금융보안원
FINANCIAL SECURITY INSTITUTE

# 금융권의 제로트러스트 아키텍처 도입 방안 연구

## - 제로트러스트 도입 시 보안 위협 시나리오 분석을 중심으로

김은지* · 황혜경** · 이은진** · 김병민***· 이재윤****

* 서울여자대학교 정보보호학과

** 세종대학교 정보보호학과

*** 인하공업전문대학 컴퓨터정보공학과

****연세대학교 법무대학원

**요 약**

최근 금융권 환경에서 많은 변화가 일어나고 있다. 기존 금융 시스템의 보안 정책으로 적용되었던 망분리 제도의 개선 계획이 공식적으로 발표되었다. 이로 인해 금융 시스템의 경쟁력이 크게 제고될 것으로 기대되는 한편, 보안에 대한 우려의 목소리도 나온다. 이러한 상황에서 제로트러스트는 망분리 제도를 대체하여 금융 시스템의 보안을 강화하는 모델로 작동할 수 있다. 제로트러스트는 기존의 보안 모델이 대비하지 못하는 위협까지 효과적으로 방어할 수 있다. 본 연구에서는 제로트러스트의 기본 원리, 핵심 구성 요소, 성숙도 모델 및 도입 등에 대하여 살펴본다. 이후 내부자 유출, DoS, 공급망 공격, APT 공격 등 금융권에 발생할 수 있는 위협 시나리오와 이에 대한 제로트러스트 대응 방안을 제시한다. 대표적으로 최소한의 권한만을 부여하는 최소 권한 원칙, 모든 접속 요청을 검증하는 접근 제어, 여러 인증 과정을 거치는 MFA 등이 있다. 이를 통해 금융권의 기존 보안 모델을 대체할 새로운 보안 패러다임인 제로트러스트 도입 방안에 대해 살펴보고자 한다.

## 키워드

제로트러스트, 성숙도 모델, 최소 권한 원칙, 접근 제어, 보안 위협 시나리오

## 목 차

# I. 서론

2020년 코로나19 팬데믹 이후, 재택근무 형태가 확산되면서 외부 접속으로부터의 기업망 보안 유지가 더욱 중요시되었다. 이에 많은 기업이 VPN을 도입하였지만, 네트워크 속도 저하, 공격 지점 증가 등의 문제점을 겪고 있다. 또한 원격 접속 기기의 다양화와 클라우드 서비스 도입 등으로 인해 보안 경계가 모호해지고, 공격 경로가 복잡해졌다. 이러한 상황에서 제로트러스트 모델이 해결 방안으로 주목받고 있다.

제로트러스트 모델은 '신뢰할 수 있는 네트워크' 개념을 배제하고, 모든 사용자와 기기, 네트워크 트래픽을 기본적으로 비신뢰 상태에서 검증한다. 이를 통해 조직 내 데이터와 리소스 같은 자산에 접근하는 모든 주체에 대해 지속적으로 검증하고, 위험성을 평가하며, 위험을 완화할 수 있을 것으로 평가된다.

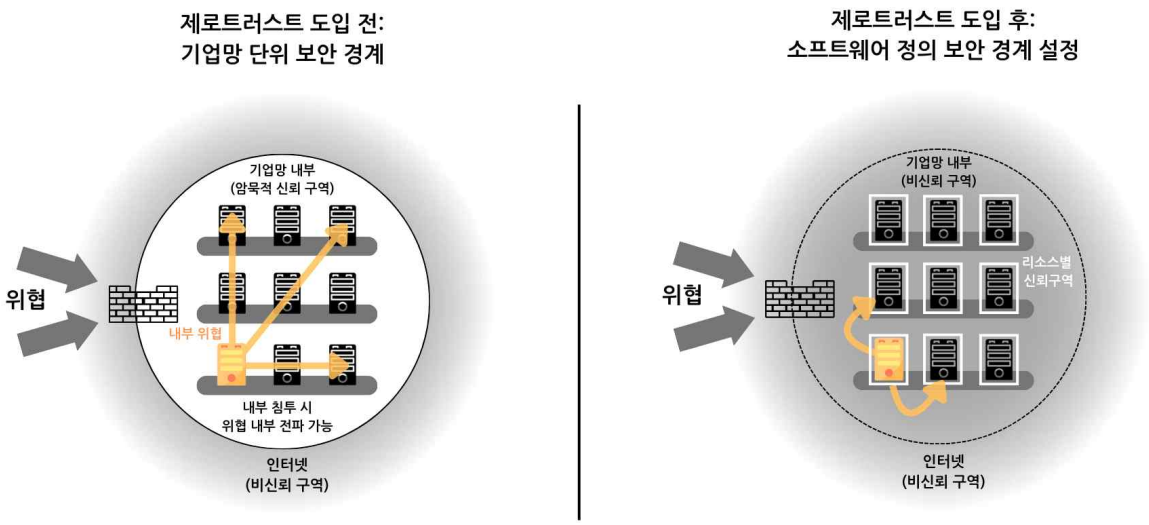
한편, 금융기관에서도 코로나19 팬데믹 이후 업무 환경의 급격한 변화를 맞이하고 있다. 업무 환경이 디지털화되면서 기존 금융권의 보안 체계였던 망분리의 문제점이 본격적으로 수면 위로 떠오르기 시작했다. 원격 근무 시 업무망 접속 불가, 클라우드, AI, SaaS와 같은 신기술 도입의 제약 등과 같이 디지털화되는 업무 환경에서 망분리 제도의 한계가 드러났다. 이에 따라 망분리 규제를 완화해야 한다는 분위기가 형성되었고, 2024년 8월 13일 금융위원회는 「금융분야 망분리 개선 로드맵」을 발표하여 단계적으로 망분리 규제를 완화할 계획임을 밝힌 바 있다. 이렇게 기존의 보안 체계가 완화됨에 따라 이를 대체할 강화된 보안 모델이 필요하며, 그 중 하나로 제로트러스트 원칙 도입이 고려되고 있다 [1].

본 연구는 금융권 보안 위협 시나리오와 대응 방안을 통해 금융권의 제로트러스트 아키텍처 도입 방안 제시를 목표로 하며, 구성은 다음과 같다. 2장에서는 경계 기반 보안 모델의 한계와 제로트러스트의 개념, 원리, 논리 구성 요소 및 신뢰도 평가 알고리즘을 포함한 제로트러스트의 아키텍처 개요를 살펴본다. 3장에서는 제로트러스트 성숙도 모델, 도입 시 고려사항, 단계별 도입 방안에 대해 다룬다. 4장에서는 금융권의 보안 환경과 금융권에서 발생할 수 있는 위협 시나리오를 작성하고 이에 대해 제로트러스트 관점에서의 대응 방법에 대해 분석한다. 이를 바탕으로 금융권의 제로트러스트 아키텍처 구현 방안을 제안한다. 마지막으로 5장에서는 연구의 시사점 및 결론을 도출한다.

# Ⅱ. 제로트러스트 아키텍처 개요

## 1. 경계 기반 보안 모델의 한계와 제로트러스트 등장

최근 발생하는 수많은 사이버 보안 공격 사례는 기존의 경계 기반 보안 모델의 한계점을 드러내고 있다. 경계 기반 보안 모델은 외부와 내부 네트워크 사이의 경계를 정의하고, 외부와 내부 네트워크를 각각 비신뢰 구역과 신뢰 구역으로 구분한다. 비신뢰 구역인 외부로부터의 접근에 대해서는 비정상 행위를 탐지하고 대응하는 반면, 신뢰 구역의 내부자에게는 암묵적 신뢰를 바탕으로 높은 권한을 부여한다. 즉, 네트워크 내부에서 발생하는 접속 요청은 일정 수준의 신뢰를 바탕으로 시작한다. 공격자가 네트워크 경계에 설치된 방화벽, IDS 등의 보안 체계를 통과하여 내부 시스템에 침투하게 되면 암묵적 신뢰 하에 많은 권한을 획득하고, 내부의 다양한 리소스에 접속하여 매우 쉽게 공격을 전파할 수 있게 된다. 이러한 기존의 경계 기반 보안 모델은 신뢰 구역에서 신뢰할 수 없는 대상인 공격자를 식별할 수 없기 때문에 한 번 인증된 기기나 사용자에 적용되는 검증 방법이 매우 미흡하다. 따라서 악성코드 감염 등 악의적인 방법으로 공격자가 내부망에 침투하면 높은 신뢰를 바탕으로 권한을 부여받아 내부 데이터를 탈취하거나 시스템을 손상시킬 수 있다. 파일을 암호화하여 돈을 요구하는 ‘랜섬웨어’ 공격, 이미 유출된 계정 정보를 이용하여 여러 웹사이트에 무작위로 대입함으로써 로그인을 시도하고 개인정보 및 자료를 유출하는 ‘크리덴셜 스터핑(Credential Stuffing)’ [2], 공격 대상에게 장기간 걸쳐 다양한 수단을 총동원하는 ‘지능형 지속 공격(APT)’ 등의 보안 위협에 효과적으로 대응하지 못한다. 공격자는 무조건 외부에만 존재하는 것이 아니라, 먼저 내부로 침투한 이후 공격을 수행할 수 있음을 인지해야 하는 것이다. 이처럼 갈수록 보안 위협이 고도화, 지능화되면서 기존의 보안 모델이 한계에 다다르게 되었고, 그에 따라 내부자에 대해서도 인증 후에도 끊임없이 신뢰성을 검증하는 제로트러스트 보안 모델이 주목받고 있다.




**<그림 1> 기존 경계 기반 보안과 제로트러스트 개념 비교**

제로트러스트(Zero Trust)는 2010년 포레스터 리서치 수석연구원인 존 킨더버그(John Kindervag)가 제시한 개념이다. 제로트러스트의 기본 개념은 “Never Trust, Always Verify”로, 공격자가 네트워크 내부와 외부 어디든 존재할 수 있기 때문에 모든 접속 요구는 신뢰할 수 없다는 가정에서 시작한다. 미국표준기술연구소(NIST)는 제로트러스트를 “항상 네트워크가 침해되었다고 가정하고, 보호해야 할 데이터 및 컴퓨팅 서비스 등에 대한 접근 요구에 대해 정확하고 최소한의 권한을 부여하는 아이디어와 개념의 모음”으로 설명한다 [3]. 절대적 신뢰 구역을 최소화하는 것을 목표로, 보호해야 할 모든 리소스의 경계를 분리하고 보호한다. 사용자가 특정에 접근하고자 할 때, 정책결정지점(PDP)[1]과 정책시행지점(PEP)[2]을 통해 해당 접근이 적절한지 판단한다. 정책시행지점을 통과하면 리소스를 제공받는 신뢰 구역이 된다. 정책결정지점 및 정책시행지점과 자원을 최대한 가깝게 하여, 암묵적인 신뢰 구역을 최소화한다. 하나의 자원에 대한 권한을 획득한 후에는 그 권한 안에서만 활동할 수 있으며, 다른 자원에 접근하고자 할 때에는 추가적인 인증이 요구된다 [4, 5].

1) 정책결정지점(PDP) : 접속 요청을 기반으로 보안 정책에 따라 접근 허용 여부를 판단하는 지점
2) 정책시행지점(PEP) : PDP의 결정에 따라 실제로 보안 정책을 적용하고, 접근을 허용하거나 차단하는 지점


**<그림 2> 제로트러스트 접근 개념 모델**

## 2. 제로트러스트 기본 원리

기존의 경계 기반 보안 모델은 사용자의 네트워크상에서의 위치를 매우 중요하게 고려하였다. 그러나 앞서 언급한 바와 같이 기존의 경계 기반 보안 모델은 점차 고도화되는 공격을 효과적으로 방어하는 데 한계가 드러났으며, 원격 접속 등 업무 환경이 변화함에 따라 더 이상 디지털화된 업무 환경에 적합하지 않게 되었다. 따라서 기존의 경계 기반 보안 모델을 대체하기 위해 제로트러스트 아키텍처를 구성할 필요성이 대두되고 있다.

Forrester, Google 등 다양한 기업 보고서와 NIST SP 800-207, CSA SDP, DoD 제로트러스트 참조모델 등은 각각 제로트러스트 원리를 정의하고 있다. 그 중 Forrester, Google, NIST SP 800-207에서 정의한 제로트러스트 핵심 원칙은 <표 1>과 같다.

