4차 산업혁명과 정보보호 기술

김익균*, 나중찬, 김수형, 진승헌

1. 서 론

최근, 전 세계는 ‘초연결성(Hyper-Connected)’, ‘초지능화(Hyper-Intelligent)’로 특징되는 디지털 혁신의 제4차 산업혁명 시대 진입으로 사회·경제·문화 전반에 대변혁이 촉발되고 있다. ‘20년, 인터넷 가입자 30억명, 500억개 스마트 디바이스가 연결된 세상의 도래로 디지털 혁신(DX)에서 한걸음 더 나아가, 각 국가는 ‘국가 경제·사회시스템의 지능형 디지털 혁신(IDX[1])’을 통한 미래 성장 동력의 선점을 목표로 하고 있다.

하지만, 모든 것이 연결되고 디지털화된 세상의 도래는 새로운 기회와 위기가 공존하여, 지능화된 사이버위협에 대한 선제적 대응이 없다면 개인과 사회에 막대한 피해를 초래할 위기가 잠재되어 있다. 예를 들어, 악성코드 ‘미라이’에 감염된 50만개 IoT기기를 이용한 DDoS 공격 발생(‘16.10)이나, ’워너크라이‘등의 랜섬웨어 공격으로 전 세계(150개국)에 혼란이 야기되고(‘17.5), O2O업체 ‘여기 어때’의 340만건 개인정보 유출 피해 사고(‘17.4) 등이 잠재적 위협의 대표적인 사례로 볼 수 있다.

지능정보사회를 대표하는 자율주행, AI비서, 스마트시티 등의 新서비스는 개인의 안전과 프라이버시가 전제된 신뢰 기반 구축 없이는 사상누각(沙上樓閣)으로 전락될 우려가 있다.

모든 사물이 인터넷으로 연결되는 超연결사회(Hyper-connected Society)로 진입이 급속하게 진행되면서 나날이 지능화·고도화되고 있는 사이버공격으로 인해 막대한 경제적 피해와 국가·사회적 혼란이 야기되는 등 그 위력이 사이버 공간을 넘어서 이미 현실적 위협으로 전이되고 있다. 이와 더불어, 정보보호 산업은 빠르게 성장 중이며 세계적으로 사이버보안은 단순히 산업의 영역을 벗어나 국가안보와 국민생명이 직결된 국가기간산업으로서 가치가 강조되는 추세이며, 주요 국가들은 정부 주도하에 사이버보안 기술 확보에 주력하고, 급성장하고 있는 시장에서 우위 선점을 위해 막대한 투자를 병행하고 있다.

본 고는 4차 산업혁명이라고 불리는 디지털 혁신이 진행되는 과정에서 반드시 동반 성장되어야 하는 정보보호 산업에 필수적인 기술들에 대하여 세부 기술분야 별 현황을 살펴본다. 제 2장에서는 정보보호 산업에 기반이 되는 다양한 보안기술 동향을 살펴보고, 제 3장에서 결론을 맺는다.

*교신저자(Corresponding Author) : 김익균, 주소 : 대전광역시 유성구 가정로 218 한국전자통신연구원 정보보호연구본부 전화: 042-860-5442, FAX: 042-860-1471, E-mail : ikkim21@etri.re.kr

1) Intelligent Digital Transformation: ‘지능 → 초지능’, ‘연결 → 초연결’, ‘실감 → 초실감’으로의 변화를 가져올 수 있는 과감·도적적인 시도를 의미

2. IDX시대의 정보보호 기술 동향

보안 산업에 기반이 되는 정보보호 기술은 암호, 인증, 인식, 분석/감시 등의 보안기술이 적용된 제품을 생산하거나, 관련 보안기술을 활용하여 개인·기업·국가의 안전과 신뢰를 보장하는 서비스를 제공하는 기술로 정의된다. 네트워크·시스템 기반의 정보보안, 안전·안심 생활을 위한 물리보안, 보안기술과 전통 산업간 융합으로 창출되는 융합보안을 포함하고 있고, 컴퓨터·네트워크 수준의 보안을 넘어 치안감시, 의료, 전력 등 사회 전반의 보안으로 확장되면서, IT기반 미래 지식정보사회에서 개인·기업·국가 안보의 핵심역할을 수행한다.

