

의안번호	2215639
의 퇴 인	최민희의원
회 답 일	2026. 3. 5.
추 계 번호	25B7249

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

【비용추계서】

I. 비용추계 결과

- (일부추계) 개정안에 따라 과학기술정보통신부장관이 ‘제로트러스트 보안체계 관련 기술의 연구개발 및 표준화, 제로트러스트 보안체계 관련 전문인력 양성’ 사업을 추진할 경우, 추가재정소요는 2027년부터 2031년까지 5년간 총 51억원(연평균 10억 2,000만원)으로 추계됨
- 개정안의 다른 재정수반요인에 대해서는 추계가 곤란하여 일부 재정수반요인에 대해서만 추계한 결과로, 개정안의 전체적인 추가재정소요액은 추계된 금액을 상회할 수 있음

[표 1] 개정안에 따른 비용추계: 2027~2031년

(단위: 백만원)

	2027	2028	2029	2030	2031	합계	평균
제로트러스트 보안체계 관련 기술의 연구개발 및 표준화 (안 제46조의3제2항제1호)	900	900	900	900	900	4,500	900
제로트러스트 보안체계 관련 전문인력의 양성 (안 제46조의3제2항제2호)	120	120	120	120	120	600	120
합 계	1,020	1,020	1,020	1,020	1,020	5,100	1,020

주: 과학기술정보통신부 제출자료 및 유사사례를 참고하여 추계한 것으로, 실제 사업 규모 및 연간 사업비, 실제 교육인원 및 교육과정 수 등에 따라 추가재정소요는 달라질 수 있음
자료: 국회예산정책처

Ⅱ. 재정수반요인

연번	조·항(조제목)	주요내용	비고
1	안 제46조의3(제로트러스트 보안체계의 구축 등) 신설	과학기술정보통신부장관은 제로트러스트 보안체계의 확산을 위하여 다음 각 호의 시책을 수립·추진할 수 있음(제2항) 1. 제로트러스트 보안체계 관련 기술의 연구개발 및 표준화 2. 제로트러스트 보안체계 관련 전문인력의 양성 3. 제로트러스트 보안체계의 시범 적용 사업 4. 「중소기업기본법」 제2조제1항에 따른 중소기업(이하 “중소기업”이라 한다)에 대한 제로트러스트 보안체계 도입 지원 5. 그 밖에 제로트러스트 보안체계의 확산에 필요한 사항 과학기술정보통신부장관은 중소기업이 제로트러스트 보안체계를 도입하는 경우 그에 필요한 경비의 전부 또는 일부를 예산의 범위에서 지원할 수 있음(제3항) 과학기술정보통신부장관은 정보통신서비스 제공자가 제로트러스트 보안체계를 효과적으로 구축·운영할 수 있도록 제로트러스트 보안체계의 구축·운영에 관한 가이드라인을 정하여 고시할 수 있음(제4항)	재량규정

Ⅲ. 비용추계의 전제와 상세내역

1. 재정수반요인별 추계 여부

연번	조·항(조제목)		추계 여부	비고(추계 미 실시 사유)
1	안 제46조의3(제로트러스트 보안체계의 구축 등) 신설	제로트러스트 보안체계 관련 기술의 연구개발 및 표준화(제2항제1호)	○	• 유사사례 등을 참고하여 추계
		제로트러스트 보안체계 관련 전문인력의 양성(제2항제2호)	○	• 유사사례 등을 참고하여 추계

