방송통신정책연구 2022-0-00016

정책연구 22-24-04

사이버 위협 인텔리전스 기반 차세대 보안

Next-Generation Cybersecurity Based on Cyber Threat Intelligence

2022. 12

주관연구기관 : 정보통신정책연구원

연구기관 : (사)한국정보과학회

과학기술정보통신부
Ministry of Science and ICT

정보통신기획평가원
Institute of Information & Communications Technology Planning & Evaluation

방송통신정책연구 2022-0-00016
정책연구 22-24-04

사이버 위협 인텔리전스 기반 차세대 보안

Next-Generation Cybersecurity Based on Cyber Threat Intelligence

홍지만 외

2022. 12.

주관연구기관 : **정보통신정책연구원**
연구기관 : **(사)한국정보과학회**

과학기술정보통신부 정보통신기획평가원

이 보고서는 2022년도 과학기술정보통신부 방송통신발전기금 방송통신정책연구사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 과학기술정보통신부의 공식입장과 다를 수 있습니다.

제 출 문

과학기술정보통신부 장관 귀하

본 보고서를 『**디지털 대전환 메가트렌드 연구: 사이버 위협 인텔리전스 기반 차세대 보안**』의 연구결과보고서로 제출합니다.

2022년 12월

연 구 기 관 : (사)한국정보과학회
총괄책임자 : 홍지만 교 수
참여연구원 : 김동균 교 수
김봉재 교 수
이문규 교 수
이중희 교 수
허준영 교 수
이원준 교 수
이석준 교 수
이재흥 교 수

목 차

요약문 ····· xi

제1장 서 론 ····· 1

제1절 연구의 필요성 및 목적 ····· 1

제2절 연구의 범위 ····· 4

제3절 보고서 구성 ····· 5

제2장 차세대 사이버 보안 기술 로드맵 ····· 6

제1절 공통 기반 보안 ····· 6

제2절 시스템 · 네트워크 보안 ····· 66

제3절 융합 보안 ····· 116

제4절 기술 로드맵 · 시나리오 ····· 133

제3장 사이버 보안 정책 현황과 미래 전략 ····· 153

제1절 보안 위협 대응 정책 현황과 미래 전략 ····· 153

제2절 보안 산업 정책 현황과 미래 전략 ····· 174

제3절 R&D, 인력 양성 정책 현황과 미래 전략 ····· 205

제4장 결 론 ····· 213

참고문헌 ····· 216

표 목 차

〈표 2-1〉 NIST의 PQC 표준화 진행 일정 ····· 17
〈표 2-2〉 NIST의 경량 암호 표준화 진행 일정 ····· 19
〈표 2-3〉 무자각 지속인증의 특성 ····· 29
〈표 2-4〉 DID 표기법에서의 세 영역 ····· 32
〈표 2-5〉 완전동형암호 세대별 분류 ····· 37
〈표 2-6〉 오픈소스 기반 완전동형암호 라이브러리 목록 ····· 38
〈표 2-7〉 STIX 2.0 도메인 객체 정의 ····· 68
〈표 2-8〉 STIX 2.0 관계 객체 정의 ····· 69
〈표 2-9〉 IoT 보안사고 사례 ····· 75
〈표 2-10〉 공통 보안 기술 로드맵 ····· 133
〈표 2-11〉 시스템·네트워크 보안 기술 로드맵 ····· 134
〈표 2-12〉 공통 보안 기술 로드맵 ····· 136
〈표 2-13〉 IT 시스템과 OT 시스템 비교 ····· 148
〈표 2-14〉 OT 시스템 보안 관련 표준 및 가이드라인 ····· 150
〈표 3-1〉 정부부처별 컨트롤 타워 지정 논거 및 비판 ····· 171
〈표 3-2〉 정보보호산업법에 따르는 정보보호산업의 정의 ····· 174
〈표 3-3〉 국내 정보보호산업 매출 현황 ····· 176
〈표 3-4〉 글로벌 정보보호산업 시장규모 및 성장률 전망 (가트너) ····· 177
〈표 3-5〉 전세계 사이버보안 시장규모 전망(2022~2026) ····· 177
〈표 3-6〉 일본 사이버 보안 산업 관련 법·제도 ····· 184
〈표 3-7〉 중국내 사이버 보안 산업 관련 법·제도 ····· 186
〈표 3-8〉 정보보호산업 활성화를 위한 법적 근거 ····· 187
〈표 3-9〉 국가 사이버안보기본계획 부처별 시행 계획 ····· 190
〈표 3-10〉 정보보호기업 권역별 맞춤형 지원(안) ····· 195

〈표 3－11〉 ISMS 인증 의무대상자 ····· 197
〈표 3－12〉 정보보호 등급 부여기준 ····· 199
〈표 3－13〉 클라우드 서비스 유형 및 평가대상 ····· 200
〈표 3－14〉 정보보호인증의 유형 ····· 201

그 림 목 차

〔그림 1-1〕 국가의 정보보호 전략과 5G+의 핵심 서비스인 보안의 중요성 ····· 2
〔그림 1-2〕 사이버 보안 위협과 대응 기술 진화 ····· 3
〔그림 2-1〕 C. Bennett과 G. Brassard의 양자 키분배 논문 (1984년) ····· 8
〔그림 2-2〕 S.Wiesner의 Conjugate Code (양자 켤레코딩) ····· 9
〔그림 2-3〕 BB84 키분배 프로토콜 개요 ····· 10
〔그림 2-4〕 양자 키분배 시스템에 성공적으로 적용된 공격 리스트 ····· 11
〔그림 2-5〕 양자컴퓨터 개발의 동기: 양자 알고리즘의 역사 ····· 13
〔그림 2-6〕 소인수분해 및 타원곡선이산대수 문제를 풀기 위한 이론적 양자자원량 ·· 14
〔그림 2-7〕 IBM의 양자컴퓨터 개발 로드맵 ····· 15
〔그림 2-8〕 24시간 내에 RSA-2048 공격 가능한 양자컴퓨터 전문가 예측 ····· 16
〔그림 2-9〕 PQC(양자내성암호) 종류 ····· 16
〔그림 2-10〕 ASCON 알고리즘의 암복호화 구조 ····· 20
〔그림 2-11〕 Tel Aviv 대학의 부채널 공격 장치 ····· 21
〔그림 2-12〕 부채널 공격 기법으로 PIN 우회에 성공한 위조 카드 ····· 22
〔그림 2-13〕 멀티팩터 인증의 예 ····· 26
〔그림 2-14〕 다양한 서비스 상의 2단계 인증 방법 ····· 27
〔그림 2-15〕 FIDO 2.0 시스템 구조 ····· 28
〔그림 2-16〕 스마트밴드에 기반한 무자각 지속인증의 예 ····· 30
〔그림 2-17〕 DID의 표기 예 (W3C) ····· 32
〔그림 2-18〕 분산 ID 신뢰 모델 기반 검증가능한 크리덴셜 시나리오 예 ····· 33
〔그림 2-19〕 동형 암호의 활용 예 - 환자 데이터 처리 ····· 35
〔그림 2-20〕 동형 암호에서의 덧셈 보존과 곱셈 보존 개념도 ····· 36
〔그림 2-21〕 완전동형암호를 최초로 제안한 Craig Gentry ····· 36
〔그림 2-22〕 4-anonymity의 예 ····· 40

〔그림 2-23〕 애플 기기상에서 수집된 데이터의 차등 프라이버시 적용 ····· 41
〔그림 2-24〕 차등 프라이버시의 두 가지 방식 ····· 42
〔그림 2-25〕 윈도 운영체제의 TPM 사용 방법 ····· 44
〔그림 2-26〕 ARM의 TrustZone 구조 개념도 ····· 45
〔그림 2-27〕 VIA PUF 이미지 ····· 46
〔그림 2-28〕 이미지 센서 데이터 학습 및 이를 이용한 SW-PUF ····· 47
〔그림 2-29〕 회피 공격의 예 ····· 49
〔그림 2-30〕 오염 공격과 백도어 공격의 예 ····· 50
〔그림 2-31〕 비지도 학습을 통한 적대적 예제 탐지 ····· 52
〔그림 2-32〕 영리한 한스 (Clever Hans) ····· 53
〔그림 2-33〕 GARD 프로그램의 목표 ····· 54
〔그림 2-34〕 이상 감지 시스템 ····· 63
〔그림 2-35〕 설명 가능한 AI 기술 개념도 ····· 65
〔그림 2-36〕 알려진 표적공격 그룹 수 및 제로데이 공격 사용 그룹 비율 ····· 66
〔그림 2-37〕 TAXII 위협 공유 모델 ····· 70
〔그림 2-38〕 랜섬웨어 감염 프로세스 ····· 71
〔그림 2-39〕 비용 지불 시 랜섬웨어 복구 프로세스 ····· 72
〔그림 2-40〕 IoT 시장 규모 ····· 74
〔그림 2-41〕 미라이 봇 세부 동작 과정 ····· 76
〔그림 2-42〕 5G 보안 구조 ····· 78
〔그림 2-43〕 클라우드 컴퓨팅 서비스 모델 ····· 80
〔그림 2-44〕 2022년 클라우드 컴퓨팅 보안 위협 Top 11 ····· 82
〔그림 2-45〕 공급망 위협 개념도 ····· 83
〔그림 2-46〕 하드웨어 공급망 공격 분석 및 탐지의 어려움 ····· 84
〔그림 2-47〕 ASUS 업데이트 서버 공격 절차 ····· 85
〔그림 2-48〕 넷사랑 서버 공격 절차 ····· 86
〔그림 2-49〕 미국의 사이버 위협 정보공유 체계 ····· 88
〔그림 2-50〕 C-TAS 시스템 ····· 89

〔그림 2-51〕 KOSIGN 시스템 개요 ····· 90
〔그림 2-52〕 랜섬웨어 단순 흐름도 ····· 91
〔그림 2-53〕 지갑 탈취형 악성코드의 행위 예시 ····· 92
〔그림 2-54〕 채굴형 악성코드의 행위 예시 ····· 93
〔그림 2-55〕 서비스형 랜섬웨어의 조직화의 예 ····· 94
〔그림 2-56〕 5G 모바일 네트워크에 따른 구간별 보안 위협 개요 ····· 98
〔그림 2-57〕 AWS 보안 서비스 워크플로우 ····· 101
〔그림 2-58〕 GCP 보안 모델 ····· 103
〔그림 2-59〕 AES 모듈 백도어 검출 절차 ····· 105
〔그림 2-60〕 자동차 공급망 위험관리 프로세스 ····· 106
〔그림 2-61〕 Trust-Hub 분류 체계 ····· 107
〔그림 2-62〕 FirmFuzz 작업 흐름 ····· 108
〔그림 2-63〕 랜섬웨어 공격 타임라인별 대응 분류 ····· 110
〔그림 2-64〕 하드웨어 보안 취약성 탐지를 위한 종합적인 분석 체계 ····· 115
〔그림 2-65〕 스마트 시티 통합 플랫폼 개념 ····· 117
〔그림 2-66〕 자율 주행 수준 ····· 119
〔그림 2-67〕 V2X에서 사이버 공격의 위협 ····· 120
〔그림 2-68〕 디지털 헬스케어 서비스 구성요소 ····· 121
〔그림 2-69〕 스마트 공장의 구성요소 ····· 122
〔그림 2-70〕 LG CNS의 스마트시티 정보 보호 프레임워크 ····· 124
〔그림 2-71〕 수신측에서 IDS에 의해 감지되는 클럭 스큐 ····· 125
〔그림 2-72〕 Medigate 솔루션 구조 ····· 128
〔그림 2-73〕 사용자의 행동 패턴에 기반한 무자각 지속 인증 ····· 137
〔그림 2-74〕 기존 인증과 무자각 지속인증의 차이점 ····· 139
〔그림 2-75〕 무자각 지속인증 기본 절차 ····· 140
〔그림 2-76〕 걸음걸이 기반 인증 (Gait Recognition) ····· 141
〔그림 2-77〕 양자 우월성을 달성한 양자 회로에서의 제어 연산 ····· 142
〔그림 2-78〕 PQC 전환의 3단계 ····· 143

〔그림 2－79〕 PQC 전환을 위한 준비 과정 ····· 145
〔그림 2－80〕 OT 관련 용어 개념 및 구성 ····· 146
〔그림 2－81〕 OT 시스템 사이버 보안 사고 사례 ····· 147
〔그림 2－82〕 PERA 모델을 기반으로 한 OT 시스템 아키텍처 ····· 149
〔그림 2－83〕 보안 관제 기술발전 시나리오 ····· 151
〔그림 2－84〕 SOAR 개념 및 구성 요소 ····· 152
〔그림 3－1〕 마이크로소프트 익스체인지 제로데이 공격 과정 ····· 154
〔그림 3－2〕 다크사이드 랜섬웨어 감염 과정 ····· 155
〔그림 3－3〕 Log4j 취약점 시나리오 ····· 156
〔그림 3－4〕 온라인 커뮤니티에서 공유된 국내 아파트 월패드 해킹 영상 ····· 157
〔그림 3－5〕 한국원자력연구원 VPN 취약점을 통한 비인가 접속 IP 이력 분석 ····· 158
〔그림 3－6〕 POS 악성코드를 통한 카드결제 정보 탈취 ····· 159
〔그림 3－7〕 카드 정보 유출 사이클 ····· 160
〔그림 3－8〕 오바마 행정부 사이버 보안 추진 체계도 ····· 162
〔그림 3－9〕 트럼프 행정부 사이버 보안 추진 체계도 ····· 163
〔그림 3－10〕 「사이버보안기본법」 제정 이전 일본의 사이버 보안 체계 ····· 165
〔그림 3－11〕 「사이버보안기본법」 제정 이후 일본의 사이버 보안 체계 ····· 166
〔그림 3－12〕 영국의 사이버 보안 체계 ····· 167
〔그림 3－13〕 독일의 사이버 보안 추진 체계 ····· 168
〔그림 3－14〕 국내 사이버 보안 관리 체계 ····· 169
〔그림 3－15〕 정보보호산업의 정의 및 세부분야 ····· 175
〔그림 3－16〕 2016년 제1차 정보보호산업 진흥계획 비전 및 전략 ····· 189
〔그림 3－17〕 2020년 제2차 정보보호산업 진흥계획(2021~2025) 비전 및 전략 ····· 191
〔그림 3－18〕 정보보호산업의 전략적 육성 방안 목표 및 추진전략 (2022) ····· 193
〔그림 3－19〕 인공지능 기반 보안 산업활성화를 위한 사이버보안 AI 데이터셋 개방 ··· 194
〔그림 3－20〕 지역정보보호협의회 구성(안) ····· 196
〔그림 3－21〕 ISMS-P 인증기준 ····· 198

요 약 문

1. 제 목

사이버 위협 인텔리전스 기반 차세대 보안

2. 연구 목적 및 필요성

디지털 전환이 가속화되면서 사이버 보안 위협 역시 더욱 커지고 있다. 사이버 보안은 디지털 전환 시대 공동 번영을 위한 기본 바탕임과 동시에 적절한 대응이 이루어지지 않을 경우 디지털 공동 번영의 최대 위험 요소가 될 수 있다. 이를 위해서는 사이버 보안 기술의 발전과 더불어 적절한 정책적 지원이 꼭 필요한 상황이다.

본 연구 보고서는 국내외 사이버 보안 기술 동향을 확인하고 지속 가능한 디지털 전환과 디지털 플랫폼의 신뢰성 제공을 위한 차세대 사이버 보안 기술 방향을 제시한다. 추가로, 우리나라와 주요국들이 사이버 보안 정책 현황을 살펴보고 중장기적으로 정부의 지원 및 규제, 지원 방향에 대해 논의한다.

3. 연구의 구성 및 범위

본 보고서에서 다루는 사이버 보안 기술은 공통 보안 기술, 시스템・네트워크 보안 기술, 융합 보안 기술로 나누어 현황과 미래 기술 방향을 제시한다. 각각에서 다루는 세부 보안 기술은 다음과 같다. 공통보안기술에는 암호 기술, 인증・인가 및 접근제어 기술, 데이터 보안, 하드웨어 기반 보안, AI 보안을 포함한다. 시스템・네트워크 보안 기술에는 사이버 위협 인텔리전스(CTI), 랜섬웨어 대응, IoT 디바이스 보안, 5G 보안, 클라우드 보안, 공급망 보안을 포함한다. 융합 보안 기술에는 스마트 시티 보안, 스마트 자율 주행 이동체

보안, 디지털 헬스케어 보안, 스마트 공장 및 산업제어 보안을 포함한다. 이들 세부 기술에 대한 기술 발전 방향과 2030년까지의 기술 개발 로드맵을 제시한다.

현재 사이버 보안 기술 수준으로 인한 문제점을 해소하고 발전된 미래 기술을 제시하기 위해 기술 발전 시나리오를 무자각 인증, 양자 대비 암호, OT 통합 보안, AI 기반 보안 관제에 대해 제시하고, 각 시나리오에 대해 현재 기술, 미래 기술 수준을 정의하고 미래 기술 수준에 도달하는 데 필요한 기술을 제시한다.

4. 연구 내용 및 결과

사이버 보안 기술 현황 및 차세대 사이버 보안 기술 관련하여 다음의 기술을 중심으로 다루었다.

- 공통보안기술
  - (암호 기술) 양자 암호, 양자내성 암호, 경량 암호, 암호 부채널 분석 공격 및 대응
  - (인증・인가 및 접근제어 기술) 멀티팩터 인증, FIDO, 무자각 지속 인증, 분산 ID
  - (데이터 보안) 동형 암호, 차등 프라이버시
  - (하드웨어 기반 보안) 신뢰 플랫폼 모듈, 신뢰 실행 환경, 물리적 복제방지 기능
  - (AI 보안) 적대적 공격

- 시스템・네트워크 보안
  - (사이버 위협 인텔리전스) STIX, TAXII, CTIIC, CTA, C-TAS, KOSIGN
  - (랜섬웨어 대응) 랜섬웨어 감염 프로세스, 감염 사례, 세대별 발전 과정
  - (IoT 디바이스 보안) IoT 보안사고 사례, PUF, TPM, HSM
  - (5G 보안) 5G 보안 구조, 5G 보안 기능, 5G 보안 이슈
  - (클라우드 보안) 클라우드 컴퓨팅 보안 위협, 아마존 AWS 보안 서비스, 마이크로소프트 Azure 보안 서비스, 구글 GCP 보안 서비스
  - (공급망 보안) 공급망 공격 사례, Trust-Hub 분류 체계

- 융합보안
  - (스마트 시티 보안) RADICS
  - (스마트 자율 주행 이동체 보안) 이상 침입 탐지, 정보 중복, 암호화, 차량 간 V2X 통신보안, 차량용 이더넷 보안, 차량 취약점 분석
  - (디지털 헬스케어 보안) 의료정보 비식별화, 접근권한 관리, 의료기기 해킹 방지, 의료 랜섬웨어 대응, 생체신호 기반 보안통신, 헬스케어 데이터 보안
  - (스마트 공장 및 산업제어 보안) 계층적 방어를 위한 DiD 전략

5. 정책적 활용 내용

본 보고서에서 다루는 사이버 보안 정책 현황과 미래 전략은 보안 위협 대응 정책, 보안 산업 정책, R&D・인력양성 정책으로 나누어 제시한다.

현재 우리나라의 사이버 보안 위협 대응 체계는 여러 기관에 분산되어 대응 체계를 하나로 통합할 필요가 있다는 점에 대해서는 모두 동의하고 있지만 방법론에 있어서 다양한 이견이 존재한다. 국가차원의 통합적 사이버 보안 위협 대응 체계 수립을 위한 다양한 법안들이 발의되었으나 합의에 이르지 못해 아직 입법화되지 못하고 있다. 우리나라의 경우 사이버 보안 컨트롤 타워 역할 부여로 정보기관의 역할이 강화되는 것에 대한 사람들의 우려, 사이버 보안 관련 청와대 내 전문성 부족, 현재 각 부처에서 독립적으로 수행 중인 사이버 보안 업무 통합의 어려움 등 다양한 사항들을 고려하여 국가차원의 통합적 사이버 보안 위협 대응 체계 수립을 위한 논의가 이루어져야 할 것으로 보인다.

우리나라는 다른 국가와 비교하였을 때, 사이버 보안 시장의 양적 규모가 과거와 비교하여 상당히 빠르게 성장했으나 국내 사이버 보안 기업들의 규모는 대체로 크지 않으며 보안 솔루션의 개발이 회사별로 파편화되어 통합하기 힘든 구조로 되어 있어, 신기술 개발과 보안 패러다임의 변화에 대응하기 쉽지 않다. 이러한 시기에, 2021년 국가필수전략기술 중 하나로 사이버보안을 선정하고, 2022년 정보보호산업의 전략적 육성 방안을 발표한 것은 시의 적절하다고 볼 수 있다. 핵심은 이러한 세부 전략의 구체적 실행 과정에 있을 것이다. 또한 '디지털플랫폼정부' 추진 과정에서 사이버 보안의 중요성을 이해하고, 새로운 보안 패러다임

을 시범 적용해봄으로써 민간에게 방향성을 제시할 필요가 있다. 사이버 보안 신기술 연구개발, 사이버 보안 인증 제도, 보안 위협 대응 전략 등의 정책 개발 및 추진 과정에서 중복투자 방지와 일관된 제도 수립 등을 위해 부처별 역할을 정의하고 소관 업무를 조정할 수 있는, 국내 사이버 보안 산업의 진흥과 보호를 책임질 수 있는 컨트롤 타워에 대한 논의도 필요할 것이다.

사이버 보안 인력 양성과 관련하여 새 정부에서 10만 인재 양성 등 강력한 의지를 보이고 있다. 양적인 부분에 대해서는 긍정적이며 다만 이에 대해 새로운 인력 양성 방향과 구체화 노력이 필요할 것으로 보인다. 이를 위해 산업계의 수요를 반영한 인재 양성 정책을 수립해야 한다. 산업계의 수요라 함은 필요한 인력의 유형뿐 아니라 재교육이 어려운 중소기업들을 고려한 정책이 필요하다. 사이버 보안은 특히 개개인의 능력에 따라 결과가 매우 차이가 큰 분야이다. 기업의 보안을 지키면서 고급 인력을 공유하거나 기존 인력의 재교육을 통한 고급 인력 양성 등의 정책 논의가 필요할 것이다.

6. 기대효과

국내외 사이버 보안 기술 동향을 확인하고 디지털 전환 시대 공동 번영을 위한 사이버 보안 발전 방향에 대해 고찰함으로써 관련 정책을 수립하는데 있어 많은 도움이 되리라 기대한다.

SUMMARY

1. Title

Next-Generation Cybersecurity Based on Cyber Threat Intelligence

2. Objective and Importance of Research

As digital transformation accelerates, so too do cybersecurity threats. Cybersecurity is the basic basis for co-prosperity in the era of digital transformation, and at the same time, it can become the biggest risk factor for digital co-prosperity if appropriate responses are not made. To this end, the development of cybersecurity technology and appropriate policy support are essential.

This research report identifies trends in cybersecurity technologies and presents future directions for next-generation cybersecurity technologies to provide sustainable digital transformation and reliability of digital platforms. In addition, we will examine the current status of cybersecurity policies of Korea and major countries and discuss future direction of the government's support and regulation in cybersecurity.

3. Contents and Scope of the Research

The cybersecurity technologies covered in this report are divided into common security technologies, system and network security technologies, and convergence security technologies to present the current status and future technology directions. The detailed security techniques covered by each are as follows. Common security technologies include

cryptographic technologies, authentication, authorization and access control technologies, data security, hardware-based security, and AI security. System and network security technologies include cyber threat intelligence (CTI), ransomware response, IoT device security, 5G security, cloud security, and supply chain security. Convergence security technologies include smart city security, smart autonomous vehicle security, digital healthcare security, and smart factory and industrial control security. It presents the direction of technology development for these detailed technologies and a roadmap for technology development by 2030.

To address the challenges caused by the current cybersecurity technology level and present advanced future technologies, we present technology development scenarios for autonomous authentication, encryption for quantum era, OT integrated security, and AI-based security controls. For each scenario, we present the technology needed to reach the future technology level.

4. Research Results

In relation to the current state of cybersecurity technology and next-generation cybersecurity technology, the following technologies were mainly dealt with.

- Common Security
  - Cryptography
  - Authentication, Authorization and Access Control
  - Data Security
  - Hardware-based Security
  - AI Security
- System and Network Security
  - Cyber Threat Intelligence (CTI)

- Ransomeware
- IoT Device Security
- 5G Security
- Cloud Security
- Supply Chain Security

• Convergence Security
- Smart City Security
- Smart Autonomous Vehicle Security
- Digital Healthcare Security
- Smart Factory and Industrial Control Security

5. Policy Suggestions for Practical Use

The current status and future strategies of cybersecurity policies covered in this report are divided into security threat response, security industry, and R&D and human resource development.

Currently, Korea's cybersecurity threat response system is distributed to various institutions. Everyone agrees that the response system needs to be integrated into one, but there are various differences in methodology. Various bills have been proposed to establish an integrated cybersecurity threat response system at the national level, but have not yet been legislated as an agreement has not been reached. In Korea, discussions should be held to establish an integrated cybersecurity threat response system considering various matters such as people's concerns about strengthening the role of intelligence agencies, lack of expertise in cybersecurity, and difficulties in integrating cybersecurity tasks.

Compared to other countries, the quantitative scale of the cybersecurity market has grown considerably faster than in the past. But the size of domestic cybersecurity

companies is generally not large and the development of security solutions is fragmented by companies, making it difficult to cope with the development of new technologies and changes in security paradigm. At this time, it is timely to select cybersecurity as one of the national essential strategic technologies in 2021 and announce strategic fostering measures for the information protection industry in 2022. The key to success will be the specific implementation process of these detailed strategies. In addition, it is necessary to understand the importance of cybersecurity in the process of promoting the "digital platform government" and to present directions to the private sector by piloting a new security paradigm. In the process of developing and implementing policies such as research and development of new cybersecurity technologies, cybersecurity certification systems, and security threat response strategies, it is necessary to discuss a control tower that can define roles and coordinate its duties.

Regarding the training of cybersecurity experts, the new government is showing a strong will, such as training 100,000 talents. It is positive about the quantitative part, but it seems that new manpower training directions and concrete efforts will be needed. To this end, it is necessary to establish a talent training policy that reflects the demand of the industry. The demand of the industry is not only the type of manpower required, but also a policy that considers small and medium-sized companies that have difficulty in retraining. Cybersecurity is an area where the results are especially depending on the individual's ability. It will be necessary to discuss policies such as sharing high-quality manpower while protecting corporate security or training high-quality manpower through retraining of existing manpower.

6. Expectations

It is expected to help establish related policies by identifying domestic and foreign cybersecurity technology trends and examining the cybersecurity development direction for co-prosperity in the era of digital transformation.

CONTENTS

Chapter 1. Introduction

Purpose of the Study

Scope of the Study

Organization of the Report

Chapter 2. Next-Generation Cybersecurity Technologies

Common Security Technologies

System · Network Security

Security Convergence

Roadmap · Scenario of Cybersecurity Technologies

Chapter 3. Cybersecurity Policy: Status and Suggestions

Security Threat Response Policy

Security Industry Policy

R&D, Human Resources Development Policy

Chapter 4. Conclusions

제1장 서 론

제1절 연구의 필요성 및 목적

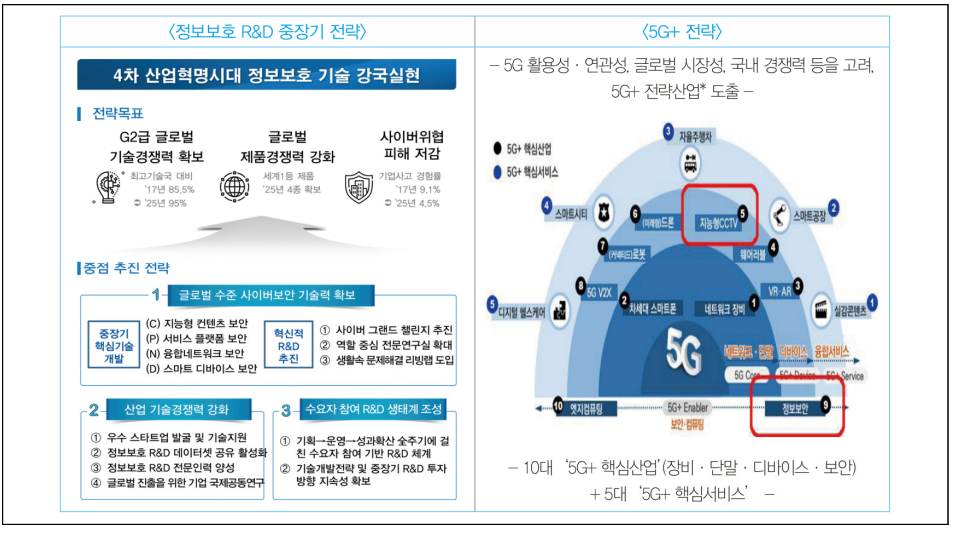
1. 연구의 필요성

인공지능을 포함한 정보통신(ICT) 기술의 발전으로 다양한 분야에서 고도화된 정보통신 기술이 활용되고 디지털 전환을 가속화하고 있다. 정보통신 기술은 점차 초연결 네트워크를 지양하여 더 많은 컴퓨터가 네트워크로 연결되고 있다. 그리고 그 적용 분야가 거의 모든 산업 분야를 아우르고 있다. 즉, 교통, 건설, 공장 제어, 의료, 교육, 전력, 치안 등 셀수 없이 많은 분야에서 정보통신 기술이 디지털 전환을 이끌고 있다. 이러한 디지털 전환은 빠른 경제, 사회 변화를 야기하고 높은 성장을 가져오지만 빠른 변화로 인한 사회, 경제적 불균형을 심화시킬 수도 있다. 즉, 정보통신 기술은 인류에 큰 도움을 주겠지만 한편으로 정보의 불균형, 사이버 보안 위협으로 인한 피해 등 다양한 취약점을 드러내고 있다.

사이버 보안 위협은 컴퓨터 시스템 수준에 머무르지 않고 재산과 생명에까지 직결되는 수준으로 커졌으며, 그 위협이나 공격이 점차 복잡, 다양해지고 있다. 즉, 사이버 공격 사후 조치만으로는 그 피해를 줄이는 것이 한계에 다다르고 있어 사전 예방을 위한 보안 역량을 최대로 끌어 올려야 하는 상황이다.

미국, EU, 중국 등 주요국들은 사이버 보안의 중요성을 일찍부터 인식하고, 사이버 보안 기술의 확보뿐 아니라 사이버 보안 위협에 빠른 대응을 위해 관련 법률, 정책 등에서 체계적인 사이버 보안 환경 구축에 노력하고 있다. 우리나라도 사이버 보안 기술을 10대 국가 필수 전략 기술로 선정하고 개인, 기업, 국가의 안전과 신뢰를 보장하는 사이버 보안 기술 개발에 힘쓰고 있다.

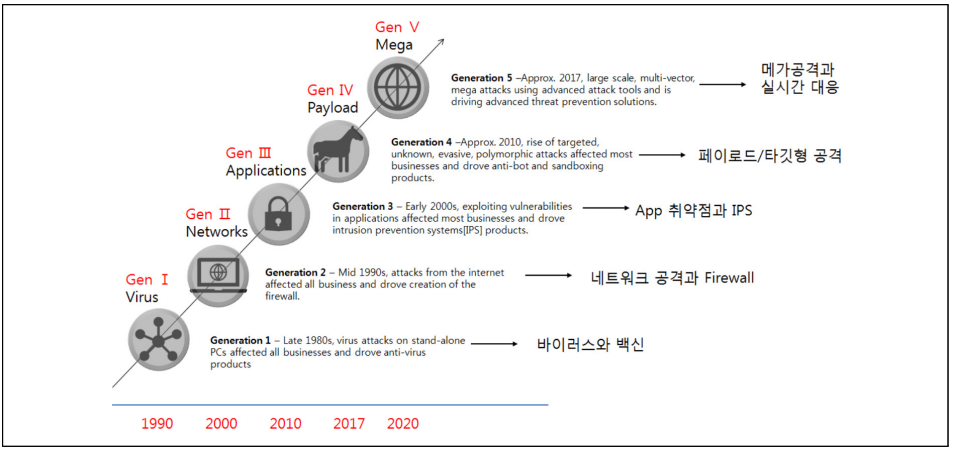
〔그림 1-1〕 국가의 정보보호 전략과 5G+의 핵심 서비스인 보안의 중요성



자료: 정보통신기획평가원, "ICT R&D 기술로드맵 2025, 차세대보안 분야"

사이버 보안 기술은 암호, 인증, 보안 반도체 등의 공통 기반 기술부터 악성 코드, 네트워크 및 클라우드 보안, 위협 분석 및 관제 등의 시스템·네트워크 기술과, 각종 분야와 융합된 자동차, 의료, 산업제어 등에서 필요한 융합 보안 기술까지 매우 분야가 다양하고 복잡하다. 4차 산업혁명의 기반이 되는 인공지능, IoT, 5G, 등의 핵심 정보통신 기술로 인해 각종 산업 분야에 초연결, 디지털, 지능화되어 미래에는 정보통신 기술의 역할이 더 커지겠지만 그만큼 사이버 보안 위협이 더욱 커지는 것도 사실이다.

〔그림 1-2〕 사이버 보안 위협과 대응 기술 진화



자료: 한글 주석은 정보통신기획평가원, “주간기술동향, 1916호, 2019”, 원본 그림은 “Check Point Infinity Whitepaper, 2019”

사이버 보안 위협의 수준도 더욱 커져서, 기존의 컴퓨터 시스템 손상, 정보 유출 수준에서 초연결, 디지털, 지능화의 결과로 물리 보안까지 위협하는 수준이 되어, 사이버 물리 시스템(Cyber Physical System) 보안이 필요하게 되었다.

사이버 보안은 디지털 전환으로 인한 공동 번영을 위한 기본 바탕임과 동시에 적절한 보안 조치가 없을 경우 디지털 공동 번영의 최대 위험 요소가 될 수 있다. 여기에는 사이버 보안 기술의 발전과 함께 적절한 지원과 정책 또한 뒷받침되어야 함은 자명하다. 본 연구에서는 디지털 공동 번영을 위해 이러한 사이버 보안의 중요성을 다시한번 강조하고 향후 사이버 보안 기술 발전 방향과 정책 방향에 대해 논하고자 한다.

2. 연구의 목적

본 연구의 목적은 국내외 사이버 보안 기술 동향을 확인하고 지속 가능한 디지털 전환과 디지털 플랫폼의 신뢰성 제공을 위한 차세대 사이버 보안 기술 방향을 제시하고 특히 사이버 위협 인텔리전스(CTI)를 기반으로 한 차세대 사이버 기술 전략에 대한 방향을 제시한다. 추가로 주요국들이 국가 차원에서 진행하고 있는 사이버 보안 정책을 확인하고 시사점을 도출하고 정부의 지원 및 규제, 지원 방향에 대해 논의한다.

제 2 절 연구의 범위

본 보고서에서 사이버 보안 기술 개발 현황과 향후 개발 방향을 다룬다. 사이버 보안 기술의 분야 중 다음의 기술을 중심으로 다룬다.

- 공통보안기술
  - 암호 기술
  - 인증·인가 및 접근제어 기술
  - 데이터 보안
  - 하드웨어 기반 보안
  - AI 보안
- 시스템·네트워크 보안
  - 사이버 위협 인텔리전스
  - 랜섬웨어 대응
  - IoT 디바이스 보안
  - 5G 보안
  - 클라우드 보안
  - 공급망 보안
- 융합보안
  - 스마트 시티 보안
  - 스마트 자율 주행 이동체 보안
  - 디지털 헬스케어 보안
  - 스마트 공장 및 산업제어 보안

제 3 절 보고서 구성

본 보고서의 구성은 다음과 같다. 2장에는 사이버 보안 기술의 현황과 차세대 사이버 보안 기술을 보안 세부 분야별로 제시한다. 3장에는 사이버 보안 관련 정책 현황과 방향에 대해 논의한다. 마지막으로 4장에서 본 보고서의 결론을 요약하고 마친다.

제 2 장 차세대 사이버 보안 기술 로드맵

제 1 절 공통 기반 보안

1. 개요 및 관련 기술

공통 기반 보안 기술은 사이버 보안 기술에 포함되는 다양한 종류의 기술들에 공통적으로 적용될 수 있는 기반이 되는 보안 기술로, 본 보고서에서는 암호 기술, 인증 기술, 데이터 보안 기술 및 하드웨어 기반 보안 기술을 포함한다.

최근, 4차 산업혁명 시대로의 진입과 함께 모든 산업에서 초연결・디지털・지능의 결합이 이루어짐으로써 디지털 대전환이 이루어지고 있으나, 한편으로는 그에 대한 부작용으로 공격 지점(Attack Surface)이 다양해지고 언제 어디서든 사이버 위협이 발생할 수 있는 문제점이 있어, 이에 대응하기 위한 차세대 보안 기술이 활발히 연구되고 있다. 차세대 보안 기술에서 요구하는 다양한 형태의 보안 요구 사항은, 이를 뒷받침하기 위한 차세대 공통 기반 보안 기술의 연구를 필요로 한다.

예컨대, 1980년대 이론적으로 언급되던 양자컴퓨터의 경우, 2019년 이미 구글에 의해 “양자 우월성”이 증명되고 IBM이 2025년 4000큐비트 이상의 성능을 가지는 양자컴퓨터의 개발 계획을 밝힘으로써, 수년 내에 양자컴퓨터와 결합된 수많은 응용이 도출될 것으로 보이나, 한편으로는 양자컴퓨터에 의한 RSA/ECC 암호 공격이 점점 현실적으로 다가오고 있다. 이는 곧, RSA/ECC에 대해 공격 가능한 양자컴퓨터가 존재하더라도, 안전한 형태의 암호(PQC, 양자내성암호)의 개발이 필요함을 의미한다.

또한, 코로나19와 함께 비대면 업무환경이 가속화되고 접속 기기와 위치가 다양화됨과 동시에, 기존 기업망 내부에서 모든 기업 내부의 데이터 및 리소스를 관리하던 환경이 클라우드로 이전되는 등의 변화는 그만큼 기업망에 대한 공격 지점이 다양해지고, 경계가 모호해지기 때문에 기존 경계 기반 보안(Perimeter Security) 방식이 더 이상 효과적이지 않게 되고 있다. 이는 곧, 기업망 내 주요 데이터의 안전을 위해서는 강력하고 지속적인 인증과 접근 제어 기술이 필요함을 의미할 것이다.

그 외에도, 인공지능 기술의 발달로 인한 수많은 기술의 지능화는, 한편으로 그 지능화에 대한 역기능을 우려하게 만듦으로써 이를 대응하기 위한 보안 기술이 필요할 수도 있음을 의미하게 된다.

따라서, 본 절에서는 차세대 사이버 보안 기술의 공통 보안 기술로서, 암호 기술, 인증·인가 및 접근제어 기술, 데이터 보안 기술, 하드웨어 기반 보안 기술 및 인공지능 보안 기술 등을 다루고자 한다.

가. 암호 기술

최근 차세대 암호 기술로 가장 관심을 받는 기술 중 하나는 다름 아닌 양자보안과 관련한 암호이다. 1900년대 초반 막스 플랑크의 에너지 양자화 가설로부터 태동되어 1920년대 후반 코펜하겐 해석, 그리고 물리학자들 사이에서 격론속에 서서히 완성되어 온 양자역학은 1980년대 초반 정보통신 기술과 융합되어 암호 기술에 많은 영향을 주기 시작했다. 첫 번째는 1981년도 R. Feynman에 의한 양자 컴퓨터의 개념적 제안이었으며, 1990년대 양자 컴퓨터에 의해 공개키 암호가 공격당할 수 있음이 이론적으로 알려진 후 양자내성암호에 대한 필요성이 도출되어 많은 연구가 진행 중에 있으며, 두번째는 1984년 C. Bennett과 G. Brassard에 의해 제안된 양자 암호로, 이론적으로는 증명 가능한 안전성을 제공한다고 알려져 있으며 주로 양자키분배에 대한 연구가 활발히 진행되고 있다.

그 외에도 IoT 등 자원이 열악한 환경에서도 안전하게 사용할 수 있는 경량 암호 기술, 암호 구현 과정에서의 약점을 이용하여 실행 단계에서 부차적으로 얻을 수 있는 암호 소요시간, 소비 전력, 방출 전자기파 등에 의한 암호 부채널 공격 및 대응 기술 등도 활발하게 연구되고 있으며, 차세대 보안 기술로서의 가치가 크다고 볼 수 있다.

1) 양자 암호

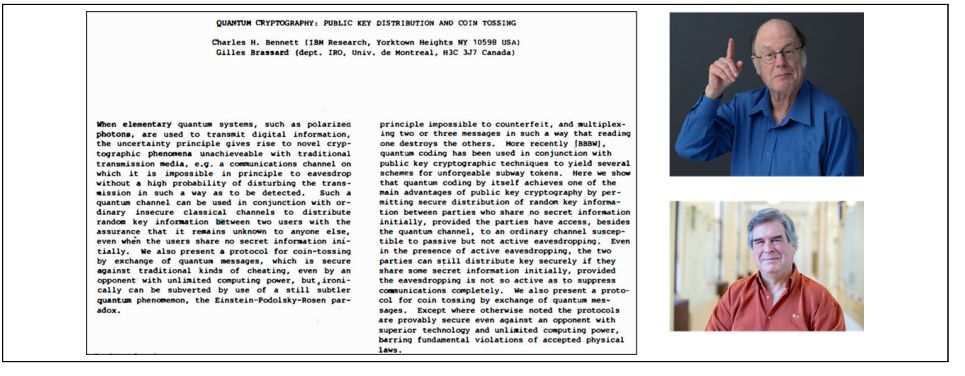
양자 암호(Quantum Cryptography)의 사전적 의미는, “암호학적인 작업 혹은 데이터의 안전한 전송을 위해 양자 역학(Quantum Mechanics)의 특징을 활용하는 암호의 한 분야”로 볼 수 있다. 즉, 양자 역학적 성질을 이용한 암호 기술을 통칭하는 것인데, 암호(Cryptography) 분야라고 하면 단순히 데이터 기밀성을 보장하기 위한 암호와/복호화

(Encryption/Decryption)만을 의미하는 것이 아니라, 키 생성과 키 은닉, 난수 생성, 전자서명 등의 암호 관련 기능을 모두 포함하므로, 양자 역학적 성질을 기반으로 이러한 암호 기능을 강화시키는 것을 모두 양자 암호라고 할 수 있다.

물론 양자 암호가 보호하고자 하는 데이터는 일반적으로 비트 단위로 표현할 수 있는 고전적 데이터로 볼 수 있으나, 차후 양자 컴퓨터 및 관련 기술(양자 메모리, 양자 저장장치 등)이 발전할 경우 흔히 큐비트 단위로 언급이 되는 양자적 데이터에 대한 안전성 이슈도 언젠가는 관심을 받게 될 것으로 보인다.

양자암호의 출발은 1984년 C. Bennett과 G. Brassard가 제안한 양자 키분배 기술 논문(이하, BB84)으로 보고 있으며, 양자 컴퓨터와는 독립적으로 발전한 기술 분야이다.

〔그림 2－1〕 C. Bennett과 G. Brassard의 양자 키분배 논문 (1984년)



QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

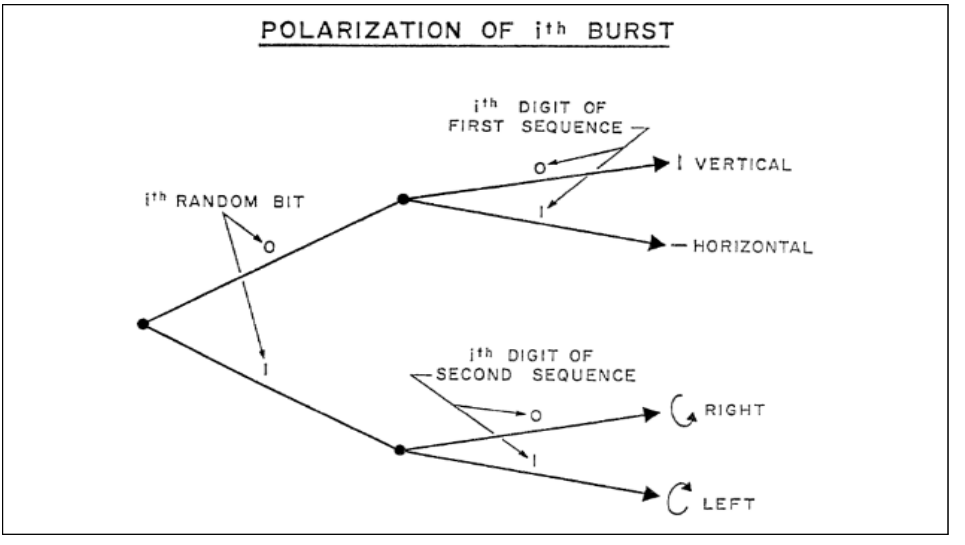
When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachieveable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected. Such a quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else, even when the users share no secret information initially. We also present a protocol for coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but, ironically can be subverted by use of a still subtler quantum phenomenon, the Einstein-Podolsky-Rosen paradox.

principle impossible to counterfeit, and multiplexing two or three messages in such a way that reading one destroys the others. More recently [BBBW], quantum coding has been used in conjunction with public key cryptographic techniques to yield several schemes for unforgeable subway tokens. Here we show that quantum coding by itself achieves one of the main advantages of public key cryptography by permitting secure distribution of random key information between parties who share no secret information initially, provided the parties have access, besides the quantum channel, to an ordinary channel susceptible to passive but not active eavesdropping. Even in the presence of active eavesdropping, the two parties can still distribute key securely if they share some secret information initially, provided the eavesdropping is not so active as to suppress communications completely. We also present a protocol for coin tossing by exchange of quantum messages. Except where otherwise noted the protocols are provably secure even against an opponent with superior technology and unlimited computing power, barring fundamental violations of accepted physical laws.

자료: 이석준, “양자 암호, 그리고 양자 시대의 안전성”, Netsec-KR 2022

Bennett 등은 이 논문이 S. Wiesner가 제안한 ‘Conjugate Coding’이라는 양자 코딩 기법에 영향을 받은 것임을 밝혔는데, S. Wiesner의 논문이 1983년에 발표되었으나 사실 해당 논문은 1970년경 이미 저널 게재가 거절당한 바 있었으므로 양자 역학이 ICT 기술과 결합된 것은 그 즈음으로 보는 것이 타당하다. S. Wiesner는 논문에서 2개의 메시지를 하나의 (양자) 메시지로 결합시켜 보내지만, 1개의 메시지를 읽는 경우 나머지 하나는 더 이상 읽을 수 없는 코딩 방식을 제안하였다.

〔그림 2－2〕 S.Wiesner의 Conjugate Code (양자 켤레코딩)



자료: S. Wiesner, "Conjugate Coding", ACM SIGACT News (1983)

여기에서 영감을 받은 C. Bennett 등은 두 참여자(보통, 암호분야에서는 안전한 데이터를 주고 받고자하는 두 사용자를 Alice와 Bob, 이 사이에서 도청 혹은 그 외의 방식으로 해킹하고자 하는 공격자를 Eve로 표현) 사이에 키를 나누어가질 수 있는 형태의 양자 키 분배를 제안하였다. 그 절차는 다음과 같다.

(1) Alice는 Bob에게 전송하고자 하는 임의의 랜덤 비트열을 생성한다.

(2) 랜덤 비트열을 전송할 때 사용하고자 하는 기저를 랜덤하게 선택한다.

(3) Alice는 랜덤 비트열 0 혹은 1에 대하여, 광자를 선택된 기저에 따라 편광시켜 전송한다. 예컨대, 1을 십자편광 기저에 따라 전송하고자 할 경우, 〔그림 2－3〕 아래 표의 두번째 열과 같이 수직 방향으로 편광시켜 전송하게 되며, 0은 세번째 열과 같이 수평 방향으로 편광시켜 전송하게 된다.

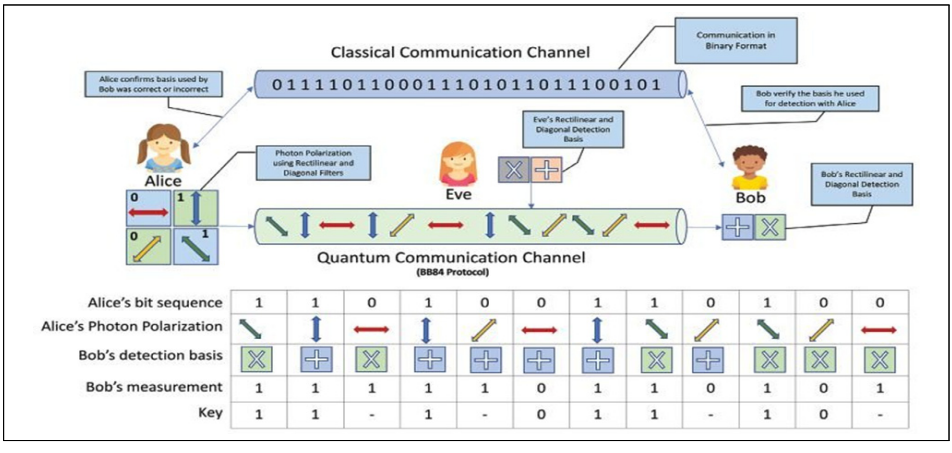
(4) Bob은 광자를 임의의 기저로 편광시켜 수신한 후 관측한다. 만일, Alice와 Bob이 특정 순서에서 사용한 기저가 같다면 동일한 비트가 관측되며, 만약 다르다면 동일한 비트가 관측될 확률은 1/2이다.

(5) Alice와 Bob은 인증된 고전 채널을 통하여 각자 랜덤하게 선택한 기저 정보를 교환한

후, 같은 기저에 해당하는 순서 상의 비트열만 추출한다. 추출된 비트열에 대해서는, Alice가 생성한 비트열과 Bob이 관측한 비트열이 일치할 것이다.

(6) 추출된 비트열 중 일부를 교환하여 에러 비율을 체크한 후, 이 값이 일정 수준을 넘지 않으면 도청이 없었다고 판단한 후 나머지 비트열을 교환된 키로서 사용한다.

〔그림 2－3〕 BB84 키분배 프로토콜 개요



자료: T. Jawaid, "Quantum Computing and the Future Internet", ISSA Journal (2020)

만약 여기에서 Eve가 개입하여 Alice가 전송한 광자의 일부 혹은 전체를 도청할 경우, Eve는 Alice가 선택했던 기저 정보를 알 수가 없으므로, 임의의 기저로 관측한 후 다시 광자를 편광시켜 Bob에게 전송해야 한다. 이 과정에서 Alice와 Eve가 선택한 기저가 다를 경우(1/2의 확률), Bob이 수신한 후 Alice의 기저로 관측하였을 때 다른 값으로 관측될 확률은 1/2가 된다. 따라서, Eve가 도청을 통해 개입하는 경우 6) 단계에서 에러 비율은 확률적으로 25% 발생하게 되므로, 적정 수준에서의 에러율을 선택할 경우 도청 여부를 판단하는 임계값으로 활용할 수 있는 것이다.

이후, 이를 변형한 프로토콜(B92 등), 그리고 얽힘의 특성을 활용한 프로토콜(E91, BBM92 등)들이 나왔다. 기저를 선택하고 광자로 편광시켜 전송하는 방법에 일부 차이는 있지만, 대체로 0 혹은 1을 인코딩할 때 선택한 편광 기저와 관측 과정에서 선택한 기저가 다를 때는, 해당 값이 중첩된 효과가 발생하여 관측할 때 랜덤한 값이 관측되는 특징을 이

용하는 것는 거의 비슷하다.

양자 키분배 프로토콜들은 대부분 이산대수 문제 혹은 소인수문제 등 기존 컴퓨터에서 빠르게 풀리지 않은 문제들에 기반한 키분배/키캡슐화 알고리즘과 달리, 증명 가능한 안전성을 가지고 있기 때문에, 양자 컴퓨터에 의한 공격에도 영향을 받지 않는다는 장점을 가지고 있다.

그러나, 암호 알고리즘이 이론적으로 완벽하더라도 암호 알고리즘을 구현하고 실행하는 과정 등에서 오류나 취약점이 존재할 수 있으며, 이론에서 요구하는 가정을 만족하도록 구현하는 것에 상당한 어려움이 있다. 일반적인 양자키분배 프로토콜은 완벽한 단일광자 생성, 오류없는 비트 인코딩, 완벽한 단일광자 감지 등을 가정하고 있는데, 문제는 이들 가정 자체가 현실적이지 않으며 최대한 만족시키기 위해서는 상당히 고가의 장비를 사용해야 한다는 데 있다.

예를 들어, PNS(Photon Number Splitting, 광자분리) 공격의 경우 단일광자생성이 이루어지지 않는 경우에 대한 도청 취약점을 드러내게 된다. 이를 해결하기 위하여 황원영 교수는 2003년 Decoy State라고 불리우는 미끼 신호를 이용하여 단일광자생성에 대한 문제점들을 해결한 바 있으며, 현재 양자 키분배 표준 혹은 구현 환경에서 널리 활용되고 있다.

〔그림 2-4〕 양자 키분배 시스템에 성공적으로 적용된 공격 리스트

Table 2.1: A list of attacks that have been launched successfully on QKD systems.

Attacks	Target Component	QKD System	References
Time shift attack	Detector	ID Quantique	[36]
Phase remapping attack	Phase modulator	ID Quantique	[37]
Faked state attack	Detector	Research system	[38]
Channel calibration attack	Detector	ID Quantique	[39]
Bright illumination blinding	Detector	ID Quantique MagiQ	[40]
Thermal blinding	Detector	ID Quantique	[41]
Superlinear detector attack	Detector	ID Quantique	[42]
Deadtime attack	Detector	Research system	[43]
After-gate attack	Detector	ID Quantique	[44]
Laser damage attack	Detector	Research system	[45]
Source tampering attack	Source	Research system	[46]
Source tampering attack	Source	Research system	[47]

자료: Z. Tang, "Measurement-Device-Independent Quantum Cryptography", Ph. D. Thesis (2016)

그럼에도 여전히 〔그림 2-4〕와 같이 양자 키분배 프로토콜에 대한 다양한 공격들이 나온 바 있으며, 이들 공격의 상당수는 광자감지기에 집중되고 있어 감지기가 아킬레스건이 되고 있는 것이 사실이다. 이러한 문제를 해결하기 위하여 MDI(Measurement-Device-Independent) 양자 키분배 방식이 출현하기도 하였으며, 실용화를 위해서는 성능과 안전성에 대한 실증 연구가 더욱 필요한 상황이다.

양자 키분배 기술 외에도 양자 난수생성기 역시 많은 연구개발이 이루어져온 분야이다. 암호키 생성 뿐만 아니라 다양한 암호 기술에서 활용되어야 하는 난수 생성과정에서 의사난수(Pseudo-Random Number)가 아닌 완전 난수 혹은 진성 난수(True Random Number)를 생성하기 위해 양자역학의 특성을 활용하는 사례들이 있는데 이를 양자난수생성기(QRNG, Quantum Random Number Generator)라고 한다.

양자 난수생성기는 크게 비광학적 방식과 광학적 방식이 있으며, 비광학적 방식은 방사성 붕괴를 활용한 방식과 전자 샷 노이즈 방식이 있고, 광학적 방식에는 광학 경로, 광자 도착 시간, 광자 수, 레이저 위상 소음 등 광자의 생성 및 전송 과정에서 보이는 랜덤한 성질을 활용하게 된다. 이렇게 생성된 난수는 생성된 값 그대로 활용되기보다는 결정적 난수비트 생성기(DRBG, Deterministic Random Bit Generator)의 입력값으로 사용된다.

이 외에도, 상대방의 양자 컴퓨터를 활용하면서도 입출력 값을 노출 시키지 않고자 하는 양자 은닉 계산(Quantum Blind Computation), 양자적으로 문서를 서명하여 정보 이론적으로 해당 문서를 전달하고자 하는 양자 일회성 전자 서명(Quantum One-Time Digital Signature), 안전하지 않은 채널 상에서 사전 교환키 없이 위치를 기반으로 안전한 통신을 하고자 하는 위치기반 양자 암호(Position-based Quantum Cryptography), 서로 믿을 수 없는 참가자간 데이터를 공유하고자 하는 양자 비트 커밋(Quantum Bit Commitment), 양자적으로 암호학적 해시 함수와 유사한 기능을 만들고자 하는 양자 지문(Quantum Fingerprinting) 등 수많은 양자 암호 기술 분야가 있으나, 양자 키분배와 양자 난수생성기를 제외하면 대부분 이론적인 연구 수준에 머물러 있으며 현실적인 응용을 찾지 못한 상태이다.

2) 양자내성암호

앞서 언급한 바와 같이, 1981년 R. Feynman은 양자역학의 현상을 컴퓨터로 시뮬레이션

하는 과정에서의 폭발적인 연산량을 해결하기 위한 방법으로서, 양자 컴퓨터를 제안한 바 있다. 처음에는 양자 시뮬레이션 외에 다른 컴퓨팅 응용으로의 적용 가능성에 대해선 크게 관심을 받지 못했으나, 1985년 D. Deutsch가 Deutsch 문제를 제안하고 이를 고전컴퓨터보다 지수적으로 빠르게 해결할 수 있는 양자 알고리즘을 제안함으로써 처음으로 양자컴퓨터가 고전컴퓨터보다 특정 문제들을 빠르게 해결할 수 있는 가능성을 열게 되었다.

Deutsch 문제의 경우 확률적인 알고리즘을 허용하는 경우는 고전컴퓨터에서도 양자알고리즘처럼 빠르게 문제를 해결할 수 있기 때문에, 엄밀히 보면 반드시 양자컴퓨터의 우월성을 증명하는 경우는 아니었다. 그러나, 1993년 Bernstein과 Vazirani는 새로운 문제를 정의하여 양자컴퓨터와 고전컴퓨터 사이에 비결정적인 양자 이득이 존재함을 증명하였으며, 1994년 Simon의 주기 발견 양자알고리즘에 영향을 받은 Shor 알고리즘이 다항 시간내에 소인수분해와 이산대수 문제를 해결할 수 있음이 알려지면서 양자컴퓨터는 본격적으로 많은 관심을 받게 되었다. 이후, 1996년 비구조화된 데이터 검색알고리즘의 양자적 성능개선이 가능한 Grover 알고리즘이 발표되었으며, 이 알고리즘은 Shor 알고리즘처럼 특정 암호를 깰 수 있는 수준은 아니지만 안전성 비도 자체를 절반 수준으로 만들 수 있는, 또다른 강력한 양자 알고리즘이다.

〔그림 2－5〕 양자컴퓨터 개발의 동기: 양자 알고리즘의 역사

자료: 이석준, “암호 양자보안 검증 플랫폼 <Q!Crypton>”, Netsec-KR 2020

기존 컴퓨터에서는 정보 처리 기본 단위로 비트를 사용하며, 이는 0 혹은 1의 확정된 값으로 연산을 수행하게 된다. 그러나 양자 컴퓨터의 경우, 0과 1이 중첩된 상태로 존재할 수 있는 큐비트를 정보 처리의 기본 단위로 사용하기 때문에, 중첩된 상태에서 연산이 가능하여 병렬 계산이 가능한 특성을 가지고 있다. 연산 면에서는 월등한 능력을 가지고 있으나, 단 중첩된 상태는 관측되지 않은 상태에서만 유지가 가능하며, 큐비트 상태를 알아보기 위하여 관측을 할 경우 0 혹은 1 중 하나의 상태, 즉, 고전비트로 붕괴되는 특성이 있다. 따라서, 모든 문제(특히, NP)에 대해 지수적인 성능 개선을 보일 수는 없으나, 우연히도 RSA 혹은 ECC와 같이 현대 암호에서 많이 활용되는 공개키 암호 알고리즘의 기반 문제인 소인수분해와 이산대수 문제를 다항시간안에 풀 수 있어, 현대 암호의 근간이 흔들리게 되었다.

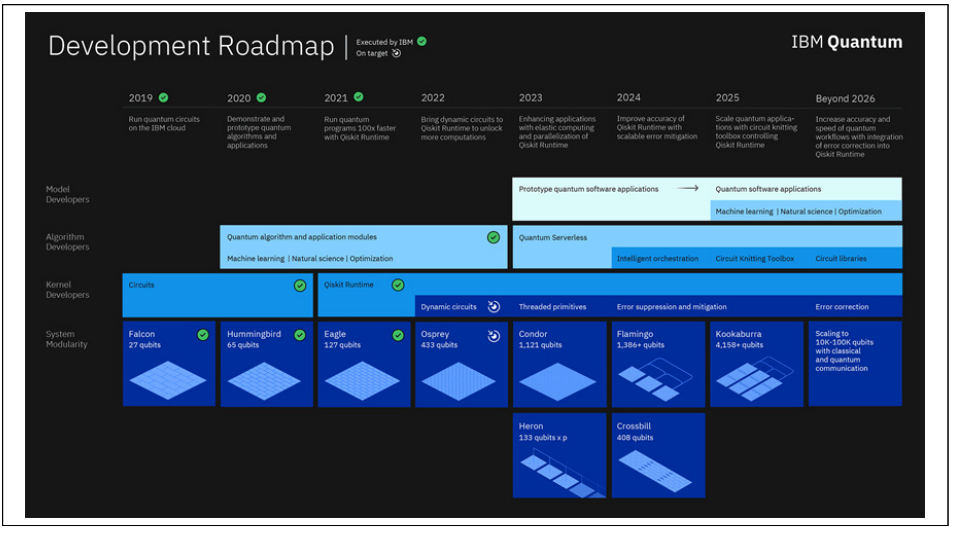
소인수분해와 소수 기반의 타원곡선이산대수 문제를 풀기 위한 양자컴퓨터의 자원량(큐비트 수 및 토폴리 양자게이트 수)은 〔그림 2-6〕과 같다. 이 그림에서 현재 많이 사용되는 RSA-2048을 공격하기 위해서는 최소 4098큐비트가 필요함을 알 수 있다. 〔그림 2-7〕과 같이 IBM이 최근 발표한 로드맵에 따르면, IBM은 2025년 4158큐비트를 갖는 양자컴퓨터를 개발하고자 함으로 RSA에 대한 공격이 얼마 남지 않은 것으로 보일 수 있다.

〔그림 2-6〕 소인수분해 및 타원곡선이산대수 문제를 풀기 위한 이론적 양자자원량

ECDLP in $E(\mathbb{F}_p)$ simulation results					Factoring of RSA modulus N interpolation from [21]		
$\lceil \log_2(p) \rceil$ bits	#Qubits	#Toffoli gates	Toffoli depth	Sim time sec	$\lceil \log_2(N) \rceil$ bits	#Qubits	#Toffoli gates
110	1014	$9.44 \cdot 10^9$	$8.66 \cdot 10^9$	273	512	1026	$6.41 \cdot 10^{10}$
160	1466	$2.97 \cdot 10^{10}$	$2.73 \cdot 10^9$	711	1024	2050	$5.81 \cdot 10^{11}$
192	1754	$5.30 \cdot 10^{10}$	$4.86 \cdot 10^{10}$	1 149	–	–	–
224	2042	$8.43 \cdot 10^{10}$	$7.73 \cdot 10^{10}$	1 881	2048	4098	$5.20 \cdot 10^{12}$
256	2330	$1.26 \cdot 10^{11}$	$1.16 \cdot 10^{11}$	3 848	3072	6146	$1.86 \cdot 10^{13}$
384	3484	$4.52 \cdot 10^{11}$	$4.15 \cdot 10^{11}$	17 003	7680	15362	$3.30 \cdot 10^{14}$
521	4719	$1.14 \cdot 10^{12}$	$1.05 \cdot 10^{12}$	42 888	15360	30722	$2.87 \cdot 10^{15}$

자료: M. Roetteler et al, “Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms”, Asiacrypt 2017

〔그림 2-7〕 IBM의 양자컴퓨터 개발 로드맵

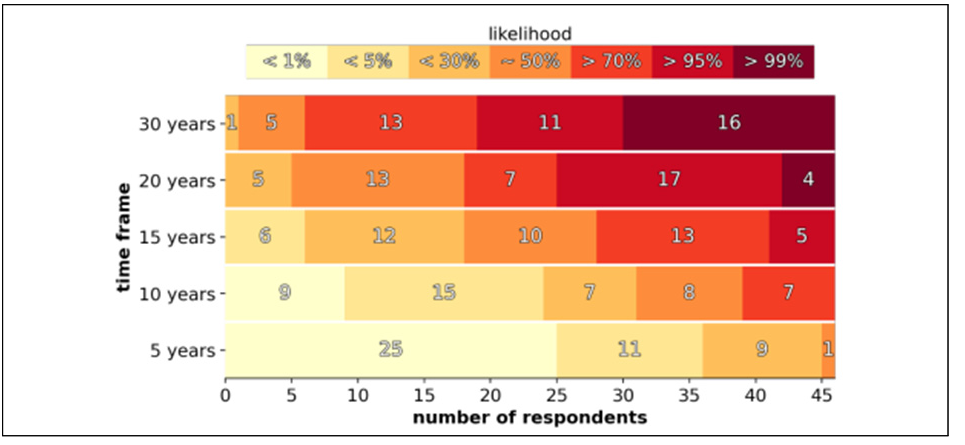


자료: IBM, "Our new 2022 Development Roadmap", https://www.ibm.com/quantum/roadmap (Last accessed: 2022년 9월 26일)

그러나, 논리적 수준에서의 양자자원량과 물리적 수준에서의 양자 자원량 사이에는 차이가 있을 수 밖에 없다. 양자 상태를 오래 유지하기 위한 결맞음시간, 양자큐비트 칩이 본질적으로 내재하는 오류, 양자 큐비트칩상의 큐비트간 구조 등을 고려하면 실질적으로는 훨씬 많은 양자자원량을 필요로 하며, C. Gidney 등도 2021년 발표한 논문에서 RSA-2048 정수를 소인수분해 하기 위해서는 물리 큐비트의 경우 약 2천만 큐비트가 필요하다고 밝히고 있다. 이 논문 역시 여러 가정에 근거하여 계산한 것이므로, 가정과 현실이 다를 경우 이 숫자는 일부 조정될 여지가 있다.

Mosca의 부등식으로 유명한 M. Mosca는 2015년 RSA-2048이 2026년까지 깨질 확률이 1/7, 2031년까지 깨질 확률은 1/2라고 언급하였으나, 이는 약간 과한 주장으로 보이며 M. Mosca는 2022년 초 발표한 자신의 리포트에서 관련 전문가들로부터 조사를 한 경과 〔그림 2-8〕과 같은 결과를 얻은 바 있다. 해당 조사를 분석하면 향후 15년 정도(2037년) 후에 깨질 확률이 1/2 정도로 여겨진다는 것이다.

〔그림 2－8〕 24시간 내에 RSA-2048 공격 가능한 양자컴퓨터 전문가 예측

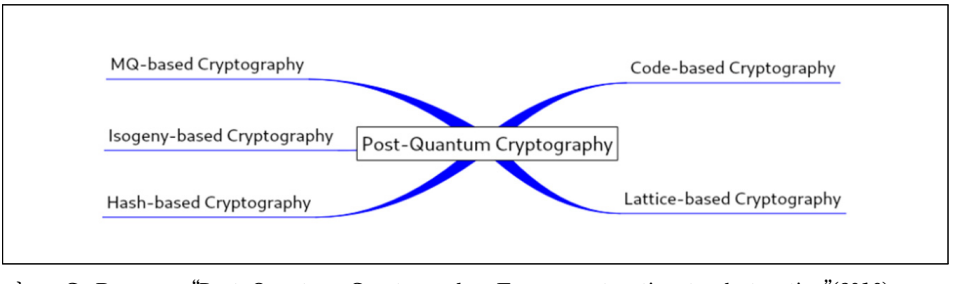


자료: M. Mosca et al, “2021 Quantum Threat Timeline Report”, Global Risk Institute (2022)

중요한 것은, 현재 사용하는 주요 공개키 암호 알고리즘은 향후 20~30년 이내에 깨질 확률이 상당히 높다는 것으로, 이 위험성은 곧 이들 암호 알고리즘을 대체할 수 있는, 즉 양자컴퓨터에 의해서도 강인한 암호인 양자내성암호의 필요성을 야기하게 되었다.

사실, 양자내성암호의 경우 이미 2000년대 초중반부터 많은 연구가 있었다. 이를 기반 문제에 따라 분류할 경우, 격자(Lattice) 기반, 코드 기반, 다변수 이차식(MQ) 기반, 아이소제니 기반, 해시 기반 등의 기법들이 있는데, 특히 많은 연구가 이루어진 것이 격자 기반 공개키 암호이다.

〔그림 2－9〕 PQC(양자내성암호) 종류



자료: G. Banegas, “Post-Quantum Cryptography: From construction to destruction”(2019)

미국 표준기관이자 AES, SHA 등 주요 암호에 대한 표준 알고리즘을 공모 절차를 통해서 표준화한 NIST에서는 2015년부터 이에 대한 준비를 하였다. NIST에 의한 PQC 표준화는 공개키 암호화(PKE)/키 캡슐화 방법(KEM) 알고리즘과 전자서명 알고리즘 트랙으로 나누어 진행하였으며, 진행 일정은 〈표 2-1〉과 같다. 2017년 82개 후보의 등록을 시작으로, 2017년 Round 1, 2019년 Round 2, 2020년 Round 3 발표에 이어 2022년 7월 2022년 표준 알고리즘 4종(격자기반 PKE/KEM 1종, 격자기반 전자서명 2종, 해시기반 전자서명 1종)을 발표하였고, 추가로 4종에 대한 Round 4 진행을 공표하였다.

〈표 2-1〉 NIST의 PQC 표준화 진행 일정

시기	PQC 표준화 진행 사항 및 계획
2015.08	NSA, "IAD 주도로 양자내성암호 개발 필요" 인지
2016.02	NIST, 양자내성암호 리포트 발간 (NISTIR 8105) 및 표준화 계획 예비 발표
2016.08 ~ 2016.09	NIST, 초안 제출 요구사항 및 평가 기준 의견 수렴
2016.12	요구사항 및 기준 확정 3가지 분야 (전자서명, 암호화, 키교환) 후보 공개 모집
2017.11	전세계로부터 82개 PQC 후보 제출받음
2017.12	69개 PQC 후보 게재 (Round 1) (이후 5개 철회) - Lattice기반 26개, Code기반 19개, MQ기반 9개, 해시기반 3개, 기타 7개
2018.04	1st NIST PQC Workshop
2019.01	26개 PQC 후보 발표 (Round 2) - Lattice기반 12개, Code기반 7개, MQ기반 4개, 해시기반 1개, 기타 2개
2019.08	2nd NIST PQC 표준화 컨퍼런스
2020.07	7개 최종 PQC 후보 및 8개 대체 후보 (Round 3)
2022.07	4개 PQC 표준 알고리즘(안) 및 추가 후보 발표 (Round 4)
2024	최종 표준 공표 예정

이미 선택된 알고리즘이 4종이 있음에도 추가로 Round 4를 진행하는 이유는, 현재까지 성능과 안전성 면에서 많은 장점이 있는 격자 기반 암호화 방식이 주로 선정되었기 때문인데, 혹시라도 이 문제가 새로운 공격에 의해 안전성에 문제가 될 가능성에 대비하여 다

른 방식의 암호에 대한 논의를 추가로 진행하고자 함이다. 그렇지만, 최종 표준 알고리즘으로 선정된 CRYSTALS-Kyber 및 CRYSTALS-Dillithium, Falcon 등이 가장 먼저 활용될 가능성이 높다고 보인다.

3) 경량 암호

초창기 컴퓨터 및 인터넷 기술은 하드웨어의 성능이 개선되고 비용이 저렴해지면서 서버 기반 환경에서 점차 PC, 스마트 기기, IoT 기기로 이동해왔으며, 기존의 유선 환경도 이동통신과 무선랜 및 저전력 통신 근거리 통신 기술의 발달로 모바일로 영역이 확장되면서, 점차 IoT 기반의 초연결 사회로 진화를 할 수 있는 바탕이 되었다.

초소형 컴퓨팅와 저전력 네트워크 기술을 모두 포괄하는 IoT 기술의 발달은, IT 기술이 기존 산업과 결합되어 새로운 산업을 만드는 원동력이 되어, 헬스케어, 제어 시스템, 자율주행 자동차, 드론 뿐만 아니라 일상에서 사용하던 기존 기기(예, TV, 냉장고, 청소기, 스피커 등)들을 모두 스마트한 환경으로 바꿈으로서 사용자들에게 편리함과 유용함을 제공하고 있다.

그러나, 점점 늘어나는 IoT 기기, 스마트 기기들은 그 자체에서 생성하는 데이터 및 정보들이 사용자의 민감 정보 혹은 프라이버시 관련 정보를 활용하는 것이 일반적일 뿐만 아니라, 그 자체로 공격에 대한 진입점을 다양화하는 결과를 초래한다. 그럼에도, IoT 기기는 컴퓨터 등 기존 컴퓨팅 기기와 비교하였을 때 계산 능력, 공급 전력 등이 제한적이기 때문에, 기존 암호 기법에 기반한 보안 방식을 그대로 사용하기가 어렵다.

NIST에서는 이러한 이슈를 해결하기 위해서 양자내성암호와 같은 다른 종류의 암호 알고리즘과 마찬가지로 경량 암호에 대한 필요성을 인식하여 표준화 작업을 진행하고 있으며, 진행 일정은 〈표 2-2〉와 같다. 요구사항으로는 기밀성과 무결성을 위해 AEAD를 지원할 수 있어야 하며, 해시 기능을 선택적으로 지원할 수 있다. 또한 기존 NIST 표준 암호 알고리즘과 비교하여 제한된 환경(HW/SW 플랫폼)에서 더 나은 성능을 보여야 하며, 짧은 메시지에도 효율적이고, 부채널 공격 및 Fault 공격에 대응하기가 쉬운 구현을 요구하였다.

