Journal of the Korea Convergence Society
Vol. 11. No. 10, pp. 37-44, 2020

ISSN 2233-4890 / eISSN 2713-6353
https://doi.org/10.15207/JKCS.2020.11.10.037

공공기관 물리적 망분리 환경에서의 비대면 스마트워크 근무 환경구축을 위한 보안 모델 연구

박상길[1], 김기봉[2], 손경자[2], 이원석[2], 박재표[3*]
[1]웨어비즈 대표, [2]숭실대학교 IT정책경영학과 박사과정, [3]숭실대학교 정보과학대학원 교수

A study on a security model for the establishment of a non-face-to-face smart work working environment in a physical network separation environment of public institutions

Sang-Kil Park[1], Gi-Bong Kim[2], Gyeong-Ja Son[2], Won-Suk Lee[2], Jae-Pyo Park[3*]
[1]CEO, Warebiz
[2]Ph. D. Course, Soongsil University, Department of IT Policy Management
[3]Professor, Soongsil University, Graduate School of Information Science

요 약 최근 COVID 19 팬데믹 현상으로 공공기관의 재택근무가 활성화 되고 있는 상황으로 공공기관에서의 업무는 시간과 공간의 제약이 사라지는 스마트워크 업무 환경으로 급변하고 있다. 하지만 현재 상당수의 공공기관은 인터넷망과 업무망을 분리하는 물리적 망분리 시스템으로 인해서 효율적인 스마트워크 업무환경을 위한 보안모델이 미흡한 상황이다. 이에, 본 논문에서는 공공기관의 물리적 망분리 환경에서 스마트워크를 구현하기 위한 현재의 한계를 기술하고 이를 보완하기 위한 업무환경에 필요한 보안 모델을 제안하고자 한다. 관련 연구로 SSL VPN에 대하여 설명하고 SSL VPN의 보안 한계를 극복하기 위한 SDP(Software Defined Perimeter), RDP(Remote Desktop Protocol), VDI(Virtual Desktop Infrastructure)의 보안 모델 연구를 통해서 스마트워크 업무 모델을 설명함으로써 물리적 망분리 보안 가이드를 준수하면서 공공기관에 적합한 스마트워크 환경 보안모델 방안을 제시하고자 한다.

주제어 : 스마트워크, 재택근무, 망분리, SSL VPN, SDP, RDP, VDI

Abstract Due to the recent COVID 19 pandemic, public institutions are increasingly working from home. Working in public institutions is rapidly changing into a smart work environment where time and space constraints disappear. However, many public institutions currently lack a security model for an efficient smart work environment due to the physical network separation system that separates the Internet network and the business network. Therefore, in this paper, we describe the current limitations for implementing smart work in a physical network separation environment of public institutions, and propose a security model necessary for a work environment to supplement them. As a related study, explain SSL VPN and explain smart work business model through security model research of SDP (Software Defined Perimeter), RDP (Remote Desktop Protocol), and VDI (Virtual Desktop Infrastructure) to overcome the security limitations of SSL VPN. As a result, we intend to propose a security model for a smart work environment suitable for public institutions while complying with the physical network separation security guide.

Key Words : Smart work, Telecommuting, Network separation, SSL VPN, SDP, RDP, VDI

*Corresponding Author : Jae-Pyo Park(pjerry@ssu.ac.kr)
Received September 14, 2020
Revised October 6, 2020
Accepted October 20, 2020
Published October 28, 2020

1. 서론

스마트워크 근무는 특정한 근무 장소를 정하지 않고 정보통신망을 이용하여 업무를 수행하는 것으로, 재택근무, 스마트워크센터 근무, 이동(모바일) 근무를 포함하는 것으로 정의할 수 있다[1].

정부에서는 일과 삶의 균형이 핵심 인재 확보 및 생산성을 높이는 인식의 확대와 중앙행정기관의 세종시 이전과 공공기관의 혁신도시 이전에 따른 업무 공백을 해소하고 행정 효율을 높이기 위한 방안으로 스마트워크 이용 확대를 강조하고 있다. 그러나 필요성의 인식 확대에도 불구하고 스마트워크 근무 운영률은 2017년 7.8%에서 2018년 14.3%로 향상되었으나 아직 저조한 운영률을 보이고 있다[2]. 그러나 최근 COVID 19 팬데믹 상황을 계기로 중앙행정기관 및 지방자치단체는 영상회의, GVPN 등 비대면 업무 시스템 활용률이 300 ~ 800% 대폭 증가하는 스마트워크 업무 시스템 이용이 폭발적으로 증가하고 있다[3].