연 번	조·항(조제목)		추계 여부	비고(추계 미 실시 사유)						
		제로트러스트 보 안체계의 시범 적 용 사업(제2항제 3호)	-	•미대상 - 과학기술정보통신부는 현재 제로트러스트 도입 시범사업, 제로트러스트 보안체계의 구축·운영에 관한 가이드라인 수립 등의 사업을 실시하고 있음 - (시범사업) 제로트러스트 제품·서비스에 대한 연동체계 개발 및 수요기업 대상 보안모델 도입·운영 지원을 위한 시범사업 실시('24년~) - (가이드라인) 기존 경계 중심 보안 모델을 대체하는 제로트러스트 보안체계의 확산 추진을 위해 두 차례의 가이드라인 발간 [제로트러스트 확산 지원 사업 현황] (단위: 백만원) <table><tr><th>사업명</th><th>사업내용</th><th>2026</th></tr><tr><td>제로트러스트 신보안체계 실증확산 (제로트러스트 확산 지원)</td><td> - 제로트러스트 도입·확산을 통해 국내 ICT 환경에 적합한 新보안모델 개발 및 시범 적용 - 제로트러스트 보안체계 도입·확산을 위한 가이드라인 수립 등 </td><td>4,510</td></tr></table> 자료: 과학기술정보통신부	사업명	사업내용	2026	제로트러스트 신보안체계 실증확산 (제로트러스트 확산 지원)	- 제로트러스트 도입·확산을 통해 국내 ICT 환경에 적합한 新보안모델 개발 및 시범 적용 - 제로트러스트 보안체계 도입·확산을 위한 가이드라인 수립 등	4,510
	사업명	사업내용		2026						
	제로트러스트 신보안체계 실증확산 (제로트러스트 확산 지원)	- 제로트러스트 도입·확산을 통해 국내 ICT 환경에 적합한 新보안모델 개발 및 시범 적용 - 제로트러스트 보안체계 도입·확산을 위한 가이드라인 수립 등	4,510							
	제로트러스트 보안 체계의 구축·운영 에 관한 가이드라 인 수립(제4항)									
	중소기업에 대한 제로트러스트 보안 체계 도입 지원(제 2항제4호, 제3항)	×	•제3호: 의안의 내용이 선언적·권고적인 형식으로 규정되는 등 기술적으로 추계가 어려운 경우 - 과학기술정보통신부에 따르면 제로트러스트 보안체계로의 전환을 위한 요구사항, 전환비용, 소요기간 등이 기업마다 상이하며, 현 시점에서는 제로트러스트 도입 중소기업의 수를 예측하기 어려우므로, 개정안에 따른 소요 비용을 합리적으로 추계하는 데 한계가 있음							

2. 비용추계의 총괄적 전제

- 개정안 부칙은 공포 후 6개월이 경과한 날부터 시행하도록 규정하고 있으므로, 추계기간은 2027년부터 2031년까지 5년으로 함

3. 재정수반요인별 상세 추계내역

가. 제로트러스트 개요

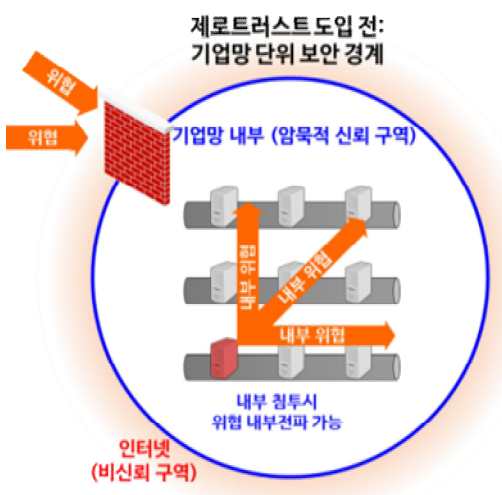
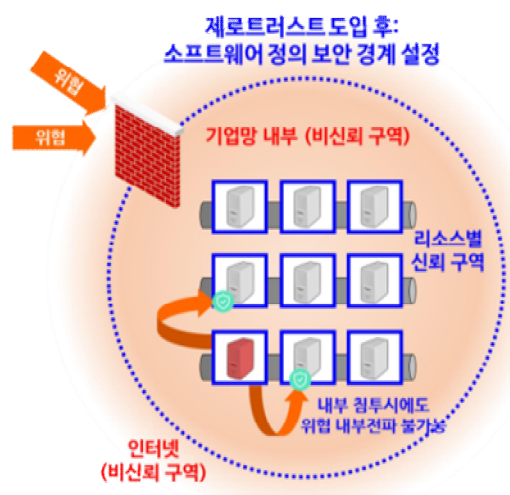
□ ‘제로트러스트’란 네트워크, 물리적 위치 또는 기기에 상관없이 신뢰를 배제하고 항상 네트워크 침해의 가능성을 가정하여 접근 요구에 정확하게 최소의 권한만 부여하는 보안 원칙임

○ 제로트러스트는 기존의 경계 기반 보안 모델이 가진 한계를 극복하기 위하여 제시된 개념임

- 경계 기반 보안 모델은 내부망과 같이 경계를 기준으로 한 번 인증된 기기나 사용자 혹은 트래픽에 대해서는 신뢰를 부여하여 접근을 허용하는 방식으로 현재 가장 보편적으로 사용되고 있는 모델임

