Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 8 pp. 524-533, 2023

https://doi.org/10.5762/KAIS.2023.24.8.524
ISSN 1975-4701 / eISSN 2288-4688

방산업체 클라우드 업무환경 도입에 따른 기술보호 방안 연구

이경민[1], 이용준[2*]
[1]극동대학교 인공지능보안학과, [2]극동대학교 해킹보안학과

A study on technology protection measures according to the introduction of the cloud business environment for defense companies

Kyung-Min Lee[1], Yong-Joon Lee[2*]
[1]Department of Artificial Intelligence Security, Far East University
[2]Department of Hacking Security, Far East University

요 약 우리는 지금 4차 산업혁명 시대에 살고 있다. 인공지능, 사물 인터넷, 빅데이터, 모바일 등이 이미 주목받기 시작했으며, 우리 생활 속에서도 많은 부분 실 사용되고 있다. 4차 산업혁명에 있어 기반 기술은 단연 클라우드라 할 수 있다. 이에 국내 방산업체에서는 클라우드 업무환경을 도입하고 있다. 그러나 최근 사이버 공격을 통한 기술유출 통해 방산업체의 핵심기술을 유출하는 사례가 발생하였다. 그러므로 클라우드 업무환경 도입 과정에서 발생할 수 있는 보안위협들을 식별하고 방산기술보호 위협을 최소화하는 과정이 필요하다. 본 연구에서는 방산업체 망분리 정책 개선 검토, 방산기업 정보보호 공유정책 마련, 차세대 망분리 기술 마련 등 세가지의 중·장기 대책 마련을 제시하였는데, 향후 방산기업에서 증가하는 보안위협에 대비하여 제시한 보안대책을 조속히 적용함으로써 클라우드 업무환경 시스템이 방산업체에 안정적으로 운영되기를 바란다.

Abstract We are now living in the era of the 4th Industrial Revolution. Artificial intelligence, the internet of things, big data, mobile technology, etc. have already begun to attract attention and are being used in many parts of our lives. In the 4th Industrial Revolution, the base technology can be said to be the cloud. Accordingly, domestic defense companies are introducing a cloud work environment. However, there has been a recent case of leaking core technologies in defense companies through cyberattacks. Therefore, it is necessary to identify security threats that may occur in the process of introducing a cloud work environment and minimize threats to protect defense technology. In this study, three mid- and long-term measures are proposed: a review of the improvement of defense companies' network separation policy, preparation of information-protection sharing policy for defense companies, and preparation of next-generation network separation technology. We hope that the cloud work environment system will be stably operated by defense companies by quickly applying these countermeasures.

Keywords : Defense Industrial Security, Cloud Computing Work Environment, Defense Technology Protection, Network Separation Policy, Information Protection Sharing Policy, Network Separation Technology

*Corresponding Author : Yong-Joon Lee(Far East University)
email: 2020032@kdu.ac.kr
Received July 7, 2023 Revised August 9, 2023
Accepted August 10, 2023 Published August 31, 2023

1. 서론

한국 방위산업의 급격한 발전으로, 경쟁국들의 국가 지원을 받는 것으로 추정되는 해커나 산업 스파이의 주된 공격 대상이 되고 있으며, 우리나라 방위 산업체 또한, 이러한 보안 위협에 항상 노출되어 있지만, 24시간 365일 보안 유지 체제를 개별 방산업체에서 갖추기에는 어려움이 큰 점도 영세한 기업이 많은 우리나라 방산업체의 보안 현실이다. 최근 클라우드 관련 사이버 공격 증대 등은 국내 방산업체에 대한 보안 환경을 더욱 어렵게 하고 있다. 클라우드를 이용하는 방산업체의 비대면 업무환경의 변화에 따른 새롭게 등장한 가상사설망(VPN)의 취약점을 이용한 해킹이나 랜섬웨어, 비즈니스 이메일 침해(BEC) 해킹 등 교묘하고 고도화되는 각종 보안 위협에 대해, 기존 국방부 국군방첩사령부의 보안측정, 재택근무를 위한 보안 규정이나 전통 보안(Perimeter Security) 대책만으로는 미흡한 실정이다[1]. 방산업체 보안 역량 강화를 위한 정부의 소관 부처가 명확하지 않으며, 정부 지원제도나 정책 또한 거의 부재한 우리나라 방산업체의 보안 현실로는, 방산업체의 사이버 위협 정보 공유는 물론이고 보안 관제, 해킹 대응, 교육 및 훈련 등 기본적인 방산업체의 사이버 대응 체계조차 갖출 수 없는 실정이다. 이에 방산기업의 클라우드 업무환경 안정적 도입 및 운영 활성화와 발전을 위해서는 방산기술 보호 위협을 감소시키기 위한 대책마련과 규정개선 등 실질적인 노력이 필요하다[2].

2. 클라우드 업무환경 동향

2.1 국내 · 클라우드 추진 방향

클라우드(Cloud)는 컴퓨팅 자원(CPU, 메모리, 디스크 등)을 원하는 대로 가져다 쓸 수 있는 서비스로 각 PC에서 개별적으로 프로그램을 설치하여 각각의 데이터를 저장하던 기존의 방식에서 벗어나, 네트워크를 통해 데이터를 저장 및 개별 컴퓨터에 할당하는 개념으로서, 물리적으로 서로 다른 위치에 있는 컴퓨터의 데이터를

가상화 기술을 사용하여 통합, 제공하는 것이다.

클라우드는 구축 유형에 따라 공공 클라우드, 하이브리드(Hybrid), SaaS, PaaS, IaaS, 프라이빗(Private) 클라우드가 있다. 퍼블릭 클라우드는 AWS, Microsoft, Google과 같은 외부의 클라우드 컴퓨팅 사업자가 HW와 SW 및 기타 IT 자원을 소유하고 서비스를 제공한다.

