https://doi.org/10.5392/JKCA.2022.22.09.104

뉴노멀 시대의 공공기관 원격보안 모델 개선방안

Improvement Plan for Public Institution Remote Security Model in the New-Normal Era

신승우, 조인준
배재대학교대학원 사이버보안학과

SeungWoo Shin(newincow@naver.com), In-June Jo(injune@pcu.ac.kr)

요약

지난 3년간 지속된 COVID-19 바이러스에 의한 팬데믹 사태는 사회와 사람들의 삶의 방식을 다양한 방식으로 변화시켰다. 이러한 변화는 사이버공간에도 영향을 주어 팬데믹 이전의 정보보안 모델과 기준은 현재 상황에 적용할 때 한계가 있다. 본 논문에서는 뉴노멀 시대의 다양한 상황을 고려한 공공기관의 정보보안 모델 개선방안을 새롭게 제안하였다. 즉, 제시된 정보보안 모델을 통해 기존의 공공기관 정보보안 운영의 취약점인 원격근무의 정책적, 기술적 보완을 통해 외부 침입의 가능성을 사전 차단한다. 또한 안전한 VPN 환경 구축을 통해 비정상적 인증 시도를 방어하는 방법, COVID-19로 인한 두려움과 불확실성을 노린 사회공학기반 사이버 공격(Social Engineering Cyber Attack)을 예방하는 방법, 원활한 네트워크 사용 및 원격근무 환경 조성을 위해 서비스 가용성을 확보하는 방법 등을 추가로 제시하였다.

■ 중심어 : | 정보보안 | 뉴노멀 | COVID-19 | 원격보안 | 사회공학공격 |

Abstract

The pandemic caused by the COVID-19 virus, which has lasted for the past three years, has changed society and the way people live in many ways. These changes also affect cyberspace, so the pre-pandemic information security model and standards have limitations when applied to the current situation. In this paper, a new method to improve the information security model of public institutions was proposed in consideration of various situations in the new normal era. In other words, through the proposed information security model, the possibility of external intrusion is blocked in advance through the policy and technical supplementation of remote work, which is a weakness of the existing information security operation of public institutions. Also, how to prevent abnormal authentication attempts by building a secure VPN environment, how to prevent social engineering cyber attacks targeting fear and uncertainty caused by COVID-19, and how to use a smooth network and create a remote work environment. For this purpose, methods for securing service availability were additionally presented.

■ keyword : | Information Security | New Normal | COVID-19 | Remote Security | Social Engineering Attack |

접수일자 : 2022년 06월 22일
수정일자 : 2022년 08월 02일
심사완료일 : 2022년 08월 08일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

2020년 1월 중순 스웨덴 공중보건국(Swedish Public Health Department)은 공식 웹사이트에 “중국을 통해 새로운 바이러스가 확산되고 있다.”고 처음으로 보고했다[1]. 이 후 보고된 바이러스의 확산이 점차 커지고, 2020년 3월 스웨덴 공중보건청의 권고안이 제시됐다. 전 세계는 지금껏 경험해보지 못한 새로운 유형의 바이러스에 의해 정치, 경제, 사회, 문화 등 전방위적 혼란을 겪게 되었다. 약 3년간 이러한 혼란은 지금까지 유지되었던 일반적인 생활환경을 현저히 바꾸어 놓았다. 그것은 비단 오프라인에서만 적용되는 것이 아닌, 사이버공간에서도 유효하게 적용되었다. 특히, 업무와 관련된 변화가 가장 두드러진 것으로 판단된다. 감염위험을 피하기 위해 여러 공공기관과 민간 기업이 기존의 업무 환경을 벗어나 대다수의 근로자에게 재택근무를 적용했기 때문이다. 문제는 이러한 갑작스러운 변화를 예측하지 못한 공공기관과 민간 기업의 재택근무 관련 제도적·기술적 대책의 미비함에 있으며, 팬데믹으로 인한 시대적 변화가 시작된 ‘뉴노멀(New Normal)’의 시작 이후에도 여전히 공공기관 사이버보안 문제의식의 관점에서 재택근무 시 모호한 보안기준 적용, 네트워크 인프라 가용성 확보 미비, 기존과 달라진 사이버 공격방식에 대책 부실, 포스트 팬데믹(Post Pandemic) 사이버보안을 위한 예방대책 마련 소홀 등과 같은 문제점이 남아있다. 또한 기존의 공공기관에서 이루어지는 정보보호 활동은 대부분 상위기관에서 사전 규정된 항목들만을 대상으로 시행된다. 이는 매우 수동적인 형태의 정보보호 활동으로 최소한의 보안 수준을 만족시킬 수 있는 정보보안 표준의 소극적 이행이기 때문이다. 그러나, 다양한 사이버 위협이 새롭게 등장하는 뉴노멀시대에는 후행적이고 단순한 정보보호 활동은 더이상 유효하지 않다. 사회의 혼란을 이용한 악의적인 해커들의 공격이 점차 다양해지고 지능화되기 때문이다. 따라서, 공공기관 원격근무 보안체계의 커다란 잠재적 보안 위협을 예방하기 위해 다음과 같은 대책이 필요하다.

첫째, 재택근무 시 행정망 접속을 위한 보안 요소를 세부적으로 강화해야 한다. 단순히 보안장비에 의존한 수동적 대응보다 다양한 사이버 공격의 변화를 고려하여 강화된 기술적·정책적 기준이 필요하다. 둘째, 뉴노멀시대에 적합한 공공기관 원격보안 사전점검 체크리스트를 개발해야 한다. 팬데믹 이전 일반적 기준의 진단 항목의 취약 요소들의 사전 진단 및 제거가 공공기관 원격 네트워크 안전의 핵심이기 때문이다.