※ [참고자료] 제로트러스트 개요

[표 2] 경계 기반 보안 모델과 제로트러스트 모델 비교

경계 기반 보안 모델	제로트러스트 모델
○ 경계(perimeter) 기준 한번 인증된 기기나 사용자, 트래픽은 모두 허가 → VPN, 방화벽 등 ※ 내부자에게 높은 신뢰도를 부여하는 기존 모델의 약점을 이용하여 내부자 권한 탈취를 통한 공격 사례 증가	○ 네트워크 혹은 물리적 위치, 기기에 상관없이 ‘무신뢰’ 원칙(Never Trust, Always Verify) ○ 강화된 인증 및 기기 상태 모니터링 등을 통하여 지속적인 검증을 통해 접근 권한 부여
제로트러스트 도입 전: 기업망 단위 보안 경계  기업망 내부 (암묵적 신뢰 구역) 인터넷 (비신뢰 구역) 내부 침투시 위협 내부전파 가능	제로트러스트 도입 후: 소프트웨어 정의 보안 경계 설정  기업망 내부 (비신뢰 구역) 인터넷 (비신뢰 구역) 리소스별 신뢰 구역 내부 침투시에도 위협 내부전파 불가능

자료: 과학기술정보통신부

나. 제로트러스트 보안체계 관련 기술의 연구개발 및 표준화(안 제46조의3제2항제1호)

□ 과학기술정보통신부장관이 ‘제로트러스트 보안체계 관련 기술의 연구개발 및 표준화’ 사업을 추진할 경우 추가재정소요는 유사사례의 사업비를 참고하여 추계함

□ 유사사례로, 과학기술정보통신부는 ‘정보통신·방송 기술개발사업 및 표준개발지원사업’을 실시하고 있음

○ 정보통신·방송 기술개발사업 및 표준개발지원사업 중 사이버보안부문 지원사업은 2026년 기준 11과제에 대하여 실시하고 있으며, 과제별 사업비는 연간 9억원임

[표 3] 정보통신·방송 기술개발사업 및 표준개발지원사업 중 사이버보안부문 지원사업 개요
(단위: 백만원)

부문	번호	사업명	과제명	'26년 사업비 (총사업비)
사이버 보안	1	정보보호핵심원천기술개발 (데이터및네트워크보호기술개발)	사이버공격 실시간 방어수준 계량평가 및 전주기 자율보안을 위한 시뮬레이터 개발	900 (4,500)
	2	정보보호핵심원천기술개발 (데이터및네트워크보호기술개발)	글로벌 표준 준용 AI기반 한국형 제로트러스트 오픈 플랫폼 기술개발	900 (4,500)
	3	정보보호핵심원천기술개발 (취약점대응및신산업융합보호 기술개발)	사이버 위협 대응을 위한 영상보안 카메라(IP Camera, CCTV) 용 고화질 AI 시스템 반도체 및 모듈 개발	900 (4,500)
	4	정보보호핵심원천기술개발 (공공서비스보호강화)	멀티모달 기반 이중·이형 디지털 증거 전처리 기술 개발	900 (3,300)
	5	AI생태계보안내재화 핵심기술개발 (AI생태계보안내재화핵심기술개발)	LMM(Large Multimodal Model) 생태계의 보안 위협 및 취약점 분석과 안전성 검증 기술개발	900 (4,500)
	6	AI생태계보안내재화핵심기술개발 (AI생태계보안내재화핵심기술개발)	AI 에이전트 신뢰성과 안전성 확보를 위한 자율통제 및 선제적 억제기술 개발	900 (4,500)
	7	AI생태계보안내재화 핵심기술개발 (AI생태계보안내재화핵심기술개발)	AI 서비스의 개발부터 배포까지 전주기의 평가 프레임워크 개발	900 (4,500)

