요약

제로트러스트 가이드라인 1.0

2023. 6

과학기술정보통신부 Ministry of Science and ICT
KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY
한국제로트러스트포럼

요약

제로트러스트 가이드라인 1.0

2023. 6

과학기술정보통신부 Ministry of Science and ICT
KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY
한국제로트러스트포럼

제로트러스트
가이드라인 1.0 (요약)

가이드라인(요약)의 구성

본 가이드라인(요약)은 총 5장으로 구성되어 있다. 요약본은 정부·공공, 다양한 산업분야 및 정보보호 분야 전문가, 일반인 등 폭넓은 독자층을 대상으로 하고 있어 본문에서는 제로트러스트의 개념과 원리를 쉽게 이해할 수 있도록 집중 설명하였다. 본 서를 통해 제로트러스트에 대한 기본 개념을 파악한 후 가이드라인 전체본을 읽으면 조금 더 쉽게 다양하고 깊은 내용을 파악할 수 있도록 요약본과 전체본을 차별화하여 구성하였다.

제1장에서는 새로운 기술의 확산 및 비대면 사회 가속화에 따른 네트워크 환경의 변화와 기존 경계 기반 보안모델의 한계를 분석하였고, 특히, 최근 사이버보안 침해사고 분석을 통해 구체적인 사례를 제시하는 한편, 이에 대응하는 미국의 제로트러스트 도입 관련 동향을 제시하였다.

제2장에서는 제로트러스트의 개념을 충실하게 이해할 수 있도록 기본개념 및 보안원리, 기존 경계 기반 보안모델과 제로트러스트 보안모델의 보안원리를 비교하여 제로트러스트의 보안 우수성을 제시하였다.

제3장에서는 제로트러스트 보안모델의 전체 원리를 정확히 이해할 수 있도록 구성하였다. 이를 위해 제로트러스트의 기본철학을 제시하고, 이를 구현할 수 있는 접근방법 또는 핵심원칙과 함께 접속요구에 대한 처리방법 등에 관한 사항을 정리하였다.

제4장에서는 제로트러스트 개념 이해를 바탕으로 업무환경에 제로트러스트 보안모델을 도입할 경우 참고할 수 있도록 제로트러스트 도입계획 수립과정과 함께 참고할 수 있는 성숙도 모델을 제시하였고 제로트러스트 도입 전후 보안모델의 변화를 도식화 하여 제시하였다.

제5장에서는 제로트러스트 도입 참조 모델로 최근 이슈가 되고 있는 원격지 근무 환경을 제시하고 이에 대한 제로트러스트 도입 모델을 제시하였다. 또한, 제로트러스트 도입 전후 침투 시나리오를 적용하여 제로트러스트 도입시 보안성이 강화됨을 침투 시나리오 적용을 통해 설명하였다.

마지막으로 본 서의 집필 과정에서 참고한 자료들을 정리하였다. 여기에 제시한 자료 목록만으로도 많은 정보를 제공해줄 수 있다고 판단하여 중요 자료 중심으로 정리하였다.

ZERO TRUST

CONTENTS

ZERO TRUST

서 문

디지털전환과 사이버보안은 상호 균형을 이루면서 각각 수레바퀴의 한축을 담당하고 있어서, 양쪽의 수레바퀴가 보조를 맞출 때 제대로 굴러갈 수 있을 것입니다. 이는 곧 디지털전환이 심화되면서 사이버보안 역시 이에 맞춰 진화해가야 한다는 것을 의미합니다.

모바일·사물인터넷 기기가 널리 확산되고, 클라우드 기반의 재택·원격근무 환경이 조성되었고, 코로나19로 인해 비대면 환경이 가속화되었습니다. 이와 같은 네트워크 환경의 변화는 기존 경계 기반 보안모델의 한계 상황을 초래하고 있습니다. 최근 우리나라를 비롯하여 국제적으로 이슈가 되었던 랩서스 해킹 사례 등을 종합 분석해보면 더 세밀한 인증체계, 보호대상을 각각 분리하여 보호하고, 모든 접근 요구를 정확하게 제어하여 최소권한을 부여할 수 있는 새로운 보안체계로 전환이 요구되는 시점입니다.

미국, 유럽 등에서는 정부 차원에서 기존 경계 기반 보안체계의 보완 대책으로 제로트러스트 도입을 본격 추진하고 있습니다. 또한 글로벌 기업들은 보안 패러다임 전환 시기를 맞이하여 기존 시장에서 확보하고 있는 경쟁력을 기반으로 새로운 시장을 선점하고, 이를 확대하기 위해 노력하고 있습니다.

과학기술정보통신부는 이와 같은 4차 산업혁명 기반의 네트워크 환경 변화와 보안 패러다임 전환을 중심으로 펼쳐지고 있는 주요국의 정책동향 및 시장상황 변화를 모니터링하고, 면밀하게 분석해왔습니다.

이를 기반으로 전문가 대응체계를 만들어 본격 대응하기 위해 작년 10월 산·학·연·관 전문가들이 참여하는 '한국제로트러스트포럼'을 구성하고, 국내외 기술동향 분석, 토론회 등 전문가 의견을 모아 「제로트러스트 가이드라인 1.0」을 발간하여 제로트러스트 도입을 검토하고 있는 국내 정부·공공 기관 및 기업 관계자들에게 실질적인 도움을 주고자 하였습니다.

가이드라인 1.0은 제로트러스트로 가는 긴 여정의 시작점입니다. 과학기술정보통신부는 체계적인 제로트러스트 실증을 지원하는 한편 이의 성과와 환경변화를 반영하고, 전문가들의 고견을 수용하여 '제로트러스트 가이드라인'을 지속적으로 보완·고도화해나가도록 하겠습니다.

또한, 대통령 직속 디지털플랫폼정부위원회(위원장 고진)도 지난 4월 「디지털플랫폼정부 실현 계획」을 발표하면서 새로운 디지털환경에서의 사이버보안을 위해 국가적 차원의 제로트러스트 도입을 추진하겠다고 밝힌 바, 이번에 마련된 「제로트러스트 가이드라인 1.0」을 각 분야로 확산시켜 나가겠습니다.

과학기술정보통신부장관 **이 종 호**

ZERO TRUST

Forrester Research의 수석 애널리스트인 John Kindervag은 2010년 처음으로 제로트러스트의 개념을 소개하였습니다. 그러나 이는 기존에 없던 완전히 새로운 개념이 아니라, 기존 경계 기반 보안모델의 한계를 보완하기 위한 여러 논의와 시도들(예, Jericho Forum의 탈경계화 등)을 네트워크 관점에서 적용하기 위한 보안 철학입니다. 제로트러스트는 점점 다양화·지능화되는 사이버 공격을 효과적으로 대응하기 위한 방법으로 받아들여졌으며, 이후 데이터 중심의 보안 전략으로 확장되어 왔습니다.

미국의 바이든 행정부는 2021년 5월에 발표한 "국가 사이버 보안 개선을 위한 행정 명령(Executive Order 14028)"에서 연방정부 차원의 보안수준을 높이기 위해서 점진적인 개선보다 대담한 변화와 의미 있는 투자가 필요함을 역설하고, 제로트러스트 아키텍처의 도입을 공식화하였습니다.

그러나 미국을 제외하면, 많은 국가들이 공공·민간 분야에서 제로트러스트 도입의 필요성을 인지하면서도 도입 방안을 구체화하지 못하고 있습니다. 이는 제로트러스트가 새로운 보안 패러다임으로 개념 자체가 추상적이며 도입 사례 역시 많지 않기 때문일 것입니다.

우리나라에서도 많은 보안 전문가들이 제로트러스트 도입 필요성을 언급하고 있습니다. 그러나 현장에서 제로트러스트 철학을 적용하고 기술을 도입해야 하는 보안 책임자들은 많은 어려움을 호소하고 있습니다. 이는 보안

정책 준수를 위한 솔루션 도입이 관행화된 상황에서 제로트러스트를 전사적으로 도입하기 위한 전략 수립 과정은 지난한 어려움의 연속일 것입니다.

본 가이드라인은 경영진을 포함하는 비전문가들로부터 보안 책임자·실무자에 이르기까지 제로트러스트 개념을 이해하고 도입하는데 도움을 주기 위해 작성되었습니다. 이를 위해 공공과 기업 등 일반적인 조직이 내부 네트워크에 적용하기 위한 제로트러스트의 개념부터 보안 모델, 도입 절차와 구현 전략 등을 담았습니다.

한국제로트러스트포럼은 본 가이드라인 발간을 통해 국내에서 제로트러스트를 도입을 지원하는 첫걸음을 내딛게 되었습니다. 포럼은 제로트러스트 도입·확산을 지원하기 위해 가이드라인을 지속적으로 보완하고, 다양한 지침서를 개발할 계획입니다. 국내 많은 전문가들이 포럼에 참여하여 같이 활동하시기를 바라며, 포럼은 국내에 제로트러스트가 빠르게 뿌리를 내릴 수 있도록 함께 노력하겠습니다.

한국제로트러스트포럼

Ⅰ 제로트러스트 추진배경

환경의 변화

모바일, 사물인터넷, 클라우드의 확산으로 **원격재택 근무환경이 조성**되었고, 코로나 19로 **비대면사회가 가속**되어 기업망 보호를 위한 **전통적인 사이버보안 체계의 변화**가 필요

- **디지털 대전환의 가속화**로 **네트워크 경계의 확장** 및 **다변화**로 **사이버보안 영역** 또한 **국민의 일상생활 및 다양한 산업분야**로 **확장**
  - 모바일·IoT기기, 클라우드 확산과 **원격·재택 근무** 등 비대면 사회의 가속화로 **리소스 위치 다변화, 접속 요구 시간·위치 또한 예측 불가**
- 점점 늘어나는 사용자, 수많은 단말과 장비, 이로 인해 **복잡해지는 권한 관리** 등 각 기관·기업의 **사이버보안 관리가 어려워짐**
  - 관리·분석 대상 **패킷이 다양화·대량화**되고, 사이버 공격 또한 **고도화·지능화**되고 있어 기존 **경계 보안모델의 한계 도달**
- **최근 침해사고 유형**은 **내부자 공모** 또는 **권한탈취** 등 경계보안의 **암묵적 신뢰 정책의 허점**을 이용하는 형태가 증가
  - 점점 **고도화되고 있는 수많은 해킹 및 랜섬웨어 공격**의 경우, 피해가 사이버 공간에 머무르지 않고 **국가 안보·인프라에 위협**

〈경계보안 체계의 한계 및 최근 대표적인 사이버 침해사고〉

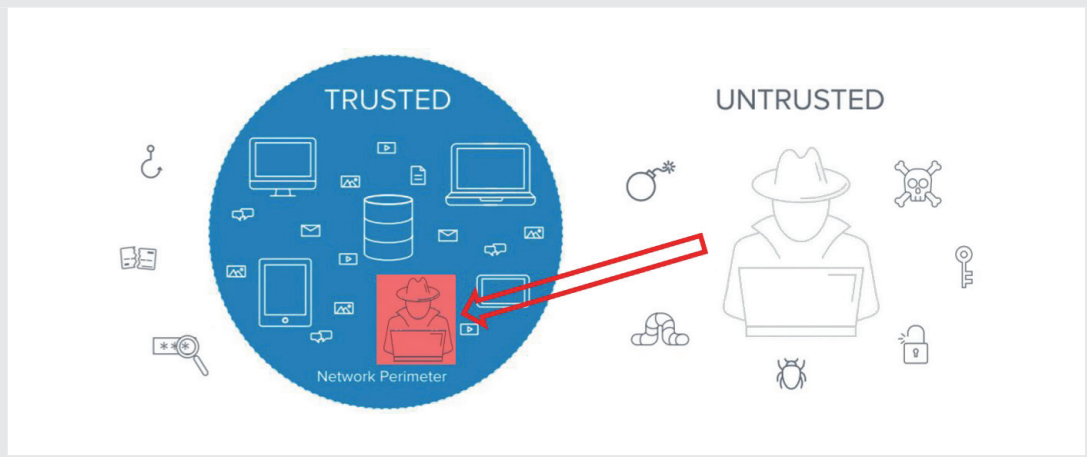
기존 경계 기반 보안모델의 한계

최근 발생한 수많은 해킹 및 랜섬웨어 공격 사례는 **경계 기반 보안모델의 한계점**을 드러내고 있으며, 최근 등장하는 보안 솔루션만으로는 완벽한 해결책을 제공하지 못함

- 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 트래픽**에 대해 외부에서 요구하는 접속과 비교하여 **높은 수준의 신뢰성**을 부여
  - 공격자는 **악성코드, 크리덴셜 스터핑*** 등을 통한 내부 시스템 침투 후 **횡적이동****을 통한 DB 관리자 권한 획득 및 데이터 유출
    * Credential Stuffing : 사용자 ID, 이메일 주소, 인증서 등 사용자 자격 증명을 도용한 후 이를 통해 사이버 공격을 하는 행위
    ** Lateral Movement : 공격자가 기업망 내부 침투 후, 민감한 데이터나 고가 자산을 찾기 위해 기업망 내부의 중요 서버로 이동하는 것을 의미

