정 보 보 호 학 회 지
제34권 제3호, 2024. 6

NIST 7 Tenets 기반 제로 트러스트 표준 모델 점검 항목

최 여 정*, 정 윤 정**, 이 만 희***

요 약

오늘날 보안 패러다임은 경계 기반 보안 체계에서 제로 트러스트로 변화하고 있다. 이에 NIST는 NIST SP 800-207(Zero Trust Architecture)을 발간하며 제로 트러스트 기본 원칙인 7 Tenets를 제시하였다. 하지만 7 Tenets에 대한 구체적인 구현 및 검증 방안이 부재하여, 제로 트러스트 기술 적용 범위를 정하는 데 어려움을 겪고 있다. 이에 본 논문은 제로 트러스트 제품이 제로 트러스트 표준 모델에 부합하는지 검증할 수 있는 NIST 7 Tenets 기반 점검 항목을 제안한다. 점검 항목은 총 59개의 문항으로, 필수적으로 요구되는 필수 기능 28개와 선택적으로 요구되는 선택 기능 31개로 구성된다. 수립한 내용에 근거하여 5개의 기업 제품을 검증한 결과, 필수 기능을 모두 만족하는 제품은 없었으며 적용된 제로 트러스트 원칙이 상이함을 확인하였다. 이는 본 논문에서 제안한 점검 항목을 통한 제품의 표준 모델 부합성 검증이 가능함을 보여주며, 향후 국가·공공기관에서의 제로 트러스트 사용 및 유연한 국외 제품 도입 시 활용될 것으로 기대한다.

Ⅰ. 서 론

기존 네트워크는 경계 기반 보안(perimeter security) 솔루션을 이용하여 외부 사용자로부터 네트워크를 보호하였으나[1], 내부 사용자에 의한 보안사고, 새로운 유형의 공격 벡터(attack vector), 권한 탈취 기반 공격 증대 등의 보안 문제가 지속적으로 발생하고 있다. 이처럼 기존 보안 모델을 통한 네트워크 보호가 어려워짐에 다양한 위협 가능성을 고려한 고도화된 보안 모델로 제로 트러스트(zero trust)가 대두되고 있다[2].

제로 트러스트는 위치, 사용 이력과 관계없이 네트워크 및 자원에 접근하는 모든 사용자를 인증한 후 최소 접근 권한만 제공하는 보안 모델이다. MFA(Multi-Factor Authentication), 제로 트러스트 기반의 PIM(Privileged Identity Management), PAM (Privileged Access Management) 등 인증 모듈을 통해 사용자의 이용 환경을 확인하며 공격표면(attack surface)을 축소 시킨다[3][4][5]. 이처럼 비신뢰를 전제로 모든 패킷에 대해 지속적이고 세밀하게 통제하여 네트워크의 안전성을 확보하는 동시에 자원을 보호한다.

이에 미국은 정부 주도하에 제로 트러스트 보안 전략 및 관련 정책을 추진하고 있다[6]. 2021년 5월, 美 바이든 정부는 ‘EO(Executive Order) 14028’을 통해 사이버 보안을 현대화하기 위한 지향점으로 제로 트러스트를 지목하며 연방 정부의 제로 트러스트 도입을 공식화하였다. 이외에도 영국, 일본 등 주요국은 제로 트러스트를 도입하기 위한 국가 차원의 전략을 발표하고 있다. 하지만 제로 트러스트 기능 요구사항에 대한 명확한 기준이 마련되지 않아, 다양한 기업에서 강조하는 제로 트러스트 기술 구현에 대한 사실 여부를 확인하는 데 고충을 겪고 있다. 또한, 제로 트러스트 도입 기관이 구현해야 하는 기술 수준의 범위 역시 모호한 실정이다.