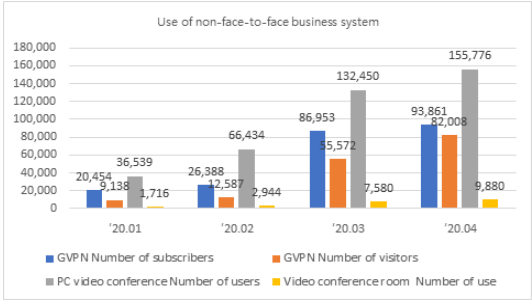

Fig. 1. Use of non-face-to-face business system (2020.01~2020.04)

Fig. 1에 의하면 자택이나 이동 시 원격으로 업무 시스템에 접속할 수 있는 GVPN 가입 수는 358% 증가했으며 이용자 수는 797% 증가하였음을 알 수 있다[3]. 하지만, 중앙행정기관 및 지방자치단체와는 다르게 공공기관의 경우는 2013년 국가정보원 망분리 가이드에 의한 물리적 망분리를 수행한 상태로 물리적 망분리 환경에서는 원천적으로 인터넷 망의 PC가 업무망 PC로 접속할 수 없는 환경이 구성되어 스마트워크 업무 환경을 위한 대안이 필요한 상황이다. 본 논문에서는 상당수 공공기관이 갑작스러운 COVID 19 환경에 대응하기 위하여 스마트워크 근무 중 재택근무 환경을 마련하고 있는 상황에서 망분리 환경의 보안요소를 충족하면서 스마트워크 환경을 구축할 수 있는 다양한 보안 모델 종류와 기법의 장단점을 살펴보고 업무환경에 적합한 보안 모델을 제시하고자 한다.

2. 관련연구

2.1 공공기관 물리적 망분리

망분리 제도는 사이버 위협으로부터 정보를 안전하게 지키기 위해 정부 주도하에 2006년부터 시행[4]되었으며 망분리는 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망 차단조치를 의미한다[5]. 이를 통해 인터넷 PC와 업무 PC를 분리하여 인터넷 서비스망과 업무 전산망 영역으로 구분하여 운영함으로써 인터넷으로부터 업무 관련 중요한 정보에 접근하는 것을 원천적으로 차단할 수 있다. 망분리는 물리적 망분리와 논리적 망분리로 크게 구분할 수 있으며 물리적 망분리 기준의 망분리 방안은 크게 3가지로 구분 할 수 있다[6,7].

Table 1. Physical network separation plan

division	concept
Use of 2 PCs	By separating the network using two PCs, you can perform work on a PC dedicated to the business network, and use another PC dedicated to the Internet for Internet use.
Using network separation switching device	The resources necessary for network connection, such as hard disk, IP address, and routing information, are divided for business and Internet, and the user selects it from the PC through the network separation switching device.
Multi PC use	One PC is used for business and the Internet is connected to the host PC through a separate connection device.

Table 1의 물리적 망분리 3가지 적용방안 중에서 국내 다수의 공공기관은 2대 PC를 이용하여 외부로 침입을 원천적으로 차단할 수 있는 보안강화를 목적으로 물리적 망분리 시스템을 적용하고 있다. 이는 2007년부터 2018년까지 10년간 망분리 사업 참여, 사례연구, 국가종합전자조달 나라장터 입찰공고서 기반으로 조사한 결과에서 조사대상 253개 공공기관 중에서 169개 기관(전체 66%)에서 물리적 망분리 시스템을 구축한 것으로 확인할 수 있었다.

Table 2. Status of construction of network separation for public institutions (2007~2018)

division	Sum	Physical network separation	Logical network separation
Number of institutions	253	169	84
Applicable organization (example)	-	Korea Expressway Corporation, Korea Petroleum Institute, Korea Industrial Technology Promotion Agency, Korea Airports Corporation, National Sports Promotion Agency, Korea Institute of Energy Technology Assessment, Social Security Information Service Korea Water Resources Corporation, Korea Industrial Complex Corporation, Korea Testing Laboratory, etc.	Labor Welfare Corporation, Gyeonggi Credit Guarantee Foundation, Korea Rural Community Corporation, National Police Agency, Korea Copyright Commission, etc.
ratio	100%	66%	36%

