



IV

차세대보안 차세대보안

차세대보안

목차

I

표준화 개요

1.1. 기술 개요	293
1.2. 중점 표준화 항목	294
1.3. 표준화 비전 및 기대효과	301

II

국내외 현황분석

2.1. 연도별 주요 현황 및 이슈	304
2.2. 정책 현황 및 전망	305
2.3. 기술개발 현황 및 전망	308
2.4. IPR 현황 및 전망	314
2.5. 표준화 현황 및 전망	317
2.6. 오픈소스 현황 및 전망	331

III

국내외 표준화 추진전략

3.1. 표준화 SWOT 분석	332
3.2. 중점 표준화 항목별 국내외 추진전략	333
3.3. 중기(3개년) 및 장기(10개년) 표준화 계획	360

작성위원	363
------------	-----

참고문헌	364
------------	-----

약어	366
----------	-----

I. 표준화 개요

1.1. 기술 개요

차세대 보안기술은 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 침해사고를 방지하며, 여러 기술이 융합된 시스템에서의 보안을 제공하기 위한 기술로, 암호기술, 인증서 및 바이오인식 기반 인증기술, 사이버 보안기술, 시험평가 기준 및 관리를 위한 보안관리/평가 기술, 의료보안 및 제조보안 등을 위한 융합보안기술로 구분



<차세대보안 기술 개요도>

1.2. 중점 표준화 항목

○ 중점 표준화 항목 범위의 설정

- (중분류 범위 설정) 보안의 공통 기반기술인 암호기술, 인증기술, 사이버 보안기술, 이를 관리/평가하기 위한 기술, 각종 ICT에 적용하기 위한 융합보안기술 중 4차 산업혁명을 뒷받침할 수 있는 기술을 “차세대 보안기술”로 설정
- (중점 표준화 항목 선정 이유) 표준화전략맵 차세대보안 분과에서는 아래 기술을 중점 표준화 항목으로 선정
 - (암호기술) 암호 알고리즘에 대한 표준화가 선행되어야 하는 암호 프로토콜 운용 기술과 양자 암호통신 기술 기반 구축과 실증을 통해 표준화 항목 도출이 필요한 양자 암호기술을 제외하고 암호 알고리즘을 중점표준화항목으로 선정
 - (인증기술) 기존 인증기술을 기반으로 관련 산업계의 수요가 급격히 증가하고 표준화가 빠르게 진행되고 있는 PKI 기반 기기인증, FIDO 및 응용기술, 멀티팩터 인증기술, 바이오인식 응용서비스, 생체신호기반 텔레바이오 인증기술을 중점표준화항목으로 선정
 - (사이버 보안) 사이버 공격이 정교해지면서 기존 네트워크 보안장비들의 보안 플랫폼은 머신러닝, 인공지능(AI) 기술을 활용하는 사이버 위협 인텔리전스 기술로 발전하고 있으며, 능동형 사이버 침해정보 및 위협정보에 대한 수집, 보존, 분석 및 공유 기술 중 능동적 사이버보안 기술 개발에 필수적인 사이버 침해정보 수집 및 보존 기술을 중점표준화항목으로 선정
 - (보안관리/보안평가) 보안평가는 보안기능과 암호모듈 검증에 대한 평가 기술이 있으나, 다양한 ICT 기술이 접목된 IT제품의 안전성과 신뢰성 확보를 위한 IT제품 보안성 표준화를 중점표준화 항목으로 선정
 - (융합보안) 기존 산업에서 ICT 기술을 접목함으로써 앞서 기술을 선점할 수 있는 분야 중 다양한 분야에 포함될 수 있는 공통 성격이 있으며, 국제 표준화하여 선도적으로 관련 분야 기술을 선점할 수 있는 의료보안, 제조보안을 중점 표준화 항목으로 선정

표준화 항목		표준화 내용	Target SDOs	표준화 특성	중점 항목
암호 기술	암호 알고리즘	신규 ICT 환경(IoT/M2M, 클라우드, 빅데이터, 스마트기기, DBMS 등)의 정보보호에 적합한 차세대 암호 알고리즘 표준	JTC1 SC27, IETF	⑤	O
	암호 프로토콜 운용기술	주요 암호/인증 프로토콜(TLS, IPsec 등)에 차세대 암호 알고리즘을 적용하기 위한 표준	IETF	⑤	X
	양자 암호 기술	양자 암호 키 분배 기술 규격, 안전성 표준	JTC1 SC27, ETSI	③	X
인증 기술	PKI 기반 기기인증	다양한 IoT 기기를 식별/인증하는 기기인증 분야, 특히 자율협력주행(C-ITS)을 위한 PKI 기반의 차량인증 표준	IEEE 802, ITU-T SG17, CAMP	③	O
	FIDO 및 응용기술	FIDO 2.0에 기반을 둔 O2O 차세대 바이오 인증으로 스마트폰/App, PC/웹브라우저, 그 외 확장된 Device/응용솔루션의 규격, 성능평가 표준	FIDO Alliance	⑤	O

표준화 항목		표준화 내용	Target SDOs	표준화 특성	중점 항목
	멀티팩터 인증기술	하나 이상의 인증 수단을 활용하여 객체를 인증하는 기술 및 규격 표준	ITU-T SG17, JTC1 SC27	⑤	O
	바이오인식 응용 서비스	IC카드, PKI 기술, 의료정보 보안기술 등 바이오인식기반 융합기술 - 모바일 바이오인식 응용기술 및 시험 표준 - 위변조 방지 등 바이오정보 보호표준	JTC1 SC27/SC37, ITU-T SG17, ABC	⑤	O
	생체신호기반 텔레바이오 인증기술	생체신호를 이용한 인증기술 - 생체신호 인증정보 통신 프로토콜 표준 - 생체신호 인증 알고리즘 성능 시험 표준 - 생체신호인증기반의 헬스모니터링 분석 표준	ISO TC215, ITU-T SG17	⑤	O
	프라이버시 보호 인증기술	영지식, blind 전자서명 등에 기반한 사용자의 프라이버시를 보호하는 인증 표준	JTC1 SC27, ITU-T SG17	⑤	X
	PKI 기반 사용자 인증	사용자를 식별/인증 기술로 인증, 바이오 인증, 블록체인 인증 등 사용자 인증 표준	JTC1 SC27, ITU-T SG17	⑤	X
	ID 관리 기술	ID 통합관리 서비스를 제공하기 위한 기반 및 응용 표준	JTC1 SC27, ITU-T SG17	⑤	X
	비대면 본인확인 기술	비대면 본인확인을 제공하는 인증 서비스의 기반 및 응용 표준	JTC1 SC27, ITU-T SG17	⑤	X
사이버 보안	능동형 사이버보안 침해정보 수집 및 보존 기술	사이버 침해정보를 수집 및 보존하기 위한 기능 및 구현 지침 표준	ITU-T SG17, JTC1 SC27, ETSI	③	O
	사이버 위협정보 공유 포맷 및 프로토콜	STIX/TAXII 기반의 사이버 위협분석 정보 표현 포맷 표준 및 정보 전달 프로토콜 표준	ITU-T SG17 WG2, OASIS CTI TC	⑤	X
	사이버 위협정보 공유 유즈케이스	STIX/TAXII 기반의 사이버 위협분석 정보 공유 유즈케이스 표준	ITU-T SG17 WG2, OASIS CTI TC	②	X
	AI 기반 악성코드 분석 및 백신 기술	Zero-day 악성코드 대응을 위한 AI 기반 악성코드 분석 및 백신 표준	ITU-T SG17	③	X

표준화 항목		표준화 내용	Target SDOs	표준화 특성	중점 항목
보안 관리/ 보안 평가	정보보호 관리 체계	27002에 기초한 블록체인 분야 정보보안통제 - 서비스 제공자와 이용자 측면에서 수행해야 할 블록체인 보안 통제 및 일반 보안통제의 구현 지침 표준	ISO TC307, JTC1 SC27, ITU-T SG17	②	O
	IT제품 보안성 평가기준	IT제품 보안성 평가기준 표준	JTC1 SC27 WG3, CCRA, CCUF	②	O
	차세대 정보보호 관리 체계	사이버 보안 개요 및 개념 표준 - 사이버 보안 프레임워크를 개발하기 위한 지침 표준 - 의도적인 정보보안 사고에 대한 보험을 제공하기 위한 보안 지침 표준	JTC1 SC27, ITU-T SG17	①	X
	개인정보보호 정책 및 운영관리 기술	개인정보보호 정책 및 운영 관리관리 표준	JTC1 SC27, ITU-T SG17	①	X
	암호모듈 시험평가 기준	CC 평가기관 및 암호모듈 시험기관 자격기준 - 암호모듈 시험기준 표준	JTC1 SC27	②	X
융합 보안	진료정보 교류시 보안표준 모델	중앙집중형, 지역 분산형, 대등관계형 등 진료정보 교류 유형에 따른 적합한 보안 모델	ISO TC215, ITU-T SG17	①	O
	의료기기 안전 및 보안 프레임워크	생명에 연계된 의료기기에 대한 안전과 보안 표준 프레임워크	ISO TC215, ITU-T SG17, IEEE PHD WG	②	O
	스마트공장 기기 상호 보안인증기술	스마트공장 내 상호인증에 필요한 기기인증서 프로파일과 알고리즘 및 기기인증서 발급/관리를 위한 인프라스트럭처	IEC TC65, ISA 99	②	O
	중소기업용 스마트공장 보안 관리 기술	중소기업 스마트공장에 적용될 보안 플랫폼 및 적정 보안 통제 항목 및 보안 플랫폼	IEC TC65, ISA 99	②	O
	스마트의료정보 통합보안 체계	모바일, 클라우드, 빅데이터, 사물인터넷 등이 접목된 의료정보시스템의 규모 및 특성별로 적합한 보안 가이드라인	ISO TC215 WG4	①	X
	원격의료 보안 가이드라인 표준	원양어선, 군 부대, 섬, 격오지 등의 원격의료 서비스 모델에 대한 보안 가이드라인	ISO TC215	②	X
	스마트공장 최소보안요구사항	공장에서 발생 가능한 침해 위협 요소 소개, 위협에 대한 최소한의 대응방안	IEC TC65, ISA 99	②	X

표준화 항목		표준화 내용	Target SDOs	표준화 특성	중점 항목
의료 정보보호관리체계 인증기준		의료정보시스템 및 기간계 시스템 등에서 처리되는 의료정보의 기밀성, 효율성, 가용성을 수준별 인증을 부여할 수 있는 인증기준	ISO TC215	②	X
의료정보 비식별화 표준		보건의료 환경과 빅데이터 특성을 적절하게 반영한 상위 수준의 보건의료 빅데이터 정보보호 및 개인정보보호 프레임워크	ISO TC215	②	X
의료 정보공유분석센터 (ISAC) 표준 모델		의료기관을 대상으로 해킹 및 사이버테러 등 전자적 침해행위에 대한 공격을 효과적으로 예방, 탐지 및 대응할 수 있는 시스템 및 조직	ISO TC215	②	X
제조 분야 ISMS 인증기준		제조분야에 특화된 통제항목을 도출하고 ISO/IEC 27001, 27002를 기반으로 스마트공장에 적용 가능한 정보보호 관리체계	IEC TC65, ISA 99	②	X
스마트공장 설비의 보안 등급 인증기준		각 설비의 보안 취약점을 분석하고 보안 구비요건에 따라 등급화하고 설비의 보안 기술 적용 등급 확인하고 각 설비의 보안 등급에 따라 차별화 된 인증 부여	IEC TC65, ISA 99	②	X
스마트공장 네트워크 연결에 따른 보안 적용 차등화 기준		각 네트워크 상의 입출력 Data 종류 및 네트워크 연결 범위에 따라 차등 적용되는 보안 기술	IEC TC65, ISA 99	②	X
스마트공장 정보보호 체계		RAMI 4.0, Industries 4.0, IEC 62443, ISA 99, NIST SP 800-82 ICS Security 등을 기반으로 스마트공장 에서 보안을 적용할 대상과 범위, 규모별, 산업별 공통 분모를 고려한 표준 모델	IEC TC65, ISA 99	②	X
스마트공장 정보보호 프레임워크		정보보호 체계(Security Architecture)에 대한 구체적인 실현·구현 모델 표준으로 단계별 적용 방안(예:Level0~5)	IEC TC65, ISA 99	①	X
스마트공장 위험관리 프레임워크		스마트공장의 위험 분석·평가 등 관련 국제표준 연구 및 국내 스마트공장 환경에 적합한 사이버보안 위험관리 프레임워크와 연계방안	IEC TC65, ISA 99	①	X
해사클라우드 인가정보 상호연동 가이드라인		해사클라우드에서 사용자 및 해사 자원의 인가정보를 상호 연동하기 위한 가이드라인 제시	IALA ENAV	⑤	X
영상감시시스템 암호화 기술		CCTV 카메라와 스토리지 디바이스간의 암호화 방법에 대한 표준화 추진	ITU-T SG17, IEC TC79	③	X
ITS 보안위협 및 가이드라인		V2X 통신과 자율주행 차량 및 기반 서비스에 대한 보안 위협 식별 및 가이드라인 표준 개발 * '자율자동차' 중점기술 참조	ITU-T SG17, SAE DSRC Committee, ISO TC204 WG16	②	X

표준화 항목		표준화 내용	Target SDOs	표준화 특성	중점 항목
	자율주행 보안 시스템 프레임워크	안전한 자율주행을 위한 차량 내/외부에서 발생할 수 있는 악의적인 공격 및 이상행위 탐지 기술 표준 개발 * ‘자율자동차’ 중점기술 참조	ITU-T SG16/SG17, SAE DSRC Committee, ISO TC22 SC31/SC32	③	X
	IoT 통합보안 프레임워크 표준	IoT 단말, 네트워크 및 클라우드 전체를 포함하는 통합보안 플랫폼 표준화 - IoT 디바이스 자율보안, IoT 네트워크 보안, IoT 보안관리 통합을 위한 연동 인터페이스 정의 - IoT 통합보안 프레임워크의 글로벌 사실표준 플랫폼 적용 기술 * ‘사물인터넷’ 중점기술 참조	OCF, oneM2M, ITU-T SG17	③	X
	블록체인기반 IoT 인증 프레임워크 표준	블록체인을 IoT 보안/인증의 기반기술로 이용하는 프레임워크 - 블록체인기술 기반으로하는 IoT기기-IoT서비스 상호인증 - 블록체인기술 기반의 접속기록 변조 방지 및 확인 - 탈 중앙화 공공개방망 IoT 단말접속 보안기술 * ‘사물인터넷’ 중점기술 참조	oneM2M SEC, IEEE SA, FIDO Blockchain SG	③	X
	분산원장기반의 지불결제 서비스에 대한 보안 위협 및 보안 요구사항 표준	분산원장기반 지불결제 서비스를 분석하고, 이에 기초하여 발생할 수 있는 보안 위협 및 요구사항을 표준화 - 분산원장기반 지불결제 서비스 Use cases 및 용어 정의 제시 - 분산원장기반 지불결제 서비스 모델 제시 - 분산원장기반 지불결제 서비스 보안 위협 분석 - 분산원장기반 지불결제 서비스 보안 요구사항 * ‘블록체인’ 중점기술 참조	ITU-T SG17	②	X
	분산원장기술을 활용한 온라인투표에 대한 보안 위협 표준	정보통신 인프라 기반의 온라인투표 시스템의 모델을 제시하고, 투표 절차 상에 잠재된 보안 위협을 크게 5가지 유형으로 분류하여 식별 및 정의 - DLT를 활용한 온라인투표의 범위 정의 - 주요국가의 DLT를 활용한 온라인투표 활용사례 제시 - DLT를 활용한 온라인투표모델 제안 - DLT를 활용한 온라인투표모델에 근거한 보안 위협정의 * ‘블록체인’ 중점기술 참조	ITU-T SG17	②	X
	개인정보보호 지침 표준	블록체인의 무결성 관리기능을 개인정보의 보호 및 기밀성에 적용하는 표준 - 무결성을 바탕으로 정보가 공개되는 환경에서 개인정보의 보호 및 기밀성을 고려하는 지침 * ‘블록체인’ 중점기술 참조	ISO TC307, JTC1 SC27 WG5, ITU-T SG17	①	X

<표준화 특성>

① : 개념, 정의 표준

② : 유즈케이스 및 요구사항 표준

③ : 기능 도출 및 참조구조 표준

④ : 데이터포맷, 스키마 표준

⑤ : 프로토콜, 인터페이스 표준

○ 추진경과

- Ver.2017(2016년)에서는 Ver.2016과 동일하게 3개 분야(공통기반보안, 네트워크/디바이스보안, 서비스/융합보안)로 구분하고, 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 추가
- Ver.2018(2017년)에서는 이전의 3개 분야(공통기반보안, 네트워크/디바이스보안, 서비스/융합보안)를 하나로 통합하고, 암호기술, 인증기술, 능동형사이버보안, 보안관리/보안평가, 융합보안 그룹으로 나누어 각 그룹 별 표준화 항목을 선정
- Ver.2019(2018년)에서는 Ver.2018과 동일하게 암호기술, 인증기술, 사이버보안, 보안관리/보안평가, 융합보안 그룹으로 나누어 각 그룹 별 표준화 항목을 선정하였으며, 범용인증기술의 모호성 해소를 위하여 FIDO 및 응용기술, 멀티팩터 인증기술로 세분화하였으며, 다른 분과의 보안기술은 융합보안에 참조로 포함

<버전별 중점 표준화 항목 비교표>

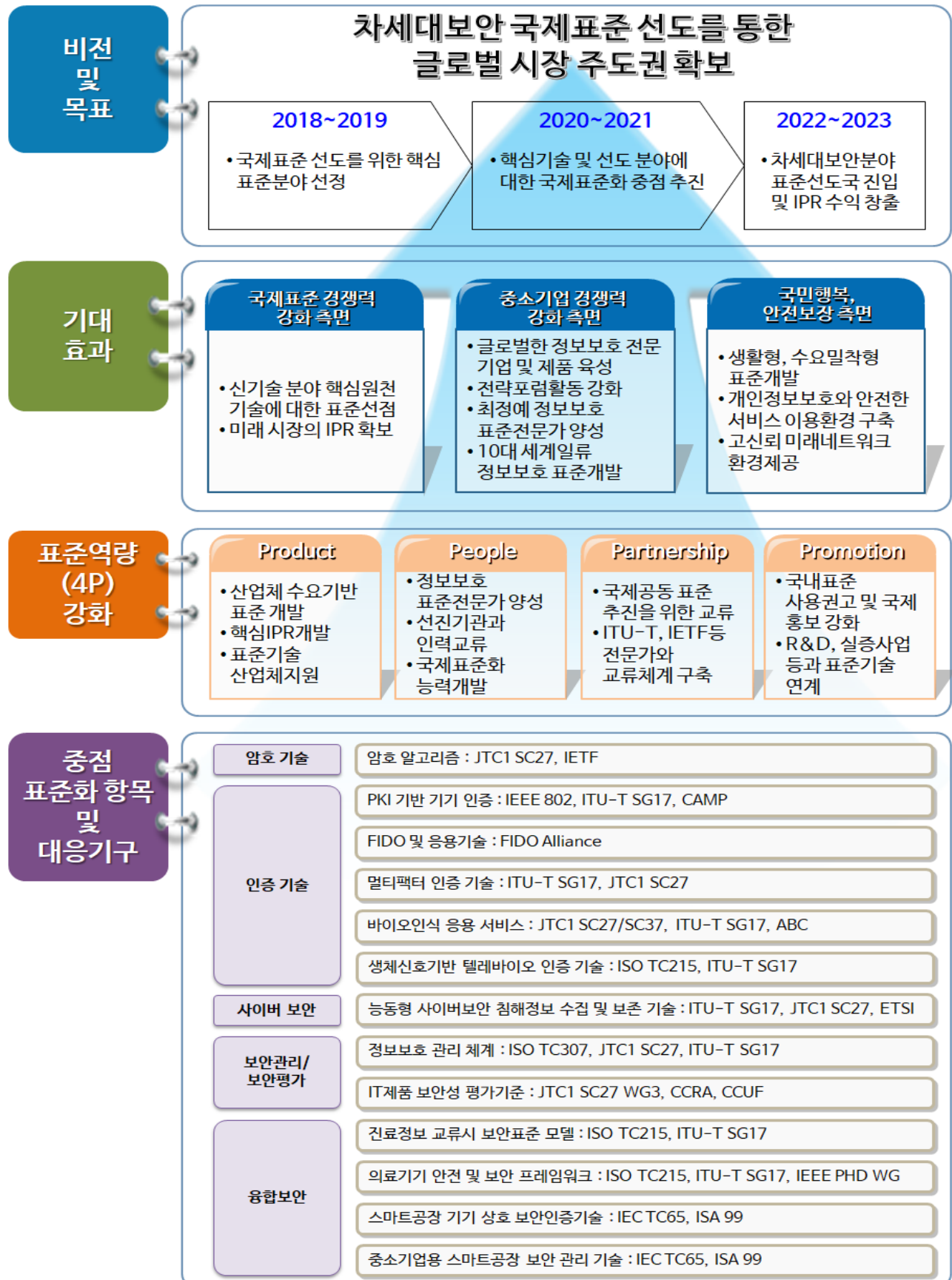
* Ver.2019 신규 항목

구분	Ver.2017	Ver.2018	Ver.2019
암호기술	차세대 암호 및 적용	차세대 암호기술	암호 알고리즘
인증기술	PKI 기반 인증 및 응용기술	PKI 기반 인증 및 응용기술	PKI 기반 기기 인증
	범용인증기술	범용인증기술	FIDO 및 응용기술
	-	-	멀티팩터 인증기술*
	바이오인식 응용 서비스	바이오인식 응용 서비스	바이오인식 응용 서비스
	생체신호기반 텔레바이오인식 기술	생체신호기반 텔레바이오인식 기술	생체신호기반 텔레바이오인증기술
	모바일 결제·인증 기술	-	-
	개인정보보호 정책 및 운영관리 기술	개인정보보호 정책 및 운영관리 기술	-
사이버보안	-	-	능동형 사이버보안 침해정보 수집 및 보존 기술*
보안관리/보안평가	정보보호 경영전문가 자격 기준	정보보호 관리체계	정보보호 관리체계
	정보보호 감사관리 지침		
	분야별 정보보호 관리체계 및 인증		
	유형별 보안성 시험평가기준	유형별 보안성 시험평가기준	IT제품 보안성 평가기준
융합보안	전자건강기록(EHR) 보안 프레임워크 기술	의료보안	진료정보 교류시 보안표준 모델*
	개인건강기록(PHR) 서비스 보안		의료기기 안전 및 보안 프레임워크*
	-	제조보안	스마트공장 기기 상호 보안인증기술*
			중소기업용 스마트공장 보안 관리 기술*

구분	Ver.2017	Ver.2018	Ver.2019
	SDN/NFV 보안 프레임워크와 메커니즘	-	-
	SDN/NFV 보안 응용 및 서비스	-	-
	보안정보공유 및 연동 프레임워크	보안 솔루션 위협정보 공유 및 연동 프레임워크	-
	악성코드 분석 및 보고 형식	-	-
	침해사고 분석을 위한 네트워크 포렌식 도구 요구사항	-	-
	스마트폰 환경에서의 저장장치 보안 프레임워크	-	-
	스마트폰 기반의 봇넷 대응을 위한 보안 요구사항	-	-
	클라우드 컴퓨팅 서비스에서의 개인정보 국외교환 프레임워크	-	-
	클라우드 컴퓨팅 서비스 보안 요구사항	-	-
	클라우드 인증 및 접근제어 보안 프레임워크	-	-
	신뢰 클라우드 연동 보안	-	-
	내용기반 빅데이터 접근제어	빅데이터 데이터 보안	-
	웹 매쉬업 보안	-	-
	유해정보 차단 정책 및 기술	-	-
	융합서비스 환경에서의 속성기반 접근제어	-	-
	핀테크 서비스 보안 기술	-	-
	금융거래 이상 징후 방지 기술	-	-
	바이오인식기반 CCTV보안기술	바이오인식기반 CCTV보안기술	-
	스마트그리드 보안 기능 구조	-	-
	안전한 단방향 데이터통신	-	-
	스마트그리드 보안 기능구조	-	-
	스마트그리드 보안관리	-	-
	스마트그리드 기기 보안	-	-
	V2X 통신 보안 프레임워크	-	-

