 기준과 함께 중소규모의 정보보호 활동을 지원하고 있는 준비도 평가의 기준을 호환하는 국내 표준의 개발이 필요함 |
| **표준 특허 전략** | - **해당사항 없음**<br>- 정보보호 관리체계는 국내외 인증 제도와 규제 등에 반영되었었고 오랜 시간 논의 되어 오던 부분이 많아 별도의 IPR를 확보할 가능성은 높지 않을 것으로 판단됨 |
| **기술개발 -표준화 -IPR 연계 방안** | - 표준화-기술개발 병행추진<br>- (세부전략) 과학기술정보통신부, 방송통신위원회, 행정안전부 등 정부기관을 중심으로 정보보호 관리체계에 대한 통합 추진과 함께 한국인터넷 진흥원, 인증기관, 산업계 등과의 협력을 통하여 정보보호 관리체계 인증 기준 및 지침의 개발 및 국제회의 등의 커뮤니티(Technical Community) 참여를 통해 표준화에 기여할 수 있음 |

## (적극공략 | 후행) 개인정보보호 정책 및 운영관리 기술

<table>
<tr><td rowspan="3">전략적 중요도 / 국내 역량</td><td colspan="2" rowspan="3"> 
</td><td rowspan="3">표준화 기구/ 단체</td><td>국내</td><td>TTA 개인정보보호 및 ID관리 (PG502)</td></tr>
<tr><td>국제</td><td>JTC1 SC27, ITU-T SG17</td></tr>
<tr><td>국내 참여 업체/ 기관</td><td>KISA, TTA, 순천향대학교</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="2">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td><td>기술 수준</td><td>100% (선도국가대비)</td></tr>
<tr><td>국외</td><td colspan="2">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td><td>기술 격차</td><td>0년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국, 일본, 미국, EU</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="2">□과제기획↦□과제승인↦□개발↦■검토↦□표준채택</td><td>표준 수준</td><td>100% (선도국가대비)</td></tr>
<tr><td>국제</td><td colspan="2">□과제기획↦□과제승인↦□개발↦■검토↦□표준채택</td><td>표준 격차</td><td>0년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국, 일본, 미국, EU</td></tr>
</table>

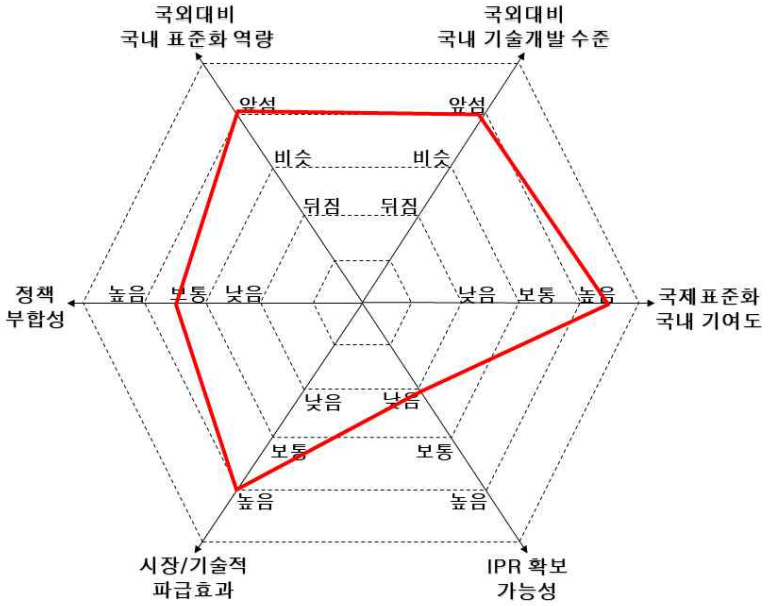
- **Trace Tracking** : 다각화협력(Ver.2017) → 적극공략(Ver.2018)
  개인정보보호분야는 각 국가별 표준화 및 기술개발 기반 하에 각국의 법규를 수용하기 위한 인터페이스로 국제 표준화가 진행되고 있으며, 국내 표준화 전문가가 국제 표준화에서 주도적으로 활동을 수행하고 있으며, 기술개발 및 국제표준화가 거의 완료단계이고 서비스/시장 확산을 위해 적극공략 항목으로 분류

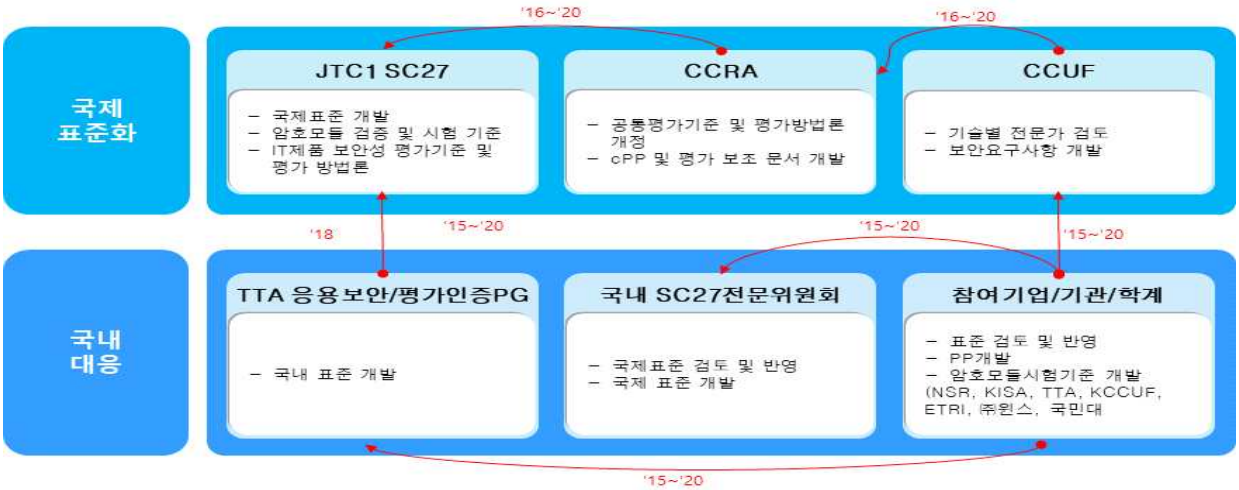



**<국제표준화 대응체계>**

| | |
|---|---|
| **국제 표준화 대응 방안** | **<현황>**<br>– 개인정보보호기술은 ITU-T SG17과 ISO/IEC JTC1 SC27의 국제표준기구에서 국내 표준 전문가들의 적극적인 참여로 주도적인 표준개발이 진행되고 있으며, 국내 산업의 글로벌 진출을 지원하기 위한 국제표준의 선도적 활동을 위해서 지속적인 활동에 참여가 필요<br>– 개인정보보호지침이 한국 에디터 주도적 활동에 의해 ISO/IEC의 29151과 ITU-T의 X.1058로 2017년 개발 완료 후 최종 승인됨<br>**<경쟁표준/기구의 전략>**<br>– 변화하는 국제 사회의 환경을 고려한 국내 산업의 글로벌 비즈니스 활동을 지원과 국제표준화 주도권 유지가 필요. 또한 IoT, 스마트그리드 기술에 개인정보보호기술 적용 표준화는 초기 단계로, 국내 개인정보보호 전문가가 적극적인 활동이 필요함<br>**<대응방안>**<br>– (국제표준화기구 신규 과제 제안) ISO29100 privacy framework가 현재 재개정 준비를 하고 있어, 국내 전문가의 적극적인 참여를 통해 개인정보보호를 위한 국제 표준개발의 주도권을 지속적으로 추진 |
| **국내 표준화 추진 계획** | **<현황>**<br>– ISO29151과 ITU-T X.1058이 개인정보보호지침의 국제표준으로 개발됨에 따라 국내의 PIMS인증 제도와의 호환성 검토를 통한 개인정보보호 관리체계 국내 표준의 개정 필요<br>– 개인정보보호법 제정에 따라 개인정보보호기술에 대한 컴플라이언스 요구가 활발하여 다양한 기술개발이 추진되고 있으나, 표준화 추진은 다소 미흡한 실정<br>**<추진계획>**<br>– (표준화위원회 PG 활동) TTA 개인정보보호 및 ID관리(PG502)를 통해 국내 표준화를 진행할 예정 |
| **표준특허 전략** | – **해당사항 없음** |
| **기술개발 -표준화 -IPR 연계 방안** | – 표준화-기술개발 병행추진<br>– (세부전략) 클라우드 환경의 서비스 등 글로벌 정보통신 서비스의 증가에 따라 개인정보의 국외이전 요구가 증가하고 있으나, 각 국가별 법규의 상이성 문제를 해결하는 복잡한 컴플라이언스를 충족하는 기술개발이 필요하며, 이 기술개발과 함께 국가간 상호 연동성을 위한 국제 표준화의 추진 및 표준특허 확보가 요구됨 |

