https://doi.org/10.33778/kcsa.2023.23.4.131

한국군 맞춤형 제로 트러스트(Zero Trust) 구축방안 연구★

신 규 용*, 길 총 경**, 최 경 식***, 김 용 철****

요 약

최근 내부자에 의한 국방망 침해사고가 빈번하게 발생하고 있다. 이러한 추세는 현재 우리 국방부가 고수하고 있는 물리적 망 분리정책이 더 이상 안전을 보장할 수 없다는 반증이라 할 수 있다. 따라서 보다 강력한 사이버보안 대책이 필요하다. 이와 관련해 '절대 신뢰하지 말고, 항상 검증하라'는 제로 트러스트가 새로운 보안의 패러다임으로 등장하고 있다. 본 논문은 미 국방부에서 현재 추진중에 있는 제로 트러스트 구축 동향을 분석하고, 이를 통해 도출된 시사점을 바탕으로 한국군 맞춤형 제로 트러스트 구축방안을 제안한다. 본 논문이 제안하는 한국군 맞춤형 제로 트러스트 구축방안은 한국군 맞춤형 제로 트러스트 구축전략, 전담조직 편성 및 예산 확보방안, 제로 트러스트 구축기술 확보방안 등을 포함하고 있다. 본 논문에서 제안하는 한국군 맞춤형 제로 트러스트는 기존의 물리적 망 분리 정책에 기반한 사이버보안과 비교해 보안적인 측면에서 다양한 장점을 갖는다.

A Study on Zero Trust Establishment Plan for Korean Military

Kyuyong Shin*, Chongkyung Kil**, Keungsik Choi***, Yongchul Kim****

ABSTRACT

In recent years, there have been frequent incidents of invasion of national defense networks by insiders. This trend can be said to disprove that the physical network separation policy currently applied by the Korea Ministry of National Defense can no longer guarantee military cyber security. Therefore, stronger cybersecurity measures are needed. In this regard, Zero Trust with a philosophy of never trusting and always verifying is emerging as a new alternative security paradigm. This paper analyzes the zero trust establishment trends currently being pursued by the US Department of Defense, and based on the implications derived from this, proposes a zero trust establishment plan tailored to the Korean military. The zero trust establishment plan tailored to the Korean military proposed in this paper includes a zero trust establishment strategy, a plan to organize a dedicated organization and secure budget, and a plan to secure zero trust establishment technology. Compared to cyber security based on the existing physical network separation policy, it has several advantages in terms of cyber security.

Key words : Cyber Security, Zero Trust, Military Zero Trust, Zero Trust Strategy, Zero Trust Plan

접수일(2023년 08월 25일), 수정일(2023년 09월 07일), 게재확정일(2023년 09월 27일)

★ 본 논문은 육군사관학교 화랑대연구소의 2023년도 연구활동비 지원을 받아 연구되었음.(연구번호: 2023B1008).

* 육군사관학교 컴퓨터과학과(주저자)

** ㈜씨더블유리서치(공동저자)

*** 사이버작전사령부(공동저자)

**** 육군사관학교 전자공학과(교신저자)

1. 서 론

2010년 제로 트러스트라는 개념을 창안한 존 킨더바그는 최근 미 국방부가 주최한 심포지엄에서 제로 트러스트가 향후 사이버보안을 위한 유일한 전략이 될 것이며 사이버 전쟁을 승리로 이끄는 열쇠가 될 것이라고 강조하였다[1].

이와 관련해 최근 미국, 영국 등 주요 선진국들은 제로 트러스트 구축을 위해 국가 정책을 발표하고 관련된 기술을 개발하여 전략적 우위를 선점하기 위해 노력하고 있다. 특히 미국의 경우 바이든 대통령이 2021년 행정명령(Executive Order on Improving the Nation's Cybersecurity 10428)으로 제로 트러스트 보안을 채택하게 하였고, 미 국방부는 2022년 국방 제로 트러스트 전략과 로드맵을 발표하였다[2, 3]. 해당 로드맵에 따르면 미군은 2027년까지 제로 트러스트 환경을 구축하는 것으로 되어 있으며 이미 이를 위한 실행에 착수했다. 또한, 구글이나 마이크로소프트와 같은 해외 유수의 기업들은 물론이고 국내 기업들도 앞다투어 제로 트러스트를 반영하고 있다[4, 5]. 이러한 점에 비추어 볼 때 향후 우리 군도 제로 트러스트 적용이 필수 불가결할 것으로 예상된다.

