GISC 2024

Global ICT Standards Conference 2024

2024. 11. 4.(MON) ~6.(WED)

ELTOWER GRACE Hall 6F

(세션4) 차세대 보안: 안전한 디지털 미래를 위한 표준

디지털 전환 시대의 보안 패러다임: 제로트러스트 표준화와 구현 전략

염흥열, 명예교수, 순천향대학교

ICT Standards and Intellectual Property : Inclusive Innovation

주최 과학기술정보통신부 특허청 주관 국립전파연구원 TTA IITP KEA kisto ETRI

목 차

1

제로트러스트 배경

1 환경의 변화

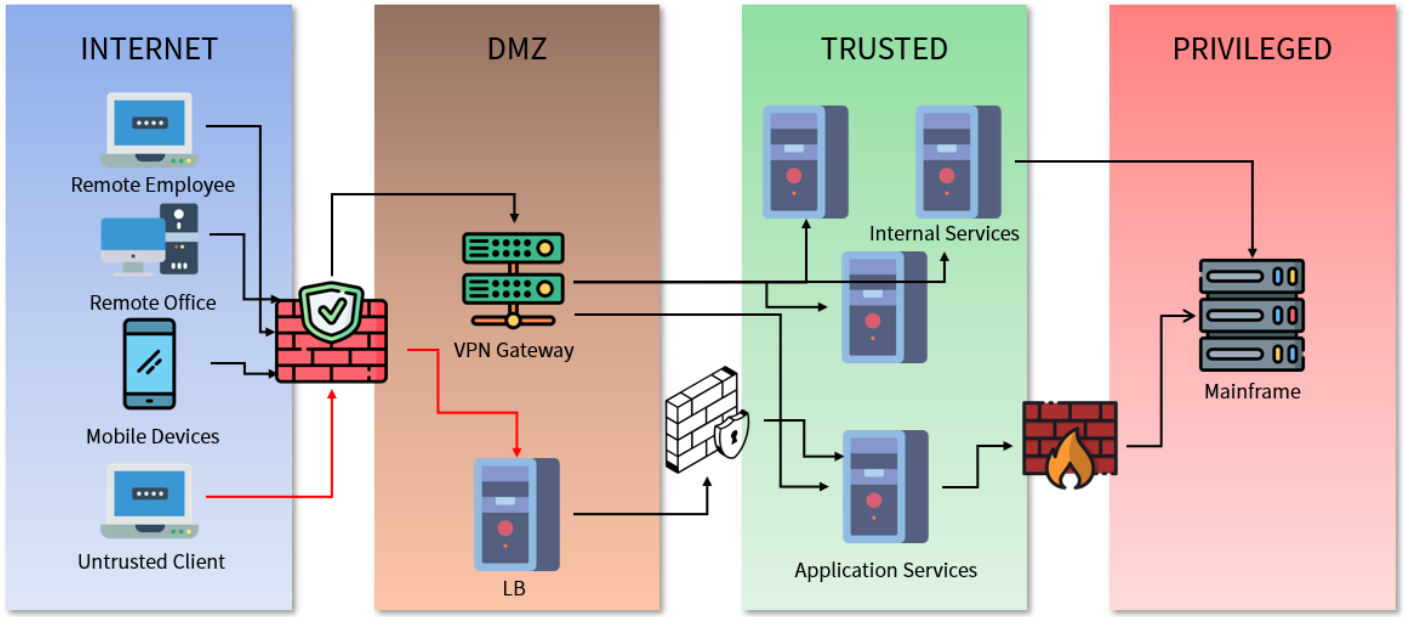
〈경계보안 체계의 한계 및 최근 대표적인 사이버 침해사고〉

(출처: 제로트러스트 가이드라인 1.0 요약본, 과기정통부, 2023.06)

- ❑ 디지털 전환의 가속화로 사이버보안 영역 또한 다양한 산업 분야로 확장(IoT, 원격, 재택 근무 등)
- ❑ 사용자와 디바이스의 증가로 인한 복잡한 권한 관리 등 각 조직의 사이버보안 관리가 어려움
- ❑ 최근 침해사고 유형은 내부자 공모 or 권한 탈취 등 경계보안의 암묵적 신뢰 정책 허점을 이용하는 형태가 증가

2 경계 기반 보안의 네트워크 구성 예

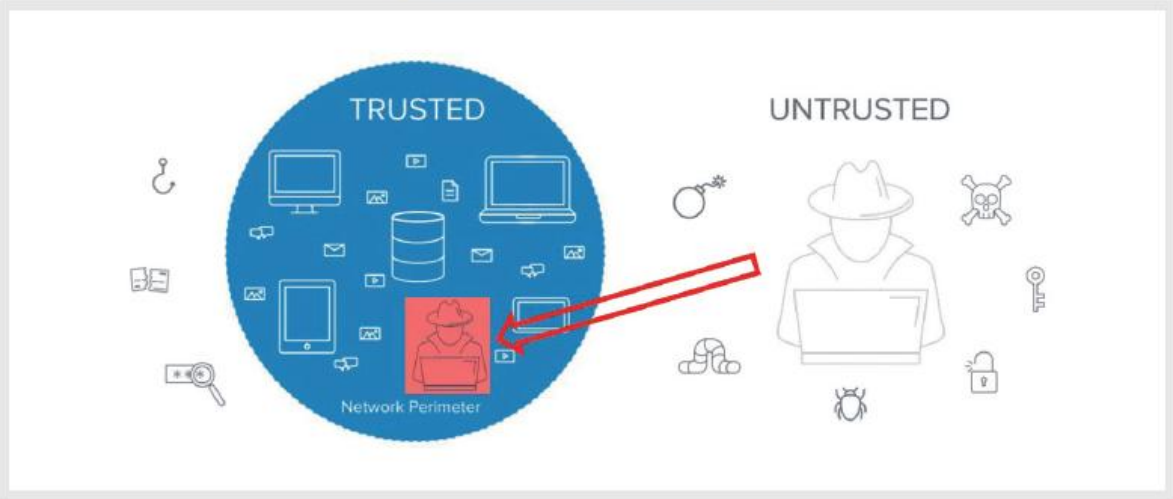
- **경계 기반 보안**
  - 외부 공격자가 기업 네트워크에 액세스하지 못하도록 차단하는 전통적인 모델
  - 다양한 영역(인터넷, 비무장 영역, 신뢰할 수 있는 영역, 권한이 부여된 영역)이 VPN 게이트웨이와 같은 다양한 통제를 통해 보호
- **인터넷**
  - 신뢰할 수 없는 네트워크
- **방화벽, IDS/IPS**
- **DMZ**
  - 권한이 부여된 네트워크와 인터넷 사이에 존재하는 영역
  - 로컬 브로커, VPN 게이트웨이
- **신뢰 네트워크**
  - 내부 서비스, 애플리케이션 서비스
- **Privileged**
  - 메인프레임, 모든 거래를 담당하는 핵심 뱅킹 시스템.



*LB: Local Broker

3 기존 경계 기반 모델 한계

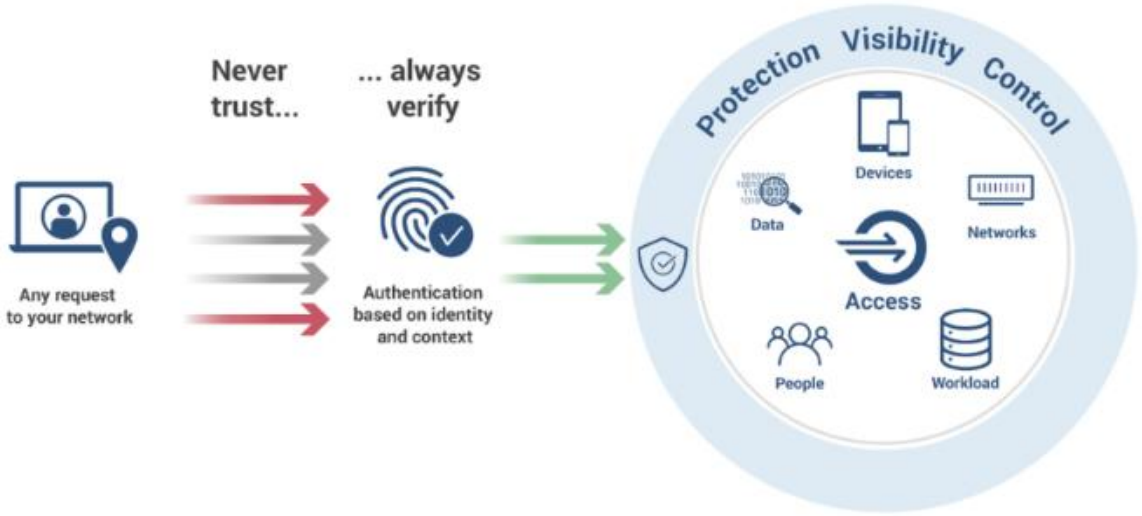
〈경계 기반 보안모델의 한계 상황〉



(출처: 제로트러스트 가이드라인 1.0 요약본, 과기정통부, 2023.06)

