특집 03

제로 트러스트 기술 동향 및 사례 분석

이송희 (한국폴리텍대학), 조원배 (한국인터넷진흥원)

목 차

1. 서 론

4차 산업혁명으로 촉발된 디지털 전환이 가속화됨에 따라 IT 기술과 다양한 산업 간의 경계가 허물어지고, IT 기술을 기반으로 하지 않는 산업군에서도 이제는 기존에 경험하지 못한 사이버 공격 위협에 대응해야 하는 환경에 놓여있다. 또한 코로나 19 팬데믹으로 인해 정부, 공공기관, 민간기업, 교육기관 등에서는 비대면 및 원격·재택근무 환경으로의 전환이 확산되면서 새로운 보안문제가 대두되었다. 급작스러운 디지털 업무환경으로의 전환에 따라 공격표면(Attack Surface)이 확대 되면서 보안 솔루션이 적용된 조직 내 네트워크로 침투하는 것보다 개인 PC에 침투하는 엔드포인트를 노린 사이버 공격이 강화되는 경향을 보였다. 특히, 랜섬웨어, APT 공격, 원격근무 중 VPN 해킹 등 지능화되고 다양한 사이버 위협이 증가되었다. 이처럼 조직의 경계가 존재하지 않고 업무환경과 구성원이 점점 분산되는 오늘날의 비즈니스 환경에서는 네트워크 경계를 기반으로 접근을 통제하는 전통적인 보안 모델은 적합하지 않다는 사실이 부각되면서 제로 트러스트(Zero Trust) 개념은 갈수록 주목을 받고 있다. 특히 주요국에서는 국가 차원에서 제로 트러스트를 단계적으로 도입 및 구축하고자 정책적으로 추진하고 있다.

2022년 10월 과학기술정보통신부와 한국인터넷진흥원(KISA)은 ‘제로 트러스트·공급망 보안 포럼’을 발족하여 제로 트러스트와 공급망 보안을 국내 정보보호환경에 도입하여 보안 패러다임의 변화에 능동적으로 대응하고 있다[1]. 또한, 최근 과학기술정보통신부는 국내 기업들을 위한 사이버 위협 선제적 대응 방안에 대한 가이드를 발표하여 제로 트러스트 기반의 기업 보안 전환의 방향성을 제시하고 있다. 美 조 바이든 대통령은 2021년 국가 사이버 보안 개선에 대한 행정명령(Executive Order on Improving the Nation’s Cybersecurity 10428)을 발표하면서 美 행정부는 2024년까지 연방정부의 사이버 보안을 현대화하고 클라우스 서비스로의 전환을 가속화하기 위해 제로 트러스트로의 전환을 요구하는 등 제로 트러스트로의 전환에 속도를 내고 있다[2,3].

본 고에서는 제로 트러스트의 의미를 정의한 후 기술동향을 살펴보고 적용사례들을 정리하여 제

로 트러스트를 구현하고자 하는 국내 주요 기관 및 기업에 조금이나마 도움을 주고자 한다.

2. 기술 표준 동향

제로 트러스트(Zero Trust)는 2010년 포레스터 리서치 수석연구원인 존 킨더버그(John Kindervag)가 제시한 개념(Concept)이다. 제로 트러스트는 "아무것도 신뢰하지 않는다"를 전제로 하며, 조직의 외부 뿐만아니라 내부에서 접근하는 사용자와 단말에 대해서도 무조건적으로 신뢰하지 않고 지속적으로 모니터링하고 검증하는 것이 기본 개념이다. 즉, 사용자 또는 단말이 리소스에 대한 접근을 요청할 때마다 신원(ID)에 대한 철저한 검증을 실시하고, 검증을 통과한다고 해도 최소한의 권한만을 부여해 접근을 허용한다는 개념이다[4,5].

제로 트러스트 아키텍처(Zero Trust Architecture)는 하나의 기술이 아니라 보안상태를 개선하기 위한 보안 모델(Security Model)로 구성요소간의 관계와 워크플로우 설계, 접근 정책, 운영 등 여러 개념을 조합한 일종의 기술 집약형 '환경'이다. 따라서 제로 트러스트 아키텍처는 조직의 사이버 보안 계획이다. 제로 트러스트 네트워크 접근(Zero Trust Network Access)는 접근 주체가 신원(ID) 또는 문맥(Context)를 기반으로 리소스에 접근시 논리적인 경계를 만들어주는 제품이나 서비스이다[4,5].

제로 트러스트의 구현은 전통적인 보안모델에서 탈피한 7가지 기본 원칙을 바탕으로 조직의 현재 상황을 판단하여 아키텍처와 핵심요소를 정의하고 단계적으로 성숙도를 향상시켜 목표로 하는 '최종단계의 보안상태'에 이르게 하는 것이다. 본 절에서는 주요 제로 트러스트 아키텍처 모델, 성숙도 모델을 소개한다.

