https://doi.org/10.33778/kcsa.2023.23.1.009

제로 트러스트 명문화를 통한 신 보안체계 강화 방안 연구 - 전자금융거래법상 법적 개선을 중심으로 -

이 민 원*, 권 헌 영*

요 약

코로나19로 재택근무가 일상이 되면서 비대면 환경에서 안전한 보안인 제로 트러스트 개념이 주목받고 있다. 미국 바이든 대통령은 2021년 5월 국가 사이버보안 개선에 대한 행정명령에서 제로 트러스트 도입을 강조하였으며, 제로 트러스트는 글로벌 트렌드로 자리잡고 있다. 그러나 현재 우리나라에서 제로 트러스트와 같은 신기술 도입• 활용에 가장 어려움이 있는 부분은 클라우드 및 망 분리의 과도한 규제로, 이에 대하여 전자금융거래법상 클라우드 및 망 분리 규제 개선이 2023년 시행을 앞두고 있으나 전통적 경계 보안 모델에 기반을 두며, 비대면 환경으로 인한 새로운 정보보호 통제를 모두 반영하지 못하는 한계점을 가지고 있다. 특히, 정부의 망 분리 완화 정책이 실효성이 있는 정책이 되기 위해서는 제로 트러스트 명문화가 필수적이라고 판단된다. 따라서 본 논문에서는 전자금융거래법상 제로 트러스트 개념을 반영하는 법적 개선을 연구하고자 한다.

A study on ways to strengthen the new security system through the stipulation of zero trust : legal improvement under the Electronic Financial Transactions Act

Min-won Lee*, Hun-yeong Kwon**

ABSTRACT

Due to COVID-19, the concept of Zero Trust, a safe security in a non-face-to-face environment due to telecommuting, is drawing attention. U.S. President Biden emphasized the introduction of Zero Trust in an executive order to improve national cybersecurity in May 2021, and Zero Trust is a global trend. However, the most difficulty in introducing new technologies such as Zero Trust in Korea is excessive regulation of cloud and network separation, which is based on the boundary security model, but is limited to not reflecting all new information protection controls due to non-face-to-face environments. In particular, in order for the government's policy to ease network separation to become an effective policy, the zero trust name culture is essential. Therefore, this paper aims to study legal improvements that reflect the concept of zero trust under the Electronic Financial Transactions Act.

Key words : Zero Trust Security, The New Security System, Electronic Financial Transactions Act, Cloud Computing, Network separation

접수일(2022년 10월 30일), 게재확정일(2023년 02월 05일)

* 고려대학교 정보보호대학원 석사과정(주저자)
** 고려대학교 정보보호대학원 교수(교신저자)

1. 서 론

1.1. 연구 배경 및 목적

코로나19로 인한 비대면 환경으로의 전환은 기업의 보안 환경에도 영향을 미치고 있다. 클라우드를 및 다양한 모바일 기기 등 다양한 환경/기기에서 대내 리소스에 접속하게 되면서, 물리적 경계는 불분명해졌고, 기존 경계 보안 모델을 사용하는 것도 어려워졌다. 이에 따라 우리나라 기업들은 새로운 환경에 적합한 제로 트러스트에 주목하게 되었다.

다만 기업들은 제로 트러스트 도입을 고려하고 있지만, 구체적인 기준 및 구현 방법이 정립되지 않아 도입에 어려움을 겪고 있다. 따라서 국가적 차원에서 제로 트러스트를 법적으로 명문화하여 적용 기준을 정립하고, 도입을 추진하는 것이 필요하다. 현재 제로 트러스트와 같은 신기술을 도입• 활용에 가장 어려움이 있는 부분은 클라우드 및 망 분리의 과도한 규제로, 이에 대하여 전자금융거래법상 클라우드 및 망 분리 규제 개선이 2023년 시행을 앞두고 있으나 전통적 정보보호 모델(경계 기반 모델)에 기반을 두며, 비대면 환경으로 인한 새로운 정보보호 통제를 모두 반영하지 못하는 한계점을 가지고 있다.

