



제 432회 국회 (임시회)
제1차 과학기술정보방송통신위원회

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

검 토 보 고

〈제로트러스트 보안체계 구축·운영 지원〉

■ 최민희의원 대표발의(의안번호 제2215639호)

2026. 2.

과학기술정보방송통신위원회

수석전문위원 이복우

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	2
1. 제로트러스트 보안체계 구축·운영 지원(안 제46조의3 신설)	2

I. 제안경위

가. 발 의 자 : 최민회의원 등 11인

나. 발 의 일 : 2025. 12. 26.

다. 회 부 일 : 2025. 12. 29.

II. 제안이유 및 주요내용

현행법은 정보통신망의 안정성 및 신뢰성 확보를 위하여 정보보호 최고책임자의 지정 및 정보보호 관리체계 인증 등에 관한 사항을 규정하고 있음.

그러나 최근 클라우드 서비스의 확산, 공급망 공격 및 내부자 위협의 증가 등으로 기존의 경계 기반 보안만으로는 새로운 유형의 위협에 대응하기 어려워지고 있음. 이에 따라 내부 또는 외부 네트워크의 위치와 관계없이 신뢰를 부여하지 아니하고 지속적으로 검증하는 제로트러스트 보안체계의 필요성이 높아지고 있음.

이에 정보통신서비스 제공자가 제로트러스트 보안체계를 구축·운영하도록 규정하고, 중소기업이 제로트러스트 보안체계 도입 시 필요한 경비를 지원할 수 있도록 함으로써 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하려는 것임(안 제46조의3 신설).

Ⅲ. 검토의견

1. 제로트러스트 보안체계 구축·운영 지원(안 제46조의3 신설)

가. 개정안 요지

- 정보통신서비스 제공자는 정보통신망의 안전한 보호를 위하여 정보통신망 또는 정보통신시스템에 대한 접근 요청에 대하여 제로트러스트 보안체계를 구축·운영하도록 노력하여야 함(안 제46조의3 제1항).
- 과학기술정보통신부장관은 제로트러스트 보안체계의 확산을 위하여 다음의 시책을 수립·추진할 수 있음(제2항)
 - 제로트러스트 보안체계 관련 기술의 연구개발 및 표준화
 - 제로트러스트 보안체계 관련 전문인력의 양성
 - 제로트러스트 보안체계의 시범 적용 사업
 - 중소기업에 대한 제로트러스트 보안체계 도입 지원
- 과학기술정보통신부장관은 중소기업이 제로트러스트 보안체계를 도입하는 경우 그에 필요한 경비의 전부 또는 일부를 예산의 범위에서 지원할 수 있음(제3항)
- 과학기술정보통신부장관은 정보통신서비스 제공자가 제로트러스트 보안체계를 효과적으로 구축·운영할 수 있도록 가이드라인을 정하여 고시할 수 있음(제4항).

- 과학기술정보통신부장관은 시책을 효율적으로 추진하기 위하여 한국인터넷진흥원 또는 대통령령으로 정하는 전문기관에 그 업무를 위탁할 수 있음(제5항).

나. 개정안 조문대비표

현 행	개 정 안
<신 설>	제46조의3(제로트러스트 보안체계의 구축 등) ① 정보통신서비스 제공자는 정보통신망의 안전한 보호를 위하여 정보통신망 또는 정보통신시스템에 대한 접근 요청에 대하여 내부 또는 외부 네트워크의 위치와 관계없이 신뢰를 부여하지 아니하고 지속적으로 검증하며, 접근 권한을 최소화하는 원칙(이하 “제로트러스트 원칙”이라 한다)에 따른 정보보호 체계(이하 “제로트러스트 보안체계”라 한다)를 구축·운영하도록 노력하여야 한다. ② 과학기술정보통신부장관은 제로트러스트 보안체계의 확산을 위하여 다음 각 호의 시책을 수립·추진할 수 있다.

