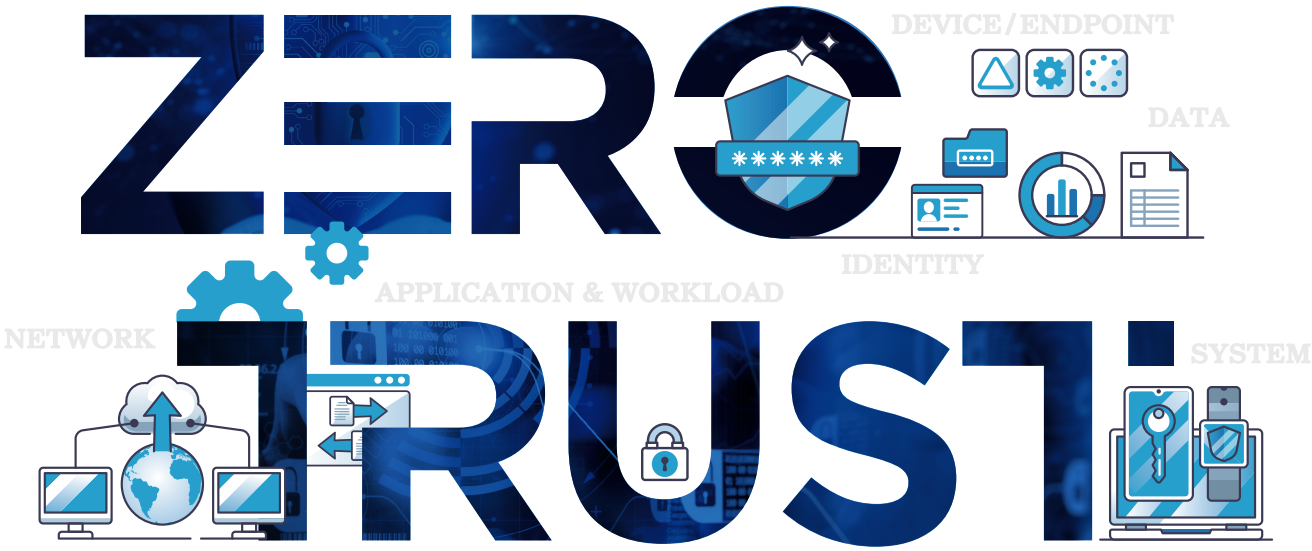
제로트러스트 가이드라인 2.0

2024. 12.



과학기술정보통신부
KISA 한국인터넷진흥원
한국제로트러스트포럼

제로트러스트 가이드라인 2.0

2024. 12.

과학기술정보통신부
KISA 한국인터넷진흥원
한국제로트러스트포럼

CONTENTS

제로트러스트 가이드라인 2.0

제1장

제로트러스트 가이드라인 2.0 개요

제2장

제로트러스트 보안 모델 및 도입 필요성

제3장

제로트러스트 성숙도 모델 및 세부역량

제4장

제로트러스트 도입 준비 방안

제5장

제로트러스트 도입 수준 분석

부록

| 제1절 | 가이드라인 2.0 발간 배경 ····· 8
| 제2절 | 가이드라인 2.0 목적 및 구성 ····· 14
| 제3절 | 가이드라인 2.0 주안점 ····· 17

| 제1절 | 제로트러스트 아키텍처 보안 모델 ····· 22
| 제2절 | 기업은 왜 제로트러스트를 도입해야 하는가? ····· 28

| 제1절 | 제로트러스트 성숙도 모델 2.0 ····· 35
| 제2절 | 제로트러스트 성숙도 모델 기반 보안 세부역량 ····· 51
| 제3절 | 제로트러스트 성숙도 모델 기반 구현 방안 ····· 90

| 제1절 | 제로트러스트 아키텍처 도입 고려사항 ····· 106
| 제2절 | 제로트러스트 아키텍처 도입을 위한 조직 내 역할 및 목표 설정 ····· 120
| 제3절 | 제로트러스트 아키텍처 구성 방안 ····· 128
| 제4절 | 제로트러스트 아키텍처 도입 준비 예시 ····· 139

| 제1절 | 제로트러스트 성숙도 기반 도입 수준 분석 ····· 150
| 제2절 | 제로트러스트 침투 시험 기반 효과성 분석 ····· 170

| 제1절 | 용어 및 약어 정의 ····· 184
| 제2절 | 국내 기업 제로트러스트 인식 수준 ····· 194
| 제3절 | 제로트러스트 아키텍처 참조 모델 실증 사례 ····· 202
| 제4절 | 미 연방정부 제로트러스트 도입·실증 현황 ····· 216
| 제5절 | 성숙도 모델 개념 ····· 229
| 제6절 | ISMS-P 인증기준과 제로트러스트 성숙도 모델 연계 ····· 234
| 제7절 | 참고 문헌 ····· 240

서문

최근 급변하는 디지털 전환기에서 AI의 진화, 클라우드 서비스 보편화 등 혁신적 기술들은 계속 등장하고 새로운 서비스와 가치를 창출하고 있습니다. 하지만, 악의적인 공격자들은 끊임없이 진화하여 다양한 신기술을 활용한 새로운 공격 방식을 통해 기업을 위협하고 있습니다. 사이버 위협은 기업의 지속 가능성을 위협하는 중대한 리스크이므로 기업은 사이버보안 강화를 경영 전략의 핵심 요소로 고려할 필요가 있으며 기업이 보유한 자산을 지키기 위해 방어 전략 및 체계 역시 진화가 시급한 상황입니다. 이러한 가운데 급부상하고 있는 제로트러스트는 기업의 사이버 위협 대응의 체질 개선을 위해 필수적으로 도입해야 하는 도전 과제라고 할 수 있습니다.

2023년 7월 과학기술정보통신부와 한국인터넷진흥원, 한국제로트러스트포럼의 공동 작업으로 '제로트러스트 가이드라인 1.0'을 발표했습니다. 가이드라인은 우리 기업들의 디지털 업무 환경 안전 체계를 제로트러스트로 이행하는 긴 여정의 첫 발걸음을 내딛는 과정이었습니다. 실제로 공공·민간의 많은 분야에서 가이드라인이 활용되었고 제로트러스트의 철학을 공유하고 기본적인 이해를 하는 데 도움이 됐다는 평이 주를 이루었습니다. 하지만, 한편으로 가이드라인이 제로트러스트 도입을 고려하는 기업의 입장에서 충분한 수준으로 작성을 한 것일까에 대한 걱정도 일부 있었습니다. 각 분야의 전문가들께서는 가이드라인에 대한 격려의 말씀과 함께 가감 없는 현실적인 조언을 전해주셨습니다. 이러한 다양한 의견은 제로트러스트 정책 방향성을 결정하는 데 많은 도움이 되었습니다.

제로트러스트 가이드라인 1.0이 나온 지도 벌써 1년 이상 지났습니다. 그 사이에 글로벌 제로트러스트 정책을 선도하는 미국은 많은 변화가 있었습니다. 연방정부의 각 기관은 대통령 안보 각서에 따라 OMB(관리예산실)에 제로트러스트의 도입과 요구 사항을 충실히 이행하였으며, 주정부와 지방 행정 기관도 제로트러스트의 도입을 추진하는 등 제로트러스트를 더 이상 이상적인 개념이 아닌 현실에서 구현하기 위한 실체적인 움직임을 보이고 있습니다.

우리나라는 2023년 과학기술정보통신부와 한국인터넷진흥원이 국내 제로트러스트 실증 사업을 성공적으로 진행한 바 있으며, 2024년 시범사업을 연이어 추진함으로써 다양한 도입 사례 확보를 통해 제로트러스트 보안 모델 확산을 위해 노력하고 있습니다. 또한 공공, 금융, 군 등에서도 공공 데이터 활용, 혁신적 AI·클라우드 서비스의 도입, 유연한 근무 방식, 개발 환경 개선 등을 위하여 획일적인 보안 체계와 규정을 보완 하는 등 우리 사회 각 분야의 제로트러스트 보안 체계 전환의 공감대는 증가하고 있습니다.

2024년 5월 과학기술정보통신부와 한국인터넷진흥원 및 한국제로트러스트포럼 정책·제도분과 소속 산학연관 전문가들은 연구반을 구성하여 보안 담당자들의 어려움을 조금이라도 해소할 수 있는 새로운 가이드라인 발간을 기획했습니다. 연구반에서는 지난 수개월 동안 회의와 토론, 수정을 거쳤으며 그 결과물로 제로트러스트 성숙도 모델을 세부 역량 수준으로 상세히 기술하고, 제로트러스트 도입 과정과 도입 수준 분석 방안을 구체화하는 형태의 가이드라인 2.0이 완성하게 되었습니다.

가이드라인 2.0은 제로트러스트의 철학이 기업의 문화에 뿌리를 내릴 수 있도록 최고경영자와 정보보호 최고책임자, 실무자들이 반드시 읽어야 할 항목들을 정의하였으며, 기업의 구성원들이 적극적으로 제로트러스트 이행 과정에서 각자의 역할을 수행할 수 있는 기반을 제공하고자 합니다. 국내 기업들이 전사적으로 제로트러스트를 도입함으로써 위험을 완화하고 보안 수준을 향상한다면, 각 산업 분야에서 더욱 경쟁력을 갖춘 강력한 기업으로 성장하는 밑거름이 될 수 있을 것으로 생각합니다. 앞으로 본 가이드라인 2.0이 기업의 제로트러스트 도입 과정에서 도움이 될 수 있기를 기대하며, 많은 의견과 관심을 부탁드립니다.

과학기술정보통신부 KISA 한국인터넷진흥원 한국제로트러스트포럼

제로트러스트
가이드라인 2.0

제 1 장

제로트러스트 가이드라인 2.0 개요

| 제1절 | 가이드라인 2.0 발간 배경
| 제2절 | 가이드라인 2.0 목적 및 구성
| 제3절 | 가이드라인 2.0 주안점

| 제1절 |

가이드라인 2.0 발간 배경

1. 제로트러스트 보안 체계 전환의 필요성

2010년 미국의 연구기관 포레스터 리서치(Forrester Research)의 수석 애널리스트 존 킨더백(John Kindervag)은 제로트러스트라는 기업망 보안에 대한 기존의 경계 보안 체계와는 차별화된 새로운 탈경계화 기반의 접근 방법론을 제시하였다.

기업[1]들이 그동안 기업망[2]에 구축해 왔던 네트워크 보안 모델은 업무 공간에서 발생할 수 있는 기업 자산 탈취, 파괴, 조작 등 외부의 물리적인 공격에 대응하기 위한 전략과 유사하다고 볼 수 있다. 일반적인 기업의 업무 공간은 외부와 물리적인 경계가 형성되어 있으며, 단일 혹은 다수의 출입문을 통해 내·외부자의 진입과 이동을 통제하고 있다. 그러나, 출입 통제 시스템만으로는 모든 종류의 침투에 대응하기 어려울 뿐 아니라, 정상적인 출입 통제 절차를 지키거나 우회하여 들어온 침입자가 업무 공간 내부의 기업 자산을 탈취, 파괴하는 모든 행위를 막을 수는 없을 것이다.

따라서, 이를 감시·대처하기 위하여 업무 공간의 각 경계 구간에 별도 출입 통제 장치를 둠으로써 공격자가 권한이 없는 공간에 접근할 수 없도록 조치하거나(Micro-Segmentation), CCTV를 설치하여 수상한 행위에 대해 감시하고(Visibility & Analytics), 중요 자산은 금고에 보관함으로써 추가적인 권한 혹은 인증 수단(Multi-Factor Authentication)을 가지고 있어야 접근할 수 있도록

---

1 본 가이드라인에서의 '기업'은 일반적인 사기업 및 민간 비영리 조직 등 국내 민간 분야의 중·대규모 조직을 통칭하여 표현한다. 본 가이드라인은 제로트러스트의 도입에 대한 정보를 제공하는 것이 목적으로, 정부 및 공공, 군 분야 혹은 민간 분야에 속하더라도 금융 혹은 주요정보통신기반시설 등 별도의 법령 및 규정을 준수해야 하는 기업·기관은 본 가이드라인을 단순 정보 습득을 위하여 활용할 수 있으나 각 분야별 별도의 제로트러스트 도입 지침 혹은 규정이 나올 경우 그 지침 및 규정을 준수하는 것이 우선임을 밝힌다.

2 본 가이드라인에서의 '기업망'은 'Enterprise Network'을 번역하여 사용하고 있는 단어로, 일반적으로 'Enterprise Network'는 중·대규모 조직에서 사용자와 기기, 애플리케이션 프로그램 간 연결을 제공하는 IT 인프라 및 네트워크 시스템을 의미한다. 제로트러스트 보안 철학이 적용되어야 할 중·대규모 조직은 기업뿐만 아니라 민간 비영리 조직 등 역시 해당된다. 따라서, 본 문서 내에서 기업망으로 표현되어 있다 하더라도 명시적으로 기업에서 운용하는 망을 의미하는 것이 아니라면, 기업뿐만 아니라 민간 영역에서의 비영리 기관 등에서 운용하는 네트워크 및 정보시스템을 모두 포괄하는 것으로 이해하는 것이 바람직하다.

조치하기도 한다. 이는 기업 업무 공간 역시 기업 외부와 마찬가지로 더 이상 신뢰할 수 있는 공간이 아니며, 내부에서도 공격자가 존재할 수 있다는 어쩌면 당연하다고 할 수 있는 기본적인 보안의 철학이 반영된 결과라고 할 수 있다.

하지만 물리적인 업무 공간과 다르게 네트워크 영역에서는 이러한 접근통제가 지켜지지 않는 경우가 많다. 경계 기반의 보안 체계를 운영하는 상당수 기업의 내부 인가된 사용자는 네트워크만 연결되어 있다면 폭넓은 권한을 통해 시스템 리소스에 언제든지 접근(Access)할 수 있는 것이 현실이다. 이것은 기업의 복잡한 업무 환경의 특성과 구성원의 업무 처리 절차의 신속성, 편의성 확보 등의 다양한 요인이 작용한다. 이러한 내부자 신뢰를 전제로 하는 접근통제 정책의 문제는 내부자의 계정 탈취 또는 내부자에 의한 악성 행위에 대한 안전장치가 없다는 것이다.

최근 다양한 디지털 신기술의 등장으로 사이버 공격의 형태가 고도화·은밀화되고 네트워크의 복잡성 및 관리 포인트가 급격히 증가하는 현 상황은 기업의 운영자와 보안 담당자에게 안전한 네트워크 운영을 위한 많은 고민과 숙제를 안겨 준다. 제로트러스트는 각 네트워크 경계에 있는 진입점을 드나드는 패킷을 감시함으로써 공격 여부를 판단하기보다 리소스 보호에 중점을 두고 사용자 및 접속 기기가 어떤 형태로든 적극적으로 통제하는 개념으로 그동안 보안 분야의 문제를 해결할 수 있는 새로운 방향성을 제시하고 있다. 따라서 근본적인 보안 체계의 체질 개선을 위해 제로트러스트 보안 체계 전환은 필연적이라고 할 수 있으며 이는 보안 산업 분야에서 새로운 기회의 장이 될 수 있을 것이다.

2. 제로트러스트 구현 노력

미국은 제로트러스트 도입에 가장 적극적이며 글로벌 정책을 주도하고 있다. 2014년 OPM(인사관리처)의 대규모 정보 유출 사고를 겪은 이후 미 하원은 약 2년간의 조사와 원인을 분석하였고 감독개혁위원회 보고서를 통해 연방정부의 보안 강화를 위한 제로트러스트 도입을 권고했으며 이후 NIST(국립표준기술연구소)는 2020년 SP 800-207 문서를 통해 제로트러스트 아키텍처를 최초로 정의했다. 2021년 바이든 행정부 출범 이후 고도화되는 사이버 위협은 기존 사이버 보안 체계로 대응할 수 없다는 판단하에 2021년 5월, '국가 사이버 보안 개선을 위한 행정 명령(Executive Order 14028 – Improving the Nation's Cybersecurity)'을 발표하면서 연방민간행정기관(FCEB) 전체의 제로트러스트 아키텍처의 도입을 명시하고 공식화하였다. 또한,

연방정부 차원에서 제로트러스트 구현을 현실화하기 위한 다양한 프로젝트를 진행해 오고 있다. NIST의 국가사이버보안센터(NCCoE)에서는 주요 보안 기업들과 함께 제로트러스트 아키텍처 구현 프로젝트를 통한 실증을 진행하고 그 결과로 2023년 7~9월 NIST SP 1800-35 시리즈 문서의 3rd Preliminary Draft를 발간하였으며 2024년 7월 시리즈 문서를 모두 통합한 4th Preliminary Draft를 발간하기도 하였다.

미 국방부(DoD)와 국가안보국(NSA)은 2022년 발표했던 제로트러스트 참조 아키텍처 2.0 및 제로트러스트 전략, 역량 실행 로드맵 이후 이를 뒷받침하는 제로트러스트 핵심 요소 7가지에 대한 성숙도 문서를 2023년 4월부터 2024년 7월까지 발간하였다. 또한 2024년 제로트러스트 오버레이 문서를 발간하여, 제로트러스트 핵심 요소, 제로트러스트 구현 활동과 NIST SP 800-53과의 관련성을 분석하였다. 이는 각 연방 기관들이 제로트러스트 아키텍처를 도입하는 데 있어 단순히 특정 기능만을 도입하라는 것이 아니라, 기관 성격에 맞는 다양한 가이드 문서들을 발간함으로써 각 기관이 자율적이면서도 정부의 일관된 원칙하에 제로트러스트 아키텍처를 구축하고 솔루션을 도입할 수 있는 체계를 구성함과 동시에 사례를 지속 확보·수집하고 있다.

각 연방 기관들은 관리예산실(OMB)이 제시한 일정에 따라 각 기관이 세운 2024년 9월까지의 계획하에 OMB 각서를 참고하여 제로트러스트 아키텍처를 도입해 왔으며, 최근 Mike Duffy 연방 CISO 대행은 최근 인터뷰에서 각 기관들의 제로트러스트 구현에 대해 엄청난 진전이 있었음을 공개했다. 미 국방부 역시 Thunderdome 프로젝트를 통하여 국방부 및 산하 기관 등과 SASE 중심의 제로트러스트 아키텍처를 도입하여 사용 중이다. 이처럼 미국은 연방정부에서 실질적으로 활용할 수 있는 많은 가이드 및 관련 문서 발간을 통해 각 기관이 제로트러스트를 도입하는 관점에서 폭 넓은 시야와 전략을 제공하고 있다.

표 1-1 제로트러스트 관련 미 연방정부 주요 정책 대응 현황

시기	기관	주요 문서 및 발간 자료
2023.07~09	NIST	'제로트러스트 아키텍처 구현 (SP 1800-35A~E, 3rd Preliminary Draft)' 발간
2023.09	NIST	'다중 클라우드 환경 상의 클라우드 네이티브 응용에서 접근제어를 위한 제로트러스트 아키텍처 모델 (SP 800-207A)' 발간
2023.10	DHS	'제로트러스트 구현 전략' 발간
2023.10	NSA	'기기 핵심 요소를 통한 제로트러스트 성숙도 개선' 발간
2024.02	DoD	'제로트러스트 오버레이 v1.0' 발간
2024.02	GSA	'제로트러스트 아키텍처 - 구매자 가이드 3.1' 발간
2024.03	NSA	'네트워크 및 환경 핵심 요소를 통한 제로트러스트 성숙도 개선' 발간
2024.04	GAO	'사이버 보안 - 주요 조치를 해결하기 위해서는 행정명령 요구사항 이행이 필수적' 발간
2024.04	NSA	'데이터 핵심 요소를 통한 제로트러스트 성숙도 개선' 발간
2024.05	NSA	'애플리케이션 및 워크로드 핵심 요소를 통한 제로트러스트 성숙도 개선' 발간
2024.05	NSA	'가시성 및 분석 핵심 요소를 통한 제로트러스트 성숙도 개선' 발간
2024.06	CISA 등	'네트워크 접근 보안에 대한 최신 접근방식' 발간
2024.06	DoD	'제로트러스트 오버레이 v1.1' 발간
2024.07	NIST	'제로트러스트 아키텍처 구현 (SP 1800-35, 4th Preliminary Draft)' 발간
2024.07	NSA	'자동화 및 통합 핵심 요소를 통한 제로트러스트 성숙도 개선' 발간
2024.08	GSA	'제로트러스트 전략 구매자 가이드 1.3 - DoD 제로트러스트 전략' 발간
2024.08	CISA	'연결된 커뮤니티 가이던스: 상호 연결된 시스템을 보호하기 위한 제로트러스트' 발간
2024.09	OMB	M-22-09 각서에서 요구한 연방 기관 제로트러스트 도입 일정 종료

제로트러스트 도입을 통한 보안 체계의 전환은 비단 미국 연방정부 시스템에만 국한되지 않는다. 물론 미국처럼 구체적으로 적용 단계는 아니지만 영국, 일본, 싱가포르, 캐나다, 중국 등 글로벌 각국 정부 역시 제로트러스트 보안 체계 전환의 필요성을 공감하고 가이드·전략 발표 등 다양한 정책적 움직임을 보이고 있다.

3. 가이드라인 2.0 추진 경과

2023년 7월 과학기술정보통신부와 한국인터넷진흥원, 한국제로트러스트포럼이 공동으로 '제로트러스트 가이드라인 1.0'(이하, 가이드라인 1.0)을 발간한 바 있다. 가이드라인 1.0은 제로트러스트 아키텍처의 도입을 검토하고 있는 기업들의 보안 전략 수립 책임자 및 실무자에게 제로트러스트의 기본 개념 및 원리, 보안 모델 등을 정의하고, 도입 절차와 구현 유스케이스를 상위 수준에서 기술함으로써 각 기업 환경에 적합한 도입 로드맵과 전략을 구성하는 데 도움을 주려는 목적으로 발간되었다.

가이드라인 집필진은 가이드라인 1.0 발간 이후 정부 부처, 관계 기관, 수많은 기업 담당자로부터 다양한 피드백을 받았다. 우리나라에서 실질적으로 처음 발행된 제로트러스트에 대한 가이드라인이다 보니 많은 분야에서 관심을 가지고 다양하게 인용됐으며 제로트러스트에 대한 이해를 한층 높일 수 있었고 조직 차원에서 제로트러스트 아키텍처를 도입해야 할 필요성에 대한 인식을 확산하고 공감하는데 좋은 기본서가 됐다는 긍정적인 평이 많았다.

하지만 가이드라인 1.0은 제로트러스트에 대한 개념을 정의하는 등의 상위 수준에서 기술할 수밖에 없는 태생적 한계가 있었다. 그 이유는 기업마다 망 구조와 보안 아키텍처의 구성이 전부 다르고 실증 결과를 반영할 수 없었기에 구체적인 도입 사례나 방법론을 담을 수 없었기 때문이다. 따라서 제로트러스트를 해당 기업망에 실제로 도입하기 위한 의사 결정이나 구체적 계획을 잡기 위해서 도입 과정을 구체화하는 형태로 문서 수준을 높이고 도입 관점의 전략을 세울 수 있도록 가이드라인의 구체화를 희망하는 요구가 꾸준히 있어 왔다.

제로트러스트는 '절대 신뢰하지 말고, 항상 검증하라(Never Trust, Always Verify)'는 새로운 보안 철학이자 개념으로, 도입 과정에서 제로트러스트의 원리를 최대한 준수하는 것이 핵심이다. 이 과정에서 특정 보안 기술이나 솔루션을 강제하지 않으며, 기업의 보안 담당자들은 기존 기업망 구조와 레거시 보안 방식, 보안 목표 등을 고려하여 도입 전략을 수립해야 한다. 하지만 아직까지는 실 환경에서 제로트러스트 아키텍처 도입·운용 사례가 거의 없어 도입에 대한 효과를 분석하기 어려운 상황이며, 보안 담당자들은 어떤 기술·솔루션을 선택하고 도입 계획을 수립해야 할지 어려움을 겪고 있다. 따라서, 본 문서의 집필진은 가이드라인 1.0의 부족한 점을 보완하고 수요기업 보안 담당자들의 어려움을 고려하여 제로트러스트 도입 과정을 보다 구체화하고 도입 수준을 분석할

수 있는 방안을 제시함으로써 각 기업들의 제로트러스트 아키텍처 도입을 가속화하는 데 도움을 주고자 가이드라인 2.0 발간을 계획하게 되었다.

본 가이드라인 2.0의 발간을 위하여 과학기술정보통신부와 한국인터넷진흥원 및 한국제로트러스트 포럼 정책·제도분과 소속 산학연관 전문가들을 중심으로 2024년 5월 제로트러스트 가이드라인 연구반을 구성하였다. 이후 연구반 위원들이 함께 가이드라인 2.0 구성 및 초안 작성을 진행했으며, 2024년 6월 첫 회의를 시작으로 약 5개월간 5차례 공식 회의, 별도 비공식 온라인 회의, 집필진 간 개별 토론 및 수정 작업 등 열띤 협의 과정을 거쳐 2024년 11월 최종적으로 본 가이드라인 2.0을 발간하게 되었다.

특히 집필진들이 모여 발간 계획을 논의하는 과정에서 제로트러스트 도입 과정을 구체화하고자 하는 작성 방향이 단순히 기존 가이드라인 1.0의 업데이트만으로 해결할 수 없다는 공통의 인식하에, 성숙도 모델의 구체화, 수요기업의 도입 준비 방안 제시, 도입 이후 효과성 분석 방안 제시 등 기존 가이드라인에 없던 새로운 내용을 반영하는 것에 초점을 맞추었다. 집필 초기부터 이러한 작성 방향이 수요기업에게 현실적으로 훨씬 도움이 될 것이라는 철학을 집필진들 사이에 공유하고 있었기 때문에, 가이드라인 1.0을 단순히 업데이트하는 것이 아닌 별도 문서 형태로 가이드라인 2.0을 작성하게 되었다.

정부는 향후 산업 도메인이나 시나리오별 참조 아키텍처, 제로트러스트 관점이 적용된 보안 통제 혹은 인증 기준 등 다양한 제로트러스트 가이드 문서를 추가 개발하는 것도 고려하고 있으며, 이에 관한 많은 의견과 제안이 있기를 기대한다.

| 제2절 |

가이드라인 2.0 목적 및 구성

앞서 언급한 바와 같이, 기업 소속의 보안 담당자들이 가이드라인 1.0을 참고하여 제로트러스트 아키텍처를 도입하는 과정에서의 어려움을 조금이라도 해소할 수 있도록, 제로트러스트 도입 시 반드시 고려해야 할 사항 및 도입 준비 방안, 그리고 도입 이후 제로트러스트 수준 분석 방안을 본 문서에서 제안하고자 한다.

기업들은 기업의 규모, 적용받는 관련 규정, 보안에 투자할 수 있는 비용, 현재 활용 중인 디지털 자산과 이용하는 서비스의 종류 등이 모두 다를 수 있다. 기존의 망 분리 조치를 계속 유지해야 하는가에 대한 고민, 클라우드 서비스의 활용 관점에서의 보안 전략 고민 등이 있을 수 있으며 랜섬웨어 등 이미 특정 공격에 피해를 입은 경험을 바탕으로 고도화된 위협에 대응할 수 있는 새로운 보안 구조를 만들고 싶을 수도 있을 것이다.

이러한 다양한 상황과 관점에 비추어, 제로트러스트 보안 구조를 상세히 규정하는 것은 적절하지 않으며 본 가이드라인의 목적과 맞지 않는다. 본 가이드라인 2.0의 목적은, 보안 담당자들의 제로트러스트 도입 전략 수립 과정에서 반드시 검토해야 할 사항을 강조함으로써 도입 전략 수립을 지원하고, 도입 후 보안 수준 및 효과성 분석 방안을 제안함으로써 보안 모델을 어떻게 지속적으로 개선해 나갈 수 있을지에 대한 방향성 설정에 도움을 주기 위함이다.

상기 목적을 위하여 본 문서는 다음과 같이 구성하였다.

먼저, 2장에서는 제로트러스트 아키텍처에 대해 간략히 소개하고자 한다. 즉, 제로트러스트 아키텍처 및 용어에 대한 정의, 보안 모델 및 기본 원리와 함께 기업이 제로트러스트 아키텍처를 도입해야 하는 이유를 다루었다.

3장은 제로트러스트 성숙도 모델 및 세부역량[3]을 다루고 있으며, 제로트러스트 도입을 위해 반드시 고려해야 할 성숙도 모델에 대해 그 의미와 역할 활용 방안에 대해 소개한 후, 구체적인 성숙도 모델을 제시한다. 가이드라인 1.0에서의 3단계 성숙도에서 '초기' 단계를 추가하고, 각 단계에서 요구하는 기능을 보완하였으며, 특히 이에 대한 기술 도입을 고려한 보안 세부역량까지 제시하였다. 이를 통해 각 기업들이 제로트러스트 아키텍처를 설계하려고 할 때 어떤 보안 역량이 필요한지를 참고할 수 있을 것으로 보인다.

4장은 제로트러스트 도입 준비 방안을 다룬다. 먼저 제로트러스트 아키텍처를 도입할 경우 반드시 고려해야 하는 여러 관점을 소개하고, 제로트러스트 도입을 위한 조직 구성 및 목표 설정, 기업의 제로트러스트 아키텍처 구성 방안(현재 기업망 분석과 제로트러스트 아키텍처 정의 등)을 다루었으며, 개발망에 대한 예시를 통하여 이해를 도울 수 있도록 하였다.

5장은 제로트러스트 도입 이후 효과성을 분석하는 데 도움을 줄 수 있는 내용을 포함한다. 즉, 제로트러스트 성숙도를 기반으로 자체 보안 수준을 평가함으로써 보안 성숙도 고도화에 참고할 수 있는 분석 방안을 제시하였으며, 제로트러스트 아키텍처 도입에 대한 침투 시험을 기반으로 효과성을 분석할 수 있는 방안도 함께 제시한다.

이 외에 부록에서는 가이드라인 2.0의 이해를 돕기 위하여, 보안 기술 및 솔루션 관련 용어 소개, 국내 기업의 제로트러스트 인식 수준, 2023년 과학기술정보통신부에서 수행한 제로트러스트 실증 사업을 통한 제로트러스트 아키텍처 참조 모델 사례 제시, 미 연방정부 제로트러스트 도입·실증 현황(NIST 제로트러스트 아키텍처 구현 프로젝트, 미 국방부 Thunderdome 프로젝트), 성숙도 모델에 대한 기초 개념, ISMS-P 인증기준과 제로트러스트 성숙도 모델 연계, 참고 문헌 등을 기술하였다.

〈표 1-2〉는 기업 구성원 역할에 따라 반드시 읽기를 권장하는 항목을 정리하였다.

---

3 부록 1절에서 세부역량을 '일련의 작업을 수행하기 위한 수단과 방법의 조합을 통해 원하는 요구사항 혹은 효과를 달성할 수 있는 능력 및 능력을 바탕으로 구현되는 구체적 기능'으로 정의내리고 있다. 세부역량에 대해서는 소프트웨어·하드웨어 구현까지 고려하여 구체적으로 정의를 내리는 것이 적절하며, 이렇게 구체적인 정의 과정을 통하여 CISA 등 기존 성숙도 모델의 기능이 추상적으로 정의가 되어있는 한계를 보완할 수 있다. 본 가이드라인 3장에서는 제로트러스트 기능 정의와 함께 도입·구현 과정에서 참고할 수 있도록 기능의 하위 개념으로 세부역량을 정의하였다.

표 1-2 기업 구성원별 필독 항목

기업 구성원	본 가이드라인의 필독 항목
최고경영자 (CEO)	▸ 제1장 제로트러스트 가이드라인 2.0 개요 ····· 8P ▸ 제2장 제2절 기업은 왜 제로트러스트를 도입해야 하는가? ····· 28P ▸ 제4장 제2절 제로트러스트 아키텍처 도입을 위한 조직 내 역할 및 목표 설정 ····· 120P
정보보호 최고책임자 (CISO)	▸ 제1장 제로트러스트 가이드라인 2.0 개요 ····· 8P ▸ 제2장 제로트러스트 보안 모델 및 도입 필요성 ····· 22P ▸ 제3장 제1절 제로트러스트 성숙도 모델 2.0 ····· 35P ▸ 제3장 제2절 제로트러스트 성숙도 모델 기반 보안 세부역량 ····· 51P ▸ 제4장 제1절 제로트러스트 도입 고려사항 ····· 106P ▸ 제4장 제2절 제로트러스트 아키텍처 도입을 위한 조직 내 역할 및 목표 설정 ····· 120P ▸ 제5장 제1절 제로트러스트 성숙도 기반 도입 수준 분석 ····· 150P
정보보호관리자 및 담당자	▸ 문서 전반에 걸친 이해 필요 ▸ 제3장 제로트러스트 성숙도 모델 및 세부역량 ····· 35P ▸ 제4장 제로트러스트 도입 준비 방안 ····· 106P ▸ 제5장 제로트러스트 도입 수준 분석 ····· 150P

| 제3절 |

가이드라인 2.0 주안점

본 가이드라인 2.0은 가이드라인 1.0과 비교하여 다음에 주안점을 두고 작성하였다.

첫째, 제로트러스트 성숙도 모델을 더욱 구체화하였다. 3장에서는 제로트러스트 보안 모델 도입의 수준을 판단할 수 있는 성숙도 모델을 세분화하여 한국형 성숙도 모델을 정립하고자 하였으며, 성숙도 모델에서 요구하는 보안 기능 및 세부역량 구체화를 통하여 제로트러스트 도입을 희망하는 기업의 실질적인 도입 전략 수립을 지원하고자 하였다. 성숙도 모델 2.0에서는 성숙도 수준 '초기' 단계를 추가하여 가이드라인 1.0의 성숙도 수준인 기존, 향상, 최적화 3단계에서 기존, 초기, 향상, 최적화의 4단계로 늘어나고, 각 단계별 특징을 보다 구체화된 형태로 포함하고 있다. 특히 3.2절에서는 6가지 핵심 요소 및 2가지 교차기능에 대한 52가지 보안 세부역량, 세부역량의 성숙도 수준별 특징을 정의하여 현재 기업망의 수준을 평가할 때 그리고 실제 제로트러스트 기술·솔루션을 도입하고자 할 때 고려해야 하는 기능을 최대한 다룰 수 있도록 하였다.

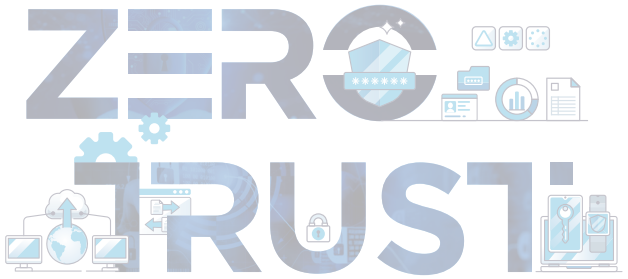
둘째, 제로트러스트 도입 절차를 구체화하였다. 4장에서는 먼저 제로트러스트 아키텍처의 도입 과정에서의 고려 사항을 정리함으로써 수요기업들이 제로트러스트에 대하여 정확한 개념을 인식할 수 있도록 돕고 있으며, 제로트러스트를 실제 도입할 기업이 제로트러스트 아키텍처를 도입하기 위한 조직 내 역할(기업 내 임직원 간 역할과 책임, 각 구성원의 역할) 및 목표 설정 방안을 제안하였다. 3절에서는 제로트러스트 아키텍처를 처음 도입하는 기업들이 준비 단계로 진입하기 전부터 준비 단계에 이르기까지 진행해야 하는 업무를 구체화하여 다루었으며, 4절에서는 도입을 준비하는 과정에서 어떤 일들을 하게 되는지 예시를 통해 기술하였다.

셋째, 제로트러스트 아키텍처를 도입한 기업이 자사 기업망에 도입한 제로트러스트의 수준 혹은 효과성을 분석할 수 있는 방안을 제시하였다. 5장에서 성숙도 기반의 체크리스트 수준 분석, 모의 침투시험 효과성 분석과의 연계 등을 통하여 제로트러스트 아키텍처의 도입 수준과 효과를

분석하는 방안을 제시함으로써, 보안 수준의 향상 정도를 도입 기업이 자체적으로 판단할 수 있도록 하였다.

표 1-3 본 문서와 가이드라인 1.0 비교

주요 내용	가이드라인 1.0	본 문서 작성·추가 사항
제로트러스트 성숙도 모델	‣ **3단계 성숙도 수준** 정의 ‣ **기업망 핵심 요소별 20가지 기능** 정의 (교차 기능 제외)	‣ '초기' 단계를 추가한 **4단계 성숙도 수준** 정의 ‣ **기업망 핵심 요소별 27가지 기능** 정의 (교차 기능 제외) 및 각 단계별 특징 구체화 ‣ 기업망 핵심 요소 및 2가지 교차 기능에 대한 **52가지 보안 세부역량 및 각 세부역량의 성숙도 수준별 특징** 정의 ‣ 성숙도 모델에 기반한 구현 방안 제시
제로트러스트 도입 절차	‣ 제로트러스트 아키텍처 **도입 고려사항 정리** (성숙도 모델 관점 및 기업 내외부 환경 관점) ‣ 총 **5단계의 제로트러스트 아키텍처 도입 단계 제시** (준비 → 계획 → 구현 → 운영 → 피드백 및 개선) ‣ OMB 각서를 참고하여 제로트러스트 구현에 따르는 **핵심 요소별 초기 전략 제시**	‣ 제로트러스트 아키텍처 **도입 과정에서의 고려사항 구체화** (제로트러스트에 대한 명확한 이해 및 기업 내 인식 제고 등 추가) ‣ **제로트러스트 도입 준비 단계 구체화** (업무 구체적 기술 및 예시 제시) ‣ 제로트러스트 아키텍처 도입을 위한 **조직 내 역할 및 목표 설정 방안** 제시
기타	‣ **제로트러스트 구현에 관한 6가지 유스케이스** 및 목표·요구사항, 구현 방안 등 제시 ‣ 제로트러스트 도입 후 **보안 수준 평가 방안 없음**	‣ 제로트러스트 **도입 후 기업망 보안 수준을 평가할 수 있는 2가지 방안** 제시 (성숙도 기반 도입 수준 분석을 위한 체크리스트, 침투시험 기반 제로트러스트 효과성 분석 방안) ‣ 부록에서 2023년도 **제로트러스트 실증 사례 소개**


ZERO
TRUST

제로트러스트
가이드라인 2.0

제2장

제로트러스트 보안 모델 및 도입 필요성

| 제1절 | 제로트러스트 아키텍처 보안 모델

| 제2절 | 기업은 왜 제로트러스트를 도입해야 하는가?

| 제1절 |

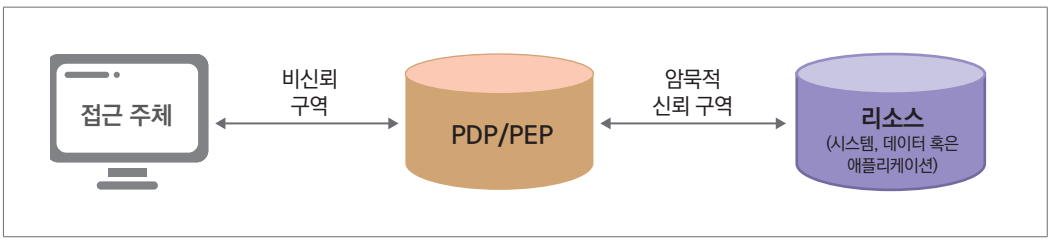
제로트러스트 아키텍처 보안 모델

1. 제로트러스트 개념 모델

제로트러스트의 개념은 기존의 경계 기반 보안과 달리, 접근 주체에 대하여 네트워크 혹은 물리적 위치만으로 신뢰를 부여하지 않는 것으로부터 출발한다. 기업망의 보안 담당자는 접근 주체의 리소스 접근 과정에서 개별적인 제어를 통해 접근 승인 여부를 결정할 수 있어야 한다. 이 과정에서, 최종적인 접근 결정 및 시행에 대한 역할은 정책결정지점(PDP) 및 정책시행지점(PEP)이 맡게 된다.

NIST SP 800-207에서는 제로트러스트 관점에서의 접근에 대해 [그림 2-1]과 같은 개념 모델을 제시한 바 있다. 이 개념 모델은 과거 다양한 형태의 접근제어 모델과 논리적 구조 측면에서 크게 다르지 않지만, 가장 큰 차이점은 접근 주체의 접근 시도 과정에서 인증 등 신뢰도 평가가 이루어지기 전에는 비신뢰를 가정한다는 것에 있다. 기업망 차원에서, 보안 책임자는 접근 주체가 인증되었으며 현재의 접근 요청이 유효함을 보증할 수 있는 경우 해당 주체가 리소스에 접근할 수 있도록 승인[4]하여야 한다.

그림 2-1 제로트러스트 접근의 개념 모델



4 마치 공항에서 승객이 탑승 게이트에 접근하기 위하여 정당한 신분증과 탑승권을 소지하고 있는 상태에서 보안 검색대에서 이를 확인한 후 탑승 구역으로 보내는 것과 유사한 개념으로 볼 수 있으며, 접근 요청에 대해 승인받은 접근 주체는 해당 리소스에 대한 암묵적 신뢰 구역(탑승 구역)에 진입(접근)한 것으로 생각할 수 있다.

2. 제로트러스트 아키텍처 기본 원리

제로트러스트 아키텍처를 구성하기에 앞서 중요하게 고려해야 하는 것은, 기업이 제로트러스트 도입을 통해 달성하고자 하는 최종적인 목표가 기업망 및 내부 리소스에 대한 보호임을 잊지 말아야 한다는 것이다. 물론 기존 경계기반의 레거시 보안 아키텍처를 통해서도 외부의 대응은 어느 정도 가능하다. 하지만 제로트러스트가 등장하게 된 이유는 더 이상 경계 기반 보안이 적합하지 않다는 문제 인식에서 시작됐다.

그동안 경계 기반 보안은 네트워크 상의 경계에서 외부로부터의 공격에 대응하는 다양한 방법을 고려해왔으나, 재택·원격 근무의 확대, 클라우드 기술의 등장 등으로 접근 주체와 리소스의 네트워크 상의 위치가 다양해지고 경계가 불분명해짐에 따라 기존 보안 방식만으로는 모든 위협에 대응하기 쉽지 않게 되었다. 또한, 공격자가 내부 침투에 성공하는 경우 경계에서의 보안 대책은 더 이상 공격에 대한 대응책이 될 수 없다는 단점이 존재한다.

따라서, 제로트러스트 아키텍처의 기본 원리는 기업망에 구성하려는 보안 아키텍처를 통해 기업망 및 내부 리소스의 안전한 보호라는 제로트러스트의 목표를 달성하기 위한 방법적 관점에서 기술되어야 한다. 이러한 기준 하에, 가이드라인 1.0에서는 제로트러스트 아키텍처의 기본 원리를 〈표 2-1〉과 같이 정리한 바 있다.

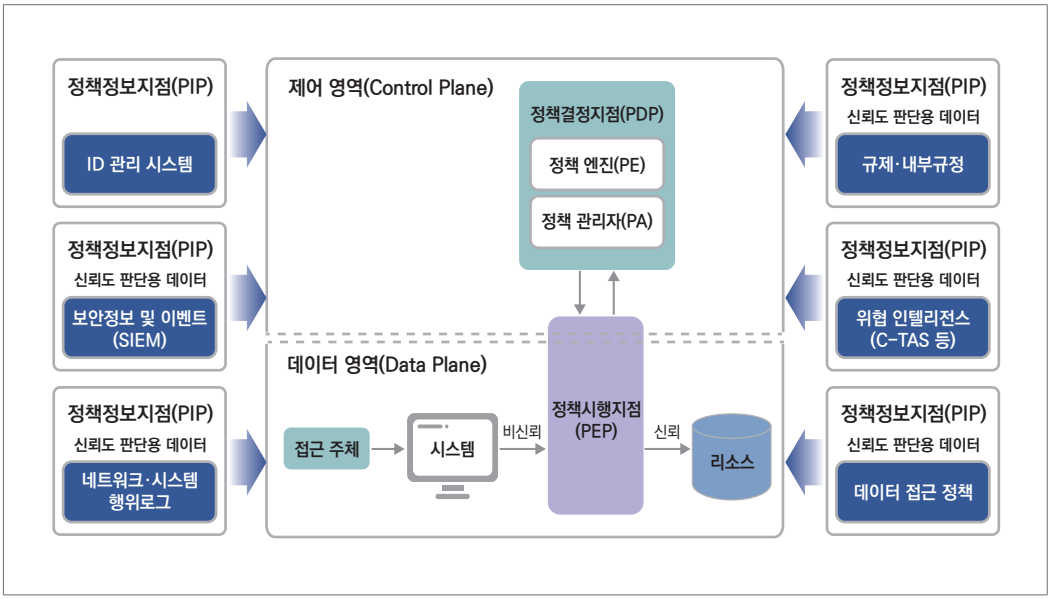
표 2-1 제로트러스트 아키텍처 기본 원리

가. 기본 원칙: 모든 종류의 접근에 대해 신뢰하지 않을 것 (명시적인 신뢰 확인 후 리소스 접근 허용)
- 접근: 기업망에 존재하는 가치 있는 리소스에 대한 모든 접근 시도를 의미 - 모든 종류의 접근에 대해 기본적으로 접근을 거부함을 의미 - 일정 수준의 인증 과정을 거친 접근 주체에게만 최소한의 리소스 접근 허용 - 성공적인 인증 후에도, 지속적인 모니터링을 통하여 신뢰성에 의심이 가는 상황이 발생하는 경우 강화된 추가 인증을 받거나 현재의 접근 세션에 대한 강제 종료 필요
나. 일관되고 중앙집중적인 정책 관리 및 접근제어 결정, 실행 필요
- 접근 정책을 관리하는 지점(주로 PDP)이 분산되어 있는 경우의 문제: 일관된 정책 수립이 어렵고, 새로운 접근 주체 및 리소스 추가 시 일관된 정책 적용이 어려움 - 정책을 실행하는 지점(PDP 및 PEP 혹은 일부 기능)은 분산되어 있을 수 있으나, 가급적이면 중앙집중적인 정책 관리에 의한 접근 여부 결정이 필요 예) 특정 직원 퇴사 시, 해당 직원 ID를 통한 내부 리소스 접근이 불가능하도록 반영되어야 함
다. 사용자, 기기에 대한 관리 및 강력한 인증
- 내부 사용자 및 기기에 대한 목록화를 기반으로, 강력한 사용자 인증 및 기기 상태 관리 필요 - 등록된 기기가 아니면 기업망 혹은 특정 리소스 접근을 원천 봉쇄하거나 접근 가능 리소스를 정확히 분류하고 중요 리소스에 대한 접근이 불가능하도록 정책 결정 필요 - 등록되지 않은 기기 혹은 보안 상태가 명확히 확인되지 않은 경우 추가 인증 요구도 가능
라. 리소스 분류 및 관리를 통한 세밀한 접근제어 (최소 권한 부여)
- 접근 주체 및 리소스의 종류 및 다양한 요인에 따르는 세밀한 접근제어 필수 - 공격자가 기업망 내부 특정 기기 혹은 시스템 침투에 성공했더라도 횡적 이동을 통한 추가 피해를 최소화할 수 있도록, 사용자 및 기기에 필요한 최소한의 권한 부여
마. 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
- 세밀한 접근제어는 필연적으로 리소스 간 경계를 요구할 수 있으나, 정책을 실시간으로 반영하고 세분화하기 위해서는 논리적으로 경계를 설정할 수 있는 방안 필요 - 또한, 리소스별로 긴 시간의 접속을 허용하지 않고 세션 단위 접근만을 허용 필요 - 논리적 경계뿐만 아니라 통신상에서 데이터의 기밀성 및 무결성을 보호할 수 있는 기술 필요
바. 모든 상태에 대한 모니터링, 로그 및 이를 통한 신뢰성 지속적 검증, 제어
- 모든 상태: 신뢰도 평가에 관련 있는, 접근 주체, 리소스, 기업망 등의 모든 관련 정보를 의미 - 상태 정보는 기업망에서 반드시 모니터링되어 현재의 상태를 수치적으로 시각화하여 파악할 수 있어야 하며, 상세한 분석을 통한 신뢰도 평가 및 감사가 가능해야 함

3. 제로트러스트 아키텍처 보안 모델

앞서 언급한 제로트러스트의 개념 모델 및 아키텍처 기본 원리를 고려하면, 제로트러스트 아키텍처는 접근 주체의 리소스에 대한 접근을 신중하게 다루어야 한다. 가이드라인 1.0에서는 기업망이 제로트러스트 아키텍처를 실현하기 위하여 접근 주체가 리소스에 접근하는 것에 대한 허용·거부 정책을 다루어야 하며 가장 중요한 핵심 기능은 접근제어 정책임을 언급한 후 제로트러스트 아키텍처 보안 모델 및 논리 구성 요소를 표현한 바 있다. 본 문서에서의 정책정보지점(PIP)[5]은 가이드라인 1.0의 보안 모델에서 정책결정지점으로 입력되는 신뢰도 판단용 데이터를 제공하는 역할을 담당하고 있다. 이를 반영한 결과는 [그림 2-2]와 같다.

그림 2-2 제로트러스트 아키텍처 보안 모델 및 논리 구성 요소



제로트러스트 아키텍처 보안 모델을 구성하는 논리 구성 요소인 정책결정지점 (정책 엔진 및 정책 관리자), 정책시행지점, 정책정보지점의 기능과 역할에 대해서는 다음 페이지를 참고할 수 있으며, 〈표 2-2〉에서 요약하여 설명하고 있다.

5 가이드라인 1.0 2.1.2절의 라. 항목에서는 해당 논리 구성 요소를 접근 결정을 위해 사용하는 데이터 입력 요소로 표현하고 있으나 본 문서에서는 정책정보지점이라고 정의한다.

참고 제로트러스트 아키텍처 보안 모델의 논리 구성 요소

정책 엔진 (PE)

정책 엔진은 접근 주체가 리소스에 접근할 수 있을지를 최종적으로 결정한다. 정책 엔진은 신뢰도 평가 알고리즘에 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.

정책 관리자 (PA)

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.

정책시행지점 (PEP)

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.

정책정보지점 (PIP)

PIP는 제로트러스트 아키텍처를 실행하는 기업이 접근 결정을 위해 정책 엔진의 입력 혹은 정책 규칙으로 활용할 수 있는 정보를 생성·전달하는 논리 구성 요소로, 기업 내부에서 운영하는 시스템과, 기업이 운영하거나 제어하지 않는 외부 시스템 모두 가능하다. 다음과 같은 시스템 등이 포함될 수 있으나, 이 외에도 신뢰도 판단에 도움이 될 수 있는 정보를 생성하는 시스템이라면 모두 정책정보지점으로 볼 수 있다.

- 규제·내부 규정(Industry Compliance)
- 데이터 접근 정책(Data Access Policies)
- 보안 정보 및 이벤트(SIEM) 시스템
- 위협 인텔리전스(Threat Intelligence)
- ID 관리 시스템(ID Management System)
- 네트워크·시스템 행위 로그(Network and System Activity Logs)

PIP가 제공할 수 있는 신뢰도 판단용 데이터의 예시로 6가지(규제·내부 규정, 데이터 접근 정책, 보안 정보 및 이벤트, 위협 인텔리전스, ID 관리 시스템, 네트워크·시스템 행위 로그 등)를 소개하고 있으나 신뢰도 판단용 데이터를 제공하는 PIP는 이 외에도 다양하게 존재할 수 있으며, 반드시 기업망 내에서 존재하지 않을 수도 있다. 신뢰도 판단에 도움이 될 수 있는 성격의 데이터로 기업망에서 수집해서 사용할 수 있다면 종류와 관계없이 신뢰도 판단용 데이터로 활용할 수 있으며, 그 정보를 PDP에 제공하는 논리 개체는 그 위치 및 정보의 종류와 관계없이 모두 PIP로 본다.

표 2-2 제로트러스트 아키텍처 논리 구성 요소

구분	구성 요소		역할
핵심 구성 요소	정책 결정 지점	정책 엔진	‣ 다양한 입력 요소를 검토하여 접근 주체의 리소스에 대한 접근 허용 여부를 최종 결정 ‣ 신뢰도 평가 알고리즘을 활용하며, 이 알고리즘에 대한 입력으로 기업망에 대한 정책 및 그 외 다른 정보를 활용
		정책 관리자	‣ 주체와 리소스 간 통신 경로 설정 및 종료 관리 ※ 세션 별 인증·인가 토큰 또는 크리덴셜 생성 ‣ 정책시행지점에게 명령하여 접근 주체와 리소스 사이의 통신 경로를 생성하거나 폐쇄 ‣ 세션을 최종적으로 허락하거나 거부하는 결정을 정책 엔진에 의존
	정책시행지점		‣ 주체에 할당된 정책 실행, 연결 활성화, 모니터링, 종료 ‣ 정책 관리자와 통신하며, 접근 요청을 포워딩하고 업데이트된 정책을 수신
신뢰도 판단용 데이터 제공자 (접근 결정에 활용)	정책 정보 지점	규제·내부 규정	‣ 법적 규제 정보 및 이를 위한 기업 내부 규정을 준수하는지 확인 ‣ 기업이 규제 준수를 위해 개발한 모든 정책 규칙 포함
		데이터 접근 정책	‣ 기업 리소스 접근에 대한 속성, 규칙, 정책 등
		보안 정보 및 이벤트	‣ 차후 분석용 보안 정보 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)

| 제2절 |

기업은 왜 제로트러스트를 도입해야 하는가?

기업에서 제로트러스트 도입을 시도하는 것은 필연적으로 시간과 인적 자원, 비용을 수반한다. CEO는 보안 기술의 세부 사항 외에 경영 관점에서 도입 효과와 가치를 고려할 수 있으므로, 기존 보안 아키텍처를 제로트러스트 아키텍처로 전환하는 이유에 대한 명확한 이해와 근거가 필요할 수 있다. 따라서, CISO 혹은 보안담당자(이하, CISO)는 제로트러스트와 비즈니스 목표의 관계, 비용 절감 효과, 위험 관리 등을 중점적으로 소개함으로써 제로트러스트 도입시 기업 전체에 미치는 긍정적인 영향을 설명하는 것이 바람직하다.

1. 제로트러스트와 비즈니스 목표의 관계

기업이 새로운 비즈니스 모델을 지속적으로 발굴하는 것은 기업의 생존과 직결되는 문제로 볼 수 있다. 만약 기업 내·외 규정과 요구사항을 준수하고 보안 위협에 대응하기 위하여 기존에 구축한 보안 아키텍처가 비즈니스 목표를 설정하고 새로운 비즈니스 모델을 발굴하는 데 장애가 된다면, 이를 극복할 수 있는 방안이 필요하다.

예를 들어, 어떤 기업에서 기업망 보안을 위한 조치로, 해외에서는 등록된 IP 외에 기업망 내부에 접근할 수 없도록 조치하였다면, 해외 지사가 이전·확장한 경우 혹은 해외 협력 기업에 파견된 직원이 기업망 내부 리소스에 접근하는데 있어 상당한 어려움이 있을 것이다. 그 외에도 접근권한을 세밀하게 적용하지 못하는 보안 아키텍처로 인하여 혁신적인 외부 서비스(SaaS, AI 등)를 내부 업무 환경에 적용하지 못하는 사례가 있을 수 있다.

이러한 경우, 보안성은 기존 보안 환경보다 높은 수준을 달성하면서도 새로운 서비스 개발에 유연한 제로트러스트 아키텍처를 설계·도입함으로써 해당 문제를 해결할 수 있을 것이다. 또한,

지속적으로 바뀌는 IT 환경, 즉 원격·재택 근무의 증가, 클라우드로의 전환, 협력사와의 협업 환경 변화, 비인간개체의 증가 등의 상황에서 제로트러스트는 안전한 환경을 제공하면서도 비즈니스 연속성을 보장할 수 있다는 점을 강조할 수 있다.

2. 비용 절감 효과 및 ROI(투자 대비 수익)

기업망에 제로트러스트 아키텍처를 도입하는 경우 초기 도입에 일정한 투자가 필요하며 지속적으로 투자 및 관리 비용을 요구하게 된다. 따라서, 초기 도입 과정에서 요구하는 투자에 대한 효과가 충분한지를 분석하는 것이 바람직할 것이다.

아직은 제로트러스트 아키텍처를 본격적으로 도입 중인 기업이 많다고 보기는 어려우나, 앞서 언급한 바와 같이 레거시 보안 기술과 제로트러스트 보안 기술은 명확한 구분되는 것이 아니기 때문에 이미 제로트러스트의 초보적인 철학이 담겨 있을 수 있다. 이 경우 이미 제로트러스트 성숙도는 다소 낮지만 제로트러스트의 도입이 일부 이루진 것으로 볼 수 있으며, 기업의 중요한 디지털 자산을 보호하고 위험을 완화함으로써 장기적으로 보안 사건 대응 비용, 데이터 유출 방지 비용 등을 절감할 수 있으며 제로트러스트가 사이버 공격에 대한 방어 능력을 향상시킴으로써, 비즈니스 운영의 연속성을 보장할 수 있다.

또한 장기적으로 보면 보안 아키텍처를 운용하는 관점에서 기존보다 효율적인 자원 활용이 가능하다. 제로트러스트를 통해 세분화된 보안 정책과 자동화된 인증 프로세스를 도입하면, 인적 자원과 보안 관리 비용을 줄일 수 있으며 새로운 접근 주체와 리소스가 지속적으로 업데이트되더라도 자동화된 접근제어 정책을 부여함으로써 IT와 보안 인프라에서 불필요한 복잡성을 줄이고 효율성을 증대시킬 수 있다.

3. 현재 보안 환경의 취약점 및 한계 개선을 통한 위험 관리

미 연방정부의 모든 기관들이 제로트러스트 아텍처를 도입할 경우 그 과정에서 대규모 예산이 소요될 것으로 예상됨에도 불구하고 추진한 것은 연방 기관들이 갖추고 있었던 기존 보안 환경의 취약점과 한계를 인식했기 때문이다. 2014년부터 2015년까지 약 1년여에 걸쳐 이루어진 연방 인사관리처의 개인정보 유출 사고가 대표적으로, 인사관리처에 접속할 수 있었던 협력 업체의 자격

증명 권한이 해커들에게 유출 당한 것으로 공격자의 내부망 접속에 대한 감시가 잘 이루어지지 않음을 이용한 공격 사례이다. 그뿐만 아니라 미 연방정부는 2020년 벌어진 솔라윈즈 공급망 공격 사례를 통하여, 서드파티 및 협력사가 공급한 소프트웨어를 통해 내부 시스템이 공격당할 수 있으므로 이를 일방적으로 신뢰하지 말고 지속적인 검증을 통하여 탐지·대응 능력을 강화하는 형태의 정교한 보안 체계가 필요함을 깨달았다.

전통적인 경계 기반 보안 모델이 내부자 위협에 취약한 반면, 이러한 공격을 완화하기 위해 등장한 제로트러스트 아키텍처는 정상 사용자의 자격 증명 권한이 유출되었다 하더라도 현재 접근에 대한 컨텍스트(접속 IP 주소, 접속 시간, 요청 리소스 정보 등)를 분석하여 동적으로 접근 허용 여부를 판단하고 비정상적 접근을 차단함으로써 개인정보의 불법 유출을 피할 수 있었을 것이다. 이러한 방식으로 제로트러스트가 기존의 보안 체계의 한계를 보완하는 데 중요한 역할을 함으로써 위험을 줄일 수 있음을 고려하면 기업이 제로트러스트 아키텍처를 도입할 충분한 가치가 있다고 판단할 수 있다.

이처럼 경계 기반 보안 환경에서 지속 발생하는 보안 사고를 사례로 들면 기업에게 제로트러스트가 왜 필요한지 그리고 제로트러스트 아키텍처 도입을 통하여 해당 보안 사고에 어떻게 대응할 수 있을지를 구체적인 데이터와 경험을 기반으로 소개할 수 있다.

예를 들어, 미국에서 벌어진 체인지 헬스케어에 대한 랜섬웨어 공격은 의료 관련 기업의 사이버 보안 공격 대응 능력에 관하여 참고할 수 있는 좋은 사례가 될 수 있다. 모회사인 UHG의 사태 수습 및 매출 손실로 인한 비용이 10억 달러로 추정될 뿐만 아니라 소규모 의료 서비스 제공업체 및 약국 중 일부는 파산에 가까운 상황까지 이르게 한 이 공격 사례에서, (불법적으로 설치된) 특정 애플리케이션이 민감한 의료 데이터를 대량으로 읽거나 수정하는 경우에 대해 제로트러스트 아키텍처를 바탕으로 최소 권한 부여, 평소와 다른 패턴의 데이터 접근·수정 시 접근 차단, 추가 인증 요구 및 관리자 보고 등이 이루어졌다면 공격을 차단하거나 피해를 최소화하는 것이 가능했을 것으로 보인다. 이러한 사례는 의료 기업들에게 제로트러스트 아키텍처의 도입 필요성을 충분히 인식시켜줄 수 있을 것이다.

특히 제로트러스트를 도입한 기업이 사이버 공격을 성공적으로 방어한 사례가 있다면, 이러한 사례 소개를 통하여 앞으로 지속적으로 발생할 수 있는 고도화된 공격에 대한 위험을 낮추는 효과가

있음을 설득력 있게 강조할 수 있다.

4. IT 환경 변화에 대한 적응력

제로트러스트는 단순히 보안을 강화하는 것에만 초점을 맞추기보다는, 기업이 더 빠르고 민첩하게 변화할 수 있는 환경을 만들어줄 수 있다. 예를 들어, 새로운 기술 도입을 도입하는 과정에서 위험을 최소화하면서도 비즈니스 확장에 대한 유연성을 제공하는 것이 가능하다. 예를 들어, 암호화 관련하여 암호 민첩성을 강조하는 것도 하나의 예로 볼 수 있다.

제로트러스트는 기업이 법적 규제나 규정 준수와 관련한 요구사항을 충족하는 데 도움을 줄 수 있는데, 이는 제로트러스트에서 세밀한 접근제어와 지속적 모니터링을 강조하고 있기 때문으로 볼 수 있다. 제로트러스트 아키텍처가 도입되면 누가 언제 어떤 자원에 접근했는지를 명확히 기록하고 추적할 수 있으며, 이는 많은 법적 규제 및 보안 통제에서의 요구 사항을 준수하는 데 유리할 뿐만 아니라, 규정 준수 및 감사 지원을 위한 데이터 접근 기록을 유지하고 로그 등 필요한 데이터를 빠르게 제공할 수 있는 능력을 가진다. 이러한 제로트러스트 아키텍처의 특징은 개인정보보호와 데이터 보안 규제들이 강화되고 있는 상황에서 필요한 기능을 강력하게 지원함으로써 규제에 대한 적응력과 함께 기업의 신뢰성을 높일 수 있다.

5. 기업 이미지 개선

기업은 제로트러스트 아키텍처를 도입함으로써 사이버 공격으로부터 중요한 고객 정보 및 기업의 디지털 자산을 강력하게 보호할 수 있을 뿐만 아니라, 이를 통하여 고객 신뢰를 강화하고 브랜드 이미지를 개선할 수 있다는 장점이 있다. 즉, 안전한 환경에서 비즈니스를 운영하면 사이버 위협으로부터 발생할 수 있는 위험을 완화함으로써 사업 안정성 측면에서 경쟁 우위를 확보할 수 있다. 그 뿐만 아니라 제로트러스트는 디지털 혁신을 지원하는 핵심 보안 인프라로, 클라우드 전환, 원격 근무 지원, 빠른 기술 도입 등을 가능하게 함으로써, 기업이 디지털 전환 목표를 수립했거나 추진 중인 경우, 이 목표를 더욱 안전하고 빠르게 달성할 수 있는 역할을 담당할 것이다.

제로트러스트
가이드라인 2.0

제3장

제로트러스트 성숙도 모델 및 세부역량

| 제1절 | 제로트러스트 성숙도 모델 2.0

| 제2절 | 제로트러스트 성숙도 모델 기반 보안 세부역량

| 제3절 | 제로트러스트 성숙도 모델 기반 구현 방안

3장에서는 제로트러스트 성숙도 모델 및 세부역량에 대해서 기술한다. 제로트러스트 성숙도모델은 기업이 자사 기업망의 제로트러스트 수준을 평가하고 더 높은 성숙도를 갖는 제로트러스트 아키텍처로 진화하는데 참조할 수 있는 기준으로서 그 가치가 있다. 또한 제로트러스트 기능과 세부역량을 정의함으로써 각 기업들이 제로트러스트 아키텍처를 구현하는 데 있어 어떤 보안 기능들이 필요한지 분석할 때 참고할 수 있는 수단을 제공하고자 한다.

이를 위해, 1절에서는 제로트러스트 성숙도 모델의 의미와 역할, 제로트러스트 도입 절차의 세부 단계별 성숙도 모델 활용 방안, 기업망 핵심 요소 등을 소개하였으며, 가이드라인 1.0에서 정의한 성숙도 모델 이후 발간된 제로트러스트 성숙도 모델 관련 문서 및 여러 전문가 의견을 참조하여, '초기' 단계의 성숙도 수준을 추가하고 각 단계별 제로트러스트 기능을 구체화한 제로트러스트 성숙도 모델 2.0을 제안한다.

2절은 앞서 정의한 제로트러스트 성숙도 모델 2.0 및 보안 기능의 모호성과 추상성을 극복하고 구현까지 고려하여 구체적인 정의를 포함하는 제로트러스트 세부역량 및 각 성숙도 수준을 담았다. 여기에서 정의한 제로트러스트 역량은 성숙도 모델을 더욱 구체화함으로써, 기업 내 정보보호 담당자들이 제로트러스트 원칙을 더욱 정확하게 이해하고, 이를 성공적으로 구현하는 데 큰 도움이 될 것이다.

마지막으로 3절에서는 제로트러스트를 기업망에 적용하는 관점에서 세부역량과 성숙도를 바탕으로 기업망에 제로트러스트를 적용·구현하는 방법에 대해 기술하고 있다. 제로트러스트 철학을 구현하는 방법은 한 가지로 규정할 수 없는 만큼 이 방법이 절대적일 수는 없으며 각 기업은 상황에 따라 다르게 설정하겠지만, 성숙도 모델을 구현 과정에 활용하는 방안으로서 참고할 수 있다.

| 제1절 |

제로트러스트 성숙도 모델 2.0

성숙도 모델은 일반적으로 특정 프로세스·기술에 대한 조직의 수준 분석 및 측정을 위한 도구로서 지금과 유사한 형태의 성숙도 모델은 1979년 소개되었다. 현재 성숙도 모델은 소프트웨어 엔지니어링, 보안 등 다양한 분야에서 활용되고 있으며 조직의 현재 역량 및 기술 수준을 평가하고 더 성숙도가 높은 조직으로 진화하는데 참조할 수 있는 기준을 제시한다. 하지만 아무래도 성숙도라는 단어가 일상적으로 사용하지 않는 용어다 보니 다소 낯설게 느껴질 수 있다.

제로트러스트 분야의 성숙도 모델은 미국의 CISA를 비롯하여 다양한 기업에서 제로트러스트 제시한 바 있으며 성숙도 모델에 대한 개념과 보안 성숙도 모델에 대해서 더 상세히 알고 싶은 독자를 위하여 부록의 5절에서 성숙도 모델의 개념을 상세하게 소개하고 있으니 참고 바란다.

본 절에서는 제로트러스트 성숙도 2.0 모델을 정의하기에 앞서, 성숙도 모델의 의미와 역할, 그리고 도입 과정에서 제로트러스트 성숙도 모델을 활용하는 방안을 소개하고자 한다.

1. 제로트러스트 성숙도 모델의 의미와 역할

기업이 보안 아키텍처를 구성하는 궁극적인 목적은 내부 디지털 자산에 대한 공격 가능성 및 위험을 완화·관리함으로써 조직의 자산을 보호하고자 하는 것이다. 문제는 해당 조직의 보안 수준을 어떻게 평가할 수 있는가이며, 특히 보안 아키텍처를 구축하는 데 있어 비용을 투자하였거나 투자할 예정인 기업 내 경영진(예, 최고 경영자, 재무 담당자 등)은 조직 내 기업망에 대한 현재 혹은 향후 보안 수준을 정량적으로 평가하고 싶을 것이다.

제로트러스트 아키텍처를 도입하여 구현하고자 하는 기업에서는 다양한 조직의 요구 사항과 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 보안 담당자들에게 제로트러스트에 대한 구체적인 이해와 도입 계획을 수립하는 데 있어 어려움을 줄 것이다. 또한 수립 계획을 바탕으로 도입 비용을 산정하고, 비용을 승인할 권한이 있는 경영진 혹은 재무 관련 책임자를 설득하는 것 역시 쉽지 않을 것이다.

기존에 제시된 보안 성숙도 모델들은 기업들의 현재 보안 성숙도 수준을 평가할 수 있는 방법론을 제시함으로써, 조직 내 보안 역량을 객관적으로 평가할 수 있는 수단을 제공한다. 제로트러스트 관점에서도 이와 유사한 방식으로 보안 성숙도 수준을 평가할 수 있는 모델이 존재한다면, 제로트러스트 아키텍처를 도입·구축하는 데 있어 왜 이 아키텍처를 도입해야 하는지, 도입 계획은 어떻게 수립해야 하는지 등에 대한 객관적 근거로 활용할 수 있을 것이다.

2021년 바이든 대통령의 '국가 사이버보안 개선에 관한 행정 명령(EO-14028)'에 따라 제로트러스트를 도입해야 하는 연방시민행정기관(FCEB)들 역시 제로트러스트 도입 과정에서 어려움을 겪을 수 있었기 때문에, CISA는 같은 해 기관들을 돕기 위하여 기업망 내 5가지 핵심 요소에 대해 3가지 성숙도 수준을 갖는 '제로트러스트 성숙도 모델 v1.0'을 공개한 바 있으며, 2023년에는 성숙도 수준을 4단계로 확장하고 각 수준별 보안 기능에 대해 더욱 구체화한 바 있다.

2022년 바이든 대통령의 국가안보각서(NSM-08)에 따라 제로트러스트를 도입하는 국방부 및 정보 공동체 시스템 등에 적용할 수 있도록, NSA는 2023년 4월부터 2024년 7월까지 기업망 핵심 요소 7가지의 성숙도 개선에 관한 문서를 각각 발간하였다. 이 문서들은 2023년 4월에 발간한 '사용자(User)' 핵심 요소를 제외하면, 국방부 제로트러스트 전략 문서에서 정의하고 있는 핵심 요소별 보안 역량(Capability)에 대한 성숙도 수준을 제안하였다.

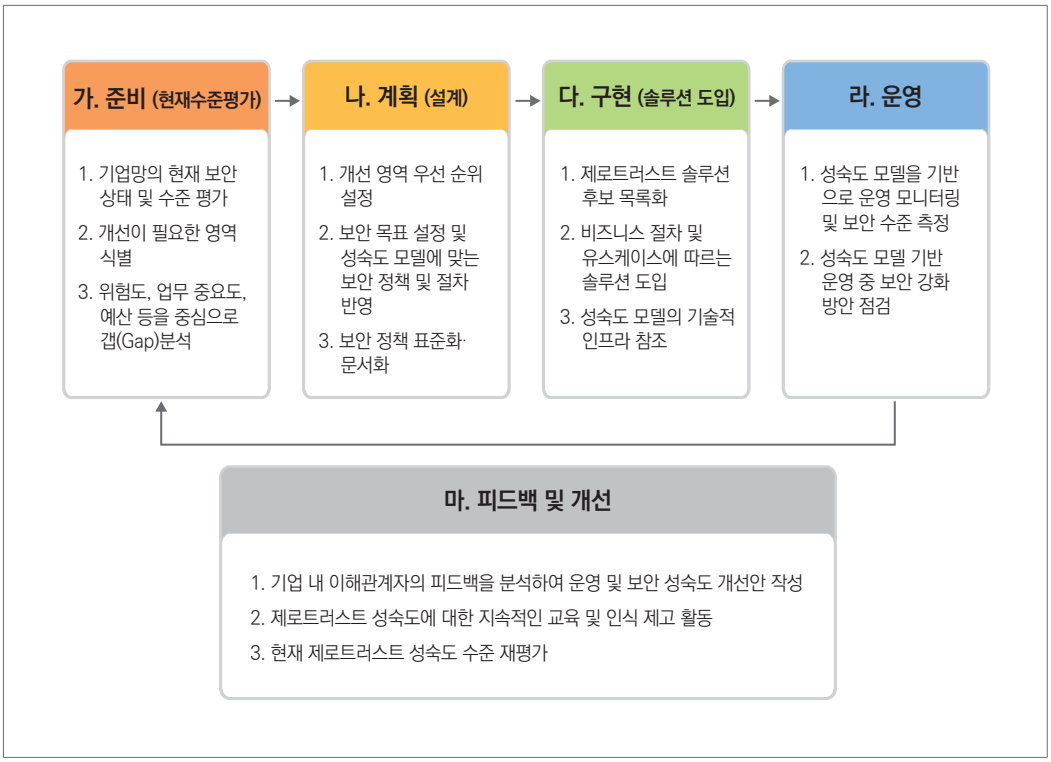
따라서, 본 가이드라인 2.0에서도 제로트러스트를 도입하는 국내 기업이 해당 조직의 현재 제로트러스트 수준을 파악하고 도입 계획을 수립할 수 있도록, 3.2절에서 가이드라인 1.0의 제로트러스트 성숙도 모델을 개선하여 제시하고자 한다. 본 가이드라인의 제로트러스트 성숙도 모델이 조직 내 제로트러스트 아키텍처를 구성하는데 있어 절대적인 답안을 제공하는 것은 아니지만, 현재 제로트러스트 수준을 평가(Assessment)하고 구현·도입하는 데 도움을 줄 수 있을 것이다.

2. 제로트러스트 도입 절차의 세부 단계별 성숙도 모델 활용 방안

제로트러스트를 도입하는 국내 기업은 제로트러스트 성숙도 모델을 활용할 수 있다. 가이드라인 1.0에서 제로트러스트 도입 절차를 '준비→계획→구현→운영→피드백 및 개선'의 총 5가지 세부 단계로 구성되는 순환 주기로 소개한 바 있으며, 이 과정을 통해 제로트러스트 아키텍처를 운영하면서 사용자들로부터의 피드백 및 개선 요구를 통하여 더 높은 수준의 제로트러스트 성숙도 목표를 세우거나, 혹은 차후 계획을 재검토할 수 있다고 언급하였다.

여기에서는 각 세부 단계에서 앞에서 언급한 성숙도 모델을 어떻게 활용할 수 있는지 [그림 3-1]에서 표현하고, 이를 구체적으로 설명한다.

그림 3-1 제로트러스트 도입 절차의 세부 단계별 성숙도 모델 활용 방안



가. 준비 단계 - 현재 보안 상태 평가 및 갭 분석에 활용

준비 단계에서는 현재 기업의 상황과 현재 수준을 정확히 파악하고 평가하는 것을 목표로 한다. 제로트러스트의 도입은 단 한 번의 절차로 완료되지 않기 때문에, 이 단계는 제로트러스트를 처음 도입할 때의 가장 첫 단계일 수도 있고 이미 도입하여 운영 중인 기업망에 대해 더 높은 수준의 성숙도를 갖는 제로트러스트 아키텍처로 진화하기 위한 준비 단계일 수도 있다.

