정 보 보 호 학 회 지
제 31 권 제5호, 2021. 10

코로나19에 따른 사이버위협 및 대응기술 동향 (보안관제와 침해대응 서비스를 중심으로)

이 윤 수*, 문 형 우**, 박 건 량**, 김 태 용**, 송 중 석***

요 약

코로나19 팬데믹은 현실뿐만 아니라 사이버 공간에도 지대한 영향을 미쳤다. 재택근무와 비대면(온라인) 회의 뿐만 아니라 온라인 게임/쇼핑과 스트리밍 서비스 등과 같이 네트워크를 활용한 서비스의 이용자가 급증하였으며, 이로 인해 사이버 공간은 더욱 활성화되고 확장되었다. 그러나 사이버 공간의 확장은 이를 대상으로 하는 사이버 공격들도 함께 증가시켰으며, 그 피해규모 또한 증가하고 있어 대응방안 마련이 매우 시급한 상황이다. 본 논문에서는 코로나19 팬데믹 영향에 따른 사이버공격 동향을 살펴보고, 실제 사이버위협을 탐지・대응하는 보안관제, 침해대응 실무현장에서 발생하는 사이버위협을 분석해 사이버위협 동향 변화를 확인해 본다. 또한, 대응기술로서 인공지능과 설명가능 인공지능 기반 정보보호 연구·개발에 대해 소개한다.

Ⅰ. 서 론

코로나19 팬데믹은 사람들의 일상생활을 대면 중심에서 비대면 중심으로 크게 변화시켰다. 즉, 전염병 감염 우려로 면담, 회의, 출・퇴근과 같은 대면 방식 활동이 불가능해지면서 화상회의 및 원격근무 등 비대면 방식 활동의 수요가 세계적으로 증가하였다. 이로 인해 사이버 공간은 일상생활 전반으로 확장되었으며, 사람들은 사이버 공간을 활용함으로써 코로나19 감염의 위험에서 벗어나 교육, 업무 등 활동을 할 수 있게 되었다.

하지만, 사이버 공간 확장과 함께 이를 노리는 사이버 공격 또한 급증하고 있다. 한 설문조사에서는 글로벌 기업 76%가 코로나19 팬데믹으로 사이버공격이 급증했다 답했고, 대다수 응답자가 원격근무가 주요 요인이라고 지적했다[1]. 특히, 원격 근무자들이 이용하는 이메일, 웹 필터 등에 대한 공격 증가로 스피어 피싱 공격은 전년 대비 7배 증가하였고[2], SSL-VPN(Fortinet社)에 대한 공격은 2021년 1분기에 1,916%로 급증 했으며[3], 코로나19를 미끼로 한 피싱, 스팸, 랜섬웨어 등의 공격도 증가했다[4]. 이에 사이버공격이 전 세계적으로 유행한다는 뜻의 사이버 팬데믹이 올 것이라는 전망도 나오고 있다[5].

뿐만 아니라 사이버공격의 범위와 대상이 일상활동 전반으로 확대되고, 공격방법도 크게 고도화되었다. 피싱 공격은 문자나 음성 메시지와 같은 다양한 채널을 사용하고 백신 개발에 관한 뉴스도 활용한다. 공급망에 대한 공격이 증가하고, 지정학적 긴장 상태에 따른 사이버공격 양상의 변화도 목격되고 있다. 또한, 인공지능(AI)과 머신러닝(ML) 활용을 통해 피싱 등의 공격은 더 정교해지고 있다.[6].

이러한 코로나19 팬데믹에 의한 사이버위협 변화 상황에 대해서, 세계 각국은 대응책을 준비하고 있다. 미국은 연방기관은 원격근무 시 발생하는 사이버안보 이슈에 대한 가이드라인을 발표했고, 유럽연합은 근무 형태 디지털화와 디지털 인프라에 대한 의존 확대를 반영해 사이버안보 전략을 개정했으며, 한국도 국가적 대응차원에서 비대면 시대의 위험에 대한 국가 정보보안 기본지침 관련 내용 개정, 원격업무 통합매뉴얼 발표 등 재택근무, 원격서비스 확산에 대비하고 있다[7].

이런 상황에서 팬데믹에 의한 사이버위협동향 및 영향을 파악하고 대응방안을 마련하는 것은 매우 시급

본 연구는 한국과학기술정보연구원(KISTI) ‘인공지능 기반 공동활용 보안체계 구축[K-21-L02-C03]’ 과제의 지원으로 수행되었습니다.
* 한국과학기술정보연구원 과학기술사이버안전센터 (선임연구원, zizeaz@kisti.re.kr)
** 한국과학기술정보연구원 과학기술사이버안전센터 (연구원, hwmoon@kisti.re.kr, gypark@kisti.re.kr, skytaeyong@kisti.re.kr)
*** 한국과학기술정보연구원 과학기술사이버안전센터 (책임연구원, song@kisti.re.kr)

한 현안이다. 본 논문에서는 팬데믹의 영향에 따른 사이버공격 동향을 살펴보고, 실제 사이버위협을 탐지 및 대응하는 보안관제, 침해대응 실무현장에서 발생하는 사이버위협을 분석함으로써 팬데믹 영향에 의한 사이버위협 동향 변화를 확인한다. 또한, 효과적 대응책이 될 수 있는 연구·개발에 대해 소개한다.

