1916호
2019.10.02.
ISSN 1225-6447

Weekly ICT Trends

주간기술동향

IITP 정보통신기획평가원

Weekly ICT Trends
주간기술동향 1916호
ISSN 1225-6447

기획시리즈 2

차세대 사이버보안 기술 동향

[이대성/부산가톨릭대]

Ⅰ. 서론
Ⅱ. 사이버 공격 및 차세대 보안기술 정책 동향
Ⅲ. 차세대 보안기술 개발 동향
Ⅳ. 결론

ICT 신기술 16

산업제어시스템의 국가별 사이버 보안 현황

[강민균/㈜소프트아이텍]

Ⅰ. 서론
Ⅱ. ICS 사이버 보안 현황
Ⅲ. 결론

ICT R&D 동향 25

병원 내 중대 이벤트 예측 시스템

[최재식/울산과학기술원]

머신러닝 기반 녹내장 진단 기술

[오세종/단국대학교]

chapter 1

차세대 사이버보안 기술 동향

이대성 ‖ 부산가톨릭대 교수

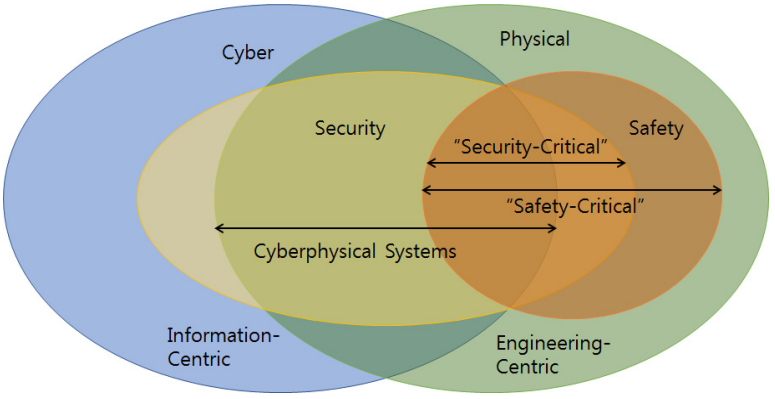
IoT, 5G, 클라우드, 빅데이터와 같이 4차 산업혁명을 이끄는 핵심기술들이 국가 사회경제 인프라 전반에 걸쳐 스마트 융합화를 촉진함에 따라 사이버 보안의 영역도 기존의 시스템 훼손, 서비스 방해, 정보 유출과 같은 정보시스템 보호라는 개념에서 초연결, 초신뢰를 구현하는 안전과 보안이 융합된 CPS (Cyber Physical System) 보호라는 개념으로 확장되고 있다. 따라서 본 고에서는 최근 사이버 공격자의 고도화된 자동화 도구를 이용한 메가 공격에 대응하여 활발하게 기술 개발이 진행되고 있는 차세대 사이버 보안영역의 변화 추세와 함께 SOAR(Security Orchestration, Automation and Response)나 Zero Trust와 같은 사이버보안 기술의 개념적 변화를 소개한다. 또한, 이를 전략적으로 구현하기 위한 주요국 정부의 R&D 정책 동향과 사이버 메가 공격에 실시간 대응하기 위한 핵심적인 차세대 사이버 보안 기술들의 개발 동향을 살펴보기로 한다.

I. 서론

인공지능(AI)을 기반으로 IoT, 클라우드 컴퓨팅, 빅데이터, 5G, 로봇, 드론 등 4차 산업혁명을 이끄는 혁신기술들의 실용화로 인해 사이버 공간과 현실 공간이 빠르게 융합되면서, 현장 생산활동의 효율성과 소비활동의 편리함이 빠르게 향상되고 있다.

하지만, 자율적으로 동작하는 멀웨어, 취약성을 악용하여 감염을 확산시키는 워너크라

* 본 내용은 이대성 교수(☎ 051-510-0653, dslee@cup.ac.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.



〈자료〉 Gartner, Innovation Insight for a Safety Critical, Safety Critical Practice, 2016. 10.

[그림 1] CPS 진전에 따른 차세대 사이버 보안의 개념 변화

이(WannaCry)와 같은 새로운 형태의 사이버 공격에 의한 위협도 함께 증대되고 있어, 대규모 피해의 발생 가능성도 점차 높아지고 있다. 특히, IoT와 더불어 드론, 자율주행차 등에 대한 사이버 공격의 가능성은 기존 사이버 보안 영역인 정보 훼손, 유출, 서비스 방해 등의 범위를 뛰어넘어 [그림 1]과 같이 인명과 재산의 안전을 보장해야 하는 영역까지 확대되고 있으며, LTE보다 수십 배 빠른 초고속을 구현한 5G의 상용화로 인해 초연결, 초신뢰 및 방대한 용량의 동시 접속 시에 필요한 초저지연 보안기술의 구현을 필요로 하고 있다.

따라서, 본 고에서는 4차 산업혁명시대의 핵심 키워드인 CPS(Cyber Physical System)의 포괄적인 안전·신뢰성 확보 및 리질리언스(resilience) 구현을 목표로 하는 차세대 사이버 보안기술과 관련된 보안 개념의 변화, 국내외 주요국들의 R&D 정책 및 세부 사이버 보안 핵심기술들의 연구개발 동향을 살펴보기로 한다.

II. 사이버 공격 및 차세대 보안기술 정책 동향

1. 사이버 공격 동향

지난 10여 년간 사이버 보안기술은 제로데이(zero-day) 공격이나 APT 공격을 방어하

기 위한 안티봇(anti-bot)이나 악성코드를 탐지하는 샌드박스(sand-box) 개발이 중심을 이루었다. 하지만 최근에는 국내외에서 IP 카메라 해킹, 랜섬웨어, 가상통화 취급업소 공격, 전파 송신기를 활용한 자동차 해킹 등 새로운 형태의 사이버 사고 발생이 보고되고 있다.

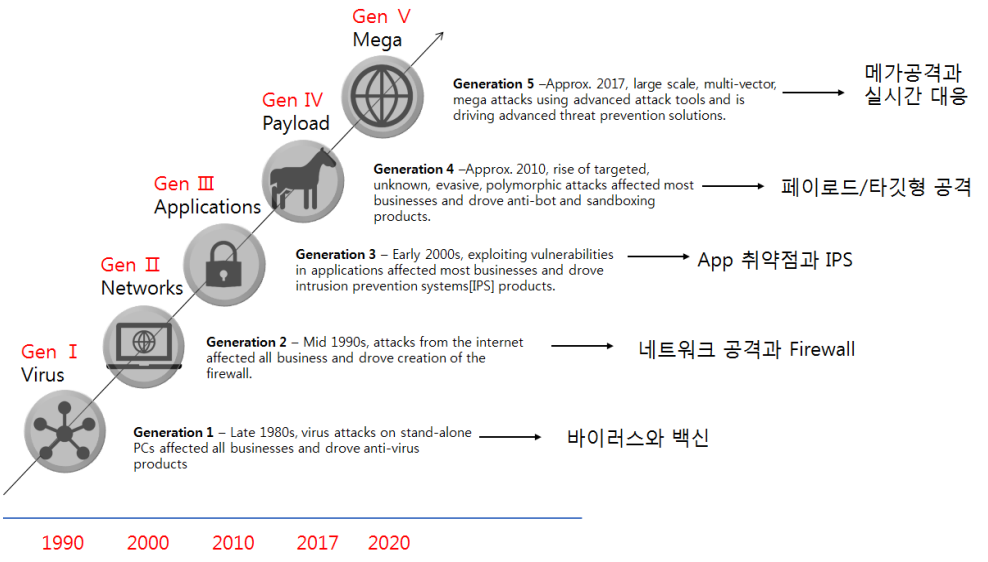
차세대 사이버보안기술 개발 동향 분석과 관련하여 국내외에서 발생한 주요 사이버 보안사고들을 정리하면 [표 1]과 같다.

[표 1] 국내외 주요 사이버 보안사고

발생시기	사고내용	비고
2018년 1월	일본 가상화폐거래소 5,800억 원 불법 송신	해외
2017년 5월	랜섬웨어 워너크라이(WannaCry) 감염(영 병원, 불 르노)	"
2016년 12월	우크라이나 전력회사 변전소 공격(1시간 정전)	"
2016년 11월	국내 IP 카메라 해킹	국내
2016년 9월	Mirai에 의한 IoT 디바이스 대규모 DDoS 공격	해외
2015년 11월	미국 소니 픽처스 해킹	"
2014년 6월	6.25 사이버공격(한수원 해킹)	국내
2013년 3월	3.20 사이버테러(한국 주요 언론사, 금융권 전산망 다운)	"
2011년 3월	3.3 디도스 공격(한국 정부기관, 포털, 은행 사이트)	"
2010년 6월	이란 Stuxnet 원전 사이버 공격	해외
2009년 7월	7.7 디도스 공격(한국, 미국의 정부기관, 포털, 은행사이트)	국내
2009년 4월	미 F-35 전투기 기밀 해킹	해외
2007년 4월	러-에스토니아 사이버전	"
2003년 1월	슬래머웜에 의한 1.25 인터넷대란(DNS서버 마비)	국내
2001년 7월	코드레드 웜바이러스(IIS 버퍼 오버플로 취약점 악용)	"
1998년 6월	CIH 바이러스(MS 윈도 95, 98, ME 감염)	"

〈자료〉: 부산가톨릭대 융합보안공학센터 재작성, 2019. 7.

이와 같은 사이버 보안사고의 시대별 변화를 기준으로 체크포인트는 [그림 2]와 같이 2017년 4월에 발생한 워너크라이(WannaCry) 공격을 경계로 하여 현재 시점을 4세대 보안시기에서 5세대 보안시기로 이행되는 과정으로 예측하고 있다[11]. 이는 기존에 이메일 첨부파일을 통해 유포시키는 일반적인 랜섬웨어와는 달리, MS 윈도의 파일 공유에 사용되는 서버 메시지 블록(SMB) 원격코드의 취약점을 악용하여, 인터넷 네트워크에 접



〈자료〉 Check Point Infinity Whitepaper, 2019.

[그림 2] 사이버 보안기술의 세대별 진화과정 및 특징

속만 해도 감염되는 방법을 취함으로써 기존의 침입기술을 보다 지능화하면서 암호화 기법을 사용하였기 때문인 것으로 판단된다.