- 기존 경계 기반 보안모델은 내부자에 대한 **암묵적 신뢰**와 함께 **높은 권한**을 부여함에 따라 고도화·지능화되는 보안 위협에 한계 노출
  - 내부 접속 사용자·기기 또는 내부 트래픽에 대해 외부에서 요구하는 접속과 비교하여 높은 수준의 신뢰성을 부여
- 다수 기업들은 기존 보안기술을 일부 개선·보완·진화한 **SIEM, SOAR, XDR** 등의 보안관제 솔루션을 도입·운용 중
  - 그러나 기업망 내부의 다양한 악성 행위 감시, 리소스 외부 유출에 대한 철저한 모니터링·분석, 보안 기능 자동화·통합 등에 한계

4 제로 트러스트 아키텍처 근본 요소



- 최소 접근 권한
- 디바이스 검증
- 다중요소 인증 (MFA)
- 마이크로 세그먼트
- 모니터링

(출처: https://www.privacyaffairs.com/zero-trust-network/)

5 제로 트러스트 핵심 논리적 구성 요소

❑ 정책 엔진(PE)

- 이 구성 요소는 특정 주체에 대한 리소스 액세스 권한을 부여하는 최종 결정을 담당.

❑ 정책 관리자(PA)

- 이 구성 요소는 대상과 리소스 간의 통신 경로를 설정하거나(관련 PEP에 대한 명령을 통해) 대상과 리소스 간의 통신 경로를 차단하는 역할 수행.

❑ 정책 시행 지점(PEP)

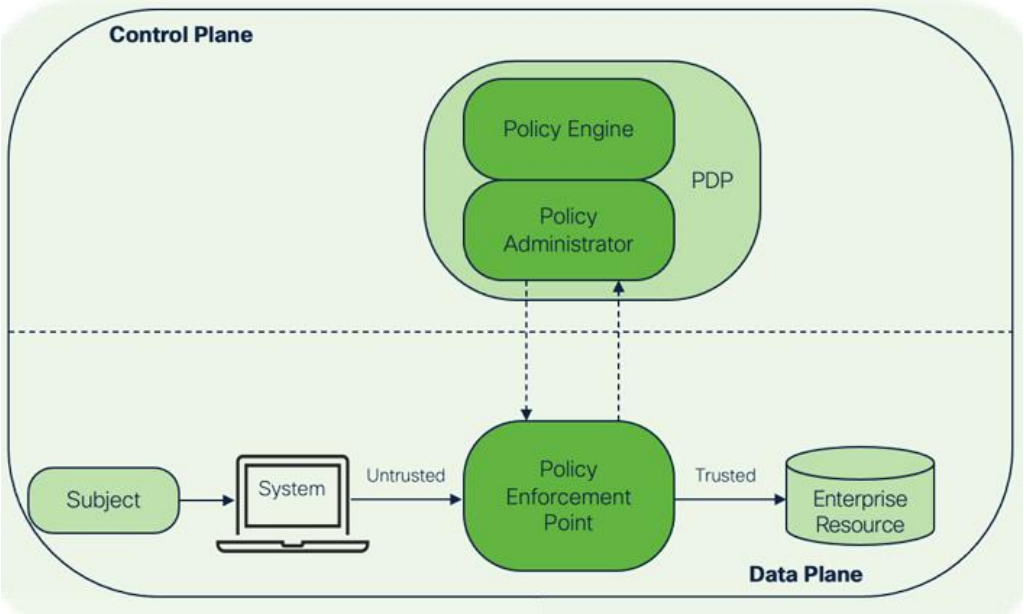
- 이 시스템은 대상과 엔터프라이즈 리소스 간의 연결을 활성화하고, 모니터링하며, 최종적으로 연결을 종료하는 역할을 담당.

❑ 주체 (subject)

- 엔터프라이즈에 대한 액세스 권한이 필요한 주체
- 액세스 권한은 정책 결정 지점(PDP)과 해당 정책 시행 지점(PEP)을 통해 부여.
- 리소스에 대한 액세스를 요청하는 최종 사용자, 애플리케이션 또는 엔터티.

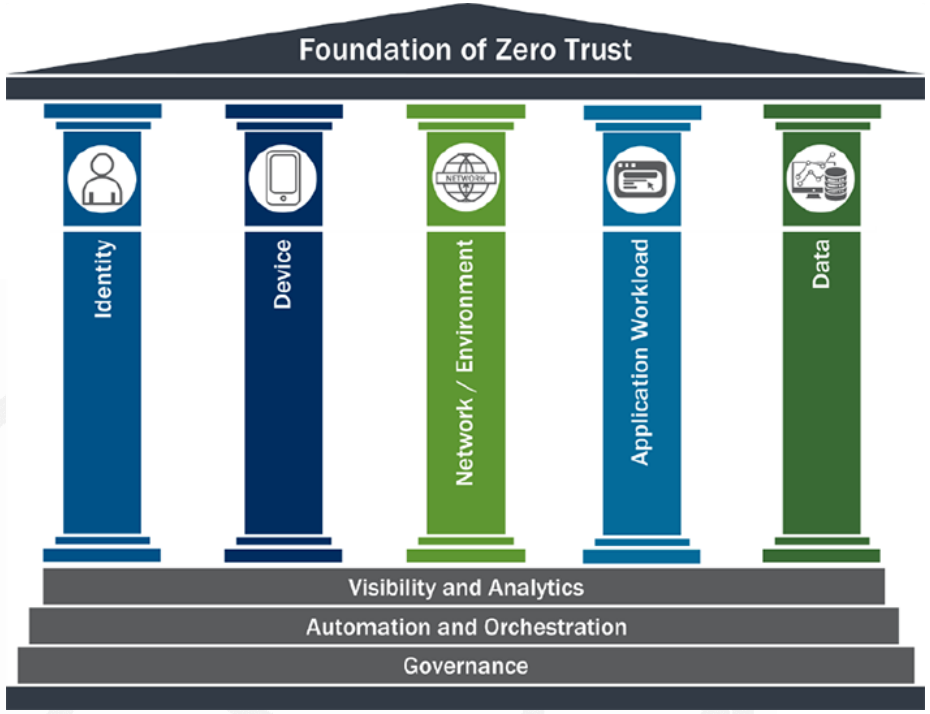
❑ 리소스

- 데이터, 컴퓨팅 리소스, 애플리케이션/서비스 등.
- 보호할 자산.



