제로트러스트 가이드라인 1.0

2023. 6

과학기술정보통신부 Ministry of Science and ICT

KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

한국제로트러스트포럼

제로트러스트 가이드라인 1.0

2023. 6

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

제로트러스트 도입 가이드라인 구성과 특징

1. 목적 및 필요성

2021년 5월, 미국의 바이든 행정부는 “국가 사이버 보안 개선을 위한 행정 명령(Executive Order 14028 – Improving the Nation’s Cybersecurity)”을 내린다. 이는 최근 급등하는 대규모 사이버 공격 사례에 대응하기 위하여 국가의 사이버 보안 기능을 강화할 필요성이 있었기 때문이며, 특히 주목할 만한 내용은 연방 정부의 사이버 보안을 현대화하기 위하여 제로트러스트 아키텍처의 도입을 포함하고 있다는 점이다.

이처럼 제로트러스트는 단순히 사이버 보안을 위한 추상적인 개념이나 선언이 아닌, 기업망과 정부·공공망을 위해 반드시 도입해야 하는 새로운 보안 패러다임이자 구조이다. 기업망과 정부·공공망에서는 기존과 비교하여 모바일, IoT, 클라우드 등 새로운 기술의 등장으로 네트워크가 복잡해지고, 코로나19 팬데믹으로 인한 근무 환경의 변화 등 업무 환경에서의 경계가 계속해서 허물어지고 있다. 이러한 변화 속에서, 제로트러스트는 ‘절대 신뢰하지 말고, 항상 검증하라’는 철학에 따라 전통적인 경계 기반 보안(Perimeter Security)을 대체하는 것을 목표로 한다.

제로트러스트는 이를 위하여 네트워크 위치에 관계없이 리소스에 접근하고자하는 모든 요청에 대하여 지속적인 인증을 수행하고, 최소한의 권한부여 및 세밀한 접근제어를 수행하는 보안 활동을 포괄한다. 미국 정부 뿐만 아니라, 일본, 영국 등 세계 각국의 정부, 그리고 수많은 기업에서 제로트러스트 기반의 보안 체계를 도입하고자 하는 움직임을 보이고 있으며, 그에 발맞추어 글로벌 보안 기업들을 중심으로 제로트러스트 보안 솔루션을 출시하고 있다.

그럼에도 정부와 기업 등이 보유하고 있는 네트워크 구조, 기 도입되어 있는 보안 방식 등 환경이 각기 다를 뿐만 아니라, 네트워크 및 보안 관리자들이 제로트러스트 도입·적용하기 위하여 어떤 과정을 거쳐야 하는지를 파악하는 것은 쉽지 않다.

제로트러스트는 특정한 제품군이나 솔루션을 의미하는 것이 아니라 보안 패러다임의 변화를 의미한다. 미 국방부에서는 기업·기관 등 전체 조직 차원에서 공통된 이해를 바탕으로 제로트러스트 철학을 도입이 필요함을 강조하고 있다. 이를 위해 국방부가 보편적으로 이해·수용할 수 있는 제로트러스트 프레임워크로 사이버 보안 정책을 전환하고자 하며, 전문가 핵심 그룹을 개발하는 등 단순한 기술 도입이 아닌 문화적 채택을 첫 번째 목표로 삼고 있다. 이는 미 국방부 뿐만 아니라 제로트러스트를 새로운 보안 패러다임으로 받아들이고자 하는 모든 조직에 해당된다고 볼 수 있다.

특정 보안 제품이나 솔루션들에 대하여 제로트러스트 보안 솔루션이냐 아니냐를 이분법적으로 판단하기에 어려울 뿐만 아니라, 기업망의 보안 솔루션을 모두 교체한다면 도입 비용도 상당히 클 수밖에 없다. 기업망에

기 도입된 혹은 새로 도입하는 모든 보안 솔루션에 제로트러스트의 철학이 담겨 있어야 한다. 각 개별 솔루션들은 유기적으로 협업하여 기업망의 정상적인 사용자에게 지속적으로 인증함으로써 신뢰를 부여하고, 기업 리소스에 대한 접근을 세밀하게 관리함으로써 제로트러스트의 철학이 실천되어야 한다.

본 가이드라인은 이러한 어려움을 고려하여, 제로트러스트 아키텍처의 도입을 검토하고 있는 정부와 지자체, 기업 등의 보안 전략수립 책임자 및 실무자에게 필요한 정보를 제공하는 것을 그 목적으로 한다. 이를 위하여 제로트러스트의 기본 개념 및 원리, 아키텍처 보안 모델 등을 정의하고, 도입 절차와 구현 유스케이스를 상위 수준에서 기술함으로써 각 환경에 적합한 도입 로드맵과 전략을 구성하는데 도움이 되도록 한다.

차후 본 가이드라인을 기반으로, 제로트러스트 도입을 위한 성숙도 수준 평가 모델과 함께, 정부와 지자체, 기업 등 다양한 환경에서의 제로트러스트 아키텍처 도입·전환 시나리오, 지침, 실증 전략 및 로드맵 등 보다 구체적이며 기술적 내용을 포괄하는 문서를 개발할 수 있을 것이다.

2. 문서 구조와 기술 범위

이러한 목적을 달성하기 위하여 본 문서는 다음과 같은 구조를 갖는다.

먼저, 1장에서는 제로트러스트에 대한 소개를 다루고자 한다. 즉, 제로트러스트의 기본 개념 및 역사, 기존 경계 기반 보안 모델의 한계와 제로트러스트 도입의 필요성, 기대 효과 등을 다루며, 제로트러스트 기본 원리 등을 다루게 된다.

2장은 제로트러스트 아키텍처 보안 모델에 대한 내용을 포함하며, 이를 위하여 제로트러스트 아키텍처와 보안 모델을 제안하고, 세부 구성 요소에 대한 구체적인 설명을 포함한다.

3장은 제로트러스트 도입 절차를 다룬다. 먼저 제로트러스트 성숙도 모델을 제안함으로써 이에 따라 제로트러스트 환경을 도입할 때 고려할 수 있는 각 구성 요소들의 성숙도 수준을 정리한 후, 제로트러스트 솔루션을 도입하는데 있어 고려해야 할 점, 그리고 도입 단계, 도입·운영 시 주의사항 등을 언급한다.

마지막으로, 4장은 제로트러스트 구현 유스케이스에 관한 것으로, 현재 업무 네트워크 환경에 제로트러스트를 도입·적용하는 경우에 대하여, 새로운 네트워크 보안 인프라를 구축하는 경우와 기존 레거시 네트워크 보안 인프라를 제로트러스트 기반 보안 인프라로 전환하는 경우 필요한 시나리오와 요구 사항, 절차 등을 다루고자 한다.

제로트러스트
가이드라인 1.0

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 보안 모델의 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 환경변화와 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 실현계획」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

제로트러스트
가이드라인 1.0

ZERO TRUST

제1장

제로트러스트 개요

제1절 | 제로트러스트란?

1. 제로트러스트의 등장

제로트러스트(Zero Trust)는 '신뢰할 수 있는 네트워크'라는 개념 자체를 배제하며, 기업망[1] 내외부에 언제나 공격자가 존재할 수 있고, 명확한 인증 과정을 거치기 전까지는 모든 사용자, 기기 및 네트워크 트래픽을 신뢰하지 않으며, 인증 후에도 끊임없이 신뢰성을 검증함으로써 기업의 정보 자산을 보호할 수 있는 보안 모델을 의미한다. '절대 신뢰하지 말고, 항상 검증하라(Never Trust, Always Verify)'[2]라는 문구로 대표되는 제로트러스트 보안 모델은 전통적인 사이버 보안 접근방식인 경계 기반 보안(Perimeter Security)으로는 업무 환경의 변화와 진화하는 공격에 대응할 수 없어 등장하게 되었다.

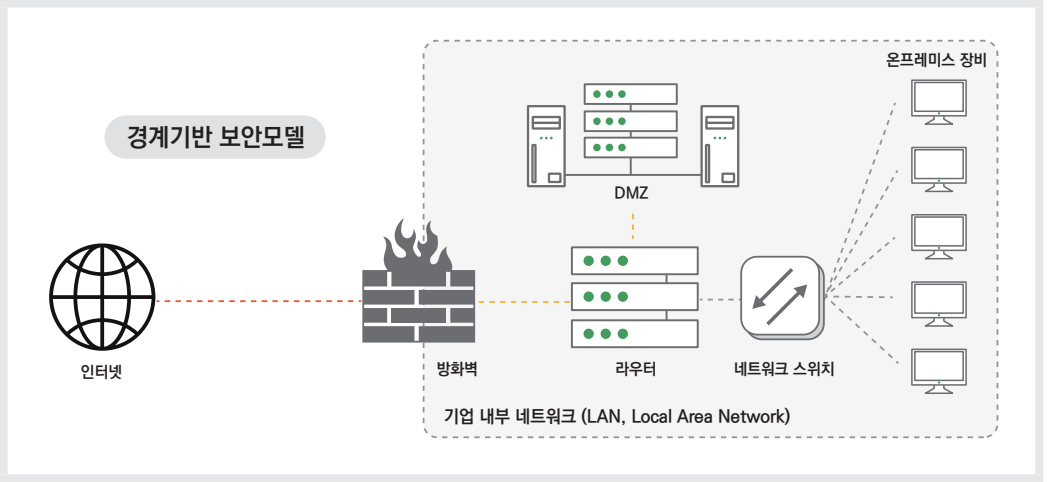
업무 환경의 변화는, 기업에서 생산성을 유지하기 위하여 구축하고 있는 기업망 환경이 기술의 발전에 따라 급속도로 변화하고 있음을 의미한다. 전통적으로 기업은 업무를 위한 기업망을 두고, 이 기업망은 인터넷과 같은 외부망과 연동을 하되 그 경계선에서 방화벽, 침입탐지시스템 등의 보안 솔루션을 통하여 침입이나 해킹 공격에 대응하는 경계 기반 보안 방식을 채택하는 것이 일반적이었다. 기존 기업망 환경의 경우 기업망과 외부망으로 구분되는 구조가 단순하고 경계가 명확했기 때문에, 경계 기반의 전통적인 방식은 상당수의 공격에 대응하기에 매우 효과적이었다.

---

1 본 문서에서의 '기업망'은 'Enterprise Network'을 한국어로 번역하여 사용하고 있는 단어이나, 일반적으로 'Enterprise Network'은 중·대규모 조직에서 사용자와 장치, 응용 프로그램 간 연결을 제공하는 IT 인프라 및 네트워크 시스템을 의미한다. 제로트러스트 보안 철학이 적용되어야 할 중·대규모 조직은 기업 뿐만 아니라 정부나 지자체, 공공기관 등 역시 해당되므로. 본 문서내에서 기업망으로 표현되어 있다 하더라도, 명시적으로 기업에서 운용하는 망을 의미하는 것이 아니라면, 정부나 지자체, 공공기관 등에서 운용하는 네트워크 및 정보시스템을 모두 포괄하는 것으로 이해하는 것이 바람직하다.

2 러시아 속담인 "Trust, but Verify (Доверяй, но проверяй)"에서 온 표현으로, 해당 속담은 1980년대 학자 수잔 매시(Suzanne Massie)가 미국 대통령인 로널드 레이건(Ronald Reagan)에게 러시아인들이 속담을 활용하는 것을 좋아하므로 배울 것을 권한 표현이며, 차후 레이건 대통령은 소비에트 연방과의 관계에 대해 토론할 때 이 속담을 자주 인용하였다.

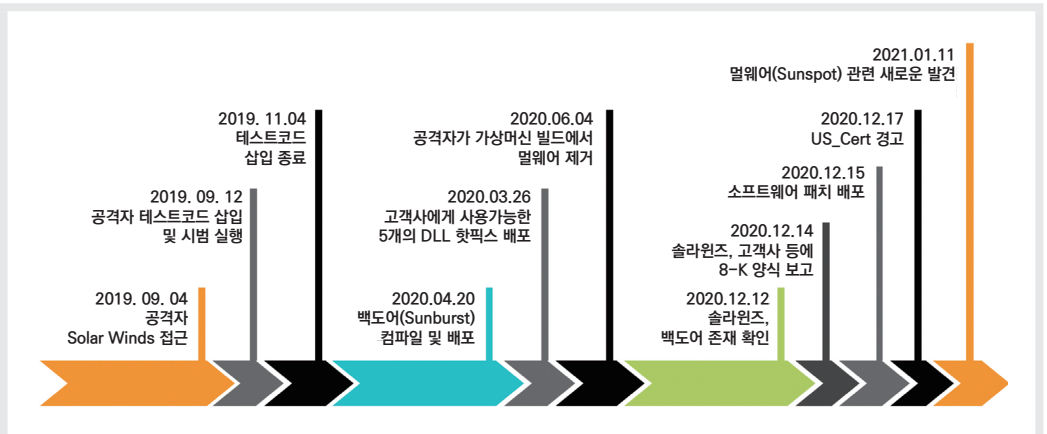
[그림 1-1-1] 경계 기반 보안 모델



(출처: digital.com)

그러나 최근 벌어지는 수많은 해킹 및 랜섬웨어 공격 사례는 경계기반 보안 방식의 한계점을 보여주고 있다. 2020년 솔라윈즈(SolarWinds) 공급망 해킹 사례의 경우, 해커들은 솔라윈즈가 공급하는 오리온(Orion) 업데이트 서버를 공략하여, 악성코드가 고객사에게 배포되도록 함으로써 대략 18,000개의 고객사로 침투할 수 있는 경로를 만든 후 중요 정보를 유출하는 등 피해를 양산하였다. 2021년 콜로니얼 파이프라인, 솔 오리엔스 등은 랜섬웨어 공격을 당했는데, 이는 해킹으로 인한 피해가 기업 내부에 머무르지 않고 사회 경제에 악영향을 미치거나 생명, 국가 안보를 위협하는 사례를 보여준다.

[그림 1-1-2] 솔라윈즈 공급망 해킹



(출처: 솔라윈즈)

이러한 해킹 사례를 살펴보면, 해커들은 공격 과정에서 일차적으로 피싱과 같은 사회적 공격이나 크리덴셜 스터핑, VPN 취약점 등을 통해 내부 침투를 시도하고 있다. 기업망 외부에서 직접 중요 시스템에 접근하는 것은 쉽지 않다. 그러나, 내부 침투에 성공한 공격자는 해당 기기를 활용하여 상대적으로 쉽게 중요 시스템에 찾아보고 접근할 수 있다. 즉, 횡적 이동(Lateral Movement)[3]을 통해 기업에 피해를 입힐 수 있는 위험이 존재한다.

공격자가 이러한 방식을 선호하는 것은, 경계 기반 보안 모델에서는 경계 내부에 위치한 기기 혹은 시스템, 즉 내부자에게 상대적으로 높은 신뢰를 주기 때문이다. 보안 관점에서 특정 사람이나 기기에 신뢰를 부여하는 것은 이들의 행위에 취약해질 가능성을 내포하며, 따라서 신뢰를 부여할수록 위험이 증가하게 되므로 매우 신중해야 한다.

또한, 각 국가·지역별 사무실에 대한 기업망 운용으로 인한 다변화된 네트워크 구성, 직원의 재택근무 혹은 출장지 등에서의 원격 접속, 모바일과 클라우드 환경의 도입 등이 이루어지면서 기업망 구조가 점점 복잡해지고 있다. 직원들은 다양한 기기로 위치와 관계없이 자유롭게 기업 내 응용과 데이터에 접근하기를 희망하고 있으며, 기업은 정보 시스템 유지 보수의 어려움, 비용과 유연성 등의 이유로 클라우드 서비스를 도입하여 기업의 중요 디지털 자산을 이전하고 있다. 이 과정에서 기업망 내외부의 경계가 모호해지면서 기존 경계 기반 보안 방식으로 기업망을 보호하는 것이 점점 더 어려워지고 있다.

따라서 이러한 환경에 대응할 수 있는 새로운 보안 모델로서, 제로트러스트가 각광을 받기 시작했다. 제로트러스트 보안 모델에서는 기업망 내외부에 언제나 공격자가 존재할 수 있으며, 기존 기업망에서의 신뢰성이 더 이상 유효하지 않기 때문에 기업 내 자산(데이터 혹은 리소스)에 접근하는 모든 주체에 대해 지속적으로 인증하고, 자산에 대한 위험성을 지속적으로 평가하며, 위험을 완화시킬 수 있는 대책을 포함하고자 한다.

---

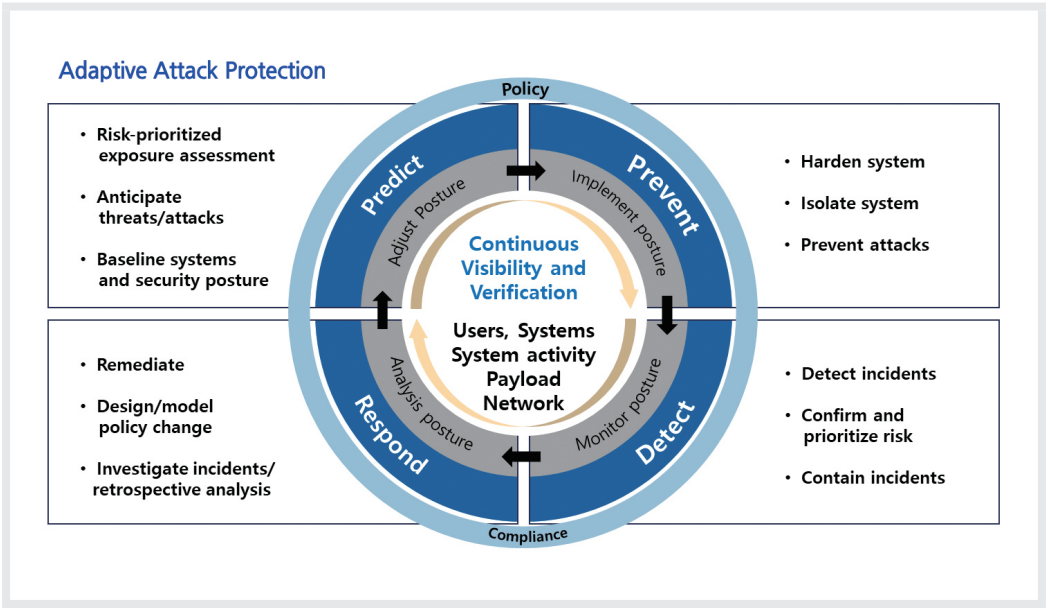
3 횡적 이동이란, 공격자가 초기 접근 권한을 획득한 후, 민감한 데이터나 고가 자산을 찾기 위해 기업망 내부에서 더 깊이 이동하는 것을 의미하며, 공격자는 네트워크에 진입 후 위조한 환경을 통해 이동하고 다양한 툴을 이용하여 상승된 권한을 확보함으로써 지속적으로 접속을 유지한다.

2. 제로트러스트 개념의 발전

현재의 제로트러스트와 유사한 개념은 2000년대 초반 미국 국방부의 글로벌 정보 그리드(Global Information Grid) 네트워크 동작 프레임워크(Network Operations, NetOps)에서 블랙코어(Black Core, BCORE)라는 네트워크 전략을 개발한 바 있으며, 이러한 개념은 소프트웨어 정의 경계(Software-Defined Perimeter, SDP)로 발전하였다. 또한, 비슷한 시기에 산업보안 전문가 그룹인 제리코 프로젝트(Jericho Project)에서 다룬 '탈경계화(De-perimeterization)'를 제로트러스트 개념의 출발로 보는 시각도 있다.

'제로트러스트'라는 용어가 본격적으로 사용되기 시작한 것은, 2010년 Forrester Research 수석 애널리스트 John Kindervag이 기업망에서 더 엄격한 사이버 보안 및 접근제어 방식의 필요성 강조를 위해 2010년 9월과 11월 두 단계에 걸쳐 제로트러스트 네트워크 모델을 제안하면서부터이다. 이와 독립적으로, 구글은 자사 네트워크 보안 방식 및 업무 환경을 개선하기 위해 BeyondCorp이라고 불리우는 제로트러스트 보안 구조를 구현·공개(2014년)한 바 있다.

[그림 1-1-3] Gartner의 CARTA 보안 전략

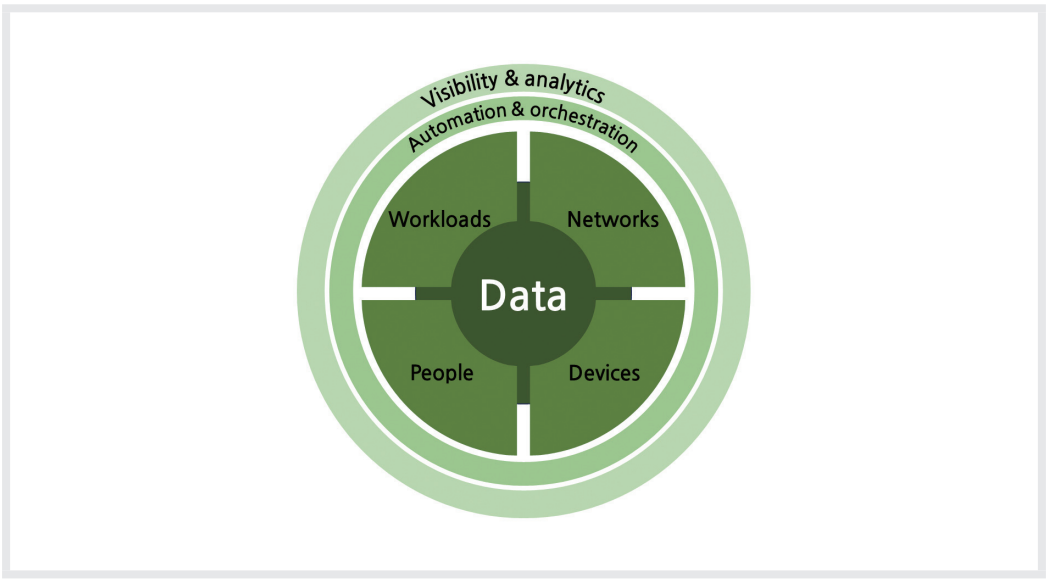


(출처: Gartner)

2017년 Gartner에서는 제로트러스트의 개념을 확장하여, 모든 공격에 대해 예방이 불가능하며, 신속한 탐지 및 대응을 통해 사이버 복원력을 높여 사업 연속성을 제공하기 위한 보안 전략 'CARTA(Continuous Adaptive Risk and Trust Assessment)'를 발표하고, 예측, 예방, 탐지, 대응으로 구성되는 이 전략 모델 중 '예방'에 해당하는 영역을 제로트러스트로 표현하였다.

2018년 Forrester Research는 초창기 데이터 중심의 제로트러스트 전략을 확장한 '제로트러스트 확장 생태계 프레임워크(Zero Trust eXtended Ecosystem Framework)'를 발표하였다. 여기에서는 제로트러스트가 단지 네트워크 분할에 국한되는 개념이 아님을 강조하고, 이 프레임워크에서는 핵심 요소로 데이터, 사용자, 기기, 네트워크와 워크로드를 포함하였으며, 전 영역에 걸쳐 가시성 확보, 자동화 및 통합 운영까지 범위를 확장하였다. 이 프레임워크는 차후 ACT-IAC의 제로트러스트 보안 모델(2019년),[4] CISA의 제로트러스트 성숙도 모델(2021년)[5] 등에 영향을 끼쳤다.

[그림 1-1-4] 제로트러스트 확장 생태계 구성 요소



(출처: Forrester 재구성)

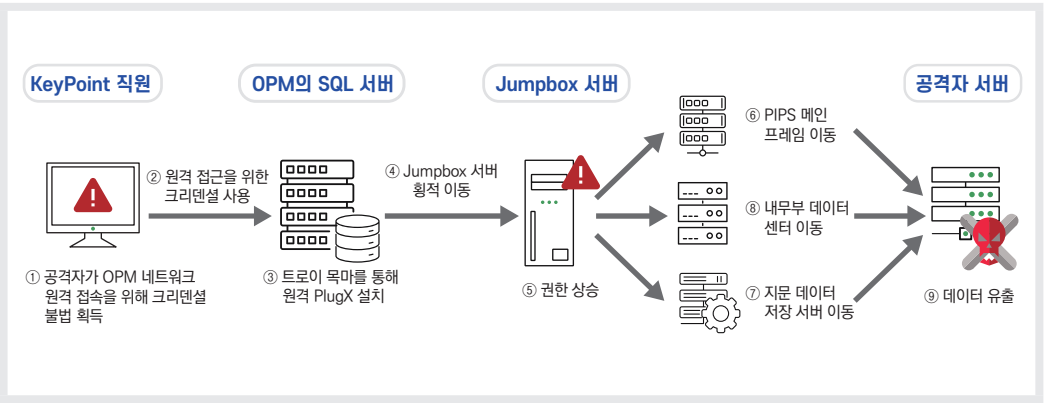
4 ACT-IAC, "Zero Trust Cybersecurity Current Trends" (2019)

5 CISA, "Zero Trust Maturity Model" (2021)

3. 미 연방정부의 제로트러스트 도입

2014년부터 2015년까지 두 차례에 걸쳐, 미국 연방정부의 인사관리처(US Office of Personnel Management, OPM)에서 대량의 개인정보 유출사고가 발생하였다. 미국 역사상 최악의 해킹 사례 중 하나로 기록된 이 사고에서, 대략 2,150만명에 해당하는 전·현직 직원 및 가족의 개인정보가 유출된 것으로 파악되었다. 미 하원 감독개혁위원회(Committee on Oversight and Government Reform)는 2015년 4월부터 2016년 9월까지 약 1년 5개월간의 조사 후 채택한 보고서에서 해킹의 원인과 영향 등을 분석한 후 연방 정부에게 총 13가지 권고안을 내놓았는데, 이 중 두 번째 권고안에서 지능적이고 지속적인 공격에 대응하기 위하여 연방정부의 정보보안 및 IT 아키텍처를 제로트러스트 모델로 이행할 것을 촉구하였다.

[그림 1-1-5] OPM 개인정보 유출사고 해킹 방법



(출처: H. Saleem et al, “Sok: Anatomy of Data Breaches”, PET 2020)

2018년 연방CIO위원회(Federal Chief Information Officers Council)에서는 연방정부차원에서 제로트러스트의 도입을 논의하기 위해 Zero Trust/SDN Steering Group을 설립하였으며, 미국 기술산업자문위원회(American Council for Technology and Industry Advisory Council, ACT-IAC)를 통하여 제로트러스트 기술 동향을 연구하였다. 2019년 연방CIO위원회의 권한 하에 NIST의 NCCoE(National Cybersecurity Center of Excellence)는 제로트러스트 아키텍처 프로젝트를 시작하였으며, 제로트러스트 아키텍처의 논리적 보안 모델 및 구현 방안에 대한 연구를 수행하였다.

2020년 8월, NIST에서는 기업 및 연방 기관의 보안 아키텍처를 위한 '제로트러스트 아키텍처 (Zero Trust Architecture, SP 800-207)'를 발표하고, 제로트러스트 정의, 원칙과 보안 위협, 전환 단계 등을 기술하였다. 2021년 5월 바이든 대통령은 '국가 사이버보안 개선'에 관한 행정 명령을 통하여, 연방 정부가 제로트러스트 모범 사례를 채택해야 하며 이를 위하여 각 정부 기관장들은 NIST의 표준·지침을 따르는 제로트러스트 아키텍처 도입 계획을 60일 이내에 개발하도록 지시하였다.

2021년 6월 CISA는 이러한 대책의 일환으로 각 정부 기관들의 제로트러스트 아키텍처 구현 계획 설계를 지원하기 위한 문서 '제로트러스트 성숙도 모델 (Zero Trust Maturity Model)'를 발간한다. 이 문서는 제로트러스트 구현에 필수적인 5가지 핵심 요소(5 Pillars: 식별자, 기기, 네트워크, 응용 및 워크로드, 데이터)과 3가지 교차 기능(가시성과 분석, 통합과 자동화, 거버넌스), 3단계 성숙도 수준을 정의하였으며, 이후 2023년 4월 성숙도 수준을 4단계로 확장한 버전 2.0 문서도 발표하였다. 2022년 1월 백악관 예산관리실(Office of Management and Budget, OMB)은 각 기관장들에게 회계연도 2024년 말까지에 대한 제로트러스트 보안 목표, 도입 계획 및 예산 추정치 등을 수립하여 제출할 것을 명령하면서, 이 목표는 CISA의 제로트러스트 성숙도 모델과 일치하여야 함을 강조하였다.

NIST NCCoE는 협력 기업들과 함께 현재 상업적으로 이용 가능한 기술을 활용하여 NIST SP 800-207의 개념과 원칙에 부합하는 제로트러스트 아키텍처를 상호운용 가능하고 공개된 표준 기반 방식으로 구현하고 있으며, 이에 대한 구현 접근 방안과 참조 아키텍처 및 구현 진행 결과를 NIST SP 1800-35 시리즈의 형태로 지속적으로 공개하고 있다.

이러한 일련의 노력들을 바탕으로 이해할 수 있는 점은, 미국 연방 정부에서는 최근 급등하는 대규모 사이버 공격 사례에 대응하기 위하여 사이버 보안 기능을 강화하고 현대화하기 위하여, 제로트러스트를 사이버 보안 현대화 전략의 주요 원칙으로 판단하고 있다는 것이다. 위에서 따로 언급하지는 않았지만, 국방부 역시 사용자·자산·리소스에 중점을 둔 사이버 방어체계 구축을 위해 제로트러스트 도입을 적극적으로 노력하고 있다.

이와 관련하여 연방 정부에서 진행한 내용을 〈표 1-1-1〉에 정리하였다.

〈표 1-1-1〉 제로트러스트 관련 미 연방정부 진행 사항

시기	기관	미 연방정부 진행 사항
2019.04	ACT-IAC	제로트러스트 사이버 보안 동향 소개
2020.08	NIST	제로트러스트 아키텍처(SP 800-207) 발간
2021.02	DISA/NSA	국방부 제로트러스트 참조 아키텍처 버전 1.0 발간
2021.02	NSA	제로트러스트 보안 모델 수용 지침 발간
2021.05	바이든 대통령	'국가 사이버 보안 개선을 위한 행정 명령 (EO-14028)' 발표
2021.06	CISA	제로트러스트 성숙도 모델 (Pre-decisional Draft) 발간
2021.06	GSA	제로트러스트 아키텍처 – 구매자 가이드 발간
2021.07	NIST	행정 명령(EO-14028) 관련 주요 소프트웨어에 대한 보안성 관련 지침 발표
2022.01	바이든 대통령	'국가 안보, 국방부 및 정보 공동체 시스템의 사이버 보안 개선에 관한 각서 (NSM-08)' 발표
2022.01	OMB	'제로트러스트 사이버 보안 원칙을 향한 미 연방 정부 전략에 관한 각서' 발표
2022.02	NSTAC	'제로트러스트 및 신뢰할 수 있는 ID 관리' 대통령 보고서 발표
2022.03	CISA	엔터프라이즈 모빌리티에 제로트러스트 원칙 적용 (Draft for Public Comment) 발간
2022.05	NIST	제로트러스트 아키텍처 계획: 연방 관리자를 위한 계획수립 지침 (CSWP 20) 발간
2022.06	법무부	제로트러스트 도입을 포함하는 '2022-2024 회계년도를 위한 미국 법무부 정보기술 전략 계획' 발표
2022.07	DISA/NSA	국방부 제로트러스트 참조 아키텍처 버전 2.0 발표
2022.06~08	NIST	제로트러스트 아키텍처 구현 (SP 1800-35A~D, Preliminary Draft) 발간
2022.11	DoD	국방부 제로트러스트 전략, 기능 실행 로드맵 발표
2022.12	NIST	제로트러스트 아키텍처 구현 (SP 1800-35A~E, 2nd Preliminary Draft) 발간
2023.04	NSA	사용자 핵심요소를 통한 제로트러스트 성숙도 개선
2023.04	CISA	제로트러스트 성숙도 모델 2.0 발간

제2절 | 왜 제로트러스트인가?

1. 경계 기반 보안 모델의 한계

전통적인 기업망의 경우 망의 구조가 비교적 단순하고 경계가 명확했기 때문에 경계 기반 보안 모델을 적용할 경우 상당수의 공격에 효과적으로 대응할 수 있었으며, 비용면에서도 매우 유리하였다. 그러나, 경계 기반 보안 모델의 가장 큰 약점은 내부 접속 사용자나 기기 혹은 내부 트래픽에 대해 단순히 네트워크 위치만으로 (외부 접속자 혹은 기기 등과 비교하여) 높은 수준의 신뢰성을 부여한다는 점에 있었다.

외부에 있는 사용자 혹은 기기가 기업망에 접속하고자 할 경우, 기본적으로 신뢰성이 낮다고 판단하며 사용자에게 가상사설망(Virtual Private Network, VPN) 혹은 데스크톱 가상화(Virtual Desktop Infrastructure, VDI)와 같이 별도의 접속 환경을 구성하고 추가 인증 작업을 거치도록 함으로써 내부 사용자와 유사한 신뢰성을 부여하는 것이 일반적이었다. 다소 불편하기는 하나, 외부 접속이 빈번하지 않은 환경에서는 적절한 방법으로 볼 수 있었다.

그러나, 2020년 전 세계적인 코로나19 팬데믹으로 인하여, 직원들이 비대면 및 원격·재택근무 환경이 확산되면서 이러한 환경에서도 기업망의 보안성을 유지하는 것이 필수가 되었다. 외부에서의 원격 접속을 위해 대다수 기업들은 VPN 망을 활용하였으나, 다수의 직원이 VPN으로 접속함으로써 공격·침해 경로가 늘어나고 VPN 할당량을 초과하는 등 다양한 문제들이 발생하기 시작했다.

또한, 직원들의 원격 접속용 기기가 다양해지고, 직원이 생산·활용하는 데이터, 사내 업무 솔루션 등을 편리하게 접근할 수 있도록 클라우드 서비스의 도입이 늘어나고 있다. 이에 따라, 조직 내 자산과 서비스, 사용자와 접속 기기와 같은 모든 구성 요소들이 조직 내외부에 모두 존재할 수 있는 온프레미스-클라우드 하이브리드 환경으로 계속해서 변화하고 있다. 이러한 변화는, 보안 영역과 비 보안 영역의 경계가 모호해지고 공격 침투 경로가 더욱 복잡해지는 현상을 야기하였다.

직원이 언제 어디서든 접속할 수 있다는 것은, 한편으로는 직원으로부터의 공격 위협 또한 예전보다 커졌음을 의미한다. 직원들이 원격으로 내부 데이터를 접근할 수 있다는 것은, 말 그대로 언제 어디서나 내부자 공격이 가능함을 의미한다.

2010년, John Kindervag는 경계 기반 보안 모델의 위험성에 대해 다음과 같이 정리한 바 있다.

〈표 1-2-1〉 경계 기반 보안 모델의 위험성

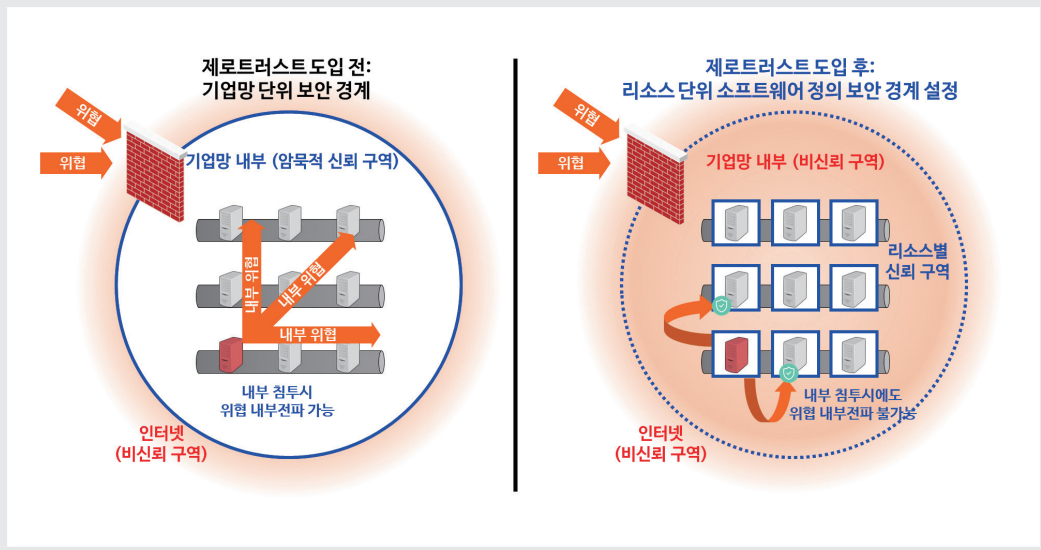
구분	위험	설명
1	'신뢰' 네트워크를 식별하는 것은 불가능하다.	‣ 정보 서비스는 네트워크로 연결되며, 네트워크 상에서 '신뢰할 수 있는 대상'을 구별하는 것은 사실상 불가능하다. ‣ 신뢰할 수 있는 네트워크에서 신뢰할 수 없는 대상을 식별할 수 없다.
2	'신뢰하지만 검증하라'는 문구는 허황된 표현이다.	‣ 신뢰하는 네트워크에 존재하는 실체를 검증하여 신뢰여부를 판단할 수 있다. ‣ 그러나 이미 '신뢰할 수 있는 네트워크'로 가정하기 때문에, 적용되는 검증 방법은 매우 미흡하여 '신뢰할 수 없는 대상으로 판별'하기 어렵다.
3	악의적 내부자들은 때때로 '신뢰'된 위치에 있다.	‣ 신뢰된 주체는 다양한 시스템에 접근할 수 있으며, 다양한 정보를 취급하는 등의 많은 권한을 갖는다. ‣ 신뢰된 주체가 악의적인 계획이 있다면, 그 계획 실행은 매우 쉽다.
4	'신뢰'는 패킷에 적용할 수 없다.	‣ 신뢰할 수 있는 대상은 '주체'이지 '수단'이나 '방법'을 의미하지 않는다. ‣ 네트워크는 표준을 준수하는 기술이므로, 이 기술을 신뢰하거나 불신할 수 없다.

이를 요약하면 3가지 측면에서의 IT 환경 변화가 발생한 것인데, 첫 번째로 직원들이 다양한 단말을 이용하여 장소와 상관없이 기업망에 접속이 가능해졌으며, 두 번째로는 기업 데이터가 기업망에만 존재하는 것이 아니라 클라우드 상에도 존재할 수 있게 되었다. 세 번째로 공격방식이 점차 정교해지고, 내부자 공격 또한 점점 늘어나고 있는 추세다. 이러한 상황에서 기존의 경계 기반 보안 방식은 매우 복잡하고 다변화된 현재의 기업망 환경에서 더는 적합하지 않은 것으로 보인다.