2.2 물리적 망분리의 스마트워크 업무 한계

물리적으로 인터넷망과 업무망이 분리되어 있는 환경에서는 기본적으로 외부에서 인터넷망을 경유하여 내부 업무망으로 직접 접속이 불가능하기 때문에 스마트워크를 위한 원격근무와 재택근무가 불가능하다. 이러한 이유로 최근 COVID 19 팬데믹 현상으로 재택근무가 필요한 공공기관에서는 SSL VPN을 이용하여 사용자 인증과 공인망 구간 암호화 터널링을 적용하여 업무망 PC에 접속하게 하는 일시적 방법을 통해 재택근무를 사용 할 수밖에 없는 상황이다. SSL VPN은 표준 웹 브라우저에서 SSL을 활용해 언제, 어디서나, 손쉽게 인터넷을 통한 가상사설망을 구성하는 개념으로 기밀성, 무결성, 서버인증을 위한 표준화된 암호화 알고리즘을 적용하는 방식이다[7]. SSL VPN을 이용한 스마트워크 원격근무는 구성이 용이하고 비용이 저렴하다는 장점[7]이 있지만, 다수의 인원이 동시에 접속할 경우 접속 수만큼 공개키 연산을 해야 함으로 응답시간이 저하될 수 있다[8]. 그리고 외부에 VPN 서버가 노출될 수밖에 없고 사용자의 인증 정보(아이디/패스워드)가 노출되면 외부 해커의 접속을 위한 경유지로 활용될 수 있는 위험성을 가지고 있다[9]. 또한, 원격지 PC에서 기관 인터넷망을 경유한 업무망의 직접 접속과 내부 데이터를 원격지 PC에 저장하여 자료가 외부로 유출될 수 있는 보안 취약점이 있어 인터넷망에는 데이터 저장을 금지하는 물리적 망분리 본연의 취지와도 부합되지 않는다.

3. 물리적 망분리 환경에서의 스마트워크 보안 모델

물리적 망분리 환경에서 스마트워크 업무를 수행하기 위해서는 SSL VPN 통신을 통한 내부 업무망으로 접속이 불가피한 상황이지만 외부로부터의 해킹 및 악성코드 감염과 자료 유출 등 보안취약점을 내포하고 있다. 따라서 본 논문에서는 스마트워크를 위한 법적 근거를 바탕으로 보다 효율적이고 보안에 안전한 스마트워크 환경을 위한 보안 모델을 제시한다.

3.1 스마트워크(원격근무)를 위한 법적 근거

COVID 19 비상상황에 의거 현상에 따라 금융당국은 COVID 19가 종식될 때 까지 한시적으로 망분리 규정들을 예외로 인정해 주는 비조치의견서[1]를 통해 유연하게 대응을 하고 있다[10]. 공공기관의 경우 스마트워크(재택근무) 업무 관련해서는 전자정부법 제32조에서 온라인 원격근무에 대한 내용을 규정하고 있다.

Table 3. Article 32 of the e-Government Act

Article 32 (Execution of electronic work, etc.) ③ If necessary, the head of an administrative agency, etc., may allow his/her employees to perform online remote work using an information and communication network without specifying a specific workplace. In this case, the head of an administrative agency, etc. shall prepare other measures to prevent illegal access to the information and communications network

산업통상자원부 정보화 업무규정에서는 GVPN (Government Virtual Private Network)을 사용하고 원격근무 PC에 대해서는 업무 자료 저장을 금지하며 최신 백신으로 PC를 점검하도록 규정하고 있다[11]. 또한, 한국인터넷진흥원에서는 재택·원격근무를 위한 사용자와 보안 관리자의 「정보보호 6대 실천 수칙」을 Table 4에서와 같이 제시하고 있는 상황이다.

1) 비조치의견서는 금융회사 등이 수행하려는 행위에 대해 금융감독 원장이 법령 등에 근거하여 향후 제재 등의 조치를 취할지 여부를 회신하는 문서를 의미. Financial Supervisory Service. (2016.12). Non-Measurement Opinion System Guidance, Inquiries, and Meetings..

Table 4. 6 information security practices

division	User Practice Rules	Security Manager Practice Rules
1	Personal PC latest security update	Recommended to use remote working system (VPN)
2	Antivirus program update and scan	Establishing security guidelines for telecommuters and raising security awareness
3	Home router security settings (password) and Refrain from using private Wi-Fi and public PCs	User accounts and access rights management for telecommuters
4	Recommend corporate mail, pay attention to personal mail	Network blocking in absence of a certain time
5	Refrain from using unnecessary websites	Enhanced remote access monitoring
6	Beware of downloading files (Beware of ransomware infection)	Data security such as personal and corporate information (Beware of ransomware infection)

위에서 규정 한 법적 근거를 살펴보면 기본적인 재택근무를 위해서는 사용자 인증, 암호화 통신, 원격 PC의 자료유출방지, 사용자 모니터링의 4가지 보안 요소를 기본적으로 준수해야 함을 알 수 있으며 원격 PC의 바이러스 감염 및 악성코드 유입에 대한 보안 대책도 필요함을 알 수 있다. 또한 물리적 망분리 환경에서 스마트워크 환경을 위한 구체적이고 현실적인 보안 가이드라인의 마련도 필요하다는 것을 알 수 있다.

