제로트러스트 가이드라인, 새로운 사이버 보안 전략의 시작

이석준 / 가천대 컴퓨터공학부 교수
(junny@gachon.ac.kr)

1. 개요

최근 빅데이터, 인공지능, IoT, 5G, 클라우드 등 정보통신 기술의 발전과 함께, 이들 기술이 기존의 산업·비즈니스와 결합이 되면서 사회의 다양한 분야에서 새로운 파괴적 변화가 이루어지고 있다. 이러한 사회적 변화를 '디지털 전환(Digital Transformation)'이라고도 하는데, 이는 디지털 기술을 사회 전반에 적용함으로써 전통적인 사회 구조를 혁신하는 것을 의미한다.

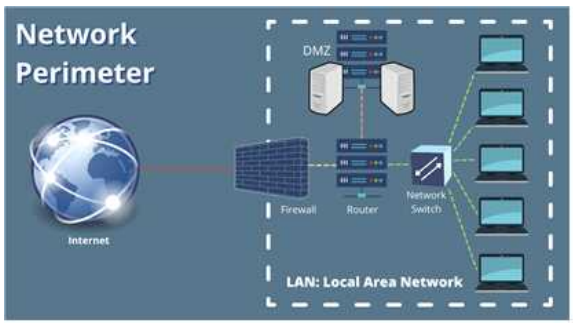
디지털 전환은 기존에 해결하지 못했던 여러 문제의 해결 방안을 제시하여 주며, 새로운 산업과 시장을 창출함으로써 사용자에게 그동안 경험하지 못한 놀라운 서비스를 제공하기도 하지만, 이러한 변화는 해커들에게는 새로운 먹잇감이 늘어나는 것을 의미한다. 즉, 점점 더 많은 기기와 사물에서 컴퓨팅과 통신, 인터넷 연결이 가능해짐에 따라, 이들 모두 사이버 공격의 통로와 수단으로 활용될 가능성이 생기기 시작한 것이다. 사이버 공격은 공격 과정 및 피해가 눈에 잘 보이지 않을 뿐만 아니라, 피해가 발생하는 순간 퍼져나가는 속도가 매우 빠르기 때문에 이로 인한 피해를 예측하기가 매우 어렵다. 또한 과거 사이버 공격으로 인한 피해가 대부분 사이버 공간에 한정되었던 것과 달리, 자율주행차 혹은 의료 기기·기관, 원자력 발전소 등 다양한 분야에서 벌어지는 최근의 해킹 사례들을 보면, 이 사이버 공격이 국민의 재산과 생명, 기업의 생존, 국가 안보를 위협하는 수준으로 발전하고 있음을 알 수 있다.

각국 정부 및 기업들은 이러한 변화에 대응하기 위하여, 제로트러스트(Zero Trust) 보안 전략에 관심을 갖기 시작했다. 제로트러스트는 '절대 신뢰하지 말고, 항상 검증하라(Never Trust, Always Verify)'라는 표현으로 대표되는 새로운 보안 패러다임이다. 우리나라 역시 많은 관심을 갖고

정책을 추진해 왔으며, 2023년 7월 과학기술정보통신부(이하, 과기정통부)와 한국인터넷진흥원(이하, KISA), 한국제로트러스트포럼(이하, 포럼)은 공동으로 제로트러스트 가이드라인 1.0을 발표하였다. 본고에서는 제로트러스트의 개념과 국내외 도입 동향, 그리고 제로트러스트 가이드라인에 대해 소개하고, 새로운 사이버 보안 전략에 대한 시사점을 살펴보도록 한다.

2. 제로트러스트란?

제로트러스트는 단어 자체에서 의미하는 바와 같이, '신뢰할 수 있는 네트워크'라는 개념 자체를 배제하고, 기업·기관 네트워크 내외부에 언제나 공격자가 존재할 수 있다는 가정 하에 명확한 인증과 신뢰도 평가를 거치기 전까지는 모든 사용자와 접속기기, 네트워크 트래픽을 신뢰하지 않고 인증 이후에도 끊임없이 신뢰도를 검증함으로써 기업·기관의 중요한 정보 자산을 보호하려는 보안 모델을 의미한다.



