韓國IT서비스學會誌
第20卷 第5號
2021年 10月, pp.119-136

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2021.20.5.119

# 코로나19 관련 사이버 공격 및 대응현황 분석

이용필* · 이동근**

# An Analysis of Cyber Attacks and Response Cases Related to COVID-19

Yongpil Lee* · Dong-Geun Lee**

■ Abstract ■

Since the global spread of COVID-19, social distancing and untact service implementation have spread rapidly. With the transition to a non-face-to-face environment such as telework and remote classes, cyber security threats have increased, and a lot of cyber compromises have also occurred. In this study, cyber-attacks and response cases related to COVID-19 are summarized in four aspects: cyber fraud, cyber-attacks on companies related to COVID-19 and healthcare sector, cyber-attacks on untact services such as telework, and preparation of untact services security for post-covid 19. After the outbreak of the COVID-19 pandemic, related events such as vaccination information and payment of national disaster aid continued to be used as bait for smishing and phishing. In the aspect of cyber-attacks on companies related to COVID-19 and healthcare sector, we can see that the damage was rapidly increasing as state-supported hackers attack those companies to obtain research results related to the COVID-19, and hackers chose medical institutions as targets with an efficient ransomware attack approach by changing 'spray and pray' strategy to 'big-game hunting'. Companies using untact services such as telework are experiencing cyber breaches due to insufficient security settings, non-installation of security patches, and vulnerabilities in systems constituting untact services such as VPN. In response to these cyber incidents, as a case of cyber fraud countermeasures, security notices to preventing cyber fraud damage to the public was announced, and security guidelines and ransomware countermeasures were provided to organizations related to COVID-19 and medical institutions. In addition, for companies that use and provide untact services, security vulnerability finding and system development environment security inspection service were provided by Government funding programs. We also looked at the differences in the role of the government and the target of security notices between domestic and overseas response cases. Lastly, considering the development of untact services by industry in preparation for post-COVID-19, supply chain security, cloud security, development security, and IoT security were suggested as common security reinforcement measures.

Keyword : Cyber Incidents, Cyber Security Response, Covid-19, Post Covid-19, Untact Services Security

Submitted : July 19, 2021 1st Revision : September 23, 2021 Accepted : September 30, 2021

* 한국인터넷진흥원 수석연구원
** 한국인터넷진흥원 단장, 교신저자

# 1. 서 론

2020년 1월 코로나19 감염자가 국내에서 최초로 발생하고 빠르게 확산되면서, 코로나19 확산 방지를 위해 '사회적 거리 두기' 시행과 직장 내 확진자 발생에 따른 근무 장소 폐쇄 등으로 인해 비대면 업무방식이 급속하게 확산되었다. 공공부문에서는 공무원 교대 재택근무 의무화 및 비대면 근무 활성화 등 인사혁신처 근무지침이 시행되었고(인사혁신처, 2020), 민간 기업들도 크기·업종에 상관없이 재택근무를 시행하게 됨에 따라, 고용노동부에서는 "재택근무 종합 매뉴얼"을 발표하여 재택근무 관련 정부차원의 가이드를 제시하였다(고용노동부, 2020).

이러한 비대면 환경으로의 급속한 변화에 따라 IT 전반에 걸쳐 코로나19 대응에의 역할을 요구받게 되었고, 비대면 환경에서 재택근무가 활성화 되고, 온라인 회의가 일상적으로 받아들여지고 있다.

국내 보안분야에서는 비대면 환경에 따른 재택근무 및 온라인 회의 관련 보안대책들이 주로 발표되어 왔다(과학기술정보통신부, 교육부, 2020; 과학기술정보통신부, 한국인터넷진흥원, 2020; 금융보안원, 2020; 방위사업청, 2021).

그러나, 언택트 환경으로의 전환에 따라 보안 분야에서 다루어야 할 부분이 재택근무, 온라인 회의 서비스로 한정되는 것은 아니다. 대면 접촉을 최소화하기 위해 신규 서비스로 무인점포가 확대되고 있고, 오프라인 매장에서는 키오스크 채택이 증가하고 있으며, 온라인 서비스 증가에 따라 기업 내부 전산자원의 한계로 클라우드 이용이 증가하고 있다. 각국이 코로나 확산 방지를 위한 셧다운으로 해외 공급망 리스크 이슈가 부각되고, 이외에도 다양한 IT 이슈들이 보안과 연계되어 다루어져야 할 것이다.

재택근무, 온라인 회의 관련해서도 기존에 보안측면에서 전혀 다루어지지 않았던 것은 아니다. 원격근무, 온라인 스트리밍 이용자를 위한 보안 관련 내용들이 10년 전부터 스마트워크 보안 등으로 준비되고, 실행되고 있었고, 코로나 환경에서 급하게 재택근무를 채택하면서 재택근무와 온라인 회의 서비스를 운영하기 위한 보안가이드라는 이름으로 재정리해 발표했다고 보는 것이 정확할 것이다(방송통신위원회, 2011; 방송통신위원회, 한국인터넷진흥원, 2011; 이경복 외, 2011).

그렇다면 코로나19 팬데믹 발생과 사이버보안 과의 관련성은 어떻게 해석하고 설명해야 할까? 우선, 코로나19 관련 사회적 이벤트가 발생했고, 이를 사이버범죄자들이 사이버 사기에 활용할 때 성공률을 높일 수 있는 미끼로 이용하는 측면이다. 이는 피싱, 스미싱 등에 코로나19 관련 뉴스, 백신 접종 예약, 국민재난지원금 등 국민들의 관심이 집중되는 이벤트들을 활용함으로써 사이버 범죄자들이 유인 도구로 활용할 수 있기 때문이다.

둘째, 사이버 범죄자들은 돈이 되거나 해킹할 가치가 있는 사냥감을 찾는데, 그 대상으로 백신 개발업체, 백신 연구소, 공공기관 등 코로나19 관련 대상들과 의료기관들이 새롭게 공격대상에 추가되는 측면이다.

셋째, 코로나19의 높은 전염성과 무증상 감염 가능성으로 인해 사람과의 만남이나 접촉 자체를 피하고 비대면, 비접촉, 무인 방식을 선호하게 되면서 비대면, 언택트 관련 서비스들이 확대되고, 이 서비스들이 가지고 있는 보안상 취약점으로 인해 개인정보 유출, 서비스 중단, 영업기밀 유출 등의 위험성이 증가할 수 있는 측면이다.

이를 다시 두 가지로 나누어 보면, 하나는 코로나19 전염병 확산에 따라 즉각적인 비대면 서비스(재택근무, 화상회의 등) 적용에 따른 사이버 위협 증가 및 사이버 보안 대응 측면과 전염병 확산을 위한 감염자 및 접촉자 추적에 따라 발생하는 개인정보보호 이슈이다. 다만, 개인정보보호 이슈는 사이버 보안에서 다루기에는 너무 범위가 넓어 이 논문에서는 중점적으로 다루지는 않고 일부 개인정보유출과 관련된 부분만을 포함한다.

다른 하나는 다양한 언택트 서비스들의 등장에 따라 서비스별 보안 강화 및 보다 장기적으로 포스트 코로나 이후의 가속화되는 디지털 트랜스포메이션(또는 4차 산업혁명)과 연계하여 보안 대응 관련 과

제들을 제시해 보는 측면이 있을 것이다. 비대면, 언택트 관련 사이버 보안 이슈는 코로나19 발생 이전부터 제기되고 있었던 것들이면서도 관련 서비스들이 산업 분야별로 다양하게 제기되어 개별적으로 대응하는 것을 적는다면 범위가 무한정 확대될 수 있다. 따라서, 코로나19로 확대된 대표적인 언택트 서비스 분야(원격근무, 원격회의)를 한정해서 접근하였고, 다른 분야들은 공통적인 보안 관련 과제를 제언하는 것으로 정리하였다.

코로나19 팬데믹 동안 주요 사이버 공격 통계 자료들을 살펴보면, 먼저 코로나19 를 주제로 한 피싱 공격이 크게 증가했는데, Paloalto Networks에 따르면 2020년 3월과 4월 사이에 8만 6,000개 이상의 악성 고위험 코로나 관련 도메인이 등록됐다고 보고되었으며, 2월에서 3월 사이에는 악성 도메인 등록이 약 560% 증가한 것으로 나타났다(Paloalto, 2020a; Paloalto, 2020b). 또한, 소닉월(SonicWall)에 따르면, 2020년 랜섬웨어 공격이 전년대비 62% 이상 급증했으며, 특히 백신을 연구하는 의료 기관 및 연구기업에 대한 공격이 두드러졌다(SonicWall, 2021). Kaspersky에 의하면 개별 기업들이 준비기간이 부족한 상황에서 재택근무를 시작하면서, 윈도우 서버에 원격으로 접속할 수 있는 RDP 프로토콜을 활용하게 되는데, RDP 프로토콜 대상 무차별 대입 공격이 2020년 3, 4월에 400% 증가했으며, 온라인 회의 등이 활발히 진행되면서, Zoom 및 Teams와 같은 영상회의 앱 파일을 위장한 악성코드들이 2000년 3월 10만 건 이하에서 2021년 1월에는 115만 건으로 큰폭으로 증가했다(Kaspersky, 2021). 팬데믹 기간 동안 증가한 다른 위험에는 내부자 위협이 포함되는데, 테시안(Tessian)에 따르면, 2018년에 비해 코로나19 기간을 거치면서 47%나 증가했다(Tessian, 2021).