3.2 RDP를 이용한 스마트워크 환경 모델

물리적 망분리 환경에서 4가지 보안 요소를 충족하는 스마트워크 모델의 첫 번째는 RDP를 이용한 방식이다. RDP(Remote Desktop Protocol)는 원격 데스크톱 프로토콜로 마이크로소프트사가 개발한 사유 프로토콜로, 다른 컴퓨터에 그래픽 사용자 인터페이스(GUI)를 제공하는 프로토콜이다[12]. RDP는 PC의 콘솔이 아닌 별도로 생성된 원격 세션으로 접속되어 국내 보안 프로그램 및 기타 프로그램이 동작하지 않는 경우가 있어 PC콘솔 세션으로 접속하는 경우 이를 해결할 수 있다[13]. 이 방식을 통해 원격 프로토콜을 이용하여 물리적 망분리 환경에서 스마트워크 보안 모델 구축을 고려해 볼 수 있다.

3.2.1 인프라 구성

물리적 망분리 환경에서 인터넷망에 RDP Gateway 서버를 구성하여 원격 PC 사용자 정보를 사전에 인증하고 RDP Gateway는 원격 PC와 내부망 사용자 PC를 RDP로 접속하도록 한다. 이러한 흐름을 통해서 Fig. 2의 스마트워크 업무를 위한 인프라를 구성할 수 있다.

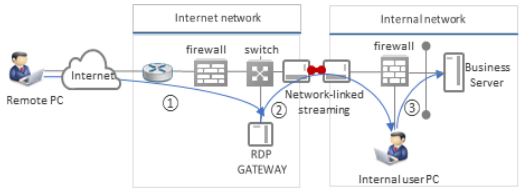

Fig. 2. RDP Smart Work Infrastructure Configuration Diagram

3.2.2 RDP 스마트워크 워크플로우

원격 PC에서 업무망에 접속하기 위해서는 사전에 배포된 클라이언트를 이용하여 RDP 게이트웨이를 통해 ID, PW, PC MAC 등 사용자 인증수단을 사용하여 인증을 수행한다. 인증받은 원격 PC는 SSL 보안 통신으로 RDP 가상채널을 통해 RDP Gateway를 경유한다[13].

RDP Gateway는 내부망 업무 PC와 RDP Proxy를 통해 네트워크 접속을 하며, 네트워크 상의 망연계 스트리밍 장비를 통해 세션을 연결하도록 한다. 이를 통해 원격 PC는 업무망의 사용자 PC와 원격 터미널 연결을 통해 사무실과 동일한 환경의 스마트워크 업무를 수행할 수 있다.

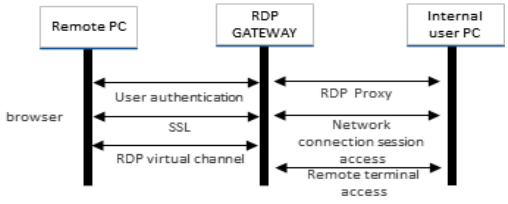

Fig. 3. RDP secure access procedure

3.2.3 RDP 보안 기능

RDP는 랜섬웨어 공격자가 정당한 목적으로 사용되는 프로토클을 통해 시스템에 접근할 수 있기 때문에 랜섬웨어 유포 방법으로 활용되는 보안 취약점이 있다[14]. 하지만 RDP 보안 위험 노출을 완화하기 위한 조치[2] 기준으로 RDP Gateway 구성과 사용자 인증, 암호화, 데

2) RDP 공격에 대한 노출을 완화하기 위한 방법으로 '강력한 비밀번호 사용, 역할 기반 엑세스 제한, 사전 신원인증, RDP 포트변경, RDP 서버 로그 및 모니터링 활성화, RDP Gateway 활용 등의 조치를 이행을 권고함. ITWorld. (2020.09.14.). What is an RDP attack What is it, 7 tips to mitigate RDP exposure. http://www.itworld.co.kr/news/110782

이터저장 금지, 모니터링을 강화하면 Table 5의 보안 기능을 제공할 수 있어서 스마트워크 환경을 위한 보안 모델로 검토 할 수 있다.