〈그림 1〉 경계기반 보안 모델 개념도.
출처: https://www.pomerium.com/blog/the-perimeter-problem/

과거의 전통적인 보안 모델을 흔히 '경계기반 보안(Perimeter Security)'이라고 부른다. 일반적으로 과거에는 기업·기관의 사용자(직원)와 정보자산이 네트워크로 연결된 하나의 물리적 공간에 있었으며, 이는 자연스럽게 외부 인터넷과의 경계를 형성하였다. 해커들이 존재하는 인터넷과의 연결 진입점에서 방화벽, 침입탐지시스템 등 강력한 네트워크 기반 보안 솔루션을 통하여 내부를 지키고자 하는 이 보안 전략은, 마치 중세 시대 높은 성벽을 통해 내외부를 구분 짓는 경계를 형성하고, 성문에서 적을 탐지하는 구조와 유사하다고 볼 수 있다.

물리적 혹은 네트워크 경계를 통해 내부와 외부를 분리하고 진입점에서 모든 네트워크 트래픽을 감시하는 방식은 매우 자연스러운 보안 전략으로 볼 수 있다. 그러나 최근 사회적·기술적 변화들은 경계 확장 전략이 더 이상 유효하지 않음을 보여준다. 첫째, 직원들은 재택근무 혹은 출장지 원격접속 등에 대한 요구가 있었으며, 이는 COVID-19 이후 더욱 가속화됐다고 볼 수 있다. 둘째, 관리 부담, 사용 편의성 등을 위하여 내부(On-premise) 서버에서 유지하던 정보 자산을 클라우드로 이동하고 있다. 이에 따라 기업·기관 네트워크는 점점 복잡해지고 내외부 경계가 모호해지고 있으며, 공격자가 침투할 수 있는 경로가 다양해지고 있다.

또한, 경계기반 보안모델은 네트워크 내부에 위치한 사용자 및 기기에 상대적으로 높은 신뢰를 부여한다는 특징을 보인다. 이 때, 공격자는 신뢰를 악용하기 위한 전략으로 내부 서버 혹은 단말에 침투하는 것을 1차 목표로 삼게 된다. 사용자 계정 해킹을 통한 VPN 접속, 피싱 메일 등을 통한 악성 코드 삽입 등을 통하여 기업·기관의 내부 네트워크로 진입하는데 성공할 경우, 중요 데이터가 위치한 서버로 횡적 이동을 통해 침투하여 피해를 입히게 된다.

이러한 경계 기본 보안 모델의 약점을 극복하려는 시도는 2000년대 초반부터 있었다. 산업보안

전문가 그룹인 제리코 프로젝트(Jeridcho Project)에서는 탈 경계화(De-perimeterization)라는 개념을 제안하였으며, 미 국방부는 내부 네트워크 IP 계층에서의 종단 간 암호화를 제공하는 블랙코어(Black Core 혹은 Black Transport)라는 네트워크 전략을 개발하였는데, 이는 소프트웨어 정의 경계(SDP, Software-Defined Perimeter) 기술로 진화하였다. 이러한 논의들은 네트워크 내부 역시 신뢰하기 어렵다는 제로트러스트 전략의 초창기 개념을 제공했다고 볼 수 있다.

2010년 포레스터 리서치(Forrester Research)의 수석 애널리스트인 존 킨더박(John Kindervag)은 '제로트러스트' 용어의 정의 및 개념 제안을 통해, 기업망에서 악의적인 내부자가 '신뢰'하는 위치에 존재할 수 있으므로 새로운 보안 전략이 필요함을 강조했다. 이후 이 개념을 더욱 발전시키는 과정에서 네트워크뿐만 아니라 사용자, 기기, 워크로드로부터 데이터에 이르는 기업망의 모든 핵심 요소에 제로트러스트 전략의 도입 필요성이 강조됐고, 기업망 전 영역에 걸쳐 가시성 확보와 자동화 및 통합 운영까지 범위가 확장돼 왔다.

