

과기정통부, 철통 인증 지침(제로트러스트 가이드라인) 2.0 발표

- 기업 철통 인증(제로트러스트) 도입 수준을 진단하고 역량 강화를 위한 방법론 제시 -
- 기업 철통 인증(제로트러스트) 도입 시 실질적인 지침서 역할 기대 -

과학기술정보통신부(장관 유상임, 이하 ‘과기정통부’)와 한국인터넷진흥원(원장 이상중, 이하 ‘KISA’)은 산·학·연 전문가들과 함께 국내·외 최신 동향, 도입 사례를 분석하고 수요·공급기관 대상 의견 수렴을 거쳐 국내 기업들이 철통 인증(제로트러스트) 보안 모형을 도입하는데 참조할 수 있는 「철통 인증 지침(제로트러스트 가이드라인) 2.0」을 마련하였다고 밝혔다.

철통 인증(제로트러스트, Zero Trust)는 정보체계 등에 대한 접속 요구가 있을 때 연결망이 이미 침해된 것으로 간주하여 “절대 믿지 말고, 계속 검증하라(Never Trust, Always Verify)”는 새로운 보안 개념이다.

기존의 보안 모형은 연결망의 내·외부를 구분하여 내부자에게 암묵적인 신뢰를 부여하는 ‘경계기반’ 보안 방식이었다. 하지만, 인공지능·인터넷 기반 자원공유(클라우드)와 같은 새로운 디지털 기술 활용, 재택·원격 근무의 확산으로 기존 보안 모형이 한계를 보임에 따라 보안의 근본적인 체계 전환이 필요한 상황이 되었다.

이에 2023년 7월 과기정통부는 철통 인증(제로트러스트) 보안 모형의 확산을 촉진하고자 「철통 인증 지침(제로트러스트 가이드라인) 1.0」을 마련하여 기본 개념과 원리, 핵심 원칙 등에 대한 설명을 통해 도입 필요성에 대한 인식을 제고하기 위해 노력하였다. 또한, 지침(가이드라인) 1.0에서 제시한 철통 인증(제로트러스트) 보안 모형을 실제 기업환경에 적용하고 검증하는 실증·시범사업을 진행하여 국산 철통 인증(제로트러스트) 보안 모형의 확산 기반을 마련해 왔다.

이번에 발표하는 「철통 인증 지침(제로트러스트 가이드라인) 2.0」은 철통 인증(제로트러스트) 보안 모형에 대한 개념 소개와 인식 제고를 넘어 실제 기업에서 도입하고 활용하는데 실질적인 도움이 될 수 있도록, 미국 등 해외 최신 정책 문서(전략, 지침 등)를 참고하고 철통 인증(제로트러스트) 기존 실증사업 결과를 포함하여 도입을 위한 세부 절차와 방법론을 보강하는 등 철통 인증(제로트러스트) 보안모형 도입·적용을 희망하는 수요자 관점에서 구성하였다.

특히, 각 기업이 철통 인증(제로트러스트) 보안 모형을 도입하고자 할 때 현재 수준을 진단·분석하거나 목표를 설정하고 검증하는 데 활용할 수 있도록 기존 3단계에서 4단계로 구체화된 ‘성숙도 모형’을 정의하였으며, 기업망을 구성하는 핵심요소에 대한 세부역량과 성숙도 수준별 특징을 설명하고 평가를 위한 점검표 제공 및 향상 방안을 제시하였다.

또한, 단순히 철통 인증(제로트러스트)의 기술적 방안을 설명하는 데 그치지 않고, 단계별 고려사항, 조직의 역할, 단계별 이행안 수립을 위한 구체적 방법론 및 예시를 포함하여 도입을 위한 준비부터 실제 운영·정착까지 도움이 될 수 있도록 하였다.