- 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
    * 여전히 기업망 내부 사용자에 '높은 신뢰'를 부여함으로써, 내부자는 기업내 서버 침투 및 데이터 유출이 상대적으로 용이(제로트러스트 실질적 미도입 상태)

〈경계 기반 보안모델의 한계 상황〉



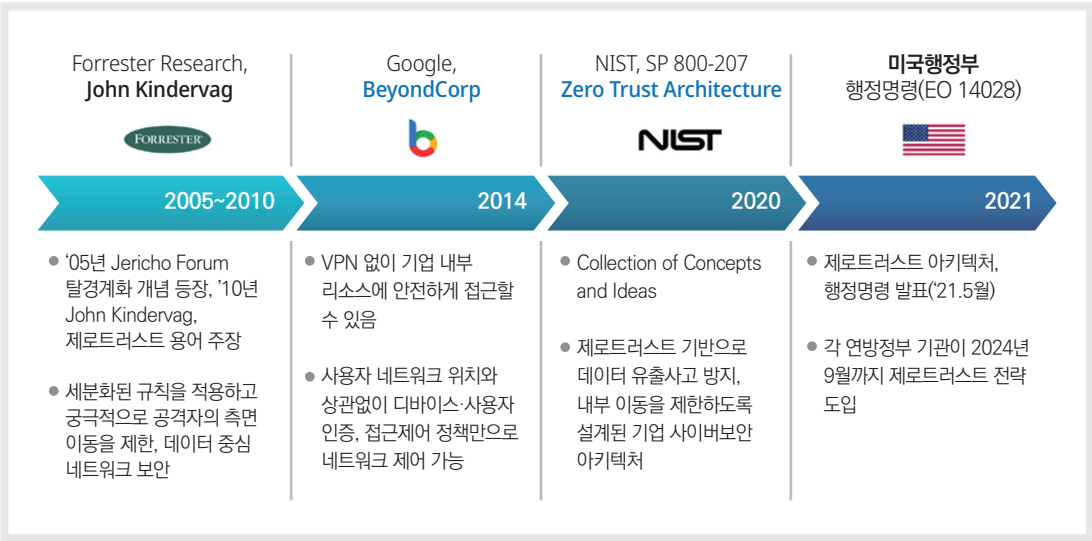
[What is Zero Trust Security / Okta 재구성]

미국의 제로트러스트 도입 동향

美 민간의 **제로트러스트 논의 및 도입**, NIST의 문서 발표('20.8월 SP 800-207) 후 **미 연방정부 행정명령**(EO 14028)을 통해 **연방정부 차원의 제로트러스트 본격 도입 중**

- **탈경계화**(제리코 포럼, '05년) 등 경계 기반 보안모델의 한계 극복 시도 이후, Forrester Research의 **존 킨더백**이 **'제로트러스트'** 용어 및 개념 제시('10년)
- CSA(Cloud Security Alliance) 등 민간 중심으로 **제로트러스트 접근법 중** 하나로 알려진 SDP(SW Defined Perimeter) 등에 대한 논의가 활발하게 진행
  * CSA는 '13년 SDP Specification 1.0을 발표한 후 '22.10월에 Spec 2.0 발표
- 미국표준기술연구소(NIST)는 **7가지 사상**(7 Tenets), 접근방법 등을 포함한 **'제로트러스트 아키텍처**(NIST SP 800-207, '20.8월)' 발표
  * 제로트러스트 도입에 적극적인 DoD 등 연방정부 외에도 Google Cloud, MS, PaloAlto Networks, Aruba Networks, Cisco, Akamai, SailPoint, Okta 등도 ZTA 도입 중
- 바이든 행정부도 **연방정부의 사이버보안 강화**를 위해 **제로트러스트와 공급망 보**안을 추진하는 **행정명령 발표**(EO 14028, '21.5월)
  * "Moving the U.S. Gov. Toward Zero Trust Cybersecurity Principles" 발표(OMB, '22.1월), '24년까지 ZT 목표 달성, CISA 성숙도 모델 따를 것, 60일 내로 ZT 도입 계획 수립 및 예산계획 제출 등 요구

〈제로트러스트 관련 연차별 주요 문서 현황〉



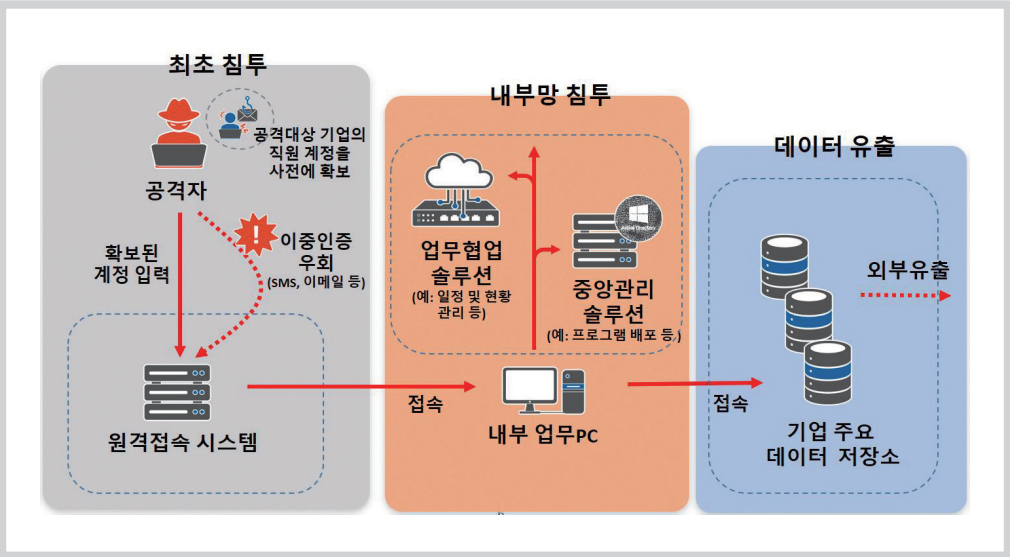
※ 미연방 인사관리처의 해킹사건(공무원 인사정보 유출, 2015년)도 ZT 도입의 배경으로 판단

참고 1 | 최근 국내외 침해사고 분석

■ 국내·외 침해사고에 대한 분석

● 최근 국내외 침해사고 분석 결과를 종합해보면, 외부로부터 ①**최초 침투 단계,** ②**내부망 침투 단계** 및 ③**데이터 유출 단계** 등으로 구분

〈사이버 공격 단계별 침투방법 분석〉



① **최초 침투 단계** 해커는 **공격대상 기업**의 **사용자 계정 등을 다크웹** 등에서 구입하거나 **업무 관련**으로 위장한 **악성 메일**를 보내 **계정**을 **수집**하는 등 다양한 방식을 활용하였으며, **일회용 비밀번호** 등의 **추가 계정 인증** 요구도 **우회**하는 형태를 보임

② **내부망 침투 단계** **내부 시스템**에 **침투**한 이후, **다수 계정·단말**을 관리하는 **중앙서버** 또는 기업 내 **프로그램 관리 서버** 등에 **접속**하여 추가 정보 습득을 위한 **악성코드**를 **배포**하는 방식 등으로 접근하기도 함

③ **내부자료 유출 단계** 내부망 침투 이후에는 **제품 및 영업 관련 정보** 또는 **내부 직원 정보 등**이 저장된 데이터 수집소에 접근한 뒤 관련 파일을 확보하여 **외부 반출**로 이어짐

II 제로트러스트 소개

미국표준기술연구소(NIST)의 제로트러스트 아키텍처 문서에서는 '제로트러스트'에 대해 항상 네트워크가 침해되었다고 가정하고, 보호해야할 데이터 및 컴퓨팅 서비스 등에 대한 접근 요구에 대해 정확하고 최소한의 권한(Least Privilege)을 부여하는 아이디어와 개념의 모음이라고 소개하고 있다.

기존 경계 기반 보안체계에서는 공격자가 네트워크 경계에 설치된 방화벽/IDS/IPS/VPN 등의 보안체계를 통과하고 나면 암묵적 신뢰 기반 하에 기관·기업 내부의 다양한 서버, 데이터베이스, 저장장치 등에 접속할 수 있었다. 물론 이와 같은 체계를 보완하기 위해 NAC, EDR 등 다양한 보안 솔루션들이 함께 운영되고 있지만 보안체계에 대한 근본적인 변화를 염두에 둔 것은 아니다.

서두에서 말한 것처럼 제로트러스트는 새로운 보안체계에 대한 개념으로 다양한 기관 및 기업에서 나름대로의 정의를 제시하고 있다. 본 장에서는 국내외 소개된 다양한 제로트러스트 개념을 분석하고, 조금 더 쉽게 이해할 수 있도록 재구성하였다. 다만, 잊지 말아야 할 것은 제로트러스트가 망분리를 포함한 기존 경계 기반 보안체계를 완전히 대체하는 것 아니라 이를 보완하여 상당 기간 공존할 것이라는 것이다.

제로트러스트 개념

전통적인 **경계 기반 보안**(Perimeter Security)으로는 업무 환경의 변화와 진화하는 사이버 위협에 효과적으로 대응하기 어려워 **'제로트러스트(Zero Trust)'** 개념 등장

- 랩서스 그룹의 해킹 사례, 갈수록 다양화·지능화되는 보안 위협등 기존 경계 기반 보안 모델로는 막기 어려운 공격 출현
- 보안위협이 **언제 어디서든 발생 가능**하다는 전제하에 요건*을 **갖추지 않은 사용자·기기**는 자원(데이터, 컴퓨팅 서비스 등) **접근을 제한**

  * 신뢰도 평가, 지속적 인증, 세밀한 권한 부여 등 각종 접근제어
- 기관·기업의 '경계' 기반 보안체계 구축보다 **'내부 데이터 보호'**에 집중하는 새로운 보안 패러다임

제로트러스트 개념

① **제로트러스트(ZT)**란? **정보 시스템 및 서비스**에 대한 **접속요구**가 있을 때 **네트워크가 이미 침해**된 것으로 간주하고, 주어진 권한을 정확하고 최소한으로 부여하는데 있어서 **불확실성을 최소화하도록 설계된 개념 및 아이디어 모음**(NIST SP 800-207, '20년)

② **제로트러스트 아키텍처?** ZT 개념을 사용한 **기업 사이버보안 계획**으로 **컴포넌트간 관계, 워크플로우 설계, 접근 정책**이 포함됨(NIST SP 800-207, '20년)

③ **제로트러스트? 악의적인 상대에 의해 지속적으로 노출되고 잠재적으로 침해**될 수 있는 **시스템의 구성요소, 서비스 및 사용자**를 다루는 **일련의 원칙**(MIT 링컨 연구소, '22년)

기존 보안으로 막기 어려운 공격 출현

2022년 랩서스(LAPSUS$)의 글로벌 IT 기업 해킹을 통한 기밀정보 유출사례

1. 공격 대상 임직원 계정 정보 확보 후 내부 침투
2. 네트워크 정찰 및 주요 서버 접근, 권한 상승
3. 기밀 데이터 획득 및 외부 유출

Why? 글로벌 대기업들은 높은 수준의 보안 기술을 사용중임에도왜 해킹을 당했는가?

1. 탈취된 임직원 계정으로 로그인하여 기업망에 침투하는 해커를 막을 방법은 없는가?
2. 해커가 회사 관리 자산이 아닌 기기로 기업망에 접근할 때 어떤 정책을 적용해야 하는가?
3. 공격자가 내부 침투 후 기업망 내부 네트워크를 정찰하고 주요 서버에 접근하는 것을 막을 수 없는가?
4. 공격자가 대량의 기밀 데이터 획득 후 외부로 유출하는 행위를 막을 방법은 없는가?

