J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

비전통 위협에 대한 국방 업무수행체계 유지방안 (감염병 위협 중심으로)

Consideration for defense preparedness against non-traditional security threats (focused on the threat of infectious diseases)

권 혁 진[1] 신 동 규[2] 신 용 주[3*]
Hyukjin Kwon Donggyu Shin Youngjoo Shin

요 약

국방은 감염병과 같은 비전통 위협에 대한 직·간접적인 영향에서도 중단없는 의사결정 업무 수행이 필요하다. 모든 업무는 정보시스템을 활용하기에 정보시스템의 가용성을 보장하는 것이 매우 중요하다. 특히, 국방업무는 보안관리 측면에서 네트워크를 국방망과 상용인터넷망으로 이원화하여 수행되고 있다. 본 연구는 효과적인 국방정보체계 운용을 통해서 인터넷에서 수행되는 업무의 효율성과 보안의 효과성을 고려한 업무수행 방안을 제시하였다. 국방망과 상용인터넷이 연결되는 네트워크 접점을 최소화하고 다양한 업무 중 우선순위가 높은 것을 선정하여 효율적으로 운용하는 방안이 필요하다. 이를 위해 A기관을 대상으로 실제 사례를 조사하고 특성을 제시하였다. 본 논문에서 제시한 국방업무의 효과성을 향상하고 보안성을 보장하기 위한 대상 업무와 운용방안을 통해 감염병과 같은 비전통 위협에서도 업무수행의 가용성을 높일 수 있을 것이다.

☞ 주제어 : 온라인 업무체계, 비전통 위협, 정보시스템 가용도, 업무연속성계획

ABSTRACT

The national defense requires uninterrupted decision-making, even under direct or indirect impacts on non-traditional threats such as infectious diseases. Since all work utilizes the information system, it is very important to ensure the availability of the information system. In particular, in terms of security management, defense work is being performed by dividing the network into a national defense network and a commercial Internet network. This study suggests a work execution plan that takes into account the efficiency of work performed on the Internet and the effectiveness of security through effective defense information system operation. It is necessary to minimize the network contact point between the national defense network and the commercial Internet, and to select a high-priority one among various tasks and operate it efficiently. For this purpose, actual cases were investigated for "A" institution and characteristics were presented. Through the targeted tasks and operation plans to improve the effectiveness of defense tasks and ensure security, presented in this paper, it will be possible to increase the availability of task performance even in non-traditional threats such as infectious diseases.

☞ keyword : online business system, non-traditional threats, information system availability, business continuity plan(BCP)

1. 서 론

재난, 감염병 등 비전통 위협에 대한 국가차원의 포괄적 안보의 중요성이 계속 강조되고 있다. 감염병으로 인해 시스템의 운용인력이 격리되고 시설이 폐쇄되더라도 24시간 중단없는 업무의 연속성이 유지되는 것이 필요하다. 업무의 공백을 최소화할 수 있는 비대면 업무가 안정적으로 수행할 수 있도록 환경 및 체계의 구비가 중요 이슈로 대두되고 있다. 군은 코로나19가 큰 위협이 됨에 따라 정보시스템의 전환 훈련 등을 시작하였으나, 우선순위와 명확한 목적에 따른 수행체계의 정립이 필요하다. 또한, 비대면 상황에서의 업무수행 시 정보 유출 및 서비스 장애에 대한 대응방안이 강구되어야 한다. 본 연구의 목표는 감염병과 같은 비전통 위협에 대한 업무수행체계

1 Dept. of Protection and Safety Engineering, SEOULTECH, 232, Gongneung-ro, Nowon-gu, Seoul, 01811, Korea.
2 Dept. of Computer Engineering and Convergence Engineering, Sejong Univ., 209, Neungdong-ro, Gwangjin-gu, Seoul, 05006, Korea.
3 Center for Military for Analysis and Planning, KIDA, 37, Hoegi-ro, Dongdaemun-gu, Seoul 02455, Korea.
* Corresponding author (keen56@kida.re.kr)
[Received 12 October. 2021, Reviewed 20 Octboer 2021(R2 15 November 2021), Accepted 23 November 2021]

유지방안을 도출하는 것이다. 감염병으로 인한 원격 비대면 업무수행체계를 지원하는 방안이 요구되고 있다.

내부 네트워크와의 연결접점이 증가됨에 따라, 내부자 또는 인가받지 않은 외부자로부터 기밀정보 유출, 해킹으로 인한 서비스 장애 등에 대한 대비방안도 필요하다. 국방은 코로나19에 따른 대응훈련을 실시하고 있으나, 비대면 업무 수행체계를 확정하지 못하고 있다. 물론 모든 업무가 비대면으로 수행되어야 하는 것은 아니다. 우선순위는 무엇이고, 어떠한 목적을 갖고 어떻게 해야 하는지 등의 체계를 갖추는 것이 요구된다.

