디지털 국가의 초석, 디지털 안전

유재홍 선임연구원
소프트웨어정책연구소 AI정책연구팀
jayoo@spri.kr

생활 깊숙이 들어온 디지털

디지털은 우리 일상이 됐다. 스마트폰은 말할 것도 없고, 눈을 뜨고 있을 때는 물론, 눈을 감고 있는 순간까지 우리 삶은 디지털 기술 위에 놓여 있다. 어느 아침, 토스트는 맞춰진 시간에 따라 노릇하게 구워지고, 인덕션에서는 설정된 온도에 맞춰 계란프라이가 익어가며, 전자레인지에서는 밀키트로 제작된 양송이수프가 데워진다. 3℃로 설정된 냉장고에서 사과 하나를 꺼내 입에 베어 물고, TV를 켠다. 셋톱박스가 켜지면서 TV에서는 깨끗한 디지털 영상이 나온다. 뉴스 속보를 확인한 후 유튜브를 켜 간밤에 보던 예능 프로그램을 재생시킨다. 스마트폰에 음성으로 오늘 날씨를 물으니 간간이 소나기가 내릴 것이라며 화면에 구름 지도를 보여준다. 출근하기 위해 스마트워치를 차고, 주차된 자동차의 문을 스마트키로 연다. 매일 가는 길이지만 평소처럼 네비게이션을 켜고, 라디오를 튼다. 회사에 도착해 엘리베이터 버튼을 누른다. 해당 층에 도달하자 엘리베이터 문이 열린다. 정문 출입구에서 네임택을 찾는데 보이지 않는다. 집에 두고 온 모양이다. 지문 인식기에 손가락을 가져다 대문을 연다. 출입구에 설치된 열화상 카메라에 얼굴을 맞추어 '정상 온도'임을 확인하고 자리로 가 컴퓨터를 켠다. 하루의 시작이다.

고압 전류선을 타고 우리 컴퓨터까지 온 전기는 어떤 원자력 발전소에서 생산된 것일 수 있다. 또, 우리는 알게 모르게 무인 전철과 자동으로 운항하는 비행기를 타고 여행길에 오르고 있을 수 있다. 하루에도 몇 번씩 송금하고, 주식 거래를 하며, 가상화폐의 시세를 확인하고 매매한다. 많은 사람이 월 구독료를 기꺼이 납입하며 음악을 듣고, 전자 도서를 읽으며, TV 콘텐츠를 사서 본다. 그리고 데이터를 저장할 클라우드 공간을 임대해 쓴다. 스마트폰으로 찍은 사진은 설정에 따라 구글 포토로, 아이클라우드로, 네이버 클라우드로 실시간 전송된다. 온라인 뱅킹, 온라인 쇼핑, 온라인 게임 등 이제는 온라인이란 말을 빼도 인터넷을 우선 생각하는 시대가 됐다.

디지털에 문제가 생기면 우리의 삶도 심각한 타격을 받는다. 2018년 11월 22일 오전 미국의 아마존 웹서비스(AWS)에 서버 장애가 발생했다. AWS 서비스를 받고 있던는 국내 업체 쿠팡, KBS, 배달의 민족이 먹통이 되었다.[1] AWS는 2021년 12월에만 세 번의 장애를 일으켜 암호화폐 거래소 코인베이스, 에픽게임즈스토어, 동영상 스트리밍 훌루+, 기업용 메신저 슬랙 등이 피해를 입었다. 2022년 2월 6일 AWS 서버에 장애가 또 다시 발생했다. 배달의 민족, 요기요, 카카오게임즈의 오딘, 라스트 오리진, 에픽세븐 등이 마비되었다. 피해는 22분 남짓 이어졌다.