과기정통부 류제명 네트워크정책실장은 “사이버 침해가 갈수록 고도화 되고 다양한 디지털 신기술의 확산으로 기업의 보안 관리 요소가 급격히 증가하는 상황에서 철통 인증(제로트러스트) 보안 체계 전환은 시급하다”면서,

“본 지침(가이드라인)이 앞으로 각 산업 분야의 철통 인증(제로트러스트) 보안 모형 도입을 위한 구체적 실무 진행의 좋은 참고서가 될 것으로 기대하며, 정부는 앞으로도 지속적으로 국내 기업의 제로트러스트 확산을 지원하겠다”고 말했다.

지침(가이드라인)은 과기정통부, 한국인터넷진흥원(KISA), 한국정보보호산업협회(KISIA) 홈페이지를 통해 2024년 12월 3일(화) 14:00부터 무료로 내려받아 사용할 수 있음

담당 부서	정보보호네트워크정책관	책임자	과 장	최영선 (044-202-6450)
	정보보호산업과	담당자	사무관	김소완 (044-202-6451)
	한국인터넷진흥원(KISA)	책임자	팀 장	하병욱 (061-820-1288)
	정책연구실 신기술대응팀	담당자	책임연구원	이혜진 (061-820-1202)

< 제1장 제로트러스트 가이드라인 2.0 개요 >

□ 가이드라인 2.0 목적 및 주안점

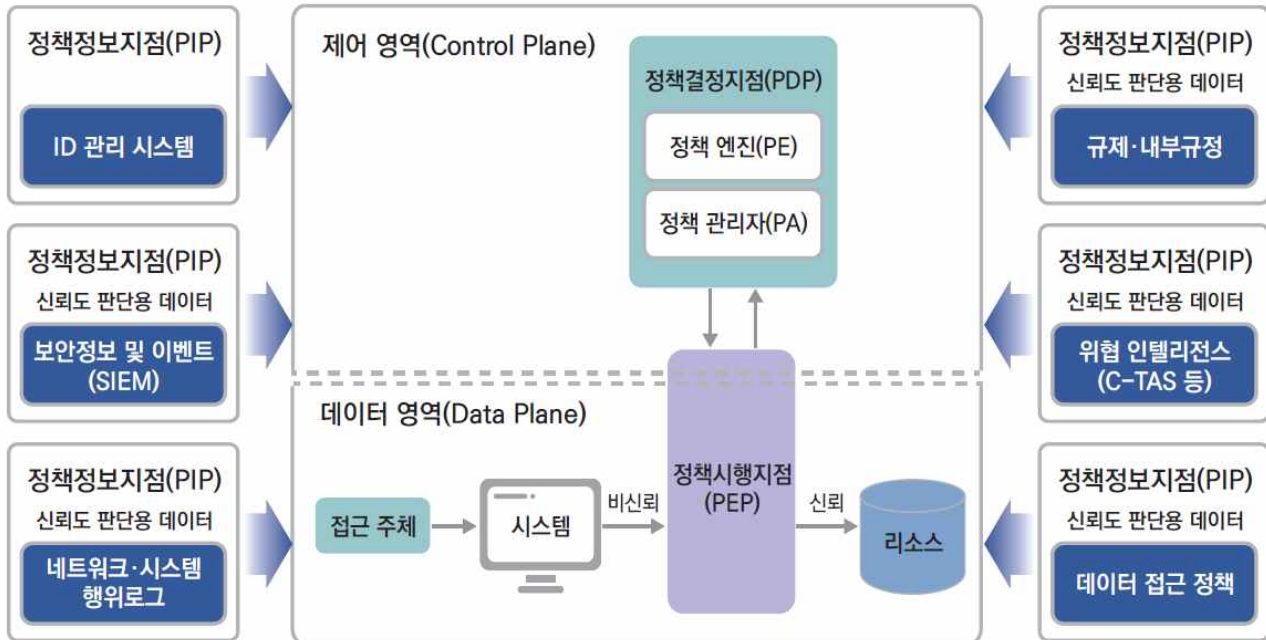
- 대내·외 환경변화 및 실증사업(‘23년) 결과 등을 반영, 조직 의사결정자 및 담당자가 실질적으로 활용할 수 있는 ‘가이드라인 2.0’ 제작