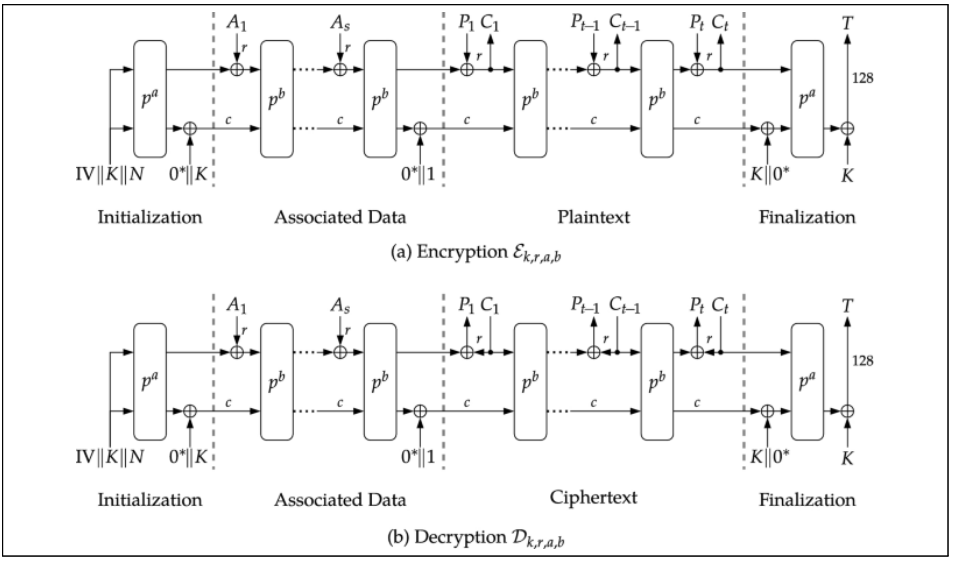
〈표 2-2〉 NIST의 경량 암호 표준화 진행 일정

시기	경량 암호 표준화 진행 사항 및 계획
2015.07	1차 경량암호 워크숍 개최
2016.10	2차 경량암호 워크숍 개최
2018.08	경량암호 제안 알고리즘 요구사항 및 평가기준 확정, 공표
2019.02	경량암호 제출 마감 (총 57종)
2019.04	56개 경량암호 후보 알고리즘 선정 (Round 1)
2019.08	32개 경량암호 후보 알고리즘 선정 (Round 2)
2019.11	3차 경량암호 워크숍 개최
2020.10	4차 경량암호 워크숍 개최
2021.03	10개 최종 후보 알고리즘 선정 (ASCON, Elephant, GIFT-COFB, Grain128-AEAD, ISAP, Photon-Beetle, Romulus, Sparkle, TinyJambu, Xoodyak)
2021.07	2라운드 후보 현황 보고서 발간 (NIST IR 8369)
2022.05	5차 경량암호 워크숍 개최
2023	NIST 경량암호 최종 알고리즘 채택 (예정)

NIST의 표준화 공모 이전인 2012년 시저(CAESAR) 경진대회가 시작되어, 경량성과 보안성을 갖춘 인증 암호화 기법에 대한 경쟁이 있었고, ASCON은 경량 응용(리소스가 제한된 기기 환경) 카테고리에서 우승한 경량 인증암호 알고리즘이다.

ASCON은 〔그림 2-10〕과 같이 12라운드의 sponge 구조를 채택했으며, sponge 구조에 사용된 블록암호는 SPN(Substitution-Permutation Network) 구조이다. Substitution 계층에 사용되는 S-Box는 Diffusion을 향상시키기 위하여 SHA-3(Keccak)의 S-Box에 아핀변환을 적용하여 얻은 새로운 S-Box를 사용하였으며, Permutation Layer는 SHA-2의 Σ 함수와 유사한 선형함수를 사용했다. 안전성을 위해 일반적인 Sponge 구조에서에서 키를 사용한 초기 함수와 최종 함수를 사용하였으며, 효율성 관점에서는 64비트 워드 연산(NOT, AND, OR, XOR, Rotation)만 사용하여 구현할 수 있어, 별도의 메모리가 필요하지 않고 효율적인 병렬처리가 가능하도록 설계되었다.

〔그림 2－10〕 ASCON 알고리즘의 암복호화 구조



자료: C. Dobraunig et al, “Ascon v1.2: Lightweight Authenticated Encryption and Hashing”, Journal of Cryptology (2021)

4) 암호 부채널 분석 공격 및 대응 기술

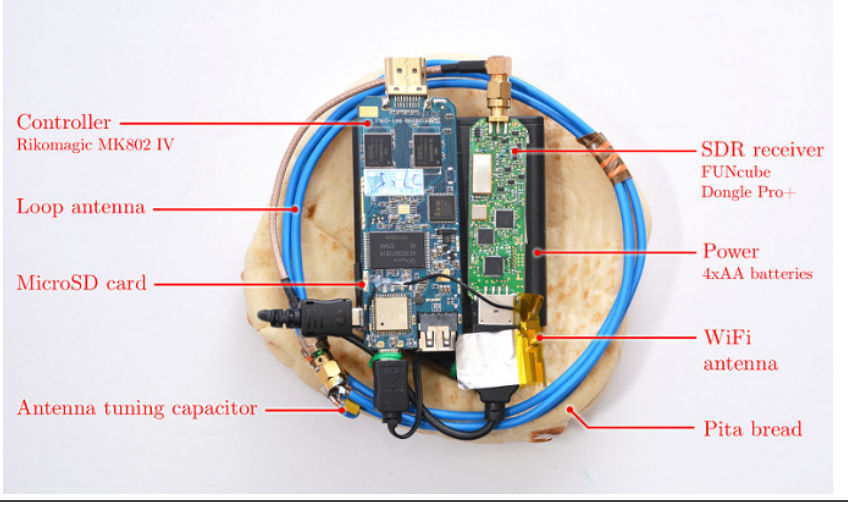
현대 암호의 기본 원칙은 암호 시스템에 관한 모든 것, 즉 알고리즘이나 평문-암호문 쌍이 공개된다 하더라도 키가 안전하게 유지될 경우, 안전성이 유지되어야 한다. 따라서 이러한 원칙하에 설계된 현대 암호들은, 이론적으로 키가 노출되지 않는다는 전제하에 안전하기 때문에 키를 랜덤하게 생성하고 공격자가 접근할 수 없는 위치에 저장하는 것을 매우 중요하게 고려하였다.

그러나, 이론적 안전성(증명 가능한 안전성 혹은 계산적 안전성)과 함께 비밀키가 안전하게 보호받는 암호 알고리즘이라 하더라도, 특정한 시스템 혹은 하드웨어에서 운용되는 과정에서 의도하지 않은 부가 정보가 발생할 수 있다. 이러한 정보를 부채널 정보라고 하는데, 여기에는 암호 소요시간, 소비 전력, 방출 전자기파 혹은 그 외에 다른 부차적인 정보들을 포함하게 되며, 이러한 정보를 활용하여 키 혹은 암호 알고리즘의 안전성에 대해 공격하는 기법을 부채널 분석 공격이라고 한다.

1999년 P. Kocher에 의한 DES 공격이 이루어진 이후, 이론적인 안전성이 어느 정도 검

증된 암호 알고리즘이라 하더라도 구현 및 운용 과정에서의 공격 가능성이 알려지면서 많은 연구들이 진행되었으며, 특히 전력과 전자기파를 부채널 정보로 활용한 공격들이 스마트카드와 같은 저사양기기를 중심으로 많이 이루어졌다. 2014년 이스라일의 Tel Aviv 대학에서는 〔그림 2-11〕과 같은 피타 브레드(Pita Bread) 모양의 디바이스를 사용하여 컴퓨터에 저장된 암호화 키를 공격한 사례를 발표한 바 있으며, 이 장치는 50cm 정도 떨어져 1.7MHz 범위의 전자기파 신호를 모은 후 RSA 및 ElGamal 암호 알고리즘을 사용하는 오픈소스 GnuPG 1.x 구동 노트북에서 신호를 수집하여 키를 추출하는 방식으로 공격을 수행하였다.

〔그림 2-11〕 Tel Aviv 대학의 부채널 공격 장치



자료: D. Genkin et al, "Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation", CHES 2015

또한 RSA 알고리즘이 구동중인 공격 대상 PC의 프로세서에서 발생하는 소리를 마이크로 수집하여 필터링 후 분석하여 RSA 비밀키를 분석한 사례가 있으며, 심지어 2011년에 발생한 신용카드 도난 및 이를 사용한 범죄 사건에서 2010년 학회에서 실험실 수준으로 수행한 부채널 공격 방법이 사용된 사례가 있었다(〔그림 2-12〕).

〔그림 2－12〕 부채널 공격 기법으로 PIN 우회에 성공한 위조 카드

자료: H. Ferradi et al, "When Organized Crime Applies Academic Results: A Forensic Analysis of an In-Card Listening Device", Journal of Cryptographic Engineering (2016)

부채널 분석 공격은 크게 논프로파일링 공격과 프로파일링 공격으로 나뉜다. 논프로파일링 공격은 공격자가 공격 대상 장비로부터만 부채널 정보를 얻는 공격이며, 단순전력분석(SPA, Simple Power Analysis), 차분전력분석(DPA, Differential Powr Analysis), 상관전력분석(CPA, Correlation Power Analysis), 상호정보량분석(MIA, Mutual Information Analysis) 등이 있다. 프로파일링 공격은 공격 대상 장비와 동일하며 프로그래밍 가능한 프로파일링 장비가 있는 환경에서의 공격을 의미하며, 템플릿 공격(Template Attack), Stochasitic Model 등이 있다.

부채널 분석 공격에 대응하기 위한 방법으로는 마스킹 대응 기법과 하이딩 대응 기법 등이 주로 활용되는데, 마스킹 대응 기법은 실제 랜덤 값을 이용하여 중간값을 랜덤하게 보이도록 함으로써 중간값을 추정하지 못하게 하는 방지 기법이며, 하이딩 대응 기법은 신호대잡음비(SNR, Signal-to-Noise)를 감소시킴으로써 부채널 정보와 연산, 처리 데이터 간 관계성을 감소시키는 방법으로 연산 순서를 바꾸거나 연산과 데이터에 무관하게 일정한 부채널 정보를 발생시키는 방법 등이 가능하다.

최근 부채널 공격 기술 동향과 관련하여 크게 2가지 중요 흐름이 있다고 보인다. 첫번째로는 부채널 공격 대상으로 PQC 암호 알고리즘에 대한 부채널 공격에 대한 연구가 많이

진행되고 있다는 것이며, 두번째로는 딥러닝 등 인공지능 기술을 부채널 분석에 활용하는 연구도 활발히 진행되고 있다.

PQC 관련해서는, 2018년 L. Bruinderink 등에 위해 격자 기반 전자서명인 qTESLA와 CRYSTALS-Dilithium 등이 오류주입공격을 통한 서명위조 공격이 가능함을 보인 바 있으며, 2017년과 2019년 P. Pessl 등은 격자 기반 암호 알고리즘에서 활용되는 NTT 연산에 대한 템플릿 공격을 제안한 바 있다. 또한 2020년 P. Ravi 등은 P. Pessl의 부채널 공격에 대응하기 위한 안전한 셔플링 및 마스킹 기법을 제안하여 CRYSTALS-Kyber와 CRYSTALS-Dilithium에 적용하여 시험한 사례 등이 대표적이다. 다변수 이차식 기반의 PQC 알고리즘에 대한 부채널 공격도 2019년 J. Krämer 등에 의해 연구되었으나, 알고리즘 자체의 안전성이 취약하다는 연구 결과가 나오기 시작하면서 부채널 공격에 대한 연구는 거의 진행되지 않을 것으로 보인다.

딥러닝 기법을 이용한 부채널 분석은 전력 모델링에 신경망을 활용하는 방법, 대칭키 및 공개키 암호에 대한 프로파일링 중간값/키 분석에 딥러닝을 활용하는 방법, 논프로파일링 공격에 딥러닝을 활용하는 공격, 파형 인코딩 및 전처리에 딥러닝을 활용하는 방법, 설명가능한 인공지능 기술(XAI, Explainable Artificial Intelligence) 기반의 부채널 누출신호 탐색 기법 등이 있다.

나. 인증・인가 및 접근제어 기술

인증(Authentication)은 통신 당사자간 상대의 신분을 확인하는 절차를 의미한다. 기기에 대한 인증도 가능하지만, 일반적으로 인증이라 함은 사용자별로 식별 정보를 만들고, 그 식별 정보가 그 사람의 것임을 증명하기 위한 인증 정보를 동시에 혹은 추가적으로 제공함으로써 절차를 진행하는 것이 일반적이다. 서비스 제공자 혹은 사용자가 속한 회사 등은 인증이 완료된 사용자에 대해서 어떤 리소스(데이터, 네트워크, 서비스 등)에 접근할 수 있는지에 대한 권한을 허용해야 하는데 이러한 과정을 인가(Authorization)라고 한다. 허용된 권한 및 상황에 따라, 서비스 제공자가 해당 리소스에 대한 접근을 허락하거나 거부하는 등의 절차를 거치는 것을 접근제어라고 한다.

인증은 특정 서비스 혹은 네트워크에서 사용자로부터 신뢰를 확보하는 가장 첫 단계이자, 필수적인 절차이므로 보안에 있어서 가장 중요한 기술 중 하나이다. 코로나19와 함께

비대면 업무환경이 가속화되고 접속 기기와 위치가 다양화됨과 동시에, 기존 기업망 내부에서 모든 기업 내부의 데이터 및 리소스를 관리하던 환경이 클라우드로 이전되는 등의 변화는 그만큼 기업망에 대한 공격 지점이 다양해지고, 경계가 모호해지기 때문에, 패스워드와 같은 단순한 방식의 인증이나 인가, 접근 제어는 더 이상 효과적이지 않다.

즉, 응용 서비스 혹은 기업망 내 주요 데이터와 리소스의 안전을 위해서는 강력하고 지속적인 인증과 접근 제어 기술이 필요함을 의미할 것이다. 따라서, 차세대 보안 기술 관점에서는 사용자에게 불편함을 주지 않으면서도 안전하고 빠르게 서비스를 제공하는 방향으로의 진화가 필요하며, 특히 멀티팩터 인증, 무자각 인증, 블록체인 기반 분산 ID 기술 등을 눈여겨 보아야 할 것이다.

접근제어 기술의 경우, 최근 사용자의 속성, 권한과 역할이 다양해지고 데이터, 네트워크, 리소스 등 구조가 복잡해지면서, 특히 기업망 등을 중심으로 보안을 위한 세밀한 형태의 접근제어 기술을 요구하고 있다. 역할 기반 접근제어 혹은 속성 기반 접근제어의 이론적 개념 자체는 나온지 오래 되었으나, 일반적으로 접근제어가 사용되는 환경의 관리 복잡성으로 인하여, 그 목적에 맞도록 세밀하게 접근제어를 하는 것이 쉽지 않다. 즉, 차세대 보안 관점에서의 인가 및 접근 제어는 기술보다는 관리, 통제, 거버넌스 등의 관점에서 접근하는 것이 바람직하므로 본 문서에서는 다루지 않는다.

1) 멀티팩터 인증

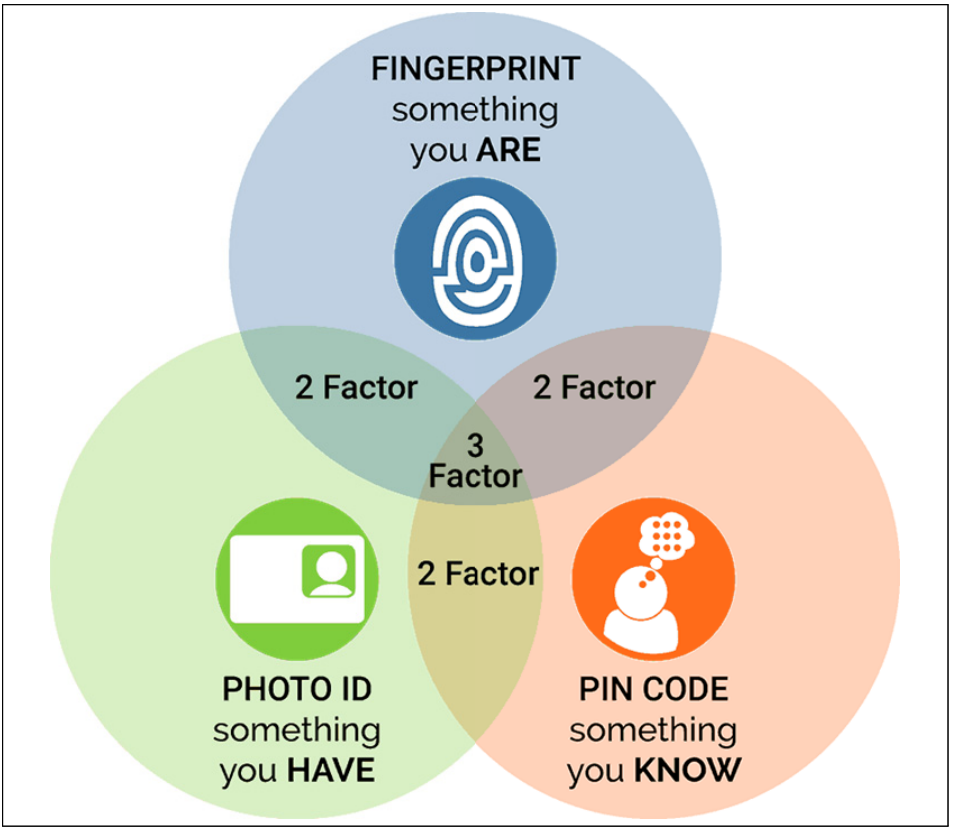
사용자를 인증하는 방법은 어떠한 인증 요소(Factor)을 사용하느냐에 따라 각각 지식기반 인증, 소유기반 인증, 속성 기반 인증으로 나누게 된다. 여기서 지식기반 인증이라함은 사용자만 알고 있는 것으로, 흔히 사용하는 패스워드, PIN코드값 등이 일반적이며 일부 환경에서는 미리 설정해놓은 답변 등을 요구하기도 한다. 소유기반 인증은 사용자가 소유하고 있는 것으로, 휴대폰 SMS 기반 인증, 보안카드, OTP, 공인인증서 등이 있으며, 신분증이나 사원카드, 신용카드 등이 활용되기도 한다. 속성기반 인증은 사용자만의 고유한 속성을 의미하는 것으로 지문, 정맥, 홍채, 얼굴과 같은 생체 인증이나 서명, 필체와 같은 행동기반 인증 등을 포함한다.

이들 인증 방법들은 각각 장단점을 가지고 있는데, 예를 들어 패스워드와 같은 지식기반 인증은 가장 편리한 반면 사회공학적으로 해당 지식이 유출될 가능성이 상대적으로 높

고, 무작위 대입, 사전 공격 등에 대응할 수 있는 기법이 적용되어야 한다는 단점이 있다. 소유기반 인증의 경우, 지식기반 대비 유출 가능성이 적으나 그럼에도 도난 가능성이 있으며 본인이라 하더라도 인증시 소유하고 있지 않으면 인증을 받을 수 없다는 단점이 있다. 속성 기반 인증은 편리하지만, 인식 과정에서 오류가 발생할 수 있고 별도의 장치가 필요하다는 단점이 있다. 또한 탈취의 가능성은 가장 적으나 그럼에도 고해상도 사진 혹은 해킹된 스마트폰 등을 이용하여 탈취되는 사례 등이 있으며, 한번 탈취되면 변경이 불가능하여 피해가 누적될 수 있다는 단점이 있다.

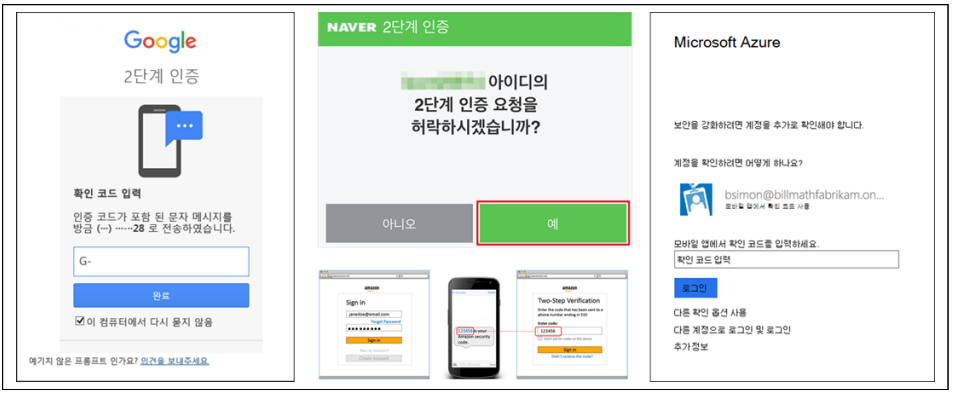
인증 과정에서 이러한 인증 요소를 하나가 아닌 둘 이상 결합하여 사용하는 것을 멀티팩터 인증(MFA, Multi-Factor Authentication)이라고 한다. 〔그림 2－13〕에서와 같이 신분증과 지문을 동시에 사용하는 것은 멀티팩터 인증 중에서도 2-Factor 인증으로 볼 수 있으며, 여기에 PIN Code를 같이 사용하면 3-Factor 인증이 될 것이다. 구글의 경우, 구글 서비스에서 2-Factor 인증을 자동 활성화함으로써 계정 해킹을 50% 줄였다고 밝힌 바 있으며, 〔그림 2－14〕에서 보는 바와 같이 구글이나 네이버, 아마존, MS 등 서비스 제공 업체, 또한 시스코, RSA, 이셋 등 다양한 기업망 보안 솔루션 업체들도 멀티팩터 인증을 지원하고 있다.

〔그림 2－13〕 멀티팩터 인증의 예



자료: https://www.borer.co.uk/borer-technology/multi-factor-identity-authentication/ (Last accessed: 2022년 9월 26일)

〔그림 2－14〕 다양한 서비스 상의 2단계 인증 방법



자료1: https://support.microsoft.com/ko-kr/office/outlook에-gmail-계정-추가-70191667-9c52-4581-990e-e30318c2c081
자료2: https://help.naver.com/service/5640/contents/19238?osType=PC&lang=ko
자료3: https://kdp.amazon.com/en_US/help/topic/G6HTFZJLJ7AJQ56R
자료4: https://support.microsoft.com/ko-kr/account-billing/2단계-인증-방법을-사용하여-직장-또는-학교-계정에-로그인-c7293464-ef5e-4705-a24b-c4a3ec0d6cf9 (Last accessed: 2022년 9월 26일)

2) FIDO (Fast IDentity Online)

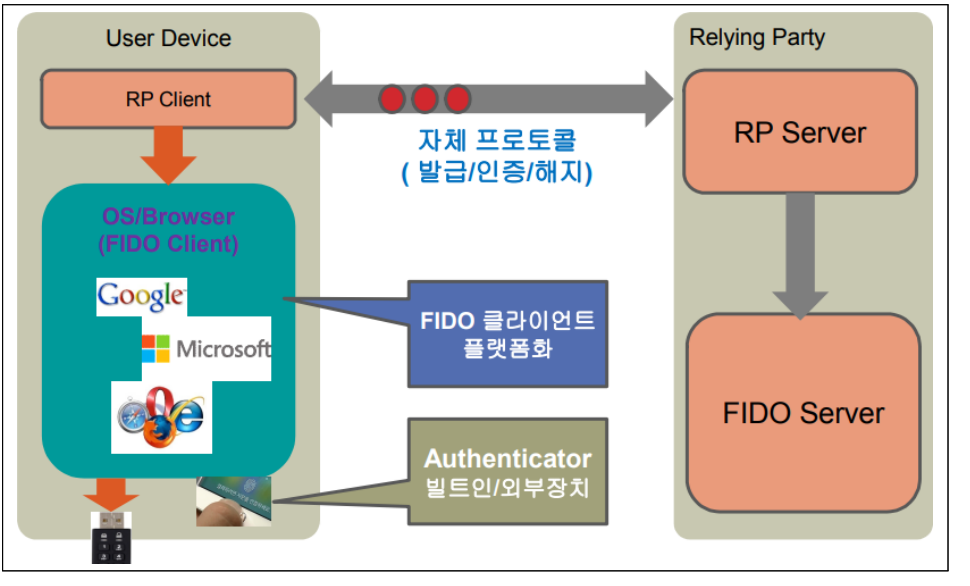
멀티팩터 인증의 중요성과 인증 자체의 안전성이 강조되면서, 패스워드나 PIN 번호와 같은 단순한 형식의 인증 요소 외에도 휴대폰 SMS, 생체 등 다양한 인증 방식을 활용하는 사례들이 늘어나고 있다. 특히, 카메라, 지문인식센서 등 생체 인증장치를 기본적으로 탑재한 스마트폰과 같은 기기들이 널리 활성화되고, 수많은 인증 기법들이 사용되면서 이들을 모두 수용할 수 있는 범용인증기술에 대한 요구가 나날이 커지고 있었다.

이를 위해 2013년 2월 구글, 레노버, 비자, 마스터, 페이팔 등 다양한 IT, 보안, 금융 기업들이 참여하여 FIDO(Fast IDentity Online) Alliance가 출범하였는데, 여기에서는 온라인 환경에서 보다 편리하고 안전한 인증 시스템을 공동으로 구축하고, 이에 대한 기술표준을 제공하는 역할을 수행하고자 하였다.

FIDO는 2014년 12월에 2가지 인증 관련 표준을 제정하여 공개하였는데, 첫번째는 U2F(Universal 2ad Factor) 기술로 패스워드만 사용하는 웹사이트에서 추가 인증방법으로 보안토큰을 사용할 수 있도록 하여 보안성을 높이는 멀티팩터 인증 기술이며, 두번째는

UAF(Universal Authentication Factor) 기술로 보안성이 취약한 패스워드 대신 지문, 얼굴 등 생체인식 혹은 스마트폰 잠금해제 패턴이나 하드웨어 칩에 기반한 강력한 인증 수단을 사용할 수 있는 인증 및 전자서명 기술이다. FIDO 1.0 시스템에서는 사용자 기기상의 RP 클라이언트와 서버 내부에 위치한 RP 서버 사이에 UAF 프로토콜을 통해 인증 정보(발급/인증/해지)를 전달하도록 되어 있다. 이후, FIDO 2.0으로 버전이 올라가면서, RP 클라이언트 역시 서버에서 구현하여 제공하는 것을 고려하여 UAF 표준 프로토콜 대신 자체 프로토콜을 사용하도록 하였다. RP 클라이언트가 인증 등을 위해 FIDO 클라이언트에 접근하는 것은 API를 통해서 이루어지도록 하였으며, 이 API를 참고하여 FIDO 응용 개발을 하면 된다.

〔그림 2－15〕 FIDO 2.0 시스템 구조



자료: 조상래 등, “FIDO 2.0 범용인증기술 소개”, 정보보호학회지 (2016)

결론적으로, FIDO 프로토콜을 사용할 경우, 사용자 인증은 FIDO 클라이언트에서 관리함으로써 사용자 기기가 제공하는 수많은 인증 방식을 편리하게 활용할 수 있으며, FIDO 서버에서는 강력한 혹은 멀티팩터 인증을 위해 별도의 하드웨어나 인식 장치를 사용하지 않고도 사용된 인증 방식과 결과에 대해 안전하게 전달받음으로써 보다 편리하고 안전한 인

증 기능을 제공할 수 있다는 장점이 있다.

스마트폰과 같은 사용자 기기는 지문인식 센서, 카메라(홍채, 얼굴), 마이크(음성) 등의 하드웨어 장치를 기본적으로 탑재하고 있으며, GPS 등 다양한 센서를 추가적으로 보유하고 있어 생체 및 위치 등을 기반으로 사용자 인증 방식을 다양하게 제공할 수 있다.

3) 무자각 지속 인증 (Implicit and Continuous Authentication)

일반적인 인증방식은 사용자에 대하여 명시적인 인증절차를 거치게 된다. 문제는 이러한 명시적인 인증절차가 사용자에게 특정한 행동(패스워드 입력, 보안 카드 제시 등)을 요구하므로 사용자에게 불편함을 주게 된다. 일단 명시적 인증을 통과한 이후 해당 세션이 종료될 때까지 인증을 추가로 요구하지 않는 경우, 공격자가 인증세션을 가로채는 공격이 가능하다.

따라서, 인증받은 세션과 세션 사용자에 대한 신뢰성을 유지하기 위하여 인증을 지속적으로 받는 것이 바람직하며, 지속적 인증과정에서 발생할 수 있는 사용자의 불편을 최소화하기 위하여 명시적이지 않은 형태의 무자각 혹은 비침투형 인증 기술이 필요하다. 이러한 유형의 인증은 A. Masri는 능동 인증(Active Authentication)이라고 정의한 바 있으며, 김승현 등은 무자각 지속인증이라고 부르며 “행위 및 환경 정보를 활용하여 사용자의 명시적 개입 없이 지속적으로 신원을 검증하는 기술”이라고 정의를 내렸다.

‘능동 인증’이라는 용어는 다른 의미로 사용되는 사례가 있기에 본 문서에서는 ‘무자각 지속인증’의 용어를 사용하는데, 이 인증기술은 〈표 2-3〉과 같은 2가지 특성을 만족하여야 한다.

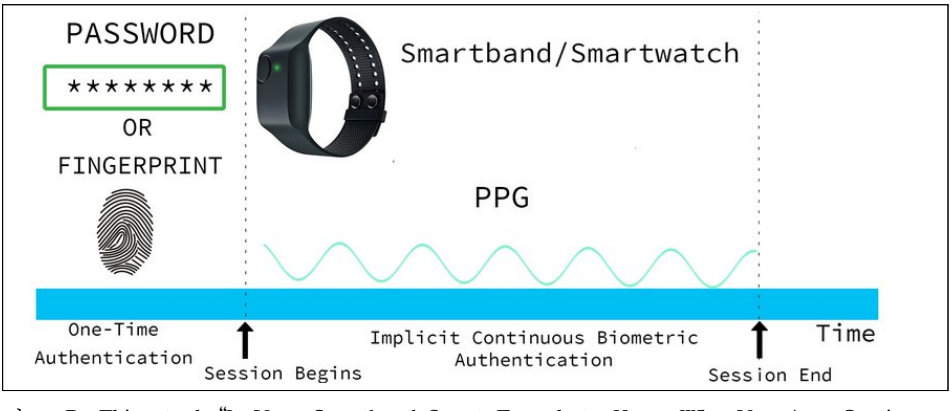
〈표 2-3〉 무자각 지속인증의 특성

특성	의미
무자각 인증	사용자에게 명시적으로 알리거나 별도의 명시적 인증을 요구하지 않고 사용자의 신원을 확인함으로써, 사용자가 인증을 받고 있음에 대한 자각없이 정상적인 서비스가 이루어져야 함
지속 인증	최초 인증 이후 정상적인 서비스가 이루어지는 환경에서 지속적으로 사용자의 신원을 확인하여야 함

사용자가 자각하지 않는 상태에서 지속적으로 인증을 하기 위하여 가장 널리 사용되는 것은 속성기반 인증이 많이 사용되는데, 이 중 생체인증 기술이 가장 많이 사용된다. 〔그림 2-16〕은 스마트밴드를 이용하여 광혈류측정을 통한 심박수를 측정함으로써 사용자를 지속적으로 인증하는 방식이며, 그 외에도 사용자의 행동 패턴이나 물리적 위치 등을 활용한 인증 방식도 널리 사용된다. 대표적인 인증 수단으로, 얼굴, 음성, 걸음걸이, 키스트로크 다이나믹스, 마우스 다이나믹스, 터치 다이나믹스, 문체, 위치, 앱 사용습관, 기타 모바일 장치에 의존한 방식들이 가능하다.

다만, 이러한 인증 방식들은 100% 확실한 인증을 보장하지 못하기 때문에, 정확도를 높이기 위한 여러 기술들이 결합되어야 하며, 최근 딥러닝 기술을 활용하여 사용자에 대한 인증정보를 사전에 학습한 후, 무자각 지속인증 과정에서 수집되는 인증정보의 패턴을 보고 판단하는 기술들이 출현하고 있다.

〔그림 2-16〕 스마트밴드에 기반한 무자각 지속인증의 예



자료: D. Ekiz et al, "Is Your Smartband Smart Enough to Know Who You Are: Continuous Physiological Authentication in The Wild", https://arxiv.org/pdf/1912.04760.pdf (Last accessed: 2022년 9월 26일)

4) 분산 ID

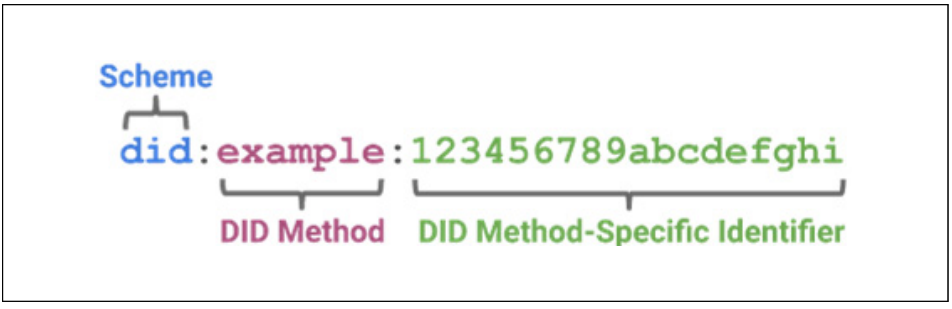
최초 ICT 환경에서의 사용자 인증시 인증 정보들은 개별 서비스를 제공하는 서비스 사업자에게 저장되어 있었으며, 사용자는 개별 서비스마다 ID/패스워드와 같은 인증정보를 등록하고 기억해야 하는 불편함이 있었다(Silo 모델). 이러한 불편함을 해결하기 위하여 싱글사인온과 같은 통합 인증서비스가 활용되지만(중앙집중형 및 연계형 모델), 사용자의 인증정보와 개인정보가 통합인증서비스 제공기관(IdP)에 집중됨으로써, 이들 서버에 해킹이 일어날 경우 개인정보 유출 및 침해 우려가 매우 크다.

유럽의 개인정보보호규정(GDPR, General Data Protection Regulation) 등 관련 법률은 개인정보 주체의 권한을 강화하는 경향을 보이며, 국내에서도 데이터3법(개인정보보호법, 정보통신망법, 신용정보법)에서 개인정보 전송권과 같은 자기결정권이 강화되고 있다. 이러한 흐름은 중앙집중형 모델이나 연계형 모델에서와 같이 통합인증서비스 제공기관에 가입자 정보가 집중되는 관리 체계가 더 이상 적절하지 않은 것으로 보이게 되어 최근 들어 분산 ID 모델에 대한 요구가 강하게 드러나고 있다.

분산 ID 모델은 기존 모델과 달리, 개인 식별 정보가 중앙 저장소 혹은 통합인증서비스 제공기관, 인증 기관 등에 종속되지 않도록 설계되었다. 핵심 기술로는 분산 식별자(DID, Decentralized Identifier) 기술과 검증 가능한 크리덴셜(VC, Verifiable Credential) 기술이 있으며, 이에 대한 표준화는 W3C에서 진행하고 있다. 최근(2022년 7월 19일) DID 버전 1.0(https://www.w3.org/TR/did-core/)에 대한 표준안이 나왔으며, VC의 경우 2019년 11월에 버전 1.0이 표준화된 후, 2022년 3월에 버전 1.1(https://www.w3.org/TR/vc-data-model/)로 업데이트된 표준 권고안이 공개된 바 있다.

대부분의 DID 기술은 블록체인 기술(Blockchain or Distributed Ledger) 혹은 다른 형태의 분산기술 기반으로 구현되는 것이 일반적이다. 〔그림 2－17〕과 같이 사용자(혹은 기기, 서비스, 조직과 같은 엔티티)에 대하여 전세계적으로 고유한, 그리고 암호학적으로 검증 가능한 영구적인 식별자를 정의하게 되며, 사용자는 이 정보와 결합하여 본인 단말에 다양한 증명서를 발급, 저장, 제출하는 서비스를 활용할 수 있게 되었다.

〔그림 2－17〕 DID의 표기 예 (W3C)



자료: M. Sporny et al, "Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations", W3C Recommendation (2022)

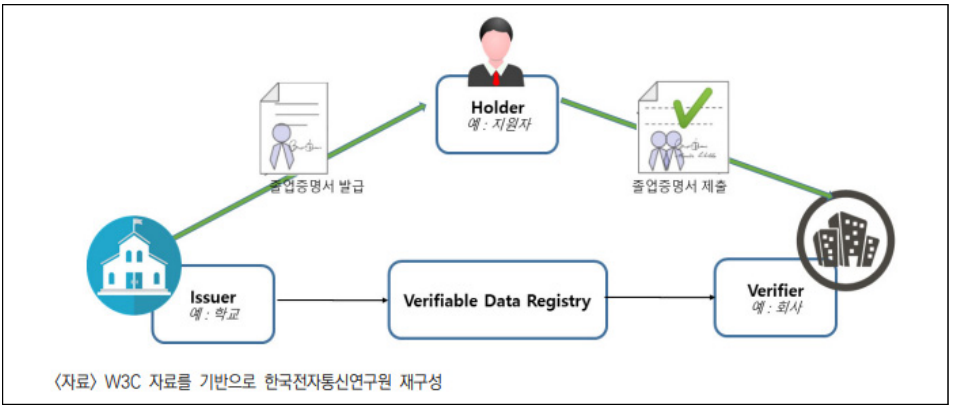
〔그림 2－17〕의 세 영역에 대한 설명은 〈표 2－4〉에서 다룬다.

〈표 2－4〉 DID 표기법에서의 세 영역

특성	의미
Scheme	DID 식별자임을 표시하는 것으로 모든 DID는 'did'로 시작
DID Method	DID 생성, 업데이트 등의 CRUD(Create, Read, Update, Delete)를 수행할 수 있는 방법 지정. 현재까지 제안된 방법으로는 did/web(URI를 DID로 사용), did:git(개발자용 DID), did:ipid(분산 파일 시스템 기반 DID), did:PROPREITARY(특정 사업자 제공 DID), did:peer(P2P용 DID), did:key(공개키 기반 DID) 등이 제안됨
DID Method Specific String	DID Method에 해당하는 ID 문자열

〔그림 2－18〕은 검증가능한 크리덴셜의 예로서 졸업증명서를 발급 및 제출하는 시나리오를 보여준다. 여기에서 검증가능한 데이터 저장소 역할을 하는 Verifiable Data Regisry는 DID, 키, 관련 데이터, 취소 저장소, 발급자 공개키 정보 등에 대한 생성과 검증을 중개하는 시스템으로 검증가능한 크리덴셜을 사용하기 위해 반드시 필요하다. Issuer는 VC를 발급하여 Holder에게 전달하며, 발급을 위하여 Holder의 identifier 정보를 검증할 수 있다. Holder는 identifier를 등록하고, VC를 발급받으며 Verifier에게 VC를 제출한다. Verifier는 VC와 Holder의 identifier 정보를 검증한다.

〔그림 2－18〕 분산 ID 신뢰 모델 기반 검증가능한 크리덴셜 시나리오 예



자료: 진승헌 등, “디지털 ID 관리 기술 현황”, 주간기술동향 (2020)

다. 데이터 보안

데이터 보안 기술은 넓은 의미에서 데이터의 생성, 유통, 소멸에 이르는 수명 주기 전체에서 무단 액세스 및 데이터 위변조 혹은 손상으로부터 데이터를 보호하는 모든 기술을 의미한다. 그러나, 앞서 언급한 바와 같이 4차 산업혁명 시대로의 진입과 함께 모든 산업에서 초연결・디지털・지능의 결합이 이루어짐으로써 디지털 대전환이 빠르게 이루어지고 있는 현실에서, 데이터는 네트워크, 인공지능과 함께 D.N.A로 표현되는 디지털 시대의 핵심 중 하나이다.

즉, 디지털 시대에서 수집・유통되는 다양한 데이터를 인공 지능으로 분석하여 가공된 정보가 유무선 네트워크를 통해 전달됨으로써, 산업과 생활의 모든 영역에서 디지털・지능화가 이루어지게 된다. 그러나, IoT 센서, 스마트기기 등 대량의 데이터를 생산, 가공, 유통되는 환경에서는 개인의 민감 정보 혹은 프라이버시 연관 데이터가 수집될 수 있으며, 이러한 개인 정보의 주체와 해당 데이터를 가공, 유통하는 주체가 서로 다를 수 있으며, 이 과정에서 개인의 프라이버시를 침해하거나 공격 당하는 사례가 발생할 수 있다.

따라서 여기에서는 데이터 보안을 좁은 의미로 해석하여, 프라이버시가 보호・유지되는 상태에서 데이터를 가공하는 기술 혹은 이를 가능하게 해주는 보안 기술로 정의하고자 한다.

이 중 동형암호는 암호화된 데이터를 복호화 없이 연산할 수 있는 암호화 방법 혹은 알

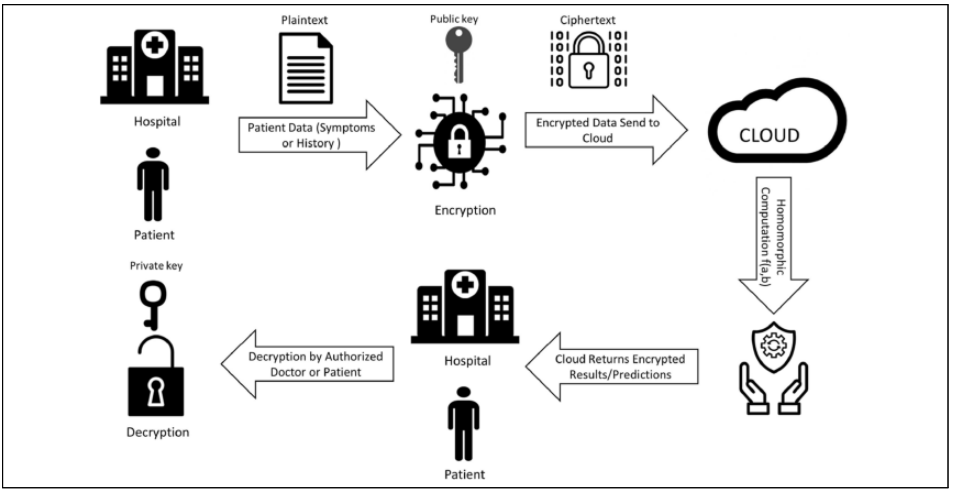
고리즘을 의미한다. 암호화되어 있는 상태에서 연산이 가능한 동형암호를 사용할 경우, 데이터를 가공하는 시스템에서는 데이터의 내용을 알지 못하면서도, 암호화된 상태에서 원하는 가공을 할 수 있는 수단이 될 수 있을 것이다.

또 다른 기반 기술로는 차등 프라이버시 기술이 있다. 차등 프라이버시 기술은 2016년 Dwork(2016)가 처음 제안한 것으로, 원래 데이터에 수학적 노이즈를 추가함으로써 프라이버시 노출 가능성을 낮추는 기술이다.

1) 동형 암호(HE, Homomorphic Encryption) 기술

동형암호는 1978년 Rivest, Adleman, Dertouzos 등이 공동으로 발표한 논문에서 처음 제안되었으며, 암호화된 데이터를 복호화 없이 연산할 수 있는 암호화 방법 혹은 알고리즘을 의미한다. 이들은 동형암호의 개념을 소개하면서 제시한 응용에서는, 데이터베이스를 운영하기 어려운 소규모 대부업자가 외부 업체에 데이터의 저장을 위탁하고, 이 데이터를 프라이버시가 보존된 상태에서 가공하도록 할 때 동형암호를 사용한다는 것이다. 최근 널리 사용중인 클라우드 상에서의 데이터 처리시, 데이터에 대한 프라이버시에 대한 요구사항을 추가한 것과 같은 개념으로 볼 수 있으며, 프라이버시에 민감한 데이터의 종류와 소유주를 변경하면 다양한 응용이 가능해질 수 있는데, 〔그림 2-19〕는 환자 데이터를 보유하고 있는 병원이 데이터를 동형암호화하여 클라우드를 통해서 프라이버시가 보존된 데이터 처리 서비스를 받는 과정의 예 도식화한 것이다.

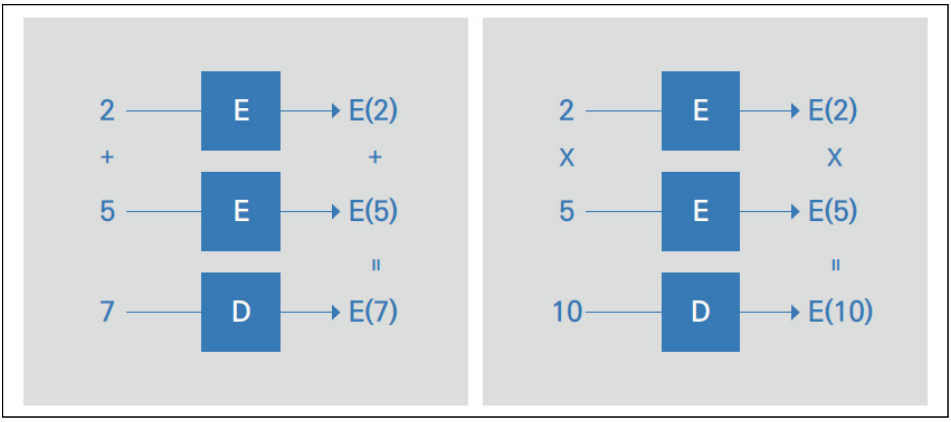
〔그림 2－19〕 동형 암호의 활용 예 - 환자 데이터 처리



자료: K. Munjal et al, "A systematic review of homomorphic encryption and its contributions in healthcare industry", Complex & Intelligent Systems (2022)

사실, RSA를 포함하는 기존 암호에서도 일부 연산에 대해서는 암호화된 상태에서의 연산이 가능하다. 예를 들어, ElGamal과 RSA는 곱셈연산을 암호화한 상태에서 수행하는 것이 가능하며, 그 외에도 덧셈 혹은 XOR 연산이 유지되는 동형암호들도 있으나, 1978년 Rivest 등이 제시한 개념에서는 덧셈과 곱셈이 모두 수행가능하여야 한다는 요구사항이 있었기에 일부 연산이 가능한 동형암호는 부분동형암호(PHE, Partial Homomorphic Encryption)로 인식된다.

〔그림 2－20〕 동형 암호에서의 덧셈 보존과 곱셈 보존 개념도



자료: 윤성욱, “인공지능의 발전에서 동형암호가 갖는 의미”, AI TREND WATCH (2020)

최초로 덧셈과 곱셈이 모두 가능한 완전동형암호(FHE, Fully Homomorphic Encryption)은 2009년 최초로 C. Gentry(〔그림 2－21〕)에 의해 제안되었으며, 여기에서는 격자 기반 암호를 사용하며 연산을 거듭하면서 에러가 증폭됨으로써 일정 횟수가 넘어가면 복호화가 불가능한 유한동형암호를 먼저 제안하고, 이 유한동형암호에 재부팅(Bootstrapping) 과정을 추가함으로써 이론적으로 무한한 횟수만큼 연산이 가능하도록 하였다.

〔그림 2－21〕 완전동형암호를 최초로 제안한 Craig Gentry

자료: https://www.youtube.com/watch?v=pXb39wj5ShI (Last accessed: 2022년 9월 26일)

이후, 동형암호는 재부팅과정의 제거 혹은 고속화, 평문데이터 구조의 다양화, 성능 고속화, 추가 연산 기능 등을 포함하면서 발전을 이루어 왔는데, 이를 1~4세대로 분류하면 〈표 2-5〉와 같다.

〈표 2-5〉 완전동형암호 세대별 분류 <참조: 인공지능의 발전에서 동형암호가 갖는 의미>

세대	대표 기법	방식
1세대	Gentry(2009)	준동형암호 연산시 기하급수적으로 증가하는 암호문 내의 잡음을 줄여주는 재부팅 도입을 통하여 반복적 연산 가능
2세대	BGV(2011) LTV(2012) BFV(2012) BLLN(2013) CKKS(2016)	모듈러스 또는 키교환(Key-switching)을 통해 동형곱셈시 발생하는 잡음증가 속도를 감소시켜 재부팅 없이 가능한 곱셈횟수를 획기적으로 증가
3세대	GSW(2013) FHEW(2014) TFHE(2016)	동형곱셈에서의 잡음을 줄이고, 재선형화 단계를 피하는 완전암호동형체계 구축 매작동마다 암호문을 갱신하여 재부팅 시간 감소
4세대	CKKS(2017)	근사계산을 통해 잡음 증가를 제어하여 회로 재부팅 횟수를 줄임 반올림연산 시간을 덧셈 수준으로 줄임으로써 기계학습 등 근사연산을 활용하는 응용분야에 상용화 가능성 대두

동형암호를 연구하는 그룹들을 중심으로 표준화 단체를 만들어(Homomorphic Encryption Standardization, https://homomorphicencryption.org/), 동형암호에 관한 안전성, API 및 응용에 관한 표준화를 진행하여 2018년 11월 표준문서를 발간하였으며, 여기에는 우리나라의 서울대, 삼성SDS 외에 마이크로소프트, 인텔, IBM, 구글, 마스터카드와 같은 산업계, NIST, ITU와 같은 정부기관 혹은 국제단체, UCSD, MIT, Columbia 대학과 같은 학계가 모두 참여하고 있다.

특히, 서울대학교 천정희 교수 연구팀을 비롯하여 IBM, 마이크로소프트 등이 이 분야를 주도하면서, 〈표 2-6〉과 같이 오픈소스 기반의 완전동형암호 라이브러리를 공개하여 활성화가능성을 엿보고 있다.

〈표 2-6〉 오픈소스 기반 완전동형암호 라이브러리 목록

개발자	이름	구현한 완전동형암호
IBM	HElib	BGV, CKKS
Microsoft	SEAL	BGV, CKKS, BFV
MIT 등	PALISADE	BGV, CKKS, BFV, FHEW, TFHE
서울대	HEAAN	CKKS
Leo Ducas 등	FHEW	FHEW
Ilaria Chillotti 등	TFHE	TFHE
CryptoExperts	FV-NFLlib	BFV
NuCypher	NuFHE	TFHE
EPFL-LDS	Lattigo	CKKS, BFV
Zama	Concrete	TFHE

완전동형암호는 암호화된 데이터에 대하여 복호화 과정을 거치지 않고도 데이터를 처리하기 위한 여러 연산을 수행하는 것이 가능하기에, 평문 상태에서 데이터를 처리할 때 발생할 수 있는 개인정보 유출이 일어날 가능성이 적다. 그러나, 컴퓨터에서 가능한 모든 연산을 수행할 수 없으며, 암호화 과정에서 데이터가 늘어나는 비율이 기존 암호와 비교하여 매우 크고(약 10-100배), 암・복호화 속도가 기존 공개키 암호(RSA 등)와 비교해서도 상당히 느리며(수십배), 암호화 과정에서 커지는 잡음의 크기를 제어하기위한 재부팅 과정이 필요하다는 단점이 여전히 존재한다는 것은, 실제 응용에서 활용되는데 있어 걸림돌로 작동한다.

따라서, 아직도 완전동형암호는 실제 응용에 사용되기 위해 기능과 성능 면에서 모두 개선이 필요하다고 볼 수 있으며, 많은 연구자들에 의해 일정 부분 극복이 된다면 디지털 대전환 시기에 프라이버시를 보존하는 형태로 데이터 마이닝을 하는 다양한 환경에서 활용될 가능성이 있으므로 많은 관심이 필요하다.

2) 차등 프라이버시 (Differential Privacy)

안전한 데이터 활용을 지원하는 차세대 보안 기술 중 또 다른 하나는 차등 프라이버시 기술이다. 차등 프라이버시는 인공지능 학습용 데이터 처리 혹은 개인정보를 포함하는 데이터 통계 처리 등의 과정에서 개인정보 보호를 위해 해당 데이터셋에 임의의 노이즈를 삽입함으로써 개인정보가 제 3자에게 노출되지 않도록 보호하는 기술로, 차분 프라이버시라고도 불리운다.

차등 프라이버시는 2006년 Dwork의 논문에서 처음 제안되었는데, Dwork는 공개된 자료에 특정인의 정보가 포함되지 않은 경우에도 그 사람의 개인정보가 노출될 수 있다는 주장을 하였으며, 그는 이에 대한 사례로 "Terry Gross는 리투아니아 여자의 평균 키보다 2인치 작다. 국가별 남녀의 평균 키를 제공하는 자료가 존재한다면 Terry Gross의 키는 노출될 수 있다"라고 언급하였다.

프라이버시를 보호하면서 통계처리를 하기 위하여 기존에는 익명화, 가명화, 범주화 등의 기술을 통하여 개인 식별 정보를 제거한 후 k-anonymity, l-diversity, t-closeness 프라이버시 보호 모델을 적용하여, 프라이버시가 충분히 보장되는지를 판단하였다. 그러나, 이러한 기술은 몇 가지 약점을 가지고 있었는데, 첫번째로는 데이터의 과도한 삭제, 일반화 등을 통하여 통계적 유용성을 떨어뜨리는 경우가 많았다는 점이고, 두번째로는 익명화를 적용하였음에도 배경지식, 사회공학적 기법 등을 활용하는 공격에 의해 프라이버시 노출되는 경우가 있었다는 점이다.

예를 들어, 〔그림 2-22〕는 초기 비식별화된 데이터베이스에 대해 4-anonymity를 적용한 사례이다. 그런데, 만약 첫번째 그룹에 'Cardiac disease(심장병)'을 거의 앓지 않는 한 명의 일본인이 있다는 사실이 알려진다면, 그 일본인의 병은 'Infectious disease(전염병)'이라는 사실을 강하게 추론할 수 있을 것이다. 혹은, 3-anonymity를 보장하는 의료 데이터는 최소 3명의 사람이 같은 병력과 소득을 얻고 있는 형태로 데이터를 배포하게 되는데, 만약 2명이 폐 질환, 1명이 간 질환을 앓고 있다는 정보를 공격자가 아는 상태에서 또 한명의 의료 정보가 추가되었음에도 데이터가 배포되지 않는다면, 추가된 사람은 폐질환을 앓고 있지 않다는 것을 알 수도 있을 것이다.

〔그림 2－22〕 4-anonymity의 예

Anonymous DB

id	Zipcode	age	nationality	disease
1	13053	28	Russia	Cardiac disease
2	13068	29	US	Cardiac disease
3	13068	21	Japan	Infectious dis.
4	13053	23	US	Infectious dis.
5	14853	50	India	Cancer
6	14853	55	Russia	Cardiac disease
7	14850	47	US	Infectious dis.
8	14850	49	US	Infectious dis.
9	13053	31	US	Cancer
10	13053	37	India	Cancer
11	13068	36	Japan	Cancer
12	13068	35	US	Cancer

4-anonymity DB

id	Zipcode	age	nationality	disease
1	130**	<30	*	Cardiac disease
2	130**	<30	*	Cardiac disease
3	130**	<30	*	Infectious dis.
4	130**	<30	*	Infectious dis.
5	1485*	≥40	*	Cancer
6	1485*	≥40	*	Cardiac disease
7	1485*	≥40	*	Infectious dis.
8	1485*	≥40	*	Infectious dis.
9	130**	3*	*	Cancer
10	130**	3*	*	Cancer
11	130**	3*	*	Cancer
12	130**	3*	*	Cancer

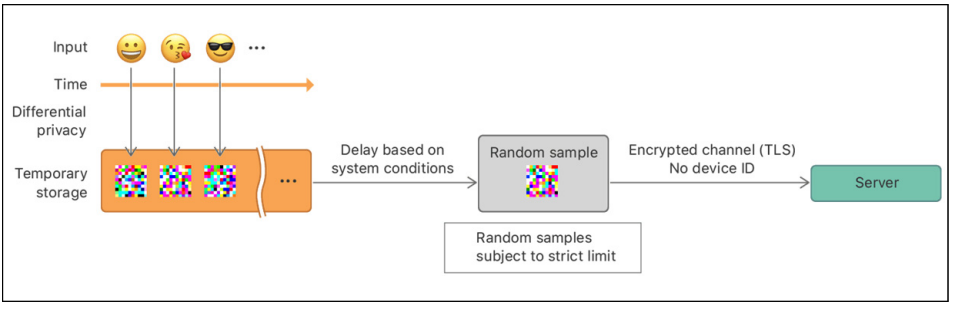
자료: H. Nakagawa, "Introduction of Privacy Protection Mathematical Models"(2016)

이를 막기 위하여 개인정보가 전체 자료에 추가로 포함될 때 프라이버시 노출 위험을 차등 프라이버시라고 정의하고 이를 수학적으로 측정하는 식을 제안한 바 있다. 차등 프라이버시는 암호학에서 유래하는 "semantic security(의미론적 안전성)" 의 개념에서 영감을 얻었는데, 의미론적 안전성이란 암호문으로부터 평문에 관한 어떠한 정보도 얻을 수 없음을 의미한다. 즉, 암호문을 확인한 후 평문에 대해 알려진 지식은, 암호문을 확인하기 전에 이미 알려진 것을 의미한다.

그러나 데이터베이스 관점에서는 의미론적 안전성을 확보하는 것이 불가능하다. 통계 정보를 통해 추가적인 정보를 습득할 경우, 어떤 유용성이 발생하게 되기 때문인데, 프라이버시 보호 모델에서는 이러한 유용성을 제공하면서도 일정 수준의 프라이버시를 보장할 필요가 있는 것이다.

애플이 2017년 인공지능 기반의 음성비서인 '시리'의 학습을 위한 데이터 처리 과정에서 개인정보보호를 위해 차등 프라이버시 기법을 적용한다는 것을 밝히면서 차등 프라이버시 기술이 주목을 받게 되었으며, 미국 통계청에서 2018년 인구조사에서 개인정보보호를 강화하기 위한 기본 프레임워크로 차등 프라이버시 적용을 공표하기도 하였다. 그 외에도 많은 글로벌 기업들이 데이터마이닝, 머신러닝/딥러닝 기술에 차등 프라이버시 기술을 접목하고 있다.

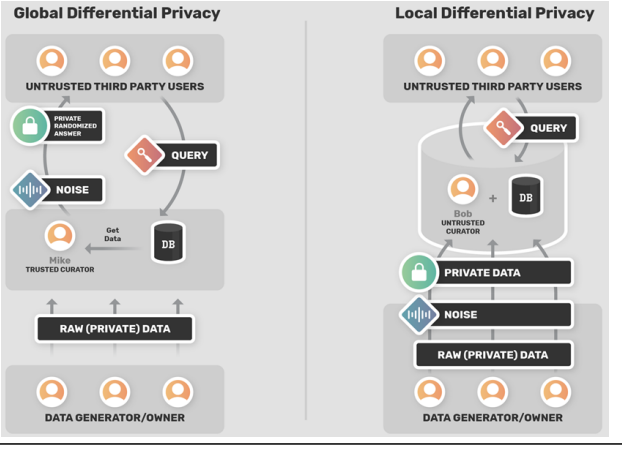
〔그림 2－23〕 애플 기기상에서 수집된 데이터의 차등 프라이버시 적용



자료: https://machinelearning.apple.com/research/learning-with-privacy-at-scale (Last accessed: 2022년 9월 26일)

차등 프라이버시에서는 한 개체가 전체 데이터에 추가될 때 증가하는 프라이버시 노출 위험도를 수학적으로 측정하여, 노출 위험을 낮추기 위한 노이즈 데이터를 주입하게 된다. 노이즈가 작으면 정확성이 유지되며, 크면 프라이버시를 더 많이 보호하게 되는 것이다. 노이즈가 추가되는 위치에 따라 지역 차등 프라이버시(Local Differential Privacy)와 글로벌 차등 프라이버시(Global Differential Privacy), 2가지 종류로 나뉘며 이는 〔그림 2－24〕와 같다. 지역 차등 프라이버시 방식에서는 각각의 개별 원시 데이터(Raw Private Data)에 노이즈를 추가한 후 해당 데이터들을 신뢰할 수 없는 큐레이터(Untrusted Curator)가 수합하며, 글로벌 차등 프라이버시 방식에서는 신뢰 큐레이터(Trusted Curator)가 여러 사람의 원시 비공개 데이터에 액세스하여 원시 데이터를 분석하고 노이즈를 추가하여 처리된 데이터를 제공한다.

〔그림 2-24〕 차등 프라이버시의 두 가지 방식



자료: https://blog.openmined.org/basics-local-differential-privacy-vs-global-differential-privacy/ (Last accessed: 2022년 9월 26일)

현재 구글의 머신러닝 학습 및 개발 프레임워크인 TensorFlow의 TensorFlow Privacy 모듈, 마이크로소프트에서 제공하는 클라우드 기반 Azure Machine Learning 플랫폼의 WhiteNoise 기능, 페이스북의 고속 머신러닝 라이브러리 Opacus 등에 모두 프라이버시를 강화하는 인공지능 학습이 가능한 차등 프라이버시 기능이 도입되어 있다. 차등 프라이버시 기술은 앞으로도 인공지능 학습을 위한 데이터셋 학습 과정에서 개인 데이터를 사용하되, 학습 결과를 통해 개인을 식별하거나 개인정보를 침해할 수 없도록 하는 환경에서 널리 사용될 것이다.

라. 하드웨어 기반 보안

응용 프로그램을 위한 보안 기술 혹은 보안 프로토콜은 대체로 소프트웨어적으로 구현되어 운영체제 위에서 동작한다. 이러한 소프트웨어 기반 보안 기술은 운영체제 상위에서 동작을 하며, 운영체제 역시 하드웨어 상위에서 동작을 한다. 이 경우, 소프트웨어 기반 보안 기술은 운영체제와 하드웨어에 대한 보안이 확립되어 있어야 한다는 것을 의미하며, 이를 위한 신뢰성이 확보되어 있어야 함을 의미한다.

만약 메모리가 언제든지 해킹될 수 있다거나, 공격자에 위해 변조된 운영체제가 동작하

고 있어서 사용자로부터 입력되어 보안 기술에서 활용하는 모든 정보(예, 키보드를 통한 패스워드 입력, 카메라를 통한 홍채 정보 입력 등)가 공격자에게 수집・도청・변조될 수 있다면, 보안 기술 자체를 신뢰하기 어렵게 될 것이다. 컴퓨터가 당초 의도된 대로 동작하고 있다는 신뢰성 자체가 확보되어야 하는 것이다.

하드웨어 보안 기술은, 일반적으로 소프트웨어 기반 보안 기술의 신뢰성을 확보해주고, 안전성을 증대시켜주는 역할을 한다. 본 절에서는 가장 대표적인 하드웨어 보안 기술로서, TPM과 TEE, PUF에 대해 다루고자 한다.

1) 신뢰 플랫폼 모듈 (TPM, Trusted Platform Module)

TPM은 외부에서 접근이 불가능한 장소에 키를 보관하고 내부에서 암호화 연산을 수행하도록 고안된 하드웨어 칩이다. TPM 내부적으로는 변조 방지를 위한 물리적 보안 메커니즘이 적용되어 있어 악성 소프트웨어는 TPM 보안 기능을 변조할 수 없으며, 시스템 정보와 사용자가 입력한 PIN을 수집하여 이전에 저장한 정보와 비교하여 일치할 경우에만 정상적으로 부팅이 이루어지도록 한다.

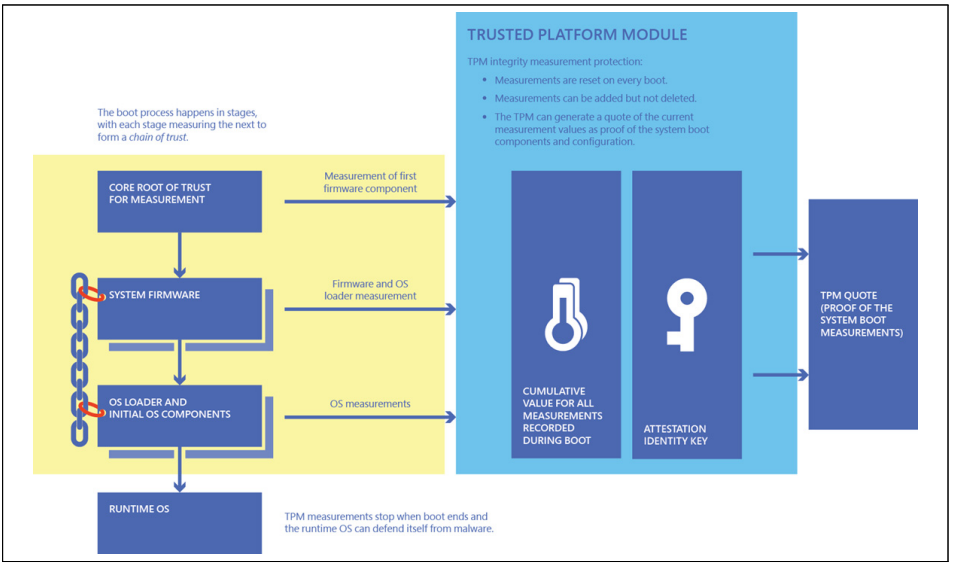
TPM은 산업계 콘소시엄인 TCG(Trusted Computing Group)에 의해 구상되어 표준 작업이 진행되었으며, 2009년 ISO/IEC 11889:2009로 표준화된 후 2011년 리비전을 완료하였다. 이후, 2014년 TPM Library Specification 2.0으로 대대적인 업그레이드를 할 것임을 발표하였으며, 알고리즘과 명령어를 추가하여 2015년 ISO/IEC 11889:2015 표준화가 되었고, 리비전 과정을 거쳐 2019년 11월 2.0 버전으로 발표하였다.

TPM은 다음과 같은 영역에 활용 가능하다.

- 플랫폼 무결성
- 디스크 암호화
- 응용 서비스를 위한 보안 기능
  - 디지털 저작권 관리 (DRM)
  - Window Defender
  - 소프트웨어 저작권 보호 및 적용
  - 온라인 게임 상의 속임수 방지

윈도와 같은 운영체제에서 TPM을 사용하여 안전하게 부팅하는 방법을 〔그림 2-25〕에서 보인다. 가장 먼저 펌웨어 컴포넌트에 대해 무결성을 확인하고, 펌웨어와 운영체제 로더, 그리고 운영체제의 무결성을 차례로 검증한 후 부팅이 완료되면 TPM의 무결성 검증 절차는 종료되며, 이후 실행중인 운영체제는 스스로를 안전하게 보호할 수 있다.

〔그림 2-25〕 윈도 운영체제의 TPM 사용 방법



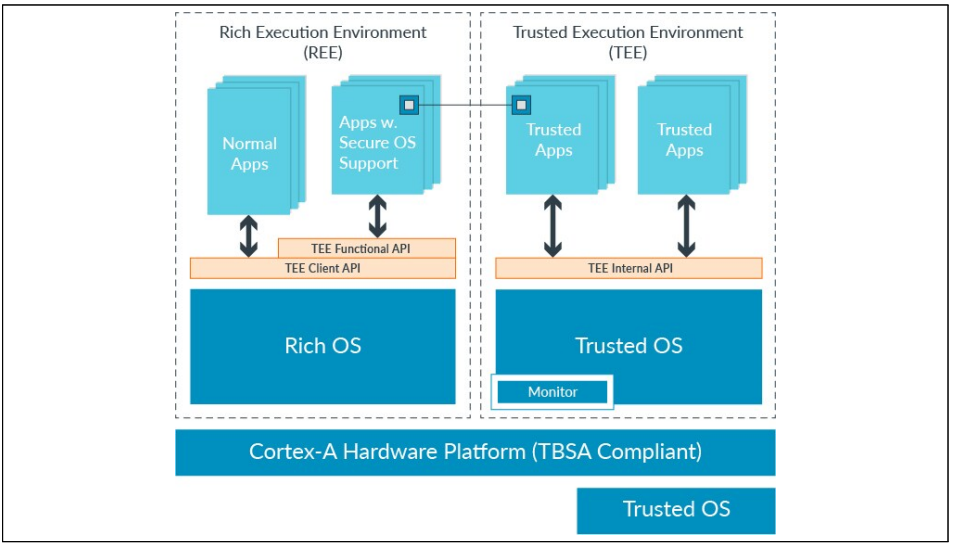
자료: https://learn.microsoft.com/ko-kr/windows/security/information-protection/tpm/how- windows-uses-the-tpm (Last accessed: 2022년 9월 26일)

2) 신뢰 실행 환경 (TEE, Trusted Execution Environment)

TEE는 스마트폰과 같은 모바일 기기에서 프로세서를 보안영역과 일반영역으로 나누고 민감한 정보의 저장과 처리를 보안영역에서 수행하도록 함으로써 신뢰성을 보장하는 시스템이다. 일반 영역에서는 기존 안드로이드와 같은 일반 OS가 실행되는 환경으로, 보안이 상대적으로 중요하지 않은 앱이 실행되며, 보안 영역에서는 결제나 DRM과 같은 보안이 중요한 앱이 안전하게 실행될 수 있다. 일반적으로 일반영역과 보안영역은 물리적으로 분리되어 있으며, 일반영역에서 보안영역을 접근할 때에는 TEE에서 제공하는 API를 통해서만 가능하다.

TPM이 일반적으로 프로세서와 분리된 별도의 칩을 이용하는 경우가 많다면, TEE는 메인 프로세서에 포함되어, 기밀성과 무결성 관점에서 실행되는 코드와 데이터의 안전성을 보증해주고, TEE 외부에서 인가받지 않은 엔티티가 데이터에 접근하거나 수정하는 시도를 막게 된다. 인텔의 SGX, ARM의 TrustZone 등이 대표적인 TEE 기술이다.

〔그림 2－26〕 ARM의 TrustZone 구조 개념도



자료: https://embeddedbits.org/introduction-to-trusted-execution-environment-tee-arm-trustzone/ (Last accessed: 2022년 9월 26일)

GlobalPlatform의 TEE 위원회에서는 TEE 구조 및 API에 관한 표준화, RISC-V 접목, IoT 플랫폼 보안성 프로파일 개발, TEE 공격 분석을 통한 보안성 개선 등의 작업을 수행 중에 있다.

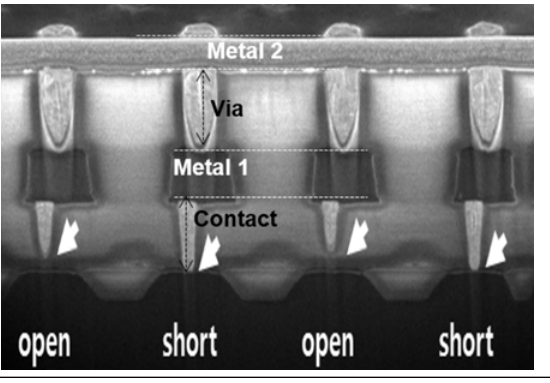
3) 물리적 복제방지 기능 (PUF, Physically Unclonable Function)

PUF는 기존 소프트웨어 기반의 키 생성 등에서 발생할 수 있는 위험성을 해결하기 위하여, 반도체 구조 공정에서 불가피하게 나타나는 공정 편차를 이용하여 해당 기기에 연관된 고유의 값을 생성하는 하드웨어 기반 보안 방식이다. PUF는 공정 편차에 의해 랜덤하

게 발생하므로 복제가 불가능하여, 디바이스의 유일성을 확인할 수 있다는 아이디어에서 출발하였다. 이렇게 유일한 정보가 생성되는 경우, 복제가 불가능한 암호키나 식별 정보로 활용할 수 있는데, 이 값들은 비휘발성 메모리 등에 저장할 필요가 없어 유출 등의 보안 위협에 상대적으로 안전하다는 장점이 있다.

초창기 PUF의 구현은 반도체 칩 구현시 소자의 특성에 기반한 아이디어를 FPGA 혹은 ASIC으로 구현하는 것이 일반적이었으며, 구현대상에 따라 Arbiter-PUF, RO-PUF, LoopPUF, VIA PUF 등이 있다. 〔그림 2-27〕에서, VIA는 서로 다른 메탈 층을 연결하는 미세한 구멍을 일컫는데, VIA PUF는 반도체 공정 상에서 디자인 룰로 적절한 VIA 크기를 정할 경우 VIA가 랜덤하게 생성되는 특징을 활용하여 랜덤값을 생성하는 PUF이다.

〔그림 2-27〕 VIA PUF 이미지



자료: https://www.technologyreview.kr/puf-iot-security/ (Last accessed: 2022년 9월 26일)

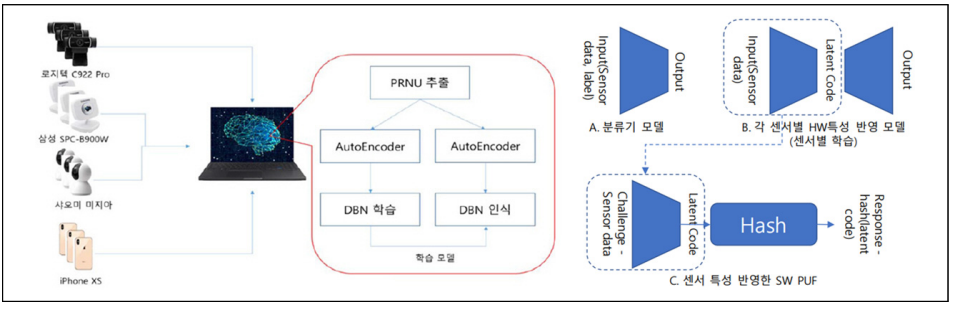
이 외에도 상용 기기 내부의 부품의 물리적 특성을 활용하여 직접 PUF 출력을 유도하는 기술이 등장하였으며, SRAM 혹은 DRAM 기반의 방식이 알려졌다. 이 방식은 별도의 반도체 칩을 만들 필요가 없으므로 기존 기기에 곧바로 적용할 수 있기 때문에 호환성과 비용 절감 측면에서 유리한 반면, 아직은 기술 성숙도가 상대적으로 낮다는 단점이 있다.