여기에서 제로트러스트 성숙도 모델은 다음과 같이 활용할 수 있다. 제로트러스트 성숙도 모델을 통하여 기업망의 현재 보안 상태를 평가하고 갭(Gap) 분석을 할 수 있다. 현재 기업망에 도입하여 운영 중인 전체 보안 아키텍처 및 솔루션들에 대하여 제로트러스트 성숙도 모델의 기준에 맞춰 수준을 평가하고 개선이 필요한 영역을 식별하는 것이 가능하다. 갭 분석 과정에서 우선순위를 설정하기 위하여, 갭 분석 결과에 대해 위험도, 업무 중요도, 예산 등을 중심으로 정리할 수 있을 것이다.

나. 계획(설계) 단계 - 우선순위 설정 및 정책·절차 수립에 활용

계획 단계에서는 기업망 차원에서 제로트러스트를 도입하기 위한 계획을 수립하고 설계한다. 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.

준비 단계에서 제로트러스트 성숙도 모델을 통하여 현재 보안 상태를 평가하고 갭 분석을 진행하였다면, 그 결과를 바탕으로 어떤 부분을 먼저 개선할지에 대한 우선순위를 설정해야 한다. 앞서 위험도, 업무 중요도, 예산 등을 중심으로 갭 분석이 이루어졌다면, 조직 내외부 관련자 및 전문가와 함께 우선순위를 어떤 기준으로 정리할지를 결정하여야 한다. 예를 들어, 비용이 많이 들더라도 위험을 최소화하기 위하여 민감한 데이터 보호가 우선시 될 수 있으며, 현재 조직 차원에서의 통합 인증 시스템이 구축되어 있지 않아 식별자 핵심 요소에 대한 성숙도가 낮다면 이를 더욱 시급하게 생각할 수도 있을 것이다.

우선순위 설정이 되었다면 이를 현 단계에서의 보안 목표로 설정하고 그에 맞춰 계획 단계를 진행하게 되는데, 여기에서 제로트러스트 성숙도 모델의 각 단계에 맞는 보안 정책과 절차를

파악하여 반영하게 된다. 이러한 정책이 조직 전반에 걸쳐 일관되게 적용될 수 있도록 구현해야 하는 보안 기능 및 그에 따르는 활동 계획, 구현 책임자, 도입 솔루션 후보에 대한 평가 등을 표준화·문서화된 형태로 정리하여 구현 단계로 진입할 수 있어야 한다.

다. 구현(솔루션 도입) 단계 – 비즈니스 프로세스 및 유스케이스에 적합한 솔루션 도입에 활용

구현 단계에서는 제로트러스트 도입 대상이 되는 비즈니스 프로세스 후보가 구성된 상태에서, 제로트러스트 솔루션 후보에 대한 목록을 작성하고 비즈니스 프로세스 및 유스케이스에 따라 적합한 솔루션을 선택하여 도입한다.

제로트러스트 성숙도 모델은 일반적으로 필요한 보안 기능과 역량 등 기술적 인프라를 같이 기술하고 있다. 따라서, 도입 절차에서 기업망에 적합한 솔루션을 선택할 때 어떤 보안 기능과 역량을 활용할 수 있는지를 미리 참조할 수 있으며, 특히 현재 도입 절차의 목표에 어울리지 않는 보안 인프라를 도입하는 것을 막을 수 있다. 특히 접근 주체와 리소스에만 집중을 하면, 기업망이 복잡해짐에 따라 안전한 운영 관점에서 매우 중요한 시각화 및 분석, 자동화 및 통합 등에 대한 보안 기능 도입에 소홀해질 가능성이 있다. 그러나 제로트러스트 성숙도 모델을 충분히 활용하는 경우, 이러한 영역까지 상세히 기술되어 있어 제로트러스트 도입과 아키텍처 구현에 큰 도움이 될 것이다.

라. 운영 단계 – 현재 운영 중인 보안 솔루션의 실제 성숙도 분석 및 재평가

운영 단계에서는 제로트러스트 솔루션이 도입되어, 특정 비즈니스 프로세스에 대한 제로트러스트 아키텍처 보안 모델이 구현되어 있는 상태에서 기업 관리자가 해당 솔루션을 기반으로 정책을 설정하고 시행하게 된다. 따라서, 현재 실행 중인 솔루션들에 대해서 보안 기능과 역량이 잘 구현되어 있는지 성숙도 모델을 기반으로 운영 과정을 모니터링함으로써 보안 수준을 측정할 수 있다. 보안 기능이 구현되어 있지만 운영 상에서 활용하기 어려울 수도 있고, 혹은 기능을 활용 중이기는 하나 더 높은 성숙도로 이동하기 어려운 형태로 구현되어 있을 수도 있다.

운영 중에는 실제로 해당 보안 솔루션의 보안 기능과 역량이 잘 구현되어 있는지, 처음 달성하고자 했던 성숙도 목표와 일치하는지를 정확히 판단할 수 있다. 따라서, 성숙도 모델을 기반으로 모니터링 및 보안 수준 측정을 통해 보안 솔루션의 실제 성숙도 및 운영 관련 정보를 획득하여 보안 강화 방안을 점검 후, 개선 필요성을 검토할 수 있도록 피드백 및 개선 단계에 제공한다.

마. 피드백 및 개선 단계 - 인식 제고 및 성숙도 수준 재평가

피드백 및 개선 단계에서는 기업 관리자의 판단하에 기업망에서 제로트러스트 아키텍처 및 이를 구성하는 보안 솔루션들이 원활하게 작동되고 있다는 가정하에, 기업 내 임직원 및 이해관계자들이 운영 개선을 위한 피드백을 제공하고 관리자가 이를 분석하여 운영 및 보안 성숙도 개선안을 만들게 된다.

이러한 피드백이 원활하게 이루어지기 위해서는, 임직원 및 이해관계자들이 제로트러스트의 원칙 및 기업 내 도입 전략과 계획에 대해 명확하게 이해하고 있어야 한다. 현재의 제로트러스트 성숙도를 고려한 피드백이 이루어질 수 있도록 이에 대한 지속적인 교육과 인식 제고 활동이 필요하다고 볼 수 있다.

또한, 현재 운영 중인 제로트러스트 아키텍처에 대한 성숙도가 처음 목표한 수준과 동일한지, 또한 구현된 보안 기능이 처음 달성하고자 했던 목표 수준과 일치하는지를 운영 단계에서 분석하여 보안 솔루션의 실제 성숙도 및 운영 관련 정보를 획득할 수 있다. 이 정보를 기반으로 현재의 성숙도 모델에 대한 개선이 필요하지 않은지 분석함으로써 현재 제로트러스트 성숙도 수준을 재평가하고 다음 도입 주기로 진입하는데 활용할 수 있을 것이다.

3. 제로트러스트 아키텍처 적용을 위한 기업망 핵심 요소

제로트러스트는 앞서 정의한 바와 같이 적극적인 신뢰도 평가 없이 접근을 허용하지 않는 보안 모델 및 아이디어의 집합을 의미하고 있으나, 이러한 정의는 제로트러스트 아키텍처를 자사의 기업망에 도입하기 위하여 목표 및 도입 전략·계획을 수립해야 하는 기업에게는 매우 추상적으로 느껴질 수 있다.

기업망 핵심 요소는 제로트러스트 관점에서 기업망의 보안성을 개선하기 위하여 무엇을 보호해야 하는가에 대한 답으로 볼 수 있다. 조금 더 살펴보면, 기업망에서 가장 중요한 보호의 대상은 데이터(Data)로 볼 수 있다. 식별자(Identity)로 구분되는 사용자는 기기(Device)를 이용하여 기업 네트워크(Network) 상에서 애플리케이션 및 워크로드(Application & Workload)를 통해 데이터에 접근하게 되며, 데이터는 중요 데이터 서버 등 시스템(System)에 위치할 수 있다. 이들은 모두 사이버 공격 대상이 될 수 있어, 제로트러스트 관점에서 기업망의 핵심 요소로 볼 수 있다.

표 3-1 제로트러스트 아키텍처 적용을 위한 기업망 핵심 요소

기업망 핵심 요소	설명
식별자·신원 (Identity)	▸ 사람, 비인간개체(서비스 혹은 IoT 기기 등)를 고유하게 설명할 수 있는 속성 혹은 속성의 집합을 의미 ▸ 기업은 식별자를 가진 사람 혹은 기기가 리소스에 접근하고자 하면 강한 인증 방식을 사용하여 해당 식별자를 검증하고 세밀한 접근제어 규칙에 따라 적절한 시간 내에 해당 리소스에 접근을 보장
기기 및 엔드포인트 (Device/Endpoint)	▸ IoT 기기, 휴대폰, 노트북, PC, 서버 등을 포함하여 기업망에 연결하여 데이터를 주고받는 모든 하드웨어 기기 ▸ 일반적으로 기업 소유이나 BYOD와 같은 개인 기기일 수도 있음 ▸ 기업은 기기에 대한 목록을 유지하여야 하며, MDM 등의 기술을 활용하여 리소스에 접근하려는 기기에 대한 신뢰도를 평가하는 등 허가받지 않았거나 신뢰할 수 없는 기기가 리소스에 접근하는 것을 막을 수 있어야 함
네트워크 (Network)	▸ 기업망의 유무선 네트워크, 클라우드 접속을 포함하는 인터넷 등 데이터를 전송하기 위해 사용되는 모든 형태의 통신 매체를 포함 ▸ 기업은 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)	▸ 중요 애플리케이션을 구동하거나 중요 데이터를 저장하고 관리하는 서버들을 포함하며, 온프레미스(On-Premise) 및 클라우드에 구축 운용 중인 모든 서버 시스템들이 여기에 해당 ▸ 시스템의 주요 파일의 읽기 및 쓰기, 주요 명령어 사용 등 시스템 리소스 접근에 관한 세밀하고 상세한 접근제어 필요 ▸ 매 세션마다 다중인증(MFA) 등 강력한 신원 확인 및 위험 관리 절차를 포함하여야 함
애플리케이션 및 워크로드 (Application & Workload)	▸ 기업망 관리 시스템, 프로그램, 온프레미스 및 클라우드 환경에서 실행되는 서비스를 포함하며, 데이터를 주고받기 위한 인터페이스 제공 ▸ 기업에서는 애플리케이션 계층 및 컨테이너, 가상 머신 등을 보호·관리하고 데이터의 안전한 전달을 보장할 수 있어야 함
데이터 (Data)	▸ 가장 최우선으로 보호해야 할 리소스 ▸ 기업은 데이터 목록을 작성, 분류 및 레이블 지정하고, 필요에 따라 암호화 기법을 적용하여 저장 혹은 전송 중인 데이터를 보호하며 허가받지 않은 데이터 유출에 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.

표 3-2 기업망 핵심 요소에 대한 교차 기능

기업망 핵심 요소에 대한 교차 기능	설명
가시성 및 분석 (Visibility & Analytics)	▸ 사용자 혹은 기기, 애플리케이션 및 워크로드의 상태 확인 등 중요하고 상황에 맞는 세부 정보를 이용하여 분석하고 가시성을 제공하는 교차 기능 ▸ 기업은 기업망 내부에서 벌어지는 비정상 행위에 대한 탐지를 개선하고, 보안 정책 및 접근제어 결정을 동적으로 적용하는 데 활용 ▸ 네트워크 트래픽을 패킷 단위로 직접 캡처하고 분석함으로써, 네트워크를 통해 진입하는 모든 종류의 위협을 관찰하고 지능화된 방어 기법을 적용하여야 함
자동화 및 통합 (Automation & Orchestration)	▸ 기존에 수동적으로 적용하던 보안 프로세스를 개선하여 자동화된 정책 기반 보안 프로세스를 적용함으로써 보다 신속한 보안 조치를 가능하게 하는 교차 기능 ▸ SIEM 및 기타 자동화된 보안 솔루션 통합, SOAR 적용 등의 방법을 통하여, 기업망의 모든 환경에서 정의된 프로세스와 일관된 보안 정책을 시행함으로써 자동화된 통합 보안 대응 가능

제로트러스트 성숙도 모델은 각 기업들이 제로트러스트 아키텍처를 도입하는 관점에서 반드시 고려해야 한다. 본 가이드라인에서 정의하는 제로트러스트 성숙도 모델 2.0은 가이드라인 1.0 이후 발간된 다양한 제로트러스트 관련 문서 및 여러 전문가 논의를 통하여 기업망 핵심 요소들에 대한 제로트러스트 성숙도 모델을 업데이트하고 보안 기능을 구체화하는 내용을 포함한다.

4. 제로트러스트 성숙도 모델 2.0

제로트러스트 성숙도 모델은 조직의 보안 시스템이 “신뢰하지 말고 항상 검증하라”는 제로트러스트 원칙에 얼마나 성숙하게 대응하고 있는지를 측정하는 도구이다. 성숙도 모델은 조직이 현재 위치한 성숙도 수준을 파악하고, 제로트러스트 전략을 더욱 강화하는 데 필요한 기술적, 조직적, 절차적 변화를 제시한다.

성숙도 모델은 조직의 현재 성숙도를 이해하고, 이 성숙도를 높이기 위해 필요한 구체적인 행동 계획을 수립하는 데 사용된다. 이를 통해 조직은 보안 위협에 더 잘 대응할 수 있는 능력을 갖추고, 변화하는 사이버 위협 환경에 효과적으로 적응할 수 있다. 조직은 이 모델을 통해 제로트러스트 보안 전략의 구축 및 운영에 대한 체계적인 로드맵을 마련할 수 있으며, 이를 통해 지속적인 개선과 최적화가 가능하다.

제로트러스트 성숙도 모델은 제로트러스트 보안 전략을 조직에 맞게 단계적으로 구현하고, 그 성과를 측정하며, 점진적으로 성숙도를 높이는 데 중점을 둔 프레임워크라고 할 수 있다. 또한,

기본적인 수준에서 출발하여 최적의 보안 수준을 추구하는 장기적인 여정이다. 신뢰 없는 환경을 가정하고 모든 접근과 트래픽을 검증하는 보안 철학으로 점차 나아가는 과정이다.

제로트러스트 성숙도는 기업망의 전반적인 보안성을 높이기 위하여 한 번의 작업 혹은 단기간에 최적화 수준을 달성할 수 없으며, 수차례 도입 및 피드백 등을 거쳐 점진적인 변화를 통해 최적화 수준에 다가가는 모양으로 발전하게 된다. 제로트러스트 성숙도 관점에서 핵심 요소별 기능 및 각 성숙도 수준별 의미에 대해서는 가이드라인 1.0에 상세하게 설명한 바 있다.

본 가이드라인 2.0에서는 2023년 4월 발표한 CISA 성숙도 모델 2.0, 그리고 2023년부터 2024년까지 핵심 요소별로 발표한 NSA 성숙도 개선 문서 등을 참고하여 성숙도 수준을 〈표 3-3〉과 같이 4단계로 재정의하였으며, 4단계로 재구성한 제로트러스트 성숙도 모델 2.0 및 각 핵심 요소에 대한 성숙도 수준별 특징을 [그림 3-2]와 같이 정의한다.

표 3-3 제로트러스트 성숙도 모델 2.0의 성숙도 수준 4단계

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

여기에서 반드시 기억해야 하는 사항은, 제로트러스트 성숙도 모델이 제로트러스트 아키텍처를 도입하는 데 있어서 절대적인 답안지로 오해하여 모든 기능을 최적화 수준으로 달성하고자 할 필요는 없다는 것이다. 본 가이드라인에서 제시하는 성숙도 모델을 참조하여, 기업의 규모와 분야, 접근 주체, 리소스 종류, 네트워크 아키텍처, 대상 규정 등에 따라 성숙도 모델을 재정의할 수

6 가이드라인 1.0에서 없었던 단계로, 본 가이드라인 2.0에서 새로 추가되었음

있으며, 이 과정에서 제로트러스트 아키텍처의 기본 원리와 기업 상황을 고려하여 제로트러스트 기능과 성숙도 수준을 선택, 수정 혹은 구체화하여도 무방하다.

그림 3-2 제로트러스트 성숙도 모델 2.0 요약

	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
식별자 · 신원	• 온프레미스ID 사용 • 패스워드 혹은 다중인증 방식 • 수동접근 및 자격증명 관리	• 클라우드와 온프레미스 기반 ID 연계 • 다중인증 및 FIDO 기반인증 • 수동 및 정적 규칙 기반 위험 판단	• 컨텍스트 기반 ID 인증 • 일부 자동화된 및 동적 규칙을 이용한 위험도 평가 • 세션 기반 접근 지원	• 클라우드와 온프레미스 시스템 전반에 걸친 글로벌ID • AI 기반 위험도 결정 및 지속적 보호 • 자동화된 적시·최소 권한 접근 적용
기기 및 엔드포인트	• 제한된 정책준수정보 • 단순하고 수동적 기기 목록 관리 • 수동적위협보호 기능 적용	• 대부분의 기기에 정책 준수 시행 메커니즘 사용 • 모든 기기에 대해 목록화 • 기기 보안솔루션 자동 관리	• 규정 준수 여부에 따른 접근 권한 부여 • 검증된 기기만 데이터 접근 • 자동화, 중앙집중식 위협 보호 및 자산관리 기능 통합	• 지속적인 기기 보안 상태 모니터링 및 검증 • 모든 환경에 걸쳐 자산 및 취약점 관리 통합 • 모든 기기에 대해 위협 보호
네트워크	• 경계분리 네트워크 구조 정의 • 알려진 위협 및 정적 트래픽 필터링 • 매우 중요한 애플리케이션 및 워크로드에 대한 기능 회복	• 소규모 경계를 통해 확장된 네트워크 구조 정의 • 내부 애플리케이션 모든 트래픽 및 외부 일부 트래픽 암호화 • 위험성이 없는 워크로드에 대한 탄력적인 네트워크 회복	• 마이크로 세그먼트를 통해 엔드포인트 및 애플리케이션 격리메커니즘 배포 • 비정상적인 데이터 흐름 격리 및 제거 • 자동화된 위험 인식 기반 동적 네트워크 규칙 생성	• 컨텍스트 기반 및 기계학습 기반 위협 보호 통합 • 암호화 민첩성 • 우선 순위 지정 가능한 동적 네트워크 규칙 생성
시스템	• 로컬 시스템 기반 ID/패스워드 등 단순인증 • 정적 속성 등 최소한의 권한 분리 정책 적용 • 온프레미스 시스템보안 패치 및 정책 수동 변경	• 독립적인 시스템으로 계정 관리 • 일부 중요도에 따르는 네트워크 세분화 • 온프레미스 및 클라우드 시스템에 대한 패치 수준 자동 확인 기능	• 동적 접근 권한 통제 • 등급 및 기능별 네트워크 분류 • 온프레미스 및 클라우드 시스템에 대한 자동화된 보안 패치	• 다중인증 및 신뢰도 기반 접근 인가 • 세분화된 리소스별 접근 정책 적용 • 온프레미스 및 클라우드 상의 모든 시스템 실시간 모니터링 및 자동화된 보안 패치
애플리케이션 및 워크로드	• 로컬 인가 및 정적 속성 기반 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대해 최소한의 통합 • 정적·수동테스트 수행	• 애플리케이션 워크플로우와 위협 보호에 대한 기본적인 통합 • CI/CD 파이프라인 DevSecOps, SBOM 적용 • 동적 테스트 방법 사용	• 확장된 컨텍스트 정보 및 최소권한 원칙의 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대한 강력한 통합 • 정기적인·자동화된 테스트	• 실시간 위험 분석을 통해 지속적 애플리케이션 인가 • 모든 애플리케이션에 사용자 및 단말 직접 접근 가능 • 자동화된 코드 배포 및 소프트웨어 검증
데이터	• 정적, 수동 데이터 분류 및 접근제어 • 온프레미스 및 암호화되지 않은 데이터 저장소 • 제한된 임시 데이터 분류	• 일부 자동화된 추적 기반 수동데이터 분류 및 목록화 • 최소한의 권한 요소를 통합한 데이터 접근 • 정적 레이블 및 수동 메커니즘 데이터 분류	• 속성에 기반한 최소 권한 제어기법으로 접근관리 • 저장소의 모든 데이터 암호화 • 레이블 지정 프로세스 계층화 및 데이터 목록화 자동화	• AI를 이용한 지속적인 데이터 분류 및 목록화 자동화 • 적시·최소권한 동적 데이터 접근 • 사용중인 데이터 암호화 및 최신 암호화 적용

가. 식별자·신원

'식별자·신원' 핵심 요소의 경우 4가지 기능(식별자 관리, 인증, 위험도 평가, 접근 관리)이 있으며, 교차 역량(가시성 및 분석, 자동화 및 통합)을 반영한 표는 아래와 같다.

표 3-4 식별자·신원 핵심 요소에 대한 제로트러스트 성숙도 모델

기능	기존	초기	향상	최적화
식별자 관리	▸ 온프레미스 ID 사용	▸ 클라우드와 온프레미스 시스템을 기반으로 ID 연계 ▸ SSO 지원	▸ ID 통합 관리 시스템 구축	▸ 클라우드 및 온프레미스 환경 전반에 걸쳐 글로벌 ID 활용
인증	▸ 패스워드 혹은 다중인증 방식	▸ 다중인증 방식 기반 인증·FIDO 기반 인증	▸ 컨텍스트 기반 ID 인증	▸ 접근권한 승인 때 뿐만 아니라, 지속적인 신원 검증
위험도 평가	▸ 위험에 대한 제한된 결정	▸ 수동 분석과 정적 규칙을 기반으로 식별자 위험도 판단	▸ 일부 자동화된 분석과 동적 규칙을 사용한 위험도 평가	▸ AI 기반 실시간 사용자 행동 분석을 통해 위험도 결정 및 지속적 보호
접근 관리	▸ ID 기반, 수동으로 관리되는 그룹 및 역할을 사용하여 접근 관리 ▸ 시스템 별 각기 다른 관리 기능	▸ 관리 기능 통합 ▸ 최소 권한 원칙에 따라 접근 정책 검토	▸ 사용자 및 리소스에 맞는 조정된 권한을 사용하여 세션 기반 접근 지원	▸ 자동화를 통해 개별 요구사항에 맞는 적시·최소권한 접근 적용
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	▸ 일부 사용자 및 엔티티에 대한 자동화된 분석 수행·가시성을 위한 수집 정보 확대	▸ 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 연계 및 ID 저장소를 통한 관리 허용을 위한 기본 자동화 통합	▸ 특정 권한이 필요한 ID만 수동으로 하고 나머지 모든 ID에 대한 통합 자동화	▸ ID 생명 주기를 완벽히 통합하고, 동적 사용자 프로파일링, 동적 ID 및 그룹 멤버십, 적시·최소권한 접근제어 구현

나. 기기 및 엔드포인트

'기기 및 엔드포인트' 핵심 요소의 경우 4가지 기능(정책 준수 모니터링, 데이터 접근제어, 자산 관리, 기기 위협 보호)이 있으며, 교차 역량(가시성 및 분석, 자동화 및 통합)을 반영한 표는 아래와 같다.

표 3-5 기기 및 엔드포인트 핵심 요소에 대한 제로트러스트 성숙도 모델

기능	기존	초기	향상	최적화
정책 준수 모니터링	▸ 기기 정책 준수를 위한 제한된 정보 제공	▸ 대부분의 기기에 정책 준수 시행 메커니즘 사용	▸ 규정 준수 여부에 따른 접근권한 부여	▸ 지속적인 기기 보안 상태 모니터링 및 검증 ▸ 규정 위반 시 동적으로 권한 수정
데이터 접근제어	▸ 데이터 접근 기기에 대한 정보에 의존하지 않음	▸ 첫 데이터 접근 시 기기 상태 고려	▸ 검증된 기기만 데이터 접근	▸ 기기에 대한 실시간 위험 분석을 통한 동적 접근 결정
자산 관리	▸ 단순하며 수동으로 추적되는 기기 목록 관리	▸ 모든 기기에 대한 완벽한 목록 보유	▸ 자동화된 방법을 이용하여 자산 관리, 취약성 식별, 자산에 대한 패치 적용	▸ 클라우드 및 원격을 포함한 모든 환경에 걸쳐 자산 및 취약점 관리 통합
기기 위협 보호	▸ 일부 기기에 위협 보호 기능 수동 적용 ▸ 수동 취약점 파악, 패치 적용	▸ 기기 보안 솔루션 자동 설치·관리 ▸ EDR 솔루션 사용 ▸ 자동 패치 확인 기능 보유	▸ 중앙 집중식 솔루션에 위협 보호 기능 통합 ▸ 연계기반 이상 행위 분석 등을 통한 비정상 행위 모니터링 및 대응 (XDR 등) ▸ 펌웨어 유지 관리 프로세스 도입	▸ 모든 기기에 대하여 기기 위협 보호, 정책 시행, 규정 준수 모니터링을 위한 솔루션 배포 ▸ 모든 패치 자동화
가시성 및 분석	▸ 기기 관리는 라벨 수동 검사, 주기적 네트워크 검색 및 보고에 의존	▸ 수동 모니터링 및 일부 리소스에 대한 자동화된 분석	▸ 승인되지 않은 기기 감지 및 인벤토리 수집, 이상 탐지 자동화	▸ 기업은 지속적으로 기기 상태 평가 실행
자동화 및 통합	▸ 기업 내에서 기기를 수동으로 프로비저닝, 구성 및 등록	▸ 기기에 대한 프로비저닝, 구성, 등록, 해제 프로세스 자동화	▸ 규정 미준수한 구성요소 격리	▸ 기기 및 가상 자산 프로비저닝, 등록, 모니터링, 격리, 수정 및 해제 완전 자동화

다. 네트워크

'네트워크' 핵심 요소의 경우 5가지 기능(네트워크 세분화, 위협 대응, 트래픽 암호화, 트래픽 관리, 네트워크 회복성)이 있으며, 교차 역량(가시성 및 분석, 자동화 및 통합)을 반영한 표는 아래와 같다.

표 3-6 네트워크 핵심 요소에 대한 제로트러스트 성숙도 모델

기능	기존	초기	향상	최적화
네트워크 세분화	▸ 대규모 경계·분리를 사용하는 네트워크 구조 정의	▸ 일부 내부적인 세분화를 갖는 송수신 소규모 경계를 통해 더 많은 네트워크 구조 정의	▸ 마이크로 세그먼트 (Micro-Segment) 간 송수신 제어를 통해 더 많은 네트워크 아키텍처에 엔드포인트 및 애플리케이션 격리 메커니즘 배포	▸ 네트워크 구조는 주변 애플리케이션 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	▸ 비정상적인 데이터 흐름 격리 및 제거	▸ 컨텍스트 기반 신호와 기계학습 기반 위협 보호 및 필터링 통합
트래픽 암호화 (가이드라인 1.0의 암호화)	▸ 최소한의 내외부 트래픽에 대한 명시적 암호화	▸ 내부 애플리케이션에 대한 모든 트래픽 및 일부 외부 트래픽 암호화	▸ 가능한 경우, 내외부로 전달되는 모든 트래픽 암호화	▸ 암호 민첩성[7] 적용
트래픽 관리	▸ 제한된 모니터링 (수동적)	▸ 애플리케이션 별 트래픽 매칭	▸ 자동화된 위험 인식 기반 동적 네트워크 규칙 및 구성	▸ 애플리케이션 우선 순위 재지정이 가능한 동적 네트워크 규칙 및 구성
네트워크 회복성	▸ 매우 중요한 애플리케이션 및 워크로드에 대한 기능 회복	▸ 추가 애플리케이션 회복 ▸ 위험하지 않은 워크로드에 대한 탄력적 네트워크 회복	▸ 대부분의 애플리케이션에 대한 가용성 및 회복	▸ 모든 워크로드에 대한 가용성
가시성 및 분석	▸ 중앙 집중식 수집 및 분석을 통하여 경계에서 가시성 제공	▸ 알려진 지표 기반 네트워크 모니터링 기능 사용	▸ 이상 기반 네트워크 감지 기능 사용 ▸ 모든 환경에 대한 상황 인식, 분석 수행	▸ 모든 네트워크 트래픽에 대한 가시성 유지 ▸ 상관관계 분석을 통한 모니터링
자동화 및 통합	▸ 수동 정책 기반 상황 인식 및 리소스 관리	▸ 일부 네트워크 또는 환경에 대한 수명주기 관리	▸ 모든 네트워크 환경에 대한 관리 및 리소스 수명 주기 관리	▸ 네트워크에 대한 자동화된 변경 및 관리 기능 수행

7 암호 민첩성(Cryptographic Agility)은 암호화 정책과 기술을 유연하고 빠르게 변화하는 환경에 맞게 조정하고, 상황에 따라 적절한 암호화 기법을 신속하게 적용할 수 있는 능력을 의미하며, 미국 국토안보부(DHS)는 주변 인프라를 수정하거나 교체할 필요 없이 향후 암호화 알고리즘 및 표준을 업데이트할 수 있는 설계 기능으로 정의하고 있음

라. 시스템

'시스템' 핵심 요소의 경우 4가지 기능(접근통제, 시스템 계정 관리, 네트워크 분리 정책, 시스템 보안 및 정책 관리)이 있으며, 교차 역량(가시성 및 분석, 자동화 및 통합)을 반영한 표는 아래와 같다.

표 3-7 시스템 핵심 요소에 대한 제로트러스트 성숙도 모델

기능	기존	초기	향상	최적화
접근통제	▸ 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 접근하거나 주요 명령어를 실행할 때 접근제어 정책에 따라 보안 정책 적용	▸ 접근 요청 사용자와 요청에 사용되는 기기·시스템에 따라 접근권한이 동적으로 달라짐	▸ 시스템 접근 시 다중 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 프로비저닝됨	▸ 접근 인가를 진행하는 권한 사용자의 계정 관리가 독립 시스템을 기반으로 통합적으로 이루어지고 권한 사용자의 보안 관리 정책이 계정관리와 통합 및 중앙 일원화 되어 접근제어 정책 적용	▸ 세분화된 리소스 별 접근 정책 적용되며, 권한 사용자의 이상 행위를 판별하여 실시간으로 시스템 계정 잠금·해제 기능 제공
네트워크 분리 정책	▸ 중요도 구분 없이 망분리 등 네트워크 경계형 모델을 기반으로 시스템 영역을 구분하고 배치	▸ 일부 시스템을 중요도에 따라 세분화하여 시스템들 간 접속 이동에 있어 보안 정책 적용	▸ 등급 및 기능별 분류, 세분화 및 강력한 시스템 보안 접근 정책을 기반으로 분류 그룹 간 이동 통제	▸ 분류 그룹 간 재인증없이 이동이 가능하게 하는 추가적인 정책 적용
시스템 보안 및 정책 관리	▸ 온프레미스 시스템 보안 패치 및 정책 변경은 수동으로 이루어짐	▸ 온프레미스 및 클라우드 시스템에 대한 패치 수준 자동 확인 기능 제공	▸ 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	▸ 센서 및 시스템과 격리된 상태에서 시스템 상태 및 보안 모니터링 수행	▸ 외부 센서 및 시스템과 격리된 상태에서 시스템 상태 및 보안 모니터링 일부 자동화	▸ 일부 외부 센서와 시스템을 사용하여 컨텍스트 관점에서, 시스템 상태 및 보안 모니터링 수행	▸ 외부 센서와 시스템을 사용하여 지속적이고 동적인 애플리케이션 상태 및 보안 모니터링 수행
자동화 및 통합	▸ 시스템 제공 시, 애플리케이션 호스팅 위치와 접근을 설정	▸ 변경된 상태를 기기와 네트워크 구성 요소에 알림	▸ 보안과 성능 최적화를 위한 지속적인 환경 변화에 적응	▸ 모든 시스템에 대한 중앙 집중 관리 및 AI 기반 시스템 이상행위 탐지

마. 애플리케이션 및 워크로드

'애플리케이션 및 워크로드' 핵심 요소의 경우 5가지 기능(애플리케이션 접근, 애플리케이션 위협 보호, 접근 가능한 애플리케이션, 안전한 애플리케이션 배포, 소프트웨어·애플리케이션 보안)이 있으며, 교차 역량(가시성 및 분석, 자동화 및 통합)을 반영한 표는 아래와 같다.

표 3-8 애플리케이션 및 워크로드 핵심 요소에 대한 제로트러스트 성숙도 모델

기능	기존	초기	향상	최적화
애플리케이션 접근(가이드라인 1.0의 접근 인가)	▸ 애플리케이션 접근은 주로 로컬 인가 및 정적 속성에 기반	▸ 애플리케이션 접근은 중앙집중적 인증, 인가, 모니터링과 속성에 의존	▸ 확장된 컨텍스트 정보와 최소 권한 원칙의 애플리케이션 접근	▸ 실시간 위험 분석을 고려하여 애플리케이션 접근을 지속적으로 인가
애플리케이션 위협보호 (가이드라인 1.0의 위협보호)	▸ 알려진 위협에 대한 범용 보호 기법을 적용하여, 애플리케이션 워크플로우와 위협 보호에 대한 최소한의 통합	▸ 일부 애플리케이션 별 보호 기법을 사용하여 알려진 위협에 대한 보호를 적용하여, 애플리케이션 워크 플로우와 위협 보호에 대한 기본적인 통합	▸ 애플리케이션 동작을 이해하고 설명하는 보호 기법을 제공하는 분석을 사용하여, 애플리케이션 워크 플로우와 위협 보호에 대한 강력한 통합	▸ 정교한(맞춤형) 공격에 대한 보호
접근 가능한 애플리케이션 (가이드라인 1.0의 접근성)	▸ 일부 중요 클라우드 애플리케이션은 인터넷을 통해 사용자가 직접 접근하며, 그 외의 다른 애플리케이션은 VPN을 통한 접속	▸ 모든 클라우드 애플리케이션과 일부 온프레미스 애플리케이션은 인터넷을 통해 사용자가 직접 접근하며, 그 외 다른 애플리케이션은 VPN을 통한 접근	▸ 모든 애플리케이션은 인터넷을 통해 사용자가 직접 접근 가능	▸ 모든 애플리케이션은 인터넷을 통해 사용자 및 단말이 직접 접근 가능
안전한 애플리케이션 배포	▸ 강력하지 않은 코드 배포 메커니즘	▸ CI/CD 파이프라인을 통한 코드 배포 매메커니즘 보유 ▸ 테스트 및 생산 환경 인프라 제공	▸ 배포되는 애플리케이션에 대한 정기적인·자동화된 시험을 사용하여, 개발·배포 과정에서 애플리케이션 보안 테스트 통합	▸ 자동화된 코드 배포 및 관리자 권한 접근 제거 ▸ 공급망 손상이 있는 것으로 식별된 모든 소프트웨어를 격리·관리
소프트웨어·애플리케이션 보안	▸ 주로 정적·수동 검사 방법을 통해, 배포 전 애플리케이션 보안 테스트 수행	▸ 동적 시험 방법 사용을 포함하여, 애플리케이션 개발 및 배포 과정에 애플리케이션 보안 테스트 통합 ▸ DevSecOps적용 ▸ SBOM 제공	▸ 프로세스 전반에 걸친 SBOM 제공 ▸ 모든 소프트웨어에 대해 가능한 한 최대한 검증 프로세스 구현	▸ 소프트웨어를 개발 조직 프로세스 격리와 마이크로 세그멘테이션 적용 ▸ 런타임 소프트웨어를 포함한 자동화된 소프트웨어 검증
가시성 및 분석	▸ 외부 센서 및 시스템과 격리된 상태에서 애플리케이션 상태 및 보안 모니터링 수행	▸ 일부 외부 센서와 시스템을 사용하여 컨텍스트 관점에서, 애플리케이션 상태 및 보안 모니터링 수행	▸ 휴리스틱 기반 분석 및 보안 모니터링 자동화	▸ 외부 센서와 시스템을 사용하여 지속적이고 동적인 애플리케이션 상태 및 보안 모니터링 수행
자동화 및 통합	▸ 애플리케이션 제공 시, 애플리케이션 호스팅 위치와 접근 설정	▸ 변경된 상태를 기기와 네트워크 구성 요소에 알림	▸ 자동화된 상태 변화 전송	▸ 보안과 성능 최적화를 위한 지속적인 환경 변화에 적응

바. 데이터

'데이터' 핵심 요소의 경우 5가지 기능(데이터 목록 관리, 접근 결정 방법, 데이터 암호화, 데이터 분류, 데이터 손실 방지)이 있으며, 교차 역량(가시성 및 분석, 자동화 및 통합)을 반영한 표는 아래와 같다.

표 3-9 데이터 핵심 요소에 대한 제로트러스트 성숙도 모델

기능	기존	초기	향상	최적화
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	‣ 데이터 목록 자동화 및 데이터 사용 패턴 분석 기술 적용	‣ 강력한 태그 작업 및 추적으로 지속적인 목록 작업. 기계 학습 모델을 사용하여 분류 강화
접근 결정 방법	‣ 정적 접근제어를 사용하여 데이터 접근 관리	‣ 최소한의 권한 요소 등을 통합한 데이터 접근	‣ 식별자, 기기 위험도 및 기타 속성을 고려하는 최소 권한 제어 기법을 사용하여 데이터 접근 관리	‣ 데이터 접근은 적시·최소권한 원칙 및 지속적인 위험기반 결정을 지원하며, 동적으로 이루어짐
데이터 암호화 (가이드라인 1.0의 암호화)	‣ 온프레미스 데이터 저장소에 암호화되지 않은 상태로 데이터 저장	‣ 클라우드 혹은 원격 환경에서 암호화 저장	‣ 저장소의 모든 데이터 암호화	‣ 사용 중인 데이터 암호화 ‣ 조직 차원의 안전한 키 관리를 위한 최소 권한 원칙 ‣ 최신 표준을 사용한 암호화 적용 및 암호 민첩성 ‣ DRM과 AI 기반 기술 통합[8]
데이터 분류	‣ 제한된 임시 데이터 분류 ‣ 데이터 태깅 및 라벨링 표준 정의	‣ 정의된 레이블 및 수동 메커니즘을 통한 데이터 분류	‣ 단순화·구조화된 형식을 통한 데이터 분류 ‣ 레이블 지정 프로세스 계층화 및 일부 자동화	‣ 데이터 분류 및 레이블 지정 자동화 ‣ 데이터 태깅 및 라벨링에 대한 분석 수행 자동화
데이터 손실 방지	‣ DLP 솔루션을 배포하기 위한 범위 지정 ‣ 민감한 데이터를 식별하는 기술이 확립	‣ DLP 솔루션은 검사 적용 지점에 배포 ‣ DLP 솔루션은 모니터링 수준으로 활용	‣ DLP 솔루션 결과 분석, 정책 미세 조정을 통한 관리 ‣ DLP 솔루션을 통하여 데이터 유출 방지	‣ 자동화된 데이터 모니터링을 통해 추가 DLP 배포에 대한 누락된 시행 지점 식별 ‣ 자동화된 데이터 태그를 활용하여 민감한 데이터 식별
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	‣ 자동화된 분석 및 상관관계 분석, 예측 분석 등의 기능 사용	‣ 데이터는 목록화되어 언제든지 관리 가능 ‣ 의심스러운 행위에 대한 모든 접근 이벤트 로그 및 분석 ‣ 암호화된 데이터에 분석 수행
자동화 및 통합	‣ 자동화 및 통합을 어렵게 하는, 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	‣ 일관되고 계층화된 방식의 자동화	‣ 높은 가치의 데이터에 대한 엄격한 접근제어 자동 집행 ‣ 높은 가치의 데이터는 모두 저장 위치에 관계없이 백업됨 ‣ 데이터 목록은 자동으로 업데이트

8 AI 기술은 데이터의 비정상적인 사용을 탐지하고 경고하는데 활용될 수 있으며, 이때 DRM에 걸린 권한을 자동으로 변경한다거나 키를 변경하는 등의 기술 통합을 통한 대응도 가능할 수 있음

| 제2절 |

제로트러스트 성숙도 모델 기반 보안 세부역량

제로트러스트의 도입과 아키텍처 설계에 있어 성숙도 모델의 활용은 매우 중요하지만, 개념적으로 정의된 현재의 제로트러스트 성숙도 모델은 여전히 고수준에서 머물러 있다. 기업의 보안 담당자들이 제로트러스트를 조직에 이를 실질적으로 도입하는 과정에서 제로트러스트 성숙도 모델이 갖는 모호성과 추상성 때문에 제로트러스트의 원칙을 명확히 이해하고 구체적인 정책이나 기술적 구현으로 전환하는 데 큰 어려움을 초래한다.

이 때문에 현재는 대부분 성숙도 모델을 기업의 보안 수준을 평가하는 도구의 역할로 활용하는데 머물러 있다. 예를 들어, 준비 단계에서 초기 단계로의 전환 시 요구되는 세부적인 기술적 요건이나, 기업의 어떤 부분에 집중적으로 자원을 투입해야 하는지에 대한 구체적인 지침이 있어야 하지만 기존의 제로트러스트 성숙도 모델이 단계별로 제시하는 보안 조치들은 일반적인 권고사항 수준에서 끝나는 경우가 많다. 각 단계에서 구체적으로 어떤 기술을 도입하고, 어떤 절차를 마련해야 하는지에 대한 가이드가 부족하다면 기업 내 제로트러스트 구현이 체계적이고 일관되게 진행되지 못할 가능성이 크다.

이 때문에 정보보호 담당자들은 막연한 목표를 가지고 많은 시행착오를 겪게 되며, 기업 내에서 제로트러스트 모델을 성공적으로 구현하는 데 필요한 시간과 자원이 과도하게 소모될 수 있다.

따라서, 제로트러스트 성숙도 모델은 단순한 평가 도구에서 벗어나, 정보보호 담당자들이 이를 기반으로 실질적인 보안 전략을 세울 수 있도록 더욱 세부적이고 구체적인 정의가 필요하다. 각 단계별로 요구되는 기술적 요건과 절차적 요소들을 명확하게 제시하고, 기업의 특성과 상황에 맞게 이를 어떻게 적용할 수 있는지에 대한 구체적인 예시와 사례가 필요하다. 또한, 성숙도 모델을 따르는 과정에서 예상되는 도전과 이를 극복하기 위한 전략들까지 포함하여 보다 실질적이고 실무적인 가이드라인을 제공함으로써, 정보보호 담당자들이 제로트러스트의 원칙을 효과적으로 기업에 구현할 수 있도록 도와야 한다.

미 국방부는 제로트러스트 참조 아키텍처 및 전략, 로드맵 문서에서 제로트러스트 역량(Capability)[9]을 제시하고 있으며, 이는 앞에서 언급한 〈표 3-4〉부터 〈표 3-9〉까지 정의한 기능 및 CISA 성숙도 모델에서 제안하는 기능(Function)과는 개념이 다소 다르다.

이들을 고려하여, 본 문서에서는 제로트러스트 성숙도 모델의 모호성과 추상성을 극복하고 정보보호 담당자들이 더 명확하고 구체적인 지침을 따를 수 있도록 세부역량(Capability)을 제안한다. 세부역량은 소프트웨어·하드웨어 구현까지 고려하여 구체적으로 정의를 내리는 것이 적절하며, 이렇게 구체적 정의 과정을 통하여 기존 성숙도 모델이 가지는 기능이 추상적으로 정의가 되어있는 한계를 보완할 수 있다. 즉, 세부역량을 구체화하는 과정에서 구체적인 정의와 실행 방안을 포함하게 되며 이를 통해 성숙도 모델을 보다 실질적이고 적용 가능한 프레임워크로 전환할 수 있을 것이다.

따라서, 본 문서에서의 세부역량을 활용하면 다양한 보안 요소와 기술적 요건을 명확히 정의하고, 각 요소가 기업의 특정 보안 목표를 달성하기 위해 어떻게 활용될 수 있는지에 대해 상세하게 설명할 수 있다. 이를 통해 정보보호 담당자들은 각 성숙도 단계에서 필요한 구체적인 보안 조치와 기술적 요구사항을 명확히 이해할 수 있으며, 기업 내에서 제로트러스트를 체계적이고 효과적으로 구현하는 데 필요한 실질적인 전략을 수립할 수 있다. 이는 궁극적으로 정보보호 담당자들이 제로트러스트 원칙을 더욱 정확하게 이해하고, 이를 조직 내에서 성공적으로 구현하는 데 큰 도움이 될 것이다. 제로트러스트 성숙도 모델 2.0에서 각 핵심 요소별로 가지는 기능 및 그에 따르는 세부역량을 요약하면 [그림 3-3]과 같으며, 〈표 3-10〉에서는 연계표의 형태로 정리하였다.

---

9 미 국방부에서 발간한 제로트러스트 참조 아키텍처에서의 산출물은 국방부 아키텍처 프레임워크(DoDAF)에서 유래한다고 언급되어 있다. 즉, 이는 제로트러스트 참조 아키텍처에 사용된 다이어그램, 모델, 설계 청사진 등이 DoDAF의 표준을 따름을 의미하는데, 그에 비추어 용어 역시 DoDAF의 용어를 따른다고 볼 수 있을 것이다. DoDAF에서의 역량(Capability)은 '일련의 작업을 수행하기 위한 수단과 방법의 조합을 통해 지정된 표준과 조건에서 원하는 효과를 달성할 수 있는 능력'으로 정의가 되어 있으며, 본 가이드라인의 세부역량에 대해서도 유사한 관점으로 정의하는 것이 적절하다.

그림 3-3 제로트러스트 성숙도 모델 2.0에서 제시한 기능 및 세부역량

표 3-10 제로트러스트 성숙도 모델 2.0 핵심요소, 기능, 세부역량 연계표

핵심요소	기능	세부역량
1. 식별자·신원	1.1 식별자 관리	1.1.1 사용자 인벤토리 1.1.2 ID 연계 및 사용자 자격 증명
	1.2 인증	1.2.1 다중인증 (MFA) 1.2.2 지속 인증
	1.3 위험도 평가	1.3.1 통합 ICAM 플랫폼 1.3.2 행동, 컨텍스트 기반 ID 및 생체 인식
	1.4 접근관리	1.4.1 조건부 사용자 접근 1.4.2 최소 권한 접근
2. 기기 및 엔드포인트	2.1 정책 준수 모니터링	2.1.1 기기 감지 및 규정 준수
	2.2 데이터 접근제어	2.2.1 실시간 검사를 통한 기기 권한 부여
	2.3 자산관리	2.3.1 기기 인벤토리 2.3.2 통합 엔드포인트 관리 및 모바일 기기 관리
	2.4 기기 위협 보호	2.4.1 엔드포인트 및 확장된 탐지·대응 (EDR 및 XDR) 2.4.2 자산, 취약성 및 패치 관리 자동화
3. 네트워크	3.1 네트워크 세분화	3.1.1 매크로 세그멘테이션 3.1.2 마이크로 세그멘테이션 3.1.3 소프트웨어 정의 네트워킹
	3.2 위협 대응	3.2.1 위협 대응
	3.3 트래픽 암호화	3.3.1 트래픽 암호화
	3.4 트래픽 관리	3.4.1 데이터 흐름 매핑
	3.5 네트워크 회복성	3.5.1 네트워크 회복성
4. 시스템	4.1 접근통제	4.1.1 접근통제
	4.2 시스템 계정 관리	4.2.1 PAM 4.2.2 자격 증명 관리
	4.3 네트워크 분리 정책	4.3.1 네트워크 세분화 및 그룹 간 이동
	4.4 시스템 보안 및 정책 관리	4.4.1 시스템 환경에 따른 정책 관리
5. 애플리케이션 및 워크로드	5.1 애플리케이션 접근	5.1.1 리소스 권한 부여 및 통합
	5.2 애플리케이션 위협 보호	5.2.1 지속적인 모니터링 및 진행 중인 승인
	5.3 접근 가능한 애플리케이션	5.3.1 원격 접속
	5.4 안전한 애플리케이션 배포	5.4.1 안전한 애플리케이션 배포 5.4.2 애플리케이션 인벤토리
	5.5 소프트웨어·애플리케이션 보안	5.5.1 안전한 소프트웨어 개발 및 통합 5.5.2 소프트웨어 위험 관리

핵심요소	기능	세부역량
6. 데이터	6.1 데이터 목록 관리	6.1.1 데이터 카탈로그 위험 정렬 6.1.2 기업 데이터 거버넌스
	6.2 접근 결정방법	6.2.1 데이터 접근제어
	6.3 데이터 암호화	6.3.1 데이터 암호화 및 권한 관리
	6.4 데이터 분류	6.4.1 데이터 라벨링 및 태그 지정
	6.5 데이터 손실 방지	6.5.1 데이터 손실 방지 (DLP) 6.5.2 데이터 모니터링 및 감지
7. 가시성 및 분석 (공통)		7.1 모든 관련 활동 기록 7.2 중앙집중적 보안 정보 및 이벤트 관리 7.3 보안 위협 분석 7.4 사용자 및 기기 동작 분석 7.5 위협 인텔리전스 통합 7.6 자동화된 동적 정책
8. 자동화 및 통합 (공통)		8.1 정책 통합 8.2 중요 프로세스 자동화 8.3 인공지능 8.4 보안 통합, 자동화 및 대응 8.5 데이터 교환 표준화 8.6 보안 운영 조정 및 사고 대응

단, 여기에서 정의하는 제로트러스트 관점의 세부역량에 대하여 주의할 점은 다음과 같다. 첫째, 여기에서 정의하는 세부역량은 절대적으로 따라야 할 지침으로 이해하는 것은 곤란하며, 참고할 수 있는 모델로 인식하여야 한다. 각 기업은 여기에서 정의한 세부역량과 성숙도 수준에 따르는 정의를 참고하되, 각 기업의 상황을 고려하여 어떤 세부역량을 어떤 수준으로 도입할지 정하는 것이 바람직하다.

둘째, 기업망 핵심 요소에 대한 교차 기능으로 정의한 '가시성 및 분석'과 '자동화 및 통합'에 대하여 여기에서는 별도의 핵심 요소로 표현하였다. 이는 보안 세부역량을 구체화할 때 실제 기술·솔루션 구현을 고려하여야 하기 때문이다. 기능으로 접근할 때에는 이들을 각 기업망 핵심 요소 안에서 교차 기능으로 정의하여 기술하는 것이 적절하나, 이를 구체화하기 위하여 실제 제로트러스트 도입 및 기술 개발 과정에서 독립적으로 요구되는 세부역량으로 정의하고자 하는 접근 철학을 반영한 것이다. 이 접근은 네트워크, 자산, 인증 정보 등 다양한 보안 데이터를 일관성 있게 수집하고, 이를 통합적으로 분석하며 자동화된 방식으로 보안 관리 및 대응을 가능하게 하는 데 중점을 둘 수 있다.

1. 식별자·신원

가. 식별자 관리

식별자 관리는 제로트러스트 보안의 출발점이다. 기업은 모든 사용자의 신원을 정확하게 파악하고 관리하는 것이 기본이기 때문에, 사용자 인벤토리와 ID 연계 세부역량을 우선적으로 도입해야 한다. 자격 증명은 사용자의 신원을 확인하는 핵심적인 요소로서, 적절한 방식으로 자격 증명을 관리하지 않으면 보안이 근본적으로 약화된다. 이 단계에서의 목표는 기업 내에서 모든 사용자를 신뢰할 수 있도록 식별을 명확히 하고, 여러 시스템 간의 통합된 신원 관리를 통해 일관성을 유지하는 것이다.

표 3-11 식별자·신원 핵심 요소의 식별자 관리 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
사용자 인벤토리	사용자 인벤토리는 시스템에 접근하는 모든 사용자와 그들의 권한을 기록하고 관리하는 시스템이다. 이 기능은 사용자에 대한 정확하고 최신 정보를 제공하여 적절한 접근제어를 가능하게 한다.	기존	‣ 사용자 목록을 수집하고 기록하기 시작 ‣ 기본적인 사용자 정보 관리 및 문서화
		초기	‣ 사용자의 역할 및 권한을 포함한 상세 인벤토리 구축 ‣ 주기적인 검토와 업데이트 절차 설정
		향상	‣ 자동화된 인벤토리 관리 도구 도입을 통한 사용자 데이터 정확성 보장 ‣ ID 통합 관리 시스템을 구축 ‣ 비정상적인 사용자 활동 탐지 기능 추가
		최적화	‣ 인벤토리 통합을 통한 기업 전반의 사용자 및 권한 관리 최적화 ‣ 인공지능 기반 분석을 수행하여 사용자 행동 예측 및 대응 전략 강화
ID 연계 및 사용자 자격 증명	여러 시스템 간의 사용자 자격 증명과 인증을 통합하는 프로세스로, 처음에는 ID 생명주기 관리(ILM) 프로세스를 표준화하고, 표준 조직 IDP 솔루션과 통합하는 데 초점을 맞춘다. 이를 완료한 후, 단일 솔루션이나 ID 연계(Federation)를 통해 기업용 ILM 프로세스·솔루션을 구축하는 것으로 전환된다.	기존	‣ 기본적인 ID 연계 솔루션을 설정 및 자격 증명 통합 시작 ‣ 중앙에서 사용자 인증 정보 관리
		초기	‣ 여러 시스템 간 자격 증명 연동으로 사용자 경험 통합 ‣ 기업 내외부 시스템과의 연동 강화
		향상	‣ 다양한 ID 제공자 통합을 통한 ID 연계 확대 ‣ 보안 프로토콜 강화로 데이터 보호 개선
		최적화	‣ 글로벌 수준의 ID 연계 구현을 통한 통합 사용자 경험 제공 ‣ ID 연계 정책 및 프로세스의 지속적인 최적화

나. 인증

기업의 보안 강도를 더욱 높이기 위해 다중인증(MFA)과 지속 인증 세부역량을 도입한다. 단일 인증 방식은 공격자가 쉽게 타겟으로 삼을 수 있으므로, 사용자에게 추가적인 인증 방법을 요구하는 MFA는 필수적이다. 지속 인증은 사용자가 처음 인증을 받은 후에도, 시스템이 지속적으로 그들의 신원을 확인하는 방식으로 보안을 강화한다.

표 3-12 식별자·신원 핵심 요소의 인증 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
다중인증 (MFA)	사용자가 시스템에 접근하기 위해 두 개 이상의 인증 방법을 요구하는 보안 조치로, 중앙집중적 사용자 관리를 가능하게 하기 위해 MFA와 식별자 제공자(Identity Provider)를 도입하는 데 초점을 맞춘다. 성숙도 수준이 높아짐에 따라 대체 가능하고 유연한 MFA 방식을 적용하여 내부 사용자와 외부 사용자에게 접근을 제공하는데 사용될 수 있도록 한다.	기존	‣ 기본적인 패스워드 방식과 함께 MFA 도입 및 설정 (예: SMS 코드, 이메일 확인) ‣ MFA 지원 시스템 구축
		초기	‣ 다양한 MFA 방법 구현으로 보안 수준 강화 (예: 인증 앱, 하드웨어 토큰) ‣ MFA 정책 표준화 및 적용 ‣ FIDO 기반 인증 기법 적용
		향상	‣ 상황에 맞춘 맞춤형 MFA 기능 제공 및 새로운 인증 방법 지속 도입 ‣ MFA 절차 자동화 및 사용자 경험 최적화 ‣ 컨텍스트 기반 ID 인증 방식 채택
		최적화	‣ 비정상적인 로그인 시도 실시간 탐지 및 대응 ‣ MFA 기반 고급 보안 정책 설정 ‣ 이상 행위 발생 시 자동 재인증 요구 등 지속적 신원 검증 수행
지속 인증	제로트러스트가 도입되면 지속적인 속성 기반 인증(Continuous Attribute-Based Authentication)으로 체계적으로 이동할 것이다. 초기에는 기존의 단일 인증을 기업에서 승인한 IDP와 사용자 및 그룹을 기준으로 표준화하는 데 초점을 맞추고, 둘째 단계에서는 시간 기반의 규칙 기반 인증을 추가하며, 궁극적으로 애플리케이션·소프트웨어 활동 및 요청된 권한에 기반한 지속 인증으로 발전하게 된다.	기존	‣ 세션 기반 인증 ‣ 사용자 행동 및 접속 상태 모니터링
		초기	‣ 모니터링을 통한 이상행위 탐지 및 추가 인증 요구 ‣ 사용자 세션 중 추가 인증 요구 시스템 도입
		향상	‣ 동적 인증 기술 적용으로 실시간 인증 상태 조정 ‣ 지속 인증을 위한 고급 분석 및 경고 기능 통합
		최적화	‣ 이상 행위 탐지 시 세션 종료 또는 재인증 요구 등 동적 자동 인증 상태 조정

다. 위험도 평가

위험도 평가는 보안 수준을 한층 더 강화하는 것을 목표로 한다. 다양한 데이터와 행동 패턴을 기반으로, 사용자의 신뢰도를 실시간으로 평가하는 것이다. 통합 ICAM 플랫폼을 통해 기업은 ID 관리와 접근 관리를 통합적으로 처리하며, 행동, 상황적 ID 및 생체 인식과 같은 고도화된 기술을 도입해 사용자의 행동 패턴을 분석하고, 상황에 따라 더 정밀하게 보안을 적용할 수 있다.

표 3-13 식별자·신원 핵심 요소의 위험도 평가 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
통합 ICAM 플랫폼	통합 ICAM 플랫폼은 식별자, 자격 증명, 접근 관리 기능을 중앙에서 통합하여 관리하는 시스템이다. 기업 수준의 식별자 관리 및 공개키 인프라(PKI) 시스템을 활용하여 네트워크 전반에 걸쳐 사용자, 관리자 및 비인간개체 식별자를 추적하고, 접근이 필요한 자와 적절한 권한을 가진 자로 제한되도록 보장하여야 한다. 기업은 자격 증명 관리 시스템, 식별자 거버넌스 및 관리 도구, 접근 관리 도구를 통해 접근권한이 필요하고 적절한지 검증하여야 한다.	기존	‣ 기본적인 ICAM 시스템 구축 및 주요 기능 통합 ‣ 초기 사용자 및 권한 관리 설정 ‣ 위험도 평가가 적용되지 않은 사용자 권한 관리
		초기	‣ ICAM 시스템 기능 확장 및 중앙 집중형 관리와 모니터링 구현 ‣ 사용자 인증 및 접근 관리 정책 표준화 ‣ 사용자 및 권한 관리에 대한 기본적인 위험도 평가 도입
		향상	‣ 다양한 보안 기술 및 시스템 통합으로 ICAM 플랫폼 강화 ‣ 고급 분석 및 자동화 기능 도입으로 ICAM 최적화 ‣ 다양한 사용자 그룹과 역할에 따른 고도화된 위험도 평가 적용
		최적화	‣ AI 기반 ICAM 플랫폼을 통한 실시간 보안 강화 ‣ 통합 ICAM 솔루션을 통해 보안 정책과 절차 지속 개선 및 최적화 ‣ AI 기반의 실시간 위험도 평가로 모든 사용자 권한 관리 최적화
행동, 컨텍스트 기반 ID 및 생체 인식	사용자의 행동 패턴, 컨텍스트, 생체 데이터를 활용하여 인증 및 접근제어를 강화하는 기술이다. 기업 IDP를 활용하여 기본 사용자 속성으로 사용자 및 개체 행동 분석(UEBA)을 활성화 한다. UEBA를 PAM 및 적시/최소권한접근(JIT/JEA) 시스템과 통합하여 이상 행위 및 악의적인 활동을 보다 효과적으로 탐지할 수 있다.	기존	‣ 기본적인 생체 인식 기술 도입 (예: 지문, 얼굴 인식) ‣ 사용자 행동 패턴 기록 및 수동 분석 시작
		초기	‣ 행동 및 생체 인식 기술 통합으로 인증 절차 강화 ‣ 컨텍스트 기반 접근권한 조정
		향상	‣ 고급 행동 분석 및 생체 인식 기술을 통한 인증 정확도 향상 ‣ 실시간 사용자 행동 및 컨텍스트 변화 반영으로 접근제어 조정
		최적화	‣ AI 기반 행동 분석 및 생체 인식 솔루션을 통한 고도화된 보안 제공 ‣ 새로운 기술 도입을 통한 인증 절차 지속 최적화

라. 접근 관리

접근 관리에서는 조건부 사용자 접근과 최소 권한 접근과 같은 보안 기능이 적용된다. 조건부 사용자 접근은 사용자가 접속하는 위치, 시간, 기기 상태 등을 고려해 접근을 동적으로 허용하거나 차단하는 기능으로, 실시간 보안 제어가 가능하다. 최소 권한 접근은 모든 사용자가 업무에 필요한 최소한의 권한만 부여받도록 하여, 기업망 전체의 공격 표면을 줄이는 방식이다.

표 3-14 식별자·신원 핵심 요소의 접근 관리 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
조건부 사용자 접근	사용자의 위치, 기기 상태, 시간대 등 다양한 조건에 따라 접근권한을 동적으로 조정하는 기능이다. ICAM 전반에 걸친 전통적인 역할 기반 접근제어에서 시작하여, 애플리케이션 중심의 역할로 확장되며, 궁극적으로는 동적 접근 규칙을 제공하기 위해 기업 속성을 활용한다.	기존	‣ 조건부 접근 정책의 기본 개념 정의 및 구현 ‣ 사용자 활동 및 조건 수집을 위한 기초 시스템 구축 ‣ 시스템별 개별 접근 관리 기능 보유
		초기	‣ 통합 관리 기능 및 정책 기반 특정 조건에서 사용자 접근제어 ‣ 시간 및 위치 기반 접근제어를 통해 최소 권한 원칙 적용
		향상	‣ 정교한 조건과 규칙을 활용한 다단계 접근 정책 구현 ‣ 조건에 따른 실시간 접근 결정 자동화 ‣ 세션별 별도의 접근 지원
		최적화	‣ 고급 분석 및 ML을 활용한 사용자 행동과 환경 기반 정교한 조건부 접근 제공 ‣ 동적 접근 정책을 실시간으로 조정 및 최적화
최소 권한 접근	사용자가 수행하는 작업에 필요한 최소한의 권한만 부여하여, 타 리소스 및 워크로드에 대한 접근을 제한하는 방식이다. 이를 통하여 리소스 탈취 등을 최소화할 수 있다.	기존	‣ 최소 권한 원칙 정의 및 적용 가능한 시스템 구축 ‣ 권한 부여 절차 문서화 및 시작
		초기	‣ 권한 부여 절차 표준화 및 역할 기반 권한 부여 ‣ 권한 요청 및 변경 관리 시스템 도입
		향상	‣ 권한 요청 및 사용에 대한 자동화된 모니터링과 분석 구현 ‣ 권한 관리 정책 지속적 검토 및 업데이트
		최적화	‣ 권한 관리 정책 동적 변경 및 최소 권한 부여 구현 ‣ 최소 권한 원칙 전사적 적용 및 실시간 조정

2. 기기 및 엔드포인트

가. 정책 준수 모니터링

기업 내 기기들이 보안 정책을 준수하고 있는지 모니터링하는 기능을 도입한다. 기기 감지 및 규정 준수는 네트워크에 연결된 모든 기기를 탐지하고, 보안 규정을 준수하는지 확인해 정책 위반을 예방하는 것이 핵심이다.

표 3-15 기기 및 엔드포인트 핵심 요소의 정책 준수 모니터링 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
기기 감지 및 규정 준수	네트워크에 연결된 기기가 기업 보안 규정을 준수하는지 확인하고, 비준수 기기를 탐지하여 경고하는 시스템이다.	기존	‣ 기기 감지 기능을 구축하여 리소스에 연결된 기기를 식별 ‣ 초기 규정 준수 요구 사항을 설정하고, 수동으로 준수 여부를 확인
		초기	‣ 자동화된 감지 시스템을 도입하여 실시간으로 기기를 탐지하고 규정 준수를 평가 ‣ 비준수 기기에 대한 경고 및 접근 제한 기능 설정
		향상	‣ 규정 준수 평가를 정교화하여 다양한 규정 기준을 적용 ‣ 자동으로 교정 조치를 취할 수 있는 기능 추가 ‣ 규정 준수 상태를 지속적으로 모니터링하고, 규정 준수에 따른 접근권한 부여
		최적화	‣ AI를 활용하여 기기 규정 준수 평가를 최적화하고, 실시간으로 조치 자동화 ‣ 규정 준수 데이터와 보안 분석을 통합하여 기기 보안 강화 ‣ 규정 준수 여부에 따라 동적으로 권한 수정

나. 데이터 접근제어

기기가 리소스에 접근할 때, 실시간으로 검사를 진행해 그 기기에 권한을 부여한다. 실시간 검사를 통한 기기 권한 부여 기능을 통해 기기가 정상적인 상태에서만 네트워크와 데이터에 접근할 수 있도록 하여, 보안 위협을 미연에 방지한다.

표 3-16 기기 및 엔드포인트 핵심 요소의 데이터 접근제어 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
실시간 검사를 통한 기기 권한 부여	기기가 네트워크에 접근하기 전에 보안 상태를 평가(NextGen AV, AppControl, FIM 등 이용)하고, 안전한 기기만 접근을 허용하는 기능이다.	기존	‣ 자산 접근 기기 정보 수집 계획 수립 ‣ 초기 보안 기준 설정
		초기	‣ 기본적인 보안 검사 프로세스를 수립하여 기기가 자산에 접근하기 전에 수동 검사를 시행
		향상	‣ 실시간 보안 검사 도구를 도입하여 기기의 상태를 자동으로 평가 ‣ 보안 기준을 충족하는 기기만 접근을 허용 ‣ 검사를 통과하지 못한 기기에 대해 접근 제한을 설정
		최적화	‣ 실시간 검사를 고도화하여 보다 정교한 보안 기준을 적용하고, 기기의 보안 상태를 지속적으로 평가 ‣ 보안 상태에 따라 실시간으로 기기 접근권한 조정 ‣ AI 기반의 실시간 보안 검사 시스템을 통해 기기의 보안 상태를 자동으로 평가하고, 실시간으로 대응 ‣ 실시간 검사를 다른 보안 시스템과 통합하여 종합적인 기기 보안 전략을 구현

다. 자산 관리

소유하거나 사용하는 모든 기기를 관리하는 것은 기업 입장에서 매우 중요하다. 기기 인벤토리를 통해 자산 목록을 체계적으로 관리하며, 통합 엔드포인트 관리(UEM) 및 모바일 기기 관리(MDM) 기능을 통해 모든 엔드포인트 기기를 일괄적으로 관리하고 보안을 유지한다.

표 3-17 기기 및 엔드포인트 핵심 요소의 자산 관리 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
기기 인벤토리	모든 기기의 목록을 작성하고 관리하는 시스템이다. 이는 기업 보안을 위해 모든 기기의 상태, 소유자, 위치 등을 정확히 파악할 수 있게 해준다. 기기 속성에는 PKI(802.1x) 시스템 인증서, 기기 개체, 패치·취약성 상태 등을 확인할 수 있는 기술 세부 정보가 포함된다.	기존	‣ 기본 인벤토리를 작성하고 수동으로 업데이트 ‣ 주요 기기의 정보를 수집하고 관리
		초기	‣ 자동화된 기기 인벤토리 시스템을 도입하여 보유한 모든 기기를 실시간으로 기록 ‣ 기기 유형, 운영체제, 위치 등의 세부 정보를 포함한 정교한 인벤토리 구축
		향상	‣ 기기 인벤토리를 지속적으로 업데이트 ‣ 비정상적이거나 승인되지 않은 기기를 탐지하는 기능 추가 ‣ 인벤토리 데이터를 분석하여 보안 취약점을 파악하고 대응 전략 마련
		최적화	‣ AI 기반의 인벤토리 관리 솔루션을 활용하여 기기 인벤토리를 자동화하고 최적화 ‣ 실시간 모니터링 및 예측 분석을 통해 기기 보안을 강화
통합 엔드포인트 관리 및 모바일 기기 관리	모든 엔드포인트와 모바일 기기를 중앙에서 통합 관리하고, 보안을 유지하는 기능이다. 이는 원격으로 관리될 수 있어야 하며, 보안 정책을 적용할 수 있어야 한다.	기존	‣ 기본적인 엔드포인트 및 모바일 기기 관리 시스템을 도입하여 주요 기기를 관리 ‣ 초기 보안 정책 설정
		초기	‣ 엔드포인트 및 모바일 기기의 보안 설정을 중앙에서 관리하고, 보안 업데이트를 자동으로 배포 ‣ 기기 상태를 지속적으로 모니터링하여 보안을 유지
		향상	‣ 모든 엔드포인트와 모바일 기기의 보안을 중앙에서 통합 관리하고, 고급 보안 정책 적용 ‣ 실시간 모니터링 및 위협 탐지 기능을 추가하여 보안 강화
		최적화	‣ AI 기반 엔드포인트 및 모바일 기기 관리 솔루션을 통해 보안 최적화 및 실시간 대응 ‣ 모든 기기 보안을 중앙에서 통합적으로 관리하고, 자동화된 위협 대응 구현

라. 기기 위협 보호

기기의 위협을 실시간으로 탐지하고 대응하는 고도화된 보안 기능을 도입한다. 엔드포인트 및 확장된 탐지 및 대응(EDR 및 XDR)은 기기에 대한 위협을 신속하게 탐지하고 처리하며, 자산, 취약성 및 패치 관리 자동화를 통해 보안 업데이트와 취약성 관리를 자동으로 수행해 보안성을 강화한다.

표 3-18 기기 및 엔드포인트 핵심 요소의 기기 위협 보호 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
엔드포인트 및 확장된 탐지·대응 (EDR 및 XDR)	엔드포인트와 확장된 영역에서 실시간으로 위협을 탐지하고 대응하는 고급 보안 솔루션으로 이를 이용하여 엔드포인트의 이상 행위를 탐지해야 한다.	기존	‣ 기본적인 EDR 솔루션을 도입하여 엔드포인트 위협을 탐지하고 대응 ‣ 초기 위협 탐지 및 대응 정책 설정
		초기	‣ EDR 시스템을 고도화하여 실시간 위협 탐지 및 자동 대응 구현
		향상	‣ XDR 솔루션을 도입하여 네트워크 전반에 걸친 위협 탐지 확대 ‣ 고급 분석 및 ML을 통합하여 위협 탐지 정확도 향상
		최적화	‣ AI 기반의 EDR·XDR 솔루션을 통해 실시간으로 모든 기기에 대한 위협을 탐지하고 자동화된 대응 구현 ‣ 위협 인텔리전스를 통합하여 예측 분석 및 사전 대응 전략 수립
자산, 취약성 및 패치 관리 자동화	네트워크에 연결된 모든 기기의 보안 취약점을 관리하고, 최신 보안 패치를 자동으로 적용하는 기능이다.	기존	‣ 자산 및 취약성을 수동으로 평가하고 패치를 수동으로 적용하는 프로세스 수립 ‣ 주요 자산 및 취약성 목록 작성
		초기	‣ 자동화된 취약성 평가 및 패치 관리 도구를 도입하여 주요 자산의 보안 강화 ‣ 취약성 발견 시 자동으로 패치를 적용하는 시스템 구축
		향상	‣ 모든 자산에 대해 지속적인 취약성 평가 및 패치 관리 자동화 ‣ 취약성 및 패치 관리 시스템을 다른 보안 시스템과 통합하여 종합적인 보안 관리 전략 구현
		최적화	‣ AI 기반의 예측 분석을 활용하여 취약성을 사전에 식별하고, 자동으로 패치 적용 ‣ 자산 관리, 취약성 평가, 패치 관리를 통합하여 실시간으로 보안 최적화

3. 네트워크

가. 네트워크 세분화

네트워크를 세분화하여 각 영역에 맞는 보안을 적용하는 것이 목표다. 매크로 세그멘테이션은 네트워크를 큰 단위로 나누어 각 구역 간의 보안을 강화하는 방법이다. 이는 대규모 네트워크에서 쉽게 적용 가능하며, 내·외부 네트워크를 분리해 보안을 강화하는 데 유용하다. 마이크로 세그멘테이션은 네트워크를 더욱 세부적으로 나누어 각 구역을 더 세밀하게 보호한다. 이는 내부 위협에 대응하는 데 효과적이며, 세부적으로 제어된 보안 정책을 적용할 수 있게 한다. 소프트웨어 정의 네트워킹(SDN)은 클라우드 환경 등에서 네트워크의 트래픽을 소프트웨어로 관리하여, 더욱 유연하고 효율적인 보안 정책을 적용할 수 있도록 돕는다. 이를 통해 네트워크 상의 모든 트래픽을 중앙에서 통제하고, 세밀한 보안 제어를 가능하게 한다.

표 3-19 네트워크 핵심 요소의 네트워크 세분화 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
매크로 세그멘테이션	매크로 세그멘테이션은 네트워크를 대규모 세그먼트로 나누어 주요 보안 영역을 구분하는 기술이다. 이는 네트워크 전체를 보호하는 데 필요한 보안 경계를 설정하는 데 사용된다.	기존	‣ 네트워크를 주요 비즈니스 영역별로 분할하여 기본적인 매크로 세그먼트 설정 ‣ 네트워크 내 주요 자산과 트래픽 흐름을 기반으로 매크로 세그먼트 구성
		초기	‣ 매크로 세그먼트를 확장하여 각 세그먼트 간에 보안 정책 적용 ‣ 경계를 강화하고, 세그먼트 간의 트래픽을 모니터링 및 비정상적인 활동 탐지
		향상	‣ 매크로 세그먼트를 보다 세분화하여 보안 관리 정밀도 향상 ‣ 각 세그먼트에 맞춤형 보안 정책 적용 ‣ 매크로 세그먼트 간의 트래픽을 자동으로 조정 및 보안 위협에 신속 대응
		최적화	‣ AI 기반 매크로 세그먼트 관리 도구 사용 ‣ 실시간 세그먼트 간 트래픽 분석 및 자동 대응 ‣ 매크로 세그먼트를 동적으로 조정하여 네트워크 보안 최적화

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
마이크로 세그멘테이션	마이크로 세그멘테이션은 네트워크를 세분화하여 각 워크로드나 애플리케이션별로 세그먼트를 설정하는 기술로, 보다 정밀한 보안 제어를 가능하게 한다. 접속하는 ID 또는 애플리케이션 접근을 기반으로 네트워크 세분화를 정의하거나 물리적 세분화를 수행하고 문서화하여야 한다. 또한 가능하다면 호스트 수준의 프로세스 마이크로 세그멘테이션을 수행한다.	기존	‣ 주요 애플리케이션 및 워크로드 기준 초기 마이크로 세그먼트 설정 ‣ 수동으로 세그먼트를 구성하고 기본적인 보안 정책 적용
		초기	‣ 마이크로 세그먼트를 확장하여 맞춤형 보안 정책 자동 적용 ‣ 네트워크 수준에서 마이크로 세그멘테이션 수행 및 워크로드 간 이동 탐지·차단 ‣ 마이크로 세그먼트 간의 트래픽 모니터링 및 실시간 위협 탐지
		향상	‣ 마이크로 세그먼트 관리 자동화 강화 ‣ 모든 네트워크 트래픽에 대한 정밀한 보안 제어 구현 ‣ 애플리케이션 별 격리 메커니즘 적용 및 위협 탐지·대응 시스템과 통합
		최적화	‣ AI·ML을 활용하여 마이크로 세그먼트를 실시간 최적화 ‣ 위협에 자동 대응하고, 종합적인 보안 관리 전략 구현
소프트웨어 정의 네트워킹	네트워크를 소프트웨어 기반으로 관리하고 제어하는 기술로, SDN 프로그래밍 가능 인프라를 구현하여 제어 영역과 데이터 영역을 분리하고 데이터 영역의 요소를 중앙에서 관리 및 제어를 수행한다. 네트워크의 유연성을 높이고 보안을 강화하는 데 사용된다.	기존	‣ 네트워크 구성 요소의 기본 소프트웨어 정의 제어 도입 ‣ SDN 기본 구조 설정 및 네트워크 트래픽을 소프트웨어로 제어
		초기	‣ SDN을 통해 네트워크 트래픽을 중앙에서 관리 및 실시간 정책 적용 ‣ 네트워크 보안 정책을 SDN 환경에 통합하여 자동화된 보안 구현
		향상	‣ SDN 기능 확장 및 네트워크 전반 트래픽 관리 및 보안 최적화 ‣ 실시간 네트워크 구성 및 정책 조정
		최적화	‣ AI 기반 SDN 솔루션 도입하여 네트워크 트래픽 예측 및 자동 최적화 ‣ SDN을 통해 네트워크 보안 실시간 강화 및 자동화된 위협 대응 구현

나. 위협 대응

네트워크 상의 위협을 신속하게 탐지하고 대응하는 기능이 강조된다. 위협 대응 기능은 네트워크에서 발생할 수 있는 다양한 위협을 실시간으로 감지하고, 즉각적인 조치를 취하는 데 중점을 둔다. 이를 통해 외부 공격이나 내부에서 발생하는 이상 활동에 신속히 대응할 수 있으며, 네트워크의 정상 운영을 유지하면서도 보안 위협을 최소화할 수 있다. 위협 탐지와 대응 기능은 제로트러스트 모델의 핵심인 '항상 의심하고, 검증하는' 원칙에 맞게, 지속적으로 네트워크 활동을 모니터링하고 보안 사고를 예방하는 데 필수적이다.

