https://doi.org/10.33778/kcsa.2024.24.1.027

망분리 환경에서 제로 트러스트를 활용한 DevOps 운영에 관한 연구

한 봉 용*, 최 영 근**, 소 가 연**, 신 용 태***

요 약

망분리는 침해 사고의 예방과 데이터를 보호할 수 있는 중요한 정책이다. 최근 소프트웨어 개발에 있어 재택 근무와 클라우드, 오픈소스 활용 등 IT 환경이 변화하고 있다. 이러한 변화에 핀테크 기업들은 망분리 규제로 개발 생산성과 효율성이 낮아지고 있어 이에 대한 망분리 완화 요구가 계속되었다. 정부는 IT환경 및 핀테크 기업의 망분리의 완화 요구에 전자금융감독규정을 개정하였다. 2023년 01월 01일부터 시행된 전자금융감독규정 일부 개정안은 클라우드 환경에서의 연구개발 목적인 경우에 한정하여 망분리가 완화되었다. 클라우드 개발 환경에서 개발된 소프트웨어를 배포 시스템을 통해 운영 시스템에 적용할 경우 기존 경계 기반 모델로는 망분리 조건을 충족하지 못할 것이다. 본 연구에서는 제로 트러스트 보안 체계를 활용하여 망분리 환경에서의 DevOps 체계를 유지할 수 있는 방안을 제안하고자 한다.

A Study On Operation for DevOps Using Zero Trust in Network Separation Environment

Bong-Yong Han*, Young-Kun Choi**, Ga-Yeon So**, Yong-Tae Shin***

ABSTRACT

Network separation is an important policy that Cyber Incident prevent cyber and protect data. Recently, the IT environment is changing in software development, such as remote work, using the cloud, and using open sources. Due to these changes, fintech companies' development productivity and efficiency are lowering due to network separation regulations, and the demand for easing network separation continued. The government revised the regulations electronic financial supervision(hereafter EFS) in response to needs for mitigation of network separation in the IT environment and fintech companies. Some amendments to the EFS, which took effect on 01/01/2023, mitigate network separation only for research and development purposes in cloud environments. If software developed in a cloud development environment is applied to an operating system through a distribution system the existing perimeter-based security model will not satisfaction the network separation conditions. In this Study, we would like to propose a way to maintain the DevOps system in a network separation environment by Using the zero trust security system.

Key words : (Zero Trust, Network Separation, DevOps, Pillars, SDP)

접수일(2024년01월 11일), 수정일(1차: 2024년 02월 07일), 게재확정일(2024년 02월 26일)

* 숭실대학교/IT정책경영학과 (주저자)
** 숭실대학교/IT정책경영학과 (공동저자)
*** 숭실대학교/컴퓨터학부 (교신저자)

1. 서 론

스마트시대, 원격 근무 등 일상적 업무 환경의 변화, 오픈 소스를 활용한 빠른 응용 SW개발등 IT의 환경이 빠르게 변화하고 있다. 핀테크 산업에서도 새로운 신규 서비스의 개발이 발빠르게 진행되고 있다. 개발 환경도 온-프레미스에서 클라우드 네이티브로 빠르게 전환되고 있다. 핀테크 기업들은 오픈 소스 및 오픈 API를 활용한 신규 비즈니스 SW 개발에 많은 투자를 하고 있다. 그러나 금융 및 핀테크 기업은 망분리라는 규제로 인해 개발 생산성과 업무 효율성이 낮은 환경에서 개발을 하고 있어 산업의 발전이 더디다[1]. 또한 COVID-19를 거치면서 근무 형태 또한 원격지 근무 유형이 일상화 되었고 이러한 환경은 더욱 더 망분리로 인해 효율적이지 못한 업무 환경이 지속적으로 이어져 개발자의 이탈도 발생되고 이직의 원인을 제공한다는 조사가 있다[2]. 최근 망분리 완화 정책이 적용되었으나 현장에서는 불만이 지속되고 있다. 개발된 소프트웨어를 상용 서비스를 위한 배포 하기위해 망연계등 DevOps의 체계를 유지하는데 어려움을 겪고 있다. 본 논문에서는 새로운 보안 체계인 제로 트러스트 모델을 활용하여 IT DevOps 환경을 SDP, 마이크로 세그먼트 및 6Pillars 영역에서 워크로드별 엑세스 대상을 적용하여 최근 시행된 망분리 완화 정책[3], [4]보다 보안이 강화된 DevOps 환경을 제안하고자 한다.