국내 역시, 새로운 보안 체계로 전환하기 위해 제로 트러스트 도입 방법론으로 전망되는 ‘제로 트러스트 가이드라인 2.0’ 공개를 앞두며 국가적 차원의 도입을 추진하고 있다. 또한, 기존 보안 모델 대비 보안성이 41% 향상된 ‘K-제로 트러스트 기본모델’ 2종을 발표

본 연구는 ETRI부설연구소의 위탁연구과제(2022-134)로 수행하였습니다.
이 논문의 내용을 발표하는 때에는 ETRI부설연구소에서 수행한 위탁결과임을 밝혀야 합니다.
본 논문에 기술된 점검 항목, 제품 점검 결과 및 적용 가능성 등의 의견은 연구 위탁기관과 무관합니다.
* 국가보안기술연구소 (연구원, choiyeojeong98@gmail.com)
** 한남대학교 컴퓨터공학과 (대학원생, jeongyunjeong.hnu@gmail.com)
*** 한남대학교 컴퓨터공학과 (교수, manheelee@hnu.kr)

하였다. 자체적으로 평가 지표를 생성한 후 보안성을 검토한 것으로, 제로 트러스트 도입과 관련하여 구체적인 기술 평가 기준이 부재한 상황이다. 이에 제로 트러스트 도입에 따른 보안성 검토를 위한 기술적 연구가 필요하다.

제로 트러스트는 국내외를 불문하고 보안분야의 이슈로 자리잡았지만, 기술 도입에 따른 보안성 검토에 대한 연구는 미비하다. 2020년 8월, NIST는 제로 트러스트의 개념 및 원칙이 포함된 'NIST 800-207(Zero Trust Architecture)'를 공개하며 ZTA가 포함해야할 기본 원칙 7가지를 제시했다. 하지만 해당 문건 역시 7 Tenets를 구현하기 위한 세부적 구현 방안이 부재하여, 특정 제품이 제로 트러스트를 제대로 구현했는지에 대한 점검 방안으로 사용하기 어려운 상황이다.

본 논문은 NIST가 제시한 7 Tenets를 분석하고, 이를 기반으로 제로 트러스트가 적용된 제품의 주요 기능 및 안전성을 검증하기 위한 점검 항목을 도출하였다. 점검 항목은 총 59개의 문항으로, 필수적으로 요구되는 필수 기능 28개와 선택적으로 요구되는 선택 기능 31개로 구성된다. 수립한 내용에 근거하여 5개의 기업 제품을 검증한 결과, 필수 기능을 모두 만족하는 제품은 없었으며 적용된 제로 트러스트 원칙이 상이함을 확인하였다. 이는 본 논문에서 제안한 점검 항목을 통한 제품의 제로트러스트 표준 모델 부합여부 검증이 가능함을 보여주며, 향후 국가·공공기관에서의 제로 트러스트 사용 및 유연한 국외 제품 도입 시 활용할 것으로 기대한다.

본 논문은 다음과 같이 구성된다. 먼저 2장에서 제로 트러스트에 관한 개념적 지식 및 국내외 사이버 보안 동향에 관해 기술한다. 그 후, 3장에서 NIST에서 제시한 7 Tenets에 관해 설명하며 제로 트러스트 적용 제품의 점검 항목을 제안한다. 4장에서는 제안한 점검 항목에 근거하여 5개 제품에 대해 검증하며 5장에서 결론을 맺는다.

Ⅱ. 배경지식

2.1. 제로 트러스트

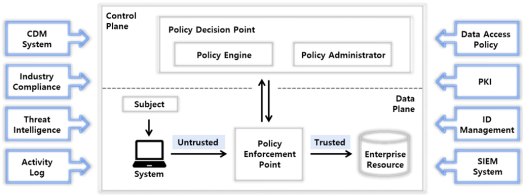
제로 트러스트는 비신뢰를 바탕으로 자원에 접근 가능한 사용자나 장치에 대한 신원 및 접근 권한을 증명하는 네트워크 보안 모델이다[7]. '보안시스템을 통과하여 IT(Information Technology) 시스템에 접속한 모든 사용자나 단말기는 신뢰하지 않는다.'를 전제로, 이용 환경, 요청 컨텍스트(context) 등 사용자나 장치에 대한 다양한 정보를 수집하여 신원을 확인하고 RBAC(Role-Based Access Control)를 통해 최소한의 권한만 부여한다. 이에 권외 활동을 수행하기 위해서, 사용자는 거듭된 인증 절차를 통해 권한을 획득해야 한다. 즉, 인증을 통한 권한 부여 과정은 이전의 사용 이력과 관계없이 네트워크 및 자원에 접근할 때마다 진행됨을 의미한다. 또한, 보안성 확보를 위해 사용자 신원 확인에 있어 MFA, PIM 및 PAM과 같은 인증 모듈을 사용한다. 더불어 네트워크를 통해 들어오는 모든 패킷을 지속해서 관리하며, 자원에 대해 접근 권한이 부여된 계정의 활동, 세션 로그를 지속적으로 모니터링하여 유효성을 입증한다. 이때 이상 행위가 탐지된 계정은 제공된 권한을 회수하고 접근이 제한된다.