## (적극공략 | 병행) 유형별 보안성 시험평가기준

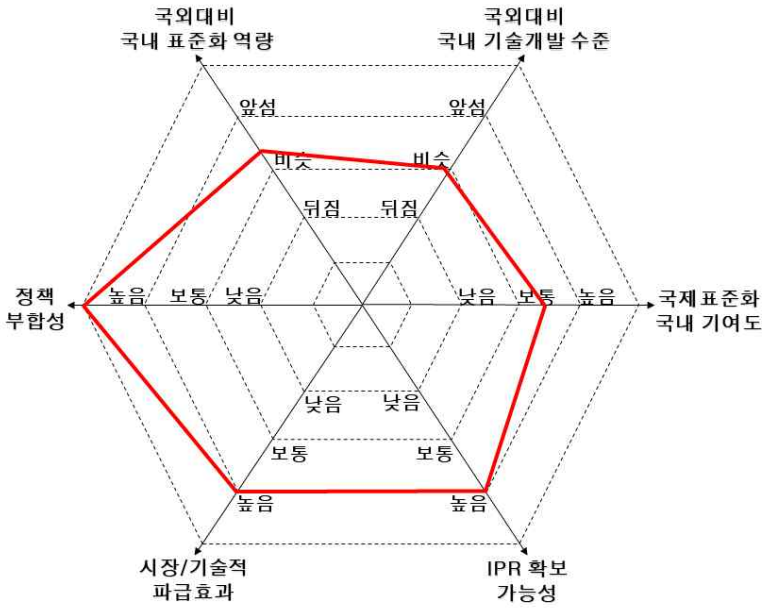
<table>
<tr><td rowspan="3">전략적 중요도 / 국내 역량</td><td colspan="2" rowspan="3"> 
</td><td rowspan="3">표준화 기구/ 단체</td><td>국내</td><td>TTA 응용보안/ 평가인증 PG, 국가기술표준원 SC27전문위원회</td></tr>
<tr><td>국제</td><td>JTC1 SC27, CCRA, CCUF</td></tr>
<tr><td>국내 참여 업체/ 기관</td><td>NSR(국가보안기술연구소), KISA, TTA, ETRI, KCCUF, ㈜윈스, ㈜에스프린팅솔루션, 국민대, ㈜유넷시스템</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="2">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td><td>기술 수준</td><td>100%</td></tr>
<tr><td>국외</td><td colspan="2">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td><td>기술 격차</td><td>0년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국/(주)에스프린팅솔루션 , 미국/Atsec,Microsoft, 독일/Tuvit, 프랑스/Gelmato</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="2">□과제기획↦□과제승인↦□개발↦□검토↦■표준채택</td><td>표준 수준</td><td>100%</td></tr>
<tr><td>국제</td><td colspan="2">□과제기획↦□과제승인↦□개발↦□검토↦■표준채택</td><td>표준 격차</td><td>0년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">한국/NSR,ETRI,TTA, 미국/NIST,Atsec, Micosoft, 독일/BIS, 일본/IPA, AIST</td></tr>
<tr><td colspan="6">- Trace Tracking : 적극공략(Ver.2017) → 적극공략(Ver.2018)<br>보안성 평가 기술 및 표준은 국내 CC 평가제도 및 암호모듈 검증제도 등에 적용되고 있으며, 관련 기술개발이 활발히 진행되고 있어 국내외 보안산업에 파급효과가 크므로 적극공략으로 분류</td></tr>
</table>