2. 망분리 현황과 DevOps 환경

2.1 망분리 도입 배경

우리나라 망분리 규제는 2006년 국가사이버 안 전 전략회의에서 최초로 망분리가 보고된 이 후 2007년부터 국가기관을 중심으로 망분리에 대한 시범 사업이 시행되었다[5]. 2008년 01 월 중국인 해커로 추정되는 이들은 옥션의 웹서버에 침입 하 여 1,080 만명의 개인정보(이름,주민등록번호,주소, 계좌번호 등)을 유출 하였고, 2008 월 07 월 GS 칼 텍스 협력 업체인 GS 넥스테이션 직원이 1,151 만 명의 개인정보(이름, 주민등록번호,주소,전화번호,이 메일 등)를 빼냈다. 이렇게 내외부에 의하여 대규모의 정보유출 사고가 발생되자 2012년 정보통신 망법을 개정하여 개인 정보를 취급하는 기업에 대한 망분리를 의무화 하였고 2014년 1 월에 발표한 카드사(롯데, 농협, KB)의 경우 2012년 10 월부터 2013년 12 월까지 지속적으로 개인정보가 유출되는 사고가 발생 되었다. 이에 따라 홈페이지 취약점을 공격하여 금융권 및 방송사의 동시 다발적 전산 장애를 유발한 3.20 발생 후 금융위는 “금융전산 보안 강화 대책”을 발표하고 전자금융감독규정을 개정하여 금융 전산의 망분리를 의무화 하였다.

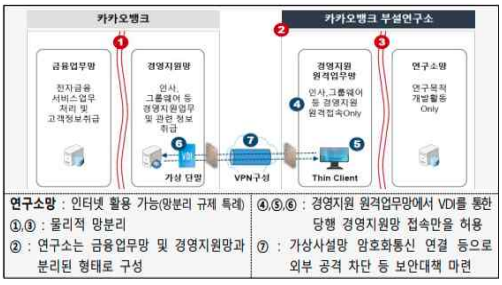
2.2 망분리 규제 현황

현재 국내에서 망분리를 의무화하는 규정은 크게 ‘국가정보보호기본지침’, ’개인정보보호법’, ’전자금융감독규정’이며 이를 준수해야 하는 영역은 공공,민간, 금융이다[2], [5]. 공공기관을 대상으로 하는 망분리 규제는 국가정보원에서 배포하는 국가정보보안기본지침에 근거하고 있으며, 해당 지침에서는 모든 공공 기관을 망분리 대상으로 규정하고 있고 업무 지침에 따라 전산망과 업무망을 분리 운영해야 한다. “민간부문의 망분리 규제는 2012.8.17 「정보통신망 이용촉진 및 정보보호 등에 관 한 법률 시행령」 제 15 조 20 에서 도입되었다”[2]. 2020.01.09 데이터 3 법의 개정으로 망분리는 개인정보보호법으로 이관 되었다. 개인정보보호법 제 29 조에서는 개인정보처리자의 개인정보 안전성 확보조치를 규정하고, 세부기준인 개인정보의 기술적·관리적 보호조치 기준(이하 “개인정보보호법 고시”라고 한다.) 고시에서 망분리 규정을 두고 있다. 금융회사나 전자금융업자와 같은 핀테크 기업의 경우 전자금융거래법의 망분리 조항이 적용된다. 전자금융거래법 제 21 조에서는 금융회사와 전자금융업자를 대상으로 안전성 확보 의무를 부여하고 있으며, 전자금융감독규정 제 15 조 제 3 호와 제 5 호에 망분리 조항을 두고 있다. 핀테크 관련 사업에 진출한 ICT 기업은 개인정보보호법 고시와 전자금융감독규정의 망분리 조항을 적용받게 된다. 두 고시는 망분리를 규정하고 있다는 점에서는 동일하지만 고시의 적용대상과 망분리 대상, 망분리 방법 등을 다르게 규정하고 있다[5]. 이러한 핀테크 기업의 경우 과도한 망분리 규제로 핀

테크 산업의 높은 진입 장벽과 투자비용의 증가에 불만을 토로하고 있다[6]. 최근 전자금융감독규정 개정('연구.개발 목적의 망분리 예외 적용)으로 개인의 고유식별정보 또는 개인신용정보를 처리하지 않는 개발연구 목적의 경우에 한하여 망분리 규제가 완화 되었다[4].

