

보도시점 2023. 7. 9.(일) 12:00
(2023. 7. 10.(월) 조간)

배포 2023. 7. 9.(일) 09:00

과기정통부, 제로트러스트 가이드라인1.0 발표!

- 제로트러스트 개념·보안원리·핵심원칙 등을 설명하는 가이드라인 발표 -
- 국산 제로트러스트 기술 실증으로 국가적 보안수준 높인다! -

과학기술정보통신부(장관 이종호, 이하 ‘과기정통부’)는 작년 10월 국내 산·학·연·관 전문가로 구성된 「제로트러스트포럼(간사기관 : 한국인터넷진흥원)」을 구성하고 미국, 유럽, 일본 등의 동향 분석, 자료검토, 토론회 등을 통해 의견을 모아 국내 환경에 적합한 「제로트러스트 가이드라인 1.0」 마련하였다고 밝혔다.

또한, 대통령 직속 디지털플랫폼정부위원회(위원장 고진)와 함께 지난 4월 「디지털플랫폼정부 실현계획」을 발표하면서 새로운 디지털환경에서의 정보보안을 위하여 국가적 차원의 제로트러스트 도입을 추진하겠다고 밝힌 바, 이번에 마련된 「제로트러스트 가이드라인 1.0」을 각 분야로 확산시켜나갈 계획이다.

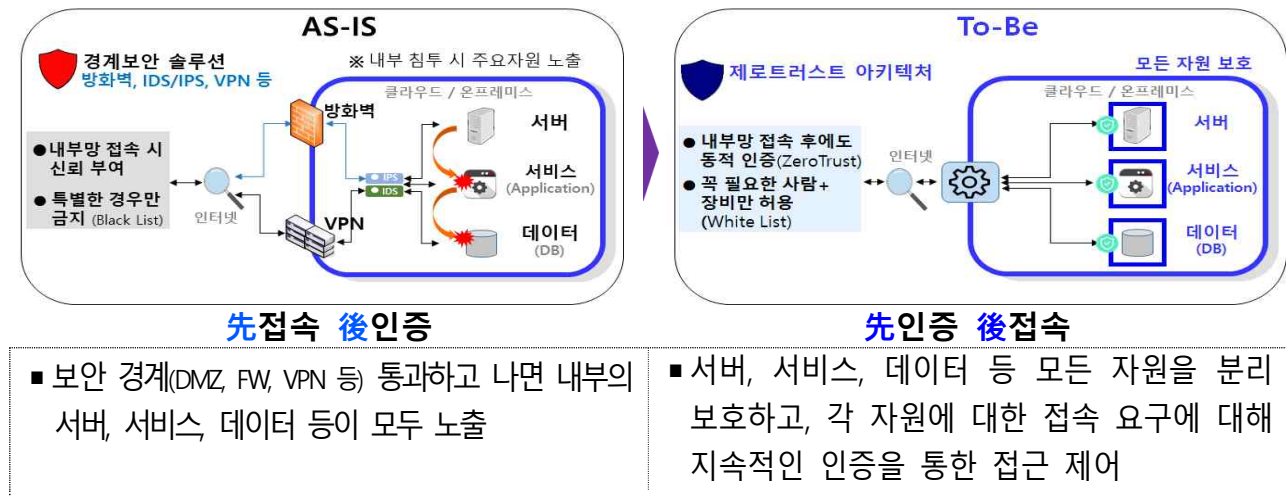
제로트러스트(Zero Trust)는 정보 시스템 등에 대한 접속요구가 있을 때 네트워크가 이미 침해된 것으로 간주하고, “절대 믿지 말고, 계속 검증하라는 새로운 보안개념(Never Trust, Always Verify)”이다.

모바일·사물인터넷(IoT) 기기, 클라우드 기반의 원격·재택 근무환경이 조성되고, 코로나 19로 인해 비대면 사회가 가속화됨에 따라 전통적으로 네트워크의 내·외부 경계를 구분하고 내부자에게 암묵적 신뢰를 부여하는 기존 경계 기반 보안모델은 한계에 도달하여 새로운 보안모델로 전환이 필요한 상황이다.