본 연구에서는 2023년 시행 예정인 전자금융거래법 고시에서 클라우드 및 망 분리 규제 완화 시 제로 트러스트 정책 명문화를 통한 보완의 필요성을 강조하고자 한다.

2. 이론적 배경

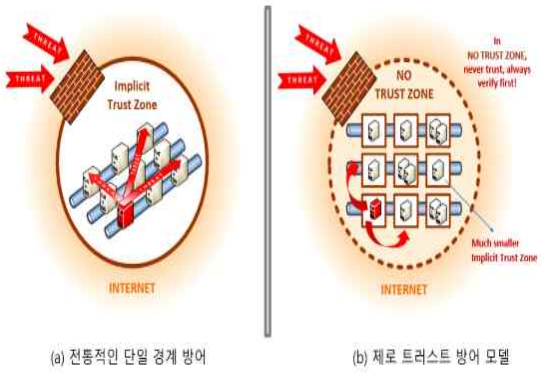
2.1. 제로 트러스트의 개념 및 전통적 보안 시스템의 한계점

제로 트러스트는 네트워크 경계와 관계없이 아무도, 그리고 어떤 활동이든 기본적으로 신뢰하지 않는 것에 바탕을 둔 보안 개념이다[1].

미국 국방부 제로 트러스트 참조 아키텍처(Department of Defense (DOD) Zero Trust Reference Architecture)[2]에 따르면, 제로 트러스트의 기본 원칙은 각 사용자, 장치, 애플리케이션 및 트랜잭션에 대한 지속적인 검증을 하는 것으로 인프라, 네트워크 및 데이터를 보호하는 방법에 대한 극적인 패러다임 전환이라고 표현한다[3].

반면 경계 보안 모델은 기본적으로 방화벽 및 IDS, IPS 등 불법 침입 탐지를 위한 보안 시스템을 통해 비인가자가 내부로 접근하는 것을 방지한다. 이 모델에서는 보안담당자가 회사 네트워크로 접속하는 모든 사용자와 단말기를 관리해야 하므로, 상시 취약점을 판단하고 신속하게 대응하는 것이 현실적으로 어렵다는 문제가 있다. 또한, 내부 네트워크를 무조건 신뢰한다고 판단하므로 내부자를 통한 데이터 유출 발생에 취약한 문제가 있다[4].

NIST는 전통적 방어 모델 및 제로 트러스트 방어 모델을 (그림 1)과 같이 비교하였다.



(그림 1) 네트워크 경계 기반의 전통적인 방어 모델 vs. 제로 트러스트 방어 모델 (출처 : nist.gov)

위 개념도와 같이 제로 트러스트는 악의를 품은 사용자는 항상 신뢰 구간 바깥에 있고, 신뢰 구간 안에 있는 사용자는 늘 믿을 수 있다는 기존의 경계 보안 모델과 대비된다. 모든 사용자가 신뢰할 수 없다고 간주되기 때문에 제로 트러스트의 접근은 매우 엄격한 제어 방식을 필요로 한다. 이를 위한 고도의 IAM(Identity and Access Management; ID 및 액세스 관리) 기능이 요구되며, 시스템에 접근하기 위해서는 접근 권한 등에서 유효성을 입증해야 한다[5].

2.2. 금융 분야 클라우드 및 망 분리 규제 개선의 주요 내용

기존 모델의 한계로 신기술 도입의 필요성이 제기되었으나, 클라우드, 망 분리 등 현행 금융보안 규제가 지나치게 엄격하여 적극적인 디지털 신기술 도입•활용을 통한 금융혁신을 저해한다는 의견이 지속적으로 제기되어 왔다. 이에 정부는 전문가 및 이해관계자 등의 의견을 청취하여 디지털 혁신을 위한 클라우드 및 망 분리 규제 개선방안을 마련하기로 결정했다. 현재 2022년 제도 개선사항을 반영한 전자금융거래법 시행령 및 감독 규정 개정안을 입법 예고된 상황이며, 조속한 개정을 통해 2023년부터 시행 예정이다[6].

