

보도시점 2023. 12. 11.(월) 14:00
(2023. 12. 12.(화) 조간)

배포 2023. 12. 11.(월) 09:00

과기정통부, 국산 제로트러스트 보안모델 본격 확산 기반 마련!

- 클라우드 및 구축형(원격·재택) 업무환경 적용 제로트러스트 모델 발표 -
- 보안효과성 검증모델을 적용하여 체계적인 제로트러스트 확산 지원 -
- 국산 제로트러스트 보안모델 해외진출 지원 -

과학기술정보통신부(장관 이종호, 이하 ‘과기정통부’)와 한국인터넷진흥원(원장 이원태, 이하 ‘KISA’)은 향후 제로트러스트* 보안 패러다임 전환을 위해 12월 11일(월) 국내 기업망 환경에 적용할 수 있는 ‘제로트러스트 기본모델 2종’을 발표했다고 밝혔다.

* Zero Trust : 정보 시스템 등에 대한 접속요구가 있을 때 네트워크가 이미 침해된 것으로 간주하고, “절대 믿지 말고, 계속 검증하라는 새로운 보안개념(Never Trust, Always Verify)”이다. (제로트러스트 가이드라인 1.0)

과기정통부와 KISA는 올해 7월 7일 국내 최초로 발표한 「제로트러스트 가이드라인1.0」을 기반으로 통신, 금융 등 국민 생활과 밀접한 분야를 중심으로 국산 제로트러스트 보안모델을 적용·실증하고, 기존 경계보안 모델보다 한 단계 높은 보안수준을 구축할 수 있는 가능성을 확인하였다.

< 제로트러스트 가이드라인1.0 >

제로트러스트 보안모델을 쉽게 이해할 수 있도록 기본개념과 보안원리, 핵심원칙 및 접근제어원리, 도입계획 수립을 위한 세부절차 및 도입 참조모델 등을 제시,

핵심원칙으로 ① 강화된 인증(아이디/패스워드 외에도 다양한 인증정보를 활용한 다중인증 등 지속적인 인증을 포함), ② 마이크로 세그멘테이션(서버·컴퓨팅 서비스 등을 중심으로 하는 작은 단위로 분리), ③ 소프트웨어 정의 경계(소프트웨어 기반으로 보호 대상을 분리·보호할 수 있는 경계를 만들 수 있어야함)를 제시하였고,

안전하고 지속적인 접근제어를 위해 ‘제어영역’과 ‘데이터 영역’으로 구분되어야 하며, 자원에 대한 접근 요구가 있을 때 접속을 결정하는 정책결정지점(PDP, Policy Decision Point)과 접속을 시행하는 정책시행지점(PEP, Policy Enforcement Point)을 두고 운영토록 함

※ 과기정통부, 한국인터넷진흥원, 한국정보보호산업협회 홈페이지 보도자료 사이트 참고

올해 실증사업은 제로트러스트 가이드라인1.0에서 제시한 제로트러스트 보안모델을 실제 기업망 환경에 적용한 첫 사례로 글로벌 보안기업들이 제로트러스트 시장 선점을 위해 노력하고 있는 가운데 국산 제로트러스트 보안모델의 보안효과성을 확인함으로써 향후 수입 대체효과 및 더 나아가 글로벌시장 진출을 위한 초석을 다졌다.

특히, 이번에 마련한 모델은 두 가지로 개발하였는데 ① 클라우드형 및 ② 구축형(On-Premise) 등 다양한 업무 환경에서 제로트러스트 보안모델의 보안효과성을 검증함으로써 업종, 업무 환경에 상관없이 제로트러스트 보안모델을 적용할 수 있도록 하였다.

또한 과기정통부는 실증사업의 ③ 보안효과성 검증을 위한 침투시나리오 및 보안성 점검 체크리스트를 개발·적용함으로써 체계적인 제로트러스트 보안모델의 확산은 물론 제로트러스트 보안성 검증체계를 발전시켜나갈 수 있는 기반을 마련하였다.