2. 제로트러스트 도입의 필요성

이를 해결하기 위해서는 보안 패러다임이 근본적으로 바뀌어야 하며, 이를 위해 등장한 개념이 바로 제로트러스트이다. 제로트러스트 모델에서는 '신뢰할 수 있는 네트워크'라는 개념 자체를 배제하며, 기업망 내외부에 언제나 공격자가 존재할 수 있고, 모든 사용자, 기기 및 네트워크 트래픽을 신뢰하지 않는다. 네트워크 혹은 물리적 위치, 접속 기기에 상관없이 기본적으로 '비 신뢰'에서 출발하여 강화된 인증 및 기기 상태 모니터링 등을 통하여 계속 검증한 후 신뢰도가 일정 수준을 넘어갈 때, 기업망 혹은 기업 데이터를 접근할 수 있는 권한을 부여하는 것이 제로트러스트의 원칙이 된다.

[그림 1-2-1] 보안 패러다임의 변화



(출처: A.Kerman / NIST, "Zero Trust Cybersecurity:Never Trust, Always Verify"의 그림 재구성)

이러한 모델에서 기업망 보안 담당자의 역할은 분명하다. 모든 내부 리소스의 안전성을 지속적으로 검증, 보호하여야 하며, 기업 리소스에 대한 접근제어를 더욱 세밀하고 엄격하게 시행해야 하고, 기업망·외부망 경계뿐만 아니라 기업망에서 끊임없이 전달되는 모든 네트워크 트래픽을 감시·기록하여야 한다. 기업망·외부망에서 접근하는 모든 사용자와 기기의 신뢰성이 보장되지 않기 때문에, 즉 사용자와 공격자를 구분하는 것이 매우 어렵기 때문에, 사용자 혹은 기기의 접근 경로와 방식, 물리적 위치, 기업망 보안 상태 등에 따라

신뢰도를 평가하고 신뢰도와 리소스의 보안 등급에 따라 접근 여부를 판단하는 구조도 필요하다.

따라서, 기업은 제로트러스트 패러다임에 맞는 보안 기술을 채택함으로써 기업망 및 시스템, 데이터 등 리소스를 보호할 수 있어야 하는데, 이는 사용자와 단말에 대한 지속적인 인증·신뢰도 검증, 마이크로 세그멘테이션(Micro-Segmentation), 소프트웨어 정의 경계(Software-Defined Perimeter, SDP)을 통한 리소스 보호, 지속적인 모니터링 및 가시성을 기반으로 하는 새로운 보안 거버넌스를 요구하게 된다.

예를 들어, 직원이 VPN을 통하여 접속을 허용하면 기업망 경계 내부에서 진입한 것과 동일한 혹은 유사한 수준의 신뢰도를 부여하거나, 망분리를 통하여 물리적으로 업무망에 접속한 사용자와 기기에게 높은 신뢰도를 부여하는 전통적인 모델은 사용자에게 불편을 안겨줄 뿐만 아니라 다변화된 기업망에 더 이상 어울리지 않는다. 인증 시스템, 방화벽과 침입탐지시스템 등 기존 보안 솔루션들은 그 자체로 보안에 도움이 될 수 있으나, 진화된 기능을 포함하거나 혹은 제로트러스트 모델에서 요구하는 새로운 기능을 가지는 보안 솔루션으로 대체될 가능성이 높다.

기업과 정부·공공기관 등에서 제로트러스트 보안 모델을 채택할 경우 진화하는 다양한 형태의 네트워크 환경에 적응하기 적합하며, 물리적 위치에 구애받지 않고 여러 접속 기기를 활용하여 기업 리소스에 접근하고자 하는 사용자에게 불편을 주지 않으면서도 기업망과 기업 리소스의 보안성을 유지할 수 있는 효과를 가질 것으로 보인다.

3. 제로트러스트 도입 시 기대할 수 있는 개선 사항 (침해대응 시나리오)

제로트러스트의 기본 목적은 사용자와 기기, 처리 과정이 데이터와 어떻게 연관되어 있는지를 이해하고 제어하는 데 있다. 다음은 NSA에서 발간한 “Embracing a Zero Trust Security Model” 문서에서 언급한 내용으로, 제로트러스트 구현이 성숙된 상태에서 악의적인 공격에 대해 기존 보안 아키텍처 대비 기대할 수 있는 개선 사항을 담은 몇 가지 시나리오이다.

공격자의 기기로 사용자의 자격증명만을 도용하는 시나리오부터, 정상 사용자의 기기를

도용하거나 내부 사용자가 직접 공격하는 시나리오, 그리고 공급망을 침투함으로써 정상 기기의 프로그램까지 침투하는 시나리오까지 간단히 다룸으로써, 제로트러스트를 도입할 경우 기존 경계 기반 보안 모델 대비 어떤 효과를 기대할 수 있는지 간단히 살펴본다.

- 사용자 자격증명 도용
- 원격 공격 혹은 내부자 위협
- 공급망 침투

〈표 1-2-2〉 시나리오별 제로트러스트 도입시 효과

시나리오	경계 기반 보안 모델의 한계	제로트러스트 보안 모델의 대응 시나리오
사용자 자격증명 도용	‣ 일반적으로 사용자 자격 증명이 위조될 경우, 기기와 관계없이 기업망 내부 리소스 접근할 수 있어 피해 발생 ‣ 기업 외부 접속 시 강화된 다중 인증 등 인증 환경을 강화함으로써 일부 대응 가능	‣ 위장 기기인 경우, 접근 권한이 부여되지 않고 해당 정보에 대한 로그 및 모니터링 ‣ 정상적인 자격 증명 후에도 신뢰도가 충분하지 않은 이벤트 발생 시 강화된 다중 인증 적용을 통한 대응
원격 공격 혹은 내부자 위협	‣ 네트워크에 접속, 권한 상승 후 횡적 이동을 통해 다양한 리소스에 접근하거나 손상시키는 등 피해를 줄 수 있음	‣ 네트워크는 마이크로 세그멘테이션 되어 관리되므로, 공격자의 횡적 이동이 쉽지 않음 ‣ 데이터 접근은 보안 정책, 사용자 역할, 기기 속성 등에 따라 제한되며, 세밀한 접근제어를 통해 민감한 데이터 접근 불가 ‣ 사용자 행위에 대한 모니터링을 통해 비정상적인 활동시 추가 인증 요구 혹은 동적인 접근 제한 가능
공급망 침투	‣ 해당 접속에 대해 신뢰성이 부여되어, 이후 벌어지는 대다수 공격에 대한 대응 불가	‣ 정상적인 기기에 정상적으로 배포된 프로그램이라 하더라도 일단 신뢰하지 않으므로, 데이터 접근은 최소화로 이루어져 피해를 최소화할 수 있음 ‣ 모든 네트워크 연결이 감시되므로, 허가받지 않은 원격 접속을 통한 공격 명령/통제 및 데이터 전송 역시 대응 가능

가. 사용자 자격증명 도용 (Compromised user credentials)

이 시나리오에서는, 악의적인 공격자가 정당한 사용자의 자격 증명을 위조하여 기업 내 리소스에 접근하고자 한다. 이 경우, 악의적인 공격자는 원격으로 혹은 기업 내 무선랜에 접속하는 위장 기기와 같이, 허가받지 않은 기기를 사용하고 있다고 가정한다.

기존 기업망 환경에서는 일반적으로 사용자의 자격 증명만 위조할 수 있다면 기업망 내부의 리소스에 대한 접근 권한이 부여되는 것이 일반적이다. 그러나 제로트러스트 환경에서는 접속 기기 역시 신뢰를 확인하기 위한 대상이기에, 위장 기기인 경우에는 접근 권한이 부여되지 않고 해당 정보에 대한 로그 및 모니터링이 이루어지게 될 것이다.

또한 제로트러스트에서는 일반적으로 사용자 및 기기에 대한 강력한 인증을 요구하며, 활동을 종합적으로 분석하여 정상적인 자격 증명 후에도 신뢰가 충분하지 않을 경우 강화된 다중 인증을 요구할 수 있다. 예를 들어, 갑작스럽게 접속 기기의 물리적 위치가 변경되었거나 평상시 접속하지 않는 기기를 이용하여 접속한 경우, 혹은 권한이 없는 리소스에 지속적으로 접근하고자 하는 등 정상적인 경우라고 판단하기 어렵거나 모호한 경우, 해당 접속한 사용자에 대한 신뢰도가 충분하지 않다고 볼 수 있을 것이다.

공격자가 다중 인증까지 검증을 통과하기에는 훨씬 어려울 수 있으므로, 기존 기업망 환경과 비교하여 안전성이 높아지게 될 것이다.

나. 원격 공격 혹은 내부자 위협 (Remote exploitation or insider threat)

이 시나리오에서는 악의적인 공격자가 인터넷 기반 악성 코드를 이용하여 사용자 기기를 가로채거나 혹은 공격자가 악의적인 의도를 가진 내부자인 경우이다.

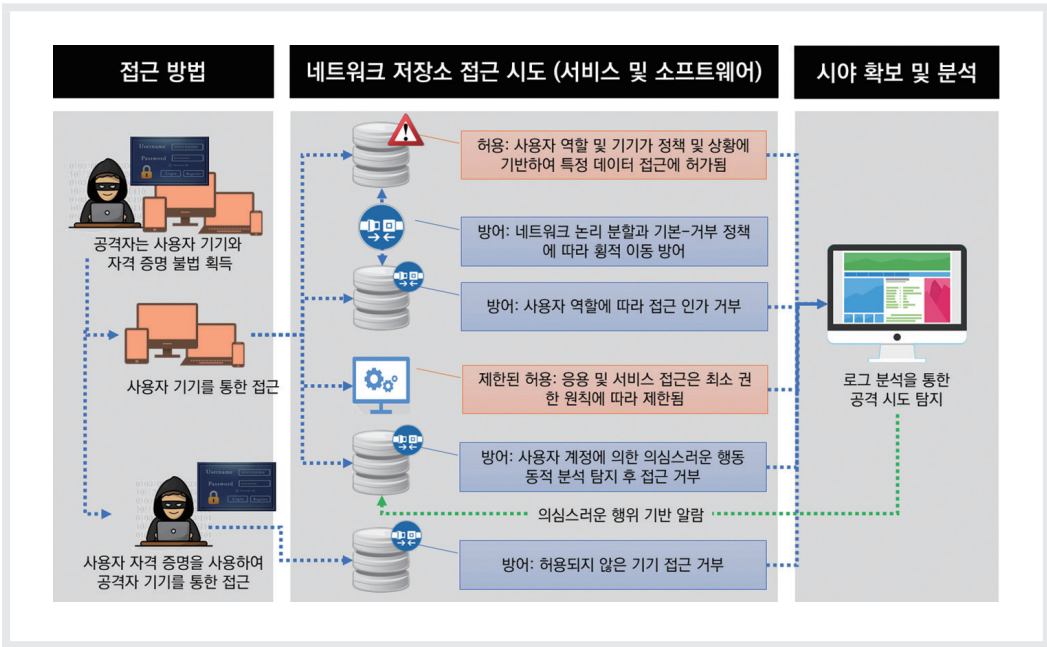
기존 기업망 환경에서 이러한 악의적인 공격자는 정상 사용자의 자격 증명을 불법 이용한 네트워크 접속, 권한 상승, 횡적 이동을 통하여 방대한 데이터 저장소를 손상시키는 행위를 지속할 수 있다.

그러나 제로트러스트 환경에서는 위조된 사용자의 자격 증명과 기기 역시 정상적인 것으로 입증되기 전까지는 의심스럽다고 가정하기 때문에, 네트워크는 논리적으로 분할(마이크로 세그멘테이션)되어 횡적 이동이 불가능해진다. 물론, 악의적인 공격자가 사용자 자격 증명 및 기기 인증 모두 통과할 수 있으나 데이터에 대한 접근은 보안 정책, 사용자 역할, 기기 속성 등에 따라 제한되게 되고, 세밀한 접근제어를 하게 되므로 민감한 데이터로 작업하는 것이 어렵게 될 것이다.

또한, 사용자 행위에 대한 지속적인 로그와 모니터링을 통한 분석을 함으로써, 사용자

계정과 기기의 네트워크 활동 및 데이터 접근이 비정상적인 것으로 판단될 경우 추가 인증을 요구하거나 동적으로 접근을 제한하는 것도 가능하다. 따라서, 이 시나리오에서는 부득이하게 일부 피해가 발생할 수 있지만 피해를 받는 리소스 범위가 줄어들며 보안 시스템이 이 공격을 적절하게 완화시킬 수 있는 신속한 대응이 가능해질 것이다.

[그림 1-2-2] 제로트러스트 상에서의 원격 공격 시나리오



(출처: NSA, “Embracing a Zero Trust Security Model”)

다. 공급망 침투 (Compromised supply chain)

이 시나리오에서는, 악의적인 공격자는 기업망에 있는 기기나 응용 프로그램에 악성 코드를 삽입한다. 기기 혹은 응용 프로그램은 기존 모범 사례에 따라 조직 네트워크 내부에서 유지 관리되고 정기적으로 업데이트가 될 것이다. 기존 기업망 환경에서는 정상적인 사용자가 이렇게 업데이트되어 악성 코드가 삽입된 기기 혹은 응용 프로그램을 통해 기업 리소스에 접근할 경우, 잠재적으로 신뢰할 가능성이 크므로 이러한 공격은 특히 심각하다.

그러나 제로트러스트 아키텍처를 높은 수준으로 구현하는 경우, 기기 혹은 응용 프로그램에 대해 기본적으로 신뢰하지 않는 것으로 판단하기 때문에, 공격에 대한 방어 측면에서 유리한

점이 있다. 데이터에 대한 접근 권한 및 실제 접근은 엄격히 제어되고 최소한으로 주어지며 모니터링 된다. 정책적으로 네트워크 분리가 적용되며, 비정상적인 활동에 대한 모니터링을 위한 분석 작업도 활용될 것이다.

기기가 서명된 응용 프로그램 업데이트를 다운로드할 수 있으나, 제로트러스트 환경에서는 기기의 네트워크 연결을 기본적으로 거부하는 보안 정책을 채택하므로, 명령과 통제를 위하여 다른 원격 주소에 연결하려는 모든 시도는 차단될 가능성이 높다. 그 외에도, 허가된 접근이 아닌 다른 기업 리소스 접근 요청은 해당 기기에 대한 모니터링 과정을 통해 감지 및 차단될 것이다.

제3절 | 제로트러스트 아키텍처 기본 원리

기업이 제로트러스트 보안 모델을 채택하는 경우, 기업망 관리자는 접근제어를 가능한 세밀하게 하여, 데이터 및 기업 자산에 대한 허가되지 않은 접근을 방지하는 것을 포함하는 기본 원리에 따라야 한다. 이를 위해, 본 가이드라인에서 제로트러스트를 정의하고, 제로트러스트의 기본 원리가 무엇인지 정의한다.

1. 제로트러스트 정의 및 개념 모델

앞서 언급한 제로트러스트의 배경과 개념의 발전 과정, 기존 문서들의 정의들을 참고하여 본 문서에서 정의하는 제로트러스트 및 제로트러스트 아키텍처의 정의는 다음과 같다.

제로트러스트는 위협이 언제 어디서든 발생 가능하다는 인식하에 기업 내부의 네트워크, 시스템 혹은 리소스에 접근하고자 하는 어떤 사용자·기기에 대해서도 지속적인 인증, 세밀한 접근제어를 통한 최소 권한 부여 등 적극적인 신뢰도 평가 없이 접근을 허용하지 않는 보안 모델 및 이를 구현·실체화하기 위한 아이디어의 집합을 의미한다.

제로트러스트 아키텍처란, 제로트러스트의 개념을 활용하여 기업 내부의 네트워크, 시스템 및 리소스를 보호할 수 있는 추상적인 보안 구조이며 해당 목적을 달성하기 위한 기업망의 구성 요소, 구성 요소 간 인터페이스 정의와 인증, 접근제어, 보안 모니터링 및 가시화 등 보안 정책을 포함한다.

〈표 1-3-1〉 참고: 기존 문서에서 정의한 제로트러스트 및 제로트러스트 아키텍처

문서	정의 혹은 개념
NIST SP 800-207, 'Zero Trust Architecture'	▸ 제로트러스트는 정적·네트워크 기반 경계로부터 사용자·자산·리소스에 중점을 둔 방어로 이동 및 진화하는 사이버 보안 패러다임의 집합을 나타내는 용어이다. (Abstract)[6] ▸ 제로트러스트란, 네트워크가 이미 침투당했다는 관점에서 정보 시스템 및 서비스에서 '정확한', '최소 권한의', '요청 단위 접근 결정'을 강제하여 불확실성을 최소화하기 위해 설계된 개념과 아이디어 모음이다. (2장)
	▸ 제로트러스트 아키텍처란, 제로트러스트 개념을 사용한 기업 사이버 보안 계획이며 컴포넌트 간 관계, 워크플로우 설계, 접근 정책이 포함된다.
CSA, 'Software Defined Perimeter (SDP) and Zero Trust'	▸ 제로트러스트는 조직이 기존 경계 내부 혹은 외부의 어떤 것도 신뢰해서는 안 된다는 믿음을 중심으로 하는 네트워크 보안 개념으로, 기업 자산을 보호하는 것을 목표로 한다.
NSA, 'Embracing a Zero Trust Security Model'	▸ 제로트러스트는 위협이 전통적인 네트워크 경계의 내외부 모두에 존재한다는 인식에 기반한 보안 모델, 시스템 설계 원칙과 조직화된 사이버 보안 및 시스템 관리 전략이다.
Gartner, 'Predicts 2023: Zero Trust Moves Past Marketing Hype Into Reality'	▸ 제로트러스트는 위험 관점의 최적화를 위해, 조직의 보안 태세를 암묵적 신뢰 대신 보안 인프라에서 지원하는 ID 및 컨텍스트를 기반으로 지속적으로 명시적 위험 및 신뢰 수준을 평가하는 보안 패러다임이다.

NIST SP 800-207에서는 제로트러스트 관점에서의 접근(Access)에 대해 [그림 1-3-1]와 같은 개념 모델을 제시하였다. 이 그림에서 승인된 접근 주체[7]는 기업 내 데이터 및 리소스[8]에 접근할 필요가 있을 수 있는데, 이 때 정책결정지점(PDP) 및 정책시행지점(PEP)[9]을 통해 승인이 이루어지게 된다.

여기에서 불확실성을 줄이기 위해서 인증·인가 및 절대적 신뢰 구역 축소에 초점을 맞춘다. 가용성을 위해서는 인증 방식의 지연 시간을 최소화하면서 필요한 권한을 최소화하기 위하여 접근 규칙을 가능한 한 세밀하게 만들어야 한다.

---

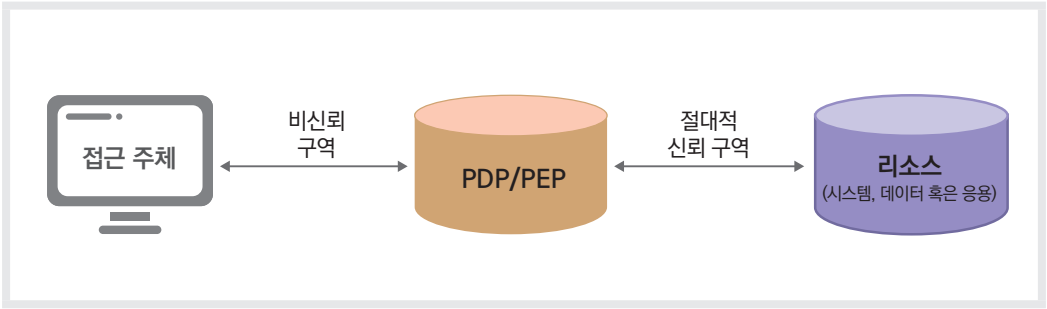
6 미 국방부에서 발간한 제로트러스트 관련 문서들의 경우, 이 정의를 채택하여 사용하고 있다.

7 승인된 접근 주체(subjects)는 사용자와 응용(혹은 서비스), 기기의 조합이며, 그 외의 주체는 공격자일 수 있다.

8 리소스는 데이터를 포함하는 개념으로, 프린터, 컴퓨팅 리소스, IoT 액추에이터 등 기업망 내부의 자산을 모두 포함한다.

9 PDP와 PEP로 이루어지는 접근제어의 개념은 OASIS XACML 2.0에 정의되어 있다. 이 문서에서 PDP, PEP의 정의는 IETF RFC 3198(Terminology for Policy-Based Management)에서 내린 정의를 따르며, 다음과 같다.
- PDP(Policy Decision Point): 정책 결정을 요청하는 (자신의 혹은 외부) 네트워크 요소를 위해 정책 결정을 내리는 논리 개체
- PEP(Policy Enforcement Point): 정책 결정을 강제하는 논리 개체
이 문서에서의 정책 결정은 2가지 관점이 존재하는데, 첫 번째는 정책 룰의 조건에 따르는 평가를 다루는 "절차" 관점이며, 두 번째는 정책 룰의 조건이 '참'일 때 강제하는 조치를 다루는 "결과" 관점이다.

[그림 1-3-1] 제로트러스트 접근의 개념 모델



전체 정보 시스템은 접근 주체가 인증되었고, 접근 요청이 유효함을 보증할 수 있어야 한다. PDP과 PEP는 주체가 리소스에 접근할 수 있도록 적절하게 판단하며, 이것은 제로트러스트가 '인증'과 '인가' 2가지 기본 영역에 적용됨을 의미한다.

- 현재 요청한 접근 주체의 신원에 대한 신뢰도는 어느 정도인가?
- 접근 주체의 신원에 대한 현재 신뢰도 수준에서, 리소스 접근이 허용 가능한가?
- 요청 기기의 보안 상태는 적절한가?
- 신뢰도를 변경하는 다른 고려 요인이 있는가? (예, 접속 시간, 접근 주체의 물리적 위치, 보안 상태 등)

전체적으로 기업은 리소스 접근에 대한 동적 위험 기반 정책을 개발 및 유지 관리하고 이 정책이 개별 리소스 접근 요청에 대해 정확하고 일관되게 시행되도록 시스템을 설정해야 한다. 즉, 접근 주체가 기본 인증 수준(예, 로그인)을 충족할 경우, 이후의 리소스 요청들을 모두 유효한 것으로 간주하는 절대적 신뢰성에 의존하지 말아야 함을 의미한다.

[그림 1-3-1]에서 절대적 신뢰 구역은 모든 접근 주체가 신뢰되는 구역을 나타낸다. 예를 들어, 공항에서 승객은 탑승 게이트로 접근하기 위해 공항 보안 검색대(PDP/PEP)를 통과하며, 터미널 내에 있는 승객과 공항 직원, 승무원은 모두 신뢰할 수 있는 것으로 간주된다. 공항에서는 절대적 신뢰 구역이 바로 탑승 구역인 것이다.

PDP과 PEP은 PEP를 거쳐간 모든 트래픽이 공통 수준의 신뢰를 갖도록 제어한다. PEP를 거쳐간 트래픽에 대해서는 더 이상의 정책을 적용할 수 없으므로, 구체적인 정책을 적용할

수 있도록, 절대적 신뢰 영역이 가능한 한 작아야 한다. 제로트러스트는 PDP와 PDP가 리소스에 더 가까워지는 것에 관한 일련의 원칙과 개념을 제공하여야 하는데, 여기에서의 핵심 아이디어는 기업을 구성하는 모든 주체, 자산과 워크플로우를 명시적으로 인증하고 인가하는 것이다.

이러한 기본 원칙에 따라서, 제로트러스트의 철학은 경계 기반 보안이 현재의 일반적인 기업망 환경에 적합하지 않다는 것을 전제한다. 이는 제로트러스트의 보안 철학이 경계를 기반으로 하는 모든 보안 방식을 거부한다는 의미가 아니며, 기업망을 신뢰할 수 있는 영역, 외부망을 신뢰할 수 없는 영역으로 구분하는 이분법적 방식의 보안을 거부하는 것을 의미한다. 즉, 기존에 경계기반 보안 기술로 많이 활용되어온 망분리, VPN, 방화벽, 침입탐지시스템 등을 무조건 배제하여야 한다고 이해하는 것은 바람직하지 않다. 제로트러스트에서는 오히려 접근제어를 더욱 세분화·세밀화 함으로써 불확실성을 최소화하고자 하는데, 이 경우 접근 주체와 리소스에 따라 세밀한 경계(Micro-segmentation 혹은 Micro-perimeter)를 설정하여야 한다.

2. 제로트러스트 아키텍처 기본 원리

제로트러스트 아키텍처를 통해 달성하고자 하는 목표는, 정보보호의 기본 원칙과 다를 바가 없을 것이다. 정상적인 사용자는 원하는 서비스를 안전하게 제공받을 수 있어야 하며, 기업망 관리자는 기업 리소스 등 기업의 가치 있는 자산이 공격자로부터 탈취당하지 않아야 한다. 달성 목표는 이전과 크게 다르지 않음에도, 목표를 달성하기 위한 방법적 측면에서 기존 접근 방식이 적합하지 않기 때문에 이를 바꾸고자 하는 것이며 제로트러스트 아키텍처의 기본 원리는 이 관점에서 기술되어야 한다.

2장에서 보다 구체적으로 기술되겠지만, 제로트러스트 아키텍처의 기본 원리를 설정하기 위해서는 기업망 등을 구성하는 기본적인 모델을 가정해야 한다. 추상적·논리적 관점에서, 이 모델은 누군가(접근 주체)가 무엇(리소스)에 접근하는 것을 허용 혹은 거부(정책)할 것인가를 다루어야 할 것이다.

기존의 경계 기반 보안 모델에서는 접근 주체의 물리적(혹은 네트워크 상의) 위치를 매우

중요하게 다뤘으며 외부로부터의 공격에 대응하는 다양한 방법적 측면을 고려하였다. 그러나, 앞서 언급한 다양한 이슈들로 인하여 더 이상 이러한 방식은 다양한 형태의 공격에 효과적이지 않으며, 지사·원격 접속 환경, 써드파티 협업 환경, 망분리 환경 등 다양한 시나리오에서 기업망에 접근하는 정상적인 사용자에게 VPN 등 불편한 보안 솔루션을 강제하는 단점이 존재한다.[10]

반드시 필요한 경우를 제외하고는 이런 보안 솔루션의 사용을 최소화하기 위해서는 다음의 원리에 따라 제로트러스트 아키텍처를 구성하는 것이 바람직하다. Forrester, Google 등 기업 보고서, CSA SDP, NIST SP 800-207, DoD 제로트러스트 참조모델 등에서 정의된 제로트러스트의 원리(부록 2절 참고)를 참고하였으며, 본 문서 앞부분에서 언급한 제로트러스트 개념 등을 고려하여 총 6가지 원리를 정의하였다.

〈표 1-3-2〉 제로트러스트 기본 원리

6가지 제로트러스트 기본 원리
가. 기본 원칙: 모든 종류의 접근에 대해 신뢰하지 않을 것 (명시적인 신뢰 확인 후 리소스 접근 허용)
나. 일관되고 중앙 집중적인 정책 관리 및 접근제어 결정, 실행 필요
다. 사용자, 기기에 대한 관리 및 강력한 인증
라. 리소스 분류 및 관리를 통한 세밀한 접근제어 (최소 권한 부여)
마. 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
바. 모든 상태에 대한 모니터링, 로그 및 이를 통한 신뢰성 지속적 검증, 제어

10 이 표현이 곧, VPN과 같은 기존 보안 솔루션을 절대로 사용하지 말라는 것을 의미하지는 않는다. 다만, 접속 위치와 단말, 네트워크 구조 등 다양한 환경에서 사용자에게 VPN과 같은 별도의 보안 절차(보안 프로그램 설치 및 강제화 등)를 요구하는 경우 정상 사용자에게 불편함을 줄 수 있다. 따라서, 제로트러스트 아키텍처를 적용하는 과정에서 이러한 솔루션을 사용하지 않더라도 기존보다 개선된 안전성을 제공할 수 있다면, 사용자 체험 면에서 매우 큰 장점을 갖게 될 것이다.

가. 기본 원칙: 모든 종류의 접근에 대해 신뢰하지 않을 것 (명시적인 신뢰 확인 후 리소스 접근 허용)

여기에서 모든 종류의 접근이라는 것은, 기업망에 존재하는 가치 있는 리소스에 대한 모든 접근 시도를 의미한다. 즉, 접근 주체(사용자 혹은 기기)의 식별 정보, 네트워크 접속 혹은 리소스 접근 시간, 네트워크 접속 위치, 네트워크/프로토콜 종류, 접근 대상 리소스 등에 대해 기본적으로는 접근을 거부하며, 일정 수준의 인증 과정을 거친 접근 주체에게만 제한된 수준의 리소스 접근을 허용하는 것을 원칙으로 하여야 한다.

심지어, 인증을 거친 접근 주체라 하더라도, 사용자가 고의적으로 기업망을 공격하고자 하는 경우, 기기 혹은 응용 프로그램이 공격자에 의해 탈취당한 상태, 정상 인증을 통해 설립한 접속 세션을 공격자가 원격으로 탈취한 상태 등 다양한 공격의 가능성이 있으므로, 현재 접속 세션에 대한 보안 상태의 지속적인 모니터링을 통해 신뢰성에 의심이 가는 상황 발생 시 강화된 추가 인증을 받거나 현재의 접근 세션을 종료시키는 등의 조치가 필요할 것이다.

나. 일관되고 중앙 집중적인 정책 관리 및 접근제어 결정, 실행 필요

기업은 반드시 리소스에 대한 접근에 대해 일관되고 중앙 집중적인 정책 관리 및 접근제어 결정, 실행 조치가 필요하다. 만약, 접근 정책을 관리하는 지점이 흩어져 있다면, 일관된 정책을 수립하기가 어려우며 새로운 접근 주체 및 리소스를 추가할 때에 대한 정책을 적용하기가 매우 어려울 것이다.

또한, 특정한 접근 주체가 어떤 리소스에 접근할 때에도, 해당 정책을 결정하고 실행하는 지점에서는 이미 수립되어 있는 일관되고 중앙 집중적인 정책에 따라야 한다. 접속 방식이나 리소스 종류, 신뢰도 평가에 따라 정책을 결정하고 실행하는 지점(예, NIST SP 800-207의 PDP 및 PEP 혹은 일부 기능)이 분산되어 있더라도, 반드시 중앙 집중적인 정책 관리에 의해 접근 여부를 일관되게 결정하여야 한다.

예를 들어, 특정 직원이 퇴사한 경우 이 직원의 식별 정보를 이용하려는 접근 주체는 직원에 의해서만 접근 가능한 리소스에 접근할 수 없도록 정책이 반영되어, 어디서 어느 리소스에 접근을 시도하더라도 일관되게 접근이 거부되어야 할 것이다.

다. 사용자, 기기에 대한 관리 및 강력한 인증

사용자는 기업 리소스에 접근하기 위하여 기기 및 그 기기상에 있는 응용 프로그램을 활용한다. 사용자는 일반적으로 본인의 식별 및 인증 정보를 이용하여 인증 과정을 거치지만, 사용자가 사용 중인 기기가 공격자에 의해 해킹을 당하였거나, 혹은 승인되지 않은 기기일 가능성이 있다.

사용자와 기기에 대한 관리는, 등록된 사용자와 기기에 대한 관리로부터 출발한다. 등록된 내·외부 사용자에 대하여 식별 및 인증 정보를 통한 강력한 인증을 적용하는 것은 기본일 뿐만 아니라, 등록된 기기 정보 및 상태 관리 역시 반드시 필요하다.

예컨대, 등록된 기기가 아니면 기업망 접속 혹은 특정 리소스 접근을 원천적으로 봉쇄한다거나, 혹은 등록된 기기와 등록되지 않은 기기에 대해 접근할 수 있는 리소스를 정확히 분류할 수도 있을 것이다. 그 외에도, 등록되지 않은 기기 혹은 명확히 보안 상태가 확인되지 않는 기기에 대해서는 추가 인증을 요구하는 방법이 있을 수 있다.

라. 리소스 분류 및 관리를 통한 세밀한 접근제어 (최소 권한 부여)

사용자 및 기기가 접근하고자 하는 리소스는 기업에 따라 매우 다양할 것이다. 예를 들어, 업무용 데이터, 응용 서비스, 웹 서버, 프린터와 같은 하드웨어, 외부망 접속 등 다양한 계층에 따라 분류할 수 있으며, 같은 리소스 종류라 하더라도 접근 주체의 직급이나 보안 상태, 시간에 따라서 다양한 형태의 접근제어 정책이 가능할 것이다.

접근제어 솔루션이 역할 기반이냐 속성 기반 방식을 지원하느냐를 판단하기에 앞서, 제로트러스트 아키텍처를 설계·구현하는 담당자는 반드시 리소스에 대해 명확하게 분류하고 접근 주체의 종류 및 다양한 요인에 따라 세밀하게 접근을 제어할 수 있어야 한다. 세밀한 접근제어가 가능해야만, 사용자 및 기기에게 필요한 최소한의 권한을 부여할 수 있으므로 공격이 발생하더라도 횡적 이동을 통한 피해를 최소화할 수 있게 될 것이다.

마. 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용

접근 주체가 특정 리소스에 접근하게 되면, 현재의 접근제어 정책에서 허용하는 범위를 넘어서는 다른 리소스에 접근할 수 없어야 한다. 이를 막기 위해서는 기존의 물리적 경계가

아닌 소프트웨어 정의 경계와 같은 방식으로 경계가 설정되어야 하며 강력한 인증을 통해 접근을 허용하였더라도 리소스에 따라서 긴 시간 동안의 접속을 허용하지 않는 것이 바람직하다.

공격자가 세션을 가로채거나 인증 방식을 도용하는 등의 시나리오를 고려하면 세션 단위의 접근만을 허용하는 것이 최선이며, 인증된 해당 접근 세션이 새로운 리소스에 대한 접근을 자동으로 허용하는 등의 정책은 바람직하지 않을 것이다.

또한, 리소스에 접근하는 모든 접근에 대해 논리 경계를 생성 후 통신을 할 때, 네트워크 위치와 관계없이 이를 보호하는 기술이 적용되어야 한다. 공격자는 리소스로 향하는 모든 통신에 대해 모니터링, 패킷 위변조 등을 통하여 리소스에 불법적으로 접근하려고 시도할 수 있기에, 통신 과정에서 기밀성과 무결성을 보호할 수 있어야 한다.

바. 모든 상태에 대한 모니터링, 로그 및 이를 통한 신뢰성 지속적 검증, 제어

여기에서 모든 상태라는 것은, 접근 주체(사용자와 기기)와 리소스(데이터, 응용, 서버, 하드웨어, 네트워크, 클라우드 서비스 등) 및 정책 서버의 다양한 상태를 포함한다. 예를 들어, 현재 시간, 사용자의 물리적 위치, 기기의 보안 상태, 현재 접속 중인 사용자의 수, 특정 접근 주체의 데이터 접근 횟수, 네트워크 트래픽 양 등 기업망 보안성 혹은 특정 접근 주체의 신뢰성 등을 추정할 수 있는 모든 정보가 포함될 것이다.

이러한 상태에 대한 정보는 기업망에서 반드시 모니터링되어 현재의 상태를 수치적 혹은 시각적으로 파악할 수 있어야 하며, 로그를 통해 차후 상세한 분석을 통한 감사가 가능해야 할 것이다. 이러한 모니터링 및 로그는 현재 접속 중인 모든 접근 주체 및 기업망에 대한 신뢰성을 지속적으로 검증하고, 접근을 동적으로 관리할 수 있도록 도움을 줄 것이다.

제2장에서는 제로트러스트 아키텍처 보안 모델에 대해서 정의한다. 제1절에서는 제로트러스트 아키텍처에 대한 모델 및 논리 구성 요소를 소개하고, 제2절에서는 제로트러스트 아키텍처 접근 방안에 대해 설명한다.*

* 제2장에서 정의하는 제로트러스트 아키텍처 보안 모델은 기본적으로 NIST SP 800-207 문서에서 정의된 내용을 최대한 준용한다. NIST SP 800-207은 제로트러스트 아키텍처를 처음으로 정의한 문서로 추상적인 수준에서 논리적 아키텍처를 기술하고 있으며, 다수의 글로벌 벤더 및 정부 등이 이 문서를 기본으로 준용하거나 참조하고 있다. 따라서, 제2장에서도 상위 수준에서 제로트러스트 아키텍처 보안 모델을 기술하고 있는바, 해당 문서와 구분되는 형태로 아키텍처를 구성하기보다는 최대한 준용하는 것으로 하였으며, 단, 기업이나 기관에서 제로트러스트 아키텍처 구현·도입시, 논리적 아키텍처와 구성 요소들에 대한 구체적인 실현 방법은 각자 다를 수 있다.

ZERO TRUST

제2장

제로트러스트 아키텍처 보안 모델

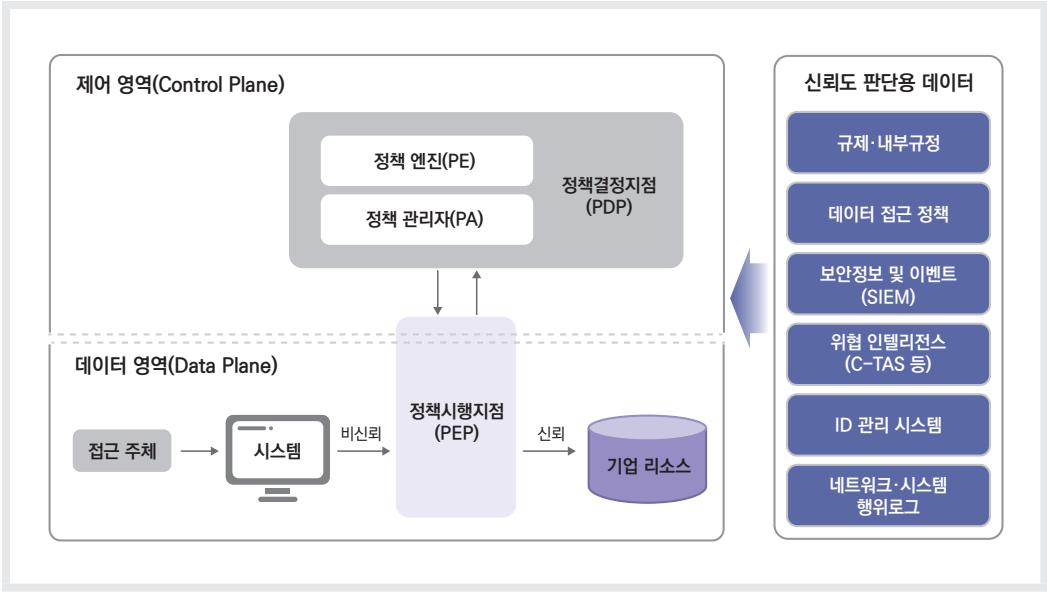
제1절 | 제로트러스트 아키텍처 보안 모델

1. 제로트러스트 아키텍처 보안 모델

앞서 1.4절에서 제로트러스트 아키텍처의 기본 원리를 소개한 바 있다. 특히, NIST SP 800-207에서는 제로트러스트 관점에서의 접근에 대한 개념 모델([그림 1-3-1])을 제시한 바 있으며, 이러한 개념 모델에서는 누군가(접근 주체)가 무엇(리소스)에 접근하는 것을 허용 혹은 거부(정책)할 것인가를 다루어야 한다. 이는 추상적으로 정의된 개념 모델이므로, 여기에서는 제로트러스트 아키텍처의 구체적인 보안 모델 및 논리 구성 요소를 소개하고자 한다.