2.1 NIST, SP 800-207의 제로 트러스트 아키텍처

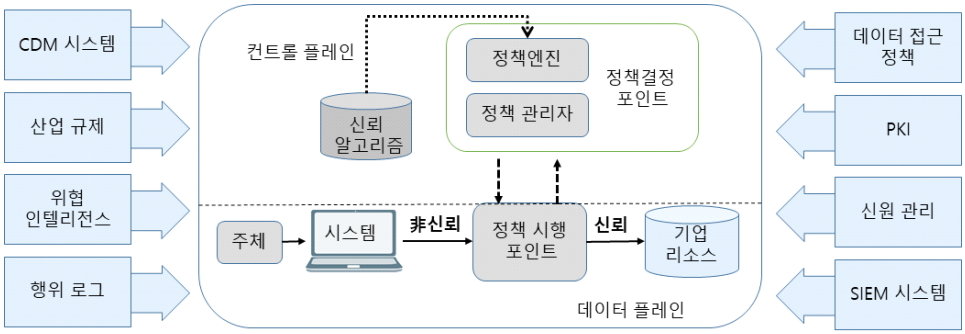
SP 800-207[4]에서는 제로 트러스트의 개념과 구성요소를 제시하고, 이를 운영할 수 있는 제로 트러스트의 아키텍처, 레거시 환경과의 연동 시나리오 등을 제시한다.

<표 1>은 제로 트러스트 구현을 위해 반드시 준수해야 할 7가지 기본 원칙과 각 원칙이 의미하는 보안 요구사항[6]을 나타낸다.

SP 800-207에서 제시하는 제로 트러스트의 논리적인 핵심 구성요소는 (그림 1)과 같이 정책 엔진(PE), 정책 관리자(PA), 정책 시행 포인트(PEP)로 구성된다. 정책 엔진은 CDM 시스템, 산업 규제, 위협 인텔리전스, 활동 로그 등 외부 소스의

〈표 1〉 SP 800-207의 제로 트러스트 7가지 기본 원칙

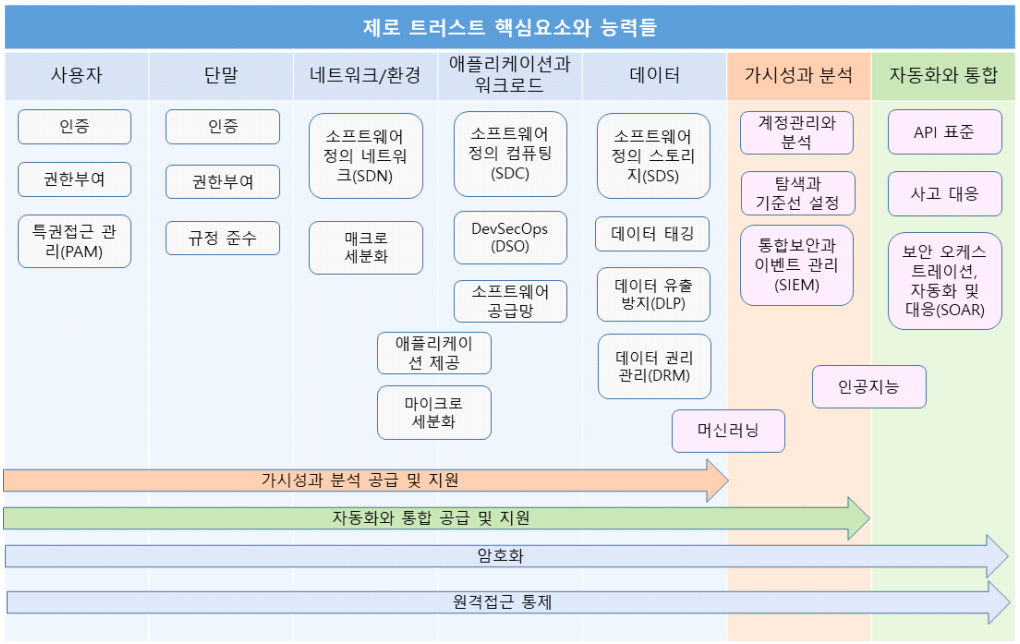
번호	기본 원칙	보안 요구사항
1	모든 데이터 소스와 컴퓨팅 서비스는 리소스로 간주한다.	리소스 식별
2	네트워크 위치와 관계없이 모든 통신을 안전하게 만든다.	안전한 통신 확보
3	조직의 리소스에 대한 접근은 각 세션 기반으로 승인된다.	접근 권한 부여
4	리소스에 대한 접근 ID, 애플리케이션, 서비스, 자산의 상태 등은 동적 정책에 의해 최소한의 권한으로 결정한다.	접근 권한 정책
5	조직은 모든 소유 및 관련 자산의 무결성과 보안 상태를 모니터링하고 점검한다.	보안상태 유지
6	모든 리소스에 대한 인증 및 승인은 동적으로 수행하고 접근을 허용하기 전에 엄격히 적용/다중요소 인증이 필요하다.	선 인증 후 접속
7	조직은 자산, 네트워크, 인프라 통신 상태를 수집하고 이를 활용해 보안상태를 개선한다.	보안상태 개선



