Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.6, Dec. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.6.1001

제로 트러스트 아키텍처 적용 방안에 대한 연구: 재택근무 시스템 구성을 중심으로*

도 재 우,[1†] 강 금 석[2‡]
[1]한국항공우주연구원 (선임기술원), [2]한국과학기술원 경영대학 (교수)

A Study on Applying Zero Trust Architecture: Focusing on Implementing Remote Work System*

Jaewoo Do,[1†] Keumseok Kang[2‡]
[1]Korea Aerospace Research Institute (Senior Engineer),
[2]KAIST College of Business (Professor)

요 약

코로나19 이후로 재택근무의 대폭 활성화로 기업 네트워크의 내부와 외부의 경계가 모호해졌다. 이로 인해 전통적인 경계형 보안으로는 기업의 업무 생산성이 정체되고 정보 유출 등의 위험 관리가 어려워졌다. 제로 트러스트 아키텍처 모델이 등장하였으나 기업별로 다양하게 구성된 IT 환경에 적용하기에는 어려움이 있다. 이에 재택근무 시스템 구성을 예시로 온-프레미스, 클라우드 및 망 분리 등의 네트워크 환경에서도 제로 트러스트 모델을 적용할 수 있는 구성과 방법론을 제시하였다. 이를 통해 사이버 위협에 능동적으로 대응하는 지능형 체계인 제로 트러스트 아키텍처를 적용하려는 기업에 가이드를 제공하여 안전하면서도 편리한 사이버 환경 조성에 기여 하고자 한다.

ABSTRACT

As massive increase in remote work since COVID-19, the boundaries between the inside and outside of corporate networks have become blurred. As a result, traditional perimeter security has stagnated business productivity and made it difficult to manage risks such as information leakage. The zero trust architecture model has emerged, but it is difficult to apply to IT environments composed of various companies. Therefore, using the remote work system configuration as an example, we presented a configuration and methodology that can apply zero trust models even in various network environments such as on-premise, cloud, and network separation. Through this, we aim to contribute to the creation of a safe and convenient cyber environment by providing guidance to companies that want to apply zero trust architecture, an intelligent system that actively responds to cyber threats.

Keywords: Zero Trust, Remote work, Device Agent, Resource Portal, Methodology

I. 서 론

디지털 전환과 클라우드의 활성화로 기업의 내부 업무 환경에도 많은 변화가 일어나고 있다. 글로벌화로 타 국가에서 수행하는 업무가 확대되고 코로나19 이후 재택근무를 활용하는 기업이 증가하면서 기업

Received(10. 11. 2023), Accepted(11. 21. 2023)
* 본 연구는 한국과학기술원 경영대학 석사학위논문(2023) "제로 트러스트 아키텍처 적용 방안에 대한 연구: 재택근무 시스템 구성을 중심으로"을 수정·보완한 것입니다.
* 본 연구의 저자 강금석은 정보통신기획평가원의 대학ICT연구센터육성지원사업((IITP-2023-2021-0-01816))의 지원을 받았습니다.
† 주저자, itpe.jwdo@gmail.com
‡ 교신저자, keumkang@kaist.ac.kr(Corresponding author)

업무 환경에서 내부와 외부의 경계가 모호해졌다.

하지만 이러한 IT 환경의 변화는 반드시 호재로만 작용하지 않는다. 사이버 공격은 점점 지능적으로 발전하고 있고, IT시스템의 증가는 공격 대상의 증가로 이어져 정보 유출 사고 발생의 경로가 되고 시스템이 빠르게 증가하면서 내/외부로부터 안전하게 보호할 능력을 확보하지 못해 보안 사고가 발생하기도 한다.

그렇다면 기업에서 안전한 업무 환경을 구성하는 방법을 모색하지 않을 수 없다. 언제라도 쉽게 유출될 수 있는 상황이라면 아무리 좋은 IT시스템이라도 활용하지 못하는 상황이 생길 수 있기에 생산성을 향상하면서 사이버 공격에 대응할 수 있는 IT 인프라가 필요하다.

이러한 변화로 네트워크 분리로 안전한 구역을 정해 보호하는 경계형 보안 대신 제로 트러스트 아키텍처 모델로 보안 환경이 전환되고 있다. '21년 5월 바이든 미 대통령이 서명한 행정 명령 내용 중에 연방정부에 제로 트러스트 보안 정책을 채택하도록 하였다[1]. 그만큼 제로 트러스트 모델이 중요하게 부상하고 있기에 앞으로 제로 트러스트 모델을 활용하려는 시도는 점점 늘어날 것으로 보인다.

하지만 국내 환경에서 제로 트러스트 아키텍처를 바로 적용하기에는 무리가 있다. 대부분의 국내 기업들은 On-Premise 환경으로 운영하고 있어 클라우드 시스템에 상대적으로 적합한 제로 트러스트 모델을 참고할 만한 자료 찾기도 어렵다. 이에 재택근무 시스템을 구성하는 방법을 통해 기업이 변화하는 사이버 위협에 능동적으로 대응하여 지능적으로 사이버 위협 예방과 사용성을 확보할 수 있는 제로 트러스트 아키텍처를 적용할 수 있는 방안을 제시하고자 한다.

II. 선행 연구 조사

업무 형태가 스마트 워크로 변화되고, 코로나19로 인한 재택근무로의 전환이 늘어나면서 재택근무 환경에 대한 보안 위협에 관한 연구가 활발히 진행되었다. 이경복 등은 스마트 워크 환경에서는 서비스 제공자 측면(인프라, 공용 컴퓨터 보안), 관리자(단말기/서비스/콘텐츠 보안, 인적 자산 관리, 침해 사고 대응 절차), 이용자 측면(정보자산 취급/관리, 인식 제고, 침해 사고 대응)의 고려가 필요하며 해결방안으로는 재택 환경에서는 생체인증, VPN 사용, 물리적 설치 공간 통제가 필요하고, 모바일 오피스 환경에서는 플랫폼, 애플리케이션, 네트워크 공격과 정보 유출, 오작동, 과금 회피에 대한 대응이 필요하며 스마트워크센터는 물리적 보안 통제, 정보자산 보안대책, DRM 적용 등이 필요함을 연구하였다[2]. 김소연 등은 원격근무에 대한 위협으로 시스템/OS, 네트워크, 애플리케이션, 정보보호 일반적 위협 등이 있으며, 취약한 단말 시스템, 접근제어 취약점, 네트워크 취약, 다수의 원격접속, 취약한 App, 웹캠 해킹, 취약한 로그, 중요 데이터 유출 등이 있음을 연구하였다[3]. Nurse 등은 재택근무 위험 요소에는 사이버 공격 피해자가 될 위험, 재택근무 보안 훈련 부족, 보안 고려의 우선순위 감소 등의 직원 관계된 보안 위험과 신뢰할 수 없거나 테스트 되지 않은 기술의 적용, 기술 이해 부족으로 인한 보안 요소 적용 실수, 원격 업무/소통기술 보안 문제 등의 기술적 위험과 사생활 침해의 위험이 있음을 연구하였다[4]. Malecki는 코로나19 이후 사이버 공격이 폭증하였고, 이에 대응하기 위해서는 비즈니스 데이터 보호(이미지 백업, 원격 네트워크 보안(단말 보안, VPN, 바이러스 검사, 의심스러운 연결 검사, IT 지원팀에의 오류 해결, 보안 표준 준수한 소통 도구 사용), 직원 의식 제고, 공격에 당하더라도 침착한 대응이 필요함을 제시하였다[5].

제로 트러스트 아키텍처를 구현하는 방안에 관한 연구도 진행되었다. Tao Chuan 등은 제로 트러스트 아키텍처의 구현 전략에 대해 구조와 평가로 나눴다. App 서버가 제로 트러스트 검증을 거치면 토큰 생성 서버로부터 토큰을 발급받아 해당 토큰을 가지고 게이트웨이를 거쳐 내부 접속을 하는 구조를 제시하였고, 필수 프로그램 설치, 비인가 서비스/프로그램 기동, 비인가 계정 활성화, 고위험 포트 개방, 취약 비밀번호, 취약점, 민감정보 보호, 웹사이트 공격 탐지, 보안 구성을 포함하여 계산하는 평가를 제시하였다[6]. 고민혁 등은 제로 트러스트 기반 보안체계 구축 프로세스는 주체의 식별, 자산 식별, 핵심 프로세스 식별 및 위험 평가, 제로 트러스트 아키텍처 후보에 대한 정책 수립, 솔루션 후보 식별, 초기 시행 및 모니터링, 제로 트러스트 아키텍처 확대 순서로 이뤄짐을 연구하였다[7]. Songpon Teerakanok 등은 제로 트러스트 아키텍처로 통합할 때의 프로세스와 도전과제, 구현 방법에 관해 연구하였다. 프로세스로

는 평가, 위험 평가 및 우선 순위화, 구현과 검증 단계를 지속적 순환으로 수행하여야 하고, 이 과정에서 절차의 변경, 위험 관리, 접속 주체 관리, 법과 제도의 고려가 필요하다고 하였다. 도전과제로는 벤더 Lock-in과 내부 운영성, 데이터 포맷 적정성과 표준화 필요성, 사용자 혼선 방지, 신뢰성 수준과 자원 분류, 관리되지 않은 디바이스 처리, 신뢰 알고리즘(Trust Algorithm, TA) 향상을 제시하였다. 구현 절차로는 사용자와 장치 식별, 암묵적인 신뢰 제거, 업무 흐름 외부화를 제시하였다[8]. 한성화 등은 제로 트러스트 모델을 적용 시 보안체계 구축 비용의 증가, Security Process Integration과 운영 비용 증가를 고려하여 설계하여야 함을 연구하였다[9].

구글은 BeyondCorp라는 제로 트러스트 시스템을 구축하는 방안을 제시하였고, 실제로 구축한 내용을 논문으로 발표하였다. 구글은 네트워크로 분리하여 안전한 영역을 구분하는 보안 구조인 경계형 보안은 안전성을 보장하지 못하기 때문에 제로 트러스트 아키텍처를 제시하였다. 구글도 이전에는 VPN을 통해 접속하여 내부 자원을 활용하는 방식을 구현하였으나 해외에서도 접속하여 사용하기 때문에 내부 시스템이 더는 안전할 수 없다고 보았다. 이러한 관점으로 내부 시스템도 인터넷 클라우드의 서비스 형태로 구축하고, 회사 내 등록된 장치에 대해서만 접속할 수 있도록 하였으며, 내/외부 장치 인증과 추적관리 등을 적용하였다. 대신 사용자 경험을 반영하여 VPN 사용 대신 HTTPS 프락시를 활용하여 접근성을 향상하였고, 내부 사용자는 802.1x 인증, 외부 사용자는 Captive Portal을 활용한 인증으로 내/외부 사용자의 보안 수준을 유지하면서 사용자들의 사용성도 향상하는 방법을 구현하였다[10-15].