기업망에서 제로트러스트 아키텍처를 실현하기 위해서는 앞서 언급한 접근 주체가 리소스에 대해서 접근하는 것에 대한 허용·거부 정책에 대해서 다루어야 한다. 따라서, 여기에서 가장 중요한 핵심 보안 기능은 접근제어 정책이 될 것이다. NIST SP 800-207에서는 이러한 정책 결정을 위한 보안 모델, 필요한 논리 구성 요소 및 각 구성 요소 간 상호작용에 대해서 정의하였으며, 이를 참고하여 본 문서에서는 [그림 2-1-1]과 같이 표현하였다.

[그림 2-1-1] 제로트러스트 아키텍처 보안 모델 및 논리 구성 요소



접근제어 정책이 결정되는 논리적 공간은 제어 영역(Control Plane)으로 부르며, 정책이 시행됨으로써 접근 주체가 기업의 리소스에 접근하는 논리적 공간은 데이터 영역(Data Plane)으로 부른다.

2. 제로트러스트 아키텍처 논리 구성 요소

[그림 2-1-1]의 제어 영역에서는 정책결정지점(PDP)과 정책시행지점(PEP)에서 통신을 통해, 접근 주체가 요청하는 기업 리소스에 대한 접근 허용 여부를 판단하기 위한 정보와 해당 결과를 교환하게 된다. 여기에서 PDP는 다시 각 논리적 역할에 따라 정책 엔진(PE, Policy Engine)과 정책 관리자(PA, Policy Administrator)로 나눌 수 있다. PEP는 데이터 영역에서 접근 주체가 기업 리소스에 접근하고자 할 때 결정된 정책에 따라 연결하거나 종료하는 역할을 담당한다.

기업의 내외부로부터 생성되는 데이터를 제공하는 입력 요소들이 PDP와 PEP 주변에 존재하여, 접근 결정을 위해 필요한 다양한 정보를 제공하기도 한다.

앞서 언급한 바와 같이, 정책을 결정·시행하는 것은 제로트러스트 아키텍처에서 가장 중요한 핵심 보안 기능이다. 따라서, 제로트러스트 아키텍처에서 PDP와 PEP는 핵심 논리 구성 요소라고 볼 수 있다. 그러나, 핵심 논리 구성 요소를 통해 정책을 결정하고 시행하는데 있어 다양한 정보를 제공할 수 있는 데이터 입력 요소 역시 중요한 역할을 수행할 것이다. 이 관점에서 각 논리 구성 요소(3가지 핵심 구성 요소 및 데이터 입력 요소)에 대해서 정리한다.

여기서 유의할 점은, 이들 구성 요소 혹은 데이터 입력 요소를 갖추고 있다고 하여 제로트러스트 아키텍처의 구현 철학을 만족한다고 볼 수 없다는 점이다. 이들은 반드시 유기적으로 상호 작용함으로써, 1.3절에서 언급한 제로트러스트 아키텍처의 기본 원리를 만족하여야 한다.

가. 정책 엔진(PE, Policy Engine)

정책 엔진은 접근 주체가 리소스에 접근할 수 있을지를 최종적으로 결정한다. 정책 엔진은 신뢰도 평가 알고리즘[11]에 대한 입력으로 현재 기업망에 대한 정책과 그 외 다른 정보를

활용하며, 이를 바탕으로 접근을 허가하거나 거부, 혹은 현재 허가되어 있는 상태의 접근을 취소할 수 있다. 정책 엔진은 접근에 대한 승인을 담당하며, 정책 관리자는 결정을 실행한다.

나. 정책 관리자(PA, Policy Administrator)

정책 관리자는 정책 엔진과 함께 PDP를 구성하며, PEP에 명령하여 접근 주체와 리소스 사이의 통신 경로를 생성하거나 폐쇄한다. 정책 관리자는 세션에 대한 인증·인가 토큰을 생성함으로써 접근 주체가 기업 리소스에 접근하는데 사용하도록 한다. 정책 관리자는 세션을 최종적으로 허락하거나 거부하는 결정을 정책 엔진에 의존한다.

세션이 인가되면 정책 관리자는 PEP에게 세션 시작을 허용하며, 세션이 거부되거나 취소되는 경우 PEP에게 해당 연결을 끊으라고 신호를 보낸다. 구현에 따라서 정책 엔진과 정책 관리자는 하나의 서비스에서 동작할 수 있으나, 본 문서에서는 두 논리적인 기능을 분리하여 설명한다. 정책 관리자는 통신 경로를 생성할 때 PEP와 통신하며, 이는 제어 영역에서 이루어지는 것으로 본다.

다. 정책시행지점(PEP, Policy Enforcement Point)

PEP는 접근 주체와 기업 리소스 사이를 연결하고 모니터링하며 최종적으로 연결을 종료하는 논리 구성 요소이다. 이는 정책 관리자와 통신하며, 접근 요청을 포워딩하고 업데이트된 정책을 수신한다.

제로트러스트 아키텍처 관점에서 PEP는 하나의 논리 구성 요소이지만, 2개의 다른 구성 요소로 구분될 수 있다. 예를 들어, 노트북에 설치된 에이전트에 해당하는 클라이언트 기능과 리소스 앞에서 접근을 제어하는 게이트웨이 기능으로 분리되어 동작할 수도 있으며, 통신 경로 상에서 문지기 역할을 하는 하나의 포탈 구성 요소로 동작하는 것도 가능하다. PEP를 넘어서면, 기업 리소스를 제공하는 신뢰 영역이 된다.

경계 기반 보안에서 많이 활용되는 방화벽(PEP), 제로트러스트 네트워크 관점에서 접근을 제어하는 NAC(구성 요소로서 PDP, PEP 기능 포함), 소프트웨어 정의 경계 방식의 SDP

---

11 2.2절의 3항에서 다루며, 접근 주체가 리소스 접근시, 이에 대한 허가 여부를 최종적으로 판단하기 위해, 현재 접근 주체 혹은 접근 그 자체의 신뢰도를 계산하는 알고리즘이다.

Controller(PDP) 및 SDP Gateway(PEP), 클라우드 상의 리소스 제어에 관한 CASB, 웹 기반 위협 관점에서 트래픽을 차단하는 SWG(PEP), 혹은 이들 기능을 포함하는 SSE, SASE 등이 PDP 및 PEP의 역할을 부분 혹은 전체적으로 담당하는 솔루션이 될 수 있다.

라. 접근 결정을 위해 사용하는 데이터 입력 요소

제로트러스트 아키텍처를 실행하는 기업은 접근 결정을 위해 데이터 입력 요소를 정책 엔진의 입력 혹은 정책 규칙으로 활용할 수 있다. 데이터 입력 요소는 기업이 생성하거나 제어하지 않는 외부 데이터 입력 요소와 내부 데이터 입력 요소들이 있을 수 있으며, 여기에는 다음과 같은 시스템 등이 포함될 수 있다.

- **규제·내부 규정(Industry Compliance)**: 기업이 영향을 받을 수 있는 규제(예, 정보보호 혹은 프라이버시 관련 법안, 의료 또는 금융 등 산업별 정보보호 요구사항 등)를 준수하는지 확인하며, 이는 기업이 규제 준수를 위해 개발한 모든 정책 규칙 포함함.
- **데이터 접근 정책(Data Access Policies)**: 이는 기업 리소스 접근에 관한 속성, 규칙, 정책을 의미함. 규칙들은 정책 엔진에 관리 인터페이스를 통해 입력되거나 동적으로 생성되며, 정책들은 기업 계정·응용·서비스에 대한 기본 접근 권한을 생성하여 리소스에 대한 접근을 인가하는 시작점이 됨. 이 정책들은 반드시 해당 기관에서 정의한 역할과 필요에 기반을 두어야 함.
- **보안 정보 및 이벤트(SIEM)**: 차후 분석을 위한 보안 정보를 수집하며, 이 정보는 정책을 개선하고 기업 자산에 가능한 공격을 경고하는데 활용함.
- **위협 인텔리전스(Threat Intelligence)**: 내외부 데이터 입력 요소로부터 정책 엔진의 접근 결정을 도울 수 있는, 새로 발견된 공격이나 취약점에 관한 정보 제공함. 새로 발견된 소프트웨어 취약점, 새로 식별된 멀웨어, 외부 자산에 대한 보고된 공격 등을 포함할 수 있으며 KISA의 C-TAS,[12] CIRCL의 MISP,[13] Alien Vault[14]의 OTX 등이

12 KISA(한국인터넷진흥원)이 운영하는 사이버 위협정보 분석·공유 시스템(Cyber Threat Analysis & Sharing)으로, 국내외 기업 및 기관들과 사이버 위협의 지능화·고도화로 인한 침해사고 조기 대응 및 피해 확산방지를 목적으로 위협 관련 정보를 분석·공유하기 위하여 구축하였으며, 위협 IP, 악성코드, 악성파일과 같은 공격 정보를 이용기관에게 공개

13 CIRCL(룩셈부르크 컴퓨터 사고 대응 센터)는 컴퓨터 보안 위협과 사고 정보를 수집, 검토, 보고 및 대응하기 위해 만들어진 룩셈부르크 CERT(Computer Emergency Response Team)이며, 여기에서는 MISP(Malware Information Sharing Platform)라는 오픈 소스 위협 인텔리전스 및 공유 플랫폼을 개발하여 공개하고 있음

여기에 해당됨

- **ID 관리 시스템(ID Management System)**: 기업 사용자 계정 및 식별 기록을 생성, 저장, 관리하는 시스템임. 필요한 접근 주체의 정보 및 특징(역할, 접근 속성, 할당 자산 등)을 포함할 수 있으며, 사용자 계정에 연관된 정보를 위해 PKI 등 다른 시스템을 때때로 활용함. 외부 협력을 위해 외부 근로자 혹은 자산을 포함하거나 더 큰 연합 공동체의 일부로서 존재할 수 있음. IAM, ICAM 등이 이 시스템에 해당됨
- **네트워크·시스템 행위 로그(Network and System Activity Logs)**: 로그 시스템은 자산 로그, 네트워크 트래픽, 리소스 접근 행위 및 기업망의 보안상태에 관한 실시간 피드백을 제공하는 기타 이벤트를 수집함.

다음 〈표 2-1-1〉은 위에서 설명한 제로트러스트 아키텍처의 논리 구성 요소 및 데이터 입력 요소에 대한 설명을 요약한 것이다.

〈표 2-1-1〉 제로트러스트 아키텍처 논리 구성 요소

구분	구성 요소		역할
핵심 구성 요소	정책결정 지점	정책 엔진	‣ 다양한 입력 요소를 검토하여 자원에 대한 접근 허용 여부 결정
		정책 관리자	‣ 주체와 자원 간 통신 경로 설정 및 종료 관리 ※ 세션 별 인증/인가 토큰 또는 크리덴셜 생성
	정책시행지점		‣ 주체에 할당된 정책 실행, 연결 활성화, 모니터링, 종료
신뢰도 판단용 데이터 제공자 (접근 결정 시 사용)	규제·내부 규정		‣ 법적 규제 정보 및 이를 위한 기업 내부 규정을 준수하는지 확인
	데이터 접근 정책		‣ 기업 리소스 접근에 대한 속성, 규칙, 정책 등
	보안 정보 및 이벤트		‣ 차후 분석용 보안정보 수집, 정책 개선 및 기업 자산 공격 경고에 활용
	위협 인텔리전스		‣ 내·외부에서 발생하는 보안 위협 정보 ※ 새로운 공격 기법, 악성코드, 취약점, SW 결함 등
	ID 관리 시스템		‣ 기업 사용자 계정 및 식별 기록 생성, 저장, 관리 (접근 주체의 정보, 특징 등 포함 가능)
	네트워크·시스템 행위 로그		‣ 각종 로그 및 로그 분석 결과(공격 가능성 등)

14 Alien Vault는 2007년 설립된 보안 관련 기업으로 2018년 AT&T에게 인수되어 현재 AT&T Cybersecurity라는 사명으로 변경되었으며, 2003년 시작된 오픈 소스 보안 정보 관리 프로젝트(OSSIM)을 운영하는 것으로 잘 알려져 있다. OTX(Open Threat Exchange)는 글로벌 인텔리전스 공유 커뮤니티로, 기업과 독립 연구자, 정부 기관 등이 공개적으로 협력하여 새로운 위협이나 공격, 악의적 행위에 관한 최신 정보를 공개하는 체계임

제2절 | 제로트러스트 아키텍처 접근 방법

1. 제로트러스트 아키텍처 접근 방법

기업에서 앞서 언급한 제로트러스트 아키텍처 보안 모델을 구성하기 위한 접근 방법은 여러 가지가 있다. 제로트러스트 아키텍처 보안 모델로 이행하는 과정은 단순하지 않으며, 적은 인원이 수일에서 수개월 정도에 해당하는 단시간의 노력만으로 달성할 수 없다. 기업마다 구성하고 있는 접근 주체와 리소스가 다르고, 제로트러스트 관점에서의 보안 기능에 대한 중요도가 다를 수 있다.

이를 위해 NIST SP 800-207에서는 접근 방법을 아래와 같이 3가지 추상적인 요소로 분류하였다. 만일 기업에서 완벽하게 제로트러스트 아키텍처의 보안 모델을 구현한 경우 모든 접근 방법을 포함하게 될 것이며 기업망의 개별 상황에 따라 이 중 특정 접근법이 우선적으로 고려될 수 있을 것이다.

〈표 2-2-1〉 제로트러스트 아키텍처 접근 방법

접근 방법	세부 내용
인증 체계 강화	▸ 행위자의 식별자를 핵심 요소로 설정하여 정책 작성 ▸ 개방형 네트워크, 방문객 접근 허용 기업망, 기업 소유가 아닌 기기가 자주 연결되는 기업망 등에 적합 ▸ 클라우드 기반 응용/서비스 사용 환경에도 유리 ▸ 리소스 포털 배치 모델에 효과적
마이크로 세그멘테이션 (Micro-Segmentation)	▸ 보안 게이트웨이로 보호되는 단독 네트워크 구역(segment)에 개별 리소스 (혹은 리소스 그룹) 배치 ▸ 다양한 유스케이스 및 배치 모델에 적용 가능 ▸ 게이트웨이 기기 및 방화벽으로 일부 구현 가능하나 관리 비용 등 단점
네트워크 인프라 및 소프트웨어 정의 경계	▸ 소프트웨어 정의 경계 기법을 활용하여 정책 엔진의 결정에 따라 컨트롤러가 네트워크를 재구성 ▸ 에이전트/게이트웨이 배치 모델 활용 ▸ 클라우드 가상 네트워크 혹은 IP 기반이 아닌 네트워크 등에서도 변형된 형태로 사용 가능

2. 제로트러스트 아키텍처 논리 구성 요소의 배치 모델

1절에서 언급한 모든 구성 요소들은 모두 논리 구성 요소이다. 따라서, 이들 구성 요소들은 단독 시스템일 필요가 없으며, 단독 시스템이 다수 논리 구성 요소의 역할을 수행할 수도 있고, 하나의 논리 구성 요소가 다수의 하드웨어 혹은 소프트웨어로 구성될 수도 있다.

예를 들면, 기업 PKI가 기기에 인증서를 발행하는 구성 요소와 사용자에게 인증서를 발행하는 구성 요소 등으로 구성될 수 있지만, 동일한 CA 인증서를 사용할 수 있다. 어떤 제로트러스트 제품들은 정책 엔진과 정책 관리자가 하나의 서비스로서 제공되기도 한다.

NIST SP 800-207에 따르면 제로트러스트 아키텍처 논리 구성 요소의 배치 모델에 대해서는 일반적으로는 다음과 같은 모델들을 고려할 수 있다. 기업에서 관리의 편의성을 고려하면 하나의 모델을 사용하는 것이 바람직하나, 기업망이 구축되어 있는 상황에 따라 내부 절차 혹은 기기, 리소스의 특성으로 인하여 하나의 배치 모델만을 사용하는 것이 불가능할 수도 있다. 하나의 기업 내에서 여러 모델을 활용하는 것이 가능하며, 때로는 아래 모델들을 모두 포함하는 통합 배치도 가능할 것이다.

- 기기 에이전트 - 게이트웨이 배치 모델
- 리소스 그룹 배치 모델
- 리소스 포탈 배치 모델
- 기기 응용 샌드박스 배치 모델

상기 배치 모델들은 모두, [그림 2-1-1]에서 언급한 제어 영역과 데이터 영역 내에서 각 논리 구성 요소를 구체화하게 된다. 그러나, 데이터 영역에서 접근 주체가 리소스에 접근하는 과정에서 PEP가 어떻게 배치되는가가 가장 핵심적이라고 할 수 있다.

전반적으로는 기기 에이전트 - 게이트웨이 배치 모델이 가장 높은 수준에서 제어를 할 수 있다. 자산에 설치되어 기업의 관리가 가능한 에이전트와 개별 리소스에 위치한 게이트웨이간 연결되어 있으므로, 사용자와 기기, 접근하고자 하는 리소스에 대해 구체적으로 정책을 집행하는 것이 가능하기 때문이다.

그러나, 리소스 혹은 접근 프로토콜에는 레거시 기술을 포함할 가능성도 있으므로 모든 리소스에 게이트웨이를 설치하는 형태로 배포하는 것이 불가능할 수 있다. 이는 특정 리소스

대신 여러 리소스들의 그룹(Enclave)에 게이트웨이를 구현하는 방식이 필요할 수 있음을 의미하며, 이 경우, 게이트웨이는 특정 리소스가 아닌 리소스 그룹에 대한 접근 권한을 부여하게 된다.

심지어, 구형 기기, 기기의 성능, 관리 영역에 있지 않은 기기 등의 이유로 기기에 에이전트를 설치할 수 없는 환경이라면 세번째인 리소스 포탈 배치 모델을 고려할 수 있다. 이는 기존의 경계 기반 보안 모델과 유사성이 있으며, 기업의 자산에 대해 완전히 모니터링 및 통제가 불가능한 단점이 있다.

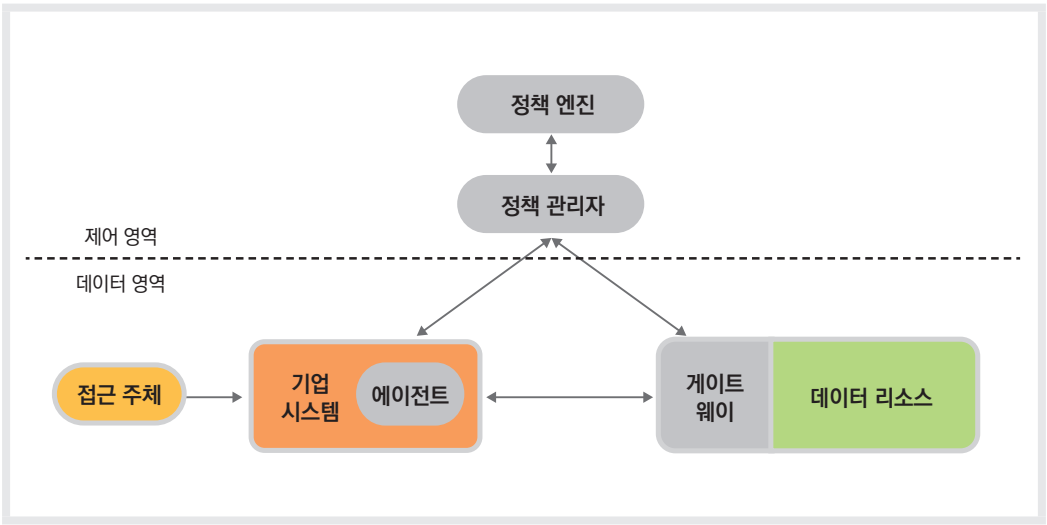
기기 응용 샌드박스 배치 모델은 기기 에이전트 - 게이트웨이 배치 모델의 변형된 형태로 볼 수 있으나, 기기가 가진 위험이나 취약점으로부터 상대적으로 안전하며, 한편으로는 응용이 자산과 논리적으로 분리되기 때문에 리소스 포탈 배치 모델과 유사하게 기업의 자산에 대한 완전한 모니터링 및 통제가 불가능하다.

가. 기기 에이전트 – 게이트웨이 배치 모델

이 배치 모델에서는 기기 에이전트와 리소스 게이트웨이가 PEP를 구성한다. 리소스는 오직 게이트웨이와 통신하며, 기업이 지급한 자산에 기기 에이전트 소프트웨어를 설치한다. 에이전트는 리소스 접근을 위해 필요한 트래픽을 적절한 정책집행지점으로 전송하며, 게이트웨이는 정책 관리자와 통신하여 정책 관리자에 의해 승인된 통신 경로만을 허용하게 된다.

예를 들어, 기업에서 지급한 노트북을 소유하고 있는 사용자(접근 주체)가 인사 프로그램 혹은 데이터베이스와 같은 기업 리소스에 접속하는 경우를 생각해보자. 노트북 상의 에이전트는 접근 요청을 받고, 이 요청을 정책 관리자에게 전달한다. 정책 관리자 및 정책 엔진은 기업의 온프레미스 혹은 클라우드 상에 존재할 수 있으며, 정책 관리자는 권한 평가를 위해 해당 요청을 정책 엔진으로 전달한다. 만약 요청이 인가된다면, 정책 관리자는 데이터 영역에서 기기 에이전트와 리소스 게이트웨이 사이에 통신 채널을 설정하며, 여기에는 IP 주소, 포트, 세션, 보안 데이터 등을 포함할 수 있다. 기기 에이전트와 게이트웨이가 연결되면, 암호화된 데이터 채널이 시작되며, 관련 업무가 종료되거나 보안 이벤트(예, 세션 타임아웃, 재인증 실패)에 의해 정책 관리자가 강제로 접속을 종료해야 하는 상황이 발생하면 에이전트와 게이트웨이 사이의 연결은 종료된다.

[그림 2-2-1] 기기 에이전트 – 게이트웨이 배치 모델



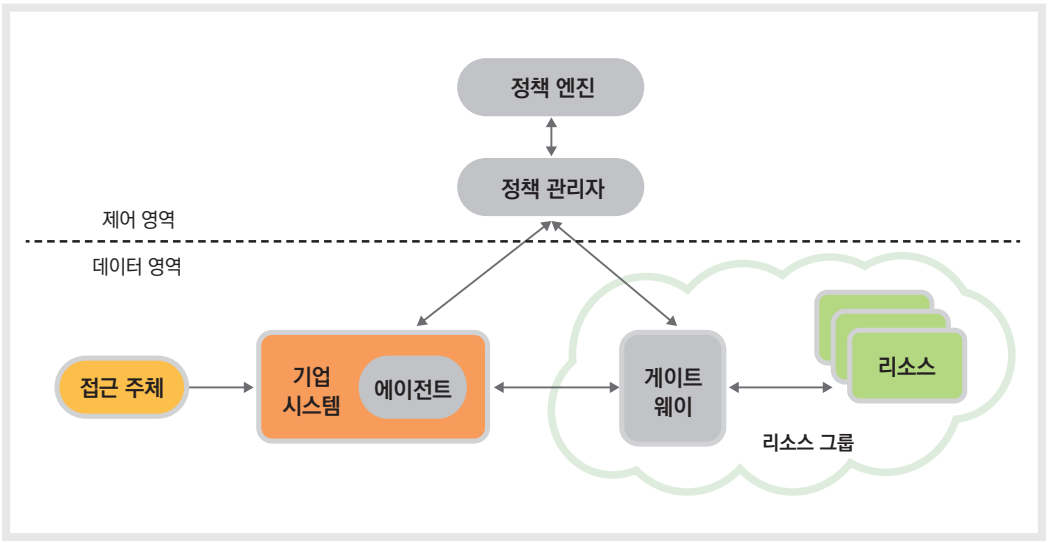
이 모델은 개별 리소스가 게이트웨이와 통신할 수 있고, 강력한 기기 관리 프로그램을 도입한 기업에게 가장 잘 활용될 수 있다. 클라우드 서비스를 중점적으로 활용하는 기업에게, 이는 소프트웨어 정의 경계표준의 클라이언트-서버 구현이 된다. 또한 BYOD 정책을 도입하지 않는 기업에게도 적절하다. 기업 소유 자산에 설치된 기기 에이전트에 의해서만 접근이 가능하기 때문이다.

이 모델에서 의사결정의 핵심은 정책 엔진에 있으며, 정책 엔진은 다양한 시스템들로부터 데이터를 수집하여 신뢰도를 판단하고 접근제어 규칙을 구성하게 된다.

나. 리소스 그룹 배치 모델

이 배치 모델은 기기 에이전트 - 게이트웨이 배치 모델의 변형으로 볼 수 있으며, 게이트웨이가 단일 리소스가 아닌 리소스 그룹 앞에 있는 모델이다. 리소스 혹은 접근 프로토콜에는 레거시 기술을 포함할 가능성도 있다. 예를 들어, 게이트웨이와 통신하기 위한 API를 가지고 있지 않은 레거시 데이터베이스 시스템 혹은 하나의 비즈니스 프로세스를 위한 클라우드 기반의 소규모 서비스 사례 등이 있을 수 있다. 이러한 경우, 모든 리소스에 게이트웨이를 설치하는 형태로 배포하는 것이 불가능할 수 있기 때문에 특정 리소스 대신 여러 리소스의 그룹(Enclave)에 게이트웨이를 구현하는 배치 모델이 필요하다.

[그림 2-2-2] 리소스 그룹 배치 모델

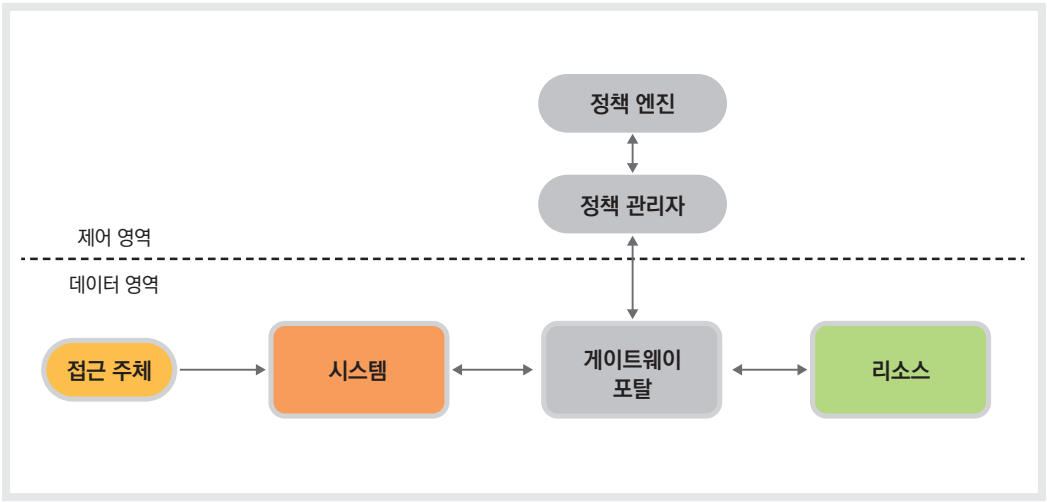


이 모델은 기기 에이전트 - 게이트웨이 배치 모델과 함께 적용하는 것도 가능하다. 이 하이브리드 모델에서 모든 기업 자산은 기기 에이전트를 가지며, 일부 리소스의 경우 해당 리소스를 위한 게이트웨이와 통신하고, 일부 리소스의 경우에는 해당 리소스 그룹을 위한 게이트웨이와 통신하는 형태가 될 것이다. 이 모델은 개별적으로 게이트웨이를 가질 수 없는 레거시 응용 혹은 데이터 센터를 보유한 기업에 유용할 것이며, 기기 에이전트 설치와 관리를 위한 자산 관리 프로그램이 필요하다. 기기에 대한 모니터링 및 통제는 가능하겠지만, 개별 리소스에 대한 보호는 불가능할 수 있다.

다. 리소스 포탈 배치 모델

다른 두 모델과 마찬가지로 이 모델에서 게이트웨이는 사용자 접근을 제어하기 위해 리소스 앞에 배치되며, 차이점은 PEP가 사용자 기기 혹은 응용 프로그램에 에이전트 형태로 통합되지 않는다는 것이다. 게이트웨이 포탈은 앞의 두 모델에서처럼 리소스별 배치 혹은 리소스 그룹 앞에 배치될 수 있다.

[그림 2-2-3] 리소스 포탈 배치 모델

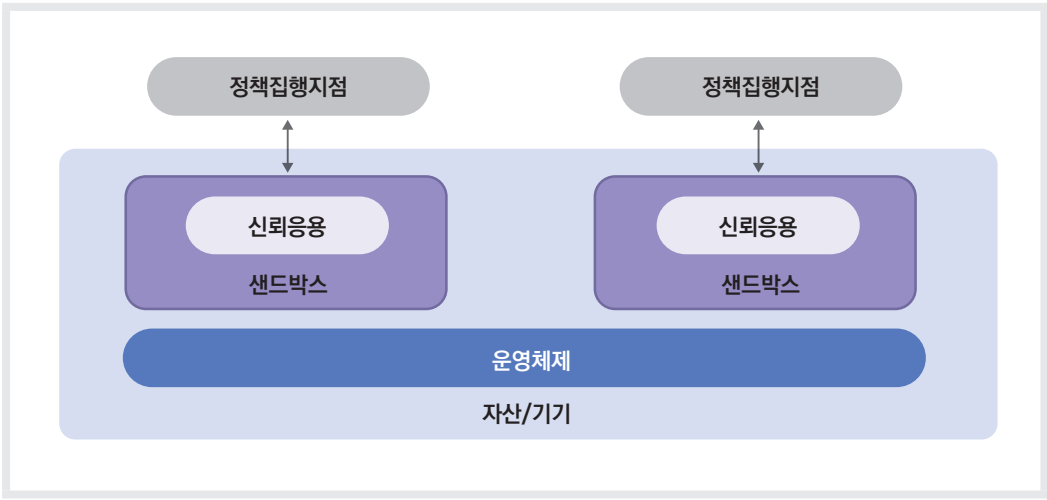


에이전트가 사용자 기기에 설치되지 않으므로, BYOD 정책 혹은 기업 간 협업 등에 유연하게 적용할 수 있다는 장점이 있다. 기업 관리자는 기기에 에이전트의 설치 여부를 확인할 필요가 없는 대신, 기기를 모니터링 할 수 없으므로 기기가 게이트웨이 포탈에 접속할 때에만 제한된 정보를 추측할 수 있다. 기기에 악성코드 혹은 취약점이 있는지, 적절한 보안 설정을 가지고 있는지 지속적인 모니터링이 불가능하며, 임의로 통제할 수도 없다. 또한, 공격자가 포탈을 검색하여 접근하려고 하거나, 서비스 거부 공격 등을 시도할 수 있으므로, 이에 대한 대책이 필요하다.

라. 기기 응용 샌드박스 배치 모델

이 모델은 기기 에이전트 - 게이트웨이 배치 모델의 또 다른 변형으로, 확인된 신뢰응용을 자산에서 격리하여 실행한다. 이러한 격리는 가상 머신이나 컨테이너 등을 활용할 수 있으며, 자산에서 실행 중인 다른 응용 혹은 침해 가능성이 있는 공격자로부터 리소스 접속을 위한 신뢰응용을 보호하고자 함이다.

[그림 2-2-4] 기기 응용 샌드박스 배치 모델



사용자는 기기에서 기업이 승인한 신뢰응용을 샌드박스에서 실행하고, 이 응용은 정책 집행지점과 통신하여 리소스 접근을 요청한다. 정책집행지점은 기업망에 위치하거나 혹은 클라우드 서비스일 수 있으며, 동일 자산의 다른 응용의 요청을 거부한다. 신뢰응용이 자산 내에서 독립적으로 실행되기 때문에, 신뢰응용이 악성코드에 감염되지 않도록 보호할 수 있다는 장점이 있으나, 기업은 신뢰응용을 관리하여야 하며 자산에 대한 모니터링 및 통제가 어려울 수 있다. 기업이 '신뢰응용이 안전하다'는 것을 확인할 수 있어야 하는데, 이는 기기를 모니터링하는 것보다 어려울 수 있다.

3. 신뢰도 평가 알고리즘

제로트러스트 아키텍처를 실시하는 기업에서는, 접근 주체가 리소스에 접근하고자 할 때 그에 대한 신뢰도를 평가할 수 있어야 한다. 신뢰도 평가 알고리즘은 정책 엔진에서 현재의 접근을 최종적으로 허가 혹은 거부하기 위해 실행된다. 정책 엔진은 [그림 2-1-1]에서와 같이 다양한 입력값을 논리 구성 요소로부터 가져오게 되는데 이 입력값들은 다음과 같은 값들을 가지게 된다.

〈표 2-2-2〉 신뢰도 평가 알고리즘에 대한 입력값

입력값	세부 내용
접근 요청	▸ 설명: 접근 주체의 리소스 접근 요청 ▸ 주요 정보: 요청된 리소스 및 요청자 정보(OS 버전, 사용 중인 소프트웨어, 패치 정보 등)
접근 주체 데이터베이스	▸ 설명: 리소스에 접근을 요청하는 접근 주체의 정보 ▸ 주요 정보: 기업 또는 협력사 직원 혹은 프로세스 및 이들에 할당된 속성/권한 – 사용자 식별자: 논리 식별자(예, 계정ID)의 조합, 정책집행지점이 수행한 인증 확인 결과 등을 포함할 수 있음 – 속성: 시간과 지리적 위치 포함 – 권한: 권한은 개별적으로 접근 주체에게 할당되어야 하며, ID 관리 시스템 및 정책 데이터베이스에 저장해야 함. 어떤 신뢰도 평가 알고리즘에서는 과거에 관찰된 접근 주체의 행동에 관한 데이터를 포함할 수도 있음
자산 데이터베이스	▸ 설명: 기업 소유(및 기업 소유가 아니지만 인지할 수 있는/BYOD) 자산(물리/가상/기타)의 상태를 포함하는 데이터베이스 ▸ 주요 정보: OS 버전, 설치된 소프트웨어, 무결성, 위치(네트워크/지리적), 패치 정보 등 ▸ 접근 요청 정보상의 자산 상태와 자산 데이터베이스를 비교하여 접근제어
리소스 요구사항	▸ 설명: 리소스 접근을 위한 최소한의 요구사항 정의 ▸ 주요 정보: 네트워크 위치(예, 해외 IP 접근 거부), 데이터 민감도 등의 인증 보증 레벨, 자산 설정 요구사항
위협 인텔리전스	▸ 설명: 일반적인 위협 및 유행하는 악성코드 정보 피드 ▸ 주요 정보: 의심스러운 기기로부터의 통신과 관련한 특정 정보 포함 가능, 공격 패턴 혹은 보완 대책 ▸ 기업보다는 외부 서비스가 통제할 가능성이 높은 유일한 구성 요소

각 입력값 혹은 입력값을 제공하는 구성 요소에 대한 가중치는 외부 개발 평가 알고리즘에 의존할 수도 있고, 기업이 직접 설정할 수 있다. 신뢰도가 평가되면 실행에 대한 최종 결정은 정책 관리자가 하며 필요한 PEP를 설정하여 승인된 통신을 가능하게 할 수 있다. 정책 요구사항에 따라 연결을 재인증·재인가하기 위해 통신 세션을 보류하거나 정지시킬 수도 있으며(예, 타임아웃 등의 이유로 보안 이벤트 발생시) 종료시키기 위한 명령을 내릴 수도 있다.

가. 신뢰도 평가 방식

신뢰도를 평가하는 방식에 따라 이 알고리즘이 다르게 구현될 것이다. 신뢰도를 평가하는 방식은 입력값의 평가 방식 및 접근 요청에 대한 주변 컨텍스트의 고려 여부에 따라 달라질 수 있다. 일반적으로는 점수 기반, 컨텍스트 기반 방식이 더 동적으로 세밀하게 접근을 통제할 수 있다.

〈표 2-2-3〉 신뢰도 평가 방식

평가 방식 기준점	세부 내용	
입력값 평가 방식	기준 기반	점수 기반
	▸ 리소스 접근 승인 혹은 액션(읽기/쓰기) 허가전 반드시 만족해야 하는 속성 검증, 모든 기준을 만족한 경우에만 허가 ▸ 기업이 설정하며, 모든 리소스에 대해 독립적으로 설정	▸ 모든 입력값 제공 구성 요소에 대한 가치 및 기업 설정 가중치에 기반한 신뢰도 계산 ▸ 점수가 사전 설정된 경계값보다 크면, 접근 혹은 액션 허가, 작으면 접근 거부 혹은 권한 축소
접근 요청 주변 컨텍스트 활용	단독 판단	컨텍스트
	▸ 각 접근 요청을 개별적으로 처리하며 평가시 접근 주체의 이력을 고려하지 않음 ▸ 공격이 접근 주체에게 허용된 역할 내에서 이루어지면 탐지되지 않을 가능성 존재	▸ 접근 요청 평가시 접근 주체 혹은 에이전트의 최근 이력 고려 (정책 엔진은 접근 주체 및 응용 상태 정보를 유지해야 함) ▸ 정책 엔진은 접근 주체와 상호작용하는 정책 관리자 및 PEP에 사용자의 행위를 알려야 함. 행위 분석을 통하여 허용 가능한 행위 모델 생성 가능하며, 편차를 벗어날 경우 추가 인증 혹은 리소스 접근 거부 등을 수행할 수 있음

나. 컨텍스트 기반 신뢰도 평가 알고리즘

앞서 언급한 바와 같이, 제로트러스트 관점에서 보다 이상적인 신뢰도 평가 알고리즘은 주변 컨텍스트 기반이어야 한다. 문제는, 컨텍스트 기반 신뢰도 평가가 모든 기업 인프라에 적용가능하지 않을 수도 있다는 것이다. 신뢰도 평가 알고리즘 역시 보안 기능 중 하나이므로 '보안과 사용성', '비용 대비 효과'의 균형을 이루는 것이 중요하다.

기업 내부에서 이루어지는 일반적인 행위에 대해 지속적으로 재인증을 요구하면 사용성에 이슈가 발생할 수 있다. 예를 들어, 인사팀 직원이 하루에 20~30명의 직원 기록에 접근하는

것이 일반적이라면, 이 알고리즘에서는 하루에 100명에 대한 기록에 접근하고자 할 때 혹은 근무 시간 이후에 알 수 없는 장소에서 접근하고자 할 때 경고를 보내고 재인증을 요청할 수 있다.

각 리소스에 대한 기준 혹은 가중치, 경계값 등을 설정할 때에는 계획과 테스트가 필요하다. 기업 관리자는 제로트러스트 아키텍처 실행 초기에 잘못된 설정으로 승인되어야 할 접근 요청이 거부되는 경우가 발생할 수 있으므로, 튜닝을 거쳐 정책이 적절히 적용될 수 있도록 기준 또는 점수의 가중치, 경계값을 조정해야 할 것이다.