최근 들어서는 스마트폰 등의 기기에서 활용 중인 다양한 센서(예, 이미지 센서, 가속도 센서, 자이로 센서, 지자기 센서 등)에서도 센싱 데이터의 오차를 이용하여 PUF와 같이 유일한 정보를 생성하는 기술이 연구되고 있다. 일반적으로 센싱 데이터의 오차를 이용하므

로, 센싱 데이터 자체를 활용하기 보다는 오차에 대한 분석 및 특징 추출과 같은 과정이 필요하다.

특히, 이미지 센서의 경우 생산과정에서의 불완전성 때문에 빛에 균일하게 반응하지 못하는 현상(PRNU, Photo Response Non-Uniformity)이 발생한다. 이 값은 카메라로 찍은 영상이나 이미지의 품질을 결정하는 값이지만, 고유성이 있음이 알려지면서 초창기 불법 영상물 배포의 소스 카메라를 검증하기 위한 포렌식 기술로 활용하기 위한 연구가 많이 진행되었으며, 〔그림 2-28〕와 같이 PUF와 유사한 일종의 소프트웨어-PUF로도 활용할 수 있음이 알려졌다.

〔그림 2-28〕 이미지 센서 데이터 학습 및 이를 이용한 SW-PUF



자료: 김주한 등, “센서 기반의 디바이스 DNA 기술 동향”, 전자통신동향분석 (2020)

아직은 PUF를 기반으로 하는 응용이 다양하지 않으나, TPM, TEE와 비교하여 비용이 상대적으로 저렴하며, 하드웨어적으로 복제할 수 없는 유일한 식별정보를 생성하고 이를 활용하는 기능을 갖추고 있기에, 스마트폰이나 드론, 자동차와 같은 임베디드 기기 외에도, 최근 폭발적으로 늘어나는 IoT 기기 등에서 인증, 암호화 등 하드웨어 기반의 보안 기능을 제공함으로써 폭넓게 활용될 가능성이 있다.

마. AI 보안

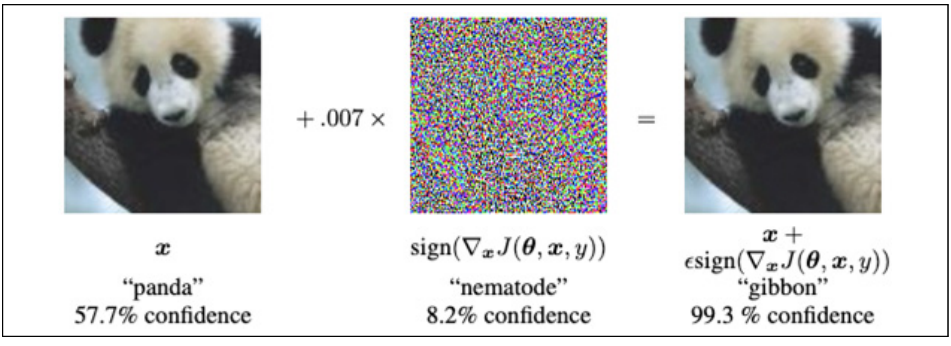
AI 보안은, 다른 ICT 기술들과 보안 기술이 융합될 때와 마찬가지로 크게 두 가지로 분류할 수 있는데, 첫번째로는 AI 기술을 활용한 보안이며 두번째로는 AI를 위한 보안 기술이다. AI 기술을 활용한 보안이라 함은, 예를 들어 생체인증의 정확도를 높이기 위하여 딥러닝 기술을 활용하는 예 등이 있을 수 있다. 이는 엄밀히 보면 인증 분야에서 발생하는 기술의 진보 혹은 진화라고 볼 수 있을 것이므로, 1.5절에서 별도로 다룰 내용은 아니다.

인공지능 기술의 급속한 발전과 확산이 이루어짐에 따라 개인정보 노출, 알고리즘 차별 등 예측하기 어려운 잠재 위험에 대한 우려가 증가되고 있다. 이를 대응하기 위하여 유럽연합이 도입하고자 하는 인공지능법(Artificial Intelligence Act)은 2021년 초안을 발표하였으며 회원국 간 협의 및 승인을 거쳐 2023년 이후 시행될 것으로 보인다. 이 법에서는 인공지능 기술에 대하여 위험 수준에 따라 4단계(최소 위험, 제한적 위험, 고위험, 불허용 위험)로 구분하고 단계에 따르는 규제를 달리하고 있다.

이러한 배경에는 인공지능이 일상생활과 밀접해지면서 인간 사회의 다양한 문제가 인공지능에 투영되는 사례가 지속적으로 발생하고 있기 때문이다. 예를 들어, 인공지능이 학습 데이터에 대한 불균형으로 인하여 성차별 혹은 인종 차별을 보인다거나, 인권 및 개인정보 침해, 정치적 혼란 야기, 사회적 편견 유발, 안전성 결여 등 다양한 사례가 발생한 바 있다. 악의적인 익명 사용자들에 의해 백인우월주의라든지 혐오 발언을 학습하고 발언한 Microsoft 사의 챗봇 '테이'와 인종·성소수자·장애인 등에 대한 혐오 발언을 한 것으로 알려진 국내 인공지능 챗봇 '이루다' 등의 그 대표적인 사례 중 하나이다.

이런 사례들처럼 AI 시스템이 오작동할 때 발생하는 역효과를 AI 역기능이라고 하는데, 이런 역기능을 유발하는 공격들이 있다. 2013년 Biggio 등은 자신들의 논문에서 처음으로 적대적 예제를 언급하였다. 적대적 예제를 기반으로 회피 공격(Evasion Attack)의 가능성에 대해 주장하였으며, 공격자가 공격을 위해 학습하는 대리 학습자(Surrogate Learner)의 개념도 제시하였으며, 이 두 가지 개념은 심층 신경망에 대한 공격 기술에서 많이 활용되고 있다. 〔그림 2-29〕는 판다 곰으로 확인된 이미지에 공격용 노이즈를 삽입한 결과 긴팔원숭이(Gibbon)로 판단하는 회피 공격의 사례이다. 이때 노이즈가 삽입되어 변조된 데이터를 적대적 예제(Adversarial Example)라고 부른다.

〔그림 2－29〕 회피 공격의 예

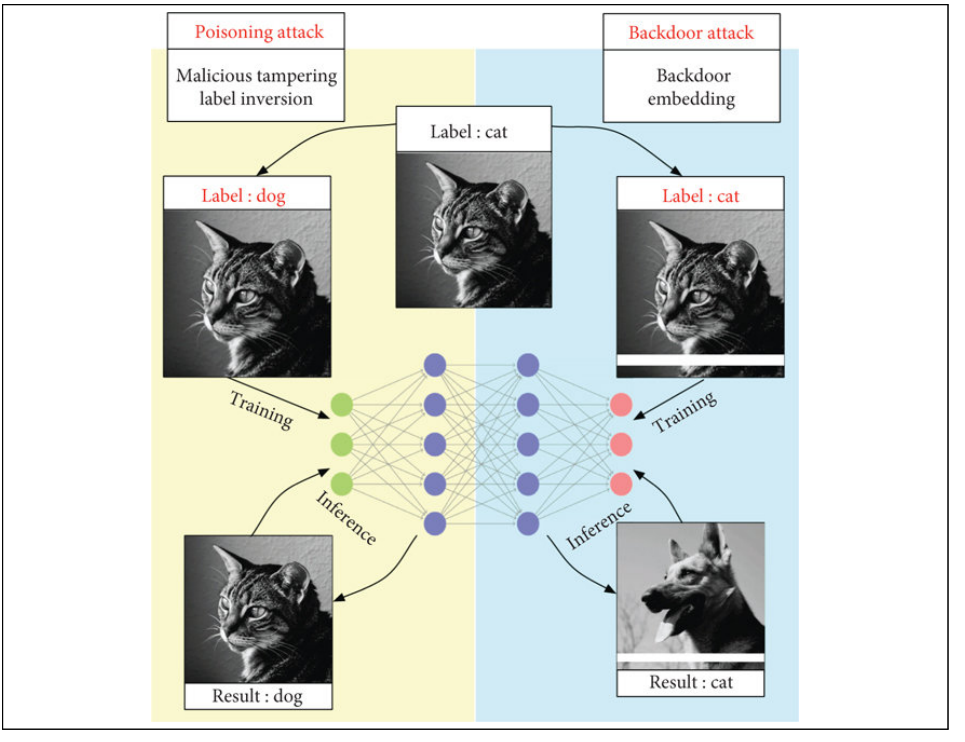


자료: I. J. Goodfellow et al, "Explaining and Harnessing Adversarial Examples"(2014)

이 외에도 학습데이터의 레이블에 고의적으로 잘못된 정보를 넣은 오염 데이터를 포함시켜 학습된 모델의 정확도를 떨어뜨리는 오염 공격(Poisoning Attack)도 있다. 예를 들어, 〔그림 2－30〕의 왼쪽 예와 같이 고양이 사진에 '개' 레이블을 붙이는 것도 이러한 오염 공격이 된다. 오염 공격이 발생하는 시나리오는 학습 모델의 생성 방법에 따라 다음과 같은 경우가 있다. 첫째 아웃소싱을 통해 학습데이터를 구축하거나 AI 모델을 개발할 때 오염데이터를 주입하는 경우, 둘째 이미 학습된 모델에 자신의 오염된 학습데이터를 추가하는 경우, 셋째 분산된 클라이언트가 로컬모델을 학습한 후 가중치 값 등 학습 파라미터를 서버에 전송하는 연합 학습(Federated Learning)에서 특정 클라이언트가 오염데이터를 학습하여 생성된 파라미터를 전송하는 경우 등이 있다.

백도어 공격(Backdoor Attack)은 학습데이터에 트리거라고 불리는 특정한 패턴을 포함하여 학습시키고, 활용단계에서는 트리거를 포함한 입력 데이터를 특정 클래스로 분류하도록 하는 공격을 의미한다. 〔그림 2－30〕의 오른쪽 예와 같이, 그림 하단에 하얀 줄 패턴을 학습시킨 결과, 동일한 패턴이 있는 개의 사진을 고양이로 판단하는 경우가 백도어 공격의 예가 된다.

〔그림 2－30〕 오염 공격과 백도어 공격의 예



자료: C. Zhou et al, "Novel Defense Schemes for Artificial Intelligence Deployed in Edge Computing Environment"Wireless Communications and Mobile Computing (2020)

심지어, 이러한 학습 데이터를 디지털 데이터 수준에서 변조시키는 것 뿐만 아니라, 실제 도로 표지판이나 사람 얼굴 등에 스티커를 부착해서 오염을 일으키는 물리적 공격도 가능하다. 또한, 학습 대상 및 AI의 응용에 따라 이미지 뿐만 아니라, 네트워크 침입 탐지를 위한 인공지능 엔진을 속이고자, 네트워크 공격 혹은 악성 코드 학습용 데이터를 위변조하는 적대적 공격도 가능하다.

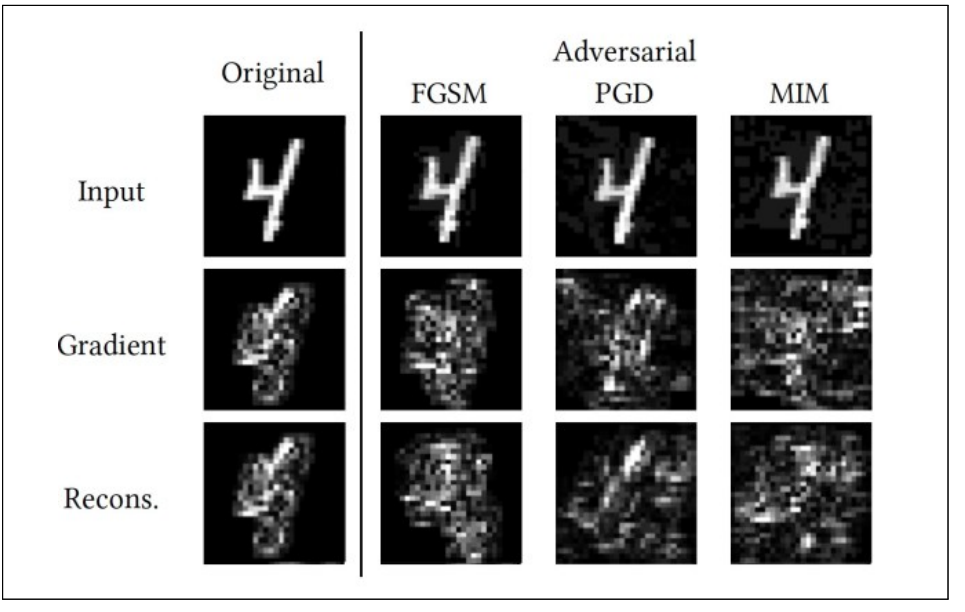
적대적 공격에 대한 대응 기술은, 크게 3가지 관점에서 이루어진다. 첫번째는 탐지 기술로서, 적대적 데이터와 진짜 데이터를 구별하는 대응 기술이다. 두번째는 이미 학습된 인공지능 엔진을 검증함으로써 대응하는 기술이며, 세번째는 적대적 데이터로부터 분류기를 보호하기 위한 기술이다.

이 중 가장 중요한 것은 첫번째 대응 기술인 적대적 데이터 탐지 기술일 것이다. 2017년 J. Metzen 등은 적대적 데이터와 진짜 데이터를 구별하는 이진 분류 작업을 훈련시킨 작은 '탐지기'를 기존 심층신경망의 일부로 사용하여 해당 심층신경망을 강화하는 방법을 제안하였다. 학습 데이터의 각 이미지마다 학습된 심층신경망에 대한 적대적 예재를 생성하고, 다시 검출기를 학습시킴으로써 적대적 데이터를 탐지할 수 있도록 하였다.

그럼에도, N. Carlini 등은 대부분의 탐지 기술이 쉽게 우회 가능하며, 심지어 탐지기가 학습되더라도 제한된 상황에서의 공격 시나리오에서 조차 탐지기를 우회할 수 있었다고 밝히고 있다. 이들은 어떻게 탐지 성능을 평가할 것인가에 대해 논의하였는데, MNIST 데이터셋으로만 평가하지 말 것, 전체 방어를 최소화할 것, 강력한 반복 공격을 사용할 것, 소스 코드를 공개할 것의 4가지 결론을 얻었다.

2021년 KAIST의 고기혁 박사는 비지도 학습을 통하여 적대적 예제 공격을 탐지하는 논문을 발표한 바 있다. 여기에서는 '설명 가능 인공지능(XAI, eXplainable Aritificial Intelligence) 기법'을 활용하여 적대적 제재를 구별하고 있으며, XAI에서 가장 널리 사용되는 방법 중 하나가 중요도 맵(Saliency Map)인데, 적대적 예제를 생성하기 위해 원본 이미지에 노이즈를 더하면 비정상적인 중요도 맵이 생성된다는 점에 착안하여 정상 이미지와 적대적 이미지를 분류하도록 하였다. 기존 탐지 관련 연구들은 대체로 지도 학습 기반으로 구성되었기 때문에 일반적으로 적대적 예재를 생성하는 단계에 크게 의존적이며 시간・계산 비용이 많이 필요하고 회피 가능성이 컸으나, 이 방식은 비용이 크지 않고 알려지지 않은 적대적 공격에도 대응 가능하다는 장점이 있다고 밝혔다.

〔그림 2－31〕 비지도 학습을 통한 적대적 예제 탐지
(적대적 예제는 중요도 맵의 재구성에 오차가 많음)



자료: G. Ko et al, "Unsupervised Detection of Adversarial Examples with Model Explanations"(2021)

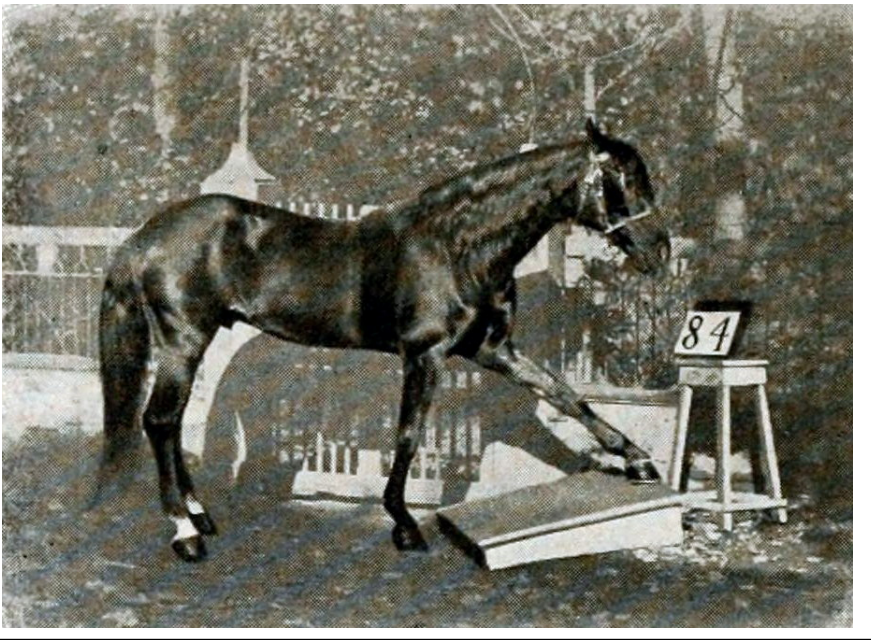
이 외에도 적대적 예제를 탐지하기 위하여, 공격자의 공격 공간을 줄이기 위해 여러 기법을 사용하는 Feature Squeezing 기, 적대적 예제에 포함된 노이즈를 제거하기 위한 기술 등이 연구된 사례가 있으며, 사이버 보안의 다른 분야와 마찬가지로 공격과 대응 기술이 서로 창과 방패처럼 주고받으며 급속도로 많은 기술적 변화·발전을 이루고 있다.

이러한 기술적 발전을 지원하기 위하여 구글은 적대적 공격 및 방어 기법들을 연구하는 자사의 오픈소스 소프트웨어 라이브러리 'CleverHans'[1]를 공개하고 있다. 미국의 DARPA에서는 AI 모델 보안을 위한 GARD(Guaranteeing AI Robustness against Deception) 프로그램을 운영하고 있으며, 주로 기만 공격을 방어하기 위한 연구를 지원하고 있다. GARD는

1) 'CleverHans'라는 이름은 19세기 말에서 20세기 초 독일에서 수학 문제를 푸는 것으로 유명해진 말(〔그림 2－32〕)의 이름으로, 한스는 간단한 수식을 보여주면 발굽을 두드린 횟수로 정답을 맞혔는데, 당시 유명한 심리학자인 O. Pfungst는 한스가 수학 문제를 이해하고 푼 것이 아니라 주변 사람들의 반응에 따라 발굽을 두드린 것임을 밝혀냈다.

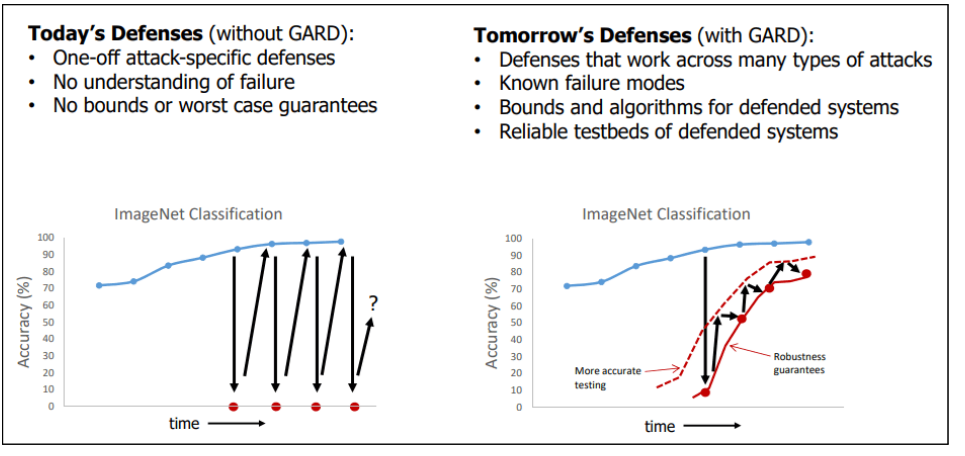
〔그림 2－33〕과 같이 많은 종류의 공격에 대응할 수 있으며, 새로운 공격이나 재공격에 완전히 무력화되지 않는 방어 기술을 개발하는 것, 대응 시스템에 대한 신뢰할만한 테스트베드 등을 목표로 한다.

〔그림 2－32〕 영리한 한스 (Clever Hans)



자료: https://www.amusingplanet.com/2020/05/clever-hans-horse-who-could-do-math.html (Last accessed: 2022년 9월 26일)

〔그림 2－33〕 GARD 프로그램의 목표



자료: https://www.eyerys.com/articles/news/using-guaranteeing-ai-robustness-against-deception-darpa-enhances-cybersecurity-ai (Last accessed: 2022년 9월 26일)

2. 기술 개발 현황

공통 기반 보안 기술에 관한 기술 개발 현황은 다음과 같다.

가. 국외 기술 개발 현황

1) 암호 기술

- (양자암호) 양자키분배 및 양자통신 기술은 주로 유럽, 중국을 중심으로 많은 연구가 이루어지고 있음
  - 미국 기업인 QuantumXchange는 2019년 에너지, 금융, 연방정부, 제조 분야 등에 활용할 수 있는 Phio 양자네트워크 구축. 2020년 Verizon은 워싱턴DC에서 QKD 네트워크 실험
  - EU는 2018년부터 수행중인 Quantum Flagship 프로그램의 일부 연구과제에서 QKD를 연구하고 있으며, H2020 프로젝트에서 OpenQKD 과제를 통해 13개국 38개 파트너와 함께 QKD 실험 플랫폼을 구성하는 것이 목표임
  - 중국과학원은 2017년 묵자(양자통신위성)를 통해 베이징-오스트리아간 7600km 양자암호통신 성공. 2개의 위성-지상 통신기와 700개 QKD 링크를 통합하는

4600km에 광섬유 네트워크 구축

- (양자내성암호) NIST를 중심으로 양자내성암호 공모를 통하여 일부 암호 표준안이 도출되었으며, 여기에는 미국과 유럽, 중국 등 많은 양자내성암호 전문가가 참여, 2024년경 추가적인 후보와 함께 최종 표준이 나올 것으로 예상됨
- (경량암호) 2012년 인증암호에 대한 시저(CAESAR) 경진대회의 첫번째 포트폴리오는 경량 응용(리소스가 제한된 기기 환경)이었으며, ASCON과 ACORN 등이 최종 후보로 선택됨. 양자내성암호와 유사하게 현재 경량암호에 대한 표준화 절차가 NIST에 의해 진행되고 있으며, 현재 최종 후보로서 10개의 알고리즘이 선정되어 있으며, 2023년경 최종 표준이 완료될 것으로 보임
- (부채널 분석 및 대응) AI기술이 발달함에 따라 이를 부채널 분석에도 활용하는 시도들이 많이 있으며, Cagli 등은 jitter 기반 하이딩 대응 기법에 대해 CNN을 이용한 분석이 가능함을 보임. 캐나다 임베디드보안 전문기업인 NewAE는 ChipWhisperer라는 오픈소스 기반 부채널 툴체인을 제공 중.

2) 인증・인가 및 접근제어

- (멀티팩터 인증) 멀티팩터 인증은 주로 구글, 아마존, 마이크로소프트와 같은 서비스 제공 업체, 시스코, RSA, 이셋 등 기업망 보안 솔루션 업체 등에서 관련 시장을 형성하고 있으며, 최근 코로나19 팬데믹 등 비대면 근무환경으로 인한 인증의 중요성이 커지면서 기업망 등에서도 많이 도입하고 있음
- (FIDO) FIDO에 대한 기술표준은 구글, 레노버, 비자, 마스터, 페이팔 등이 참여하고 있는 FIDO Alliance에서 제정하고 있으며, W3C의 웹인증 표준에서도 FIDO 2.0 기술이 공식적인 웹 표준이 됨으로써 더욱 널리 활용될 것으로 보임
- (무자각 지속 인증) 구글 등은 핸드폰 전면 카메라로 실시간 안면 인식을 수행할 수 있게 해주는 알고리즘을 개발한 바 있으며, 주로 학계에서 스마트기기를 통해 주로 생체 혹은 사용자의 행동패턴을 수집하여 딥러닝 기술을 활용하여 무자각 지속인증을 해주는 기술 연구 중. 정확도와 신뢰성 문제로 상대적으로 낮은 보안성을 요구하는 응용에서만 일부 활용 (특정 지역에서 핸드폰 잠금 화면 자동 해제 등)
- (분산ID) W3C를 중심으로 분산ID 표준화가 진행되어 왔으며, 마이크로소프트,

Accenture 등은 공식적인 아이덴티티 없이 살고 있는 난민 등에게 신원 정보를 부여하기 위한 ID2020 Alliance에 가입하였음. 에스토니아에서는 e-residence 시스템을 통해 가상거주자로서 에스토니아 디지털 국가에 합류하여 법적 신원을 부여받을 수 있으며, 유럽연합은 2020년 모바일 신분증의 자기주권 신원관리를 위한 프레임워크 ESSIF 발표

3) 데이터 보안

- (동형 암호) 덧셈과 곱셈이 가능한 최초의 동형암호를 IBM의 C. Gentry가 제안한 이후, 토론토 대학, 스탠포드 대학 등 대학과 연구소에서 재부팅과정의 제거 혹은 고속화, 평문데이터 구조의 다양화, 성능 고속화, 추가 연산 기능 등을 포함하면서 발전. 동형암호 연구 그룹을 중심으로 표준화 단체 Homomorphic Encryption Standardization를 만들어, 2018년 표준문서 발간. IBM, Microsoft, MIT, 서울대, CWI 등 다양한 연구그룹에서 오픈소스 기반 동형암호 라이브러리를 개발, 배포하고 있으며, 프라이버시 보존형 통계처리, 인공지능 등의 활용 방안 연구 중
- (차등 프라이버시) 2006년 마이크로소프트의 C. Dwork가 차등 프라이버시의 개념을 제안한 후, 애플이 자사의 음성비서 '시리'의 학습 데이터 처리에 차등 프라이버시 기법 적용 및 미국 통계청 인구조사에서 개인정보보호 강화를 위한 기본 프레임워크로 활용. 현재 구글의 TensorFlow, Microsoft의 WhiteNoise, 페이스북 Opacus 등 인공지능 학습모델에 적용 중

4) 하드웨어 보안

- (TPM) TCG(Trusted Computing Group)에서 TPM 표준 규격에 대한 표준화 작업을 진행하고 있으며, 동시에 ISO/IEC에서 표준화 진행. 인피니온, Nuvoton, STMicroelectronics 등이 TPM 칩을 생산하고 TCG 인증을 받았으며, Microsoft는 TPM 2.0 규격에 대한 공식 레퍼런스 구현. IBM에서는 소프트웨어 TPM을 개발하였으며, 인텔, AMD, 퀄컴 등은 CPU의 TEE 환경에서 동작하는 펌웨어 TPM 개발
- (TEE) GlobalPlatform의 TEE 위원회에서 TEE 표준 규격에 대한 표준화 작업을 진행하고 있으며, AMD의 PSP(Platform Security Processor), ARM의 TrustZone, IBM의

Secure Service Container, Intel의 SGX(Software Guard eXtension), RISC-V의 MultiZone 등이 계속해서 개발 중.

- (PUF) PUF는 ISO/IEC JTC1 SC27에서 PUF 요구사항 및 시험 방법에 대하여 각각 ISO/IEC 20897-1(2020년), 20897-2(2022년)로 표준화 완료됨. MIT, KU Leuven 외에도 다양한 대학 및 연구소에서 PUF의 다양한 물성 및 안전성에 대한 연구를 지속하고 있음. Secure-IC에서 Loop PUF, NVE에서 Spintronics Memory PUF, Intrinsic ID SRAM PUF을, 그 외에도 Def-Logix, Verayo, Lewis Innovative Technologies, CardLogix 등 많은 회사들이 PUF 칩 생산·판매 중.

5) AI 보안

- (적대적 공격) B. Biggio는 2013년 적대적 공격의 개념을 처음 정의하였으며, 이후 수많은 대학과 연구기관에서 새로운 형태의 적대적 공격, 혹은 이를 대응하기 위한 기법에 대한 연구를 진행하였음. I. Goodfellow, M. Dezfooli, N. Papernot, N. Carlini 등은 적대적 사례 생성방법을 각각 제시하여, 이를 기반으로 다양한 공격들이 연구되었으며, B. Liang, N. Papernot 등이 입력데이터를 조작하여 노이즈를 제거하거나 강건한 딥뉴럴네트워크를 구축하는 등의 대응 기법을 제안하였고, 그 외에도 다양한 대응 기법들이 연구 중에 있음. 초창기 주로 이미지 분야에서의 적대적 공격과 대층기법이 연구되었다면, 이후 음성, 텍스트, 의료 등 다양한 도메인에서의 사례도 계속해서 많은 연구가 이루어지고 있음

나. 국내 기술 개발 현황

1) 암호 기술

- (양자암호) KISTI는 현재 양자암호 기반 차세대 국가연구망을 구축 중으로 과학기술연구망 연동 및 키관리 기술 개발·실증이 목표임. SKT와 KT도 유무선 양자통신 기술 실증에 적극적으로 투자
- (양자내성암호) NIST 표준 공모전에서 국내 대학 및 연구소를 중심으로 Lizard 등 양자내성암호 후보를 제출하였으나 모두 1라운드를 넘기지 못하고 탈락함. 현재 정부와 국가보안기술연구소를 중심으로 한국형 양자내성암호 표준을 연구·개발하

기 위한 양자내성암호연구단(KpqC연구단)을 발족하여 NIST와 유사하게 공개키암호, 키설정, 전자서명 등의 항목으로 양자내성암호 국가공모전을 진행 중에 있음. ETRI는 기존 암호 및 양자내성암호에 대한 양자안전성을 검증하는 연구를 수행 중에 있음.

- (경량암호) 고려대에서는 2006년 경량블록암호인 HIGHT를 제안한 바 있으며, 국보연을 중심으로 2013년 LEA 제안후 2019년 ISO 경량암호 표준으로 제정. 2020년 효율적인 비트슬라이싱 구현 기반 신규 경량암호인 PIPO가 발표되는 등 고려대, 국민대, 한성대 등을 중심으로 경량암호에 대한 효율적인 구현 및 안전성 연구 중
- (부채널 분석 및 대응) 2010년대 초반 한국전자통신연구원 Scarf 프로젝트를 중심으로 많은 연구가 있었으며, 학계를 중심으로 점차 양자내성암호에 대한 부채널 분석, 인공지능 기반 부채널 분석 등의 연구 진행 중

2) 인증·인가 및 접근제어

- (멀티팩터 인증) ETRI는 2015년부터 2018년까지 상황인지기반 멀티팩터 인증 기술에 관한 연구를 수행하였으며, 생체 외에도 위치, 상황 인지의 인증 요소와 함께 인공지능 기술을 결합한 형태의 멀티팩터 인증 등에 대한 연구도 진행
- (FIDO) ETRI는 FIDO 기술을 지속적으로 개발하여 기술이전을 하고 있으며, 은행, 카드사 등 금융계에서 핀테크 인증 기술로 적극적으로 활용하고 있음. 최근 국정원은 공공분야 보안제품에 FIDO·생체인증 기본 탑재를 포함하는 국가용 보안요구사항 개발 계획을 발표
- (무자각 지속 인증) ETRI는 O2O 서비스를 위한 무자각 바이오 기반 식별자 추출 기술 등을 연구한 바 있으며, 국내에서는 주로 학계보다는 일부 생체인증 기업 등을 중심으로 관련 제품 개발을 하고 있음
- (분산ID) ETRI는 SKT 등과 함께 5G 환경에서의 자기통제형 분산 디지털 신원 관리 연구를 수행 중에 있음. 정부에서는 분산ID 기술을 이용한 모바일공무원증, 운전면허증 및 코로나백신 접종증명서비스 등을 차례로 도입하고 있으며, 분산ID의 활성화를 위한 오픈블록체인·DID협회 및 DID Alliance 등이 설립되어 활동 중임.

3) 데이터 보안

- (동형 암호) 서울대 천정희교수 연구팀은 근사계산을 통해 잡음 증가를 제어하여 회로 재부팅 횟수를 줄이고, 반올림 연산을 덧셈 수준으로 줄인 4세대 동형 암호를 2017년 발표하고, 암호 전문 스타트업 크립토랩 설립 후 라이브러리 HEAAN을 공개. 2016년 서울대 등은 DNA분석 및 생체인증에 활용 가능한 실용화 기술을 연구하였으며, 기계학습 활용 실용화 연구 수행 중. ETRI에서는 2022년부터 고성능 동형암호 최적화 컴파일러 기술 개발 과제 수행 중으로 헬스케어, 통계 분야 등에 활용하기 위한 원천기술 연구 진행 중이며, 네오와인 등은 동형 암호 고속화를 위한 하드웨어 개발 연구 중
- (차등 프라이버시) 서강대는 차등 프라이버시 기반 비식별화 연구를 진행한 바 있으며, 이지서티 등은 대용량 개인정보 가명・익명 자동처리에 차등 프라이버시를 활용하는 연구를 진행. 그 외에도 AI 학습을 위한 차등 프라이버시 적용 연구들이 기초 수준에서 진행 중이나, 많은 연구가 진행되지는 않음

4) 하드웨어 보안

- (TPM) 2007년 ETRI에서 모바일용 TPM 칩에 대한 연구개발을 수행한 바 있으며, 최근 경희대에서 IoT에 적용하여 신뢰 플랫폼 환경을 제공하는 연구를 수행하였음. 국내 기업으로는 삼성, SK하이닉스 등이 TCG 그룹에 참여 중임
- (TEE) 카이스트 등에서 TEE 보안성 향상 연구, 클라우드 환경의 실행 환경 보호 연구 등을, 인하대에서 바이오인식에 활용하는 연구를 수행한 바 있음. TEE를 IoT, 블록체인, 5G등에 활용하여 보안성을 높이고자 하는 응용 연구가 아이오트러스트, 케이스마텍, 티이이웨어 등에 의해 수행된 바 있음. 삼성의 경우, ARM TrustZone 등을 활용한 보안 솔루션 녹스(Knox)을 개발하여 자사 스마트폰 및 태블릿 등에 탑재하고 있음
- (PUF) 국내에서 PUF에 관한 연구는 초창기 한양대와 ICTK가 주도하였으며, ICTK는 VIA PUF를 이용한 PUF 보안칩을 개발하여 생산・판매 중. ETRI는 IoT 환경에서의 안전한 키은닉을 위하여 RF PUF, 통신-PHY PUF, Flash PUF 등 원천기술을 개발한 바 있으며, 다양한 센서의 PRNU를 기반으로 소프트웨어-PUF 등을 개발하

여 기술이전하였음. 그 외에도 PUF를 의료(임플란터블 기기), 영상감시 등 IoT 환경에 적용하여 보안성을 높이기 위한 연구들이 진행 중에 있음

5) AI 보안

- (적대적 공격) 국내에서도 서울대, 카이스트, 육군사관학교, 숭실대 등을 중심으로 다양한 적대적 공격 방법과 이에 대한 탐지・대응 기술을 연구하고 있음. 카이스트의 고기혁 박사는 비지도 학습을 통한 적대적 예제 공격 탐지 관련 연구를 수행하여 발표한 바 있으며, XAI 기법을 활용함.

3. 기술 발전 방향

가. 암호

암호 분야에서 가장 중요한 기술 이슈는, 양자 기술로 인하여 촉발되는 암호 안전성 문제를 어떻게 해결하느냐이다. 양자컴퓨터 상에서 동작가능한 Shor 알고리즘, Grover 알고리즘 등은 암호에 상당히 많은 영향을 미치고 있으며, 특히 현대 암호에서 광범위하게 사용되고 있는 공개키 암호 대부분 이산대수와 소인수분해 문제에 기반을 하고 있어, 수천만 큐비트 이상 혹은 에러정정기능을 내장하고 있는 수천큐비트 수준의 양자컴퓨터가 등장할 경우 Shor 알고리즘에 의해 DH 키교환, RSA, ECC 등이 모두 깨지게 된다.

현대 공개키 암호에 대한 양자 위협문제를 대응하기 위해 새로운 암호 체계를 도입하려면 여러 가지 요구사항을 만족해야 하는데, 대략적으로 다음과 같은 요구사항이 있을 것으로 보인다.

- 현재 사용중인 (고전) 컴퓨터에서 동작가능하여야 하며, 가급적 새로운 장비를 필요로 하지 않아야 한다.
- 현재 사용중인 공개키 암호가 제공하는 최소한의 기본 기능(공개키 기반 암호화, 키 교환/캡슐화, 전자 서명)을 제공할 수 있어야 한다.
- 키 길이, 암호문/서명문 길이, 하드웨어/소프트웨어 모듈 크기와 속도 등 성능면에서 현재 사용중인 응용이나 보안 프로토콜에 적용 가능해야 한다.
- Shor 알고리즘과 같은 양자 암호공격 알고리즘에 강인해야 한다.

이를 대응하기 위한 기술로, 흔히들 양자암호와 양자내성암호를 거론한다. 앞서 언급한 바와 같이 양자암호 기술은 양자 역학적 성질을 이용한 암호 기술을 의미하지만, 양자 암호는 마지막 항목을 제외한 다른 요구사항을 만족하기 어렵다고 보이므로 현재 공개키 암호 체계를 대체하기는 어려울 것으로 보인다.

현재 가장 성숙한 양자암호 기술은 양자키분배(QKD) 기술인데, QKD의 경우 물리(physical) 계층에만 적용과 구현이 가능하고 별도의 고가 장비를 필요로 한다. 또한, 점대점(Point-to-Point) 프로토콜이므로 종래 적용된 End-to-End Security를 만족하기 어렵고, Denial-of-Service 공격에 더 민감할 것으로 추정되며, 마지막으로 인증된 고전 통신 기술을 활용하여 편광 정보 공유가 필요하기 때문이다. 또한, 현재의 공개키 암호가 제공하는 보안 기능(특히, 인증, 전자서명 등)을 만족하기 어렵다.

이 때문에 미국의 NSA나 영국의 NCSC에서도 QKD를 정부·군과 같은 국가의 중요한 정보를 보호하기 위하여 사용을 권장하지 않고 있다. QRNG와 같은 난수발생기도, 현재 다른 방식으로 제공하는 TRNG를 반드시 대체해야 할 수준은 아닌 것으로 보인다.

현재까지, 양자 위협에 대처하기 위한 유일한 방법은 양자내성암호를 도입하는 것으로 보인다. 일각에서의, 양자내성암호의 안전성이 증명되지 않았다는 주장은 엄밀히 사실에 가깝지만, RSA 혹은 DH의 (고전 컴퓨터상의) 안전성 역시 수학적으로 엄밀히 증명되지 않고 지금까지 사용 중인 것을 고려하여야 한다. 초창기 공개키 암호 알고리즘도, 수학적인 난제에 기반하여 연구가 많이 되었으나, 그 중 많은 수의 알고리즘이 안전성에 문제가 생기기도 하였다.

RSA의 (고전 컴퓨터 상의) 안전성을 엄밀히 보려면 2가지 측면이 고려되어야 한다. 첫 번째로, 기반이 되는 소인수분해 문제가 안전한가이며, 두 번째로는 소인수분해 문제와 RSA 암호를 푸는 문제가 동일한 안전성을 갖는가이다. 지금까지 공격당한 대부분의 알고리즘은 두 번째 측면이 완벽하지 않아서 깨진 경우이다. 아마도 양자내성암호의 경우에도 두 번째 측면에서 공략가능하여 깨지는 알고리즘이 나올 가능성이 있다. 그러나 양자내성암호도 이미 20여년전부터 연구가 되어왔다는 것을 고려하면, 안전성이 수학적으로 엄밀히 증명된 것이 아니므로 수학적으로 증명가능한 양자 암호를 써야 한다는 주장은 맞지 않으며, 양자내성암호는 양자컴퓨터 시대에 많이 활용될 것으로 보이므로, 양자내성암호가 현대의 암호·보안 체계 및 응용과 결합 방법, 성능 개선을 위한 효율적인 구현, 안전

성에 대한 지속적인 검증 등에 대한 연구가 이루어질 것으로 보인다.

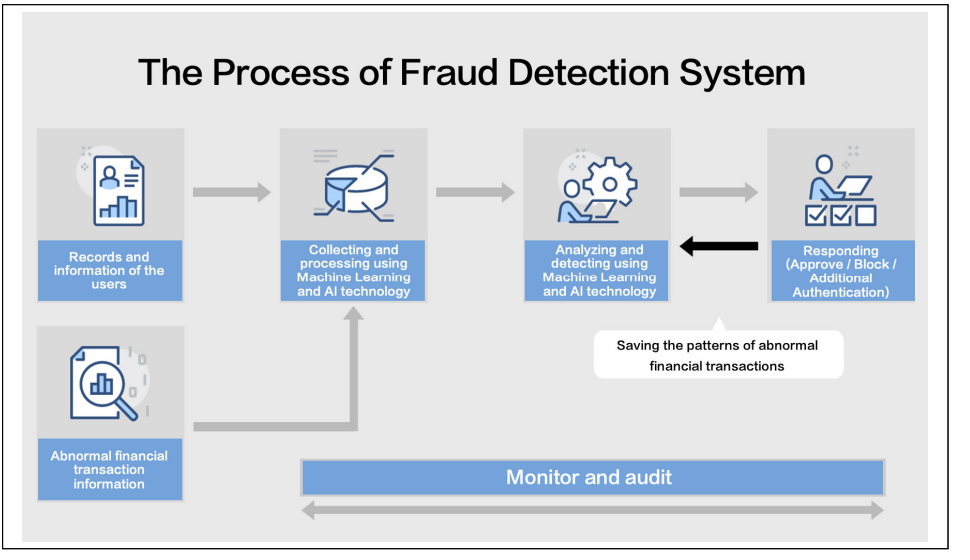
나. 인증·인가 및 접근제어

최근 제로트러스트 아키텍처와 같은 보안 모델이 떠오르면서, 정부·기업망 등에 접속한 사용자에 대하여 지속적인 인증 및 세밀한 접근제어에 대한 이슈가 많이 언급되고 있다.

현재 접속한 사용자에 대하여 신뢰성을 지속적으로 확인하고, 신뢰도가 부족한 사용자에 대해서는 멀티팩터 인증 등 보다 복잡한 형태로 인증함과 동시에, 인증이 완료된 이후라도 무조건 신뢰하는 것이 아니라 위치, 기기 상태, 사용자 행동 등 부가적인 정보를 파악하여 특정한 리소스에 무제한적인 접근을 허용하지 않고 신뢰도가 떨어지면 다시 한번 인증을 하게끔 하거나 접근을 제한하는 등의 조치가 이루어지도록 하는 것이다.

이렇게 인증과 접근 제어를 담당하는 솔루션을 보통 IAM(Identity and Access Management), ICAM(Identity, Credential and Access Management)로 부르는데, 현재의 기술 추세는 이러한 솔루션에 사용자·기기 모니터링 및 로그 기능을 갖는 보안 솔루션과 연동하여 사용자에 대해 지속적인 검증 및 신뢰도 평가, 의심스러울 경우 추가 인증 및 접근제어 기능까지 포함하는 것이 일반적이다. 이는 금융권에서 사용한 이상감지 시스템(FDS, Fraud Detection System)과 유사하며, 이들 기술들은 대체로 인공지능을 활용하여 신뢰도나 위험도를 점수 등의 형태로 평가하게 된다.

〔그림 2－34〕 이상 감지 시스템



자료: https://www.pentasecurity.com/blog/fraud-detection-system-fds-with-ai-technology/ (Last accessed: 2022년 9월 26일)

다. 데이터 보안

사용자의 프라이버시에 대한 의식이 높아지고 법령, 규정이 강화되는 반면, 주변에 있는 수많은 스마트기기 및 센서들은 여러 가지 목적으로 사용자에 관한, 혹은 사용자 주변의 데이터를 수집하고 있다. 이렇게 수집된 데이터는 통계 처리, 인공지능을 위한 학습 등 다양한 목적으로 처리되는데, 이 과정에서 앞서 언급한 프라이버시 문제가 발생할 경우, 해당 서비스 제공업체는 상당한 타격을 입을 가능성이 있다.

따라서 동형 암호 및 차등 프라이버시 기술은 모두 가트너와 같은 시장 조사 기관 및 MIT 등에서 꼽은 혁신적 기술 중 하나이므로, 앞으로도 널리 사용될 것으로 보인다. 특히, 동형 암호의 경우 지원 연산이 다양해지고 성능이 개선된다면 응용 분야는 무궁무진할 것으로 보이지만, 아직은 동형암호가 본격적으로 제품이나 서비스에 사용될 정도의 수준은 아니지만 많은 영역에서 실증 및 시험이 이루어지고 있으므로 조만간 기반 기술로서 널리 활용될 것으로 보인다. 차등 프라이버시 역시 애플, 구글, 마이크로소프트, 페이스북 등에서 활용·지원하는 기술이므로 AI 기술의 발전에 필수적인 기술이 될 것으로 보인다.

라. 하드웨어 보안

하드웨어 보안 기술은, 소프트웨어 안전성만으로는 부족한 부분을 해결해주고, 물리적인 안전성을 제공하고 있으므로 그 활용가치가 매우 높을 것으로 보인다. 특히 컴퓨터나 노트북 외에도 스마트폰, IoT, 스마트카, 스마트 헬스케어 기기와 같은 스마트 기기가 늘어나고 있으나, 이들은 물리적인 탈취 등에 더욱 취약하므로, 이로 인한 부가적인 공격(스마트폰 상의 데이터 노출, IoT 키 해킹 등)으로부터 전체 시스템을 보호해줄 수 있는 하드웨어 보안 기술은 그 중요성이 나날이 커지고 있음이 명백하다.

오픈 소스 기반 IoT TEE 환경 구축, 오픈소스 하드웨어인 RISC-V 상의 TEE 설계 등의 연구가 활발히 진행되고 있음을 고려하면, 가격이 보다 저렴해지고 개발 과정이 간편해질 경우 다양한 환경에서 하드웨어 보안 기술들이 사용될 것으로 보인다. 키 누출 공격에 저렴하게 대응할 수 있는 PUF 역시 TEE까지 사용하기 어려운 저사양 기기에서 활용될 가능성이 높을 것이다.

마. AI 보안

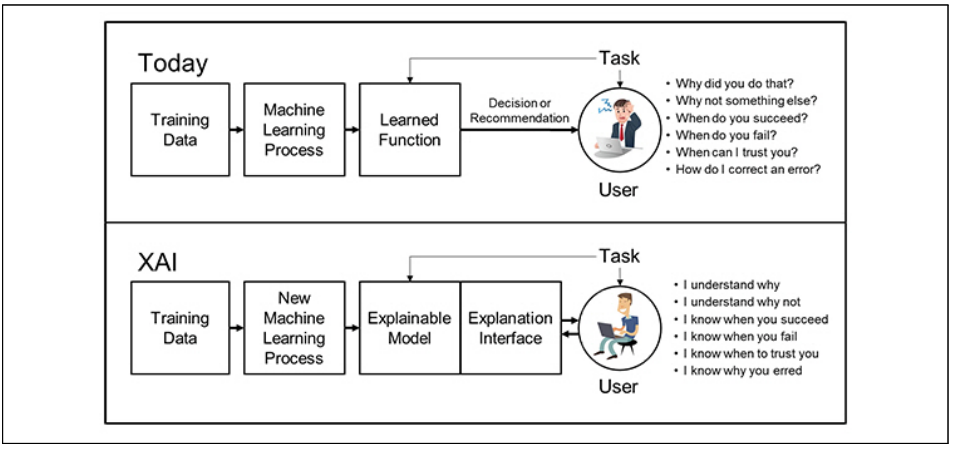
AI 보안 관점에서 가장 중요한 키워드는 '적대적 공격'이며, 오염 데이터를 주입함으로써 정상적인 학습 과정을 방해함으로써 학습 결과의 신뢰도를 낮추거나 오분류가 이루어지게 함으로써 서비스 이용자에게 잘못된 결과를 도출하게 만듦으로서 AI 기술 자체의 신뢰성을 떨어뜨리게 될 것이다. 특히, 인간의 생명과 연관된 자율주행자동차, 의료AI 등에 이런 문제를 일으킬 경우, AI 기술 발전에 상당한 걸림돌이 될 것임이 분명하므로, 이러한 적대적 공격을 탐지하거나 대응할 수 있는, 혹은 정상적으로 학습할 수 있는 방법들이 필요할 것이다.

딥러닝 혹은 AI 엔진의 내부적인 형태는 심층 신경망 구조를 활용하는 등 복잡하여 내부적인 구조를 통하여, 적대적 공격으로 인한 결과가 발생하는 원인을 찾는 것에 어려움이 있을 수 있으며, 그 외도 인공지능의 의사결정이 얼마나 신뢰할만한지에 대한 본질적인 의문이 있을 수도 있을 것이다.

이를 위해서는 〔그림 2-35〕와 같은 설명 가능한 AI(XAI) 기술이 하나의 해결책이 될 수도 있을 것으로 보인다. XAI는 주어진 데이터에 대한 분류, 예측 뿐만 아니라 결정에 대한 인과관계를 분석하여 사용자 수준에서 설명 가능하도록 하는 기술이다. 단순히 사용자 수

준에서의 해석 가능성 뿐만 아니라, 입력값이나 매개변수의 변경에 따르는 변화를 확인할 수 있어야 할 것으로, 충분히 성숙될 경우 모델 개량, 새로운 통찰, 법적 책임 등 다양한 이점이 있을 것으로 예상된다. 다만, 아직은 기술적으로 성숙하지 못한 상태이므로, 이에 대한 많은 연구가 있어야 할 것이다.

〔그림 2-35〕 설명 가능한 AI 기술 개념도



자료: https://www.darpa.mil/program/explainable-artificial-intelligence (Last accessed: 2022년 9월 26일)

제 2 절 시스템·네트워크 보안

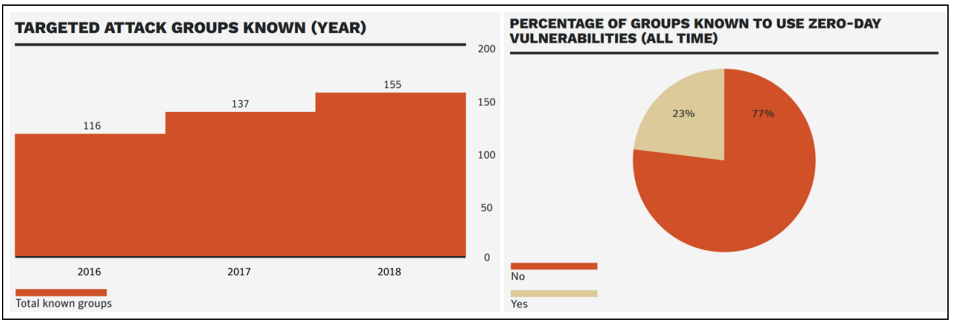
1. 개요 및 관련 기술

이 절에서는 시스템·네트워크 보안 분야의 차세대 핵심 요소기술로 사이버 위협 인텔리전스, 랜섬웨어 대응, IoT 디바이스 보안, 5G 보안, 클라우드 보안, 공급망 보안 등을 다룬다.

가. 사이버 위협 인텔리전스

지금은 미국 반도체 기업 브로드컴에 인수된 글로벌 보안회사 시만텍이 발간한 2019년 인터넷 보안 위협 보고서에 의하면 〔그림 2-36〕과 같이 알려진 표적 공격 그룹의 수는 2016년 116개, 2017년 137개, 2018년 155개로 꾸준히 증가하고 있으며, 그 중 제로데이 공격 사용 그룹 비율은 23%로 그렇게 많지 않음을 알 수 있다. 이는 대부분의 표적 공격 그룹이 이전에 사용했던 공격 기법 및 도구를 일부 수정하여 비슷한 방법으로 다시 공격을 시도하는 경우가 많다는 것을 의미한다.

〔그림 2-36〕 알려진 표적공격 그룹 수 및 제로데이 공격 사용 그룹 비율



자료: Internet Security Threat Report (ISTR) Volume 24, 2019, https://docs.broadcom.com/doc/istr-24-2019-en.

이러한 상황에서 발생하는 유사한 공격이나 변종 공격에 효율적으로 대응하기 위해 기존의 단편적으로 수집・공유되었던 데이터를 한 시스템에서 수집하여 공격 간의 연관성을 조사하고 공격의 유사성을 분석하는 사이버 위협 인텔리전스(Cyber Threat Intelligence; CTI) 기술이 필요하다. 일례로 SANS의 2019 사이버 위협 인텔리전스 보고서에 의하면 IT, 공공, 금융 등 여러 분야에서 근무하는 보안 담당자 중 다수(80.8%)가 사이버 위협 인텔리전스 활용이 효과가 있다고 응답했다.

한국정보통신기술협회(TTA)에서는 "사이버 위협 인텔리전스는 사이버 시스템의 안전을 위협하는 정보를 수집하여 상황을 분석하고 사이버 보안 위협에 효과적으로 대응하는 방법"이라고 정의하고 있다. 또한 미국 사이버 위협 정보 공유 가이드라인인 NIST SP 800-150를 살펴보면 사이버 위협 정보는 다음과 같이 다섯 종류로 분류 가능하다.

1) 지시자(Indicator) - 공격이 진행되거나 완료된 후 발생하는 산출물이나 지표를 의미하는 지시자

2) 전략・기술・절차(TTPs: Tactics, Techniques, and Procedures) - 공격자의 공격에 대한 전체적 흐름의 전략과 전략을 실행하기 위해 사용하는 기술, 그리고 이 기술의 세부 활동 순서를 설명하는 과정

3) 보안 경보(Security alerts) - 취약점, 보안 이슈와 관련된 보고서나 기사 등을 포함하는 보안 경보

4) 위협 첩보 보고서(Threat intelligence reports) - 위협이 발생하고 진행되는 이유와 목적을 총괄적으로 분석하고 해석하여 조직에서 의사결정을 할 수 있도록 작성된 보고서

5) 위협 정보의 수집, 교환, 처리, 분석, 사용을 지원하기 위해 사용되는 도구와 그 설정을 의미하는 도구 설정(Tool configuration)

각 기관 간에 사이버 위협 정보를 공유하기 위해서 사이버 위협 정보를 기술하는 언어가 필요하다. 그리고 언어로 표현된 문서의 교환 방식을 상호 표준화할 필요가 있다. 다수 기업 간의 위협 정보 공유 표준화를 위해 미국 국토안보부는 MITRE와 함께 2013년 사이버 보안 위협 정보공유 표현 표준 STIX(Structured Threat Information Expression)와 전송 표준 TAXII(Trusted Automated eXchange of Indicator Information)를 발표하였다.

STIX는 사이버 위협 정보를 규격화하고, 각 위협 정보의 특징을 명시하고 공유하기 쉬운 형태의 구조적 표현 방법을 채택하였다. STIX는 상호 운용성, 일관성, 효율성 및 일반

적인 상황에서 위협 인식 기능을 제공하기 위한 방법 체계를 제공한다. STIX를 이용하면 사이버 위협 정보를 일관성 있고 기계 판독이 가능한 방식으로 서로 공유할 수 있으므로 공격을 효과적이고 빠르게 예측하고 대응할 수 있게 된다. 2017년 발표된 STIX 2.0은 파일 형식이 기존 XML(Extensible Markup Language)에서 JSON(JavaScript Object Notation)으로 바뀌었으며 〈표 2-7〉과 〈표 2-8〉에 나타난 바와 같이 12개의 도메인 객체와 2개의 관계 객체로 구성된다.

〈표 2-7〉 STIX 2.0 도메인 객체 정의

객체	설명
공격 패턴(Attack Pattern) 객체	공격 패턴은 악의적 사용자가 대상의 훼손을 시도하는 방법을 설명하는 TTP(Tactics, Techniques, and Procedures)의 한 형식이다.
캠페인(Campaign) 객체	캠페인은 특정 목표군을 대상으로 일정 기간 동안 발생하는 일단의 악의적 활동 또는 공격을 설명하는 악의적 동작의 집합이다.
조치(Course of Action) 객체	조치는 공격을 예방하거나 진행 중인 공격에 대응하기 위해 실행한 작업이다.
ID(Identity) 객체	ID는 실제 개인, 조직 또는 그룹은 물론 개인, 조직 또는 그룹의 부류를 표현할 수 있다.
Indicator 객체	Indicator는 수상한 또는 악의적 사이버 활동을 검색하는 데 사용할 수 있는 패턴을 포함하고 있다.
침입 단체(Intrusion Set) 객체	침입 단체는 단일 조직이 지휘한다고 판단되는 공통 속성을 가진 악의적 동작과 리소스의 그룹화된 집합체이다.
멀웨어(Malware) 객체	멀웨어는 일명 악성코드 및 악성 소프트웨어라고도 알려진 TTP의 일종이며, 피해자의 데이터, 응용 프로그램 또는 시스템에 대한 기밀성, 무결성 또는 가용성을 훼손하거나, 또는 다른 방법으로 피해자를 괴롭히거나 붕괴시킬 의도를 가지고 시스템에 삽입하는 프로그램을 가리킨다
관측 데이터(Observed Data) 객체	관측 데이터는 사이버 관측 가능 객체 사양을 사용하여 시스템과 네트워크에 대해 관측한 정보를 전달한다. 예를 들어 관측 데이터는 IP 주소, 네트워크 연결, 파일 또는 레지스트리 키의 관측 정보를 포함할 수 있다.

객체	설명
보고서(Report) 객체	보고서는 위협 행위자, 멀웨어 또는 컨텍스트와 관련 세부 정보를 포함한 공격 기법에 대한 설명과 같이 하나 이상의 주제에 초점을 맞춘 위협 인텔리전스의 모음이다.
위협 행위자(Threat Actor) 객체	위협 행위자는 악의적인 의도를 가지고 운영된다고 판단되는 실제 개인, 그룹 또는 조직이다.
도구(Tool) 객체	도구는 위협 행위자가 공격을 수행하기 위해 사용할 수 있는 합법적인 소프트웨어이다.
취약성(Vulnerability) 객체	취약성은 해커가 시스템 또는 네트워크에 대한 액세스 권한을 얻기 위해 직접 사용할 수 있는 소프트웨어의 취약한 부분이다.

자료: 양준호, 김찬진, 김미연, 김지혜, 김종현, 염흥열, “사이버 위협 인텔리전스 공유 체계 연구”, 한국정보통신학회, 종합학술대회논문집 Vol. 22. No. 2., 2018.

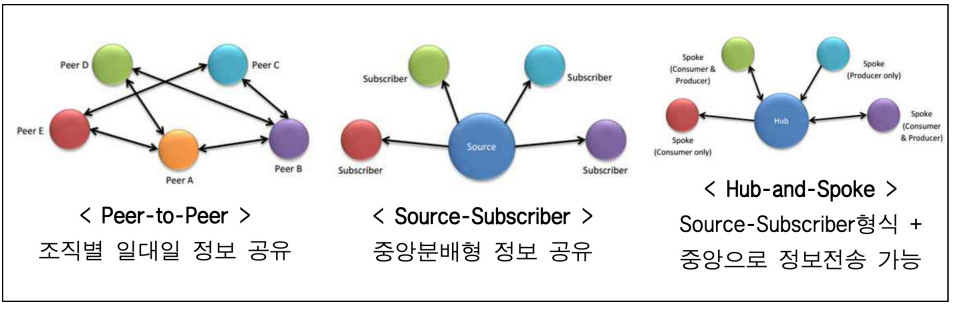
〈표 2-8〉 STIX 2.0 관계 객체 정의

객체	설명
관계성(Relationship) 객체	관계성은 두 SDO가 서로 관련된 방법을 설명하기 위해 이들을 서로 연결하는 데 사용된다.
발견(Sighting) 객체	발견은 Indicator, 멀웨어, 도구, 위협 행위자 등 CTI의 무언가가 발견되었다는 사실을 기술한다

자료: 양준호, 김찬진, 김미연, 김지혜, 김종현, 염흥열, “사이버 위협 인텔리전스 공유 체계 연구”, 한국정보통신학회, 종합학술대회논문집 Vol. 22. No. 2., 2018.

TAXII는 STIX로 표현된 사이버 위협 정보를 HTTPS를 통해 공유하기 위한 전송 규격으로서 HTTP의 장점을 최대한 활용하는 RESTful(REpresentational State Transfer) API와 TAXII 클라이언트 및 서버에 대한 요구사항의 집합을 정의하고 있다. TAXII는 〔그림 2-37〕에서와 같이 Peer-to-Peer, Source-Subscriber, Hub-and-Spoke 등의 다양한 위협 공유 모델을 지원한다.

〔그림 2-37〕 TAXII 위협 공유 모델



자료: 美 사이버 위협 정보공유 체계, 금융보안원.

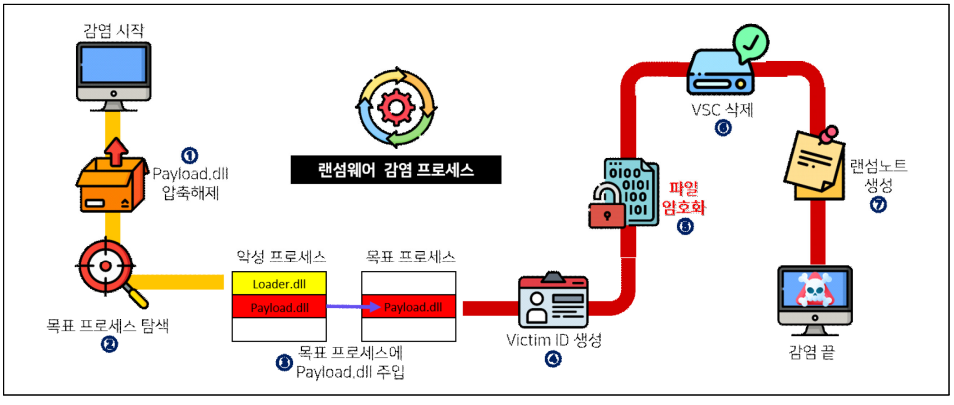
나. 랜섬웨어 대응

랜섬웨어는 몸값을 의미하는 랜섬(Ransome)과 소프트웨어(Software)의 합성어이다. 랜섬웨어는 피해자의 시스템이나 데이터 및 정보들을 인질로 삼아 피해자들에게 금전적인 요구를 하는 악성 소프트웨어이다. 랜섬웨어 피해의 증가 요인은 비트코인과 같은 가상화폐의 등장을 꼽을 수 있다. 가상화폐는 익명성을 보장하며, 공격자의 계좌 추적이 어렵기 때문에 랜섬웨어 공격자들은 몸값의 대가로 가상화폐를 요구하고 있다. 가상화폐의 가치는 천문학적으로 높아지고 있으며, 공격자들은 제작 시간 대비 고수익을 얻을 수 있다. 또한 서비스형 랜섬웨어(RaaS, Ransomware as a Service)의 등장으로 랜섬웨어 공격의 진입장벽이 낮아졌다. 전문 지식이 없는 사람도 만들어진 랜섬웨어를 구매하여 쉽게 공격을 수행할 수 있다. 그 결과 수많은 변종 랜섬웨어가 등장하고 있으며, 공격 사례는 지속적으로 증가하고 있다.

〔그림 2-38〕은 랜섬웨어 감염 프로세스를 총 7단계로 나타낸 것이다. 랜섬웨어 감염이 시작되면 악성 프로세스 역할을 수행하는 Payload.dll을 압축 해제한다(1). 그 다음 목표 프로세스를 탐색(2)하여 악성 프로세스를 목표 프로세스에 주입한다(3). 이로써, dll을 프로세스의 로드된 모듈로 등록하지 않아도 되어 dll 로드 모니터링 툴을 우회할 수 있다. 이후 피해자를 특정할 수 있는 Victim ID를 생성(4)하고, 파일 암호화를 수행한다(5). 5단계에서 파일 암호화 키를 생성하여 파일들을 암호화한다. 파일 암호화 키 관리 방법과 파일 암호화 방식은 랜섬웨어마다 다르기 때문에 감염된 파일 복구를 위해서는 이 부분에 대해 면

밀히 분석할 필요가 있다. 파일 암호화가 완료되면, 시스템 복원을 막기 위해 VSC(Volume Shadow Copy)를 삭제한다(6). 마지막으로 비용 지불 방법을 포함한 랜섬노트를 생성하여 시스템에 출력하고 감염이 완료된다.

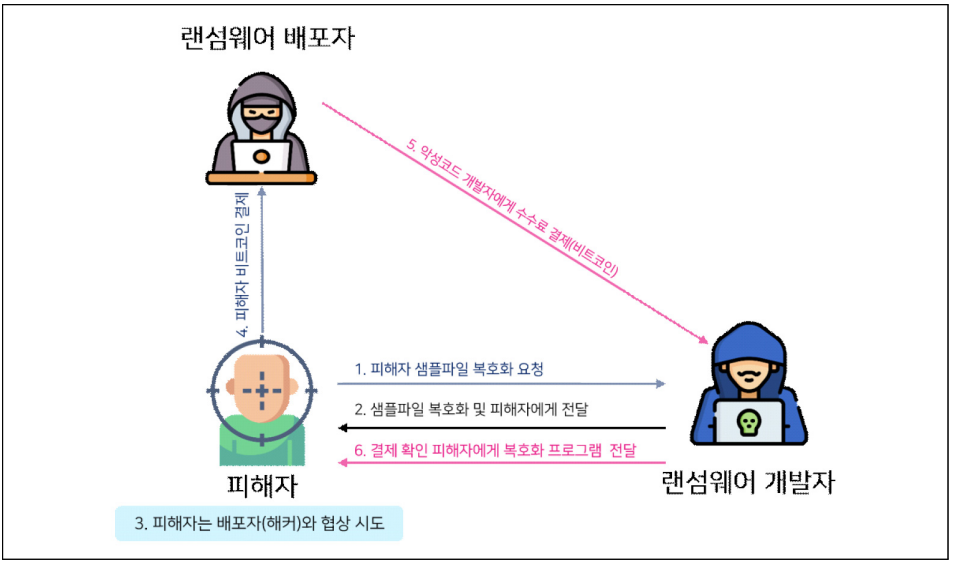
〔그림 2-38〕 랜섬웨어 감염 프로세스



자료: 박명서, “랜섬웨어의 파일 암호화 키 관리 방법 분류와 그에 따른 분석 대상 식별”, The Korea Institute of Information Security and Cryptology, vol. 32, no. 3, pp. 5-10, 2022.

피해자는 랜섬웨어 감염 이후 감염된 파일 복구를 위해 비용을 지불할 수 있다. 이때 화면에 출력되는 랜섬 노트를 통해 랜섬웨어 개발자에게 연락하는 파일 복구를 수행하게 되는데 〔그림 2-39〕는 이 과정에 대한 구체적인 프로세스를 나타낸다. 먼저 피해자는 랜섬웨어 개발자에게 감염된 파일의 복구 능력을 확인하기 위해 감염 파일 중 하나를 샘플 파일로 복호화 요청한다(1). 랜섬웨어 개발자는 감염된 파일 내에 있는 파일 암호화 키를 복구하여 샘플 파일을 복호화한 후 피해자에게 전달한다(2). 복구 능력을 확인한 패해자는 무료 복호화 도구 제공 및 가격 협상을 랜섬웨어 배포자와 시도한다(3). 피해자가 비트코인으로 비용을 결제(4)하면, 랜섬웨어 배포자는 그 중 일부를 수수료로 랜섬웨어 개발자에게 전달한다(5). 이 후 랜섬웨어 개발자가 피해자에게 복호화 프로그램을 전달(6)하면, 피해자는 그 프로그램을 이용하여 감염된 파일을 복구하게 된다.

〔그림 2－39〕 비용 지불 시 랜섬웨어 복구 프로세스



자료: 박명서, “랜섬웨어의 파일 암호화 키 관리 방법 분류와 그에 따른 분석 대상 식별”, The Korea Institute of Information Security and Cryptology, vol. 32, no. 3, pp. 5-10, 2022.

최근 몇 년간 발생한 주요 랜섬웨어 피해 사례들을 소개하면 다음과 같다.

2017년 전 세계 150여 개 국가가 워너크라이(WannaCry) 랜섬웨어에 공격을 받았다. 국내에서도 대학교 및 대형병원, 다수의 기업들이 공격당하였다고 알려졌다. 해당 랜섬웨어는 SMB 서비스 취약점을 이용하여 공격을 수행하였다. 한국인터넷진흥원(KISA)에 따르면 감염된 피해 시스템들은 모두 포트번호 445번을 통해 SMB 서비스를 실행하고 있었고, 오래 동안 보안 업데이트를 수행하지 않았다.

2017년 국내의 웹호스팅 업체가 Erebus 랜섬웨어에 공격당하였다. 이 인터넷호스팅 업체에서 관리하는 153대의 Linux 서버를 대상으로 공격을 수행하였으며 그 결과 약 3,000여 개의 홈페이지가 마비되는 사태가 발생하였다. 이 업체에서는 복호화 키를 전달받기 위하여 약 13억 원에 해당하는 금액을 지불하였다. 이후 공격자에게 복호화 키를 전달받았지만, 피해 받은 데이터들을 완벽하게 복구하지 못하였다.

2020년 국내의 대기업이 클롭(Clop) 랜섬웨어의 공격을 받았다. 랜섬웨어에 감염된 시스템은 일부 매장의 포스(POS) 단말기 등과 연동되어, 백화점 등 약 20여 곳의 매장이 영업

을 중단할 수밖에 없었다. 그룹의 사내 네트워크에서 랜섬웨어 감염이 발생되었으며 전산 복구 작업에만 수 주일의 시간이 필요하였다. 공격을 수행한 해킹 그룹은 약 200만 건의 카드 정보를 획득하였다고 주장하였으며, 약 4천만 달러의 금액을 요구하였다.

2021년 랜섬웨어의 공격을 받아 미국 최대의 송유관 운영업체가 마비상태에 이르렀다. Darkside 라는 해킹 그룹이 공격한 것으로 알려져 있으며, 해당 공격으로 송유관 약 8,850km 구간이 폐쇄되었다. 그 결과 미국 동부 지역 석유 공급 약 45%를 담당하는 업체의 마비로 인하여 석유값이 폭등하기도 하였다. 이 업체는 복구를 위하여 약 500만달러의 금액이 지불하기도 하였고, 미국은 비상사태를 선포하며 이번 사건을 유례없는 일로 규정하였다.

2021년 미국의 세계 최대의 육류 가공 업체가 랜섬웨어에 공격받았다. 이 기업은 호주와 미국, 캐나다와 브라질에 생산 시설을 두고 있는 대기업으로서 식품 업계 전체에 큰 피해가 예상되었다.

2021년 프랑스 보험사의 아시아 지사(태국, 말레이시아, 홍콩, 필리핀 지역 등)들이 랜섬웨어로부터 공격을 받았다. Avaddon 이라는 해킹 그룹은 자신들이 공격을 수행하였으며 3TB의 데이터를 갈취하였다고 밝혔다. 탈취된 정보들은 고객들의 개인정보, 의료 정보, 은행 계좌 등이 포함된 것으로 알려졌다.

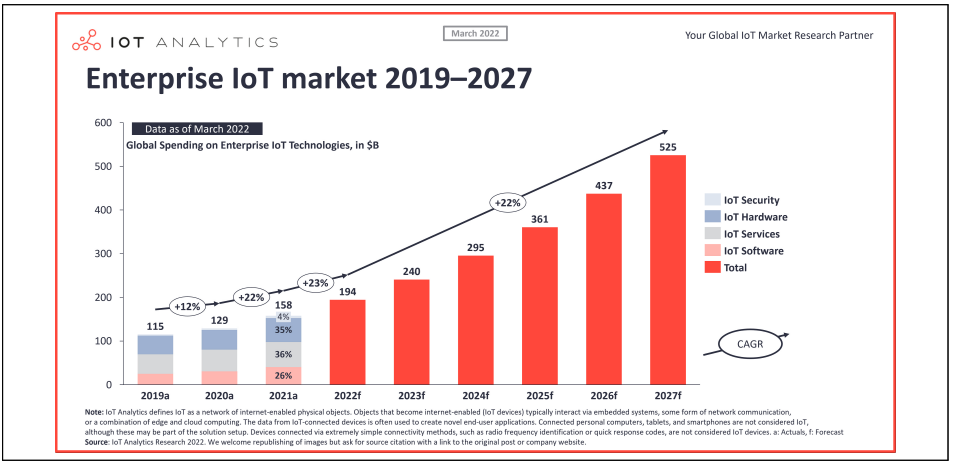
2021년 에콰도르의 최대 은행이 랜섬웨어에 공격을 받아 온라인 뱅킹, 모바일 앱, ATM 네트워크 등의 서비스가 중단되었다. 공격을 수행한 해킹 그룹 HotarusCorp은 탈취한 약 6,500 여개의 정보를 공개하였다. 공개된 정보에는 고객들의 개인정보, 비밀번호, 금융정보 등이 포함되었다.

2022년 일본의 유명 자동차 회사의 부품 제조사가 랜섬웨어 공격을 받아 설계 도면, 발주 서류 등 약 15만 건의 정보가 유출된 것으로 파악되고 있다. 공격을 수행한 해킹 그룹은 '기밀 데이터를 탈취하였으며, 정보들을 공개하겠다.'고 협박하였다. 또한 비슷한 시기에 주요 부품 거래처도 공격을 받았다. 그 결과 부품 공급 데이터 시스템이 마비되었고. 일본 내의 전 공장이 멈춰서는 피해를 입었다.

다. IoT 디바이스 보안

IoT(Internet of Things)는 다양한 사물에 센서와 통신 기능을 추가하여 무선 통신을 통해 각종 사물을 연결하는 기술을 말하며 4차 산업혁명의 핵심 기술 중 하나로 주목받고 있다. IoT Analytics에 의하면 서로 연결된 IoT 디바이스의 수는 2022년 말 기준 145억 개에 이를 것으로 보이며, IoT 시장의 규모도 〔그림 2-40〕과 같이 매해 평균 22.0% 성장할 것으로 기대하고 있다.