이 글에서는 코로나19 상황에서의 사이버 공격 및 사이버 보안 대응 현황을 위에서 정리한 4가지로 나누어 살펴보았다. 이를 위해 먼저 제2장 문헌연구에서 코로나19 관련 사이버보안 선행연구들과 언택트 서비스의 정의 및 분류들을 정리해 보았다. 제3장에서는 본 논문의 분석 프레임워크를 제시하고, 코로나19 관련 및 언택트 서비스 보안위협 및 침해사고 사례들을 보고서, 통계 자료 등을 참고해 정리하였다. 이어서 제4장에서는 코로나19 관련 국내 보안강화 대책, 해외 사례 및 언택트 서비스 보안관련 제언을 담았다. 제5장은 결론으로 분석 내용정리 및 한계점을 제시하였다.

## 2. 문헌 연구

### 2.1 코로나19 관련 사이버보안 선행 연구

코로나19 확산이 세계적인 대유행으로 확산되면서, 코로나19 관련 사이버 공격이 발생하고, 재택근무로의 전환에 따른 사이버보안 측면에서의 위협이 증가하자, 각국 정부에서는 코로나19에 따른 사이버 보안 가이드 등을 발표하기 시작하였다. 이응용(2020)은 이들을 정리하여 코로나19관련 위협사례와 미국 등 각국 정부의 초기 대책들을 소개하였다. 오형근(2020)은 코로나19 이후의 10대 사회변화와 이에 따라 요구되는 정보보호 7대 이슈(비대면 서비스 확대에 따른 정보유출 가능성 증대 등)를 분석하였다. Weil and Murugesan(2020)은 코로나19가 미치는 영향과 대응을 산업별로 분석한 후, NIST 사이버보안 프레임워크(Cybersecurity Framework) 모델을 이용해 코로나19에 대한 사이버보안 대응을 설명하고 있다. 이동휘, 김현아(2020)는 코로나19 관련 사이버 침해사고 사례를 원격근무 환경에 대한 공격, 코로나19 관련 스미싱, APT 공격 등으로 나누어 제시하였다. 국경완(2020)은 코로나19 관련 공격으로 스피어피싱을 주목하였고, 이를 예방하기 위해 금융감독원의 사이버보안 수칙과 인터폴의 사이버안전 점검 항목을 제시하고 있다.

Lallie et al.(2021)은 코로나19 발생 이후 코로나19와 관련된 이벤트들을 타임라인에 적고, 각국에서 발생한 사이버공격을 종류별로 분석하였다. 이를 통해 코로나19 관련 각국 정부 등이 발표한 내용을 이용해 스미싱/피싱-악성코드  다운로드-금융사기/랜섬웨

어 갈취 등으로 이어지는 일련의 공격이 발생하는 연관성을 분석하였다. Pritom et al.(2020)은 코로나19 관련 사이버공격을 5가지로 구분하고, 사이버 킬 체인 모델에 이들을 배열하였다. Pranggono and Arabo(2021)는 코로나19 팬데믹과 사이버공격 증가 사이에 상관관계가 있음을 보여주었고, 코로나19의 두려움이 커질수록 APT 공격그룹들의 공격 성공률도 높아지고 있음을 보여주었다. 또한, 재택근무와 의료기관들이 주요 공격 타겟이 되고 있음을 제시하였다. Hijji and Alam(2021)은 공식, 비공식 문헌 연구를 통해 코로나19 팬데믹 기간 동안 사회공학적 사이버 공격의 기술, 공격 방법, 사용된 악성코드 종류, 공격 대상, 경제적 피해 등에 대해 조사하였다.

## 2.2 재택근무 보안 가이드

미국 NIST(2016)에서는 재택근무를 위한 보안가이드(NIST SP 800-46 rev.2)를 2016년 7월 발표하였으며, 이 문서가 코로나 팬데믹 이후 미국을 비롯해 전 세계적으로 재택근무를 하는 기업들에게 기본 가이드 역할을 하였고, 국내에도 금융보안원 재택근무 보안안내서 작성 등에 영향을 미쳤다.

이 가이드는 다음의 내용을 담고 있다. 첫째, 기업의 원격근무 및 원격접속 솔루션에 대한 일반적인 취약점, 위협(3.3.1에서 설명)과 원격접속 방법의 상위 수준 아키텍처와 각 아키텍처의 보안 특성을 설명하고 있다. 원격접속 방법으로는 터널링, 어플리케이션 포털(포털 활용, VDI 활용), 원격 데스크탑 접속, 어플리케이션 직접 접속 등 4가지를 제시하고 있다.

둘째, 원격접속에 이용되는 서버의 보안, 서버 배치 및 클라이언트 소프트웨어 보안을 포함하여 원격접속 솔루션을 보호하기 위한 권장 사항을 제시하고. 원격접속 솔루션에서의 인증, 권한 부여 및 접속 제어를 다루고 있다.

셋째, 원격근무 클라이언트 장치(외부 단말기)를 보호하고 장치에 있는 데이터를 보호하기 위한 권장 사항을 제공하고 있다.

마지막으로는 원격근무 및 원격접속 수명 주기 전반의 보안에 대해 설명하고 있다. 원격 근무 보안 정책 수립, 설계, 구현, 운영 및 유지관리, 폐기 시 보안 고려 사항 등이 있다. 원격 근무 보안 정책에는 원격 근무 접속 방식 및 원격 접속 클라이언트 장치 정의, 권한 부여, 인증 및 원격 접속 솔루션 서버 배치 및 관리, 원격 접속 클라이언트 장치 관리 등에 대한 내용이 포함되며, 어떤 유형의 원격 근무 클라이언트 장치에서 어떤 수준의 원격 액세스를 허용해야 하는지에 대해 자체 위험 기반 결정을 내리고 주기적으로 재평가해야 한다.

NIST SP 800-46 문서는 조직 및 정보시스템 보안을 다루는 NIST SP 800-53을 기본으로 하고, 원격근무, 원격접속 및 BYOD보안 측면에서 관련된 부분을 특화하여 보안가이드를 낸 것이다. 또한 원격접속 서버 보안(NIST SP 800-123), 사용자 신원확인(NIST SP 800-63), BYOD 기기 사용자 보안지침(NIST SP 800-124), 기업 내 모바일 기기 보안지침(NIST SP 800-114 rev1), 시스템 개발 보안지침(NIST SP 800-64 rev2) 등에 대해서는 각각 별도의 NIST 표준 문서들을 참고해야 한다.

## 2.3 언택트 서비스 정의 및 분류

언택트는 부정을 뜻하는 접두어 'un'과 'contact'를 합한 신조어로, 비대면, 비접촉, 무인 방식을 일컫는 단어로 널리 쓰이고 있으나, 한국식 영어로, 해외의 경우는 그동안 드론이나 무인 배달 로봇 등과 같이 무인 기술이나 무인 서비스를 지칭하기 위해 'unmanned'를 쓰는 경우가 많았고, 비대면과 무인을 아우르는 언택트의 의미로서 'unmanned'라는 용어를 사용한 학술논문의 경우는 역시나 국내 연구진인 Kwak and Cho(2019)등 소수에 불과하다. 최근 코로나19 사태로 인해 해외 언론들도 비대면 서비스를 지칭하는 용어들을 쓰기 시작했는데, 대표적인 예는 'no-contact,' 'zero contact,' 혹은 'noncontact' 등을 들 수 있다. 언택트 서비스는 김난도 외(2018), Lee(2018), Lee and Lim(2018), Lee and Lee(2019), 전승화 외(2020) 등의 연구에서 보여지는 바와 같이

기본적으로 인공지능, 로봇, 가상증강현실, 사물인터넷, 클라우드, 빅데이터 등 혁신적인 디지털기술에 기반하고 있으며, Horn et al.(2015)과 Amar et al.(2019) 등이 지적하는 바와 같이 온라인 플랫폼을 통해 사람들 간의 커뮤니케이션과 상호작용을 대신하는 경우가 많다. 즉, 디지털기술과 온라인플랫폼을 통해 사람이 하던 일이나 사람 간의 상호작용을 대신하는 것이 곧 언택트 서비스라 할 수 있으며, 크게 사람과 사람 간의 대면활동과 상호작용을 최소화하는 비대면·비접촉 서비스와 사람이 하던 일을 디지털 기술로 대체해 버리는 무인서비스로 나누어 볼 수 있다.

이들 언택트 서비스는 온라인 플랫폼과 결합하여 기존에 오프라인에서 아날로그 방식으로 행해지던 다양한 경제활동을 온라인에서 디지털 방식으로 할 수 있게 변환한 서비스라고 할 수 있다. 즉, 언택트 서비스는 기본적으로 기업이 상품이나 서비스를 고객에게 제공하는 방식에 디지털 기술이나 온라인 플랫폼을 활용하는 것을 의미하며, 이는 곧 기업의 디지털 트랜스포메이션활동과 직결된다고 할 수 있다(전승화, 김정호, 2020).

