미 국방부의 제로 트러스트 추진에 따른 우리 군의 고려사항에 관한 연구

이경복

한국국방연구원

kblee@kida.re.kr

A Study on the considerations for Korean Military in accordance with the US DoD's Zero Trust Implementation

Lee Kyung Bok

Korea Institute for Defense Analyses

요 약

본 논문은 제로 트러스트의 개념이 처음으로 구현되고 있는 미국 국방 분야 추진 현황을 분석하고, 이러한 분석을 바탕으로 우리 군이 제로 트러스트의 개념 도입을 위해 무엇을 고려해야 하는지를 고찰하였다. 미국과 같이 우리 군은 기본적으로 기술적 측면에서 사이버보안 강화를 위한 새로운 패러다임으로 접근할 필요가 있고, 이를 위해 개념, 대상, 구현방법 등의 구체화를 위한 체계적인 계획을 마련할 필요가 있다. 또한, 미국은 연합 영역에 대해서도 제로 트러스트를 추진하고 있어 기술 수준을 넘어 군사작전 및 전략적 관점에서 우리 군이 제로 트러스트를 어떻게 구현할 것인지 종합적인 논의가 필요하다.

Ⅰ. 서 론

2010년 새로운 정보보호 모델의 개념으로 제로 트러스트의 개념이 보안 분야에서 처음 사용된[1] 이후, 최근 미국 국방 분야에서 본격적으로 제로 트러스트의 적용이 추진되고 있다. 본 논문은 제로 트러스트 개념이 처음으로 구현되고 있는 미국 국방 분야의 추진 현황을 분석하고, 이러한 분석을 바탕으로 우리 군이 제로 트러스트의 개념을 도입하기 위해 무엇을 고려해야 하는지를 제시하고자 한다.

Ⅱ. 미 국방부의 제로 트러스트 추진 현황

'21년 5월, 제로 트러스트 도입을 포함하는 사이버보안 현대화 추진에 대한 미 대통령 행정명령(E. O. 14023) 발표 이후,[2] '22년 1월 발표된『국가안보각서-8』을 통해 국가안보시스템(National Security System)의 제로 트러스트 아키텍처 채택 및 구현 계획 수립이 지시됨에 따라,[3] 미 국방부는 국방 분야에 특화된 제로 트러스트 능력을 정의하고 시범사업을 완료하는 등 국방 분야 제로 트러스트 구현을 적극적으로 추진하고 있다.

가장 먼저, '21년 2월, 미 국가안보국(NSA)과 국방정보체계국(Defense Information Systems Agency)는 국방 분야에서 요구되는 제로 트러스트 능력과 아키텍처를 발표하였다. 이에 발맞춰 미 국방부는 '22년 1월, 제로 트러스트 전담부서 ZT PfMO(Zero Trust Portfolio Management Office)를 신설하고『'22년도 국방수권법』을 통해 국방부 CIO(Chief Information Officer)와 사이버사령부에 국방부정보네트워크(DoDIN) 전반에 구현될 제로 트러스트 전략, 원칙, 모델 아키텍처 개발의 책임을 부여하였다.[4]

'22년 3월 발표된『국방전략서』는 통합억제를 위한 '회복탄력성에 의한 억제(deterrence by resilience)'의 사이버 회복탄력성 강화방안의 예시로 제로 트러스트 아키텍처를 제시하는 등, 제로 트러스트가 군사적 관점의 주요 개념으로 다뤄지기 시작했고, '22년 10월『국방부 제로 트러스트 전략』이 수립되었다.[5] 동 전략은 '27년까지 모든 국방정보체계의 제로 트러스트 구현을 위한 접근 방법, 전략 목표, 추진 방식 등을 제시한다. '23년 4월에는 상기 전략에 제시된 행동방침(COA: Course of Action)을 점검하는『국방부 제로 트러스트 능력 실행 로드맵(COA 1)』이 발표되었다.[6]