부문	번호	사업명	과제명	'26년 사업비 (총사업비)
	8	AI생태계보안내재화 핵심기술개발 (AI생태계보안내재화핵심기술개발)	AI 지식재산권 보호를 위한 AI 모델 증류 방지 및 증류 추적 기술 개발	900 (4,500)
	9	범국가양자내성 암호전환핵심기술 개발 (범국가양자내성 암호전환핵심기술 개발)	PQC와 QKD를 결합한 도메인 간 양자보안 시스템 개발	900 (4,500)
	10	범국가양자내성 암호전환핵심기술 개발 (범국가양자내성 암호전환핵심기술 개발)	Quantum-Safe 초소형다마이스 실현을 위한 초경량 하드웨어 PQC 전환 기술 개발	900 (4,500)
	11	범국가양자내성 암호전환핵심기술 개발 (범국가양자내성 암호전환핵심기술 개발)	DevOps 기반 양자내성암호 전환 자동화기술 및 오픈플랫폼 개발	900 (4,500)

자료: 과학기술정보통신부

□ 개정안에 따른 ‘제로트러스트 보안체계 관련 기술의 연구개발 및 표준화’ 사업은 유사사례의 과제별 사업비 및 사업기간을 참고하여, 2027년부터 2031년까지 매년 실시(연간 사업비: 9억원)하는 것으로 가정함

○ 이때, 연간 사업비는 추계기간 동안 변동하지 않는 것으로 가정

□ (추계 결과) 과학기술정보통신부장관이 ‘제로트러스트 보안체계 관련 기술의 연구개발 및 표준화’ 사업을 추진할 경우, 추가재정소요는 2027년부터 2031년까지 5년간 총 45억원(연평균 9억원)으로 추계됨

[표 4] 제로트러스트 보안체계 관련 기술의 연구개발 및 표준화에 따른 비용추계: 2027~2031년
(단위: 백만원)

	2027	2028	2029	2030	2031	합계	평균
제로트러스트 보안체계 관련 기술의 연구개발 및 표준화	900	900	900	900	900	4,500	900

주: 과학기술정보통신부 제출자료 및 유사사례를 참고하여 추계한 것으로, 실제 사업 규모 및 연간 사업비 등에 따라 추가재정소요는 달라질 수 있음

자료: 국회예산정책처

다. 제로트러스트 보안체계 관련 전문인력의 양성(안 제46조의3제2항제2호)

- 과학기술정보통신부장관이 ‘제로트러스트 보안체계 관련 전문인력 양성’ 사업을 추진할 경우 추가재정소요는 유사사례의 사업비를 참고하여 추계함
- 유사사례로, 과학기술정보통신부는 ‘정보보호전문인력 양성사업’을 실시하고 있음
 - 과학기술정보통신부는 정보보호전문인력 양성사업 중 사이버보안 분야(클라우드 보안, 블록체인 보안, SW공급망 보안, AI 보안) 전문인력 양성을 위한 교육과정을 운영하고 있으며, 각 분야별 연간 평균 80명(인당 교육단가 150만원)을 대상으로 교육을 실시하고 있음

[표 5] 정보보호전문인력 양성사업 중 사이버보안 분야(클라우드 보안, 블록체인 보안, SW공급망 보안, AI 보안) 교육과정 현황: 2025년 기준

교육분야	총 예산(백만원)	교육 인원(명)	인당 교육단가(백만원)
클라우드 보안	231	150명	1.5
블록체인 보안	115	75명	1.5
SW공급망 보안	77	50명	1.5
AI 보안	79	50명	1.6
평 균		80명	1.5

자료: 과학기술정보통신부

- 개정안에 따른 ‘제로트러스트 보안체계 관련 전문인력 양성’ 사업은 유사사례의 평균 교육인원 및 교육단가를 참고하여, 2027년부터 2031년까지 매년 실시(교육인원 80명, 인당 교육단가 150만원)하는 것으로 가정함
 - 이때, 연간 교육인원 및 교육단가는 추계기간 동안 변동하지 않는 것으로 가정
- (추계 결과) 과학기술정보통신부장관이 ‘제로트러스트 보안체계 관련 전문인력의 양성’ 사업을 추진할 경우, 추가재정소요는 2027년부터 2031년까지 5년간 총 6억원(연평균 1억 2,000만원)으로 추계됨

[표 6] 제로트러스트 보안체계 관련 전문인력의 양성에 따른 비용추계: 2027~2031년

	2027	2028	2029	2030	2031	합계	평균
교육인원 수(A, 명)	80	80	80	80	80	—	—
인당 교육단가(B, 만원/명)	150	150	150	150	150	—	—
추가재정소요(D=A×B, 백만원)	120	120	120	120	120	600	120

주: 과학기술정보통신부 제출자료 및 유사사례를 참고하여 추계한 것으로, 실제 교육인원 및 교육과정 수, 사업비 등에 따라 추가재정소요는 달라질 수 있음