본 논문에서는 이러한 문제점들을 개선하기 위해 원격근무 시 활용 가능한 보안기술을 공공기관 더 나아가 민간 기업까지 다양한 상황에 적용 가능하도록 제안하였다. 그리고 정보보호 관리영역별 중요 요소의 체크리스트 고도화를 통해 원격근무 보안체계의 관리적·기술적·예방적 측면의 보안성을 제고하였다.

II. 기존 공공기관 원격 정보보호 현황 및 문제점 요약

1. 기존 공공기관 원격 정보보호 체계의 문제점

공공기관에서 정보보안 활동은 일반적으로 국가정보보호 기본지침을 기반으로 한 각 기관 내규에 의해 수행된다. 하지만 기본지침에 명시된 핵심 보안지침 이상으로 기관 내규를 설정하는 경우는 드물다고 볼 수 있다. 그리고 팬데믹(Pandemic) 이전의 국가 정보보호 기본지침의 경우, 현재 정보보호 흐름을 온전히 반영하는 것은 어려웠다. 이러한 이유로 기존 유지되어왔던 공공기관 정보보호 체계는 해커들의 치밀하고 정교한 공격에 취약할 수밖에 없었다[2]. 즉, 최근까지 대부분의 공공기관은 포스트 팬데믹(Post Pandemic) 사이버 위협 환경에 적합하지 않은 정보보호 기준을 적용하였다. 그리고 기존 공공기관 정보보호 프로세스를 활용하여 보호 대상 IT 자산을 객관적·능동적 침해위협 대응하는 것은 구조적으로 쉽지 않다. 또한, 이러한 수동적 침해위협 행위는 고도화·다변화되는 해커의 공격에 매우 취약하다.

2. 원격근무 업무환경 보안 문제점

COVID-19 바이러스 대유행으로 민간 기업과 정부 모두 업무 연속성 유지를 위한 방법을 모색함에 따라 원격근무로의 대규모 전환[3]이 이루어졌다. 이로 인해,

직원들은 가정에서 로그인할 때 개인 장치(Devices)의 의존도가 현저히 높아졌다. 이제 개인 장치와 홈네트워크는 갑자기 업무 인프라의 핵심 부분이 되었다. 그러나 인터넷 트래픽이 증가함에 따라 개인 장치와 홈네트워크는 해커에게 더 큰 공격 기회를 제공한다. 재택근무를 하는 직원 수가 증가함에 따라 IT 보안 운영의 효율성이 떨어지며, 장치(Devices)와 인프라를 사이버 공격으로부터 보호하기 힘들다. 결국, 외부 재택근무 직원의 기관 내부 네트워크 접속 시 즉시 적용 가능한 기술적 정보보호 프로세스를 수반한 보안 의식 교육이 필요하다. [표 1]은 한국인터넷진흥원 "원격근무 환경 보안 점검 체크리스트 항목"[4]을 나타낸 것이다. 2020년 수립되어 각 기관에 배포된 비대면 업무환경 보안 체크리스트는 존재한다. 그러나 해당 체크리스트는 기업을 위한 것으로, 공공기관에 적용하기에 힘든 부분이 존재한다. 현재 공공기관 조직 특성과 비대면 시대의 변화에 적합한 기술적, 제도적 가이드라인 보완 및 개정이 미흡하여 당면과제로 남아있다.

표 1. 원격근무 환경 보안 점검 체크리스트, 한국인터넷진흥원 (KISA)

담당	구분	점검내용	점검 결과
원격 근무자	근무장소	■ 업무 수행 장소가 공개된 공간이 아닌 전용 근무 장소인가?	
	단말기 보안관리	■ 기업에서 지급한 원격근무용 단말기만 사내 네트워크 접속이 가능한가?	
		■ 원격근무용 단말기(노트북, 스마트폰, 태블릿 등)는 최신 보안 업데이트 상태로 관리하는가?	
		■ 가족, 손님 등 타인의 원격근무 단말기 사용이 불가능한 상태인가?	
	단말기 설치프로그램	■ 원격근무용 단말기에 원격근무자가 임의로 신규 프로그램을 설치하는 것이 불가능한 상태인가?	
		■ 원격근무자가 직원 간 대화에 사내 메신저 만을 사용하고 있는가?	
		■ 모든 사용 프로그램은 최신 보안 업데이트를 주기적으로 적용하는가?	
		■ 백신, DLP/DRM 등 데이터 보호 프로그램을 사용하는가?	
		■ 회사에서 승인한 정당한 라이선스가 있는 프로그램만을 사용하고 있는가?	
	USB 외부미디어	■ 데이터 복사/전송을 위한 USB외부 저장장치 사용을 제한하고 있는가?	
		■ 제한적 USB 외부 저장장치 사용시, USB 자동 실행 방지 및 자동 바이러스 검사를 시행하고 있는가?	
		■ 원격근무용 단말기의 USB 포트는 읽기 전용으로만 사용하고 있는가?	
		■ 구글 드라이브, iCloud 등 사용 클라우드에 업무 자료 저장을 금지하고 있는가?	
기 업 (기관)	네트워크	■ 원격근무 시 개방형 Wi-Fi를 사용한 사내 망에 접속을 제한하고 있는가?	
		■ 홈 네트워크 사용 시 공유기의 관리자 계정/암호를 안전하게 설정했는가?	
		■ 홈 네트워크에 허가된 사용자만 접속할 수 있게 보안정책을 적용하는가?	
		■ 무선 접속시 암호화방식은 WPA2 이상을 사용하고 있는가?	
		■ 회사가 제공하는 안전한 접속 방법만을 사용하여 접속하고 있는가?	
	비밀번호 보안	■ 비밀번호는 8자 이상으로 대소문자, 숫자, 특수문자 중 2가지 이상 조합하여 사용하고 있는가?	
		■ 업무용 계정을 개인용 계정과 구분하여 사용하고 있는가?	
		■ 사용하는 서비스 계정마다 별도의 암호를 사용하고 있는가?	
		■ 브라우저의 암호 자동 저장하기 기능을 사용하지 않도록 하였는가?	
	이메일 보안	■ 메일 본문에 있는 URL의 보안을 자동으로 검사하는 보안시스템이 있는가?	
		■ 원격근무자는 VPN을 이용하서 기업 메일 서버에 접속하는가?	
		■ 원격근무자가 메일서버에서 클라이언트로 메일을 다운받는 경우 암호통신을 지원하는가?	
		■ 상용 메일 사용시, 로그인 과정에 2단계 인증을 사용하고 있는가?	
		■ 메일 시스템을 내부망과 외부망으로 구분하여 사용하고 있는가?	
	네트워크 보안	■ 지정한 단말기만 기업 네트워크에 접속할 수 있는가?	
		■ VPN 접속 시 원격 단말기의 보안상태(백신 설치, 최신 보안 업데이트 적용 여부)를 점검하고 있는가?	
		■ VPN 인증 시 다중 인증(MFA, multi-factor authentication)을 적용하고 있는가?	
		■ VPN 운영 및 연결자원 현황을 지속적으로 모니터링 하고 있는가?	
		■ VPN을 대상으로한 DDoS 공격에 대비하여 비상 접속 방법을 준비하고 있는가?	
	사용자 인증	■ 기업 전산환경의 모든 접속은 단일 계정으로 통합 인증을 수행하고 있는가?	
		■ VPN 접속 통합인증으로 사용자 접속 이력 및 추적성을 확보하고 있는가?	
		■ 민감한 서버 로그인/관리자 계정에 다중 인증(MFA, multi-factor authentication)을 적용하고 있는가?	
		■ 사용자 이상징후 탐지를 위해 사용자 접속 이력, 접속 출발지 등을 지속적으로 모니터링 하고 있는가?	
	기업망 모니터링 강화	■ SIEM 운영 등을 이용하여 기업 전산시스템 시스템 로그를 상시 모니터링하여 외부 위협 탐지를 시행하고 있는가?	
		■ 원격근무 사용자 전용 네트워크 주소를 할당 하고 있는가?	
		■ 백신 설치, 최신 보안 업데이트, 내부 자원 모니터링 등을 통해 원격근무 사용자가 접속하는 업무 시스템의 보안성을 강화하고 있는가?	
		■ 불필요한 서버간 접근을 최소화하고 필요시 계정별 권한을 부여하는 접근통제를 적용하고 있는가?	