〔그림 2-40〕 IoT 시장 규모



자료: IoT Analytics. https://iot-analytics.com/iot-market-size/

IoT 디바이스는 그 특성상 저전력 및 저비용으로 구현되어야하기 때문에 높은 성능을 필요로 하는 보안 기술적용에 어려움이 따른다. 게다가 다양한 방법으로 공격자가 접근하기 쉬운 환경인 경우가 많아 보안이 취약하거나 공격 가능성이 높은 경우가 많다. 아래 〈표 2-9〉는 실제 보고된 IoT 보안사고 피해사례를 나타낸 것이다.

〈표 2-9〉 IoT 보안사고 사례

년도	월	보안사고 사례
2020	06	공격자가 UPNP 서비스를 이용하여 IoT 장치에 DDoS 공격을 수행하고 내부 네트워크에 접근이 가능한 보안 취약점 공개(CallStranger)
2019	07	VxWorks RTOS를 사용하는 프린터, 라우터, 스카다 시스템, IoT 장치 공격이 가능한 'Urgent11' 보안취약점 공개
	06	메드트로닉 사에서 만든 인슐린 펌프 장비 일부에서 공격자가 무선 네트워크 침투를 통해 인슐린 양을 조절할 수 있는 취약점 발견
	01	삼성 디지털 도어록에 스마트 워치를 "키"로 사용할 경우, 등록 되지 않은 스마트 워치로 모든 삼성 디지털 도어록 열림 현상 발생
2018	11	엡해킹으로 통해 국내 반려동물 사이트를 해킹하여 1만 5,000여명의 IP카메라 정보 획득 후, 획득한 정보를 통해 264대의 IP카메라에 무단 접속하여 불법 촬영 발생
	07	시스코 탈로스(Cisco Talos)에서 삼성 스마트싱스 허브(Samsung SmartThings Hub) 장치 펌웨어서 20개 취약점 발견
2017	08	심장 박동기에 공격자가 무단 접속을 통해 명령을 내리고 설정을 변경하거나 기능들을 방해할 수 있는 취약점 발견
2016	10	DNS 서비스 업체 다인(Dyn)이 IoT 장치를 이용한 대규모 DDoS 공격으로 넷플릭스, 트위터, 뉴욕타임즈 등 총 70 여개의 사이트가 서비스 지연 또는 마비되는 사건 발생
2015	07	크라이슬러 체로키의 유커넥트 시스템에 접속하고 자동차의 펌웨어를 변경하여 제어권을 탈취하여 차량을 컨트롤할 수 있는 취약점 발견

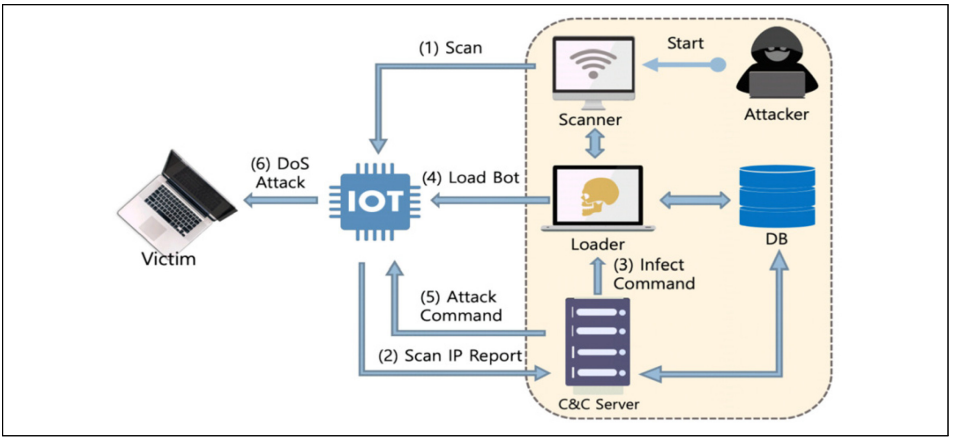
자료: 조영민, "IoT 펌웨어 취약점 분석 효율성 제고를 위한 시스템 개발에 관한 연구", 한국산업보안연구, Vol. 12. No. 1., pp. 31-50, Apr. 2022.

여기서는 실제 IoT 디바이스 공격이 어떻게 일어나는지 알아보기 위해 2016년 10월 DNS 서비스 업체 Dyn 공격에 사용되었던 미라이 봇(Mirai bot)의 세부 동작 과정을 살펴보도록 하겠다.

미라이 봇의 세부 동작 과정은 〔그림 2-41〕과 같다. 미라이 봇은 초기 실행 시 네트워크 스캔 기능을 수행한다. 이를 위해 랜덤 IP 주소를 생성한 후 Telnet 서비스가 사용하는 23번 포트를 통하여 IoT 디바이스를 대상으로 무차별 대입 공격(Brute Force Attack)의 일종인 사전 공격(Dictionary Attack)을 시도한다. 사전 공격을 통해 IoT 기기 접속에 성공하면 미라이 봇 악성코드를 해당 기기에 전송하여 실행하는 과정을 반복하며 거대한 봇넷

(Botnet)을 형성한다. 마지막으로 봇넷은 C&C(Command and Control) 서버에 접속하여 대기하다가 공격 명령이 떨어지면 DDoS 공격을 수행한다.

〔그림 2－41〕 미라이 봇 세부 동작 과정



자료: 이형우, "IoT 봇넷 악성코드 기반 침해사고 흔적 수집 방법", 사물인터넷융복합논문지, vol. 7, no. 3, pp. 1-8, 2021.

라. 5G 보안

우리가 5G라고 부르는 모바일 네트워크 기술은 국제 이동통신 표준화 기구인 3GPP에서 제정한 5세대 이동통신 기술로 초고속, 초연결, 초저지연의 특징을 가져 4차 산업혁명의 핵심 기술 중 하나로 주목받고 있다. 여기서는 3GPP에서 Release 15로 발간한 TS 33.501 "Security Architecture and Procedures for 5G System" 문서를 바탕으로 5G 보안 구조에 대해 살펴보겠다.

3GPP 표준에서는 〔그림 2－42〕와 같이 보안 구조를 총 6개의 도메인으로 구분하여 정의한다.

(Ⅰ) 네트워크 접속 보안(Network Access Security)은 휴대폰, 태블릿 또는 노트북과 같이 최종 사용자가 직접 통신하는 사용자 장비가 3GPP이거나 3GPP가 아닌 접속망을 통해 안전하게 서비스를 인증하고 접속할 수 있도록 하며, 특히 무선 인터페이스에 대한 공격으로부터 망을 보호한다.

(Ⅱ) 네트워크 도메인 보안(Network Domain Security)은 네트워크 노드가 신호 메시지와 사용자 데이터를 안전하게 교환할 수 있도록 하는 보안 기능 집합으로 서비스 네트워크(SN)와 사용자가 가입한 홈 네트워크(HN) 사이 또는 접속 네트워크와 핵심 네트워크 사이의 인터페이스에 대한 보안 기능을 정의한다.

(Ⅲ) 사용자 도메인 보안(User Domain Security)은 모바일 기기에 대한 사용자의 접근을 보호하는 보안 기능 집합이다. 모바일 기기는 PIN(Personal Identification Number) 코드와 같은 내부 보안 메커니즘을 이용하여 모바일 기기와 USIM (Universal Subscriber Identity Module) 사이의 보안을 보장한다.

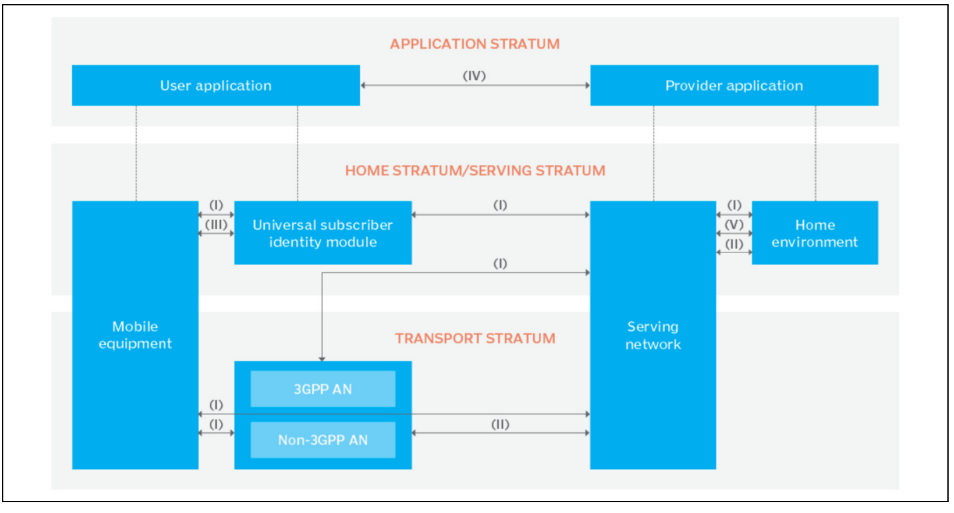
(Ⅳ) 응용 도메인 보안(Application Domain Security)은 사용자 도메인과 서비스 공급자 도메인의 응용 프로그램이 메시지를 안전하게 교환할 수 있도록 하는 보안 기능 집합이다.

(Ⅴ) 서비스 기반 구조(Service based Architecture; SBA) 도메인 보안(SBA Domain Security)은 서비스 기반 구조에 의해 네트워크 기능들을 안전하게 구현하고 수행하기 위해 사용되는 보안 기능 집합이다.

(Ⅵ) 보안의 가시성과 설정가능성은 〔그림 2-42〕에는 나타나 있지 않지만, 보안 기능이 작동 중인지 사용자가 알 수 있도록 하는 기능 집합이다.

이와 같이 6개의 도메인으로 정의된 5G 보안 구조가 이전의 4G 보안 구조와 비교할 때 가지는 가장 큰 차이는 네트워크 접속 보안에서 3GPP 접속망 뿐만이 아닌 3GPP가 아닌 접속망까지 동일한 하나의 인증 체계를 통해 접속할 수 있도록 개선된 점과 서비스 기반 구조 도메인 보안이 새롭게 추가된 것이라 할 수 있다.

〔그림 2－42〕 5G 보안 구조



자료: What's the answer for 5G security? https://www.techtarget.com/searchsecurity/opinion/Whats-the-answer-for-5G-security.

5G에 이르러 새롭게 추가되거나 기존에 비해 기능이 강화된 주요 보안 기능을 소개하면 다음과 같다.

1) 가입자 식별정보 암호화

5G 이전의 이동통신에서 가장 이슈가 되었던 보안 위협 중 하나는 단말과 기지국 사이의 무선 구간에서 가입자 식별정보인 IMSI(International Mobile Subscriber Identity)가 암호화되지 않은 채 전달되어 공격자에 의해 탈취될 수 있다는 점이다. 5G에서는 가입자 식별정보가 전달되는 초기 접속과정에 이를 암호화하여 전달하도록 보안 기능을 강화하였다.

2) 상호 인증 과정 개선

이동통신 네트워크에 접속하기 위한 단말과 네트워크 사이의 상호 인증을 위해 4G LTE 환경에서는 EPS(Evolved Packet System) AKA(Authentication and Key Agreement) 절차를 사용한다. 하지만 EPS AKA 절차는 앞에서 언급한 바와 같이 가입자 식별정보인 IMSI를 암호화하지 않은 채 전달하여 공격자에게 탈취될 수 있는 위험이 존재하고 네트워크가 단말

을 인증하는 과정에서 단말이 접속한 서비스 네트워크(SN)는 단말을 인증하지만 단말이 가입되어 있는 홈 네트워크(HN)은 인증과정에 참여하지 못하는 단점을 가진다.

5G에서는 인증을 위해 5G AKA와 EAP(Extensible Authentication Protocol)-AKA' 절차 두 가지를 주요 인증 규격으로 정의하여 인증 방법 선택에 있어 유연성을 가지면서 앞에서 이야기한 문제점들을 해결하였다.

3) 무선 구간 사용자 데이터 보호 강화

단말과 네트워크 사이의 상호 인증 과정이 성공적으로 이루어지면 단말과 네트워크 사이에 주고받는 신호 메시지와 사용자 데이터를 보호하기 위한 암호화 및 무결성 보호 과정이 진행된다. 4G LTE에서는 이와 관련하여 신호 메시지에 대한 무결성 보호만이 강제사항이고 사용자 데이터에 대한 무결성 보호는 부하 증가로 인해 요구사항에 넣지 않았다.

하지만 5G에서는 사용자 데이터에 대한 무결성 보호를 강제사항은 아니지만 선택사항으로 넣음으로써 상황에 따라 사용자 데이터 무결성 보호가 가능하도록 하였다. 또한 암호화에 있어서도 4G에서는 신호 메시지와 사용자 데이터 암호화가 단순 선택사항이었으나 5G에서는 특별한 제약사항이 없으면 가능하면 사용하도록 보안을 강화하였다.

4) 서비스 기반 구조 보안

5G 시스템 구조에서 새롭게 추가된 부분이 서비스 기반 구조이다.

모든 네트워크 기능은 HTTP(Hypertext Transfer Protocol)로 이루어진 서비스 기반 인터페이스(Service based Interfaces)를 통해 동작하며 IPSec(IP Security)과 같은 네트워크 계층에서의 보안 프로토콜 외에 전송 계층에서도 메시지 보안을 위해 TLS 프로토콜을 반드시 지원하도록 하였다.

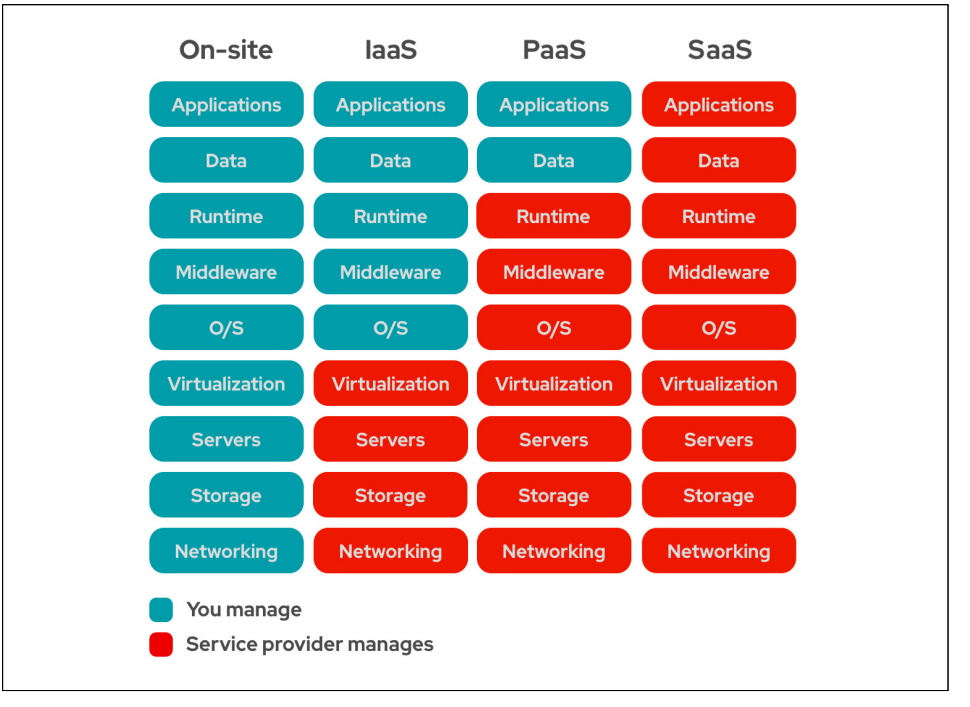
5) 이동통신 네트워크 사이 신호 메시지 보호 강화

5G 환경에서는 로밍 시 신호 메시지 보호를 위해 SEPP(Security Edge Protection Proxy) 기능을 새롭게 정의하였다. SEPP를 통해 로밍 시 이동통신망 사업자 사이에 주고 받는 신호 메시지에 대한 무결성 보호 및 기밀성을 제공한다.

마. 클라우드 보안

NIST(National Institute of Standards and Technology)에 따르면 클라우드 컴퓨팅은 사용자의 시스템 관리를 최소화하고 서비스 제공자와의 상호 작용만으로 컴퓨팅 시스템의 자원들을 빠르고 편리하게 제공받는 서비스이다. 클라우드 컴퓨팅은 〔그림 2-43〕과 같이 사용자에게 제공하는 서비스 유형에 따라 Iaas, PaaS, SaaS의 3가지 서비스 유형(모델)으로 구분할 수 있다.

〔그림 2-43〕 클라우드 컴퓨팅 서비스 모델



자료: IaaS, PaaS 및 SaaS 비교 https://www.redhat.com/ko/topics/cloud-computing/iaas-vs-paas-vs-saas.

IaaS(Infrastructure as a Service)는 서버, 저장장치, 네트워크와 같은 물리적인 컴퓨팅 자원에 대한 제어권을 사용자에게 제공하는 서비스이다. 보통 논리적으로 완전한 기능을 수행하는 하나의 컴퓨팅 환경으로, 하나의 물리적 서버에 여러 개의 가상 머신 또는 컨테이

너를 포함하는 형태로 구성되며 다른 부분으로부터 격리된 환경이 제공된다.

PaaS(Platform as a Service)는 사용자가 어플리케이션 개발, 테스트 및 배포에 있어 필요한 운영체제, 프로그래밍 언어, 라이브러리 같은 플랫폼을 클라우드 서비스 형태로 사용자에게 제공하는 서비스이다. 사용자는 서버, 운영체제, 네트워크, 저장장치와 같은 클라우드 인프라에 대한 관리 및 제어권은 가지지 못하나 어플리케이션 실행을 위한 환경 설정이나 해당 어플리케이션에 대한 제어권을 가진다.

SaaS(Software as a Service)는 다양한 사용자 장치로부터 네트워크를 통하여 어플리케이션 소프트웨어를 클라우드 서비스 형태로 제공하는 서비스로, 사용자는 특정 어플리케이션의 설정 사항을 포함하여 해당 어플리케이션 소프트웨어가 구동되는 클라우드 인프라에 대한 관리 및 제어가 불가능하다.

클라우드 컴퓨팅은 사용 대상 및 구성에 따라 퍼블릭, 커뮤니티, 프라이빗, 하이브리드 클라우드로 구분할 수 있다.

퍼블릭 클라우드(Public Cloud)는 일반 사용자들을 위하여 개방된 형태로, 인터넷에 접속 가능한 모든 사용자를 위한 클라우드이다. 서비스 내부에 저장된 데이터나 기능, 컴퓨팅 자원은 각 서비스에서 사용자마다 별도의 권한 관리가 이루어지며 사용자 간에 간섭이 존재하지 않도록 구성된다.

커뮤니티 클라우드(Community Cloud)는 임무, 정책, 규정, 보안 요구사항 등 공동의 목적을 공유하는 특정 기관들에 의해 운영되며 해당 기관 구성원들에게만 접근이 허용된다.

프라이빗 클라우드(Private Cloud)는 단일 기관에 의해 배타적으로 운영되는 형태로 컴퓨팅 자원의 제어권을 해당 기관이 가지고 있어, 다른 모델에 비해 상대적으로 보안 측면에서 안전한 편이며 접근 권한을 부여받은 사용자들만 서비스 이용이 가능하다.

하이브리드 클라우드(Hybrid Cloud)는 퍼블릭, 커뮤니티, 프라이빗 클라우드의 조합으로 구성된 형태로, 보안이 중요하거나 컴퓨팅 자원에 대한 제어가 필요한 서비스에서는 프라이빗 클라우드 및 커뮤니티 클라우드를 이용하고 그렇지 않은 경우에는 퍼블릭 클라우드를 이용한다.

다수의 사용자들이 원격 접속을 통해 제공받는 클라우드 서비스 환경은 가상화 기술의 적용, 자원의 공유, 정보의 위임, 이용되는 단말의 다양성 등의 특성으로 인해 다양한 보안 위협이 발생 가능하다. 2022년 6월 클라우드 보안 연합(Cloud Security Alliance)에서 발표

한 보고서에 의하면 〔그림 2-44〕와 같이 다양한 클라우드 컴퓨팅 보안 위협이 있음을 알 수 있다.

〔그림 2-44〕 2022년 클라우드 컴퓨팅 보안 위협 Top 11

Survey Results Rank	Survey Average Score	Issue Name
1	7.729927	Insufficient ID, Credential, Access and Key Mgt, Privileged Accounts
2	7.592701	Insecure Interfaces and APIs
3	7.424818	Misconfiguration and Inadequate Change Control
4	7.408759	Lack of Cloud Security Architecture and Strategy
5	7.275912	Insecure Software Development
6	7.214493	Unsecure Third Party Resources
7	7.143066	System Vulnerabilities
8	7.114659	Accidental Cloud Data Disclosure/ Disclosure
9	7.097810	Misconfiguration & Exploitation of Serverless & Container Workloads
10	7.088534	Organized Crime/ Hackers/ APT
11	7.085631	Cloud Storage Data Exfiltration

자료: Top Threats to Cloud Computing https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven.

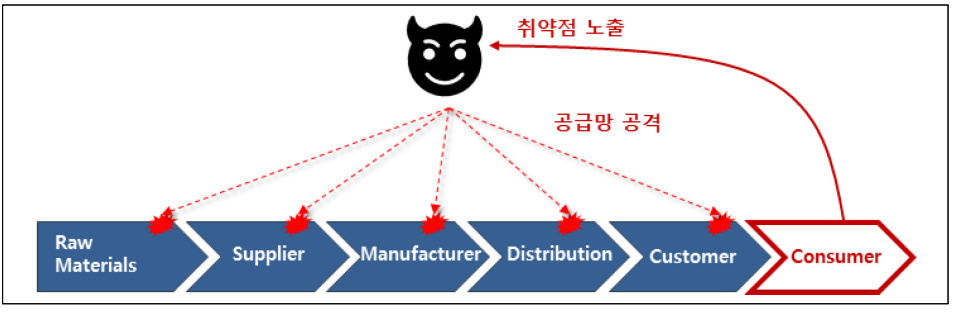
클라우드 보안 연합의 최근 발표 자료에 따르면 클라우드 컴퓨팅 보안에 있어서 위협이 되는 부분은 시스템이나 프로그램의 취약점 같은 기술적인 부분보다는 사용자나 관리자의 부적절한 사용이나 부주의 같은 관리적인 문제가 더욱 중요함을 지적하고 있다. 따라서 보안 위협에 대한 기술적 대응 못지않게 내부자의 보안 인식 제고 같은 관리적인 부분도 중요함을 알 수 있다.

바. 공급망 보안

4차 산업혁명 시대를 맞이하여 다양한 분야에 디지털 트랜스포메이션(Digital Transformation)이 도입되면서 이와 관련한 사이버 공격 또한 증가하고 있다. 많은 기업이 제품과 서비스의 설계・개발・제조・운용・보수・폐기에 이르는 전 과정 중 일부를 외부에 위탁하여 처리하곤 하는데 이러한 공급 프로세스를 공급망(Supply Chain)이라 한다.

많은 기업이 생산 단가 인하 등의 목적으로 공급망을 해외로 이전하면서 정치적 이슈를 포함한 다양한 문제로 공급망 위험 또한 증가하고 있다. NIST SP 800-161에 따르면 하드웨어나 소프트웨어로 구성된 ICT 제품의 공급망은 전 세계적으로 분산되면서 여러 계층으로 구성되어 복잡하면서 상호 연결된 공급망 생태계에 의존하기 때문에 제품의 설계・생산・배포 모든 단계에서 위・변조 방지 및 투명한 관리가 쉽지 않다. 따라서 〔그림 2-45〕와 관련하여 다양한 공급망 보안 사고들이 보고되고 있다.

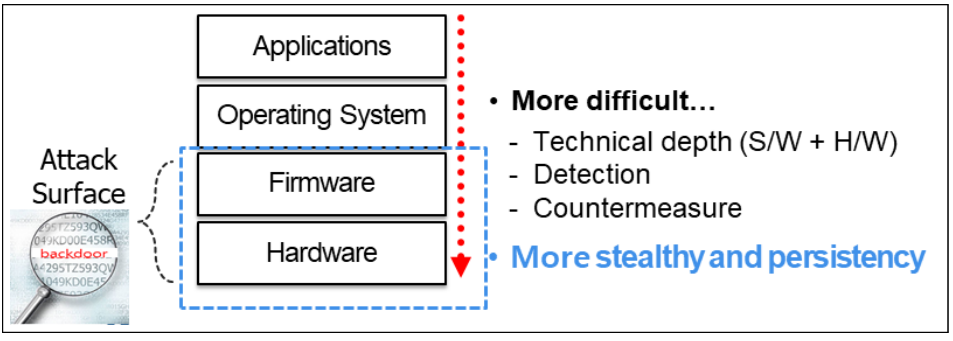
〔그림 2-45〕 공급망 위협 개념도



자료: 김대원, 강동욱, 최용제, 이상수, 최병철, "공급망 보안기술 동향", Electronics and Telecommunications Trends, vol. 35, no. 4, pp. 149-157, Aug. 2020.

특히 〔그림 2-46〕과 같이 하드웨어 제조과정에 백도어를 숨겨서 공격하는 방법은 탐지 및 분석이 어렵기 때문에 점차 확대되는 추세로 대응 기술 역시 일반적인 소프트웨어 기반 백도어에 비해 복잡한 분석을 요구하고 있으며, 이를 위해 주로 펌웨어/PCB(Printed Circuit Board)/IC(Integrated Circuit)칩을 대상으로 분석 및 취약점 탐지를 수행한다.

〔그림 2－46〕 하드웨어 공급망 공격 분석 및 탐지의 어려움

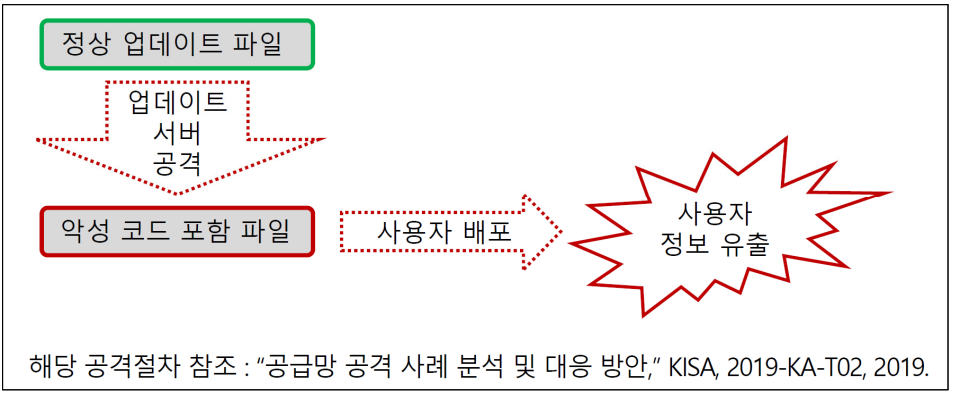


자료: 김대원, 강동욱, 최용제, 이상수, 최병철, “공급망 보안기술 동향”, Electronics and Telecommunications Trends, vol. 35, no. 4, pp. 149-157, Aug. 2020.

대표적인 공급망 공격 사례에는 ASUS 업데이트 서버 공격, CCleaner 업데이트 서버 공격, MEDoc 업데이트 서버 공격 등이 있다.

ASUS 업데이트 서버 공격은 2019년 1월 해외 보안 기업 카스퍼스키(Kaspersky)사가 자체 탐지 솔루션에 공급망 공격을 탐지하기 위한 코드 스캐닝 기법을 적용하여 처음 탐지하여 ‘셰도우해머 작전(Operation ShadowHammer)’으로 불리는 공격이다. 공격자는 〔그림 2－47〕에서와 같이 ASUS 업데이트 서버에 침투하여 업데이트 파일을 악성 코드를 포함한 파일로 바꾸어 전 세계적으로 총 100만 대 이상의 PC를 감염시킨 것으로 추정된다. 탐지를 회피하고자 악성 코드를 포함한 업데이트 파일을 유효한 ASUS 인증서로 서명하였으며, 악성 코드에 하드코딩된 MAC(Media Access Control) 주소 리스트를 통해 추가 악성코드를 다운로드 받을 수 있도록 구현하였다.

〔그림 2－47〕 ASUS 업데이트 서버 공격 절차



자료: 김대원, 강동욱, 최용제, 이상수, 최병철, "공급망 보안기술 동향", Electronics and Telecommunications Trends, vol. 35, no. 4, pp. 149-157, Aug. 2020.

CCleaner 업데이트 서버 공격은 2017년 8월 공격자가 보안 업체 Avast가 만든 PC 최적화 소프트웨어인 CCleaner의 공식 업데이트 서버에 침투하여 해당 소프트웨어에 악성코드를 은닉한 후 약 한 달에 걸쳐 이를 다운로드한 대략 220만 사용자의 PC를 감염시킨 공격이다. 이 공격을 통해 일반 사용자 PC가 주로 감염되었으나 데이터베이스 분석을 통해 공격자가 실제로 노린 건 시스코, 마이크로소프트, 구글, 소니, HTC를 포함한 18개의 대형 IT 기업들이었던 것으로 추정된다.

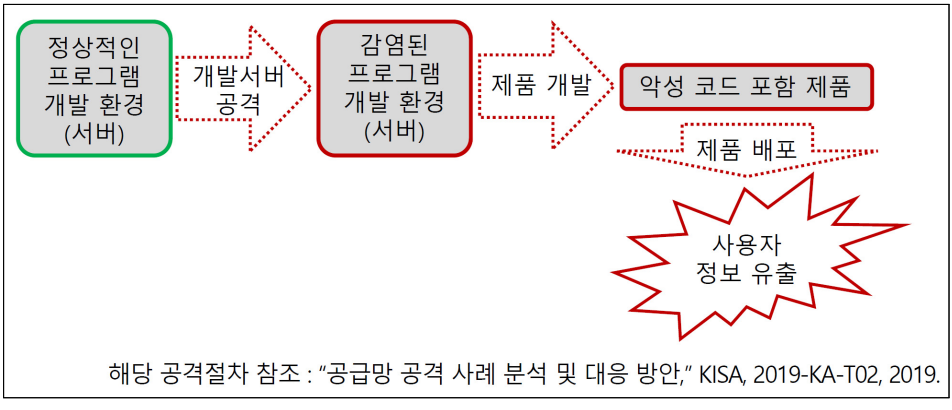
MEDoc 업데이트 서버 공격은 2017년 공격자가 우크라이나 기업이 개발한 회계 관리 소프트웨어인 MEdoc의 업데이트 서버에 침투하여 업데이트 요청 시 낫페트야(NotPetya) 랜섬웨어가 사용자에게 전달되도록 변조한 공격이다. 당시 피해자가 돈을 지불해도 파일을 복구하는 것이 불가능했기 때문에 이 사고를 통해 MEdoc을 사용하는 우크라이나와 유럽 기업들이 입은 경제적 피해는 대략 10조원 정도로 추정된다.

국내에도 넷사랑 서버 공격이나 SK커뮤니케이션즈 개인정보 유출 사건과 같은 비슷한 공급망 공격 사례가 있다.

넷사랑 프로그램은 전 세계 수백 개 기업이 사용하는 윈도우 서버 관리 소프트웨어로 넷사랑 서버 공격은 2017년 7월 공격자가 넷사랑 서버 관리 소프트웨어 패키지에 일명 셰도우패드(ShadowPad)라 불리는 백도어를 삽입해 배포한 공격이다. 공격자는 〔그림 2－48〕

과 같이 개발 서버의 원격 관리 도구(팀 뷰어) 계정을 탈취하여 서버에 침투한 후, 링커 프로그램으로 위장한 악성 코드를 통해 셰도우패드 백도어를 삽입하였다. 넷사랑 사용자들은 변조된 파일을 통해 악성 코드에 감염이 되었으며 이를 통해 공격자는 사용자 정보를 C&C(Command and Control) 서버를 통해 수집할 수 있었으며 숨겨진 백도어를 통해 언제든지 사용자 시스템에 접근할 수 있었던 것으로 보인다. 이 공격은 비정상 도메인에 접속한 것을 발견한 해외 보안 업체인 카스퍼스키사에 의해 발견되었다.

〔그림 2－48〕 넷사랑 서버 공격 절차



자료: 김대원, 강동욱, 최용제, 이상수, 최병철, "공급망 보안기술 동향", Electronics and Telecommunications Trends, vol. 35, no. 4, pp. 149-157, Aug. 2020.

SK커뮤니케이션즈 개인정보 유출 사건은 2011년 7월 SK커뮤니케이션즈가 운영하는 네이트와 싸이월드 회원 약 3,500만 명의 개인정보가 유출된 사건이다. 공격자는 SK커뮤니케이션즈 사내 특정 업데이트 서버를 해킹하는데 성공한 후 정상 업데이트 파일을 악성파일로 바꿔 보내는 방법으로 사내망에 있는 PC들을 감염시켰다. 그 후 공격자는 악성코드에 감염된 PC들을 통해 개인정보가 보관된 데이터베이스 서버에 접근할 수 있는 정보를 일주일에 걸쳐 수집했으며 데이터베이스 접근에 성공해 3,500만 고객의 개인정보들(아이디, 비밀번호, 이름, 주민등록번호, 전화번호, 주소 등)을 중국으로 유출하였다.

앞의 사례들은 주로 공급망 서버를 공격하는 방식이었지만 아래와 같이 실제로는 공급망의 모든 과정이 공격의 대상이 될 수 있어 공급망의 모든 단계에서 주의가 필요하다.

1) 실제 아마존에서 판매되었던 일부 저가 안드로이드 스마트폰에 설치된 악성 펌웨어로 인하여 72시간 간격으로 문자 메시지, 위치 정보, 통화 기록 등의 개인 정보를 중국에 있는 서버에 전송하도록 한 공격 사례

2) 미국 특정 업체의 네트워크 스위치 생산과정에 삽입된 플래시 카드로 인하여 시스템이 손상되고 해당 장비에 의해 악성코드가 확산된 공격 사례

3) 제품 생산 후 배송 단계에서 악성코드가 설치된 공격 사례

또한 공격의 범위는 각 제품을 구성하는 하드웨어 부품으로까지 확대할 수 있다. 2018년 10월 블룸버그는 서버 제조업체 슈퍼마이크로사가 애플과 아마존에 공급한 서버에 스파이 칩이 내장되어 있다고 보도하였다. 슈퍼마이크로사는 즉각 보도 내용을 부인하였으며 제3자 기관에 의뢰해 진행한 검증에서도 관련 증거는 찾지 못했다. 실제 스파이 칩이 내장되어 있는지 여부는 알 수 없지만 이러한 공격이 가능하고 위험한 것은 사실이다. 2019년 10월 Wired지에 게재된 내용에 따르면 인터넷을 통해 쉽게 구매 가능한 소형 프로세서에 악성코드를 탑재하여 시스코 방화벽 장비의 인증 체계를 쉽게 우회할 수 있음이 드러나기도 하였고, 이러한 방식으로 공격할 경우 기존 소프트웨어 방식의 탐지 기술로는 찾는 것이 거의 불가능한 것으로 알려져 있다.

2. 기술 개발 현황

가. 사이버 위협 인텔리전스

여기서는 사이버 위협 인텔리전스 공유를 위해 만들어진 다양한 조직들을 통하여 인텔리전스 공유 현황을 살펴보겠다.

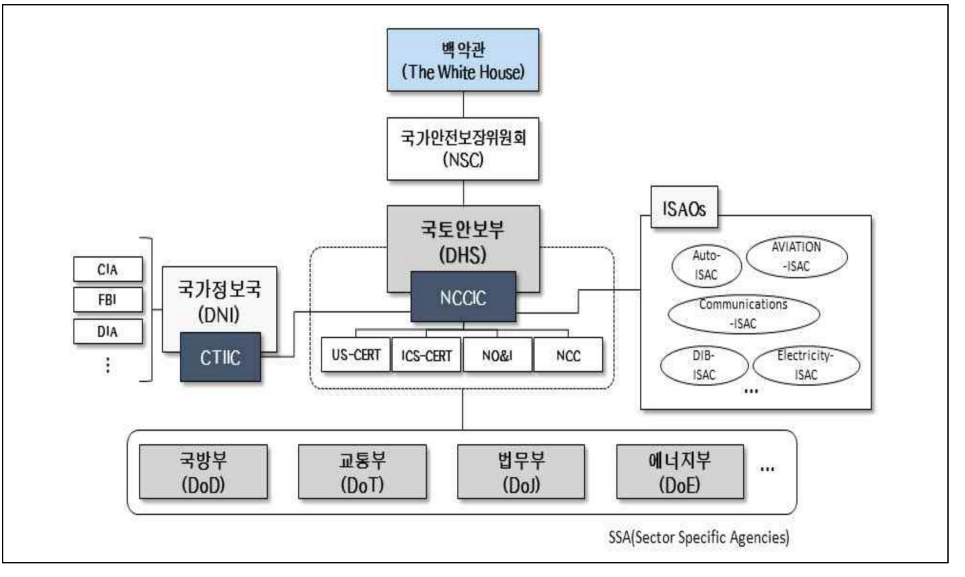
1) CTIIC(Cyber Threat Intelligence Integration Center)

미국 국가정보국(DNI) 산하 기구로 설립되어 사이버 사령탑 역할을 수행하며 미국의 국익에 영향을 미치는 외국의 사이버 위협과 사이버 사고와 관련된 통합된 모든 출처의 인텔리전스 분석을 제공하는 것이 목적이다.

미국의 사이버 위협 정보공유 체계는 〔그림 2-49〕와 같이 국토안보부(DHS)와 국가정보국 중심으로 국토안보부는 연방사이버안보통신통합센터(NCCIC, National Cybersecurity &

Communications Integration Center)를 설치하여 주요 정부기관과 민간 업체를 대상으로 사이버 위협 정보를 공유하는 창구 역할을 수행하도록 하고 있고, 국가정보국은 정보기관을 중심으로 국가안보에 영향을 미칠 수 있는 국내외 사이버위협 정보를 수집하고 공유함으로써 공공 기관과 민간 업체의 효과적인 대응을 지원하고 있다. 국가정보국에 소속된 모든 부처와 기관은 미국의 국익에 영향을 줄 수 있는 사이버 위협 및 사고와 관련된 모든 정보를 CTIIC와 공유하도록 되어 있으며, CTIIC는 NCCIC, 미 사이버사령부(USCYBERCOM, U.S. Cyber Command) 등 다양한 기관들과 협력관계를 유지하며 사이버 위협 관련 정보업무를 지원하고 있다.

〔그림 2－49〕 미국의 사이버 위협 정보공유 체계



자료: 윤오준, 조창섭, 박정근, 배선하, 신용태, “주요국의 사이버위협정보 공유체계 분석을 통한 국내 적용모델 연구”, 융합보안 논문지, vol. 16, no. 7, pp. 101-111, 2016.

2) CTA(Cyber Threat Alliance)

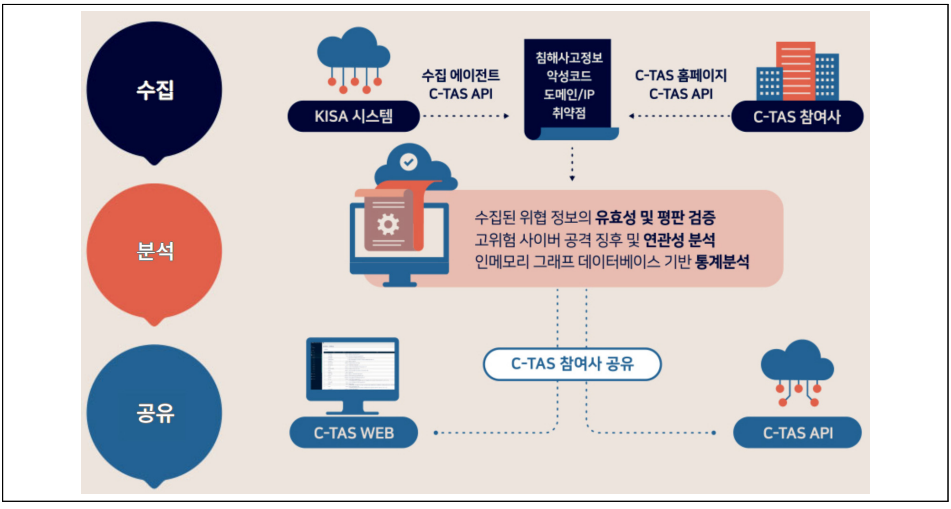
마이크로소프트, 맥아피, 팔로알토 네트웍스, 시만텍, 포티넷 등 세계 주요 보안 기업들이 모여 위협정보를 공유하기 위해 설립한 비영리 국제단체로 회원사가 매일 의무적으로 제출하는 위협정보를 클라우드 플랫폼을 통해 취합·분석하여 공유함으로써 사이버공격

공동대응 수준을 높이는 것을 목적으로 설립되었다.

3) C-TAS(Cyber Threat Analysis & Sharing)

사이버 위협 정보 분석, 공유 시스템으로 한국인터넷진흥원(KISA)에서 주관하고 있으며 2014년 8월 사이버 침해사고의 신속한 대응을 위한 '국가 사이버안보 종합 대책'에 따라 구축되었다. C-TAS는 〔그림 2-50〕과 같이 수집, 분석, 공유 단계로 구성된다. 수집 단계에서는 KISA 내부 시스템과 C-TAS 참여 기관으로부터 침해사고 이전 또는 침해사고 이후 발생한 위협 및 사고정보 등을 수집하며 수집된 정보는 XML 기반의 자체 표준양식인 CTEX(Cyber Threat EXpression) 형태로 저장한다. 분석 단계에서는 수집된 사이버 보안 데이터의 유효성 및 평판을 검증하고 연관성 분석, 통계 분석을 통해 사이버 보안 데이터를 분석하며, 공유 단계에서는 C-TAS Web과 API를 통해 사이버 위협 인텔리전스를 신속하게 참여 기관에 전달한다.

〔그림 2-50〕 C-TAS 시스템

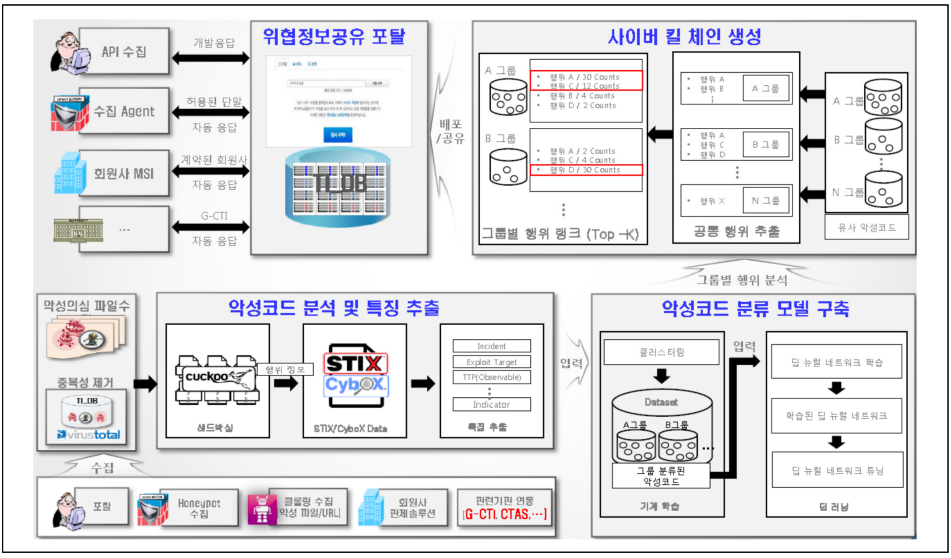


자료: 사이버 위협정보 분석공유(C-TAS) 시스템, https://www.krcert.or.kr/webprotect/ctas.do.

4) 코사인(KOSIGN, Korea Open Security Intelligence Global Networks)

〔그림 2-51〕과 같이 사이버 위협 정보 국제 표현 규격인 STIX에 기반하여 수많은 보안 장비에서 생성되는 보안 이벤트를 자동으로 수집·분석하고 이를 토대로 위협에 대한 대응 방안을 공유하기 위한 시스템이다.

〔그림 2-51〕 KOSIGN 시스템 개요



자료: 임원식, 윤명근, 조학수, "KOSIGN:정보보호제품 관점의 사이버위협정보 공유 체계", The Korea Institute of Information Security and Cryptology, vol. 28, no. 2, pp. 20-26, 2018.

나. 랜섬웨어 대응

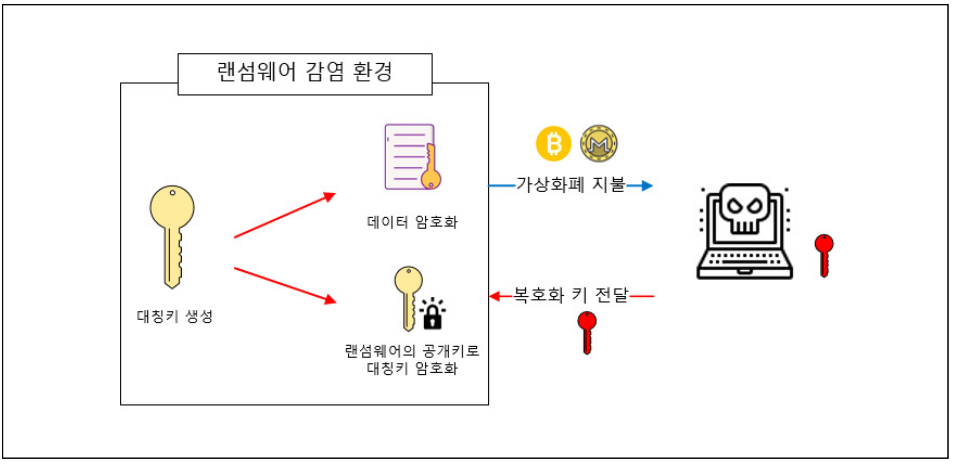
여기서는 랜섬웨어의 기술 발전 단계를 세대별로 나누어 살펴보도록 하겠다.

1) 랜섬웨어의 등장 - 1세대

최초의 랜섬웨어는 1989년 등장한 PC Cyborg Trojan(AIDS Trojan)이다. 이는 우편으로 디스켓 형태로 보내져서 실행될 경우 PC의 루트 디렉터리를 암호화하였으며, 복호화의 대가로 약 $189에서 $378를 요구하였다. 당시 배포 방식의 한계와 제한된 공격 대상 수로 인하여 큰 피해를 입히지 않았지만 많은 관심을 받게 되었다.

1세대 랜섬웨어는 락커(Locker) 계열과 크립토(Crypto) 계열로 나눌 수 있다. 락커 계열 랜섬웨어는 단순하게 로그인이나 장치에 대한 접근을 차단하여 사용자에게 잠금 해제에 필요한 코드를 받으려면 금액을 지불하라고 요구한다. 크립토 계열 랜섬웨어는 시스템 상의 데이터 및 정보을 암호화하여 사용자에게 복호화 키를 받으려면 금액을 지불하라고 요구한다. 〔그림 2-52〕는 크립토 계열의 1세대 랜섬웨어의 행위를 단순화하여 나타낸 것이다.

〔그림 2-52〕 랜섬웨어 단순 흐름도



자료: 문기운, 이종혁, "최신 랜섬웨어 동향 및 발전 방향", Electronics and Telecommunications Trends, vol. 32, no. 3, pp. 33-39, Jun. 2022.

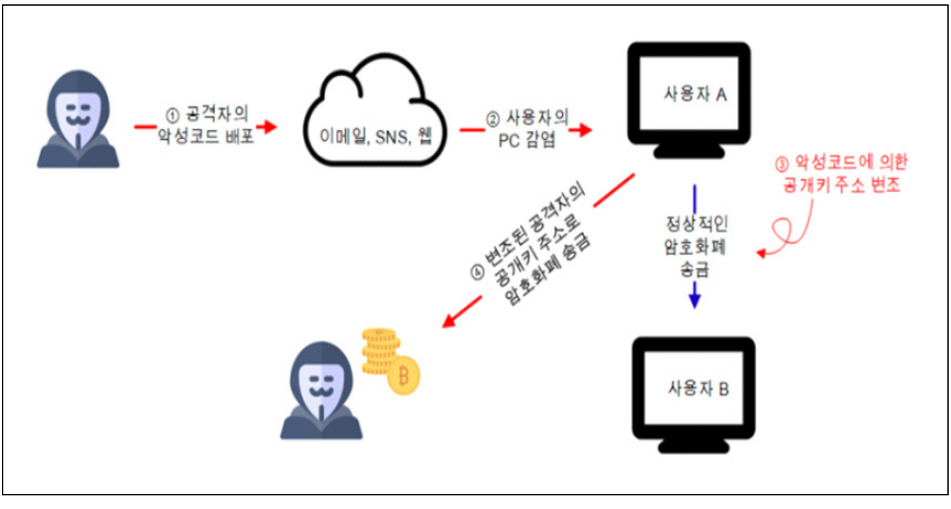
랜섬웨어의 행위를 단순화하여 살펴보면 다음과 같은 과정으로 수행된다. 우선적으로 랜섬웨어에 감염된 환경에서 랜섬웨어가 실행되면 정보 및 데이터 암호화에 사용할 대칭키를 생성한다. 암호화에 사용된 대칭키는 핸섬웨어의 자체에 존재하는 공개키로 암호화되어 은닉된다. 암호화 수행이 완료되면 바탕화면 변조나 랜섬노트를 생성하여 사용자에서 감염 사실을 알린다. 랜섬노트에는 지불해야할 가상화폐 금액과 공격자의 가상화폐 주소가 기록되어 있다. 공격자는 금액이 지불되면 사용자에게 복호화 키를 전달한다.

2) 이중 갈취 - 2세대

2세대 랜섬웨어는 이중 갈취를 목적으로 공격을 수행한다. 공격자들은 암호화 이전에 데이터를 먼저 확보한 후, 공격 대상의 데이터를 암호화한다. 암호화된 시스템을 인지한 사용자들이 요구 금액을 지불하지 않을 때, 공격자는 우선적으로 입수한 사용자의 데이터 및 정보를 다크웹이나 자신들이 운영하는 웹사이트에 공개하기 시작한다. 순차적으로 탈취한 정보를 공개함으로써 금액을 지불하도록 유도한다.

또 다른 방법으로 랜섬웨어 제작과 더불어 크립토재킹 악성코드를 제작하여 배포하는 경우도 있다. 크립토재킹 악성코드는 지갑 탈취형, 채굴형 악성코드로 나눌 수 있으며 〔그림 2-53〕은 지갑 탈취형 악성코드의 행위 예시를 나타낸다. 지갑 탈취형 악성코드는 피해자가 암호 화폐를 송금하기 위하여 수신자의 지갑 주소를 입력할 때, 해당 주소를 공격자 자신의 지갑 주소로 바꿔치기한다. 이때 공격자는 약 1만개의 지갑 주소를 악성코드에 심어 놓았으며, 피해자가 입력하는 송신자의 지갑 주소와 가장 유사한 것을 선택하여 바꿔치기한다. 결과적으로 피해자가 송금하는 암호 화폐는 공격자에게 전달된다.

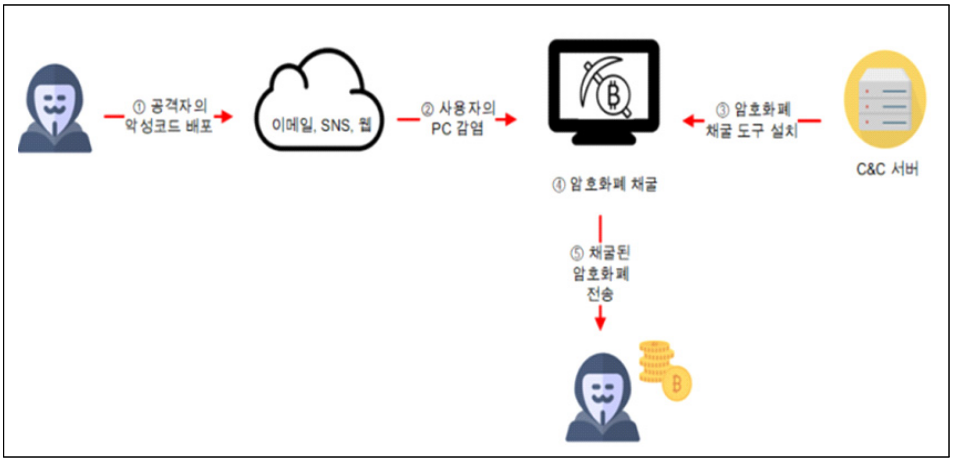
〔그림 2-53〕 지갑 탈취형 악성코드의 행위 예시



자료: 문기운, 이종혁, "최신 랜섬웨어 동향 및 발전 방향", Electronics and Telecommunications Trends, vol. 32, no. 3, pp. 33-39, Jun. 2022.

〔그림 2-54〕는 채굴형 악성코드의 행위 예시를 나타낸다. 채굴형 악성코드들은 랜섬웨어에 감염된 사용자의 환경에 가상화폐 채굴 도구를 설치한다. 감염된 환경에서 채굴된 가상화폐를 공격자 자신의 계좌로 전송하여 가상화폐를 획득한다. 공격자는 감염 환경의 컴퓨팅 자원을 사용하여 부가적인 수익을 얻을 수 있다.

〔그림 2-54〕 채굴형 악성코드의 행위 예시



자료: 문기운, 이종혁, "최신 랜섬웨어 동향 및 발전 방향", Electronics and Telecommunications Trends, vol. 32, no. 3, pp. 33-39, Jun. 2022.

3) 3중 협박 (RDDoS) - 3세대

앞서 살펴본 2세대 랜섬웨어들은 사용자의 데이터 및 정보를 암호화하고 볼모로 삼아 금전적인 요구를 하였다. 사용자들이 금전을 지불하지 않는다면 사전에 미리 유출한 정보들을 순차적으로 공개하며 협박하기도 하였다. 3세대 랜섬웨어는 3중 협박 형태로 랜섬디도스(RDDoS) 공격을 수행한다.

랜섬디도스(RDDoS)는 랜섬웨어 공격과 더불어 디도스(DDoS) 공격을 혼합한 형태를 말하며 특정한 서비스나 전제적인 네트워크를 디도스 공격을 수행하여 중단시키겠다고 협박한다. 디도스 공격을 먼저 수행하고 공격 중단을 위하여 금전을 요구하거나, 디도스 공격 이전에 희생자에게 먼저 연락하여 금전을 요구하는 방식을 사용한다. 보통은 개인보다는 기업을 대상으로 공격을 수행하며, 공격 받은 기업의 이메일이나 보안담당자에게 이메일

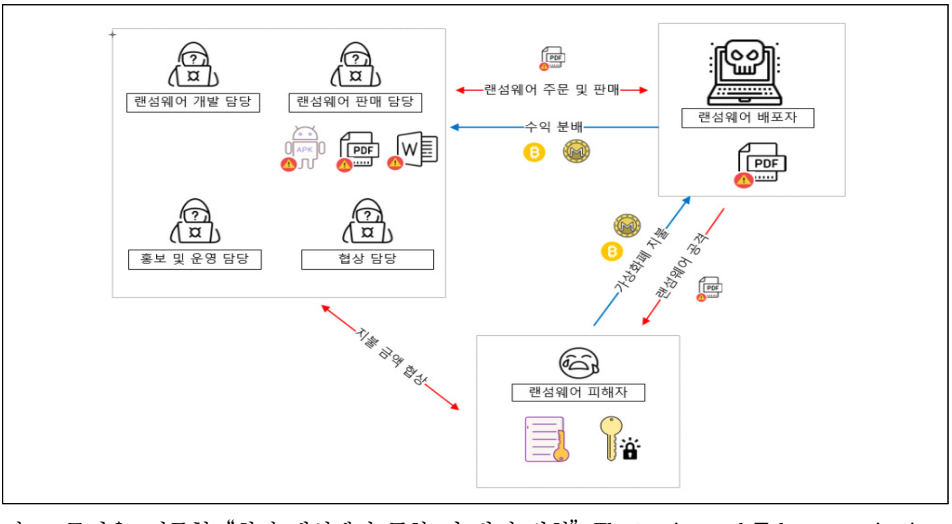
로 협박을 수행한다. 기업에서 대응하지 않거나 금전을 지불하지 않을 경우에는 실제로 작은 규모의 디도스 공격을 수행하기도 한다.

랜섬디도스 공격은 특정 분야에 국한되지 않고 공기업, 금융기관, 전자상거래 전문 기업과 같이 다수의 고객을 대상으로 서비스하는 기업들을 선정한다. 2020년 6월에는 대형 유럽 은행을 대상으로 809Mpps(Million Packets Per Second)에 달하는 공격이 수행되었으며, Armada Collective라는 해킹 그룹이 국내 금융사를 대상으로 공격을 수행하겠다고 협박 메일을 보낸 사례도 존재한다.

4) 서비스형 랜섬웨어 (RaaS) - 4세대

랜섬웨어 제작자들은 서비스형 랜섬웨어를 제작하여 판매하며 직접 공격을 수행하지 않고도 수익을 거둘 수 있다. 전문 지식이 없는 개인도 랜섬웨어 제작자로부터 배포 키트를 대여하거나 구매하여 랜섬웨어를 이용해 수익을 거둘 수 있다. 서비스형 랜섬웨어 제작자는 랜섬웨어 인프라 제작 및 구축, 지속적인 업데이트 및 지원 등을 제공하는 대가로 구매자에게 수익을 배분받는다. 〔그림 2-55〕는 서비스형 랜섬웨어 조직화의 예를 나타낸다.

〔그림 2-55〕 서비스형 랜섬웨어의 조직화의 예



자료: 문기운, 이종혁, “최신 랜섬웨어 동향 및 발전 방향”, Electronics and Telecommunications Trends, vol. 32, no. 3, pp. 33-39, Jun. 2022.

파이어아이는 해킹그룹 다크사이드의 랜섬웨어 운영에 대한 보고서를 발표하였다. 다크사이드는 2020년 8월부터 15개국 이상의 조직과 산업 전반을 대상으로 공격을 진행하였으며 희생자들의 데이터를 사전에 탈취한 뒤 랜섬웨어 공격을 수행한다. 또한 서비스형 랜섬웨어를 제작하여 판매하기도 하였다.

서비스형 랜섬웨어는 랜섬웨어를 제작하여 판매하는 조직과 실제로 랜섬웨어를 배포하는 배포자가 수익을 분배한다. 원활한 협상이 필요하다면 조직의 협상 전문가가 협상을 진행하기도 한다. 2020년 11월부터 RaaS 랜섬웨어 구매자를 모집하는 광고를 자신들의 블로그에 게시하였다. 광고 내용에 따르면, 구매자가 공격을 수행하여 50만 달러 미만의 랜섬웨어 몸값을 받는 데 성공할 경우에 수익의 25%를 랜섬웨어 제작자에게 분배하여야 한다. 또한 수익이 500만 달러가 넘는 경우에는 10%의 수익을 분배한다는 계약 조건이 명시되어 있었다. 이러한 명시된 조건에 해당하지 않는 작은 금액이라도 수익은 분배하고 있으며, 박리다매 형식으로 광범위하게 공격을 수행하여 큰 수익을 거둘 수 있다.

다. IoT 디바이스 보안

저전력 및 저비용으로 구현된 IoT 디바이스의 보안성을 높이기 위한 다양한 방법들이 연구되고 있다. 여기서는 하드웨어 보안 기술을 중심으로 보안성을 높이기 위한 방법을 살펴보도록 하겠다.

1) IoT 하드웨어 보안 기술 개념

하드웨어 보안 기술은 특별한 보안 서비스를 제공하기 위해 특정 시스템을 대상으로 하드웨어 모듈을 제작하는 경우와 범용 목적의 보안 하드웨어를 제작하는 경우로 구분할 수 있다. 구현 방법으로 나눌 경우 크게 FPGA(Field Programmable Gate Array) 형태나 ASIC(Application Specific Integrated Circuit) 형태로 구분할 수 있다.

FPGA는 프로그래밍을 통해 내부 논리를 변경할 수 있어 범용성을 가지지만 효율성은 다소 떨어진다. ASIC는 범용 용도로 변경이 불가능한 특정 용도를 위해 맞춤 제작된 집적회로이기 때문에 전력이나 성능 면에서 고효율 특성을 만족한다. 이러한 특성으로 인해 IoT 디바이스에 사용가능한 보안 모듈로 많이 활용된다.

또한 중앙 처리 장치(CPU), 메모리, 입출력 포트, 암호화 모듈 등을 하나의 칩으로 구현한 SoC(System on Chip) 기술이 발전하여 메모리가 칩 외부에 존재할 때 발생 가능한 물리적 탐침으로 인한 데이터 유출에 상대적으로 안전해졌고 TLS 보안칩과 같이 중요한 보안을 위해 하드웨어 보안이 활용된다.

2) PUF(Physically Unclonable Function)

PUF는 물리적 복제방지 기능을 제공함으로써 IoT 기기의 지문 역할을 하여 신뢰점(Root of Trust) 구성에 있어 핵심 기반 기술로 주목받는 기술이다. 일반적인 하드웨어 회로는 쉽게 복제가 가능하지만 PUF는 논리 수준으로 회로를 복제하더라도 제조 공정에서 발생하는 고유한 물리적 차이로 인해 다른 결과를 생성한다. 따라서 디바이스의 아날로그 특성에 의존하는 것이 일반적이다. PUF는 기본적으로 복제 불가능하므로 이러한 특성을 이용하여 비밀 키 생성, 디바이스 인증 등 다양한 보안 목적으로 활용 가능하다.

PUF에 대한 공격 기법으로는 전자기 공격(Electromagnetic Attack; EM Attack)과 모델링 공격(Modelling Attack), 차등 템플릿 공격(Differential Template Attack) 등이 있으며 이러한 공격에 대응하기 위한 기법으로 재구성 가능(Reconfigurable) PUF와 삭제 가능(Erasable PUF)가 있다.

3) TPM(Trusted Platform Module)

TPM은 신뢰 컴퓨팅(Trusted Computing)을 구현하기 위한 목적으로 만들어진 모듈로 다양한 보안 기능을 제공한다.

신뢰 컴퓨팅 그룹(Trusted Computing Group; TCG)에서는 신뢰 컴퓨팅을 위한 표준을 제안하였으며 이를 TCG 구조라 부른다. TCG 구조의 특징으로 저장 공간 보호, 암호화 기능 제공, 보호된 실행, 원격 검증 등이 있는데 TPM이 바로 이를 위한 TCG 구조의 기반의 되는 모듈이다.

TPM은 암/복호화를 위해 사용되는 키를 안전하게 생성하고 관리하는 기능을 제공하기 때문에 이를 통해 플랫폼의 무결성 검증 및 디스크 암호화 등 다양하게 활용 가능하며, IoT 디바이스에서도 키 관리 또는 무결성 검증을 위해 사용될 수 있다.

4) HSM(Hardware Security Module)

HSM은 암호 알고리즘 관련하여 다양한 기능을 갖춘 하드웨어 모듈이다. HSM은 키의 안전한 생성 및 관리, 암/복호화, 서명 및 검증, 해시 함수 계산 등을 빠르게 할 수 있는 하드웨어 가속 모듈을 가지고 있다. 이러한 하드웨어 모듈은 소프트웨어에 비해 연산이 빠르며 전력도 더욱 효율적으로 사용하기 때문에 IoT 디바이스 보안을 위해 다양하게 활용 가능하다.

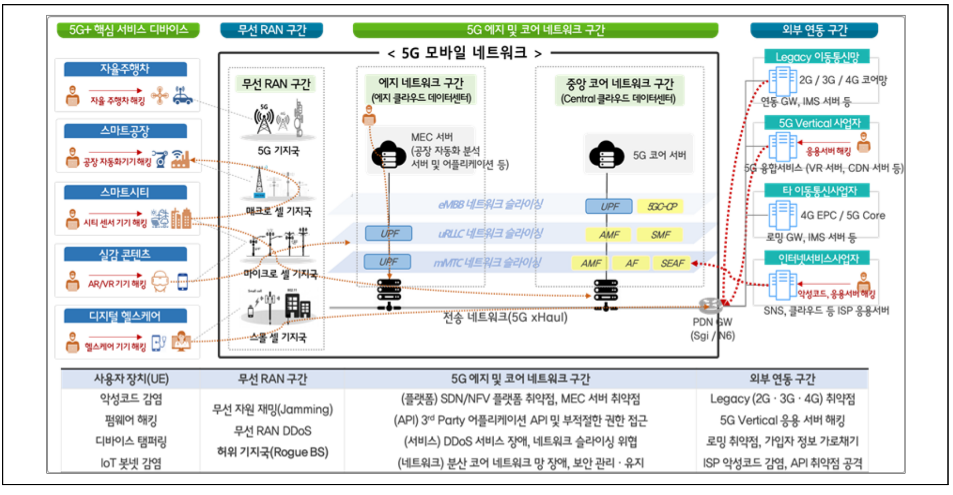
IoT 디바이스의 경우 센싱 디바이스 또는 게이트웨이 등 목적에 맞게 기능을 맞춘 다양한 HSM이 존재한다. 이러한 HSM은 IoT 환경에서의 키 관리 및 분배 문제 해결 또는 자원 효율적 실시간 암호 연산 등에 활용 가능하다.

라. 5G 보안

5G 이동통신 기술은 초고속, 초연결, 초저지연의 특성으로 4차 산업혁명을 이끌 핵심 기술 중 하나로 주목받고 있으나 다양한 기기들이 연결되는 초연결 네트워크로 복잡성이 증가하면서 해결해야 할 사이버 보안 문제 역시 많아질 것으로 보인다.

〔그림 2-56〕은 5G 모바일 네트워크를 중심으로 연결되는 구간별 보안 위협 개요를 나타낸 것이다. 일반적인 모바일 통신 경로는 사용자 장치(UE: User Equipment)에서 무선 라디오 액세스 네트워크(RAN : Radio Access Network)와 코어 네트워크(이동성 관리, 인증, 과금 등을 위한 모바일 네트워킹 기능)를 통해 외부 연동 구간(인터넷 서비스 사업자, 국가 간 로밍 연동 등)의 응용 서버와 연결된다.

〔그림 2－56〕 5G 모바일 네트워크에 따른 구간별 보안 위협 개요



자료: 김환국, 최보민, 고은혜, 박성민, “5G 네트워크 기술 진화에 따른 새로운 5G 보안 도전과제와 해외 보안 아키텍처 연구 동향”, The Korea Institute of Information Security and Cryptology, vol. 29, no. 5, pp. 7-20, 2019.

다음은 5G 모바일 네트워크의 특성에 따라 고려해야 하는 6가지 보안 이슈를 정리한 것이다.

1) IoT 기기 및 DDoS 공격 이슈

5G 네트워크에 연결 가능한 IoT 기기의 수가 폭발적으로 늘어나면서 보안이 취약한 IoT 기기들이 DDoS 공격에 사용되면서 5G 네트워크에 위협이 될 수 있다. 유럽 ENISA Threat Landscape Report 2018 보고서에 의하면 2016년 미라이 악성코드 이후 IoT 기기를 통한 DDoS 공격이 다양한 방법으로 이루어지고 있으며 공격의 규모와 세기는 역시 커지는 추세이다.

IoT 기기의 경우 기기 종류, 설치된 애플리케이션, 공급망 생태계가 다양하므로 공통된 아키텍처나 보안 표준을 설계하는 것이 쉽지 않다. 게다가 저사양 IoT 기기는 비용 문제로 고수준의 보안 기능을 탑재하기 힘들어 다양한 보안 위협에 노출될 수밖에 없는 상황이다.

공격자는 이러한 IoT 기기를 공격하여 IoT 봇넷을 구성하여 공격 수단으로 활용할 수 있다. 이를 통한 공격 대상으로 5G 네트워크 인프라, 5G 네트워크 인프라를 통해 연결된 인

터넷 서비스 서버, 5G에 연결된 단말기 등이 있으며 이를 통해 대규모 서비스 장애가 발생 가능한 상황이다.

2) 5G 무선 RAN 구간 보안 이슈

무선 RAN 구간은 사용자 기기와 기지국 간의 무선통신 구간과 다양한 기지국 장비로 구성된다.

이를 대상으로 한 첫 번째 보안 위협은 악성코드에 감염된 다수의 IoT 봇넷에 의한 DDoS 공격 및 무선 신호 채널을 대상으로 한 재밍(Jamming) 공격이다. 이를 통해 정상적인 데이터 수신을 방해하여 서비스 장애가 발생할 수 있다.

두 번째 보안 위협은 허위 기지국(Rogue Base Station) 이슈이다. 공격자는 허위 기지국을 이용하여 사용자 기기와 5G 네트워크 사이에서 중간자 공격을 통해 사용자 위치 정보 탈취, 정보 변조 등 다양한 공격 수행이 가능한 상황이다.

3) 분산 5G 코어 구조 보안 이슈

5G 네트워크가 이전과 비교해 크게 바뀐 부분 중 하나는 4G 코어 네트워크가 중앙 집중형 네트워크 구조로 중앙 국사로 트래픽이 집중되는 형태였음에 반해 5G가 되면서 코어 네트워크와 에지 네트워크로 나누어져 분산화되었다는 점이다. 제어 트래픽과 사용자 데이터 트래픽의 경로가 물리적으로 나누어져 제어 트래픽은 중앙 국사에서 주로 처리하고 사용자 데이터 트래픽은 지역 국사에 있는 에지 통신센터에서 주로 처리한다. 이러한 분산 구조는 초저지연 서비스 제공을 위해서는 효과적이나 보호해야 할 대상이 지역적으로 광범위하게 나누어지기 때문에 이로 인한 다양한 보안 이슈들이 있을 수 있다.

4) 가상화 및 네트워크 슬라이싱 보안 이슈

소프트웨어 기반 5G 네트워크 인프라는 통신 서버와 네트워크 장비 그리고 네트워크 슬라이싱 서비스를 가상화 기술을 통해 구현한다. 이를 통해 하나의 물리적 네트워크를 다수의 가상 네트워크로 나누어 응용 서비스별 독립적인 네트워크 슬라이싱 서비스를 제공할 수 있고 전용 장비 대신 범용 서버를 통해 네트워크 통신 기능을 구현할 수 있다. 하지만 이를 통해 물리적 하드웨어 자원에 대한 가용성 공격, 공유 자원의 허가 받지 않은 접

근 및 악성 코드 전파 등 다양한 공격이 가능해질 수 있다.

첫째, SDN(Software Defined Networing)/NFV(Network Function Virtualization) 등의 가상화 보안 이슈이다. SDN은 네트워크 장비의 제어 기능과 전송 기능을 분리하여 하나의 SDN 컨트롤러가 여러 네트워크 장치를 제어할 수 있도록 하는 기술로 SDN 컨트롤러와 네트워크 장비 간 제어 인터페이스 취약점을 악용하여 트래픽을 우회시키거나 DoS 공격을 통한 공격이 가능하다. 그리고 값비싼 전용 장비 대신 범용 서버를 사용해 구현 가능한 NFV 기술은 하이퍼바이저 커널 보안, 악성 가상머신 이전 문제, 가상화된 네트워크 기능 위에서 동작하는 응용 프로그램 사이의 신뢰 관계, 다시 말해 응용 프로그램의 변경 또는 인증과 네트워킹 기능에 대한 권한 부여 이슈가 중요하다.

둘째, 네트워크 슬라이싱 보안 이슈로 네트워크 슬라이스를 통해 하나의 물리적 네트워크를 다수의 가상 네트워크로 나누어 애플리케이션마다 할당하는 것이 가능하다. 하지만 나누어진 가상 네트워크들이 적절하게 격리되지 않으면 공격자가 하나의 슬라이스에서 다른 슬라이스로 공격을 수행하는 것이 가능할 수 있다.

5) 다중 액세스 에지 컴퓨팅(MEC) 보안 이슈

다중 액세스 에지 컴퓨팅(Multi access Edge Computing)은 사용자 단말과 가까운 곳에서 컴퓨팅을 수행하는 개념을 의미하며, 에지 네트워크에서 데이터를 바로 분석할 수 있어 초저지연 서비스 제공을 가능하게 하는 기술이다. 이와 관련한 주요 보안 위협으로 MEC에 저장된 사용자 또는 서비스 정보를 유출하거나 조작하는 공격, MEC 호스트의 자원을 비정상적으로 고갈시켜 같은 호스트에서 실행 중인 다른 서비스의 장애나 중단을 유발하는 공격, 조작 등 악성코드에 감염된 MEC 애플리케이션을 통해 다른 서비스의 장애를 유발하거나 민감한 정보를 유출하는 공격 등이 있다.

6) 서비스 기반 인터페이스(SBI) 보안 이슈

5G에서 모든 네트워크 기능은 HTTP로 이루어진 서비스 기반 인터페이스를 통해 이루어지며 내부 통신 기능과 서비스 기능을 서비스 제공자에게 개방함으로써 API 개방화가 가속화될 것으로 예상된다. 이를 통해 기존 웹 애플리케이션 서비스가 가진 보안 취약점을 그대로 악용하거나 API 개방에 따른 새로운 보안 이슈 발생 등의 문제가 생길 수 있다.

따라서 이미 잘 알려진 웹 어플리케이션 서비스의 취약점 관리 및 개방형 API에 대한 보안 통제가 중요할 보안 이슈가 될 것으로 보인다.

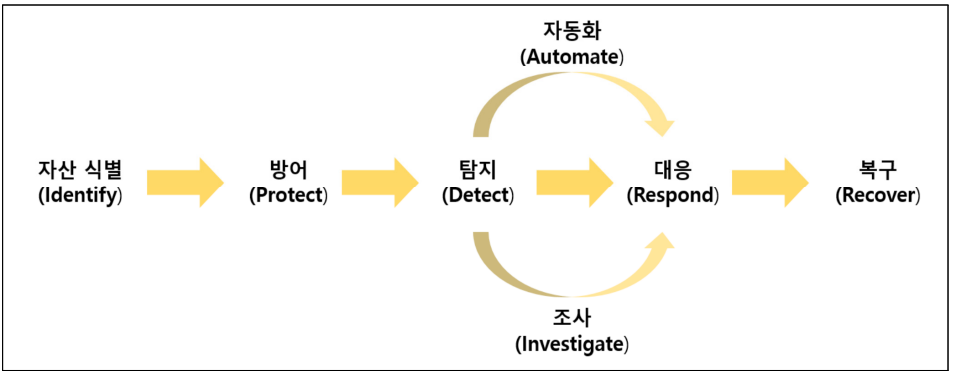
마. 클라우드 보안

여기서는 글로벌 클라우드 서비스인 아마존 AWS(Amazon Web Service), 마이크로소프트 Azure, 구글 GCP(Google Cloud Platform)의 보안 서비스를 살펴보도록 하겠다.