혹은 기계 학습 등의 기술을 활용하여 재인증 혹은 2차 인증의 성공, 실패 여부 및 다양한 입력값(근무 시간으로부터 얼마나 많이 벗어났는지, 담당자의 출장 여부, 최근 악성코드 혹은 위협 사례·횟수 등)을 고려하여 자동으로 가중치와 경계값을 재조정하는 방법도 가능할 것이다. 이러한 방법 역시 정확성과 사용성, 비용 대비 효과를 모두 고려하여 도입 여부를 검토해야 할 것이나, 궁극적으로는 기업 관리자에게 가장 이상적인 방식이 될 것이다.

3장에서는 기업들이 기업망에 제로트러스트를 도입하기 위한 절차를 기술하고자 한다. 이를 위해, 먼저 제1절에서는 제로트러스트 아키텍처 도입을 위한 기업망의 핵심 요소와 함께 성숙도 모델을 정의함으로써, 각 기업들이 제로트러스트 아키텍처를 완전히 도입하기 위한 핵심 요소별 목표 및 현재 수준을 이해할 수 있도록 한다. 제2절에서는 도입을 위해 필요한 고려사항을 정리하고, 제3절에서는 실제 도입을 위해 필요한 단계 및 해당 단계에서 필요한 절차를 언급한다. 마지막으로, 제로트러스트를 도입하고 운영하는 과정에서 인식하고 있어야 할 주의사항을 제4절에서 다룬다.

ZERO TRUST

제3장

제로트러스트 도입 절차

제1절 | 제로트러스트 성숙도 모델

성숙도 모델은 일반적으로 특정 프로세스·기술에 대한 조직의 성숙도를 측정하기 위한 프레임워크를 의미하며 보안 아키텍처 관점에서도 다양한 형태의 성숙도 모델[15]이 제안된 바 있다. 성숙도 모델은 기업·기관이 가지고 있는 목표 및 규정 준수를 위한 요구사항과 일치하는 접근 방법을 제공하고, 현재의 상태를 평가·검증함으로써 추가적인 기술 도입 및 투자에 대한 방향성을 정하는데 도움을 줄 수 있는 일종의 참조 아키텍처의 역할을 수행할 수 있다.

제로트러스트 아키텍처는 보안에 대한 패러다임의 전환 관점에서 다양한 아이디어를 포함하고 있으나, 제로트러스트 아키텍처에 대한 목표 및 도입 전략·계획을 수립해야 하는 기업·기관 관점에서는 매우 추상적으로 느껴질 수 있다. 다른 성숙도 모델과 마찬가지로 제로트러스트 성숙도 모델이 절대적인 답안은 아니지만, 기업·기관에게 현재 제로트러스트 수준을 평가(Assessment)하고 구현·도입을 수립하는데 도움을 줄 수 있다.

제로트러스트 성숙도 모델에 대해서는 다양한 기업과 기관에서 언급한 바 있다. 물론, 모든 기업과 기관의 기업망 운용 방식이나 보안 정책, 국가별 규제 및 관련 법규가 모두 다르므로, 제로트러스트 아키텍처 구현·도입 방법이 하나로 정해지는 것은 아니다.

국내 환경에 적합한 제로트러스트 구현·도입 방법 기술을 위하여 국내 법·제도의 특수성으로 인한 기업망 환경을 고려할 필요가 있다. 본 절에서는, 기업망의 핵심 요소에 대한 해외 정의 사례를 먼저 살펴보고, 국내 환경을 위한 제로트러스트 도입을 위한 핵심 요소 및 성숙도 모델을 제안한다.

---

15 예를 들어, The Open Group에서 2017년 정의한 정보보호 관리 성숙도 모델, O-ISM3(Open Information Security Management Maturity Model) Version 2.0이라든지, ISO/IEC 21827:2008 SSE-CMM(Systems Security Engineering – Capability Maturity Model) 등 다수의 보안 관련 성숙도 모델이 존재한다.

1. 제로트러스트 도입을 위한 기업망의 핵심 요소

가. 제로트러스트 도입을 위한 기업망의 핵심요소 해외 정의 사례

여기에서는 제로트러스트 도입을 위한 기업망의 핵심 요소를 정의함으로써, 이들 핵심 요소에 대한 성숙도 수준 및 평가 방법을 포함하는 성숙도 모델 수립에 도움을 주고자 한다. 〈표 3-1-1〉에서 보는 바와 같이, 다양한 기업 및 기관에서 제로트러스트 도입을 위한 성숙도 모델 및 핵심 요소를 정의한 바 있으며, 특히 CISA에서는 [그림 3-1-1]과 같이 제로트러스트의 토대가 되는 핵심 요소 및 주요 기능을 표현하였다.[16]

〈표 3-1-1〉 각 기업/기관에서 정의한, 제로트러스트 도입을 위한 기업망의 핵심 요소

Forrester[17]	Microsoft[18]	SAP[19]	DISA/NSA (DoD) [20]	CISA[21]
7가지 핵심 요소 ‣ Data ‣ Networks ‣ People ‣ Workloads ‣ Devices ‣ Visibility and Analytics ‣ Automation and Orchestration	**6가지 핵심 요소** ‣ Identities ‣ Devices ‣ Applications ‣ Data ‣ Infrastructure ‣ Networks	**6가지 핵심 요소** ‣ Identities ‣ Data ‣ Network ‣ Applications ‣ Infrastructure ‣ Endpoints	**7가지 핵심 요소** ‣ User ‣ Device ‣ Network/ Environment ‣ Applications and Workload ‣ Data ‣ Visibility and Analytics ‣ Automation and Orchestration	**5가지 핵심 요소** ‣ Identity ‣ Device ‣ Network/ Environment ‣ Applications Workload ‣ Data **3가지 교차 기능** ‣ Visibility and Analytics ‣ Automation and Orchestration ‣ Governance

16 CISA의 핵심 요소는 OMB(예산관리실) 각서에서 미 연방정부 기관장들의 제로트러스트 전략적 목표 수립시 일치해야 한다고 규정하였으므로 참고할 가치가 있다.

17 Forrester, "The Zero Trust eXtended (ZTX) Ecosystem", 2018년 1월

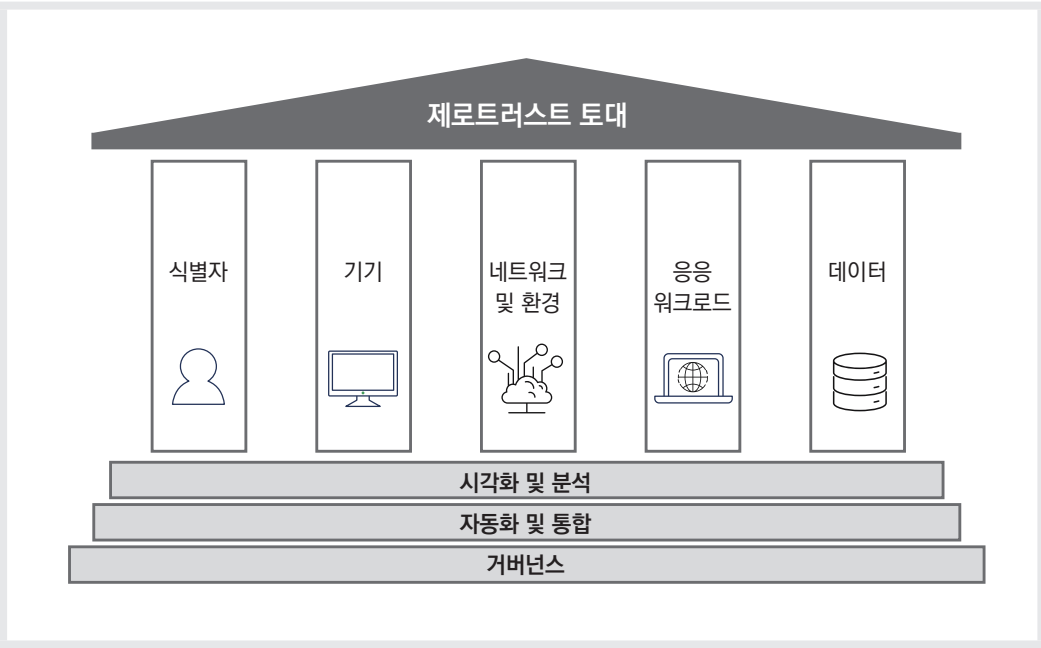
18 Microsoft, "Zero Trust Maturity Model", 2019년 10월

19 SAP, "RISE with SAP: Adopting to Zero Trust Architecture Principles with SAP Cloud Services", 2022년 2월

20 DISA and NSA, "Department of Defense (DOD) Zero Trust Reference Architecture Version 2.0", 2022년 7월

21 CISA, "Zero Trust Maturity Model (Version 2.0)", 2023년 4월

[그림 3-1-1] 제로트러스트 토대



(출처: CISA, "Zero Trust Maturity Model")

나. 국내 환경에 적합한 제로트러스트 도입을 위한 기업망의 핵심요소

앞에서 정리한 바와 같이 CISA, DISA/NSA 등은 공통적으로 5개의 핵심 요소와 2~3개의 교차 기능으로 제로트러스트 구성을 정의하였다. 여기에서 공통된 핵심 요소 및 교차 기능을 살펴보면 Identity(User), Device(Endpoint), Network, Application(Workload), Data, Visibility and Orchestration, Automation and Orchestration 등 7가지가 주로 언급됨을 볼 수 있다.

기업망에서 가장 중요한 보호의 대상은 데이터(Data)로 볼 수 있으며, 식별자(Identity)로 구분되는 사용자(User)는 기기(Device)를 이용하여 기업 네트워크(Network) 상에서 응용 및 워크로드(Application/Workload)를 통해 데이터에 접근하게 된다. 이 과정에서 이들은 모두 공격 대상이 될 수 있으며 따라서 제로트러스트 관점에서 필요한 보안 기능을 요구하게 된다.

일반적으로 기기(Device)는 온프레미스와 클라우드를 모두 포함하는 기업망에 연결된

모든 컴퓨팅 가능한 장치를 의미한다. 따라서, 이들 기기는 사용자가 기업망 내부 응용 및 데이터에 접근하기 위해 사용하는 단말만을 의미하는 것이 아니라, 기업망 내부에서 사용되는 모든 기기(서버, 프린터, 네트워크 장비, 클라우드 스토리지 등)를 포함한다. 다만, Microsoft의 경우 사용자 단말과 구분되는 온프레미스 서버나 클라우드 기반 가상 머신 등을 인프라스트럭처(Infrastructure) 핵심 요소로 분리하였으며, SAP도 유사한 구조를 가지고 있다. 사용자 단말과 인프라를 하나의 핵심 요소로 둘 것인가 분리할 것인가는 그 두 요소에 별도로 요구되는 보안 기능이 존재하는가를 고려하여 결정해야 한다.

국내에서는 금융망 및 국가 기반 시설에 대한 망분리 기반 보안 정책 및 공공기관 클라우드 보안 인증 관련 기준을 준수해야 하므로, 이들 환경에서는 시스템 및 인프라스트럭처 영역에 대하여 추가 고려하여야 한다.

원격근무나 재택근무의 경우는 보안 관점에서 제로트러스트 도입 시 중요하게 다루어져야 할 부분은 시스템 관리자 또는 개발자들이 기업망 내 중요 데이터(예, 금융기업에서 보유한 고객 정보, 고객간 거래 정보 등 중요 정보)를 저장하고 있는 시스템에 접근할 수 있는 경우이다. 원격으로 최고 권한을 갖는 시스템 관리자 계정의 접속이 가능한 경우 해당 계정에 대한 해킹으로 인한 피해는 이루 말할 수 없을 정도이다. 또한 운영 체제의 보안 패치가 제때 이루어지지 않는 등 취약점을 내재하고 있는 시스템의 경우, 정상적인 접근제어를 회피하는 공격이 가능할 수 있다. 이러한 공격이 가능하다면 기업망의 중요 정보에 대한 탈취 및 파괴가 가능할 수 있으므로, 이들 공격에 대응·완화하기 위하여 시스템(System) 영역을 별도의 핵심 요소로 고려할 필요가 있다.

이 점을 고려하여 본 문서에서는 제로트러스트 도입을 위한 기업망의 6가지 핵심 요소를 다음과 같이 정의한다. 단, 앞서 언급한 바와 같이 기업망 차원에서 시스템(System)이 명시적으로 기기(Device)와 구분되는 보안 기능을 요구하지 않는 환경에서는 CISA에서 정의한 바와 마찬가지로 별도의 핵심 요소로 판단하지 않고 하나의 핵심요소(기기)로 통합하여 볼 수 있다.

- **식별자·신원 (Identity)**: 사람, 서비스 혹은 IoT 기기 등을 고유하게 설명할 수 있는 속성 혹은 속성의 집합을 의미하며, 기업 혹은 기관은 식별자를 가진 사람 혹은 기기가 리소스에 접근하고자 하면 강한 인증 방식을 사용하여 해당 식별자를 검증하고, RBAC

혹은 ABAC 등을 활용한 세밀한 접근제어 규칙에 따라 적절한 시간 내에 해당 리소스에 접근을 보장할 수 있어야 함.

- **기기 및 엔드포인트 (Device/Endpoint)**: 기기는 IoT 기기, 휴대폰, 노트북, PC, 서버 등을 포함하여 Network에 연결하여 데이터를 주고 받는 모든 하드웨어 장치를 의미하며, 해당 기기는 일반적으로 기관 소유이나 BYOD와 같은 개인 기기일 수도 있음. 기업 혹은 기관은 기기에 대한 목록을 유지하여야 하며, MDM 등의 기술을 활용하여 리소스를 접근하려는 기기에 대한 신뢰도를 평가하는 등 허가받지 않았거나 신뢰할 수 없는 기기가 리소스에 접근하는 것을 막을 수 있어야 함.

- **네트워크 (Network)**: 네트워크는 기업망의 유무선 네트워크, 클라우드 접속을 포함하는 인터넷 등 데이터를 전송하기 위해 사용되는 모든 형태의 통신 매체를 포함하며, 기업 혹은 기관은 네트워크 환경을 작은 단위로 나누어 접근을 제어하고, 내외부 데이터 흐름을 관리할 수 있어야 하며, 특히 공격자가 접근해서는 안 되는 네트워크로 이동하는 것을 방지할 수 있어야 함.

- **시스템 (System)**: 시스템은 중요 응용 프로그램을 구동하거나 중요 데이터를 저장하고 관리하는 서버들을 포함하며, 온프레미스(On-Premise) 및 클라우드에 구축 운용 중인 모든 서버 시스템들이 여기에 해당함. 시스템 관리자 또는 개발자가 시스템에서 루트 계정과 같은 주요 권한 자격자로 접속하여 시스템을 관리하고 제어하는 경우, 시스템의 주요 파일의 읽기 및 쓰기, 주요 명령어 사용 등 시스템 리소스 접근에 관한 세밀하고 상세한 접근제어가 이루어져야 하며, 매 세션마다 다중 인증(MFA) 등 강력한 신원 확인 및 위험 관리 절차를 포함하여야 함.

- **응용 및 워크로드 (Application & Workload)**: 응용 및 워크로드, 이에 연관된 API는 기업망 관리 시스템, 프로그램, 온프레미스 및 클라우드 환경에서 실행되는 서비스를 포함하며, 데이터를 주고받기 위한 인터페이스를 제공함. 기업 혹은 기관에서는 응용 계층 및 컨테이너, 가상 머신 등을 보호·관리하고 데이터의 안전한 전달을 보장할 수 있어야 함.

- **데이터 (Data)**: 기업 혹은 기관에서 가장 최우선적으로 보호해야 할 리소스이며, 기업 혹은 기관은 데이터 목록을 작성, 분류 및 레이블 지정하고, 필요에 따라 암호화 기법을

적용하여 저장 혹은 전송 중인 데이터를 보호하며 허가받지 않은 데이터 유출을 대응하기 위한 기법을 적용하여야 함.
또한, 상기 핵심 요소들에 대해 보안성과 신뢰도에 대한 판단을 강화하고, 적절하고 세밀한 접근제어가 이루어지도록 제로트러스트 아키텍처를 구현하는 기업망에서 2가지 교차 기능이 모든 핵심 요소에 걸쳐 이루어져야 한다.

- **가시성 및 분석 (Visibility and Analytics)**: 사용자 혹은 기기, 응용 및 워크로드의 상태 확인 등 중요하고 상황에 맞는 세부 정보를 이용하여 분석하고 가시성을 제공할 경우, 기업 혹은 기관에서는 비정상 행위에 대한 탐지를 개선하고, 보안 정책 및 접근제어 결정을 동적으로 변화시킬 수 있음. 또한, 네트워크에 대한 원격 감시 이상으로 트래픽을 패킷 단위로 직접 캡쳐하고 분석함으로써, 네트워크를 통해 진입하는 모든 종류의 위협을 관찰하고 지능화된 방어 기법을 적용하여야 함.

- **자동화 및 통합 (Automation and Orchestration)**: 기존에 수동적으로 적용하던 보안 프로세스를 개선하여 자동화된 정책 기반 보안 프로세스를 적용할 경우, 보다 신속한 보안 조치가 가능해질 수 있음. SIEM 및 기타 자동화된 보안 솔루션 통합, SOAR 적용 등의 방법을 통하여, 제로트러스트 아키텍처를 구현하고자 하는 기업망의 모든 환경에서 정의된 프로세스와 일관된 보안 정책을 시행한다면 자동화된 통합 보안 대응이 가능함.

2. 제로트러스트 성숙도 모델

제로트러스트 아키텍처를 도입하여 구현하고자 하는 기업 혹은 기관에서는 다양한 조직의 요구사항과 함께, 현재 구현·활용 중인 보안 기술 및 솔루션이 모두 다르므로, 이를 바탕으로 제로트러스트 아키텍처를 도입하는 방법과 방향성이 상이할 수 있다. 이러한 특징은, 실제로 구현을 하고자 하는 기업 및 기관 보안 담당자들에게 제로트러스트에 대한 구체적인 이해와 도입 계획을 수립하는데 있어 어려움을 주게 된다.

완전한 제로트러스트 도입·구현을 위해 가장 먼저 필요한 것은 제로트러스트 도입을 위한 기업망의 핵심 요소들에 대한 분류와 함께, 현재 기업망에 대한 제로트러스트 관점에서의 성숙도 수준을 정확히 이해하는 것이라고 할 수 있다. 제로트러스트 아키텍처는 기업망에

포함된 모든 핵심 요소들에 제로트러스트 철학을 담고 있는 모든 기술들이 유기적으로 반영되어야 하므로, 가장 완전한 수준으로 한 번에 구현하는 것은 불가능하다. 또한 현재 기업망에 적용되어 있는 모든 레거시 보안 솔루션들이 제로트러스트의 철학이 전혀 반영되어 있지 않다고 볼 수도 없을 것이다.

따라서, 여기에서는 제로트러스트의 성숙도를 여러 단계로 분류하고, 각 핵심 요소마다 성숙도 단계에서 가지고 있는 특징을 소개함으로써, 현재 기업망이 완전한 제로트러스트 단계로 이전하기 위해 필요한 부분들을 도출하기 위한 기초 자료로 활용할 수 있도록 한다.

〈표 3-1-2〉 각 기업/기관에서 정의한, 제로트러스트 성숙도 단계

성숙도 모델 발표기관	Microsoft[22]	NSTAC[23]	DISA/NSA(DoD)[24]	CISA[25]
기관별 성숙도 단계	▸ Traditional ▸ Advanced ▸ Optimal	▸ Initial ▸ Repeatable ▸ Defined ▸ Managed ▸ Optimized	▸ Baseline ▸ Intermediate ▸ Advanced	▸ Traditional ▸ Initial[26] ▸ Advanced ▸ Optimal

이미 각 기업 혹은 기관에서 발표한 제로트러스트 성숙도 모델 단계는 〈표 3-1-2〉와 같다. 단계에 대한 표현이나 의미, 전체 단계가 일부 다르지만, 전반적으로는 현재, 중간, 최적의 3단계로 나누어 기술하고 있으며, NSTAC에서는 총 5단계로 분류하여 다른 기업·기관이 발표한 3단계보다 더 세분화되어 있다. CISA의 성숙도 모델은 2021년 6월 공개 버전에서는 3단계였으나, 2023년 4월 발표한 버전 2.0에서는 Initial 단계를 추가한 4단계로 구성되어 있다.

본 문서에서는 많은 기관들이 제시한 바와 같이 국내 제로트러스트 성숙도 모델을 총 3단계 수준(기존, 향상, 최적화)으로 나누어 〈표 3-1-3〉과 같이 기술한다.

---

22 Microsoft, "Zero Trust Maturity Model", 2019년 10월

23 NSTAC, "DRAFT REPORT TO THE PRESIDENT – Zero Trust and Trusted Identity Management", 2022년 2월

24 DISA and NSA, "Department of Defense (DOD) Zero Trust Reference Architecture Version 2.0", 2022년 7월

25 CISA, "Zero Trust Maturity Model (Version 2.0)", 2023년 4월

26 버전 2.0에서 추가된 성숙도 수준 (버전 1.0에서는 없었음)

〈표 3-1-3〉 제로트러스트 성숙도 모델 3단계 수준

성숙도 수준	해당 수준의 의미	해당 수준에서 요구하는 보안 기술 특징
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)	‣ 수동 설정 및 속성 부여, 정적 보안 정책 ‣ 온프레미스 ID (때때로 SSO 및 다중인증방식 적용) ‣ 외부 시스템에 대해 정밀하지 않은 종속성을 가진 핵심 요소별 솔루션 ‣ 프로비저닝에서 최소 기능 구축 ‣ 정책 적용에서 독점적이고 유연하지 않은 핵심 요소 ‣ 수동적인 사고 대응 및 완화 배포
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)	‣ 세밀한 수준에서의 사용자 및 기기 접근제어 ‣ 중앙 집중적 ID 제어 및 정책 적용, 상태 평가에 기반한 일부 최소 권한 변경 ‣ 네트워크가 일부 세분화되어, 전체 환경에 영향을 미치는 공격의 위험이 줄어듦 ‣ 일부 핵심 요소간 정합 ‣ 중앙 집중적 가시성 부분 제공 ‣ 사전 정의된 완화 기법을 통한 일부 사고 대응 ‣ 외부 시스템과 종속성 측면에서 세부 정보 증가
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)	‣ Federated ID 및 싱글사인온 등 ID 통합 관리 및 지속적 신원 및 신뢰도 검증, 자동화/실시간 분석을 통한 동적 접근제어 ‣ 자산 및 리소스에 대한 완전 자동화된 속성 부여, 최소 권한 접근을 위한 종속성 부여 ‣ 네트워크는 고유한 접근 규칙을 갖는 세분화된 영역으로 구분 ‣ 핵심 요소간 상호운용성을 위한 개방형 표준을 통한 조정 ‣ 특정 시점의 상태 기억을 위한 히스토리 기능을 가진 중앙 집중적 가시성 제공

위에서 언급한 제로트러스트 성숙도 수준은 기업망이 가지고 있는 6가지 핵심 요소별로 다시 정리할 수 있다. 앞서 언급한 바와 같이, 각 기업 혹은 기관은 조직의 요구 사항과 현재 구현·활용 중인 보안 기술 및 솔루션이 모두 다르기 때문에, 제로트러스트 아키텍처를 도입하여 최적화 수준으로 진행하기 위하여 핵심 요소별로 각 수준에서 요구하는 보안 기술의 특징을 분석하고 현재 기업의 상태를 이해함으로써 추가적으로 도입하여야 하는 기술의 특징을 이해할 수 있을 것이다.

각 핵심 요소에 따르는 성숙도 수준별 보안 기능에 대해서는 CISA의 성숙도 모델

버전 1.0을 참고하되, CISA의 핵심요소로 포함되지 않은 시스템 영역에 대해는 추가로 기술하였다.

가. 핵심 요소 1: 식별자·신원

〈표 3-1-4〉 식별자·신원에 대한 성숙도 수준별 특징

기능	기존 수준	향상 수준	최적화 수준
식별자 관리	▸ 온프레미스 ID 공급자	▸ 클라우드와 온프레미스 시스템을 기반으로 ID 연합	▸ 클라우드 및 온프레미스 환경 전반에 걸쳐 글로벌 ID 활용
인증	▸ 패스워드 혹은 다중 인증 방식	▸ 다중 인증 방식 기반 인증	▸ 접근 권한을 승인할 때 뿐만 아니라, 지속적인 신원 검증
위험도 평가	▸ 위험에 대한 제한된 결정	▸ 단순한 분석과 정적 규칙을 기반으로 식별자 위험성 판단	▸ 기계학습 알고리즘으로 실시간 사용자 행동 분석을 통해 위험 결정 및 지속적 보호
가시성 및 분석	▸ 기본적이며 정적인 속성을 기반으로 사용자 활동에 대한 가시성 분류	▸ 기본 속성으로 사용자 활동에 대한 가시성 집계 후 분석 및 보고를 통한 수동적 개선	▸ 높은 정확도의 속성, 사용자 및 개체 행동 분석(UEBA) 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(just-in-time)·적절한(just-enough) 접근제어 구현

나. 핵심 요소 2: 기기 및 엔드포인트

〈표 3-1-5〉 기기 및 엔드포인트에 대한 성숙도 수준별 특징

기능	기존 수준	향상 수준	최적화 수준
정책 준수 모니터링	▸ 기기 정책 준수를 위한 제한된 정보 제공	▸ 대부분의 기기에 정책 준수 시행 메커니즘 사용	▸ 지속적인 기기 보안 상태 모니터링 및 검증
데이터 접근제어	▸ 데이터 접근 기기에 대한 정보에 의존하지 않음	▸ 첫 데이터 접근시 기기 상태 고려	▸ 기기에 대한 실시간 위험 분석 고려

기능	기존 수준	향상 수준	최적화 수준
자산 관리	‣ 단순하며 수동으로 추적되는 기기 목록 관리	‣ 자동화된 방법을 이용하여 자산 관리, 취약성 식별, 자산에 대한 패치 적용	‣ 클라우드 및 원격을 포함한 모든 환경에 걸쳐 자산 및 취약점 관리 통합
가시성 및 분석	‣ 기기 관리는 라벨의 수동 검사 및 주기적 네트워크 검색·보고에 의존	‣ 정책 미준수 구성 요소를 격리하며, 기기 목록 재조정	‣ 지속적으로 기기 상태 평가 (예, EDR 툴 사용)
자동화 및 통합	‣ 정적 용량이 할당된 기기를 수동 관리	‣ 정책 기반 용량 할당 및 사후 조정을 통한 자동·반복적 방법을 사용하여 기기 관리	‣ 동적 조정을 통한 지속적 통합·지속적 배포(CI/CD) 원칙

다. 핵심 요소 3: 네트워크

〈표 3-1-6〉 네트워크에 대한 성숙도 수준별 특징

기능	기존 수준	향상 수준	최적화 수준
네트워크 세분화	‣ 대규모 경계·분리를 사용하는 네트워크 구조 정의	‣ 일부 내부적인 세분화를 갖는 송수신 소규모 경계를 통해 더 많은 네트워크 구조 정의	‣ 네트워크 구조는 주변 응용 워크플로우를 기반으로 완벽히 분산된 송수신 세부 경계 및 더욱 깊은 내부 세분화로 구성됨
위협 대응	‣ 알려진 위협 및 정적 트래픽 필터링을 핵심 기반으로 위협 보호 수행	‣ 위협을 사전에 발견하기 위한 기본 분석 포함	‣ 컨텍스트 기반 신호와 기계학습 기반 위협 보호 및 필터링 통합
암호화	‣ 최소한의 내외부 트래픽에 대한 명시적 암호화	‣ 내부 응용에 대한 모든 트래픽 및 일부 외부 트래픽 암호화	‣ 가능한 경우, 내외부로 전달되는 모든 트래픽 암호화
가시성 및 분석	‣ 중앙 집중식 수집 및 분석을 통하여 경계에서 가시성 제공	‣ 수동 정책 기반 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석	‣ 자동화된 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석
자동화 및 통합	‣ 변경 관리 워크플로우에 따라 네트워크 및 환경 변경을 수동으로 초기화 및 실행	‣ 수동으로 네트워크 및 환경 변화를 시작하기 위한 자동화된 워크플로우 사용	‣ 네트워크 및 환경 설정을 위해 지속적 통합·지속적 배포(CI/CD) 배포 모델에 따라, 자동화와 함께 코드로서의 인프라를 사용

라. 핵심 요소 4: 시스템

〈표 3-1-7〉 시스템에 대한 성숙도 수준별 특징

기능	기존 수준	향상 수준	최적화 수준
접근 통제	▸ 시스템 접근을 위한 계정 인증은 로컬 시스템에 저장된 ID/패스워드 등 단순 인증을 기반으로 하고 정적 속성 등 최소한의 권한 분리 정책 적용	▸ 시스템 접근 시 중앙 집중적 인증, 인가, 모니터링과 속성에 의존하며, MFA 인증을 기본으로 시스템 파일, 디렉토리에 접속하거나 주요 명령어를 실행할 때 접근제어 정책에 따라 보안정책 적용	▸ 시스템 접근 시 MFA 인증 및 엔드포인트 시스템의 신뢰도를 기반으로 접근인가 진행. 시스템에 영향을 미치는 명령 실행 시 실시간 신뢰도 재산정 및 위험 분석을 기반으로 강력하고 지속적인 접근제어 정책 적용
시스템 계정 관리	▸ 접근 인가를 진행하는 권한 사용자의 계정 관리가 시스템별로 상이하게 관리	▸ 접근 인가를 진행하는 권한 사용자의 계정 관리가 독립 시스템으로 이루어지고 다른 시스템들과 동기화 및 프로비저닝 됨	▸ 접근 인가를 진행하는 권한 사용자의 계정 관리가 독립 시스템을 기반으로 통합적으로 이루어지고 권한 사용자의 보안 관리 정책이 계정관리와 통합 및 중앙 일원화되어 접근제어 정책이 적용
네트워크 분리 정책	▸ 네트워크 상에서 시스템들이 분리되어 있지 않거나, 중요도 구분 없이 네트워크 경계형 모델을 기반으로 시스템 영역을 구분하고 배치	▸ 일부 시스템을 중요도에 따라 세분화하여 시스템들 간 접속 이동에 있어 보안 정책 적용	▸ 중요 등급 및 기능별 분류, 세분화 및 강력한 시스템 보안 접근 정책을 기반으로 분류 그룹간 이동 통제
시스템 보안 및 정책 관리	▸ 온프레미스 시스템 보안 패치 및 정책 변경은 수동으로 이루어짐	▸ 온프레미스 및 클라우드 시스템에 대한 일관되고 자동화된 보안 패치 가능	▸ 온프레미스 및 클라우드 상의 모든 시스템 보안 상태에 대한 실시간 모니터링, 심각한 위협에 대한 자동화된 보안 패치 및 정책 변경 가능
가시성 및 분석	▸ 외부 센서 및 시스템과 격리된 상태에서 시스템 상태 및 보안 모니터링 수행	▸ 일부 외부 센서와 시스템을 사용하여 컨텍스트 관점에서, 시스템 상태 및 보안 모니터링 수행	▸ 외부 센서와 시스템을 사용하여 지속적이고 동적인 응용 상태 및 보안 모니터링 수행
자동화 및 통합	▸ 시스템 제공시, 응용 호스팅 위치와 접근을 설정	▸ 변경된 상태를 기기와 네트워크 구성 요소에 알림	▸ 보안과 성능 최적화를 위한 지속적인 환경 변화에 적응

마. 핵심 요소 5: 응용 및 워크로드

〈표 3-1-8〉 응용 및 워크로드에 대한 성숙도 수준별 특징

기능	기존 수준	향상 수준	최적화 수준
접근 인가	‣ 응용 접근은 주로 로컬 인가 및 정적 속성에 기반	‣ 응용 접근은 중앙 집중적 인증, 인가, 모니터링과 속성에 의존	‣ 실시간 위험 분석을 고려하여 응용 접근을 지속적으로 인가
위협 보호	‣ 알려진 위협에 대한 범용 보호기법을 적용하여, 응용 워크플로우와 위협 보호에 대한 최소한의 통합	‣ 일부 응용별 보호 기법을 사용하여 알려진 위협에 대한 보호를 적용하여, 응용 워크플로우와 위협 보호에 대한 기본적인 통합	‣ 응용 동작을 이해하고 설명하는 보호 기법을 제공하는 분석을 사용하여, 응용 워크플로우와 위협 보호에 대한 강력한 통합
접근성	‣ 일부 중요 클라우드 응용은 인터넷을 통해 사용자가 직접 접속하며, 그외의 다른 응용은 VPN을 통한 접속	‣ 모든 클라우드 응용과 일부 온프레미스 응용은 인터넷을 통해 사용자가 직접 접속하며, 그외의 다른 응용은 VPN을 통한 접속	‣ 모든 응용은 인터넷을 통해 사용자가 직접 접속 가능
응용 보안	‣ 주로 정적·수동 검사 방법을 통해, 배포 전 응용 보안 테스트 수행	‣ 동적 시험 방법 사용을 포함하여, DevSecOps 형태의 응용 개발 및 배포 과정에 응용 보안 테스트 통합	‣ 배포되는 응용에 대한 정기적인·자동화된 시험을 사용하여, 개발과 배포 과정에서 응용 보안 테스트 통합
가시성 및 분석	‣ 외부 센서 및 시스템과 격리된 상태에서 응용 상태 및 보안 모니터링 수행	‣ 일부 외부 센서와 시스템을 사용하여 컨텍스트 관점에서, 응용 상태 및 보안 모니터링 수행	‣ 외부 센서와 시스템을 사용하여 지속적이고 동적인 응용 상태 및 보안 모니터링 수행
자동화 및 통합	‣ 응용 제공시, 응용 호스팅 위치와 접근을 설정	‣ 변경된 상태를 기기와 네트워크 구성 요소에 알림	‣ 보안과 성능 최적화를 위한 지속적인 환경 변화에 적응

바. 핵심 요소 6: 데이터

〈표 3-1-9〉 데이터에 대한 성숙도 수준별 특징

기능	기존 수준	향상 수준	최적화 수준
데이터 목록 관리	▸ 데이터를 수동으로 분류하고 데이터 목록 작업이 부실하여, 일관되지 않은 데이터 분류	▸ 일부 자동화된 추적을 기반으로, 수동으로 데이터 목록 작업 수행. 수동·정적인 방식을 조합하여 데이터 분류	▸ 강력한 태그 작업 및 추적으로 지속적인 목록 작업. 기계 학습 모델을 사용하여 분류 강화
접근 결정방법	▸ 정적 접근제어를 사용하여 데이터 접근 관리	▸ 식별자, 기기 위험도 및 기타 속성을 고려하는 최소 권한 제어 기법을 사용하여 데이터 접근 관리	▸ 데이터 접근은 적시·적절한 원칙 및 지속적인 위험기반 결정을 지원하며, 동적으로 이루어짐
암호화	▸ 온프레미스 데이터 저장소에 암호화되지 않은 상태로 데이터 저장	▸ 클라우드 혹은 원격 환경에서 암호화 저장	▸ 저장소의 모든 데이터 암호화
가시성 및 분석	▸ 특정 상황을 제외하고는, 유용한 가시성 및 분석을 방해하는 제한된 데이터 목록 보유	▸ 대부분 데이터는 목록화되어 마지막 목록 업데이트 이후 관리 가능. 분석은 평문 데이터에 한정됨	▸ 데이터는 목록화되어 언제든지 관리 가능. 의심스러운 행위에 대한 모든 접근 이벤트 로그 및 분석. 암호화된 데이터에 분석 수행
자동화 및 통합	▸ 자동화 및 통합을 어렵게하는, 일관되지 않은 분류 및 레이블 지정. 일부 데이터 관리 작업은 자동으로 실행	▸ 정기적 감사를 통해 높은 가치의 데이터를 찾고, 접근제어 분석. 접근제어 적용 및 백업 보증을 위한 제한된 범위의 자동화된 통합	▸ 높은 가치의 데이터에 대한 엄격한 접근제어 자동 집행. 높은 가치의 데이터는 모두 저장 위치에 관계없이 백업됨. 데이터 목록은 자동으로 업데이트

제2절 | 제로트러스트 도입 고려사항

1. 도입 고려사항

앞서 언급한 제로트러스트 성숙도 모델에 대해 각 기업과 기관들은 최종적으로는 모든 핵심 요소들에 대하여 최적화 수준에 이르는 것이 목적이 될 것이다. 제로트러스트로의 전환을 목표로 하는 기업 관리자 입장에서는 목표 달성을 위한 전환 및 도입 계획을 수립하여야 하나, 그 전에 고려해야 할 점들이 있다.

이 고려사항은 성숙도 모델 관점에서 도입시 고려해야 할 원칙과 그 외 기술, 문화, 정책, 규제 등 제로트러스트 보안 아키텍처를 출발하기 위한 기업 내외부 환경 관점에서 고려해야 할 사항들이 있을 것이다. 여기에서는 이들을 나누어서 언급하고자 한다.

가. 성숙도 모델 관점에서 도입시 고려해야 할 원칙

기업 관리자는 성숙도 모델을 구성하는 모든 핵심 요소 및 주요 기능들이 최적화 수준에 도달하는 것을 최종적인 목표로 삼고자 할 수 있다. 사실, 가장 높은 수준에만 이를 수 있다면 발생할 수 있는 공격에 효과적으로 대응하고 위험을 최소화할 수 있기 때문에 가장 바람직하겠지만, 그럼에도 기업 관리자는 다음의 3가지 측면을 고려하여야 한다.

첫번째, 최적화 수준은 절대로 단기적으로 달성할 수 있는 목표가 아니다. 모든 핵심 요소들은 유기적으로 동작하며, 1~2가지 보안 솔루션과 단계 계획만으로는 제로트러스트의 최적화 수준에 이를 수가 없다. 현재 기업에서 가장 중요한 핵심 요소를 먼저 파악하고 이들을 중심으로 먼저 성숙도 수준을 높이면서, 자연스럽게 다른 핵심 요소와 주요 기능의 성숙도가 따라갈 수 있는 장기적인 계획과 실천이 필요하다. 실천 과정에서 발생하는 다양한 부작용과 이에 대한 피드백을 지속적으로 계획에 반영·수정하면서 진행해야 궁극적인 목표를 달성할 수 있을 것이다.