따라서 차세대 보안기술 개발의 중심은 초연결 IT 시스템의 취약점에 대한 메가 공격(mega-attack) 실시간 대응이 차세대 기술 개발의 핵심을 이룰 것으로 보이며, 시스템에 접속하고자 하는 모든 사물에 접속 권한을 부여하기 전에 ID 확인 과정을 거치는 Zero Trust나 SOAR의 개념 구현이 5세대 사이버 보안 기술 개발의 중심이 될 것으로 전망된다.

2. 주요국의 차세대 보안기술 정책 동향

4차 산업혁명의 글로벌 확산으로 디지털 경제로의 이행이 순조롭게 진행되는 가운데, 가트너는 세계 사이버 시장규모를 2018년 1,141억 달러에서 2019년에는 1,241억 달러로 8.7% 성장할 것으로 전망하고 있다[12]. 이에 따라 미국, EU, 중국, 일본 등 주요국들은 사이버 보안 분야에서의 주도권을 확보하기 위해 사이버보안 전략을 마련하며 자국의 사이버 보안 투자를 확대하고 있다.

사이버보안 분야에서 최고의 원천기술 경쟁력을 보유한 미국은 2018년 9월, 연방차원

의 사이버 보안수준 강화와 기술 발전에 필요한 “국가 사이버 전략(National Cyber Strategy)”을 발표하였으며, 구글, 아마존과 같은 글로벌 기업의 지속적인 대규모 투자와 새로운 기술을 갖고 시장에 진입하는 스타트업들이 미국 사이버보안 산업구조의 양대축을 형성하면서 사이버보안 분야에서의 세계적인 주도권을 강화해 나갈 것으로 보인다.

EU는 사이버 전문기관인 ENISA(European Union Agency for Network Information Security)의 역할이 증대되는 가운데, BAE systems, KPMG, 카스퍼스키, Avast, F-Secure 등의 보안기업들이 역내 사이버보안 산업을 주도하고 있다. 특히, 2019년 6월부터 사이버보안법(EU Cybersecurity)이 시행됨에 따라 ENISA를 중심으로 기관 간에 인증업무를 분담하기로 함으로써 향후 역내 네트워크에 접속되는 제품에 대한 보안인증서를 요구할 것으로 예상된다.

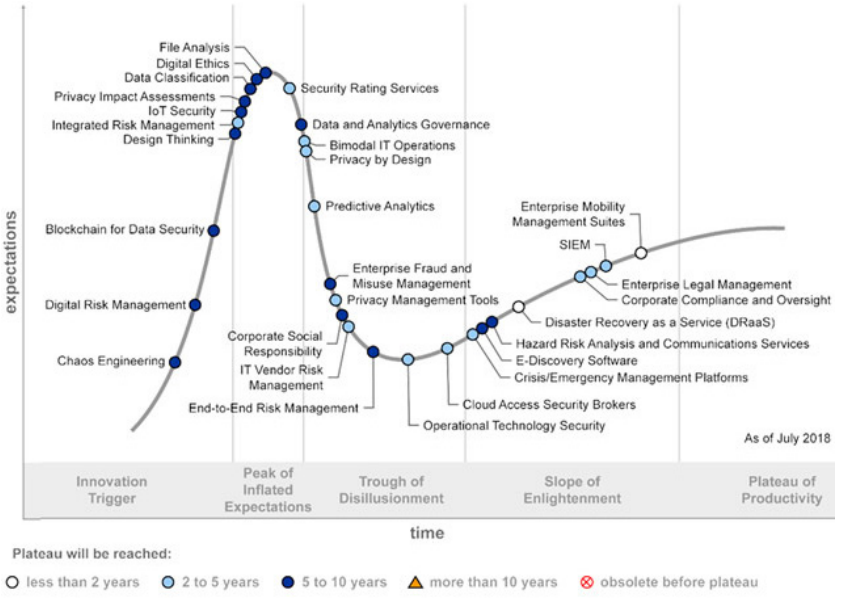
중국은 2017년 6월부터 중국 내에서 IT, 운송, 에너지, 금융 등 중요 인프라를 운영하는 기업은 데이터를 반드시 중국 내에 저장하고, 중국 정부가 요구할 경우 데이터 제공을 골자로 하는 사이버 보안법을 시행하였고, 2017년에는 사이버강국 실현과 사이버 상의 국가 주권 및 이익 보호 등을 목표로 하는 국가 사이버보안 전략을 발표하였다. 이 전략은 사이버보안 기초역량 강화, 사이버 공간 주권 수호 등 9개 항으로 구성되어 있다.

일본은 2019년 5월 사이버 보안 정책을 담당하는 총리실 직속 사이버보안 전략본부의 사무국인 NISC(National center of Incident readiness and Strategy for Cybersecurity)가 사이버보안 2019를 발표하였으며, 핵심항목은 2020 동경올림픽 사이버안전 확보, IoT 디바이스 보안강화, 사이버 안전사고의 탐지, 보고 및 대응 인재 양성으로 구성되어 있다. 사이버보안 전략본부는 2017년에 중요 인프라에 대한 4차 보안대책을 통해 사이버 공격과 자연재난에 따른 중요 인프라의 서비스 장애 및 복구 대책을 제시하였고, 민간 사이버 보안인재 양성을 위한 “사이버보안 인재양성 프로그램”을 발표하였다.

III. 차세대 보안기술 개발 동향

1. 사이버보안기술 개황

IITP에 따르면, 현재 사이버 보안기술의 국가별 수준은 미국을 100%로 할 때, EU



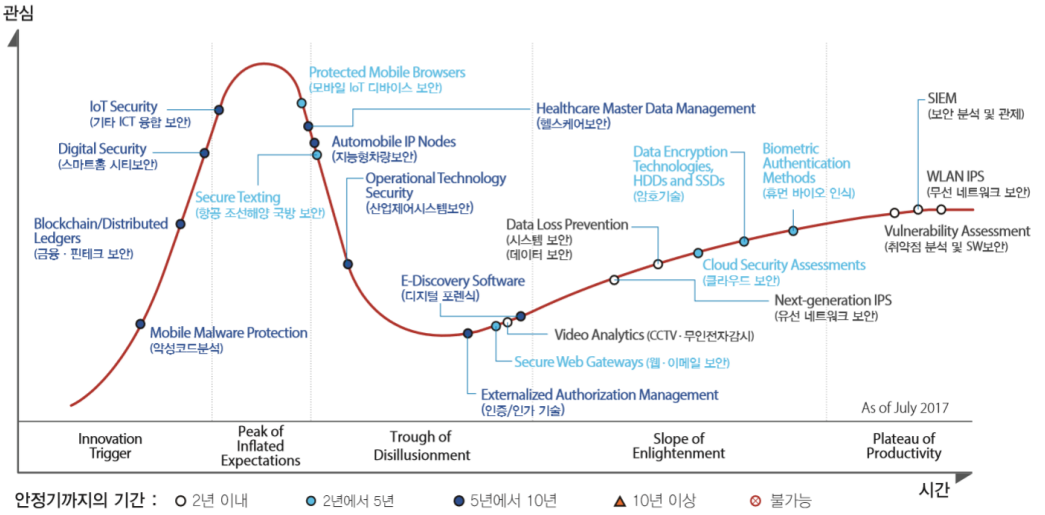
〈자료〉 Gartner, Hype Cycle for Risk Management, 2018. 7.

[그림 3] Gatner사의 위험관리 기준 차세대 보안기술 영역 예측

89.7%, 한국 85.5%, 일본 83.2%, 중국 81.2%의 순이며, 우리나라의 사이버 보안 기술수준은 기초, 응용, 상용화 단계에서 비슷하게 14.5%의 격차를 보이고 있는 것으로 평가하였다[2].

차세대 보안 기술을 추정하려는 경우, [그림 3]과 같이 미 가트너사가 개발한 하이프 사이클(Hype Cycle)을 활용하는 것이 유용하다. 이 사이클은 기술 촉발(Technology Trigger), 기대의 정점(Peak of Inflated Expectations), 환멸(Trough of Disillusionment), 계몽(Slope of Enlightenment), 생산성 안정(Plateau of Productivity)의 5단계로 구성되며, 차세대 보안기술 영역은 주로 1단계인 기술촉발단계에 위치하고 있다[14].

가트너는 사이버 위험관리를 기준으로 하여 Chaos Engineering, Digital Risk Management, Blockchain for Data Security, Design Thinking, Integrated Risk Management, IoT Security, Privacy Impact Assessments, Data Classification, Digital Ethics, File Analysis를 1단계 보안기술로 예측하고, 2단계 기술로는 Security Rating Services, Data and Analytics Governance, Bimodal IT Operation, Privacy by Design, Predictive Analysis로 예상하고 있다.



〈자료〉 IITP, ICT 기술수준조사보고서, 2018. 5.

[그림 4] 국내 보안전문가에 의한 차세대 사이버보안 기술 예측

이를 토대로 국내 보안전문가들이 사이버보안 기술 관점에서 작성한 하이프 사이클에서는 [그림 4]와 같이 Blockchain for Data Security, Digital Security, IoT Security, Mobile Malware Protection의 4개 기술로 압축시킨 것이 대조를 이룬다[2]. 위 자료들을 분석해 본 결과 IT 영역에서는 사이버 공격기술의 진화와 대규모 사이버 공격에 대비하여 악성 웹사이트 탐지, 멀웨어 감염탐지, 봇 프로파일링, 도메인 평가 기술 고도화에 중점이 두어지고 있으며, IoT/OT 영역에서는 인증/인가, 보안 프레임 관리, 탐지/대응기술, 그리고 중요정보통신시설 영역에서는 대규모/복합연동 시스템화가 진전됨에 따라 기술의 범용화, 오픈화, 신기술 적용 트렌드를 수용하는 리스크 관리기술이 차세대 보안기술의 주류가 될 것으로 보인다.

2. 보안 분야별 기술개발 동향

차세대 보안기술은 IoT 및 5G를 기반으로 하는 초연결 플랫폼의 안전·신뢰성과 리질리언스를 구현하기 위해 사이버 보안 전 구간을 대상으로 한 메가 공격에 실시간 대응할 수 있는 통합적 사이버 위기관리(Cyber Risk Management)를 목표로 기술 개발이 진행될 것으로 전망된다.