표 3-20 네트워크 핵심 요소의 위협 대응 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
위협 대응	위협 대응 기능은 네트워크 내에서 발생하는 모든 잠재적 위협을 신속하게 감지하고 대응하는 시스템을 말한다. 이 기능은 침입 탐지 및 방지 시스템(IDS·IPS), 위협 인텔리전스, 자동화된 대응 시스템 등을 포함한다.	기존	‣ 위협 인텔리전스와 기본적인 IDS·IPS 솔루션 도입 ‣ 수동 대응이 주를 이루며, 보안 사고 발생 시 기본 절차에 따라 대응
		초기	‣ 자동화된 위협 탐지 및 대응 시스템 도입 ‣ 위협 인텔리전스 활용 네트워크 모니터링 및 자동 경고 생성
		향상	‣ 실시간 위협 감지 및 선제 대응 ‣ 머신러닝 기반 분석 도입, 비정상 활동 자동 탐지 및 차단
		최적화	‣ 완전히 통합된 위협 대응 플랫폼 구축 ‣ AI 기반 예측 분석으로 잠재 위협 사전 감지 및 차단

다. 트래픽 암호화

네트워크 트래픽을 보호하기 위해 암호화 기능이 필수적으로 적용된다. 네트워크를 통해 전달되는 데이터는 암호화를 통해 외부의 도청이나 침입으로부터 보호된다. 암호화는 데이터를 전송하는 동안에도 보호하며, 민감한 정보가 네트워크를 통해 유출되거나 변경되지 않도록 한다. 이를 통해 기업은 네트워크 내에서 발생할 수 있는 데이터를 안전하게 보호하며, 내부 정보 유출을 방지하는 데 큰 도움을 얻는다.

표 3-21 네트워크 핵심 요소의 트래픽 암호화 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
트래픽 암호화	트래픽 암호화는 네트워크 내에서 데이터의 기밀성을 유지하고, 전송 중인 데이터를 보호하기 위한 기술이다. 이는 SSL·TLS, VPN, 데이터 암호화 및 전송 계층 보안 등을 포함한다.	기존	▸ 기본 암호화 기술 도입, 민감 데이터 보호 ▸ SSL·TLS 등 표준 프로토콜로 웹 트래픽 보호, VPN을 통한 추가 보안
		초기	▸ 암호화 기술 전사적 확대 적용, 모든 중요 데이터 및 통신 채널 암호화 ▸ 전사적 암호화 정책 수립 및 데이터 전송 암호화 필수화
		향상	▸ 고도화된 암호화 기법 적용, 전송 데이터 및 저장 데이터 보호 ▸ 고급 암호화 키 관리 시스템 도입 및 전방위적인 보호 체계 구축
		최적화	▸ 성능 저하 없는 암호화 기술 최적화 ▸ 양자내성암호 도입, 최고 수준의 보안 유지 ▸ 암호화 및 복호화 자동화, 통합 키 관리 시스템 운영

라. 트래픽 관리

네트워크 트래픽의 흐름을 세밀하게 관리하고 모니터링하는 기능이 중요하다. 데이터 흐름 매핑은 네트워크 내에서 트래픽이 어떻게 이동하고, 어떤 경로를 통해 데이터를 전달하는지 파악해 이를 기반으로 최적화된 보안 정책을 수립하는 역할을 한다. 이를 통해 기업은 네트워크 상에서 비정상적인 흐름이나 예기치 않은 데이터 이동을 즉각 감지하고 차단할 수 있다. 데이터 흐름을 명확히 파악함으로써 네트워크 트래픽을 효율적으로 관리하고, 잠재적인 보안 위협을 사전에 차단하는 데 기여한다.

표 3-22 네트워크 핵심 요소의 트래픽 관리 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
데이터 흐름 매핑	네트워크 내에서 데이터가 어떻게 이동하는지를 시각화하고 분석하는 과정이다. 이를 통해 데이터의 출처, 목적지, 경로 등을 파악하여 보안 정책을 설계하고 위협을 예측할 수 있다.	기존	‣ 네트워크 내 주요 데이터 흐름을 수동으로 매핑하고 분석 ‣ 초기 데이터 흐름 다이어그램 작성 ‣ 데이터 트래픽에 대한 수동적 모니터링 수행 ‣ 최소한의 암호화를 통해 데이터 흐름 파악
		초기	‣ 애플리케이션 단위에서 트래픽 매핑 및 분석 ‣ 자동화된 데이터 흐름 매핑 도구 도입
		향상	‣ 보안 정책을 수립하여 비정상적인 데이터 이동 탐지 ‣ 데이터 흐름 상관관계 분석 및 보안 위협 사전 식별 ‣ 데이터 흐름과 보안 정책을 실시간으로 업데이트 및 최적화
		최적화	‣ AI 기반 예측 분석 도구로 데이터 흐름 변화 실시간 감지 및 자동 대응 ‣ 네트워크 트래픽 우선순위 동적 변경 ‣ 데이터 흐름 매핑을 다른 보안 시스템과 통합하여 종합적인 네트워크 보안 전략 수립

마. 네트워크 회복성

네트워크의 안정성과 복원력을 강화하는 기능이 중심이 된다. 네트워크 회복성은 네트워크에 문제가 발생했을 때 빠르게 복구하고, 중단 없는 서비스 운영을 보장하는 데 중점을 둔다. 네트워크 중단이나 공격으로 인해 발생하는 서비스 장애를 최소화하고, 위협을 감지한 후에도 네트워크가 정상적으로 작동하도록 보장하는 것이 목표다. 회복성을 강화함으로써 기업은 장기적인 보안 체계를 유지하고, 중대한 네트워크 장애 상황에서도 신속한 복구를 통해 비즈니스 연속성을 보장할 수 있다.

표 3-23 네트워크 핵심 요소의 네트워크 회복성 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
네트워크 회복성	네트워크 회복성은 네트워크가 다양한 위협이나 장애로부터 신속하게 복구하고, 지속적으로 가용성을 유지할 수 있도록 하는 능력이다. 이 기능은 다중 경로 설계, 자동 복구, 재해 복구 계획 등을 포함한다.	기존	‣ 네트워크 주요 구성 요소에 대한 기본 복구 계획 및 백업 경로 마련 ‣ 주기적 백업 실시 및 장애 대응 절차 마련
		초기	‣ 다중 경로 설계 및 자동 복구 시스템 도입 ‣ 중요한 네트워크 구성 요소에 대해 자동화된 장애조치(페일오버, Failover) 메커니즘 도입 ‣ 네트워크 가용성 보장을 위한 이중화 설계 완료
		향상	‣ 네트워크 복구 능력 고도화 ‣ 재해 복구 계획 통합 및 복구 시나리오 주기적 테스트
		최적화	‣ 자율 복구 시스템 도입, 네트워크 장애 실시간 감지 및 복구 ‣ 모든 복구 절차 자동화 ‣ 재해 복구 테스트 정기적 수행 및 회복성 지표 지속 모니터링

4. 시스템

가. 접근통제

시스템에 접근하는 사용자나 기기의 권한을 엄격히 통제하는 기능이 도입된다. 접근통제는 사용자가 시스템 리소스에 접근할 때, 적절한 권한이 있는지 확인하고 불필요한 접근을 차단한다. 이를 통해 최소 권한 원칙을 적용해 시스템 리소스를 보호할 수 있다.

표 3-24 시스템 핵심 요소의 접근통제 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
접근 통제	사용자와 기기가 네트워크와 시스템에 접근할 때, 허용된 리소스만을 사용할 수 있도록 권한을 부여하고 이를 엄격하게 관리하는 보안 기능이다. 이를 통해 적절한 자격을 가진 사용자만이 필요한 리소스에 접근할 수 있으며, 보안 사고를 예방할 수 있다.	기존	‣ 기본적인 접근제어 체계 수립 ‣ 사용자 및 기기별로 수동으로 권한 부여 ‣ 사용자는 주로 역할 기반 접근제어(RBAC)를 통해 리소스에 접근 ‣ 권한 관리를 수동으로 수행
		초기	‣ 자동화된 접근제어 시스템을 도입 ‣ 사용자 역할과 권한을 기반으로 네트워크 및 시스템 접근을 중앙에서 관리 ‣ 실시간으로 접근권한 부여 ‣ 권한 변경 사항 자동으로 반영 ‣ 특정 리소스에 대한 접근을 제한하거나 승인하는 정책 적용
		향상	‣ 속성 기반 접근제어(ABAC) 시스템을 도입 ‣ 사용자와 기기의 속성에 따라 더욱 세밀한 접근제어 수행 ‣ 사용자의 위치, 기기 상태, 시간 등 다양한 조건을 바탕으로 접근권한 동적 관리 ‣ 실시간으로 접근통제 강화
		최적화	‣ AI를 기반으로 자율적인 접근통제 시스템 구축 ‣ 사용자의 행동 패턴과 기기 상태를 실시간으로 분석하고 자동으로 권한 조정 ‣ 모든 접근제어는 중앙집중적 시스템에서 실시간으로 관리 ‣ 시스템에 영향을 미치는 명령 실행 시 실시간 신뢰도 재산정 ‣ 위험 분석 기반 지속적인 접근제어 정책 적용

나. 시스템 계정 관리

PAM과 자격 증명 관리를 통해 시스템의 계정 및 인증 정보를 보호하는 것이 핵심이다. PAM은 중요 시스템에 접근할 수 있는 특수 권한 계정을 관리하고, 모니터링하며, 세밀한 권한 제어를 제공해 내부자 위협 및 계정 남용을 방지한다. 자격 증명 관리는 계정 및 인증 정보를 안전하게 저장하고, 계정 탈취나 유출로부터 보호하는 역할을 한다. 이를 통해 계정 보안의 전반적인 수준을 높일 수 있다.

표 3-25 시스템 핵심 요소의 시스템 계정 관리 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
PAM	PAM은 권한 있는 사용자 및 시스템의 접근을 관리하고 모니터링하는 보안 체계로, 영구적인 관리자 권한 등 높은 권한을 제거하는 데 중점을 두며, 이를 위해 먼저 PAM 시스템을 구축하고, 권한 사용자를 이 시스템으로 이전하는 작업을 수행한다. 이후, 권한 상승 승인을 자동화하고, 시스템에 분석 데이터를 입력하여 이상 탐지를 수행하는 방식으로 사용된다.	기존	‣ 기본적인 PAM 시스템을 구축 ‣ 권한 있는 사용자 계정을 관리 ‣ PAM 정책 수립
		초기	‣ PAM 솔루션을 통해 권한 있는 사용자 접근 모니터링 및 제어 ‣ 자동화된 권한 상승 승인 기술 도입
		향상	‣ PAM 시스템에 분석 및 경고 기능을 통합하여 비정상적인 활동 탐지 ‣ 권한 관리 절차 정교화 및 감사 로그 강화
		최적화	‣ AI 기반의 위협 탐지 및 대응 기능을 활용하여 PAM 시스템 고도화 ‣ PAM 정책, 절차 지속적 개선 및 최적화
자격 증명 관리	자격 증명 관리는 사용자와 기기의 인증 정보를 안전하게 저장하고 관리하는 기능으로, 이를 통해 네트워크 및 시스템 접근 시 올바른 자격 증명이 이루어지도록 한다. 이는 패스워드, 인증서, MFA 등을 포함한다.	기존	‣ 자격 증명을 수동으로 관리 ‣ 패스워드 기반 인증 방식에 의존 ‣ 사용자 인증이 고정된 방식으로 이루어짐 ‣ 자격 증명 관리가 체계적이지 않고 수동으로 이루어짐
		초기	‣ 자격 증명 관리 자동화 ‣ MFA 도입 등 보다 안전한 인증 방식 적용 ‣ 자격 증명 시스템 중앙 관리
		향상	‣ 고급 인증 방식을 도입(생체 인증 및 인증서 기반 인증 추가) ‣ 자격 증명 관리 시스템이 고도화 ‣ 자격 증명의 무결성 보장, 실시간으로 인증 정보 관리를 통한 인증 프로세스 강화
		최적화	‣ AI 기반의 자격 증명 관리 시스템을 통해 실시간으로 인증 정보를 분석 ‣ 비정상적인 인증 시도 즉각 차단 ‣ 자격 증명 관리 시스템 자율적으로 운영 ‣ 모든 자격 증명 데이터 중앙 관리 ‣ 실시간 인증 정책 조정

다. 네트워크 분리 정책

이 기능에서는 네트워크 세분화를 점진적으로 적용하여 시스템 내 네트워크를 여러 구역으로 나누고, 각 구역에 맞는 보안 정책을 설정하는 것이 핵심이다. 네트워크 세분화를 통해 보안 경계를 만들고 구역 간 보안 수준을 높이다 보면, 구역 간에 합법적인 접근이 필요해지는 경우가 생기며, 이때 그룹 간 이동이 중요한 역할을 한다. 그룹 간 이동 기능을 통해 구역 간 트래픽을 제어하고, 인증된 사용자만이 네트워크 내에서 허가된 리소스에 접근할 수 있도록 하여, 보안성을 유지하면서도 필요한 이동을 지원할 수 있다.

표 3-26 시스템 핵심 요소의 네트워크 분리 정책 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
네트워크 세분화 및 그룹 간 이동	네트워크 세분화는 네트워크를 더 작은 단위로 나누어 보안을 강화하는 방식으로, 그룹 간 이동을 통해 세분화된 네트워크 간에 안전한 이동을 보장한다. 이는 보안 정책을 세밀하게 적용하고, 필요에 따라 특정 그룹 간의 트래픽 이동을 제어하는 데 사용된다.	기존	▸ 보안 정책 일괄적 적용 ▸ 그룹 간 이동에 대한 제어가 이루어지지 않음 ▸ 망분리 등의 기본적인 경계형 네트워크 모델이 적용 ▸ 네트워크 세분화 및 이동 통제 미비
		초기	▸ 일부 중요 시스템을 네트워크 세분화를 통해 나눔 ▸ 세분화된 네트워크 간 접속 이동의 경우 보안 정책 적용 ▸ 시스템의 중요도에 따라 네트워크 분리 ▸ 중요 시스템과 일반 시스템 간의 접속과 이동을 제한하는 보안 정책 도입 ▸ 트래픽 이동을 모니터링하고, 제한적인 보안 통제를 적용하여 그룹 간 이동 제어
		향상	▸ 네트워크 등급 및 기능별 세분화 ▸ 각 네트워크 그룹 간의 이동은 강력한 접근통제와 인증을 기반 엄격한 관리 ▸ 네트워크 간 이동 시 실시간 보안 검사 적용 ▸ 그룹 간 이동이 동적으로 통제 ▸ 민감한 자산 및 시스템 간의 트래픽 이동에 대해 세밀한 관리 수행
		최적화	▸ 그룹 간 이동 실시간 분석 및 제어 ▸ 그룹 간 이동 시 재인증 없이 이동이 가능하도록 추가적인 정책 적용 ▸ 세분화된 네트워크 내에서 트래픽 이동 실시간 감시 ▸ 위협이 감지되면 즉각적으로 차단 ▸ 자율적인 네트워크 세분화, 보안 관리 수행 ▸ 그룹 간 이동이 보안 위험 없이 안전하게 이루어질 수 있도록 실시간 보안 정책 조정

라. 시스템 보안 및 정책 관리

이 기능은 시스템 환경에 맞는 보안 정책을 관리하는 것을 의미하다. 이는 기업이 시스템을 온프레미스에서 클라우드 환경으로 점진적으로 전환할 때, 각 환경에 맞는 보안 정책을 수립하고 관리하는 데 중점을 둔다. 온프레미스 환경에서는 기존의 보안 정책을 준수하면서도 클라우드 전환 과정에서는 클라우드 환경에 적합한 보안 정책을 적용해 이행할 수 있어야 한다. 이를 통해 환경 변화에 따른 보안 취약점을 최소화하고, 정책 일관성을 유지할 수 있다.

표 3-27 시스템 핵심 요소의 시스템 보안 및 정책 관리 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
시스템 환경에 따른 정책 관리	시스템 환경에 따른 정책 관리는 온프레미스(사내 데이터센터) 환경에서 클라우드 환경으로 전환되면서 보안 정책이 달라져야 하는 상황을 반영한 관리 체계이다. 각 환경에 맞는 보안 정책을 수립하고, 변화하는 환경에 맞춰 정책을 조정한다.	기존	‣ 온프레미스 환경에서 보안 정책 수립 및 관리 ‣ 정책이 고정된 상태로 운영 ‣ 클라우드 환경으로의 전환이 이루어지지 않음
		초기	‣ 클라우드 환경으로의 전환 시작 ‣ 온프레미스와 클라우드 환경 간의 차이를 반영한 보안 정책 수립 ‣ 클라우드 환경에 맞는 보안 요구사항 반영 ‣ 자동으로 클라우드 환경에 정책 적용
		향상	‣ 클라우드 환경으로의 전환 가속화 ‣ 하이브리드 클라우드 환경을 위한 통합된 보안 정책 적용 ‣ 온프레미스와 클라우드 환경에서 실시간으로 보안 정책을 조정 ‣ 환경 변화에 따라 동적으로 정책 변경
		최적화	‣ AI 기반 정책 관리 시스템 적용 ‣ 클라우드 환경의 변화에 따라 보안 정책이 자동으로 최적화 ‣ 온프레미스, 클라우드, 하이브리드 환경 모두에서 실시간으로 정책 조정 ‣ 보안 위협에 맞춘 자율적인 정책 적용 가능 ‣ 정책 관리 완전 자동화

5. 애플리케이션 및 워크로드

가. 애플리케이션 접근

애플리케이션과 워크로드에 대한 접근 인가를 관리하는 데 중점을 둔다. 리소스 권한 부여 및 통합 기능을 통해, 사용자가 애플리케이션과 워크로드에 접근할 때 적절한 권한을 부여하고 이를 중앙에서 통합 관리한다. 이를 통해 각 리소스에 대한 접근권한을 일관되게 관리하고, 최소 권한 원칙에 따라 불필요한 접근을 차단한다.

표 3-28 애플리케이션 및 워크로드 핵심 요소의 애플리케이션 접근 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
리소스 권한 부여 및 통합	애플리케이션 및 시스템에 대한 접근권한을 관리하고, 이를 다른 보안 시스템과 통합하여 보안을 강화하는 과정으로, 표준화된 리소스 승인 게이트웨이를 설정하여 관리한다.	기존	‣ 기본적인 접근권한 관리 시스템 도입 ‣ 사용자 및 시스템의 권한 수동 관리 ‣ 각 리소스에 대한 접근권한 정의 ‣ 로컬 인증·인가 기능 및 정적 속성에 기반한 접근제어 수행
		초기	‣ 중앙 집중식 접근권한 관리 시스템 도입 ‣ 모든 리소스에 대한 권한 중앙 관리 ‣ 접근권한 관리 시스템을 기업의 다른 보안 시스템과 통합
		향상	‣ 다수의 컨텍스트 정보를 조합하여 최소 권한 원칙 적용 ‣ RBAC과 ABAC 결합
		최적화	‣ AI를 활용하여 사용자 행동 분석 ‣ 이상 징후를 자동으로 탐지하여 권한 조정 ‣ 자동화된 접근권한 부여 및 회수 시스템 도입 ‣ 실시간 권한 관리 및 비정상적인 접근 차단 ‣ 모든 리소스 권한 부여 및 관리 자동화 ‣ 지속적인 모니터링 및 최적화

나. 애플리케이션 위협 보호

애플리케이션 및 워크로드에 대한 지속적인 모니터링과 실시간 승인 관리가 필요하다. 지속적인 모니터링 및 진행 중인 승인을 통해 사용자의 행위와 워크로드의 상태를 실시간으로 모니터링하며, 변경 사항에 따라 동적으로 접근 승인을 유지하거나 차단한다. 이는 잠재적 위협을 빠르게 탐지하고 대응할 수 있도록 하며, 제로트러스트 원칙에 따라 끊임없이 신원을 검증하는 역할을 수행한다.

표 3-29 애플리케이션 및 워크로드 핵심 요소의 애플리케이션 위협 보호 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
지속적인 모니터링 및 진행 중인 승인	자동화된 도구와 프로세스를 사용하여 애플리케이션 및 시스템의 보안 상태를 지속적으로 모니터링하고, 실시간으로 보안 승인을 관리하는 과정이다.	기존	‣ 수동으로 애플리케이션 및 시스템 보안 상태 모니터링, 보안 이벤트 기록 ‣ 초기 보안 승인 프로세스 수립 ‣ 주요 시스템 변경 사항에 대한 보안 검토 실시
		초기	‣ 자동화된 보안 모니터링 도구 도입 ‣ 실시간 보안 이벤트 수집 및 분석 ‣ 진행 중인 승인 프로세스 도입 ‣ 모든 시스템 변경 사항에 대해 보안 검토 수행
		향상	‣ AI 기반의 보안 모니터링 시스템 도입 ‣ 보안 이벤트 분석 및 이상 징후 실시간 탐지 ‣ 보안 승인 프로세스 자동화 ‣ 보안 위험이 있는 변경 사항 자동으로 차단/수정
		최적화	‣ 보안 모니터링 최적화 ‣ 위협 사전 예측 및 대응 ‣ 모든 시스템의 보안 상태 지속적으로 평가 ‣ 자동화된 보안 승인 프로세스 적용

다. 접근 가능한 애플리케이션

원격 접속 기능을 통해, 애플리케이션과 워크로드에 안전하게 원격으로 접근할 수 있도록 한다. 이는 특히 재택근무나 외부에서의 접속을 지원하는 환경에서 필수적인 기능이다. 이를 통해 원격에서 접속하는 사용자와 기기에 대한 보안 검증을 강화하고, 원격으로 이루어지는 모든 상호작용을 철저히 통제한다.

표 3-30 애플리케이션 및 워크로드 핵심 요소의 접근 가능한 애플리케이션 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
원격 접속	사용자가 외부에서 안전하게 기업망에 접속할 수 있도록 하는 보안 조치이다. 최소 권한 기준을 설정하기 위해 기존 기기 접근 프로세스 및 도구를 사용한다. 승인된 애플리케이션에 대해 기업 IDP를 사용하는 기기 및 IoT 등이 원격 접속 지원을 포함하도록 확장한다.	기존	‣ 기본적인 원격 접속 솔루션(VPN 등)을 도입하여 외부 접속 지원 ‣ 초기 보안 정책 수립과 함께 애플리케이션에 대한 접근제어가 제한적
		초기	‣ 원격 접속 보안 강화를 통한 사용자 인증 및 데이터 암호화 구현 ‣ 애플리케이션별 접근제어가 추가되어, 사용자 및 기기의 보안 상태에 따라 애플리케이션 기능 접근 제한
		향상	‣ 원격 접속 기기 실시간 모니터링 및 제어 ‣ 애플리케이션의 기능 사용을 시나리오별로 제한하고, 접속 상황에 따라 동적 보안 정책을 적용하여 애플리케이션 기능 필요시 제한
		최적화	‣ AI를 활용하여 원격 접속 보안 고도화 ‣ 애플리케이션 접근이 사용자 행동 및 접속 상태에 따라 자동으로 조정되며, AI를 통해 위험 요소가 탐지될 경우 애플리케이션 기능이 즉각적으로 제한 또는 차단

라. 안전한 애플리케이션 배포

애플리케이션 배포 과정에서의 보안이 강조된다. 안전한 애플리케이션 배포 기능을 통해 애플리케이션을 안전하게 배포하고, 배포된 모든 애플리케이션 프로그램에 대한 애플리케이션 인벤토리를 유지하여 전체 상태를 체계적으로 관리한다. 이를 통해 배포된 애플리케이션이 지속적으로 보안 검사를 통과하도록 하고, 인벤토리를 통해 취약점을 추적하고 관리할 수 있다.

표 3-31 애플리케이션 및 워크로드 핵심 요소의 안전한 애플리케이션 배포 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
안전한 애플리케이션 배포	안전한 애플리케이션 배포란 애플리케이션을 배포할 때 발생할 수 있는 보안 위협을 최소화하기 위한 프로세스와 도구를 사용하는 것을 의미한다. 이는 보안 정책 준수, 취약점 검사, 자동화된 배포 파이프라인, 코드 무결성 검증, 환경 격리 및 모니터링을 포함한다.	기존	‣ 애플리케이션 배포 시 기본적인 보안 검토 실시 ‣ 보안 가이드라인을 준수하는 초기 배포 절차 마련 ‣ 배포 전 수동으로 코드 검토 및 취약점 검사 수행 ‣ 기본적인 접근제어를 적용하여 배포 과정에서의 보안 사고 방지
		초기	‣ 보안이 내재된, 자동화된 배포 파이프라인 구축 ‣ 애플리케이션 배포 시 보안 자동으로 적용 ‣ CI/CD 파이프라인에 자동화된 취약점 검사 도구 통합 ‣ 배포 전후로 코드 무결성 확인 ‣ 배포 환경을 격리하여 공격 표면 최소화
		향상	‣ 배포 과정 전반에 걸쳐 고급 보안 검사 추가 ‣ 배포 환경에 대한 지속적인 모니터링 수행 ‣ 보안 위협을 실시간으로 감지 및 대응 ‣ 보안 정책 준수 여부를 자동으로 검증하는 도구 도입 ‣ 애플리케이션의 모든 구성 요소가 배포 전후로 보안 검사를 거치도록 구성 ‣ 배포 중에 발생할 수 있는 비정상적인 활동 모니터링 및 대응
		최적화	‣ 완전히 자동화된 보안 중심 배포 파이프라인 구성 ‣ 애플리케이션 배포 시 최상의 보안 상태를 유지 ‣ AI를 활용한 고도화된 위협 탐지 및 대응 시스템을 배포 파이프라인에 통합 ‣ 배포 환경 전반에 걸쳐 자율 보안 기능 적용 ‣ 모든 배포 프로세스 중앙 관리 ‣ 배포 과정에서 보안 준수 여부 자동 보고 및 추적
애플리케이션 인벤토리	기업 내에서 사용되는 모든 애플리케이션을 식별하고, 이를 체계적으로 관리하는 과정이다. 인벤토리를 통해 애플리케이션의 상태, 소유권, 사용 목적 등을 파악할 수 있다.	기존	‣ 기업 내 모든 애플리케이션 수동 목록화 ‣ 초기 애플리케이션 인벤토리 작성 ‣ 애플리케이션 기본 정보(이름, 소유자, 위치 등)를 기록하여 관리
		초기	‣ 자동화된 인벤토리 도구를 도입 ‣ 애플리케이션 자동 식별 및 주기적으로 업데이트 ‣ 애플리케이션 생명주기 관리 기능을 도입하여 인벤토리를 지속적으로 유지
		향상	‣ 애플리케이션 인벤토리에 보안 정보 추가 ‣ 각 애플리케이션의 보안 상태 평가 및 관리 ‣ 인벤토리 데이터를 기반으로 보안 정책 적용
		최적화	‣ AI 기반의 인벤토리 관리 시스템을 도입 ‣ 애플리케이션의 변경 사항 실시간 반영 ‣ 보안 상태 지속적 모니터링 ‣ 애플리케이션 인벤토리를 다른 보안 시스템과 통합, 종합적인 보안 관리 전략 구현

마. 소프트웨어·애플리케이션 보안

소프트웨어와 애플리케이션의 개발 및 배포 전반에 걸친 보안이 중점적으로 다루어진다. 안전한 소프트웨어 개발 및 통합은 보안이 내재된 소프트웨어 개발 프로세스를 통해, 애플리케이션이 처음부터 안전하게 개발되도록 한다. 또한 소프트웨어 위험 관리는 소프트웨어의 잠재적인 위험을 사전에 식별하고 관리하여, 취약점이 발생하기 전에 미리 대비할 수 있도록 한다.

표 3-32 애플리케이션 및 워크로드 핵심 요소의 소프트웨어·애플리케이션 보안 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
안전한 소프트웨어 개발 및 통합	소프트웨어 개발 생명주기(SDLC) 전반에 걸쳐 보안 요소를 내재화하고, 개발된 소프트웨어를 안전하게 통합하는 과정이다. 코드 검토, 런타임 보호, 보안 API 게이트웨이, 컨테이너 및 서버리스 보안과 같은 제어 기능이 통합되고 자동화된다. DevSecOps를 통하여 워크플로우를 구성한다.	기존	‣ 개발 프로세스에 기본적인 보안 코딩 표준, 가이드라인 도입 ‣ 코드 배포 전, 정적/수동 보안 테스트 수행
		초기	‣ 안전성 검토와 테스트를 SDLC에 통합 ‣ 개발 단계에서부터 보안 취약점 식별 및 수정 ‣ CI/CD 파이프라인에 정적 및 동적 분석 도구를 통합하여 자동화된 보안 검사 수행 ‣ DevSecOps 문화 도입 ‣ 주요 개발 내용에 대한 SBOM 문서 작성
		향상	‣ 서드파티 라이브러리 및 오픈소스 소프트웨어 보안 검사 자동화 및 인벤토리 반영 ‣ 프로세스 전반에 걸친 SBOM 문서를 작성 ‣ SBOM 문서 작성을 자동화하기 위한 도구 이용
		최적화	‣ 소프트웨어 개발과 관련된 기업의 프로세스 격리 및 마이크로 세그멘테이션 수행 ‣ 모든 소프트웨어 개발 및 통합 프로세스 자동화 ‣ 런타임 소프트웨어에 대한 분석 자동화를 통한 보안성 지속 유지 및 최적화
소프트웨어 위험 관리	소프트웨어 개발 및 운영 과정에서 발생할 수 있는 보안 위험을 식별, 평가, 완화하는 프로세스이다.	기존	‣ 소프트웨어 개발 및 운영에 따른 기본적인 위험 요소 식별 및 문서화 ‣ 위험 관리 계획을 수립하여, 발생 가능한 보안 사고에 대비
		초기	‣ 위험 평가 프로세스 도입 ‣ 각 소프트웨어의 위험 수준 평가 및 우선순위 지정 ‣ 위험 완화 전략 수립 및 정기적 검토 후 보안 정책 반영
		향상	‣ 위험 관리 시스템 자동화 ‣ 실시간 소프트웨어 위험 상태 모니터링 및 대응 ‣ 소프트웨어 공급망에 대한 보안 검사 강화
		최적화	‣ AI 기반 예측 분석 도입 ‣ 잠재적인 보안 위험 사전 식별 및 대응 ‣ 맞춤형 공격 대응 체계 확보 ‣ 기업 전체에 걸쳐 위험 관리 통합

6. 데이터

가. 데이터 목록 관리

기업이 보유한 데이터를 체계적으로 목록화하고, 데이터를 적절히 관리하는 것이 핵심이다. 데이터 카탈로그를 통해 기업 내 데이터를 일관성 있게 정리하고 관리하며, 위험 정렬을 통해 데이터를 중요도에 따라 분류하고 보안을 적용한다. 기업 내부 데이터 거버넌스는 조직 전반에 걸쳐 데이터 사용과 관리를 규정하고 일관된 정책을 수립하는 데 중점을 둔다.

표 3-33 데이터 핵심 요소의 데이터 목록 관리 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
데이터 카탈로그 위험 정렬	기업의 모든 데이터를 분류하고, 데이터가 식별 및 목록화되고 데이터 환경에 대한 모든 변경 사항이 자동으로 감지되어 카탈로그 내 포함되는지 확인하는 것을 의미한다. 각 데이터 항목에 대한 위험 수준을 평가하여 이를 체계적으로 관리하는 과정이다.	기존	‣ 데이터 자산의 초기 카탈로그 작성 ‣ 주요 데이터 유형 수동 분류 ‣ 데이터에 대한 기본적인 위험 평가 정의 및 문서화
		초기	‣ 자동화된 데이터 카탈로그 도구 도입 ‣ 데이터 자산 일부 자동화를 통한 수집 및 분류 ‣ 데이터의 위험 수준을 평가하기 위한 기본적인 기준과 지침 수립
		향상	‣ 고급 분석 도구를 통한 데이터 민감도 및 위험 수준 정밀 평가 ‣ 데이터 카탈로그 완전 자동화 ‣ 카탈로그 지속적 업데이트 및 위험 정렬을 기반으로 한 데이터 보호 정책 적용 ‣ 데이터 사용 패턴 분석 수행
		최적화	‣ AI를 활용하여 데이터 위험 요소 실시간 분석 및 카탈로그 반영 ‣ 데이터 카탈로그와 다른 보안 시스템 통합
기업 데이터 거버넌스	기업 내 모든 데이터의 사용, 보호, 관리에 대한 규칙과 절차를 정의하고, 이를 준수하는 과정을 의미한다.	기존	‣ 데이터 거버넌스 정책 수립 및 데이터 관리에 대한 기본적인 지침 마련 ‣ 데이터 소유자와 관리자 지정 ‣ 초기 거버넌스 구조 구성
		초기	‣ 데이터 거버넌스 프레임워크를 도입 ‣ 기업 내 모든 데이터 관리 및 보호 표준화 ‣ 데이터 정책 준수를 위한 정기적인 감사 및 검토 수행
		향상	‣ 데이터 거버넌스 도구를 사용하여 데이터 관리 프로세스를 자동화 ‣ 데이터 정책 준수 실시간 모니터링 ‣ 거버넌스 정책을 지속적으로 업데이트하여, 변화하는 규제와 비즈니스 요구사항에 대응
		최적화	‣ AI 기반의 거버넌스 관리 시스템을 도입 ‣ 데이터 정책 준수 상태 실시간 평가 및 최적화 ‣ 데이터 거버넌스를 기업의 모든 시스템과 통합하여, 일관된 데이터 관리 및 보호

나. 접근 결정방법

데이터를 접근하는 방식에 관한 접근 결정방법을 관리하고 통제한다. 데이터 접근제어 기능을 통해 데이터에 접근할 수 있는 사용자와 권한을 세밀하게 관리하여, 적절한 사용자가 필요한 데이터에만 접근하도록 제한한다. 이를 통해 데이터 접근을 중앙에서 통제하고, 무단 접근을 방지할 수 있다.

표 3-34 데이터 핵심 요소의 접근 결정방법 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
데이터 접근제어	데이터를 보호하기 위해 데이터에 접근할 수 있는 권한을 부여하고, 이를 엄격하게 관리하는 과정이다. 데이터 및 사용자·비인간개체·기기 속성을 기반으로 데이터에 대한 적절한 접근 및 사용을 보장하여야 한다.	기존	‣ 데이터 접근제어 정책 수립 ‣ 초기 권한 체계 수동 관리 ‣ 데이터 접근권한 부여 및 기본적인 접근제어 시행
		초기	‣ 중앙 집중식 접근제어 시스템을 도입 ‣ 최소한의 권한 요소 확인을 통한 데이터 접근 여부 결정
		향상	‣ ABAC 도입을 통해 보다 세밀하고 유연한 접근권한 관리 구현 ‣ 접근제어 시스템을 다른 보안 시스템과 통합하여, 종합적인 보안 정책 적용
		최적화	‣ AI 기반 데이터 접근제어 최적화 및 실시간 권한 조정 ‣ 모든 데이터 접근제어 자동화 및 조직의 보안 정책에 맞춰 지속적으로 최적화

다. 데이터 암호화

데이터가 전송되거나 저장되는 동안 보호받을 수 있도록 데이터 암호화 기능이 적용된다. 암호화는 데이터를 외부 위협으로부터 안전하게 보호하며, 권한 관리를 통해 암호화된 데이터를 접근할 수 있는 사용자와 시스템을 제어한다. 이를 통해 민감한 정보의 유출을 방지하고, 데이터의 무결성을 유지한다.

표 3-35 데이터 핵심 요소의 데이터 암호화 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
데이터 암호화 및 권한 관리	데이터의 무결성과 기밀성을 보호하기 위해 데이터를 암호화하고, 접근권한을 관리하는 과정이다. 저장 및 전송 중인 데이터를 암호화하기 위한 전략을 수립하고 구현하여야 한다.	기존	‣ 주요 데이터 수동으로 암호화 ‣ 기본적인 암호화 정책 수립 ‣ 데이터 보호를 위한 초기 권한 관리 체계 수립
		초기	‣ 자동화된 데이터 암호화 도구 도입 ‣ 모든 중요한 데이터 자동으로 암호화 ‣ 중앙 집중식 데이터 권한 관리 시스템 도입
		향상	‣ 고급 암호화 기술을 도입 ‣ 권한 관리 시스템을 다른 보안 시스템과 통합 ‣ RBAC·ABAC 결합을 통한, 보다 정밀한 권한 관리 구현
		최적화	‣ AI 기반의 암호화 및 권한 관리 시스템 도입을 통하여 데이터 보호 최적화 및 실시간 권한 조정 ‣ 모든 데이터 암호화 및 권한 관리 자동화

라. 데이터 분류

데이터를 보다 세밀하게 분류하고 관리할 수 있도록 데이터 라벨링 및 태그 지정 기능이 도입된다. 데이터를 다양한 카테고리로 분류하고 태그를 지정함으로써, 중요도에 따라 다른 보안 정책을 적용하거나 민감한 데이터를 구분할 수 있다. 이를 통해 데이터가 어떻게 사용되고 보호되어야 하는지 명확하게 관리할 수 있다.

표 3-36 데이터 핵심 요소의 데이터 분류 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
데이터 라벨링 및 태그 지정	데이터를 식별하고 분류하기 위해 메타데이터를 추가하는 과정이다. 데이터 소유자는 레이블 지정·태깅 정책에 대한 관리 지침을 준수하여 데이터에 레이블을 지정하고 태그를 지정한다. 단계가 발전함에 따라 자동화되며, 확장 요구 사항을 충족하고 더 나은 정확성을 제공하여야 한다. 이를 통해 데이터의 보안 수준을 강화할 수 있다.	기존	‣ 라벨링 및 태그 지정 지침 수립 ‣ 일관된 데이터 분류 체계 마련
		초기	‣ 데이터에 기본적인 라벨 및 태그 수동 지정 ‣ 민감한 데이터에 대해 특수 라벨 적용 및 차등적 보안 정책 적용
		향상	‣ 자동화된 라벨링 및 태그 지정 도구 도입 ‣ 데이터 자산 자동 분류 및 식별 ‣ 데이터 라벨링과 태그 지정 정보를 다른 보안 시스템과 연계
		최적화	‣ 고급 메타데이터 관리 도구를 사용 ‣ 데이터 라벨링과 태그 지정 프로세스를 최적화 및 자동화된 규칙 적용 ‣ AI를 활용하여 데이터 라벨링과 태그 지정을 실시간 최적화 ‣ 변화하는 데이터 환경에 따라 자동으로 태그 조정 ‣ 라벨링 및 태그 지정 정보를 모든 보안 시스템과 통합

마. 데이터 손실 방지

데이터 손실 방지(DLP) 기능을 통해 데이터를 외부로부터 보호하고, 내부적으로도 민감한 정보가 유출되지 않도록 한다. 데이터 모니터링 및 감지를 통해 데이터를 실시간으로 감시하여 이상 징후나 데이터 유출이 발생할 경우 즉시 탐지하고 대응할 수 있다. 이는 데이터를 안전하게 유지하고 손실을 방지하는 데 필수적이다.

표 3-37 데이터 핵심 요소의 데이터 손실 방지 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
데이터 손실 방지 (DLP)	민감한 데이터의 유출을 방지하고, 데이터의 무단 접근을 차단하기 위한 기술과 정책이다. 시행 지점을 식별하여 승인된 DLP 도구를 배포하고 태그가 지정된 데이터 속성을 DLP와 통합한다. 처음에 DLP 솔루션은 비즈니스 영향을 제한하기 위해 "모니터링 전용" 모드로 사용하고 나중에 분석 사용은 "방지" 모드로 사용한다. 이후, AI와 통합하여 사용한다.	기존	▸ DLP 정책을 수립 ▸ 민감한 데이터의 유출 가능성 수동 평가 ▸ DLP 도구를 도입하기 위한 기업 내 범위 지정
		초기	▸ 초기 DLP 도구를 도입, 주요 데이터 유출 경로 모니터링 ▸ DLP 정책 중앙 관리 및 다양한 데이터 채널을 통한 유출 차단 ▸ DLP 솔루션 모니터링 모드로 사용
		향상	▸ DLP 시스템을 기업 전반에 도입, 실시간 데이터 보호 및 유출 방지 ▸ DLP 시스템을 다른 보안 시스템과 통합, 종합적인 데이터 보호 전략 구현 ▸ DLP 솔루션 방지 모드로 사용
		최적화	▸ AI를 활용한 데이터 유출 탐지와 예방 기능을 강화 ▸ 데이터 유출 위험 실시간 예측 및 차단 ▸ 모든 DLP 프로세스를 자동화 ▸ 변화하는 데이터 환경에 맞춰 자동으로 보안 정책 최적화
데이터 모니터링 및 감지	데이터 사용과 이동을 실시간으로 모니터링하고, 비정상적인 활동을 탐지하여 보안을 유지하는 과정이다. 데이터 소유자는 데이터 자산의 접근, 공유, 변환 및 사용에 대한 정보가 포함된 활성 메타데이터를 모니터링한다. DLP(데이터 손실 방지) 및 DRM(데이터 권한 관리) 적용 지점 분석을 수행하여 분석 도구를 배포할 위치를 결정한다. 파일 공유, 데이터베이스 등 DLP 및 DRM 범위 밖의 데이터는 대체 도구를 사용하여 변칙적이고 악의적인 활동이 있는지 적극적으로 모니터링하여야 한다.	기존	▸ 데이터 활동 수동 모니터링 ▸ 주요 보안 이벤트 수동 기록 ▸ 초기 데이터 모니터링 및 감지 프로세스 수립
		초기	▸ 자동화된 데이터 모니터링 도구를 도입 ▸ 실시간 데이터 활동 감시 및 비정상적인 행동 탐지 ▸ 모니터링 결과 기반 보안 정책 조정
		향상	▸ AI 기반의 모니터링 시스템을 도입, 데이터 활동 분석 및 이상 징후 실시간 탐지 ▸ 데이터 모니터링 결과를 다른 보안 시스템과 연계하여, 종합적인 보안 대응 구현
		최적화	▸ AI를 활용하여 데이터 모니터링 최적화 ▸ 사전에 위협 예측 및 대응 ▸ 모든 데이터 활동 지속적 평가 및 자동화된 보안 대응 시스템 구축

7. 가시성 및 분석

가시성 및 분석 교차 기능에 대해서는 각각 모든 관련 활동 기록, 중앙집중적 보안 정보 및 이벤트 관리, 보안 위협 분석, 사용자 및 기기 동작 분석, 위협 인텔리전스 통합, 자동화된 동적 정책 세부역량 등을 정의하였다.

표 3-38 가시성 및 분석 교차 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
모든 관련 활동 기록	네트워크, 사용자, 기기, 애플리케이션 등에서 발생하는 모든 이벤트를 기록하고 저장하는 기능이다. 이는 로그 데이터를 생성하고, 이를 기반으로 향후 분석을 위한 데이터를 축적하는 역할을 한다. 관련 활동에는 로그인 시도, 접근권한 변경, 데이터 전송, 애플리케이션 실행 등 보안과 관련된 모든 행동이 포함된다. 이 기능은 잠재적인 보안 위협을 식별하고, 사건 발생 시 정확한 추적과 분석을 가능하게 한다.	기존	‣ 네트워크 및 시스템에서 발생하는 주요 보안 이벤트 기록 ‣ 수동적 로그 기록 ‣ 로그 데이터는 특정 시스템에서만 수집 ‣ 주요 보안 이벤트(예: 로그인 시도, 접근 실패, 권한 변경) 기록 ‣ 보안 사고 발생 시 수동으로 로그를 추적하여 분석할 수 있는 기본적인 체계 마련
		초기	‣ 다양한 시스템에서 자동으로 로그 데이터 수집 ‣ 활동 기록 중앙집중적 수집 ‣ 로그 수집은 네트워크, 애플리케이션, 기기 등 여러 곳에서 이루어지며, 실시간으로 보안 이벤트 기록 ‣ 로그 수집 및 관리 자동화 ‣ 보안 사고 발생 시 신속하게 로그를 분석하고 대응할 수 있는 기반 마련
		향상	‣ 수집된 데이터를 분석하여 보안 위협을 실시간으로 탐지하고 경고 생성 ‣ 로그 기록의 무결성 보장 ‣ 로그 데이터를 기반으로 예측 분석 시작 ‣ 비정상적인 활동 사전 감지
		최적화	‣ AI를 활용한 로그 분석 시스템 구축 ‣ 실시간으로 활동 기록 분석 및 자동으로 보안 위협 탐지·대응하는 자율 보안 체계 구축 ‣ 로그 데이터 관련 항목 포맷 자동화 및 정규화 ‣ 실시간 로그 분석을 통한 보안 정책 자동 조정 ‣ 모든 활동 기록 중앙 관리

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
중앙집중적 보안 정보 및 이벤트 관리	중앙집중적 SIEM은 다양한 보안 이벤트 및 로그 데이터를 한 곳에서 수집하고 관리하는 시스템이다. SIEM은 다수의 보안 도구에서 데이터를 통합하여, 실시간 모니터링, 로그 분석, 경고 및 보고서 작성 기능을 제공한다. 이를 통해 네트워크 전체의 보안 상태를 중앙에서 파악하고, 빠르게 보안 사고에 대응할 수 있다. SIEM은 보안 정책 준수 및 규제 요구사항을 충족하는 데도 도움을 준다.	기존	‣ 보안 이벤트 및 로그 데이터 수동 수집·저장 ‣ 각 시스템에서 발생하는 보안 기록 개별적 관리 ‣ 수동 데이터 분석 ‣ 사고 발생 시 필요한 정보를 추적하는 체계 마련
		초기	‣ 다양한 시스템에서 발생하는 보안 이벤트와 로그 데이터를 자동으로 중앙집중적 SIEM 시스템으로 전송·수집·관리 ‣ 수집된 데이터 실시간 모니터링 ‣ 보안 사고 발생 시 신속하게 대응할 수 있는 중앙집중적 보안 관리 체계 구축
		향상	‣ 중앙집중적 SIEM 시스템에서 실시간으로 보안 이벤트를 분석하고 경고 생성 ‣ SIEM 시스템과 다양한 보안 도구 연동을 통한 보안 데이터 종합적 분석
		최적화	‣ AI를 도입하여 SIEM 시스템에서 수집된 데이터를 기반으로 보안 이벤트 자동 분석 ‣ 비정상적인 활동 실시간 탐지 ‣ 자율적으로 보안 정책 조정 및 보안 사고 발생 시 자동 대응 기능 구현
보안 위협 분석	네트워크에서 발생하는 다양한 활동 및 로그를 분석하여, 잠재적인 보안 위협을 식별하고 대응하는 기능이다. 이는 수집된 로그와 데이터를 기반으로 공격 패턴, 취약점, 이상 행동 등을 분석하여 위협을 사전에 탐지하고, 필요 시 자동으로 조치를 취하는 데 사용된다. 보안 위협 분석은 실시간으로 수행되며, 침입 시도나 악성 활동을 빠르게 파악하여 피해를 최소화할 수 있다.	기존	‣ 수동으로 보안 위협 식별 ‣ 보안 사건 발생 시 추적/분석하는 시스템 구축 ‣ 보안 로그 및 데이터를 기본적으로 수집 ‣ 보안 사고 발생 후 사후 분석을 통한 대응 ‣ CVE, ExploitDB 등 취약점 수집
		초기	‣ 알려진 취약점에 대한 위험성 평가 기준 구현 ‣ 수집된 데이터를 기반으로 보안 위협을 빠르게 분석하고, 경고 생성
		향상	‣ 자동화된 보안 위협 분석 도구 도입 ‣ ML을 활용하여 비정상적인 활동 실시간 분석 ‣ 지속적인 위협 탐지 수행
		최적화	‣ AI 기반의 예측 분석 시스템을 통한 실시간 위협 탐지 및 자동 대응 ‣ 자율 보안 체계 구축 ‣ 보안 위협 발생 전 차단

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
사용자 및 기기 동작 분석	네트워크 내의 사용자의 행동 패턴과 기기 활동을 모니터링하여, 비정상적이거나 의심스러운 활동을 탐지하는 기능이다. 이를 통해 정상적인 행동과 이상 행동을 구분하고, 악의적인 활동을 탐지할 수 있다. 예를 들어, 평소와 다른 시간에 접속하거나, 특정 사용자가 비정상적으로 많은 데이터를 전송할 경우 이를 탐지하여 경고를 발송할 수 있다. 이 기능은 AI·ML을 활용하여 행동 패턴을 학습하고, 실시간으로 분석을 수행한다.	기존	‣ 사용자와 기기의 기본적인 활동 데이터 수집 및 수동 분석 ‣ 비정상적인 행동 수동 탐지 ‣ 기본적인 사용자 행동 패턴 기록 ‣ 의심스러운 활동 추적
		초기	‣ 자동화된 사용자 및 기기 동작 분석 도구 도입 ‣ 네트워크 내 모든 활동 실시간 모니터링 ‣ 사용자 행동 패턴과 기기 활동 자동으로 분석 ‣ 이상 행동 감지 시 즉각 경고 생성 및 대응
		향상	‣ 고급 행동 분석 기능을 도입 ‣ 비정상적인 사용자 활동과 기기 동작을 더욱 정밀하게 탐지 ‣ AI·ML을 활용하여 사용자 및 기기의 행동 패턴 학습 ‣ 지속적으로 변화하는 패턴에 따라 실시간 대응
		최적화	‣ AI 기반 자율적인 사용자 및 기기 동작 분석 시스템 구축 ‣ 비정상적인 활동 예측 및 사전 차단 ‣ 보안 정책을 자동으로 조정하여 최소 권한 부여
위협 인텔리전스 통합	외부의 보안 위협 정보를 수집하고 이를 기업 내 보안 시스템에 적용하여 위협 대응 능력을 향상시키는 기능이다. 위협 인텔리전스는 악성 IP 주소, 도메인, 취약점 정보 등 다양한 외부 데이터를 포함하며, 이를 통해 기업 내에서 발생할 수 있는 위협을 사전에 탐지하고 차단할 수 있다. 이 기능은 위협 데이터베이스와 연동되어 지속적으로 최신 정보를 업데이트하며, 보안 시스템과 통합되어 자동으로 대응 조치를 할 수 있다.	기존	‣ 외부의 보안 위협 정보를 수동으로 수집 후, 내부 보안 시스템에 적용 ‣ 외부 위협 인텔리전스를 수동으로 확인 ‣ 위협 데이터를 기업 내 시스템과 수동으로 연동
		초기	‣ 자동화된 위협 인텔리전스 통합 도구 도입 ‣ 외부에서 수집된 보안 정보를 실시간으로 내부 보안 시스템과 연동 ‣ 위협 인텔리전스를 자동으로 업데이트를 통한 위협 탐지 및 차단 기능 강화
		향상	‣ 고급 위협 인텔리전스 통합 시스템을 통해 외부 위협 정보를 더욱 세밀하게 분석, 내부 보안 정책과 실시간으로 연계 ‣ 위협 인텔리전스를 내부 시스템과 통합
		최적화	‣ AI 기반의 위협 인텔리전스 시스템을 구축 ‣ 외부 위협 정보 실시간으로 수집, 분석, 적용 ‣ 자율적으로 위협 인텔리전스를 기반으로 보안 정책 업데이트

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
자동화된 동적 정책	실시간으로 발생하는 보안 이벤트와 분석 결과를 기반으로 네트워크의 보안 정책을 자동으로 변경하는 기능이다. 이는 보안 위협이나 비정상적인 활동이 감지되었을 때, 사전에 정의된 정책을 자동으로 적용하거나 새로운 정책을 실시간으로 생성하여 네트워크 보안을 강화하는 데 사용된다. 예를 들어, 특정 사용자의 행동이 이상하다고 판단되면 그 사용자의 접근권한을 자동으로 제한하거나, 네트워크 세그먼트를 재조정할 수 있다. 자동화된 동적 정책은 빠르고 유연한 대응을 가능하게 하여, 보안 사고를 최소화할 수 있다.	기존	‣ 기본적인 보안 정책을 수동 관리 ‣ 보안 이벤트가 발생할 경우 관리자가 직접 정책을 수정하여 대응 ‣ 정책 변경이 수동으로 이루어지며, 보안 사고 발생 후 대응
		초기	‣ 자동화된 정책 관리 시스템을 도입 ‣ 보안 이벤트 발생 시 자동 정책 변경 및 적용 ‣ 위협이 감지되면 사전 정의 정책을 자동 실행
		향상	‣ 동적 정책을 실시간으로 조정하여, 보안 이벤트 발생 시 즉각적으로 새로운 정책을 생성하고 적용 ‣ 위협 탐지와 연계하여 동적으로 정책 조정
		최적화	‣ AI 기반의 자동화된 동적 정책 시스템 구축 ‣ 보안 이벤트 분석 결과에 따라 자율적인 정책 조정 ‣ 실시간으로 네트워크의 보안 상태를 모니터링하고, 상황에 따라 정책을 유연하게 변경

8. 자동화 및 통합

자동화 및 통합 교차 기능에 대해서는 각각 정책 통합, 중요 프로세스 자동화, 인공 지능, 보안 통합, 자동화 및 대응, 데이터 교환 표준화, 보안 운영 조정 및 사고 대응 세부역량 등을 정의하였다.

표 3-39 자동화 및 통합 교차 기능에 대한 세부역량 및 성숙도 정의

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
정책 통합	기업 내 보안 정책을 자동으로 조정하고, 여러 시스템과 네트워크 장비에 일관된 정책을 적용하는 프로세스이다. 보안 이벤트 발생 시 실시간으로 정책을 변경하거나 조정할 수 있으며, 이를 통해 신속하고 일관된 보안 대응이 가능해진다.	기존	‣ 기업 내 보안 정책을 수동 관리 ‣ 각 시스템에 개별적으로 적용 ‣ 정책 조정 시 수동으로 각 시스템에 변경 사항을 반영
		초기	‣ 자동화된 정책 통합 시스템을 도입 ‣ 보안 정책을 중앙에서 관리하고 여러 시스템에 동시 적용 ‣ 정책 변경 자동화
		향상	‣ 정책 통합 시스템을 고도화하여 실시간 보안 이벤트를 기반 정책 동적 조정 ‣ 위협에 따라 즉각적으로 정책 수정/적용하는 자동화된 프로세스 정착
		최적화	‣ AI 기반 자율 정책 통합 시스템 도입 ‣ 상황에 맞게 정책 자동 조정 ‣ 보안 이벤트를 실시간으로 분석하여 필요한 정책 변경을 자율적으로 수행 ‣ 정책 적용이 모든 시스템에 빠르게 동기화

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
중요 프로세스 자동화	보안 및 운영에 필요한 핵심 프로세스를 자동화하여, 업무의 효율성을 높이고 인적 오류를 줄이는 것을 목표로 한다. 이는 중요한 시스템 이벤트 처리, 데이터 백업, 장애 대응 등의 프로세스를 포함한다.	기존	▸ 핵심 보안 및 운영 프로세스 수동으로 관리 ▸ 특정 사건이 발생할 때마다 관리자가 직접 개입하여 처리 ▸ 자동화 도구의 제한적 사용 ▸ 수동 절차에 의존
		초기	▸ 중요한 프로세스에 대한 자동화 도구를 도입 ▸ 반복적인 작업과 기본적인 보안 절차 자동으로 처리 ▸ 데이터 백업 및 기본 장애 대응과 같은 주요 업무 자동화
		향상	▸ 자동화된 프로세스를 확장하여, 보안 사고 발생 시 신속한 자동 대응 ▸ 주요 보안 이벤트에 대한 실시간 경고 및 대응 시스템이 도입
		최적화	▸ AI·ML을 기반으로 모든 중요 프로세스가 자율적으로 운영 ▸ 이상 상황 발생 시 즉각 대응 ▸ 자동화 시스템은 모든 프로세스를 실시간으로 최적화 ▸ 업무 중단 없이 중요한 프로세스를 자동으로 조정
인공 지능	보안 위협을 감지하고 분석하는 데 있어 인간의 개입을 최소화하고, 네트워크와 시스템에서 발생하는 데이터를 기반으로 보안 결정을 자동화하는 기능을 제공한다.	기존	▸ AI 기술이 적용되지 않은 상태 ▸ 수동 분석과 경고 시스템에 의존 ▸ 데이터를 수동으로 수집하고 분석 ▸ 수동적 보안 위협 대응
		초기	▸ 기본적인 AI 기반 도구를 도입 ▸ 보안 이벤트를 분석하고 패턴 식별 ▸ AI가 보안 위협을 자동으로 탐지 및 경고 생성 ▸ 기본적인 자동 대응 가능
		향상	▸ AI 기반의 보안 시스템 고도화를 통한 실시간위협 탐지 및 대응 ▸ AI는 복잡한 활동을 분석하여 보다 정교한 위협 탐지와 실시간 대응 수행
		최적화	▸ AI가 모든 보안 시스템에 완전히 통합 ▸ 자율적으로 보안 위협을 감지하고 대응하며, 정책을 동적으로 조정 ▸ AI는 데이터와 행동 패턴을 학습하여 지속적으로 보안을 최적화 ▸ 잠재적 위협 사전 차단
보안 통합, 자동화 및 대응 (SOAR)	SOAR는 보안 이벤트에 대한 대응을 자동화하고, 여러 보안 도구와 시스템을 통합하여 일관된 보안 통합을 수행하는 시스템이다. 이를 통해 기업은 보안 사고에 신속하게 대응하고, 반복적인 작업을 자동화하여 운영 효율성을 높일 수 있다.	기존	▸ 보안 도구와 시스템이 각각 독립적으로 운영 ▸ 수동 대응에 의존 ▸ 보안 사고 발생 시 여러 도구에서 데이터를 수집 및 분석하며, 대응 절차도 개별적으로 수행
		초기	▸ SOAR 시스템을 도입 ▸ 보안 도구와 시스템을 통합하고, 기본적인 보안 이벤트에 대한 자동화된 대응 절차 마련 ▸ 보안 이벤트가 발생하면 여러 시스템에서 데이터를 수집하여 중앙에서 대응
		향상	▸ SOAR 시스템 고도화 ▸ 복잡한 보안 사고에 대해 자동화된 대응과 실시간 통합 수행 ▸ 보안 경고가 발생하면 즉각적인 대응 가능 ▸ 여러 도구와 연동하여 신속하게 위협 차단
		최적화	▸ AI·ML 기반의 SOAR 시스템을 통해 자율적인 보안 대응 수행 ▸ 모든 보안 이벤트 중앙에서 자동으로 처리 ▸ 대응 프로세스가 최적화되어 기업 전반에서 실시간 대응 가능 ▸ 자율 통합을 통해 보안 사건 관리 자동으로 수행

세부 역량	세부역량 설명	성숙도 수준	성숙도 수준에 따르는 정의
데이터 교환 표준화	기업 내외부에서 발생하는 다양한 데이터를 일관된 형식으로 관리하고, 보안 시스템 간에 효율적으로 데이터를 공유할 수 있도록 하는 프로세스이다. 이를 통해 여러 시스템에서 수집된 데이터를 통합적으로 분석하고, 보안 위협에 대응할 수 있다.	기존	‣ 각 시스템에서 수집된 데이터를 상이한 형식으로 저장 ‣ 비효율적 데이터 교환 ‣ 보안 시스템 간 데이터 교환 수동으로 이루어지며, 분석 속도 느림
		초기	‣ 데이터 교환 표준을 도입 ‣ 기업 내 모든 시스템에서 일관된 형식으로 데이터를 저장하고 공유 ‣ 보안 시스템 간 데이터 교환 자동화
		향상	‣ 데이터 교환 표준화가 고도화되어, 다양한 외부 시스템 및 파트너와도 데이터 공유 가능 ‣ 데이터 교환 절차 실시간 수행 ‣ 여러 보안 도구 간의 상호 운용성 개선
		최적화	‣ AI를 통해 데이터 교환 표준화 자율적 관리 ‣ 외부 파트너와의 데이터 교환까지 실시간 자동화 ‣ 모든 시스템에서 일관된 데이터 형식이 적용 ‣ 보안 위협이 발생할 때마다 실시간으로 데이터를 교환하고 분석
보안 운영 조정 및 사고 대응	기업 내 보안 사고가 발생했을 때, 이를 신속하게 대응하고 기업 내 여러 부서와 조율하여 보안 문제를 해결하는 프로세스를 의미한다. 이를 통해 보안 사고가 발생할 때 적절한 대응 절차를 신속하게 이행할 수 있으며, 피해를 최소화할 수 있다.	기존	‣ 보안 사고 발생 시 대응 절차 수동으로 수행 ‣ 보안 팀이 수동으로 여러 부서와 소통하고 조정 ‣ 정형화되어 있지 않은 보안 사고 대응 절차 ‣ 보안 사고 발생 후 대응
		초기	‣ 보안 사고 대응 계획 수립 ‣ 사고 대응 절차를 표준화 ‣ 기업 내 여러 부서와 효율적 협력 ‣ 보안 사고가 발생 시 자동화된 경고 생성 ‣ 보안 팀과 관련 부서 빠르게 대응
		향상	‣ 사고 대응 절차가 자동화 ‣ 보안 운영 팀과 다른 부서 간 실시간 조율 ‣ 보안 사고가 발생하면 즉시 대응 팀이 경고를 받고, 각 부서가 신속하게 협력 ‣ 자동화된 보고 시스템을 통해 보안 사고의 진행 상황 지속적 공유
		최적화	‣ AI 기반 사고 대응 및 운영 조정 시스템 도입 ‣ 보안 사고가 발생하기 전 예측하고 선제적 대응 ‣ 사고 대응 절차는 완전 자동화 ‣ 보안 팀과 관련 부서가 신속하고 일관된 대응 수행 ‣ 자율적인 조정 시스템을 통해 사고 발생 시 모든 관련 부서 실시간 협력 ‣ 대응 결과 즉시 보고

| 제3절 |

제로트러스트 성숙도 모델 기반 구현 방안

제로트러스트를 기업망에 적용하기 위해서는 체계적이고 단계적인 접근이 필요하며, 이를 구현하기 위해서는 다양한 보안 기능·세부역량과 성숙도를 고려한 전략이 요구된다. 아래에서는 이러한 세부역량과 성숙도를 바탕으로 기업망에 제로트러스트를 적용·구현하는 방법을 설명한다. 그러나, 이 구현 방안이 절대적인 것은 아니며, 기술한 순서가 시간이나 중요도를 의미하는 것은 아니다. 가급적 사용자 및 자산에 대한 인벤토리부터 시작하는 것이 적절할 수 있으나, 각 기업은 비즈니스 모델과 규모, 보안 목표, 네트워크 아키텍처, 준수해야 하는 규정 등에 따라 다르게 설정할 수 있다.

1. 식별자·신원 성숙도 기반 구현 방안

먼저, 기업은 1.1.1 사용자 인벤토리를 구축하는 것으로 시작해야 한다. 모든 사용자를 식별하고 이를 체계적으로 관리할 수 있는 인벤토리를 생성하는 것이 중요하다. 초기 단계에서는 기본적인 사용자 데이터베이스를 구축하고, 이를 정기적으로 업데이트하는 시스템을 마련한다. 이후, 자동화된 도구를 사용해 사용자의 식별 정보를 지속적으로 관리하고, 이를 기반으로 적절한 보안 조치를 취할 수 있도록 발전시켜야 한다.

1.1.2 ID 연계 및 사용자 자격 증명 관리는 기업망에서 다양한 인증 시스템을 통합하기 위한 핵심 기능이다. 초기에는 기업 내에서 사용되는 ID와 인증 시스템을 표준화하고, 이를 기업의 ID 관리 시스템에 통합한다. 이후, ID 연계를 통해 여러 시스템 간의 사용자 인증을 통합하고, 최종적으로는 전사적 수준에서 단일 ID 관리 체계를 구축해 모든 시스템에서 일관된 인증을 지원한다.

1.2.1 다중인증 (MFA) 도입도 필수적이다. 초기 단계에서는 기본적인 MFA 시스템을 구축하고, 기업 내 모든 사용자가 이를 통해 인증을 받도록 한다. 이후, MFA 시스템을 더욱 발전시켜 다양한 인증 요소를 통합하고, 외부 사용자까지도 안전하게 인증할 수 있도록 확장해야 한다. 최적화 단계에서는 피싱 방지 기능이 적용된 MFA 시스템을 통해 사용자 행동 분석을 기반으로 동적으로 인증 절차를 조정한다.

1.2.2 지속 인증을 도입해 사용자가 네트워크에 접속해 있는 동안에도 지속적으로 인증을 요구할 수 있다. 초기 단계에서는 시간 기반 인증을 도입해 일정 시간마다 재인증을 요구한다. 이후, 사용자의 활동과 권한 요청에 따라 인증 주기를 조정하는 시스템을 도입하고, 최종적으로는 실시간으로 사용자 활동을 분석해 동적으로 인증을 요구하는 수준으로 발전시킨다.

1.3.1 통합 ICAM 플랫폼을 통해 모든 ID 및 접근 관리 기능을 중앙에서 통합 관리해야 한다. 초기 단계에서는 기업 내 ID 및 접근 관리 시스템을 통합하는 작업을 수행하고, 이를 통해 모든 사용자의 ID를 중앙에서 관리한다. 이후, 이 시스템을 더욱 확장해 기업 내 모든 보안 시스템과 통합하고, 최종적으로는 AI 기반의 ICAM 플랫폼을 구축해 모든 ID와 접근권한을 실시간으로 관리한다.

1.3.2 행동, 컨텍스트 기반 ID 및 생체 인식 기술을 통해 사용자 인증의 정확성과 보안을 더욱 강화할 수 있다. 초기 단계에서는 기본적인 행동 분석 도구를 사용해 사용자 활동을 모니터링하고, 이를 통해 비정상적인 행동을 탐지한다. 이후, 상황적 요소와 생체 인식을 추가해 사용자 인증의 신뢰성을 높이고, 최종적으로는 모든 인증 과정에 이를 통합해 실시간으로 보안 위협을 탐지한다.

1.4.1 조건부 사용자 접근을 구현해야 한다. 처음에는 전통적인 역할 기반 접근제어(RBAC)를 적용해 사용자의 역할에 따라 접근권한을 부여한다. 이후, 상황에 맞게 접근권한을 동적으로 조정할 수 있는 시스템을 도입하고, 최종적으로는 AI를 통해 실시간으로 접근권한을 조정하는 수준까지 성숙도를 높여야 한다.

1.4.2 최소 권한 접근제어를 통해 기업망의 보안을 더욱 강화할 수 있다. 초기 단계에서는 사용자가 업무 수행에 필요한 최소한의 권한만을 부여하는 정책을 수립한다. 이후, 이 정책을 자동화된 시스템으로 발전시켜 모든 사용자의 접근권한을 지속적으로 모니터링하고, 필요할 때 권한을 자동으로 조정한다.

2. 기기 및 엔드포인트 성숙도 기반 구현 방안

2.1.1 기기 감지 및 규정 준수 관리를 통해 네트워크에 연결된 모든 기기의 보안 상태를 평가하고 관리해야 한다. 초기 단계에서는 자동화된 감지 시스템을 도입해 실시간으로 기기를 탐지하고, 규정 준수 여부를 평가하여 비준수 기기에 대한 경고 및 접근 제한 기능을 설정한다. 이후, 다양한 규정 기준을 적용하고, 비준수 기기에 대해 자동으로 교정 조치를 취하며 규정 준수 상태에 따라 접근 권한을 동적으로 부여한다. 최종적으로는 AI 기반의 실시간 규정 준수 평가와 조치 자동화를 통해 보안을 최적화하고, 규정 준수 데이터와 보안 분석을 통합해 기기 보안을 더욱 강화한다.

2.2.1 실시간 검사를 통한 기기 권한 부여는 기기의 보안 상태를 평가해 네트워크 접근권한을 부여하는 과정을 의미한다. 초기에는 수동으로 기기 상태를 평가하고, 필요 시 접근권한을 부여한다. 이후, 자동화된 시스템을 통해 실시간으로 기기 상태를 평가하고, 동적으로 접근권한을 조정하는 수준으로 발전시킨다.

2.3.1 기기 인벤토리 관리를 통해 모든 네트워크에 연결된 기기를 체계적으로 관리해야 한다. 초기 단계에서는 자동화된 기기 인벤토리 시스템을 도입해 모든 기기를 실시간으로 기록하고, 운영체제, 위치 등 세부 정보를 포함한 인벤토리를 구축한다. 이후, 기기 인벤토리를 지속적으로 업데이트하고 비인가된 기기를 탐지하며, 인벤토리 데이터를 분석해 보안 취약점을 파악하여 대응 전략을 마련한다. 최종적으로는 AI 기반의 인벤토리 관리 솔루션을 통해 기기 관리를 완전 자동화하고, 예측 분석을 통해 기기 보안을 최적화한다.

2.3.2 통합 엔드포인트 관리 및 모바일 기기 관리를 통해 모든 엔드포인트와 모바일 기기를 중앙에서 관리해야 한다. 초기 단계에서는 기본적인 엔드포인트 보안 도구를 도입하고, 이후, 이를 확장해 모바일 기기 관리(MDM) 시스템을 통합하며, 최종적으로는 모든 엔드포인트를 중앙에서 실시간으로 관리하고 보호하는 시스템을 구축한다.

2.4.1 엔드포인트 및 확장된 탐지·대응(EDR 및 XDR) 기능을 도입해 모든 엔드포인트에서 발생하는 보안 위협을 실시간으로 탐지하고 대응할 수 있어야 한다. 초기에는 기본적인 EDR 시스템을 도입해 엔드포인트에서 발생하는 위협을 탐지하고 대응한다. 이후, 이를 XDR 시스템으로 확장해 네트워크 전반에서 발생하는 위협을 종합적으로 탐지하고 대응할 수 있도록 발전시킨다.

2.4.2 자산, 취약성 및 패치 관리 자동화를 통해 네트워크 내 모든 자산을 안전하게 관리해야

한다. 초기에는 주요 자산과 취약성을 수동으로 관리하고, 필요 시 패치를 적용한다. 이후, 자동화된 시스템을 도입해 자산, 취약성, 패치 관리를 실시간으로 수행하고, 최종적으로는 AI 기반의 시스템을 통해 모든 관리를 자동화하고 최적화한다.

3. 네트워크 성숙도 기반 구현 방안

제로트러스트 네트워크 성숙도를 설정하기 위해서는 네트워크의 다양한 보안 요소들을 단계적으로 관리하고 발전시켜 나가야 한다. 매크로 세그멘테이션, 마이크로 세그멘테이션, 소프트웨어 정의 네트워킹(SDN), 위협 대응, 트래픽 암호화, 데이터 흐름 매핑, 네트워크 회복성과 같은 요소들은 네트워크 보안을 체계적으로 강화하기 위해 중요한 역할을 한다. 이러한 보안 요소들은 네트워크의 성숙도 단계에 따라 점차 자동화되고, 실시간으로 대응할 수 있는 자율적인 시스템으로 발전하게 된다.

3.1.1 매크로 세그멘테이션은 초기 단계에서 네트워크 보안을 강화하기 위한 기본적인 방법으로 사용된다. 매크로 세그멘테이션은 네트워크를 큰 단위로 나누어 주요 자산과 민감한 시스템을 독립된 네트워크로 분리하는 과정이다. 이를 통해 네트워크 전반에 걸친 보안 사고의 확산을 방지하고, 각기 다른 네트워크에 맞는 보안 정책을 적용할 수 있게 한다. 성숙도가 높아지면, 마이크로 세그멘테이션으로 발전하게 된다.

3.1.2 마이크로 세그멘테이션은 네트워크 내부에서 더욱 세부적으로 구분된 세그먼트를 구축하여, 각 워크로드와 애플리케이션에 고유한 보안 정책을 적용한다. 이를 통해 세그먼트 간의 트래픽을 세밀하게 통제하고, 워크로드별로 독립적인 보안 관리가 가능해진다. 최종적으로는 AI 기반의 자동화된 세그멘테이션 시스템을 도입하여 실시간으로 트래픽을 모니터링하고, 위협이 감지되면 즉시 보안 정책을 자동으로 조정할 수 있는 자율적인 보안 체계로 발전한다.

3.1.3 소프트웨어 정의 네트워크(SDN)는 네트워크 성숙도를 더욱 높이기 위해 중요한 역할을 한다. SDN은 네트워크 인프라를 중앙에서 관리하고, 네트워크를 동적으로 제어할 수 있는 기술로, 네트워크의 보안 정책을 유연하게 적용할 수 있게 한다. 초기에는 기본적인 네트워크 구성을 중앙에서 관리하는 방식으로 시작되지만, 이후에는 네트워크 트래픽의 흐름을 실시간으로 제어하고, 보안 정책을 동적으로 조정할 수 있는 체계로 발전시켜야 한다. 이를 통해 네트워크 내에서 발생하는

위협에 즉각적으로 대응하고, 변화하는 보안 상황에 맞춰 유연하게 대응할 수 있다.