2021년 10월 4일 페이스북, 왓츠앱, 인스타그램이 거의 6시간 동안 다운되었다. 최고경영자인 마크 저커버그는 "혼란을 드려 죄송하다"며 직접 사과문을 올렸다. 일상적인 시스템 유지 보수 작업을 하면서 자사의 엔지니어가 의도치 않게 페이스북 데이터 센터와 인터넷의 연결을 끊는 명령을 내렸다고 밝혔다. 저커버그의 사과에는 82만 명이 넘는 사람들이 댓글을 달았다. 미국 경제지 '포브스'는 페이스북이 6시간 접속 중단으로 광고주가 이탈하며 약 6,600만 달러의 손실을 입었다고 주장했다.

지난 2022년 7월 3일 일본의 3대 이동통신사 중 하나인 KDDI의 통신망에 장애가 발생했다. KDDI는 3,100만 명의 개인과 법인 고객까지 합하면 6,200만 명이 사용하는 서비스다. 장애는 86시간 이어졌다.[2] 휴대전화, 데이터 통신은 물론이고 KDDI 망을 사용하는 현금자동입출금기(ATM), 닛폰유빈(일본 우편)의 화물정보 시스템에 문제가 생겨 우편 배달이 지연되었다. 일본 기상청의 기온, 강수량의 관측 정보를 다루는 시스템에도 문제가 생겼다. 전국 1,300개 기상 관측소 중 200곳이 영향을 받았다. 나리타공항, 하네다공항에서는 직원들의 무선 장비가 먹통이 되어 업무에 차질을 빚었다. 도요타, 마쓰다, 스바루 등 자동차 업체의 '커넥티드 카' 시스템 일부도 작동하지 않았다. KDDI는 약 3,915만 명이 장애로 인한 피해를 입은 것으로 추정했고 2022년 7월 2일 새벽에 발생한 설비 고장으로 VoLTE 교환기에 트래픽이 폭주하면서 서비스에 문제가 생겼다고 밝혔다. 다카하시 마코토 사장은 "고객에 큰 불편을 끼쳐 죄송하다"는 말밖에 할 수 없었다.

1) https://it.chosun.com/site/data/html_dir/2018/11/22/2018112201040.html

2) https://www.joongang.co.kr/article/25083967#home(2022.7.3.), https://www.techm.kr/news/articleView.html?idxno=99361

이보다 앞선 2021년 10월에는 일본 최대 통신사인 NTT도코모도 29시간 통신 장애를 겪었던 적이 있다. 이것은 KDDI 사고 발생 이전 사상 최대의 일본 통신망 장애 사건이었다. 가네코 야스이 일본 총무상도 7월 3일 오전 10시 긴급 기자회견을 열고 "국민 생활과 사회 경제의 중요한 인프라인 휴대전화 서비스 문제로 인해 많은 분이 장시간 이용 곤란을 겪고, 국민의 생명과 재산을 지키기 위한 소방·구급 등의 긴급 통보에 지장을 일으킨 사실을 심각하게 받아들이고 있다"며 사과했다. 일본에선 1시간 이상 장애로 3만 명 이상의 이용자에게 영향이 발생해 긴급 신고 등을 하지 못하는 경우 이동통신 사업자가 '중대사고'로 규정하고 총무성에 신고하도록 되어 있다.

2022년 7월 6일 독일 연방도로교통청(KBA)은 테슬라 모델Y, 모델3 차량의 리콜을 결정했다. 이유는 테슬라의 일부 차량에서 심각한 사고가 발생할 경우 긴급 구조대에 자동으로 연락되도록 설계된 '이콜(eCall)'이 고장을 일으켰고, 전 세계의 모델Y, 모델3 차량 약 5만 9,000여 대가 관련 영향을 받을 것으로 파악한 것이다.[3] 테슬라는 2022년 2월에도 미국 내 완전자율주행(FSD) 베타 버전 탑재 테슬라 차량 5만 3,822대의 리콜 계획을 발표했다. FSD 소프트웨어가 정지 신호에서 완전히 멈추지 않고, 속도만 살짝 줄인 뒤 그대로 주행하는 '롤링 스톱(Rolling Stop)'을 허용했기 때문이다. 미국 도로교통안전국(NHTSA)에 따르면 리콜 대상은 2016~2022 판매된 모델S, 모델X, 2017~2022년에 생산된 모델3, 2020~2022년 생산된 모델Y가 그 대상이었다. 테슬라는 2021년 11월에 소프트웨어 결함으로 2017년부터 미국에 판매된 차량 가운데 1만 1,704대를 리콜 중인 것으로 나타났다. 차량에 탑재된 소프트웨어가 전방 충돌 경고를 제대로 작동시키지 못하고, 긴급 제동 장치가 갑자기 활성화되는 등 주행 시 문제가 발생할 수 있다는 점이 그 이유다.[4]