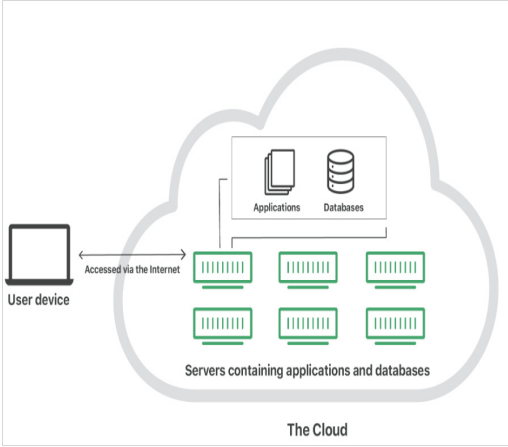

Fig. 1. cloud computing concept

기업에서 소유하고 운영하며 공용 네트워크를 통해 저렴한 비용으로 컴퓨팅 자원에 빠르게 접근할 수 있도록 지원한다[3]. 퍼블릭 클라우드 서비스를 사용하면 하드웨어, 소프트웨어 또는 지원 인프라를 제공업체에서 소유하고 관리하므로 별도로 구입할 필요가 없다. 프라이빗 클라우드는 내부적으로 또는 타사에서 관리되는지와 관계없이 단일 조직 전용으로 운영되는 인프라이다. 프라이빗 클라우드를 사용하면 자원에 대한 제어를 강화하고 멀티 테넌시를 명시적으로 조정하면서 클라우드의 효율성을 활용할 수 있다. 하이브리드 클라우드는 프라이빗 클라우드를 기반으로 퍼블릭 클라우드 서비스를 전략적으로 통합하고 사용한다. 실제로 프라이빗 클라우드는 회사 내 다른 IT 자원 및 퍼블릭 클라우드와 격리된 상태로 존재할 수 없다. 프라이빗 클라우드를 사용하는 대부분 기업은 통상 하이브리드 클라우드를 구축하여 데이터센터, 프라이빗 클라우드 및 퍼블릭 클라우드 전체에서 워크로드를 관리한다. 이 외에 SaaS, PaaS, IaaS는 다음과 같다.

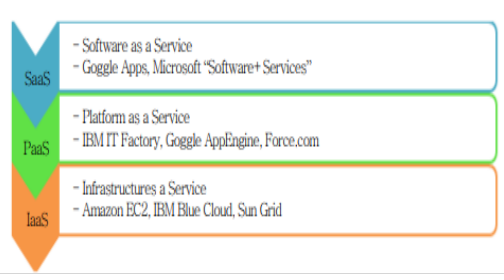

Fig. 2. Classification of cloud computing according to service construction

국내외 다양한 기업들이 정보를 효과적으로 관리하기 위해 많은 시간과 비용을 들여 위와 같은 클라우드를 구축하고 있다. 국내외를 막론하고 코로나19 팬데믹으로 기업의 업무환경 및 공간이 원격형태 변하였고, 이를 경험해본 사람들의 인식변화로 인해 높아진 원격업무를 안전하게 보장하기 위해서이다. 이에 각국의 기관 및 기업에서도 경영의 효율화를 위해 유연성을 보장하고 시간과 장소에 관계없이 업무에 접근할 수 있는 클라우드 업무 보장을 위한 정책을 지속 개발하고 있다[4]. 이러한 정책은 기업 중심의 공공 클라우드와 정부 주도의 공공 클라우드를 기술적인 관점에서 비교·분석할 수 있다. 이러한 클라우딩에 대한 수요는 앞으로 지속해서 늘어날 것이다. 가트너(Gartner)가 발표한 전세계 공공 클라우드 서비스 사용자 비용 규모 전망치를 살펴보면, 2021년 4,109억 달러에서 20.4% 증가한 4,947억 달러에 달하며, 2023년에는 그 규모가 6,000억 달러에 달할 것으로 예측되었다. 서비스 등이 IT기술을 중심으로 재편되었고 이러한 기술을 구현하는 인프라 환경은 기업 비즈니스를 영위하는데 중요한 요소가 되었으며, 최근 기술의 흐름에 따라 많은 기업들이 인프라 환경을 공공 클라우드로 구성하는 사례가 늘어나며, 기업의 정보자산을 공공 클라우드 환경에 보관하는 사례가 늘어나게 되었다[5]. 이 뿐 아니라 국내 공공 클라우드 시장도 지속 발전하고 있다.

Table 1. Domestic public cloud service market size
(unit: billion won)

year	2018	2019	2020	2021	2022
budget	1,940.7	2,342.8	2,781.8	3,240.1	3,723.8

공공 클라우드의 장점은 워크로드를 간단히 확장하고, 축소할 수 있다는 점이다. 공공 클라우드를 사용하고자 하는 사용자는 클라우드 공급 업체를 통해 사용 신청을 하고 필요한 리소스를 간단하게 생성시킬 수 있다. 예를 들어 웹 서비스를 하기 위해 기존에는 서버를 구매하거나, 임대하고 그 장비들을 위치할 장소를 선택해야 한다. 서버의 구매나 임대의 과정에는 짧게는 며칠에서 길게는 몇 주의 기간이 필요하다. 하지만 공공 클라우드를 사용하게 된다면, 몇 시간 만에 서버를 생성하고 서비스를 제공할 수 있게 된다[6]. 또한 사용한 만큼만 비용이 발생하기 때문에 효과적으로 워크로드를 구현할 수 있다. 또한 최근에는 클라우드 공급업체가 제공하는 PaaS(Platform as a Service)를 통해 서비스를 구현하고 있다. 기존에 우리가 알고 있던 네트워크와 서버 없이 서비스를 제공하는 환경이 마련되어진 것과 같다. 또한 공공 클라우드는 하드웨어에 대한 유지관리가 필요하지 않다는 점과 무제한에 가까운 확장성을 제공한다는 장점을 가지고 있다[7].

2.2 국내 · 외 클라우드 도입 사례

국외의 경우 가트너(Gartner)가 발표한 2022년 전세계 퍼블릭 클라우드 서비스에 대한 최종 사용자 지출 전망에 따르면, 전 세계 퍼블릭 클라우드 서비스 지출은 2021년의 4,109억 달러에서 20.4% 증가한 4,947억 달러로 성장할 전망이다. 2023년에는 최종 사용자 지출이 6,000억 달러에 달할 것이라는 분석이다[8].

Table 2. Global cloud market size
(unit: billion dollars)

division	2021 year	2022 year	2023 year
budget	410,915	494,654	599,840

클라우드 서비스에 가장 부각되고 있는 분야는 서비스형 인프라(IaaS) 분야다. 서비스형 인프라(IaaS)는 2022년에 30.6%로 가장 높은 최종 사용자 성장세를 보일 것으로 나타났다. SaaS는 2022년 최종 사용자 지출이 1,766억 달러에 이를것으로 예상되는 최대 퍼블릭 클라우드 서비스 시장 부문으로 남아있다. 가트너는 기업이 클라우드 마켓플레이스와 같은 다양한 경로를 통해 SaaS 시장에 진입하고 보다 효율적인 데브옵스(DevOps) 프로세스를 위해 더 큰 규모의 단일 애플리케이션을 구성 가능한 부분으로 계속 분할함으로써 해당 부분에 대

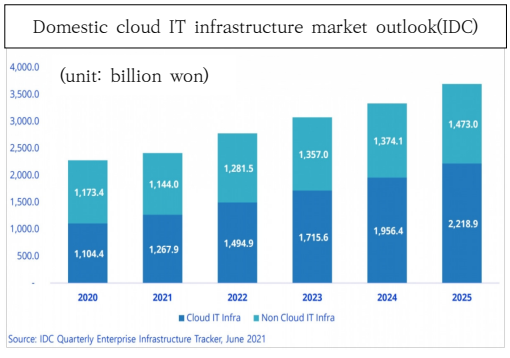

Fig. 3. Domestic cloud IT infrastructure market outlook

한 기대가 늘어날 것으로 전망하고 있다.