제로트러스트 기반 대응 방법

(신뢰도 판단 전까지 모든 접근 비신뢰 및 접근 거부)

기업망 내부자 행위 모니터링·감시·분석

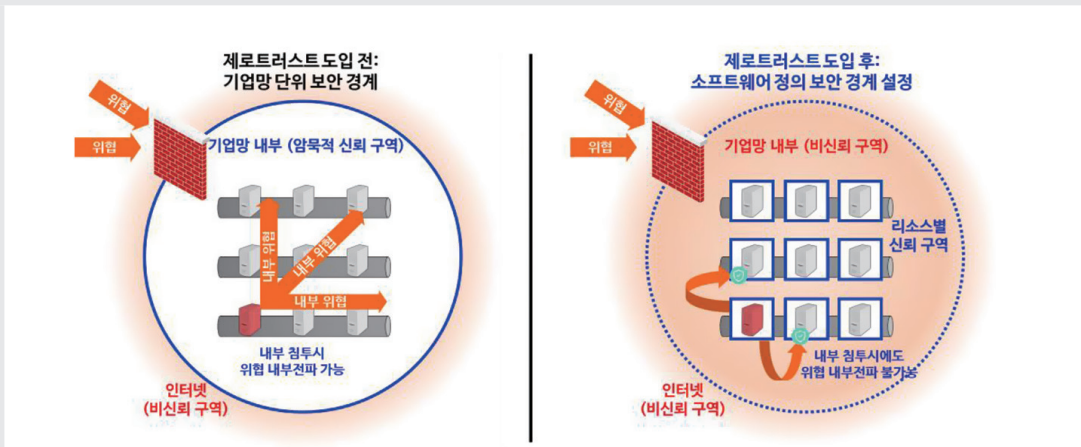
명확한 신뢰도 판단에 근거한 최소 권한 부여

제로트러스트 보안원리

"Never Trust, Always Verify"를 구현하기 위해 보호해야할 **모든 데이터**와 **컴퓨팅 서비스**를 자원(resourcee)으로 분리·보호하고, 각 자원에 접속 요구마다 인증

- 기존 **경계 기반 보안모델**은 네트워크 내부 접속 요구(사용자, 기기 등)는 **어느 정도 신뢰할 수 있다**는 가정에서 시작
  - 반면, **제로트러스트 모델**은 해커가 네트워크 **내·외부 어디든 존재할 수** 있으며, 모든 접속 요구는 신뢰할 수 없다는 가정에서 시작
- 경계 기반 보안모델은 **신뢰하는 자원**(내부 네트워크)과 **신뢰하지 않은 자원**(인터넷) 사이에 보안 경계의 벽을 세움
  * 내부자 **공모** 또는 **권한탈취** 후 침투, **권한 상승 및 횡적이동을 통한 데이터 유출**
  - 반면, **제로트러스트 모델**은 보호해야할 모든 데이터와 컴퓨팅 서비스를 각각의 자원(Resource)으로 분리·보호
    * 모든 자원의 **경계를 구분하여 분리·보호**, 하나의 자원에 접속한 후에는 **정해진 권한만큼**만 활동이 가능하고, **인근 자원에 대한 추가 접속 요구** 시 **지속적 인증**으로 침투 제한

〈기존 경계 기반 보안과 제로트러스트 개념 비교〉



▲ 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

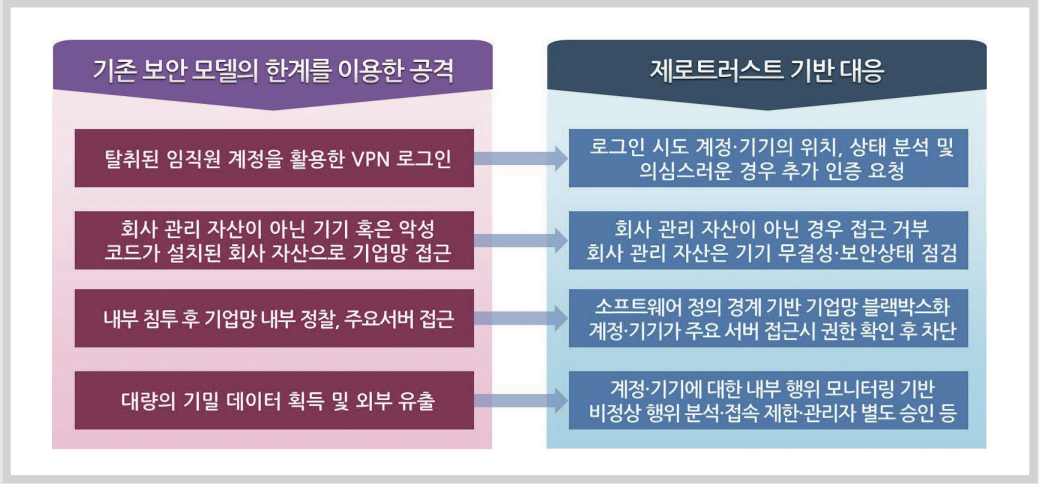
[참조 : A.Kerman / NIST 재구성]

※ 제로트러스트는 ①SW Defined Perimeter, ②Micro-Segmentation, ③Enhanced Identity Governance에 기반을 두며, 각각의 자원에 대한 접속요구에 **동적인증을 통한 선인증 후 접속,** 이후에도 **가시성 확보를 통한 지속적 모니터링**으로 보안 수준을 높임

참고 2 | 기존 경계 기반 VS 제로트러스트 보안모델 비교

■ 제로트러스트의 기본 개념은 **"Never Trust, Always Verify"**이며, 이를 위한 첫 번째가 **보호해야 할 모든 데이터와 컴퓨팅 서비스**를 각각의 **자원으로 분리·보호**하는 것이며, 이를 기반으로 **각 자원**에 접속 요구에대한 **지속적인증 등 접근제어 및 모니터링**을 통해 **보안 수준을 높일 수** 있음

■ 외부 침투에 대한 기존 VS 제로트러스트 보안모델 비교



■ 최근 침해 사고에 대한 제로트러스트 대응 시나리오

① **(랩서스 해킹)** 랩서스 해킹('22년)은 블랙마켓 등을 활용한 사용자 자격증명을 도용하여 글로벌 대기업의 기업망 내부에 침투(횡적이동 및 권한 상승 등)하여 소스코드 등 기밀데이터 유출

→ **(제로트러스트 도입시)** 특정 사용자·기기의 의심스러운 활동에 대해 검증(기기 보안상태 확인, 사용자 행위 모니터링, 신뢰도 검증 등), 인증 강화 및 내부자원 이동 제한(추가 인증 요구, 최소 권한 부여, 마이크로 세그멘테이션 등)을 통해 대응 가능

② **(솔라윈즈 사태)** IT 솔루션 및 소프트웨어 제공 업체인 솔라윈즈의 업데이트 파일 오염('20년)을 통해, 18,000여개 이상의 솔라윈즈 고객사에 악성 코드 감염 사고 발생

→ **(제로트러스트 도입시)** 기기내 설치된 정상 프로그램에 대해서도 연결 권한을 확인하여 비정상적 접근에 대한 기본적인 차단, 허가되지 않은 중요 자원 접근 등 악성행위 모니터링을 통한 감지 및 대응, 해킹사고사례 공유(위협 인텔리전스) 정보기반 연관 행위 분석

Ⅲ 제로트러스트 아키텍처

전 장에서 확인한 바와 같이 제로트러스트에 대한 다양한 정의에도 불구하고 공통적으로 언급되는 핵심철학은 “결코 신뢰하지 말고, 항상 검증하라(**Never trust, Always verify**)”는 것이다. 또한 **Collection of Concept and Ideas**(NIST SP 800-207) 또는 **a Set of Principles**(MIT 링컨 연구소)라고 언급되기도 한다. 따라서 미국표준기술연구소에서는 7가지 사상(Tenets)과 3가지 접근법(Approach)을 제시하였고, 구글(BeyondCorp), 포레스터(Forrester) 등에서도 각각 제로트러스트의 기본철학 또는 원칙을 제시하였다.

그렇다면 제로트러스트는 어떻게 구현될 수 있을까? 제로트러스트 포럼 전문가들은 이와 같은 사항들을 분석한 후 국내 네트워크 환경 등을 고려하여 6가지 기본철학과 함께 제로트러스트 구현을 위한 3가지 핵심원칙을 제시하였다. 즉, 제로트러스트의 기본철학 6가지를 기술적으로 가능하게 해주는 것이 3가지 핵심원칙이다.

제로트러스트의 기본철학에 따라 보호해야 할 모든 데이터와 컴퓨팅 서비스는 각각의 자원(Resource)으로 분리·보호된다. 이를 가능하게 해주는 접근방법이 SDP(SW Defined Perimeter)와 마이크로 세그멘테이션이라고 할 수 있으며, 이렇게 분리된 각각의 자원에 대한 접속 요구는 강화된 인증체계를 통해 제어·관리된다고 할 수 있을 것이다.

또한 제로트러스트의 가장 중요한 철학 중 하나인 ‘선인증 후접속‘은 이와 같이 각 자원이 분리·보호되어 있어서 하나의 자원에 접속한 후 다른 자원에 접속할 때는 매번 인증을 받아야 접속이 가능하다. 특히, 각 자원에 대한 접속 요구시 인증 및 신뢰도 평가를 통해 접속허가가 결정되면 접속 요구자(또는 기기)와 자원간에 접속이 이루어지게 된다.

제로트러스트 기본철학 및 핵심원칙

제로트러스트는 **하나의 보안 솔루션이 아니라** 더 높은 수준의 보안성을 확보하기 위한 **개념들의 모음**이며, 이에 대한 **기본철학, 핵심원칙 및 동작원리**를 제시함

- **(기본철학)** 제로트러스트는 **특정 제품에 종속되지 않으며,** 기술적인 접근 外 조직의 문화, 프로세스 개선도 일부분으로 도입 가능
  - → 국내 제로트러스트 포럼 전문가 논의를 통해 해외에서 발표된 원칙(Tenet)* 등을 포함시킬 수 있는 방향으로 국내 환경에 적합한 기본철학(6가지) 도출
    * NIST SP 800-207 기본원칙(7가지), Forrester 기본개념(3가지), Google BeyondCorp 원칙(3가지), DoD 기본원칙(5가지) (※가이드라인(전체본) 부록 참고)

제로트러스트 기본철학

① 모든 종류의 접근에 대해 신뢰하지 않을 것(명시적인 신뢰 확인 후 리소스 접근 허용)
② 일관되고 중앙집중적인 정책 관리 및 접근제어 결정·실행 필요
③ 사용자, 기기에 대한 관리 및 강력한 인증
④ 자원 분류 및 관리를 통한 세밀한 접근제어(최소 권한 부여)
⑤ 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
⑥ 모든 상태에 대한 모니터링, 로그 기록 등을 통한 신뢰성 지속 검증·제어

- **(핵심원칙)** 제로트러스트 아키텍처를 구현하기 위한 **접근방법**으로 **네트워크 환경**에 따라 일부 상이할 수 있으나, 완전한 제로트러스트 솔루션은 **3가지 핵심원칙**을 모두 포함
  * 기존 경계 기반 보안과 달리 내부자조차도 더 이상 신뢰하지 않으므로, 강력한 관리, 인증, 접근제어 및 상태 감시를 통한 통제 필요

〈제로트러스트 구현 핵심원칙〉

핵심 원칙	세부 내용
인증 체계 강화 (기본철학 중 ①②③⑥)	▲ 각종 리소스 접근 주체에 대한 신뢰도(사용하는 단말, 자산 상태, 환경 요소, 접근 위치 등을 판단)를 핵심요소로 설정하여 인증 정책 수립 ※ 기업내 사용자에 대한 여러 아이디를 허용하여 일관된 정책을 적용하지 않거나, 신뢰도 판단없이 단일 인증 방식만으로 접속을 허용할 경우 **크리덴셜 스터핑**에 취약
마이크로 세그멘테이션 (기본철학 중 ②④⑤)	▲ 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 가능성**이 높아짐
소프트웨어 정의 경계 (기본철학 중 ①②⑤)	▲ 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 가능성**이 커짐

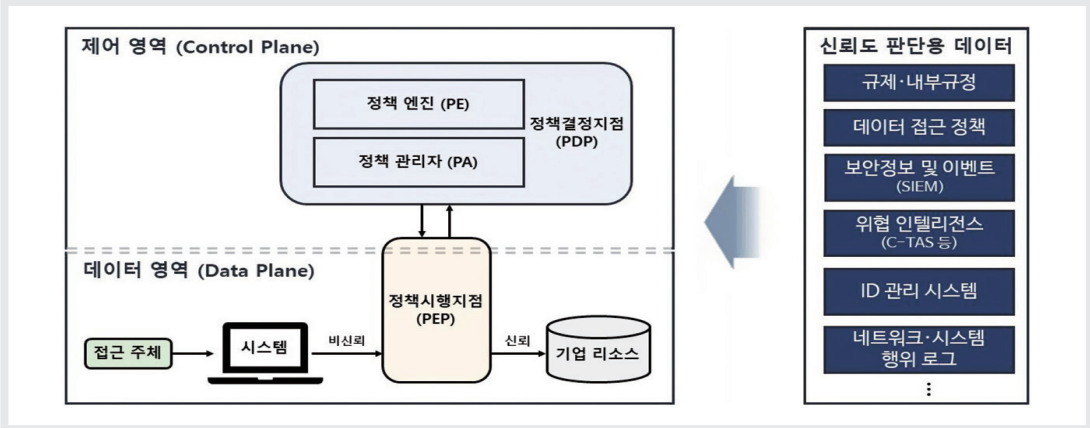
[NIST SP 800-207, 제로트러스트 아키텍처에 대한 다양한 접근법(3.1절)을 기반으로 작성]

제로트러스트 접근제어 원리

제로트러스트 아키텍처의 핵심 보안 기능은 **접근제어** 정책이며, 모든 자원 접근에 대한 **신뢰도평가·인증·허가**는 **정책결정지점**(PDP)과 **정책시행지점**(PEP) 간 통신에 의해 결정됨