< ① 클라우드 업무환경을 위한 제로트러스트 기본모델(붙임 1) >

첫 번째 실증사례에는 국내외에 특허 등록한 제로트러스트 보안모델이 적용되었다. 기존 무선통신 및 클라우드 환경에서는 디도스공격 또는 횡적이동공격으로 인해 요금 과다청구 등의 문제가 있어서 한 단계 높은 수준의 보안체계가 요구되는 상황이다.

이를 위해 보호해야할 서비스, 서버, 어플리케이션, 데이터 등을 각각 논리적으로 분리하여 보호하였고, PEP(정책시행지점)가 탑재된 제로트러스트 전용 라우터를 세계 최초로 개발·적용하여 보안 수준을 크게 향상시킬 수 있는 모델로 세계적으로 드문 사례이다.

이 사례에서는 실증 현장에 대한 보안효과성 검증을 위해 국내 전문시험기관이 참여하여 97개의 평가항목을 개발하고 각 항목에 대한 현장 시험 및 확인을 통해 개선된 보안효과성을 확인하였다.

< 제로트러스트 보안모델 적용 전후 비교 >

제로트러스트 적용 전	제로트러스트 적용 후
- o 라우터 또는 단말의 멀웨어 감염 증가 - o 인터넷에 연결된 라우터 및 단말에 대한 DDoS 공격 및 침투위협 증가 - o IP 화이트리스트 기반 보안강화시 3일 이상 소요	- o 라우터 또는 단말에 대한 접근제어 가능으로 멀웨어 감염 차단 - o 라우터와 단말을 인터넷과 논리적으로 차단하여 DDoS 공격 등 차단 - o SPA(Single Packet Authorization)을 통한 신속한 접근제어

※ 대표적인 일부 특성을 제시한 것임

< ② 구축형 업무환경을 위한 제로트러스트 기본모델(붙임 2) >

두 번째 사례는 국내 다수의 대표 보안기업이 참여하여 개발한 보안 모델을 적용하였다. 코로나 19 팬데믹으로 가상사설망 기반의 원격·재택 근무가 급속하게 확산되었으나 크리덴셜 스테핑을 이용한 해킹 등의 사이버 공격의 타겟이 되고 있어서 보안강화 방안이 필요한 상황이다.

이를 위해 접속 요구자의 보안 수준을 점수화하여 접속단계에서부터 보안을 강화하고, 접속 중이라도 점수에 변경이 생기면 접속 차단 또는 접속 가능한 리소스를 제한할 수 있도록 하는 동적인증체계를 구현하였다.

특히 제로트러스트 성숙도모델을 기반으로 점검 항목 리스트를 개발하고 실증현장에 대한 점검을 통해 개선된 보안효과성을 확인하였고, 보안솔루션 연동을 통해 다양한 기업환경에 적용할 수 있는 현장 맞춤형 제로트러스트 보안모델을 제공할 수 있다는 것을 입증하였다.

< 제로트러스트 보안모델 적용 전후 비교 >

제로트러스트 적용 전	제로트러스트 적용 후
- o 단순한 ID/PW 관리로 크리덴셜 스테핑을 통한 VPN 통과 - o 본사 내부 시스템 접속 후 횡적 이동을 통한 모든 자원에 대한 접속 및 자료 유출	- o 사용자 통합관리 등 강화된 인증체계를 적용하여 크리덴셜 스테핑을 통한 접속 불가 - o 시스템, 애플리케이션, 데이터 등이 논리적으로 분리·보호되어 횡적 이동 불가

※ 대표적인 일부 특성을 제시한 것임

< ③ 제로트러스트 보안효과성 점검방안 >

올해 제로트러스트 보안모델 실증사업에서는 각 실증사례에 참여한 기업들이 자체적으로 개발하여 적용한 검증방법 외에도 제로트러스트 보안모델의 객관적인 보안효과성 검증을 위해 보안효과성 검증 전문기업이 참여하였다.