(그림 1) 제로 트러스트의 논리적 구성요소

입력을 신뢰 알고리즘(Trust Algorithm)을 기반으로 접근 권한을 결정한다. 정책 관리자는 리소스에 접근하는 승인된 접근 주체의 인증정보, 키 또는 토큰 등을 생성하여 세션을 시작한다. 정책 시행 포인트는 게이트웨이 역할로서 모든 접근 주체의 신원(ID)에 대해 식별, 인증, 승인을 수행하고 접근 주체의 리소스 연결을 활성화하고 모니터링하거나 종료한다[4].

SP 800-207에서는 조직의 워크플로우에 따라 아키텍처를 수립할 수 있는 예시를 제공한다. 우선, 신원과 할당된 속성을 기반으로 접근을 결정하는 강화된 신원 거버넌스 접근 방법, 네트워크 세그먼트에 개별 리소스 또는 리소스 그룹을 배치할 수 있는 마이크로 세그멘테이션 접근 방법, 소프트웨어 정의 경계(SDP)를 이용한 네트워크 재구성 접근 방법이다. 또한, 정책 엔진과 정책 관리자를 하나의 서비스로 제공하거나 게이트웨이와 리소스간의 배치 및 통신 방법 등 제로 트러스트



(그림 2) 제로 트러스트 핵심요소와 능력들

의 논리적인 구성요소들을 다양하게 배치하여 조직의 상황과 목적에 적합하게 적용할 수 있는 제로 트러스트 아키텍처를 제시한다[4].

2.2 DoD, 제로 트러스트 참조 아키텍처 1.0

2021년 발표된 美 국방부(DoD)의 제로 트러스트 참조 아키텍처(Zero Trust Reference Architecture)는 제로 트러스트 구현을 위해 공통적으로 필요한 7가지 핵심요소(Pillars)와 각 요소별 필요한 일련의 활동을 수행하기 위한 방법과 수단을 조합하여 원하는 목표를 달성하는 능력들(Capabilities)을 제시하고 그들 간의 인터페이스를 정의한다[7].

제로 트러스트의 핵심요소별 능력들을 살펴보면, 첫 번째, 사용자 수준에서 제로 트러스트를 구현하기 위한 '사용자 인증', '사용자 권한 부여', '특권 접근 관리'의 능력이 정의된다. 이들 능력은 다중요소인증(MFA)와 같은 기술을 사용하여 사용자의 신원(ID)을 확인하고 최소한의 권한을 부여한다. 지속적인 인증, 권한 부여, 모니터링을 통해 모든 상호 작용을 보호하고 보안을 유지하면서 사용자의 접근 및 권한을 제어한다. 두 번째, 단말과 관련된 '단말 인증', '단말 권한 부여', '단말 규정 준수'의 능력은 단말 수준에서 제로 트러스트 개념을 구현하는 능력으로, 접근하는 모든 단말을 식별, 인증, 권한 부여, 목록 작성하고, 엔드포인트 관련 정책 및 규정을 준수하는지 검증한다.

세 번째, 네트워크/환경 수준에서는 세분화된 접근 및 정책 제한으로 네트워크 환경을 분할, 격리, 제어하는 '소프트웨어 정의 네트워킹(SDN, Software-Defined Networking)'과 '매크로 세분화(Macro Segmentation)'의 능력을 정의한다. 매크로 세분화를 통해 경계가 더욱 세분화됨에 따라 마이크로 세분화는 DAAS(Data, Application, Asset, Service)에 대한 보호 및 제어 기능을 강화하고, 특히 권한 있는 접근 제어, 내부 및 외부 데이터 흐름 관리, 측면 이동 방지를 통해 제로 트러스트를 구현한다.

네 번째, 애플리케이션/워크로드의 개발·관리 관련 능력은 온프레미스의 시스템 또는 서비스, 클라우드에서 실행되는 애플리케이션 또는 서비스를 보호하고 적절히 관리하고 개발된 소스코드와 공통 라이브러리는 처음부터 개발보안 및 운영(DevSecOps)을 통해 제로 트러스트를 구현한다. 다섯 번째, 데이터 수준에서는 DAAS를 정의 및 분류하고 스키마 개발, 미사용 및 전송 중인 데이터 암호화를 통해 제로 트러스트를 구현한다. 또한 데이터 보호를 위해 DRM, DLP, 소프트웨어 정의 스토리지(SDS) 및 세분화된 데이터 태깅과 같은 솔루션 배치를 통해 제로 트러스트 구현을 지원한다.