따라서 본 논문은 네트워크 경계 중심의 보안에서 사용자와 자산 그리고 리소스(resource) 중심의 새로운 보안 패러다임인 제로 트러스트로의 전환에 대응하기 위해 한국군 맞춤형 제로 트러스트 구축방안을 제안한다. 이를 위해 본 논문은 제로 트러스트 분야의 명실상부한 퍼스트 무버(first mover)라 할 수 있는 미 국방부의 사례를 벤치마킹함으로써 한국군에 적합한 제로 트러스트를 구축하는 패스트 팔로어(fast follower) 전략을 추구하고자 한다. 따라서 본 논문은 먼저 미 국방부에서 발간한 제로 트러스트 추진 전략과 제로 트러스트 이행을 위한 로드맵을 면밀하게 분석하고, 미 국방부의 제로 트러스트 추진 최신 동향을 살펴본다. 또한, 미 국방부의 제로 트러스트 구축 최신 동향에서 도출된 시사점을 바탕으로 한국 국방 현실에 맞는 한국군 맞춤형 제로 트러스트 구축방안을 제시한다. 이때 한국군 맞춤형 제로 트러스트 구축방안은 한국군에 특화된 제로 트러스트 구축전략, 한국군 맞춤형 제로 트러스트 구축을 위한 전담조직 및 예산 확보방안, 그리고 국방 제로 트러스트 기술 확보방안 등을 포함한다.

본 논문의 구성은 다음과 같다. 2장에서는 이 분야에 생소한 독자들을 위해 제로 트러스트의 개념에 대해서 설명한다. 3장에서는 미 국방부의 제로 트러스트 구축 동향을 살펴보고, 4장에서는 3장에서 도출된 시사점을 바탕으로 한국군 맞춤형 제로 트러스트 구축방안을 제안한다. 마지막으로 5장에서는 본 논문의 결론을 맺고 향후 연구 방향을 제시한다.

2. 제로 트러스트(Zero Trust)의 개념

지금까지 대부분의 조직 및 기관은 사용자를 내부자와 외부자로 구분하고, 내부자와 외부자에 대해 서로 다른 신뢰도를 설정하는 소위 네트워크 중심의 보안경계(security perimeter) 개념을 적용해왔다. 우리 국방부도 인터넷과 인트라넷(국방망)을 물리적으로 구분하는 강력한 망 분리 정책을 적용해오고 있다. 하지만 최근 연구결과에 따르면 이러한 물리적 망 분리 정책이 각종 보안 공격으로부터 안전하지 않다는 것을 보여주고 있다[6]. 따라서 최근에는 네트워크 내·외부를 막론하고 사용자와 단말을 신뢰하지 않는 제로 트러스트(Zero Trust) 개념이 부각되고 있다[7].

제로 트러스트라는 개념의 출현은 4차 산업혁명의 시대에서 디지털 자산이 국가의 부를 창출하는 핵심 동력임과 동시에 국가 간 경쟁을 촉발한다는 점에서 중요한 변곡점이 되고 있다. 이는 제로 트러스트의 실질적이고 효과적인 범국가적 정책과 전략적 구현이 곧 보이지 않는 데이터 전쟁에서 선제적 우위를 차지하게 된다는 의미를 내포하는 것이다.

미국 국립표준기술연구소(NIST)는 제로 트러스트를 새로운 보안 모델로 제시하며 기존의 네트워크 경계(perimeter) 중심 보안에서 사용자와 자산 그리고 리소스(resource) 중심 보안으로 보안 패러다임의 전환에 대한 필요성을 강조하였으며, 바이든 정부는 2024년까지 범정부적으로 제로 트러스트를 구축하기 위해 노력을 집중하고 있다[8].

제로 트러스트 구현의 핵심은 디지털 자산과 리소스(resource)에 대한 보호를 통해 아군(我軍) 데이터에 대한 신뢰도, 안정성, 활용성을 보장하는 것이다. 이를

위해 디지털 자산과 리소스(resource)에 접근하는 사용자를 얼마나 효과적·효율적으로 지속적인 검증을 할 수 있는지가 제로 트러스트 도입 및 구축에 있어 가장 중요한 핵심요인이라고 할 수 있다.

3. 미 국방부의 제로 트러스트 구축 동향

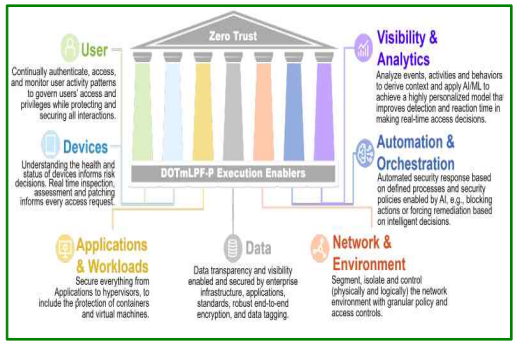
이번 장에서는 제로 트러스트 구축 관련 퍼스트 무버(first mover)라 할 수 있는 미군의 제로 트러스트 구축 동향을 살펴본다. 이를 위해 먼저 미 국방부의 제로 트러스트 전략과 제로 트러스트 이행을 위한 로드맵을 면밀하게 분석하고, 제로 트러스트 추진과 관련된 최신 동향을 살펴본다. 이때 제로 트러스트 추진을 위한 미 국방부의 전담조직 및 예산 편성 현황은 4장 한국군 맞춤형 제로 트러스트 구축방안과 연계하여 분석한다.

3.1 미 국방부 제로 트러스트 전략

미 국방부는 고도화되는 사이버 위협에 대비하기 위해 2022년 11월에 제로 트러스트를 새로운 보안 모델로 선정하였으며, 2027년까지 이를 이행하기 위한 전략을 발표하였다[2]. 미 국방부의 제로 트러스트 전략은 4개의 전략 목표와 이를 구축하기 위한 7개의 기둥(pillar)으로 요약할 수 있다.

