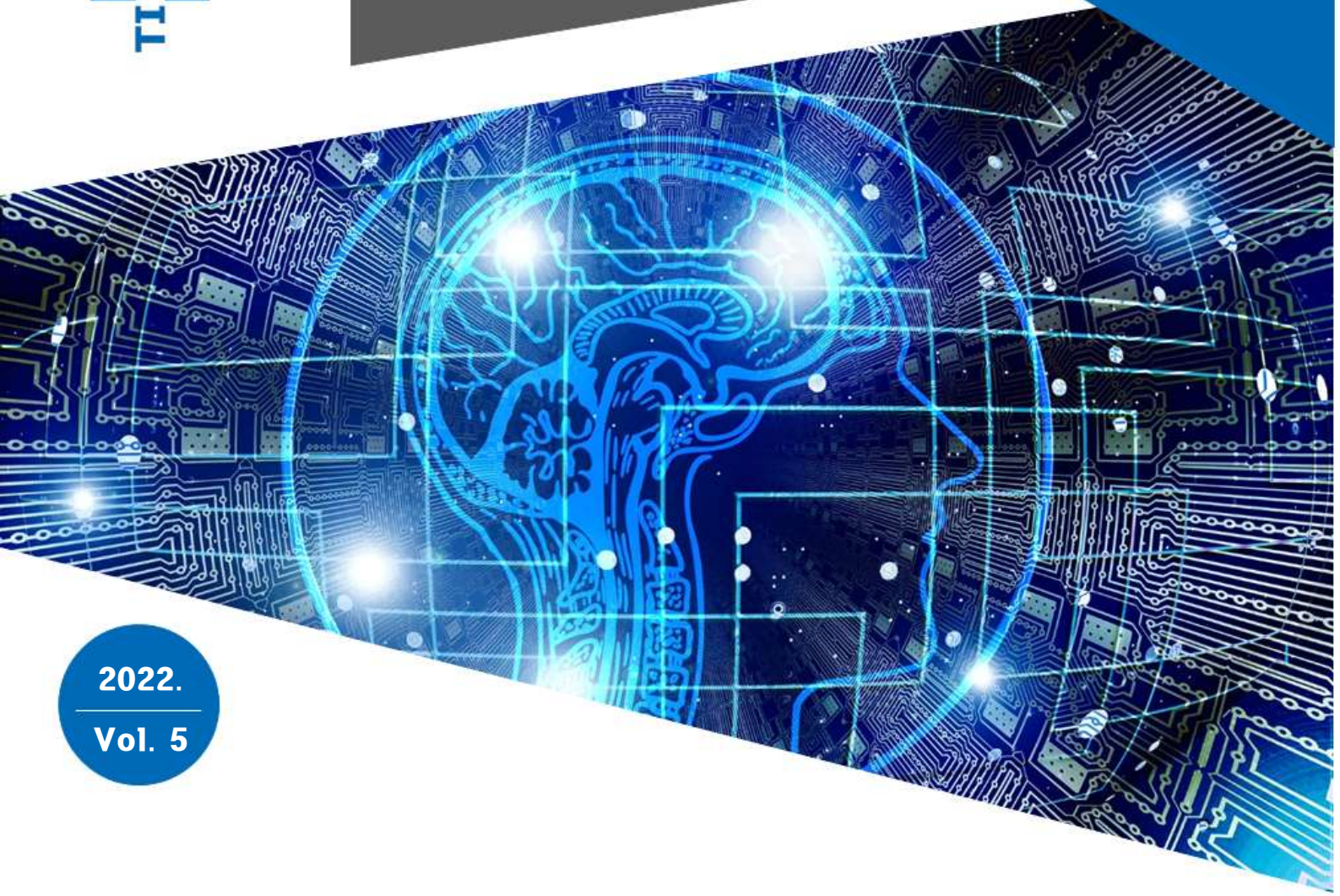
중소기업기술정보진흥원

TIPA

2022년 중소기업 전략기술로드맵

ISSUE REPORT



2022.
Vol. 5

차세대 데이터 보호기술과 중소기업

TIPA | 이슈 리포트

차세대 데이터 보호기술과 중소기업

Ⅰ. 데이터 보호기술 개요

1 데이터 보호기술 정의

☐ 데이터 보호기술은 데이터 라이프 사이클(생성→저장→갱신→활용→폐기) 전주기에 걸쳐 개인정보, 기업비밀 등 민감정보의 유출을 방지하기 위한 정보보호기술을 의미[1)]

- 데이터 보호와 활용 강화를 위한 기반기술과 데이터 가공·활용 과정의 보호를 위한 응용기술로 구분

☐ 정보보호는 암호, 인증, 인식, 분석/감시 등의 보안 기술이 적용된 제품을 생산하거나, 관련 보안 기술을 활용하여 개인·기업·국가의 안전과 신뢰를 보장하는 서비스를 제공하는 기술[2)]

- 컴퓨터·네트워크 기반의 정보보안, 안전·안심 생활을 위한 물리보안, 정보통신 기술과 타 산업 기술이 융합된 환경의 융·복합 보안 기술을 포함
- 컴퓨터·네트워크 수준의 보안을 넘어 치안감시, 의료, 에너지, 제조, 공급망 등 사회 全영역 보안으로 확장되면서, ICT 기반 미래 지식정보사회에서 개인·기업·국가 안보의 핵심역할을 수행
- 차세대보안은 디지털 전환, 디지털 트윈, 메타버스 등 4차 산업혁명 시대 진입과 全산업의 초연결화·디지털화·지능화로 인해 야기되는 고도의 사이버위협과 같은 부작용을 해소하여 실생활에서 국민의 안전과 자산을 보호하는 신규기술을 포함

[정보보호의 범위와 분류]

* 출처: ICT R&D 기술로드맵 2025-차세대보안-블록체인(정보통신기획평가원, 2020.12)

1) 데이터보호 핵심기술 개발 전략(과학기술정보통신부, 2021.11)
2) ICT R&D 기술로드맵 2025-차세대보안-블록체인(정보통신기획평가원, 2020.12)

2 데이터 보호기술의 분류[3]

□ '데이터보호 핵심기술 개발 전략'에서 정의하고 분류한 데이터 보호기술은 정보보안과 유사한 개념이지만 조금 더 범위를 넓힌 것으로 판단되며, 국가전략의 방향성과 일치와 혼선의 방지를 위해 데이터 보호기술의 분류와 정의를 해당 전략의 내용을 중심으로 기술하고자 함

□ (기반기술) 데이터 속의 중요한 정보를 보호하여 안전한 데이터 활용 기반을 마련하기 위한 개인정보보호 강화기술, 차세대암호 원천기술

- (개인정보보호 강화기술) 민감정보가 포함된 데이터의 활용성을 넓히기 위한 기술로 정형·비정형 데이터 비식별 처리 등을 포함
  - (정형 데이터 비식별) 일정한 규칙에 따라 정보가 배열된 통계, 신상, 회계 등 대용량의 정형 데이터에 대한 가명·익명처리 자동화
  - (비정형 데이터 비식별) 영상, 대화기록 등 규칙이 없이 정보가 배열된 비정형 데이터를 안전하게 활용하기 위한 개인식별정보 익명 처리 기술
  - (차등정보보호) 데이터에 적절한 노이즈를 추가하여 추론에 의한 민감정보 노출방지
- (암호원천기술) 중요 정보를 암호화하여 제3자에게 노출을 방지하는 기술로 최근 데이터 활용성 강화를 위한 동형 암호 등 부각
  - (동형 암호) 데이터를 암호화한 상태에서 연산을 수행할 수 있는 암호기술
  - (양자 내성 암호) 양자컴퓨터를 이용한 공격에도 해킹이 불가능한 암호기술

□ (응용기술) 데이터가 주로 사용되는 인공지능, 데이터유통, 융합서비스 환경에서의 민감정보 유출 방지

- (AI 데이터 보호) AI 학습 과정에서 데이터를 보호하기 위한 기술(연합학습 등)과 AI를 활용한 데이터 보호 기술(재현 데이터 등)
  - (AI 연합학습) 스마트폰 등 개별단말기에서 AI 학습을 수행하고 각 기기에서 학습된 결과만을 서버에서 취합하여 더 강화된 AI 모델을 만들어 내는 인공지능 학습 방식
  - (재현 데이터) AI를 기반으로 원본 데이터의 통계적 특성을 따르는 가상데이터를 생성하여 활용함으로써 민감정보를 외부에 노출하지 않고 데이터 사용 가능
- (데이터 권리 보호) 기업비밀 등 중요 정보의 유출을 방지하고, 데이터 유통 등 과정에서 정보 주체의 권리를 보장하기 위한 기술
  - (정보유출 방지) 기업비밀 등 중요 정보의 유출을 방지하기 위한 DRM(Digital Right Management), 사용자 ID 은닉(워터마크) 등 데이터 유출 방지 및 추적 기술
  - (영지식 증명) 상대방에게 어떤 정보도 드러내지 않고 신원, 정보 소유 등을 증명
  - (정보주체 권리보장) 개인의 데이터가 활용될 때마다 본인의 동의를 받도록 하는 동적동의 기술 등
- (융합 산업·서비스 보호) 산업제어시스템(ICS, Industrial Control System), 스마트시티, 의료정보, 자율주행차 등 융합산업 데이터의 안전한 관리와 활용을 지원하기 위한 보안기술

3) 데이터보호 핵심기술 개발 전략(과학기술정보통신부, 2021.11)을 근거로 하였으며, 데이터 보호 기술은 기존의 여러 보안기술을 종합하여 정부가 새롭게 정의하였기 때문에 정부의 정의를 인용하였음

[데이터 보호 방향과 기술분류 연계]

* 출처: 데이터보호 핵심기술 개발 전략(과학기술정보통신부, 2021.11)

[데이터 보호 기술분류]