- 제로트러스트 아키텍처는 **제어영역**과 **데이터 영역**으로 구분되어야 하며, 접속 요구 제어를 위한 **정책결정지점**(PDP)과 **정책시행지점**(PEP)이 있음
  - PDP는 **정책엔진**(PE)과 **정책관리자**(PA)로 나뉘며, PE는 **신뢰도**를 판단하여 **접속 허가**를 최종 결정, PA는 PEP에 명령하여 **정책을 실행**
    * PE, PA, PEP 등은 논리 컴포넌트로서 기업 네트워크 환경과 리소스 종류, 접근제어 기술에 따라 구현 방식이 달라질 수 있음
  - 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
    * 신뢰도 평가는 신뢰도 판단용 데이터(아래 구성도 참고)를 기반으로 인공지능(AI·ML) 기술을 활용하여 결정

〈제로트러스트 접근제어 논리 컴포넌트 구성도〉



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

〈제로트러스트 접근제어를 위한 주요 컴포넌트〉

구분		주요기능
정책 결정지점 (Policy Decision Point)	**정책 엔진** (Policy Engine)	▲'신뢰도 평가 알고리즘'* 기반으로 접근 주체가 리소스에 접근할 수 있을지를 최종적으로 결정 * ① 접근정보(OS 이름·버전, 사용중 소프트웨어, 권한 등) → ② 특정기준, 접수, 가중치, 머신러닝 등 다양한 방식으로 신뢰도를 평가하는 알고리즘
	정책 관리자 (Policy Administrator)	▲정책엔진의 결정을 정책시행지점에 알려주어 접근 주체와 리소스 사이의 통신 경로를 생성 또는 폐쇄
정책시행지점 (Policy Enforcement Point)		▲데이터 영역에서 접근 주체가 기업 리소스 접근 시 결정된 정책에 따라 최종적으로 연결·종료 역할 담당 ※ 방화벽, 네트워크 접근통제 등 단순 일부 제품 도입을 통해 높은 성숙도의 제로트러스트 보안모델 구현은 어려우며, 다양한 정책·제품이 조화를 이루어야 함

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

● 예를 들어, **소프트웨어 정의 경계**(SDP) 기술 기반으로 제로트러스트 아키텍처를 구현하면, SDP 컨트롤러가 **PDP**(PE+PA), **리소스** 혹은 **리소스 게이트웨이**(Accepting Hosts, AH)가 PEP 역할 수행

- 단말(Initiating Hosts, IH)이 리소스(AH)에 접속을 요청할 때, SDP 컨트롤러는 **인증·신뢰도 판단 결과** 등을 기반으로 **접속을 허가·거부**하는 결정을 내리며, 이에 따라 리소스(AH)는 접속 연결·거부

  * 아래 그림에서 ①-1은 기업이 관리하는 사용자 단말[1], ①-2는 기업 관리 대상이 아닌 사용자 단말을 의미하며, ②-1은 리소스 A를 직접 관리하는 AH, ②-2은 여러 리소스들을 관리하는 AH 의미

- 참고로 NIST SP 800-207에서는 다음과 같은 4가지 형태의 제로트러스트 아키텍처 구현방법을 제시함

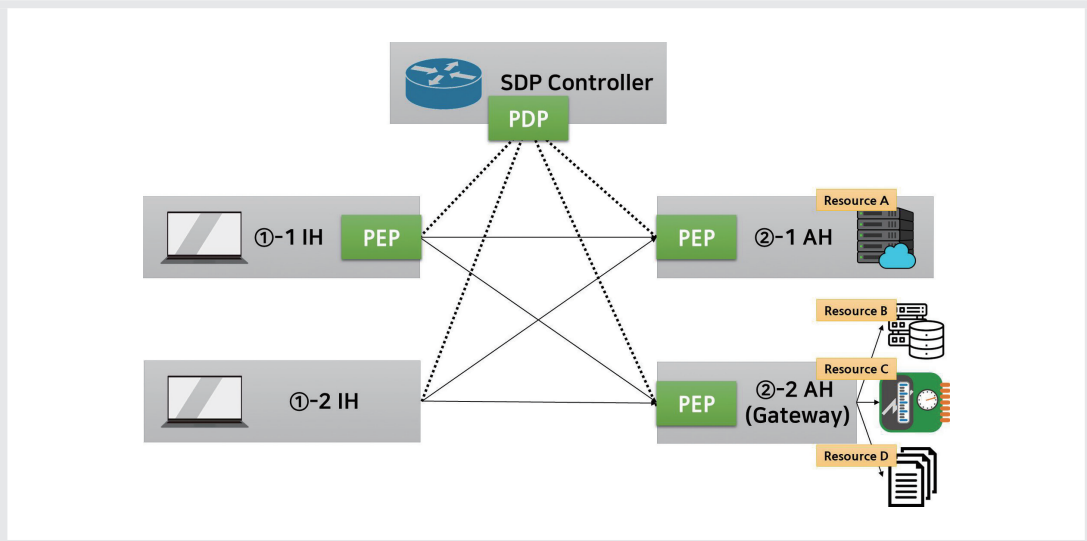
1) **(에이전트/게이트웨이 기반 배치)** 기업에서 지급한 단말(①-1)과 리소스(②-1)에 PEP 기능 분산 및 접속 승인시 암호화된 통신 경로 허용

2) **(리소스 그룹 배치)** 1)의 배치와 유사, 리소스(②-2)에서 직접 PEP 역할을 수행하는 대신 별도의 PEP 게이트웨이 역할

3) **(리소스 포탈 배치)** 기업 관리 대상이 아닌 단말(①-2)은 별도의 PEP 기능이 없으며, 리소스(②-1, ②-2)에서 단독으로 PEP 역할을 수행

4) **(기기 응용 샌드박스 배치)** 1)의 변형된 형태로, 샌드박스 내의 신뢰할 수 있는 응용은 단말 외부에 있는 PEP(②-1, ②-2)에게 접속 요청

〈소프트웨어 정의 경계 기반 제로트러스트 아키텍처 구성도〉



1) 단말에 PEP 기능을 포함하며, SDP Controller(PDP)의 신뢰도 평가를 위해 단말 보안 상태 정보를 확인·제공 필요
2) 단말이 기업내부 자산이 아닌 경우에 해당하며, 이 경우 일반적으로 단말에 PEP 기능을 포함할 수 없음

참고 3 | 글로벌 기업의 사례(구슬 BeyondCorp, MS)

1 구글 BeyondCorp

- **제로트러스트 아키텍처** 및 **접근 제어 모델**로 기존 경계 중심에서 벗어나 **사용자, 디바이스, 애플리케이션** 등에 기반하여 보안을 적용

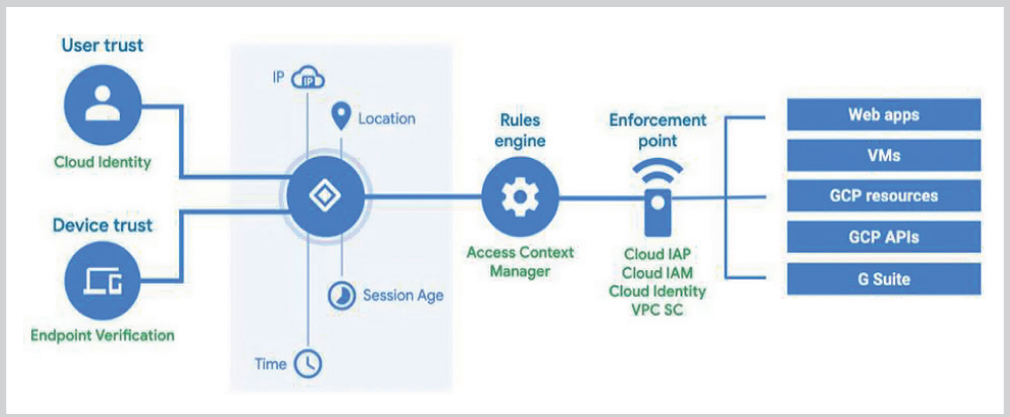
  ※ 3원칙 : ① 강력한 기기/사용자 식별, ②네트워크의 제로트러스트화, ③기기/사용자 신뢰도 추론 및 접근제어

  - **사용자**의 신원, **디바이스**의 상태, 접근하려는 **애플리케이션** 등 다양한 요소를 고려하여 접근을 허용 또는 거부

- 구글 클라우드의 **4가지 솔루션**을 결합하여 제로트러스트 보안 제공, ① **IAP**(Identity-Aware Proxy), ② **IAM**(ID 및 접근 관리), ③ **Access Context Manager**, ④ **엔드포인트** 확인

  - **사용자를 인증**하고, 접근 요청별로 **콘텍스트화**(user, role, type, label 등)하여 **세분화된 접근권한 관리가 가능**하게 함, **모든 규칙과 조건을 충족**하지 않는 한 **아무도 자원에 접근할 수 없으며, 네트워크 수준에서 자원을 분리하지 않고, 개별 장치 및 사용자**에 따라 접근권한 부여

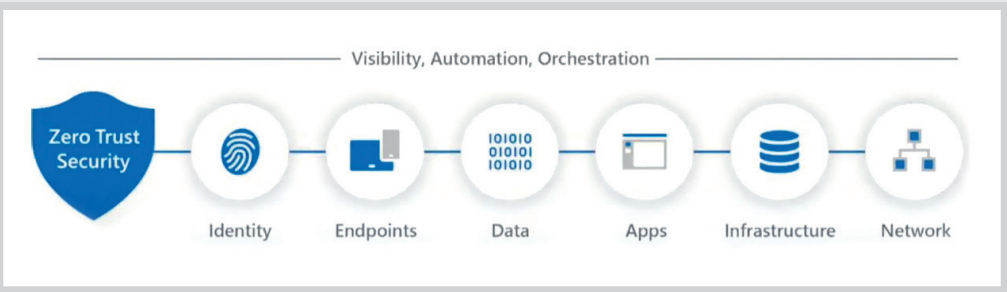
〈구글 BeyondCorp 구성도〉



2 MS 제로트러스트

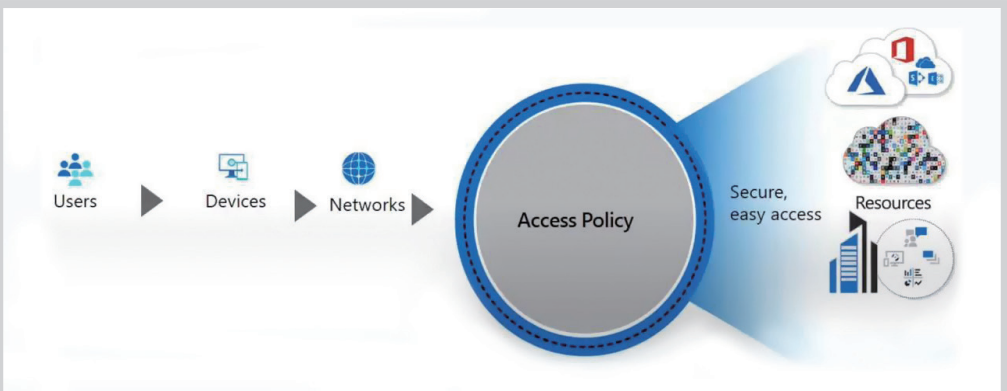
- MS는 제로트러스트 **준비상태**를 확인하고, **전략 도입**을 지원하기 위해 **ZT 배포센터** (Deployment Center) 출시
  - 배포센터는 배포지침을 **기술부문별**로 이해하기 쉽게 설명하고, **고객의 환경**에 특화된 제로트러스트 전략 수립을 지원
  - 또한, **사용자 인증, 기기 인증, 데이터관리, 애플리케이션 관리, 인프라관리, 네트워크 관리** 및 **모니터링·자동화·오케스트레이션** 등 7가지 단계를 순차적으로 적용하도록 관리

〈MS 제로트러스트 배포센터 관리단계〉



- 제로트러스트를 통해 기존의 **신뢰 중심**이었던 접근방식에서 누구도 **신뢰하지 않는** 접근방식으로 바뀜
  - 모든 통신 및 접근 요청을 **위협으로 간주**하고, **예외 또는 경고 상황** 발생시 자동으로 관리자에게 알리는 통합관리가 가능
  - **공격**을 찾아 쉽게 **탐지**하고 이에 대응하며, **조직 전체**에서 원치 않는 **이벤트**가 발생하는 것을 **차단하거나 방지**

〈MS 제로트러스트 체계도〉



Ⅳ 제로트러스트 도입

1장에서는 제로트러스트 추진배경을 기술하였고, 2장을 통해 제로트러스트의 개념과 도입 필요성 등을 확인하였다. 3장에서는 제로트러스트 구현을 위한 기본 철학에서부터 제로트러스트 접근제어 원리까지 정리하였다. 4장에서는 기업 및 기관 등에 제로트러스트를 도입하는 과정에서 참고할 수 있는 내용을 다루고 있다.

제로트러스트는 기존 보안체계를 대체하는 수단이나 솔루션이 아니라 기존 보안체계와 상당 기간 공존하면서 제로트러스트 기본철학을 달성할 수 있도록 발전해가는 긴 여정이라고 할 수 있다.