만약 우리나라에서 자율주행차가 문제를 일으키면 어떻게 될까? 대검찰청 자료에 따르면 2022년 1월부터 시행된 중대재해처벌법에 근거해 자율주행차 운행 중 소프트웨어 결함이나 오작동으로 교통사고 및 인명 피해가 발생할 경우 '중대 시민 재해'로 인정돼 제조회사 대표가 처벌을 받게 된다.[5]

3) https://biz.chosun.com/international/international_general/2022/07/04/4DNKIUOQFRA3TIG47GODUZL4UY/
4) https://www.hankyung.com/international/article/202111022025Y
5) https://www.mk.co.kr/news/society/view/2022/03/192768/ (대검찰청 중대재해법 벌칙 해설서)

디지털 위험원의 다양화

전통적인 소프트웨어 오류는 코딩의 잘못으로 인한 경우가 대다수였다. 소프트웨어 공학적 접근을 통해 설계, 개발, 테스트 과정에서 오류를 꼼꼼히 확인하고 점검하는 접근을 하고 있으나 아직 학술 영역 외 산업계의 적용은 활발하지 못하다. 일부 대기업과 SW 전문기업을 중심으로 CMMI (Capability Maturity Model Integration), SP (Software Process), GS (Good Software)와 같은 소프트웨어 품질, 개발 프로세스 인증을 통해 안전성을 높이고자 하는 움직임은 있으나 대체로 규제 준수, 사업 낙찰을 위한 요건 확보, 사업자 선정 평가 시 가점 등의 혜택을 받기 위해 수행하는 경우가 대부분이다. 소프트웨어 오작동으로 인해 수백억, 수천억 원의 프로젝트가 먹통이 되거나 시스템 오류로 이어진 예들은 불행하게도 많이 찾아볼 수 있다.

지난 2022년 8월 30일 발생한 이스트시큐리티의 보안 소프트웨어인 알약 오류 사태가 대표적이다. 1,600만 명의 이스트시큐리티의 공개용 보안 소프트웨어인 알약에는 랜섬웨어 탐지 기능을 강화한 업데이트가 실시됐다. 그 과정 중 일부 PC에서는 랜섬웨어 탐지 오류로 인한 화면 멈춤 오류가 발생했다. 오전 11시 30분 랜섬웨어 탐지 기능을 강화한 업데이트를 실시하고 오류 발견 후 오후 1시 30분경 즉각적으로 업데이트를 중지했으며 당일 오후 11시 30분 서비스 정상화를 이뤘다. 하지만 알약 오류로 인한 PC 먹통 사태의 여파로 무료 소프트웨어를 이용하던 자영업자, 프리랜서 등이 업무에 차질을 빚은 것으로 나타났으며 집단 소송 움직임도 일었다. 정상원 대표는 8월 31일 SNS를 통해 "알약이 국내 사용자분의 PC 환경에 많은 영향을 줄 수 있기에 출시 전 안정성을 확인하는 자동화 빌드 및 테스트 출시 프로세스가 구축되어 있으나 이번 오류를 잡아내지 못하였습니다. 이번 일을 계기로 기존 테스트 프로세스를 전면적으로 재검토하여 더욱 안정적인 서비스를 제공할 수 있도록 만전을 가하겠습니다"라고 밝혔다. 이스트시큐리티는 사건이 발생하고 5일이 지난 9월 5일 재발 방지 방안을 발표했다.