**<표 1> 기업 및 기관별 제로트러스트 핵심 원칙**

| Forrester | Google | NIST SP 800-207 |
|---|---|---|
| - 모든 개체는 기본적으로 신뢰할 수 없음.<br>- 최소 권한 접근을 적용함.<br>- 종합적인 보안 모니터링을 구현해야 함. | - 모든 사용자와 기기를 신뢰하지 않음.<br>- 모든 리소스 접근을 검증하고, 최소 권한 원칙에 따라 동적 보안 정책 사용함.<br>- 내부에 공격자가 있을 수 있다는 가정하에 접근 요청을 면밀히 검토하고 자원을 보호함.<br>- 자원 접근은 동적 및 정적 속성을 고려해 일관되게 처리함.<br>- 최소한의 접근 권한만 부여함.<br>- 지속적인 보안 모니터링 필요함. | - 모든 데이터와 컴퓨팅 서비스는 리소스로 간주함.<br>- 네트워크상의 모든 통신은 안전하게 보호해야 함.<br>- 리소스에 대한 접근은 세션 단위로 부여함.<br>- 접근 권한은 동적 정책에 따라 결정함.<br>- 리소스의 무결성과 보안을 지속적으로 모니터링하고 측정해야 함.<br>- 인증 및 권한 부여는 동적이며, 엄격하게 수행함.<br>- 자산과 인프라의 상태를 |

| | | |
|---|---|---|
| | | 지속적으로 평가하여 보안 환경을 개선함. |

Forrester는 제로트러스트의 세 가지 핵심 원칙으로 모든 개체는 기본적으로 신뢰할 수 없다는 점을 강조하고, 최소 권한 접근을 적용하며, 종합적인 보안 모니터링을 구현해야 한다고 제안한다 [6]. Google에서 발표한 제로트러스트 운영 원칙은 다음과 같다. 첫째, 모든 사용자, 기기, 워크로드, 애플리케이션 및 데이터 흐름을 신뢰하지 않는다. 둘째, 모든 리소스에 대한 접근을 항상 검증하여 권한을 부여하며, 최소 권한 원칙에 기반해 동적 보안 정책을 사용한다. 셋째, 공격자가 이미 내부에 존재한다는 가정하에 모든 접근 요청 면밀 검토, 자원 접근 제한, 데이터 암호화 등의 조치를 통해 리소스를 보호해야 한다. 넷째, 자원에 대한 모든 접근은 동적 및 정적 속성을 고려하여 일관된 방식으로 이루어져야 한다. 다섯째, 작업을 수행하는 데 필요한 최소한의 접근 권한만을 부여해야 한다. 마지막으로, 지속적인 종합 보안 모니터링이 필요하다 [7]. NIST SP 800-207에서 발표한 제로트러스트 기본 원칙은 다음과 같다. 첫째, 모든 데이터와 컴퓨팅 서비스는 리소스로 간주한다. 둘째, 모든 통신은 네트워크상의 위치와 관계없이 안전하게 보호되어야 한다. 셋째, 세션 단위로 개별 리소스에 대한 접근이 부여된다. 넷째, 리소스에 대한 접근은 동적 정책을 통해 결정된다. 다섯째, 모든 보안 상태와 리소스의 무결성을 측정하고 모니터링해야 한다. 여섯째, 모든 리소스에 대한 권한 부여와 인증은 동적이며, 접근이 허용되기 전 엄격하게 수행되어야 한다. 마지막으로, 자산, 네트워크 인프라, 통신의 현재 상태에 대한 가능한 많은 정보를 수집하고 이를 통해 보안 환경을 개선한다 [4].

국내 ‘제로트러스트 가이드라인 1.0’에서는 위에서 살펴본 내용을 참고하여 6가지 제로트러스트 기본 원리를 다음과 같이 정의하고 있다 [8].

(1) 기본 원칙 : 모든 종류의 접근에 대해 신뢰하지 않을 것

모든 접근 시도를 거부하며, 인증된 사용자에게만 제한된 접근을 허용하는 것을 원칙으로 한다. 인증을 거친 후에도 지속적인 모니터링을 통해 의심스러운 상황 발생 시 추가 인증을 요구하거나 세션을 종료시키는 등의 조치를 취해야 한다.

(2) 일관되고 중앙 집중적인 정책 관리 및 접근제어 결정, 실행 필요

접근 정책에 대해 일관되고 중앙 집중적인 관리가 필요하다. 또한, 리소스 접근

요청에 대해 이미 수립된 중앙 집중적인 정책에 따라 일관된 결정을 내려야 하며, 여러 지점에서 정책을 결정 및 시행하더라도 일관된 정책 결정이 이루어져야 한다.

(3) 사용자, 기기에 대한 관리 및 강력한 인증

등록된 사용자와 기기에 대해 강력한 인증과 상태 관리가 필요하다. 또한 등록되지 않은 기기에 대해서는 접근을 원천적으로 차단하고, 보안 상태가 확인되지 않은 기기에 대해서도 추가적인 인증을 요구해야 한다.

(4) 리소스 분류 및 관리를 통한 세밀한 접근제어

리소스를 분류하는 명확한 기준을 세우고 사용자의 업무 범위, 직급, 시간 등에 따라 세밀한 접근제어가 이루어져야 한다. 이를 통해 공격자가 기업망 내부에 침투하더라도 횡적 이동으로 중요 데이터에 접근을 최소화할 수 있다.

(5) 소프트웨어 정의 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용

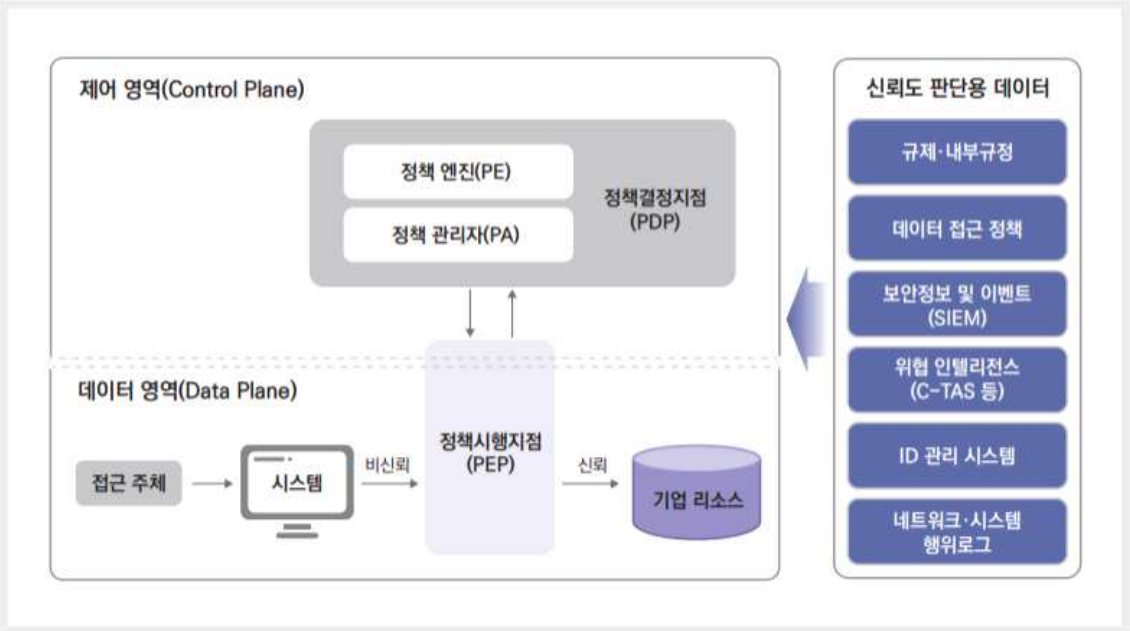
소프트웨어 정의 경계와 같은 방식을 통해 리소스 사이의 경계를 설정하여 보호하고, 허용된 리소스 접근 시간을 장기간 유지하지 않아야 한다. 리소스 접근을 세션 단위로 허용해야 하며, 인증된 세션으로 다른 리소스에 접근하는 것을 제한해야 한다. 또한, 통신 과정에서 기밀성 및 무결성이 보장되어야 한다.

(6) 모든 상태에 대한 모니터링, 로그 및 이를 통한 신뢰성 지속적 검증, 제어

사용자, 리소스, 정책 서버 등 모든 상태를 모니터링하고 로그를 분석하여 신뢰성을 지속적으로 검증한다. 이는 사용자 및 기업망에 대한 신뢰성을 확보하며 접근을 동적으로 관리하는 데 중요한 역할을 한다.

## 3. 제로트러스트 논리 구성 요소

기업망에서 제로트러스트 아키텍처를 구현하기 위해서는 사용자의 리소스 접근에 대한 정책이 필요하다. 리소스에 대한 접근 허용 또는 거부 결정은 정책에 기반하므로, 접근제어 정책은 제로트러스트 아키텍처에서 가장 핵심적인 보안 기능이다.




**<그림 3> 제로트러스트 아키텍쳐 보안 모델 및 논리 구조 (출처: 과학기술정보통신부 제로트러스트 가이드라인 1.0)**

위 그림에서 제어 영역(Control Plane)은 접근제어 정책이 결정되는 논리적 공간이다. 제어 영역에서 정책결정지점과 정책시행지점 사이의 통신을 통해 사용자가 접근하고자 하는 리소스에 대한 접근 허용 여부를 판단하는 데 필요한 정보 및 판단 결과를 교환한다. 데이터 영역(Data plane)은 정책이 시행되어 사용자가 리소스에 접근하는 논리적 공간이다. 데이터 영역에서 사용자가 리소스에 접근하고자 할 때 정책시행지점이 결정된 정책에 따라 리소스로의 연결 또는 종료를 수행한다. 제로트러스트 아키텍처의 핵심 보안 요소 중 정책결정지점(PDP)는 제어 영역에, 정책시행지점(PEP)은 데이터 영역에 속해 있다.

(1) 정책결정지점(PDP, Policy Decision Point)

정책결정지점은 리소스에 대한 사용자의 접근 요청을 검증하고, 정책에 따라 접근 허가를 결정한다. 정책결정지점은 정책 엔진(PE, Policy Engine)과 정책 관리자(PA, Policy Administrator)로 구성된다.

(2) 정책 엔진(PE, Policy Engine)

정책 엔진은 리소스에 대한 사용자의 접근을 최종적으로 결정한다. 정책 엔진은 신뢰도 평가 알고리즘[1]에 현재 기업망에 대한 정책과 그 외 정보를 입력하고, 이를 통해 접근 허용 여부를 결정하거나 현재 허가된 상태 접근을 취소할 수 있다. 즉 정책 엔진은 접근에 대한 승인을 담당하는 역할을 한다.

(3) 정책 관리자(PA, Policy Administrator)

정책 관리자는 정책결정지점을 정책 엔진과 함께 구성하며, 정책시행지점에 명령하여 사용자와 리소스 간의 통신 경로를 생성하거나 폐쇄한다. 즉 정책 엔진으로부터 결정된 승인 여부를 실행하는 역할을 담당한다. 정책 관리자는 세션에 대한 인증 및 인가 토큰을 생성하여 사용자가 리소스에 접근하는 데 사용한다. 최종적으로 세션을 허락 또는 거부하는 결정은 정책 엔진이 수행한다.
세션이 인가되면 정책 관리자는 정책시행지점에게 세션 시작을 허용한다. 세션이 거부 혹은 취소되는 경우에는 정책시행지점에게 해당 연결을 끊을 것을 요청하는 신호를 보낸다.

(4) 정책시행지점(PEP, Policy Enforcement Point)

정책시행지점은 사용자와 리소스 사이의 연결을 생성하고 모니터링하며 최종적으로 연결 종료까지 수행하는 논리 구성 요소이다. 정책시행지점은 정책 관리자와 통신하여 접근 요청이나 업데이트된 정책을 수신하고 이를 기반으로 동작을 수행한다.

(5) 접근 결정을 위해 사용하는 데이터 입력 요소

핵심 논리 구성 요소가 정책을 결정하고 시행하는 데 있어 다양한 정보를 제공하는 데이터 입력 요소가 있다. 이는 신뢰도 판단용 데이터로, 제로트러스트 아키텍처에서 데이터 입력 요소를 정책 엔진의 입력이나 정책 규칙으로 활용할 수 있다. 데이터 입력 요소는 내부 데이터와 조직이 생성하거나 제어하지 않는 외부 데이터 입력 요소들이 있으며, 다음과 같은 시스템이 포함될 수 있다.

1) 규제 및 내부 규정(Industry Compliance) : 정보보호 및 프라이버시 관련 법안이

1) 신뢰도 평가 알고리즘 : 접근 주체가 리소스 접근 시, 이에 대한 허가 여부를 최종적으로 판단하기 위해, 현재 접근 주체 혹은 접근 그 자체의 신뢰도를 계산하는 알고리즘

나 산업별 정보보호 요구사항 등과 같은 법적 규제를 준수하는지 확인한다. 이는 법적 규제를 준수하기 위해 조직이 개발한 모든 정책 규칙을 포함한다.

2) 데이터 접근 정책(Data Access Policies) : 리소스 접근에 대한 속성, 규칙, 정책을 의미한다. 정책들은 기본 접근 권한을 생성하여 리소스에 대한 접근을 인가하는 시작점이 되므로, 해당 기관에서 정의한 역할과 필요를 반드시 바탕으로 해야 한다.

3) 보안 정보 및 이벤트(SIEM) : 차후 분석을 위하여 보안 정보를 수집하고 이 정보들은 정책 개선과 발생할 수 있는 공격을 경고하는 데 활용된다.