구분	소분류	요소기술
공통기반 보안	암호기술	암호 설계, 암호 부채널 분석, 암호 분석
	인증/인가 기술	범용 인증, ID 관리 및 접근제어, 바이오 인증
	데이터 보안	프라이버시 보호, 데이터 유출 방지, 디지털저작물 침해/권리 보호,1 빅데이터 보안관리 및 DB 보안
	인공지능 보안	인공지능 보안위협 분석 기술, 로봇 보안 및 제어
시스템·디바이스 보안	보안취약성	SW취약점분석, HW취약점분석
	악성코드	악성코드 대응, 랜섬웨어 대응
	시스템 보안	운영체제 보안, 가상화 보안, 시스템 접근통제
	디지털 포렌식	디지털 증거 수집 및 분석, 안티 포렌식 대응
	디바이스 보안	IoT 디바이스 보안, 스마트 디바이스 보안, 웨어러블 디바이스 보안, 기타 디바이스 보안
네트워크·응용서비스 보안	유선 네트워크 보안	경계보안, 보안 연결, DDoS대응
	무선 네트워크 보안	이동 통신망 보안, 무선근거리통신망보안
	클라우드·엣지 보안	가상화 플랫폼 보안, 클라우드 보안 서비스, 소프트웨어 정의 보안, 엣지 컴퓨팅 및 네트워크 보안
	위협분석 및 관제	지능형 사이버위협 분석, 보안정보 분석 및 로그 관리, 보안 관제
	응용서비스 보안	웹 보안, 이메일 보안, 전자화폐 보안, 블록체인 보안, 전자거래 이상행위 탐지, 거래·사기 방지
물리보안	휴먼/바이오인식	바이오인식 센서, 바이오인식 엔진, 휴먼인식 및 검색, 휴먼/바이오인식 응용
	CCTV 감시/관제	카메라 및 저장장치, VMS/통합관제, 지능형 영상감시, CCTV 인프라 보호
	보안검색 및 무인전자경비	대인 검색기, 수화물/화물 검색기, 알람 모니터링, 무인전자경비 서비스
융합보안	스마트시티 보안	홈·시티 디바이스 보안 및 제어, 홈·시티 데이터 프라이버시
	산업제어시스템 보안	스마트공장 보안, 기반시설 보안, 스마트 에너지 보안
	자동차 및 이동체 보안	자동차 및 이동체 내·외부 통신 보안, 내·외부 접근제어, 침입탐지, 보안취약점 진단
	헬스케어·의료 보안	헬스케어 디바이스·센서 보안, 의료 데이터 보안 및 공유
	선박·해양·항공 보안	자율운항 선박 해킹방지, 해운항만 통신 보안, 해양 인프라 보안 관제, 무인비행체 보안, 항공 인프라 보안 관제

* 출처: ICT R&D 기술로드맵 2025-차세대보안-블록체인(정보통신기획평가원, 2020.12)

Ⅱ. 최근(미래)의 다양한 보안 위협

1 사이버 공격

☐ 2022년 2월에 발발한 러시아의 우크라이나 침공 이전인 2월 15일에 우크라이나 국방부, 외무부, 문화부 등 정부 부처 사이트들과 2개의 대형 은행 등 적어도 10개 사이트가 사이버 공격으로 접속이 어려웠으며 관련 기관들은 러시아의 사이버 공격을 의심

- 클라우드, 분산 컴퓨팅, 사물 인터넷(IoT, Internet of Thins), 모바일 디바이스 등의 인프라 유연성 확대에 따라 공격표면이 증가하고 솔라윈즈(SolarWinds)사고, 콜로니얼 파이프라인(Colonial Pipeline) 랜섬웨어 감염 사고, MS Exchange Server 해킹 사건과 같이 국가 주도 APT 해킹그룹에 의한 공급망 공격(Supply Chain Attack)이 증가하면서 사이버 공격으로 인한 국가적, 사회적, 개인적 피해가 폭발적으로 증가

☐ 코로나19 이슈나 정치적 이슈를 활용한 사회공학기법의 사이버공격은 계속 진행 중

- 사이버 공격 성공 여부는 공격기법에 의해 크게 좌우되며 인공지능 등의 신기술을 결합하여 고도화되고 지능화된 공격기법이 꾸준히 증가

- 재택근무나 원격근무 등의 확산으로 인해 OSINT정보, 무차별 대입공격(Brute Force Attack)등에 사회공학 기법을 결합한 공격 성공률 역시 지속적으로 증가

[사이버 공격의 최근 동향]

소분류	요소기술
공격대상 (Attack Target)	• 산업 유형별 구분 : 제조, 유통, 통신, 교육, 공공, 금융, 국방 등 • ICT/OT 관점 : ICT 인프라, ICS/OT 인프라 • 인프라 구성요소 관점 : On-Premise, Cloud, Hybrid • Architecture 관점 : HW, SW, NW, Data, Application
공격주체 (Attack Subject)	• 개인주도공격 : 자기 과시 , 금전적 이익 추구 • 국가주도 공격 : Cyberwarfare, APT 공격 주도 - 미국 , 영국 , 캐나다 , 한국 순 해킹표적을 대상으로 정보수집 - 공공기관을 넘어 민간영역의 공격 증가 - 사이버 공간의 공격으로 인해 물리 공간에 영향도가 확산되면서 사이버 공격을 통합방위범주에 포함하려는 논의 활발
공격기법 (Attack Techniques)	• 공격도구 및 공격수단 - SW 방식 : Hacking, 바이러스 , 웜 , 스팸메일 , 피싱 , 스피어피싱 - HW 방식 : Chipping, EMP, 나노머신 , HERF RUN • 사이버 보안 모델 프레임워크 : Cyber Kill-Chain, MITRE ATT&CK, Gartner Cyber Attack Chain Model, ISO/IEC 27001/ISO 27002, NIST Cybersecurity Framework, NIST 800-53 Cybersecurity Framework

* 출처: 2021년 보안위협 분석을 통한 2022년 보안위협 및 보안기술 전망(이글루시큐리티 홈페이지)

2 비대면 시대에 따른 보안 위협

□ 코로나19 팬데믹은 산업, 문화, 교통, 통신 등의 다양한 분야에 사회적인 파급효과를 일으키는 현상을 의미하는 '이머징 이슈(Emerging Issue)'를 유발

- 특히 디지털 전환을 통한 비대면 환경을 촉진하면서 생활뿐만 아니라 근무환경에도 큰 변화
- 원격접속 프로그램이나 VPN(Virtual Private Network), SDP(Software Defined Perimeter)를 기반한 원격근무 환경(재택근무, 분산 오피스)에서 XR, 홀로그램, 메타버스 등 다양한 ICT 융합기술을 활용해 시간과 공간의 제약없이 업무를 수행할 수 있는 디지털 업무공간(Digital Workspace)으로 발전
- 클라우드 서비스를 통한 지리적·기술적 제약 해소 및 망분리 규제 완화에 따른 제도적 지원을 통해 근무체계 유연화 가속화

□ 직장이 아닌 외부의 다른 어떤 공간에서 업무를 하는 원격근무 환경은 내부망으로 업무를 보는 것에 비해 보안이 취약하여 이를 이용한 공격자들의 표적이 되기 용이

- 공격자들은 이를 악용하여 원격근무자의 네트워크 및 시스템에 불법적으로 침입할 수 있으며, 특히 민감한 개인정보를 많이 다루면서도 보안관련 예산 및 조직이 미비한 기관 · 기업들은 이러한 불법적 공격자의 주요 표적

□ 원격근무 환경의 보안위협을 융합보안(관리 · 물리 · 기술적) 관점에서 살펴보면,

- (관리적 보안 측면) 참석자에 대한 신원인증 문제와 원격 · 화상회의가 비대면 방식으로 진행되므로 업무 도중 다양한 보안공격에 노출될 수 있으며, 원격근무 시 잠시 자리를 비운 경우 제3자에 의해 자료가 위 · 변조, 탈취될 수 있는 위협이 존재
- (물리적 보안 측면) 장비 자체가 조직 내부가 아닌 외부에 위치하므로 도난 및 분실 문제가 발생할 수 있고, 개인의 PC를 사용해서 직장 내부망에 접속하는 것은 직장의 기밀자료를 집에서도 열람이 가능해지는 것이고 이러한 자료들이 로컬 등에 보관될 경우 기밀유출사고가 발생할 위험이 존재
- (기술적 보안 측면) 사용자 단말기의 보안 취약으로 악성코드에 감염될 경우 단일실패지점(single point of failure)이 되는 점과, 원격근무에 사용되는 네트워크 환경이 안전하지 않을 경우 내부 데이터가 유출되는 것이 가능

□ 화상회의를 진행하면서 안전성을 보장받기 위해서는 기관-기업에서 승인된 안전한 플랫폼과 단말기, 그리고 보안접속 프로그램(VPN, SDP 등)이 필요(플랫폼 전용 장비는 기관-기업에서 직접 구축하는 방식과 클라우드 SaaS 서비스를 이용하는 방식)

- 영상회의에 허가받지 않은 사용자가 회의실에 무단으로 접속할 수 있는 위협이 상존
- 사무실의 위치 · 개인정보 등이 카메라로 보여지면서 사용자의 민감정보가 노출
- 영상회의 통신이 암호화가 되어 있지 않은 경우 회의 데이터가 유출될 가능성이 존재
- 화상회의에서도 영상과 음성이 합성된 딥페이크는 여전히 주요 위협 중 하나

3 공급망 공격

□ 생산자 중심에서 소비자 중심으로 공급망 가치 사슬이 재편됨에 따라, 공급망 구조가 사용자의 다양한 요구사항을 반영할 수 있도록 진화

- 기존에는 요구사항 분석을 토대로 하드웨어나 소프트웨어를 설계해 제조업체나 개발업체가 구현한 산출물을 소비자에게 배포하는 것이 일반적인 공급망 관리 프로세스였으나, 최근 그 프로세스에 ICT 기술이 접목되면서 공급망의 자동화, 공정간 조율, 제어, 관리를 통해 비즈니스 유연성을 확보하고 생산성을 향상시키는 방향으로 발전