3. 부족한 네트워크 인프라

일반적으로 공공기관 내의 네트워크 인프라는 기관 내 네트워크 사용량의 월평균을 준용하여 구성한다. 그리고 이러한 방법은 지금까지 효과적이었다. 그러나 Pandemic 이후 사용자들은 이전과 달리, 업무와 교육 등 여러 가지 측면에서 네트워크 사용이 폭발적으로 증가했다. 내·외부에서의 잦은 시스템 접근, 화상회의를 위한 스트리밍 서비스 이용, 원격 업무의 증가 등이 그 예이다. 이것은 네트워크 관리자에게 의도하지 않은 DDoS 공격으로 작용할 수 있다. 이러한 네트워크 서비스 가용성 손상 가능성을 배제하기 위해, 공공기관에서는 이전보다 여유있는 네트워크 대역폭 할당이 요구된다. 그리고 규정보다 높은 성능을 지닌 네트워크 시스템의 이중화 구성이 필수이다. 또한, 사용하지 않는 서비스의 엄격한 관리와 VPN을 사용한 업무 목적 외 스트리밍 서비스의 규제가 필요하다.

Ⅲ. 뉴노멀시대의 주요사이버 위협

COVID-19 대유행은 전 세계적으로 막대한 혼란을 야기했을 뿐만 아니라 전 세계 인력과 사이버보안 환경도 변화시켰다. 이러한 변화에는 광범위한 사이버 위협과 도전과제도 포함되어있다. 따라서 기관과 기업 모두 악의적 해커의 행동 패턴 변화와 공격 증가 추이를 관찰하고 신중히 대응해야 한다. 이미 해커는 공격 대상을 변경하고 전술을 조정하고 있기 때문이다. 뉴노멀시대에 가장 심각한 위협으로 분류되는 사이버 위협은 다음과 같다.

1. RDP(Remote Desktop Protocol) 공격

전 세계적으로 COVID-19 검역이 강화되어 RDP(Remote Desktop Protocol) 서비스 사용이 증가되었다. 이러한 상황을 이용한 해커가 “RDP 무차별 대입공격”을 대량으로 시도한 정황이 탐지되었다[5]. 재택근무 관련 정책 수용의 방향에 따라 해당 공격은 증가할 것으로 예상된다.

2. Crawling과 Keylogging

이전부터 정보 수집과 키로깅은 해커들의 주요 활동 영역이었다. 일반적으로 해커는 피해자로부터 이름, Wi-Fi 비밀번호, 은행계좌 정보 등 광범위한 정보를 수집한다. 그러나, 현재는 시스템 및 네트워크 정보와 같은 고급데이터 또는 암호화폐 지갑 정보를 훔치는 정교한 키로거를 사용한다.

3. IoT 기기 공격

IoT의 장치는 가정, 기업 및 의료 부문에서 계속해서 인기를 얻고 주목받고 있다. 현재 세계의 정부는 COVID-19를 억제하는 데 도움이 되는 접촉 추적 앱을 점점 더 많이 사용하고 있다. 해커는 이러한 앱과 장치의 취약점을 계속 탐색하여 공격을 시작하고 사용자 개인정보를 훔칠 것이다. 또한 이러한 앱의 대규모 사용이 예상되는 뉴노멀시대에 공격이 강화될 것이다.

4. 피싱 및 랜섬웨어

해커들은 이제 이메일, PDF 첨부 파일 및 신뢰할 수 있는 SaaS(Software-as-a-Service)를 활용하는 다단계 피싱 공격을 선호하고 있다. 이전과는 달리, 현재의 피싱 공격은 기존 사이버 방어를 우회하기 위해 여러 사이버 공격 기술을 결합한 정교하고 고도화된 방식의 위협적인 공격으로 진화[6]했다.