Table 5. Security function

division	Security function
certification	Access control through user authentication
encryption	Data section SSL encrypted communication
Data storage	Prevent data storage on remote PC
monitoring	User monitoring on gateway

3.3 SDP를 이용한 스마트워크 환경 모델

물리적 망분리 환경에서 4가지 보안 요소를 충족하는 스마트워크 모델의 두 번째는 SDP를 이용한 방식이다. SDP는 2007년 전후 미국의 정부기관 DISA (Defense Information Systems Agency)에서 수행한 컴퓨터 보안 접근방식이 발전, 변형된 형태로 블랙 클라우드 (Black Cloud)로 언급[15]되며 CSA[3]는 소프트웨어 정의 경계(Software Defined Perimeter, SDP) Spec 1.0을 발표하였다[16]. 이는 사용자의 상태 및 신원을 기반으로 하는 접근제어 프레임워크로 물리적 망분리 환경에서 스마트워크 업무 모델을 고려할 수 있다.

3.3.1 인프라 구성

물리적 망분리 환경에서 인터넷 망에 SDP Controller, SDP Gateway 서버를 구성한다. SDP Controller는 원격 PC의 신원확인 인증을 통해 통신 허용 여부를 결정하며 SDP Gateway는 인증된 사용자에 대한 서비스 접근 경로를 제공하고 SDP Gateway는 연결 상태에 대한 모니터링, 로깅, 리포팅 기능을 수행하도록 구성할 수 있다[17]. 이러한 흐름을 통해서 Fig. 4의 스마트워크 업무를 위한 인프라를 구성할 수 있다

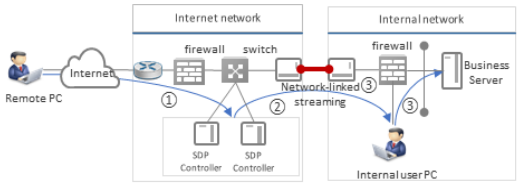

Fig. 4. SDP Smart Work Infrastructure Configuration Diagram

3) CSA (Cloud Security Alliance)는 클라우드 컴퓨팅 내에서 보안 보장을 제공하기 위한 모범 사례의 사용을 장려하고 클라우드 컴퓨팅 사용에 대한 교육을 제공하여 다른 모든 형태의 보안을 지원하는데 도움이 되는 비영리 조직 임 https://en.wikipedia.org/wiki/Cloud_Security_Alliance

3.3.2 SDP 스마트워크 워크플로우

SDP 구성요소는 Table 6 같이 SDP Controller, Initiating SDP Host(이하 IH), Accepting SDP Host (이하 AH), SDP Gateway로 구성된다[17].

Table 6. SDP components and roles

Component	role
SDP Controller	-Determine whether to communicate between SDP hosts -Determining whether to communicate by linking with authentication services such as external identification and location information
Initiating SDP Host	-Host requesting communication -Request a list of AHs that can communicate with the controller
Accepting SDP Host	-Host providing service -Accept IH's request according to controller's instructions
SDP Gateway	-Provides a path to access processes and services to authenticated users/devices -Provides monitoring, logging, and reporting functions for the connection between IH/AH

원격 PC에서 업무망에 접속하기 위한 절차는 SDP 컨트롤러에 대한 연결을 수신하는 호스트를 인증, 식별을 하고 보안 정책 (호스트 유형, 악성 코드 검사, 시간 등)에 대해 호스트를 검증하며 VPN (가상 사설망) 터널을 사용하여 연결을 수행한다[18]. 세부적인 절차는 Fig. 5의 7단계 절차에 의거 망분리 환경의 원격 PC에서 안전하게 내부망으로 접속하여 사무실과 동일한 환경으로 스마트워크 업무를 수행할 수 있다.

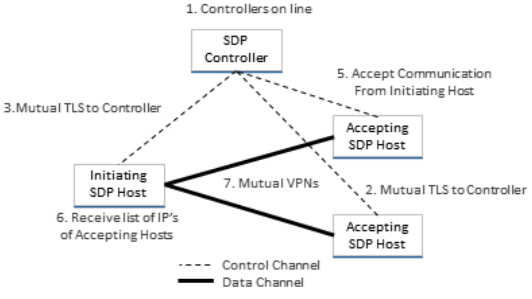

Fig. 5. SDP secure access procedure

3.3.3 SDP 보안 기능

SDP는 원격 사용자에 대한 선인증 후 연결, IP기반이 아닌 신원 중심 엑세스 제어, 암호화된 세그먼트 관리, 새로운 자원에 대한 동적 정책관리의 기능을 바탕으로 Table 7의 보안 기능을 제공하기에 스마트워크 환경을 위한 보안 모델로 고려할 수 있다.