3.2.1 위협 대응은 네트워크 보안의 핵심 요소로, 초기 단계에서는 네트워크에서 발생하는 비정상적인 트래픽을 모니터링하고 경고를 생성한다. 이 단계에서는 수동으로 경고를 분석하고 대응하는 방식이 주를 이루지만, 성숙도가 높아지면 자동화된 시스템으로 발전시켜야 한다. 이를 통하여 네트워크 전반뿐만 아니라 엔드포인트, 서버, 클라우드 등 다양한 요소에서 발생하는 위협을 종합적으로 분석하고 대응할 수 있으며, 이를 통해 보안 위협에 대해 보다 빠르고 자동화된 대응이 가능해진다. 최종적으로는 AI 기반의 자율 보안 시스템이 도입되어, 위협이 실시간으로 탐지되고 즉시 차단되는 수준으로 발전하게 된다.

3.3.1 트래픽 암호화도 네트워크 보안에서 매우 중요한 역할을 한다. 초기 단계에서는 중요한 데이터를 보호하기 위해 기본적인 전송 계층 보안(SSL/TLS) 암호화가 적용된다. 이를 통해 네트워크를 통해 이동하는 민감한 데이터를 보호하고, 데이터 유출을 방지할 수 있다. 성숙도가 높아짐에 따라 네트워크 전반에 걸쳐 더욱 정교한 암호화 기술을 적용해야 하며, 데이터 흐름이 발생하는 모든 구간에서 암호화가 이루어지도록 확장한다. 또한, 암호화 키 관리 시스템을 도입하여 암호화된 데이터의 무결성을 유지하고, 권한이 부여된 사용자만 데이터에 접근할 수 있도록 보안을 강화해야 한다.

3.4.1 데이터 흐름 매핑은 네트워크에서 데이터가 어떻게 이동하는지를 명확하게 파악하고 관리하는 데 중요한 역할을 한다. 초기에는 네트워크 내 주요 데이터 흐름을 수동으로 매핑하고, 데이터를 안전하게 이동시킬 수 있는 기본적인 보안 정책을 수립하는 데 중점을 둔다. 이후에는 자동화된 데이터 흐름 매핑 도구를 도입해 네트워크 내 데이터 흐름을 실시간으로 분석하고, 잠재적인 보안 취약점을 파악한다. 성숙도가 높아지면 데이터 흐름을 보다 정밀하게 모니터링하고, 트래픽 이동 경로에 대한 보안 정책을 자동으로 조정하는 체계로 발전한다. 이를 통해 민감한 데이터가 안전하게 이동하고 저장될 수 있도록 지속적으로 관리할 수 있다.

3.5.1 네트워크 회복성은 네트워크에서 보안 사고가 발생했을 때 신속하게 복구할 수 있는 능력을 의미한다. 초기 단계에서는 기본적인 백업과 복구 절차를 마련하고, 보안 사고가 발생했을 때 수동으로 복구하는 방식이 주를 이룬다. 성숙도가 높아지면 재해 복구(DR) 및 비즈니스 연속성(BC) 계획을 도입하여, 네트워크 장애나 보안 사고가 발생했을 때 자동으로 복구 절차가 실행되도록

발전시킨다. 최종적으로는 AI 기반의 예측 분석 시스템을 통해 네트워크에서 발생할 수 있는 장애나 위협을 사전에 감지하고, 문제가 발생하기 전에 예방할 수 있는 자율 회복성 체계를 구축하는 것이 목표다. 이를 통해 네트워크가 중단 없이 운영되고, 보안 사고에도 신속하게 대응할 수 있는 회복성을 확보하게 된다.

4. 시스템 성숙도 기반 구현 방안

제로트러스트 모델에서 시스템 관리는 기업망의 보안을 강화하는 데 핵심적인 역할을 하며, 접근 통제, PAM(Privileged Access Management), 자격 증명 관리, 네트워크 세분화 및 그룹 간 이동, 시스템 환경에 따른 정책 관리와 같은 요소로 분류하여 각각의 성숙도를 발전시켜 나가는 것이 중요하다.

먼저, 4.1.1 접근 통제는 시스템 보안의 기본 요소로, 초기 단계에서는 단순한 역할 기반 접근제어(RBAC)를 통해 사용자 권한을 설정하고 관리한다. 이 단계에서는 각 사용자의 역할에 따라 정해진 권한을 부여하며, 수동으로 접근제어를 관리하는 방식이 주를 이룬다. 이후에는 속성 기반 접근제어(ABAC)로 발전하게 되며, 사용자의 상황, 기기 상태, 위치 등의 속성을 기반으로 접근권한을 동적으로 조정할 수 있게 된다. 성숙도가 높아지면 AI 기반의 동적 접근 통제 시스템을 도입해, 사용자나 기기의 실시간 상태를 분석하고, 신뢰도가 변할 때마다 접근권한을 자동으로 조정하는 자율적인 체계로 발전한다. 또한, 시스템에 영향을 미치는 명령 실행 시 실시간 신뢰도 재산정 및 위험 분석을 기반으로 지속적인 접근제어 정책을 적용한다.

4.2.1 PAM은 시스템 내에서 특권 계정을 관리하고, 이를 통해 민감한 데이터나 중요한 자산에 대한 접근을 제어하는 역할을 한다. 초기 단계에서는 특권 계정을 별도로 관리하며, 이를 통해 중요한 시스템에 접근할 수 있는 사용자의 수를 제한하고, 특권 계정을 수동으로 모니터링하는 방식이 사용된다. 이후 성숙도가 높아지면 자동화된 특권 계정 관리 시스템을 도입해, 특권 계정의 사용을 실시간으로 모니터링하고, 비정상적인 활동이 감지되면 즉시 접근을 제한하는 방식으로 발전한다. AI 기반의 PAM 시스템을 통해 특권 계정의 활동을 실시간으로 분석하고, 특권 사용 시 다중 인증(MFA)을 추가적으로 요구하는 등 보안을 강화한다.

4.2.2 자격 증명 관리는 사용자와 기기의 인증 정보를 안전하게 관리하는 기능으로, 초기에는

단순한 패스워드 기반 인증 시스템에 의존한다. 이 단계에서는 사용자 인증 정보를 수동으로 관리하며, 데이터베이스에 저장된 인증 정보를 기반으로 인증 절차가 이루어진다. 이후에는 다중 인증(MFA) 시스템을 도입하여 패스워드 외에도 추가적인 인증 요소를 요구하고, 인증 절차의 보안을 강화한다. 성숙도가 높아지면 인증서 기반 인증 및 생체 인증과 같은 고급 인증 방식을 도입해 자격 증명의 신뢰성을 높이며, 최종적으로는 AI 기반의 자격 증명 관리 시스템을 통해 인증 정보를 실시간으로 분석하고, 인증 과정에서 비정상적인 시도가 감지되면 자동으로 차단하는 수준으로 발전시킨다.

4.3.1 네트워크 세분화 및 그룹 간 이동은 네트워크를 더 작은 단위로 나누어 보안을 강화하고, 세분화된 네트워크 간의 이동을 안전하게 관리하는 역할을 한다. 초기에는 기본적인 네트워크 세분화를 통해 주요 자산과 민감한 시스템을 분리하고, 각 네트워크에 독립적인 보안 정책을 적용한다. 이후에는 마이크로 세그멘테이션으로 발전하여, 네트워크 내에서 각 세그먼트가 고유한 보안 정책을 갖도록 하며, 세그먼트 간 트래픽 이동을 동적으로 제어할 수 있는 체계로 발전시킨다. 최종적으로는 AI 기반의 네트워크 세분화 시스템을 통해 실시간으로 트래픽 이동을 모니터링하고, 그룹 간 이동을 자율적으로 관리하는 수준으로 발전한다.

마지막으로, 4.4.1 시스템 환경에 따른 정책 관리는 온프레미스에서 클라우드 환경으로의 전환에 따라 시스템 보안 정책이 어떻게 적용되어야 하는지를 다룬다. 초기에는 온프레미스 환경에 맞춘 보안 정책을 적용하며, 각 시스템에 맞는 보안 설정을 수동으로 관리한다. 이후 클라우드 환경으로의 전환이 이루어지면서 하이브리드 클라우드 보안 관리 체계를 도입해, 온프레미스와 클라우드 환경 간에 일관된 보안 정책을 유지하는 방향으로 발전시킨다. 성숙도가 높아지면, 클라우드 기반의 보안 관리 시스템을 통해 각 시스템 환경에 맞춘 정책을 실시간으로 조정하고 적용하는 자동화된 체계로 발전하게 된다.

5. 애플리케이션 및 워크로드 성숙도 기반 구현 방안

5.1.1 리소스 권한 부여 및 통합은 애플리케이션과 워크로드에 대한 접근권한을 적절하게 부여하고, 이를 통합 관리하는 과정을 의미한다. 초기 단계에서는 기본적인 역할 기반 접근제어(RBAC)를 통해 리소스 접근권한을 수동으로 관리한다. 이 단계에서는 조직 내에서 정해진 역할에 따라 리소스 권한을 부여하며, 역할 변경 시 수동으로 권한을 조정하는 방식이다. 이후 성숙도가

높아짐에 따라 속성 기반 접근제어(ABAC)를 도입해 사용자의 속성이나 상황에 맞게 권한을 동적으로 조정할 수 있는 체계로 발전시킨다. 최종적으로는 AI 기반의 접근 통제 시스템을 도입해 실시간으로 사용자와 워크로드의 상태를 분석하고, 필요한 경우 자동으로 권한을 재조정하는 자율적 시스템을 구축한다.

5.2.1 지속적인 모니터링 및 진행 중인 승인은 애플리케이션과 워크로드의 활동을 실시간으로 모니터링하고, 사용자의 접근권한을 지속적으로 확인하고 승인하는 기능을 포함한다. 초기에는 애플리케이션과 워크로드의 활동을 수동으로 모니터링하고, 비정상적인 활동이 감지되면 관리자가 이를 승인하거나 차단하는 방식으로 이루어진다. 이후에는 자동화된 모니터링 시스템을 도입해 모든 활동을 실시간으로 추적하고, 비정상적인 행동이 탐지되었을 때 자동으로 경고를 발행하거나 접근을 제한하는 수준으로 발전시킨다. 최종적으로는 AI 기반의 시스템을 통해 애플리케이션 활동이 자율적으로 모니터링되며, 승인 프로세스도 실시간으로 자동화되는 체계로 전환된다.

5.3.1 원격 접속은 제로트러스트 모델에서 중요한 보안 요소로, 특히 외부에서 애플리케이션과 시스템에 접근할 때 발생하는 보안 위험을 최소화하는 데 중점을 둔다. 초기 단계에서는 VPN이나 기본적인 보안 솔루션을 통해 원격 접속 보안을 강화한다. 이후에는 다중 인증(MFA) 및 조건부 접근제어를 도입해 원격 접속 시 사용자의 위치나 기기 상태에 따라 동적으로 보안 요구사항을 조정한다. 최종적으로는 AI 기반의 원격 접속 관리 시스템을 통해 모든 원격 접속이 실시간으로 모니터링되고, 보안 위협이 감지되면 즉시 차단되는 자율적 관리 체계로 발전한다.

5.4.1 안전한 애플리케이션 배포는 애플리케이션을 배포할 때 발생할 수 있는 보안 위협을 최소화하는 데 중점을 둔다. 초기에는 수동으로 애플리케이션 코드를 검토하고, 보안 취약점이 없는지 확인하는 방식으로 배포가 이루어진다. 이후에는 자동화된 CI/CD 파이프라인을 도입해 애플리케이션 배포 시 보안 검사를 자동화하고, 배포 후에도 애플리케이션의 보안 상태를 지속적으로 모니터링할 수 있는 체계를 구축한다. 성숙도가 높아지면 AI 기반의 애플리케이션 배포 관리 시스템을 통해 애플리케이션 배포 과정에서 실시간으로 보안 위협을 감지하고 대응하는 자율적인 시스템으로 발전시킨다.

5.4.2 애플리케이션 인벤토리는 조직 내에서 사용되는 모든 애플리케이션을 체계적으로 관리하는 데 중점을 둔다. 초기 단계에서는 주요 애플리케이션을 수동으로 인벤토리에 등록하고

관리한다. 이후에는 자동화된 애플리케이션 인벤토리 시스템을 도입해 실시간으로 애플리케이션 상태를 모니터링하고, 새로운 애플리케이션이 추가되거나 변경될 때마다 자동으로 업데이트되는 체계를 구축한다. 최종적으로는 AI 기반의 애플리케이션 관리 시스템을 통해 모든 애플리케이션이 자동으로 인벤토리에 등록되고, 보안 상태가 지속적으로 평가되는 체계로 발전하게 된다.

5.5.1 보안 소프트웨어 개발 및 통합은 애플리케이션 개발 초기 단계부터 보안을 내재화하는 것을 목표로 한다. 초기에는 소프트웨어 개발 과정에서 기본적인 보안 가이드라인을 적용하고, 코드 검토를 통해 보안 취약점을 수동으로 관리한다. 이후에는 자동화된 보안 코드 분석 도구를 도입해 개발 중인 소프트웨어에 대해 실시간으로 보안 검사를 수행하고, 취약점을 자동으로 감지하고 수정할 수 있는 체계를 구축한다. 최종적으로는 AI와 머신러닝을 통해 소프트웨어 개발 과정에서 발생하는 보안 문제를 예측하고, 자율적으로 해결할 수 있는 보안 개발 체계를 마련한다.

5.5.2 소프트웨어 위험 관리는 개발된 애플리케이션이 배포된 이후에도 보안 취약점을 지속적으로 관리하고, 이를 통해 보안 위험을 최소화하는 역할을 한다. 초기 단계에서는 소프트웨어의 보안 취약점을 수동으로 점검하고, 위험이 발견될 경우 수동으로 패치를 적용한다. 이후에는 자동화된 취약점 관리 시스템을 도입해 소프트웨어에서 발생할 수 있는 보안 취약점을 실시간으로 모니터링하고, 패치를 자동으로 배포하는 체계를 구축한다. 최종적으로는 AI 기반의 소프트웨어 위험 관리 시스템을 통해 모든 취약점이 자율적으로 감지되고, 패치와 수정이 자동으로 이루어지는 자율 보안 체계로 발전하게 된다.

6. 데이터 성숙도 기반 구현 방안

6.1.1 데이터 카탈로그 위험 정렬은 조직이 보유한 모든 데이터를 체계적으로 분류하고, 데이터의 위험 수준에 따라 보안 정책을 적용하는 과정을 의미한다. 초기 단계에서는 조직 내에서 사용되는 주요 데이터를 수동으로 분류하고, 데이터의 민감도와 중요도를 평가하는 방식으로 이루어진다. 이후, 자동화된 데이터 분류 시스템을 도입해 데이터를 실시간으로 분석하고, 각 데이터의 위험도를 자동으로 평가하는 체계를 구축해야 한다. 성숙도가 높아지면, AI 기반의 데이터 카탈로그 시스템을 통해 데이터 위험을 자율적으로 정렬하고, 민감한 데이터에 대해 자동으로 보안 조치를 취하는 수준으로 발전할 수 있다.

6.1.2 기업 데이터 거버넌스는 조직 내 데이터의 관리와 보호를 위한 정책과 절차를 정의하고, 이를 실시간으로 적용하는 과정을 포함한다. 초기 단계에서는 데이터 관리 정책을 수립하고, 수동으로 데이터 거버넌스를 실행하는 방식으로 운영된다. 이 단계에서는 데이터 사용에 대한 기본적인 가이드라인이 적용되고, 데이터 소유권과 책임이 명확하게 규정된다. 이후, 데이터 거버넌스 관리 도구를 도입해 데이터 거버넌스 정책이 조직 전반에서 자동으로 적용되도록 하며, 데이터 사용에 대한 규정을 지속적으로 모니터링하고 준수 여부를 확인하는 체계로 발전한다.

6.2.1 데이터 접근제어는 민감한 데이터에 접근할 수 있는 사용자를 제한하고, 데이터를 안전하게 보호하는 중요한 역할을 한다. 초기 단계에서는 역할 기반 접근제어(RBAC)를 통해 민감한 데이터에 대한 접근을 수동으로 관리한다. 이후, 성숙도가 높아지면 속성 기반 접근제어(ABAC)를 도입해 사용자의 상황, 위치, 기기 상태 등에 따라 동적으로 접근권한을 조정할 수 있는 체계를 구축해야 한다. 최종적으로는 AI 기반의 지능형 접근제어 시스템을 통해 실시간으로 데이터 접근을 모니터링하고, 위험이 감지되면 즉시 접근을 차단하거나 제한하는 자율적인 시스템으로 발전시킬 수 있다.

6.3.1 데이터 암호화 및 권한 관리는 데이터를 전송하거나 저장하는 과정에서 발생할 수 있는 보안 위협으로부터 데이터를 보호하는 역할을 한다. 초기 단계에서는 민감한 데이터를 보호하기 위해 기본적인 암호화 기술을 적용한다. 이후에는 암호화 적용 범위를 확대해 엔드투엔드 암호화를 도입하고, 네트워크 내에서 이동하는 모든 데이터가 암호화되도록 한다. 또한, 암호화 키 관리 시스템을 도입해 암호화된 데이터의 무결성을 유지하고, 권한 있는 사용자만이 데이터를 복호화할 수 있도록 관리해야 한다. 성숙도가 높아지면 AI 기반의 암호화 관리 시스템을 통해 데이터의 암호화 상태를 실시간으로 모니터링하고, 권한 부여와 복호화 과정이 자동으로 이루어지도록 한다.

6.4.1 데이터 라벨링 및 태그 지정은 데이터의 중요도와 민감도에 따라 적절한 보안 태그를 부여하는 작업을 의미한다. 초기 단계에서는 수동으로 데이터를 라벨링하고, 데이터의 민감도를 평가하는 방식으로 보안 정책이 적용된다. 이후, 자동화된 데이터 라벨링 도구를 도입해 데이터를 자동으로 분류하고, 민감한 데이터에는 적절한 보안 태그가 부여되도록 한다. 최종적으로는 AI와 머신러닝을 통해 데이터를 실시간으로 라벨링하고, 새로운 데이터가 생성될 때 자동으로 태그가 부여되는 자율적 데이터 관리 시스템으로 발전시킨다.

6.5.1 데이터 손실 방지(DLP)는 민감한 데이터가 외부로 유출되지 않도록 보호하는 중요한

보안 요소다. 초기 단계에서는 기본적인 데이터 유출 방지 정책을 수립하고, 수동으로 데이터를 모니터링하며, 민감한 데이터가 외부로 나가는 것을 차단한다. 이후에는 자동화된 DLP 솔루션을 도입해 네트워크 트래픽을 실시간으로 모니터링하고, 비인가된 데이터 유출이 감지되면 자동으로 차단하는 체계로 발전한다. 최종적으로는 AI 기반의 DLP 시스템을 통해 데이터 유출이 자율적으로 감지되고, 실시간으로 대응이 이루어지는 수준으로 발전할 수 있다.

마지막으로, 6.5.2 데이터 모니터링 및 감지는 데이터를 실시간으로 모니터링하고, 데이터의 사용 상태와 접근 패턴을 분석해 잠재적인 위협을 탐지하는 기능을 포함한다. 초기 단계에서는 데이터 사용 현황을 수동으로 모니터링하고, 비정상적인 사용 패턴이 감지되면 관리자가 이를 분석하고 대응하는 방식이다. 이후에는 자동화된 데이터 모니터링 시스템을 도입해 데이터 사용과 접근을 실시간으로 추적하고, 비정상적인 활동이 탐지되면 자동으로 경고를 발행하거나 접근을 차단하는 방식으로 발전한다. 최종적으로는 AI와 머신러닝을 통해 데이터 활동이 자율적으로 모니터링되고, 잠재적인 위협이 실시간으로 감지되어 대응할 수 있는 자율적 보안 관리 체계로 발전하게 된다.

7. 가시성 및 분석 성숙도 기반 구현 방안

7.1 모든 관련 활동 기록은 기업망 내에서 발생하는 모든 보안 이벤트, 사용자 활동, 시스템 로그를 기록하는 것을 의미한다. 초기 단계에서는 수동으로 주요 이벤트를 기록하고, 보안 관련 활동에 대한 기본적인 로그를 수집하는 수준이다. 이 단계에서는 주로 로그 데이터를 별도로 저장하여 사후 분석을 위한 참조 자료로 활용한다. 성숙도가 높아지면, 자동화된 로그 수집 시스템을 통해 네트워크와 시스템 전반에서 발생하는 모든 활동을 실시간으로 기록하고, 이를 분석에 활용할 수 있는 체계로 발전한다. 최종적으로는 AI 기반의 로그 분석 시스템을 통해 활동 기록이 실시간으로 모니터링되며, 비정상적인 활동이 탐지되면 즉각적인 대응이 가능해지는 자율적 로그 관리 체계로 발전할 수 있다.

7.2 중앙집중적인 보안 정보 및 이벤트 관리(SIEM)는 조직 내에서 발생하는 보안 이벤트와 로그 데이터를 한 곳에서 수집하고, 이를 분석해 보안 위협을 실시간으로 감지하는 시스템이다. 초기에는 각 시스템에서 발생하는 보안 이벤트를 개별적으로 모니터링하며, 중앙집중적 관리가 이루어지지 않는 상태다. 이후 성숙도가 높아짐에 따라 SIEM 도구를 도입해 모든 보안 이벤트를 중앙에서 관리하고, 실시간으로 분석할 수 있는 체계를 구축한다. 이를 통해 다양한 보안 이벤트를 한 곳에서

모니터링하며, 즉각적인 대응이 가능해진다. 최종적으로는 AI 기반의 SIEM 시스템을 통해 보안 이벤트와 로그 데이터가 실시간으로 분석되고, 위협이 감지되면 자동으로 대응하는 자율적인 보안 관리 체계로 발전하게 된다.

7.3 보안 위협 분석은 수집된 로그와 보안 이벤트 데이터를 분석하여 잠재적인 보안 위협을 사전에 감지하고, 이를 통해 즉각적인 대응 조치를 취하는 것을 목표로 한다. 초기 단계에서는 수동으로 보안 데이터를 분석하고, 비정상적인 활동이나 위협이 발생했을 때 사후적으로 분석하여 대응하는 방식이다. 이후에는 자동화된 위협 분석 도구를 도입해 수집된 데이터를 실시간으로 분석하고, 위협이 감지되면 경고를 발행하거나 자동으로 대응할 수 있는 체계로 발전시킨다. 최종적으로는 AI와 머신러닝 기반의 위협 분석 시스템을 통해 보안 위협을 자율적으로 감지하고, 실시간으로 대응하는 자율 보안 체계로 발전하게 된다.

7.4 사용자 및 기기 동작 분석은 네트워크와 시스템에 접속하는 사용자와 기기의 행동 패턴을 분석하여 비정상적인 활동을 감지하는 기능을 포함한다. 초기 단계에서는 기본적인 사용자 행동 패턴을 수동으로 모니터링하고, 비정상적인 활동이 감지되면 수동으로 대응하는 방식이다. 이후 성숙도가 높아짐에 따라 사용자 및 기기 행동 분석 도구(UEBA)를 도입해 실시간으로 사용자와 기기의 활동을 추적하고, 비정상적인 패턴이 탐지되면 자동으로 경고를 발행하거나 접근을 차단하는 체계로 발전시킨다. 최종적으로는 AI 기반의 동작 분석 시스템을 통해 사용자와 기기의 행동을 실시간으로 모니터링하고, 위협을 자율적으로 감지하여 대응하는 체계로 발전한다.

7.5 위협 인텔리전스 통합은 외부에서 수집된 보안 위협 정보를 조직의 보안 시스템과 통합하여 최신 위협을 신속하게 감지하고 대응하는 기능을 의미한다. 초기 단계에서는 외부 위협 정보를 수동으로 수집하고 분석하여 조직 내 보안 정책에 반영하는 방식으로 운영된다. 이후에는 자동화된 위협 인텔리전스 통합 도구를 도입해 외부에서 수집된 위협 정보를 실시간으로 분석하고, 이를 조직 내 보안 시스템과 통합하여 위협 대응 속도를 높인다. 최종적으로는 AI 기반의 위협 인텔리전스 시스템을 통해 외부 위협 정보가 자율적으로 수집되고, 실시간으로 대응하는 자율적 보안 체계로 발전한다.

마지막으로, 7.6 자동화된 동적 정책은 보안 위협과 네트워크 상황에 맞춰 실시간으로 보안 정책이 자동으로 조정되는 체계를 의미한다. 초기 단계에서는 고정된 보안 정책을 수동으로

적용하고, 상황이 변할 때마다 관리자가 정책을 수동으로 조정하는 방식으로 운영된다. 이후 성숙도가 높아짐에 따라 정책 오케스트레이션 도구를 도입해 네트워크와 시스템의 상태에 맞춰 보안 정책이 자동으로 조정되는 체계를 구축하게 된다. 최종적으로는 AI 기반의 정책 오케스트레이션 시스템을 통해 보안 정책이 실시간으로 변화하는 보안 위협과 환경에 맞춰 동적으로 조정되는 자율 보안 체계로 발전한다.

8. 자동화 및 통합 성숙도 기반 구현 방안

8.1 정책 통합은 조직 내 다양한 보안 정책을 중앙에서 관리하고 일관되게 적용하는 것을 목표로 한다. 초기 단계에서는 개별 시스템이나 네트워크에 맞춰 수동으로 정책을 관리하는 방식이 주를 이룬다. 이 단계에서는 보안 정책이 분산되어 있어, 정책 적용에 일관성이 부족할 수 있다. 성숙도가 높아지면, 정책 오케스트레이션 도구를 통해 조직 전반에서 보안 정책을 통합 관리하고, 모든 네트워크와 시스템에 일관되게 적용하는 체계로 발전시켜야 한다. 최종적으로는 AI 기반의 정책 통합 시스템을 통해 보안 정책이 실시간으로 자동 조정되고, 새로운 보안 위협이나 환경 변화에 맞춰 동적으로 반영되는 자율적 체계로 발전할 수 있다.

8.2 중요 프로세스 자동화는 조직 내에서 반복적이거나 중요한 보안 프로세스를 자동화하는 작업을 포함한다. 초기 단계에서는 보안 프로세스가 수동으로 관리되며, 반복적인 보안 작업이나 위협 대응 절차가 자동화되지 않는 상태일 수 있다. 이후, 자동화된 워크플로우 관리 시스템을 도입해 보안 프로세스의 자동화를 시작하고, 중요한 보안 프로세스나 위협 대응 절차를 자동화하는 체계로 발전시킨다. 최종적으로는 AI 기반의 자동화 시스템을 통해 중요한 보안 프로세스가 자율적으로 실행되며, 관리자의 개입 없이도 보안 작업이 자동으로 이루어지는 체계로 발전하게 된다.

8.3 인공지능(AI)은 보안 운영에서 발생하는 대규모 데이터를 실시간으로 분석하고, 위협을 예측하고 대응하는 데 중요한 역할을 한다. 초기 단계에서는 AI가 적용되지 않고, 수동으로 데이터 분석과 보안 작업이 이루어진다. 이후 성숙도가 높아짐에 따라 AI 기반 분석 도구를 도입해 보안 데이터와 위협 정보를 실시간으로 분석하고, 잠재적인 보안 위협을 사전에 예측할 수 있는 체계를 구축해야 한다. 최종적으로는 AI 기반의 자율 보안 시스템을 통해 보안 이벤트를 실시간으로 분석하고, 위협 대응 절차를 자율적으로 조정하는 체계로 발전할 수 있다.

8.4 보안 통합, 자동화 및 대응은 보안 이벤트와 위협에 대해 자동으로 대응할 수 있는 체계를 의미한다. 초기 단계에서는 보안 이벤트 발생 시 수동으로 대응하며, 이벤트 처리가 분산되어 있을 수 있다. 성숙도가 높아지면 SOAR 도구를 도입해 보안 이벤트를 중앙에서 관리하고, 대응 절차를 자동화하여 위협 발생 시 빠르고 일관된 대응이 가능하게 한다. 최종적으로는 AI 기반의 SOAR 시스템을 통해 보안 이벤트가 실시간으로 분석되고, 대응 절차가 자동으로 실행되어 위협을 신속히 차단하는 자율적인 보안 대응 체계로 발전한다.

8.5 데이터 교환 표준화는 조직 내외부에서 데이터를 안전하게 교환하기 위한 표준화된 프로세스와 기술을 도입하는 것을 의미한다. 초기 단계에서는 데이터 교환이 수동으로 이루어지고, 표준화된 절차 없이 데이터를 공유할 수 있다. 이후 성숙도가 높아지면 데이터 교환 표준화 도구를 도입해 데이터가 안전하게 교환될 수 있도록 보안 프로토콜과 표준을 적용하고, 외부 파트너나 시스템 간의 데이터 교환이 안전하게 이루어질 수 있는 체계를 구축해야 한다. 최종적으로는 AI 기반의 자율 데이터 교환 관리 시스템을 통해 모든 데이터 교환이 실시간으로 모니터링되고, 표준화된 보안 절차에 따라 자동으로 관리되는 체계로 발전한다.

8.6 보안 운영 조정 및 사고 대응은 보안 사고 발생 시 이를 신속하게 감지하고 대응하는 역할을 한다. 초기 단계에서는 보안 사고 대응 절차가 수동으로 관리되며, 보안 팀이 각 보안 사고에 대해 개별적으로 대응하는 방식이 주를 이룬다. 이후 성숙도가 높아지면 사고 대응 자동화 시스템을 도입해 보안 사고 발생 시 신속하게 대응 절차가 자동화되고, 사고 처리 속도가 크게 향상된다. 최종적으로는 AI 기반의 자율 사고 대응 시스템을 통해 보안 사고가 실시간으로 감지되고, 자동으로 대응 절차가 실행되어 사고의 영향을 최소화하는 자율적 보안 운영 체계로 발전할 수 있다.

이와 같이, 자동화 및 통합의 각 요소는 초기 단계에서 수동적이고 개별적으로 운영되지만, 성숙도가 높아지면서 점차 자동화되고, AI 기반의 자율적 관리 체계로 발전해 나간다. 이를 통해 조직은 보안 위협에 신속하게 대응하고, 보안 운영을 일관되게 관리하며, 궁극적으로 자율적인 보안 환경을 구축할 수 있다.

제로트러스트
가이드라인 2.0

제4장

제로트러스트 도입 준비 방안

| 제1절 | 제로트러스트 아키텍처 도입 고려사항

| 제2절 | 제로트러스트 아키텍처 도입을 위한 조직 내 역할 및 목표 설정

| 제3절 | 제로트러스트 아키텍처 구성 방안

| 제4절 | 제로트러스트 아키텍처 도입 준비 예시

| 제1절 |

제로트러스트 아키텍처 도입 고려사항

가이드라인 1.0의 3.2절에서는 제로트러스트로의 전환을 목표로 하는 기업이 목표 달성을 위한 전환 및 도입 계획을 수립할 때, 성숙도 모델 관점에서 고려해야 하는 원칙 및 기업 내외부 환경 관점에서 고려해야 할 사항을 언급한 바 있다. 이를 요약하면 다음 〈표 4-1〉과 같다.

표 4-1 가이드라인 1.0의 3.2절에서 제시한 제로트러스트 도입 고려사항

관점	설명
성숙도 모델 관점	▸ 최적화 수준은 절대로 단기적으로 달성할 수 있는 목표가 아님. 기업에서 가장 중요한 핵심 요소를 먼저 파악 후 이들을 중심으로 먼저 성숙도 수준을 높이면서, 다른 핵심 요소에 대한 성숙도가 따라갈 수 있는 장기적인 계획 및 실천 필요 ▸ 성숙도 모델은 제로트러스트 전환을 위한 여러 경로 중 하나로, 한 가지 경로만 존재하는 것이 아님. 어떤 경로를 선택하는 것이 바람직한지는 각 기업별 상황에 따라 다름 ▸ 모든 기업이 반드시 모든 핵심 요소에 대하여 최적화 수준을 도달해야 하는 것이 아님. 기업의 규모, 기업망 구성 방식, 리소스 종류 등에 대한 관리 수준과 필요성 등을 고려하여 최종적인 목표를 스스로 설정해야 함
기업 내·외부 환경 관점	▸ 기술: 현재 기업이 사용하고 있는 레거시 보안 기술 파악 및 제로트러스트 핵심 기능을 제공하는 기술·솔루션을 지속적으로 모니터링하여, 기존 기술을 대체·보완하는 방법 파악 필요 ▸ 기업 문화: 결정권자 및 이해관계자가 제로트러스트의 필요성을 인지할 수 있는 적극적인 노력 필요 ▸ 정책: 접근 주체가 리소스에 접근할 때에 대한 정책이 모두 변경될 것으로, 접근제어 정책과 신뢰도 평가 알고리즘을 정교하게 설정할 때 신중하게 접근 필요 ▸ 규제 환경: 사이버 위험을 줄이기 위한 국가 차원의 표준이나 지침(예, 보안적합성 검증 제도, 클라우드 서비스 보안인증 제도, ISMS-P)이 운용되고 있으므로, 이러한 규제 환경을 고려한 제로트러스트 도입 계획 수립이 중요

위 도입 고려사항은 기업이 제로트러스트 아키텍처를 도입하는 데 있어 기본적으로 고려해야 할 원칙을 정리한 것이다. 가이드라인 1.0 뿐만 아니라 미국을 중심으로 다양한 제로트러스트 관련 문서 및 참고 자료들이 발간되고 있음에도 불구하고, 제로트러스트 아키텍처를 도입하고자 하는 기업들이 제로트러스트에 관하여 잘못 이해하고 있는 경우가 많다.

기업 담당자들이 제로트러스트에 대해 바라보는 관점 및 이해 수준에서 차이가 있을 수 있으나,

제로트러스트와 관련한 용어 정의 및 개념을 잘못 이해함으로써 이해 관계자들끼리 의견이 일치되지 못하거나 각자 이해 수준에 괴리가 발생하는 경우 기업망에 제로트러스트 아키텍처를 도입하는데 있어 상당한 걸림돌이 될 수밖에 없다.

이 절에서는 기업 보안 담당자들이 제로트러스트 도입 과정에서 다양한 이해 관계자들과 합의하여야 하는 개념에 대해 명확한 이해를 돕는 고려사항을 다룬다.

1. 제로트러스트에 대한 명확한 이해

가이드라인 1.0, 그리고 본 문서 1장에서 제로트러스트에 대한 정의를 내리고 있으며, NIST SP 800-207 등 다양한 문서에도 그 개념을 명확히 설명하고 있음에도 불구하고 기업의 의사결정권자 및 도입 담당자들이 잘못 이해하는 경우가 있다.

예를 들어, 제로트러스트 아키텍처를 도입하면 경계 기반 보안 방식으로는 막을 수 없는 해킹 공격들을 원천 차단할 수 있는 것 아니냐고 생각하는 이들이 있으며, 특정 제로트러스트 기술이 제로트러스트 아키텍처를 구축하는 데 있어 필수적으로 반영되어야 한다고 생각하거나, 특정 레거시 보안 기술이 제로트러스트 철학과 반대되는 개념이므로 반드시 제거되어야 한다고 보는 시각들도 일부 존재한다.

제로트러스트에 대해 정확히 이해하기 위해서는, 본 가이드라인 외에도 제로트러스트를 정의하는 대다수 문서들이 가지고 있는 공통적인 개념을 다시 한번 생각해 볼 필요가 있다. 이 공통 개념은 다음과 같은 3가지 내용을 포함한다. 첫째, 기업망 내부 네트워크는 이미 침투당한 상태일 가능성을 포함하고 있으며, 둘째, 정확한(신뢰도 평가에 기반하고 지속적이며 동적인) 접근제어를 하고자 한다는 것이고, 마지막으로 제로트러스트는 특정 기술이 아니라 보안 개념, 패러다임, 아이디어의 집합이라는 것이다.

제로트러스트라는 단어의 사전적인 의미로 인하여 '신뢰 제거'에 초점을 맞출 수 있으나, 이보다는 접근제어 과정에서 '정확하게 신뢰도를 평가'하여야 한다는 개념으로 보아야 한다. 또한 제로트러스트 모델이 기존 경계 기반 보안 모델을 대체하기 위해 나온 배경으로 인하여 기업망 내부와 인터넷의 '경계를 제거'하는 것에 중점을 두려고 할 수 있으나, 그보다는 경계를 리소스 단위로 마이크로 세그멘테이션(Micro-Segmentation)하는 것이 훨씬 중요하게 받아들여야 하는 개념이다.

2.1절에서도 언급하였듯이, 제로트러스트 역시 기존 경계 기반 보안 모델과 마찬가지로, 최종적인 목표는 기업망 및 내부 리소스에 대한 보호이며, 이는 곧 내부 리소스를 불법적인 접근으로부터 보호하고 정당한 권한을 가진 사용자가 정상적으로 접근할 수 있도록 만드는 것을 의미한다. 따라서, 이러한 목적을 달성하기 위한 접근법에 대해서 제로트러스트의 성숙도 수준을 평가할 수는 있으나, 특정 보안 기술이 절대 제로트러스트가 아니라고 얘기할 수는 없는 것이다.

제로트러스트에 대한 오해를 나열하기에 앞서, 제로트러스트 기술 및 솔루션에 대해서는 다음과 같이 정의하고자 한다.

제로트러스트 기술·솔루션(Zero Trust Technology·Solution)은 제로트러스트 개념을 부분적으로 만족하는 혹은 지원하기 위한 요소 기술·솔루션이다. 여기에서 주의해야 할 것은 특정 제로트러스트 기술의 도입만으로 기업망에서 제로트러스트의 기본 원리를 달성할 수 없다는 점이다. 기업망 핵심 요소별 보안 기능은 1~2개의 제로트러스트 기술만으로 모두 만족할 수 없으며, 이들 기술·솔루션들은 현재 접근에 대한 신뢰도를 정확하게 평가할 수 있도록 통합·연동되어야 한다.

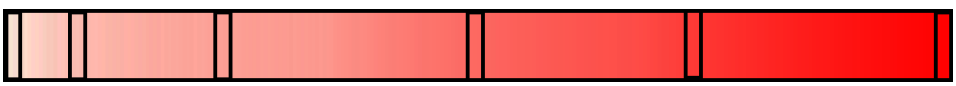
제로트러스트를 구축하고자 하는 보안 담당자뿐만 아니라 기업의 모든 구성원들은, 앞서 언급한 관점을 염두에 두고 제로트러스트에 대하여 다음과 같이 정확하게 이해하는 것이 바람직하다.

가. 레거시 보안 기술과 제로트러스트에 대한 이해

제로트러스트 기술과 레거시 보안 기술은 명확히 다르거나 구분되는 기술이 아니다. 제로트러스트 아키텍처 구축을 위해서는 레거시 보안 기술·솔루션을 모두 걷어내기보다, 적절히 유지하면서 새로운 보안 기술을 도입·연동하면서 제로트러스트 성숙도 수준을 끌어올릴 수 있다.

예를 들어, [그림 4-1]의 붉은색 막대그래프를 보면 어디서부터 붉은색인지에 대해 단정 짓기 매우 어려울 것이다. 심지어 흰색에 가까운 가장 왼쪽 부분조차도 약간의 붉은색을 띠고 있다고 느껴질 수 있다. 붉은색 자체를 보안성과 비교하여 생각해 보면, 보안 기술은 시간이 지나면서 [그림 4-1]의 막대그래프 중 왼쪽 부분에서 오른쪽으로 진화하고 있는 것과 유사한 관점으로 볼 수 있다.

그림 4-1 붉은색 막대그래프



과거에 활용해오던 레거시 보안 기술 역시 기본적으로는 앞서 언급한 보안 목표 즉 기업망 및 내부 리소스에 대한 보호를 추구하고 있으므로, 기본적으로는 제로트러스트의 초보적인 철학이 담겨 있다고 볼 수 있으며 기술 관점에서 성숙도가 낮을 수 있지만 절대 제로트러스트 기술이 아니라고 할 수 없다. 또한 기업망에 대해서 제로트러스트 성숙도를 평가할 때는 하나의 기술만으로 평가하는 것이 바람직하지 않으며, 기업의 상황과 지켜야 하는 규정, 보호하고자 하는 리소스에 대한 위험도 등을 종합적으로 분석하여야 한다.

따라서, 기업망의 제로트러스트 수준을 평가할 때, 망분리, VPN, 방화벽 등과 같은 특정 레거시 기술의 적용여부를 절대적인 기준으로 판단하는 것은 적절하지 않다.

물론, 망분리를 통해 인터넷망과 내부망을 물리적으로 분리하고 있는 환경에서는 클라우드 기반의 다양한 서비스라든지 외부 AI 기술에 대한 연동 등 기업의 필요성 혹은 고객에 의한 도입 요구가 발생할 수 있다. 신기술을 도입하는 과정에서 레거시 기술을 계속 이용하기 어렵다면 이로 인해 발생할 수 있는 보안 위협을 완화하여 보안성을 유지할 수 있는 조치를 함께 도입하는 것을 고려할 수 있을 것이다.

그러나 매우 민감한 데이터 혹은 리소스를 보유하고 있는 기업이라면, 망분리 기술과 동적 접근제어 기술, 내부망 위험 분석 기술을 같이 활용하는 것이 보안 측면에서 훨씬 적절할 것이다. 미 국방부 역시 민간 클라우드 서비스 활용 시, 데이터의 민감도에 따라 직접 접속, 논리적 망분리 및 물리적 망분리 기술을 적절하게 이용하고 있다. 제로트러스트 철학에서 경계하는 것은, 망분리 기술을 적용했으니 인터넷망과 물리적으로 차단된 내부 업무망은 안전할 것이라고 여겨(즉, 충분히 신뢰할 만하다고 평가하여) 업무망 혹은 내부 디지털 자산에 대한 추가적인 보호 조치를 더 이상 취하지 않는 경우일 뿐이다.

제로트러스트 아키텍처의 최종적인 목적은 일반적인 보안 아키텍처와 마찬가지로 결국 기업망의 핵심 디지털 자산을 보호하는 데 있으며, 따라서 레거시 기술이 적용되어 있다는 이유 하나만으로 제로트러스트의 성숙도 수준이 낮다고 평가하거나 이 기술을 제거해야 한다고 주장하는 것은 바람직하지 않다. 망분리를 통해 인터넷과 물리적으로 차단된 업무망에 대해서도, 강력한 인증 및 기기 보호 조치, 애플리케이션과 네트워크에 대한 세밀한 접근제어, 분석을 통한 가시성 확보 등을 통하여 기존보다 보안 수준을 높일 수 있다면 이 역시 제로트러스트 철학에 한 걸음 다가가는 것으로 볼 수 있다.

또한, 레거시 보안 기술은 실환경에서 오랫동안 활용된 경우가 많아 가격 대비 성능이 높고 안정적이며 검증된 기술이라는 장점 역시 존재한다. 제로트러스트의 성숙도를 끌어올리는 것에만 초점을 맞추다 보면 기존 기술·솔루션을 무조건 배제해야 하는 것으로 오해할 수 있으나, 기업의 목표와 환경, 규정 등에 따라 기업망 보안 수준을 끌어올리는 데 있어 기존 보유 중인 레거시 기술·솔루션을 보완·유지하면서 현재 도입되지 않았거나 고도화가 필요한 기술에 대해서만 새로 도입하는 등 전략적인 접근을 고려할 수 있다.

나. 완벽한 보안이 아닌 위험 완화

> 완벽한 보안이라는 것은 존재하지 않으며, 제로트러스트 철학을 모두 구현하더라도 지속적으로 위험을 완화하는 것을 목표로 해야 한다.

먼저 언급하고 싶은 것은, 보안에 대한 전문가라면 당연히 알고 있을 사실이지만 '완벽한 보안'이라는 것은 절대로 존재할 수 없다는 것이다. 제로트러스트 철학은 기본적으로 **'이미 공격당했을 가능성'을 염두에 두고 기업망의 위험을 완화하는 전략**이며, 이러한 전략이 기업망 전체에서 반영될 수 있도록 보안 기술을 도입함으로써 제로트러스트 아키텍처를 구축할 수 있게 되는 것이다. 가트너 역시, 제로트러스트와 관련한 보고서에서 다음과 같이 언급한 바 있다.

"CISO와 위험 관리 책임자는 제로트러스트가 사이버 위협을 제거할 것이라고 가정해서는 안 됩니다. 대신 제로트러스트는 위험을 줄이고, 공격의 영향을 제한합니다"

이뿐만 아니라, CISO 및 보안 실무자들이 추가로 이해하고 있어야 하는 사항은 다음과 같다.

- 제로트러스트 아키텍처를 구현하더라도, 해당 구조로 인해 발생할 수 있는 위협이 존재한다.
- 이론적으로는 완벽하더라도, 제로트러스트 기술·솔루션을 구현하는 과정에서 이미 내재하고 있거나, 도입 및 운용하는 과정에서 발생할 수 있는 취약점의 존재 여부를 지속적으로 확인해야 한다.

가이드라인 1.0의 3.4절에서도 언급하고 있듯, 첫 사항이 제로트러스트 아키텍처가 근본적인 취약점을 갖는다거나 기존 환경과 비교하여 더 취약해질 수 있음을 의미하지는 않는다. 공격자들은 늘 기업망의 빈틈을 찾아 공격을 시도할 뿐이며, 제로트러스트 아키텍처는 정책 엔진과 정책 관리자, 정책시행지점 등의 권한이 막강하며, 접근을 제어하는 과정에서 많은 정보를 수집하기

때문에 운영에 유의해야 함을 의미하는 것이다. 구체적인 위협과 이를 완화하는 방안은 (가이드라인 1.0의 〈표 3-4-1〉)를 참조할 수 있다.

참고 **제로트러스트 아키텍처 도입·운영 시 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

(출처: 가이드라인 1.0)

첫 사항이 제로트러스트 아키텍처의 논리적 구조로 인한 위협이라면, 둘째 사항은 기술·솔루션 도입 및 운용 과정에서 보안 취약점이 존재함으로써 발생할 수 있는 위협을 의미한다. 기업망에서 다양한 보안 솔루션의 도입으로 인하여 공격 대응 수준이 높아짐에 따라, 기업망에서 사용 중인 보안 기술의 취약점을 노리거나 보안 솔루션에 대한 공격 시도가 점차 늘고 있으며, 보안 담당자들은 사이버 위협 인텔리전스(CTI), 보안운영센터(SOC) 등을 활용하여 지속적으로 이들에 대한 보안 취약점 혹은 공격 사례가 없는지를 확인해야 한다.

다. '최적화 수준' 제로트러스트 아키텍처 구현의 완성

제로트러스트 아키텍처 구현은 단기간에 '최적화 수준'으로 완성하기 어려우며 장기적인 목표와 단계적 전략 수립이 필요하다.

기업망의 보안 담당자가 경영진 및 재무 담당자 등의 승인하에 제로트러스트 아키텍처 도입을 위한 계획을 세우더라도 여러 어려움을 극복할 수 있어야 한다. 일부 사례를 살펴보면, 제로트러스트 도입이 어렵지 않으며 단기간 내에 구축이 가능하다는 점을 강조하는 경우가 있다. 이 표현이 무조건 잘못된 의견이라고 볼 수는 없으나, 단기간 내에 구축이 가능하다는 것이 제로트러스트 아키텍처의 완성을 의미하는 것으로 해석해서는 안 되며, 제로트러스트의 철학을 바탕으로 기업망의 보안 수준과 성숙도를 부분적으로 개선할 수 있다고 해석하는 것이 정확할 것이다.

기업의 보안 담당자 및 경영진은 제로트러스트 기술·솔루션을 도입하는 것이 제로트러스트 아키텍처의 완성을 의미하는 것은 아니며, 지속적으로 보안성을 개선시켜 성숙도 수준을 끌어올리기 위한 장기간의 프로젝트임을 정확히 이해하여야 한다.

장기간의 프로젝트라는 것은 두 가지 측면에서 바라볼 수 있어야 하는데, 첫째는 기술 관점에서의 어려움이다. 앞서 언급한 제로트러스트 성숙도 모델 관점에서 보면, 가장 높은 최적화 수준에서는 AI 기반 사용자 행동 분석 및 신뢰도 검증, 실시간 위험 관리, 동적 접근제어, 자동화된 프로비저닝 등 기술적으로 상당히 높은 수준의 기술 구현을 요구하고 있다. 이 중 일부는 아직 구현이 되어 있지 않거나 혹은 충분한 검증이 이루어지지 않은 기술을 포함하므로 단기간 내에 이렇게 높은 제로트러스트 성숙도를 갖추는 것은 불가능하다.

둘째는 각 보안 기술 및 솔루션 간 연동의 어려움이다. 일부 기업들은 기업망 관점에서 상당히 넓은 영역을 포괄하는 보안 솔루션 체계를 구성하여 판매하고 있으나, 제로트러스트 아키텍처를 구축하는 것은 일반적으로 다양한 보안 기업들이 각자 전문성을 갖추어 개발한 솔루션들에 대한 연동을 요구하게 된다. 이는 제로트러스트는 특정한 영역에서의 보안 기술만으로 달성할 수 있는 것이 아니라, 기업망 관점에서 존재하는 모든 핵심 요소 및 이들을 보호하기 위한 보안 전략 및 기술들이 유기적으로 조합되어 구축되어야 하기 때문이다. 그러나 현재 솔루션 간 연동을 위한 보안 기능 및 인터페이스가 표준화된 형태로 정의되어 있지 않으며 보안 정책 관리 및 시행 과정이 기업별로 상이하여, 이들을 통합하여 연동하는 것은 상당한 어려움을 요구하게 된다. NIST SP 1800-35 및 일부 실증 사례에서도 제로트러스트 아키텍처를 구축하는 과정에서 솔루션 간 정책 연동의 어려움을 호소하는 경우가 있다.

또한, 이러한 기술적 어려움과 연동의 어려움이 어느 정도 해소된다 하더라도, 도입하고자 하는 기업은 최적화 수준의 제로트러스트를 성공적으로 구현하여 운영 중인 사례를 참고하기를 원할 것이지만 현재까지는 이에 대한 성공 사례가 많지 않다는 점도 단기간 내에 제로트러스트 도입이 쉽지 않은 또 다른 근거가 된다.

미 연방정부에 소속된 기관 중 제로트러스트 아키텍처의 구현과 도입을 가장 선도하고 있는 국방부의 경우 2022년 발표한 제로트러스트 전략 문서에서 가장 높은 수준의 제로트러스트(Advanced Zero Trust)를 2032년까지 도입하겠다는 로드맵을 세운 바 있으며, 국가안보통신자문위원회(National Security Telecommunications Advisory Committee, NSTAC) 역시 2022년 대통령 보고서에서 제로트러스트에 대한 범정부적 구현은 수년에서 수십년이 걸린다고 언급한 바 있다. 범정부적 구현보다 개별 기업에서의 구현이 훨씬 속도가 빠르겠지만, 그럼에도 1~2년만에 제로트러스트 아키텍처를 '최적화 수준'으로 완성시킬 수 있다고 생각하는 것은 바람직하지 않다.

따라서, 제로트러스트 아키텍처를 도입하고자 하는 기업 역시 단기간 내에 도입하겠다는 계획보다는, 최종 목표와 함께 몇 단계의 단기 목표와 실천 방안을 구성함으로써 최적화 수준의 성숙도를 향한 장기적인 도입 계획을 마련하는 것이 좋을 것이다.

라. 제로트러스트 도입 전략에 대한 이해

제로트러스트 전략은 기술·솔루션 도입만을 의미하지 않으며, 기업이 제로트러스트를 채택하는 과정에서 인식 제고, 교육 등 부가적인 업무를 필요로 한다.

많은 기업 보안 담당자들이 제로트러스트 아키텍처 도입에 있어 기술·솔루션의 도입을 우선시하고 있다. 그러나, 먼저 보안 담당자들은 왜 제로트러스트를 도입하려고 하는가에 대한 근본적인 질문을 할 수 있어야 한다. 기술 및 솔루션의 도입은 전체적인 제로트러스트 도입 과정 중 셋째 단계인 구현(도입) 단계에 해당한다. 그러나 전체 과정은 준비 단계부터 이루어져야 하며, 준비 단계에 들어가기 전에 기업 소속 전체 임직원들에게 비전과 최종 목표를 제시할 수 있어야 한다.

미 국방부에서 발간한 제로트러스트 전략 문서에서는 "무엇을 달성할 것인가"의 관점에서 비전을 "완전히 구현된 국방부 차원의 제로트러스트 사이버 보안 프레임워크에 의해 보호되는 국방부 정보 엔터프라이즈"로 제시하고, 다음과 같은 목표(Goal)를 제시하였다.

표 4-2 미 국방부 제로트러스트 전략

비전 달성을 위한 질문	목표
우리는 무엇을 이해·동의하는가?	▸ 제로트러스트에 대한 문화적 채택: 국방부 제로트러스트 생태계 전반에서 정보 기술의 설계, 개발, 통합 및 배포를 이끄는 제로트러스트 보안 프레임워크 및 사고방식
무엇을 해야 하는가?	▸ 보호·방비되는 국방부 정보시스템: 국방부 정보시스템에서 조직 차원의 복원력 달성을 위하여 제로트러스트를 통합 및 운영하는 국방부 사이버보안 사례
어떻게 제로트러스트를 달성할 것인가?	▸ 기술 가속화: 제로트러스트 기반 기술을 산업계 발전 속도와 같거나 그 이상의 속도로 배포하여 변화하는 위협 환경에 앞서 나갈 것
어떤 지원이 필요한가?	▸ 제로트러스트 달성 지원: 부처 및 하부조직 수준 프로세스와 통합된, 지속적이고 조직화된 제로트러스트 실행

이 전략에서 기업망 내부에서 보호 대상이 되는 핵심 요소 선정은 둘째 목표에 해당되며, 어떤 기술·솔루션을 도입할 것인가는 셋째 목표에 해당한다. 다른 두 가지 목표(첫째와 넷째)를 살펴보면, 미 국방부는 조직 차원에서 제로트러스트의 정확한 이해를 위한 문화적 채택과 구체화된 실행 전략을 담은 지원 계획 수립 역시 전략적 목표 수립에 있어 필수적이라고 파악하고 있음을 확인할 수 있다.

미 국방부의 세부적인 전략 모두가 모든 기업에게 해당하는 것은 아니지만, 기업이 제로트러스트를 원활하게 도입하기 위해서는 조직 차원에서 공통적으로 이해 가능한 비전을 제시하고 인식을 제고하며 필요시 보안 담당자의 전문성을 키울 수 있어야 한다. 또한 제로트러스트 아키텍처를 구축하기 위한 정책과 계획, 로드맵(일정), 자금 조달, 기술 도입 및 배포 방안, 제로트러스트 성능 평가 방안을 구체적으로 수립하여야 하며, 조직의 규모에 따라 필요한 경우 제로트러스트 책임 조직을 구성하는 것도 도움이 될 것이다.

마. 기업 임직원의 업무 편의성 증대

제로트러스트 도입 시 직원들이 클라우드 및 AI와 같은 혁신 기술을 편리하게 활용할 수 있게 되어 직원들의 편의성이 증대될 것을 기대하지만, 엄격한 접근제어 및 보안 강화로 인하여 새로운 불편이 생길 수도 있다.

보안 기술 중에는 보안 강화의 목적하에 직원의 업무 효율성을 떨어뜨리는 경우가 다수 존재하며, 일부 기업에서는 법규 혹은 내부 규정으로 망분리, VPN, 기기 관리 솔루션 등을 강제함으로써 불편함을 가중시키는 사례가 많이 존재한다. 업무 효율성 측면에서 불편한 여러 레거시 보안 기술에 대한 대체수단으로 제로트러스트 기술을 활용하려는 기업 임직원들에게는 제로트러스트 아키텍처의 도입을 적극적으로 추진할 명분을 갖게 해준다.

그러나 제로트러스트 아키텍처는 기업 차원의 강화된 인증, 기기 및 리소스 관리 등을 요구하며, 보안 강화 및 위험 완화를 위하여 리소스 접근시 최소 권한 부여를 통한 엄격한 접근제어를 시행하게 될 것이다. 기기 관리 측면에서는 특히 업무용 기기를 강제화하고, 기기에 대한 보안 상태 점검, OS 및 보안 업데이트 등을 지속적으로 요구하게 될 가능성이 있으며, 리소스 관리 측면에서는 실험 목적 등으로 인한 임시 기기의 사용조차 엄격한 자산 및 식별자 등록 절차를 강제할 가능성이 있다. 이러한 엄격한 보안 점검은 직원들의 기존 관행과 다를 수 있으므로, 직원들이 적응하기까지는 불편함을 줄 가능성이 있다. 물론, 높은 수준의 제로트러스트 성숙도를 만족하게 될 경우 이러한 과정 중 상당 부분은 자동화가 이루어져 편의성을 다시 확보할 수 있다.

또한, 제로트러스트 아키텍처 구축 초기에는 동적 접근제어를 위하여 정상 사용자의 활동도 엄격하게 확인하는 과정에서, 신뢰도 판단 알고리즘의 오류 혹은 정책에 대한 잘못된 설정으로 정상

사용자의 활동에 대해서도 의심스러운 행위로 오탐할 가능성이 존재한다. 지속적인 운영 및 피드백 과정에서 이러한 오탐은 줄어들겠지만 그 과정에서 일반 직원에게 불편함을 줄 수 있음을 인지하고 이에 대한 대책을 마련해야 한다.

그 외에도, 동적 접근제어를 위하여 현재 리소스에 접근하는 직원의 물리적 혹은 네트워크상의 위치, 사용 프로그램 등 활동을 지속적으로 모니터링하여 프라이버시 이슈가 발생할 수도 있다. 따라서, 제로트러스트 도입 및 운영 과정에서 직원들이 새로 겪을 수 있는 불편을 최소화하면서도 보안성을 유지·고도화할 수 있는 제로트러스트 도입 전략이 필요하다.

2. 기업 내 인식 제고의 필요성

앞서도 언급했지만, 많은 기업에서 제로트러스트 아키텍처 도입 계획을 세울 때 가장 먼저 기술·솔루션 혹은 도입 사례를 분석하는 경우가 많은 것으로 보인다. 그러나, 미 국방부 제로트러스트 전략 문서에서도 언급한 바와 같이, 조직 차원에서 제로트러스트 도입 시 가장 먼저 해야 할 일은 비전 제시와 함께 해당 비전을 만족시킬 수 있는 목표를 설정하는 것이다. 이를 통하여, 조직 내 모든 구성원들이 같은 보안 지향점을 갖고, 제로트러스트 전환에 각자의 역할에 따라 지원 및 협력할 수 있는 체계를 수립할 수 있어야 한다. 이와 같은 일들은 모두 기업 내 제로트러스트에 대한 인식을 제고하는 과정으로 볼 수 있다.

기업 내 인식을 제고하기 위해서는, 제로트러스트 전환에 드는 시간과 비용, 제로트러스트 운영 과정에서 신규 보안 솔루션 도입이나 정책 변경으로 인한 임직원의 불편 등에 대해 설득할 수 있어야 하며, 이를 위해서 특히 경영진을 설득하여 지원을 이끌어내는 것은 필수적이라고 볼 수 있다. 그러나 제로트러스트 전환이 막연하게 기업망에 대한 보안성을 높일 수 있다거나 혹은 다른 기업들이 다들 도입을 진행 중임을 강조하는 등 추상적인 표현으로는 부족함이 있을 것이다.

따라서, 크게 보면 다음과 같이 제로트러스트에 대해 사전에 분석하여 정리하는 것은 필수적으로 볼 수 있다.

가. 제로트러스트 아키텍처 도입 장점 파악

도입으로 인한 일반적인 장점, 즉 내부 침투시에도 위험을 완화할 수 있다는 장점은 보안 전문가가 아닌 임직원을 설득하기 어려울 것이다. 그보다는 현재 소속 기업의 특성이나 환경을

고려하여 장점이 드러나는 제로트러스트 기반 유스케이스를 구체화하는 것이 필요하다.

예를 들어, 보안성을 강화하기 위해 망분리 기술을 도입하고 있는 기업이라면, 망분리를 완화한 형태의 제로트러스트 아키텍처 기반 업무 유스케이스를 제안함으로써 부가적으로 다양한 클라우드 서비스 혹은 AI 기반 서비스를 직접적으로 업무에 활용 가능하게 되며, 이를 통하여 업무 효율성 및 생산성이 매우 커질 수 있음을 제시할 수 있을 것이다. 혹은 소프트웨어 개발 기업에서는 제로트러스트 아키텍처를 기반으로 소프트웨어 개발 환경의 보안성을 강화함으로써 공급망 보안에 기여할 수 있음을 주장할 수 있을 것이다.

이 과정에서 필연적으로 발생하는 도입 시간과 인적 자원, 자본 등 비용에 대해서도, 효과적인 방어를 통해 얻을 수 있는 이점을 강조할 수 있어야 한다. 보안에 대한 비용은 계속해서 늘어날 가능성이 높은데, 이는 지속적으로 공격이 고도화되고 있고 공격 수단이 다양해지고 있기 때문에 예전에 고려하지 않았던 보안 솔루션들이 추가로 필요하기 때문이다. 그리고 이런 신규 보안 솔루션의 도입은 그 자체로 보안 성숙도를 높이는 제로트러스트 전환의 과정으로 볼 수 있다. 그 외에도, 보안 사고 발생 시 예상 가능한 피해 규모를 미리 산정하여 예측하는 것도 필요할 수 있다.

나. 임직원의 역할과 책임에 대한 사전 정의

많은 기업들은 법적 의무 준수 혹은 경영상의 의무로 조직 차원에서 보안 거버넌스 혹은 이와 유사한 체계를 유지하고 있다. 제로트러스트 전환에 대한 결정이 이루어지더라도, 기업 내 구성원들의 역할, 권한과 책임 등이 명확하지 않으면 제로트러스트 아키텍처 도입, 운영, 피드백, 보안 사고 발생에 대한 대응 등 다양한 상황에서 현장에서의 혼란은 불가피할 것이다.

예를 들어, 제로트러스트 아키텍처 도입 단계 중 준비 단계에서는 현재 기업의 현재 수준을 정확히 파악하기 위하여 사용자 및 기기, 리소스에 대한 식별 및 성숙도 수준 평가가 필요하지만 이는 제로트러스트 전환 담당자만의 노력으로 이루어질 수 없다. 따라서, 도입 준비 단계부터 운영 단계, 피드백 및 개선 단계에 이르는 모든 도입 과정에서 임직원의 역할과 책임을 정의하고 난 후, 그들과 협력하에 계획을 수립하는 것이 적절하다.

3. 제로트러스트 전환을 통한 보안 성숙도 분석

이 부분은 제로트러스트 아키텍처 도입에 대한 장점을 파악하는 것과 일부 유사성이 있으나, 보안 관점에서 구체적인 분석의 필요성에 대해 다룬다. 제로트러스트 전환 담당자는 조직 내 설득을 위해서 제로트러스트 전환 과정에서 제로트러스트 혹은 보안에 대한 성숙도 수준 분석 방안에 대해서 고민할 필요가 있다. 즉, 제로트러스트 전환을 시작할 때, 혹은 전환 과정에서 현재의 제로트러스트 혹은 보안 수준이 어느 단계에 있으며, 현재의 절차를 마무리했을 때 어느 단계에 있을지를 경영진 등 내부 구성원들에게 객관적으로 보여줄 수 있어야 한다.

이를 위해서, 본 가이드라인 5장에서는 제로트러스트 도입 이후 보안 수준을 분석하여 객관적으로 제시할 수 있는 방안을 보여준다. 5장에서 제안하는 내용을 절대적인 기준으로 볼 수는 없으나, 담당자들이 참조하여 객관화하는데 도움이 될 수 있을 것으로 보인다.

이 외에도, 부록 4절에서 언급한 다른 종류의 성숙도 모델을 이용하여 분석하는 것도 가능하며, 민감한 정보를 다루는 기업들은 최근 미 국방부가 2025년부터 시행하는 것으로 발표한 사이버보안 성숙도 모델 인증(Cybersecurity Maturity Model Certification, CMMC) 제도 등을 참고할 수도 있다. CMMC는 미 국방부에 연방 계약 정보(Federal Contract Information, FCI) 및 통제된 미분류 정보(Controlled Unclassified Information, CUI)를 보호하기 위해 조달 기업들이 지켜야 하는 보안 성숙도 수준을 정의하고 있으며, 상기 정보에 따르는 3단계의 보안 수준에 대해서 수준별로 지켜야 할 요구사항을 정의하고 있다.

4. 기타 고려사항

2.1절에서는 제로트러스트 아키텍처의 기본 원리를 제공하고 있으며, NIST SP 800-207 등 다양한 문서에서도 제로트러스트 개념을 준수하기 위해 지켜야 할 원리 혹은 원칙들을 다루고 있다.

제로트러스트 도입을 준비하는 과정에서 제로트러스트 성숙도, 기술 및 솔루션을 분석하는 단계로 진행될 경우, 특정 기술·솔루션이 가진 장단점에 편향되어 제로트러스트가 본질적으로 추구하는 철학을 놓칠 수 있다. 도입을 준비하는 단계부터 실제 운영, 피드백에 이르기까지 이러한 기본 원리를 잊지 않고 지속적으로 검증하는 것은 매우 중요하다.

또 다른 측면으로는 기업망 보안의 특성상 중요한 디지털 자산의 보호에 우선해야 한다는 점에서, 해당 기업에서 가장 중요한 비즈니스를 중심으로 제로트러스트의 성숙도를 끌어올리려는 노력이 필요하다. 예를 들어, 자체적으로 업무용 소프트웨어·서비스를 개발하여 자사망에 구축하거나 다른 기업에게 공급하는 기업들은, 개발 및 공급망에 대한 제로트러스트 기반 안전성에 대해 심도있게 분석하여야 한다. 공격자가 개발망 혹은 공급망에 침투할 가능성이 있는 상황이라면 해당 환경에서 개발하는 소프트웨어·서비스로 인한 위험은 상당히 높다고 볼 수 있다.

2024년 5월 발간된 SW 공급망 보안 가이드라인 1.0 등을 참고하여, 개발 및 공급 환경에 대한 관리를 철저히 할 수 있는 제로트러스트 아키텍처를 구성해야 하며, 관련 핵심 요소(특히 시스템, 애플리케이션 및 워크로드)에 대한 제로트러스트 성숙도를 최대한 빠르게 끌어올릴 수 있도록, 전략의 우선 순위 조정이 필요하다. 또한, 개발 환경에서의 취약점 발견, 해당 소프트웨어·서비스 사용 부서 혹은 기업에서의 비정상적인 접근 등 문제 발생 시 해당 소프트웨어·서비스에 악성 코드 등이 침투하지 않았는지를 검증하기 위한 개발 부서와의 협력 체계 등을 갖출 필요가 있을 것이다.

| 제2절 |

제로트러스트 아키텍처 도입을 위한 조직 내 역할 및 목표 설정

1. 기업 내 임직원 간 역할과 책임

4.1절의 제로트러스트 아키텍처 도입 고려사항에서 제로트러스트 아키텍처를 도입하는 기업 내 인식 제고를 위하여, 임직원의 역할과 책임에 대해 사전에 정의하여야 한다고 서술한 바 있다.

제로트러스트 아키텍처는 결국 제로트러스트의 개념을 활용하여 기업 내부의 네트워크, 시스템 및 리소스를 보호할 수 있는 보안 아키텍처이다. 기업이 제로트러스트 아키텍처를 받아들이는 것은 기업 전체에서의 보안 상태와 정책, 방향성을 근본적으로 변화시키는 작업이므로 정보보호 최고책임자(CISO)의 역할이 매우 중요하다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)에서는 정보통신서비스 제공자가 지정하는 CISO의 업무를 다음과 같이 정리하고 있다.

■ 정보보호 최고책임자의 업무

- 정보보호 계획의 수립·시행 및 개선
- 정보보호 실태와 관행의 정기적인 감사 및 개선
- 정보보호 위험의 식별 평가 및 정보보호 대책 마련
- 정보보호 교육과 모의 훈련 계획의 수립 및 시행

또한 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도에서는 최고경영자가 CISO 관련하여 다음과 같은 업무를 수행할 것을 인증 기준으로 두고 있다. 그러나, 이 업무만으로는 최고경영자의 제로트러스트 아키텍처 도입 과정에서 필요한 모든 업무를 수행했다고 보기는 어려우며, 최소한의 기준으로 보는 것이 바람직하다. 최고경영자가 정보보호에 관한 전문성을

갖추지는 못하더라도, 제로트러스트 아키텍처 도입의 필요성을 이해하려는 노력과 함께 CISO 및 실무조직의 활동을 적극 지원·승인하는 것이 바람직하다. 특히, 제로트러스트 아키텍처 도입 과정에서 타 임원·부서와의 갈등이 다양하게 발생할 수 있기 때문에, 경영진 간 협의체에 참여하여 적절한 의사 결정을 내릴 수 있어야 한다.

■ 최고경영자의 정보보호 관련 업무

- 최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
- 최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.

정보보호조치에 관한 지침에서는 정보보호조치의 구체적인 내용을 포함하고 있으며, 관리적 보호조치로서 정보보호 조직의 구성과 운영을 다음과 같이 시행할 것을 권고하고 있다.

표 4-3 정보보호 조직의 구성과 운영

정보보호 조직의 구성·운영	세부조치사항
정보보호 조직의 구성	‣ 정보보호 최고책임자, 정보보호관리자, 정보보호담당자로 구성된 정보보호조직을 운영
정보보호 최고책임자의 지정	‣ 기업의 정보보호를 책임지는 이사 이상의 상근임원으로 지정
정보보호조직 구성원의 역할	‣ 정보보호 최고책임자는 정보보호 업무와 조직을 총괄 지휘 ‣ 정보보호관리자는 정보보호 업무의 실무를 총괄하고 관리 ‣ 정보보호담당자는 정보보호 업무의 분야별 실무를 담당

2. 제로트러스트 도입 과정에서 각 구성원의 역할

2019년 금융보안원에서 발간한 '금융보안 거버넌스 가이드'에서는 금융권 업무 특성을 반영한 효과적인 금융보안 거버넌스의 도입을 권고하고, 금융 기업의 보안 위험을 완화하기 위한 거버넌스 전략 및 각 구성원들의 역할, 권한, 책임을 구체적으로 정의하였다.

제로트러스트 아키텍처의 도입 과정도 각 구성원들에 대한 역할이 명확하지 않으면, 도입 현장

에서 구성원간 책임을 서로 미루는 등 여러 문제점이 발생할 수 있다. 따라서, 관련 법령·제도에서 정의한 각 구성원의 업무, '금융보안 거버넌스 가이드' 등을 참고하여 제로트러스트 도입 과정에서 각 구성원의 역할을 다음과 같이 정의할 수 있으며, 각 기업들은 아래 정의된 역할을 구체화하여 제로트러스트 아키텍처를 도입하는 것이 바람직하다.

가. 제로트러스트 도입 과정에서 최고경영자(CEO)의 역할

제로트러스트 도입을 추진하는 기업에서 최고경영자의 역할은 다음과 같다.

- 최고경영자 스스로 제로트러스트 아키텍처의 필요성을 이해하고, CISO 및 실무조직의 제로트러스트 전문성 확보 등 계획 수립 단계부터 지원
- 제로트러스트 도입 계획 수립 및 검토를 위한 CISO 중심의 전문 인력 확보 및 전담 조직 구성 계획 승인
- 제로트러스트 도입 과정에서 필수적인 논의가 가능하도록 최고경영자와 CISO 등 경영진 간 협의체 마련
- CISO가 수립한 정보보호 비전 및 제로트러스트 도입 목표, 중장기 전략 및 로드맵에 대한 승인
- 제로트러스트 아키텍처 도입 세부 계획에 필요한 예산 및 도입 프로젝트 최종 승인

나. 정보보호 최고책임자(CISO)의 역할

제로트러스트 도입을 추진하는 기업에서 정보보호 최고책임자의 역할은 다음과 같다.

- 제로트러스트 아키텍처 도입 전략에 대한 최고책임자 역할 수행
- 제로트러스트 도입 계획 수립 및 검토를 위한 제로트러스트 전문 인력 확보 및 전담 조직 구성
- 협의체 운영 등을 통하여 제로트러스트 비전 및 도입 목표, 관련 정보 공유를 통하여, 제로트러스트 아키텍처 도입에 대한 조직 차원 의사 결정 지원
- 기업망의 특성과 비즈니스를 고려한 정보보호 비전 및 제로트러스트 도입 목표, 전략 및 로드맵 수립
- 제로트러스트 아키텍처와 관련한 각종 법률, 규정 및 정책, 기술, 솔루션 등에 대한 최신 동향 파악

- 실무조직이 수립한 제로트러스트 아키텍처 도입을 위한 단계별 목표 및 세부 계획에 대해, 제로트러스트 성숙도 수준, 예산, 위험 완화 방안의 적절성 등 종합적인 검토 및 승인, 필요시 경영진에 승인 요청
- 도입 프로젝트 수행 시 프로젝트 관리 및 감독, 조직 내 협력 및 조정을 통하여, 각 단계에서 발생하는 주요 의사결정 주도 및 조직 내 갈등 해소, 예산 및 일정 관리 등에 대한 책임
- 제로트러스트 아키텍처 운영 과정에서 임직원에 대한 보안 교육 및 인식 제고 활동
- 제로트러스트 아키텍처 도입의 전반적인 활동에 대해 외부 전문가를 통한 주기적 평가

다. 정보보호관리자 및 담당자 등 실무조직의 역할

제로트러스트 도입을 추진하는 기업에서 실무조직의 역할은 다음과 같다.

- CISO의 제로트러스트 도입 활동 업무에 대한 전반적인 지원 및 정책 수행
- 조직 내 접근 주체, 기기, 리소스에 대한 식별 및 제로트러스트 성숙도 수준 평가
- 제로트러스트 아키텍처 도입을 위한 단계별 목표 및 세부 계획 수립, 요구사항 정의 및 아키텍처 구체화, 도입하고자 하는 기술·솔루션 검토 및 선별
- 도입 과정의 전반적인 실무 수행 및 제로트러스트 기술·솔루션 도입·구축 과정 검증, 공급기업과 소통
- 제로트러스트 아키텍처 운영을 위한 전사적 정책 수립, 제로트러스트 아키텍처 운영 및 유지관리, 임직원들로부터 피드백 확보 및 개선 등
- 신기술 동향 파악 및 기타 정보보호 전반에 걸친 실무 수행, 필요 시 CISO 보고

3. 제로트러스트 아키텍처 도입 목표 설정

제로트러스트 아키텍처를 도입하는 과정에서 기업망 구조 및 현재 보안 아키텍처에 대한 분석이 완료되었으면, 다음으로 진행해야 할 일은 제로트러스트 아키텍처 도입을 위한 비전 혹은 전략적 목표를 제시하는 것이다. 이 과정에서 가장 중요한 것은 기업의 비즈니스 목표와 일치하는 형태로 기업 보안의 미래 방향성을 설정해야 한다는 것이다.

비전 혹은 전략적 목표는 제로트러스트 도입을 통해 기업이 어떤 사이버 위협에 대비할 수 있으며, 비즈니스에 대한 연속성을 어떻게 강화하고 위험을 완화할 수 있는지 설명하고, 기업망

보안에 대한 방향성을 설정할 수 있어야 한다. 비전과 전략적 목표는 차후 구체적인 목표 설정, 참조 아키텍처 및 로드맵 수립을 위한 기초를 제공할 뿐만 아니라, 일반 직원들의 제로트러스트 인식을 제고하고 새로운 보안 환경에 적응하는 것에 대한 동기 부여가 가능할 것이다.