위와 같이 제로 트러스트 아키텍처와 관련된 위협과 구축방안 등에 관해 연구가 활발히 되었지만, On-Premise와 클라우드 환경에서의 구성 방안에 관한 연구는 확인하기 어려웠다. 국내의 경우 망 분리 환경과 On-Premise 시스템 위주의 IT 인프라 구성으로 제로 트러스트 아키텍처를 바로 적용하기에 무리가 있다. 장기적으로는 클라우드 환경으로의 전환이 이뤄질 수 있으나 현재의 인프라에서도 적용이 가능한 방안을 모색할 필요가 있다. 이에 본 논문에서는 다양한 IT 환경에서 제로 트러스트 아키텍처를 적용할 방안을 제시하여 글로벌 사이버 보안 환경의 변화에 대응하고자 한다.

III. 보안 위협 대응을 위한 제로 트러스트 아키텍처

3.1 제로 트러스트 아키텍처란

미국 국립표준기술연구소(National Institute of Standards and Technology, 이하 NIST)에서는 제로 트러스트 아키텍처에 대한 표준을 수립하였다[16]. 제로 트러스트 아키텍처란 제로 트러스트(Zero Trust) 원리를 기반으로 데이터 유출을 방지하고 내부 이동을 제한하도록 설계된 통합적 사이버 보안 아키텍처다. 여기서 제로 트러스트 원리는 신뢰가 없다 (No Trust). 즉, '아무도 믿지 마'라는 개념으로, 제로 트러스트 아키텍처는 네트워크를 불완전한 상태로 간주하여 정보시스템 및 서비스에 요청당 최소 권한에 정확한 접근 결정을 시행할 때 불확실성을 최소화하는 원리이다.

기존의 경계형 보안에서는 정보시스템 및 서비스를 안전한 영역에 배치하고 접속 주체가 안전한 영역에 접근해도 되는지 확인하는 절차적 사이버 보안 아키텍처이다. 반면에 제로 트러스트 아키텍처에서는 정보시스템 및 서비스에 접근할 때 정책 엔진(Policy Engine)과 정책 관리자(Policy Administrator)를 통해 접속 주체에 대한 위험성을 지속적으로 검증하고 위협이라 판단되면 능동적 대응을 통해 예방하는 지능형 사이버 보안 아키텍처이다.

NIST에서 제시한 제로 트러스트 아키텍처의 논리적 핵심 구성 요소는 Fig. 1. 과 같다[16].

- 정책 엔진(Policy Engine, 이하 PE): 요청 주체에 대해 자원접근을 허용할지에 대해 신뢰 알고리

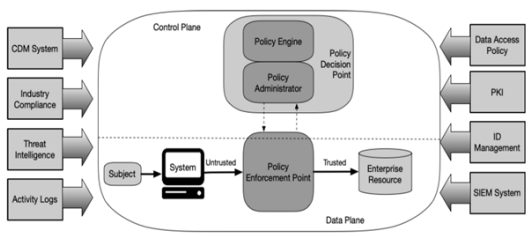


Fig. 1. Core Zero Trust Logical Components (Source : NIST[16])

즘을 통해 권한 부여, 거부, 취소를 결정한다.
- 정책 관리자(Policy Administrator, 이하 PA): 주체와 자원 간의 교류 경로를 수립하거나 차단하는 역할을 한다.
- 정책 강화 지점(Policy Enforcement Point, 이하 PEP): 주체와 회사 자원 간 연결 허용, 모니터링, 종료를 수행한다.
- 데이터 소스: PE가 접근 결정을 하기 위해 활용되는 CDM 시스템, 산업 준법 시스템, 위협 인텔리전스, 네트워크 및 시스템 활동 로그 등의 정보 원천 데이터

또한 사이버 보안 및 인프라 보안국(Cyber-security and Infrastructure Security Agency, 이하CISA)에서는 제로 트러스트 성숙도 모델을 발표하였는데 2023년 5월 기준 최신 보안 성숙도 모델은 Fig. 2. 와 같이 신원(Identity), 장치(Device), 네트워크(Network), 애플리케이션 및 작업량(Applications & Workloads), 데이터(Data) 등 5가지로 구분하여 제시하였다[17].

각 요소에 대해 전통적(Traditional), 초기(Initial), 고급(Advanced), 최적(Optimal) 수준으로 분류하였으며, 요소별로 갖춰야 할 내용에 대해 명시하였다.

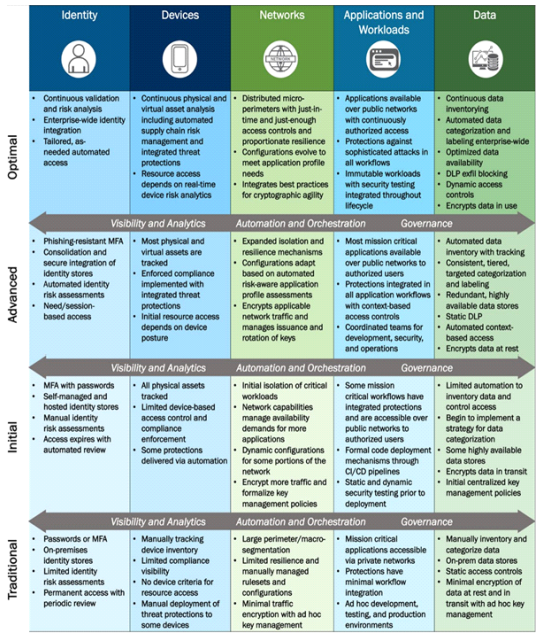


Fig. 2. High-Level Zero Trust Maturity Model Overview (Source : CISA[17])

NIST에서 제안한 제로 트러스트 아키텍처 모델은 총 4가지로 그 내용은 다음과 같다.

3.1.1 Device-Agent/Gateway-based Deployment

이 모델은 Fig. 3. 과 같이 기업용 자산(노트북 등)이 연결 중계를 수행하는 에이전트를 설치하고, 각 자원은 게이트웨이에만 통신하기 위한 컴포넌트가 있어 게이트웨이의 역할을 하는 구현 방법이다. 에이전트는 자원접근 요청들이 검토되도록 트래픽을 적절한 PEP에 할당되도록 한다. 게이트웨이는 PA에 의해 인가된 통신만 수행할 수 있도록 한다.

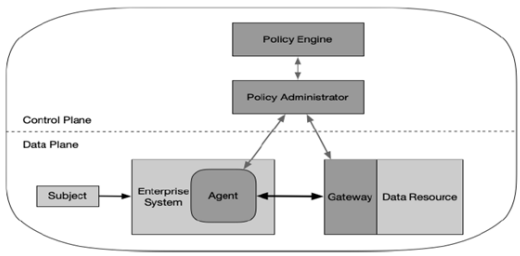


Fig. 3. Device-Agent/Gateway-based Model (Source : NIST[16])

3.1.2 Enclaved-based Deployment

이 모델은 위의 Device Agent/Gateway 모델과 유사하지만, 게이트웨이가 자원 영역에 있는 모델이다. 또한 각 비즈니스 프로세스가 클라우드 기반의 마이크로 서비스로 사용하거나 On-Premise 데이터 센터 또는 레거시 애플리케이션을 가지는 기업에 유용하다. 기업은 device agent를 설치 및 설정하기 위한 강력한 자산 및 설정 관리 프로그램이 필요하

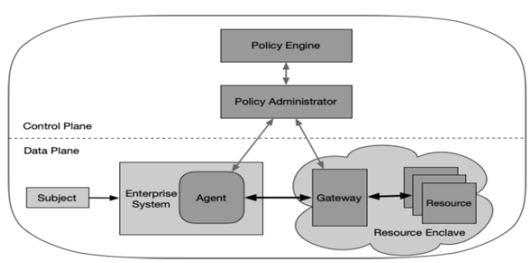


Fig. 4. Enclaved-based Model (Source : NIST[16])

다. 게이트웨이가 각 자원을 개별 관리가 아닌 집합으로 관리하기 때문에 접속 주체가 접근권한이 없는 자원에 대해 열람할 가능성이 있다. 이 모델의 구성은 Fig. 4. 와 같다.

3.1.3 Resource Portal-based Deployment

이 모델에서 PEP는 접속 주체의 요청을 위한 게이트웨이 역할을 하는 단일 컴포넌트이다. 게이트웨이 포털은 개별 자원용이거나 단일 비즈니스 기능에 사용되는 자원 집합에 대한 보호구역이 될 수 있다. 이 모델의 구성은 Fig. 5. 와 같다.

이 모델은 모든 클라이언트 장치에 소프트웨어 컴포넌트를 설치할 필요가 없는 장점이 있다. 또한 BYOD정책과 내부 조직 융합 프로젝트에 더 유연성을 가진다. 하지만 이 모델은 PEP 포털에 연결할 때만 자산과 연결장치를 스캔 및 분석하기 때문에 멀웨어, 취약점 등에 대해 지속적인 모니터가 안 될 수 있다. 이 모델은 또한 공격자들이 포털을 찾고 접속 시도하거나 포털에 서비스 거부 공격을 하는 것을 허용하기 때문에 포털 시스템은 가용성 확보가 요구된다.

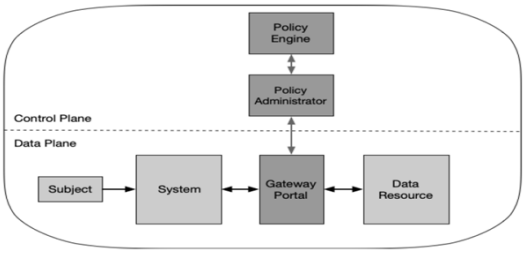


Fig. 5. Resource Portal-based Model (Source : NIST[16])

3.1.4 Device Application Sandboxing

이 모델은 Fig. 6. 과 같이 검증된 애플리케이션 또는 프로세스가 자산 내 구역화되어 실행된다. 구역은 가상머신, 컨테이너, 또는 다른 방식의 구현일 수 있으나 목표는 자산 내에서 실행되고 있는 손상 가능성이 있는 호스트 또는 애플리케이션으로부터 보호하는 것이다.

접속 장치는 샌드박스 내에 승인되고, 검증된 애플리케이션을 실행한다. 애플리케이션은 자원접근 요청을 위해 PEP와 통신하지만, PEP가 자산 내 다른 애플리케이션 접근을 거부한다.

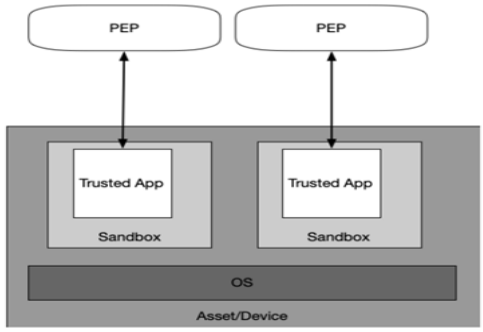


Fig. 6. Device Application Sandboxing Model (Source : NIST[16])

IV. 제로 트러스트 아키텍처를 적용한 재택근무 시스템 구성

4.1 재택근무 시스템에 제로 트러스트 아키텍처 적용 개요

4.1.1 재택근무 시스템에서 제로 트러스트 아키텍처 적용 필요성

재택근무 환경에서는 일반 업무 환경과는 다르게 상시로 기업 외부에서 접속하여 업무가 진행된다. 네트워크 분리를 통한 경계형 보안을 적용한 기업 내에서 업무를 수행하는 경우 신원이 확인된 인원이 기업에서 제공하는 단말기를 내부 네트워크에 연결하여 승인된 애플리케이션으로 업무를 수행하므로 정보 교류가 사내망에서 주로 이뤄지는 데 반해 재택근무는 개인 또는 기업의 단말기를 집에서 인터넷을 통해 내부 시스템을 접속하여야 하기에 단말기에 대한 보안 관리의 어려움과 사용자의 신원 확인 문제, 내부의 중요 데이터를 외부로 유출하는 등의 비정상 행위 탐지 문제 등이 발생할 수 있다. 따라서 재택근무 시스템을 구성할 때 단말기 안전성 검증과 사용자 인증, 네트워크 구간 암호화와 정보 유출 모니터링을 중점적으로 확인하여야 한다.