여섯 번째, '가시성과 분석'에 대한 능력을 통해 제로 트러스트의 보안을 위한 기준선을 설정하고, 모든 관련 보안 이벤트를 수집 및 분석한다. 또한, 인공지능 기반으로 보안 이벤트의 데이터를 연구함으로써, 비정상적인 동작의 탐지를 개선하고 보안 정책 및 실시간 접근 결정을 동적으로 변경할 수 있는 기능을 통해 제로 트러스트 구현을 지원한다.

마지막으로 '자동화와 통합'의 능력은 수동 보안 프로세스와 보안도구를 자동화하고 통합하여 자동화된 보안 대응을 통해 일관된 보안 정책을 시행하고 선제적인 명령과 제어를 통해 제로 트러스트의 개념이 구현된다.

2.3 DoD, 제로 트러스트 참조 아키텍처 2.0

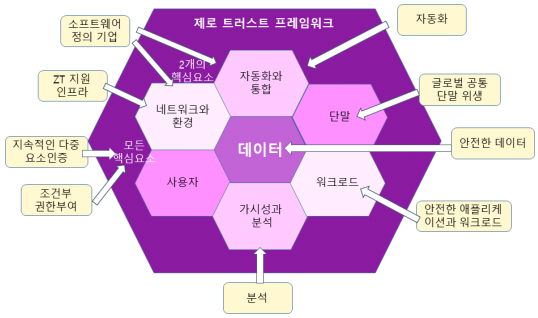
2022년 美 국방부(DoD)는 기존의 능력을 재구성하고 우선순위 변경하고 보완함으로써, 경계에서 벗어나 DAAS 보호에 중점을 둔 사이버 보안 참조 아키텍처(Cyber Security Reference Architecture)를 발표하였다[8]. 이전에 발표된 제

로 트러스트 아키텍처들과의 가장 큰 차이점은 제로 트러스트의 개념 정의를 벗어나 제로 트러스트 전환시 대두 될 수 있는 문제점들을 인식하고 이를 고려한 제로 트러스트 프레임워크와 전략을 제시한다.

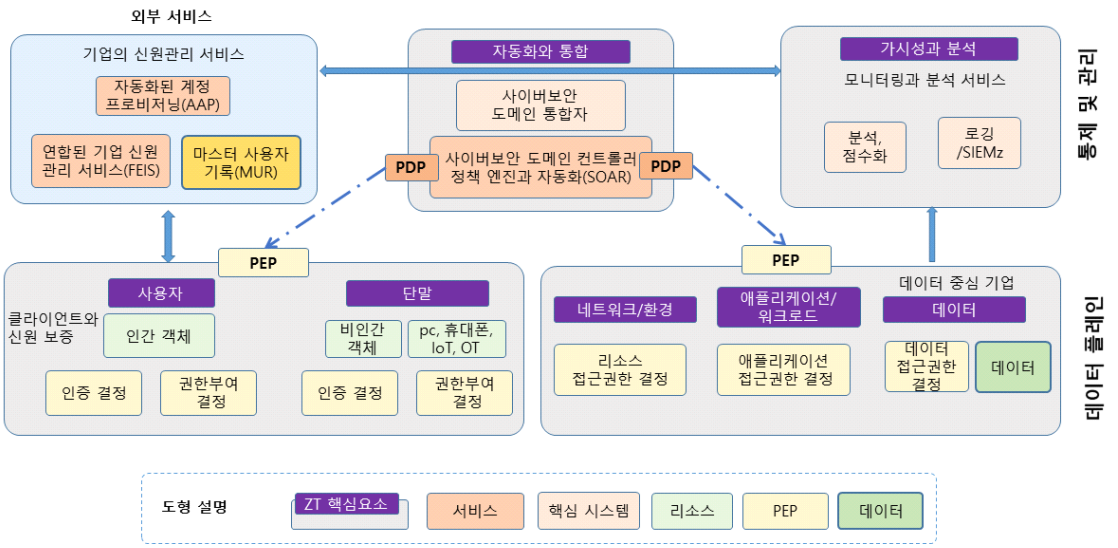
제로 트러스트의 7개 핵심요소는 운영 환경에서 제로 트러스트 기능을 수행할 수 있는 능력과 기술을 제공한다. 정의된 능력과 다수의 하위 능력은 적용가능한 현재 기술을 반영하고, 이러한 계층적인 구조는 제로 트러스트를 유연하게 통제 및 구현할 수 있도록 지원한다.

(그림 3)의 제로 트러스트 프레임워크에서 화살표는 각 능력이 어떤 핵심요소에 작용하는지를 보여준다.