1.3. 표준화 비전 및 기대효과

○ 표준화 비전



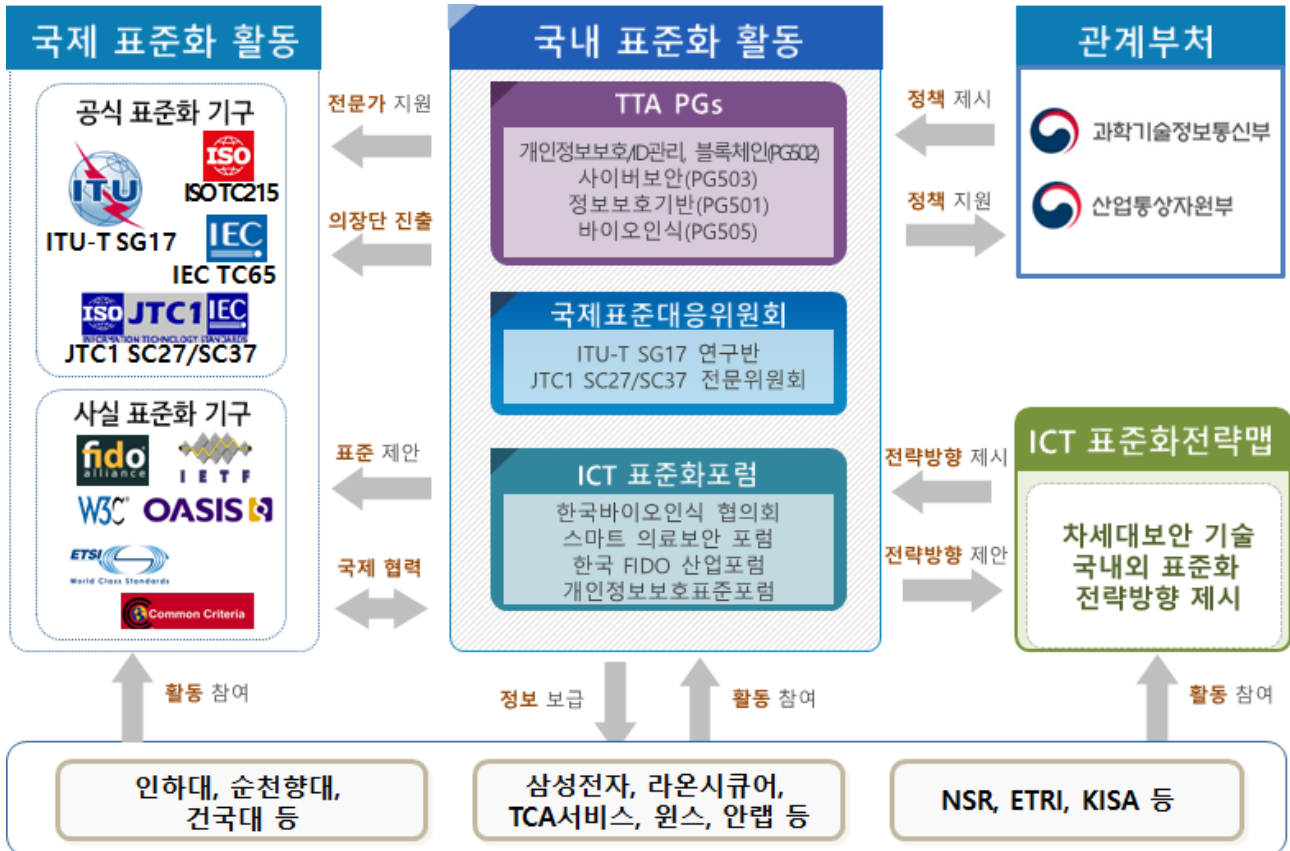
○ 표준화 목표

- 차세대 보안 분야 국제 표준화 선도 및 글로벌 시장 주도권 확보를 위하여 다음과 같은 표준화 목표를 설정
 - (2019년경까지), 신규 분야의 국제표준 선도를 위한 주요 핵심기술에 대한 표준 선점 및 시장 주도권 확보를 위한 IPR 확보에 기여
 - (2021년경까지), 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
 - (2023년경까지), 차세대 보안 분야 표준 선도국 진입 및 IPR 수익 창출에 기여하고 국민이 안전하고 신뢰할 수 있는 미래 네트워크 및 서비스 이용환경을 제공

○ 표준화 기대효과

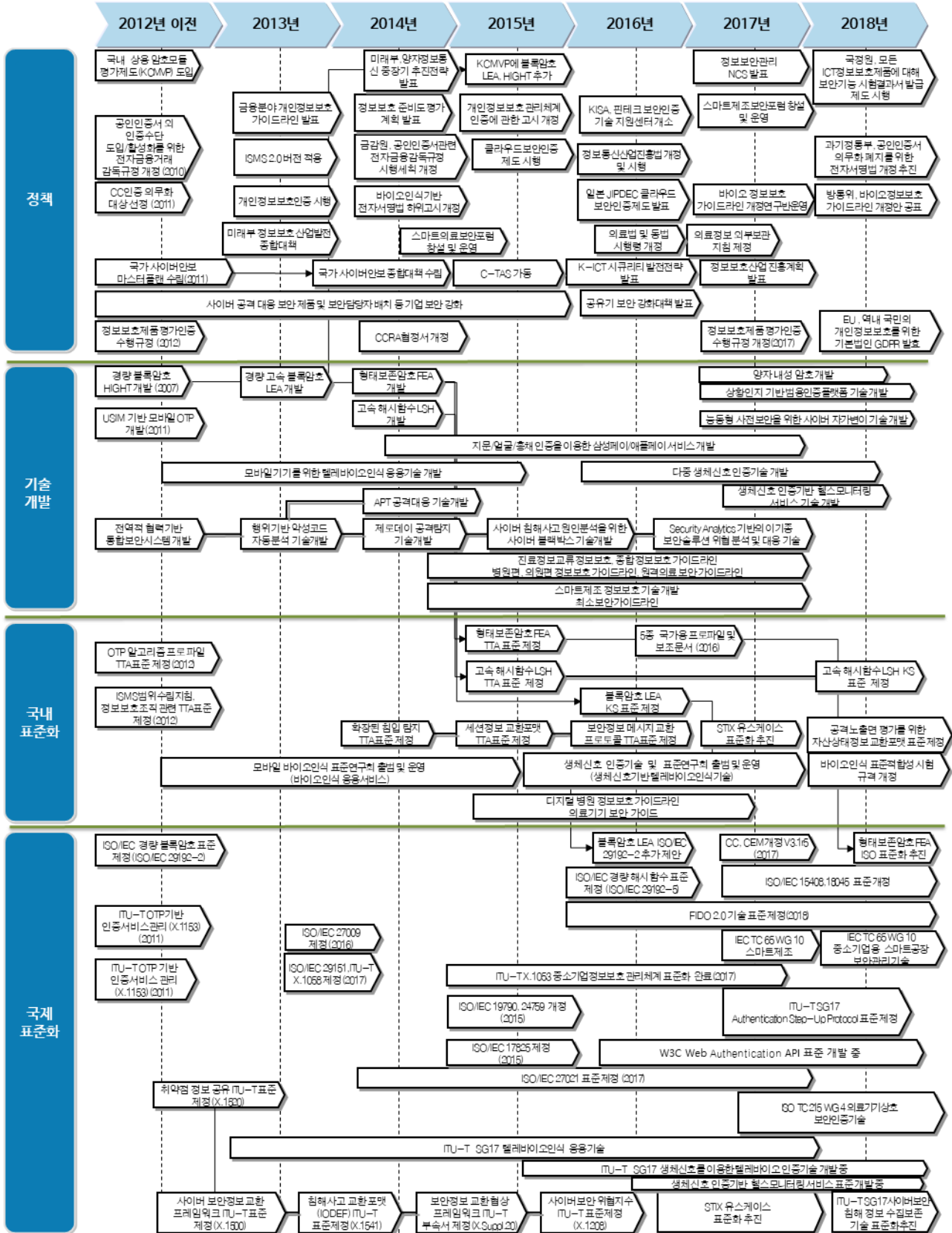
- 국제표준 경쟁력 강화 측면
 - 신규 ICT 환경의 정보보호 핵심 원천기술인 경량, 고속 암호기술과 미래 암호기술인 양자 암호기술 표준 개발 주도
 - 세계 최초로 개발 중인 지문·심전도·심박수 등 다중 생체신호를 이용한 텔레바이오 인식기술을 차세대 바이오인식기술로 발전시켜 국제표준화를 선도
 - 국제표준과 연계하여 4차 산업혁명 시대에 필요한 의료, 제조 등 융합산업에서의 보안 요소기술 선점
- 중소기업 경쟁력 강화 측면
 - 우수 성능의 차세대 암호기술 사전 적용을 통한 국산 암호제품 시장 경쟁력 확보
 - 다양한 인증기술을 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, 국내 보안정책 및 보안 산업계의 의견을 국제표준 개발에 적극 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
 - 중소병원, 공장 등 중소기업 생태에 알맞은 융합 보안기술 개발 및 제공을 통해 선진국과의 격차 해소 및 안전성·보안성 강화
- 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 이용환경 제공
 - 사물인터넷 기기 중 의료·제조 분야 인증제도 및 서비스를 발굴하고 기기·설비들의 안전성·보안성을 보장하기 위한 기기 간 상호 보안 인증 기술 국제표준화와 관련 요소 기술 특허 확보 및 선점을 통한 시장 경쟁력 확보
 - 국민의 생활 안전과 생명과 직결된 의료기기, 제조설비 등에 대한 안전성·신뢰성·보안성 등 확보

○ 표준화 추진체계



II. 국내외 현황분석

2.1. 연도별 주요 현황 및 이슈



2.2. 정책 현황 및 전망

구분	주요 현황
한국	<ul style="list-style-type: none"> - 과기정통부, 공인인증서 의무화 폐지를 위한 전자서명법 개정 추진 중 [2018.4] - 국가용 정보보호제품 보안요구사항중 3종(통합보안관리 제품, 호스트 자료유출방지 제품, 소프트웨어 기반 보안USB제품) 개정 [2018.4] - 국정원, 모든 ICT정보보호제품에 대해 보안기능 시험결과서 발급 제도 시행 [2018.3] - 방통위, 바이오정보보호 가이드라인 개정안 공표 [2018.1] - 2018년 정보보호관리체계 인증제도(ISMS)와 PIMS 통합 [2018] - 2015년부터 시행된 클라우드 보안인증제를 2018년 기존 IaaS에서 SaaS를 포함하도록 범위 확대 [2018] - 정보보호제품 평가인증 수행규정 [2017.9] - 과기정통부, 정보보호시스템 평가인증 지침 고시(과학기술정보통신고시 제2017-7호) [2017.8] - 국가용 통합인증 보호프로파일 V1.0 [2017.8] - 국가용 문서 암호화 보호프로파일 V1.0 [2017.8] - 국가용 데이터베이스 암호화 보호프로파일 V1.0 [2017.8] - 국가용 무선침입방지시스템 보호프로파일 V1.0 [2017.8] - 한국산업인력공단에서 정보보호관리·운영 국가직무능력표준 발표 [2017.1] - IT보안인증사무국은 정보보호제품 평가인증 안내서 작성 [2017] - CCRA의 보조문서로 보증연속성 적용가이드 및 인증서 유효성 적용가이드 발표(2017)에 따라 국내용 인증서 효력연장 수행 가이드 작성 공지 [2017] - 과기정통부, 정보보호시스템 평가인증지침 고시(과학기술정보통신부 고시 제2017-7호) [2017] - 미래부, 양자 암호 등 정보보호 신시장 창출 및 양자 정보통신 지원 확대를 포함하는 2017년 업무계획 발표 [2017] - 바이오정보보호 가이드라인 2차 개정 연구반 운영 중 [2017] - 정보통신망법 개정에 따라서 연간 매출액 또는 세입 등이 1,500억 이상인 자 중 대통령령으로 정하는 기준을 해당하는 기관 중 직전 연도 기준 재학생 수 1만명 이상인 대학 37곳과 「의료법」 제 3조의 4에 따라 상급 종합병원 43개 모두 정보보호관리체계(ISMS) 인증이 의무화됨. 한편 기존 인증 의무대상이었던 전자금융거래법에 따른 금융회사는 중복규제 등의 우려를 이유로 제외 [2016.6] - 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] - 미래부 사이버 위협정보 공유 확대 계획 등 'K-ICT 시큐리티 2020' 발표 [2016.6] - 행정자치부는 "개인정보 비식별 조치 가이드라인"을 발표하고 공공 데이터 공개 가이드라인으로 활용 [2016.6] - 2016년 개인정보보호 관리체계(PIMS)와 개인정보보호인증제(PIPL) 통합 [2016] - 방송통신위원회, 개인정보보호 관리체계(ISMS) 인증 등에 관한 고시 (방송통신위원회 고시 제2015-29호) [2016] - 행정자치부, 개인정보 비식별 조치 가이드라인 고시 [2016] - 「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] - 금융위원회, 전자금융거래감독규정 고시(금융감독위원회공고 제2015-7호) [2015] - 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 [2015]

구분	주요 현황
	<ul style="list-style-type: none"> - ‘사이버위협정보공유에 관한 법률안’ 발의 [2015] - 원자력안전법에 따라 규제기관인 KINS(원자력안전기술원)에서 KINS/RG-N08_22 (디지털 계측 및 제어장치의 사이버보안)가 개정되어 실무적으로 활용 [2014.11] - KISA, C-TAS(Cyber Threat Analysis & Sharing) 구축 [2014] - 미래부, 양자 정보통신 중장기 추진전략을 수립하고 단계별로 수도권과 대전권 연결 양자 암호통신 시험망 구축 추진 [2014] - 바이오인식기반 전자서명법 하위고시 개정 [2014] - 지문인증을 이용한 삼성페이 서비스 개발 [2015] - 미래창조과학부고시 제2013-51호, 정보보호시스템 공통평가기준 [2013] - IT보안인증사무국은 국가용 보호프로파일 및 보조문서를 개발하여 공개 - 의료법 시행규칙 제16조 개정(2016.2.5)으로 전자의무기록의 의료기관 내부 또는 외부보관이 가능해지고 보관장소(의료기관 내부 또는 외부)별 시설과 장비에 관한 구체적인 세부기준을 마련함에 따라 관련 기술의 확산 예상 - 제조업의 창조경제 구현을 목표로 4대 추진방향, 13대 세부 추진과제를 중심으로 제조업 혁신 3.0 전략을 수립하여 시행 중 - 산업통상자원부와 스마트공장추진단 주관 하에 스마트공장 보급확산 사업을 펼치고 있으며, 2017년 현재 2,800여개 중소기업에 스마트공장 기술 접목 - 2022년까지 스마트공장 2만개 확산을 통해 중소·중견기업 공장(20인 이상)의 약 1/3을 IT기반 생산관리 이상 수준으로 스마트화
미국	<ul style="list-style-type: none"> - NIST, 경량 환경 전용 암호 표준의 필요성을 확인하고 주요 암호 알고리즘 (인증 암호화, 해시 함수)의 표준화를 위한 공모 사업 추진 [2018] - NIST, 미국 연방정부 사용 공개키 암호를 양자 내성을 가지는 알고리즘으로 대체하기 위한 양자 내성 암호(Post-Quantum Cryptography) 선정 중 [2017.11] - NIST, 디지털 아이덴티티 가이드라인 800-63-3 공개. 3가지 정책권고 사항으로 구성되며 높은 보장성을 갖는 AAL3 레벨이상의 인증방법 사용 권고 (즉 공개키 암호화 방식사용, 개인정보를 디바이스에 저장, 바이오인식과 같은 새로운 인증사용 권고) [2017.6] - 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 - NIAP, SSL/TLS 인스펙션 프록시 모듈의 보호프로파일 V1.0, 소프트웨어 파일 암호화 V2.0 보호프로파일, 주변기기공유장치(PSD) 보호프로파일V4.0 개발 중 - NIAP, 2016부터 응용 소프트웨어, 인증, 암호화 저장, IDS/IPS, 모바일, 네트워크 디바이스, 네트워크 암호화, 운영시스템, 원격접속, VPN, 가상화, Vo IP, 무선랜 부문의 보호프로파일을 개발하여 공개 [2017] - 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 [2016.3] - NIST, 비식별 처리 관련 가이드라인 “De-Identification of Personal Information” 발표 [2015.12] - NIST, 산업제어시스템 정보보호 지침(Guide to Industrial Control Systems(ICS) Security, NIST SP 800-82 Rev.2) 개정 2판을 발행 [2015.5] - ‘국가정보국(Office of the Director of National Intelligence, ONDI)’ 내에 ‘사이버 위협정보 통합센터(Cyber Threat Intelligence Integration Center, CTIIC)’를 설립을 통해 범정부 차원의 효과적인 사이버위협 대응 [2015] - 사이버 보안 정보공유법(Cybersecurity Information Sharing Act, CISA S.754)’ 제정 [2015]

구분	주요 현황
	<ul style="list-style-type: none"> - NIST, 서버 컴퓨터의 BIOS 보안 표준(BIOS Protection Guidelines, NIST SP 800-147B)을 발행 [2011.8] - NIST, 데스크톱/노트북용 BIOS 보안 표준(BIOS Protection Guidelines, NIST SP 800-147)을 발행 [2011.4] - 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 - NIST, 의료기관에서 무선 약물주입펌프에 대한 보안지침 발표 - NIST, NCCoE은 직원의 모바일 장치에 저장된 기밀정보를 유지할 수 있는 가이드라인을 발표 - FDA, ONC, FCC는 ONC 협조를 통해 각종 행위와 민간 영역의 역량에 기반한 위험 관리 기반의 IT 규제 프레임워크를 만들 것을 제안 - 스마트공장의 안전 및 보안을 위하여, 산업 제어 시스템 사이버 대응팀(ICS-CERT: Industrial Control Systems Cyber Emergency Response Team)을 독자적으로 운영 - 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	<ul style="list-style-type: none"> - 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 - 바이오인식 위변조 탐지기술 개발 및 PAD 시험인증 법제화 추진 중 [2016] - ‘사이버보안 기본법’ 제정으로 사이버보안 정책 수립 [2014] 및 기본법을 기반으로 ‘사이버보안 전략 2015’ 발표 [2015] - 기존 신성장전략, 일본재생전략에 이은 세 번째 성장전략의 구체적인 정책으로서 「일본재흥전략(日本再興戰略 JAPAN is BACK)」을 수립하여 발표 [2013]
유럽	<ul style="list-style-type: none"> - EU 역내 국민의 개인정보보호를 위한 기본법인 GDPR 발효 [2018.5] - EU에서는 GDPR에 앞서 2018년 1월부터 유럽은행연합의 PSD2(Payment Services Directive2)가 시행됨. PSD2는 고객이 동의한 경우, 은행권은 타 산업군에 오픈API 형태로 금융 데이터를 제공해야 하는 것으로 유럽금융권에서의 FIDO 솔루션의 적용확대에 긍정적 영향을 주고 있음 [2018.1] - EU, Horizon 2020 R&D 프로그램을 통해 ICT 핵심기술 확보를 위한 다수의 차세대 암호기술 개발 프로젝트 출범 [2014] - 영국은 비식별화 사례를 구현하기 위해 민간조직 UKAN을 설립하고 “익명화 프레임워크” 가이드라인 발표 [2016] - 바이오인식 위변조 탐지기술 개발 및 PAD 시험인증 법제화 추진 중 [2016] - EU의 유럽 연합 대응기구인 ENISA에서 빅데이터 프라이버시 보호 가이드라인 발표 [2015] - ‘주요 정보 기반 시설 보호(CIIP)’ 협력을 통해 사이버 보안에 관련된 14개의 법을 시행함으로써, EU 차원에서 각국의 ICT 인프라를 보호하기 위한 대책 및 회복 역량을 확보하는 등 보안 수준을 강화
중국	<ul style="list-style-type: none"> - 2025년까지 제조 강국에 진입하는 것을 목표로 하는 ‘중국제조 2025’를 발표 [2015.5] - 향후 30년간 3단계로 나누어 산업구조 고도화 계획

2.3. 기술개발 현황 및 전망

암호기술	국내	<input type="checkbox"/> 기초연구 → <input type="checkbox"/> 실험 → <input type="checkbox"/> 시작품 → <input checked="" type="checkbox"/> 제품화 → <input type="checkbox"/> 사업화	국내외 격차	90% (선도국 가대비)
	국외	<input type="checkbox"/> 기초연구 → <input type="checkbox"/> 실험 → <input type="checkbox"/> 시작품 → <input type="checkbox"/> 제품화 → <input checked="" type="checkbox"/> 사업화		
인증기술	국내	<input type="checkbox"/> 기초연구 → <input type="checkbox"/> 실험 → <input type="checkbox"/> 시작품 → <input checked="" type="checkbox"/> 제품화 → <input type="checkbox"/> 사업화	국내외 격차	95% (선도국 가대비)
	국외	<input type="checkbox"/> 기초연구 → <input type="checkbox"/> 실험 → <input type="checkbox"/> 시작품 → <input type="checkbox"/> 제품화 → <input checked="" type="checkbox"/> 사업화		
사이버보안	국내	<input type="checkbox"/> 기초연구 → <input type="checkbox"/> 실험 → <input checked="" type="checkbox"/> 시작품 → <input type="checkbox"/> 제품화 → <input type="checkbox"/> 사업화	국내외 격차	95% (선도국 가대비)
	국외	<input type="checkbox"/> 기초연구 → <input type="checkbox"/> 실험 → <input type="checkbox"/> 시작품 → <input checked="" type="checkbox"/> 제품화 → <input type="checkbox"/> 사업화		
보안관리/ 보안평가	국내	<input type="checkbox"/> 기초연구 → <input type="checkbox"/> 실험 → <input checked="" type="checkbox"/> 시작품 → <input type="checkbox"/> 제품화 → <input type="checkbox"/> 사업화	국내외 격차	90% (선도국 가대비)
	국외	<input type="checkbox"/> 기초연구 → <input type="checkbox"/> 실험 → <input type="checkbox"/> 시작품 → <input checked="" type="checkbox"/> 제품화 → <input type="checkbox"/> 사업화		
융합보안	국내	<input type="checkbox"/> 기초연구 → <input type="checkbox"/> 실험 → <input type="checkbox"/> 시작품 → <input checked="" type="checkbox"/> 제품화 → <input type="checkbox"/> 사업화	국내외 격차	75% (선도국 가대비)
	국외	<input type="checkbox"/> 기초연구 → <input type="checkbox"/> 실험 → <input type="checkbox"/> 시작품 → <input type="checkbox"/> 제품화 → <input checked="" type="checkbox"/> 사업화		

2.3.1. 국내 기술개발 현황 및 전망

- (암호기술) 국가보안기술연구소(NSR)와 ETRI를 중심으로 경량, 고속 암호기술, DBMS 적합형 암호기술 등 주요 차세대 암호기술 개발
 - (NSR) 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
 - (ETRI) 형태보존/순서보존/검색가능 암호 등 다수의 DBMS 환경용 암호기술 개발
 - (서울대) 동형 암호 알고리즘을 개발하고 다양한 응용서비스 적용을 위한 관련 기술을 개발 중
 - (KISA, NIMS, 서울대, 고려대, 서강대) 양자 내성 암호 알고리즘을 개발하여 NIST 공모사업 제안
 - (삼성SDS) 서버/클라이언트 모델에서 보안 세션 수립을 위한 키 교환 프로토콜 개발
- (인증기술) ETRI와 KISA를 중심으로 차세대 인증기술 연구가 수행되고 있으며, 삼성/LG와 같은 민간분야는 스마트 디바이스를 위한 생체 인증기술을 상용화 수준으로 개발 중
 - (삼성, LG전자, 유파인스) 스마트폰에 지문·얼굴·홍채·음성인식기술을 탑재한 모바일 바이오인식기술의 대중화와 함께 스마트폰의 터치스크린에 지문인식센서 탑재 등 박막형 지문인식센서를 개발 중에 있으며, 생체신호를 측정 및 생체신호기반 텔레바이오인식 기술개발에 박차를 가하고 있는 추세
 - (한국인터넷진흥원, 한국도로공사) 자율협력주행(C-ITS) 보안인증관리체계 구축 및 운영 방안 연구를 통한 최상위인증기관, 차량용 인증서 발급기관 등 기관별 역할 정의를 통한 C-ITS 보안인증관리체계 시범구축사업 추진방안 마련
 - (KISA) 2016년 7월부터 KISA 주관하에 글로벌 프로젝트를 착수하여, 스페인 마드리드대학교와 미국의 Telebiometrics 민간기업 연구소와 국제공동연구를 통하여 심전도·지문 등 다중 생체신호 인증메커니즘, 생체신호센서용 스마트밴드, 생체신호정보