(Source: NIST SP 800-207)

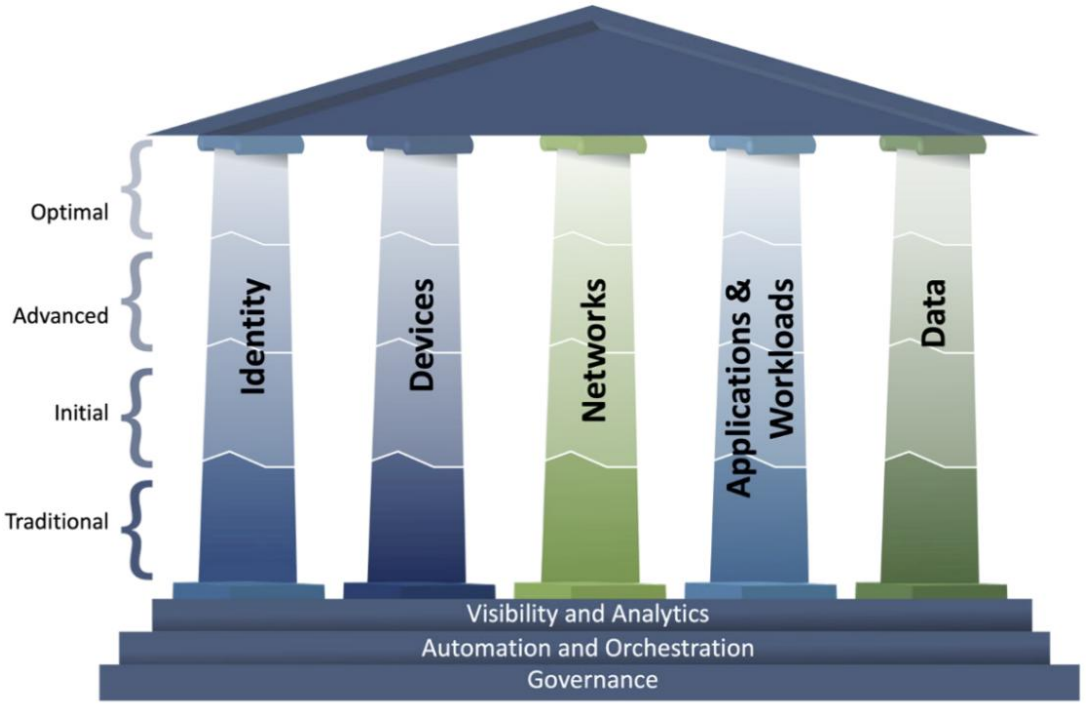
CISA : 제로 트러스트 필러



(Source: CISA)

- **신원(identity):** 지속적인 유효성 검사 및 행동 분석을 통해 사용자 액세스를 관리.
- **디바이스(device):** 소유권에 관계없이 네트워크에 액세스하는 모든 디바이스의 인벤토리 유지
- **네트워크/환경(network/environment):** 경계 방어가 아닌 내부 및 외부 트래픽 관리에 집중
- **애플리케이션 워크로드(application/workload):** 온프레미스 및 클라우드 기반 애플리케이션에 대한 세분화된 접속 제어 및 보호 정책 구현
- **데이터(data):** 데이터의 상태에 관계없이 지속적인 모니터링 및 암호화 보장
- **가시성 및 분석(visibility and analysis):** 정책 의사 결정 및 위협 대응 강화
- **자동화 및 오케스트레이션(automation and orchestration):** 인사이트를 활용해 운영을 간소화하고 위험을 완화.
- **거버넌스(governance):** 다양한 규제 및 운영 요건 준수 보장

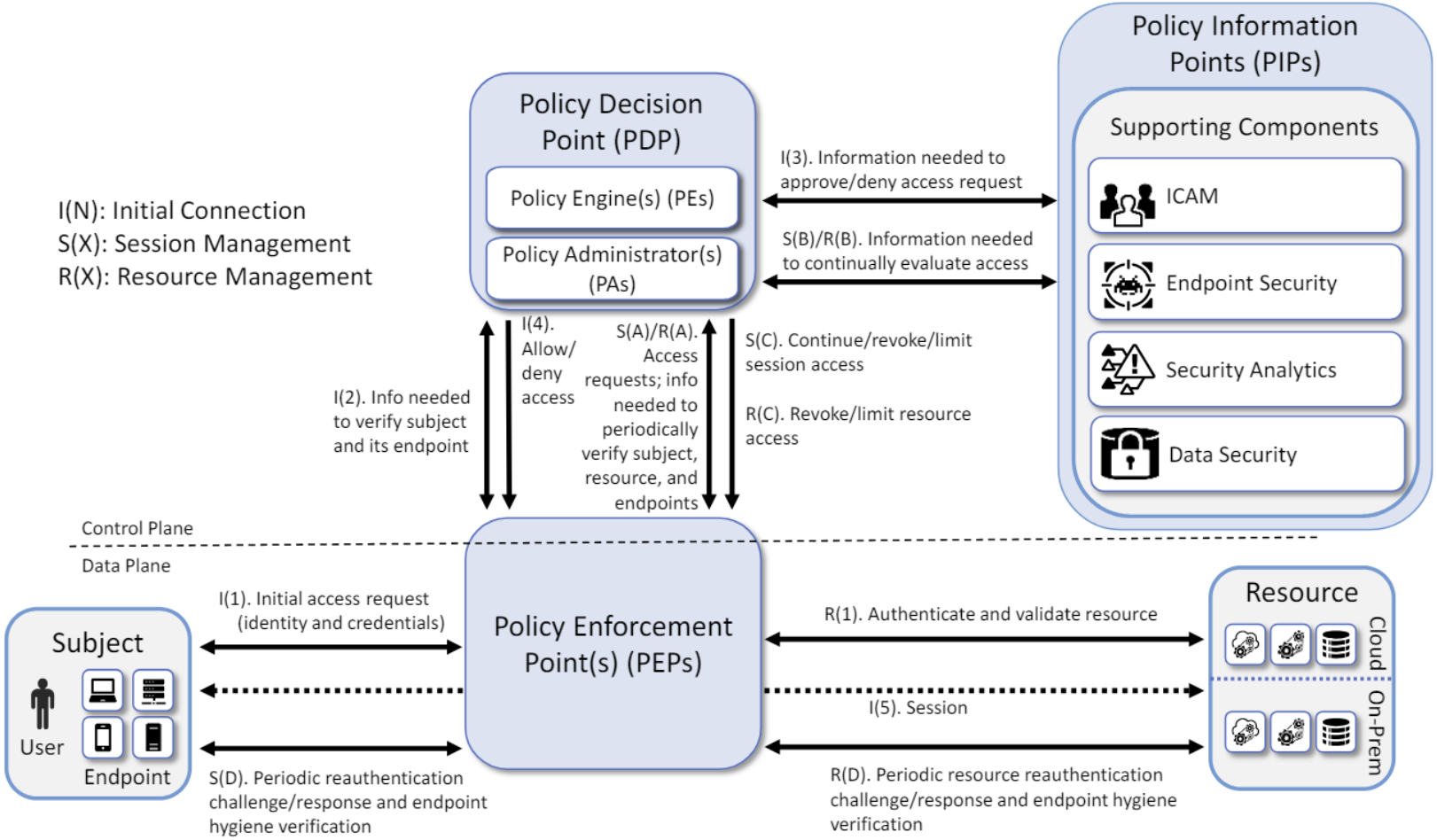
CISA : 제로트러스트 성숙도 모델



(Source: CISA)

- 기존
  - 수동 구성 및 사일로화된 정책 적용을 통한 기본 보안 조치.
- 초기
  - 구성 및 적용 결정에 자동화를 도입하여 내부 시스템에 대한 가시성을 높입.
- 고급
  - 중앙 집중식 가시성과 위험 평가를 기반으로 한 동적 정책 시행을 통한 자동화된 제어.
- 최적
  - 동적 정책과 자체 보고 자산을 갖춘 완전 자동화된 시스템.

일반적 ZTA 참조 구조 (NIST)