제로트러스트 보안모델이 적용된 실증 대상에 대한 보안효과성 점검을 위해 침투시나리와 함께 개선된 보안성을 점검할 수 있는 점검리스트를 개발하고 각 현장에 적용하여 기존보다 더 높은 보안수준을 확인할 수 있었다.

국제적으로 제로트러스트 보안모델 보안효과성 검증을 위한 표준화된 검증방법이 없는 상황에서 이번에 국내 기업이 개발한 제로트러스트 보안효과성 검증방안은 향후 국제 표준화에 기여할 수 있도록 더 발전시켜나갈 계획이다.

과기정통부 홍진배 네트워크정책실장은 “전 세계 국가들이 제로트러스트 보안모델을 도입하기 위해 국가적 차원에서 노력하고 있고, 글로벌 기업들은 신시장을 선점하려고 경쟁하고 있다”고 강조하면서

“과기정통부는 향후 제로트러스트 성숙도 모델을 계속 발전시켜나가고, 국산 제로트러스트 보안모델의 성공적인 확산을 지원하여 국가적인 차원의 사이버보안 수준을 한 단계 높이는 한편, 국내 기업의 체계적인 해외진출도 지원하겠다”는 정책 의지를 밝혔다.

담당 부서	정보보호네트워크정책관 정보보호산업과	책임자	과 장	정은수 (042-202-6450)
		담당자	사무관	김성환 (044-202-6451)
	한국인터넷진흥원 보안산업진흥팀	책임자	팀 장	변순정 (061-820-1309)
		담당자	선임연구원	최슬기 (061-820-1309)



개요	· 네트워크 중심 제로트러스트 보안모델 실증
실증환경	· 클라우드, SaaS, 무선통신망 환경
구성	
주요성과	· 국내 최초 3요소(EIG, SDP, Micro Segmentation) 통합 기술 실증 · 기간통신 사업자 무선망 제로트러스트 적용 모델 발굴 · 안전한 민간 클라우드 및 SaaS 이용 환경 조성
참고	· TTA '시험인증 서비스'를 통한 자체 효과성 검증 수행

