국회입법조사처 | 2025. 11. 25. | 제2432호

이슈와 논점
Issues and Perspectives

# 정보보호 사각지대 해소를 위한 중소기업 보안 역량 강화 방안

강 은 수

최근 SK텔레콤, KT, 롯데카드 등 대기업을 대상으로 한 대규모 사이버 침해사고가 잇따르면서 대기업과 국가 핵심 인프라 보안 강화에 관심이 집중되고 있다. 그러나 실제 사이버공격의 주요 표적은 중소기업이며, 대기업과 하청·협력 관계로 연결된 산업 생태계상 이들의 보안 취약성은 국가 전체의 사이버 안전을 위협할 수 있다. 정보보호 사각지대에 놓인 중소기업의 보안 역량 강화를 위해서는 매년 축소되고 있는 중소기업 정보보호 지원 예산을 확대하고, 정보통신망법 개정을 통해 제로트러스트 보안체계 확산을 위한 법적 기반을 마련하며, 정보보호 투자에 대한 세제혜택 등 유인책을 통해 자율적 투자를 촉진할 필요가 있다.

## 1 급증하는 중소기업 사이버 침해사고

최근 SK텔레콤, KT, 롯데카드 등 대기업을 대상으로 한 대규모 사이버 침해사고가 연이어 발생하면서, 언론과 정책 당국의 관심은 주로 대기업과 국가 핵심 인프라 보안 강화에 집중되고 있다.

그러나 사이버공격의 주요 표적은 중소기업으로, 대기업과 하청·협력 관계에 있는 산업 생태계를 고려할 때 중소기업의 보안취약성은 전체 사이버 안전망의 구조적 약점으로 이어질 수 있다.

실제로 중소기업 침해사고 신고 건수는 2021년 518건에서 2024년 1,575건으로 3배 이상 급증했으며, 2024년 전체 신고 건수(1,887건)의 약 83.5%가 중소기업 신고 건이었다.[1] 더욱이 중소기업은 침해사고 발생사실을 인지조차 못하는 경우가 많아[2] 통계에 잡히지 않는 '숨은 피해'까지 고려하면 실제 피해 규모는 훨씬 클 것으로 추정된다.

[표 1] 기업 규모별 침해사고 신고 현황

(단위: 건)

| 구분 | 2021 | 2022 | 2023 | 2024 | 2025.8월 |
|---|---|---|---|---|---|
| 대기업 | 20 | 31 | 54 | 56 | 52 |
| 중견기업 | 62 | 78 | 120 | 141 | 149 |
| 중소기업 | 518 | 954 | 1,034 | 1,575 | 1,185 |
| 비영리 | 40 | 79 | 69 | 115 | 87 |
| 합계 | 640 | 1,142 | 1,277 | 1,887 | 1,473 |

※ 주: 2022년부터 침해탐지시스템 또는 사고 조사 중 확인된 해킹 경유지 등에 대해 적극적으로 신고를 안내하여 신고 건수 증가

※ 자료: 과학기술정보통신부 제출자료(2025.10.15.)

중소기업은 보안 전문 인력, 예산, 기술 인프라가 부족하여 단순한 침해사고조차 대응이 어려운 상황이나, 정부의 정책적 지원이 충분하지 않아 보안 역량은 여전히 취약한 수준에 머물러 있다.

이 글에서는 기업 규모에 따른 정보보호 실태를 살펴보고, 중소기업 정보보호 정책의 한계를 분석하며, 정보보호 사각지대에 놓인 중소기업의 보안 역량을 강화할 수 있는 정책 과제와 개선방안을 모색하고자 한다.

1) 과학기술정보통신부 제출자료(2025.10.15.)

2) 한국인터넷진흥원, 『중소기업 침해사고 피해지원 서비스 동향 보고서 (2024년 4분기)-정보유출 침해사고 사례』, 2024, p.1.

NARS www.nars.go.kr
발행처 국회입법조사처
발행인 이관후 국회입법조사처장
저 자 강은수 사회문화조사실 과학방송통신팀 입법조사관
02-6788-4712 eunsu@assembly.go.kr
국회입법조사처 NATIONAL ASSEMBLY RESEARCH SERVICE

## 2 기업 규모별 정보보호 격차

한국정보보호산업협회의 '2024 정보보호 실태조사'에 따르면, 기업 규모에 따라 정보보호 수준에 뚜렷한 격차가 존재한다.