알약 오류 사태 이후 이스트시큐리티가 발표한 재발 방지 방안

① 랜섬웨어 테스트 프로세스 강화
- 다양한 사용자 환경에서 충분한 검증이 될 수 있도록 랜섬웨어 탐지 기술 적용 전, 사전 검증 체계

② 전략적 배포 프로세스 개선
- 다양한 조건별 배포 프로세스 정교화
- 배포의 전 과정을 상세하게 모니터링하고 통제할 수 있는 배포 시스템 고도화

③ 오류 조기 발견/차단 시스템 고도화
- 랜섬웨어 탐지 오류를 포함한 오작동을 신속하게 인지하고 선제적 대응을 위한 통계적 모니터링 시스템 개선
- 수집된 오류의 범위와 수준에 따른 자동화된 차단 시스템 수립

④ 실시간 대응 시스템 개선
- 랜섬웨어 차단 오류 방지를 위한 조기 발견/차단 시스템과 딥러닝 기반의 악성코드 위협 대응
- 솔루션 쓰렛 인사이드(Threat Inside) 연계, 최단 시간 내 정상 엔진 복구를 위한 대응 구조 강화

최근에는 인공지능, 블록체인, 메타버스 등 소프트웨어 기반의 다양한 신기술이 등장하면서 디지털 기술의 잠재적 위험원들도 다양화, 다변화되고 있다. 가령 욕설이나 왜곡된 정보로 학습된 인공지능 챗봇은 사람과의 대화에서도 편향되거나 문제의 소지가 있는 대답을 자동적으로 내놓을 수 있다. 이것은 물리적이거나 신체적 피해는 주지 못하지만 잘못된 규범, 사회적 인식을 심어줄 수 있으며 왜곡된 정보 제공으로 잠재적인 문제를 일으킬 소지가 다분하다. 여기에는 코딩의 오류, 보안 이슈, 통신망 장애 등과 같은 문제는 개입되지 않으나 인공지능에 어떠한 학습용 데이터를 사용했는지가 문제 된다. 인공지능 신뢰성 이슈는 기계학습이 핵심적인 소프트웨어 기술로 부상함에 따라 데이터의 품질, 편향성, 공정성 관리가 새로운 디지털 위험원 관리의 영역까지 고려되어야 함을 시사한다.

블록체인의 사건·사고도 끊이지 않고 있다. [6] 카카오 블록체인 자회사인 그라운드X가 개발한 퍼블릭 블록체인 플랫폼 클레이튼은 2021년 11월 13일 24시간 이상 작동이 멈췄다. 이 사고로 클레이튼에 기반한 대체불가토큰(NTF)의 거래가 불가능해졌고 클레이, 위믹스, 보라 등 클레이튼 기반 코인의 입출금이 중단되었다. 사고의 원인으로 메모리 공유 관련 버그가 지적되었다.[7] 블록체인 기반의 암호화폐, NFT에 대한 해킹도 문제다. 한 블록체인 관련 기업이 발간한 보고서에 따르면 2021년 디지털 자산 불법 거래 금액이 한화로 약 16조 8,000억에 이르며 이 숫자는 2020년 대비 79% 이상 증가한 것이다. 2022년 3월 29일에는 NFT 기반의 P2E(Play to Earn)의 대표적 사례인 액시 인피니티(Axie Infinity)에서 약 620억 달러 규모의 암호화폐가 유출되는 사건이 발생했다. 블록체인의 단점인 데이터 전송 속도, 수수료 등을 개선하기 위해 사용하는 사이드체인에서 보안 사고가 발생한 것이다.