4) 위협 인텔리전스(Threat Intelligence) : 정책 엔진의 접근 결정에 도움을 줄 수 있는, 내외부에서 발생하는 최신 보안 위협에 관한 정보를 제공한다. 새로운 공격 기법 및 악성코드, 새로 발견된 소프트웨어 취약점 등이 포함될 수 있다.

5) ID 관리 시스템(ID Management System) : 기업 사용자 계정 및 식별 기록을 생성하고, 그 정보를 저장 및 관리하는 시스템이다. 역할, 접근 속성, 할당된 자산과 같이 사용자의 정보 및 특징과 외부 협력을 위한 외부 사용자를 포함할 수 있으며, 더 큰 연합 공동체의 구성 요소로서 동작할 수도 있다.

6) 네트워크 및 시스템 행위 로그(Network and System Activity Logs) : 로그 시스템은 네트워크 트래픽, 자산 로그, 리소스 접근 행위와, 기업망의 보안 상태에 관해 실시간 피드백을 제공하는 기타 이벤트를 수집한다.

## 4. 제로트러스트 신뢰도 평가 알고리즘

사용자의 리소스에 대한 접근을 제어하기 위해서는 이에 대한 신뢰도를 평가할 수 있어야 한다. 앞서 언급한 바와 같이 접근을 제어하는 정책 엔진은 신뢰도 평가 알고리즘을 통해 리소스에 대한 접근을 최종적으로 결정한다. 신뢰도 평가 알고리즘에 입력되는 값으로는 접근 요청, 접근 주체 데이터베이스, 자산 데이터베이스, 리소스 요구사항, 위협 인텔리전스가 있다. 신뢰도가 평가 실행에 대한 최종 결정은 정책 관리자가 수행하며, 필요한 곳에 정책시행지점을 설정하여 승인된 접근에 대해 통신을 가능하게 한다.

(1) 접근 요청 : 사용자의 정보와 그 사용자의 접근 요청에 관한 정보를 의미한다. 이는 사용 중인 소프트웨어, OS 버전, 패치 정보 등의 요청된 리소스 및 요청자 정보가 포함된다.

(2) 접근 주체 데이터베이스 : 리소스에 접근을 요청하는 사용자의 정보를 의미한다. 이는 논리 식별자의 조합이나 정책집행지점이 수행한 인증 확인 결과 등의 사용자 식별자와 이에 할당된 시간 및 지리적 위치 속성, 권한 정보 등을 포함한다.

(3) 자산 데이터베이스 : 조직이 소유 또는 인지할 수 있는 물리, 가상, 기타 자산의 상태를 포함하는 데이터베이스를 의미한다. 이는 OS 버전, 설치된 소프트웨어, 무결성, 네트워크 위치, 지리적 위치, 패치 정보 등을 포함하며, 접근제어를 수행하기 위해 자산 데이터베이스에 저장된 정보를 활용한다.

(4) 리소스 요구사항 : 리소스 접근을 위한 최소한의 요구사항을 의미한다. 해외 IP 접근 거부와 같은 네트워크 위치 요구사항, 데이터 민감도 등의 인증 보증 레벨 요구사항, 자산 설정 요구사항이 포함된다.

(5) 위협 인텔리전스 : 일반적인 사이버 위협 및 악성코드 최신 동향에 대한 정보 집합을 의미한다. 이는 의심스러운 기기로부터의 통신과 관련된 정보, 공격 패턴 또는 보완 대책이 포함된다.

# Ⅲ. 제로트러스트 도입 방안

## 1. 제로트러스트 성숙도 모델

성숙도 모델은 일반적으로 특정 프로세스 및 기술에 대한 조직의 성숙도를 측정하기 위한 프레임워크를 의미한다 [8]. 보안 아키텍처 관점에서도 성숙도 모델에 대한 다양한 형태가 제안되었다. 이는 조직의 목표 및 규정 준수를 위한 요구사항을 만족시킬 수 있는 접근 방법을 제공하고, 현 상태를 평가 및 검증하여 추가적인 기술 도입과 투자 방향을 설정하는 데 도움을 줄 수 있는 참조 아키텍처의 역할을 수행할 수 있다.

보안 아키텍처에 대한 도입 전략, 계획 및 목표를 수립해야 하는 조직의 관점에서 제로트러스트라는 개념은 추상적으로 다가올 수 있다. 이때 제로트러스트 성숙도 모델은 조직에 제로트러스트 수준을 평가하고 구현 및 도입을 수립하는 데 도움을 줄 수 있다.

제로트러스트 성숙도 모델(ZTMM)은 제로트러스트 모델 기반의 보안 개념이 얼마나 잘 적용되어 운영되고 있는가를 객관적으로 표현하기 위한 모델이다. 다양한 해외 기업 및 기관에서 제로트러스트를 도입하기 위한 성숙도 모델과 핵심 요소를 정의하였다.

**<표 2> 기업 및 기관별 제로트러스트 핵심 요소**

| Forrester | Microsoft | SAP | DISA/NSA(DoD) | CISA |
|---|---|---|---|---|
| - 데이터<br>- 네트워크<br>- 사람<br>- 워크로드<br>- 장치<br>- 가시성 및 분석<br>- 자동화 및 오케스트레이션 | - 정체성<br>- 엔드포인트<br>- 어플리케이션<br>- 인프라<br>- 데이터<br>- 네트워크 | - 정체성<br>- 데이터<br>- 엔드포인트<br>- 어플리케이션<br>- 인프라<br>- 네트워크 | - 사용자<br>- 장치<br>- 어플리케이션 및 워크로드<br>- 데이터<br>- 네트워크와 환경<br>- 자동화 및 오케스트레이션<br>- 가시성 및 분석 | - 정체성<br>- 장치<br>- 네트워크와 환경<br>- 어플리케이션 및 워크로드<br>- 데이터<br>- 가시성 및 분석<br>- 자동화 및 오케스트레이션<br>- 거버넌스 |

Forrester는 제로트러스트 도입을 위한 기업망의 7가지 핵심 요소를 다음과 같이 제시한다. 7가지 핵심 요소는 데이터, 네트워크, 사람, 워크로드, 장치, 가시성 및 분석, 자동화 및 오케스트레이션으로 구성된다 [9]. Microsoft는 정체성, 엔드포인트, 애플리케이션, 인프라, 데이터, 네트워크로 총 6가지 핵심 요소를 정의한다 [10]. SAP 또한 6가지 핵심 요소를 제시하고 있으며 정체성, 데이터, 엔드포인트, 애플리케이션, 인프라, 그리고 네트워크를 중요 요소로 강조한다 [11]. DISA/NSA (DoD)는 7가지 핵심 요소를 정의하고 있다. 사용자, 장치, 애플리케이션 및 워크로드, 데이터, 네트워크와 환경, 자동화 및 오케스트레이션, 가시성 및 분석을 포함하여 포괄적인 보안 접근 방식을 취하고 있다 [12]. CISA의 제로트러스트 성숙도 모델은 5가지 핵심 요소와 3가지 교차 기능으로 구성되어 있다. 5가지 핵심 요소는 정체성, 장치, 네트워크와 환경, 애플리케이션 및 워크로드, 데이터이며, 이와 함께 가시성 및 분석, 자동화 및 오케스트레이션, 거버넌스를 교차 기능으로 제시한다 [13]. 이처럼

다양한 기업과 기관들이 정의한 핵심 요소와 교차 기능에서 사용자, 기기, 네트워크, 애플리케이션, 데이터, 가시성, 자동화 및 오케스트레이션 등 7가지가 주로 언급된다는 것을 확인 할 수 있다.

제로트러스트를 성공적으로 도입하기 위해서는 우선 기업망의 핵심 요소들을 분류하고 성숙도의 현재 수준을 정확하게 파악하는 것이 중요하다. 이미 여러 기관에서는 제로트러스트 성숙도 모델 단계를 발표하였는데, 기관마다 제로트러스트 도입의 성숙도를 평가하는 기준이 다르며 각기 다른 접근 방식을 취하고 있다.

CISA가 발표한 제로트러스트 성숙도 모델의 4단계는 다음과 같다. '전통(Traditional)' 수준은 설정부터 폐기까지의 수명 주기가 수동으로 이루어진다. 보안 정책과 관련하여 설정이나 로그 관리는 정적으로 관리되며, 외부 시스템에 대한 의존성을 가지고 있다. 최소한의 권한만을 부여하는 방식이지만 프로비저닝 시에만 설정되고, 보안 정책 집행이 분리되어 있다. 또한, 대응과 완화 조치는 수동으로 이루어지고 종속성, 로그, 텔레메트리의 상관관계가 제한적으로 연결성이 부족하다. '초급(Initial)' 수준에서는 보안관리의 일부인 속성 할당과 수명주기 관리, 정책 결정 및 집행이 자동화된다. 또한 외부 시스템과의 통합이 이루어진다. 자산 설정 후에만 일부 최소 권한 수정이 이루어지며, 정책 집행이 서로 분리되어 있다. 수동으로 대응 및 문제해결을 하고 로그나 의존성 간의 연결이 부족하다. '고급(Advanced)' 수준은 가능한 모든 부분에서 라이프 사이클과 정책 할당이 자동화되고, 기둥 간 조정이 이루어진다. 중앙집중식 가시성과 신원 관리가 가능하며, 정책 집행이 통합된다. 미리 정의된 대응 조치에 따라 문제를 해결하고 위험평가 및 자세 평가에 따라 최소권한이 수정되며, 조직 전반에서 인식 수준을 높인다. '최적(Optimal)' 수준에서는 모든 라이프사이클과 자산 속성 할당이 완전히 자동화된다. 자산 및 리소스가 스스로 정보를 보고하는 동적 자산 및 각각에 대한 최소 권한 액세스를 따른다. 또한 지속적인 모니터링을 통하여 교차 기둥 간에 상호 운영성이 있으며, 중앙에서 상황을 종합적으로 파악할 수 있는 중앙 집중화된 가시성을 가지고 있다.

모든 과정이 완전히 자동화되고, 자산이 스스로 정보를 보고하며 동적인 정책을 따른다. 자산과 그 의존성에 대해 필요한 만큼만 접근할 수 있게 하며, 지속적으로 모니터링하고 교차 기둥 간에 원활하게 작동하며, 상황을 종합적으로 파악할 수 있는 중앙 집중식 시스템을 갖추고 있다 [13].

위에서 살펴본 CISA의 성숙도 모델을 기반으로, 국내 '제로트러스트 가이드라인

1.0’에서는 성숙도 모델 3단계 수준을 다음과 같이 정의하고 있다. ‘기존(Traditional)’은 아직 제로트러스트를 적용하지 않은 수준으로, 대부분 기존의 네트워크 방어가 중심인 경계 기반 보안 모델을 사용하고 있는 상태를 말한다. 해당 수준에서는 정교한 공격 및 내부자 공격 등에 일부 취약하다. ‘기존’ 수준에서 요구하는 보안 기술의 특징으로는, 수동적인 설정 및 속성 부여, 정적 보안 정책, 온프레미스 ID (때때로 SSO와 다중 인증 적용), 외부 시스템에 대해 정밀하지 않은 종속성을 가진 핵심 요소별 솔루션, 프로비저닝에서 최소 기능 구축, 독점적이고 유연하지 않은 정책 적용, 그리고 수동적인 사고 대응 및 완화 배포를 포함한다. ‘향상(Advanced)’은 부분적으로 제로트러스트 철학을 도입한 수준으로, 제로트러스트 원칙이 보안 아키텍처에서 핵심 기능이 되는 상태이다. ‘향상’ 수준에서는 최소 권한 접근, 네트워크 분할, 로깅 및 모니터링 등이 부분적으로 적용되어 ‘기존’보다 높은 보안성을 보장할 수 있다. 이 수준에서 요구하는 보안 기술 특징으로는 세밀한 수준에서의 사용자 및 기기에 대한 접근제어, 중앙 집중적인 ID 제어와 정책 적용, 상태 평가를 기반으로 최소 권한 부여, 네트워크 일부 세분화를 통해 공격 위험 감소, 일부 핵심 요소 간 일관성, 중앙 집중적인 가시성 부분 제공, 사전 정의된 완화 기법을 통해 일부 사고 대응, 그리고 외부 시스템과 종속성 측면에서 세부 정보 증가를 포함한다. ‘최적화 (Optimal)’ 수준은 전반적으로 조직에 제로트러스트 철학이 적용된 상태이다. ‘최적화’ 수준에서는 자동화 운영, 네트워크 세분화, 지속적인 신원 검증을 통해 최소 권한의 안전한 접근제어 등 보안성이 크게 향상된다. 이 수준에서는 Federated ID와 Single Sign On 등의 ID 관리 통합 관리 및 지속적인 신원 검증과 신뢰도 검증, 실시간 분석을 통한 동적 접근제어, 자산과 리소스에 대한 완전 자동화된 속성 부여 및 최소 권한 접근 적용, 고유한 접근 규칙을 적용하는 세분된 영역으로 구분된 네트워크, 핵심 요소 간 상호운용성을 위한 개방형 표준을 통한 조정, 특정 시점의 상태 기억을 위한 히스토리 기능을 갖춘 중앙 집중적 가시성 제공을 포함한다 [13].