종사자 250명 이상 기업의 경우 정보보호 정책 보유율은 98.7%, 조직 보유율은 87.0%에 달하는 반면, 10~49명 기업의 경우 정책 보유율은 48.9%, 조직 보유율은 26.2%에 그치는 것으로 나타났다.[3)]

**[표 2] 기업 규모별 정보보호 정책·조직 보유율**

(단위: %)

| 구분 | 10~49명 | 50~249명 | 250명 이상 |
|---|---|---|---|
| 정책 보유율 | 48.9 | 58.7 | 98.7 |
| 조직 보유율 | 26.2 | 60.4 | 87.0 |

※자료: 한국정보보호산업협회, 『2024정보보호 실태조사』, 2024, 조사관 재구성

이와 같은 기업 규모별 정보보호 격차는 일부 지역에서 실시한 조사 결과에서도 확인된다.

2025년 10월 대구상공회의소가 대구 소재 기업을 대상으로 실시한 조사에 따르면, 100인 미만 사업장의 경우 정보보호 전담부서·전담자 보유율이 11.0%에 그친 반면, 100인 이상 사업장은 64.5%에 달해 뚜렷한 차이를 보였다. 정보보호 예산 편성률 역시 100인 미만 사업장은 18.9%에 불과했으나, 100인 이상 사업장은 66.1%가 관련 예산을 편성한 것으로 조사되었다.[4)]

**[표 3] 대구 소재 기업 규모별 정보보호 조직·예산 격차**

(단위: %)

| 구분 | 100인 미만 | 100인 이상 |
|---|---|---|
| 전담부서·전담자 보유율 | 11.0 | 64.5 |
| 관련 예산 편성율 | 18.9 | 66.1 |

※ 자료: 대구상공회의소 보도자료, 「기업 정보보호 대응 실태 및 애로 조사」, 2025.10.16., 조사관 재구성

이처럼 규모가 작은 기업일수록 재정 여력이 부족하여 효과적인 정보보호 체계를 구축·운영하기 어려운 구조적 한계를 지니고 있어, 정부 차원의 적극적인 지원이 필수적이다.

3) 한국정보보호산업협회, 『2024 정보보호 실태조사』, 2024.

4) 대구상공회의소 보도자료, 「기업 정보보호 대응 실태 및 애로 조사」, 2025.10.16.

## 3 중소기업 보안 역량 강화 방안

### (1) 중소기업 정보보호 지원 예산 확보 필요

중소기업을 대상으로 한 사이버공격은 지속적으로 증가하고 있으나, 최근 관련 예산이 대폭 감액되면서 지역 중소기업의 정보보호 역량 강화에 차질이 우려된다.

정부는 지역 중소기업의 정보보호 역량 강화를 위하여 2014년부터 지역정보보호지원센터[5)]를 중심으로 '지역 중소기업 정보보호 지원' 사업을 추진해 왔다. 이 사업은 지역 중소기업을 대상으로 맞춤형 정보보호 컨설팅 및 보안솔루션, 클라우드 기반 보안서비스(SECaaS)[6)] 도입 비용을 지원하는 사업이다.

최근 5년간('21~'25년) 이 사업의 추진 내역을 살펴보면, 2023년까지는 매년 100억 원 이상의 예산이 편성되어 지원 규모가 1,300~1,500개 사 수준이었으나, 2024년 이후 예산이 매년 절반 수준으로 감액('24년 58억, '25년 26.4억)되면서 지원 규모도 2024년 700개 사, 2025년 406개 사로 축소되었다. 이러한 추세는 2026년도 예산안까지 이어지고 있다.[7)]

**[표 4] '지역 중소기업 정보보호 지원' 사업 예산 현황**

(단위: 억 원, 개사)

| 구분 | | 2021년 | 2022년 | 2023년 | 2024년 | 2025년 | 2026년 (편성안) |
|---|---|---|---|---|---|---|---|
| 예산 | | 109.5 | 101.8 | 105 | 58 | 26.36 | 13 |
| 예산상 | 컨설팅 등 | 600 | 600 | 300 | 200 | 60 | 26 |
| 지원 | SECaaS | 700 | 700 | 1,200 | 500 | 346 | 174 |
| 규모 | 합계 | 1,300 | 1,300 | 1,500 | 700 | 406 | 200 |

※ 자료: 과학기술정보통신부 제출자료(2025.10.15.)