기존 경계 기반 보안모델은 침입자가 내부자와 공모 또는 권한 탈취를 통해 정보시스템에 접속하고 나면 내부의 서버, 컴퓨팅 서비스, 데이터 등 모든 보호 대상에 추가 인증 없이 접속할 수 있어서 악의적 목적을 위해 데이터가 외부로 유출될 수 있다.

반면에 제로트러스트 보안모델은 제로트러스트 보안개념을 토대로 서버, 컴퓨팅 서비스 및 데이터 등을 보호해야할 자원으로 각각 분리·보호하며, 이를 통해 하나의 자원이 해킹되었다고 하더라도 인근 자원은 보호할 수 있으며, 사용자 또는 기기 등의 모든 접속 요구에 대해 아이디/패스워드 외에도 다양한 정보를 이용해 인증하는 방식으로 보안수준을 높일 수 있다.

< 경계 보안 Vs 제로트러스트 보안 비교 >



미국, 유럽 등에서는 4차 산업혁명 기술 기반으로 비대면 사회가 가속화됨에 따라 기존 경계 기반 보안모델의 전환이 필요한 상황에서 다양화·지능화되는 사이버위협에 대응할 수 보완수단으로 제로트러스트 보안모델 도입이 본격화되고 있다.

< 제로트러스트 가이드라인 1.0 주요내용 >

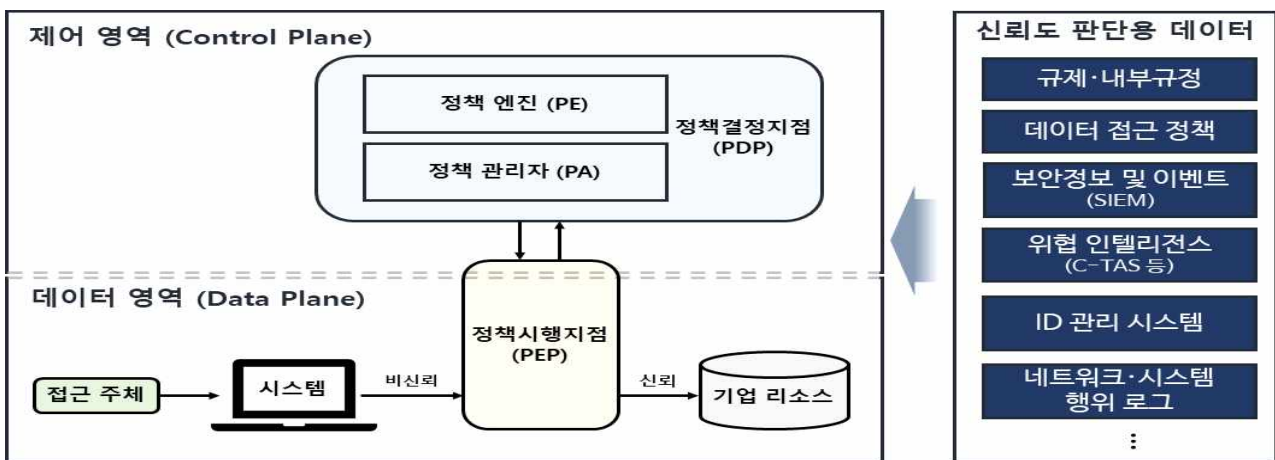
제로트러스트 가이드라인 1.0은 제로트러스트의 기본개념과 보안원리, 제로트러스트 보안모델의 핵심원칙 및 접근제어원리, 도입계획 수립을 위한 세부절차 및 도입 참조모델 등을 제시하고 있다.

(핵심원칙) 제로트러스트 보안은 ‘절대 믿지 말고, 계속 검증하라’는 기본철학을 구현하기 위한 ① 강화된 인증(아이디/패스워드 외에도 다양한 인증 정보를 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 말한다.