2022년 1월에는 글로벌 NFT 거래소인 오픈시(OpenSea)에서도 버그를 악용해 2억짜리 NFT가 200만 원에 거래가 된 사고가 발생했다. 공격자들은 오프체인에 남아 있던 과거 등록된 저가의 NFT 가격을 불러와 블록체인 유효성 검증을 통과했고 온체인으로 전송했다. 블록체인에 기록된 데이터를 직접 위변조하는 것이 사실상 불가능하기 때문에 데이터를 전송하는 단계에서 공격이 이뤄지고 있다.[8]

최근 주목 받고 있는 메타버스 역시 디지털 안전 문제에서 자유롭지 않다. 오히려 현실과 가상을 넘나들며 다양한 정보 보안, 해킹, 디지털 오류의 위험에 노출되어 있다. 메타버스 기기, 네트워크 인프라에 대한 기존 사이버 보안의 위험을 그대로 내포한 채 신기술을 접목하면서 관련 기술 위험도 고스란히 동반하고 있다. 가령 메타버스의 가상공간은 빠르게 NFT 기반 토큰 이코노미를 수용하면서 블록체인, NFT의 잠재적 위험성에 노출되었으며 가상공간 속 인공지능 기술도 여전히 해결되지 않은 공정성, 신뢰성, 편향성 이슈를 가지고 있다. 나아가 가상공간이라는 새로운 사회적 환경에서 다양한 사회적 범죄가 발생한다. 사이버 공간에서의 디지털 캐릭터, 아바타에 대한 성범죄가 대표적이다. 아바타를 대상으로 성적 수치심을 일으키는 표현이나 스토킹, 음란행위 등에 대한 처벌 요구가 높아지고 있다.[9]

6) 아주경제(2022.1.25.), "NFT거래소 버그로 2억짜리 NFT가 200만원에 팔렸다" https://japan.ajunews.com/view/20220125080343716
7) ZDNET(2021.11.15.), "카카오 블록체인 '클레이튼' 먹통 사고" https://zdnet.co.kr/view/?no=20211115183224
8) 아주경제(2022.4.3.), "암호화폐 NFT 노리는 해킹 증가 블록체인은 안전할까?" https://www.ajunews.com/view/20220403073351876
9) 매일경제(2022.8.1.), "메타버스서 아바타 음란행위 스토킹 시 징역형" https://www.mk.co.kr/news/it/view/2022/08/675726/

종합적인 국가 디지털 안전 정책 필요

디지털 기술은 점점 촘촘하게 우리 사회와 국가 저변에 확장되고 있다. 문제는 디지털 기술에서 발생하는 사소한 오류나 사고가 개인의 신체적, 정신적 피해는 물론 사회와 경제시스템에 큰 타격을 주는 재앙으로 비화될 수 있다는 점이다. 데이터 오류, 소프트웨어 품질, 안전한 개발, 사이버 공격과 위험으로부터 보호, 개인정보 유출, 네트워크 장애, 인공지능의 편향성과 공정성 이슈, 데이터센터 화재 등 각종 디지털 안전을 위협하는 요인으로부터 사전 예방, 신속 대응, 사후 조치의 유기적 연계가 필요하다.

한국의 개인정보 보호 수준은 유럽의 일반데이터보호규정(GDPR)에 준하는 인정을 받고 있다. 초기 인터넷의 성장 단계에서부터 오랜 시간 관리되고 발전된 결과라 할 수 있다. 인터넷을 통한 각종 해킹, 시스템 공격, 사용자 정보 유출, 피싱, 스미싱 등 사기성 정보를 통한 정보 탈취, 악성코드를 심어 시스템을 마비시키고 금전적 대가를 요구하는 랜섬웨어에 이르기까지 문제는 날로 커지고 있다. 특히 랜섬웨어가 심각한 문제로 부상하고 있다. 2021년 정보보호 실태에 따르면 기업 침해사고 중 47.7%가 랜섬웨어 공격으로 나타났다. 전 세계적으로도 2021년 기준 랜섬웨어 피해액이 6억 2,000만 달러를 넘어 2016년 대비 25배 이상 증가했다. [10] 해킹, 악성코드, 랜섬웨어, 디도스 공격 등 사이버 보안 이슈는 앞으로도 점차 다양화, 지능화될 것으로 예상된다.