최근의 예산 삭감은 사업의 필요성 감소가 아닌 정부의 재정 여건과 우선순위 조정 과정에서 비롯된 것으로 보이는데,[8)] 이는 중소기업 대상 사이버

5) 한국인터넷진흥원 소속으로 10개의 센터가 구축·운영 중이다.

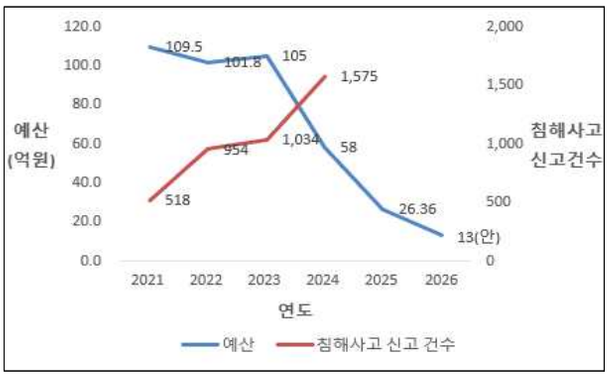
6) Security as a Service는 ICT 인프라 구축이 어려운 중소기업에 별도 보안 활동 없이도 클라우드 보안 서비스 업체가 원격에서 필요한 보안 서비스를 지원하는 것이다(과학기술정보통신부 제출자료(2025.10.15.)).

7) 과학기술정보통신부 제출자료(2025.10.15.)

8) 2026년 '지역 중소기업 정보보호 지원'사업 예산 요구안은 약 146억 원이었으나, 10%에도 미치지 못하는 13억 원만 정부안으로 반영되었는데, 과학기술정보통신부는 사업비 증액을 위해 노력하였으나, 재정투자 우선 순위 등으로 증액이 이루어지지 않았다고 답변하였다(과학기술정보통신부 제출자료(2025.10.20.)).

침해사고 급증 추세에 역행하는 것이며, 정부의 정책 방향에도 부합하지 않는다.[9] 현 정부는 '보안이 취약한 지역·중소기업 등 보안 사각지대에 대한 지원 강화'를 국정과제로 채택하며[10] 보안 사각지대 해소에 대한 정책 의지를 보이고 있다.

**[그림 1] 중소기업 침해사고 신고 건수 및 정보보호 지원 예산**




※ 자료: 과학기술정보통신부 제출자료(2025.10.15.) 조사관 재구성

그러나 2026년 정부 예산안에서도 관련 예산이 감액 편성되면서, 해당 과제를 이행할 수 있을지 우려되는 상황이다.

따라서 정부는 중소기업의 보안역량을 강화하기 위하여 중소기업 침해사고 증가 추세와 사업 수요[11], 정보보호 투자 여력 등을 종합적으로 고려하여 합리적인 지원 규모와 예산 수준을 재산정하고, 필요한 재정을 확보할 필요가 있다.

아울러 선제적 예방이 최선의 대응인 만큼 재정당국은 중소기업 정보보호 지원 예산을 비용이 아닌 국가 전체 사이버안보 역량 강화를 위한 필수 투자로 인식하고 재정 여건을 이유로 관련 사업을 후순위로 미루거나 예산 삭감이 반복되지 않도록 해야 한다. 국회도 2026년 예산안 심의 과정에서 이러한 정책적 중요성을 고려해 적정 예산이 확보되도록 해야 할 것이다.

9) '제21대 대통령선거 더불어민주당 정책공약집'에는 '지역 및 중소기업 등 사이버보안 사각지대 해소를 위하여 중소기업을 대상으로 SECaaS 시장 확대를 지원하고 지역 영세기업 대상 컨설팅 등을 확대'한다는 내용이 포함되어 있었다(제21대 대통령선거 더불어민주당 정책공약집 제15대 정책과제 중 '3.국민생활안전 및 재난대응'(16. 사이버 위협으로부터 안전한 나라를 만들겠습니다.)).