Ⅱ. 코로나19에 따른 사이버공격 동향

2.1. 원격근무 대상 공격

코로나19 팬데믹에 의한 재택 원격근무로의 전환은 사이버공격의 양상을 크게 변화시켰다. 감염병 예방 목적의 사회적 거리두기 실천을 위해 온라인 활동이 장려되면서 비대면 서비스가 급증하고 원격접속 대상 사이버공격 또한 급격히 증가했다. 원격근무자의 수가 크게 증가하면서 기관이나 기업들은 늘어난 관리범위를 감당하지 못해 데이터 침해에 취약해졌고, 직원들은 적절한 보안가이드를 제공 받지 못하고 달라진 업무방식에 적응하기 바빠 보안에 소홀해졌다. 전례 없이 달라진 원격근무 일상화 등의 업무 방식이 새로운 형태의 사이버위협 리스크를 대두시켰다.

첫째로, 클라우드 서비스를 노리는 공격이 증가했다. 코로나19 이후 원격근무가 빠르게 도입됨에 따라 클라우드 기반 서비스・인프라에 대한 수요가 급격히 증가했다. 클라우드 서비스는 확장성, 효율성 및 비용절감과 같은 다양한 이점을 제공하지만 잘못 구성된 스토리지, 잘못된 아이디 (ID) 및 액세스 관리 제어, 안전하지 않은 애플리케이션 프로그래밍 인터페이스 (API), 데이터 손실, 침해 및 누출의 위험으로 인해 사이버공격에 매우 취약한 실정이다[8].

둘째로, 홈 네트워크를 노리는 공격의 증가가 했다. 재택 원격근무의 증가로 기관・기업의 네트워크가 집에까지 확대됨에 따라 기업 정보를 노리는 해커가 가장 보안이 취약한 홈 네트워크 및 PC를 노릴 위험이 커졌다. 홈 네트워크는 기관 보안정책의 영향을 받지 않을 위험이 크기 때문에 취약한 무선 네트워크, IoT 기기, PC 등을 악용한 해커의 위험에 무방비로 노출될 위험이 큰 실정이다[9].

셋째로, 내부자 위협이 증가했다. 급하게 재택 원격근무 환경 구축이 요구되면서 기관・기업의 보안관리자들은 보안대책을 충분하게 확보하지 못한 상태에서 개인용 기기 사용이나 생산성을 높이기 위한 협업 도구(Slack, microsoft teams, zoom)의 허용을 요구받고 있다. 이는 데이터 보안 및 규정 준수 등의 문제를 야기하고 내부자 위험을 높이는 원인이 된다.

2.2. 사회공학적 공격

코로나19 팬데믹 상황을 악용한 피싱과 랜섬웨어 등 사람들의 취약점을 공략하는 사회공학적 공격이 급증했다. 감염병 관련 정보를 제공하는 사이트로 위장한 사이버공격이 증가했고 의료, 통신, 기술, 금융, 교육 분야에서 코로나19 관련 내용을 미끼로 한 랜섬웨어, 피싱, 스캠 공격이 크게 증가했다[10].

해커들은 랜섬웨어 감염시 대가 지불 가능성이 높은 병원, 의료 센터 및 공공기관을 주요 공격대상으로 삼고 있으며, 감염된 링크나 첨부 파일이 포함된 이메일, 손상된 직원 자격 증명 또는 시스템의 취약성을 이용한다[11]. 또한, 원격근무 수요가 증가하는 것을 활용하기 위해 새로운 악성 프로그램을 개발했다. 팬데믹 이전에는 신규 악성 프로그램을 활용한 해킹의 비율이 약 20%였는데, 팬데믹 시기에는 35%까지 증가했다[12]. 해커들은 악성 프로그램, 스파이웨어 및 트로이 목마를 대화형 코로나 바이러스 지도 및 웹 사이트에 포함시키고, 사용자가 컴퓨터나 모바일 장치에 악성 프로그램을 다운로드하는 링크를 클릭하도록 유도하고 있다.

개인이나 기업, 기관 특성을 사전에 파악하여 관심을 끌만한 주제로 이메일 등을 발송하는 ‘스피어 피싱(spear phishing)’ 공격이 자주 활용되고 있으며[13], 코로나19 백신과 관련된 피싱도 활발해 예방접종 예약 이메일로 위장한 피싱 공격과 제약회사와 백신 유통업체에 대한 공격이 급증하고 있다[8].