제로트러스트 성숙도 수준은 성숙도 모델과 함께 국내 가이드라인에서 정의한 기업망의 핵심 요소인 식별자, 신원, 기기 및 엔드포인트, 시스템, 응용 및 워크로드, 데이터로 다시 정리를 할 수 있다. 앞서 언급한 바와 같이 성숙도 모델은 ‘기존’, ‘향상’, ‘최적화’ 수준으로 구성되어 있지만, 본 논문에서는 제로트러스트 아키텍처 도입 방안에 관한 연구이므로 제로트러스트가 전반적으로 적용된 ‘최적화’ 수준에 대해서만 다루도록 한다.

(1) 식별자 및 신원(Identity)

식별자 및 신원은 사람, 서비스, IoT 기기 등을 고유하게 설명할 수 있는 속성 혹은 속성의 집합을 의미한다. 조직에서는 강력한 인증을 통해 사용자의 신원을 검증하고, 역할 기반 접근제어(RBAC)나 속성 기반 접근제어(ABAC)와 같은 세밀한 접근제어 규칙을 활용하여 접근 요청을 처리해야 한다.

식별자 및 신원 관련 5가지 기능에 대한 최적화 수준은 다음과 같다. 첫 번째로 식별자 관리는 클라우드 및 온프레미스 환경 전반에 걸쳐 글로벌 ID를 활용한다. 이를 통해 다양한 환경에서의 일관된 식별 체계를 구축할 수 있다. 두 번째로, 인증은 접근 권한을 승인할 때뿐만 아니라 지속적인 신원 검증을 수행하여, 사용자의 신원을 실시간으로 확인하고 보안을 강화한다. 세 번째로, 위험도 평가는 기계학습 알고리즘을 활용하여 실시간 사용자 행동 분석을 통해 위험을 결정하고 지속적인 보호를 제공한다. 이러한 접근은 잠재적인 위협을 조기에 식별하고 대응할 수 있는 능력을 향상시킨다. 네 번째로, 가시성 및 분석은 높은 정확도의 속성과 사용자 및 개체 행동 분석(UEBA) 솔루션을 통해 사용자 가시성을 확보하고 중앙 집중화를 구현한다. 이는 더욱 효과적으로 모니터링하고 분석할 수 있는 환경을 만들 수 있다. 마지막으로, 자동화 및 통합은 ID 생명 주기를 완벽히 통합하고, 동적 사용자 프로파일링, 동적 ID 및 그룹 멤버십, 적시(just-in time), 적절한(just-enough) 접근제어를 구현한다. 이러한 자동화를 통해 관리의 일관성을 높일 수 있다.

(2) 기기 및 엔드포인트(Device, Endpoint)

기기 및 엔드포인트는 네트워크에 연결되어 데이터를 주고받는 모든 하드웨어 장치를 의미한다. 이는 조직 소유 기기 외에도 BYOD(Bring Your Own Device)와 같은 개인 기기를 포함한다. 조직은 기기에 대한 목록을 유지하고 기기의 신뢰도를 평가하여, 허가받지 않았거나 신뢰할 수 없는 접근을 차단하는 것이 중요하다.

기기 및 엔드포인트 관련 5가지 기능에 대한 최적화 수준은 다음과 같다. 첫 번째로, 정책 준수 모니터링은 지속적인 기기 보안 상태 모니터링과 검증이 이루어진다. 이를 통해 조직은 정책 위반을 신속하게 감지하고 대응할 수 있다. 두 번째로, 데이터 접근제어 기능은 기기에 대한 실시간 위험 분석이 반영되어, 각 기기의 보안 상태를 지속적으로 평가하고 이를 바탕으로 접근 권한을 조정함으로써 보다 안전한 데이터 보호가 가능해진다. 세 번째로, 자산 관리는 클라우드와 원격을 포함한 모든 환경에 걸쳐 자산 및 취약점 관리가 통합된다. 이를 통해 조직은 자산을 더욱

효과적으로 관리하고 취약점에 대한 즉각적인 대응이 가능하다. 네 번째로, 가시성 및 분석 기능은 지속적으로 기기 상태를 평가한다. EDR(Endpoint Detection and Response)과 같은 툴을 사용하여 기기의 보안 상태를 실시간으로 모니터링하고 분석할 수 있다. 이러한 가시성은 위협을 조기에 발견하고 대응할 수 있는 기반이 된다. 마지막으로, 자동화 및 통합 기능은 동적 조정을 통해 지속적 통합 및 지속적 배포(CI/CD) 원칙을 적용하여, 기기를 보다 효과적으로 관리할 수 있다.

(3) 네트워크(Network)

네트워크는 데이터를 전송하기 위해 사용되는 모든 형태의 통신 매체를 의미한다. 조직은 네트워크 환경을 작은 단위로 나누고, 구역별로 접근을 제어해야 한다. 특히 공격자가 접근해서는 안 되는 네트워크 구역으로 이동하는 것을 막는 것이 매우 중요하다.

네트워크 관련 5가지 기능에 대한 최적화 수준은 다음과 같다. 첫 번째로, 네트워크 세분화 기능은 네트워크 구조가 주변 응용 프로그램의 워크플로우를 기반으로 하여 완전히 분산된 송수신 세부 경계와 더욱 깊은 내부 세분화로 구성된다. 이러한 세분화 기능을 통해 데이터 흐름을 보다 효과적으로 관리한다. 두 번째로, 위협 대응은 컨텍스트 기반 신호와 기계 학습 기술을 활용한 위협 보호 및 필터링이 통합되어, 더욱 정교하고 효과적인 위협 대응 체계를 구축한다. 세 번째로, 암호화 기능은 가능한 경우 내외부로 전달되는 모든 트래픽을 암호화하여 데이터 보호를 극대화한다. 이는 외부 위협으로부터 데이터를 안전하게 보호하는 데 기여한다. 네 번째로, 가시성 및 분석은 자동화된 경고 및 트리거를 사용하여 여러 센서 종류와 위치를 통한 통합 분석이 진행된다. 이를 통해 보다 신속하고 효율적인 대응이 가능해지고, 위협을 조기에 식별할 수 있는 능력이 강화된다. 마지막으로, 자동화 및 통합은 네트워크 및 환경 설정을 위해 지속적 통합 및 지속적 배포(CI/CD) 배포 모델에 따라, 자동화와 함께 코드로서의 인프라를 사용하는 방식이다. 이에 따라 신속한 변화에 대응할 수 있는 유연성을 확보할 수 있다 [8].

(4) 시스템(System)

시스템은 중요한 응용 프로그램을 운영하거나 중요한 데이터를 저장하고 관리하는 서버들을 포함한다. 여기에는 온프레미스(On-Premise)와 클라우드에서 구축 및 운영 중인 모든 서버 시스템이 해당된다. 시스템 관리자나 개발자가 루트 계정과

같은 주요 권한을 가진 자격자로 시스템에 접속할 때, 시스템의 핵심 파일에 대한 읽기 및 쓰기, 주요 명령어 실행 등 시스템 리소스 접근에 대해 세밀하고 정교한 접근제어가 필요하다. 또한, 세션마다 다중 인증(MFA)과 같은 강력한 신원 확인 절차 및 위험 관리 절차를 포함해야 한다.

시스템 관련 5가지 기능에 대한 최적화 수준은 다음과 같다. 첫 번째로, 접근 통제는 MFA 인증과 엔드포인트 시스템의 신뢰도를 기반으로 접근 인가가 진행된다. 또한 시스템에 영향을 미치는 명령어를 실행할 때 실시간 신뢰도 재산정 및 위험 분석을 통해 강력하고 지속적인 접근제어 정책이 적용된다. 두 번째로, 시스템 계정 관리는 접근 인가를 진행하는 권한 사용자의 계정 관리가 독립 시스템을 기반으로 통합적으로 이루어진다. 이때 권한 사용자의 보안 관리 정책이 계정 관리와 통합되어 중앙에서 일원화되어 접근제어 정책이 효과적으로 적용될 수 있다. 세 번째로, 네트워크 분리 정책은 중요 등급 및 기능별 분류를 통해 시스템을 세분화하고, 강력한 시스템 보안 접근 정책을 기반으로 그룹 간 이동을 통제한다. 이러한 접근은 네트워크의 보안을 강화하고, 중요 시스템에 대한 무단 접근을 방지하는 데 효과적이다. 네 번째로, 시스템 보안 및 정책 관리는 온프레미스 및 클라우드상의 모든 시스템 보안 상태에 대한 실시간 모니터링이 이루어지며, 심각한 위협에 대해서는 자동화된 보안 패치 및 정책 변경이 가능하다. 이러한 접근은 보안 관리의 효율성을 극대화하고, 시스템의 안전성을 더욱 강화하는 데 기여한다. 다섯 번째로, 가시성 및 분석 기능은 외부 센서와 시스템을 사용하여 지속적이고 동적인 응용 상태 및 보안 모니터링 수행된다. 이는 실시간으로 시스템의 상태를 분석하고 즉각적인 대응이 가능하게 하여, 보안 관리의 효율성을 크게 향상시킨다. 마지막으로, 자동화 및 통합은 보안과 성능 최적화를 위한 지속적인 환경 변화에 적응이 이루어진다. 이를 통해 자동화된 프로세스를 통해 시스템이 변화하는 요구에 신속하게 대응하고, 최적의 성능을 유지할 수 있도록 한다.

(5) 응용 및 워크로드(Application, Workload)

응용 및 워크로드는 기업망 관리 시스템, 프로그램, 그리고 온프레미스 및 클라우드 환경에서 실행되는 다양한 서비스를 포함한다. 이러한 요소들은 데이터 전송을 위한 인터페이스를 제공한다. 조직은 응용 계층, 컨테이너, 가상 머신 등을 안전하게 보호하고 관리하여 데이터의 안전한 전달을 보장해야 한다.

응용 및 워크로드 관련 6가지 기능에 대한 최적화 수준은 다음과 같다. 첫 번째

로, 접근 인가는 실시간 위험 분석을 고려하여 응용 접근을 지속적으로 인가한다. 이를 통해 실시간으로 변화하는 환경에 적응하여 보안을 강화할 수 있다. 두 번째로, 위협 변호 기능은 응용 동작을 이해하고 설명하는 보호 기법을 제공하는 분석을 사용하여, 응용 워크플로우와 위협 보호에 대한 강력한 통합이 이루어진다. 이는 동적인 위협 환경에 대한 효과적인 대응을 가능하게 한다. 세 번째로, 접근성은 사용자가 인터넷을 통해 모든 응용에 직접 접속하는 것을 가능하게 한다. 이에 따라 사용자는 네트워크상의 다양한 서비스와 응용에 더 쉽게 접근할 수 있다. 네 번째로, 응용 보안은 배포되는 응용에 대해 정기적이고 자동화된 시험을 수행하여 개발과 배포 과정에서 응용 보안 테스트가 통합되도록 한다. 이를 통해 지속적인 보안 점검과 개선이 이루어진다. 다섯 번째로, 가시성 및 분석은 외부 센서와 시스템을 사용하여 지속적이고 동적인 응용 상태 및 보안 모니터링이 이루어진다. 실시간으로 시스템의 상태를 모니터링함으로써 즉각적인 대응이 가능하여 보안 관리의 효율성을 크게 향상시킬 수 있다. 마지막으로, 자동화 및 통합 기능은 보안과 성능 최적화를 위한 지속적인 환경 변화에 적응한다. 이는 자동화된 프로세스를 통해 시스템이 변화하는 요구에 신속하게 대응하고, 최적의 성능을 유지할 수 있도록 한다.

(6) 데이터(Data)

데이터(Data)는 조직에서 가장 우선적으로 보호해야 할 리소스이다. 이를 위해 조직은 데이터 목록을 작성하고, 이를 분류 및 레이블 지정해야 한다. 필요에 따라 암호화 기법을 적용하여 저장 중이거나 전송 중인 데이터를 안전하게 보호하고, 허가받지 않은 데이터 유출에 대응하기 위한 다양한 기법을 마련해야 한다. 또한, 이러한 핵심 요소들에 대한 보안성과 신뢰도를 강화하는 것이 중요하다. 이를 위해 적절하고 세밀한 접근제어가 이루어지도록 제로트러스트 아키텍처를 구현해야 한다.