2. 관련 연구

2.1 비전통 위협 연구

'비전통 안보 위협요인 분석 및 대응방안'(송은희 외, 2016)에서 전문가를 대상으로 한 델파이 방법으로 사이버 공격(해킹 등 사이버 범죄, 국가차원의 사이버전)을 제1순위의 위협요인으로 선정하였다. 코로나19로 인해 비대면 업무가 활성화되면 이러한 경향은 더욱 커질 것이다. 안전한 업무 환경을 위한 준비가 더욱 필요하게 된다.

2.2 감염병 관련 연구

'무기체계 연구개발시 COVID-19의 영향성 연구'(이승만 외, 2020)에서 공급체인의 작동 문제로 인한 전력화의 어려움을 해소해야 할 문제로 보았다.

'언택트 시대의 그림자: 사이버위협의 일상화'(오일석, 2020)에서 비대면 접촉의 증대로 사이버공간의 신뢰성과 안전성 확보의 중요성을 강조하였다.

연결접점이 크게 늘어나고 복잡도는 기하급수적으로 많아지므로 기존의 방식으로 관리하는 것은 곤란하다. 사이버에 대한 고려와 운용의 효율성과 효과성을 동시에 고려해야 하는 상황은 지속될 것이다. 모든 시스템을 이중화하고 통제를 이원화하는 것이 가장 좋은 방법이다. 하지만 예산과 인력 등 현실적으로 어려운 문제이다. 이를 어떻게 최적화해서 목적한 효과를 낼 수 있는지에 대한 연구가 필요한 것이다.

2.3 사례연구

2.3.1 금융기관 사례

금융기관은 금융감독원의 전자금융감독규정을 준수하고 있다. 전자금융감독규정 시행세칙 개정(2020.11. 6)에 따른 정보보호 통제를 준수한다. "신종 코로나 바이러스의 사내 확산과 감염 직원의 자택격리 등에 따른 업무중단 사태 방지를 위한 원격근무활용 환경(재택근무)" 심의ㆍ의결(제4차 정보보호위원회, 2020.2.13.)한 규정을 적용한다. 기관의 환경에 기반하여 독자적인 원격 비대면 시스템 접근통제 수립 적용 및 업무연속성계획(BCP, Business Continuity Plan)에 따라 비상대응체계를 가동하고 있다. 원격 비대면(재택근무) 운영방안을 수립하고 장애, 재해, 파업, 테러 등에서 표1, 2와 같이 긴급 상황 기준을 정의하고 상황별 재택근무 운영하고 있다.

(표 1) 사회적 거리두기 단계기준
(Table 1) Criteria for social distancing

구분	2~3단계 (지역적 유행)	4단계 (전국적 유행)
재택근무비율	25%	별도통보
시스템 접근대상	불가(생체인증)	가능(QR인증)
계정 접속대상	사전승인자 (지급단말)	재택 대상자 전체

(표 2) 근무지 폐쇄기준
(Table 2) Criteria for closing workplaces

구분	폐쇄 없음	층 폐쇄	건물 폐쇄
재택근무비율	25%	해당층전체	해당건물 전체
시스템 접근대상	불가 (생체인증)	해당층가능 (QR인증)	해당건물 가능 (QR인증)
계정접속 대상	사전승인자 (지급 단말)	재택 대상자 전체	

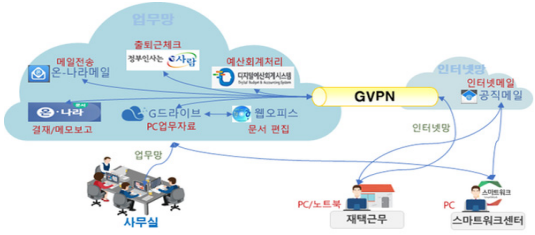
시스템·기술 측면에서는 불법 원격접속 방지를 위한 사용자 인증, 암호화 등 추가인증 수단을 적용한 보안대책을 강구하였다. 아이디와 비밀번호의 인증방식에 mOTP를 추가로 적용하였다. 국내IP에 대해서만 접속 허용하여 해외IP는 차단하였으며, 사전에 등록된 공인 IP에 대해서만 접근이 가능하다. 자택의 PC에서는 USB 방식의 외부 저장매체를 차단하고 로컬 프린터기를 차단하였다. 원격접속용 외부단말기와 내부업무용 시스템은 구간 암호화 통신을 수행한다. 통신 구간은 SSL VPN(가상 사설망)의 암호화 통신을 적용하고, 내부 인입구간에서는 방화벽을 운영하여 의도되지 않은 접속을 차단한다.