3. 국내외 제로트러스트 도입 동향

가. 미국 연방정부의 제로트러스트 도입

2014년에서 2015년까지 미 연방정부 인사관리처에서는 중국계로 추정되는 해커 그룹에게 약 2,150만 명에 달하는 개인정보가 유출되는 사고가 있었다. 2016년 미 하원 감독개혁위원회는 해당 사고의 원인 및 경과 등에 관한 보고서를 공개했는데, 이 보고서에서 제로트러스트 전략의 도입에 대한 권고가 포함됐다. 이후, 연방CIO위원회는 제로트러스트/SDN Steering Group을 설립하고 NIST와 함께 관련 연구를 진행했으며, 2019년 NIST는 제로트러스트 아키텍처 프로젝트를 시작하고 2020년 'Zero Trust Architecture(SP 800-207)' 가이드를 통하여 제로트러스트에 대한 정의, 원칙, 보안 위협, 전환 방안 등을 공개했다.

바이든 대통령은 2021년 5월 '국가 사이버보안 개선'에 관한 행정명령(EO-14028)을 통해 연방정부의 사이버보안 현대화를 위한 제로트러스트 전략 채택을 발표했다. 행정명령 공포 60일 이내 각 기관장들이 NIST 표준 및 지침의 절차에 따르는 제로트러스트 아키텍처 도입 계획을 개발해야 하며, 클라우드 기술 도입 시 제로트러스트 아키텍처 채택 의무 등의 내용을 포함하고 있다. 2021년 9월 CISA는 연방민간행정기관(FCEB)이 제로트러스트 도입에 있어 어떤 기술을 고려해야 하는지에 관한 '제로트러스트 성숙도 모델 1.0'을 발표했으며, 2022년 1월 관리예산실(OMB)는 각 기관장들에게 회계연도 2024년 종료 시까지 달성하고자 하는 제로트러스트 보안 목표를 상기 CISA 문서를 기반으로 작성할 것, 60일 이내 구현 계획 및 예산 추정치를 제출할 것, 30일 이내 기관별 전략 실행 책임자를 지정할 것 등을 포함하는 각서(M-22-09)를 발표했다.

미 국방부는 2021년 2월 '제로트러스트 참조 아키텍처 버전 1.0', 2022년 7월 동일 문서의 버전 2.0을 발표했으며, 미 국방부가 바라보는 관점에서의 운영 전략, 비전, 핵심 기능과 원칙, 유스케이스 등을 포함하고 있다. 바이든 대통령은 2022년 1월 '국가 안보, 국방부 및 사이버 보안 개선을 위한 국가안보각서(NSM-8)'를 통하여 국방부를 포함하는 안보 기관들이 제로트

러스트 구현 계획을 개발하기 위한 원칙을 발표했다. 국방부는 발표 직후, 책임 조직으로 '제로트러스트 포트폴리오 관리실(Zero Trust Portfolio Management Office)'을 설립하였으며 같은 해 11월 '제로트러스트 전략' 및 '역량 실행 로드맵(Capability Execution Roadmap)'을 발표하였다. 이 발표에서는 목표 수준의 제로트러스트를 2027년까지, 개선 수준의 제로트러스트는 2032년까지 달성 로드맵과 함께 각 세부 기능까지 공개했다.

따라서 현재 미 연방민간행정기관들은 관리예산실의 각서에 따라 2024년 9월까지 각 기관별 목표 수준을 만족하는 제로트러스트 아키텍처를 구현하게 될 것으로 보이며, 국방부를 포함한 안보기관들은 각 기관별 목표에 따라 제로트러스트 도입을 진행하고 있는 것으로 보인다. 다만 2024년까지 달성하려는 기관별 목표는, 관리예산실 각서 및 NIST와 기업 간 실증 프로젝트 추진 상황 등을 고려할 때 제로트러스트 성숙도 수준은 높지 않을 것으로 추정할 수 있다.