통신메커니즘 등으로 구성되는 다중 생체신호 인증플랫폼을 개발중으로 한국·미국·중국지역의 관련기술 특허를 출원

- (KISA, 한국바이오인식협회) 모바일 바이오인식제품의 성능시험기술, 바이오인식 제시형 공격 탐지기술 개발 중
- (ETRI) 사용자 행위, 환경 정보 인지 및 무자각 멀티팩터 인증을 통해 보안성과 편의성을 강화하고, 모바일 앱의 동적 보안정책을 지원하는 상황인지 기반 범용인증플랫폼 기술 개발
- (삼성전자, BCCard, 라온시큐어, ETRI 등) 2018년 1월부터 FIDO Alliance산하의 한국워킹그룹 출범. 국내 FIDO솔루션의 글로벌 표준화를 위한 방안협의 및 프로세스 확립 추진 중

○ (사이버 보안) 보안정보 및 자산정보의 수집, 공유를 기반으로 동적 방어 및 보안 기술에 대한 연구개발이 진행 중

- (ETRI)
 - 2017년부터 선제적 방어를 수행하기 위한 “능동형 사전보안을 위한 사이버 자가변이 기술 개발” 사업 수행
 - 2017년부터 사이버위협 탐지·대응을 위한 Security Analytics 기반의 사이버위협정보를 분석·공유하는 “Security Analytics 기반의 이기종 보안솔루션 위협 분석 및 대응 기술 개발” 사업에 참여
- (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) 광주과학기술원(GIST)은 미국 육군 연구소와 협력하여 AI 기반의 MTD 소프트웨어 공동 개발추진

○ (보안관리/보안평가) 보안관리는 KISA, 보안제품 평가는 NSR IT 보안인증사무국에서 관리하고 있으며 관련 심사/평가 기술을 개발 중

- (KISA) 2018년 기존 IaaS 중심의 클라우드 보안 평가를 SaaS로 확대 시행
- (NSR IT보안인증사무국) 정보보호제품의 평가에 CCRA에서 제정한 CC, CEM 적용하며, 한국인터넷진흥원(KISA), 한국정보통신기술협회(TTA), 한국시스템보증(KOSYAS), 한국아이티평가원(KSEL), 한국정보보안기술원(KOIST), 한국기계전기전자시험연구원(KTC) 에서 평가를 수행하고 IT보안인증사무국에서 인증서를 발행 중
- (TTA) FIDO Alliance의 공인보안시험소 및 공인바이오인식 시험소로 지정되어 Authenticator의 보안성 평가, Biometric 평가를 통한 인증수행을 준비 중

○ (융합보안) 최첨단 선도 기술, 국제 표준, 다양한 서비스 개발, 정부·공공·민간 분야의 다양한 협업 체계 등 첨단 융·복합 기술에 대한 선점 경쟁이 치열함

- (ETRI) 정보보호본부에서 제조보안 분야와 의료기기, 의료생체 보안 분야를 중점적으로 R&D 및 표준화 활동을 수행하면서 경량암호알고리즘, 생체인식보안 기술 등을 개발하여 민간에 기술이전 하고 있으며, 산학연을 아우르는 위험도전형 기술개발 과제를 기획 중
- (NSR) 제어시스템 보안 인증 기준과 관련한 기술들을 개발 하여 제공하고 있음. 보건산업진흥원에서 진료정보교류시스템 기능성, 상호운영성, 보안성 인증 기술 및 기준을 개발하여 적용할 예정

- (NNSP) 제어시스템 보안성을 위한 단방향 통신장비를 개발하여 전력 분야에 운용하고 있고, 해외 유수의 제어시스템 공급사들이 비표준 독자기술을 공급하면서 블랙박스화하여 제공하는 기기들을 대상으로 보안성을 확인할 수 있는 기술을 개발 중
- (㈜솔, ㈜H3시스템 등) 다목적 광센서 의료측정기기, 전자체온계 등을 개발하는 과정에서 사이버보안 인증 기준에 적합한 기기를 개발 중

<국내 주요 사업자 서비스 동향>

사업자	주요 현황
삼성전자, LG전자	- 2018년 3월, 스마트폰에 지문·얼굴·홍채·음성인식기술 동시에 탑재
K-뱅크	- 2017년 4월, 인터넷전문은행 국내최초로 비대면인증수단으로 바이오인식서비스 도입 추진 중
유파인스	- KISA와 공동으로 심전도·심박수 측정센서용 스마트밴드 시제품 제작
원스	- 국내 IPS 네트워크 보안 분야의 1위 업체로 자체 CERT 조직을 보유하고 있으며, 지속적인 위협정보를 수집/분석/대응 체계를 가짐 - 자사 및 타사의 보안제품을 통합 관리하는 제품(TMS-Plus) 보유
KT	- AI Speaker인 기가지니에 화자인식 기술 탑재 준비 중
BC카드	- 국내 최초 FIDO기반 안면인증 서비스 도입
비트컴퓨터	- EMR 의료정보시스템, PACS 의료영상처리시스템 등을 개발하여 공급 중
인성정보	- EMR 의료정보시스템 등을 개발하여 공급 중
삼성메디슨	- 초음파 의료기기 등을 개발하여 국내·외에 판매 중
인피니트	- CT, MRI 의료기기 등 전문 의료기기를 개발하여 국내·외 판매 중
광림	- 다양한 위 내시경, 수술용 내시경 등 장비 개발하여 판매 중
LS산전	- 스마트 제조 필수 설비 중 PLC 제품 약 33%의 국내 시장 점유율 확보
(주)ACS	- 현대기아자동차, 포스코 등 국내외 1,200여 업체에 제조 관련 솔루션을 시스템 통합 형태로 구축 - 자동차 부품 제조업 및 전기전자 부품 제조업 분야에 적합한 공통 패키지 기능을 ANSI S-95, IEC 62264와 미국 MESA(Manufacturing Enterprise Solution Associates) 모델에서 제시하는 표준 기능으로 개발
(주)유노믹	- 2011년부터 국내 공작기계 제조사와 함께 모바일 기반의 공작기계 제어 소프트웨어를 개발 - 2013년부터 북미 표준 제조 기술규격인 MTConnect 및 OPC UA를 중심으로 공작기계 모니터링 시스템을 개발 - 50여 가지 제조 공정 모니터링 및 제어를 위한 소프트웨어를 제공
(주)엔엔에스피	- 산업제어시스템 보안기술, 스마트 그리드 보안기술 등을 개발 - KC, GS, CC 인증 등을 획득한 하드웨어 기반의 물리적 단방향 보안 게이트웨이, 산업용 네트워크 포트 이중화 장비 등을 자체 개발하여 국내·외 판매
펜타시큐리티	- 펜타 스마트 팩토리 시큐리티(Penta Smart Factory Security) 솔루션을 적용, 스마트공장 운영 과정에서 발생할 수 있는 보안 위협을 최소화하는 제품 개발 - 데이터 수집부터 모니터링, 프로세스 제어까지 가능하도록 안전한 스마트 팩토리 환경을 구축하는 솔루션 개발 판매 중
안랩	- 다양한 융·복합 기기에서 사용 가능한 내장형 보안 솔루션 개발 판매 중

2.3.2. 국외 기술개발 현황 및 전망

- (암호기술) 미국과 유럽은 각각 국가 기관과 학계를 중심으로 차세대 암호 알고리즘의 개발 및 국제표준화를 통한 시장 주도권 선점을 추진 중
 - (미국 HPE Security) 형태보존 블록 암호 운영 모드 FFX 개발 및 미국 연방정부 사용 승인(NIST SP 800-38G)
 - (벨기에 COSIC) 경량 메시지 인증 코드 알고리즘 Chaskey와 LightMAC 개발
 - (독일 Ruhr-Univ. Bochum, 싱가포르 난양대, 덴마크 기술대, 일본 NTT) 경량 블록암호 SKINNY 개발
 - (싱가폴 난양대) 경량 블록 암호 Deoxys-BC와 이를 기반으로 한 인증 암호화 알고리즘 Deoxys 개발
 - (미국 IBM, Microsoft 등) 다수의 동형 암호 알고리즘을 개발하고 의료 분야 등 다양한 응용서비스 적용 기술을 개발 중
- (인증기술) 미국 유럽 등 주요 선진국의 주도 하에 연구소와 학계에서 생체신호 개인식별 등 원천 기술 연구가 진행되고 있으며, 금융권과 IT기업은 사용자의 보안을 위해 최신 인증 기술을 활발히 도입하고 있음
 - (미국 CAMP SCMS, 유럽 European Commission) 정부기관인 교통국(US DOT)의 주도로 뉴욕, 탬파, 와이오밍 3개의 주에서 V2X 통신을 이용한 안전서비스의 제공을 위해 CV Pilot을 구축 중이고 유럽연합 집행위원회(European Commission)의 주도로 PKI기반의 정책기관(Policy Authority), 신뢰리스트 관리기관(Trust List Manager), 최상위인증기관(Root CA), 등록CA, 익명CA로 이루어진 C-ITS 신뢰모델을 설계함
 - (NIST, UN 난민기구) 스마트카드와 연동기술인 바이오인식기반의 MoC(Match-On-Card) 카드형태의 미국 연방정부의 PIV 카드, 유엔 지문스마트카드·난민식별카드 등 상용제품을 널리 보급
 - (Apple, NTT 도코모 등 주요 스마트폰 개발업체) 지문·얼굴·정맥·음성인식기술을 탑재한 스마트폰을 출시함과 동시에 스마트폰의 터치스크린에 탑재하는 박막형 지문인식센서를 활발히 개발 중
 - (Amazon, Facebook, Line 등) 최근 1년간 Line, Amazon, Facebook이 FIDO Alliance 보드로 가입하면서 FIDO2등 FIDO표준 및 바이오인식기술을 적용한 솔루션이 2018년, 2019년 본격 출시될 것으로 보임
 - (NIST, 유럽 핀테크 금융업체) 미국·유럽 등 주요 선진국 금융권에서는 비대면 본인확인에 활용되는 바이오인식제품을 도입 시에 바이오인식 제시형 공격 탐지기술(PAD) 국제표준(ISO/IEC 30107) 적합성 시험인증기술을 활발히 개발중에 있으며 시험·인증서비스에 대한 법제도 정비를 서두르고 있는 추세
 - (Texas Instrument, 미국 위싱턴대학교) 뇌파·심전도·심박수·근전도 등 생체신호 측정용 의료장비 및 웨어러블 디바이스, 생체신호센서용 MoC IC칩 등 미국 TI(Texas Instrument)사를 중심으로 활발히 제품화가 진행 중에 있으며, 미국의 위싱턴 대학 등 대학교를 중심으로 뇌파·심전도·심박수 등 생체신호 개인식별 기술에 대한 연구가 활발히 진행 중

- (Halipax 은행, Bionym) 영국의 Halipax 은행, 캐나다 왕립은행 등 주요선진국 금융권에서는 시범사업으로 캐나다 Bionym에서 개발한 심박수 측정용 웨어러블 디바이스를 통하여 생체신호를 이용한 고객통장의 개인식별 서비스를 시행 중
 - (IBM) 멀티팩터 인증과 위험 관리 인가를 제공하기 위해 센서로부터 다양한 정보(바이오, 장치, 위치)를 수집하여 바이오 멀티팩터 인증 및 위험 평가 후 서비스 제공여부를 결정하는 아키텍처 개발
 - (Cisco) 사물인터넷 서비스 플랫폼인 시스코 제스퍼 컨트롤 센터에서 투-팩터 인증 서비스가 포함된 멀티 레이어 보안 제공
 - (Microsoft) 자사의 클라우드 서비스인 Azure 인증앱을 통해 삼성 기어 시리즈나 애플워치와 같은 웨어러블 기기와 연동되는 투팩터 인증 제공
 - (Amazon) 아마존 웹 서비스(AWS)에 멀티팩터 인증을 도입하여 사용자 이름과 암호, 디바이스 인증코드를 이용하여 암호 이외에 보안수준을 강화하는 수단 제공
- (사이버 보안) 기존 보안기술 분야에 동적 변이 기술 및 인공지능 기술의 접목을 통해 능동적이고 선제적인 보안을 제공하기 위한 연구 개발이 진행되고 있으며, 미국을 중심으로 서로 다른 기관간의 보안정보 공유를 통한 협력기반의 연동 프레임워크 기술에 대한 연구를 활발히 진행 중
- (DHS) 동적으로 보안조치를 수행해서 공격대상을 보호하는 Moving Target Defense는 미국 백악관이 2011년에 발표한 “사이버보안 연구개발 전략” 중 가장 주목받았던 연구 분야로서 현재 미국 국토안보부(Homeland Security)에서 연구를 수행 중
 - 미국 국토안보부 과학 기술국(DHS S&T)은 SVIP(Silicon Valley Innovation Program)를 통해 금융기관의 사이버 보안 기술 개발을 지원 중
 - NexiTech와 Veramine이 FSCSAD(Finance Service Cyber Security Active Defense)부문에 채택되어 스토리지 디바이스, 호스트 보호를 위한 MTD 핵심기술 개발을 진행 중
 - 미국 국토안보부는 MITRE 프로젝트에서 개발된 사이버 위협정보를 공유하는 자동화된 표준 운용기술 결과물을 오픈소스로 발표(Cybox, STIX, TAXII)
 - 2014년 글로벌 보안벤더 시만텍, 포티넷, 팔로알토네트웍스, 인텔시큐리티 등 참여하는 위협 인텔리전스 정보 공유 플랫폼 CTA(Cyber Threat Alliance : 사이버위협연합) 운영
 - 2016년 3월, 마이크로소프트(MS)가 미국내에 사이버보안센터 구축완료, 사이버위협 및 분석 정보를 정부와 공유하는 민관협력 창구로 활용할 계획
- (보안관리/보안평가) 보안관리의 경우 NIST 등을 중심으로 국가기관 및 신기술에 대한 보안지침을 개발하고 있으며 보안제품 평가의 경우 CC 개발 및 참가 기관을 중심으로 기술 및 기준을 개발 중
- (NIST) 위협관리를 위해 여러 시스템으로 복잡하게 구성된 외부 공급자에게 의존하는 시스템 및 구성요소의 중요도를 평가하기 위한 심각도 분석 프로세스 모델(Criticality analysis process model), 대외비 정보의 보안 요구사항 평가 및 비연방 시스템의 대외비 보호 지침 등 개발 및 제개정
 - (CCRA) IT제품의 공통 평가기준(CC)과 평가방법론(CEM)을 개발하고 추가적으로 평가에 필요한 기술들을 개발함. iTC 그룹을 유지하며 USB 이동 저장 장치, Full 디스크 암호화, 네트워크,

- 어플리케이션 소프트웨어, 보안 전용 컴포넌트, 생체인식 등의 공동보호프로파일(cPP)을 개발 중
 - (ISO/IEC JTC1 WG3) CCRA에서 개발한 CC와 CEM을 ISO/IEC 15408과 ISO/IEC 18045로 표준화하고, IT제품의 보안성 평가에 활용될 수 있는 표준으로 평가자 자격 요건과 구현된 암호모듈의 검증 기준들을 개발 중
 - (CCUF) 국제 CC사용자 포럼은 글로벌 IT기업들과 평가기관 전문가들로 구성되어 있으며, IT제품에 적용되는 보안기능 요구사항과 평가에 활용하는 보조문서(supporting document) 개발에 참여 중
- (융합보안-의료보안) '17년 9월 심장박동기에 대한 해킹 위협과 보안 취약성이 집중적으로 거론되면서 개인건강기기와 의료기기 등에 대한 사이버공격과 해커들에 의한 공격이 증가하고, 의료기관을 대상으로 한 랜섬웨어 공격 등이 활발해짐에 따라서, 유럽 주요 국가들과 특히 미국 FDA를 중심으로 의료정보시스템과 의료기기에 대한 보안 기술 개발과 대응책 마련에 집중 중
- (UL) 미국 연방정부, FDA와 협력하여 의료기기 중에서 심장박동기, 인슐린펌프 등 약물주입펌프 기기부터 우선적으로 국제표준 기반하에 보안성 인증 프로그램을 개발하여 작용할 예정
- (융합보안-제조보안) 독일에서 제조업 기반으로 플랫폼 인더스트리 4.0을 전개하면서 관련 기술 개발을 주도하고 있으며, 미국, 일본 등이 이에 맞서 주도권을 확보하고자 경쟁적으로 작업을 진행하고 있으나, 보안 분야에 대한 기술개발과 투자는 세계적인 다국적 기업을 제외하고 거의 활성화되지 못하고 있음
- (UL) 미국 연방정부와 협력하여 제어시스템에서 중점적으로 사용되는 PLC(Programmable Logic Controller) 기기부터 우선적으로 국제표준 기반하에 보안성 인증 프로그램을 개발하여 작용할 예정

<국외 주요 사업자 서비스 동향>

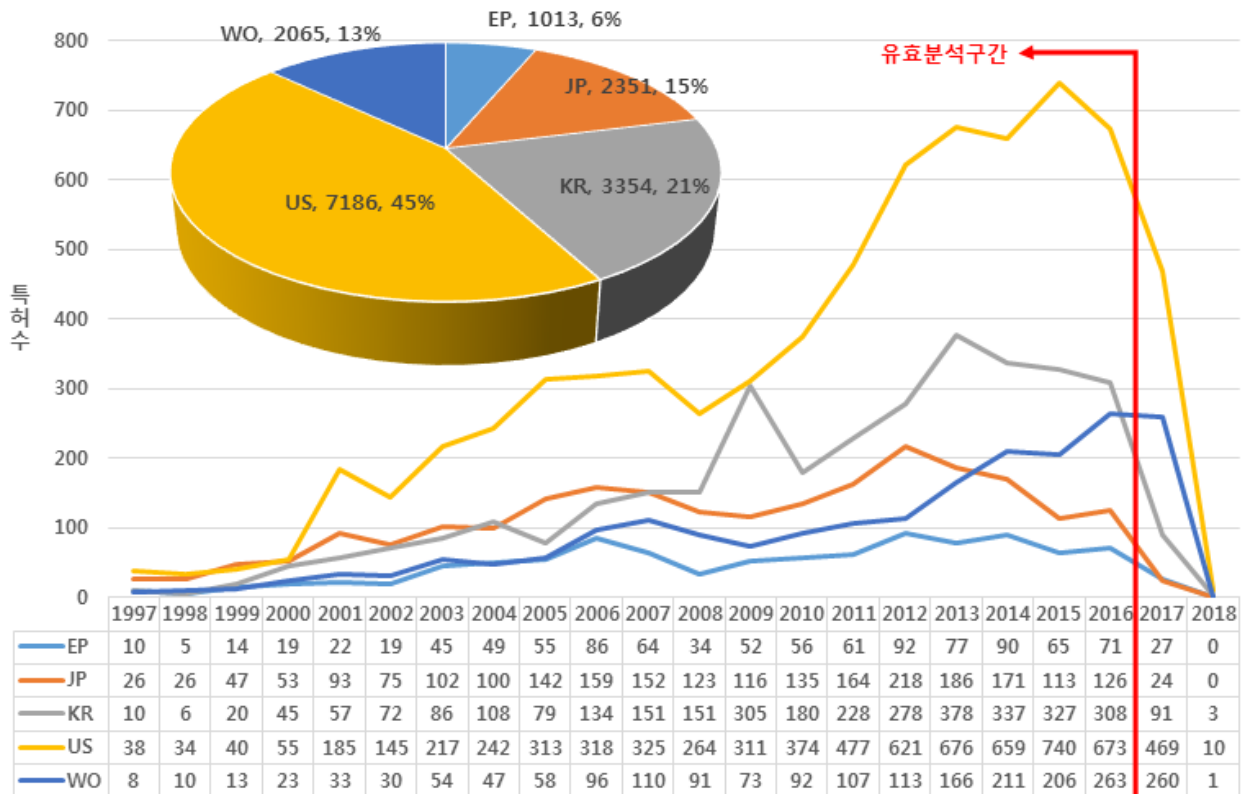
사업자	주요 현황
BSI, TUV 등	- 다양한 인증심사기관, 컨설팅 업체 등이 ISMS 컨설팅 및 인증심사 서비스를 제공 중
TI	- 2017년 12월, 심전도·심박수들 동시에 측정하는 생체신호 센서용 MoC 제품화
Halipax, Royal Bank	- 2016년, 심전도·심박수 등 생체신호 인증기술을 이용한 금융고객 신원확인서비스
Symantec	- 사이버 보안 분야를 선도하는 글로벌 기업이며, 엔드포인트, 클라우드, 인프라 전반을 정교한 공격으로부터 방어할 수 있는 전략적인 통합 솔루션 제품 개발 - 2014년부터 글로벌 보안업체들이 참여하는 위협 인텔리전스 정보 공유 플랫폼(CTA)에서 핵심 역할을 담당
Trend Micro	- 개인용 안티바이러스 백신에서부터 기업용 APT 대응 솔루션과 물리서버, 가상화서버, 클라우드 보안에 이르는 다양한 솔루션을 제공 - 보안위협을 분석하는 Deep Discovery, 가상화 보안 및 물리서버 보안을 제공하는 Deep Security와 클라우드 보안센터와의 연동을 통한 통합보안 솔루션을 개발
Facebook	- 2017년 1월부터 FIDO Alliance 보드멤버사로 활동 중인 Facebook은 전세계 20억 명이 넘는 사용자가 FIDO인증 솔루션을 지원하는 보안키를 사용해 로그인 할 수 있도록 지원 중

2.4. IPR 현황 및 전망

○ 특허분석 개요

- 차세대 보안 분야에 있어서, 2018년 5월 현재까지 한국, 미국, 일본, 유럽, 국제 공개(등록)된 특허들을 대상으로 앞서 제시된 표준화 항목에 따라 검색/추출된 총 15,969건의 특허를 대상으로 분석을 수행함

○ 특허 출원년도별 특허공보별 동향



* 특허 분석구간(1997년~2018년) : 출원일 기준으로 분석하며, 일반적으로 특허출원 후 18개월이 경과된 때에 출원 관련정보를 대중에게 공개하고 있음. 따라서 아직 미공개 상태의 데이터가 존재하는 2017년 이후 자료의 경우 미 공개분이 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 출원량이 늘어나고 있는 것으로 나타남
- 한국(KR)을 비롯하여 미국(US), 국제(WO) 특허 출원량이 최근에 많은 것으로 보아 차세대 보안 기술 분야에 대한 관심도가 높고 연구개발이 활발한 것으로 판단
- 국가공보별로는 미국(US) 특허가 7186건(45%)으로 가장 많은 출원량을 나타내고 있으며, 한국(KR)에 출원된 특허가 3354건(21%)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 예상