2.3.2 공공기관

코로나19와 같은 감염병이 확산되는 상황에서 비대면 업무체계를 구축하고 재택근무와 원격근무로 전환하고

있다. 감염병 사태에 대응할 수 있도록 업무연속성계획(BCP)을 수립하고 비상대응체계를 가동하였다. 관련 규정은 '코로나19 확산 차단을 위한 공무원 대상 유연근무 이행지침' 시행 ('20.03.12)이다. 사무실 밀집도를 낮추기 위해 부서별로 적정비율로 의무적으로 교대 원격근무를 시행한다. 재택근무자는 업무전화을 착신전환하고 GVPN을 설치하여 재택근무의 여건을 조성한다. 행안부 '스마트워크 활성화 추진전략(2010.7)'에 근거하여 스마트워크센터를 구축 및 운영 한다. 비대면 업무수행을 위한 지침을 수립하여 안전한 원격근무 및 화상회의 구축 가이드라인 및 보안을 위한 점검 목록 제공한다. 이는 과기정통부의 '비대면 업무환경 도입, 운영을 위한 보안가이드'와 고용노동부 '재택근무 종합 매뉴얼'에 따른 것이다.

클라우드 기반 정부원격 근무서비스(GVPN+G-Cloud)를 통하여 그림1과 같이 원격근무를 수행한다. 일부기관은 클라우드 기반의 데스크톱 가상화(VDI)환경으로 원격 비대면 업무를 수행한다. 행안부는 스마트워크센터의 구축을 통해 원격지에 구축된 업무 공간에서 업무 수행한다. 스마트워크센터 이용 및 운영지침(2019.10.7. 개정)에 따른 것이다.



(그림 1) 공공기관 시스템 및 기술 현황

(Figure 1) Systems and technologies in public institutions

2.3 시사점

업무 프로세스 관점에서는 감염병 확산을 포함하여 재해, 재난 상황에 대비해 군 정보시스템의 중단요소에 대한 적극적인 대응방안 수립을 위한 체계화된 매뉴얼이 필요하다. 예를 들면, 공공기관 및 기업의 업무연속성계획(BCP)와 같은 것이다. 이와 같은 업무연속성계획에 훈련 주기, 시나리오, 우선순위 대상, 훈련 결과에 대한 개선책 수립 방안 등이 포함되어 있어야 실효성이 있게 된다.

관련 규정 측면에서는 코로나19와 같은 감염병 상황이 장기화가 되는 상황에서 군 정보시스템의 필수인력이 업무수행이 제한되는 것을 극복하여야 한다. 비대면 업무수행으로 전환하기 위한 원격근무 방안 등 비대면 업무의 전환을 위한 국방 규정, 지침 등 제도적 인프라 확충의 필요하다.

인사·조직·교육 관점으로 보면, 감염병 위기상황에 체계적, 선제적으로 대응하기 위한 군 전담조직의 설립을 통한 체계화된 대응전략의 확보가 요구된다.

시스템·기술 관점에서는 기존의 망분리 정책을 따르던 국가 주요기관 및 공공기관의 원격근무의 전환과 미군의 원격근무 사례를 잘 볼 필요가 있다. 우리 군 역시 원격 비대면 업무수행을 위한 시스템 환경과 보안대책 강구가 필요하다. 예를 들면, 생채인증 기반 원격접속 시스템 등이다.

국·내의 비대면 업무수행 방식은 각 기관별 장·단점을 비교하는 것보다 해당 기관과 업무의 특성을 반영하여 적용하는 것이 필요하다.

3. 국방환경 현황

감염병의 확산 상황에 대한 국방정보체계의 체계적인 관리와 대응을 보완하는 것이 필요하다. 실제 상황 발생 시 많은 혼란과 어려움이 발생하기 때문이다. 감염병의 직·간접 접촉으로 인한 핵심인력의 자가 격리 시에 정상적인 업무수행이 제한된다.

국방정보시스템을 운용하고 있는 관련 기관에서 시스템 전환 등의 제한적인 훈련 실시하고 있지만, 이를 위한 근거가 없고 비계획적으로 실시하고 있다.

원격 비대면 업무수행을 위한 시스템의 환경의 구비가 필요하다. 상용 인터넷을 통한 원격업무 환경은 보안을 보장하는 방안을 강구해야 한다. 현재 인터넷과 국방망의 연동방식은 표3과 같이 훈령에서 간접연동방식만을 허용하고 있다.