2.3 개정된 망분리 완화 정책

정부에서는 변화된 IT 환경과 핀테크 산업 발전에 영향을 주고 있는 망분리에 대한 규제 완화 정책인 전자금융 감독규정 개정안이 금융위원회에서 의결되어 2023.01.01 일부로 망분리 완화 정책이 시행되었다. 실제 금융위원회에서는 보도자료를 통해 망분리 완화를 (그림 1)와 같은 운영 방안 사례를 제시하였다.

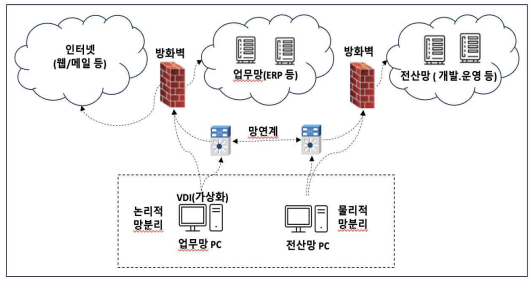


(그림 1) 카카오뱅크 '금융기술연구소' 운영사례[4]

기존 망분리 규제 완화 정책 시행에도 기업들은 반기는 분위기보다 기술적 보안 대책은 부실하고 8 년전 망분리 정책과 보안체계를 그대로 유지하는게 맞는지에 대한 평가가 있다[8], [9]. 완화된 망분리의 경우는 업무망 VPN 을 통한 접속만 허용하는 수준에서 완화 되었다. 완화된 망분리 정책은 기존의 DevOps 환경에서의 경계기반모델 보다 복잡하게 운영되어야 하는 구조를 갖는다.

2.4 망분리 적용된 DevOps 환경

핀테크 기술 변화는 오픈 소스의 활용과 개발자 커뮤니티, 개발 협업 시스템의 클라우드화등 개방된 환경에서 진행되고 있는 추세이다. 그러나 망분리 환경에서는 외부 인터넷과 통신이 차단된 상태에서 개발 진행시 개발자의 생산성과 업무 효율성이 떨어지는 결과가 초래되고 있다[7]. 전자금융업 또는 핀테크 회사의 경우 (그림 2)과 같이 물리적 망분리와 논리적 망분리로 구성된 3 개 망의 단말기를 사용하고 있다. 업무 환경을 살펴보면 IT 직군과 비 IT 직군간 협의는 업무망에서 오픈소스, 개발자 커뮤니티, 메일등은 논리적 망분리된 VDI 환경을 이용하며 개발은 폐쇄된 망에서 개발과 배포가 이루어지고 있다. 이러한 환경에서 망을 전환해 가며 업무를 수행 하다 보면 개발 생산성과 효율성이 낮아지고 신기술의 도입과 활용에 제약이 따를 수밖에 없다. 이와 같은 문제는 핀테크 산업의 개발 직군의 인력 지원을 꺼리는 현상에도 영향을 준다. 기업 입장에서도 초기 투자 비용과 인력난에 어려움을 겪고 있다[6].



(그림 2) 망분리 적용된 IT 환경

완화된 망분리를 기준으로 개발 환경에서 개발된 소프트웨어를 서비스하기 위해서는 소프트웨어를 배포해야 한다. 결국 망연계를 이용하여 전산망으로 소프트웨어를 복제하여 배포해야 하는 DevOps 환경이 비효율적으로 운영이 될 수밖에 없다. 이러한 DevOps 환경을 효율적으로 운영하기 위한 제로 트러스트의 보안 모델을 적용하여 자동화된 배포 시스템 체계가 요구된다.

3. 제로 트러스트 보안 모델

3.1 제로 트러스트 보안 모델 개요

제로 트러스트는 정적인 네트워크 경계 기반에서 사용자, 데이터, 자산 및. 리소스에 초점을 맞춰 보안 체계를 수립하는 보안 모델이다[10]. 2004 년부터 정적 경계기반 방어에는 한계가 있다는 생각들로 인하여. 네트워크 경계선을 제거하는 비 경계화(the idea of