2023년 시행 예정인 전자금융 감독규정 일부개정 고시 안 중, 망 분리 완화 관련 주요 내용은 아래 <표 1>과 같다.

<표 1> 전자금융감독규정 일부개정고시안
(망 분리 완화 관련 주요내용)

개정 전	개정 후
제15조(해킹 등 방지대책) 3. 내부통신망과 연결된 내부업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)	제15조(해킹 등 방지대책) 3. 내부통신망과 연결된 내부업무용시스템은 인터넷(무선 통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지. 다만, 다음 각목의 경우에는 그러하지 아니하다.
<신 설>	가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망 분리 대체 정보보호통제를 적용한 경우에 한한다) 나. 업무상 불가피한 경우로서 금융감독원장의 확인을 받은 경우
5. 전산실 내에 위치한 정보처리 시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리 할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)	5.전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부 통신망으로부터 물리적으로 분리할 것. 다만, 다음 각목의 경우에는 그러하지 아니하다. 가. 이용자의 고유식별정보또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망 분리 대체 정보보호통제를 적용한 경우에 한한다) 나. 업무 특성상 분리하기 어려운 경우로서 금융감독원장이 인정하는 경우

상기 위 <표 1>에서 제15조(해킹 등 방지 대책) 제3호의 가목에서, 망 분리 대체 정보보호 통제에 대하여 명시하고, 상세 내용은 <별표7>에 기술되어 있다. 다만 이는 전통적인 경계 모델을 상정하고 기재되어 있어, 다양한 접속 환경을 충분히 반영하고 있지 못하고 있다는 한계가 있는데, 현재 이러한 환경에서 가장 적절한 보안체계는 제로 트러스트로, 선진국에서는 이미 이러한 도입이 구체적으로 이루어지고 있으나, 우리나라의 경우 도입을 고려하는 수준이다. 후술하여 설명한다.

3. 미국 제로 트러스트 정책 및 국내 제로 트러스트 정책 현황

3.1. 미국 제로 트러스트 정책 현황

3.1.1. 사이버 보안 행정명령

2021년 5월 미국 조 바이든 대통령이 서명한 행정명령에는 연방정부와 클라우드 서비스 공급업체는 제

로 트러스트 보안 정책을 채택하고 각 기관장은 이를 구축하기 위한 계획을 수립하도록 명령하고 있다.
이에 따라 산하기관은 2024년 9월까지 '제로 트러스트' 네트워크 아키텍처를 채택할 준비를 하고 있으며, 미국 사이버 보안 및 인프라 보안국(CISA(Cybersecurity and Infrastructure Security Agency))과 예산관리국(OMB(Office of Management and Budget))은 이러한 목표를 달성하기 위해 따라야 하는 기술 로드맵 작성을 감독할 계획이라고 밝혔다[7].

한편, 행정명령에 따라 행정부 부서 및 기관은 2022년부터 2024년까지의 제로 트러스트 구현 계획과 2023년 및 2024년 예산 추정치를 OMB에 제출해야 한다.

3.1.2. 제로 트러스트 성숙도 모델

美 인프라 보안국인 CISA는 예산관리국인 OMB의 지침에 맞춰 '제로 트러스트 성숙도 모델(zero trust maturity model)'을 공개함으로써 각 기관의 제로 트러스트 구축을 통한 개선방안 상세 모델을 다음과 같이 일부 제시하였다.

첫째, CISA 성숙도 모델은 OMB의 Federal Zero Trust Strategy를 보완하며 기관에 최적의 제로 트러스트 환경을 달성하기 위한 로드맵과 리소스를 제공하도록 설계되었다.

둘째, 신원(identity), 디바이스(devices), 네트워크(network), 응용프로그램 작업(application workload)로 분류하여 작성되었다[8].