(그림 4)에서는 제로 트러스트 참조 아키텍처 내에서 보안을 어떻게 구현할 지에 대한 운영적인 관점을 제시한다. 운영 흐름의 가독성을 높이기 위해 저자의 판단으로 불필요한 내용은 제거를 하였다. 우선, SIEM으로 전송된 각종 로그는 분석되어 인간객체와 비인간객체에 대한 신뢰 수준을 점수화된다. 만약 신뢰도의 점수가 측정된 임계값보다 높은 경우 요청된 인증과 권한이 부여되고, 신뢰 수준과 정의된 보안 정책에 따라 리소스, 애플리케이션, 데이터에 대한 접근 권한이 결정된다. 또한 데이터 태깅을 통해 데이터를 식별, 분류, 처리, 유지 및 폐기 등의 프로세스로 데이터를 보호 및 관리한다. 정책 엔진에서는 위협관리, 사고 대응, 정책 시행 및 보안 정책을 자동화하고 각 정책 시행 포인트로 정책을 자동으로 전달하여 제로 트러스트가 구현이 되도록 지원한다[8].



(그림 3) 제로 트러스트 프레임워크, 핵심요소에 능력 매핑



(그림 4) 제로 트러스트 참조 아키텍처 핵심요소, 리소스, 능력 매핑

2.4 제로 트러스트 성숙도 모델

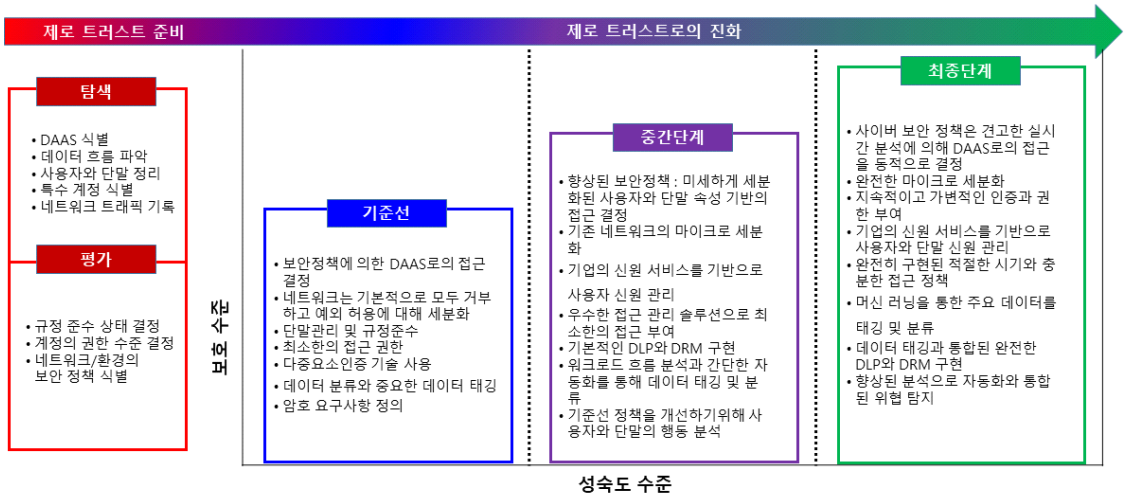
기존 아키텍처에서 제로 트러스트 최종 목표 상태로의 전환은 우선 기준선을 정의하고 능력을 향상하고, 가상화 및 자동화, 보안정책 개선과 분석을 반복적으로 수행함으로써 가능하다. 예를들어, ID와 속성 기반 인증, 권한 부여를 통합하여 엔드포인트 보안을 향상시키거나, 연결에 사용되는 단말의 규정 준수와 더불어 네트워크 접근 전에 사용자를 검증해서 이전에는 불가능 했던 위험 기반의 조건부 접근 결정을 가능하게 하는 것이다. 따라서 제로 트러스트로의 전환은 단번에 구현되는 것이라기보다 조직의 상황에 따라 단계적으로 성숙도를 향상시키는 것이다.

처음으로 미국의 NSA는 목표로 하는 제로 트러스트 아키텍처로 전환하기 위해 기존 아키텍처를 탐색 및 평가함으로써 준비작업을 수행하고, 기본, 중간, 최종 세가지 성숙도 단계를 제안하였다[9]. 美 국방부(DoD)의 제로 트러스트 참조 아키텍처 버전 1.0에서는 NSA의 성숙도 모델에 따라 (그림 5와) 같은 성숙도 모델을 제시하고 있다[10]. 각 단계에서는 능력들의 기능을 향상시키거나 새로운 기술이나 제품/서비스를 적용 및 구현하여 성숙도를 향상시키고, 최종단계에서 보안수준이 최고에 이르게 함으로써 제로 트러스트를 구현한다.

CISA는 <표 2>와 같이 NSA와는 조금 다른 성숙도 모델을 제시하였는데, 사용자, 단말, 네트워크/환경, 애플리케이션 워크로드, 데이터의 영역으로 구분하여 제로 트러스트 모델을 적용하였으며, 기존, 개선, 최적의 3단계로 성숙도를 정의한다.