한편 외부 공격에 무관하게 소프트웨어 자체적, 기능적 안전성과 오류의 최소화를 추구하는 SW품질 및 안전 확보도 중요한 분야로 떠오르고 있다. 소프트웨어 사고에서는 단순한 시스템 오류가 큰 피해로 이어진 경우가 많았음을 앞서 살펴봤다. 설계, 개발 단계에서의 다양한 시나리오를 가정한 안전 점검과 테스팅을 이룰 수 있는 개발 환경과 개발 문화의 정착이 요구된다. 우리 정부는 2020년 '소프트웨어 진흥법'을 개정하면서 소프트웨어 안전 확보를 법으로 규정하였으며 '소프트웨어 안전 확보를 위한 지침'을 고시로 제정해 소프트웨어 안전 확보를 법적 기반으로 마련해 두었다. 하지만 소프트웨어의 안전 개념, 안전 관리 소프트웨어의 대상 지정 등 세부적인 관리 계획 마련이 필요하다.

10) 체이널리시스(2022.5.2.), "2022 가상자산 범죄 보고서" https://www.concert.or.kr/bbs/board.php?bo_table=newsletter&wr_id=498

인공지능, 블록체인, 메타버스 등 신기술이 품고 있는 잠재적 기술 위험을 빠르게 인지하고 대처하는 것도 필요하다. 특히 인공지능의 신뢰성 문제는 앞으로 국가의 디지털 안전 확보에 필수적이다. 학습 데이터를 기반으로 의사결정의 자동화를 통해 다양한 언어적, 시각적, 지능적 판단을 하는 인공지능은 점차 우리 사회의 핵심 디지털 기술 기반으로 자리매김하고 있다. 최근 윤리적 인공지능, 신뢰할 만한 인공지능 구현을 위한 국내외 정책적 노력이 활발한 이유가 이러한 영향력에 대한 우려가 커지고 있음을 반증한다. 인공지능이 학습의 원천으로 삼고 있는 데이터의 무결성, 공정성에 대한 검증이 이뤄지고 블랙박스 영역으로 남아 있는 인공지능 모델에 대한 투명성, 설명가능성을 높이기 위한 기술적 노력들이 이뤄지고 있다. 나아가 인공지능의 오작동으로 인한 피해 발생 시 책임 소재를 명확히 하고자 하는 논의도 활발하다. 가령, 인간의 개입 없이 스스로 작동하는 자율주행차의 사고 발생 시, 사고 발생 원인을 소프트웨어의 오류나 결함에서 찾으려는 노력을 통해 피해 발생의 책임 소재를 좀 더 명확히 할 수 있다면 소비자의 걱정을 더욱 불식시켜 자율주행차의 확산을 좀 더 가속화시킬 수 있을 것이다.

또, 한 가지 살펴볼 것은 무료 소프트웨어의 피해보상 문제다. 통상 무료 소프트웨어 버전의 경우 이용약관에 면책 규정이 포함된 경우가 많아 이 경우에는 보상받기 어렵다. 또한 이용자가 피해 규모를 입증하기도 모호하고, 개발사의 과실과 고의로 인해 손해가 발생했음을 판단하는 것도 어렵다. 기업이 사과문을 게시, 긴급 수동 조치를 공지하고 재발 방지 대책을 내놓고, 사용자 불편을 해소하는 후속 조치도 적극적으로 한다면 재판에 참작이 될 것이다. 대부분의 플랫폼 서비스가 프리미엄(Freemium) 전략을 사용해 가입자를 유치한 후 유료 상품으로 전환하는 전략을 택하고 있어 무료 서비스의 피해보상에 대한 고민도 필요하다. 페이스북, 구글 등 플랫폼의 접속 장애가 나더라도 현재로서는 무료이기 때문에 별도의 피해보상이 없다는 입장이다. 소프트웨어의 기업 전략이 무료 소프트웨어의 배포와 이를 통한 유료화 전환, 고객 락인(Lock-In)이기 때문에 무료 소프트웨어가 문제를 일으켰을 시 단순 민사상의 문제로만 치부하는 것이 공익에 부합하는지는 보다 면밀한 검토가 필요하다.

