

통권 제342호

'데이터 보안' 시대의 10대 미래유망기술

KISTEP 기술예측센터 박창현 · 임현



‘데이터 보안’ 시대의 10대 미래유망기술

(KISTEP 10 Emerging Technologies in the Era of Data Security)

박창현·임현

Changhyun Park·Hyun Yim

I. 연구 배경

II. 연구 절차

III. 연구 결과

IV. 결론 및 시사점

[참고문헌]

I. Research Backgrounds

II. Research Process

III. Results

IV. Conclusion and Implications

[References]



한국과학기술기획평가원
Korea Institute of S&T Evaluation and Planning



요 약

■ 연구 배경

- 미래유망기술 선정을 통해 현재 우리 사회에서 중요하게 생각하는 이슈와 과학기술의 미래 방향성 제시 필요
- 미래이슈에 대응하기 위한 10대 유망기술을 선정하고, 유망기술별 심층분석 자료를 제공하여 미래모습을 구체화하고 활용성을 강화

■ 연구 절차

- 미래이슈 선정, 미래유망 후보기술 발굴, 미래유망기술 선정, 미래유망기술 심층 분석 등의 순으로 연구 수행
- 2022년 KISTEP 미래유망기술 주제(이슈)는 ‘데이터 보안 시대’로 선정되었으며, 문헌조사, 설문조사, 전문가 회의 등을 통해 10대 유망기술을 최종 선정
- 10대 유망기술별 기술 개요(기술명, 정의, 범위), 국내외 동향, 2030 미래 전망, 다른 미래유망기술과의 관계, 기술적 난제 및 정책제언 등 분석 수행
- 10대 유망기술별 논문·특허분석 기반 기술추세 및 수준 분석의 심층 분석을 수행

■ 연구 결과

- 국내외 미래 전망 동향 분석, 미래예측 전문가 대상 설문, 결과 활용성 등을 고려해 향후 10년 이내에 한국 사회에 커다란 변혁을 가져올 ‘데이터 보안 시대’를 주제로 삼아 미래유망기술을 발굴하고 심층분석을 수행
- 데이터의 보안 및 보호에 기여할 수 있는 정도가 큰 10대 미래유망기술 ① 자율 무인 이동체 활용을 위한 인프라 통합 보안 기술, ② 인공지능 기반 지능형 사이버 보안 관제 및 자동대응 기술, ③ 5G/6G 네트워크 보안 기술, ④ 제조(산업) 공급망 및 시스템 보안 취약점 진단 자동화 기술, ⑤ 프라이버시 강화 데이터 안전 활용을 위한 동형암호 등 지능형 암호 및 응용기술, ⑥ 메타버스 등 가상환경에서의 사용자 보호 및 보안 기술,

⑦ 양자시대의 절대적 데이터보안을 위한 양자암호기술, ⑧ 디지털 신기술 악용 사이버범죄 예방 및 추적기술, ⑨ 안전한 가상화 환경 활용을 위한 클라우드·엣지 보안 기술, ⑩ 안전한 디지털 경제 활용을 위한 암호화폐 신뢰성 보장 기술

■ 결론 및 시사점

- 미래유망기술은 5~10년 후 디지털전환 시대 데이터의 폭발적 증가에 따른 데이터의 보안 및 보호에 기여 가능함
- 각 미래유망기술은 타 기술과 상호보완적 관계를 나타내고 있어 데이터 보안 및 보호에 기여하기 위한 긍정적 시너지 효과를 창출할 것으로 기대
- 미래유망기술의 조속한 실현과 발전을 위해서는 법·제도 개선, 인력양성, 인프라 확보 노력이 필요
- (법·제도) 데이터 주권, 디지털 정보의 안전과 보안 등과 같은 법·제도 정비 및 양자암호기술 등과 같은 신기술 적용을 위한 평가검증 제도 마련
- (인프라 구축) 표준화, 인증을 위한 기반을 구축하고 해당 기술의 적용을 위한 산학연 협력체계 마련 및 테스트베드 구축
- (인력양성) 타산업과 데이터 보안 간의 융합적 인재 양성 및 산업 전반에 전문 인력 수급이 가능한 보안인력 양성 프로그램 추진
- 논문 및 특허 분석에 따르면, 10개 미래유망기술 대부분은 성장기에 있으며 영향력 측면에서는 미국과 유럽이 주도하고 있는 것으로 파악됨
- 논문 및 특허 분석에 따르면, 10개 미래유망기술의 논문영향력과 특허영향력에 따라 차별화된 기술확보전략이 필요하며, 상대적으로 논문영향력 및 특허영향력의 경쟁력이 낮은 보안 기술은 정부 차원의 지원이 중요하고 상대적으로 논문영향력 및 특허영향력의 경쟁력이 높은 보안 기술은 높은 기대성도가 예상되어 집중적 투자가 필요

※ 본 이슈페이퍼는 한국과학기술기획평가원에서 발간한 연구보고서 「2023년 KISTEP 미래유망기술 선정에 관한 연구」의 내용을 발전시킨 것으로 한국과학기술기획평가원의 공식 의견이 아닌 필자의 견해를 밝힙니다.



Abstract

■ Backgrounds

- It is necessary to present the future direction of science and technology through the selection of emerging technologies
- 10 emerging technologies have identified to prepare for future issues, and in-depth analysis data is provided for each technology to shape the future and strengthen usability

■ Research Process

- The research was carried out in the four main steps including identification of future issues, nomination of technology candidates, selection of 10 emerging technologies, and in-depth analysis of the selected technologies
- The future issue of KISTEP 10 emerging technologies is selected as “data security era” and 10 emerging technologies are selected after literature review, survey, and expert meeting
- 10 emerging technologies are analyzed in terms of technology introduction, technology trends, 2030 future outlook, relationship with other technologies, technological hurdle and policy proposal etc.
- 10 emerging technologies are deeply analyzed in terms of technology trends and technology levels according to paper and patents analysis

■ Results

- Under the issue of “data security era”, which will bring great change to Korean society in the next 10 years, emerging technologies have identified and in-depth analysis are conducted

- 10 emerging technologies along with data security era ① Infrastructure integration security technology for autonomous unmanned vehicles, ② Artificial intelligence-based intelligent cyber security control and automatic response technology, ③ 5G/6G network security technology, ④ Manufacturing (industry) supply chain and system security vulnerability diagnosis automation technology, ⑤ Functional encryption and application technology such as homomorphic encryption for privacy-enhancing data safety utilization, ⑥ User protection and security technology in virtual environments such as metabus, ⑦ Quantum cryptography technology for absolute data security in the quantum age, ⑧ Cybercrime prevention and tracking technology exploiting new digital technology, ⑨ Cloud/edge security technology for safe virtualization environment utilization, ⑩ Cryptocurrency reliability assurance technology for safe digital economy utilization

■ Conclusion and Implications

- Each emerging technology can contribute to the security and protection of data in accordance with the explosive increase in data in the era of digital transformation after 5 to 10 years
- Each emerging technology shows a complementary relationship with other technologies, which is expected to create positive synergy effects to contribute to data security era
- To promote the commercialization and development of emerging technologies, it is necessary to improve laws and regulations, to foster experts, and to build infrastructure
- (Laws and systems) Arrangement of laws and systems such as data sovereignty and safety and security of digital information, and establishment of evaluation and verification systems for application of new technologies such as quantum cryptography technology

- (Infrastructure construction) Establish a foundation for standardization and certification, prepare industry-academia-research cooperation systems and establish test beds for the application of the technology
- (Cultivation of human resources) Convergence of talents between other industries and data security, and promotion of security human resource training programs that can supply and demand specialized human resources throughout the industry
- According to the paper and patent analysis, most of the 10 emerging technologies are in the growth phase, and the US and Europe are leading the way in terms of influence
- According to the paper and patent analysis, a differentiated technology securing strategy is required according to the paper influence and patent influence of 10 emerging technologies. Government-level support is important for security technologies with relatively low competitiveness in paper influence and patent influence, and security technologies with relatively high competitiveness in paper influence and patent influence are expected to have high expected results, requiring intensive investment

I

연구 배경

- 사회 각 분야의 디지털 전환, 탄소중립 기반 에너지전환, 감염병 확산에 따른 비대면 시대 확산 등 급격한 기술변화 추세 및 기술패권경쟁 등으로 미래 대내외 환경의 불확실성 심화
 - 이러한 환경변화 속에서 지속적이고 주도적인 성장을 위해 우리나라도 미래사회 변화를 예측하고 과학기술 자체의 발전을 견인하는 독자적인 혁신(Breakthrough) 기술을 선점하여 확보하는 것이 필요
 - 혁신(Breakthrough) 기술 선정을 통해 현재 우리 사회에서 중요하게 생각하는 이슈와 과학기술의 미래 방향성 제시 필요
- 디지털 전환 시대에 데이터의 폭발적 증가에 따른 데이터의 보안 및 보호 관련 가능한 이슈를 전망하고, 이에 대응할 수 있는 기술을 발굴하는 것이 중요해지고 있음
 - 디지털 전환과 기술 융합이 가속화되며 새로운 유형의 보안 위협이 빠르게 확산되고 있고, 경제·정치·군사적 목적의 해킹 증가, 데이터 위변조 및 오남용 위험 증가
 - 디지털 전환의 핵심은 데이터 기술력으로 IDC(IT 시장분석 및 컨설팅 기관)에 따르면, 오는 2025년에는 163ZB의 데이터가 생성될 것으로 예상
- KISTEP은 2009년부터 매년 10대 유망기술을 선정
 - 미래유망기술 선정 연구는 기관 고유 업무로 기술 추격국에서 벗어나 기술 선도국으로 진입하는 단계에서 우리만의 미래유망기술 선정 및 제시에 의의가 있으며, KISTEP의 기술예측 역량 제고를 위해서도 지속적으로 연구가 필요
 - KISTEP의 10대 미래유망기술은 국내 주요 기관에서 발표하는 미래유망기술 중 인지도 및 활용도가 가장 높으며 미래사회 대비와 전략 수립에 활용
 - ※ 미래유망기술 정보는 '신규 R&D사업 및 과제 기획을 위한 아이디어 발굴'에 주로 활용되고 있으며 이를 위해 미래유망기술 정의 및 설명, 관련 사회·경제적 이슈, 기술 동향, 단계별 세부기술, 당면 과제 등 기술기획을 위한 내용 제시

II

연구 절차 및 세부내용

■ 2022년 KISTEP 미래유망기술 주제(이슈)는 ‘데이터 보안 시대’로 선정되었으며, 문헌조사, 설문조사, 전문가 회의 등을 통해 10대 유망기술을 최종 선정

- (STEP 1 - 미래이슈 선정) 국내외 문헌조사 및 전문가 의견수렴 등을 통해 미래 이슈 후보군을 발굴하고, 미래예측 전문가 및 KISTEP 정책고객 등을 대상으로 설문조사를 통해 최종 확정

[표 1] 미래이슈 선정을 위한 설문조사 평가지표

평가지표	설명
참신성	과거에 발표되었던 KISTEP 유망기술 주제와 중복되지 않는 정도
사회적 관심도 및 시의성	향후 10년 내 해당 주제에 대한 사회적 관심도 및 그로 인한 연구의 시의 적절성
파급효과의 크기	해당 주제가 경제·사회·문화·윤리·환경 등 여러 분야에 영향을 미치는 정도
과학기술과의 연관성	해당 주제와 관련하여 발생하는 새로운 수요 및 문제점 대응에 있어 과학기술이 기여할 수 있는 정도 ※ 과학기술 외 방안(규제, 정책, 외교 등)으로 해결될 수 있는 주제는 제외
결과의 활용 가능성	최종적으로 도출된 유망기술 목록이 미래사회 대비, 과학기술 전략 수립, R&D 사업 및 과제 기획을 위한 관련 아이디어 수집 등에 활용될 가능성