3. 제로 트러스트 사례 분석

포레스트 리서치에서 '제로 트러스트 모델' 개념이 처음 제안된 이후 제로 트러스트 환경을 구현하는 방식은 접근하는 기업에 따라 차이를 보인다. 소위 빅테크 기업으로 불리는 거대 IT기업은 자사 클라우드를 중심으로 서비스 모델을 제안하고 있으며, 보안 솔루션 기업들은 기존에 보유한 솔루션을 제로 트러스트 환경에 맞게 조합한 엔터프라이즈 보안 솔루션으로 개편하여 새로운 제품을 선보이고 있다. 본 절에서는 주요 제로 트러스트 구축 사례들이 어디에 중점을 두어 제로 트러



(그림 5) 美 국방부(DoD)에서 제시한 제로 트러스트 성숙도 모델

(그림 6) CISA의 제로 트러스트 성숙도 모델

〈표 2〉 제로 트러스트 참조 아키텍처에서 대표성 있는 능력의 성숙도 정의

	△	○	◎
사용자/단말	• 인증 및 정적인 권한 부여	• MFA와 동적인 권한 부여 • IAM 구현	• 지속적인 MFA와 동적인 권한 부여 • IAM과 PAM 구현
네트워크/환경	• 매크로 세분화	• 일부 마이크로 세분화	• 완전한 마이크로 세분화
애플리케이션과 워크로드	• 대부분 VPN을 이용한 애플리케이션 접근	• 일부 VPN을 이용한 애플리케이션 접근	• VPN없이 애플릮케이션 접근
데이터	• 데이터 분류와 일부 태깅	• 데이터 태깅과 분류 • DLP 구현	• 머신러닝 통한 데이터 태깅과 분류 • 데이터 태깅과 통합된 DLP 구현
가시성과 분석	• 모니터링 제공	• 모니터링과 분석제공	• 실시간 모니터링과 분석 • 자체 SIEM 구현 • UEBA(사용자 계정 행위 분석) 구현
자동화와 통합	• 자동화 제공하지 않음	• 간단한 자동화	• 완전한 자동화 • 자체 SOAR 구현

스트를 구현하고 있는지 美 국방부의 제로 트러스트 참조 아키텍처의 핵심 요소와 능력을 기반으로 분석하였다. 다만, 공개된 자료를 통해 확인이 어려운 능력들이 다소 존재하여, <표 2>와같이 각

핵심요소에서 대표성이 있는 능력과 기술을 구현하였는지 관점에서 살펴보았다. 다만, 7가지의 핵심요소 중 사용자와 단말의 대표성 있는 능력이 동일하여 이들을 하나로 표기하였다. 또한 美 국방부와 CISA의 성숙도 모델을 참조하여 대표성 있는 각 능력의 수준을 3가지로 구분해 성숙도를 판단하였다. 마지막으로, 본 절에서 분석한 내용들은 공개된 자료들을 토대로 작성하였으며, 현재 시점에서 실제 구현이 되었지만 미공개 된 내용에 대해서는 고려하지 않았음을 전제로 한다.

국외 주요 기업에서 제로 트러스트를 구축하거나 기업차원에서 제시하는 제로 트러스트 아키텍처에 대해 <표 2>의 능력들을 구현 및 제시하고 있는지 분석하였다. 구글의 BeyondCorp은 단말 인벤토리 서비스와 MFA기반 SSO인증, IAP(Identity-Aware Proxy)접근 제어 엔진을 통한 모든 접속 요청에 대한 검증 등을 통해 사용자의 네트워크 위치에 관계없이 단말 상태와 사용자 자격증명을 기반으로 인증 및 승인, 암호화한다[11-13]. 또한 리소스에 대한 마이크로 세분화를 구현하여 VPN구현 없이 모든 네트워크와 애플리케이션에 접근하고 Chrome에 DLP를 통합하여 데이터를 보호한다. 크로니클, 맨디언트 등의 기업인수를 통해 구글 클라우드에 통합시킴으로써 위협탐지 및 대응을 자동화하고 있다[14]. 마이크로소프트는 '명확하나 검증', '최소한의 권한 접근', '침해가정'을 원칙으로 Azure Active Directory를 구축하여 단말과 사용자의 신원증명, MFA와 PAM을 제공하고 이용하여 VPN없이 네트워크와 애플리케이션에 접근가능하다. 또한 Azure 머신러닝 스튜디오를 통한 데이터 분류하고 통합된 DLP를 구현하고 있으며, Sentinel을 이용해서 사용자 및 엔터티의 동작을 제공하고 보안 위협에 대응하여 자동화 규칙과 플레이북을 사용한다[15].