두번째, 이 성숙도 모델은 제로트러스트 전환을 위한 여러 경로 중 하나로 볼 수 있으며, 반드시 한 가지 경로만 존재하는 것이 아니라는 점이다. 어떤 경로를 선택하는 것이 바람직한지, 혹은 어떤 핵심 요소를 우선 진행하는 것이 좋을지는 각 기업 혹은 기관별 상황에 따라 다를 것이다. 아래에서는 이러한 도입 전략에 도움을 주기 위하여, 각 핵심

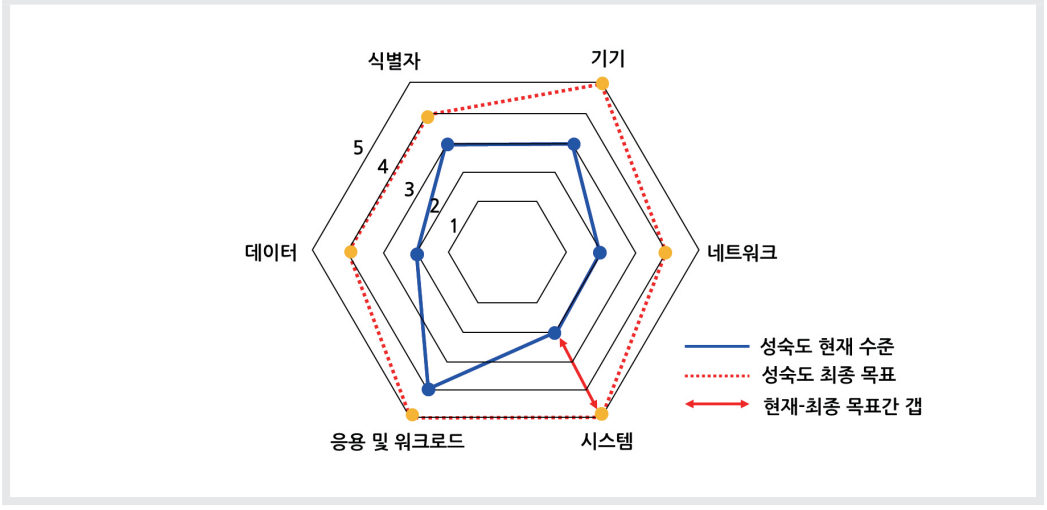
요소가 제로트러스트 성숙도 수준에서 가지고 있는 특징 및 다음 단계로 나아가기 위한 준비 사항 등을 언급하고자 한다.

세번째, 모든 기업이 반드시 모든 핵심 요소와 주요 기능에 대하여 최적화 수준에 도달해야 할 필요가 있는 것은 아니다. 기업의 규모, 기업망의 구성 방식, 접근 주체와 리소스의 종류, 보유 자산에 대한 관리 수준과 필요성 등을 고려하여, 최종적인 목표를 스스로 설정하는 것이 바람직할 것이다.

세번째 원칙과 관련하여, 최종적인 목표를 스스로 설정하였다면 기업 관리자는 기업의 현재 성숙도 수준을 평가하고, 그 평가를 바탕으로 목표 성숙도 레벨을 달성하기 위하여 필요한 업무를 정리하고, 이를 실행하기 위한 리소스 투입량 및 예산, 우선 순위를 정하여 제로트러스트 도입을 준비할 필요가 있다.

만약 기업의 최종적인 목표와 현재 성숙도 수준이 모두 정리가 되었다면, [그림 3-2-1]과 같은 다이어그램을 표현하는 것이 가능할 것이다. 물론, 반드시 이 형태로 표현해야 하는 것은 아니지만, 현재와 목표 사이의 갭(Gap)을 한 눈에 파악할 수 있으며, 앞의 성숙도 모델과 비교하여 어떤 업무들이 필요한지 보다 빠르게 알아낼 수 있는 형태로 정리하는 것이 바람직하다. 이렇게 해서 갭을 기준으로 필요한 업무, 예산, 우선 순위 등을 정리한다면, 이를 고려하여 기관별 목표 일정을 구체화할 수 있을 것이다.

[그림 3-2-1] 제로트러스트 성숙도 목표 다이어그램의 예시



나. 기업 내외부 환경 관점에서의 고려 사항

기업이 성공적으로 제로트러스트 아키텍처를 도입하기 위해서는 앞서 언급한 바와 마찬가지로, 기술, 기업문화, 정책, 규제 등에 대해서도 중요하게 검토하여야 한다. 이는 앞서 언급한 현재의 수준과 최종 목표와의 갭을 해결해나가기 위하여 어떤 업무들이 필요한지 파악하는 데 도움이 될 수 있다. 〈표 3-2-1〉과 같은 질문을 할 수 있는데 이는 하나의 예시일 뿐으로 기업의 특성과 내외부 환경에 따라 이루어져야 할 것이다.

〈표 3-2-1〉 기업 내외부 환경 관점에서 제로트러스트 도입시 가능한 질문의 예

구분	질문
1	조직이 사용하고 있는 기존 보안 솔루션은 무엇인가?
2	어떤 종류의 데이터/서비스를 사용하고 있는가?
3	현재 사용 중인 클라우드 서비스는 무엇인가?
4	사용자 및 단말간 접근 통제는 어떤 형태로 구현·운영하고 있는가?
5	ID는 어떻게 관리되고, 어떤 툴로 구현됐는가?
6	리소스에 대한 접근제어 정책은 어떻게 관리하고자 하는가?
7	기존에 도입하여 운용 중인 망분리 솔루션을 계속하여 유지할 것인가?
8	SOAR 솔루션 도입시 운용중인 인증, 접근제어 솔루션과 연동되는가?
9	현재 온프레미스로 운용 중인 응용과 데이터를 클라우드로 이전할 것인가?

- **기술**: 기존 기술들은 주로 경계 기반 보안 관점에서 보안 기능을 제공해 왔으며 많은 기업들이 현재까지도 이러한 기술들을 채택하고 있다. 제로트러스트 구현 관점에서 현재 기업이 사용하고 있는 레거시 기술에 대한 파악과 함께, ICAM(신원증명 및 접근관리), SDN(소프트웨어 정의 네트워크), Micro-Segmentation 환경, IAP(신원인식 프록시), NAC, SASE, SDP 등 제로트러스트에 관한 핵심 기능을 갖춘 기업의 기술과 솔루션을 지속적으로 모니터링함으로써, 기존 기술을 대체·보완하는 방법을 파악할 필요가 있다.

- **기업 문화**: 제로트러스트를 도입하기 위해서는, 변화에 대응하고 새로운 기술을 받아들이는데 적극적인 문화를 가진 기업이 유리하며, 결정권자 및 이해관계자가 제로트러스트의 필요성을 인지할 수 있는 적극적인 노력이 중요하다.
- **정책**: 제로트러스트 아키텍처를 도입하는 경우, 접근 주체가 리소스에 접근할 때에 대한 정책이 모두 변경될 것이다. 이는 기업에 있어, 모든 인프라와 응용, 데이터 전체에 영향을 끼칠 것이나, 모든 이해관계자가 이를 긍정적으로 평가하지 않을 수 있다. 특히, 클라우드와 온프레미스가 혼합된 환경, 다양한 형태의 기기가 활용되는 환경 등에서 접근제어 정책과 신뢰도 평가 알고리즘을 정교하게 설정하는 것은 매우 어려울 수 있음을 이해하고, 신중하게 접근하여야 한다.
- **규제 환경**: 사이버 위험을 줄이기 위한 국가 차원의 표준이나 지침 등이 존재할 수 있다. 예를 들어, 미국에서는 NIST에서 발행한 위험 관리 프레임워크나 사이버 보안 프레임워크 등이 있으며, 이들 프레임워크는 보안 평가, 구현, 인가, 모니터링 등에 대한 지침을 제공한다. 제로트러스트와 관련해서는 2021년 5월 12일, 바이든 대통령의 '국가 사이버 보안 개선'을 위한 행정 명령(EO-14028)은 연방 정부가 사이버 보안을 개선하기 위하여 취해야 할 조치 중 하나로 제로트러스트 아키텍처를 도입할 것을 언급하였으며, 백악관 산하 관리예산실(OMB)은 제로트러스트 사이버 보안 원칙을 향한 미 연방 정부 전략에 관한 각서를 발표한 바 있다. 우리 나라의 경우에도, 예를 들어 공공기관의 사이버 위험을 줄이기 위한 보안적합성 검증 제도, 클라우드 서비스 보안인증 제도라든지, 민간기업의 사이버 위험을 줄이기 위한 정보보호 및 개인정보보호 관리체계 인증 제도 등이 운용되고 있다. 따라서, 기업이나 기관에서는 이러한 규제 환경을 고려한 제로트러스트 도입 계획을 수립하는 것이 중요할 것이다.

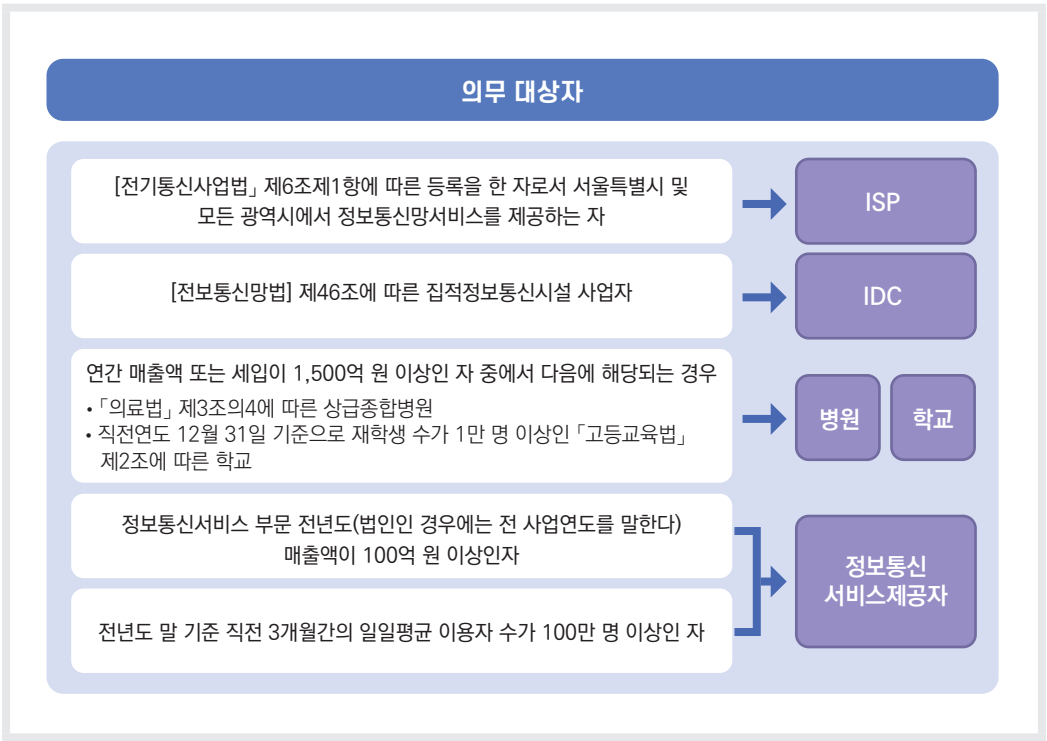
2. 기존 인증 체계와의 연관성

가. 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)

정보보호 및 개인정보보호 관리체계 인증제도는 정보통신망의 안정성 확보 및 개인정보보호를 위해 기업이 수립한 일련의 조치와 활동이 인증 기준에 적합하는지를 인증기관이 평가하는 제도로, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라

함) 제47조와 제47조의2 및 시행령, 시행규칙 등에 따른 정보보호 관리체계 인증 등을 법적 근거로 한다. 정보통신망법 제47조 제2항에 따른 ISMS 의무대상자는 ISMS 또는 ISMS-P 인증을 취득함으로써 인증의무를 이행한 것으로 본다. 여기에서 ISMS 의무대상자의 범위는 다음과 같다.

[그림 3-2-2] ISMS 의무대상자



ISMS 의무대상자로서, 제로트러스트의 도입을 목표로 하는 기업은 제로트러스트 전환을 위해 도입하는 기술적 솔루션들이 ISMS에서 요구하는 보호대책 요구사항을 만족하는지를 계획 단계에서 먼저 확인하여야 할 것이다. 예를 들어, 의무대상자가 운용하는 정보통신서비스를 위한 인터넷 구간 및 서버 구간의 네트워크 시스템과 보안 시스템은 모두 인증범위에 포함될 것이다. 이 구간에서 제로트러스트를 위해 도입된 접근 주체에 대한 인증 및 접근제어 시스템, 소프트웨어 정의 경계 기술 등은 모두 ISMS 인증 상의 보호 대책 요구사항을 만족하여야 한다.

나. 클라우드 서비스 보안인증

클라우드 서비스 보안인증제는 클라우드 서비스 제공자가 제공하는 서비스에 대해 「클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조 제2항에 따라 정보보호 기준의 준수여부 확인을 인증기관이 평가·인증하여 이용자들이 안심하고 클라우드 서비스를 이용할 수 있도록 지원하는 제도이다. 이 제도는 공공기관에 안전성 및 신뢰성이 검증된 민간 클라우드 서비스를 공급하는 것이 목적이다.

〈표 3-2-2〉 클라우드 서비스 유형 및 평가대상

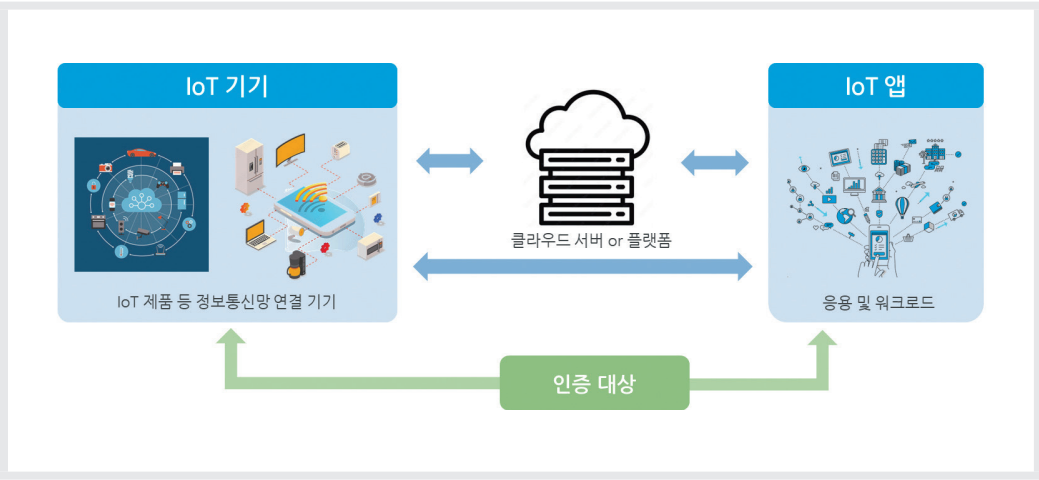
구분	서비스 유형
IaaS	컴퓨팅 자원(CPU), 스토리지 등 정보시스템의 인프라를 제공하는 서비스
SaaS	인프라(IaaS) 외에 각종 응용프로그램(소프트웨어)을 제공하는 서비스
PaaS	클라우드 관련 서비스를 개발하는 환경(플랫폼) 제공
DaaS	가상 PC 제공을 위한 서비스 ※ 행정·공공기관 인터넷망 PC 대체를 위해 도입하는 가상PC

따라서, 클라우드 서비스를 도입하여 운용하는 공공기관들이 제로트러스트 도입을 희망하여 클라우드 서비스 및 클라우드 기반 보안 기술(SASE 등)을 새로 채택하고자 할 때 해당 클라우드 서비스를 운용하는 사업자가 적절한 클라우드 서비스 보안인증을 받았는지를 확인하여야 한다.

다. 정보통신망연결기기등 정보보호인증

정보통신망연결기기등 정보보호인증 제도는 IoT제품(및 연동앱) 등 정보통신망연결기기가 일정 수준의 보안성을 갖추었는지를 시험하여 인증 기준에 적합한지를 검증하는 제도이다. 해당 인증 기준으로는 1) 식별 및 인증, 2) 데이터 보호, 3) 암호, 4) 소프트웨어 보호, 5) 업데이트 및 기술지원, 6) 운영체제 및 네트워크 보안, 7) 하드웨어 보안 등 7개 영역에 대해 평가를 한다.

[그림 3-2-3] 정보통신망연결기기등 정보보호인증 대상



일정 수준 이상의 보안성을 갖춘 IoT기기의 사용이 필요한 기업 혹은 기관에서는 해당인증을 받은 제품을 사용하는 것이 바람직하다. IoT기기에 대한 인증유형으로는 라이트(Lite), 베이직(Basic), 스탠다드(Standard)로 나뉘는데, 이는 IoT기기의 성능(센서 등 소형IoT기기, 저사양 OS탑재 중소형 IoT기기, 중대형 스마트가전 기기 등으로 분류)에 따른다.

제로트러스트를 도입하는 기업이나 기관에서, 이 정도의 기능요구사항은 필수로 생각되며, 해당 인증을 받은 제품을 도입하는 것이 바람직할 것이다. IoT기기는 그 자체로 특정한 리소스에 접근하고자 하는 기기로서 동작할 수도 있고, 센서 데이터 등을 제공하는 리소스일 수도 있다. IoT앱의 경우, 응용 및 워크로드의 하나로 볼 수도 있다. 따라서 각 인증유형에 따라서 제로트러스트 성숙도 수준을 분석할 수 있을 것이다.

제3절 | 제로트러스트 도입 단계

제로트러스트 아키텍처를 도입하기 위해서, 기업에서 가장 중요한 행위는 현재 수준을 평가(Assessment)하는 것이다. 현재 기업에서 업무를 수행하는데 있어 활용하고 있는 업무 프로세스 내지는 워크플로우에 대한 정확한 파악을 통해, 어떤 접근 주체가 어떤 리소스에 접근하는 것을 허용하는지를 알 수 있을 것이며, 접근 주체와 리소스에 대해서도 명확한 식별이 있어야 할 것이다.

앞서 언급한 바와 같이, 기업이 단기간에 제로트러스트의 최적화 수준으로 이행하는 것은 거의 불가능하다. 부분적으로 제로트러스트의 성숙도 수준을 상승시키는 것을 수차례 반복 진행하는 것이 바람직할 것이다. 기업은 2가지 관점에서 부분적인 성숙도 상승 단계를 올리는 방향으로 제로트러스트 아키텍처를 도입하거나 고도화할 수 있을 것이다.

첫번째로는 기업망의 핵심 요소 중 특정한 하나의 요소부터 초점을 맞추는 것이다. 예를 들어, 첫번째 단계로 식별자 중심의 제로트러스트 도입에 초점을 맞추는 기업의 경우, 주요 업무에 포함된 접근 주체 중 특히 사용자에 대한 식별자부터 현황을 파악한 후, Federated ID 기반의 IAM, ICAM 등의 관련 솔루션을 도입·전환하는 일부터 시작할 수 있을 것이다.

이 경우, 식별자부터 제로트러스트 성숙도를 높이고 해당 기능에 대해 검증한 후, 기기와 네트워크, 응용, 데이터 등의 성숙도를 차례로 올려 나가는 전략이 될 수 있다. 이 방법의 단점은 시작단계부터 수많은 업무와 연관됨으로써 기능 검증이 오래 걸릴 수 있다는 점이다. 또한, 현재의 핵심 요소에 지나치게 집중하여 다른 핵심 요소를 고려하기 전에 현재 핵심 요소에 대한 성숙도를 최적화 수준으로 달성하는 것이 현실적으로 불가능하다는 점도 고려하여야 한다. 현재 핵심 요소에 대해 적정한 목표를 달성하면, 다른 핵심 요소에 대해서도 같이 고려하는 것이 바람직하다.

두번째로는 특정 비즈니스 프로세스부터 시범적으로 제로트러스트의 도입을 시작하는 것이다. 이 경우에는, 프로세스에 연관된 사용자, 기기, 관련 리소스와 그에 연관된 정책을 명확히 파악하고 강화된 인증 기법과 접근제어 정책을 기반으로 한 마이크로 세그멘테이션과 소프트웨어 정의 경계 기능을 포함시킨 후, 이 프로세스에 관한 워크플로우

연동 시나리오를 정립하고 이를 실행해가면서 기능을 검증하는 것이다.

이 방법의 단점은 개별 프로세스마다 연관된 기업망의 핵심 요소들이 많으며, 이들을 모두 고려한 제로트러스트 솔루션을 도입하여야 하므로 초기부터 도입 시간과 비용이 커질 수 있다. 그러나, 기능 검증 항목이 워크플로우에 연관되어 비교적 범위가 좁혀지므로 검증 시간이 적게 들 수 있다. 일반적으로는 비즈니스 프로세스를 기반으로 제로트러스트 아키텍처 도입에 접근하는 것이 더 효율적일 가능성이 높다. 그럼에도 불구하고 해당 비즈니스 프로세스를 통해 제로트러스트의 모든 보안 기능 목표를 검증하는 것이 어렵다면, 첫 번째 방법과 마찬가지로 이 비즈니스 프로세스 내에서 식별자 및 기기 등 일부 핵심 요소에 초점을 맞추는 것도 전략이 될 수 있다.

NIST SP 800-207에서는 제로트러스트 전환 단계에 대하여, 기업이 제로트러스트 아키텍처 도입을 시작하기 전 자산과 접근 주체, 데이터 흐름, 워크플로우 등에 대해 조사해야 한다고 명시하고 있다. 정책 엔진은 리소스의 요청을 평가할 때 이에 대한 지식이 있어야 하는데, 이 지식이 완벽하지 않으면 불충분한 정보로 인하여 정책 엔진이 정상적인 요청을 거부할 가능성이 있다. 따라서, 현재의 운영 상태를 명확히 파악하여야 하며, 그를 바탕으로 어떤 신규 시스템이나 프로세스가 필요한지를 결정하여야 한다.

제로트러스트 아키텍처를 도입하기 위한 단계는, NIST SP 800-37의 위험 관리 프레임워크에서 제시하는 각 단계(〈표 3-3-1〉)와 대응할 수 있다. 제로트러스트 아키텍처 채택 그 자체가 기관의 업무 기능에 대한 위험을 줄여줄 수 있기 때문이다.

〈표 3-3-1〉 NIST SP 800-37 위험 관리 프레임워크의 단계

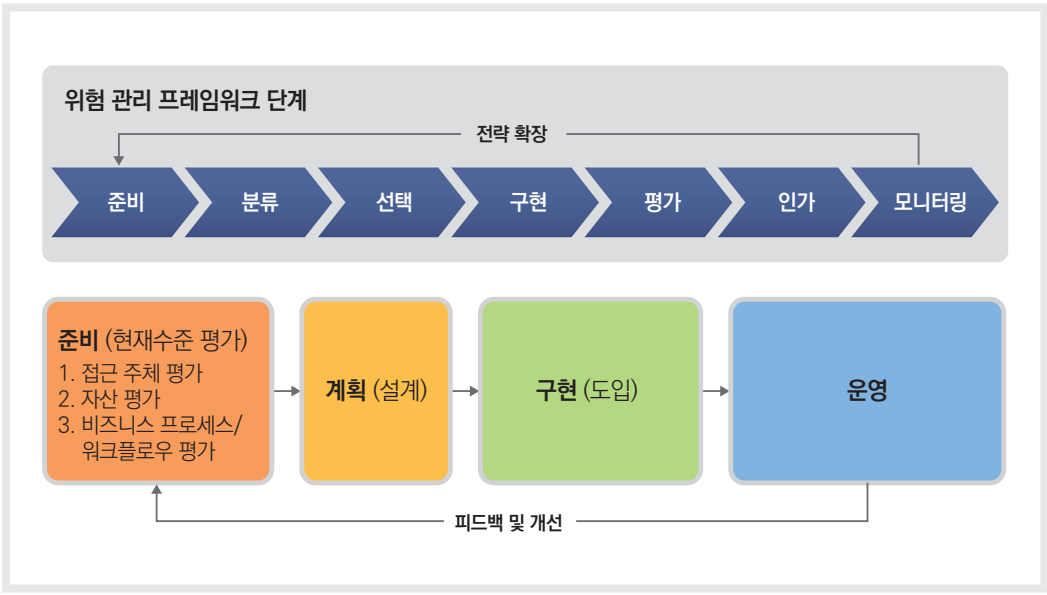
단계	의미
준비	조직이 보안과 프라이버시 위험을 관리하기 위해 준비하는 필수 활동
분류	영향 분석에 기반하여 처리, 저장, 전송되는 시스템 및 정보 분류
선택	위협 평가에 기반하여 시스템을 보호하기 위한 NIST SP 800-53 제어 세트 선택
구현	제어 구현 및 제어 배포 방법 문서화
평가	제어가 제자리에서 의도한 대로 작동하며 원하는 결과를 생성하는지 판단하기 위한 평가
인가	상급 관리자는 시스템 작동을 인가하기 위해 위험 기반 결정
모니터링	제어 구현 및 시스템에 대한 위험을 지속적으로 모니터링

본 문서에서는 제로트러스트 아키텍처를 도입하기 위한 단계를 다음과 같이 정리한다. '준비→계획→구현→운영→피드백 및 개선'의 한 사이클이 돌면서 운영이 이루어지면, 최초로 계획했던 제로트러스트 아키텍처가 원하는 목표에 맞게 정상적으로 운영되고 있는지를 확인할 수 있을 것이다.

운영 중에도 사용자들로부터 다양한 형태의 피드백 및 개선 요구들이 발생할 수 있으며 또한 더 높은 수준의 제로트러스트 성숙도 목표를 세우거나 재검토할 수도 있을 것이다. 다음 목표에 대하여, 첫번째 사이클과 마찬가지로 현재 수준을 재평가하고 그에 맞게 계획을 세워, 구현, 운영, 피드백 및 개선 등을 통한 두번째, 세번째 사이클까지 적용하면 최적화 수준의 제로트러스트 성숙도 수준으로 점점 나아갈 수 있을 것이다.

첫번째 제로트러스트 아키텍처 도입 과정에서 다양한 문제가 발생할 가능성을 고려한다면, 적당한 규모의 비즈니스 프로세스를 선정하여 파일럿 프로그램 형태로 시도하는 것도 하나의 방법이 될 수 있다.

[그림 3-3-1] 제로트러스트 도입 단계



1. 준비 단계 (현재수준 평가)

준비 단계에서는 기업이 제로트러스트 아키텍처 도입을 위하여, 현재 기업의 상황과 현재 수준을 정확히 파악하고 평가하는 것을 목표로 한다. **제로트러스트아키텍처의 도입은 단 한 번의 절차로 완료되지 않는다.** 따라서 준비 단계는 제로트러스트 아키텍처를 처음으로 도입할 때의 가장 첫 단계이기도 하지만 기 도입하여 운영 중인 제로트러스트 아키텍처 및 관련 솔루션에 대하여 더 높은 수준의 성숙도를 갖기 위한 준비 단계로 볼 수도 있다. 이 준비 단계에서, 각 기관 혹은 기업은 현재 운용 중인 기업망에서 접근 주체, 자산·기기 및 워크플로우을 점검하여 정확히 식별하고, 제로트러스트 성숙도 수준을 정량적으로 평가할 수 있어야 한다.

가. 접근 주체 식별 및 성숙도 평가

첫번째 평가 대상은 접근 주체로서, 사용자뿐만 아니라 리소스와 상호 작용을 하는 모든 접근 주체를 의미한다. 접근 주체에 대한 식별 정보, 인증 방법 등을 점검하고 명확하게 파악하는 것은 기본이며, 정확히 분류하고 분류한 접근 주체 그룹에 따라 인증 방법 및 접근제어 정책 등을 검토하여야 한다.

특히, 개발자 및 시스템 관리자와 같이 특수 권한을 가진 사용자에게 어떤 속성이나 역할을 할당하여야 하는 경우 정밀한 조사가 필요하다. 제로트러스트 아키텍처를 도입하기 전 또는 성숙도 수준이 낮은 상태의 보안 아키텍처에서, 특권이 부여된 계정은 모든 리소스에 접근하여 영향을 줄 수 있는 포괄적인 권한을 가질 수도 있으나 이는 제로트러스트 관점에서 바람직하지 않으며 개발자 및 관리자는 업무에 필요한 최소한 권한만을 만족함으로써, 횡적 이동이 불가능하여야 한다. 또한, 로그와 모니터링, 감사를 통해 접근 패턴을 식별하고, 비정상적인 접근으로 판단될 경우에 대한 대응 정책 계획도 수립해야 한다.

접근 주체에 대한 성숙도 수준을 평가하는 경우 다음과 같은 부분을 중점적으로 고려하여야 한다.

- 특권이 부여된 계정, 계정의 담당자 식별 및 명시 여부.
- 업무 상 필요한 권한이 적절히 부여되었는지 등 정기적 감사 여부.
- 세부 인증 기술, 싱글사인온(SSO), 다중 인증(MFA) 방법 및 안전성 .

- 지속적인 신원 인증 방법 및 안전성.
- 컨텍스트 기반 인증, 사용자 모니터링 및 행동 분석, 가시성 확보 방법.
- 최소 권한 부여 정책 도입 여부 등.
- 접근제어 기술 및 수준 (ex. RBAC 혹은 ABAC 적용 여부).
- 개발자 및 시스템 관리자와 같은 특수 권한 사용자의 접근 권한에 대한 정밀한 제어 기술.

나. 자산·기기 식별 및 성숙도 평가

제로트러스트 아키텍처의 기본 원리에서 강조되었던 것 중 하나는 사용자 및 기기를 관리하고 강력한 인증이 필요하다는 것이다. 제로트러스트 아키텍처는 사용자 뿐만 아니라 기업 리소스에 접근하는 기기 중에서 기업이 소유한(등록한) 기기와 기업 소유가 아닌 기기를 식별하고 모니터링할 수 있어야 한다.

기업의 자산은 일반적으로 하드웨어로 구성되어 통신 기능을 포함하는 기기(노트북, 핸드폰, 컴퓨터, IoT) 뿐만 아니라, 디지털 정보 및 소프트웨어 컴포넌트(사용자 계정, 응용, 인증서 등)를 포함한다. 물론, 기업의 규모와 능력에 따라 모든 자산을 완벽히 이해하는 것은 어려울 수 있다. 그러나, 현재 기업망에 접속하여 리소스에 접근하고자 하는 자산에 대해 식별·구분하여 필요시 등록·관리하고 접근할 수 있는 체계를 갖춰야 한다(예, 에이전트 설치 등).

현 자산의 상태를 실시간으로 모니터링하고 설정할 수 있는 기능이 필요하며, 이는 기업에서 자산에 대한 다양한 현황·상태 정보를 유지할 수 있는 체계가 있어야 함을 의미한다. 이 정보를 통해 정책 엔진이 해당 기기의 리소스 접근에 대해 결정할 수 있어야 한다. 기업의 소유가 아닌 자산이나, 혹은 기업의 소유이나 등록되지 않은 기기 등을 빠르게 판단하고 관리할 수 있는 체계 역시 중요하다. 자산식별 및 관리 솔루션을 보유하고 있는 경우 자산·기기 식별 및 성숙도 평가 관점에서 높게 평가될 수 있다.

자산·기기에 대한 성숙도 수준을 평가하는 경우 다음과 같은 부분을 중점적으로 고려해야 한다.

- 모든 기업 소유 자산 및 담당자, 속성 식별 및 분류 여부.
- 기기 로그인(비밀번호, PIN, 생체 인식 등) 방법 및 안전성.

- 기기에서 제공하는 사용자 인증 방법의 안전성.
- BYOD 단말 보안 및 접근제어 정책.
- 자동화된 단말 등록 및 자산·취약점 관리 수준.
- 기기 상태 및 정책 준수에 대한 실시간 지속 모니터링, 가시성 확보, 검증 방법.
- 등록되지 않은 기기의 접근 권한 차등 부여 혹은 접근 차단 정책, 감시 방법.

다. 비즈니스 프로세스/워크플로우 식별 및 리소스 성숙도 평가

기관은 접근 주체가 리소스에 접근하는 것에 대해 허용/거부에 대한 정책을 결정하기 위해서는 기업 내부의 비즈니스 프로세스와 워크플로우를 평가하는 과정이 필요하다. 비즈니스 프로세스는 리소스에 대한 접근 요청에 대해 허가/거부를 결정할 수 있는 근거가 된다.

제로트러스트 도입 관점에서, 위험도가 낮은 프로세스부터 전환하는 것이 상대적으로 안전하다. 제로트러스트 도입 과정에서 문제가 발생할 경우, 기업에 미치는 영향이 상대적으로 적기 때문이다. 이후, 지속적으로 운영 과정에서의 문제점을 검토하며 문제가 없을 경우, 중요하지만 상대적으로 위험도가 높은 프로세스에 도입하는 것을 고려할 수 있을 것이다.

클라우드 기반 리소스 혹은 원격 근무자가 사용하는 비즈니스 프로세스는 상대적으로 제로트러스트 아키텍처를 도입하기 적합할 수 있다. 기업의 보안 경계를 클라우드로 확장하거나 원격 근무자가 VPN을 통해 기업망에 접근하지 않고도, 기업의 리소스에 접근하는 사용자에 대해 접근 전에 정책을 적용하는 것이 용이해지기 때문이다. 단, 제로트러스트 아키텍처를 도입하는 과정에서, 리소스 접근에 대한 속도, 가용성에 대한 문제가 생길 가능성, 기기의 성능을 떨어뜨릴 가능성, 비즈니스 프로세스와 워크플로우 취약점 발생 가능성 등을 고려해야 한다.

리소스에 대한 성숙도 수준을 평가하는 경우 다음과 같은 부분을 중점적으로 고려하여야 한다.

- 소프트웨어 정의 네트워크 등 네트워크 추상화 및 세밀한 분할 기술.
- 패킷 검사 및 동적 필터링, 암호화 패킷 분석 등 위협 대응 기술.
- 네트워크 암호화 기술.

- 온프레미스·클라우드 시스템 계정 관리 및 접근 통제 기술.
- 응용 및 워크로드 접근에 대한 중앙 집중적 인증·인가 및 실시간 위험 분석.
- 응용 개발·배포와 관련한 DevSecOps 등 적용.
- 자동화된 데이터 분류 및 위험 기반 동적 접근제어 정책.
- (특히 민감한) 데이터 저장시 암호화 기술.
- 데이터 분류 시 중요(민감) 정보 태깅.
- 데이터 분류 기준에 따라 암호화 요구사항 적용.

2. 계획(설계) 단계

사용자와 자산, 비즈니스 프로세스 및 워크플로우에 대한 식별 및 평가가 이루어지면, 제로트러스트를 도입하기 위한 계획을 수립하고 설계하는 단계로 진행할 수 있다. 어떤 비즈니스 프로세스 혹은 핵심 요소에 제로트러스트를 도입하는 것이 좋은지를 판단하고, 선정된 비즈니스 프로세스에 대해서는 중요성과 관련 접근 주체 및 리소스 현황을 파악하여, 이를 고려한 정책을 수립하여야 한다. 현재 상태에는 현재 도입되어 있는 제로트러스트 아키텍처 기술에 대한 성숙도 수준을 포함할 수 있으며, 정책에는 현 단계에서 지향하는 제로트러스트 아키텍처 성숙도 수준을 포함할 수 있다. 비즈니스 프로세스가 결정되고 나서도, 기업망의 핵심 요소별 세부 계획을 분할하여 접근하는 시도도 가능하다.

비즈니스 프로세스와 연관된 자산과 워크플로우가 식별되면, 해당 워크플로우에 연관된 모든 리소스와 접근 주체를 식별하여야 한다. 연관된 접근 주체와 리소스의 범위가 크지 않은 프로세스부터 시작하는 것이 상대적으로 용이할 수 있다.

기업 관리자는 도입하는 신뢰도 평가 알고리즘을 고려하여, 해당 프로세스가 사용하는 기준 혹은 중요도에 따른 가중치 혹은 점수를 결정해야 한다. 정상 사용자가 리소스에 접근이 제한되거나, 비정상 사용자가 리소스에 접근하는 경우와 같은 경우를 최소화하기 위하여 도입 단계 및 운영 단계에서 지속적으로 조율하는 과정을 거쳐야 할 수 있다.

3. 구현(도입) 단계

비즈니스 프로세스 후보가 구성되면, 제로트러스트 아키텍처를 설계하는 기업 담당자는 제로트러스트 솔루션 후보에 대한 목록을 작성할 수 있다. 앞서 2.2절의 2에서 언급한 것처럼 여러 배치모델이 있으며, 유스케이스에 따라 적합한 솔루션을 선택해야 할 수도 있다. 솔루션을 선택함으로써 제로트러스트 아키텍처 를 구현·도입하는 현 단계에서는 다음과 같은 점을 고려해야 한다.

- 도입을 위해 검토하는 솔루션이 제로트러스트 아키텍처 기본 원리를 준수하는가? 예를 들어, 리소스에 대한 접근은 반드시 강력한 인증 등을 통하여 접근 주체에 대한 신뢰도를 명시적으로 확인한 뒤 허용하는가?
- 기기에 에이전트와 같은 소프트웨어 컴포넌트를 설치하는가? 다양한 기기를 지원하는가? BYOD 혹은 외부 사용자 기기에 에이전트 설치를 지원하는가?
- 해당 비즈니스 상의 리소스 위치(클라우드, 온프레미스)를 모두 혹은 부분적으로 지원하는가?
- 분석을 위한 로그 및 모니터링 정보를 주고받거나, API를 제공하는가?
- 다양한 응용, 서비스, 프로토콜을 지원하는가?
- 특정 서비스 혹은 프로토콜 상의 명령(예, SSH 기반 컴파일, 명령어 제어, 파일 제거 등)에 대한 통제 등 세밀한 접근제어가 가능한가?
- 강화된 정책이 사용자 및 기기의 행위에 영향을 주는가? 또한, 사용자의 편의성을 희생시키지 않는가?

4. 운영 단계

제로트러스트 솔루션이 도입되어, 특정 비즈니스 프로세스에 대한 제로트러스트 아키텍처 보안 모델이 구현되었다면, 기업 관리자는 운영 단계에 진입하게 된다. 기업 관리자는 해당 솔루션을 기반으로, 정책을 설정하고 시행해야 한다. 정상 사용자가 필요한 리소스에 대한 접근이 거부되거나, 어떤 사용자에게 실제보다 과도한 권한이 허락되는 등의 문제가 발생할 가능성이 있으며, 한 번에 완벽한 정책 시행은 일반적으로 불가능하다.

정책 시행 과정에서 민감한 문제가 발생할 수 있다면, 리포팅만 수행하는 모드로 운영할

수도 있다. 리포팅만 수행한다는 것은, 인증 실패시 접근 거부와 같은 기본적인 정책을 제외한 대부분의 접근 요청을 허가하면서 접속 로그를 분석하여 최초 수립된 정책과 비교하는 방식을 의미한다.

물론, 리포팅만 수행함으로써 대부분의 접근 요청을 허가하는 형태의 시범 운영이 보안이나 기업 정책상 불가능할 경우, 기업 운영자는 로그를 주의깊게 모니터링하면서 비정상적인 접근제어가 이루어지는지를 확인해야 하며, 문제가 있다고 판단되는 경우 접근제어 정책을 지속적으로 수정함으로써 운영을 개선해야 한다.

5. 피드백 및 개선 단계

시범 운영이 정상적으로 잘 이루어지면, 관리자의 판단하에 기업이 정상적으로 운영을 하게 될 것이다. 제로트러스트 솔루션이 정상적으로 작동한다면, 성숙도 수준에 맞추어 사용자와 자산, 네트워크를 지속적으로 모니터링하고, 트래픽과 관련 정보를 로그에 기록할 것이다. 여전히 기업 관리자는 필요시 접근제어 정책을 튜닝할 수도 있으나, 해당 조정이 기업망 전체에 심각한 영향을 주지 않도록 특히 유의해야 한다.

운영 과정에서 접근 주체, 리소스 혹은 프로세스의 이해관계자는 운영 개선을 위한 피드백을 제공할 수 있으며, 관리자는 피드백을 적극적으로 장려해야 한다. 이 단계에서 해당 피드백과 운영 경험을 바탕으로 기업 관리자는 제로트러스트 아키텍처를 개선시키고 성숙도를 높이는 다음 도입 계획을 고려해볼 수 있다. 이 경우 첫번째 단계인 접근 주체, 자산, 비즈니스 프로세스/워크플로우에 대해 다시 한번 식별·평가하는 과정을 시작할 수 있다.