그리고 NSA(National Security Agency)의 성숙도 모델은 조직의 제로 트러스트 환경의 성숙도를 아래와 같이 4단계로 구분한다. 이를 토대로 조직은 현재 제로 트러스트 환경의 수준을 평가할 수 있고, 향후 개선 및 고도화 해나가야 할 방향성을 설정할 수 있다. ①준비 단계는 초기 발견 및 평가활동을 수행하며, ②기초 단계는 기본적인 통합 기능을 구현한다. ③중급 단계는 통합의 수준을 높이는 가운데 기능을 개선한다. ④상급 단계는 강력한 분석 및 오케스트레이션으로 고급 보호와 제어 실현한다[9][10].

3.1.3. 연방 제로 트러스트 전략

美 관리 예산실(OMB)이 발표한 연방 제로 트러스트 전략은 인터넷 경계 내외의 어떤 대상도 묵인하지 말라는 분명한 메시지를 연방정부 각급 기관에 보내는 것으로, 각급 기관이 2024년 9월 말까지 "구체적인 제로 트러트스 보안 5대 목표"를 달성하고 이를 기관의 실천 계획에 추가할 것을 요구했다. 이 문서에서 CISA의 제로 트러스트 성숙도 모델을 뒷받침하는 5가지 기둥을 사용하여 그룹화한 목표는 다음과 같다.

① 신원 : 기관 직원은 업무에 사용하는 애플리케이션에 액세스하기 위해 전사적 신원을 사용한다. 피싱 방지 MFA는 정교한 온라인 공격으로부터 해당 직원을 보호한다.

② 장치 : 연방 정부는 정부에서 사용하도록 승인하고 작동하는 모든 장치에 대한 완전한 목록을 가지고 있으며 이러한 장치에서 발생하는 사고를 감지하고 대응할 수 있다.

③ 네트워크 : 기관 내 모든 DNS 요청과 HTTP 트래픽을 암호화한다. 환경을 파악하고 애플리케이션을 중심으로 네트워크를 분할하기 시작한다. 연방 정부는 전송 중인 이메일을 암호화하는 실행 가능한 경로를 식별한다.

④ 응용 프로그램 : 기관은 모든 응용 프로그램을 인터넷에 연결된 것으로 취급하고 정기적으로 응용 프로그램을 엄격한 테스트를 거쳐 외부 취약점 보고를 환영한다.

⑤ 데이터 : 기관은 철저한 데이터 분류. 기관은 클라우드 보안 서비스를 활용하여 민감한 데이터에 대한 액세스를 모니터링하고 전사적 로깅 및 정보 공유를 구현한다[11][12].

3.2. 국내 제로 트러스트 정책 현황

3.2.1. 디지털 플랫폼 정부 핵심 과제

국내의 경우 제20대 대통령직 인수위원회 디지털 플랫폼 정부 TF 는 디지털 플랫폼 정부 핵심 과제 발표에서 신 보안체계 구축에 제로 트러스트, 블록체인 등 최신 보안 기법, 확산을 강조하였다[13].

추가적으로, 정부는 망 분리 규제를 완화하고 해결할 수 있는 구체적 대안 마련을 위해 제로 트러스트 관련 여러 지원 프로그램을 시행하고 민간 전문 기관

이 참여하여 성공적으로 수행하도록 다양한 기회를 제공하고 있다[14][15].

3.2.2. 최근 사이버 위협 동향 및 대응 방안 (KISA 및 과학기술정보통신부)

2022년 과학기술정보통신부와 한국인터넷진흥원(이하 'KISA')은 우리 기업들이 코로나19 이후 일상화된 재택근무 등 업무 환경 변화와 지능화, 조직화되는 사이버 위협에 체계적, 선제적으로 대응할 수 있도록 최근 사이버위협 동향을 분석하고, '사이버 위협 동향 분석 및 국내 기업 대응 방안'을 발표하였다[9]. 대응 방안에서 KISA는, 최근 발생한 여러 국내·외 침해 사고에 대한 분석을 종합해서, 외부로부터의 사이버 공격 단계를 ① 최초 침투 단계, ② 내부망 침투 단계 및 ③ 데이터 유출 단계 등 3단계로 나누어 가이드 하였으며, 개별 기업은 이러한 비대면 업무가 지속 유지·확대되는 것에 대비하여 제로 트러스트 관점에서 단계별 조치를 강화할 필요가 있다고 하였다[16].