5. 인공지능(AI), 기계학습(ML) 공격

COVID-19 이후 경제 및 사회 복지에 대한 전염병 확산 결과를 예측하는 AI(Artificial Intelligence) 및 ML(Machine Learning) 알고리즘의 증가가 나타났다. 해커는 동일한 AI 스크립트 및 프로그램의 악용을 통해 정부와 경제, 의료 시스템에 더 심각한 사이버 위협을 만들 것이다.

6. 온라인 교육 위협

뉴노멀 시대에도 사회적 거리두기 지침을 준수하기 위해 직장과 학교에서 온라인 교육은 상당히 보편화되었다. 그러나 수많은 해킹 피해사례는 개인과 조직의 온라인 교육 활성화에 부정적인 영향을 미친다.

Ⅳ. 뉴노멀시대의 공공기관 원격 정보보안 모델 개선방안 제안

1. 제안 아이디어 구성

제안한 기본 아이디어는 다음의 두 가지로 요약할 수 있다. 첫째, 팬데믹 이후 급증한 공공기관의 원격근무에 대한 네트워크 구성의 보안성 강화방안. 둘째, 뉴노멀 시대의 새로운 보안 침해위협을 반영한 원격보안점검 체크리스트 고도화이다.

기존의 일반적인 공공기관 원격 네트워크 구성은 원격 업무를 고려하지 않은 디자인이다. 이는 폭발적으로 수요가 증가하는 원격근무에 대해 많은 보안취약점을 가지고 있다. 보안 통제의 부정적 변수가 많은 기관 외부 단말과 내부 업무 단말의 연결로 인한 보안 취약성 증가 등이 그것이다. 이를 해결하고자 본 논문에서는 첫 단락에서 제시한 두 가지 아이디어를 가지고 기존 공공기관 원격 정보보안 모델의 문제점을 보완하려 한다. 즉, 진보된 네트워크 구성과 기술을 활용하여 원격근무 보안 침해위협을 예방하고, 뉴노멀시대의 주요 사이버위협을 반영한 원격근무 사전 체크리스트 개선을 통해 잠재적 원격보안 취약점 제거 방안을 제안하였다.

[그림 1]의 간소화된 제안 구성도를 기준으로 원격 네트워크 보안성 강화 구성의 간략한 설명은 다음과 같다.

① 기관 내·외부망에 인터넷 브라우저에서 직접 접근 가능한 VDI(Virtual Desktop Infrastructure) 클라우드 환경을 구축한다. 이때, VDI 브라우저는 반드시 Sandbox 형태로 개인 단말과 데이터 교환을 차단한다.

② 사용자가 외부 네트워크에서 내부망 접근 시 OTP(One Time Password)를 적용한 VPN 보안 연결을 이용한 접근만을 허용[3]한다

③ 보안시스템은 VDI 환경의 호환성과 보안을 위해 VDI 시스템 내 모듈 형태의 가상 하드웨어로 설치한다.

④ 사용자는 기관 내·외부에서 네트워크 접근 시 개인에게 부여된 전용 ID로 VDI에 로그인하여 장소에 구애받지 않는 동일한 업무환경을 경험한다. 기관 내부 업무 또한 동일한 VDI 에서 업무를 수행한다.

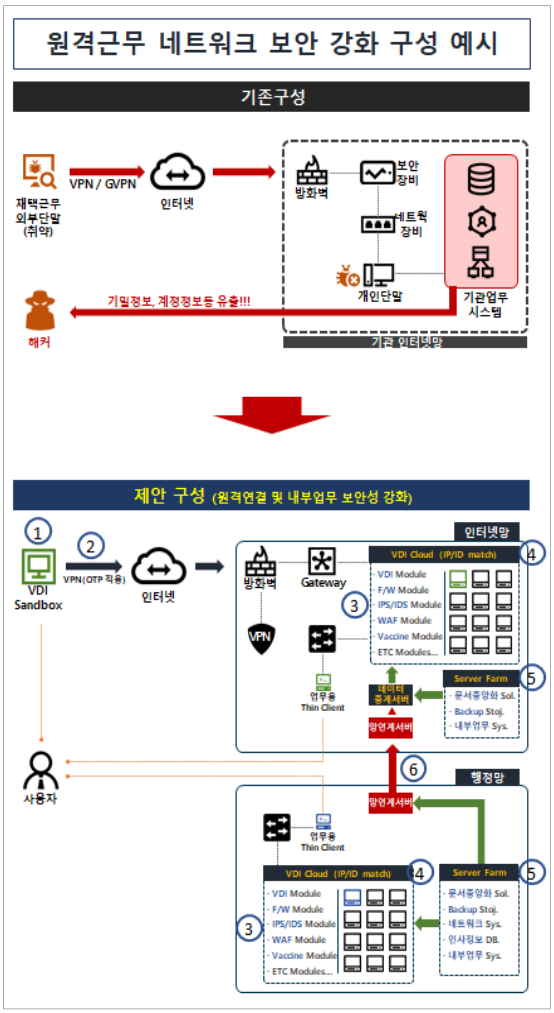


그림 1. 원격근무 네트워크 보안 강화 구성 예시

⑤ 문서중앙화 시스템[7]을 활용하여 온·오프라인 구별 없이 중요정보가 사용자 단말에 저장되지 않도록 설계, 중요정보 유출의 가능성을 차단한다.

⑥ 마지막으로 중요정보(인사 정보, 민감정보 등)는 망연계 시스템 일방향 전송의 이점[8]을 이용, 인터넷망으로부터 내부망 중요 서버의 접근을 차단한다.