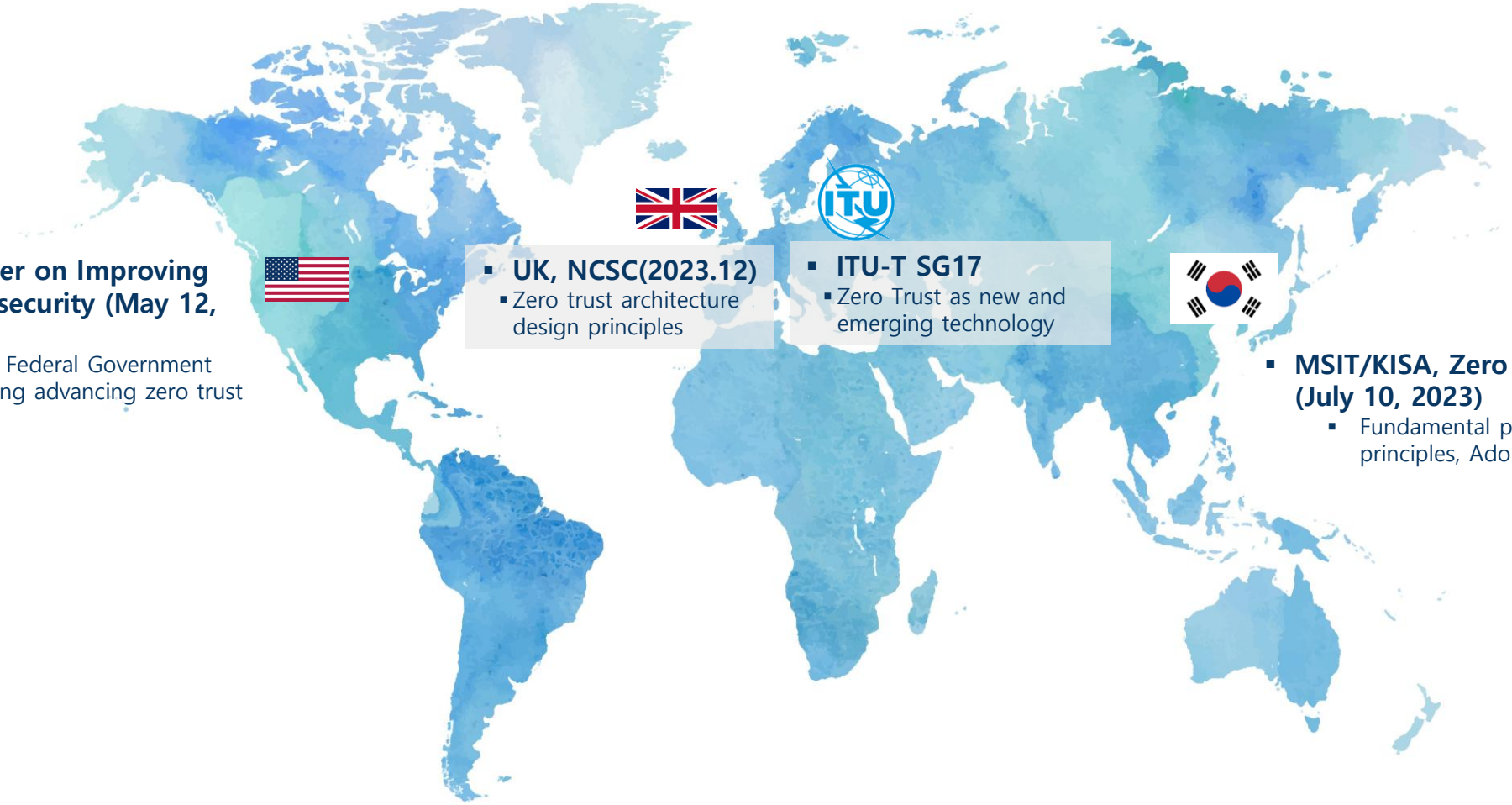


(source: NIST-1800-35)

2

제로 트러스트 주요국 정책 및 표준화 동향

제로 트러스트 보안 정책 동향 개요



- **WH, Executive Order on Improving the Nation's Cybersecurity (May 12, 2021)**
  - Sec. 3. Modernizing Federal Government Cybersecurity including advancing zero trust architecture.

- **UK, NCSC(2023.12)**
  - Zero trust architecture design principles

- **ITU-T SG17**
  - Zero Trust as new and emerging technology

- **MSIT/KISA, Zero trust guidelines 1.0 (July 10, 2023)**
  - Fundamental principles, Access control principles, Adoption reference model, etc.

2 제로 트러스트 관련 주요국 정책 동향

구분	내용
美 NIST, SP 800-207: Zero Trust Architecture('20년) NIST 1800-35, Implementing a Zero Trust Architecture ('23)	(800-207) 제로트러스트 아키텍처 정의, 원칙, 보안위협, 전환 단계 등 제로트러스트 도입과 관련한 내용 정의 (1800-35)상호 운용 가능한 개방형 표준 기반 ZTA 예제 구현 구축
美 조 바이든 행정부, 사이버 보안 강화를 위한 EO('21년)	행정명령(EO)에 제로트러스트 용어가 11번 언급되는 등, 제로트러스트를 활용한 보안 정책을 강조
美 CISA, Zero Trust Maturity Model('21년)	제로트러스트 성숙도 모델에 대해 제시 (제로트러스트 아키텍처 구성을 위한 방향성을 제시)
ITU-T SG17, ITU-T TR.zt-acp('21년)	통신 네트워크에서의 제로트러스트 기반 접근 제어 플랫폼 가이드라인 접근 제어 프로세스에서의 보안 위협과 세부 요구사항 등을 제시
美 DoD, Zero Trust Strategy('22년)	제로트러스트 전략에 대해 제시 (제로트러스트 개발과 제로트러스트로의 변화와 관련한 지침에 대해 설명)
3GPP, Study on applicability of the zero trust security principles in mobile networks('22년)	5G 코어 네트워크에 적용 가능한 제로트러스트 보안 원칙 제시 잠재적인 보안 위협, 연구 필요성, 보안 강화 사항 등을 제안
美 CISA, Zero Trust Maturity Model v2.0 ('23년)	제로트러스트 성숙도 모델 2.0 발간
ITU-T SG17, ITU-T X.ztmc('24년)	통신 네트워크에서 상위 수준의 제로트러스트 모델과 보안 기능에 대한 가이드라인 8개의 주요 영역과 각 영역이 갖추어야 할 보안 능력을 제안
IEEE WG on WG on zero trust security ('24년)	IEEE Computer Society - Cybersecurity and Privacy Standards Committee - ZTSWG - Zero Trust Security 신설 (2024년), 현재 P3409, Standard for a Zero Trust Security Framework 워크 아이템 개발 중

WH, 국가 사이버 보안 개선에 관한 행정 명령(EO 14028) - 2021년 5월 12일

❑ Contents

- Section 1. Policy.
- Section 2. Removing Barriers to Sharing Threat Information.
- Sec. 3. 연방 정부 사이버 보안 현대화
  - 연방 정부는 위협에 대한 연방 정부의 가시성을 높이는 등 사이버 보안에 대한 접근 방식을 현대화하기 위한 결정적인 조치를 취해야 함
  - 연방 정부는 보안 모범 사례를 채택하고 제로 트러스트 아키텍처로 나아가야 함.
- Sec. 4. Enhancing Software Supply Chain Security
- Sec. 5. Establishing a Cyber Safety Review Board
- Sec. 6. Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents.
- Sec. 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks.
- Sec. 8. Improving the Federal Government's Investigative and Remediation Capabilities
- Sec. 9. National Security Systems
- Sec. 10. Definitions

MAY 12, 2021

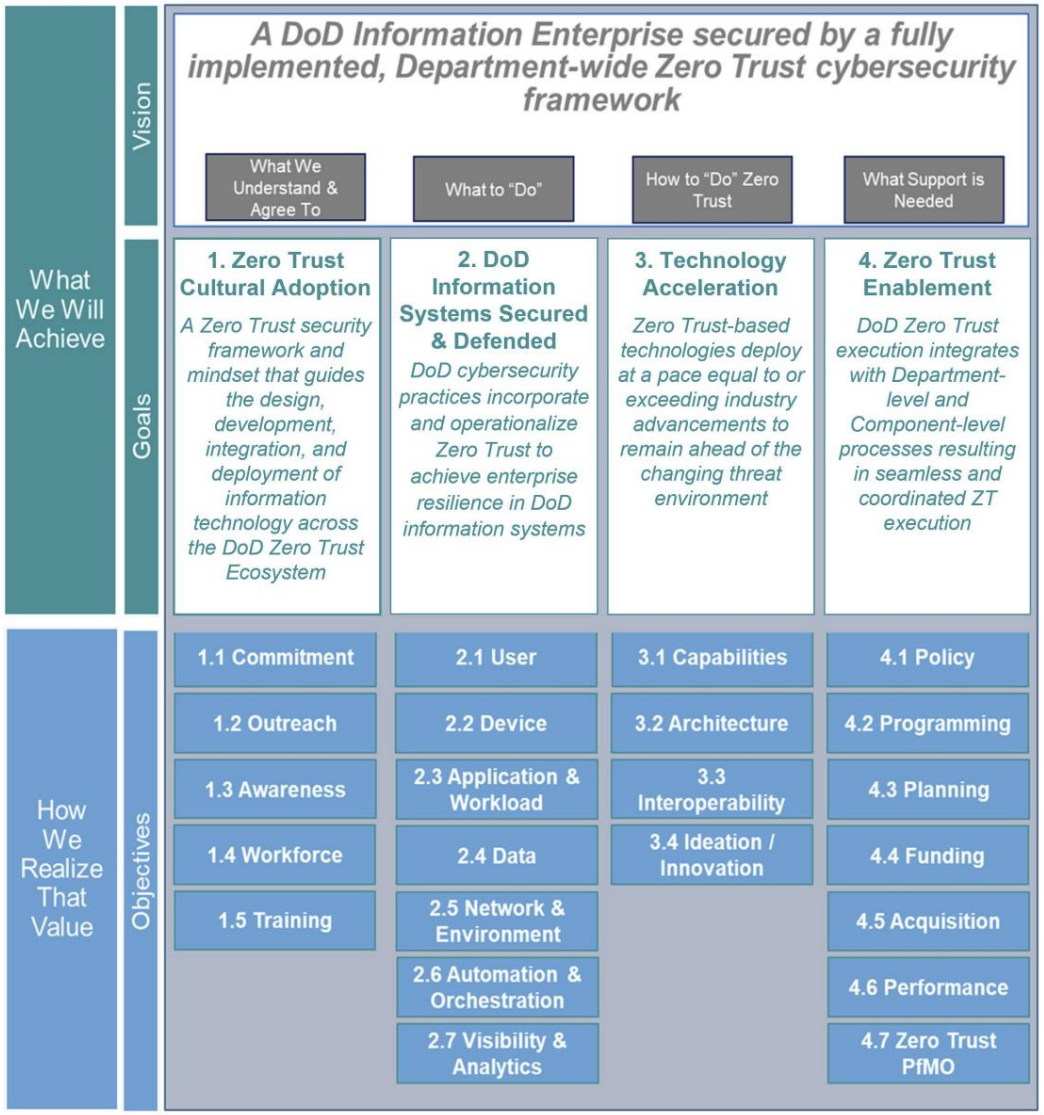
Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