국내 사례를 살펴보면, IDC는 2021년 클라우드 IT 인프라 시장 전망 보고서에서 국내 클라우드 환경에 도입되는 IT 인프라 시장이 향후 5년간 연평균 성장률(CAGR) 15%로 2025년에는 2조 2189억원의 매출 규모에 이를 것으로 평가했다.

지속적인 기업의 디지털화로 인해 증가하는 클라우드 시장에 도입되는 국내 디지털 인프라 시장을 전망한다. COVID-19 이후 일반 기업은 물론 금융, 공공, 교육 등 다양한 조직의 클라우드 전환이 가속화되면서 클라우드 환경으로 도입되는 IT 인프라는 전체 시장의 50%를 넘어설 것으로 예상된다. 또한, 클라우드 컴퓨팅 리소스의 지속적인 증가로 대기업을 포함한 하이퍼스케일 사업자들이 클라우드 인프라를 점진적으로 확장하면서 2025년에는 국내 IT 인프라 시장의 60%가 클라우드 환경으로 도입될 전망이다. 해당 보고서에 따르면, 최근 국내 기업들은 보다 유연하고 민첩한 비즈니스를 지원하기 위해 전통적이 IT 인프라 기반의 시스템 환경에서 퍼블릭을 포함한 프라이빗 클라우드 환경으로 전환하는 추세이다[9]. 복잡해지는 요구사항과 꾸준히 증가하는 컴퓨팅 리소스 및 데이터의 효율적 관리의 필요성은 클라우드로의 전환을 더욱 확대시키고 있는 것으로 분석됐다. 특히 팬데믹의 장기화는 기업의 디지털화에 큰 몫을 했다. 클라우드로의 전환에 보수적이었던 금융권에서는 프라이빗 클라우드 뿐만 아니라 퍼블릭 클라우드에 대한 관심도 높아지고 있으며, 정부의 클라우드 장려 정책은 클라우드 서비스 공급자를 포함한 사용자 지원 정책을 강화해 국내 에코시스템을 견고히 만들고 있다[10].

국내 클라우드 기업은 IDC를 설립하기 시작했다. IDC는 클라우드를 구현에 절대적으로 필요한 핵심 요소이다. 과거 기업들은 서버를 운용하는 별도의 서버실을 뒀고, IT 담당자들은 서버실에서 회사의 IT 인프라를 관리했다. 하지만 최근에는 IT 인프라 트렌드가 클라우드로 옮겨서, 이 같은 인프라를 확보하고 관리하고 있다. 국내 CSP(Colude Service Provider) 기업인 KT, NHN, 네이버는 클라우드 서비스 품질과 네트워크, AI 품질 등을 고도화하기 위해 고성능의 IDC를 새로이 짓거나 고도화하기 시작했다. 데이터센터 설립과 관련, 일각에서는 해외 클라우드 사업자들이 IDC를 적극적으로 설립하기 시작하자 데이터 주권을 강점으로 내세우던 국내 CSP들은 보다 차별화되고 해외 기업에 견줄만한 클라우드 서비스를 제공하고자 인프라를 확충하고 있다는 분석도 나온다[11].

KT 클라우드는 KT의 클라우드·IDC 사업부에서 추진하던 IDC 비즈니스를 모두 흡수한 결과 기존 KT가 보유했던 IDC 소유권을 모두 가져와서, 목동 1, 2를 비롯해 여의도, 부산, 대전, 대구, 천안, 김해 등에 보유했던 IDC를 고도화하는 쪽으로 방향으로 2021년 기준 총 14개의 IDC를 보유하게 됐다. 네이버 클라우드는 신규 IDC 설립 외에도 시, 도에서 설립하는 IDC의 데이터센터를 AI화 할 수 있도록 부천시에 AI데이터센터를 설립하였다. 네이버클라우드는 뉴로클라우드를 기반으로 부천시 데이터센터와 네이버클라우드의 서비스를 하이브리드 클라우드 환경으로 구현하였다. NHN 클라우드는 김해시와 5,000억을 투자해 2023년 상반기 착공 계획을 위해 클라우드 데이터센터를 건립하고 R&D 센터를 구축하며 스마트시티 플랫폼을 기반으로 한 스마트홈 시범단지를 조성한다는 협약을 체결했다. 아울러 순천시와 민관협력형 클라우드 데이터센터 설립에 돌입했다.

코로나19 팬데믹에서 비롯되어 보편적으로 확장된 원격업무가 다양한 장점을 보장한다는 것이 증명되자 많은 기업들이 업무방식을 바꿔 원격업무의 유지 및 확장 방안에 집중하고 있으며, 이를 위해 클라우드 환경이 적극 도입되고 있다[12]. 다수의 기업들은 애플리케이션 운영, 자동화, 인공지능(AI), 챗봇 등 인프라를 필요로 하는 신기술을 도입하였다. 그러나, 신기술의 기능을 제대로 활용하기 위해서는 클라우드가 핵심이고, 기존 인프라 환경에서는 대용량의 데이터를 저장하기도 쉽지 않고, AI와 머신 · 딥러닝을 활용한 데이터 분석이 어려웠기 때문에, 많은 기업들이 이러한 것을 가능케 하는 환경을 구축 중에 있다. 따라서 향후에는 멀티 클라우드 또는 하이브리드 클라우드에 대한 수요가 있을 것이다. 멀티 또는 하이브리드 클라우드는 특정 공급기업에 국한되지 않고 상황에 맞는 최적의 시스템을 활용할 수 있는 장점으로 주목받고 있다[13]. Right Scale에 따르면 종업원 1,000명 이상 기업은 82%, 1,000명 미만 기업은 64%가 이러한 클라우드 전략을 추구한다. 데이터와 컴퓨팅 특성과 사용 목적에 따라 자체 인프라 또는 퍼블릭 클라우드 중에서 어느 쪽이 최적인지를 판단하고 복수의 서로 다른 시스템을 넘나들면서 효과적으로 활용할 수 있는 기술과 역량이 중요해졌다. 이러한 클라우드를 실현하는 과정에서 컨테이너의 활용이 확대되고 관련 기술 개발이 빨라질 전망이다. 컨테이너를 활용하면 다른 서비스 공급자의 시스템으로 손쉽게 이전하여 원활한 작업이 가능해지기 때문이다. 다중 컨테이너를 관리하는 시스템은 구글의 쿠버네티스가 시장의 표준으로 안착하고 있어 구

글의 클라우드 기술 분야에서의 영향력은 더욱 커질 전망이다.

