Journal of the Korea Convergence Society
Vol. 12. No. 1, pp. 1-9, 2021

ISSN 2233-4890 / eISSN 2713-6353
https://doi.org/10.15207/JKCS.2021.12.1.001

비대면 시대의 신 융합보안 위협과 대응 방안에 대한 고찰

유동현[1], 김용욱[2], 하영재[3], 류연승[4*]
[1]명지대학교 보안경영공학과 박사과정/육군대위, [2]명지대학교 보안경영공학과 박사과정/육군준장(예)
[3]명지대학교 보안경영공학과 박사과정/육군준장, [4]명지대학교 보안경영공학과 주임교수

Consideration of New Convergence Security Threats and Countermeasures in the Zero-Contact Era

Dong-Hyun Yu[1], Yong-Uk Kim[2], Young-Jae Ha[3], Yeon-Seung Ryu[4*]
[1]R.O.K Army CPT, Security Management Engineering, Graduate School, MyongJi University
[2]R.O.K Army Reserve BG, Security Management Engineering, Graduate School, MyongJi University
[3]R.O.K Army BG, Security Management Engineering, Graduate School, MyongJi University
[4]Head Professor, Department of Security Management Engineering, MyongJi University

요 약 최근 우리나라는 IT기술 발전 등의 환경 변화에 따라 새로운 유형의 보안 범죄가 꾸준히 발생하고 있으며, 이러한 위협에 대한 대응은 개인이나 기업뿐만 아니라 안전한 사회의 구축을 위해 국가 차원에서 수행되어야 할 핵심과제가 되었다. 한편 코로나19 팬데믹 이후 비대면 시대가 도래하면서 기존 IT발전에 따른 보안 위협과 비대면 시대의 특징이 결합된 신종 융합보안 위협이 우리 사회를 위협하고 있다. 이에 이러한 새로운 차원의 위협을 예방하고 교정하기 위한 연구가 지속 요구되고 있으며, 이를 위해 본 연구에서는 1장에서 신 융합보안 위협이 발생한 원인과 관련 선행연구를 살펴보고 2장에서는 비대면 시대에 주요 융합보안 위협 5가지로 사이버보안 · 가짜뉴스 · 원격투표 · 원격근무 및 영상보안 위협을 선정하여 유형별 특징에 대해 설명하였으며. 3장에서는 이에 대한 대응 방안의 논의와 정책적 함의를 고찰하였고, 4장에서는 결론과 함께 향후 연구방향을 제시하였다.

주제어 : 코로나19, 비대면, 융합보안, 가짜뉴스, 원격근무, 영상보안, 딥페이크

Abstract Recently, new types of security crimes have been steadily occurring in Korea due to environmental changes such as the development of IT technology, and responding to these threats has become a key national task for the establishment of a safe society as well as individuals and businesses. Meanwhile, as the Zero-Contact Era has arrived since the COVID-19 Pandemics, a new convergence security threat that combines the characteristics of the Zero-Contact Era with the existing IT development is threatening our society. Research to prevent and correct these new levels of threats is continuously required in this study. Chapter 1 examined the causes of new convergence security threats and Chapter 2 discussed cybersecurity, fake news, remote voting · work and video security threats as five major threats.

Key Words : COVID-19, Zero-Contact, Convergence Security, Fake News, Telecommuting, Video Security, Deepfake

*Corresponding Author : Yeon-Seung Ryu(ysryu@mju.ac.kr)
Received October 12, 2020 Revised December 18, 2020
Accepted January 20, 2021 Published January 28, 2021

1. 서론

우리나라는 코로나19 팬데믹 이후 비대면 시대가 도래하면서 원격근무, 1인 미디어, 온라인 투표 및 쇼핑 등 비대면 기반 산업이 급격히 발전하였다. 그러나 이러한 비대면 시대로의 빠른 전환은 다양한 측면에서 우리 사회의 제반 안전을 위협하고 있어 이에 대응하기 위한 연구는 지속해서 해나갈 필요가 있다. 한편 이러한 위협과 관련된 선행연구를 살펴보면 코로나19 이후 신안보 위협과 대응을 연구한 석재왕 외 1인은 코로나19 이후 발생하는 위협을 국가안보의 패러다임과 연결하여 '신안보'라는 새로운 개념의 제시와 함께 국가차원의 대응 방안을 제시하였으며[1], 이동휘 외 1인은 코로나19 관련된 위협을 사스·신종플루 등 과거 재난 시기의 위협과 비교하여 재난 시기에 위협이 증가하는 이유와 대응 방안을 제시 및 연구하였고[2], 오형근은 코로나19 이후 주요 사회적 변화와 향후 정보보안 이슈의 고찰 및 대응 방안을 제시하였다[3], 이에 본 연구는 이러한 코로나19 이후 위협에 대한 대응을 주장한 선행연구에서 착안하여 그 관점을 코로나19 관련 '신 융합보안 위협'에 중점을 두고 위협분석 및 대응방안을 고찰하였으며 이를 통해 사회차원의 대응을 위한 정책적 함의를 제시하고자 한다. 이를 위해 2장에서는 비대면 시대의 주요 신 위협의 유형을 제시하였고 3장에서는 이러한 위협에 대한 대응 방안을 분석하였으며, 4장에서는 결론과 더불어 향후 필요한 연구를 제시하였다.