스캠(scam)도 코로나 상황에서 자주 발생하고 있다. 2020년 4월 미국 연방수사국(FBI)은 코로나19 대응에 필요한 마스크 등의 보호 장비나 기타 물자를 구입하는 자치 단체를 대상으로 하는 비즈니스 이메일 침해(BEC) 스캠이 증가하고 있다고 경고했다. 스캠메일을 받은 단체는 거래대상 회사의 계좌가 아닌 해커의 계좌로 대금을 입금함으로써 금전적 손실을 입는다.[14] 코로나의 영향력을 고려하면 앞으로도 이러한 공격은 해가 거듭될수록 커질 것으로 보인다.

2.3. 자동화 공격

해커들은 인공지능을 공격 자동화에 활용하고 있다. 해커들은 비용이 적게 들고 더 자동화되며 더 쉽게 사이버공격을 실행할 수 있게 된다. 인공지능과 머신러닝을 사용하여 오래된 악성 프로그램의 새로운 변형을 만들고, 취약성을 찾고, 암호를 추측하고, 음성을 복제한다. 인공지능이 제어하는 자동화 시스템은 시스템과 네트워크를 테스트하여 악용될 수 있는 새로운 취약점을 검색할 수도 있다. 이 기술은 또한 사회공학적 공격의 성공률을 크게 높일 수 있다. 향후에는 해커가 인공지능을 조작해 새로운 스마트 악성 혁신을 설계할 것으로도 예상된다[9].

특히, 코로나 이전에도 전 세계 사이버 공격의 90%에 활용될 정도로 영향력이 컸고, 코로나 이후에는 더욱 기승을 부리고 있는 피싱은 향후 자동화된 윈도우 피싱 공격이 감염병, 정치, 경제를 둘러싼 공포를 넘어설 것으로 예상된다. 해커들은 악성 첨부파일, 하이퍼링크로 피싱 이메일을 만드는 데 많은 시간을 할애했으나 수작업 과정을 자동화하기 위해 인공지능과 머신러닝을 사용함에 따라 이러한 경향은 변화할 것으로 보인다. 예를 들어, 고급 피싱 도구 키트를 사용하는 국가 지원 해커는 소셜 미디어 네트워크 및 조직 웹 사이트를 검색하여 엄청난 양의 데이터를 얻을 수 있다. 이 데이터를 사용하면 각 피해자에게 맞춤화된 신뢰할 수 있는 콘텐츠를 사용하여 대량의 윈도우 피싱 공격을 시작할 수 있다. 이 자동화된 프로세스는 해커가 한 번에 보낼 수 있는 윈도우 피싱 이메일의 수를 증가시켜 성공 가능성도 높일 것이다.

Ⅲ. 보안관제 및 침해대응 데이터 분석

3.1. 보안관제 데이터 분석

국내에서는 국가·공공기관의 정보통신망에 대한 사이버공격을 실시간으로 탐지·분석하여 즉각 대응조치를 할 수 있도록, 총 42개의 부문보안관제센터를 운영하고 있다[15].

국내 부문보안관제센터 중 하나인 과학기술사이버안전센터(S&T-CSC)는 지난 2005년부터 과학기술 분야 연구·공공기관 62개에 대한 보안관제 및 침해대응 업무를 전담하고 있으며, 본 논문에서는 과학기술

〔표 1〕 최근 9년간 보안이벤트 수집 및 침해대응 현황

구분	보안이벤트	침해대응
2012년	1,165,780,019	2,093
2013년	4,457,431,724	2,611
2014년	7,669,366,325	2,329
2015년	9,299,910,213	2,423
2016년	5,142,182,012	1,671
2017년	6,782,338,158	863
2018년	5,826,722,829	438
2019년	2,013,667,894	503
2020년	3,799,502,860	596
계	46,156,902,034	13,527

사이버안전센터를 통해 수집·분석 및 대응되는 통계를 중심으로 설명한다.

[표 1]과 같이 과학기술사이버안전센터에서는 최근 9년간 약 460억건 이상의 사이버위협정보를 수집하여 총 13,527건의 침해대응 기술지원을 수행하였다.

특이한 점은 2015년까지 지속 상승하던 보안이벤트 개수가 2016년, 2019년을 기점으로 급격히 감소한 것이다. 자체적인 분석 결과, 2016년은 국가·공공기관 웹사이트의 암호화 미조치를 언론에서 문제제기한 2015년 전후로 국내 웹사이트에 대한 HTTPS 및 SSL 적용이 급증하였기 때문인 것으로, 2019년은 11월에 발생한 코로나19 팬데믹에 의해 HTTPS를 사용하는 화상회의, 원격근무 등의 증가가 원인인 것으로 분석하고 있다.