그러나 구체적으로 필요성을 인정하는 것 이외에 구체적인 정책은 없어 구체적인 규정의 명문화를 통해 이를 도입할 필요성이 대두된다.

4. 제로 트러스트 정책 명문화를 통한 신 보안체계 강화 방안

4.1. 기존 보안체계의 한계에 따른 신 보안체계 도입의 필요성 및 방향

현재 우리나라의 법제를 고려할 때, 2023년 시행 예정인 전자금융감독규정 망 분리 완화에 이와 관련된 제로 트러스트 적용을 명시하여 이를 보완함으로써, 금융기업을 시작으로 다양한 산업의 기업들이 도입하는 것이 적절하다고 판단된다.

전자금융감독규정시행세칙 <별표 7> 망 분리 완화 대체 통제는 경계 기반 모델을 기반의 통제사항으로 구성되어 있으며, 다음과 같이 한계를 가지고 있는 바, 정보보호 환경을 반영하고 기존 경계 보안 모델의 문제점을 해결하기 위해, 전자금융감독규정시행세칙 <별표 7>을 개선하여 제로 트러스트 모델 기반의 망 분리 대체 정보보호 통제를 적용하는 방식을 취하였다.

첫째, 지능형 해킹(APT) 차단 대책 수립/적용의 경우, 기존 경계 보안 모델로 급격히 증가하는 APT 공격에 대응하기에는 한계점이 존재한다. 또한 특정 APT 공격이 아닌 전반적 사이버 공격에 대한 대응이 필요하다. 따라서 제로 트러스트 관점에서 사이버 공격에 대한 단계별 대응 방안 수립/적용이 필요하다.

둘째, 현재 망 분리 대체 통제사항은 수동적으로 처리되며, 정적인 보안 통제라는 한계가 있다. 통제사항 중, 모니터링의 경우 '사후 모니터링'이며 이는 능동적/실시간으로 사용자의 이상행위를 모니터링하는 현재의 발전된 정보보호 기술을 반영하고 있지 않다. 따라서 제로 트러스트 기반 실시간 모니터링이 필요하다.

셋째, 코로나19로 인한 새로운 접속 환경(모바일 기기 등 다양한 접속 기기, 클라우드를 통한 접속의 경우)가 반영되어 있지 않다. 제로 트러스트 모델 기반의 새로운 접속 환경을 추가함으로써, 현재 환경에 적합한 망 분리 대체 통제를 구성해야 할 것이다.

4.2. 전자금융거래법 고시 개선

제로 트러스트 명문화 관련하여, 저자가 제시하는 망 분리 대체 정보보호 통제 개정안은 다음과 같다.

<표 2> 전자금융감독규정시행세칙[17][18] <별표 7> 망 분리 대체 정보보호 통제 개정안

구분		통제사항
경계 보안 모델	공통	· 외부망에서 내부망으로 전송되는 전산자료를 대상으로 악성코드 감염여부 진단·치료 · 지능형 해킹(APT)차단 대책 수립·적용 · 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링
	메일시스템	· 본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립·적용 · 메일을 통한 정보유출 탐지·차단·사후 모니터링 대책 수립·적용