2. 비대면 시대의 신 융합보안 위협

과거 사스·신종플루 등 사태에서 증명되었듯이 사람들은 어떠한 재난상황과 안전이 위협되는 상황이 발생하였을 때 불안한 심리를 가지게 되며, 이와 관련된 신속한 정보를 습득하길 원한다. 공격자들은 이러한 사람들의 불안한 심리를 악용하여 새롭고 다양한 방법으로 사회안전을 위협한다[4]. 2장에서는 이처럼 비대면 시대 환경에서 기존에는 없었거나 혹은 진보된 대응이 요구되는 신 융합보안 위협의 유형을 살펴보았다.

2.1 사이버 보안 위협

KAIST 사이버보안 연구센터에 따르면 코로나19 전과 후의 같은 시기('19.1~9월)의 악성 웹 탐지 건수를 비교해 봤을 대, '19년 대비 '20년에는 약 43%가 증가했다. 올해 탐지된 악성코드는 Tojan이 44%로 가장 많았고, Ransomware가 36%, Backdoor가 15%로 뒤를 이었는데, 이러한 것들이 시사하는 것은 지난해와 비교했을 때 사이버 공격이 크게 증가했다는 것이다. 또한 Palo Alto에 다르면 최근 웹상에 신규 등록된 도메인 중 코로나19(COVID-19) 관련 키워드 도메인이 40% 이상을 차지했는데, 이는 코로나19와 관련된 주제의 악의적인 공격을 다각적인 측면에서 깊이 있게 통찰한 필요가 있음을 나타낸다. 국내에서 많이 발생한 공격기법으로는 피싱(Phishing)을 통해 특정 사이트로 유도 후 개인정보를 수집하거나 악성 웹 설치를 유도하는 것으로, 이를 통해 개인 스마트폰 원격 조정 및 데이터를 수집하는 방법 등이었으며, 구체적으로는 코로나19 관련 위장메일을 통한 워터링 홀(Watering Hole) 공격이나 드라이브 바이 다운로드(Drive-by-downloads)에 의한 악성코드 유포 공격을 꼽을 수 있다[5]. 이러한 공격은 주로 '코로나19와 관련된 단어를 사용하거나 주요 관련기관(질병관리청, 마스크 판매업체, 검·경등 수사기관)을 사칭하는 문자메세지나 이메일을 활용하는 지능형 지속공격(Advanced Persistent Threat) 기법으로 이뤄지며 있다. 또한 딥페이크(Deepfake)를 통해 직장 상사의 목소리로 위장하여 부하직원에게 송금을 유도한다거나 하는 방식도 주요 위협중 하나이다. 이러한 방법들은 대체로 적은 비용으로 공격자가 수익을 얻을 수 있는 구조이므로 오늘날과 같은 비대면 시대에서 끊임없이 지속될 것으로 예상된다.

2.2 가짜뉴스 위협

오늘날은 다양한 플랫폼으로 개인방송이 영향력을 행사하는 '1인 미디어' 시대이며, 이는 비대면 시대에 이르러 우리나라 사회 전반에 더 큰 영향력을 행사하고 있다. 이러한 1인 미디어는 시청자가 곧 돈이 되는 경제적 특징을 가지고 있으므로 방송자들은 항상 더 많은 시청자를 모으기 위해 다양한 방법을 고민한다. 이러한 특징과 비대면 시대 환경에서 사람들의 불안한 심리가 결합되면서 일부 악의적인 공격자에 의한 자극적이고 선정적인 가짜뉴스들이 생산 및 유포되기에 이르렀다[6]. 이러한 가짜뉴스들은 사회 제반안전에 심각한 악영향을 끼칠 수 있는데, 최근 우리나라의 경우를 예로 들면 악의를 가진 공격자들이 정부 방역정책과 관련된 가짜뉴스를 유포하여 대정부 신뢰도를 훼손시키거나 아래 Fig. 1과 같이 코로나 확진자 관련 가짜뉴스들을 퍼트려 사람들의 심리를 위축시키기도 했다. 특히 진보된 AI 기술은 더욱 진위를 가리기 힘든 가짜뉴스를 생산할 수 있는데, 딥페이크 형

태의 가짜뉴스는 유명 경제인 및 정치인의 얼굴과 목소리를 흉내내며, 이는 육안으로 쉽게 진위를 가리기 힘든 수준이다. 이렇듯 딥페이크의 악용은 비대면 시대의 불안한 심리를 가진 사람들을 현혹하고 글로벌 기업의 산업보안과 대선 및 총선 등 사회 주요 사항에 대해 계속해서 악영향을 끼칠 것이다[7].

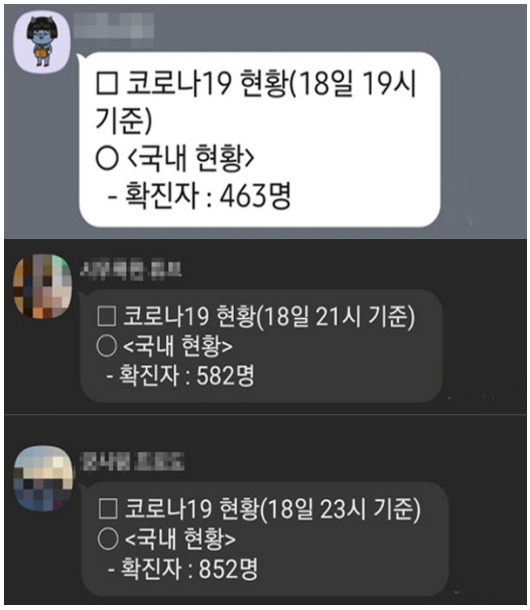

Fig. 1. Fake News Related to Coronic[8].