[표 2]는 코로나19 팬데믹이 발생한 최근 3년간 과학기술사이버안전센터에서 처리한 침해사고를 5가지 유형(경유지 악용, 단순침입시도, 웜·바이러스, 자료훼손/유출, 홈페이지 ·변조)으로 구분·분류했다(2021년은 1~9월 데이터 기준).

년도별 침해사고 총 건수는 2019년 503건, 2020년 596건, 2021년 566건, 월 평균 건수는 각각 42건, 50건, 63건 수준으로 매년 지속적으로 증가한 것으로 나타났다.

특히, 단순 침입시도 유형은 2019년 까지는 거의 발생하지 않다가 2020년부터 급격히 발생한 침해사고 유형으로, 전체 침해사고에서 차지하는 비중이 2020년 29%, 2021년 40%로 매우 높다. 공격유형은 전체(2020년, 2021년) 침해사고 399건 중 시스템 취약점 165건, 웜·바이러스 153건, 웹 취약점 53건, 스캐닝 28건으로 탐지된 이벤트명 및 패킷에 대한 자체 분석

〔표 2〕 최근 3년간 침해사고 대응 현황

침해 유형	2019	2020	2021 (~9월)
경유지 악용	16	29	7
단순침입시도	0	173	226
웜•바이러스	289	218	216
자료훼손/유출	195	174	117
홈페이지 위/변조	3	2	0
총계	503	596	566

결과, 시스템 취약점, 웜·바이러스, 스피어 피싱, 스팸메일, 경유지 접근 등이 주요 원인으로 밝혀졌다.

자료훼손/유출 유형의 공격은 각각 195건, 174건, 117건으로 2017년 92건, 2018년에 76건에 비해 많이 발생하였다. 이를 미루어 해당 유형의 공격은 2019년 발생한 코로나19 팬데믹의 영향으로 증가했다 추정해 볼 수 있다.

또한, 최근 3년간 침해사고 중 코로나19 팬데믹에 의한 증가가 예상되는 랜섬웨어, 악성메일, VPN 공격을 [표 3]과 같이 정리한 결과, 최근 3년간 총 건수는 2019년 170건, 2020년 183건, 2021년 129건, 월 평균 건수는 각각 14건, 15건, 14건 수준으로 매년 유사한 수준으로 발생했다. VPN 대상 침해사고는 2019년 6건, 2020년 13건, 2021년 57건으로 매년 2~4배의 급격한 증가세를 보였다.

〔표 3〕 최근 3년간 코로나19 관련 침해사고 현황

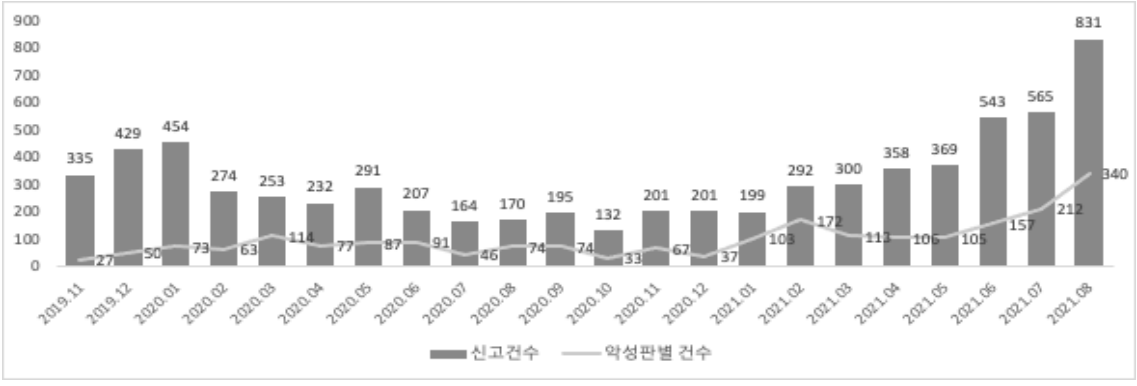
침해사고 유형	2019	2020	2021 (~9월)
랜섬웨어	11	4	3
악성메일	153	166	69
VPN	6	13	57
총계	170	183	129

3.2. 침해대응 데이터 분석

과학기술사이버안전센터에서는 대상기관 사용자들이 해킹에 악용된 것으로 의심되는 이메일을 신고하면 이를 분석해 주는 “악성의심메일 분석 서비스”를 제공하고 있다.