예를 들어, 다음과 같은 비전 및 전략적 목표 수립이 가능할 것이다.

- 병원: 의료 네트워크와 환자 데이터에 대한 철저한 보호를 통해 제로트러스트가 지켜주는 병원
- 자동차 생산 기업: 스마트 공장, 글로벌 공급망, 지능형 차량을 지속적으로 검증·보호하여, 안전하고 효율적인 자동차 생산 환경 구축
- 금융 기업: 지속 인증과 철저한 접근통제를 통해 고객 데이터를 보호하고, 생성형 AI 및 클라우드를 활용하여 신뢰할 수 있는 금융 혁신 서비스를 제공하는 제로트러스트 아키텍처 구축
- 발전사: 발전소 운영 연속성 보장 및 사이버 보안 강화를 통하여 신뢰할 수 있는 전력 공급을 책임지는 제로트러스트 아키텍처 구현
- SW개발 기업: 코드, 데이터, 그리고 개발 환경의 지속적인 신뢰 검증을 통해 사이버 위협을 방지하고, 안전하고 혁신적인 소프트웨어 개발 문화 조성

기업망의 현재 보안 아키텍처와 보안 수준 분석이 어느 정도 진행되고 제로트러스트 아키텍처 도입의 필요성과 함께 비전이 제시되었다면, 비전을 구체화함으로써 제로트러스트 아키텍처를 어느 수준으로 어떻게 달성할지에 대한 명확한 목표를 설정할 필요가 있다.

가. 비즈니스 목표와 연계

기업이 제로트러스트 아키텍처를 도입하는 경우, 자신의 비즈니스 목표를 달성하는 과정에서 사이버 위협을 통해 발생할 수 있는 위험을 완화·최소화하는 방법을 제공해야 한다. 예컨대, 비즈니스 목표를 달성하는 데 있어 외부 클라우드 기반 SaaS의 도입이 필수적일 수도 있고, 혹은 IoT 기기를 통한 센서 데이터 수집을 기반으로 다양한 서비스를 만들어낼 수도 있을 것이다. 신기술을 활용하여 서비스를 제공할 경우, 그 신기술이 보안에 미치는 영향을 고려하여 기업망의 특정 핵심 요소 혹은 그 핵심 요소의 특정 보안 기능(예, 마이크로 세그멘테이션)의 성숙도 수준을 높이는 것이 최우선시 되어야 할 수도 있다.

또한 기업이 처할 수 있는 위험을 평가하는 것도 결국 비즈니스 목표와 연계가 된다. 기업이 비즈니스의 효율성을 위하여 온프레미스에서 유지하던 핵심 디지털 자산을 클라우드로 이전한다면, 클라우드 관련 보안 위협들은 곧 그 기업이 직면한 주요 사이버 위험으로 식별될 수 있다. 이 경우, 클라우드 상의 데이터 혹은 클라우드 서비스에 대한 보안 혹은 제로트러스트 성숙도 수준을 높은 수준으로 끌어올려야 할 것이다.

기업망 보안, 특히 제로트러스트 아키텍처를 도입하는 데 있어서 이렇게 비즈니스 목표와 연계한다면 전략적 목표가 분명해질 수 있다. 전략적 목표를 바탕으로 장·단기 목표를 설정한다면, 보다 구체적으로 제로트러스트 아키텍처 도입 계획을 수립하는 데 큰 도움이 될 것이다.

나. 목표 설정 원칙

기업망 보안을 위한 전략적 목표를 정의하는 경우, 목표에 대해 효과적으로 달성할 수 있도록 돕는 방법론과 원칙이 필요하다. 즉, 설정된 전략적 목표를 달성했는지를 평가할 수 있는 성과 지표가 있어야 하며, 달성한 성과를 경영진에 보고하고 기업 내부의 모든 구성원과 공유할 수 있는 체계가 있어야 한다. 경영진 및 기업 내부의 구성원들로부터 받은 평가와 피드백을 통해 전략적 목표에 대한 변경이 필요한지를 검토할 수 있으며, 사이버 위협 환경이 지속적으로 변화하고 고도화되는 과정에서 마찬가지로 전략적 목표에 대한 지속적인 개선이 이루어질 수 있어야 한다.

기업은 각자의 목표 설정 원칙을 통해 성과 지표를 확정하는 것이 일반적이며, 본 가이드라인에서는 많은 조직들이 활용하는 SMART 목표(혹은 SMART 표준)를 이용할 수 있음을 제시한다. 이 방법은 절대적인 것은 아니지만, 각 기업은 이와 유사한 방식으로 제로트러스트의 전략적 목표를 수립할 수 있다.

- Specific (구체적): 목표는 정확하고 구체적이어야 함. 예를 들어, “기업망 내부 접속은 반드시 MFA와 같은 강력한 사용자 인증을 통해 확인된 후 허용되어야 한다.”와 같은 목표를 수립할 수 있다.
- Measurable (측정 가능): 목표 달성 여부를 확인할 수 있도록 정량적·정성적 기준이 포함되어야 함. 예를 들어, “향후 1년 이내 모든 사용자의 네트워크 접근 시 FIDO 활용 비율을 100% 달성한다”와 같은 목표가 가능하다.
- Achievable (달성 가능): 목표는 현실적이고 달성 가능해야 함. 예를 들어, “올해 보안 예산을

활용하여 제로트러스트 전문 인력을 1명 확충하고, 전사적 ID 관리 시스템 구축 계획 수립을 전담시킨다."와 같은 목표가 가능할 것이다.

- Relevant (관련성): 설정된 목표는 기업의 비전과 전략과 일치해야 함. "기업 내 고객 및 재고 관리를 위한 클라우드 서비스의 도입 과정에서 위험을 최소화하기 위하여, 제로트러스트 아키텍처를 통한 클라우드 보안 위협을 완화한다."와 같은 목표 수립이 가능하다.
- Time-bound (시간 제한): 목표에는 달성 기한이 있어야 함. "제로트러스트 아키텍처에 대한 기본 설계 및 파일럿 프로젝트를 6개월 이내에 완료한다."와 같은 목표를 수립할 수 있다.

다. 기업 보안 문화 및 인식 강화 목표 수립

제로트러스트 아키텍처 목표 설정 과정에서는 기업 보안 문화 정착과 인식 강화를 위한 목표를 포함시키는 것이 바람직하다. 기업 보안 문화 및 인식 강화에는, 조직 내 모든 직원이 보안의 중요성을 인식하고, 제로트러스트 원칙을 이해하며 실천할 수 있도록 만드는 방안이 포함되어야 한다.

이는 기업들이 기존에 시행해 온 다양한 보안 인식 강화 교육 및 보안 문화 정착을 위한 캠페인과 비슷하다고 볼 수 있다. 기존 교육 및 캠페인에는 다음과 같은 사례가 있으며 제로트러스트 아키텍처를 도입하는 과정에서도 기본적인 보안 문화 정착은 필수적이므로, 기업은 다음 사례와 같은 노력을 지속적으로 유지·강화하는 것이 중요하다.

- 사이버사고 사례 중심의 보안 인식 교육: 피싱, 스미싱 등 사이버 사기 및 해킹 공격은, 그 공격 유형을 잘 모르는 경우 피해를 볼 확률이 상대적으로 더 높기 때문에, 조직이 처한 상황과 유사한 위험에 대해서는 사이버사고 사례 중심의 집합 교육 및 정보 공유를 통해 보안 의식을 강화
- 조직 구성원의 자율보안 인식 개선: 매월 보안의 날을 정함으로써, 내PC지키미(혹은 내PC돌보미) 실행을 통한 보안 점검, 정기적 보안 업데이트 수행 등을 통하여 직원들이 자율적으로 보안 인식을 개선할 수 있는 방법 제공
- 보안 우수사례에 대한 인센티브: 보안 인식을 높이기 위한 인센티브 제도를 도입하여 직원들이 자발적으로 보안 문화 확산에 참여하도록 유도하기 위함으로, 보안 정책을 적극적으로 따르거나 새로운 보안 취약점 발견, 우수 표어 창작 등 보안에 직간접 기여를 한 직원에게

보상을 제공하는 프로그램을 도입하여 동기를 부여하고 정기적으로 우수 직원이나 팀을 선정해 포상하는 방식으로 보안 인식 제고

제로트러스트 철학이 반영된 기업 보안 문화 및 인식 강화를 위해서 상기 사례들을 적용함과 동시에, 제로트러스트의 특성을 고려하여 다음과 같은 목표를 추가로 수립할 수 있다.

- 제로트러스트 문화 확립: 기업 전반에 걸쳐 제로트러스트 보안 문화를 확립하여, 모든 직원이 보안의 역할과 중요성에 관한 인식을 갖도록 교육하는 것이 목표로, 보안은 IT 부서뿐만 아니라 모든 직원의 책임이라는 인식을 심어주고, 제로트러스트 원칙인 항상 검증(Never Trust, Always Verify), 최소 권한 원칙을 실천할 수 있는 교육 프로그램 개발이 필요함
- 최소 권한 원칙에 대한 인식 강화: 모든 직원이 최소 권한 원칙을 준수하도록 유도하고, 불필요한 권한을 최소화할 수 있는 인식을 강화하는 것이 목표로, 직원들이 필수적인 업무에만 접근할 수 있도록 권한이 제한된다는 점을 이해하게 하여, 최소 권한 원칙을 실천하는 문화를 확립. 또한, 이를 위한 권한 요청 및 관리 절차를 간소화하고 보안 정책을 투명하게 운영
- 상시 보안 모니터링 및 보고 문화 확립: 직원들이 의심스러운 활동이나 이상 징후를 발견하면 즉시 보안 팀에 보고하는 문화를 정착시키는 것이 목표로, 실시간 모니터링을 통해 이상 징후를 발견할 수 있는 보안 인식을 강화하고, 모든 직원이 자발적으로 보안 위협을 탐지하고 보고할 수 있도록 간단한 보고 프로세스 및 신속한 대응 체계를 마련

| 제3절 |

제로트러스트 아키텍처 구성 방안

제로트러스트 아키텍처의 본격적인 도입 계획 수립에 앞서, 준비 단계에서 필요한 업무들이 있다. 이는 가이드라인 1.0에서 제시한 제로트러스트 도입 단계(준비 → 계획 → 구현 → 운영 → 피드백 및 개선) 중 가장 첫 단계인 준비 단계에 진입하기 전부터 시작하여 준비 단계에 이르기까지 진행해야 하는 업무를 구체화한 것이다.

1. 현재 기업망 보호 대상 및 보안 아키텍처 분석
2. 기업망을 위한 제로트러스트 아키텍처 정의 및 구현 로드맵 수립

기업망을 위한 제로트러스트 아키텍처를 구체적으로 정의하는 과정에서 선택해야 하는 접근 방법을 고려해야 한다. 가이드라인 1.0에서는 제로트러스트 아키텍처 보안 모델을 구성하고 접근 주체의 리소스 접근 여부를 최종적으로 결정하기 위한 접근법 3가지를 언급한 바 있는데, 인증 체계 강화, 마이크로 세그멘테이션, 네트워크 인프라 및 소프트웨어 정의 경계(SDP) 등이 이에 해당한다. 각 기업들은 각 접근법의 특징과 현재 기업망 보안 아키텍처 등을 고려하여 기업에 맞는 접근법을 선택할 수 있다.

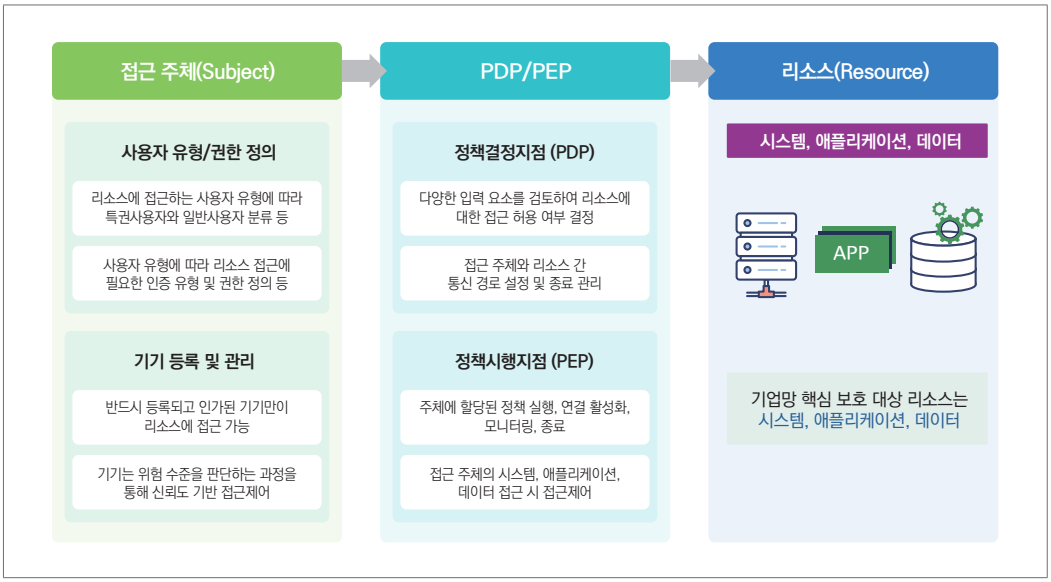
1. 현재 기업망 보호 대상 및 보안 아키텍처 분석

가. 현재 기업망 보호 대상 파악

제로트러스트 아키텍처 도입 및 구축을 위해서는 현재 기업망에서 보호 대상을 파악하는 것이 초기 단계에서 이루어져야 할 가장 중요한 업무이다. 가장 중요한 핵심 보호 대상으로는 리소스에 해당하는 시스템, 애플리케이션, 데이터들이 있으며, 접근 주체에 해당하는 사용자 및 기기 역시 또 다른 보호 대상이 될 수 있다. 제로트러스트 아키텍처 관점에서 아래 [그림 4-2]와 같이 접근 주체와 보호 대상 리소스를 구별할 수 있으며, 보호 대상은 기업 내 중요한 자산으로서 명확하게 식별할 수

있어야 그에 맞는 적절한 보호 전략을 설계할 수 있다.

그림 4-2 제로트러스트 아키텍처 접근 주체와 보호 대상 리소스



기업망에서 가장 중요한 핵심 보호 대상은 접근 대상에 해당하는 리소스로 이들은 기업망 내부에서 각자 가치를 가진 디지털 자산으로 볼 수 있으며, 도입을 준비하는 과정에서 이들에 대해 식별하여 목록화하는 것은 반드시 필요한 업무이다. 다음 리소스에 대해서는 반드시 누락되지 않고 목록화를 해야 하며, 목록화 과정에서 어떤 접근 주체가 어떤 권한을 갖는지에 대한 정보를 포함하여야 한다.

- 시스템: 중요 애플리케이션을 구동하거나 데이터를 저장·관리하고 있으며, 온프레미스·클라우드(IaaS)에 구축 운용 중인 모든 서버 (DBMS, 개발시스템, 웹서버, 메일시스템 등)
- 애플리케이션: 기업 내부에서 사용하는 온프레미스·클라우드(PaaS) 애플리케이션 및 워크로드
- 데이터: 온프레미스·클라우드(SaaS)에 위치한 중요한 비즈니스 데이터(고객 정보, 인사·재무 데이터, 개발 중인 소프트웨어, 지적 재산, 기타 비즈니스에 필수적인 모든 종류의 데이터)

기업망 내부를 구성하는 접근 주체 역시 보호 대상으로 볼 수 있으며, 여기에는 내부 직원뿐만 아니라 외부 협력 기업, 계약 기업, 자동화된 서비스 계정 등 비인간개체 등을 모두 포함하여야 한다.

- 사용자: 내부 직원, 외부 협력 기업 및 계약 기업 직원, 자동화된 서비스 계정 등 비인간개체 등을 포함
- 접속 기기: 사용자가 리소스에 접근하기 위해 활용하는 기기 및 엔드포인트 등 하드웨어 장치

리소스에 접근하는 사용자들은 해당 사용자들의 업무, 접근해야 할 리소스 등에 따라 특권 사용자(Privileged User)와 일반 사용자로 구분될 수 있다. 예를 들면 어떤 기업 내에서 서버 시스템의 관리자들은 해당 시스템에 항상 접근하는 중요 관리자이기에 특권 관리자로 분류될 수 있다. 또한, 어떤 기업 내 중요 소프트웨어 개발자들도 중요 자산인 소스 코드에 접근하고 또 이를 개발하는 개발자이기에 특권 사용자로 구분할 수 있다. 반면, 일반적으로 기업 내 대부분의 사용자는 업무를 위한 일반적인 애플리케이션에 접속하거나, 일반적인 데이터를 다루는 일반 사용자로 분류될 수 있다.

접근 주체 및 리소스에 대한 식별과 목록화가 완료되면, 접근제어에 대한 구체적인 시나리오 혹은 유스케이스를 구성할 수 있다. 이는 특정 사용자가 리소스에 접근할 때에 대한 신뢰도 평가 및 접근권한 부여 방안을 제시할 수 있다.

예를 들어, 사업부서 혹은 경영부서 임직원들은 주로 기업의 업무 애플리케이션에 접속하여 본인의 부서 업무를 진행하게 된다. 이때 일반 사용자들이 자신들의 업무 수행을 위해 업무 애플리케이션에 접속 시 해당 사용자에 대한 신뢰도 평가가 우선시 되어야 할 수 있다. 이 경우, PDP는 해당 사용자 계정, 인증 정보 및 기타 신뢰도 판단용 데이터를 확인함으로써 각 애플리케이션에 접속 가능한 신뢰도를 확인하고, 충분한 신뢰도가 확인되는 경우 애플리케이션에 대한 접근을 제어하는 PEP를 통해 해당 애플리케이션에 접근하는 시나리오를 생각해 볼 수 있다. 또한, 여기에서 해당 사용자가 평상시 이용하지 않는 기기를 이용하여 접속하는 경우, 추가 인증을 요구하거나 관리자 확인을 거쳐야만 충분한 신뢰도를 갖는 것으로 판단할 수도 있을 것이다.

또한, 이를 통하여 제로트러스트 아키텍처의 도입을 위해 필요한 보안 기능 및 구조, 기업망 세분화 전략에 대한 상위 수준의 접근이 가능할 것이다. 예를 들어, 기업에 따라 통합 ICAM 및 PAM에 대한 요구가 발생할 것이며, 시스템, 애플리케이션, 데이터에 대한 각각의 접근제어 전략을 실현시켜주는 PDP·PEP 구조를 구체화할 수 있을 것이다. 또한, 어떤 리소스들끼리 그룹화하여 네트워크를 세분화하고 접근 경로를 제한하는 것이 적절한지에 대한 전략을 구상할 수 있고, 이를 통하여 세분화된 구역에서의 개별적인 보안 정책, 각 구역 간 트래픽 허용 정책 등을 수립하는 것이

가능하다.

나. 현재 보안 아키텍처 분석

앞에서는 기업망에서의 보호 대상인 접근 주체와 리소스를 식별하고 이를 기반으로 제로트러스트 관점의 접근제어 시나리오 혹은 유스케이스를 수립할 수 있음을 언급하였다. 또한, 이를 바탕으로 제로트러스트 아키텍처 도입을 위해 필요한 보안 기능 및 구조, 기업망 세분화 전략을 상위 수준에서 수립할 수 있음을 제시하였다.

기업망의 현재 보안 아키텍처 및 보안 수준을 분석하는 것은, 현재 상황(As-Is)을 바탕으로 필요한 보안 기능을 구체적으로 도출하는 과정을 통하여 제로트러스트 목표 모델(To-Be)을 설계하는 데 있어 필수적인 과정이다. 이러한 현재 상황 분석과 목표 모델 수립은 3장에서 정의한 제로트러스트 성숙도 모델 2.0에 기반하여 수행할 수 있다.

제로트러스트 도입을 준비하는 담당자는 먼저 현재 기업망의 보안 아키텍처를 분석해야 한다. 기업망 내부에 있는 다양한 시스템과 애플리케이션, 데이터에 대한 식별이 되어 있는 상태이며, 이들에 대한 공격 및 비정상 접근 등을 방어할 수 있는 보안 아키텍처는 완전히 파악된 상태가 아닐 수 있다. 일부 기업들은 필요한 애플리케이션을 도입하는 과정에서 IT 담당 직원과 보안 담당자 간 충분한 논의를 거치지 못하여 기존 보안 체계와 잘 연동되지 않게 되거나, 해당 애플리케이션에 특화된 보안 기술을 같이 도입함으로써 일관된 보안 정책이 적용하지 못하는 사례가 있다.

따라서 현재의 보안 아키텍처를 명확하게 분석하여야 하며, 이는 IT 담당 직원, 외부 용역 직원 및 일반 직원들의 협조가 필요할 수 있다. 이들과 인터뷰, 기업망 내부 인프라 시스템 도입 관련 문서, 실사 등을 통하여 기업망 전반에 걸쳐 구현되어 있는 보안 아키텍처를 정확히 파악하여야 한다. 이를 위해 다음과 같은 과정을 진행할 수 있다.

- 네트워크 인프라 확인: 기업의 네트워크 구조, 주요 네트워크 장치(방화벽, 라우터, 스위치 등), 서브넷 구조, 클라우드 등 외부 네트워크 기반 서비스 이용 현황 파악
- 보안 솔루션 분석: 방화벽, 침입 탐지 시스템, 인증 시스템 및 서비스 인가 구조, 단말 보호 솔루션 등 현재 운영 중인 모든 보안 도구 및 솔루션 파악
- 보안 정책 및 규칙 분석: 네트워크 내 트래픽 제어를 위한 방화벽 규칙, 접근제어 목록(ACL),

NAC, VPN 정책 등을 검토하여 현재 어떤 보안 정책이 적용되고 있는지 파악

- 달성해야 할 보안 규정·기준 파악: 기업이 달성해야 하는 보안 규정이나 기준이 존재하는 경우 위반할 수 없으므로 관련 규정과 기준을 명확히 분석하여 적용해야 하는 기술적·관리적 조치 및 현재 달성 여부 파악

기업들은 주기적인 취약점 점검 및 보안 감사 등을 통하여 기업망 전반에 걸친 보안 아키텍처를 파악하고 있으나, 이 과정에서의 목적은 구체적인 파악을 통하여 일관된 보안 정책이 적용되고 있는지, 기업망 내부에 대한 가시성을 확보하고 보안 상태를 중앙집중적으로 분석할 수 있는 구조인지를 알아내는 과정으로 볼 수 있다. 또한 일반 직원들과 인터뷰 과정에서 보안 아키텍처로 인하여 업무에 불편한 점에 대한 개선 방안 등을 파악할 수도 있을 것이다.

파악된 현재의 보안 정책과 절차를 문서화하고 이러한 내용이 제로트러스트 아키텍처 기본 원리와 부합하는지, 또한 성숙도 및 보안 수준은 어느 정도인지를 평가할 필요가 있다. 이 과정은 제로트러스트 아키텍처 도입 목표 수립을 위해서 반드시 필요하며, 제로트러스트 성숙도 모델에서 제시하고 있는 각 기업망 핵심 요소별 기능 및 세부역량에 대한 성숙도 수준과 비교함으로써 현재의 보안 수준을 진단할 수 있다. 이 과정을 거칠 경우 현재 기업망의 제로트러스트 수준이 어느 위치에 있는지 한 눈에 파악할 수 있으며, 이후 목표 제로트러스트 성숙도 및 보안 기능 달성을 위하여 도입해야 할 제로트러스트 보안 기술·솔루션에 대한 검토 후 단계별 목표 달성 전략 및 계획을 수립하는 데 도움이 될 것이다.

2. 기업망을 위한 제로트러스트 아키텍처 정의 및 구현 로드맵 수립

가. 제로트러스트 도입 로드맵 수립을 위한 미 국방부 사례

제로트러스트 아키텍처 기반으로 기업 혹은 기관이 제로트러스트 도입 및 구축을 진행하고 있는 가장 중요한 참고 사례 중 하나는 미 국방부의 사례이다. 이미 제로트러스트를 중요한 사이버 보안 전략의 하나로 고려하고 있던 미 국방부는 다른 미 연방 기관들보다 빠르게 제로트러스트 아키텍처 구축 계획을 수립하기 시작했다.

미 국방부는 미 연방정부 차원의 제로트러스트 아키텍처 도입을 선언한 '국가 사이버보안 개선'에 관한 바이든 대통령 행정명령보다 빠른 2021년 2월 제로트러스트 참조 아키텍처 1.0(Zero Trust

Reference Architecture V1.0)을 발표한 바 있으며, 이후 첫 버전을 더욱 상세하게 수정하고 보완하여 2022년 7월 제로트러스트 참조 아키텍처 2.0(이하, ZTRA 2.0)을 발표하였다. 또한, 2022년 10월 ZTRA 2.0을 기반으로 미 국방부는 제로트러스트 전략(Zero Trust Strategy) 및 로드맵을 발표하였다. 해당 전략 문서에 따르면 미 국방부는 2027년 말까지 목표(Target) 수준의 제로트러스트 아키텍처 구축을 진행 중에 있다. ZTRA 2.0의 목차 및 내용은 다음과 같이 이루어져 있다.

표 4-4 미 국방부 ZTRA 목차 및 주요 내용

목차	주요 내용
1. 목적과 전략적 목표	▸ 제로트러스트 도입의 배경과 목적 설명 ▸ 제로트러스트가 적용될 미 국방부의 대상 시스템과 환경에 대한 정의 ▸ 제로트러스트 구현을 통해 달성한 목표에 대한 정의
2. 핵심 요소와 원칙	▸ 제로트러스트 구현 원칙을 정의 ▸ 제로트러스트 구현 핵심이 되는 제로트러스트 성숙도 모델의 핵심 요소(Pillar) 정의
3. 역량	▸ 제로트러스트 핵심 요소 별로 필요한 상세 제로트러스트 보안 역량(Capability) 정의 ▸ 미 국방부 내 IT 시스템과 제로트러스트 핵심 요소, 그리고 제로트러스트 보안 기능을 상호 연결하여 최종 목표 구조 정의
4. 유스케이스	▸ 다양한 보안 기능 측면에서 제로트러스트 아키텍처를 적용하기 전과 후의 모델 비교를 통하여 구현 사례 예시 ▸ 상세 사례를 통해 제로트러스트 보안 역량이 어떻게 구현되어야 할지, 어떻게 동작되어야 할지 사례를 보여줌
5. 기술적 위치	▸ 제로트러스트 아키텍처를 구현함에 준용해야 할 IT 보안 기술과 표준, 특히 제로트러스트 관련 중요 표준 또는 가이드라인에 대해서 정의 ▸ 더불어 미 국방부 내의 IT 관련 정책 또는 현존하는 시스템들과의 연계 구조, 기 정의된 제로트러스트 기반 기술들의 활용에 대해 정의
6. 보안 평가	▸ IT 보안 측면의 기존 거버넌스 정책이 제로트러스트 아키텍처를 도입할 때 어떻게 검토되고 연계되어야 하는지에 대한 정책 검토를 정의 ▸ 데이터 거버넌스 정책과 애플리케이션 개발 거버넌스 정책에 대하여 제로트러스트 보안 체계 도입 시 검토되고 고려되어 제로트러스트 설계가 진행되어야 함을 설명
7, 아키텍처 유형	▸ 제로트러스트 아키텍처 유형의 예제를 정의하고 이에 필요한 제로트러스트 보안 역량과 매핑 ▸ ID 서비스에 대한 외부 서비스 연계를 정의하고 설명
8. 아키텍처 전환 계획	▸ 제로트러스트 성숙도 모델을 제시하고 이에 맞는 형태로 제로트러스트 아키텍처 전환계획 추진 설명 ▸ 전환을 위한 IT 시스템의 영역 기준을 설명하고 이에 대한 항목들을 제시
9. 부록	▸ 시스템 및 서비스 구성 요소의 내용을 설명 ▸ 기술용어 및 참조 표준 정리 요약 ▸ 제로트러스트 보안 역량에 대한 상세한 정리
10. 참고	참고 문헌

나. 제로트러스트 아키텍처 구축 방안

1) 제로트러스트 성숙도 모델 기준 정의

제로트러스트 성숙도 모델은 어떤 IT 시스템의 보안체계를 제로트러스트 아키텍처 구조로 전환될 때 참조할 수 있는 성숙도 모델로, 기업들이 달성해야 하는 개념적 보안 목표를 포함하고 있다고 볼 수 있다. 성숙도 모델은 각 기업망의 핵심 요소에 대해 제로트러스트 관점에서 요구되는 보안 기능에 대하여 제로트러스트 성숙도에 따르는 기능별 수준을 명시한다.

본 가이드라인은 기업망의 핵심 요소를 식별자·신원, 기기 및 엔드포인트, 네트워크, 시스템, 애플리케이션 및 워크로드, 데이터로 정의하고 있으며, 3.1절에서 4단계 성숙도 수준을 정의하였다. 기업이 자체 제로트러스트 아키텍처를 수립하는 경우 본 가이드라인의 성숙도 모델을 참고하도록 권고한다.

이 단계에서 제로트러스트 성숙도 모델을 정의하는 것이 중요한 이유는 기업이 제로트러스트 아키텍처 도입을 추진하는 경우 반드시 기준이 되는 제로트러스트 성숙도 모델 및 세부역량을 정의하여야, 이후 목표 모델을 정의해 나갈 수 있기 때문이다. 이렇게 정의된 제로트러스트 성숙도 모델은 현재 혹은 도입 이후 기업망의 제로트러스트 수준을 지속적으로 평가하고 진단하는 데도 활용할 수 있게 된다.

2) 보안 세부역량 도출 및 단계별 구축 계획 수립

제로트러스트 성숙도 모델을 기반으로 기업망에 제로트러스트 아키텍처를 도입하고자 하는 경우 제로트러스트 성숙도 모델의 목표 단계를 달성하기 위한 구체적인 제로트러스트 아키텍처 보안 세부역량을 도출함으로써 단계별 구축 계획을 수립할 수 있다.

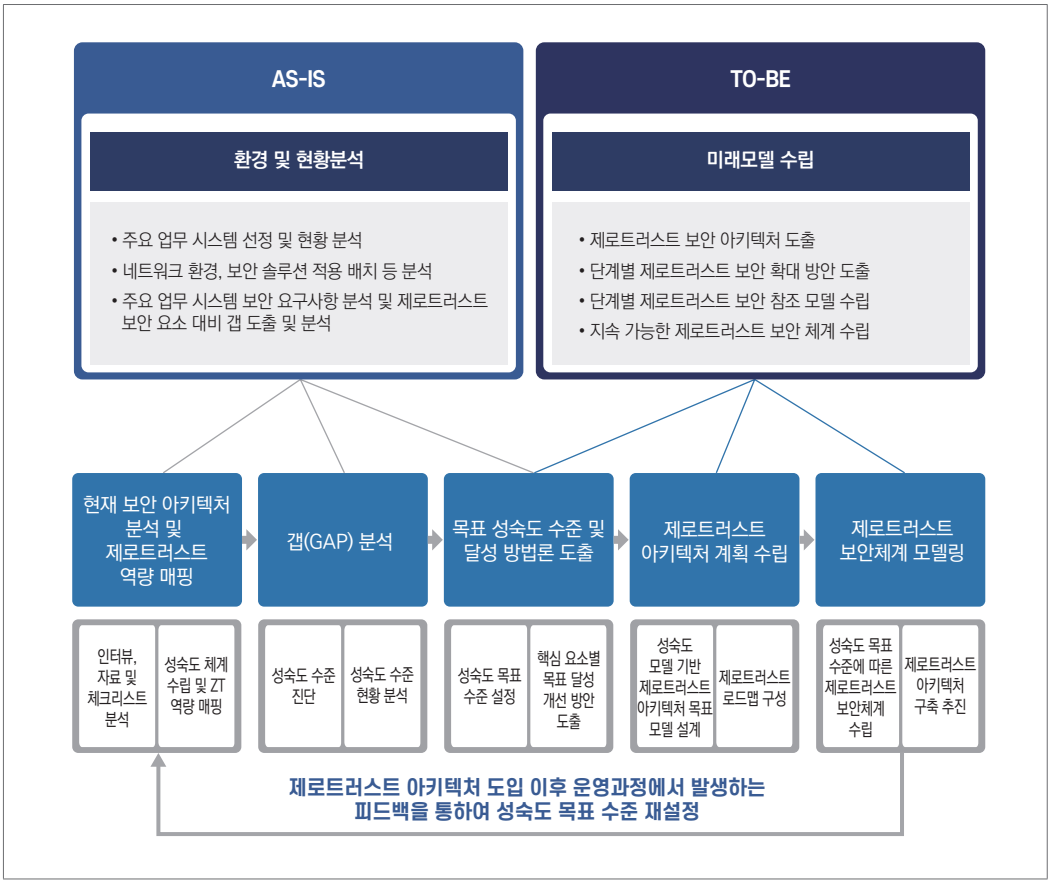
본 가이드라인 3.2절에서는 미 국방부의 보안 역량 정의 등을 참고하여 제로트러스트 성숙도 모델 2.0을 따르는 보안 세부역량 및 세부적인 성숙도 수준을 제시하였다. 현 단계에서 가장 구체화되어야 하는 부분은 제로트러스트 보안 세부역량을 정의하고 설계하는 것으로, 이는 기업망의 핵심 요소에 대한 성숙도 단계별 보안 항목을 구현하기 위한 보안 솔루션의 도입 계획으로 이어지게 될 것이다.

제로트러스트 아키텍처를 구축하고자 하는 기업은 본 가이드라인 3.2절의 제로트러스트 성숙도 모델 2.0에 따르는 보안 세부역량을 참고하여 자사 기업망 보안 아키텍처 분석 결과를 통하여 필요한 세부역량 및 목표 성숙도 수준을 정의한다. 즉 이 단계에서는 기업망에서 필요한 세부역량을 비즈니스 목표와 연계하여 도출한 후 기업의 비전과 목표에 따라 단계별 달성 전략을 수립할 필요가 있다.

3) 현재 보안 아키텍처 분석 결과와 제로트러스트 세부역량 연계

제로트러스트 아키텍처 계획 수립에서 핵심이 되는 부분은 현재 기업망의 보안 수준을 진단하고 이를 기반으로 목표 설계 모델을 도출하는 것이다. 아래 [그림 4-3]은 제로트러스트 아키텍처 모델을 설계하는 전체 절차를 보여주고 있다.

그림 4-3 제로트러스트 성숙도 모델 기반 제로트러스트 아키텍처 분석 및 설계



첫 단계는 앞에서 분석한 기업망의 현재 보안 아키텍처와 제로트러스트 성숙도 모델에서 정의하는 세부역량을 연계 및 연결하는 것이다. 각 기업은 기업망 보안 아키텍처 및 수준, 달성해야 할 보안 규정·기준이 다를 수 있기 때문에 각 기업에 가장 적합한 제로트러스트 성숙도 체계를 수립해야 하며, 이를 기반으로 보안 세부역량과 연계되는지를 확인해야 한다. 또한 이 단계에서는 목표 세부역량 및 성숙도 수준도 구체화할 수 있다.

둘째 단계는 현재 시스템에 대한 목표 모델과의 갭 분석을 추진하는 것이다. 이를 위해서 각 기업은 첫 단계에서 수립한 자체 제로트러스트 성숙도 수준 및 보안 세부역량 달성 계획을 기반으로 해당 항목이 성숙도 모델 4단계 중 어디에 위치하고 있는지 분석해야 한다. 이를 통해 현재 기업망의 보안 아키텍처가 어느 수준의 성숙도에 위치하는지, 목표 모델과는 어느 정도의 성숙도 수준 차이가 있는지 판단할 수 있게 된다.

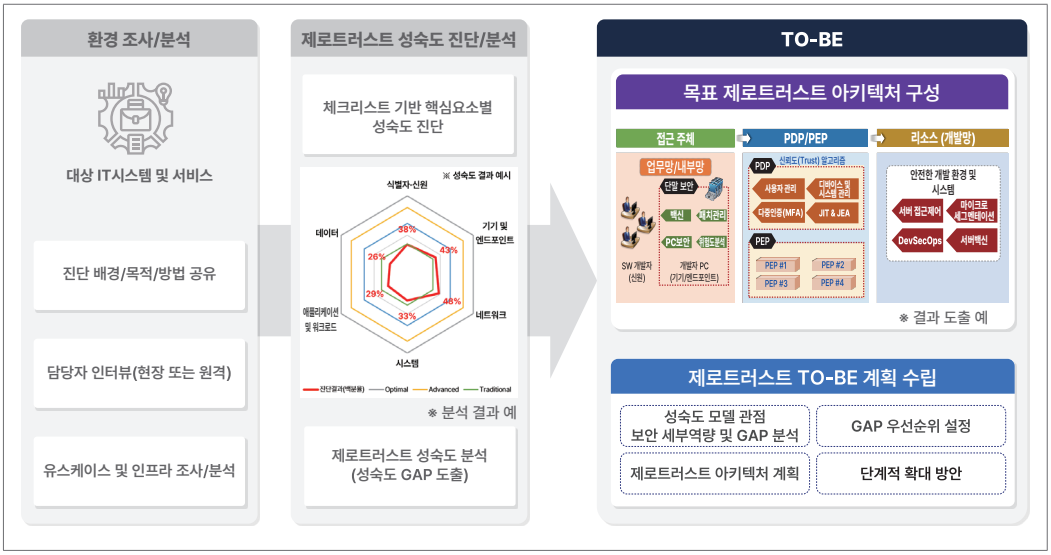
셋째 단계는 첫 단계에서 정리된 달성해야 할 목표 성숙도 수준 및 세부역량을 달성하기 위한 구체적인 방법론을 도출하는 것이다. 둘째 단계에서의 갭 분석을 통해 목표를 달성하기 위해 도입이 필요한 제로트러스트 보안 기술·솔루션을 검토하고 이를 통합 적용하는 방법론을 도출하고 검토해야 한다. 이를 통해 한 번에 모든 것을 검토하고 구축하는 것은 일반적으로 사실상 불가능하므로, 단계별·연차별 달성 전략을 통해 도입 보안 기술·솔루션에 대한 단계별 구축 계획을 수립해야 한다.

넷째 및 다섯째 단계는 앞서 세 단계에서 정리된 내용들을 기반으로 기업 고유의 제로트러스트 아키텍처에 대한 계획을 수립하고 제로트러스트 로드맵을 구성하여 해당 계획의 내용에 맞추어 기업망의 보안 체계 수립 및 제로트러스트 아키텍처 구축을 추진하는 것이다.

4) 제로트러스트 아키텍처 목표 모델 설계

현재 기업망의 보안 아키텍처 및 보안 수준을 분석할 때 앞서 설명한 대로 제로트러스트 성숙도 모델과 세부역량 기준 정립이 제일 중요하며, 이후 해당 기준을 근거로 현재 시스템에 대한 현황 분석이 중요한 절차가 된다. [그림 4-4]는 현황 분석과 이를 기반으로 목표(To-Be) 모델을 설계하는 절차와 내용을 보여주고 있다.

그림 4-4 현재 보안 아키텍처 성숙도 수준 분석 후 목표 제로트러스트 아키텍처 모델 구성 절차



기업망의 현재 보안 아키텍처에 대한 환경 조사 및 분석을 진행하고 기업망에 대한 성숙도 진단 및 분석 과정을 통하여 구체적인 보안 세부역량이 도출이 되었다면 제로트러스트 수준이 어느 위치에 있는지 한눈에 파악될 수 있을 것이다. 도출된 세부역량 정보와 앞서 설정한 제로트러스트 아키텍처 도입 목표를 바탕으로 갭 분석 및 도입해야 할 제로트러스트 보안 기술·솔루션에 대한 검토 후 우선순위를 설정함으로써 단계별 목표 달성 전략 및 계획을 수립할 수 있다.

5) 제로트러스트 아키텍처 구현 로드맵 수립

기업이 자사에 적용할 제로트러스트 성숙도 모델을 정의하고, 이를 기반으로 도입하고자 하는 제로트러스트 아키텍처를 설계하여 보안 세부역량을 구체화했다면, 마지막으로는 이를 기반으로 제로트러스트 아키텍처 구현 로드맵을 수립하고 제로트러스트 아키텍처에 포함해야 한다.

이를 위해서는 아키텍처 수립 과정에서 설계된 제로트러스트 성숙도 모델과 제로트러스트 세부역량을 기반으로 현재 기업망 보안 체계 전반에 대해 현재 제로트러스트 성숙도 수준을 분석하고, 달성 가능한 제로트러스트 수준을 결정한 후 이에 대한 해당 세부역량을 기준으로 제로트러스트 아키텍처 기능 수립 방법 및 일정 계획 수립에 대한 로드맵을 설계해야 한다.

4.1절에서 최적화 수준의 제로트러스트 아키텍처 구현이 단기간에 달성하기 어려움을 언급하고 최종 목표와 함께 몇 단계의 단기 목표와 실천 방안을 포함하는 장기적인 도입 계획 마련을 제안한 바 있다. 따라서, 구현 로드맵 수립은 이 제안을 고려하여 기존 IT 시스템 보안 체계를 단계별, 기간별로 제로트러스트 아키텍처 보안 체계로 전환하는 과정에서 상세 전략과 전술로 이용되어야 하며, 다음과 같은 과정을 거칠 수 있을 것이다.

① 기업에서 비즈니스 관점에서의 우선순위를 선정하여 가장 우선시되는 영역부터 도입하는 것을 목표로, 클라우드 도입, 재택 근무, 개발망 오픈 등 해당 기업 환경에서 우선 고려할 수 있는 유스케이스와 연관된 비즈니스 영역부터 도입 계획 수립

② 해당 유스케이스 및 비즈니스 영역에 대하여 반드시 필수적인 보안 세부역량 및 목표 보안 성숙도 수준을 정의

③ 보안 세부역량에 대한 성숙도 수준에 따라 세부적인 구현 수준으로 나누고, 개별적인 구현 수준에 대해 언제 어느 시기에 해당 기능을 도입·연동할지를 판단

④ 모든 세부역량에 대해 시기별로 달성 계획을 정리하면 구현 로드맵 형태로 구성하는 것이 가능하며, 예산과 솔루션 도입 시기, 기업의 우선순위, 규제 시기 등을 고려하여 2~3단계로 나누어진 세부 로드맵을 만들 수 있음. 이 세부 로드맵은 각 단계에서 달성하고자 하는 단계 목표 및 달성하고자 하는 세부역량, 그에 대한 성숙도 등을 포함하여야 함

| 제4절 |

제로트러스트 아키텍처 도입 준비 예시

본 절에서는 기업이 제로트러스트 아키텍처를 도입하기 위하여, 안전한 온프레미스 소프트웨어 개발 시스템 환경 구축 시나리오에 비추어 어떤 절차와 방법을 통하여 구현할 수 있는지 구성 예를 들고, 그에 대한 모델 분석을 통해 구체적으로 도입 준비 방안을 설명하고자 한다.

본 예시에서는 전체 기업망 환경에 대하여 제로트러스트 아키텍처를 도입하는 것이 아닌 개발 시스템 환경이라는 특정 비즈니스 프로세스에 대해 도입하는 과정을 예로 들고 있으며, 준비 과정으로 언급한 6가지 세부 과정 중에서 안전한 개발 환경 구축 관점에서는 기존 기업망 구조, 보호 대상 분석 및 보안 아키텍처, 보안 수준 분석 등이 이미 이루어진 상태로 볼 수 있다.

이 예시에서는 제로트러스트 아키텍처를 구체적으로 정의하는 과정에서의 접근법 3가지(인증 체계 강화, 마이크로 세그멘테이션, 네트워크 인프라 및 소프트웨어 정의 경계(SDP)) 중 ICAM을 중심으로 하는 인증 체계 강화 기반 접근을 가정하였다. 따라서 접근제어 정책 결정의 중심에는 식별자가 있으며, PDP는 사용자 및 기기의 식별자를 중심으로 위험도 분석 및 신뢰도 평가를 진행하여 접근 여부, 재인증 여부 등을 결정하게 된다. 이 접근법은 단지 예시일 뿐이므로, 기업망에서 도입을 하는 경우 뿐 ICAM을 중심으로 접근 정책을 결정하여야 하는 것은 아니며 다양한 방법이 가능하다는 점을 미리 밝힌다.

1. 제로트러스트 아키텍처 도입 목표 설정

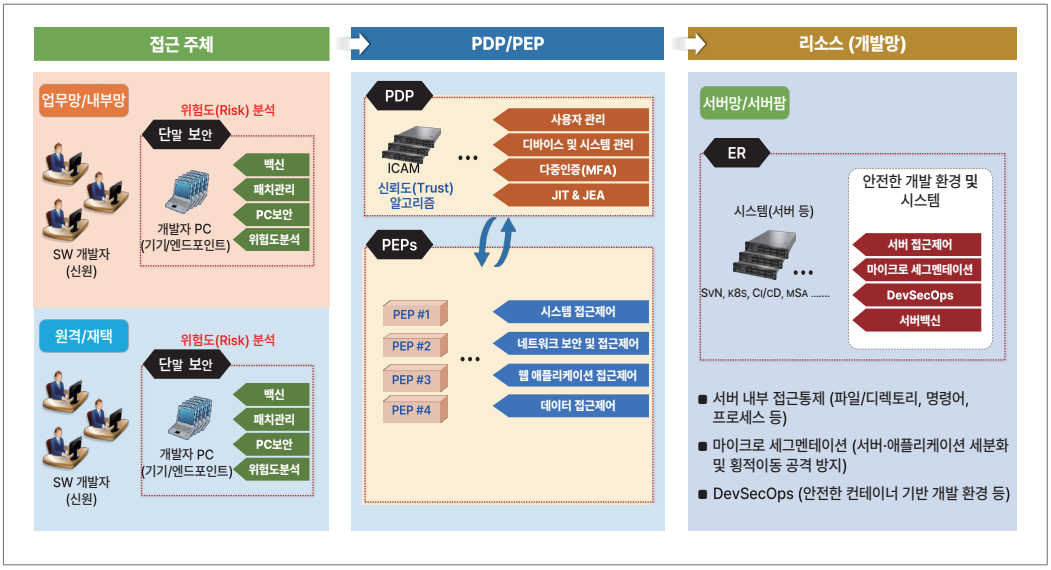
본 예제의 목표는 기업 내 소프트웨어를 개발하는 개발자 그룹에서 안전한 소프트웨어 개발 환경을 구축하는 것을 목표로 한다. 기업 개발 환경은 온프레미스 개발 환경과 퍼블릭 클라우드 개발 환경으로 나뉠 수 있는데 본 예제는 온프레미스 개발 환경 구성을 가정하여 안전한 개발 환경을 위한 제로트러스트 아키텍처 도입을 준비하는 과정으로 본다.

기업에서 중요 소프트웨어 개발자들은 외부 해킹 공격의 주요 목표가 된다. 해커들은 개발 환경에 침입하여 개발자의 권한을 탈취하고 이를 이용하여 소프트웨어 내 악성코드를 삽입하여 추가적인 공격 수단(예, 기업망 내부 모니터링, 악성코드 배포 등)으로 사용하기도 하고, 해당 기업의 주요 소프트웨어 소스 코드를 탈취하여 이를 무단사용·배포할 수도 있다. 그러므로, 기업에서 소프트웨어 개발 환경의 안전한 구축은 중요한 보안 목표 중 하나이다.

2. 제로트러스트 아키텍처 및 구성요소별 기능

제로트러스트 아키텍처를 기반으로 하는 안전한 소프트웨어 개발 환경 구축의 예에서 접근제어 대상 사용자는 특권 사용자로 분류될 수 있는 소프트웨어 개발자이고 보호 대상이 되는 리소스는 개발 환경이 구성된 서버 시스템과 개발에 사용되는 개발 도구, 그리고 개발 시스템 내에 있는 소프트웨어 코드 데이터 등이 될 수 있다.

그림 4-5 안전한 소프트웨어 개발 환경 구축을 위한 제로트러스트 아키텍처



안전한 소프트웨어 개발 환경 구축을 위한 제로트러스트 아키텍처를 간단히 요약하면 [그림 4-5]와 같다. 아키텍처 내부의 각 논리 구성요소 및 여기에서 필요한 성숙도 모델 기준과 세부역량에 대해서는 다음과 같이 표현할 수 있다.

1) 접근 주체 구성

소프트웨어 개발자들은 본 환경에서 '접근 주체'에 해당하는 특권 사용자들로서 제로트러스트 아키텍처의 보호 대상이자 관리 대상이 된다. 해당 개발자들은 개발을 위하여 자신들의 PC를 사용하며 이는 제로트러스트 관점에서 '기기 및 엔드포인트'로 정의된다.

제로트러스트 아키텍처 구성에서 모든 개발자들은 자신의 개발자 PC에 위험도 분석을 위한 사용자 보안 소프트웨어(예: UEM)를 설치한다. 해당 소프트웨어는 개발자가 개발 환경 접속 시 해당 개발자 기기의 보안 상태(멀웨어·바이러스 점검 결과, 패치 업데이트 상태 등)를 점검하고 위험도를 분석하여, 사용자와 단말의 보안 컨텍스트 정보를 PDP에 제공하게 된다.

2) 정책결정지점(PDP)/정책시행지점(PEP) 구성

소프트웨어 개발자들은 본 환경에서 개발 환경망 내에 있는 리소스인 개발 시스템에 접근하기 위해서는 PEP를 통해 리소스 접근 승인을 받아야 한다. 리소스마다 별도의 PEP 게이트웨이를 구성할 수 있으며, 본 예제에서는 크게 4개의 접근제어 PEP를 구성하였다. 이들은 각각 다음과 같은 목적과 기능을 제공한다.

- 시스템 접근제어 PEP: 시스템 개발자의 경우 해당 개발 시스템의 개발 환경을 사용하는 것이 우선이지만 때에 따라서 개발한 소스코드 테스트 및 환경구성을 위해서 시스템 운영체제(OS) 관리자 계정으로 접속하여 다양한 시스템 구성 및 운영 작업을 수행할 수 있다. 이를 위해 PAM 세부역량을 통해 해당 서버 관리자 계정에 접속하기 전 해당 사용자의 계정, 인증, 권한 등을 확인하여 상세한 접근제어를 진행할 수 있다.
- ZTNA PEP: 소프트웨어 개발자들은 기업 내에서 근무하면서 개발시스템에 접속할 수도 있고, 재택 근무 또는 원격 근무지에서 개발시스템에 접속할 수도 있다. 이러한 경우 해당 기기는 전통적인 네트워크 보안 채널 구성인 VPN(가상사설망)이나 SSL-VPN(웹 가상사설망)을 사용하여 외부에서 기업 내부 네트워크로 접속하게 된다. 일반적으로 ZTNA는 네트워크 보안 접속 기능에 추가적으로 웹 애플리케이션(서비스) 접속에 대한 접근제어를 포함한다. ZTNA를 통해 원격지에서의 안전한 네트워크 접속 및 중요 웹 기반 개발 업무시스템의 접근제어를 함께 수행할 수 있다.
- 웹 애플리케이션 접근제어 PEP: 기존에 이미 VPN이나 SSL-VPN을 사용하고 있는 환경이고, 별도의 ZTNA 체계 도입 없이 웹 애플리케이션 접근제어를 하고자 한다면 웹

애플리케이션 접근제어를 위한 PEP를 도입할 수도 있다. 이는 기존의 원격 접속에 대한 네트워크 보안 체계는 전통적인 방식을 사용하고 추가적으로 웹 애플리케이션 접근제어 PEP를 구성하여 해당 PEP가 웹 애플리케이션 접속을 진행하는 기기로 사용될 수 있다. 예를 들어 차세대방화벽(NGFW)은 웹 애플리케이션인 L7 레이어를 통제할 수 있기 때문에 웹 애플리케이션 PEP로 사용될 수 있다. 그러나, 그 외 기능이 필요하다면 또 다른 형태의 보안 기술이나 솔루션이 사용될 수 있다.

- 데이터 접근제어 PEP: 개발 환경은 다양한 소스코드와 해당 코드에 관련된 문서 산출물이 존재하게 된다. 소스코드의 경우 다양한 개발 소프트웨어 기반 개발 도구들을 사용하기 때문에 개발자가 작성한 코드가 해당 개발자에 의해 외부로 유출되거나 소스 코드 저장소에 외부 해커가 접속하여 소스 코드 유출을 방지해야 할 필요가 있게 된다. 또한, 소스 코드와 관련된 각종의 개발 산출물 문서의 외부 유출 역시 막아야 할 필요가 있게 된다. 이를 위해 기업은 소스 코드 생성 시 자동으로 로컬 또는 소스 코드 저장소 서버에 암호화하여 저장하게 할 수도 있고 동시에 외부로 소스 코드가 유출되는 것을 탐지하고 막기 위해서 데이터 유출 방지 기술인 DRM 및 DLP 세부역량을 이용하여 소스 코드 및 문서 유출 탐지를 진행할 수 있다. 이때 DRM 및 DLP가 동작하는 지점을 PEP로 정의하여 해당 보안 기능의 동작 시 소프트웨어 개발자의 신뢰도를 판단할 수 있는 컨텍스트 정보와 인증 등을 PDP와 연동시켜 데이터 접근제어의 보안 기능을 강화할 수 있다.

상기 접근 요청에 대해 최종적으로 승인하는 것은 PDP의 역할이다. 본 예시에서는 ICAM에 PDP를 구축하여 활용하는 것을 가정하고 있으며, PEP로부터 접근 요청 정보, 사용자 및 기기 식별자 기반 인증 정보, 그리고 개발자 PC에 설치된 사용자 보안 소프트웨어가 제공하는 보안 컨텍스트 정보, 그 외 보안 이벤트 등을 이용하여 현재 접근에 대한 신뢰도를 도출한다. 도출된 신뢰도는 사용자·기기에 대한 접근 허용을 위한 중요한 정보로 사용된다. 개발자가 개발 시스템 접근 후 업무를 진행하는 경우에도 해당 신뢰도는 주기적으로 점검되며, 만약 개발 PC의 보안 위협이 발생하여 신뢰도가 낮아지는 경우 PDP에서는 PEP를 통하여 개발자에게 재인증을 요청하거나 현재 세션을 종료시킬 수 있다.

3) 개발망에서의 리소스 구성

소프트웨어 개발망은 다양한 개발 환경 및 시스템으로 구성될 수 있다. 주로 개발 소스코드에

대한 형상관리를 진행하는 형상관리시스템과 GitHub, Gitlab과 같은 소스코드 저장소(Repository) 등으로 구성되며 필요시 외부 클라우드 형상관리시스템이나 소스코드 저장소가 사용될 수 있다.

내부 개발 시스템의 경우 형상관리시스템이나 소스코드 저장소를 보안 등급에 따라 다수의 존으로 물리적 분리를 진행할 수 있고 가상환경에서 VM 분리를 통한 논리적 분리를 진행할 수도 있게 된다. 물리적 구성 분리의 경우 네트워크 보안 기반의 매크로 세그멘테이션을 진행하여 각 보안 등급 간 물리적 구역의 횡적 이동을 어렵게 할 수 있다. 이때 보안 기능으로는 네트워크 방화벽(Firewall), 침입탐지시스템(IDS) 및 침입방지시스템(IPS) 등이 사용될 수 있다.

만약 가상환경 기반의 VM 단위 또는 컨테이너(Container) 단위로 논리적 분리를 진행한다면 VM이나 컨테이너 간 횡적이동 공격을 막기 위한 마이크로 세그멘테이션(Micro Segmentation) 보안 기능이 적용되어야 할 필요가 있다. 해당 기능은 호스트 기반의 방화벽이나 침입탐지 및 차단시스템, 그리고 호스트 접근제어 등이 사용될 수 있으며, 더불어 서버 백신, 무결성 관리, 화이트리스트 기반 제어 등의 보안 기술이 사용될 수 있다.

또한, 컨테이너 기반의 MSA 개발 환경을 구성하고 이를 위하여 DevOps(Development Operations) 기반의 개발 환경을 구성하여 사용한다면 클라우드 네이티브 보안 체계인 CNAPP 보안 체계를 도입하여 개발 과정에서 발생할 수 있는 다양한 보안 위협을 줄일 수 있도록 개발 시스템을 구성할 수 있다. 이때 소프트웨어 개발자의 개발 환경 접근 시 PEP와 PDP를 이용한 사용자 인증, 사용자 PC 보안 강화 등을 연계, 연동시켜 보안성을 강화할 수 있다.

다. 제로트러스트 아키텍처 관점 성숙도 모델 및 세부역량 분석

앞서 구성한 제로트러스트 아키텍처에서는 구성요소 및 필요한 보안 기능들을 언급하였다. 이를 구체화하기 위하여 성숙도 모델 및 세부역량 기준에 대한 정의가 필요하며, 차후 이를 토대로 아키텍처를 수립한 후 제로트러스트 아키텍처 및 구현 로드맵을 수립할 수 있을 것이다. 안전한 소프트웨어 개발 환경 구축을 위한 제로트러스트 아키텍처는 제로트러스트 성숙도 모델을 기준점으로 삼았고, 이를 위한 보안 세부역량을 도출하여 구성된 것이다.

〈표 4-5〉은 목표 시스템 구성을 위한 제로트러스트 세부역량 도출의 예를 보여주며, 전체 6대 핵심 요소 중 첫째 요소인 식별자·신원에 대한 필요 성숙도 기능 및 보안 세부역량을 정의·설명하였다. 앞서 간단히 언급한 바와 같이, 본 예시에서 PDP는 ICAM이 그 역할을 담당하고 있다고 가정하고 있으며, 실제 기업들은 각자 상황에 따라 적절하게 PDP를 구성할 수 있다.

표 4-5 SW 개발 시스템에서 사용자 핵심 요소의 제로트러스트 성숙도 및 보안 기능

성숙도 기능	세부역량	세부역량 설명
식별자 관리	사용자 인벤토리	‣ 사용자 그룹 중 소프트웨어 개발자를 특권 사용자로 구분하여 사용자 계정을 등록하고 관리함 ‣ 해당 보안 기능은 PDP 역할을 하는 ICAM에서 구현되며 사전에 개발자의 계정을 등록하고 적용할 MFA 종류를 결정하며, 개발 환경 접속 시 필요한 신뢰점수를 속성 관리 값으로 등록함
	ID 연계 및 사용자 자격 증명	‣ 전체 소프트웨어 개발자의 규모가 크고 다양한 부서와 다양한 개발 환경으로 분산되어 있는 경우 기 구축된 인사정보시스템 또는 계정관리시스템과 연동하여 개발자 그룹에 대한 계정 관리를 동기화하고 일원화함 ‣ 개발자 인증 시 인증 시스템과의 통합 인증 연동체계도 동작될 수 있도록 구성함
인증	다중인증 (MFA)	‣ 소프트웨어 개발 시스템에 접속 시 개발자는 반드시 MFA를 사용하도록 함 ‣ 개발자 시스템 접속 인증 시 필요한 경우 접속 시점의 상황을 인지하고 이를 인증 요소에 반영할 수 있는 체계도 마련할 수 있도록 함
	지속 인증	‣ 개발자 소프트웨어 개발 시스템에 접속하여 업무를 진행하는 경우 최초 접속 시 한 번의 인증만으로 무한정 업무를 진행하는 것이 아니라 수시로 개발자 PC의 보안 상태 정보나 개발자의 상황 환경을 파악하여 위험정보가 판단되는 경우 재인증 요청 또는 강제 세션 종료를 통해 지속적 인증 체계를 수립함
위험도 평가	통합 ICAM 플랫폼	‣ 정책결정지점이 PDP에서 ICAM 시스템을 기반으로 특권 사용자인 소프트웨어 개발자의 계정을 관리하고 인증 수행을 진행하며, 접속 권한에 필요한 신뢰점수 값을 등록 관리함 ‣ 정책에 따라 개발자의 속성 정보 값을 이용하여 최소한의 권한 관리체계를 구축
	행동, 상황적 ID 및 생체 인식	‣ 개발자의 행동 패턴, 상황적 정보를 인지하여 이상 징후 발생 시 추가 MFA 인증 진행 ‣ PAM과 적시/최소권한접근(JIT/JEA) 제어 시스템과 연계하여 적절한 개발자의 접근 제어를 수행
접근 관리	조건부 사용자 접근	‣ 개발자들이 소프트웨어 개발 시스템에 접속 시 적절한 시간 내에만 접속할 수 있도록 적시접근(JIT) 기능을 제공하고 PAM과 연계하여 최소권한접근(JEA)을 가질 수 있는 조건부 접근 체계를 마련함 ‣ 이는 ICAM에서 이루어지며 이를 위해 기업 리소스 내 모든 시스템들은 사전에 ICAM에 등록 관리되어야 함
	최소 권한 접근	‣ 개발자들이 소프트웨어 개발 시스템에 접속하여 개발업무를 수행하는 경우 일반적으로 두 가지 기업 리소스에 대한 접근이 필요할 수 있음. 첫째는 개발 업무를 지원하는 개발 애플리케이션에 접속하여 개발 업무를 진행하는 경우이고, 둘째는 개발 업무를 진행하면서 해당 서버 시스템에 관리자로 접속하여 다양한 시스템 설정 관리 업무를 진행하는 경우임 ‣ 이때 둘째 경우에는 해당 개발자는 다양한 개발 환경 설정 업무를 위해서 루트 권한을 확보하여 중요 업무를 수행하게 되는데 이때 JIT/JEA 권한 제어가 이루어지지 않게 되는 경우 해당 계정 및 업무가 외부 해커에 장악되는 등 심각한 피해가 발생할 수 있음

상기 과정을 각 기업망 핵심 요소 별로 정리하고 필요한 보안 기능을 도출한다면 기업은 해당 보안 기능 구현을 위한 보안 기술 및 보안 솔루션 도입을 정의할 수 있게 된다.

아래 〈표 4-6〉은 보안 기능 도출 과정을 거친 후 해당 보안 기능을 위해 필요로 하는 제로트러스트 보안 기술(기능 혹은 보안 세부역량 기반)을 최종 도출한 것이다. 이러한 일련의 과정을 통해 기업은 기업망 내 다양한 유형 및 유스케이스에 대한 제로트러스트 아키텍처를 구축할 수 있는 단계적 절차를 이해할 수 있을 것이다.

표 4-6 SW 개발 시스템에 제로트러스트 아키텍처 적용을 위한 기업망 핵심 요소 및 보안 기술 정의

기업망 핵심 요소	대상	필요로 하는 제로트러스트 보안 기술
식별자·신원 (Identity)	▸ 소프트웨어 개발자	▸ ICAM 등록 관리 ▸ 다중인증(MFA) ▸ 적시/최소권한접근(JIT/JEA) 제어
기기 및 엔드포인트 (Device/Endpoint)	▸ 소프트웨어 개발자가 사용하는 개발용 업무 PC	▸ 신뢰도 판단 ▸ PC 위생(Hygiene) → UEM
네트워크 (Network)	▸ 기업 내 온프레미스 환경 내에서 개발 연구소 내 개발자 PC부터 개발 서버 시스템까지의 네트워크 연결 구간 ※ 기업 외부에 접속하는 경우(재택/원격 근무) 해당 개발자 PC에서 기업 내 개발 서버 시스템까지의 연결 구간	▸ 암호화 채널 ▸ 다양한 네트워크 보안 기술 및 체계 ▸ 마이크로 세그멘테이션
시스템 (System)	▸ 개발 도구 애플리케이션이 설치된 서버 시스템 ▸ 개발 소스 코드가 저장된 서버 시스템	▸ 시스템 접근제어 (PAM)
애플리케이션 및 워크로드 (Application & Workload)	▸ 개발 도구 애플리케이션 ▸ 가상화 환경에서의 PaaS 플랫폼 (VM, 컨테이너, 쿠버네티스 등)	▸ 애플리케이션 접근제어 ▸ 워크로드 보호 ▸ 안전한 컨테이너 네이티브 개발 환경 (DevSecOps)
데이터 (Data)	▸ 개발 소스 코드	▸ 데이터 암호화 ▸ DRM ▸ DLP

제로트러스트 아키텍처 도입을 추진하는 경우 기업은 우선 제로트러스트 아키텍처를 적용하고자 하는 대상 시스템을 선정해야 한다. 그리고 해당 대상 시스템에 제로트러스트 아키텍처로의 논리적 구성 전환을 시도하며, 어떠한 제로트러스트 보안 기능·세부역량이 적용되어야 하는지 3.2절을 참고하여 구성할 수 있다. 이때 기업은 각 제로트러스트 성숙도 모델과 제로트러스트 보안 기능

기준을 기반으로 현재 구성된 기업망의 현재 수준을 진단하고 이를 기반으로 향후 구현할 단계별 수준을 목표로 설정하게 되면 이것이 각 기업·기관이 도입하려는 제로트러스트 아키텍처의 핵심 기준이 될 수 있다.

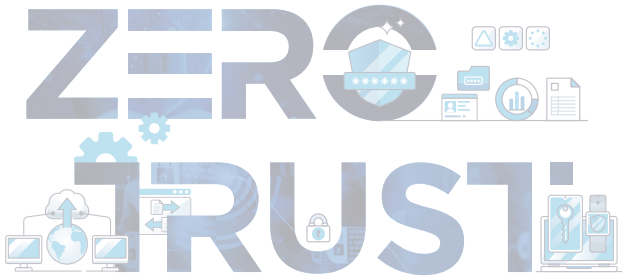
3. 제로트러스트 아키텍처 구현 로드맵 수립

제로트러스트 아키텍처 구현 로드맵 수립은 본격적으로 제로트러스트 아키텍처를 도입하기 전에 수립하는 것이 바람직하다. 최종 목표와 필요한 보안 세부역량 등이 정의가 되어 있기 때문에, 이들에 대해서 한 번에 도입할 수 있는지, 세부 단계를 나누어 단계별 목표 수립 및 도입을 추진할 것인지에 대해 결정을 해야 한다.

예를 들어, 세부 단계로 나눈다면 사용자 핵심 요소와 관련하여 다음과 같은 단계별 실행 계획 수립이 가능할 것으로 보인다.

- 1단계: 빠르게 도입 가능한 영역 식별. 사용자 인벤토리, MFA 도입, 통합 ICAM 플랫폼, 조건부 사용자 접근 등 기술 적용
- 2단계: ID 연계 및 사용자 자격 증명 기법 도입 및 고도화, 최소 권한 접근 세부역량 적용
- 3단계: 실시간 모니터링과 이상 탐지 시스템 구축이 가능한 구조 확립. 지속 인증이나 행동, 상황적 ID 및 생체 인식 기술 등 적용

각 단계별로 기업 규모에 맞는 도입 시기와 시간, 예산 등을 결정하여야 하며, 이보다 앞서 구체적인 시스템 구성도, 보안 기능 동작 절차도, 도입할 보안 솔루션 정의, 보안 솔루션 도입·구축 계획 등을 정의할 수도 있으나, 먼저 단계별 도입 기간을 확립한 후 그에 맞춰 위 내용을 상세히 정리할 수도 있다. 필요에 따라서는 사용자, 기기, 시스템, 데이터 등에서 어떤 요소가 먼저 보호되어야 하는지를 정의하여 리소스를 효율적으로 사용하고 가장 중요한 자산부터 보호하는 전략도 필요하다.


ZERO
TRUST

제로트러스트
가이드라인 2.0

제5장

제로트러스트 도입 수준 분석

| 제1절 | 제로트러스트 성숙도 기반 도입 수준 분석

| 제2절 | 제로트러스트 침투 시험 기반 효과성 분석

| 제1절 |

제로트러스트 성숙도 기반 도입 수준 분석

1. 제로트러스트 성숙도 수준 평가를 통한 보안 수준 분석 방안

제로트러스트 성숙도 수준을 평가하여 보안 수준을 분석하는 것은 조직의 보안 체계를 체계적으로 진단하고 강화하기 위한 중요한 과정이다. 이 평가 방법은 조직이 현재 어떤 수준의 제로트러스트 보안 체계를 구축하고 있는지를 파악하고, 향후 개선해야 할 영역을 식별하며, 이를 통해 전반적인 보안 성숙도를 높이는 데 도움을 준다.

먼저, 제로트러스트 성숙도 수준을 평가하기 위해서는 명확한 성숙도 모델과 평가 프레임워크를 설정해야 한다. 성숙도 모델은 일반적으로 여러 단계로 나뉘어 있으며, 각 단계는 보안 정책, 기술적 요건, 운영 절차, 조직의 보안 문화 등을 포함한다. 이러한 모델은 단계별로 조직의 보안 성숙도를 평가할 수 있도록 도와준다.

앞에서 우리는 성숙도 모델을 네 가지 단계로 설명하였다. 준비 단계에서는 제로트러스트 도입을 위한 기초 작업이 이루어지며, 조직이 보안 인프라를 점검하고 초기 계획을 수립하는 단계이다. 기본 단계에서는 기초적인 보안 정책과 기술이 마련되며, 제로트러스트의 기본 원칙이 일부 구현되기 시작한다. 향상 단계에서는 제로트러스트 원칙이 더 체계적으로 적용되며, 다양한 보안 조치들이 조직 전반에 걸쳐 통합되고 강화된다. 최적화 단계에서는 제로트러스트의 모든 원칙이 전반적으로 구현되고, 이를 바탕으로 지속적인 모니터링과 개선이 이루어지는 상태를 의미한다.

이후에는, 제로트러스트 성숙도에 대한 이해를 바탕으로 성숙도 평가의 핵심인 평가 요소를 선정해야 한다. 제로트러스트 성숙도 수준을 평가하기 위해서는 조직의 다양한 보안 측면을 다각도로 분석해야 한다. 주요 평가 요소는 성숙도 모델에 기반하여 다음 장에서 설명한다.

평가 요소가 선정되었다면, 이제 실제 평가를 수행하게 된다. 이 과정에서는 조직의 현재 상태를

기준으로 각 평가 요소별로 상세한 분석이 이루어진다. 이를 위해서는 다음과 같은 다양한 방법이 사용될 수 있다.

- 설문조사 및 인터뷰: 조직 내 보안 담당자 및 관련 부서와의 인터뷰와 설문조사를 통해 현재 보안 정책과 기술 도입 수준을 파악한다.
- 기술적 평가: 보안 인프라, 네트워크, 애플리케이션 등을 대상으로 기술적인 점검과 테스트를 통해 실제 보안 상태를 진단한다. 예를 들어, 침투 테스트(penetration testing)나 취약점 스캔(vulnerability scanning)을 통해 현재 보안 체계의 강점과 약점을 파악할 수 있다.
- 문서 검토: 조직 내 보안 정책, 절차, 가이드라인 등을 검토하여 문서화된 내용과 실제 운영 상태 간의 일치 여부를 확인한다.
- 결과 분석 및 보고: 평가가 완료되면, 수집된 데이터를 분석하여 조직의 제로트러스트 성숙도 수준을 평가한다. 이를 통해 조직이 현재 어떤 수준에 있는지, 각 평가 요소별로 어떤 부분이 미흡한지를 명확하게 도출할 수 있다. 분석 결과는 단계별 성숙도 모델과 비교하여 조직의 현재 위치를 정확히 파악하고, 이를 바탕으로 향후 보안 전략을 수립할 수 있도록 도울 수 있다.

보고서는 조직 내 이해관계자들에게 쉽게 이해될 수 있도록 작성되어야 하며, 각 단계별로 구체적인 개선 방안과 실행 계획을 포함해야 한다. 이러한 보고서는 경영진의 의사 결정을 지원하고, 보안 예산 배정, 우선순위 설정 등에 중요한 역할을 한다.

조직의 보안 성숙도를 높이기 위해서는 평가 결과를 바탕으로 개선 계획을 수립해야 한다. 여기에는 다음과 같은 내용이 포함될 수 있다.

- 기술 도입: 필요에 따라 새로운 보안 기술이나 솔루션을 도입하여 제로트러스트 원칙을 강화한다. 예를 들어, 더 강력한 인증 체계나 자동화된 보안 모니터링 도구 등을 도입할 수 있다.
- 정책 및 절차 개선: 보안 정책과 절차를 재검토하고, 필요한 경우 이를 업데이트하여 조직 전반에 걸쳐 일관된 보안 원칙이 적용되도록 한다.
- 교육 및 인식 제고: 조직 내 모든 구성원이 제로트러스트 원칙을 이해하고, 이를 실천할 수 있도록 교육 프로그램을 운영한다. 이는 보안 성숙도 향상에 중요한 요소이다.
- 지속적 모니터링 및 재평가: 성숙도 수준은 지속적으로 모니터링되고, 주기적으로 재평가하여

필요한 개선 사항을 신속히 반영해야 한다.

이러한 전반적인 과정은 조직의 보안 수준을 체계적으로 분석하고, 제로트러스트 원칙을 기반으로 한 보안 성숙도를 지속적으로 높여 나가는 데 필수적이다.

2. 제로트러스트 성숙도 수준 평가를 위한 체크리스트

본 장에서는 제로트러스트 성숙도 수준 평가를 위한 체크리스트를 제공한다. 제로트러스트 성숙도 모델을 기반으로 한 체크리스트는 기업의 정보보호 상태를 평가하고, 향후 제로트러스트 도입을 위한 계획 수립과 예산 편성에 중요한 지침을 제공한다. 이 체크리스트는 기업이 현재 보안 환경의 강점과 약점을 식별하고, 제로트러스트 모델의 도입에 필요한 구체적인 조치를 계획하는 데 필요한 고수준의 평가 도구로 작동할 것이다.

이 체크리스트는 기업의 보안 책임자들이 기존의 보안 상태를 명확히 이해하고, 어떤 부분에서 제로트러스트 원칙을 강화해야 할지를 결정하는 데 도움을 준다. 이를 통해 기업은 제로트러스트 도입의 첫 단계를 보다 효과적으로 준비할 수 있으며, 장기적으로 조직의 보안 성숙도를 향상시킬 수 있는 기반을 마련할 수 있다.

하지만, 이 체크리스트는 정보보호 상태를 고수준에서 평가하는 도구이기 때문에, 너무 세부적인 항목보다는 핵심 영역에 집중하여 작성될 것이다. 이렇게 함으로써, 기업 담당자가 체크리스트에 매몰되지 않고, 전반적인 보안 상태를 파악하는 데 집중할 수 있도록 돕는다. 체크리스트의 각 항목은 제로트러스트 성숙도 모델의 주요 요소를 반영하되, 기업이 추가로 필요한 기술 및 솔루션을 판단하고, 세부 사항을 추가하거나 수정할 수 있도록 유연하게 구성될 것이다.

기업마다 보안 환경과 요구사항이 다르기 때문에, 체크리스트의 항목들은 각 조직의 상황에 맞게 조정이 필요하다. 예를 들어, 특정 기술이나 솔루션이 이미 도입된 상태라면, 해당 항목을 평가에서 제외하거나, 반대로 추가적인 보안 조치가 필요한 경우 새로운 항목을 추가할 수 있다. 이와 같은 유연성을 통해, 체크리스트는 기업이 자체적인 보안 전략을 효과적으로 수립하고 실행하는 데 실질적인 도움을 줄 것이다.