우리는 산업화 사회를 거치면서 각종 재난·재해를 경험하고 있다. 대규모 자연재해가 아니라면 대형 사고라 하더라도 피해는 국지적이었다. 하지만 촘촘하게 연결된 디지털 기술이 사회 기반으로 자리매김한 지금은 국지적 문제가 국가적 문제, 나아가 글로벌 문제로 걷잡을 수 없이 빠르게 커질 수 있다. 소위 디지털 블랙아웃 또는 디지털 팬데믹이 수시로 나타날 수 있음을 염두에 두어야 한다. 이를 위한 더욱 강력하고 촘촘한 국가적 차원의 디지털 안전 확보가 시급하다.

디지털 안전 확보를 위해 3단계 즉 예방, 신속한 조치, 사후 대응 단계에서 좀 더 철저한 관리 체계가 필요하다. 사전적으로 소프트웨어 개발 시 오류를 최소화하고 각종 사이버 공격으로부터 강건하며, 문제가 발생하더라도 회복력(Resilience)을 갖춘 시스템을 개발할 수 있는 기술적 노력이 필요하다. 이후 사고의 신속한 대응과 사건 발생 후 철저한 원인 조사를 통해 재발을 방지하는 법적 기반, 거버넌스 체계 마련이 시급하다. 특히 디지털 안전은 전 분야, 전 부처의 협력이 필요하다. 자율주행차, 의료기기, 원자력, 건축물, 금융 시스템, 교통, 물류, 상거래, 커뮤니케이션 등 어느 것 하나 소프트웨어로 작동하지 않는 영역이 없다. 소프트웨어 융합과 디지털 기술에 대한 의존도가 점차 높아지고 있다. 이에 따라 범부처 거버넌스 체계에서 전 산업 분야의 소프트웨어 기술 역량을 높이며, 사고 대응과 사후 원인 조사 및 조치가 이뤄지는 정책 마련이 필요하다. 안전한 디지털 세상, 나아가 디지털 선진국가의 도약은 촘촘한 디지털 안전에서 시작된다. 안전에는 경계가 없다!

< 참고문헌 >

- 매일경제(2022.3.11.), " '소프트웨어 결함' 자율주행차 사고나면…완성차 CEO가 중대법 처벌받을 수도", https://www.mk.co.kr/news/society/view/2022/03/192768/
- 매일경제(2022.8.1.), "메타버스서 아바타 음란행위 스토킹 시 징역형" https://www.mk.co.kr/news/it/view/2022/08/675726/
- 아주경제(2022.4.3.), "암호화폐 NFT 노리는 해킹 증가 블록체인은 안전할까?" https://www.ajunews.com/view/20220403073351876
- 아주경제(2022.1.25.), "NFT거래소 버그로 2억짜리 NFT가 200만원에 팔렸다" https://japan.ajunews.com/view/20220125080343716
- 조선일보(2022.7.04.), "獨, 테슬라에 리콜 명령...전세계 6만대가 '소프트웨어 결함", https://biz.chosun.com/international/international_general/2022/07/04/4DNKIUOQFRA3TIG47GODUZL4UY/
- 중앙일보(2022.7.3.), "日 4000만명 휴대전화 먹통 대란…교통·금융·물류 마비됐다", https://www.joongang.co.kr/article/25083967#home,
- 체이널리시스(2022.5.2.), "2022 가상자산 범죄 보고서" https://www.concert.or.kr/bbs/board.php?bo_table=newsletter&wr_id=498
- 한경(2021.11.2.), "테슬라, 소프트웨어 결함으로 美서 1만2천대 리콜" , https://www.hankyung.com/international/article/202111022025Y
- IT조선(2018.11.22.), "AWS 장애로 국내 IT 서비스도 마비…'클라우드'가 뭐길래", https://it.chosun.com/site/data/html_dir/2018/11/22/2018112201040.html
- TechM(2022.7.14.), "日 최악의 통신장애 일으킨 통신사 KDDI "86시간 멈췄다...3915만 회선 피해"", https://www.techm.kr/news/articleView.html?idxno=99361
- ZDNET(2021.11.15.), "카카오 블록체인 '클레이튼' 먹통 사고" https://zdnet.co.kr/view/?no=20211115183224