표 2. 개선된 원격근무 환경 보안 점검 체크리스트

담당	구분	점검내용	점검결과
원격근무자	일반	■ 업무 수행 장소가 공개된 공간이 아닌 전용 근무 장소인가?	
		■ 원격근무 관련 교육을 받고, 정확한 이용 방법을 인지하였는가?	
		■ 원격근무용 단말기를 이용한 개인 목적 사용 금지에 대해 인지하였는가?	

담당	구분	점검내용	점검결과
기 관	단말기 보안관리	■ 기관에서 지급한 원격근무용 단말기만 관내 네트워크 접속이 가능한가?	
		■ 원격근무용 단말기(노트북, 스마트폰, 태블릿 등)는 최신 보안 업데이트 상태로 관리하는가?	
		■ 원격근무용 단말기는 도난·분실에 대비해 하드디스크 전체 암호화가 되어있는가?	
		■ 단말기에 설치된 백신으로 근무 중 1회 이상 바이러스 검사를 수행하는가?	
		■ VPN 연결 시 단말기의 보안프로그램 업데이트는 원활하게 실행되는가?	
		■ 노트북의 경우 CMOS / 사용자 로그인 패스워드 설정이 되어있는가?	
	단말기 설치프로그램	■ 원격근무용 단말기에 원격근무자가 임의로 신규 프로그램을 설치하는 것이 불가능한 상태인가?	
		■ 원격근무자가 직원 간 대화에 기관(공공) 메신저만을 사용하고 있는가?	
		■ 모든 사용 프로그램은 최신 보안 업데이트를 주기적으로 적용하는가?	
		■ 백신, DLP/DRM, USB보안 솔루션 등 기관 필수 정보보호 프로그램을 누락 없이 사용 하는가?	
		■ 기관에서 승인한 정당한 라이선스가 있는 프로그램만을 사용하고 있는가?	
		■ 모바일기기의 경우, 비업무용 앱 다운로드 불가능한 환경인가?	
	USB 외부미디어	■ 데이터 복사/전송을 위한 USB외부 저장장치 사용을 제한하고 있는가?	
		■ 제한적 USB 외부 저장장치 사용시, USB 자동 실행 방지 및 자동 바이러스 검사를 시행하고 있는가?	
	네트워크	■ 원격근무 시 개방형 Wi-Fi를 사용한 관내 망에 접속을 제한하고 있는가?	
		■ 홈 네트워크 사용 시 공유기의 관리자 계정/암호를 기관 규정에 맞게 설정했는가?	
		■ 홈 네트워크에 허가된 사용자만 접속할 수 있게 보안정책을 적용하는가?	
		■ 무선 접속시 암호화방식은 WPA2 이상을 사용하고 있는가?	
		■ 기관이 제공하는 안전한 접속 방법만을 사용하여 접속하고 있는가?	
	비밀번호 보안	■ 비밀번호는 8자 이상으로 대소문자, 숫자, 특수문자 중 2가지 이상 조합하여 사용하고 있는가?	
		■ 브라우저의 암호 자동 저장하기 기능을 사용하지 않도록 하였는가?	
		■ 90일에 1회 이상 비밀번호를 변경하여 사용하고 있는가?	
		■ 브라우저의 암호 자동 저장하기 기능을 사용하지 않도록 하였는가?	
	이메일 보안	■ 메일 본문에 있는 URL의 보안을 자동으로 검사하는 보안시스템이 있는가?	
		■ 원격근무자는 VPN을 이용하여 기관 메일 서버에 접속하는가?	
		■ 원격근무자가 메일서버에서 클라이언트로 메일을 다운받는 경우 암호통신을 지원 하는가?	
		■ 수신된 전자우편의 첨부파일이 자동실행 되지 않는 기능이 설정되어있는가?	
		■ 메일 시스템을 내부망과 외부망으로 구분하여 사용하고 있는가?	
	일반	■ 원격근무를 위한 업무수행 범위를 명확히 구분하였는가?	
		■ 원격근무 인력 대비 전용 단말기의 수량은 적절하게 확보되었는가?	
		■ 원격근무 전용 단말기의 보안관리 방안은 마련되었는가?	
		■ 원격근무시 원격근무자 수칙이 명시된 원격근무 보안관리지침이 수립되었는가?	