2.3 원격투표 보안 위협

'20년 7월 우리나라 정부는 '한국판 뉴딜' 정책을 발표하면서 포스트코로나 시대의 비대면 서비스 확대 및 디지털 인프라 구축을 주요 골자로 하는 내용을 발표했다. 이중에서 특히 주목할 부분 중 하나가 원격투표 제도의 활성화이다. 우리나라는 K-Voting 시스템을 통해 코로나19 이전부터 원격투표를 실시하고는 있지만 예능방송을 위한 인기투표 등 일부에서만 활용되고 있으며, 다양한 보안위협으로 인해 대선·총선 및 지자체장 선거 등 정치적으로 중요한 선거에 투입하기는 시기상조로 판단되어진다. 이는 해외에서도 마찬가지로 영국의 경우 2001년 이후 Kiosk, 인터넷, 모바일 등 다양한 방식의 원격투표를 도입했고 2008년 처음으로 의회 선거에서 활용되었지만 종료 후 개표 과정에서 투표된 용지 일부 식별해 실패하여, 여러 시민단체의 반대로 원격투표를 통한 정치참여가 전면 취소됐다. 한편 2004년에는 유럽의회 선거에서 REV 기법을 도입한 원격투표가 실시되면서 전 세계적인 원격투표제 시행이 예고 되었다. 그러나 2006년 한 시민단체가 원격투표의 안정성에 대한 결함을 증명하면서 공개하면서 결국 원격투표는 전면 금지됐다. 이후 원격투표를 대선·총선·지방선거등에 활용한 국가는 없었지만 이제는 이런 것들에 대한 논의가 다시 이뤄져야할 시점이다. 팬데믹으로 인한 비대면 시대에도 종이투표를 고할 경우에는 전염병 확진자 발생확률이 높아지거나 전체적인 투표율이 낮아져서 국민의 정치참여가 제한될 수 있다. 따라서 앞서 언급한 원격투표의 보안상 문제점을 해소해야 하는데, 국가의 경제·정치적 중요한 선거에 원격투표를 활용할 경쟁상태의 있는 상대국가의 정보기관이나 불법조직 등이 선거시스템을 침입하여 투표결과가 조작될 수 있으므로 원격투표에 대한 보안위협은 대책 마련이 시급한 과제이다.

2.4 원격근무 보안위협

2.4.1 융합보안 위협

원격근무는 업무수행자가 직장의 정해진 공간이 아닌 외부의 다른 어떤 공간에서 업무를 보는 환경의 총칭이며, 이러한 환경은 조직에 출근해서 내부망으로 업무를 보는 것에 비해 보안이 허술할 수 밖에 없다. 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 표적이 되고 있다. 이러한 원격근무 환경의 보안위협을 융합보안(관리·물리·기술적) 측면에서 살펴보면 첫째, 관리적 측면에서는 참석자에 대한 신원인증 문제와 원격·화상회의가 비대면 방식으로 진행되므로 업무도중 다양한 보안공격에 노출될 수 있으며, 원격근무 시 잠시 자리를 비운 경우 제3자에 의해 자료가 위·변조, 탈취 될 수 있는 위협이 존재한다. 둘재, 물리적 보안 측면은 장비 자체가 조직 내부가 아닌 외부에 위치하므로 도난 및 분실문제가 발생할 수 있고, 개인의 PC를 사용해서 직장 내부망에 접속하는 것은 직장의 기밀자료를 집에서도 열람이 가능해지는 것이고 이러한 자료들이 로컬 등에 보관될 경우 기밀유출 사고가 발생할 위험이 존재한다. 세 번재 기술적 보안 측면에서는 사용자 단말기의 보안취약으로 악성코드에 감염될 경우 단일실패지점(single point of failure)이 되는 점과, 원격근무에 사용되는 네트워크 환경이 안전하지 않을 경우 내부 데이터가 유출될 수 있는 것들을 나열할 수 있다[9].

2.4.2 VPN 보안 위협

원격근무자와 직장의 네트워크 연결 시 망을 분리하는 것은 비용이 비싸기 때문에 원격접속시 공중망을 사용하면서 망분리 효과를 가져오는 VPN을 이용한 패킷 암호화가 선호되고 있다. 그러나 VPN의 사용도 안전성을 100% 보장해주지는 못한다. 첫째로 VPN 솔루션 자체가 공격대상이 되는 점이 있다. 최신 패치가 되지 않은 VPN의 경우 쉽게 /etc/passwd 및 VPN DB의 노출이 빈번하게 일어난다. 또한 VPN 업무환경이 구축되어 있더라도 대부분의 제품은 장비 1대당 접속자 수가 제한되어 있기 때문에 원격근무 추가 소요가 발생할 경우에는 라이선스를 추가 구입해야 하는데, 이러한 경우 급격한 트래픽 증가로 VPN의 가용성이 제한될 수 있다. 이는 분산서비스공격(DDoS) 공격에 대한 취약성을 초래한다. 두 번째로 RDP 공격 위협이다. 이 기법은 전통적으로 공격자들이 선호하던 기법으로, 최근에는 대부분의 기관들이 최신 OS를 사용하여 원격 데스크톱을 통해 쉘을 획득하는 공격이 제한된다고는 하지만 아직도 최신 운영체제를 사용하지 않는 경우 공격자에 의해 쉘이 탈취될 수 있는 위협이 존재한다.