- 그러나 문제는 이와 같은 긍정적인 효과에도 불구하고 인공지능, 빅데이터, 클라우드, IoT 등 융합 기술의 확대가 공격 대상 지점의 증가로 이어지게 되면서 새로운 위협 요소로도 작용

□ 공급망 공격(Supply chain attack)은 자사의 시스템 및 데이터에 접속할 수 있는 외부 협력업체나 공급업체를 통해 누군가가 시스템에 침투할 때 발생

- 지난 몇 년 동안 더 많은 공급업체와 서비스 제공업체가 민감한 데이터를 접촉하면서 일반 기업의 공격 표면(Attack Surface)이 극적으로 변화

- 하드웨어나 소프트웨어 기반의 1차 공급망(Primary Production)에서 최종 소비자(Program Office)에 이르기까지 공급망을 구성하는 하드웨어, 소프트웨어, 펌웨어, 데이터는 악의적인 공격(Malicious Insertion)의 대상이 되며, 정상 파일이나 프로세스의 교체 및 유입으로 인해 기밀성과 무결성이 훼손되고, 최종적으론 제품이나 서비스의 가용성에도 영향

□ 공급업체에 의해 야기된 주요 사이버 피해는 매우 다양하고 피해 규모가 상대적으로 큼

- 2013년 미국 소매점 타겟(Target)의 데이터 유출 사건은 공기조화기술(HVAC; heating, ventilation & air conditioning) 공급업체의 허술한 보안으로 인해 발생되었고 이로 인해 Target은 개인정보 유출 사건 피해자들에게 총 1,000만 달러를 배상

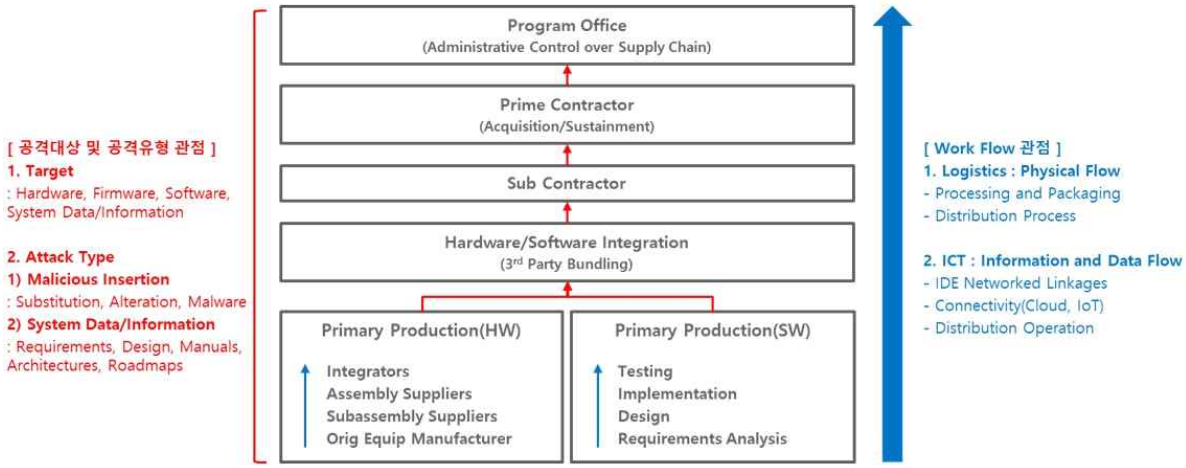
- 미국인 1억 4,400만 명의 이름, 주소, 생년월일, 사회보장번호, 운전면허번호 등이 노출된 것으로, 미국 인구의 40% 이상이 영향을 받은 것으로 알려진 미국 개인 신용정보업체 에퀴팩스(Equifax)의 2017년 데이터 유출 사건은 사용 중인 외부 소프트웨어의 결함으로 밝혔다가 이후 다른 공급업체 웹사이트의 악성 다운로드 링크에서 비롯됐다고 책임을 돌림

□ 마이터(MITRE)에서 발표한 '공급망 공격 프레임워크 및 공격 패턴(Supply Chain Attack Framework and Attack Patterns)'에 따르면, 공급망 공격의 발생 지점은 크게 물리적 측면(Physical Flow)과 정보 및 데이터 측면(Information and Data Flow)으로 구분

- 물리적 측면에서는 제품 제조 공정이나 패키징 과정에서 의도하지 않은 부품이나 기능이 포함

- 정보 및 데이터 측면에서는 공급망을 구성하고 있는 지속적 통합, 지속적 제공/지속적 배포 (CI/CD : Continuous Integration, Continuous Delivery / Continuous Deployment) 인프라 취약점, 분산 운영환경, 접근제어 미흡 등으로 데이터 유출이나 주요 시스템 파괴 등의 공격이 발생 가능

[공급망 공격 프레임워크]



* 출처: 공급망 공격 사례 분석 통한 '위험관리 핵심전략'(IT Daily, 2021.10.21.)

☐ 소프트웨어 기반 공급망 공격 프로세스는 크게 4가지 단계 구성

- 첫 번째 단계인 '공격 대상 선정 및 경로 확보 단계'에서는 제3자 소프트웨어 개발자, 시스템 관리자들을 대상으로 스피어피싱, 워터링 홀과 같은 사회공학적 공격 기법을 통해 진입점을 확보하거나, 중앙관리형 소프트웨어 및 VPN, 방화벽 등의 관리자 페이지 노출, 접근 제어 미흡 등을 통해 내부망 또는 개발망의 직·간접적인 접근 경로를 확보

- 다음 단계에서는 수집된 정보를 토대로 업데이트 서버, 배포 서버, 형성관리 서버 등에 접근해 악성코드 설치 및 백도어 등의 방식으로 공격을 유지

- 이후 권한 상승, 자격증명탈취 등으로 권리자 권한을 확보하고, 탐지 솔루션 무력화 및 추가 공격 대상에 위·변조된 소스 코드, 실행 파일, 업데이트 파일, 모듈 등의 패치 파일을 배포해 시스템 파괴, 내부 시스템 악성 파일 감염 등을 유발

- 그리고 마지막 단계에서는 내부 시스템에 배포된 악성 파일들을 이용해 C&C(Command & Control)로 내부 데이터 유출, 시스템 무결성 및 가용성의 손상을 끝으로 공격을 종료

4 디지털 전환과 보안위협

□ 2021년 2월 경제협력개발기구(OECD)는 '보안 취약점 관리에 관한 보고서'를 공개하고 전 세계적으로 추진되고 있는 디지털 전환에 보안 취약점이 위협이 될 것이라고 지적

- OECD는 보안 취약점에 대한 사회적 인식을 바꿔야 하며 각 정부 정책 관계자들이 보안 취약점을 고려해야 한다고 강조
- OECD는 이례적으로 디지털 보안, 그중에서도 보안 취약점 문제를 거론하면서 "소프트웨어 코드는 취약점을 포함하기 마련이고, 모든 스마트 제품은 코드를 보유하기 때문에 어느 정도 취약할 수밖에 없다"며 "스마트 제품 취약점을 이용한 공격은 막대한 경제·사회적 비용을 초래할 수 있다"고 지적
- OECD는 그 예로 2017~2020년 사이 안드로이드, iOS 혹은 윈도우 등 널리 이용되는 운영체제(OS) 제품에서 매일 평균 40개의 새로운 취약점이 공개됐고, 더 많은 취약점이 발견됐으나 공개되지 않았을 확률이 높다고 설명

□ 디지털 뉴딜의 초연결 신사업 중 보안 이슈의 중심에 있는 메타버스는 가상현실(Virtual Reality)과 증강현실(Augmented Reality)을 데이터 통신기술과 결합하여 경제, 사회, 문화 활동을 영위하면서 현실세계와 상호작용이 가능한 공간을 의미

- 가상현실에 모델링을 하는 것을 넘어 현실 세계의 자아와 인터렉션을 수행하는 '멀티 페르소나'를 통해 재화나 상품유통까지 가능하기 때문에 개인정보보호 및 데이터 위·변조 등의 보안 이슈가 대두될 될 것으로 예상
- 메타버스 플랫폼 사용자는 마우스나 키보드와 같이 단순 입력장치를 통한 데이터 전송을 넘어 뇌파, 혈압, 호흡과 같은 생체신호와 행동 및 감정정보 데이터를 활용할 수 있기 때문에 접속시간이나 방문 위치, 소비성향, 재화 보유현황 등 디지털화된 개인정보로 인해 악용될 경우 심각한 개인 사생활 침해 및 자산가치 하락 등의 악영향이 예상됨에 따라 선제적인 규제와 대응방안 수립이 필요할 것으로 판단
- 특히 수집되는 사용자 데이터가 저장형태, 저장위치, 법규 준수성(Compliance) 등에 따라 규제범위와 처리방식이 상이해지기 때문에 개인정보보호를 위한 제도적 지원과 사이버보안 강화는 산업 활성화를 위한 필수 불가결적 요소

□ 디지털 전환의 핵심 기술 중 하나인 인공지능의 양면성으로 인한 기대감과 우려

- 실제 영상이나 이미지와의 차이점을 판단하기 어려운 딥 페이크(Deepfake)를 통해 가짜뉴스가 유포되거나, 인공지능 프로세스 과정에 개입해 중독 공격(Poisoning attack)이나 회피 공격(Evasion attack)을 유발하여 자율주행 자동차의 교통사고가 발생되는 등 인공지능 활용에 따른 부작용을 방지하기 위해 제도적, 기술적, 사회적 지원이 필요
- 편향된 데이터나 알고리즘, 인공지능으로 발생하는 악의적인 사이버 공격과 프라이버시 침해사고 등의 역기능을 방지하기 위해서는 기술적인 측면에서 암호화 기술 및 암호화된 상태에서 데이터를 처리할 수 있는 암호화 기술(동형 암호) 연구 및 AI백신 연구 등을 통해 악의적인 오용 가능성을 방지할 수 있으며, 인력적인 측면에서는 인공지능 보안인력 육성·양성을 위한 투자가 중요과제