(Source: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)

4 DoD 제로 트러스트 전략

- **비전**
  - 부서 전체에 완벽하게 구현된 제로 트러스트 사이버 보안 프레임워크
- **목표**
  - 제로 트러스트 문화 도입
  - 구현 시스템 보안 및 방어
  - 기술 가속화제로 트러스트 활성화
- **제로 트러스트를 실현하는 방법**
  - 헌신, 아웃리치, 인식, 인력, 교육
  - 사용자, 디바이스, 애플리케이션 및 워크로드, 데이터, 네트워크 환경, 자동화 및 오케스트레이션, 가시성 및 분석
  - 기능, 아키텍처, 상호 운용성, 아이디어/혁신
  - 정책, 계획, 자금, 인수, PMO, ... 등



(Source: DoD)

UK NCSC - 제로 트러스트 아키텍처 설계 원칙 (2021년 7월 23일)

❑ 8대 원칙

- 사용자, 디바이스, 서비스, 데이터를 포함한 아키텍처 파악
- 사용자, 서비스 및 디바이스 ID 파악
- 사용자 행동, 디바이스 및 서비스 상태 평가
- 정책을 이용하여 요청 승인
- 어디서나 인증 및 권한 부여
- 사용자, 디바이스, 서비스에 모니터링 집중
- 내 네트워크를 포함한 어떤 네트워크도 신뢰하지 않음.
- 제로 트러스트를 위해 설계된 서비스 선택

National Cyber Security Centre

(Source: NCSC)

6 제로트러스트 가이드라인 1.0 발표 (과기부/한국인터넷진흥원)

GISC 2024

❑ 제로트러스트 가이드라인1.0 발표

- 일시: 2023.7.9
- 산·학·연·관 전문가로 구성된 「제로트러스트포럼」을 구성하고 미국, 유럽, 일본 등의 동향 분석, 자료검토, 토론회 등을 통해 의견을 모아 국내 환경에 적합한 「제로트러스트 가이드라인 1.0」 마련

❑ 주요 내용

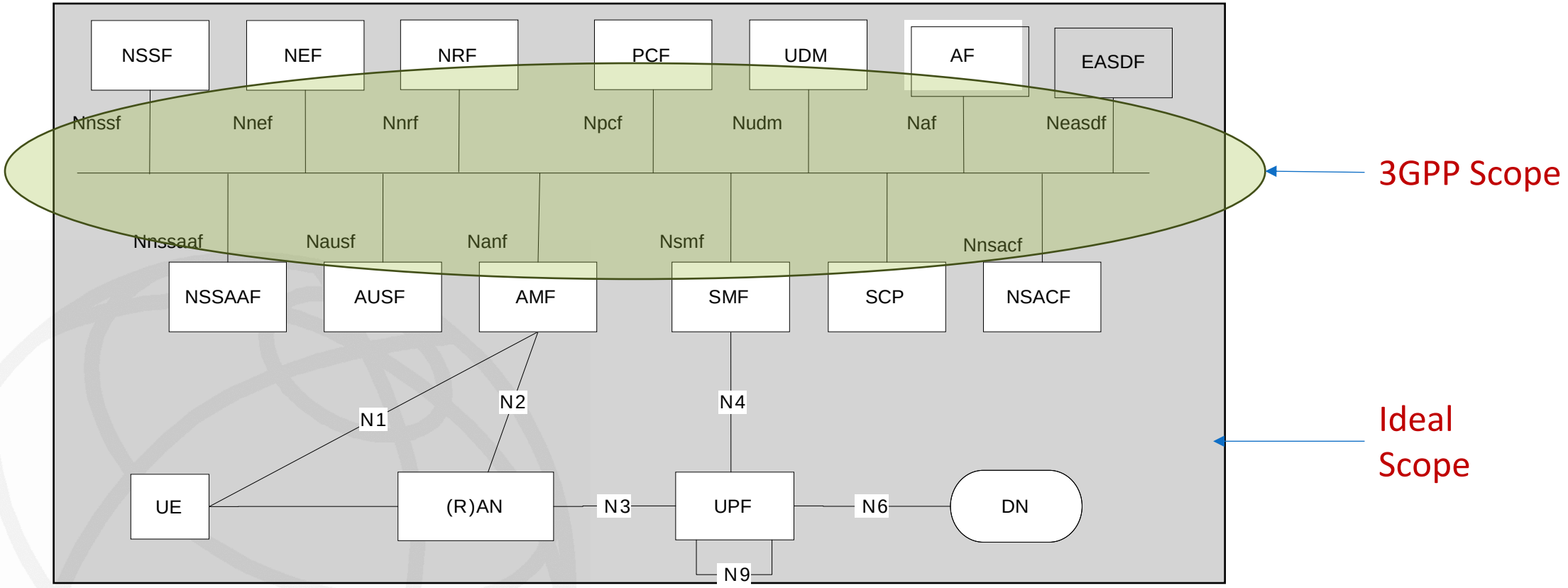
- (핵심원칙) 제로트러스트 보안은'절대 믿지 말고, 계속 검증하라'는 기본철학을 구현하기 위한
- ① 강화된 인증(아이디/패스워드 외에도 다양한 인증정보를 활용한 다중인증 등 지속적인 인증을 포함)
- ② 마이크로 세그멘테이션(서버·컴퓨팅 서비스 등을 중심으로 하는 작은 단위로 분리)
- ③ 소프트웨어 정의 경계(소프트웨어 기반으로 보호 대상을 분리·보호할 수 있는 경계를 만들 수 있어야 함)

제로 트러스트 표준화 개요

표준화 활동 개요

SDO/group	Items	content	Status
ITU-T SG17	ITU-T SG17, ITU-T TR.zt-acp	Guidelines for zero-trust (ZT) based access control platform (ACP) in telecommunication networks	Published
	ITU-T SG17, ITU-T X.ztmc	Guidelines for high-level Zero trust model and its security capabilities in telecommunication networks	Under development
NIST	SP 800-207	Zero Trust Architecture	Published
	SP 1800-35	Implementing a Zero Trust Architecture	Under development
3GPP SA3	TR 33.894	Study on applicability of the zero trust security principles in mobile networks	Published
	TR 33.794	Study on enablers for Zero Trust Security	Under development
IEEE WG on zero trust security (established in February 2024)	IEEE P2887	Recommended Practice for Zero Trust Security	Under development
	IEEE P3409	Standard for a Zero Trust Security Framework	Under development

3GPP – 3GPP 제로 트러스트 표준 범위



(Source: TS 23.501, Figure 4.2.3-1: Non-Roaming 5G System Architecture)

3

제로트러스트 국제표준 추진을 위한 준비 활동

다음 연구회기를 위한 신규 표준화 주제 및 연구과제 결정 (2023.03)

2023년 3월 SG17 회의

INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2022-2024

SG17-C234
STUDY GROUP 17
Original: English

Question(s): All/17 — Geneva, 21 February – 3 March 2023

CONTRIBUTION

Source: Korea (Republic of)

Title: Proposal for SG17's potential hot topics for the next study period (2025-2028)

Contact: Heung Youl Youm
Soonchunhyang University
Korea (Republic of)

Contact: Heung Ryong Oh
TTA
Korea (Republic of)

Contact: Sungchae Park
Soonchunhyang University
Korea (Republic of)

Contact: Juhee Ki
IITP
Korea (Republic of)

and released faster.