(접근제어 원리) 보호 대상 자원에 대한 접근 요구에 대해 접속을 허락 할지 말지를 결정하는 과정으로 제로트러스트 기본철학을 구현하는 가장 중요한 원리 중 하나이다.

안전하고 지속적인 접근제어를 위해서 제로트러스트 보안모델은 ‘제어 영역’ 과 ‘데이터 영역’ 으로 구분되어야 하며, 자원에 대한 접근 요구가 있을 때 접속을 결정하는 정책결정지점(PDP)과 접속을 시행하는 정책시행 지점(PEP)을 두고 운영해야 한다.

< 제로트러스트 접근제어 논리 컴포넌트 구성도 >



(핵심요소의 식별과 관리) 제로트러스트 도입을 검토하고 있는 기관 및 기업의 관계자들은 네트워크, 컴퓨팅 자원 중 어떤 요소를 어느 정도 보안 수준으로 설계를 해야 할지, 관련 예산계획 수립, 도입 기간 중 진행상황 점검 등을 위한 지표를 필요로 한다.

이를 위해 식별자·신원, 기기, 네트워크, 시스템, 응용·네트워크, 데이터 등 6개 핵심요소에 대한 보안 수준의 성숙도 단계별 기능을 정의하여 실질적인 정보를 제공할 수 있도록 하였다.

(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 있다.

이를 위해 최근 우리나라에 일상화되어 있는 재택·원격지 근무 환경에 제로트러스트 보안모델을 적용한 네트워크에 침투 시나리오를 적용하여 제로트러스트 도입 시 보안성이 강화될 수 있음을 파악할 수 있게 했다.

이번 가이드라인 1.0은 7월10일부터 과기정통부, KISA 및 유관기관 홈페이지를 통해 이용할 수 있으며, 향후 실증사례의 보안 효과성 분석 결과와 변화되는 환경 등을 고려하여 「제로트러스트 가이드라인 2.0」을 준비하는 등 지속적으로 보완·고도화해 나갈 계획이다.

하반기에는 SGA솔루션즈 컨소시엄과 프라이빗테크놀로지 컨소시엄은 올 해 6월부터 12월까지 통신·금융·공공 분야 등 다양한 환경에 제로트러스트 보안 모델을 구현하고, 세계적 수준의 화이트 해커들이 공격 시나리오로 구성된 검증 모델을 적용하여 제로트러스트 도입 전후 보안 효과성을 검증할 계획이다.

과기정통부 박윤규 제2차관은 “국민의 일상생활 및 다양한 산업분야로 네트워크가 확장되는 상황에서 보안체계가 전환되어야 하는 패러다임 전환 시기에 이런 상황에 적합한 대안을 찾아야 한다” 면서,

“과기정통부는 정부·공공 기관 및 기업들에게 실질적인 도움이 될 수 있도록 제로트러스트 가이드라인을 지속적으로 보완·고도화하는 한편, 실증 사업을 통해 다양한 분야로 제로트러스트 보안모델이 확산될 수 있도록 지원하겠다”고 말했다.