따라서 4세대 보안까지 주류를 이루었던 보안 장비 중심의 기술 개발로부터 딥러닝 등 AI 관련 기법을 활용하여 공격자의 진화에 예방적으로 대응하는 지능방어(Predictive Intelligence), 정상행위의 자동학습을 통해 비정상 행위를 탐지하는 행태분석탐지(Behavioral Analytics/Anomaly Detection), 엔드포인트의 대용량 트래픽을 보호 처리하는 자동 보안(Automated Security), 변종 바이러스와 좀비에 대응하는 디셉션 보안(Deception Security), 리스크가 적은 불필요한 데이터를 자동 삭제하는 Dark Data 식별기술 등이 차세대 보안기술 개발의 주류를 형성할 것으로 예측된다.

또한, 국가 차원에서는 사회혼란을 조성하거나 국가기밀을 탈취하기 위해 조직적/의도적으로 시도되는 사이버 공격의 진화에 대비하여 공격단계별로 가해지는 위협요소를 사전에 차단하는 이른바 사이버 타격순환 개념인 사이버 킬 체인(Cyber Kill Chain) 기술과 보안 supply chain에 대한 보안성 등급 평가기술(Security Rating Services: SRS)도 활발하게 연구될 것으로 보인다.

가. SOAR

시스템 보안에서는 공격자들이 바이러스 백신과 APT 공격 차단을 우회하여 공격하기 위해 엔드포인트를 경유하면서 방어자들은 안티 바이러스 기능을 시스템 보안과 기능적으로 결합하는 추세를 보이고 있다. 이에 따라 시스템 보안기술은 기존의 NAC, ESM 중심에서 SIEM(Security Information and Event Management)이나 UEBA(User and Entity Behavior Analytics)와 같이 로그 데이터의 실시간 분석과 엔드포인트 보호 중심으로 기술영역이 확장되었다.

SIEM은 네트워크, 서버, 엔드포인트 전 구간에서 발생하는 공격 탐지, 차단, 대응을 위해 실시간으로 보안위협을 모티터링하는 기술적 특성을 갖고 있으며, UEBA는 ML을 기반으로 엔드포인트에서 내부자들의 행위기반으로 자동 감지 및 대응하는 기술이라 할 수 있다. 최근에는 SIEM과 UEBA의 확장 개념으로 알려지지 않은 위협에도 대응할 수 있는 EDR(Endpoint Detection and Response)이 차세대 시스템보안 기술로 주목되고 있다.

이와 관련된 기술 동향으로 IBM은 인지 보안 기술을 적용하여 연구 보고서, 웹 텍스트 및 위협 데이터를 분석하여 사용자 질의에 대한 답변 생성 및 추론과 조언을 제공함으로써 실시간 대응하고 있으며, MS는 머신러닝과 AI 기술이 접목된 통합 보안 솔루션(SPE)을

개발하여 2,000억 이메일의 스팸 및 악성코드 분석, 180억 이상의 빙(Bing) 웹페이지 스캔을 종합하여 실시간 통합 분석을 수행하고 있다.

디바이스 보안영역에서는 모바일 디바이스와 IoT에 대한 보안기술 연구가 활발하게 진행되고 있으며, 5G 모바일의 상용화는 현재의 연구개발 사이클을 더욱 빠르게 촉진시킬 것으로 전망된다. 그 동안 국내에서는 모바일 백신과 MDM(Mobile Device Management)을 중심으로 기술 개발이 추진되었으나, 미국 등에서는 기존의 시그니처를 머신러닝하여 모바일 네트워크와 모바일 엔드포인트를 보호하는 기술들이 개발되고 있다.

나. 지능형 취약점 분석

취약점 분석기술 분야에서는 수동으로 취약점을 분석할 경우 9개월 이상의 시간이 소요되기 때문에 제로데이 공격 등 자동으로 수행되는 해킹 도구를 이용한 신규 취약점에 효과적으로 대응할 수 있도록 익스플로잇 자동 생성 기술을 구현하고, 소프트웨어 취약점 자동 패치(Hardening) 기술을 구현하는 바이너리 코드(Binary Code) 분석기술을 중심으로 연구가 진행되어 왔다.

하지만 다양한 플랫폼에서 다양하게 활용되는 소프트웨어별로 취약점 탐색을 자동화한다는 것은 사실상 불가능하므로 앞으로는 딥러닝을 기반으로 악성코드를 탐지하고 유사도를 자동 측정하는 기술과 정보공유 채널 확보 및 상호운용 플랫폼 개발이 추진되면서 차세대 SRM(Security Risk Management) 영역을 확장시켜 나갈 것으로 전망된다.

또한, SW에 내재된 보안위협을 자가 탐지하거나 복원하기 위한 기술과 HW에 대한 보안성 분석과 구현상 보안 결함 진단기술이 강조되고 있는 가운데, 시스템의 정상 상태를 기억하여 외부 공격을 식별하고, 내재된 보안취약점을 스스로 제거하여 정상상태로 되돌리는 일종의 자기학습형 사이버 면역기능을 갖는 지능형 사이버위협 대응기술(CTI)도 활발하게 연구될 전망이다.

다. 초신뢰 데이터 보안

초신뢰 데이터 보안을 구현하기 위해서는 사용자 중심의 안전한 데이터 유통을 보장해야 하며, 이를 위해 차세대 암호인 양자컴퓨터 위협 대응이나 양자내성 암호 기반의 보안 인프라 구성을 위한 연구가 중점적으로 추진되고 있다.

LPN(Learning Parity with Noise)을 응용한 경량 사용자 인증 프로토콜인 HB(2001)

를 개선한 HB-MP+(2008) 프로토콜을 이용하여 2m bit의 통신 오버헤드와 보안성이 개선되고 있는 가운데, 국내외적으로 부채널 분석 등 키 누출 공격이 심화됨에 따라 키은닉 기술 개발의 중요성이 강조되고 있다[8].

한편, 모바일 디바이스의 보급과 소셜 비즈니스의 확산으로 다양한 서비스를 지원할 수 있는 개인인증 기술의 고도화가 요구되고 있다. 이에 따라 ID 패스워드와 공인인증서를 대체할 수 있는 지문인식, 홍채인식, 정맥인식 등 바이오 인증기술의 융합과 사용자의 행위적 정보를 이용한 인증기술이 개발되고 있다.

또한, 사이버 공격자의 주 타깃인 관리자 계정의 보호를 위해 클라우드 기반에서의 PAM(Privileged Access Management) 기술, 피싱에 대응하는 비즈니스 이메일 컴프로마이즈 기술, 안티 fraud 및 ID 관리기술도 중점 연구될 것으로 보인다.

라. 차세대 네트워크 보안

네트워크 보안은 방화벽(Firewall), 침입방지시스템(IPS), DDoS 방어시스템, 웹 방화벽(WAF)을 중심으로 발전해 왔으나, 이들 제품들은 허가된 주소, 프로토콜, 애플리케이션을 통한 악성코드 유입 차단에 기술적 한계를 노출하고 있다. 따라서 차세대 네트워크는 이동성과 클라우드 컴퓨팅을 지원하고 변화하는 위협 환경에 대응할 수 있도록 발전해 갈 것으로 보인다.

특히, 네트워크 가상화와 안전한 5G 서비스 제공을 위한 유무선 네트워크 및 장비 보안 원천기술 개발, 스마트 IoT 서비스 네트워크 보호를 위한 사이버공격 대응 원천기술 개발, 초연결 네트워크 보안기술이 중점 기술개발 영역으로 부상할 전망이다.

SDN/NFV 보안 기술은 클라우드 기반 SDsec(Software Defined Security)의 개념으로 확장되고 있으며, 시스코, 스탠포드대학교, 브이엠웨어, CSA 등이 SDN/NFV 플랫폼 보안을 위한 가상화 네트워크 플랫폼 통합 보안, SDN 기반 보안 언어, SDsec 컨트롤러, SDN/NFV 지능형 보안기술을 활발하게 개발하고 있다.

마. IoT 보안

4차 산업혁명의 핵심동력으로 불리우는 IoT 보안기술 개발은 차세대 보안에서 가장 주목받는 영역이다. IoT 루프 봇넷은 악성 프로그램 탐지율을 낮추면서도 매우 빠른 속도로 IoT 장치들을 감염시키기 때문에 미라이 봇넷보다 훨씬 강력한 공격도구인데, 실제로

감염된 IoT 장치들의 수는 아직 정확히 파악이 되고 있지 않다. 또한, 차세대 센싱 데이터는 초대용량의 비정형 데이터를 유발함으로써 데이터를 수집, 처리, 배포하는 플랫폼에서 비식별화에 의한 개인정보보호도 주요 기술 이슈로 인식되고 있다.

현재는 IoT 단말 제작회사들이 제공한 오픈 하드웨어 형태의 통합개발 환경을 이용한 다양한 D.I.Y 보안 디바이스가 개발되고, 저전력/경량 IoT 디바이스용 RTOS(tinyOS, Contiki, RIOT 등)에서 링크 계층의 메시지 무결성 및 암호기능이 제공되었다. M2M 기기 인증 및 신뢰통신 보안 서비스 제공기술도 연구 개발이 진행중인데, Gemalto가 M2M 기기용 기기 인증 및 보안 기능을 제공하는 임베디드 SIM을 개발하고 있다.

또한, IoT 연결성 플랫폼인 퀄컴의 Alljoyn은 앱 단위의 기본적인 인증, 암호 기능을 제공하고, 인텔, 어드벤택, 유로텍, 프리스케일 등이 다수의 IoT 게이트웨이를 출시하고 있으나, 상이한 HW 자원 통신방식 보안구조를 지원하는 초연결성 보안 기능은 미탑재된 상태이다.

이에 따라, 차세대 IoT 보안영역에서는 보안이 취약한 경량 디바이스로 구성된 IoT에 트러스트 보안중심센터 기능을 제공하는 경량 IoT 보안 게이트웨이 및 초연결 기기에 대한 무인원격 보안관리 서버기술 개발이 필요하며, HW 제약·성능 등이 상이한 이기종 디바이스를 위한 기기 맞춤형 보안 운영체제와 경량/저전력 디바이스 성능, 응용에 특화된 보안 HW 모듈 등 IoT 디바이스의 고가용성 보장을 위한 보안 기술 개발이 요구된다.