4차 산업혁명 시대의 정보보안 산업은 개인에게 디지털 안심생활 인프라를 제공하고, 사회전반에 걸쳐 안전한 디지털 치안 인프라를 구축하며, 국가적으로는 디지털 안보 인프라 마련을 지향하고 있다.

그림 1. 디지털 안심생활 인프라

2.1 디지털 안심생활 인프라

4차 산업혁명시대에 개인 생활과 직접적으로 관련된 대표적인 현안으로는 공인인증서 등 불편한 금융거래와 개인정보 유출에 의한 프라이버시 침해, 지능정보사회의 부작용으로 스마트 자동차/의료/헬스케어의 해킹 위협과 신규 ICT 기술 적용에 대한 불안이 증가되고 있는 상황이다.

(그림 1)과 같이 개인 안심 분야는 사용자가 불편하지 않고, 프라이버시 침해없는 디지털 안심생활 인프라 구축을 지향하고 있다. 복잡한 금융거래 보안절차로 인한 불편함을 해소하고, 빅데이터 프라이버시 보호로 개인정보 유출 방지하며 개인의 생명과 재산을 위협할 수 있는 新디지털 라이프 서비스에 대한 신뢰와 안전을 보장하는 안심 생활 인프라 관련 보안기술이 개발되고 있고, 세부 분야별 기술동향은 아래와 같다.

▫ **핀테크 보안**: 바이오, 행위, 환경, 관계 등 정보를 이용한 간편한 인증과 분산 거래 서비스를 위한 O2O(Online to Offline) 분산거래 보안 플랫폼 제공을 목표로 하고 있다. 간편 결제・인증 기술로 편리한 인증과 안전한 거래를 지원하는 FIDO(Fast Identification On-line)[1]기반 간편 결제・인증 기술이 최신 금융・IT 기술과 접목을 통해 사회 全분야로 빠르게 확산 중에 있으며, FIDO와 TEE[2], NFC-HCE[3], MST[4] 등 최신 IT 보안기술

2) TEE : Trusted Execution Environment

이 적용된 간편 결제 서비스가 미국, 일본, 중국 등에 빠르게 확산되고 있으며, 전자금융, 이동통신, 전자정부 분야에서도 다양한 인증수단을 적용한 FIDO 간편 인증 서비스도 제공 중에 있다.

▫ **빅데이터 프라이버시**: 클라우드 및 빅데이터 환경에서 개인정보유출에 대한 우려가 커지면서, 개인정보 빅데이터의 비식별화 및 암호화된 상태에서의 연산을 통한 개인정보 유출 방지 기술이 새롭게 주목을 받고 있다. 모바일, 클라우드 환경에서의 ICT 신규 산업 및 서비스 출현에 따라 프라이버시 보호를 위해 기존에 없던 암호 응용기술이 요구되고 있고, 단기/실용적인 관점에서 형태보존[3], 순서보존[4], 검색가능 암호 등의 연구가 진행되고 있으며, 중장기적으로는 동형암호 연구[5]가 핵심기술로 부각되고 있다. 민감한 개인정보로 구성된 데이터베이스에서 프라이버시를 보호하면서 통계량을 정확히 추출하기 위해 Differential Privacy, PPDM(Privacy Preserving Data Mining) [2]등이 연구되고 있으며, Differential Privacy 기술은 구글의 오픈 소스 RAPPOR, 애플의 iOS 10 등에 적용되고 있다.

▫ **자동차/의료/헬스케어 보안**: 개인의 생명을 위협할 수 있는 스마트 자동차 및 의료 서비스의 안전한 운영을 보장할 안심케어 기술이 새로운 보안 기술영역으로 주목을 받고 있다.

지능형 차량 보안기술은 차량 내・외부 네트워크 및 내부장치 보안 기술을 위주로 연구개발이 진행되고 있으며, 차량과 기반시설 간의 안전한 통신을 위한 인증기술 개발 및 C-ITS[5] 보안기술 개발이 지속 추진될 것으로 예상된다. 차량 간 통신 기술은 상용화 수준까지 진행되고 있으나, 보안 기술은 ECU[6] 및 차량내부통신망(CAN[7]) 보안 등 제한적으로 진행되고 있다.