(표 3) 현 훈령에서 인터넷과 국방망의 연동방식

(Table 3) In the current guidelines, interworking method between the Internet and the defense network

○ 국방보안업무훈령 제134조(정보통신망 연동) - 비밀등급이 다른 망간에는 반드시 연동장비를 통한 간접연동을 하도록 의무화 ○ 국방사이버보안훈령 별표 4(국방정보시스템 보호기준 및 보호요구사항) - 비밀등급이 동일(국방망 ↔ 국방망 / 전장망 ↔ 전장망)할 경우에는 간접 및 직접연동이 모두 가능하며, 비밀등급 상이한(전장망 ↔ 국방망)할 경우에는 간접연동만 가능하도록 기준 제시

ICT 발전에 따른 새로운 연동방식(VDI기술 활용)에 대한 명확한 기준이 미흡하다. VDI 기술을 활용한 연동방식을 직접 및 간접방식으로 구분하기에는 그 기준이 불분명하다. 국방보안업무훈령과 국방사이버훈령에는 직접연동방식과 간접연동방식에 대한 명확한 차이점을 제시하지 않고 있다. 연동방식 구분을 위한 기준이 모호한 것이다. 국방 정보체계 망 연동 보안 가이드라인('17.11.01.)에는 망연동 방식에 대해 다음과 같이 기술되어 있다. 직접연동방식은 물리적으로 연결되어 있고 동일한 보안(비밀)등급의 체계를 연동하는 방식이다. 간접연동방식은 망간 물리적 분리 특성을 유지하여 보안(비밀)등급이 상이한 체계를 연동하는 방식이다. VDI 기술을 활용한 연동방식은 훈령 및 국방부 가이드라인에서 기술되어 있지 않다.

4. 비대면 업무수행방안

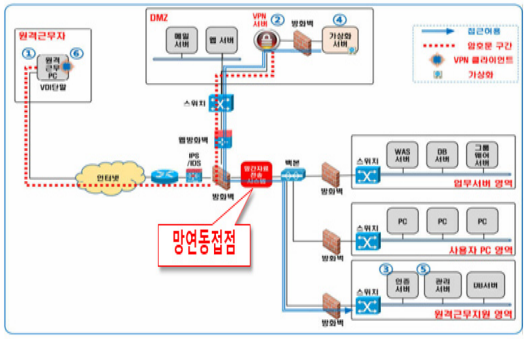
4.1 기본 요구사항

감염병 상황 및 유사시 시간과 장소에 제한 없이 업무의 연속성 보장이 필요하다. 또한, 외부에서 수행해야 할 업무 정의가 필요하다. 상용 인터넷 환경에서 수행할 수 있는 업무와 사용자를 구분해야 한다. 실시간으로 유연하게 수행되어야 하는 업무는 무엇인지를 식별해야 한다. 사용자(의사결정권자, 연구원, 관리원 등)별 수행하는 업무를 고려해야 한다. 기술적인 측면과 보안적인 측면을 동시에 고려해야 한다. VDI 기술을 활용한 논리적 망분리와 같은 국방망과 상용인터넷과 안전한 연결 보장이 요구된다. 물론 자료유출 및 보안사고 방지방안도 수립이 필요하다.

4.2 비대면업무수행체계 구성방안

인터넷 기반 원격 비대면 업무방안의 구성도는 그림 2와 같으며, 국정원『원격업무 통합보안메뉴얼(2020.5.)』을 활용하였다. 인터넷에 연결되어 있는 원격근무자가 국방망 내에 위치한 정보체계를 접속하는 절차는 아래와 같다.

① 원격근무자는 원격PC에 설치된 VPN 클라이언트를 이용, VPN서버에 접속
② VPN서버에서 원격근무를 위한 VPN 사용자 인증
③ 가상화서버에서 인가된 원격근무자 확인을 위하여 인증서버로 인증 요청
④ 인증된 원격근무자는 가상화서버에서 관리 서버로 가상데스크톱 요청
⑤ 관리서버는 인증된 사용자에게 가상데스크톱 할당
⑥ 원격근무자는 할당받은 가상데스크톱을 이용하여 원격근무 수행



(그림 2) 원격 비대면 업무방안 구성도
(Figure 2) System of remote, non-face-to-face work plans

VDI 기술을 통한 네트워크 연동방식은 원격업무에 적용할 수 있는 가장 합리적이고 안전한 방식으로 알려져 있다. 가상화 방식의 VDI를 DMZ에 설치하고 VPN으로 외부에서 원격접속을 실시하는 방식을 통하여 물리적 망분리의 특성을 유지할 수 있으며, 실시간에 가까운 데이터 지연으로 인해 네트워크의 효율성을 보장받을 수 있다.