클라우드/빅데이터 기반 IoT 서비스 환경에서는 보안 연동 및 프라이버시 보호를 위한 크로스도메인 IoT 경량 보안 서비스 플랫폼 기술이 확보되어야 하며, 경량형 IoT 기기의 취약점을 이용한 해킹에 의한 기기 비인가 접속을 제어하고 통신 상의 데이터를 보호하여 사이버 상의 위협을 방어하는 경량형 인증/접속제어 및 관제 시스템기술이 중점 개발될 것으로 보인다[8].

이와 함께 5G 이동통신망과 연계되어 Pre-5G 통신 기반 코어망 보안 기술, LPWAN 침입방지 기술, 이기종 IoT 무선 네트워크 보안을 위한 원격 신뢰 접속 제어 Secure GW 기술 개발 등도 주요 연구개발 분야이다.

바. 클라우드 보안

클라우드 컴퓨팅 기술은 IoT에서 수집된 대규모의 데이터를 처리하기 위한 고기능 클라우드 인프라 기술과 인공지능기술을 활용한 클라우드 플랫폼 운영기술 개발이 중심을

이루고 있으며, 클라우드 자체를 보호하기 위해 SecaaS 및 가상화 기반에 보안기능을 제공하여 보안 서비스의 유연성 확보, 클라우드 환경에서의 보안기능 지능화, 보안 기능의 동적 구성이 가능한 고성능 보안 가상화 플랫폼 기술 개발이 추진되고 있다. 특히, SDsec 및 NFV 환경에서 보안기능의 동적 재구성, 고성능 제어, 가시성을 확보하기 위해 네트워크 하이퍼바이저, 컴퓨팅과 네트워킹이 결합된 서버-스위치 등 고성능 클라우드 보안 플랫폼 기술 개발이 진행 중이다.

클라우드 아키텍처 레이어별 취약성 분석 및 공격 시나리오 연구에서 가상화 네트워크 침해대응 기술 개발에 이르기까지 솔루션 공급이 확대될 것으로 예상되나 인프라 보안 기술 개발은 미흡한 상태이므로, IoT 기기의 상태와 보안위협 정보를 수집하여 대량의 데이터를 고속 처리와 분석 데이터를 확보하기 위한 기술 개발이 요구된다.

사. 5G/모바일 보안

5G 네트워크의 최대 잠재 속도는 20Gbps이고, 통상적으로 10Gbps의 속도를 유지하기 위해 인빌딩 및 지하공간용 소출력 이동통신 중계기 개발, LED-ID를 이용한 근거리무선통신 시스템 홈네트워크 기술 개발, 2GHz대역 LTE/WLAN AP용 적응형 빔형성 안테나 시스템 개발 등과 같은 이동통신시스템 성능을 향상시키는 연구가 중점 추진될 것으로 전망된다.

이에 맞추어 5G 모바일 보안에서는 국제기구를 중심으로 DDoS 공격 대응과 LTE 내의 공격 없는 라디오 접근망으로부터 5G 내 다중 통신망 레벨의 취약점이 존재함에 따라 5G 보안 구조, 접근 제어, 프라이버시보호, 보안 모니터링 및 관리, 5G 보안 표준화 등이 연구되고 있다.

아. 블록체인

블록체인 기술 분야에서는 다양한 합의 알고리즘들의 한계점과 불안전성, 낮은 거래처리 성능, 거버넌스 부재로 인한 하드포크 발생 등을 고려하여 BOScoin, ICON, 그라운드X, 블로코 등이 플랫폼 개발을 진행중이다. 주요 프로젝트로서는 D-CENT(Decentralized Citizens Engagement Technology)의 분산형 시민 참여 플랫폼 개발(2016), DECODE(Decentralized Citizen Owned Data Ecosystem)의 스마트 계약 기반의 분산형 시민 소유 데이터 생태계 구축, MHMD(My Health My Data)의 개인 건강 데이터의 소유권/

통제권 보장, BLOOMEN(Blockchains in the new era of participatory media experience)의 블록체인 기반 콘텐츠 보안, SHOGANAI(World's first real-time solution for controlling airplane operating costs)의 항공기 운영 데이터와 블록체인 원장 기록을 통한 항공사와 협력업체간 스마트 컨트랙트에 기반한 청구서 자동 생성 등의 기술개발이 보고되고 있다[9].

자. 스마트 융합 인프라 보호

스마트 융합 인프라 보호기술은 IoT, 클라우드, 빅데이터, 증강현실 등의 첨단기술들이 도시 자원과 융합적으로 연동되기 때문에 생명 위협 및 생산 중단과 직결되는 보안 기술영역이다.

스마트시티 보안기술은 미국이 앞서고 있지만, 전기나 수도, 가스를 커버하는 AMI (Advanced Metering Infrastructure) 기술은 EU에서 활발하게 연구되고 있다. 주요 기술개발 과제로는 암호화 및 디지털 서명을 사용하여 소프트웨어의 무결성을 보장하고, 카메라 및 스마트 장치에서 수집한 데이터의 도청, 차단 및 수정을 방지하기 위한 기술들이 있으며, IoT를 활용한 생활 안전, 재난 모니터링 예측, 재난 대응 로봇 개발 등이 추진중이다[7].

SCADA 보안은 산업시스템 연계구간별 보안, 네트워크 침입탐지, 암호인증, 보안취약점 탐지 기술이 중점 연구되고 있다. 산업제어시스템 연계구간에서는 망의 완전분리를 구현하기 위한 물리적 단방향 보안게이트 기술과 도메인 간의 안전한 자료 전달에 필요한 CDS(Cross Domain Solution) 기술들이 중점 개발되고 있다.

한편, 자율주행차 보안기술은 전용 OS를 갖춘 IT 플랫폼이 외부 네트워크에 연결되어 있어 각 통신구간에서 보안사고가 발생할 경우 운전자 생명, 교통혼란 등 치명적인 사회재난으로 연결될 수 있기 때문에 자동차/개인프라이버시 보호, 안티 멀웨어, 블록체인 기반 키관리, 코드 난독화, 고속 서명 등의 보안기술이 중점 개발될 전망이다. 그리고 스마트카의 보안기술 품질을 보증하기 위해 개발 전주기 과정의 보안성 시험 기술과 클라우드 기반의 보안 서비스 기술도 개발될 전망이다[5].

Ⅳ. 결론

차세대 보안기술은 대용량 초고속의 트래픽을 유발하는 IoT와 5G로 구성된 초연결 CPS 인프라에 대한 초신뢰를 실시간 대응방식기술로 대응하는 방향으로 나가고 있다. 특히, 사이버 공격자들이 AI 기반의 자동화 도구를 사용하여 메가 공격을 할 것이 예상되므로, 방어자 측면에서도 AI 기반의 실시간 대응이 필수적이다. 이를 위해 AI 기반의 위협정보 빅데이터 수집, 처리, 분석기능을 자동화하고 실시간 모니터링과 리포팅 체계를 구현하는 SOAR와 새로운 경량 암호인증에 의한 화이트리스트 기반의 Zero Trust를 구현하는 기술이 주류를 형성할 것으로 전망된다. 이러한 사이버 보안기술의 차세대 발전 방향은 사이버보안 엔지니어들에게는 기밀성, 무결성, 가용성 보장이라는 기존 사이버보안 기술영역을 넘어선 것이므로 머신러닝이나 딥러닝과 같은 AI/빅데이터 기술 역량을 대폭 강화해야 할 것으로 판단된다.

[참고문헌]

[1] 과학기술정보통신부, “민간부문 정보보호 종합계획”, 2019, pp.8-12, pp.19-21.
[2] IITP, “ICT 기술수준조사보고서”, 2018, pp.154-155, pp.167-174
[3] 중소기업벤처부, “중소기업 기술로드맵(2018~2020)”, 2018, pp.6-15, pp.35-37.
[4] TTA, “차세대보안”, ICT 표준전략맵, 2019, pp.305-313.
[5] 과학기술정보통신부/IITP, “지능형 자동차 보안 위협 및 대응방안 보고서”, 2017, pp.28-30.
[6] BISTEP/부산가톨릭대, “ICT 융합 생활안전플랫폼 기술기획”, 2018, pp.9-29.
[7] 김도우, “융합보안 기술 및 특허동향”, IITP, 주간기술동향, 2017. 6, pp.17-19.
[8] 김정녀, “스마트 홈/시티 IoT 인프라 및 차세대 IoT 보안 기술”, ETRI, 2018, pp.21-25.
[9] 정성교, “블록체인 기술 및 연구 동향 분석(TM)”, KERC. 2018. 7, pp.4-10.
[10] White House, “National Cyber Strategy”, 2018, pp.6-13.
[11] Check Point, “Step Up to Gen V Cyber Security,” 2019. 8.
[12] Gartner, “Global Information Security Spending To Exceed $124B In 2019,” 2019. 4.
[13] Gartner, “Top 10 Security Project,” 2018. 12.
[14] Gartner, “Hype Cycle for Risk Management,” 2018. 7.
[15] CBInsights, “Cybersecurity’s Next Frontier,” 2017. 6.
[16] Gartner, “Innovation Insight for a Safety Critical, Safety Critical Practice,” 2016. 10.
[17] 보안뉴스, “2019년을 이끌 차세대 보안기술 9가지”, 2018. 11.
[18] 보안뉴스, “차세대 보안을 위해 연구해야 할 R&D 보안기술 6가지”, 보안뉴스, 2018. 11.

chapter 2

산업제어시스템의 국가별 사이버 보안 현황

강민균 ‖ ㈜소프트아이텍 수석연구원

I. 서론

산업제어시스템(Industrial Control Systems: ICS)은 산업 공정 제어에 사용되는 여러 유형의 제어시스템 및 관련 계측시스템을 의미한다. 또한, ICS는 감시 제어 및 데이터 수집(Supervisory Control and Data Acquisition: SCADA) 시스템, 분산제어시스템(Distributed Control System: DCS), 프로그래머블 로직 컨트롤러(Programmable Logic Controller: PLC) 등을 활용하여 구현되며 기반 시설 및 공장 등의 대규모 시설부터 제어 루프가 거의 없는 소규모 시스템까지 구성할 수 있다[1]. 이러한 ICS는 일반적으로 전력, 운송, 물, 가스 및 기타 중요한 인프라와 관련된 물리적 프로세스를 제어한다.