의료기기 침해 방지 기술은 헬스케어/의료 기기 및 게이트웨이에서의 보안취약성을 탐지/차단하기 위한 기술 개발이 지속적으로 진행되고 있다. 미국 MIT에서는 의료기기 악성코드 탐지기법 등 60여개 이상의 헬스케어보안(SHARPS) 프로젝트 진행하고 있고, 퍼듀와 프린스턴 대학은 무선 심박동기 및 인슐린 펌프 등 의료기기용 외장형 방화벽인 'MedMon'을 개발[8]했으며, Arxan사는 화이트박스암호를 이용한 모바일의료 앱 템퍼링 방지/치유, MHR(Medical Health Record) 데이터 프라이버시, 기밀성보장 솔루션을 개발하였다.

▫ **증강/자율거래 보안**: 개인의 일상에서 안전 위협요소와 위・변조 정보를 자동인식하고 지능을 가진 사물이 안전하게 거래할 수 있는 신뢰 기반을 제공하기 위한 솔루션들이 개발되고 있다. 이와 관련하여 바이오인증 및 이상행위탐지 기술은 이용환경, 행위패턴 등 사용자 중심의 기계학습 분석을 통해 인증을 강화하고 효과적인 이상행위 탐지가 가능한 연구 투자가 확대되고 있다.

행위기반 바이오인증(Behavioral Biometrics) 기술은 학계, 스타트업, 글로벌 IT기업 등에서 활발히 연구되고 있으며, 금융권의 적용시도가 증가되는 추세이며, 패스워드를 대체하기 위해 비헤비오섹 인증솔루션, 구글의 Abacus 프로젝트 등은 사용자 기기에서 센싱되는 다양한 행위정보로 사용자를 인증하는 기술을 개발 중이며, 금융기업과 협업을 진행 중이다.

최근, 전자금융 거래의 탈중앙화, 투명성, 확장

3) NFC-HCE : Near Field Communication-Host Card Emulation
4) MST : Magnetic Secure Transmission
5) C-ITS : Cooperative Intelligent Transport Sytem
6) ECU : Engine Control Unit
7) CAN : Car Area Network

성, 보안성을 높이기 위한 방안으로 블록체인 기술에 대한 관심 증가와 원천 연구가 활발히 진행 중이다. 블록체인 기술의 금융권 적용 방안을 모색하기 위해 글로벌 블록체인 콘소시엄(R3 CEV)이 구성되었으며[9], 블록체인의 불변성(immutability) 특성을 활용한 다양한 보안 응용 솔루션이 개발되고 있다. 예를 들어, R3 CEV는 JP모간, 씨티그룹, BoA, 모건스탠리, 도이체방크 등 글로벌 금융회사들이 멤버로 참여하고 있고 Blockai는 사진, 그림 등 저작물의 해시를 블록체인에 저장 관리하는 저작권 보호 서비스를 개발하였다. DAO(Decentralized Autonomous Organization), BaaS(Blockchain as a Service), Blockchain of Things 등 다양한 응용분야 적용을 위한 프로젝트가 다수 진행 중이나 충분한 보안 검토 없이 진행된 프로젝트에 일부 우려가 제기되고 있다. 세계 제2의 가상화폐인 이더리움의 스마트 컨트랙트 기술을 통해 운영되는 DAO의 해킹 사례로 보안의 우려가 증가되는 측면도 있다.('16.5)

그림 2. 지능형 디지털 치안 인프라

2.2 디지털 치안 인프라 구축

보안산업 측면에서의 대표적인 사회적 현안로는 금융망마비, DDoS, 랜섬웨어 등 지능화・은밀화되고 있는 표적공격에 대한 실시간 대응 미흡으로 사회 안전 위협이 고조되는 바, 사이버 및 물리적 환경에서 효율적인 사회 안전 시스템 구축이 필요한 상태라고 할 수 있다.

따라서, 사이버범죄 및 물리적 신변 위협에 지능적으로 대응하는 디지털 치안 인프라 구축을 위해 (그림 2)와 같이 사이버위협 사전・사후 대응을 위한 지능형 침해대응, 시공간 위험 인지의 지능형 도시감시 기술, 초연결 위협에 대응하는 고신뢰 IoT보안 인프라 및 기계가 스스로 대응하는 자율 해킹 방어 기술 개발이 진행되고 있다.