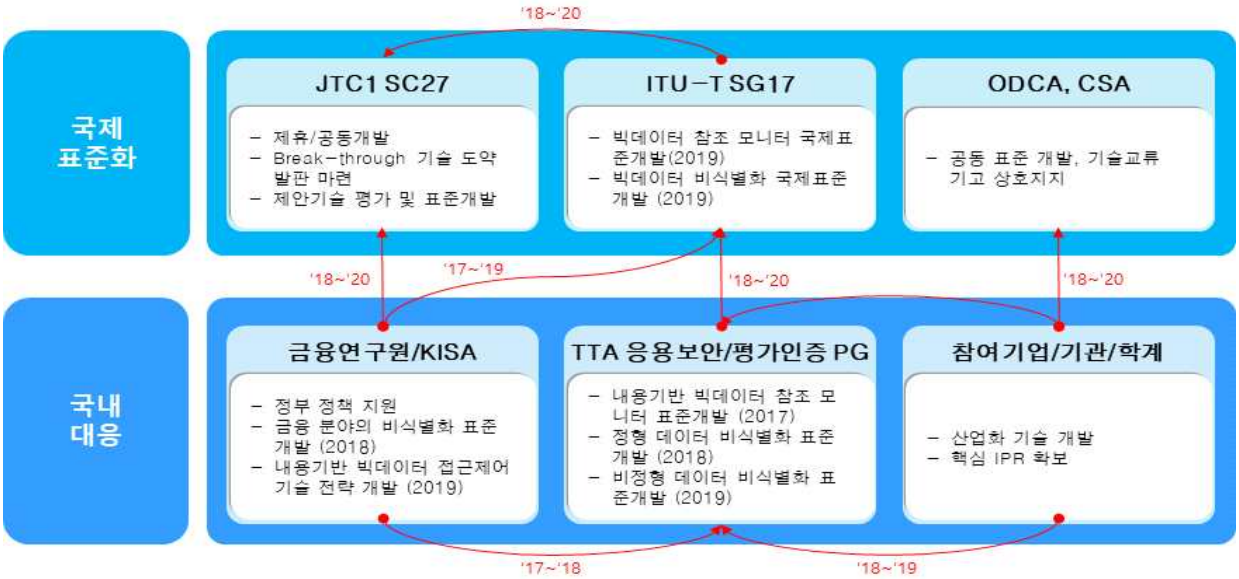

**<국제표준화 대응체계>**

| | |
|---|---|
| 국제 표준화 대응 방안 | **<현황>**<br>- ISO/IEC JTC1 SC27은 IT제품의 보안성 평가기준 및 암호검증기준과 시험기준 표준을 개발하고 시험자 및 평가자의 자격요건에 대한 요구사항을 개발<br>- CCRA는 공통평가기준(CC)과 평가방법론(CEM)을 개정하고 ISO/IEC JTC1 SC27과 협력하여 국제표준인 ISO/IEC15408(보안성평가기준)과 ISO/IEC18045(평가방법론)의 개정을 진행하고 있음. ISO/IEC JTC1 SC27은 각국의 전문가들로 부터 개정 이슈 사항을 수집하고 개정 작업에 착수<br>- CCRA는 공통평가기준(CC)과 평가방법론(CEM)을 개발하고 그 외 각 제품별로 활용될 수 있는 기술적인 요구사항에 대한 cPP와 cPP SD를 개발하여 CCRA 가입국에서 활용하도록 하고 있음. CCUF는 글로벌 벤더들이 주도적으로 참여하며 CCRA의 기술그룹(iCT)를 통해 cPP개발에 참여 중<br>**<경쟁표준/기구의 전략>**<br>- NSR IT보안인증사무국과 국내 전문가들(정책기관, 평가기관, 산업체(KCCUF))은 공통평가기준 2020년 개정과 유형별 cPP 기준 개발에 주도적 참여하여 국내 이익을 대변<br>- 한국은 JTC1 SC27에서 ISO/IEC 19790(암호모듈 검증기준) 등 5건 국제표준 제정에 주도적으로 참여하여 국내 산업계 이익을 대변 중<br>※ ISO/IEC 19790 암호모듈 검증기준('18 예정, NSR)<br>※ ISO/IEC 24759 암호모듈 시험기준('18 예정, NSR)<br>※ ISO/IEC 20540 암호모듈 현장시험 가이드('18년 예정, NSR 주도)<br>※ ISO/IEC 20543 난수발생기 시험방법('18년 예정, NSR 및 국민대)<br>※ ISO/IEC 20897 물리적 복제불가 기능 시험방법('19년 예정, ETRI 주도)<br>**<대응방안>**<br>- (국제표준화기구 의장단 수임) 한국이 에디터로서 ISO/IEC15408(보안성평가기준)과 ISO/IEC18045(평가방법론)의 개정 추진 (2020년까지)<br>- 사실표준화기구(CCRA) 활동 적극대응 |
| 국내 표준화 추진 계획 | **<현황>**<br>- ISO/IEC JTC1 SC27에서 한국/미국/일본 공동으로 ISO/IEC 19790(암호모듈 검증기준), ISO/IEC 24759(암호모듈 시험기준) 2018년 표준개정 후, 2019년 국가기술표준원 KS X 표준에 반영 예정<br>- ISO/IEC JTC1 SC27에서 진행되고 있는 암호모듈 관련 국제표준 제정 후 국가기술표준원 KS X 표준에 반영 예정<br>- NSR의 IT보안인증사무국은 CCRA의 CC와 CEM의 개정사항을 한글화하여 홈페이지에 게시 예정<br>**<대응방안>**<br>- (SO/IEC15408, ISO/IEC18045) 국외 표준화 후 국내 KS X 표준 제정 예정 |
| 표준특허전략 | - **해당사항 없음** |
| 기술개발-표준화-IPR 연계 방안 | - 표준화-기술개발 병행추진<br>- (세부전략) 정책기관, 인증기관, 평가/시험기관, 산업체 등 협력을 통한 평가 기술 개발 및 국제회의 및 기술 커뮤니티 참여를 통해 기술 개발 및 표준화. 기술 개발 참여 확대를 통해 표준화 기여도 제고 |

## (차세대공략 | 병행) 빅데이터 데이터 보안

<table>
<tr><td rowspan="3">전략적 중요도 / 국내 역량</td><td colspan="2" rowspan="3"> 
</td><td rowspan="3">표준화 기구/ 단체</td><td>국내</td><td>TTA 응용보안/ 평가인증 (PG504)</td></tr>
<tr><td>국제</td><td>JTC1 SC27, ITU-T SG17, ODCA, CSA</td></tr>
<tr><td>국내 참여 업체/ 기관</td><td>행자부, 금융보안원, KISA, ETRI</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="2">■기초연구↦□실험↦□시작품↦□제품화↦□사업화</td><td>기술 수준</td><td>90% (선도국가대비)</td></tr>
<tr><td>국외</td><td colspan="2">□기초연구↦□실험↦■시작품↦□제품화↦□사업화</td><td>기술 격차</td><td>1.0년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">미국/NIST, 영국 ICO(영국정보국), EU ENISA</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="2">■과제기획↦□과제승인↦□개발↦□검토↦□표준채택</td><td>표준 수준</td><td>95% (선도국가대비)</td></tr>
<tr><td>국제</td><td colspan="2">□과제기획↦□과제승인↦■개발↦□검토↦□표준채택</td><td>표준 격차</td><td>0.5년</td></tr>
<tr><td>선도국가/ 기업</td><td colspan="4">미국/NIST, 영국 ICO(영국정보국), EU ENISA</td></tr>
</table>

- Trace Tracking : 차세대공략(Ver.2017) → 차세대공략(Ver.2018)
  최근 온라인 분석 기술인 OLAP 기술이 글로벌 기업을 중심으로 새롭게 부각 되면서 표준화에 대한 다양한 이슈가 발현되고 있음. 특히 공공정보 공개와 맞물려 비식별화 기술 및 빅데이터 분석에서 식별화에 대한 감시 기술이 중요시 되고 있으나 국내 역량이 아직 부족하여 차세대공략 항목으로 분류

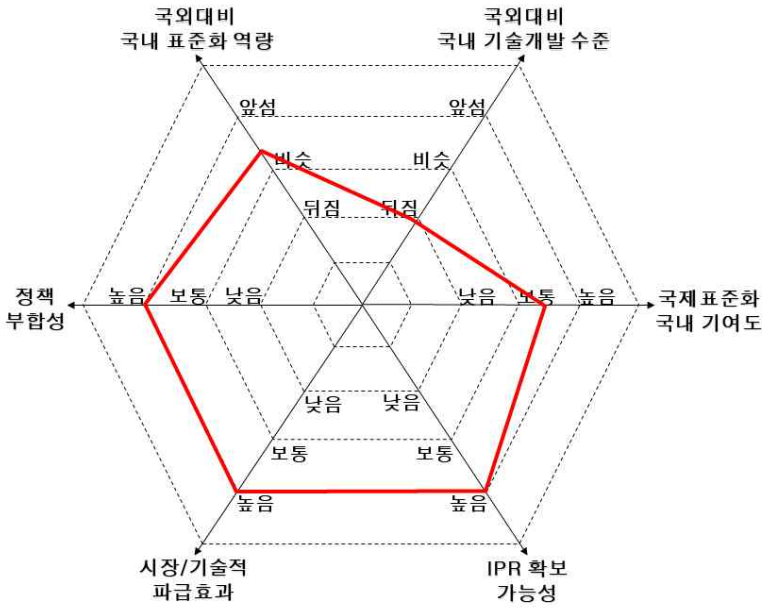



**<국제표준화 대응체계>**

| | |
|---|---|
| 국제 표준화 대응 방안 | **<현황>**<br>- 빅데이터 활용 측면에서 데이터 형식 및 사용 인터페이스는 ODCA, CSA를 통해 산업체 중심으로 표준화가 집중 추진되고 있으며, 공적 표준화 기구인 ISO/IEC JTC1 BD-SG, ITU-T SG17에서는 빅데이터 분석 과정의 보안 이슈를 표준화 추진 중<br>**<경쟁표준/기구의 전략>**<br>- 미국은 NIST 가이드라인 준수를 주장하고 있으나, 국가 간 이익이 맞물려 있어 쉽게 적용되고 있지 않고, ISO/IEC JTC1 SC27은 개인정보 보호 차원에서 접근하고 있어 활용 및 서비스 관련 내용이 포함되지 못함<br>**<대응방안>**<br>- (국제표준화기구 의장단 수임) 금융보안원, KISA, ETRI 협력으로 비식별화 기술에 대한 ITU-T SG17 의 에디터쉽을 확보하고 주도적으로 표준 개발을 추진하고 있으며, ETRI에서 수행하는 참조 모니터 기술과 중국에서 제안한 모바일 환경에서 데이터 보안 이슈를 접목하여 관련분야 표준 벨트(묶음)를 전략적으로 추진 |
| 국내 표준화 추진 계획 | **<현황>**<br>- 국내 인공지능/빅데이터 분야에서 활용하는 데이터는 공공정보 활용과 맥을 같이 하고 있으며, 행정자치부 주도의 데이터 활용 가이드라인을 제정하고 이를 국제 표준화 및 금융 분야 표준으로 추진하고 있는 상황임<br>**<추진계획>**<br>- (정형/비정형 데이터의 비식별화 추진) 공공정보 공개를 위한 데이터 가공 분야와 금융분야에서 공개 및 유출되는 정보의 분석을 위한 기술을 병행 개발하고 이를 표준으로 추진하는 전략이 필요 |
| 표준 특허 전략 | - **표준 및 R&D 초중기 전략 : 특허를 통한 표준 아이템 도출 전략**<br>- (세부전략) 기존의 비식별화 기술은 정보의 삭제를 통한 비식별화에 중점을 두고 있다면, 최신의 기술은 정보를 압축하거나 변형하여 필요한 경우 복원할 수 있는 기술로 집중되고 있어 새로운 비식별화 기술 확보 및 관련 특허 및 IPR의 선행적 확보 |
| 기술개발 -표준화 -IPR 연계 방안 | - 표준화-기술개발 병행추진<br>- (세부전략) 빅데이터 데이터 보안 기술 확보와 동시에 국제 표준화 작업 추진 |