먼저, 미 국방부의 제로 트러스트 전략적 목표 4가지는 다음과 같다. ① 제로 트러스트 문화 채택 : 모든 국방부(DoD) 직원은 제로 트러스트 중심의 사고방식과 문화를 인식하고 이해하며 교육을 받는다. ② 국방부(DoD) 정보 시스템 보안 및 방어 : 레거시 시스템(legacy system)을 포함한 모든 DoD 시스템에 제로 트러스트를 통합하고 운영한다. ③ 기술 가속화 : 기술 발전을 산업계의 발전과 같거나 그 이상으로 추월한다. ④ 제로 트러스트 활성화 : 모든 부서 및 구성 요소 수준에서 프로세스, 정책, 예산 지원을 제로 트러스트 원칙과 일치시킨다.

다음으로 제로 트러스트 시행을 위한 7개의 기둥은 (그림 1)에서 보는 바와 같이 제로 트러스트 기반을 구축하는 것으로 사용자(User), 장치(Device), 애플리케이션과 워크로드(Applications & Workloads), 데이터(Data), 네트워크와 환경(Network & Environment), 자동화와 오케스트레이션(Automation & Orchestration), 가시화와 분석(Visibility & Analytics) 등으로 구성된다[2].



(그림 1) US DoD Zero Trust 7 Pillars [2]

7개의 기둥은 NIST가 제시한 7 Tenets for Zero Trust를 미 국방부의 사이버공간 환경에 적용한 것이라 볼 수 있는데 그 세부 내용은 다음과 같다. ① 사용자(user) 측면에서는 개인 및 엔티티들의 액세스에 대해 강력히 그리고 지속적으로 인증을 시행한다. ② 장치(Device) 측면에서는 실시간으로 모든 장치에 대해 식별, 승인, 인증 및 패치를 실시한다. ③ 애플리케이션과 워크로드(Applications & Workloads) 측면에서는 컨테이너 및 가상 머신(virtual machine) 보호를 포함하여 모든 애플리케이션 및 워크로드를 보호한다. ④ 데이터(Data) 측면에서는 엔터프라이즈 인프라, 애플리케이션, 표준, 강력한 종단 간 암호화 및 데이터 태깅 등을 통해 데이터의 투명성과 가시성을 활성화하고 보호한다. ⑤ 네트워크와 환경(Network & Environment) 측면에서는 세분화된 액세스 및 정책 제한을 통해 (논리적 및 물리적) 네트워크 환경을 분할, 격리, 제어한다. ⑥ 자동화와 오케스트레이션(Automation & Orchestration) 측면에서는 수동 보안 및 기타 적용 가능한 프로세스를 자동화하여 속도와 규모에 따라 전사적 정책기반을 조성한다. ⑦ 가시화와 분석(Visibility & Analytics) 측면에서는 각종 이벤트, 활동, 동작 등을 면밀하게 분석하여 컨텍스트(context)를 도출하고, 인공지능 및 머신러닝(AI/ML) 기술을 적용하여 실시간으로 액세스 여부를 결정한다. 미 국방부는 각 기둥들 내의 모든 기능은 중심 기둥인

데이터(Data) 기둥을 효과적으로 보호하기 위해 통합된 방식으로 함께 작동해야 함을 강조하고 있다. 이를 통해 우리는 향후 데이터 보호가 사이버보안 모델의 핵심임을 미루어 짐작할 수 있다.

3.2 제로 트러스트 이행을 위한 로드맵

다음은 제로 트러스트 이행을 위한 로드맵으로 미 국방부는 (표 1)에서 보는 바와 같이 제로 트러스트 전략 목표를 달성하기 위해 갖추어야 할 요구능력(Zero Trust Capabilities)을 총 45개로 세분화하였다. 또한, <표 1>에서 보는 바와 같이 요구능력별로 고급 수준까지(Advanced Level) 도달해야 할 시기를 제시하고 있다[3].

<표 1> DoD Zero Trust Capabilities

기둥	요구능력	달성연도
사용자	User Inventory	2025
	Conditional User Access	2031
	Multi-factor Authentication	2030
	Privileged Access Management	2029
	Identify Federation & User Credentialing	2028
	Behavioral, Contextual ID, and Biometrics	2028
	Least Privileged Access	2024
	Continuous Authentication	2030
	Integrated ICAM Platform	2030
장치	Device Inventory	2029
	Device Detection and Compliance	2029
	Device Authorization, Real Time Inspection	2030
	Remote Access	2031
	Partially & Fully Automated Asset, Vulnerability and Patch Management	2025
	Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	2025
	Endpoint & Extended Detection & Response (EDR & XDR)	2028
애플리케이션 과 워크로드	Application Inventory	2027
	Secure Software Development & Integration	2029
	Software Risk Management	2025
	Resource Authorization & Integration	2027
	Continuous Monitoring and On going Authorizations	2029
데이터	Data Catalog Risk Alignment	2024
	DoD Enterprise Data Governance	2024
	Data Labeling and Tagging	2031
	Data Monitoring and Sensing	2030
	Data Encryption & Rights Management	2031
	Data Loss Prevention (DLP)	2032
	Data Access Control	2029
네트워크	Data Flow Mapping	2024
	Software Defined Networking	2031
	Macro Segmentation	2026
	Micro Segmentation	2029
자동화 및 오케스트레이션	Policy Decision Point (PDP) & Policy Orchestration	2027
	Critical Process Automation	2027
	Machine Learning	2025
	Artificial Intelligence	2030
	Security Orchestration, Automation & Response (SOAR)	2030
	API Standardization	2025
	Security Operation Center (SOC) & Incident Response	2030
가시성 및 분석	Log All Traffic (Network, Data, Apps, Users)	2025
	Security Information and Event Management (SIEM)	2029
	Common Security and Risk Analytics	2026
	User and Entity Behavior Analytics (UEBA)	2028
	Threat Intelligence Integration	2026
	Automated Dynamic Policies	2032