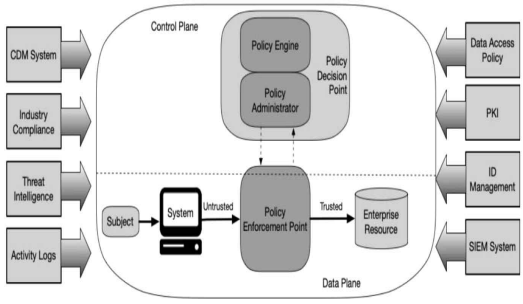
de perimeterization)의 논의가 시작되었다. 미국의 국방정보시스템(DISA,Defense Information System Agency)에서는“블랙코어”(BCORE)라고 불리는 안전한 조직 전략에 대한 연구 결과를 발표하였다. 2004년 개최된 제리코(JERICHO)포럼에서 비 경계화에 대한 개념이 공개되었고 그 이후 2010년 Forrest 에서 John Kindervag에 의해 만들어진 제로 트러스트라는 큰 개념으로 발전하였다[10],[11]. 이후 미 상무부 소속의 국가표준연구소(NIST)는 2020년 08월 미 연방정보에서의 제로 트로스트 도입을 위한 제로 트러스트 아키텍처(ZTA:Zreo Trust Architecture)는 NIST SP 800-207을 통해 공개하였다[10]. 또한 바이든 미 대통령은 2021년 05월 국가 사이버보안 개선 행정명령(EO-14028)을 내리고 미 연방 차원의 국가 사이버보안 체계를 강화하는 절차를 진행중이다[12][13]. 기본적으로 보안 사고는 내/외부를 가리지 않고 발생되고 있으므로 제로 트러스트 “신뢰할 수 있는 네트워크”라는 개념을 배제하는 “Naver Trust, Always Verify(절대 신뢰하지 말고 항상 검증하라)” 라는 보안 전략을 통해 보안 모델의 페러다임 변화를 가져오고 있다[13].

3.2 제로 트러스트 원칙과 아키텍처

제로 트러스트 아키텍처는 7가지 원칙을 기반으로 한 보안 모델을 제시하였다. 다음은 7가지 원칙의 내용이다.

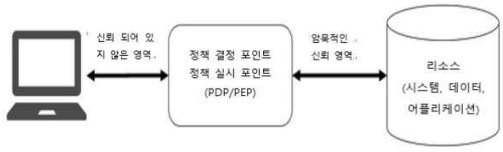
1) 데이터와 컴퓨팅, 서비스는 하나의 리소스
2) 네트워크 장소에 관계없이 통신은 모두 보호
3) 조직의 리소스에 대한 모든 접근은 개별 세션마다 허가
4) 리소스간 이동 및 엑세스는 동적인 정책에 의해서 결정
5) 모든 자산의 무결성 및 보안 상태를 모니터링하고 측정
6) 리소스의 인증과 인가는 강력한 인증 체계
7) 자산, 네트워크, 통신 상태의 많은 정보를 수집, 분석하여 높은 안정성을 제공한다[10], [11].

이러한 원칙을 적용하기 위해 다양한 컴포넌트가 제로 트러스트에 적용되었다. (그림 3) 제로 트러스트 아키텍처(ZTA:Zreo Trust Architecture)는 산업별 규제정책, 인증체계, 로그관리, 위협관리, 모니터링 등 여러 보안 컴포넌트와 정책엔진(PE:Policy Engine), 정책관리자(PA:Policy Administrator) 그리고 정책 결정에 따른 엑세스를 제어하는 정책실행시점(PEP:Policy Enforcement Point)로 구성되어 있다[10], [11].



(그림 3) 제로 트러스트 아키텍처 [10], [11]

(그림 4)와 같이 PDP(Policy Decision Point)의 PE와 PA 정책 결정에 따라 PEP가 리소스에 대한 접근을 수행한다[11]. 조직의 업무와 구성원의 역활, 보호할 자산, 데이터 등을 고려하여 워크로드별 세그먼트로 정책을 수립하여 리소스를 보호한다.

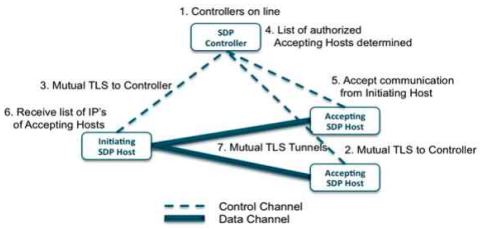


(그림 4) 제로 트러스트 엑세스 [11], [14]

3.3 워크로드별 SDP

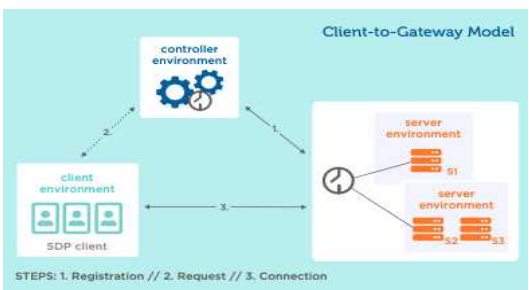
SDP(Software Define Perimeter)는 SDP Agent가 접속을 시작하는 호스트(IH:Initiating Host)와 서비스를 받아들이는 호스트(AH:Accepting Host)는 mTLS를 이용하여 연결해 주는 SDP Controller를 통해 접속 허용에 대한 인증 절차를 (그림 5)와 같이 수행하고[15], [16] SDP GateWay에 정의된 리소스에 접속이 가능하다. 이러한 접속 형태는 엔터프라이즈에서