## (차세대공략 | 병행) 의료보안

**전략적 중요도 / 국내 역량**




**표준화 기구/단체**

| | |
|---|---|
| 국내 | TTA 바이오인식 PG, 스마트의료보안 포럼 |
| 국제 | ITU-T SG17, ISO TC215 |
| 국내 참여 업체/기관 | KISA, 고려대, 건국대, 삼성의료원, 분당서울대학병원 |

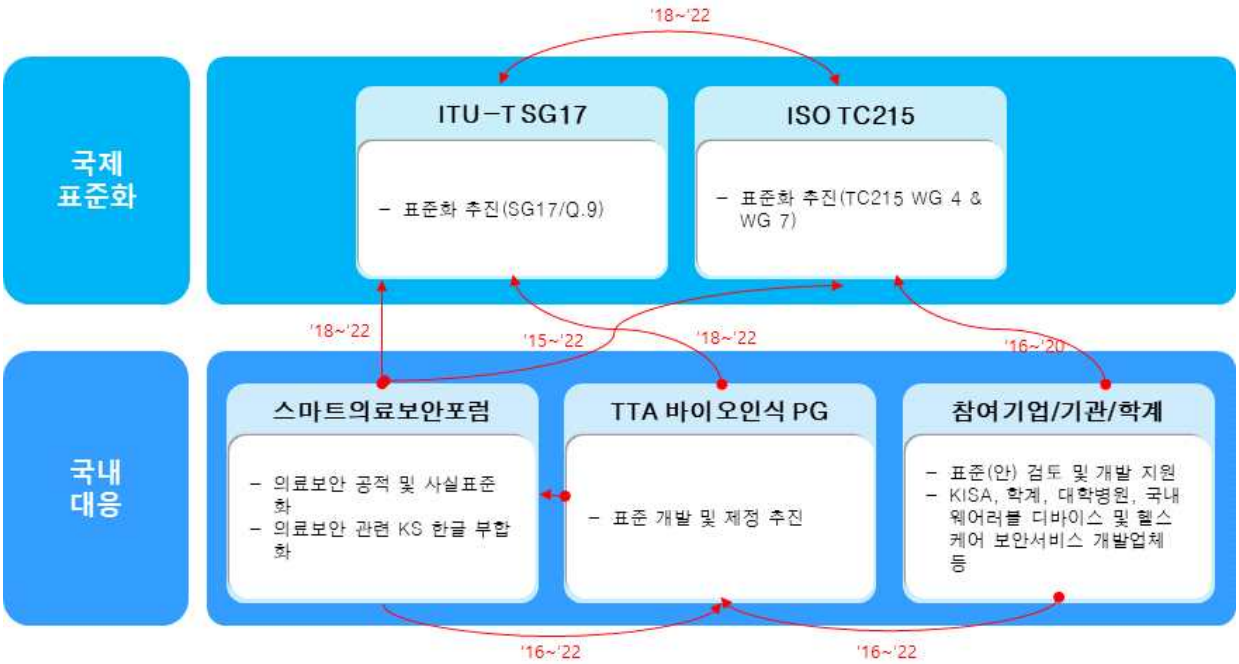
**기술 개발 단계**

| | | | |
|---|---|---|---|
| 국내 | □기초연구↦□실험↦■시작품↦□제품화↦□사업화 | **기술 수준** | 70% (선도국가대비) |
| 국외 | □기초연구↦□실험↦■시작품↦□제품화↦□사업화 | **기술 격차** | 2년 |
| 선도국가/기업 | 미국, 유럽/GE Healthecare, Phillips, Simens 등 | | |

**표준화 단계**

| | | | |
|---|---|---|---|
| 국내 | □과제기획↦□과제승인↦■개발↦□검토↦□표준채택 | **표준 수준** | 95% (선도국가대비) |
| 국제 | ■과제기획↦□과제승인↦□개발↦□검토↦□표준채택 | **표준 격차** | 0.5년 |
| 선도국가/기업 | 미국, 유럽/GE Healthecare, Phillips, Simens 등 | | |

- **Trace Tracking** : 차세대공략(Ver.2018 신규항목)
  '17년초부터 의료기기를 대상으로 한 보안 취약성과 의료정보시스템에 대한 랜섬웨어 공격이 빈발함에 따라, 의료기기간 상호 보안인증에 대한 국제표준안을 제안하여, 한국 주도로 표준 작성과 더불어서 관련된 요소기술을 파악하여 특허화를 위한 차세공략으로 분류

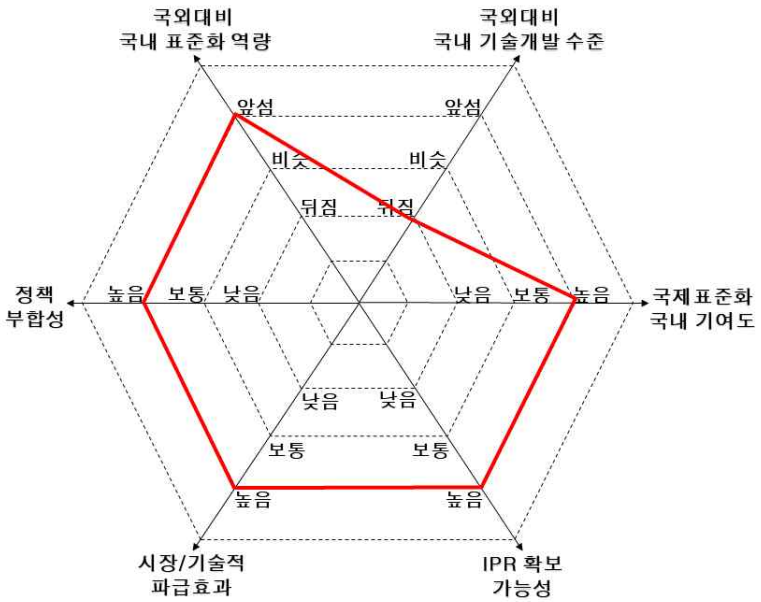



<국제표준화 대응체계>

| | |
|---|---|
| 국제 표준화 대응 방안 | **<현황>**<br>- ISO TC 215 보건의료 표준화 위원회에서 국제표준화 작업을 체계적으로 잘 진행하고 있으며, 국내에서도 관련 분야 전문가 20인으로 구성된 전문위원회에서 적극적으로 참여하여 표준화 작업을 진행하고 있음<br>**<경쟁표준/기구의 전략>**<br>- 보건의료 분야 국제표준화 단체와 사실 표준화 단체 등과의 교류 활동을 통한 협력체계 구축 필요(ONC, HL7, IHE 등)<br>**<대응방안>**<br>- (국제표준화기구 신규 과제 제안) ISO TC215 WG 4와 WG 7 에 의료기기 상호보안 인증 신규 표준을 제안(2017년 5월 중국 항저우 표준총회)하였고, 과제 승인을 위해 미국, 일본, 유럽 등 각국 대표단과 긴밀하게 국제협력체계 구축하여 진행하는 것이 필요함 |
| 국내 표준화 추진 계획 | **<현황>**<br>- TTA PG 505 그룹과 스마트의료보안포럼, 고려대, 성균관대, 건국대, 사회보장정보원 등과 협업하여 의료분야 보안 표준화 그룹 참여를 통한 표준화 기반 마련<br>**<추진계획>**<br>- (연구개발 표준화 연계 개발) 국가기술표준원 국제표준화 기술력 향상사업에 참여하여 국제표준화 작업 추진<br>- (국내 표준화 활동기반 마련) TTA PG 505 보안 분야 표준화 그룹 참여를 통한 표준화 기반 마련 |
| 표준 특허 전략 | - **표준 및 R&D 초중기 전략 : 표준화 방향에 따른 출원 및 기고 전략**<br>- (세부전략) 국제 표준화와 작업 방향을 예측하여 관련 기술 특허 확보 |
| 기술개발-표준화-IPR 연계 방안 | - 표준화-기술개발 병행추진<br>- (세부전략) 보건의료 분야 보안기술 Use Case를 확보하여 국제 표준화 작업 추진 |