▫ **지능형 침해 대응**: 날로 고도화된 사이버 범죄의 사전방어를 위한 사이버 자가방어 기술 및 신종 악성코드 대응 등의 클라우드기반 지능형 보안서비스 기술 개발을 목표로 AI기술을 이용한 지능형 침해 대응기술 개발이 진행되고 있다. 인공지능 기반 침해사고 분석/대응 기술은 딥러닝/머신러닝 등을 이용한 인공지능 기반의 침해사고 자동탐지 및 이를 통한 침해사고 대응정보 자동생성 기술 개발로 발전하고 있다. MIT에서는 인공지능과 침해사고 분석가의 직관력을 결합하여 알려지

지 않은 공격에 대한 사전 탐지가 가능한 AI2를 개발하였으며[6], 또한, 기 분석된 침해사고 보고서 및 현재 발생되고 있는 모니터링 정보의 기계학습을 통해 현재 발생되고 있는 정보 중 침해사고와 연관된 정보와 이를 조치할 수 있는 정보를 분석가에게 제공하는 기술을 연구 중에 있다. IBM의 Watson 시스템의 보안 적용을 통한 IBM Cognitive Security 서비스[8]를 '16년 말 출시하였으며, 이를 통해 보안 분석가의 수동분석 지원, 침해사고 의심정보 제공 및 의심정보의 대응 방법을 제공하고 있다.

ㅁ지능형 도시 감시: 물리적 시공간에서 발생하는 다양한 위험상황을 전지적 감시 시점으로 인식, 추적, 검색, 예방 및 대응하는 차세대 AI치안 플랫폼 개발이 진행되고 있다. 광역 도메인(도시 등) 내의 다중 센서 정보를 복합 연계・분석해서 위험상황을 실시간 탐지, 대응 및 과거 위험을 역추적하고 미래 위험을 예측하는 지능형 영상분석의 City Surveillance 연구 개발이 진행되고 있다. 미국은 CCTV, 차량 번호판 감지기, 방사능 측정기, 911 전화 등을 실시간 복합・연계해서 도시 전체의 위험상황을 감지/대응하기 위한 Intelligent City Surveillance가 운용중이며, DAS(Domain Awareness System)는 NYPD, MS 등이 공동으로 개발하고 있는 상태이다.

영상기반 City Surveillance기술은 기존 알고리즘 방식에서 기계학습 기반 신경망 기술(딥러닝)로 발전하고 있으며, 다양한 융합산업 분야에 확대・접목되고 있다. 구글은 세계 최고수준의 딥러닝 기술과 빅데이터를 기반으로 인지, 검색 등에서 독보적 입지 구축하고 있고, MCT(Multi Cameras Tracking), 대규모 이미지/비디오의 분류, 검색 등 지능형 영상분석 원천기술력 확보에 주력하고 있다.

휴먼 바이오인식 기술은 인식 성능과 사용자 편리성, 보안성을 동시에 보장하는 비제약형 바이오인식 기술로 발전하고 있으며, 융합산업 핵심 길목기술로 대두되고 있다. 페이스북은 하루 10억명 이상 사용자 빅데이터를 기반으로 인간의 시각지능 수준의 딥러닝 기술을 개발해서 얼굴인식/분류/검색에 적용하고 있다[9]. 중국 바이두는 딥러닝 권위자인 앤드류 응 교수를 영입해서 단숨에 세계수준의 영상, 음성인식(Deep Speech) 원천기술 보유하고 있고, 매년 인공지능연구에 3억 달러, 300명 이상 전문연구인력을 투자하며, 이미지넷 오브젝트 분류 벤치마크에서도 5.98 EER(Equal Error Rate) 성능을 기록하고 있다[10]. 또한, 다양한 바이오인식 센서(지문, 얼굴, 홍채, 음성 등)을 연동해서 위험인물을 실시간 검색・추적하기 위하여 미국 FBI에서는 NGI(Next Generation Identification) 시스템이 파일럿 프로그램으로 운용 중에 있다.[7]

ㅁ능동보안 인프라: 모든 사물이 초연결되는 새로운 IoT 환경에서 사물주체, 객체들이 스스로 협력하여 자율적 대응이 가능한 고신뢰 자율 네트워크 인프라 구현을 목표로 진행하고 있다.
각 사물의 실행 환경 오염 방지, 정보 위변조 방지 및 악의적 재사용 방지를 위한 IoT 디바이스 별로 암호 키를 별도의 하드웨어를 이용하여 보호하는 신뢰 플랫폼 모듈(Trusted Platform Module) 기술 개발이 개발되었다. HP, IBM, MS에 의해 설립된 TCG(Trusted Computing Group)는 신뢰할 수 있는 컴퓨팅 플랫폼 표준화를 추진하고 있으며 저장