결국, 이 체크리스트는 기업이 현재 보안 상태를 평가하는 출발점이자, 제로트러스트 도입을 위한 로드맵을 설계하는 데 있어 기본 틀의 역할을 한다. 기업 담당자는 이 체크리스트를 통해

조직의 보안 성숙도를 고수준에서 평가하고, 이를 바탕으로 향후 보안 전략을 구체화하며, 필요한 예산과 리소스를 계획하는 데 활용할 수 있다. 단, 본 체크리스트는 기업에서의 성숙도 수준을 파악하기 위한 참조 성격의 내용을 담은 것으로, 정부·공공 기관의 보안 수준 혹은 제로트러스트 성숙도 수준을 파악하는 용도로 활용하는 것은 적절하지 않으며 기업이나 공공 기관이 필수적으로 준수해야 하는 규정보다 우선시할 수 없다.

가. 식별자·신원 핵심 요소 체크리스트 예시

표 5-1 식별자·신원 핵심 요소 체크리스트

세부역량	확인방법	성숙도	Check
사용자 인벤토리	• 사용자 목록에 대한 문서화가 되어있는가?	기존	☐
	• 사용자 역할에 따른 상세 인벤토리가 구축되어 있는가?	초기	☐
	• 자동화된 인벤토리 관리 기구가 도입되어 있는가?	향상	☐
	• 비정상적인 사용자 활동에 대한 탐지가 가능한가?	향상	☐
	• AI 기반 사용자 행동에 따른 관리가 되는가?	최적화	☐
	• 인벤토리가 통합되어 사용자 및 권한 관리 최적화가 되어 있는가?	최적화	☐
ID 연계 및 사용자 자격 증명	• 사용자 자격 증명에 대한 ID 연계 솔루션이 적용되어 있는가?	기존	☐
	• 여러 시스템 간 사용자 자격 증명에 대한 연동이 되어 있는가?	초기	☐
	• ID 통합 관리 시스템이 구축되어 있는가?	향상	☐
	• 글로벌 수준의 ID 연계 솔루션이 적용되어 있는가?	최적화	☐
다중인증 (MFA)	• 패스워드와 단순한 MFA(SMS, 이메일)가 같이 적용되어 있는가?	기존	☐
	• 인증 앱, 하드웨어 토큰 등 다양한 MFA가 구현되어 있는가?	초기	☐
	• FIDO 기반 인증 기법이 적용되어 있는가?	초기	☐
	• 상황에 따른 맞춤형 MFA가 지원 가능한가?	향상	☐
	• 컨텍스트(단말 위치, 네트워크, 접속 시간 등)를 고려한 ID 인증 방식이 적용되어 있는가?	향상	☐
	• 비정상적 로그인 시도를 실시간으로 탐지하고 대응 가능한가?	최적화	☐
지속 인증	• 세션 기반 인증이 수행되는가?	기존	☐
	• 사용자의 행동 및 접속 상태 모니터링이 가능한가?	기존	☐
	• 이상행위가 탐지되면 세션 중간에 추가 인증하는 시스템이 도입되어 있는가?	초기	☐
	• 동적 인증 기술을 토대로 실시간으로 인증 상태에 대한 조정이 가능한가?	향상	☐
	• 이상 행위 발생 시 자동 재인증 요구, 세션 종료 등 인증에 대한 지속적 검증이 실시간으로 가능한가?	최적화	☐

세부역량	확인방법	성숙도	Check
통합 ICAM 플랫폼	• ICAM 시스템이 구축되어 있는가?	기존	☐
	• ICAM 시스템 기반 중앙 집중 관리 및 모니터링이 되는가?	초기	☐
	• 사용자 인증 및 접근 관리에 대한 정책이 표준화되어 있는가?	초기	☐
	• 사용자 및 권한 관리에 대한 기본적인 위험도 평가가 도입 되었는가?	초기	☐
	• 다양한 보안 기술 및 시스템 통합으로 ICAM 플랫폼이 안정화되었는가?	향상	☐
	• ICAM 플랫폼이 자동화되어 있는가?	향상	☐
	• AI 기반의 ICAM 플랫폼을 통해 보안 강화가 이루어지는가?	최적화	☐
	• 실시간 분석을 통한 ID 위험 평가가 이루어지는가?	최적화	☐
행동, 컨텍스트 기반 ID 및 생체 인식	• 기본적인(지문, 얼굴인식) 생체 인식 기술이 적용되어 있는가?	기존	☐
	• 사용자 행동 패턴이 수동으로 분석되는가?	기존	☐
	• 행동 및 생체 인식 기술을 통합하여 인증이 가능한가?	초기	☐
	• 컨텍스트 정보 기반 접근권한이 조정되는가?	초기	☐
	• 실시간 사용자 행동 및 컨텍스트 변화 반영으로 접근제어 조정이 가능한가?	향상	☐
	• AI 기반 행동 분석 및 생체 인식 솔루션이 도입되어 있는가?	최적화	☐
조건부 사용자 접근	• 사용자 활동 및 조건을 수집할 수 있는 기초 시스템을 구축하였는가?	기존	☐
	• 조건부 접근 정책에 대한 개념을 정의하였는가?	기존	☐
	• 시스템 별 각기 다른 접속 관리 기능이 있는가?	기존	☐
	• 특정 조건에 따른 사용자 접근제어가 가능한가?	초기	☐
	• 시간, 위치 기반으로 최소 권한 원칙에 따른 접근제어가 가능한가?	초기	☐
	• 세션별 접근권한 부여가 가능한가?	향상	☐
	• 조건을 정교하게 나누어 다단계 접근 정책이 적용되어 있는가?	향상	☐
	• 리소스별 접근권한 부여가 가능한가?	향상	☐
	• 동적 접근 정책을 실시간으로 적용 가능한가?	최적화	☐
	• AI 기반 실시간 상황 파악을 통한 사용자 접속 관리가 가능한가?	최적화	☐
최소 권한 접근	• 최소 권한 원칙에 대한 정의가 이루어져 있는가?	기존	☐
	• 권한 부여에 대한 절차가 문서화 되어 있는가?	기존	☐
	• 권한 부여 절차가 표준화 되어 있는가?	초기	☐
	• 권한 요청 및 변경 관리 시스템이 도입되어 있는가?	초기	☐
	• 자동화된 권한 상승이 가능한가?	향상	☐
	• 권한 관리 정책이 지속적으로 업데이트 되는가?	향상	☐
	• 권한 관리가 동적으로 변경 가능한가?	최적화	☐
	• 최소 권한 원칙이 실시간으로 조정 가능한가?	최적화	☐

나. 기기 및 엔드포인트 핵심 요소 체크리스트 예시

표 5-2 기기 및 엔드포인트 핵심 요소 체크리스트

세부역량	확인방법	성숙도	Check
기기 감지 및 규정 준수	• 리소스에 연결된 기기를 식별할 수 있는가?	기존	☐
	• 수동으로 규정 준수에 대한 확인이 가능한가?	기존	☐
	• 실시간으로 기기를 탐지하고 규정 준수를 평가할 수 있는가?	초기	☐
	• 비준수 기기에 대한 경고 및 접근 제한이 되는가?	초기	☐
	• 자동으로 규정 기준을 적용하고 교정 조치가 가능한가?	향상	☐
	• 규정 준수에 대한 모니터링 및 이에 따른 접근권한 부여가 가능한가?	향상	☐
	• 규정 준수 여부에 따라 동적으로 권한이 수정되는가?	최적화	☐
	• 규정 준수 평가를 AI 기반으로 실시간으로 할 수 있는가?	최적화	☐
실시간 검사를 통한 기기 권한 부여	• 자산 접근 기기에 대한 정보가 수집되는가?	기존	☐
	• 기기가 자산에 접근하기 전 수동 검사를 수행하는가?	초기	☐
	• 기기의 상태를 자동으로 평가하고 보안 기준을 충족하는 기기만 접근 허용이 되는가?	향상	☐
	• 보안 상태에 따라 기기의 접근권한을 조정할 수 있는가?	최적화	☐
	• 종합적인 기기 보안 전략을 구현하여 다른 보안 시스템과 연동하였는가?	최적화	☐
기기 인벤토리	• 기기의 인벤토리를 작성하고 수동으로 업데이트 하는가?	기존	☐
	• 주요 기기에 대한 정보를 수집하고 관리하는가?	기존	☐
	• 기기 인벤토리를 자동화하고 모든 기기를 실시간으로 기록하는가?	초기	☐
	• 기기 인벤토리에 비정상적이거나 승인되지 않은 기기를 탐지하는 기능을 포함하는가?	향상	☐
	• 인벤토리 분석을 통하여 보안 취약점을 파악하는가?	향상	☐
	• 실시간 모니터링 및 이상 행위 예측 분석을 통해 기기 관리를 수행하는가?	최적화	☐

세부역량	확인방법	성숙도	Check
통합 엔드포인트 관리 및 모바일 기기 관리	• 기본적인 엔드포인트 및 모바일 기기 관리 시스템이 도입되었는가?	기존	☐
	• 기본적인 보안 정책을 설정하였는가?	기존	☐
	• 엔드포인트 및 모바일 기기의 보안 설정을 중앙에서 관리하고 보안 업데이트를 자동 배포하는가?	초기	☐
	• 기기 상태를 지속적으로 모니터링 하는가?	초기	☐
	• 모든 엔드포인트와 모바일 기기에 대하여 보안 정책을 중앙에서 자동으로 적용하고 관리하는가?	향상	☐
	• 모든 기기의 보안을 중앙에서 통합적으로 관리하고, 자동화된 위협 대응이 가능한가?	최적화	☐
엔드포인트 및 확장된 탐지·대응 (EDR 및 XDR)	• 기본적인 EDR 솔루션을 도입하였는가?	기존	☐
	• EDR 시스템을 고도화하여 실시간 위협 탐지 및 자동 대응이 가능한가?	초기	☐
	• XDR 솔루션을 도입하였는가?	향상	☐
	• AI 기반 EDR·XDR 솔루션을 통해 실시간으로 모든 기기에 대한 위협 탐지가 가능한가?	최적화	☐
자산, 취약성 및 패치 관리 자동화	• 자산 및 취약성을 수동으로 평가하는가?	기존	☐
	• 주요 자산 및 취약성 목록이 작성되어 있는가?	기존	☐
	• 자동화된 취약성 평가 및 패치 관리 도구를 도입하여 취약성 발견 시 자동 패치가 이루어지는가?	초기	☐
	• 모든 자산에 대해 지속적인 취약성 평가 및 패치 관리가 자동화되어 있는가?	향상	☐
	• 취약성 및 패치 관리 시스템을 다른 보안 시스템과 통합하여 종합적인 보안 관리가 가능한가?	향상	☐
	• 취약점을 사전에 식별하고 자동으로 패치 적용이 가능한가?	최적화	☐
	• 자산 관리, 취약성 평가, 패치 관리 시스템이 통합되어 있는가?	최적화	☐

다. 네트워크 핵심 요소 체크리스트 예시

표 5-3 네트워크 핵심 요소 체크리스트

세부역량	확인방법	성숙도	Check
매크로 세그멘테이션	• 비즈니스 영역별로 매크로 세그멘테이션이 되어 있는가?	기존	☐
	• 네트워크 내 주요 자산과 트래픽 흐름 기반으로 매크로 세그먼트가 구성되어 있는가?	기존	☐
	• 매크로 세그먼트 간에 보안 정책을 적용하였는가?	초기	☐
	• 매크로 세그먼트 간에 트래픽을 모니터링하고 비정상적 활동을 탐지하는가?	초기	☐
	• 매크로 세그먼트 간 맞춤형 보안 정책이 설정되었는가?	향상	☐
	• 매크로 세그먼트 간 트래픽을 조정하고 보안 위협에 대응 가능한가?	향상	☐
	• AI 기반 매크로 세그먼트 관리 도구가 적용되었는가?	최적화	☐
마이크로 세그멘테이션	• 애플리케이션 및 워크로드 기준으로 마이크로 세그멘테이션이 되어 있는가?	기존	☐
	• 수동으로 세그먼트를 구성하는가?	기존	☐
	• 애플리케이션 및 워크로드에 따른 마이크로 세그멘테이션 보안 정책이 설정되었는가?	초기	☐
	• 네트워크 수준에서 마이크로 세그멘테이션을 수행하여 워크로드 간 이동을 탐지·차단 할 수 있는가?	초기	☐
	• 마이크로 세그먼트 간 트래픽 모니터링이 가능한가?	초기	☐
	• 모든 네트워크 트래픽에 대한 보안 정책 설정 및 제어가 가능한가?	향상	☐
	• 애플리케이션 별 격리 메커니즘이 적용되었는가?	향상	☐
	• AI 기반 마이크로 세그먼트 관리 도구가 적용되어 위협에 자동으로 대응 가능한가?	최적화	☐
소프트웨어 정의 네트워킹	• 소프트웨어 정의 네트워크가 도입되어 있는가?	기존	☐
	• 클라우드 적용 시, SDN 기본 구조를 설정하고 트래픽을 제어할 수 있는가?	기존	☐
	• 클라우드 적용 시, SDN을 활용하여 네트워크 트래픽을 중앙에서 관리하고, 정책을 실시간으로 적용 가능한가?	초기	☐
	• 클라우드 적용 시, SDN 기능을 확장하여 트래픽 관리 및 보안을 적용하고 있는가?	향상	☐
	• 클라우드 적용 시, AI 기반 위협 관리 및 트래픽 예측 등이 가능한 SDN 기능을 적용하였는가?	최적화	☐

세부역량	확인방법	성숙도	Check
위협 대응	• IDS·IPS 등의 솔루션을 도입하여 주요 위협에 대한 감시 체계가 이루어지고 있는가?	기존	☐
	• 네트워크 정적 규칙에 의한 수동적 트래픽 관리가 이루어지는가?	기존	☐
	• 자동화된 위협 탐지 및 대응 시스템이 도입되어 보안 이벤트 발생 시 즉각 대응이 가능한가?	초기	☐
	• 애플리케이션 프로파일에 따른 트래픽 관리가 이루어 지는가?	초기	☐
	• 실시간 위협 탐지 및 위협 행위에 대한 선제적 대응 체계가 마련되어 있는가?	향상	☐
	• 네트워크 동적 규칙에 의한 네트워크 트래픽 관리가 이루어지는가?	향상	☐
	• 네트워크 전반에서 발생하는 위협에 대하여 즉각적이고 자동화된 대응이 가능한가?	최적화	☐
	• 애플리케이션 프로파일의 변화 등을 탐지하여 동적 네트워크 트래픽 관리가 가능한가?	최적화	☐
트래픽 암호화	• 내·외부 트래픽 일부 암호화가 가능한가?	기존	☐
	• SSL, TLS 등 표준 프로토콜 사용과 VPN 등을 사용하고 있는가?	기존	☐
	• 네트워크 전반에 걸쳐 암호화 기능이 적용되어 있는가?	초기	☐
	• 데이터 전송 시 암호화를 필수로 하고 있는가?	초기	☐
	• 전송 중 데이터 암호화 및 저장된 데이터도 모두 암호화하고 있는가?	향상	☐
	• 최신 암호화 기술을 적용하고, 고급 암호화 키 관리 시스템이 도입되어 있는가?	향상	☐
	• 최신 암호화 기술을 도입하고 성능 저하 없이 데이터 보호가 가능한가?	최적화	☐
	• 통합된 키 관리 시스템을 통하여 안전한 키 관리가 이루어지고 있는가?	최적화	☐
데이터 흐름 매핑	• 데이터 트래픽에 대한 수동적 모니터링을 수행하는가?	기존	☐
	• 네트워크 내 주요 데이터 흐름을 수동으로 매핑하는가?	기존	☐
	• 애플리케이션 단위의 트래픽 매핑이 가능한가?	초기	☐
	• 자동화된 데이터 흐름 매핑 도구를 도입하여 네트워크 내 모든 데이터 흐름이 실시간으로 매핑되는가?	초기	☐
	• 주요 데이터 트래픽과 관련된 보안 정책이 수립되어 비정상적 데이터 이동을 탐지하는가?	향상	☐
	• 데이터 흐름에 대한 분석을 상관관계를 통하여 분석하고, 위협을 사전에 식별 가능한가?	향상	☐
	• AI 기반 예측 분석 도구를 활용하여 데이터 흐름의 변화를 실시간으로 감지하는가?	최적화	☐
	• 네트워크 트래픽 우선순위를 동적으로 변경하고 구성할 수 있는가?	최적화	☐

세부역량	확인방법	성숙도	Check
네트워크 회복성	• 애플리케이션 및 워크로드에 대한 기본적인 복구 계획과 백업 경로가 마련되어 있는가?	기존	☐
	• 재해 복구에 대한 주기적 백업 실시가 이루어지는가?	기존	☐
	• 네트워크 장비에 대한 장애 대응 절차가 수립되어 있는가?	기존	☐
	• 네트워크 내 다중 경로가 설계되어 있고, 자동 복구 시스템이 도입되어 있는가?	초기	☐
	• 자동화된 장애 조치(Failover) 메커니즘이 적용되어 있는가?	초기	☐
	• 네트워크 이중화 설계가 되어 있는가?	초기	☐
	• 네트워크가 장애나 공격에도 지속적으로 서비스 지원이 가능한가?	향상	☐
	• 재해 복구 계획에 따라 주기적으로 테스트하여 항상 준비 상태가 유지되어 있는가?	향상	☐
	• 어떠한 상태에서도 네트워크 서비스의 중단 없이 지속적 운영이 가능한가?	최적화	☐
	• 네트워크 장애를 실시간으로 감지하고 복구하며, 모든 복구 절차를 자동화하였는가?	최적화	☐

라. 시스템 핵심 요소 체크리스트 예시

표 5-4 시스템 핵심 요소 체크리스트

세부역량	확인방법	성숙도	Check
접근통제	• 사용자 및 기기에 수동으로 권한을 부여하는가?	기존	☐
	• RBAC 기반 접근제어를 수행하는가?	기존	☐
	• 권한 관리를 수동으로 수행하는가?	기존	☐
	• 역할과 권한 기반으로 중앙 집중형으로 권한 부여가 가능한가?	초기	☐
	• 실시간 접근권한 부여가 가능한가?	초기	☐
	• 권한 변경 사항이 자동으로 반영되는가?	초기	☐
	• 특정 리소스에 대한 접근 제한·승인 정책이 자동으로 적용 가능한가?	초기	☐
	• ABAC 기반 접근제어를 수행하는가?	향상	☐
	• 다양한 조건을 바탕으로 세밀하고 동적으로 실시간 접근권한이 부여되는가? (위치, 기기 상태, 시간 등)	향상	☐
	• 사용자·기기의 상태를 실시간으로 분석하고 실시간·자동으로 권한 조정이 가능한가?	최적화	☐
	• 모든 접근제어는 중앙집중적인 시스템에서 실시간으로 관리되는가?	최적화	☐
	• 시스템에 영향을 미치는 명령 실행 시 실시간 신뢰도 재산정이 가능한가?	최적화	☐
	• 위험 분석 기반 지속적인 접근제어 정책이 도입되어 있는가?	최적화	☐

세부역량	확인방법	성숙도	Check
PAM	• PAM 시스템을 구축하였는가?	기존	☐
	• PAM 정책이 수립되어 있는가?	기존	☐
	• PAM 솔루션을 통해 사용자 접근을 모니터링하고 제어 가능한가?	초기	☐
	• 자동화된 권한 상승 승인 기술이 도입되어 있는가?	초기	☐
	• PAM 솔루션을 통해 비정상적 활동이 탐지 가능한가?	향상	☐
	• AI 기반 위협 탐지 및 대응 기능을 활용하여 PAM 시스템에 적용하였는가?	최적화	☐
자격 증명 관리	• 자격 증명이 수동으로 관리되는가?	기존	☐
	• 패스워드에 기반한 인증 방식에 의존하는가?	기존	☐
	• 자격 증명 관리가 체계적이지 않고 수동적인가?	기존	☐
	• 자격 증명 시스템이 중앙에서 관리되며 자동화 되는가?	초기	☐
	• MFA 등 보다 안전한 인증 방식이 적용되어 있는가?	초기	☐
	• 생체 인증 등 고급 인증 방식이 도입되어 있는가?	향상	☐
	• 자격 증명 관리 시스템을 고도화하여 관리하는가?	향상	☐
	• 자격 증명의 무결성을 보장하고 인증 프로세스가 강화되었는가?	향상	☐
	• AI 기반으로 실시간으로 인증정보 분석이 가능한가?	향상	☐
	• 비정상적인 인증 시도를 실시간으로 차단 가능한가?	최적화	☐
	• 실시간으로 인증 정책 조정이 가능한가?	최적화	☐
	• 모든 자격 증명 데이터가 중앙관리 되며, 자율적으로 운영되는가?	최적화	☐
네트워크 세분화 및 그룹 간 이동	• 네트워크 세분화 및 이동 통제가 거의 이루어지지 않는가?	기존	☐
	• 기본적인 경계형 네트워크 모델이 적용되어 있는가?	기존	☐
	• 시스템 중요도에 따라 네트워크가 분리되어 있는가?	초기	☐
	• 제한적인 보안 통제를 적용하여 네트워크 간 이동 제어가 가능한가?	초기	☐
	• 네트워크가 워크로드 별로 세분화되어 보안정책이 각각 이루어지는가?	향상	☐
	• 네트워크 그룹 간 이동 시 강력한 접근통제와 인증이 수반되는가?	향상	☐
	• 네트워크 그룹 간 이동 시 실시간 보안 검사 및 트래픽 이동에 대한 관리가 이루어지는가?	향상	☐
	• 그룹 간 이동 시 실시간으로 분석되고 제어되는가?	최적화	☐
	• 재인증 없는 그룹 간 이동이 가능한가?	최적화	☐
	• 실시간 보안 정책 조정을 통한 안전한 그룹 간 이동을 보장하는가?	최적화	☐

세부역량	확인방법	성숙도	Check
시스템 환경에 따른 정책 관리	• 온프레미스 환경에서 보안 정책을 수립하고 있는가?	기존	☐
	• 수동으로 보안 정책을 유지·관리하고 있는가?	기존	☐
	• 클라우드 환경으로 전환하면서 보안 정책을 각각에 맞게 수립하고 있는가?	초기	☐
	• 정책이 자동으로 적용되는가?	초기	☐
	• 하이브리드 클라우드 환경으로 전환되면서 실시간으로 보안정책이 조정되는가?	향상	☐
	• 환경 변화에 따라 정책이 동적으로 변경 가능한가?	향상	☐
	• 보안 위협에 맞춘 자율적인 정책 적용이 가능한가?	최적화	☐
	• 정책 관리가 완전히 자동화되어, 변화하는 환경에서도 일관된 보안 정책을 유지할 수 있는가?	최적화	☐

마. 애플리케이션 및 워크로드 핵심 요소 체크리스트 예시

표 5-5 애플리케이션 및 워크로드 핵심 요소 체크리스트

세부역량	확인방법	성숙도	Check
리소스 권한 부여 및 통합	• 접근에 대한 사용자·시스템 권한을 수동으로 관리하는가?	기존	☐
	• 리소스에 대한 접근권한을 정의하고, 정적 속성에 기반한 접근제어를 수행하는가?	기존	☐
	• 워크로드 접근에 대하여 중앙 집중식 관리 시스템이 도입 되었는가?	초기	☐
	• 모든 리소스에 대한 권한을 중앙에서 관리하는가?	초기	☐
	• 다수의 컨텍스트 정보(위치, 시간 등 포함)을 통한 최소 권한을 부여한 리소스 접근이 가능한가?	향상	☐
	• 정밀한 권한 관리가 구현되어 이를 통한 리소스 접근이 가능한가?	향상	☐
	• 실시간 위험 분석, 행동 패턴 분석 등을 통한 워크로드 및 리소스 접속이 가능한가?	최적화	☐
	• 자동화된 접근권한 부여 및 회수 시스템이 도입되어 있는가?	최적화	☐
	• 실시간 권한 관리 및 비정상적인 접근 차단이 가능한가?	최적화	☐
	• 모든 리소스 권한 부여가 자동화되어 있는가?	최적화	☐

세부역량	확인방법	성숙도	Check
지속적인 모니터링 및 진행 중인 승인	• 애플리케이션 및 시스템에 대한 보안 상태를 수동으로 모니터링하는가?	기존	☐
	• 보안 이벤트 기록을 수동으로 수행하는가?	기존	☐
	• 자동화된 보안 모니터링 도구를 도입하여 실시간으로 보안 이벤트를 수집하고 분석하는가?	초기	☐
	• 시스템 변경 사항에 대하여 보안 검토를 수행하는가?	초기	☐
	• 보안 이벤트를 AI 기반으로 분석하고 이상 징후를 탐지하는가?	향상	☐
	• 보안 승인 프로세스를 자동화할 수 있는가?	향상	☐
	• 모든 시스템의 보안 상태를 실시간으로 탐지하고 위협을 사전에 예측할 수 있는가?	최적화	☐
원격 접속	• VPN을 통해서 외부 접속을 지원하는가?	기존	☐
	• 애플리케이션에 대한 접근제어가 제한적인가?	기존	☐
	• 원격 접속 기기의 보안 상태를 자동으로 평가하고 접근을 제어하는가?	초기	☐
	• 원격 접속 기기의 실시간 모니터링 및 제어가 가능한가?	향상	☐
	• 다양한 원격 접속 시나리오에 대한 맞춤형 보안 정책을 수립하였는가?	향상	☐
	• 접속 상황에 따라 동적 보안 정책을 적용하여 애플리케이션 기능이 필요시 제한하는가?	최적화	☐
	• AI를 활용하여 원격 접속 보안을 고도화 하였는가?	최적화	☐
	• AI를 통하여 위험 요소가 탐지되면 애플리케이션 기능이 즉각적으로 제한 또는 차단되는가?	최적화	☐
안전한 애플리케이션 배포	• 애플리케이션 배포 전 수동으로 코드 검토 및 취약점 검사를 수행하는가?	기존	☐
	• 보안 가이드라인을 준수하는 초기 배포 절차를 마련하였는가?	기존	☐
	• 기본적인 배포 접근제어를 적용하여 배포 과정에서의 보안 사고를 방지하고 있는가?	기존	☐
	• 보안이 내재된 자동화된 배포 파이프라인을 구축하였는가?	초기	☐
	• 애플리케이션 배포 시 보안이 자동으로 적용되는가?	초기	☐
	• CI/CD 파이프라인을 통하여 자동화된 취약점 검사 도구를 적용하였는가?	초기	☐
	• 배포 전후로 코드 무결성을 검사하고 배포 환경을 격리하였는가?	초기	☐
	• 배포 과정 전반에 걸쳐 지속적인 모니터링을 수행하는가?	향상	☐
	• 보안 정책 준수를 자동으로 검증하는 도구가 도입되어 있는가?	향상	☐
	• 배포 중 발생하는 비정상적인 활동을 모니터링하여 즉각 대응 가능한가?	향상	☐
	• 애플리케이션의 모든 구성 요소가 배포 전후로 보안 검사를 거치도록 구성하였는가?	향상	☐
	• 완전히 자동화된 코드 배포 및 관리자 권한 접근제어가 가능한가?	최적화	☐
	• AI를 활용한 고도화된 위협 탐지 및 대응 시스템을 배포 파이프라인에 통합하여 중앙에서 관리하고 자동 보고 및 추적 관리가 가능한가?	최적화	☐

세부역량	확인방법	성숙도	Check
애플리케이션 인벤토리	• 모든 애플리케이션의 인벤토리를 수동으로 목록화하였는가?	기존	☐
	• 애플리케이션 기본 정보를 기록하여 관리하는가?	기존	☐
	• 자동화된 인벤토리 도구를 도입하여 애플리케이션을 자동으로 식별하고 관리할 수 있는가?	초기	☐
	• 애플리케이션 인벤토리에 보안 정보를 추가하여 애플리케이션의 보안 상태를 평가·관리할 수 있는가?	향상	☐
	• AI 기반 인벤토리 관리 시스템을 도입하여 애플리케이션 변경 사항을 실시간으로 반영할 수 있는가?	최적화	☐
	• 애플리케이션 인벤토리를 다른 보안 시스템과 통합, 종합적인 보안 관리가 이루어지고 있는가?	최적화	☐
보안 소프트웨어 개발 및 통합	• 개발 프로세스에 보안 코딩 표준이 적용되어 있는가?	기존	☐
	• 코드 배포 전, 정적이고 수동으로 보안 테스트를 수행하는가?	기존	☐
	• 보안 검토와 테스트를 소프트웨어 개발 라이프사이클에 통합하여 개발 단계부터 보안 취약점을 식별하는가?	초기	☐
	• DevSecOps 문화를 도입하였는가?	초기	☐
	• 주요 개발 내용에 대한 SBOM 문서를 작성하는가?	초기	☐
	• 서드파티 라이브러리 및 오픈소스 소프트웨어의 보안 검사를 자동화하여 수행하는가?	향상	☐
	• 프로세스 전반에 걸친 SBOM 문서를 작성하는가?	향상	☐
	• 소프트웨어 개발과 관련된 조직의 프로세스가 격리되어 있는가?	최적화	☐
	• 런타임 소프트웨어에 대한 분석이 자동화되어 있는가?	최적화	☐
	• 모든 소프트웨어 개발 및 통합 프로세스가 자동화되어 있는가?	최적화	☐
소프트웨어 위험 관리	• 최소한의 위험 요소가 식별되고 문서화 하였는가?	기존	☐
	• 소프트웨어 위험 관리 계획이 수립되어 있는가?	기존	☐
	• 위험 평가 프로세스를 도입하여 소프트웨어의 위험 수준을 평가하는가?	초기	☐
	• 소프트웨어 공급망에 대한 보안 강화를 통하여 전주기적 자동화 위험 관리가 이루어지는가?	향상	☐
	• AI 기반 예측 분석을 도입하여 잠재적 보안 위험을 식별할 수 있는가?	최적화	☐
	• 맞춤형 공격에 대응 가능한가?	최적화	☐

바. 데이터 핵심 요소 체크리스트 예시

표 5-6 데이터 핵심 요소 체크리스트

세부역량	확인방법	성숙도	Check
데이터 카탈로그 위험 정렬	• 데이터 자산의 초기 카탈로그가 작성되어 있는가?	기존	☐
	• 데이터를 파악하고, 유형 분류를 수동으로 하는가?	기존	☐
	• 데이터에 대한 기본적인 위험 평가를 문서화 하였는가?	기존	☐
	• 자동화된 데이터 카탈로그 도구가 도입되어 있는가?	초기	☐
	• 데이터 자산을 일부 자동으로 수집하고 분류하는가?	초기	☐
	• 데이터 위험 수준 평가를 위하여 기본적인 기준과 지침이 마련되어 있는가?	초기	☐
	• 데이터의 민감도와 위험 수준을 평가하기 위한 분석 도구가 있는가?	향상	☐
	• 데이터를 자동화하여 파악하고, 위험한 데이터에 대한 보호 정책이 적용되어 있는가?	향상	☐
	• 데이터 사용 패턴 분석이 가능한가?	향상	☐
	• AI 기반 데이터 위험 요소를 실시간으로 분석하는가?	최적화	☐
	• 데이터 카탈로그와 다른 보안 시스템이 통합되어 관리되는가?	최적화	☐
기업 데이터 거버넌스	• 데이터 거버넌스 정책 수립 및 데이터 관리에 대한 기본적인 지침이 마련되어 있는가?	기존	☐
	• 데이터 소유자와 관리자를 지정하였는가?	기존	☐
	• 데이터 거버넌스 프레임워크가 도입되어 있는가?	기존	☐
	• 데이터 정책 준수를 위하여 정기적인 감사와 검토가 수행되는가?	초기	☐
	• 데이터 거버넌스 도구를 이용하여 데이터 관리 프로세스를 자동화하였는가?	향상	☐
	• 데이터 정책 준수에 대한 실시간 모니터링이 가능한가?	향상	☐
	• 데이터 거버넌스를 조직의 모든 시스템과 통합하여 일관된 데이터 관리가 가능한가?	최적화	☐
데이터 접근제어	• 데이터 접근 정책이 수립되어 있는가?	기존	☐
	• 데이터 접근권한이 수동으로 부여되는가?	기존	☐
	• 중앙 집중식 접근제어 시스템이 도입되어 있는가?	초기	☐
	• 최소한의 권한 요소를 확인하여 데이터 접근 여부를 결정하는가?	초기	☐
	• ABAC을 통하여 컨텍스트 기반으로 접근권한 관리가 구현되어 있는가?	향상	☐
	• 데이터 접근제어를 최소화하고 AI를 이용하여 데이터 접근에 대한 실시간 권한 조정이 가능한가?	최적화	☐

세부역량	확인방법	성숙도	Check
데이터 암호화 및 권한 관리	• 데이터를 수동으로 암호화하는가?	기존	☐
	• 암호화 정책이 수립되어 있는가?	기존	☐
	• 데이터를 보호하기 위한 초기 권한 관리 체계가 수립되어 있는가?	기존	☐
	• 자동화된 암호화 도구를 통하여 중요한 데이터를 자동으로 암호화하는가?	초기	☐
	• 중앙 집중식 데이터 권한 관리 시스템이 도입되어 있는가?	초기	☐
	• 고급 암호화 기술을 도입하고, 권한 관리 시스템과 통합하여 관리하고 있는가?	향상	☐
	• RBAC과 ABAC을 결합하여 보다 정밀한 권한 관리가 이루어지는가?	향상	☐
	• AI 기반 암호화 및 권한 관리를 통하여 데이터 보호 최적화 및 실시간 권한 조정이 가능한가?	최적화	☐
	• 데이터에 대하여 실시간 권한에 따른 마스킹이 가능한가?	최적화	☐
데이터 라벨링 및 태그 지정	• 라벨링 및 태그 지정 지침을 수립하였는가?	기존	☐
	• 일관된 데이터 분류 체계가 마련되어 있는가?	기존	☐
	• 데이터에 기본적인 라벨과 태그를 수동으로 지정하여 식별·분류하는가?	초기	☐
	• 민감한 데이터에 특수 라벨을 적용할 수 있는가?	초기	☐
	• 민감한 데이터에 보안 정책이 차등적으로 적용되는가?	초기	☐
	• 자동화된 라벨링 및 태그 지정 도구를 도입하여 자산을 자동으로 분류·식별 가능한가?	향상	☐
	• 타 보안 시스템과 연계하여 데이터 보호가 가능한가?	향상	☐
	• 고급 메타데이터 관리 도구를 통하여 데이터 라벨링과 태그 지정 프로세스를 적용하는가?	최적화	☐
	• AI를 활용하여 변화하는 데이터 환경에 따른 분류가 자동 조정 되는가?	최적화	☐
데이터 손실 방지 (DLP)	• DLP 정책을 수립하고 수동으로 평가하는가?	기존	☐
	• DLP 도입을 위한 기업 내 범위가 지정되어 있는가?	기존	☐
	• DLP 도구를 도입하여 주요 데이터 유출 경로를 모니터링할 수 있는가?	초기	☐
	• DLP 정책을 중앙에서 관리하는가?	초기	☐
	• DLP 솔루션이 모니터링 모드로 동작하는가?	초기	☐
	• DLP 시스템이 전체적으로 도입되어 실시간으로 데이터를 보호하고 유출을 방지하는가?	향상	☐
	• DLP 솔루션이 방지 모드로 사용되는가?	향상	☐
	• DLP 시스템에 AI를 적용하여 데이터 유출 위험을 실시간으로 예측하고 차단할 수 있는가?	최적화	☐
	• 변화하는 데이터 환경에 맞춰 자동으로 보안 정책이 최적화되는가?	최적화	☐

세부역량	확인방법	성숙도	Check
데이터 모니터링 및 감지	• 데이터 활동을 수동으로 모니터링하고, 이벤트를 수동으로 기록하는가?	기존	☐
	• 데이터 모니터링 및 감지 프로세스가 수립되어 있는가?	기존	☐
	• 자동화된 모니터링 도구를 통하여 데이터 활동을 감시할 수 있는가?	초기	☐
	• 모니터링 결과를 기반으로 보안 정책 조정이 가능한가?	초기	☐
	• 데이터 활동을 분석하고 이상 징후를 실시간으로 탐지 가능한가?	향상	☐
	• 데이터 모니터링 결과를 다른 보안 시스템과 연계하여, 종합적인 보안 대응이 가능한가?	향상	☐
	• 모든 데이터 활동을 지속적으로 평가하고, 컨텍스트 기반 접근에 따라 최소 접근제어가 가능한가?	최적화	☐

사. 가시성 및 분석 핵심 요소 체크리스트 예시

표 5-7 가시성 및 분석 핵심 요소 체크리스트

세부역량	확인방법	성숙도	Check
모든 관련 활동 기록	• 로그 기록을 수동으로 수행하는가?	기존	☐
	• 로그 데이터가 특정한 시스템에서만 수집되는가?	기존	☐
	• 다양한 시스템에서 자동으로 로그를 수집하는가?	초기	☐
	• 로그 수집 및 관리가 자동화 되었는가?	초기	☐
	• 수집된 데이터를 분석하여 보안 위협을 실시간으로 탐지 가능한가?	향상	☐
	• 로그 기록의 무결성을 보장하는가?	향상	☐
	• 로그 데이터를 기반으로 예측 분석(향후 발생한 위협 분석)이 가능한가?	향상	☐
	• 로그를 기반으로 자율 보안 체계가 구축되었는가?	최적화	☐
	• 로그 항목을 자동으로 포맷을 맞추고 정규화가 가능한가?	최적화	☐
	• 로그 분석을 통해 보안 정책이 자동으로 조정되는가?	최적화	☐
중앙집중적 보안 정보 및 이벤트 관리	• 보안 이벤트가 발생하면 수동으로 데이터를 분석하는가?	기존	☐
	• SIEM 시스템이 도입되었는가?	초기	☐
	• 중앙집중적 보안 관리 체계가 구축되었는가?	초기	☐
	• SIEM 시스템은 다양한 보안 도구와 연동되어 보안 데이터를 종합적으로 분석하는가?	향상	☐
	• AI 기반으로 보안 이벤트를 분석하는가?	최적화	☐
	• 비정상적인 활동에 대하여 자동 대응이 가능한가?	최적화	☐

세부역량	확인방법	성숙도	Check
보안 위협 분석	• 보안 로그 및 데이터를 수동으로 수집하는가?	기존	☐
	• CVE, ExploitDB 등의 취약점을 수동으로 수집하는가?	기존	☐
	• 알려진 취약점에 대한 평가 기준을 마련하였는가?	초기	☐
	• 수집된 취약점에 대한 경고가 자동으로 이루어지는가?	초기	☐
	• 자동화된 보안 위협 분석 도구를 도입하였는가?	향상	☐
	• 실시간 보안 위협 탐지가 가능한가?	향상	☐
	• AI 기반 예측 분석 시스템을 통하여 위협에 대한 예측이 가능한가?	최적화	☐
사용자 및 기기 동작 분석	• 사용자와 기기의 기본적인 활동 데이터를 수집하는가?	기존	☐
	• 비정상 행동을 수동으로 탐지하는가?	기존	☐
	• 기본적인 사용자 행동 패턴을 기록하고, 의심스러운 활동을 발견하면 이를 추적하는가?	기존	☐
	• 자동화된 사용자 및 기기 동작 분석 도구를 도입하였는가?	초기	☐
	• 사용자의 행동 패턴과 기기의 활동을 자동으로 분석하는가?	초기	☐
	• 행동 분석 기능을 도입하여 비정상적인 사용자 활동과 기기 동작을 탐지하는가?	향상	☐
	• AI 기반으로 사용자 및 기기의 행동 패턴을 학습하고, 지속적으로 변화하는 패턴에 따라 실시간으로 대응 가능한가?	향상	☐
	• 사용자 및 기기 동작에 대하여 비정상 행위를 자동으로 파악하여 보안 정책을 자동으로 조정하고 최소 권한을 부여할 수 있는가?	최적화	☐
위협 인텔리전스 통합	• 외부의 보안 위협 정보를 수동으로 수집하는가?	기존	☐
	• 위협 데이터를 조직 내 시스템과 수동으로 연동하는가?	기존	☐
	• 자동화된 위협 인텔리전스 통합 도구를 도입하였는가?	초기	☐
	• 위협 인텔리전스를 내부 시스템과 통합하였는가?	향상	☐
	• AI 기반의 위협 인텔리전스 시스템을 구축하였는가?	최적화	☐
자동화된 동적 정책	• 보안 정책을 수동으로 관리하는가?	기존	☐
	• 보안 이벤트가 발생할 경우 관리자가 직접 정책을 수정하여 대응하는가?	기존	☐
	• 자동화된 정책 관리 시스템을 도입하였는가?	초기	☐
	• 보안 이벤트 발생 시 자동으로 정책을 변경하고 적용하는가?	초기	☐
	• 동적 정책을 실시간으로 조정하여, 보안 이벤트 발생 시 즉각적으로 새로운 정책을 생성하고 적용하는가?	향상	☐
	• 위협 탐지와 연계하여 동적으로 정책을 조정하는가?	향상	☐
	• AI 기반의 자동화된 동적 정책 시스템을 구축하여, 보안 이벤트 분석 결과에 따라 자율적으로 정책을 조정하는가?	최적화	☐

아. 자동화 및 통합 핵심 요소 체크리스트 예시

표 5-8 자동화 및 통합 핵심 요소 체크리스트

세부역량	확인방법	성숙도	Check
정책 통합	• 정책 조정 시 수동으로 각 시스템에 일일이 변경 사항을 반영하는가?	기존	☐
	• 자동화된 정책 통합 시스템을 도입하여 보안 정책을 중앙에서 관리하는가?	초기	☐
	• 정책 변경이 자동으로 이루어지는가?	초기	☐
	• 실시간 보안 이벤트를 기반으로 정책을 동적으로 조정하는가?	향상	☐
	• 위협에 따라 즉각적으로 정책을 수정하고 적용하는 자동화된 프로세스가 존재하는가?	향상	☐
	• AI 기반의 자율 정책 통합 시스템을 통해, 상황에 맞게 정책을 자동으로 조정 가능한가?	최적화	☐
중요 프로세스 자동화	• 수동 절차에 의존하며, 핵심 보안 및 운영 프로세스가 수동으로 관리되는가?	기존	☐
	• 중요한 프로세스에 대한 자동화 도구를 도입하여, 반복적인 작업과 기본적인 보안 절차를 자동으로 처리하는가?	초기	☐
	• 데이터 백업 및 기본 장애 대응과 같은 주요 업무가 자동화되어 있는가?	초기	☐
	• 자동화된 프로세스를 확장하여, 보안 사고 발생 시 신속한 자동 대응이 가능한가?	향상	☐
	• 자동화 시스템은 모든 프로세스를 실시간으로 최적화하고, 업무 중단 없이 중요한 프로세스를 자동으로 조정 가능한가?	최적화	☐
인공지능	• 데이터를 수동으로 수집하고 분석하며, 보안 위협에 대한 대응도 수동으로 이루어지는가?	기존	☐
	• 기본적인 AI 기반 도구를 도입하여 보안 이벤트를 분석하고 패턴을 식별하는가?	초기	☐
	• AI 기반의 보안 시스템이 고도화되어, 실시간으로 위협을 탐지하고 대응 가능한가?	향상	☐
	• AI가 모든 보안 시스템에 완전히 통합되었는가?	최적화	☐
	• 자율적으로 보안 위협을 감지하고 대응하며, 정책을 동적으로 조정가능한가?	최적화	☐
보안 통합, 자동화 및 대응	• 보안 도구와 시스템이 각각 독립적으로 운영되며, 수동 대응에 의존하는가?	기존	☐
	• 보안 사고 발생 시 여러 도구에서 데이터를 수집하고 분석하며, 대응 절차도 개별적으로 수행되는가?	기존	☐
	• SOAR 시스템을 도입하였는가?	초기	☐
	• 보안 이벤트는 여러 시스템에서 데이터를 수집하여 중앙에서 대응 가능하도록 관리되고 있는가?	초기	☐
	• SOAR 시스템을 고도화하여 복잡한 보안 사고에 대해 자동화된 대응과 실시간 통합이 가능한가?	향상	☐
	• 여러 도구와 연동하여 신속한 위협 차단이 가능한가?	향상	☐
	• 모든 보안 이벤트가 중앙에서 자동으로 처리되는가?	최적화	☐
	• 자율 통합을 통해 자동으로 보안 사건 관리가 되는가?	최적화	☐

세부역량	확인방법	성숙도	Check
데이터 교환 표준화	• 수집된 데이터가 상이한 형식으로 저장되는가?	기존	☐
	• 데이터 교환이 비효율적으로 이루어지는가?	기존	☐
	• 보안 시스템 간 데이터 교환이 수동으로 이루어지는가?	기존	☐
	• 데이터 교환 표준을 도입하였는가?	초기	☐
	• 보안 시스템 간 데이터 교환이 자동화되었는가?	초기	☐
	• 다양한 외부 시스템 및 파트너와도 데이터 공유가 원활하게 이루어지는가?	향상	☐
	• 여러 보안 도구 간의 상호 운용성이 제공되는가?	향상	☐
	• 데이터 교환 표준화가 자율적으로 관리되며, 외부 파트너와의 데이터 교환까지 실시간으로 자동화되는가?	최적화	☐
	• 모든 시스템에서 일관된 데이터 형식이 적용되어 있는가?	최적화	☐
	• 보안 위협이 발생할 때마다 실시간으로 데이터를 교환하고 분석하는가?	최적화	☐
보안 운영 조정 및 사고 대응	• 보안 팀이 수동으로 여러 부서와 소통하고 조정하는가?	기존	☐
	• 보안 사고 대응 절차가 정형화되어 있지 않는가?	기존	☐
	• 보안 사고 대응 계획을 수립하고, 사고 대응 절차를 표준화하였는가?	초기	☐
	• 보안 사고가 발생하면 자동화된 경고가 생성되는가?	초기	☐
	• 사고 대응 절차가 자동화되고, 보안 운영 팀과 다른 부서 간 조율이 실시간으로 이루어지는가?	향상	☐
	• 자동화된 보고 시스템을 통해 보안 사고의 진행 상황이 지속적으로 공유되는가?	향상	☐
	• 보안 사고가 발생하기 전에 이를 예측하고 선제적으로 대응 가능한가?	최적화	☐
	• 사고 대응 절차는 완전히 자동화되어, 보안 팀과 관련 부서가 신속하고 일관된 대응이 가능한가?	최적화	☐
	• 사고 발생 시 모든 관련 부서가 실시간으로 협력하고, 대응 결과가 즉시 보고되는가?	최적화	☐

| 제2절 |

제로트러스트 침투 시험 기반 효과성 분석

1. 제로트러스트 침투 시험을 통한 효과성 분석 방안

조직의 보안 취약점을 파악, 개선하는 효과적인 방법의 하나로 제로트러스트 침투 시험을 고려할 수 있다. 해당 방법은 공격자 관점에서 실제 공격과 가장 유사한 시나리오를 구현함으로써, 조직의 위협 대응 능력을 객관적으로 검증한다. 특히, 악성코드(멀웨어, 랜섬웨어 등) 유포, 권한 탈취 등 다양한 공격 기법을 선제 검증하고, 보안 취약점을 종합적으로 판단하기 때문에 가장 실질적으로 효과성을 입증하는 방법이라 할 수 있다.

제로트러스트 침투 시험은 조직의 보안 능력을 검증하여 제고한다는 점에서 보안 자생력 강화에 효과적이다. 시험을 통해 도출한 결과를 기반으로 각 조직의 특성에 적합한 제로트러스트 보안 솔루션을 개발, 적용할 수 있는 이유에서다. 제로트러스트 침투 시험은 조직의 보안 인식 수준 및 보안 대응 능력을 객관적으로 파악하는 데 방점을 찍는다. 따라서 침투 시험 결과는 내부 자산의 중요도 및 조직의 취약점을 판단하고, 이를 토대로 조직의 거시적 보안 전략을 수립하는 유의미한 근거로 활용할 수 있다.

제로트러스트 침투 시험은 제로트러스트 아키텍처가 목표로 하는 보안 상태를 제대로 평가하기 위하여 침투 시험의 효과성, 리소스 사용 및 실행 위험성 등을 면밀히 검토해야 한다. 또한, 실질적 취약점을 파악하고, 체계적인 검증 프로세스를 정립해 개선 사항을 수립하고, 지속적인 모니터링 및 개선 근거 자료를 확보할 수 있다는 장점과 함께 전문 기술 도입을 위한 경영 관리 비용 증가 등의 단점도 존재한다. 제로트러스트 침투 시험 시 고려 사항 및 장단점을 구체적으로 살펴보면 다음과 같다.

가. 제로트러스트 침투 시험에서의 고려 사항

1) 침투 시험 범위 설정

제로트러스트 환경은 기업망 내부에서의 다양한 네트워크 세그먼트, 사용자 인증 프로세스, 기기 인증 등이 포함되므로 시험할 범위를 명확히 설정해야 한다. 시험 범위가 너무 넓거나 좁으면 효과적인 평가를 얻기 어려우며, 내부 침투와 외부 침투를 나누어 평가하거나 특정 시스템에 중점을 두는 등의 구체적인 목표를 설정하는 것이 중요하다.

표 5-9 침투시험 유형

구분	침투시험 유형		
	Black-Box	Grey-Box	White-Box
침투 시험 목적	외부 침투	내부 침투 (내부자 공격)	정밀한 공격
사전에 부여된 권한 및 지식	없음 (완전한 외부 공격자)	내부 정보 및 시스템 접근권한	시스템·SW에 관한 완전한 권한(소스코드 등)

[출처: Technical Guide to Information Security Testing and Assessment, NIST SP 800-115]

2) 기업망 시스템 영향 가능성

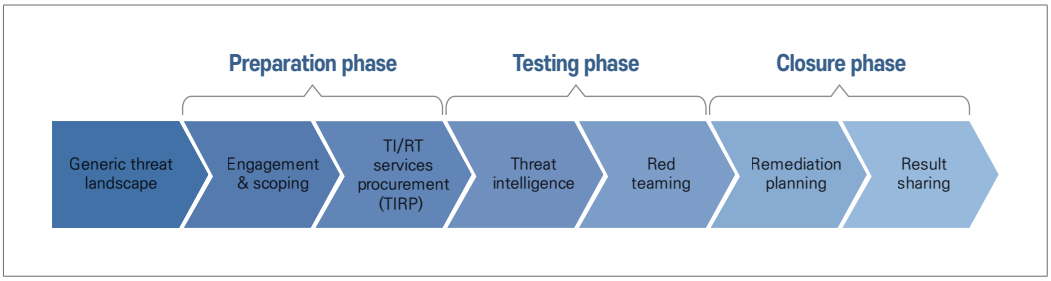
침투 시험은 실제 환경에서 수행되므로, 시험 중 시스템 및 서비스가 공격에 영향을 받을 가능성을 고려해야 하며, 특히 발전소, 금융기관 등 실시간 시스템이 중요한 조직의 경우, 시스템 백업 등 이에 대한 대비가 필요할 수도 있다. 실제로, 전문적으로 침투 시험을 수행하는 화이트해커들은 실제적인 시스템 및 서비스에 영향을 초래하는 단계의 공격을 수행하지 않고, 그 가능성을 증명하는 단계까지만 침투 시험을 수행하는 것이 통상적이다.

3) 외부 전문가에 의한 공격 시나리오 설계

제로트러스트 아키텍처는 여러 방어 계층을 통해 보호를 강화하기 때문에, 이들을 고려하는 다양한 공격 시나리오를 포함한 시험이 필요하다. 내부자 공격, 외부 위협, 권한 상승 시도 등을 포함해 다양한 위협 모델을 고려해야 하며, 이를 위해 다양한 공격 기술과 최신 위협 정보를 반영하여 침투 시험 시나리오를 설계해야 한다.

최근에는 해당 기업 및 시스템 또는 유사한 산업군을 대상으로 활동하는 공격자의 공격 목표, 공격 사례, 피해 규모 등을 조사해, 해당 기업 및 시스템에서 발생 가능성이 높은 공격 TTP(전술·기법·절차)를 도출하고 이를 침투 시험에 적용하는 것이 일반화되고 있다. 유럽연합(EU) 금융 인프라·기관을 대상으로 시행하는 침투 시험인 TIBER-EU의 절차를 살펴보면 TI(위협 인텔리전스)와 RT(레드티밍)를 결합하고 있다. TI 전문업체가 대상 인프라·기관에 대한 위협을 선제적으로 파악하고 RT 전문업체는 이를 이용해 최적화된 침투 시험 시나리오를 구성하여 침투 시험을 실시한다.

그림 5-1 EU 금융 인프라·기관을 대상으로 시행하는 침투 시험인 TIBER-EU 프레임워크



침투 시험을 개발하는 것은 고도의 전문 지식이 필요한 작업이므로, 내부 직원이 직접 계획하여 수행하기 어렵다. 일반적으로 외부 보안 전문가나 침투 시험 전문 업체를 활용하는 것이 적절하며, 보안 담당 직원은 외부 전문가가 조직의 환경에 맞는 시나리오를 잘 이해하고 반영할 수 있도록 충분한 정보를 제공해야 한다.

나. 제로트러스트 침투 시험의 장점

1) 제로트러스트 아키텍처의 실질적 취약점 진단 및 위협 대응 능력 평가

침투 시험은 이론적인 보안 상태를 평가하는 것이 아니라, 실제로 시스템이 공격을 방어할 수 있는지 검증할 수 있는 유일한 방법이며, 제로트러스트 아키텍처를 통해 구축한 다중 인증, 네트워크 세분화, 지속적인 인증 등이 실제로 공격에 얼마나 효과적인지 테스트할 수 있다. 일반적으로 침투 시험을 통한 효과성을 분석하는 것은 공격자 관점에서 조직의 보안 상태를 종합적으로 파악할 수 있으며, 제로트러스트 아키텍처를 적용하여 개선한 보안 체계의 안전성을 실질적으로 살펴보고 취약점을 분석할 수 있다는 장점이 있다.

또한, 실제 공격과 유사한 상황에서 기업이 얼마나 신속하게 탐지하고 대응하는지 평가할 수 있으며, 제로트러스트 아키텍처의 실시간 모니터링과 자동화된 탐지 시스템이 제 기능을 하는지 확인할 수 있다.

2) 체계적 검증 프로세스 정립 기반 취약점 식별 및 개선 사항 도출

침투 시험 시 침투 범위 설정, 공격 시나리오 수립, 침투 시험 수행, 결과 분석 등의 과정을 통한 보안 개선 방안을 수립하게 된다. 침투 시험은 보안 체계 내 숨겨진 취약점을 발견하는 데 매우 유용하며, 제로트러스트 아키텍처에서도 실수나 설정 오류로 인해 발생할 수 있는 취약점을 사전에 파악하고 수정할 수 있다. 이를 통해 제로트러스트 아키텍처의 구축 완료 후에도 지속적 개선을 위한 기반을 마련할 수 있다. 즉, 제로트러스트 보안 체계의 종합적 검증을 통한 보안 강화 지표를 마련하고, 보안 사고 발생에 대비한 본질적인 해결 방안을 도출 및 지속적 검증을 위한 기반 자료를 확보할 수 있다.

다. 제로트러스트 침투 시험의 한계점

1) 침투 시험 결과가 보안성을 완벽하게 보장하는 것은 아님

침투 시험은 기업의 보안 체계가 일부 공격에 대응할 수 있는지를 평가하지만, 모든 상황의 위협 시나리오를 다루는 것은 어렵다. 침투 시험 항목 및 시나리오를 만드는 것이 어려울 뿐만 아니라 모든 보안 취약점을 점검하는 것이 사실상 불가능하며, 가능한 많은 영역을 커버하는 고도의 공격 시나리오를 만드는 것은 여전히 어렵다. 즉, 침투 시험이 성공적이었다고 해서 완전한 보안을 의미하지는 않으며, 지속적인 보안 개선이 필요하다.

특히 유의해야 할 점은, 침투 시험에서 설정한 공격에 모두 대응 가능했다고 하더라도, 이를 바탕으로 모든 공격에 대응 가능한 것으로 착각하지 말아야 한다는 점이다.

최근에는, 이러한 침투 시험의 단점을 해결하는 BAS(Breach and Attack Simulation) 기술이 발전하고 있다. BAS는 침투 시험 절차를 자동화하고 지속적으로 수행하는데 유용하며 다양한 종류의 공격TTP를 시험할 수 있고, 이를 조합하여 복잡한 공격 시나리오를 구성할 수 있다. 특히, 제로트러스트의 각 기능을 시험하기 위한 공격 시나리오를 BAS에 구축하고 제로트러스트 솔루션과 연계하여 그 수행결과를 확인한다면 매우 유용한 제로트러스트 기능검증 방법이 될 수 있다.

2) 제로트러스트 침투 시험 도입에 따른 비용

앞서 언급한 바와 같이, 고도의 전문 지식이 필요한 침투 시험은 외부 보안 전문가나 침투 시험 전문 업체를 활용하여 진행하게 될 가능성이 높다. 이는 곧, 침투 시험이 상당한 비용과 시간이 필요함을 의미한다. 또한, 제로트러스트 환경은 복잡한 설정이 많아 시험 범위가 넓어질수록 더 많은 시간이 필요하다. 침투 시험 과정에서 비용과 시간의 발생 원인은 다음과 같이 정리할 수 있다.

- 제로트러스트에 대한 전문 지식, 해킹 기술 등 고도화된 전문 기술을 보유·실행하기 위한 도입 비용 발생
- 화이트 해커 등 전문 보안 인력 및 업체 투입 시 인건비 발생

2. 제로트러스트 침투 시험 시나리오 및 분석 방법

가. 제로트러스트 침투 시험

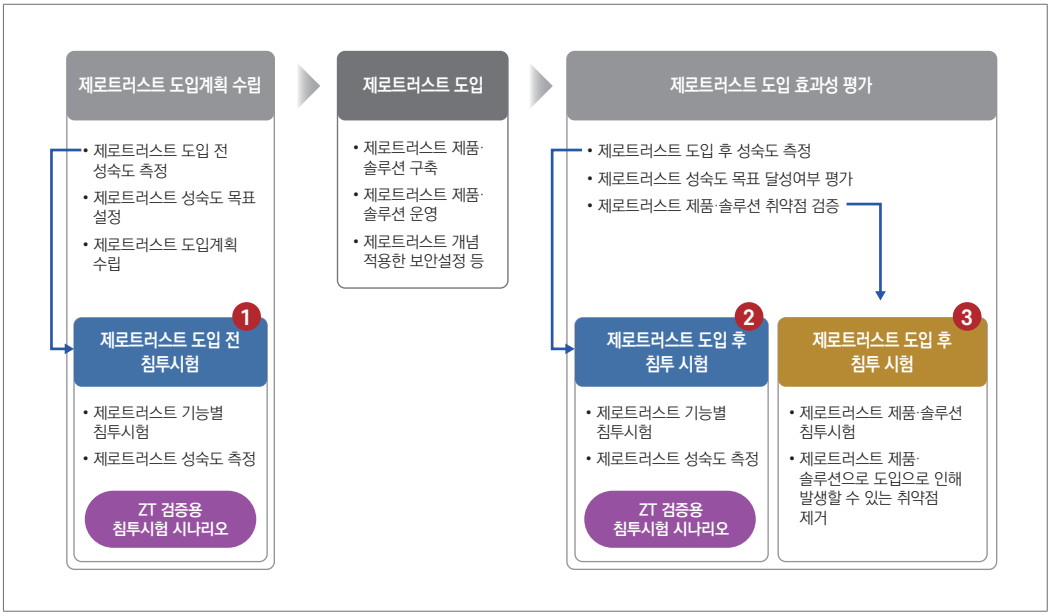
제로트러스트 침투 시험은 제로트러스트 도입계획 수립(도입 전) → 도입 → 도입 효과성 평가(도입 후) 등을 포함한 제로트러스트 도입 전·후 최소 3회 이루어질 수 있다.

첫 번째, 제로트러스트 도입 전 계획수립 단계에서는 조직의 제로트러스트 성숙도를 먼저 측정한 후, 조직의 성숙도 목표와 측정된 성숙도의 차이를 분석하고 성숙도 목표를 만족하기 위한 제로트러스트 제품·솔루션의 도입을 추진하게 된다. 이 과정에서 조직의 제로트러스트 성숙도 측정에 침투 시험을 활용할 수 있다.

두 번째, 제로트러스트 제품 및 솔루션을 구축하고 운영하는 단계에서는 제로트러스트 도입 효과성을 평가하게 되는데, 이때 침투 시험을 통해 제로트러스트 성숙도를 한번 더 측정하여 조직의 제로트러스트 성숙도 목표를 만족하는지 평가한다.

세 번째, 제로트러스트 제품·솔루션 자체 또는 구축·운영 과정에서 보안 취약점을 내재할 수 있으므로, 침투 시험을 통해서 이를 확인하고 조치(취약점 제거 등)를 취할 수 있다.

그림 5-2 제로트러스트 침투 시험



나. 제로트러스트 보안모델 적용 전·후 효과성 분석을 위한 침투시험 시나리오 예시

가이드라인 1.0 및 본 문서 3.1절에서 언급한 기업망에서의 6가지 핵심 요소 및 2가지 교차 기능에 대해 각 항목의 보안성을 측정할 수 있는 침투시험 시나리오를 〈표 5-10〉과 같이 정리할 수 있다. 침투시험 시나리오를 구성하는 개별 공격기법은 침투시험 전문 업체들이 보유하고 있는 공격 TTP를 이용하는 것으로 고려하였으며, 제로트러스트 성숙도 모델 상의 각 핵심 요소별 기능(3.1절)을 반영하여 침투시험 시나리오 40개를 구성하였다. 이 중 외부 공격자 관점의 점검으로 확인이 가능한 항목 24개는 침투시험을 수행하고, 시스템 내부 동작구조 식별을 통해서만 확인이 가능한 항목 16개는 수요기업과의 인터뷰를 통해 점검을 수행할 수 있을 것이다.

다음 그림은 제로트러스트 침투시험 시나리오 중 네트워크 세분화 기능 검증을 위한 침투시험을 나타낸 것으로 MITRE ATT&CK 기준 Remote System Discovery (TA0007.T1018) 공격기법을 사용한다. 해당 침투시험 시나리오는 단말에서 동작 중인 서로 다른 애플리케이션 A, B에 침투한 후 네트워크 스캐닝을 통해 추가 공격(횡적이동 등)을 위한 대상을 탐색하는 것이다. 제로트러스트 도입 “전” 스캐닝 결과는 애플리케이션 A, B 모두 동일하나, 제로트러스트 도입 “후” 스캐닝 결과는 애플리케이션 A, B 각각의 권한과 워크로드에 따라 서로 다른 스캐닝 결과가 도출되는 것을 확인할 수 있다.

그림 5-3 제로트러스트 침투시험 예시 (네트워크 세분화 검증 시나리오)

본 제로트러스트 침투시험 시나리오는 네트워크 세분화와 관련된 마이크로 세그멘테이션 역량에 초점을 맞춰 수행되므로, 침투시험 결과를 「네트워크 핵심 요소 체크리스트」에 적용해 마이크로 세그멘테이션 성숙도를 측정하면 다음 표와 같이 "초기" 수준으로 판단할 수 있다.

표 5-10 제로트러스트 침투시험(네트워크 세분화 검증)을 통한 마이크로 세그멘테이션 성숙도 측정 (예시)

세부역량	확인방법	성숙도	Check
마이크로 세그멘테이션	**• 애플리케이션 및 워크로드 기준으로 마이크로 세그멘테이션이 되어 있는가?**	**기존**	✓
	• 수동으로 세그먼트를 구성하는가?	기존	☐
	• 애플리케이션 및 워크로드에 따른 마이크로 세그멘테이션 보안 정책이 설정되었는가?	초기	☐
	• 네트워크 수준에서 마이크로 세그멘테이션을 수행하여 워크로드 간 이동을 탐지·차단 할 수 있는가?	**초기**	✓
	• 마이크로 세그먼트 간 트래픽 모니터링이 가능한가?	초기	☐
	• 모든 네트워크 트래픽에 대한 보안 정책 설정 및 제어가 가능한가?	향상	☐
	• 애플리케이션별 격리 메커니즘이 적용되었는가?	향상	☐
	• AI 기반 마이크로 세그먼트 관리 도구가 적용되어 위협에 자동으로 대응 가능한가?	최적화	☐

〈표 5-11〉은 가이드라인 2.0 기반 침투시험 시나리오 상의 시험 방안을 보인다. 앞에서 언급한 네트워크 세분화 기능 검증을 위한 침투시험의 예시와 같이 시나리오를 구체화할 수 있으나 절대적인 것이 아니며, 〈표 5-11〉에서 제시한 세부 시나리오 및 공격기법은 시험 대상 시스템의 구조, 공격 표면, 적용된 제로트러스트 세부 기능 등에 따라 구체화 방법이 달라질 수 있다. 특히 표에 언급된 점검 형태나 MITRE ATT&CK 기반 공격 전술 및 기법 등은 예시에 불과할 뿐 절대적인 항목이 아님을 미리 밝힌다. 침투 시험을 설계하는 전문 기업이 지속적으로 진화하는 공격 전술과 제로트러스트 성숙도 기능 등을 반영하여, 적합한 점검 방안을 마련하여야 한다.