## (차세대공략 | 병행) 제조 보안

**전략적 중요도 / 국내 역량**




**표준화 기구/단체**

| | |
|---|---|
| 국내 | TTA CPS PG |
| 국제 | IEC TC65, ITU-T SG17 |
| 국내 참여 업체/기관 | KISA, 건국대 |

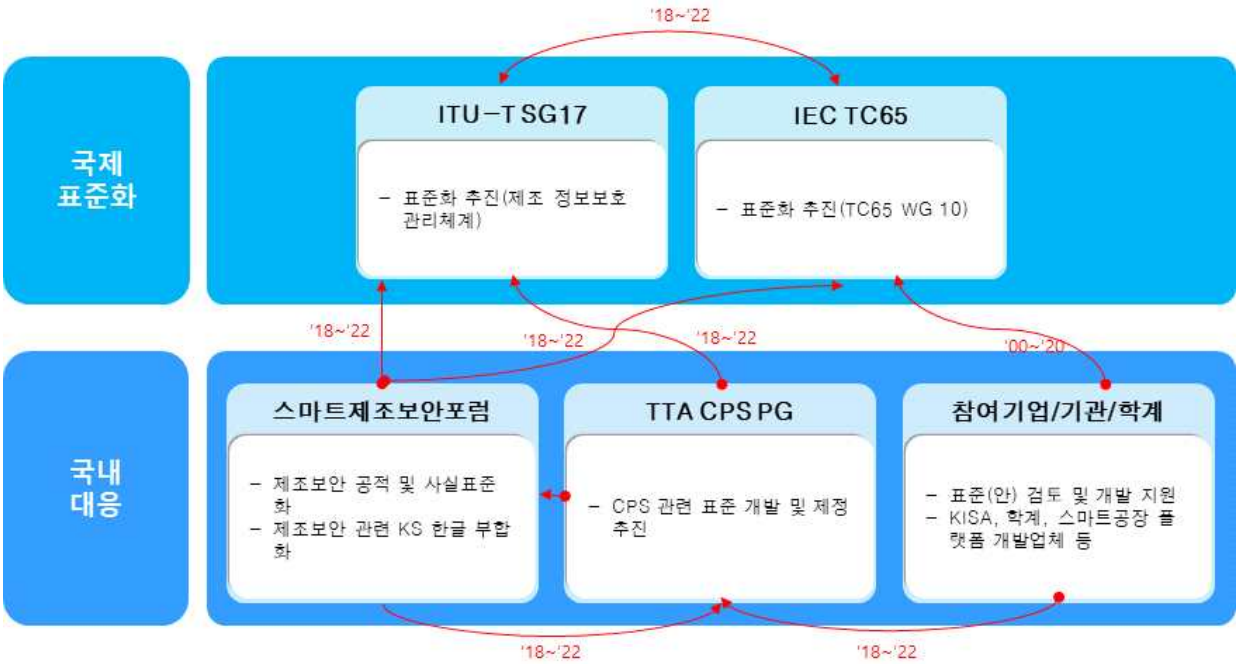
**기술 개발 단계**

| | | | |
|---|---|---|---|
| 국내 | □기초연구↦□실험↦■시작품↦□제품화↦□사업화 | **기술 수준** | 60% (선도국가대비) |
| 국외 | □기초연구↦□실험↦■시작품↦□제품화↦□사업화 | **기술 격차** | 3년 |
| 선도국가/기업 | 한국/KISA<br>미국/ISA 99 | | |

**표준화 단계**

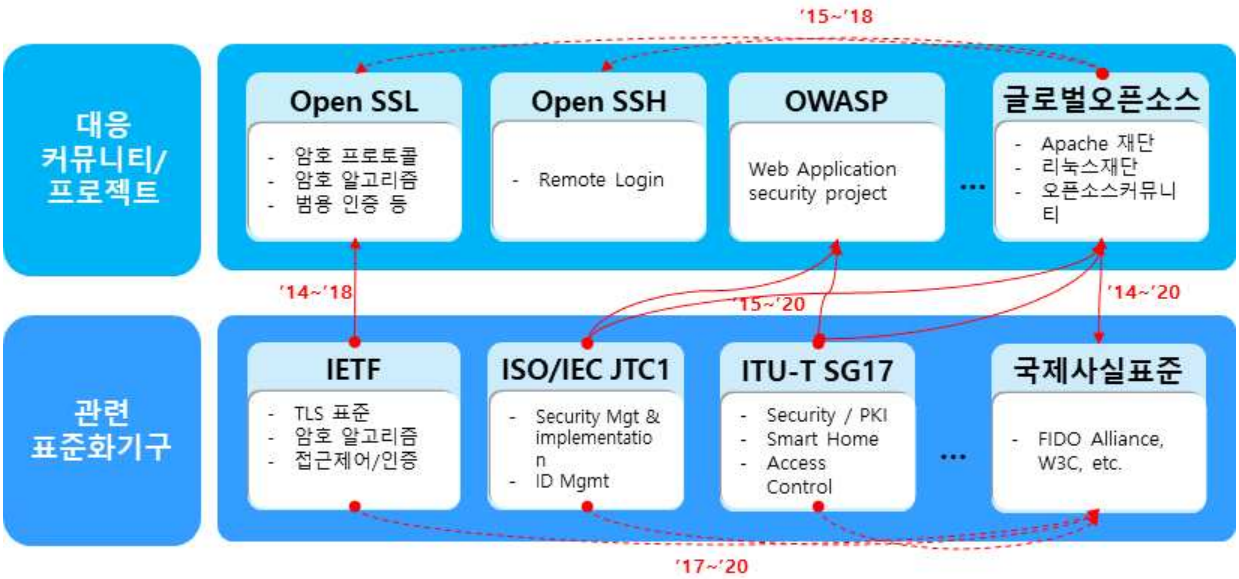
| | | | |
|---|---|---|---|
| 국내 | ■과제기획↦□과제승인↦□개발↦□검토↦□표준채택 | **표준 수준** | 100% (선도국가대비) |
| 국제 | ■과제기획↦□과제승인↦□개발↦□검토↦□표준채택 | **표준 격차** | 0년 |
| 선도국가/기업 | 한국/KISA<br>미국/ISA, NIST | | |

- **Trace Tracking** : 차세대공략 (Ver.2018 신규항목)
  KISA 정보보호관리체계 인증으로 전 산업분야에 대한 보안관리 인증을 수행하고 있으므로, 이를 바탕으로 제조 분야에 대한 인증 기준을 마련하여 다각화 협력을 통한 표준화 공략이 필요하여 차세대공략으로 분류




| | |
|---|---|
| 국제 표준화 대응 방안 | **<현황>**<br>- IEC 62443 시리즈는 크게 네 개의 시리즈로 분류되며, 총 13권으로 구성되어 표준화 작업 중으로 미국이 공적표준화 활동에 주도적인 역할을 수행하는 중임<br>**<경쟁표준/기구의 전략>**<br>- 미국 NIST, ISA 99 제조 보안 분야 국제협력체계 구축<br>**<대응방안>**<br>- (국제표준화기구 회의 참여) IEC TC 65 WG 10 보안 분야 그룹 참여를 통해 “제조 정보보호 관리체계” 국제표준 제안 예정(‘18.2Q) |
| 국내 표준화 추진 계획 | **<현황>**<br>- TTA CPS PG(PG 609)에서 제조 보안 관련 표준 개발 중<br>**<추진계획>**<br>- (연구개발 표준화 연계 개발) 국가기술표준원 국제표준화 기술력 향상사업에 참여하여 국제표준화 작업 추진<br>- (국내 표준화 활동기반 마련) TTA PG 609 참여 및 제조보안 포럼 창설을 통한 표준화 기반 마련(‘18) |
| 표준 특허 전략 | **- 표준 및 R&D 초중기 전략 : 표준화 방향에 따른 출원 및 기고 전략**<br>- (세부전략) 국제 표준화와 작업 방향을 예측하여 관련 기술 특허 확보 |
| 기술개발-표준화-IPR 연계 방안 | - 표준화-기술개발 병행추진<br>- (세부전략) 제조 분야 보안기술 Use Case를 확보하여 국제 표준화 작업 추진 |