대부분의 재택근무 시스템에서 적용된 보안 기술은 ID/PW에 OTP, 생체인증 등을 같이 적용하는 다중 인증과 SSL VPN으로 통신 구간 암호화, VDI 기반 가상 PC로 이뤄진다. 여기에 기업망에서 운영하는 정보보호 시스템을 연계하여 구성하는데 DDoS 보호장비, IPS, 방화벽, 웹 방화벽 등이 주로

활용된다. 하지만 기존의 경계형 보안으로 시스템을 구성하면 인증 절차가 일회성으로 이뤄지고 안전한 영역으로 들어오면 시스템에 대한 접속이 무방비 상태가 된다. 이로 인해 해커가 신원을 탈취 또는 시스템 자체의 취약점 등을 이용하여 사용자 인증을 우회하거나 통과하면 사이버 위협에 무방비 상태가 될 수 있다. 또한 사이버 공격 시도를 탐지하고 대응하려면 관제 시스템, 대응 인력 등 비용 소모가 많다.

이와 같은 문제는 제로 트러스트 아키텍처와 접목으로 지속적인 위협 모니터링과 지능화된 대응을 할 수 있다. 매 트래픽 마다 정책 관리자(PA)와 정책 엔진(PE)에서 보안 사항 준수 여부를 확인하고 이상 행위가 있으면 능동적인 세션 차단으로 예방과 피해 확산 방지가 가능하다. 또한 정보시스템의 정책 엔진 연동으로 중요 정보 유출 위험을 감소시킬 수 있다. 이를 통해 실시간 대응 능력을 확보할 수 있고 기업에서 상대적으로 적은 비용으로 정보 유출 대응 능력을 확보할 수 있다. Fig. 7. 은 제로 트러스트 아키텍처를 적용 시 얻을 수 있는 효과를 보여준다.

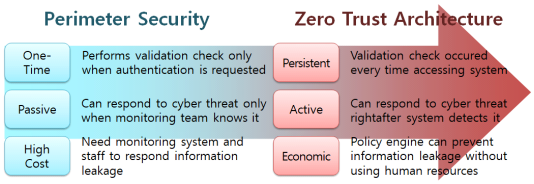


Fig. 7. Effects of applying Zero Trust Architecture

4.1.2 재택근무 시스템에서 제로 트러스트 아키텍처 적용 시 고려사항

재택근무 시스템에서 고려하여야 할 요소는 앞서 기술한 단말기 안전성 검증과 사용자 인증, 네트워크 구간 암호화와 정보 유출 모니터링에 더해 망 분리, 3-Tier 구조, 이중화 등의 시스템 운영 사항도 같이 고려해야 한다. 망 분리는 국내의 경우 2006년부터 추진하기 시작하여 주요 정부 기관으로 확대되었고 2013년 이후 금융기관에 망 분리가 의무화되었으며 개인정보 보호법에 따라 정보통신서비스 제공자 등은 개인정보처리시스템에 접속하는 개인정보 취급자의 컴퓨터에 대해 외부 인터넷망을 차단하도록 제도적으로 수행하고 있다[18]. 여기에 중요한 시스템을 별도로 관리하기 위해 구간 분리가 필요한데 국내 공공기관의 경우 정보공개법에 따른 비공개 대상 정보를 활용하기도 하고, 기업에서는 내부적으로 중요도에 따라 구분하여 분리 운영하기도 한다[19].

본 논문에서 고려한 사항으로는 크게 제로 트러스트 아키텍처 구성, 시스템 설계 요구사항, 재택근무 시스템 보안 요소가 있다. 제로 트러스트 아키텍처 구성으로는 제로 트러스트 아키텍처에서 제시하는 관리 영역(Control Plane)과 데이터 영역(Data Plane)의 분리와 On-Premise 환경과 클라우드 환경에서 정책 엔진(PE)을 연동하는 방안과 회사 업무에 개인 단말기를 사용하는 BYOD(Bring Your Own Device) 활용 여부에 따른 제로 트러스트 아키텍처 모델 선정을 고려하였다. 시스템 설계 요구사항으로는 개인정보 등이 포함된 인증 시스템 분리, 서비스 영역과 데이터 영역을 분리하는 3-Tier 구조와 국내법/제도 및 업무 구간 별도화를 위해 내부망과 외부망을 구분하는 망 분리 수행 여부, 가상 데스크톱을 이용하여 업무 하는 VDI 시스템 운영을 반영하였다. 재택근무 시스템 보안 요소로는 중요도가 높아 기업에서 재택근무로 수행이 불가한 시스템 운영 환경과 홈 네트워크에서 기업 네트워크까지 기밀성을 유지하기 위해 SSL VPN 또는 HTTPS를 활용한 통신 구간 암호화, 재택근무에서 활용하는 단말기의 안전성 여부를 확인하는 단말기 보안과 접속하는 사용자가 내부 직원 등 확인을 위한 다중 인증을 고려하였다. Table 1. 는 각 고려사항 별 반영하여야 할 요소를 보여준다.

Table 1. Considerations of Implementing Zero Trust-Enabled Remote Work System

Category	Considerations	Reflections
Zero Trust Architecture Configuration	Divide Control Plane and Data Plane	Separate policy system segments that include Policy Administrator (PA) and Policy Engine (PE)
	Policy Engine (PE) Integrations	On-Premise: Operations Integration with individual information systems Cloud environment: CNAPP (Cloud Native Application Protection Platform) integration

Category	Considerations	Reflections
	BYOD Utilization	With BYOD (Resource Portal-based) and without BYOD (Device Agent/Gateway-based) Present system configuration
System Design Requirements	Authentication System Separation	Separate Authentication System zones, separate Gateway Portal bands
	3-Tier Architecture	Separate the DMZ zone from the data zone
	Applying Network Segregation	Separate system configurations for network segregated environments
	Operating VDI System	Present system configuration and workflow when utilizing a VDI system
Elements of Remote Work System	Possible to Access from Remote	Distinguish between jobs that can be done online and jobs that are done onsite
	Device Security	Device Agent/Gateway-based : Check the device agent Resource Portal-based : Terminal using SSLVPN Security check
	Multi Authentication	Device Agent/Gateway-based : Device auth, secondary auth Resource Portal-based : Primary and secondary auth on Gateway Portal Network separation environment : Internal network authentication on VDI after external network authentication Cloud environment: Utilize CASB (Cloud Access Security Broker)
	Network Encryption	On-Premise : Configure an HTTPS Reverse Proxy or Utilize SSLVPN Cloud environment : HTTPS communication

4.2 On-Premise 환경에서의 시스템 구성

클라우드가 활성화되기 전에 디지털 인프라를 구축한 기업들은 클라우드로 전환하기에는 기존 인프라에 대한 전환비용이 상당하여 On-Premise 환경에서 확장하는 형태로 구현하기도 한다. 그러다 보니 클라우드에서 제공하는 보안 서비스 대신 별도의 하드웨어 또는 소프트웨어 솔루션을 활용하는 경우가 있다. 기업에서 재택근무와 관련하여 운영할 수 있는 주요 보안솔루션은 아래와 같다.

1. SSL VPN : 전송구간 암호화와 사용자 인증을 위해 SSL 암호화 기술을 활용하여 외부 단말기와 기업망 간의 가상 암호화 통신망을 구현하는 솔루션
2. 방화벽 : 내/외부에서 네트워크 구간에 대한 비인가된 접근(IP, Port 등)으로부터 보호하기 위해 네트워크 접근 제어하는 솔루션
3. IPS/IDS : OSI 7계층 전체에 대해 알려진 공격 패턴 등으로 침입 여부를 탐지(IDS), 차단(IPS)을 수행하는 솔루션
4. DDoS 보호장비 : 외부에서 대용량의 트래픽 전달 등으로 서비스 거부를 초래하는 DoS/DDoS 공격을 보호하기 위한 솔루션
5. 웹 방화벽 : 공격 시도가 자주 일어나는 웹 서비스 공격에 대응하기 위해 HTTP, HTTPS 프로토콜을 이용한 웹 공격패턴을 탐지하여 차단하는 솔루션
6. 엔드포인트 보안솔루션 : 단말기 상에서 발생하는 악성코드 감염, 정보 유출 등을 보호하기 위해 백신, 매체 제어, 문서 암호화, 인증 등의 기능을 수행하는 솔루션
7. 인증 시스템 : 시스템에 접속하는 사용자에 관한 확인을 위해 지식 기반(ID/PW 등), 소유기반(OTP, 스마트카드 등), 생체 기반(지문인식, 얼굴인식 등)으로 검증하는 시스템
8. 망 연계 시스템 : 기업에서 망 분리(내부 네트워크와 인터넷 네트워크를 분리)를 한 경우 업무용 네트워크와 인터넷 네트워크 간의 자료 이동, 통신 연계 등을 제공하는 솔루션

금융기관, 공공조직, 대기업 등은 이용자 보호와 법제도 준수 등으로 위의 솔루션을 구축하여 운영하나 중소기업, 소상공인, 스타트업 등은 위에 쓴 솔루션을 운영하기 어려운 경우가 많다. 그러다 보니 웹

서비스를 운영하려는 경우 웹 호스팅 업체를 통해 기초적인 보안 지원을 받았으나 클라우드가 확대되면서 클라우드 서비스를 구매할 때 포함하기도 한다. 제로 트러스트 환경에서는 VPN 운영 대신 HTTPS를 활용한 프락시 기술 적용을 고려하기도 하지만, On-Premise 환경에서 VPN을 대체할 시스템을 단기적으로 구성하기 어렵다. 제로 트러스트 아키텍처를 처음 구상한 회사는 구글, MS 등 클라우드 중심 기업이기에 클라우드 환경에서 구현이 쉽다. 따라서 제로 트러스트 환경을 성공적으로 구현하려면 장기적으로는 On-Premise 시스템 대신 클라우드 시스템으로의 전환을 고려할 필요가 있다.

On-Premise 환경에서 제로 트러스트 아키텍처를 적용한 재택근무 시스템을 구성할 때 Device Agent/Gateway-based 모델과 Resource Portal-based 모델 적용 여부, VDI 시스템 활용 여부, 망 분리 적용 여부로 구분할 수 있다.