아마존은 별도의 제로 트러스트 솔루션을 제공하고 있지 않으나 제로 트러스트 구현을 위한 클라우드 보안 아키텍처(ZTNA)를 제시하고 있다. 아마존의 AWS는 IAM, PAM Management Console, Verified Access 등을 이용하여 MFA와 동적인 권한을 부여하고 있으나 지속적으로 MFA를 수행하는지에 대해서는 공식적인 자료를 찾을 수는 없었다[11,16-18]. 또한 Verified Access를 사용하여 VPN없이도 애플리케이션에 접근을 제공하고 모든 접근 시도를 로깅하여 S3, Amazon CloudWath Logs, Amazone Kinesis Data Firehose등으로 전송하여 SIEM과 SOAR와 연동하여 로그를 더 쉽게 분석할 수 있다. 아마존 AWS는 자체적인 SIEM, SOAR 솔루션을 보유하고 있지 않으나 IBM, Splunk 등의 관련 제품들과 연동을 지원한다. AWS Systems Manager는 AWS 서비스의 운영 데이터를 보고 AWS 리소스 전체의 운영 작업을 자동화할 수 있는 통합 사용자 인터페이스를 제공한다[18].

블랙베리는 컨텍스트 및 위치 데이터의 실시간 분석을 사용해 행동과 위치 패턴으로 사용자와 단말을 검증하는 'Zero Touch'를 제시하고 있다. 즉, 사용자가 별도 인증 절차를 거치지 않아도 자원에 접근할 권한을 얻을 수 있고 접근에 대한 위험은 실시간으로 스코어링하여 최상의 보안 상태를 유지하는 방식이다[11,19]. 또한 지속적인 모니터링과 위험 스코어링을 모든 엔드 포인트에 적용하기 위해 인공지능 기술을 활용해 작업 맥락을 구분하고, AI가 구간별 맵핑을 반복해 Zero Trust 원칙이 지켜지는지 끊임없이 확인하고, 가시성을 지원한다. 블랙베리의 CylanceGATEWAY는 ZTNA로 애플리케이션에 동적으로 접근권한을 부여하여 위험을 줄여 VPN을 대체한다. 블랙베리 스파크는 EDR, UBEA, DLP, IAM 등 특히 엔드포인트 보안에 특화된 기능들을 제공하고 있다[11,19].

구축사례는 아니지만 눈에띄는 기업으로, 넷플릭스는 2018년 실용적인 ZTA라는 주제로 위치

〈표 3〉 주요기업의 제로 트러스트 구축/제안 사례 분석

	구글, BeyondCorp	마이크로소프트, Azure	아마존, AWS ZTA	블랙베리, Zero Touch
사용자/단말	◎	◎	○	○
네트워크/환경	◎	◎	◎	◎
애플리케이션과 워크로드	◎	◎	◎	◎
데이터	◎	◎	◎	○
가시성과 분석	◎	◎	○	○
자동화와 통합	◎	◎	○	○

독립적 보안 접근 (Location Independent Security Access, LISA)를 발표했다. 기본 전제는 애플리케이션 앞에 VPN 대신에 프록시를 설치하여 VPN을 완전히 배제하는 방식은 아니지만, 큰 비용을 들이지 않고 Zero Trust를 구현하는 방법을 제안했다. 애플리케이션 앞에 프록시를 설치해 사설 VLAN으로 보안을 강화하는 LISA의 아이디어는 현재 IoT 보안에 주로 활용되고 있다[20].

국내의 경우는 국내 인프라 운영 실정과 제도적으로 아직까지는 망분리에 초점이 맞추어져있어 전사적 관점의 제로 트러스트 모델을 적용한 사례가 많지 않지만, 대형 IT 기업, 금융 기업들을 중심으로 도입 움직임을 보이고 있다. 대표적인 기업은 NC소프트는 존 망분리 네트워크 기반 형의 보안 모델의 한계를 인지하고 제로 트러스트 모델을 도입하였으며, 마이크로소프트 솔루션을 기반으로 구축하였다[21]. 사용자 ID를 중심으로 사내 IT자원에 대한 체계적인 통제기반을 마련하고, 기계학습을 통해 악의적인 공격 및 비정상적인 사용자의 행동 패턴을 분석, 위협 요소를 사전에 감지할 수 있도록 하는 향상된 서비스를 도입하였다[21]. 다만, NC소프트는 마이크로소프트의 솔루션 모델을 차용하고 VPN을 여전히 유지하고 있으며, 재택근무 분야에 한정된 제로 트러스트 모델이기 때문에 과도기라고 볼 수 있다. NC소프트는 제로 트러스트 보안 모델을 전사적으로 도입하기 위해 가장 앞서 있는 것은 사실이지만, 해외 사례와 달리 마이크로소프트 솔루션 중심이기 때문에 사용자 인증 등에서 윈도우 계열 종속이 심하다는 단점이 있다.

제로 트러스트 솔루션 및 서비스 등을 자사의 인프라 환경에 도입한 국내 사례는 일부 있지만, 제로 트러스트를 제품화하여 공급한 국내 제조사는 적다. 지니언스의 Genian ZTNA는 FIDO, OAuth 등 다양한 인증과의 연동을 지원하고 SD-WAN, SDP 등 SDx기술과 네트워크 가상화를 통해 유연한 네트워크 환경 구성을 지원한다. 또한 클라우드에서 애플리케이션까지 가시성을 확보할 수 있으며, IoT/IIoT에 특화된 탐지 및 정보를 제공하고 마지막으로 마이크로 세분화 구현으로 유연하고 세밀한 접근 통제를 제공하고 있다[22].