담당	구분	점검내용	점검결과
기 관	식별	■ 자산관리 시스템을 사용한 원격근무 전용 단말의 실시간 식별이 가능한가?	
		■ 기관 내 업무를 위해 필요한 모든 승인된 소프트웨어의 정기적 목록화가 가능한가?	
		■ 원격근무 단말에서 승인된 소프트웨어만 실행되도록 기술적 조치가 가능한가?	
	네트워크 보안	■ NAC를 사용한 원격근무 전용 단말의 승인/제거/격리가 가능한가?	
		■ 원격근무시스템의 서버 네트워크는 기타 서버 및 전산망에 접근 불가능한가?	
		■ 원격근무자 인증 후 일정시간 미 입력 시 재인증 기능이 활성화 되어있는가?	
		■ VPN 접속 시 원격 단말기의 보안상태(백신 설치, 최신 보안 업데이트 적용 여부)를 점검하고 있는가?	
		■ VPN 인증 시 다중 인증(MFA, multi-factor authentication)을 적용하고 있는가?	
		■ VPN 운영 및 연결자원 현황을 지속적으로 모니터링 하고 있는가?	
		■ VPN을 대상으로한 DDoS 공격에 대비하여 대응 방법을 준비하고 있는가?	
	교육	■ 기관의 모든 인력 구성원이 정기적으로 완료해야 할 보안 인식 프로그램이 준비 되어있는가?	
		■ 보안 인증 활성화 및 활용의 중요성에 대해 교육이 준비되어있는가?	
		■ 피싱, 사칭전화 등과 같은 사회공학공격을 식별하는 교육이 준비되어있는가?	
		■ 민감한 정보를 식별하고 저장, 전송, 보관 및 파기하는 방법의 교육이 준비되어 있는가?	
		■ 원격근무용 단말기 분실 등 의도하지 않은 데이터 노출 관련 교육이 준비되어있는가?	
	사용자 인증	■ 기관 전산환경의 모든 접속은 단일 계정으로 통합인증을 수행하고 있는가?	
		■ VPN 접속 통합인증으로 사용자 접속 이력 및 추적성을 확보하고 있는가?	
		■ 민감한 서버 로그인/관리자 계정에 다중 인증(MFA, multi-factor authentication)을 적용하고 있는가?	
		■ 사용자 업무에 알맞은 계정 권한을 부여하고 있는가?	
	데이터 복구	■ 모든 원격근무시스템 관련 데이터가 정기적으로 자동백업 되고 있는가?	
		■ 원격근무 단말 VDI 스냅샷이 정기적으로 설정되고, 자동백업 되고 있는가?	
		■ 백업이 저장될 때와 네트워크를 통해 이동 할 때 기술적 보안대책이 적절히 마련되었는가?	
		■ 모든 백업에 하나 이상의 오프라인 백업 대상이 존재하는가?	
	취약점 진단	■ 원격근무시스템의 무선, 클라이언트, 웹 애플리케이션 등 혼합공격 침투 테스트를 정기적으로 수행하는가?	
		■ 보호되지 않는 시스템 및 정보 존재 여부 관련 자동 취약점 스캐닝을 수행하는가?	
		■ 자산의 주기적 위험평가 프로세스를 활용, 취약점 수정의 우선순위를 지정하는가?	
		■ 취약점 진단 리포트를 기반으로 취약점 제거 활동을 수행하는가?	
	모니터링 강화	■ 원격근무 네트워크에 대한 집중 보안관제를 수행하고 있는가?	
		■ 원격근무 사용자 전용 네트워크 주소 및 ID를 할당하고 있는가?	
		■ 백신 설치, 최신 보안 업데이트, 내부 자원 모니터링 등을 통해 원격근무 사용자가 접속하는 업무시스템의 보안성을 강화하고 있는가?	
		■ 불필요한 서버간 접근을 최소화하고 필요시 계정별 권한을 부여하는 접근통제를 적용 하고 있는가?	

또한, 제안 아이디어는 [표 2]의 “개선된 원격근무 환경 보안점검 체크리스트”와 함께 활용하면 원격근무를 통해 발생 가능한 다양한 침해위협 예방에 효과적이다. 기관 내규 또는 지침에 원격근무 시 정보보호 관련된 세부 지침이 수립되지 않은 경우 특히 유효하다. [표 2]에 제안된 체크리스트의 “원격근무자” 부분은 근무 시 숙지해야 할 필수지침을 세부적으로 제시하였다. 특히, 원격근무에 대한 개인의 정보보안 인식 부분 및 단말 보안에 중점을 두어 기존과 차별화하였다. 또한 체크리스트 중 “기관” 부분은 기관의 정보보호 담당자가 원격근무시스템을 통한 서비스를 제공하는데 필요한 기술적, 정책적 필수 고려사항을 기존 기준보다 고도화된 기준으로 제시하였다. 기존에 존재하지 않았던 “일반”, “식별”, “교육”, “데이터 복구”, “취약점 진단” 섹션의 추가된 내용이 그것이다. 따라서 개선된 체크리스트와 구성도를 활용하여 기관에서 원격근무시스템에 대해 설계할 경우, 다음과 같은 순서로 진행하면 보안성을 고려한 안정적 구축이 가능하다.

① 제안 체크리스트의 “기관” 부분을 참고하여 원격근무시스템의 기술적, 정책적 토대설정 및 구축 근거 확보
② 사용자 범위 및 시스템 규모 설정, 활용 가능 예산 범위 책정 후 [그림 1] 제안 구성도를 참고, 도입 가능한 수준의 시스템 구성 결정.
③ 세부 시스템 구성과 사업계획서의 내/외부 보안성 검토
④ 구성된 원격근무시스템의 안전한 사용을 위한 직원교육 실시. 단, [표 2] 체크리스트의 “기관” 부분 “교육” 섹션의 내용이 반드시 포함되도록 구성
⑤ 제안 체크리스트를 바탕으로 사용자, 시스템 주기적 보안 점검 실시

V. 기존 원격보안 모델 및 제안모델 비교 분석

이 장에서는 제안한 원격보안 모델 아이디어가 기존 모델과 비교하여 효용성이 있는지 점검하기 위해 비교를 진행하였다. 비교는 두 가지 부분에서 진행되었다. 첫째는 원격근무 증가 대비 네트워크 구성의 보안성 강화, 둘째는 새로운 보안 침해위협을 반영한 원격 보안 점검 체크리스트이다. 각 비교의 검증 및 신뢰도 향상을 위해 “공공기관을 위한 네트워크 표준 구축 모델[9]”, “비대면 업무환경 도입·운영을 위한 보안 가이드”의 관련 내용을 참고하였다.

표 3. 공공기관 원격 네트워크 구성 모델 비교

	기존 네트워크 모델	제안 네트워크 모델
네트워크 장비	• L2, L3(L4), 백본, 라우터 • 방화벽, IPS, VPN	• L2, L3(L4), 백본, 라우터 • 방화벽, IPS, VPN, WAF 백신 등(가상 모듈형) • VDI 가상 클라이언트
보안	• IPSec VPN 기술 적용 • 검증된 암호화 모듈 사용	• SSL VPN 기술 적용 • 단말보안 솔루션 적용(캡처방지, DRM 등) • 문서중앙화 시스템 적용
인증/제어	• 단말기, 사용자 인증 • 내부 서버팜과 인증시스템 연동 • Access Control 기능	• 개인 VDI, 사용자 인증 • 2FA(OTP 적용 등) • SSO 기술 적용 • 망연계 서버를 활용한 일방향 보안통신
단말	• GPKI 등을 이용한 인증 • IP-in-IP Encapsulation • ARIA, SEED 등의 알고리즘을 이용한 IPSec 보안	• OTP 등을 이용한 간편인증 • 개인 VDI 적용 및 Thin Client 활용으로 내/외부 동일 업무환경 구현
장점	비교적 간단한 네트워크 구성으로 인해 구축 비용 절감	외부 원격보안 및 내부 네트워크 보안성 상향, VDI를 적극 활용한 구성으로, 장소에 구애받지 않는 업무환경 구축
단점	간단한 네트워크 구성으로 인해 정보보호 가용성은 향상, 기밀성과 무결성 보장은 어려움	원격 및 사용자 보안 네트워크 구성으로 최적의 형태를 지니고 있으나 구축 시 고비용