8) https://www.ibm.com/security/cognitive/

9) Facebook's DeepFace 성능: 97.25%, 사람의 얼굴인식 성능: 97.53%

10) 구글 성능: 6.66 EER, 사람: 5.1 EER

키 기반의 (하드웨어 칩 기반 암호화 처리 모듈을 위한) TPM 표준을 개발 중에 있다.

IoT 기기의 이상징후를 상황정보 기반으로 스스로 분석・판단하기 위한 경량화된 분석・탐지 기술 개발과 악성코드 감염, 취약점 존재 여부 등의 상세분석을 통해 대응 기반 정보 생성을 위한 클라우드 기반 보안 분석 기술이 개발 중이다. 특히, IBM의 Watson IoT Platform은 장비 인증, 통신 암호화, 메시지 체크섬 관련 API 등 Platform 측면에서 보안 기능을 제공하고 있어, IoT 디바이스 측면에서 스스로 분석 판단하여 빠르게 대응 할 수 있는 기술이 대표적이라고 할 수 있다.

▫ **자율 해킹 방어**: 기계가 스스로 신규 보안취약점을 발견하고 공격대상이 스스로 변이하여 해킹에 대응하는 AI기반 능동적 자율방어 기술개발이 진행되고 있다. 취약점 검색 및 분석 기술이 네트워크 시스템 영역에서 웹/IoT 환경 특화된 취약점 스캔으로, 정적/동적 방식의 개별 테스트에서 정적+동적 방식의 결합 테스트로 변화・발전하고 있고, 취약점 검색은 기존 IP/Port, 시스템 정보 스캔 기술에서 웹 어플리케이션 및 IoT 환경에 특화된 디바이스/통신 프로토콜/소프트웨어 등의 취약점 스캔으로 기술 트렌드가 변화하고 있다. 대표적인 기업은 IBM의 AppScan, Accunetix WVS 등 웹 어플리케이션에 특화된 취약점 스캔 기능을 제공하고 있고, SHODAN, Censys 등 IoT 환경에서 사용되고 있는 응용 및 암호 통신 프로토콜에 대한 스캐닝 기술에 대한 연구가 본격화 되고 있다. IoT 디바이스의 경우 오픈소스의 사용 비중이 높아, 오픈소스 기반의 IoT 소프트웨어에 내포된 취약점을 스캔하기 위한 오픈소스 취약점 자동 분석 기술 연구가 활발하게 이루어지고 있다.

능동적 자율방어 기술로 대표적인 연구개발 주제인 Moving Target Defense(MTD)는 지능화되고 있는 사이버 공격에 능동적으로 대응하기 위한 혁신적인 보안 전략 기술이다. MTD는 미국 백악관이 2011년에 발표한 “사이버보안 연구개발 전략” 중 가장 주목 받았던 연구 분야로서 2017년 현재 미국 국토안보부(Homeland Security)에서 연구를 수행하고 있다. 네트워크 환경에서 사이버 공격 대상(Target:목표)의 주요 속성(IP Address, Port, Protocol, Platform, OS 등)을 이동(Moving)시킴으로써 공격자의 공격 또는 분석(취약점 분석) 행위를 능동적(Active)으로 방어(Defense)하기 위한 보안 기술이다.

2.3 디지털 안보 인프라

최근 정보보안 분야는 국가 안보 분야로서 국가적으로 중요하게 다루어지고 있어 국방・기반시설 보호를 위한 디지털 안보 인프라 구축이 시급한 실정이다. 국방부 전산망해킹, 워너크라이 등 국가적 인프라에 대한 공격 경로의 복잡・다양화 및 고도화가 되고 있으며, 적대적 국가로부터 국방・기반시설의 사이버 위협이 심화되고 있는 상황이고, 사이버・물리 위협대응을 위해 심층방어 및 자가복원 기술과 사이버전 대응 및 스파이 행위 감시 기술 개발을 추진되고 있다.