〈표 1〉 언택트 서비스 종류 및 주요 기술

| 서비스 분류 | 주요기술 |
|---|---|
| 재택근무 | 클라우드, 기업용 SW(SaaS) |
| 화상회의 | 클라우드, 기업용 SW(SaaS) |
| 원격의료 | IoT, AI, 빅데이터, 클라우드 |
| 온라인교육 | 클라우드, 기업용 SW(SaaS) |
| 테크핀 | 클라우드, 빅데이터, AI, 블록체인 |
| 프롭테크 | AR/VR, 클라우드, 빅데이터, AI |
| 무인매장 | IoT, 결제솔루션, 클라우드 |
| 드론배송 | 드론, AI, IoT, 영상인식 |
| 스마트팩토리 | IoT, AI, 빅데이터, 클라우드 |
| 자율주행 | IoT, AI, 빅데이터, 클라우드 |
| 키오스크 | 결제솔루션, 클라우드 |

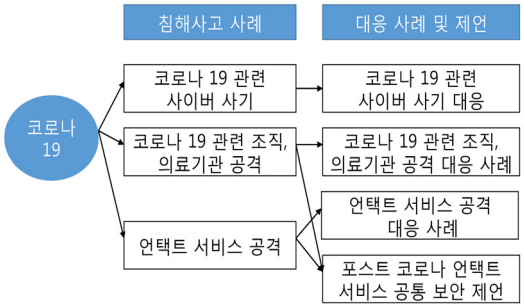
참고: 전승화, 김정호(2020) 표 일부 수정.

언택트 서비스는 위 <표 1>과 같이 서비스 분야별로 다양하게 이용되거나 준비 중이며, 적용되는 주요기술로는 클라우드, IoT, 기업용SW(SaaS) 등을 활용하고 있다.

## 3. 보안위협 및 침해사고 사례

### 3.1 사례분석 프레임워크

본 논문의 코로나19 관련 사이버보안 침해사고 사례 및 대응현황을 분석하기 위한 프레임워크는 [그림 1]과 같다.




[그림 1] 코로나19 관련 사이버 공격 사례 분석 프레임워크

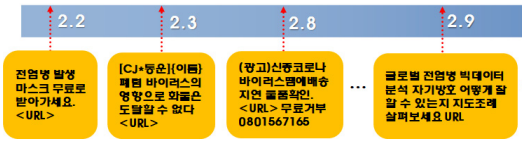
먼저 문헌연구 결과를 참고하여, 코로나19 관련 침해사고 사례를 사이버 사기 관련 사례, 코로나19 관련 조직과 의료기관에 대한 공격 사례, 언택트 서비스 공격 사례로 구분하였다. 이에 대한 대응 사례 및 제언은 3가지 각 공격에 대한 국내외 대응사례를 정리하고, 포스트 코로나 이후의 언택트 서비스 보안을 위한 공통 제언으로 구성하였다.

### 3.2 코로나19 관련 침해사고 사례

#### 3.2.1 코로나19 관련 사이버 사기 침해사고 사례

코로나19 바이러스에 대한 국민들의 불안감에 편승하여 마스크 무료 배포 등을 사칭한 스미싱 문자가 '20.2.2일 발견되었다. 아래 [그림 2]와 같이 이후 코로나로 인한 운송 지연 안내, 코로나19 환자 발생 정보 제공 등으로 관련 스미싱 문자가 지속되었다. 코로나19 관련 스미싱 문자가 3월30일 기준 9,886건이 발생하였다. 2020년 하반기에는 국민재난지원금

지급, 2021년에는 코로나 백신 접종 안내 등 이후 코로나19 관련된 스미싱이 지속되었다.




[그림 2] 코로나19 관련 스미싱 사례 (한국인터넷진흥원, 2020a)

### 3.2.2 코로나19 관련 조직, 의료기관 대상 공격 사례

국내 한국산업기술보호협회 산하 중소기업 기술지킴센터에 따르면, 코로나19 발생 직전 2019년 12월 국내 생명공학 분야 기업 대상 사이버 공격 시도는 9건에 그쳤으나 2020년 3월 53건, 이후 매달 건수는 증가하였다(머니투데이, 2020).

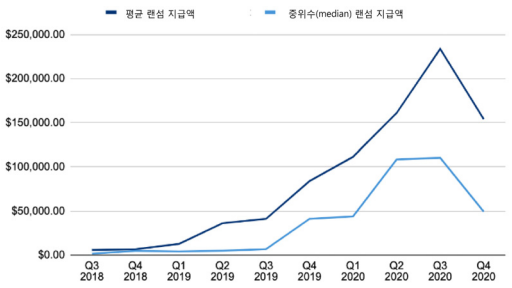
2020년 7월에는 미국 법무부가 중국 정부가 지원하는 중국 해커 2명을 미국 코로나 백신 관련 업체 등을 해킹한 혐의로 기소하였다(FBI & CISA, 2020; AP News, 2020).

2020년 10월에는 인도의 상위 제약기업이자 코로나 백신을 개발하는 다국적 제네릭 의약품 기업인 Dr. Reddy's Laboratories(닥터 레디스 래버러토리스)가 사이버 공격(정보유출, 랜섬웨어)을 받아 모든 데이터센터 서비스를 차단하였고, 그 영향으로 미국, 브라질, 인도, 러시아의 공장이 일시적으로 문을 닫았다(The Times of India, 2020).

2020년 12월에는 북한 해커들이 코로나19 백신 정보를 얻기 위해 영국, 미국, 한국 등 최소 9개 제약업체 대상으로 해킹을 시도하였고, 2020년 9월에 시작된 북한의 해킹 시도는 가짜 사이트를 만들어 그곳에 로그인하는 직원들의 비밀번호를 노리는 방식으로 이루어졌다(TV Chosun, 2020).

유럽의약품청(European Medicines Agency)에 따르면 2020년 12월 9 Pfizer/BioNTech 대상 사이버 공격으로 COVID-19 백신 데이터가 유출되었으며, 공격 직후 일부 데이터가 온라인에 불법적으로 공개되었다(HealthcareITnews, 2021).

다른 한편으로 코로나19 이후 미국 의료 산업에 대한 랜섬웨어 공격이 급증하였는데 2020년에는 최소 91개의 미국 의료 기관이 랜섬웨어 공격을 받았으며 이는 전년도의 50건에서 80% 이상 증가한 수치이다. 2020년에는 클라우드 소프트웨어 제공업체인 Blackbaud에 대한 주요 랜섬웨어 공격도 있었으며 이 공격은 최소 100개의 미국 의료 기관에 영향을 미친 것으로 알려져 있다. 아래 [그림 3]과 같이 랜섬웨어 피해액이 2020년 큰 폭으로 증가하는 것을 볼 수 있다.




출처: Health Sector Cybersecurity Coordination Center (2021a).

[그림 3] 미국 대상 랜섬웨어 공격으로 분기별 랜섬 지급액

의료기관을 대상으로 하는 해킹 공격은 파일 암호화뿐만 아니라 개인정보 공개를 미끼로 협박을 하고, 돈을 받는 것과 별개로 개인정보는 별도로 판매하여 돈을 버는 2중 착취를 하고 있다. 2021년 상반기 발생한 랜섬웨어 침해사고 중 정보유출이 같이 발생한 건은 72%에 해당한다(Health Sector Cybersecurity Coordination Center, 2021b). 2019년 Maze 랜섬웨어가 독보적이었다면, 2020년에는 18개의 랜섬웨어가 등장해 의료기관 들을 대상으로 해킹을 하였으며, RaaS(ransomware-as-a-service)로 랜섬웨어 개발과 공격을 분리해 운영하고, 자동화된 피싱도구를 이용해 피싱 후 랜섬웨어 공격으로 연결하는 등 해커들도 효율적으로 공격을 진행하고 있다(Health Sector Cybersecurity Coordination Center, 2021a). 이는 공격자의 공격 방식이 "spray and pray"에서 "big-game hunting" 형태로 변화하는 것을 나타내

며, 개인이나 중소기업 대상 무차별 다수를 대상으로 공격하기보다는 돈이 되는 특정 의료기관 등을 대상으로 타겟 공격을 하는 것이 범죄 수익률이 높기 때문이다.

의료기관들에 대한 해킹으로 데이터 유출도 심각한데, 미국에서는 지난 1년 동안(20.8~21.7) 500명 이상의 기록이 유출된 건수가 706건 발생하였으며, 유출된 개인정보 기록은 44,369,781건이나 되었다. 이는 평균 한 달에 58.8건, 370만 명의 기록이 유출되고 있는 상황이다(HIPAA Journal, 2020).

국내에서도 의료기관을 대상으로 한 침해사고 현황을 보면, 2020.3~12월까지 진료정보침해대응센터를 통해 신고된 침해사례 중 92%가 랜섬웨어 침해사례였다(보건복지부, 2021).

## 3.3 코로나19 관련 언택트 서비스 보안위협 및 공격 사례

### 3.3.1 원격근무 시스템 보안위협

원격근무란 업무 수행자가 기업 및 기관 내부의 정해진 사무 공간이 아닌 외부 다른 공간에서 업무를 수행하는 것을 통칭한다.