데이터 관련 5가지 기능에 대한 최적화 수준은 다음과 같다. 첫 번째로, 데이터 목록 관리 기능은 강력한 태그 작업과 추적을 통해 지속적인 목록 작업이 이루어진다. 기계 학습 모델을 사용하여 분류를 강화시켜 보다 정확하고 일관된 데이터 관리가 가능해진다. 두 번째로, 접근 결정방법은 데이터 접근이 적시에 적절한 원칙에 따라 이루어지며, 지속적인 위험 기반 결정을 지원한다. 또한, 이 과정은 동적으로 이루어져 실시간으로 변화하는 상황에 맞춰 접근 권한이 조정된다. 세 번째로, 암호화는 저장소의 모든 데이터를 암호화하여 저장한다. 이에 따라 데이터 보호가 모든 면에서 이루어지며, 모든 데이터에 대해 강력한 보안이 적용된다. 네 번째로, 가시

성 및 분석은 데이터가 목록화되어 언제든지 관리가 가능하며, 의심스러운 행위에 대한 모든 접근 이벤트 로그 및 분석이 이루어진다. 이 과정에서 암호화된 데이터에 대해서도 분석을 수행할 수 있다. 마지막으로, 자동화 및 통합은 높은 가치의 데이터에 대한 엄격한 접근제어가 자동으로 집행된다. 높은 가치의 데이터는 모두 저장 위치와 관계없이 백업되며, 데이터 목록은 자동으로 업데이트되어 항상 최신 상태를 유지할 수 있게 된다. 이를 통해 데이터 관리의 효율성과 안전성이 크게 향상된다.

또한, 위의 핵심 요소들에 대해 보안성과 신뢰성을 높이고, 적절하고 세밀한 접근제어가 이루어지도록 제로트러스트 아키텍처를 기업 네트워크에 적용해야 한다. 이를 위해 모든 핵심 요소에 걸쳐 두 가지 교차 기능이 필요하다.

가시성 및 분석(Visibility and Analytics)은 사용자, 기기, 응용 프로그램 및 워크로드의 상태를 확인하고 상황에 맞는 세부 정보를 활용하여 분석함으로써, 조직이 비정상 행위 탐지를 개선하고 보안 정책 및 접근제어 결정을 동적으로 조정할 수 있도록 한다. 네트워크에 대한 원격 감시를 넘어, 트래픽을 패킷 단위로 직접 캡처하고 분석함으로써 네트워크를 통해 유입되는 모든 종류의 위협을 관찰하고 지능적인 방어 기법을 적용하는 것이 중요하다.

자동화 및 통합 (Automation and Orchestration)는 기존에 수동으로 적용하던 보안 프로세스를 개선하여 자동화된 정책 기반 보안 프로세스를 도입하면, 보다 신속한 보안 조치가 가능하다. SIEM 및 기타 자동화된 보안 솔루션을 통합하고 SOAR을 적용함으로써 제로트러스트 아키텍처를 구현하려는 조직의 모든 환경에서 정의된 프로세스와 일관된 보안 정책을 시행하게 되면, 자동화된 통합 보안 대응이 가능해진다.

## 2. 제로트러스트 도입 시 고려사항

제로트러스트 성숙도 모델을 도입하려는 조직은 최종 목표로 모든 핵심 요소에 대한 최적화 수준에 도달하는 것을 설정해야 한다. 제로트러스트 아키텍처는 점점 더 중요해지고 있으며, 이를 도입하려는 조직은 성숙도 모델 관점에서 도입 시 고려해야 하는 원칙과 기술, 문화, 정책, 규제 등 조직 내외부 환경 관점에서의 고려사항을 이해하고 준비하는 것이 필요하다.

성숙도 모델 관점에서 도입 시 고려해야 할 원칙 중 첫 번째는 제로트러스트의 최적화 수준이 절대적으로 단기간에 달성될 수 없으며, 모든 핵심 요소가 유기적으

로 동작해야 한다는 것이다. 조직에서 현재 가장 중요한 핵심요소 파악 후, 이를 중심으로 성숙도 수준을 높임과 동시에 다른 핵심 요소와 주요 기능의 성숙도가 자연스럽게 이어지도록 장기적인 계획을 실천해야 한다. 또한, 이 과정에서 발생하는 다양한 부작용에 대한 피드백을 반영한 계획이 반복적으로 수정되며 진행되어야 한다. 두 번째는 제로트러스트 전환을 위한 경로는 한 가지 방법만 존재하는 것이 아니라는 점이다. 따라서 조직의 상황에 따라 어떤 경로를 선택하는 것이 적절하며, 어떤 핵심 요소를 우선적으로 진행할 것인지 다르다. 세 번째는 모든 기업이 모든 핵심 요소와 주요 기능에 대해 최적화 수준에 도달할 필요가 없으며, 기업 규모, 기업망의 구성 방식, 사용자와 리소스의 종류, 보유 자산에 관한 관리 수준과 필요성 등을 고려하여 적절한 최종 목표를 세워야 한다. 기업 관리자는 기업의 성숙도 수준을 평가 후, 이를 바탕으로 목표 성숙도 레벨을 달성하기 위한 업무를 정리하고 실행을 위한 리소스 투입량, 예산, 우선순위를 결정하여 제로트러스트 도입을 준비해야 한다.

이와 함께 제로트러스트 아키텍처를 도입하기 위해서는 기술, 기업 문화, 정책, 규제 등 여러 관점에서 검토가 필요하다. 기술적 측면에서는 현재 기업이 많이 사용하고 있는 경계 기반 보안 관점에서의 보안 기술을 파악하는 것과 이를 대체하고 보완할 수 있는 방법을 파악해야 한다. 예를 들어, 제로트러스트의 핵심 기술인 ICAM(신원증명 및 접근관리), SDN(소프트웨어 정의 네트워크), 마이크로 세그먼테이션, IAP(신원인식 프록시), NAC(네트워크 접근제어), SASE(서비스형 보안), SDP(소프트웨어 정의 경계) 등을 갖춘 기업의 솔루션을 지속적인 모니터링을 할 필요가 있다.

기업 문화 측면에서는 제로트러스트 필요성을 결정권자 및 이해관계자가 충분히 인식하고 받아들이는 것이 중요하다. 특히, 변화에 대응하고 새로운 기술을 받아들이는 데 적극적인 문화를 가진 기업들이 제로트러스트 도입에 있어서 유리하다. 따라서 내부 교육과 홍보 등을 통해 제로트러스트의 중요성을 강조하여 새로운 변화에 대한 거부감을 최소로 줄이기 위한 노력이 필요하다.

정책적인 부분에서는 제로트러스트 아키텍처 도입 시 리소스 접근에 관한 정책이 큰 변화를 불러오게 된다. 이는 기업의 모든 인프라, 응용 프로그램, 데이터 전체에 영향을 끼칠 것이며, 특히 클라우드와 온프레미스가 혼합된 환경이나 다양한 형태의 기기가 활용되는 환경에서 접근제어 정책과 신뢰도 평가 알고리즘을 정교하게 설정하는 것은 어렵다. 따라서 신중하게 접근하여 기업 내외부의 다양한 요구를 균

형 있게 반영할 수 있는 정책을 수립해야 한다.

마지막으로, 규제 환경도 중요하게 고려해야 한다. 미국에서는 NIST가 보안 평가, 구현, 인가, 모니터링 등에 대한 지침에 대한 내용을 발행한 위험 관리 프레임워크 혹은 사이버 보안 프레임워크처럼 각 국가마다 사이버 위험을 줄이기 위한 다양한 국가 차원 표준이나 지침이 존재한다. 우리나라도 보안적합성 검증 제도, 클라우드 서비스 보안인증제도, 정보보호 및 개인정보보호 관리체계 인증제도 등이 운영되고 있다. 따라서 이러한 규제 환경의 충분한 이해를 통해 기업은 제로트러스트 도입 계획을 수립하여야 한다.

## 3. 제로트러스트 도입 단계

제로트러스트 아키텍처를 도입하기 위해서 조직은 현재 수준을 평가하고 업무 프로세스와 워크플로우를 파악하여야 한다. 또한 조직은 제로트러스트 아키텍처를 이행하기 위해 부분적으로 성숙도를 상승시키는 방향으로 아키텍처를 도입할 수 있다. NIST SP 800-207에서는 자산, 접근 주체, 데이터 흐름에 대한 조사를 권장하며, NIST SP 800-37의 위험 관리 프레임워크는 준비, 분류, 선택, 구현, 평가, 인가, 모니터링의 7단계로 구성된다. 우리나라의 제로트러스트 가이드라인 1.0은 준비, 계획, 구현 운영, 피드백 및 개선의 4단계로 제로트러스트 아키텍처 도입 과정을 정리하고, 운영 중에 발생하는 피드백을 통해 성숙도를 최적화하는 구조를 다음과 같이 제시한다.

### (1) 준비 단계

준비 단계에서는 현재 기업의 상황과 수준을 정확하게 파악하고 평가하는 것을 목표로 한다. 이 단계는 제로트러스트 아키텍처를 도입하는 첫 단계이기도 하지만 도입하여 운영 중인 제로트러스트 아키텍처 및 관련 솔루션에 대해 더 높은 수준으로 성숙도를 갖도록 하는 준비 단계이기도 하다. 준비 단계에서는 기관 혹은 기업에서 현재 사용 중인 기업망에 접근 주체, 자산 및 기기와 워크플로우를 점거하고 정확히 식별하여 제로트러스트 성숙도 수준을 정량적으로 평가할 수 있도록 해야 한다. 평가 대상은 다음과 같다.

#### 1) 접근 주체

첫 번째 평가 대상은 접근 주체이다. 이는 사용자뿐만 아니라 리소스와 상호작용

하는 모든 접근 주체를 포함한다. 이 단계에서는 접근 주체에 대한 식별 정보와 인증 방법 등을 점검하여 명확히 파악하고, 각 주체를 분류한 후 접근 주체 그룹에 따른 인증 방법 및 접근제어 정책을 검토한다. 특히, 많은 리소스에 접근이 가능한 개발자 및 시스템 관리자와 같은 특수 권한 사용자에 대해서 최소한의 권한만을 부여하여 횡적 이동이 불가능하게 해야 한다.

2) 자산 및 기기 식별

사용자 및 기기를 관리하고 강력한 인증을 요구하는 것은 제로트러스트 아키텍처의 주요 요소이다. 따라서 사용자부터 조직 리소스에 접근하는 기기 중 조직이 등록한 기기와 그렇지 않은 기기를 식별할 수 있어야 한다. 조직은 자산을 하드웨어와 소프트웨어 컴포넌트 모두 포함하여 관리해야 하며, 이를 통해 리소스에 접근하는 기기를 식별하고 강력한 인증을 적용해야 한다.

3) 비즈니스 프로세스 및 워크플로우

기업 내부의 비즈니스 프로세스와 워크플로우를 평가하는 과정은 접근 주체가 리소스에 접근 시 허용 혹은 거부를 결정하는 정책의 근거이다. 제로트러스트 도입 과정에서 문제가 있을 시 기업에 미치는 영향도가 적기 때문에 위험도가 낮은 프로세스부터 시작하는 것이 안전하다. VPN을 통해 기업망에 접근하지 않고 기업의 리소스에 접근하는 사용자에 대해 접근 전에 정책을 적용하는 것이 용이해지기 때문에, 클라우드 기반 혹은 원격 근무 환경에서의 적용이 특히 효과적일 수 있다. 리소스에 대한 성숙도 수준을 평가할 때 다음과 같은 사항들을 중심적으로 고려해야 한다. 소프트웨어 정의 네트워크 등 네트워크 추상화 및 세밀한 분할 기술, 패킷 검사 및 동적 필터링과 암호화 패킷 분석 등 위협 대응 기술, 네트워크 암호화 기술, 온프레미스 및 클라우드 시스템에서 계정 관리와 접근 통제 기술, 응용 및 워크로드 접근에 대한 중앙집중적 인증과 실시간 위험 분석, 응용 개발 및 배포에 대한 DevSecOps 등 적용, 자동화된 데이터 분류와 위험 기반 동적 접근제어 정책, 민감한 데이터의 암호화 기술, 중요 정보 태깅 등이 있다.

(2) 계획 단계

계획 단계는 제로트러스트 아키텍처 도입을 위한 사용자와 자산, 비즈니스 프로세스 및 워크플로우에 대한 평가 후에 계획을 세우고 설계하는 단계이다. 이 단계

에서는 비즈니스 프로세스나 핵심 요소를 선정하고, 그 중요성과 관련한 접근 주체와 리소스의 현황을 파악하여 정책을 수립하여야 한다. 현재 도입된 제로트러스트 아키텍처 기술에 대한 성숙도 수준을 정책에 반영하는 것은 중요하다. 비즈니스 프로세스가 선정된 후 관련된 자산과 워크플로우를 식별하면, 해당 워크플로우에 연관된 모든 리소스와 접근 주체를 명확하게 파악해야 한다. 연관된 접근 주체와 리소스 범위가 넓지 않은 프로세스부터 하는 것이 도입 과정에서 상대적으로 용이할 수 있다. 조직 관리자는 신뢰도 평가 알고리즘을 고려해 해당 프로세스가 사용하는 기준 혹은 중요도에 따른 가중치나 점수를 결정해야 한다. 이 과정에서 정상 사용자가 리소스 접근이 제한되거나 비정상 사용자가 리소스 접근 제한되거나 비정상 사용자가 접근하는 상황을 최소화하기 위해 도입 및 운영 단계에서 지속적으로 조율해야 한다.