본 장에서는 기업 및 기관 등의 상황에 맞는 제로트러스트를 도입하기 위해서는 현재 상황을 분석하고 반영하는 '도입계획 수립', 제로트러스트 아키텍처의 근간을 이루는 '핵심요소' 정의 및 제로트러스트 도입계획 수립 시 목표 설정 및 도입단계별 진행 수준 점검에 참고할 수 있는 '성숙도(Maturity) 모델'을 제시하고 있다.

각 기업 및 기관별 네트워크 구조가 상이할 수 있으므로 본 장에서 제시하는 내용을 반드시 따라야 하는 것은 아니며 각 기업 및 기관의 상황을 고려하여 적절히 참고할 수 있다.

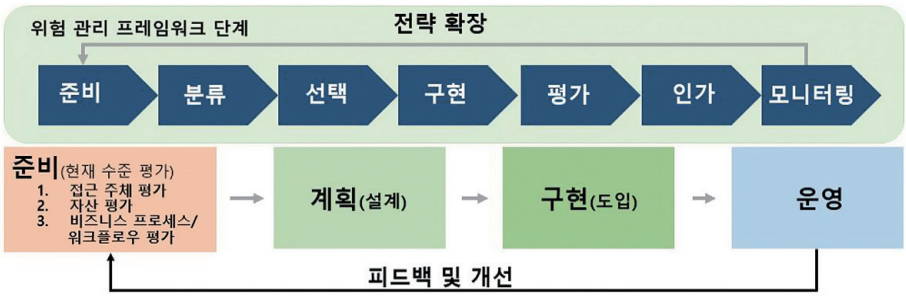
제로트러스트 도입 계획

제로트러스트 도입은 많은 **자원, 시간, 소요예산** 등이 필요한 작업으로 **충분한 검토** 및 **체계적인 준비**가 필요하며, 이를 위해 다양한 요소를 고려한 도입 계획 수립이 필요

- **도입계획 수립**은 보유 자원에 대한 보안 위협을 줄이기 위한 절차로 '**위험 관리 프레임워크**(NIST)'와 연계하여 도입단계* 검토가 가능

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

〈제로트러스트 도입을 위한 세부 절차〉



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

① **준비** 제로트러스트를 도입하기 전에 **기업망 핵심요소***를 중심으로 각 기업 및 기관 등의 **현재 보안 대상·수준**에 대한 평가** 필요

* 식별자, 기기, 네트워크, 시스템, 응용 및 워크로드, 데이터

** 접근 주체, 자산·기기, 비즈니스 프로세스/워크플로우 식별 및 성숙도 평가

② **계획** **성숙도 모델**을 기반으로 기존 보안체계와 **조화**를 이루어 **더 높은 수준**의 보안성 확보를 위한 **도입 설계 및 예산 검토**

③ **구현** 주요 자원의 **위치, 프로토콜***, 다양한 서비스 등을 고려하여 각 기업 및 기관 등의 생태계에 적합한 **솔루션 검토 및 구현**

* (자원 위치) 온프레미스, 클라우드 등, (프로토콜) 웹, SSH, IPv4, IPv6 등

④ **운영** 구현된 제로트러스트 아키텍처에서 **기본철학**(6개, 10P 참고)를 중심으로 **핵심원칙**(3개, 10P 참고)이 적절하게 동작할 수 있도록 설정·관리

⑤ **피드백·개선** 제로트러스트 성숙도 기반의 **완성도 비교, 모니터링** 및 **개선방안 도출** 등 각 단계의 **반복적 관리**를 통한 수준 고도화

제로트러스트 도입을 위한 기업망 핵심요소

성공적인 도입을 위해서는 다양한 네트워크 자원 중 제로트러스트 **기본철학, 핵심원리**와 연결되는 **네트워크 핵심요소**를 중심으로 **보안수준 진단** 및 **단계별 도입계획 수립**

- 제로트러스트 도입 계획 수립, 구현 및 운영 과정에서 現 보안 수준 평가 및 제로트러스트 아키텍처 구현 성숙도 평가 기준 필요
- 미국 CISA, DoD 등에서 제로트러스트 핵심요소를 정의하고 있으나 적용 대상 기관·기업의 특성, 네트워크 환경에 따라 상이

〈제로트러스트 도입을 위한 기업망 핵심요소〉

Forrester(7종)	CISA(5종)	DoD(7종)	SAP(6종)
①Data, ②Networks, ③People, ④Workloads, ⑤Devices, ⑥Visibility & Analytics, ⑦Automation & Orchestration	①Identity, ②Device, ③ Network/Environment, ④Applications Workload, ⑤Data	①User, ②Device, ③Network/Environment ④Applications&Workload ⑤Data, ⑥Visibility & Analytics, ⑦Automation & Orchestration	①Identities, ②Data, ③Network, ④Applications, ⑤Infrastructure, ⑥Endpoints

[참조 : Forrester, CISA, DoD, SAP]

- 본 가이드라인에서는 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 주고받는 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

제로트러스트 성숙도 모델

성숙도 모델은 제로트러스트 **도입 계획수립** 단계에서 현재 **보안수준에 대한 평가** 및 **목표 수립, 예산검토, 구현·운영 단계** 등에서 완성도를 가능할 수 있는 기준 제시

● 제로트러스트 성숙도 모델은 일반적으로 **3단계로 제시**하고 있으며, 일부 기관(美 CISA*, NSTAC)은 더 세분화하여 정의하고 있음

※ 美 대통령 행정명령('21.5월)의 실행을 지원하기 위해 예산처(OMB)는 연방 정부 각 기관이 CISA의 성숙도 모델을 기준으로 제로트러스트 도입예산을 요청토록 알림

〈제로트러스트 성숙도 단계〉

구분	Microsoft(3단계)	CISA(4단계)	DoD(3단계)	NSTAC(5단계)
성숙도 단계	①Traditional, ②Advanced, ③Optimal	①Traditional, ②Initial, ③Advanced, ④Optimal	①Baseline, ②Intermediate, ③Advanced	①Initial, ②Repeatable, ③Defined, ④Managed, ⑤Optimized

- 포럼 전문가들은 국내 환경에 적합한 성숙도 3단계 모델과 함께 앞서 제시한 핵심요소(6종)별로 성숙도 제시(CISA 성숙도 모델 참고·보완)

〈제로트러스트 성숙도 단계(국내)〉

구분	주요 내용
기존 (Traditional)	▲아직 제로트러스트 아키텍처를 적용하지 않은 수준으로, 대체로 네트워크 방어에 초점을 맞춘 경계 기반 보안모델이 적용되어 있는 상태(정교한 공격, 내부자 공격 등에 일부 취약성을 가짐)
향상 (Advanced)	▲제로트러스트 철학을 부분적으로 도입한 수준으로 제로트러스트 원칙이 보안 아키텍처에서 핵심 기능이 되는 상태(최소 권한 접근, 네트워크 분할, 로깅 및 모니터링 등이 부분적으로 적용되어 기본보다 높은 보안성 달성)
최적화 (Optimal)	▲제로트러스트 철학이 전사적으로 적용된 상태(자동화된 운영, 네트워크 세분화, 신원에 대한 지속적인 검증을 통한 최소 권한의 안전한 접근제어 등을 통하여 보안성이 크게 개선)

- 아래 표는 식별자·신원 핵심요소에 대한 성숙도 단계별 기능을 예시로 제시한 것으로 상세 내용은 가이드라인(전체본) 참조

〈기업망 핵심요소별 성숙도 단계〉 (※ 상세내용은 가이드라인(전체본) 참조)

① (예시)식별자·신원

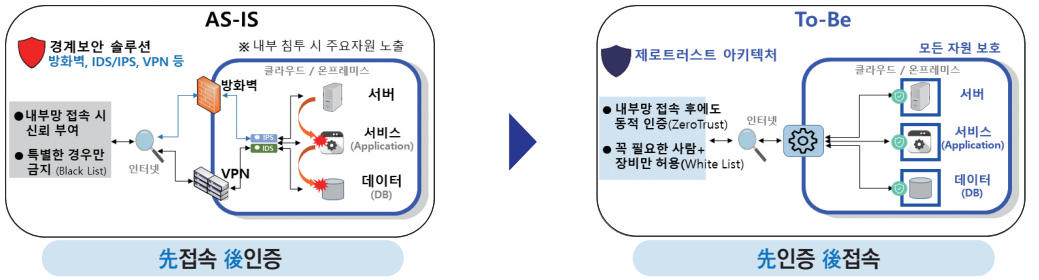
구분	기존 수준	향상 수준	최적화 수준
식별자 관리	▲온프레미스 ID 공급자	▲클라우드/온프레미스 시스템 기반 ID 연합	▲클라우드/온프레미스 환경 전반 통합 ID 활용
인증	▲패스워드 또는 다중 인증 방식	▲다중 인증 방식	▲접근 권한 승인뿐만 아닌 지속적 신원 검증
위험도 평가	▲위험에 대한 제한된 결정	▲단순 분석, 정적 규칙 기반 식별자 위험성 판단	▲실시간 사용자 행동 분석을 통해 위험 결정 및 지속적 보호
가시성 및 분석	▲기본 속성 기반 사용자 활동에 대한 가시성 분류	▲기본 속성 기반 사용자 활동에 대한 가시성 집계·분석 및 보고를 통한 수동적 개선	▲높은 정확도의 속성, 사용자 및 개체 행동 분석 솔루션을 통해 사용자 가시성 확보 및 중앙 집중화
자동화 및 통합	▲ID와 자격 증명을 수동으로 관리·통합	▲ID 연합 및 ID 저장소를 통한 관리 허용을 위한 기본 자동화 통합	▲ID 생명 주기를 완벽히 통합하고, 동적 사용자 프로파일링, 동적 ID 및 그룹 멤버십, 적시+적절한 접근제어 구현

제로트러스트 도입 전후 비교

제로트러스트는 보호 대상 자원에 대한 접속 요구 시마다 **아이디, 패스워드, 최종 사용위치** 등 **다양한 신뢰도 평가**를 통해 **先인증** 후 접속을 허용

● 제로트러스트 보안은 '**先인증 後접속**'을 기반으로 **동적인증**을 통해 접속요구를 제어함으로써 **횡적이동**에 의한 **보안사고 방지** 가능

〈경계 보안 Vs 제로트러스트 보안 비교〉



先접속 後인증	先인증 後접속
● 보안 경계(DMZ, FW, VPN 등) 통과시 암묵적 신뢰	● 내·외부 구별, 사용자·네트워크의 위치 등에 관계 없이 모든 요청을 신뢰하지 않음
	● 모든 자산 보호, 최소 권한, 동적인증* * 각 자원의 접근권한 세분화 및 강화된 인증 적용
● SSL VPN에는 장비 인증 기능이 없어 ID/PW 탈취만으로 시스템 접속 가능	● 동적인증, OTP 등 다중인증체계로 ID/PW 탈취만으로 침입 불가능

- NSA는 제로트러스트 **도입 전후 비교**를 위해 대표적인 **악의적 공격 3가지**에 대해 제로트러스트 기반 대응 시나리오 제공('21년)

〈침해 시나리오 적용시 경계 보안 Vs 제로트러스트 보안 비교〉

구분	경계 기반 보안모델 한계	제로트러스트 대응 시나리오
사용자 자격증명 도용 (공격자 기기 사용)	▲제3자에 의해 사용자 자격 증명이 탈취되거나 위조될 경우 접속기기와 무관하게 기업망 내부 자원 접근 및 피해 발생 ※ 기업 외부 접속 시 강화된 다중 인증 등을 통해 일부 대응 가능	▲접속 기기 모니터링*을 통한 **접근 권한 즉시해제** * 기업자산 여부, 기기 보안상태 등을 확인 ▲정상 인증 후에도 **비정상 행위**(기밀 자료 접근 등) 지속 모니터링 및 **필요시 강화된 다중 인증 적용**
원격 공격 혹은 내부자 위협 (내부 기기 장악)	▲공격자가 기업망 내부 접속 후 권한이 높은 계정에 접근하여 다양한 자원 접근, 손상 등의 피해 유발	▲데이터에 대한 최소 권한 부여 및 세밀한 접근 제어를 통해 **권한이 없는 중요 데이터 접근 불가** ▲사용자 행위 모니터링을 통해 **비정상적인 활동 감지 시 추가 인증 요구 또는 접근 제한**
공급망 공격 (내부 기기 및 정상 프로그램 장악)	▲기업망 내부 접속 시 높은 신뢰성이 부여되어 다양한 공격 가능	▲**정상적인 기기, 정상 배포 프로그램도 비신뢰** 및 최소권한 부여 원칙 적용 ▲모든 연결 및 접속 기기의 행위를 모니터링하여 악성 코드를 통한 **공격 명령·제어, 데이터 유출 시도 차단**(권한이 없는 원격 접속 강제 종료)

V 제로트러스트 도입 참조모델

지금까지 제로트러스트 추진배경에서부터 제로트러스트 아키텍처 도입을 위한 절차 등을 간략하게 알아보았다. 미국표준기술연구소(NIST) 800-207에서는 5가지 제로트러스트 아키텍처 사용사례(use case)를 제시하고 있다.