VDI 기술은 물리적으로 존재하진 않지만, 실제 작동하는 컴퓨터 안에서 작동하는 또 하나의 컴퓨터를 만들 수 있는 기술이다. 클라우드 서버는 VDI 기술을 이용하여 인증된 사용자에게 약속된 자원(CPU, 메모리 등)을 할당해 VM를 생성하고, 사용자의 요구에 따라 OS, 프로그램 등을 VM 상에서 실행시켜 가상의 데스크톱을 생성한다. 클라우드를 기반으로 VDI 서버에 일반 PC와 동일한 가상 PC환경을 구성하고 다양한 디바이스에서 네트워크를 통해 이용할 수 있는 가상 데스크톱 서비스를 제공한다. 현재 VDI 관련 기술은 네트워킹, 컴퓨팅 및 리소스를 소프트웨어에 의해 추가로 제어할 수 있도록 단일 위치로 가상화하는 아키텍처 기술과 다양한 운영체제의 개발 및 DaaS(Desktop as a Service) 관련 HW의 기술 발전 등이 활발하게 진행되고 있다.

업무의 가용성과 보안강화를 높이는 방안으로 VDI 기술이 활발히 도입되고 있다. 이러한 VDI 및 DaaS 기술을 통해서 물리적 PC의 시간·공간적인 제약을 극복하여 사용자에게 단말 이용환경을 제공할 수 있다. 패치, 백업,

업그레이드 등 데스크톱 관리를 중앙에서 수행하여 관리 및 유지보수가 용이하다. 데이터를 직접 저장·관리하는 물리적인 PC와 달리 PC에 저장하지 않고, 클라우드저장소에 개별 저장·관리함으로써 보안성이 개선된다. 장애 및 재난·재해의 발생 시 새로운 데스크톱을 신속히 제공하여 업무 연속성 확보가 용이하다. 시간과 공간의 제약을 극복하여 언제, 어디서나 원하는 정보에 접근할 수 있어 업무 이동성이 확대된다.

VDI 기술은 화면의 속성에 따라 텍스트와 이미지, 동영상으로 분류한다. 분류된 속성에 따라 텍스트는 무손실 압축을 하고, 이미지는 JPEG Turbo 방식으로, 동영상은 H.264 또는 MPEG-2 방식으로 압축하여 전체화면을 압축하는 방식에 대비하여 CPU의 사용량이 감소하고 네트워크 트래픽도 낮아질 수 있다. 실제로 400대의 VM를 운영중인 환경에서 사용자당 평균 100kbps 미만의 대역폭을 사용하였다. 그러므로 QoS 정책으로 3MB을 보장하는 환경에서는 네트워크망 증설 없이 VDI 운영이 가능하다.

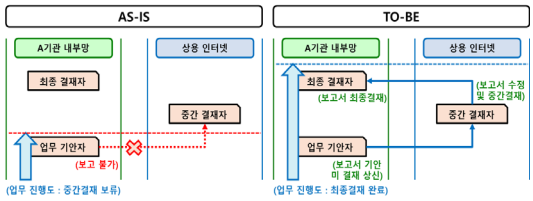
VDI 기술은 양자화(Quantization)를 통한 궁극의 보안환경을 제공한다. 화면 속성에 따른 선택적 압축 방법으로 Low 대역폭에서의 빠른 화면전송은 물론 좌표값만 전송되므로 해커가 중간에 탈취하더라도 전혀 그 내용을 확인할 수 없다. 즉, 보안 가상화에 특화된 프로토콜을 사용하여 서버에서 클라이언트로 보내는 정보가 Data Gran (스트리밍)이 아닌 화면값(숫자)로 송신하기 때문에 정보탈취와 해독이 불가능하다. 이러한 VDI 기술을 통해서 관제실과 상황실에서 필요한 컴퓨터 환경을 구축하면 네트워크가 연결된 어느 장소에서도 동일한 작업환경에서 임무를 수행할 수 있다. 예비상황실과 스마트워크센터 구축을 위해 필요한 단말기만 설치하면 작업환경은 주상황실과 동일하게 구성이 가능하다.

국정원 『원격업무 통합보안 매뉴얼』에서 VDI를 적용한 원격근무시스템 권장하고 있으며, 국방부 안보지원사령부 국방보안연구소의 『국방 온라인 재택근무체계 도입방안 연구』의 결과에서도 가장 합리적이고 안전하다고 제시하였다. VPN은 기술자체 보다는 관리 및 운영상의 취약점이 노출되어 있다. 예를 들면 보안패치 미적용과 디폴트계정 유지 등이다. VPN+VDI+DMZ 조합으로 국방망 원격근무가 가능한지를 실험하는 것이 필요하다.