5 양자 시대의 보안 위협

❑ 양자컴퓨터는 중첩(superposition), 얽힘(entanglement) 등 양자의 고유한 물리학적 특성을 이용하여, 다수의 정보를 동시 처리할 수 있는 새로운 개념의 컴퓨터로 기존 디지털 컴퓨터로 해결이 어려운 문제를 풀 수 있는 강점을 보유

- 양자컴퓨터는 정보 처리의 기본 단위로 큐비트(qubit)를 사용하며, 큐비트는 “0”이면서 동시에 1도 될 수 있는 중첩(superposition)원리와 여러 큐비트 중 하나의 상태가 변하면 다른 큐빗의 상태를 예측 가능한 방식으로 동시에 변경되는 얽힘(entanglement) 현상으로 양자컴퓨터는 구동

❑ 1990년대 이론화된 양자 알고리즘 ‘쇼어 알고리즘’은 고성능 양자컴퓨터가 큰 정수의 소인수를 빠르게 찾을 수법을 제시

- 이것이 현실화되면 현재 널리 사용되고 있는 ‘RSA 암호’ 등의 암호기술은 고성능 양자컴퓨터에 의해 쉽게 해독될 위험
  - 오늘날의 RSA 암호화 알고리즘의 경우에 기존 컴퓨터는 2,048비트 디지털 키로 보호되는 통신을 중단하는 데 약 300조 년이 걸리지만 4,099 큐비트로 구동되는 양자 컴퓨터는 10초면 충분하다는 주장도 존재

❑ 2017년 양자컴퓨터 환경의 급속한 발전에 대비하기 위해 미국 NIST에서는 양자 내성암호 표준화 작업을 진행

- NIST 양자 내성 암호 표준화 작업은 초기에 약 10년으로 계획되었지만, 급속한 양자컴퓨터의 발달로 인해 현재는 그 기간이 대폭 단축되는 중
- 2019년 8월로 예정되어 있었던 1차 선정 결과 발표가 2019년 1월로 변경되었고, 2차 선정 결과 발표 역시 초기에는 2021년을 목표로 하였지만 실제로는 2020년 7월에 발표

[NIST 양자 내성 암호 2차 선정 결과]

소분류	구분	Finalist	Alternate	장점	단점
격자 기반	암호화/키교환	CRYSTALS-KYBER,NTRU, SABER	FrodoKEM, NTRU Prime	빠른 연산 속도	파라미터설정 어려움
	전자서명	CRYSTALS-DILITHIUM, FALCON			
다변수 다항식기반	암호화/키교환			작은 서명 크기와빠른 연산 속도	큰 키사이즈
	전자서명	Rainbow	GeMSS		
해시 기반	암호화/키교환			안전성 증명 가능	큰 서명사이즈
	전자서명		SPHINCS+		
아이소지니 기반	암호화/키교환		SIKE	작은 키 사이즈	느린 연산속도
	전자서명				
코드 기반	암호화/키교환	Classic McEliece	BIKE, HQC	빠른 암호화 및복호화 속도	큰 키사이즈
	전자서명				
영지식 기반	암호화/키교환			numbertheoretic 혹은 structuredhardness에 기반하지 않음	큰 서명사이즈
	전자서명		Picnic		

* 출처: 양자컴퓨터와 양자 내성 암호 동향(주간기술동향, 정보통신기획평가원, 2021. 1. 13.)

Ⅲ. 데이터 보호기술 전망과 육성 정책

1 데이터 보호기술 시장 전망

☐ (세계시장) 세계시장 규모는 2019년 2,765억 달러이며, 연평균 약 11.1%로 성장하여 2025년에는 시장규모가 5,201억 달러에 이를 것으로 전망[4)]

- 2019년 세계 정보보호 시장에서 정보보안은 1,682억 달러로 가장 큰 비중으로 나타나며, 물리보안, 융합보안의 순서로 큰 규모
- 세계적으로 대형 사이버공격과 정보유출 사고가 빈번함에 따라, 정보보호 제품·서비스 수요와 투자가 늘어 성장세는 지속될 것으로 예상
- 2020년 전 세계 사이버보안 시장규모 1,522억 1,000만 달러(한화 약 171조 1,601억 원)로 추정[5)]
  - 전 세계 사이버보안 시장에서 PC 부문이 절반(50.0%)을 차지, 뒤이어 IoT(27.4%), 모바일 네트워크(16.1%) 순

☐ (국내시장) 국내 정보보호산업 시장은 2019년 11조 4,570억 원에서 연평균 12.7% 성장하여 2025년에는 23조 5,040억 원까지 증가될 것으로 예상됨

- 시장규모는 물리보안 시장이 가장 크지만 연평균 성장률 측면에서는 융합보안 분야가 가장 빠르게 성장할 것으로 예상

[데이터 및 정보보호 관련 시장전망]

(단위: 십억달러(세계), 십억원(국내))

구분		'19	'20	'21	'22	'23	'24	'25	CAGR
정보보안	세계	168.2	185.4	204.3	225.1	248.1	273.4	301.3	10.2%
	국내	3,278	3,815	4,442	5,170	6,019	7,007	8,156	16.4%
물리보안	세계	90.3	96.9	104.0	111.5	119.7	128.4	137.8	7.3%
	국내	7,280	7,833	8,428	9,069	9,758	10,499	11,297	7.6%
융합보안	세계	18.0	23.1	29.7	38.2	49.1	63.0	81.0	28.5%
	국내	900	1,156	1,486	1,909	2,453	3,152	4,051	28.5%
전체(합계)	세계	276.5	305.4	338.0	374.9	416.8	464.9	520.1	11.1%
	국내	11,457	12,804	14,355	16,148	18,230	20,658	23,504	12.7%

* 출처: ICT R&D 기술로드맵 2025-차세대보안-블록체인(정보통신기획평가원, 2020.12)의 자료를 기반으로 재가공

4) ICT R&D 기술로드맵 2025-차세대보안-블록체인(정보통신기획평가원, 2020.12) 참조
5) 2020 글로벌 정보보호 산업시장 동향조사 보고서(한국인터넷진흥원, 2021.03)

☐ 디지털 전환이 데이터 보안에 미치는 영향으로는 사이버 공간의 확장, 보호 대상의 증가, 신기술로 무장한 사이버 공격의 진화로 요약할 수 있음

- (사이버공간 확장) 사이버공간이 정보통신망과 서비스 제공 공간에서 신기술 기반의 초연결 융합서비스로 확장
- (보호대상의 증가) 사이버공간의 확장에 따라 보호대상이 ICT 정보자산에서 IoT 기기, 의료기기, 산업제어시스템(스마트 팩토리) 등으로 확대
- (사이버공격 진화) 기존 사이버위협이 대규모 테라급으로 확대되고 AI 해커에 의한 공격 등 신기술로 무장한 사이버공격의 진화

[공급망 공격 프레임워크]

* 출처: ICT R&D 기술로드맵 2025-차세대보안-블록체인(정보통신기획평가원, 2020.12)

☐ 디지털 전환에 따라 비대면 환경과 디지털 경제 인프라를 뒷받침하기 위한 제로 트러스트, 데이터 보호 등 기술개발 증가

- (제로 트러스트 보안) 비대면 환경 확산에 따라 경계망 보호(방화벽, VPN, SDP 등)에서 사용자 중심 비경계 보안기술 연구가 진행 중
  - 2023년까지 전체 기업의 60%가 VPN에서 벗어나 제로트러스트(Zero Trust) 기반의 SDP 보안 개념으로 바뀔 전망('20, Gartner)
- (데이터 보호) 안전한 데이터 이용을 지원하기 위한 암호기술, 프라이버시 보호 기술 등 데이터 보호기술 활용 확산 전망

☐ AI를 폭넓게 활용한 보안기술 도입이 시도되고 있으며, 6G, 양자 등 미래 신기술에 대한 정보보호 원천기술 개발 예상

- (AI 보안) 보안 프로세스(모니터링-분석-사고대응) 全과정에 AI를 접목하여 보안 위협 자율 대응과 AI 역기능 해결을 위한 연구 진행 중
- (미래 기술 전략 대응) 글로벌 환경에서 사이버보안 주도권 확보를 위해 국가 간 6G 보안, 양자 보안 분야 기술개발 국제 협력 확대

2 국가별 데이터 보호 관련 정책[6]

□ (미국) 미국은 2003년 연방정부, 지방정부, 민간부문에 이르는 사이버보안을 아우르는 정책으로 '사이버안보를 위한 국가전략'을 수립하고 이후 국가 안보적 차원에서 지속적으로 추가적인 정책을 수립 중