[그림 1]은 코로나19 팬데믹이 시작된 2019년 11월부터 2021년 8월까지 월별 해당 서비스 신고건수 및 악성으로 판별된 건수이다. 월별 신고 건수는 서비스가 시작된 2019년 평균 382건 으로 높았다가, 2020년 약 231건으로 낮아지고 2021년 약 432건으로 다시 높아지는 추세를 보인다. 2019년의 높은 평균은 서비스가 시작되는 시점에 신청이 몰려 발생한 것으로 보이며, 이후 소강상태를 보이다가 악성메일의 증가로 인해 2021년 6월부터 급격한 증가세를 보인 것으로 판단된다.

최근 3년의 평균 악성판별 건수는 39건, 70건, 164건 으로 모두 지속 증가했으며, 연도별 신고 대비 악성판별 건수의 비율도 10%, 30%, 38%로 꾸준히 증가해 신고대비 사고의 비율이 증가하고 있음을 확인할 수 있다. 특히, 2021년 은 월 평균 신고건수, 악성판별 건수가 전년대비 약 2배 증가하였고, 월별 악성판별 건수도 모두 100건 이상으로 매우 높아 악성메일을 활용한 해킹이 현저히 증가했음을 확인할 수 있다.



〔그림 1〕 악성의심메일 분석 서비스 현황(2019.11~2021.08) - 악성메일 의심신고 건수 및 악성판별 건수

Ⅳ. 대응기술 소개

코로나19 팬데믹에 따른 사이버위협의 변화는 원격 접근 허용에 의해 증가하는 보안접점 문제와 사이버공격 지능화에 대한 대응방안 부재로 요약될 수 있다. 급변한 사이버위협에 효과적으로 대응하기 위해서는 대응기술도 지능화 및 자동화 되어야 한다. 뿐만 아니라 발생한 침해사고의 대응조치를 수행하기 위해서는 도출된 결과에 대한 원인을 규명할 수 있어야 한다. 본 장에서는 이러한 방향에서 연구되고 있는 인공지능 및 설명가능 인공지능 기반 정보보호 기술을 소개한다.

4.1. 인공지능 기반 정보보호 기술

인공지능의 성능과 발전속도가 보여주는 가능성에 힘입어, 전세계는 인공지능을 인류, 국가의 핵심역량으로 분류하고 장기적 전략을 수립하고 있다. OECD는 2019년 OECD AI권고안을 통해 신뢰 가능한 인공지능의 주요 구성요소 5가지(포용 및 지속 가능, 인간중심, 투명성 및 설명가능성, 견고성 및 안전성, 책임완수)를 제시했고[16], 미국 인공지능국가안보위원회(NSCAI: National Security Commission on Artificial Intelligence)는 2021년 3월 AI에 대한 미국의 국가종합전략 수립을 제안하는 보고서를 발간하며, 또다른 AI강국인 중국을 견제하기 위해 5개 영역(거버넌스, 인재양성, 지식재산, 반도체, 기술동맹) 중심의 국가역량 총동원을 촉구했다[17].

우리나라도 OECD, 미국 등과 AI발전에 협력하며 AI혜택을 극대화 하고 위험 및 부작용을 최소화함으로써 사람 중심의 인공지능 강국 실현을 위해 2021년 5월 「신뢰할 수 있는 인공지능 실현 전략」을 수립하고 3가지 전략(신뢰 가능한 인공지능 구현 환경 조성, 안전한 인공지능 활용을 위한 기반 마련, 사회 전반 건전한 인공지능 의식 확산)을 제시하고[18], K-사이버 방역 정책을 통해 AI 기반 사이버 보안위협 대응체계 구축을 핵심 국정과제로 선정하고 과학기술 발전이 선도하는 4차 산업혁명을 위한 역기능 대응방안으로 고려하고 있다

전 세계 인공지능 보안 시장은 2020년 50.8억 달러(한화 약 5조 7,125억 원)이며, 연평균 18.64% 성장할 것으로 전망된다. 국내 보안관제 전문기업들은 서비스 차별화와 시장확대를 위해 AI 기술적용을 적극 추진하고 있다. 대표적 사례로, ADT캡스(구 SK인포섹)의 “Secudium”은 빅데이터 기반의 인텔리전스 DB를 머신러닝 기술에 접목해 사이버위협 실시간 탐지에 활용하고 있으며, 시큐아이의 “GOVERNANCEMAX”는 IBM Watson을 활용한 인지기반 AI분석을 잠재적 위협 탐지에 사용한다. 이글루시큐리티의 “D-Security”는 SIEM과 AI기반 보안관제체계를 연계, 지도학습 기법을 활용해 고위험군의 이벤트를 선별한다[19, 20]. 또한, 정보보안 전문기업들도 AI 기술을 다양한 분야에 적용하여 상용 솔루션 개발을 추진 중이다. 머신러닝 엔진을 장착한 국내 첫 AI백신임을 강조하는 세인트시큐리티의 “MAX”나 머신러닝 기술을 적용해 단순반복작업의 획기적인 감소를 주요 특징으로 하는 파수닷컴의 “스패로우”가 대표적인 사례이다[21, 22].