제로 트러스트는 발생 가능한 모든 위험성을 고려하여 IP 별로 접속 시스템 및 서비스의 사용을 통제한다. 개별적인 자원 관리로 보안 위협에 대한 빠른 대응이 가능해졌으며, 이는 기존 네트워크 보안 모델이 지닌 허용된 계정에 대한 특정 서비스, 단말기 제재 불가능의 문제점을 보완하였다[8]. 또한, 인증에 중점을 두어 사이버 위협 차단 정책으로 신뢰 가능한 데이터를 모아놓은 화이트리스트(whitelist)에 기반하여 인가된 사용자 및 장치만 자원에 접근 가능하도록 한다. 하지만, 기존 장비와 네트워크를 재구성함에 따라 구축이 장기화 될 수 있으며, 광범위한 작업 환경으로 다양한 사용자 형태가 등장하여 정책 관리의 어려움이 발생할 수 있다.

2.2. 제로 트러스트 아키텍처

제로 트러스트에 기반 한 ZTA는 기업 내 구성 요소 간의 관계, 워크플로 계획 및 접근 정책을 적용하기 위한 사이버 보안 계획이다[9][10]. PEP(Policy Enforcement Point), PDP(Policy Division Point), PE(Policy Engine), PA(Policy Administrator), 데이터 소스로 구성되며 역할은 다음과 같다.

- PEP : PDP에 요청 전달, 사용자와 자원 사이의 게이트웨이, 네트워크 모니터링
- PDP : 사용자와 기업 자원의 통신 활성화 및 종



〔그림 1〕 ZTA의 핵심 구성 요소

료 결정

- PA : 사용자와 자원의 통신 경로 설정, 자격 증명 생성
- PE : 사용자의 자원 접근 권한 부여에 대한 최종 결정
- 데이터 소스 : 기업 내 자산 현황

사용자의 접근 권한 획득 과정은 [그림 1]과 같다. 자원에 대한 사용자의 접근 요청은 PEP를 통해 PE와 PA로 구성된 PDP로 전달된다. 이에 PE는 권한 제공 여부를 판단하기 위해 TA(Trust Algorithm) 알고리즘의 입력값인 외부 및 데이터 소스의 가중치를 평가하며 기업 내 상황을 확인한다. TA는 권한 제공에 있어 사용자 및 기업의 자산 현황 등에 대해 평가하는 알고리즘으로, 입력되는 데이터 소스는 CDM(Continuous Diagnostics and Mitigation) 시스템, 산업 규정 준수 시스템, 위협 정보, 행동 로그, 데이터 접근정책, PKI, ID 관리 시스템, SIEM(Security Information and Event Management) 시스템으로 구성된다. PE의 결정에 따라 PA는 사용자와 자원 간의 통신 경로를 설정하고 세션별 자격 증명을 생성한다. 이와 같이 사용자와 자원 간 통신에 대한 결정을 확립한 PDP는 PEP에 전달하여 연결을 활성화하며 업무 수행이 가능하도록 한다.

ZTA 구현에 있어, PDP는 사용자와 자원 간 통신 설정에 많은 영향을 주며 네트워크의 성능을 좌우한다. 따라서 PA와 PE의 적절한 구성 및 유지관리가 필요하며 보다 안전한 환경에 배치하는 것이 중요하다[11]. 또한, 사용자에 대한 실효성 및 신뢰 수준을 확보하는 것 역시 ZTA 구현의 주요 사항 중 하나이다. 이에 지속적으로 사용자 인증을 수행하고, 최소 권한 제공 및 접근 제어를 충족하여 자원에 대해 세분화된 가시성을 확보해야한다[12].