제로 트러스트 모델	업무단말기		· 사용자의 관리자 권한 제거 · 승인된 프로그램만 설치·실행토록 대책 수립·적용 · 전산자료 저장 시 암호화
	원격접속	외부단말기	· 공통(상세내용 생략)
			· 업무용 단말기를 경유하여 내부망에 접속하는 경우(간접접속) (상세내용 생략)
			· 외부 단말기에서 내부망에 직접 접속하는 경우(직접접속) (상세내용 생략)
		내부망 접근통제	· 업무상 필수적인 IP, Port에 한하여 연결 허용 · 원격접속 기록 및 저장
		인증	· 이중 인증 적용 · 일정 횟수(예 : 5회) 이상 인증 실패 시 접속 차단
		통신회선	· 안전한 알고리즘으로 네트워크 구간 암호화 · 내부망 접속시 인터넷 연결 차단 · 원격 접속 후 일정 유휴시간 경과 시 네트워크 연결 차단
		기타	· 원격접속자 보안서약서 징구 · 공공장소에서 원격 접속 금지
	공통		· 최소 권한 원칙 기반 접근제어 · 모든 데이터 소스와 컴퓨팅 서비스는 리소스로 간주 · 네트워크 위치와 관계없이 모든 통신을 안전하게 구축 · 개별 엔터프라이즈 리소스에 대한 액세스는 세션 별 승인 · 클라우드 및 재택근무, 다양한 기기(모바일 기기, 태블릿 PC 등)를 통해 접속하는 환경에 적합한 제로 트러스트 모델 적용 · 모든 인증/승인은 동적으로 수행되며, 접근허용 전 엄격히 적용 · 기업은 모든 소유 및 관련 자산의 무결성과 보안상태를 모니터링하고 측정 · 통합/자동화된 계정 관리 및 접근통제 시스템, 다중요소 인증 필수 적용 · 사이버 공격에 대한 제로 트러스트 관점 단계별 대응방안 수립/적용
	단말기		· 외부망에서 내부망으로 접속 시 디바이스 인증을 통해 접근권한 또는 사용권한 부여 · 다양한 단말기를 이용해 네트워크와 시스템에 접근하는 사용자는 연결 시도할 때마다 사용자뿐만 아니라 장치도 확인 · 인가된 기기의 행동이력 관리
	사용자		· 내부망에 접속 시 신원 확인 및 인증을 통해 접근권한 또는 사용권한 부여 · 인가된 사용자의 행동이력 관리 · 조직 네트워크와 시스템에 접근하는 사용자 권한확인은 자동화 기반 정책을 통해 이루어져야 함
	네트워크		· 사용자 또는 단말기가 내부망에 접속 시 신원확인 및 인증을 통해 접근권한 또는 사용 권한 부여 · 네트워크/트래픽 가시성 확보 및 보안상태 지속적 모니터링
	애플리케이션		· 사용자 또는 단말기가 내부망 애플리케이션에 접속 시 신원 확인 및 인증을 통해 접근권한 또는 사용권한 부여 · 악성코드 식별 및 모니터링
	데이터		· 외부망에서 내부망으로 전송되는 전산자료를 대상으로 악성코드 유입에 대한 탐지 및 대응 · 전산자료 외부전송 시 데이터 유출에 대한 행위분석을 통해 탐지 및 대응 · 클라우드 또는 원격 환경에 저장된 데이터는 미사용 시 암호화
기타			· 그 외 금융감독원장이 인정한 망 분리 대체 정보보호 통제

위와 같이 전체적인 분류는 공통/단말기/사용자/네트워크/어플리케이션/데이터로 분류하였다. 통제사항은 제로 트러스트 도입 시 필수적으로 적용되어야 하는 핵심사항 위주로 기술하여 명문화하는 방안을 고

안하였으며, 나아가 명문화된 제로 트러스트 기반 통제사항에 대하여, 기업이 실천할 수 있는 상세 가이드라인 배포가 필요하다.

그리고 제로 트러스트 적용 미 이행 시 전자금융거래법 제51조(과태료)를 적용함으로써, 기업의 시행을 의무화해야 할 것이다.

4.3. 국내 기업의 제로 트러스트 적용 전략 (가이드라인)

고시 개정 이외에도 기업들의 제로 트러스트 도입을 위하여 국가적 차원의 구체적 가이드라인을 수립 및 배포가 필요하다. 도입이 완료된 이후에는 제로 트러스트의 구현이 보다 고도화될 수 있도록 가이드라인의 보완을 통해 기업들이 제로 트러스트 적용을 고도화하여 제로 트러스트 도입 및 성장을 촉진할 수 있을 것이다.