1) 아마존 AWS

아마존 AWS는 미국 국립표준기술연구소 NIST의 사이버 보안 프레임워크에 기반하여 〔그림 2-57〕과 같이 보안 서비스를 식별, 방어, 탐지, 대응, 복구 단계로 나눌 수 있다. 이 중에서 식별, 탐지, 대응 단계의 보안 서비스를 살펴보도록 하겠다.

〔그림 2-57〕 AWS 보안 서비스 워크플로우



자료: 주간기술동향 1977호, IITP - 클라우드 보안 기술 및 표준 동향

식별 단계의 서비스로서 AWS Config가 있으며 이는 AWS 리소스의 변경사항을 추적하고 감사하는 서비스이다. 통합 Account Dashboard를 통해 보안 규정을 위반하는 리소스나 규정 위반 건수 등의 모니터링이 가능하다. 그리고 AWS Config Rules를 통해 기준 정책 위배 시에 자동화된 차단 및 통지를 할 수 있다.

탐지 단계의 서비스에는 Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS

Security Hub 등이 있다. Amazon GuardDuty는 머신러닝 기반으로 AWS 계정 및 워크로드에 대한 이상 행위를 탐지할 수 있는 지능형 위협 탐지 및 통지 서비스이다. Amazon Inspector는 에이전트 기반의 보안 취약점 점검 서비스로 리눅스, 윈도우즈 서버를 대상으로 보안 진단 결과와 취약점에 대한 대응 가이드를 제공한다. Amazon Macie는 머신러닝 기반으로 AWS에 저장된 개인식별정보(Personally Identifiable Information)와 같은 민감 데이터를 식별하여 이 데이터가 유출되는 것을 차단하기 위한 서비스다. AWS Security Hub는 AWS 계정 전반에 걸쳐 빠른 대응이 필요한 보안 경고 및 규정 준수 여부를 전체적으로 확인할 수 있는 서비스이다.

대응 단계의 서비스에는 AWS CloudTrail, Amazon CloudWatch, Amazon Detective 등이 있다. AWS CloudTrail은 AWS API 요청 처리 내역을 로그를 통해 기록하는 서비스이다. 머신러닝을 통해 비정상적인 계정 활동 같은 의심스러운 API 요청 내역을 찾아낼 수 있다. Amazon CloudWatch는 AWS 리소스와 AWS에서 실행 중인 애플리케이션에 대한 모니터링 서비스이다. CPU, 메모리, 디스크 입출력, 네트워크 모니터링 데이터와 애플리케이션 로그를 수집・모니터링하고 경보를 설정할 수 있다. Amazon Detective는 보안 사고의 원인을 찾아내기 위한 서비스이다. 머신러닝과 시각화 기술을 바탕으로 잠재적인 보안 문제나 보안 침해가 의심되는 활동에 대한 원인 분석 및 조사가 가능하다.

2) 마이크로소프트 Azure

마이크로소프트 Azure의 주요 보안 서비스에는 Azure Monitor, Azure Sentinel, Azure Active Directory, Azure Security Center 등이 있다.

Azure Monitor는 인프라, 네트워크, 애플리케이션과 같은 Azure 클라우드 리소스에 대한 모니터링을 수행하는 서비스이다. 모니터링을 위해 가상머신 로그와 CPU, 메모리, 디스크 입출력 등의 정보를 수집하여 윈도우 및 리눅스 가상 머신의 성능과 상태를 분석한다.

Azure Sentinel은 SaaS 형태의 클라우드 네이티브 통합보안관제(SIEM) 서비스이다. 클라우드에 방화벽, 침입 탐지 시스템(IDS), 침입 방지 시스템(IPS), 웹 어플리케이션 방화벽(WAF) 등의 가상화된 보안 시스템을 구축한 후 로그를 수집한다. 보안 규칙 설정을 통해 위협 탐지 및 사고 대응이 가능하며 위협 헌팅(Threat hunting) 기능과 인공지능 분석이 가능하다.

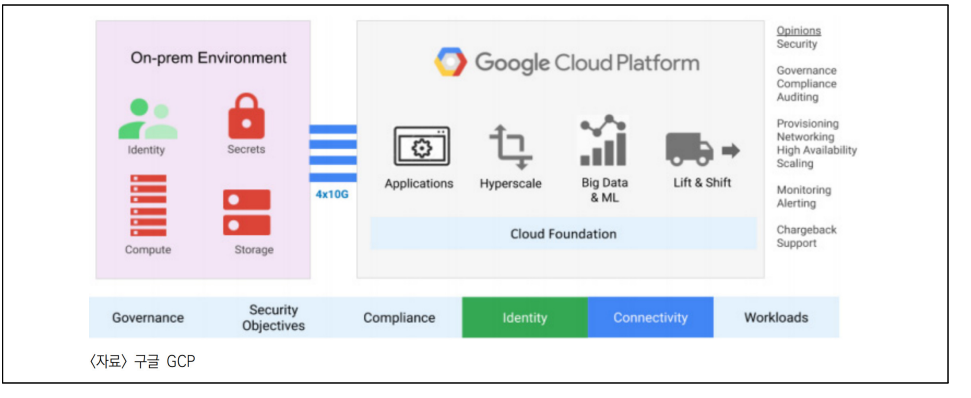
Azure Active Directory는 클라우드 기반 인증 및 계정 관리 서비스로 하나의 계정으로 여러 클라우드 애플리케이션에 로그인 가능한 싱글사인온(Single Sign-On)과 다단계 인증을 제공한다. 사용자 계정을 생성한 뒤 조직에 맞는 디렉토리를 생성하여 사용자별 권한을 생성할 수 있으며 ID 거버넌스를 통해 ID와 접근 수명 주기 관리가 가능하다.

Azure Security Center는 보안 정책 및 자동화를 통하여 Azure 클라우드 리소스에 대한 가시성을 제공하는 서비스이다. 대규모 환경에서 신속하게 위협을 식별하여 대응이 가능하며 조직 보안 정책 준수 관리도 가능하다.

3) 구글 GCP

GCP(Google Cloud Platform)는 〔그림 2-58〕과 같이 온프레미스(On-Premise) 환경과 연계된 보안 모델을 제공하며, GCP의 주요 보안 서비스에는 Cloud Identity and Access Management, Cloud Key Management Service, Cloud Asset Inventory, Security Command Center 등이 있다.

〔그림 2-58〕 GCP 보안 모델



자료: 주간기술동향 1977호, IITP - 클라우드 보안 기술 및 표준 동향

Cloud Identity and Access Management는 조직 전체를 대상으로 하는 보안 정책에 대한 통합적인 뷰를 제공하며 규정 준수 여부를 확인하기 위한 감사 기능을 제공한다. 그룹 및 역할을 바탕으로 사내 직무를 나누어 접근 권한을 부여하며 머신러닝 기반의 추천자 기능을 사용한다.

Cloud Key Management Service는 구글 클라우드에서 암호화 키 관리를 담당하는 서비스이다. 중요한 정보의 경우에는 하드웨어 보안 모듈(Hardware Security Module)을 사용할 수 있으며 EKM(External Key Manager)을 통한 외부 키 관리도 가능하다.

Cloud Asset Inventory는 프로젝트와 서비스 전반의 모든 자원을 가시화하여 모니터링하고 분석하는 기능을 제공한다. GCP 서비스, 쿠버네티스 리소스 및 RBAC 정책을 포함한 Anthos 배포 모니터링을 지원하며 언제든지 전체 인벤토리의 스냅샷을 내보낼 수 있을 뿐만 아니라 구성 변경에 대한 실시간 알람을 받는 것도 가능하다.

Security Command Center는 Google Cloud의 표준 보안 및 위험 데이터베이스로 조직 전체의 Google Cloud 보안 및 데이터 위험을 이해하고 개선하기 위한 지능적인 위험 대시보드이자 분석 시스템이다.

바. 공급망 보안

여기서는 공급망 보안 관련하여 최근 많은 주목을 받고 있는 하드웨어 기반 공격에 대한 대응 기술들을 살펴본다.

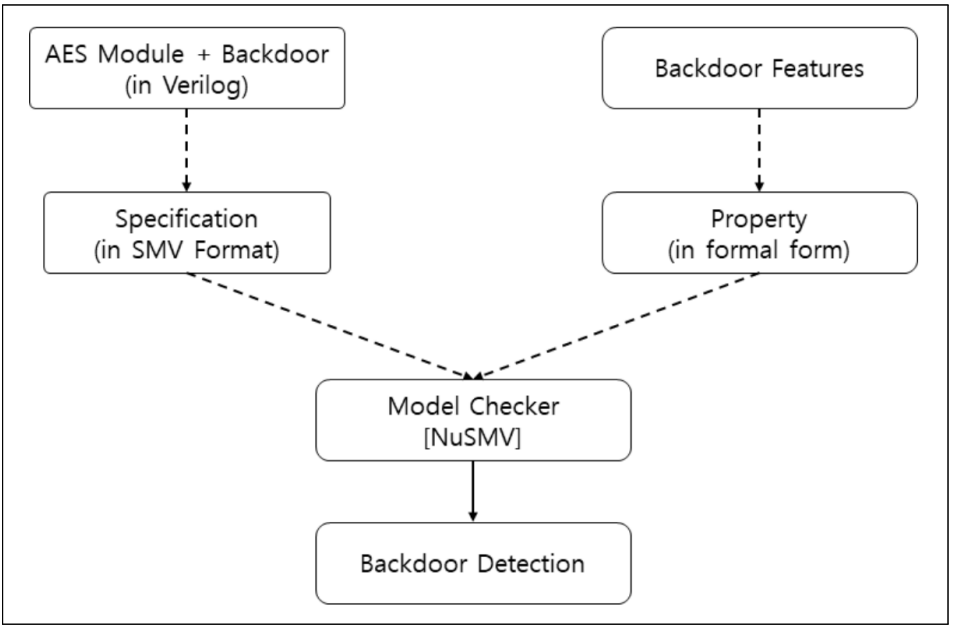
1) 국내 기술 개발 현황

아직까지 국내에서는 공급망 보안 관련하여 하드웨어 수준의 보안 취약점을 분석하는 기술의 구체적인 사례는 찾기 힘들다. 하지만 일부 개념 검증 수준의 취약점 탐지 기술과 공급망 공격에 대한 대응 체계를 다루는 연구가 존재한다.

고려대학교 김승주 교수 연구팀은 기존 하드웨어 AES(Advanced Encryption Standard) 모듈 백도어의 확장된 정의를 제안하고, 이를 통해 AES 비밀 키 외의 암호화 과정에서 생성되는 중간 결과 값이 유출되는 백도어를 탐지하는 기술을 제시하였다. 이를 위해 〔그림 2-59〕와 같이 Verilog HDL(Hardware Description Language)로 구현된 AES 모듈 코드를

정형 검증 도구인 NuSMV 모델 체커를 사용하여 분석하여 백도어 포함 여부를 확인하였다.

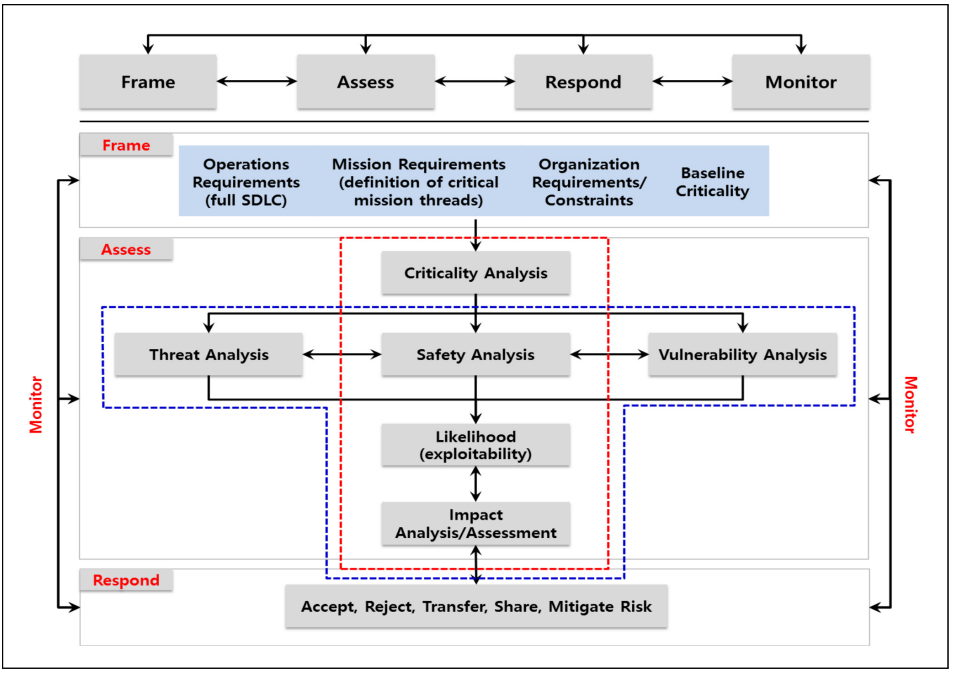
〔그림 2－59〕 AES 모듈 백도어 검출 절차



자료: 박재현, 김승주, “정형 기법을 이용한 하드웨어 AES 모듈 백도어 탐색 연구”, The Korea Institute of Information Security and Cryptology, vol. 29, no. 4, pp. 739-751, 2019.

고려대학교 최진영 교수 연구팀은 자동차 공급망에서 발생할 수 있는 위험을 식별, 평가 및 통제하기 위한 위험관리 방법을 제안하였다. 이를 위해 자동차 시스템에서 보호해야 할 자산과 발생할 수 있는 보안 위협을 분석하였고 이를 참고하여 〔그림 2－60〕의 자동차 공급망 위험관리 프로세스 모델을 제안하였다.

〔그림 2－60〕 자동차 공급망 위험관리 프로세스



자료: 김동원, 한근희, 전인석, 최진영, “자동차 공급망 위험관리(A-SCRM) 방안 연구”, The Korea Institute of Information Security and Cryptology, vol. 25, no. 4, pp. 793-805, 2015.

제안 모델은 기준 정의 단계(Frame), 평가 단계(Assess), 실행 단계(Respond), 모니터링 단계(Monitor)로 구성된다. 기준 정의 단계는 다른 3계층(평가 단계, 실행 단계, 모니터링 단계)에 대한 문맥을 설정하는 단계이다. 평가 단계는 수집된 모든 데이터를 활용하여 위험 평가를 수행하는 단계이며, 실행 단계에서는 안전 경로와 보안 경로에서 분석한 결과를 통해 도출된 위험을 통제하기 위한 수단을 결정한다. 최종 모니터링 단계에서는 실행 중인 위험관리 방안을 보완하면서 위험 수준을 수용 가능한 범위 내로 유지되도록 돕는다.

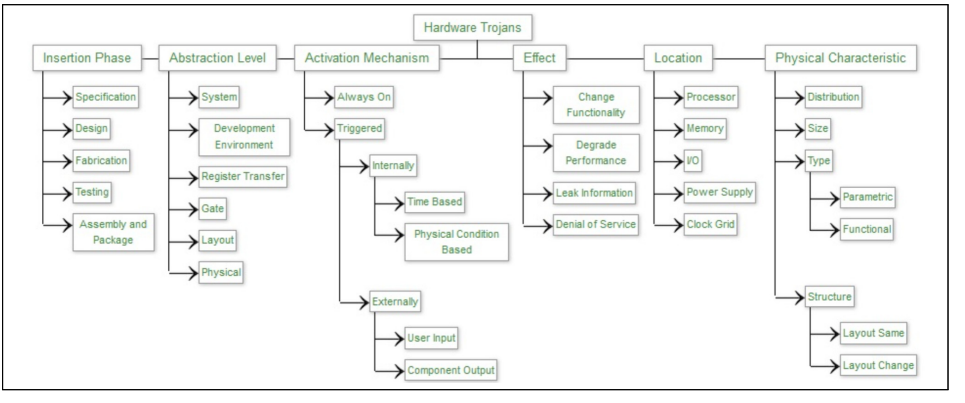
2) 해외 기술 개발 현황

해외에서도 하드웨어 기반 공급망 공격에 대한 심각성을 인지하고 있으며 관련 사례 및 기술 자료를 공개하거나 자동화된 탐지 기술 관련하여 다양한 선행 연구가 진행 중이다.

미국의 Trust-Hub는 하드웨어 보안 및 신뢰 관련 정보를 공유하기 위한 웹 기반 플랫폼

으로 하드웨어 기반 백도어와 부채널 공격 사례 튜토리얼과 함께 하드웨어 취약점 분석 및 공격 관련 논문과 같은 다양한 자료를 제공한다. 〔그림 2-61〕에서와 같이 공개된 분류 체계는 삽입 단계(Insertion Phase), 추상화 수준(Abstraction Level), 활성화 메커니즘(Activation Mechanism), 영향(Effect), 삽입 위치(Location), 물리적 특성(Physical Characteristic)에 따라 분류된다.

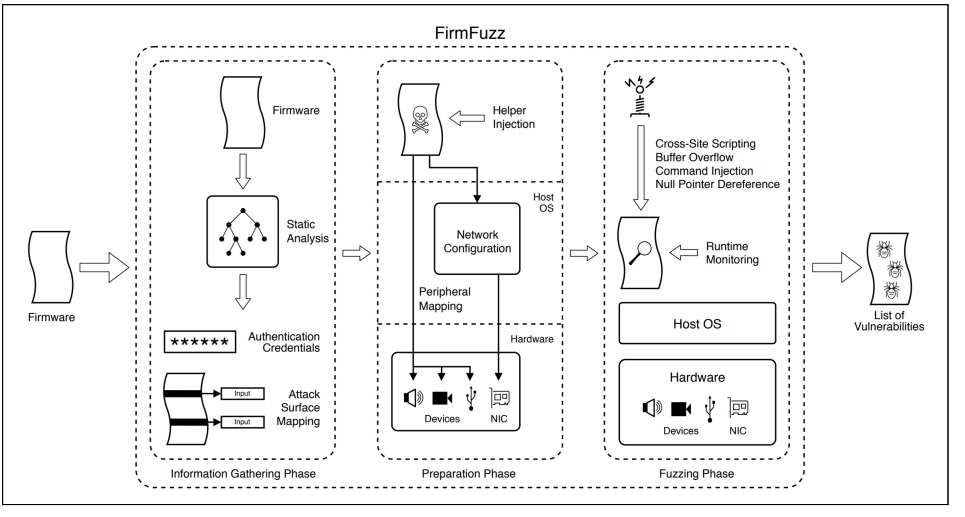
〔그림 2-61〕 Trust-Hub 분류 체계



자료: 서준범, 김동규, "Trust-HUB 기반 하드웨어 백도어의 구현가능성 분석", 2020년도 대한전자공학회 하계종합학술대회 논문집, pp. 583-585, 2015.

퍼듀대학의 Prashast Srivastava 등은 리눅스 기반 펌웨어 이미지에 대한 자동화된 장치 독립적 에뮬레이션 및 동적 분석 프레임워크인 FirmFuzz를 제안하였다. FirmFuzz는 〔그림 2-62〕에서와 같이 정보 수집(Information Gathering), 분석 준비(Preparation), 퍼징(Fuzzing)의 세 단계로 구성된다. 정보 수집 단계는 정적 분석을 통해 퍼징 과정의 적용 범위를 늘리기 위한 정보를 수집하고 분석 준비 단계는 에뮬레이션을 위한 펌웨어 이미지를 만든다. FirmFuzz는 27개 장치의 32개 펌웨어 이미지를 에뮬레이션하고 동적으로 분석하여 6개의 다른 장치(2개의 IP 카메라와 4개의 라우터)에서 7개의 지금까지 알려지지 않았던 취약점을 발견하였다.

〔그림 2－62〕 FirmFuzz 작업 흐름



자료: Prashast Srivastava, Hui Peng, Jiahao Li, Hamed Okhravi, Howard Shrobe, and Mathias Payer, "FirmFuzz: Automated IoT Firmware Introspection and Analysis", In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things (IoT S&P'19). ACM, New York, NY, USA, pp. 15-21, 2019.

3. 기술 발전 방향

가. 사이버 위협 인텔리전스

사이버 위협 인텔리전스 공유를 위하여 STIX나 TAXII 같이 표현 및 전송 프로토콜을 표준화하고 공유 시스템을 구축하면 공격 대응에 있어 다양한 이점이 생기는 것은 명확하다. 하지만 사이버 위협 인텔리전스 공유에 있어 다음과 같은 문제가 발생할 수 있어 해결을 위한 고민이 필요한 상황이다.

1) 무임승차 문제

여러 기관이 정보를 공유하는데 있어 생길 수 있는 문제 중 하나는 참가자 중 일부가 무임승차와 같이 다른 사람이 제공한 정보는 사용하되 자신은 정보를 제공하지 않으려 하는 것이다. 이 같은 참가자가 많아지면 공유되는 정보의 품질이 점점 나빠져 장기적으로 공유를 지속하기 힘든 상황에 이르게 된다.

무임승차 문제의 해결 방안으로 공유되는 정보의 품질을 계량화하여 참가자의 기여도를 평가하는 방법이 있다. KOSIGN의 경우 이를 위해 정확성(Correctness), 관련성(Relevance), 효용성(Utility), 유일성(Uniquiness)의 4가지 기준을 통해 공유 정보의 품질을 계량화하여 기여도를 계산한다.

2) 개인정보 또는 민감 정보 공유 가능성

사이버 위협 인텔리전스 공유에 있어 누군가의 실수로 개인정보 또는 관리되지 않은 민감 정보를 포함하여 정보를 공유하는 경우가 있을 수도 있다. 이 경우 공유 정보 제공자는 정보통신망법과 개인정보보호법으로 법적 처벌을 받을 수도 있으며 상당한 금전적 손실도 각오해야 하는 상황이다. 이러한 위험은 참가자들이 사이버 위협 인텔리전스 공유에 적극적으로 참여하기 어렵게 만든다.

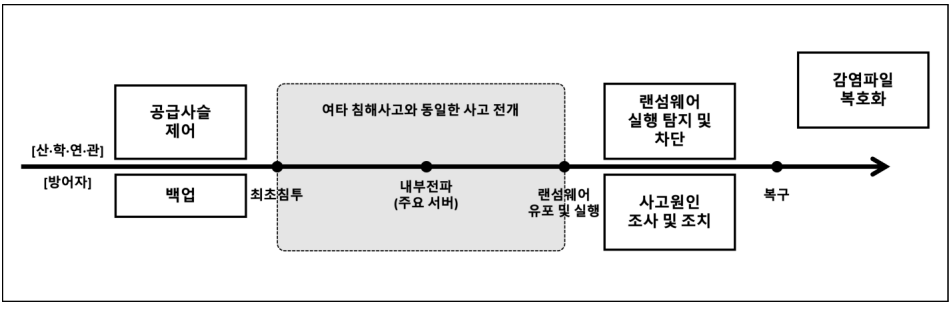
3) 사이버 위협 인텔리전스 구조 변경 가능성

사이버 위협은 지속적으로 변화, 발전하고 있으므로 공유해야 할 사이버 위협 인텔리전스의 구조 또한 시간이 지나면서 바뀔 수 있다. 이미 만들어진 공유 체계를 바뀐 구조에 맞게 수정하기 위해서는 막대한 비용이 소요될 수도 있다. 따라서 사이버 위협 인텔리전스의 구조가 바뀌더라도 유연하게 대응할 수 있는 공유 체계를 설계하기 위한 방법론에 대한 연구가 필요하다.

나. 랜섬웨어 대응

과거의 랜섬웨어가 주로 불특정 다수를 대상으로 스피어피싱 이메일과 같은 단순한 방법으로 공격을 수행했다면 최근에는 특정 기관이나 기업을 노린 APT 공격 형태의 표적형 공격이 많아지고 있다. 여기서는 랜섬웨어에 대응하기 위한 기술을 〔그림 2-63〕과 같이 분류하였다.

〔그림 2－63〕 랜섬웨어 공격 타임라인별 대응 분류



자료: 이슬기, 김동욱, 이태우, “랜섬웨어 피해 저감을 위한 공격 타임라인별 대응전략 및 기술”, The Korea Institute of Information Security and Cryptology, vol. 32, no. 3, pp. 27-31, 2022.

1) 랜섬웨어 피해 최소화

랜섬웨어에 의한 피해를 최소화하기 위한 방법에는 제로트러스트 개념의 도입과 복구를 위한 백업 서버 구축 등이 있다. 제로트러스트는 접근하는 단말기가 무엇이든 상관없이 사용자 및 단말을 신뢰하지 않는다는 개념에서 출발하며, 매번 정상 사용자 기기를 식별하고, 안전한지 컨텍스트를 확인하는 절차를 거친다. 다양한 조직 및 기업에서 기존 보안 환경에 제로트러스트 개념을 도입하기 위해 노력하고 있다. 그리고 약간의 비용 부담이 있기는 하지만 백업 서버를 구축해 놓는 것도 랜섬웨어로 의한 피해를 줄이는 방법이 될 수 있다.

2) 랜섬웨어 유포 인프라 제어

랜섬웨어를 유포하는 인프라를 차단하는 방법으로 랜섬웨어 공격을 잠시 중단시킬 수도 있다. 랜섬웨어의 공격 행동 패턴을 분석하여 공개하면 공격자도 유포를 위한 새로운 인프라를 찾아야 하고 공격 기법도 수정해야 하므로 공격자에게도 부담이 된다.

3) 클라이언트에서의 탐지 및 차단

공격의 대상이 되는 클라이언트에서 랜섬웨어를 탐지 및 차단하는 기술은 일반적인 악성코드를 탐지 및 차단하는 기술과 큰 차이가 없다. 탐지 방법에는 오용 탐지(Misuse

Detection)와 이상 탐지(Anomaly Detection)가 있는데 오탐률(False Positive)이 높지만 제로데이 공격(Zero-day Attack)에도 대응할 수 있는 이상 탐지와 관련한 연구가 활발히 이루어지고 있다.

4) 랜섬웨어 복구 도구 제작

랜섬웨어에 감염된 경우 이론상으로는 복호화가 불가능에 가깝지만 몇몇 랜섬웨어의 경우 설계 또는 구현의 문제로 복호화가 가능한 경우가 일부 있었다. 하지만 최근 들어 랜섬웨어의 완성도가 높아지면서 복호화 가능성이 점점 더 줄어들고 있어 이에 대한 대응이 필요하다.

5) 사후 대응

랜섬웨어에 감염되어 복구를 완료한 후에는 백도어 존재 여부 확인과 최초 침투 방법 확인 및 대응이 반드시 이루어져야 한다. 그렇지 않을 경우 재공격의 원인이 될 수 있다.

다. IoT 디바이스 보안

다음은 IoT 디바이스 보안 관련하여 앞으로 해결해야 할 문제들을 나열한 것이다.

1) 자원 제약

많은 IoT 디바이스가 다음과 같은 이유로 적절한 보안을 제공하지 못하고 있다.

- 보안을 위한 컴퓨팅 능력 부족
- IoT 디바이스의 미흡한 접근 제어
- 펌웨어 보안 분석을 위한 예산 부족
- 부족한 예산 또는 디바이스의 기술적 한계로 인한 업데이트 미비
- 물리적 공격에 대한 취약한 보호

이러한 환경에서 어떻게 하면 효율적으로 적절한 보안을 제공할 수 있을지에 대한 연구가 필요하다.

2) 안전하지 않은 통신

안전한 통신을 위해 만들어진 기존 보안 기법은 대부분 데스크톱 컴퓨터를 대상으로 설계되었으며 제한된 컴퓨팅 능력을 가진 IoT 디바이스에는 적용이 힘든 경우가 많다. 따라서 IoT 디바이스와 같이 제한된 컴퓨팅 능력을 가진 경우에도 사용 가능한 새로운 보안 기법에 대한 연구가 필요하다.

3) 악성코드

앞에서 살펴본 미라이 봇의 경우처럼 많은 경우 IoT 디바이스는 악성코드에 취약하다. 이는 특히 IoT 디바이스의 패스워드가 'admin'이나 '0000' 같이 기본 설정에서 한 번도 바뀌지 않은 경우 더욱 그렇다. 한 예로 Go 프로그래밍 언어로 작성된 악성코드인 BotenaGo의 경우 여러 라우터 및 IoT 디바이스에 대한 악용할 수 있는 취약점이 30가지가 넘는다. 이러한 IoT 디바이스 대상 악성코드에 효과적으로 대응하기 위한 연구가 필요하다.

4) 사이버 공격

앞에서 설명한 경우 외에도 IoT 디바이스는 다양한 사이버 공격의 대상이 될 수 있다. IoT 디바이스에 대한 일반적인 공격 유형은 아래와 같다.

서비스 거부(Denial of Service; DoS) 공격: IoT 디바이스는 처리 능력이 제한되어 있어 서비스 거부 공격에 취약하다.

수면 거부(Denial of SLeep; DoSL) 공격: IoT 디바이스는 배터리 절약을 위해 절전 모드로 동작하는 경우가 많은데 이를 강제로 깨워 배터리를 빠르게 소모시키는 공격이다.

디바이스 스푸핑: IoT 디바이스의 인증 기능이 부적절하게 구현된 경우 스푸핑 공격이 가능하다.

물리적 침입: 대부분의 공격은 원격에서 수행되지만 IoT 디바이스의 경우 물리적 침입 역시 고려할 필요가 있다.

애플리케이션 기반 공격: IoT 디바이스의 펌웨어 또는 소프트웨어에 취약점이 있거나 클라우드 서버 또는 백엔드 애플리케이션에 취약점이 있는 경우 애플리케이션 기반 공격이 가능하다.

라. 5G 보안

5G 코어 네트워크에 대한 주요 보안 기능은 어느 정도 정의가 마무리되어 5G 코어 네트워크에 대해서는 새로 발견되는 보안 이슈에 대해서만 수정이 논의되는 것으로 보인다. 5G 보안 관련하여 현재 활발하게 논의 중인 분야는 신규 서비스와 관련된 부분으로 네트워크 슬라이싱, 엣지 컴퓨팅, 모바일 IoT 등이 있다.

아래는 5G 서비스 운영 단계에서 보안을 위해 고려해야 할 사항이다.

1) 분산 DDoS 공격 대응

미라이 봇넷과 같이 대량의 IoT 기기로 인한 분산 DDoS 공격이 최근 이슈가 되고 있다. 이러한 공격에 빠르게 대응하는 방법으로 공격 시작 지점에 가까운 기지국 또는 에지 네트워크에 탐지 기능을 배치하는 방법이 있다.

2) 유연하고 확장성 있는 보안

5G 코어 네트워크는 유연하고 확장 가능한 구조를 위해 서비스 기반 구조를 채택하고 있다. 따라서 보안에 있어서도 서비스별로 서로 다른 보안 요구 사항을 만족시키기 위해 보안 기능의 구성을 유연하게 다르게 할 수 있어야 한다.

3) 자동화된 5G 보안 관제

점점 더 많아지고 정교해지는 사이버 공격에 대응하기 위해서는 5G 보안 관제 역시 자동화가 필요하다.

4) 제로 트러스트 보안 모델 적용

제로 트러스트 보안 모델은 기존 도메인의 경계를 기준으로 보안모델을 설계하던 방식에서 내・외부 가리지 않고 접근을 허용하기 전에 관련된 모든 것을 검증해야 한다는 신뢰기반의 보안 모델이다. 현재까지 알려진 다양한 보안 취약점 이슈들이 신뢰하는 요소로부터의 접근을 추가 검증 없이 허용함으로써 발생하였다. 따라서 모든 경우에 검증 후 접근을 허용하는 새로운 보안 모델이 필요하다.

마. 클라우드 보안

여기서는 클라우드 보안과 관련하여 최근 주목받고 있는 개념인 CSPM, CWPP, CASB에 대해 알아보도록 하겠다.

1) CSPM(Cloud Security Posture Management)

CSPM은 컴플라이언스 또는 기업 보안 정책에 따라 클라우드 인프라에서 발생 가능한 위험 요소를 지속적으로 탐지 및 제거하여 클라우드 내 공격 발생 가능성을 낮추는 솔루션이다. CSPM을 사용하면 자산을 효과적으로 가시화할 수 있으며 취약한 설정을 지속적으로 찾아내어 대응할 수 있어 보안 사고를 줄일 수 있을 것으로 기대된다.

2) CWPP(Cloud Workload Protection Platform)

CWPP는 서버 워크로드를 보호하기 위하여 개발된 새로운 범주의 솔루션이다. CWPP는 가상머신이나 컨테이너 같은 서버 워크로드에 대한 가시성을 지원하며 시스템 무결성 보장, 애플리케이션 제어, IPS, 안티멀웨어, 행위 모니터링 등의 기능을 통해 워크로드를 공격으로부터 보호하여 안정적인 클라우드 구성을 보장할 수 있도록 한다.

3) CASB(Cloud Access Security Broker)

CASB는 클라우드 서비스 사용자와 클라우드 서비스 공급자 중간에 위치하여 사용자가 클라우드 기반 자원에 접근할 때 기업 보안 정책을 반영하여 클라우드 이용에 있어 안전을 담보해 주는 중개자 기능을 제공한다. CASB를 통해 기업의 클라우드 사용에 있어 가시성을 제공하고 데이터를 보호하며 기업 보안 정책을 실현할 수 있다.

바. 공급망 보안

4차 산업혁명 시대를 맞이하여 공급망을 대상으로 한 사이버 공격은 지속적으로 증가하고 있으며 최근에는 하드웨어 장치로까지 공격 범위가 넓어지고 있다. 특히 하드웨어 제조과정에 백도어를 숨겨서 공격하는 방법은 탐지나 분석이 어렵고 해당 하드웨어를 제거하지 않는 한 문제를 근본적으로 해결할 수 없는 경우가 많다. 하지만 CPU 칩과 같이 몇몇 기능이 비교적 명확한 부품이 아니면 겉보기만으로 어떠한 부품인지 알 수가 없어 사람들이 위협 여부를 파악하기가 힘든 어려움이 있다.

향후 예상되는 공급망 대상의 하드웨어 기반 공격에 대응하기 위해서는 〔그림 2-64〕와 같은 하드웨어 보안 취약성 탐지를 위한 종합적인 분석 체계가 필요하며 이와 관련한 다양한 연구 개발이 이루어 질 것으로 판단된다.

〔그림 2-64〕 하드웨어 보안 취약성 탐지를 위한 종합적인 분석 체계

자료: 김대원, 강동욱, 최용제, 이상수, 최병철, “공급망 보안기술 동향”, Electronics and Telecommunications Trends, vol. 35, no. 4, pp. 149-157, Aug. 2020.

제3절 융합 보안

1. 개요 및 관련 기술

융합 보안은 물리 보안과 정보 보안의 융합을 의미한다. 여기에서 물리 보안은 시설이나 장비 등에 대한 비인가 접근을 막고 개인이나 자산을 파손이나 탈취 등의 물리적 위협으로부터 보호하는 것이다. 정보 보안은 사이버 보안을 의미하며 디지털 정보 및 자산을 디지털 공격으로부터 보호하는 것이다. 융합 보안은 사이버 세상과 물리 세상의 융합 형태 서비스들과 함께 등장하였고 이런 융합 서비스들이 발전함에 따라 그 필요성이 더욱 강조되고 있다. 이러한 서비스들에는 스마트 시티, 스마트·자율 주행 이동체, 디지털 헬스케어, 스마트 공장 및 산업제어 등이 포함된다.

본 절에서는 이런 융합 서비스들을 위한 보안 기술에 대해 살펴보도록 하겠다.

가. 스마트 시티 보안

스마트 시티는 스마트도시법 제2조에 "도시의 경쟁력과 삶의 질의 향상을 위하여 건설·정보통신기술 등을 융·복합하여 건설된 도시기반시설을 바탕으로 다양한 도시서비스를 제공하는 지속가능한 도시"라고 정의되어 있다. 즉, 정보통신기술이등 물리 세상을 구축하는 건설기술과 융합한 서비스이다. 스마트 시티는 하나의 특정 서비스가 아니라 매우 복잡하고 다양한 서비스들로 구성된다. 그리고 도시 곳곳의 센서에서 수집되는 디지털 정보를 모으고 스마트 시티 서비스와 연계하도록 도와주는 통합플랫폼(또는 스마트시티운영센터)이 존재한다.

스마트 시티에서 수집 가능한 정보에는 CCTV, 교통정보, 에너지 사용량, 대기 또는 수질 등의 환경 정보 등 매우 다양한 것들이 포함된다. 이러한 디지털 정보를 기반으로 기존 서비스의 향상 또는 새로운 서비스를 제공할 수 있다. 하지만, 이렇게 많은 데이터가 다양한 곳에서 수집되고 활용되기 때문에 그만큼 사이버 또는 물리적 위협의 가능성에 항상 노출되어 있다. 특히 통합플랫폼에 데이터가 집중되기 때문에 통합플랫폼이 공격당하면 스마트 시티 전체가 마비되거나 물리적 피해가 발생할 수 있다. 또한 도시 곳곳의 수많은 기기가 네트워크로 연결되어 있기 때문에 취약한 기기가 존재할 가능성도 상당히 높다.

즉 한 기기를 공격하고 그 기기를 통해 네트워크에 연결된 다른 기기나 중앙 관제 통합 플랫폼에 대한 공격이 가능할 수 있다.

〔그림 2－65〕 스마트 시티 통합 플랫폼 개념

자료: 국토교통부, “스마트시티 통합플랫폼 기반구축, 2020”

스마트 시티는 크게 사물 인터넷 기술, 클라우드 기술 등이 사용되기 때문에 해당 기술에 대한 보안 이슈를 함께 고려해야 하며, 다양한 이기종 기기들이 연결된 초연결 네트워크이기 때문에 각 기기들에대한 시스템 보안 또한 고려되어야 한다. 추가로 스마트 시티에는 개인정보가 포함된 데이터가 많기 때문에 개인정보 등의 데이터 보호 관련 기술과 개인 인증 기술 등도 포함되어야 한다.

나. 스마트·자율 주행 이동체 보안

스마트 카, 커넥티트 카, 자율 주행 자동차(self-driving car) 등은 진보된 정보통신 기술을 자동차에 적용한 융합 기술이다. 일차적으로는 운전자, 보행자 또는 타 이동체의 안전을 높이고 운전자의 편의를 향상시키는 것을 목표로 한다. 더 발전한 형태로 운전자 없이 자율 주행이 가능한 자동차를 목표로 한다. 보통 스마트 카, 커넥티트 카는 자율 주행보다 운전자 보조를 통해 편의 제공을 목적으로 하고, 자율 주행 자동차는 운전자가 없이 이동이 가능한 자율 주행을 목적으로 한다. 자동차가 아닌 선박이나 무인 항공기, 서비스 로봇 등에도 비슷한 융합 기술이 적용될 수 있다.

자율 주행 자동차는 첨단 정보통신 기술이 적용된 매우 유망한 응용이며 지능형 교통 시스템과 함께 변화를 일으키고 있다. 통신 기술이 향상됨에 따라, 차량을 연결하고 도로 인프라 및 인터넷과 통신하는 개념인 커넥티드 카의 개념이 실현되었고 자주 자율 주행 자동차의 기술과 함께 발전하고 있다.

자율 주행 자동차에는 비자동화에서 완전 자동화까지 다양한 레벨이 있다. 2018년에 SAE(Society of Automotive Engineers)는 차량 자동화의 5가지 수준을 구체적으로 제시하였다. 이 다섯 가지 수준은 레벨 0인 비자동화, 레벨 1의 운전자 지원, 레벨 2의 부분 자동화, 레벨 3의 조건부 자동화, 레벨 4의 고도 자동화, 레벨 5의 완전 자동화로 이루어져 있다.

〔그림 2－66〕 자율 주행 수준

< 운전 자동화의 단계적 구분 >

레벨 구분	레벨 0	레벨 1	레벨 2	레벨 3	레벨 4	레벨 5
	운전자 보조 기능			자율주행 기능		
명칭	자율주행 없음 (No Automation)	운전자 지원 (Driver Assistance)	부분 자동화 (Partial Automation)	조건부 자동화 (Conditional Automation)	고도 자동화 (High Automation)	완전 자동화 (Full Automation)
자동화 항목	없음	방향조작 or 속도	방향조작 & 속도	방향조작 & 속도	방향조작 & 속도	방향조작 & 속도
운전주시	항시 필수	항시 필수	**항시 필수** (운전대 상시 잡고 있어야함)	**시스템 요청시** (운전대 잡을 필요X, 제어권 전환시만 필요)	**작동구간 내 불필요** (제어권 전환X)	전 구간 불필요
자동화 구간	-	특정구간	특정구간	특정구간	특정구간	전 구간
시장 현황	대부분 완성차 양산	대부분 완성차 양산	7~8개 완성차 양산	1~2개 완성차 양산	3~4개 벤처 생산	없음

자료: 산업통상자원부, “산업통상자원뉴스, 2021”

자율 주행 자동차는 레이저, 레이더, 카메라, GPS, LiDAR와 같은 많은 센서 구성 요소와 이동 통신, 블루투스, Wi-Fi와 같은 다양한 통신 기법이 사용된다. 센서 구성 요소는 자율 주행 자동차가 장애물을 주행 중에 탐지할 수 있도록 해준다. 이러한 감지 센서의 데이터를 사용하여 주변 환경과 차량의 위치가 동시 위치 및 매핑(SLAM) 방법으로 계산된다. 통신을 통해 더 많은 데이터를 축적하고 학습함으로써 운전자의 운전 경험이나 자율 주행 시스템을 개선한다. 예를 들어 지능형 운전자 지원 시스템(IDAS), 차량 대 인프라 통신(V2I)을 통한 안전 기능이나 차량 대 차량 통신(V2V)을 통한 안전 기능이 있다. 이러한 센서 구성 요소와 통신 기법은 안전과 비용면에서 상당한 개선을 가져오지만, 반면에 사이버 공격의 위협에 노출될 가능성이 커졌다.

〔그림 2－67〕 V2X에서 사이버 공격의 위협

자료: KISA 한국인터넷진흥원

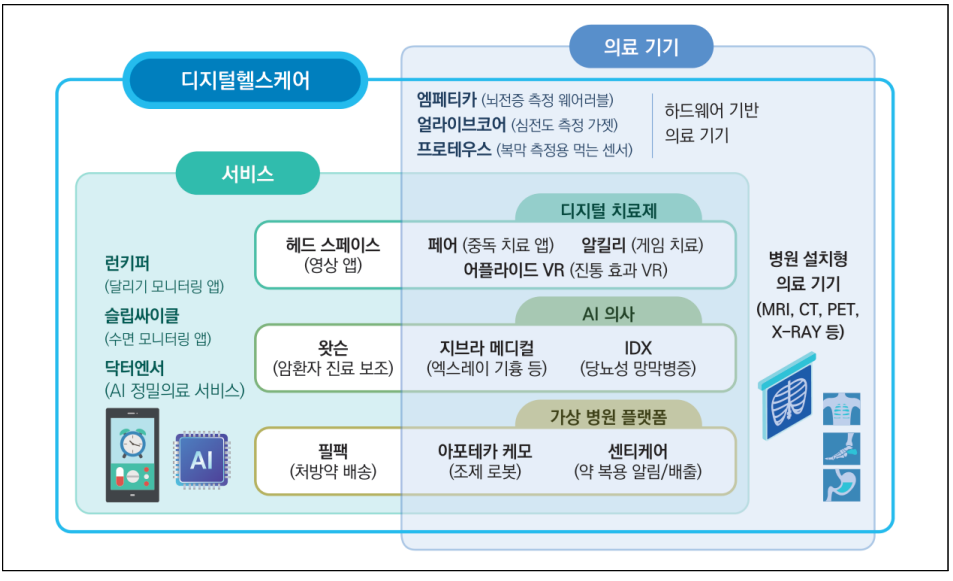
앞서 말했듯이 자율 주행 자동차는 다양한 센서 구성 요소와 통신 기술을 사용하는데, 이들이 곧 공격 대상이 될 수 있다. 이 중 하나라도 공격을 당하면 전체 시스템이 불안정해지거나 최악의 경우 차량 사고로 이어져 인명과 재산 피해가 발생할 수 있다. 공격 대상에는 OBD(On-board Diagnostic Port), ECU(Electronic Control Unit), CAN(Controller Area Network)과 같은 기본적인 자동차 전장 시스템을 포함하여, LiDAR, 레이더, GPS, 카메라 등과 같은 센서 구성 요소와 통신 장비 등이 포함될 수 있다. 공격자는 원격으로 공격을 할 수도 있고, 직접 물리적으로 접근하여 공격을 할 수도 있다. 그리고 공격을 통해 운전 조작을 방해하거나, 차량이나 정보를 탈취하려고 할 수 있다.

이런 공격에 대비하기 위한 기술로 기존의 보안 기술을 포함하여 새로운 자율 주행 자동차를 위한 보안 기술의 개발이 필요할 수 있다.

다. 디지털 헬스케어 보안

디지털 헬스케어는 의료 서비스에 정보통신 기술에 융합되어 건강 및 질환을 케어하는 종합 의료 서비스이다. 개인이 휴대하는 기기에서 수집된 데이터, 의료 정보 클라우드에서 확인 가능한 데이터 등의 분석을 통해 개인 맞춤형 서비스를 제공한다. 또한 원격 의료의 영역도 포함한다.

〔그림 2-68〕 디지털 헬스케어 서비스 구성요소



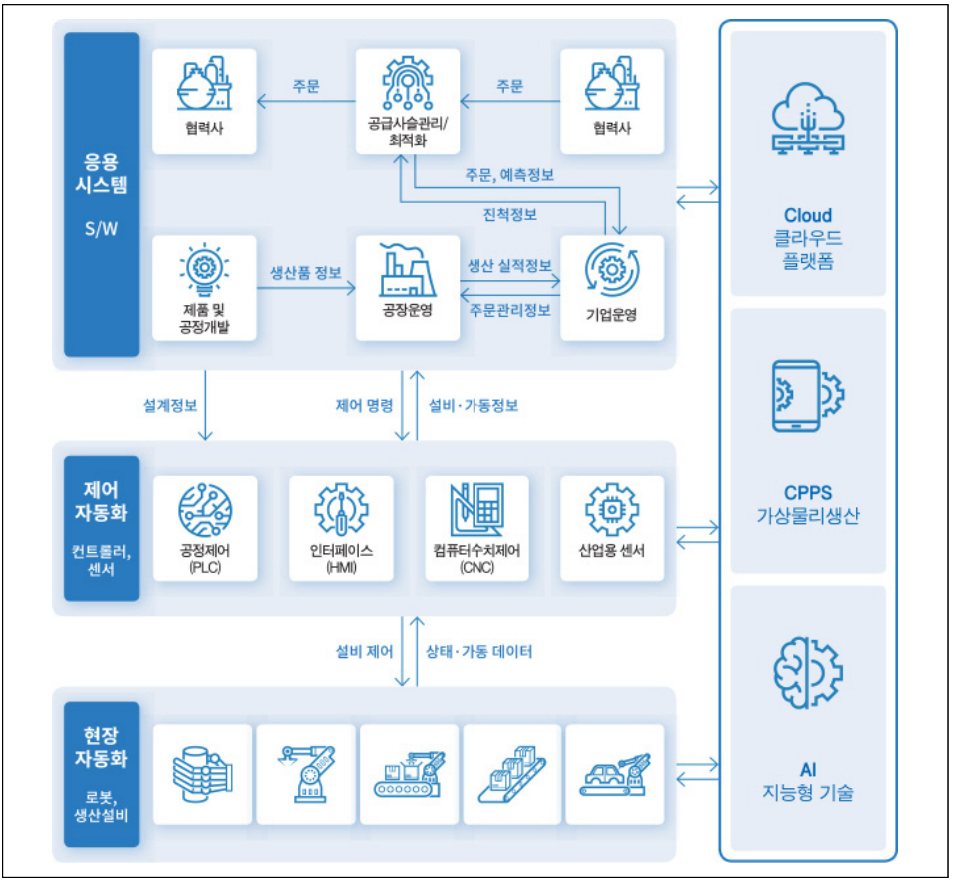
자료: KISA, 한국인터넷진흥원 "디지털 헬스케어 보안모델, 2021"

디지털 헬스케어에는 IoT, 클라우드, 빅데이터 등의 정보통신 기술이 결합되어 혁신적인 의료 서비스를 제공할 수 있으나 반면에 이런 정보통신 기술의 보안 취약점에 노출될 가능성도 안고 있다. 그로 인한 결과는 매우 치명적일 수 있다. 실제로 보안 취약점과 위협에 대한 보고가 존재하며 이로 인해 향후 디지털 헬스케어에서 보안 사고가 발생할 수 있다.

라. 스마트 공장 및 산업제어 보안

스마트 공장은 정보통신 기술을 융합한 첨잔 지능형 공장이다. 스마트제조혁신단에서 말하는 스마트 공장의 정의는 "제품의 기획부터 판매까지 모든 생산과정을 ICT(정보통신) 기술로 통합해 최소 비용과 시간으로 고객 맞춤형 제품을 생산하는 사람 중심의 첨단 지능형 공장"으로 되어 있다. 또한 그 범위는 제품을 생산하는 공정만이 아니라 "제품 기획·개발부터 양산까지, 주문에서부터 완제품 출하까지 제조 관련 모든 과정 포함하며 응용 시스템뿐 아니라 현장자동화와 제어자동화 영역까지 공장 운영의 모든 부분을 포함"하는 것으로 본다.

〔그림 2－69〕 스마트 공장의 구성요소



자료: 스마트제조혁신추진단, https://www.smart-factory.kr/smartFactoryIntro

스마트 공장은 정보통신 기술의 접목으로 생산 설비 등의 기기가 네트워크로 연결되고 외부와도 연결되고 있어 그만큼 보안 취약점이 발생할 수밖에 없다. 실례로 공장 제어 및 운영 시스템이 랜섬웨어에 감염되어 큰 피해가 발생한 경우도 있다.

스마트 공장에는 IoT를 비롯하여 클라우드, 인공지능 기술 등이 활용되어 이를 위한 보안 기술 뿐 아니라 스마트 공장 전반에 대한 보안 위협 분석과 대응 체계 구축도 필요하다. 한국인터넷진흥원에서는 스마트공장 보안 모델 문서를 통해 스마트 공장 관리자들이 보안 강화에 활용할 수 있도록 도움을 주고 있다.

2. 기술 개발 현황

앞에서 설명한 스마트 시티, 스마트·자율 주행 이동체, 디지털 헬스케어, 스마트 공장 및 산업제어 등의 융합 서비스에 대한 융합보안 기술 개발 현황을 살펴본다.

가. 스마트 시티 보안

스마트 시티 보안 기술은 스마트 시티 인프라를 구성하는 기기와 네트워크를 보호하기 위한 보안 기술과 네트워크 상에서 접근 가능한 개인 정보 등의 데이터를 보호하는 기술로 나눌 수 있다. 전체 시스템이 매우 방대하기 때문에 이를 고려한 기존 기술의 적용 및 개선이 필요하다.

국내에서는 세종과 부산에 스마트 시티 국가 시범 도시를 마련하고 다양한 서비스를 실증하고 있으며 이외에도 시흥시 등에서도 스마트 시티 사업을 진행하고 있다. 또한 스마트 시티 챌린지나 리빙랩 등의 사업을 통해 새로운 스마트 서비스를 발굴하고 스마트 시티 조성을 위해 노력하고 있다. 그러나 보안과 관련하여서는 뚜렷한 기술 개발을 위한 노력이 눈에 띄지 않는다. LG CNS와 같은 기업에서 스마트 시티 보안을 위해 기존 기술을 기반으로 하여 보호할 대상을 정의하고 필요한 보안 대책을 수립하는 컨설팅 수준의 보고들은 있으나 이를 기술로 정의하여 개발한 사례는 확인되지 않는다. 개별 서비스에서 보안과 연관된 서비스, 예를 들어 블록체인 기반의 분산ID 서비스를 이용한 스마트 시민증 구현 정도이다.

〔그림 2－70〕 LG CNS의 스마트시티 정보 보호 프레임워크

자료: LG CNS, https://www.lgcns.com/blog/cns-tech/smartcity/2805/

미국에서는 그리드에 대한 사이버 공격 복구를 위한 프로젝트 RADICS를 개발하고 있으며 일부는 실제 미국 전력망 일부에 배치되어 운영중이다. DARPA의 RADICS(Rapid Attack Detection, Isolation, and Characterization Systems)라는 프로그램으로 개발된 이 기술은 테크놀로지의 기본 개념은 그리드 사이버 공격에 의한 피해를 제한하면서 “블랙 스타트 복구“를 가능하게 한다. 블랙 스타트 복구는 전기 시스템 컴포넌트가 다운되었을 때 정상 동작을 회복하는 것을 말한다.

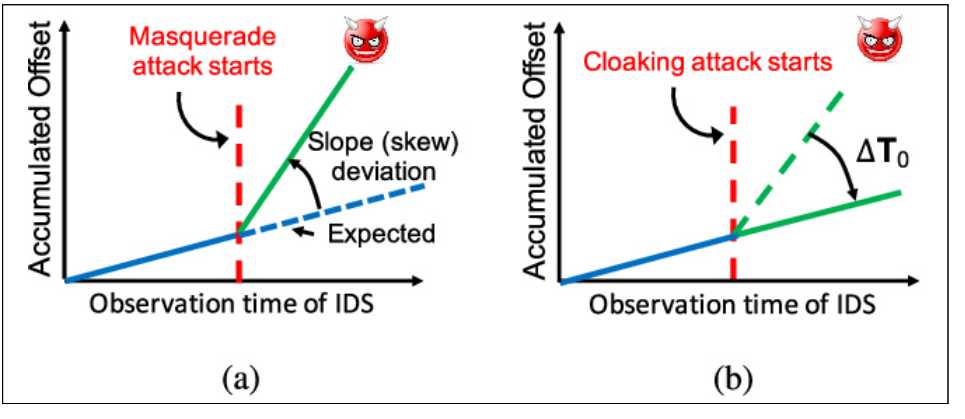
RADICS는 3가지 핵심 기능을 제공하는 툴셋을 개발하였다. 첫째는 가시성 또는 상황 인식을 통해 운영자는 적시 정보를 기반으로 사이버 공격 전, 중간, 후의 그리드 상태를 이해할 수 있다. 둘째, 공격 중 감시 제어 및 데이터 수집 트래픽을 침해된 네트워크로부터 전송하는 긴급 네트워크를 격리하는 기능이다. 셋째는 그리드 사이버 공격을 특징짓고 손상된 구성 파일이나 제어 시스템에 주입된 악성 코드 등 공격의 특정 요소에 대응할 수 있다.

나. 스마트·자율 주행 이동체 보안

스마트·자율 주행 이동체 보안 기술은 크게 기존 보안 기술을 활용하여 가능한 공격에 대응하기 위한 연구들과 근본적으로 이동체의 보안 수준을 향상시키기 위한 연구로 나눌 수 있다. 전자의 경우는 크게 이상 침입 탐지 시스템(IDS), 정보 중복, 암호 기법 등이 있다. 후자에는 차량 간 V2X 통신보안, 차량용 이더넷 보안 및 취약점 분석 기술 등이 있다.

이상 기반 침입 탐지 시스템(IDS)은 무단 액세스 또는 위조 데이터를 탐지하는 기술이다. IDS는 일반적으로 신호 또는 사이드 채널 정보로부터 비정상적인 데이터를 감지한다. 예를 들어, ECU의 클럭 스큐(클럭 신호가 약간 다른 시간에 다른 ECU에 도착하는 현상)를 측정하고 이 정보를 사용하여 비정상적인 클럭 스큐를 확인하여 침입을 감지할 수 있다. 위조된 신호를 보내는 CAN 공격이나 LiDAR 스푸핑, 레이더 스푸핑, GPS 스푸핑에 이런 기법을 적용할 수 있다. 하지만 카메라에 대한 적대적 이미지 공격을 방어하는 데는 적절하지 않다.

〔그림 2-71〕 수신측에서 IDS에 의해 감지되는 클럭 스큐



자료: Ying, Xuhang, Sang Uk Sagong, Andrew Clark, Linda Bushnell and Radha Poovendran. (2019). "Shape of the Cloak: Formal Analysis of Clock Skew-Based Intrusion Detection System in Controller Area Networks." IEEE Transactions on Information Forensics and Security 14, pp2300-2314.

정보의 중복 기법은 다른 차량이나 인프라로부터 정보를 얻거나 차량 내에 중복하여 정보를 저장하는 방법이다. 이는 사이버 공격으로부터 방어할 뿐만 아니라 자율 주행에 필요한 센서 데이터의 정확성을 향상하는데도 도움이 된다. 이를 이용하여 일반적으로 LiDAR 방해, 레이더 방해, 카메라 블라인딩과 같은 서비스 거부 유형의 공격 방어가 가능하다. 예를 들어 파장이 다른 여러 LiDAR 센서를 사용함으로써 LiDAR 센서에 고출력 광선을 보내는 공격으로부터 방어할 수 있다. 그러나 이 방법은 GPS 교란에는 효과적이지 않다. 이 기법의 단점은 중복을 위해 비용이 많이 든다는 것이다.

암호와 방법은 보안의 가장 기본적인 기법이다. 센서용 CAN 및 신호 등 인증 방법이 부족한 구성 요소를 악용하는 공격 방어를 위해 암호화 방법을 적용할 수 있다. CAN 및 센서 신호의 보안을 위해 다양한 암호화 방법이 제안되었다. 그러나 GPS 수신기에는 암호화된 무선 신호를 보낼 수 있도록 위성을 수정하는 데 비용이 너무 많이 들기 때문에 암호화 방법이 적용되기 곤란하다.

차량 간 V2X 통신보안을 위해 WAVE(Wireless Access in Vehicular Environments) 관련 국제 표준인 IEEE 1609.2에서 보안 서비스를 정의하고 있다. 이 보안 서비스는 보안 처리 서비스(Security Processing Servies)와 보안 관리 서비스(Security Management Services)로 구성된다. 보안 처리 서비스는 차량 데이터와 WSA가 보안 통신을 하기 위한 절차를 제공한다. 여기에서 WSA는 WAVE Service Advertisements이다. 보안 관리 서비스는 인증 관련 서비스를 제공한다. 인증 관련 서비스를 위해 PKI(Public Key Infrastructure)를 사용한다. 그런데 차량간 통신인 V2V에서는 차량의 익명성 보장이 중요하다. 따라서 익명성을 보장하지만 인증기관(CA)으로부터 신뢰가 보장됨을 확인할 수 있는 인증서가 필요하다. 따라서 차량에서 사용할 인증서는 V2I에서 사용할 차량 식별이 가능한 인증서와 V2V에서 사용할 차량 식별이 불가능한 익명성 보장되는 인증서가 필요하다. 전자는 표준으로 되어 있으나 후자는 표준에 정의되어 있지 않아 보통 미국은 CAMP에서 정의한 방식을, 유럽은 C2C-CC를 사용한다.

차량 내의 ECU가 100개 이상으로 많아지고 있는 상황에서 ECU를 위한 보안 기술 개발이 이루어지고 있다. 시큐어 부트, 가상화 솔루션 등이 개발되고 있다. 차량용 미들웨어 표준인 AUTOSAR에 정의된 보안 기능을 구현하여 적용하고 있고, 하드웨어 기반의 보안 모듈을 ECU에 적용하는 연구도 진행 중이다.

차량 내의 ECU가 많아지고 네트워크 트래픽이 높아지면서 기존 방식이 아닌 이더넷 기반의 고속 전송 백본 네트워크를 필요로 하고 있다. 이더넷 도입에 따른 보안 연구가 필요하여 ESCRYPT, NXP 등에서 자동차 이더넷 보안을 위한 기술 요구사항 및 구조를 제안하고 후속 연구를 진행하고 있다.

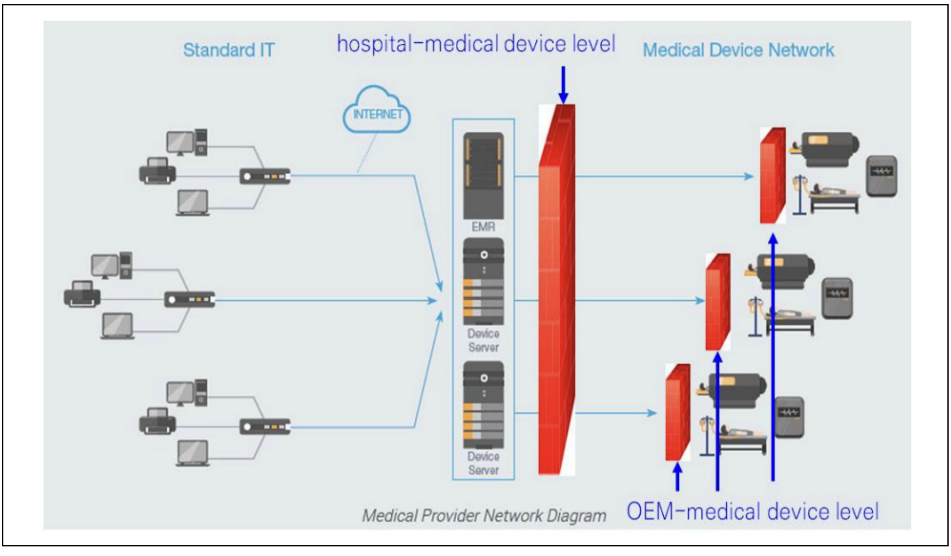
차량 취약점 분석 및 진단과 관련한 기술로 부품에 대한 보안 평가나 취약성 분석에 대한 연구가 진행되고 있다. 또한 포렌식 관련 기술 개발도 진행중이다. SAE에서는 2015년 사이버 보안을 위한 자동차 개발 프로세스 및 가이드라인을 정의하였다.

다. 디지털 헬스케어 보안

디지털 헬스케어 관련 보안 기술 개발은 크게 개인 정보 보호와 헬스케어 서비스에 대한 보호로 나누어 볼 수 있다. 개인 정보 보호를 위해서 의료정보 비식별화, 접근권한 관리 등 의료 민감정보의 불법 유출 방지 중심의 연구가 진행 중이다. 서비스에 대한 보호로 의료기기 해킹 방지, 의료 랜섬웨어 대응, 생체신호 기반 보안통신, 헬스케어 데이터 보안 기술 등에 대한 기초연구가 진행 중이다.

대형 병원의 경우 만여 개 이상의 의료기기가 설치되어 있고, 이러한 대규모 기기들에 대한 관리가 적절히 이루어지지 못하고 있다. 결과적으로 오래된 고가 장비, 소프트웨어 업데이트가 제대로 되지 않은 경우, 보안 소프트웨어 설치가 곤란한 경우 등 보안 위협이 매우 높은 상황이다. 따라서 이러한 의료 기기들이 동작이나 네트워크를 모니터링하여 이상 행위를 탐지하고 대응하는 연구와 제품 개발이 활발하다. 대표적으로 Medigate사의 헬스케어 IoT 보안 솔루션은 병원 네트워크에서 의료기기의 이상 징후를 예측,탐지하여 공격에 대응하는 기술을 개발하여 제품을 출시하였다. 기기별로 탐지 센서를 두어 이상 징후를 탐지하는 방식과 전자의무기록(Electronic Medical Record, EMR) 시스템에서 전체 기기에서 발생하는 트래픽을 모니터링하여 이상 징후를 탐지하는 방식이 있다.

〔그림 2－72〕 Medigate 솔루션 구조



자료: 정보통신기획평가원, “주간기술동향 - 커넥티드 의료기기 보안 동향 및 이슈, 2019”

기계학습을 이용하여 헬스케어 기기에서 이상 행위를 탐지하는 연구도 기업, 대학에서 많이 연구되었다. EHR 솔루션 업체인 메디테크(MediTech)사는 인공지능 기반 분석을 통해 기기에 대한 해킹 예측 및 이상 징후 탐지 기술을 개발하였다. 징박스(ZingBox)는 딥러닝 기반으로 기기에서 이상 행위 탐지 기술을 개발하였다. 징박스는 기계 학습, 인공지능, 위협 인텔리전스를 사용하여 장치를 식별 및 프로파일링하고, 장치의 동작을 분석하고, 취약성과 위험을 평가한다. 식별된 위험 및 위협의 교정 작업을 조정하고 기기를 적절한 네트워크 세그먼트에 내장하여 컨텍스트 인식을 통해 정밀한 세분화를 지원한다. 이렇게 함으로써 공격에 노출되는 부분이 줄어들고 신뢰할 수 있는 동작만 허용할 수 있게 된다. 징박스의 IoT Guardian은 인공지능을 사용하여 각기기의 고유한 특징을 학습하고 이를 통해 자동으로 기기를 식별한다. 이는 기기의 모니터링, 보고, 업그레드 등을 단순화할 수 있고 연결된 기기들을 실시간으로 검색, 제어 및 관리할 수 있다.

심박조율기 및 제세동기와 같은 많은 이식형 의료기기는 환자의 상태를 모니터링하고 조정할 수 있도록 임상 데이터를 원격으로 전송할 수 있다. 그러나 이 과정에서 해커들은 환자 개인 의료 데이터에 접근하거나 악성 프로그램을 사용하여 환자를 인질로 삼거나 의

료 데이터를 가로챌 수 있거나 상호 연결된 다른 기기나 IT 시스템을 감염시킬 수 있다. 애리조나 대학에서는 이런 이식형 으료기기가 어떻게 데이터를 안전하게 전송하고, 전력 소비를 최적화하며, 전자기 방사선을 처리하는지를 평가하는 것을 포함하여 모든 각도에서 보안 취약성을 해결하려는 연구를 수행하였다. 이 연구에서 개발한 장치는 심박조율기에서 심장 기록 시스템으로 데이터를 계산하고 전송합니다. 정상적이고 정확한 시간에서 벗어난 것은 악성 프로그램의 존재를 나타낼 수 있고, 만약 변화가 감지되면, 의사들은 즉시 환자에게 해를 끼치지 않도록 시정 조치를 취할 수 있도록 알려준다. 또 다른 연구에서는 시간뿐만 아니라 전력 소비와 전자기 방사선의 변화를 분석하기 위한 수학적 모델을 개발하고 있다.

프린스턴과 퍼듀 대학에서는 무선 채널 모니터링 및 이상 탐지를 기반으로 한 의료기기의 보안을 위한 일반적인 프레임워크를 연구하였다. 이 연구는 의료기기와 주고받는 모든 무선 주파수 무선 통신을 모니터링하고 다층 이상 탐지를 사용하여 잠재적으로 악의적인 트랜잭션을 식별하는 의료 보안 모니터(MedMon)를 기반으로 한다. 악성 트랜잭션을 탐지하면 MedMon은 적절한 대응 조치를 취하는데, 이는 수동적(사용자에게 알림)에서 능동적(의료 기기에 도달하지 않도록 패킷을 방해)에 이르기까지 다양하다. MedMon의 주요 이점은 환자가 사용 중인 기존 의료기기에 하드웨어나 소프트웨어 수정 없이 적용할 수 있다는 것이다. 따라서 이러한 장치의 전력 오버헤드도 발생하지 않는다.

라. 스마트 공장 및 산업제어 보안

스마트 공장 및 산업제어 보안은 기존 보안 기술을 어떻게 잘 적용하여 보안성을 높일 것인지에 대해 지침이나 보안 모델 등이 다수 발표되었고 스마트 공장만을 위한 보안 요소 기술에 대한 연구는 많지 않다.

국내 지침으로는 한국인터넷진흥원에서 발표한 “스마트공장 사이버보안 가이드”, “스마트공장보안 모델” 이 있다. 국외 지침으로는 NSA(National Security Agency)의 DiD(Defense-in-Depth) 전략이 있다. 이는 계층적 방어 개념으로 OT(Operational Technology)와 IT(Information Technology)의 융합으로 ICS(Industrial Control Systems) 네트워크와 기업 네트워크의 연결에 따른 복잡성이 증가하는 스마트 공장에 적용할만 하다.

국내 국가 KS표준으로 2020년에 산업자동화제어시스템(IACS)을 사이버 공격으로부터 보호하기 위한 표준이 제정되었고 이는 최초 국가 표준 사례이다.

국내 삼성 SDS나 LG CNS 등에서는 산업용 제어시스템의 인프라 보호를 위한 지능형 산업제어시스템 보안 기술과 스마트공장 융합보안 기술을 개발 중이다. 국외의 Tofino Indegy 등의 기업에서는 산업제어설비의 초연결성으로 인해 IT 영역의 위협방지에서 OT 영역의 위협방지기술 개발로 확대 하여 산업제어시스템의 실시간 행위 모니터링을 통한 인공지능 기반 이상행위 탐지 기술을 적용하여 침해사고를 사전에 식별하는 기술을 개발하였다.

중국 등에서 전통적인 IIoT에서 분산 네트워크를 구축하기 위한 새로운 방식인 블록체인 아키텍처를 연구하였다. 블록체인 기반 아키텍처를 설계하는 데 도움이 되는 보안 및 개인 정보 보호 모델을 제시하고 새로운 멀티 센터 부분 분산 아키텍처를 만들었다.

3. 기술 발전 방향

앞에서 설명한 스마트 시티, 스마트·자율 주행 이동체, 디지털 헬스케어, 스마트 공장 및 산업제어 등의 융합 서비스에 대한 융합보안 기술 발전 방향을 제시한다.

가. 스마트 시티 보안

보안과 프라이버시는 스마트 시티의 가장 중요한 부분이지만 충분한 연구가 되어 있지 않다. 향후 스마트 시티 보안 강화를 위해 필요한 연구 방향에 대해 제시한다.

스마트 시티에서 수집되는 방대한 데이터 처리 과정에서 보안과 개인정보 보호가 필수적이다. 스마트 시티를 위한 빅데이터 처리 프레임워크에 대한 연구는 되었으나 여기에서 보안이나 개인정보 보호에 대한 연구는 미흡하다. 또한 데이터를 수집하는 IoT 기기는 연산 능력이나 에너지 제약인 경우가 많은데 이를 위해 매우 효율이 높고 가벼운 암호 알고리즘이 필요하다.

클라우드 기반 프레임워크는 스마트 시티의 스토리지 문제를 효율적으로 해결할 수 있는 방법이다. 스토리지 하드웨어의 비용이 감소함에도 이러한 대규모 스토리지 관리에 드는 비용이 매우 높기 때문에 클라우드가 좋은 해결책이 된다. 스마트시티에서 IoT 기기가

수집한 방대한 데이터를 클라우드 스토리지에 아웃소싱하고 데이터 관리를 클라우드 관리 회사에 위임할 수 있다. 그러나 클라우드는 본질적으로 안전하지 않고 신뢰할 수 없으며, 클라우드 컴퓨팅에서 아웃소싱된 데이터의 무결성에 새로운 문제를 제기한다. 이런 문제 해결에 원격 데이터 감사(RDA) 등의 기법을 스마트 시티 빅데이터 처리에 적용하는 방안 등의 연구가 필요하다. 원격 데이터 감사는 전체 데이터를 다운 받지 않아도 데이터의 무결성을 보장할 수 있는 기법이다.

나. 스마트·자율 주행 이동체 보안

자율 주행 자동차에서 네트워킹의 다양화와 고도화로 지금 보다 더 많은 차량 해킹 시도가 발생할 것으로 예상된다. 향후 자율 주행 자동차의 보안 강화를 위해 필요한 연구 방향에 대해 제시한다.

차량 내 네트워크가 다양해짐에 따라 혼합네트워킹으로 구성되고 이 네트워크들 간의 보안을 강화하기 위한 보안 게이트웨이 연구가 필요할 것이다.

데이터의 양이 커지고 네트워크 참여 객체간의 소통이 많이 짐에 따라 객체의 인증과 접근 제어 등의 연구가 필요할 것이다.

차량의 원격 주행, 군집 주행등 고도화된 자율 주행 서비스를 위해 5G 도입이 필수적인데, 이에 따라 5G 기반 차량통신 보안 기술의 개발이 필요하다.

V2I를 통해 자율 주행 차량의 데이터 통신이 크게 폭증할 것으로 예상되며 이에 대처하기 위한 보안 기술 개발이 필요하다.

다. 디지털 헬스케어 보안

랜섬웨어 등 병원 네트워크의 피해 사례가 증가하고 있어 병원 의료기기의 특성에 맞는 비침습적 위협 탐지와 위협 대응을 위한 기술 개발이 필요하다. 해외에서는 퍼듀대학교, Medigate, Zingbox 등에서 이와 관련한 연구가 활발히 진행되고 있으나 국내에서는 관련 연구가 부족하여 적극적인 연구가 필요하다.

일부 의료기기의 경우 환자의 몸 안에 이식하는 체내이식형이 있는데, 이런 기기의 경우 탈부착을 위해서는 외과적 수술을 필요로 하기 때문에 기기가 수명을 다할 때까지 탈

착이 곤란하다. 그런데 이런 체내이식형 기기에서 보안을 위해 암호 키를 사용을 하는 경우 키를 변경하려고 할 때 안전하게 키를 변경하는 것이 쉽지 않다. 이런 경우를 고려하여 핀란드의 Turfu 대학에서는 신체의 ECG(심전도) 정보를 분석하여 활용하는 일회용 암호 키를 생성하는 기술을 개발하였다. 이는 생체 신호를 그대로 사용하기 때문에 외부에서 키를 전달할 필요가 없고 내부에서 스스로 키를 생성하여 키를 전달하는 과정에 노출될 위험이 없다. 이와 같이 생체 신호를 기반으로 한 바이오 암호 기술에 대한 연구가 필요하다.