- →Zero trust(ZT) architecture or Mesh security as an industry's first Zero Trust architecture solution: Zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources[NIST SP 800-207]. This term is derived from the principle of "never trust, always verify". It is designed to protect organization's data and resources by using strong authentication methods, leveraging network segmentation, preventing lateral movement, providing "least access" policies. Mesh Security is the industry's first Zero Trust Posture Management (ZTPM) solution, providing real-time visibility, control, and protection across

INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2022-2024

SG17-C235
STUDY GROUP 17
Original: English

Question(s): All/17 — Geneva, 21 February – 3 March 2023

CONTRIBUTION

Source: Korea (Republic of)

Title: Proposal for existing or new Question(s) to address potential hot topics identified by the CG-sg17-wtsa24-prep

Contact: Heung Youl Youm
Soonchunhyang University
Korea (Republic of)

Hot topics	Category	Impact on	Existing or new Questions	Remarks
metaverse(immersive virtual universe) security and PII protection	Application/Sector specific area	Single Question	New Question on Metaverse security and PII protection	→Take deliverables from FG on metaverse
Future network security such as 6G(IMT for 2030 and beyond) security	Application/Sector specific area	Single Question	Q2	→In line with 3GPP work progress
Software supply chain security including SBOM (Software Bill of Materials)	Fundamental core area	Multiple Questions	New Question on Software security or Q4	
DevSecOps	Fundamental core area	Multiple Questions		
Zero trust(ZT) architecture or Mesh security as an industry's first Zero Trust architecture solution	Fundamental core area	Multiple Questions	Q2, Q4, Q10	

2 ITU workshop 제로트러스트 표준화 추진 필요성 합의 (2023.09)

2023년 8월 ITU workshop on zero trust and software supply chain security

Session 1: Takeaways and suggestions (1/3)

Takeaways and conclusions

- NIST released SP 800-207 Zero Trust Architecture (ZTA), which includes 7 tenets of zero trust. It's suggested that the guidance in SP 800-207 needs to be adjusted for 5G System.
- The concept of Zero Trust, common understanding for Zero Trust, misconceptions and how to understand the paradigm are elaborated.
- With the evolution of telecom networks, security boundary is becoming vague, and traditional passive static security defense methods are no longer sufficient. Zero trust is a good approach to improve identity management for O&M System in telecom networks and to secure service access between multiple clouds.

Suggestions to ITU-T SG17

- SG17 is developing TR.zt-acp, *Guidelines for zero trust based access control platform in telecommunication networks*, with introducing zero trust to telecom networks.
- More studies on zero trust in 5G system and telecom networks are welcome to SG17 in the future.

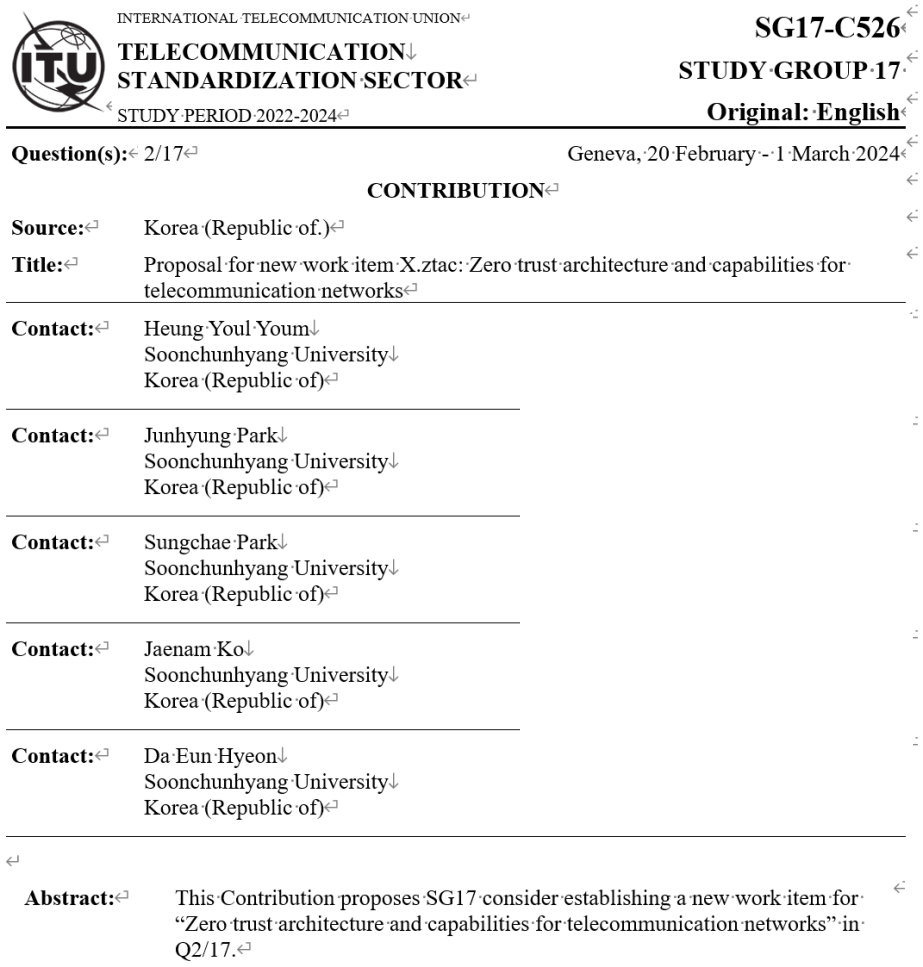
3 신규 워크아이템 제안을 위한 사전 국제협력 활동 (미국, 영국 등)

4

ITU-T SG17 추진 성과 및 쟁점 사항

1 ITU-T X.ztmc 신규 표준화 아이템 제안

- 통신 네트워크를 위한 상위 수준의 제로 트러스트 모델 과 보안 기능 가이드라인
(Guidelines for high-level Zero trust model and its security capabilities in telecommunication networks)



INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG17-C526

STUDY GROUP 17

Original: English

Question(s): 2/17 Geneva, 20 February - 1 March 2024

CONTRIBUTION

Source: Korea (Republic of.)

Title: Proposal for new work item X.ztac: Zero trust architecture and capabilities for telecommunication networks

Contact: Heung Youl Youm
Soonchunhyang University
Korea (Republic of)

Contact: Junhyung Park
Soonchunhyang University
Korea (Republic of)

Contact: Sungchae Park
Soonchunhyang University
Korea (Republic of)

Contact: Jaenam Ko
Soonchunhyang University
Korea (Republic of)

Contact: Da Eun Hyeon
Soonchunhyang University
Korea (Republic of)

Abstract: This Contribution proposes SG17 consider establishing a new work item for "Zero trust architecture and capabilities for telecommunication networks" in Q2/17.