미 국방부는 (표 1)에서 제시한 45개의 요구능력에 대해 대부분 2027년 이내에 목표 수준까지(Target Level) 달성하는 것을 중기 목표로 추진하고 있다. 나아가 인공지능(AI) 기술 등을 접목한 인프라를 확보하여 앞서 제시한 요구능력을 2032년까지 고급 수준(Advanced Level)으로 끌어올리고, 지속적으로 향상시키는 것을 장기 목표로 설정하고 있다. 미 국방부는 이와 같은 행동지침을 통해 (Course of Action) 제로 트러스트 로드맵을 구체화하였다.

3.3 제로 트러스트 추진 최신 동향

미 국방부는 제로 트러스트 추진을 위한 전담조직으로 22년 1월에 국방부(DoD) 최고정보책임자(CIO) 산하에 제로 트러스트 포트폴리오 관리 사무소(Zero

Trust Portfolio Management Office, ZT PfMO)를 신설하였다. 제로 트러스트 포트폴리오 관리 사무소(ZT PfMO)는 제로 트러스트의 구축을 위해서는 기반기술 개발도 중요하지만 조직의 문화를 바꾸는 것이 선행되어야 한다고 판단하였다. 따라서 제로 트러스트로의 인식 전환을 위한 콘텐츠를 개발하여 국방획득대학 등에서 제로 트로스트 인식과정(Zero Trust Awareness Course) 등 다양한 과정을 개설하여 기초부터 실무수준에 이르는 교육 훈련을 실시하고 있다.

제로 트러스트 포트폴리오 관리 사무소(ZT PfMO)는 2023년부터 제로 트러스트 전략의 실행에 착수하였고, 5월에는 기존 요구능력을 91개로 세분화시켰으며, 매 분기 150명이 넘는 관계자가 참석하는 회의를 통해 미 국방부의 전반적인 제로 트러스트 추진상태를 점검하고 있다. 제로 트러스트 포트폴리오 관리 사무소(ZT PfMO)의 책임자는 아마존, 구글 등의 민간기업과의 협력을 통해 합동 전투 클라우드 기능(Joint Warfighting Cloud Capability)에 제로 트러스트 적용이 가능할 것으로 관망하였으며, 올해 10월에는 국방부 제로 트러스트 실행 계획(DoD ZT Implementation Plan)을 발표할 예정이라고 밝혔다[1].

미 육군은 육군사이버사령부 예하에 육군 제로 트러스트 기능 관리 사무소(Army ZT Functional Management Office, A-FMO ZT)를 신설하여 제로 트러스트를 추진하고 있다[9]. 미 육군의 경우 제로 트러스트 구축의 최종 상태를 6가지로 정의하여 추진하고 있는 것이 특징인데 이를 살펴보면 ① 데이터 중심의 제로 트러스트 아키텍처(A data-centric ZTA), ② 하이브리드 클라우드 리소스 호스팅(Hybrid cloud resource hosting), ③ 리소스에 대한 중개 액세스 및 인터넷 액세스 제어를 위한 서비스 에지(A service edge for brokered access to resources and control of internet access), ④ 클라우드 기반의 인터넷 액세스가 가능한 통합 엔드 포인트 및 보안 관리(Cloud-based, internet-accessible unified endpoint and security management), ⑤ 인터넷에 액세스할 수 있는 ID 공급자(An internet accessible identity provider), ⑥ 로깅, 분석 및 자동 응답(Logging, analytics and automated response) 등이다[9].

4. 한국군 맞춤형 제로 트러스트 구축방안

이번 장에서는 앞서 3장에도 도출된 시사점을 바탕으로 한국군 맞춤형 제로 트러스트 구축전략을 제시하고, 제로 트러스트 전담조직 편성방안과 예산 확보방안을 제안한다. 이때 제로 트러스트 추진 전담조직 및 예산은 미 국방부의 사례에 비추어 패스트 팔로워(fast follower)가 되기 위한 방안을 제안한다. 또한, 한국군 맞춤형 제로 트러스트를 구축하는데 필요한 기술 확보 방안을 모색하고, 마지막으로 한국군 맞춤형 제로 트러스트를 구축했을 때의 장점에 대해 논의한다.