- (STEP 2 - 미래유망 후보기술군 발굴) 미래이슈 대응 관련 유망기술을 발굴하기 위해 국가과학기술 표준분류체계, ICT R&D 기술로드맵, 개인정보 보호·활용기술 R&D 로드맵 등의 데이터 보안 분야 기술분류체계를 기준으로 후보기술 도출
- (STEP 3 - 미래유망기술 선정) 후보기술별 미래예측 전문가 논의, 전문가 서면평가 등을 종합하여 최종 10대 유망기술 선정

[표 2] 미래유망기술 선정을 위한 평가지표

평가지표	설명
기술적 실현 가능성	해당 기술이 국내에서 10년 내 상용화 될 가능성
경제적 파급 효과	해당 기술의 구현으로 시장에서 예상되는 부가가치의 규모
데이터 보안 및 보호 기여도	해당 기술이 데이터 보안 및 보호에 기여할 수 있는 정도

- (STEP 4 - 미래유망기술 심층분석) 10대 유망기술별 기술 개요(기술명, 정의, 범위), 국내외 동향, 2030 미래 전망, 다른 미래유망기술과의 관계, 기술적 난제 및 정책제언 등 분석 수행

[표 3] 2023년 KISTEP 미래유망기술 연구절차

구분	세부 내용	방법
(1) 미래이슈 선정	미래이슈 후보 발굴	<ul style="list-style-type: none"> • 미래예측 보고서를 중심으로 미래이슈 관련 DB 구축 ※ 제6차 과학기술예측조사, 미래전략 2045, NIC Global Trends 2040, NISTEP S&T foresight, WEF Global Issue 등
	미래이슈 우선순위 평가	<ul style="list-style-type: none"> • 기술수준평가 전문가 및 KISTEP 정책고객을 대상으로 우선순위 평가 • 미래예측 전문가 및 KISTEP 내부 직원을 대상으로 우선순위 평가
(2) 미래유망 후보기술 발굴	미래수요에 대응 가능한 미래유망기술 후보기술 발굴	<ul style="list-style-type: none"> • 디지털전환 시대 데이터의 폭발적 증가에 따른 데이터의 보안 및 보호에 기여할 수 있는 기술로 범위 설정 • 국가과학기술 표준 분류체계, ICT R&D 기술로드맵, 개인정보 보호·활용기술 R&D 로드맵 등의 데이터 보안 분야 기술분류체계에서 후보군 발체 • 부문별 기술 전문가의 서면평가로 후보기술군을 조정하고 미래이슈와의 부합성 평가
	미래유망기술 선정	<ul style="list-style-type: none"> • 전문가 자문 및 내부연구진 토의를 통해 최종 10개 미래유망기술 선정
(4) 미래유망기술 분석	기술별 분석	<ul style="list-style-type: none"> • 기술 개요, 국내외 동향, 2030년 미래 활용 모습, 다른 미래유망기술과의 관계, 기술적 난제 및 정책제언 등 도출
(5) 미래유망기술 심층 분석	기술별 심층분석	<ul style="list-style-type: none"> • 논문·특허분석 기반 기술추세 및 수준 분석

III

연구 결과

1. 미래이슈 선정

■ 2023년 KISTEP 미래유망기술 주제(핵심 트렌드)를 선정하기 위해 다양한 문헌조사 실시

- 최근 발표된 국내외 미래전망보고서의 트렌드와 이슈, 제6회 과학기술 예측조사 보고서, 미래전략 2045, 일본 예측조사보고서('20) 등을 수집·분석하여 정치, 경제, 사회, 환경, 기술의 관점에서 미래사회 트렌드를 도출함
- (정치) 글로벌 밸류체인 변화, 자국중심주의 강화, 민주주의 위협, 기존 제도와 지배구조 불균형, 스마트 행정 실현, 결정적 분기점, 큰 정부의 귀환 등
- (경제) 온라인 경제의 주류화, 플랫폼 자본주의 확산, 디지털 재화 시장의 성장, Cashless 사회 도래, 디지털 사회의 일자리 변화, 디지털 제조기술 확산, 자원 고갈에 대비한 농어업·제조업·에너지 혁신, 서비스 무역, 플랫폼 영향력 확대, 구독 경제의 확산, 간접 체험 서비스 증가, 디지털 금융 활성화, 자동화의 확산, 황금 사각형 경제 구조로 전환, 고용시장의 변화와 불안정한 일자리 등
- (사회) 인구구조의 변화, 초연결 스마트시티의 가속, 원격근무 수요 증가, 메가시티, 메가리전, 지방 중소도시의 몰락, 사이버·데이터 안보, 인구변화, 초연결사회, 더 큰 도시화, 더 긴 건강 수명을 목표로, 홈루덴스 문화 확산, 위협 예방과 감시의 혼돈 등
- (환경) 기후변화, 재난재해, 환경오염의 위협, 미세먼지 등 대기오염, 탄소중립을 위한 에너지 전환, 온실가스 저감, 전기차 수요 확대, 수자원 확보와 공급 위기, 자원의 선순환, 자원 부족과 생물다양성 감소, 미세 플라스틱, 생활 방역의 일상화, 식물성 식품의 부상 등
- (기술) 우주 생활 시대, 극지 자원 및 항로 개발, 심해 자원 발굴, 스마트 소재, 스마트 생산, ICT를 혁신하는 전자·양자 디바이스, 서비스 로봇의 부상, 클라우드로의 전환 가속화, 3D 프린팅의 활용, 블록체인 등

■ 향후 10년 이내 주요 이슈로 부상할 가능성이 크며 최근 주요 사회 이슈와 연관성이 높은 4개 트렌드를 후보 주제(표 4)로 선정

- 그동안 KISTEP 10대 미래유망기술 주제로 선정되었던 트렌드는 되도록 제외하여 기존 연구와의 차별성을 확보
- 과학기술 전반의 흐름과 정책 동향에 대한 이해도가 높은 KISTEP 정책고객과 미래예측 전문가를 대상으로 선호도 조사 및 주제 추가 발굴

[표 4] 2023년 KISTEP 미래유망기술 후보 주제

후보 주제	설명
우주생활 시대를 준비하는 10대 미래유망기술	<ul style="list-style-type: none"> • 우주 생활권 실현 및 관련 소재·건축 산업의 형성과 발생 가능한 이슈를 전망하고, 이에 대응할 수 있는 기술을 발굴 - 관련 이슈(예) : <ul style="list-style-type: none"> • 미지의 영역 개척 및 우주 자원 발굴 • 생활권의 우주로의 확장 • 불멸의 호기심으로 신세계를 지향하는 탈공간 사회
데이터 보안시대를 준비하는 10대 미래유망기술	<ul style="list-style-type: none"> • 디지털 전환 시대에 데이터의 폭발적 증가에 따른 데이터의 보안 및 보호 관련 가능한 이슈를 전망하고, 이에 대응할 수 있는 기술을 발굴 - 관련 이슈(예) : <ul style="list-style-type: none"> • 사이버·데이터 안보 • 개인정보와 감시의 혼돈 • 보안성을 강화한 전자·양자 디바이스의 발달
제조 분야의 디지털 전환을 대비하는 10대 미래유망기술	<ul style="list-style-type: none"> • 다양한 분야에서 발생하고 있는 디지털 전환 중에 산업과 밀접한 제조 분야에 특화하여 발생 가능한 이슈를 전망하고, 이에 대응할 수 있는 기술을 발굴 - 관련 이슈(예) : <ul style="list-style-type: none"> • 디지털 제조기술 확산 • 인간의 신체적·지적 능력 보완·확장 • 최적화된 맞춤형 개인화 서비스의 확산
디지털 경제를 준비하는 10대 미래유망기술	<ul style="list-style-type: none"> • 디지털 재화, 디지털 금융 등 디지털에 기반하여 촉진되는 경제 및 사회활동으로 발생하는 다양한 이슈를 전망하고, 이에 대응하는 기술을 발굴 - 관련 이슈(예) : <ul style="list-style-type: none"> • 디지털 재화 시장의 성장 • 디지털 금융 활성화 • 온택트 경제의 부상

■ 미래유망기술 후보 주제에 대해 기술수준평가 전문가 및 KISTEP 정책고객 등을 대상으로 설문조사 수행

[표 5] 2023년 KISTEP 미래유망기술 후보 주제 설문조사 결과

평가지표	후보 주제			
	우주생활 시대	데이터 보안	제조 분야의 디지털전환	디지털 경제
참신성	5.15	4.79	4.91	4.87
관심도·시의성	4.52	5.76	5.32	5.52
파급효과	4.85	5.93	5.65	5.58
기술 연관성	6.00	5.70	5.61	5.02
결과 활용성	4.67	5.99	5.75	5.44
합계	5.04	5.63	5.45	5.29

※ 평가지표별 점수 : 1(매우 낮음) - 4(보통) - 7(매우 높음)

설문조사 결과를 바탕으로 ‘데이터 보안 시대’를 2023년 미래유망기술 주제로 선정

- 참신성 및 과학기술과의 연관성은 ‘우주생활 시대’가 가장 높았으나, 나머지 모든 평가지표에서 ‘데이터 보안 시대’가 1위를 차지

2. 10대 미래유망기술 후보군 도출 및 선정

디지털 전환 시대에 데이터의 폭발적 증가에 따른 데이터의 보안 및 보호 관련 가능한 이슈를 전망하고, 이에 대응할 수 있는 기술을 발굴하는 것이 중요해지고 있음

- 디지털 전환의 핵심은 데이터 기술력으로 IDC(IT 시장분석 및 컨설팅 기관)에 따르면, 오는 2025년에는 163ZB*의 데이터가 생성될 것으로 예상

* 제타바이트(Zettabyte, ZB)란 10의 21제곱 바이트인 데이터 자료량 단위

- 디지털 전환과 기술 융합이 가속화되며 새로운 유형의 보안 위협이 빠르게 확산되고 있고, 경제·정치·군사적 목적의 해킹 증가, 데이터 위변조 및 오남용 위험 증가

미래유망기술은 향후 10년 내 한국 사회에 커다란 변혁을 가져올 수 있는 이슈를 대상으로 하므로 디지털전환 시대 데이터의 폭발적 증가에 따른 데이터의 보안 및 보호에 기여할 수 있는 정도가 큰 기술을 선정코자 함

■ 후보군은 국가과학기술 표준분류체계, ICT R&D 기술로드맵, 개인정보 보호·활용기술 R&D 로드맵 등의 데이터 보안 분야 기술분류체계를 기준으로 발체

■ 상기 데이터 보안 및 보호 기술분류(안)을 바탕으로 전문가 서면 평가를 통해 10개 미래유망기술 선정

● 전문가 서면 평가로부터 얻어진 총 182개의 기술 중 추천 수, 평가지표 점수* 등을 검토

* 3개의 평가지표(기술적 실현 가능성, 경제적 파급효과, 데이터 보안 및 보호 기여도)