Table 7. Security function

division	Security function
certification	Access control through user authentication (ADIUS, PKI, OpenID, OAuth, LDAP, etc.)
encryption	Communication using TLS protocol, which is more secure than SSL protocol
Data storage	Prevent data storage on remote PC
monitoring	Integrated policy management and monitoring by gateway

3.4 VDI를 이용한 스마트워크 환경 모델

물리적 망분리 환경에서 4가지 보안요소를 충족하는 스마트워크 모델의 세 번째는 VDI를 이용한 방식이다.

VDI(Virtual Desktop Infrastructure)는 개인이 사용하는 PC를 개인이 가지는 것이 아니라 대용량 CPU와 메모리를 장착한 서버와 같이 고사양 장치의 특정 영역을 개인 PC로 만들어 개인에게 할당하고 이를 원거리에 있는 개인이 S/W를 사용하여 원격 접속 후, 마치 자신의 앞에 PC가 있는 것처럼(Virtual) 사용하는 형태를 통칭한다[19]. VDI을 활용한 망분리 구축 방법에 대해 정부는 2011년부터 본격적으로 VDI를 이용한 논리적 망분리를 허용함으로써 상당수 공공기관에서 도입하여 구축하고 있는 상황이다. 하지만 최근 COVID 19 팬데믹으로 인해 물리적 망분리 시스템을 구축한 기관에서도 안전한 스마트워크 업무환경을 위해서 기 검증된 VDI를 스마트워크보안 모델로 검토하고 있는 상황이다.

3.4.1 인프라 구성

물리적 망분리 환경에서 VDI를 이용한 스마트워크 인프라는 먼저 SSL VPN 신원인증을 통해서 업무망 VDI서버에 접속한다. 사용자 인증으로 VDI 서버에 접속하여 문서 생성, 조회, 다운로드 되는 일련의 과정이 가상화 서버영역을 벗어날 수 없어 정보 유출을 차단하고 사용자 이력 관리가 가능하다[20]. 이렇듯 VDI의 사용자 인증으로 원격업무를 위한 서비스 접근경로를 제공하도록 구성할 수 있다. 이러한 흐름을 통해서 Fig. 6의 스마트워크 업무를 위한 인프라를 구성할 수 있다.

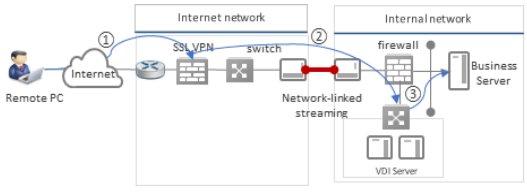

Fig. 6. VDI Smart Work Infrastructure Configuration Diagram

3.4.2 VDI 스마트워크 워크플로우

원격 PC에서 업무망에 접속하기 위해서는 사전에 배포된 SSL VPN 클라이언트를 이용하여 VDI 관리포털에 접속하여 사용 권한 인증을 받는다. 또한, VDI업무에 대한 사용 권한 인증은 VDI AD 서버를 통해 인증권한을 부여받는 절차로 진행한다. 업무망의 VDI 서버의 개인별 가상 PC는 물리적으로 안전한 특정 영역에 집중 관리되며 원격 PC는 업무망 VDI PC의 화면정보만 전송받고 암호화된 채널을 통해 키보드, 마우스 등의 입력 정보만을 가상 PC로 전송하게 된다. 이를 통해 원격 PC는 업무망의 사용자 PC와 원격 터미널 연결을 통해 사무실과 동일한 환경의 스마트워크 업무를 수행할 수 있다. 이러한 절차는 Fig. 7에서의 절차로 도식화 할 수 있다.

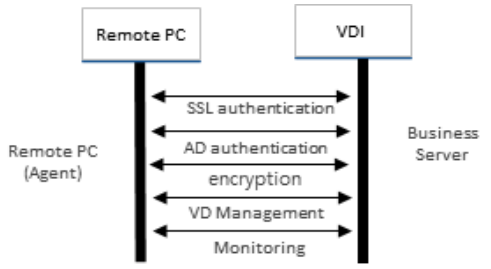

Fig. 7. VDI secure access procedure

3.4.3 VDI 보안 기능

VDI는 원격 사용자의 SSL VPN과 VDI의 사용권한 인증의 2단계 인증, 원격 PC와 VDI 서버의 암호화 통신, 외부로부터의 데이터 저장 방지, 접속사용자에 대한 모니터링 및 정책 관리 기능을 제공하면 Table 8의 보안기능은 스마트워크 환경을 위한 보안 모델로 고려할 수 있다.