Device-Agent/Gateway 모델을 적용하고 망 분리를 하지 않는 경우 네트워크 구성은 Fig. 8. 과 같다. 이 경우 Proxy 서버를 통해 HTTPS 리버스 프락시로 홈 네트워크와 기업 사내망과의 구간 암호화를 수행하고 PA 서버와 단말기 인증, 2차 인증 시스템과 연동하여 사용자 인증을 수행하며, PE 서버에 세션 검증을 하게 된다. 그 후 서비스 제공 서버가 Gateway 역할을 하여 단말기와 연결을 수립하게 된다. 기업에서 제공된 단말기에는 Agent가 설치/연결되어 인증을 수행하게 된다. VDI 시스템을 활용하면 Gateway가 VDI 시스템이 되어 연결 수립한다. VDI 내에서 서비스 제공 서버에 접속할 때 인증 시스템을 통해 PA, PE 과정을 거친 후 Gateway 연동을 수행하게 된다. VDI를 활용하지 않으면 접속 순서는 홈 N/W의 기업용 단말기가 인터넷을 통해 PA 서버에 도달하면 1차, 2차 인증으로 사용자 인증을 수행한다. 그 후 PE 서버로 전달하여 세션 접속 허용 여부를 결정한 후 인증 시 재택가능 서비스를 이용하게 된다. VDI를 활용하면 인증 시 VDI 시스템에 접속하게 되고 VDI 상에서 서비스 접속 시 재인증을 통해 내부 시스템을 이용할 수 있다.

Device-Agent/Gateway 모델을 적용하고 망 분리를 적용하면 네트워크는 Fig. 9. 과 같다. 이 경우 VDI 시스템을 활용하는 것을 권장하는데 그 이유는 VDI를 활용하지 않으면 하나의 단말기가 외부 서비스와 내부 서비스를 같이 이용하게 될 수 있어 혼용이 발생할 수 있기 때문이다. 따라서 재택근무 시 사용하는 단말기는 외부 인증 시스템에서 인증이 되면 외부 서비스를 이용할 수 있도록 하고, 내부 서비스를 이용하고자 한다면 VDI 시스템을 통해 VDI 상에서 내부 서비스를 이용할 수 있도록 하는 구성이 필요하다. 이 때문에 외부에서 접속 시 내부에 있는 VDI를 연계하려면 외부망 구간에 Broker 시스템을 통해 연계할 수 있도록 하여 VDI가 직접적으로 외부와 접점이 생기지 않도록 구성하여야 한다.

접속 순서는 홈 N/W의 기업용 단말기가 인터넷을 통해 Proxy 서버로 접속 후 기업 외부망 PE 서버에 도달하면 1차, 2차 인증을 거친 후 PE 서버에 세션 접속 허용 여부를 전달한다. 그 후 외부 시스템 개방하여 외부 서비스를 이용하고 Broker 서버를 통해 VDI 시스템에 접속하게 된다. 그 후 VDI를 통해 내부 시스템 접속하려면 내부의 PA, PE를 통해 인증

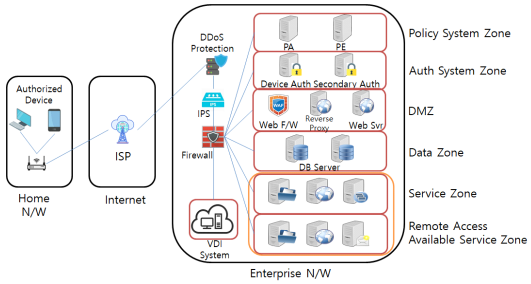


Fig. 8. Topology of Device Agent/Gateway-based Model(Network Segregation Not Applied)

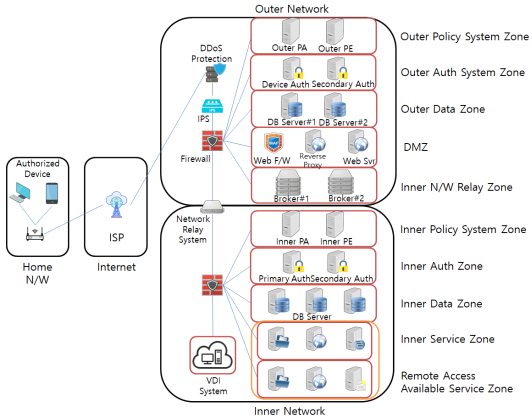


Fig. 9. Topology of Device Agent/Gateway-based Model(Network Segregation Applied)

및 세션 검증 후 재택 가능한 내부 서비스를 이용할 수 있다. VDI 시스템 내 VDI는 대체로 내부 인증 시스템과 연동하여 사용자 인증 기능이 적용되어 있으나 필요에 따라서 시스템 접속 시 2차 인증을 통해 보안성 강화를 수행할 수 있다.

Device Agent/Gateway 모델에서는 단말기에 설치된 Agent 프로그램을 통해 단말기 보안 수준을 검증하고, 기업에서 단말기 목록 관리를 수행하며 전송구간 암호화는 PE 서버에 HTTPS 프로토콜을 활용한 프락시 구성 등으로 통신 구간 암호화를 수행하기 때문에 SSL VPN에서 제공하는 단말기 보안 수준 검증과 통신 구간 암호화를 대체할 수 있다. 이는 Resource Portal 모델에서도 단말기 목록 관리를 제외하면 적용할 수 있지만, 국내에서 구축한 재택근무 시스템의 경우 SSL VPN을 활용하여 구성한 사례가 많아 Resource Portal-based 모델에서는 SSL VPN에서 제공하는 단말기 보안 수준 검증과 통신 구간 암호화를 활용하는 방안을 고려할 필요가 있다.

Resource Portal-based 모델을 적용하고 망 분리를 하지 않는 경우 구성은 Fig. 10. 과 같다. 이 경우 SSL VPN이 Gateway 역할을 하고 2차 인증 시스템, PA 서버와 연동하며 PE 서버에서 세션 검증을 하게 된다. 그 후 SSL VPN에서 서비스 제공 시스템에 연결을 수립하게 된다. SSL VPN 시스템에는 IP, MAC 주소 제한, 보안프로그램 실행 여부 확인 등의 기본적인 단말기 인증이 적용되어 BYOD(Bring Your Own Device, 이하 BYOD) 임에도 허용된 단말기만 접속할 수 있다.

접속 순서는 BYOD를 통해 기업의 SSL VPN 시스템에 접속하면 VPN 접속 및 2차 인증 수행을 완료 후 PA 서버에 세션을 전달한다. PA 서버는 PE 서버에 전달하여 검증한 후 SSL VPN 시스템이 내부 서비스에 연동하게 된다. VDI 시스템을 활용하면 VDI로 접속한 후 내부 시스템 접속 시 PA, PE 서버 검증 절차를 수행 후 이용하게 된다.

Resource Portal-based 모델을 적용하고 망 분리를 수행하면 Fig. 11. 과 같다. 이 경우에도 Device Agent/Gateway 모델을 적용할 때와 같은 이유로 VDI 시스템을 활용하는 것을 권장하고, 필요에 따라 내부망에서 2차 인증 적용을 통해 보안성 강화할 수 있다. SSL VPN이 외부 Gateway 역할을 하면서 유사한 절차로 Broker를 통해 VDI를 접속하면 내부의 PA, PE 서버와 연동하여 서비스를 이

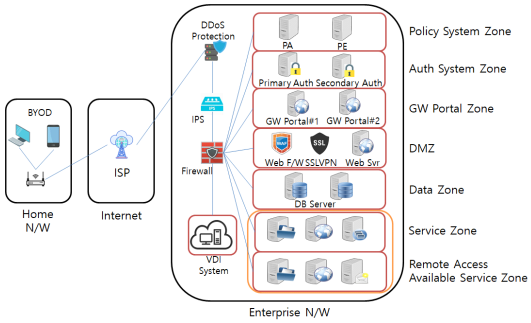


Fig. 10. Topology of Resource Portal-based Model(Network Segregation Not Applied)

용하게 된다.

망 분리 환경에서 Device Agent/Gateway 모델과 Resource Portal-based 모델을 적용할 때 PA, PE 서버를 분리하는 이유는 외부망에서는 단말기와 세션 검증 후 종료의 목적이고, 내부망에서는 VDI의 세션 검증의 목적이기 때문이다. 이 때문에 PA, PE 서버를 혼용하게 되면 해당 서버를 매개체로 내부 시스템을 공격하는 데 활용될 여지가 있으므로 망별로 분리하여 사용이 필요하다. 또한 Device Agent/Gateway 모델에서는 정책 서버 네트워크 구간과 인증 서버 네트워크 구간을 분리하는 것을 권장하는데, 그 이유는 Device Agent/Gateway 모델의 PE 서버는 외부에서 Agent를 통한 직접적인 연결이 수행되기 때문에 외부위협에 노출이 되어있다고 볼 수 있다. 따라서 피해가 발생하더라도 타 구간에 확산하지 않게 하려면 별도로 구성할 필요가 있다.

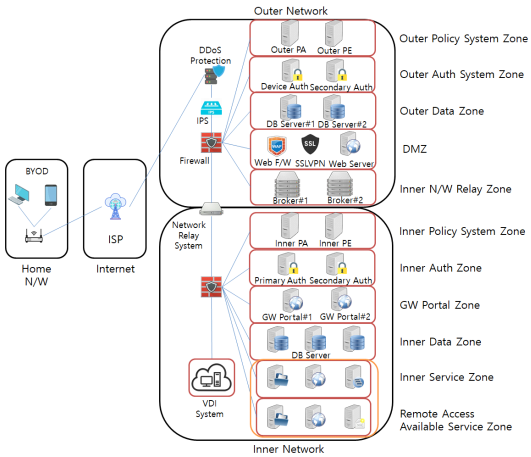


Fig. 11. Topology of Resource Portal-based Model(Network Segregation Applied)

4.3 클라우드 환경에서의 시스템 구성

클라우드의 확산으로 기업들이 별도의 보안솔루션 운영 대신 클라우드에서 제공하는 보안 서비스를 활용하여 보안체계를 구축하는 방안을 고려할 수 있다. 클라우드에서도 On-Premise와 같은 기능을 하는 보안솔루션을 클라우드 벤더에서 제공하기도 하고, 클라우드 환경에 초점을 맞춘 보안 서비스도 다양하게 개발되었다. 클라우드 환경에서 적용 가능한 보안 기능은 아래와 같다.

1. 클라우드 액세스 보안 브로커(Cloud Access Security Broker, CASB) : 클라우드 기반 자원에 접근할 때 클라우드 서비스 소비자와 공급자 사이에 배치되어 기업 보안 정책과 결합 및 개입하는 On-Premise 또는 클라우드 기반 보안 정책 적용 브로커
2. 클라우드 인프라 자격 관리(Cloud Intrastructure Entitlement Management, CIEM) : 클라우드 인프라에 대해 최소 권한의 액세스가 가능하도록 설계된 ID 및 거버넌스 기능 제공하는 기능
3. 클라우드 워크로드 보호 플랫폼(Cloud Workload Protection Platform, CWPP) : 복잡한 클라우드 환경을 보호할 수 있도록 클라우드 전반에 대해 워크로드를 관리 및 보호하는 플랫폼
4. 클라우드 보안 형상 관리(Cloud Security Posture Management, CSPM) : 클라우드 서비스 구성, 보안 설정, 규정 준수, 거버넌스 등 클라우드에서 발생 가능한 문제를 기록, 감지, 보고하는 기능
5. 클라우드 네이티브 애플리케이션 보호 플랫폼(Cloud Native Application Protection Platform, CNAPP) : 개발 및 프로덕션 전반에서 클라우드 네이티브 애플리케이션을 보호하도록 설계된 보안 기능 플랫폼으로 정적, 동적 애플리케이션 보안 테스팅, API 보안 테스팅, IaC(코드형 인프라) 스캐닝, 위협 모델링을 포함한다.