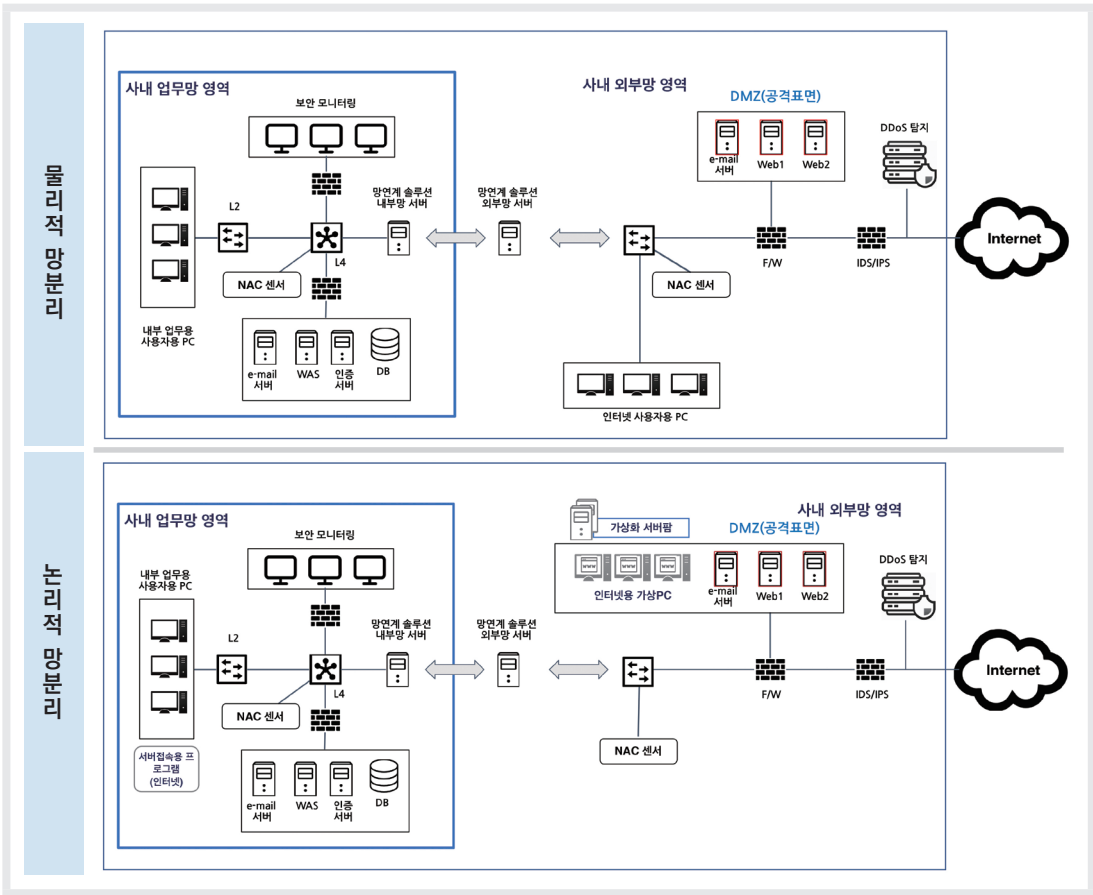
이와 관련하여 제로트러스트 포럼의 민간 전문가들은 NIST의 사례를 그대로 제시하는 것에 많은 고민과 토론을 거쳤다. 미국의 사례를 그대로 제시할 경우 가이드라인 작업이 훨씬 수월한 반면에 제로트러스트 아키텍처를 도입한 후 개선되는 보안성을 명확하게 제시하기 어려울 것이라는 의견이 많았다. 따라서 포럼에서는 국내 일반인 및 보안 관련 전문가들이 국내 네트워크 환경 제로트러스트 아키텍처를 도입했을 때 그 효과성을 조금 더 구체적으로 체감할 수 있도록 제시할 필요가 있다고 의견을 모았다.

본 장에서는 기존 경계 기반 보안모델과 제로트러스트 보안모델의 차이점을 비교하고 사이버 공격에 대한 안전성을 제시하며, 이를 위해 COVID-19 이후 국내에서 보편화된 원격근무(재택근무) 환경을 참조 모델(예시)로 제시하였다. 또한 각각의 네트워크에 해킹 시나리오를 적용하여 제로트러스트 아키텍처 도입 시 보안이 강화되는 원리를 제시하였다. 여기에 제시된 사례는 실제 우리나라의 연구자들이 시험용 네트워크를 구성하여 실험한 결과이다. 다만, 본 서에서 제시된 제로트러스트 아키텍처 구현 제품에 대한 정보는 국내 기업 간의 공정 경쟁을 통한 기술발전 및 제로트러스트 저변 확대를 위해 명시하지 않기로 하였다.

COVID-19 이전 원격근무 환경

- 코로나 19 확산 이전 우리나라 **정부·공공기관** 및 **중요 정보통신기반 시설**들은 물리적 **망분리** 또는 **논리적 망분리** 형태로 운영
- **(물리적 망분리)** 물리적으로 내외부 망을 구분하고, 망연계 솔루션을 이용하는 형태로 PC 2개(업무용, 인터넷용)를 사용
  - 이에 따라 사이버 공격 표면은 DMZ의 웹과 이메일 서버가 됨
- **(논리적 망분리)** VDI(Virtual Desktop Infrastructure) 서버를 기반으로 1개 PC를 업무망과 인터넷용으로 **논리적으로 분리** 활용
  - 최근에는 별도 **VDI 서버 설치 없이** 1 PC 자체를 **가상화**하여 **업무망용과 인터넷용**으로 가상자원을 할당하여 사용하는 경우도 있음
  - 이 경우도 공격 표면은 **DMZ의 웹과 이메일 서버**가 됨

〈망분리 유형에 따른 네트워크 구성(예시)〉

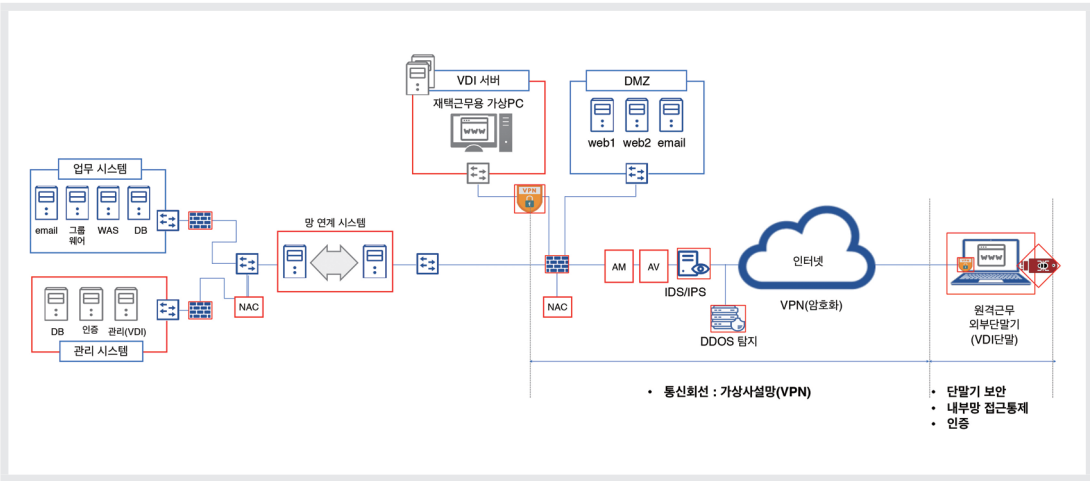


※ 보안수칙을 준수한다면, 외부 공격 대상은 웹 서버와 이메일 서버임.
이의 경우 경계 기반 보안모델에서는 웹 서비스와 이메일 관련된 보안에 집중하여 효과성을 높일 수 있으나 현실은 그렇지 못함

COVID-19 이후 일반화된 원격근무 환경

- 코로나 19 이후 일반화된 **원격근무 네트워크**는 **VDI를 기반**으로 하며 **원격 근무 시스템** 외에 보안시스템 등으로 구성됨
  - **보안 시스템:** VPN, 방화벽/WAF, AM(Anti-Malware), AV(Anti-Virus), NAC, IDS/IPS, DDoS 탐지, 망연계시스템, PC보안
  - **원격시스템:** VDI 서버, VDI 관리 서버, 외부단말기(VDI/VPN 단말)
  - 원격근무에 따른 **공격표면**(VPN): 아래 그림은 **SSL VPN**을 나타내며, 원격근무 외부단말기와 VDI 서버 VM과 터널링이 생성되면 이는 두 단말 사이에 논리적인 망이 생성됨을 의미함

〈코로나19 이후 일반화된 원격근무 형태〉

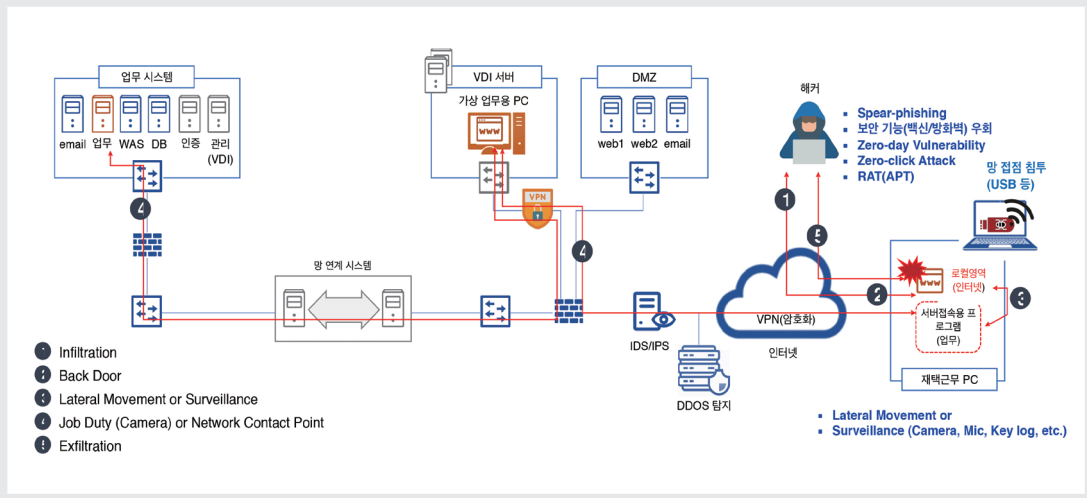


- 기존의 경계 기반 보안모델은 이와 같이 **원격·재택 근무** 등으로 네트워크 경계를 **구분하기 모호**해지면서 한계에 봉착
  - 경계에 설치된 보안시스템만 통과하면 암묵적 신뢰가 부여됨에 따라 내부자 권한 탈취에 이어 보안시스템 통과 후 내부 접속
  - 내부 시스템 접속 이후에는 횡적이동을 통한 권한 상승을 이용하여 DBMS에 접근, 대량 정보 유출로 이어지는 사례가 나타나고 있음

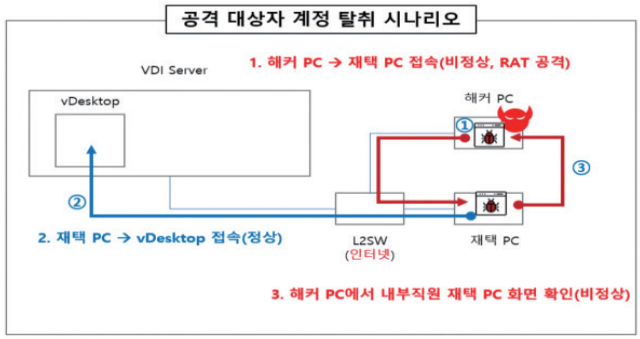
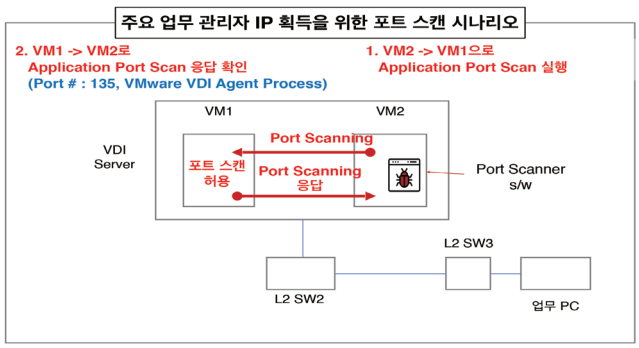
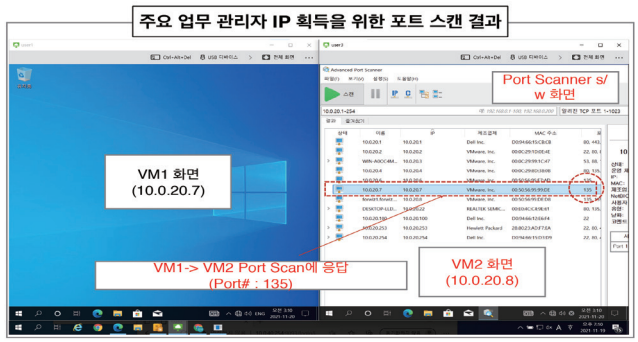
일반적 원격근무 환경에 대한 공격 사례