## 3.3. 오픈소스 국내외 추진전략

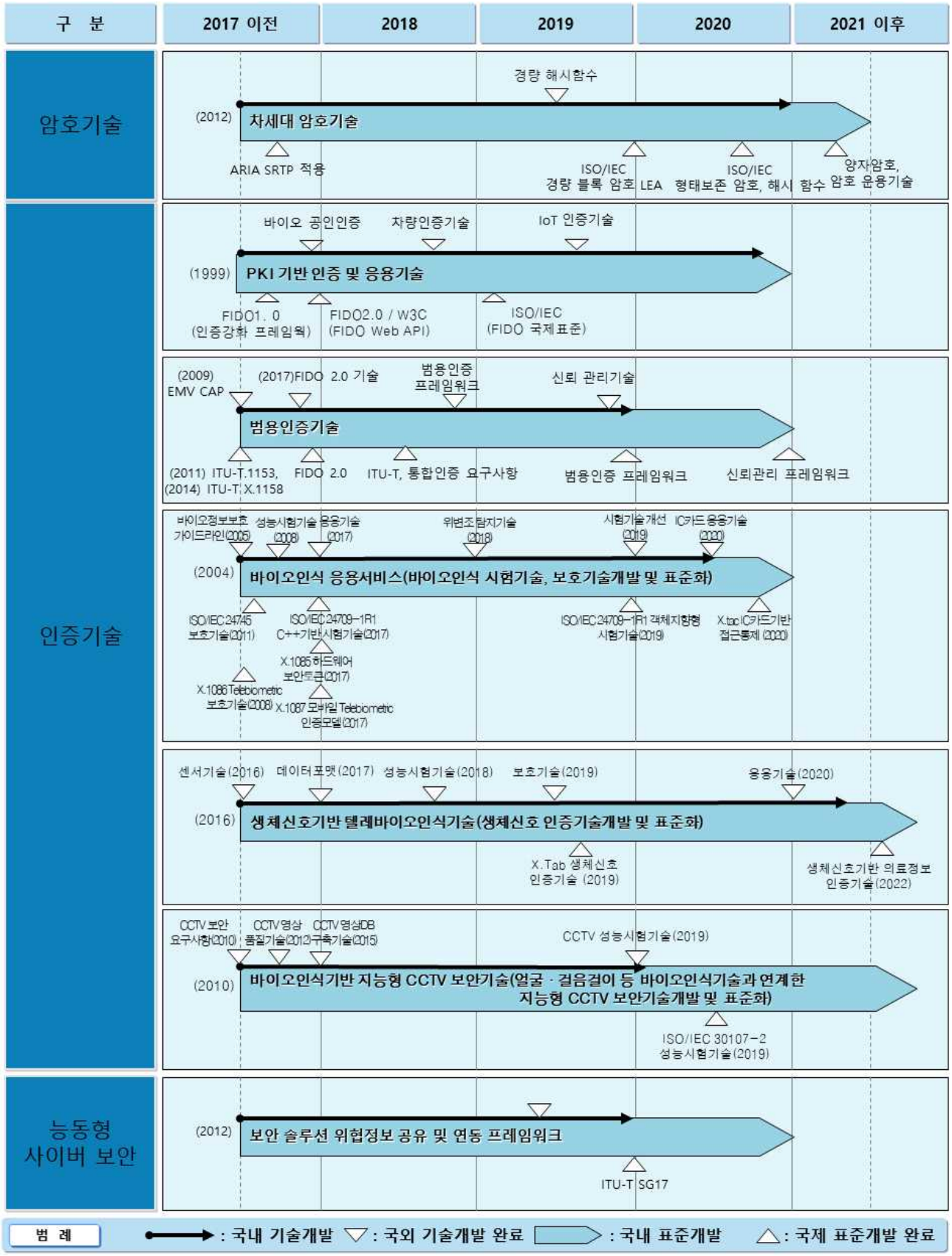


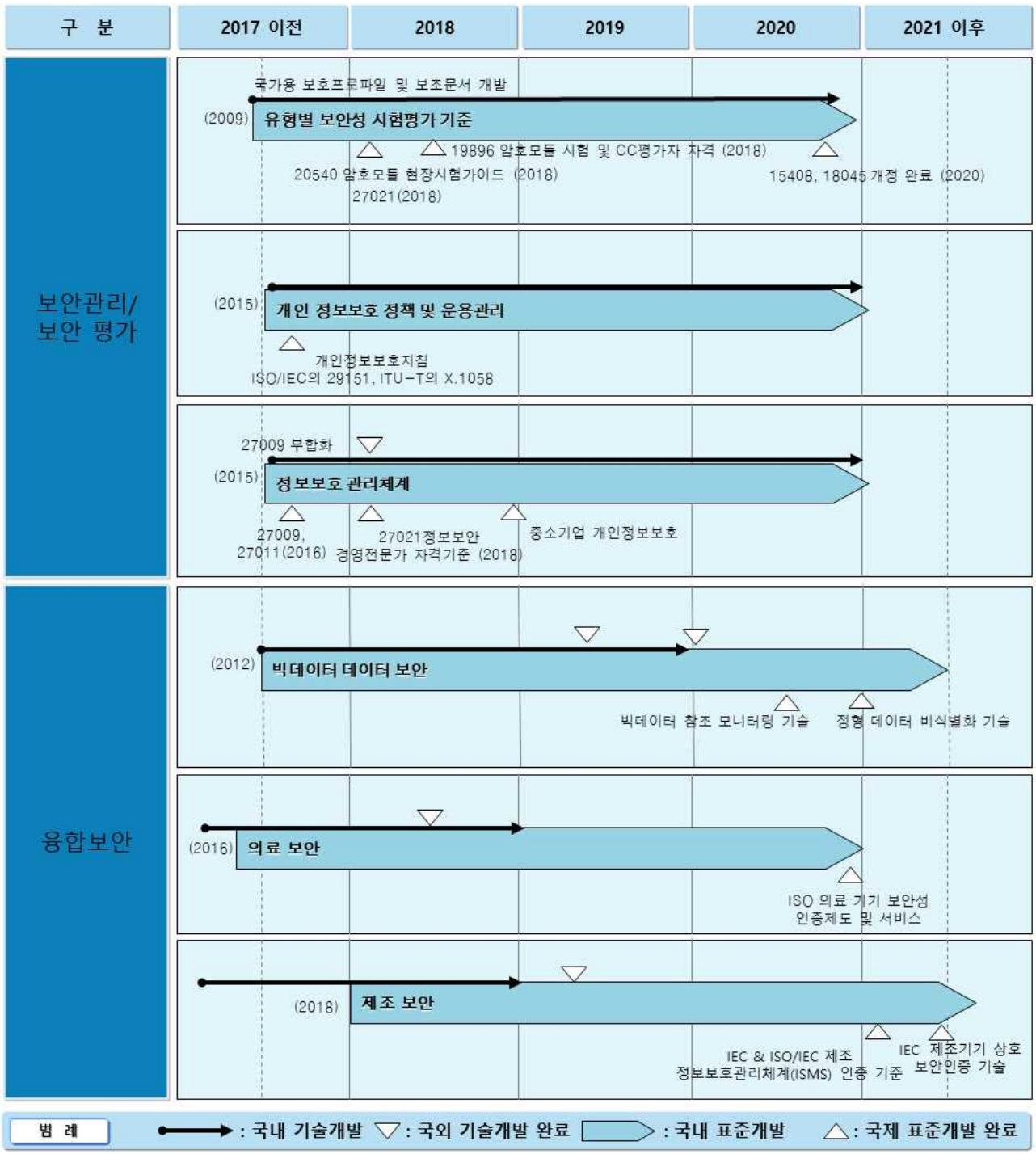

<오픈소스 커뮤니티 대응체계>

| | |
|---|---|
| **오픈소스 대응전략** | - 보안기술 분야에 대해서는 OpenSSL, OpenSSH, OWASP등의 다양한 오픈소스 커뮤니티를 통해 활발한 활동이 이루어지고 있음. 보안 분야 오픈소스의 국내 역량 증진을 위해서는 국내 개발자들의 오픈소스 프로젝트에 대한 참여를 장려하고 실용화된 구현 기술에 대해 공유를 통한 활성화를 지원할 수 있는 제도 마련이 필요함. 국내 보안전문가 및 개발자들이 오픈소스 커뮤니티에 적극적으로 참여 할 수 있도록 함으로써 국내 기술력의 발전에 지속적으로 영향력을 높일 수 있는 기회의 제공 필요<br>- 보안관련 오픈소스 프로젝트는 특정 프로젝트로 국한 되지 않고 버티컬하게 활동되고 있거 많은 오픈소스커뮤니티에서 공통으로 다루고 있음. 국내 업체의 참여는 활발하지 않으나, 보안 분야에 있어 연관기관과 분야별 전문가들에 의한 국제 표준과의 연계를 위한 활동이 활성화 되고 있는 단계임. 오픈소스 프로젝트의 동향 공유 및 기술 전파를 통해 다양한 글로벌 오픈소스 프로젝트의 참여가 이루어 질 수 있도록 권장 필요 |
| **표준화 연계전략** | - 먼저, 국내 오픈 소스 커뮤니티에서의 활동이 국내 표준화로의 진행은 활발하지 않으나 오픈소스 기술 등에 대한 표준화가 시도 되고 있음 (오픈소스 → 표준화)<br>- 표준화와 오픈소스의 병행을 통해 국내 현실을 반영한 한국형 표준화-오픈소스 프로젝트 모델의 발굴 및 플랫폼화가 필요 (오픈플랫폼 ↔ 표준화)<br>- 다양한 글로벌 오픈소스 프로젝트의 참여 및 이를 통해 오픈소스에 적용이 확인된 국내 기술을 표준화의 주제로 제안하고, 국제표준화 함으로써 국내 기업 개발 기술의 국제표준화 및 이를 통한 글로벌 시장 선점 및 확산을 추진 (오픈소스/오픈플랫폼 → 표준화)<br>- 활용도가 가장 높은 Open SSL 공개소트웨어에 한국의 contribution이 가능하도록 주체하는 기관을 정하고 전략맵에 포함하여 진행하는 것이 필요,<br>국내에서 개발한 암호 알고리즘으로는 SEED가 OpenSSL 암호 라이브러리 cipher 목록에 포함되어 있으며, 신규 버전에 ARIA 추가 예정임. 