'23년 6월, 국방 분야 제로 트러스트 추진 간 최종 모습에 대한 이해 차이를 해결하기 위해, ZT PfMO 주관으로 국방 분야 제로 트러스트 추진을 위한 각 군과 이익공공체(Community of Interest)가 참여한 정기 회의가 시작되었고, 이후 10월, 각 군 및 국방 기관에서 총 43개 이행계획이 수립되어 국방부로 제출되어, 계획의 목표수준 달성 방법, 국방부 관점의 계획 일관성, 각 부대/기관의 고유요소 등이 검토되어, 미 국방 분야 군 및 기관들에서 제로 트러스트 구축이 진행되고 있다.

이와 함께 시범사업도 함께 추진되었다. '21년 9월, 국방정보체계국은 상용기술을 활용한 제로 트러스트 실증 시범사업을 계획하고, '22년 1월, Booz Allen Hamilton을 통해 총 12개월 630만 달러 규모의 시범사업 Thunderdome을 수행하였다. 이후 '23년 3월, Thunderdome 시범사업의 성공적 완료가 발표되었고, 국방부 내 사업 확산을 위한 5년 18억 달러 규모의 후속사업('23년 8월 ~ '28년 8월)이 동일 업체를 통해 수행되고 있다.

미 국방부는 제로 트러스트 개념을 '정적인 네트워크 기반 경계로부터 사용자·자산·자원에 집중하도록 방어를 이동하는 진화하는 사이버보안 패러다임의 집합'으로 정의한다. ZT PfMO 부서장 Randy Resnick은 이러한 개념을 '구매하는 능력·기기가 아닌 악성 행위자의 가장 중요한 자산 접근을 방지하고 현재의 공격표면을 축소하는 보안 프레임워크, 구조적인 접근방식, 방법론'으로 설명한다. 미 국방 분야의 제로 트러스트 개념은 적대적 환경을 가정하고, 침해를 상정하며, 신뢰를 금지하고 항상 확인하며, 명시적으로 면밀히 조사하고, 통합분석을 적용하는 5가지 기본 원리(tenet)를 바탕으로 한다. 또한, 데이터 중심 접근 방식의 차세대 사이버보안 아키텍처가 제로 트러스트의 비전이다. 사용자·기기·애플리케이션·트랜잭션의 지속 검증 설정을 위해 데이터 중심 접근방식을 사용하며, 보안 경계 내외부에서 동작하는 행위자·시스템·네트워크·서비스의 기본 신뢰를 배제하는 차세대 사이버보안 아키텍처로, 제로 트러스트를 정의한다.

미 국방부는 제로 트러스트를 활용하여 악성사이버활동(Malicious Cyber Activities)으로부터 국방부 정보·시스템·핵심기반시설의 보호·방

어를 목표로 하는데, 이는 국방부가 소유하지 않는 네트워크의 국방부 정보를 포함한다. 국방 분야의 모든 운영(작전) 환경에서 악성사이버활동을 탐지·억제·거부·방어·복구하기 위해 제로 트러스트를 사용하는 것이다. 또한, 가장 중요한 임무-필수 데이터·애플리케이션·자산·서비스(Data, Application, Assets, and Services) 보호를 중심으로 확장 가능하고, 복원성이 있고, 추적할 수 있고, 방어 가능한 프레임워크를 개발하는 것이 미 국방부 제로 트러스트 추진의 목표이다.

미 국방부는 목표 달성을 위해 제로 트러스트 구현의 핵심 영역을 사용자, 기기, 애플리케이션, 업무, 데이터, 네트워크··환경, 자동화·통합, 가시성·분석의 7가지로 구분하고, 요망효과 달성을 위해 필요한 방법과 수단의 조합을 영역별 총 45개의 능력(capabilities)으로 제시하고, 각 능력을 구현하는 세부적인 152개의 활동(activities)을 제시하였다. 그리고 이러한 능력과 활동에 있어 국방부 내 일반 정보시스템이 달성해야 할 수준(목표 수준)과 국가안보시스템과 같이 매우 중요한 정보시스템이 달성해야 할 수준(고급 수준)을 구분하고, '27년까지 목표 수준 달성을 위한 영역별 능력의 추진 일정을 명시한 능력 로드맵을 함께 제시하였다.