○ 각 표준화 항목에 대한 연도별 출원 동향

표준화 항목 출원 년도	FIDO	PKI 기반 인증	멀티 팩터 인증	바이오 인식	보안 관리 평가	보안 정보 공유	차세대 암호 기술	의료 보안	제조 보안
1997	0	15	16	0	2	0	23	25	11
1998	0	10	22	0	0	2	21	21	5
1999	0	24	29	5	2	12	32	26	4
2000	0	28	45	10	3	17	19	53	20
2001	2	55	68	13	8	19	56	152	17
2002	0	59	72	13	7	22	50	90	28
2003	1	69	127	21	11	29	80	134	32
2004	0	108	95	25	19	32	100	126	41
2005	0	106	129	32	7	28	135	149	61
2006	0	139	202	26	16	24	136	167	83
2007	0	165	222	42	16	31	111	156	59
2008	0	133	178	57	19	20	80	127	49
2009	0	107	325	94	10	26	112	138	45
2010	0	142	224	93	12	26	114	180	46
2011	1	174	325	129	20	29	101	214	44
2012	7	194	358	246	22	28	121	286	60
2013	29	178	409	265	39	29	119	340	75
2014	57	183	397	255	35	24	143	281	93
2015	121	180	324	225	37	30	159	257	118
2016	154	236	175	202	38	40	155	307	134
2017	116	134	48	213	19	15	44	193	89
2018	0	2	0	2	0	1	2	4	3
합계	488	2441	3790	1968	342	484	1913	3426	1117

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

○ 각 표준화 항목에 대한 특허공보별 출원 동향

표준화 항목 출원 국가	FIDO	PKI 기반 인증	멀티 팩터 인증	바이오 인식	보안 관리 평가	보안 정보 공유	차세대 암호 기술	의료 보안	제조 보안	합계
한국특허	81	519	1089	457	124	300	217	379	188	3354
미국특허	285	626	1448	1031	123	84	785	2273	531	7186
일본특허	35	831	230	236	45	71	429	418	56	2351
유럽특허	18	160	273	57	8	7	186	120	184	1013
국제특허	69	305	750	187	42	22	296	236	158	2065

- 멀티팩터인증기술에 대한 출원은 대부분 국가에서 많은 출원이 이루어지고 있으며, 미국의 경우 의료보안, 일본의 경우 PKI 기반 인증, 유럽은 제조보안, 한국은 PKI 기반인증 및 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	FIDO	PKI 기반 인증	멀티 팩터 인증	바이오 인식	보안 관리 평가	보안 정보 공유	차세대 암호 기술	의료 보안	제 조 보안	합계
비즈모델라인	0	15	179	40	0	0	0	1	0	235
ETRI	1	25	56	11	11	34	41	4	5	188
삼성전자	25	32	17	22	2	4	13	17	7	139
케이티	0	22	39	3	3	7	1	5	2	82
SK텔레콤	0	11	10	1	5	4	14	7	0	52
에이티 솔루션즈	0	2	30	0	0	0	0	5	0	37
QUALCOMM	0	20	3	7	0	0	3	2	2	37
고려대학교	0	13	6	1	0	1	9	1	0	31
엘지전자	0	13	1	12	0	2	0	1	1	30
SK플래닛	9	19	0	0	0	0	0	0	0	28

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

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

표준화 항목 출원인	FIDO	PKI 기반 인증	멀티 팩터 인증	바이오 인식	보안 관리 평가	보안 정보 공유	차세대 암호 기술	의료 보안	제 조 보안	합계
NEC	1	72	24	13	2	2	144	15	1	274
Rockwell Automation	0	2	1	0	0	0	0	1	254	258
MICROSOFT	12	30	87	27	3	6	36	14	0	215
IBM	1	21	92	14	3	0	41	39	1	212
삼성전자	32	43	39	20	0	1	20	34	3	192
TOSHIBA	2	46	7	7	2	3	57	60	0	184
NTT	8	85	14	9	1	1	53	7	0	178
QUALCOMM	9	70	22	43	0	1	9	7	7	168
FUJITSU	9	62	13	18	2	3	45	9	0	161
SIEMENS	2	10	9	2	0	1	3	63	70	160

- 해외특허 다수 출원인은 NEC, Rockwell Automation, Microsoft, IBM, 삼성전자, Toshiba 등의 순으로 나타남
- 주요 출원인들은 주로 통신, 전자제품, 소프트웨어 등에 관련된 기업이며, 특히 PKI 기반 인증 및 차세대암호기술에 집중하여 특허를 출원하는 것으로 나타남
- 삼성전자는 해외에도 활발한 특허출원을 하고 있으며, ETRI, LG전자, SK텔레콤, 삼성SDS, SK플래닛, 등과 같은 한국기업이 해외에도 출원 중

2.5. 표준화 현황 및 전망

암호기술	<input type="checkbox"/> 개념/정의, <input type="checkbox"/> 유즈케이스/요구사항, <input type="checkbox"/> 기능/참조구조, <input type="checkbox"/> 데이터포맷/스키마, <input checked="" type="checkbox"/> 프로토콜/인터페이스	표준 수준	100% (선도국가 대비)
인증기술	<input type="checkbox"/> 개념/정의, <input type="checkbox"/> 유즈케이스/요구사항, <input type="checkbox"/> 기능/참조구조, <input type="checkbox"/> 데이터포맷/스키마, <input checked="" type="checkbox"/> 프로토콜/인터페이스	표준 수준	95% (선도국가 대비)
사이버보안	<input type="checkbox"/> 개념/정의, <input type="checkbox"/> 유즈케이스/요구사항, <input checked="" type="checkbox"/> 기능/참조구조, <input type="checkbox"/> 데이터포맷/스키마, <input type="checkbox"/> 프로토콜/인터페이스	표준 수준	90% (선도국가 대비)
보안관리/ 보안평가	<input type="checkbox"/> 개념/정의, <input checked="" type="checkbox"/> 유즈케이스/요구사항, <input type="checkbox"/> 기능/참조구조, <input type="checkbox"/> 데이터포맷/스키마, <input type="checkbox"/> 프로토콜/인터페이스	표준 수준	95% (선도국가 대비)
융합보안	<input type="checkbox"/> 개념/정의, <input checked="" type="checkbox"/> 유즈케이스/요구사항, <input type="checkbox"/> 기능/참조구조, <input type="checkbox"/> 데이터포맷/스키마, <input type="checkbox"/> 프로토콜/인터페이스	표준 수준	70% (선도국가 대비)

구분	표준화 기구		표준화 현황
국제 (공적)	JTC1	SC27	<p>(WG1-Information security management systems) 정보보호통제 표준인 ISO/IEC 27002의 개정안 개발을 개시하였으며 정보보호통제 평가지침인 ISO/IEC 27008은 2차 개정판을 발행. 분야별 응용을 위한 요구사항 ISO/IEC 27009는 2017년 조기 개정을 개시하여 CD 단계로 진입, ISO/IEC 27006 ISMS 감사 및 인증기관 요구사항 개정을 위한 연구를 개시하는 등 관련 표준을 지속적으로 개발 및 재개정 중</p> <p>(WG2-Cryptography and security mechanisms) 경량 암호 알고리즘을 중심으로 ICT 정보보호를 위한 핵심 암호기술의 표준화 추진 중. 신규 기술 수요에 따른 경량 암호 분야의 표준화 항목 및 대상 증가 전망. 또한, 인증 요소 기술(영지식/blind 전자서명 기반 인증, 바이오메트릭 기반 인증, 속성 기반 익명 비연결 실체 인증) 및 객체 인증 보증 프레임워크 표준화 추진 중</p> <p>(WG3-Security evaluation, testing and specification) IT제품의 보안성 평가기준표준인 ISO/IEC 15408과 평가방법론 ISO/IEC 18045를 2020년 개정할 예정</p> <p>(WG5-Identity management and privacy technologies) 바이오인식기반 하드웨어 보안토큰(17922) 등을 개발완료하였으며, 바이오정보 보호기술(24745R1) 개정안을 개발 중. WG1과 공동으로 ISO/IEC 27552 개인정보 보호경영을 위한 27001 확대 요구사항 표준 개발 진행 중</p>
		SC37	<p>(WG2-Biometric technical interfaces) 객체지향형 바이오인식 호환규격 (30106-4), 객체지향형, 바이오인식 호환성 시험기술(30106-1AMD1) 개발 중</p> <p>(WG5-Biometric testing and reporting) 얼굴인식을 결합한 지능형 CCTV 성능시험기술 개발 중</p>
	ISO	TC215	<p>(WG4-Security, Safety and Privacy) 개인건강정보를 포함한 보건의료 빅데이터를 대상으로 개인정보보호를 위한 비식별화 표준 개정 완료. 의료분야 정보보호관리체계 관련, 전 산업에 공통적으로 적용하는 ISO 27001 ISMS(정보보호관리체계)를 기반으로 의료 분야에 대한 ISMS인 ISO 27799 개정 완료. 스마트의료기기 안전과 보안 인증을 통한 IoT 의료기기 안전성·보안성 확보 및 민감한 의료정보의 개인정보보호를 보장하기 위한 스마트 의료기기 보안인증기술 표준화 추진 중</p>

구분	표준화 기구		표준화 현황
	IEC	TC65	(WG10-Security for industrial process measurement and control) 미국 ISA 99 위원회와 협업으로 스마트 공장, 제조 등에 대한 보안 표준을 개발하고 있고, 최근 스마트공장 실현을 위한 요소기술 표준화에 주력하고 있으며, 최근 신기술에 기반한 표준 개정 작업 중
	ITU-T	SG17	<p>(Q.4) 사이버보안 침해증거 수집 및 보존 관련 사이버보안 침해사고 증거를 수집 및 보존하는 도구를 위한 가이드라인 표준 개발을 진행 중</p> <p>(Q.7) 경량 클라이언트-서버 모델에서 하이브리드 인증 및 키관리 메커니즘 표준화 추진 중</p> <p>(Q.9) 모바일기기를 위한 텔레바이오인식 보호지침(X.1087), 바이오인식기반 하드웨어 보안토론(X.1085) 등의 표준을 제정 완료하였으며, 스마트 ID카드를 이용한 원격 바이오 접근제어(X.tac) 등을 개발 중</p> <p>(Q.9) 생체신호를 이용한 텔레바이오인식 인증기술(X.tab)을 개발 중으로 추후 생체신호 인증기반 헬스케어 보안기술 표준화를 ISO TC215와 공동으로 추진할 예정</p> <p>(Q.10) 객체 인증 보증 프레임워크와 접근하는 자원별로 상이한 인증 수준을 적용하기 위한 스텝업 인증 프로토콜 표준화 추진 중</p>
	IETF	SEC	(Security Area) 인터넷 환경에서 원활한 정보보호 서비스를 제공할 수 있는 다양한 암호 프로토콜 및 이를 뒷받침하기 위한 핵심 암호기술과 적용 가이드라인에 대한 표준화 추진 중
국제 (사실)	FIDO		<ul style="list-style-type: none"> - 온라인과 오프라인상 FIDO솔루션의 확산을 위해 W3C, EMVCo, GSMA등과 협업함과 동시에 FIDO 2.0(모바일+웹, PC운영체제)로의 업그레이드 및 이와 관련된 표준화 완료단계 - 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 - IoT 및 블록체인의 연계 필요성 및 방안에 대한 논의가 진행 중
	CCRA		- 공통평가기준(CC)와 평가방법론(CEM) 개정, CCRA내 국제기술커뮤니티(ITC)를 통해 cPP와 cPP SD문서 지속 개발 진행 중
	ISA-99		- 제조 분야 전반에 대한 보안 기술 표준화 진행 중
지역 표준화 협의체	CJK IT Standard Meeting		<ul style="list-style-type: none"> - CJK IT Standard Meeting 안에 정보보호 작업반(WG)에서 한중일 전문가들의 의견 공유 및 지역 표준화 개발 - 블록체인의 국제표준화 활동을 위해 한중일 3국 간 협력을 제안하였으며, 정보보호 작업반(WG) 산하에 블록체인 임시그룹(Adhoc Group)을 신설(2017.8)하기로 결정

구분	표준화 기구		표준화 현황
국내	TTA	PG501	(정보보호기반) 주요 차세대 암호기술의 표준화 완료 및 양자 키 분배 시스템 규격 표준화 추진 중이며 패스워드와 IBC(ID 기반 암호시스템)를 이용한 키 교환 프로토콜 표준 제정
		PG502	(개인정보보호/ID관리, 블록체인 보안) 개체 인증에 대한 보증 프레임워크, 금융 서비스에 신뢰 등급이 가능한 인증 등급, FIDO 유니버설 이증인증(U2F) 규격 표준 제정중이며 개인정보 영향평가 보고서 작성을 위한 지침, 개인 정보 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 역할기반 접근제어 생성언어 등을 개발 중
		PG503	(사이버보안) STIX 기술 관련, 구조화된 위협 정보 표현 규격(STIX 2.0)에 대한 시리즈 표준을 개발 중
		PG504	(응용보안/평가인증) 응용 보안 평가 인증 부문 정보통신단체 표준 제·개정, 정보보안 평가 및 검증 기술실무반(WG5041)을 신설하여 해당 분야 국내 표준 개발하기로 결정(2018.5)
		PG505	(바이오인식) 바이오인식 응용서비스 관련, 일회용 ID기반 바이오 인증기술, 모바일 바이오인식제품 위조샘플 탐지를 위한 시험평가지침, 바이오인식과 IC카드를 이용한 접근제어용 개인확인시스템 등을 개발 중이며 생체신호기반 텔레바이오인식기술 관련, 생체신호 인증알고리즘 성능시험기준, 생체 신호정보 프라이버시 보호지침, 개인인증용 생체신호 데이터포맷 등을 개발 완료 하였으며, 생체신호를 이용한 헬스케어 응용서비스 기술보고서를 개발 중
	RRA		(SC27-K) - 한국/미국/일본 공동으로 ISO/IEC 19790, ISO/IEC 24759 표준을 2018년 개정 후, KS X 표준 2019년 개정 예정 - ISO/IEC15408, ISO/IEC18045 관련 한국암호모듈검증제도의 암호모듈 보안 요구사항과 시험 요구사항 제·개정 - 해시 함수 LSH, 블록암호 운영모드 KS X 표준화 추진 (SC37-K) 바이오인식 응용서비스 관련, 바이오인식 정보의 보호를 위한 기술적 관리적 지침(KSX1966), 바이오인식 제시형 공격 탐지기술(KSXISO/IEC 30107-1), BioAPI 적합성 시험기술 개정(KSXISO/IEC24709-1R1) 등 KS 국가표준을 제·개정
	스마트의료보안포럼		- 개인정보의 비식별화 모바일 디바이스에서 전자기록의 보안- 위험 평가 및 결과, 의료기관내 무선 의료기기 활용서비스의 보안참조 모델 등의 표준 개발 중
	개인정보보호포럼		- 개인정보보안 기술 관련 국내/국제 표준 개발 및 제·개정 - 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 및 FIDO 신규보안평가 시스템의 국내 공유 중 - 국내표준을 FIDO의 글로벌 표준에 반영 중

2.5.1. 국내 표준화 현황 및 전망

- (암호기술) TTA를 중심으로 신규 ICT 정보보호를 위한 핵심 암호기술 규격의 표준화를 완료하였고, 현재 양자 키 분배 시스템 표준화를 시작. 양자 키 분배 시스템 표준화는 시스템 구축 및 실증과 연계되어 본격적으로 진행될 것으로 전망
 - (TTA 정보보호기반 PG(PG501)) KCMVP 참조 규격으로 활용되는 표준에 대한 정비 작업을 진행하고 있으며, 양자 암호 시스템 규격에 대한 표준화 시작
 - (RRA, JTC1 SC27-Korea) 신규 ICT 정보보호를 위한 경량 블록 암호 LEA의 표준화에 이어, 고속 해시 함수 LSH의 표준화 진행 중

<국내 표준화 현황>

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
TTA PG501	2017-855, BB84 양자 키 분배 프로토콜을 적용한 장비 간 연동	2018	암호 알고리즘
	TTAK.KO-12.0271, n비트 블록암호 운영모드	2016	
	TTAK.KO-12.0189/R1, 결정론적 난수발생기 - 제1부- 블록암호 기반 난수발생기	2015	
	TTAK.KO-12.0272, 블록암호 기반 키 유도 함수	2015	
	TTAK.KO-12.0275, 형태 보존 암호 FEA	2015	
	TTAK.KO-12.0276, 해시 함수 LSH	2015	
RRA	해시 함수 LSH	진행 중 (2018)	암호 알고리즘
	KS X 3246, 128 비트 블록 암호 LEA	2016	
	KS X 3254, n비트 블록 암호 운영 모드 - 제1부 일반	2016	

- (인증기술) 국내 표준은 TTA를 중심으로 멀티팩터 인증, FIDO인증, 바이오인식 표준이 개발 또는 준용되어 왔으며, RRA에서 바이오 인식 기술의 국가표준을 개발 중
 - (TTA 정보보호기반 PG(PG501)) 패스워드와 ID 기반 암호시스템을 이용한 암호 및 서명으로 멀티팩터 인증을 제공
 - (TTA 개인정보보호/ID관리, 블록체인 보안 PG(PG502)) 개체 인증에 대한 보증 레벨, 신뢰 등급이 가능한 인증 등급을 통해 멀티팩터 인증의 강도를 분류함. 또한 FIDO 표준의 유니버설 이증인증(U2F)에 대한 표준화를 완료
 - (TTA 바이오인식 PG(PG505)) KISA, 인하대, 충북대, 경인여대 등 국내 전문가그룹이 모바일 바이오인식제품 위조샘플 탐지를 위한 시험기술, IC카드기반의 MoC 바이오인식 융합기술, 생체신호기반의 텔레바이오인식 기술에 대한 단체표준을 활발히 개발 중
 - (RRA JTC1 SC37-Korea) 전문위원회를 중심으로 바이오인식 표준적합성 시험규격 개정안을 완료하였으며, 바이오정보 보호기술, 바이오인식 위변조 탐지기술 등에 대한 국가표준을 개발 중
 - (RRA ITU-T SG17-Korea) KISA, 충북대, 서울대, 유파인스 등 전문위원회를 중심으로 텔레바이오인식 응용기술, 생체신호기반 텔레바이오인식기술 등에 대한 국가표준을 개발 중
 - (사물인터넷융합포럼)자동차관련 이터넷 네트워크 보안 요구사항, 클라우드 커넥티드 자동차 보안 요구사항 등에 대한 표준화 진행 중(2017)

- (FIDO한국워킹그룹) 2018년 1월부터 FIDO한국워킹그룹 및 한국FIDO산업포럼 회원사 중심으로 FIDO솔루션관련 국내표준화 추진하고 이를 글로벌표준화로 연계 추진 중

<국내 표준화 현황>

개발기구		표준(안)명	개발연도	관련 중점 표준화 항목
사물인터넷 융합포럼		자동차용 이더넷 네트워크 보안 요구사항(안)	2017	PKI기반 기기인증
		클라우드 커넥티드 자동차 보안 요구사항(안)	2017	
TTA PG501		TTAK.KO-12.0270-Part1, 패스워드와 IBC(ID 기반 암호시스템)를 이용한 키 교환 프로토콜 - 제1부 ID 기반 암호 이용	2015	멀티팩터 인증 기술
		TTAK.KO-12.0270-Part2, 패스워드와 IBC(ID 기반 암호시스템)를 이용한 키 교환 프로토콜 - 제2부 ID 기반 서명 이용	2015	
		TTAK.KO-12.0221, 모바일 기기를 이용한 다중 요소 인증 메커니즘	2013	
TTA PG502		TTAK.KO-12.0313, 금융 서비스에 신뢰 등급이 가능한 인증 등급	2017	멀티팩터 인증 기술
		TTAE.OT-12.0018, FIDO 유니버설 이중인증(U2F)	2016	멀티팩터 인증 기술, FIDO 및 응용기술
		TTAI.IT-Xeaa, 개체 인증에 대한 보증 프레임워크	2010	멀티팩터 인증 기술
TTA PG505		2017-415, 일회용 ID기반 바이오인증기술	진행 중 (2018)	바이오인식 응용서비스
		2017-050, 모바일 바이오인식 제품의 위조샘플 탐지를 위한 시험 평가 지침	진행 중 (2018)	
		2017-049, 바이오인식과 IC 카드를 이용한 접근제어용 개인확인시스템	진행 중 (2018)	
		TTAE.IT-X.1085, 바이오인식 보안토큰을 이용한 원격 바이오인증 프레임워크	2017	
		TTAE.IT-X.1087, 모바일 디바이스에서의 텔레바이오인식 보안지침	2017	
		TTAK.KO-12.0322, 바이오인식 응용카드 기반의 개인 인증 시스템	2017	
		TTAK.KO-12.0324, 개인인증용 생체신호 정보보호 지침	2017	생체신호기반 텔레바이오인증 기술
		TTAK.KO-12.0325, 생체신호 인증 알고리즘 성능 시험 지침		
		TTAK.KO-12.0323, 개인인증용 심전도 및 광용적맥파 특징점 데이터 교환 포맷		
RRA	SC37-K	KSXISO/IEC30107-2, 생체인식 제시형 공격 탐지기술 -파트2: 데이터포맷	진행 중 (2019)	바이오인식 응용서비스
		KSXISO/IEC30107-3, 생체인식 제시형 공격 탐지기술 -파트3: 성능시험방법	진행 중 (2019)	
		KSXISO/IEC19794-15, 손금인식 데이터 교환규격-파트15	진행 중 (2019)	
		KSX1966, 바이오정보 보호를 위한 기술적·관리적 지침	2018	
		KSXISO/IEC24709-1R1, BioAPI를 위한 적합성 시험 방법-파트1: 시험방법 및 절차	2018	
		KSXISO/IEC30107-1, 생체인식 제시형 공격 탐지기술 -파트1: 프레임워크	2018	
	ITU-T SG17-K	KSXITUTX.1085, 바이오인식 보안토큰을 이용한 원격 바이오인증 프레임워크	진행 중 (2019)	바이오인식 응용서비스
		KSXITUTX.1087, 모바일 디바이스에서의 텔레바이오인식 보안지침	진행 중 (2019)	

- (사이버 보안) 국내 표준은 TTA, ETRI, KISA를 중심으로 개발되어 왔으며, 사이버보안 정보공유 프레임워크와 정보공유 프로토콜은 ITU-T와 IETF 등 국제표준화 기구에서 제정한 표준을 국내 상황에 맞게 준용 중
 - (TTA 응용보안/평가인증 PG(PG504)) 공격 노출점 평가에 필요한 자산 상태정보를 정의하고, 수집된 자산 상태정보를 통합 연계할 수 있는 교환 포맷을 규격화하기 위한 표준이 2017년 8월에 제안. 상태정보 정의 및 교환 포맷의 스키마를 명시한 표준문서가 2018년도에 제정
 - (TTA 사이버보안 PG(PG503)) 침해사고 정보 전달 포맷 및 프로토콜에 대한 표준이 제정되었으며, 사이버 위협정보 공유 관련하여 STIX 2.0 표준과 유스케이스에 대한 표준이 개발 중

<국내 표준화 현황>

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
TTA PG503	TTAE.IT-X.1544, 사이버 공격 패턴 목록 및 분류	2017	능동형 사이버보안 침해정보 수집 및 보존 기술
	TTAI.OT-12.0020-part1, 구조화된 위협 정보 표현 규격(STIX) 제1부: 개요	2016	
	TTAI.OT-12.0020-part2, 구조화된 위협 정보 표현 규격(STIX) 제2부: 공통	2016	
	TTAI.OT-12.0020-part3, 구조화된 위협 정보 표현 규격(STIX) 제3부: 코어	2016	
	TTAE.IT-X.1546, 악성코드 속성 목록 및 특성	2016	
	TTAK.KO-12.0279, 보안 정보 메시지 교환 프로토콜	2015	
	TTAE.IF-RFC4766, 침입 탐지 메시지 교환 요구사항	2015	
	TTAK.KO-12.0282, 침입탐지시스템을 위한 보안 정책 메시지 및 배포 프로토콜	2015	
	TTAK.KO-12.0283, Snort 기반 침입탐지시스템 탐지 규칙 요구사항	2015	

- (보안관리/보안평가) 국내 자체 개발 표준 및 국제 표준의 부합화를 통해 국내 요구와 국제 동향을 지속적으로 반영
 - (PG 504) 정보보호역량 성숙도 모델 표준화 등 관련 표준의 제개정 및 폐지를 통해 정보보호관리체계 관련 표준의 지속적 관리 중
 - (국가기술표준원) 27003 정보보호관리시스템 구현 지침 개정 등 ISO/IEC 27001 관련 표준 시리즈의 지속적인 제개정을 통해 부합화 표준을 현행화하고 있음
 - 2009년 12월 공통평가기준 국제표준을 준용하는 국내 표준 KS X ISO/IEC 15408-1, 15408-2, 15408-3을 개정하였으며, 2010년 12월 공통평가방법론 국제표준을 준용하는 국내 표준 KS X ISO/IEC 18045를 개정
 - (NSR IT보안인증사무국) CCRA에서 제정한 CC 및 CEM을 홈페이지에 게시하고 있으며, 제품 유형별 보호프로파일을 개발하여 공개