▫ **사이버 킬체인** : 사이버공격을 프로세스 상으로 분석, 사전에 단계별 위협요소를 제거, 영역별 다중방어체계를 구축하여 공격자 의도와 활동을 분쇄 및 사이버피해의 자가복원(Resilience)을 통하여 안전의 지속성을 확보하는 기술이 주목을 받고 있다.

그림 3. 국가 디지털 안보 인프라

▫ **CPS(사이버-물리체계)[11] 보안** : 주요기반시설에 대한 통신채널 통제 기술과 사이버공격으로 인한 현실 공간의 피해 확산을 막는 사이버 킬스위치(Kill-Switch)[12] 기술 개발이 진행되고 있다. 주요기반시설의 침입차단 기술로 네트워크를 통한 산업제어시스템 침입을 차단할 수 있는 물리적 단방향 게이트웨이 및 제어기기 단위로 제어프로토콜 DPI 기반 침입을 차단할 수 있는 기술을 적용하여 산업제어시스템 네트워크 및 중요 제어기기의 보안성을 강화하는 추세이다. 대표적인 기업으로는 Waterfall의 USG (Unidirectional Security Gateway), Owl Tech.의 PDS(Perimeter Defense Solutions), CDS(Cross Domain Solutions)와 같은 데이터 다이오드 기술이 산업제어시스템에 적용되고 있다. Tofino사의 Industrial Security Solution 등이 상용화되었으며, 다양한 ICS 제어프로토콜을 지원하는 제품이 개발 중이다.

산업제어시스템 엔드포인트 보안 기술로는 산업용 네트워크 경계구간 보안 연구개발이 진행중이나, 산업용 단말에 대한 엔드포인트 보안기술은 기초 연구 수준이고, 산업용 네트워크 경계구간 보안기술은 적용이 추진되고 있으며, 산업용 네트워크 및 엔드포인트 보안기술에 대한 개발도 활발히 진행되고 있다. 대표적인 기업으로는 Bit9의 Security Platform, McAfee의 Application Control과 같은 엔드포인트 보안 제품도 출시되고 있다.

이외에도 공세적인 기술로 사이버 무기체계개발과 정교한 사이버 적군 타격을 위한 사이버 안보 감시체계 구축 기술 등이 있다.

▫ **사이버 무기 체계** : 사이버전 발생 시 전장상황을 직관적으로 인지하고 효과적인 지휘통제가 가능한 사이버 전장 상황인지 기술과 이에 따른 자동 공격 및 대응 수행용 사이버 무기 기술 확보가 절실한 상태이다..

▫ **사이버 안보 감시 체계** : 적대적 국가의 고도화된 정보수집 기술에 대응하기 위해 심층화된 스파이 활동 탐지 기술 및 이의 역추적이 가능한 전술적 포렌식 기술이 요구된다.

2.4 미래 지향적 Beyond Security 원천기술

양자 컴퓨터 출현, 생체정보 활용, AI기술 등 보안 패러다임 변화에 대응하기 위하여 새로운 보안

11) CPS(Cyber Physical System): 인터넷기반의 가상환경과 물리환경의 통합-융합을 추구하는 인더스터리 4.0의 새로운 패러다임
12) 킬스위치: 종료가 불가능한 위기 상황에 처한 장치나 기계를 종료하기 위해 사용되는 안전 매커니즘

패러다임을 선도하기 위한 미래 지향적 Beyond Security 원천 기술 개발이 진행되고 있다. 양자 컴퓨팅 환경을 위한 암호원천 기술, 융합형 바이오 암호키 기술, 사이버・물리 융합 환경에서 범죄 예측 기술 등의 미래 지향적인 원천 기술 개발이 지속적으로 투자될 것이다.

▫ **차세대 암호** : 양자 컴퓨팅에서도 안전한 Quantum-Safe 암호 및 암호키 관리의 원천적인 문제를 해결하기 위한 인공 신경망 기반 암호 체계 개발을 시작하는 시점이다. Quantum-Safe 암호기술은 양자컴퓨터 실현 가능성이 높아짐에 따라 PQC (Post-Quantum Cryptography)에 대한 암호 프로젝트, 공모사업 등으로 본격 연구개발 착수하였으며 격자, 다변수방정식, 코드기반 공개키 암호 등 신규 PQC 연구가 증가하는 추세이다. 미국 NSA는 기밀 보호용 암호 알고리즘(Suite B)을 양자컴퓨터 해독에 안전한 것으로 변경할 계획 공표하였으며('15.8.) 양자컴퓨터에 안전한 암호 표준이 준비되기 전까지 사용할 목적으로 CNSA(Commercial National Security Algorithm) Suite를 발표하였다. ('16.1.)