VPN을 통한 내부 자원의 노출 약점을 개선할 수 있는 대체할 수 있는 보안 구성이다[15], [17]. DP Controller의 인증과 SDP GateWay를 통해 접속하므로 서버의 IP, PORT 정보가 노출되지 않아 안전한 엑세스를 제공한다[11]. CSA 클라우드 보안 얼라이언스 가이드에서 제시한 SDP 모델은 Client To Server, Client To GateWay, Server To Server 등의 여러 모델이 존재한다.



(그림 5) CSA가 공개한 SDP Specification 1.0 아키텍처[18]

이중 Client To GateWay 모델을 중심으로 (그림 6)와 같이 연결에 대한 보안 인증을 하고 접속 후 데이터 전송이 가능한 형태의 보안 모델이다[17]. SDP에 개발과 운영에서 접속 가능한 리소스를 구분하여 정책 설정이 되어야 보안을 강화할 수 있다. 망분리 환경에서 업무망 접속시 사용되던 VPN의 구성을 제로 트러스트의 주요 보안 체계인 마이크로 세그먼트와 SDP를 활용할 경우 (그림 6)과 같이 SDP GateWay를 통해서 서버 및 리소스에 접근하므로 기존의 VPN 기능을 대체할 수 있는 보안 구성이 가능하다[16]. SDP를 통해 접속을 강화하기 위해서는 기업의 업무별 기능과 역할을 정의하고 워크로드별 접근되어야 할 시스템과 리소스에 권한과 범위를 정의하여 횡적 이동을 제한하여 보안을 강화시킬 수 있다.



(그림 6) SDP의 Client To GateWay 모델[16], [17]

3.4 제로 트러스트 핵심 요소

과학기술정통부, 한국인터넷진흥원, 한국제로스트포럼은 제로 트러스트 가이드 1.0을 2023년 06월 제시하였다. NIST에서는 제로 트러스트 핵심 요소를 5가지(5 pillars) 유형으로 제시[14]하였으나 국내 IT의 자산 분류 관점에서 시스템을 추가로 핵심 요소로 6가지(6 pillars)로 분류하여 설명하고 있다[14].

<표 1> 제로 트러스트 가이드 1.0 핵심 요소[14]

핵심 요소	주요 내용
Identity & User	사람, 서비스, IoT기가 등을 고유하게 정의하고 설명할 수 있는 속성
Device & Endpoint	IoT, 노트북, 단말기(PC), 패드, Node 장치, 서버 등을 포함하여 네트워크 연결이 가능하여 통신을 수행하는 하드웨어 장치
Network	기업망의 유/무선 네트워크, 클라우드 접속이 가능한 인터넷 환경, 가정용 네트워크 등 데이터 통신이 가능한 모든 통신 매체
System	중요 서비스를 제공하거나 중요한 데이터 및 정보를 저장하는 서버
Application & Workload	기업 정보 관리 시스템, 프로그램, 온-프레미스 및 클라우드 환경에서 실행되는 서비스 및 프로세스
Data	기업이 최우선으로 보호해야 하는 데이터

워크로드별 네트워크 세그먼트 구성과 <표 1>의 핵심 요소별 리소스에 대한 접근 권한과 모니터링을 체계화하여 보안을 강화하면 망분리에서 DevOps 체계 환경 개선이 될 것이다.

4. 워크로드를 활용한 DevOps 운영

4.1 제로 트러스트 핵심 요소별 워크로드 정책

제로 트러스트 아키텍처 보안 모델을 구성하기 위한 접근 방법에는 NIS SP 800-207에서 제시한 세 가지 방법은 인증 체계 강화, 마이크로 세그먼테이션, SDP(Sofrware Defined Perimeter) 접근법이다[19]. SDP는 리소스에 대한 접근 제한 모델을 제시함으로써 VPN의 역활을 대신할 수 있는 보안 체계이나 이