2.5 영상보안 위협

2.5.1 열화상카메라 보안 위협

비대면 시대 도래 이후 정부의 방역 정책으로 인해 다중이용시설 및 관공서 입구에서 쉽게 열화상카메라를 발견할 수 있으며, 최근에는 방역과 보안의 기능을 결합한 열화상 CCTV도 많은 곳에 설치되어 있다. 그러나 이러한 카메라 일부 제품은 사용자의 얼굴사진을 자동으로 저장하고 삭제되지 않는 문제점이 있는 것으로 확인되었다[10]. 얼굴 사진은 특정인을 식별할 수 있는 분명한 개인정보이며 이러한 것들이 정보주체의 동의 없이 촬영되고 저장되는 것은 명백한 불법인 동시에 개인정보 자기결정권이 보장받지 못한다는 점에서 헌법적 가치의 훼손이기도 하다. 이는 비대면 시대의 주요 위협으로 간주되고 있다.

2.5.2 화상회의 보안 위협

코로나19 이후 가장 중요한 업무매체인 화상회의를 진행하면서 안전성을 보장받기 위해서는 기관/기업에서 승인된 안전한 플랫폼과 단말기, 그리고 보안접속 프로그램(VPN)이 필요하다. 이 중에서 특히 플랫폼 전용장비는 기관/기업에서 직접 구축하는 방식과 클라우드 SaaS 서비스를 이용하는 방식으로 나눌 수 있는데, 각 방식에 위협이 되는 부분은 동일하다. 이를 자세히 살펴보면 첫째, 영상회의에 허가받지 않은 사용자가 회의실에 무단으로 접속할 수 있는 것이 있고 둘째, 사무실의 위치 · 개인정보 등이 카메라로 보여지면서 사용자의 민감정보가 노출될 수 있다. 셋째, 영상회의 통신이 암호화가 되어 있지 않은 경우 회의 데이터가 유출될 가능성이 존재한다.또한 화상회의에서도 영상과 음성이 합성된 딥페이크는 여전히 주요 위협 중 하나다[11].

3. 비대면 시대 신 융합보안 위협 대응

코로나19 팬데믹은 방역과 안보를 막론하고 기존의 위협에 대한 방어개념을 완전히 바꿔놓았는데, 이를 비유하면 코로나19 이전은 전쟁에서 국경선의 경계만 완벽하게 해내면 적의 침투를 차단할 수 있었는데 비해 비대면 시대에는 그러한 경계선 자체가 사라진 것에 비유할 수 있다. 이렇듯 3장에서는 새롭게 발생한 융합보안 위협에 대해 기존위협과 비교하여 어떻게 대응할 것인가의 방법론을 논의하였다.

3.1 사이버 보안 위협 대응

첫째, 정기적인 보안인식 교육을 실시하는 것은 새로운 위협들에 대해서도 여전히 가장 기본적인 해결책 중 하나이다. 앞서 살펴본 주요 사이버 위협인 피싱 · 스미싱(SMishing) 및 랜섬웨어도 정기적인 보안교육을 통해 최소화 할 수 있다. 직장 내 보안관리자(CSO)는 연간 보안교육 계획을 작성할 때 비대면 시대에 적용해야할 위협대응 방안 및 인식제고를 포함해야 하며, 반드시 최고관리자(CEO등)의 서명을 받아서 이를 실시해야 한다[12]. 또한 이러한 것들의 교육 이수여부를 상여금 심의 시 적극 반영하고 정기적으로 평가(필기 · 행동화)를 실시하여 우수자에게 승진가점을 부여하면 상기 위협들에 대해 안전함을 보장받는데 도움을 줄 것이다. 둘째, 직장 내 보안 바운티 제도의 운영이다. 이는 조직원의 심리를 강화함으로써 위협요소를 최소화 할 수 있다. 예를 들어 상기 위협들은 대게 주소나 전화번호 등의 링크가 걸려 있고 공격자들은 이것을 눌러보고 싶도록 사용자를 궁금하게 만드는데, 보안 바운티 제도가 운영되는 조직은 이러한 공격의 궁금증 보다도 승진 · 포상 등을 필요로 하게 되므로 이를 예방할 수 있는 것이다. 셋재, 직장 보안내규를 정비해야 한다. 조직의 보안내규를 관리 · 물리 · 기술적

위협 및 대응으로 장을 나누고 구체적인 위협과 사용자 준수사항을 명시해야 한다. 예를 들면 '모든 구성원은 악성 앱의 방지를 위해 구글·애플 앱스토어 등 공식적인 것만 사용해야 하며, 보안업데이트가 중단된 앱은 지체없이 삭제 해야 한다'거나, '사용 계정의 2차 비밀번호 인증을 반드시 활성화해야 한다' 등이 포함되어야 한다. 이러한 것들을 기관/기업의 조직내규로 명문화함으로써, 미준수시 일벌백계한다면 결과적으로 사회 전반의 사이버 안전 구축에 도움이 될 것이다. 이를 정리하면 아래 Table 1과 같다.