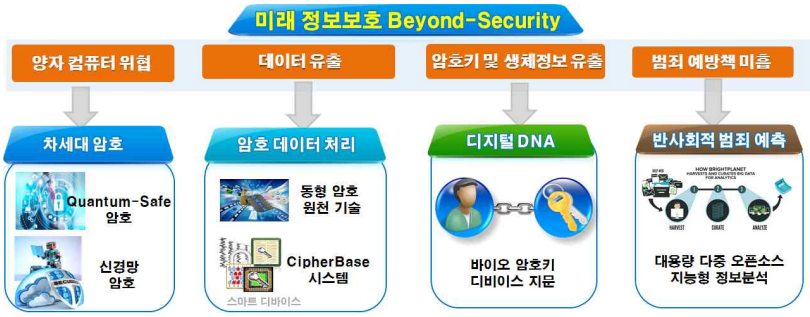

그림 4. 미래 지향적 Beyond Security 원천기술

유럽(EU)은 양자컴퓨터에 안전한 암호기술 연구사업인 SAFEcrypto와 PQcrypto 착수하였다. ('15.3.) Quantum-Safe 암호 관련 산업계 동향으로, Microsoft는 SIDH (Supersingular Isogeny Diffie-Hellman) SW 라이브러리를 발표하였으며 ('16.4.), Google은 자사 개발판 브라우저(Canary)에 격자 기반 키교환 프로토콜 'New Hope'를 탑재하여 시험을 시작하였다.('16.7.)

경량 암호기술은 ICT 디바이스의 소형화와 자원 제약적인 기기의 증가로 경량 암호기술의 필요성이 증대됨에 따라 관련 연구가 활발한 상태이다. 미국 NSA가 ISO/IEC 표준 PRESENT, HIGHT를 비롯한 기존 경량 블록암호 성능을 압도하는 블록암호 SIMON/SPECK을 발표하였고('13), 룩셈부르크 대학의 암호 연구 그룹 CryptoLUX는 8비트 AVR, 16비트 MSP, 32비트 ARM 등 경량 SW 환경에서 암호 알고리즘의 성능을 평가하는 FELICS 프레임워크를 발표하였으며 성능 평가를 진행하였다.('15)

키 은닉, 키 관리 기술은 데이터 보호를 위한 암호 구현의 효율성 경쟁에서 부채널분석 등 구현상의 키누출 공격 심화로 정보보호 全분야에 안전 구현 및 키은닉 기술 중요성이 확대되고 있다. 물리적 복제방지 기법인 PUF(Physically Unclonable

Function) 기술을 기반으로 안전한 키의 동적 생성 기술 연구가 진행 중이며, NXP에서는 Intrisic-ID의 PUF기술을 자사 차세대 IC카드 솔루션에 탑재 개발 중이고, ICTK에서는 HW기반 키 은닉 원천 기술인 PUF기술에 대한 연구개발 진행 중이다.

이외에도 신규 보안기술로 개발될 분야는 아래와 같은 것으로 예상해 본다.

▫ **디지털 DNA**: 디바이스 및 생체정보 유출을 방지하고 실시간으로 암호키 전 주기관리(생성/사용/은닉/폐기)가 가능한 바이오 암호키 및 디바이스 지문 기술이 활성화 될 것이다.

▫ **범죄 행위 예측**: [13]OSINT, HUMINT, IMINT, MASINT등 ICT 전반의 대규모 정보를 지능적으로 분석하여 사전에 사이버・물리환경의 반사회적 범죄 행위를 예측하는 기술이 미래 정보 분석기술로 주목을 받을 것이다.