클라우드 환경에서는 On-Premise 에서보다 더 세분되고 통합적으로 관리할 수 있으며 별도의 솔루션을 사용하는 대신 클라우드에서 제공하는 기능으로 관리할 수 있는 장점이 있지만, 인프라가 벤더사에 종속되는 lock-in 현상이 생기며, 클라우드 내 일부 기능 오류가 발생 시 전체 서비스가 중단이 발생할 수 있는 위험성도 가지고 있다.

보안 서비스의 경우 클라우드 벤더 사에서 내장된 기능으로 하기도 하지만 보안 서비스 클라우드를 별도로 사용하면 서비스 활용을 다양화할 수 있고, 내부 클라우드 보안 기능을 활용할 때보다 보안 기능 변경에 따른 서비스의 영향도를 낮출 수 있는 이점이 있다. CASB와 CNAPP는 외부 서비스를 활용할 수도 있으나 사용자 계정과 서비스 영향과도 연관이 있어 내부 클라우드 서비스로의 활용에 대한 고려가 필요하다.

클라우드로 Device-Agent/Gateway 모델을 적용하면 네트워크 구성은 Fig. 12. 와 같다. 이 경우 보안 서비스용 클라우드를 외부로부터 활용할 수 있고, 기업용 클라우드에 포함하여 운영할 수 있다. 외부 클라우드를 활용하면 최신 사이버 위협에 대한 대응을 실시간으로 할 수 있어 위협 대응에 쉽지만, 기업 환경에 부합하는 설정을 적용하기에는 어려움이 있다. 반대로 기업용 클라우드에 보안 서비스를 탑재하면 기업 환경에 부합하는 보안체계를 구현하기 쉽지만, 보안 서비스를 기업용 클라우드 벤더사와 호환되는 플랫폼 여부를 고려하여야 한다.

CASB에서 기업용 단말기에 2단계 인증을 연계하여 인증 체계를 구현할 수 있고, CNAPP에서 Gateway 역할을 대신할 수 있으나 개별 자원의 중요도가 다를 수 있으므로 별도의 Gateway 모듈을 활용하는 방법을 고려할 필요가 있다. 또한 CNAPP를 활용하면 플랫폼에서 대체로 방화벽 기능을 포함하기 때문에 별도의 방화벽 설치가 불필요하며 각 자

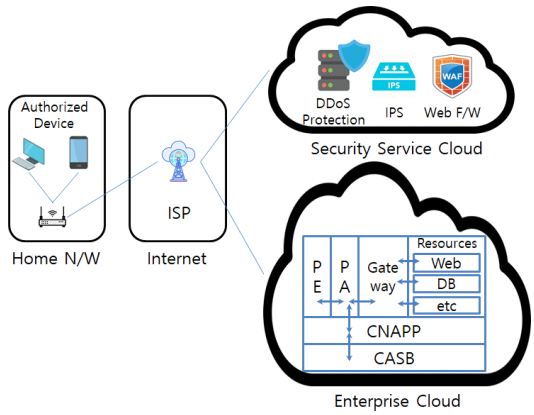


Fig. 12. Topology of Cloud-based Device Agent/Gateway-based Model

원별 관리가 쉽다.

접속 순서는 기업용 단말기에서 인터넷을 통해 보안 서비스 클라우드를 거치면 CASB로 인증을 수행한 후 PA에 전달되면 PE의 세션 검증을 통해 Gateway로 접속하여 이용하게 된다. PA는 PE와 Gateway와 CNAPP와의 연계를 수행하여 자원 접근관리를 수행하게 된다.

클라우드로 Resource Portal/Gateway 방식으로 재택근무 시스템에 적용할 경우의 구성은 Fig. 13. 과 같다.

위의 경우 BYOD 활용이 가능하고 사내 시스템에 유연한 적용이 가능한 장점이 있지만, 디바이스 단계에서의 취약 요소를 검증하기 어려우므로 단일 클라우드로 구축할 때 Device-Agent/Gateway 모델을 우선으로 고려해볼 필요가 있다. 하지만 기업에서 디바이스 관리가 어려우면 Resource Portal/Gateway 모델을 적용할 때 CASB 단계에서 인증 강화 요소를 고려하여 적용할 수 있다.

클라우드를 활용하면서 망 분리를 적용할 때 Device-Agent/Gateway 모델과 Resource Portal-based 모델을 적용하면 네트워크 구성은 Fig. 14. 와 같다.

이 경우 별도의 Broker 서버를 외부 클라우드와 연계하여 구현하는 방법과 외부망 내 클라우드에서 Broker 서버를 가상시스템으로 구현하여 연계하는 방안을 고려할 수 있다. 또한 외부망과 내부망의 클라우드 벤더를 별도로 구성하는 것도 고려해야 하는데 그 이유는 하나의 클라우드 시스템으로 모두 구현할 때 Lock-in 현상으로 인해 회사 시스템이 클라우드 벤더사에 종속적으로 운영될 수 있기 때문이다. 그렇게 되면 특정 벤더사에서 나타나는 취약점에 모든 회사 시스템이 노출될 수 있어 피해가 발생하게 되면 운영 연속성을 보장하기 어렵다. 또한 내부 시스템의 경우 Resource Portal Gateway 모델로 구현하면 내부 시스템과의 유연성을 극대화하면서 보안성도 충족시킬 수 있다. 이를 통해 VDI를 통해 접속하는 방식과 사내에서 시스템에 접근하는 요소를 모두 충족할 수 있어 내부 정책을 재택근무 환경에서도 적용하기 쉬운 측면이 있다.

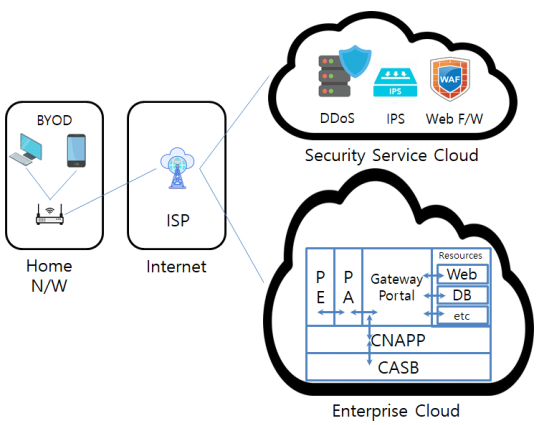


Fig. 13. Topology of Cloud-based Resource Portal-based Model

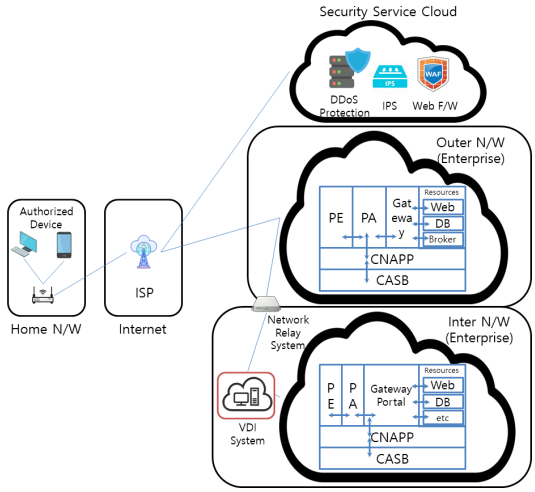


Fig. 14. Topology of Cloud-based Hybrid Model(Network Segregation Applied)

4.4 제로 트러스트를 적용한 재택근무 시스템 업무 흐름

본 논문에서는 Device Agent/Gateway 모델과 Resource-Portal based 모델로의 구축을 기준으로 서술하였다. Enclaved-based 모델은 Device-Agent 모델에서 Gateway와 내부 시스템을 클라우드로 구현한다는 차이만 있기에 Device-agent 모델을 참고하여 적용할 수 있다. Application Sandbox 모델의 경우 업무 시스템과 일체화된 단말기를 구성하여 PE, PA, Gateway 등을 통하지 않고 직접적으로 내부 시스템에 접속하는 방식이므로 별도의 시스템 구축과정을 명시하지 않았다.

Device Agent/Gateway 모델은 기업에서 재택근무를 위해 직원들에 별도의 단말기를 지급하거나 기업에 접속 가능한 단말기로 등록되었을 때 이점이

있고, Resource Portal-based 모델은 BYOD를 적용하거나 On-Premise 시스템이 주로 사용될 때 적용이 유용하다. 회사에서 재택근무를 수행할 때 VDI를 활용한 가상 PC 접속하여 수행하거나 직접 단말기를 내부 시스템에 접속하는 방법이 있을 수 있는데 VDI를 활용하는 경우 보안성이 더 높을 수 있으나 사용자별로 가상 PC를 제공해야 하기에 비용적 측면의 고려가 필요하고, 반대로 단말기를 직접 연결하면 비용 절감 효과가 있으나 단말기에서 발생하는 보안 위험을 기업에서 감수하여야 하는 문제가 있을 수 있다. 따라서 제로 트러스트를 적용한 재택근무 시스템 구성은 VDI 활용 여부도 고려되어야 한다.

Fig. 15. 와 Table 2. 은 Device Agent/Gateway 모델을 적용하고 VDI 시스템을 운영하지 않을 경우의 재택근무 시스템 업무 흐름을 보여준다.

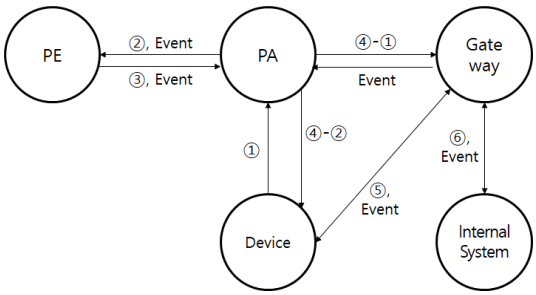


Fig. 15. Device Agent/Gateway-based Model Workflow (VDI Not Applied)

Table 2. Device Agent/Gateway-based Model Workflow (VDI Not Applied)

Seq.	Direction	Activity
1	Device → PA	Request PA to access internal systems
2	PA → PE	PA requests PE to judge session availability
3	PE → PA	PE notifies PA of access decision
4-1	PA → Gateway	Deliver session information to the gateway for permitted sessions.
4-2	PA → Device	Terminate unauthorized session
5	Device ↔ Gateway	Establish connection between gateway and device
6	Gateway ↔ Internal System	Access internal system through gateway

위의 과정 중 PE가 3의 과정에서 허용 결정을 내리면 4-1의 과정을 진행 후 5번의 과정을 진행하고, 거부 결정을 하면 4-2 과정으로 진행하여 세션 종료를 하게 된다. 이 경우 PE가 가부 결정을 할 때 오수락률(False Acceptance Rate), 오거부율(False Rejection Rate)이 높게 나타날 수 있다.

Device Agent/Gateway 모델을 적용하고 VDI 시스템을 운영할 경우의 재택근무 시스템 업무 흐름은 Fig. 16. 와 Table 3. 와 같다.