이렇게 중요한 인프라에 사용되는 ICS는 100%의 가용성이 필요하다는 것을 의미하므로 보안 업데이트와 같은 이유로 시스템을 중단시키는 것은 매우 어렵고 비용이 많이 든다. 전력, 물, 가스 같은 경우는 서비스가 중단될 경우 수백만의 사람들에게 영향을 줄 수 있다. 또한, 원자로를 사용하는 시설(원자력 발전소 등)의 경우, 일반적으로 가동 주기를 18개월로 하고 있으며, 가동 중지 시 시간당 약 33,000 파운드의 비용이 소모된다.

* 본 내용은 강민균 수석연구원(☎ 042-520-8133, mgkang@sit21c.com)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

기존의 IT(Information Technology) 시스템과 ICS는 사이버보안 측면에서 보안 목적, 네트워크 분할, 네트워크 접속 방식, 기능 분할 파티션, 물리적 구성요소, 사용자 계정, SIS(Safety Instrumented System), 소프트웨어, 패치작업, 보안 인식까지 10가지 관점에서 차이점을 보이고 있다[2]. 따라서 기존의 정보시스템 분야에서 활용하고 있는 보안 방식을 ICS에 적용하기에는 한계가 있다.

사이버보안 분야의 선진국들은 이미 보안 취약점에 대해 다양한 관점에서의 약점을 체계적으로 도출할 수 있는 보안 평가 도구에 대한 방법을 제안하였고, 현재 사용하고 있다. 미국의 국립표준기술연구소(National Institute of Standards and Technology: NIST)에서는 ICS의 사이버보안을 위한 규제치짐 표준안들을 개발하여 제공하고 있으며[1], 사이버보안 및 인프라보호기관(Cybersecurity and Infrastructure Security Agency: CISA)에서는 ICS의 사이버보안 평가 도구인 CSET(Cyber Security Evaluation Tool)를 제공하고 있다. 또한, 일본의 JPCERT/CC(Japan Computer Emergency Response Team Coordination Center)는 간단하게 평가 항목을 제공하는 SSAT(SCADA Self Assessment Tool)를 개발 및 제공하고 있다.

이와 같이 여러 국가에서는 현재 운영하고 있는 ICS에 대한 사이버 위협에 대응하기 위해 센터를 설립하여 사이버보안 지침을 제정하고, 인력양성, 인증된 컨설턴트들의 사이버보안 컨설팅, 공인 교육, 공인 학위, 침투 테스트, 상용제품 보증(CPA), CC(Common Criteria) 인증 등을 진행하고 있다. 본 고에서는 ICS 사이버보안과 관련한 세계적인 추세와 국내 현황을 살펴보았으며, 향후 대응 방안을 모색하였다.

II. ICS 사이버보안 현황

1. 사이버보안 및 인프라보호기관(미국)

미국 CISA는 사이버 위협으로부터 방어하기 위해 파트너들과 협력하고 미래를 위해 보다 안전하고 탄력적인 인프라를 구축하기 위해 기존 US-CERT(U.S. Computer Emergency Readiness Team)와 ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)를 2018년 통합하여 설립된 기관이다.

CISA는 이해 관계자들에게 광범위한 사이버보안 및 인프라 보안 지식과 정보를 제공하고, 그 지식을 공유하여 더 나은 위험 관리를 가능하게 하고, 국가의 필수 자원을 보호하기 위해 연방 네트워크 보호, 종합적인 사이버 보호, 인프라 복원력 및 현장 운영, 비상 통신을 수행한다.

표준과 관련하여, 미국 ISA의 표준기구인 ASCI(Automation Standards Compliance Institute) 산하에 ISCI(ISA Security Compliance Institute Society Interest Group)를 구성하고, ICS 환경에 적합하도록 보안요구사항 및 위험분석에 따른 보안대책을 특성화한 ISA-62443을 국제표준으로 등록하였다.

또한, 미국의 NIST에서는 ICS의 사이버보안을 위한 규제지침 표준안들을 개발하여 제공하고 있으며, 대표적인 문서는 NIST Special Publication 800-82로서, SCADA시스템, DCS 및 PLC와 같은 제어시스템 구성을 포함하여 ICS를 보호하는 방법에 대한 지침을 제공한다. 이 문서는 ICS 및 일반적인 시스템 토폴로지에 대한 개요를 제공하고 이러한 시스템에 대한 일반적인 위협 및 취약성을 식별하며 관련 위험을 완화하기 위한 권장 보안대책을 제공한다. 이 문서는 유럽, 영국, 일본, 한국 등 여러 나라에서 인용되어지고 있으며, 각 국가의 지침을 만드는데 영향을 주고 있다[1].

2 유럽연합사이버보안기구(유럽)

유럽연합사이버보안기구 ENISA(European Union for Cybersecurity)는 그리스 아테네와 헤라클리온에 위치하고 있으며, 유럽연합의 사이버보안을 유지하고자 2004년 설립된 기관이다.

ENISA는 유럽 사이버보안 정책을 수립하고 EU 회원국이 2개 이상 영향을 받는 경우 국경을 넘는 대규모 사이버 사고에 대응할 수 있도록 지원하고 있다.

또한, ENISA는 네트워크 및 정보 보안과 관련된 문제에 관한 유럽연합의 정책 및 법률의 개발 및 구현을 지원하며, 회원국과 유럽연합 기구 및 기관이 자발적으로 취약성 공개 정책을 수립하고 구현할 수 있도록 지원하고 있다.

2019년부터 사이버보안법(규정 2019/881)이 시행된 이후 ENISA는 제품, 프로세스 및 서비스의 전달을 지원하는 “유럽 사이버보안 인증 체계”를 준비하고 있다[2].

3. 국가기반보호센터(영국)

영국의 경우 국가기반보호센터(Centre for the Protection of National Infrastructure: CPNI)에서 정의한 국가 인프라는 국가가 기능하고 일상생활에 의존하는 데 필요한 시설, 시스템, 사이트, 정보, 사람, 네트워크 및 프로세스이다. 여기에는 필수 서비스는 아니지만 잠재적인 위험(예; 원자력 및 화학 시설)으로 인해 보호가 필요한 일부 기능, 시설 및 조직도 포함된다. 또한, 13개의 국가 인프라 부문으로 화학, 국방, 응급 서비스, 에너지, 금융, 식품, 정부, 건강, 우주, 운송 및 물을 정의하였으며, 위협 요소로 사이버, 스파이활동, 테러, 대량 살상 무기, 조직 범죄 등으로 분류하여 대응하고 있다. 사이버 위협에 대한 대비는 국립사이버보안센터(National Cyber Security Centre: NCSC)에서 대응하고 있다. NCSC는 다양한 제품, 서비스 및 조직을 포괄하는 인증을 제공하고, 정책 표준을 충족시키는 공인 지원 제품(Certified Assisted Products: CAPS), 인증된 컨설턴트들(Cyber Security Professionals: CCP)의 사이버보안 컨설팅, 공인 교육, 공인 학위, 침투 테스트, 상용제품 보증, CC 인증, 보증된 서비스(Cyber security Assured Services: CAS)를 제공하고 있다[3].

4. IPA 산업사이버보안센터(일본)

일본은 경제·사회를 지탱하는 중요한 인프라 및 산업 기반의 사이버 공격에 대한 방어력을 근본적으로 강화하기 위해 2017년 4월 1일 IPA(Information-technology Promotion Agency) 예하에 산업사이버보안센터(Industrial Cyber Security Center of Excellence: ICSCoE)를 출범시켰다. 산업사이버보안센터는 모의 발전소를 활용하여 사이버 공격과 방어를 수행하는 해킹방어대회를 통해 인력을 양성하고, 최신 사이버 공격 정보의 조사·분석 등을 통해 사회 인프라·산업 기반의 사이버보안 위험에 대응하는 인재·조직·시스템 기술을 만들고 있다. 일본의 사회 인프라 산업 기반과 관련한 제어시스템의 안전성·신뢰성에 대한 리스크 평가를 실시하고, 모든 공격 가능성을 확인하고 필요한 대책을 수립하고 있다.

또한, ICSCoE에서는 제어시스템을 위한 사이버보안 교육과 사회 인프라 및 산업 기반의 사이버보안 인재 육성 등에 대한 보고서를 제공하고 있으며, 다음과 같이 지침과 도구를 제공하고 있다.

- 제어시스템 환경에서 사이버보안 문화의 지원을 목적으로 한 운영 보안(OPSEC)의 사용: 2010년 대부분의 조직은 제어시스템 영역에서도 강력한 아키텍처를 채용하여 사무망과 제어망 통합을 추진함으로써 업무의 강화와 비용 절감을 도모하고 있다.
- NIST SP 800-82 산업제어시스템(ICS) 보안: SCADA 시스템, 분산제어시스템(DCS), 프로그래머블 로직 컨트롤러(PLC) 등을 포함한 산업제어시스템의 보안을 확보하기 위한 지침이 정리되어 있다. 이 지침은 산업제어시스템의 전형적인 시스템 토폴로지 위협과 취약성, 그 해결 방법을 정리하고 있다.
- IEC(ISA) 62443 시리즈: 제어시스템 분야에서도 다양한 보안 기준이 책정되어 있다. 개별 산업 분야(전력, 교통, 석유 화학 등)에 특화된 표준 및 업계에 의존하지 않고 범용적으로 활용할 수 있는 기준으로 ISA 62443을 이용하고 있다. ISA 62443은 첫째로 기본적인 용어 및 보안 생명주기를 설명하고, 둘째로 조직 및 정책에 필요한 절차 및 프로세스를 제시하고, 셋째로 ICS 시스템에 적용하기 위한 보안 기술 및 보안 기능 요구사항을 제시하고, 마지막으로 ICS 컴포넌트의 보안 기능 요구사항 및 절차/프로세스를 제시하고 있다[4].