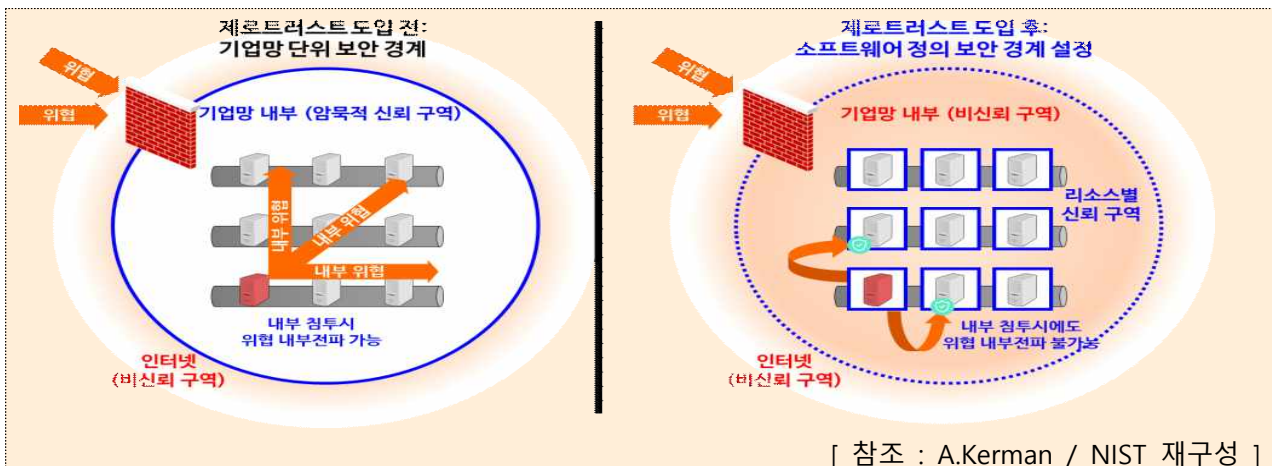
담당 부서	정보보호산업과	책임자	과 장	정은수 (042-202-6450)
		담당자	사무관	김성환 (044-202-6451)
	한국인터넷진흥원(KISA) 보안산업진흥팀	책임자	팀 장	변순정 (061-820-1309)
		담당자	선 임	최슬기 (061-820-1638)

붙임 1

제로트러스트 가이드라인 1.0 주요내용

- (환경변화) 디지털 대전환의 가속화로 네트워크의 경계의 확장 및 다변화로 사이버보안 영역 또한 일상생활 및 다양한 산업분야로 확장
 - 모바일·IoT기기, 클라우드 확산과 원격·재택 근무 등 비대면 사회의 가속화로 리소스 위치 다변화, 접속 요구 시간·위치 또한 예측 불가
- (경계보안 vs 제로트러스트) 경계기반 보안모델은 신뢰하는 자원(내부망)과 신뢰하지 않은 자원(외부망) 사이에 보안 경계를 세움
 - * 내부자 공모 또는 권한탈취 후 침투, 권한상승 및 횡적이동을 통한 데이터 유출
 - 반면, 제로트러스트는 보호해야할 모든 데이터와 컴퓨팅 서비스를 각각의 자원(Resource)으로 분리·보호
 - * 모든 자원의 경계를 구분하여 분리·보호, 하나의 자원에 접속한 후에는 정해진 권한만큼만 활동이 가능하고, 인근 자원에 대한 추가 접속 요구 시 지속적 인증으로 침투 제한

< 기존 경계기반 보안과 제로트러스트 개념 비교 >



[참조 : A.Kerman / NIST 재구성]

- ▲ 기업망 내부에 접속한 이후 내부 자원에 대한 자유로운 접속 및 데이터 유출
- ▲ 기업망 내부 모든 자원이 개별적으로 보호되고 선인증 후 접속 등 지속적인 접속 관리

※ 제로트러스트는 ①Enhanced Identity Governance, ②Micro-Segmentation, ③SW Defined Perimeter에 기반을 두며, 각각의 자원에 대한 접속요구에 동적인증을 통한 선인증 후 접속, 이후에도 가시성 확보를 통한 지속적 모니터링으로 보안 수준을 높임