체내이식형 의료기기는 앞의 키 이슈 뿐 아니라 배터리 문제를 갖고 있다. 배터리는 일반적인 상황을 고려하여 용량을 정하는데, 만일 공격자가 불필요한 무선 전파를 송신하여 배터리를 고갈시키는 공격 등을 할 경우 위험할 수 있다. 이런 공격 등에 대응하기 위해 스스로 전기를 생산할 수 있는 심장박동기가 개발되었으나, 이 기술은 심장이라는 특수한 장기를 대상으로 한 기술이라는 한계가 있다. 결국에는 인체 내에서 확보 가능한 체온, 혈류, 인체의 움직임 등 체내 에너지를 통해 배터리를 스스로 충전할 수 있는 체내 에너지 하베스팅 등의 기술에 대한 연구가 필요하다.

라. 스마트 공장 및 산업제어 보안

스마트 공장에서 사용 가능한 ICS 보안 도구들은 스마트 공장의 요구를 100% 만족해주지 못하고 있다. 즉 현장에서 사용하는 프로토콜을 모두 지원하지 못하고 있으며 이를 추가하기 위한 개발 노력이 필요하다.

ICS 보안 도구들이 해결해야할 연구 방향으로 다양한 현장 산업 프로토콜을 지원하고 이를 위한 IDS의 규칙들에 대한 연구가 필요하다.

공장내 기기들을 자동으로 검색하고 취약성을 제공하거나 필요한 규칙들을 제공해주는 도구들에 대한 연구가 필요하다.

제 4 절 기술 로드맵·시나리오

1. 기술 로드맵

공통 보안 기술과 시스템·네트워크 보안 기술에 대하여 2030년까지의 기술 개발 로드맵을 다음과 같이 제시한다.

가. 공통 보안 기술 로드맵

〈표 2-10〉 공통 보안 기술 로드맵

	2023		2025		2030	
암호 기술	양자내성 암호보안 인프라	암호 인프라 양자안전성 분석 기술	AI 기반 암호 설계 및 안전성 분석 기술	초저지연 암호 기술	초연결 환경 암호키 신뢰 관리기술	양자내성 검증 플랫폼
인증·인가 및 접근제어 기술	무자각 인증 및 ID 관리 자동화 기술	원격의료 보호 기술	분산 디지털 신원지갑 보호 및 상호연동 기술	안전한 원격 근무를 위한 논리적 망분리 기술	온 디맨드 멀티모달 기반 지속인식 기술	EEG분석 기반 Pass-Thought 기술
데이터 보안	안전한 가명정보 활용 및 결합을 위한 가명처리 기술	가명정보 활용에 따른 프라이버시 침해 위험 검증 기술	동형암호, 안전계산 기술	차분 프라이버시 기술	AI 활용 가능한 프라이버시 보호 기술	
하드웨어 기반 보안	신뢰 실행 환경 기술	양자 난수 생성기	드론 등 융합 환경에서의 물리적 복제 방지 및 키 생성 기술			
AI 보안	적대적 공격 대응 기술	안전하고 재사용 가능한 인공지능 플랫폼 기술	온디바이스 AI 기술		고신뢰 AI 기술	설명 가능한 AI 기술

나. 시스템·네트워크 보안 기술 로드맵

〈표 2-11〉 시스템·네트워크 보안 기술 로드맵

	2023		2025		2030	
사이버 위협 인텔리전스	클라우드 환경 지능형 통합보안관제 기술	지능형 보안 오케스트레이션, 자동화 및 대응 기술(SOAR)	AI 기반 사이버 공격 시뮬레이션 기술	AI 기반 악성코드 탐지 기술	AI 기반 무인 보안관제 기술	
랜섬웨어 대응	서비스형 랜섬웨어(RaaS) 인프라 식별 기술	랜섬웨어 복구를 위한 변경 불가 백업 기술	랜섬웨어 공격 근원지 추적 기술	민감정보 노출방지 암호기술	AI 기반 랜섬웨어 탐지 및 분석 기술	
IoT 디바이스 보안	저전력 암호 알고리즘 기술	펌웨어 암호화 및 서명 기술	시큐어 업데이트 기술	서버, 디바이스 간 인증 기술	경량 보안 운영체제 기술	보안 SoC 칩 기술
5G 보안	5G 코어망 분산 DDoS 공격 탐지 및 대응 기술	5G 보안 관제 자동화 기술	5G MEC 인프라 보안 기술	6G 보안 내재화 구조 설계 기술	사이버 위협 인텔리전스 연동 지능형 5G 보안 기술	6G 보안을 위한 양자 암호 기술
클라우드 보안	서비스형 보안 (SECaaS) 기술	멀티 테넌시 보안 기술	멀티 클라우드 보안 기술	엣지 클라우드 보안 기술	제로 트러스트 클라우드 보안 기술	SASE(Secure Access Service Edge) 기술
공급망 보안	소프트웨어 취약점 탐지 및 분석 기술	퍼징 기반 하드웨어 취약점 탐지 기술	소프트웨어 업데이트 코드 안전성 검증 기술	AI 기반 하드웨어 취약점 탐지 기술	하드웨어 및 펌웨어 백도어 탐지 기술	공급망 SW 및 HW 통합 위협 분석 기술

2. 기술 발전 시나리오

현재 사이버 보안 기술 수준으로 인한 문제점을 해소하고 발전된 미래 기술을 제시하기 위해 기술 발전 시나리오를 다음과 같이 제시한다.

- 수동·반복되는 명시적 인증 → 무자각 지속 인증 및 ID 관리 자동화
- 양자 위협에 노출된 암호 → 양자 위협에 대비한 암호
- IT 중심 보안 → OT가 통합된 융합 보안
- 인력 중심의 보안 관제 → AI 기반의 자동화된 보안 관제

각 발전 시나리오에 대해 현재 기술 수준, 미래 기술 수준을 정의하고 미래 기술 수준에 도달하기 위한 필요 기술을 제시한다.

가. 수동·반복되는 명시적 인증 → 무자각 지속 인증 및 ID 관리 자동화

1) 현재 기술 수준

현재의 사용자들은 컴퓨터 뿐만 아니라 모바일 앱 등을 통하여 다양한 형태의 온라인 서비스를 이용하고 있다. 최근에는 O2O 서비스를 통하여, 오프라인에서 조차 온라인과 연계된 서비스를 받고 있는데, 이런 서비스에서는 대부분 인증이 필수적이다. 인증은 대체로 지식 기반, 소유 기반, 생체 기반 인증으로 나누며 이는 다음과 같다.[2)]

2) 간혹, 현재 위치 등 여기에 포함되지 않는 인증 방식이 이용되기도 하지만, 일부 응용에서만 활용하는 경우가 대부분이다.

〈표 2-12〉 공통 보안 기술 로드맵

인증 방식	의미	인증 방식의 예	특징
지식	기억하고 있는 정보를 이용하여 인증 수행	ID/패스워드, PIN 번호, 패턴그리기 등	공유 가능, 망각
소유	신분증, OTP 장치 등 소유물을 통하여 인증 수행	신분증, OTP 장치, 카드, 열쇠, 토큰, 인증서 등	공유 가능, 복제
생체	얼굴, 홍채 등 생체 정보를 이용하여 인증 수행	얼굴, 음성, 지문, 홍채, 정맥 등	공유불가능, 부인방지

지식 기반 인증은 현재 가장 널리 사용되는 인증 방식으로, 패스워드 또는 PIN 번호, 통장 비밀번호와 같이 기억할 수 있는 정보를 통해 사용자의 신원을 확인한다. 지식 기반 인증은 사용이 편리한 장점에 있는 반면, 무차별 대입 공격(Brute Force), 사전 공격(Dictionary Attack), 어깨 너머 넘보기 공격(Shoulder surfing) 등 다양한 공격에 취약하며, 같은 인증 정보를 사용하였을 때 공격의 피해가 매우 커질 수 있다는 단점이 있다.

소유 기반 인증은 신분증, OTP 장치, 인증서와 같이 사용자가 소지하고 있는 물리적/논리적 객체를 기반으로 사용자를 인증하는 방식을 의미한다. 사용자가 반드시 소지해야 하므로 지식 기반 인증에 비해 보안성이 높으나, 객체를 발급받기 위한 절차가 까다롭고, 반드시 소유를 해야하기에 사용자의 불편함이 가중될 수 있다는 단점이 있다.

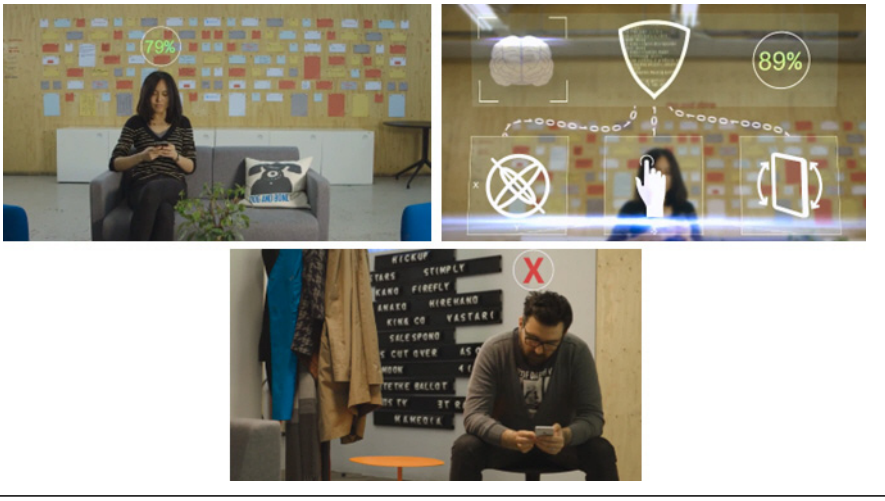
생체 기반 인증은 얼굴이나 홍채와 같은 사용자의 고유한 생체 정보를 통하여 사용자를 인증하는 방식을 의미한다. 생체 인식은 일반적으로, 얼굴, 음성, 지문, 홍채, 정맥 등 물리적 유형을 활용하지만, 최근들어 서명이나 키입력 패턴, 걸음걸이 등 행동적 유형을 활용한 인증 방식이 쓰이기도 한다. 생체 기반 인증은 복제가 쉽지 않으며, 사용자가 기억해야 하거나 별도의 인증용 객체를 소유하지 않아도 되므로 편의성이 높다. 대신, 인증 환경이나 장비 성능에 따라 인증 정확도가 떨어지거나 손가락을 다쳐 지문이 훼손되는 등 생체 정보가 변경되는 경우, 생체 정보의 재등록이 필요하기도 하다.

기존의 인증 방식은 사용자의 신원을 확인하기 위해서는 반드시 명시적 인증 절차를 거쳐야 한다. 명시적 인증이라 함은, 인증 방식에 따라 사용자에게 지식, 소유, 혹은 생체 정보를 확인하는 정의된 인증 프로토콜을 거치는 것을 의미한다. 이 과정에서 사용자의 불편함이 생기는 것은 피하기 어려우며, 한편으로 명시적 인증을 통과한 이후에는 (일반적으로, 일정 기간-세션 동안) 다시 신원 확인을 하지 않으므로 세션 가로채기 등의 공격을 당하는 경우 위험할 수 있다.

2) 미래 기술 수준

따라서, 인증 기술 분야에서는 무자각 지속 인증에 대한 논의와 연구가 진행되고 있다. 이는 사용자가 의식하지 않는 방식으로(무자각), 끊임없이(지속) 사용자를 인증하는 기술을 의미한다. 무자각 지속 인증이 가능해지는 경우, 앞서 언급한 명시적 인증의 문제점과 불편함이 해소될 수 있다.

〔그림 2-73〕 사용자의 행동 패턴에 기반한 무자각 지속 인증



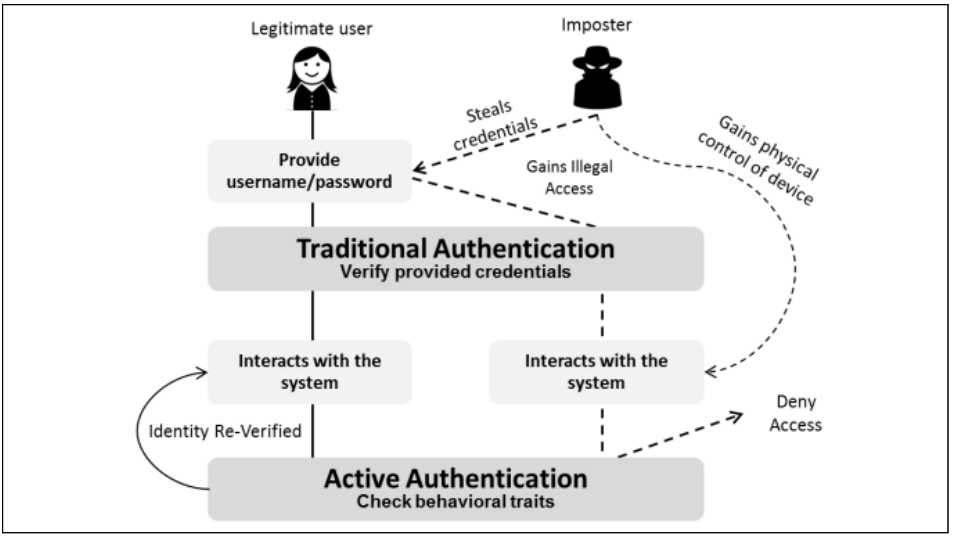
자료: https://zighra.com/

첫째, 지속적으로 사용자의 신원을 검증하는 과정이 존재하므로, Credential Stuffing과 같이 인증 방식을 불법적으로 통과하였거나, 명시적 인증 절차를 거친 인증 세션을 가로챈 해커라 하더라도, 지속적인 무자각 인증 과정을 통과하지 하지 못하도록 만들 수 있는 장점이 있다.

예를 들어, 컴퓨터로 특정한 응용 서비스에 아이디와 패스워드를 입력하여 로그인(지식 기반 명시적 인증)을 한 사용자가 있다고 가정하면, 이 사용자가 잠시 화장실을 가능 등 본인의 컴퓨터에서 멀어졌을 때, 근처에 있던 공격자가 해당 컴퓨터를 바로 사용함으로써 인증 세션을 가로챌 수 있으며, 이 과정에서 개인정보 및 데이터 유출, 서비스의 불법적 이용 등 다양한 공격이 가능해질 수 있다. 그러나, 만약 무자각 지속 인증이 가능하다면, 공격자가 지속 인증 과정을 통과하지 못함으로써 서비스 이용이 거부되거나 추가적인 명시적 인증을 요구받을 수 있다.

둘째, 인증 세션의 유효 기간을 늘림으로써 사용자는 불편함 명시적 인증 절차를 계속해서 요구당하지 않을 수 있다. 인증 세션은 일반적으로 유효 기간이 있으며, 이는 앞서 언급한 세션 가로채기 공격 등을 최소화하기 위한 목적이다. 그러나, 무자각 지속 인증이 가능하다면, 유효 기간을 무한대로 늘리지는 못하더라도, 현재 수준보다는 훨씬 길게 가져갈 수 있을 것이다. 이 경우, 사용자가 서비스를 이용하는 동안 요구받는 명시적 인증 절차의 횟수가 줄어들게 되어 그만큼 사용자의 서비스 이용 경험이 좋아질 것이다.

〔그림 2－74〕 기존 인증과 무자각 지속인증의 차이점



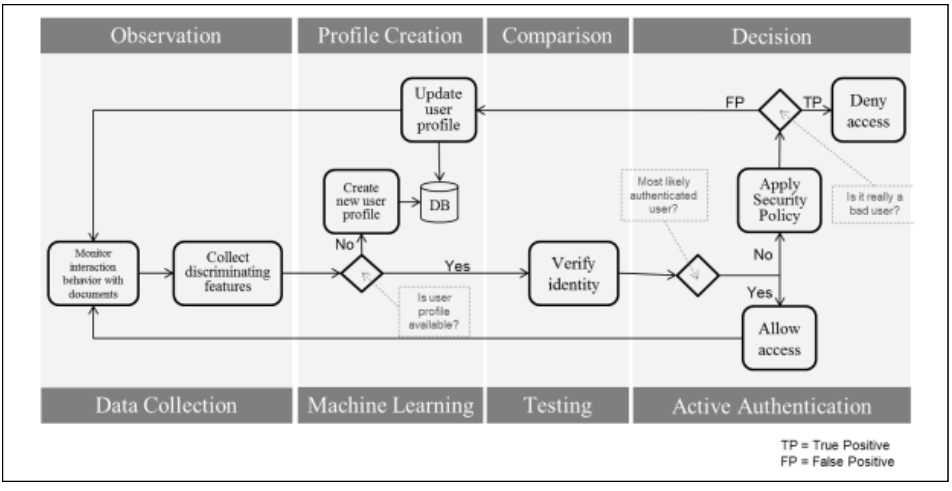
자료: A. Masri, "Active Authentication Using Behavioral Biometrics and Machine Learning", PhD Thesis, Goerge Mason University (2016)

3) 필요 기술

무자각 지속인증은 일반적으로 명시적 인증 과정을 거치지 않아야 하므로, 생체 기반 인증에서 행동적 유형을 활용하는 경우가 많다. 행동적 유형의 경우, 사용자의 고유한, 다른 사람과 구분되는, 그러나 일정하지 않은 행동을 기반으로 인증하여야 하므로 머신 러닝 기술을 활용하는 경우가 많다.

어떤 행동을 기반으로 인증을 수행하느냐에 따라 다를 수 있지만, 일반적인 머신 러닝과 같이 다음 그림과 같은 과정을 거친다.

〔그림 2-75〕 무자각 지속인증 기본 절차

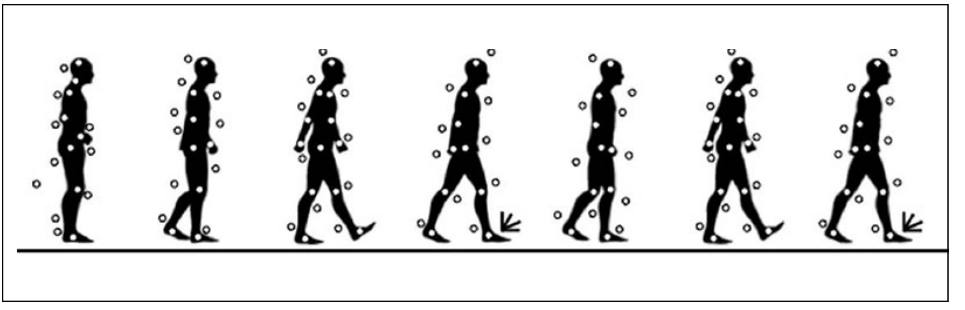


자료: A. Masri, "Active Authentication Using Behavioral Biometrics and Machine Learning", PhD Thesis, Goerge Mason University (2016)

관찰(Observation) 단계에서는 인증 시스템이 사용자와의 상호 작용을 통하여 무자각 인증에 활용하기 위한 사용자 특화된 속성 데이터를 수집하며, 프로파일 생성 단계에서는 이전에 상호 작용 과정에서 수집된 데이터를 이용하여 머신러닝 기반의 학습을 한다. 비교 단계에서는 사용자가 앞서 학습한 내용을 기반으로 현재 수집한 데이터와 비교함으로써 시험·검증하는 단계이며, 마지막으로 결정 단계는 실제 무자각 지속 인증을 하는 과정으로 현재 사용자에 대해서 데이터를 수집하면서 그 사용자가 맞는지를 결정내리고 문제가 있는 경우 서비스 이용을 중단시키는 등의 조치를 취하는 과정이다.

따라서, 이런 과정을 위해서는 효율적이고 정확도가 높은 머신러닝 기반의 인증 수단에 대한 연구가 필요하다. 현재 가장 많이 연구되고, 무자각 지속 인증에 부분적으로 활용되는 인증 방식으로는 얼굴(안면) 인식, 음성 인식, 걸음걸이, 키스트로크 다이나믹스, 마우스 다이나믹스, 터치 다이나믹스, 문체, 위치, 앱 사용습관 등이 가능하다. 어떤 인증 방식을 사용할 지는 앱이나 응용에 따라 해당 응용 환경에서 인식 가능한 생체 정보의 종류, 정확도, 사용자의 편의성에 따라 달라질 것이다.

〔그림 2－76〕 걸음걸이 기반 인증 (Gait Recognition)



자료: https://www.bayometric.com/gait-recognition-identify-with-manner/

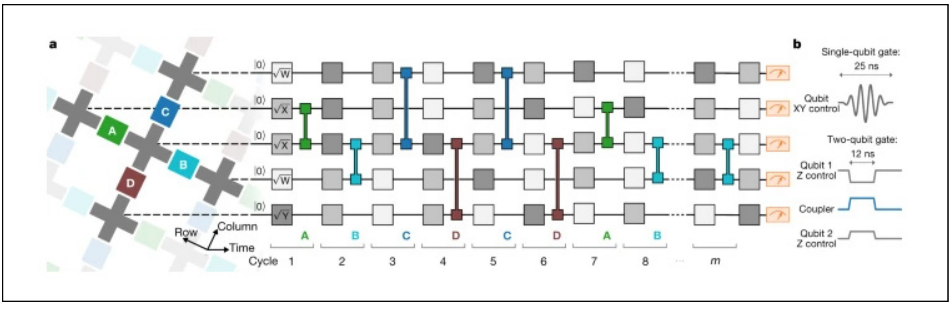
나. 양자 위협에 노출된 암호 → 양자 위협에 대비한 암호

1) 현재 기술 수준

1980년대 초반 R. Feynman 등에 의해 이론적으로 제안된 양자 컴퓨터는, 당시 컴퓨터로 진행하던 양자역학 시뮬레이션 연구를 보다 빠르게 할 수 있는 기술적 방법을 찾고자 하는 의도에서 제안된 것이다. 그러나, 1994년 P. Shor에 의해 대규모 큐비트(논리 수준에서 대략 4,000~10,000큐비트 수준)를 갖는 양자컴퓨터가 만들어진다면, 현재 ICT 보안에서 필수적인 공개키 암호 알고리즘인 RSA, DH, ECC 등이 깨진다고 이론적으로 증명되었다.

이 당시만 하더라도, 대규모 큐비트를 갖는 양자 컴퓨터의 실현이 가능한지 조차 불분명 하였으나, 최근 수년간 구글과 IBM, IonQ, Rigettie 등 수많은 글로벌 기업들의 연구 개발에 힘입어 엄청난 기술적인 진보가 있었으며, 현재도 이러한 진보는 계속되고 있다. 구글은 2019년 10월 네이처 저널의 발표를 통하여, 자사의 53큐비트 양자컴퓨터 Sycamore를 이용하여 최초로 양자우월성을 달성하였다고 발표한 바 있다.

〔그림 2－77〕 양자 우월성을 달성한 양자 회로에서의 제어 연산



자료: https://www.bayometric.com/gait-recognition-identify-with-manner/

작년 IBM은 초전도 방식의 127큐비트 양자 큐비트칩을 개발했다고 발표하였으며, 2023년 1,121 큐비트, 2025년 4,158 큐비트 양자 큐비트칩을 개발하고자 하는 로드맵을 공개한 바 있다. IonQ는 이온 트랩 방식으로 32큐비트를 갖는 양자 큐비트칩을 개발하여 공개하였다.

앞서 2장에서 언급하였던 바와 같이, Mosca의 부등식으로 유명한 M. Mosca는 2015년 RSA-2048이 2026년까지 깨질 확률이 1/7, 2031년까지 깨질 확률은 1/2라고 주장한 바 있으며, 최근 M. Mosca는 자신의 리포트에서 관련 전문가들로부터 조사하여 〔그림 2－78〕과 같은 결과를 얻은 바 있는데, 이 조사에 따르면 향후 15년 정도(2037년) 후에 깨질 확률이 1/2 정도로 예상할 수 있으며, 적어도 30년 후(2052년)에는 응답자의 87%가 RSA-2048이 깨질 확률을 50% 이상, 응답자의 35%는 99%이상의 확률로 깨진다고 예측하였다.

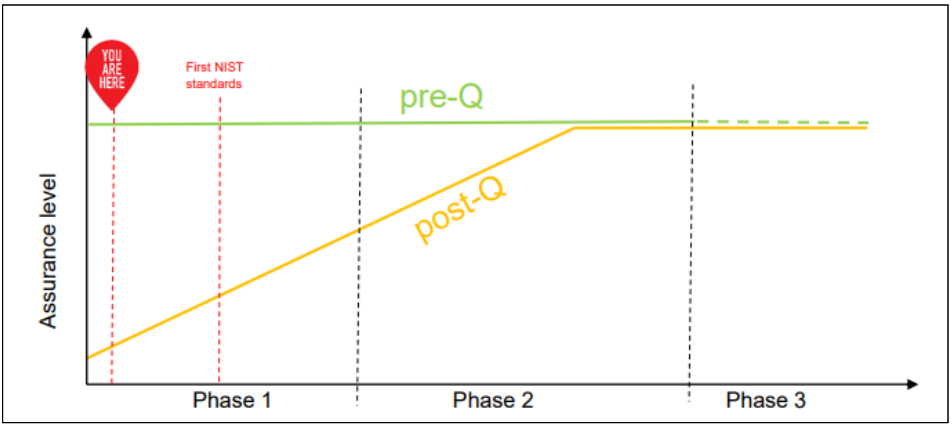
따라서, 현재 사용중인 RSA, ECC 등에 대하여 대규모 큐비트를 갖는 양자 컴퓨터 환경에서도 안전한 암호의 개발은 필수적이며, 이들에 대한 연구는 1990년대 후반부터 진행되어 암호학자들을 중심으로 논의되어 왔다. 2017년, NIST에서 양자내성암호(PQC, Post-Quantum Cryptography) 표준화를 진행하였으며, 2022년 7월 표준 알고리즘 4종을 선정하고 표준안 작업을 진행 중이다.

그러나, 표준화가 되었다고 해서 바로 사용할 수 있는 것은 아니다. 현재 ICT 환경에서는 TLS/DTLS와 같은 암호 프로토콜, 혹은 응용에서 암호 알고리즘을 사용하고 있는데, 공개키 기반 암호가 필요한 경우 거의 대부분 RSA, ECC, DH 등의 기술을 사용하고 있다. 따라서, 기존 공개키 암호 알고리즘을 걷어내고 새로운 PQC 표준 암호 알고리즘을 도입하여야 하는데, 이를 PQC 전환(Transition)이라고 부른다.

2) 미래 기술 수준

앞서 언급한 PQC 표준 암호를 기존 ICT 환경에서 사용 중인 암호 프로토콜 및 응용에서 활용하게 된다면, 양자 컴퓨터의 위협에도 관계없이 공개키 암호를 사용할 수 있게 될 것이다.

〔그림 2－78〕 PQC 전환의 3단계



자료: M. Rossi, "PQC Transition ANSSI View" (2021)

PQC 전환은 위 그림과 같은 3단계의 과정을 거칠 것으로 보인다. 첫 번째 단계에서는 전환 과정을 시작하여 양자 내성 안전성에 최선을 다하는 단계이다. 양자내성암호와 일반 암호는 공존하고 있으며 일부에서는 하이브리드 형태로 사용할 가능성도 있다. 이 단계에서 첫 번째 NIST 표준이 확정되어 사용자들이 서서히 표준암호를 도입하게 될 것이다. 일부에서는 여러 가지 이유로 표준화에 성공하지 못한 암호를 사용할 가능성도 있다.

두 번째 단계는 요구사항을 강화하여, 보안 제품들에서 양자내성암호의 사용이 강제되기 시작할 것이다. 점점 양자내성암호 사용의 비율이 높아지고, 많은 분야에서 기존 공개키암호가 대체될 것이다. 하드웨어/소프트웨어를 업데이트하기 어려운 일부 분야(예, 오래된 산업제어 장비 등)에서만 기존 공개키 암호가 사용되고 있으나, 그 비중이 매우 적을 것이다.

세 번째 단계는 하이브리드 사용이 없어지고, 기존 공개키암호가 거의 사라져 가는 단계이다. 절대 다수의 보안 제품에서 양자내성을 갖는 것이 필수요구사항이 될 것이며, 극소수의 기존 암호가 남아 있을 가능성이 높다. 이 시기에 양자컴퓨터에 의해 실제로 RSA 등의 암호가 깨질 가능성이 있으며, 그럼에도 극히 일부를 제외하면 RSA가 깨지는 것에 영향을 받지 않을 것이다. 양자 컴퓨터는 암호를 깨기 위한 것이 아니라, 양자 AI, 양자역학 시뮬레이션, 양자 최적화 알고리즘 등 독자적인 영역을 개척하여, 널리 사용되고 있을 것이다.

3) 필요 기술

양자 보안성을 갖는 공개키 암호 기술로는[3], 양자 암호와 양자내성암호가 언급되고 있으나, 양자 암호는 공개키 암호를 대체하기 위하여 나온 기술은 아니다. 또한 Point-to-Point 보안 방식으로 키교환 기능만 제공 가능하며, 공개키 암호를 통해 가능한 공개키 기반 암호화, 전자 서명 등은 현재까지는 불가능하다. 따라서, 양자 암호는 해당 기술이 필요한 특정 분야에서 활용될 것으로 보이며, 현재 공개키 암호가 사용되는 영역은 모두 양자내성암호가 대체하게 될 것이다.

예컨대, 현재 ICT 환경에서 가장 많이 사용되는 보안 프로토콜은 TCP 계층에서 인증과 메시지 보호 기능을 제공하는 TLS(Transport Layer Security)이다. TLS 현재 버전에서의 키교환 및 인증 과정에서는 여전히 기존 ECC 및 RSA 암호가 사용된다. 그 외에도 특정 분야의 네트워크 혹은 응용에서는 별도의 보안 기법들을 사용하기도 하는데, 예를 들어, 자동

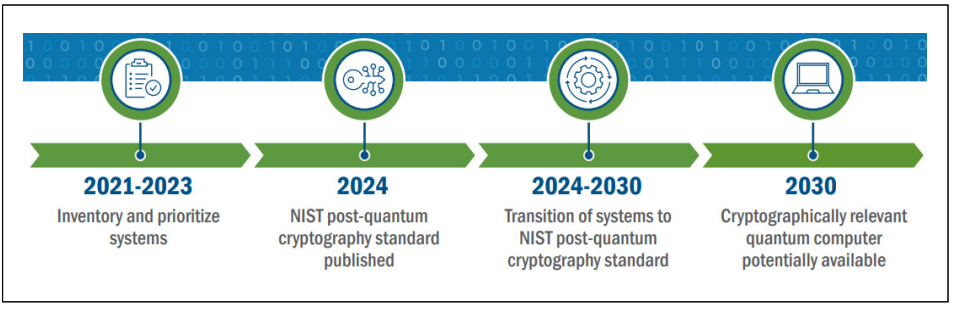
3) 대칭키 암호 및 해시 알고리즘과 같은 암호 기술은 대체로 양자저항성을 유지한다. Grover 양자 알고리즘 등으로 공격을 받더라도, 키 길이 혹은 해시 길이를 조절하는 선에서 해결될 것이다.

차간 통신에서 활용되는 IEEE 1609.2에서는 ECDSA 기반 전자서명 기술이 필수이다.

따라서, 이러한 예에서는 앞서 언급한 바와 같은 PQC 전환 과정이 필요한데, 이는 단순히 암호 알고리즘의 교체로 끝이 나는 것이 아니다. 키 길이, 암호화 및 서명메시지 구조 등이 모두 달라지고, 암복호화 및 서명 속도와 메모리 사용량 등 역시 달라지므로, 이러한 점을 고려한 별도의 프로토콜 설계가 필요할 수 있으며, 특정 하드웨어에서는 새로운 암호를 동작시키기에 성능이 부족할 수도 있다.

PQC 전환은 긴 시간에 걸쳐 이루어질 것으로 보이며, 비교적 프로토콜 구성과 성능 면에서 유연하고 여유로운, 일반적인 인터넷 영역에서 가장 먼저 적용될 가능성이 높다. 임베디드, IoT, 저속 통신 환경, 산업제어 등 특수 영역은 PQC 전환 속도가 다소 느릴 수 있으나, 최소한 양자 공격이 현실화되기전에 어느 정도 이루어질 수 있도록 연구개발과 실증이 필요할 것이다.

〔그림 2－79〕 PQC 전환을 위한 준비 과정



자료: NIST, “Preparing for Post-Quantum Cryptography” (2021)

다. IT 중심 보안 → OT가 통합된 융합 보안

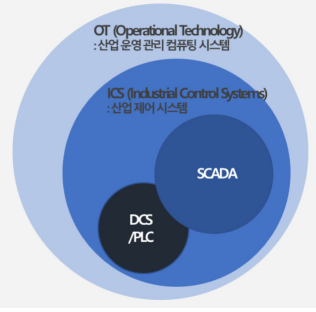
1) 현재 기술 수준

디지털 트랜스포메이션(Digital Transformation, DX)이 화두가 되면서 다양한 분야에 ICT 기술이 적용되어 기존의 전통적인 운영 방식 및 서비스를 혁신해 나가고 있다. 사이버 보

안의 대상 역시 기존에는 IT(Information Technology) 시스템이 대부분이었으나 최근 들어 OT(Operational Technology) 시스템을 대상으로 하는 공격이 늘어나면서 OT 시스템 보안 역시 주목받고 있다.

OT는 아래 그림과 같이 ICS(Industrial Control System, 산업제어시스템), SCADA (Supervisory Control And Data Acquisition, 작업공정 감시/제어 및 데이터 수집), DCS (Distributed Control System, 분산제어시스템), PLC(Programmable Logic Controller, 프로그램 가능한 제어기) 등 산업용 기계 및 공정 운영을 모니터링하고 설비를 직접 제어하기 위한 모든 기술 및 시스템을 포괄하는 개념을 의미한다.

〔그림 2－80〕 OT 관련 용어 개념 및 구성



구분	내용
OT	• Operational Technology, 산업운영관리 컴퓨팅 시스템 • ICS, SCADA 등을 포괄하는 산업용 기계, 공정 운영을 위한 기술 및 시스템
ICS	• Industrial Control System, 산업제어시스템 • 공장이나 시설의 각종 기계나 공정을 제어하기 위한 시스템
SCADA	• Supervisory Control and Data Acquisition, 작업공정 감시/제어 시스템 • HMI(Human-Machine Interface), PLC 등을 포함하며 공정시설과 설비를 제어하기 위해 원격제어시스템/통신시설 기반의 산업제어 및 감시 시스템
DCS	• Distributed Control System, 분산제어시스템 • 자동제어프로그램이 내장 된 제어용 컴퓨터를 기능별로 분산시켜 중앙관리 및 제어를 하는 시스템
PLC	• Programmable Logic Controller, 프로그램된 제어장치 • 산업플랜트의 자동 제어 및 감시에 사용하는 제어시스템

자료: 이글루시큐리티, OT 보안을 위한 넓고 얕은 지식, https://www.igloo.co.kr/security-information/ot-%EB%B3%B4%EC%95%88%EC%9D%84-%EC%9C%84%ED%95%9C-%EB%84%93%EA%B3%A0-%EC%96%95%EC%9D%80-%EC%A7%80%EC%8B%9D/

OT 시스템이 자동화 및 디지털화되고 많은 부분이 인터넷에 연결되면서 OT 시스템을 대상으로 하는 사이버 공격 역시 빈번해지고 있다. 아래 그림은 그동안 발생한 OT 시스템 사이버 보안 사고 사례를 나타낸다.

〔그림 2－81〕 OT 시스템 사이버 보안 사고 사례

구분	공격 대상	공격기법	내용 요약
2021.06	미국 송유관 업체 (콜로니얼 파이프라인)	Darkside 랜섬웨어	- 미국 남동부 8,851KM송유관 가동 중단 - 미 남동부지역 석유가 고갈 사태 발생 되어 항공 운항 변경, 석유가격 급등
2020.12	미국 시스템 모니터링 SW (솔라윈즈 오리온)	SUNSPOT, SUNBURST 악성코드	- 솔라윈즈 오리온 IT 모니터링/관리 SW가 백도어 감염되어 업데이트를 통해 전파 - IT기업, 미 정부(국방부, 국토안보부, 상문, 재무부 등 포함), NGO, 각종 단체 등 3만 3천개 사의 시스템이 감염
2020.06	일본 자동차 공장 (혼다)	Snake(EKANS) 랜섬웨어	- 감염 시 OT 관련 SW 프로세스를 종료 후 파일을 암호화 - 내부 시스템 네트워크 장애, 생산라인 관리 시스템 장애, 완성차 출하 중단
2019.03	노르웨이 알루미늄 생산 공장 (Norsk Hydro)	Locker Goga 랜섬웨어	- 랜섬웨어로 인해 공장 시스템 데이터가 암호화되어 생산/운영 차질 - 전세계 알루미늄 가격 상승
2018.08	대만 반도체 생산 공장 (TSMC)	Wanna Cry 랜섬웨어	- 새로 도입된 설비에SW 설치 과정에서 USB를 통해 랜섬웨어 감염 - 하루동안 일부 생산라인 가동 중단
2017.06	사우디 아라비아 정유 공장	Triton 악성코드	- Schneider 시스템의 취약점을 이용하여 ESD(안전 중단 시스템, Emergency Shutdown)의 중단 - 시스템 사고 발생시 안전 장치 동작이 불가하여 시설 파괴 및 인명 피해를 포함한 재해 발생 가능
2016	우크라이나 전력망 공격	KillDisk / industroyer 악성코드	- 키예프의 3곳의 배전 회사 IT 시스템을 공격 - 변전소와 전기 연결이 중단되어 225,000 가구가 피해 발생
2010	이란 원자력 시설	stuxnet 악성코드	- USB 스틱으로 밀반입된 것으로 추정 - SCADA를 표적으로 하여 이란의 한 시설에서 우라늄 농축에 사용되는 원심분리기를 파괴

자료: LG CNS 블로그, [OT보안] DX 시대, 이젠 OT/ICS 보안도 달라져야 할 때! 1편, https://blog.lgcns.com/2704

이와 같이 OT 시스템을 대상으로 하는 사이버 공격이 꾸준히 늘어나고 있음에도 불구하고 이와 관련한 연구는 아직 초기 단계에 머물러 있는 수준이다. 아래 표에서 볼 수 있다시피 OT 시스템은 IT 시스템과 많은 부분에서 차이가 있기 때문에 OT 시스템 환경에 맞는 사이버 보안 기술에 대한 연구가 필요하다.

〈표 2-13〉 IT 시스템과 OT 시스템 비교

구분	IT 시스템	OT 시스템
보안우선순위	기밀성 > 무결성 > 가용성	가용성 > 무결성 > 기밀성
성능 요구	실시간, 배치 등 다양화	실시간, 준 실시간(Near-realtime)
가용성	재시작 허용, 상대적으로 낮음	고가용성 요구, 계획된 중단만 허용
보호대상	정보, 핵심 IT자산	설비, 프로세스, 필드장치 등
시스템 운영체계	범용 운영체제(Windows, Linux)	전용 운영체제
생애주기	3 ~ 5년	15 ~ 20년
통신	표준 프로토콜(TCP/IP)	전용 프로토콜
SW 변경관리	보안정책에 따라 자동 적용	사전 시험 후 점진적 적용, 계획된 정지시기에 적용
접근용이성	지역에 국한, 접근 용이	넓은 영역에 퍼짐(SCADA), 물리적 접근 노력 필요

자료: 김경호, 산업제어시스템 보안, 주간기술동향 1981호 - 정보통신기획평가원

2) 미래 기술 수준

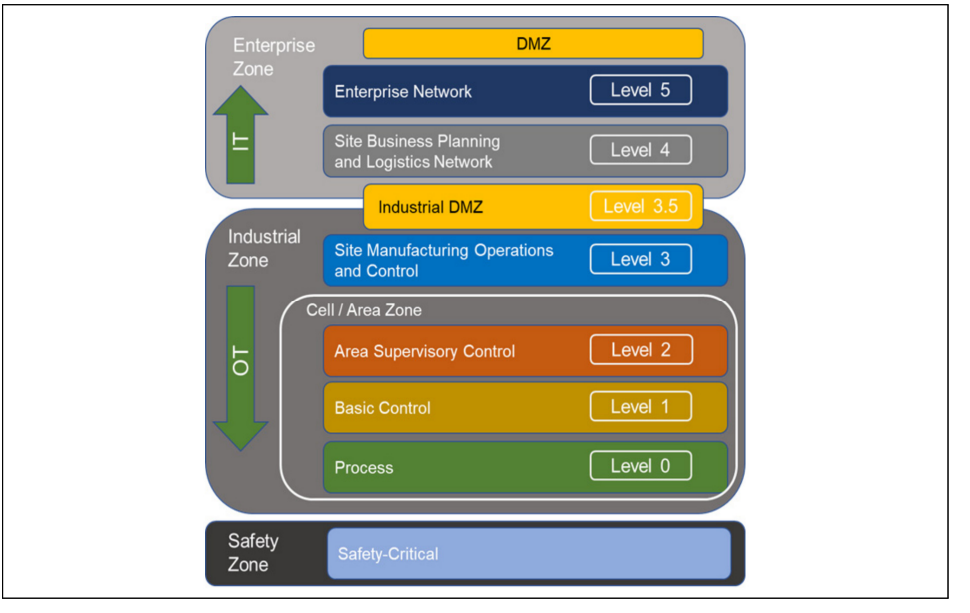
4차 산업혁명의 등장으로 기존 제조산업에 ICT 기술이 결합되면서 스마트 팩토리(Smart Factory)와 같은 지능화된 공장이 더 많이 생겨날 것으로 기대된다. 이에 따라 공격자가 인터넷을 통해 OT 시스템에 접근할 수 있는 경로가 더 많아질 것이며, 심지어는 망분리를 통해 에어 갭(Air-gap)을 만들어도 이를 우회하기 위한 다양한 방법이 개발되고 있어 이에 대한 대비가 필요한 상황이다.

이에 대응하여 OT 시스템 보안에 대한 관심이 증가하고 있으며 이와 관련한 학계의 연구 및 기업의 투자가 다양하게 이루어지고 있다. 시간이 지남에 따라 OT 환경에 대한 이해가 깊어지면서 OT 환경에 맞는 사이버 보안 관리체계 및 솔루션들이 개발되고 도입되면 OT 보안도 IT 보안과 비슷한 수준 또는 그 이상으로 제공이 가능할 것으로 보인다. 이를 통해 기존 IT 중심의 보안에서 OT가 통합된 융합 보안이 사이버 보안의 중심이 되리라 기대하고 있다.

3) 필요 기술

OT 환경에서의 보안 위협을 파악하고 이에 대응하기 위해서는 OT 시스템 아키텍처 및 이를 구성하는 요소들에 대한 이해가 있어야 한다. OT 시스템 아키텍처를 설명하기 위해 가장 많이 사용하는 모델이 PERA(Purdue Enterprise Reference Architecture) 모델이다. PERA 모델은 시스템을 계층으로 나누어 이해하기 쉽게 구성한 참조 모델로, 이를 기반으로 ISA(International Society of Automation) 99 표준 및 IEC(International Electrotechnical Commission) 62443 산업 사이버 보안 프레임워크가 개발되었다. 아래 그림은 PERA 모델을 기반으로한 OT 시스템 아키텍처이다.

〔그림 2－82〕 PERA 모델을 기반으로 한 OT 시스템 아키텍처



자료: 김경호, 산업제어시스템 보안, 주간기술동향 1981호 - 정보통신기획평가원

OT 시스템 보안에 대한 관심이 증가하면서 관련하여 아래 표에서와 같이 다양한 표준이 발표되었다. 이 중 ISA/IEC 62443, NIST CSF, NIST 800-82가 OT 시스템 보안을 위해 많이 활용된다.

〈표 2-14〉 OT 시스템 보안 관련 표준 및 가이드라인

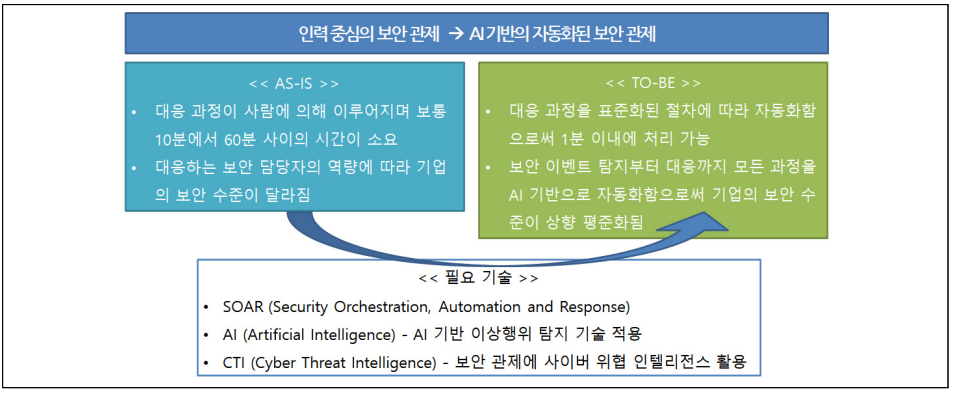
표준	설명	표준	설명
ISA/IEC 62443	산업망 네트워크 및 시스템 보안	NIST CSF	사이버보안 프레임워크
NAMIURA NA 115	산업자동망 시스템 IT 보안	NIST 800-82	산업제조시스템 보안 가이드
ISO 27000	정보보호관리시스템 국제 표준 체계	NIST 800-83	정보 및 개인정보 보호 통제
VDI/VDE 2182	산업자동화를 위한 정보보안	CRR(Cyber Resilience Review)	운영 회복성과 사이버보안 실행력 평가 방안

자료: 김경호, 산업제어시스템 보안, 주간기술동향 1981호 - 정보통신기획평가원

OT 시스템 보안 관련하여 연구 중인 대표적인 기술에는 제어시스템과 외부 인터넷망의 연결을 완전히 차단하기 위한 물리적 단방향 보안게이트 기술과 서로 다른 도메인 사이에 안전한 정보 전달을 위한 CDS(Cross Domain Soultion) 기술이 있다. 국가정보원의 국가 정보보안 기본지침과 과학기술정보통신부고시 제2021-103호 주요정보통신기반시설 취약점 분석·평가 기준에 따르면 주요 정보통신 기반시설의 제어시스템은 인터넷망 및 업무망과 물리적인 망분리를 통해 차단하는 것이 필수적이기 때문에 물리적 단방향 보안게이트 기술은 중요하다고 볼 수 있다.

라. 인력 중심의 보안 관제 → AI 기반의 자동화된 보안 관제

〔그림 2－83〕 보안 관제 기술발전 시나리오



1) 현재 기술 수준

현재 인력 중심으로 이루어지는 보안 관제는 대응 과정이 사람에 의해 이루어지기 때문에 보통 10분에서 60분 사이의 시간이 소요되며 대응하는 보안 담당자의 역량에 따라 조직의 보안 수준이 달라진다. 이와 같이 시간이 오래 걸리며 보안 담당자의 역량에 의존하는 방식의 보안 관제는 갈수록 지능화되고 복잡해지는 사이버 위협에 대응하기에 적합하지 않다고 볼 수 있다.

2) 미래 기술 수준

앞으로의 보안 관제는 AI 기반으로 자동화되어 대응 과정을 표준화된 절차에 따라 자동화함으로써 1분 이내에 처리할 수 있어야 하며 보안 이벤트 탐지부터 대응까지 모든 과정을 AI 기반으로 자동화함으로써 기업의 보안 수준을 상향 평준화할 수 있어야 한다.

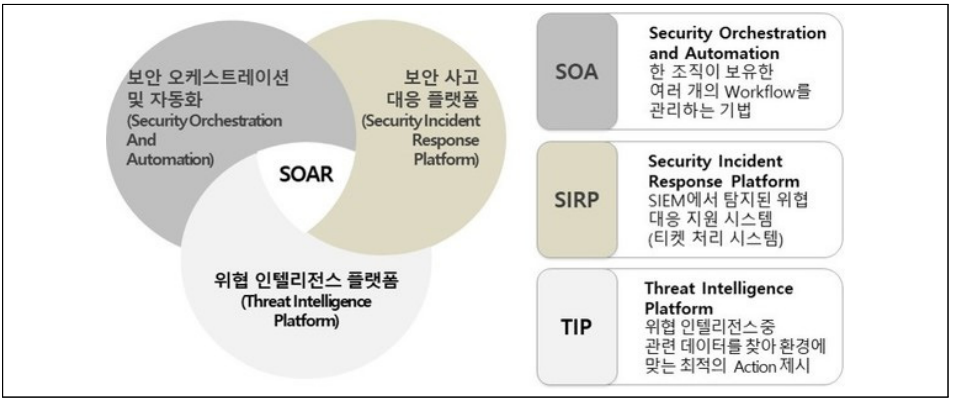
3) 필요 기술

AI 기반의 자동화된 보안 관제를 위해서 필요한 기술로는 SOAR (Security Orchestration, Automation and Response), AI (Artificial Intelligence), CTI (Cyber Threat Intelligence) 등이 있다.

SOAR은 보안 위협에 대한 대응 프로세스를 자동화하여 보안 업무의 효율성을 높이는

솔루션으로 아래 그림과 같이 보안 오케스트레이션 및 자동화(Security Orchestration and Automation, SOA), 보안 사고 대응 플랫폼(Security Incident Response Platform, SIRP), 위협 인텔리전스 플랫폼(Threat Intelligence Platform, TIP)으로 구성된다. 보안 오케스트레이션 및 자동화는 조직이 보유한 여러 개의 워크플로우(Workflow)를 관리하며 보안 대응팀의 단순하고 반복적인 업무를 파악하여 효율성을 높임으로써 업무에 소요되는 시간을 단축시킨다. 보안 사고 대응 플랫폼은 보안 사고가 발생했을 때 사고 유형별로 보안 사고 대응 정책에 의해 미리 정해진 프로세스에 따라 누가 어떠한 업무를 수행해야 하는지를 알려준다. 위협 인텔리전스 플랫폼은 사이버 위협 인텔리전스(CTI)를 분석하여 관련 데이터를 찾아 현재 상황에서 수행해야 할 최적의 행동을 제시한다.

〔그림 2－84〕 SOAR 개념 및 구성 요소



자료: 투이컨설팅, 보안 관제의 디지털 탈바꿈, SOAR의 개념과 주요 기능, https://www.2e.co.kr/news/articleView.html?idxno=300903

보안 관제 업무 자동화의 완성도를 높이기 위해 SOAR에 AI 기술이 적용되는 것은 필연적이다. 현재 많은 보안 관제가 IPS(Intrusion Prevention System, 침입 차단 시스템)나 TMS(Threat Management System, 위협 관리 시스템) 중심으로 운영 중이며 매일 수십만 건 발생하는 경고를 하나하나 관제 요원이 분석하는 것은 불가능하다. SOAR에 AI 기반 이상행위 탐지 기술을 적용함으로써 경고의 정/오탐 여부를 판단하는데 드는 부담을 줄임으로써 큰 도움이 될 수 있다.

제3장 사이버 보안 정책 현황과 미래 전략

제1절 보안 위협 대응 정책 현황과 미래 전략

1. 사이버 보안 위협 현황

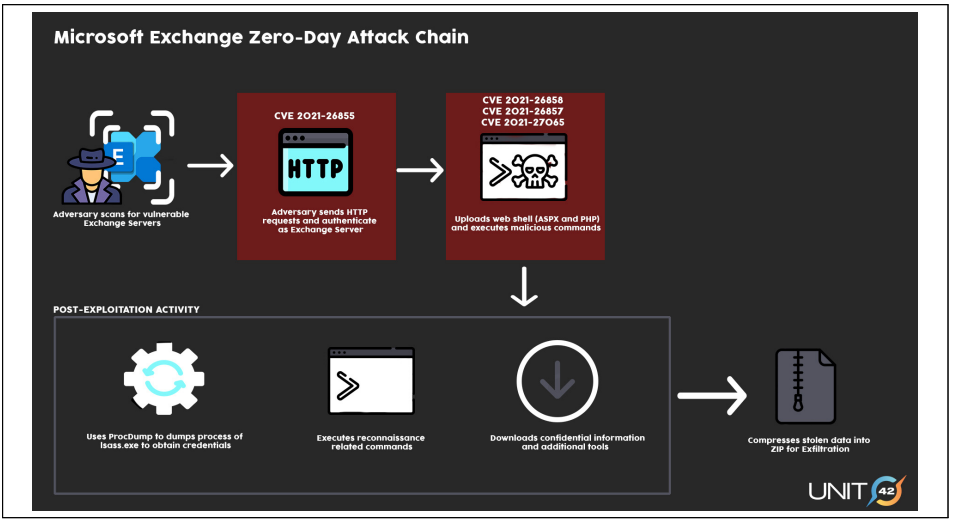
2022년 6월 국가정보원이 과학기술정보통신부, 행정안전부, 개인정보보호위원회, 금융위원회, 외교부 등과 함께 발간한 2022 국가정보보호백서에 따르면 사이버 보안 위협 관련하여 최근 다음과 같은 이슈들이 주목받고 있다.

가. 국경을 넘은 공급망 공격과 첨단기술 탈취 심화

국가기반시설 또는 주요 사회 인프라를 대상으로 한 사이버 공격의 강도와 빈도가 지속해서 증가하는 추세이다. 게다가 개인이나 소규모 조직이 아닌 국가가 배후에서 지원하는 단체가 이러한 공격을 주도하며 고도화된 지능형 지속 공격(Advanced Persistent Threat, APT) 기법을 통해 공격을 수행함으로써 이에 대한 대응이 쉽지 않은 상황이다. 지능형 지속 공격은 기존 불특정 다수를 대상으로 한 공격과는 다르게 하나의 대상만을 표적으로 삼아 침입에 성공하기까지 오랜 시간에 걸쳐 은밀하게 다양하고 복잡한 방법으로 공격을 시도한다.

2021년 발생한 대표적인 사건으로 2월 미국 플로리다주의 수처리 시설을 해킹하여 상수도에 유독물질 유입을 시도하였던 공격과 3월 마이크로소프트 익스체인지 서버를 대상으로한 제로데이 공격이 있다. 수처리 시설 공격의 경우 대응이 늦어졌을 경우 몇만 명의 인명피해로까지 이어질 수 있었으며 익스체인지 서버 공격의 경우 아래 그림과 같은 과정을 통해 이루어져 사건 초기 약 3만 개의 기관과 기업이 공격 대상이 된 상당히 심각한 사건이었다.

〔그림 3-1〕 마이크로소프트 익스체인지 제로데이 공격 과정



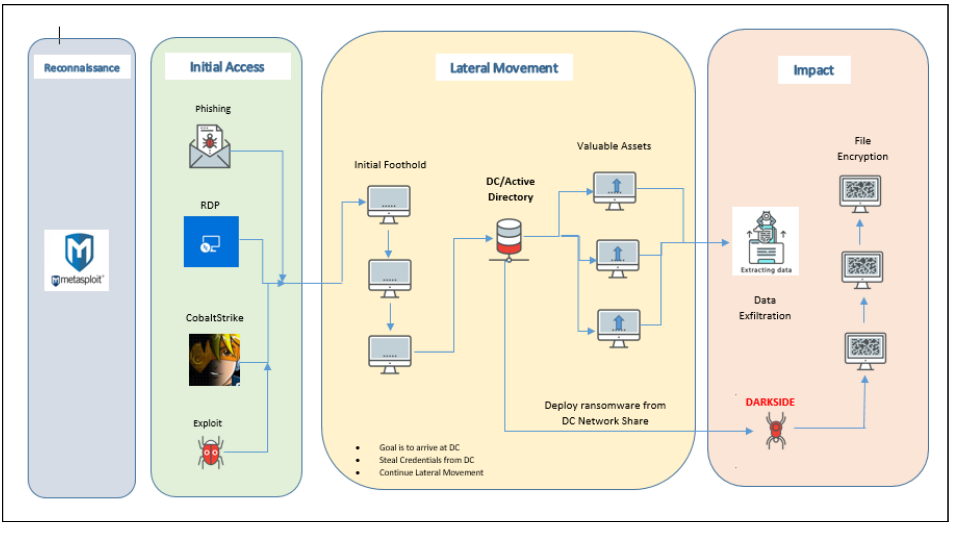
자료: Threat Assessment: Active Exploitation of Four Zero-Day Vulnerabilities in Microsoft Exchange Server, https://unit42.paloaltonetworks.com/microsoft-exchange-server-vulnerabilities

나. 랜섬웨어 조직의 진화와 공격 대상 확장

랜섬웨어 공격은 서버 시스템 및 단말기 등에 무단 침입하여 백업시스템 삭제, 중요 데이터 암호화 또는 탈취를 통하여 시스템에 접근할 수 없도록 한 후, 복구를 위한 금전적 데이터를 요구하는 사이버범죄이다. 이러한 랜섬웨어 공격의 대상이 2015년 초 PC 단말기에서 시작하여 데이터가 저장된 서버 인프라를 거쳐 2021년부터는 인공지능과 IoT, 스마트공장, 공급망 시스템 등으로 계속하여 확대되고 있다.

2021년 발생한 대표적인 사건으로 세계 최대 육가공 업체 JBS Foods에 대한 레빌(Revil) 랜섬웨어 공격과 미국 최대 송유관 관리업체 콜로니얼 파이프라인을 대상으로 한 다크사이드(Darkside) 랜섬웨어 공격이 있다. JBS Foods에 대한 랜섬웨어 공격으로 미국, 오스트레일리아, 캐나다 등에 위치한 생산 시설의 운영이 중단되었으며 콜로니얼 파이프라인의 경우 아래 그림과 같은 과정을 거쳐 감염되어 사건 당일 비트코인으로 약 440만 달러어치를 송금하여 복호화 코드를 확보하였음에도 불구하고 약 6일간 운영에 차질을 겪어 연료 가격이 상승하는 등 사회, 경제적인 피해도 발생하였다.

〔그림 3-2〕 다크사이드 랜섬웨어 감염 과정



자료: Darkside Ransomware Information, https://success.trendmicro.com/dcx/s/solution/000286466?language=en_US&sfdcIFrameOrigin=null

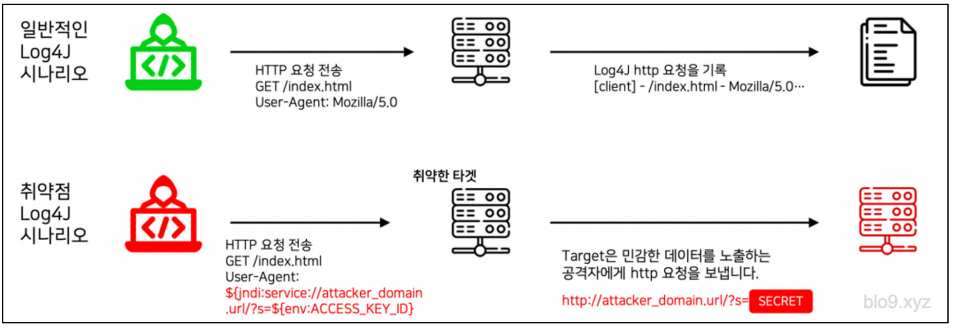
다. Log4j 등 오픈소스 프로그램의 심각한 보안 취약점 노출

오픈소스는 누구나 공개적으로 접근하여 자유롭게 활용할 수 있는 프로그램으로 높은 효율성으로 인하여 개발 과정에서의 활용이 보편화되고 있는 추세이다. 하지만 오픈소스를 기반으로 개발한 소프트웨어는 각 구성요소의 정확한 추적관리가 매우 어렵고 일괄적인 문제 해결이 힘들기 때문에 보안 취약점 노출과 같은 문제가 발생하였을 때 피해가 커질 수 있다.

2021년 발생한 대표적인 사건으로 Log4j 보안 취약점이 있다. Log4j는 자바 기반 프로그램을 개발할 때 로그 기록을 위해 사용되는 가장 유명한 오픈소스 라이브러리이다. Log4j는 로그를 기록할 때 조직 내부 자원에 접근하는 기능을 가지고 있는데 이는 필요 이상으로 높은 권한이었으며 수행 명령 출처에 대한 유효성도 검증하지 않아 문제가 되었다. 공격자는 이를 통해 아래 그림과 같이 원하는 원격 코드를 실행시킬 수 있었으며 Log4j는 오픈소스이기 때문에 각 조직에서 Log4j를 사용하는 서드파티(3rd-party) 제품이 있는지 여

부를 식별하는 것이 힘들어 신속한 대응에 어려움이 있었다. 또한 Log4j 취약점 발견 초기에는 해당 취약점을 통해 침입한 경우 남는 흔적인 IoC(Indicator of Compromise, 침해지표)가 명확하지 않아 침입 여부를 확인하는데 있어서도 어려움이 있어 더욱 문제가 되었다.

〔그림 3－3〕 Log4j 취약점 시나리오



자료: 김현구, “Apache Log4j 취약점 (CVE-2021-44228, CVE-2021-45046, CVE-2022-23302, CVE-2022-23305, CVE-2022-23307)”, http://blo9.xyz/2021/12/11/Security/Anlaysis/cve/CVE-2021-44228

라. 스마트홈·IoT 기기와 통합 관리의 취약성

인공지능 스피커, 로봇 청소기 등 스마트홈·IoT 기기의 사용이 증가하고 있지만 이들은 주로 편의성에만 집중할 뿐 높은 권한에 비해 보안에 대한 고려가 부족해 다양한 보안 위협의 대상이 될 수 있다.

2011년 발생한 대표적인 사건으로 11월 아래 그림과 같이 국내 아파트로 추정되는 집안 내부를 불법 촬영한 영상이 대량 유출된 사건이 있다. 공격자는 아파트 각 세대 사이 영상통화 목적으로 삽입된 월패드 카메라를 해킹하여 가장 민감한 개인정보라고 할 수 있는 집안 사생활을 적나라하게 노출하였다.

〔그림 3－4〕 온라인 커뮤니티에서 공유된 국내 아파트 월패드 해킹 영상

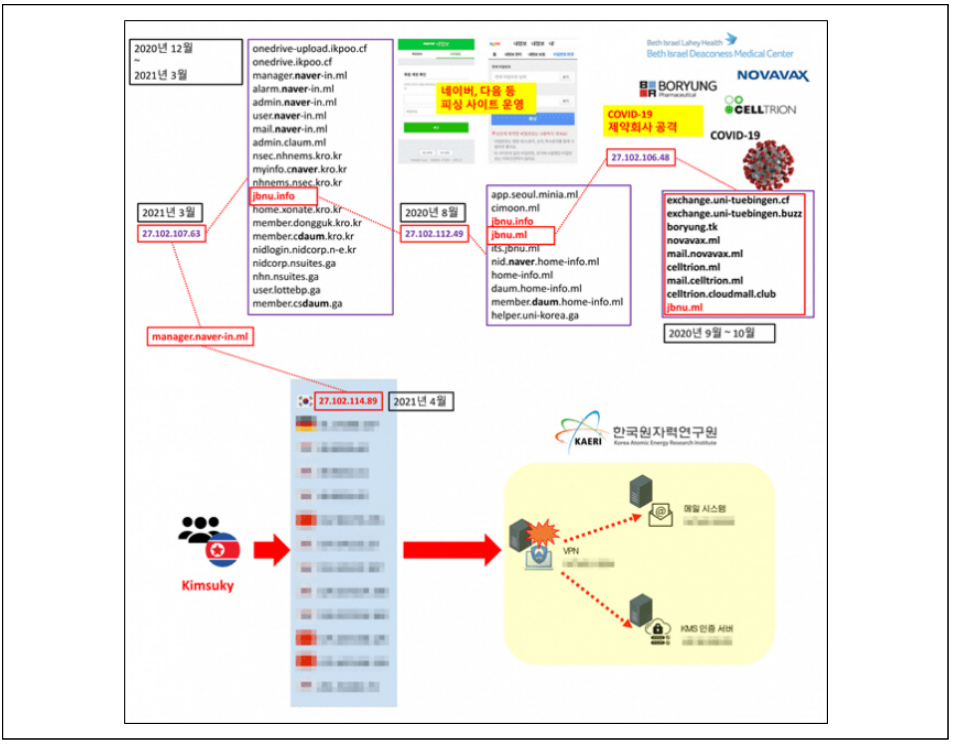
자료: 머니투데이, “집안 사생활 다 보고 있었다... 아파트 월패드 해킹 이젠 문제없나”, https://news.mt.co.kr/mtview.php?no=2022060807403293755

마. 해커의 먹잇감, 코로나19와 비대면 서비스 환경

코로나19 팬데믹이 길어지면서 재택 또는 원격근무가 일상화되면서 관련된 보안 위협도 많아지고 있다. IT 중심의 비대면 서비스는 원격 업무 솔루션이나 가상 사설망(VPN) 등을 중심으로 이루어지는데 이들이 해커의 주요 표적이 되어 관련 보안 이슈가 지속적으로 발생하고 있다.

2011년 발생한 대표적인 사건으로 한국원자력연구원(5월)과 국내 방산업체(7월)가 VPN 취약점을 통해 해킹된 사건이 있다. 이와 같은 국가 주요 기반시설이 공격 대상이 될 경우 국가 핵심기술 유출을 통한 중대한 안보 위협이 될 수 있다. 특히 한국원자력연구원 VPN 공격의 경우 접속 IP 이력 분석 결과 비인가 접속자가 아래 그림과 같이 북한 배후의 해커로 추정되어 이슈가 되었다.

〔그림 3－5〕 한국원자력연구원 VPN 취약점을 통한 비인가 접속 IP 이력 분석

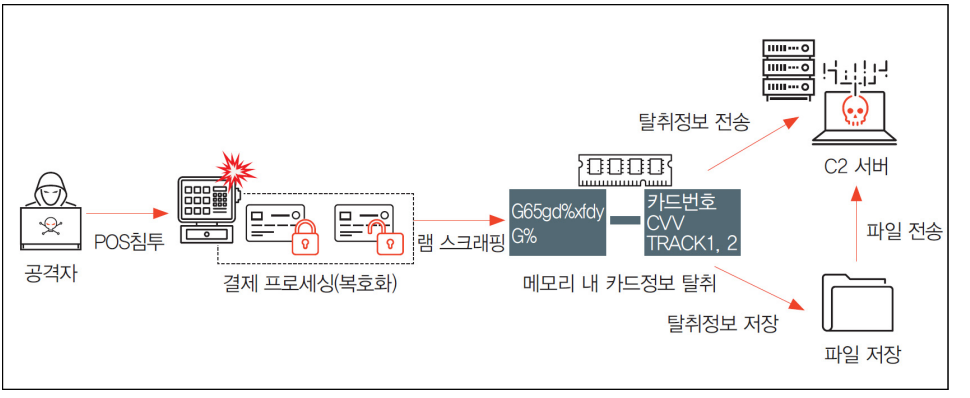


자료: ZDNet Korea, “원자력연구원 해킹… 북한 해커 소행인 듯”,
https://zdnet.co.kr/view/?no=20210618153600

바. 금융정보를 노리는 사이버공격의 진화

금전적 이득을 얻기 위해 금융정보를 탈취하는 기술 역시 다양한 방향으로 빠르게 발전하고 있다. 탈취 대상이 되는 대표적인 금융정보가 바로 신용카드 정보인데 신용카드는 사용의 편리함으로 현재 우리나라에서 가장 많이 사용되는 지급수단이 되었지만 편리함의 이면에는 다양한 보안 위협 역시 존재한다. 신용카드 정보는 주로 온라인 또는 오프라인 결제 과정에서 유출되는데 공격자는 온라인 유통업체를 해킹하여 카드 정보를 얻거나 아래 그림과 같이 오프라인 결제에 사용되는 POS 단말기에 악성코드를 심어 카드 정보를 획득한다.

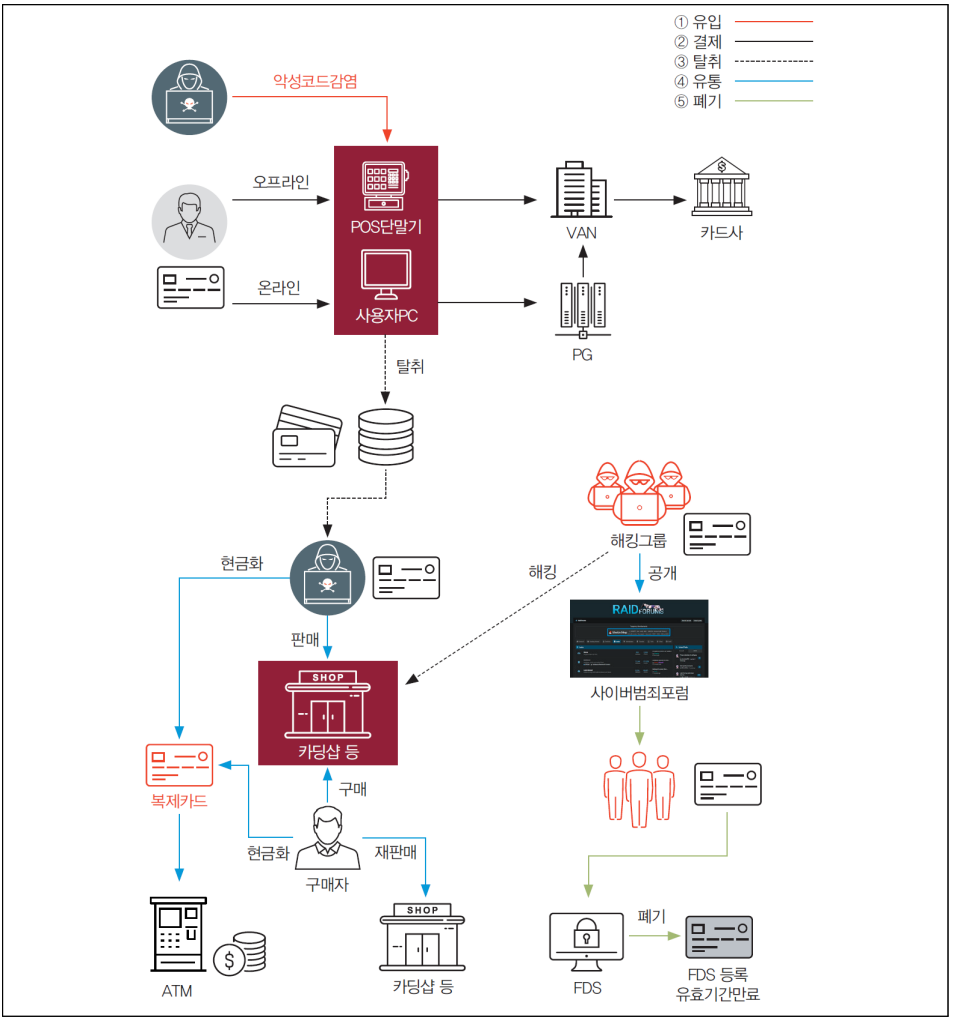
〔그림 3－6〕 POS 악성코드를 통한 카드결제 정보 탈취



자료: 금융보안원, “신용카드 정보를 노리는 사이버 공격 위협 분석 (2021 사이버 위협 인텔리전스 보고서)”

해커가 탈취한 신용카드 정보는 아래 그림과 같이 여러 단계에 걸쳐 다크웹을 통해 유통된다. 이와 관련한 거래 규모는 지속적으로 증가하고 있으며 우리나라도 예외가 아니다. 한 조사에 따르면 다크웹에서 판매된 4백만 개의 카드 정보 중 약 12,500개 정도가 우리나라 카드 정보였다고도 한다.

〔그림 3-7〕 카드 정보 유출 사이클



자료: 금융보안원, "신용카드 정보를 노리는 사이버 공격 위협 분석 (2021 사이버 위협 인텔리전스 보고서)"

사. 가상융합경제의 폭발적 확장을 노린 사이버위협의 등장

가상융합경제의 핵심이 되는 가상융합기술(eXtended Reality)은 현실과 가상세계를 연결함으로써 성장 가능성이 아주 큰 기술이지만 관련한 보안 위협 역시 다양하게 존재한다. 공격자는 메타버스(Metaverse) 단말기의 보안 취약점을 통해 관리자 권한을 획득할 수도 있으며 중앙 관리 서버에 침투해 정보를 획득하는 것 역시 가능하다. 메타버스와 관련한 대체불가능토큰(Non-Fungible Token, NFT) 역시 강력한 위・변조 방지 기능을 제공하지만 접근 권한 탈취 또는 신종 스캠(신용사기)에 악용될 수 있다.

2. 보안 위협 대응 국외 정책 현황

앞에서 살펴본 바와 같이 나날이 지능화 및 고도화되는 사이버 보안 위협에 대응하기 위해 전 세계 각국 정부는 국가안보의 관점에서 정책적 대응 방안을 마련하고 있다. 이 절에서는 각 국가별 사이버 보안 위협 대응 방안을 살펴본다.

가. 미국

미국은 사이버 보안 위협 대응을 위해 국가차원의 통합적 사이버안보 실무 및 조정기구를 설치하여 운영 중이다. 2001년 9.11테러 발생 후 만들어진 「국토안보법(Homeland Security Act)」에 의해 국가안보 강화를 목적으로 설립한 행정부처인 국토안보부(Department of Homeland Security, DHS)에 물리적 시설뿐만 아니라 사이버 안보 기능도 국가 차원에서 관리하도록 권한과 책임을 부여하였다.

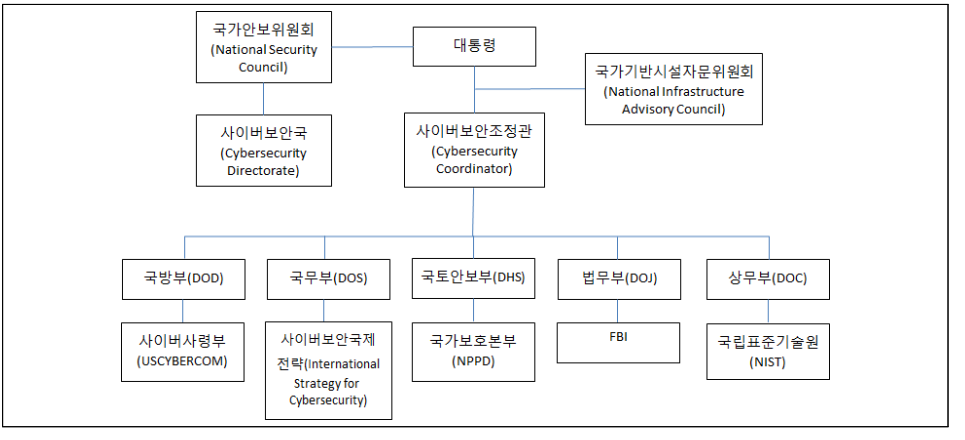
오바마 행정부가 들어선 2009년까지 국토안보부가 미국의 사이버 안보를 주도하다 대통령 직속 기구인 국가안보위원회(National Security Council) 산하 사이버 보안국(Cybersecurity Directorate)이 설치되면서 사이버 보안국이 범정부차원의 사이버안보 정책을 담당하게 되었다. 또한 대통령 직속으로 사이버보안 조정관(Cybersecurity Coordinator)을 새롭게 임명하였는데 사이버보안 조정관은 다음과 같은 역할을 수행하였다.