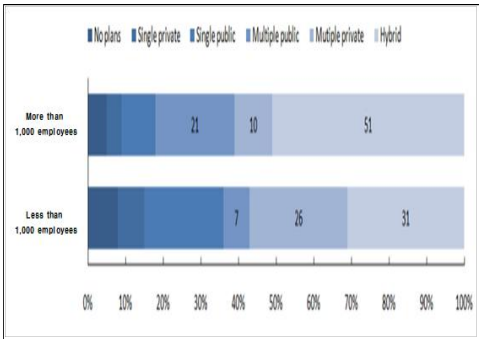

Fig. 4. Cloud strategy by company size (reference: Right Scale (2018))

2.3 방산업체 클라우드 추진방향

원격근무 관련해서 방산업체의 경우 클라우드 기반 VDI(Virtual Desktop Infrastructure) 기술에 주목하고 있다. VDI는 기존사용자 컴퓨터에서 가상머신(Virtual Machine)을 구동하던 기술에서 발전하여 서버의 자원을 통해 어느 PC에서든 가상의 Desktop 환경을 사용할 수 있도록 하는 시스템이다[14]. 이러한 VDI는 PC에 LAN선만 연결되어 있으면 모든 프로세스를 서버에서 처리하여 그 결과를 원격근무 PC ↔ 회사 내부망 등에 전송해주며, 서버가 모든 데이터를 중앙 통제하기 때문에 통해 관리적과 보안적인 이점을 가진다. 현재 국내외 여러 기업에서 활용중이며, 특히 국방에서는 이러한 VDI를 내부망으로 운용하여 보안을 강화하고자 2015년부터 국방통합데이터센터를 중심으로 각 부대의 전산시스템을 단계적 통합 및 클라우드 퍼스트 정책을 추진하여 주요 체계의 클라우드 전환을 진행중에 있다. 방산업체 VDI 도입 타당성은 국방과 같이 보안권한 관리 모델이 Role-Base인 만큼 군과 VDI를 통해 사용자의 작업환경을 중앙관리하면 원격근무가 지원되면서도 효율인 시스템 운영이 가능하고, 업데이트나 패치 관리가 용이하여 제반능률 향상에 기여할 수 있다. 또한 업무 특성상 국가안보에 직결되는 군이나 방산업체의 경우 중앙통제 권한 확대로 보안에 유리한 환경을 조성할 수 있는 여건이 마련되었다. 국방 및 방산업체에서 클라우드 기반 VDI를 도입 시 미칠 영향은 다음과 같다.

관리적 측면에서 VDI기술의 NAC(Network Access Control)를 통해 업무용 PC의 접근을 통제하고 PMS(Patch Management System) 등을 관리하고 있음을 알 수 있

Table 3. Feasibility of adopting cloud-based VDI for defense and defense industries

division	current system	building VDI
administrative	Individual user management	Central integrated management
secure	user short hair security burden	virtual environment realtime monitoring
economical	high-end terminal PC periodic replacement	system construction cost

는데, VDI가 도입되면 서버를 통해 관리자가 직접 통제하여 업데이트나 패치를 하므로 PMS 등을 추가 운용해야 할 필요가 없어 관리 소요를 줄일 수 있고, 데이터를 중앙에 저장하기 때문에 손실의 우려가 적으며 저장공간도 중복된 부분이 없이 효율적으로 활용이 가능하다. 이러한 이점을 통해 사용자는 어떤 PC를 사용하더라도, 원격으로 업무의 연속성을 보장할 수 있고 다양한 우발 시 비상계획에 대한 고려가 감소한다. 또한 성능 측면에서 컴퓨팅 자원을 효과적으로 분배할 수 있어서 사용자 작업환경의 성능 극대화와 자원의 효율적 분배가 동시에 가능하다. 망분리 모델에서는 개인PC를 사용하다가 공격자에게 탈취되어 데이터의 손실이 발생할 경우 네트워크를 통해 서버가 직접 피해를 입을 수 있는데, 이러한 경우에는 PC의 이상징후와 네트워크 트래픽, 서버의 영향을 연관시키기 위해 많은 노력과 시간이 필요하고, 이러한 보안체계를 실시간으로 연동하기 위해서는 큰 노력이 투입된다. 반면 VDI의 경우 VDI 작업환경에 대한 원격접속만 가능하며 그 외의 접속은 차단할 수 있고, VDI를 통한 통제된 작업환경만 제공되어 악성 앱이나 악성코드 등의 유입을 차단할 수 있으며, 악성코드가 유입되더라도 모든 프로세스가 VDI서버에서 통제되므로 외부의 침해에 대한 실시간 감시 및 대응이 중앙에서 가능하여 모든 PC에 대한 일괄적 보안정책 적용이 가능한 장점이 있다. 또한 모든 자료는 서버 외 유출통제와 사용자 작업환경의 모든 로그가 실시간 감시되기 때문에 특히 내부자 위협에 대해서도 보안이 보장된다. 경제적 측면에서 초기 체계 구축 비용이 발생할 수 있다. 이러한 이유로 많은 방선업체에서 VDI의 도입에 제한을 가진다. 하지만 업무용 PC 도입 및 리스에 투입되는 예산을 차단하고 저사양의 PC환경에서도 충분히 일할 수 있는 환경을 제공하는 VDI는 초기 체계구축 비용에도 불구하고 장기적으로 보면 예산 절감에 기여할 수 있다.