- (핵심원칙) 제로트러스트 아키텍처를 구현하기 위한 접근방법으로 3가지 핵심원칙을 모두 포함할 때 완성도가 높다고 할 수 있음

< 제로트러스트 구현 핵심원칙 >

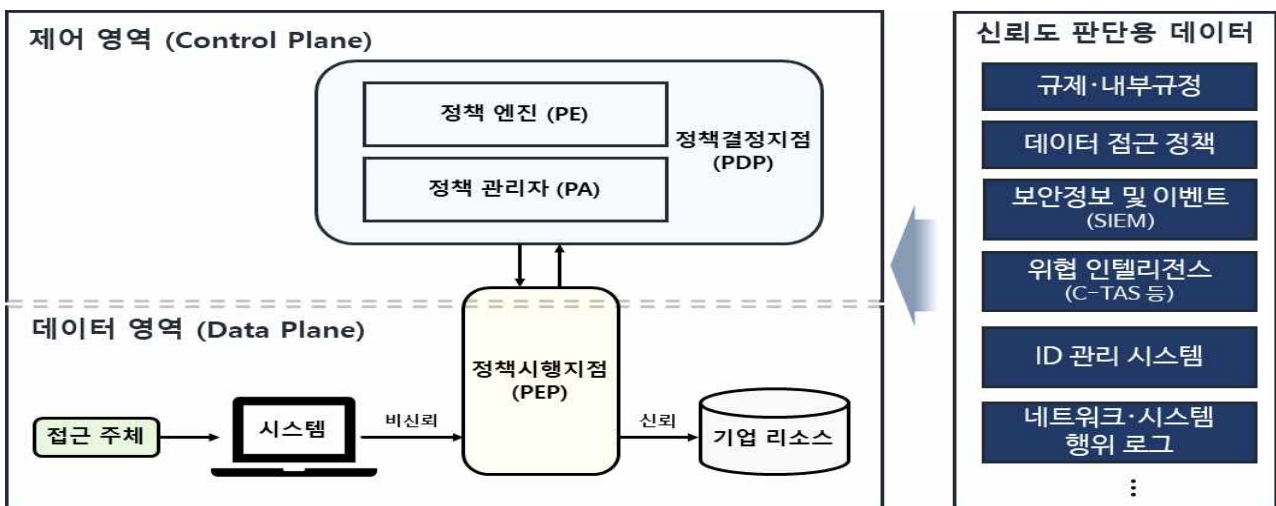
핵심 원칙	세부 내용
인증 체계 강화	▲ 각종 리소스 접근 주체에 대한 신뢰도(사용하는 단말, 자산 상태, 환경 요소, 접근 위치 등을 판단)를 핵심요소로 설정하여 인증 정책 수립 ※ 기업내 사용자에게 대한 여러 아이디를 허용하여 일관된 정책을 적용하지 않거나, 신뢰도 판단없이 단일 인증 방식만으로 접속을 허용할 경우 크리덴셜 스토핑에 취약
마이크로 세그멘테이션	▲ 보안 게이트웨이를 통해 보호되는 단독 네트워크 구역(segment)에 개별 자원(자원그룹)을 배치하고, 각종 접근 요청에 대한 지속적인 신뢰 검증 수행 ※ 개별 자원별 구역 설정이 없으면, 기업망 내부에 침투한 공격자가 중요 리소스로 이동하기 쉬워 횡적이동 공격 성공 가능성이 높아짐
소프트웨어 정의 경계	▲ 소프트웨어 정의 경계 기법을 활용하여 정책 엔진 결정에 따르는 네트워크 동적 구성, 사용자·단말 신뢰 확보 후 자원 접근을 위한 데이터 채널 형성 ※ 클라우드·온프레미스로 구성된 기업 네트워크 내부에서 단말이 임의 데이터를 전송할 수 있다면, 네트워크 및 호스트 취약성에 따르는 피해 가능성이 커짐

[NIST SP 800-207, 제로트러스트 아키텍처에 대한 다양한 접근법(3.1절)을 기반으로 작성]

□ (접근제어논리) 제로트러스트 아키텍처는 제어영역과 데이터 영역으로 구분되어야 하며, 정책결정지점(PDP)과 정책시행지점(PEP)이 있음

- PDP는 정책엔진(PE)과 정책관리자(PA)로 나뉘며, PE는 신뢰도를 판단하여 접속 허가를 최종 결정, PA는 PEP에 명령하여 정책을 실행
- PDP는 PEP 및 다양한 보안솔루션(SIEM, C-TAS, IAM, LMS 등)에서 생성한 보안 정보 등을 바탕으로 한 '신뢰도 평가*'를 통해 자원 접근 여부를 결정하고, 접근 허가 후에는 양방향 보안 통신경로 생성