현행	개정안
	1. 제로트러스트 보안체계 관련 기술의 연구개발 및 표준화 2. 제로트러스트 보안체계 관련 전문인력의 양성 3. 제로트러스트 보안체계의 시범 적용 사업 4. 「중소기업기본법」 제2조제1항에 따른 중소기업(이하 “중소기업”이라 한다)에 대한 제로트러스트 보안체계 도입 지원 5. 그 밖에 제로트러스트 보안체계의 확산에 필요한 사항 ③ 과학기술정보통신부장관은 중소기업이 제로트러스트 보안체계를 도입하는 경우 그에 필요한 경비의 전부 또는 일부를 예산의 범위에서 지원할 수 있다. ④ 과학기술정보통신부장관은 정보통신서비스 제공자가 제로트러스트 보안체계를 효과적으로 구축·운영할 수 있도록 제로트러스트 보안체계의 구축·운영에 관한 가이드라인을 정

현행	개정안
	<u>하여 고시할 수 있다.</u> ⑤ <u>과학기술정보통신부장관은 제2항 각 호의 시책을 효율적으로 추진하기 위하여 한국인터넷진흥원 또는 대통령령으로 정하는 전문기관에 그 업무를 위탁할 수 있다.</u>

다. 검토사항

- 제로트러스트란 네트워크, 물리적 위치 또는 기기에 상관없이 신뢰를 배제하고 항상 네트워크 침해의 가능성을 가정하여 접근 요구에 정확하게 최소의 권한만 부여하는 보안 원칙으로, 기존의 경계 기반 보안 모델이 가진 한계를 극복하기 위하여 제시된 개념임.
- 경계 기반 보안 모델은 내부망과 같이 경계를 기준으로 한 번 인증된 기기나 사용자 혹은 트래픽에 대해서는 신뢰를 부여하여 접근을 허용하는 방식으로 현재 가장 보편적으로 사용되고 있는 모델임.
- 그런데, 이러한 경계 기반 보안 모델은 이미 신뢰도를 부여받은 사용자, 기기에 대해서 별도의 검증 없이 접근을 허용하는 만큼 내부자 권한이 탈취될 경우 데이터 유출 등 침해사고로 이어질 가능성이 크다는 문제가 있음.

- 한국인터넷진흥원에 따르면 최근 빈번하게 발생하고 있는 침해사고의 유형은 내부자 계정탈취 후 내부시스템에 침투하여 데이터를 유출하는 횡적이동(Lateral Movement) 공격 형태임.

경계 기반 모델 및 제로트러스트 모델 비교

경계 기반 보안 모델	제로트러스트 모델
○ 경계(perimeter) 기준 한 번 인증된 기기나 사용자, 트래픽은 모두 허가 → VPN, 방화벽 등 ※ 내부자에게 높은 신뢰도를 부여하는 기존 모델의 약점을 이용하여 내부자 권한 탈취를 통한 공격 사례 증가	○ 네트워크 혹은 물리적 위치, 기기에 상관없이 ‘무신뢰’ 원칙(Never Trust, Always Verify) ○ 강화된 인증 및 기기 상태 모니터링 등을 통하여 지속적인 검증을 통해 접근 권한 부여
제로트러스트도입 전: 기업망 단위 보안 경계 기업망 내부 (암묵적 신뢰 구역) 인터넷 (비신뢰 구역) 내부 침투시 위협 내부전파 가능 내부 위협	제로트러스트도입 후: 소프트웨어 정의 보안 경계 설정 기업망 내부 (비신뢰 구역) 인터넷 (비신뢰 구역) 내부 침투시에도 위협 내부전파 불가능 내부 위협

자료 : 한국인터넷진흥원

- 이미 해외 주요 빅테크 기업을 중심으로 제로트러스트 보안 모델 도입이 선도적으로 추진되고 있으며, 제로트러스트가 특정 보안 기능이나 개별 솔루션이 아니라 보안에 대한 기본 원칙과 작동 원리의 집합이라는 점을 고려할 때, 그 확산을 위해서는 체계적인 구축과 정책적 지원이 필요하다는 점은 공감할 수 있음.