5. 호주신호정보국(호주)

호주는 호주신호정보국(Australian Signals Directorate: ASD) 예하에 ACSC(Australian Cyber Security Center)를 2014년 설립하여 타 국가, 학계 및 전문가와 협력하여 사이버보안 위협에 대한 솔루션을 연구 개발하고 있다. 현재 사이버보안 문제에 관해 약 200여 개의 파트너와 협력하여 국가적 생태계를 구축하고 있으며, 사이버 범죄와 싸우기 위해 법 집행기관과 협력하고 있다.

ACSC에서는 마시는 물, 전기 및 운송 수단을 통제하는 산업제어시스템에 대한 사이버 위협을 완화하여 필수 서비스가 모든 사람에게 지속적으로 제공되도록 다음과 같은 전략을 수립하였다.

- 제어시스템 네트워크에 대한 외부 액세스를 엄격하게 제어하거나 방지하고, 회사 네트워크 및 인터넷과 같은 다른 네트워크와 분리
- 권한 있는 계정 및 회사 또는 외부 네트워크에서 시작된 액세스에 대한 2단계 인증을 구현

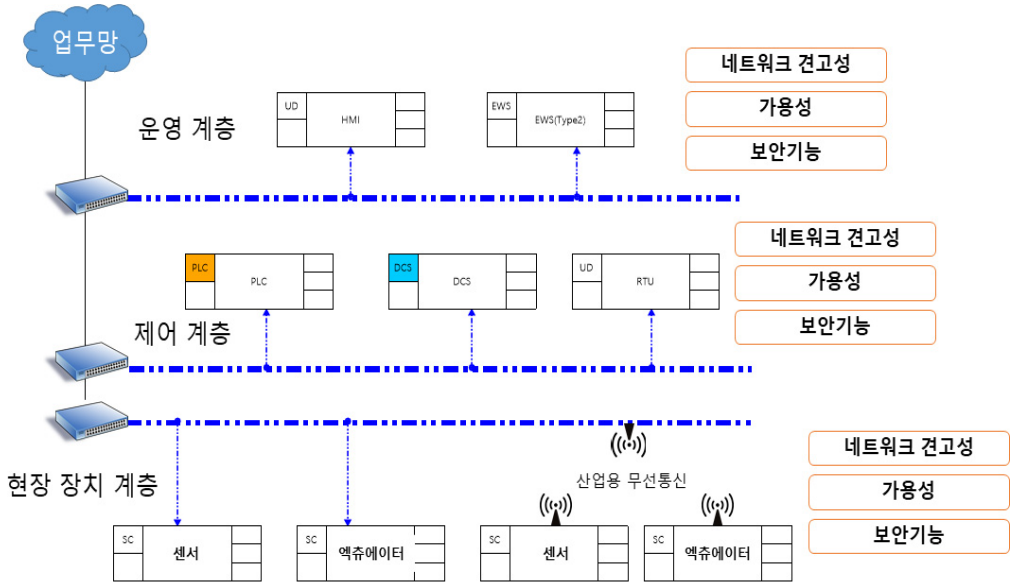
- 제어시스템 장치에서 사용하지 않는 외부 포트를 비활성화
- 조직 고유의 안티 탬퍼 스티커를 사용하여 제어시스템 환경 내부의 승인된 장치를 눈에 띄게 표시
- 시스템 구성을 정기적으로 백업 및 격리하고, 복원 절차를 테스트하고 정기적으로 백업 무결성을 확인
- 방화벽 설정을 정기적으로 검토하여 정상 상태를 유지
- 제어시스템 네트워크 내부의 장치가 회사 네트워크나 인터넷에 연결되지 않도록 유지
- 제어시스템 장치에서 로깅을 활성화하고 중앙 위치에 로그를 저장하고 정기적인 모니터링 및 사고 대응 사례를 연구하여 이상을 식별, 조사 및 관리
- 외부 소프트웨어 및 패치를 제어시스템에 도입하는 프로세스를 정의하고, 필요한 경우 코드를 검토하고 승인된 바이너리를 허용
- 공급 업체 지원 응용 프로그램 및 운영 체제를 사용하고 관련 보안 취약점을 적시에 패치

이러한 전략을 이행하기 위한 세부자료로 미국 ICS-CERT의 “Seven steps to effectively defend industrial control systems”, DOE의 “21 steps to improve cyber security of SCADA networks”, NIST의 “Guide to industrial control system(ICS) security (PDF)”를 추가 자료로 공고하고 있다[5].

6. 국가보안기술연구소(한국)

국내의 경우 한국전자통신연구원의 부설연구소인 국가보안기술연구소에서 한국정보통신기술협회에 “ICS 보안 요구사항”이라는 표준으로 2017년 등록하였으며, 이 표준에서는 3계층, 즉 운영 계층, 제어 계층, 현장장치 계층으로 구성하고 ICS의 보안요구사항을 정의하였다.

ICS는 기존의 IT시스템과 달리 가용성의 중요도가 매우 높다. 이 표준에서는 이와 같은 특징을 반영하여 ICS 보안 개념과 보안참조모델을 [그림 1]과 같이 정의하였다. 이 표준은 [표 1]과 같이 ICS의 보안 요구사항을 현장장치 계층, 제어 계층, 운영 계층별로 분류하여 정리하였다. 보안 기능에 대한 분류의 명칭은 동일하지만 세부 보안 요구사항은 각 계층별로 상이하며, 세부 보안 요구사항을 계층별로 정의하여 상황에 적절하게 활용할 수 있도록



[그림 1] ICS 보안참조모델

[표 1] ICS 보안 요구사항 정리

구분	현장장치 계층	제어 계층	운영 계층
네트워크 견고성	퍼징 테스트	퍼징 테스트	퍼징 테스트
		스트레스 테스트	-
서비스 지속성	자원 가용성	자원 가용성	자원 가용성
	물리적 인터페이스 보호	물리적 인터페이스 보호	-
	이벤트 대응	이벤트 대응	이벤트 대응
보안 기능	보안 감사	보안 감사	보안 감사
	식별·인증	식별·인증	식별·인증
	접근 통제	접근 통제	접근 통제
	전송 데이터 보호	전송 데이터 보호	전송 데이터 보호
	저장 데이터 보호	저장 데이터 보호	저장 데이터 보호
	보안 기능 관리	보안 기능 관리	보안 기능 관리
	상태 관리	상태 관리	상태 관리
세부 보안 요구사항	52개	57개	55개

〈자료〉 TTAK.KO-12.0307(ICS 보안요구사항)

기술하였다. 이러한 요구사항은 기술적으로 도입하는데 시간이 필요하며 그에 따른 추가적인 전략이 필요하다[6].

III. 결론

ICS에 대한 각 국의 사이버보안 동향을 분석한 결과, 국가마다 차이는 있지만 공통적으로 센터를 설립하여 지침을 제정하고, 인력양성, 인증된 컨설턴트들의 사이버보안 컨설팅, 공인 교육, 공인 학위, 침투 테스트, 상용제품 보증(CPA), Common Criteria 인증을 진행하고 있는 것으로 나타났다. 국내의 경우 IT산업의 경우 사이버보안을 담당하는 기관은 있지만 ICS 산업은 준비 중인 것으로 확인되었다. 향후 국내에서 이에 대응하기 위해서는 다양한 노력이 필요하다. 이를 위해 다음과 같은 연구가 필요할 것으로 예상된다.

첫 번째로, 실증시설 확대 구축 및 인력양성이 필요하다. 현재 국내기관에서 실증시설을 구축하고 운영하고 있으나 이용에 한계가 있어 확대 구축이 필요하다. 또한, 이렇게 확대 구축된 실증시설을 활용하여 ICS 보안사고 매뉴얼 개발 및 정보 공유 체계 마련, ICS 보안사고 대응훈련 방안 마련, ICS 정보보호대책의 효과 검증, ICS 융합 보안 전문 인력 양성을 추진해야 할 것이다.

두 번째로, 시험 도구 및 평가 기술 개발이 필요하다. 해외 일부 국가에서는 국가 차원에서 평가 도구 및 시험 도구를 개발하고 있다. 그러나 사이버보안 측면에서 외산 제품을 활용하는 부분은 한계가 있으며 국내 환경에 맞는 신뢰할 수 있는 기관이 제공하는 국산 제품이 필요하다. 이러한 시험 도구 및 평가 기술을 활용하여 ICS 보안성 평가기술 개발, 보안성 검증 패턴정보, 프로토콜별 시험 시나리오, 운영환경별 시험 시나리오 등으로 활용할 필요가 있다.

[참고문헌]

[1] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn, “Guide to Industrial Control Systems(ICS) Security,” NIST, NIST SP 800-82, 2015. 1.

[2] 강민균, “IT, IoT, ICS에 대한 보안 관점에서의 현황 및 차이점”, IITP, 주간기술동향 1813호, 2017. 9.

[3] Louis Marinos, Marco Lourenco, “ENISA Threat Landscape Report 2018,” ENISA, ETL

2018, 1, 2019.
[4] HM Government, “National Cyber Security Strategy 2016-2021,” 2016. 11.
[5] Information-technology Promotion Agency, “Security Risk Assessment Guide for Industrial Control Systems,” 2018. 4.
[6] Australian Cyber Security Centre, “Threat Report,” 2017. 2, p.24, p.32.
[7] 이종후, 조영준, 최승오, 박경미, 신동훈, 김경민, 민법기, 이진경, 김우년, 오흥룡, “ICS 보안요구사항”, 한국정보통신기술협회, TTAK.KO-12.0307, 2017. 6. 28.

chapter 3-1

병원 내 중대 이벤트 예측 시스템

최재식 ‖ 울산과학기술원 교수

I. 결과물 개요

개발목표시기	2019. 12.	기술성숙도(TRL)	개발 전	개발 후
			TRL 4	TRL 8
결과물 형태	SW	검증방법	의료기기 인증 및 전향 검증	
Keywords	Sepsis, severe sepsis, septic shock, mortality prediction			
외부기술요소	Open Source 기반	권리성	SW	