Table 1. Zero-Contact Cyber Threats Maneuver

Zero-Contact Cyber Threats Maneuver	
1. Strengthen Security Education	· Regular security education mandatory · The security education plan must be signed by the CEO · Giving disadvantages in case of Zero-recurring
2. Operating the Security Bounty System	· Compensation for the reporter by promotion, reward, etc.
3. Establishing Security by laws	· Operate a security organization (person in charge) in the workplace · Designation of regular security education obligations · Review of security-related performance bonuses

3.2 가짜뉴스 위협 대응

가짜뉴스 위협은 최근 전 세계적으로 화두가 되고 있다. 먼저 이러한 위협과 관련된 해외 대응을 살펴보면, 미국의 경우 SNS기업 및 언론기관이 연대하여 가짜뉴스를 최소화 하고자 하는 노력을 하고 있다. 특히 트위터(Twitter)의 경우, 사실이 아니거나 의심되는 글이 게제되면 추가검증이 요구된다는 메시지와 함께 이를 검증할 수 있는 사이트를 제공해주는 정책을 시행중에 있다. 프랑스의 경우는 프랑스TV, 리베라시옹 등 주요 언론기관들이 협력하여 팩트에크 기관인 '크로스체크'를 만들어 가짜뉴스 위협에 대응하고 있다[13]. 크로스체크는 신고된 사안이 허위일 때에는 사안에 '허위정보' 표식을 게시하는 방법으로 대응하고 있다. 특히 독일의 경우는 한층 강력한 대응을 시행중인데, '18년 6월 'SNS상의 법 집행 개선에 관한 법률' 및 동 시행령을 통해 가짜뉴스나 혐오표현에는 5천만 유로 이하의 벌금을 부과하는 등 형사처벌을 통해 이를 통제하고 있다. 이와 같이 세계 주요국들이 글로벌 SNS 기업등과 연대하여 주도적으로 가짜뉴스에 대응하고 있다. 우리나라도 이와 같이 정부 당국과 함께 주요 SNS 및 포털사이트 제공기업의 공조와 협력이 중요할 것으로 생각되며, 이에 대한 모니터링과 더불어 형사처벌을 포함하는 법·제도적 접근이 병행되어야 한다. 구체적으로 살펴보면 방통위, 행안부(경찰청) 등 정부기관에서 국내 웹 포털 및 SNS서비스 플랫폼과연계하여 코로나19와 연관된 가짜뉴스 유통방지를 위한 TF를 구성하여 운영하는 방법이 가짜뉴스 억제에 도움을 줄 것이다. 특히 딥페이크의 경우, 법·제도적 대응뿐 아니라 기술적 대응에 관한 논의도 본격화 해야 한다. 이를 위해 경찰청 내 딥페이크를 탐지하는 전문부서를 신설하고 과기부와 KISA에서 이를 위한 기술고문 역할을 해주면 향후 가짜뉴스 탐지 및 색출이 쉬울 것이다. 주요사항을 정리해보면 아래 Table 2와 같다.

Table 2. Countermeasure for Fake News Threats

Countermeasure for Fake News Threats	
1. Cooperation between SNS companies and government agencies	· Strengthen monitoring of fake news through cooperation between the public and private sectors · Fake news distribution prevention TF operation
2. Establishment of Deepfake Specialized Investigation Organization	· Establishment of a specialized investigation organization within the National Police Agency · Ministry of Science and Technology, Korea Internet Security Agency (KISA) serves as a technical advisor

3.3 원격투표 보안 위협 대응

다양한 위협에도 불구하고 온라인투표 확대는 비대면 시대에 반드시 발전시켜야할 핵심기술이다. 이를 위해 블록체인 기술의 활용을 고려해볼 수 있다[14]. 먼저 신원이 확인된 투표자의 모바일앱 내부에서 블록체인 키쌍(PKI 기반)을 생성하고 신원인증 전자지갑을 구성한다. 이후 선관위는 블록체인에 미리 등록된 스마트 계약서를 통해 투표자에게 토큰을 전송하되 이 때 중복투표게 제한되도록 후보자의 주소로 토큰을 전송한다. 한편 투표정보는 다양한 파라미터를 가지도록 설계하여 누가 누구에게 투표했는지 추측할 수 없도록 솔팅된 해쉬값, 블록넘버 등의 기법을 활용한다. 마지막으로 생성토큰 양과 전송토큰의 양을 비교하교 투표가 자동종료 되도록 설계하면 최소한의 익명성 확보와 더불어 외부 공격자의 위협을 최소화 할 수 있을 것이다. 물론 이러한 방법이 선조작의 위협으로부터 완전히 안전하다고 단언하긴 힘들다. 그러나 이러한 투표시스템을 중요도가 비교적 낮은 선거나 기타 투표 등에 활용하면서 계속해서 취약점을 발견 및 보완하며 이와 관련된 법·제도를 정비해 나간다면 향후 총선이나 지방선거 등 주요선거에 활용하는 것도

고려할 수 있을 것이다. 이러한 것들은 향후 비대면 시대의 안전한 원격투표를 보장하는 밑거름이 될 것이다. 이를 정리하면 아래 Table 3과 같다.