우리나라 기업의 경우, 정보보호 환경이 대부분 경계 보안 모델을 기반으로 구성되어 있다. 따라서 단기적으로는 기존 보안 시스템과 제로 트러스트의 융합을 통해 구현이 필요하다. 중장기적으로는 제로 트러스트 구현에 적합하지 않은 기존 보안 시스템의 경우, 노후화 시기에 따라 점차적으로 제로 트러스트 기반 보안 시스템의 적용으로 전환하며, 제로 트러스트 모델의 완벽한 구현을 향해 나아가야 할 것이다.

우리나라 기업들의 제로 트러스트 적용 전략을 위한 가이드라인(안)은 다음과 같으며, 총 4단계로 구성된다. 다만 제로 트러스트는 특정 아키텍처를 모든 기업이 획일적으로 구현하는 것이 아니라, 각사의 환경이나 요구사항에 맞게 구현하는 것이 필요할 것이다.

<표 3> 국내 기업의 제로 트러스트 적용 전략[19]

단계	제로 트러스트 적용 전략
Phase 1 (정보보호 환경 및 요구사항 분석)	▪ 정보보호 환경 및 요구사항을 분석하는 단계 ▪ 운영 중인 기존 보안 시스템 목록과 정책 현황 파악하고, 기업의 현재 정보보호 환경/아키텍처를 분석하며, 제로 트러스트 관련 법적 요건 및 가이드라인 요구사항 분석을 수행
Phase 2 (설계 원칙 수립)	▪ 제로 트러스트 구현을 위한 설계 원칙을 수립하는 단계 ▪ identity와 device 식별 이행 - 보호가 필요한 모든 자원(어플리케이션, 데이터, 네트워크 등) 및 모든 주체를 식별(사용자, 기기 등) - 접근통제 강화를 위해, 최소 권한 원칙을 적용하고, 사용자 및 기기의 신뢰성 검증, 지속적인 위험평가 결과를 접근통제 정책에 반영 - 모니터링 수행 시, 모든 행위는 저장 및 관리되며, 자원의 보안상태를 지속적으로 모니터링 및 분석 수행
Phase 3 (적용 대상 및 아키텍처 설계)	▪ 적용 대상 및 아키텍처를 설계하는 단계 ▪ 먼저 적용이 용이한 대상(부서, 시스템 등)부터 시작하여 점진적인 전사 확대 시행 ▪ 기업에 적합한 제로 트러스트 아키텍처(정책 관리, 인증, 접근통제, 모니터링)를 정의 및 보안 정책 수립
Phase 4 (구현 방안 수립 및 이행/개선)	▪ 구현 방안 수립 및 이행/개선하는 단계 ▪ 우선적으로 세 번째 단계에서 수립한 제로 트러스트 보안정책이 기존 IT/보안 시스템으로 구현 가능 여부를 판단 ▪ 기존 IT/보안 시스템과의 융합을 고려하여, 융합 또는 신규 도입이 필요한 시스템 목록을 도출한다. ▪ NSA 성숙도 모델 기준으로, 현재 제로 트러스트 수준 평가하고, 개선점과 방향성을 수립 ▪ 성숙도 모델 기준, 초기/단기적으로는 준비/기초 단계이며 중장기적으로 중급/상급 단계로 전환하며 제로 트러스트를 고도화 시키는 전략이다.

추가적으로, 미국 행정명령에서 행정부 부서 및 기관은 2022년부터 2024년까지의 제로 트러스트 구현 계획과 2023년 및 2024년 예산 추정치를 제출 명령을 한 것과 같이, 우리나라도 구체적인 제로 트러스트 적

용을 위한 구체적인 이행 시기가 포함된 로드맵을 수립하여야 할 것이다.

5. 결 론

지금까지 제로 트러스트의 개념 및 국내 및 해외 제로 트러스트 정책 현황, 그리고 국내 명문화 방안에 대해 살펴보았다.

제로 트러스트 정책을 당장 모든 업무에 적용하는 것은 무리이며, 점진적 확대 방안이 필요하다. 미국 행정명령에서 제로 트러스트를 강조 및 명시한 바와 같이, 우리나라는 저자가 <표 2>에서 제시한 바와 같이, 전자금융감독규정 고시 <별표 7>에 대한 망분리 대체 정보보호 통제를 개정하는 것이 제로 트러스트 명문화에 대한 방법이 될 수 있을 것이다.