<국내 표준화 현황>

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
TTA PG504	TTAK.KO-12.0316, 클라우드 컴퓨팅 환경에서 개인 정보보호 지침	2017	정보보호 관리 체계
	TTAK.KO-12.0293, 암호모듈현장시험지침	2016	IT제품 보안성 평가기준
	TTAK.KO-12.0284, 정보보호 역량 성숙도 모델 지침	2015	정보보호 관리 체계
국가기술 표준원	KS X ISO/IEC 27009, 정보기술-보안기술-ISO/IEC 27001의 분야별 적용 - 요구사항	2018	정보보호 관리 체계
	KS X ISO/IEC 27011, 정보기술-보안기술-ISO/IEC 27002에 기초한 통신조직을 위한 정보보호통제	2018	
	KS X ISO/IEC 27003, 정보기술-보안기술-정보보호 관리시스템 이행지침	2017	
IT보안인증 사무국	KECS-PP-0822-2017, 국가용 통합인증 보호프로파일	2017	IT제품 보안성 평가기준
	KECS-PP-0821-2017, 국가용 문서 암호화 보호프로파일	2017	
	KECS-PP-0820-2017, 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	
	KECS-PP-0714-2016, 국가용 네트워크 장비 보호프로파일	2016	
	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	

- (융합보안) 의료보안 분야는 PG505 바이오인식 그룹과 스마트의료보안포럼에서 최근 사회적 이슈가 되고 있는 의료기기 안전성 및 보안성을 위한 TTA 표준 문서들을 개발하고 있으며, 제조보안 분야는 국가보안기술연구소에서 산업제어시스템에 대한 보안요구사항 표준을 개발하였으나, 의료기관이나 제조업 현장에서 보안 표준 및 기술을 제한적으로만 적용 중
- (TTA 바이오인식PG(PG505)) 의료와 보안 양쪽을 아우르기 위한 작업으로 의료보안 표준 기술을 스마트의료보안포럼과 협업 하에 개발 중

- (국가기술표준원) ISO TC 215 보건의료 표준 위원회 중 WG4 안전, 보안과 개인정보보호 그룹에서 의료보안 표준 작업을 지속적으로 추진 중이고, 2018년 10월 부산 벡스코에서 개최될 IEC 국제표준 총회를 기점으로 제조보안 분과에 적극 참여 계획 중
- (스마트의료보안포럼) 의료보안 분야 정책, 기술, 기기, 표준 등을 수행하는 분과를 중심으로 국제표준화 작업 및 국내 기술 전파와 인식 강화를 위한 작업 진행 중
- (건국대학교) 의료보안과 제조보안을 기반으로 한 국제 표준 기술 개발과 관련 전문가 양성 및 인재 교육을 위한 융합보안대학원 설립 추진 중

<국내 표준화 현황>

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
TTA PG505, 스마트 의료보안포럼	2018-1735, 의료기관내 무선의료기기 활용서비스의 보안참조 모델	진행 중 (2018)	진료정보 교류시 보안표준 모델, 의료기기 안전 및 보안 프레임워크
	2018-1736, 모바일 디바이스에서 전자건강기록의 보안 Part V : 위험 평가 및 결과	진행 중 (2018)	
	2018-1737, 개인의료정보의 비식별화	진행 중 (2018)	
TTA PG504	TAK.KO-12.0307-part1, 산업제어시스템 보안요구사항 - 제1부: 개념 및 참조모델	2017	스마트공장 기기 상호 보안인증기술, 중소기업용 스마트공장 보안 관리 기술
	TAK.KO-12.0307-part2, 산업제어시스템 보안요구사항 - 제2부: 현장장치 계층	2017	
	TAK.KO-12.0307-part3, 산업제어시스템 보안요구사항 - 제3부: 제어 계층	2017	
	TAK.KO-12.0307-part4, 산업제어시스템 보안요구사항 - 제4부: 운영 계층	2017	

2.5.2. 국제 표준화 현황 및 전망

- (암호기술) ISO와 IETF는 경량 환경용 암호 알고리즘과 암호 프로토콜 규격의 표준화를 진행 중이고, ETSI는 양자 키 분배 시스템 규격 표준화를 활발히 진행 중임. 특히 경량 환경용 암호의 필요성이 증가함에 따라, ISO 경량 암호 분야(29192)의 표준화 항목 및 대상이 증가할 것으로 전망
- (JTC1 SC27) 경량 환경을 위한 암호 알고리즘 및 신규 암호기술 규격에 대한 표준화가 활발히 진행 중
 - 한국에서 개발한 블록 암호 LEA를 경량 블록 암호 표준(29192-2)에 추가하기 위한 작업 진행 중
 - 경량 메시지 인증 코드 표준(29192-6) 항목이 신설되었고, 벨기에 COSIC에서 개발한 Chasky와 LightMAC이 포함된 표준 개발 중
 - 경량 인증 프로토콜 표준(29192-7) 항목이 신설되었고, TESLA 프로토콜이 포함된 표준 개발 중

- 범용 암호화 알고리즘 표준에 동형 암호 표준(18033-6) 항목이 신설되었고, 표준화 작업이 진행 중
- 한국에서 개발한 서버/클라이언트 모델용 키 교환 프로토콜을 키 관리 방식 표준(11770-4)에 추가하기 위한 작업 진행 중
- 미국 연방정부용 신규 해시 함수 SHA-3를 전용 해시 함수 알고리즘 표준(10118-3)에 추가하기 위한 작업 진행 중
- 경량 블록 암호 SKINNY와 Deoxys-BC, 그리고 형태보존 암호의 표준화 적합성 검토 진행 중
- (IETF SEC, IRTF CFRG) 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
- 경량/소형 기기에서의 암호기술 활용을 위한 패스워드 기반 암호 알고리즘 다수 표준화
- 해시 함수 SHA-3의 암호 프로토콜 적용을 위한 표준화가 진행될 것으로 전망

<국제 표준화 현황>

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
JTC1 SC27	ISO/IEC 29192-6, Lightweight cryptography - Part 6(CD): Message authentication codes (MACs)	진행 중 (2020)	암호 알고리즘
	ISO/IEC 29192-7, Lightweight cryptography - Part 7(CD): Broadcast authentication protocol	진행 중 (2020)	
	ISO/IEC 29192-2, Lightweight cryptography - Amendment to Part 2 - LEA	진행 중 (2019)	
	ISO/IEC 18033-6, Encryption algorithms - Part 6(DIS): Homomorphic encryption	진행 중 (2019)	
	ISO/IEC 11770-4, Amendment 1 to Part 4	진행 중 (2019)	
	ISO/IEC 10118-3, Hash-functions - Part 3(FDIS): Dedicated hash-functions	2018	
	ISO/IEC 11770-4, Key management - Part 4(NP): Mechanisms based on weak secrets	2017	
	ISO/IEC 29192-4, Lightweight cryptography - Amendment 1 to Part 4	2016	
	ISO/IEC 29192-5, Lightweight cryptography - Part 5: Hash-functions	2016	
	ISO/IEC 29192-4, Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques	2013	
	ISO/IEC 29192-2, Lightweight cryptography - Part 2: Block ciphers	2012	
	ISO/IEC 29192-3, Lightweight cryptography - Part 3: Stream ciphers	2012	
IETF	RFC 8236, J-PAKE: Password-Authenticated Key Exchange by Juggling	2017	암호 알고리즘

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
	RFC 8235, Schnorr Non-interactive Zero-Knowledge Proof	2017	
	RFC 8133, The Security Evaluated Standardized Password-Authenticated Key Exchange(SESAPAKE) Protocol	2017	
	RFC 8032, Edwards-Curve Digital Signature Algorithm(EdDSA)	2017	
	RFC 7914, The script Password-Based Key Derivation Function	2016	
	RFC 7748, Elliptic Curves for Security	2016	

- (인증기술) ISO와 ITU-T를 중심으로 멀티팩터, 바이오인식 기술의 표준화가 활발히 진행되고 있으며, FIDO Alliance가 W3C를 통해 FIDO 기술의 표준화 추진 중
- (IEEE) 자율협력주행 차량을 위한 WAVE(Wireless Access for Vehicle Environment) 국제표준이 2013년 처음 만들어졌고 2016년에 추가 개정되어 사용 중이며 실증프로젝트의 결과를 반영하여 향후 추가 개정될 예정임
 - (미국) SCMS(Security Credential Management System) 시스템을 이용하여 현재 CV Pilot를 진행하고 있으며 홈페이지(<https://wiki.campllc.org/>)에 결과를 반영하여 문서를 수정 중
 - (European Commission) 유럽 지역에 자율협력주행(C-ITS) 구현 및 운영을 위한 인증서 정책 방안 가이드라인을 발표함(2017.7)
 - (JTC1 SC27)
 - 인증 요소 기술(영지식/blind 전자서명 기반 인증, 바이오메트릭 기반 인증, 속성 기반 익명 비연결 실체 인증) 및 객체 인증 보증 프레임워크 표준화 추진 중
 - ITU-T SG17과 공동으로 바이오인식기반 하드웨어 보안토큰(17922)을 개발 완료하였으며, 바이오정보보호기술(24745R1) 개정작업을 추진 중
 - (JTC1 SC37) C++기반 바이오인식 호환규격 적합성 시험기술 개정작업(24709-1R1)은 완료되었으며, C#·JAVA 등 객체지향형 바이오인식 호환규격 적합성 시험기술(30106-1AMD1, 30107-4)을 개발 중
 - (ITU-T SG17)
 - (Q.7) 경량 클라이언트-서버 모델에서 하이브리드 인증 및 키관리 메커니즘 표준화 추진 중
 - (Q.9) 모바일 디바이스에서의 텔레바이오인식 보안지침(X.1087), 바이오인식기반 하드웨어 보안토큰(X.1085)은 개발 완료하였으며, 생체신호를 이용한 텔레바이오인식기술(X.tab), 스마트 ID카드를 이용한 원격 바이오 접근제어기술(X.tac)을 개발 중. 향후 ISO TC215와 공동으로 생체신호 인증기반의 헬스모니터링 분석기술에 대한 국제표준을 신규로 개발할 예정
 - (Q.10) 객체 인증 보증 프레임워크와 접근하는 자원 별 서로 다른 인증 수준을 적용하기 위한 스텝업 인증 프로토콜 표준화 추진 중
 - (FIDO Alliance) 기존 모바일 중심의 FIDO1.0/1.1/1.2에서 모바일뿐만 아니라 웹, PC운영체제로의 Upgrade되어 W3C를 통해 표준화 추진 중. EMVCo, GSMA, ISO와도

Liaison을 맺고 표준화 관련 협업 중. 또한 효율적인 사실표준화를 위해 5개의 Regional WG을 FIDO Alliance 산하조직으로 운영 중(한국/중국/일본/유럽/인도)

<국제 표준화 현황>

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
IEEE	Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages(IEEE Std. 1609.2-2016)	2016	PKI 기반 기기 인증
U.S. DOT/ NHTSA	Security Credential Management System Proof-of-Concept Implementation, EE Requirements and Specifications Supporting SCMS Software Release 1.2.2 NHTSA,(November 15, 2016)	2016	PKI 기반 기기 인증
	Security Credentials Management System(SCMS) Design and Analysis for the Connected Vehicle System, U.S. Department of Transportation, Research and Innovative Technology Administration (December 27, 2013)	2013	
European Commission	Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems(C-ITS)	2017	PKI 기반 기기 인증
JTC1 SC27	ISO/IEC NP 9798-5, Entity authentication – Part 5: Mechanisms using zero-knowledge techniques	진행 중 (2022)	멀티팩터 인증 기술
	ISO/IEC NP 29115, Entity authentication assurance framework	진행 중 (2022)	
	ISO/IEC AWI 27551, Requirements for attribute-based unlinkable entity authentication	진행 중 (2022)	
	ISO/IEC 24745R1, Biometric Information Protection	진행 중 (2021)	바이오인식 응용 서비스
	ISO/IEC CD 20009-3, Anonymous entity authentication – Part 3: Mechanisms based on blind signatures concepts	진행 중 (2020)	멀티팩터 인증 기술
	ISO/IEC CD 24761, Authentication context for biometrics	진행 중 (2020)	
	X.1085 ISO/IEC 17922, Telebiometric authentication framework using biometric hardware security module	2017	바이오인식 응용 서비스
	ISO/IEC 29115, Security techniques – Entity authentication assurance framework	2013	멀티팩터 인증 기술
JTC1 SC37	30106-1AMD1, Object oriented BioAPI – Part 1: Architecture – Amendment 1: Additional specifications and conformance statements	진행 중 (2019)	바이오인식 응용 서비스
	30106-4, Information technology – Object oriented BioAPI – Part 4: C++ Implementation	진행 중 (2019)	
	24709-1R1, Conformance Test for BioAPI Part1 revision	2017	
	19794-15, Biometric data interchange format – Part 15: Palm crease image data	2017	
ITU-T SG17	X.te, Trust Elevation Protocol – Authentication Step-Up Protocol and Metadata Version 1.0	진행 중 (2022)	멀티팩터 인증 기술

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
	X.1254rev, Entity authentication assurance framework	진행 중 (2020)	
	X.sup-1254rev, Supplement to X.1254rev on use cases and high level abstract implementations	진행 중 (2020)	
	X.hakm, Guidelines on hybrid authentication and key management mechanisms in the client-server model	진행 중 (2019)	
	X.tab, Telebiometric Authentication using Biosignals	진행 중 (2019)	생체신호기반 텔레바이오 인증 기술
	X.tac, Telebiometric Access Control with smart ID	2018	바이오인식 응용 서비스
	X.1087, A guideline to technical and operational countermeasures for telebiometric applications using mobile devices(X.tam)	2017	
	X.1085 ISO/IEC 17922, Telebiometric authentication framework using biometric hardware security module	2017	
	X1158, Multi-factor authentication mechanisms using a mobile device	2014	멀티팩터 인증 기술
	X.1254, Entity authentication assurance framework	2012	
FIDO Alliance	FIDO2	진행 중 (2018)	FIDO 및 응용기술
	UAF 1.1(Universal Authentication Framework)	2017	
	U2F 1.2(Universal 2nd Factor)	2017	

○ (사이버 보안) 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 작업이 OASIS의 CTI(Cyber Threat Intelligence) 기술 위원회에서 진행 중

- (ITU-T SG17)

- 사이버 보안 침해 데이터의 증거능력을 높이기 위해 수집보존 도구에 대한 가이드라인을 표준화하여 수집된 데이터의 신뢰성 확보를 기대
- 신규 표준 아이템으로 Guidelines for Collection and Preservation of Cybersecurity Incidence Evidence와 같이 표준화 아이템이 제안되어 논의 중

- (IETF) 침해사고 데이터형식인 IODEF(Incident Object Description Exchange Format)와 침해사고 추적 프로토콜인 RID(Real-time Inter-network Defense)의 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 표준화를 한국주도로 진행 중

- (OASIS) 2016년 사이버위협에 대응하기 위한 유관기관간의 침해사고 정보공유 포맷 및 협업형 통합제어 프레임워크 개발 중

- 사이버 위협 정보 표현방식은 지속적으로 발전/통합되고 있으며, 또한 다른 위협 정보의 내용과 연동성을 제공하는 기능들을 제공하는 방식으로 발전 중

<국제 표준화 현황>

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
ITU-T SG17	X.1500 Amd.12 - X.1500(2011) Amendment 12, Overview of cybersecurity information exchange(CYBEX)	2018	사이버 위협정보 공유 포맷 및 프로토콜
	X.1500 Appendix I - X.1500(2011) Amendment 11, Overview of cybersecurity information exchange(CYBEX)	2017	
	Revised X.1541 - Incident object description exchange format version2	2017	
	X.1500 Appendix I - X.1500(2011) Amendment 7, Overview of cybersecurity information exchange(CYBEX)	2015	
	X.1525 - Common weakness scoring system	2015	

○ (보안관리/보안평가)

- (JTC1 SC27, CCRA) CCRA에서 2017년에 개정한 CC 및 CEM은 ISO/IEC JTC1과 협력하여 ISO/IEC 15408, ISO/IEC 18045로 개정 중이며, 기존의 ISO/IEC 15408 part1/2/3에 part4/5를 추가하여 확장

<국제 표준화 현황>

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
JTC1 SC27	ISO/IEC 15408-1, Evaluation criteria for IT security Part1: Introduction and general model(Amendment)	진행 중 (2020)	IT제품 보안성 평가기준
	ISO/IEC 15408-2, Evaluation criteria for IT security Part2: Security functional components(Amendment)	진행 중 (2020)	
	ISO/IEC 15408-3, Evaluation criteria for IT security Part3: Security assurance components(Amendment)	진행 중 (2020)	
	ISO/IEC 15408-4, Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities(Amendment)	진행 중 (2020)	
	ISO/IEC 15408-5, Evaluation criteria for IT security - Part 5: Pre-defined packages of security requirements(Amendment)	진행 중 (2020)	
	ISO/IEC 18045, Methodology for IT security evaluation(Amendment)	진행 중 (2020)	
	TR 22216, Introductory guidance on Evaluation for IT security(Amendment)	진행 중 (2020)	
	ISO/IEC 19896-1, Competence requirements for information security testers and evaluators	진행 중 (2019)	
	ISO/IEC 19896-3, Competence requirements for information security testers and evaluators-Part 3:	진행 중 (2019)	

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
	Knowledge, skills and effectiveness requirements for CC evaluators		
	ISO/IEC 15446, Guide for the production of Protection Profiles and Security Targets(Amendment)	진행 중 (2019)	
CCRA	Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5	2017	IT제품 보안성 평가기준
	Common Methodology for Information Technology Security Evaluation, Version 3.1, revision 5	2017	
	collaborative Protection Profile for Network Devices v2.0	2017	
	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 Stateful Traffic Filter Firewalls v1.0	2015	

- (융합보안) 의료보안 분야는 ISO TC 215 WG 4와 WG7을 중심으로 의료정보기술과 의료기기에 대한 보안 표준 제·개정 및 신규 표준안 개발 작업 진행중이고, 제조보안 분야는 IEC TC65 WG10에서 미국 ISA 99 위원회와 협업하여 IEC 62443 제조보안시스템 시리즈를 개발하였고, 새로운 기술 적용에 대한 제·개정 작업을 진행 중
- (ISO TC215 WG4) 의료기기에 대한 위험 분석과 요구사항 표준(11633-1)이 개정 완료되었고 IoT 의료기기에 대한 보안 표준, PKI 응용 등에 대한 표준 제·개정 및 신규 개발 작업 중
 - (IEC TC65 WG10) 2018년 10월 부산 벡스코에서 개최될 표준 회의에 참가하여 제조보안에 대한 국제표준화 아이템 발굴과 인적 네트워크 확보 계획 중

<국제 표준화 현황>

개발기구	표준(안)명	개발연도	관련 중점 표준화 항목
ISO TC215 WG4/WG7	ISO 25237, Health informatics - Pseudonymization	2017	진료정보 교류시 보안표준 모델, 의료기기 안전 및 보안 프레임워크
	ISO 22696, Guidance for an identification and authentication framework of networked PHD	2017	
	ISO 27799, Health informatics - Information security management in health using ISO/IEC 27002	2016	
IEC TC65 WG10	IEC 62443-1, General Series	2017	스마트공장 기기 상호 보안인증기술, 중소기업용 스마트공장 보안 관리 기술
	IEC 62443-2, Policy & Procedure) Series	2017	
	IEC 62443-3, System Series	2017	
	IEC 62443-4, Component Series	2017	

2.6. 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 킷 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 있으며, 조만간 국내 개발 블록 암호 ARIA를 포함하는 1.1.1 버전 배포 예정. 2006년 오픈소스 중 최초로 1.0버전에 대한 FIPS 140-2 검증을 받았으며, 2016년 7월 OpenSSL 1.1에 대한 FIPS 140-2 검증을 시작

○ 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, 2013, 2017년을 기준으로 발표되었고, 문서를 공개

○ 기타 오픈소스 보안 툴

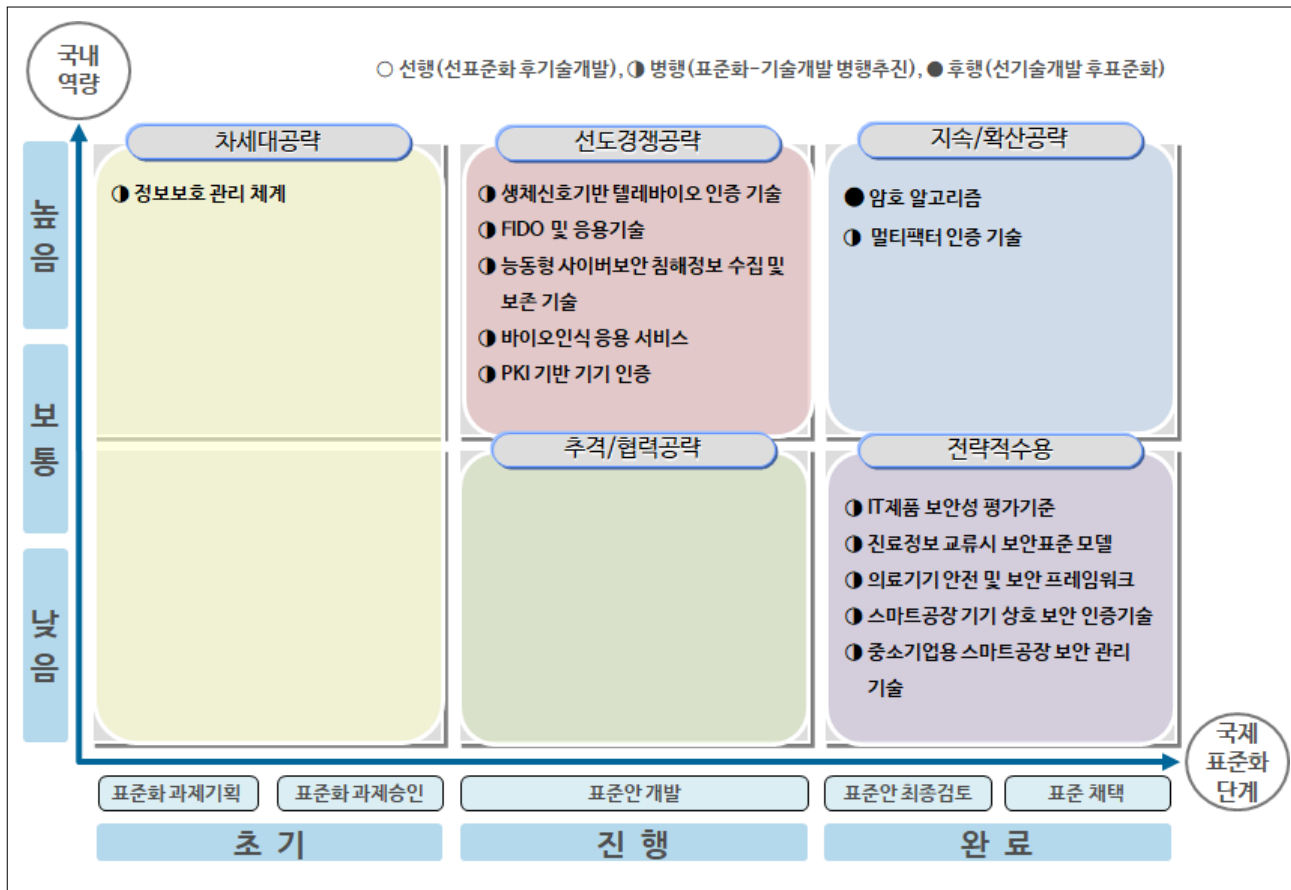
오픈소스 보안툴	설 명
Nmap	가장 널리 알려진 네트워크와 포트를 스캐닝 하는 툴임. Nmap은 네트워크 서비스에 관한 취약성, 잘못된 구성 및 보안 관련 정보를 탐지할 수 있는 NSE 스크립트를 제공
OpenVAS	오픈소스 취약점 스캐닝 툴로써, 웹기반의 대쉬보드를 통해 보안 취약점을 관리 가능
OSSEC	호스트 기반의 침입탐지시스템으로 설치 및 구성이 쉬우며, 누구나 쉽게 사용 가능
Security Onion	네트워크 보안모니터링 툴로 설치 및 구성이 쉬움. 최소한의 노력으로 APT를 포함한 네트워크 기반의 이상행위를 탐지 가능
Metasploit Framework	공격자의 관점에서 보안의 수준을 테스트할 수 있음. 침투테스트 도구로 익스플로잇과 스캐닝 그리고 감사기능을 포함
Wireshark	트래픽을 캡처하여 분석할 수 있는 기능을 제공해 주는 오픈 소스툴로 다양한 OS 환경을 지원
Kali Linux	Back Track Linux 기반으로 만들어졌으며, 데비안 기반의 보안 테스트를 위한 리눅스용 배포판
Nikto	10년이 넘는 웹서버 테스트 툴, 알려진 취약한 스크립트, 구성실수 및 관련 보안 문제를 찾기 위해 웹 서버에서 실행하기에 적합
Moloch	패킷캡처 분석 툴로 pcap으로부터 빠른 검색이 가능함. 캡처된 패킷의 디코딩을 지원하며 트래픽 분석에 유용한 툴
Bro IDS	시그니처기반의 전통적인 IDS의 기능을 넘어 프로토콜을 디코딩하고 트래픽 내에서의 특이점을 탐지 가능
Snort	실시간 트래픽 분석 및 패킷 로깅 도구로서 전통적인 IDS와 유사하게 동작
OSQuery	Facebook Security Team에서 시작한 크로스플랫폼으로 시스템에 에이전트 기반으로 동작하면서 이상 행위와 보안관련된 이벤트를 모니터링 가능
GRR	보안 사고를 신속하게 대응하기 위해 Google이 제작한 툴로, 파이썬 에이전트와 서버의 조합을 통해 사고 대응을 원격에서 수행 가능