Table 8. Security function

division	Security function
certification	Provides two-factor authentication of SSL VPN and VDI authentication (Account management, Account lock)
encryption	Encrypted communication such as RC5(128bit)
Data storage	Prevent data storage on remote PC
monitoring	Manager's policy management and monitoring

3.5 스마트워크 보안 모델 비교

앞에서 물리적 망분리 환경에서 안전하고 효율성 있는 스마트워크 환경구축을 위한 보안 모델 3가지를 살펴보았다. 3가지 보안모델의 특징 및 기능적 차이는 있지만,

스마트워크 환경을 위해서는 외부 접속 PC 사용자 인증, 데이터 저장방지, 암호화 통신, 모니터링은 기본적으로 필요 하다는 것이다. Table 9는 관련 연구에서 살펴 본 내용을 기초로 비교하였으며 보안성 측면에서 RDP 에 비해 상대적으로 SDP와 VDI가 높은 수준의 보안성을 제공하고 있음을 알 수 있다. 또한, 운영 측면에서는 구축 사례가 많은 VDI 모델이 업무 적용이나 확장성 측면에서 유용하다는 것을 알 수 있다.

Table 9. Security model comparison

division	VPN	RDP	SDP	VDI
certification	○	○	◎	◎
encryption	○	○	◎	◎
Prevent remote PC data storage	X	○	○	○
Connection history (Log)	○	○	○	○
Integrated monitoring	X	△	△	○
Ease of installation	facility	facility	facility	Relative difficulty
cost	lowness	lowness	Relatively cheap	height
case	plenty	-	Relative little	plenty

◎: High acceptance, ○: Accept, △: Relative acceptance, X: Not accepted

4. 결 론

최근 들어 COVID 19 팬데믹 현상이 장기간 지속하고 있어 스마트오피스에 대한 관심이 더욱더 높아져 가고 있다. 하지만 다수의 공공기관은 물리적인 망분리에 의한 인터넷망과 업무망을 분리해서 운영하는 상황으로 효율적인 스마트워크 업무환경을 구축하기 위한 기준을 설정하는 데 어려움이 있으며 제도적으로도 구체적인 보안 가이드라인도 부족한 상황이다.

본 논문에서는 스마트워크 업무의 연속성을 보장하면서 보안 강화를 할 수 있는 물리적 망분리 환경에서 적용 가능한 스마트워크 보안 모델 3가지를 제시하였다. 하지만 3가지 보안 모델이 완벽한 보안환경을 제공할 수 없으며 백신, 랜섬웨어 방지, DRM, APT 등 원격 인터넷망 PC의 보안을 강화할 수 있는 이기종의 보안 소프트웨어와 상호운영 하여 보안을 강화해야 한다.

그러나 본 논문을 통해서 망 분리 환경에서 스마트워크 환경구축 시 필요한 요소를 공감하고 향후 스마트워크 환경의 보안 모델 구축 사업을 준비하는 기관의 보안 담당자들이 해당 기관의 규모, 업무환경, 보안환경에 부합하는 보안정책을 마련하고 적용하는데 기본 자료로 활용될 수 있을 것이다.

더불어, 공공 IT환경에 적합한 현실적인 스마트워크 보안 모델 가이드라인을 위한 정책 수립에도 도움이 되기를 기대해 본다.

REFERENCES

[1] Ministry of Public Administration and Security. (2016). *Smart Work Center Usage and Operation Guidelines,* Seoul.

[2] Ministry of Science and Technology, Korea Information Society Agency. (2019). *2019 informatization statistics collection.*

[3] Ministry of Public Administration and Security. (2019). *The use of non-face-to-face business systems in public sectors exploded on the occasion of Corona.* [Online], https://www.mois.go.kr/

[4] B. H. Lim. (2014). *A Study on the Deployment of an Partitioned-Network for Information Security.* Electronic Trade Research, *12(4),* 1-10. DOI : 10.17255/etr.12.4.201411.1

[5] Korea Communications Commission. (2013). *Standards for technical and managerial protection measures for personal information.*

[6] K. Y. Lee. (2019). *Study on the effectiveness of network separation policy*. Master's Thesis. Korea University, Seoul.

[7] H. Y. Woo. (2005). *The Study of SSL VPN Benchmarking with Network Analysis*. Master's Thesis. DongKuk University, Seoul.

[8] J. H. Yoon & T. K. Kwon. (2003). Analysing the SSL VPN model compared with IPSec VPN. *Journal of the Korean Information Science Society, 30(21),* 760-762.