10) 이재명정부 123대 국정과제 23번(국민의 안전과 보편적 삶의 질 제고를 위한 'AI 기본사회' 실현) 과제에 포함되어 있다.

11) 과기부에 따르면 2021년부터 2024년까지의 평균 경쟁률은 1:1.50이다.

### (2) 제로트러스트 법제화 및 지원 사업 강화

최근 전방위적으로 사이버공격이 급증하면서 '제로트러스트(Zero Trust)'가 핵심 보안 전략으로 부상하고 있다.[12] '제로트러스트'는 기존 경계 기반 보안과 달리 정보시스템 등에 대한 접속 요구 시 네트워크가 이미 침해된 것으로 간주, 절대 믿지 말고 계속 검증하라는 새로운 보안개념이다.[13]

2025년 7월 과학기술정보통신부는 SK텔레콤 해킹 사건에 대한 최종 조사 결과에서 제로트러스트를 통한 보안 관리 강화를 재발 방지 대책으로 밝힌 바 있다.[14]

이와 같은 보안 전략 변화는 중소기업 역시 예외가 아니다. 한국인터넷진흥원은 2024년 보고서에서 중소기업 정보유출 침해사고의 주요 원인으로 '취약한 인증 및 세션 관리 등'을 지적하며, 대응 방안으로 제로트러스트 보안 모델 도입이 필요하다고 분석했다.[15]

정부는 2023년 '정보보호산업의 글로벌 경쟁력 확보 전략'에서 2027년까지 제로트러스트의 전면 확산을 유도한다는 계획을 밝히고[16], 2023년 '가이드라인 1.0', 2024년 '가이드라인 2.0'을 발간하였다. 또한 제로트러스트 확산 기반 마련을 위해 2023년 실증사업에 이어 2024년부터는 시범사업 및 컨설팅 사업[17]을 추진하고 있다.

그러나 현재 제로트러스트 확산을 뒷받침할 법적 근거가 미비하고, 정부 지원 또한 충분하지 않아 중소기업이 이를 현장에 도입·적용하기는 사실

12) 박정수, 「해킹 사태에 중소기업 82% 뚫려…보안 해답 '제로트러스트' 급부상」, 『마켓in』, 2025.9.24.

13) 과학기술정보통신부, 『정보보호산업의 글로벌 경쟁력 확보 전략』, 2023, p.3.

14) 과학기술정보통신부 보도자료, 「SK텔레콤 침해사고 최종 조사결과 발표」, 2025.7.4., p.8.

15) 한국인터넷진흥원, 앞의 글, pp.1~25.

16) 과학기술정보통신부, 위의 글, p.3.

17) △실증사업: NIST 800-207 등에 명시된 제로트러스트 모델에 대한 설계·개발 및 PoC(Proof of Concept) 등 지원, △시범사업 : 제로트러스트 제품·서비스에 대한 연동체계 개발 및 수요기업 대상 보안모델 도입·운영 지원, △컨설팅 : 민간 기업 대상 제로트러스트 관점에서 현 보안현황을 진단하고 향후 도입·전환에 대한 계획 수립 지원

상 어려운 실정이다.

실제로 한국정보보호산업협회가 2023년 실시한 '제로트러스트 수요·공급기업 실태조사'에 따르면, 공급기업들은 제로트러스트 활성화 방안으로 관련 법령 등 도입정책이 가장 중요하다고 답변하였다.[18)]

하지만 현재 관련 근거는 가이드라인 수준에 머물고 있으며, 기업 지원을 위한 법적 장치도 부재하다.

더욱이 정부의 제로트러스트 지원 사업 예산도 2024년 62억 원에서 2025년 56억 원, 2026년 45억 원(예산안 기준)으로 매년 줄어들고 있다.[19)]

이처럼 제한적인 예산 규모로 인해 시범사업이나 컨설팅 사업과 관련하여 중소기업이 체감할 수 있는 실질적 지원은 충분하지 않으며,[20)] 중소기업의 특성과 보안 여건을 고려한 '중소기업 특화형 지원 사업'은 부재한 상황이다.

따라서 중소기업에 제로트러스트를 본격적으로 확산하기 위해서는 법적 근거를 마련하여 정책의 지속성과 안정성을 확보하고 현장에서 체감 가능한 재적정 지원도 뒷받침될 필요가 있다.