원격근무에 따른 주요 보안위협으로 NIST SP 800-46 rev2에서 제시하는 것으로는 다음 4가지가 있다. 첫째, 원격근무 클라이언트 장치(외부 단말기)가 물리적으로 보안통제가 미흡한 상황에서 사용될 수 있으므로, 장치의 분실, 도난에 따른 장치내 데이터의 유・노출 위험이 있다.

둘째, 외부에서 원격근무에 사용되는 네트워크 환경(와이파이 장비 등)이 보안통제가 되지 않을 경우 MITM(Mans in the Middle) 공격으로 도청을 당하거나 통신자료가 수정될 수 있다.

셋째, 악성코드에 감염된 원격근무 클라이언트 장치로 내부 네트워크에 접속 시 내부 네트워크에 연결된 시스템들이 악성코드에 감염될 수 있다.

넷째, 원격 접속을 신규로 허가하게 될 경우 내부 자원에의 외부 접근 위협이 발생하게 된다.

NIST 가이드에는 없지만, 추가적으로, 원격 접속 솔루션 구현 및 운영 시 발생하는 VPN, 소프트웨어 취약점, 클라우드 환경 이전 시 보안설정 미흡 등 공급망과 클라우드 보안위협이 존재한다.

### 3.3.2 재택근무 서비스 공격 사례

2020년 재택근무 및 관련 인프라가 사이버 공격 대상으로 부상한 가운데, 트렌드마이크로는 분당 약 11만 9,000건의 위협을 탐지했다고 밝혔다(트렌드마이크로, 2021). 또한 사이버 범죄자는 홈 네트워크를 통해 기업 시스템을 공격하거나 봇넷으로 IoT 기기에 대한 공격을 감행했다. 트렌드마이크로가 탐지한 재택근무 환경 대상 공격은 210% 급증해 29억 건에 육박했으며, 이는 전체 재택 환경의 15.5%에 해당한다. 홈 네트워크 대상 73%의 주요 공격은 무작위 대입 공격(브루트 포스)을 통해 라우터 또는 스마트 디바이스에 대한 제어권 강탈 시도였다(트렌드마이크로, 2021). 원격근무 등을 위해 사용되는 VPN 관련 위협으로는 한 보안업체의 VPN 서버 제품 취약점을 이용해 VPN 서버 계정 정보를 유출해 다크웹에 공개한 사건이 발생하였는데, 약 900여개 기업의 VPN 계정정보(아이디, 비밀번호)가 판매되고 있는 정황이 포착되었다(보안뉴스, 2021a).

원격근무 시스템에 도입되는 소프트웨어와 하드웨어를 공급, 유지보수하는 공급망의 취약점을 이용한 공격도 증가하고 있다. 개별 조직의 전산자원을 관리하는 소프트웨어 공급업체를 해킹하여 업데이트 시 해킹된 소프트웨어를 업데이트 하도록 하고, 해당 소프트웨어를 사용하는 기업들의 정보를 해킹할 수 있도록 하는 도구를 유포하는 공격들이 발생하고 있다. 또한 네트워크 하드웨어 장비의 취약점을 이용해 해킹할 수 있도록 하는 취약점도 지속적으로 발견되고 있어, 이를 이용한 해킹 시도도 발생하고 있다. 외국 피해사례로는 Pulse Secure VPN (CVE-2019-11510) 등 원격근무에 이용되는 VPN 장비의 취약점을 이용한 해킹 공격으로 침해사고가 발생하는 일이 발생하였고(Health Sector Cybersecurity Coordination Center, 2020), 국내에서도 보안기업, 방산기업, 공공기관 등이 원격근무에 이용

되는 VPN 취약점으로 침해사고를 당하기도 하였다(ZDNet Korea, 2021).

IBM Security가 2021년 발간한 "데이터 유출 비용 보고서 2021"에 따르면, 코로나 팬데믹 이후 원격근무 때문에 발생한 정보유출 사고 시 발생하는 피해액은 그렇지 않은 정보유출 사고의 피해액보다 평균 107만 달러 더 높았으며, 이번 유출 사고를 공개한 기업들 중 17.5%가 '재택근무 체제로 인한 유출 사고'였음을 주장하였다(IBM Security, 2021). 또한, 클라우드 도입률이 80% 이상인 경우, 퍼블릭 클라우드 사용 조직의 평균 피해액은 480만 달러, 프라이빗 클라우드 사용 조직은 455만 달러, 온프레미스 사용 조직은 415만 달러, 하이브리드는 361만 달러인 것으로 집계됐다. 클라우드 도입률이 높으면 높을수록 평균 피해액이 늘어났는데(평균 512만 달러), 이 경우도 클라우드가 나쁘다고 보는 게 아니라, 클라우드에 덜 익숙한 게 문제라고 이 보고서는 지적하였다.

### 3.3.3 영상회의 보안위협

영상회의는 물리적으로 원격에 있는 사람들이 전용장비/프로그램을 이용하여 회의를 진행하는 것을 통칭한다(과학기술정보통신부, 한국인터넷진흥원, 2020). 기업 본사와 지사(또는 해외 사무소)간의 업무 회의, 원격 강의 등 교육에도 활용되고 있다.

영상회의 접속 시 보안위협으로는 첫째, 물리적 보안위협을 들 수 있다. 화상카메라와 마이크는 참가자 정보 및 회의 내용을 전달하는 통로 역할을 수행할 수 있다. 카메라로 보여지는 사무실 위치 · 개인 이력 · 벽에 걸린 자격증 등을 통해 사용자의 개인정보가 노출될 수 있다. 마이크는 주변 음성을 전달하므로 의도하지 않은 추가 기밀 정보들이 마이크를 통해 타인에게 전달될 수 있다.

둘째, 외부에서 원격근무에 사용되는 네트워크 환경(와이파이 장비 등)이 보안통제가 되지 않을 경우 MITM(Man in the Middle, 중간자) 공격으로 도청을 당하거나 통신자료가 수정될 수 있다.

셋째, 영상회의 프로그램 또는 서비스에 취약점이 존재할 경우 추가 공격(화면 탈취, 무단 참가, 자료 유출 등)에 악용될 수 있다. 영상회의 통신이 E2E(End to End) 암호화되어 있지 않은 경우 영상 및 음성내용이 노출될 가능성이 있다. 넷째, 영상회의 개설자의 미비한 보안 환경설정또는 영상회의실 주소가 인터넷에 공개될 경우, 접속권한이 없는 외부인이 입장하여 회의를 방해하거나, 해당 서버를 대상으로 디도스 공격 등으로 인해 업무 장애가 발생할 수 있다.

### 3.3.4 영상회의 침해사고 사례

2020년 3월 국내 대학 온라인 강의에서 수강생이 아닌 사람들이 강의실에 입장하여 수업을 방해하는 행위가 발생하였다.

비인가 사용자가 영상회의실에 침입하여 회의를 방해하는 행위를 줌 폭격(Zoom Bombing)이라고 하며, 미국 FBI는 Zoom을 이용한 원격 강의에 허가받지 않은 사용자가 입장하여 교사를 비난하고 집 주소를 공개한 사례, 수업과 관련 없는 사용자가 원격수업용 Zoom 회의실에 입장하여 혐오스러운 문신을 카메라로 공개한 경우를 사례로 들고 있다(FBI, 2020). 가짜 영상회의 초대장으로 사용자 계정을 탈취하는 공격의 경우에는 영상회의를 초청하는 메일에 회의실 주소, 회의실 입장 비밀번호와 같은 일정한 형식이 제공되었다(과학기술정보통신부, 한국인터넷진흥원, 2020).

영국 국방부, NATO와 미국 기업 SpaceX는 보안수준이 높은 대화를 위해서는 서비스형 영상회의 Zoom 사용을 금지하기도 하였는데, 이는 서비스형 영상회의 대표기업인 Zoom이 End-to-End 보안을 지원하지 않는 것으로 확인되었기 때문이다(The Guardian, 2020; Reuters, 2020; Ars Technica, 2020). Zoom은 사용자 ↔ Zoom 서버 ↔ 사용자의 형태로 영상회의를 진행하며, 사용자와 Zoom 서버 구간만 암호화를 진행하였고, Zoom 서버에서는 암호화되지 않은 영상회의 내용이 존재하므로 데이터 유출 위험이 존재하였다. 이후 Zoom은 문제 해결을 위해 사용자↔사용자간의 암호 방식인 End-to-End 보안지원을 발표하였다(Zoom, 2020).

# 4. 보안강화 대책 사례 및 향후 제언

## 4.1 코로나19 사이버 사기 대응

국내에서는 코로나19 긴급 대응 체계 구축 및 모니터링 강화를 2020년 1월 30일부터 진행하였고, 코로나19 스미싱 대응 상황반 구성 및 운영을 2월 11일부터 본격화하였고, 대국민 보안공지를 2.28에 홈페이지에 공지하였다(한국인터넷진흥원, 2020a).

한국인터넷진흥원에서는 통신사들과 협력하여 코로나19 관련 스미싱 11,759건, 악성앱 44건, 악성앱 유포지 123건을 차단조치 하였다(한국인터넷진흥원, 2021).