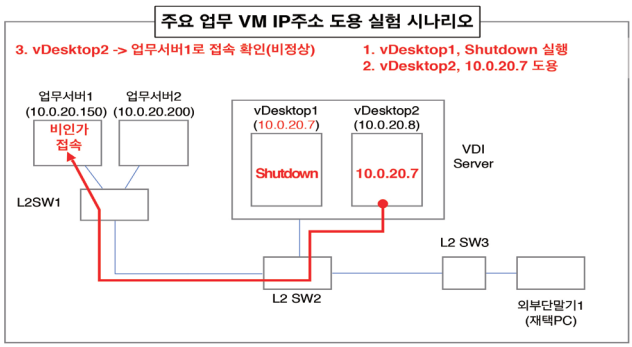
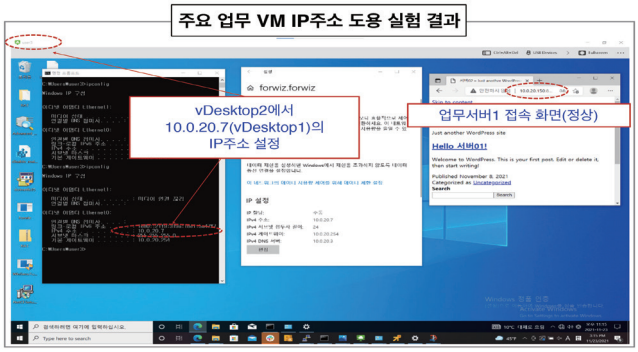
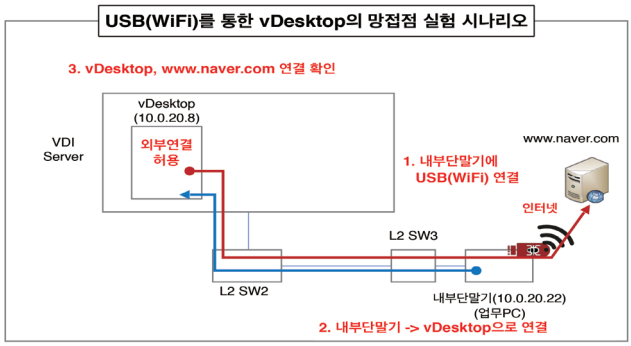
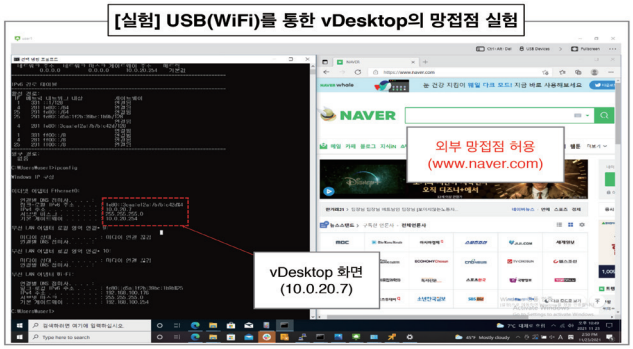
- 기존 경계 기반 보안모델이 적용된 원격지 근무환경에서의 공격 시나리오
  - 공격 시나리오는 외부의 악의적인 공격자와 내부 공격자로 구분, ① 외부 공격자는 상당한 실력자로 가정, ② 내부 직원은 간단한 조작으로 공격이 가능하도록 구성 함
  - 외부 공격자는 1) 공격대상자(주요 업무 담당자)의 재택 PC에 악성코드 RAT(Remote Access Trojan)을 주입하여 ID/Password 탈취, 2) SSL-VPN 서버와 클라이언트 간 설정 취약점을 이용 VPN의 논리적인 망분리 무력화 후 공격대상자의 권한으로 VDI(원격업무를 위한 가상 PC) 접속, 3) 주요 업무 취급자(권한 상승 공격)의 권한 획득, 4) 접근 금지된 서버에 접속하여 데이터 탈취할 수 있도록 실험 시나리오를 구성함
  - 내부 직원은 VPN의 논리적인 망분리 무력화를 위해 단순히 USB 타입 WiFi 동글을 이용하여 망접점 생성 후 업무 정보를 외부로 유출 하도록 설계함

〈원격근무 환경에 대한 사이버 공격 환경 셋팅〉



외부 공격자 공격 실험

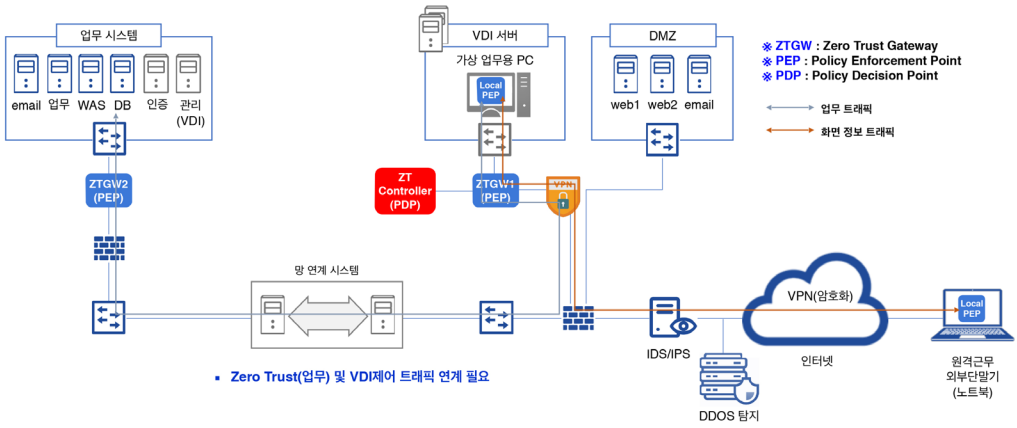
공격 시나리오	실험 시나리오 및 결과
■ 원격 근무자 계정 탈취 ① RAT 감염 ② VPN 논리적인 망 무력화 ③ 키로그 및 주요정보 전송	
■ 주요정보 해킹 결과 ① 공격 대상자 카메라 마이크획득 ② 키로그 정보 획득(계정탈취가능) ③ 대상자 VM 화면 정보 획득	
■ 주요 업무자 권한 획득을 위한 Port 스캔 ① 공격 대상자의 VM에 포트 스캔 S/W 설치 가정 ② VM ↔ VM 포트 스캐닝 ③ Port 번호를 보고 주요 서비스에 접근하는 VM을 알수 있음 ④ 예: DBA VM IP 정보 획득	
■ VM ↔ VM 포트 스캔 결과 ① 포트 스캔 결과가 오른쪽 하단에 나타남 ② 포트 번호를 이용 주요 업무를 수행하는 IP 획득	

공격 시나리오	실험 시나리오 및 결과
■ IP 도용을 통한 비인가 서버 접속 ① 주요 업무 수행자 IP 주소 획득 ② 주요 업무자의 업무 공백시 VM은 비 활성화 된 상태 ③ 공격자 VM이 주요업무 IP 주소로 변경하여 업무 서버 접속 ④ 비 인가 업무서버 접속 가능	
■ IP 도용을 통한 비인가 접속 실험 결과 ① 공격대상 VM이 비 활성화 되었을때 ② VM의 IP 설정 변경이 이루어짐 ③ 비인가 서버에 접속이 성공적으로 이루어짐	
■ 망접점 발생 (WiFi를 통한 망접점 생성 시나리오) ① 내부 업무 PC에서 WiFi 동글 이용 ② 내부의 가상화 서버 접속 ③ 내부의 정보를 외부로 유출 ④ 내부적으로 인증이 이루어짐에 따라 모니터링을 수행하지 않음	 

안전한 원격근무를 위한 제로트러스트 참조 모델

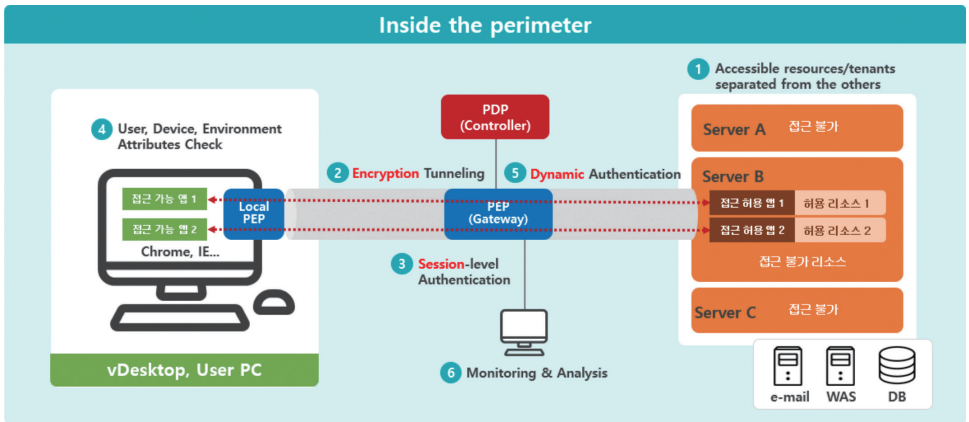
- 우리나라에 일반적인 원격지 근무환경에 제로트러스트 아키텍처를 도입하여 실험을 위한 인프라를 구축
  - 보호해야할 데이터 및 컴퓨팅 서비스가 각각의 자원(Resource)으로 분리·보호되고, 각 자원에는 PEP 또는 제로트러스트 게이트웨이가 배치됨

〈원격근무 환경에 제로트러스트 아키텍처를 도입한 예〉

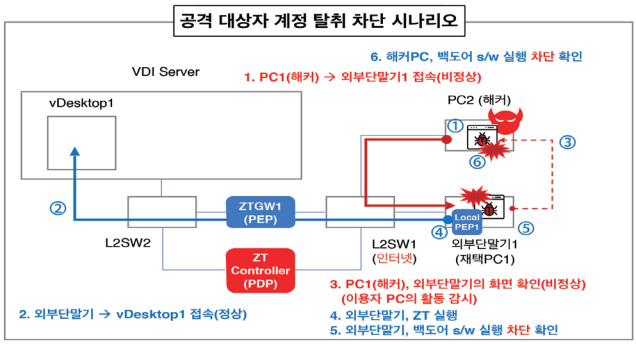
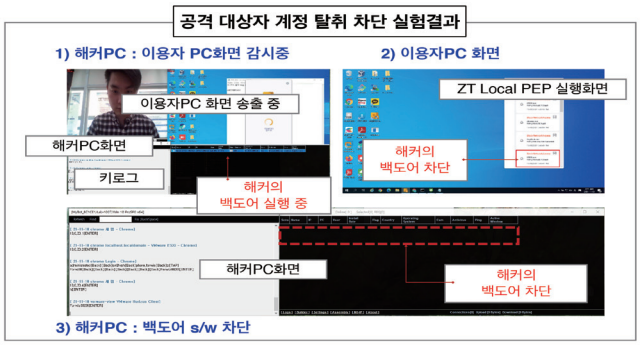
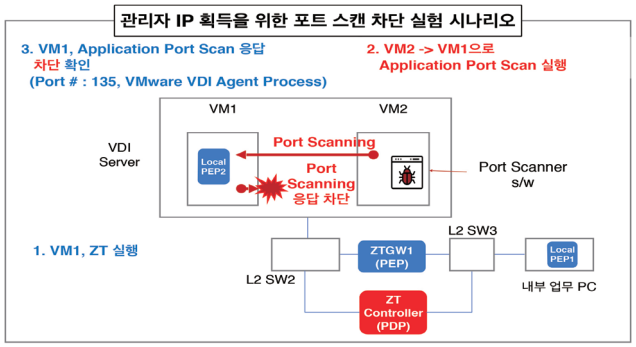
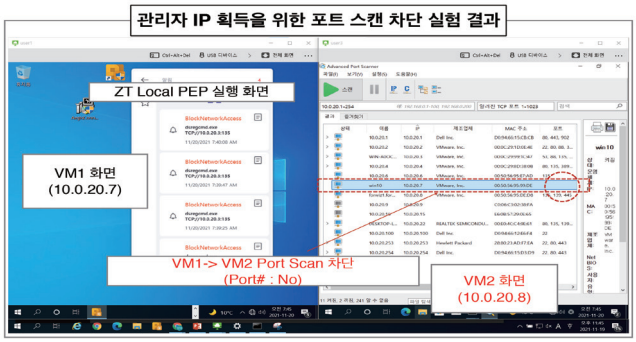