- 해당 국가전략의 주요 내용은 사이버 위협에 대한 미국의 핵심 인프라 방어, 사이버 위협에 직면한 국가적 약점 감소, 공격으로 인한 피해 최소화와 같은 세 가지 전략 목표를 제시
- (미국국가사이버보안전략) 「국가사이버보안전략」은 자국민·국토·시민의 삶에 대한 보호, 미국의 번영 촉진, 힘을 통한 평화 유지, 미국의 영향력 증대의 4개 전략영역(Pillar) 및 전략과제로 구성되었으며 미국이 직면한 사이버 위협으로부터의 정보보호 및 연방정부의 사이버 역량 강화를 위한 수행 단계 제시
- (NITRD[7]) 2019년 9월에 나온 미국 ICT R&D 프로그램인 NITRD(Networking & Information Technology Research & Development Program)은 $55억 규모(요구안 기준)로 11개 투자 분야를 선정, 그 중 사이버보안 분야는 12%(6,600억 원) 비중으로 투자계획 수립
- (NISTIR 8228) 미국 국립표준기술연구소(NIST)는 IoT의 사이버보안 및 개인정보보호 관리와 관련된 과제와 해결방안을 제시한 보고서 「NISTIR 8228」(2019년 6월)을 발간하였으며, 개별 IoT 기기와 관련된 사이버보안 및 개인정보보호 위험성에 대한 연방 및 기타 기관들의 이해·관리 증진을 지원하기 위한 목적
- 바이든 신정부의 출범으로 사이버보안 정책 추진에 박차 전망
  - 조 바이든 제46대 미국 대통령은 취임 이후 '모든 정부부처 수준에서 사이버보안을 최우선 순위로 삼을 것'이라고 강조
  - 미국의 ICT 정책은 크게 ▲빅테크 규제, ▲디바이스 해소, ▲국제 테크놀로지 리더십과 같은 3대 기조로 추진 전망

□ (독일) 2020년 12월 연방정부, 정보기술법 개정 초안 통과

- 제품 및 서비스의 디지털화 증가, IoT 제품 확산, 정교한 사이버보안 위협의 출현 등 빠르게 변화하는 환경에 대응하기 위한 개정안 발의
  - 해당 법안은 2021년 1분기 내 의회에서 공식 제정될 예정이며 사이버보안 강화를 위한 신규 기관 다수 설립 예정
- 2020년 8월 국가 사이버보안 강화를 위한 설립계획 발표, 2023년까지 사이버보안 기관 창설에 약 3억 5,000만 유로(한화 약 4,710억 원)의 초기 자금 투입 예정

6) 2020 글로벌 정보보호 산업시장 동향조사 보고서(한국인터넷진흥원, 2021.03)의 내용을 근간으로 작성
7) NITRD : 각 부처별 ICT 분야 R&D 사업들을 하나로 통합한 범부처 ICT R&D 프로그램으로, 대통령 직속기구인 국가과학기술위원회(NSTC) 관리 하에 운영

■ 2021년 1월 연방보안청(BSI), 비즈니스 연속성 관리 시스템(BCMS) 설정을 위한 새로운 표준 발표

- 해당 표준은 비상 상황 발생 시 신속한 대응이 가능하도록 정보보안을 포함한 IT 시스템 및 인프라 보호에 관한 요구 및 권장 사항을 포함

[독일 정보기술법 개정안 주요 내용]

구분	세부 내용
연방보안청 역할 강화	▷ 연방보안청의 감사 및 연방 행정부가 사용하는 IT 시스템 및 제품에 대한 통제 권한 강화를 위해 다음과 같은 권한을 부여 - 연방 행정부의 IT 시스템 및 제품에서 생성된 로그 데이터를 처리하고, 보안 위협을 감지 및 통보하는 권한 - 일부 예외를 제외하고, 연방 행정부에 통신 서비스를 제공하거나 이에 참여하는 모든 기관에 로그 데이터를 요청할 수 있는 권한 - 연방정부에서 사용하는 IT 시스템 및 제품의 최소 보안표준 설정 권한
소비자 보호 강화	▷ 소비자 보호를 강화하기 위해 연방사무소에 다음과 같은 권한 부여 - 보안 위협에 대한 경고 및 지침 발행 권한 - 소비자에게 제품의 IT 보안 수준을 알리는 IT 보안 레이블 설정 권한
기업의 예방 조치 강화	▷ 주요 네트워크 운영자 및 IT 시스템의 전반적인 보안 수준 강화 - 에너지 공급 네트워크 및 시스템 운영자를 포함한 핵심 인프라 운영자는 공격 탐지를 위한 시스템을 사용해야 함 - 중요 인프라 운영자에게 이미 적용되고 있는 보고 의무는 향후 방산 기업, IT 기업 등 공익성과 고부가가치로 국가적으로 중요한 기업에도 적용
국가 보호 기능 강화	▷ 중요 인프라 운영자가 공인인증기관에서 평가 및 인증하지 않은 주요 구성요소를 사용하는 것을 금지

* 출처: 2020 글로벌 정보보호 산업시장 동향조사 보고서(한국인터넷진흥원, 2021.03)

☐ (영국) 1998년 제정된 「정보보호법(Data Protection Act 1998)」은 2018년 12월 추가 개정되었으며, 영국 정보보호의 근간이 되는 법률이고, 「개인정보보호법」은 보호 대상이 되는 개인정보를 규정, 개인정보 관리자의 통보의무, 국가보안·범죄·보건·언론·예술 등 개인정보보호 적용 예외 산업, 개인정보보호 효력 등에 대한 내용을 담고 있음

■ (NIS 규정) 2018년 유럽 네트워크 정보보호원(ENISA, European Union Agency for Network and Information Security)의 「네트워크 및 정보시스템 지침(NISD, Network Information Systems Directive 2016)」에 따라 마련된 규정

- 국가 주요 인프라 및 디지털 기반의 서비스를 운영하는 자(OES) 또는 디지털 서비스 제공자(DSPs)에게는 보호 조치를 실시하고 침해사고 발생 시 이를 통지하는 등의 법적 의무 발생

■ (국가사이버보안전략) 2016년 「국가사이버보안전략(National Cyber Security Strategy)」 수립을 통해 2021년까지 사이버보안 인프라 구축을 추진

- 컴퓨터 및 인터넷이 보편화되며 사이버범죄가 급증하자 개인정보 보호 및 민간부문의 사이버범죄 대응능력 제고를 위해 지난 2009년과 2011년 「사이버보안전략」 발표

- 사이버범죄 대응 역량을 향상하고 사이버보안 분야의 글로벌 경쟁력을 확대하는 것을 주요 목적으로 하며, 이를 위해 5년 동안 19억 파운드(한화 약 2조 8,628억 원)를 투자

- 영국은 2019년 시행된 EU 개인정보보호법(General Data Protection Regulation, GDPR)과 자국의 개인정보보호법을 동시 적용
  - 브렉시트 이후에도 EU 일반 개인정보보호법이 적용될 것으로 예상되나, 유럽에서 영국으로 개인정보를 전송하는 행위는 제한될 수 있을 것으로 보임
  - 디지털문화미디어스포츠부, 2020년 12월 온라인유해백서 세부규정 공개 및 온라인 피해 근절에 관한 정부성명 발표
  - 또한 2020년 9월에는 데이터 활용 증진 및 혁신을 촉진하기 위해 데이터보호 및 적정성 확보 방안에 관한 국가데이터전략(National Data Stratege, NDS)을 발표

□ (일본) 2014년 6월, 일본 정부 산하 IT종합전략본부가 마련한 개인정보보호법 개정 초안은 빅데이터 활용에 사용되는 스마트폰의 위치정보 및 웹사이트 이용 이력 등 데이터 관리에 대한 제도적 근거를 마련

- 2013년 6월 정보보안정책회의를 통해 최초로 도입되었으며, 2015년 1월 사이버보안기본법 시행 이후 사이버보안전략본부가 주무 부처 역할을 하고 있음
  - 현재와 향후의 사이버 위협에 대한 국가 차원의 대응 방안을 수립하고 공공과 민간의 관련 당사자들을 위한 전략적 대처 방안을 제시하는 기능을 담당
  - 3년 단위로 정기적인 업데이트가 이뤄지고 있는 사이버보안전략은 2018년 6월 내각사이버보안센터(NISC)가 최신 전략 버전을 확정하여 공공의견 수렴을 거친 뒤, 2018년 7월 말 각료회의를 통해 해당 안을 승인
- 2020년 도쿄 올림픽을 앞두고 사이버공격의 지능화 및 대규모화에 대한 대응 차원에서 또 한 차례의 개정안이 발의
  - 개정안에서는 대량의 데이터를 분석·활용하는 사례가 늘어나면서 사이버 위협 발생 시 실생활에 미치게 될 파급력이 커지고 있는 상황과 2020년 도쿄 올림픽, 장애인 올림픽 등 대규모 행사를 앞두고 향후 3년 동안의 새로운 사이버보안 시책 목표와 시행 방침을 명시

□ (중국) 2020년 6월 1일부터 해당 법률에 따르면, 주요 정보 인프라 운영자는 네트워크 제품 서비스 및 구매가 국가보안에 영향을 미치거나 미칠 가능성이 있을 시 보안 심사를 받아야 하는 네트워크 안전심사판법(网络安全审查办法) 시행

- 중국 국가발전개혁위원회, 국가안전법 등 관련 법률에 의거하여 「국가기술안전관리 리스트제도」 수립을 추진 중
  - 국가발전개혁위원회는 해당 제도의 마련을 통해 국가 안전 위험을 더욱 효과적으로 예방 및 해결할 것이라고 발표
- 2020년 중국 사이버보안 주간, 정저우에서 개최(2020년 9월)
  - 2020년 중국 사이버보안 주간은 중국 중부 허난성 정저우에서 개최(2020.9.14.~9.20.)
  - 2020년 사이버보안 주간의 주요 행사는 디지털 전시회로, 100개 이상의 기업이 라이브 스트리밍 및 3D 모델링을 사용하여 사이버보안 주요 성과, 첨단 기술, 최신 제품을 전시

3 우리나라의 데이터보호 관련 전략

◎ 데이터보호 핵심기술 개발 전략(2021년 11월)

□ (개요) 디지털대전환으로 데이터는 4차 산업혁명의 핵심자원으로 부상하였으며 이를 잘 활용하기 위해 데이터 보호기술의 확보가 필수적이어서 2021년 11월 과학기술정보통신부는 '데이터보호 핵심기술 개발 전략'을 수립하고 발표