<가이드라인 1.0 대비 2.0 비교표>

구분	가이드라인 1.0	가이드라인 2.0
제로트러스트 성숙도 모델	▶ 3단계(기존-향상-최적화) 성숙도 수준 정의 ▶ 기업망 핵심 요소별 20가지 기능 정의	▶ ‘초기’ 단계를 추가한 4단계(기존-초기-향상-최적화) 성숙도 수준 정의로 고도화 ▶ 기업망 핵심 요소별 27가지 기능 정의 및 각 단계별 특징 구체화 ▶ 기업망 핵심 요소 및 2가지 교차 기능에 대한 52가지 보안 세부역량 및 각 세부역량의 성숙도 수준별 특징 정의 ▶ 성숙도 모델에 기반한 구현 방안 제시
제로트러스트 도입 절차	▶ 제로트러스트 아키텍처 도입 고려 사항 정리(성숙도 모델 관점 및 기업 내외부 환경 관점) ▶ 총 5단계의 제로트러스트 아키텍처 도입 단계 제시(준비 → 계획 → 구현 → 운영 → 피드백 및 개선) ▶ 美OMB 문서를 참고하여 제로트러스트 구현에 따르는 핵심 요소별 초기 전략 제시	▶ 제로트러스트 아키텍처 도입 과정에서의 고려사항 구체화(제로트러스트에 대한 명확한 이해 및 기업 내 인식 제고 등 추가) ▶ 제로트러스트 도입 준비 단계 구체화(업무 구체적 기술 및 예시 제시) ▶ 제로트러스트 아키텍처 도입을 위한 조직 구성 및 목표 설정 방안 제시
기타	▶ 제로트러스트 구현에 관한 6가지 유스케이스 및 목표·요구사항, 구현 방안 등 제시 ▶ 제로트러스트 도입 후 보안 수준 평가 방안 부재	▶ 제로트러스트 도입 후 기업망 보안 수준을 평가할 수 있는 2가지 방안 제시(성숙도 기반 도입 수준 분석을 위한 체크리스트, 침투시험 기반 제로트러스트 효과성 분석 방안) ▶ 부록에서 2023년도 제로트러스트 실증 사례 소개

< 제2장 제로트러스트 보안 모델 및 도입 필요성 >

□ 제로트러스트 보안 모델 및 구성요소



○ (제어 영역, Control Plane) 제로트러스트 아키텍처의 접근제어 정책이 결정되는 논리적 공간으로 정보 및 해당 결과 교환

- 정책결정지점(PDP)*과 정책시행지점(PEP)**에서 통신을 통해, 접근 주체가 요청하는 기업 리소스에 대한 접근 허용 여부를 판단

* 정책 엔진(PE, Policy Engine)과 정책 관리자(PA, Policy Administrator)로 구분

** 데이터 영역에서 접근 주체가 기업 리소스에 접근하고자 할 때 결정된 정책에 따라 연결하거나 종료하는 역할 담당

○ (데이터 영역, Data Plane) 정책이 시행됨으로써 접근 주체가 기업의 리소스에 접근하는 논리적 공간

○ (정책정보지점, Policy Information Point) 신뢰도 판단용 데이터를 제공하는 역할 담당

- 정책 결정을 내리는데 활용하기 위해 수집한 사용자, 기기 및 기타 정책 관련 정보 제공

< 제3장 제로트러스트 성숙도 모델 및 세부역량 >

□ 제로트러스트 성숙도 모델 2.0

- (제로트러스트 성숙도 모델) 조직의 현재 성숙도를 이해하고, 이를 향상시키기 위해 필요한 구체적인 행동 계획 수립 시 사용
 - (활용) 조직의 보안 위협 대응 능력 향상, 변화하는 사이버 위협 환경에 효과적 적응 및 체계적인 로드맵 마련, 구체화된 개선·최적화 가능
 - (구성) 美 CISA의 4단계 성숙도 모델과 NSA의 성숙도 개선 문서 등을 참고하여 성숙도 모델 2.0으로 고도화