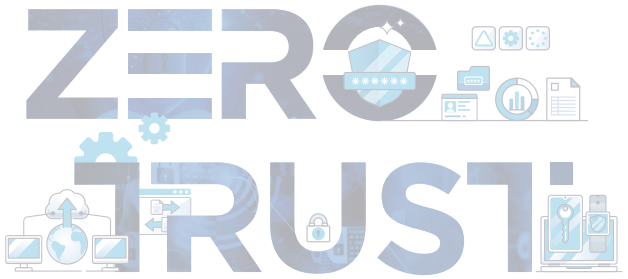
표 5-11 가이드라인 2.0에 따른 침투시험 시나리오 예시

제로트러스트 보안모델		점검 형태	침투시험			
			침투시험 시나리오	MITRE ATT&CK		
핵심 요소	기능			공격전술 (Tactic)	공격기법 (Technique)	ID
1 식별자·신원 (Identity)	식별자 관리	인터뷰	-	-	-	-
	인증	침투 시험	식별자 인증 효과성 검증 시나리오	Credential Access	Brute Force	TA0006.T1110
	위험도 평가	인터뷰	-	-	-	-
	접근 관리	인터뷰	-	-	-	-
	가시성 및 분석	침투 시험	식별자 행위 추적 검증 시나리오	Lateral Movement	Exploitation of Remote Services	TA0008.T1210
	자동화 및 통합	침투 시험	식별자 보안 통합 및 자동화 검증 시나리오	Initial Access	Valid Account	TA0001.T1078
2 기기 및 엔드포인트 (Device/ Endpoint)	정책 준수 모니터링	침투 시험	엔드 포인트 정책 준수 검증 시나리오	Defense Evasion	Impair Defenses	TA0005.T1562
	데이터 접근제어	침투 시험	엔드 포인트 접근제어 검증 시나리오	Discovery	File and Directory Discovery	TA0007.T1083
	자산 관리	인터뷰	-	-	-	-

제로트러스트 보안모델		점검 형태	침투시험			
			침투시험 시나리오	MITRE ATT&CK		
핵심 요소	기능			공격전술 (Tactic)	공격기법 (Technique)	ID
	기기 위협 보호	침투 시험	펌웨어 변조 검증 시나리오	Impact	Firmware Corruption	TA0040.T1495
		침투 시험	비정상 행위에 대한 EDR 탐지 검증 시나리오	Defense Evasion	Hide Artifacts	TA0005.T1564
				Discovery	Account Discovery	TA0007.T1087
				Lateral Movement	Remote Services	TA0008.T1021
	가시성 및 분석	인터뷰	–	–	–	–
	자동화 및 통합	인터뷰	–	–	–	–
3 네트워크 (Network)	네트워크 세분화	침투 시험	네트워크 세분화 검증 시나리오	Discovery	Remote System Discovery	TA0007.T1018
	위협 대응	침투 시험	네트워크 위협 대응 검증 시나리오	Lateral Movement	Exploitation of Remote Services	TA0008.T1210
	트래픽 암호화	침투 시험	네트워크 암호화 검증 시나리오	Collection	Adversary-in-the-Middle	TA0009.T1557
	트래픽 관리	침투 시험	네트워크 토폴로지 동적구성 검증 시나리오	Reconnaissance	Network Topology	TA0043.T1590.004
	네트워크 회복성	침투 시험	DoS 공격을 이용한 네트워크 회복성 검증 시나리오	Impact	Network Denial of Service	TA0040.T1498
	가시성 및 분석	인터뷰	–	–	–	–
	자동화 및 통합	인터뷰	–	–	–	–

제로트러스트 보안모델		점검 형태	침투시험			
			침투시험 시나리오	MITRE ATT&CK		
핵심 요소	기능			공격전술 (Tactic)	공격기법 (Technique)	ID
4 시스템 (System)	접근통제	침투 시험	시스템 접근 통제 시나리오	Lateral Movement	Remote Services	TA0008.T1021
	시스템 계정 관리	침투 시험	시스템 계정 관리 시나리오	Lateral Movement	Remote Services	TA0008.T1021
	네트워크 분리 정책	침투 시험	시스템 네트워크 분리 정책 시나리오	Lateral Movement	Remote Services	TA0008.T1021
	시스템 보안 및 정책 관리	인터뷰	–	–	–	–
	가시성 및 분석	인터뷰	–	–	–	–
	자동화 및 통합	인터뷰	–	–	–	–
5 애플리케이션 및 워크로드 (Application & Workload)	애플리케이션 접근	침투 시험	애플리케이션 접근 인가 검증 시나리오	Execution	User Execution	TA0002.T1204
	애플리케이션 위협 보호	인터뷰	–	–	–	–
	접근 가능한 애플리케이션	인터뷰	–	–	–	–
	안전한 애플리케이션 배포	침투 시험	애플리케이션 공급망 공격을 이용한 안전한 배포 검증 시나리오	Initial Access	Supply Chain Compromise	TA0027.T1474
	소프트웨어· 애플리케이션 보안	침투 시험	응용 소프트웨어 보안 검증 시나리오	Initial Access	Exploit Public-Facing Application	TA0001.T1190
	가시성 및 분석	인터뷰	–	–	–	–
	자동화 및 통합	침투 시험	응용 소프트웨어 보안 자동화 검증 시나리오	Privilege Escalation	Create or Modify System Process	TA0004.T1543

제로트러스트 보안모델		점검 형태	침투시험			
			침투시험 시나리오	MITRE ATT&CK		
핵심 요소	기능			공격전술 (Tactic)	공격기법 (Technique)	ID
6 데이터 (Data)	데이터 목록 관리	인터뷰	–	–	–	–
	접근 결정방법	침투 시험	데이터 접근제어 검증 시나리오	Collection	Data from Local System	TA0009.T1005
	데이터 암호화	침투 시험	데이터 암호화 검증 시나리오	Defense Evasion	Obfuscated Files or Information	TA0005.T1027
	데이터 분류	인터뷰	–	–	–	–
	데이터 손실 방지	침투 시험	DLP 우회를 이용한 데이터 손실방지 검증 시나리오	Exfiltration	Exfiltration over Web Service	TA0010.T1567
					Transfer Data to Cloud Account	TA0010.T1537
					Exfiltration over Alternative Protocol	TA0010.T1048
	가시성 및 분석	침투 시험	데이터 추적 검증 시나리오	Execution	User Execution	TA0002.T1204
	자동화 및 통합	침투 시험	데이터 보안 자동화 검증 시나리오	Collection	Data from Local System	TA0009.T1005


ZERO
TRUST

제로트러스트
가이드라인 2.0

부 록

| 제1절 | 용어 및 약어 정의

| 제2절 | 국내 기업 제로트러스트 인식 수준

| 제3절 | 제로트러스트 아키텍처 참조 모델 실증 사례

| 제4절 | 미 연방정부 제로트러스트 도입·실증 현황

| 제5절 | 성숙도 모델 개념

| 제6절 | ISMS-P 인증기준과 제로트러스트 성숙도 모델 연계

| 제7절 | 참고 문헌

| 제1절 |

용어 및 약어 정의

1. 용어 정의

표 S-1 제로트러스트 가이드라인 2.0 용어 정의

용어	정의
기능 (Function)	▸ 어떤 일이나 목적, 요구사항을 달성하기 위해 필요한 능력 ▸ 제로트러스트 성숙도 모델 2.0에서 정의하는 기능은, 기업망에서 제로트러스트 아키텍처를 구현하는데 있어서 필요한 보안 능력을 의미
리소스 (Resource)	▸ 데이터를 포함하여 기업망 내부에서 보호 대상이 되는 모든 종류의 디지털 자산을 의미하며, 데이터 외에도 프린터, 컴퓨팅 리소스, IoT 액추에이터 등을 포함하기도 함
비인간개체 (NPE, Non-Person Entity)	▸ 기업망에서 사용자가 아닌 기기, 서버, 애플리케이션, 서비스 등으로 특정 리소스에 접근을 하는 접근 주체 역할을 수행할 수 있으며, 이 경우 신원 확인 및 권한 검증, 신뢰도 확인 등이 이루어져야 함
세부역량 (Capability)	▸ 일련의 작업을 수행하기 위한 수단과 방법의 조합을 통해 원하는 요구사항 혹은 효과를 달성할 수 있는 능력 및 이를 바탕으로 구현되는 구체적 기능
워크로드 (Workload)	▸ 기업망에서 시스템, 애플리케이션 등이 처리해야 하는 작업 혹은 일련의 작업 리스트 등을 의미하며, 제로트러스트 관점에서는 온프레미스 혹은 클라우드에 위치한 리소스에 접근하는 모든 서비스, 애플리케이션 및 솔루션 등을 포괄
접근 (Access)	▸ 접근 주체가 리소스를 이용하는 과정으로, 단순히 데이터를 읽는 것 뿐만 아니라 수정, 삭제 및 데이터 이외의 디지털 자산에 데이터를 전송하거나 전송받는 등의 행위를 포함
접근 주체 (Subject)	▸ 사용자와 애플리케이션(혹은 서비스), 기기의 조합이며, 여기에 악의적인 공격자 혹은 불법적인 애플리케이션, 감염된 기기 등이 포함될 수 있음
정책결정지점 (PDP, Policy Decision Point)	▸ 접근 주체가 리소스에 접근할 수 있는지를 최종적으로 결정하여 이를 정책시행지점(PEP)에게 명령하는 논리적 개체로, 정책 엔진(PE)과 정책 관리자(PA)로 구성

용어	정의
정책 관리자 (PA, Policy Administrator)	▸ 접근 주체와 리소스 사이의 통신 경로를 생성하거나 취소하기 위한 결정을 정책시행지점(PEP)에게 전달하는 논리 개체
정책 엔진 (PE, Policy Engine)	▸ 접근 주체가 리소스에 접근할 수 있는지를 최종적으로 결정하는 논리적 개체로, 정책정보지점(PIP)으로부터 신뢰도를 평가할 수 있는 알고리즘에 대한 입력을 수신하여, 현재 리소스 접근 요청을 승인하거나 거부 혹은 현재 연결 중인 상태의 접근을 취소할 수 있음
정책시행지점 (PEP, Policy Enforcement Point)	▸ 접근 주체와 리소스 사이를 연결하고 모니터링하며 최종적으로 연결을 종료하는 논리적 개체로, PDP의 정책 관리자에게 접근 요청을 전달하고 접근 승인 여부를 전달받아 현재 접근 세션에 직접 반영
정책정보지점 (PIP, Policy Information Point)	▸ 정책결정지점이 정책 결정을 내리는 데 활용하기 위해서 수집한 사용자, 기기 관련 정보 및 기타 정책 관련 정보를 제공하는 논리적 개체로, 이러한 정보에는 기업이 생성하거나 제어하지 않는 외부 데이터와 기업 내부적으로 생성되는 내부 데이터로 분류할 수 있으며 규제·내부규정, 데이터 접근 정책, 보안 이벤트, 위협 인텔리전스, 사용자 및 기기 인증 정보, 네트워크 및 시스템 상의 행위 로그 등을 포함할 수 있음
제로트러스트 (Zero Trust)	▸ 위협이 언제 어디서든 발생 가능하다는 인식하에 기업 내부의 네트워크, 시스템 혹은 리소스에 접근하고자 하는 어떤 사용자·기기에 대해서도 지속 인증, 세밀한 접근제어를 통한 최소 권한 부여 등 적극적인 신뢰도 평가 없이 접근을 허용하지 않는 보안 모델 및 이를 구현·실체화하기 위한 아이디어의 집합을 의미 ▸ 영어 원문을 발음대로 쓴 표현으로 두 단어의 결합인 점을 고려하면 '제로 트러스트'라고 표현할 수 있으나, 이 문구가 '제로(무)'와 '트러스트(신뢰)'의 단순 단어 결합이 아닌 새로운 보안 모델로서의 의미를 담고 있음을 고려하고 독자들이 해당 의미를 받아들이는 데 도움이 될 수 있도록 본 가이드라인에서는 두 단어를 붙인 형태의 새로운 단어로 표현하고 있음
제로트러스트 아키텍처 (Zero Trust Architecture)	▸ 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 포함
컨텍스트 (Context)	▸ 특정 접근 주체가 리소스에 접근할 때 접근제어 및 신뢰도 평가에 있어 활용될 수 있는 모든 상황 정보를 의미하며, 이러한 정보에는 사용자의 신원, 기기 상태 및 위치, 사용자의 실행 애플리케이션, 접속 시간, 접근하고자 하는 리소스, 네트워크 상태 등을 포함할 수 있음 ▸ 제로트러스트 성숙도 수준이 높아질 경우 가급적 많은 컨텍스트 정보를 실시간으로 확보하여 현재 접근 요청에 대해 동적으로 신뢰도를 판단하기 위해 사용함
프로비저닝 (Provisioning)	▸ 기업망에서 사용자, 기기 등이 서비스를 받기 위해 필요한 리소스 및 이에 대한 접근권한, 정책 등을 사전에 준비하고 배포하는 절차 및 과정을 의미

2. 약어 정의

- **ABAC** Attribute-Based Access Control
- **ACL** Access Control List
- **AI** Artificial Intelligence
- **API** Application Programming Interface
- **AV** Anti-Virus
- **BYOD** Bring Your Own Device
- **CCTV** Closed Circuit TeleVision
- **CEO** Chief Executive Officer
- **CESS** Customer Edge Security Stack
- **CISO** Chief Information Security Officer
- **CI/CD** Continuous Integration/Continuous Deployment
- **CNAPP** Cloud Native Application Protection Platform
- **CSP** Cloud Service Provider
- **CTI** Cyber Threat Intelligence
- **CVE** Common Vulnerabilities and Exposures
- **DB** Data-Base
- **DDoS** Distributed Denial of Service
- **DLP** Data Loss Prevention
- **DMZ** De-Militarized Zone
- **DoS** Denial of Service
- **DRM** Digital Rights Management
- **EDR** Endpoint Detection and Response
- **EIG** Enhanced Identity Governance
- **FCEB** Federal Civilian Executive Branch
- **FIDO** Fast IDentity Online
- **FIM** File Integrity Monitoring
- **HW** Hard-Ware
- **IaaS** Infrastructure-as-a-Service
- **ICAM** Identity, Credential and Access Management
- **IDP** IDentity Provider
- **IDS** Intrusion Detection System
- **IL** Impact Level
- **ILM** Identity Lifecycle Management
- **IoT** Internet of Thing
- **IPS** Intrusion Protection System
- **ISMS** Information Security Management System
- **ISMS-P** Personal Information & Information Security Management System
- **JIT/JEA** Just-In Time/Just-Enough Access
- **MDM** Mobile Device Management

- **MFA** Multi-Factor Authentication
- **ML** Machine Learning
- **MSA** Micro-Service Architecture
- **NAC** Network Access Control
- **NPE** Non-Person Entity
- **OS** Operating System
- **PA** Policy Administrator
- **PaaS** Platform as a Service
- **PAM** Privileged Access Management
- **PDP** Policy Decision Point
- **PE** Policy Engine
- **PEP** Policy Enforcement Point
- **PIP** Policy Information Point
- **PKI** Public Key Infrastructure
- **PW** Pass-Word
- **RBAC** Role-Based Access Control
- **RDP** Remote Desktop Protocol
- **SaaS** Software as a Service
- **SASE** Secure Access Service Edge
- **SBOM** Software Bill Of Materials
- **SDLC** Software Development Life-Cycle
- **SDN** Software-Defined Networking
- **SDP** Software-Defined Perimeter
- **SMS** Short Message Service
- **SOAR** Security Orchestration, Automation and Response
- **SOC** Security Operation Center
- **SPA** Single Packet Authorization
- **SSE** Security Service Edge
- **SSO** Single Sign On
- **SW** Soft-Ware
- **TTP** Tactics, Techniques & Procedures
- **UEM** Unified Endpoint Management
- **URL** Uniform Resource Locator
- **VDI** Virtual Desktop Infrastructure
- **VM** Virtual Machine
- **VPN** Virtual Private Network
- **XDR** eXtended Detection and Response
- **ZT** Zero Trust
- **ZTA** Zero Trust Architecture
- **ZTNA** Zero Trust Network Access

3. 보안 기술 및 솔루션 용어 설명

표 S-2 보안 기술 및 솔루션 용어 설명

용 어	의 미
ABAC (Attribute-Based Access Control)	▸ 속성 기반 접근제어 모델로, 속성 정보(사용자의 속성, 기기 정보, 위치 정보)를 사용하여 접근제어 관리하는 보안 모델 ▸ 예를 들어, 사용자가 접근하려는 리소스의 위치나 사용자가 접속하는 기기 등의 속성에 따라 접근을 허용하거나 거부 가능
AV (AntiVirus)	▸ 컴퓨터 바이러스, 랜섬웨어 등 악성 코드를 탐지하고 방어하기 위한 보안 솔루션
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 PEP ▸ 다양한 보안 정책(예, 인증, Single Sign-On, 권한 부여, 자격 증명 매핑, 기기 프로파일링, 암호화, 토큰화, 로깅, 경고, 멀웨어 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)
CESS (Customer Edge Security Stack)	▸ 미 국방부 Thunderdome 프로젝트에서 포함하고 있는 보안 기능의 모음으로, 네트워크 보안 기능(NGFW, IDS·IPS)들을 엣지에서 사용자에게 좀 더 가깝게 이동한 것
CI/CD (Continuous Integration/ Continuous Deployment)	▸ 소프트웨어 개발 및 배포 프로세스의 자동화를 의미하는 용어로, 개발부터 배포까지의 과정에서 코드 통합, 테스트, 릴리스, 배포를 빠르고 지속적으로 자동화하여 소프트웨어의 품질을 높이고 배포 시간을 단축하는데 중점을 둔 개발 방식
CTI (Cyber-Threat Intelligence)	▸ 사이버 공격과 관련된 정보를 수집, 분석, 해석하여 보안 방어를 강화하는 전략적 정보 ▸ 이를 통해 조직은 잠재적 또는 실제 사이버 위협에 대해 더 깊이 이해하고, 사전 예방적 대응을 할 수 있으며, 주로 사이버 공격의 동향, 공격자의 의도, 공격 기법, 표적 정보 등을 분석하는 데 사용
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

용 어	의 미
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 과거 IT 조직 체계로는 급속도로 변화하는 비즈니스 환경에서 발생하는 문제점 해결을 위해, DevOps와 보안(Security)이 결합하여 개발 파이프라인의 과정에서 보안 정책 및 기술 반영
DLP (Data Loss Prevention)	‣ 중요한 데이터에 대한 무단 접근, 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, 접근제어 및 모니터링과 같은 다양한 기능을 포함함으로써 민감한 데이터의 기밀성, 무결성 및 가용성을 보장하고 데이터 손실 또는 위반 방지
DRM (Digital Rights Management)	‣ 영화, 음악 및 전자책과 같은 디지털 콘텐츠를 무단 복사, 배포 및 사용으로부터 보호하기 위한 솔루션 ‣ 일반적으로 암호화, 접근제어, 복사 및 배포 제한, 사용량 모니터링 등의 기능을 제공함으로써 권한 없는 사용자가 디지털 콘텐츠에 접근·공유하는 것을 제한
EDR (Endpoint Detection and Response)	‣ 기업에서 단말(Endpoint) 동작에 대한 보안 위협을 탐지하고 대응하기 위한 솔루션으로, 컴퓨터, 서버, 랩톱, 모바일 기기 등과 같은 단말에 에이전트 소프트웨어를 설치하여, 실시간으로 네트워크 활동을 모니터링하고 이상 징후를 탐지하는 역할을 수행 ‣ 단말에 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
FIM (File Integrity Monitoring)	‣ 현재 파일 상태와 이미 알려진 기준선 사이의 검증 방법을 이용하여 운영 체제 및 애플리케이션 파일의 무결성을 확인하는 내부 통제 혹은 절차로, 일반적으로 암호학적 체크섬 혹은 다른 파일 속성을 활용하여 무결성을 모니터링
ICAM (Identity, Credential and Access Management)	‣ 기업에서 접근 주체에 대한 디지털 식별자 및 관련 속성의 유지 관리, 자격 증명 발급 및 이에 기반한 인증, 인증된 식별자 및 연관 속성을 기반으로 내부 리소스에 대한 접근을 관리, 모니터링함으로써 기업 내부 IT 인프라를 보호하기 위한 보안 솔루션 및 시스템을 의미
IDP (IDentity Provider)	‣ 접근 주체에 대한 디지털 식별자 및 관련 정보를 생산, 저장, 관리하는 시스템 ‣ 접근 주체에 대하여 직접 인증을 수행하거나, 혹은 외부 기업에게 사용자 인증 서비스를 제공할 수 있음
Macro-Segmentation	‣ 네트워크를 여러 워크로드 및 시스템 단위로 묶음으로써 역할에 따르는 큰 범위로 나누어 각 구역에 보안 정책이나 네트워크 트래픽 제어를 적용하는 보안 기법 혹은 기술
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 분실 시 원격 자료삭제 등이 가능하며, 악성 프로그램 및 기타 사이버 위협으로부터 기기를 안전하게 보호하는 기능을 포함하기도 함

용 어	의 미
MFA (Multi-Factor Authentication)	▸ 다중인증으로 사용자의 신원 확인을 위해 2개 이상의 인증 요소를 사용하는 보안 기술 ▸ 사용자가 알고 있는 것(비밀번호 등 지식), 가지고 있는 것(스마트 카드 등 소유), 사용자 자신의 특징(생체 정보 등 존재), 사용자의 행동 특성(서명, 키 입력 패턴 등) 등 여러 인증 요소 중 2개 이상을 사용하여 인증함으로써, 공격자가 특정 인증 요소(예: 비밀번호)를 획득하더라도 최종적으로 인증에 성공하기 어렵게 만드는 방법
Micro-Segmentation	▸ 기업망 내부의 모든 리소스(네트워크, 시스템, 워크로드, 애플리케이션, 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, 기기, 애플리케이션 등의 인증, 권한 부여, 접근제어 등) 시행 - Endpoint Security: Agent를 통해, 단말 보안 소프트웨어 업데이트, 악성 코드 검사 등을 수행 - Authentication and Authorization: 사용자와 기기 식별, 인증, 권한 부여를 담당하며, 사용자는 사용자 이름과 비밀번호로, 기기는 MAC 주소, IP 주소 등으로 인증 - Network Enforcement: 네트워크에서 규칙에 맞지 않는 접근 차단 및 정책 시행 (규칙 위반 여부 확인 후 규칙 위반 기기에 대해 차단, 격리, 경고 등의 조치)
NGFW (Next Generation Fire-Wall)	▸ 차세대 방화벽으로, 기존 네트워크 방화벽 기능(네트워크 트래픽 분석 및 패킷 필터링, 상태 기반 검사, VPN 트래픽 식별 등)에 추가적으로 애플리케이션 인식 및 제어, 침입 방지, 위협 인텔리전스 등 향상된 보안 기능이 추가된 보안 솔루션
OAuth (Open Authorization)	▸ 인터넷 사용자들이 패스워드를 제공하지 않고 다른 웹사이트 상의 자신들의 정보에 대해 웹사이트나 애플리케이션의 접근권한을 부여할 수 있는 공통적인 수단으로 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(예: 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
PAM (Privileged Access Management)	▸ PAM은 중요한 리소스에 대한 무단 접근을 모니터링, 감지 및 방지함으로써 사이버 위협으로부터 조직을 보호하기 위한 ID 보안 솔루션 ▸ 사용자, 프로세스 및 기술을 조합하여 작동하며, 아래 기능을 통하여 권한 있는 계정을 사용하는 사람과 로그인 중에 수행 작업에 대한 가시성 제공 - 다단계 인증 요구 - JIT 접근 제공 - 보안 자동화 - 활동 기반 접근제어 - 권한 있는 접근제어 및 모니터링 등

용 어	의 미
RBAC (Role-Based Access Control)	▸ 역할 기반 접근제어 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 접근권한 없음)
SASE (Secure Access Service Edge)	▸ 2019년 Gartner가 현대적인 사이버 보안 아키텍처를 표현하기 위해 개발한 용어로, SWG, CASB, ZTNA, NGFW 등의 서비스형 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 같으며, 그 외 공급기업에 따라 FWaaS, DLP, NAC, EPP 등 다른 보안 기능이 추가로 제공되기도 함 - SD-WAN (일반 인터넷 기반 오버레이 네트워크 VPN 서비스) - SWG (보안 웹 게이트웨이, 악성 트래픽 검사 및 차단) - CASB (클라우드 가시성 확보, 위협 방지 등 보안 기능) - ZTNA (다양한 보안 기술·솔루션을 결합하여 접근 주체에 최소 권한 및 세션 단위 접근 허용)
SBOM (Software Bill Of Materials)	▸ SW 구성요소 명세서라고 하며, 소프트웨어 구성요소를 서술하는 일종의 메타데이터로 소프트웨어 전체의 구성요소를 목록화한 기록 ▸ 소프트웨어 공급망 공격으로 인한 피해를 최소화하기 위하여, 소프트웨어 내 어떤 구성요소가 존재하는지 신속하게 파악하고 위험에 대처하기 위한 도구로 활용 (출처: SW 공급망 보안 가이드라인 v1.0)
SDLC (Software Development Life-Cycle)	▸ 고품질의 소프트웨어를 계획, 설계, 구현, 테스트 및 유지 관리하기 위한 방법론 ▸ 일반적으로 사전 계획을 통해 프로젝트 위험을 최소화하여 사용자 요구사항을 충족하는 고품질의 유지 관리 가능한 소프트웨어를 제공하는 것이 목적으로, 소프트웨어의 품질과 전반적인 개발 프로세스를 개선하는 방법을 정의하게 됨
SDP (Software Defined Perimeter)	▸ 안전하지 않은 네트워크로부터 서비스를 격리하기 위해 필요한 경계 기능을 애플리케이션 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 오케스트레이터가 모든 네트워크 활동을 모니터링하여 실시간 분석 및 보고 제공

용 어	의 미
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
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 발생 시 보안 운영 센터 관리자가 쉽게 대응할 수 있도록 지원
SOC (Security Operation Center)	▸ 기업의 전제 IT 인프라에 대해 연중무휴로 모니터링함으로써 사이버 보안 위협 및 사고를 예방, 실시간 탐지, 분석, 대응하고 규정 준수에 대한 이행 여부를 평가하기 위한 전담 조직
SSE (Security Service Edge)	▸ 웹, 클라우드 서비스 및 개인 애플리케이션에 대한 접근 보호를 위한 보안 솔루션을 의미하며, SASE의 보안 부분(CASB, SWG, ZTNA 등)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
TMS (Threat Management System)	▸ 기업이 잠재적인 보안 위협을 식별·관리할 수 있도록, 사이버 공격을 예방하는 사전 조치, 위협을 나타낼 수 있는 이상 징후나 패턴 탐지 기술, 보안 사고를 해결하고 완화하는 대응 프로세스 등을 포함하여 기업 내 디지털 자산 및 데이터를 안전하게 보호하기 위한 목적의 보안 솔루션
UEBA (User and Entity Behavior Analytics)	▸ 사용자 및 엔티티 행동 분석 솔루션으로, 사용자 및 엔터티(예: 기기, 애플리케이션, 서버 등)의 행동 패턴을 분석하여 비정상적이거나 잠재적으로 악의적인 활동을 탐지하는 보안 기술 ▸ 일반적으로 기계 학습과 데이터 분석 기술을 사용하여 사용자와 엔터티의 정상적인 활동 기준을 정의한 후, 그 기준에서 벗어난 이상 행동을 탐지하며, 주요 기능으로 비정상 행위 탐지, 내부자 위협 탐지, 외부 위협 탐지, 행동 분석 등을 포함하여 계정 탈취 및 악의적 내부자의 활동을 탐지하고, 랜섬웨어 등 보안 사고를 사전에 감지하는 역할 수행
UEM (Unified Endpoint Management)	▸ 통합 단말 관리 솔루션을 의미하며, 일반적으로 단일 콘솔에서 단말의 운영 체제나 위치에 관계없이 데스크탑, 노트북, 스마트폰 등 조직의 최종 사용자 기기를 모니터링, 관리, 보호 등 보안 관리 기능 제공

용 어	의 미
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 및 세션 관리 소프트웨어 – 가상 데스크톱 소프트웨어 스택의 프로비저닝 및 유지보수 관리 도구
VPN (Virtual Private Network)	▸인터넷을 통해 기기 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, 경계 기반 보안 기술이 도입된 기업망에서 경계를 확장하는 용도(재택·원격 근무자의 기업망 접속 지원 등)로 사용되며, 두 기기 간 네트워크에 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
XDR (eXtended Detection and Response)	▸보안 사고 탐지 및 자동화된 대응 기능과 함께, 여러 소스의 위협 인텔리전스 및 원격 분석 데이터를 보안 분석과 통합하여 보안 경고에 대한 컨텍스트 및 상관 관계 정보를 제공하는 통합 보안 솔루션 ▸NDR(네트워크 탐지 및 대응) 및 EDR(엔드포인트 탐지 및 대응), 그 외 보안 관련 데이터를 연계하여 보안 관리 부서에게 원격 분석 및 중앙집중적인 가시성을 제공
ZTNA (Zero Trust Network Access)	▸하나의 애플리케이션 혹은 애플리케이션 집합 주위에 신원 혹은 컨텍스트 기반 논리 접근 경계를 생성하는 솔루션 혹은 서비스 ▸애플리케이션은 검색에서 숨겨지며, 접근은 신뢰 브로커를 통해 명명된 접근 주체 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

4. 제로트러스트 가이드라인 1.0과 용어 비교표

표 S-3 제로트러스트 가이드라인 1.0과 용어 비교표

가이드라인 2.0	가이드라인 1.0	설명
애플리케이션	응용	▸응용 소프트웨어(Application Software)를 의미하는 표현으로, '응용'보다 더 널리 사용되는 '애플리케이션'으로 용어 통일
애플리케이션 및 워크로드	응용 및 워크로드	▸'응용' 대신 '애플리케이션' 사용으로, 핵심 요소 중 하나인 '응용 및 워크로드'도 같이 변경

| 제2절 |

국내 기업 제로트러스트 인식 수준

2023년 한국정보보호산업협회(KISIA)는 과학기술정보통신부로부터 의뢰를 받아 수행한 '국내 제로트러스트 보안로드맵 마련을 위한 실증방안 연구'에서, 제로트러스트 아키텍처 도입 대상인 수요기업과 이들 기업에 정보보호 기술·솔루션을 자체 제작·공급하는 공급기업에 대한 실태조사를 위하여, 2023년 8월 28일부터 10월 6일까지 진행한 설문조사를 통하여 제로트러스트와 관련한 인식, 기술 수준, 정책적 요구 사항 등을 파악하였다.

이와 관련하여 상세한 내용은 2024년 5월 23일 과학기술정보통신부 홈페이지에서 공개하고 있는 정책연구보고서를 통하여 확인할 수 있다.

1. 국내 기업 인식 수준 평가를 위한 조사 개요

해당 조사는 '국내 제로트러스트 관련 현황 조사·분석을 통해 국내 맞춤형 제로트러스트 보안로드맵 마련과 보안 모델 전환 체계 구축에 기여'하는 것을 목적으로, 다음과 같이 조사 대상을 정의하고 모집단 설정 후 응답률 20%를 기준으로 실사를 진행하여 총 수요기업 200개사, 공급기업 50개사에 대하여 설문조사를 완료하였다.

- 조사 대상
  - 수요기업: 정보보호 공시 대상 기업을 중심으로 정보보호 솔루션 및 제품을 사용할 수 있는 IT 인프라가 갖춰진 일반 민간 기업
  - 공급기업: 국내 시장 환경에서 정보보호 솔루션 및 제품을 자체 제작·공급 가능한 정보보호 전문 업체

- 조사 모집단 및 실사 기업
  - 수요기업: 분야별 모집단 711개사 선정 후 이 중 정보통신업 65개사, 제조업 70개사, 보건업 19개사, 그 외 46개사 등 총 200개 기업 실사
  - 공급기업: KISIA 회원사 및 임원사, 판교 정보보호 클러스터 입주 정보보호 기업, 한국제로트러스트위원회 소속 정보보호 기업, 정보보호 분야 혁신기술 보유기업 등 총 50개 기업 실사

- 질의 내용
  - 수요기업: 제로트러스트 관련 수요인식, 도입 솔루션 보안 기술 수준 등 질의
  - 공급기업: 제로트러스트 도입 및 기술 현황, 주력보안영역, 제로트러스트 관련 협력 희망 분야, 제로트러스트 기술개발 투자 현황 등 질의

2. 수요 기업의 제로트러스트 인식 수준

가. 제로트러스트 인식 수준

국내 수요기업의 62.5%는 제로트러스트라는 용어를 모른다고 응답하였으며, 31.0%는 용어를 들어봤으나 자세히 모른다고 응답하였다. 그 중, 제로트러스트 보안 개념을 적용하려는 의향이 있는 기업 중 용어를 모른다고 응답한 기업은 6.5%, 용어를 들어봤으나 자세히 알지 못한다고 응답한 기업은 65.2%인 것으로 나타났다. 이처럼, 조사 당시 전체 수요기업의 약 90% 이상은 제로트러스트를 정확히 인지하지 못하고 있는 것으로 조사되어, 인식 개선 및 홍보가 필요하다고 판단되었다.

표 S-4 제로트러스트 인지도 (단위: %)

구분	전체	제로트러스트 적용 중이거나 의향이 있는 기업
모른다	62.5	6.5
용어는 들어봤으나, 자세히 알지는 못한다.	31.0	65.2
용어에 대해 자세히 알고 있다.	6.5	28.3

또한 제로트러스트를 이미 적용하고 있는 기업이 2.5%, 적용하고 있지만 구체적인 도입 계획이 있는 기업이 3.0%인데 반하여, 도입 의사는 있지만 어떻게 해야 하는지 모르겠다는 기업이 17.5%,

도입 계획이 전혀 없다는 기업이 77%로 조사되었다. 제로트러스트 도입 계획이 없는 이유에 대해서는 제로트러스트에 대한 정보 부족(62.0%), 보안 강화의 필요성을 못 느껴서(23.6%) 등으로 조사되었으며, 적용 기업의 도입 계기에 대해서는 IT환경의 변화에서 보안성을 높이기 위함이 50%, 정교해지는 보안 공격에 대한 보안 강화가 39.1% 등으로 조사되었다.

표 S-5 제로트러스트 도입 계획이 없는 이유 (단위: %)

구분	응답 비중
임원진의 보안 의식 부족	14.7
보안 강화의 필요성을 못 느껴서	23.6
제로트러스트 도입 비용의 부담	4.6
도입 시 업무상 불편 증가	2.9
제로트러스트에 대한 정보 부족	62.0
기타	3.3

제로트러스트 보안 솔루션 도입 시 기대 효과에 대해서는 전체적인 보안 기능 향상을 기대한다는 응답(54.3%)이 가장 높았고, 그 뒤로 사고 후 복원력 향상(23.9%), 사용자의 이용환경 개선(17.4%) 등이 뒤를 이었다. 그러나 2순위 응답까지 포함할 경우, 사용자의 이용환경 개선이 높은 응답률을 보임으로써 수요기업들은 제로트러스트 도입을 통하여 보안 기능 향상과 사용자의 이용 환경 개선을 모두 기대하는 경우가 많다는 것을 알 수 있었다.

표 S-6 제로트러스트 보안 솔루션 도입 시 기대 효과 (단위: %)

구분	1순위	1+2순위
전체적인 보안 기능 향상	54.3	84.8
사고 후 복원력 향상	23.9	39.1
사용자의 이용 환경 개선	17.4	60.9
IT 비용 절감	2.2	13.0
기타	2.2	2.2

제로트러스트 관련 보안 솔루션 도입 시 애로사항에 대하여 각 선택지에 대한 점수(5점 만점)의 평균을 조사한 결과 기존 사용 중인 보안 제품과의 호환성에 대한 애로사항이 3.78점으로 가장

높았으며 도입 시 필요한 예산의 부족이 3.57점으로 뒤를 이었다.

표 S-7 제로트러스트 보안 솔루션 도입 시 애로사항 (단위: 점, 5점 만점)

구분	응답 점수
고성능 제품을 보유한 공급사 부족	3.07
제로트러스트 도입 전략에 대한 지식 부족	3.20
경영진의 제로트러스트에 대한 개념 및 인식 부족	3.00
기존 사용 중인 보안 제품과의 호환성	3.78
도입 시 필요한 예산의 부족	3.57

나. 제로트러스트 기술

가이드라인 1.0에서 제시한 제로트러스트 성숙도와 관련해서, 기존 수준(1점), 향상 수준(5점), 최적화 수준(10점)으로 기업망 핵심 요소에 대한 성숙도 수준을 조사한 결과, 수요기업들의 제로트러스트 성숙도 수준은 향상 수준에 미치지 못하는 낮은 수준들로 조사되었으며, 특히 애플리케이션 및 워크로드,[10] 데이터의 성숙도 수준이 상대적으로 더 낮게 평가되었다.

표 S-8 제로트러스트 관련 보안 기술의 성숙도 수준 현황 (단위: 점, 5점 만점)

기업망 핵심 요소	응답 점수
식별자·신원	3.28
기기 및 엔드포인트	3.52
네트워크	3.04
시스템	2.74
애플리케이션 및 워크로드	1.30
데이터	1.46

또한 각 핵심 요소들의 교차 기능(가시성 및 분석, 자동화 및 통합)에 대해서는 활용하지 않는다는 응답이 각각 80.4%, 76.1%로 상당히 높은 비중을 차지하고 있어, 수요기업이 보유하고 있는 보안 기술이 제로트러스트 성숙도 관점에서 높지 않은 수준임을 파악할 수 있다.

10 원문에서는 가이드라인 1.0에 따라 '응용 및 워크로드'라고 표현하고 있으나, 본 문서의 용어 정의에 따라 여기에서는 모두 '애플리케이션 및 워크로드'라고 표현한다.

표 S-9 제로트러스트 관련 보안 기술 보유 수준 현황 (단위: %)

구분	가시성 및 분석	자동화 및 통합
식별자·신원	10.9	4.3
기기 및 엔드포인트	8.7	10.9
네트워크	6.5	4.3
시스템	6.5	2.2
애플리케이션 및 워크로드	3.3	1.2
데이터	4.3	13.0
활용 안 함	80.4	76.1

다. 제로트러스트 정책

수요기업들이 각 핵심 요소별로 제로트러스트 도입에 대한 중요성 및 시급성을 조사한 결과 네트워크(중요성 6.83점, 시급성 7.13점)에 대해 가장 높은 응답 결과를 보였으며, 식별자·신원(중요성 5.65점, 시급성 5.91점)이 그 다음으로 높은 응답을 보였다. 애플리케이션 및 워크로드(중요성 2.09점, 시급성 2.00점)는 중요성 및 시급성이 상대적으로 매우 낮게 인식되고 있었으나 클라우드 전환 등을 고려하면 차후에는 더 높은 중요성 및 시급성을 보일 가능성이 높다고 보인다.

또한 수요기업들은 제로트러스트 도입을 위해 필요한 정책으로 '보안 강화 및 제로트러스트 필요성 인식 제고'(78.3%)를 꼽고 있다.

표 S-10 제로트러스트 도입 시 필요한 정책 (단위: %)

구분	응답 비중
제로트러스트 도입 관련 구체적인 방법 및 절차	67.4
보안 강화 및 제로트러스트 필요성 인식 제고	78.3
제로트러스트 도입 시 보안 인증 관련 제도 완화	37.0

3. 공급 기업의 제로트러스트 인식 수준

가. 제로트러스트 출시 현황

국내 정보보호 공급기업의 68.5%는 제로트러스트 관련 솔루션을 출시하였거나, 개발 및 계획 단계에 있다고 조사되었으며, 관련 제품을 보유하고 있다고 응답한 기업은 24.1%였다.

표 S-11 제로트러스트 솔루션 출시 현황 (단위: %)

솔루션 출시 현황	비중
출시 (관련 제품이 있음)	24.1
개발 단계	7.4
개발 계획 단계	37.0
개발 계획 전혀 없음	31.5

제로트러스트 솔루션 출시와 관련하여 공급기업의 애로사항으로는 '공급절차의 복잡성'이었으며, 정책 및 방향성의 부재, 전문 인력의 부족 등이 그 뒤를 이었으나, 주요 애로사항에 대하여 전반적으로 어려움을 겪고 있는 것으로 조사되었다.

표 S-12 제로트러스트 솔루션 출시 주요 애로사항 (단위: 점, 5점 만점)

솔루션 출시 현황	비중
공급 절차의 복잡성	4.0
정책 및 방향성의 부재	3.9
전문 인력의 부족	3.8
수요기업의 제로트러스트 도입에 대한 인식 부족	3.7
시장의 불확실성 때문에 사업 확대 시 위험 부담	3.6
수요기업의 기존 솔루션과의 연동이 어려움	3.5
기술 개발의 어려움	3.4

제로트러스트 핵심 원칙에 대한 우선순위는 인증체계 강화(54.1%)가 마이크로 세그멘테이션(16.2%), 소프트웨어 정의 경계(29.7%)보다 높게 나타났으며, 이 수치는 수요기업과 비교하여 소프트웨어 정의 경계의 비중이 더 높은 것을 알 수 있다.

나. 보유 기술 현황

공급기업의 보안 기술 영역은 기업망 핵심 요소 관점에서 네트워크 영역이 가장 높은 수준을 보였으며, 가시성 및 분석, 자동화 및 통합 부분에서는 기기 및 엔드포인트 영역에서 가장 높은 수준을 보였다. 또한 대부분의 항목에서 향상에서 최적화 사이의 성숙도 수준으로 답하는 경향을 보였다.

표 S-13 제로트러스트 보유 솔루션 기술 수준

(단위: 점, 10점 만점)

기업망 핵심 요소	기술 수준	가시성 및 분석	자동화 및 통합
식별자·신원	6.18	4.73	5.55
기기 및 엔드포인트	6.84	7.89	6.50
네트워크	7.06	6.91	6.00
시스템	5.93	4.00	5.50
애플리케이션 및 워크로드	4.86	5.40	3.60
데이터	6.85	6.00	5.43

다. 제로트러스트 기술 연구 개발 현황

제로트러스트 연구개발 시 애로사항으로는 공급기업의 67.6%가 '기술개발 인력 확보의 어려움'과 '각종 행정규제 및 제도의 미비'를 가장 많이 응답하였으며, '자금 부족'(29.7%)에 관한 응답에 비해 훨씬 높은 비중을 차지하였다. 또한 공급기업의 70.3%가 타 공급기업과의 협업 의향이 있다고 답하여, 단일 솔루션으로 구현할 수 없음을 인식하고 있다고 해석할 수 있었다.

라. 제로트러스트 산업 활성화를 위한 필요 정책

제로트러스트 산업 활성화를 위한 필요 정책으로 '법·제도 제·개정'(중요성 32.4%, 시급성 21.6%)을 가장 중요하게 인식하고 있으며, 가장 시급하게 보는 정책으로는 '수요기업과 공급기업을 연계하는 사업 확대'(중요성 24.3%, 시급성 24.3%)를 선택하였다.

표 S-14 제로트러스트 산업 활성화를 위한 필요 정책 (단위: %, 1순위)

산업 활성화를 위한 필요 정책	기술 수준	가시성 및 분석
수요기업과 공급기업을 연계하는 사업 확대	24.3	24.3
법·제도 제·개정	32.4	21.6
공공부문의 시장 수요 창출	13.5	21.6
기술 개발 지원	13.5	13.5
제로트러스트 관련 홍보 확대	8.1	13.5
전문인력 양성	8.1	5.4

4. 제로트러스트 인식 제고 방안

설문조사 결과에 따르면 수요기업의 대부분은 제로트러스트에 대한 인지도가 낮은 상태이며 기술 수준 역시 기존과 향상의 중간수준에 머물러 있는 것으로 나타났다. 제로트러스트 활성화를 위한 정책적 요구사항으로는 제로트러스트 도입에 따른 인센티브보단 제로트러스트 도입의 필요성(관련법령 또는 의무화 제도)을 더 중요시 여기는 것으로 나타났다.

공급기업은 과반수 이상 제로트러스트 보안 솔루션 출시, 개발, 기획단계에 있었으며, 기술 수준은 향상과 최적화의 중간수준에 있는 것으로 나타났다. 이는 수요기업이 도입한 기술이 현재 공급기업이 출시중인 제품이 아닌 과거 공급한 기술이라는 시간적 갭이 있음을 의미할 수 있다. 정책적 활성화 방안으로 공급기업은 도입정책(관련법령 및 의무화 제도)이 가장 중요하다고 응답했으며 수요기업과 공급기업을 연결하는 실증사업이 가장 시급하다고 답했다.

마지막으로, 해당 조사에 대한 보고서에서는 제로트러스트 활성화를 위해 법제도 측면에서 관련 제품 인증개선, 성숙도에 따른 평가방법론 개발 등이 필요하며, 현재 과기부와 한국인터넷진흥원에서 진행하는 실증사업 및 가이드라인의 고도화가 필요함을 언급하였다. 기술 개발 측면에서는 제로트러스트 보안모델의 구현을 위해 기존 보안 솔루션 간의 연동환경 기반조성, 통합보안제품군과 기존제품과의 연동, 통합보안제품군과 PDP 및 PEP 간 연동이 필요함을 주장하였다. 인식 제고를 위하여, 제로트러스트 관련 포럼 및 컨퍼런스 활성화, 그리고 재직자 및 구직자를 대상으로 하는 정보보호교육의 필요성을 강조하였으며 실증사례의 홍보 및 장기적 관점에서 모범사례집 발간 등을 언급하였다.

| 제3절 |

제로트러스트 아키텍처 참조 모델 실증 사례

3절에서는 제로트러스트 아키텍처에 대해 2023년 과학기술정보통신부에서 진행한 2가지 실증 사례를 제시한다. 해당 실증 사례는 첫째 클라우드 환경 제로트러스트 적용 실증 사례, 둘째 온프레미스 통합 환경 제로트러스트 적용 실증 사례에 대해 제로트러스트 철학을 기반으로 보안성을 개선하면서도 상기 문제를 해결하는 방안에 대한 참조 모델을 제안하는 것으로 볼 수 있다.

다만, 본 문서의 독자들은 여기에서 제시하는 참조 모델이 상기 사례에 대하여 제로트러스트 철학을 기반으로 문제를 해결하는 하나의 아키텍처를 제안하고 있으나, 이 방식이 가장 적절한 해결책은 아니며 또한 제로트러스트 관점에서도 가장 높은 수준의 성숙도가 아니라는 점을 이해하여야 한다. 기업 입장에서는 해당 사례를 참조하되, 기업망 환경에 적절한 제로트러스트 도입 전략과 고유의 제로트러스트 아키텍처를 수립하는 것이 필요하다.

1. 클라우드 환경 제로트러스트 적용 실증 사례

가. 개요

국내 기업의 클라우드 도입에 대한 시장의 요구는 나날이 늘어가고 있다. 국내 기업의 약 69.8%가 클라우드 서비스를 이용[11]하고 있으나 클라우드 보안 사고는 증가하는 추세[12]이고 기업의 서비스가 중단되는 등 많은 보안의 문제점이 노출되고 있다. 이와 함께 클라우드 환경에서 보안은 클라우드 도입과 확산의 측면에서 큰 불안 요소로 인식[13]된다. 이러한 보안의 위협은 SaaS

11 '2023년도 정보화 통계 조사' 클라우드 컴퓨팅을 활용하는 서비스는 이메일(80.9%), 전사적 자원관리(ERP) 소프트웨어(52.5%), 오피스 소프트웨어(49.0%) 순

12 클라우드 사용 조직 23% "한 번 이상 보안사고 당해", 제5회 클라우드 보안 & SECaaS 인사이트 2023' 참가자 설문조사, 데이터넷(https://www.datanet.co.kr)

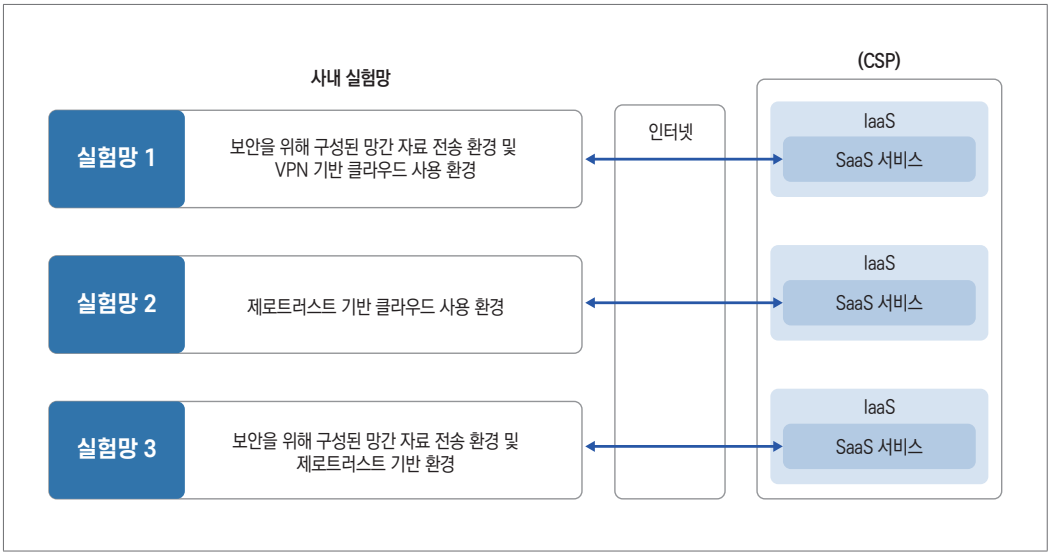
13 "2024년 국내 클라우드 컴퓨팅 및 AI 현황과 전망"에 따르면 클라우드 도입 및 활용과정의 어려움 중 1위가 클라우드 비용 통제 항목(47.8%)이고 그 다음이 데이터 프라이버시 및 보안 항목(30.6%)이다.

기반 애플리케이션 등 인터넷에 상시 연결된 클라우드 서비스를 완벽히 통제할 수 없기 때문이다. 또한, 기존 레거시 보안 기술로 구성된 CSP의 보안 관제 인프라로는 세밀한 접속 제어 및 보안 관제 등 세부 내용을 충족할 수 없다. 기존 레거시 보안 기술은 클라우드 서비스를 공급하는 CSP와 고객 간 보안 책임에 대한 경계가 모호한 경우도 존재하기 때문에, 이에 대한 근본적인 대책이 필요하다.

본 실증 사례의 제로트러스트 보안 모델은 기업망 내·외부에 언제 어디서든 공격자가 존재할 수 있으며, 기존 기업망에서의 신뢰성이 더 이상 유효하지 않다는 전제로 진행하였다. 따라서 기업 내 자산(데이터 혹은 리소스)에 접근하는 모든 주체를 지속적으로 인증하고, 자산에 대한 위험성을 끊임없이 평가하며, 위험을 완화하는 대책을 포함하였다.

클라우드 기반 SaaS를 사용하고자 하는 기업환경에 제로트러스트 보안 모델을 적용함으로써 실제 클라우드 사용할 경우 발생할 수 있는 보안 문제점을 확인·분석하였으며, 각 환경 대비 개선 효과 분석을 위해 다음의 3가지 실험망 환경 구성 및 실험 시나리오를 수립해 실증을 진행했다.

그림 S-1 클라우드 환경 제로트러스트 실증을 위한 실험망 개념도



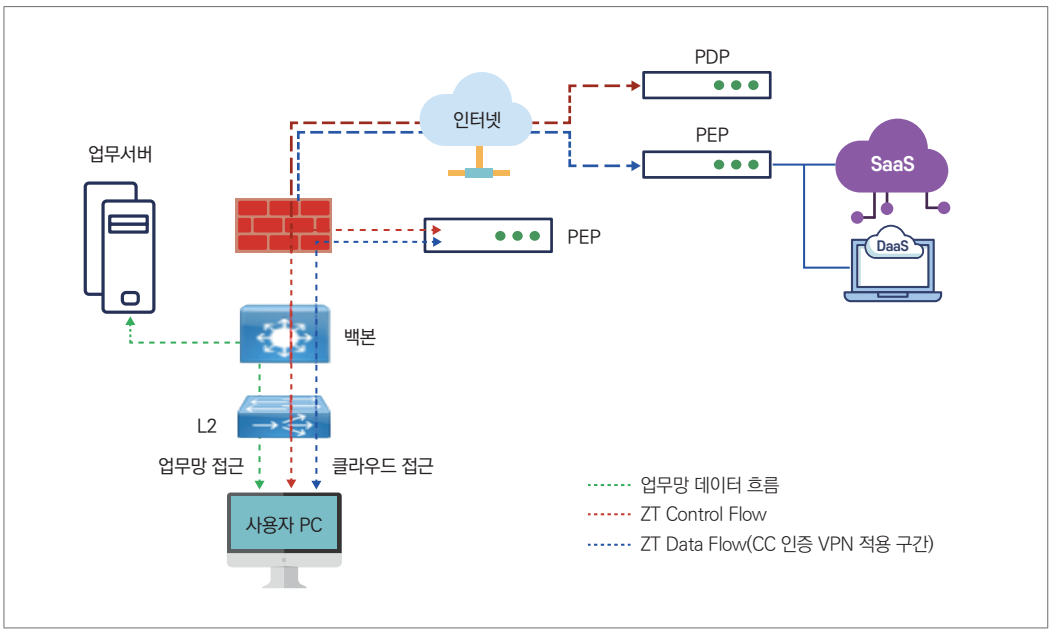
나. 실증 환경 및 방법

1) 실증 환경 및 내용

- ‘A 기업’의 경우 제로트러스트 기반 SaaS 보안 관제 연동 시험 사업을 통해 실증을 진행. 구체적으로 SaaS 보안 관제 및 세밀한 접근권한을 부여함으로써 보안성이 높은 SaaS 사용 환경을 구성한 후, 시험 진행
- 제로트러스트 시험망은 SaaS 인프라 환경을 반영해 독립적으로 구성
- 기존 보안 아키텍처를 가정한 접속 통제·VPN 기술 적용 환경(실험망 1)과 제로트러스트 아키텍처 적용 환경(실험망 2, 3)으로 구분하여 실험을 수행하였으며, 실험망 별 세부 환경은 다음과 같음
  - (실험망 1) 보안을 위해 구성된 망간 자료 전송 환경 및 VPN 기반 클라우드 사용 환경
  - (실험망 2) 제로트러스트 기반 클라우드 사용 환경
  - (실험망 3) 보안을 위해 구성된 망간 자료 전송 환경 및 제로트러스트 기반 클라우드 사용 환경

2) 실증 방법 및 네트워크 구성

그림 S-2 클라우드 환경 제로트러스트 실증을 위한 실험망 구성도

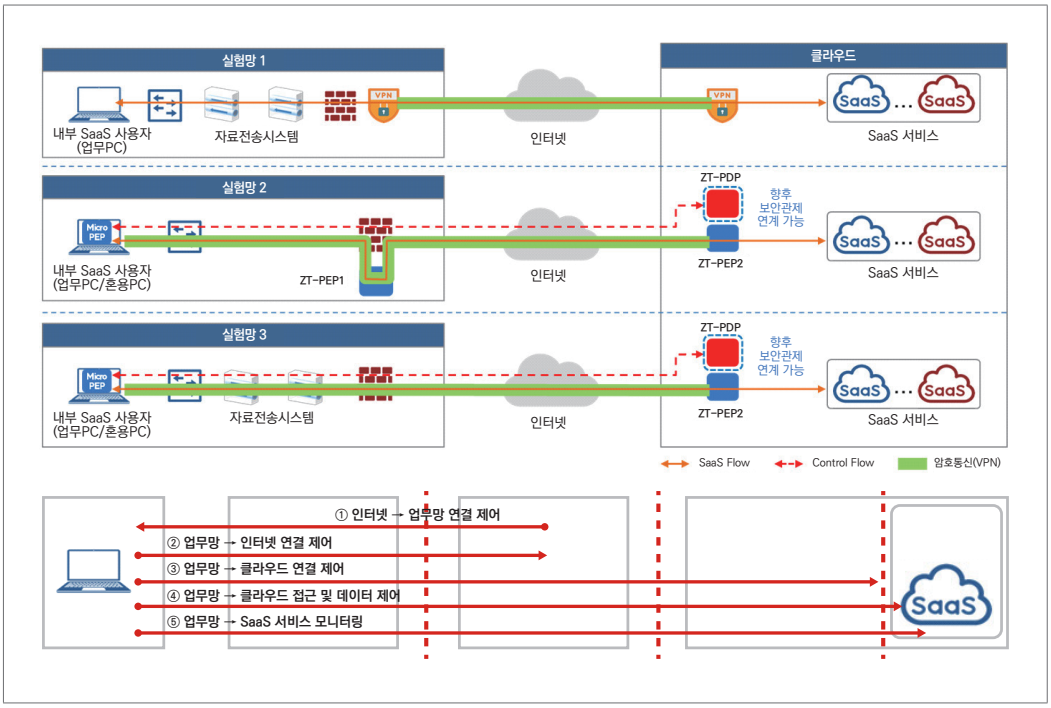


- (실험망1) 파일 송수신 제어, VPN을 이용한 암호 통신
- (실험망2) 제로트러스트를 이용한 SaaS 접근제어, 파일 송수신 제어, 암호 통신 및 모니터링
- (실험망3) 파일 송수신 제어, 제로트러스트를 이용한 SaaS 접근제어, 암호 통신 및 모니터링

3) 실증 시나리오

- 사용자·단말의 SaaS 사용 접근을 제어 영역(①~④)과 모니터링 영역(⑤)으로 구분, 25개의 시험 항목을 도출

그림 S-3 클라우드 환경 제로트러스트 실증 시나리오 개념도



① 인터넷 → 업무망 연결 제어

(1) 인터넷에서 업무망에 연결된 단말 또는 리소스 접속

(2) 인터넷에서 업무망에 연결된 단말로 파일 전송 제어

② 업무망 → 인터넷 연결 제어

(3) 업무망 연결 단말의 인터넷(웹 서비스) 접속 차단

③ 업무망 → 클라우드 연결 제어

(4) 업무망 연결 비인증 단말의 클라우드 접속 차단

(5) 업무망 연결 비인증 단말의 SaaS 접속 차단

(6) 강화된 인증 수행 단말(및 사용자)의 비허용 된 SaaS 접속 차단

(7) 강화된 인증 수행 단말(및 사용자)의 허용된 SaaS 접속 허용

(8) 강화된 인증 수행 단말(및 사용자)의 SaaS 접속 시, 일원화된 인증(SSO) 처리

(9) 일원화된 인증(SSO) 기반 SaaS 사용 시, 인증 정보 보호

(10) 보안 규정 미준수 단말의 SaaS 접속 차단

(11) 지속적 검증을 통해 보안 규정 미준수 단말의 접속 해제

(12) 허용되지 않은 소프트웨어로 SaaS 접속 차단

(13) 허용된 소프트웨어로 허용되지 않은 SaaS 접속 차단

(14) 소프트웨어 공급망보안 검사 기반 안전하지 않은 소프트웨어의 SaaS 접속 차단

(15) 사용자 정보 삭제 시 SaaS 접속 해제

(16) 단말 또는 업무망과 클라우드 간 터널링 기반 데이터 패킷 보호

④ 업무망 → 클라우드 접근 및 데이터 제어

(17) 인증된 사용자가 SaaS 내 허용되지 않은 기능접근 차단

(18) 인증된 사용자의 SaaS 내 파일 업로드 차단 수행

(19) 인증된 사용자의 SaaS 내 파일 다운로드 차단 수행

(20) 인증된 사용자의 SaaS 내 파일 업로드 백신 검사 기반 차단 수행

(21) 인증된 사용자의 SaaS 내 파일 다운로드 백신 검사 기반 차단 수행

⑤ 모니터링 (접속 통제 및 망간 자료 전송)

(22) 실시간 통신 구간을 통과하는 모든 사용자, 단말, 소프트웨어, SaaS 접속기록

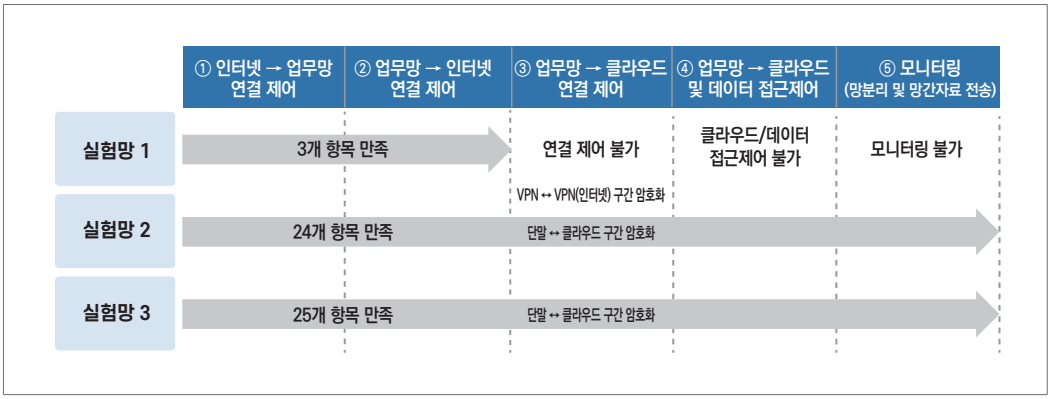
(23) 실시간 통신 구간을 통과하는 모든 사용자, 단말의 보안 컴플라이언스 준수 여부 기록

(24) 실시간 통신 구간을 통과하는 모든 사용자, 단말의 SaaS 내 기능(URL)접근 기록

(25) 접속 통제 및 망간 자료 전송 실시간 통신 구간을 통과하는 모든 사용자, 단말의 SaaS 내 파일 업로드 및 다운로드 기록

다. 실증 결과 및 개선 효과

그림 S-4 클라우드 환경 제로트러스트 실증 환경별 시험 항목 만족 수준



- (실험망 1) '물리적 접속 통제+망간 자료 전송+VPN' 환경은 업무망 ↔ 클라우드(③), 업무망 ↔ 클라우드/데이터 접근(④), SaaS 사용 모니터링(⑤) 부분에서 제어 및 모니터링 기능을 제공하지 않는 환경으로 구성함
  - 현재 망간 자료 전송 시스템은 SaaS 서비스에 대한 파일 송수신 제어 기능을 제공하지 않는 등 보안 취약점 발생
- (실험망 2) 접속 통제가 불가능한 환경에 제로트러스트 기술을 적용하면 SaaS 서비스 접근제어, 암호 통신 및 모니터링 등 추가 보안 기능 사용할 수 있어 보안성 강화
- (실험망 3) '물리적 접속 통제+망간 전송' 환경에 제로트러스트 기술을 적용하면 SaaS 서비스 접근제어와 파일 송수신 제어 및 모니터링 부분에서 보안성 강화
  - SaaS 보안 관제 및 세밀한 접근권한을 부여함으로써, SaaS 사용 환경에서 기존 보안 시스템 대비 보안을 강화할 수 있다는 사실을 확인함

1) 가이드라인 1.0을 준수하는 대안 기술 제시

- 가이드라인 1.0에 기반한 모델을 통하여 클라우드 보안 강화 방안을 마련
- 외부 인터넷과 논리적으로 격리된 제로트러스트 기반 단말 격리 기술을 적용함
- 클라우드 내 SaaS와 업무망 내 PC 간 제로트러스트 기반 접속 통제 기술을 적용함
- 先인증 後접속 통신 제어 메커니즘 기반 SaaS에 특화된 관제 기술을 적용함

2) 기존 보안 기술과 제로트러스트 접속 제어 비교 개선 효과 도출

- 각종 보안 지침의 준수 및 보안성이 강화된 제로트러스트 기반의 접속 통제 환경을 통해 보안성을 강화함
- 각종 보안 솔루션을 통한 파일 전송 제어 환경의 경우, 실시간 통신 구간의 관제 기술이 없으므로 클라우드와 SaaS 사용이 불가능할 수 있음
- 제로트러스트 기반 논리적 접속 통제된 환경에서 클라우드 전송 제어 기술 적용 시 SaaS 관제 및 기존 보안 솔루션과 같은 파일 전송 제어가 가능함

3) 애플리케이션 레벨 보안 관제 및 통제 기준 마련

- 기존 보안 솔루션의 취약점인 실시간 통신 구간의 관제 사각지대 개선
- SaaS 관제 및 효율적인 접속 통제 문제 해결을 통해 통제 가능한 보안에 특화된 SaaS 모델 제시
- 상기 요소를 통해 안전하고 보안성이 강화된 SaaS 사용 환경 기준 절차를 마련

4) SaaS 공급 및 수요기업의 보안 수준 제고 방안 마련

- SaaS 수요 희망 기업에 제로트러스트 모델을 적용하여 안전하게 SaaS 서비스를 이용할 수 있는 보안 수준 제고 방안 마련
- SaaS 공급기업은 제로트러스트 모델을 사용해 수요기업에 SaaS 공급
- SaaS 수요기업은 제로트러스트 모델이 적용된 SaaS 도입 가능 여부를 확인 가능

5) SaaS 보안 플랫폼 및 거버넌스 확보

- 안전한 SaaS 사용을 위한 보안 플랫폼 적용을 위해서 제로트러스트 모델 중심의 다양한 보안 기술과 연동해 보안성을 강화할 수 있음
- SaaS를 적용 추진하고자 하는 기업의 SaaS 공급자의 시스템 접근권한 및 SaaS 사용 관리자 접근권한 승인 체계 확보
- 제로트러스트 모델 적용으로 SaaS에 특화된 관제 로그의 기업 내 공유 체계 확보
- 제로트러스트를 적용, 접속 통제 환경에서 발생하는 보안 사각지대를 해소함으로써 클라우드 기반 SaaS를 보다 안전한 환경에서 사용할 수 있도록 개선

  - 레거시 보안 환경에서 클라우드 기반 SaaS 사용 시, 보안 사각지대 발생
  - 제로트러스트 기술을 적용해 다양한 환경에서 클라우드 기반 SaaS 사용에 따른 보안 사각지대를 개선하는 결과 도출
- 제로트러스트 모델 기반, SaaS에 최적화된 보안 관제 체계 구축
  - SaaS 환경에서는 인증된 사용자가 허용된 서비스를 사용해야 함. 따라서, TMS, SIEM 등 관제 방식과 함께 SaaS에 특화된 관제 기술 및 체계 필요
  - 본 실증을 통해 제로트러스트를 적용한 SaaS 특화 관제 기술 확보. 향후 다양한 보안 관제 시스템(TMS, SIEM 등)과 결합한 SaaS 특화 관제 체계를 도입할 경우, 보안성 강화 효과

2. 온프레미스 통합 환경 제로트러스트 실증 사례

가. 실증 개요

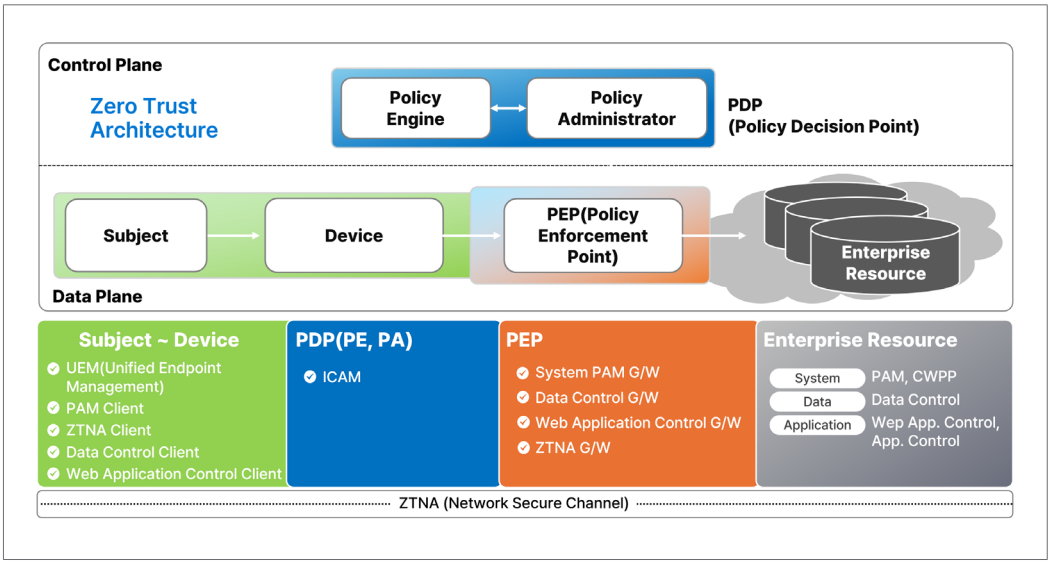
본 실증은 기업 리소스의 시스템, 애플리케이션, 데이터를 모두 보호할 수 있는 제로트러스트 아키텍처 프레임워크를 구축하는 것이다.

이를 위해 사용자 기기(PC)에는 신뢰도를 도출하기 위하여 기기 위험 상태를 판단하여 위험도를 확인하는 사용자 UEM이 구축된다. 이를 통해 사용자가 리소스에 접속하는 경우에는 항상 기기의 신뢰도 점수를 기반으로 PDP에서 접근권한 승인 여부를 평가하게 된다. PEP는 리소스의 종류(시스템, 애플리케이션, 데이터)에 따라 각각 3개의 PEP가 구축되었고, 이 중 애플리케이션을 위한 PEP는 VPN을 대체하고 안전한 네트워크 연결기능을 제공하는 ZTNA의 역할도 수행하였다.

PDP는 ICAM을 기반으로 구축되었고, 해당 ICAM은 사용자, 기기 및 엔드포인트(PC), 리소스 중 시스템 등의 자산과 계정을 등록하고 관리하는 기능, MFA 통합 인증 제공 기능, 접근제어 정책 관리 기능 등을 제공하도록 하였다. 특히 본 실증에서는 4개의 PEP와 PDP가 상호 연동되어 제로트러스트 아키텍처를 실현하는 사례를 구현하였다.

마지막으로 리소스 중 시스템에 대하여 가상화 환경에서의 제로트러스트 핵심 구현 사항 중 하나인 마이크로 세그멘테이션(Micro Segmentation)을 실증하였다.

그림 S-5 온프레미스 통합 환경 제로트러스트 실증을 위한 환경 구성



- (제로트러스트 아키텍처) NIST 제로트러스트 아키텍처 및 가이드라인 1.0의 구성요소를 모두 준용한 제로트러스트 보안 모델
- (리소스 보호 강화) 시스템, 데이터, 애플리케이션으로 정의된 엔터프라이즈 리소스의 보호, 리소스별 세부 보호
- (ZTA + ZTNA) 접근 주체로부터 리소스에 이르는 전 영역에 대해 구체적인 제로트러스트 목표 보안 모델 및 시스템 제시
- (제로트러스트 원리 및 접근법 반영) 가이드라인 1.0의 제로트러스트 아키텍처 기본 원리, NIST SP 800-207의 제로트러스트 기본 원리 7가지 및 접근법 3가지에 부합하는 보안 시스템 실증

나. 실증 환경 및 방법

1) 목표 제로트러스트 아키텍처 시스템 논리적 구성

목표 시스템 구성은 크게 온프레미스 통합 환경 상의 사용자 기기(PC), PEP, PDP, 리소스로 구분된다. 우선 사용자 PC에는 크게 5개의 사용자 클라이언트 SW가 설치된다. 첫 번째는 사용자 PC의 신뢰도 평가를 지원하는 엔드포인트용 클라이언트, 두 번째는 시스템 접근제어

기능을 제공하는 시스템 접근제어 클라이언트, 세 번째는 네트워크 보안 기능을 제공하는 ZTNA 클라이언트, 네 번째는 데이터 접근제어 기능을 제공하는 데이터 접근제어 클라이언트, 다섯 번째는 웹 애플리케이션 제어 기능을 제공하는 웹 애플리케이션 제어 클라이언트이다.

PEP의 경우에는 총 4개의 PEP가 구성되었는데 시스템 접근제어를 위한 PEP, 애플리케이션 접근제어 PEP, 네트워크 보안 기능을 제공하는 PEP, 그리고 데이터 접근제어 기능을 제공하는 데이터 제어 PEP이다.

PDP의 경우에는 ICAM 중심의 PDP를 구축하고 이를 기반으로 기업 사용자 계정, 사용자 PC, 리소스를 모두 등록하여 인가된 사용자와 인가된 시스템만 운용 가능하게 한다. 또한 MFA 기반의 사용자 통합 인증 기능을 제공함으로써 각각의 PEP가 리소스 접속 시 사용자 계정 및 통합인증 관리를 수행하는 역할을 한다.

마지막으로 리소스는 서버 시스템, 애플리케이션, 데이터로 구성된다. 이 중 서버 시스템, 애플리케이션 보호 및 데이터 보호는 PEP에서 지원되며, 서버 시스템의 마이크로 세그멘테이션은 시스템 접근제어 에이전트, 워크로드 보호 에이전트 등을 기반으로 구성된다.

그림 S-6 온프레미스 통합 환경 제로트러스트 아키텍처 논리 구성도

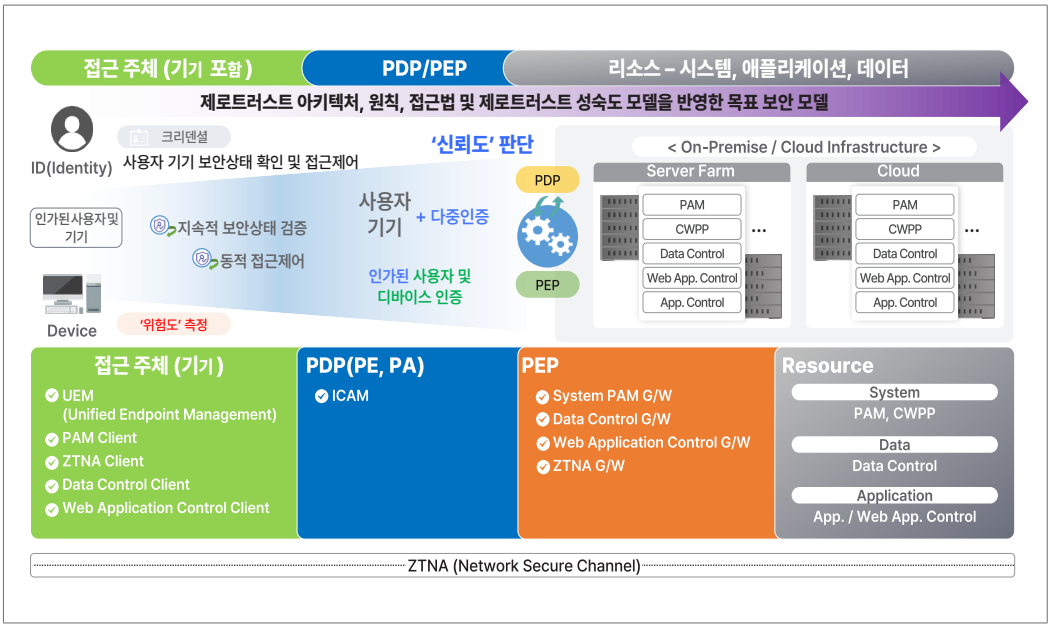


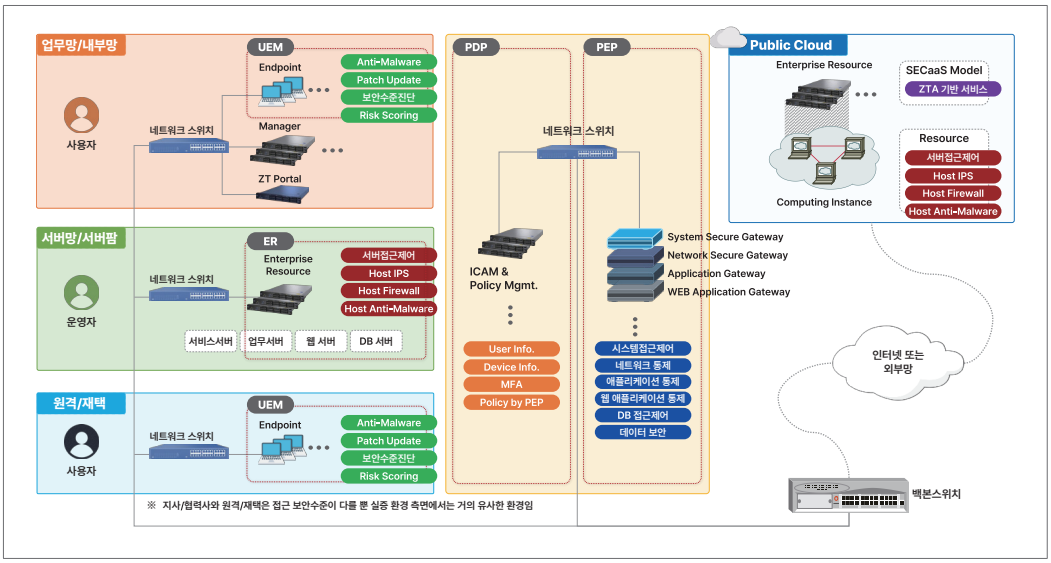
표 S-15 상기 논리 구성도 상 보안 영역별 주요 기능

보안 영역별 주요 기능	UEM	사용자 기기 통합 엔드포인트 보안 관리 및 평가
	Data Control	파일 접근/저장 제어, 무해화 검사
	Web App. Control	웹 애플리케이션 통제
	ICAM	사용자, 기기 인증 및 접근제어 정책관리
	PAM G/W	시스템 접근제어 G/W
	PAM	보안 커널 기반 접근제어
	CWPP	VM 워크로드 보안
	ZTNA	안전한 채널 구성, 접근통제

2) 목표 제로트러스트 아키텍처 물리적 구성

앞에서 언급한 제로트러스트 아키텍처의 논리적 구성을 기반으로 실제 실증 환경에서 구성이 되는 물리적 구성은 아래 [그림 S-7]과 같다. 그림에서 실증 기업의 온프레미스 환경은 “업무망/내부망”과 “서버망/서버팜”으로 이루어지며 기업 내 내부 직원들도 해당 존에 함께 존재하게 된다. 또한, 재택 또는 원격 근무를 수행하는 기업 직원들이 존재할 수 있는데 이를 “원격/재택”으로 표현한다. PEP와 PDP 시스템은 기본적으로 기업 내부에 존재하게 되는데 퍼블릭 클라우드를 사용하는 환경에서는 클라우드 존에 구성되어 운용될 수도 있다.

그림 S-7 온프레미스 통합 환경 제로트러스트 아키텍처 물리적 구성도



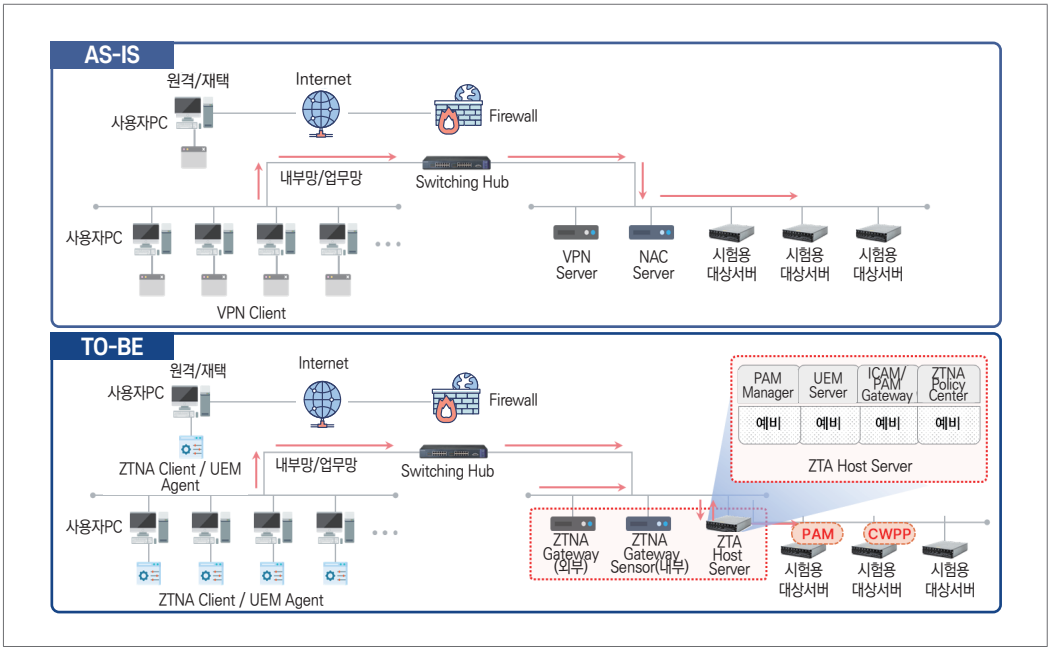
- 경계 보안 모델 대비 구성
  - 접근 주체로부터 리소스에 이르는 보안 영역별 목표 보안 모델 물리적 구성
  - 경계 보안 모델은 외부는 신뢰하지 않는 영역, 내부는 신뢰하는 영역으로 구분
  - 제로트러스트 모델은 내·외부 경계를 구분하지 않고 모두 신뢰하지 않는 영역으로 구분
- 업무환경 별 물리적 구성
  - 업무망/내부망, 서버망/서버팜, 원격/재택 물리 구성 기준 실증
  - 업무환경 별 물리적 제로트러스트 보안 시스템 구성
  - 온프레미스, 클라우드(Private/Public), 원격/재택 업무환경 별 물리적 구성

3) 기존(As-Is) 시스템과 개선(To-Be) 시스템 비교

상기 모델을 기반으로 기존 시스템과 제로트러스트 아키텍처를 도입한 후의 개선된 시스템을 비교하면 아래 [그림 S-8]과 같다. 기존 시스템은 제로트러스트 아키텍처가 도입되기 전이고 개선된 시스템은 제로트러스트 아키텍처가 구축된 이후의 모델이다. 제로트러스트 아키텍처 구성을 위해서 PDP와 PEP 시스템을 제로트러스트 아키텍처 호스트(Host) 서버에 설치·구성하였고 애플리케이션 보호를 위한 PEP이자 ZTNA는 독립 서버를 기반으로 ZTNA 게이트웨이 형태로 구축하였다. 백엔드(Back-end) 서버팜(Server Farm) 존에는 마이크로 세그멘테이션을 위한 시스템 접근제어와 워크로드 보안 제품을 설치하여 운영하였다.

- 레거시 보안 모델 (As-Is 검증 환경)
  - 수요기관 기존 보안 모델 시스템 구성도
  - 일반적인 레거시 보안 솔루션 통합 구성
  - 사용자의 엔터프라이즈 리소스 접근 흐름
- 제로트러스트 보안 모델 (To-Be 검증 환경)
  - 제로트러스트 보안 모델 시스템 구성도
  - 본 사업 목표 보안 모델 구성요소로 재배치
  - 제로트러스트 기반 엔터프라이즈 리소스 접근 흐름

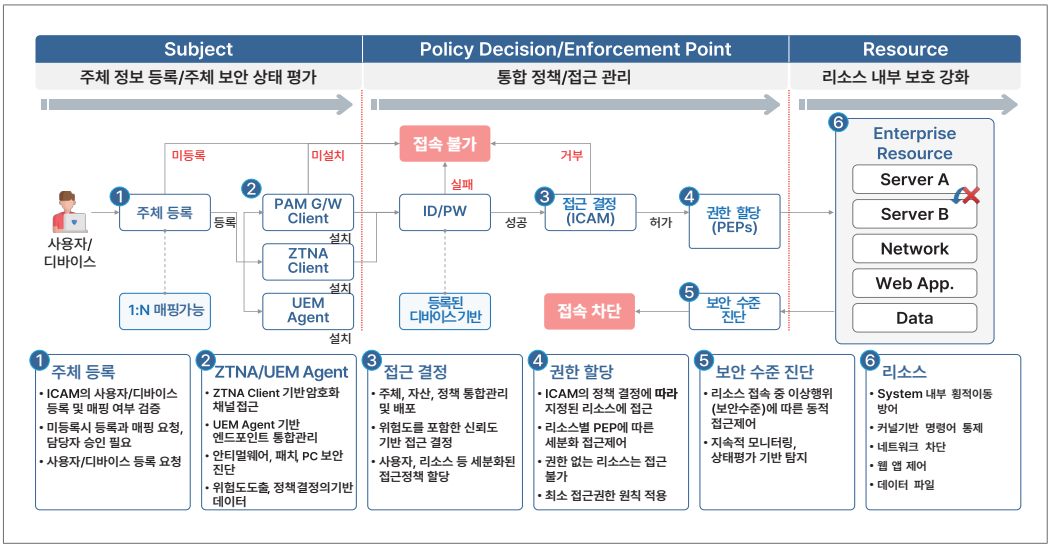
그림 S-8 온프레미스 통합 환경 제로트러스트 아키텍처 구성 도입 이후 개선 시스템 비교



다. 실증 결과

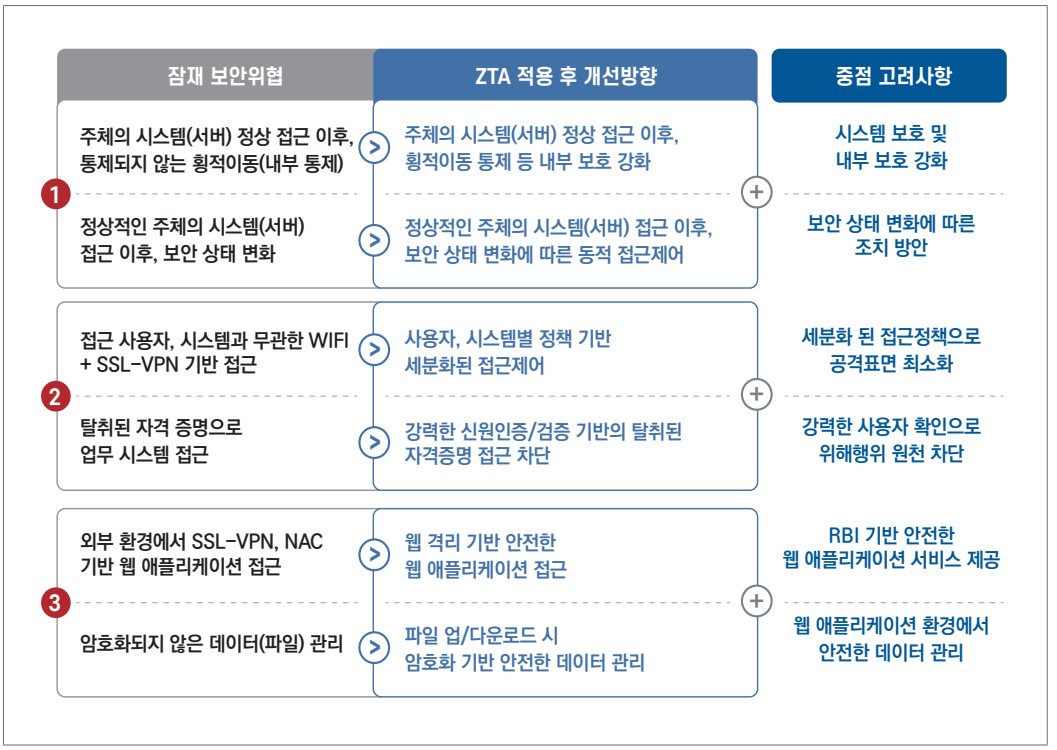
각 실증 수요기관들의 현재 시스템에서 보완해야 하는 추가 보안 필요 기능을 도출하고 이를 제로트러스트 아키텍처 보안 시스템을 구성하여 제공함으로써 제로트러스트 아키텍처 적용 후 보안 기능이 개선된 모델을 구현하였다.