원격 네트워크 보안 구성 비교 결과는 다음과 같다. 비교결과 네트워크 구성 장비의 종류는 기존과 비교하여 제안모델이 약 2배 이상 다양해졌다. 그러나 대부분 가상화(솔루션 모듈)를 활용하여 물리적, 공간적 볼륨은 오히려 감소하였다. 또한 보안 및 인증에서 기존 구성과 제안모델은 다양한 차이를 보였다. 이는 다양하고 복잡해진 해커의 공격을 반영한 것으로, 제안모델의 주요 개선사항은 다음과 같다.

① SSL VPN 솔루션의 MFA(다중인증)을 이용
② 개인 VDI와 외부 단말의 1:1 IP 매칭 이용
③ 단말보안 강화(DRM, 화면캡처 방지 등)를 통한 외부 위협요소 차단
④ 문서중앙화 시스템 적용, 중요 내부정보 유출 사고 사전 방지
⑤ 망연계솔루션 및 중계 서버를 활용한 VDI(개인단말)의 서버팜 직접 접근 차단
⑥ 모듈형 네트워크 장비, 보안솔루션 이용으로 기존에 비해 유연하고 강력한 장비 배치

이러한 차이점들을 바탕으로 제안모델은 네트워크 보안성 구성 측면에서 기존과 완전히 차별화된 장점을 지닌다. 특히, 외부 네트워크의 개인 단말 접근 시, 내부의 Thin Client에서 접근하는 경우 모두 보안성이 최대한 보장된 상태의 동일한 업무환경을 장비와 공간의 제약 없이 재현 가능한 것이 연속성 측면에서 가장 큰 장점이다.

표 4. 원격근무 환경보안 점검 체크리스트 비교

	기존 체크리스트	제안 체크리스트
점검대상	• 원격 근무자에 초점 • 기업 및 범용 기준	• 점검 주체와 근무자에게 균등한 초점 • 공공기관, 범용(심화)
범위설정	• 근무자 : 기술적 범위 • 기업 : 기술적 범위(제한적)	• 단말보안 및 보안인식 확인 관련 점검범위 보강 • 공공기관에 즉시 적용 가능한 기술·관리적 범위
카테고리	• 근무자 : 7개 27항목 • 기업 : 3개 13항목	• 근무자 : 7개 29항목 • 기관 : 8개 35항목
관리보안	• 해당없음	• "일반" 카테고리 및 기타 카테고리 세부항목 적용
접근통제	• 적용	• "식별" 카테고리 및 기타 카테고리 세부항목 적용
단말보안	• 적용	• 기존 점검항목 대비 세부 점검항목 추가
인적보안	• 해당없음	• "일반", "교육" 카테고리 세부항목 적용
데이터 복구	• 해당없음	• 카테고리, 점검항목 추가
모니터링	• 적용	• 기존 점검항목 대비 세부 점검항목 추가
취약점 진단	• 해당없음	• 카테고리, 점검항목 추가

[표 4]는 원격근무 환경보안 점검 체크리스트를 기존과 비교한 결과이다. 기존 모델의 경우 대국민 원격근무 보안성 강화를 위해 범용적 기준을 적용하였다. 그러나 제안모델의 경우 까다로운 공공기관 네트워크 보안기준 및 법령을 고려하여 점검항목을 개발하였다. 강화된 '기관(기업)' 환경보안 점검항목의 개발 및 배치, 사용자 보안 인식 강화 개선 등 원격근무 네트워크 보안의 예방적 측면에서 장점이 있음을 볼 수 있다. 기존 대비 제안모델의 주요 개선점은 다음과 같다. 첫째, 기관의 관리적보안을 강화하기 위한 원격단말 보안관리 및 사용자 지침 마련 등사전점검 범위를 명확히 하였다. 둘째, 보안성 강화의 가장 큰 과제인 인적보안 이슈 중 "사용자 보안" 취약점 제거를 지속적 보안교육[10]을 통해 시도하였다. 사용자의 지속·반복적 보안 인식 강화 교육을 통해, 뉴노멀 시대에 더욱 증가하는 피싱, 해킹 메일, 사회공학공격, 개인정보유출 공격 등의 예방이 상당 부분 효과가 있기 때문이다. 셋째, 데이터 복구 측면의 중요성을 부각해, 언제든지 발생 가능한 비상상황에 사전대비할 수 있도록 점검항목을 구성하였다. 넷째, 정기적인 원격 네트워크 구성 시스템의 취약점 점검 및 취약점 제거 프로세스 항목을 삽입하여 원격 네트워크 보안의 안정성 강화를 견고히 하였다.

상기 비교·분석내용에서 보듯이 제안모델은 기존 공공기관 원격보안 모델의 불완전한 부분을 보완하였다. 특히, 제안모델은 공공기관 정보보안 측면에서 네트워크 구성이라는 물리적 보안 관점. 그리고 사전점검 및 사후감사를 대비한 관리적, 기술적 보안 요소를 점검하고 재정비할 수 있는 체크리스트를 모두 제공한다는 점에서 상호보완의 관계를 맺는다. 따라서, 공공기관(또는 기업)에서 제안모델을 이용하기 위해서는 네트워크 구성과 체크리스트를 해당 기관의 상황에 적합하게 "함께" 사용해야 원격근무 전산 인프라의 보안성 및 안전성 제고에 최적의 긍정적 영향을 미칠 수 있다.