< 제로트러스트 성숙도 수준 4단계 >

1. 기존 단계 (정적, 경계 기반, 수동)	2. 초기 단계 ⁶ (일부 자동화)	3. 향상 단계 (자동화, 중앙집중적, 통합)	4. 최적화 단계 (동적, 완전 자동화)
- 주요 구성 요소들이 수동으로 설정되며, 정적인 보안 정책으로 인해 유연하지 못하게 정책시행 - 경계 기반 보안 위주의 보안 아키텍처 구성 - 수동으로 사고에 대응하며, 시스템에 대한 가시성이 제한적	- 일부 프로세스가 자동화되며, 핵심 요소별 연계가 일부 이루어짐 - 속성 할당과 생명주기 관리가 부분적으로 자동화되며, 내부 시스템에 대한 기본적인 모니터링 제공 - 프로비저닝 이후 최소 권한 변경에 대응 가능	- 자동화의 범위가 확장되고, 중앙 집중 제어가 강화되는 단계 - 중앙 집중식으로 통합된 가시성 제공 - 중앙 집중식 ID 관리를 통해 핵심 요소 간 상호작용에 기반한 정책 시행	- 자산 및 리소스에 대한 속성이 완전히 자동으로 할당되며, 동적인 정책이 적용되는 단계 - 자동화된 트리거에 기반한 동적 정책 생성 - 자산에 대해 동적 최소 권한 기반 접근 허용 - 구성요소 간 상호운용성을 위한 개방형 표준 준수 이행 및 강화