2.3. 국내외 사이버 보안 동향

2021년 5월, 美 바이든 정부는 솔라윈즈(solarwinds) 공격과 같이 정교해지는 사이버 위협으로부터 주요 안보 기관을 보호하기 위해 EO 14028을 발표했다[13]. 그 중 'Sec. 3. Modernizing Federal Government Cybersecurity.'를 통해 사이버 보안을 현대화하기 위한 지향점으로 ZTA를 지목하며, 명령일로부터 60일 이내 NIST를 중심으로 ZTA 구현 계획을 수립하고 관련 보고서를 OMB(Office of Management and Budget)와 APNSA(Assistant to the President for National Security Affairs)에 제공할 것을 명시하고 있다. 이에 NIST는 ZTA 개념과 원칙이 제시된 'NIST SP 800-207'을 바탕으로 Appgate, Google Cloud, Palo Alto Networks 등 24개의 기업과 함께 시현하였으며, 수립된 제로 트러스트 구현 계획은 'NIST SP 1800-35'를 통해 제공하고 있다[14].

또한, 2022년 1월 OMB는 EO 14028에 근거하여 'M-22-09 Federal Zero Trust Strategy'을 발행했다[15]. 해당 문서는 전 분야에 걸쳐 미국의 주요 시스템 및 데이터를 보호하기 위해 CISA에서 개발한 ZTMM(Zero Trust Maturity Model)에 기반하여 연방 정부의 ZTA 전략을 제시한다. 정교해지고 있는 피싱(phishing)에 대응하기 위한 방안으로 엔터프라이즈 ID, 접근 제어를 사용하는 MFA를 통해 새로운 접근 제어 규정을 수립하여 ID 시스템을 통합하고, 연방 보안 팀과 데이터 팀이 협력하여 중요 데이터에 대한 접근을 자동으로 탐지 및 차단하기 위한 보안 규칙을 개발할 것을 명시하고 있다. 이에 2024년 연방 회계 연도 말까지 문서에 제시된 구체적인 제로 트러스트 보안 목표를 달성하기 위해 노력하고 있다. 이처럼 미국이 제로 트러스트 표준화를 위해 움직이고 있으며, 이외에도 영국, 일본 등 주요국이 제로 트러스트 도입을 위해 국가 차원의 전략을 발표하고 있다.

한편, 과학기술정보통신부와 한국인터넷진흥원은 '제로 트러스트 가이드라인 2.0'(이하 가이드라인 2.0) 공개를 앞두고 있다[16][17]. 제로 트러스트 도입 방법론을 제시하는 데 초점을 둘 것으로 전망되는 문건으로, 앞서 2023년 7월에 발표된 '제로 트러스트 가이드라인 1.0'(이하 가이드라인 1.0)을 보완하는 데 주력할 것으로 예상된다. 가이드라인 1.0은 국내 공공기관과 기업을 위해 ZTA의 개념 및 핵심 원리를 정의하였다

[18]. 하지만 제로 트러스트 도입을 위한 참조 모델, 도입 검증 방안 등 실질적으로 기업이 적용하기 위한 세부 규정이 부재하였다. 이에 가이드라인 2.0은 수요 기관의 제로 트러스트 도입을 위해 가이드라인 1.0에 대한 의견을 수렴하고, 실증 사업 결과를 반영할 예정이다.

실증 사업 중 하나로, 2023년 12월 과학기술정보통신부와 한국인터넷진흥원은 클라우드, 온프레미스 등 국내 기업망 환경에 적용할 수 있는 'K-제로 트러스트 기본모델' 2종을 발표하였다[19]. 가이드라인 1.0을 준수한 최초의 보안 모델로, 기존 보안 대비 보안성이 41% 향상되었다. 기본모델 2종은 각각 TTA '시험인증 서비스' 및 성숙도 모델 기반 시나리오를 통해 자체 효과성 검증을 수행하였으며, 해당 실증 사업 결과는 가이드라인 2.0에 반영하여 고도화될 예정이다. 하지만 국내의 경우 제로 트러스트 개념 확립 및 도입 초기 단계로, 제로 트러스트 기반 제품의 보안성을 확인하기 위한 직접적 규정 및 평가 지표가 마련되어 있지 않아 자체적으로 평가 지표를 정의하여 진행하고 있는 실정이다.