한화시스템처럼 ICT 기반 업무를 하는 업체는 원격소요가 있지만, 제조업 중심의 대부분의 업체는 원격근무

소요 자체가 적다. 이에 VDI 같은 체계를 구축하려 하지 않을 수 있다. 또한 기존 업체들이 망분리가 안되어 있다면 VDI를 우선 구축하겠지만, 대부분 업체가 실태조사 등을 받아야 하는 이유로 방산망 등 망분리와 VPN 등이 이미 구축되어 있기 때문에 VDI를 추가로 도입하려 하지 않을 수 있다. 따라서 VDI의 도입이 시행되기 위해서는 각 업체별 VDI도입에 대해 관리, 보안, 경제성 측면을 면밀히 분석하여 타당성을 제시하고, 현재 VDI를 도입한 업체의 임직원을 대상으로 설문조사를 진행하여 VDI를 제공할 수 있도록 홍보가 필요하다.

3. 클라우드 시대의 보안 위협

3.1 클라우드 환경에서의 보안에 대한 우려

클라우드의 등장을 계기로 기존과는 다른 새로운 보안 위협과 과제가 등장하고 있다는 게 전문가들의 진단이다. 미국의 클라우드 컴퓨팅 관리 회사인 라이트스케일(RightScale)에 따르면 기업들은 클라우드 도입 시 보안 이슈를 가장 큰 어려움으로 생각한다고 보고서를 통해 전했다. 엔터프라이즈 컴퓨팅 기업 뉴타닉스가 발표한 2019 글로벌 엔터프라이즈 클라우드 인덱스 보고서에서도 조사 응답자 중 60%가 클라우드 전반의 보안 현황이 향후 클라우드 배포에 가장 큰 영향을 미칠 것이라는 조사 결과를 발표했다. 클라우드의 도입은 혁신, 비용절감, 유연성 등 여러 장점이 있지만, 클라우드 전문가 부족과 보안에 대한 문제가 가장 큰 우려 사항이라는 것이다.

최근 1~2년 동안 클라우드에서 발생한 보안 사고는 큰 파장을 일으켰다. 2018년 11월 AWS 서울 리전에서 내부 DNS 서버 설정 오류로 인해 84분 동안이나 DNS 기능을 할 수 없어 AWS를 사용하는 쿠팡, 배달의민족, 이스타항공, 업비트 등에서 접속 오류 현상이 나타났다. 2019년 7월 미국의 대형 은행인 캐피탈 원(Capital One)에서는 1억 600만 명이 넘는 고객 정보가 해킹 당했는데, 유출된 데이터는 AWS에 저장된 것으로 알려져 AWS의 보안 취약성이 드러나기도 했다. AWS는 클라우드 보안의 문제라기보다 클라우드를 사용하는 기업이 보안 설정을 잘못했기 때문이라고 밝혔다. 이 같은 클라우드 보안 사고에서 보듯이 가트너는 95% 이상의 클라우드 보안 사고가 클라우드 사용자의 관리 책임이 원인일 것이라고 발표했다.

IT 인프라 운영 및 보안 전문가들이 가장 우려하는 점은 데이터의 유출 또는 유실이다. 이러한 우려는 여러 원인이 있지만, 플랫폼으로서의 서비스(Platform as a Service) 활용이 보편화 되면서 클라우드에서 이루어지는 작업 대부분이 블랙박스 형태로 전문가들조차 내부에서 무슨 일이 일어나는지 확인이 어렵기 때문이다.

3.2 클라우드 환경에서의 보안 위협

클라우드 보안 협회(Cloud Security Alliance, CSA)는 241명의 클라우드 전문가들을 대상으로 설문조사를 진행해 2019 클라우드 위협 보고서를 발표했다. 이 보고서는 전통적으로 클라우드의 위협, 위험 및 취약성에 대한 인식을 제고하기 위한 것이다[15]. 응답자들은 클라우드 환경에서의 주요 위협을 다음의 11가지로 꼽았다.

1. 데이터 침해
2. 잘못된 구성 및 부적절한 변경 제어
3. 클라우드 보안 아키텍처 및 전략 부족
4. 불충분한 아이덴티티, 자격 증명, 액세스 및 키 관리
5. 계정 도용
6. 내부자 위협
7. 안전하지 않은 인터페이스와 API
8. 취약한 제어 영역
9. 메타 구조와 응용 구조 실패
10. 제한된 클라우드 사용 가시성
11. 클라우드 서비스의 남용 및 악의적인 사용

서비스 거부, 공유 기술 취약성 및 CSP(Cloud Service Provider) 데이터 손실, 시스템 취약성과 같은 문제는 이 보고서에서 제외했다. CSP의 책임하에 있는 전통적인 보안 문제는 그다지 중요하지 않은 것으로 판단했기 때문이다. 대신, 고위 경영진들은 기존 기술보다 높은 보안 문제를 해결해야 할 필요성이 커지고 있다.

3.3 전문가 의견

클라우드 보안은 사이버 위협, 무단 액세스 및 데이터 위반으로부터 클라우드 플랫폼에서 호스팅되는 데이터, 애플리케이션 및 인프라를 보호하는 것과 관련된 클라우드 컴퓨팅의 중요한 측면이다. 클라우드 컴퓨팅이 계속해서 대중화되고 널리 채택됨에 따라 클라우드 보안은 민감한 데이터를 저장하고 처리하기 위해 클라우드에 의존하는 기업, 조직 및 개인에게 최우선 순위가 되었다.

국내 전문가 의견에 따르면 클라우드 보안은 위험을 완화하고 클라우드 기반 리소스의 기밀성, 무결성 및 가

용성을 보장하기 위해 다계층 접근 방식이 필요한 복잡하고 진화하는 분야이다. 클라우드 보안 에코시스템에는 다양한 유형의 사이버 위협으로부터 보호하기 위해 클라우드 서비스 공급자와 클라우드 고객 모두가 구현하고 유지 관리해야 하는 다양한 보안 제어, 도구 및 프로세스가 포함된다[7].

클라우드 서비스 공급자는 인프라와 고객 데이터를 보호하기 위해 강력한 보안 조치 및 표준을 구현할 책임이 있다. 이러한 조치에는 물리적 보안, 액세스 제어, 암호화, 네트워크 보안 및 사고 대응 계획이 포함될 수 있다. 반면에 클라우드 고객은 적절한 보안 조치를 구현하고 강력한 암호, 다단계 인증 및 정기적인 보안 평가와 같은 모범 사례를 준수하여 클라우드를 안전하게 사용하고 있는지 확인해야 한다.

또한 클라우드 보안은 만능 접근 방식이 아니라는 점에 유의해야 한다. 조직 또는 개인의 보안 요구 사항은 데이터 유형, 산업, 규정 요구 사항 및 위험 허용 범위에 따라 다를 수 있다. 따라서 클라우드 보안이 효과적이려면 이러한 요소를 고려한 맞춤형 접근 방식이 필요하다.