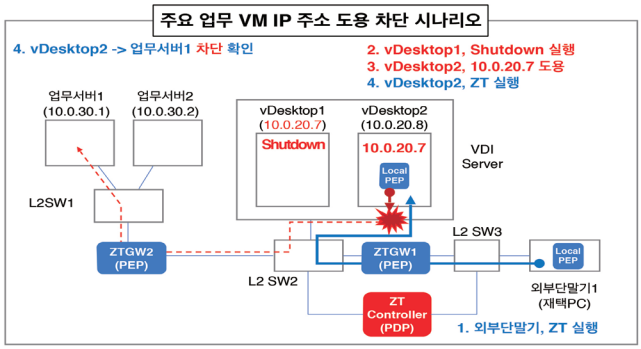
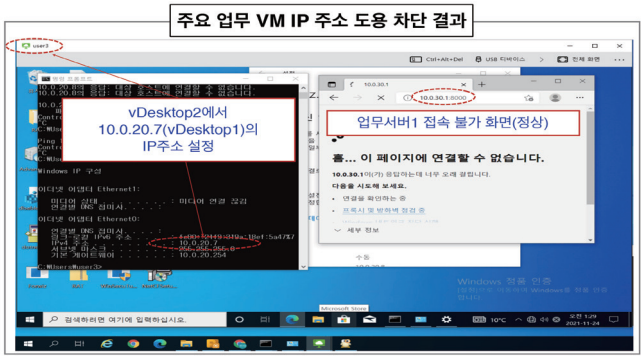
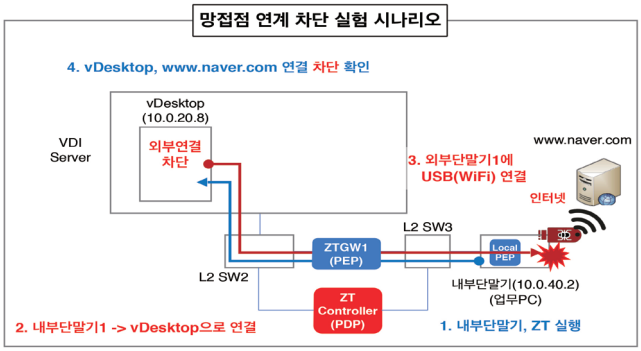
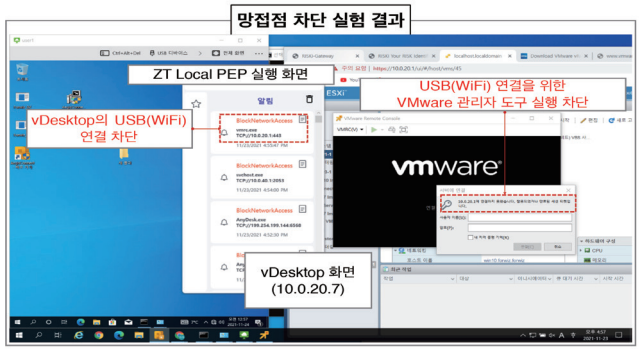
- 각각의 자원은 서로 분리·보호①, 사용자, 기기 등의 접근요구④에 대해 PEP 게이트웨이는 PDP의 허가를 받아 접속 허용⑤, 사용자 또는 기기와 허용리소스1 간 암호통신②, 세션 단위 통신 허용③으로 자원 간(리소스1 → 리소스2) 횡적이동 불가능

〈데이터 플로우 제어 구조(예시)〉



외부 공격 차단 실험

정책 및 실험결과	차단 실험 시나리오 및 결과
■ 제로트러스트 기반 해커의 재택PC를 이용한 VM 접속 차단 ① Local PEP에 의해 인가된 App만이 통신이 가능 하도록 구성 ② 해커의 RAT는 실행 및 통신이 되지 않도록 구성	
■ 실험결과 ① 해커의 백도어가 차단됨 ② 카메라 및 마이크 차단됨 ③ 키로그가 차단됨	
■ 주요 업무자 권한 획득을 위한 Port 스캔 차단 ① 공격 대상자 VM에 Local PEP 설치 ② 화이트 리스트를 제외한 App에서의 통신 응답 차단	
■ VM ↔ VM 포트 스캔 차단 결과 ① Local PEP에 의해 차단되어 포트 스캐닝된 결과가 전송되지 않음	

정책 및 실험결과	차단 실험 시나리오 및 결과
■ IP 주소를 도용한 비인가 업무서버 접근 차단 ① Local PEP에는 처음 환경 설정시 자신의 IP 주소를 가지고 있음 ② 정책 서버로부터 IP 주소 변경 허가 없이는 IP 주소 변경이 불가능 하도록 구성	**주요 업무 VM IP 주소 도용 차단 시나리오** 
■ 실험결과 ① IP 주소 변경이 안됨 ② 업무서버 1로 접속 불가	**주요 업무 VM IP 주소 도용 차단 결과** 
■ 망접점 발생 차단 (WiFi를 통한 망접점 생성 차단) ① 정책 서버는 단말기의 Local PEP에 접속가능한 IP를 부여 ② 정책 리스트에 없는 통신을 수행하지 않음 ③ 망 접점이 원천적으로 차단됨	**망접점 연계 차단 실험 시나리오**  **망접점 차단 실험 결과** 

Ⅵ 참고문헌

[1] John Kindervag (Forrester), “No More Chewy Centers: Introducing the Zero Trust Model of Information Security”, 2010.09

[2] John Kindervag (Forrester), “Build Security Into Your Network's DNA: The Zero Trust Network Architecture”, 2010.11

[3] CSA, “Software Defined Perimeter”, 2013.12

[4] Rory Ward et al (Google), “BeyondCorp - A New Approach to Enterprise Secuirty”, 2014.12

[5] Barclay Osborn et al (Google), “BeyondCorp - Design to Deployment at Google”, 2016.03

[6] Luca Cittadini et al (Google), “BeyondCorp Part III - The Access Proxy”, 2016.12

[7] Jeff Peck et al (Google), “Migrating to BeyondCorp - Maintaining Productivity While Improving Security”, 2017.06

[8] Victor Escobedo et al (Google), “BeyondCorp 5 - The User Experience”, 2017.09

[9] Hunter King et al (Google), “BeyondCorp - Building a Healthy Fleet”, 2018.03

[10] ACT-IAC, “Zero Trust Cybersecurity Current Trends”, 2019.04

[11] Microsoft, “Zero Trust Maturity Model”, 2019.10

[12] CSA, “Software Defined Perimeter (SDP) and Zero Trust”, 2020.05

[13] 니시무라 히로시 등, “政府情報システムにおけるゼロトラスト適用に向けた考え方 (정부 정보 시스템에서 제로트러스트 적용을 위한 사고 방식)”, 2020.06

[14] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[15] Cyolo, “4 Zero Trust Use Cases for CISOs and IT Managers”, 2020.12

[16] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, “Department of Defense Zero Trust Reference Architecture, Version 1.0”, 2021.02

[17] NSA, “Embracing a Zero Trust Security Model”, 2021.02

[18] Steve Turner et al (Forrester), “A Practical Guide To A Zero Trust Implementation”, 2021.03

[19] ACT-IAC, “Zero Trust Report - Lessons Learned from Vendor and Partner Research”, 2021.05

[20] Executive Order 14028, “Improving the Nation’s Cybersecurity”, 2021.05

[21] CISA, “Zero Trust Maturity Model - Pre-decisional Draft Version 1.0”, 2021.06

[22] GSA(연방총무청), “Zero Trust Architecture - Buyer’s Guide”, General Services Administration, 2021.06

[23] ZeroTrustMaturity.org, “Zero Trust Maturity Model (ZTMM) assessment results”, 2021.06

[24] 정보처리추진기구(일본), “ゼロトラスト導入指南書 - 情報系·制御系システムへのゼロトラスト導入”, 2021.06

[25] CISA, “Cloud Security Technical Reference Architecture Version 1.0”, 2021.08

[26] 니시무라 히로시 등, “ゼロトラストネットワークを実現するための 政府職員のアカウントやアセットの管理 (제로트러스트 네트워크를 실현하기 위해 정부 직원의 계정 및 자산 관리)”, 2021.08

[27] Microsoft, “Evolving Zero Trust - How real-world deployments and attacks are shaping the future of Zero Trust strategies”, 2021.09

[28] CSA, “Toward a Zero Trust Architecture - A Guided Approach for a Complex and Hybrid World”, 2021.10

[29] OMB(미국 관리예산실), “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”, 2022.01

[30] NSTAC(국가안보통신자문위원회), “Draft Report to the President - Zero Trust and Trusted Identity Management”, 2022.02

[31] CISA, “Applying Zero Trust Principles to Enterprise Mobility”, 2022.03

[32] CSA, “Software-Defined Perimeter (SDP) Specification v2.0”, 2022.03

[33] Kate Lake (Jumpcloud), “Why Assess Your Zero Trust Maturity?”, 2022.04

[34] NIST CSWP 20, “Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators”, 2022.05

[35] DoJ (미국 법무부), “U.S. Department of Justice Information Technology Strategic Plan”, 2022.06

[36] NIST SP 1800-35A, “Implementing a Zero Trust Architecture - Volume A: Executive Summary”, 2022.06

[37] 디지털청(일본), “常時リスク診断 · 対処 (CRSA) システム (상시 위험 진단 및 대처(CRSA) 시스템 아키텍처)”, 2022.06

[38] 디지털청(일본), “ゼロトラストアーキテクチャ 適用方針 (제로트러스트 아키텍처 적용 정책)”, 2022.06

[39] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, “Department of Defense Zero Trust Reference Architecture, Version 2.0”, 2022.07

[40] NIST SP 1800-35B, “Implementing a Zero Trust Architecture - Volume B: Approach, Architecture, and Security Characteristics”, 2022.07

기관 또는 기업의 입장에서는 사업의 내용, 비즈니스 영역, 고객의 범위 등 다양한 요소를 고려하여 제로트러스트를 도입할 수도 있고, 기존 경계 기반 보안체계로도 충분한 경우가 있을 것이다. 그러나 현재보다 더 높은 보안 수준을 요구하거나 보안 수준을 높여야 할 필요가 있는 기관·기업들이 있을 수 있다. 이와 같이 제로트러스트 도입 여부를 결정하는 것은 각 기관·기업의 자체적인 판단하에 이루어질 것으로 본다.

본 서는 국내 정부 기관·기업 등이 제로트러스트 도입을 위해 다양한 사항을 검토할 때 가장 먼저 참고할 수 있는 가이드라인 제공을 목적으로 하였다. 가이드라인 대상 독자층이 기관·기업의 경영진, 보안 책임자, 그 외 임직원 및 일반인에 이르기까지 광범위하여 집필 과정에서 많은 어려움이 있었다. 따라서, 가이드라인 전체본의 경우 보안전략수립 책임 및 실무자에게 필요한 정보를 제공하는 것을 목적으로 하되, 본 요약서는 비전문가인 기관장 혹은 기업 경영진 및 일반 임직원 등을 대상으로 제로트러스트의 개념을 보다 쉽게 설명하고자 노력하였다. 이는, 조직내 모든 구성원들이 보안 패러다임 전환 및 제로트러스트 도입의 필요성 및 개념을 이해할 필요가 있다는 것과 함께, 기관·기업내 보안전략 수립 또는 의사 결정이 비전문가인 정책 수립자, 기관장 또는 기업 경영진이 최종 결정하는 경우가 많다는 점을 함께 고려한 것이다.

본 서의 핵심 내용은 미국 국가표준기술연구소(NIST)의 “제로트러스트 아키텍처(NIST SP 800-207)”에 기반을 두고 있지만, 최대한 국내 연구자들의 경험과 지식을 녹여내려고 노력하였으며, 제로트러스트 도입 참조 모델에 제시한 네트워크 구조 등은 국내 현실을 최대한 반영하였다. 특히 유럽, 중국, 일본 등도 제로트러스트 도입을 서두르고 있지만 미국의 추진상황을 많이 고려하고 있음을 비추어 보면 NIST의 “제로트러스트 아키텍처”를 기반으로 정리한 것은 타당하다고 할 수 있을 것이다.

올해 하반기에 과학기술정보통신부와 KISA는 국내 기업 업무환경을 위한 제로트러스트 실증 시범 사업을 추진한다. 기업, 공공기관 등 다양한 환경에 제로트러스트 관련 기술을 실제 적용해보고 검증해봄으로써 국내 환경에 적합한 제로트러스트 모델이 도출될 수 있을 것으로 기대하고 있다. 또한 각 기업들은 이런 실증 사업을 통해서 국내 보안 솔루션 기업간 협력과 경쟁을 기반으로 실질적인 사례를 차근차근 축적함으로써 기술발전의 기회를 마련하고, 향후 해외 시장 진출을 위한 경쟁력을 확보할 수 있을 것이다.

본 서의 세부 내용에 대해 국내 전문가들의 많은 이견이 있을 수 있다. 제로트러스트라는 새로운 보안 개념을 국내에 도입하기 위한 첫 삽을 뜨는 과정이라 생각하며, 국내 전문가들의 고견을 겸허히 수용하고, 실증사업을 통해 도출된 결과를 반영하여 좋은 자료가 될 수 있도록 계속 발전시켜 나갈 계획이다. 끝까지 읽어주셔서 고맙고, 더 좋은 가이드라인이 될 수 있도록 더 많은 관심과 고언을 부탁드린다.

제로트러스트 가이드라인 1.0

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

한국제로트러스트포럼