그림 S-9 온프레미스 통합 환경 제로트러스트 아키텍처 도입 이후 업무 접근 프로세스



제로트러스트 아키텍처 적용 후 모든 사용자의 리소스 접근은 상기 [그림 S-9]와 같은 프로세스로 이루어지게 되었다. [그림 S-10]의 접근법을 기반으로 수요 기업들은 기존의 보안 위협 문제점을 개선할 수 있는 새로운 차세대 제로트러스트 아키텍처 기반 시스템 구성을 하게 되었고, 이를 통하여 잠재적인 보안 위협을 제거할 수 있게 되었다.

그림 S-10 온프레미스 통합 환경 제로트러스트 아키텍처 도입 후 강화된 보안 방향



| 제4절 |

미 연방정부 제로트러스트 도입·실증 현황

4절에서는 미 연방정부 제로트러스트 아키텍처 도입·실증에 현황에 대해 2가지 실증 사례를 소개한다. 해당 실증 사례는 각각 NIST SP 1800-35 제로트러스트 아키텍처 구현 프로젝트와 미 국방부 Thunderdome 프로젝트로, NIST 및 미 국방부에서 자체적으로 제로트러스트 아키텍처를 구현하여 도입하는 과정 및 구현하면서 얻은 결과에 대해 정리한다.

다만, 여기서 설명하는 제로트러스트 실증 사례들은 어디까지나 미국 환경에 초점을 맞춘 것이므로 망분리 정책과 같은 법적 규제가 있는 국내 환경에서는 적절하지 못한 사례일 수도 있다는 점을 인지하여야 한다. 기업 입장에서는 해당 제로트러스트 도입 실증 사례를 참고하되, 실증을 진행한 방법보다는 실증을 통해 얻은 교훈(어려움, 고려사항, 결과 등)에 초점을 맞추어 자체적인 제로트러스트 아키텍처를 수립하는 것이 필요하다.

1. NIST SP 1800-35 구현 현황

가. NIST SP 1800-35 문서 개요

NCCoE(National Cybersecurity Center of Excellence)는 NIST 산하의 사이버보안 센터로, 다양한 산업체 및 미 연방정부 기관과 협력하여 실질적인 사이버 보안 솔루션을 개발하고 있다. 특히, NIST SP 1800-35에서 중요한 역할을 담당하며, 제로트러스트 아키텍처 구현을 위한 다양한 접근법을 시연하기 위해 24개의 공급업체와 협력하여 프로젝트를 진행했으며, 단계적 접근 방식을 통해 기존 기업 환경에서 출발해 점진적으로 기능을 확장하거나 조정하는 방식으로 제로트러스트 아키텍처 솔루션을 개발했다. 첫 단계에서는 NIST SP 800-207에 명시된 세 가지 도입 방식 중 하나인 강화된 인증 거버넌스(EIG)를 도입하였으며, 초기 클라우드 기능을 포함하지 않는 단계인 EIG 초기 단계(EIG Crawl Phase)로부터 시작했다. 둘째 단계로, 클라우드 기능을

추가하여 EIG 실행 단계(EIG Run Phase)로 발전시켰다. 이후, 마이크로 세그멘테이션, SDP, SASE의 배포 방식에 대해서도 실증 사례를 추가하여 2024년 7월 현재 EIG 초기 및 실행 단계를 포함 총 17개의 사례를 실행하였으며, 각 사례가 제로트러스트 아키텍처 원칙을 만족하고 있다고 기술하였다.

이 프로젝트의 목표는 다양한 제로트러스트 아키텍처를 개발하고 시연하는 것이다. NCCoE는 NIST SP 800-207에 설명된 제로트러스트 아키텍처 원칙을 충족하는 기술 공급업체와 협력하여 여러 제로트러스트 아키텍처 솔루션을 구축함으로써 제로트러스트 아키텍처의 역량을 입증하고 있다. 이 솔루션의 목적은 기업 보안 정책을 준실시간 및 동적으로 적용하여 인증되고 권한이 부여된 사용자, 기기에 대한 접근을 제한하면서도 다양한 비즈니스 요구를 유연하게 지원하는 것이다. 구축된 제로트러스트 아키텍처는 기존 기업 및 클라우드 기술과 상호 운용성을 유지하면서 최종 사용자에게 미치는 영향을 최소화하도록 설계되었다.

그림 S-11 컨소시엄별 참여 기업

		Enterprise 1	Enterprise 2	Enterprise 3	Enterprise 4
EIG 초기 단계	Build1	AWS, IBM, Ivanti, Mandiant, Okta, Radiant Logic, SailPoint, Tenable, Zimperium	Cisco Systems, IBM, Mandiant, Palo Alto Networks, Ping Identity, Radiant Logic, SailPoint, Tenable	F5, Forescout, Lookout, Mandiant, Microsoft, Palo Alto Networks, PC Matic, Tenable	
EIG 실행 단계	Build2	AWS, IBM, Ivanti, Mandiant, Okta, Radiant Logic, SailPoint, Tenable, Zscaler		F5, Forescout, Mandiant, Microsoft, Palo Alto Networks, PC Matic, Tenable	
	Build3	AWS, IBM, Ivanti, Mandiant, Okta, Radiant Logic, SailPoint, Tenable, Zscaler	Cisco Systems, IBM, Mandiant, Palo Alto Networks, Ping Identity, Radiant Logic, SailPoint, Tenable, VMware	F5, Forescout, Mandiant, Microsoft, Palo Alto Networks, PC Matic, Tenable	IBM, Mandiant, Palo Alto Networks, Tenable, VMware
SDP, 마이크로 세그멘테이션, SASE	Build4	AWS, Appgate, IBM, Ivanti, Mandiant, Okta, Radiant Logic, SailPoint, Tenable, Zimperium	Google Cloud, IBM, Mandiant, Okta, Radiant Logic, SailPoint, Symantec by Broadcom, Tenable, VMware	F5, Forescout, Mandiant, Microsoft, Palo Alto Networks, Tenable	IBM, Mandiant, Tenable, VMware
	Build5	AWS, IBM, Mandiant, Okta, Palo Alto Networks, Radiant Logic, SailPoint, Tenable	Google Cloud, IBM, Lookout, Mandiant, Okta, Radiant Logic, SailPoint, Tenable, VMware	Mandiant, Microsoft, Tenable	
	Build6	AWS, IBM, Ivanti, Mandiant, Okta, Radiant Logic, SailPoint, Tenable			

이 프로젝트는 총 4개 컨소시엄의 장비들을 NIST NCCoE 환경에 배치하여 네트워크 구성 및 실증을 진행하였다. 해당 4개의 실험실 환경은 참여 기업간 협력을 위한 일종의 컨소시엄으로 각각 Enterprise 1~4로 불리는데, 각 환경에서 참여 기업의 클라우드 인프라를 사용하여 다양한 사례를 구현하고 시연하였다. [그림 S-11]은 각 환경에서 빌드별로 어떤 협력 기업들이 참여하였는지 보여준다.

1) NIST SP 1800-35 문서 발간 흐름

NCCoE는 이러한 프로젝트와 관련하여 2022년부터 5권(A~E)의 시리즈 문서를 발행하고, 지속적으로 의견을 수렴하여 수정 작업을 진행해왔다. 2023년 8월 기준 각 권별로 2~3번째 예비 초안(Preliminary Draft)이 발간되었다.

표 S-16 NIST SP 1800-35 문서 시리즈

권	제목	내용
A	Executive Summary	프로젝트 개요 (22.06, 22.12)
B	Approach, Architecture, and Security Characteristics	제로트러스트 참조 아키텍처 및 단계, 조직·빌드 소개, 구현 결과 및 교훈 등 (22.07, 22.12, 23.07)
C	How to Guides	빌드별 설정, 설치, 통합 방법 소개 (22.08, 22.12, 23.07)
D	Functional Demonstrations	빌드별 기능 데모 계획(유스케이스별) 및 결과 (22.08, 22.12, 23.08)
E	Risk and Compliance Management	위협, 취약점, 위험에 대한 정의 등 위험 분석과 제로트러스트 참조 아키텍처 빌드별 기능과 각 규정(CSF, 800-53 통제항목, EO-14028 보안조치)에 매핑 (22.12, 23.09)

이후, 2024년 7월경 방대한 내용을 담고 있는 각 시리즈 문서들을 통합하여 4번째 예비 초안으로써 두 가지 형식(PDF, 웹)으로 문서를 제공하기 시작했다. PDF 형식의 문서는 프로젝트 목표, 참조 아키텍처, 다양한 제로트러스트 아키텍처 구현 사례 및 결과에 대한 요약을 담아 프로젝트에서 얻은 주요 통찰을 제공하는 소개 자료로 활용된다. 웹 형식의 문서는 제로트러스트 아키텍처 구현 과정에서 활용된 기술, 통합 및 구성 방법, 입증된 사용 사례, 시나리오 등 심층적인 세부 정보를 제공한다.

2) 제로트러스트 아키텍처 구현 과제

NCCoE는 이 프로젝트 전반에 걸쳐 조직이 제로트러스트 아키텍처를 구현하는 데 있어서 직면할 수 있는 어려움들을 크게 3가지 관점(조직, 기본 요소, 기술)에서 분석하였다. 해당 내용은 다음 〈표 S-17〉에 기술되어 있다.

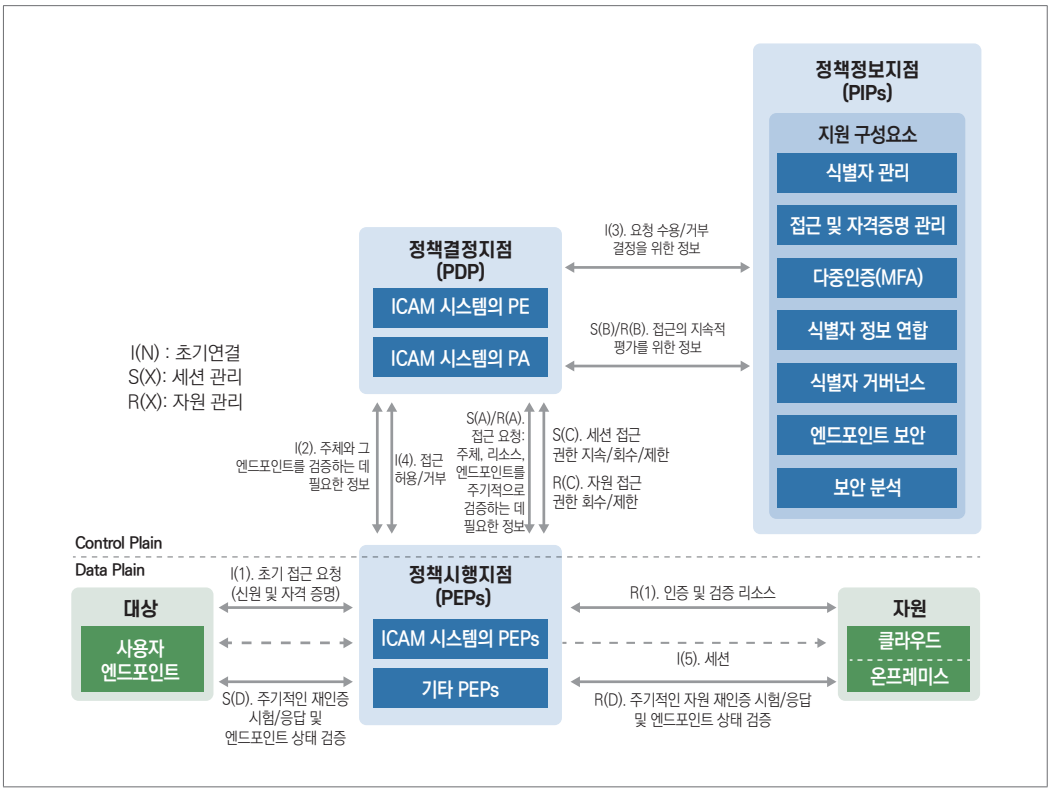
표 S-17 제로트러스트 아키텍처 구현에서의 어려움

관점	내용
조직 관점	▸ 제로트러스트 아키텍처가 대규모 조직에만 적합하며 상당한 투자가 필요하다는 인식, 제로트러스트 아키텍처가 모든 규모의 조직에 적용될 수 있는 일련의 지침 원칙이라는 사실을 충분히 이해하지 못함 ▸ 제로트러스트 아키텍처가 환경 운영이나 최종 사용자 경험에 부정적인 영향을 미칠 수 있다는 우려 ▸ 전환 계획을 수립하기 위하여 필요한 정책, 시범 또는 개념 증명 구현을 개발할 자원이 부족함 ▸ 기존 투자를 활용하면서 제로트러스트 아키텍처로 전환하는 과정에서 현대화 추진과 우선순위를 균형있게 맞추는 문제 ▸ 관리자, 보안 인력, 운영자, 최종 사용자, 정책 결정권자에게 필요한 기술과 교육의 중요성에 대한 이해 부족
기본 요소 관점	▸ 비즈니스 애플리케이션, 자산, 보호해야 할 프로세스를 완전히 이해하기 위한 적절한 자산 목록 및 관리가 부족하며, 이러한 리소스의 중요성에 대한 명확한 이해가 없음 ▸ 특정 애플리케이션과 서비스에 대해 세밀하고 필요한 접근 정책을 적용하기 위한 조직 전반에 걸친 사용자 역할의 디지털 정의, 관리, 추적이 부족 ▸ 조직의 통신 및 사용 패턴에 대한 가시성이 부족하여 조직의 주체, 자산, 애플리케이션 및 서비스 간의 상호작용에 대한 이해가 제한적이며, 이를 식별하는데 필요한 데이터가 부족함 ▸ 조직의 공격 표면 전반에 대한 정보를 충분히 확보하지 못함
기술 관점	▸ 성숙도가 다양한 여러 상용 기술을 통합하고, 그 기능을 평가하며 기술 격차를 식별해 완전한 제로트러스트 아키텍처를 구축하는 과제 ▸ 보안 정책을 배포·관리·적용하는 데 필요한 표준화된 정책이 부족하여 조직이 단편적인 정책 환경이나 운용되지 않는 구성요소에 직면하는 문제 ▸ 커뮤니티와 조직 내에서 제로트러스트 아키텍처에 대한 공통된 이해와 용어가 부족하여 제로트러스트 성숙도를 측정하고, 비즈니스에 가장 적합한 제로트러스트 아키텍처 접근 방식 결정하며, 구현 계획을 수립하는 어려움 ▸ 모든 조직에 동일하게 적용할 수 있는 단일 제로트러스트 아키텍처는 존재하지 않으며, 조직별 요구사항, 위험 감수도, 기존 기술 및 환경에 맞춰 설계되고 통합되어야 함

나. 제로트러스트 아키텍처 배포 방식별 참조 아키텍처

1) EIG 초기(Crawl) 단계 및 EIG 실행(Run) 단계 참조 아키텍처

그림 S-12 EIG 초기 단계 참조 아키텍처



EIG 접근법은 주로 주체의 신원을 정책 생성의 핵심 구성요소로 사용하여 리소스에 대한 접근권한을 부여하며, 이외에도 기기의 보안 상태나 환경적 요인 또한 접근 허가에 영향을 미칠 수 있다. [그림 S-12]에서 볼 수 있듯이, ICAM을 통하여 PE와 PA 기능을 제공하며, 이는 기존의 ICAM 및 엔드포인트 보호 솔루션만으로 지원 가능한 제로트러스트 아키텍처 기능을 시연하려는 의도로 설계되었다.

EIG 실행 단계는 EIG 초기 단계 아키텍처를 기반으로 하며, PE와 PA 기능이 ICAM 제품에 의존하지 않는다. 실행 단계에서는 클라우드에 저장된 리소스 접근 보호 기능이 추가되었으며, 새로운 기기 탐지 시 모니터링 및 경고 수행 기능, 규정을 위반하는 기기 차단 등 초기 단계에서 제공되지 않은 추가 기능들이 포함된다.

2) 마이크로 세그멘테이션, SDP 및 SASE 참조 아키텍처

마이크로 세그멘테이션 배포 방식은 리소스를 고유한 네트워크 세그먼트에 배치하거나, 엔드포인트에 소프트웨어 에이전트 혹은 방화벽을 설치하여 호스트 기반 세그멘테이션을 구현하는 방식이다. SDP는 네트워크를 접근 결정 정책에 따라 재구성하며, 애플리케이션 계층에서는 소프트웨어 에이전트와 리소스 게이트웨이 간의 안전한 채널을 설정하여 동작한다. SASE는 SD-WAN, 보안 웹 게이트웨이, 차세대 방화벽, ZTNA와 같은 네트워크 및 보안 기능을 서비스 형태로 제공하여 원격 근무자, 온프레미스의 보안을 지원한다.

다. 제로트러스트 아키텍처 실증으로부터 발견한 점

1) EIG 초기 단계에서 발견한 점

EIG 초기 단계에서 두 가지 문제를 발견했다. 첫째, ICAM 솔루션을 PDP로 활용했으나, 많은 공급업체 솔루션들이 서로 즉시 통합되지 않아서 네트워크 수준의 PEP(라우터, 방화벽 등)는 ICAM과 통합되지 않았다. 다만, 신원 인식 네트워크 PEP는 ICAM과 통합될 수 있었으며, 엔드포인트 보호 솔루션은 MDM·UEM 솔루션과 통합되어 ICAM과 간접적으로 연동되었다. 둘째, 맞춤형 통합 대신 제공업체가 제공하는 기본 통합을 사용했지만, 이는 모든 제로트러스트 기능을 지원할 수 없었다.

빌드 E1B1, E3B1을 실증한 결과 리소스 관리를 지원하지 못하는 문제가 생겼다. 사용자 및 엔드포인트의 인증, 재인증, 상태 검증을 기반으로 접근 결정을 내렸으나, 리소스를 호스팅하는 엔드포인트의 신원이나 상태는 확인하지 않았다. 또한, 두 빌드 모두 리소스 관리 기능이나 네트워크 수준에서 엔드포인트의 네트워크 접근을 통제하는 기능을 지원하지 않았다. 향후 빌드에서는 이러한 리소스 관리 기능을 추가할 예정이다.

2) EIG 실행 단계에서 발견한 점

EIG 실행 단계를 통해 EIG 초기 단계와 비교하여 다음과 같은 추가 기능을 입증하였다.

- 정책에 따라 PEP가 리소스 저장 위치와 관계없이 요청 엔드포인트에서 리소스로 안전하고 직접 접근하는 터널을 구축

- 인증된 사용자가 내부 리소스에 접근하면서, 외부에서 리소스가 발견되거나 노출되지 않도록 보장하는 프록시 역할의 커넥터 사용
- 원격 사용자가 기업망을 경유하지 않고 클라우드에 호스팅된 리소스에 직접 접근할 수 있도록 보호하는 기능
- 클라우드 또는 인터넷 리소스로 전송되는 트래픽에 대해 정책 제어를 모니터링, 검사 및 시행하는 기능
- 네트워크에서 새로운 엔드포인트를 발견하고, 정책을 위반하는 엔드포인트를 차단하는 기능

3) 마이크로 세그멘테이션, SDP 및 SASE 단계에서 발견한 점

제로트러스트 아키텍처를 효과적으로 구현하려면 다양한 공급업체의 보안 제품을 통합하고, PDP가 여러 보안 도구 및 지원 구성요소와 연동되어 실시간으로 접근 요청의 위험을 평가할 수 있어야 한다. 제로트러스트 아키텍처에서 여러 PDP가 존재하는 것은 드문 일이 아니며, 각 PDP는 하나 이상의 다른 지원 요소 및 PEP와 통합될 수 있다. 이러한 구조적 특성으로, 제로트러스트 아키텍처의 전체적인 정책을 종합적으로 이해하고, 명확하게 표현하고, 관리하기 어려우며, 여러 PDP는 일반적으로 정보를 공유하기 위해 서로 통합되지 않기 때문에 어떤 사용자, 엔드포인트 또는 기타 주체가 위험을 초래할 수 있는지에 대한 공유된 이해가 없다. 여러 PDP가 존재하는 경우, 이들이 정보를 공유할 수 있는 통합 접근 방식을 통해 위험에 대한 공통의 통합된 이해를 공유하여 의사 결정을 내리는 것이 바람직하다.

SIEM 및 SOAR 시스템은 PDP가 접근 요청을 판단하는 데 필요한 중요 정보를 제공하며, 이러한 정보는 실시간으로 전달되어야 한다. 또한, 데이터 보안 도구와 통합하여 PDP가 데이터 보호를 위해 차단된 접근 요청을 인지할 수 있어야 한다.

단말의 규정 준수 여부를 감지하고, 비준수 단말의 리소스 접근을 차단하는 도구는 필수적이다. 이러한 도구는 자동으로 문제를 해결할 수 있는 솔루션과 결합되어 조직의 구성 및 패치 관리 시스템과 통합되어야 한다. 단말 관리 솔루션이 리소스도 관리할 수 있지만, 리소스 관리에 특화된 솔루션을 사용하는 것이 더욱 효과적이다.

라. 제로트러스트 여정의 핵심 교훈

NCCoE는 제로트러스트를 배포하고 구현하려는 조직을 위해 실제 연구실에서 구현한 실증 사례를 바탕으로 얻은 7가지의 핵심 교훈들을 공유한다.

1) 기존 환경을 식별하고 목록화할 것

기업이 제로트러스트 아키텍처를 도입하기 위한 첫 단계는 현재 IT 환경에 존재하는 모든 리소스(HW, SW, 애플리케이션, 데이터, 서비스)를 식별하고 목록화하는 것이다. 이를 위해 트래픽을 모니터링하여 어떤 리소스가 활성화되어 있고, 어떻게 접근되고 사용되는지 파악할 수 있는 도구를 배포하는 것이 필요하다.

이 과정은 제로트러스트 아키텍처의 보호 대상을 이해하는 데 필수적이다. 목록에서 누락된 리소스는 보호되지 못할 가능성이 크며, 이는 침해, 변경, 삭제, DDoS 및 기타 공격에 취약해질 수 있다. 따라서 온프레미스와 클라우드 환경을 포함한 모든 리소스를 포괄적으로 식별하고 지속적으로 관리하는 것이 중요하다.

2) 임무 및 비즈니스 사용 사례를 지원하기 위한 접근 정책 수립할 것

기존 환경과 자산을 식별한 후에는 각 리소스에 대한 접근권한을 규정하는 정책을 수립해야 한다. 이 정책은 최소 권한 원칙을 기반으로 하며, 리소스에 필요한 권한만 접근 주체에게 부여하도록 설계되어야 한다. 정책 수립 시에는 사용자 유형, 접근 요구사항, 기기 유형, 작업 위치, 시간대 등의 요소를 고려해야 한다.

기업은 처음부터 직원별로 필요한 리소스가 무엇인지 식별·이해하기가 어려울 수 있다. 이러한 경우, 트래픽 모니터링 도구를 활용하여 직원들의 리소스 접근 패턴을 분석한 후 이를 바탕으로 정책을 수립할 수 있다. 또한, 제로트러스트 아키텍처는 다양한 구성요소들로 이루어질 수 있기 때문에 접근 정책이 중앙 집중화되지 않고 여러 제품에 분산될 수 있다. 이러한 분산된 정책을 효과적으로 관리하기 위해서 조직은 접근 규칙뿐만 아니라 각 규칙이 설정된 위치도 명확하게 기록하여 정책의 일관성을 유지하는 것이 필요하다.

3) 기존 보안 기능 및 기술을 식별할 것

대부분의 조직은 이미 보안 솔루션을 갖춘 인프라와 기술 시스템을 갖추고 있기 때문에, 이를 제로트러스트 아키텍처에 통합할 필요가 있다. 기존 IT 장비나 보안 기능을 고려하여 기능을 식별 및 목록화하고, 이를 어떻게 제로트러스트 아키텍처에 통합할지 방식을 고려해야 한다.

조직은 기존 보안 구성요소들을 목록화한 뒤, 이러한 요소들이 제로트러스트 아키텍처 내에서 계속 활용될 수 있는지 검토해야 한다. 물론 기존 기술을 재활용하면 비용 절감의 효과는 있겠지만, 이를 성공적으로 통합하기 위해서는 호환성 문제를 해결해야 한다.

4) 데이터 중요도를 기반한 위험 기반 접근 방식을 적용하여 제로트러스트 정책 및 프로세스의 격차를 제거할 것

보안 기능을 목록화한 후에는 인프라를 어떻게 분할할지, 그리고 각 리소스를 얼마나 세분화할지를 고려하여 접근 보호 토폴로지[14]를 설계해야 한다. 이 토폴로지는 위험 기반 접근 방식을 사용하여 설계되며, 중요한 리소스는 독립된 공간에 격리하고, 중요도가 낮은 리소스는 공유 신뢰 영역에서 보호되도록 구성할 수 있다.

접근 보호 토폴로지를 설계할 때, 조직은 각 리소스를 보호할 PEP와 리소스 접근 결정을 내릴 기술을 결정해야 한다. 이전에는 경계 기반 보호에 의존하여 단일 PEP를 통해 모든 리소스를 보호하였으나, 제로트러스트 아키텍처를 도입하면서 인프라를 더 작은 신뢰 영역으로 분할하여 잠재적 침해 또는 공격의 영향을 최소화할 수 있다.

5) 제로트러스트 아키텍처 구성요소(사람, 프로세스, 기술)를 구현하고 배포된 보안 솔루션을 점진적으로 활용할 것

접근 보호 토폴리지 설계가 완료되면, 조직은 환경을 지속적으로 모니터링하는 도구를 배치하고 이를 통해 제로트러스트 아키텍처의 검증을 수행해야 한다. 제로트러스트 아키텍처 구현 초기 단계에서는 ID관리, 인증, 권한 부여가 중요한 요소로 인식되며, ICAM 솔루션과 통합할 수 있는 엔드포인트 보호 솔루션 또한 중요한 구성요소가 될 수 있다.

---

14 네트워크 혹은 시스템의 요소들을 물리적, 논리적으로 연결해 놓은 것

6) 제로트러스트 결과를 지원하는 구현 사항을 검증할 것

조직은 네트워크 트래픽을 실시간으로 모니터링하여 의심스러운 활동을 탐지하는 등 행동 분석을 통해 이상 활동을 감지해야 한다. 배포된 보안 도구를 활용하여 제로트러스트 아키텍처의 접근 정책이 올바르게 시행되고 있는지 지속적으로 검증해야 한다. 또한, 다양한 시나리오에 대해 주기적인 테스트를 수행하며, 제로트러스트 아키텍처의 새로운 기능을 배포하기 전에 검증할 수 있는 일련의 테스트 과정을 마련하는 것이 바람직하다.

7) 위협 환경, 임무, 기술 및 규정의 변화에 따라 지속적으로 개선하고 발전할 것

제로트러스트 아키텍처가 배포된 후에도, 제로트러스트 아키텍처는 변화하는 환경에 지속적으로 적응해야 한다. 제로트러스트 아키텍처에 사용된 기술 구성요소가 업그레이드되거나 폐기될 경우 새로운 기술로 교체해야 하며, 혁신적인 보안 기술이 등장할 때 기존 제로트러스트 아키텍처에 통합할 수 있는지 검토할 필요가 있다.

이상적인 제로트러스트 아키텍처는 알려진 위협이나 제로데이 공격과 같은 악성 공격을 감지할 수 있도록 행동 기반 모니터링을 수행해야 한다. 따라서, 위협 환경이 변화할 때마다 조직의 CISO 및 보안 팀은 제로트러스트 아키텍처의 토폴리지, 구성요소 및 정책을 지속적으로 평가하여 새로운 위협에 대처해야 한다.

2. 국방부 Thunderdome 프로젝트

가. Thunderdome 프로젝트 개요

미 국방부는 자체적으로 사용하고 있었던 네트워크 보안 아키텍처 JRSS(Joint Regional Security Stack)을 단계적으로 폐지하고, 그 대안으로 제로트러스트 아키텍처를 고려한 Thunderdome 프로젝트를 개시하였다. 이 프로젝트는 미 국방부가 사이버 보안 위협에 대응하기 위해 추진한 제로트러스트 아키텍처 구현 계획의 일환으로 시작되었으며, 국방정보시스템국(DISA)이 주도하여 개발되었다.

2022년 1월 DISA는 제로트러스트 비전을 충족시키기 위해 Booz Allen Hamilton과 680만 달러 규모의 계약을 체결하여 Thunderdome 프로토타입을 개시했다. Thunderdome 프로토타입은

실제 적용 가능한 솔루션을 테스트하고 검증하기 위해 개발된 시범 모델로, 주로 SASE 보안 프레임워크 내에서 제로트러스트 아키텍처를 구상했다. 2023년 3월, DISA는 Thunderdome 프로토타입 작업을 공식적으로 끝마쳤다고 발표했으며, DISA는 약 1,500명의 테스트 사용자를 통해 Thunderdome의 원격 및 온프레미스 기능을 사용하여 일상적인 업무를 수행했다고 밝혔다.

2024년 4월, DISA는 2024년내로 60개 사이트에 Thunderdome 프로그램을 출시할 예정이며, 지금까지 23개 사이트에 제로트러스트 프로그램을 배포 완료했다고 밝혔다. DISA의 배포 계획에는 미국 해안 경비대, 미국 남부 사령부 등을 포함하고 있으며, Thunderdome 프로젝트가 미국의 군사 기밀 시설에 긍정적인 영향을 줄 것으로 보인다.

나. Thunderdome 프로젝트를 진행하면서 직면한 어려움

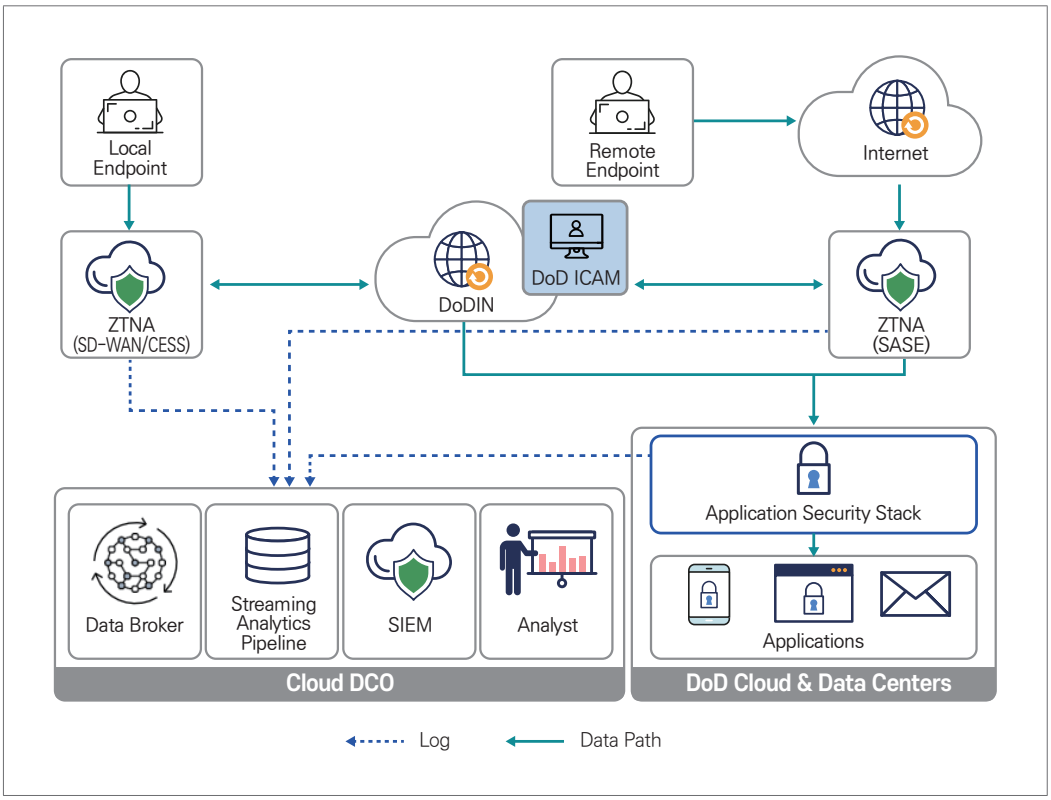
DISA는 Thunderdome 프로젝트를 진행하면서 겪은 어려움에 대해 다음과 같이 5가지를 제시하였다.

- 기존 국방부 네트워크 구조는 매우 가변적이고 복잡하여 제로트러스트 구현 및 전환에 많은 시간이 소요됨
- 기술을 구현하는 것은 쉽지만, 이를 뒷받침하는 조직의 문화·정책·절차의 변화는 장기적인 과제
- 다른 제로트러스트 관련 계획과의 상호 운용성이 필요
- 파생된 자격 증명을 활용한 모바일 사용자 접근 관리에 있어서 노력 필요
- 국방부 전역에서 단말 인증 솔루션이 부족함

다. Thunderdome 프로토타입 구성요소

DISA는 Thunderdome 프로토타입 구성요소를 다음과 같이 구성하였다.

그림 S-13 Thunderdome 프로젝트 논리적 구성요소



(출처: DISA)

① 지역·원격 엔드포인트

ZTNA를 통해 네트워크 및 애플리케이션에 연결하려는 원격(Remote) 또는 사내(Local) 사용자

② Zero Trust Network Access (SD-WAN/CESS, SASE)

ICAM에서 제공한 사용자 신원 및 엔드포인트 기기 상태를 기반으로 네트워크에 대한 조건부 접근을 구현

③ Application Security Stack (AppSS)

네트워크 및 애플리케이션 계층 기반 공격에 대한 마이크로 세그멘테이션, 침입 및 측면 이동 보호 기능을 제공하는 확장 가능한 보안 스택

④ Cloud Defense Cyber Operation (DCO)

AI를 활용하고 지속적인 가시성 및 위협 개선 기능을 제공하는 클라우드 기반 솔루션

다. Thunderdome 프로젝트 교훈

미 국방부의 사이버보안 및 분석 실장인 Brian Hermann은 2023년 4월 Thunderdome 프로젝트의 파일럿 단계 종료 후 국방부의 제로트러스트 구현에 관한 다음 계획을 논의하면서, Thunderdome 프로젝트 파일럿 단계로부터 얻은 교훈을 밝힌 바 있다. 여기에서는 기술적인 성공에 대한 언급과 함께, 한편으로는 정책적, 문화적 변화의 필요성도 있음을 소개하였다.

- 상용 기술의 효과적 통합: SASE와 SD-WAN 같은 상용 기술이 미 국방부의 기존 네트워크 인프라에 성공적으로 통합되었으며, 이를 통해 보안 성능 및 네트워크 성능이 개선되었으며, 상용 솔루션이 국방부 수준의 보안 요구 사항을 충족할 수 있음을 확인
- 조건부 접근 및 보안 강화: 사용자의 속성(위치, 장치 유형, 시간 등)에 따라 접근을 제어하는 조건부 접근 개념을 도입함으로써, 필요한 경우에만 적절한 권한을 부여할 수 있었음. 이를 통해 불필요한 접근을 방지하고, 데이터 보호 수준을 강화할 수 있었음.
- 단순화 및 자동화: Thunderdome 프로젝트는 네트워크 관리의 복잡성을 줄이기 위해 보안 정책을 자동화함으로써, 정책을 한 번 설정하면 모든 장치에 일관되게 적용되어, 관리의 효율성과 보안의 일관성 향상
- 실제 사용자와의 성능 검증: 1,500명의 테스트 사용자가 다양한 위치에서 Thunderdome 시스템을 사용해보는 실험을 통해, 보안 강화 외에도 네트워크 성능이 개선됨을 확인함으로써 원격 사용자와 온프레미스 사용자 모두에게 성능상의 이점 제공
- 문화적 및 정책적 변화의 필요성: 기술적 도입 외에도 조직 문화와 정책의 변화가 필수적으로, 제로트러스트의 원칙을 완전히 실현하기 위해서는 기술적 프로젝트에 그치지 않고, 모든 부문에서 정책과 절차가 변경되고 제로트러스트 철학을 수용해야 함을 알게 됨
- 확장성: Thunderdome 파일럿 단계는 미 국방부의 다양한 환경, 특히 기밀 네트워크까지도 제로트러스트 아키텍처로 확장 가능함을 보여주었으며, 향후 더 넓은 범위 적용을 위한 기반 마련

| 제5절 |

성숙도 모델 개념

1. 성숙도 모델 개요

최초 성숙도에 대한 개념은 1930년대 품질 관리에서 출발하였으나, 현재의 성숙도 모델과 공통점을 가지고 있지 않다. 1979년 Crosby는 분석 및 측정을 위한 단순하지만 효과적인 도구를 제공하는 성숙도 단계의 개념을 소개하였으며, 여기에서 5가지 성숙도 단계와 6가지 측정 분류 기준에 따라 모범 사례를 분류하는 품질 관리 절차 성숙도 기준을 제안한 바 있다.

이후, 미 국방부는 카네기 멜론 대학에 자금을 지원하여 소프트웨어 엔지니어링 연구소(SEI, Software Engineering Institute)를 설립하였으며, SEI는 1993년 소프트웨어 역량 성숙도 모델(Capability Maturity Model for Software, SW-CMM) v1.1을 개발하여 기술 보고서 형태로 공개한 바 있다. SW-CMM v1.1에서는 소프트웨어 프로세스 성숙도의 기본 원칙을 설명하고, 소프트웨어 조직이 소프트웨어 프로세스의 성숙도를 개선하기 위한 지침으로 활용할 수 있도록 구성하였다.

미 국방부가 SEI를 통해 소프트웨어 기능 성숙도 모델을 개발한 것은 당시 많은 조직들이 프로젝트가 늦어지거나 예산을 초과하는 사례를 통하여 조직 차원에서 소프트웨어 프로세스 관리에 대한 필요성을 파악하였기 때문으로 보인다.

미성숙한 조직에서의 소프트웨어 프로세스는 실무자와 경영진에 의해 즉흥적으로 만들어지는 경우가 많고, 혹은 이미 지정된 프로세스가 있다 하더라도 엄격하게 준수·시행되지 않아 당장 직면한 위기를 해결하는데 급급한 경향을 보인다. 그러나 성숙된 조직에서는 소프트웨어 개발 및 유지 관리 프로세스를 관리할 수 있는 조직 차원에서의 역량을 갖추고 있으며, 계획된 프로세스에 따라 업무 활동이 수행되고 역할과 책임이 조직 전체에 걸쳐 명확하다. 이러한 관점에서, 일반적인

조직들이 성숙도가 높은 조직으로 진화하는데 참조할 수 있도록 소프트웨어 프로세스 성숙도 프레임워크를 개발한 것이 SW-CMM으로 볼 수 있다.

SW-CMM에서는 소프트웨어 프로세스 성숙도 수준을 총 5단계로 구분하였으며, 〈표 S-18〉에서는 각 수준별 특징 및 각 단계에 대한 설명을 소개한다.

표 S-18 SW-CMM에서의 소프트웨어 프로세스 성숙도 수준

성숙도 수준	수준별 특징	수준에 대한 설명
초기 (Initial)	▸ 소프트웨어 프로세스는 즉흥적이고 혼란스럽다는 특징이 있음 ▸ 정의된 프로세스는 거의 없으며 성공 여부는 개인의 노력에 달려 있음	▸ 즉흥적이고 심지어 혼란스러운 대신, 예산과 일정을 초과하더라도 제대로 작동하는 제품을 개발하는 경우가 많음 ▸ 초기 단계 조직에서의 성공은 조직 구성원들의 역량과 영웅심에 달려 있음 ▸ 유능한 인재를 선발, 채용, 개발, 유지하는 것은 모든 성숙도 수준의 조직에서 중요한 문제이지만 대부분 CMM의 범위가 아님
반복 가능 (Repeatable)	▸ 비용, 일정, 기능 추적을 위한 기본 프로젝트 관리 프로세스가 확립되어 있음 ▸ 유사한 애플리케이션 분야를 가진 프로젝트에서 이전 성공 반복을 위해 필요한 프로세스 규정 존재	▸ 프로젝트의 규모와 복잡성이 커지면서 기술적 문제에서 성숙도의 초점인 조직 및 관리 문제로 관심 이동 ▸ 최고의 직원이 배운 교훈을 문서화된 프로세스에 통합하고, 이러한 프로세스를 효과적으로 수행하는 데 필요한 기술을 구축하며(보통 교육을 통해), 업무를 수행하는 사람들로부터 학습하여 지속적으로 개선 ▸ 반복 가능 단계 조직은 프로젝트가 적절한 관리 프로세스를 수립하도록 안내하는 정책 보유 ▸ 정의 단계 조직은 전체 소프트웨어 프로세스를 정의, 통합 및 문서화함으로써 프로젝트 관리 기반 구축 (통합이란, 한 작업의 결과물이 다음 작업의 입력으로 원활하게 이루어짐을 의미) ▸ 또한, 지나치게 경직되지 않고, 업무 수행자에게 권한을 부여하는 프로세스 구축
정의 (Defined)	▸ 관리 및 엔지니어링 활동 모두에 대한 소프트웨어 프로세스는 문서화, 표준화 및 조직 표준 소프트웨어 프로세스에 통합되어 있음 ▸ 모든 프로젝트는 소프트웨어 개발 및 유지 관리를 위해 조직의 표준 소프트웨어 프로세스의 승인된 맞춤형 버전을 사용	
관리 (Managed)	▸ 소프트웨어 프로세스 및 제품 품질에 대한 자세한 측정값 수집 ▸ 소프트웨어 프로세스와 제품 모두 정량적으로 이해·제어됨	▸ 품질 결함으로 인한 재작업 발생 사례를 품질 개선에 활용 ▸ 관리 단계의 초점은 프로세서를 제어하는 것으로, 프로세스는 이미 안정적으로 작동하고 있어 예외적인 상황이 발생할 경우 '특별한 원인'을 파악하여 해결 ▸ 최적 단계의 초점은 프로세스를 지속적으로 개선하는 것으로, 만성적인 품질 결함을 줄이는 새로운 기준선을 설정하여 '비효율의 공통 원인'을 파악하여 프로세스 개선 ▸ 최고 성숙도에 도달한 조직은 예측 가능한 비용과 스케줄 내에서 매우 안정적인 소프트웨어 생산 프로세스를 갖추게 됨
최적 (Optimizing)	▸ 프로세스로부터의 정량적 피드백과 혁신적인 아이디어와 기술의 시범 운영을 통해 지속적인 프로세스 개선 가능	

이후, 소프트웨어 엔지니어링 역량 성숙도 모델(SE-CMM, Software Engineering Capability Maturity Model), 통합 제품 개발 역량 성숙도 모델(IPD-CMM, Integrated Product Development Capability Maturity Model) 등이 등장한 후, SEI는 SW-CMM와 이들을 통합하여 다양한 분야에 확장할 수 있는 프레임워크로서 역량 성숙도 모델 통합(CMMI, Capability Maturity Model Integration)을 제안하였다. 최초에 제안된 CMMI는 개발용 CMMI(CMMI for Development, CMMI-DEV), 조달용 CMMI(CMMI for Acquisition, CMMI-ACQ), 서비스용 CMMI(CMMI for Services, CMMI-SVC) 등으로 구성되었으나, 버전 2.0부터는 통합되어 제공되고 있으며 2023년 4월 버전 3.0이 공개된 바 있다. 2013년 이후 CMMI에 대한 관리가 카네기 멜론에서 신설한 CMMI Institute로 이관되었다.

CMMI에서의 성숙도 수준은 SW-CMM와 유사하게 5단계로 정의되어 있으며, 수준별 특징은 다음과 같다.

- 초기 (Initial): 예측할 수 없고, 제대로 제어되지 않으며 반응성이 떨어지는 프로세스 (표준화나 문서화가 거의 이루어지지 않음)
- 기초적 관리 (Managed): 프로젝트에 특화되고, 가끔 반응성이 있는 프로세스 (프로세스가 기본적으로 관리되지만, 표준화나 문서화 부족)
- 정의 (Defined): 조직에 특화되고, 가끔 사전 예방적인 프로세스 (표준화 및 문서화된 프로세스)
- 정량적 관리 (Quantitatively Managed): 정량적으로 측정되고 제어되는 프로세스 (조직은 프로세스의 변동성과 성과를 명확히 이해)
- 최적화 (Optimizing): 프로세스 개선에 집중 (환경 변화에 신속하게 적응하고 프로세스의 효율성을 극대화)

조직 차원에서 어떤 분야(예, 소프트웨어, 보안 등)의 성숙도 모델을 고려하는 경우, 성숙도 모델은 조직의 현재 위치를 파악하고 다음 단계로 발전하기 위한 구체적인 목표와 계획을 세울 수 있도록 도와주며, 프로세스를 개선할 수 있는 기회를 제공한다. 또한, 성과를 정량적으로 측정하고 관리할 수 있는 기준과 함께 조직 차원에서의 일관된 프로세스를 도입할 수 있도록 함으로써 경쟁력을 강화하고 위험을 관리할 수 있는 장점을 누리게 된다.

다만, 조직이 추구하는 목표보다 성숙도 모델을 우선하는 경우, 형식에 매몰되어 상당한 도입 비용과 시간이 소요되고 유연성이 부족한 조직이 될 수 있으므로 성숙도 모델을 지나치게 맹신하지 않도록 유의하여야 한다.

2. 보안 성숙도 모델

앞서 제안된 성숙도 모델이 지속적으로 연구되면서, 조직이 수립한 보안 아키텍처 관점에서도 다음과 같은 다양한 형태의 성숙도 모델이 제안된 바 있다.

- 사이버보안 기능 성숙도 모델 통합(CMMI for Cybersecurity): CMMI Institute이 제안한 성숙도 모델로, 조직의 사이버 보안 성숙도를 평가하고 개선하는데 중점을 두며, 사이버 보안 리스크를 관리하고 지속적으로 보안 능력을 향상시키는데 필요한 프로세스 개선을 지원하고자 만들어졌다. 총 7가지 카테고리(거버넌스 프레임워크 보장, 위험 관리 절차 수립, 위험 식별 및 관리, 위험 완화 보장, 위험 탐지 보장, 위험 대응 보장, 사이버 복원력 보장), 22개의 역량 영역(Capability Area)에 대하여 하위 활동(Activity)을 두어, 각 Activity 별로 총 5단계의 성숙도 수준을 두고 개별 활동에 대한 성숙도를 평가하는 방식을 취한다.
- 성숙도 모델 보안성 구축(Building Security In Maturity Model, BSIMM) Version 7: 소프트웨어 보안 프레임워크를 정의하는 문서로, 거버넌스(Governance), 인텔리전스(Intelligence), SSDL, 배포(Deployment) 도메인에 대해 12개 사례에 대한 113개의 활동(Activity)를 정의하고 각 Activity에 대응하는 성숙도 수준을 정의함으로써 어떤 Activity를 수행하였는가를 바탕으로 조직의 소프트웨어 보안 성숙도 평가가 가능하다.
- 사이버 보안 역량 성숙도 모델(Cybersecurity Capability Maturity Model, C2M2) Version 2.1: 미국 에너지부(DoE)에서 개발한 모델로, 특히 에너지 부문에서의 사이버 보안 성숙도를 평가하기 위해 설계되었으며. 자산, 변화 및 설정 관리, 위협 및 취약성 관리, 위험 관리, 식별자 및 접근 관리, 상황 인식, 이벤트 및 사고 대응, 운영의 지속성, 제3자 위험 관리, 직원 관리, 사이버보안 구조, 사이버보안 프로그램 관리 등 총 10개의 도메인에 대해 세부 사례별 4단계의 성숙도 지표 수준(Maturity Indicator Level)을 두고 평가할 수 있다.

이 외에도, OWASP의 소프트웨어 보증 성숙도 모델(Software Assurance Maturity Model, SAMM), ISF의 정보보호 성숙도 모델(Information Security Maturity Model, ISMM), The

Open Group의 공개 정보보호 관리 성숙도 모델(Open Information Security Management Maturity Model, O-ISM3) Version 2.0, ISO/IEC 21827:2008 시스템 보안 엔지니어링 - 역량 성숙도 모델(Systems Security Engineering - Capability Maturity Model, SSE-CMM) 등 다수의 보안 관련 성숙도 모델이 존재한다.

이러한 보안 관련 성숙도 모델들은 기업과 같은 조직에 대한 보안 성숙도 수준을 평가할 수 있는 방법론을 제공하고 있으며, 이를 통하여 해당 조직은 보안 성숙도 모델을 통하여 조직의 사이버 보안 능력을 더 정확하게 평가하고 유연하게 대응할 수 있는 능력을 향상 시킬 수 있다. 그 외에도 다음과 같은 목적을 달성할 수 있을 것이다.

- 조직의 현재 보안 역량에 대한 객관적 평가
- 조직이 당면한 사이버 보안 위험을 효과적으로 관리할 수 있는 체계적 접근 방법 제공 (위험 식별, 분석, 평가 및 대응 전략 개발)
- 조직이 지속적으로 보안 관리 프로세스를 개선할 수 있는 로드맵 제시
- 보안 투자 시 우선순위 결정에 도움
- 법·규제 요구 사항과 규정을 준수할 수 있도록 도움
- 보안 관련 정보를 조직 내부에서 혹은 외부와 효과적으로 소통하는데 활용 가능

보안 아키텍처를 구축하여 운영 중인 기존 조직들은 각 조직이 속한 영역, 조직의 특성 혹은 보안 수준을 달성할 수 있는 역량 등을 고려하여야 하며, 제로트러스트와 같은 새로운 보안 철학 혹은 기존에 없던 보안 요구 사항이 등장할 경우 보안 성숙도 모델을 구체화하고 지속적으로 개선해야 한다. 개선 과정에서 다양한 참조 모델 분석과 체계적인 문헌 검토를 통하여 새로운 성숙도 모델을 도출할 수 있을 것이다. 이렇게 새로운 성숙도 모델을 도출하면 조직의 보안 상황을 보다 정확하게 평가할 수 있으며, 관리자는 다양한 영역에서 의사결정 프로세스를 개선할 수 있을 것으로 기대할 수 있다.

| 제6절 |

ISMS-P 인증기준과 제로트러스트 성숙도 모델 연계

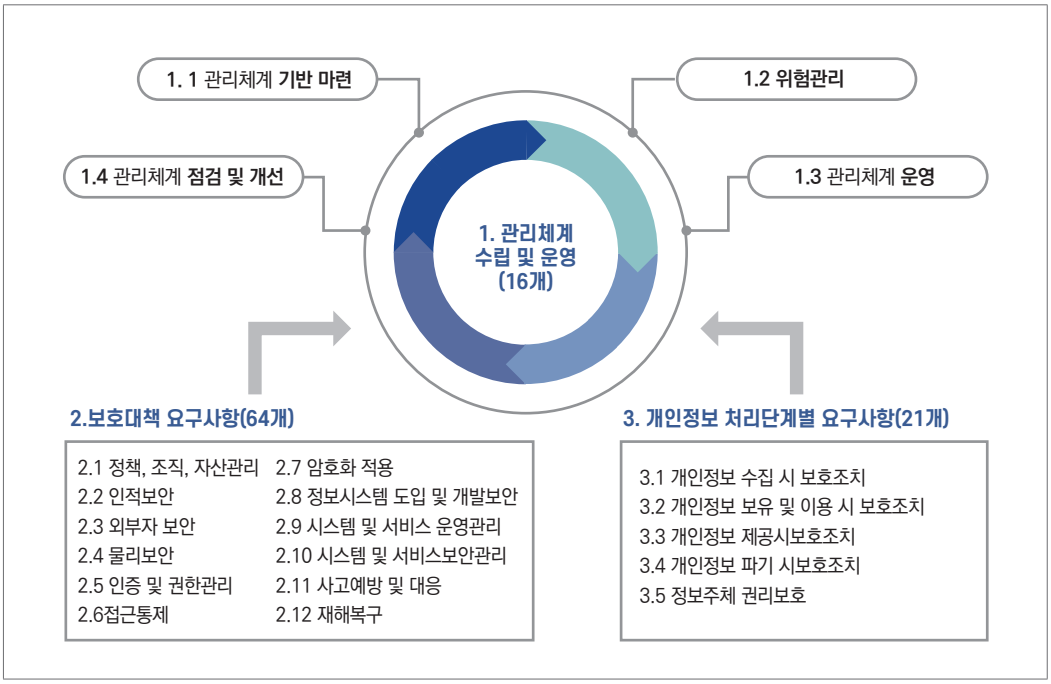
현재 국내에서 가장 널리 알려져 있고 매년 지속적으로 확대 적용되고 있는 보안 인증제도로는 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도가 있다. ISMS-P 인증제도는 정보통신망의 안정성 확보 및 개인정보보호를 위해 기업이 수립한 일련의 조치와 활동이 인증기준에 적합하는지를 인증하는 제도로, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 함) 제47조(정보보호 관리체계의 인증)와「개인정보 보호법」 32조의2(개인정보 보호 인증), 동 법 시행령 및 고시 등을 법적 근거로 한다.

ISMS-P 인증기준[15]은 '1. 관리체계 수립 및 운영(16개)', '2. 보호대책 요구사항(64개)', '3. 개인정보 처리단계별 요구사항(21개)'으로 구성되어 있다. 이 중 '1. 관리체계 수립 및 운영'은 전반적인 관리체계 운영 라이프사이클을 구성하며, '2. 보호대책 요구사항'은 총 12개 분야에 대한 인증기준으로, 정책, 조직, 자산, 교육 등 관리적 부문과 개발, 접근통제, 운영·보안관리 등 물리적·기술적 부문의 보호대책에 관한 사항을 포함한다. '3. 개인정보 처리 단계별 요구사항'은 개인정보 생명주기에 따른 보호조치 사항으로 구성된다.

기업은 ISMS-P 인증기준을 통해 체계적이고 종합적인 정보보호 및 개인정보보호 관리체계를 구현함으로써 일회성 정보보호 대책에서 벗어나 정보보호 및 개인정보보호 관리수준을 향상시킬 수 있다. 관리적·기술적·물리적·개인정보 생명주기로 구성된 인증기준의 준수는 해킹, DDoS 등의 침해사고와 개인정보 유출사고 발생 시 신속하게 대응할 수 있는 관리체계를 구축·운영하고 있음을 의미한다.

15 2023년 11월 기준

그림 S-14 ISMS-P 인증기준



제로트러스트 성숙도 모델은 앞서 2장에서 언급한 바와 같이 기업의 보안 시스템이 제로트러스트 원칙에 얼마나 성숙하게 대응하고 있는지 객관적으로 평가할 수 있는 수단을 제시하는 것으로, 기업이 ISMS-P 인증기준에 따른 요구사항을 만족하거나 고도화함으로써 제로트러스트 아키텍처를 도입하고 성숙도를 높이는 계기가 될 수 있다.

예를 들어, 제로트러스트 성숙도 모델에 따르는 보안 세부역량으로 '사용자 인벤토리'가 있다. 이는 시스템에 접근하는 모든 사용자와 권한에 대해 관리하고, 정확하고 최신 정보를 제공함으로써 적절한 접근제어를 가능하게 해주는 기능을 요구하고 있으며, 성숙도 수준 관점에서 단순히 사용자 목록을 수집하고 기록하는 '기존' 수준, 사용자의 역할과 권한을 포함하는 상세 인벤토리를 구축하고 주기적인 검토와 업데이트 절차를 설정하는 '초기' 수준, 자동화된 인벤토리 관리 도구 도입을 통하여 사용자 데이터의 정확성을 보장하는 '향상' 수준, 기업 전반의 사용자 및 권한 관리 최적화가 가능한 '최적화' 수준 등을 통해 보안 수준을 지속적으로 끌어올릴 수 있다. 이러한 포괄적인 사용자 인벤토리 세부역량은 ISMS-P 인증기준의 '2.5.1 사용자 계정 관리', '2.5.2 사용자 식별', '2.5.6 접근권한 검토' 등과 연계할 수 있다.

또한, 사용자 인벤토리의 세부 기능을 강화하는 과정에서, 비정상적인 사용자 활동 탐지 기능이 추가된 '향상' 수준, 인공지능 기반 분석을 통한 사용자 행동 예측 및 대응 전략을 강화하는 '최적화' 수준 등 보안 수준을 끌어올릴 수 있을 것이다. ISMS-P 인증기준의 '2.11.3 이상행위 분석 및 모니터링'에서는 침해시도 탐지를 위한 로그 등 수집·분석·모니터링 등을 언급하고 있으며, 이를 위해 상기 성숙도 수준으로의 진화를 통하여 기업망 내부에서 사용자 계정 중심의 활동 관련 정보를 생성·분석할 수 있을 것이다.

위의 예시와 같이, 기업은 기업 내 중요 디지털 자산을 보호하는데 있어 제로트러스트 성숙도를 높이는 과정에서 자연스럽게 ISMS-P의 인증기준도 만족할 수 있다. 또한 ISMS-P 인증을 취득한 기업도 제로트러스트를 도입하여 운영하는 경우, 보안 세부역량과 연계하여 연관된 인증기준 점검을 통해 안전하고 지속적인 정보보호 관리체계를 구축·운영할 수 있을 것으로 보인다. 이는 인증기준 준수와 함께 보안 성숙도 개선이라는 두 가지 목표를 동시에 달성할 수 있는 장점을 가지게 될 것으로 기대된다.

앞서 예시로 언급한 것과 같이, 3.2절의 보안 세부역량에 대해 연계하여 고려할 수 있는 ISMS-P 인증기준을 정리하면 〈표 S-19〉와 같다.

표 S-19 제로트러스트 세부역량과 ISMS-P 인증기준 연계

핵심 요소	세부역량	ISMS-P 인증기준 연계
식별자·신원	사용자 인벤토리	2.5.1 사용자 계정 관리, 2.5.2 사용자 식별, 2.5.6 접근권한 검토, 2.11.3 이상행위 분석 및 모니터링
	ID 연계 및 사용자 자격 증명	2.5.1 사용자 계정 관리, 2.5.2 사용자 식별, 2.5.3 사용자 인증, 2.5.5 특수 계정 및 권한관리
	다중 인증	2.5.3 사용자 인증, 2.5.4 비밀번호 관리, 2.11.3 이상행위 분석 및 모니터링
	지속 인증	2.5.3 사용자 인증, 2.5.4 비밀번호 관리, 2.6.2 정보시스템 접근, 2.11.3 이상행위 분석 및 모니터링
	통합 ICAM 플랫폼	1.1.5 정책 수립, 2.1.1 정책의 유지관리, 2.5.1 사용자 계정 관리, 2.5.3 사용자 인증, 2.5.6 접근권한 검토, 2.6.2 정보시스템 접근, 2.11.3 이상행위 분석 및 모니터링
	행동, 컨텍스트 기반 ID 및 생체 인식	2.5.3 사용자 인증, 2.5.4 비밀번호 관리, 2.11.3 이상행위 분석 및 모니터링
	조건부 사용자 접근	1.1.5 정책 수립, 2.1.1 정책의 유지관리, 2.5.1 사용자 계정 관리, 2.5.6 접근권한 검토, 2.11.3 이상행위 분석 및 모니터링
	최소 권한 접근	2.5.5 특수 계정 및 권한관리, 2.5.6 접근권한 검토, 2.11.3 이상행위 분석 및 모니터링

핵심 요소	세부역량	ISMS-P 인증기준 연계
기기 및 엔드포인트	기기 감지 및 규정 준수	1.1.5 정책 수립, 1.2.1 정보자산 식별, 2.1.1 정책의 유지관리, 2.5.6 접근권한 검토, 2.11.3 이상행위 분석 및 모니터링
	실시간 검사를 통한 기기 권한 부여	1.1.5 정책 수립, 1.2.1 정보자산 식별, 2.5.6 접근권한 검토, 2.8.1 보안 요구사항 정의, 2.8.2 보안 요구사항 검토 및 시험, 2.11.3 이상행위 분석 및 모니터링
	기기 인벤토리	1.1.5 정책 수립, 1.2.1 정보자산 식별, 2.1.3 정보자산 관리, 2.9.4 로그 및 접속기록 관리, 2.11.2 취약점 점검 및 조치, 2.11.3 이상행위 분석 및 모니터링
	통합 엔드포인트 관리 및 모바일 기기 관리	1.1.5 정책 수립, 2.1.1 정책의 유지관리, 2.1.3 정보자산 관리, 2.10.1 보안시스템 운영, 2.10.8 패치관리, 2.11.1 사고 예방 및 대응체계 구축, 2.11.3 이상행위 분석 및 모니터링
	엔드포인트 및 확장된 탐지·대응 (EDR 및 XDR)	1.1.5 정책 수립, 2.10.6 업무용 단말기기 보안, 2.10.1 보안시스템 운영 2.11.1 사고 예방 및 대응체계 구축, 2.11.3 이상행위 분석 및 모니터링
	자산, 취약성 및 패치 관리 자동화	1.2.1 정보자산 식별, 2.10.8 패치관리, 2.11.2 취약점 점검 및 조치, 2.11.3 이상행위 분석 및 모니터링
네트워크	매크로 세그멘테이션	2.6.1 네트워크 접근, 2.10.1 보안시스템 운영, 2.10.2 클라우드 보안, 2.11.1 사고 예방 및 대응체계 구축, 2.11.3 이상행위 분석 및 모니터링
	마이크로 세그멘테이션	1.1.5 정책 수립, 2.6.1 네트워크 접근, 2.6.3 응용프로그램 접근, 2.10.1 보안시스템 운영, 2.10.2 클라우드 보안, 2.11.1 사고 예방 및 대응체계 구축, 2.11.3 이상행위 분석 및 모니터링
	소프트웨어 정의 네트워킹	1.1.5 정책 수립, 2.1.1 정책의 유지관리, 2.6.1 네트워크 접근, 2.11.3 이상행위 분석 및 모니터링
	위협 대응	2.6.1 네트워크 접근, 2.11.1 사고 예방 및 대응체계 구축, 2.11.3 이상행위 분석 및 모니터링
	트래픽 암호화	1.1.5 정책 수립, 2.7.1 암호정책 적용, 2.7.2 암호키 관리
	데이터 흐름 매핑	1.3.1 보호대책 구현, 2.6.1 네트워크 접근, 2.6.3 응용프로그램 접근, 2.7.1 암호정책 적용, 2.11.3 이상행위 분석 및 모니터링
	네트워크 회복성	2.6.1 네트워크 접근, 2.9.2 성능 및 장애관리, 2.9.3 백업 및 복구관리, 2.12.1 재해·재난 대비 안전조치, 2.12.2 재해 복구 시험 및 개선,
시스템	접근통제	2.5.1 사용자 계정 관리, 2.5.5 특수 계정 및 권한관리, 2.5.6 접근권한 검토, 2.6.2 정보시스템 접근, 2.11.3 이상행위 분석 및 모니터링
	PAM	2.5.3 사용자 인증, 2.5.5 특수 계정 및 권한관리, 2.5.6 접근권한 검토, 2.11.3 이상행위 분석 및 모니터링
	자격 증명 관리	2.1.1 정책의 유지관리, 2.5.3 사용자 인증, 2.5.5 특수 계정 및 권한관리, 2.11.3 이상행위 분석 및 모니터링
	네트워크 세분화 및 그룹 간 이동	2.1.1 정책의 유지관리, 2.5.3 사용자 인증, 2.6.1 네트워크 접근, 2.11.3 이상행위 분석 및 모니터링
	시스템 환경에 따른 정책 관리	1.1.5 정책 수립, 2.1.1 정책의 유지관리, 2.10.2 클라우드 보안

핵심 요소	세부역량	ISMS-P 인증기준 연계
애플리케이션 및 워크로드	리소스 권한 부여 및 통합	2.5.3 사용자 인증, 2.5.5 특수 계정 및 권한관리, 2.5.6 접근권한 검토, 2.10.1 보안시스템 운영, 2.11.3 이상행위 분석 및 모니터링
	지속적인 모니터링 및 진행 중인 승인	2.1.3 정보자산 관리, 2.5.5 특수 계정 및 권한관리, 2.6.2 정보시스템 접근, 2.6.3 응용프로그램 접근
	원격 접속	2.1.1 정책의 유지관리, 2.6.6 원격접근 통제
	안전한 애플리케이션 배포	2.1.1 정책의 유지관리, 2.1.3 정보자산 관리, 2.8.2 보안 요구사항 검토 및 시험, 2.8.3 시험과 운영 환경 분리, 2.8.6 운영환경 이관, 2.9.1 변경관리, 2.11.2 취약점 점검 및 조치
	애플리케이션 인벤토리	1.1.5 정책 수립, 1.2.1 정보자산 식별, 2.1.3 정보자산 관리, 2.6.3 응용프로그램 접근, 2.9.4 로그 및 접속기록 관리, 2.11.2 취약점 점검 및 조치, 2.11.3 이상행위 분석 및 모니터링
	보안 소프트웨어 개발 및 통합	2.1.1 정책의 유지관리, 2.9.1 변경관리, 2.9.4 로그 및 접속기록 관리, 2.11.1 사고 예방 및 대응체계 구축, 2.11.3 이상행위 분석 및 모니터링
	소프트웨어 위험 관리	1.2.3 위험 평가, 1.2.4 보호대책 선정, 1.3.1 보호대책 구현, 2.2.2 직무 분리, 2.8.1 보안 요구사항 정의, 2.8.2 보안 요구사항 검토 및 시험, 2.8.3 시험과 운영 환경 분리, 2.11.1 사고 예방 및 대응체계 구축
데이터	데이터 카탈로그 위험 정렬	1.1.5 정책 수립, 1.2.1 정보자산 식별, 1.2.3 위험 평가, 1.4.2 관리체계 점검, 2.1.1 정책의 유지관리, 2.1.3 정보자산 관리, 2.11.3 이상행위 분석 및 모니터링
	기업 데이터 거버넌스	1.1.5 정책 수립, 2.1.1 정책의 유지관리
	데이터 접근제어	1.1.5 정책 수립, 2.5.5 특수 계정 및 권한관리, 2.5.6 접근권한 검토, 2.10.1 보안시스템 운영
	데이터 암호화 및 권한 관리	1.1.5 정책 수립, 2.7.1 암호정책 적용
	데이터 라벨링 및 태그 지정	1.1.5 정책 수립, 1.2.1 정보자산 식별, 2.1.3 정보자산 관리
	데이터 손실 방지 (DLP)	2.1.1 정책의 유지관리, 2.5.5 특수 계정 및 권한관리, 2.10.1 보안시스템 운영, 2.11.3 이상행위 분석 및 모니터링
	데이터 모니터링 및 감지	2.1.1 정책의 유지관리, 2.5.5 특수 계정 및 권한관리, 2.10.1 보안시스템 운영, 2.11.1 사고 예방 및 대응체계 구축, 2.11.3 이상행위 분석 및 모니터링

핵심 요소	세부역량	ISMS-P 인증기준 연계
가시성 및 분석	모든 관련 활동 기록	2.1.1 정책의 유지관리, 2.9.4 로그 및 접속기록 관리, 2.9.5 로그 및 접속기록 점검
	중앙집중적 보안 정보 및 이벤트 관리	2.1.1 정책의 유지관리, 2.9.4 로그 및 접속기록 관리, 2.9.5 로그 및 접속기록 점검
	보안 위협 분석	2.9.4 로그 및 접속기록 관리, 2.11.2 취약점 점검 및 조치, 2.11.3 이상행위 분석 및 모니터링
	사용자 및 기기 동작 분석	2.5.5 특수 계정 및 권한관리, 2.9.4 로그 및 접속기록 관리, 2.9.5 로그 및 접속기록 점검, 2.11.3 이상행위 분석 및 모니터링
	위협 인텔리전스 통합	2.10.1 보안시스템 운영, 2.10.5 정보전송 보안
	자동화된 동적 정책	2.1.1 정책의 유지관리, 2.10.1 보안시스템 운영
자동화 및 통합	정책 통합	1.1.5 정책 수립, 2.1.1 정책의 유지관리
	중요 프로세스 자동화	1.3.1 보호대책 구현, 2.9.3 백업 및 복구관리, 2.10.1 보안시스템 운영, 2.11.1 사고 예방 및 대응체계 구축
	인공지능	2.9.4 로그 및 접속기록 관리, 2.9.5 로그 및 접속기록 점검, 2.10.1 보안시스템 운영, 2.11.3 이상행위 분석 및 모니터링
	보안 통합, 자동화 및 대응	2.10.1 보안시스템 운영, 2.11.1 사고 예방 및 대응체계 구축
	데이터 교환 표준화	2.1.3 정보자산 관리, 2.10.1 보안시스템 운영 2.10.5 정보전송 보안, 2.11.3 이상행위 분석 및 모니터링
	보안 운영 조정 및 사고 대응	1.3.2 보호대책 공유, 2.11.1 사고 예방 및 대응체계 구축, 2.11.3 이상행위 분석 및 모니터링, 2.11.5 사고 대응 및 복구

| 제7절 |

참고 문헌

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

[2] CSA, “SDP Specification 1.0”, 2014.04

[3] Chase Cunningham (Forrester), “The Zero Trust eXtended (ZTX) Ecosystem – Extending Zero Trust Security Across Your Digital Business”, 2018.01

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

[5] 금융보안원, “금융보안 거버넌스 가이드 Ver 3.0”, 2019.12

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

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

[8] 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

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

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

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

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

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

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

[15] OMB, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”, 2022.01

[16] NSTAC, “Draft Report to the President - Zero Trust and Trusted Identity Management”, 2022.02

[17] Jaspreet Gill, “Booz Allen Hamilton nabs $6.8M Thunderdome prototype contract”, BREAKING DEFENSE, 2022.02

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

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

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

[21] Katherine MacPhail, “Thunderdome is DISA’s ‘Trial-By-Fire’ Answer to Zero Trust Architecture”, GovCIO, 2022.04

[22] 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

[23] DoD, “DoD Zero Trust Strategy”, 2022.11

[24] DoD, “DoD Zero Trust Capability Execution Roadmap (COA 1)”, 2022.11

[25] Julian Breyer, “Thunderdome : A Year In Review”, 2023.02

[26] CISA, “Zero Trust Maturity Model Version 2.0”, 2023.04

[27] NSA, “Advancing Zero Trust Maturity Throughout the User Pillar”, 2023.04

[28] Chirs Pymm, “Thunderdome : Realizing Zero Trust”, 2023.05

[29] PR Newswire, “DISA announces successful completion of Thunderdome prototype”, 2023.05

[30] 과학기술정보통신부 등, “제로트러스트 가이드라인 1.0”, 2023.07

[31] NSA, “Advancing Zero Trust Maturity Throughout the Device Pillar”, 2023.10

[32] Chirs Pymm, “Thunderdome : Realizing Zero Trust”, 2023.10

[33] 과학기술정보통신부 등, “정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 안내서”, 2023.11

[34] 과학기술정보통신부 등, “공공부문 SaaS 이용 가이드라인”, 2024.02

[35] NSA, “Advancing Zero Trust Maturity Throughout the Network and Environment Pillar”, 2024.03

[36] NSA, “Advancing Zero Trust Maturity Throughout the Data Pillar”, 2024.04

[37] GSA, “Zero Trust Architecture - Buyer’s Guide Version 3.1”, General Services Administration, 2024.04

[38] Lisbeth Perez, “DISA Plans to Deploy Thunderdome to 60 Sites in FY2024”, MeriTalk, 2024.04

[39] NSA, “Advancing Zero Trust Maturity Throughout the Application and Workload Pillar”, 2024.05

[40] NSA, “Advancing Zero Trust Maturity Throughout the Visiblity and Analytics Pillar”, 2024.05

[41] 한국정보보호산업협회, “국내 제로트러스트 보안로드맵 마련을 위한 실증방안 연구”, 과학기술정보통신부 정책연구보고서, 2024.05

[42] NIST SP 1800-35, “Implementing a Zero Trust Architecture: Full Document, Fourth Preliminary Draft”, 2024.07

[43] NSA, “Advancing Zero Trust Maturity Throughout the Automation and Orchestration Pillar”, 2024.07

[44] 과학기술정보통신부 등, “정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도 안내서”, 2024.07

[45] 금융위원회, “금융분야 망분리 개선 로드맵”, 2024.08

집필진

- 가천대학교 이석준 교수
- 강남대학교 박정수 교수
- 대구대학교 김창훈 교수
- 국민대학교 김환국 교수
- 국가보안기술연구소 이택규 책임
- 에스지에이솔루션즈(주) 최영철 대표
- 프라이빗테크놀로지(주) 김주태 전무
- (주)엔키화이트햇 이철호 연구소장
- 과학기술정보통신부 정보보호산업과
- 한국인터넷진흥원(KISA)
  - 정책연구실 황보성 실장, 신기술대응팀 하병욱 팀장, 이혜진 책임, 이재혁 주임
  - 보안산업단 임채태 단장, 보안산업진흥팀 고현봉 팀장, 최슬기 선임
  - 보안인증단 이익섭 단장, ISMS인증팀 박창열 팀장, 양선주 책임
- 한국제로트러스트포럼 정책·제도분과

제로트러스트 가이드라인 2.0

과학기술정보통신부
KISA 한국인터넷진흥원
한국제로트러스트포럼