4. 시사점

본고에서는 제로 트러스트의 기술 동향을 정리하고 주요 구축 사례를 美 국방부의 제로 트러스트 참조 아키텍처의 대표적인 능력과 기술을 기반으로 구현의 성숙도를 살펴보았다. 해외에서는 특히 미국의 정부와 기업을 중심으로 제로 트러스트로의 전환을 가속화 하고 있고, 국내의 경우에는 일부 기업에서 도입을 하고 있으나 주로 해외 특정 솔루션을 기반으로 구축한 사례들이 대부분이

며 그 안을 자세히 들여다보면 아직 과도기 단계에 머물러 있어 내재화 되기까지는 상당 시일이 걸릴 것으로 보여진다.

그러나 포스트 코로나 이후 디지털 전환이 가속화됨에 따라 경계기반의 보안 모델에서 데이터 중심의 보안모델로의 전환은 당연한 현상이 되었고 우리에게 닥친 당면 과제라고 볼 수 있다. 따라서 정부차원에서 제로 트러스트 기술 확보를 위한 연구, 기술개발 등을 적극 지원하고, 제로 트러스트 전환을 위해 망분리 의무화 등의 걸림돌이 될 수 있는 요소들을 제거하는 등 제도적 기반 마련을 우선적으로 고려할 필요가 있다.

참 고 문 헌

[1] 과기정통부, '제로트러스트 · 공급망 보안' 포럼 발족, https://zdnet.co.kr/view/?no=20221026161607

[2] 美 국방부의 제로 트러스트 개념과 시사점, 이경복, 안영오, 제1900호(22-21), 국방논단, 2022

[3] 제로 트러스트 보안기술 동향과 적용방안, 이후기, KCISA 2022-6호(제36호), 2022.

[4] NIST, SP 800-207 Zero trust architecture, 2020

[5] 제로트러스트(Zero Trust)의 올바른 이해, https://www.genians.co.kr/resources/genian-blog/ genian-nac-blog/zt,

[6] '사이버보안 강화를 위한 제로트러스트 활용 및 구축방안', 박완성, 제19회 해킹보안 세미나

[7] DoD, Department of Defense (DoD) Zero Trust Reference Architecture Version 1.0, 2021

[8] DoD, Department of Defense (DoD) Zero Trust Reference Architecture Version 2.0, 2022

[9] NSA, Embracing a Zero Trust Security Model, 2021

[10] CISA, CISA Zero Trust Maturity Model, 2021

[11] 사이버 보안의 대세는 'Zero Trust', 7가지 기본 원칙을 살펴보자!, LG CNS Tech,https://www.lgcns.com/blog/cns-tech/security/31896/

[12] Google BeyondCorp, https://www.beyondcorp.com

[13] 구글, '비욘드코프 리모트 액세스'로 제로 트러스트 시장 진입, https://www.itworld.co.kr/ news/150716

[14] 맨디언트 인수로 구글이 얻는 것, '클라우드-엔드투엔드 보안', https://byline.network/2022 /03/10-213/

[15] Microsoft Azure, https://learn.microsoft.com/ko-kr/azure

[16] Amazon AWS, https://aws.amazon.com/

[17] PAM and AWS: Keeping pace with AWS privileged accounts, https://security boulevard.com/2020/02/pam-and-aws-keeping-pace-with-aws-privileged-accounts

[18] Building a Zero Trust Architecture In AWS, https://im5tu.io/article/2020/12/building-a- zero-trust-architecture-in-aws

[19] Blackberry CylanceGATEWAY, https://www.blackberry.com/us/en/products/ cylance-endpoint-security/cylance-gateway

[20] LISA(Location Independent Security Access, LISA): A Practical Zero Trust Architecture, https://www.usenix.org/conference/enigma2018/presentation/zimmer

[21 NC소프트의 Zero Trust를 통한 디지털트랜스포메이션 여정, https://www.youtube.com/ watch?v=cQYaY9U7JeA

[22] Genians, https://www.genians.co.kr/products/genian-ztna/

저 자 약 력

이 송 희

이메일 : sophie@kopo.ac.kr

- 2009년 고려대학교 컴퓨터학과 (박사)
- 2009년~2012년 고려대학교 연구교수
- 2012년~2020년 한국인터넷진흥원 책임연구원
- 2020년~현재 한국폴리텍대학 사이버보안과 교수
- 관심분야 : 정보보호제품 평가 및 인증, 제로 트러스트, AI 보안 등

조 원 배

이메일 : wbcho@kisa.or.kr

- 2016년~현재 한국인터넷진흥원 선임연구원
- 2017년 조선대학교 컴퓨터공학과 (학사)
- 관심분야 : ISMS-P, 제로 트러스트, 개인정보보호, 클라우드