● 내부 전문가 논의를 통해 주제와의 부합성 및 파급효과가 큰 10개 기술을 선정

[표 6] 데이터 보안 및 보호에 기여할 10대 미래유망기술

연번	대분류	기술명	기술 개요
1	차세대 보안	자율 무인 이동체 활용을 위한 인프라 통합 보안 기술	자율 무인 이동체 활용을 위한 인프라 통합 보안 기술은 다양한 사회 인프라 정보 시스템과 통합 운영을 위해 필요한 통합 보안 기술
2	차세대 보안	인공지능 기반 지능형 사이버 보안 관제 및 자동대응 기술	AI 기계해커에 의한 정밀·자동화된 사이버공격으로부터 국가·사회 인프라와 기업망의 침해사고를 AI 기술을 이용하여 위협 예측·탐지·분석·대응 업무를 자동화하기 위한 기술
3	차세대 보안	5G/6G 네트워크 보안 기술	5G 및 미래 6G 이동통신 환경에서 다양화·지능화·고도화 되는 사이버 위협을 분석·탐지·대응하기 위한 기술
4	차세대 보안	제조(산업) 공급망 및 시스템 보안 취약점 진단 자동화 기술	하드웨어 및 소프트웨어 솔루션 공급망(유통망 포함), 어플리케이션 등 IT 시스템에 내재된 보안취약점을 AI 기술을 활용하여 자동으로 탐지하고 보안 위협에 자율적으로 대응하는 기술
5	차세대 보안	프라이버시 강화 데이터 안전 활용을 위한 동형암호 등 기능형 암호 및 응용기술	데이터 경제 시대의 도래로 데이터의 중요 정보를 보호 하면서 데이터 활용성을 높이고, 데이터 활용 전주기에 대해 프라이버시 강화와 안전한 데이터 활용을 위한 암호 및 응용 기술
6	차세대 보안	메타버스 등 가상환경에서의 사용자 보호 및 보안 기술	가상과 현실이 융합된 공간에서 사람·사물이 상호작용 하며 경제·사회·문화적 가치를 창출하는 세계인 메타 버스에서 사용자·인프라·서비스를 보호하는 기술
7	양자 정보통신	양자시대의 절대적 데이터보안을 위한 양자암호기술	양자의 불확정성, 복제불가능성원리 등을 이용한 암호 기술로, 양자컴퓨터 등 컴퓨팅 발전 및 컴퓨팅에 기반한 해독 방법에 영향을 받는 현대암호와 달리, 절대적 안전성 보장 암호기술
8	차세대 보안	디지털 신기술 악용 사이버범죄 예방 및 추적기술	디지털 신기술(5G, AI, 클라우드 등)이 확산되고 있는 디지털 대전환 환경에서 고도화·지능화된 사이버범죄에 대응하기 위한 사이버위협 인텔리전스 기술

연번	대분류	기술명	기술 개요
9	보안기술	안전한 가상화 환경 활용을 위한 클라우드·엣지 보안 기술	클라우드 기술은 구성 가능한 컴퓨팅 자원의 공유 집합에 대해 어디서나 편리하게 사용자의 요구에 따라 네트워크를 통한 접근 및 사용을 가능하게 하는 모델
10	차세대 보안	안전한 디지털 경제 활용을 위한 암호화폐 신뢰성 보장 기술	블록체인 기술, 분산원장 기술 등 디지털 화폐 또는 자산의 발행 또는 거래와 연관되어 신뢰성을 부여할 수 있는 기술

3. 10대 미래유망기술 심층 분석

1) 자율 무인 이동체 활용을 위한 인프라 통합 보안 기술

■ (정의) 자율 무인 이동체 활용을 위한 인프라 통합 보안 기술은 다양한 사회 인프라 정보 시스템과 통합 운영을 위해 필요한 통합 보안 기술

■ (범위) 자율 무인 이동체 환경 속 클라우드 보안, 이더넷 기반 자율 무인 이동체 통신망 보안, 제어 신호 통신 보안, 에너지 교환 정보 보안, 안전 위협 정보 보안

● (자율 무인 이동체 환경 속 클라우드 보안) 자율 무인 이동체 환경 속 클라우드 보안은 이동체 환경에서 클라우드 기반 이벤트 데이터 레코더의 취약점, 보안 요구 사항 및 사용 사례를 다룸

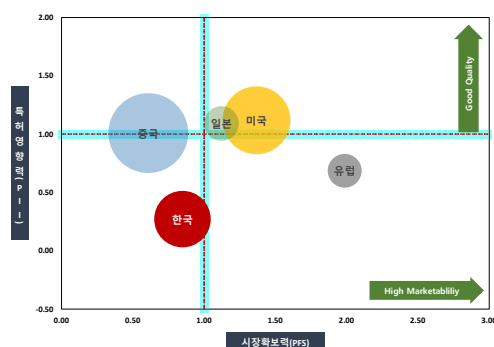
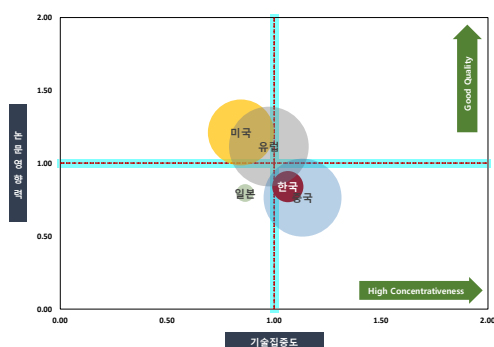
● (이더넷 기반 자율 무인 이동체 통신망 보안) 이더넷(예 : DoIP 또는 XCP)을 통한 IP 기반 연결을 가능하게 하는 표준 정의 프로토콜은 외부 환경과 자율 무인 이동체간의 통신에 사용되고 있음

■ (필요성) 디지털 전환(Digital Transformation)이 빠르게 일어나면서 자율 무인 이동체가 독립적 정보 장치에서 협업과 환경과의 정보 에코시스템을 이루면서 활발한 정보교류가 발생하고 있어 이에 대한 보안의 필요성이 지속적으로 늘어나고 있음

■ (국내외 동향) 전 세계적으로 자율주행 시장을 선점하기 위해 주요 정책 및 로드맵 발표 중이고 관련 보안 이슈도 함께 논의되고 있음

● (한국) 정부는 2019년 10월 미래자동차 산업 발전전략에서 2027년까지 완전 자율주행 도로 세계 최초 상용화를 목표로 자율주행 시장 선점할 계획

- (미국) 미국 ‘2020 Automated Vehicle 4.0’에서는 자율주행차 기술 진흥을 위한 첨단제조, 인공지능, STEM 교육 및 인력 배양과, 협업과제인 기초연구, 인프라, 규제, 세제, 지적재산권, 환경 등 광범위한 분야에 대한 방향성 제시
- (유럽) ETSC(유럽교통안전위원회), ERTRAC(유럽도로교통연구자문위원회) 중심으로 표준화 추진하고 있으며 ERTRAC는 공동의 로드맵(Automated Driving Roadmap)을 마련
- (2030 전망) 드론과 자율 자동차 활용한 자율 이동체 계획을 진행 중이며 2030년을 완전주행 자동차 달성 계획하고 있어 자동차 중심의 자율 이동체 운영이 이루어질 예정
- 스마트 시트 계획 등이 실용화 단계에 이르러 사회 인프라 정보망이 자율 이동체와 연결
- (다른 미래유망기술과의 관계) 클라우드·엣지 보안 기술과 인공지능 기반 지능형 사이버 보안 관제 및 자동대응 기술과 상호보완적 관계
- 안전한 가상화 환경 활용을 위한 클라우드·엣지 보안 기술은 자율 무인 이동체 환경 속 클라우드 보안과 밀접한 관계를 가지며 공통의 보안 이슈 공유
- 인공지능 기반 지능형 사이버 보안 관제 및 자동대응 기술은 자율 무인 이동체의 자율주행을 모니터링하고 대응하는데 필수적인 기술
- (논문·특허 심층분석) 한국, 미국, 일본, 유럽(영국 포함 28개국), 중국의 최근 12년 논문 및 특허 분석 결과, 기술집중도¹⁾는 중국이 가장 높고 시장확보력²⁾은 유럽이 가장 높은 것으로 조사됨

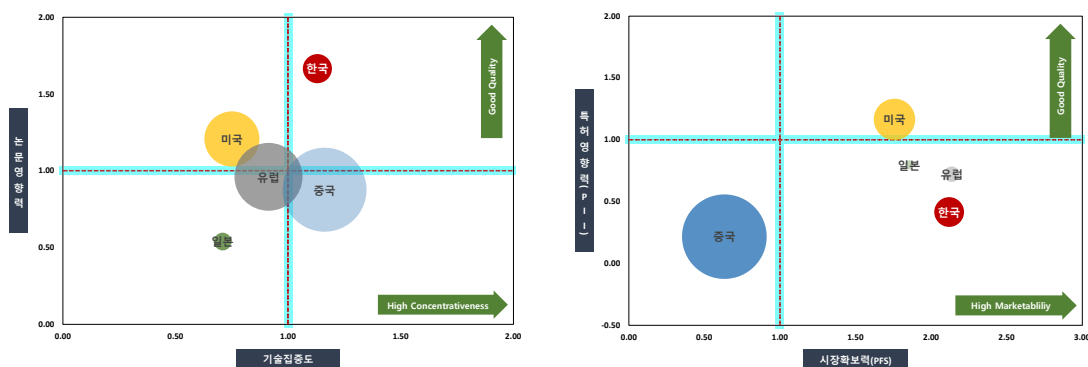


1) 기술집중도 : (최근 3년 중요논문 건수) / (중요논문 건수) * 100 (%), 중요논문 : CITATION 10 이상인 논문
 2) 외국인에 의한 특허 출원 증가율

2) 인공지능 기반 지능형 사이버 보안 관제 및 자동대응 기술

- (정의) AI 보편화에 따라 AI 기계해커에 의한 정밀·자동화된 사이버공격으로부터 국가·사회 인프라와 기업망의 침해사고를 AI 기술을 이용하여 위협 예측·탐지·분석·대응 업무를 자동화하기 위한 기술
- (범위) AI기반 지능형 사이버보안관제/자동대응기술의 주요 범위는 보안오케스트레이션 및 자동화 기술(SOA), 보안사고대응기술(SIRP), 그리고 위협인텔리전스기술(TIP)로 분류하고 있음
 - (SOA, Security Orchestration and Automation) 기술은 이기종의 보안 솔루션을 단일 플랫폼으로 통합하고 각 장비별 보안 워크플로우를 표준화하여 반복적인 보안 업무를 자동화 기술
 - (SIRP, Security Incident Response Platforms) 술은 보안사고 발생 시 해킹사고 유형별로 사전에 정의된 보안위협대응 레벨에 따라 자동으로 분류하고 의사결정을 지원하는 기술
 - (TIP, Threat Intelligence Platforms) 기술은 조직에서 발생하는 보안 위협의 분석 업무를 지원하기 위해 내외부의 위협 데이터를 실시간으로 수집, 상관 분석해 주는 기능
- (필요성) 사람 중심의 단순 반복 보안 관제 업무를 효율화하고 다양한 보안 이벤트를 신속 정확하게 분석하며 대응 프로세스를 자동화하는 기술로서 진화 필요
- (국내외 동향) 국내에서는 기술 확보를 위한 국가 R&D 프로젝트 및 예산 투자 중이며, 주요국에서 행정명령 발표 및 사이버보안역량을 강화 중
 - (한국) 과학기술정보통신부와 IITP는 지능형보안관제 자동화를 위한 중장기 기술개발 로드맵을 수립하고 관련 기술 확보를 위한 국가 R&D 프로젝트 및 예산 투자 중
 - (미국) 2021년 바이든 행정부는 미국 연방정부의 사이버공격대응역량강화를 위해 ‘국가 사이버보안 강화를 위한 행정명령 (Executive Order on Improving the Nation’s Cybersecurity)’ 발표
 - (유럽) EU 집행위는 유럽의 디지털 10년(Digital Decade)을 위한 디지털 대전환 정책으로 디지털권리, 사이버보안법, 사이버보안전략 수립을 통해 범 EU 차원의 사이버보안역량을 강화하는 추세