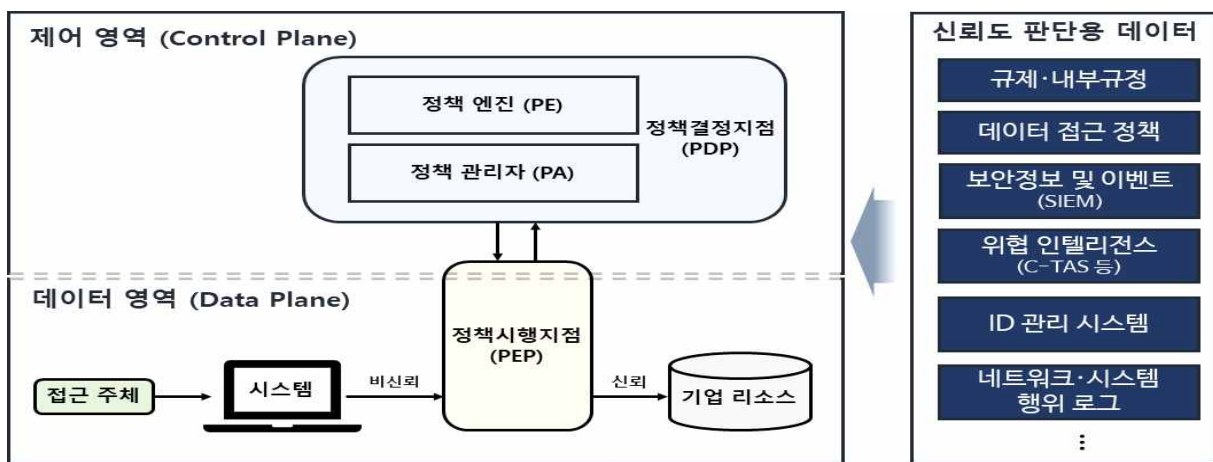
개요	· IT 보안기업(47개사)들의 제품 간 연동을 통한 제로트러스트 아키텍처 통합 구축
실증환경	· 온프레미스 환경(재택근무, 본사-지사 접속환경 등 일반 업무환경)
구성	The diagram illustrates the Zero Trust Architecture (ZTA) model, showing the integration of various security products across different environments. It is divided into three main sections: 본사 (Headquarters), 외부환경 (재택 등) (External Environment (Remote, etc.)), and 지사 (Branch Office). 본사 (Headquarters): Subject/System: Includes 업무망 (사용자망, 운영관리망) (Business Network (User Network, Operation/Management Network)), 통합 '엔드포인트' 관리 시스템 (UEM Agent) (Anti-Malware, Patch Mgmt., Security Level), ZTNA Agent (Auth, SSL Client, Device Posture & Visibility), and 보안상태 확인, ID/FW, MFA, 형상 관리, Context 수집 등 (Security Status Confirmation, ID/FW, MFA, Configuration Management, Context Collection, etc.). PEP (Policy Enforcement Point): Includes Web App. Control G/W, PAM G/W, Zero Trust Web Portal, and ZTNA G/W. Enterprise Resource: Includes System (OS, DB, etc.) and Application (App, RPP, etc.). PDP (Policy Decision Point): Includes Risk Score, 부가 정보 (Additional Information), Trust Algorithm, 정책 통합관리 시스템 (ICAM) (Policy Integrated Management System), and ZTNA Center. Interactions: Secure Access, 미등록 사용자/디바이스 접근 통제 (Control access for unregistered users/devices), Trust Score 기반 동적 접근제어 (Dynamic access control based on Trust Score), 정책 이행 (Policy Enforcement), 접근 결정 (Access Decision), and Trust Score 기반 동적 접근제어 (Dynamic access control based on Trust Score). 외부환경 (재택 등) (External Environment (Remote, etc.)): Subject/System: Includes 인터넷망 (Internet Network), 통합 '엔드포인트' 관리 시스템 (UEM Agent) (Anti-Malware, Patch Mgmt., Security Level), ZTNA Agent (Auth, SSL Client, Device Posture & Visibility), and 보안상태 확인, ID/FW, MFA, 형상 관리, Context 수집 등 (Security Status Confirmation, ID/FW, MFA, Configuration Management, Context Collection, etc.). Interactions: Secure Access, 사용자 (User), and Internet. 지사 (Branch Office): Subject/System: Includes 인터넷망 (Internet Network), 통합 '엔드포인트' 관리 시스템 (UEM Agent) (Anti-Malware, Patch Mgmt., Security Level), ZTNA Agent (Auth, SSL Client, Device Posture & Visibility), and 보안상태 확인, ID/FW, MFA, 형상 관리, Context 수집 등 (Security Status Confirmation, ID/FW, MFA, Configuration Management, Context Collection, etc.). Interactions: 사용자 (User) and Internet.
주요성과	· 사용자, ZTA 정책엔진, 기업자원 소구간에 걸친 연동 검증 · 보안제품 간 통합 구현을 통한 ZTA 실증 · 시스템 및 애플리케이션 레벨의 동적 접근제어 가능
참고	· 성숙도 모델 기반 시나리오로 자체 효과성 검증 수행

- 제로트러스트 보안모델에 대한 국제적 논의가 활발하게 진행되고 있는 상황에서 국내 정부·공공 기관 및 기업의 실무자, 의사결정자들이 빠른 기간 내에 제로트러스트 보안모델을 이해하고, 도입을 준비할 수 있도록 마련(요약본과 전체본 등 2권)