따라서 SEED와 ARIA 이외의 국제 표준으로 채택된 암호 알고리즘 및 표준화 추진 중인 암호 알고리즘이 cipher 목록에 포함될 수 있도록 적극 참여 추진(표준화 → 오픈소스)<br>- 국내 보안 기술의 활용도가 떨어지는 이유는 글로벌 보안 기술에 포함되어 있지 않기 때문임. 사실상 표준으로 사용되고 있는 오픈소스의 이점을 활용하는 차원으로 국가 경쟁력을 위해 기관과 기업이 참여할수 있도록 장려하는 것이 필요 |

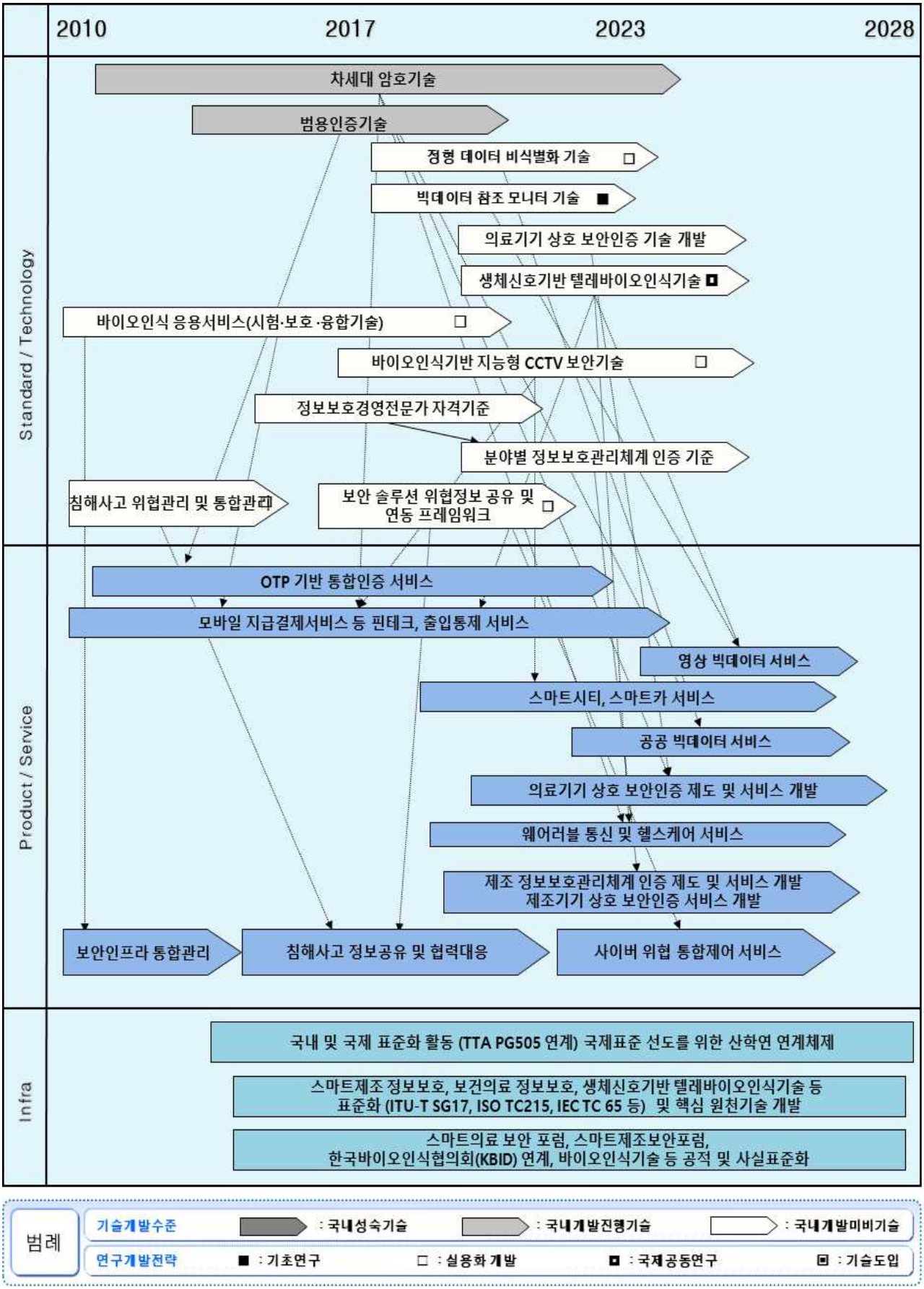
## 3.4. 중기(3개년) 및 장기(10개년) 표준화 계획

○ 중기(2018~2020) 표준화 계획




구 분
2017 이전
2018
2019
2020
2021 이후
보안관리/
보안 평가
국가용 보호프로파일 및 보조문서 개발
(2009)
유형별 보안성 시험평가 기준
19896 암호모듈 시험 및 CC평가자 자격 (2018)
20540 암호모듈 현장시험가이드 (2018)
27021(2018)
15408, 18045 개정 완료 (2020)
(2015)
개인 정보보호 정책 및 운용관리
개인정보보호지침
ISO/IEC의 29151, ITU-T의 X.1058
27009 부합화
(2015)
정보보호 관리체계
27009,
27011(2016)
27021정보보안
경영전문가 자격기준 (2018)
중소기업 개인정보보호
융합보안
(2012)
빅데이터 데이터 보안
빅데이터 참조 모니터링 기술
정형 데이터 비식별화 기술
(2016)
의료 보안
ISO 의료 기기 보안성
인증제도 및 서비스
(2018)
제조 보안
IEC & ISO/IEC 제조
정보보호관리체계(ISMS) 인증 기준
IEC 제조기기 상호
보안인증 기술
범 례
: 국내 기술개발
: 국외 기술개발 완료
: 국내 표준개발
: 국제 표준개발 완료