국방망 원격근무에 시스템 구축을 위한 훈령 및 규정의 개정이 필요하다. 훈령개정을 위한 시스템 구축 및 시험운영, 안정성 평가 후 훈령개정 추진하는 것이 필요하다.

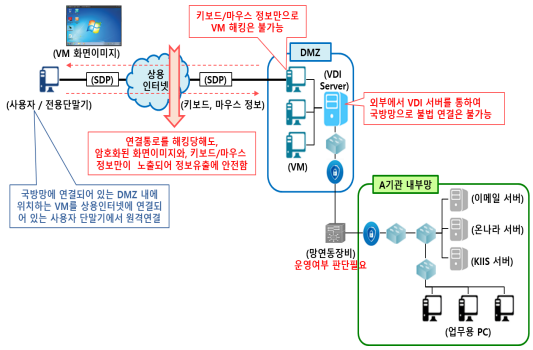
4.3 업무공간 발전개념(A기관 사례연구)

인터넷 업무환경에서 수행할 수 있는 업무와 사용자 개념 정립이 필요하다. AS-IS는 A기관의 외부 인터넷 공간에서 업무 협업 불가하다. TO-BE는 인터넷 업무공간에서 업무의 연속성 보장하는 것이다.



(그림 3) 업무공간 발전개념
(Figure 3) Concept of workplace development

기술적 보안적 측면에서 VDI + DMZ + VPN 조합을 통한 논리적 망분리 환경 구축한다. 국정원 『원격업무 통합보안 매뉴얼(20.05.)』에서 VDI 기술을 적용한 원격근무시템을 권장하였다. 또한, 국방보안연구소 『국방 온라인 재택근무체계 도입방안 연구』에서 VDI 기술을 원격업무에 적용할 수 있는 가장 합리적이고 안전한 방안으로 제시하였다. 국정원의 권장안과 국방보안연구소의 제시안을 바탕으로 그림 4와 같은 인터넷 기반 원격 비대면 업무방안을 구성하였다.

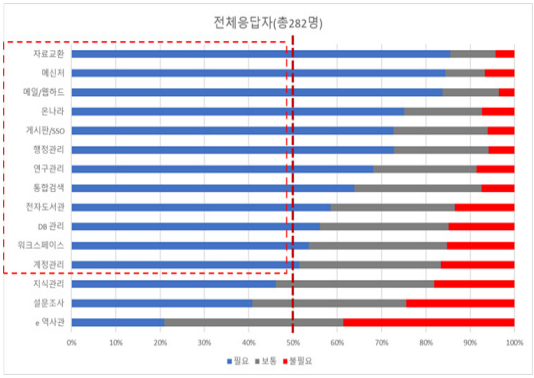


(그림 4) 인터넷 기반 원격 비대면 업무방안 구성도
(Figure 4) System of of Internet-based remote non-face-to-face business plan

상용인터넷을 통한 국방망의 DMZ에 VPN으로 접속하고, 사용자는 DMZ 내의 VDI서버 에서 VM를 할당받아 국방망 내의 서비스를 제공받는다. 사용자는 DMZ 내의

VM를 VPN을 통하여 원격접속한다. 모든 서비스의 실행은 DMZ 내의 VM에서 수행되기 때문에 인터넷을 통하여 송수신되는 파일이나 기타 정보들은 존재하지 않는다. VPN 구간에서는 VM의 데스크탑 화면의 이미지가 국방망에서 인터넷으로 송신되고, 사용자의 키보드와 마우스를 조작하는 키 정보가 국방망으로 송신된다. VPN 구간에서 송수신되는 데이터는 암호화된다. 그러므로 VPN 구간에서 송수신되는 데이터를 임의로 획득하더라도 그 내용을 확인할 수 없으며, 근본적으로 모든 자료는 DMZ 내의 VM에서 수행되기 때문에 인터넷으로 정보유출은 발생하지 않는다. 또한, 인터넷상에 존재하는 사용자 단말기가 해킹당하여 좀비PC가 되더라도 원격시스템을 접속하기 위해서는 이중화 인증을 요구하고 있으며, 인터넷상으로 자료를 송신할 수 있는 방법이 없기 때문에 안전하다. 그리고 인터넷에서 국방망으로 송신되는 키보드와 마우스 키 조작 정보로 VDI 서버와 국방망 내부의 정보체계를 해킹하는 것은 불가능하다. 결과적으로 VDI + DMZ + VPN 기술들의 조합으로 이기종의 네트워크를 안전하게 연동하여 서비스를 제공하는 것이 가능하다.