나. 기타 국가의 도입 상황

다른 국가들 역시 제로트러스트 보안 전략이 높은 수준의 보안성을 제공할 수 있어 각 정부 및 기반 시설, 민간 기업들이 채택해야 할 필요성을 느끼고 있으나, 한편으로는 이를 선도하고 있는 미국 중심의 보안 기업들이 자국의 보안 시장 점유율을 높이게 될 것을 우려하고 있는 것으로 보인다. 또한, 제로트러스트 개념에 대한 성공적인 실증 사례가 아직은 없는 만큼, 미국 연방정부의 도입 상황을 살펴보며 자국의 도입 전략을 구체화하려는 움직임도 보인다.

현재 GovZTA 프레임워크를 통해 제로트러스트를 적극 추진하고 있는 싱가폴 등 일부 국가를 제외하면, 아직까지 대다수 국가들은 제로트러스트 아키텍처와 원칙에 관한 지침을 발표하고 제로트러스트 전환 계획을 선언하는 수준으로 보는 것이 타당하다.

다. 국내 도입 동향

과기정통부는 2022년 KISA 및 민간전문가들과 함께 '사이버보안 패러다임 전환 연구반'을 구성해 민간 영역에서 제로트러스트 도입의 필요성, 국내 보안 기업들의 신시장 창출 등을 위한 신보안체계 등을 연구했다. 연구반에서 논의한 국내외 관련 이슈 및 정책 추진 방향을 기반으로, 보다 폭넓은 논의의 장 마련을 위하여 같은 해 10월 26일 한국제로트러스트포럼을 발족하며, 이후 포럼 내부 논의 및 검토, 과기정통부 및 KISA 협의 등을 거쳐 2023년 7월 제로트러스트 가이드라인 1.0을 공개했다. 이는 민간 수요 기업의 제로트러스트 전략 수립에 도움을 주기 위한 것으로, 이와 별도로 보안 기업의 경쟁력 강화 및 사례 확보를 위해 2023년 6월부터 11월까지 실증 지원 사업을 진행했으며 2024년부터 이를 더욱 확대할 계획이다.

국가정보원 역시 국가·공공 영역에서의 사이버보안 강화를 위한 제로트러스트 도입의 필요성을 인지해, 사이버안보 민관합동협의체에서 제로트러스트에 대한 정책을 논의하고 있으며, 2023년 7월 언론사 초청 사이버안보간담회를 통하여 2024년까지 K-제로트러스트 구축 가이드라인 개발 및 부처별 시범 적용, 2026년부터 전 국가·공공기관 대상 적용을 포함하는 로드맵을 발표했다.

과기정통부는 민간 기업들의 안전성 증대 및 국내 보안 기업을 포함하는 산업 경쟁력 강화에

보다 초점이 맞춰져 있는 반면, 국가정보원은 국가·공공기관을 사이버 위협으로부터 보호하기 위해 필수적으로 지켜야 할 정책적 보안 지침을 제공하려는 차별점이 존재한다.

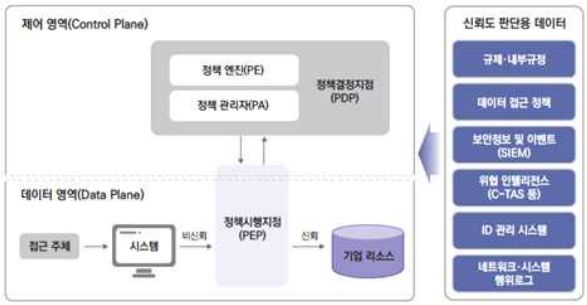
4. 제로트러스트 가이드라인 1.0 소개

6가지 제로트러스트 기본 원리
가. 기본 원칙: 모든 종류의 접근에 대해 신뢰하지 않을 것 (명시적인 신뢰 확인 후 리소스 접근 허용)
나. 일관되고 중앙 집중적인 정책 관리 및 접근제어 결정, 실행 필요
다. 사용자, 기기에 대한 관리 및 강력한 인증
라. 리소스 분류 및 관리를 통한 세밀한 접근제어 (최소 권한 부여)
마. 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
바. 모든 상태에 대한 모니터링, 로그 및 이를 통한 신뢰성 지속적 검증, 제어

〈그림 2〉 6가지 제로트러스트 기본 원리.
출처: 과학기술정보통신부, 한국인터넷진흥원, 한국제로트러스트포럼(2023)