## 4.2 코로나19 백신 등 관련 조직 해킹 대응

국내 진단키트 제조업체에 대한 해킹・사기 시도가 잇달아 발생하자 한국산업기술보호협회는 2020년 3월 20일 분자진단, 백신・치료제 개발 등 코로나19 관련 생명공학 업체들에 '이메일 무역사기 주의 권고문'을 발송하였고, 국가정보원등과 산업기밀 보호를 위한 TF를 구성하였다(중앙일보, 2020).

한국인터넷진흥원에서는 2020년 6월 이후 바이오기업 긴급 보안점검을 실시하여 미인지 해킹시도 2건, 해킹메일을 통한 정보탈취 93건, 서버 등 취약점 17건 발견 및 조치 등을 취하였다(한국인터넷진흥원, 2021).

보건복지부는 의료분야에 대한 사이버보안을 강화하는 법제도 등을 정비(의료법, 2020.2.28 시행)하고, 의료분야 사이버보안 전문기관으로 사회보장정보원에 진료정보침해대응센터를 2020년 7월 설립하였다(보건복지부, 2021). 이미 2018년 의료ISAC을 설치하여 의료기관 공동보안관제센터(20개 상급종합병원)를 운영하기 시작한 이후 본격적인 의료기관 사이버보안 대응이 가능하게 되었다.

진료정보침해대응센터는 개소 후 의료기관용 랜섬웨어 예방・대응을 위해 안내서(사회보장정보원, 2020), 코로나19 예방접종 위탁전문기관(의원) 대해 기관별 최대 5대 PC까지 안티랜섬웨어 소프트웨어를 무상으로 제공하고 있으며(사회보장정보원, 2021a), 의료부문 공격자 그룹 분석보고서를 발간하였다(사회보장정보원, 2021b). 다만, 의료기관들도 보건복지부, 교육부, 국가보훈처, 고용노동부, 경찰청, 과학기술정보통신부, 지자체 등으로 관리 대상이 분산되어 있고, 진단키트 및 백신 개발업체는 산업통상자원부 및 국가정보원에서 산업기밀로 관리하고, 그 밖의 민간 기업들의 사이버 보안은 과학기술정보통신부가 관리하는 등 담당 부처들이 흩어져 있다(보건복지부, 2021).

## 4.3 코로나19 관련 언택트 서비스 보안관련

### 4.3.1 비대면 업무환경을 위한 보안지침

3월에 코로나19 확산을 방지하기 위해 사회적 거리두기를 실시하면서 정부는 2020년 3월 30일 "재택・원격근무 정보보호 6대 실천 수칙"을 발표하였다. 사용자 실천수칙과 보안관리자 실천수칙으로 나누어 각각 6가지씩 제시하고 있는 것이 특징이다(한국인터넷진흥원, 2020b).

원격수업을 진행하게 되면서 교육현장에 급하게 보안수칙을 제공해야할 필요성이 발생하였다. 이를 위해 과기정통부와 교육부는 10개 항목의 실천수칙을 만들어 2020년 4월 9일 배포하였다(과학기술정보통신부, 교육부, 2020).

과기정통부와 한국인터넷진흥원은 2020년 6월 "비대면 업무환경(원격근무, 영상회의) 도입・운영을 위한 보안가이드"를 제작, 배포하였다(과학기술정보통신부, 한국인터넷진흥원, 2020). 이 가이드에는 비대면 업무환경의 보안위협을 원격근무, 영상회의를 나누어 설명하고 근무자와 원격근무 환경 운영자/관리자의 보안수칙으로 구분하여 제시하고 있다.

금융감독원은 2020년 12월 "금융회사 재택근무 보안 가이드"를 제작하여 배포하였다(금융감독원, 2020). 금융회사 임직원의 상시 원격접속을 허용하는 내용이며, 원격접속 방식으로 사내 업무망에 직접 연결하는 방식과, 가상데스트탑을 경유하여 간접연

결하는 방식 모두 가능하도록 하고 있다. 이 가이드는 '전자금융감독규정 세칙'을 개정하여 재택근무를 할 수 있도록 하였고, NIST의 원격근무 보안가이드를 참조하여 작성하였다.

방위사업청에서도 방산 및 협력업체 대상으로 재택근무 보안은 금융감독원 가이드를 참고로 하고, 추가적으로 영상회의 관련 보안가이드를 더한 보안안내서를 배포하였다(방위사업청, 2020).

많은 기업들이 VPN을 활용한 원격근무 시스템을 급하게 도입하면서, 인프라, 비즈니스 애플리케이션이 원격 액세스를 통해서만 작동할 수 있도록 하기 위해서 일부 방어 계층(방화벽 및 네트워크 세분화를 통해 제공됨)을 완화하였고, 패치되지 않은 VPN 시스템을 도입하면서 사이버 범죄 행위자의 타겟이 되는 우려스러운 일이 발생하기도 하였다(Health Sector Cybersecurity Coordination Center, 2020).

국내에서는 정부의 직접적인 역할강화로 비대면 사회의 사이버보안을 위해 2021년 2월 'K-사이버 방역 전략'을 발표하였으며, 이 전략 안에는 아래 개인PC 보안강화, 비대면 서비스 취약점 점검 등 다양한 보안대책들을 담았다(과학기술정보통신부, 2021).

#### 4.3.2 개인 PC 보안 강화

원격근무에 이용되는 원격 클라이언트의 엔드 보안을 위해서는 재택근무를 하는 개인들의 PC의 보안을 높여야 하는데, 재택근무를 하는 개인PC의 보안 상황을 개인들에게 맡겨 놓는 것은 일반인이 점검하는데 한계가 있을 수 있다. 이를 해결하기 위해 정부에서는 한국인터넷진흥원을 통해 '내 PC 돌보미'(원격 PC 점검 서비스) 사업을 2020년 하반기에 진행하여, 개인PC 원격 점검(2020년 16,350여 건)을 지원하였다(한국인터넷진흥원, 2021).

#### 4.3.3 비대면 서비스 취약점 점검

한국인터넷진흥원에서는 모바일 앱·홈페이지를 통한 비대면 서비스(원격 근무/교육/의료/쇼핑 등)를 제공 중인 중소기업을 대상으로 취약점 점검을 해주고 있다(한국인터넷진흥원, 2021). 2020년 원격협업 솔루션 7개 제품에서 30개 취약점을 발견하고, 집중 신고기간을 운영해 총116개 보안취약점을 발견하여 조치를 지원해 주었고, 개발사 운영환경 보안이 취약하여 해킹되는 것을 막기 위해 4개 기업의 운영환경을 점검하여 총278개 취약점을 찾아 보완할 수 있도록 안내하였다(한국인터넷진흥원, 2021).

### 4.4 외국 정부의 사이버보안 강화 대책 사례

#### 4.4.1 미국의 코로나19 관련 대응

미국의 코로나19 관련 대응은 미국 사이버 보안을 총괄하는 국토안보부 CISA(Cybersecurity and Infrastructure Security Agency, 사이버보안 및 기반시설보호국)의 활동 중심으로 살펴보았다. 사이버보안 및 기반시설 보호 전담기관인 CISA는 2020년 3월 6일, 2페이지 분량의 짧은 내용 속에 4가지 분야 즉, 주요기반시설보호를 위한 활동, 공급망을 위한 활동, 조직의 사이버보안 활동, 직원 및 고객을 위한 사이버보안 활동을 요약해 제시하였다(CISA, 2020a). 특히 이 보고서를 조직의 경영진을 대상으로 작성하여, 미리 대응할 것을 명시적으로 언급하고 있다. 같은 날 개인들에게 코로나19 관련 사이버 사기에 조심하라고 주의안내 공지를 하였다(CISA, 2020b). 이는 WHO에서 3월 11일 세계적인 팬데믹을 선언하기 이전이었다.

이후 3월 13일 원격근무를 고려하는 기업 대상 VPN 보안 관련 경고를 발표하였다(AA20-073A)(CISA, 2020c). 여기서는 원격근무에 VPN을 활용하는 경우, 해커의 목표물이 될 수 있고, 원격근무에 활용되는 VPN이 24/7 가동에 따라 최신 업데이트가 되지 않고 이용하는 문제점, Multi Factor Authentication 사용을 하지 않는 문제점을 지적하며, 원격근무 관련 보안을 강화하고 NIST SP 800-46 rev2에 따라 기업 보안정책에 문서화 할 것을 권고하고 있다.

CISA는 연방 민간 기관들이 원격근무를 위해 전산자원 확보를 위해 클라우드를 사용하게 되는 경우가 발생하게 되면서, 클라우드 사용 옵션과 보안관련 고

려사항을 정리하여 임시로 개정된 원격근무 가이드가 4월 8일(TIC 3.0 Interim Telework Guidance) 발표하였고(CISA, 2020d), 비디오 컨퍼런스와 관련된 보안가이드는 5월 1일 발표하였다(CISA, 2020e).