- 대통령에게 사이버 보안 관련 사항을 정기적으로 보고
- 주, 지방정부 및 민간부문을 포함하는 미국 내 모든 사이버 보안 담당자들과 긴밀한 협력 유지

- 대규모 침해사고 발생 시 국방부, 국가안보국, 국토안보부 등과 협력하며 총지휘관 역할 담당
- 국가안전보장회의에 상주하며 대통령과 국가안전보장회의에 사이버 보안 관련 정책을 정기적으로 보고
- 미군과 민간기관의 연방정부 사이버 안보 정책 마련을 위한 자문 역할 수행

이러한 변화를 통해 여러 부처에 걸쳐 있는 사이버 보안 업무를 사이버보안 조정관을 통해 대통령이 직접 관리할 수 있게 함으로써 사이버 안보의 주도권을 국토안보부에서 대통령을 중심으로 한 백악관으로 이전하였다. 이 시기의 사이버 보안 추진 체계는 아래 그림과 같다.

〔그림 3-8〕 오바마 행정부 사이버 보안 추진 체계도



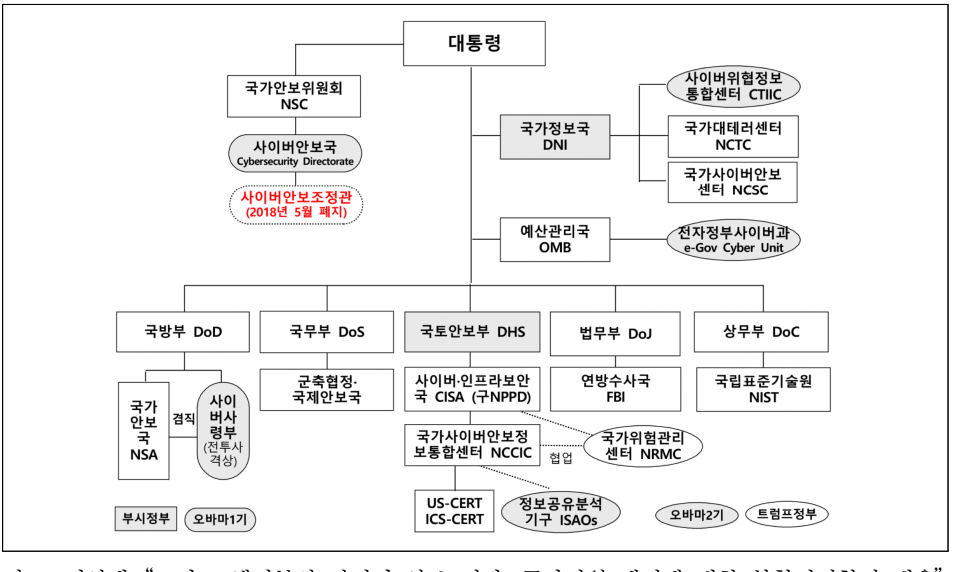
자료: 박영철 외, “사이버보안체계 강화를 위한 정보보호법제 비교법연구”, 한국인터넷진흥원, 2015.

트럼프 행정부가 출범하면서 오바마 행정부 시기 만들어진 사이버보안 조정관은 폐지되었으며 다시 사이버 안보의 주도권이 국토안보부로 이동하였다. 2018년 5월 발표된 국토안보부의 사이버 보안 전략(U.S. Department of Homeland Security Cybersecurity Strategy)은 사이버 공간에서의 위험 평가와 관리를 최우선으로 하며 (1) 위험 식별(Risk Identification), (2) 취약성 감소(Vulnerability Reduction), (3) 위협 감소(Threat Reduction), (4) 결과 완화

(Consequence Mitigation), (5) 사이버 보안성과 창출(Enable Cybersecurity Outcomes) 5개의 전략을 통해 연방정부의 정보 시스템 보호와 기관의 취약성을 보호하며 이해관계자들과 협력하여 주요 기반시설을 보호하는 것을 주요 목표로 하였다.

또한 범부처 차원의 사이버 위협 정보 공유 및 위기 대응 체계를 마련하고자 국가사이버안보통신통합센터(National Cybersecurity and Communications Integration Center, NCCIC), 사이버위협정보통합센터(Cyber Threat Intelligence Integration Center, CTIIC), 국가사이버안보통신통합센터(National Cybersecurity and Communications Integration Center, NCCIC), 정부부처조정위원회(Government Coordinating Councils, GCCs) 및 분야별 전문기관(Sector-Specific Agencies, SSAs)를 설립하였다. 한편 민간분야에서는 주요 기반 시설 운영자들을 중심으로 분야별 협력 위원회(Sector Coordinating Councils, SCCs)와 정보공유분석센터(Information Sharing & Analysis Center, ISACs)를 설립해 사이버안보 대응 체계를 구축하였다.

〔그림 3-9〕 트럼프 행정부 사이버 보안 추진 체계도



자료: 김상배, “트럼프 행정부의 사이버 안보 전략: 국가지원 해킹에 대한 복합지정학적 대응”, Journal of International Area Studies, vol. 27, no. 4, pp. 1-35, 2018.

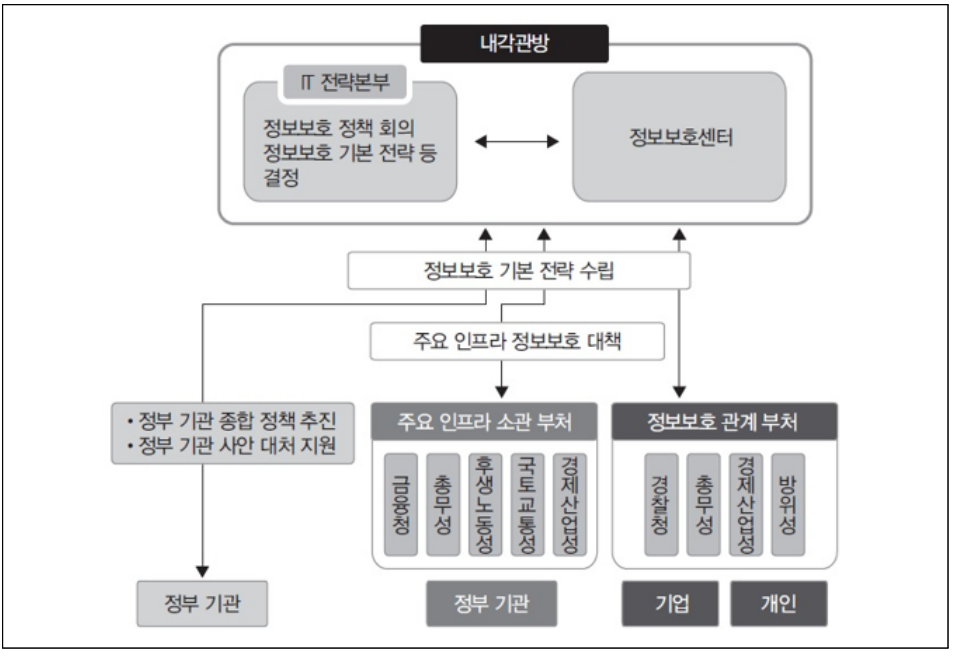
바이든 행정부가 출범하면서 「국방수권법(NDAA 2021)」 개정을 통해 국가사이버실(Office of the National Cyber Director, ONCD)이 신설되어 사이버 안보 정책의 부처 간 조정 역할을 수행하게 되었다.

나. 일본

일본의 사이버 보안 정책은 2014년 11월 제정된 「사이버보안기본법(サイバーセキュリティ基本法)」 이전과 이후로 나눌 수 있다. 「사이버보안기본법」의 입법취지는 기존 정부부처 별로 나누어졌던 사이버 보안 위협 대응기구를 내각관방 내 사이버보안 전략본부로 일원화하면서 기존 조직 및 관계 부처와 유기적 협조관계를 유지하면서 주도적으로 컨트롤타워 역할을 수행하도록 법률로서 보장하는 것이다.

「사이버보안기본법」 제정 이전 일본의 사이버 보안 관련 기본법은 「고도 정보통신 네트워크 사회형성 기본법」이었으며 이 법에 의해 설립된 IT 전략본부가 일본 내 사이버 보안을 포함한 정보화 분야 전반의 정책을 담당하며 컨트롤 타워 역할을 수행하였다. 사이버 보안 위협 대응은 훈령에 근거하여 각 정부 부처가 각각 주관하되, 부처 간 조정 역할은 내각관방 내 정보보호센터(National Information Security Center, NISC)가 담당하였다. 정보보호센터는 정보보호 기본 전략 수립, 정부 종합대책 촉진, 정부 사안대처 지원, 주요 인프라 보안대책 등과 같은 업무를 수행하였으며 정보 공유 체제 수립과 같은 정보보안 관련한 다양한 활동을 수행하였다. 「사이버보안기본법」 제정 이전 일본의 사이버 보안 체계는 아래 그림과 같다.

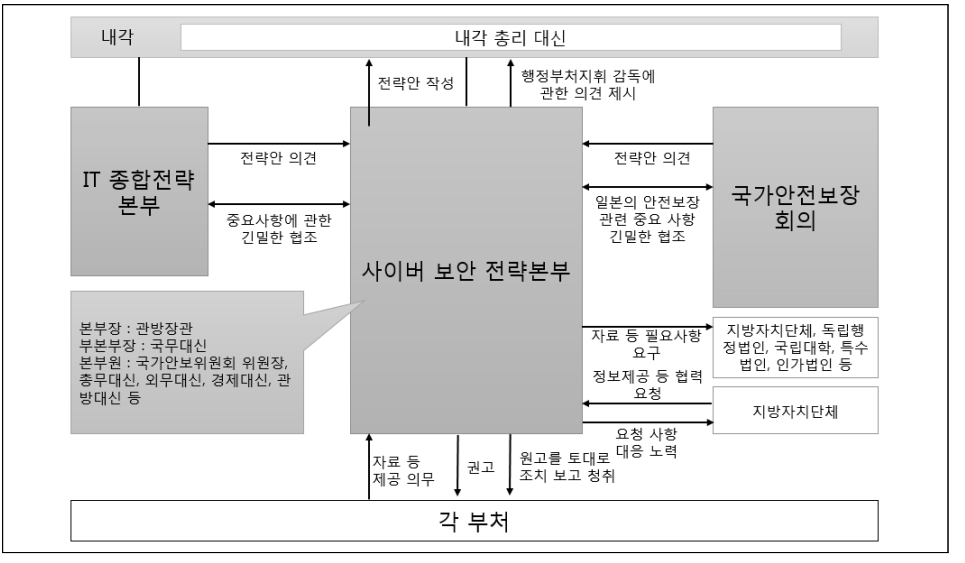
〔그림 3－10〕 「사이버보안기본법」 제정 이전 일본의 사이버 보안 체계



자료: 김경곤, "IT CookBook, 인터넷 해킹과 보안 개정3판: 정보 보안 개론과 실습", 한빛아카데미(2017)

「사이버보안기본법」이 제정되면서 일본 내 사이버 보안 정책은 내각관방이 주도하게 되었다. 이 법에 따라 새롭게 사이버 보안 전략본부가 설치되어 실질적인 일본의 사이버 보안 컨트롤 타워 기능을 담당하게 되었으며 기존 정보보호센터는 사이버보안센터(National center of Incident readiness and Strategy for Cybersecurity, NISC)로 개편하여 여전히 사이버 보안 분야에서 중요한 역할을 담당하게 되었다. 이를 통해 기존 훈령에 근거를 두었던 사이버 보안 조직체계가 법률차원으로 격상되었다. 「사이버보안기본법」 제정 이후 일본의 사이버 보안 체계는 아래 그림과 같다.

〔그림 3－11〕 「사이버보안기본법」 제정 이후 일본의 사이버 보안 체계



자료: 박영철 외, “사이버보안체계 강화를 위한 정보보호법제 비교법연구”, 한국인터넷진흥원, 2015.

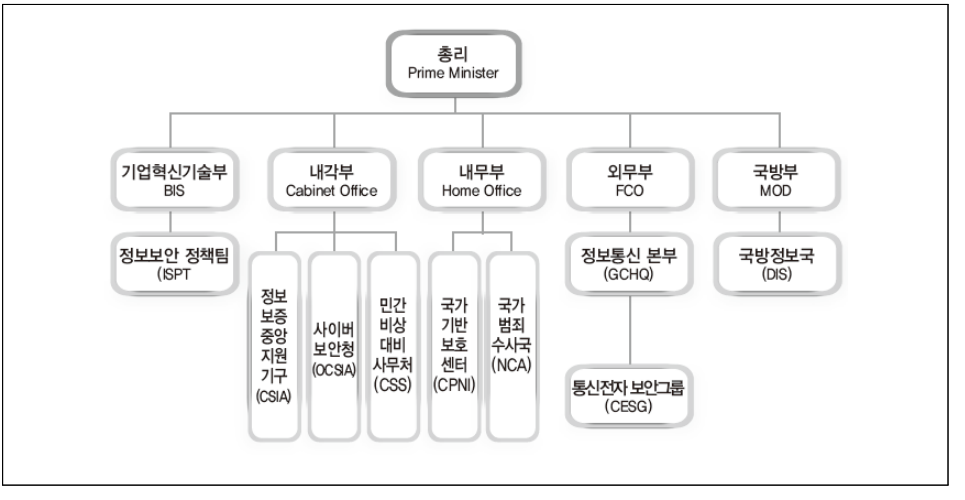
일본 내 사이버 보안은 「사이버보안기본법」을 통해 사이버 보안 전략본부를 컨트롤 타워로 두고 사이버 보안 전략본부에서 제시하는 구체적인 사항은 사이버보안센터에 위임해 업무를 수행하는 체제를 갖추었다. 「사이버보안기본법」 제정 이전 사이버 보안 조직은 IT 전략본부와 같이 법률에 근거를 둔 것도 있었지만, 그 외의 대부분은 법률이 아닌 훈령에 의해 설치된 것이었다. 하지만 「사이버보안기본법」 제정을 통해 사이버 보안 전략본부와 사이버보안센터에게 법률적 근거를 전제로 조직과 권한을 부여함으로써 실질적으로 일본 내 전체 사이버 보안 관련 컨트롤 타워이자 전문기관으로 기능할 수 있도록 한 점에 가장 큰 의의가 있다고 할 수 있다.

다. 영국

영국의 경우 수상을 지원하고 정부의 효과적 운영을 책임지는 내각부(Cabinet Office)가 사이버 보안 정책을 총괄하고 각 정부기관의 사이버 보안 업무를 조정하는 기능을 담당하지만 업무 범위는 중앙부처 내로 한정되며 개별 영역의 사이버 보안 정책에 대한 최종적

책임은 내무부(Home Office)·외무부(Foreign & Commonwealth Office, FCO)·국방부(MoD) 등 각각의 부처에 귀속된다. 영국 내 사이버 보안 관련 조직으로는 내각부 산하에 정보보증 중앙 지원기구(Central Sponsor for Information Assurance, CSIA), 사이버 보안청(Office of Cyber Security and Information Assurance, OCSIA), 민간비상대비사무처(Civil Contingencies Secretariat, CSS) 등이 있으며, 외무부 산하에는 정부통신 본부(Government Communications Head Quarters, GCHQ) 및 통신전자 보안그룹(Communications Electronics Security Group, CESG) 등이 있고, 내무부 산하에는 국가기반보호센터(Center for the Protection of National Infrastructure, CPNI) 및 국가범죄수사국(National Crime Agency, NCA)이 있다. 또한 국가 산업 발전을 위해 정보보호 정책을 담당하는 기업혁신기술부(Department for Business Innovation and Skills, BIS) 산하 정보보안 정책팀(Information Security Policy Team, ISPT) 역시 영국의 사이버 보안을 담당하고 있는 대표적인 정부기관이다. 영국의 사이버보안 체계를 그림으로 표현하면 아래와 같다.

〔그림 3－12〕 영국의 사이버 보안 체계

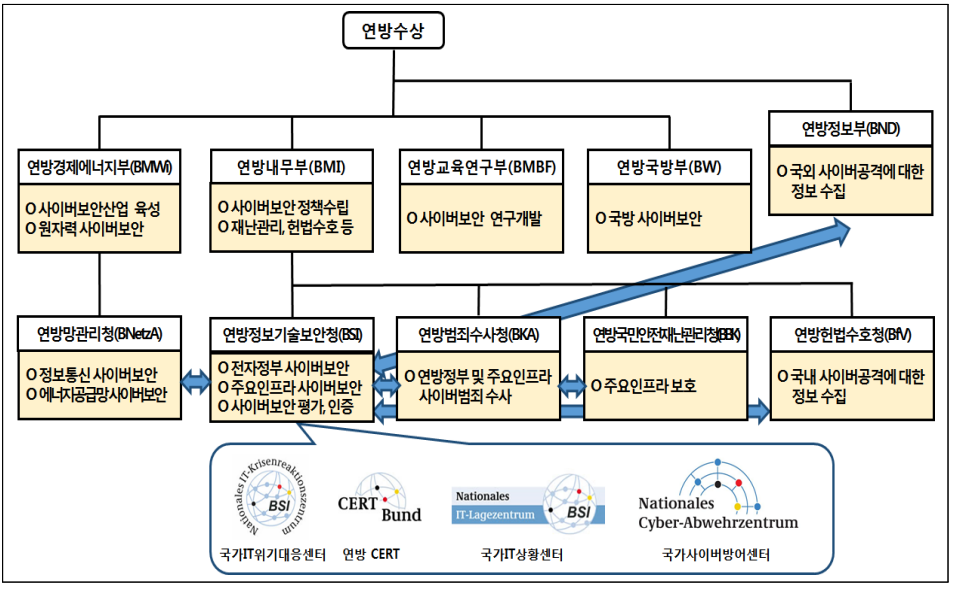


자료: 배병환, 강원영, 김정희, “영국의 사이버보안 추진체계 및 전략 분석”, Internet & Security Focus, 2014.

라. 독일

독일은 국가차원의 통합적 사이버보안 정책 추진을 위해 연방내무부(Bundesministerium des Innern und für Heimat, BMI)와 연방정보기술보안청(Bundesamt für Sicherheit in der Informationstechnik, BSI)을 중심으로 사이버보안 거버넌스를 구축하고 있다. 연방내무부는 사이버보안 정책 수립을 담당하고 있으며 연방정보기술보안청은 사이버보안 정책을 집행하는 역할을 수행한다. 이들 두 기관을 중심으로 연방경제에너지부(사이버보안 산업 육성), 연방교육연구부(사이버보안 연구개발), 연방국방부(국방 사이버보안) 등 각 부처가 자신의 소관 분야에서 사이버보안 관련하여 각자의 역할을 수행한다. 또한 16개로 이루어진 각 주(Land)는 자신의 영역에서 사이버보안을 담당한다. 독일의 사이버보안 체계를 그림으로 표현하면 아래와 같다.

〔그림 3－13〕 독일의 사이버 보안 추진 체계

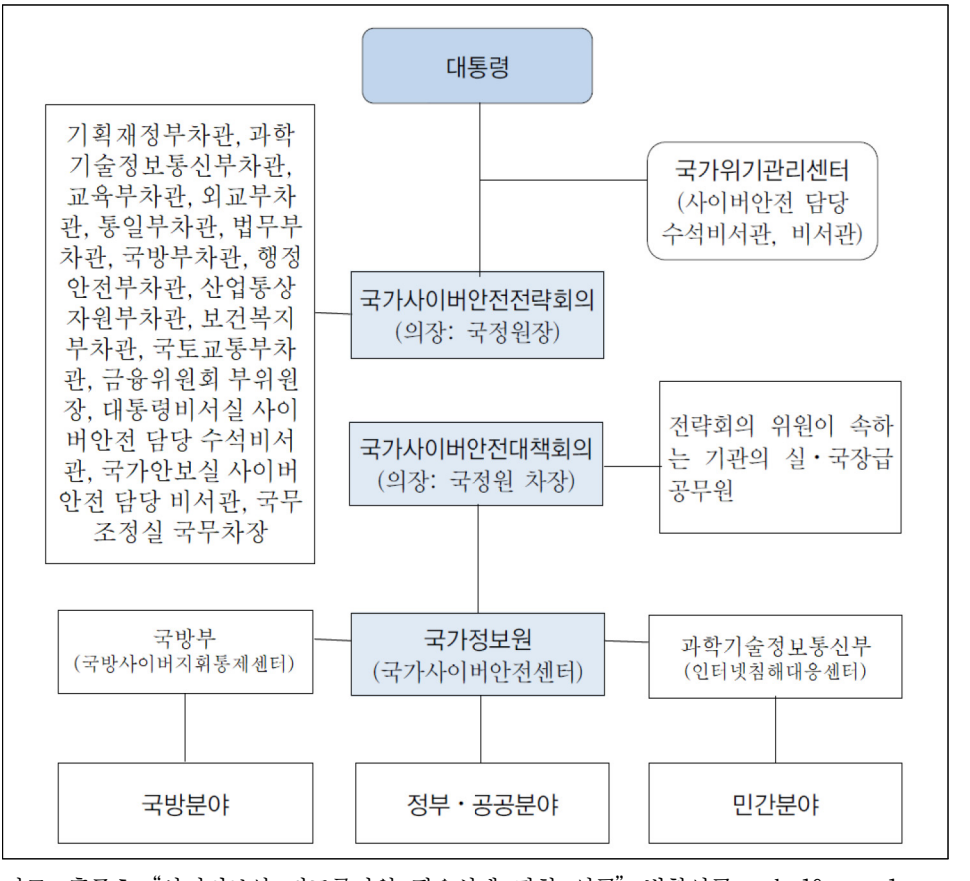


자료: 박영철 외, “사이버보안체계 강화를 위한 정보보호법제 비교법연구”, 한국인터넷진흥원, 2015.

3. 보안 위협 대응 국내 정책 현황

우리나라는 사이버 보안 위협 대응을 위해 아래 그림과 같이 정부·공공분야, 국방분야, 민간분야로 나누어 정부·공공분야는 국가정보원이, 국방분야는 국방부가, 민간분야는 과학기술정보통신부가 컨트롤 타워 역할을 수행하는 분야별 책임기관 체제를 바탕으로 보안 위협에 대응하고 있다.

〔그림 3－14〕 국내 사이버 보안 관리 체계



자료: 홍준호, “사이버보안 컨트롤타워 필요성에 관한 연구”, 법학연구, vol. 19, no. 1, pp. 235-254, 2019.

국내 사이버 보안 위협 대응 관련한 법령에는 「국가사이버안전관리규정」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반보호법」이 대표적이다.

대통령훈령인 「국가사이버안전관리규정」은 중앙행정기관, 지방자치단체 및 공공기관을 포함한 공공부문을 대상으로 하며(제3조), 공공부문 중에서도 국방분야는 국방부에서 따로 관리하도록 별도의 특례 규정을 두고 있다(제18조). 사이버안전 관련하여 기본적으로 중앙행정기관의 장이 소관 정보통신망에 대하여 안전성을 확보할 책임이 있지만(제4조), 국가사이버안전과 관련된 정책 및 관리에 대해서는 국가정보원장이 총괄・조정하도록 한다(제5조).

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 민간부문에 적용된다. 이에 따르면 과학기술정보통신부장관은 침해사고에 적절히 대응하기 위하여 ① 침해사고에 관한 정보의 수집 · 전파, ② 침해사고의 예보 · 경보, ③ 침해사고에 대한 긴급조치, ④ 그 밖에 대통령령으로 정하는 침해사고 대응조치 등의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다(제48조의2).

또한 공공과 민간의 주요기반시설 관련해서는 「정보통신기반보호법」이 있다. 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 ① 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성, ② 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도, ③ 다른 정보통신기반시설과의 상호연계성, ④ 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위, ⑤ 침해사고의 발생가능성 또는 그 복구의 용이성 등을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다(제8조).

주요정보통신기반시설을 관리하는 기관의 장이 기본적으로 기반시설을 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적 · 기술적 대책을 포함한 관리대책을 수립 · 시행하도록 하고 있으며(제5조), 과학기술정보통신부나 국가정보원에게 주요정보통신기반시설의 보호대책 이행 여부를 확인할 권한을 부여하고 있다(제5조의2).

현행 사이버 보안 관련 법제는 정부・공공분야, 국방분야, 민간분야로 나누어 개별적으로 각자 대응하도록 되어 있어 사이버 공격이 분야를 가리지 않고 동시에 발생하고 있는 점을 고려하면 권한과 책임의 분산 또는 중복 등으로 인해 적절한 대응에 어려움이 존재한다. 또한 「국가사이버안전관리규정」이 법이 아닌 행정규칙인 훈령으로 되어 있어 소

관기관의 실절적 권한 행사가 어렵다는 비판 또한 존재한다.

이러한 문제를 해결하기 위해 국회에서는 다양한 대안이 논의되어 왔다. 이러한 대안들은 크게 세 가지 범주로 나눌 수 있다. 첫 번째는 국가정보원이 보안 위협 대응을 총괄하는 안으로 2013년 3월 26일 하태경 의원이 대표 발의한 "국가사이버안전관리에 관한 법률안", 2013년 4월 9일 서상기 의원이 대표 발의한 "국가사이버테러방지에 관한 법률안", 2016년 5월 30일 이철우 의원이 대표 발의한 "국가사이버안보에 관한 법률안", 2020년 6월 30일 조태용 의원이 대표 발의한 "사이버안보 기본법안" 등이 있다. 두 번째는 과학기술정보통신부가 보안 위협 대응을 총괄하는 안으로 2014년 1월 9일 변재일 의원이 대표 발의한 "정보통신기반 보호법 개정안"이 있다. 세 번째는 대통령 소속하에 보안 위협 대응을 위한 별도 컨트롤 타워를 설립하는 안으로 2017년 1월 3일 정부가 국회에 발의한 "국가사이버안보법안"이 있다.

하지만 개인의 자유침해, 정보독점에 따른 정부기관의 권력불균형, 사이버안보에 있어 민간역할의 미비 등의 비판으로 아직 입법화되지 못한 상태이다.

4. 중장기 전략

앞에서 살펴본 바와 같이 현재 정부・공공분야, 국방분야, 민간분야로 나누어져 있는 사이버 보안 대응체계를 하나로 통합하기 위한 다양한 시도가 있어왔다. 이를 정리하면 아래 표와 같다.

〈표 3-1〉 정부부처별 컨트롤 타워 지정 논거 및 비판

정부부처	논거	비판
국가정보원	사이버안보 관리체계상 실무총괄을 맡고 있고, 국가사이버안전센터를 운영하여 많은 업무를 수행중임. 사이버테러나 사이버안보에 대한 법률 제정될 경우 컨트롤타워 지정 가능.	평시의 국가안전보장사무 수행할 수 있는 법률이 없어 법치주의에 따른 업무가 사실상 불가능, 빅브라더로 변모할 우려 존재

정부부처	논거	비판
청와대 및 국가안보실	국가안보에 관해 대통령을 보좌하는 역할을 하므로 행정내부적인 컨트롤타워 역할을 가능함	대외적 구속력이 없는 보좌기관이므로 법률에 컨트롤타워로 국가안보실장을 규정하는 것은 적절하지 않음
국민안전처	현대사회에서의 재난을 온라인과 오프라인을 구분할 이유는 없음	물리적 재난 대응을 목적으로 운영되고 있어 사이버위협 대응이 명시되지 않음. 심각한 사이버침해사고 발생 시 국무총리가 담당하는 것은 신속한 대응과 복구에 어려움이 있음
과학기술 정보통신부	민간분야의 사이버보안을 위한 컨트롤타워 역할 법적 근거 마련되어 있음	공공 및 국방 분야와 분리되어 있고, 국가사이버안전관리규정에 의하여 지시를 받아야 하며, 국가차원의 사이버보안을 위한 컨트롤타워 역할이 가능한 법적 근거가 없음
국무조정실	국무총리 보좌기관으로서, 정보통신기반시설보호에 관련하여 효율적으로 분야별 대응이 가능	통합과 조정의 업무를 중심으로 하는 곳이므로 신속성이 우선인 사이버보안에 대해 즉시 적극적으로 대응이 가능할지 미지수

자료: 홍준호, “사이버보안 컨트롤타워 필요성에 관한 연구”, 법학연구, vol. 19, no. 1, pp. 235-254, 2019.

그 중 유력한 첫 번째 안으로 국가정보원을 사이버 보안 위협 대응을 위한 컨트롤 타워로 지정하는 방법이 있다. 그 근거에는 국가정보원이 정보기관으로서 사이버 보안 위협 대응 관련한 경험이 많고 우리나라의 경우 최대 사이버 보안 위협 대상이 북한이며 법률 제정을 통해 컨트롤 타워 지정이 가능하다는 점 등이 있다. 하지만 정보기관이 사이버 보안 위협 대응을 위한 컨트롤 타워 역할을 수행하는 경우가 해외의 경우 그다지 흔하지 않고, 민간을 사찰하는 빅브라더(Big Brother)가 될 수 있다는 우려가 있으며, 정보기관의 특성으로 대국민 활동 및 언론 대응에 있어 어려움이 있어 컨트롤 타워로서 적절하지 않다는 비판 역시 존재한다.

두 번째 유력한 안으로 청와대가 통합적 사이버 보안 위협 대응을 위한 컨트롤 타워 역할을 하는 방법이 있다. 청와대를 중심으로 국가정보원, 국방부, 과학기술정보통신부가 협력하는 방식으로 사이버 보안 위협 대응을 수행함으로써 실질적인 사이버 보안 컨트롤 타워 역할을 청와대가 수행하는 것이다. 그 근거로 이미 일본에서 이와 유사한 제도를 운영

하고 있으며, 유관 기관 협력이 용이하다는 점 등이 있다. 하지만 현재 사이버 보안 분야를 담당하고 있는 국가안보실은 외교, 국방, 안보를 모두 다루고 있어 사이버 보안에 특화되어 있지 않으며 인적 구성도 외교 전문가 위주로 되어 있어 나날이 진화하는 사이버 공격에 적절하게 대응하기에는 전문성이 부족할 수 있다는 걱정 역시 존재한다. 따라서 청와대가 컨트롤 타워 역할을 수행할 경우 전문성 확보를 위해 청와대 안에 사이버 보안 전담 조직을 신설하거나 이를 지원하기 위한 민관합동위원회를 설립하는 방안이 같이 진행되어야 할 것으로 보인다.

마지막 유력한 안으로 독일의 경우처럼 사이버 보안 위협 대응을 위한 별도의 전담 대응 기구를 설치하는 방법이 있다. 이와 관련하여 우리나라에서도 가칭 '국가사이버안전청' 설립과 관련하여 정치권과 학계를 중심으로 다양하게 논의가 있어 왔다. 사이버 공격의 경우 분야를 가리지 않고 동시에 발생할 수 있다는 점에서 통합해서 관리하는 것이 효율적이며 따라서 이를 위한 독립적인 전담 조직이 필요하다는 주장이다. 하지만 사이버 보안 위협 대응을 위한 전담 조직의 경우 타 부처의 협조를 얻기가 쉽지 않고, 현재 각 부처에서 독립적으로 수행 중인 사이버 보안 업무를 하나로 통합하는 것도 현실적으로 쉽지 않을 것이라는 비판 역시 존재한다.

이와 같이 현재 분산되어 있는 사이버 보안 위협 대응 체계를 하나로 통합할 필요가 있다는 점에 대해서는 모두 동의하고 있지만 방법론에 있어서 다양한 이견이 존재한다. 앞에서 살펴본 바와 같이 미국, 일본, 영국, 독일 등의 해외 주요 선진국은 자국의 정치, 경제, 사회, 문화, 안보 환경을 고려하여 관련 법령 제정을 통해 다양한 형태로 사이버 보안 위협 대응 체계를 수립하고 있다. 우리나라 역시 국가차원의 통합적 사이버 보안 위협 대응 체계 수립을 위한 다양한 법안들이 발의되었으나 합의에 이르지 못해 아직 입법화되지 못하고 있다. 우리나라의 경우 사이버 보안 컨트롤 타워 역할 부여로 정보 기관의 역할이 강화되는 것에 대한 사람들의 우려, 사이버 보안 관련 청와대 내 전문성 부족, 현재 각 부처에서 독립적으로 수행 중인 사이버 보안 업무 통합의 어려움 등 다양한 사항들을 고려하여 국가차원의 통합적 사이버 보안 위협 대응 체계 수립을 위한 논의가 이루어져야 할 것으로 보인다.

제 2 절 보안 산업 정책 현황과 미래 전략

1. 국내외 산업 환경

가. 사이버 보안 산업의 정의

사이버 보안(Cybersecurity)과 혼용되는 용어로는 '정보보호' 혹은 '정보보안'이 많이 사용된다. 이들 용어들은 각자 유사한 의미를 가지고 있으나, 산업 관점에서 정보보호산업은 2015년 제정된 '정보보호산업의 진흥에 관한 법률(이하, 정보보호산업법)' 제 2조에서 정의하는 바를 따르는 것이 일반적이다.

〈표 3-2〉 정보보호산업법에 따르는 정보보호산업의 정의

용어	정의
정보보호	다음 각 목의 활동을 위한 관리적·기술적·물리적 수단(이하 "정보보호시스템"이리 한다)을 마련하는 것을 말한다. 가. 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것 나. 암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하는 것
정보보호산업	정보보호를 위한 기술(이하 "정보보호기술"이라 한다) 및 정보보호기술이 적용된 제품(이하 "정보보호제품"이라 한다)을 개발·생산 또는 유통하거나 이에 관련한 서비스(이하 "정보보호서비스"라 한다)를 제공하는 산업을 말한다.

해당 법률에 의거하여 정보보호산업의 진흥을 책임지고 있는 과학기술정보통신부에서는 상기 정의를 준용하여 정책을 수립하고 있으며, 〔그림 3-12〕와 같이 기술의 적용영역이나 제품·서비스의 특징에 따라 3종류(정보보안, 물리보안, 융합보안)의 세부분야로 분류할 수 있다. 북미, 유럽, 일본 등 주요 선진국이 정보보호 시장의 90% 가량을 차지하고 있으나, 최근 중국이 새로운 보안 시장으로서 급성장하고 있다고 알려져 있다.

〔그림 3－15〕 정보보호산업의 정의 및 세부분야

< 정보보호산업의 정의 >

"정보보호를 위한 기술 및 정보보호기술이 적용된 제품을 개발·생산 또는 유통하거나 이에 관련한 서비스를 제공하는 산업(정보보호산업법 제2조)"

정보보안	물리보안	융합보안
"클린인터넷경제"	"안전안심생활"	"안전성강화"
네트워크 상의 정보 유출·훼손 방지	재난·재해, 범죄 등 방지	他 산업분야의 보안내재화

자료: 과학기술부 등, "디지털 대전환 시대 정보보호산업의 전략적 육성 방안" (2022)

한편, 사이버 보안 산업에 대해서는 명확한 정의가 없으나, 일부 문서에서는 다음과 같이 정의하기도 한다.

"사이버 보안은 사이버 상의 범죄, 테러, 해킹 목적의 접근 및 스파이 행위 등으로부터 정보, 시스템, 네트워크를 보호하는 IT솔루션을 모두 통칭하는 개념으로, 암호, 인증, 인식, 감시 등의 정보보호 기술이 적용된 제품을 생산하거나 해당 기술을 활용해 재난•재해•범죄 방지 서비스를 제공하는 산업을 의미한다."(출처: 이지현(KOTRA), 2021년 미국 사이버 보안 산업, https://dream.kotra.or.kr/kotranews/cms/news/actionKotraBoardDetail.do?SITE_NO=3&MENU_ID=200&CONTENTS_NO=1&bbsSn=403&pNttSn=192645)

상기 정의에 따르면 사이버 보안 산업에서 다루는 제품・서비스는 사이버 위협에 대응하는 IT 솔루션을 의미하는 것이 일반적이므로, 정보보호산업에서의 세부분야 중 하나인 재난・재해, 범죄 등을 방지하기 위한 CCTV 등 각종 물리보안 제품들은 포함되지 않을 수 있으며, 다른 세부분야 중 정보보안 전체, 그리고 융합보안 분야의 일부가 포함될 수 있을 것으로 보인다. 다만, 아직까지는 융합보안 제품・서비스를 별도의 시장으로 구분하기보다는 정보보안 혹은 사이버 보안 산업의 일부로 포함하는 경우가 많으므로, 본 문서에서

특별한 언급이 없으면 사이버 보안 산업과 정보보호산업의 정보보안 분야를 같은 의미로 사용하고자 한다.

나. 사이버 보안 산업 시장의 규모

사이버 보안 산업은 국내·국외 시장 모두 급성장 중인 산업이다. 이는 AI, 빅데이터, 클라우드, IoT 등 새로운 ICT 기술이 등장하고, 이러한 ICT 기술이 기존의 사이버 환경 뿐만 아니라 산업제어, 의료, 자동차 등 실세계의 다양한 서비스와 결합하면서 그 영역이 더욱 넓어짐으로써 사이버 보안 기술·제품을 통하여 보호해야 할 대상과 가치가 더욱 확대되고 있기 때문이다.

과학기술부는 매년 한국정보보호산업협회와 함께 정보보호산업 실태조사를 하고 있으며, 2021년 정보보호산업 실태조사에 따르면 2014년부터 2020년까지 사이버 보안에 해당하는 정보보안 분야의 산업 매출은 연평균 14.5% 성장하고 있으며, 이는 소프트웨어 산업의 성장률 혹은 제조업 분야 성장률과 비교하였을 때 매우 높은 수치로 볼 수 있다.

〈표 3-3〉 국내 정보보호산업 매출 현황

[표] 정보보호산업 매출 현황

구분	정보보안			물리보안			합계		
	2018년	2019년	2020년	2018년	2019년	2020년	2018년	2019년	2020년
매출액 (백만원)	3,082,926	3,618,773	3,921,387	7,034,918	7,561,734	8,302,865	10,117,844	11,180,507	12,224,252
성장률 (%)	17.4%	8.4%		7.5%	9.8%		10.5%	9.3%	

자료: 과학기술부 등, "2021 정보보호산업 실태조사" (2021)

국외 시장의 경우에도 시장조사 전문기관인 가트너(Gartner)의 2021년 보고서에 따르면 〈표 3-3〉과 같이 사이버 보안 시장규모는 2020년 1319억 달러로 전년대비 4.8% 성장한 바 있으며, 2024년까지 연평균 9.4%의 고성장을 기록할 것으로 예측한 바 있다. 이 수치는 2022년 보고서에서 다시 한번 조정이 되었는데, 2022년 1725억 달러를 기록할 것이며, 2026년 2673억 달러로 예상, 연평균 11.0%로 폭발적인 성장을 예상하였다.

〈표 3-4〉 글로벌 정보보호산업 시장규모 및 성장률 전망 (가트너)

< 글로벌 정보보호 산업 시장규모 및 성장률 전망 >

구분	2020	2021	2022	2023	2024
시장규모(억 달러)	1,319	1,432	1,570	1,722	1,887
성장률(%)	4.8	8.6	9.7	9.7	9.6

※ Gartner(2021), 'Forecast: Information Security and Risk Management

자료: 과학기술부 등, "디지털 대전환 시대 정보보호산업의 전략적 육성 방안" (2022)

또한, STATISTA에서 2021년 발표한 전세계 사이버보안 시장규모 전망에 따르면, 가트너와는 약간 차이가 있으나, 연평균 9.6%의 성장률과 함께 2022년 1451억 달러에서 2026년 2098억 달러로 상당한 성장세를 보일 것으로 유사하게 예측하였다.

〈표 3-5〉 전세계 사이버보안 시장규모 전망(2022~2026)

<전 세계 사이버보안 시장규모 전망(2022~2026)>

(단위: 백만 달러, %)

구분	2022f	2023f	2024f	2025f	2026f	비중 ('26)	증감률	
							전년비 (25/26)	연평균 (22/26)
합계	145,199	159,167	174,560	191,532	209,842	100.0	9.6	9.6
IT서비스	69,084	77,317	86,558	96,950	108,426	51.7	11.8	11.9
소프트웨어	47,651	50,853	54,257	57,871	61,601	29.4	6.4	6.6
하드웨어	28,465	30,997	33,744	36,712	39,814	19.0	8.4	8.8

* 출처: STATISTA(2021)

자료: 한국인터넷진흥원, "2021 글로벌 정보보호 산업시장 동향조사" (2021)

사이버 보안 산업 시장이 급격한 성장세를 보이는 요인으로, 첫째 코로나19로 재택근무, 비대면・비접촉, 출입통제 강화 등 전세계 기업 및 조직이 디지털화되며 사이버보안에 대한 수요가 급격히 증가하였고, 둘째, 2021년 전세계 기업 네트워크를 대상으로 한 사이버 공격 횟수가 전년 대비 50% 증가하였으며, 셋째, 2021년 사이버 위협의 방식이 정교해짐으로써 데이터 침해, 피싱 공격, 조직내 실수 등으로 인한 사이버 보안 사고가 증가하였고, 넷째, 사이버보안에 대한 수요의 급증과 함께 전세계적인 사이버보안 인력부족 현상이 심

화되고 있기 때문이라는 분석이 있었다. (한국인터넷진흥원, “2021 글로벌 정보보호 산업 시장 동향조사” (2021))

다. 사이버 보안 산업의 특성

사이버 보안 산업의 특징은 진화하는 보안 위협에 대응하기 위해 지속적으로 연구 개발이 이루어지고, ICT 기술이 적용되는 분야가 확대됨에 따라 보호해야 하는 대상 역시 지속적으로 늘어난다는 점에 있다. 보안 위협이 실현될 경우 그 피해가 개인・기업・기관・국가 등 사회 전반에 걸쳐 영향을 미칠 수 있기 때문에 국가 안보와도 연결될 수 있으며, 일회성 지출이 아닌 지속적으로 비용과 인력을 투자해야 하는 산업으로 볼 수 있다.

앞서 언급한 ‘2021 국내 정보보호산업 실태조사’에 따르면, 사이버 보안 산업은 다음과 같은 중요한 특징을 가지고 있다고 언급하고 있다.

첫째, 사이버 보안 산업은 성장발전 가능성이 높은 신성장 산업이다. 사이버 보안 산업은 시스템・네트워크 중심의 보안 뿐만 물리와 융합 보안으로 그 영역이 지속적으로 확대되고 있으며, 지능화된 보안 위협, 자동차・안전과 같은 신규 보안 이슈 등의 확대를 고려하면 시장의 규모는 나날이 커질 것으로 보인다.

둘째, 사이버 보안 산업은 국가 안보와 관련한 방위 산업으로 볼 수 있다. 좁은 의미로 보면 개인의 안전과 재산을 지켜주는 분야이며, 보다 더 넓은 의미로 확대할 경우 각종 테러 및 보이지 않는 정보화 전쟁으로부터 국가의 안위를 책임지는 방위 산업이다. 특히, 사이버 상에서의 위협과 공격은 물리적 위치를 가리지 않고 이루어질 수 있으며, 국제해커조직으로부터 국가 기반 시설, 정부 기관 등에 가해지는 공격으로 인한 피해는 개인과 기업을 넘어, 국가 안보에 큰 영향을 주게 된다.

셋째, 사이버 보안 산업은 차세대 고부가가치 미래지향 산업이다. 최근 수년간 ICT 산업은 스마트기기 기반 모바일 환경, IoT, 클라우드 컴퓨팅 기술들의 발달로 많은 변화를 만들어 왔다. 즉, ICT 기술과 제품이 현재 각 개인의 실생활에 큰 영향을 주고 있을 뿐만 아니라, 가까운 미래에는 ICT 세상과 실제 물리 세상의 경계가 구분되지 않는 삶으로 진화하

는데 있어 큰 역할을 할 것으로 보인다. 그러나 이런 환경일수록, 사이버 위협이 기존 인터넷 망의 정보시스템 뿐만 아니라 우리의 삶에 큰 영향을 줄 수 있으며, 따라서 미래 생활에서는 더더욱 사이버 보안 산업 기술이 포함되어 응용될 것으로 보인다.

2. 국외 정책 동향

앞서 언급한 바와 같이, 사이버 보안 산업은 미래지향 신성장 산업이면서 국가 안보와 연관된 방위 산업의 특징을 가지고 있다. 점점 고도화되고 있는 사이버 위협과 공격은, 사이버 공간을 넘어서서 실세계에 영향을 끼치는 등 개인과 기업, 국가에게 막대한 경제적 피해를 줄 뿐만 아니라 국가적 혼란을 야기할 수 있기 때문에 다른 산업과 다른 특성을 지닌다. 예를 들어, 2021년에 발생한 미국 송유관 업체인 콜로니얼 파이프라인(Colonial Pipeline)를 마비시킨 사이버 공격의 사례는, 국가 핵심 인프라 시설을 대상으로 사이버 공격이나 테러가 이루어졌을 때 국가안보에 상당한 영향을 줄 수 있음을 보여준다.

따라서, 사이버 보안 산업을 주도하는 미국 뿐만 아니라 전세계 각국 정부는 사이버 보안 관련 법규와 제도를 도입함으로써, 국가·국민의 안전과 자국 사이버 보안 산업의 보호 및 활성화라는 두 마리 토끼를 잡고자 한다. 예컨대, 국내에서 정보통신망서비스를 제공하는 업체 혹은 상급종합병원 등 인증 의무대상자는 반드시 정보보호 및 개인정보보호 관리체계 인증(ISMS-P, Personal information & Information Security Management System)을 받도록 하고 있으며, 그 외에도 사이버 보안과 관련한 인증제도(예, 클라우드 보안인증제)를 시행함으로써 이러한 사업자로부터 서비스를 받는 사용자들을 보호할 수 있는 수단을 제공하고, 이들 사업자들은 사이버 보안 솔루션을 구축하도록 유도함으로써 이러한 제도는 국내 보안 산업의 활성화에도 기여하게 된다.

또한, 사이버 보안의 영역이 실세계와 연동되는 물리보안 혹은 융합보안까지도 확장되어감에 따라, 이러한 제도가 사이버 보안 산업의 보호에만 국한되지 않는 경우도 있다. 예를 들어, 2020년 6월 유엔의 유럽경제위원회(UNECE, United Nations Economic Commission for Europe)는 차량 사이버 보안 관련 법규인 'UNR 155(Cyber security and cyber security

management system)'를 채택하였는데, 이는 차량의 사이버보안 관리 체계(CSMS)에 관한 것으로 UNECE 회원국에 승용차 등 차량을 판매하고자 하는 자동차 제조사는 2022년 7월부터 CMSM 인증을 취득해야만 신차에 대한 차량 형식 승인이 가능하다. 따라서, 이 인증을 받지 못한 자동차 제조사는 유럽 및 일본 등 UNECE 회원국에 차량을 판매하지 못하는 만큼, 해당 법안은 일종의 수출 규제 역할을 할 수 있다.

가. 미국

미국은 전세계적으로 ICT 전분야를 선도하는 국가로서, 사이버 보안 산업에서도 핵심 기술을 보유한 글로벌 기업들이 많은 만큼, 전세계적인 흐름을 주도하는 등 사이버보안 기업의 매출 규모가 가장 높은 수준이다. 한편으로는 2021년 6월 기준 미국내 랜섬웨어 공격 건수가 7,840만 건으로 사상 최고치를 기록하는 등 사이버 공격과 위협 역시 전세계에서 가장 많이 일어나고 있는 것은 또 다른 현실이다.

자유로운 시장경제 질서를 선호하는 미국은, 한편으로는 국가 안보 역시 국가차원에서 가장 중요시하는 가치이기 때문에, 2가지 방향으로의 사이버 보안 산업 정책 집행이 이루어지고 있다고 보인다. 첫 번째로는 영업의 자유・학문의 자유 등 자유시장경제질서를 침해하지 않는 범위내에서, 학교와 연구소, 기업에 법규를 강제하기보다는 지침 혹은 가이드라인, 표준 등의 방식으로 해당 산업을 규제하거나 지원하는 정책을 편다는 것이다.

그러나, 사이버 보안 산업이 국가 안보에 직접적인 영향이 크지 않고 미미하던 과거의 시기에는 이러한 방식의 정책이 가능했으나 점점 사이버 보안 위협이 국가안보에 영향을 주고, 러시아, 중국 등 사회주의 국가로 미국 정부, 기업, 국민의 중요한 데이터가 유출될 우려에 따라 미국 역시 사회주의 국가의 사이버보안 법 체계를 일부 벤치마킹함으로써 그러한 사례를 사전예방하기 위한 움직임을 보이기 시작하였다.

2021년 5월, 바이든 대통령은 '국가 사이버보안 향상에 관한 행정명령(Executive Order 14028 of May 12, 2021 - Improving the Nation's Cybersecurity)'에 서명하였다. 이 행정명령에서는 ICT 기술 뿐만 아니라 산업제어시스템과 같은 운영 기술(OT)을 포함하여, 악의적인 사이버 위협으로부터 미국을 보호가 위하여 연방 정부와 민간의 협력을 강화할 것을

명시하고 있다.

사이버 보안 산업 관점에서 눈여겨 볼 점이 몇 가지 있는데, 첫 번째로는 연방 정부 사이버보안의 현대화로, 시민에 대한 프라이버시와 자유를 보호하면서도 사이버 위협에 대한 가시성을 확보하고, 제로트러스트 아키텍처와 클라우드 서비스 보안 강화 정책 등을 도입하는 등의 내용을 포함하고 있다. 두 번째로, 소프트웨어 공급망 보안 강화를 통해, 연방 정부가 사용하고자 하는 소프트웨어의 보안성을 강화하는 내용을 포함한다. 그 외에도, 위협 첩보 공유에 있어 방해가 되는 난관을 제거하고, 사이버 취약점 및 사건 대응을 위한 연방 정부 차원의 플레이북 표준화와 같은 내용을 포함하고 있다.

따라서, 이러한 법령에 따라 연방 정부들은 제로트러스트 아키텍처를 만족하는 새로운 보안 솔루션을 도입하는 등 사이버 보안 산업에 긍정적인 효과를 가져올 수 있겠으나, 한편으로는 소프트웨어 공급망 보안 등 ICT 하드웨어 혹은 소프트웨어를 납품하는 기업 입장에서는 책임이 커지고 연방 정부와의 계약조건이 강화되는 것에 대한 부정적인 효과도 일부 있을 것으로 보인다.

2022년 3월에 미국 상원에서 승인된 '사이버보안 강화법(Strengthening American Cybersecurity Act)'은 에너지 및 금융 서비스 등 중요 기반 시설을 보유한 기업을 주요 인프라 기업으로 지정하고 있으며, 총 3가지 측면에서의 법(연방정부 정보보호 현대화 법, 중요 인프라에 대한 사이버 사고 보고법, 연방 보안 클라우드 개선 및 고용법)을 포함하고 있다.

연방정부 정보보호 현대화 법에서도 제로트러스트 아키텍처 도입에 관한 내용이 포함되어 있으며, 중요 인프라에 대한 사이버 사고 보고법에서는 주요 인프라 기업이 사이버 공격을 받은 경우, 해당 사이버 사고가 발생했다고 합리적으로 믿은 시점으로부터 72시간 내에 CISA에 보고하도록 하고 있으며, 랜섬웨어 공격을 받고 대가를 지불한 경우 이에 대해서도 보고하도록 하고 있다.

이 외에도 미국 의회에는 하원 혹은 상원에 제출된 수많은 사이버 보안 관련 법안이 존재한다. 이 중 상당수는 하원 혹은 상원에서 통과되지 못할 수 있겠으나, 사이버 보안 산업 관점에서 눈여겨 볼 만한 것으로는 다음과 같은 법안이 있다. 이 리스트를 통해 사이버 보안 산업 관점에서 미국 의회 혹은 정부가 중요하게 생각하는 부분을 일부 살펴볼 수 있을 것으로 보인다.

- **의료 및 헬스케어 보안**: 헬스케어 사이버 보안법 (H.R. 8806, S. 3904), 의료 기기를 위한 사이버 보안 강화법 (S. 4336)
- **소규모 기업 및 주/지방 정부 보안**: 소규모 기관 사이버보안 개선법(S. 2483), 소규모 기업, 비영리 기관, 지방 정부의 사이버 보안 개선법 (H.R. 6541), 주 및 지방 사이버 보안 개선법(S. 2585, H.R. 3138), 주/지방 정부 사이버 보안법(S. 2520, H.R.5960),
- **양자 위협 대응**: 양자 컴퓨팅 사이버 보안 대비법(S. 4592, H.R. 7535)
- **산업제어 등 인프라 보안**: 국가안보국 산업제어시스템 능력 개선법(S. 2439, H.R. 1833), 중요한 주요 인프라에 시스템적 안전성 강화법(H.R. 5491), 공공-민간 파트너십을 통한 그리드 보안 강화법(H.R. 2931), 주 에너지 보안 계획 및 위급상황 대비 개선법(H.R. 1374)

나. 영국

영국은 사이버 컨설팅, 보안 위협에 관한 분석, 모니터링, 탐지와 관련한 기술을 선도하고 있으며, 산업제어 시스템 및 IoT 보안 솔루션 제공 기업이 성장하고 있다. 다만, 브렉시트로 인한 정치적 혼란 및 향후 정책 방향에 대한 불확실성이 시장 성장 면에서 좋지 않은 영향을 주고 있다. 그럼에도, 2019년 3월 발표된 ITU 사이버 보안 지수에 따르면, 영국은 전세계 1위로 한국(당시 15위)보다 높은 수준이었으며, 최근들어 사이버 공격과 테러 예방을 위한 정책을 강화함으로써 관련 기기, 솔루션 등의 수요가 계속 증가하는 중이다.

2021년 11월 통신보안법을 개정하고, 제품보안통신인프라법을 도입하였는데, 여기에서 통신보안법은 2003년 도입되었던 기존 법안에 대해, 영국 전역의 네트워크 보안을 강화하도록 통신 회사에 법적 의무를 부여하였으며, 제품보안통신인프라법은 쉽게 추측할 수 있

는 패스워드 탑재 금지, 보안 업데이트 일정 공개 등의 의무를 명시함으로써 사이버 위협에 대응하기 위함이다.

다. 독일

독일은 현재 사이버 보안 산업 관점에서 클라우드 보안과 양자 암호 기술을 선도하고 있다. 특히 독일의 양자 암호 시장은 2026년까지 24억 5천만 달러에 이를 것으로 보이며, 유럽의 양자 기술 시장을 선도할 것으로 보인다. 양자 보안 분야에서 미국은 양자내성암호 외에 큰 관심을 보이지 않고 있으며, 양자 암호는 현재 유럽과 중국 위주로 많은 투자가 이루어지고 있다고 판단된다.

독일이 2021년 발표한 연방데이터전략(Datenstrategie)에서는 데이터 인프라 확보 및 양자 컴퓨터 개발과 관련한 조치를 포함하고 있으며, 사이버보안전략 초안 2021에서는 국가와 사회의 공동 의무, 디지털 주권, 디지털화의 성공을 위한 보안, 보안 정책의 투명성 등을 포함하고 있다.

라. 일본

일본은 다른 선진국과 비교하여 ICT 및 스마트 환경으로의 이행이 상대적으로 느린 편에 속하며, 이는 사이버 보안 분야에서도 유사한 경향성을 보이는 것으로 보인다. 이를 반영하듯, IDC Japan의 조사(2021)에서 일본 기업의 60%가 정보 보안 투자 예산이 별도로 존재하지 않는 것으로 파악되었으며, 영국의 국제전략연구소는 '사이버 역량과 국력(Cyber Capabilities and National Power: A Net Assessment)' 보고서에서 일본의 사이버 방어 능력을 최하위 등급으로 평가한 바 있다. 이 보고서에 따르면, 일본의 사이버보안 방어 능력을 '국익을 위협하는 사이버 위협에 대해 필요한 역량이 현저히 취약한 안보・방위 부문이 존재한다'고 평가하였다.

이를 만회하기 위하여 2021년 9월 디지털청이 출범하여 국가의 디지털 개혁을 주도하고 있으며, 전기・정보통신 등 14개 민간기업에 사이버 공격 대비 의무화 조치를 취하도록 함으로써, 이 기업들은 사이버 공격에 대한 대처 계획, 책임 소재, 긴급대응 조직 등을 마

련하도록 함으로써, 기업들이 사이버 보안에 투자할 긍정적 효과로 작용할 가능성이 높다.

〈표 3-6〉 일본 사이버 보안 산업 관련 법·제도

사이버 보안 산업 관련 법·제도	내 용
사이버보안기본법	- 국가 차원의 사이버보안에 관한 대응 전략 추진 목적 - 사이버보안을 '정보시스템 및 정보 통신망의 안전성 및 신뢰성 확보를 위해 필요한 조치를 강구하고 그 상태가 적절하게 유지 및 관리되는 것'으로 정의 - 사이버보안협의회 창설, 사이버보안전략본부 연락 조정 권한 부여 등
주요기반시설 정보보안 안전기준 지침	- 주요기반시설의 사이버 방어 프로세스 전반에 걸친 대응 기준 - 중요 데이터는 해외 및 클라우드 대신 일본 내 서버에 보관하도록 권장, 정보 시스템 및 서버를 재해 영향이 없는 장소에 두도록 하는 내용 포함
IoT·5G 보안 종합대책	- 2017년 IoT 보안 종합대책을 수립하여, 보안 개선사항 검토, 보안 내재화, 취약점 조사 및 대응 등 IoT 기기 생명 주기에 따른 보안 정책에 집중 투자하는 내용 포함 - 2017년 IoT 보안 종합대책을 근간으로 보완 및 5G 보안 대책 추가
텔레워크 보안 가이드라인	- 기업의 안전한 원격근무 지침으로, 거버넌스 리스크 관리, 자산·구성 관리, 취약성 관리 등 보안 대책 포함
사이버보안전략 2021	- 사이버 공격 활동에 대한 방위성 및 자위대 사이버 방위 능력 향상 - 심각한 사이버 공격에 대해 정보 수집, 분석, 조사, 평가, 주의 환기 등을 실시하는 컴퓨터비상대응팀(CSIRT/CERT) 강화

마. 중국

중국은 다른 주요국가와는 달리 공산주의 및 사회주의를 채택하고 있는 국가로서, 다른 국가들과 비교하여 시장 통제 중심의 산업 환경을 가지고 있으며, 한편으로는 미국 및 미국의 동맹국과 경쟁하며 자국의 이익을 극대화하기 위한 정책을 펴고 있다.

미국 및 유럽은 각각 사이버보안법을 발표(2015년, 2019년)하여 자국의 권리를 보호하는 한편, 미국의 클린 네트워크 프로그램(CNP, Clean Network Program)을 통하여 동맹국과 함께 5G 통신, 모바일 어플리케이션, 해저 케이블, 클라우드 등 미국이 신뢰할 수 없다고 판단한 중국 기업을 사업상의 협력에서 배제하는 정책을 추진하고 있다.

한편, 중국 역시 2017년 사이버 공간에서의 침해 예방, 대응, 보호를 위한 사이버보안법을 발표한 바 있으며, 여기에서는 사이버보안 표준체계 구축, 사이버공간운영 안정, 핵심정보 기반시설 보호, 온라인 실명제, 개인정보보호, 사이버 공간의 정부 통제 강화 등을 규정하고 있다. 특히 데이터 관점에서 보면, 사이버보안법에서는 중요 정보 핵심 기반시설 관련 중요 데이터는 중국 현지 서버 저장을 의무화하고 있으며, 데이터보안법에서는 중국 내 수집・생성 중요 데이터의 역외 이전 제한을 명시하고 있고, 개인정보보호법은 개인정보에 대하여 국외 이전 조건을 충족할 경우 이전을 허가하는 등의 내용을 담고 있다. (자료: 박민숙, 이효진, '중국의 사이버보안 정책 연구', 대외경제정책연구원 및 박민숙, 이효진, '최근 중국의 사이버보안 정책 동향: 입법규제를 중심으로', 한국과학기술기획평가원 등 참조).

앞서 언급한 클린 네트워크 프로그램 등 미국의 대중 기업 규제 정책 등에서 미국과 중국의 입장 차이가 매우 크게 드러나고 있다. 즉, 신뢰있는 데이터의 자유로운 이동에 동의하는 미국・일본 및 부분적인 제한 정책을 갖는 한국과 다르게 중국의 경우 '데이터 주권론'을 내세우며 자국 데이터 관련 산업 육성, 정치적 안정 등을 위하여 러시아, 베트남 등 공산국가와 함께 데이터 해외 이전에 대해 반대하고 있다. 이러한 상황에서 사이버보안법, 데이터보안법과 개인정보보호법의 제정은 중국이 내부 정치적인 상황을 고려함과 동시에 미국 및 다른 선진국과의 규제로부터 중국내 ICT・데이터 및 사이버 보안 산업의 발전을

도모할 수 있는 정책이 될 것으로 보인다. 또한 이들 법을 기반으로 〈표 3-7〉과 같이 사이버 보안 산업과 관련한 법과 제도를 운용함으로써 자국의 사이버 보안 산업에 대한 규제 및 자국 제품에 대한 보호가 가능하도록 하고 있다.

〈표 3-7〉 중국내 사이버 보안 산업 관련 법·제도

사이버 보안 산업 관련 법·제도	내 용
핵심 정보 기반시설 안전보호 조례	- 핵심 정보 기반시설의 정의, 구축, 운영, 관리·감독, 안전 보호 등에 대한 내용 포함 - 핵심 정보 기반시설 안전지침에서 주요 산업 운영에 필요한 정보시스템 또는 산업시스템 정의 - 핵심 정보 기반시설로 정의된 시설·설비는 사이버보안심사법에 의거 보안에 대한 심사를 받아야 함
사이버보안심사방법	- 사이버보안법 제35조에 규정된 '핵심 정보 기반시설 운영자의 네트워크 상품 및 서비스 구매가 국가 안보에 영향을 미칠 가능성이 있는 경우 보안 심사를 받아야 한다'는 조항에 대한 실시세칙
네트워크 핵심 설비 보안검사 및 안전인증	- 국가정보보안제품 인증(CCIS): 중국정부에서 조달 구매할 제품 대상, 국가인증인가감독관리위원회가 인증 및 평가를 담당 - 정보기술보안 강제인증(ISCCC): 외국기업이 16개 분야 IT관련제품(정보보안제품)을 외국기업에서 조달할 경우 정보보인인증센터를 통해 의무적으로 받아야 함
네트워크 보안등급 보호제도	- 네트워크 보안등급을 인터넷 중요도와 피해시 파급효과를 고려하여 5단계로 구분하고 등급별 기준을 제시 - 2등급 이상 네트워크 운영자는 전문가를 조직하여 등급평가 실시 후 해당 산업부처에 확인 및 검토
암호법	- 암호를 핵심암호, 일반암호, 상용암호로 구분하여 관리. 이 중 핵심암호와 일반암호는 국가비밀에 속하며 법에 의해 엄격하고 통일되게 관리 - 상용암호는 국민, 법인 등이 법에 따라 네트워크 보호 및 안전에 사용 가능하며, 네트워크 핵심제품 및 사이버보안 전용제품 리스트에 추가하여 평가기관으로부터 평가 및 인증 취득 후 판매 가능

3. 국내 정책 동향

가. 정보보호산업 활성화를 위한 법적 근거

정부는 정보보호산업을 활성화하기 위한 다양한 조치를 취할 수 있으며, 이 중 법적 근거는 정보보호산업법 제2장(정보보호산업의 활성화, 제6조~13조) 및 제3장(정보보호산업 진흥의 기반조성)에 담겨 있다. 여기에서는 전자정부법 제2조제2호에 따른 행정기관 또는 공공기관의 장은 소관 기관・시설의 정보보호 수준을 강화하기 위하여 매년 정보보호기술 등에 대한 구매수요 정보를 과학기술정보통신부장관에게 제출하여야 하는 의무 등 정보보호활성화를 위한 내용을 포함하고 있다.

〈표 3-8〉 정보보호산업 활성화를 위한 법적 근거

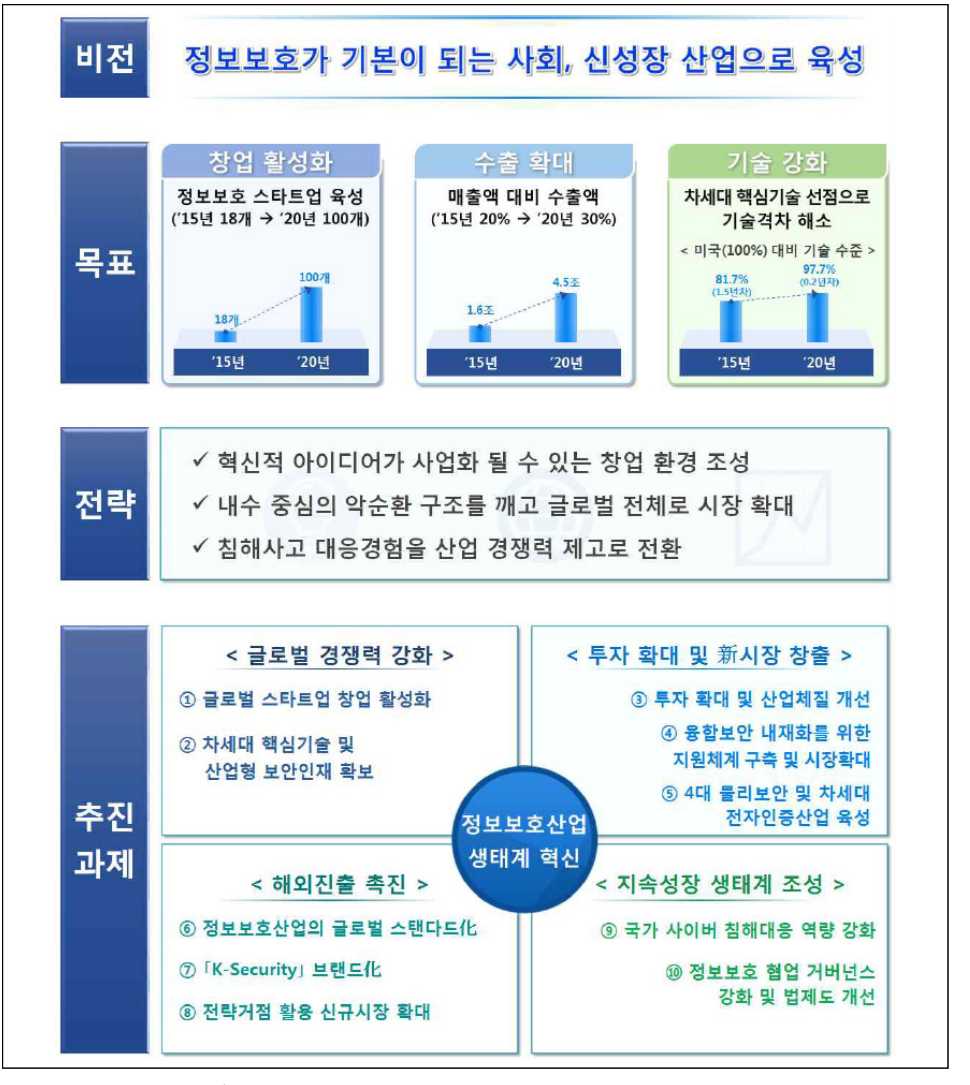
목적	법적 근거
(정보보호산업법 제2장) 정보보호산업 활성화	- 제6조: 구매수요정보의 제공 - 제7조: 공공기관등의 정보보호시스템 구축 계약 - 제8조: 사업 하도급의 승인 - 제9조: 정보보호시스템의 하자담보 책임 - 제10조: 정보보호제품 및 정보보호서비스의 대가 - 제11조: 정보보호산업의 융합 촉진 - 제12조: 정보보호 준비도 평가 지원 - 제13조: 정보보호 공시
(정보보호산업법 제3장) 정보보호산업 진흥의 기반조성	- 제14조: 기술개발 및 표준화 추진 - 제15조: 전문인력 양성 - 제16조: 국제협력 추진 - 제17조: 성능평가 지원 - 제18조: 우수 정보보호기술 등의 지정 - 제19조: 우수 정보보호기업의 지정 - 제20조: 자금융자 - 제21조: 수출지원 - 제22조: 세제 지원 등 - 제23조: 정보보호 전문서비스 기업의 지정・관리 - 제24조: 한국정보보호산업협회의 설립

정부는 이 외에도, 과학기술정보통신부 등을 중심으로 국가정보원, 기획재정부 등 관계부처와 함께 2021년부터 각 분야별로 규정된 사이버 보안 법제도를 종합해서 체계화하기 위한 사이버보안기본법 제정을 추진해 왔으며, 민관 협력체계 강화, 기반시설 관리 강화 등의 내용을 포함하고 있다. 그러나, 사이버보안청 등 일원화된 사이버 보안 전담기구의 설립, 사이버 위기경보 제재 강화, 경보 체계 등 여러 이슈가 있어 아직은 여전히 논의 중인 것으로 보인다.

나. 정보보호산업 활성화 정책

정부는 2015년 'K-ICT 시큐리티 발전전략'을 수립하고, 앞서 언급한 정보보호산업법을 제정하였으며, 2016년 '제1차 정보보호산업 진흥계획'을 발표한 바 있다. 이 진행계획에서의 주요 정책 과제로 창업활성화 전략, 정보보호 투자확대 및 신시장 창출 전략, 글로벌 시장확대 추진, 국가사이버 침해대응 역량 강화 등을 포함하였다.

〔그림 3－16〕 2016년 제1차 정보보호산업 진흥계획 비전 및 전략



자료: 관계부처 합동, '정보보호산업 육성 및 전문 일자리 창출을 위한 제1차 정보보호산업 진흥계획'(2016)

정보보호산업법 제정을 통하여 정보보호시장 창출 등 산업 선순환 생태계를 강화, 체계적인 정보보호산업 진흥 기반조성을 위한 규정을 마련함으로써 국내 사이버 보안 산업을 강화할 수 있는 법적 근거 및 기반을 마련했다고 볼 수 있다.

이후, 2019년 4월에는 청와대 국가안보실에서 '국가사이버안보전략'을 발표하고 6대 전략 과제 중 4번째로, '사이버보안 산업 성장기반 구축'계획을 포함하였다. 이는 국가 사이버안보의 기반역량이 되는 기술·인력·산업의 경쟁력 확보를 위해 제도 개선, 지원 확대 등 보안산업 혁신 생태계를 조성하는 것이 목적으로, 세부 전략으로서 1) 사이버보안 투자 확대, 2) 보안 인력·기술 경쟁력 강화, 3) 보안기업 성장환경 조성, 4) 공정경쟁 원칙 확립을 수립하였다. 이는 정보보호산업 진흥의 기반조성의 목적성이 있는 것으로 보인다.

이후, 관계부처인 과학기술정보통신부, 국가정보원, 행정안전부, 외교부, 교육부 등은 합동으로 2019년 9월 국가 사이버안보기본계획을 수립하였다. 각 부처에서 발표한 주요 세부과제 중 사이버 보안 산업과 관련이 있는 항목을 〈표 3-9〉에서 정리하였다.

〈표 3-9〉 국가 사이버안보기본계획 부처별 시행 계획 (사이버 보안 산업 연관 내용만 별도 발췌)

소관 부처	주요 세부과제
과기정통부	- 5G 통신망 보안수준 제고 및 네트워크 신뢰도 확보 - 산·학·연 협업 기반 창업 환경 조성 및 해외진출 지원
기획재정부	- 정보보호 인증제품 공공 시장 확대 지원
교육부	- 교육기관 노후 정보통신장비 보안 관리 강화
행정안전부	- 국가정보자원 보안취약점 상시 관리체계 구축

이후 2020년 과학기술정보통신부는 '제2차 정보보호산업 진흥계획(2021~2025)'을 발표하여 디지털 전환 가속화 및 민간 사이버 복원력 확보를 통한 안전한 디지털 신뢰사회를 구현하고자 하였다. 여기에서의 중점 추진 과제는 1) 디지털 전환에 따른 정보보호 신시장 창출, 2) 민간 주도 사이버 복원력 확보를 위한 투자 확대, 3) 지속성장 가능한 정보보호 생태계 조성 등을 포함하고 있으며, 각 중점 추진과제 별로 세부 추진과제를 포함하고 있다.

〔그림 3－17〕 2020년 제2차 정보보호산업 진흥계획(2021~2025) 비전 및 전략

비전	정보보호가 기본이 되는 신뢰 기반의 디지털 경제 확산		
목표		<2019년>	<2025년>
	전체매출액	10.5조원	→ 20조원 (9.5조원, 연평균 11.3%↑)
	300억이상 기업	37개	→ 100개 (63개, 연평균 18%↑)
	일자리	13.5만명	→ 16.5만명 (3만명, 매년 6천명↑)
중점 추진 과제	디지털 전환에 따른 정보보호 신시장 창출	① 비대면 서비스 관련 보안시장 활성화	
		② 정보보호 데이터 활용기반 조성	
		③ AI기반 물리보안 산업 육성	
		④ 5G+ ICT 융합보안 산업 저변확대	
	민간 주도 사이버 복원력 확보를 위한 투자 확대	⑤ 공공·민간 분야 정보보호 투자 확대	
		⑥ 중소 정보보호기업 성장지원	
		⑦ 정보보호 해외진출 및 국제협력 강화	
	지속성장 가능한 정보보호 생태계 조성	⑧ 차세대 보안 新기술 확보	
		⑨ 정보보호산업 규제 및 법·제도 개선	
		⑩ 정보보호 전문인력 양성	

자료: 관계부처합동, '제2차 정보보호산업 진흥계획 - 디지털 경제 전환을 정보보호산업 성장의 기회로 -'(2020)

이후 2022년 과학기술정보통신부는 전통산업과 ICT 기술이 융합된 스마트공장, 스마트카 등의 보안내재화를 위한 융합보안 시장 성장 등을 포함하는 '정보보호산업의 전략적 육성 방안'을 발표하였다. 2021년 과기부장관회의에서 글로벌 기술패권 경쟁에 대응한 국가 필수전략기술 중 하나로 사이버보안이 선정되었으며, 보다 빠르게 디지털 전환 가속화 및

사이버 보안 위협에 대응하고 산업을 육성·보호하기 위한 일환으로 보인다.