< 제로트러스트 접근제어 논리 컴포넌트 구성도 >



[참조 : NIST SP 800-207, 제로트러스트 아키텍처 논리 컴포넌트 재구성]

- (기업망 핵심요소) 금융망 및 국가 기반시설 보안 정책, 공공 클라우드 보안 인증 기준 등을 고려하여 국내 환경에 적합한 핵심요소(6종) 도출
- 금융망 등 시스템 관리자(개발자) 계정 해킹으로 인한 시스템 주요 파일 접근 훼손 등 침해사고 대책 차원에서 기업망 핵심요소로 '시스템' 추가 및 성숙도별 기능 정의

< 제로트러스트 도입을 위한 기업망 핵심요소 >

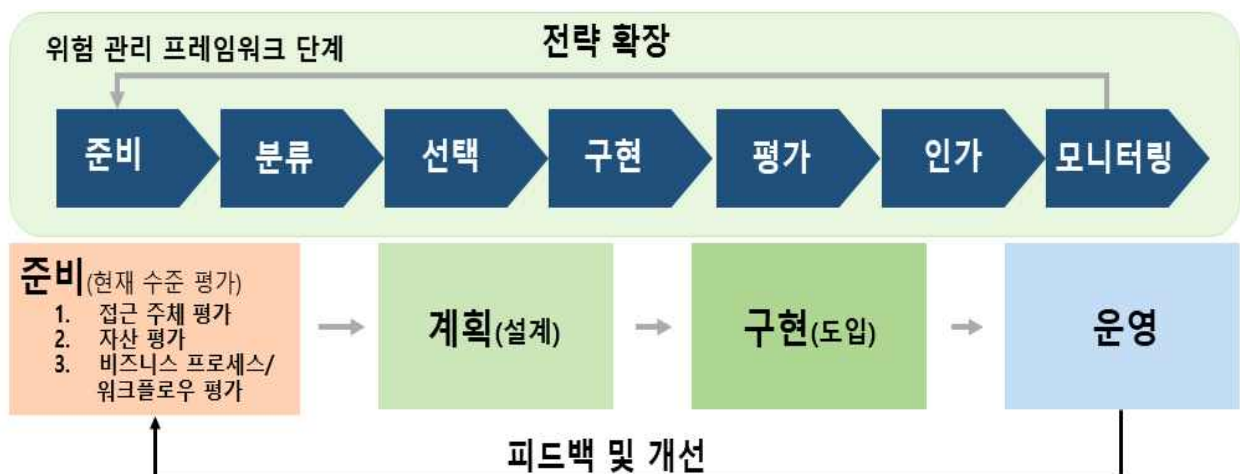
핵심 요소	주요 내용
식별자·신원 (Identity & User)	▲ 사람, 서비스, IoT 기기 등을 고유하게 설명할 수 있는 속성(속성의 집합)
기기 및 엔드포인트 (Device & Endpoint)	▲ IoT 기기, 휴대폰, 노트북, PC, 서버 등을 포함하여 네트워크에 연결하여 데이터를 주고 받는 모든 하드웨어 장치
네트워크 (Network)	▲ 기업망의 유선 네트워크, 무선 네트워크, 클라우드 접속을 포함하는 인터넷 등 데이터를 전송하기 위해 사용되는 모든 형태의 통신 매체
시스템 (System)	▲ 중요 응용프로그램을 구동하거나 중요 데이터를 저장하고 관리하는 서버
응용 및 워크로드 (Application & Workload)	▲ 기업망 관리 시스템, 프로그램, 온프레미스 및 클라우드 환경에서 실행되는 서비스
데이터 (Data)	▲ 기업(기관)에서 가장 최우선적으로 보호해야 할 자원