- 이에 개정안은 모든 정보통신서비스제공자에게 제로트러스트 보안 체계 구축을 위한 노력 의무를 부과하는 한편, 중소기업에 대한 제로트러스트 보안 체계 구축 지원, 제로트러스트 보안 체계 구축·운영 가이드라인 제정 등 정부가 제로트러스트 보안 체계 확산을 지원할 수 있는 법적 근거를 마련하려는 것으로 보임.
- 제로트러스트 보안 체계의 구축은 내부자 계정 탈취 등으로 인한 침해사고를 예방함으로써 정보주체 보호 및 사회 전반의 정보보안 수준 제고라는 공익적 효과가 기대되며, 특히 보안 체계 전환에 따른 비용 부담이 상대적으로 큰 중소기업의 경우 정부 지원의 필요성이 인정되는 측면이 있음.
- 다만, 특정한 보안 체계를 정보통신서비스제공자가 도입하도록 법률에 명시하는 방식이 가져올 수 있는 보안 모델의 경직성 문제를 고려할 필요가 있어 보임.
- 향후 제로트러스트 보안 체계와는 다른 새로운 유형의 보안 모델이 등장할 가능성을 배제할 수 없는 가운데, 법률에서 일률적으로 하나의 보안 체계 도입을 명시할 경우에 새로운 보안 모델로의 교체·기존 모델의 수정이 필요할 경우에는 법률의 제·개정 절차에 소요되는 시간으로 인해 보안 체계에 있어서 기술 도입이 늦어지거나 공백이 발생할 수도 있으므로, 법률에서는 완화하여 규정하되 구체적 보안 모델은 대통령령 등으로 위임하는 방안도 검토할 수 있을 것임.

- 또한, 이미 한국인터넷진흥원(KISA)이 제로트러스트 가이드라인¹⁾을 제작하여 발표한 바 있고 정부 예산으로 제로트러스트 확산을 지원하는 사업²⁾도 운영되고 있는 상황임을 감안할 때, 개정안을 통한 입법이 가지는 실익이 정부가 지원하는 보안 체계를 보다 탄력적으로 정하기 어렵게 되는 한계보다 충분히 크다고 볼 수 있는지에 대해서는 추가적인 검토가 필요할 것으로 보임.
- 아울러, 장기적인 관점에서 시장 환경의 변화 및 기술 발전에 유연하게 대응하기 위해서는 보안 패러다임의 전환이 정부 주도의 규범적 강제를 통해 이루어지기보다는 기업이 소비자와 시장의 요구에 부응하여 자발적으로 보안 체계의 혁신을 추구할 수 있도록 유인하는 방안이 보다 적합한 측면이 있다는 점을 감안한 검토가 필요함.
- 과학기술정보통신부는 법안 취지에 공감하되, “항상 네트워크 침해를 가정”한다는 내용을 제로트러스트 개념에 추가함으로써 제로트러스트가 네트워크 혹은 물리적 위치나 기기에 상관 없는 무신뢰 원칙이며, 접근 권한을 최소한으로 부여하는 원칙임을 강조할 필요가 있다는 의견을 제출함.

문 의 처

02)6788-5228

1) 과학기술정보통신부와 한국인터넷진흥원은 지난 2023년 7월에 처음으로 제로트러스트 가이드라인 1.0을 발표한 것에 이어 지난 2024년 12월에 제로트러스트 가이드라인 2.0을 제작하여 발표하였음.
 2) 과학기술정보통신부 소관 제로트러스트 신보안체계 실증확산 사업(2333-307)은 제로트러스트 보안모델 시범사업을 추진하고 기업을 대상으로 제로트러스트 컨설팅을 실시하는 사업으로, 2024년에 처음으로 편성되어 2026년 예산에 약 105억원이 반영되었음.