과기정통부, KISA, 포럼 등이 발표한 제로트러스트 가이드라인(이하, 가이드라인)은 크게 2가지 버전(요약본 및 전체본)으로 구성됐다. 포럼 내부에서 가이드라인에 대한 초창기 논의 당시, 각 기업들의 보안 전략수립 책임자 및 실무자들을 대상으로 제로트러스트 전략 수립에 도움을 주기 위한 문서를 진행했으나, 이후 과기정통부 및 KISA와의 협의를 거쳐 기업의 의사 결정 과정에 포함된 정책 결정권자 및 경영진, 일반 직원들 역시 제로트러스트에 대한 이해와 인식이 필요하다는 공감대를 반영하여 비전문가의 이해를 돕는 요약본도 동시에 발표하였다. 요약본에서는 제로트러스트의 추진 배경과 개념, 아키텍처, 도입 방안, 원격 근무 참조 모델 등을 간략히 설명하고 있으며, 전체본에서는 제로트러스트 개념과 보안 모델, 도입 절차 및 유스케이스 등을 상세히 기술하고 있다.

가이드라인에서 언급하고자 하는 제로트러스트의 배경과 기본 원리, 아키텍처와 논리적 구성요소는 사실상 미국과 차별화하기 어렵다고 볼 수 있다. 따라서 기본적인 구조는 NIST 및 CISA 등이 발표한 관련 문서를 참고하였으며 기본 철학을 유지하고 있다. 다만, 제로트러스트의 기본 원리는 미국 NIST 및 국방부, 영국 NCSC 등을 참고하되 국내 기업이 이해하기에 더 적합한 표현으로 새로 작성했으며, 아키텍처 역시 정책 결정에 있어 신뢰도 판단용 데이터를 적극 활용해야 함을 보다 분명하게 알 수 있도록 구성했다.



〈그림 3〉 제로트러스트 아키텍처.
출처: 과학기술정보통신부, 한국인터넷진흥원, 한국제로트러스트포럼(2023)

국내 환경에서는 기업망에서 중요 응용 프로그램을 구동하고 중요 데이터를 저장·관리하는 온프레미스 서버를 많이 활용하는 환경에서, 일반적인 단말과 동일한 보안 기능을 통해 제로트러스트 철학을 달성하기 어렵다는 인식하에 단말과 별도로 '시스템' 핵심 요소를 추가하고, 이에 대한 성숙도 수준별 보안 기능을 기술하였다. 시스템의 보안 기능으로는 시스템 계정 관리 등을 통하여 중앙 일원화된 접근제어 정책이 적용되어야 하는 등의 내용을 포함하고 있다. 단, 기업망 차원에서 시스템이 명시적으로 단말과 구분되는 보안 기능을 요구하지 않는 경우 이를 고려하지 않아도 된다.

요약본에서는 제로트러스트의 도입 효과를 비전

문가들이 빠르게 이해할 수 있도록, 논리적 망 분리를 포함하는 원격 근무 환경에서도 업무망으로의 공격이 가능함을 소개하고, 제로트러스트 보안 철학을 만족하는 기술 도입 시 어떻게 대응할 수 있는지에 대한 참조 모델을 소개하고 있다. 다만, 이 참조 모델은 하나의 참조할 수 있는 사례로서 언급하는 것일 뿐, 이 방법이 절대적이진 않으므로 기업별 상황에 따라 새로운 아키텍처를 고려할 수 있다.

5. 시사점

본고에서는 제로트러스트의 개념과 국내외 도입 동향, 그리고 제로트러스트 가이드라인에 대해 소개했다. 제로트러스트는 그 자체로 기술, 제품이나 솔루션이 아니며, 이미 내부에 공격이 침투했을 가능성에 대비하기 위한 새로운 보안 전략으로 보는 것이 타당하다. 이미 침투했을 가능성을 포함한다는 것은, 제로트러스트가 모든 공격을 완벽히 차단하는 전략이 아니라는 것을 의미하며, 이미 침투가 이루어진 환경에서조차 공격자의 횡적 이동, 권한 상승을 통한 중요 데이터의 갈취를 어렵게 만들고 공격에 빠르게 대응함으로써 위험을 최소화하는 전략으로 보는 것이 타당하다.