Ⅲ. 국내외 표준화 추진전략

3.1. 표준화 SWOT 분석

국외환경요인		국내역량요인		강점요인(S)	약점요인(W)		
		시장	기술	표준	시장		
						기술	표준
시장	- 신규 ICT 환경에 기반한 범용/바이오 인증 서비스 시장 규모 확장	기술	- 각종 보안 이슈 대응을 위해 기업 및 기관의 침해사고 대응 장비 구매 증가 - 보안 필요성에 대한 높은 범사회적 인식	표준	- 세계 시장 대비 국내 보안 시장 규모 협소 - 국내개발 암호기술의 제품 적용사례 미흡		
기술	- 웹2.0, 클라우드, 빅데이터 등의 활성화에 따른 개인 정보보호에 대한 지속적 수요 - 해킹기술의 고도화 등으로 정보보호 강화 요구 증가 - 적용환경 변화 및 취약요소 증가에 대응 가능한 새로운 암호 기술 개발수요 확대	표준	- 국제 경쟁력을 갖춘 범용 및 신규 ICT용 암호 기반기술 및 인증 응용기술 다수 확보 - 침해사고 대응체계 구축 및 풍부한 운용 경험 보유	표준	- 차세대 암호·인증 기술, 정보보호 관리체계 구축 등 관련 고급 개발인력 부족 - 의료, 제조 분야 등 융합보안 분야에서 보안기술 적용 미흡		
표준	- ISO/IEC JTC1, ITU-T 등 국제표준화 기구에서 논의 초기 단계인 양자암호 표준화 선도	표준	- 보안 분야에서 국내 전문가의 국제표준화 기여도 높음 - 국내 및 국제표준화 경험을 토대로 신규 표준화 활동 용이	표준	- 학계와 KISA, ETRI 등 정부기관 중심의 표준화 진행과 산업체의 참여 미흡 - 표준화 전문인력 부족으로 다양한 표준화 기구를 통한 표준화 추진이 어려움		
기획요인(O)		시장	【SO전략】		【WO전략】		
		기술	-(시장) 범용/바이오 인증 등 시장 확대예상 분야에서 기존 인프라와 결합을 통한 선점 효과 극대화 -(기술) 국내 개발 차세대 암호·인증기술을 다양한 신규 ICT 보안에 활용하여 응용 측면의 융합보안 기술 확보 -(표준) ISO/IEC, ITU-T에서 활동 중인 국제 표준 전문가를 활용한 국제표준화 추진, 양자암호 암호 안전성 기준 조기 수립 및 국내표준화를 통한 관련 국제표준화 주도		-(시장) 정보보호 관리체계 조기 구축을 통한 정보보호 관리 영역 확대 및 클라우드, 빅데이터, 의료 등의 개인정보보호 제품 적용 분야 확대 추진 -(기술) 국내 산업계의 요구사항을 반영한 소요기술 개발 및 제품 조기 적용을 통한 제품 경쟁력 향상 -(표준) 융합보안 관련 분과와 협력하여 보안기술 적용 표준 도출		
		표준					
위협요인(T)		시장	【ST전략】		【WT전략】		
		기술	-(시장) 국내 환경 선적용을 통해 제품 인지도와 완성도를 제고하여 해외 시장 경쟁력 확보 -(기술) 신규 ICT 서비스 중심의 암호·인증 원천기술 및 융합보안 기술 개발을 통한 국제 경쟁력 확보 -(표준) 개발 기술의 적용 경험을 바탕으로 도출된 다양한 Use Case를 기반으로 표준화 초기 단계에서 주도권 확보 추진		-(시장) 국내 산·학·연 연계를 통한 기술 개발 및 활용의 선순환 체계 구축 -(기술) 국책 연구개발 과제를 통한 IPR 획득 및 이를 통한 기술 및 서비스 제공 -(표준) 활용성이 담보된 표준 개발을 통한 산업계 참여 확대 및 산업계 표준화 소요 조기 대응		
		표준					
표준화 추진상의 문제점 및 현안 사항							
- 차세대보안 원천기술의 국내 산업경쟁력이 선진국대비 격차가 존재하나, 차세대 암호기술, 바이오·인증 기술 등 국제표준화에 적극적인 대응 추진							
- 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							

3.2. 중점 표준화 항목별 국내외 추진전략



○ 영역별 특징 및 대응전략

- **차세대공략** : 미래 핵심기술 및 유망서비스 신규 표준 제안을 통해 표준화를 선점할 수 있는 분야
: 국제 표준 기획 단계부터 주도적 참여를 통해 국제표준화 선도 기반 확보
: 관련 표준화기구에서의 적극적인 제안으로 국내 핵심 기술의 국제표준화를 위한 발판 마련
- **선도경쟁공략** : 표준화 경쟁이 치열하지만 국내역량이 높아 국제표준 선도가 가능한 분야
: 국내 기술의 국제표준 반영을 위한 관련 표준화기구에서의 적극적인 표준화활동 추진
- **추격/협력공략** : 국제표준화가 활발히 진행 중인 분야 중 국내 진입시기가 다소 늦어졌지만 타 국가의 표준화 수준에 도달하기 위해 후발주자로서 추격하거나 다각화된 협력이 필요한 분야
: 국제 공식 및 사실표준화기구, 포럼, 컨소시엄에서의 다각적인 대응 방안 모색
: 전략적 대외협력 강화 및 제휴를 통한 기술/표준의 Catch-up 전략 추진
- **지속/확산공략** : 국제표준화가 거의 완료단계이나 국내역량이 높아 후속/개정 표준화에서의 선도가 예상되며, 표준 기반 서비스 및 시장 확산에 집중이 필요한 분야
: 높은 국내 역량을 바탕으로 한 후속/개정 표준화 주도 및 추가적인 틈새표준 발굴을 모색
: 표준기반 킬러 애플리케이션 개발 및 서비스 적용을 통한 표준 활용 촉진
- **전략적수용** : 국제표준화가 거의 완료된 분야 중 국내역량은 낮지만 전략적으로 수용이 필요한 분야
: 국제 표준의 수용 및 적용을 통한 국제 호환성 확보와 국내 시장 확산

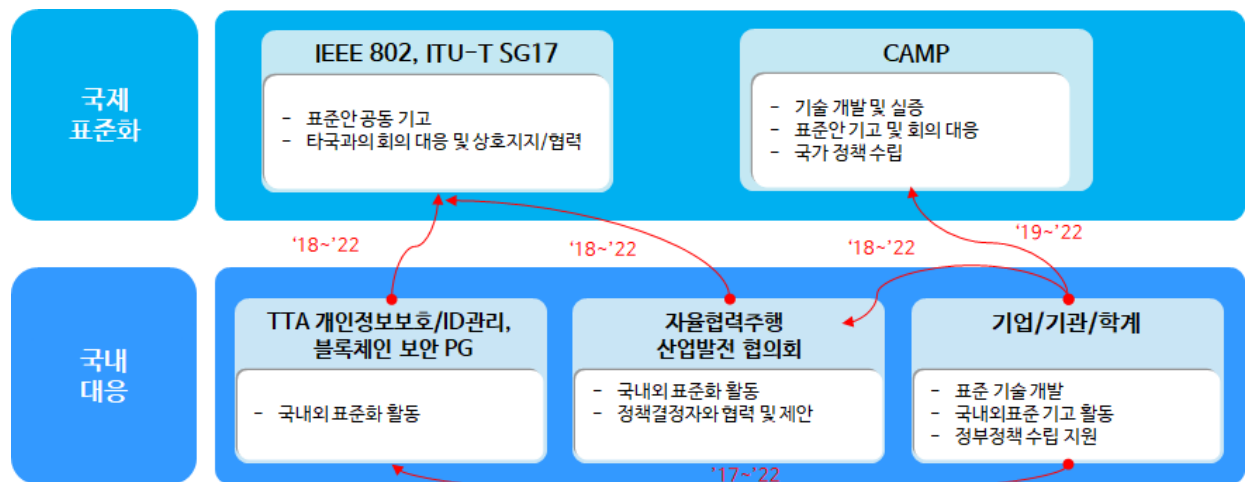
(지속/확산공략 | 후행) 암호 알고리즘

전략적 중요도 / 국내 역량	<p>정책 부합성</p> <p>국제표준화 국내 기여도</p> <p>IPR 확보 가능성</p> <p>시장/기술적 파급효과</p> <p>국외대비 국내 표준화 역량</p> <p>국외대비 국내 기술개발 수준</p>		표준화 기구/ 단체	국내	TTA 정보보호기반 PG
	국제	JTC1 SC27, IETF			
	국내 참여 업체/ 기관	NSR, ETRI, 삼성 SDS			
기술 개발 단계	국내	□기초연구→□실험→□시작품→■제품화→□사업화	기술 수준	90% (선도국가대비)	
	국외	□기초연구→□실험→□시작품→□제품화→■사업화			
	선도국가 /기업	한국/NSR, 일본/NTT 벨기에/COSIC, 싱가포르/난양대 미국/NSA, IBM, MS			
표준화 단계	국내	□과제기획→□과제승인→□개발→□검토→■표준채택	표준 수준	100% (선도국가대비)	
	국제	□과제기획→□과제승인→□개발→■검토→□표준채택			
	선도국가 /기업	미국/NIST 일본/Sony 벨기에/COSIC			
<p>- Trace Tracking : 차세대공략(Ver.2018) → 지속/확산공략(Ver.2019)</p> <p>암호 알고리즘의 경우 국내 확보 기술(블록 암호 LEA, 해시 함수 LSH, 형태보존 암호 FEA)과 관련한 국제표준이 기 제정되었거나 신규 제안이 필요한 상황에서, 현재 미국 등의 자국 암호기술 위주 표준화 추세에 대응하고 관련 개정/신규 표준화 과정에서의 리더십을 확보하기 위해 먼저 암호기술 활용성 강화와 국제 협력 추진이 필요하다고 판단되어, Ver.2019에서는 “지속/확산공략” 항목으로 분류</p>					



(선도경쟁공략 | 병행) PKI 기반 기기 인증

전략적 중요도 / 국내 역량				표준화 기구/ 단체	국내	TTA 개인정보 보호 및 ID관리, 블록체인 보안 PG
					국제	IEEE 802, ITU-T SG17, CAMP
					국내 참여 업체/ 기관	KISA, 한국도로공사, 한국정보인증, 펜타시큐리티
기술 개발 단계	국내	□기초연구→□실험→□시작품→■제품화→□사업화			기술 수준	95% (선도국가대비)
	국외	□기초연구→□실험→□시작품→□제품화→■사업화				
	선도국가 /기업	미국/NHTSA 유럽연합위원회/Escrypt				
표준화 단계	국내	□과제기획→□과제승인→□개발→■검토→□표준채택			표준 수준	95% (선도국가대비)
	국제	□과제기획→□과제승인→■개발→□검토→□표준채택				
	선도국가 /기업	미국/NHTSA 유럽연합위원회				
<p>- Trace Tracking : 다각화협력(Ver.2018) → 선도경쟁공략(Ver.2019)</p> <p>PKI 기기인증 기술은 4차산업 혁명을 사용되는 다양한 IoT 기기들에 대한 사용이 증가하고 있고 특히 이러한 기기들의 안전하고 신뢰성있는 사용을 위한 기기인증의 필요성이 증대되고 있음. IoT 기기 중에서 차량의 자율주행을 위한 부분은 사람의 생명과 직결되어 있고 전 세계적으로 많은 연구가 진행 중이 있으며 우리나라도 세종시 시범사업이후 서울/제주의 시범사업이 진행 예정이고 정부에서도 2020년 Level 3 상용화를 위해 다양한 노력을 진행하고 있음, 따라서 선도경쟁공략 항목으로 분류</p>						



<국제 표준화 대응체계>

국제 표준화 대응 방안	<p><현황></p> <ul style="list-style-type: none"> - 2016년 IEEE를 통하여 V2X 관련 표준이 개정된 후에 미국은 국토부를 중심으로 3개 주에 통한 시범사업을 진행 중이고 유럽의 경우 인증모델을 정하고 유럽전체에 적용 가능한 인증정책 등을 개발 중 <p><대응방안></p> <ul style="list-style-type: none"> - (공식표준화 대응전략 : 국제표준화기구 활동(적극대응)) 다양한 표준화 활동에 적극 참여하여 동향을 파악하고 이를 한국에 적용하고 준비가 필요
국내 표준화 추진 계획	<p><현황></p> <ul style="list-style-type: none"> - KISA와 한국도로공사와 같이 차량용 보안인증체계 구축을 위한 컨설팅을 진행하고 있음 - 자율협력주행 산업발전 협의회는 국토부 장관과 민간 공동의장 4명을 비롯해 자동차·인프라·정보통신 등 160여개 유관기관 소속 400여명이 참여하여 자율주행 산업생태계가 조속히 조성될 수 있도록 협의회를 통해 데이터 공유, 시험환경 제공, 대·중소기업 간 네트워크 행사를 적극 추진 <p><추진계획></p> <ul style="list-style-type: none"> - (국내 표준 개발) 차량용 인증기관에 대한 인증체계, 인증업무준칙, 시설 및 장비 규정 등에 대해 검토하여 표준화 추진 예정 - (자율협력주행 산업발전 협의회) 자율협력주행을 위한 통신, 정밀지도, 보안 분과를 통하여 표준화 추진 예정
표준특허 전략	<ul style="list-style-type: none"> - 표준 및 R&D 중후기 전략 : 특허 권리범위 보완전략 - 자율협력주행 산업발전 협의회 등을 중심으로 다양한 Use case 분석을 통한 특허 권리범위 보완 추진
기술개발 -표준화 -IPR 연계방안	<ul style="list-style-type: none"> - 표준화-기술개발 병행추진 - 표준화가 완료됨과 동시에 자율협력주행(C-ITS) 산업에 즉시 활용될 수 있는 기술들이 많은 분야임. 따라서 기술 개발과 동시에 표준화를 병행 추진함으로써 기술의 파급효과를 높이며 더 많은 부가가치를 창출하는 IPR을 확보함

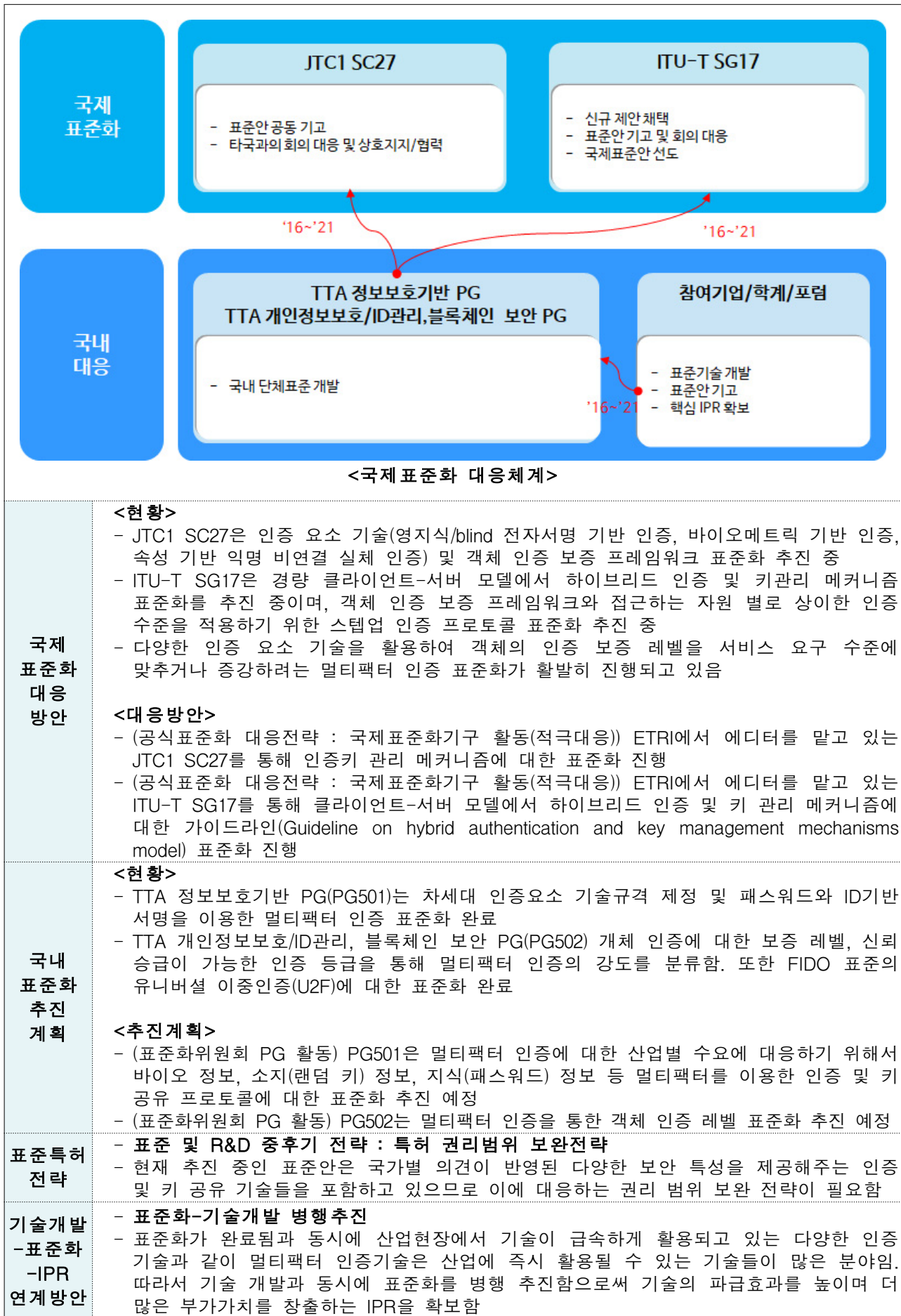
(선도경쟁공략 | 병행) FIDO 및 응용기술

전략적 중요도 / 국내 역량	<p>정책 부합성 국제표준화 국내 기여도</p> <p>국외대비 국내 표준화 역량 국외대비 국내 기술개발 수준</p> <p>시장/기술적 파급효과 IPR 확보 가능성</p>			표준화 기구/ 단체	국내	FIDO한국워킹 그룹, TTA 정보보호 기반 PG,
	국제	FIDO Alliance				
	국내 참여 업체/ 기관	삼성전자, BC 카드, 라운시큐어(보 드멤버사) ETRI				
기술 개발 단계	국내	□기초연구→□실험→□시작품→□제품화→■사업화		기술 수준	100% (선도국가대비)	
	국외	□기초연구→□실험→□시작품→□제품화→■사업화				
	선도국가 /기업	미국/Google, Microsoft, Paypal 한국/삼성전자, BC 카드, 라온시큐어, ETRI 중국/Lenovo 일본/NTT DOCOMO, Line, Yahoo Japan 유럽/Gemalto				
표준화 단계	국내	□과제기획→□과제승인→■개발→□검토→□표준채택		표준 수준	90% (선도국가대비)	
	국제	□과제기획→□과제승인→■개발→□검토→□표준채택				
	선도국가 /기업	미국/Google, Microsoft, NokNok				
<p>- Trace Tracking : 적극공략(Ver.2018) → 선도경쟁공략(Ver.2019)</p> <p>FIDO1.X의 개발 및 글로벌 상용화가 진행되고 있으며 올해부터 FIDO2의 상용화가 시작됨. 2019년부터는 다양한 업계로의 상용화 및 확산이 예상됨. 국내 FIDO한국워킹그룹 창설을 계기로 국내과제의 국제표준 채택추진 등 리더십을 확보하기 위해 먼저 FIDO기술 활용성 강화와 선도적인 표준화가 필요하여, “선도경쟁 공략” 항목으로 분류</p>						



(지속/확산공략 | 병행) 멀티팩터 인증 기술

전략적 중요도 / 국내 역량	<p>국제표준화 국내 기여도</p>		표준화 기구/ 단체	국내	TTA 정보보호 기반 PG, TTA 개인정보 보호 및 ID관리, 블록체인 보안 PG
				국제	ITU-T SG17, JTC1 SC27
				국내 참여 업체/ 기관	ETRI, 삼성전자
기술 개발 단계	국내	<input type="checkbox"/> 기초연구→ <input type="checkbox"/> 실험→ <input type="checkbox"/> 시작품→ <input type="checkbox"/> 제품화→ <input checked="" type="checkbox"/> 사업화		기술 수준	90% (선도국가대비)
	국외	<input type="checkbox"/> 기초연구→ <input type="checkbox"/> 실험→ <input type="checkbox"/> 시작품→ <input type="checkbox"/> 제품화→ <input checked="" type="checkbox"/> 사업화			
	선도국가 /기업	한국/ETRI, 한국CA테크놀로지스 미국/IBM, Cisco, Microsoft, Amazon			
표준화 단계	국내	<input type="checkbox"/> 과제기획→ <input type="checkbox"/> 과제승인→ <input type="checkbox"/> 개발→ <input type="checkbox"/> 검토→ <input checked="" type="checkbox"/> 표준채택		표준 수준	90% (선도국가대비)
	국제	<input type="checkbox"/> 과제기획→ <input type="checkbox"/> 과제승인→ <input type="checkbox"/> 개발→ <input checked="" type="checkbox"/> 검토→ <input type="checkbox"/> 표준채택			
	선도국가 /기업	미국/IBM, Google, Microsoft 유럽/INRIA, Gemalto 중국/China Mobile, Alibaba 한국/ETRI, 삼성SDS			
<p>- Trace Tracking : 지속/확산공략(Ver.2019 신규)</p> <p>영지식, 바이오메트릭, 익명 인증 등 다양한 인증 요소 기술을 활용하는 표준화 뿐만 아니라, FIDO 얼라이언스의 유니버설 이중인증, 하이브리드 인증 또는 스텝업 인증으로 개체의 인증 보증 레벨을 관리하는 멀티팩터 인증 표준화가 완료 단계이고 관련 기술의 사업화가 지속적으로 진행되어 시장 확산 및 추가적인 표준화 이슈가 예상되므로, 본 기술에 포함되는 멀티팩터 인증 기술에 대해 지속/확산공략 항목으로 분류</p>					