자료: 국회예산정책처

IV. 부대의견

- 과학기술정보통신부 제출자료 및 유사사례를 참고하여 추계한 것으로, 실제 사업 규모 및 연간 사업비, 실제 교육인원 및 교육과정 수 등에 따라 추가재정소요는 달라질 수 있음
- 개정안의 다른 재정수반요인에 대해서는 추계가 곤란하여 일부 재정수반요인에 대해서만 추계한 결과로, 개정안의 전체적인 추가재정소요액은 추계된 금액을 상회할 수 있음

V. 작성자

□ 성명

국회예산정책처	분석관	과장
경제비용추계과	최동완	예승우

□ 대표연락처

성명	전화번호	이메일 주소
최동완	02-6788-3746	dongwaniii@nabo.go.kr

[참고자료] 제로트러스트 개요

(과학기술정보통신부 제출자료)

□ 제로트러스트 개요

- (추진배경) 클라우드 컴퓨팅과 원격·재택 근무 확산에 따른 네트워크의 다변화로 기존 경계 기반 보안 모델의 한계 봉착
 - ※ 최근 침해사고 유형은 내부자 계정탈취 → 내부시스템 침투 → 데이터 유출 등 내부자 권한 탈취에 이은 **횡적이동(Lateral Movement)** 공격이 증가
- (기본개념) 항상 네트워크 침해를 가정, 접근 요구에 정확하고 최소의 권한만 부여하는 Collection of Concepts & Ideas

< 경계 기반 모델과 제로트러스트 모델 비교 >

경계 기반 보안 모델	제로트러스트 모델
○ 경계(perimeter) 기준 한 번 인증된 기기나 사용자 트래픽은 모두 허가 → VPN, 방화벽 등 ※ 내부자에게 높은 신뢰도를 부여하는 기존 모델의 약점을 이용하여 내부자 권한 탈취를 통한 공격 사례 증가	○ 네트워크 혹은 물리적 위치 기기에 상관없이 '무신뢰' 원칙(Never Trust, Always Verify) ○ 강화된 인증 및 기기 상태 모니터링 등을 통하여 지속적인 검증을 통해 접근 권한 부여
제로트러스트도입 전: 기업망 단위 보안 경계	제로트러스트도입 후: 소프트웨어 정의 보안 경계 설정

< 침해 시나리오 적용시 경계 보안 VS 제로트러스트 비교 >

시나리오	경계 기반 보안 모델의 한계	제로트러스트 대응 시나리오
사용자 자격 증명 도용	일반적으로 사용자 자격 증명이 위조될 경우 기기와 관계 없이 기업망 내부 리소스에 접근할 수 있어 피해 발생	- 위장기기인 경우, 접근 권한이 부여 되지 않고 해당 정보에 대한 로그 및 모니터링 - 정상적인 자격 증명 후에도 신뢰도가 충분하지 않은 이벤트 발생시 강화된 다중 인증 적용을 통한 대응
원격공격 혹은 내부자 위협	네트워크에 접속, 권한 상승 후 횡적 이동을 통해 다양한 리소스에 접근하거나 손상시키는 등 피해를 줄 수 있음	- 데이터 접근은 보안정책, 사용자 역할 기기 속성 등에 따라 제한, 세밀한 접근 제어로 민감데이터 접근 불가 - 사용자 행위 모니터링으로 비정상 활동시 추가 인증 요구 혹은 동적인 접근 제한 가능

- **(구현상의 특징)** 제로트러스트 모델은 특정 보안 기능이나 솔루션을 도입하는 것으로 구현될 수 없으므로 단기간 내 구축보다 중장기 계획 필요

※ 글로벌 시장을 선두하고 있는 빅테크 기업(MS, 구글 등)들도 제로트러스트 구축을 위해 이미 7~8년 전부터 보안기업과 M&A 등 협업체제 구축을 하고 있음

< 제로트러스트 구현을 위한 접근 방법 >

접근 방법	세부 내용
① 강화된 인증	· ID, 비밀번호 외에도 다양한 인증 정보를 활용한 다중 인증 등
② 마이크로 세그멘테이션 (Micro Segmentation)	· 서버, 데이터 등을 세부적인 단위로 분리하여 관리
③ 소프트웨어 정의 경계 (Software Defined Perimeter)	· 소프트웨어 기반으로 보호 대상을 분리보호할 수 있는 경계를 생성