Table 3. Remote Voting Security Threat Maneuver

Remote Voting Security Threat Maneuver	
1. Block chain-based remote voting	· Create a block chain pair inside the voters' mobile app → Organize an ID card electronic wallet · Voting Token Sent (Counselor → Voter Address) · Use Solting Hash, Block Number, Symbol Number for Voting Information · Comparing the amount of token generated with the amount of token transferred and setting the voting to end automatically
2. Try to resolve the vulnerability	· Continue to identify and remediate vulnerabilities · Continuous maintenance of relevant laws and systems

3.4 원격근무 보안 위협 대응

3.4.1 융합보안 위협 대응

원격근무 환경에서 다양한 보안위협들로부터 안전을 보장 받기 위해서는 보안관리자에 의한 올바른 보안정책이 수립되는 것이 중요하다. 이를 정리해보면 다음과 같다. 첫째, 원격근무자가 기관/기업의 내부 네트워크에 접속하는 경우 2차 인증 등 다양한 인증방안을 사용하도록 해야 한다. 둘째, 각 개인이 계정을 공유할 수 없도록 접근통제 모델을 적용하여 개별 사용자마다 구분된 권한을 부여해야 한다. 이를 통해 접속이력, 출발지 및 목적지 등을 모니터링 할 수 있다. 셋째, 원격근무시 내부망에 접근하도록 하는 보안접속 프로그램은 허가된 사용자와 단말기 만이 접근할 수 있도록 환경을 구축해야 한다. 이때 트래픽 경로를 단일화하여 모니터링의 가시성을 확보해야 한다. 뿐만 아니라 이러한 정책의 효율을 극대화 할 수 있도록 직장 내 보안내규 정비도 병행하는 것이 좋다. 보안의 준수는 결국 사용자의 편의성이 일부 제한되는 것이므로 규정을 통한 통제와 신상필벌로서 보장할 수 있다. 원격근무간 관련 보안내규에 명시되어야할 사용자 준수사항은 다음과 같다. 첫째, 원격근무는 항상 보안성이 보장되는 전용공간에서 실시되어야 하며, 둘째, 기관/기업에서 허가된 프로그램만을 사용하되 보안성이 증명되지 않은 임의의 프로그램을 사용해서는 안된다. 넷째, 신뢰할 수 없는 개방형 Wi-Fi는 사용하지 않도록 통제해야 하며 비밀번호는 최소 9자 이상에 문자·숫자·특수문자를 조합하여 사용해야 한다. 다섯째, SNS나 이메일에서 출처가 불분명한 웹사이트 링크를 함부로 클릭하거나 첨부파일 실행을 금지해야 한다. 마지막으로는 서버기반 자산관리 시스템의 도입을 통해 내부 기밀유출을 방지할 수 있다. 문서 중앙화 솔루션과 같이 원격근무중 생성되는 모든 문서가 중앙서버에 저장되고 관리되는 모델은 효율적인 자산의 관리가 가능하며 랜섬웨어 위협도 최소화 시킬 수 있으며, 아래 Table 4는 상기 대응방안의 요약이다.

Table 4. Telecommuting Security Threats Maneuver

Telecommuting Security Threats Maneuver	
1. Establishing network policies related to telecommuting	· 2nd certification activation obligation · Don't share accounts · Only authorized users and terminals access the internal network · Single traffic paths when using VPN
2. Maintenance of Security by laws	· Remote work only in a dedicated space · Use approved devices only · No program, no open Wi-Fi · Use strong password · Do not click on unclear link
3. Introduction of a Server-Based Asset Management System	· Save and manage all internally generated documents on a central server · ntroduction of document centralization solution

3.4.2 VPN보안 위협 대응

악성코드가 VPN을 통해서 전파되는 경우에는 암호화로 인해 전달 과정에서 탐지 및 통제가 어렵다. 즉 VPN에서 데이터의 암호화뿐 아니라 암호화가 끝나는 단(End)에서 위협 탐지·통제 기능을 강화시키는 것은 VPN위협 대응에 방법이 될 수 있다. 또한 문서 보안 솔루션을 활용하여 중요정보의 경우 문서 출력기능을 제한하는 것은 VPN 보안 위협 해소에 큰 도움이 될 것이다. 이외에도 원격근무에 활용되는 단말기는 항상 최신 OS와 보안패치 및 백신프로그램이 운용되어야 하며, 이러한 것들을 기관/기업 보안내규에 반영하여 직접사용자에 의한 정기적인 확인 및 업데이트 실시의 의무를 부여하면 위에 설명한 위협들의 대한 대응이 될 수 있다.

3.5 영상보안 위협 대응

3.5.1 열화상카메라 보안 위협 대응

현재는 열화상카메라 사용자가 마음만 먹으면 얼마든지 개인얼굴을 촬영 및 저장할 수 있는 환경이다. 이를 방지하기 위해서는 정부기관 및 화상카메라 서비스 제공업체의 공조를 통해 문제를 해결해야 한다. 각 지자체별 코로나19 대응팀이 운용중이지만 좀 더 효율적으로 위협에 대응하기 위해서는 정부차원에서 개인정보보호위원회

가 기능을 적극 발휘해야 한다. 개인정보보호위원회는 인원 및 예산 등을 증강하여 영상보안 총괄TF를 구성하고 이와 관련된 보안법제를 정리해야 한다. 이때 특히 모든 열화상카메라가 설치된 기관은 특별한 경우(대테러 대응 등)를 제외하고는 Auto-Delete 기능이 탑재된 제품을 사용하도록 하는 것을 포함해야 한다. 또 TF내에 순찰조직을 편성하여 정기·수시로 열화상카메라 설치업체를 방문하여 규정여부를 확인하고 계도를 실시해야 한다. 이렇게 편성된 영상보안 지도팀은 순찰 뿐 아니라 정기적으로 보안감사를 실시하고 개인정보보호위원회로 결과를 보고해야 하며, 개인정보보호위원회는 보고된 사항을 해결하기 위한 적절한 정책을 마련하여 열화상카메라에 의한 보안위협을 극복해야 한다.