미 국방부는 제로 트러스트 구현을 위한 3가지 행동방침(COA)을 제시한다. 행동방침①은 국방부 내 현존 IT 기반시설의 제로 트러스트 적용이다. 이는 '23년부터 5년 이상의 현 기반시설과 환경을 활용하되 기초부터 시작하는 현대화 관점에서 추진되며, 구현에 있어 도구나 방법의 제한사항이 없이 목표·고급 수준을 달성하기 위한 다양한 능력과 활동을 활용한다. 행동방침②는 제로 트러스트에 부합하는 클라우드 환경 개발에 상용 제품을 활용하는 것이다. 이는 행동방침①보다 빠르게 최소한 목표 수준을 달성하기 위함이며, 제로 트러스트 실행을 지원하기 위해 표준화된 도구와 능력을 사용한다. 행동방침③은 정부 소유·운영 사설 클라우드 내부에 고성능 제로 트러스트를 구현하는 것이다. 이 역시 행동방침①보다 빠르게 달성하는 것이 목표이며, NSA가 검증한 설계에 따라 즉각적으로 고급 수준을 달성하기 위한 방침이다. 여기서 중요한 점은 미 국방부가 이러한 행동방침들 중 하나를 선택하는 방식이 아니라, 3가지 행동방침의 모든 조합을 고려하는 하이브리드 방식으로 제로 트러스트 구현을 추진한다는 점이다. 이를 위해 전투사령부 등을 통해 약 6개 시범 프로그램을 이미 수행하고 있다. '21년 11월, 4개의 시범 프로그램에 상용 클라우드 업체(AWS, Google, AZURE, Oracle)를 선정, 이들과 함께 행동방침② 관점에서 국방부가 정의한 제로 트러스트 능력/활동 구현 여부를 확인·평가하고 있다. 그리고 행동방침③ 활동으로 NSA 주도의 온-프레미스 클라우드 형태로 고급 수준의 제로 트러스트 시범 프로그램을 설계하고, 사이버사령부 내 구축된 NSA 국립제로트러스트센터에서 이를 추진하고 있다. 또한, 업무 의존도가 높은 마이크로소프트의 사무용 제품에 제로 트러스트 아키텍처를 적용하는 시범 프로그램을 계획하고 있다. 마이크로소프트는 이미 오피스 385의 기업용 제품 일부(E-5)에 제로 트러스트를 적용하고 있다.

국방정보체계국이 추진한 시범사업 Thuderdome은 네트워크 접근(Network Access)에 초점을 두고 상용기술 기반으로 제로 트러스트 구현 가능성을 확인하기 위한 사업이었다. 상용기술을 통해 사이버보안의 효과를 향상시키면서 사이버보안 아키텍처의 중복성과 복잡성을 축소하고, 국방부 내에 제로 트러스트 네트워크 접근(ZTNA)을 전사적으로 확대, 활용하기 위한 교훈을 생성하며, 시제품을 배치하고 각 군과 전투사령부, 국방기관, 야전 활동과 협력하기 위한 목적으로 사업이 수행되었다. 이러한 목표 달성을 위해 Thuderdome은 SASE(Security Access Service Edge), SD-WAN CESS(Customer Edge Security Stack), AppSS(Application Security Stack), Cloud DCO(Defense Cyber Operation)의 4가지 민간 상용기술을 핵심 구성요소로 사용하였다. 사용자는 SD-WAN/CESS나 SASE를 통해 국방 네트워크에 접근하며, 애플리케이션이나 데이터에서는 AppSS와 Cloud DCO가 적용되어 보안 기능을 제공한다. Thuderdome를 통해 네트워크 내·외부의 사용자는 안전하게 국방부 내 데이터·애플리케이션에 접근하며, 이러한 접근과정에서 내부/원격 사용자의 데이터 접근 등은 모두 기록·분석·가시화되고, 이를 통해 국방부 내부의 방어적 사이버작전이 수행된다.