□ (비전) 데이터 경제의 안전한 토대 마련

- (목표1) 데이터 보호기술 확보·적용을 통한 데이터 유출 피해 저감
- (목표2) 데이터 신뢰 유통을 통한 안전한 데이터 생태계 활성화 견인

□ (추진전략) 3개의 추진전략으로 구성

- [전략1] 데이터 보호기술의 글로벌 수준 경쟁력 확보
- [전략2] 데이터 보호기술의 시장안착을 위한 지원 강화
- [전략3] 지속적인 데이터보호 기술성장 기반 조성

◎ 디지털 전환시대 정보보호산업의 전략적 육성 방안(2022년 02월)

□ (개요) 국가 차원에서 정보보호산업을 전략적으로 육성하여 사이버보안 대응력을 강화하는 한편, 새로운 경제 성장 기회로써 활용할 필요로 2022년 2월 관계부처 합동으로 '디지털 전환시대 정보보호산업의 전략적 육성 방안'을 수립하고 발표

□ (비전) 튼튼한 정보보호산업 육성으로 안전한 디지털 전환 구현

- (목표) 정보보호산업 시장규모 2025년 20조원 달성

□ (추진전략) 4개의 추진전략으로 구성

- [전략1] 성장 동력 확보를 위한 정보보호 新시장 창출
- [전략2] 글로벌 일류 정보보호기업 육성
- [전략3] 정보보호산업 기반 강화를 위한 생태계 확충
- [전략3] 차세대 정보보호 기술경쟁력 확보

Ⅲ. 차세대 데이터 보호기술 개요[8]

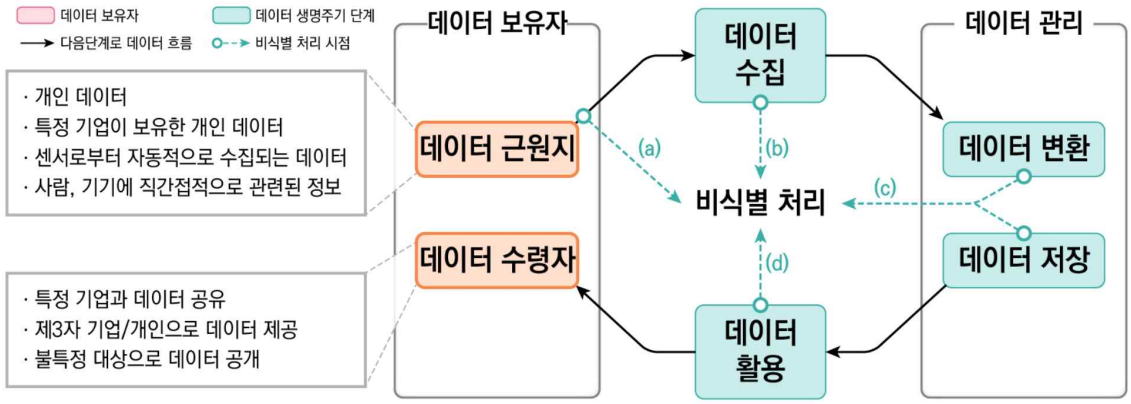
1 대표적 차세대 데이터 보호기술

◎ 공통 기반 기술

□ 데이터 비식별화

- (개념) 통계 등 정형 데이터와 영상·음성 등 비정형 데이터에 대한 개인정보 데이터 셋에서 개인을 식별할 수 있는 요소 전부 또는 일부를 삭제하거나 대체하는 방법을 활용, 개인을 알아볼 수 없도록 하는 비식별화 기술
- (필요성) 데이터 3법이 시행됨에 따라 개인의 명시적 동의 없이 연구 목적으로 사용하기 위해서는 비식별 조치가 이뤄져야 하며 이런 이유로 비식별화 시장 역시 급성장할 것으로 기대
- (정부의 지원 방향) 통계 등 정형 데이터와 영상·음성 등 비정형 데이터에 대한 개인정보 비식별화 기술을 개발하고 비식별 과정의 민감정보 노출 위험 검증 기술개발도 추진

[빅데이터 환경에서 비식별 처리를 위한 생명주기]



* 출처: 빅데이터 환경에서의 개인정보 비식별 처리방법 분석(임형진, 전자금융과 금융보안, 2017.04)

□ 차등 정보보호

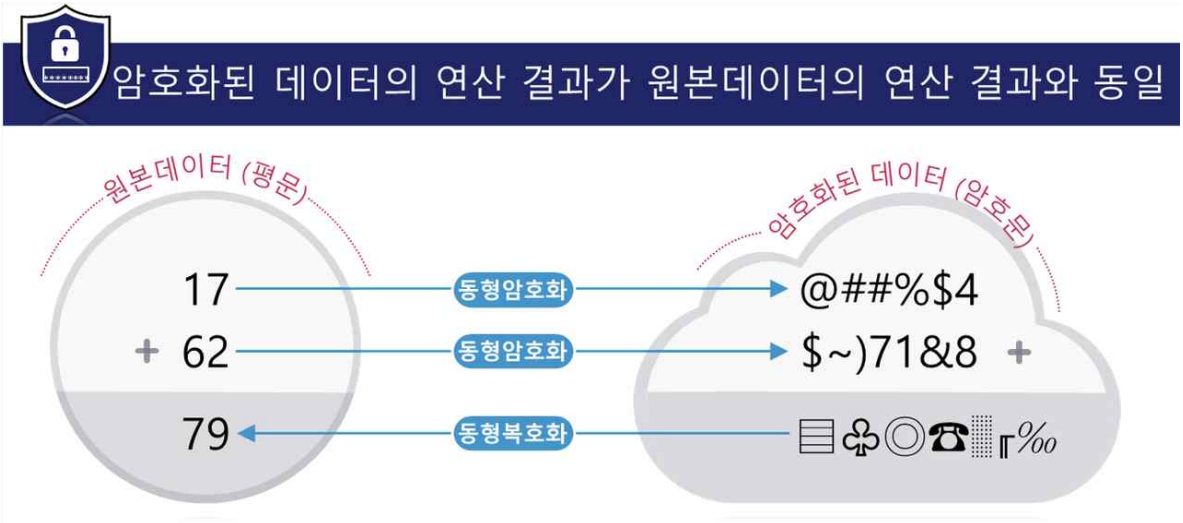
- (개념) 차등 정보보호(Differential Privacy)란 개인의 데이터를 다른 사람의 수많은 데이터와 조합해, 개인정보를 침해하지 않으면서도 통계를 얻을 수 있는 기술
- (필요성) 빅데이터와 인공지능 학습 과정에서 개인정보보호의 중요성이 부각되면서 안전한 데이터 활용을 지원하는 차세대 개인정보보호 강화 기술 중 하나로 관심 증대
- (정부의 지원 방향) 차등 정보보호에 대한 원천기술을 확보하고, AI 기계학습 등에 적용하기 위한 기술 개발 추진

8) 데이터보호 핵심기술 개발 전략(과학기술정보통신부, 2021.11)에서 도출된 기술을 기준으로 하였음

☐ 동형 암호

- (개념) 동형 암호(Homomorphic Encryption, HE)는 데이터를 암호화된 상태에서 연산이 가능한 암호화 방법으로 암호문들을 이용한 연산의 결과는 새로운 암호문이 되며, 이를 복호화하여 얻은 평문은 암호화 하기 전 원래 데이터의 연산 결과와 같을 수 있도록 하는 기술
  - 개인정보보호의 경우 암호화된 개인정보를 제공함으로써 허가받지 않은 사람이 개인정보를 확인할 수 없도록 하지만, 정상 사용자는 보호된 서비스를 받을 수 있고, 기업의 관점에서 다른 기업 및 기관과 데이터를 결합하는 경우에도 데이터 유출에 대한 우려를 없앨 수 있음
- (필요성) 스토리지 아웃소싱, 헬스케어, DNA 분석, 스마트 시티 등 가상 물리 시스템, 기계학습, 양자내성 암호, 금융 협업 등에 활용될 수 있을 것으로 기대
- (정부의 지원 방향) HW 지원 완전 동형 암호 가속 처리 기술 개발 등 동형 암호의 처리속도를 향상시키는 기술을 개발하고, 활용기반 확대를 위한 분야별 적용기술 개발

[동형 암호의 개념]



* 출처: 삼성SDS 블로그

☐ 양자내성 암호

- (개념) 양자컴퓨팅의 환경에서도 안전한 암호 알고리즘으로 기존의 공개키 암호가 가지고 있던 빠른 해독성 문제를 해결하고 대체할 수 있는 암호를 말하며, 기존의 인수분해나 이산대수 문제가 아닌 전혀 새로운 문제에 안전성을 기반
- (필요성) 몇 년 후 양자컴퓨터의 성능이 발전할 경우 기존의 암호체계는 더이상 안전하지 않으며, 이를 대비하여 선행적 기술개발이 필요
- (정부의 지원 방향) 알고리즘 취약점 등 암호 안전성을 검증하고, IoT 등 저사양 디바이스에 적용하기 위한 기반기술 확보 및 국제표준화에 대응하여 통신망, 스마트시티 등 국내 인프라에 양자 내성암호를 도입하기 위한 안전성, 효율성 검증기술 확보추진

◎ 응용 기술

☐ AI 학습 데이터 보안

- (개념) AI 모형의 학습 단계에서 데이터나 AI 모형에 대한 오염(poisoning) 공격이나 AI 모형 자체에 대한 오염공격에 대한 보호를 위한 기술
- (필요성) AI에 대한 관심과 활용도가 높아지면서 보안과 관련된 새로운 공격 방식들이 계속 나타나고 있어 이러한 공격에 대한 대비가 필요
- (정부의 지원 방향) 분산된 AI 학습으로 어뷰징·재생성[9]으로부터 안전한 연합학습 기술개발