[9] J. K. Jeong, S. G. Lee & Y. M. Kim. (2019). Improved Single Packet Authentication and Network Access Control Security Management in Software. *Journal of the Korea Contents Association, 19(12),* 407-415. DOI : 10.5392/JKCA.2019.19.12.407

[10] Digital Daily. (2020.02.26.). F*inancial Services Commission, Financial Network Separation Exception Measures'... Expanding Telework in the Corona 19 Financial Industry*. [Online], http://www.ddaily.co.kr/news/article/?no=192288

[11] Ministry of Trade, Industry and Energy. (2018.08.17). *Ministry of Trade, Industry and Energy Information Business Regulations*. Directive No. 132, 1-33.

[12] H. H Lee. (2012). *A Study of Effective Streaming on Cloud Computing Using RDP*. Master's Thesis. Chungnam

National University, Daejeon.

[13] C. S. Kim. (2014) Design and Implementation Smart Office System Based on Remote Desktop Protocol (RDP), *The journal of the institute of internet, broadcasting and communication, 14(2),* 153-159.

[14] D. S. Yoo. (2020). *A Study on the Effective Ransomware response of Endpoint Level.* Master's Thesis. Korea University, Seoul.

[15] C. W. Jae, J. I. Shin, D. B. Lee, H. Kim & D. H. Lee. (2018). Proposal of Network Security Solution based on Software Definition Perimeter for Secure Cloud Environment. *Journal of the Korean Convergence Society, 9(12),* 61-68.
DOI : 10.15207/JKCS.2018.9.12.061

[16] Brent Bilger et al. (2014). *SDP Specification 1.0,* CSA.

[17] J. K. Jung. (2020). *A Dynamic Access Control Procedure Considering User's Device Situation in Software Defined Perimeter Environment.* Doctoral dissertation, Chonnam National University, Gwangju.

[18] D. C. (2017). *Software-Defined Perimeters : An Architectural View of SDP.* IEEE Softwarization. [Online], https://sdn.ieee.org/newsletter/march-2017/software-definedperimeters-an-architectural-view-of-sdp.

[19] H. S. Lee. (2105). *Research of Security Enhancement Using VDI-Based Network Separation Architecture.* Master's Thesis. Korea University, Seoul.

[20] Y. H. Lee & S. J. Yoo. (2014). The Construction of Logical, Physical Network Separation by Virtualization. *Convergence security journal, 14(2),* 25-33.

박 상 길(Sang-Kil Park) [정회원]

· 2015년 5월 : 숭실대학교 정보과학대학원(공학석사)
· 2020년 8월 : 숭실대학교 IT정책경영학과 IT서비스학(공학박사)
· 2006년 12월 ~ 현재 : 주식회사 웨어비즈 대표
· 관심분야 : 네트워크보안, 망분리, 빅데이터, AI
· E-Mail : highroad@warebiz.co.kr

김 기 봉(Gi-Bong Kim) [정회원]

· 2012년 3월 : 국방대학교 국방관리대학원(국방관리학석사)
· 2019년 3월 ~ 현재 : 숭실대학교 IT정책경영학과 박사과정 재학
· 2020년 현재 : 해군대학 교관 (중령)
· 관심분야 : AI, Cloud, Big-data, AR/VR
· E-Mail : kkb0820@hanmail.net

손 경 자(Kyung-Ja Son) [정회원]

· 2013년 8월 : 건국대학교 축산대학원(경영학석사)
· 2000년 3월 ~ 현재 : 숭실대학교 IT정책경영학과 박사과정 재학
· 1993년 ~ 현재 : 농림축산식품부 정보통계정책담당관실
· 관심분야 : 빅데이터, IT거버넌스, 행정정보화, 농업정보화 정책
· E-Mail : shinson@korea.kr

이 원 석(Won-Suk Lee) [정회원]

· 2002년 2월 : 아주대학교 정보통신대학원(공학석사)
· 2019년 9월 ~ 현재 : 숭실대학교 IT정책경영학과 박사과정 재학
· 2018년 8월 ~ 현재 : 농림축산식품부 정보통계정책담당관실 과장
· 관심분야 : ICT전략, 빅데이터/IoT, 인공지능/챗봇
· E-Mail : wsmjmy@naver.com

박 재 표(Jae-Pyo Park) [정회원]

· 1998년 8월 : 숭실대학교 대학원 컴퓨터학과(공학석사)
· 2004년 8월 : 숭실대학교 대학원 컴퓨터학과(공학박사)
· 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수
· 관심분야 : 정보보안, 보안평가 및 인증, 디지털포렌식, FinTech
· E-Mail : pjerry@ssu.ac.kr