일부 기업들은 자사의 솔루션을 도입할 경우 제로트러스트 철학을 만족할 수 있다고 주장하나 이는 현실적으로 매우 어렵다. 미 국방부는 고수준의 제로트러스트를 달성하기 위해 10년간의 계획을 세우고 있는 점 등을 고려하면, 제로트러스트 철학을 도입하는 것은 긴 여정을 떠나는 일과 같다고 보는 것이 타당하다. 제로트러스트를 실현하는 것은 어렵고 시간이 오래 걸리는 작업이기에, 기업·기관 직원들 모두 해당 개념과 철학을 정확히 이해하는 것이 중요하며 각 기업·기관의 상황을 반영하는 장기간의 계획을 수립하는 것이 필요하다. 이러한 어려움을 조금이라도 해소하고자 2023년 7월 제로트러스트 가이드라인 1.0이 발간됐으나, 여전히 부족함이 있을 수 있다.

NIST의 제로트러스트 프로젝트 사례를 살펴보면, 실시간 위험 및 신뢰도를 측정하는 방안 및 개별 보안 솔루션간 연동 문제로 어려움을 겪고 있음을 확인할 수 있으며, 우리나라 역시 실증 과정에서 유사한 경험을 하게 될 가능성이 높다. 현재의 제로트러스트 가이드라인 1.0은 실증 사례를 포함하고 있지 않아 이러한 문제를 충분히 다루지 못하고 있으나, 이를 극복하기 위해 다양한 현장 전문가들로부터의 의견 수렴과 2023년 진행된 과기정통부의 실증 지원 사업을 참고해 제로트러스트 가이드라인 2.0을 발간할 계획이다. 해당 전략을 선도적으로 진행하고 있는 미국 연방정부 및 보안 기업들이 앞서 나아가고 있는 것이 현실이지만, 우리나라 역시 다른 나라와 비교하여 뒤처지지 않도록 노력하고 있으며 계속해서 많은 분들의 관심과 의견을 부탁드린다. KISO JOURNAL

※ Keyword : 경계기반 보안 모델, 디지털 전환, 사이버 보안 전략, 제로트러스트 가이드라인

[참고문헌]

[1] Wikipedia. De-perimeterisation, Available: https://en.wikipedia.org/wiki/De-perimeterisation
[2] Forrester(2010). 『No More Chewy Centers: Introducing the Zero Trust Model of Information Security』
[3] Forrester(2018). 『The Zero Trust Extended (ZTX) Ecosystem – Extending Zero Trust Security Across Your Digital Business』
[4] NIST(2020). 『Zero Trust Architecture』
[5] DISA and NSA(2021). 『Department of Defense Zero Trust Reference Architecture, Version 1.0』
[6] Executive Order 14028(2021). 『Improving the Nation's Cybersecurity』
[7] CISA(2021). 『Zero Trust Maturity Model – Pre-decisional Draft Version 1.0』
[8] OMB(2022). 『Moving the U.S. Government Toward Zero Trust Cybersecurity Principles』
[9] DISA and NSA(2022). 『Department of Defense Zero Trust Reference Architecture, Version 2.0』
[10] US Committee on National Security Systems(2022). 『Committee on National Security Systems (CNSS) Glossary』. CNSSI 4009
[11] DoD(2022). 『Zero Trust Strategy』
[12] CISA(2023). 『Zero Trust Maturity Model Ver 2.0』
[13] 과학기술정보통신부, 한국인터넷진흥원, 한국제로트러스트포럼(2023). 『제로트러스트 가이드라인 1.0』
[14] Singapore Government Developer Portal(2023). Government Zero Trust Architecture (GovZTA). Available: https://www.developer.tech.gov.sg/guidelines/standards-and-best- practices/government-zero-trust-architecture
- NIST(2023). 『Implementing a Zero Trust Architecture – Volume B: Approach, Architecture, and Security Characteristics』