전반적으로 클라우드 보안은 위험을 완화하고 중요한 데이터의 보호를 보장하기 위해 능동적이고 협력적인 접근 방식이 필요한 클라우드 컴퓨팅의 중요한 측면이다. 클라우드 서비스 공급자와 클라우드 고객 모두 사이버 위협으로부터 보호하기 위해 효과적인 보안 제어를 구현하고 유지 관리할 공동 책임이 있다.

4. 결론

2022년 가트너 조사에 따르면 현재 미국의 경우 DoD 등 방산과 직접 관련된 정부기관은 물론 방산기술보호 대상기관(레이시온, 록히드 마틴 등) 등이 모두 인터넷 기반 CaaS, SaaS, Paas, IaaS는 물론 하이브리드와 프라이빗 등 다양한 클라우드 컴퓨팅 기술을 적극 활용 중에 있다. 이러한 이유로 다수의 컨설팅기업은 국가안보와 직결되는 방산관련 중요정보의 적시적인 공유 필요성과 업무의 유연성 및 효율성을 극대화하고자 하는점을 꼽고 있다. 국내 방산업체는 4차 산업혁명 진행의 기조와 함께 클라우드 컴퓨팅 역시 중점적으로 고려해야 하는 신기술 분야이며, 클라우드 기술로 중요 데이터를 종합할 수 있다면 미국의 CMMC(Cybersecurity Maturity Model Certification)와 유사한 체계를 구축하는데 필요한 일을 반절이상 줄인 것과 다름없다고 평가하고 있다. 이러한 미국 CMMC와 연계하기 위해서라도 클라우드의 방산기술보호 대상기관 및 업체를 대상으로 도입할 필요성은 충분하다.

첫째, 국내 방산업체들의 보안체제는 비교적 견고하다는 평가를 받고 있다. 기존의 방산업체의 보안은 물리적 망분리인데, 이 방식의 문제는 개인 PC에 저장된 파일을 이동식저장매체를 이용해 외부로 유출할 수 있는 위험을 차단하기는 어렵다. 보안성 자체만을 비교하자면 물리적인 방식이 우위에 있으며, 국방 및 특수 정보기관에서도 불편함을 감수하고서도 물리적인 망분리를 선택하는 이유이기도 하다. 그러나 방산업체 및 방산 기술보호 대상기관에서 보안성과 업무효율을 위해서는 논리적 망분리를 고려해야 한다.

Table 4. Comparison of physical and logical network separation (Source: Somansa)

item	physical network separation	logical network separation
security	relative high	high
Ease of use	relative high	high
Managemen convenience	relative high	high
price	high price	physical network separation 50% price compared to
When working from home network separation	impossible	possible
When working from home Response to server failure	impossible	possible

특히, 원격업무 시 방산업체 및 대상기관에서는 논리적 망분리만을 적용할수 밖에 없다. 대다수 민간기업과 금융기관에서도 원격근무 시 논리적 망분리로 변경되고 있다. 원격근무 시에 장애대응을 위해 회사 주요 서버에 접근해서 복구해야 하는데, 물리적 망분리로는 조치가 불가능하기 때문이다. 대다수의 관련분야 방산 및 보안 전문가들은 국가안보를 위해서라도 일정 부분 정부의 지원이 필요하며 세부 지원방안의 마련이 필요하다.

망분리를 통한 데이터 운용에서 기밀자료의 유출을 방지하기 위해서는 먼저 기관이나 업체에서 공통으로 얘기하는 '기밀자료'라는 것이 정확히 어떤 것인지, 방산기술보호 지침이나 방산보안업무훈령 상에서 기밀자료 데이터의 분류가 잘 되어야 한다. 이는 유출되지 않고 반드시 지켜야 될 데이터와 굳이 지키지 않고 유출되어도 문제

가 없을 데이터의 분류를 의미한다. 예를 들면 정말로 유출되거나 오용되면 국가안보에 치명적 혹은 현저한 위험을 초래할 방산기술이 있다고 가정을 해보자. 이런 것들은 방산업체의 단독망인 방산망으로만 유통되어야 하고 일반 인터넷망으로는 이동 자체가 되어서는 안 될 것이다. 그러나 이러한 자료가 아니라 그냥 일반적으로 업무상에서 주고받은 자료라면 이런 것들은 인터넷망으로 소통해도 상관은 없을 것이다. 지침이나 훈령에서 이러한 데이터를 분류를 잘 해줘야 한다. 그러함에도 불구하고 현재 업체 관계자들에 대한 설문을 해보면 방사청에서 관리하는 지침과 방첩사에도 관리하는 훈령이 상이하여 데이터 분류에서조차 혼란을 초래하는 부분이 있는 것으로 확인되고 있다. 방산기술보호법에 따라 어떤 업체가 구성한 업무망이 지침상에는 물리적 망분리 조건을 충족하지 못 할 수 있음을 지적한다. 이런 경우 다양한 혼선을 초래하며, 이러한 차이는 현재 지침과 훈령상에서 다양하게 찾아볼 수 있다. 다시 말해서 “업무망과 일반망을 이분법적으로 나누면 안 되고 '비밀을 취급해야 되는 망', '군사비밀을 취급해야 하는 망', '방산기술을 취급해야 되는 망' 등을 물리적 망으로 분리해라.“ 식으로 네트워크 중심의 망분리가 아니라 데이터 중심의 분류를 제대로 해놓고 그 데이터별로 망을 어떻게 구성할 것인가를 고민해야 하며, 이러한 내용이 지침과 훈령이 일관성 있게 개정되어야 할 필요성이 있다.

둘째, 방산업체를 대형과 소형으로 분류해, 대형 방산업체는 자체 보안 대책을 강구하도록 조치하고, 소형 방산업체는 방산 ISAC(방산보안정보공유분석센터)이나 방산 공동 보안관제 센터 등을 구축 및 운영하도록 정부가 지원하는 것이 바람직하다고 생각한다. 이를 위해서는 방산업체 보안 역량 강화를 위한 정부 소관 부서를 명확히 하여, 체계적이고 지속적인 정부의 정책이 수립되고 집행되어야 한다. 마지막으로, 방산업체 보안 역량 강화는 국방사이버안보 및 국방 안보 역량 강화와 직결되므로, 방산업체 자체 보안 대책은 물론이고, 방산 공급망 보안 인식 제고 등 영세 방산업체 보안 강화 지원을 위한 방산업체 정보보호대책 가이드라인 등 방산업체 보안 정책이 제정이 필요하다.