4.1 한국군 맞춤형 제로 트러스트 구축전략

2023년 6월 우리 정부는 「제로 트러스트 가이드라인 1.0」[10]을 발표했다. 정부의 제로 트러스트 가이드라인은 제로 트러스트 개요, 제로 트러스트 아키텍처 보안 모델, 제로 트러스트 도입 절차, 그리고 제로 트러스트 구현 유즈 케이스 등을 포함하고 있다. 특히 해당 가이드라인은 인증 체계 강화, 마이크로 세그멘테이션(Micro-Segmentation), 네트워크 인프라 및 소프트웨어 정의 경계(Software Defined Perimeter, SDP) 등의 제로 트러스트 아키텍처 구축을 위한 접근 방법을 제안하고 있다.

또한, 정부의 제로 트러스트 가이드라인은 기존의 국가 기반시설 보안정책 등을 고려하여 국내 환경에 적합한 핵심요소 6가지와 교차기능 2가지를 제시하고 있다. 이때, 핵심요소 6가지는 다음과 같다. ① 식별자·신원(Identity)은 사람, 서비스 혹은 사물인터넷(Internet of Things, IoT) 기기 등을 고유하게 설명할 수 있는 속성 혹은 속성의 집합이다. ② 기기 및 엔드포인트(Device/Endpoint)는 IoT 기기, 핸드폰, PC, 서버 등을 포함해 네트워크를 통해 데이터를 주고받는 모든 하드웨어 장치이다. ③ 네트워크(Network)는 유선, 무선, 클라우드 접속을 포함하는 모든 형태의 통신 매체를 의미한다. ④ 시스템(Systems)은 중요 프로그램을 구동하거나 중요 데이터를 저장·관리하는 서버들을 일컫는다. ⑤ 응용 및 워크로드(Application & Workload)는 기업망 관리 시스템, 프로그램, 다양한 환경에서 실행되는 각종 서비스를 총칭한다. 마지막으로 ⑥ 데이터(Data)는 기업·기관에서 가장 우선으로

보호해야 할 자원을 의미한다. 또한, 위 6가지 핵심요소들에 대한 보안성과 신뢰도를 강화하고 세밀한 접근제어가 가능하도록 가시성 및 분석(Visibility and Analytics)과 자동화 및 통합(Automation and Orchestration) 등의 교차기능이 모든 핵심요소에 아우러져 구현되어야 한다고 제안하고 있다.

정부의 가이드라인에 맞춰 우리 군도 국방 사이버공간의 특성을 고려한 제로 트러스트 구축전략을 수립해야 한다. 현재 강력한 망 분리 정책에 기반한 우리 군의 보안 모델은 내부자 공모, 권한탈취 후 횡적 이동, 비인가자의 기밀 데이터 우회 접근 등 진화하는 사이버 위협에 대응하기 어려운 것이 현실이다. 따라서 고도화되는 사이버 위협에 대비하기 위해 제로 트러스트 구축전략과 실현 계획을 수립하는 것이 시급하다. 즉, 망 분리와 보안경계(Security Perimeter) 중심의 보안정책에서 과감히 탈피하고, 동적 인증, 지속적 모니터링, 데이터 중심의 제로 트러스트 보안 전략을 구상해야 한다. 하지만 제로 트러스트 구축은 상당한 예산과 자원이 투입되어야 한다. 따라서 데이터 접근제어, 다중 인증, 중요 사이버 자산 가시화, 국방분산인증 모델[6] 개발 등 예산 투입 대비 효율성이 높은 분야부터 식별하여 추진하는 한국군 맞춤형 전략 수립이 필요하다.

4.2 제로 트러스트 전담조직과 예산확보 방안

한국형 맞춤형 제로 트러스트를 구축하기 위해서는 이를 전담할 조직과 예산확보가 필수적이다. 먼저 한국형 맞춤형 제로 트러스트 구축을 위한 전담조직을 신설해야 한다. 미 국방부는 2020년 제로 트러스트 도입을 위해 DISA, NSA DoD CIO, US Cyber Command 등 다양한 기관이 참여하는 합동 제로 트러스트 엔지니어링 팀(Joint Zero Trust Engineering Team)을 편성하였으며, 이후 2년여간의 노력으로 2022년 6월에 국방 제로 트러스트 레퍼런스 아키텍쳐를 마련했다. 이와 병행하여 미 국방부 예하 각 군은 제로 트러스트 추진을 위한 자체 전담조직을 신설하여 군별 특성에 맞는 계획을 발전 및 추진 중이다. 미 국방부의 제로 트러스트 레퍼런스 아키텍처는 범세계 정보격자망(Global Information Grid, GIG) 기반하에 구상되었다. 하지만 제로 트러스트 레퍼런스 아키텍처를 한국군 환경에 바로 적용하기는 제한될 것이다.