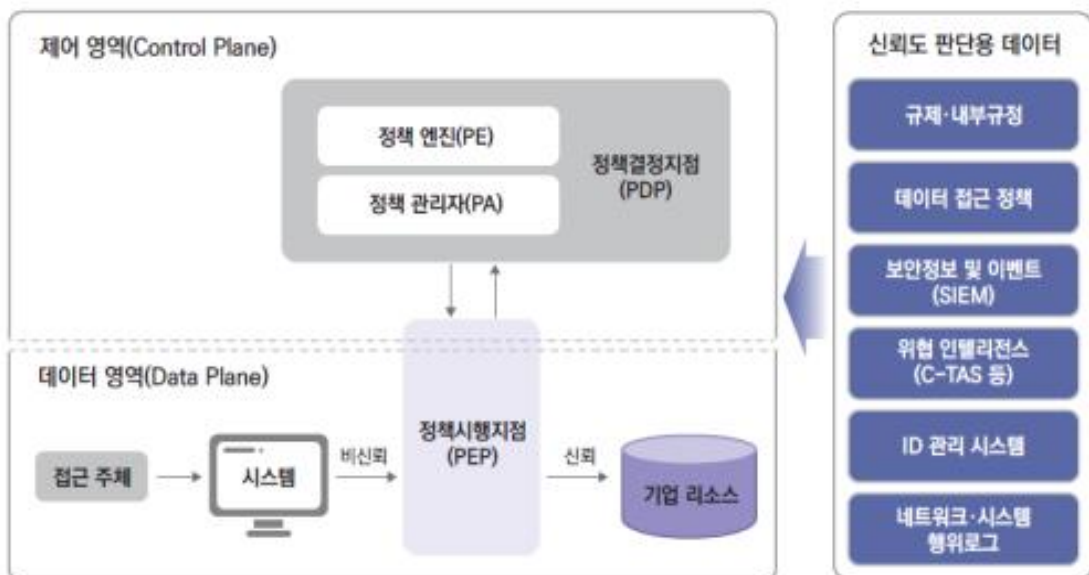
□ 보안원칙 및 구성요소

- (원칙) 제로트러스트 모델 도입에 적용되는 기본 원리로, 총 6가지로 구성

< 제로트러스트 기본 원리 >

구분
(원칙1) 기본 원칙 모든 종류의 접근에 대해 신뢰하지 않을 것 (명시적인 신뢰 확인 후 리소스 접근 허용)
(원칙2) 일관되고 중앙 집중적인 정책 관리 및 접근제어 결정, 실행 필요
(원칙3) 사용자, 기기에 대한 관리 및 강력한 인증
(원칙4) 리소스 분류 및 관리를 통한 세밀한 접근제어 (최소 권한 부여)
(원칙5) 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
(원칙6) 모든 상태에 대한 모니터링, 로그 및 이를 통한 신뢰성 지속적 검증, 제어

- (구성) 제로트러스트 모델은 제어 영역과 데이터 영역을 분리하고, 정책 결정지점(PDP), 정책 시행지점(PEP) 등으로 구성



□ 정부 주요사업

- **(시범사업)** 제로트러스트 제품·서비스에 대한 연동체계 개발 및 수요기업 대상 보안모델 도입·운영 지원을 위한 시범사업 추진('24년~)
 - **(컨설팅)** 민간 기업을 대상으로 제로트러스트 관점에서 현 보안 현황을 진단하고 향후 도입·전환에 대한 계획 수립 지원('24년~)
 - **(가이드)** 기존 경계 중심 보안 모델을 대체하는 제로트러스트 보안체계의 확산 촉진을 위해 두 차례의 가이드라인 발간 추진
 - 제로트러스트의 기본개념을 담은 **'ZT 가이드라인 10」**을 발간('23.7월)
 - 산업계 요구에 따라 구체적 도입·검증 방안을 담은 **20**을 발간('24.12월)
 - **(해설서)** 민간 기업의 자율적 제로트러스트 도입·전환을 위해 자체적인 성숙도 진단 시 활용 가능하도록 성숙도 검증 상세해설서 마련('25.12월)
- ※ 국내 제로트러스트 관련 산·학·연 전문가, 수요·공급기관의 의견수렴을 위한 연구반 운영 병행 中