< 제로트러스트 성숙도 모델 2.0 요약 >

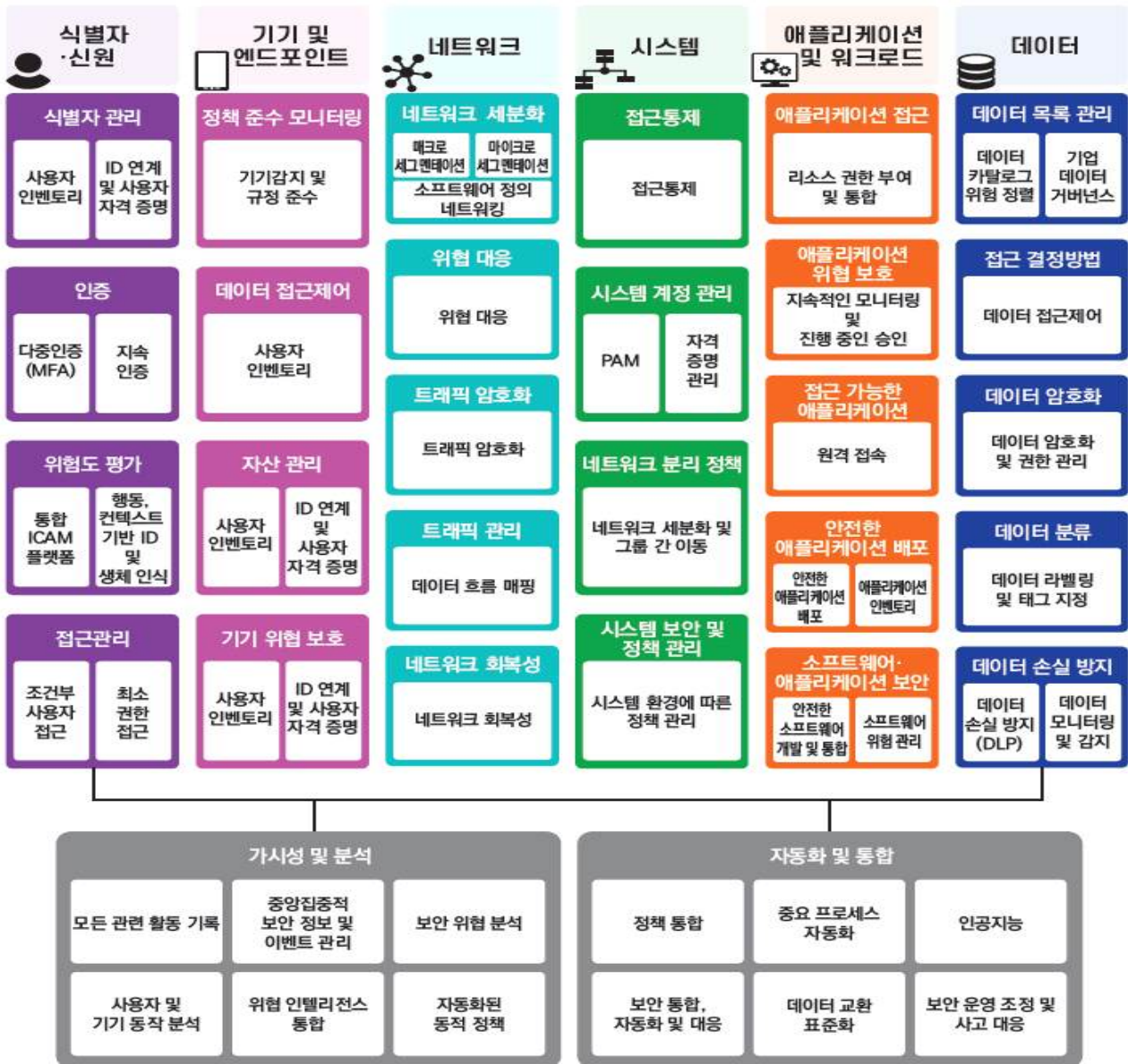
	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
식별자 · 신원	- 온프레미스ID 사용 - 패스워드 혹은 다중인증 방식 - 수동접근 및 자격증명 관리	- 클라우드와 온프레미스 기반 ID 연계 - 다중인증 및 FIDO 기반인증 - 수동 및 정적 규칙 기반 위험 판단	- 컨텍스트 기반 ID 인증 - 일부 자동화된 및 동적 규칙을 이용한 위험도 평가 - 세션 기반 접근 지원	- 클라우드와 온프레미스 시스템 전반에 걸친 글로벌ID - AI 기반 위험도 결정 및 지속적 보호 - 자동화된 적시·최소 권한 접근 적용
기기 및 엔드포인트	- 제한된 정책준수정보 - 단순하고 수동적 기기 목록 관리 - 수동적위협보호 기능 적용	- 대부분의 기기에 정책 준수 시행 메커니즘 사용 - 모든 기기에 대해 목록화 - 기기 보안솔루션 자동 관리	- 규정 준수 여부에 따른 접근 권한 부여 - 검증된 기기만 데이터 접근 - 자동화, 중앙집중식 위협 보호 및 자산관리 기능 통합	- 지속적인 기기 보안 상태 모니터링 및 검증 - 모든 환경에 걸쳐 자산 및 취약점 관리 통합 - 모든 기기에 대해 위협 보호