- (2030 전망) 대면 서비스의 성장, 데이터 경제 등장, 최첨단 기술과 융합한 무인점포 등 새로운 시장이 형성되고, AI 공격 대비 자동화된 보안관제 시장도 연평균 15.6% ~ 20.4% 고속 성장할 것으로 전망
 - 세계 보안 오케스트레이션 자동 대응 기술 시장은 2021년 11.6억 달러(한화 1.2조 원)에서 2027년 27.7억 달러(한화 3조 원)로, 연평균 15.6% 성장할 것으로 전망되고 있음(Markets and Markets, 2019)
- (다른 미래유망기술과의 관계) 타 미래유망기술 분야에서 자동화 및 인텔리전스 관련된 보안 요소 기술로 활용되고 연관성이 높음
 - AI기반 사이버 보안관제 및 자동대응기술은 조직의 보안관제센터, 보안관, 보안요소기술의 인텔리전스와 자동화와 관련된 요소기술로 타 분야에서 자동화 및 인텔리전스 관련된 요소 기술로 활용 가능
- (논문·특허 심층분석) 한국, 미국, 일본, 유럽(영국 포함 28개국), 중국의 최근 12년 논문 및 특허 분석 결과, 기술집중도³⁾는 중국이 가장 높고 시장확보력⁴⁾은 유럽이 가장 높은 것으로 조사됨



3) 기술집중도 : (최근 3년 중요논문 건수) / (중요논문 건수) * 100 (%), 중요논문 : CITATION 10 이상인 논문
 4) 외국인에 의한 특허 출원 증가율

3) 5G/6G 네트워크 보안 기술

- (정의) 5G/6G 네트워크 보안 기술은 5G 및 미래 6G 이동통신 환경에서 다양화·지능화·고도화 되는 사이버 위협을 분석·탐지·대응하기 위한 기술
- (범위) 무선 접속망 취약성 분석 기술, Open RAN 보안 기술, MEC(Multi-access Edge Computing) 보안 기술, 지능형 보안위협 분석 및 관제 기술, 양자암호통신 기술, 특화망 보안 기술 등으로 분류
 - (무선 접속망 취약성 분석 기술) 센서, 웨어러블 장치, 자동차, 드론, 로봇 등 다양한 기기의 초연결과 비지상 네트워크 등 접속기술의 다변화에 따른 잠재적 보안 취약점을 분석하고 이에 대응하는 기술
 - (Open RAN 보안 기술) Software-Defined RAN 및 기지국의 무선장치와 분산장치 간 인터페이스 표준화를 위한 개방형 5G 프론트홀 등 5G/6G 무선 인프라의 지능화, 가상화, 개방화에 따른 잠재적 보안 취약점을 분석하고 대응하는 기술
- (필요성) 5G의 초연결(mMTC) ·초저지연(uRLLC)·초고속(eMBB)의 요구사항을 충족하기 위해서, 전 산업 영역에 6G 기반의 융합 서비스를 안정적으로 적용·고도화하기 위해 6G 기술 규격 표준화 단계부터 보안 강화를 위한 기반기술 개발이 필요함
- (국내외 동향) 국내에서는 5G 및 6G 상용화 기술 개발 중이며 해외에서도 기술 확보를 위한 정책적 노력이 지속되고 있음
 - (한국) 국내 이동통신사업자와 한국전자통신연구원을 중심으로 Open RAN 기반 개방형 5G 프론트홀 인터페이스 표준화를 추진하고 있음
 - (미국) 2017년부터 THz 고주파수 대역 기술 확보를 위한 국방부 산하 연구기관인 방위고등연구계획국에서 DARPA 프로젝트를 통해 장기적인 6G R&D 수행 중임
 - (일본) 5G 상용화 이후 망 구축이 느린 점을 만회하기 위해 제 4 이동통신사업자를 중심으로 상용망에 Open RAN 기술을 초기부터 적용하는 것을 추진 중

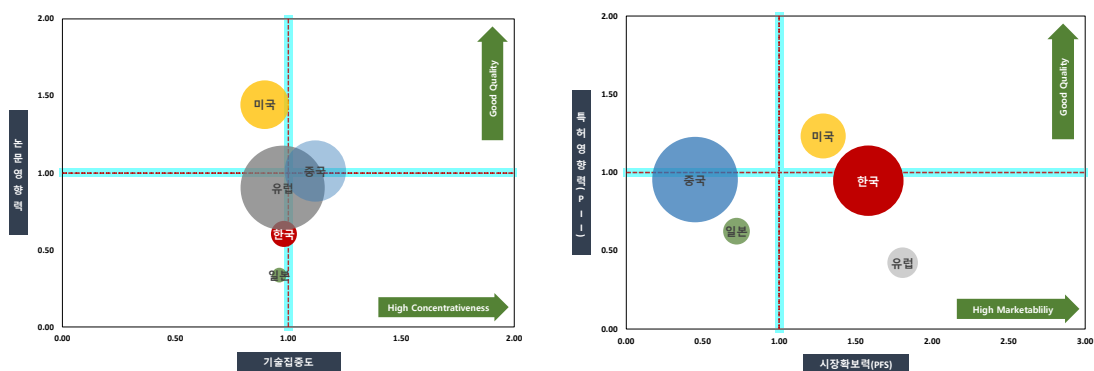
■ (2030 전망) 2028년~2030년경 3GPP의 6G 표준 규격이 제정될 것으로 예상되며, 이에 따른 보안취약점에 대한 연구가 활발히 진행될 것으로 전망됨

- 단말의 고도화로 인해 단말에서 이동통신 네트워크 전 영역에서의 인공지능 기반 지능화 프로세스가 보편화되고, 이에 따른 데이터 보호 및 보안위협 대응 협업 기술이 활성화될 전망이다

■ (다른 미래유망기술과의 관계) 지능형 사이버 보안 관제 및 자동대응 기술, 데이터보안을 위한 양자암호기술, 클라우드·엣지 보안 기술과 유기적으로 연계

- 5G/6G 네트워크 보안 기술은 지능형 사이버 보안 관제 및 자동대응 기술, 데이터보안을 위한 양자암호기술, 클라우드·엣지 보안 기술과 유기적으로 관련성이 높으며 상호 시너지를 높일 수 있을 것으로 기대됨

■ (논문·특허 심층분석) 한국, 미국, 일본, 유럽(영국 포함 28개국), 중국의 최근 12년 논문 및 특허 분석 결과, 기술집중도⁵⁾는 중국이 가장 높고 시장확보력⁶⁾은 유럽이 가장 높은 것으로 조사됨



5) 기술집중도 : (최근 3년 중요논문 건수) / (중요논문 건수) * 100 (%), 중요논문 : CITATION 10 이상인 논문

6) 외국인에 의한 특허 출원 증가율

4) 제조(산업) 공급망 및 시스템 보안 취약점 진단 자동화 기술

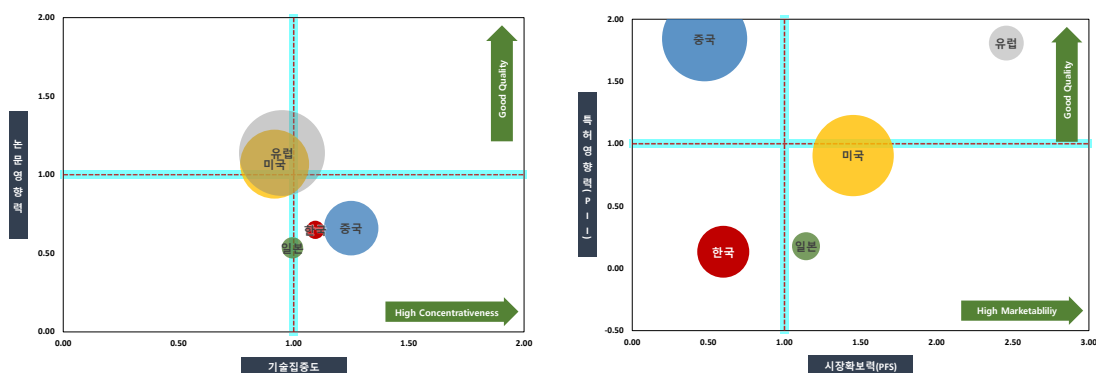
- (정의) 하드웨어 및 소프트웨어 솔루션 공급망(유통망 포함), 3자 어플리케이션 등 IT 시스템에 내재된 보안취약점을 AI 기술을 활용하여 자동으로 탐지하고 보안 위협에 자율적으로 대응하는 기술
- (범위) 보안취약점 진단 자동화 기술은 보안기술의 핵심기술이며, 분석 대상의 형태에 따라 소프트웨어 취약점 분석기술, 하드웨어 취약점 분석기술로 분류할 수 있음
 - (소프트웨어 취약점 분석기술) 소프트웨어 취약점 분석은 소스코드 취약점 분석 기술과 바이너리 취약점 분석(역공학) 기술로 구분
 - (하드웨어 취약점 분석기술) 하드웨어 장비를 구성하고 있는 IC칩, PCB보드, 펌웨어 등을 분석하여 의도된 또는 의도하지 않은 보안 취약점이나 백도어를 분석하는 기술임
- (필요성) 산업 전 분야가 디지털화가 가속화되면서 스마트공장에 대한 해킹은 실제 물리공간으로 확대되어 기업 매출에 큰 타격을 입히고, 제조설비 안전문제로 인명피해까지 이어질 수 있어 개발 필요
- (국내외 동향) 전 세계적으로 공급망 하드웨어·소프트웨어 위험관리에 정책적, 재정적 지원이 가속되고 있음
 - (한국) '20년 「ICT R&D 기술로드맵 2025(차세대보안 분야)」에서 '공급망 및 시스템 보안 취약점 진단 자동화 기술'을 12대 기술로드맵 대상기술로 선정하여 체계적인 기술개발 추진 중
 - (미국) 공급망 하드웨어·소프트웨어 위험관리에 우선순위정책을 추진하고 있으며, ICT 공급망 제품 및 서비스의 위험평가 프로세스 기준과 관련 도구 개발에 적극적으로 추진 중
 - (중국) 「네트워크 안전법」 시행을 통해 '중화인민공화국 경내에서의 네트워크 구축, 운영, 유지, 사용에 있어 보안의 관리 감독은 이 법의 적용을 받도록' 되어 있음(19.6)
- (2030 전망) 미·중 기술패권 경쟁, 코로나 19, 우크라이나-러시아 전쟁 등으로 신냉전 시대로 돌아가면서 자국의 산업을 보호하고 산업기술 유출을 방지하기 위해 사이버보안 규제가 강화되고 글로벌 무역에서 새로운 무역장벽이 될 것으로 전망

- 외산 기술의 수입 및 국산 기술의 수출 시 백도어, 보안취약점 등 사이버보안 위협요소를 사전 또는 실시간 스크리닝하여 안전하게 보안 통제할 수 있는 자동화된 기술을 해외에 의존하지 않고 자체 보유하는 것은 중요

■ (다른 미래유망기술과의 관계) 자율 무인 이동체 활용을 위한 인프라 통합 보안 기술, 디지털 신기술 악용 사이버범죄 추적기술 등에 기여 가능한 관계

- 시스템 보안 취약점 진단 자동화 기술은 자율 무인 이동체 활용을 위한 인프라 통합 보안 기술의 설계, 구축, 운영 전반의 취약점을 자동분석하여 보안사고를 예방하는데 기여할 수 있는 핵심기술
- 시스템 보안 취약점 진단 자동화 기술 중 소프트웨어 취약점 분석 기술은 범죄자의 디지털 증거물을 분석하여 디지털 신기술 악용 사이버범죄 추적기술의 기반이 될 수 있는 기술