번 연구에서는 VPN 도 하나의 리소스로 관리하며 온-프레미스의 환경을 흡수하는 구성을 고려하였다. SDP 는 사용자 인증, 장치 확인, 보안 네트워크 연결 설정, 사용자 엑세스와 같은 워크로드별로 정의된 정책을 통해 리소스에 대한 접근이 가능하다. 이러한 SDP 는 워크로드별 사용자의 접근 권한 목록 체계를 사전에 정의하여 엑세스를 관리하면 네트워크 세그먼트로 쪼개진 영역 관리와 함께 기존의 경계 기반의 보안 모델의 취약점인 횡적으로의 이동을 막을 수 있다. 또한 VPN 의 접근 또한 통제가 가능한 보안 체계를 구성할 수 있다. 국내 기관에서 발행한 제로 트러스트 가이드 1.0 에서 제시한 6 가지 핵심 요소별 관리해야 할 IT 의 워크로드를 정의하면 <표 2>와 같다.

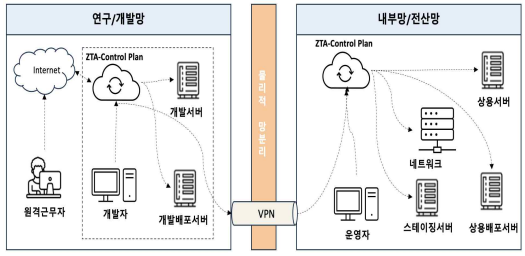
<표 2> 핵심 요소별 워크로드 정책

핵심 요소	정책
Identity & User	IT 그룹과 그 외 그룹 분류하고 그룹별 사용자 정의, 사용자 ID 와 다단계 등 2 차 인증 속성 정의
Device & Endpoint	사용자별 접속할 기기 MAC , 브라우저, SW, PORT 등록, NAC(Network Access Control), SDP Agent, EDR(Endpoint Detection and Response) 적용
Network	개발, 배포, 운영의 마이크로 세그먼트화
System	VPN 접속 허용 배포 서버 및 업무 단위별 그룹화 서버 목록정의
Application & Workload	SW 프로세스명, SW 크기, SW 계정과 그룹, 포트, 사용 자원 목록 정의, 배포/운영 대상 시스템과 계정, 망 연계 시간 지정
Data	책임 추적성을 위한 운영 로그 대상 목록화, 데이터베이스의 대상 목록을 정의, 실시간 접근 통제 이력 모니터링

핵심 요소의 워크로드별 정책은 지속적인 모니터링과 개선 그리고 정책 반영의 라이프사이클을 적용하여 보다 안전한 보안 체계를 유지할 수 있다. 제로 트러스트의 SDP 와 핵심 요소별 정책은 기업 내부적인 보안 심의와 비상계획 등에도 반영되어 관리되어야 한다.

4.2 망분리에서의 DevOps 개선 모델

제로 트러스트는 VPN 을 사용하지 않고 주요 리소스 접근을 인증과 접속 권한으로 통제하는 방식이다. 그러나 망분리 대상 규제는 VPN 을 통해 망분리 된 네트워크 간에 부분적인 접속을 허용하고 있어[4] 기존의 규제를 유지하면서 망분리를 완화할 수 있는 DevOps 환경을 제시하고자 한다. VPN 도 SDP Controller 와 SDP GateWay 가 관리해야 할 리소스의 하나이다. 망간 연계를 VPN 으로 연동함으로써 배포 시스템의 엑세스 설정을 특정 시스템으로 한정하여 배포 시스템을 구성한다면 최소한의 엑세스를 보장할 수 있다. (그림 5)와 같이 워크로드별 정의된 리소스에 대한 접근 인증, 권한을 부여함으로서 자동화된 형태의 배포 시스템을 활용하여 개발과 운영의 환경을 유지하며 편의성 및 보안성을 유지할 수 있다.



(그림 5) 제로 트러스트 모델을 적용한 DevOps 환경

제로 트러스트 보안 모델이 기존의 경계기반에 비해 강화된 보안을 제공한다고 하지만 망분리에 따른 보안 효율성도 고려해야 할 중요한 보안 요소이므로 규제를 준수하며 개발과 운영의 DevOps 체계를 유지할 수 있는 운영 환경을 제안한다. 또한 제로 트러스트의 보안 강화는 지속적인 모니터링과 개선된 보안 정책을 지속적으로 운영하여야 개선된 보안 체계를 유지 할 수 있다. 제안된 모델의 운영 절차를 살펴보면 IPSec VPN Lan To Lan 방식의 보안 터널링을 수행하여 망간 보안망을 구성한다. 배포 서버는 전산망의 스테이징 서버의 사설IP로 설정되어 배포 Target만 정의되어 있는 상태에서 개발자는 할당된 배포 서버의 접속 계정과 권한을 이용하여 배포 서버에 접속하여 배포를 수행하게 된다. 배포된 전산망 스테이징 서버 접속과 전산망 배포 서버 접속은 전산망 운영자에게 이미 할당된 서버와 접속 계정을 통해 테