네트워크	• 경계 분리 네트워크 구조 정의 • 알려진 위협 및 정적 트래픽 필터링 • 매우 중요한 애플리케이션 및 워크로드에 대한 기능 회복	• 소규모 경계를 통해 확장된 네트워크 구조 정의 • 내부 애플리케이션 모든 트래픽 및 외부 일부 트래픽 암호화 • 위험성이 없는 워크로드에 대한 탄력적인 네트워크 회복	• 마이크로 세그먼트를 통해 엔드포인트 및 애플리케이션 격리 메커니즘 배포 • 비정상적인 데이터 흐름 격리 및 제거 • 자동화된 위협 인식 기반 동적 네트워크 규칙 생성	• 컨텍스트 기반 및 기계학습 기반 위협 보호 통합 • 암호화 민첩성 • 우선 순위 지정 가능한 동적 네트워크 규칙 생성
시스템	• 로컬 시스템 기반 ID/패스워드 등 단순 인증 • 정적 속성 등 최소한의 권한 분리 정책 적용 • 온프레미스 시스템 보안 패치 및 정책 수동 변경	• 독립적인 시스템으로 계정 관리 • 일부 중요도에 따르는 네트워크 세분화 • 온프레미스 및 클라우드 시스템에 대한 패치 수준 자동 확인 기능	• 동적 접근 권한 통제 • 등급 및 기능별 네트워크 분류 • 온프레미스 및 클라우드 시스템에 대한 자동화된 보안 패치	• 다중인증 및 신뢰도 기반 접근 인가 • 세분화된 리소스별 접근 정책 적용 • 온프레미스 및 클라우드 상의 모든 시스템 실시간 모니터링 및 자동화된 보안 패치
애플리케이션 및 워크로드	• 로컬 인가 및 정적 속성 기반 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대해 최소한의 통합 • 정적 수동 테스트 수행	• 애플리케이션 워크플로우와 위협 보호에 대한 기본적인 통합 • CI/CD 파이프라인 DevSecOps, SBOM 적용 • 동적 테스트 방법 사용	• 확장된 컨텍스트 정보 및 최소 권한 원칙의 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대한 강력한 통합 • 정기적인 자동화된 테스트	• 실시간 위협 분석을 통해 지속적 애플리케이션 인가 • 모든 애플리케이션에 사용자 및 단말 직접 접근 가능 • 자동화된 코드 배포 및 소프트웨어 검증
데이터	• 정적, 수동 데이터 분류 및 접근 제어 • 온프레미스 및 암호화되지 않은 데이터 저장소 • 제한된 임시 데이터 분류	• 일부 자동화된 추적 기반 수동 데이터 분류 및 목록화 • 최소한의 권한 요소를 통합한 데이터 접근 • 정적 레이블 및 수동 메타데이터 데이터 분류	• 속성에 기반한 최소 권한 제어 기법으로 접근 관리 • 저장소의 모든 데이터 암호화 • 레이블 지정 프로세스 계층화 및 데이터 목록화 자동화	• 시를 이용한 지속적인 데이터 분류 및 목록화 자동화 • 적시 최소 권한 동적 데이터 접근 • 사용 중인 데이터 암호화 및 최신 암호화 적용

□ 제로트러스트 성숙도 향상을 위한 핵심 기능과 세부역량

- 가이드라인 2.0은 성숙도 모델의 추상성을 극복하고 기업의 정보보호 담당자들이 제로트러스트를 실질적으로 적용·실행할 수 있도록 더 명확하고 구체적인 세부역량의 성숙도 수준별 특징을 정의
- 6가지 기업망 핵심 요소 및 2가지 교차 기능에 대한 27가지 기능(Function) 및 52가지 보안 세부역량(Capability)과 성숙도 수준별 특징 제시
 - 세부역량 정의 구체화 및 실행 방안을 포함하여 기업에서 성숙도 모델을 실제 적용 가능할 수 있도록 함