Ⅵ. 결론 및 향후 연구

현재의 원격근무체계는 COVID-19 바이러스 확산 이후 일반적인 업무의 한 형태로 자리잡게 되었으며, 그에 따른 물리적·기술적·정책적 정보보안 대책 수립 역시 중요하게 되었다. 하지만 짧은 기간 안에 보안 정책을 수립하여 여러 공공기관에 적용하다 보니 재택근무, 다른 공공기관 또는 별도의 사무실에서의 원격근무 등 다양한 업무 환경을 고려하지는 못하였다. 본 논문에서는 기존 공공기관 원격근무 보안체계의 한계를 분석 후 물리적·기술적·정책적 문제점을 해결하는 방안을 다음과 같이 제시하였다. 첫째, 팬데믹 이 후 기존의 공격방식과 다르게 완전히 새로워진 사이버 공격을 대비하여 공공기관의 다양한 원격근무 환경에 적합한 안전한 네트워크 구성의 예시를 제공하였다. 둘째, 사용자 및 공공기관을 대상으로 급증하는 사이버위협의 사전·사후 대비를 위한 보안점검 체크리스트를 고도화 하였다. 이것은 기존 원격근무 보안체계와 비교하여 물리적· 기술적· 정책적 보안 측면에서 강화된 원격근무 보안체계를 공공기관뿐만 아니라 민간 기업에서도 유연하게 적용할

수 있도록 규격화 한 것이다. 따라서 제안 모델을 적절히 현재의 상황에 맞게 가감하여 적용하면 강화된 원격근무 보안환경 확보를 통해 안전성·보안성·생산성 등 많은 측면에서 공공기관(또는 민간 기업) 원격근무 보안체계의 효율성을 극대화 할 수 있을 것으로 사료된다.

본 연구는 실무 사례와 다양한 이론 그리고 연구자의 업무 경험을 중심으로 원격 네트워크 환경 구성 및 원격근무 환경보안 점검 체크리스트를 제시하였으나, 다양한 원격근무체계에서 가장 큰 보안 취약점인 사용자(End-Point) 보안 취약점을 보안 교육을 통해서만 해결하기에는 사실상 한계가 있다.

향후 연구 방향으로 본 논문에서 언급한 안전한 원격 네트워크 환경 구성의 비용적 측면의 절감을 위한 오픈소스 활용 방안 그리고 원격 근무자를 대상으로 실시간으로 진화하고 있는 사이버 공격을 현재보다 유연하게 대비·대응할 수 있는 통합 사용자(End-Point) 보안관리 방안을 연구해야 할 것이다.

참 고 문 헌

[1] 스웨덴 공중보건국, 2020. Retrieved from https://www.folkhalsomyndigheten.se/nyheter-och-press/nyhetsarkiv/2020/januari/nytt-coronavirus-upptackt-i-kina/

[2] 국가정보원·과학기술정보통신부·행정안전부·개인정보보호위원회·금융위원회·외교부, "2021 국가정보보호백서," p.30, 2021.

[3] 강동윤, 이상웅, 이재우, 이용준, "최근 사이버위협 동향과 가상사설망을 활용한 재택 근무자 보안 강화 기술 연구," 한국정보보호학회 논문지, 제31권, 제3호, pp.21-28, 2021.

[4] 한국인터넷진흥원, 비대면 업무환경 도입·운영을 위한 보안 가이드, pp.17-18, 2020.

[5] F5 LABS, 2020. Retrieved from https://f5.com/labs/articles/threat-intelligence/how-cyber-attacks-changed-during-the-pandemic

[6] 이윤수, 문형우, 박건량, 김태용, 송중석, "코로나19에 따른 사이버위협 및 대응기술 동향," 한국정보보호학회 논문지, 제31권, 제5호, pp.5-12, 2021.

[7] 윤용, 김연성, "업무문서 중앙화 서비스 제공을 위한 클라우드 시스템 운영방안," 한국IT서비스학회지, 제13권, 제4호, pp.309-324, 2014.

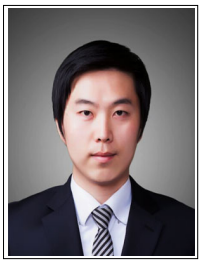
[8] 황성규, "네트워크 가상화를 이용한 망 분리 구축 방법," 한국정보통신학회논문지, 제24권, 제8호, pp.1071-1076, 2020.

[9] 강한국네트워크산업협회, 공공기관을 위한 네트워크 표준 구축 모델, p.17-20, 2012.

[10] 임명성, "정보보안 인식 교육의 효과에 대한 연구," 한국디지털정책학회, 제12권, 제2호, pp27-37, 2014.

저 자 소 개

신 승 우(Seung-Woo Shin) 준회원



- 2010년 2월 : 한남대학교 컴퓨터공학과 공학사
- 2010년 4월 ~ 2011년 12월 : (주)아이티센 사원
- 2012년 1월 ~ 2013년 3월 : (주)SAC 사원
- 2014년 2월 ~ 2018년 11월 : (주)아이티센 과장
- 2018년 11월 ~ 2019년 8월 : (주)이글루시큐리티 과장
- 2019년 5월 ~ 현재 : IQCS ISO 27001 국제심사원
- 2019년 8월 ~ 현재 : 국민권익위원회 전산주사보
- 2019년 9월 ~ 2022년 8월 : 배재대학교 사이버보안학과 공학석사

〈관심분야〉 : 통합보안관제시스템, 지능형 정보시스템, 국가기관 정보보안 관리, ISO 27001

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과 학사
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
- 1991년 ~ 현재 : 컴퓨터시스템응용기술사
- 2006년 ~ 현재 : 정보시스템수석감리원
- 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 정보보호, 컴퓨터네트워크보안, 컴퓨터시스템응용, 정보시스템감리