따라서 한국군 맞춤형 제로 트러스트 구축을 위한 모델과 핵심 기술 개발이 자체적으로 이루어져야 한다. 하지만 현재 우리 군은 제로 트러스트 추진 조직이 전무한 실정이다. 이러한 문제를 해결하기 위해서는 국방부 첨단전력기획관실 예하에 가칭 '제로 트러스트 추진팀' 신설하여 한국군 맞춤형 제로 트러스트 구축을 전담하여야 한다. 이때, 신설되는 제로 트러스트 추진팀에는 국방부 지능정보화정책관실, 합참 사이버작전과, 사이버작전사령부, 각군 사이버작전센터, 방첩사령부, 지휘통신사령부 등 관계 기관이 함께 참여하여 우리 군의 작전환경에 적합한 제로 트러스트 정책과 전략을 수립하고, 국방 제로 트러스트 성숙도 모델을 공동으로 개발할 필요가 있다.

다음으로 한국형 맞춤형 제로 트러스트 구축을 위한 예산확보가 필요하다. 2023년 미 국방부 CIO 예산 편성을 살펴보면 제로 트러스트 임무 수행을 위한 지원 예산으로 3백만 달러를 편성하였으며[11], 미 육군은 2024년 제로 트러스트 추진 예산으로 4.3조 달러($439 Billion)를 편성하였다. 이외에도 클라우드 전환 및 디지털 환경조성에 4.7천억 달러, 자동화툴 등 개발에 3.3천억 달러, 데이터 플랫폼 개발에 1.3천억 달러 편성을 요구했다[12]. 이처럼 제로 트러스트 구축을 위해서는 상당한 예산이 요구된다.

이러한 측면을 고려해볼 때 우리도 한국군 맞춤형 제로 트러스트를 구축하기 위해서는 예산확보가 필수적이다. 이에 본 논문에서 제안하는 예산확보 방안은 다음과 같다. 첫 번째 예산확보 방안은 정상적으로 국방부 자체 중기계획에 반영하는 것이다. 하지만 국방부 자체 중기계획을 통한 사업추진의 경우 올해 기준으로 26~30 국방 중기계획에 반영하더라도 예산을 확보하기까지는 최소 3년 이상을 기다려야 하는 문제가 있다. 두 번째 예산확보 방안은 국방 ICT R&D 예산을 활용하는 방안이다. 국방부와 과기정통부는 2021년 국방 전 분야에 디지털 전환을 촉진하고 민간의 테스트베드 역할을 통한 디지털 혁신 마중물 역할을 강화하기 위해 국방 ICT R&D 전담 지원조직을 신설해 예산을 지원하고 있다. 따라서 국방 ICT R&D 예산확보를 통해 한국군 맞춤형 제로 트러스트 구축사업을 추진할 수 있다. 하지만 국방 ICT R&D 예산의 경우 지금 예산확보를 추진하더라도 2026년에나 예산확보가

가능하다. 세 번째 예산확보 방안은 2025 국방 U-실험사업에 지원하는 방안이다. 국방부는 '네트워크 중심의 국방 지식 정보화'라는 비전 아래 전장관리 및 국방경영과 관련한 민간의 발달된 첨단 정보통신(IT) 기술의 국방도입으로 국방력을 강화하기 위하여 국방 U-실험사업을 추진하고 있다. 현 시점에서는 이미 2024년도 사업선정이 완료되었기 때문에 2024년 초에 한국군 맞춤형 제로 트러스트를 구축사업으로 지원한다면 2025년부터 사업추진이 가능할 것이다. 마지막으로 네 번째 예산확보 방안은 2023년 국방 불용예산을 활용하는 방안이다. 즉, 국방부 차원에서 2023년도 연도예산으로 반영했던 사업들 중에서 불가피하게 사용하지 못한 예산을 활용해 후반기부터 사업을 추진하는 것이다. 하지만 불용예산의 경우 연도이월이 불가능하기 때문에 연말까지 사업을 종료해야 하는 문제가 있다. 이와 같이 다양한 예산확보 방안을 고려해 한국군 맞춤형 제로 트러스트 구축사업을 세분화한 뒤 항목별로 2023년 후반기 불용예산, 2025년 국방 U-실험사업, 2026년 국방 ICT R&D 예산, 그리고 26~30 국방 중기계획 등에 반영하여 확보할 필요가 있다.

4.3 국방 제로 트러스트 기술 확보방안

한국군 맞춤형 제로 트러스트를 구축하기 위해서는 SDN(Software Defined Network), SASE(Secure Access Service Edge), ZTNA(Zero Trust Network Access), SOAR (Security Orchestration, Automation and Response) 등과 같은 제로 트러스트 관련 기술을 확보하고 기술성숙도를 향상시켜야 한다[13].

현재 국내의 제로 트러스트 기술성숙도는 매우 낮은 실정이다. SDN, SASE, ZTNA, SOAR 등 제로 트러스트 솔루션을 공급하는 업체는 대부분 구글, 마이크로소프트, 멘로시큐리티 등 해외 보안기업이며 국내의 경우 소프트 캠프, 지니언스, 파수 등의 국내 보안기업들이 그 뒤를 따르고 있다. 이런 시점에서 군에서 제로 트러스트 구축기술을 직접 개발하여 활용하는 것은 매우 제한적일 수밖에 없다. 따라서 현시점에서는 강력한 스핀 온(Spin-On) 전략을 추구하는 것이 바람직하다고 판단된다. 또한, 민간에서 개발되어 활용되고 있는 제로 트러스트 구축기술을 군의 환경에 맞게 재활용하는 스핀 온(Spin-On) 전략을 추진하기 위해서는 원활한 민군협력이 필요하다. 이때 군은 지속적인 투자와 더불어 중장기 가이드라인을 제시하고, 국내 보안기업들이 제로 트러스트 기술을 자체 개발할 수 있는 역량을 확보하도록 지원하며, 다양한 군내·외 실증 사업 수행을 통해 그 결과를 공유하여 기술성숙도를 높이는 전략이 필요하다.