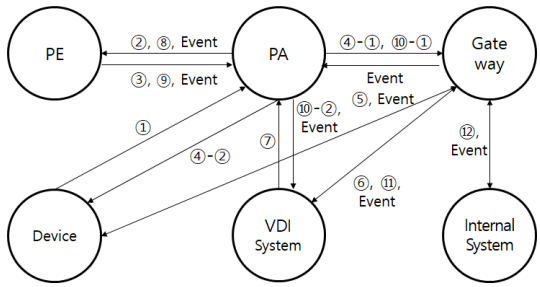


Fig. 16. Device Agent/Gateway-based Model Workflow (VDI Applied)

Table 3. Device Agent/Gateway-based Model Workflow (VDI Applied)

Seq.	Direction	Activity
1	Device → PA	Request permission to access VDI system from PA
2	PA → PE	PA requests PE to determine session access availability
3	PE → PA	PE notifies PA of access decision
4-1	PA → Gateway	PE notifies PA of access decision
4-2	PA → Device	Terminate unauthorized session
5	Device ↔ Gateway	Establish connection between gateway and device
6	Gateway ↔ VDI	Access VDI system through gateway
7	VDI → PA	VDI requests permission to access internal system from PA
8	PA → PE	PA requests PE to judge VDI session availability

Seq.	Direction	Activity
9	PE → PA	PE notifies PA of VDI access decision
10-1	PA → Gateway	Deliver session information to the gateway for permitted sessions.
10-2	PA → VDI	Terminate unauthorized session
11	VDI ↔ Gateway	Establishing a connection between VDI and Gateway
12	Gateway ↔ Internal System	Access internal system through gateway

위의 과정 중 PE가 3의 과정에서 허용 결정을 내리면 4-1의 과정을 진행 후 5번의 과정을 진행하고, 거부 결정을 하면 4-2 과정으로 진행하여 세션 종료를 하게 된다. 또한 PE가 9의 과정에서 허용 결정을 내리면 10-1의 과정을 진행 후 11번의 과정을 진행하고, 거부 결정을 내리면 10-2의 과정으로 내부 시스템으로의 접속을 차단하게 된다. VDI 접속한 때도 PA, PE의 과정이 필요한데 그 이유는 재택근무 환경에서 접속할 수 있는 시스템의 제한이 필요한 경우가 있을 수 있고, 실제 VDI 상에서의 활동 내용이 통상적인 직원이 수행하는 활동이 아닌 것으로 추정되는 경우 3번의 과정만으로는 재검증을 수행할 수 없기 때문이다. 또한 VDI 상에 자동화된 도구를 설치하면 사용자 세션 차단만으로 내부 시스템을 보호할 수 없기에 혹시 있을지 모를 악성 행위를 사전에 차단할 필요가 있다. 이를 통해 VDI 시스템 접속 시 세션 검증을 1차로 수행하여 인가된 사용자 접속을 가능하게 하고, VDI 상에서 내부 시스템 접속 시 2차 검증을 통해 내부 시스템 접속 권한 관리가 가능

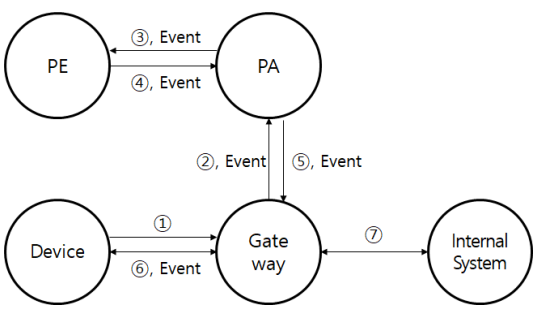


Fig. 17. Resource Portal-based Model Workflow (VDI Not Applied)

Table 4. Resource Portal-based Model Workflow (VDI Not Applied)

Seq.	Direction	Activity
1	Device → Gateway	Request permission to access internal system from Gateway
2	Gateway → PA	Gateway forwards session to PA
3	PA → PE	PA requests PE to determine session access availability
4	PE → PA	PE notifies PA of access decision
5	PA → Gateway	If PE decides to allow the access, the gateway is opened, if not, PE request the gateway to close the session.
6	Device ↔ Gateway	Establishes a connection between the gateway and device when allowed, terminate session to device when denied
7	Gateway ↔ Internal System	Access internal system through gateway

하다. 상시 활동에서는 Gateway가 단말기 및 VDI의 활동을 모니터링을 하여 지속해서 PA에 전달하고 PA는 해당 정보를 PE 전달을 통해 정상 판정 여부를 지속해서 판정하게 하여 이상 행위 시 세션 차단을 수행할 수 있도록 하여야 한다.

Resource Portal-based 모델을 적용하고 VDI 시스템을 활용하지 않으면 업무 흐름은 Fig. 17. 과 Table 4. 와 같다.

Resource-Portal based 모델을 적용하면 단말기에 별도의 Agent를 설치할 필요가 없어 BYOD 등 접속에 자유로움을 줄 수 있다. 그러나 단말기에 대한 위험 요소가 고려되지 않기 때문에 PE가 접속 허용/거부 결정을 할 때 실제 위험보다 낮은 상태로 평가를 수행할 수 있다. 따라서 이 경우는 오수락률(FAR, False Acceptance Rate)이 증가할 수 있다.

Resource-Portal based 모델을 적용하고 VDI 시스템을 활용하면 업무 흐름은 Fig. 18. 과 Table 5. 과 같다.

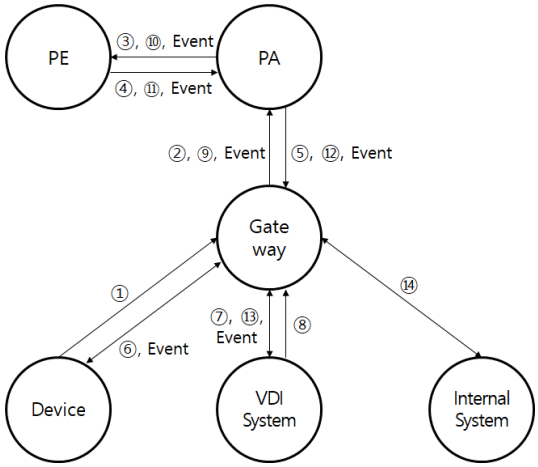


Fig. 18. Resource Portal-based Model Workflow (VDI Applied)

Table 5. Resource Portal-based Model Workflow (VDI Applied)

Seq.	Direction	Activity
1	Device → Gateway	Request permission to access VDI system from Gateway
2	Gateway → PA	Gateway forwards session to PA
3	PA → PE	PA requests PE to determine session access availability
4	PE → PA	PE notifies PA of access decision
5	PA → Gateway	If PE decides to allow the access, the gateway is opened, if not, PE request the gateway to close the session.
6	Device ↔ Gateway	Establishes a connection between the gateway and device when allowed, terminate session to device when denied
7	Gateway ↔ VDI	Access internal system through gateway
8	VDI → Gateway	VDI requests permission to access internal system from Gateway
9	Gateway →PA	Gateway forwards session to PA
10	PA → PE	PA requests PE to judge VDI session availability
11	PE → PA	PE notifies PA of VDI access decision
12	PA → Gateway	If PE decides to allow the access, the gateway is opened, if not, PE request the gateway to close the session.
13	VDI ↔ Gateway	Establishing a connection between VDI and Gateway
14	Gateway ↔ Internal System	Access internal system through gateway

위와 같이 제로 트러스트 모델별 업무 흐름에 대해 알아보았다. 추가로 각 업무 흐름에서 단말기와 내부 시스템 간의 접속이 이뤄졌다 하더라도 Gateway는 모니터링을 통해 PA에 세션별 행위에 대해 PA에 전달하여야 하고, PA와 PE는 지속해서 검토함으로 이상 행위 차단을 수행하여야 한다. 또한 제로 트러스트 모델을 적용할 때 Device-agent 모델은 PA와 PE에, Resource Portal 모델은 Gateway, PA, PE에 트래픽이 집중되면 서비스 부하가 발생할 여지가 있다. 따라서 시스템 구성 시 가용성 측면을 고려하여 설계하여야 한다. 그 외 3-Tier 구조, 이중화, 고가용성 등 시스템 설계 시 고려사항을 설계에 반영할 수 있도록 사전 검토 과정이 필요하다.

V. 제로 트러스트 재택근무 시스템 구축 방법론

5.1 제로 트러스트 재택근무 시스템 구축 방법론 개요

상기에서는 제로 트러스트 아키텍처를 적용한 재택근무 시스템을 구성하는 방식에 대해 알아보았다. 실무에서는 구축 모델을 선정하는 것도 중요하지만 어떤 절차로 구축을 진행할 것인지도 중요하다. 본 논문에서는 제로 트러스트 재택근무 시스템을 구축하는 방법론을 제시하여 현장에서 안전한 제로 트러스트 아키텍처를 적용할 방안을 모색하고자 한다. 재택근무 시스템과 같이 외부에서 기업 시스템에 접근하여 이용하는 것은 정보 유출 요인이 기업 내부뿐만 아니라 외부에서도 발생할 수 있는 위험이 있다. 실례로 재택근무가 가장 활성화된 시기인 코로나19 팬데믹

기간에 VPN을 대상으로 한 사이버 공격이 발생하여 사고로 이어진 일도 있었다. 따라서 정보시스템 설계/구축 시 위험 관리 프로세스를 연계하여야 최소화된 위험으로 시스템을 구현할 수 있다.

본 논문에서 제시하는 제로 트러스트 재택근무 시스템 구축 방법론은 Fig. 19. 과 같다.

최근에는 DevOps와 보안을 융합한 DevSecOps를 통해 개발과 운영에 이어 보안도 통합하는 방법에 관해 연구가 진행되고 있다. IT시스템이 기업의 핵심 전략 자산으로 활용되는 만큼 지속 가능한 시스템 유지를 위해 안전성을 확보하는 것이 점점 중요해지고 있다.

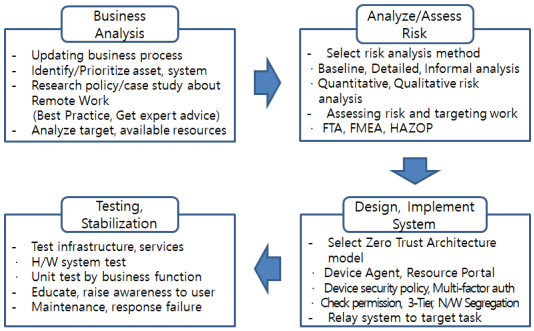


Fig. 19. Methodology of Implementing Zero Trust Remote Work System

5.1.1 업무 현황 분석(Business Analysis)

이 단계에서는 업무 프로세스 현행화, 자산 및 시스템 식별 및 중요도 산정, 재택근무 관련 제도 및 사례 조사, 재택근무 대상 인원 및 현 수준의 가용 자원 분석하는 절차가 필요하다.

업무 프로세스 현행화의 경우 평소에도 경영활동으로 수행하는 활동인데 기업의 업무 절차를 명세하고 필요하면 도식화를 통해 해당 업무의 속성을 파악하는 활동이다. 이를 통해 경영진이 현황을 이해하고 위험 관리를 위한 의사결정을 내리는 데 활용이 가능하다. ISMS-P 인증 기준에서는 업무 프로세스 현행화 대신 정보 흐름도, 개인정보 흐름도 작성을 통해 정보 서비스 현황을 식별하고 문서화하는 것을 관리체계 수립 운영 평가 기준으로 포함하고 있다[20]. 이 활동으로 재택근무 대상 업무 평가뿐만 아니라 향후 기업 내 정보 서비스를 구축할 때도 활용될 수 있으므로 평시 경영활동에 포함하여 관리하는 것이 필요하다.