(3) 구현 단계

구현 단계에서는 여러 배치 모델을 검토하고, 유스케이스에 맞는 솔루션을 선택한다. 솔루션을 선택하고 제로트러스트 아키텍처를 구현 및 도입하는 과정에서 다음과 같은 사항들을 고려해야 한다. 먼저, 선택한 솔루션이 제로트러스트 아키텍처의 기본 원리를 준수하는지를 확인해야 한다. 예를 들어, 리소스에 접근하기 위해서는 반드시 강력한 인증을 통해 접근 주체의 신뢰도를 명시적으로 확인한 후에만 접근이 허용되는지 검토해야 한다. 또한, 기기에 에이전트와 같은 소프트웨어 컴포넌트를 설치하는지, 다양한 기기를 지원하는지, BYOD나 외부 사용자 기기에 에이전트 설치가 가능한지도 고려해야 한다. 그 외에도, 해당 솔루션이 비즈니스상의 리소스 위치를 클라우드, 온프레미스 등에서 모두 또는 부분적으로 지원하는지 확인해야 한다. 분석을 위한 로그 및 모니터링 정보를 주고받거나, API를 제공하는지도 중요한 고려 사항이다. 다양한 응용 프로그램, 서비스, 프로토콜을 지원하며, 특정 서비스나 프로토콜 상에서 세밀한 접근제어가 가능 여부도 검토해야 한다. 마지막으로, 강화된 정책이 사용자 및 기기의 행위에 영향을 미치는지, 그리고 사용자의 편의성이 유지되는지도 주요 고려 사항이다.

(4) 운영 단계

운영 단계는 제로트러스트 솔루션이 도입되어 특정 비즈니스 프로세스에 대한 제로트러스트 아키텍처 보안 모델이 구현되는 단계이다. 이 단계에서 관리자는 도입

된 솔루션을 기반으로 정책을 설정하고 시행해야 한다. 이 과정에서 정상 사용자가 필요한 리소스에 접근이 거부되거나, 일부 사용자에게 과도한 권한이 부여되는 등의 문제가 발생할 가능성이 있다. 한 번에 완벽한 정책을 시행하는 것은 일반적으로 어려운 일이다. 정책 시행 중 민감한 문제가 발생할 수 있다면, 리포팅만 수행하는 모드로 운영하는 방법도 고려할 수 있다. 리포팅만 수행하는 방식은 인증 실패 시 접근을 거부하는 기본적인 정책을 제외하고 대부분의 접근 요청을 허용하며, 접속 로그를 분석하여 최초에 수립된 정책과 비교하는 방식을 의미한다. 하지만 리포팅만 수행하는 시범 운영이 보안이나 조직 정책상 불가능한 경우에는 조직 운영자가 로그를 모니터링하면서 비정상적인 접근이 이루어지는지를 확인해야 한다. 만약 문제가 발견될 시, 접근제어 정책의 지속적인 수정으로 운영을 개선해야 한다.

(5) 피드백 및 개선 단계

시범 운영이 성공적으로 마무리되면, 관리자는 제로트러스트 솔루션을 정식 운영하게 된다. 이 과정에서 솔루션은 성숙도에 맞춰 사용자, 자산, 네트워크를 모니터링하며 로그를 기록한다. 필요시 접근제어 정책을 조정할 수 있지만, 이는 기업망 전체에 영향을 주지 않도록 주의해야 한다. 운영 중에는 이해관계자의 피드백을 받아 개선해야 하며, 이를 통해 다음 단계의 성숙도를 높이는 계획을 세울 수 있다. 또한, 비즈니스 프로세스, 워크플로우, 접근 주체의 변화, 기업 내부 정책 혹은 법률 등의 변화에 따라 운영 방식을 수정할 필요시에는 현재 프로세스에 대한 중요한 개선을 이룰 수 있다.

# Ⅳ. 금융권 제로트러스트 구현 방안

## 1. 금융권의 보안 환경 특성

금융권 망분리 규제는, 2013년 ‘3.20. 사이버테러’ 사건으로 인해 국내 일부 은행의 전산 서비스가 중단된 것을 계기로 금융권의 보안을 강화하기 위한 대책으로 도입되었다. 이러한 망분리 규제는 여러 사이버 위협으로부터 금융시스템을 안전하게 보호하였지만 [14], 급격하게 변화하는 IT 환경에서 디지털 신기술 도입을 방해하는 걸림돌로 작용한다는 의견도 제기되었다. 이에 따라 금융위원회가 「금융 부문 망분리 T/F」를 개최하며 망분리 개선에 대한 의논이 본격화되었고, 마침내 2024년 8월 금융위원회에서 ‘금융 분야 망분리 개선 로드맵’을 발표하였다. 개선

로드맵에서는 생성형 AI를 활용하여 가명 정보까지 처리할 수 있도록 허용하여 활용 범위를 넓히고, 업무망에서의 데이터 범위, 프로그램 유형, 단말기 유형에 대한 SaaS 활용 범위를 대폭 확대하며, 연구 및 개발망과 업무망 간의 논리적 망분리 허용 및 결과물을 망간 이동을 허용하도록 개선하였다. 이를 통해 신기술을 도입함으로써 업무 생산성이 향상되고, 금융 데이터의 활용 또한 증가하여 금융산업 전반의 경쟁력이 크게 강화될 것으로 기대된다 [15, 16]. 그러나 한편으로는 데이터 유출 위험이나 사이버 공격 대상 확대 등의 보안 위협이 우려되는 상황이다 [17].

해외 사례를 살펴보면, 최근 은행업 대상 랜섬웨어 공격 피해가 급증하고 있다. 또한 공급망을 통하여 간접 침투하는 특성을 보이고 있으며, AI 기반으로 한 사이버 공격 등이 증가할 것으로 예상된다.

서비스형 랜섬웨어(RaaS)의 보편화 [18] 등으로 금융기관에 침투한 랜섬웨어의 비중은 2022년에 비해 45%나 급증하였다. 2023년 11월, 중국공상은행의 뉴욕 지점이 랜섬웨어 공격을 받아 채권 거래 관련 장애가 발생해 25조 달러 규모의 미국 국채 시장이 중단되면서 시장의 혼란을 유발하고 유동성에도 영향을 미쳤다. 이에 미국 정부는 랜섬웨어의 심각성을 인식하고 국제적 공조에 착수하게 되었다 [19].

은행 업무의 디지털화와 제삼자 서비스 공급업체에 대한 의존도가 높아지면서 공급망 침투를 통한 공격이 증가하고 있다. 공급업체의 낮은 보안 수준을 이용한 고객 데이터 유출과 은행 시스템 접근 공격이 증가하고 있으며, 기술 기업과의 협력으로 신속한 대응이 어려워지고 있다. 또한 2023년 2월, BofA에서는 채권추심 협력업체인 NCB Management의 시스템에서 자사 고객 190만 명의 정보가 유출되는 사건이 발생하였다. 2023년 9월에는 미국 지역은행 Northfield Bank가 제삼자 공급업체의 고객 데이터 유출 사고를 당국에 보고한 바 있다. 호주 은행 Latitude Financial의 경우, 2023년 3월 서비스 제공기업을 통해 자사 직원의 로그인 자격 증명이 해킹당하면서 거래 고객의 개인정보가 탈취당해 호주 내 최대 규모의 데이터 유출 사고가 발생하였다. 이와 관련하여 연준 및 ECB를 비롯한 주요국의 금융 규제 당국은 제삼자 위험의 효과적인 관리를 위한 지침을 채택하였으며, FSB도 공급망 위험 관리 지침을 마련해 각국에 제공하였다 [19].

AI는 사이버 공격을 자동화하여 빈도를 높이고, 기존 데이터와 보안 시스템을 학습하여 더욱 효율적이고 정교한 공격을 가능하게 한다. 피싱 공격과 딥페이크를 통한 신원 확인 회피 등 다양한 공격 가능성이 있다. 2024년 2월 초, 홍콩에 있는 다국적 기업의 재무 담당자가 영국 본사 CFO를 비롯한 임직원들과의 화상회의 이후

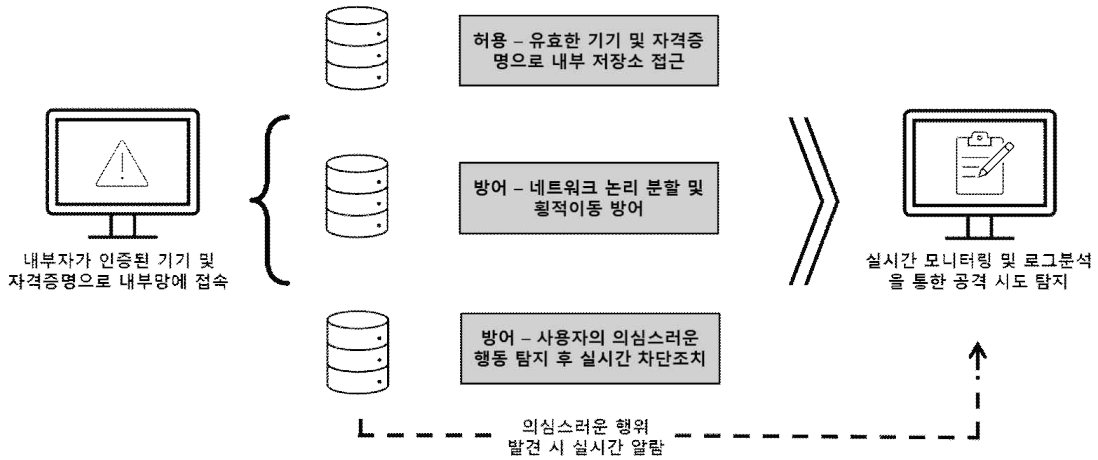
2억 홍콩달러를 송금했으나, 이는 딥페이크 사기로 확인되었다. 최근 아시아, 특히 태국과 베트남을 중심으로 은행 및 정부기관을 사칭하여 동영상 녹화를 유도함으로써 얼굴 분석 데이터를 수집하고, 딥페이크 기술로 금융기관의 안면 인식 보안 조치를 우회하는 'GoldPickaxe'라는 악성코드에 노출되었다. 생성형 AI 활용 증가로 사이버 공격 전술이 빠르게 변모할 가능성이 높아, 금융기관이 직면한 위협의 범위와 복잡성이 크게 증가할 우려가 있다 [19].

이러한 공격 사례들은 더 이상 해외에만 해당하는 내용이 아니다. 국내도 망분리 규제가 완화됨에 따라 인터넷망을 통한 공격은 월등히 증가할 것이다. 망분리로 효과적인 방어를 해왔던 공급망 침투 공격, 이메일을 이용한 악성코드 공격이나 랜섬웨어 공격 등은 국내 금융권 입장에서는 새로운 위협일 것이다. 금융위원회는 이에 따른 보안 리스크를 최소화하고자 로드맵을 작성하여 단계적인 망분리 규제 완화를 추진 중이며, 마지막 단계에서는 자율보안 체계 확립을 목적으로 하고 있다. 이에 따라 조직은 자체적으로 내부에 더 높은 수준의 보안 체계가 요구된다.

위와 같이 국내 금융기관은 단계적 망분리와 함께 자율보안 체계 구축을 준비해야 한다. 미국은 빅테크들이 클라우드에 투자하며 제로트러스트에 맞춰 보안을 강화하고 있다 [20]. 제로트러스트는 국내에서 금융권의 보안을 책임져 온 망분리를 대체할 것으로 기대받고 있다 [21]. 이에 따라 금융권에서 도입할 수 있는 가장 안전한 자율보안 체계로 제로트러스트 모델을 제안한다. 제로트러스트 모델은 금융권에서 모든 접근 요청을 지속적으로 검증하여 내부자 및 외부 위협을 방지하고, 민감한 데이터를 보호하며, 규제 준수를 강화하는 데 효과적이다. 또한, 위협이 발생하더라도 빠르게 탐지하고 차단할 수 있어 보안성을 높일 수 있다. 이를 통해 망분리 완화로 효율적인 업무 및 신기술 활용의 이점을 가져오면서, 금융권에 대한 전체적인 보안 리스크를 효과적으로 낮출 수 있다.