II. 기술의 개념 및 내용

1. 기술의 개념

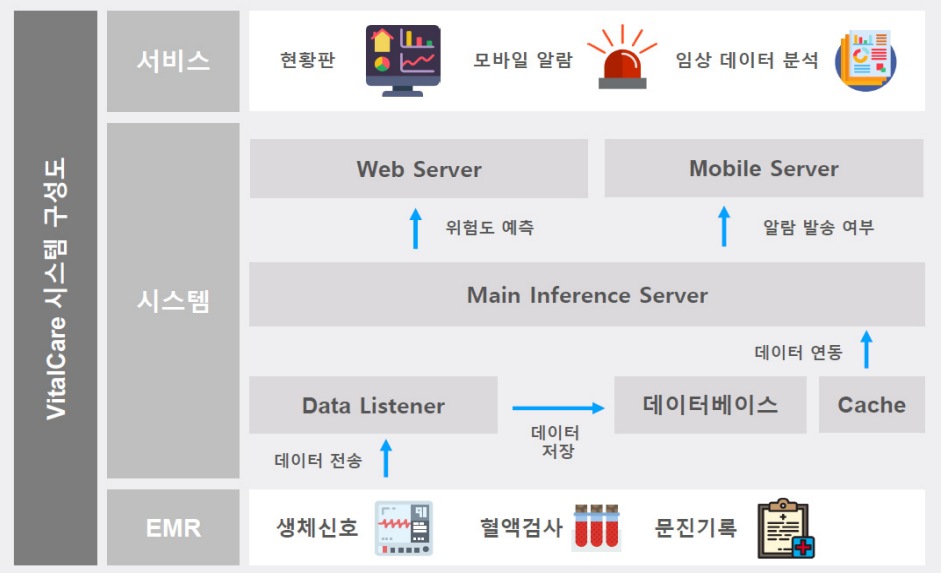
➢ 본 시스템은 해석 가능한 딥 컨볼루셔널 뉴럴 네트워크를 기반으로 패혈증 등 주요 이벤트를 조기에 예측하여 환자의 예후 향상을 도모하는 소프트웨어로서, 환자의 위험

* 본 내용은 최재식 교수(☎ 052-217-2144)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***정보통신기획평가원은 현재 개발 진행 및 완료 예정인 ICT R&D 성과 결과물을 과제 종료 이전에 공개하는 "ICT R&D 사업화를 위한 기술예고"를 2014년부터 실시하고 있는 바, 본 칼럼에서는 이를 통해 공개한 결과물의 기술이전, 사업화 등 기술 활용도 제고를 위해 매주 1~2건의 관련 기술을 소개함

도를 실시간으로 산출하여, 고위험군을 쉽게 파악할 수 있는 대시보드와 이를 통한 모바일 알람 등 다양한 기능을 포함하여, 임상 현장에 종사하는 의사, 간호사의 업무 효율 향상에 실질적으로 기여하고자 함

2. 특징 및 장점

- 임상적으로 유의미한 예측 결과를 제공하기 위해, 후향 데이터를 통해 머신러닝 모델을 학습할 때부터 엄격한 조작적 정의를 통해 데이터의 레이블을 결정하며, 이를 기반으로 해석 가능한 딥 네트워크를 학습하였기 때문에 전향 검증에서 본 시스템 사용 시 환자 예후가 향상되는 결과를 기대할 수 있음
- 본 시스템은 중환자실용 모델, 일반병동용 모델로 세분되어 있으며, 중환자실용 모델은 한 시간 간격으로 입력되는 활력 징후, 하루 간격으로 입력되는 혈액 검사 수치를 기반으로 패혈증 및 사망 여부를 조기에 예측하며, 일반병동용 모델은 8시간 간격으로 입력되는 활력 징후, 비정기적으로 입력되는 혈액 검사 수치를 기반으로 머신러닝 모델을 학습



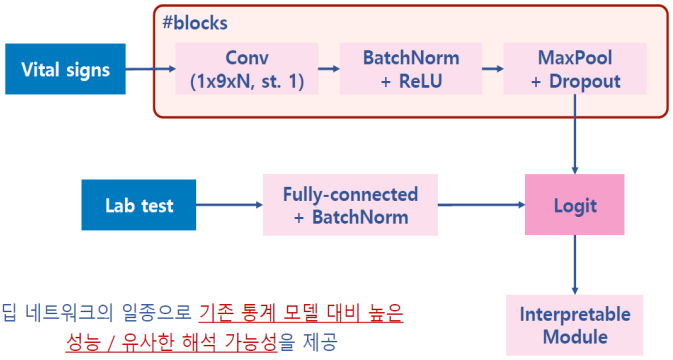
[그림 1] 시스템 구성도

➢ 이벤트 발생 예측값을 생성하기 위해 24시간 데이터만을 활용하기 때문에 컨볼루셔널 네트워크 기반으로 모델을 설계하였으며, 이벤트별 위험 인자를 추출하기 위해 해석 가능 모듈을 결합하여 임상적으로 유의미한 위험 인자를 도출함

3. 기술의 상세내용 및 사업화 제약사항

➢ 기술의 상세내용

- 본 제품의 명칭은 VitalCare이며, 사망 또는 패혈증 위험도 예측 방법 및 이를 이용한 현황판 제작, 모바일 알람 발송 기술을 포함함



[그림 2] 예측 모델 구성도

[표 1] 중환자실, 일반병동, 응급실을 기준으로 VitalCare에서 제공하는 주요 기능 요약

경쟁기술	대시보드	알람 발송	RRT 활동기록 자동화
중환자실	O	-	-
일반병동	O	O	O
응급실	O	O	-

➢ 사업화 제약사항

- 의료수가 인정을 위해서는 의료기기 인증 및 신의료기술평가를 통과해야 하며, 본 시스템을 사용할 때 환자의 예후가 유의미하게 향상되는지를 전향적으로 엄격하게 검증해야 함

III. 국내외 기술 동향 및 경쟁력

1. 국내 기술 동향

➢ 아산병원과 아주대에서 패혈증을 RNN 및 MLP 기반으로 조기에 예측하는 모델을 개발함

- "Learning Representations for the Early Detection of Sepsis with Deep Neural Networks," Computers in Biology and Medicine, 2017

2. 해외 기술 동향

➢ Dascena는 미국 스타트업으로, 중환자실 후향 데이터 중 활력 징후와 혈액 검사 수치를 기반으로 개발한 패혈증 조기 예측 모델(제품명 Insight)을 개발하였으며, 현재 해당 모델을 전향적으로 검증하고 있으며, 사업화를 진행 중임

- "A Computational Approach to Early Sepsis Detection," CBM. 2016.
- "Prediction of Sepsis in the Intensive Care Unit with Minimal Electronic Health Record Data: A Machine Learning Approach," JMIR. 2017.
- "Multicenter Validation of a Sepsis Predicton Algorithm using Only Vital Sign Data in the Emergency Department, General Ward, and ICU," BMJ Open. 2018.

3. 관련 보유 특허

No.	국가	출원번호(출원일)	상태	명칭
1	대한민국	10-2018-0120238(2018-10-10)	출원	사망 또는 패혈증 위험도 예측 방법 및 이를 이용한 사망 또는 패혈증 위험도 예측용 디바이스

4. 기술적 경쟁력

경쟁기술	본 기술의 우수성 및 차별성
주요 이벤트 예측 모델	베이지안 최적화를 통한 하이퍼-파라미터 탐색으로 모델의 예측 성능 극대화 및 변분 드롭아웃을 통해 모델 과적합 자동 방지
해석 가능 모듈 결합	중대 이벤트 발생의 위험 인자를 모델이 자동으로 찾고, 임상적으로 유의미한지를 검증하여 모델의 신뢰성 향상

IV. 국내외 시장 동향 및 전망

1. 국내 시장 동향 및 전망

➢ 머신러닝 기술을 통한 의료 영상 분석 연구가 스타트업 및 학계에서 활발히 연구되고 있으며, 주요 시장에서 선도업체들이 이미 존재하면서 산업화 초입단계로 평가됨

➢ 국내의 경우 Lunit, Vuno가 시장을 선도하고 있으며 흉부 X-ray 판독, 뼈나이 판독, 안저 영상 분석 등을 개발하여 의료기기 인증을 진행함

2. 해외 시장 동향 및 전망

➢ 머신러닝 기술을 임상 현장에 적용하여 임상의 및 간호사의 업무 효율을 향상시키고 환자 예후 향상을 도모하고자 하는 연구가 기업 및 병원에서 활발하게 진행되고 있음

- ExcelMedical은 미국에서 1996년에 설립된 기업으로, 통합 의료기기시스템과 환자 모니터링 솔루션 개발에 집중하고 있으며, 대표 제품으로 심장 질환 관련 환자의 활력 징후를 모니터링하여 의료진에게 실시간으로 알람을 발송하는 플랫폼을 보유 (제품명: WAVE)
- EarlySense는 이스라엘에서 2004년에 설립된 기업으로, 비접촉 감지시스템 개발 및 분석 솔루션을 제공하고 있는데, 환자의 활력 징후를 비접촉 센서로 측정하여 위험 상황을 조기에 알려주는 플랫폼이 대표제품임
- PeraHealth는 미국에서 2014년에 설립된 기업으로, 임상적으로 검증된 Rothmann

Index를 개발하여 환자의 건강 상태를 실시간으로 정량적 지표로 판단하여 고위험군을 쉽게 파악할 수 있는 현황판 솔루션을 보유

- 머신러닝 기반 의료 영상 분석 솔루션과 관련하여, 미국 시장은 Zebra Medical, 중국 시장은 VoxelCloud가 시장을 선도함

3. 제품화 및 활용 분야

활용 분야(제품/서비스)		제품 및 활용 분야 세부내용
1	조기 진단을 통한 환자 예후 개선	패혈증 등을 조기에 예측함으로써 적절한 치료를 제공할 수 있음
2	RRT 업무 효율 개선	일반병동 조기대응팀(RRT) 출동 우선순위 설정에 도움을 줌