3.5.2 화상회의 보안 위협 대응

외부자 공격으로부터 안전한 화상회의를 보장받기 위해서는 첫째, 네트워크 보안체계의 강화이다. 차세대 방화벽이나 네트워크 접근제어(NAC)등을 최신버전으로 유지하여 랜섬웨어, APT등 보안위협에 효과적으로 대응해야 한다. 둘째, 보안수칙 준수를 통한 피해의 최소화이다. 이를 정리해보면 ① 기관/기업에서 승인된 체계 및 단말기만 사용하여 화상회의에 참여해야 한다. ② 보안 업데이트를 주기적으로 체크한다. 공격자들이 계속해서 새로운 방법으로 원격회의에 침투해서 내용을 유출하는데, 보안 업데이트가 선행되지 않으면 화상회의 서비스 주체에서 제공하는 최신 보안솔루션을 제공받을 수 없다. ③ 회의방 무단 침입방지를 위한 PIN을 설정하고 비밀번호 재사용 금지 원칙을 준수하는 것이다. ④ 회의 웹주소와 비밀번호는 필수인원 외에는 공개하지 않아야 한다. ⑤ 모든 참여자가 회의방에 입장한 뒤에는 잠금(Locking) 기능을 활용하여 업무상 관련 없는 제 3자의 접근을 차단해야 한다. ⑥ 회의내용의 녹화를 금지하고 회의 주최자만 PC화면 공유 기능을 가져야 한다. 특히 불필요한 사적대화를 차단하는 것은 보안 유지에 도움이 될 것이다. 한편 비정기적으로 실시되는 회의에서는 딥페이크 위협이 있을 수 있다. 이때 참여자의 명확한 신원을 체크하기 위해서 영지식 증명(Zero-Knowledge Proof)의 활용을 생각해 볼 수 있다. 회의가 시작되기 전에 회의 참여자 전원의 얼굴 및 목소리를 확인하고, 회의 참여자가 서로 정말 아는 사람들이 맞는지 상호 간에 생활정보를 간단한 퀴즈형식으로 하여 확인하는 것이다. 이러한 신원 확인은 아래 Table 5처럼 영상보안 위협에 대한 예방책이 될 수 있다[15].

Table 5. Videoconferencing Security Threats Maneuver

Videoconferencing Security Threats Maneuver	
1. Compliance with safety rules for video conferencing	· Using an approved device (Security Update Periodic Check) · Password reuse prohibition principle (Do not unauthorized disclosure of passwords) · Lock Video-Conference Room, Do not record meeting contents
2. Deepfake Attack Video Meetings Maneuver	· Check the faces and voices of all participants of the meeting before the meeting begins · To check whether the participants of the meeting are really people who know each other, using simple quizzes to check each other's living information. (Zero-Knowledge Proof)

이와 같이 3장에서는 2장에서 다룬 5가지의 신 위협의 대응방안에 대해 논의하였는데, 이를 쉽게 정리할 수 있도록 앞서 언급한 위협 전체와 대응방안 및 기존의 보안위협과 차이점을 최종 요약하면 아래 Table 6과 같다.

Table 6. Total Threats and Countermeasures

Total Threats and Countermeasures	
1. Organize Overall Threats and their Counter measures	· Cyber Security - Strengthen Security Education(must be signed by the CEO) - Run the Security Bounty System, - Establishing Security by laws · Fake News - Cooperation between SNS companies and government agencies - Establishment of Deepfake Specialized Investigation Organization · Remote Voting - Blockchain-based remote voting - Continue to identify and supplement vulnerabilities and improve relevant law systems · Remote Work - Establishing network policies related to telecommuting and Maintenance of Security by laws - Strengthen threat detection and control at the end of VPN encryption - Leverage document security solutions · Video Security - Organize related security legislation - Using products with auto-delete capability - Using Zero-Knowledge Proof for Deepfake Prevention
2. Differences from existing threats	· Changes in the Information Technology Environment - Spreading the Zero-Contact keynote - Realize the use of artificial intelligence · The emergence of new convergence security threats. - Continuing new attack techniques are combined with zero-contact - Threats to political and public sectors such as fake news and remote voting issues · Under these Zero-Contact situation, the impact of hacking attacks is far higher than offline, which can paralyze the national system by clicking.

4. 결론

우리 사회는 비대면 시대를 맞이하면서 과거 경험해보지 못한 다양한 환경을 강제적으로 경험하며 허둥지둥 적응해 나가고 있다. 이러한 상황에서 발생하는 다양한 위협에 대응하기 위해 가장 관심가져야 할 것은 앞서 논의한 바의 핵심이 되는 제로 트러스트(Zero-Trust) 모델에 기반한 안전한 사회의 구현이다. 이는 곧 무엇이든 쉽게 믿어서는 안되는 것의 강조이며, 한번 더 확인하는 것이 우리 사회의 안전성을 더욱 견고하게 한다는 의미를 담고 있다. 지금 정부에서 추진하고 있는 '한국판 뉴딜(디지털 뉴딜)' 정책도 이러한 모델에 기반하여 진행되어야 한다. 모든 추진과제에 반드시 현재 및 미래 예상되는 융합보안 위협에 대한 대응개념이 포함되어야 비대면 상황에서 안전하게 목표한 대로 성과를 달성할 수 있을 것이다. 이를 위해 본 연구에서는 비대면 시대의 주요 신 융합보안 위협들을 살펴보고 대응방안을 논의하였다. 그러나 트윈데믹(Twindemic)과 같은 더 강력한 비대면 시대가 도래할 수 있음에 따라 새롭고도 다양한 위협은 지속해서 생겨날 것이다. 따라서 향후 지속적으로 비대면 시대 융합보안 위협의 진화 양상을 추적하고 새로운 공격의 분석 및 대응은 계속 연구되어야 할 과제이다.