(선도경쟁공략 병행) 바이오인식 응용 서비스					
전략적 중요도 / 국내 역량				표준화 기구/ 단체	국내 TTA 바이오인식 PG, KBID
					국제 JTC1 SC27/SC37, ITU-T SG17, ABC
					국내 참여 업체/ 기관 KISA, ETRI, 인하대, 충북대, 경인여대, 삼성전자, LG전자, 슈프리마, 유니온 커뮤니티
기술 개발 단계	국내	□기초연구→□실험→□시작품→□제품화→■사업화		기술 수준	90% (선도국가대비)
	국외	□기초연구→□실험→□시작품→□제품화→■사업화			
	선도국가 /기업	한국/삼성전자, LG전자 미국/애플 일본/NEC 프랑스/Sagem Morpho			
표준화 단계	국내	□과제기획→□과제승인→■개발→□검토→□표준채택		표준 수준	90% (선도국가대비)
	국제	□과제기획→□과제승인→■개발→□검토→□표준채택			
	선도국가 /기업	한국/KISA 미국/NIST 영국/NPL 중국/알리바바 일본/NTT 도코모			
<div>- Trace Tracking : 적극공략(Ver.2018) → 선도경쟁공략(Ver.2019)</div> <div>모바일 바이오인식기술, 바이오인식 융합기술 등의 내용을 포함하여 헬스케어, 핀테크, 스마트카 등 다양한 IoT 환경분야에서 비대면 인증수단으로 바이오인식 국산기술을 널리 활용함에 따라 선도적인 표준화가 필요하며, 선도경쟁공략으로 분류</div>					



(선도경쟁공략 | 병행) 생체신호기반 텔레바이오 인증 기술

전략적 중요도 / 국내 역량	<p>국제표준화 국내 기여도</p> <p>국제표준화 역량</p> <p>국제표준화 수준</p> <p>IPR 확보 가능성</p> <p>시장/기술적 파급효과</p> <p>정책 부합성</p>		표준화 기구/ 단체	국내	TTA 바이오인식 PG, KBID, 스마트의료정보 포럼
	국제	ISO TC215, ITU-T SG17			
	국내 참여 업체/ 기관	KISA, 서울의과대 학, 충북대, 리턴트루, 유파인스, 유니온 커뮤니티, 삼성전자, LG전자			
기술 개발 단계	국내	□기초연구→□실험→■시작품→□제품화→□사업화	기술 수준	95% (선도국가대비)	
	국외	□기초연구→■실험→□시작품→□제품화→□사업화			
	선도국가 /기업	한국/삼성전자, LG전자, KISA 미국/애플사, TISA 캐나다/Bio-Nym사			
표준화 단계	국내	□과제기획→□과제승인→■개발→□검토→□표준채택	표준 수준	100% (선도국가대비)	
	국제	□과제기획→□과제승인→■개발→□검토→□표준채택			
	선도국가 /기업	한국/KISA 미국/Telebiometrics 민간연구소, TISA 스페인/Carlos-III 마드리드대학교			
<p>- Trace Tracking : 차세대공략(Ver.2018) → 선도경쟁공략(Ver.2019)</p> <p>Ver.2019에서는 KISA에서 생체신호를 이용한 텔레바이오인식 인증기술 개발 및 국내외 표준화를 선도적으로 활발히 추진함에 따라, ITU-T SG17 국제표준(X.tab)을 2017년도부터 개발 중으로 향후 ISO TC215와 공동으로 생체신호 인증기반의 헬스모니터링 분석기술에 대한 국제표준화를 선도하기 위하여 선도적 공략이 필요</p>					



(선도경쟁공략 | 병행) 능동형 사이버보안 침해정보 수집 및 보존 기술

전략적 중요도 / 국내 역량	<p>국제표준화 국내 기여도</p>		표준화 기구/ 단체	국내	TTA 사이버보안 PG, TTA 응용보안/ 평가인증 PG
				국제	ITU-T SG17, JTC1 SC27, ETSI
				국내 참여 업체/ 기관	ETRI, KISA
기술 개발 단계	국내	□기초연구→□실험→■시작품→□제품화→□사업화		기술 수준	95% (선도국가대비)
	국외	□기초연구→□실험→□시작품→■제품화→□사업화			
	선도국가 /기업	미국/IBM, FireEye			
표준화 단계	국내	□과제기획→□과제승인→□개발→□검토→■표준채택		표준 수준	90% (선도국가대비)
	국제	□과제기획→□과제승인→■개발→□검토→□표준채택			
	선도국가 /기업	미국/NIST			
<p>- Trace Tracking : 선도경쟁공략(Ver.2019 신규)</p> <p>사이버 공격에 대한 원인분석과 능동적인 사이버보안 기술 개발을 위해 사이버보안 침해정보 및 위협 정보를 수집하고 공유하기 위한 가이드라인, 프로토콜, 프레임워크 등에 대한 표준화가 ITU-T SG17 및 ISO/IEC SC27, ETSI 등에서 지속적으로 진행되고 있으며, 사이버보안 침해정보 수집 및 보존 기술 표준화에 대한 국내역량이 높아 국제표준 선도가 가능하여 선도경쟁공략 항목으로 분류</p>					



(차세대공략 | 병행) 정보보호 관리 체계

전략적 중요도 / 국내 역량	<p>국외대비 국내 표준화 역량</p> <p>국외대비 국내 기술개발 수준</p> <p>정책 부합성</p> <p>국제표준화 국내 기여도</p> <p>시장/기술적 파급효과</p> <p>IPR 확보 가능성</p>		표준화 기구/ 단체	국내	TTA 개인정보보호 및 ID관리, 블록체인 보안 PG
				국제	ISO TC307, JTC1 SC27, ITU-T SG17
				국내 참여 업체/ 기관	TCA서비스, 금융보안원
기술 개발 단계	국내	<input type="checkbox"/> 기초연구→ <input checked="" type="checkbox"/> 실험→ <input type="checkbox"/> 시작품→ <input type="checkbox"/> 제품화→ <input type="checkbox"/> 사업화	기술 수준	80% (선도국가대비)	
	국외	<input type="checkbox"/> 기초연구→ <input type="checkbox"/> 실험→ <input checked="" type="checkbox"/> 시작품→ <input type="checkbox"/> 제품화→ <input type="checkbox"/> 사업화			
	선도국가 /기업	한국/TCA 서비스 미국/IBM 독일/Microsoft			
표준화 단계	국내	<input checked="" type="checkbox"/> 과제기획→ <input type="checkbox"/> 과제승인→ <input type="checkbox"/> 개발→ <input type="checkbox"/> 검토→ <input type="checkbox"/> 표준채택	표준 수준	100% (선도국가대비)	
	국제	<input checked="" type="checkbox"/> 과제기획→ <input type="checkbox"/> 과제승인→ <input type="checkbox"/> 개발→ <input type="checkbox"/> 검토→ <input type="checkbox"/> 표준채택			
	선도국가 /기업	한국/TCA서비스, 블로코 미국/IBM 독일/Microsoft			
<p>- Trace Tracking : 적극공략(Ver.2018) → 차세대공략(Ver.2019)</p> <p>전 세계적으로 블록체인 기술을 활용한 응용시스템이 도입되고 있으며 플랫폼 및 보안 기술이 개발되고 있으나 블록체인 서비스를 제공하는 기관이 안전하게 서비스를 운영하고 있는지 확인하기 위한 기준이 존재하지 않는 실정임. 이에 따라 블록체인 서비스 제공 기관 및 이용 기관에게 필요한 정보보안관리 통제를 제공하고 이에 기초하여 블록체인 서비스 제공 기관에 대한 인증을 부여하는 제도가 필요함. 국제 표준 제정에 따른 파급력이 크며 관련 SDO에서의 한국 영향이 높아 차세대공략 항목으로 분류</p>					



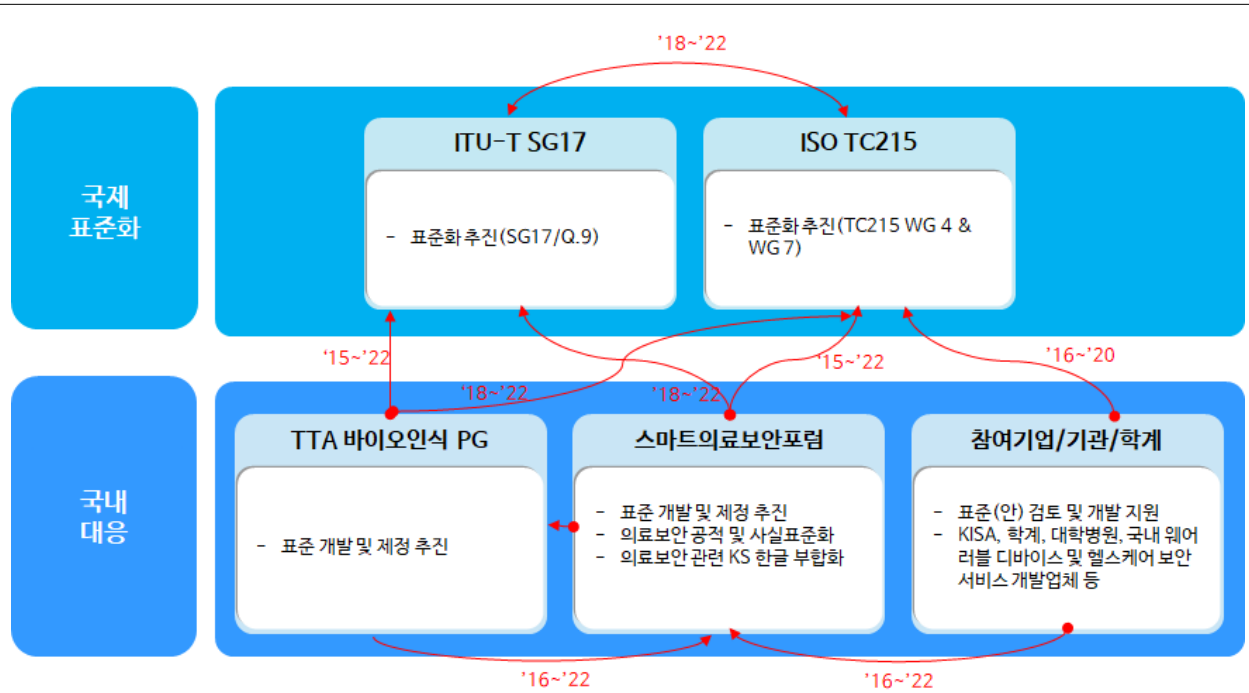
(전략적수용 | 병행) IT제품 보안성 평가기준

전략적 중요도 / 국내 역량			표준화 기구/ 단체	국내	TTA 응용보안/ 평가인증 PG, 국가기술표준원
				국제	JTC1 SC27 WG3, CCRA, CCUF
				국내 참여 업체/ 기관	NSR, KCCUF,(주)원 스,(주)안랩,(주) 시큐아이
기술 개발 단계	국내	<input type="checkbox"/> 기초연구→ <input type="checkbox"/> 실험→ <input checked="" type="checkbox"/> 시작품→ <input type="checkbox"/> 제품화→ <input type="checkbox"/> 사업화		기술 수준	80% (선도국가대비)
	국외	<input type="checkbox"/> 기초연구→ <input type="checkbox"/> 실험→ <input type="checkbox"/> 시작품→ <input type="checkbox"/> 제품화→ <input checked="" type="checkbox"/> 사업화			
	선도국가 /기업	한국/(주)안랩,(주)HP코리아 미국/Microsoft 독일/Tuvit 프랑스/Gelmato			
표준화 단계	국내	<input type="checkbox"/> 과제기획→ <input type="checkbox"/> 과제승인→ <input checked="" type="checkbox"/> 개발→ <input type="checkbox"/> 검토→ <input type="checkbox"/> 표준채택		표준 수준	90% (선도국가대비)
	국제	<input type="checkbox"/> 과제기획→ <input type="checkbox"/> 과제승인→ <input type="checkbox"/> 개발→ <input type="checkbox"/> 검토→ <input checked="" type="checkbox"/> 표준채택			
	선도국가 /기업	한국/NSR, ETRI, TTA 미국/NIST, NIAP, Atsec 독일/BIS 일본/IPA, AIST			
<div>- Trace Tracking : 적극공략(Ver.2018) → 전략적수용(Ver.2019)</div> <div>정보보호제품의 국제적인 신뢰성 확보와 국가통신망의 정보보호수준 제고 및 정보보호제품의 경쟁력 강화를 위해 법에 근거를 두고 평가인증제도가 운영되고 있으나, 국내용과 국제용으로 이원화 운영되고 국제용 인증 수요가 현격하게 줄면서 평가기술 격차가 발생함. 국제표준 개정예 전략적으로 대응할 필요가 있으므로 전략적 수용 항목으로 분류</div>					



(전략적수용 | 병행) 진료정보 교류시 보안표준 모델

전략적 중요도 / 국내 역량				표준화 기구/ 단체	국내	TTA 바이오인식 PG, 스마트의료보안 포럼
					국제	ISO TC215, ITU-T SG17
					국내 참여 업체/ 기관	보건산업진흥원, 건강보험 심사평가원, 사회보장정보원, 경북대, 건국대
기술 개발 단계	국내	□기초연구→□실험→□시작품→■제품화→□사업화			기술 수준	80% (선도국가대비)
	국외	□기초연구→□실험→□시작품→□제품화→■사업화				
	선도국가/ 기업	미국/GE Healthcare 유럽/Philips, Siemens				
표준화 단계	국내	□과제기획→□과제승인→□개발→■검토→□표준채택			표준 수준	90% (선도국가대비)
	국제	□과제기획→□과제승인→□개발→□검토→■표준채택				
	선도국가/ 기업	미국/GE Healthcare 유럽/Philips, Siemens				
<p>- Trace Tracking : 전략적수용(Ver.2019 신규)</p> <p>2016년도부터 의료기관에 대한 사이버 위협 및 공격이 빈발함에 따라, 의료기관 간 상호 진료정보교류에 대한 필요성과 요구가 증가함에 따라, 한국 주도로 표준 작성과 더불어서 관련된 요소기술을 파악하여 특허화 함으로써 시장 선점의 기회를 갖도록 함</p>						

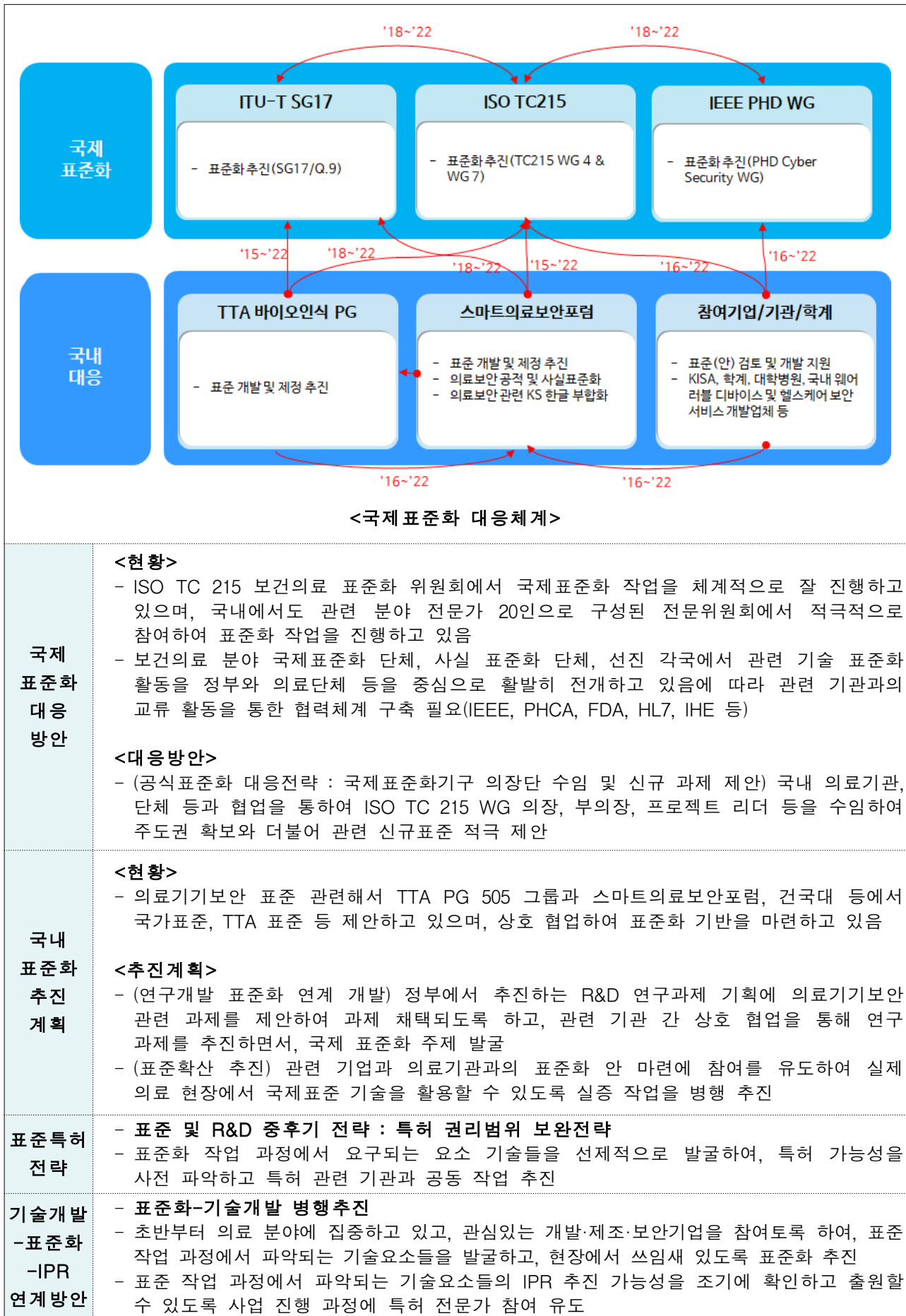


<국제 표준화 대응체계>

국제 표준화 대응 방안	<p><현황></p> <ul style="list-style-type: none"> - ISO TC 215 보건의료 표준화 위원회에서 국제표준화 작업을 체계적으로 잘 진행하고 있으며, 국내에서도 관련 분야 전문가 20인으로 구성된 전문위원회에서 적극적으로 참여하여 표준화 작업을 진행 중 - 보건의료 분야 국제표준화 단체, 사실 표준화 단체, 선진 각국에서 관련 기술 표준화 활동을 정부와 의료단체 등을 중심으로 활발히 전개하고 있음에 따라 관련 기관과의 교류 활동을 통한 협력체계 구축 필요(미국 FDA, ONC, HL7, IHE 등) <p><대응방안></p> <ul style="list-style-type: none"> - (공식표준화 대응전략 : 국제표준화기구 의장단 수임 및 신규 과제 제안) 국내 의료기관, 단체 등과 협업을 통하여 ISO TC 215 WG 의장, 부의장, 프로젝트 리더 등을 수임하여 주도권 확보와 더불어 관련 신규표준 적극 제안
국내 표준화 추진 계획	<p><현황></p> <ul style="list-style-type: none"> - 의료보안 표준 관련해서 TTA PG 505 그룹과 스마트의료보안포럼, 건국대 등에서 국가표준, TTA 표준 등 제안하고 있으며, 상호 협업하여 표준화 기반을 마련 중 <p><추진계획></p> <ul style="list-style-type: none"> - (연구개발 표준화 연계 개발) 정부에서 추진하는 R&D 연구과제 기획에 의료보안 관련 과제를 제안하여 과제 채택되도록 하고, 관련 기관 간 상호 협업을 통해 연구 과제를 추진하면서, 국제 표준화 주제 발굴 - (표준확산 추진) 관련 기업과 의료기관과의 표준화 안 마련에 참여를 유도하여 실제 의료 현장에서 국제표준 기술을 활용할 수 있도록 실증 작업을 병행 추진
표준특허 전략	<ul style="list-style-type: none"> - 표준 및 R&D 중후기 전략 : 특허 권리범위 보완전략 - 표준화 작업 과정에서 요구되는 요소 기술들을 선제적으로 발굴하여, 특허 가능성을 사전 파악하고 특허 관련 기관과 공동 작업 추진
기술개발 -표준화 -IPR 연계방안	<ul style="list-style-type: none"> - 표준화-기술개발 병행추진 - 초반부터 의료 분야에 집중하고 있고, 관심있는 개발·제조·보안기업을 참여토록 하여, 표준 작업 과정에서 파악되는 기술요소들을 발굴하고, 현장에서 쓰임새 있도록 표준화 추진 - 표준 작업 과정에서 파악되는 기술요소들의 IPR 추진 가능성을 조기에 확인하고 출원할 수 있도록 사업 진행 과정에 특허 전문가 참여 유도

(전략적수용 | 병행) 의료기기 안전 및 보안 프레임워크

전략적 중요도 / 국내 역량	 국제표준화 국내 기여도		표준화 기구/ 단체	국내	TTA 바이오인식 PG, 스마트 의료보안포럼
				국제	ISO TC215, ITU-T SG17, IEEE PHD WG
				국내 참여 업체/ 기관	국가기술표준원, 식품의약품안전 처, 의공협회, KISA, 경북대, 건국대
기술 개발 단계	국내	□기초연구→□실험→□시작품→■제품화→□사업화	기술 수준	80% (선도국가대비)	
	국외	□기초연구→□실험→□시작품→□제품화→■사업화			
	선도국가/ 기업	미국/GE Healthcare 유럽/Philips, Siemens			
표준화 단계	국내	□과제기획→□과제승인→□개발→■검토→□표준채택	표준 수준	90% (선도국가대비)	
	국제	□과제기획→□과제승인→□개발→□검토→■표준채택			
	선도국가/ 기업	미국/GE Healthcare 유럽/Philips, Siemens			
<p>- Trace Tracking : 전략적수용(Ver.2019 신규)</p> <p>2017년 초부터 의료기기를 대상으로 한 보안 취약성과 랜섬웨어 공격이 빈발함에 따라, 의료기간 상호 보안인증에 대한 국제표준 초안을 제안하여, 한국 주도로 표준안 작성을 적극 추진하고 있으며, 표준화 과정에서 관련된 요소기술을 우선적으로 파악하여 특허화 함으로써 시장 선점의 기회를 갖도록 함</p>					



(전략적수용 | 병행) 스마트공장 기기 상호 보안 인증기술

전략적 중요도 / 국내 역량	<p>국외대비 국내 표준화 역량</p> <p>국외대비 국내 기술개발 수준</p> <p>정책 부합성</p> <p>국제표준화 국내 기여도</p> <p>시장/기술적 파급효과</p> <p>IPR 확보 가능성</p>		표준화 기구/ 단체	국내	TTA CPS PG, 사물인터넷융합 포럼
	국제	IEC TC65 WG10, ISA 99			
	국내 참여 업체/ 기관	NSR, KISA, 순천향대, 건국대, NNSP, 온시큐리티			
기술 개발 단계	국내	□기초연구→□실험→■시작품→□제품화→□사업화		기술 수준	70% (선도국가대비)
	국외	□기초연구→□실험→□시작품→□제품화→■사업화			
	선도국가/ 기업	미국/GE, Rockwell 유럽/Philips, Siemens, ABB			
표준화 단계	국내	■과제기획→□과제승인→□개발→□검토→□표준채택		표준 수준	70% (선도국가대비)
	국제	□과제기획→□과제승인→□개발→□검토→■표준채택			
	선도국가/ 기업	미국/GE, Rockwell 유럽/Philips, Siemens, ABB			
<p>- Trace Tracking : 전략적수용(Ver.2019 신규)</p> <p>2017년 초부터 유럽 특히 독일을 중심으로 스마트공장 국제표준안을 제안하여 주도하고 있으며, 미국이 관련 분야 우월성을 확보하기 위해 적극적으로 나서고 있으며, 한국이 틈새 분야에 대한 표준 작성과 더불어서 관련된 요소기술을 파악하여 특허화 함으로써 시장 선점의 기회를 갖도록 함</p>					