스트 수행후 그 결과에 따라 운영 서버 배포 절차를 수행할 수 있는 운영 환경을 제공한다. 이러한 구조의 운영 환경은 개발자 및 운영자의 배포 주기 및 회수, 운영 시간을 주기적으로 모니터링 해야한다. ZTA 운영 로그와 배포 서버의 로그를 주기적으로 분석하여 VPN의 운영 시간, 배포 주기, 이상 접속, 권한 부여를 모니터링하고 워크로드 및 접속 권한 설정 범위를 통제 관리하여 보안 강화된 운영 환경을 제공할 수 있다. 이러한 개선 모델을 활용한 DevOps를 운영할 경우 소프트웨어 개발과 배포의 시간을 단축할 수 있고 IT 개발 환경의 개선에 도움이 될 것으로 생각한다.

5. 결론

핀테크 및 IT 산업이 지속적으로 발전하고 있으나 망분리 규제가 완화되지 않는다면 관련 산업은 더디게 발전할 수 있다[1]. 완화된 망분리 규제를 적용하더라도 스타트업이나 시장 진입을 원하는 기업은 망분리에 대한 투자와 개발자 모집에 어려움을 겪고 있고 이에 따라 한국 핀테크 산업에서도 망분리의 완화를 지속적으로 요구하고 있다. 현재 망분리의 기준은 업무 단위 또는 네트워크 접속 단위로 구성되어 있다. 그러나 실제 보호해야 할 중요한 것은 데이터일 것이다. 보호 데이터를 기준으로 망분리의 기준 변화 관리가 필요해 보인다. 데이터를 어떻게 보호하고 관리해야 하는지가 보안 강화를 위한 전략이 될 것이다. 데이터 중심의 보안 체계를 고려한다면 현재보다 완화된 보안 정책이 가능해 보인다[7]. 해외의 망분리 사례는 국내와 같은 규제가 존재하지 않는다[1]. 해외에서 처럼 망분리는 권고하되 이제는 침해사고의 피해가 발생할 경우 기업의 책임을 부여하여 기업 자체적으로 보안을 철저히 할 수 있는 기반 마련과 관련 산업의 발전이 필요하다[7]. 기업의 보안 의식은 규제 수준만 준수하면 된다는 생각이 강하다. 자발적 보안 체계를 고도화하거나 투자를 확대하지 않는다. 정보보안의 인식을 개선하려면 해외와 같이 보안 사고의 책임은 기업에 있다는 것을 명확히 하고 이에 대한 보안 규제의 변화가 필요하다. 본 논문에서는 워크로드별 분석과 정의를 통해 망분리 완화에서 DevOps 의 개선 모델과 운영 방안을 도출하였다. 워크로드기반에 IPSec VPN 을 적용하여 배포 관리와 지속적인 모니터링을 통해 운영 상태를 개선한다면 개발 환경 개선과 개발 생산성에 도움이 될 것이다. 또한 워크로드의 운영 관점과 더불어 제로 트러스트 핵심 요소 중 데이터를 중심으로 기업 리소스를 분류한 IT 인프라 및 망분리를 고려한다면 보안성, 편의성과 효율성을 제공하는 IT 환경이 될 것이다. 제로 트러스트 모델을 활용한 망 구성이나 제품에 대한 적용 사례가 많지 않고 기존의 온-프레미스의 보안 구성 변경에는 한계가 존재한다. 하지만 신규로 구성하는 인프라에 대하여는 제로 트러스트 모델을 적용하여 보안 체계를 변경하는 것을 고려해야 한다. 또한 기업에서는 망분리 완화에 따른 개발 환경에서 소스 코드의 유출 방지 및 보안 대책을 수립하여 소스 코드등 IT 자산이 안전하게 보호되도록 운영되어야 한다[20].

참고문헌

[1] 이경은, "국내 금융플랫폼 발전 현황과 규제 이슈", AI TREND WATCH, 제06권, 제1호, pp.1 - 9, 2022.

[2] Y.Na, J. Kim, N. Park, J. Won, and D. Lee, "A Study on the Effect of Network Separation Policy on the Development Environment of Fin tech Companies", Korean Telecommunic ations Policy Review, Vol. 29, No. 3, pp. 27 - 62, 2022.