CISA는 개별적으로 발표하던 보안지침들을 종합하여 Cyber Essential Toolkit 시리즈(6개)라는 이름으로 5월부터 11월까지 순서대로 발표하였다(CISA, 2020f). 이 Toolkit은 경영진, 직원, 시스템, 디지털 작업장, 데이터 보안, 위기대응 등 사이버 준비(readiness)를 완성하기 위해 조직문화의 6개 관련 측면에서 각 사이버 필수 요소의 구현을 위해 IT 및 C-suite(executive-level managers) 리더십이 작동하도록 설계된 모듈 세트이다. 그리고 10월에는 다시 경영진, 시스템 담당자, 직원별로 원격근무와 관련해 보안가이드를 정리해 Telework Essentials Toolkit 이라는 이름으로 발표하였다(CISA, 2020g).

이외에 FBI와 연계하여 5월 13일에는 코로나19 관련 연구기관을 대상으로 하는 중국의 사이버공격에 대해 수사를 하고 있다는 발표를 하였다(FBI & CISA, 2020).

또한, CISA는 의료기관을 대상으로 취약점점검을 2020년 3월부터 11월까지 진행하였다. 그 결과는 2021년 1월 발표하였는데, 49%의 의료기관이 인터넷에 노출된 정보자산에 대해 취약한 포트와 서비스가 있었고, 58%가 지원이 중단되거나 서비스를 받지 못하는 레거시 시스템을 사용하고 있는 등 취약점이 많았다(CISA, 2021).

#### 4.4.2 EU의 코로나19 관련 대응

EU의 코로나19 관련 대응은 EU의 사이버 보안 정책을 총괄하는 ENISA(The European Union Agency for Cybersecurity, 유럽사이버보안국)의 활동을 중심으로 살펴보았다. ENISA는 2020년 3월 15일, 집에서 재택근무 시 고용주가 취해야 할 6가지 내용을 Director 명의로 언론에 공개하였다(ENISA, 2020a). 이어서 이를 재정리해 2020년 3월 24일 재택근무 시의 사이버보안 핵심 지침(Top Tips)을 공개하였다. 내용은 1. 사업주를 위한 권고(11개)와 직원들을 위한 권고(10개), 2. 코로나19와 관련된 피싱 방지 대책으로 구성되어 있다(ENISA, 2020b).

이후 시민들이 집에서 있으면서 온라인 거래가 확대되자, '온라인 거래를 할 때의 사이버보안 지침(Tips)'을 공개하였고(2020.3.31)(ENISA, 2020c), 중소기업들을 위해 '온라인 회의 툴 선택과 이용 지침(Tips)(10개)'(2020.4.27)(ENISA, 2020d), 코로나19 관련 피싱 공격이 급증하자, 피싱 공격 사례 및 피해를 당하지 않도록 하는 안내(ENISA, 2020e), 해커들의 목표물이 되고 있는 의료부분의 사이버보안을 위해 '코로나19 상황에서의 의료부문 사이버보안'(2020.5.11)을 발표하였다(ENISA, 2020f). 이후 스마트 홈 등 원격근무 직원들의 가정 내 보안과 IoT/smart infrastructure 보안, 스마트 빌딩/오피스 보안 관련 내용으로 발표하였고(2020.5.18)(ENISA, 2020g), 중소기업을 위한 10가지 보안 지침(Tips)(2020.6.2) 순으로 발표하였다(ENISA, 2020h). ENISA의 보안지침 내용들은 대부분 1~2 페이지 분량으로 CEO, IT담당자, EU 시민들에게 코로나19 관련 위협을 인식시키고, 역할별로 대응행동 요령을 이해시키는데 중점을 두어 간단하게 되어 있는 것이 특징이다.

#### 4.4.3 시사점

시간적으로 보면, 급하게 비대면 업무환경으로의 전환에 따라 국내외적으로 우선적으로 포괄적인 가이드·지침을 제공하고, 이어서 세부적으로 대응 범위가 확대되어 가고 있었다. 예상치 못한 비대면사회로의 전환에 따라 사이버공격은 증가하였고, 비대면 환경에서의 사이버공격의 피해를 줄이기 위한 접근방식이 국내와 해외에서 차이가 있음을 확인할 수 있었다.

국내는 가이드 대상이 시스템 운영담당자와 직원으로 구분하고, 원격근무, 화상회의 중심으로 가이드를 발표하였다. 정부의 직접적인 역할강화로 의료분야는 진료정보침해대응센터를 개소하고, 의료기관 대상 안티랜섬웨어 프로그램을 무상으로 보급하는 한편, 정부차원에서의 비대면사회의 사이버보안을 위해 'K-사이버 방역 전략'을 발표하였다. 또한, 정

부가 직접 보안강화 사업을 추진하여 개인 대상 PC 보안점검, 기업들의 취약점점점 등을 실시하였다.

해외는 수칙을 발표하면서 피싱, 스미싱, 사기 등의 피해 대비를 같이 강조하였고, 수칙 안내 대상을 사업주 등 임원급을 대상으로 하는 것과 근로자가 하는 역할을 구분하여 제시하였으며, 의료부문에 대한 사이버공격에 대한 대응 가이드를 별도로 제시하기도 하였다. 그러나, 해외에서는 정부 직접 사업이 많지 않았음을 확인할 수 있었다.

## 4.5 포스트 코로나 언택트 서비스들의 공통적 보안강화 제언

언택트 서비스들의 보안을 위해서는 개별 서비스 차원에서 보안을 적용해야하는 것이 당연하지만, 향후 보안성을 강화하기 위해 각 서비스들에 공통적으로 요구되는 내용들을 먼저 정리해 둘 필요가 있다.

### 4.5.1 공급망 보안 강화

첫째, 언택트 서비스별로 다양한 공급업체들의 지원을 받아 서비스가 구축, 제공되는데, 이들 공급업체들로부터 제공받는 ICT제품, 서비스들의 보안성을 높일 수 있도록 관리하는 것이 공급망 보안 관리이다. 사이버 보안을 위해 개별 조직 차원에서 관리체계를 구성하여 운영하는 것(ISO 17002, ISMS 등)과 차이는 공급망 보안 관리는 공급자에서 소비자로 이어지는 공급 체인 과정에 조직 간 연계된 것으로 한 조직의 노력으로만 될 수 있는 것이 아니라 조직 간 계약 관리를 통해 구현되고 필요시 제도적으로 뒷받침되어야 할 부분도 존재하다.

최근 ICT 공급망에 침투하여 사용자에게 전달되는 SW · HW를 변조하는 형태의 공급망 공격이 다수 발생하고 있어(손효현 외, 2019) 공급망 보안 관리가 주요 이슈로 제기되고 있다. 이에 따라, 미국 등에서도 공공부문 ICT의 공급망 보안관리 강화를 위해 대통령 행정명령 발표(미국, 사이버보안 가이던스 행정명령, 2021.5), 법제화(독일, IT 보안법 2.0, 2021.5), 관련 표준 및 가이드(ISO/IEC 27036, NIST 800-161(NIST, 2015)) 등을 만들어 기반시설, 공공부문 등에 적용하고 있으며, 개별 조직에서 공급망보안 관리 적용을 지원하기 위한 여러 가지 툴(CSET, C-SCRM)을 제공하고 있다.

국내에서도 기반시설 등의 공급망 보안을 위한 가이드를 개발하고 있으며(과학기술정보통신부, 2021), 공급망 보안을 확산하기 위한 제도적 지원 및 이를 개별 조직들이 적용할 수 있도록 지원하는 툴을 개발, 보급하고 개별 조직들이 적용하는데 어려움을 겪을 때 이를 지원할 수 있는 지원조직 등을 확보할 필요가 있다.

### 4.5.2 SW개발보안 강화

ICT의 도움을 받는 언택트 서비스들은 소프트웨어가 이용되는 것이 대부분이며, 보안을 고려한 소프트웨어 설계, 개발이 되지 않을 경우 너무나 쉽게 취약점을 노출하게 된다. 소프트웨어 개발보안은 소프트웨어 개발과정에서 개발자의 실수, 논리적 오류 등으로 인해 침해/해킹 사고 등을 유발하는 소프트웨어에 내포 될 수 있는 보안약점(취약점)을 최소화하기 위한 보안 활동을 말한다.

공공부문에서 일정 금액 이상의 정보시스템 구축, 모바일앱 구축 시에서는 소프트웨어 개발보안 진단을 의무적으로 받도록 하고 있으나, 민간부문에서는 자율적으로 운영되고 있는 상황이다. 행정안전부에에서 제시한 개발보안 진단 기준(행정기관 및 공공기관 정보시스템 구축 · 운영 지침)은 홈페이지의 경우 설계단계 20개, 구현단계 47개 항목을 제시하고 있다(행정자치부, 2017).

개발현장에서 보안약점 진단을 위해 상용 진단 도구를 활용하고 있으나, 진단 도구를 통한 보안약점을 찾아 보완하는 것에는 명확한 한계가 있어 보안진단 도구에만 의존하면 안 되고 전문적인 보안진단 인력의 보안진단을 받을 필요가 있으며, 동시에 소프트웨어 개발자들이 처음부터 보안약점이 없도록 개발하는 것이 중요하다.