○ 장기(~2028) 표준화 계획



# [작성위원]

| 구 분 | 소속 | 성명 | 직위 | 국내외 표준화활동 |
|---|---|---|---|---|
| 총괄 | IITP | 이재일 | CP | ▸과기정통부 정보보호 CP |
| 분과장 | NSR | 권대성 | 부장 | ▸JTC1 SC27 Editor<br>▸TTA ITS/차량 ICT(PG905) 위원, 5G포럼 생태계위원회 위원 |
| 위원 | KISA | 김인섭 | 책임 | ▸차세대보안 표준화 |
| 위원 | ETRI | 김종현 | 책임 | ▸ITU-T SG17 에디터<br>▸TTA 사이버보안(PG503) 부의장 |
| 위원 | ETRI | 이주영 | 선임 | ▸사이버보안 프로젝트그룹(PG503) 위원 |
| 소분과장<br>(바이오인식) | KISA | 김재성 | 수석 | ▸ITU-T SG17 에디터, JTC1 SC37 에디터<br>▸바이오인식(PG505) 의장, 정보보호(TC5) 위원 |
| 위원 | ETRI | 김승현 | 선임 | ▸ITU-T SG17 에디터<br>▸TTA PG502 간사 |
| 위원 | 글로벌피디 | 홍동표 | 대표 | ▸FIDO Alliance 국제경영임원 (BOD) |
| 위원 | NSR | 박제홍 | 선임 | ▸IETF 암호 표준화<br>▸TTA 정보보호기반 프로젝트그룹(PG501) 부의장 |
| 위원 | 윈스 | 이수현 | 팀장 | ▸JTC1 SC27 에디터<br>▸TTA PG504 위원 |
| 위원 | 포워드벤처스 | 김창오 | 팀장 | ▸ITU-T SG17 Q3 에디터, ITU-T SG17 Q5 부라포쳐 |
| 위원 | TCA 서비스 | 오경희 | 대표 | ▸ITU-T SG 17 에디터<br>▸TTA 응용보안/평가인증(PG504) 특별위원 |
| 위원 | 호서대 | 이태진 | 교수 | ▸TTA PG503 의장 |
| 위원 | 경인여대 | 한승진 | 교수 | ▸TTA PG505 간사 |
| 위원 | 슈프리마 | 전동훈 | 수석 | ▸TTA PG505 부의장 |
| 위원 | 고려대 | 한근희 | 교수 | ▸ISO TC215 위원, 스마트헬스표준포럼 위원,<br>▸TTA PG505 위원 |
| 위원 | 유엠로직스 | 남기효 | 부사장 | ▸차세대보안 표준화 |
| 위원 | ETRI | 박종열 | PL | ▸차세대보안 표준화 |
| 위원 | ETRI | 나재훈 | 실장 | ▸ITU-T SG17 WP4 부의장, Q7/17 라포처<br>▸TTA 응용보안/평가인증(PG504) 의장 |
| 위원 | 한국정보인증 | 김재중 | 이사 | ▸차세대보안 표준화 |
| 위원 | ETRI | 진승헌 | 본부장 | ▸ITU-T SG17 위원<br>▸TTA 개인정보보호/ID관리(PG502) 의장 |
| 위원 | 카이랩 | 배인호 | 대표 | ▸유헬스(PG419), 웰니스휴먼케어(WG4196), 개인건강정보(WG4195) 간사 |
| 특허분석 | KISTA | 김병년 | 선임 | ▸차세대보안 특허분석 |
| 사무국 | TTA | 박수정 | 선임 | ▸TTA 개인정보보호/ID관리, 블록체인 보안 (PG502) 등 정보보호분과 PG 간사 |
| 사무국 | TTA | 오흥룡 | 책임 | ▸ITU-T SG17 위원<br>T▸TA 정보보호기술위원회 |
| 간사 | TTA | 김영재 | 수석 | ▸TTA 표준화전략맵 차세대보안 분야 간사 |

# [참고문헌]


1. 정보통신용어사전, http://www.tta.or.kr
2. 정보통신표준화위원회, http://committee.tta.or.kr
3. Biometrics Research Group, Inc., http://www.biometricupdate.com/research, 2014
4. Korea association for Bioemtric IDentity security(KBID), http://kbid.or.kr, 2016
5. 김재성, 생체신호 인증기술 및 표준화 동향, TTA 저널, 2016.6
6. 개인정보보호 가이드라인 -의료기관편(2015), 보건복지부/행정자치부
7. 개인정보보호 가이드라인 - 사회복지시설편(2013), 보건복지부/안전행정부
8. 개인정보보호 가이드라인 - 약국편(2013), 보건복지부/안전행정부
9. 보건의료정보 가이드라인 - 보건복지부/한국보건산업진흥원
10. ISO/DIS 27799:2014(E), "Health informatics - Information security management in health using ISO/IEC 27002"
11. ISO/IEC 27001:2013, "information security management system"
12. ISO/IEC 27002:2013, "Code of practice for information security controls"
13. NIST 800-16 "Information Technology Security Training Requirements:A Role- and Performance-Based Model"
14. NIST 800-50 "Building an Information Technology Security Awareness and Training Program“
15. 국가기술표준원, “2017 표준기반 R&D로드맵”, 2017년 5월
16. 국가기술표준원, “스마트공장 기술 및 표준화 동향”, 2015년 9월
17. FIDO Alliance, Universal Authentication Framework v1.1, 2017.2
18. W3C, Web Authentication: An API for accessing Public Key Credentials (draft), 2017.5
19. IETF RFC-4226, HOTP: An HMAC-Based One-Time Password Algorithm, 2005.12
20. IETF RFC-6749, The OAuth 2.0 Authorization Framework, 2012.10
21. ITU-T X.1254, Entity authentication assurance framework, 2012.9
22. OASIS Security Services Technical Committee, Security Assertion Markup Language V2.0, 2005.3
23. OASIS Web Services Federation TC, WS-Federation, 2009.5
24. OASIS Identity Metasystem Interoperability TC, SAML V2.0 Information Card Token Profile Version 1.0, 2010.9
25. OASIS Trust Elevation TC, Authentication Step-Up Protocol and Metadata V1.0, 2017.5
26. ISO/IEC 29100:2011, Information Technology -- Security techniques – Privacy Framework”, 2011.12
27. NIST, De-identification of Personally Identifiable Information NSTR 8053, 2015.10
28. NIST, De-identification Government Datasets, 2016.12

29. ITU-T X.fdip, Framework of de-identification processing service for telecommunication server providers, TD-2997, 2016.08.29.
30. 한국산업인력공단, 정보보호관리·운영, 2017, http://ncs.go.kr

# [약어]

| | |
|---|---|
| BERC | Biometric Engineering Research Center |
| CBP | Customs and Border Protection |
| CC | Common Criteria |
| CCRA | Common Criteria Recognition Arrangement |
| CCUF | Common Criteria Users Forum |
| CEM | Common Methodology for Information Technology Security Evaluation |
| C-ITS | Cooperative-Intelligent Transport Systems |
| cPP | collaborative Protection Profile |
| CTAP | Client to Authenticator Protocol |
| ETSI | European Telecommunications Standards Institute |
| FIDO | Fast IDentity On-line alliance |
| ICO | Information Commissioner's Office |
| iTC | international Technology Community |
| KBID | Korea association for Biometric IDentity security |
| KCCUF | Korea Common Criteria Users Forum |
| KCMVP | Korea Cryptographic Module Validation Program |
| FIDO | Fast IDentity Online |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| OASIS | Organization for the Advancement of Structured Information Standards |
| OASIS CTI | OASIS Cyber Threat Intelligence |
| PSD2 | The Second Payment Services Directive |
| PKI | Public Key Infrastructure |
| PIV | Personal Identity Verification |
| QKD | Quantum Key Distribution |
| SAML | Security Assertion Markup Language |
| SD | Supporting Document |
| STIX | Structured Threat Information eXpression |
| TAXII | Trusted Automated eXchange of Indicator Information |
| UKAN | UK Anonymisation Network |
| WAVE | Wireless Access for Vehicle Environment |