■ (논문·특허 심층분석) 한국, 미국, 일본, 유럽(영국 포함 28개국), 중국의 최근 12년 논문 및 특허 분석 결과, 기술집중도⁷⁾는 중국이 가장 높고 시장확보력⁸⁾은 유럽이 가장 높은 것으로 조사됨



7) 기술집중도 : (최근 3년 중요논문 건수) / (중요논문 건수) * 100 (%), 중요논문 : CITATION 10 이상인 논문

8) 외국인에 의한 특허 출원 증가율

5) 프라이버시 강화 데이터 안전 활용을 위한 동형암호 등 기능형 암호 및 응용기술

- (정의) 데이터의 중요 정보를 보호하면서 데이터 활용성을 높이고, 데이터 활용 전주기에 대해 프라이버시 강화와 안전한 데이터 활용을 위한 기능형 암호 및 응용기술을 의미
- (범위) 데이터 침해 위협으로부터 안전한 데이터 환경을 구축하기 위해 차등 프라이버시 보호 기술, 동형암호(Homomorphic Encryption) 등의 암호화 기술, AI 학습을 위한 인공적으로 데이터를 생성하는 합성데이터 생성기술 등으로 분류
 - (차등 프라이버시 보호 기술) 데이터에 포함된 개인정보를 보호하기 위해 통계적 특성만 유지하면서 데이터에 노이즈를 추가하는 기술
 - (동형암호 기술) 기존 암호화 방식과 달리 암호화된 상태로 데이터 분석·연산이 가능한 암호 기술로, 다양한 분야에서 안전성을 가지나 암호화 후 데이터 크기 증가로 평문 대비 데이터 처리 속도가 느림
 - (합성데이터 생성 기술) 개인 민감정보를 제거함으로써 개인정보를 보호하면서 AI 모델 학습을 위한 인공적 데이터를 생성하는 기술
- (필요성) 데이터 공유로 개인정보를 활용한 다양한 서비스가 증가하여 데이터 유출 사고를 방지하면서 공유 데이터의 활용성을 높이는 데이터 분석 목적 맞춤형 빅데이터 공유 플랫폼 필요
- (국내외 동향) 개인정보를 안전하게 보호하기 위한 암호기술 개발 및 관련 법 제정을 추진 중
 - (한국) 데이터 경제 환경에서 데이터 속 민감정보를 가리거나 추론을 방지하고 가명정보 재식별 등 정보 유출과 오남용 방지를 위해 중요 데이터를 안전하게 보호하기 위한 암호기술 개발 및 고도화
 - (미국) 일반적으로 프라이버시 보호보다 데이터 활용을 중시하고 있지만 주 차원에서 개별법으로 진행되어 주별로 소비자 프라이버시 법안을 만들어졌으며 연방법이 제정 준비중
 - (EU) 일반개인정보보호법(18)은 개인정보의 정의, 역외적용, 가명처리의 허용, 개인정보 주체의 권리 명시, 개인정보 처리자의 의무 강화 등을 포함

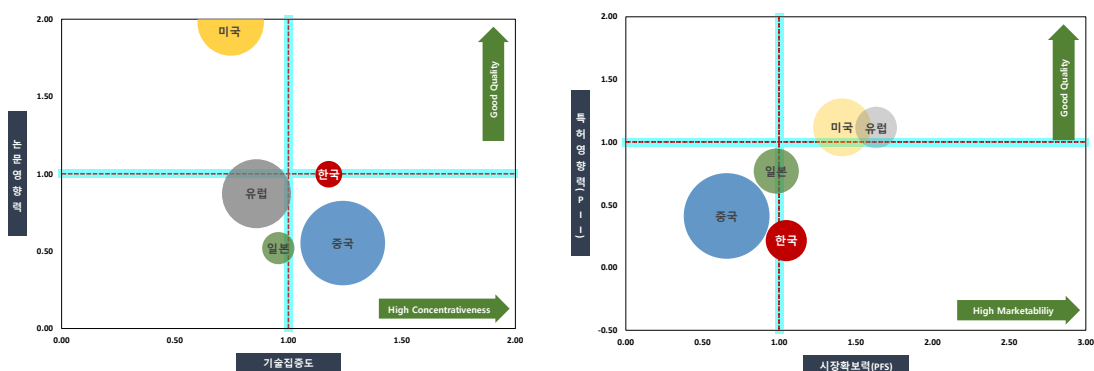
■ (2030 전망) 유통 중심의 데이터 보안이 보편화 될 것으로 예상되며, 차등프라이버시 방식, 동형암호 방식 등 기술이 진화할것으로 전망

- 제한영역의 비식별화를 넘어 범용적 비식별화 기술에 대한 요구가 자극될 것이며, 현재의 저장 중심 데이터 보안 보다는 유통 중심의 데이터 보안이 보편화 될 것으로 예상
- 데이터를 충분히 익명화하면서도 데이터의 유용성을 유지하기 위해 차등 프라이버시 방식에 적용되는 노이즈의 적절한 수준을 결정하는 것이 중요

■ (다른 미래유망기술과의 관계) 동영암호 기반기술은 의료, 금융, 공공, 국방 등 보안이 요구되는 다양한 분야에서 연계 가능

- 프라이버시를 보장하면서 AI 학습 등에 적용할 수 있는 완전동형암호 하드웨어 가속기는 의료, 금융, 공공, 국방 등 보안이 요구되는 데이터를 암호화된 상태로 다양한 융합서비스에 직접 활용하여 다양한 데이터를 기반으로 한 맞춤형 서비스 제공

■ (논문·특허 심층분석) 한국, 미국, 일본, 유럽(영국 포함 28개국), 중국의 최근 12년 논문 및 특허 분석 결과, 기술집중도⁹⁾는 중국이 가장 높고 시장확보력¹⁰⁾은 유럽이 가장 높은 것으로 조사됨



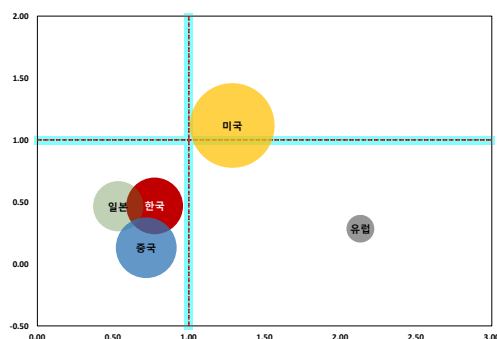
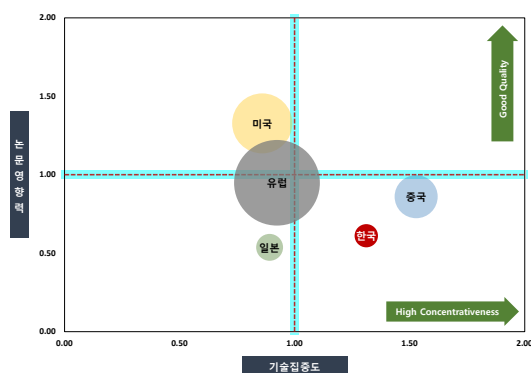
9) 기술집중도 : (최근 3년 중요논문 건수) / (중요논문 건수) * 100 (%), 중요논문 : CITATION 10 이상인 논문

10) 외국인에 의한 특허 출원 증가율

6) 메타버스 등 가상환경에서의 사용자 보호 및 보안 기술

- (정의) ‘가상과 현실이 융합된 공간에서 사람·사물이 상호작용하며 경제·사회·문화적 가치를 창출하는 세계(플랫폼)’인 메타버스에서 사용자·인프라·서비스를 보호하는 기술
- (범위) 메타버스의 정의뿐만 아니라 핵심 구현 기술과 보안 기술의 구성에 대해서는 현재 학술적으로 일치된 의견이 있지는 않고 다양한 관점과 해석이 등장하고 있는 단계임
 - 메타버스 인증 기술
 - 메타버스 프라이버시 보호 기술
 - 가상 트러스트 공간 기술
- (필요성) 메타버스는 가상과 현실이 융합된 공간에서 사람·사물이 상호작용하는 주요 특징을 가지고 있어서 기존의 온라인 환경과는 다르게 해킹의 위협이 사용자의 안전과 생명에 직접 영향을 미칠 수 있어서 사용자 보호 및 보안기술 개발이 중요함
- (국내외 동향) 국내에서는 중장기 메타버스 R&D 로드맵을 마련 중이며, 국외에서는 관련 법제정 및 표준·프로토콜 보안 연구 진행
 - (한국) 미래의 메타버스 서비스 실현을 위한 5대 핵심기술(①광역 메타공간 ②디지털휴먼 ③초실감미디어 ④실시간 UI/UX ⑤분산·개방형 플랫폼) 개발을 지원하고 중장기 메타버스 R&D 로드맵을 마련 중
 - (미국) XR에서의 프라이버시, 보안 및 윤리적 문제를 다루는 국제적 비영리단체 XRSI(XR Safety Initiative)에서는 4가지(접근-정보-관리-예방) 영역으로 구성된 프라이버시 및 안전 프레임워크를 수립, 보호조치 정의(‘20.09)
 - (중국) 메타버스를 더욱 발전시키기 위해서는 UGC 공간 보안 강화, 지식재산권 관리 역량 제고, 개인정보보호 기능 강화, 보편적인 접근 가능성 확대, 메타버스 적용 표준 및 프로토콜 등이 해결되어야 한다고 지적
- (2030 전망) 다중의 메타버스 환경을 넘나드는 멀티버스 환경에서 사용자의 정보가 안전하고 편리하게 공유 가능

- 메타버스의 모든 데이터·기능이 분산 처리되고, 플랫폼 간 상호 연동되어 공존·발전하는 멀티버스(Multiverse) 시대 도래
 - 서비스 특성에 따라 안전한 가상의 신뢰 공간을 쉽게 만들고 안전하게 관리할 수 있는 개인화된 가상 트러스트 공간 활용 확대
- (다른 미래유망기술과의 관계) 차세대 네트워크 보안 기술 및 동형암호 등 기능형 암호 및 응용기술과 밀접하게 연관
- 5G/6G 차세대 네트워크 서비스를 위한 데이터 보안 기술, 프라이버시 강화 데이터 안전 활용을 위한 동형암호 등 기능형 암호 및 응용기술은 데이터의 안전 및 활용을 위한 원천기술로써 가상환경에서의 사용자 보호 및 보안 기술에서 활용할 수 있음
- (논문·특허 심층분석) 한국, 미국, 일본, 유럽(영국 포함 28개국), 중국의 최근 12년 논문 및 특허 분석 결과, 기술집중도¹¹⁾는 중국이 가장 높고 시장확보력¹²⁾은 유럽이 가장 높은 것으로 조사됨