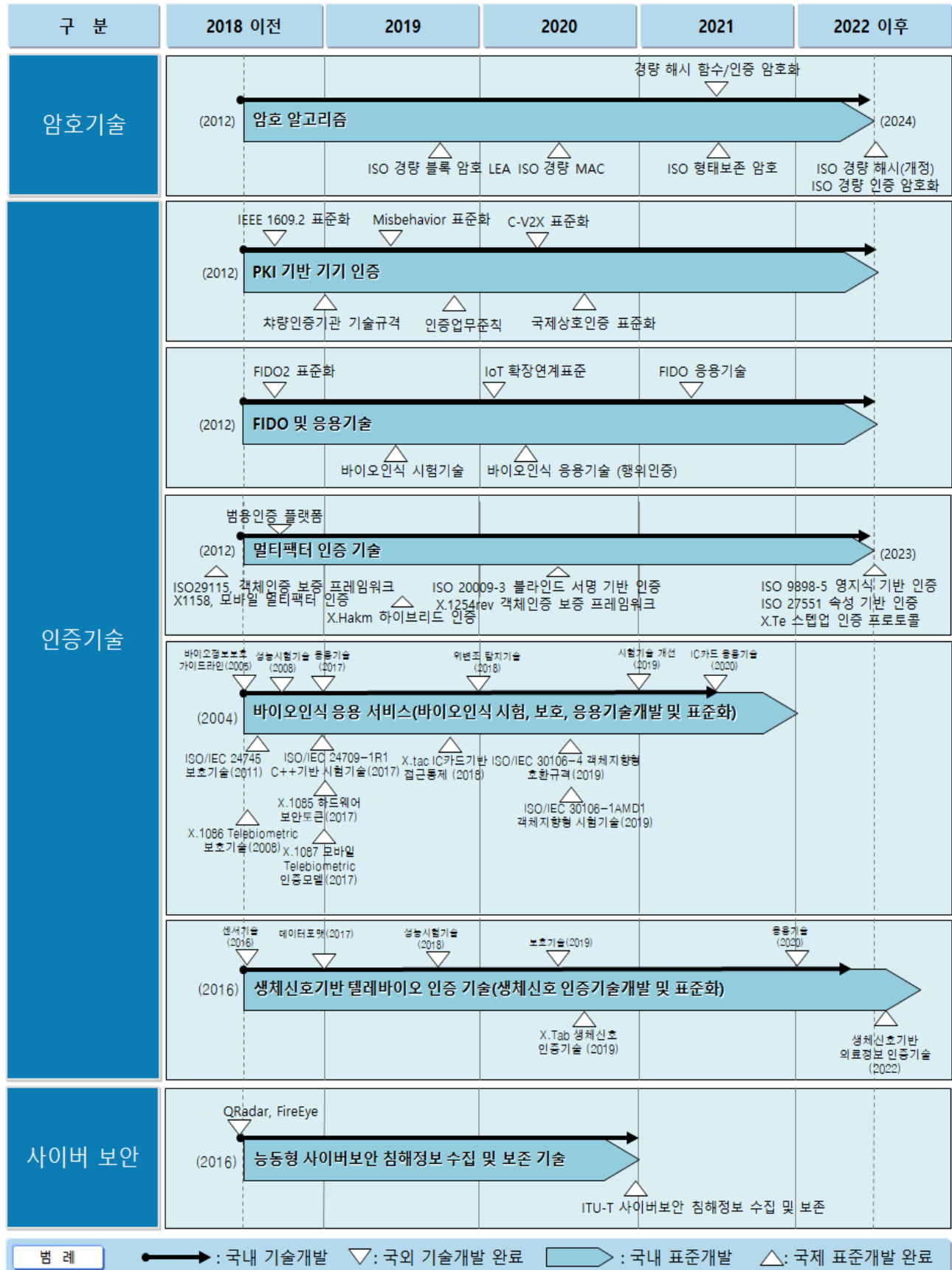
(전략적수용 | 병행) 중소기업용 스마트공장 보안 관리 기술

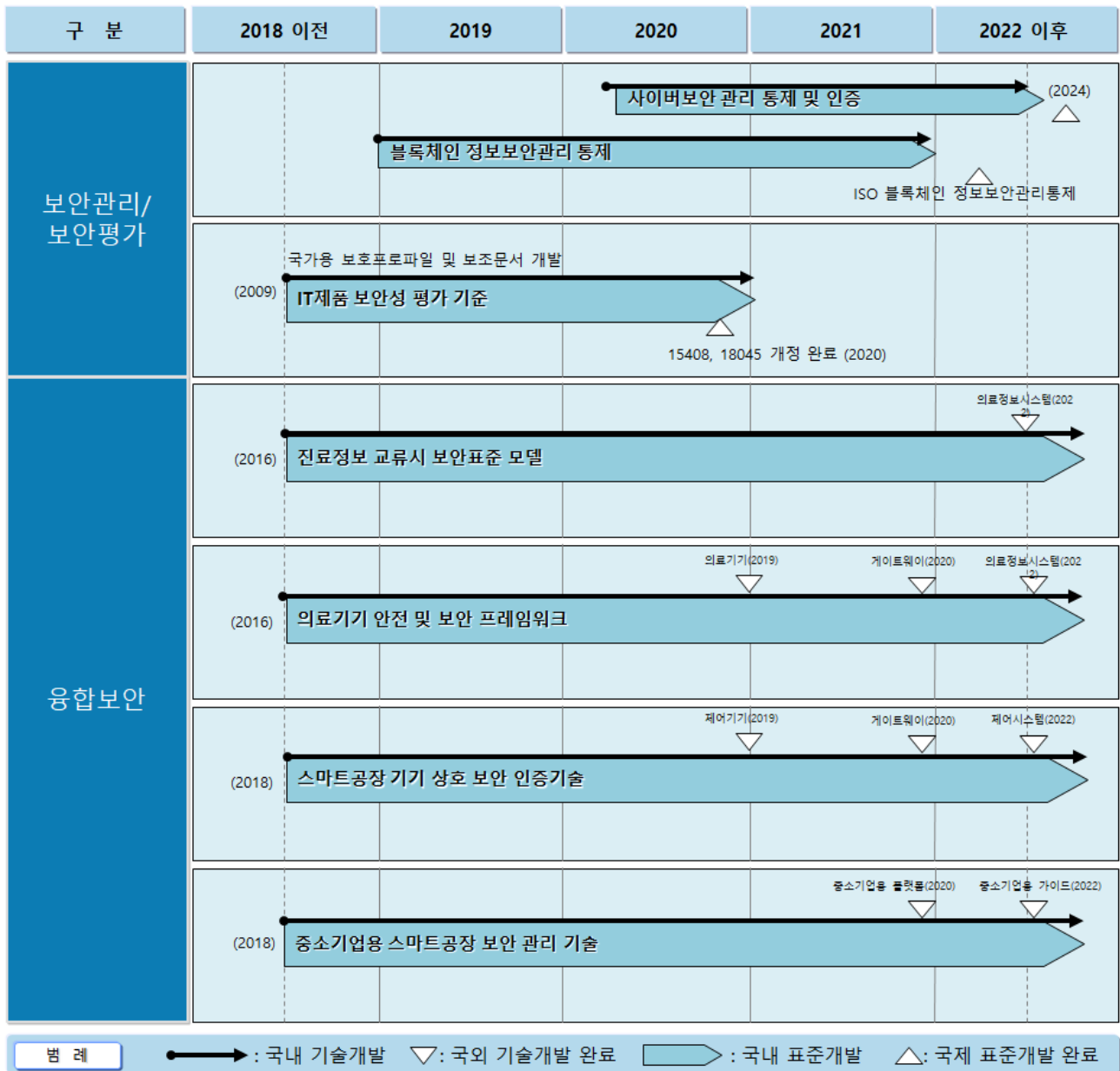
전략적 중요도 / 국내 역량	<p>국외대비 국내 표준화 역량</p> <p>국외대비 국내 기술개발 수준</p> <p>정책 부합성</p> <p>국제표준화 국내 기여도</p> <p>시장/기술적 파급효과</p> <p>IPR 확보 가능성</p>		표준화 기구/ 단체	국내	TTA CPS PG, 사물인터넷융합 포럼
	국제	IEC TC65 WG10, ISA 99			
	국내 참여 업체/ 기관	NSR, KISA, 순천향대, 건국대, NNSP, 온시큐리티			
기술 개발 단계	국내	□기초연구→□실험→■시작품→□제품화→□사업화		기술 수준	70% (선도국가대비)
	국외	□기초연구→□실험→□시작품→□제품화→■사업화			
	선도국가/ 기업	미국/GE, Rockwell 유럽/Philips, Siemens, ABB			
표준화 단계	국내	■과제기획→□과제승인→□개발→□검토→□표준채택		표준 수준	70% (선도국가대비)
	국제	□과제기획→□과제승인→□개발→□검토→■표준채택			
	선도국가/ 기업	미국/GE, Rockwell 유럽/Philips, Siemens, ABB			
<p>- Trace Tracking : 전략적수용(Ver.2019 신규)</p> <p>2017년 초부터 유럽 특히 독일을 중심으로 스마트공장 국제표준안을 제안하여 주도하고 있으며, 미국이 관련 분야 우월성을 확보하기 위해 적극적으로 나서고 있으며, 한국이 틈새 분야에 대한 표준 작성과 더불어서 관련된 요소기술을 파악하여 특허화 함으로써 시장 선점의 기회를 갖도록 함</p>					



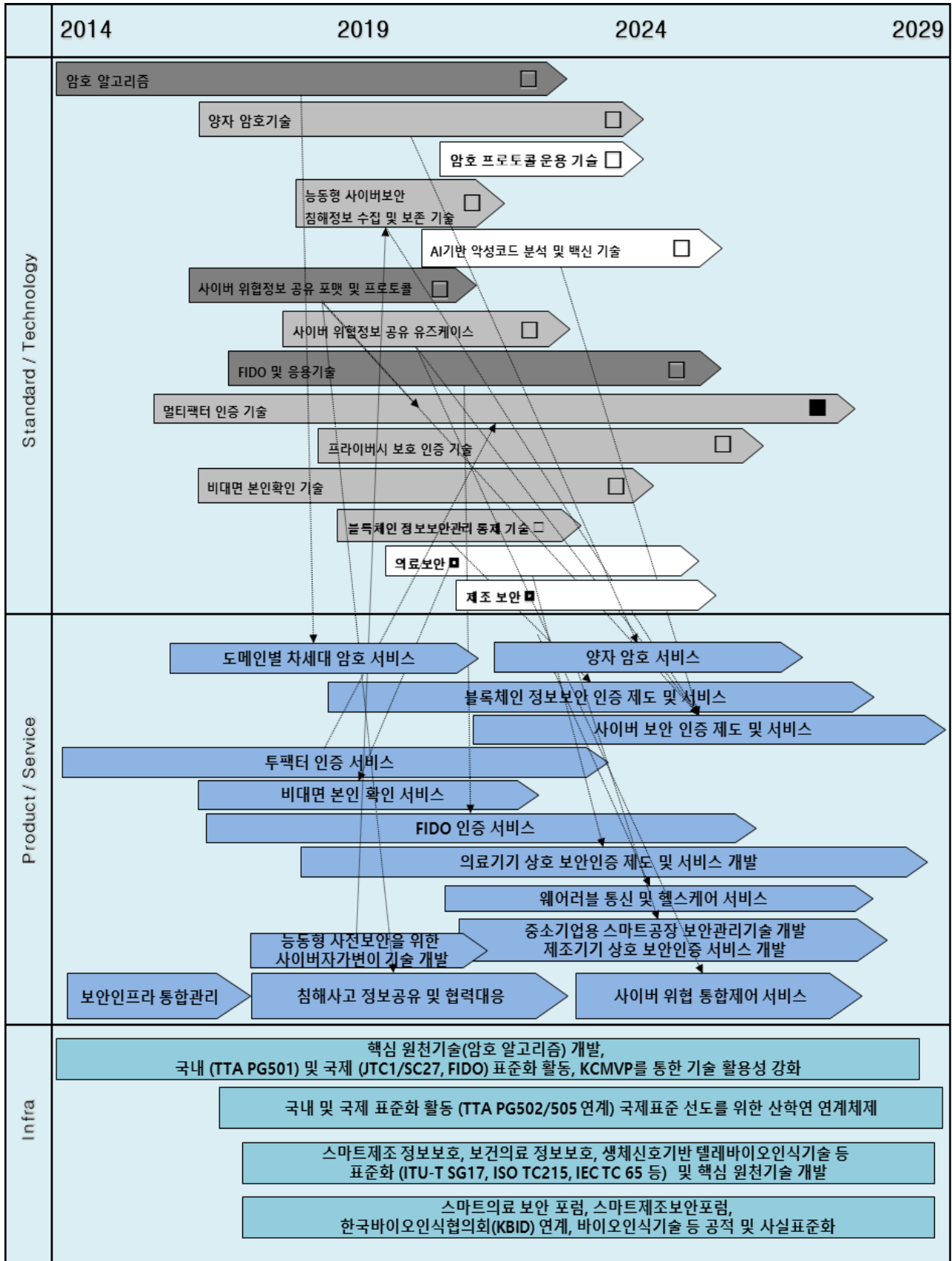
3.3. 중기(3개년) 및 장기(10개년) 표준화 계획

○ 중기(2019~2021) 표준화 계획





○ 장기(~2029) 표준화 계획



범례

기술개발수준

: 국내성숙기술

: 국내개발진행기술

: 국내개발미비기술

연구개발전략

■ : 기초연구

□ : 실용화 개발

■ : 국제공동연구

回 : 기술도입

[작성위원]

구분	소속	성명	직위	국내외 표준화활동
총괄	IITP	이재학	PM	▶ 과기정통부 정보보호 CP
분과장	NSR	권대성	센터장	▶ JTC1 SC27 전문가 ▶ JTC1 SC27 전문위원, 국가표준(KS) 정보보호 기술심의회 위원
위원	ETRI	김승현	선임	▶ TTA 개인정보보호/ID관리, 블록체인 보안(PG502) 위원
위원	KISA	김인섭	책임	▶ 차세대보안 표준화
위원	KISA	김재성	수석	▶ ITU-T SG17 에디터, JTC1 SC37 에디터 ▶ 바이오인식(PG505) 의장, 정보보호(TC5) 위원
위원	한국정보인증	김재중	상무	▶ 암호포럼, 사물인터넷융합포럼 위원
위원	ETRI	김종현	책임	▶ ITU-T SG17 에디터 ▶ TTA 사이버보안(PG503) 부의장
위원	카카오 모빌리티	김창오	팀장	▶ ITU-T SG17 Q3 에디터, ITU-T SG17 Q5 부리포처
위원	ETRI	나재훈	실장	▶ ITU-T SG17 WP4 부의장, Q7/17 라포처 ▶ TTA 응용보안/평가인증(PG504) 의장
위원	국가보안기술 연구소(NSR)	박제홍	선임	▶ TTA PG501 부의장
위원	TCA 서비스	오경희	대표	▶ JTC1 SC27 전문가, ITU-T SG17 Q14 라포처 ▶ 표준회의 위원, KS 정보기술 기술심의회 위원, SC27 전문위원 등
위원	원스	이수현	팀장	▶ JTC1 SC27 WG3 Co-Editor ▶ SC27 전문위원, TTA PG504/WG5041(정보보안 평가 및 검증)위원
위원	ETRI	이주영	책임	▶ 사이버보안 프로젝트그룹(PG503) 위원
위원	슈프리마	전동훈	수석	▶ TTA PG505 부의장
위원	ETRI	진승현	본부장	▶ ITU-T SG17 위원
위원	건국대	한근희	교수	▶ ISO TC215 위원, 스마트헬스표준포럼 위원, ▶ TTA PG505 위원
위원	경인여대	한승진	교수	▶ TTA PG505 간사
위원	글로벌피디	홍동표	대표	▶ FIDO한국워킹그룹 수석부회장
특허분석	KISTA	김병년	선임	▶ 차세대보안 특허분석
TTA PG담당	TTA	박수정	선임	▶ TTA 개인정보보호/ID관리, 블록체인 보안 PG(PG502) 담당
간사	TTA	오정엽	선임	▶ 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 NP 27002:2013, "Code of practice for information security controls",
<https://www.iso.org/standard/75652.html?browse=tc>
13. ISO/IEC PDTS 27008 Information technology -- Security techniques -- Guidelines for the assessment of information security controls,
<https://www.iso.org/standard/67397.html?browse=tc>
14. ISO/IEC CD 27009 Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 - Requirements,
<https://www.iso.org/standard/73907.html?browse=tc>
15. ISO/IEC CD 27552 Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management - Requirements,
<https://www.iso.org/standard/71670.html?browse=tc>
16. NIST, NISTIR 8197 Criticality Analysis Process Model: Prioritizing Systems and Components, <https://csrc.nist.gov/publications/detail/nistir/8179/final>
17. NIST, SP 800-171A Assessing Security Requirements for Controlled Unclassified Information, <https://csrc.nist.gov/publications/detail/sp/800-171a/final>
18. NIST, SP 800-171 Rev.1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,
<https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final>
19. NIST 800-16 "Information Technology Security Training Requirements:A Role- and Performance-Based Model"
20. NIST 800-50 "Building an Information Technology Security Awareness and Training Program"
21. 국가기술표준원, "2017 표준기반 R&D로드맵", 2017년 5월
22. 국가기술표준원, "스마트공장 기술 및 표준화 동향", 2015년 9월
23. FIDO Alliance, Universal Authentication Framework v1.1, 2017.2
24. W3C, Web Authentication: An API for accessing Public Key Credentials Level 1, 2018.3

25. ISO/IEC PDAM 11770-4/AMD 1 Information technology – Security techniques – Key management – Part 4: Key establishment mechanisms based on weak secrets – Amendment 1
26. ITU-T X.hakm Guidelines on hybrid authentication and key management mechanisms in client-server model(Draft Recommendation)
27. TTAK.KO-12.0313, 금융 서비스에 신뢰 등급이 가능한 인증 등급, 2017년 12월
28. ISO/IEC 29100:2011, Information Technology -- Security techniques – Privacy Framework”, 2011.12
29. NIST, De-identification of Personally Identifiable Information NSTR 8053, 2015.10
30. NIST, De-identification Government Datasets, 2016.12
31. ITU-T X.f dip, Framework of de-identification processing service for telecommunication server providers, TD-2997, 2016.08.29.
32. 한국산업인력공단, 정보보호관리·운영, 2017, <http://ncs.go.kr>
33. 김재성, “텔레바이오인식기반 비대면 인증기술 표준화 동향,” 정보보호학회지, 제25권, 제4호, August, 2015.
34. 김재성, 생체인식시스템 보안성 평가 및 표준적합성 시험기술, 인하대학교 공학박사 학위논문, August, 2005.
35. 박광석, “생체신호와 개인인증,” KISA 표준연구회 연구보고서, December, 2014.
36. 박광석, “국내외 생체신호 개인식별 기술분석 및 연구용 DB 구축”, KISA 용역과제 연구보고서, January, 2016.
37. 김재성, “바이오인식기술 표준화 현황 및 발전전망”, TTA 저널, June, 2015.
38. 김재성, “모바일 생체신호 인증기술 특허현황 분석보고서”, KISA 표준연구회 연구보고서, December, 2015.
39. 과기정통부 정보통신기술진흥센터, “스마트 융합보안서비스를 위한 텔레바이오인식기술 표준개발 2017년도 연구보고서,” 한국인터넷진흥원, March, 2018.
40. Jason Kim, Draft Recommendation of ITU-T SG17 X.1087 : A guideline to technical and operational countermeasures for telebiometric applications using mobile devices, March. 2017.
41. Jason Kim, Myung-Geun Chun, ISO/IEC DIS 17922 & Draft Recommendation of ITU-T SG17 X.1085 : Telebiometric authentication framework using biometric hardware security module, March. 2017.
42. Jason Kim, 3rd revised text of draft Recommendation for X.tab, Telebiometric Authentication using Biosignals, ITU-T SG17 Q.9, Match., 2018.
43. ISO/IEC FDIS 30107-1, Biometricss presentation attack detection-Part1:Framework, January. 2016.
44. ISO/IEC 24709-1R1, Conformance test for BioAPII -- Part 1: Test methods and procedures, December. 2017.
45. ISO/IEC DAM 30106-1AMD1, Object oriented BioAPI -- Part 1: Architecture-Amendment1: Additional specifications and conformance statements , January. 2018.

[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
ISMS	Information Security Management System
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
MTD	Moving Target Defense
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
PIMS	Privacy Information Management System
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

TTA는 국내외 ICT분야의 기술동향 및 표준 관련 정보를 보급하고 있으며, ICT표준화 대상의 발굴과 제정에서부터 시험인증에 이르는 One-Stop 서비스를 제공함으로써 ICT 표준화 및 4차 산업혁명을 주도하고 있습니다. 지식기반사회의 산업계 일선에서 활동하시는 귀사(소, 원, 교, 회)의 관심과 적극적인 참여를 요청 드립니다.



TTA 사업참가 (회원가입) 안내

01 사업참가자의 종류 및 분담금

사업참가자 종류	활동범위	분담금	표준총회 의결권
정회원사	TTA표준화위원회의 모든 표준화활동에 참여	2,850,000원(1구좌) 이상	1구좌당 1표
준회원사	TTA표준화위원회의 1개 특정부문 표준화활동(프로젝트 그룹)에만 참여	1,425,000원(0.5구좌)	없음
협력회원사	TTA표준화위원회의 모든 표준화활동에 참여	면제	1표

- ※ 협력회원사는 협회가 필요성을 인정하는 기관, 단체, 상호 회비면제 등이 가능한 동일기관으로 구분
- ※ 의결권은 표준의 제·개정 등의 중요사항 의결시 부여하며, 분담금 구좌수에 따른 가중투표를 실시
- ※ 정회원사의 1구좌 대상은 전전년도 매출액 5천억원 미만의 업체에만 해당
- ※ 준회원사는 전전년도 매출액이 100억원 미만의 업체에만 해당
- ※ 표준화위원회별 조직현황 및 활동내역은 “TTA홈페이지(www.tta.or.kr) → 표준화위원회” 참고

02 사업참가자의 혜택

내 용		정회원사	준회원사	협력회원사
정보통신표준화위원회 참여	정보통신표준총회	위원 1명	참관인 1명	위원 1명
	기술위원회	참가	참가권한 없음	참가
	프로젝트 그룹	참가	1개 프로젝트그룹 참가	참가
정보통신표준총회에서 TTA 표준 제·개정 및 표준화 중요사항 의결 시 투표권(분담금 구좌에 따른 가중투표제)		있음	없음	있음 (1표)
정보통신 단체표준(안) 의견수렴 권한		있음	있음 (해당부문만)	있음
자 료 보 급	TTA 표준	무료		
	TTA 간행물(TTA저널, ICT Standard Weekly), 번역출판물 및 기타	무료 또는 유료(할인)		
	세미나, 워크숍, 교육 등 유료행사	할인		
국제표준협력프로그램 (oneM2M, 3GPP, 3GPP2 등) 가입자격		있음		

1. 본 보고서는 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받은 과제(2017-0-00059, ICT 표준화 체계 및 전략 연구) 연구결과로 발간된 자료입니다.
2. 본 보고서의 무단 복제를 금하며, 내용을 인용할 시에는 반드시 정부(과학기술정보통신부) 정보통신방송표준개발지원사업의 연구결과임을 밝혀야 합니다.
 - ☐ 총괄책임자 : 구경철 (TTA 표준화본부장)
 - ☐ 사업책임자 : 김동호 (TTA 표준기획단장)
 - ☐ 표준기획단 : 강부미, 전철기, 심성구, 김정현, 김학훈, 고준호, 오정엽, 전보라, 정다운, 오지훈

ICT 표준화전략맵 Ver.2019

종합보고서 ④

2018년도 9월 28일 인쇄
2018년도 9월 28일 발행

발행소 : 한국정보통신기술협회
발행인 : 박재문
발간번호 : TTA-18061-SD
인쇄처 : (주)디자인여백플러스 (02-2672-1535)



한국정보통신기술협회
Telecommunications Technology Association

13591, 경기도 성남시 분당구 분당로 47
Tel : 031-780-9051, Fax : 031-724-0109
<http://www.tta.or.kr>