해외의 경우, 소규모 신생기업을 중심으로 AI 기반 보안기술을 보유한 업체들이 두각을 나타내고 있다. 대표적인 사례로는 영국의 벤처기업인 “다크트레이스(DarkTrace)”가 있다. 동명의 자사 솔루션 다크트레이스에 네트워크상의 시스템 별 트래픽에서 정상모델을 학습함으로써 비정상행위 및 위협을 탐지하는 기술을 적용하였으며, 삼성SDS를 포함한 다수의 기업들로부터 기술 우수성을 인정받아 투자를 유치했다. 미국의 신생기업인 “크라우드스트라이크(CrowdStrike)”는 AI 기반 보안위협 대응 솔루션을 보유하여 회사 가치가 수십억 달러에 이루는 것으로 평가되고 있다[23]. 또한, 글로벌 IT 기업들은 AI 기반 사이버보안 스타트업을 인수하여 자사의 보안역량과 사업영역 확대를 지속적으로 추진 중이다[24].

4.2. 설명가능 인공지능(XAI) 기반 정보보호 기술

현재까지 보안에 적용되는 인공지능은 생성된 알고리즘에 의해 사이버공격 여부에 대한 판단결과만 제공할 뿐, 왜 그 결과가 나왔는지, 공격의 발생원인은 무엇인지 설명해줄 수 없었다. 특히, 보안 분야에서는 공격의 발생 원인에 대한 설명이 있어야 대응책・보완책 마련이 가능하므로 설명가능한 인공지능(XAI: eXplainable AI)에 대한 연구・개발이 반드시 필요한 실정이다.

세계적으로도 인공지능이 확보해야 할 신뢰성 중 하나로 설명가능성이 필요함을 공감하고 있다. OECD

는 AI권고안 주요 구성요소 중 하나로 “투명성 및 설명가능성”을 정의했고, 미국 NSCAI는 정부에 제안한 AI기본 프레임의 5가지 이슈 중 하나로 “견고하고 신뢰 가능한 AI”를 지정했으며, 우리나라는 2021년 발표한 “신뢰할 수 있는 인공지능 실현 전략”의 제1 전략 ‘신뢰 가능한 인공지능 구현 환경 조성’에서 반드시 개발해야 할 원천기술 중 하나로 ‘설명가능’을 포함시켰다[16, 17, 18].

XAI 관련 연구도 활발해 지고 있다. 미국은 국방성 산하 방위고등연구계획국(DARPA: Defense Advanced Research Projects Agency)을 중심으로 소속 과학자, 산업계 및 학계의 전문가로 팀을 구성하여 X-AI 개발 프로젝트를 추진하고 있으며, 2017년부터 2021년까지 약 800억원의 예산을 투입하고 있는 것으로 발표하였다[25, 26, 27]. IBM에서는 AI의 편향성을 극복하기 위해 학습 데이터와 모델이 한쪽으로 치우친 부분이 없는지 검증하는 ‘AI 오픈스케일(OpenScale)’이라는 XAI 기반 편향 검증 플랫폼을 개발・공개하였다[28]. 구글에서는 ‘클라우드 AI 플랫폼’을 통해 설명가능 XAI 서비스를 제공하고 있으며, 다양한 모델의 결과로부터 각 데이터 포인트의 기여도를 정량화하여 모델의 성능을 더욱 향상시키는 결과를 얻을 수 있게 추진하고 있다[29].

국내에서도 XAI에 대한 기반기술 연구가 시작되는 추세이다. 국가보안기술연구소(NSR) 및 한국인터넷진흥원(KISA)는 명확한 근거 확보가 요구되는 보안관제 분야에서 딥러닝의 한계점인 ‘블랙박스’를 해결하기 위해 ‘설명 가능 AI’ 기반 기술 개발에 속도를 붙이고 있으며, 울산과학기술원(UNIST)는 과기정통부로부터 154억을(‘17-‘21) 지원받아 ‘설명가능 인공지능 연구센터’를 개소, 차세대 XAI 연구·개발을 수행하고 있으며 세브란스병원(의료), 코스콤(금융) 등과 협력하여 해당 기술의 실증을 준비하고 있다[30].

또한, 과학기술사이버안전센터에서는 AI/XAI 기반 보안관제 자동화 원천기술 개발 및 지능형 보안관제체계 구축을 위한 연구를 수행하고 있다. 수집, 탐지, 분석, 대응 보안관제 전 단계에 AI를 적용하기 위해 보안데이터 전처리 및 최적화, AI 분류 모델 설계・구축, XAI기반 침해사고 자동 대응방안 공유 플랫폼 구축, AI/XAI 기반기술을 실 SOC 환경에 접목한 관제체계 구축함으로써 97%의 정확도로 10분 이내에 보안관제 전 단계를 자동 처리하는 지능형 보안관제 서비스 체계를 구축하는 것을 목표로 한다.