Ⅲ. 제로 트러스트 적용 제품의 점검 항목

본 절에서는 NIST에서 발간한 'NIST SP 800-207'을 통해 ZTA의 기본 원칙인 7 Tenets에 대해 설명하고, 아키텍처 관점에서 요구되는 기능 및 필수 항목을 도출한다. 그 후, 도출한 결과를 바탕으로 제로 트러스트가 적용된 제품의 주요 기능 및 안전성 검증 방법을 수립하며 제품 개발에 대한 점검 항목을 제안한다.

3.1. 수립 요건

NIST는 'NIST SP 800-207'을 통해 ZTA가 포함해야하는 제로 트러스트 기본 원칙인 7 Tenets를 제시했다[8][20]. 'NIST SP 800-207'은 제로 트러스트를 이용하여 기업의 보안 아키텍처를 개선하기 위한 사이버 보안 지침서로, 7 Tenets는 [표 1]과 같다.

본 원칙은 ZTA 설계 시 필수로 요구되는 구현 요소가 아니므로, 일부만을 적용한 제품 개발이 가능하다. 이에 국외 기업은 해당 원칙을 바탕으로 제로 트러스트 기반 CASB(Cloud Access Security Broker), SASE(Secure Access Service Edge), SD-WAN (Software-Defined WAN), SDP(Software Defined Perimeter), SWG(Secure Web Gateway) 등 다양한 제품을 생산하고 있다. 하지만 제품 공정 과정에서의 지침서 준수 여부와 평가 과정에서의 공정성을 확인하기 위한 명확한 가이드라인이 존재하지 않아 기술 도입은 어려운 상황이다. 또한 국내의 경우, 제로 트러스트 가이드라인이 제공되고 있으나 ZTA 개념 확립에 중점을 두어 제품의 안전성 확인을 위한 구체적인 방안이 부족한 실정이다. 따라서 유연한 국외 기술 도입과 국내 제품에 대한 구체적이고 기술적인 안전성 검증을 위해 7 Tenets에 근거하여 제로 트러스트가 적용된 제품 검증 방법을 수립한다.

3.2. 점검 항목

앞서 설명한 7 Tenets를 기반으로 도출한 점검 항목은 [표 1]과 같다. 기본 원칙에 근거하여 세부적인 기능 및 관리 프로세스의 요구사항을 정의한 것으로 통신 관련 보안 정책, 사용자 인증 및 권한 제공, 트랜잭션 중 사용자 및 리소스 모니터링 등에 대해 확인한다. 점검 항목은 총 59개의 문항으로 구성되며, 28개의 필수 기능과 31개의 선택 기능으로 구분된다. 필수 기능은 각 원칙의 대표 내용에 기반 한 문항으로, 제품 검증 시 필수로 요구되며 진한 글씨로 표기하였다. 선택 기능은 각 원칙의 세부 내용에 기반을 둔 문항이며 제품 검증 시 필수가 아닌 선택 사항으로 구분된다.

Ⅳ. 제로 트러스트 적용 제품 분석

4.1. 제품 선정 및 분석 방법

본 논문에서 제안한 점검 항목의 실효성을 확인하기 위한 제품 검증은 3개의 국외 제품과 2개의 국내 제품으로 수행된다. 국외의 경우 제로 트러스트 사이버 보안 기업 Top 10에 선정된 기업의 제품 중 3개, 국내 기업 제품 2개를 선정했다.

제품을 검증하기 위해선 먼저 작동 방식 및 주요 기능을 파악해야한다. 이에 기업에서 발간한 제품 설명서 및 연구 보고서 등을 통해 정보를 수집하였다. 해당 자료는 제품 검증에 있어 중요한 평가 자료로, 이후 제안한 점검 항목[표 1]에 근거하여 기능의 유무를 확인한다. 모든 항목을 만족할 경우 1점, 일부만 만족하는 경우 0.5점, 만족하지 않은 경우 0점으로 평가한다.