현재 운영 중인 제로트러스트 아키텍처와 관련하여, 비즈니스 프로세스, 워크플로우, 접근 주체의 변화, 기업 내부 정책의 변화, 법률이나 기타 지침의 변경 등으로 현재 운영에 대한 변경도 고려할 수 있다. 이 경우, 성숙도를 높이는 형태의 진화가 아닌, 현재 프로세스에 대한 중요한 개선으로 볼 수 있을 것이다.

제4절 | 제로트러스트 도입·운영 시 주의사항

1. 제로트러스트 아키텍처 도입·운영시 발생할 수 있는 위협

제로트러스트는 경계 기반 보안 방식의 단점을 보완하여, 접근 주체와 자산에 대한 엄격한 관리, 접근 주체가 리소스에 접근할 때마다 강력한 인증과 세밀한 접근제어를 기반으로 해당 리소스에만 접근을 허가하며 상시적인 모니터링을 통하여, 기존 기술 대비 추가로 발생할 수 있는 위험을 완화하는 기술이다. 즉, **위험을 완화할 수 있지만 모든 보안 위험이나 공격 가능성을 완벽히 제거할 수는 없음을 이해하여야 한다.**

한편, 이뿐만 아니라 제로트러스트 아키텍처를 구현하였음에도, 해당 구조로 인해 발생할 수 있는 위협도 존재한다. 그러나, **이는 제로트러스트 아키텍처가 근본적인 취약점을 갖는다는 것을 의미하지는 않는다.** 해당 위협들은 대체로 기존 기업망 환경에서도 유사한 공격이 발생할 가능성이 있으며, 다만 제로트러스트에서는 정책 엔진과 정책 관리자의 권한이 막강하고 정책 집행과 관련한 정보를 많이 수집하기 때문에 잘못 운영하지 않도록 유의하여야 함을 뜻하는 것이다. 대부분의 위협은 관리하는 과정에서 완화시킬 수 있으며, 높은 수준의 보안 기술이 도입된다 하더라도 여전히 공격에 대한 가능성을 무시하지 않아야 한다.

NIST SP 800-207에서는 이와 관련하여 〈표 3-4-1〉과 같은 위협을 제시하고, 해당 위협을 완화할 수 있는 방안도 언급하였다. 대부분의 위협들은 위협이 발생할 수 있는 부분에 대한 기록, 모니터링, 감사 등을 통해 해결할 수 있으며, 시스템 정보 등 주요 데이터 및 정책 관련 논리 구성 요소에 대해서 엄격한 접근제어를 하거나, 더 강력한 보안을 적용하는 것이 바람직하다.

〈표 3-4-1〉 제로트러스트 아키텍처 도입·운영시 발생할 수 있는 위협 및 완화 방안

위협		내용
제로트러스트 아키텍처 결정 과정 무력화	위협 내용	‣ 정책 엔진의 규칙을 설정할 수 있는 기업 관리자가 승인없이 규칙을 변경하거나 기업 운영에 지장을 주는 실수 ‣ 정책 관리자에 대한 직접적인 침해를 통한 승인되지 않는 접근 허용
	위협 완화 방안	‣ 정책 엔진 및 정책 관리자를 적절하게 설정·모니터링 ‣ 모든 설정 변경을 반드시 기록·감사
DoS 또는 네트워크 장애	위협 내용	‣ 공격자가 정책집행지점, 정책 엔진 또는 정책 관리자에 대한 접근 방해/거부 (서비스 거부 공격 혹은 라우팅 가로채기) ‣ 호스팅 제공자에 의해 정책 엔진 또는 정책 관리자 오프라인 ‣ 알 수 없는 이유로 정책 관리자가 기업 리소스에 연결되지 못함
	위협 완화 방안	‣ 이들 시스템을 적절하게 보호되는 클라우드 환경에서 운영 ‣ 혹은 사이버 내성에 관한 지침에 따라 여러 위치에 복제 (단, 이러한 공격·장애는 기존 VPN에서도 발생할 수 있으며, 원천 봉쇄는 불가능)
인증 수단 도용 및 내부자 위협	위협 내용	‣ 중요한 계정의 인증 수단을 획득하기 위해 피싱, 사회 공학 등의 공격
	위협 완화 방안	‣ 컨텍스트 기반 신뢰도 평가 알고리즘을 통하여, 일반적인 패턴과 다른 리소스 접근 방지
네트워크 가시성	위협 내용	‣ 기업망의 일부 트래픽에 대한 분석의 어려움 (기업 소유가 아닌 접속 자산, 혹은 DPI 수행이 안 되거나 암호화된 트래픽을 조사할 수 없는 경우)
	위협 완화 방안	‣ 내용을 알 수 없더라도 메타데이터(출발지/목적지 IP 주소 등) 등을 활용하여 공격자 혹은 악성 코드 탐지 ‣ 머신러닝 기반 트래픽 분석 등
시스템/ 네트워크 정보 저장소	위협 내용	‣ 모니터링, 네트워크 트래픽, 메타데이터 등 분석용 데이터는 일반적으로 공격자의 타깃이 될 수 있음
	위협 완화 방안	‣ 중요 기업 데이터는 가장 엄격한 접근제어 정책 설정
전용 데이터 규격 또는 솔루션에 대한 의존	위협 내용	‣ 데이터(주체 식별정보, 자산, 위협 인텔리전스 등) 입력 요소들의 전용 데이터 규격 혹은 솔루션 사용으로 인한 상호 운용성 문제 발생 ‣ 혹은 보안 이슈 및 장애로 인한 막대한 교체 비용 및 시간 소요
	위협 완화 방안	‣ 데이터 입력 요소를 도입하기 전, 업체의 보안 통제, 교체 비용, 공급망 위험 관리, 성능, 안전성 등을 종합적으로 고려하여 평가 후 도입
비인간 객체에 의한 제로트러스트 아키텍처 관리	위협 내용	‣ 인공지능 혹은 소프트웨어 기반 에이전트의 인증 문제 ‣ 자동화된 기술이 기업의 보안 상태에 영향을 줄 수 있는 오탐과 미탐 가능성 ‣ 공격자가 비인간 객체 접속을 통해 권한이 없는 태스크를 수행하게 함
	위협 완화 방안	‣ 오탐, 미탐에 대해 정기적인 분석 및 수정·보완 ‣ 비인간 객체의 접근에 대한 모니터링 및 분석

2. 제로트러스트 아키텍처 도입시 발생할 수 있는 이슈

기업 네트워크에서 제로트러스트를 구현할 때 솔루션의 효율성을 감소시키는 몇 가지 이슈가 발생할 수 있다.

첫번째 이슈는 기업내 경영진, 관리자 또는 사용자로부터 완전한 지원이 부족할 수도 있다는 점이다. 제로트러스트 도입이 성공하려면 제로트러스트에 필요한 사고 방식을 완전히 받아들여야 한다. 그러나, 기업 대표 등 리더가 이를 구축 및 유지하는 데 필요한 비용과 시간을 투자하지 않으려는 경우, 관리자와 네트워크 방어자에게 제로트러스트 관련 전문 지식이 없는 경우 또는 사용자가 정책을 우회하도록 허용되는 경우 제로트러스트의 이점은 실현되지 않을 것이다. 기본 또는 하이브리드 성숙도 수준의 기능이라도 네트워크에 통합되면, 성숙도를 높이고 완전한 이점을 달성하기 위해 후속 조치가 필요하다. 이는 기업내 모든 직원들이 꾸준히 노력해야 함을 의미한다.

두번째 문제는 제로트러스트 도입으로 인하여 응용이 구동되고 운용되는 기기나 리소스가 탑재된 서버, 정책 관련 논리 구성 요소들이 운영되는 환경 상의 성능이 강력해야 한다는 점이다. 기업망 전체에 걸쳐 제로트러스트 아키텍처가 도입되고 성숙도 수준이 올라갈수록 기능의 확장성이 필수적이다. 레거시 혹은 낮은 성숙도 수준의 제로트러스트 환경에서는 각 접근에 대해 접근제어 결정이 한 번만 발생했을 수 있으나, 리소스에 대한 접근제어가 지속적으로 수행되므로 결정·시행·로그·모니터링을 위한 강력한 인프라가 필요하다. 또한 네트워크 센서와 같이 이전에는 접근제어 결정의 일부가 아니었던 기기들이 신뢰도를 평가하기 위한 필수 요소가 될 수 있다. 지속적으로 인프라를 개선하지 않으면 성능이 떨어지고, 정책이 원활하게 수행되지 않음으로써 사용자의 불편을 초래하거나 정상적인 리소스 접근이 어려워질 수 있다. 한편 첫번째 이슈와 결부하여, 경영진으로부터 충분한 지원을 받지 못한다면 더 이상 도입된 제로트러스트의 성숙도 수준을 높이기 어려울 수도 있을 것이다.

시간이 흘러가더라도, 제로트러스트의 철학을 유지하면서 제로트러스트 아키텍처를 적용하는 것이 반드시 필요하다. 관리자는 기본 거부 보안 정책을 지속적으로 적용하면서 항상 비신뢰와 위반 발생을 가정하는 것에 지칠 수 있지만, 관리자의 제로트러스트 철학이 흔들리면 이 아키텍처로 인한 이점이 크게 저하될 것이다. 이 경우, 제로트러스트 아키텍처로의 전환 및 도입으로 인한 비용 대비 편익이 거의 없어질 것이다.

3장에서 기업망에 제로트러스트 기반 보안 환경을 도입하여 구축하기 위한 도입 절차에 대해서 언급하였다. 그럼에도 기업망은, 기업망에 접근하는 사용자(직원 및 외부 사용자), 접근 기기, 리소스의 종류, 활용 방법 및 중요도, 클라우드 서비스의 활용 여부, 기존에 활용 중인 보안 솔루션 등이 모두 다르며, 한 가지 방식으로 구현될 수 있는 것도 아니다.

따라서, 4장에서는 기업망 혹은 공공망 등에서 현재 가지고 있는 다양한 상황을 고려하여, 이를 개략적으로 분류하고 현재 상태, 목적 및 요구 사항, 제로트러스트 구현을 위해 무엇부터 해야 하는지를 각각의 구현 유스케이스로서 정리하고자 한다. 이들 구현 유스케이스를 참조할 경우, 기업들은 제로트러스트 솔루션은 현재 접근 방식과 어떻게 다르며 해당 기업이 어떤 이점을 얻을 수 있는지와 함께 이러한 이점을 얻기 위하여 어디서 출발을 해야 하는지를 이해할 수 있을 것이다.

ZERO TRUST

제4장

제로트러스트 구현 유스케이스

제1절 | 제로트러스트 구현에 따르는 핵심 요소별 전략

여기에서는 3.1절에서 언급한 기업망의 핵심 요소에 따르는 제로트러스트 구현 전략을 언급한다. 본 절에서 언급하는 구현 전략은 2022년 1월 OMB가 미 연방정부 기관을 대상으로 발표한 '제로트러스트 사이버 보안 원칙을 향한 미 연방정부 전략'을 참고하였으며, 본 가이드라인에서 추가로 언급한 핵심 요소인 시스템에 대해서는 동일한 방식으로 작성하였다. 본 절에서의 구현 전략이 절대적으로 따라야 하는 원칙은 아니지만 제로트러스트 도입 시 고려할 수 있을 것이다.

3.3절 제로트러스트 도입 단계 중 2. 계획(설계) 단계 및 3. 구현(도입) 단계에서 제로트러스트 관련 보안 기술을 선택하고자 할 때 활용할 수 있다.

1. 식별자·신원

가. 목표

기업망에 접근하는 사용자는 기업에서 관리하는 식별 정보를 이용하여 업무에 활용하는 응용에 접근한다. 피싱 등 다양한 공격에 강한 다중 인증(MFA, Multi-Factor Authentication) 기법을 도입함으로써, 더욱 정교한 형태의 온라인 공격으로부터 사용자를 보호할 수 있어야 한다.

나. 전략

1) 전사적 통합 ID 관리 시스템의 활용

기업망에 제로트러스트 아키텍처를 도입·구현하고자 하는 기업 혹은 기관은 ID 관리 시스템과 접근제어 기술을 개선하는 것이 바람직하다. 제로트러스트 아키텍처를 도입·구현하기 위해서는, 도입 기관은 리소스가 정당한 사용자에 의해, 허가받은 시간에, 정당한 목적을 위해 접근하는 것을 보증하여야 할 것이다. 기업이 이를 가능하게 하기 위해서는 사용자의 책임과 권한에 대해 정확히 이해하고, 사용자들이 시스템 혹은 리소스

등에 접근하고자 할 때 정확히 신원을 인증할 수 있는 능력을 갖춰야 한다. 물론, 사용자가 아닌 서비스 혹은 기기에 대한 식별자에 대해서도 마찬가지이다. 이를 가능하게 하는 것은 전사적 차원에서 활용될 수 있는 통합 ID 관리 시스템을 활용하는 것이다.

사용자에 대하여 정확한 접근제어가 이루어지도록 하기 위해서는, 단순히 인증을 강하게 수행하는 것만으로는 충분하지 않으며, 사용자에 관한 다양한 부가 정보가 결합이 되어야 한다. 예를 들어, 특정 직원이 퇴사하거나, 조직 내에서 새로운 부서로 이동한다든지, 휴직, 출장 등 다양한 상황이 발생하였을 때 인사 관리 시스템과 연동되어 이러한 부가 정보가 실시간으로 업데이트될 수 있어야 할 것이다. 만약 이를 수동으로 처리해야 한다면 기관에게 ID와 접근제어를 위한 관리 부담이 상당할 것이다. 이게 가능해진다면, 보다 효과적으로 비정상적인 행위(예를 들어, 국외 출장 중이 아닌 상태에서 특정 국가로부터 기업망에 접속한다면 정상적으로 보기 어려울 것이다)에 대응하기 수월해질 것이다.

또한, 기업망에 존재하는 수많은 네트워크와 응용, 워크로드, 데이터에 접근하기 위하여 사용자가 매번 개별적인 인증 체계를 이용하여 접속하는 것보다는, 한 번의 로그인을 통해 여러 응용, 기업 내 서버 등에 접속할 수 있는 일관된 인증 및 접근제어를 제공하는 것이 관리 측면에서 유리할 것이다.

또한 이를 더 확장하여 같은 그룹사, 협력 업체나 유관 기관과 ID Federation 등을 이용하여 인증을 공유한다면 다양한 인증 시나리오에 대해서도 일관된 인증 및 접근제어 체계를 갖추기에 좋을 것이다.

2) 기업망에서 다중 인증 기술 활용

제로트러스트 아키텍처에서 강한 인증 기술을 적용하는 것은 필수적이며, 사용자에 대하여 신뢰도에 근거한 다중 인증 기술은 반드시 적용되어야 한다. 기존 VPN 등의 환경에서와 같이 사용자가 단순히 네트워크에 접속할 때 다중 인증을 받는 것이 아니라, 위에서 언급한 전사적 ID 관리 시스템 등을 통하여 응용 계층에 통합되는 것이 바람직하다.

예를 들어, 기업망에서 특정한 리소스에 접근하는 것이 인터넷과 같은 공개된 망에서 접근하는 것보다 상대적으로 안전하다고 생각해서는 안 된다. 따라서 네트워크 접속이 아닌 응용 수준에서 강하게 인증받는 것이 제로트러스트에서는 매우 중요한 철학이며,

제로트러스트의 성숙도가 높은 수준에서는 반드시 그렇게 되어야 한다.

다중 인증 기술이 중요하게 고려되어야 하는 이유는, 기존에 널리 사용되는 각각의 인증 방식에는 취약점이 있기 때문이다. 예를 들어, 패스워드 기반 인증은 취약한 혹은 노출된 패스워드를 사용함으로써 생기는 취약점이 있을 수 있는데, 이는 생체 혹은 OTP 기반의 인증 방식 등을 추가로 활용함으로써 어느 정도 극복이 가능하다. 물론, 그렇다고 해서 모든 경우에 반드시 다중 인증 기술이 적용되어야 하는 것은 아니며 또한 다중 인증 기술을 사용한다고 해서 모든 종류의 정교한 공격을 막을 수 있는 것도 아니다.

기업망 관리자는 피싱에 저항성이 있는 인증 방법을 통해 사용자를 인증하는 것이 매우 바람직하다. 만약, 다중 인증 방식에 적용될 수 있는 인증 기술 중에서도 피싱에 저항성이 부족한 인증 방식이 있다면 이를 배제하는 것이 바람직하다.

3) 정교한 수준에서의 사용자 접근제어

인증이 이루어지면, 기관에서는 사용자에 대해 정교한 수준에서의 리소스 접근제어 및 서비스 인가를 성공시켜야 한다. 제로트러스트 아키텍처에서는 2가지 측면에서의 접근제어를 고려할 수 있다.

첫번째는 모든 접근 요청을 평가하고, 현재 유효한 세션을 지속적으로 평가하는 것이다. 정상적으로 인가를 받은 세션이라 하더라도, 현재 세션에서 모니터링되는 주변 정보와 보안 이벤트 등을 중심으로 위험도가 증가하는 경우, 재인증 요구 혹은 현재 세션 종료, 특정 리소스에 대한 접근 제한 등의 조치가 있어야 한다.

두번째는 현재 많은 곳에서 사용 중인 역할기반 접근제어(RBAC, Role-Based Access Control)보다 속성기반 접근제어(ABAC, Attribute-Based Access Control)가 수행하도록 설계된 것과 같이 보다 세분화되고 동적으로 정의된 권한에 따르는 것이 바람직하다. 권한을 인가하는 것은 여러 단계에서 수행될 수 있는데, 예를 들어 응용 프로그램에 대한 접근 권한에 대해서는 ABAC을 적용하고 응용 내부에서 특정 데이터에 대한 정밀한 수준의 인가는 RBAC을 적용하는 것도 가능할 수 있다.

2. 기기 및 엔드포인트

가. 목표

기업은 업무용으로 인가되어 동작하는 모든 기기 목록을 관리하고, 해당 장치에서 발생하는 사고를 예방, 감지 및 대응할 수 있어야 한다.

나. 전략

1) 자산 목록화

전사적인 제로트러스트 아키텍처를 위해서는 기업망에서 이루어지는 접근 주체와 리소스 간 접근 및 비즈니스 프로세스에 대한 명확한 이해가 필요하며, 이를 위해서는 기업 내의 자산에 대하여 완전한 목록을 만들고 유지할 수 있어야 한다.

예를 들어, 미국 연방 정부에서 자산에 대한 명확한 이해를 기반으로 위험을 낮추고 보안성을 높이기 위한 CDM(지속적인 진단 및 완화) 프로그램을 따르는 시스템 도입을 권고하고 있는데, 이 경우 미 연방 정부 기관에서는 CDM 프로그램을 통한 자산 목록을 생성·관리하고 있다.

또한, IT 자산에 대한 탐지·식별·목록화를 지원하는 다양한 방법 및 보안 솔루션이 현재 존재한다. 예를 들어, NAC(네트워크 접근제어), DMS(데스크탑 관리 솔루션), IPAM(IP 주소 관리) 등과 같은 솔루션들이 그 예가 될 수 있을 것이다. 그럼에도 이들 솔루션을 도입하지 않았거나, 혹은 도입을 하였음에도 높은 수준의 제로트러스트를 달성하기 위한 기술(기기의 정확한 신뢰도 평가를 위한 통합·자동화의 적용 등)이 필요할 수 있다.

자산 목록화 과정은 클라우드 환경에서 보다 더 잘 이루어질 수 있을 것이다. 예를 들어, 클라우드 인프라 혹은 클라우드 관련 자산을 보유한 기업에서는 클라우드 업체가 제공하는 인터페이스를 통해 자산 목록화에 대한 자동화된 검색이 가능할 수 있다.

2) 전사적 기기 탐지 및 대응(EDR)

기업망에서 발생할 수 있는 사고의 가능성을 최소화하기 위하여, EDR 솔루션을 전사적으로 도입하는 것도 하나의 방법일 수 있다. EDR은 단말, PC 등의 행위를 모니터링하고 이상 행위와 위협을 사전에 대응하는 것이 목적이다. 따라서, 단순히 단말, PC에서 서버에

이르기까지 기기 정보만 제어하는 것이 아니라, 단말 내부 행위를 상시적으로 수집하여 의심스러운 행위를 정의하고 효과적으로 조사·분석한다.

최근 EDR 솔루션은 딥러닝 등 인공지능 알고리즘이 결합되면서 성능을 높이고자 하는 경쟁이 치열하다. EDR은 기기나 단말에서 발생하는 각종 행위를 수집, 의심스러운 행위 정의 및 탐지, 이벤트를 기반으로 조사 분석할 수 있는 기능 등을 포함함으로써 기존 레거시 보안 솔루션이 잡지 못한 위협을 탐지하고, 각종 이벤트를 조사·분석할 수 있는 기능 등을 포함함으로써 위험을 완화할 수 있다.

일부 메인프레임 및 레거시 시스템들은 호환 가능한 EDR이 없을 수도 있다. 이러한 경우에는 EDR을 사용하지 않고도 다른 제로트러스트 메커니즘을 활용하여 방어를 할 수도 있다. 예를 들어, 어떤 환경에서는 범용 컴퓨팅을 제외한 최소 권한 설계를 사용함으로써 EDR 없이 제로트러스트 원칙을 정확히 지킬 수 있다.

3. 네트워크

가. 목표

기업망 내에서 모든 DNS, HTTP 트래픽을 암호화하며, 보안 경계를 격리된 환경으로 (소프트웨어적으로) 분할하는 계획을 실행해야 한다.

나. 전략

1) 네트워크 가시성 및 공격 표면

최근 기업망 내에서도 암호화 기술이 많이 활용되고 있다. 그러나, 이는 네트워크 모니터링의 깊이와 네트워크 검사 장치에 대한 공격 성공 가능성에 대한 균형을 맞춰야 한다. 예를 들어, 로그 및 모니터링 시스템이 손상·공격당해 있다고 가정하면 기업망에 상당한 악영향을 줄 것이며, 암호화 프로토콜이 취약하거나 잘못 구현되는 경우 보안 취약성이 커질 수 있다.

정적인 암호키를 사용하기보다는 TLS 1.3 프로토콜 및 기타 암호화 프로토콜을 통한

응용 데이터의 보호가 바람직할 것이다. 네트워크 트래픽을 심층적으로 검사할 수 없거나 데이터의 민감도 등의 사유로 검사해서는 안 되는 위치가 있을 수 있다. 이런 곳에서의 트래픽 검사는 비용대비 효용성이 떨어질 수 있다. 물론, 여전히 심층적인 트래픽 검사가 효과적인 환경이 있을 수 있다.

복호화되지 않은 네트워크 트래픽은 반드시 메타데이터나 기계 학습 기술, 혹은 비정상행위 탐지를 위한 다른 전략을 사용하여 분석될 수 있으며 또한 분석되어야 한다.

2) DNS 트래픽 암호화

그동안 DNS 요청 패킷은 전통적으로 암호화되지 않았다. 이는 공격자들이 기업망 내에서 공격을 위한 모니터링을 수행하는데 유리하게 만든다. 따라서 DNS 트래픽에 대한 암호화를 수행한다면 제로트러스트의 철학에 조금 더 가까워질 것으로 보인다. 또한 기업 내 접속 기기들이 자동 네트워크 검색에 의존하기 보다는 기관이 지정한 암호화된 DNS 서버를 사용하도록 명시적으로 구성해야 한다.

3) HTTP 트래픽 암호화

웹 브라우저에서 데이터 혹은 응용 등을 제공하는 데 흔히 활용되는 HTTPS는 기업망 내에서든 외부와 연결되든 반드시 적용되어야 한다. 이는 제로트러스트 아키텍처 관점에서 지극히 정상적인 전략이 될 수 있다.

기업망 내부뿐만 아니라 기업망을 오가는 전체 통신에서 암호화되지 않은 HTTP가 사용되는 경우, 반드시 중간에 개입하여 암호화를 하여야 한다. 기업망 내부의 특정 서버가 HTTPS를 사용하지 않는 경우, 차후 패치를 통해 기업망 전체에 보안 프로토콜이 사용되기 위한 도입 전략에 대해서 고민해야 한다.

4) 전사적 아키텍처 및 격리 전략

제로트러스트 아키텍처의 도입은, 일반적으로 접근 주체의 환경을 격리하여 한 응용이나 리소스를 손상시키는 공격자가 기업 내에서 쉽게 횡적 이동을 하여 다른 환경을 손상시킬 수 없도록 하는 것이 목적이 된다.

이에 대한 접근 방식은 각 기업들의 환경과 핵심 요소의 성숙도에 따라 다를 것이며, 상기 목적을 위한 자신만의 방식으로 접근 방식을 조합하여야 한다. 일반적으로 성숙한 클라우드 인프라는 강력한 ID 및 속성기반 접근제어, 가상화된 논리적 격리 등을 지원하고 있다. 따라서, 기업은 제로트러스트 아키텍처 전략에 최적화된 클라우드 기반 인프라를 활용하는 것도 한 가지 방법이 될 수 있다.

4. 시스템

가. 목표

기업은 보유하고 있는 서버(Server) 시스템에 대해서 권한 사용자(예: 시스템 관리자 등) 레벨로 접속하는 경우 서버 시스템의 주요 파일 접근제어, 주요 사용 명령어 통제, 영역별 접근제어 등이 통제되고 관리됨으로써 외부 해커의 주요 서버 시스템 공격에 대해 대비하여야 한다.

나. 전략

1) 시스템 관리자에 대한 강력한 인증/계정관리

시스템 관리자 계정에 대해 전사적 관리를 진행하고 시스템 관리자의 직급별, 권한별 등급에 따라 접속하고자 하는 시스템의 권한 관리 정책을 등록하고 관리할 수 있도록 한다. 또한 시스템 관리자 인증은 단순 ID 및 패스워드 방식이 아닌 PKI, OTP, 생체인증(FIDO) 등이 연동 가능한 방식으로 MFA를 지원하도록 한다.

시스템 관리자들의 입사 및 퇴사 등에 따른 계정 동기화와 프로비저닝이 실시간으로 이루어짐으로써 휴면 계정으로 인한 해킹 공격의 위험을 최소화한다. 또한, 시스템 관리자들의 패스워드를 주기적으로 자동화된 생성 및 폐기 관리를 함으로써 안전하지 않은 패스워드의 사용을 제거하여 시스템 접근 및 사용 신뢰성을 높이도록 한다.

2) 게이트웨이 및 에이전트 방식의 시스템 접근제어 운용

시스템 관리자들이 서버 시스템에 접속하여 시스템 주요 파일 및 정보들은 관리 운용하는 경우 계정 탈취를 통한 외부 해커의 시스템 접근을 막기 위하여 접속하는 기기 또는

엔드포인트 시스템에 대한 신뢰점수 확인 후 접속 여부를 결정하도록 한다. 이 때 사용자 인증은 MFA 방식으로 진행함으로써 원격지 외부 해커의 계정 도용 공격을 방지 할 수 있도록 한다. 이후 대상 서버 시스템 접속 시 계정 관리시스템과 연동하여 시스템 관리자가 보유하고 있는 권한 레벨에 따라 파일 접근제어, 사용 명령어 접근제어 등을 세밀하게 하면서 서버 시스템의 안전한 운용을 수행할 수 있도록 한다.

3) 서버 시스템에 대한 마이크로 세그멘테이션 및 횡적 이동 방어

전통적인 레거시 기반(Unix, Windows 등)의 온프레미스 환경이나 프라이빗 클라우드 환경의 온프레미스 환경, 그리고 퍼블릭 클라우드 환경이 혼재하는 기업 서버 시스템 환경에서는 어느 존의 형태에서나 해커의 1차 공격 이후 내부 시스템으로 확산되는 횡적 이동(Lateral Movement)을 막아야만 한다.

이를 위해 주요 서버 시스템들을 보안 등급별로 구분하여 호스트 방화벽(Firewall)이나 네트워크 방화벽을 기반으로 하는 마이크로 세그멘테이션(Micro-segmentation) 구성을 취함으로써 횡적 이동 공격의 피해를 최소화시킬 수 있다. 또한 각 호스트(Host) OS나 가상화된 게스트(Guest) OS에 서버 백신, 방화벽, IPS 등의 기능을 설치하여 1차 해킹 이후 횡적으로 전파되는 2차 시스템 공격을 방어할 수 있도록 한다.

4) 컨테이너 구조의 DevOps 환경에서 안전한 서버 시스템 환경의 구성

기업이 프라이빗 클라우드 또는 퍼블릭 클라우드 환경을 사용하면서 IT 기반 환경을 컨테이너 구조의 MSA(Micro Service Architecture)로 가져가는 경우 기업들은 반드시 안전한 DevOps 환경(DevSecOps)을 구성해야 한다. 소스코드 개발자가 수시로 소스 코드를 수정하고 이를 이미지 빌드(Build)하여 컨테이너에 배포(Ship)하고 실행(Run)하는 경우 기업의 보안절차는 반드시 다음을 따를 수 있도록 한다.

첫 번째로 해당 개발환경에 접속하는 개발자는 반드시 접속하는 엔드포인트 시스템의 신뢰 점수가 보장되어 있어야 한다. 두 번째로 해당 개발자가 빌드 서버에 접속하는 경우 반드시 MFA로 사용자 인증을 거치도록 한다. 세 번째로 해당 개발자에 대해 권한 자격을 기반으로, 접속하는 시스템의 범위를 제한하거나 시스템에 접속 후 행할 수 있는 행위를 접근 통제를 할 수 있도록 한다.

5. 응용 및 워크로드

가. 목표

기업은 모든 응용들이 인터넷에 연결되어 있다고 간주하고, 정기적으로 응용 프로그램을 엄격하게 시험하며, 외부 취약성 보고서를 참고해야 한다.

나. 전략

1) 응용 보안 시험

미 연방 정부 행정명령 EO-14028에서는 NIST가 소프트웨어 테스트를 위한 최소 표준을 권장하도록 지시하였다. 이에 따라 NIST는 '소프트웨어의 개발자 검증을 위한 최소 표준 가이드라인(NIST IR 8397)' 문서를 만들었으며, 이 문서에서는 소프트웨어 검증 기술에 대한 11가지 권장 사항을 설명하고 기술에 대한 추가 정보와 추가 정보를 위한 참조를 제공한다. 이는 민간 기업에서도 응용 개발시 참고할 수 있을 것이다.

정교한 공격을 견뎌야 하는 기업 응용 프로그램을 위해 기업은 응용의 보안 제어 구현 및 문서화 이상의 작업이 필요할 것이다. 기업은 소프트웨어가 어디에서 구축되었는지 상관없이 소프트웨어 및 배포된 기능을 분석할 수 있어야 한다.

2) 써드파티 시험

응용에 대한 자체 시험 외에도 기업이 직원이 식별하기 어려운 취약점을 찾아내기 위하여 외부 관점에 대한 의존도를 높이는 것이 좋을 것을 보인다.

3) 응용 취약점 리포트

C-TAS와 같은 사이버 위협정보 분석 및 공유를 제공하는 보안 서비스가 공개되어 있다. 해당 기능은 제로트러스트 보안 솔루션을 만드는 곳에서 많은 관심을 두고 솔루션에 반영하겠지만, 기업 관리자에서도 위협정보 및 취약점에 대해서 이해를 하는 것이 바람직하며, 필요할 경우 기업에서 사용 중인 응용에 대한 악성코드나 취약점을 보고할 수 있을 것이다.

4) 응용의 인터넷 접근성 안전 구성

VPN 혹은 기타 보안 터널에 의존하지 않고 안전한 방식으로 응용의 인터넷 접근성을 가능하게 만드는 것이 쉬운 일은 아니다. 안전하게 구성하기 위하여 기업은 실행 가능한 최소한의 모니터링 시스템, 서비스 거부 공격에 대한 보호, 접근제어 정책 등을 마련해야 한다.

5) 인터넷 접근 가능한 응용 발견

제로트러스트 아키텍처를 효과적으로 구현하려면 기업에서 인터넷에 접근할 수 있는 자산을 완전히 이해해야 보안 정책을 일관되게 적용하고 사용자 워크플로우를 완전히 정의하고 수용할 수 있을 것이다. 실제로 대규모의 분산된 조직이 모든 자산을 안정적으로 추적하는 것은 매우 어렵다.

기업이 인터넷에 접근할 수 있는 공격 표면에 대한 이해를 하려면, 기업망 뿐만 아니라 인터넷에서 인프라의 외부 스캔을 통한 공격을 통해 파악하는 것이 바람직하다. 예를 들어, 미 연방 정부 GSA(총무청)는 오픈 소스 소프트웨어 기반으로 다양하고 유용한 속성을 측정하는 웹사이트 스캐닝 서비스[27]를 운영한다.

이러한 외부 서비스를 활용함으로써 인터넷 접근 가능한 응용을 발견하여, 공격 평면을 구체화하고, 세밀한 접근제어와 소프트웨어적인 경계를 생성하는 기초가 될 수 있을 것이다.

6) 변경 불가능한 워크로드

응용에 대해 자동화되고 변경 불가능한 배포가 가능해지면, 이는 최소 권한 구조를 크게 개선하여 기관의 제로트러스트 목표를 지원하게 될 것이다. 응용 배포에 더 이상 수동적인 접근과 개입이 필요하지 않으면서, 서버와 기타 리소스에 대한 개별 접근이 허락되지 않으면서 중앙에서의 관리가 다소 편안해질 수도 있다. 환경에 대한 수동 변경을 허용할 경우, 서로 다른 배포 제품, 다른 패치 등의 발생으로 향후 배포가 복잡해지고 오류가 발생할 가능성이 있다.

---

27 The Site Scanning Program, https://digital.gov/guides/site-scanning/

특히, 클라우드 기반 인프라에 배포될 경우, 더 이상 변경할 수 없는 워크로드를 사용하도록 노력해야 하며, CI/CD(지속적 통합/지속적 배포) 및 IaC(코드로서 인프라)를 포함한 최신 소프트웨어 개발 수명 주기 방식은 변경할 수 없는 워크로드를 기반으로 하는 안정적이고 예측 가능하며 확장 가능한 응용 생성이 용이하게 된다.

6. 데이터

가. 목표

기업은 완전한 데이터 분류를 사용하는 보호 기능을 배포하기 위해 명확하고 공유된 경로를 따른다. 기관은 클라우드 보안 서비스 및 도구를 활용하여 민감한 데이터를 검색, 분류 및 보호하고 전사적 로깅 및 정보 공유를 구현해야 한다.

나. 전략

1) 데이터 보안 전략

기업은 데이터를 분류하고 태그를 지정하는 포괄적·정확한 접근 방식을 개발하는 것이 바람직하다. 기존에는 데이터세트 단위로 관리를 하는 경우가 많았지만, 제로트러스트 관점에서는 이보다 상세한 수준의 데이터 관리가 필요하다. 데이터베이스에 저장되었거나 공개된 데이트세트 뿐만 아니라, 명확하게 구조화되지 않은 분산된 데이터 시스템 및 메타데이터에 대한 보호까지 고려하는 것은 쉬운 일은 아니다.

그럼에도 이러한 기업 내 데이터 관련 주요 이해당사자들과 모든 데이터에 대해 전사적으로 정리·분류하고, 데이터 보안을 위한 목표를 정리하여야 한다. 아직은 전사적 데이터 분류를 지원하는 기술이 충분히 성숙되어 있지 않으므로, 단기간 내에 데이터 분류 및 보안을 지원하는 표준화된 기법을 도입하기는 어려울 수 있다. 미국 연방 정부는 이와 유사한 데이터 보안 가이드라인을 개발할 것으로 예상되므로 이를 참조할 수도 있을 것이다.

2) 보안 응답 자동화

기업망 내외부에 위치한 다양한 시스템들로부터 발생하는 보안 이벤트는 다양하고 많을 것으로 예상되므로 보안 모니터링 및 처리 자동화는 매우 중요할 것이다. 이를 지원하는

기술이 SOAR(Security Orchestration, Automation, and Response)이다.

기업에서 이런 자동화 작업을 수행하면서 조직 내 일상 업무에 중단을 일으키지 않고 보안과 효율성을 개선하기 위해서는, 신중한 튜닝, 반복, 그리고 비즈니스 요구사항에 대한 민감성이 필요하다. 자동화된 보안 시스템이 효과적으로 동작하기 위해서는 오류율이 낮아야 할 것이다.

보안 관점에서의 대응을 성공적으로 자동화·통합하기 위해서는 시스템에 정보를 제공하는 데이터가 풍부해야 한다. 물론, 이런 데이터 정확한 접근제어를 위해, 데이터 유형 및 접근 요청 사용자를 포함할 수 있다. 기업은 비정상적인 행동에 대한 실시간 탐지·경고를 할 수 있도록 기계 학습에 기반한 전략을 사용하려는 노력이 필요하다. 예를 들어, 기업 관리자 혹은 경영자가 이전에 접근한 적이 없으며 앞으로도 접근하리라 예상되지 않는 시스템이나 리소스, 데이터에 접근하려고 할 때 기계학습으로부터 도움을 받을 수 있을 것이다.

물론, 현재 대다수 기계 학습 모델은 정책 결정에 대해 설명가능하지 않고, 오류율을 줄이기 위한 노력이 어려울 수 있다. 그러므로 초창기에는 기계 학습에 크게 의존하지 않은 단순한 기술로 접근하되, 차츰 기계 학습 기반 기술을 시범적으로 도입하는 것을 고려할 수 있다. 또한, 처음에는 기계 학습에 의한 자동화된 조치를 배제하고, 관리자에게 보고만 하도록 설정하는 것도 좋은 접근법이 될 수 있을 것이다.

3) 클라우드에 있는 민감 데이터 접근 감사

기업에 있는 미사용 데이터에 대해서는 암호화를 사용하는 것이 바람직하지만, 여전히 복호화가 가능한 시스템에 공격자가 침투하는 경우 해당 데이터에 접근이 가능해진다. 클라우드 인프라를 활용하여 키를 관리하고 복호화 작업에 접근할 수 있도록 한다면, 온프레미스 환경이 공격자에 의해 침투 당하더라도 감사 로그 등의 신뢰성에 의존하여 안전성을 높일 수 있을 것이다.

기업이 민감 데이터를 클라우드에 저장하고, 암호화할 때, 키 관리 도구를 활용하여 해당 데이터 접근 시도에 대한 감사 로그를 생성하는 것이 바람직하다. 클라우드 서비스 제공자가 운영하는 키 관리 도구를 사용할 수도 있고, 혹은 온프레미스 혹은 클라우드 외부 환경 상의 키 관리 도구를 사용할 수도 있다.

제로트러스트 성숙도의 최적화 수준까지 도달하기 위해서는 상기 감사 로그가 다른 보안 이벤트와 결합하도록 함으로써 보다 정교한 수준으로 보안 모니터링이 가능해질 것이다.