(핵심원칙) 제로트러스트 보안은 '절대 믿지 말고, 계속 검증하라'는 기본철학을 구현하기 위한 ① 강화된 인증, ② 마이크로 세그멘테이션, ③ 소프트웨어 정의 경계

(접근제어 원리) 보호 대상 자원에 대한 접근 요구에 대해 접속을 허락할지 말지를 결정하는 과정으로 제로트러스트 기본철학을 구현하는 가장 중요한 원리 중 하나, 안전하고 지속적인 접근제어를 위해서 제로트러스트 보안모델은 '제어영역'과 '데이터 영역'으로 구분되어야 하며, 자원에 대한 접근 요구가 있을 때 접속을 결정하는 정책결정지점(PDP)과 접속을 시행하는 정책시행지점(PEP)을 두고 운영해야함

< 제로트러스트 접근제어 논리 컴포넌트 구성도 >



(핵심요소의 식별과 관리) 기관 및 기업의 관계자들은 네트워크, 컴퓨팅 자원 중 어느 정도 보안수준으로 설계를 해야 할지, 예산계획 수립, 도입 진행상황 점검 등을 위한 지표로, 식별자·신원, 기기, 네트워크, 시스템, 응용·네트워크, 데이터 등 6개 핵심요소에 대한 보안 수준의 성숙도 단계별 기능을 정의

(도입 참조모델) 정부·공공 기관 및 기업 관계자들은 실질적인 도입 전략 수립 시 참고할 수 있는 실제 네트워크 모델과 이를 기반으로 제로트러스트 보안모델을 적용한 사례를 참조모델로 제시하여 제로트러스트 도입 전후 네트워크 구조 변화 및 보안 효과성 등을 확인할 수 있음

※ 과기정통부, KISA, KISIA 홈페이지에서 "제로트러스트" 검색하여 다운로드 이용 가능

제로트러스트 보안 모델 실증 성과공유회

2023.12.11.(Mon), 10:00 ~ 16:00

장 소

페어몬트 앰배서더 서울(B1), 그랜드볼룸 I+II

홈페이지

<https://zerotrust2023.kr>

프로그램

시간	주요내용	비고
09:30 ~ 10:00	참가자 등록 및 접수	
세션 I 제로트러스트 정책 및 기술 세미나		
10:00 ~ 10:30	제로트러스트 정책 및 기술 동향	이석준 교수(가천대)
10:30 ~ 11:00	국내 제로트러스트 산업 실태조사 결과	유진호 교수(상명대)
11:00 ~ 11:30	강화된 인증체계(EIG) 기반제로트러스트 구축 전략	신은수 보안기술총괄(AWS)
11:30 ~ 12:00	소프트웨어 정의 경계(SDP) 및 마이크로 세그멘테이션 기반 제로트러스트 구축 전략	장성민 상무(팔로알토 네트워크스)
12:00 ~ 13:30	점심식사(Luch break)	
개회식		
13:30 ~ 13:40	개회 및 참석자 소개	KISA 과기정통부(네트워크정책실장)
13:40 ~ 13:45	개회사	
13:45 ~ 13:50	환영사	
세션 II 제로트러스트 실증 및 효과성 검증 결과공유		
13:50 ~ 14:20	제로트러스트 보안모델 실증 및 검증 추진경과	과기정통부(정보보호산업과장)
14:20 ~ 14:50	제로트러스트 아키텍처 통합 구축 모델 실증 사례	최영철 대표(SGA솔루션즈)
14:50 ~ 15:20	경계 보안의 장벽을 뛰어넘은 제로트러스트 모델 실증 사례	김영량 대표(프라이빗테크놀로지)
15:20 ~ 15:50	제로트러스트 보안모델에 대한 유효성 검증 시나리오 및 검증 사례	이성권 대표(엔키)
15:50 ~ 16:00	Q&A 및 폐회	

문의처

운영사무국 | CM (주) 컬처메이커스 ☎ 070.4849.2062 ✉ info@cmcom.kr