자산 및 시스템 식별/중요도 산정은 위험 관리 활동 중 하나로 수행되기도 한다. 해당 내용은 하드웨어 등 물리적 자산과 정보 서비스 등 정보자산을 포함하며 식별된 자산을 통해 중요도 평가를 수행하게 된다. 중요도 평가는 자산에 대해 중요도 선정 기준을 통해 평가하게 되는데 정보보안 관점에서는 기밀성, 무결성, 가용성을 기준으로 평가하고 회계학에서는 평가 시점에서 감가상각을 고려한 재무적 가치에 중점을 두어 평가한다. 따라서 특정 정보자산의 중요성은 관점에 따라 달라질 수 있으므로 기업 자체적인 판단으로 결정되기도 한다.

재택근무 관련 제도와 사례 조사를 통해 재택근무 시스템을 보유한 기관 또는 기업의 방법론 또는 고려사항 등을 파악하여 요구 사항에 반영하는 활동이 필요하다. 또한 개인정보 보호법, 정보통신망법, 신용정보 보호법 등 정보시스템 구축과 관련한 법/제도 검토를 통해 중요도 산정에 고려하여야 한다. 또한 기업 내에 IT 관련 전문역량을 보유하지 못한 경우 전문가 자문 등을 통해 시스템 구현에 필요한 기술적 요구 사항 등을 확보할 필요가 있다.

재택근무 대상 인원 파악과 가용 자원 분석 절차를 통해 재택근무를 수행할 업무와 필요 비용을 계산할 수 있다. 재택근무로 수행할 수 있는 업무가 있지만 현장에서만 수행할 수 있는 업무들도 있으므로 재택근무 대상 인원을 정할 때 회사가 운영될 수 있는 필요 최소인원을 정할 필요가 있다. 또한 가용 자원 분석을 통해 시스템 구축 시 필요한 비용산정을 수행할 수 있다.

5.1.2 위험도 분석 및 평가(Analyze/Assess Risk)

앞서 업무 현황 분석 결과를 토대로 종합적인 위험도 분석 및 평가 과정이 필요하다. 이를 통해 기업에서 총괄적 위험 관리를 통해 대책을 마련하거나 감수하는 등의 활동을 수행할 수 있다.

우선 위험분석 방법을 선정하는 것이 필요한데 그 방법에는 기준선 접근법(Baseline approach), 세부적 위험분석(Detailed approach), 임의적 위험분석(Informal approach) 등이 있다. 기준선 접근법의 경우 위험에 대한 보호 기준 수준을 정하고 기준에 따라 대책을 마련하는 방법이다. 위험분석을 명확히 할 수 있고, 적용이 쉽다는 장점이 있지만, 시스템 특성을 고려하여 관리하기 어려운 점이 있다. 세

부적 위험분석은 자산가치, 위협 정도, 취약점 등을 분석하여 위험 정도를 결정하는 방법으로 각 시스템에 대한 적정한 보안 수준을 마련할 수 있는 장점이 있으나 시간이 많이 소요되고 전문지식을 보유하여야 가능한 점이 있다. 임의적 위험분석은 전문가의 지식과 경험을 활용하여 위험분석을 수행하는 방법인데 단기간에 완료할 수 있으나 전문가의 역량에 따라 편차가 발생하는 점이 있어 시급성이 필요할 경우 활용한다. 기준선 접근법과 세부적 위험분석을 연계하여 복합적 위험분석을 수행하는 방법도 있다.

위험분석 기법은 정량적 위험분석과 정성적 위험분석으로 구분할 수 있다. 정량적 위험분석의 종류로는 수식 계산법, 과거 자료 분석법, 확률 분포법, 점수법 등이 있고, 정성적 위험분석은 델파이법, 시나리오법, 순위 결정법 등이 있다. 정량적 위험분석 기법을 세부적으로 보면 수식 계산법은 위험을 수식화를 통한 계산으로 평가하는 방법으로 자산가치, 노출계수, 연간 발생률을 고려하여 연간 예상 손실액(ALE)을 수식을 통해 수치화하는 방법이다. 과거 자료 분석법은 해당 위험과 연관된 과거 사례를 조사하여 해당 사례에서 발생한 피해액 등을 통해 위험 평가를 수행하는 방법이다. 확률분포법은 표준분포식을 활용하여 PERT(Program Evaluation and Review Technique)와 같이 베타분포를 가정하여 추정하는 기법이다. 점수법의 경우 위협 발생 요인에 가중치를 부여하여 점수화를 통해 위험 평가하는 방법이다. 정성적 위험분석의 경우 델파이법, 시나리오법, 순위 결정법 등이 있다. 델파이법의 경우 전문가를 활용하여 위험분석을 통해 전문지식을 활용하는 기법이다. 시나리오법의 경우 발생 가능한 시나리오를 선정하고, 시나리오에 의해 발생 가능한 위험요인이 있는지 분석하는 기법으로 모의 해킹 등 기술적 취약점 분석에 활용되기도 한다. 순위 결정법은 순위 결정 표를 작성하여 위험 항목들에 대해 서술적으로 순위를 결정하는 방법이다[21].

위험분석의 과정을 완료하면 위험 평가와 재택근무 대상 업무 선정 과정이 필요하다. 위험 평가 기법으로는 FTA(Fault Tree Analysis), FMEA(Failure Modes and Effects Analysis), HAZOP(Hazard and operability) 방법이 있다. FTA의 경우 모든 결함 상황에 대해 트리구조로 나타내어 위험을 분석하는 방법으로 명확화된 위험 케이스를 분류할 수 있지만, 작성이 어렵고 시스템이 복잡해질 경우 고려될 상황이 급격히 늘어나는 단점이 있다. FMEA의 경우 특정 사건의 예상 결과에 관한 질문을 시작으로 생각의 범위를 넓혀가며 평가하는 기법이다. 제품을 부품 또는 기능별로 나누어 관계를 설정 후 전문가 참여를 통한 분석하는 기법인데 고차원적인 분석이 가능하지만 시간 소요가 많은 단점이 있다. HAZOP의 경우 여러 전문분야의 구성원이 난상토론을 통해 위험분석을 하는 방법인데 전문분야의 다양성을 확보하고 기초자료 확보 후 토론을 시행하여 평가할 수 있다. 평가가 완료되면 결과에 따라 재택근무를 활용할 수 있는 대상 업무를 선정하여 시스템 설계에 반영한다.

5.1.3 시스템 설계 및 구축(Design, Implement System)

시스템 설계 및 구축에서는 대상 업무 및 비용을 고려하여 적합한 제로 트러스트 아키텍처 모델을 선정하고 대상 업무 서비스를 연동한다. 3장에서 기술했듯이 On-Premise 방식 또는 클라우드로 구축할 것인지를 선정하고, Device Agent/Gateway 모델 또는 Resource Portal Gateway 모델을 선정할지를 정한다. 이때 회사 내의 단말기 보안과 2단계 인증 적용 여부, 접근권한 관리 등 보안 정책 검토와 망 분리, 3-Tier 구조, 이중화 및 고가용성 유지 등의 요소를 고려하여 설계할 필요성이 있다. 또한 위험 평가 결과에 따라 선정된 대상 업무와 관련한 시스템 연동을 통해 재택 환경에서도 업무수행이 가능하도록 구성하여야 한다.

5.1.4 테스트 및 안정화(Testing, Stabilization)

재택근무 시스템을 구축할 때 업무 시스템 연동과 네트워크, 보안 시스템 등 연동될 IT 자원들이 다수 발생하기 때문에 시스템 연동 작업 중 오류, 통신 경로 문제 등 작업 중에도 예상하지 못한 문제점이 나타나게 된다. 따라서 구축을 완료한 후에는 테스트 수행이 필요한데 하드웨어의 경우 시스템 테스트를 통해 하드웨어 및 통신 경로 등의 문제점이 없는지 확인이 필요하고, 미비한 부분을 보완하여 재구성한다. 업무 서비스는 서비스 내 기능들이 정상적으로 동작하는지 단위 테스트를 진행하여 기능 오류 또는 미 동작 등 서비스 오류를 보완한다. 클라우드로 구축을 하는 경우 기존의 클라우드 서비스와의 호환성과 외부 클라우드와의 연동 등 기업 내부뿐만 아니라 외부 환경까지 고려하여 테스트를 수행한다. 시스템

을 구축 완료하면 사용자 교육을 통해 시스템 사용 방법에 대한 교육을 수행하여 이용률을 높이고, 재택근무 시 유의 사항을 인지시켜서 사용자들이 안전하게 시스템을 이용할 수 있도록 하는 과정이 필요하다. IT 기기 사용이 익숙한 청년층 세대는 인식 전환이 빠르나 익숙하지 않은 중장년층의 경우 사용 과정에서 어려움을 겪기도 하기에 설명회, 시연 등을 통해 안내하는 것이 필요하다. 또한 재택근무 중 서비스 접속 오류 등 장애에 대응하기 위한 체계 마련과 지속적인 유지보수를 통해 운영 연속성을 유지할 수 있도록 고려해야 한다.

5.2 제로 트러스트 재택근무 시스템 구축 방법론 적용 시 고려사항

성공적인 방법론이 있어도 현장에서 적용하기 어렵거나 적용 과정에서 어려움이 발생하는 경우가 많다. DevOps 방법론이 등장한 지 여러 해가 지났지만, 기업 내부 문화에 성공적으로 안착해 운영하는 기업들은 IT 기업 또는 스타트업에서 나타나는 편이다. 이는 제로 트러스트 재택근무 시스템 구축 방법론을 적용할 때도 마찬가지라 예상되기에 적용 시 고려할 주요 사항에 대해 파악할 필요가 있다.

5.2.1 사용자 시나리오 정의

재택근무 시스템의 경우 주 사용자는 임직원으로 예상할 수 있다. 기업은 업무 속성과 형태에 따라 필요한 역량과 직무가 다르며 직무별로 업무수행 방식도 다양하다. 스타트업과 같이 업무를 발굴하거나 조직문화를 만들어 가는 회사의 경우 자체적으로 보유하는 IT 자원 대신 외부 플랫폼을 활용하여 업무를 수행하기도 하고, 공공조직이나 대기업의 경우 회사 내부에서만 활용할 수 있는 자원이 있기도 하며, 글로벌 기업의 경우 해외 지사에서 본사의 시스템을 접속하여 이용하기도 한다. 따라서 업무 현황 분석단계를 수행할 때 사용자 관점에서 업무 절차를 분석하여 시나리오를 정의하는 과정이 필요하다. 정보보호 관리체계 국제 표준인 ISO27014에서도 정보보호 조직과 이해관계자와의 소통(Communicate)이 중요 항목으로 제시되기에 사용자의 요구에 적절히 대응하기 위해서는 필수적이다[22]. 이 과정에서 활용될 수 있는 기법이 UX 설계에서 주로 사용되는 '페르소나 분석법'과 '고객 여정 지도' 등이 있다. 페르소나 분석법을 통해 사내에서 업무 하는 다양한 직군 정의가 가능하고, 고객 여정 지도로 각 직군별 업무수행 절차를 알 수 있다. 이 과정을 통해 업무 환경의 다양성을 고려하면서 위험분석 및 평가 단계에서 관리 가능한 위험 수준을 파악할 수 있는 이점이 있다. 이를 반영한 사례로 구글은 사용자 경험을 반영하기 위해 직원 VPN 사용 시나리오를 작성하여 VPN을 제거할 방안에 대해 모색하였다[14].