## 2. 금융권의 보안 위협 시나리오와 대응 방안

### (1) 내부자 유출



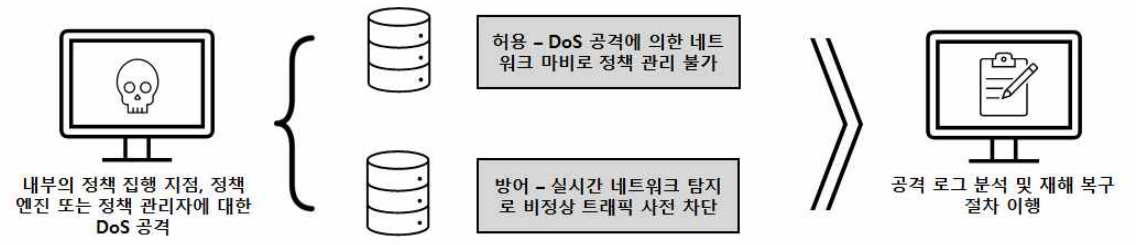

**<그림 4> 내부자 유출 시나리오**

내부자가 자신의 권한을 악용하거나 혹은 실수로 중요한 고객 데이터를 유출하는 경우 다음과 같이 대응할 수 있다. 공격 발생 전, 금융기관은 지속적인 모니터링과 감시 체계를 구축하여 이상 행위를 실시간으로 감지하고 이를 차단해야 한다. 또한 직원이 업무를 수행하기 위해 필요한 최소한의 접근 권한만을 부여함으로써 유출 위협을 최소화하는 것이 중요하다. 예를 들어, 특정 직원을 제외한 나머지 직원에 대해서는 데이터 다운로드 권한을 제한하거나, 다른 곳으로의 데이터 전송 차단 등의 조치를 취할 수 있다. 그리고 세밀한 보안 정책을 설정하고 이를 통해 접근제어를 수행함으로써 데이터에 대한 불필요한 접근을 막아야 한다. 더불어, 소프트웨어 정의 경계를 설정하여 업무 범위와 중요도에 따라 리소스를 분류 및 배치하여 만약 유출이 발생하더라도 유출되는 데이터의 양을 최소화해야 한다.

내부자가 데이터에 접근하여 실시간으로 데이터가 유출되는 경우에는, 다음과 같이 대응할 수 있다. 접속 시간, 기기 상태 등의 다양한 요소를 고려한 정책 결정을 통해 평소와 다른 의심스러운 접근을 필터링해야 한다 [22]. 더 나아가 리소스에 접근하는 사용자의 모든 상태를 지속적으로 모니터링한다. 이를 통해 평소와 다른 행동이나 의심스러운 상태를 감지함으로써 접근을 동적으로 관리하는 것이 중요하다. 뿐만 아니라, 의심스러운 접속에 대해서는 세션을 바로 차단해야 한다. 한번 세션을 차단당함에도 불구하고 지속적으로 접근을 시도하거나 이상 행동이 감지되면 해당 계정을 차단하는 정책 또한 필요하다. 또한 비인가 프로그램 설치 시도를 차단하고, 마이크로 세그멘테이션을 통해 작업 범위를 세분화하여 피해가 다른 구역으로 확산되지 않도록 해야 한다.

금융기관이 중요 데이터의 유출을 확인한 후에는 다음과 같이 대응할 수 있다. 데이터 세그먼트 세분화와 정책 강화를 통해 제로트러스트 보안을 더욱 강화해야 한다. 이와 함께 로그 분석과 SIEM을 활용하여 비정상 접속 시도를 확인하고 정밀 분석을 수행하며, 피해가 발생한 부분을 점검하고 백업 데이터를 통해 복구를 진행해야 한다. 마지막으로, 탈취당한 기기 및 자격 증명을 초기화하고 재설정하여 추가적인 피해를 방지하는 조치를 취해야 한다.

(2) DoS




<그림 5> DoS 시나리오

공격자가 금융기관의 정책 집행 지점, 정책 엔진 또는 정책 관리자에 대한 DoS 공격을 수행하려는 경우 다음과 같이 대응할 수 있다. 네트워크와 시스템에 대한 DoS 방어 솔루션을 미리 배포하여 공격을 사전에 차단하며, 정상 트래픽을 보안 정책으로 설정하고 이를 기반으로 비정상적인 트래픽을 감지해야 한다. 또한 지속적인 모니터링을 통해 DoS 공격을 탐지하고, 공격 탐지 시 동일 전송자의 트래픽을 차단하는 정책을 설정하는 등의 조치를 취해야 한다.

DoS 공격으로 정책을 통한 접근제어가 정상적으로 수행되지 않는 경우에는, 다음과 같이 대응할 수 있다. 네트워크 트래픽 모니터링을 통해 이상 트래픽 혹은 공격 시도를 실시간으로 탐지해야 한다. DoS 공격이 감지되면 자동으로 트래픽을 분산시키거나 해당 트래픽을 차단하는 등의 정책을 설정할 수 있으며, 트래픽 필터링을 위해 방화벽 및 IDS, IPS를 실시간으로 활용할 수 있다. 이와 함께 네트워크 장애로 인한 서비스 중단을 최소화하기 위해 미리 준비된 재해 복구 절차를 신속하게 실행한다. 이 외에도 클라우드 기반 DoS 방어 솔루션을 활용하여 공격 트래픽을 분산시키고 웹 애플리케이션 방화벽(WAF)을 통해 공격을 차단하는 등의 대응 조치를 취할 수 있다.

DoS 공격이 끝나고 정상 복구된 후에는 다음과 같이 대응할 수 있다. 공격 트래픽 로그를 분석하여 공격의 유형과 경로를 파악하고, 동일한 유형의 공격을 방어할 수 있는 정책을 설정해야 한다. 또한 재해 복구 절차의 실행 결과를 평가하고 복구 시간이 최적화되었는지 확인하고, 이에 따라 필요한 사항을 개선시켜 보안을 한층 강화한다. 더불어 공격 원인 및 경과를 분석하여 사후 보고서를 작성함으로써, 공격 시나리오와 대응 과정에서 발생한 문제점을 파악하고 개선점을 도출하도록 하는 과정도 필요하다. 공격 이후 DoS 방어 솔루션을 최신 상태로 유지하고, 추가적인 방어 기능 검토 및 도입해야 한다. 또한 관련 교육을 실시하여 같은 유형의 공격 발생 시 신속하고 효과적인 대응을 할 수 있도록 해야 한다.

(3) 공급망 공격


**<그림 6> 공급망 공격 시나리오**

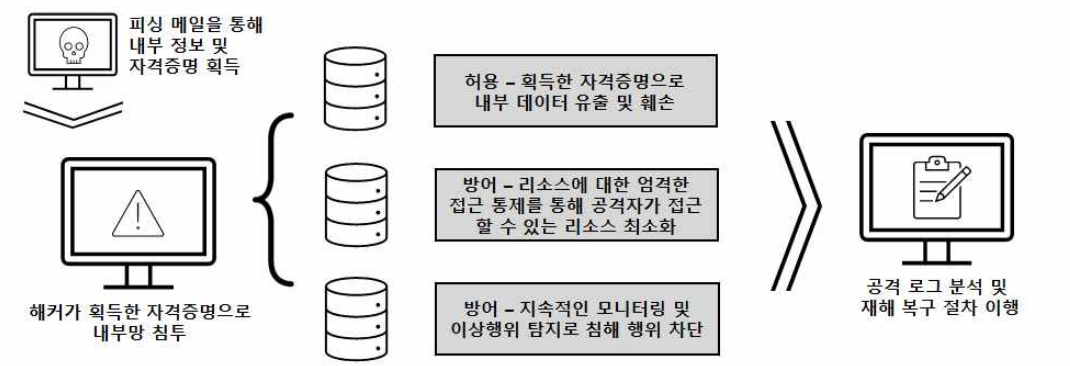
대형 은행의 온라인 뱅킹 시스템을 목표로 설정한 공격자는 해당 금융기관과 협력하고 있는 소프트웨어 공급업체 등을 침투하기 위해 사전 조사를 한다. 공격자가 네트워크상에서 인증정보를 확보하거나, 관리자의 권한을 획득하는 등의 방법을 통해 더 많은 서버와 PC의 권한을 획득할 수 있다. 이에 대한 대응 방법으로 금융기관은 최소한의 접근 권한만을 부여하여 접근할 수 있는 네트워크를 최소화하고 공격자가 더 많은 리소스에 접근하는 것을 방어한다. 또한, 업무에 필요한 사람이라 하더라도 기기 상태, 사용자 행동, 시간 등의 동적 요소를 고려하여 세밀한 접근 정책을 설정한다. 업로드되는 파일에 대해서도 기본적으로 신뢰하지 않는 접근 방식이 필요하다. 공격자는 파일 업로드 취약점을 통해 초기 침투를 시도하는 경우가

많으므로, 악성코드 여부를 검증하고, 파일을 업로드하는 사람에 대해서도 최소한의 접근 권한만을 부여하여 실행 파일 업로드를 차단해야 한다.

공격자가 제휴사의 소프트웨어 업데이트나 패치에 악성코드를 삽입하여 고객의 민감한 정보에 접근하는 경우에는 다음과 같이 대응할 수 있다 [23]. 접근제어가 중요하며, 특히 정책에서 접근을 허용하는 특정 인원을 제외한 모든 사람에 대해 중요 정보가 담긴 파일 접근을 제한하고, 지속적인 접근 시도가 발견될 시 세션 차단 및 해당 기기를 차단하는 조치를 취해야 한다. 정상적인 기기에 정상으로 배포된 프로그램이라 하더라도 기본적으로 신뢰하지 않으며, 권한을 최소화하는 방안을 적용하여 피해를 최소화해야 한다. 또한, 세션 차단 기능을 구현하여 일정 시간이 지나면 세션을 차단함으로써 공격자의 지속적인 공격을 방어할 수 있도록 한다. 지속적인 모니터링을 통해 파일 업로드 중 실시간으로 파일을 분석하고, 격리된 환경에서 먼저 파일을 실행하여 위험이 감지되면 즉시 실행을 중지하고 삭제한다. 네트워크 감시 도구를 통해 비정상적인 트래픽을 감지하거나 악성코드 탐지를 통해 경고를 발송하며, 모든 사용자와 장치의 접근 권한을 지속적으로 관리하여 권한이 없는 접근을 차단한다.

보안 팀에서 고객 데이터가 유출된 것을 확인한 후에는 다음이 같이 대응할 수 있다. 로그 분석 및 보안 정책 강화를 통해 파일 업로드 및 권한 획득과 관련하여 공격자의 모든 로그를 분석하여 정책을 강화해야 한다. 보안 정보 및 이벤트를 수집하여 해당 공격에 대한 보안 정보를 분석하고, 이를 통해 정책을 강화해야 한다. 또한, 지속적인 네트워크 모니터링을 통해 원격 접속 공격 명령 및 통제 시도를 원천 차단하는 노력이 필요하다.

(4) APT 공격




<그림 7> APT 공격 시나리오

공격자가 중요한 디지털 자산이 있는 금융기관을 공격 목표로 정한 후 조직에 관한 조사를 수행한다. 조직 구조 및 기술 인프라에 대한 세부 정보를 확보하고 직원 정보를 분석하여 피싱 이메일을 전송하여 내부망 침투를 시도한다. 이러한 공격에 대한 대응 방안은 다음과 같다. 금융기관은 공격자가 내부망에 침투하더라도 접근할 수 있는 리소스를 최소화하기 위해 소프트웨어 정의 경계를 설정하여 각 세그먼트에 최소한의 리소스만을 배치해야 한다. 그리고 등록되지 않은 사용자 및 기기에 대한 접근을 원천적으로 차단함으로써 엄격한 접근 통제를 수행해야 한다. 또한 직원들이 공격자의 피싱 메일을 통한 공격을 효과적으로 대응할 수 있도록 지속적인 사내 보안 교육 및 훈련이 필요하다.

공격자가 침투한 내부망에 상주하며 상위 권한을 획득하고 민감한 고객 데이터를 수집 및 탈취하는 경우에는, 다음과 같이 대응할 수 있다 [24]. 리소스에 대한 엄격한 접근 통제를 수행함으로써 공격자가 접근할 수 있는 리소스를 최소화한다. 지속적으로 사용자의 행동을 모니터링하고 로그를 분석하여 승인되지 않은 상위 권한 획득과 이상 행위를 감지하면 그 즉시 대응 조치를 취한다. 이 외에도 일정 시간 만료 시 세션을 차단하여 공격자가 내부망에 상주하는 것을 막고, 항상 공격자가 내부망에 존재한다는 가정 하에 세밀한 접근제어가 필요하다.

내부 침투를 식별하여 공격자가 고객 데이터에 접근한 사실을 발견한 후에는 다음과 같이 대응할 수 있다. 공격자의 내부망 침투 및 상위 권한 획득과 관련한 모든 로그를 수집 및 분석한다. 그뿐만 아니라, 보안 정보 및 이벤트로서 해당 공격과 관련된 모든 보안 정보를 수집하고 이를 분석하여 공격자가 어떤 방식으로 공격을 수행했는지 파악함으로써 향후 다시 발생할 수 있는 APT 공격에 대비해야 한다. 더불어 분석된 내용을 바탕으로 접근제어 정책을 개선하여 보안을 더욱 강화해야 한다.