11) 기술집중도 : (최근 3년 중요논문 건수) / (중요논문 건수) * 100 (%), 중요논문 : CITATION 10 이상인 논문

12) 외국인에 의한 특허 출원 증가율

7) 양자시대의 절대적 데이터보안을 위한 양자암호기술

- (정의) 양자의 불확정성, 복제불가능성원리 등을 이용한 암호기술로, 절대적 안전성을 보장할 수 있는 암호기술을 의미
- (범위) 양자를 이용하여 현대암호의 기능들을 구현하고 이의 안전성을 양자역학을 기반으로 증명할 수 있는 기술을 의미하며, 양자 암호키분배, 양자 인증 및 전자서명, 양자보안전송 등으로 분류
 - (양자 암호키분배 기술) 양자의 파동특성을 이용하여 인코딩/디코딩한 정보를 송수신하는 방식으로 암호화에 활용되는 암호키를 분배하는 기술로, 양자역학의 원리를 이용하여 도청에 대한 안전성 제시가 가능한 기술
 - (양자 인증 및 전자서명 기술) 양자 암호키분배 기술의 원리를 활용하여, 상대방을 인증하는 핵심과정에 양자를 도입하는 기술과 데이터의 전자서명을 양자를 이용하여 생성하는 기술
 - (양자 보안전송 기술) 데이터를 양자를 이용하여 안전하게 전송하는 기술로, 보안성 확보를 위하여 인증 등과 결합 필요
- (필요성) 양자의 불확정성, 복제불가능성 등의 양자역학 원리에 기반하여 1984년에 제안된 양자 암호키분배 기술은 현대암호와 달리 컴퓨팅 및 해독 방법의 발전에 무관한 절대적인 안전성을 제공하는 기술임
- (국내외 동향) 국내에서는 국가 필수전략기술로 선정되었고, 각국에서 기술 확보를 위해 법 제정, 기술력 확보 및 실용화를 추진하고 있음
 - (한국) 양자 기술은 12대 국가 필수 전략기술로 선정하여 중점 지원이 진행되고 있으며, 양자 암호기술은 양자암호통신기술 분야에 포함
 - (미국) 미국은 NQI 법을 제정하여, 양자기술에 대한 지속적인 지원을 진행하고 있으며, 양자 통신 시스템 구축은 미래 가장 중요한 기술적 과제로 인식하여 중점 지원 중
 - (EU) 양자 암호키분배, 양자난수발생기 등 연구는 유럽이 시작을 주도했으며, 우수한 기술력 확보 및 실용화를 위한 다양한 프로젝트 진행 중

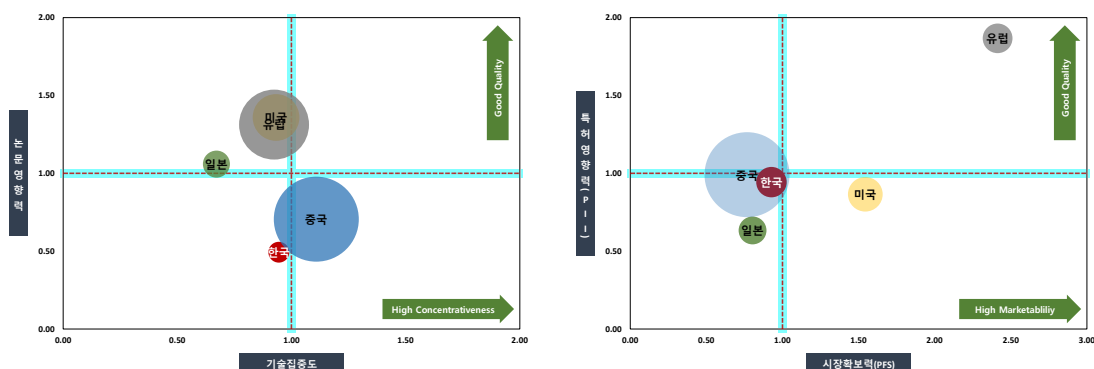
■ (2030 전망) 양자컴퓨터, AI의 등장 및 사이버 공격기술 발전으로 데이터의 탈취/변조/해독 위험이 크게 증가하여, 절대적 안전성을 제공하는 양자 암호기술을 국가 및 사회 주요 영역에서 도입 증가

- 양자 기술에 소요되는 부품의 소형화, 저가격화로 양자 암호키분배가 모바일 등 소형 디바이스에 적용 확대 예상

■ (다른 미래유망기술과의 관계) 자율 무인 이동체 보안, 가상환경에서의 사용자 보호, 프라이버시 강화 기능 등과 상호보완적 관계

- 양자 암호키분배 기술 및 양자 인증기술은 기존 사이버보안의 암호키분배 및 인증 기술과 네트워크 환경에 따라 보완적으로 결합되어, 자율 무인 이동체 보안, 가상환경에서의 사용자 보호, 프라이버시 강화 기능을 제공 가능
- 양자 암호기술은 미래 네트워크로 주목받는 양자 인터넷의 발전과 더불어 양자 인터넷에서 사이버 보안을 구현할 수 있는 기반기술로 다양한 보안기술 및 서비스의 양자화의 초석이 될 것으로 예상

■ (논문·특허 심층분석) 한국, 미국, 일본, 유럽(영국 포함 28개국), 중국의 최근 12년 논문 및 특허 분석 결과, 기술집중도¹³⁾는 중국이 가장 높고 시장확보력¹⁴⁾은 유럽이 가장 높은 것으로 조사됨



13) 기술집중도 : (최근 3년 중요논문 건수) / (중요논문 건수) * 100 (%), 중요논문 : CITATION 10 이상인 논문

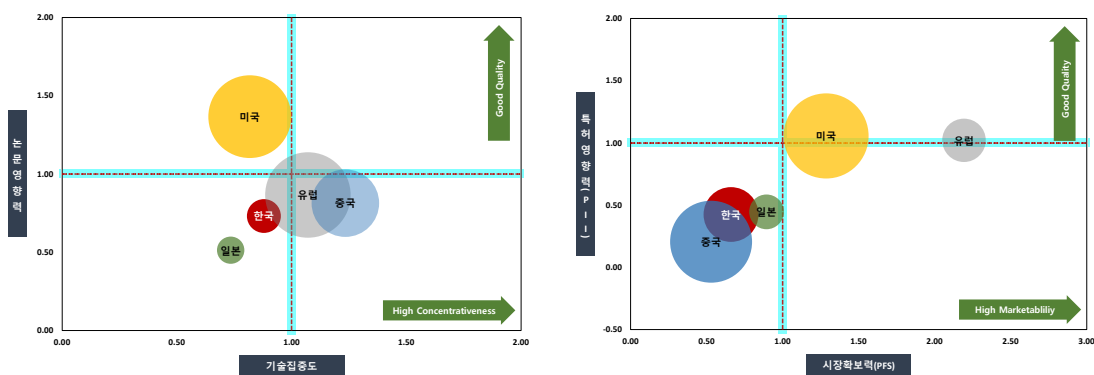
14) 외국인에 의한 특허 출원 증가율

8) 디지털 신기술 악용 사이버범죄 예방 및 추적기술

- (정의) 디지털 대전환 환경에서 고도화·지능화된 사이버범죄에 대응하기 위한 사이버위협 인텔리전스(Cyber Threat Intelligence) 기술
- (범위) 사이버 킬체인¹⁵⁾기반 공격 프로세스 분석을 통해 사이버범죄에 대한 추적·예측하는 디지털 리스크 보호기술과 공격의 선제적 대응을 위한 사이버위협 헌팅 기술
 - (디지털 리스크 보호 기술): 사이버 공격 사전단계(사이버 킬체인 1~2단계, 정찰 → 무기화)에서 정보수집 활동을 감시(추적)하고, 공격을 예측하는 기술
 - (사이버위협 헌팅): 사이버 공격 진행단계(사이버 킬체인 3~6단계, 전달 → 익스플로잇 → 설치 → 명령 및 제어)에서 위협대상의 취약점을 선제적으로 제거하기 위한 대응기술
- (필요성) 신규 사이버범죄 등장과 고도화·지능화된 사이버위협의 확산에 따라 피해 규모가 증가하고 있지만, 기존의 수동적 대응 기술(경계망 중심, 사후 대응 등)로는 한계가 있고, 검거율도 미비
- (국내외 동향) 국내에서는 국가 사이버 안보 전략을 발표하였고, 각국에서 행정명령, 협약 등을 통해 안보 위협에 대응 중
 - (한국) 해킹, 정보 절취 등 증가하는 사이버위협에 대응하여 사이버 안보 분야 정책 방향을 담은 국가 사이버 안보 전략을 발표(‘19.04)
 - (미국) 바이든 대통령은 연방정부 인프라와 네트워크를 보호하기 위해 사이버 보안 개선에 관한 행정명령 서명(‘21.05.)
 - (EU) 사이버범죄에 대응하는 각국의 법체계에 하나의 기준점을 제시하고 국가 간의 수사 공조가 신속하게 이루어지도록 사이버범죄 협약(Convention on Cybercrime) 채택
- (2030 전망) 사이버범죄는 개인, 기업을 넘어 국가를 대상으로 한 사이버위협이 증가 할 것으로 예상되며 이로 인해 국가 간 대립이 심화될 것으로 예측됨

15) 사이버 공격 절차를 7단계(공격 단계: 정찰-> 무기화->전달->익스플로잇->설치->명령 및 제어->악의적 활동)로 정의하고, 단계별로 공격자의 전략을 분석하여 체인을 단절시키기 위해 제안된 선제적 방어 모델(록히드마틴, '11)

- 2030년 사이버범죄는 지능적이고, 자가학습이 가능하도록 프로그램화될 것이며 국가 간에 인공지능을 활용한 방어와 공격이 가능할 것으로 예측
 - 5G, 클라우드, AI 등 새로운 디지털 인프라가 확대되고, 초연결 서비스가 발달하면서 공격 대상이 확대·다양성이 증가될 것으로 예측됨
- (다른 미래유망기술과의 관계) 인공지능 기반 지능형 사이버 보안관제 및 자동 대응 기술, 제조(산업) 공급망 및 시스템 보안 취약점 진단 자동화에 연계하여 활용 가능함
- 사이버 킬체인 기반의 사이버위협 헌팅 기술은 인공지능 기반 지능형 사이버 보안관제 및 자동 대응 기술과 연계되어 사이버범죄에 대응 및 시너지 효과를 기대할 수 있음
 - 사이버 킬체인 기반의 사이버위협 헌팅 기술은 제조(산업) 공급망 및 시스템 보안 취약점 진단 자동화를 위한 사이버위협 헌팅 기술을 활용할 수 있음
- (논문·특허 심층분석) 한국, 미국, 일본, 유럽(영국 포함 28개국), 중국의 최근 12년 논문 및 특허 분석 결과, 기술집중도¹⁶⁾는 중국이 가장 높고 시장확보력¹⁷⁾은 유럽이 가장 높은 것으로 조사됨

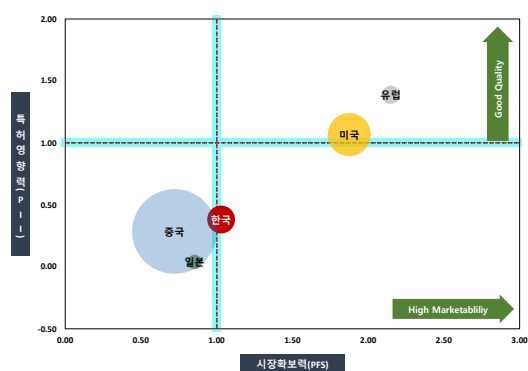
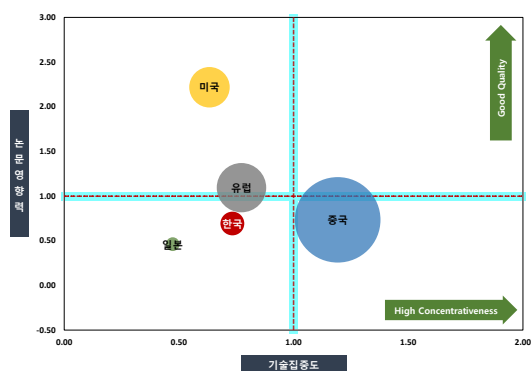


16) 기술집중도 : (최근 3년 중요논문 건수) / (중요논문 건수) * 100 (%), 중요논문 : CITATION 10 이상인 논문
 17) 외국인에 의한 특허 출원 증가율