☐ 정보 유출 방지·추적

- (개념) 사용자 접근 제어, 사용자ID 공개 등 기술을 활용한 정보유출 방지·추적 기술
- (필요성) 산업기술 유출범죄는 해마다 증가하는 추세로 과거에는 대기업과 IT 분야 중심에서 최근에는 전기·전자, 정밀기계 분야까지 확대, 보호대상은 증가하고 유출 수법은 고도화, 다변화
- (정부의 지원 방향) 사용자 접근제어, 사용자ID 공개[10] 등 기술을 활용한 정보유출방지·추적기술개발

☐ 데이터 권한 관리

- (개념) 컴퓨터에서 저장·처리되는 데이터에 대해 권한이 없는 사용자의 부적절한 접근을 막고 동시에 정당한 권한을 갖고 있는 사용자는 정보 시스템이 서비스 요구를 거부하지 않도록 보호할 수 있도록 관리하는 기술
- (필요성) 데이터 대전환의 핵심인 데이터는 크게 증가 추세이며, 빅데이터의 보안 관리가 미흡해 데이터가 손실되면 데이터를 소유한 조직체의 운영에 심대한 지장을 초래하기 때문에 매우 중요
- (정부의 지원 방향) 블록체인, 데이터주권 보호기술[11] 등으로 데이터 유통·활용과정 중 신뢰성 보장, 프라이버시 보호 등을 확보 및 개인정보의 자기결정권을 강화하기 위한 개인정보 동적 동의 기술 등

☐ 블록체인 데이터 보호

- (개념) 블록체인은 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 포괄해 더 강화된 탄력성과 암호화, 감사, 투명성을 제공할 수 있는 특징을 가지며 이를 이용해 데이터 보호에 활용하는 기술
- (필요성) 블록체인의 특성을 이용해 금융 서비스, 에너지, 제조 분야 등에서부터 콘텐츠 전송 네트워크, 스마트 그리드 시스템과 같은 애플리케이션 분야에도 확장 적용이 가능
- (정부의 지원 방향) 전자문서, 신원인증, 물류·유통 등 분야의 데이터 보호를 위해 블록체인 기술을 활용한 시범사업 추진

---

9) (어뷰징) 악의적 참여자의 데이터오염 공격, (재생성) AI 모델로부터 원본 데이터를 다시 생성
10) 내부 사용자에 의한 정보 유출을 방지하기 위해 촬영 시 사용자 ID를 출력
11) 암호화 기반 데이터 소유권 증명, 중복데이터 확인, 중재자 없는 활용 권한 전달 기술 등

☐ IoT/스마트시티 데이터 보호

- (개념) 스마트시티 운영 시스템을 대상으로 발생하는 외부(DDoS, 사이버표적공격 등) 및 내부(내부자 데이터 유출 등)의 사이버 보안 위협을 탐지하는 보안관리 기술
- (필요성) 스마트시티의 공격 대상에는 중요 인프라에 대한 정교한 사이버 공격, 산업 제어 시스템(ICS), 저전력 광대역 네트워크(LPWAN) 남용 및 장치 통신 하이잭킹, 랜섬웨어로 인한 시스템 잠금 위협, 광범위한 패닉(예: 재해 감지 시스템)을 야기하는 센서 데이터 조작 등이 포함되며 점점 증가하는 추세이며, 공격이 성공할 경우 피해 규모가 매우 큼
- (정부의 지원 방향) IoT 디바이스, 스마트시티 환경에 대한 인프라 보호 기술 개발과 스마트시티 데이터 플랫폼 보호 기술, 스마트시티 내 개인정보(출입정보, CCTV 등) 보호기술 등을 확보

☐ 자율이동체 데이터 보호

- (개념) 자율주행차 및 이종 자율 무인이동체를 통합적으로 연동할 수 있는 인프라 보호 기술 및 비인가 무인 이동체의 인증 제한기술
- (필요성) 무인 이동체가 갖는 특징과 구동 방식, 기능을 고려한 보안 시스템이 필요하지만 무인 이동체에 대한 개발 표준이 정형화돼있지 않은 상황이기 때문에 관련 기술표준과 함께 데이터 보호 관련 기술개발이 필요
- (정부의 지원 방향) 데이터 위·변조, 정보유출 등 자율주행차의 사이버 침해 대응 기술을 확보하고, 자율이동체의 위치정보, 주행 정보, 센서 데이터 등에 대한 신뢰성 및 프라이버시 확보 기술개발

☐ 의료 데이터 보호

- (개념) 개인의 의료기록 데이터의 보호와 커넥티드 의료기기의 공격에 대한 보호 등 건강관리와 의료 데이터 및 기기에 대한 안전을 보장하는 기술
- (필요성) 정부가 코로나19 사태를 계기로 의사와 환자 간의 비대면 진료를 한시적으로 허용하는 등 '비대면 산업을 적극 육성해야 한다'는 입장을 보이면서 원격의료 도입 관련 논의도 급물살을 타고 있으며, 이와 관련된 데이터 보호 기술 역시 같이 개발되어야 함
- (정부의 지원 방향) 커넥티드 의료기기의 이상행위 탐지 기술, 생리학적 개인정보(맥파·심전도등)의 암호화 기술 등을 개발하고 의료정보 시스템의 데이터 유출방지를 위한 보안관리 기술, 스마트병원의 보안관제 기술 개발도 추진

☐ 스마트제조 데이터 보호

- (개념) 스마트공장의 다양한 기기의 보안성 및 신뢰성 확보를 위한 기기별 상호 보안 인증과 비인가 접근 차단, 임베디드 디바이스, 펌웨어 바이너리 등 분석을 통한 보안 취약성 자동 진단 기술
- (필요성) 지능화된 스마트공장의 도입으로 생산 비용 및 시간 감소, 고객 맞춤형 생산, 생산 효율성 극대화 등의 이점을 불러왔지만, 공격자가 산업제어시스템에 직접 접근할 수 있는 경로인 인터넷과의 접점이 증가하면서 보안 위협은 더욱 증가
- (정부의 지원 방향) 공장 제어프로토콜[12]에 대한 보안 칩을 개발하고, 스마트공장 네트워크에 특화된 데이터 보호기술 개발추진

[데이터 보호 기술개발 로드맵]

* 출처: 데이터보호 핵심기술 개발 전략(과학기술정보통신부, 2021.11)

12) 설비에서 서비스까지 end-to-end 보안 및 실시간·고가용성을 보장

2 데이터 보호기술 관련 기술개발 동향

◎ 가명 처리 비식별화 기술 개발 플레이어

☐ SK C&C

- SK C&C는 자사 판교데이터센터에 가명정보 결합 및 검증 전문 시스템을 구축하고 있으며, 금융·통신·제조 등 다양한 분야의 고객사에 가명 정보를 기반으로 한 맞춤형 결합 서비스를 제공
  - 주요 서비스로는 데이터 결합 활용 컨설팅, 데이터 수집·연계, 가명처리 결합·분석 등
  - 고객을 위한 별도의 가명 데이터 결합·분석 환경 뿐 아니라 데이터 서비스 모델 생성부터 실행·폐기에 이르는 '데이터 서비스 라이프 사이클 관리'도 지원하며, 이를 위해 산업별 버티컬(Vertical, 수직적) 데이터 플랫폼·서비스 모델도 개발 중

☐ 케이티넥스알

- 케이티넥스알은 2021년 개인정보 비식별화 솔루션 'NEA(NexR Enterprise Anonymous)'를 출시
- NEA는 쿠버네티스 기반의 클라우드 환경에 최적화된 기능과 성능을 제공하며, 주기억장치에 데이터베이스를 저장하는 인메모리 기술을 적용해 빠른 비식별 처리가 가능

☐ 이지서티

- 이지서티는 사전검토를 위한 정형·비정형·반정형 빅데이터에 포함된 개인정보의 실시간 탐지 기능이 있으며, k-익명성을 만족하기 위한 k·l·t 방식의 비식별화 기능을 가지는 개인정보 비식별조치 솔루션인 아이덴티티 쉴드(identity shield)를 제공
- 데이터 전처리, 개인정보 자동탐지, 안전한 익명성 비식별화 및 연계 기술을 보유하며 Hadoop 시스템에서도 비식별 처리 가능한 기술 개발

☐ 컴트루테크놀로지

- 컴트루테크놀로지는 인공지능(AI)을 통해 주민등록표, 가족관계증명서 등 신분증 및 주요 증명서에서 내 개인정보를 찾아 이를 비식별화하는 기술을 개발
- 개인정보보호위원회와 한국인터넷진흥원(KISA)가 2021년 기술개발을 지원한 후, 개인정보를 탐지해 비식별처리 할 수 있는 주요 증명서의 종류가 총 13종에서 25종으로 약 2배 증가했으며, 관련 특허까지 출원했다. 증권사 납품 등 사업화도 활발하게 진행 중

☐ 데이타스

- 데이타스는 개인정보 가명·익명처리 통합관리 솔루션을 개발하는 회사로, 가명처리 대상을 식별해 위험도를 측정하고, 이에 따른 적정한 가명처리 기술을 추천하는 기술과 가명정보 재식별 가능성 및 적정성을 평가하는 기술을 보유
- 원본 데이터와 동일한 통계적 특성을 가진 가상 데이터인 재현 데이터 생성·검증 기술을 중점 개발하고 있어 향후 데이터 수요 기업의 안전한 활용을 지원하는 데 기여할 것으로 기대

◎ 동형 암호 및 양자내성 암호 기술 개발 플레이어

☐ 삼성SDS

- 삼성SDS는 마이크로소프트와 인텔, 구글, IBM, MIT 등 굵직한 글로벌 기업 및 학교와 컨소시엄을 구성해 동형암호기술의 표준화 작업을 진행하고 있으며 국내에서 참여하는 곳은 삼성SDS와 서울대학교가 유일

- 삼성SDS는 동형암호 기술을 지속 고도화하고 산업현장의 활용도를 넓혀갈 계획이며, 최근에는 금융기관의 고객 신용평가 분석과 의료기관의 중증 질환 예측 등에 동형암호 기반 분석서비스를 적용하기 위해 고객사와 기술 검증을 완료했다고 발표