- ❑ 2024년 2월 SG17 회의에 신규워크아이템 제안
- ❑ 제안 배경
  - 기존에 존재하는 다양한 제로트러스트 모델들은 통신 네트워크 관점에서 상호 운용이 가능한 모델의 설계와 운영에는 미흡
  - 제로트러스트는 하나의 새로운 보안 컨셉으로, 통신 네트워크에 적용이 필요함
  - 통신 네트워크 관점에서 관련된 보안 영역들과 보안 능력을 정의함으로써, 5G/6G, ITS 등 다양한 산업 영역에서 이용이 가능함
- ❑ 2024년 2-3월 ITU-T SG17(정보보호) 국제회의에서 미국, 영국 등 주요국의 지지를 받아 신규 표준화 항목으로 채택 (한국, 순천향대 팀 제안)
  - 과기부/IITP 차세대보안표준전문연구실 사업 (2021.4-2028.12)

2 쟁점사항 및 합의내용

- 활용
  - 세부 섹터(ITS, 5G/6G, health, 스마트 공장 등)에 제로트러스트 모델을 정의하지 않고, 일반 상위 수준의 모델을 개발하고, 다음 단계로 섹터당 세부 모델을 개발함
- 제로트러스트 용어 정의
  - NIST 용어 정의를 사용한지 근거
  - 기술적인 용어 정의이고, 3GPP SA3에서도 이 정의를 사용하고 있음
- 라우터간 제로트러스트 모델 적용 여부
  - 디바이스와 서버간, 라우터와 서버간은 모델을 적용하고, 라우터간 모델은 비용으로 인해 적용하지 않기로 합의함
- 통신망 관점의 필러 정의 필요
  - 종단 디바이스(신원)-네트워크 디바이스-통신망-응용및워크로드-데이터로 합의
- 표준 승인 프로세스
  - 규제합의가 있어서 TAP 로 변경함
- 갭 분석 필요
  - 3GPP TR 포함 등

3 ITU-T X.ztmc 신규워크아이템 합의

- 제목: Guidelines for high-level Zero trust model and its security capabilities in telecommunication networks
- 통신 네트워크를 위한 제로트러트스 모델 과 핵심 영역(Key area) 제시

  * 핵심 영역: 종단(End) 디바이스, 네트워크 디바이스, 통신 네트워크, 애플리케이션 및 워크로드, 데이터
- 제로트러스트 핵심 영역 별 보안 역량, 다양한 산업의 제로트러스트 적용 사례
- IoT, 스마트 팩토리 등 산업별 제로트러스트 모델을 정의하기 위한 참조 모델로 활용이 가능

Annex A

A.1 justification for proposed draft new Recommendation X.ztmc

Question:	Q2/17	**Proposed new ITU-T Recommendation**	Geneva, 20 February – 1 March 2024
Reference and title:	ITU-T X.ztmc: Guidelines for high level Zero trust model and its security capabilities in telecommunication networks		
Base text:	Annex B of this document	**Timing:**	2026-09
Editor(s):	Heung Youl Youm, Korea (Republic Junhyung Park, Korea (Republic of),	**Approval process:**	TAP
Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability): This draft Recommendation provides guidelines for high level zero trust model in telecommunication networks including its key areas such as end-device(identity), network-device, telecommunication network, orchestration/automation etc. It also provides security capabilities for each key area. This high level zero trust model can be used as a reference model to define various sector-specific detailed zero trust models. Use cases for various industry sectors such as IoT, smart factory, etc., using zero trust architectures are described in Appendix. Note: The scenarios of network device-to-network device communication are out of scope.			

5

제로트러스트 특허 분석

1 국제 표준 공동 대응을 위한 주요국 제로트러스트 특허 분석

GISC 2024

- 목적
  - 제로트러스트 특허와 국제표준화 활동을 연계해 국내 기업에게 관련 특허 정보를 공유하고, 국제표준화 추진시 고려함.
- 주관: 한국특허전략원/RRA 표준 특허 창출 사업
  - 참여기관: 순천향대, 대구대, 가천대, 한국과학기술원, 한국전자통신연구원, 국가보안기술연구소, 한국정보통신기술협회, 한국인터넷진흥원 등
- 일정: 2024.4 – 12.

- 목적특허 분석 기술분류체계
  - 통신제어 중심의 제로트러스트 기술
  - 성숙도 모델 상세 체계
  - 구조 연동 체계
  - 신뢰점수 체계 등
- 최종 산출물
  - 미국, 한국, 중국 등 주요국 산업체가 갖고 있는 특허 정보 분석
  - 분석 결과를 고려해 국제표준화 추진시 연계함
  - 중요 특허 부문에 대한 제안

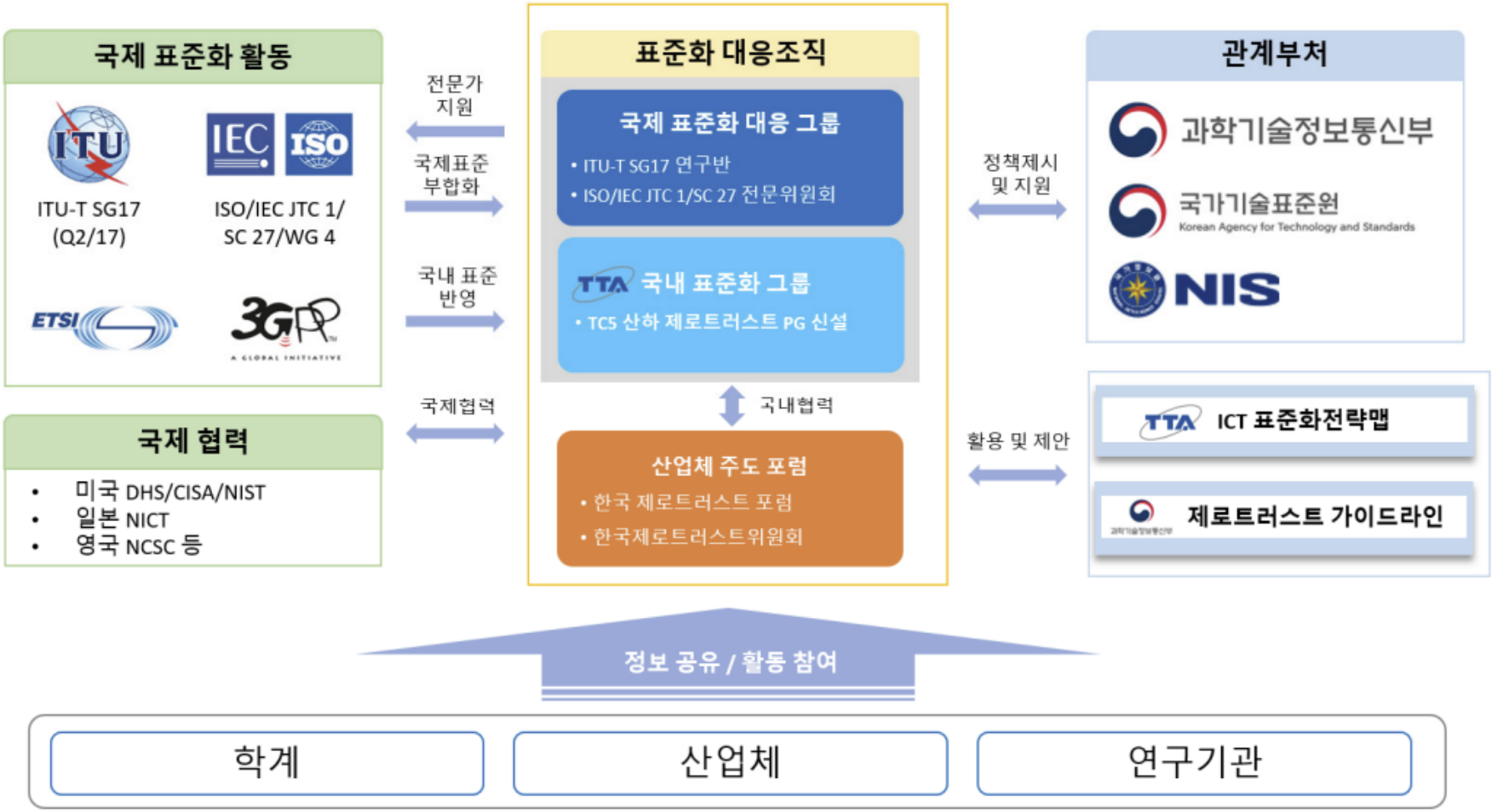
6

국제표준화 추진 체계 (안)