〔표 1〕 제안된 점검 항목

No.	Security Requirements
1	**디바이스 운영체제 유무, HW/SW, 디바이스 위치 등과 관계없이 데이터 송신 기능이 있는 모든 디바이스를 리소스로 식별할 수 있는가?**
	모든 컴퓨팅 자원을 리소스로 관리할 수 있는가?
	모든 응용 서비스를 리소스로 관리할 수 있는가?
	필요시, 개인 소유 장치를 리소스로 관리할 수 있는가?
2	**내부에서 요청한 접근에 대해 인증을 진행할 수 있는가?**
	외부에서 요청한 접근에 대해 인증을 진행할 수 있는가?
	내•외부 접근 요청에 대해 동일한 보안 요구사항을 적용할 수 있는가?
	내부에서 요청한 접근에 대한 자동 인증을 차단하는 기능이 있는가?
	내•외부 통신의 무결성을 보장하는 기술이 있는가?
	내•외부 통신의 기밀성을 보장하는 기술이 있는가?
	모든 타입의 내·외부 통신 소스를 인증할 수 있는가?
3	**리소스에 대한 접근 제어를 세션 별로 진행하는가?**
	리소스에 대한 작업 권한을 세션 별로 제공하는가?
	업무 수행에 필요한 최소한의 권한을 명세할 수 있는가?
	업무 수행에 필요한 최소한의 권한만을 부여할 수 있는가?
	허가된 권한에 대한 유효기간을 설정할 수 있는가?
	리소스 별로 인증/인가를 적용할 수 있는가?
	한 리소스에 대한 접근 허가가 다른 리소스에 대한 접근 허가로 자동 부여되는 것을 차단하는 기능이 있는가?
4	**리소스에 대한 접근은 요청자 신원 상태, 요청 자산 상태 등을 고려하는 동적 정책에 의해 결정할 수 있는가?**
	리소스에 대한 접근 결정에 행동 속성, 환경 속성을 고려할 수 있는가? **가. 요청자와 디바이스의 행동 속성을 관리할 수 있는가?** 1. 요청자의 행위를 관찰 및 분석할 수 있는가? 2. 디바이스의 행위를 관찰 및 분석할 수 있는가? 3. 요청자 및 디바이스의 사용 패턴 자동 분석을 통해 비정상 행위를 식별할 수 있는가? **나. 환경 속성을 관리할 수 있는가?** 1. 요청자의 네트워크 위치를 고려할 수 있는가? 2. 요청 및 접근 시간을 고려할 수 있는가? 3. 현재 발생 중인 공격을 고려할 수 있는가?
	요청자 신원 상태 관리를 위해 계정 외에 다양한 추가 속성을 관리할 수 있는가? **가. 요청자의 디바이스 상태를 관리할 수 있는가?** 1. 디바이스의 SW 버전을 식별할 수 있는가? 2. 디바이스의 네트워크 위치를 식별할 수 있는가? 3. 접근 요청이 발생한 시간/날짜를 식별할 수 있는가? 4. 해당 디바이스의 이전 행위 기록에 대한 로그를 관리할 수 있는가? 5. 디바이스에 저장된 인증 정보를 확인할 수 있는가?
	비즈니스 프로세스의 요구사항을 동적 정책에 반영할 수 있는가?
	기업이 감내할 수 있는 위험 수준을 동적 정책에 반영할 수 있는가?
	리소스/데이터의 민감도를 동적 정책에 반영할 수 있는가?
	최소 접근 권한 원칙을 접근성과 가시성에 적용할 수 있는가?

No.	Security Requirements
5	**모든 자산의 무결성, 보안상태를 모니터링 및 평가할 수 있는가?**
	무 인증 접근 자산을 식별하고 차단할 수 있는가?
	CDM(Continuous Diagnostics and Mitigation) 및 유사 시스템 구축을 통해 자산/애플리케이션 모니터링을 할 수 있는가?
	기업은 필요시 자산에 대한 패치를 적용할 수 있는가?
	안전하지 않은 자산은 보안성이 확인된 자산과 다르게 처리할 수 있는가? 가. 침해가 발견된 자산에 대해 접속을 차단할 수 있는가? 나. 알려진 취약점이 있는 자산에 대해 접속을 차단할 수 있는가? 다. 관리되지 않는 자산에 대해 접속을 차단할 수 있는가? 라. 기업 소유가 아닌 자산에도 상기의 정책을 적용할 수 있는가?
	모니터링 및 리포팅 시스템 구축을 통해 기업 리소스의 상태에 대한 정보를 제공할 수 있는가?
6	**모든 리소스에 대한 접근은 동적이며, 접근 허가 전에 인증/인가를 반드시 수행할 수 있도록 강제할 수 있는가?**
	ICAM 또는 자산 관리 시스템 도입을 통해 신원, 인증, 접근, 자산 관리를 할 수 있는가?
	리소스에 접근하기 위해 MFA 사용할 수 있는가?
	트랜잭션이 진행되는 동안 지속적으로 모니터링할 수 있는가?
	필요시 (시간, 새 리소스 접근 요청, 리소스 수정, 비정상적인 활동 감지 등) 재인증/재인가를 요청할 수 있는가?
7	**기업은 자산에 대한 정보를 실시간으로 수집할 수 있는가?**
	기업은 네트워크 인프라스트럭쳐 및 통신에 대한 정보를 실시간으로 수집할 수 있는가?
	기업은 수집한 데이터를 분석할 수 있는가?
	기업은 데이터 분석 결과를 보안 정책 개선에 활용할 수 있는가?
	수집한 데이터를 통해 사용자의 접근 요청 컨텍스트 파악에 활용할 수 있는가?