나아가 저자가 제안한 <표 3> 국내 기업의 제로 트러스트 적용 전략과 같이 기업이 실천할 수 있는 상세 가이드라인 배포가 필요하다. 이를 금융기업을 시작으로 다양한 산업의 기업들로 점진적 확대/도입해야 할 것이다.

정책 입안 담당자들은 전자금융거래법상 제로 트러스트 정책을 명문화하고 금융회사 등 기업은 법적 근거 및 가이드라인의 개선이 이루어짐에 있어, 전통적 경계 보안 모델에서 나아가, 제로 트러스트 기반의 신규 아키텍처 도입을 통해 보안 강화가 이루어진다면, 금융기업에서 나아가, 많은 분야의 기업들의 보안 강화로 이어지며, 우리나라 사이버보안 체계를 강화로 이루어질 것이다.

참고문헌

[1] 윤대균, “클라우드를 위한 제로 트러스트 보안”, 디지털서비스 이슈리포트, 2022.

[2] Department of Defense (DOD), “DOD Zero Trust Reference Architecture,”, 2021.

[3] Office of Management and Budget, “Moving the U.S. Government Towards Zero Trust Cybersecurity Principles”, 2021.

[4] 이선아, 김범석, 이혜인, 박원형, “제로 트러스트 기반 접근제어를 위한 기업 보안 강화 연구″, 한국정보통신학회논문지, Vol. 26, No. 2, pp. 265-270, 2022.

[5] 윤대균, “서비스로서의 아이덴티티(IDaaS)”, 디지털서비스 이슈리포트, 2022.

[6] 금융위원회 보도자료, ″금융분야 클라우드 및 망 분리 규제 개선방안″, 2022.04.14.

[7] The White House, Executive Order 14028, “Improving the Nation’s Cybersecurity”, 2021.

[8] 이후기, “제로 트러스트 보안기술 동향과 적용방안”, 문화정보 이슈리포트, 2022-6호(제36호).

[9] NSA, ″Embracing a Zero Trust Security Model″, 2021.

[10] Bobby New, 공공 부문을 위한 제로 트러스트, 아키텍처 구축 가이드, Fireeye, 2021.

[11] OMB, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”, 2022.

[12] Shalanda D. Young,“Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”, 2022.

[13] bikorea, “금융당국, ‘제로 트러스트’ 명문화에 주저 말아야”, http://m.bikorea.net/news/articleView.html?idxno=33801, 2022.

[14] 이투데이, ″SGA솔루션즈, 100억 규모 제로트러스트 개발 국책 과제 수주″, 2021.

[15] 디지털타임스, ″사이버보안 ‘생명’과 직결…양자·6G 시대 超보안기술 확보할 것″, 2020.

[16] 윤혜정, 이용우, 임효정, 전삼현, “재택근무 환경 개선을 위한 제로 트러스트 추진 동향 및 실효성 제고 방안 연구”, ‘Vol.14 No.02, pp. 2915-2921, 2022.

[17] NIST, ″Zero Trust Architecture″, NIST Special Publication 800-207, 2020.

[18] 과학기술정보통신부 보도자료, “최근 사이버 위협 동향 및 대응방안”, 2022.04.07.

[19] 김태연, ″새로운 보안경계 - 제로 트러스트에 대한 이해와 전망″, ICT 산업전망컨퍼런스, 2022.

[저 자 소 개]

이 민 원 (Min-won Lee)
2015년 2월 한양대학교 정보시스템학 학사
2019년 3월 고려대학교 정보보호대학원 정보보호학과 석사과정
email: minwon1013@naver.com

권 헌 영 (Hun-yeong Kwon)
2008년 3월~2015년 8월 광운대학교 법과대학 교수
2015년 9월~고려대학교 정보보호대학원 교수
email: khy0@korea.ac.kr