보안 관련 훈령(국방보안업무훈령, 사이버안보 훈령)의 개정이 필요하다. 현 훈령에는 직접연동방식과 간접연동방식을 구분할 수 있는 기준에 관한 구체적인 내용이 부족하며, 스토리지 방식의 “간접연동”을 통한 망연동만을 허용한다. 외부에서 VDI(DMZ+VPN)을 통한 국방망 연결이 가능할 수 있도록 개정되어야 한다. 훈령 개정전에 규제 샌드박스 개념으로 구축하여 위협요인에 대한 검증 후 국방 전 영역으로 확산하는 것이 좋을 것이다. 즉, 체계구축 전략에서 훈령 개정전에 샌드박스 개념으로 A기관의 국방망 서비스를 대상으로 한시적(1년)으로 VDI

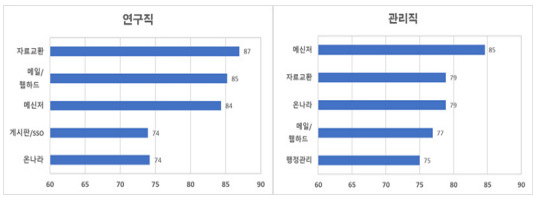


(그림 5) 설문 전체 응답결과
(Figure 5) Results of all the responses

기술을 활용한 원격근무 체계 구축한 후 시험운영하는 방안이 좋다. 제한된 범위 내에서 VDI 기술을 적용하여 국방망과 인터넷 연동 허용하고 시험하는 것이다.

인터넷 공간의 업무 수행 우선순위를 선정하기 위하여 온라인 설문조사를 수행하였다. 전체 응답자 282명 중에서 응답 직원의 과반수(141명)는 아래 기능을 필요로 하는 것으로 분석되었다. 자료교환, A기관의 메신저, 메일, 게시판, 온나라, 행정관리, 연구관리, 통합검색, 전자도서관 등이다.

직군별 업무 필요도를 분석하면, 연구직 및 관리직의 원격근무 시 업무별 필요도 Top 5는 다음과 같다. 공통적으로 메신저, 자료교환 메일 등 업무의 공백이 발생하지 않는 것에 우선순위가 있다.



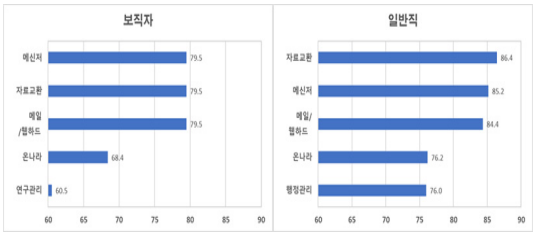
(그림 6) 직군 별 업무 필요도 분석결과
(Figure 6) Results of analyzing the need for work by job group

설문 응답률과 기타의견을 기반으로 종합적으로 분석하면 자료교환체계, 메일, A기관 메신저, 온 나라 기능은 두 직군에서 공통으로 높은 비율로 필요하다고 응답하고 있다. 비대면업무 시 별도의 독립된 재택근무용 업무를 하는 것이 아닌, 원내 직원들과 실시간 소통하며 기존 업무환경(자료)을 기반으로 업무의 연속성을 유지하는 것이 필요하다는 것을 의미한다. 그 이유는 자료교환체계가 내부망·외부망에서 업무 연속성의 유지를 위해 필요한 것이고, A기관의 메신저는 업무 진행 간 직원의 실시간 원활한 의사소통을 지원하는 것이기 때문이다. 메일은 내부 공지, 업무자료 공유, 외부 메일 확인으로 중요·긴급 업무수행을 위해 필요하다고 하였다.

의사결정과 관련된 업무가 많은 보직자와 일반직원으로 구분하여 보면, 그림6과 같이 자료교환체계, 메일, A기관 메신저, 온 나라 기능이 공통으로 높은 비율로 필요하다고 응답하였으며 이는 직군 별 필요도 분석과 유사한 결과를 보이고 있다. 단, 보직자의 경우 원격접속에 의한 보안에 우려를 많이 가지고 있었다. 전반적으로는 보직자, 일반직 모두 실시간 업무 소통, 기존 업무환경(자

료)을 기반으로 업무의 연속성을 유지하는 것을 필요로 하는 것을 알 수 있다.