법제화 방안으로 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 개정하여 제로트러스트 정의, 기본원칙, 정부 지원 근거 등을 명확히 하는 방안을 고려할 수 있다.

아울러, 정부의 제로트러스트 지원 예산을 확충하여 기존 시범사업 등을 확대하고, 특히 중소기업을 대상으로 한 특화 사업을 신설할 필요가 있다. 이와 관련해 중소기업의 제로트러스트 도입을 위한 바우처 제도[21)]를 신설하여 컨설팅 및 솔루션 도입 비용을 지원하는 등 기업의 재정적 부담을 실질적으로 완화할 필요가 있다는 의견이 있다.[22)]

### (3) 중소기업 정보보호 투자 유인책 마련

재정 여력이 부족한 중소기업의 보안역량을 강화하기 위해서는 정부의 재정 지원을 확대할 필요가 있으나, 직접적 재정 지원에는 한계가 있는 만큼 자발적 보안 투자를 유인할 수 있는 제도적 장치가 병행되어야 한다.

그런데 현행 정책은 규제 강화에 편중된 경향이 있어, 중소기업의 자발적 보안 투자 확대를 이끌어내기에는 한계가 있어 보인다.

최근 발표된 '범부처 정보보호 종합대책('25.10.22.)'에서도 보안 의무 위반에 대한 과태료·과징금 상향, 징벌적 과징금 도입 등 규제 중심의 대책은 강화되었으나, 보안 투자 시 체감할 수 있는 세제혜택 등 구체적 인센티브 등은 제시되지 않았다.

이와 관련하여 제22대 국회에는 중소기업 등의 정보보호 투자 촉진을 위한 「조세특례제한법 일부개정법률안」이 계류 중이다.[23)] 개정안은 정보보호를 위한 시스템·설비 투자비용, 컨설팅 비용, 관련 보험 가입비용과 정보보호 전문인력 신규 채용 비용에 대해 세액공제를 하되, 중소기업에는 더 높은 공제율을 적용하도록 설계되어 있다.

관련 법적 근거가 마련된다면 중소기업의 자율적 보안투자 환경을 조성하고, 정부 재정 지원에 대한 의존도를 점진적으로 완화하는 효과가 있을 것으로 기대된다.

아울러, 정보보호 투자 규모에 따른 과징금 감면, 정부조달 우대, 자율공시 중소기업에 대한 정보보호 관리체계 인증 수수료 감면 비율[24)] 확대 등 세제지원 외의 실효성 있는 유인책도 함께 모색할 필요가 있다.

『이슈와 논점』은 국회의원의 입법활동을 지원하기 위해 최신 국내외 동향 및 현안에 대해 수시로 발간하는 보고서입니다.

18) 과학기술정보통신부 외, 『제로트러스트 가이드라인 2.0』, 2024, pp.194~201.

19) 과학기술정보통신부 제출자료(2025.10.17.)

20) 2025년 기준 시범사업 수요기업 8개 사 중 중소기업은 1개 사, 컨설팅 사업 8개 사 중 중소기업은 2개 사이다(과학기술정보통신부 제출자료(2025.11.13.)).

21) 중소벤처기업부는 코로나 19 대응을 위해 한시적(2020년~2023년)으로 비대면 서비스 바우처 지원 사업(비대면 서비스 도입, 활용 등에 사용 가능한 바우처를 지급한 사업으로, 화상회의, 재택근무, 네트워크·보안 솔루션, 메타버스 사무실 서비스 분야 중 도입 지원)을 실시한 바 있다.

22) 임종인, 「AI강국으로의 도약, 제로트러스트에 길을 묻다(한국의 미래 보안 전략:시장 전망과 가속화 방안」, 한국제로트러스트보안협회 주최 AI보안 간담회 자료, 2025, p.8.

23) 이해민의원 대표발의, 「조세특례제한법 일부개정법률안(의안번호 2211163)」, 2025.6.30.

24) 현재는 「정보보호산업의 진흥에 관한 법률」 제13조(정보보호 공시) 제3항에 따라 수수료의 100분의 30에 해당하는 금액을 할인받을 수 있다.

07233 서울시 영등포구 의사당대로 1 국회입법조사처
Tel. 02-6788-4510
발간등록번호 31-9735044-001340-14
ISSN 2005-744X