국방 제로 트러스트 기술확보 시 추가로 고려해야 하는 사항은 레거시 시스템(legacy system)에 대한 기술적 극복방안이다. 우리 군이 운용 중인 네트워크와 시스템은 다양한 레거시 시스템(legacy system)을 보유하고 있어 제로 트러스트 도입에 난제로 부각될 수 있다. 따라서 다양한 국방 레거시 시스템(legacy system)에 제로 트러스트를 적용할 수 있는 래핑(wrapping) 기술을 확보해야만 실질적 제로 트러스트 구현이 가능해질 것이다.

국방 제로 트러스트 기술과 관련해서 또 다른 고려사항으로 기존의 보안정책으로부터의 과감한 탈피가 필요하다. 앞서 설명했듯이 우리 국방부는 인터넷과 인트라넷(국방망)을 물리적으로 구분하는 강력한 망분리 정책을 고수하고 있다. 하지만 한국군 맞춤형 제로 트러스트를 구축하기 위해서는 강력한 물리적 망분리에 의존하는 기존 보안정책에서 과감히 벗어나야 한다. 이와 관련해 현재 국방망과 인터넷망으로 구분하여 운용하고 있는 국방클라우드 운용의 한계점을 제로 트러스트 기반으로 극복하는 방안을 검토하여야 한다. 특히, 국방 인공지능(AI) 기술의 발전을 위해서는 데이터 확보, 축적, 자동화된 분석 기술이 매우 중요한데 현재의 국방클라우드 환경에서는 데이터 축적이 제한적일 수밖에 없다. 이러한 상황을 극복하기 위해서는 국방 클라우드를 인터넷 기반으로 과감히 전환하고, 한국군 맞춤형 제로 트러스트를 적용해야 한다. 즉, 인터넷 기반의 국방클라우드를 운용하되 한국군 맞춤형 제로 트러스트 하에서 민감한 자료는 프라이빗 클라우드에 저장하고, 일반 자료는 퍼블릭 클라우드에 저장해 활용하는 하이브리드 방식의 국방 클라우드 인프라를 구축해 활용하는 방안을 고려해야 한다.

4.4 한국군 맞춤형 제로 트러스트 장점

4장에서 우리는 한국군 맞춤형 제로 트러스트 구축 전략을 제시하였고, 제로 트러스트 전담조직 편성방안

과 예산 확보방안을 제안하였으며, 한국군 맞춤형 제로 트러스트 구축기술 확보방안을 모색하였다. 만일 본 논문에서 제안한 한국군 맞춤형 제로 트러스트를 구축한다면 기존의 물리적인 망 분리 정책과 비교하여 보안적인 측면에서 <표 2>에서 보는 바와 같은 다양한 장점을 가진다.

<표 2> 한국군 맞춤형 제로 트러스트 장점

구 분	망 분리	제로 트러스트
내부자에 의한 공모 및 침해 방지 확률	낮음(▼)	높음(▲)
불법적 데이터 접근 식별/차단 확률	낮음(▼)	높음(▲)
무기체계 및 단말기 신뢰 검증 확률	낮음(▼)	높음(▲)
랜섬웨어 유입 및 확산 차단 확률	보통(□)	높음(▲)
악성코드 감염 및 확산 방지 확률	보통(□)	높음(▲)

즉, <표 2>에서 보듯이 한국군 맞춤형 제로 트러스트가 구축되면 제로 트러스트 성숙도 모델[14]의 최상위(optimal) 단계에 도달할 수 있으므로 사용자, 장치, 네트워크, 어플리케이션과 워크로드, 데이터 측면에서 자동화된 식별 및 차단이 가능해진다. 내부자에 의한 침해시도 및 불법적 데이터 접근이 차단되고, 장치(device)에 대한 인증이 가능해지기 때문에 불법 무기체계나 단말기의 접속이 차단된다. 또한, 네트워크 및 네트워크를 통한 악성코드의 확산이 어렵게 되므로 보안 수준이 한층 향상될 것으로 기대된다.

5. 결 론

최근 우리 군에서는 내부자와의 공모를 통한 국방망 침해 시도가 자주 발생하고 있어 강력한 물리적 망 분리정책에 기반한 보안정책이 더 이상 안전하지 않다는 것을 반증하고 있다. 또한, 다양한 에어갭(air-gap) 극복 기술이 발전하면서 기존의 물리적 망 분리정책을 고집할 필요가 없어졌다. 이와 관련해 세계 주요국은 제로 트러스트라는 보안정책과 전략의 혁신을 통해 국가의 중요 디지털 자산과 리소스(resource)를 보호함으로써 국가 사이버안보 역량을 강화하려는 노력에 집중하고 있다.