☐ LG유플러스

- LG유플러스는 양자암호기술 중 '양자키 분배(QKD)' 기술과 비교해 별다른 장비 없이 소프트웨어만으로 암호키 교환, 데이터 암·복호화, 무결성 인증 등 핵심 보안요소에 적용이 가능하다는 장점을 지닌 양자내성암호(PQC) 기술을 개발하고 있음

- 이는 QKD에 집중하는 SK텔레콤·KT와 차별화된 선택이며 이 선택을 위해 PQC 분야에서의 파트너십을 강화하는 동시에 장비개발과 디지털뉴딜 사업을 통해 양자내성암호 기술의 실증사례를 수집하고 있는 중

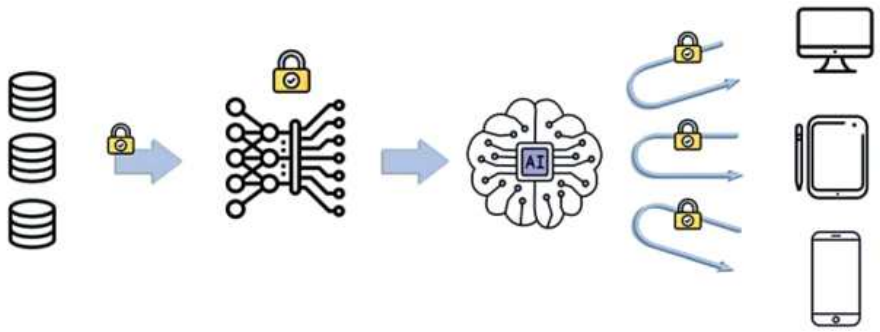
- 2021년 한국지능정보사회진흥원(NIA)이 주관하는 '양자암호통신 시범인프라 구축·운영' 사업에서도 LG유플러스는 코위버(10G급 전송장비), 서울대학교 크립토랩 등과 함께 수주받아 추후 공공·민간 부문 양자암호통신 인프라를 구축할 예정

☐ 크립토랩

- 암호기술 전문기업 '크립토랩'은 자체 개발한 동형암호 라이브러리 '혜안(HEaaN)'을 IBM의 AI 머신러닝 플랫폼 '에이치이 레이어(HElayers)'를 통해 배포한다고 '22년 3월 13일 발표

- 혜안은 임의의 연산을 무한으로 처리할 수 있는 '완전동형암호' 기술이 적용된 크립토랩의 동형암호 라이브러리로, '완전동형암호' 기술을 개발한 크립토랩과 IBM의 협력 연구를 통해 세계 최초의 '프라이버시 보호 AI 소프트웨어'인 에이치이레이어를 개발하였고 이번에 공개

[암호화된 데이터를 함수로 변형시켜 인공지능에 적용/연산 후 다양한 플랫폼으로 활용하는 과정]



* 출처: 크립토랩

Ⅳ. 결론 및 시사점

□ 코로나-19는 디지털 전환을 가속화하였으며, 정부는 한국판 뉴딜을 통해 우리나라의 새로운 경쟁력을 만들어가려고 준비하고 있으나 보안 위협도 같이 증가

- 국정원이 발간한 2021 국가정보보호백서는 현재 정부와 국가 기반시설 등을 대상으로 한 사이버공격 시도와 성공빈도가 증가하고 있다고 분석하고, 향후에도 다양한 돈벌이 목적의 사이버범죄가 끊이지 않을 것으로 전망

- IBM 시큐리티가 2021년 8월 발표한 결과에 의하면, 2020년 기업의 데이터 유출 사고 당 평균 손실액이 424만 달러(약 48억 9천만원)로, 역대 최고치를 기록

  - 코로나-19로 기업이 급격한 운영 변화를 하면서 보안 사고를 통제하기 더욱 어려워졌으며, 이 때문에 보안 사고로 인한 관련 비용도 전년 대비 약 10% 증가했다고 분석

  - 기업 중 60%가 클라우드 기반 활동을 확대했고, 원격근무 확대에 따른 기술 접근 방식 조정이 이같은 결과를 불러왔다는 분석

□ 우리나라의 경우 사이버 공격 피해가 중소기업·소상공인·개인에게 편중되어 있음에도 불구하고 기업의 정보보호 인력 부족 등으로 인해 새로운 사이버 위협 대응에 한계[13)]

- 한국인터넷진흥원이 국회 과방위에 제출한 자료에 따르면, 지난 2019년부터 2021년 7월 말 현재까지 최근 3년간 민간기업에서 발생한 해킹 사건은 1,383건이며, 이 가운데 중소기업에서 발생한 사건은 1,246건으로 90% 이상 차지[14)]

- 정보보호기업 아크로니스의 '2021 상반기 사이버 위협 보고서'에 따르면 공격자들이 MSP(관리형 서비스 제공사)의 공급망을 악용하면서 수많은 중소·중견기업이 특히 보안 위험에 노출돼있다고 경고

  - 2021년 상반기에도 SW기업 솔라윈즈와 카세야의 솔루션이 공급망 공격에 악용된 바 있음

□ 2021 국가정보보호백서에 따르면, 우리나라 정보보호 인력은 2020~2025년간 약 1만 명이 부족할 것으로 예상

- 국정원이 국가·공공부문 127개 기관을 대상으로 조사한 결과, 2020년 기준 정보보호 전담조직을 운영하는 기관은 46%에 불과했으며, 전담부서가 있는 경우도 10곳 중 4곳은 직원이 2명 이하

- 민간의 경우도 정보보호 조직을 보유한 국내 사업체의 비율은 13.4%에 그쳤으며, IT 예산 중 정보보호 예산이 차지하는 비중이 5% 이상인 사업체는 1.7%에 불과

- 지난해 정보보호산업 인력 5만 4,101명 중 물리적 보안인력을 제외한 정보보안 인력은 28.9%인 1만 5,655명에 불과

- 국정원은 "복잡한 공격에 대응하기 위해 빅데이터와 인공지능을 활용한 최첨단 보안기술 확보와 기술혁신이 포함된 연구개발 체계가 마련돼야 한다"고 제언하고 있으나 인력이 부족한 것이 현실

13) 2021 국가정보보호백서(국가정보원 등, 2021.05)
14) 사이버 위협에 노출된 중소기업, 최근 피해사례 90% 차지(보안뉴스, 2021.09.17.)

☐ 데이터 보호는 디지털 전환의 필수적인 요소로 인식해야 하며 새로운 성장동력의 하나로 육성하는 것이 필요

- 디지털 전환 가속화로 정보보호의 영역이 제조·유통·의료 등 전산업 영역으로 확장되면서 정보보호 제품·서비스 수요 증대
- 국내 정보보호 산업은 최근 3년간('18~'20년) 연평균 성장률은 8.4%로 상대적으로 높은 성장률을 보이면서, 새로운 경제 성장 기회를 창출하는 국가 전략산업으로 주목
- 글로벌 사이버보안 시장규모는 '20년 1,319억 달러로 전년 대비 약 4.8% 성장하였으며, '24년까지 연평균 9.4%의 성장전망[15)]

☐ 데이터 보호는 중소기업이 많이 진출한 업종이며 향후에도 충분히 역량을 발휘하는 것이 가능

- 정부는 2025년까지 인공지능(AI) 기반의 혁신 보안 기업 60곳을 발굴한다고 발표하였고, 이는 관련된 중소기업에 새로운 기회 요인
- 이를 위해 기술을 보유한 기업들의 협업 및 인수·합병(M&A)을 통해 기술개발의 성과를 올리고, 속도를 높이는 전략도 바람직
- 물리·정보보안산업 육성을 위한 K-사이버방역 지원사업 등을 기회로 활용하여 적극적인 성장전략을 추진할 필요
- 현재 보안 전문인력이 매우 부족한 상황이므로 인력확보를 위해 산·학 연계 과제, 해외인력 채용 등 다양한 방면의 시도가 필요하고 정책적 지원도 절실

☐ 보안 위협에 상대적으로 취약한 중소기업의 경우 보안에 대한 인식을 새롭게 하고 정부도 이를 지원하는 정책 필요

- 기업은 가장 중요한 민감 데이터를 필두로 내부 보안 우선순위를 정립하고 보안 솔루션을 도입해 운용 인력과 비용 등 제약 사항을 극복, 최적 보안 전략을 수립하는 것이 올바른 방향
- 정부는 보안 투자 여력이 부족한 중소기업 8천 300개사에 보안 컨설팅, 보안제품 도입 등을 지원하는 것으로 되어 있지만, 인적 지원 등 추가적인 정책적 배려 필요

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

참고문헌

1. ICT R&D기술로드맵2025-차세대보안-블록체인(정보통신기획평가원, 2020.12)
2. 데이터보호 핵심기술 개발 전략(과학기술정보통신부, 2021.11)
3. 정보보호산업의 전략적 육성 방안(관계부처 합동, 2020.02)
4. 2021년 보안위협 분석을 통한 2022년 보안위협 및 보안기술 전망(이글루시큐리티 홈페이지, 2022.01)
5. 비대면 시대의 신 융합보안 위협과 대응 방안에 대한 고찰(유동현외 3인, 한국융합학회 논문지, 2021)
6. 공급망 공격 사례 분석 통한 '위험관리 핵심전략'(IT Daily, 2021.10.21.)
7. 양자컴퓨터와 양자 내성 암호 동향(주간기술동향, 정보통신기획평가원, 2021. 1. 13.)
8. 2020 글로벌 정보보호 산업시장 동향조사 보고서(한국인터넷진흥원, 2021.03)
9. 빅데이터 환경에서의 개인정보 비식별 처리방법 분석(임형진, 전자금융과 금융보안, 2017.04)
10. 2021 국가정보보호백서(국가정보원 등, 2021.05)