1 제로트러스트 국제표준화 주도권 확보를 위한 대응 전략

거버넌스 대응전략	①	• 국내 산업체, 대학, 정부 및 공공기관의 국제표준화 추진을 위한 협력과 공조를 강화한다.
	②	• 향후 개발될 국제표준에 대한 국가 표준화를 추진하고, 이와 더불어 제로트러스트에 대한 국내 표준화 활동을 촉진하기 위해서 관련 그룹을 신설한다.
	③	• ITU-T SG17과 ISO/IEC JTC 1/SC 27을 국제표준화 목표 그룹으로 설정한다.
	④	• 제로트러스트의 표준 주도국인 미국, 영국, 일본 등의 주요 기관과 긴밀히 협력하여 국제표준화를 추진한다.
	⑤	• 국제표준화 그룹에서 국내 전문가의 의장단 진출을 도모함으로써 글로벌 표준화를 리드한다.
	⑥	• 제로트러스트 기술 관련 표준화 정보 및 자료의 제공, 표준화 관련 교육 및 훈련 프로그램의 확대 등을 통해 표준화 인프라를 구축한다.
국제 표준화 대응전략	⑦	• 국내 산업체가 보유한 핵심 기술의 국제표준화를 추진하여 국제표준 지재권을 확보하고 글로벌 표준화를 주도한다.
	⑧	• 정부가 향후 개발할 '제로트러스트 가이드라인 2.0'을 기반으로 각 산업군 별 제로트러스트 모델을 정의하고, 이를 국제표준화에 반영한다.
	⑨	• 기설립된 제로트러스트 관련 국내 포럼과 협업하여 국제표준화 아이템을 발굴하고 이를 국제표준 개발에 반영한다.
	⑩	• 제로트러스트 기반 기술 및 제품, 서비스의 공공 시장 진입을 위해서 평가 및 인증과 관련된 표준화 아이템을 발굴하여 국제표준 개발에 반영한다.
	⑪	• 국내 산업체의 요구사항을 반영한 표준화 아이템을 발굴하고 이를 기반으로 국내외 표준화 추진함으로써 국내 산업체의 글로벌 경쟁력을 강화한다.

2 국제표준화 추진 체계


국제 표준화 활동
ITU-T SG17 (Q2/17)
ISO/IEC JTC 1/ SC 27/WG 4
국제 협력
• 미국 DHS/CISA/NIST
• 일본 NICT
• 영국 NCSC 등
전문가 지원
국제표준 부합화
국내 표준 반영
국제협력
표준화 대응조직
국제 표준화 대응 그룹
• ITU-T SG17 연구반
• ISO/IEC JTC 1/SC 27 전문위원회
국내 표준화 그룹
• TC5 산하 제로트러스트 PG 신설
국내협력
산업체 주도 포럼
• 한국 제로트러스트 포럼
• 한국제로트러스트위원회
정책제시 및 지원
활용 및 제안
관계부처
과학기술정보통신부
국가기술표준원
Korean Agency for Technology and Standards
NIS
ICT 표준화전략맵
제로트러스트 가이드라인
정보 공유 / 활동 참여
학계
산업체
연구기관

7

ITU-T SG17 향후 국제표준화 추진 계획 (안)

1 제로트러스트 기술 표준화 비전 및 목표

vision

국제표준 선점을 통한 국내 제로트러스트 제품 글로벌 경쟁력 확보

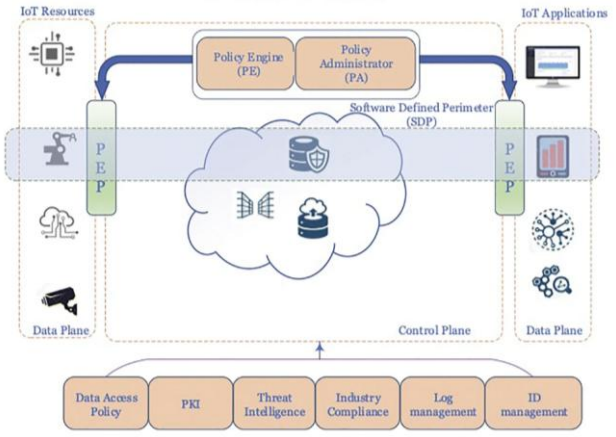
목표

2024	2026	2028
▪국내외 주요 기구 문서 분석 ▪선도 표준화 항목 선정 ▪국제 표준 선점을 위한 기술 개발과 연계 추진 ▪국내외 산학연 표준 협력 전략 마련	▪제로트러스트 공통 능력 개발 ▪제로트러스트 성숙도 프레임워크 등에서 선도 표준화 항목 선정 ▪미국, 영국, 일본 등의 주요 선진국과의 표준 협력 전략	▪제로트러스트 국제표준 선도 ▪ 제로트러스트 시장 선도 ▪글로벌 표준 협력 전략

2 ITU-T X.ztmc 의 후속 표준 개발

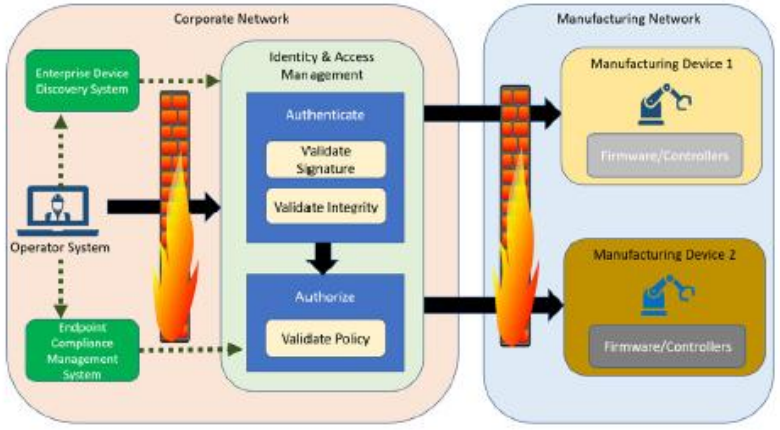
- IoT, 스마트 팩토리 등 융합산업 분야에서 제로트러스트 모델을 정의하기 위한 참조 모델 개발

[사물인터넷을 위한 제로트러스트 보안 구조]



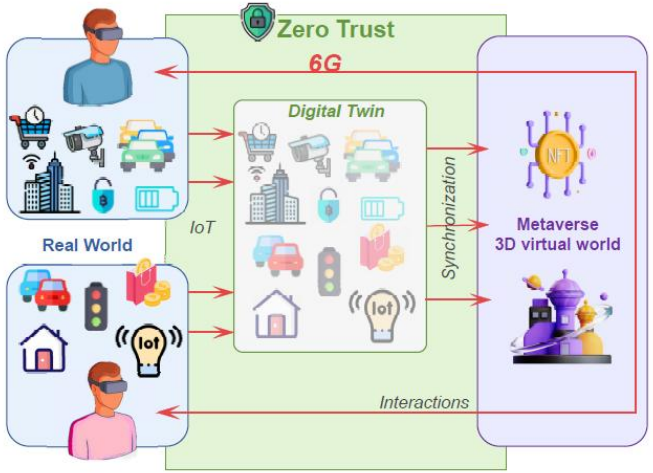
(출처: Shan Li, etc, Future Industry Internet of Things with Zero-trust Security, Springer Link, March 2022)

[스마트 공장을 위한 제로트러스트 보안 구조]



(출처: Baozhan Chen, etc., A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture, IEEE INTERNET OF THINGS JOURNAL, JULY 1, 2021)

[디지털 트윈 기반 6G 를 위한 제로트러스트 프레임워크]



(출처: Ismaeel Al Ridhawi, etc., Decentralized Zero-Trust Framework for Digital Twin-based 6G, Feb. 2023)

3 ITU-T X.ztmc 향후 추진 계획

- 미국, 영국 등과 협력으로 국제 표준화를 계속 추진
  - 6G, ITS, IoT, Smart factory, smart health 제로트러스트 보안 모델 추가 제안

8

의의 및 시사점

1 의의 및 시사점

- ITU-T 최초 제로트러스트 보안 권고 신규 워크아이템 채택
- 미국, 영국 등 주요 우방국과의 표준화 협력 추진
  - 6G 제로트러스트 보안을 위한 추가 협력 필요
- 제로트러스트 제품의 상호 연동성 보안을 위한 국내외 표준화 전략적 추진 필요
  - 제로트러스트 필러 별 제품 군 식별 및 인터페이스 국제표준 추진
- 정보보호 제품의 글로벌 경쟁력 강화 도모 및 한국 주도의 국제 표준화 활동 기반 마련
- 정부의 정책 수립과 산업체, 학계, 공공 연구기관의 협력을 바탕으로 국제표준을 선점하고 국내 제로트러스트 제품의 글로벌 경쟁력을 확보 필요

GISC 2024

Global ICT Standards Conference 2024

감사합니다.

염흥열, 명예교수, 순천향대학교