4.2. 검증 결과

앞서 수집한 5개 제품에 대한 안전성 검증을 수행하였다. [표 2]는 제품별 검증 결과로, 결과표의 카테고리는 기업별 제품명을 의미하며 각 문항에 대한 만족도를 나타낸다. 본 검증은 수집한 기업의 제품 기능 및 작동 방식이 정확하다는 가정하에 수행하였다.

검증 결과, 제품별 만족도는 A 제품 24개, B 제품 29.5개, C 제품 15.5개, D 제품 20.5개, E 제품 31개임을 확인하였다. 59개의 점검 항목을 모두 만족하는 제품은 없었으며 필수 기능을 모두 만족하는 제품 역시 없었다. 본 논문에서 제안한 점검 항목은 제품별로

〔표 2〕 기업별 제품 평가

No.	A 제품	B 제품	C 제품	D 제품	E 제품
1 (4)	0	4	0	2	4
2 (7)	5	5	5	3	5
3 (7)	7	5	4	1	5
4 (7)	2	5.5	3.5	3	3.5
5 (6)	2.5	3.5	0.5	4	5.5
6 (5)	3.5	3	2.5	3.5	4
7 (5)	4	3.5	0	4	4
Total (41)	24	29.5	15.5	20.5	31

적용되는 제로 트러스트 원칙이 상이함을 확인하며 그 실효성을 증명하였다.

Ⅴ. 결 론

본 논문은 제로 트러스트가 적용된 제품의 제로 트러스트 표준 모델 부합성 검증을 위한 점검 항목을 제안하였다. 기존 네트워크 보안 시스템은 광범위한 작업 공간으로 자원의 접근 경로가 다양해짐에 따라 새로운 보안 취약점이 등장하고 있지만, 제로 트러스트는 비신뢰를 기반으로 공격 표면을 축소시켜 네트워크 및 기업 자원에 대한 안전성을 확보한다. 이에 제로 트러스트 적용 제품에 대한 국내 점검 항목으로 NIST 지침서 기반의 기능 요구사항 및 필수 가정을 도출하였다. 또한, 도출한 점검 항목에 근거하여 5개의 제로 트러스트 제품 검증을 진행했다. 검증 결과, 필수 기능을 모두 만족하는 제품은 없었으며, 제품별로 적용되는 제로 트러스트 원칙이 상이함을 확인할 수 있었다. 이를 통해 본 논문에서 제안한 점검 항목의 실효성을 입증하였다.

본 연구를 통해 제로 트러스트 보안 모델의 개념을 확립하고 보안 침해 요소를 파악하여 제품의 안전성 검증에 기여할 것으로 예상한다. 또한, 향상된 보안을 제공함에 따라 향후 국가·공공기관의 제로 트러스트가 적용된 제품 도입이 가능해질 것으로 기대된다. 더불어 7 Tenets에 기반함에 국외 제품의 유연한 도입이 가능할 것으로 예상한다.

참 고 문 헌

[1] GETVOIP, “What is VoIP VPN? Benefits, Top Providers, and More,” Aug. 2021, https://getvoip.com/blog/voip-vpn/.

[2] Vasu Jakkal, “Zero Trust Adoption Report,” Microsoft Security, Jul. 2021.