REFERENCES

[1] J. W. Seok & I. S. Oh. (2020). Political and Social Changes and Risk Management Since Corona19. *Korean Security Journal, (64)*, 117-136. DOI: 10.36623/kssr.2020.64.5

[2] D. H. Lee & H. A. Kim. (2020). A Study on Security through Case Analysis of Corona19 Related Cyber Attacks. *Korean Society of Information and Communication, 24(1)*, 548-550.

[3] H. G. Oh. (2020). Analysis of major social changes and information security issues after COVID-19. *Communications of the Korean Institute of Information Scientists and Engineer, 38(9)*, 48-56.

[4] D. W. Kim & K. B. Lee. (2019). A Study on the Classifying the Type of Social Engineering Attacks, *Korean Journal of Industrial Security, 9(2)*, 9-21. DOI: 10.33388/kais.2019.9.2.009

[5] M. S. Jung & H. B. Jang. (2020). The Case Study of Technology Leakage in Cyber-Physical Space, *Korean Journal of Industrial Security, 10(2)*, 151-179. DOI: 10.33388/kais.2020.10.2.151

[6] H. J. Lim. (2020) The Impact of COVID-19 on Crime -Focused on 112 Report Data, *Korean Security Journal, (Special)*, 233-254. DOI: 10.36623/kssr.2020.pandemic.233

[7] B. K. Koo. (2019. 10. 3). Deepfake detection technology, will you become a fake news troubleshooter?, *The Hankyoreh,* Retrieved from http://www.hani.co.kr/arti/science/future/911878.html

[8] T. H. Kim. (2020. 11. 19.). "850 new confirmed cases?"... Ask the police to investigate Fake News. *Segye news*. Retrieved from https://www.segye.com/newsView/20201119509842

[9] Korea Internet Security Agency. (2020. 6. 24). Security Guide for Introduction and Operation of Zero-Contact Work Environment[Guide and Manual]. Retrieved from https://www.boho.or.kr/data/guideView.do?bulletin_writing_sequence=35467

[10] H. J. Son. (2020. 11. 12). No saving of thermal imaging camera pictures..." Violation of regulations? I don't know." *YTN*. Retrieved from https://www.ytn.co.kr/_ln/0103_202011120543155750

[11] S. K. Bae. (2020) A Study on Criminal Regulations against Deepfake porn, *Law Research Institute Center for International Area Studies Hankuk University of Foreign Studies, 43(3)*, 169-187. DOI: 10.17257/hufslr.2019.43.3.169

[12] J. Y. Jung & Y. H. Kim. (2020) South Korean Cyber Security Threats, Governance Measures, and Implications for SMEs, *Korean Journal of Industrial Security, 10(1)*, 81-109. DOI: 10.33388/kais.2020.10.1.081

[13] N. R. Jang. (2018. 10. 2). How do foreign countries respond to fake news with hate speech?. *The Hankyoreh,*. Retrieved from http://www.hani.co.kr/arti/society/society_general/864204.html

[14] Smartgrid. (2020. 4. 14) 'How long will the stamp vote last? Will block-chain voting be the solution?[Online Blog]. Retrieved from https://bloodkorea.com/bl_news/1001769

[15] M. S. Kim. & B. R. Kang. (2015) Generalization of Zero-Knowledge Proof of Polynomial Equality, *The Journal of the KICS, 40(5)*, 833-840. DOI: 10.7840/kics.2015.40.5.833

유 동 현(Dong-Hyun Yu) [정회원]

· 2018년 9월 : 명지대학교 융합보안학과 (석사)
· 2018년 9월 ~ 현재 : 명지대학교 보안경영공학과 박사과정
· 2020년 10월 ~ 현재 : 행정안전부 안전교육 전문인력 (정보통신안전)
· 관심분야 : 국방보안, 방위산업보안, 무기시스템 보안
· E-Mail : dhy8906@naver.com

김 용 욱(Yong-Uk Kim) [정회원]

· 1991년 4월 : 육군3사관학교 경영학과 (학사)
· 2012년 8월 : 한양대학교 무역경영학과 (석사)
· 2018년 3월 ~ 현재 : 명지대학교 보안경영공학과 박사과정
· 관심분야 : 통합방위법, 국방보안, 드론 보안
· E-Mail : kywhkc@naver.com

하 영 재(Young-Jae Ha) [정회원]

· 1988년 2월 : 연세대학교 화학과 (학사)
· 2004년 2월 : 한남대학교 안보국방정책(석사)
· 2018년 9월 ~ 현재 : 명지대학교 보안경영공학과 박사과정
· 관심분야 : 사이버 안보, 무기체계 보안, 방산기술 보호
· E-Mail : espana01@hanmail.net

류 연 승(Yeon-Seung Ryu) [정회원]

· 1990년 2월 : 서울대학교 계산통계학과 (학사)
· 1992년 2월 : 서울대학교 전산과학과 (석사)
· 1996년 8월 : 서울대학교 전산과학과 (박사)
· 2015년 3월 ~ 현재 : 명지대학교 보안경영공학과 주임교수
· 2017년 1월 ~ 현재 : 방산기술보호 연구회 위원장
· 관심분야 : 시스템 보안, 무기체계 보안, 방산기술 보호
· E-Mail : ysryu@mju.ac.kr