9) 안전한 가상화 환경 활용을 위한 클라우드·엣지 보안 기술

- (정의) 공격 점점 확대로 인한 증가된 사이버 위협에 대응하여 컴퓨팅 자원 및 데이터를 네트워크로 효율적으로 활용하고자 하는 클라우드·엣지 기술 기반 보안기술
- (범위) 공격 점점 확대에 대응하기 위한 다중 위협대응 기술, 데이터의 안전한 보호 및 처리를 위한 데이터 안전관리 기술, 비신뢰 기반으로 권한 관리를 수행하는 제로트러스트 보안관리 기술 등으로 분류
 - (다중 위협대응기술) 비승인된 액세스를 차단하는 예방적 대응, 무단 변경 사항을 도출하는 감지 대응, 즉각적으로 대응할 수 있는 자동화된 대응, 보안 정책, 절차를 처리하는 보안관리 등으로 구성된 다중 대응 보안기술
 - (제로트러스트 보안기술) 설정된 네트워크 경계와 관계없이 아무도 신뢰하지 않는 것을 전제로 정상임을 인증받고 지속적으로 검증되기 전에는 내외부의 어떤 사람 또는 디바이스에도 접속 권한을 부여하지 않는 보안기술
- (필요성) 코로나 이후 비대면 원격근무의 보편화에 따른 클라우드 의존성 증가 및 클라우드에 저장된 데이터를 대상으로 한 공격 증가
- (국내외 동향) 국내는 클라우드 보안인증제도를 도입하고, 미국, 중국은 클라우드 확산을 위해 법, 규정 및 체계 정비 등 추진 중
 - (한국) 클라우드 서비스 제공자가 제공하는 서비스에 대해 정보보호 기준의 준수여부 확인을 인증기관이 평가·인증하는 클라우드 보안인증제도 도입
 - (미국) 클라우드 선제 도입(Cloud First)정책에서 클라우드 스마트(Cloud Smart) 정책으로 전환하고, 클라우드 확산을 위해 규정 및 조달체계 정비
 - (중국) 국가정보법 및 개인정보보호법 등을 통해 정부가 클라우드 기업에 영향력을 행사할 여지를 둠
- (2030 전망) 컴퓨팅 서비스 및 데이터의 클라우드화는 더욱더 가속화될 전망이고, 각국의 클라우드 이용 관련 규제 완화와 비용 효율성으로 소수의 글로벌 클라우드 업체의 점유율이 더욱 높아질 것으로 보임

- 글로벌 기업들의 각국 규제 기준을 손쉽게 통과하기 위한 기밀계산(Confidential computing)과 같은 기술들의 개발 및 적용이 가속화 전망
- (다른 미래유망기술과의 관계) 디지털 경제 활용을 위한 암호화폐 신뢰성 보장 기술은 클라우드를 기반 기술로 동작함
- 암호화폐 기술은 대부분 클라우드를 기반으로 동작하고 있고, 특히 암호화폐의 신뢰성은 단순히 프로토콜 적인 신뢰성뿐만 아니라 클라우드 인프라의 전체적 신뢰성, 즉 제로트러스트에 대한 기술적 완성을 필요로 함
- (논문·특허 심층분석) 한국, 미국, 일본, 유럽(영국 포함 28개국), 중국의 최근 12년 논문 및 특허 분석 결과, 기술집중도¹⁸⁾는 중국이 가장 높고 시장확보력¹⁹⁾은 유럽이 가장 높은 것으로 조사됨



18) 기술집중도 : (최근 3년 중요논문 건수) / (중요논문 건수) * 100 (%), 중요논문 : CITATION 10 이상인 논문
 19) 외국인에 의한 특허 출원 증가율

10) 안전한 디지털 경제 활용을 위한 암호화폐 신뢰성 보장 기술

■ (정의) 블록체인 기술, 분산원장 기술 등 디지털 화폐 또는 자산의 발행 또는 거래와 연관되어 신뢰성을 부여할 수 있는 기술

■ (범위) 분산원장기술과 암호화폐기술로 분류

- (분산원장) 거래 정보를 기록한 원장(Ledger)을 다수의 노드(참여자)들에 동일한 데이터를 복사하여 분산 저장하는 기술
- (암호화폐기술) 합의알고리즘, 암호화, 개인정보보호 강화기술, 보안관리, 디지털 서명 등의 기술

■ (필요성) 블록체인 및 이더리움 대량 해킹으로 인한 하드포크²⁰⁾, 해킹 등 암호화폐 탈취 기술 발전, 느린 거래속도 및 확장성 보완 필요

■ (국내외 동향) 국내외 정부 주도의 블록체인 산업 지원, 기술개발 등을 추진 중이나 규제 이슈 존재

- (한국) 2020년 과학기술정보통신부는 블록체인 기술 확산 전략을 발표하고, 블록체인 응용서비스 개발과 아이디어 구현을 위한 BaaS(Blockchain as a Service) 활용 지원
- (미국) 블록체인 기술 전반에 대해 현재 가장 높은 수준의 기술을 보유하고 있고, 블록체인 분산 네트워크 및 블록 체인 계정 검증 기술 등 다양한 연구를 수행 중
- (중국) 국가 주도로 적극적인 블록체인 산업 지원, 활용 촉진 및 22개의 대규모 블록체인 산업단지 조성
- (EU) 블록체인 데이터에 대한 비식별화 정보 활용성을 인정하나 규제 존재

■ (2030 전망) 블록체인 기술에 기반한 신뢰성 있는 공공 금융서비스의 도입은 민간 결제서비스 제공자의 경쟁을 촉진하고 지급결제 체제의 효율성 제고에도 기여할 것으로 기대됨

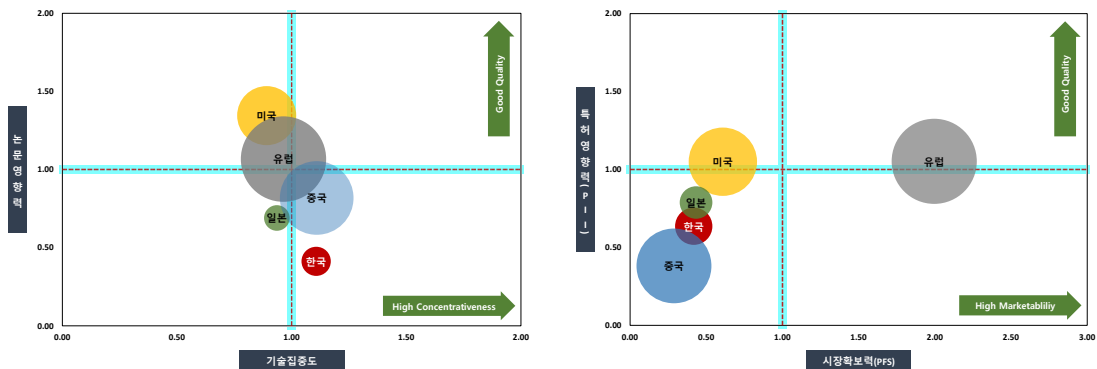
20) 하드포크는 문제를 해결하고 새로운 블록체인이 만들어지는 것을 말하고, 소프트포크는 문제를 해결하고 원래의 블록체인으로 돌아갈 수 있는 것을 말한다.

- 암호화폐의 높은 변동성과 데이터 신뢰성, 개인정보문제를 해결 할 수 있는 블록체인 및 분산원장의 한계를 극복하기 위한 기술 개발이 지속적으로 필요
- 양자컴퓨터가 일반화되면 현재의 분산원장시스템의 공격이 쉬워져 블록체인 무력화 가능성이 높아져 블록체인에 양자암호 방어 수단 필요

■ (다른 미래유망기술과의 관계) 디지털 경제 활용을 위한 암호화폐 신뢰성 보장 기술은 클라우드를 기반 기술로 동작함

- 암호화폐 기술은 대부분 클라우드를 기반으로 동작하고 있고, 특히 암호화폐의 신뢰성은 단순히 프로토콜 적인 신뢰성뿐만 아니라 클라우드 인프라의 전체적 신뢰성, 즉 제로트러스트에 대한 기술적 완성을 필요로함

■ (논문·특허 심층분석) 한국, 미국, 일본, 유럽(영국 포함 28개국), 중국의 최근 12년 논문 및 특허 분석 결과, 기술집중도²¹⁾는 중국이 가장 높고 시장확보력²²⁾은 유럽이 가장 높은 것으로 조사됨



21) 기술집중도 : (최근 3년 중요논문 건수) / (중요논문 건수) * 100 (%), 중요논문 : CITATION 10 이상인 논문
 22) 외국인에 의한 특허 출원 증가율

IV

결론 및 시사점

- 2023년 KISTEP 미래유망기술 주제를 선정하기 위해 최근 발표된 국내외 미래전망보고서의 트렌드, 제6회 과학기술 예측조사 보고서, 미래전략 2045, 일본 예측조사보고서('20) 등의 다양한 문헌 수집·분석 수행
 - 향후 10년 이내 주요 이슈로 부상할 가능성이 크고 여러 문헌에서 반복적으로 등장하고 있으며 최근 주요 사회 이슈와 연관성이 높은 ‘우주생활 시대’, ‘데이터 보안’, ‘제조 분야의 디지털 전환’, ‘디지털 경제’ 등의 4개 트렌드를 후보 주제로 선정
 - 미래유망기술 후보 주제를 기술수준평가 전문가 및 KISTEP 정책고객 등을 대상으로 설문조사를 통해 최종 ‘데이터 보안’으로 확정
- 미래유망기술은 5~10년 후 디지털 전환 시대 데이터의 폭발적 증가에 따른 데이터의 보안 및 보호에 기여할 수 있는 정도가 큰 기술을 후보군으로 선정
 - 후보군은 국가과학기술 표준 분류체계, ICT R&D 기술로드맵, 개인정보 보호·활용기술 R&D 로드맵 등의 데이터 보안 분야 기술분류체계를 기준으로 발굴
- 데이터 보안 및 보호 기술분류(안)를 바탕으로 전문가 서면 평가 등을 통해 최종 10개 미래유망기술 선정
 - 전문가 서면 평가로부터 얻어진 총 182개의 기술 중 추천 수, 평가지표 점수 등을 검토하고 내부 전문가 논의를 통해 주제와의 부합성 및 파급효과가 큰 10개 기술을 선정
 - ① 자율 무인 이동체 활용을 위한 인프라 통합 보안 기술, ② 인공지능 기반 지능형 사이버 보안 관제 및 자동대응 기술, ③ 5G/6G 네트워크 보안 기술, ④ 제조(산업) 공급망 및 시스템 보안 취약점 진단 자동화 기술, ⑤ 프라이버시 강화 데이터 안전 활용을 위한 동형암호 등 기능형 암호 및 응용기술, ⑥ 메타버스 등 가상환경에서의 사용자 보호 및 보안 기술, ⑦ 양자시대의 절대적 데이터보안을 위한 양자암호기술, ⑧ 디지털 신기술 악용 사이버범죄 예방 및 추적기술, ⑨ 안전한 가상화 환경 활용을 위한 클라우드·엣지 보안 기술, ⑩ 안전한 디지털 경제 활용을 위한 암호화폐 신뢰성 보장 기술

■ 미래유망기술의 조속한 실현과 발전을 위해서는 법·제도 개선, 인력양성, 인프라 확보 등이 필요

- (법·제도) 데이터 주권, 디지털 정보의 안전과 보안 등과 같은 법·제도 정비 및 양자암호기술 등과 같은 신기술 적용을 위한 평가검증 제도 마련
- (인프라 구축) 표준화, 인증을 위한 기반을 구축하고 해당 기술의 적용을 위한 산학연 협력체계 마련 및 테스트베드 구축
- (인력양성) 타산업과 데이터 보안 간의 융합적 인재 양성 및 산업 전반에 전문 인력 수급이 가능한 보안인력 양성 프로그램 추진