V. 기대효과

- VitalCare 솔루션 상용화를 통해 해당 제품 사용 시 환자 예후가 개선된다는 점이 전향적으로 입증된다면 의료수가 인정을 통해 의료 산업에 큰 파급효과를 줄 것으로 기대
- EHR 분석 솔루션 시장 규모가 국내외 모두 지속적으로 성장 중이므로, 초기 시장을 선점한다면 향후 국내에서 개발된 머신러닝 기반 의료기기의 국제적 경쟁력을 확보할 수 있음

chapter 3-2

머신러닝 기반 녹내장 진단 기술

오세종 ‖ 단국대학교 교수

I. 결과물 개요

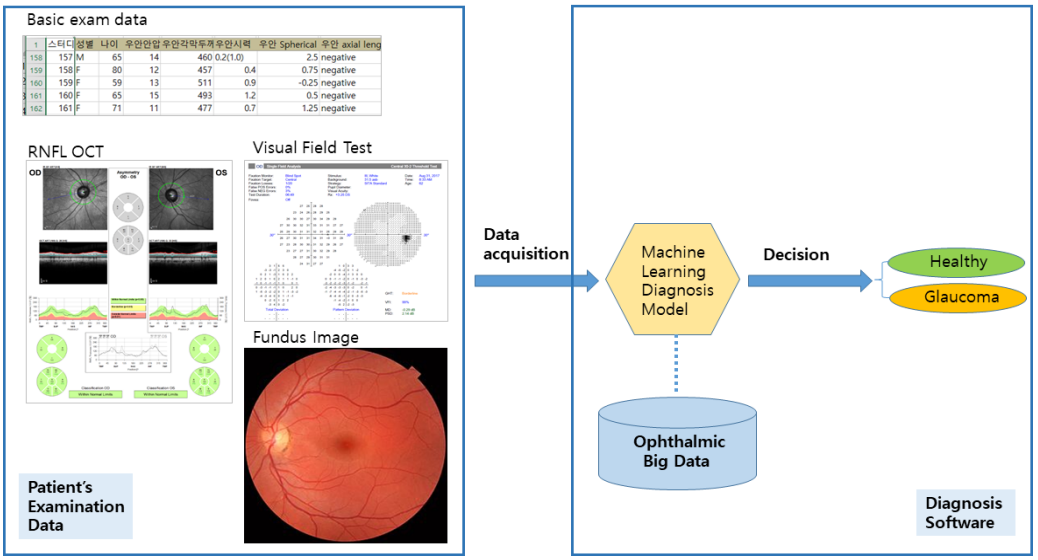
개발목표시기	2020. 12.	기술성숙도(TRL)	개발 전	개발 후
			TRL 3	(예) TRL 7
결과물 형태	SW-Platform	검증방법	자체검증, 3자검증	
Keywords	녹내장, 머신러닝, 빅데이터			
외부기술요소	100% 개발기술	권리성	특허, SW	

II. 기술의 개념 및 내용

1. 머신러닝을 적용한 녹내장 진단 기술

➢ 녹내장 진단 모델 개발을 위한 안과 빅데이터를 구축하고, 이를 활용하여 머신러닝 녹내장 진단 모델을 개발한 후, 진단 SW에 삽입함

* 본 내용은 오세종 교수(☎ 031-8005-3222)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***정보통신기획평가원은 현재 개발 진행 및 완료 예정인 ICT R&D 성과 결과물을 과제 종료 이전에 공개하는 "ICT R&D 사업화를 위한 기술예고"를 2014년부터 실시하고 있는 바, 본 칼럼에서는 이를 통해 공개한 결과물의 기술이전, 사업화 등 기술 활용도 제고를 위해 매주 1~2건의 관련 기술을 소개함



[그림 1] 기술개념도

➢ 진단 SW는 다양한 검사 데이터로부터 녹내장 진단에 필요한 정보를 자동 추출하고 이를 진단 모델에 입력하여 녹내장 유무를 판별하며, 진단 결과에 대한 근거를 설명함

2. 기술의 상세내용 및 사업화 제약사항

➢ 기술의 상세내용

- 머신러닝 기술을 적용한 녹내장 진단 모델 및 진단 SW
- 안과 검사 데이터로부터 진단에 필요한 정보 자동 추출 기능
- 안과 빅데이터 축적에 의한 녹내장 진단 모델의 지속적 업그레이드
- 진단 결과에 대한 근거 설명 기능
- 환자에 대한 검사 이력 관리 기능

➢ 기술이전 범위

- 녹내장 진단 모델 및 진단 SW
- 구축된 빅데이터는 기술이전 범위에서 제외함

➢ 사업화 제약사항

- 의료계의 원격진료에 대한 부정적 인식으로 기술의 활용 범위가 제한될 수 있음

III. 국내외 기술 동향 및 경쟁력

1. 국내 기술 동향

➢ 인공지능 기술을 적용한 진단 기술 및 장비가 식품의약품안전처로부터 의료기기로 인정받기 시작함
- 뇌경색 유형을 분류하는 소프트웨어(SW)
- 성장기 어린이 등 골연령 측정 SW
- X-레이 영상을 통한 폐결절 진단 보조 SW

➢ 연구차원에서의 시도들이 보고되고 있음
- 김안과병원(건양의대)에서 시신경 사진을 데이터로 하여 회귀분석 및 합성곱 신경망 기법을 적용했을 때 100% 가까운 녹내장 진단 정확도를 얻었다고 보고(데이터 양으로 볼 때 신뢰도는 높지 않음)
- 동국대학교일산병원 연구팀과 ㈜제이엘케이인스펙션이 기술협력을 통해 뇌졸증 뇌 MRI 영상 인공지능 진단시스템 개발 중

➢ 아직까지 녹내장 진단이 제품화된 사례는 보고되지 않음

2. 해외 기술 동향

➢ 연구 차원에서 녹내장 진단을 위한 인공지능 기술 연구가 활발히 진행되고 있음
- Optical Coherence Tomography와 Color Fundus Images를 이용한 녹내장 진단 연구
- Visual field와 optical imaging data를 이용한 녹내장 진단 연구
- 구글의 Fundus Images를 이용한 녹내장 진단 연구

➢ 아직까지는 해외에서도 제품화된 사례가 보고되지 않음

3. 관련 보유특허

No.	국가	출원번호(출원일)	상태	명칭
1	대한민국	10-2019-0037224	출원	녹내장 진단용 피처 생성 방법 및 장치, 그것을 이용한 녹내장 진단 방법 및 장치

4. 기술적 경쟁력

➢ 아직은 비교 대상 제품이 없어서 본 기술의 우수성 및 차별성을 말하기 어려움

경쟁기술	본 기술의 우수성 및 차별성
	녹내장 진단 시 참고할 수 있는 보조 정보를 제공함
	녹내장 진단에 대한 근거를 설명할 수 있음
	Stand alone 형태의 SW 개발로 환자 검사 데이터에 대한 유출 우려가 없음

IV. 국내외 시장 동향 및 전망

1. 국내 시장 동향 및 전망

➢ 연도별 시장규모 전망(인공지능 진단 기술 전체)

구분	2018년*	2023년**	2025년**
국내 시장규모(억 원)	1,696	2,500	2,550

* http://smroadmap.smtech.go.kr/0201/view/m_code/A150/s_code/A02/idx/1687
** 상기 통계에서 연도별 증가 추세로 추정

➢ 예상 수요처

수요처	국명	수요량
안과병원	대한민국	1,537 *
의료정보시스템 개발 업체	대한민국	200 **
안과질환 연구기관	대한민국	500 **

* 국민건강보험공단, 건강보험통계 참조
(http://kosis.kr/statHtml/statHtml.do?orgId=350&tblId=TX_35001_A016)
** 추정치

2. 해외 시장 동향 및 전망

➢ 연도별 시장규모 전망(인공지능 진단 기술 전체)

구분	2018년*	2023년**	2025년**
세계 시장 규모(억 원)	97,531	150,000	156,000

* http://smroadmap.smtech.go.kr/0201/view/m_code/A150/s_code/A02/idx/1687
** 상기 통계에서 연도별 증가 추세로 추정

3. 제품화 및 활용 분야

활용 분야(제품/서비스)	제품 및 활용 분야 세부내용
진단 SW	- Stand alone 형태의 소프트웨어 개발로 개별 의료기관에서 검사데이터의 유출에 대한 우려 없이 도입 가능함 - 윈도 운영체제 기반 SW로 개발 - 녹내장 의심 환자에 대한 진단에 보조적으로 사용할 수 있음

V. 기대효과

1. 기술도입으로 인한 경제적 효과

➢ 개발된 진단 기술을 검사장비에 추가함으로써 장비의 부가가치를 높일 수 있음
➢ 향후 예상되는 해외 제품의 유입에 대비한 사전 국산화로 외화 절약 가능

2. 기술사업화로 인한 파급효과

➢ 초기 진단이 어려운 녹내장의 진단에 도움을 줄 것으로 기대
➢ 안과 진료 시에 생성되는 빅데이터를 기반으로 인공지능 진단 모델을 개발함으로써, 실명을 유발할 수 있는 녹내장을 조기에 진단하거나, 스크리닝에 사용할 수가 있으며, 치료 과정 중에도 질병의 진행을 쉽게 판단할 수 있는 프로그램 개발을 통해 치료 방향 설정과 치료 목표 설정에 도움을 줄 것으로 기대
➢ 본 연구를 통해 획득되어진 데이터 처리 기술이나 인공지능 프로그램, 그리고 학습

모델(learning model)은 임상진료 환경에서 바로 사용될 수 있고, 현재 통용되고 있는 전자차트에 접목이 된다면 부가가치를 더욱 높일 수 있음

- 안과 주요 질환의 빅데이터 수집으로 역학 연구나 질병의 발생, 경과, 치료 그리고 치료제 개발에 사용될 수 있는 학문적인 핵심 자료로 활용될 수 있을 것으로 예상

- 사업책임자: 문형돈(기술정책단장)
- 과제책임자: 이성용(산업분석팀장)
- 참여연구원: 이재환, 이효은, 이상길, 안기찬, 김용균, 정해식, 김우진, 장예지, 전영미(위촉)

주간기술동향

통권 1916호(2019-38)

발 행 년 월 일 : 2019년 10월 2일
발 행 소 : IITP 정보통신기획평가원
편집인겸 발행인 : 석제범
등 록 번 호 : 대전 다-01003
등 록 년 월 일 : 1985년 11월 4일
인 쇄 인 : ㈜승일미디어그룹

IITP 정보통신기획평가원

(34054) 대전광역시 유성구 유성대로 1548(화암동 58-4번지)
전화 : (042) 612-8296, 8214 팩스 : (042) 612-8209

깨끗한 IITP, 신뢰받는 IITP

IITP 정보통신기획평가원

http://www.iitp.kr

IITP 부정비리 신고센터