4) 주기적인 로그 확인

기업은 온프레미스 혹은 클라우드 인프라에서 보안 사고 및 침해 사례가 발생할 경우, 이에 대해 조사·복구할 수 있는 능력이 있어야 할 것이다. 이를 위하여 기업은 전사적으로 혹은 정부·타기업간 침해 정보를 공유하고 대응할 수 있는 시스템 구축, 감사 로그 분류 및 분석 등이 가능해야 한다.

미 연방 정부의 각 기관들은 로그 관련 첫 번째 조치로, 전체 DNS 요청에 대한 로그를 남기고, 각 로그의 제한된 접근 및 암호화된 검증을 허용하는 무결성 조치를 구현해야 한다. 기업들에게도 이와 유사한 조치가 필요할 수 있으나, 기업의 규모와 제로트러스트 관련 솔루션의 성숙도 수준, 도입 전략에 따라 구체적인 실현 방법을 정하는 것이 바람직하다.

제2절 | 제로트러스트 구현 유스케이스

본 절에서는 앞서 언급한 전략과 함께 제로트러스트 구현이 특히 요구되는 다음의 환경에 대한 유스케이스를 정리하고자 한다. 각 유스케이스에 대하여 기존 접근법과 한계점, 그리고 이를 통해 기업에서 원하는 목표와 요구사항, 이들을 위한 제로트러스트 구현 방안을 각각 언급한다.

1) 지사·원격 접속 환경
2) 써드파티·기업간 협업 환경
3) 업무망/인터넷망 망분리 환경
4) 온프레미스·클라우드 활용 환경
5) OT/ICS 등 산업 제어 환경
6) M2M(Machine-to-Machine) 환경

1. 지사·원격 접속 환경

본사가 위치하지 않은 지역 혹은 해외에 지사를 두고 운영하는 기업들의 경우, 지사에 근무하는 직원에 대해 본사 기업망에 안전하게 접속을 보장하기 위하는 것은 상대적으로 어려운 문제이다. 전용선, MPLS 등은 비용, 관리 및 대역폭 등의 측면에서 사용 빈도가 점점 줄어가고 있으며, VPN을 통한 접속 혹은 VDI 기술은 많은 기업들이 현재에도 많이 사용하고 있다.

지사 접속 환경이 고정된 외부 위치에서 (자주 변경되지 않는) 정해진 직원과 사용자 기기가 접속하는 정적인 기업망 접속 환경이라고 본다면, 기업 외부(예를 들어, 출장 중)에서 근무하는 환경 및 코로나19 팬데믹 이후 일상화된 재택 근무 등을 통한 원격 접속 환경은 매우 동적인 기업망 접속 환경으로 볼 수 있을 것이다. 그러나 접속 위치와 기기, 사용자의 변화 관점에서 동적이냐 정적이냐의 차이를 제외하고는, 기업망 외부에서 접속한다는 면에서는 공통점이 있으므로 본 문서에서는 모두 동일한 수준에서 이들에 대한 유스케이스를 정리하고자 한다.

가. 기존 접근법

- 기존에는 기업망 내 데이터 및 응용 워크로드에 접근하기 위기 위해서는 기업망에 물리적인 접속이 되어 있어야 했음.
- 그렇지 못한 경우, VPN(가상사설망), VDI(가상 데스크톱 인프라) 등과 같은 보안 솔루션을 통한 접속 후 기업망 내 데이터 및 응용 워크로드에 접근.
- 원격·재택 근무 환경의 증가로, 원격 접속이 늘어남에 따라 VPN이 접속자 수 및 트래픽 양을 커버할 수 없을 경우, 단일 실패점(Single point of failure)이 될 가능성이 높음. 특히, 화상 회의, 미디어 교육 등으로 인한 대역폭 소비 또한 무시할 수 없는 수준임.
- 일부 회사의 경우, 보안 정책상 VPN 등 외부 접속의 경우 기업망 내 모든 데이터 및 응용 워크로드에 접근하기 어려움. 사용자 인증은 수행하였으나, 기기에 대한 신뢰성을 기업망에 있는 PC/서버 수준으로 검증하기 어렵기 때문임.
- 원격 접속 직원이 기업망 외부 클라우드 서비스에 있는 기업 데이터 및 응용 워크로드를 이용한다면, 해당 트래픽이 기업망을 경유하는 것이 바람직하지 않을 수 있음.

나. 목표 및 요구사항

- **목표**: 원격 접속 직원은, 물리적 위치에 관계없이 동일한 접근제어 정책을 통하여 데이터 및 응용 워크로드에 접속할 수 있어야 함.

- **요구사항**

  ① VPN, VDI와 같이 네트워크 트래픽을 모두 기업망으로 통과시키는 보안 솔루션을 가급적 사용하지 않아야 하며, 예를 들어 원격 접속 직원이 외부 클라우드 상의 리소스 혹은 서비스를 이용할 경우와 같이, 꼭 필요한 경우가 아니라면 해당 트래픽이 기업망을 경유하지 않아야 함.

  ② 접속하는 기기에 대한 보안성을 실시간으로 체크하여, 사용자 및 기기에 대한 신뢰도를 판단할 수 있어야 함.

  ③ 해당 신뢰도를 바탕으로, 시스템, 응용 워크로드 및 데이터 접근에 대한 세밀한 접근제어가 가능해야 함.

다. 제로트러스트 구현 방안

- ID 통합(Federation) 및 싱글사인온, 다중 인증 등을 지원하는 ID 관리 시스템 도입, 기업망 내 데이터 및 응용 워크로드에 접근 전 인증함.
- 모든 접근에 대하여 암호화된 통신 적용함.
- 접속 기기 정책 준수 여부 및 기기 상태, 이상 행위에 대한 모니터링, 보안성 검증을 통한 기기 신뢰도 확인함.
- 기업망 내 시스템, 응용 워크로드, 데이터 및 이들에 대한 접근제어 정책사전 분류함.
- ID 인증 및 기기 신뢰도 기반 세밀한 인증·접근제어 정책 적용 및 실시간 승인함.

2. 써드파티·기업간 협업 환경

두번째 유스케이스는 써드파티 혹은 기업 간 협업 환경으로, 예를 들어 기업 A와 기업 B가 공동으로 진행하는 프로젝트에서 기업 A의 데이터베이스에 기업 B의 특정 직원이 접근하는 시나리오가 가능하다. 혹은 기업 A가 개발하는 특정 제품 혹은 기업망에서 사용 중인 응용의 일부를 기업 B에 외주를 준 경우, 기업 B의 결과물이 해당 제품에 잘 결합되는지 시험하기 위하여 기업 B의 특정 직원이 기업 A의 개발 환경에서 시험해야 하는 상황이 있을 수 있다.

이러한 환경에서는 외부 회사의 특정 직원이 자사의 기업망 혹은 클라우드에 위치한 네트워크, 데이터, 응용 워크로드 등에 접근해야 한다. 이 경우, 이 외부 직원을 위하여 게스트 계정을 생성하거나 혹은 ID 통합(Federation)을 통하여 이 외부 직원의 계정을 인증하고 관계를 설정하는 것이 가능할 것이다.

이 환경은 외부 직원의 물리적 접속 위치가 외부에 위치할 수 있으며, 접속하고자 하는 데이터 혹은 응용 워크로드가 외부 클라우드에 있을 수 있다는 면에서 첫번째 유스케이스와 유사한 점이 있다. 따라서, 기존 접근법과 목표, 요구사항 및 구현 방안 역시 유사할 것이나, 외부 직원을 위한 특정 계정에 최소한의 리소스 접근 권한을 부여하고 필요시 즉각적인 해제가 가능해야 한다는 면에 초점이 맞춰지게 될 것이다.

추가로 고려해야 할 점은, 기업 B의 결과물이 기업 A의 기업망에서 사용 중 혹은 예정인 응용에 결합되는 경우, 공급망 보안 이슈 역시 중요하게 고려되어야 한다. 기업 B의 결과물에

악성 코드가 포함된 경우, 해당 결과물과 결합된 기업 A의 기업망 응용 역시 민감 데이터 접근 및 정보 유출 등 악의적인 행위를 시도할 가능성이 있다. 즉, 악성 코드에 감염된 기기는 필연적으로 권한 이상의 데이터에 접근하거나 기업망 내부의 다른 서버, 혹은 정보 유출을 위해 외부 네트워크에 평상시와 다른 패턴의 접속을 시도할 가능성이 높다.

따라서, 이러한 위험성을 고려한 제로트러스트 접근 전략이 필연적으로 요구되며, 반드시 기기에 대한 최소 권한 부여를 통해 권한이 없는 리소스에 대한 횡적 이동 및 접근이 불가능하도록 마이크로 세그멘테이션 전략이 필요하며, 모니터링 및 로그 기록을 통하여 이상 행위를 하는지 확인하여야 한다.

가. 기존 접근법

- 기존에는 외부 기업의 특정 IP 주소를, 자사의 접근 정책에 기반하여 방화벽 규칙 혹은 ACL(접근제어 리스트)에 등록했어야 함.
- 그러나 방화벽 규칙 혹은 ACL에 외부 기업의 특정 IP 주소를 등록하는 것은 매우 번거로운 절차이며, 또한 네트워크 단위가 아닌 특정한 데이터 혹은 응용 워크로드에만 접근할 수 있도록 조치하는 것이 불가능함. 또한 기기에 대한 신뢰성 역시 체크하기가 매우 어려움.
- 혹은 외부 기업의 직원이 직접 기업을 방문하여 자신의 기기를 해당 기업망에 물리적으로 연결시키거나, 기업의 컴퓨터/서버를 활용하여야 했음.
- 이 경우, 외부 직원이 반드시 해당 기업을 물리적으로 방문하여야 하는 번거로움이 있으며, 외부 직원의 신뢰할 수 없는 기기 혹은 응용 프로그램 등이 기업망에 직접 연결되어 새로운 공격 포인트가 될 가능성이 있음.
- 첫번째 유스케이스와 마찬가지로 외부 직원이 기업망 외부 클라우드 서비스에 있는 기업 데이터 및 응용 워크로드를 이용한다면, 해당 트래픽이 기업망을 경유하는 것이 바람직하지 않을 수 있음.
- 또한 외부 기업의 결과물이 악성 코드에 감염된 상태로 기업망에서 사용 중인 응용에 포함될 경우, 해당 응용은 기업망 내부에서 신뢰할 수 있는 응용으로서 동작하게 됨으로써 횡적 이동 등을 통한 공격 가능성이 있음.

나. 목표 및 요구사항

- **목표**: 외부 직원은, 방화벽 규칙 혹은 ACL의 변경없이 게스트 계정 생성 혹은 ID 통합(Federation)을 활용하여 필요한 최소한의 권한만을 부여받아야 함. 또한, 게스트 계정에 추가 권한 부여 시 세밀한 접근 통제 및 모니터링이 이루어져야 함. 기업망에 사용 중인 응용 역시 세밀한 접근 통제 및 모니터링 대상이 되어야 함.

- **요구사항**

  ① 협업 전 네트워크 접근 설정(예, 외부 기업의 특정 IP 주소를 방화벽 규칙 혹은 ACL에 등록, 협업 완료 후 제거 등)과 같은 번거로운 변경을 하지 않아야 함.

  ② VPN과 같이 네트워크 트래픽을 모두 기업망으로 통과시키는 보안 솔루션을 가급적 사용하지 않아야 하며, 외부 직원이 기업 외부 클라우드 서비스를 이용할 경우 해당 트래픽이 기업망을 경유하지 않아야 함.

  ③ 외부 직원에 대해 게스트 계정 생성 혹은 ID 통합(Federation)을 통해 인증할 수 있어야 하며, 다중 인증 등 강화된 인증을 사용하는 것이 바람직함.

  ④ 외부 직원이 접속하는 기기에서 협업을 위해 필요한 최소한의 리소스(네트워크, 시스템, 응용 워크로드, 데이터)에만 접근이 허용되어야 함. 또한 필요시 세밀한 접근제어 및 모니터링이 이루어져야 함.

  ⑤ 외부 직원의 기기에 대한 보안 상태를 실시간으로 체크하여, 사용자 및 기기에 대한 신뢰도를 판단할 수 있어야 하며, 신뢰도에 따라 필요시 즉각적으로 현재의 접근 권한을 해제할 수 있어야 함.

  ⑥ 기업망 내부 응용에 대한 보안 상태 역시 실시간으로 체크하여 신뢰도를 판단할 수 있어야 하며, 권한이 없는 리소스(네트워크, 시스템, 데이터 등)에 접근할 수 없어야 함. 또한 최초 권한에 맞춰 세밀한 접근제어 및 모니터링이 이루어져야 하며, 필요시 즉각적으로 현재의 접근 권한을 해제할 수 있어야 함.

다. 제로트러스트 구현 방안

- 게스트 계정 생성 혹은 ID 통합(Federation), 다중 인증 등을 지원하는 ID 관리 시스템 도입, 기업망 내 시스템, 응용 워크로드 및 데이터에 접근 전 인증함.

- 모든 접근에 대하여 암호화된 통신 적용함.
- 접속 기기 정책 준수 여부 및 기기 상태, 이상 행위에 대한 모니터링, 보안성 검증을 통한 기기 신뢰도 확인함.
- 기업망 내 리소스(네트워크, 시스템, 응용 워크로드 및 데이터) 및 이들에 대한 접근제어 정책 사전 분류함.
- 외부 직원 ID에 최소한의 리소스(네트워크, 시스템, 응용 워크로드 및 데이터)에만 접근을 허용할 수 있는 세밀한 접근제어 기술 적용함.
- ID 인증 및 기기 신뢰도 기반 세밀한 인증·접근제어 정책 적용 및 실시간 접근 권한 해제함.
- 기업망 내부 응용에도 세밀한 인증·접근제어 정책 적용, 이상 행위에 대한 모니터링 및 실시간 접근 권한 해제함.

3. 업무망/인터넷망 망분리 환경

세번째 유스케이스는 금융회사, 산업제어시스템(ICS, Industry Control System) 등에서 중요 업무망과 외부 인터넷망을 분리하여 운영하는 망분리 환경이다. 이러한 망분리는 외부의 침입으로부터 업무망 내부의 주요 리소스를 보호하기 위하여 널리 사용되고 있으며, 물리적 망분리와 논리적 망분리 기법의 적용이 가능하다.

구축 비용 및 업무 환경의 효율성을 이유로 논리적 망분리를 도입하기도 하지만, 금융 분야의 경우 전자금융감독규정 제15조(해킹 등 방지대책)에 의거하여 물리적 망분리를 하도록 강제하고 있다.[28] 산업제어시스템의 경우, NIST SP 800-82(Guide to Industrial Control Systems Security) 문서에서 주요한 보안 구조의 하나로 제어 네트워크와 업무 네트워크의 논리적 망분리를 언급하고 있다.

---

28 2022년 4월 금융위원회가 발표한 '금융분야 클라우드 및 망분리 규제 개선방안'에 따라 현행 망분리 규제를 개발·시험 환경부터 단계적으로 완화하는 방안 추진 중이며, 2022년 11월 개정된 전자금융 감독규정이 2023년 1월부터 시행됨에 따라 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 분야에 대해 망분리 적용 예외조치가 허용되었다.

가. 기존 접근법

- 기존에는 금융회사, 산업제어시스템 등에서 중요 업무망과 외부 인터넷 망을 분리하여 운영함.
- 일반적으로 중요 업무망과 인터넷망에 대해 별도의 컴퓨터를 사용하도록 하며, 그 외에도 전환 스위치에 의한 망분리 혹은 네트워크 카드를 2개 탑재하는 방식 등을 통해 공격자가 중요 업무망에 접근하는 것을 물리적으로 차단함.
- 높은 보안성을 가지지만, 별도 컴퓨터의 사용, 물리적 폐쇄망 구축 비용 등 비용이 높고 업무 환경의 효율성을 매우 떨어뜨리는 요인이 됨. 특히 코로나19 팬데믹 등으로 인한 재택근무 시 중요 업무망에 접근할 수 있는 모든 수단이 차단됨.
- 직원의 고의 또는 실수로 인하여 사용 컴퓨터가 원래 허용된 망이 아닌 다른 망에 연결되거나, 직원이 고의로 중요 업무망에 연결된 컴퓨터를 악용하여 공격하는 사례를 막기가 쉽지 않음.

나. 목표 및 요구사항

- **목표**: 가급적 논리적 망분리를 통해서 기존의 물리적 망분리와 동일한 보안 수준을 만족하면서, 직원의 고의 또는 실수로 인한 공격에 대응할 수 있어야 함.

- **요구사항**

① 물리적 망분리 기술 대신 논리적 망분리 기술을 활용하며, 이 경우 반드시 허용되어야 하는 조건을 만족하지 않으면 인터넷망의 모든 사용자와 기기는 중요 업무망 내부의 리소스에 접근할 수 없어야 함.

② 접속하는 모든 사용자와 기기에 대한 보안성을 실시간으로 체크하여, 사용자 및 기기에 대한 신뢰도를 판단할 수 있어야 함.

③ 중요 업무망 내부의 리소스에 접근하는 사용자와 기기는 세밀한 접근제어를 통하여 해당 리소스를 제외한 모든 리소스로의 횡적 이동이 금지되어야 하며, 이는 사용자와 기기의 현재 위치(인터넷망, 중요 업무망)와 관계없이 이루어져야 함.

④ 중요 업무망 내부 리소스에 접근하는 모든 사용자와 기기에 대해 실시간 보안성 체크 및 지속적인 모니터링을 통하여 신뢰도를 판단하여야 하며, 이상 발생 시 중요 업무망에 대한 일부·전체 접근을 물리적 망분리 수준으로 해제할 수 있어야 함.

다. 제로트러스트 구현 방안

- 기본적으로 모든 사용자와 기기는 중요 업무망 내부의 리소스에 대한 접근 금지 원칙을 포함하되, 네트워크 경계를 논리적으로 설정하는 SDP 등의 보안 기술을 통한 최소 권한으로 시작함.
- 모든 접근에 대하여 암호화된 통신 적용함.
- 접속 기기 정책 준수 여부 및 기기 상태, 이상 행위에 대한 모니터링, 보안성 검증을 통한 기기 신뢰도 확인함.
- 중요 업무망 내에서 특정 사용자 및 기기가 리소스 접속을 인가받은 경우, 현재 허용된 리소스(네트워크, 시스템, 응용, 데이터 등) 외 다른 리소스로의 횡적 이동은 별도의 명시적 접근제어 절차가 없는 경우 반드시 금지함.
- 중요 업무망(접근 사용자 및 기기, 내부 리소스 등)에 대해, 해당 업무망에 특성을 반영하여 실시간으로 공격·이상 행위 여부를 판단하여, 이상 발생시 중요 업무망에 대한 일부·전체 접근을 해제함.
- 산업제어시스템 등 구형 기기 등의 사유로 강화된 인증을 적용하기 어려운 경우, 최소 권한 부여를 통한 마이크로 세그멘테이션 및 지속적인 모니터링함.
- 안전성이 충분히 검증될 때까지는 기계학습 기반의 이상행위 모니터링 및 신뢰도 평가보다는 규칙 기반의 판단·결정함.

4. 온프레미스·클라우드 활용 환경

기존 환경에서 기업의 주요 데이터 자산 및 응용의 경우, 외부 유출로 인한 보안 사고의 두려움 등을 이유로 기업망 내부, 즉 온프레미스 환경에 구축하는 것이 일반적이었으나, 현재는 편의성과 비용, 보안 등 여러 이유로 점점 더 많은 기업들이 클라우드 활용에 대한 비중을 높여가고 있다. 즉, 온프레미스, 프라이빗 클라우드, 퍼블릭 클라우드가 혼재된 하이브리드 형태로 업무 환경을 운용하게 되면서, 접근 주체인 사용자와 기기뿐만 아니라 리소스 역시 기업망 내외부에 혼재하여 위치하고 있다.

네트워크, 데이터 혹은 응용이 클라우드에 위치하고 있다는 것은 기업이 직접 해당 리소스에 대한 직접적인 관리와 접근제어가 쉽지 않다는 점을 내포한다. 기업은 반드시

클라우드에 위치한 자신의 리소스들을 명확히 파악하고 있어야 하며, 해당 리소스의 위치(온프레미스 및 클라우드)와 관계없이 일관되고 중앙 집중적인 정책 관리 및 접근제어가 가능하여야 한다.

클라우드 상의 리소스에 대해서는 기존의 온프레미스 환경에 위치한 리소스와 보안에 대한 요구가 다르다. 전통적인 경계 기반 보안은 온프레미스 환경과 결합한 형태로 운용되어 왔으며, 물리적 보안, 방화벽과 같은 네트워크 보안, 사용자 인증 등의 보안 솔루션들이 적용되는 것이 일반적이다. 그러나, 클라우드 상의 리소스에 대한 물리적·네트워크 보안의 경우 해당 클라우드 서비스 사업자가 제공하는 보안 기법에 의존할 가능성이 높으며, 기업에서는 접근 주체에 대한 인증, 식별과 접근제어 등을 더욱 중요하게 다루게 될 것이다. 당연하게도 이 과정에서 온프레미스 상의 리소스에 대한 접근제어 시 일관된 정책을 적용할 수 있어야 한다.

가. 기존 접근법

- 기존 온프레미스 활용 환경에서는 기업의 모든 리소스가 기업 내부 서버에 위치하였으며, 리소스 관리 주체(예를 들어, 인사 관련 데이터베이스의 경우 인사 부서)가 파편화되어 운영함.
- 이에 대한 보안은 기존의 경계 기반 보안 솔루션을 통해 달성하는 것이 일반적으로, 여기에는 망분리와 같은 물리 보안, 방화벽 및 침입탐지시스템과 같은 네트워크 경계 보안 등을 포함함.
- 이 경우, 회사별로 보안 솔루션을 구축하기 위한 비용 및 인력에 대한 부담이 크고, 사용자 및 기기에 대한 통합된 인증 및 세밀한 접근제어가 이루어지지 않았으며, 이미 네트워크에 진입한 사용자 및 기기는 접근하고자 하는 리소스 외에 횡적 이동을 통한 다른 리소스에 대한 접근이 용이하여 내부자에 의한 공격이 이루어질 경우 피해가 컸음.
- 보안 비용에 대한 부담과 편의성을 이유로 클라우드 기반 서비스를 활용하기 시작하는 단계에서, 싱글사인온 등을 통한 통합 인증을 제공하기도 하였으나, 접근제어 정책이 리소스의 위치에 따라 파편화되어 있거나 사용자·기기의 신뢰도를 평가하기 위한 일관된 모니터링이 이루어지지 않음.

나. 목표 및 요구사항

- **목표**: 온프레미스·클라우드 환경에 리소스가 모두 존재하는 하이브리드 환경에서, 접근 주체인 사용자·기기에 대한 일관된 통합 인증 및 세밀한 접근제어 및 모니터링이 가능해야 함.

- **요구사항**

① 기업은 리소스의 위치와 관계없이 일관되고 세밀한 접근제어 정책 수립 및 집행이 가능해야 함.

② 리소스의 위치와 관계없이 해당 리소스에 접근하는 사용자와 기기에 대해 통합된 인증을 제공할 수 있어야 하며, 해당 사용자 및 기기에 대해 모니터링을 통하여 가시성을 확보하고 지속적으로 신뢰도를 평가할 수 있어야 함.

③ 클라우드에 위치한 리소스에 대한 데이터 노출, 훼손 등에 대해서는 클라우드 사업자가 제공하는 보안 솔루션을 이용할 수 있으며, 온프레미스에 위치한 리소스와 동일한 수준의 보안성을 확보할 수 있어야 함.

다. 제로트러스트 구현 방안

- 온프레미스·클라우드 서비스에 동일하게 적용 가능한 ID 통합(Federation), 다중 인증 등을 지원하는 통합 ID 관리 시스템을 도입함.
- 기업망 내 리소스(네트워크, 시스템, 응용 워크로드 및 데이터) 및 이들에 접근제어 정책을 사전 분류함.
- 온프레미스·클라우드 상의 모든 리소스에 일관되고 중앙 집중적인 정책 관리 및 세밀한 접근제어 기법을 적용함.
- 모든 접근에 대하여 암호화된 통신을 적용함.
- 온프레미스·클라우드 접속 기기 정책 준수 여부 및 기기 상태, 이상 행위에 대한 모니터링, 보안성 검증을 통한 기기 신뢰도 확인함.

5. OT/ICS 등 산업제어 환경

IT와 OT 기술은 전통적으로 분리된 네트워크 인프라를 통해 운영되어 왔다. OT는 보안 못지않게 가용성이 매우 중요한 기술 분야로, 특정한 사용자에 의한 안전한 접근이 필수적이며, 이는 네트워크 접근에 대해 강력한 제한을 하면서도 생산은 멈추지 않아야 함을 뜻한다. 한번 장비와 망을 구축하고 난 뒤에는 문제가 발생하지 않으면 구축된 기술을 최대한 사용하기 때문에 생명 주기(Life Cycle)가 다르며, 보안 패치도 거의 이루어지지 않는다.

그럼에도 OT 기술을 기반으로 산업제어, 기반시설 운용 등을 수행하는 기업에서는 점점 IT 기술과 OT 기술을 통합하는 추세이다. 이는 언제 어디서든 생산 혹은 제어 시설에 대해 원격으로 접속하여 처리할 수 있는 장점이 있기 때문이다. 그러나, 기존의 IT 환경에서 발생한 공격이 OT 환경에 영향을 미치는 경우 매우 심각한 문제를 발생시킬 수 있으며, 또한 점점 OT를 타깃으로 한 공격이 늘어나는 추세라는 점을 고려하면 OT 환경에 제로트러스트를 도입해야 할 필요성은 충분히 있다.

가. 기존 접근법

- 기존에는 IT와 OT 네트워크를 물리적으로 분리하여 운영하였음. 다만, 최근 들어 산업제어용 IoT 기기 등의 출현으로 IT-OT의 경계가 모호해지거나 부분적으로 통합하는 사례가 나옴.
- 대부분의 OT 기기는 구형으로, 강력한 암호화 및 인증 등의 기능을 탑재하고 있지 않거나 설정되어 있지 않으며, 보안 패치의 적용도 거의 불가능에 가까움. 새로운 제로트러스트 에이전트 등을 탑재하기 어려운 환경일 가능성이 있음, OT 환경에서는 인터넷이 아닌 산업제어용 네트워크를 사용하기도 함.
- 2021년 가트너가 발행한 'OT 보안 시장 가이드' 문서에 따르면 전 세계 기업 중 60%가 OT 보안의 중요성을 인식하는 수준에 그쳤을 뿐, 실질적인 보안 기법을 도입하지 않고 있었음.

나. 목표 및 요구사항

- **목표**: IT/OT 환경에서 발생한 공격이 OT 환경에 영향을 주지 않도록, 모든 접근 주체에게 최소 권한을 부여하여 공격자의 횡적 이동이 원천적으로 불가능하고 상황인지 기반 조건부 접근제어 가능해야 함.

- **요구사항**
  ① IT 환경에 적용된 제로트러스트 구현 원칙과 사례가 OT 환경에서도 거의 동일하게 적용되어야 함.
  ② OT 환경에서 발생할 수 있는 위험성을 최소화하면서도 지속적인 운영이 가능하도록, 정책을 집행하기 전에 신뢰도를 정확히 평가하기 위하여 OT 네트워크에 접근한 모든 기기 및 트래픽에 대한 모니터링 및 자동화, 통합 분석이 가능해야 함.
  ③ 구형 OT 기기의 성능 한계 등의 사유로 강화된 인증을 적용하기 어려운 기기들이 있을 수 있으며, 이 경우 최소권한 부여를 통한 마이크로 세그멘테이션 및 지속적인 모니터링함.
  ④ 접근제어 정책을 설계할 때 잘못된 정책 적용으로 비정상적인 접근제어가 이루어지지 않도록, 기계학습 기반 신뢰도 평가 등은 충분한 검증 후 적용함.
  ⑤ OT 가용성에 문제를 일으킬 수 있는 응용 접근 시, 가능하다면 다중 인증 등 강화된 인증 기술 적용함.

다. 제로트러스트 구현 방안

- 처음부터 전사적으로 제로트러스트를 구현하기보다는, OT 환경의 일부에 개념 증명 혹은 파일럿을 수행하는 것으로 시작함.
- 운영 전 요구사항, 접근제어 정책 등에 대해 OT 운영에 영향이 없도록 신중하게 설계함.
- 특히, OT 네트워크 혹은 내부 응용 등 OT 리소스에 접근하는 접근 주체에 대해서는 마이크로 세그멘테이션이 가능하도록 보안 및 정책 준수 요구사항을 규정하여, 다중 인증 등 강화된 인증 적용, 기기 정책 준수 여부 및 기기 상태, 이상 행위에 대한 모니터링, 보안성 검증을 통한 기기 신뢰도 확인, 컨텍스트 기반 접근제어 등 기술 적용 필요함.
- OT 기기에 제로트러스트 접근제어를 위한 에이전트 설치가 어려운 경우, 게이트웨이 포탈에서 해당 기기에 대한 엄격한 최소 권한 기반 세밀한 접근제어 정책을 생성·적용함.
- 안전성이 충분히 검증될 때까지는 기계학습 기반의 이상행위 모니터링 및 신뢰도 평가보다는 규칙 기반으로 판단·결정함.

6. M2M(Machine-to-Machine) 환경

여섯번째 유스케이스는 기기 간 통신 혹은 사물지능통신 환경에 관한 것이다. 기업에 따라서는 기업 내부에서 여러 가지 목적으로 IoT 기기, 드론, 센서 등이 통신을 하며 데이터를 주고 받을 수 있다. 기기가 외부에 있어야 하는 경우에는 기업망으로 데이터를 이동하기 위한 중개 역할을 하는 기기와 통신을 할 수도 있을 것이다. 이렇게 생성된 데이터는 일반적으로 데이터 수집을 담당하는 기기를 거쳐, 중앙 집중적인 방식으로 데이터를 가공하는 것이 일반적일 것이다.

일반적으로 이들 저성능 기기 혹은 사물은 사용자가 직접 이용하지 않으므로, 다른 기기 혹은 네트워크에 접속을 허용하기 위하여 기기 내부에 인증토큰이나 보안 키 등이 탑재되어 있다. 고성능 기기와 비교하여 물리적 탈취 등의 공격에 취약하므로 공격자가 이들을 공략하여 기업망 내부에서 횡적 이동 등의 공격 사례도 가능할 것이다.

따라서, 이 유스케이스에서는 탈취당할 위험성을 고려한 제로트러스트 접근 전략이 필요하다. 모니터링 및 로그 기록을 통하여 이상 행위를 하는지 확인하고, 횡적 이동이 불가능하도록 다른 리소스에 대한 접근을 최소화하기 위한 마이크로 세그멘테이션 전략이 매우 중요할 것이다.

가. 기존 접근법

- 사물지능통신은 응용간 통신, 데이터베이스 전송, API 호출 등의 방식으로 이루어짐.
- 이러한 통신은 2가지 방식 중 하나로 동작하며, 첫번째는 기업망 혹은 서브넷으로 제한된 기기가 다른 기기를 호출할 수 있는 권한이 있다고 가정. 이 방법은 특히 내부자 위협에 안전하지 않음. 두번째는 두 기기가 중개하는 서비스 계정 혹은 API 키를 통한 인증을 거치는 방식으로, 감사와 로그, 최소 권한 적용, 안전한 인증 등에 대한 보안 문제 발생 가능.

나. 목표 및 요구사항

- **목표**: 기기를 탈취한 공격자에 의한 위험성을 최소화함으로써 내부자 위협에 노출되지 않아야 함.

- **요구사항**

  ① 연결 위치와 관계없이 다른 리소스에 접근하기 전에 모든 기기의 ID가 인증된 후 권한을 부여되어야 함. (특히, 기기 인증을 위한 위험도 감지, 침해 방지를 위한 동적 정책 기반 접근제어 시행, 중앙 집중적 인증 정보 관리 전략 사용 필요)

  ② 필요 시, 강력한 다중 인증을 통해 패스워드를 제거해야 함.

  ③ 기계학습 및 임시 규칙을 통해 위험도/신뢰도를 지속적으로 모니터링하고 평가해야 함.

  ④ 중요한 워크로드에 접근하는 모든 주체에 대해 다음을 확인함. (특정 워크로드에 접근할 수 있는 권한 보유 여부, 정상 인증 여부, 필요할 때 추가 인증 시행)

  ⑤ 사용자/기기를 식별할 때는 사용자/기기 행동 패턴을 고려해야 함.

다. 제로트러스트 구현 방안

- 편리하고 안전한 인증 및 접근제어 관리가 가능한 보안 기술 혹은 표준[29]을 준수하는 기기를 도입함으로써, 기기에 대해 안전하게 설치 및 관리함.
- 마이크로 세그멘테이션이 가능하도록 보안 및 정책 준수 요구사항을 규정하여, 기기 정책 준수 여부 및 기기 상태, 이상 행위에 대한 모니터링, 보안성 검증을 통해 기기 신뢰도를 확인함.
- 기기에 제로트러스트 접근제어를 위한 에이전트 설치가 어려운 경우, 게이트웨이 포탈에서 해당 기기에 대한 엄격한 최소 권한 기반 세밀한 접근제어 정책을 생성·적용함.
- 기기 간 인증 및 통신 암호화 적용을 통한 데이터 보호 기법 적용함.
- 기계학습 기반의 이상 행위 모니터링 및 로그를 활용하는 자동화 및 통합 기술을 적용함.

---

29 예를 들어, IETF RFC 8520에서 정의한 MUD(Manufacturer Usage Description) 규격에서는 IoT 장비들에 대한 안전한 관리 기술의 표준을 포함하고 있다. 관리를 위해 기기 생산자가 지정한 URL을 기기에 포함하며, 기기는 네트워크에 접근할 때 URL을 전송하고 이를 수신한 라우터 혹은 보안 장비가 관리 명세를 받아오는 방식으로 동작하는데, 이 과정에서 보안을 위해 기기 식별자 및 인증을 부여한다. 해당 표준에는 명시되어 있지 않으나, 일반적으로 TPM과 같은 신뢰 모듈을 탑재하여 이 영역에서 보안 정보들의 저장 및 처리가 이루어진다.