< 제로트러스트 성숙도 향상을 위한 핵심 기능 및 세부역량 >

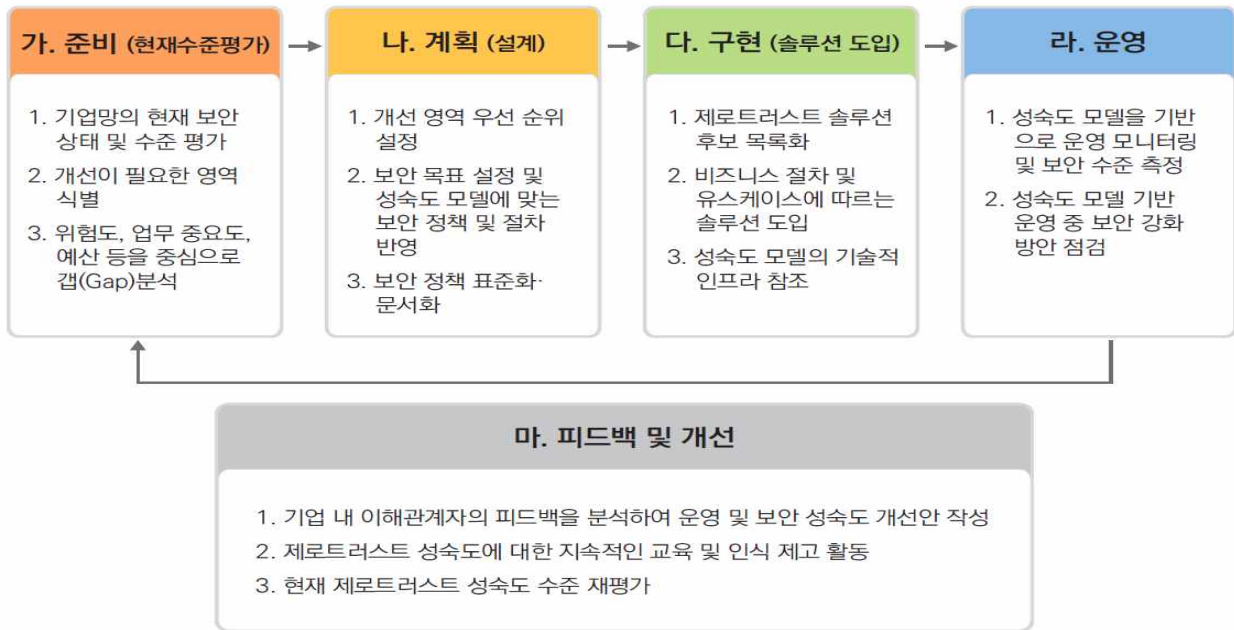


< 제4장 제로트러스트 도입 준비 방안 >

□ 제로트러스트 도입 절차 및 구성 방안

- ‘준비→계획→구현→운영→피드백 및 개선’ 총 5단계로 구성되는 순환 주기에서 성숙도 모델의 활용 방안 등을 설명
- 접근 주체, 보호 대상의 식별·정의, 현재 기업의 보안 아키텍처 분석 등을 통해 제로트러스트 구현 로드맵 수립 방안을 제시

< 제로트러스트 도입 절차 및 성숙도 모델 활용 방안 5단계 >



< 제5장 제로트러스트 도입 수준 분석 >

□ 제로트러스트 도입 수준 평가

- 기업이 제로트러스트 성숙도 수준을 평가하고 도입 계획 수립에 활용할 수 있는 성숙도 모델 기반* 체크리스트 제공

* 제3장에서 정의한 '성숙도 모델 2.0'의 52가지 세부역량과 연계하여 성숙도 수준을 구분

< (예시) 식별자·신원 핵심 요소 중 식별자 관리 기능의 체크리스트 >

세부역량	확인방법	성숙도	Check
사용자 인벤토리	• 사용자 목록에 대한 문서화가 되어있는가?	기존	☐
	• 사용자 역할에 따른 상세 인벤토리가 구축되어 있는가?	초기	☐
	• 자동화된 인벤토리 관리 기구가 도입되어 있는가?	향상	☐
	• 비정상적인 사용자 활동에 대한 탐지가 가능한가?	향상	☐
	• AI 기반 사용자 행동에 따른 관리가 되는가?	최적화	☐
	• 인벤토리가 통합되어 사용자 및 권한 관리 최적화가 되어 있는가?	최적화	☐
ID 연계 및 사용자 자격 증명	• 사용자 자격 증명에 대한 ID 연계 솔루션이 적용되어 있는가?	기존	☐
	• 여러 시스템 간 사용자 자격 증명에 대한 연동이 되어 있는가?	초기	☐
	• ID 통합 관리 시스템이 구축되어 있는가?	향상	☐
	• 글로벌 수준의 ID 연계 솔루션이 적용되어 있는가?	최적화	☐