- (도입계획수립) 보유 자원에 대한 보안위협을 줄이기 위한 절차로 '위험 관리 프레임워크(NIST)'와 연계하여 도입단계* 검토가 가능

* 준비(현재수준 평가), 계획(설계), 구현(도입), 운영, 피드백 및 개선

- 구현 목표 설정, 예산계획, 도입 과정에서 공정별 진행 상황 점검 등을 위해 기업망 핵심요소별 성숙도모델을 참고할 수 있음

< 제로트러스트 도입을 위한 세부 절차 >



[참조 : NIST SP 800-207(제로트러스트 아키텍처 전개 사이클), 800-37(위험관리 프레임워크 단계)]

붙임 2 제로트러스트 현장 간담회 개최 계획(안)

◇ 제로트러스트 가이드라인1.0 핵심 내용, 제로트러스트 실증·시범사업 추진 계획을 공유하고, 실효성 있는 제로 트러스트 실증 방안 등에 대한 심층 토론

□ 개 요

- (일시/장소) '23.7.7.(금) 14:00~16:00 / 한국지능정보사회진흥원* (서울 청계천)
- * 공공기관 최초 제로트러스트 보안체계 도입으로 정책적 상징성 높음
- (참석자) 과기정통부 2차관, 네트워크정책실장, 제로 트러스트 실증·수요기업 및 관련 전문가 20여명(붙임1 참조)
- (주요내용) 국내·외 제로 트러스트 최신 동향, 제로 트러스트 가이드라인 1.0 핵심 내용, 제로 트러스트 보안 모델 실증 및 검증 계획 공유 등

□ 세부 일정(안)

시 간	주 요 내 용	비 고
14:00~14:02(2분)	■ 개회 및 참석자 소개	정보보호산업과장
14:02~14:07(5분)	■ 기념 촬영	
14:07~14:10(3분)	■ 인사 말씀	제2차관
14:10~14:25(15분)	■ (주제1) 제로트러스트 가이드라인 1.0 핵심 내용	이석준 교수
14:25~14:35(10분)	■ (주제2) 제로 트러스트 보안 모델 실증 계획	최영철 대표
14:35~14:45(10분)		김영랑 대표
14:45~14:55(10분)	■ (주제3) 제로 트러스트 실증 모델 검증 방안	이성권 대표
14:55~15:55(60분)	■ 자유토론 ① 제로 트러스트 도입 관련 기업 애로사항 ② 실효성 있는 제로 트러스트 실증 방안	제2차관
15:55~16:00(5분)	■ 마무리 말씀	제2차관

붙임 3

제로트러스트 보안 모델 실증 · 검증기업 현황

회사명	에스지에이솔루션즈 주식회사	 에스지에이솔루션즈(주)
대표/설립	최영철 / 2002년	
주소	서울특별시 송파구 정의로8길 9, AJ빌딩 6층	
사업분야	제로 트러스트 보안, 클라우드 보안, 시스템 보안, 응용 보안, 교육 및 공공 SI(시스템 통합) 사업, 블록체인, PKI 등	
주요제품	SGA ZTA(ZT보안), RedCastle(서버보안), vAegis(클라우드보안) cAegis(컨테이너보안)	
회사명	프라이빗테크놀로지(주)	
대표/설립	김영랑 / 2018년	
주소	서울특별시 금천구 벚꽃로298 대륭포스트타워6차 13F	
사업분야	제로 트러스트 보안 소프트웨어(클라우드, 모바일, 5G/6G, IoT 등) 전문 개발 및 공급	
주요제품	PacketGo, Pribit Connect, PRIBIT Desktop	
회사명	주식회사 엔키	
대표/설립	이성권 / 2016년	
주소	경기도 성남시 수정구 고등로 3, 현대지식산업센터 412호	
사업분야	화이트햇 컨설팅(침투테스트), 악성코드 분석 및 사이버 위협 인텔리전스, 사이버 공격 방어 대회 운영 및 문제 출제 등	
대표실적	버그바운티 플랫폼 사이버 공격방어훈련(VATE), 제로데이 취약점 연구, 악성코드 분석	