제로트러스트
가이드라인 1.0

ZERO TRUST

부 록

- 제로트러스트 관련 용어
- 기존 문서에서 정의한 제로트러스트 아키텍처 기본 원리

■ 제로트러스트 관련 용어

1. 보안 기술 및 솔루션 관련 용어

〈표 S-1-1〉 보안 기술 및 솔루션 관련 용어

용 어	의 미
ABAC (Attribute-Based Access Control)	▸ 속성 기반 접근 제어 모델로, 속성 정보(사용자의 속성, 장치 정보, 위치 정보)를 사용하여 접근 제어 관리하는 보안 모델 ▸ 예를 들어, 사용자가 접근하려는 리소스의 위치나 사용자가 접속하는 기기 등의 속성에 따라 접근을 허용하거나 거부 가능
CASB (Cloud Access Security Broker)	▸ 클라우드 기반 리소스에 접근할 때 기업(조직) 보안 정책을 결합·개입하기 위해 클라우드 서비스 소비자와 클라우드 서비스 공급자 사이에 배치되는 온프레미스 또는 클라우드 기반 보안 정책 시행 지점 (Pep) ▸ 다양한 보안 정책(예, 인증, Single Sign-On, 권한 부여, 자격 증명 매핑, 장치 프로파일링, 암호화, 토큰화, 로깅, 경고, 맬웨어 탐지/방지) 시행 통합 솔루션
CDM (Continuous diagnostics and mitigation)	▸ Cisa에서 연방 정부 네트워크 및 시스템의 사이버 보안을 강화하기 위한 동적 접근 방법을 제공하는 프로그램으로, 다음 방법을 통해 참여 기관이 보안 상태를 개선하는데 도움을 주는 사이버 보안 도구, 통합 서비스, 대시 보드를 산출 - 기관에 대한 공격 표면 감소 - 연방 사이버 보안 상태에 가시성 증가 - 연방 사이버 보안 응답 능력 개선 - 연방 정보보안 현대화 법(Fisma)의 보고 절차 현대화(능률화)
CIEM (Cloud Infrastructure Entitlement Management)	▸ 클라우드 인프라 상의 Id 및 권한 관리 보안 솔루션 ▸ 최소 권한 원칙 적용: 클라우드 환경에 접근 권한을 이해한 다음 필요한 것보다 더 높은 수준의 접근 권한을 부여함으로써 발생하는 위험을 식별하고 완화
CWPP (Cloud Workload Protection Platform)	▸ 클라우드 환경에서 워크로드 보안을 제공하는 솔루션으로, 클라우드 환경에서 실행되는 애플리케이션, 서버, 컨테이너 등의 워크로드 보호 (여러 클라우드 서비스 제공업체에서 호스팅되는 워크로드를 식별하고, 보안 취약점을 식별하며, 악성 공격으로부터 보호) - 워크로드 보안: 클라우드 환경에서 실행되는 워크로드를 보호하며, 악성 코드, 스파이웨어, 랜섬웨어 등의 공격으로부터 보호 - 보안 취약점 관리: 워크로드에서 발견된 보안 취약점을 자동으로 식별하고, 이를 보고서로 제공 - 네트워크 보호: 네트워크 트래픽을 모니터링하고, 악성 트래픽을 차단하는 방화벽 기능을 제공 - 규정 준수: 규제 준수 요구 사항을 준수하기 위한 정책 및 감사 기능 제공 - 인텔리전스 기반 보안: Cwpp는 머신러닝 및 기타 인공지능 기술을 사용하여 워크로드를 식별하고, 이를 보안 평가 및 적용에 사용

용 어	의 미
DASB (Data Access Security Broker)	▸ 기업·기관 시스템 데이터에 대한 접근 제어·모니터링을 위해 설계된 보안 솔루션으로, 시스템 사용자와 사용자가 접근하는 데이터 사이에서 접근에 대한 보안 정책 및 제어 시행 역할 ▸ 클라우드, 디지털 권한 관리(Drm) 및 데이터 유출 방지(Dlp) 등을 결합하여 데이터가 생성, 수정, 저장 및 공유되는 위치에 관계없이 지속적인 데이터 보호 및 가시성 제공
Data Tagging	▸ 데이터 태깅은 관리, 검색 및 분석을 더 쉽게 만드는 방식으로 데이터에 레이블을 지정하거나 분류하는 프로세스 (레이블 또는 태그는 수동 또는 자동으로 적용할 수 있으며 범주, 속성 또는 기타 관련 특성별로 데이터를 구성하는 데 사용 가능) ▸ 데이터 관리·분석에 중요한 역할을 하며, 데이터를 분류하고 레이블을 지정함으로써 기관의 생산성, 정확성 및 협업 개선 가능
DevSecOps	▸ 데브섹옵스(Devsecops)란 소프트웨어 개발(Development)과 운영(Operation), 보안(Security)의 합성어로 애플리케이션 개발자와 운영, 보안 실무자 간의 소통과 협업, 통합을 강조하는 개발 문화를 의미 ▸ 직무분리 및 책임추적성 등을 위해 개발과 운영, 보안조직을 분리 운영했던 과거It조직 체계로는 급속도로 변화하는 비즈니스 환경에서 발생하는 문제점 해결을 위해, Devops와 보안(Security)이 결합하여 개발 Pipeline의 과정에서 보안 정책 및 기술 반영
DLP (Data Loss Prevention)	▸ 중요한 데이터에 대한 무단 액세스, 사용, 공개 또는 손실 등을 식별하고 방지하기 위한 보안 솔루션 ▸ 조직이 온프레미스, 클라우드 및 기기 등에서 민감한 정보(예, 개인 식별 정보(Pii), 금융 정보, 지적 재산 및 영업 비밀 등)를 모니터링하고 보호할 수 있는 기능 포함 ▸ 데이터 암호화, 접근 제어 및 모니터링과 같은 다양한 기능이 포함함으로써 민감한 데이터의 기밀성, 무결성 및 가용성을 보장하고 데이터 손실 또는 위반 방지
DMS (Desktop Management System)	▸ 조직 내의 컴퓨터 환경을 관리하고, 유지보수하는 소프트웨어 솔루션으로, 대규모 Pc 환경에서 소프트웨어 설치, 패치 관리 및 업데이트, 인벤토리 관리, 원격 제어, 보안, 백업 등의 효율적 수행 지원
DRM (Digital Rights Management)	▸ 영화, 음악 및 전자책과 같은 디지털 콘텐츠를 무단 복사, 배포 및 사용으로부터 보호하기 위한 솔루션 ▸ 일반적으로 암호화, 접근 제어, 복사 및 배포 제한, 사용량 모니터링 등의 기능을 제공함으로써 권한 없는 사용자가 디지털 콘텐츠에 접근·공유하는 것을 제한
EDR (Endpoint Detection and Response)	▸ 기업에서 엔드포인트 동작에 대한 보안 위협을 탐지하고 대응하기 위한 솔루션으로, 컴퓨터, 서버, 랩톱, 모바일 기기 등과 같은 엔드포인트에 에이전트 소프트웨어를 설치하여, 실시간으로 네트워크 활동을 모니터링하고 이상 징후를 탐지하는 역할을 수행 ▸ 엔드포인트에 대한 시스템 수준의 동작을 기록 및 저장하며, 다양한 데이터 분석 기술을 사용하여 의심스러운 시스템 동작 감지, 상황 정보 제공, 악의적인 활동 차단, 복원을 위한 수정 제안 등을 제공하는 솔루션
IAM (Identity Access Management)	▸ 적합한 사람과 기기가 적시에 원하는 애플리케이션, 리소스 및 시스템에 접근할 수 있도록 허용하는 프레임워크로, 인증 및 권한 관리에 사용 ▸ 로그인 기록 수집, 사용자 Id 관리, 권한 할당/부여/제거 프로세스 수행·감독 등의 기능을 포함

용 어	의 미
ID Federation (Identity Federation)	▸ 여러 기업, 기관, 서비스간의 인증 및 권한 부여 정보를 공유하여 사용자가 다른 기관이나 서비스에 로그인할 때 별도의 인증 절차를 거치지 않는 것을 지원하는 기술 ▸ Sso(Single Sign-On)은 동일한 도메인 내에서 여러 서비스에 로그인할 때 별도의 인증 과정을 거치지 않아도 된다는 개념이며, Id Federation은 서로 다른 도메인 간의 인증 정보를 공유하여 Sso를 구현하는 방법 중 하나로, Saml(Security Assertion Markup Language), Oauth(Open Authorization), Openid Connect 등의 프로토콜을 이용하여 구현 가능
IDaaS (Identity-as-a-Service)	▸ Id 및 액세스 관리(Iam)를 위한 클라우드 기반 모델로, Mfa(다중 인증), 패스워드 없는 접근부터 Sso(싱글 사인 온)에 이르기까지 광범위한 Iam 기능을 제공
IPAM (IP Address Management)	▸ Ip 주소 인프라의 종단간 계획, 배포, 관리 및 모니터링을 지원하는 통합 도구 ▸ 주소 할당, 인벤토리 관리, Ip 주소 사용 추적, Dns 및 Dhcp 구성 등의 작업을 포함하며, Ip주소 인프라 서버 및 Dns 서버를 자동 검색하여 중앙 인터페이스를 통해 관리 가능
MDM (Mobile Device Management)	▸ 스마트폰 및 미디어 태블릿에 대한 소프트웨어 배포, 정책 관리, 인벤토리 관리, 보안 관리 및 서비스 관리와 같은 기능을 제공하는 소프트웨어를 포함하는 솔루션으로, 대상 모바일 기기를 보호, 관리, 감시, 지원 기능 포함 ▸ 예를 들어, 안전한 패스워드 설정, 모바일 애플리케이션 배포, 도난 및 분실시 원격 자료삭제 등이 가능하며, 악성 프로그램 및 기타 사이버 위협으로부터 디바이스를 안전하게 보호하는 기능을 포함하기도 함
Micro-Segmentation	▸ 기업망 내부의 모든 리소스(네트워크, 시스템, 워크로드, 응용, 데이터)에 접근하는 사용자와 기기에 세분화된 접근제어 정책을 적용함으로써 공격자의 횡적 이동을 어렵게 하는 보안 기법 혹은 기술
NAC (Network Access Control)	▸ 네트워크 보안 솔루션의 하나로, 네트워크 접근을 제어하고 보안 수준을 높이기 위한 정책(사용자, 장치, 애플리케이션 등의 인증, 권한 부여, 접근 제어 등) 시행 - Endpoint Security: Agent를 통해, 단말 보안 소프트웨어 업데이트, 악성 코드 검사 등을 수행 - Authentication And Authorization: 사용자와 장치의 식별, 인증, 권한 부여를 담당하며, 사용자는 사용자 이름과 비밀번호로, 장치는 Mac 주소, Ip 주소 등으로 인증 - Network Enforcement: 네트워크에서 규칙에 맞지 않는 접근 차단 및 정책 시행 (규칙 위반 여부 확인 후 규칙 위반 장치에 대해 차단, 격리, 경고 등의 조치)
OAuth (Open Authorization)	▸ 인터넷 사용자들이 패스워드를 제공하지 않고 다른 웹사이트 상의 자신들의 정보에 대해 웹사이트나 애플리케이션의 접근 권한을 부여할 수 있는 공통적인 수단으로서 사용되는, 접근 위임을 위한 개방형 표준 ▸ 2007년 4월 처음 논의되어, 2010년 Ietf에서 Rfc 5849로 버전 1.0 발표 후, 2012년 10월 버전 2.0이 Rfc 6749로 업데이트 ▸ 동작 방식은 크게 네 가지로 분류되며 권한 부여 승인을 위해 자체 생성한 Authorization Code를 전달하는 Authorization Code Grant 방식, 자격 증명을 안전하게 저장하기 힘든 클라이언트(Ex: Javascript등의 스크립트 언어를 사용한 브라우저)에게 최적화된 Implicit Grant 방식, 간단하게 Username, Password로 Access Token을 받는 Resource Owner Password Credentials Grant 방식, 클라이언트의 자격 증명만으로 Access Token을 획득하는 Client Credentials Grant 방식으로 나뉨

용 어	의 미
PAM (Privileged Access Management)	▸ Pam(Privileged Access Management)은 중요한 리소스에 대한 무단 접근을 모니터링, 감지 및 방지함으로써 사이버 위협으로부터 조직을 보호하기 위한 Id 보안 솔루션 ▸ 사용자, 프로세스 및 기술의 조합하여 작동하며, 아래 기능을 통하여 권한 있는 계정을 사용하는 사람과 로그인 중에 수행 작업에 대한 가시성 제공 – 다단계 인증 요구 – Jit(Just In Time) 액세스 제공 – 보안 자동화 – 활동 기반 액세스 제어 – 권한 있는 액세스 제어 및 모니터링 등
RBAC (Role-Based Access Control)	▸ 역할 기반 액세스 제어 모델로, 기관·기업 내에서 사용자 역할과 권한 관리 ▸ 각 사용자는 하나 이상의 역할을 가질 수 있으며, 각 역할은 그룹화된 사용자들이 접근할 수 있는 권한 집합을 정의 (예를 들어, It 부서의 사용자들은 파일 서버에 접근할 수 있으나, 회계 부서의 사용자들은 접근 권한 없음)
SASE (Secure Access Service Edge)	▸ 2019년 Gartner가 현대적인 사이버 보안 아키텍처를 표현하기 위해 개발한 용어로, 방화벽, Casb, Ztna, Dlp 등의 클라우드 보안 기능과 Vpn, Sd-Wan 등의 네트워크 기능이 통합된 클라우드 기반 네트워크 서비스 모델 ▸ 클라우드 서비스를 이용하는 사용자들의 개별 네트워크, 보안 기능을 통합하고 지능화하여 클라우드 보안 가시성 확보 및 고품질 네트워크 서비스를 제공하며, Sase의 핵심 기능으로 포함된 기존 솔루션들은 다음과 같음 – Sd-Wan (일반 인터넷 기반 오버레이 네트워크 Vpn 서비스) – Sd-Branch (프로그래머블 네트워크 오케스트레이션 기술) – Casb (클라우드 가시성 확보, 위협 방지 등 보안 기능) – Dlp (지적재산 보호, 데이터 외부 유출 방지 및 감사)
SDP (Software Defined Perimeter)	▸ 안전하지 않은 네트워크로부터 서비스를 격리하기 위해 필요한 경계 기능을 응용 소유자에게 제공하는 기술로, 동적으로 프로비저닝되는 네트워크를 가능하게 함으로써 네트워크 기반 공격을 완화 ▸ '외부인'에게 보이지 않고 접근할 수 없다는 기존 모델의 가치를 유지하면서도 어디에서든(인터넷, 클라우드, 호스팅 센터, 사설 기업 네트워크 또는 이러한 위치의 일부 또는 전체) 논리적 네트워크 경계를 배포할 수 있는 능력을 부여함으로써 경계 기반 보안 모델의 문제를 해결 (Ztna의 구현 기술 중 하나로 보기도 하며, 마이크로 세그멘테이션을 가능하게 할 수 있음)
SD-WAN (Software Defined Wide Area Network)	▸ 기존의 광대역 인터넷과 프라이빗 링크를 통해 광역 네트워크 연결에 가상화된 리소스를 제공하는 소프트웨어 기반 네트워크 기술 및 솔루션 ▸ 클라우드 제공 및 소프트웨어 기반으로 중앙 관리 및 제어 가능하며, 임대 회선의 Wan 트래픽을 조절하고 일부를 광대역 인터넷 연결 및 클라우드 기반 애플리케이션으로 전환 가능 ▸ 모든 유형의 네트워크 트래픽을 동적으로 라우팅하여 애플리케이션과 데이터 제공을 최적화하며, 중앙에 위치한 Orchestrator가 모든 네트워크 활동을 모니터링하여 실시간 분석 및 보고 제공
SIEM (Security Information and Event Management)	▸ 소프트웨어 제품 및 서비스가 보안 정보 관리(Sim)와 보안 이벤트 관리(Sem)를 결합하여, 다양한 기타 이벤트 및 상황별 데이터 소스뿐만 아니라 보안 이벤트의 수집 및 분석(거의 실시간 및 기록 모두)을 통해 위협 감지, 컴플라이언스 및 보안 사고 관리를 지원하는 보안 솔루션 ▸ 로그 이벤트 수집 및 관리, 이종 소스로부터의 로그 이벤트 및 기타 데이터 분석, 운영 기능(예: 사고 관리, 대시보드 및 보고) 등을 포함

용 어	의 미
SOAR (Security Orchestration, Automation, and Response)	▸ Soar는 다양한 사이버 위협에 대해, 대응 수준을 자동으로 분류하고 표준화된 업무 프로세스에 따라 보안 업무 담당자와 솔루션이 유기적으로 협력할 수 있도록 지원하는 보안 기술·솔루션 ▸ 여러 유형의 사이버 위협에 대한 대응 절차를 자동화하여, 단순한 보안 이슈에 대해선 보안 업무 담당자 없이 자체 해결이 가능해야 하며, 복잡한 보안 사고 발생시 보안 운영 센터 관리자가 쉽게 대응할 수 있도록 지원
SSE (Secure Service Edge)	▸ 웹, 클라우드 서비스 및 개인 응용에 대한 접근 보호를 위한 보안 솔루션을 의미하며, Sase의 보안 부분(Casb, Swg, Ztna)만을 포함하는 기술 ▸ 기능에는 접근제어, 위협 보호, 데이터 보안, 보안 모니터링, 네트워크 기반 및 Api 기반 통합에 의해 시행되는 사용 허용 제어를 포함하고, 주로 클라우드 기반 서비스로 제공되며 온프레미스 또는 에이전트 기반 구성 요소를 포함할 수 있음
UAF (Universal Authentication Factor)	▸ 지문, 음성, 얼굴 인식 등의 사용자 고유 생체 정보를 인식하여 인증하는 모바일 중심의 인증 방식으로, 스마트폰 등 사용자 단말기의 생체 정보를 이용하여 사용자를 인증한 후 비 대칭키 쌍(개인키, 공개키)을 생성하고 서비스 제공 서버에 공개키를 등록하여 원격 인증 수행한다.
U2F (Universal 2nd Factor)	▸ 아이디, 비밀번호 방식으로 1차 인증 후 1회용 보안키가 저장된 Usb 또는 스마트카드를 이용하여 2차 인증하는 Pc 중심의 인증 방식하는 방식이다.
VDI (Virtual Desktop Infrastructure)	▸ 중앙 서버에서 가상 머신으로 실행되고, 클라이언트에서 원격으로 접근하는 가상 데스크톱을 제공·관리하는 사용자 환경 및 솔루션 ▸ 사용자는 사용자와 서버 사이에서 중개자 역할을 수행하는 연결 브로커(소프트웨어 기반 게이트웨이)를 통해 장소와 기기에 구애받지 않고 가상 데스크톱에 접근할 수 있고, 모든 처리는 호스트 서버에서 이루어짐 – 데스크톱 소프트웨어를 호스팅하는 서버 가상화 소프트웨어 (서버 워크로드) – 사용자를 데스크톱 환경에 연결하는 중개/세션 관리 소프트웨어 – 가상 데스크톱 소프트웨어 스택의 프로비저닝 및 유지보수 관리 도구
VPN (Virtual Private Network)	▸ 인터넷을 통해 디바이스 간에 사설 네트워크 연결을 생성하는 기술로, 공개 네트워크를 통해 데이터를 안전하게 전송하는 데 사용 ▸ 안전한 공개 인터넷 접근, 검색 기록 비밀 유지, 신원 보호 등을 위하여 사용되기도 하나, 경계기반 보안 기술이 도입된 기업망에서 경계를 확장하는 용도(재택·원격 근무자의 기업망 접속 지원 등)로 사용되며, 두 장치/네트워크 사이에 암호화된 개인 터널 생성 ▸ Pptp(Point-To-Point Tunnelling Protocol), L2tp(Layer Two Tunnelling Protocol), Ipsec(Internet Protocol Security), Ssl(Secure Sockets Layer)과 같은 여러 Vpn 터널링 프로토콜 존재
ZTNA (Zero Trust Network Access)	▸ 하나의 응용 프로그램 혹은 응용 프로그램 집합 주위에 신원 혹은 컨텍스트 기반 논리 접근 경계를 생성하는 솔루션 혹은 서비스 ▸ 응용 프로그램은 검색에서 숨겨지며, 접근은 신뢰 브로커를 통해 명명된 엔티티 집합으로 제한 ▸ 브로커는 접근을 허용하기 전, 특정 참가자들의 신원, 컨텍스트 및 정책 준수 여부를 확인하고 네트워크의 다른 곳에서 횡적 이동을 금지함으로써, 프로그램 자산이 공개적으로 노출되는 것을 막고, 공격 노출 영역을 크게 감소

2. 약어

- **ABAC** Attribute-Based Access Control
- **ACL** Access Control List
- **API** Application Programming Interface
- **BYOD** Bring Your Own Device
- **CA** Certificate Authority
- **CASB** Cloud Access Security Broker
- **CC** Common Criteria
- **CDM** Continuous Diagnostics and Mitigation
- **CERT** Computer Emergency Response Team
- **CI/CD** Continuous Integration/Continuous Deployment
- **CMVP** Cryptographic Module Validation Program
- **C-TAS** Cyber Threat Analysis and Sharing
- **DaaS** Desktop as a Service
- **DAAS** Data, Application, Asset, Service
- **DMS** Desktop Management System
- **EDR** Endpoint Detection and Response
- **FIDO** Fast IDentity Online
- **IaaS** Infrastructure as a Service
- **IaC** Infrastructure as Code
- **IAM** Identity and Access Management
- **IAP** Identity-Aware Proxy
- **ICAM** Identity, Credential and Access Management
- **ICS** Industrial Control System
- **IoT** Internet of Thing
- **IPAM** IP Address Management
- **ISMS** Information Security Management System
- **ISMS-P** Personal Information & Information Security Management System
- **MDM** Mobile Device Management
- **MFA** Multi-Factor Authentication
- **MISP** Malware Information Sharing Platform

- **MPLS** Multi-Protocol Label Switching
- **MSA** Micro Service Architecture
- **MUD** Manufacturer Usage Description
- **M2M** Machine-to-Machine
- **NAC** Network Access Control
- **OT** Operational Technology
- **OTP** One-Time Password
- **OTX** Open Threat eXchange
- **PA** Policy Administrator
- **PaaS** Platform as a Service
- **PDP** Policy Decision Point
- **PE** Policy Engine
- **PEP** Policy Enforcement Point
- **PKI** Public Key Infrastructuire
- **RBAC** Role-Based Access Control
- **SaaS** Software as a Service
- **SASE** Secure Access Service Edge
- **SDN** Software-Defined Networking
- **SDP** Software-Defined Perimeter
- **SD-WAN** Software-Defined Wide-Area Network
- **SIEM** Security Information and Event Management
- **SOAR** Security Orchestration, Automation, and Response
- **SSE** Secure Service Edge
- **SSO** Single Sign On
- **SWG** Secure Web Gateway
- **TLS** Transport Layer Security
- **VDI** Virtual Desktop Infrastructure
- **VPN** Virtual Private Network
- **ZT** Zero Trust
- **ZTA** Zero Trust Architecture
- **ZTNA** Zero Trust Network Access

■ 기존 문서에서 정의한 제로트러스트 아키텍처 기본 원리

1. Forrester, Zero Trust Model (2010년)

Forrester Research 애널리스트인 John Kindervag이 기업망에서 더 엄격한 사이버 보안 프로그램 및 접근제어의 필요성을 강조하기 위해 제안한 제로트러스트 네트워크 아키텍처에서는 신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크를 구별하지 않고, 모두 신뢰할 수 없는 네트워크를 그 배경으로 한다. 여기에 보호해야할 자원을 모두 식별하고, 이 자원에 대한 접근통제 기능을 적용, 모든 주체에 대한 검증과 사용자의 행위에 대한 로그 기록에 대한 요구사항을 바탕으로, 〈표 S-2-1〉과 같은 세 가지 기본적인 개념을 제안하였다.

〈표 S-2-1〉 Forrester 제로트러스트 모델의 3가지 기본 개념

구분	개념	설명
1	위치에 관계없이 모든 리소스는 안전하게 접근됨을 보증할 것	‣ 보안 경계의 개념이 제거되었으므로, 인증·검증·확인된 트래픽을 제외한 여타 트래픽은 모두 위협으로 간주한다. ‣ 모든 트래픽을 위협원으로 간주하는 범위에는 VPN 터널링 세션도 포함한다.
2	최소 권한 전략을 채택하고 접근제어를 강력히 집행할 것	‣ 권한 할당시에는 최소 권한을 적용하며, 엄격한 접근통제 기능을 적용해야 한다. ‣ 사용자가 다른 정보에 접근하려는 행위 발생 가능성을 최소화할 수 있다.
3	모든 트래픽을 검사하고 기록을 남길 것	‣ 허가된 접근이라 할지라도, 그 접근은 악의적일 수 있다. ‣ 그러므로 'Verified but Never Trust(검증하였지만 불신)'의 개념을 적용하여, 모든 트래픽에 대한 로그를 기록하고 분석하여 실시간으로 보안 위협을 식별할 수 있어야 한다.

John Kindervag은 네트워크 관점에서 제로트러스트를 주장하였으며, 사용자가 자신의 작업을 위해 필요한 리소스에만 접근하도록 제한하고, 정상적인 행위를 하는 사용자를 신뢰하기보다 사용자가 정상적인 행위를 하는지를 검증하도록 하였으며, 실시간으로 끊임없이 네트워크 트래픽을 검사하고 기록함으로써 제로트러스트를 달성할 수 있다고 주장하였다.

2010년 네트워크 관점에서 처음으로 제시한 제로트러스트의 개념인 만큼, 보호 대상에 데이터 및 응용을 포함하여 논의하고 있는 현재의 제로트러스트 모델보다는 주로 네트워크 방면으로 치우쳐져 있으며, 내부 구성 요소 및 정의가 불명확할 수 있으나, 네트워크 위치와 관계없이 세밀한 접근제어와 끊임없는 검증을 강조하고 있는 제로트러스트의 기본 철학과 개념은 여전히 참고할 만 하다.

2. CSA, Software Defined Perimeter (2013~2022년)

미국 CSA(클라우드 보안 협회)는 2013년 12월, 'Software Defined Perimeter' 문서를 발간하였으며, SDP 규격으로서 2014년 4월 'SDP Specification 1.0', 그리고 2022년 3월 'Software-Defined Perimeter (SDP) Specification v2.0' 문서를 추가로 발간하였다.

'SDP Specification 1.0' 문서에서, 기업들은 외부 보안 위협에 대항하여 데이터 센터 내부에 경계 기반 보안 솔루션을 설치하였으나, 이러한 경계 기반 보안 모델이 아래의 2가지 이유로 유용하지 않게 되었다고 하였다.

- 해커들이 경계 내부 기기에 대한 접근 권한을 획득하여 내부 응용 인프라를 손쉽게 공격하며, BYOD, 파트너 등 경계 내부에 있는 기기의 수가 많아짐에 따라 해당 취약점 또한 증가.
- 전통적인 데이터 센터는 클라우드에 기반한 외부 리소스와 결합되고 있으며, 이에 따라 경계 기반 보안 장비의 물리적 위치가 응용 인프라를 보호하기에 부적절.

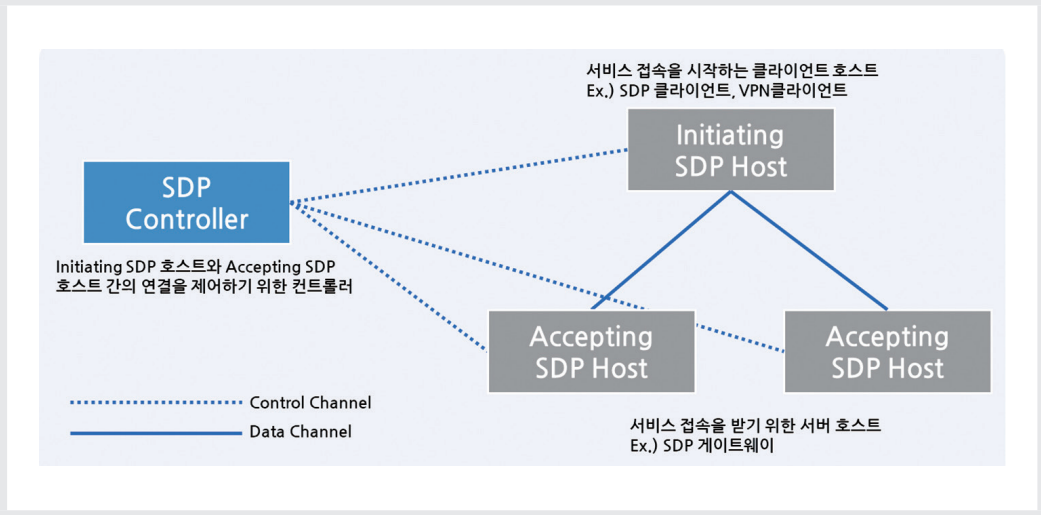
2020년 5월 발행한 'Software Defined Perimeter (SDP) and Zero Trust' 문서에서는, 위 문제와 함께 기존 네트워크 아키텍처의 일반적인 약점을 1) 연결 후 인증, 2) 단말 모니터링의 어려움, 3) 패킷 검사에서 사용자 컨텍스트 파악 한계 등 3가지로 소개한 후 제로트러스트의 전략을 SDP 관점에서 다음과 같이 기술하였다.

- 접속 전 인증
- 네트워크 연결 제한 기능
- 세밀한 신뢰 인증 메커니즘
- 의심스러운 행위 모니터링

이를 위해 CSA에서 제안한 SDP(Software Defined Perimeter, 소프트웨어 정의 경계)는 응용 소유자에게 필요한 곳에 경계 기능을 배포할 수 있는 기능을 제공하는 것을 목표로 한다. 네트워크 경계를 기반으로 하는 물리적 보안 솔루션을 응용 소유자의 통제하에 작동하는 논리적 솔루션으로 대체하며, 기기에 대한 증명 및 신원 확인 후에만 응용 인프라에 대한 접근을 제공하고자 한다.

SDP의 개념적 구조는 [그림 S-2-1]과 같다. 여기에서 SDP Controller는 어떤 SDP Host들이 통신할지를 결정하며, 이를 위해 인증, 서버 식별 등을 제공하는 외부 인증 서비스에 관련 정보를 전달할 수 있다. 또한 Initiating SDP Host는 SDP Controller와 연결 가능한 Accepting SDP Host 리스트를 요청하며, Accepting SDP Host는 SDP Controller의 요청 시에만 Initiating SDP Host와의 데이터 채널 요청을 받아들이게 된다.

[그림 S-2-1] SDP 구조



(구성 요소: SDP Host와 SDP Controller)

즉, 기존 경계 기반 보안 모델에서 활용하는 물리적 경계를 대체하기 위하여 SDP Controller를 두고 접속 기기(Initiating SDP Host)가 특정 서버 혹은 응용 서비스(Accepting SDP Host)에 접속하려고 할 때 동적으로 논리적 경계를 설정하는 구조이며, 만약 SDP Controller가 Accepting SDP Host에게 데이터 채널 요청을 받아들이라고 요청하지 않는다면 Initiating

SDP Host와 Accepting SDP Host간 데이터 전송이 불가능하게 됨으로써 매우 엄격한 제로트러스트 네트워크 구조를 형성하게 될 것이다.

다만, 여기에서는 물리적인 경계를 논리적인 소프트웨어 기반 경계로 대체하는 구조를 통한 네트워크 공격 및 횡적 이동 대응, 클라우드 서비스에 대한 논리적 접근 구조 등에만 초점을 맞추었을 뿐, 강력한 인증을 통한 사용자와 기기의 세밀한 접근제어 등에 대한 원칙은 정립되지 않거나 기초적인 수준으로만 다루어졌다.

3. Google, BeyondCorp (2014년)

Google BeyondCorp은 원격으로 접속하는 인력이 늘고 이들 인력이 활용하는 기기의 다양화와 함께 클라우드 기반 서비스를 활용하는 사례가 늘어나는 등 기존 경계 기반 보안 모델이 더 이상 적합하지 않은 상황에서도, 보안성을 개선하면서 생산성을 유지하기 위한 목표를 달성하고자 2010년대 초반부터 진행한 사내 프로젝트이다.

이 프로젝트에서 기업망을 더 이상 안전하지 않고 외부망만큼 위험하다는 가정하에 기업 리소스를 접근할 수 있는 환경을 구축하고자 하였다. 이를 위해 접근제어 기능을 네트워크 경계로부터 개별 사용자로 이전하였으며, 접근제어는 '관리되는 기기'의 개념을 통하여, 기기 및 사용자의 자격 증명에만 의존하여 VPN을 사용하지 않고도 기업 리소스에 접근할 수 있도록 구성하였다.

네트워크의 위치와 관계없이 신뢰하지 않는다는 점은 Forrester에서 제안한 제로트러스트 모델과 유사하지만, Google의 BeyondCorp에서는 특히 기기에 대한 엄격한 관리와 인증서 기반의 인증·식별, 사용자 및 그룹 데이터베이스의 엄격한 관리, 싱글사인온(Single Sign-On) 기반 다중 인증, 짧은 시간의 인가 등 제로트러스트 관점에서 사용자와 기기에 대한 인증·접근제어·모니터링 기능이 중요하게 다루어진 것이 특징이다.

구글에서 밝히는 BeyondCorp 원칙은 다음과 같다.

- 서비스에 대한 접근은 연결하는 네트워크에 의해 결정되어서는 안 된다.
- 서비스 접근 권한은 사용자와 기기의 컨텍스트 요소를 바탕으로 제공되어야 한다.
- 서비스에 대한 접근은 모두 인증, 승인, 암호화를 거쳐야 한다.

4. NIST, SP 800-207 (2020년)

NIST SP 800-207에서는 제로트러스트를 정의함에 있어, "무엇을 제외해야 하는가"보다 "포함해야 하는 기본 원리가 무엇인가"라는 관점을 고려하고 있다. 상기 문서에서 제안하는 제로트러스트의 기본 원리(tenet)는 다음과 같다.

〈표 S-2-2〉 NIST SP 800-207 제로트러스트 7가지 기본 원리

원리	세부 내용
① 모든 데이터와 컴퓨팅 서비스는 리소스로 간주	‣ 네트워크는 데이터를 수집기/스토리지로 전송하는 소형 기기, SaaS 및 다른 기능을 포함할 수 있으며, 개인 소유 단말기가 사내 리소스에 접근할 수 있는 경우 이 역시 리소스로 분류할 수 있음.
② 네트워크 위치에 관계없이 모든 통신 보호	‣ 디바이스가 기업 네트워크 내부에 있다고 해서 신뢰를 보장하지 않으며, 모든 통신의 기밀성과 무결성을 보호해야 함.
③ 기업 리소스에 대한 접근을 세션 단위로 승인	‣ 작업을 완료하는데 필요한 최소한의 방식으로 접근을 허가하며, 각 세션에 따라 달리 검토하여 승인해야 함.
④ 동적 정책으로 리소스에 대한 접근 결정	‣ 동적 정책에는 클라이언트 식별자, 응용, 요청을 보낸 자산 상태, 행동 및 환경 속성 등이 포함되며, 동적으로 리소스 접근 결정 필요.
⑤ 모든 자산의 무결성 및 보안 상태 감시·조치	‣ 기본적으로 자산을 신뢰하지 않으며, 리소스에 대한 접근 요청을 판단할 때 자산 상태 감시, 필요에 따라 패치 등 보완조치를 위한 모니터링.
⑥ 모든 리소스의 인증/인가를 강력하게 점검 후 허용	‣ 모든 리소스에 대해 접근 획득→위협 스캔 및 평가→조정→지속적인 신뢰 재평가라는 일정한 사이클로, ICAM, 자산 관리 시스템 도입 및 다중 인증 사용을 권장함.
⑦ 자산, 네트워크, 인프라 등 현 상태에 대한 정보 수집	‣ 자산의 보안 상태, 네트워크 트래픽, 접근 요청과 관련된 데이터를 수집하고 처리하여 획득한 지식을 보안 정책을 개선하기 위해 사용해야 함.

5. NSA & DISA, DoD Zero Trust Reference Architecture Version 2.0 (2022년)

미국 NSA 제로트러스트 엔지니어링 팀은 국방부 산하 DISA(Defense Information Systems Agency, 국방정보시스템국)와 함께, 2021년 2월 '국방부 제로트러스트 참조 아키텍처 버전 1.0' 문서를 발행한 바 있으며, 이후 의견 수렴을 통하여 2022년 7월 버전 2.0 문서를 발행하였다.

이 문서에서, 제로트러스트 보안 모델은 리소스에 대한 보안 접근을 구현하는 방법을 다시

고려하여, 클라이언트 식별자, 응용·서비스 및 요청 자산의 관찰 가능한 상태(다른 행동 및 환경 속성도 포함할 수 있음)를 포함한 동적 정책에 의해 결정된다고 언급하였다. 여기서의 신뢰 수준은 인증 대상의 여러 속성(신원, 위치, 시간, 기기 보안 상태)을 기반으로 구축되며 자격 증명 확인을 넘어 접근 요청을 훨씬 더 철저하게 평가할 수 있는 것이다.

이 문서에서, 제로트러스트는 다음과 같이 5가지 원칙을 가진다.

〈표 S-2-3〉 DoD 제로트러스트 참조 아키텍처 5가지 기본 원칙

원리	세부 내용
① 적대적인 환경을 가정하라	‣ 환경 내외부 모두 악의적인 공격자가 존재하며, 모든 사용자, 기기, 환경(네트워크) 및 모든 비인간 객체들은 신뢰할 수 없는 것으로 취급.
② 규칙 위반을 추정하라	‣ 내부에 늘 공격자가 있다는 가정하에 의식적으로 자원 운용 및 방어. ‣ 접근과 인가 결정에 대해 강력하고 정밀한 검사 수행.
③ 결코 신뢰하지 말고, 항상 검증하라	‣ 기본적으로 접근 거부. ‣ 모든 기기, 사용자, 응용/워크로드 및 데이터 흐름은 최소 권한, 다중 속성 및 동적 사이버 보안 정책을 사용하여 인증 및 명시적 승인.
④ 명시적으로 조사하라	‣ 모든 리소스는 여러 속성을 사용하여 안전한 방식으로 일관된 접근. ‣ 리소스 접근은 조건부이며 행동 및 신뢰 수준에 기반하여 동적 변경 가능.
⑤ 통합 분석을 적용하라	‣ DAAS(데이터, 응용, 자산, 서비스)에 대한 행동 기반 통합 분석 적용 및 모든 트랜잭션 로그 기록.

미 국방부는 웹 응용에 PKI 기반 클라이언트 인증서 혹은 상호 인증서를 기반으로 한 상호 인증이 오랫동안 효과적인 표준이었다고 판단하고 있다.

■ 참고 문헌

[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] Csa, “Sdp Specification 1.0”, 2014.04

[5] Rory Ward Et Al (Google), “Beyondcorp - A New Approach To Enterprise Secuirty”, 2014.12

[6] Barclay Osborn Et Al (Google), “Beyondcorp - Design To Deployment At Google”, 2016.03

[7] Luca Cittadini Et Al (Google), “Beyondcorp Part Iii - The Access Proxy”, 2016.12

[8] Jeff Peck Et Al (Google), “Migrating To Beyondcorp - Maintaining Productivity While Improving Security”, 2017.06

[9] Victor Escobedo Et Al (Google), “Beyondcorp 5 - The User Experience”, 2017.09

[10] Chase Cunningham (Forrester), “The Zero Trust Extended (Ztx) Ecosystem - Extending Zero Trust Security Across Your Digital Business”, 2018.01

[11] Hunter King Et Al (Google), “Beyondcorp - Building A Healthy Fleet”, 2018.03

[12] Act-Iac, “Zero Trust Cybersecurity Current Trends”, 2019.04

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

[14] Csa, “Software Defined Perimeter (Sdp) And Zero Trust”, 2020.05

[15] 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

[16] Nist Sp 800-207, “Zero Trust Architecture”, 2020.08

[17] Nist National Cybersecurity Center Of Excellence(Nccoe), “Zero Trust Cybersecurity: Implementing Zero Trust Archtecture”, Https://Www.nccoe.nist.gov

/Projects/Implementing-Zero-Trust-Architecture, 2020.10

[18] Cyolo, “4 Zero Trust Use Cases For Cisos And It Managers”, 2020.12

[19] 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

[20] Nsa, “Embracing A Zero Trust Security Model”, 2021.02

[21] Steve Turner Et Al (Forrester), “A Practical Guide To A Zero Trust Implementation”, 2021.03

[22] Act-Iac, “Zero Trust Report - Lessons Learned From Vendor And Partner Research”, 2021.05

[23] Executive Order 14028, “Improving The Nation’s Cybersecurity”, 2021.05

[24] Cisa, “Zero Trust Maturity Model - Pre-Decisional Draft Version 1.0”, 2021.06

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

[26] Zerotrustmaturity.org, “Zero Trust Maturity Model (Ztmm) Assessment Results”, 2021.06

[27] 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

[28] Cisa, “Cloud Security Technical Reference Architecture Version 1.0”, 2021.08

[29] 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

[30] Microsoft, “Evolving Zero Trust - How Real-World Deployments And Attacks Are Shaping The Future Of Zero Trust Strategies”, 2021.09

[31] Csa, “Toward A Zero Trust Architecture - A Guided Approach For A Complex And Hybrid World”, 2021.10

[32] Omb(미국 관리예산실), “Moving The U.s. Government Toward Zero Trust Cybersecurity Principles”, 2022.01

[33] Nstac(국가안보통신자문위원회), “Draft Report To The President - Zero Trust And Trusted Identity Management”, 2022.02

[34] Jana Subramanian (Sap), “Rise With Sap: Adopting To Zero Trust Architecture Principles With Sap Cloud Services”, 2022.02

[35] Cisa, “Applying Zero Trust Principles To Enterprise Mobility”, 2022.03

[36] Csa, “Software-Defined Perimeter (Sdp) Specification V2.0”, 2022.03

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

[38] Nist Cswp 20, “Planning For A Zero Trust Architecture: A Planning Guide For Federal Administrators”, 2022.05

[39] Doj (미국 법무부), “U.s. Department Of Justice Information Technology Strategic Plan”, 2022.06

[40] Nist Sp 1800-35a, “Implementing A Zero Trust Architecture - Volume A: Executive Summary (Preliminary Draft)”, 2022.06

[41] 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

[42] 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

[43] 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

[44] Nist Sp 1800-35b, “Implementing A Zero Trust Architecture - Volume B: Approach, Architecture, And Security Characteristics (Preliminary Draft)”, 2022.07

[45] Nist Sp 1800-35c, “Implementing A Zero Trust Architecture - Volume C: How-To Guides (Preliminary Draft)”, 2022.08

[46] Nist Sp 1800-35d, “Implementing A Zero Trust Architecture - Volume D: Functional Demonstrations (Preliminary Draft)”, 2022.08

[47] Dod, “Dod Zero Trust Strategy”, 2022.11

[48] Dod, “Dod Zero Trust Capability Execution Roadmap (Coa 1)”, 2022.11

[49] Nist Sp 1800-35a, “Implementing A Zero Trust Architecture - Volume A: Executive Summary (Second Preliminary Draft)”, 2022.12

[50] Nist Sp 1800-35b, “Implementing A Zero Trust Architecture - Volume B: Approach, Architecture, And Security Characteristics (Second Preliminary Draft)”, 2022.12

[51] Nist Sp 1800-35c, “Implementing A Zero Trust Architecture - Volume C: How-To Guides (Second Preliminary Draft)”, 2022.12

[52] Nist Sp 1800-35d, “Implementing A Zero Trust Architecture - Volume D: Functional Demonstrations (Second Preliminary Draft)”, 2022.12

[53] Nist Sp 1800-35e, “Implementing A Zero Trust Architecture - Volume E: Risk And Compliance Management (Preliminary Draft)”, 2022.12

[54] Cisa, “Zero Trust Maturity Model Version 2.0”, 2023.04

[55] Nsa, “Advancing Zero Trust Maturity Throughout The User Pillar”, 2023.04

제로트러스트 가이드라인 1.0

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

한국제로트러스트포럼