설문 응답자의 인구학적 통계자료는 인터넷 기반의 비대면 업무의 성격과 특성에 영향을 거의 주지 않았다.



(그림 7) 보직여부 별 업무 필요도 분석결과
(Figure 7) Results of analyzing the need for work by position status

5. 맺음말

감염병 사태에 대비한 비대면 업무방식으로의 변화는 선택이 아니라 필수이다. 민간은 감염병으로 인한 대규모 결근 사태를 대비한 비대면업무 환경으로의 전환이 신속하게 진행되어 가고 있다. 국방은 망 분리 정책으로 원격근무가 불가한 상황이다. 감염병과 같은 비전통 위협에 따라 현장업무 수행이 가능하지 못한 경우는 계속 발생할 수밖에 없을 것이다. 이때 민간 기업과 같은 업무 연속성 보장에 어려움이 있게 된다. 감염병 및 여러 가지 상황에서 업무의 연속성을 유지하는 것이 필요하다는 것은 모두 인식하고 있다.

본 연구는 감염병과 같은 비전통 위협에서도 업무의 연속성을 유지하기 위한 체계의 구축방안을 제시하였다. 다양한 업무 중에서 제한된 범위에서 우선적으로 수행해야 할 것이 무엇인지를 확인하였다. 이를 통해서 어떠한 유사시의 환경에서도 연속된 업무를 유지할 수 있는 방안을 제시하였다.

코로나19는 겪어볼 수 없었던 사태였다. 군의 의사결정 지원체계는 어떤 상황에서도 가용성이 있어야 한다. 평시에 관련 훈련과 시스템적으로 구비하는 것과 절차에 대한 검증이 중요하다. 지원하는 절차가 정립되어 있는 것도 추진의 동력을 갖는 근거가 된다. 국방은 업무의 효율성과 보안의 효과성을 함께 고려해야 한다. 지금과 같은 상황은 단발성으로 끝나는 것이 아님은 모두가 인지하고 있다. 따라서 전향적으로 관련 기관에서 함께 머리를 맞대고 현재의 환경을 개선하기 위한 노력이 요구된다.

참고문헌(Reference)

[1] Ministry of Employment and Labor, Working from home comprehensive manual, 2020.
[2] Ministry of Science and ICT, Security guide for introducing and operating non-face-to-face environment, 2020.
[3] National Security Research Institute, A study on the introduction of the defense online telecommuting system, 2020.
[4] National Intelligent Service, Integrated security manual for remote work, 2020.
[5] Ministry of National Defense, The security guideline for network linkage of defense information system, 2017
[6] D. Kim, "Contents and implications of the U.S. supervisory authority's recommendation for a plan to continue the pandemic work of financial institution", Financial Supervisory Service, 2020.
[7] J. Kim, "The military's role and direction of development against non-traditional threats", Korea Institute for Defense Analyses, 2020.
[8] Minstry of Trade, Industry and Energy, Guidelines for corporate Continuity plan in the event of an infectious disease, 2020.
[9] I. Oh, "Shadow of the untact era: the dailyization of cyber the threats", 2020.
[10] S. Lee, "A study on the impact of COVID-19 in R&D of weapon system", 2020.

◐ 저 자 소 개 ◑

권 혁 진(HyukJin Kwon)
1989년 성균관대학교 산업공학과(공학사)
1991년 성균관대학교 산업공학과(공학석사)
2000년 성균관대학교 산업공학과(공학박사)
1991.3~2021.8 한국국방연구원 책임연구위원
2017.12~2020.12 국방부 정보화기획관
2021.8～현재 서울과학기술대학교 국방방호공학과 교수
관심분야 : 국방정보화 정책, 정보화평가, 사이버보안, etc.
E-mail : kwonhj@seoultech.ac.kr

신 동 규(Dong-kyoo Shin)
1986년 서울대학교 컴퓨터과학과(학사)
1992년 Illinois Institute of Technology 대학원 컴퓨터과학과(석사)
1997년 Texas A&M University 대학원 컴퓨터과학과(박사)
1998년～현재 세종대학교 컴퓨터공학과 교수
관심분야 : 사이버전, 사이버보안, 사이버 지휘통제, 인공지능, 정보보호, etc.
E-mail : shindk@sejong.ac.kr

신 용 주(Yong-Joo Shin)
2000년 육군사관학교 무기공학(학사)
2006년 Air Force Institute of Technology 컴퓨터시스템(석사)
2014년 한국과학기술원 전산학과(박사)
2019년～현재 한국국방연구원 현역연구위원
관심분야 : 국방정보화정책, 사이버작전, 사이버보안, 정보보호, etc.
E-mail : keen56@kida.re.kr