Ⅴ. 결 론

코로나19 팬데믹은 우리 일상을 크게 변모시켰을 뿐만 아니라, 사이버공격의 양적, 질적 변화에도 커다란 영향을 미쳤다. 세계적인 비대면 요구 증가로 화상회의, 원격근무 시스템 사용이 급증했고 이를 노리는 사이버공격 또한 늘어났다.

코로나에 의한 사이버공격의 양상은 클라우드 및 홈 네트워크 서비스 등을 노리며 내부자 위협을 증가시킨 원격근무 대상 공격, 랜섬웨어, 피싱, 스캠 공격의 증가로 대변되는 사회공학적 공격, 인공지능 및 머신러닝 기술을 접목하고 피싱 등의 공격 지능화에 활용하는 자동화 공격의 증가로 요약될 수 있다.

코로나에 의한 사이버위협의 동향 변화는 실제 보안업무 현장의 데이터에서도 확인할 수 있었다. 과학기술사이버안전센터의 보안관제 데이터에서는 2019년부터 HTTPS를 활용한 화상회의, 원격근무 등의 증가를 확인할 수 있었다. 또한, 코로나19가 최초 발생한 2019년부터 현재까지 웜・바이러스, 스피어 피싱, 스팸메일, 경유지 접근 등에 의한 침해사고가 급증했고, ‘자료훼손/유출’ 유형의 침해사고도 증가했음을 확인할 수 있었다. 게다가, VPN 대상 침해사고는 매년 2~4배의 급격한 증가세를 보였다.

과학기술사이버안전센터의 악성메일 침해대응 서비스 데이터 분석에서는 2021년 월 평균 신고건수, 악성 판별 건수가 타 년도에 비해 약 2배 증가, 악성의심메일 신고 건수도 2021년 6월부터 급격히 증가해 2021년 공공기관 대상 악성메일 공격 증가를 확인할 수 있었다.

위에서 살펴본 코로나19 팬데믹에 의한 사이버위협의 동향의 주요 원인은 원격접근 허용에 따른 보안접점 증가 문제, 사이버공격 자동화・지능화에 대한 대응방안 부재로 요약될 수 있다. 이러한 사이버위협 동향에 효과적으로 대응하기 위해 국내외에서 인공지능 및 설명가능 인공지능 기술에 대해 연구하고 있다. 특히, 과학기술사이버안전센터는 AI 및 XAI기술을 활용해 보안관제 전 단계에 AI를 적용하고 자동 처리하는 지능형 보안관제 서비스 체계 구축에 힘쓰고 있다.

향후, 지속적으로 연구・개발되고 있는 인공지능 및 설명가능 인공지능 기술들이 코로나19에 의해 범위와

대상이 확대되고 자동화·지능화되고 있는 사이버위협에 대응하는 효과적 해결책이 될 것으로 예측된다.

참 고 문 헌

[1] 2021 Global Security Insight Report, VM Ware, 2021

[2] 2020년 글로벌 정보보호 산업시장 동향보고, KISA, 2020

[3] Q1 2021 Threat Report, Nuspire, 2021

[4] COVID-19's Impact on Cybersecurity, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html, Deloitte, 2020.3

[5] 코로나19 닮은 '사이버 팬데믹'시대 온다, https://www.sciencetimes.co.kr/news/코로나19-닮은-사이버-팬데믹-시대-온다/, 2020.7

[6] 코로나19 팬데믹에 따른 사이버공격 변화 양상과 대응방안, INSS전략보고, p3, 2021.08

[7] 코로나19와 포스트 코로나 시대의 정보보호, https://www.asiatime.co.kr/article/20210621500119, 2021.6

[8] 11 Emerging Cybersecurity Trends in 2021, panda. 2021

[9] Yulia De Bari, "2021 Cybersecurity Trends Report", 2021

[10] 채재병, "국제사회의 해킹 변화 추세 및 대응방안", INSS연구보고서, p10, 2020

[11] "포티넷, 사이버공격 확장으로 전례없는 사이버 위협 환경 직면," http://www.efnews.co.kr /news/articleView.html?idxno=89125, 2021. 3. 11.

[12] Cedric Nabe, "Impact of COVID-19 on Cybersecurity."

[13] 금융위원회, "코로나19 관련 상황을 틈탄 사이버공격에 대응하여 금융회사 등의 보안조치를 강화하고, 해킹 등 피해 예방수칙을 마련하였습니다," 보도자료, 2020. 3. 9.