미 해군이 '21년 추진한 새로운 클라우드 환경을 위한 Flank Speed는 행동방침②의 시범사업으로, 약 50만 명의 해군 사용자에게 클라우드 기반 서비스, 보안 데이터 액세스, 엔드포인트 장치 관리, ID 관리 등 다양한 IT 지원을 제공하는 강력한 제로 트러스트 보안 환경을 구축하여, '23~'24년 2차례의 미 국방부 보안평가를 처음으로 통과한 제로 트러스트 서비스로 인정되는 등 미군의 제로 트러스트 구축은 매우 빠르게 진행되고 있다.

Ⅲ. 우리 군의 제로 트러스트 추진 간 고려사항

우리나라도 '23년 4월 디지털플랫폼정부위원회의 『디지털플랫폼정부 실현계획』을 통해 국가 차원의 제로 트러스트 추진이 이미 선언되었다. 국방부도 '23년 『국방지능정보화 종합계획』을 통해 새로운 사이버보안 기술 아키텍처 설계에 제로 트러스트 개념을 반영할 것을 명시하였다. 하지만, 아직 제로 트러스트 구현의 필요성, 범위, 대상, 방법 등을 식별·검토하는 단계로, 국방 정보화 환경 내 제로 트러스트가 필요한 대상, 범위, 구현 방법 등을 구체화할 필요가 있다. 또한, 미국과 같이 시범사업 등을 통해 제로 트러스트 적용 가능성을 확인하는 등 체계적인 추진 계획이 필요하다.

특히, 제로 트러스트는 우리 군이 향후 추진예정인 국방 모바일 환경 및 전장 클라우드 구축을 위한 핵심 개념으로 접근할 필요가 있다. 전장 환경은 높은 보안이 요구되며 항상 신뢰가 없다는 전제하에 작전환경 유지가 중요하므로, 전장 클라우드 환경은 제로 트러스트를 반드시 갖춰야 한다.

한편, 미국은 국방 전략 차원에서 제로 트러스트를 강조하고, 전 영역 통합 지휘통제(JADC2/CJADC2)의 필수요소로 제로 트러스트를 명시하는데, 이는 향후 미국이 제로 트러스트 개념을 한미연합 영역에 요구할 가능성을 내포한다. 이미 미 국방부의 제로 트러스트 목표 환경은 연합의 임무 파트너(Mission Partner)를 포함하고 있다. 이에 우리 군은 제로 트러스트에 대해 기술적 차원의 새로운 사이버보안 패러다임을 넘어, 군사작전과 전략적 관점과 같은 보다 큰 맥락에서 체계적이고 종합적인 논의를 통해 제로 트러스트를 접근할 필요가 있다.

참 고 문 헌

[1] John Kindervag, Stephanie Balaouras and Lindsey Coit. (2010). "No More Chewy Centers: Introducing The Zero Trust Model of Information Security." Forrest Research. September 14, 2010.

[2] Executive Order 14028. Improving the Nation's Cybersecurity. 21 May 2021.

[3] National Security Memorandum 8. Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. 19 January 2022.

[4] National Defense Authorization Act of FY22. §1528 Zero Trust Strategy, Principles, Model Architecture, and Implementation Plans.

[5] DoD CIO. (2022). DoD Zero Trust Strategy. 21 October 2022.

[6] DoD CIO. (2023). DoD Zero Trust Capability Execution Roadmap (COA 1). 6 January 2023.