5.2.2 보유 IT 역량 파악

'구슬이 서 말이어도 꿰어야 보배'라는 속담이 있듯이 기업에서 시스템을 구현할 역량이 없다면 방법론이 있어도 활용하기 어렵다. 우선 TA 구현의 경우 규칙 기반 또는 점수 기반으로 구현할 것인지에 관한 결정은 기업에서 TA를 구현할 수 있는 개발 능력과 시스템 운영 역량이 필요하며, TA의 평가 정확도를 향상하기 위해 필요 데이터 확보와 연계할 데이터 항목 등 데이터 과학적 측면도 같이 고려되어야 한다. 또한 단일 구성으로 구현할지, 문맥 기반으로 수행할지도 네트워크 및 데이터 관리 수준에 따라 이력 데이터 저장 및 활용을 할 수 있다. Device Agent/Gateway 모델과 Resource Portal based 모델의 선정에서도 기업의 정보자산 관리 수준에 따라 적용 여부를 판단할 수 있기에 IT에 대한 기술력, 관리 능력에 대한 중요성은 점점 증가할 것이다. 또한 기업에서 보유하고 있는 IT 인력에 대한 기술 능력도 파악하여야 한다. 클라우드로 구성할 수 있는 기술이 있는지, 적정한 인력 배치를 하였는지를 포함하여 인력관리가 필요하다.

5.2.3 정보보호 수준 결정

CISA에서 제시하는 제로 트러스트 모델에서 고려하는 보안 요소는 크게 Identity, Device, Networks, Applications and Workloads, Data이다. Identity에서의 고려할 부분은 다단계 인증이 안전하게 이뤄지고 있는지와 Identity에 대한 지속적 위험 관리인데 Device Agent/Gateway-based 모델에서는 단말기 인증과 계정 인증이 가능하지만, Resource Portal-based의 경우 OTP/생체인증 등 다른 방법의 인증을 추가하는 방안이 필요하다. 또한 각 인증을 위한 통신은 HTTPS 프로토콜을 활용한 암호화 통신으로 구현되

어야 하며, 지속적인 접속 세션 평가를 통해 안전 여부를 검증해야 한다. Device의 경우 장치 이력 추적이 가능해야 하며 자동으로 추적 관리가 가능한지, 실시간으로 장치 위험분석이 가능한지를 고려해야 한다. Network는 분산된 형태로 실시간 접근제어와 회복력을 가질 수 있는지와 암호화 통신이 고려되어야 하며, Application and Workloads의 경우 응용 프로그램 사용 시 지속해서 인증된 접근을 수행하는지와 전체 생명주기에서 공격 방어와 보안 테스팅이 수행되는지가 고려사항이다. 마지막으로 Data의 경우 지속적인 데이터 저장과 데이터 가용성, 데이터 소실 방지, 동적인 접근제어, 데이터 암호화를 고려해야 한다. 기업의 IT 운영 수준이 같을 수 없고 운영 규모에 따라 활용할 수 있는 자원의 차이가 크기 때문에 현 수준에 부합하는 단계를 적용하고 지속적인 투자를 통해 점진적으로 정보보호 수준을 향상할 수 있도록 하여야 한다.

5.2.4 다양한 전문가 교류

업무 현황 분석 및 위험 평가를 수행할 때 전문가 자문, 참여가 필요하다. 하지만 시스템 구축 상황이 되었을 때 전문가를 확보하려면 적합하지 않은 전문가를 선정하거나 전문가를 구하지 못하는 등의 어려움을 겪을 수 있다. 그렇기에 기업에서는 평상시에 다양한 전문가를 확보하기 위한 인력 양성 체계와 내/외부 간 인적 네트워크를 구축하고, 상호 교류 활동을 통해 전문적 의견을 수용할 수 있는 체계가 필요하다.

VI. 결 론

본 연구는 NIST의 표준을 기반으로 제로 트러스트 아키텍처로 재택근무 시스템을 구성하는 방안에 대해 제시하였다. 제로 트러스트 아키텍처를 실무적으로 구축할 방안을 연구하였다는 점에서 학술적 공헌이 있으며 기업에서 제로 트러스트 아키텍처를 적용할 때 활용할 수 있는 가이드로서 공헌할 수 있다.

본 논문은 PE에 인공 지능을 활용하는 등 고수준의 구현 방법을 제시하지 못한 한계가 있다. 추후 제로 트러스트 아키텍처 수준을 향상할 수 있는 방안에 관해 연구할 필요가 있다. 또한 상기에서 제시한 구성 방법과 구현 방법론은 실제 적용된 사례가 없어 검증하지 못한 한계점이 있다. 현재로는 검증에 대한 대안이 없는 한계가 있어 실무 적용 사례 발굴 등을 통해 실효성 및 발전성 등을 확인하는 것이 중요한 향후 연구과제이다. 이를 통해 지속해서 변화하는 사이버 환경에 능동적으로 대응할 수 있는 체계를 구축하여 안전하면서도 사용성이 뛰어난 제로 트러스트 환경 조성에 이바지할 것으로 기대한다.

References

[1] Executive Order on Improving the Nation's Cybersecurity, (5/2, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] Kyung-bok Lee, Tae Hyoung Park and Lim Jong In, "Security Threats and Countermeasures according to the Environmental Changes of Smart Work", Journal of Digital Convergence, Vol9(4), pp. 29-40, Jan. 2011.

[3] So-yeon Kim, Ha Yeong Min, Kim Sung Yul, Sang-Yong Choi and Jong-Lark Lee, "The Analysis for Cyber Security Threats in Remote Working Environment", Journal of The Korea Society of Computer and Information, Vol28(2), pp. 97-98, Jul. 2020.

[4] Nurse, J. R., Williams, N., Collins, E., Panteli, N., Blythe, J., and Koppelman, B, "Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy", HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Communications in Computer and Information Science, Vol1421, pp. 583-590, July 24-29, 2021, Springer International Publishing.

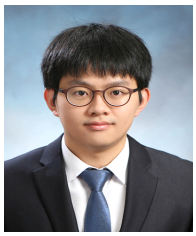
[5] F. Malecki, "Overcoming the security risks of remote working", Computer fraud & security, Vol2020(7), pp

10-12, Nov. 2021.
[6] T. Chuan, Y. Lv, Z. Qi, L. Xie and W. Guo, "An Implementation Method of Zero-trust Architecture", Journal of Physics: Conference Series, Vol1651(1), pp. 21-23, Aug. 2020.
[7] Ko Min Hyuk and Daesung Lee, "Zero Trust-Based Security System Building Process", Journal of the Korea Institute of Information and Communication Engineering, Vol25(12), pp. 1898-1903, Dec. 2021.
[8] S. Teerakanok, T. Uehara and A. Inomata, "Migrating to Zero Trust Architecture: Reviews and Challenges", Security and communication networks, Vol2021, pp. 1-10, May. 2021.
[9] HAN SUNG HWA and Hooki Lee, "Zero Trust Technology Trend and Implementation Strategy", Journal of convergence security, Vol21(5), pp. 43-50, Dec. 2021.
[10] R. Ward and B. Beyer, "Beyondcorp: A new approach to enterprise security" Usenix, Vol39(6), pp. 6-11, Dec. 2014.
[11] B. Osborn, J. McWilliams, B. Beyer and Saltonstall, M., "Beyondcorp: Design to deployment at google", Usenix, Vol41, pp. 28-34, 2016.
[12] B. Spear, L. Cittadini, B.Beyer and M. Saltonstall, "Beyondcorp: The access proxy", Usenix, Vol41(4), pp. 28-33, 2016.
[13] C. Beske, J. Peck, B. Beyer and M. Saltonstall, "Migrating to BeyondCorp: maintaining productivity while improving security", Usenix, Vol42(2), pp. 49-55, 2017.
[14] V. Escobedo, F. Zyzniewski, B. Beyer and M. Saltonstall, "BeyondCorp: the user experience", Usenix, Vol42(3), pp. 38-43, 2017.
[15] H. King, M. Janosko, B. Beyer and M. Saltonstall, "BeyondCorp 6: Building a Healthy Fleet", Usenix, Vol43(3), pp. 24-33, 2018.
[16] S. Rose, O. Borchert, S. Mitchell and S. Connelly,(2020). "Zero trust architecture", NIST Special Publication (SP) 800-207, pp. 1-50, Aug. 2020.
[17] Cybersecurity Division, "Zero Trust Maturity Model", Cybersecurity and Infrastructure Security Agency(USA), V2.0, pp. 1-32, Apr. 2023.
[18] Soohwan Lee, "Legislative and policy tasks related to digital financial innovation - Focusing on improving network separation regulations in the financial sector", NARS Current Issue Analysis, No202, pp. 1-13, Jun. 2021.
[19] OFFICIAL INFORMATION DISCLOSURE ACT, (5/16, 2023), https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B3%B5%EA%B3%B5%EA%B8%B0%EA%B4%80%EC%9D%98%EC%A0%95%EB%B3%B4%EA%B3%B5%EA%B0%9C%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0
[20] ISMS-P Certification Criteria Guide, (4/22, 2022), https://isms.kisa.or.kr/main/ispims/notice/?boardId=bbs_0000000000000014&mode=view&cntId=16
[21] Jungduk Kim and Kiyoon Kim. "Risk Analysis Methods for Information Security: Classification and Selection Criteria", Journal of The Korea Institute of Information Security and Cryptology, Vol.4(1), pp. 303-315, Nov. 1994.
[22] ISO/IEC 2020, "Information security, cybersecurity and privacy protection - Governanace of information security", ISO/IEC 27014, pp. 1-13, Apr. 2021.
[23] Domestic cloud adoption status survey results and Cloud Success Strategy, (5/8, 2023), https://www.ibm.com/downloads/cas/NVMG3MLW
[24] Protect apps with Microsoft Defender f

or Cloud Apps Conditional Access App Control, (3/21, 2023), https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

[25] What is Conditional Access?, (5/26, 2023), https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

〈저자소개〉



도 재 우 (Jaewoo Do) 정회원
2013년 8월: 서강대학교 컴퓨터공학과 학사
2023년 8월: 한국과학기술원 경영대학 정보경영 석사
2014년 1월~2015년 12월: 한국특허정보원 근무
2015년 12월~현재: 한국항공우주연구원 선임기술원
〈관심분야〉 사이버보안, 개인정보보호, IT 경영, 데이터 과학

강 금 석 (Keumseok Kang) 정회원
1996년 2월: 서울대학교 산업공학과 학사
1998년 2월: 서울대학교 산업공학과 석사
2011년 8월: 퍼듀대학교 경영학과 박사
2019년 1월~현재: 한국과학기술원 경영대학 교수
〈관심분야〉 정보시스템, IT 경영, 데이터 과학, 인공지능, 사이버보안