민간부문에는 2020년 소프트웨어진흥법 개정시에 소프트웨어 개발보안 조항이 신설되면서 정부의 역

할로 민간 개발보안 인력양성을 할 수 있도록 하고, 시행령에 민간부문에서의 보안약점 진단, 참고기준 개발 및 보완 등이 추가되었다(법제처). 민간 기업들의 소프트웨어 개발보안 강화를 위해 정부 지원사업 등을 통해 개발보안 참고기준 개발 및 보급, 진단전문 인력의 진단서비스 등을 활용한 언택트 서비스 개발보안 지원이 필요할 것이다.

#### 4.5.3 클라우드 보안 강화

ICT 언택트 서비스들 중 상당수가 클라우드 기반의 서비스를 진행하고 있다. 따라서 클라우드 보안의 중요성은 높다. 클라우드 서비스 제공자 특히, AWS, MS Azure, KT, NAVER클라우드와 같이 국내외적으로 클라우드 보안인증을 받은 클라우드 서비스 제공자들의 클라우드 인프라, 서비스 들은 상대적으로 보안성이 높게 관리되고 있다.

클라우드 인프라 위에서 서비스를 개발하거나, 이를 이용하는 기업이 보안설정을 잘못하거나, 인증관리를 잘못해서 사용자 인증정보가 유출되어 해킹되는 경우가 다수 발생하고 있다(보안뉴스, 2021). 따라서 클라우드 기반에 서비스를 개발하여 제공하는 기업이거나, 클라우드 기반에서 원격근무 등의 시스템을 운용하는 기업들은 '제로 트러스트' 관점에서 보안설정 및 관리, 운영에 주의를 기울여야 하며, 클라우드 보안 가이드(한국인터넷진흥원, 2017) 등을 준수하여 안전하게 개발, 운용하여야 한다.

#### 4.5.4 언택트 서비스의 IoT 보안 강화

스마트 헬스케어를 비롯한 많은 언택트 서비스들은 IoT 기기를 활용하고 있으며, 언택트 서비스에 이용되는 IoT기기들은 네트워크에 연결되어 있어 필연적으로 정보유출 등 해킹의 위협에 노출되며, 이를 대응하기 위한 대책 마련이 필요하다.

EU에서는 EU단일시장에서 통용될 수 있는 IoT 보안인증제를 법제화(ENISA 및 정보통신기술 사이버보안 인증과 규정 No 526/2013 폐지에 관한 2019년 4월 17일자 유럽의회 및 이사회 규정 2019/881)하였고, ENISA를 통해 구체적인 IoT 보안인증 스킴을 개발하도록 하고 있다.

미국에서도 연방정부 차원에서 IoT 보안을 강화하기 위한 제도적 기반(2020 IoT 사이버보안개선법, NIST IoT 보안가이드)을 마련하고 공공분야에서부터 적용하도록 하고 있다(이용필 외, 2021). 이렇게 해외에서도 ICT 융합기기 대상 설계부터 보안을 고려한 제품 생산 및 판매를 촉진하기 위해 보안인증을 도입하고 있으며, 이를 위해 법제화 및 인증기준과 방법을 표준화하는 작업이 진행되고 있다.

국내도 2020년 정보통신망 이용촉진 및 정보보호 등에 관한 법률이 개정되면서 네트워크에 연결된 ICT 융합기기를 '정보통신망 연결기기 등'으로 정의하고, IoT 보안인증제도 근거를 마련하였다(법제처). 새롭게 제도화된 IoT 보안인증은 과학기술정보통신부가 정책기관으로, 한국인터넷진흥원이 IoT 보안인증기관으로, 인증시험대행기관은 별도로 지정하도록 하고 있으며, IoT 보안인증은 자율적으로 신청을 받아 수행하도록 하고 있다.

스마트헬스케어, 스마트공장, 무인드론, 원격근무, 스마트시티 등 산업부문별 언택트 서비스를 담당하는 각 부처나 전문기관이 해당 서비스의 등록, 허가를 하면서 보안 요구사항에 언택트 서비스에 활용되는 IoT 보안인증을 받은 제품을 활용하도록 하거나, 언택트 서비스 공급, 수요자 스스로 IoT 보안인증을 활용하여 보안성을 높일 수 있을 것이다.

## 5. 결 론

지난 해 전 세계적인 코로나19 확산이 발생하면서, 국내에서도 '사회적 거리 두기' 시행과 직장내 확진자 발생에 따른 근무 장소 폐쇄 등으로 인해 비대면 업무방식이 급속하게 확산되었다. 원격 근무, 원격 수업 등 비대면 환경으로의 전환에 따라 보안위협이 증가하였으며, 사이버침해사고 사례들도 발생하였다.

본 사례연구에서는 코로나19와 관련된 사이버공격과 대응 사례를 사이버 사기, 코로나19 관련 기업 및 의료분야 공격, 재택근무 등 비대면 서비스 공격,

언택트 서비스의 포스트 코로나 이후 대비 등 4가지 측면에서 정리하였다.

코로나19 연구성과를 얻기 위한 국가 지원 해커 공격 사례, 랜섬웨어 공격 방식이 'spray and pray' 방식에서 'big-game hunting' 방식으로 바뀌면서 돈벌이가 될 수 있는 타깃을 정해 공격함으로 랜섬웨어 피해가 급증하고, 개인정보 유출도 증가하는 것을 확인할 수 있었다. 또한 많은 기업들이 VPN을 활용한 원격근무 시스템을 급하게 도입하면서, VPN 자체의 보안 취약점들과 패치가 되지 않은 상황에서 시스템을 운영하는 등으로 인해 사이버 공격의 대상이 되는 경우도 발생함을 확인할 수 있었다.

이어서 보안강화를 위해 정부차원에서 제시한 대책을 국내 및 해외로 나누어 분석하였다. 국내는 수칙의 내용이 재택근무에 초점을 맞추는 반면, 해외는 스미싱, 피싱 대응을 포함하고 있고, 수칙 대상자에 경영진이 명시적으로 포함되는 지에서도 차이가 있는 것을 확인할 수 있었다. 또한, 코로나19로 인해 병원 등을 대상으로 하는 사이버공격이 증가하고 있어 해외에서는 의료분야 사이버보안 가이드를 발표하고 있는 반면, 국내에서는 정부의 직접적인 역할을 강화하여 진료정보침해대응센터를 개소하고, 의료기관 대상 안티랜섬웨어 프로그램을 무상으로 보급하는 한편, 정부차원에서의 비대면사회의 사이버보안을 위해 'K-사이버 방역 전략'을 발표하고, 엔드단 보안을 위한 과제를 추진하는 등 정부의 역할에 차이가 있음을 확인할 수 있었다.

마지막으로, 포스트 코로나 이후의 언택트 서비스들이 지속적으로 운영될 것을 대비해 공급망 보안, 소프트웨어 개발보안, 클라우드 보안, IoT 보안인증 등을 공통보안 사항으로 제언 하였다.

본 사례연구의 한계점으로는 코로나19 이후의 변화된 사이버보안 환경과 이에 대응하는 측면을 다루다 보니 많은 것을 언급하게 되어 특정한 구체성이 부족한 부분이 있을 수 있다는 점이다. 원격근무 이외에 스마트의료, 자율주행차, 드론 배송 등 비대면 서비스 별 보안을 위한 구체적 연구, IoT 보안인증과 같이 개별적으로 깊이 있는 연구가 추가적으로 진행되어야 할 것이다.

## 참고문헌


고용노동부, "재택근무 종합 매뉴얼", 2020.

과학기술정보통신부, "K-사이버방역 추진 전략", 2021.

과학기술정보통신부, 교육부. "원활한 원격수업을 위해 10가지 실천수칙을 지켜요", 보도자료, 2020. 4. 9.

과학기술정보통신부, 한국인터넷진흥원, "비대면 업무환경 도입운영을 위한 보안가이드", 2020.

국경완, "코로나19 이후 사이버공격 유형 및 대응 방안", KOSEN Report, 2020. 09.

금융보안원, "금융회사 재택근무 보안가이드", 2020.

김난도, 전미영, 이향은 외 5명, 트렌드코리아 2018, 미래의 창, 2018.

머니투데이, "'한국형 진단키트' 인기끌자 해외서 국내 제조업체 해킹 시도", 2020. 3. 31.

방송통신위원회, "스마트워크 활성화를 위한 정보보호 권고", 2011.

방송통신위원회, 한국인터넷진흥원, "스마트워크 활성화를 위한 정보보호 권고 해설서", 2011.

방위사업청, "방산 및 협력업체 비대면 · 재택근무 보안 안내서", 2021.

법제처, http://www.law.go.kr.

보건복지부, "의료기관 진료정보보호 추진 방향", 2021 의료기관 개인정보보호 & 정보보안 컨퍼런스 발표자료, 2021. 7. 6.

보안뉴스, "해커, 국내 대기업 계속 노리나? 다크웹서 내부 네트워크 침투용 VPN 계정 판매", 2021a. 3. 2.

보안뉴스, "되돌릴 수도 없는데... 클라우드의 악순환, 우리 스스로 자초했다", 2021b. 9. 16.

사회보장정보원, "의료분야 랜섬웨어 예방대응안내서", 2020.