셋째, 2022년 현재 지난 5년간 우리나라 국방과학기술 수준이 크게 발전함에 따라 현재 세계 9위권으로 평가받고 있으며, 방산수출액도 2006년 2.5억불에서 2014년 이후 현재까지 매년 지속 증가하였다. 이와 같이 방산수출 및 기술이전 등의 증가로 기술유출 가능성이 점차 증대되었고, 최근 코로나19 팬데믹로 인해 사이버 공격을 통한 기술유출 통해 방산업체의 핵심기술을 유출하는 사례가 발생하였다. 이는 방산업체 뿐만 아니라 공공기관, 주요 산업시설 등 국가 주요 인프라가 사이버 공격으로 인해 기능이 마비될 경우 국가안보에 치명적 위험을 초래할 수 있기 때문이다. 특히 IoT, 클라우드, 모바일이 연결되는 초연결 시대에서 차세대 네트워크를 통한 망분리 보안은 더욱 강조되고 있다. 그간 국방부를 비롯한 국내 주요 공공기관들은 구축된 시스템의 신뢰성 높은 보안 접속·관리 기술의 부재로 사이버 공격에 취약하다는 목소리가 높았다. 기존의 물리적 망분리 중심의 네트워크 보안은 인증체계의 한계와 정보체계 관리의 어려움이 있었다. 최근 패러다임의 변화로 비인가(미확인) 애플리케이션, 모바일 단말 등의 사용이 확대되면서 기존의 보안체계로는 대응이 어렵다는 전문가들의 의견에 따라 국방부를 비롯해 주요 공공기관에서는 네트워크망 공격에 대응하는 새로운 보안기술을 도입하고 있다. 기존 망분리 방식은 시장성이 없어 이에 대한 차세대 망분리 방법을 대비하여야 한다. 현재 망분리 업계에서 기대하는 방산 시장은, 1000억원 정도 규모를 이룰것이라고 전망되는데, 이는 한 사업당 10억원 정도의 예산이 소요될 것으로 예상하고 계산한 것이다. 솔류션 비용과 OS·애플리케이션 라이선스, 2~3개월에 걸친 구축비용 등을 감안하면 벤더와 구축 업체 입장에서는 그리 큰 수익을 기대할 수 있지 않다. 그래서 민간 대기업, 외산기업들은 클라우드에 집중하여 차세대 망분리 시스템으로 대비를 하고 있다. 이에 다음과 같이 차세대 망분리 환경 구성을 위해 체계적으로 대비하여야 한다.

최근 北·中 등의 사이버 공격 위협이 갈수록 심각해지면서, 기존의 물리적 망분리만으로 국방보안과 방산업체들의 핵심 기술정보를 보호하는데 충분치 않다는 우려가 지속 제기되었다. 이에 기존의 물리적 방분리를 통한 보안시스템과 함께 클라우드 기반 IT 플랫폼을 구축해 논리적 망분리로 이를 보완해야 한다는 견해가 설득력을 얻고 있다. 또한 코로나19 팬데믹으로 인해 원격근무 등 ICT를 기반으로 하는 온라인 원격 서비스가 활성화되면서 이에 따른 보안 취약점이 발생하였다. 특히 방산업체 및 관련업체 등은 국가안보를 위해서라도 이러한 사이버 보안 위협 및 해킹 공격으로부터 피해를 입지 않도록 철저한 대비가 요구된다.

- VDI 망분리

방산업체가 망분리 사업을 할 때, 물리적 방식 외에 다른 방식을 선택할 때는 국방부 장관의 승인을 받도록

되어 있다. 그러나 업계에서는 물리적 방분리가'의무'는 아님을 강조하며 논리적 방식도 수용될 수 있다고 기대하였다. 보안 측면에서 봤을 때 논리적 방식도 물리적 방식만큼 높은 보안 수준을 가질 수 있다. VDI는 서버에서 데이터를 가져오기 때문에 데이터 저장 방식만으로 보면 물리적으로 분리된 것이나 마찬가지다. 가상 PC는 중앙에서 관리하지만 물리적 방식의 인터넷 PC는 개개인이 관리하고 중앙 관리가 쉽지 않기 때문에 보안을 우회하는 시도가 더 쉽다는 맹점도 있다. 망분리 비의무 대상 기업들은 논리적 망분리를 선호한다. 물리적 망분리가 이론적으로 가장 강력한 보안 수준을 갖고 있지만, 쉽게 보안을 위배할 수 있기 때문에 인적사고를 막을 수 없다. VDI는 사용자단이 아닌 서버단에서 업무가 진행되기 때문에 정보 유출이나 해킹이 쉽지 않고, 해킹을 당했다 해도 감염된 가상 PC만을 삭제하면 되므로 보안을 강화할 수 있다.

- 통합 망분리 환경

망분리 환경의 문제는 망연계 시스템에서 비롯된다. 망을 분리한 상태에서 외부 인터넷의 자료를 내부 업무망으로 보내려 한다면, 망연계에서 보안 정책과 보안 점검을 한 후 허용해야 한다. 보안 분석에 시간이 걸리고 망연계 시스템에서 병목현상이 발생해 자료전송에 상당한 시간이 걸리며, 이미지, 외부 링크 등은 업무망으로 전송이 어렵다. 단일 벤더에서 망분리·망연계 솔루션을 구축하기 때문에 복잡성을 해소하여 장애 발생 시 신속하게 대응할 수 있고, 구축 및 운영 비용도 크게 줄일 수 있다.

- 망연계 기술

망연계의 정식 명칭은'망간자료전송'으로 내부망과 외부망으로 망이 분리되어 서로 보안 수준이 상이한 환경에서 데이터를 안전하게 전송하는 체계를 말한다. 망분리 환경에서 자료 전송이 필요할 때 보안 정책을 가장 잘 준수하면서 사용할 수 있는 보안 솔루션이다. 망연계 기술은 1세대 스토리지(Storage), 2세대 소켓(Socket), 3세대 인피니밴드(Infiniband)로 진화되어 왔다. 특히 3세대 방식은 최소의 응답 지연을 통한 최고 속도를 제공하면서 높은 보안성과 합리적인 비용까지 보장하는 기술로 80%이상의 보급률을 보이고 있다. 최근에는 클라우드와 개방형 OS 등 최신 IT 환경에서 적용될 수 있도록 기술개발이 진행 중이다. 망연계는 Covid-19로 인해 업무 환경이 급격히 변화하면서 망분리 사업에만 국한되지 않고 망분리 환경의 보안 상태를 최대한 유지하면서 업무에 꼭 필요한 최소한의 데이터만 전송하자는 취지에서 도입되는 것이다. 그럼에도 불구하고 만약의 상황을 대비해 망연계 솔루션은 승인 및 반출 기능을 제공하며, 정보 유출 방지에 도움이 되는 APT, DRM, DLP, CDR, 백신 등의 보안 솔루션과의 연동을 지원한다.