■ 논문 및 특허 분석에 따르면, 10개 미래유망기술 대부분은 성장기에 있으며 영향력 측면에서는 미국과 유럽이 주도하고 있는 것으로 파악

- 도입기에 있는 ‘메타버스 등 가상환경에서의 사용자 보호 및 보안기술’을 제외한 나머지 9개 미래유망기술은 성장기에 있는 것으로 분석
- 양적인 측면인 논문 및 특허 점유율에서는 중국이 앞서고 있으나, 질적 측면인 논문 및 특허 영향력에서는 미국과 유럽이 앞서고 있음
- 우리나라는 미국, 유럽, 일본, 중국과 비교하면 대부분의 기술이 중하위권에 위치

■ 논문 및 특허 분석에 따르면, 10개 미래유망기술의 논문영향력과 특허영향력에 따라 차별화된 기술확보전략이 필요

- 자율 무인 이동체 활용을 위한 인프라 통합 보안 기술(논문영향력 한국 5위, 특허영향력 한국 5위), 양자암호기술(논문영향력 한국 5위, 특허영향력 한국 3위), 제조(산업) 보안 취약점 진단 자동화 기술(논문영향력 한국 4위, 특허영향력 한국 5위), 암호화폐 신뢰성 보장 기술(논문영향력 한국 5위, 특허영향력 한국 4위), 사이버범죄 예방 및 추적기술(논문영향력 한국 4위, 특허영향력 한국 4위)은 상대적으로 논문영향력 및 특허영향력의 경쟁력이 낮아서 정부 차원의 지원이 중요
- 인공지능 기반 사이버 보안 관제 및 자동대응 기술(논문영향력 한국 1위, 특허영향력 한국 4위), 5G/6G 네트워크 보안 기술(논문영향력 한국 4위, 특허영향력 한국 3위), 프라이버시 강화 기능형 암호 및 응용기술(논문영향력 한국 2위, 특허영향력 한국 5위), 가상환경에서의 사용자 보호 및 보안 기술(논문영향력 한국 4위, 특허영향력 한국 2위), 클라우드엣지 보안 기술(논문영향력 한국 4위, 특허영향력 한국 3위)은 상대적으로 논문영향력 및 특허영향력의 경쟁력이 높아서 높은 기대성과가 예상되어 집중적 투자가 필요

참 고 문 헌

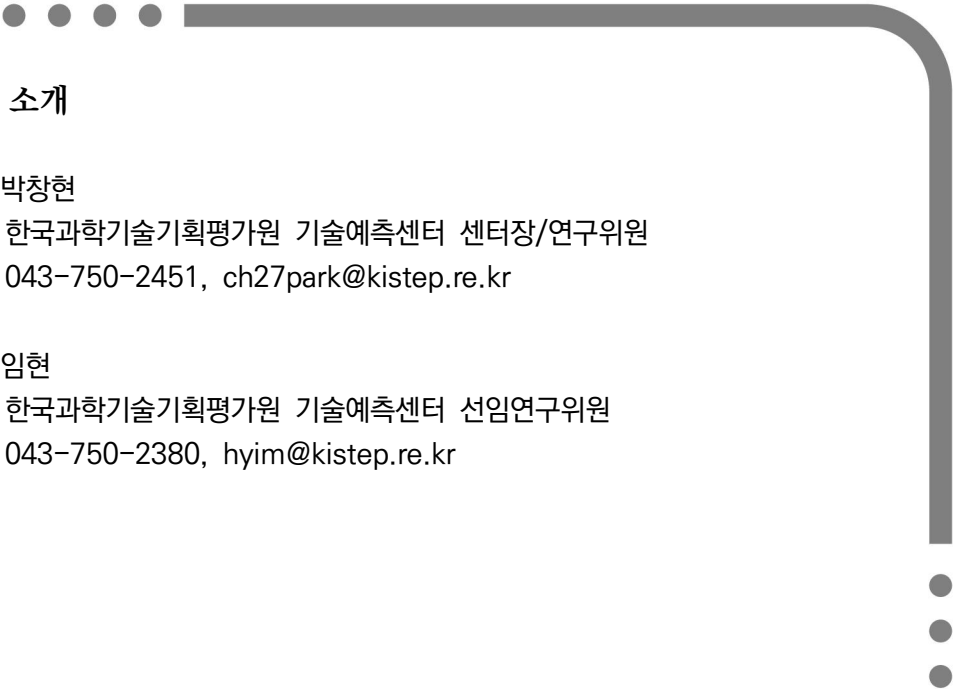
- 과학기술정보통신부, 미래전략2045 (2020)
- 박창현 외, 제6회 과학기술예측조사 연구 (2021)
- 한국과학기술기획평가원, 2019년 KISTEP 미래유망기술 선정에 관한 연구 (2019)
- 한국과학기술기획평가원, 2020년 KISTEP 미래유망기술 선정에 관한 연구 (2020)
- 한국과학기술기획평가원, 2021년 KISTEP 미래유망기술 선정에 관한 연구 (2021)
- 한국과학기술기획평가원, 2022년 KISTEP 미래유망기술 선정에 관한 연구 (2022)
- 한국과학기술정보연구원, 기술사업화 분석 리포트, 넥스트 노멀(Next Normal)시대, 새로운 비즈니스 기회를 찾다 (2020)
- 한국생명공학연구원, 2022 바이오 미래유망기술 (2022)
- 한국지능정보사회진흥원, 데이터 기반 포스트 코로나 이슈 분석과 10대 메가트렌드 (2021)
- 관계부처합동, 혁신성장을 위한 5G+ 전략, (2019.4.8.)
- 과학기술정보통신부, 6G 시대를 선도하기 위한 「미래 이동통신 R&D 추진전략」, (2020.8.6.)
- 전자통신동향분석, 공급망 보안기술 동향 (2020)
- IITP 주간기술동향, 완전동형암호 기술 및 표준 동향 (2021.09)
- IITP, 메타버스 R&D 로드맵(2021)
- KISA, 2020년 4분기 사이버위협 동향 보고서
- 클라우드 컴퓨팅 보안 기술 동향, 구동영, 정보보호학회지 제30권, 제6호, 2020
- 한국은행, 주요국의 중앙은행 디지털화폐(CBDC) 대응 현황
- NIC, Global Trends 2040 (2021)
- NISTEP, The 11th Science and Technology Foresight (2019)
- Intelligent Transport Systems (ITS); Communications Architecture, European Standard (Telecommunications series)
- Security guidelines for vehicle-to-everything (V2X) communication, TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU
- ARISTA NETWORK, The 5 Levels of Autonomous Security, 2022

- ECSO, Input to the horizon programme for cyber security (2021-2027)
- Deutsche Telekom, 5G Technology in Industry Campus Networks, (2022)
- A. Singh et. al, Quantum Internet- Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions (2021)
- <https://www.gartner.com/en/information-technology/insights/top-technology-trends>
- <https://www.technologyreview.com/2021/02/24/1014369/10-breakthrough-technologies-2021/>
- <https://www.weforum.org/press/2021/11/top-10-emerging-technologies-to-watch-in-2021/>
- <https://www2.deloitte.com/us/en/insights/focus/tech-trends.html>
- <https://www.wef.org>

KISTEP 이슈페이퍼 발간목록

발간호	제목	저자
2023-01 (통권 제341호)	KISTEP Think 2023, 10대 과학기술혁신정책 아젠다	강현규, 최대승 (KISTEP)
2022-20 (통권 제340호)	미국·일본의 과학기술혁신 행정체계와 시사점	양은진, 홍세호, 김다운 (KISTEP)
2022-19 (통권 제339호)	기술패권 시대 과학기술 인재 정책 방향	유준우, 김지홍, 이원홍 (KISTEP)
2022-18 (통권 제338호)	기술수용주기 모형 기반 2045년 미래혁신기술 분석	이재민, 박창현, 전해인 (KISTEP)
2022-17 (통권 제337호)	실험실창업, 어떻게 활성화 할 것인가? - 실험실창업 추진실태 분석과 정책제언 -	이길우, 김태현, 방형욱 (KISTEP)
2022-16 (통권 제336호)	신기후체제 시대 기후변화 적응 R&D의 주요 이슈 및 정부R&D 투자방향 제언	성민규, 박창대 (KISTEP)
2022-15 (통권 제335호)	전기차 사용후 배터리 산업 생태계 활성화 방안	이승필, 여준석, 조유진, 김태영 (KISTEP)
2022-14 (통권 제334호)	출연연의 전략성과 도전성 강화를 위한 기관평가 제도 개선 방안	김이경, 우기쁨, 정수현 (KISTEP)
2022-13 (통권 제333호)	대·중소기업의 상생·협력 R&D 활동을 어떻게 촉진할 수 있을까?	김주일, 이승필, 정두엽, 조유진, 진영현 (KISTEP)
2022-12 (통권 제332호)	신산업 분야 소재·부품·장비 미래선도품목 현황 진단 및 기술적 한계 극복전략	김진용, 김어진 (KISTEP)
2022-11 (통권 제331호)	화이트바이오 산업 활성화를 위한 유망 분야 도출 및 정부지원 방안	박지현, 홍미영 (KISTEP)
2022-10 (통권 제330호)	국가연구개발사업 학생인건비 지급의 주요 쟁점과 제언	박일주, 이지은 (KISTEP)
2022-09 (통권 제329호)	신산업 정책의 민관협력(PPP) 주요 이슈 분석	신동평, 허정, 권용완 (KISTEP)
2022-08 (통권 제328호)	감염병 위기대응 4대 영역별 핵심기술 및 정부R&D 지원방안	김주원, 홍미영 (KISTEP)

발간호	제목	저자
2022-07 (통권 제327호)	일반국민은 2022년 정부R&D예산에 대해 어떻게 생각하고 있을까?	이승규, 박지윤 (KISTEP)
2022-06 (통권 제326호)	「국가R&D 혁신방안」 추진과제 분석 및 향후 추진방향 제언	최창택 (KISTEP)
2022-05 (통권 제325호)	디지털 전환의 미래사회 위험이슈 및 대응 전략: 인공지능 역기능을 중심으로	구본진 (KISTEP)
2022-04 (통권 제324호)	대전환 시대의 과학기술혁신 정책 이슈	변순천, 구본진, 김성진, 김진하, 김현오, 박노언, 배용국, 오서연, 이원홍, 신동평, 정선민, 최창택 (KISTEP)
2022-03 (통권 제323호)	2030 국가온실가스감축목표에 기여할 10대 미래유망기술	이동기 (KISTEP)
2022-02 (통권 제322호)	국내외 환경변화에 따른 과학기술혁신 총괄기능 강화 방향	이정재 (KISTEP)
2022-01 (통권 제321호)	KISTEP Think 2022, 15대 과학기술혁신정책 아젠다	손병호·손석호 (KISTEP)



필자 소개

▶ 박창현

- 한국과학기술기획평가원 기술예측센터 센터장/연구위원
- 043-750-2451, ch27park@kistep.re.kr

▶ 임현

- 한국과학기술기획평가원 기술예측센터 선임연구위원
- 043-750-2380, hyim@kistep.re.kr

KISTEP ISSUE PAPER 2023-02 (통권 제342호)

|| 발행일 || 2023년 2월 21일

|| 발행처 || 한국과학기술기획평가원 전략기획센터
충청북도 음성군 맹동면 원중로 1339
T. 043-750-2300 / F. 043-750-2680
<http://www.kistep.re.kr>

|| 인쇄처 || 주식회사 동진문화사(T. 02-2269-4783)