사회보장정보원, "코로나19 예방접종 위탁의료기관 안티랜섬웨어 소프트웨어 설치", 2021a. 6. 4.

사회보장정보원, “국내외 의료분야 타겟형 사이버 공격그룹 분석 및 대응방안”, 2021b.

손효현, 김광준, 이만희, “미국 공급망 보안 관리 체계 분석”, *정보보호학회논문지*, 제29권, 제5호, 2019, 1089-1097.

오형근, “코로나19 이후 주요 사회변화와 정보보안 이슈 분석”, *정보과학회지*, 제38권, 제9호, 2020, 48-56.

이경복, 박태형, 임종인, “스마트워크 환경 변화에 따른 보안위협과 대응방안”, *디지털융복합연구*, 제9권, 제4호, 2011, 29-40.

이동휘, 김현아, “코로나19 관련 사이버 공격 사례분석을 통한 보안 연구”, *한국정보통신학회 종합학술대회 논문집*, 제24권, 제1호, 2020, 548-550.

이용필, 이상걸, 서영진, “국내 IoT 보안인증 제도 개선 연구”, *융합보안논문지*, 제21권, 제1호, 2021, 79-92.

이응용, “코로나-19를 이용한 사이버공격 및 대응동향”, KISA Report, Vol.5, 2020, 20-29.

인사혁신처, “‘사회적 거리두기’ 공무원 복무 관리 특별지침 시행”, 2020.

전승화, 김정호, “언택트(Untact) 산업 확산의 이론적 배경과 전망”, *신산업경영저널*, 제38권, 제1호, 2020, 96-116.

중앙일보, “韓코로나 진단키트 업체 해킹 시도…정부, TF 구성 대책 마련”, 2020. 3. 31.

트렌드마이크로, “2020 위협 결과 보고서(2020 Security Roundup Report)”, 2021.

한국인터넷진흥원, “클라우드 정보보호 안내서”, 2017.

한국인터넷진흥원, “코로나19 바이러스 사칭 스미싱 주의 안내”, 보안공지, 2020a. 2. 28.

한국인터넷진흥원, “재택·원격근무 정보보호 6대 실천 수칙”, 2020b. 3. 30.

한국인터넷진흥원, “2020년도 경영실적보고서”, 2021.

행정자치부, “소프트웨어 개발보안 가이드”, 2017.

IBM Security, “데이터 유출 비용 보고서 2021”, 2021. 7. 29.

TV Chosun, “北, 코로나 백신 개발 제약사 해킹 시도…국내 4곳도 공격”, 2020. 12. 3.

ZDNet Korea, “해커도 익숙해진 ‘원격근무’…VPN 의존하니 정보 탈탈”, 2021. 8. 7.

Amar, J., Raabe, J., and Roggenhofer, S., *Customer first: Personalizing the customer-care journey*, McKinsey & Company, New York, 2021.

AP News, “US accuses Chinese hackers in targeting of COVID-19 research”, 2020. 7. 22.

Ars Technica, “Zoom lied to users about end-to-end encryption for years, FTC says”, 2020. 11. 10.

CISA, “CISA Insights: Risk Management for Novel Coronavirus(Covid-19)”, 2020. 3. 6, 2020a. 3. 18. update.

CISA, “CISA Alert: Defending Against COVID-19 Cyber Scams”, 2020. 3 .6.

CISA, “CISA Alert : Enterprise VPN Security”, 2020c. 3. 13.

CISA, “TIC 3.0 Interim Telework Guidance″, 2020d. 4. 8.

CISA, “Guidance for Securing Video Conference”, 2020e. 5. 1.

CISA, “Cyber Essentials Toolkit : Chapter 1~6”, 2020f. 5. 11.

CISA, “Telework Essentials Toolkit”, 2020g. 10.

CISA, “CISA Insights - Cybersecurity Perspectives Healthcare and Public Health Response to COVID-19”, 2021. 1. 13.

ENISA, “Top Tips for Cybersecurity when Working Remotely”, 2020a. 3. 15.

ENISA, “Tips for cybersecurity when working from home”, 2020b. 3. 18.

ENISA, “Tips for cybersecurity when buying and selling online”, 2020c. 3. 31.

ENISA, “Tips for selecting and using online communication tools”, 2020d. 4. 27.

ENISA, “Understanding and dealing with phishing during the COVID-19 pandemic”, 2020e. 5. 6.

ENISA, “Cybersecurity in the healthcare sector during COVID-19 pandemic”, 2020f. 5. 11.

ENISA, “Securing smart infrastructure during the COVID-19 pandemic”, 2020g. 5. 18.

ENISA, “Top ten cyber hygiene tips for SMEs during COVID-19 pandemic“, 2020h. 6. 2.

FBI, “FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic”, 2020. 3. 30.

FBI & CISA, “Fbi and Cisa Warn Against Chinese Targeting of Covid-19 Research Organizations”, 2020. 5. 13.

Health Sector Cybersecurity Coordination Center, “COVID-19 Cyber Threats (Update)”, 2020. 8. 13.

Health Sector Cybersecurity Coordination Center, “2021 HPH Cybersecurity Forecast”, 2021a. 3. 11.

Health Sector Cybersecurity Coordination Center, “Ransomware Trends 2021”, 2021b. 6. 3.

HealthcareITnews, “Pfizer COVID-19 vaccine data leaked by hackers”, 2021. 1. 14.

Hijji, M. and Alam, G., “A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions”, *Access IEEE*, Vol.9, 2021, 7152-7169.

HIPAA Journal, “Cost of 2020 US Healthcare Ransomware Attacks Estimated at $21 Billion”, 2021a. 03. 11.

HIPAA Journal, “July 2021 Healthcare Data Breach Report”, 2021b. 8. 23.

Horn, I., Taros, T., Dirkes, S., Hüer, L., Rose, M., Tietmeyer, R., and Constantinides, E., “Business reputation and social media: a primer on threats and responses”, *Journal of Direct Data and Digital Marketing Practice*, Vol.16, No.3, 2015, 193-208.

Kaspersky, “COVID-19: Examining the threat landscape a year later”, 2121. 03. 15.

Kwak, Y. and Cho, Y., “Unmanned store, retailtech and digital divide in South Korea”, *Journal of Distribution Science*, Vol.17, No.9, 2019, 47-56.

Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., and Bellekens, X., “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic”, *Computers & Security*, Vol.105, No.1, 2021, 102248.

Lee, S. and Lee, D., “Untact: a new customer service strategy in the digital age”, *Service Business*, Vol.14, No.1, 2020, 1-22.

Lee, S. and Lim, S., *Living innovation: from value creation to the greater good*, Emerald Publishing, Bingley, 2018.

NIST, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”, 2015.

NIST, “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device(BYOD) Security”, 2016.

Paloalto, “Don’t Panic: COVID-19 Cyber Threats”, 2020a. 3. 24.

Paloalto, “Malicious Attackers Target Government and Medical Organizations With COVID-19 Themed Phishing Campaigns”, 2020b. 4. 14.

Pranggono, B. and Arabo, A., “COVID-19 pandemic cybersecurity issues”, *Internet Technology Letters*, Vol.4, 10.1002/itl2.247.

Pritom, M. M. A., Schweitzer, K. M., Bateman, R. M., Xu, M., and Xu, S., "Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses", *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2020, 1-6.

Reuters, "Elon Musk's SpaceX bans Zoom over privacy concerns", 2020. 4. 1.

SonicWall, "2021 SonicWall Cyber Threat Report", 2021. 3. 16.

Tessian, "Insider Threat Statistics You Should Know: Updated 2021", 2021. 06. 01.

The Guardian, "UK government told not to use Zoom because of China fears", 2020. 4. 24.

The Times of India, "Dr Reddy's admits to ransomware attack, says still restoring", 2020. 10. 28.

Weil, T. and Murugesan, S., "IT Risk and Resilience-Cybersecurity Response to COVID-19", IT Professional, Vol.22, No.3, 2020, 4-10.

Zoom, "End-to-End Encryption Update", 2020. 6.17, Available at https://blog.zoom.us/end-to-end-encryption-update/.

## About the Authors

**이 용 필 (pals@kisa.or.kr)**

서울대학교 경제학과 학사, 서울대학교 행정대학원 행정학 박사학위를 취득하였다. 2003년부터 한국인터넷진흥원에 재직 중이며, 정보보호산업기획팀장, 보안교육팀장, 사이버보안정책기획팀장, 융합보안단장 등을 역임하였다. 주요 관심분야는 사이버 보안 정책, 정보보호교육, 정보보호산업정책, 개인정보보호, 융합보안(IoT 보안 포함) 등이다.

**이 동 근 (leedg@kisa.or.kr)**

경북대학교 컴퓨터과학과 학사 및 석사를 취득하였다. 2003년부터 한국인터넷진흥원에 재직 중이며, 코드분석팀장, 사고분석팀장, 종합분석팀장, 사이버보안기획팀장, 침해사고분석단 등을 역임하였다. 현재는 침해사고 탐지 및 조치 등의 업무를 수행하는 침해대응단 단장을 맡고 있으며, 주요 관심분야는 악성코드 분석, 디지털 포렌식, 사이버 위협 정보 탐지 · 분석 · 프로파일링 등이다.