- 망분리 지원제도

방위산업기술 보호를 위한 조직, 기술보호체계 등을 스스로 마련하여 방위산업기술 유출방지 기반을 강화하는 것을 말한다. 특히 방산업체 대기업을 제외한 협력사 및 중소업체들은 망분리 사업에 사용되는 비용 문제로 인해 망분리를 구축하지 않고 심지어 보안관리자도 충분하지 않은 상태이다. 이를 위해서 정부에서는 자율적 보호체계 구축과 관련하여 우선적으로 고려하여야 할 것은 중소업체에 대한 지원방안을 마련하여 중소업체의 금전적인 부담을 경감시킬 수 있는 대책이 필요하다.

- 스마트NAC (SmartNAC)

2017년부터 국내 방산업체 24곳의 망분리 환경에 스마트NAC을 구축하여 좋은 평가를 받았다. 공공·금융·방산업체와 같이 망분리가 의무화된 곳은 망분리 환경의 운용 및 관리를 위한 네트워크 접근제어 솔루션 도입이 필수적이다. 스마트NAC은 망분리 환경에 따라 증가한 관리 단말을 IP/MAC 주소 차단 및 변경 금지, IP주소 충돌 방지, 사용 기간 지정 등의'IP주소 관리'기능을 통해 효율적으로 관리할 수 있다. 또한 인가되지 않은 단말이 네트워크에 접근하면 실시간 감지를 통해 즉시 네트워크를 차단한다. 해외 바이어, 외주 인력, 게스트 등 망을 제한적으로 사용해야 하는 경우에는'사용자 권한별 네트워크 접근통제'기능을 활용해 단계적으로 네트워크 접근 권한을 부여할 수 있다. 만약 망혼용이 발생하면'스마트NAC'은'우회경로 차단 정책','비인가 무선 AP연결 차단정책'에 따라 강제로 인터페이스를 제거한 후, 관리자 알람을 통해 신속한 조치를 지원한다. 아울러 지속적인 모니터링을 통해 테더링과 같은 불법 우회경로를 차단하고 내부 중요 정보에 대한 비인가 반출을 통제한다. 이외에도 사용자 인증, 단말 무결성 정책, 어드밴스 DHCP 서비스 기능 등을 활용해 네트워크의 안정적인 관리를 지원한다.

방산기업은 클라우드 시스템을 지속 지속적으로 도입해 운용할 계획이며, IOT, 빅데이터, 인공지능과 연계한 4차 산업혁명 시대에 클라우드 컴퓨팅은 점차적으로 그

운용범위가 확대될 것으로 전망된다. 이에 클라우드 컴퓨팅 발전추세에 맞물려 증가하는 보안위협에 따라 방산기업도 보안을 강화해야 했지만 지금까지는 미흡하였던 것이 현실이다. 이에 본 연구에서는 세가지 측면에서 보안 발전방안을 제안하였다. 향후 보안이 향상된 클라우드 컴퓨팅 시스템이 방산기업에 도입되기를 바란다.

References

[1] J.S.Lee, H.S.Kim (2010), "A Study on the Status and Activation of Smart Work", *Journal of Korea Regional Information Society*, 13(4), pp.75-96

[2] J.H.Cheon, D.W.Park (2019), "Cyber Attack and Cyber Security Design for Smart Work System", *Journal of Korea Information and Communications Society*, 23(2), pp. 207-214
DOI: https://doi.org/10.6109/JKIICE.2019.23.2.207

[3] J.S.Kim, D.S.Kim, H.W.Kim (2017) "Vulnerability Response for Information Protection in Smart Work Services," S*ervice Research. Service Science Society*, 7(4), pp. 69-81

[4] Ministry of the Interior and Safety, Korea Internet & Security Agency, "Software for Electronic Government SW Developer and Operator", 2019

[5] J.S.Ahn, J.H.Bang, E.Y.Lee (2012), "Study on the Quantitative Evaluation Criteria of the Importance of Software Security Weakness", *Journal of Information Security*, 22(6), pp 1410-1417
DOI: https://doi.org/10.13089/JKIISC.2012.22.6.1407

[6] S.J.Jung, Y.M.Bae, "Analysis of Cloud Security Threats and Technical Trends", *Security Engineering Research Paper,* Volume 10, Number 2, 2013

[7] S.C.Kim (2013), A Study on Policy Improvement for Activation of Clouding Computing, *Korea Management Science Society Conference Proceedings*, pp 451-457

[8] Software Policy Research Institute, "Remote Work Solution Technology and Market Trends and Implications", 2020

[9] Korea Internet & Security Agency, "Guide for Cloud Service Information Protection", 2017

[10] Software Policy Research Institute, "Key Issues and Countermeasures of Cloud Security", 2017

[11] IDG Korea, "What Makes Hesitant to Adopt Cloud", 2015

[12] Korea Intelligent Information Society Development Institute, "2020 Smart Work Survey Results Report", 2020

[13] Korea Internet & Security Agency, "Internet & Security Issues", 2012

[14] Korea Communications Commission, Korea Agency for Digital Opportunity and Promotion, "Smart Work Introduction and Operation Guidebook for Enterprises", 2011

[15] *S*eoul Digital Foundation, "Smart Work Policy Trends: Case of Seoul Digital Foundation's Work from Home", 2020

이 경 민(Kyung-Min Lee) [정회원]

- 2003년 2월 : 육군3사관학교 (이학사)
- 2016년 11월 ~ 2017년 11월 : 국방보안연구소 기획행정실장
- 2019년 8월 : 국민대학교 법무대학원 보안법무학과 (법학석사)
- 2022년 3월 ~ 현재 : 극동대학교 인공지능보안학과 박사과정

〈관심분야〉
방산보안, 국방보안, 인공지능보안

이 용 준(Yong-Joon Lee) [종신회원]

- 2005년 2월 : 숭실대학교 컴퓨터학과 박사
- 2010년 2월 ~ 2016년 3월 : 한국인터넷진흥원 수석연구위원
- 2016년 4월 ~ 2020년 3월 : 국방보안연구소 연구관
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
해킹보안, 국방보안, 인공지능보안