[14] Eric Richardson and Jake MahleVorys, "Cyberattacks on the rise during the Covid-19 pandemic," Jun 1, 2020

[15] 국가정보보호백서, 국가정보원, p41, 2021

[16] OECD 인공지능 권고안, NIA Special Report, p26-32, 2020

[17] Final Report, NSCAI, 2021

[18] "신뢰할 수 있는 인공지능 실현 전략(안)", 관계부처 합동, 2021.5

[19] 보안뉴스, 정보보안 서비스 매출 1위 : 보안관제 3강·3대 키워드, 2018년 7월.

[20] 디지털데일리, 인공지능 보안관제시장 격돌, 2018년 9월.

[21] BylineNetwork, 세인트시큐리티 국내 첫 AI 백신 '맥스' 국내외 공식 출시, 2018년 3월.

[22] 전자신문, [미래기업포커스] 파수닷컴, '인텔리전트 플랫폼' 강화로 SW 경쟁력 갖춘다, 2017.4

[23] 이승민, 송근혜, 정보보호동향 및 보안위협 분석, 2017.

[24] Paul, S., Microsoft confirms it is to acquire Israeli cybersecurity startup Hexadite to bring AI to Windows 10 enterprise security, venturebeat, 2017.

[25] 경향비즈, 결과만 알려주는 AI 넘어…"왜"까지 설명해주는 XAI(설명가능 인공지능) 뜬다, 2018.2.

[26] David Gunning, Explainable Artificial Intelligence (XAI), Retrieved August 11, 2016,

[27] 금융보안원, 설명 가능한 인공지능(eXplainable AI, XAI) 소개, 2018.3

[28] IT조선, "IBM, 인공지능 개발 돕는 'AI 오픈스케일' 공개", http://it.chosun.com/site /data/html_dir/2018/10/18/2018101803207.html, 2018.10.18.

[29] "구글 머신러닝 클라우드, '버텍스 AI'로 무장하다", https://slownews.kr/81261, 2021.7.5

[30] "UNIST, 설명가능 인공지능 연구센터 개소, AI 연구 본격화", https://www.aitimes.kr/ news/articleView.html?idxno=10734, 2017.9.25.

〈저 자 소 개〉

이 윤 수 (Younsu Lee)
정회원

2007년 2월 : 전남대학교 산업공학과 (공학사)
2010년 2월 : 충남대학교 대학원 컴퓨터공학과 (공학석사)
2017년 2월~현재 : 고려대학교 대학원 컴퓨터공학과 박사과정
2007년 3월 ~ 현재 : 한국과학기술정보연구원 과학기술사이버안전센터 선임기술원
<관심분야> 차세대 보안관제기술 연구 · 개발, 보안이벤트 실시간 가시화, 정보시스템 취약점 점검 · 분석

문 형 우 (Hyeongwoo Moon)
정회원

2005년 2월 : 배재대학교 컴퓨터공학과 졸업 (공학사)
2020년 8월 : 충남대학교 컴퓨터공학과 (공학석사)
2019년 4월~현재 : 한국과학기술정보연구원 과학기술사이버안전센터 연구원
<관심분야> 보안관제, 침해사고대응, 악성코드 분석, 네트워크 보안

박 건 량 (Gunyang Park)
정회원

2013년 8월 : 대전대학교 전산정보보호학과 (이학사)
2013년 9월~2018년 12월 : 국가보안기술연구소 관제기술원
2019년 6월~현재 : 한국과학기술정보연구원 과학기술사이버안전센터 연구원
<관심분야> 네트워크 보안, 악성코드 분석, 사이버보안 인텔리전스

김 태 용 (Taeyong Kim)
정회원

2014년 2월 : 목원대학교 정보통신공학과 (공학사)
2016년 2월 : 공주대학교 융합과학과 (공학석사)
2016년 6월~2019년 3월 : SK인포섹 책임
2019년 4월~현재 : 한국과학기술정보연구원 과학기술사이버안전센터 연구원
<관심분야> 보안관제, 네트워크 보안, 네트워크 가시화, 정보시스템 취약점 점검 · 분석

송 중 석 (Jungsuk Song)
정회원

2003년 2월 : 한국항공대학교 항공통신정보공학과 (공학사)
2005년 2월 : 한국항공대학교 대학원 정보통신공학과 (공학석사)
2009년 3월 : 교토대학교 대학원 지능정보학 (정보학박사)
2009년 4월~2011년 9월 : 일본정보통신연구원(NICT) 선임연구원
2011년 10월~현재 : 한국과학기술정보연구원(KISTI) 과학기술사이버안전센터 책임연구원(현 센터장)
2012년 9월~현재 : 과학기술연합대학원대학교(UST) 데이터 및 HPC 전공 교수
<관심분야> 네트워크 보안, 차세대 보안관제 기술, 기계학습, 데이터마이닝, 사이버공격 가시화