4. 결 론

모든 사물이 인터넷으로 연결되는 超연결사회로 진입이 급속하게 진행됨에 따라 사이버보안산업은 어떤 산업보다 가파르게 성장하고 있는 중이다. 정보 보안은 단순한 산업의 영역을 벗어나 국가안보와 국민생명이 직결된 핵심기간 산업으로서 중요성이 부각되고 있는 추세이며, 주요 선진국들은 정부 주도하에 관련 정보보호 기술 경쟁력 확보에 총력전을 펼치고 있다.[10]

이와 같이, ICT기술의 全사회적 확산으로 인해 기존 사이버보안 외에 개인과 사회 안전, 국가 안보 등 국가・사회적인 주요현안에 대한 해결책 제시가 필요하며, 정보보호 기술 및 산업은 디지털 경찰이자 군인으로 국민 안전과 국가 안보에 직결되어, 미래에 닥쳐올 국가・사회적 위협을 선제적으로 해소할 R&D 투자 및 범정부 차원의 협력과 정책적 지원 필요한 시점이라고 볼 수 있다.

13) OSINT: Open source intelligence, HUMINT: Human intelligence, IMINT: Imagery intelligence, MASINT: Measurement and signature intelligence

참 고 문 헌

[1] Leveraging FIDO Standards to Extend the PKI Security Model in United States Government Agencies. FIDO Alliance White Paper, https://fidoalliance.org, 2017

[2] E. Bertino, D. Lin, and W. Jiang, “A Survey of Quantification of Privacy Preserving Data Mining Algorithms,“ In Privacy-Preserving Data Mining: Models and Algorithms, vol.34, pp.183-205, Kluwer Academic Publishers, Jun. 2008.

[3] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers. Format-preserving encryption. Selected Areas in Cryptography – SAC 2009. Lecture Notes in Comput. Sci., vol. 5867, pp. 295-312, 2009

[4] D. Sacharidis, K. Mouratidis and D. Papadias, “k-Anonymity in the Presence of External Databases,“ IEEE Transactions on Knowledge and Data Engineering, 2010.

[5] 송유진, 박광용, “데이터베이스 아웃소싱을 위한 준동형성 암호기술”, 정보보호학회지, 제19권, 제3호, pp.80-89, 2009.

[6] K. Veeramachaneni, I. Arnaldo AI2: training a big data machine to defend IEEE international conference on big data security on Cloud (BigDataSecurity 2016) (2016)

[7] https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

[8] Meng Zhang, Anand Raghunathan, and Niraj K. Jha. MedMon: Securing medical devices through wireless monitoring and anomaly detection, IEEE Transactions on Biomedical Circuits and

Systems
[9] Stan Higgins (July 21, 2015). “Inside R3CEV’s Plot to Bring Distributed Ledgers to Wall Street “
[10] KOTRA, 워싱턴무역관, “미국 사이버보안시장 동향과 우리기업 진출을 위한 시사점”, 2016.8

김 익 균

- 1994년 경북대학교, 컴퓨터공학과 학사
- 1996년 경북대학교, 컴퓨터공학과 석사
- 2009년 경북대학교, 컴퓨터공학과 박사
- 1996년~현재, ETRI 지능보안연구 그룹장
- 2004년~2005년 Purdue Univ. 객원연구원
- 관심분야 : 네트워크 보안, 클라우드 보안, AI기반 보안분석 기술, IoT보안 기술

나 중 찬

- 1986년 충남대학교, 컴퓨터과학과 학사
- 1989년 숭실대학교, 전자계산학과 석사
- 2004년 충남대학교, 컴퓨터공학과 박사
- 1989년~현재 ETRI 시스템보안연구그룹장
- 관심분야 : 임베디드 시스템 보안, 산업용 IoT 시스템 보안, 펌웨어/하드웨어 역공학 분석

김 수 형

- 1996년 연세대학교, 컴퓨터공학과 학사
- 1998년 연세대학교, 컴퓨터공학과 석사
- 2016년 한국과학기술원 전산학과 박사
- 1998년~2000년 : ㈜한국정보통신 기술연구소 연구원
- 2000년~현재, ETRI 정보보호연구본부 기술총괄
- 관심분야 : 인증, 핀테크보안, 모바일지불결제, 개인정보보호

진 승 헌

- 1993년 숭실대학교, 전자계산학과 학사
- 1995년 숭실대학교, 전자계산학과 석사
- 2004년 충남대학교, 전산학(정보보호) 박사
- 1999년~현재 ETRI 정보보호연구본부 본부장
- 관심분야 : 인증, IAM, 개인정보보호, 핀테크보안