그 동안 수립된 사이버보안 산업 관련 진흥계획 및 전략을 실천하는 과정에서 국내 산업의 양적 성장이 이루어졌으나, 전세계 사이버 보안 유니콘 기업 42개 중 한국기업이 전무한 점 등 분야별 전문화 및 기업 대형화를 포함하는 기업의 질적 성장이 필요하다는 인식 또한 전략수립의 중요한 요인이다. 기본적으로 사이버 보안 산업의 시장 규모를 2025년 25조원으로 성장시키겠다는 목표는 제2차 정보보호산업 진흥계획과 같지만, 세부 추진 전략을 조정하고 구체화함으로써 사이버 보안 산업이 차세대 전략산업으로서 도약을 추진할 계획이다.

〔그림 3－18〕 정보보호산업의 전략적 육성 방안 목표 및 추진전략 (2022)

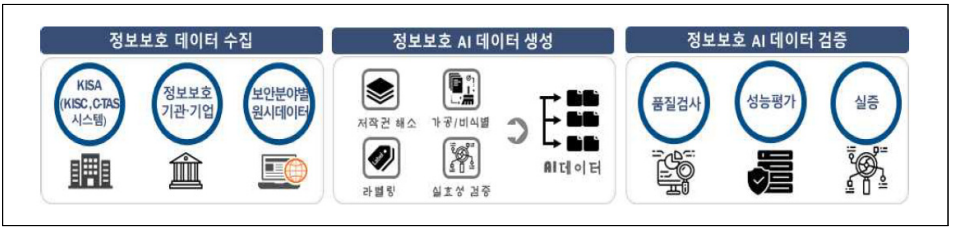
비전	튼튼한 정보보호산업 육성으로 안전한 디지털 전환 구현	
목표	정보보호산업 시장규모 2025년 20조원 달성 ※ '20년 11.9조원 → '25년 20조원	
추진 전략	[전략1] 성장 동력 확보를 위한 정보보호 新시장 창출	1 인공지능(AI)기반 보안 산업 활성화
		2 비대면 서비스 보안 시장 개척
		3 융합보안 산업 저변 확대
	[전략2] 글로벌 일류 정보보호기업 육성	1 신성장 리딩 기술·제품 사업화
		2 정보보호 초기기업 성장 지원
		3 정보보호기업 해외진출 가속화
	[전략3] 정보보호산업 기반 강화를 위한 생태계 확충	1 정보보호공시제도 의무화
		2 정보보호인증 고도화
		3 중소기업·지역 사이버보안 안전망 확충
	[전략4] 차세대 정보보호 기술경쟁력 확보	1 정보보호 新기술 개발
		2 디지털 인프라 보안기술 확보

자료: 관계부처합동, '디지털 대전환시대 정보보호산업의 전략적 육성 방안'(2022)

위 그림에서 보는 바와 같이, '디지털 대전환시대 정보보호산업의 전략적 육성 방안'은 크게 4가지 추진 전략을 가지고 있다.

이 중 첫 번째는 성장 동력 확보를 위한 정보보호 신시장 창출이다. 신시장 창출의 첫 번째 세부 전략은 인공지능 기반 보안 산업 활성화로, AI 보안기업(AI For Security, AI 융합보안, AI 역기능 방어 분야)을 단계별, 분야별로 육성하고 시제품 개발을 지원하며, 판로 개척과 해외 진출까지 연계하여 지원하는 계획을 포함한다. 또한, 사이버보안 AI 데이터셋 및 재난·안전 물리보안 데이터를 구축·개방하여 보안제품의 성능 고도화를 뒷받침한다는 전략도 포함한다. 두 번째 세부전략은 비대면 서비스 보안 시장 개척으로, 디지털·비대면 4대 분야(비대면 진료, 비대면 근무, 비대면 교육, 온라인 유통·결제) 서비스에 신보안 기술을 적용함으로써 안전·신뢰 가능한 서비스로 전환을 가속화하며, 오프라인에서는 안심스마트점포 모델을 확산, 테스트베드 구축·지원 등을 통한 AI 물리보안 솔루션의 보안 성능을 제고하는 등의 전략을 포함한다. 세 번째 세부전략은 융합보안 산업 저변 확대로서, 5G+ 융합보안 거점 기능 강화로 안전한 5G 융합서비스 환경을 조성, 실수요자 대상 원스톱패키지 보안 적용 지원 등을 확대하는 내용을 포함하고 있다.

〔그림 3－19〕 인공지능 기반 보안 산업활성화를 위한 사이버보안 AI 데이터셋 개방



자료: 관계부처합동, '디지털 대전환시대 정보보호산업의 전략적 육성 방안'(2022)

두 번째 추진전략은 글로벌 일류 정보보호 기업을 육성하는 것이다. 이를 위하여 첫째 세부 추진전략으로 신성장 리딩 기술·제품을 사업화를 추진하고자 하며, 글로벌 기업간 깃굴 격차가 큰 제품을 과제로 선정하여 전문기업 육성을 지원하고, 우수 정보보호 기술·제품에 대한 판로개척을 지원하는 등을 포함한다. 두 번째 세부 추진전략은 정보보호 초기기업 성장을 지원하고자 하는 것으로, 국내 육성 프로그램, 해외 육성 프로그램, 기술가치 평가 3단계로 맞춤형 기업 육성 프로그램을 운영하며, 금융 애로사항을 해소하기 위한 안정적 자금 운용, 투자·융자 수혜 기회 확대 등의 내용을 포함하고 있다. 세 번째 세

부추진전략으로는 정보보호기업 해외진출 가속화로, 글로벌 권역별 정보보호 시장 현황에 따른 맞춤형 목표를 설정하고 집중 공략하는 것을 목표로 하며, 성능인증, 인지도 제고 등의 약점을 극복하도록 돕고, 현지·초청 쇼케이스 개최 및 해외실증을 지원하는 내용도 포함하고 있다.

〈표 3-10〉 정보보호기업 권역별 맞춤형 지원(안)

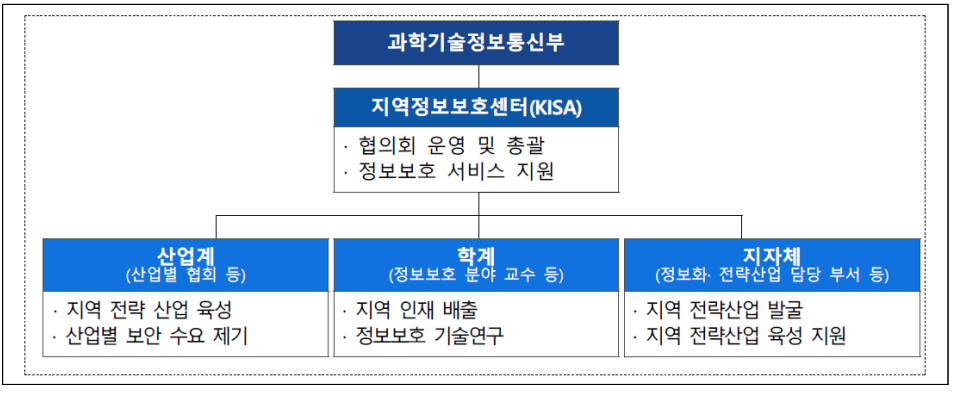
권역	유망분야	주요 세부과제
미국	CCTV 등 물리보안	- 물리보안 분야 선점 기업 정보 및 수출 지원·규제 정책 분석을 통한 전략 수립 및 핵심 수요자 파트너 발굴
동남아	비대면 서비스 보안	- 현지 핵심 플레이어(은행, 보험사 등)와의 파트너십 구축 및 타당성조사, PoC 추진을 통해 현지 사업실력·업계 평판 축적 지원
중남미	국가안보 프로젝트	- 국제개발은행(CABEI 등) 및 협력기구의 공적기금을 활용, 대규모 치안 확보 보안 인프라 프로젝트 수요 제기 및 사업화 추진

자료: 관계부처합동, '디지털 대전환시대 정보보호산업의 전략적 육성 방안'(2022)

세 번째 추진 전략은 정보보호산업 기반 강화를 위한 생태계 확충이다. 이를 위하여 첫 번째 세부 추진전략으로 정보보호공시제도의 의무화가 있다. 이는 이용자의 알권리를 보호하고, 기업의 정보보호 관련 투자를 촉진하기 위한 정보보호 공시 의무화를 시행하고자 하는 것으로, 정보보호산업법 제13조를 근거로 한다. 두 번째 세부추진전략은 정보보호인증을 고도화하는 것이다. 이를 위해 다양한 분야에서 수요가 늘고 있는 IoT 제품 군에 대하여 해킹에 대비한 정보보호 내재화 기반을 마련하기 위하여, 시험자동화 도구 및 신규 인증대상 개발 등 효율적인 보안인증을 추진하는 등의 정책을 포함하며, 정보보호제품 성능평가 제도를 개선하고, 지능형 CCTV 활성화를 위하여 이상상황(이동중 쓰러짐, 원거리 범죄 포착 등) 평가항목에 추가·개발한다. 또한 정보보호업계를 위하여 보안적합성 사전 인증 요건을 확대 하는 등의 시장 친화형 방안도 마련한다. 세 번째 세부추진전략으로는 중소기업·지역 사이버 보안 안전망 확충을 포함한다. 투자여력이 부족한 중소기업을 대

상으로 보안제품 도입 및 데이터 백업 등을 지원함으로써 민간영역의 보안 투자를 확대하고, 지역 정보보호지원센터('22년 10개소)를 중심으로 지역전략산업별 특화된 민간 사이버 구심점을 확립함으로써 지역의 보안내재화를 가속화하는 내용을 포함하고 있다.

〔그림 3－20〕 지역정보보호협의회 구성(안)



자료: 관계부처합동, '디지털 대전환시대 정보보호산업의 전략적 육성 방안'(2022)

마지막으로 네 번째 추진 전략은 차세대 정보보호 기술경쟁력을 확보하는 것이다. 이를 위한 첫 번째 세부 추진전략은 정보보호산업 성장을 위한 정보보호 신기술 개발이다. 사이버공격 대응을 위한 4대 방어 체계(억제→보호→탐지→대응) 중심의 개술개발을 추진하고, 글로벌 공급망 위협에 대응하기 위한 공급망 보안 기술, 6G와 양자를 포함하는 미래 인프라 보호 기술의 선제적 확보를 추진하기 위한 R&D 지원 등을 포함한다. 두 번째 세부 추진 전략은 안전한 디지털 전환을 뒷받침하는 디지털 인프라 보안기술 확보이다. 여기에서는 비대면 보안, 데이터 보호(동형 암호 등), IoT 보안 위협 대응 기술에 대한 R&D 지원을 포함하고 있다.

다. 사이버 보안 관련 인증제도

1) 정보보호 및 개인정보보호 관리체계인증 (ISMS-P)

정보보호 및 개인정보보호 관리체계인증제도(이하 ISMS-P)는 정보통신망 이용촉진 및 정보보호에 관한 법률 제47조, 동법 시행령 제47조~제54조, 개인정보보호법 제32조의 2 및

동법 시행령 제34조의2~제34조의8 등에 근거하여 시행하고 있으며, 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도이다.

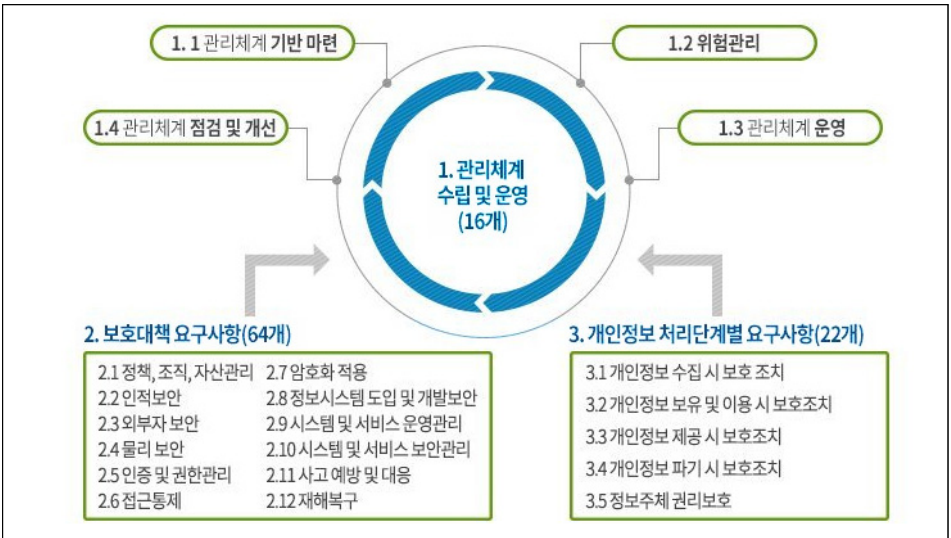
ISMS-P는 정보통신망법 제47조 2항에서 의무대상자를 정하고 있으며, 이는 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 표에서 기술한 의무대상자 기준에 하나라도 해당되는 자이다. 그 외에도, 의무대상자 기준에 해당되지 않으나 자발적으로 정보보호 및 개인정보보호 관리체계를 구축·운영하는 기업·기관은 임의신청자로 분류되며, 임의신청자가 인증 취득을 희망할 경우 자율적으로 신청하여 인증심사를 받을 수 있다.

〈표 3-11〉 ISMS 인증 의무대상자

구분	주요 세부과제
ISP	「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
IDC	정보통신망법 제46조에 따른 집적정보통신시설 사업자
다음의 조건 중 하나라도 해당되는 자	연간 매출액 또는 세입이 1,500억원 이상인 자 중에서 다음에 해당되는 경우 - 「의료법」 제3조의4에 따른 상급종합병원 - 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
	정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
	전년도 직전 3개월간 정보통신서비스 일일평균 이용자 수가 100만명 이상인 자

자료: https://isms.kisa.or.kr/main/ispims/target/

〔그림 3－21〕 ISMS-P 인증기준



구분		통합인증	분야(인증기준 개수)	
ISMS-P	ISMS	1.관리체계 수립 및 운영(16)	1.1 관리체계 기반 마련(6) 1.3 관리체계 운영(3)	1.2 위험관리(4) 1.4 관리체계 점검 및 개선(3)
		2.보호대책 요구사항(64)	2.1 정책, 조직, 자산 관리(3) 2.3 외부자 보안(4) 2.5 인증 및 권한 관리(6) 2.7 암호화 적용(2) 2.9 시스템 및 서비스 운영관리(7) 2.11 사고 예방 및 대응(5)	2.2 인적보안(6) 2.4 물리보안(7) 2.6 접근통제(7) 2.8 정보시스템 도입 및 개발 보안(6) 2.10 시스템 및 서비스 보안관리(9) 2.12 재해복구(2)
	-	3.개인정보 처리단계별 요구사항(22)	3.1 개인정보 수집 시 보호조치(7) 3.3 개인정보 제공 시 보호조치(3) 3.5 정보주체 권리보호(3)	3.2 개인정보 보유 및 이용 시 보호조치(5) 3.4 개인정보 파기 시 보호조치(4)

자료: https://isms.kisa.or.kr/main/ispims/intro/

2) 정보보호등급제

정보보호등급제도는 정보보호 관리체계(ISMS)를 유지하는 기업 대상으로 정보보호 수준을 측정하여 '우수', '최우수' 등급을 부여하는 제도로, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조의 5 및 동법 시행령 제55조의2~제55조의5에 근거한다. 이 제도는

이용자로 하여금 객관적인 기업 선택의 기준을 제시하고, 기업의 신뢰수준 및 비교 우위 경쟁력 확보를 지원하며, 기업의 정보보호 활동 기준 및 목표 수준을 마련하는데 그 효과가 있다. 정보보호 등급 부여기준은 다음과 같다.

〈표 3-12〉 정보보호 등급 부여기준

등급	등급 설명	등급 취득 기준
우수	기업에 내재된 정보보호 통제 및 프로세스를 지속적으로 측정, 관리하는 단계로 정기적으로 정보보호 상태를 점검하는 단계	우수 등급(공통+우수)에 해당하는 세부 평가기준을 모두 만족
최우수	정보보호 통제 활동에서 얻어진 문제점을 지속적으로 개선하여 반영함으로서 기업의 정보보호 수준을 최적화 하는 단계	우수등급과 최우수 등급(공통+우수+최우수)의 세부 평가기준을 모두 만족

자료: https://isms.kisa.or.kr/main/isrs/intro/

3) 클라우드보안인증제

클라우드보안인증제도는 클라우드 서비스 제공자가 제공하는 서비스에 대해『 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률 』제 23조 제2항에 따라 정보보호 기준의 준수여부 확인을 인증기관이 평가・인증하여 이용자들이 안심하고 클라우드 서비스를 이용할 수 있도록 지원하는 제도이다. 이 제도는 공공기관에 안전성 및 신뢰성이 검증된 민간 클라우드 서비스를 공급하는 것이 목적이다.

〈표 3－13〉 클라우드 서비스 유형 및 평가대상

구분	주요 세부과제
IaaS	컴퓨팅 자원(CPU), 스토리지 등 정보시스템의 인프라를 제공하는 서비스
SaaS	인프라(IaaS) 외에 각종 응용프로그램(소프트웨어)을 제공하는 서비스
PaaS	클라우드 관련 서비스를 개발하는 환경(플랫폼) 제공
DaaS	가상 PC 제공을 위한 서비스 ※ 행정・공공기관 인터넷망 PC 대체를 위해 도입하는 가상PC

자료: KISA, '클라우드서비스 보안인증제 안내서'(2020)

클라우드서비스 보안인증의 인증 종류는 IaaS, SaaS 표준등급, SaaS 간편등급, DaaS가 있으며, IaaS 분야 및 DaaS 분야 인증 유효기간은 5년, SaaS 분야 인증은 표준등급에 대해서는 유효기간을 5년, 간편등급에 대해서는 유효기간을 3년으로 운영하고 있다.

보안 기능을 포함하는 클라우드 서비스를 제공하는 경우, 각 보안 기능들이 도입인증 요건(예, CC인증, 보안기능 확인서, 검증필 암호모듈 등)을 갖춘 정보보호 제품 유형에 해당되는지를 확인하여야 한다.

4) 정보통신망연결기기등 정보보호인증

정보통신망연결기기등 정보보호인증 제도는 IoT제품(및 연동앱) 등 정보통신망연결기기가 일정 수준의 보안성을 갖추었는지를 시험하여 인증 기준에 적합한지를 검증하는 제도이다. 해당 인증 기준으로는 1) 식별 및 인증, 2) 데이터 보호, 3) 암호, 4) 소프트웨어 보호, 5) 업데이트 및 기술지원, 6) 운영체제 및 네트워크 보안, 7) 하드웨어 보안 등 7개 영역에 대해 평가한다.

정보보호인증은 요구되는 보안수준에 따라 라이트(Lite), 베이직(Basic), 스탠다드(Standard)의 3가지의 인증유형으로 구분되며, 인증신청인은 IoT 기기에 대해 3개의 인증유형 중 하나를 선택하여 정보보호인증을 신청해야 한다. 해당 인증유형에서 필수적으로 요구되는 인증기준을 모두 만족하는 경우에만 해당 인증유형의 인증서가 발급된다.

〈표 3-14〉 정보보호인증의 유형

인증유형	내용	비고
라이트	단순 해킹공격에 대응할 수 있는 필수 보안조치 수준 (개인정보를 수집·저장·전송 등 취급 시 라이트 신청 불가)	센서 등 펌웨어 기반의 소형 IoT 기기에 적합
(라이트+)	라이트 등급의 인증기준 및 추가 인증기준 포함	
베이직	중요 정보의 불법적인 접근을 차단하고 노출방지에 대응할 수 있는 일반적인 보안조치 수준	저사양 OS를 탑재한 중소형 IoT 기기에 적합
(베이직+)	베이직 등급의 인증기준 및 추가 인증기준 포함	
스탠다드	고도의 해킹공격에 대응할 수 있고 국제적인 요구사항을 포함한 종합적 보안조치 수준	중대형 스마트가전 제품 등 IoT 기기에 적합
(스탠다드+)	스탠다드 등급의 인증기준 및 추가 인증기준 포함	

자료: KISA, '정보통신망연결기기등 정보보호인증기준 상세 해설서'(2022)

5) 보안적합성 검증

보안적합성 검증 제도는 국가정보통신망의 보안수준 제고를 위해 「국가정보원법」 제4조와 「전자정부법」 제56조에 의거, 국가 · 공공기관이 도입하는 정보보호시스템 · 네트워크 장비 등 보안기능이 탑재된 IT제품 및 저장자료 완전삭제제품의 안전성을 검증하는 제도이다. 공공기관은 특정 보안제품군 및 유형에 대해서 도입요건을 규정하고 있는데, 예를 들어, 침입차단시스템(Firewall)의 경우, CC인증 혹은 보안기능 확인서가 있어야 한다. 그 외 일부제품은 검증필 암호모듈(CMVP) 등을 추가로 요구하기도 한다.

CC인증은 보안기능이 있는 IT 제품(즉, 정보보호제품)의 보안성을 평가기관에서 평가하고 이에 대한 결과를 인증기관에서 인증하는 제도이며, 우리나라는 국가정보원이 필요성을 인정하는 정보보호제품의 경우 국가·공공기관에서 CC 인증제품을 도입하도록 하고 있다.

보안기능 시험제도는 보안적합성 검증절차 간소화를 위해 정보보호시스템 · 네트워크 장비 등 IT 제품의 안전성을 사전 확인하는 제도이며, 해당 시험을 통하여 보안요구사항을

만족한 제품에 대해 보안기능 확인서를 발급받게 된다.

4. 시사점 및 정책 추진 방향

사이버 보안 산업은 앞서 언급한 바와 같이 국내·국외 시장 모두 급성장 중인 산업이다. 새로운 ICT 기술이 등장하고, 이러한 ICT 기술이 사이버 환경 뿐만 아니라 실세계의 다양한 서비스와 결합하면서 그 영역이 더욱 넓어짐으로써 사이버 보안 기술·제품을 통하여 보호해야 할 대상과 가치가 더욱 확대되고 있기 때문이다. 또한, 보안 위협이 실현될 경우 그 피해가 개인·기업·기관·국가 등 사회 전반에 걸쳐 영향을 미칠 수 있기 때문에 국가 안위를 책임지는 방위 산업으로 볼 수 있다.

사이버 보안 산업은 미래지향 신성장 산업이면서 국가 방위 산업의 특징을 모두 가지고 있기 때문에, 최근 우리 나라 뿐만 아니라 각국에서는 시장을 성장시키면서도 자국의 사이버 보안 기업을 보호하기 위한 정책을 적극적으로 반영하기 시작했다. 우리 나라 뿐만 아니라 전세계 대부분의 국가들은 사이버 보안 시장이 빠른 속도로 성장을 하고 있기에, 글로벌 대기업들로부터 자국 산업을 보호함과 동시에 자국의 안보 체계를 외산 기업에 내주지 않고자 한다.

미국의 많은 사이버 보안 기업들이 유럽, 영국, 일본, 한국 등 다양한 국가에 진출하여 시장을 잠식하고 있음에도, 미국의 국가적 정책 역시 예외가 아니다. 자유로운 시장경제 질서를 선호하지만, 한편으로는 타 산업과 다르게 국가 안보에 직결되는 사안이기 때문에, 미국 역시 시장에 대한 민주적 통제를 선호하는 유럽 등과 유사하게 프라이버시를 강화하면서도 사이버 위협에 대한 가시성을 확보하는 정책을 펴고 있다. 미국은 글로벌 시장을 주도하는 만큼 시장 보호 정책을 강하게 드라이브하지는 않지만, 언제라도 타국에 시장을 점유당하기 시작할 경우 그러한 정책을 펼 수 있을 것으로 보인다.

우리 나라는 다른 국가와 비교하였을 때, 사이버 보안 시장의 양적 규모가 과거와 비교하여 상당히 빠르게 성장했다고 볼 수 있다. 그러나, 문제는 사이버 보안 유니콘 기업 42개 중 한국 기업이 전무하며, 글로벌 시장을 선도하는 기업이 거의 없다는 점이다.최근 사

이버 보안 분야는 진화하는 위협에 대응하기 위한 신기술의 지속적 연구 개발이 필요할 뿐만 아니라, 암호, 인증, 정밀한 수준에서의 접근 제어, 네트워크 모니터링 및 시각화, 네트워크 가상화, 인공지능 기반 이상행위 탐지 등을 모두 통합하여, 공격 예방・탐지・대응 관점에서 패러다임의 변화 중에 있다. 그러나, 국내 사이버보안 기업들의 규모는 대체로 크지 않으며 이러한 보안 솔루션의 개발이 회사별로 파편화되어 통합하기 힘든 구조로 되어 있어, 신기술 개발과 보안 패러다임의 변화에 대응하기 쉽지 않다.

이러한 시기에, 2021년 국가필수전략기술 중 하나로 사이버보안을 선정하고, 2022년 정보보호산업의 전략적 육성 방안을 발표한 것은 시의적절하다고 볼 수 있다. 해당 전략은 1) 성장 동력 확보를 위한 정보보호 신시장 창출, 2) 글로벌 일류 정보보호 기업 육성, 3) 정보보호산업 기반 강화를 위한 생태계 확충, 4) 차세대 정보보호 기술 경쟁력 확보로 나뉘며, 이에 따르는 세부 전략을 포함하고 있다.

핵심은 이러한 세부 전략의 구체적 실행 과정에 있을 것이다. 아무리 좋은 전략을 세워도, 현업에 현실적으로 도움이 되는 구체적 실행 과정이 필요하다. 특히, 새로운 보안 패러다임의 전환은 현재 정부가 추진하고 있는 '디지털플랫폼정부'와도 연관성이 깊다고 볼 수 있다. 보안 패러다임의 전환은 민간에서 주도할 수 있는 일이 아니며, 특정 기업이나 연구소 등이 주도하기에 그 범위가 매우 방대하다. 따라서, '디지털플랫폼정부' 추진 과정에서 사이버 보안의 중요성을 이해하고, 새로운 보안 패러다임을 시범 적용해봄으로써 민간에게 방향성을 제시할 필요가 있다.

또한, 2022년에 발표한 정보보호산업의 전략적 육성 방안은 전임 정부에서 발표된 정책이나, 2015년 'K-ICT 시큐리티 발전전략', 2016년 '제1차 정보보호산업 진흥계획', 2019년 '국가사이버안보전략', 2020년 '제2차 정보보호산업 진흥계획' 등과 그 맥이 닿아 있다. 따라서, 현 정부도 사이버 보안산업을 육성하는 기조이므로 가급적 전임 정부에서 마련한 정책이라 하더라도, 일부 수정・보완을 통하여 일관성있게 추진하는 것이 필요하다.

마지막으로, 3.2절에서는 사이버 보안 산업과 관련한 정책을 언급하고 있으나, 산업은 사이버 보안 신기술 연구개발, 사이버 보안 인증 제도, 보안 위협 대응 전략과도 모두 연관이 있다. 이러한 정책 개발 및 추진 과정에서, 각 부처별로 전략을 세울 경우 중복 투자의 가능성이 있으며, 일관된 제도 수립이 쉽지 않을 수 있을 것이다. 따라서, 앞서 3.1절에서 언급한 바와 같이, 사이버 보안 컨트롤 타워 혹은 국가차원에서의 통합적 사이버 보안 위협 대응 체계가 필요한 것과 마찬가지로, 부처별 역할을 정의하고 소관 업무를 조정할 수 있는, 국내 사이버 보안 산업의 진흥과 보호를 책임질 수 있는 컨트롤 타워에 대한 논의도 필요할 것이다.

제3절 R&D, 인력 양성 정책 현황과 미래 전략

1. 개요

사이버 보안 역량 강화를 위해 차세대 사이버 보안 기술 개발과 인력 양성을 위해 많은 투자가 필요한 것은 자명하다. 주요 선진국 뿐 아니라 우리나라도 사이버 보안의 중요성을 인식하고 이에 대한 기술 개발과 인력 양성에 대한 투자를 꾸준히 늘리고 있는 상황이다. 본 절에서는 사이버 보안 R&D와 인력 양성에 대한 국외, 국내 정책을 살펴보고 미래 전략을 제시한다.

2. 국외 현황

가. 미국

2019년 9월 미국은 ICT R&D 프로그램인 NITRD[4] (THE NETWORKING & INFORMATION TECHNOLOGY RESEARCH & DEVELOPMENT PROGRAM)에서 55억 달러 규모의 11개 분야 투자 영역을 선정하였다. 그 중 사이버 보안은 6,600억원 정도로 전체의 12%를 차지한다.

2019년 5월 미국 트럼프 대통령은 'Executive Order on Securing the Information and Communications Technology and Services Supply Chain'과 'Executive Order on America's Cybersecurity Workforce'의 두 행정 명령을 내렸다. 전자는 정보통신 기술 및 서비스에 대한 위협에 대처하기 위해 ICT 공급망 보호에 관한 행정명령으로 공급망 보안에 대한 미국 행정부의 인식이 높아졌음을 시사한다. 후자는 사이버 보안 인력 확충에 관한 행정명령으로 사이버 보안 인력 양성의 필요성이 높아졌음을 나타낸다. 주요 내용으로는 대통령배 사이버보안 연례 경진대회 개최, 사이버보안 전문성 증진을 위한 연방직원 직무순환 프로그램 개시, 사이버보안 인력 프레임워크 도입 확산, 사이버보안 적성 평가 실시, 시스템에 대한 보안 인력 부족 해소 등이 있다.

---

4) NITRD - 각 부처별 ICT 분야 R&D 사업들을 하나로 통합한 범부처 ICT R&D 프로그램으로, 대통령 직속기구인 국가과학기술위원회(NSTC) 관리 하에 운영된다.

이 두 행정명령은 외국 적대세력의 위협으로부터 미국의 안보와 시민의 안전을 보호하고 미국 내 공급 및 사용되는 ICT와 서비스의 보안성, 무결성, 신뢰성을 보장함으로써 안보 위협에 대처하기 위한 것이다.

나. 영국

2016년 영국 정부는 국가 사이버 보안 전략 발표를 통해 사이버 보안에 대한 중요성을 인식하고 있다. 이와 함께 필수산업 분야, 신산업 분야 등 각 산업분 야에서의 사이버 공격에 대해 보호 전략을 발표하며 사이버보안 기술 발전을 지원하고 있다. 이 발전 전략에는 향후 5년간 19억 파운드(2조 7천억 원)를 사이버 보안 분야에 투자하기로 하였고, 국가 사이버 보안 센터(NCSC)와 런던 사이버 보안 혁신 센터(LORCA)를 설립하여 사이버보안 인력을 양성하고 기업을 지원하기로 하였다. 특히 필수 서비스 사업자는 효과적인 사이버 보안 조치를 취해야 하며 필수 네트워크와 인프라를 안전하고 복원력 있도록 관리 해야 한다. 이런 조치가 부족한 경우 새로운 유형의 벌금이 부과될 예정이다.

다. 독일

독일 정부는 적극적으로 사이버보안 기술 역량 확대를 위해 지원하고 있다. 최근에는 응용 사이버 보안 국가연구센터(ATHENE, https://www.athene-center.de/en/)를 설립하였다. ATHENE는 응용 사이버 보안 연구 분야에서 가장 큰 규모의 연구 조직으로 독일 연방 정부와 헤센 주의 사이버 보안 연구 프로그램의 일환으로 설립되었다. ATHENE은 프라운호퍼 연구협회의 인프라에 2개 대학교를 연계시키는 협력 모델 외에도 연구 프로젝트 수행을 중심으로 새로운 유형의 네트워크 취약점이나 공격에 민첩하게 대응할 수 있도록 하고 있다. 독일 연방 정부와 헤센 주 정부는 2019년 기준 1,250만 유로에서 2026년 기준 3,700만 유로까지 사이버 보안 연구 지원을 확대하여 연구 역량을 확대할 예정이다.

라. 일본

일본은 2019년 5월 NISC(National center of Incident readiness and Strategy for Cybersecurity)에서 사이버 보안 2019를 발표하였다. NISC는 사이버 보안 정책을 담당하는

총리실 직속 사이버보안 전략본부의 사무국이다. 이 발표의 핵심은 2020 동경올림픽 사이버 안전 확보, IoT 디바이스 보안강화, 사이버 안전사고의 탐지, 보고 및 대응 체계, 이와 관련한 사이버 보안 인재 양성으로 되어있다.

사이버보안 전략본부는 2017년에 4차 보안대책을 통해 중요 인프라에 대한 사이버 공격과 자연 재해에 따른 주요 인프라의 서비스 장애 및 복구 대책을 제시하였다. 또한 "사이버보안 인재양성 프로그램"을 발표하여 민간 사이버 보안 인재 양성을 계획하였다.

3. 국내 현황

가. 2019년 2월 4차산업혁명위원회 정보보호 R&D 중장기 전략

우리 정부는 2019년 2월 4차산업혁명위원회에서「민간부문 정보보호 R&D 중장기 계획」을 발표하였다. 이는 4차 산업혁명 시대에 혁신적인 성장을 위한 중요한 기반 기술인 정보보호 기술력 강화를 위한 중장기적 전략이다. 특히 2026년까지 G2급 글로벌 수준의 정보보호 기술 경쟁력을 확보하기 위해 지속적인 정보보호 기술 개발을 하는 것이다. 그리고 과학기술정보통신부가 진행하고 있는 정보보호 산업 핵심원천기술 개발 사업 규모를 2015년 298억 원에서 2019년는 619억 원으로 약 2배 이상 증가시키는 것이다. 그러나 ICT R&D 대비 정보보호 R&D 비중은 미국이 약16%, 일본이 20%, 한국은 6.5%로 나타나 여전히 사이버 보안 기술 투자 비중은 낮은 편이다.

중장기 전략의 추진 전략으로 정보보호 중장기 핵심기술 개발, 혁신적 R&D 추진, 정보보호 산업경쟁력 강화, 수요자 참여 R&D 생태계 조성을 발표하였다.

- 정보보호 중장기 핵심기술 개발: 빅데이터 비식별화, 양자컴퓨터 대응 암호 등 데이터 보호 기술과 ICT 서비스 플랫폼 침해 공격을 자동으로 탐지・분석・대응・예방하는 기술을 개발하고, 5G 기반 융합서비스 보호를 위해 지능형 엣지보안 등 초연결 네트워크 보안 기술과 급증하는 스마트 디바이스에 대한 악성행위와 신규위협에 대응하기 위한 기술을 개발할 예정이다. 또한, 관제센터(KISA 인터넷침해대응센터 등), 이동통신사, 금융사 등 기술수요처를 통해 중점기술들을 실증하고, 연구성과물의 활용성을 높일 계획
- 혁신적 R&D 추진: 창의・도전적 신기술 개발을 유도하고 국민이 체감할 수 있는

생활안전 분야 R&D도 추진할 계획이다. 올해부터 사이버보안 그랜드 챌린지를 추진해 신기술 분야 우수연구자를 집중지원, 고난이도 신기술 연구와 미래 위협에 대한 장기적 연구를 위해 정보보호 전문연구실을 확대 개편하고 사생활 침해, 치안 등 국민 실생활과 밀접한 사이버보안 이슈를 해결하기 위해 정보보호 리빙랩 사업을 추진

- 정보보호 산업경쟁력 강화: 우수 스타트업 발굴·기술지원, R&D 데이터 공유, 전문 인력양성, 기업 국제공동연구 등도 추진
- 수요자 참여 R&D 생태계 조성: 수요자 참여기반의 개방형 연구 생태계를 조성하고 정보보호 기술개발 전략의 지속성을 강화할 방침이다. 공공 및 민간 현장에서 요구되는 사항이 반영돼 성과까지 이루어지도록 수요기관협의체와 성과확산전담반을 운영하고, 국경 없는 사이버전, 국가안보 위협 대비를 위해 장기적으로 기술개발 전략을 수립·관리하는 기술전략 연구실을 운영
- 출처: 2019년 4차산업혁명위원회「민간부문 정보보호 R&D 중장기 계획」

나. 2019년 4월 국가사이버안보전략

2019년 청와대에서 국가사이버안보전략을 발표하였다. 그 중 전략과제 4의 사이버 보안 산업 성장기반 구축에서 인력 양성과 기술 개발에 대한 정책을 살펴볼 수 있다. 전략과제 4는 사이버보안산업 성장기반구축으로 국가 사이버안보의 기반역량이 되는 기술·인력·산업의경쟁력 확보를 위해 제도 개선, 지원 확대 등 보안산업 혁신 생태계 조성을 포함한다. 특히 전략과제 4. 의 내용 중 인력, 기술 관련 내용은 다음과 같다.

- 2 보안 인력·기술 경쟁력 강화
- 1) 고도화되는 사이버안보 위협에 대응할 수 있도록 세계 최고 수준의전문성과 경쟁력을 갖춘 사이버보안 인재를 집중 육성한다.
- 2) 기업, 정부, 군 등 국가사회 전반에 다양한 역량을 갖춘 인력이공급될 수 있도록 생애주기별 맞춤형 인력양성 프로그램을 강화한다.
- 3) 사이버보안 업무 전문성을 향상시키고 우수 인재를 유치하기 위한 사기 진작방안을 마련한다.

- 4) 선진국과 기술격차를 해소하고 글로벌 시장을 선도할 혁신적원천기술 확보를 위해 사이버보안 연구개발 예산을 대폭 확대한다.
- 출처: 2019년 청와대 국가사이버안보전략

다. 2020년 6월 과기정통부 「제2차 정보보호산업 진흥계획」

2020년 과기정통부에서 제2차 정보보호산업 진흥계획을 발표하였다. 과거 제1차 정보보호산업 진흥계획(2016~2020년)을 통해 지난 5년간 정보보호산업은 양적 성장을 이루었다. 이후 코로나19에 따른 디지털 전환과 비대면 디지털 서비스 확산으로 인한 사이버 위협이 이전에 비해 매우 커지게 되었고, 이런 위협에 대응하기 위해 정보보호산업의 질적 성장과 질적 개선이 필요하게 되었다. 이러한 디지털 환경 변화에 따라 새로운 정보보호 수요가 나타났고 정부는 이를 산업 활성화로 연결하기 위한「제2차 정보보호산업 진흥계획」을 같이 관계부처 합동으로 수립하였다.

이는 정보보호 신규 시장 발굴, 민간 주도의 정보보호 투자 확대 및 정보보호 성장 생태계 조성을 통한 정보보호산업 성장을 목표로 하고, 5년간(2021~2025년) 관계부처 합동으로 정보보호시장 10.5조에서 20조원 달성, 5년간 정보보호 전문기업(매출 300억원 이상) 37개에서 100개까지 육성, 5년간 정보보호 전문인력 인재 3만명 양성 및 일자리 창출을 세부 목표로 설정하였다.

구체적 내용은 다음과 같다.

- 첫째, 국민생활과 사회 전반에서의 디지털 안전 확보를 목적으로 하는 정보보호 패러다임 변화를 新시장 공략의 기회로 삼는다.
  - 비대면 서비스에 클라우드, 생체인식 등 신기술을 적용하는 보안강화 시범사업으로 서비스별 특징을 반영한 보안시장을 육성한다.
  - 보안이 부족한 영세 중소기업에 대해서는 보안컨설팅과 클라우드 등 안전한 업무용 서비스로의 전환을 지원한다.
  - 보안서비스의 AI 확산을 위해 한국인터넷진흥원이 보유한 정보보호 데이터(6.9억개) 등을 학습데이터로 활용하고, AI 활용 보안제품의정확도 개선과 제품 고도화를 지원한다.

- CCTV 등 다양한 제조사의 물리보안 제품을 연결하여 무인점포, 재난안전 등 물리보안을 활용한 사업모델을 개발하여 확산시킨다.
- ICT 융합산업 분야별 보안모델을 개발하여 공공분야 현장 적용*과 함께, 관련 부처들과 각 산업분야 개별법에 정보보호를 제도화하여 융합보안 시장 확산을 유도한다.

• 둘째, 민간 주도의 사이버 복원력(공격 후 이전 상태로 복구할 수 있는 역량) 확보를 위해 정보보호 투자를 확대하고 경쟁력 있는 정보보호기업을 육성한다.
- 대규모 국가 투자사업, 5G 국가망 등 선도 프로젝트에는 정보보호 투자가 포함되도록 하고, 지역의 정보보호지원센터를 확대하여 기업 정보보호 수준 제고를 위한 자발적인 투자를 유도한다.
- 정보보호기업 성장을 위해 지원시설 · 사업을 집적한 성장기반을 조성하고, 한국형 '비대면+보안 패키지 모델' 등을 개발하여 해외시장 개척을 통해 기업규모를 확대한다.

• 셋째, 지속성장 가능한 정보보호산업 생태계를 조성한다.
- 안전한 데이터 활용과 AI를 응용한 보호기술 개발, 양자암호 등 차세대 핵심 보안기술 확보를 위한 연구개발을 확대하고,
- 수요자 관점에서의 편리하고 부담을 줄일 수 있도록 규제개선과 정보보호 전문인력 양성도 3만명을 목표로 추진한다.

• 출처: 2020년 6월 과기정통부 「제2차 정보보호산업 진흥계획」

라. 2022 사이버보안 인력 양성 사업

한국인터넷진흥원(KISA)이 발표한 국내 정보보호 인력 수급전망에 따르면 2022년 국내 시장에 신규로 공급될 전문인력은 4229명인 반면, 신규 수요는 5953명으로 공급이 약 1724명 부족하다. 이러한 현상은 매년 지속돼, 2025년에는 신규 공급 인력이 2116명 부족할 전망된다. 이런 부족 인력 양성을 위해 다음과 같은 사업을 시행한다.

• 정보보호 특성화대학: 산학협력 기반 국내 대학 직무 중심 정보보호 전문인력 양성
• 융합보안대학원: 지역전략산업 특화, 산학협력으로 융합 보안 전문인력 양성

- K실드(K-Shield) : 최정예 정보보호 전문가 교육 과정
- K실드(K-Shield) 주니어 : 정보보호 산업계 취업 희망 구직자 대상, 기업 실무 기반 교육으로 산업에 즉각 투입 가능한 인력 양성
- 실전형 사이버훈련장: 가상환경에서 침해사고 사례 기반의 공격·방어 훈련 등을 통해 정보보호 인력 실전 대응 역량 강화
- 산업보안 전문인력 양성: 정보보호 분야 재직자 대상 산업 맞춤형 현장 전문인력 양성
- 전자정부 전문교육: 정보보호 담당자·정보보호 휴관 업무 담당자의 정보보호 기획, 관리 등 역량 강화

마. 2022년 7월 13일 과기정통부 사이버 10만 인재 양성 방안 발표

2021년 12.4만명에서 2026년 16.3만명의 사이버 보안 인력 수요가 예상되어 약 4만명의 신규 인력 수요 발생이 전망된다. 이런 전망속에 산업계에서는 사이버 보안 전문 지식을 갖춘 인재의 부족함을 호소하고 있는 상황이다. 이에 융합보안대학원을 8개에서 12개로 늘리고 화이트햇스쿨(화이트해커) S-개발자(보안개발자) 도입을 통한 인재의 재능사다리 마련, 실전형 '사이버훈련장'의 지역·온라인기반 확대로 인력 상시 육성환경 마련- 군 사이버작전 역량 강화를 위한 '사이버 탈피오트', '사이버 예비군' 도입을 추진한다.

2022년~2026년 10만 사이버 인재 양성을 목표로 신규 공급 인력 4만명, 재직자 연략 강화를 통해 6만명의 인력 양성을 계획하였다. 신규 공급 인력 4만명의 경우 정규과정 1만명, 특화 교육을 통해 3.9만명을 양성하는 것을 목표로 한다. 재직자 연략 강화 6만명의 경우 사이버 훈련장을 통한 2.5만명, 지역교육센터를 통한 2.6만명 양성을 목표로 한다.

최정예 육성 체계로 일반 개발자와 사고 대응을 수행하는 화이트 해커를 대상으로 화이트햇 스쿨, S-개발자 등이 고급 인력 양성 프로그램을 신설한다.

바. 2022년도 과기정통부 연구개발사업 종합시행계획

2022년도 과기정통부 연구개발사업 종합시행계획에 따르면 사어비 보안과 관련한 사업으로는 정보보호 핵심 원천 기술 개발 사업과 사이버 보안 챌린지 선도 기술 개발 사업 등

이 있다. 2021년에 비해 15% 정도가 증가하여 약 850억원 정도 규모이다.

4. 중장기 전략

사이버 보안 인력 양성과 관련하여 새 정부에서 10만 인재 양성 등 강력한 의지를 보이고 있다. 양적인 부분에 대해서는 긍정적이며 다만 이에 대해 새로운 인력 양성 방향과 구체화 노력이 필요할 것으로 보인다. 이를 위해 산업계의 수요를 반영한 인재 양성 정책을 수립해야 한다. 산업계의 수요라 함은 필요한 인력의 유형뿐 아니라 재교육이 어려운 중소기업들을 고려한 정책이 필요하다. 이를 위해 온라인, 무료 교육도 가능하겠으나 재교육에 대한 인센티브 지급도 고려할만할 것이다. 반대로 재교육 미실시의 경우 패널티를 부과하는 방안도 있을 수 있겠으나 부정적인 방법보다는 긍정적인 방법이 더 효과가 있을 것이다.

사이버 보안은 특히 개개인의 능력에 따라 결과가 매우 차이가 큰 분야이다. 즉, 소수의 뛰어나 해커가 활동하는 분야인만큼 이에 대응하기 위한 충분한 고급 인재가 필요할 수 있다. 또한 이러한 고급 인재를 대기업에서는 충분히 채용가능하다. 중소기업에서는 채용하기가 쉽지 않다. 따라서 이를 해결하기 위한 전략이 필요할 것으로 보인다. 기업의 보안을 지키면서 고급 인력을 공유하거나 기존 인력의 재교육을 통한 고급 인력 양성 등의 정책이 가능할 것이다.

우리나라는 많은 분야에서 지역간 차이가 발생하는데, 사이버 보안 인력 수준도 마찬가지이다. 수도권에 고급 인력이 몰려있고 지방 소재 기업에서는 고급 인력을 찾기가 어렵다. 이러한 불균형을 해소할 수 있는 지역 우대 정책이나 수도권 고급 인력이 지방 소재 기업의 보안 담당자와 함께 협업할 수 있는 환경 등을 마련해주는 정책이 가능할 것이다.

제4장 결 론

인공지능을 포함한 정보통신(ICT) 기술의 발전으로 다양한 분야에서 고도화된 정보통신 기술이 활용되고 디지털 전환을 가속화하고 있다. 이러한 디지털 전환은 사이버 보안 위협이 컴퓨터 시스템 수준에 머무르지 않고 재산과 생명에까지 직결되는 수준으로 커졌으며, 그 위협이나 공격이 점차 복잡, 다양해지고 있다. 즉, 사이버 공격 사후 조치만으로는 그 피해를 줄이는 것이 한계에 다다르고 있어 사전 예방을 위한 보안 역량을 최대로 끌어올려야 하는 상황이다. 여기에는 사이버 보안 기술의 발전과 함께 적절한 지원과 정책 또한 뒷받침되어야 함은 자명하다.

본 연구에서는 디지털 공동 번영을 위해 이러한 사이버 보안의 중요성을 다시 한번 강조하고, 국내외 사이버 보안 기술 동향을 확인하고 지속 가능한 디지털 전환과 디지털 플랫폼의 신뢰성 제공을 위한 차세대 사이버 보안 기술 방향을 제시하였다. 추가로, 우리나라와 주요국들이 사이버 보안 정책 현황을 살펴보고 중장기적으로 정부의 지원 및 규제, 지원 방향에 대해 논의하였다.

사이버 보안 기술을 공통 보안 기술, 시스템・네트워크 보안 기술, 융합 보안 기술로 나누어 현황과 미래 기술 방향을 제시하였다. 공통 보안 기술로는 암호 기술, 인증・인가 및 접근제어 기술, 데이터 보안, 하드웨어 기반 보안, AI 보안에 대한 현황과 미래 기술 방향을 제시하였다. 시스템・네트워크 보안 기술로는 사이버 위협 인텔리전스(CTI), 랜섬웨어 대응, IoT 디바이스 보안, 5G 보안, 클라우드 보안, 공급망 보안에 대한 현황과 미래 기술 방향을 제시하였다. 융합 보안 기술로는 스마트 시티 보안, 스마트 자율 주행 이동체 보안, 디지털 헬스케어 보안, 스마트 공장 및 산업제어 보안에 대한 현황과 미래 기술 방향을 제시하였다.

공통 보안 기술과 시스템・네트워크 보안 기술 분야에 대해서는 기술 발전 방향을 2030년까지의 기술 개발 로드맵과 기술 발전 시나리오 방식으로도 제시하였다. 기술 발전 시

나리오에서는 현재 사이버 보안 기술 수준으로 인한 문제점과 이를 해결할 발전된 미래 기술을 제시하고 미래 기술 수준에 도달하는 데 필요한 기술을 제시하였다. 기술 발전 시나리오에는 무자각 인증, 양자 대비 암호, OT 통합 보안, AI 기반 보안 관제에 대한 미래 기술을 포함하였다.

본 연구에서는 위와 같은 사이버 보안 기술에 대한 제시만이 아니라 사이버 보안 관련 정책 현황과 미래 전략에 대해서도 논의하였다. 더 구체적인 논의를 위해 정책 현황과 미래 전략을 보안 위협 대응 정책, 보안 산업 정책, R&D・인력양성 정책으로 나누어 제시하였다.

현재 우리나라이 사이버 보안 위협 대응 체계는 여러 기관에 분산되어 대응 체계를 하나로 통합할 필요가 있다는 점에 대해서는 모두 동의하고 있지만 방법론에 있어서 다양한 이견이 존재한다. 국가차원의 통합적 사이버 보안 위협 대응 체계 수립을 위한 다양한 법안들이 발의되었으나 합의에 이르지 못해 아직 입법화되지 못하고 있다. 우리나라의 경우 사이버 보안 컨트롤 타워 역할 부여로 정보 기관의 역할이 강화되는 것에 대한 사람들의 우려, 사이버 보안 관련 청와대 내 전문성 부족, 현재 각 부처에서 독립적으로 수행 중인 사이버 보안 업무 통합의 어려움 등 다양한 사항들을 고려하여 국가차원의 통합적 사이버 보안 위협 대응 체계 수립을 위한 논의가 필요할 것이다.

우리 나라는 다른 국가와 비교하였을 때, 사이버 보안 시장의 양적 규모가 과거와 비교하여 상당히 빠르게 성장했으나 국내 사이버 보안 기업들의 규모는 대체로 크지 않으며 보안 솔루션의 개발이 회사별로 파편화되어 통합하기 힘든 구조로 되어 있어, 신기술 개발과 보안 패러다임의 변화에 대응하기 쉽지 않다. 이러한 시기에, 2021년 국가필수전략기술 중 하나로 사이버보안을 선정하고, 2022년 정보보호산업의 전략적 육성 방안을 발표한 것은 시의적절하다고 볼 수 있다. 핵심은 이러한 세부 전략의 구체적 실행 과정에 있을 것이다. 또한 '디지털플랫폼정부' 추진 과정에서 사이버 보안의 중요성을 이해하고, 새로운 보안 패러다임을 시범 적용해봄으로써 민간에게 방향성을 제시할 필요가 있다. 사이버 보안 신기술 연구개발, 사이버 보안 인증 제도, 보안 위협 대응 전략 등의 정책 개발 및 추진

과정에서 중복 투자 방지와 일관된 제도 수립 등을 위해 부처별 역할을 정의하고 소관 업무를 조정할 수 있는, 국내 사이버 보안 산업의 진흥과 보호를 책임질 수 있는 컨트롤 타워에 대한 논의도 필요할 것이다.

사이버 보안 인력 양성과 관련하여 새 정부에서 10만 인재 양성 등 강력한 의지를 보이고 있다. 양적인 부분에 대해서는 긍정적이며 다만 이에 대해 새로운 인력 양성 방향과 구체화 노력이 필요할 것으로 보인다. 이를 위해 산업계의 수요를 반영한 인재 양성 정책을 수립해야 한다. 산업계의 수요라 함은 필요한 인력의 유형뿐 아니라 재교육이 어려운 중소기업들을 고려한 정책이 필요하다. 사이버 보안은 특히 개개인의 능력에 따라 결과가 매우 차이가 큰 분야이다. 기업의 보안을 지키면서 고급 인력을 공유하거나 기존 인력의 재교육을 통한 고급 인력 양성 등의 정책 논의가 필요할 것이다.

마지막으로, 사이버 보안 기술은 디지털 대전환에 따라 증폭되는 사이버 보안 피해를 예방하여 디지털 공동 번영을 위한 안전한 디지털 환경 구축의 초석이 될 것이다. 이를 위해 적절한 정부의 지원과 정책은 계속 강조해도 지나치지 않을 것이다.

참 고 문 헌

국내 문헌

이석준 (2022),『양자 암호, 그리고 양자 시대의 안전성』, 2022 Netsec-KR.

이석준 (2020),『암호 양자보안 검증 플랫폼 <Q¦Crypton>』, 2020 Netsec-KR.

조상래, 조영섭, 김수형 (2016),『FIDO 2.0 범용인증기술 소개』, 정보과학학회지.

진승헌, 김수형 (2020),『주간기술동향 1975호 - 디지털 ID 관리 기술 현황』, 정보통신기획평가원.

윤성욱 (2020),『인공지능의 발전에서 동형암호가 갖는 의미』, AI TREND WATCH.

Microsoft (2022),『Windows에서 신뢰할 수 있는 플랫폼 모듈을 사용하는 방법』, https://learn.microsoft.com/ko-kr/windows/security/information-protection/tpm/how-windows-uses-the-tpm (Last accessed: 2022년 9월 26일).

이경택 (2021),『반도체에 지문 새기는 PUF, IoT 신뢰 근간 될까?』, https://www.technologyreview.kr/puf-iot-security/ (Last accessed: 2022년 9월 26일).

김주한, 이상재, 오미경, 강유성 (2020),『센서 기반의 디바이스 DNA 기술 동향』, 전자통신동향분석.

양준호, 김찬진, 김미연, 김지혜, 김종현, 염흥열 (2018),『사이버 위협 인텔리전스 공유 체계 연구』, 한국정보통신학회, 종합학술대회논문집 Vol. 22. No. 2.

금융보안원,『美 사이버 위협 정보공유 체계』.

박명서 (2022),『랜섬웨어의 파일 암호화 키 관리 방법 분류와 그에 따른 분석 대상 식별』, The Korea Institute of Information Security and Cryptology, vol. 32, no. 3, pp. 5-10.

조영민,『IoT 펌웨어 취약점 분석 효율성 제고를 위한 시스템 개발에 관한 연구』, 한국산업보안연구, Vol. 12, No. 1, pp. 31-50.

이형우 (2021),『IoT 봇넷 악성코드 기반 침해사고 흔적 수집 방법』, 사물인터넷융복합논문지, vol. 7, no. 3, pp. 1-8.

김대원, 강동욱, 최용제, 이상수, 최병철 (2020),『공급망 보안기술 동향』, Electronics and Telecommunications Trends, vol. 35, no. 4, pp. 149-157.

윤오준, 조창섭, 박정근, 배선하, 신용태 (2016),『주요국의 사이버위협정보 공유체계 분석을 통한 국내 적용모델 연구』, 융합보안 논문지, vol. 16, no. 7, pp. 101-111.

KRCERT,『사이버 위협정보 분석공유(C-TAS) 시스템』, https://www.krcert.or.kr/webprotect/ctas.do.

임원식, 윤명근, 조학수 (2018),『KOSIGN:정보보호제품 관점의 사이버위협정보 공유 체계』, The Korea Institute of Information Security and Cryptology, vol. 28, no. 2, pp. 20-26.

문기운, 이종혁 (2022),『최신 랜섬웨어 동향 및 발전 방향』, Electronics and Telecommunications Trends, vol. 32, no. 3, pp. 33-39.

김환국, 최보민, 고은혜, 박성민 (2019),『5G 네트워크 기술 진화에 따른 새로운 5G 보안 도전과제와 해외 보안 아키텍처 연구 동향』, The Korea Institute of Information Security and Cryptology, vol. 29, no. 5, pp. 7-20.

박인상, 이호형, 조수연 (2020),『주간기술동향 1977호 - 클라우드 보안 기술 및 표준 동향』, 정보통신기획평가원.

박재현, 김승주 (2019),『정형 기법을 이용한 하드웨어 AES 모듈 백도어 탐색 연구』, The Korea Institute of Information Security and Cryptology, vol. 29, no. 4, pp. 739-751.

김동원, 한근희, 전인석, 최진영 (2015),『자동차 공급망 위험관리(A-SCRM) 방안 연구』, The Korea Institute of Information Security and Cryptology, vol. 25, no. 4, pp. 793-805.

이슬기, 김동욱, 이태우 (2022),『랜섬웨어 피해 저감을 위한 공격 타임라인별 대응전략 및 기술』, The Korea Institute of Information Security and Cryptology, vol. 32, no. 3, pp. 27-31.

국토교통부 (2020),『스마트시티 통합플랫폼 기반구축』.

산업통상자원부 (2021),『산업통상자원뉴스』.

한국인터넷진흥원 (2021),『디지털 헬스케어 보안모델』.

스마트제조혁신추진단 (2022), 『스마트공장 소개』, https://www.smart-factory.kr/smartFactoryIntro.

LG CNS (2018), 『보안 위협으로부터 '스마트시티'를 지킬 방법은?』, https://www.lgcns.com/blog/cns-tech/smartcity/2805/.

권혁찬, 김정녀 (2019), 『주간기술동향 1911호 - 커넥티드 의료기기 보안 동향 및 이슈』, 정보통신기획평가원.

이글루시큐리티 (2020), 『OT 보안을 위한 넓고 얕은 지식』, https://www.igloo.co.kr/security-information/ot-%EB%B3%B4%EC%95%88%EC%9D%84-%EC%9C%84%ED%95%9C-%EB%84%93%EA%B3%A0-%EC%96%95%EC%9D%80-%EC%A7%80%EC%8B%9D/.

LG CNS 블로그 (2021), 『[OT보안] DX 시대, 이젠 OT/ICS 보안도 달라져야 할 때! 1편』, https://blog.lgcns.com/2704.

김경호 (2021), 『주간기술동향 1981호 - 산업제어시스템 보안』, 정보통신기획평가원.

이강준 (2020), 『보안 관제의 디지털 탈바꿈, SOAR의 개념과 주요 기능』, https://www.2e.co.kr/news/articleView.html?idxno=300903.

김현구 (2022), 『Apache Log4j 취약점 (CVE-2021-44228, CVE-2021-45046, CVE-2022-23302, CVE-2022-23305, CVE-2022-23307)』, https://blo9.xyz/2021/12/11/Security/Anlaysis/cve/CVE-2021-44228/.

차현아 (2022), 『집안 사생활 다 보고 있었다…'아파트 월패드' 해킹 이젠 문제없나』, https://news.mt.co.kr/mtview.php?no=2022060807403293755.

김윤희 (2021), 『원자력연구원 해킹…북한 해커 소행인 듯』, https://zdnet.co.kr/view/?no=20210618153600.

금융보안원 (2021), 『신용카드 정보를 노리는 사이버 공격 위협 분석 (2021 사이버 위협 인텔리전스 보고서)』.

박영철 외 (2015), 『사이버보안체계 강화를 위한 정보보호법제 비교법연구』, 한국인터넷진흥원.

김상배 (2018), 『트럼프 행정부의 사이버 안보 전략: 국가지원 해킹에 대한 복합지정학적 대응』, Journal of International Area Studies, vol. 27, no. 4, pp. 1-35.

김경곤 (2017),『IT CookBook, 인터넷 해킹과 보안 개정3판: 정보 보안 개론과 실습』, 한빛아카데미.

배병환, 강원영, 김정희 (2014),『영국의 사이버보안 추진체계 및 전략 분석』, Internet & Security Focus.

홍준호 (2019),『사이버보안 컨트롤타워 필요성에 관한 연구』, 법학연구, vol. 19, no. 1, pp. 235-254.

과학기술부 외 (2021),『2021 정보보호산업 실태조사』.

한국인터넷진흥원,『ISMS-P 인증대상』, https://isms.kisa.or.kr/main/ispims/target/.

한국인터넷진흥원,『ISMS-P 제도소개』, https://isms.kisa.or.kr/main/ispims/intro/.

한국인터넷진흥원 (2020),『클라우드 서비스 보안인증제 안내서』.

한국인터넷진흥원 (2022),『정보통신망연결기기 등 정보보호인증기준 상세 해설서』.

한국인터넷진흥원 (2021),『2030 미래사회 변화 및 사이버위협 전망 연구』.

한국인터넷진흥원 (2021),『AI보안 법・제도・정책 현황 및 전망』.

한국인터넷진흥원 (2021),『디지털 안심국가 실현을 위한 중장기 로드맵』.

한국인터넷진흥원 (2021),『언택트시대 디지털 대전환을 위한 정책제언 연구』.

한국인터넷진흥원 (2021),『가상융합경제의 확산과 보안이슈 분석』, KISA Insight 2021, Vol.04.

한국인터넷진흥원 (2022),『2030 미래사회 변화 및 ICT 8대 유망기술의 사이버 위협 전망』, KISA Insight 2022, Vol.01.

한국인터넷진흥원 (2022),『빅데이터로 본 정보보호・디지털 이슈 분석』, KISA Insight 2022, Vol.02.

한국인터넷진흥원 (2022),『AI 중심사회의 도래와 보안 이슈 분석』, KISA Insight 2022, Vol.03.

한국인터넷진흥원 (2022),『메타버스와 NFT, 사이버보안 위협 전망 및 분석』, KISA Insight 2022, Vol.04.

연구개발특구진흥재단 (2021),『기술사업화 이슈&마켓 - 경쟁 우위를 점하기 위해 서비스형 소프트웨어로 눈을 돌리고 있는 사이버위협 안텔리전스(CTI) 서비스 제공사』, 디지털뉴딜 제 115호.

정보통신기획평가원 (2020),『국가차원의 침해사고 대응을 위한 사이버 위협 인텔리전스 분석(CTI) 및 정보 공유 기술 개발』.

국가정보원 외 (2021),『국가정보보호백서』.

김방룡, 홍재표, 고준수 (2015),『정보보호산업의 글로벌 동향 - 시장, 정책, 법 규제를 중심으로』, 전자통신동향분석, 제 30권, 제 2호.

양정윤, 박상돈, 김소정 (2015),『미국의 법제도 정비와 사이버안보 강화: 국가사이버안보보호법 등 제・개정된 5개 법률을 중심으로』, 입법과 정책, 제 7권, 제 2호.

관계부처 합동 (2016),『정보보호산업 육성 및 전문 일자리 창출을 위한 제 1차 정보보호산업 진흥계획 [2016 ~ 2020]』.

양천수, 지유미 (2018),『미국 사이버보안법의 최근 동향 - 사이버보안 정보공유법을 중심으로 하여』, 법제연구, 제 54호.

해외 문헌

S. Wiesner. (1983). “Conjugate Coding.“ ACM SIGACT News.

T. Jawaid. (2020). “Quantum Computing and the Future Internet.“ ISSA Journal.

Z. Tang. (2016). “Measurement-Device-Independent Quantum Cryptography.“ Ph. D. Thesis.

Martin Roetteler, Michael Naehrig, Krysta M. Svore, Kristin Lauter. (2017). “Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms.“ Asiacrypt 2017.

IBM. (2022). “Our new 2022 Development Roadmap.“ https://www.ibm.com/quantum/roadmap (Last accessed: 2022년 9월 26일).

Michele Mosca, Marco Piani. (2022). “2021 Quantum Threat Timeline Report.“ Global Risk Institute.

G. Banegas. (2019). “Post-Quantum Cryptography: From construction to destruction.“

Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer. (2021). “Ascon v1.2: Lightweight Authenticated Encryption and Hashing.“ Journal of Cryptology.

Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer. (2015). “Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation.“ CHES 2015.

Houda Ferradi, Rémi Géraud, David Naccache, Assia Tria. (2016). “When Organized Crime Applies Academic Results: A Forensic Analysis of an In-Card Listening Device.“ Journal of Cryptographic Engineering.

borer. (2022). “IDENTITY AUTHENTICATION.“ https://www.borer.co.uk/borer-technology/multi-factor-identity-authentication/ (Last accessed: 2022년 9월 26일).

Deniz Ekiz, Yekta Said Can, Yagmur Ceren Dardagan, Cem Ersoy. (2019). “Is Your Smartband Smart Enough to Know Who You Are: Continuous Physiological Authentication in The Wild.“ https://arxiv.org/pdf/1912.04760.pdf (Last accessed: 2022년 9월 26일).

Manu Sporny, Dave Longley, Markus Sabadello, Drummond Reed, Orie Steele, Christopher Allen. (2022). “Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations.“ W3C Recommendation.

Kundan Munjal, Rekha Bhatia. (2022). “A systematic review of homomorphic encryption and its contributions in healthcare industry.“ Complex & Intelligent Systems.

Office of the Director of National Intelligence. (2018). “How would you explain homomorphic encryption?“ https://www.youtube.com/watch?v=pXb39wj5ShI (Last accessed: 2022년 9월 26일).

H. Nakagawa. (2016). “Introduction of Privacy Protection Mathematical Models.“

Apple. (2017). “Learning with Privacy at Scale.“ https://machinelearning.apple.com/research/learning-with-privacy-at-scale (Last accessed: 2022년 9월 26일).

OpenMined. (2021). “LOCAL VS GLOBAL DIFFERENTIAL PRIVACY.“ https://blog.openmined.org/basics-local-differential-privacy-vs-global-differential-privacy/ (Last accessed: 2022년 9월 26일).

embeddedbits. (2021). “Introduction to Trusted Execution Environment and ARM’s TrustZone.“ https://embeddedbits.org/introduction-to-trusted-execution-environment-tee-arm-trustzone/ (Last accessed: 2022년 9월 26일).

Ian J. Goodfellow, Jonathon Shlens, Christian Szegedy. (2014). “Explaining and Harnessing Adversarial Examples.“

Chengcheng Zhou, Qian Liu, Ruolei Zeng. (2020). “Novel Defense Schemes for Artificial Intelligence Deployed in Edge Computing Environment.“ Wireless Communications and Mobile Computing.

Gihyuk Ko, Gyumin Lim. (2021). “Unsupervised Detection of Adversarial Examples with Model Explanations.“

KAUSHIK PATOWARY. (2020). “Clever Hans: The Horse Who Could Do Math.“ https://www.amusingplanet.com/2020/05/clever-hans-horse-who-could-do-math.html (Last accessed: 2022년 9월 26일).

eyerys. (2019). “Using ‘Guaranteeing AI Robustness Against Deception’, DARPA Enhances Cybersecurity With AI.“ https://www.eyerys.com/articles/news/using-guaranteeing-ai-robustness-against-deception-darpa-enhances-cybersecurity-ai (Last accessed: 2022년 9월 26일).

Pentasecurity. (2021). “Fraud Detection System (FDS) with AI Technology.“ https://www.pentasecurity.com/blog/fraud-detection-system-fds-with-ai-technology/ (Last accessed: 2022년 9월 26일).

Matt Turek. “Explainable Artificial Intelligence (XAI).“ https://www.darpa.mil/program/explainable-artificial-intelligence (Last accessed: 2022년 9월 26일).

Symantec. (2019). “Internet Security Threat Report (ISTR).“ Vol. 24.

IoT Analytics. (2022). “Enterprice IoT market 2019-2027.“ https://iot-analytics.com/iot-market-size/.

Vicki Livingston. (2019). “What’s the answer for 5G security?“ https://www.techtarget.com/searchsecurity/opinion/Whats-the-answer-for-5G-security.

RedHat (2020),『IaaS, PaaS 및 SaaS 비교』, https://www.redhat.com/ko/topics/cloud-computing/iaas-vs-paas-vs-saas

CSA. (2022). “Top Threats to Cloud Computing Pandemic Eleven.“

Prashast Srivastava, Hui Peng, Jiahao Li, Hamed Okhravi, Howard Shrobe, and Mathias Payer. (2019). “FirmFuzz: Automated IoT Firmware Introspection and Analysis.“ In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things (IoT S&P’19). ACM, New York, NY, USA, pp. 15-21.

Xuhang Ying, Sang Uk Sagong, Andrew Clark, Linda Bushnell, Radha Poovendran. (2019). “Shape of the Cloak: Formal Analysis of Clock Skew-Based Intrusion Detection System in Controller Area Networks.“ IEEE Transactions on Information Forensics and Security 14, pp2300-2314.

A. Masri (2016). “Active Authentication Using Behavioral Biometrics and Machine Learning.“ PhD Thesis, Goerge Mason University.

Danny Thakkar. “Gait Recognition Systems Can Identify You with Your Manner of Walking.“ https://www.bayometric.com/gait-recognition-identify-with-manner/.

M. Rossi. (2021). “PQC Transition ANSSI View.“

NIST. (2021). “Preparing for Post-Quantum Cryptography.“

Unit 42. (2021). “Threat Assessment: Active Exploitation of Four Zero-Day Vulnerabilities in Microsoft Exchange Server.“ https://unit42.paloaltonetworks.com/microsoft-exchange-server-vulnerabilities/.

Trend Micro. (2021). “Available solutions for Darkside Ransomware.“ https://success.trendmicro.com/dcx/s/solution/000286466?language=en_US&sfdcIFrameOrigin=null.

디지털 대전환 메가트렌드 연구 시리즈

22-24-01 디지털 대전환 메가트렌드 연구 총괄보고서 II (이호영 외, 정보통신정책연구원)

22-24-02 디지털 공동번영사회 미래전략 (이호영 외, 정보통신정책연구원)

22-24-03 디지털 대전환 시대 가상-현실세계 융합과 초연결기술 (홍인기 외, 한국통신학회)

22-24-04 사이버 위협 인텔리전스 기반 차세대 보안 (홍지만 외, 한국정보과학회)

22-24-05 디지털 대전환 시대 ICT·반도체 기술 및 인력 양성 전략 (김 훈 외, 대한전자공학회)

22-24-06 디지털 메가트렌드의 경제적 영향 분석과 대응전략 모색 (이희정 외, 정보통신정책학회)

22-24-07 지속가능한 생태계 디자인을 통한 우리나라 디지털 전환 산업 경쟁력 강화 (김연성 외, 한국경영학회)

22-24-08 디지털 대전환 시대 新디지털격차와 정부역할 (김서용 외, 한국행정학회)

22-24-09 디지털 대전환기 정치과정의 선순환 구축 (임성학 외, 한국정치학회)

22-24-10 인간-AI 협업기반 지능형 정부 구축 및 운영 방안 연구 (문명재 외, 한국정책학회)

22-24-11 디지털 전환에 따른 노동 변혁과 삶의 질 (서문기 외, 한국사회학회)

22-24-12 탄소중립 실현을 위한 디지털 전환과 그린 전환의 공존 전략 (최창용 외, 한국환경정책학회)

● 저 자 소 개 ●

홍 지 만

- 고려대 컴퓨터학과 졸업
- 서울대 컴퓨터공학과 석사
- 서울대 컴퓨터공학과 박사
- 현 숭실대학교 교수

김 봉 재

- 광운대 컴퓨터공학과 졸업
- 서울대 컴퓨터공학과 석사
- 서울대 컴퓨터공학과 박사
- 현 충북대학교 교수

이 중 희

- 서울대 컴퓨터공학과 졸업
- 서울대 컴퓨터공학과 석사
- Georgia Institute of Technology Electrical and Computer Engineering 박사
- 현 고려대학교 교수

이 원 준

- 서울대 컴퓨터공학과 졸업
- 서울대 컴퓨터공학부 석사
- University of Minnesota at Minneapolis, Department of Computer Science and Engineering 박사
- 현 고려대학교 교수

이 재 흥

- 서울대 컴퓨터공학부 졸업
- 서울대 컴퓨터공학부 석사
- 서울대 컴퓨터공학부 박사
- 현 대전대학교 교수

김 동 균

- 경북대 컴퓨터공학과 졸업
- 서울대 컴퓨터공학과 석사
- 서울대 전기컴퓨터공학부 박사
- 현 경북대학교 교수

이 문 규

- 서울대 컴퓨터공학부 졸업
- 서울대 컴퓨터공학부 석사
- 서울대 전기컴퓨터공학부 박사
- 현 인하대학교 교수

허 준 영

- 서울대 컴퓨터공학과 졸업
- 서울대 컴퓨터공학부 석사
- 서울대 컴퓨터공학부 박사
- 현 한성대학교 교수

이 석 준

- 서울대 컴퓨터공학과 졸업
- 서울대 컴퓨터공학과 석사
- 한국과학기술원 전산학부 박사
- 현 가천대학교 교수

방송통신정책연구 2022-0-00016
정책연구 22-24-04

사이버 위협 인텔리전스 기반 차세대 보안
(Next-Generation Cybersecurity Based on Cyber Threat Intelligence)

2022년 12월 일 인쇄
2022년 12월 일 발행

발행인 과학기술정보통신부 장관
발행처 과학기술정보통신부
세종 가름로 194 세종파이낸스센터
Homepage: www.msit.go.kr
인 쇄 경 성 문 화 사

과학기술정보통신부
Ministry of Science and ICT

정보통신기획평가원
Institute of Information & Communications Technology Planning & Evaluation