[3] jumpcloud, “What Role Does Multi-Factor Authentication Play in a Zero Trust Security Model?,” Oct. 2021, https://jumpcloud.com/blog/mfa-role-zero-trust-security-model.

[4] Delinea, “What is Zero Trust and Zero Trust Extended (ZTX)?,” https://delinea.com/what-is/zero-trust-and-zero-trust-extended.

[5] John Kindervag, “No More Chewy Centers: The Zero Trust Model Of Information Security,” Forrester, Mar. 2016.

[6] 강은수, “제로트러스트(Zero Trust), 새로운 보안 패러다임으로의 전환”, 국회입법조사처, Apr. 2024.

[7] Akamai, “What is Zero Trust?,” https://www.akamai.com/our-thinking/zero-trust/zero-trust-security-model.

[8] SAMSUNG SDS, “다시 주목 받고 있는 기업 보안의 패러다임, 제로 트러스트,” Jun. 2021, https://www.samsungsds.com/kr/insights/zero_trust.html.

[9] National Institute of Standards and Technology, “Zero Trust Architecture,” NIST SP 800-207, Aug. 2020.

[10] Genians, “제로트러스트(Zero Trust)의 올바른 이해,” https://www.genians.co.kr/blog/zt.

[11] Ekran, “Zero Trust Architecture: Key Principles, Components, Pros, and Cons,”, Jul. 2024, https://www.ekransystem.com/en/blog/zero-trust-security-model.

[12] Songpon Teerakanok, Tetsutaro Uehara, Atsuo Inomata, “Migrating to Zero Trust Architecture: Reviews and Challenges,” Hindawi, May. 2021.

[13] White House, “Executive Order on Improving the Nation’s Cybersecurity,” May. 2021.

[14] National Institute of Standards and Technology, “Implementing a Zero Trust Architecture,” NIST SP 1800-35, Dec. 2022.

[15] OFFICE OF MANAGEMENT AND BUDGET, “Federal Zero Trust Strategy,” M-22-09, Jan. 2022.

[16] 전자신문, “[K-제로 트러스트] “가이드라인 2.0은 제로 트러스트 도입 안내서””, Mar. 2024, https://www.etnews.com/20240314000045

[17] 디지털데일리, “제로트러스트 가이드라인 2.0 밑그림 나왔다…” 도입 방법론 제시, Apr. 2024, https://m.ddaily.co.kr/page/view/20240424165408628 21

[18] 과학기술정보통신부, “제로트러스트 가이드라인 1.0,” Jun. 2023.

[19] 전자신문, “과기정통부, ‘K-제로 트러스트 모델’ 발

표…보안성 41%↑", Dec. 2023, https://www.etnews.com/20231211000208
[20] National Institute of Standards and Technology, "제로 트러스트 아키텍처," NIST SP 800-207, Jul. 2021.

〈저 자 소 개〉

최 여 정 (Yeo-jeong Choi)
정회원
2021년 2월 : 한남대학교 수학과, 컴퓨터통신무인기술학과 졸업
2023년 2월 : 한남대학교 컴퓨터공학과 석사
2023년 9월~현재 : 국가보안기술연구소 연구원
<관심분야> 사이버안보정책, 제로 트러스트, 정보보안, 펌웨어 분석, 취약점 탐지, 양자암호

정 윤 정 (Yun-jeong Jeong)
학생회원
2024년 2월 : 한남대학교 컴퓨터공학과 졸업
2024년 3월~현재 : 한남대학교 컴퓨터공학과 석사과정
<관심분야> 공급망 보안, 제로 트러스트, 정보보안, 취약점 탐지

이 만 희 (Man-hee Lee)
종신회원
1995년 2월 : 경북대학교 컴퓨터공학과 공학사
1997년 2월 : 경북대학교 공학석사
2008년 8월 : Texas A&M 대학교 컴퓨터공학과 공학박사
1997년~2003년 : 한국과학기술정보연구원 연구원
2008년~2009년 : Cisco Systems, San Jose
2010년~2012년 : 국가보안기술연구소 선임연구원
2012년~현재 : 한남대학교 교수
<관심분야> 네트워크/시스템/스마트폰/공급망 보안, 고성능 시스템, 컴퓨터교육