[3] EBN 산업경제, '연구ㅇ개발 목적 금융권 망분리 예외 허용된다', https://ebn.co.kr/news/view/1556111, 2023.

[4] 금융위원회, '[보도자료] 클라우드 이용절차 합리화및 망분리 규제 완화를 위한 전자금융감독규정 개정안 금융위 의결 - 클라우드 및 망분리 규제 개선 방안('22.4.) 관련 -', https://www.fsc.go.kr/po010102/78962?srchCtgry=&curPage=28&srchKey=&srchText=&srchBeginDt=&srchEndDt =, 2022.

[5] J. Oh and H. Lee, "Improvement Measures of Network Separation Regulation to Activate the Digital Finance Industry," Jouranl of Information and Security, Vol. 21, No. 5, pp. 51 - 60, 2021.
[6] 머니투데이, '핀테크 발목잡는 '망분리' 뭐길래…" 비용만 5억원, 혁신 망친다', https://news.mt.co.kr/mtview.php?no=2021092916243334272, 2023.
[7] 인포스탁데일리, '[기획]비현실적 '망분리 규제 데이터 중심 망분리' 정책으로 전환해야', https://www.infostockdaily.co.kr/news/articleView.html?idxno=144210, 2023.
[8] 전자신문, '[스페셜리포트]망분리 규제 '시대착오적' vs '대안은 있나'', https://www.etnews.com/20231024000193, 2023.
[9] 파비리서치, '망분리 '규제 완화' 띄웠지만, 핀테크 업계 '망분리 규제 자체가 시대착오적'', https://research.pabii.com/policykorea/273954/, 2023.
[10] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, 'Zero Trust Architecture' Gaithersburg, MD, 2020.
[11] 박춘식, "제로 트러스트 아키텍처", 정보보호학회지, 제33권, 제4호, pp. 131 - 141, 2023.
[12] J. R. BIDEN JR., 'Executive Order 14028-Improving the Nation's Cybersecurity', Daily Compilation of Presidential Documents, 2021.
[13] 이석준, "제로트러스트, 보안 패러다임의 전환", 정보와 통신, 제40권, 제9호, pp. 3 - 10, 2023.
[14] 과학기술정통부, 한국인터넷진흥원, 한국제로트러스트포럼, '제로트러스트 가이드 1.0 전체본 (230714)', 2023.
[15] 윤혜정, 이용우, 임효정, 전삼현, "재택근무 환경 개선을 위한 제로 트러스트 추진 동향 및 실효성 제고 방안 연구", 한국IT정책경영학회 논문지, 제14권, 제2호, pp. 2915 - 2921, 2022.
[16] 데이터넷, '[CSA SDP 아키텍처 가이드] 급변하는 환경 효과적 보호 방안 제시', https://www.datanet.co.kr/news/articleView.html?idxno=162895, 2023.
[17] J. Garbis et al., 'Software-Defined Perimeter Architecture Guide 2.0', 2019.
[18] Neil MacDonald, Lawrence Orans, Joe Skorupa, 'SDP Specification 1.0', 2014.
[19] 주승현, 김진민, 권대현, 신용태, "제로 트러스트 아키텍처 도입을 통한 기업 보안 강화 방안 - 마이크로 세그먼테이션 접근법 중심으로 -", 융합보안논문지, 제23권, 제3호, pp. 3 - 11, 2023.
[20] 금융보안원, '금융분야 클라우드컴퓨팅서비스 이용 가이드', 2023.

〔저자소개〕

한 봉 용 (Bong-Yong Han)
2017년 건국대학교 공학석사
2023년 숭실대학교 IT정책경영학과 박사과정
2023년 갤럭시아머니트리(주) 상무
email : hanby49@naver.com

최 영 근 (Young-Kun Choi)
1997년 한양대학교 산업공학 석사
2023년 숭실대학교 IT정책경영학 박사과정
2023년 (사)한국산업기술융합원 보안정책연구소 소장
email : pdwall@naver.com

소 가 연 (Ga-Yeon So)
2003년 전북대학교 법학 석사
2023년 숭실대학교 IT정책경영학과 박사과정
2023년 ㈜큐앤에이네트웍스 CEO
email : sky@qnanetworks.co.kr

신 용 태 (Yong-Tae Shin)
1985년 한양대학교 산업공학 학사
1990년 Univ. of lowa 컴퓨터학 석사
1994년 Univ. of lowa 컴퓨터학 박사
1995년 숭실대학교 컴퓨터학부 교수
email : shin@ssu.ac.kr