**<표 3> 금융권 위협 시나리오 및 제로트러스트 대응 방안**

| 위협 | | 시나리오 | 대응 방안 |
|---|---|---|---|
| 내부자 유출 | 공격 전 | 금융기관 내에서 직원이 자신의 권한을 악용하여 중요한 고객 데이터를 유출하려는 악의적인 행동을 할 수 있음. | - 지속적인 모니터링 및 감시<br>- 접근 권한 최소화<br>- 소프트웨어 정의 경계 설정<br>- 철저한 보안 정책으로 민감 데이터 접근 차단 |
| | 공격 중 | 내부자가 기업의 중요한 | - 시간. 기기 상태 등을 고려해 의심스러운 접근 필터링 |

| | | | |
|---|---|---|---|
| | | 데이터를 유출하는 악의적인 행동을 하고 있음. | - 지속적인 모니터링으로 의심 행동 감지 시 접근 관리<br>- 의심 상황 시 세션 종료 및 지속 이상 행동 시 계정 차단<br>- 비인가 프로그램 설치 시도 차단<br>- 마이크로세그멘테이션으로 피해 확산 방지 |
| | **공격 후** | 기업 내부의 고객 데이터가 외부로 유출된 것을 확인하였음. | - 사후 로그 분석 및 내부자 보안 강화<br>- 대응 조치 및 보안 강화<br>- 로그 분석, SIEM 등으로 비정상 접속 시도 확인 및 정밀분석<br>- 피해 발생한 부분 점검 및 백업데이터로 복구<br>- 탈취당한 기기 및 자격증명 초기화 및 재설정 |
| **DoS** | **공격 전** | 공격자는 금융기관의 정책집행지점(예: 방화벽, 접근제어시스템), 정책 엔진(보안 정책을 관리하는 시스템), 또는 정책 관리자(관리자 계정)에 대한 DoS 공격으로 관리자 계정이 정책을 통한 접근제어를 제대로 수행하지 못하도록 하려고 함. | - DoS 방어 솔루션 사전 배포<br>- 재해 복구 절차 수립 및 정기 테스트<br>- 지속적인 모니터링을 통해 DoS 탐지<br>- 트래픽을 차단하는 정책 설정 |
| | **공격 중** | 공격자는 금융기관의 정책 집행 지점, 정책 엔진, 또는 정책 관리자에 대한 DoS 공격으로 관리자 계정이 정책을 통한 접근제어를 제대로 수행하지 못하도록 하고 있음. | - 실시간 트래픽 모니터링으로 이상 탐지<br>- DoS 공격 시 자동 트래픽 분산 및 차단 (예: 비정상 트래픽 필터링, 신뢰 트래픽만 허용)<br>- 네트워크 장애 시 재해 복구 절차로 서비스 중단 최소화<br>- 클라우드 DoS 방어 솔루션과 WAF로 공격 차단 |
| | **공격 후** | DoS 공격이 끝나고 트래픽이 정상 복구되었음. | - 공격 후 트래픽 로그 분석으로 대비책 강화<br>- 재해 복구 절차 평가 및 개선<br>- 사후분석 보고서 작성으로 문제점 파악 및 개선<br>- DoS 방어 솔루션 최신화 및 추가 기능 도입<br>- 관련 팀 교육으로 대응 역량 강화 |
| **공급망 공격** | **공격 전** | 공격자는 대형 은행의 온라인 뱅킹 시스템 등을 목표로 설정하여 타겟 금융기관과 협력하고 있는 소프트웨어 공급업체 등을 사전 조사함. | - 최소한의 접근만 허용해 네트워크 확장 방어<br>- 중요한 데이터 접근은 최소 인원으로 제한하고, 동적 요소(기기 상태, 사용자 행동, 시간 등) 고려해 정책 수립<br>- 업로드 파일은 신뢰하지 않고, 악성코드 검증과 실행 파일 업로드 차단 |
| | **공격 중** | 공격자는 제휴사의 소프트웨어 업데이트나 패치에 악성코드를 삽입하여 고객들의 민감한 정보에 접근한다. | - 특정 인원 제외, 중요 파일 접근 제한 및 시도 시 차단<br>- 정상 기기 및 프로그램 권한 최소화<br>- 일정 시간 후 세션 자동 차단<br>- 실시간 모니터링으로 파일 분석 및 위험 시 실행 중지 및 삭제<br>- 비정상 트래픽 및 악성코드 탐지 시 경고 |

| | | | |
|---|---|---|---|
| | | | - 접근 권한 주기적 검토 및 무권한 차단 |
| | **공격 후** | 보안팀에서 고객 데이터가 유출된 것을 확인했다. | - 파일 업로드 및 권한 획득 관련 로그 분석 후 정책 강화<br>- 공격 관련 보안 정보 수집으로 정책 강화<br>- 원격 접속 공격 명령/통제 시도 차단을 위한 지속적 모니터링 |
| **APT 공격** | **공격 전** | 공격자는 소셜 엔지니어링 기법을 이용해 금융기관 직원들을 대상으로 피싱 이메일을 전송하여 로그인 정보를 탈취하고, 공식 웹사이트와 소셜 미디어를 분석하여 조직 구조 및 기술 인프라에 대한 세부 정보를 확보한다. | - 각 세그먼트에 최소 리소스 배치로 내부망 침투 시 피해 최소화<br>- 엄격한 접근 통제 필요<br>- 지속적인 사내 교육으로 내부자 피싱 대응 능력 향상 |
| | **공격 중** | 공격자는 내부망에 침투하여 계속 머물며 탐색, 상위 권한을 획득하여 민감한 고객 데이터를 수집 및 탈취한다. | - 접근 통제로 미등록 사용자 및 기기 차단<br>- 모니터링과 로그 분석을 통해 이상 행동 감지 시 대응 조치<br>- 일정 시간 후 세션 만료로 공격 방어<br>- 내부 침입 가정하고 세밀한 접근제어 필요 |
| | **공격 후** | 내부 침투를 식별하여 공격자가 고객 데이터에 접근한 사실을 발견하였다. | - 보안 정보 및 이벤트에 해당 공격에 대한 보안 정보를 수집하여 정책 강화<br>- 로그 분석을 통해 내부망 침투 및 권한 획득 관련 정책 강화 |

# Ⅴ. 결론 및 시사점

최근 금융권에서 보안 위협이 증가하면서 기존의 경계 기반 모델의 한계가 드러나고 있다. 특히 망분리 제도가 완화되면서 금융 시스템의 경쟁력은 높아질 것으로 기대되지만, 이에 따른 보안에 대한 우려의 목소리도 나오고 있다. 이러한 상황에서 제로트러스트 아키텍처는 모든 접근을 의심하고 검증함으로써 금융 시스템의 보안을 강화할 수 있는 방안으로 주목받고 있다. 제로트러스트는 공격자가 네트워크 내외부 어디든 존재할 수 있다는 가정 하에 모든 접속 요구를 신뢰하지 않는다. 또한 리소스의 접근에 대한 강력한 인증을 요구하며 최소한의 권한만을 부여한다. 이를 통해 기존의 경계 기반 보안 모델에서 발생할 수 있는 취약점을 보완하여 금융 시스템을 효과적으로 방어할 수 있다.

본 연구에서는 금융권에서 일어날 수 있는 위협 시나리오와 대응 방안을 기반으로  제로트러스트 아키텍처 도입 단계에 따라 정리하였다. 준비 단계에서는 재해복구 및 대응 절차를 강화해야 한다. 계획 단계에서는 중요한 데이터 접근 권한 최

소화, 미등록 사용자 및 기기 접근 차단, 다단계 인증(MFA) 적용 등 세밀한 보안 정책 및 접근제어를 적용해야 한다. 또한, 소프트웨어 정의 경계 구현과 네트워크 세그멘테이션을 설정해야 한다. 구현 단계에서는 실시간 모니터링 시스템 도입을 통해 이상 행위를 실시간으로 차단하는 것과 제안한다. 이와 함께 비인가 프로그램 설치를 차단하고 파일 업로드 및 실행 검증 절차를 강화해야 한다. 운영 단계에서도 실시간 모니터링과 이상 행위 차단이 이루어져야 하고, 백업 및 재해 복구 절차를 운영해야 하며, 정기적인 테스트를 통해 복구를 최적화해야 한다. 또한 운영 단계와 마지막 단계인 피드백 및 개선 단계에서 위협 발생 시, 사후 로그 분석과 보안 정책 강화 및 지속적인 개선이 필요하다.

본 연구는 금융권에서 보안 위협 시나리오를 바탕으로 제로트러스트 도입 방안을 제안하였다. 그러나 실질적으로 금융권에 제로트러스트를 도입하기 위해서는 법적 측면에서의 개선이 필요하다. 현재 국내에서 제로트러스트와 관련된 법적 제도는 미비한 상황으로 정책 관련 연구가 더 필요한 실정이다. 발전하는 신기술을 산업에 효과적으로 도입하기 위해서는, 법적인 측면에 대한 발전 또한 분명 필요하다. 따라서 향후 연구로는 금융권 제로트러스트 아키텍처 도입을 위해 필요한 정책 방안에 대해 연구하고자 한다.

# [참고문헌]

[1] 뉴시스, 공공 망분리 의무화 규제 확 푼다…관공서에서 PC 한대로 업무볼까 [Internet], Available: https://v.daum.net/v/20240807060149916, 2024.8.2.

[2] 보안뉴스, 당신의 개인정보는 안전한가요? '크리덴셜 스터핑' [Internet], Available: https://m.boannews.com/html/detail.html?idx=114255, 2024.8.2

[3] 이송희, 조원배, "제로 트러스트 기술 동향 및 사례 분석", 정보처리학회지, pp.25-26, vol 29, no 4, December 2022.

[4] National Institute of Standards and Technology, "Zero Trust Architecture", U.S. Department of Commerce, Gaithersburg, MD, NIST Special Publication 800-207, 2020.

[5] 과학기술정보통신부, 한국인터넷진흥원, et.al., "제로트러스트 가이드라인 1.0 요약서", 2023.

[6] Forrester, The Definition Of Modern Zero Trust [Internet], Available: https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/, 2024.8.21.

[7] Google, "Applying Zero Trust on Google Cloud" [Internet], Available: https://services.google.com/fh/files/misc/zt_implem_guide_800_27.pdf, 2024.8.21.

[8] 과학기술정보통신부, 한국인터넷진흥원, et.al., "제로트러스트 가이드라인 1.0", 2023.

[9] Forrester, Zero Trust Security Means Business: Then And Now [Internet], Available: https://www.forrester.com/zero-trust/, 2024.8.28.

[10] Microsoft, Set up your Microsoft Zero Trust security model [Internet], Available: https://setup.cloud.microsoft/security/zero-trust-setup-guide, 2024.08.28

[11] SAP, RISE with SAP: Adopting to Zero Trust Architecture Principles with SAP Cloud Services [Internet], Available: https://community.sap.com/t5/technology-blogs-by-sap/rise-with-sap-adopting-to-zero-trust-architecture-principles-with-sap-cloud/ba-p/13544003, 2024.08.28.

[12] U.S. Department of Defense, "Department of Defense Zero Trust Overlays", Chief Information Officer, Washington D.C., 2024.

[13] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model, Version 2.0", U.S. Department of Homeland Security, Washington D.C., 2023.

[14] 법무법인 세종, 금융사도 생성형 AI를 활용할 수 있도록, 망분리 규제가 완화될 예정입니다 [Internet], Available: https://www.shinkim.com/kor/media/newsletter/2533, 2024.8.23.
[15] 금융위원회, 금융감독원, “금융분야 망분리 개선 로드맵”, 2024.
[16] 금융위원회 보도자료, “변화된 IT환경의 망분리 규제 합리화를 위한 「금융부문 망분리 T/F」 1차 회의 개최”, 2024.4.12.
[17] 전자신문, [송민택 교수의 핀테크 4.0] 망분리 규제 개선의 의미와 전망 [Internet], Available: https://m.etnews.com/20240826000140, 2024.8.26.
[18] 법률신문, 금융보안 환경 변화와 정보보호 [Internet], Available: https://www.lawtimes.co.kr/LawFirm-NewsLetter/185462, 2024.8.26.
[19] 김세나, 이상원, “글로벌 은행산업의 사이버 공격 특징 및 시사점”, 국제금융센터, 서울, 2024.
[20] 네이트 뉴스, 보안 명목 망분리 규제 10년・・・AI혁신 막고 되레 비효율성 키워 [Internet], Available: https://m.news.nate.com/view/20240501n19778, 2024.8.26.
[21] 아이티데일리, [시장동향] VPN・망분리 넘어 ‘제로트러스트’ 본격 도입 기대 [Internet], Avaliable: http://www.itdaily.kr/news/articleView.html?idxno=220044, 2024.8.26.
[22] 홍기완, “제로트러스트 보안환경을 위한 내부정보 유출행위 탐지 연구”, 박사학위, 중앙대학교, 서울, 2024.
[23] Thiago Melo Stuckert do Amaral, João José Costa Gondim, “Integrating Zero Trust in the cyber supply chain security”, 6th Workshop on Communication Networks and Power Systems (WCNPS 2021), pp.1-5, 2021.
[24] Bruno Carneiro da Rocha , Laerte Peotta de Melo, “Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model”, 6th Workshop on Communication Networks and Power Systems (WCNPS 2021), pp.2-3, 2021.