본 논문에서 우리는 새로운 보안 위협에 대응하고 우리 군의 사이버 방어역량을 강화하기 위해 한국군 맞춤형 제로 트러스트 구축방안을 제안하였다. 이를 위해 먼저 제로 트러스트 구축에 선두주자인 미 국방부의 제로 트러스트 전략, 로드맵, 최신 추진 동향을 살펴보았다. 다음으로 한국군 맞춤형 제로 트러스트 구축전략을 제시하였고, 제로 트러스트 전담조직 편성 방안과 예산 확보방안을 제안하였으며, 한국군 맞춤형 제로 트러스트 구축기술 확보방안을 모색하였다. 또한, 한국군 맞춤형 제로 트러스트를 구축한다면 기존의 물리적인 망 분리 정책과 비교하여 보안적인 측면에서 다양한 장점이 있음을 살펴보았다.

현재 우리 군은 각 군이 임무 영역별로 다양한 독자망을 구성하여 운영 중인 만큼 제로 트러스트를 단기간에 구축하기는 상당히 어려울 것으로 판단된다. 미 국방부의 경우를 살펴보더라도 제로 트러스트 개념연구와 레퍼런스 도출을 위해서만 최소 2년 이상 소요된 것을 알 수 있다. 따라서 우리 군도 한국군 맞춤형 제로 트러스트의 효율적인 구축을 위해서 더 많은 개념연구와 실증 사업을 통한 검증이 이루어져야 한다. 향후 우리는 미 NIST가 제안한 제로 트러스트 성숙도 모델을 기초로하여 우리 군에 적합한 제로 트러스트의 세부적인 원칙을 수립하고, 구체적인 국방 제로 트러스트 모델 정립을 위해 추가적으로 연구할 예정이다.

참고문헌

[1] Mylie Foy, "Symposium charts progress to zero-trust cybersecurity", MIT LINCOLN LABORATORY, 2023. https://www.ll.mit.edu/.

[2] US Department of Defense, "DoD Zero Trust Strategy", 2022. https://dodcio.defense.gov/Library/.

[3] US Department of Defense, "DoD Zero Trust Execution Roadmap", 2022. https://dodcio.defense.gov/Library/.

[4] 이민원, 권헌영, “제로 트러스트 명문화를 통한 신보안체계 강화 방안 연구 - 전자금융거래법상 법적 개선을 중심으로”, 융합보안논문지 제23권 제1호., pp. 9-17, 2023.
[5] 이다인, 이후기, "제로 트러스트 원리를 반영한 보안 강화 요소 기술 적용 방안 연구", 융합보안논문지 제22권 제3호., pp. 3-11, 2022.
[6] 신규용, “분산신원증명(DID) 기반 국방 다중인증 체계 구축방안”, 아시아태평양융합연구교류논문지, 제8권 제10호, 통권 54호 pp. 49-60, 2022.
[7] 김찬혁, 남지희, 원동훈, 차영균, “제로 트러스트를 활용한 육군 AMOS 체계 보안성 향상 방안”, 한국군사학논집 제79집 제2권, 2023. 6.
[8] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, “Zero Trust Architecture”, Special Publication (NIST SP) 800-207, National Institute of Standards and Technology, Gaithersburg, MD, 2020.
[9] FACTSHEET, "Zero Trust", U.S. Army CYBER COMMAND, 2023. https://www.arcyber.army.mil/
[10] 과학기술정통부, "제로트러스트 가이드라인 1.0", 2023.https://www.msit.go.kr/.
[11] Department of Defense, “Fiscal Year 2023 Budget Estimates”, Office of the Secretary of Defense Cyber, 2022.
[12] Jon Harper, "Army asking Congress for billions in 2024 to implement zero trust, cloud transition, BYOD and other digital transformation efforts", Defensescoop 2023. https://defensescoop.com/.
[13] 배준호, “제로 트러스트 구현을 위한 필수 기술은 무엇인가?”, IT DAILY, 2022. 9. http://www.itdaily.kr/.
[14] Cybersecurity and Infrastructure Security Agency, “Zero Trust Maturity Model Version 2.0”, Cybersecurity Division, April 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

〔저자소개〕

신 규 용 (Kyuyong Shin)
1996년 3월 육군사관학교 학사
2000년 2월 한국과학기술원 석사
2009년 12월 노스캐롤라이나 주립대학교(NCSU) 박사
email : kyshin@kma.ac.kr

길 총 경 (Chongkyung Kil)
1994년 3월 육군사관학교 학사
2002년 2월 미.공군대학원 석사
2009년 2월 노스캐롤라이나 주립대학교(NCSU) 박사
email : track9867@gmail.com

최 경 식 (Keungsik Choi)
1992년 3월 육군사관학교 학사
1998년 8월 미.오레곤주립대 석사
2007년 2월 한국과학기술원 박사
email : kschoi@gmail.com

김 용 철 (Yongchul Kim)
1998년 03월 육군사관학교 학사
2001년 11월 Univ. of Surrey 석사
2012년 01월 노스캐롤라이나 주립대학교(NCSU) 박사
email : kyc6454@gmail.com