



제429회 국회(정기회)
제7차 산업통상자원중소벤처기업위원회

산업기술의 유출방지 및 보호에 관한 법률 일부개정법률안

검 토 보 고

〈국가핵심기술 침해사고 발생 시 신고의무 부과〉

■ 김정호의원 대표발의(의안번호 제2212249호)

2025. 11.

산업통상자원중소벤처기업위원회

수석전문위원 박희석

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	2

I. 제안경위

1. 제 안 자 : 김정호의원 등 10인
2. 제 안 일 : 2025. 8. 19.
3. 회 부 일 : 2025. 8. 20.

II. 제안이유 및 주요내용

제안이유 및 주요내용

최근 글로벌 해커 조직들이 반도체, 이차전지 등 국가첨단전략산업의 대기업과 협력관계에 있는 중소기업을 해킹하여 간접적으로 산업기술을 침해하려는 사건이 발생하고 있음.

그런데 현재 국가핵심기술 및 국가연구개발사업으로 개발한 산업기술을 보유한 대상기관에 대해서는 산업기술 침해행위가 발생할 우려가 있거나 발생한 때에 즉시 산업통상자원부장관 및 정보수사기관의 장에게 그 사실을 신고하도록 의무를 부과하고 있으나, 대상기관의 협력업체의 경우에는 해킹 등 사이버 침해사고가 발생하여 산업기술 침해가 우려되더라도 신고의무가 없어 보안의 사각지대가 있는 상황임.

이에 국가핵심기술을 보유한 대상기관의 협력업체에 대하여 해킹 등 침해사고가 발생한 경우에는 신고의무를 부과하고, 침해사고 대응 및 방지를 위하여 필요한 지원을 할 수 있도록 함으로써 산업기술 보호에 만전을 기하려는 것임(안 제15조 및 제22조 등).

Ⅲ. 검토의견

개정안은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제7호에 따른 침해사고가 발생할 경우 국가핵심기술을 보유한 대상기관의 협력업체로 하여금 즉시 산업통상부장관 및 정보수사기관의 장에게 그 사실을 신고하도록 하고(안 제15조제2항 신설),

정부가 협력업체에 대하여 침해사고로 인한 보안시스템의 복구에 소요되는 비용의 보조 등 침해사고 대응 및 방지를 위하여 필요한 지원을 할 수 있도록 하려는 것임(안 제22조제2항 신설 등).

개정안 조문대비표

현행	개정안
제15조(산업기술 침해신고 등) ① (생략) <u><신설></u>	제15조(산업기술 침해신고 등) ① (현행과 같음) ② <u>국가핵심기술을 보유한 대상기관의 협력업체(대상기관에 국가핵심기술 관련 물품·용역을 공급하거나 대상기관과 「하도급거래 공정화에 관한 법률」 제2조제1항에 따른 하도급거래에 관한 계약을 체결한 자 중 대통령령으로 정하는 자를 말한다)는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제7호에 따른 침해사고(이하 “침해사</u>

② 산업통상자원부장관 및 정보수사기관의 장은 제1항의 신고를 받은 경우 또는 제14조에 따른 금지행위를 인지한 경우에는 필요한 조사 및 조치를 하여야 한다.

③ 산업통상자원부장관 및 정보수사기관의 장은 제2항에 따른 조사 및 조치를 한 경우에 그 결과를 정보수사기관의 장 또는 산업통상자원부장관에게 각각 통보하여야 한다. 다만, 정보수사기관의 장이 국가안전보장을 위하여 필요하다고 인정하는 경우에는 통보하지 아니할 수 있다.

<신 설>

제22조(산업기술의 보호를 위한 지원)

① (생략)

<신 설>

② 제1항의 규정에 따른 지원에 관하여 필요한 사항은 대통령령으로

고”라 한다)가 발생한 때에는 즉시 산업통상자원부장관 및 정보수사기관의 장에게 그 사실을 신고하여야 한다.

③ -----
-----제1항 및 제2항의 신고
-----제14조에 따른
금지행위나 제2항에 따른 침해사고
를 인지한 경우-----
-----.

④ -----
-----제3항-----

-----.

-----.

⑤ 제1항 및 제2항에 따른 신고의 대상·방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제22조(산업기술의 보호를 위한 지원)

① (현행과 같음)

② 정부는 제15조제2항에 따른 협력업체에 대하여 침해사고로 인한 보안시스템의 복구에 소요되는 비용의 보조 등 침해사고 대응 및 방지를 위하여 필요한 지원을 할 수 있다.

③ 제1항 및 제2항-----

정한다. 제34조(비밀유지의무) 다음 각 호의 어느 하나에 해당하거나 해당하였던 자는 그 직무상 알게 된 비밀을 누설하거나 도용하여서는 아니 된다. 1. ~ 3의3. (생략) 4. <u>제15조의 규정에 따라 침해행위의 접수 및 방지 등의 업무를 수행하는 자</u> 5. ~ 10. (생략) 제35조(벌칙 적용에서의 공무원 의제) 다음 각 호의 업무를 행하는 자는 「형법」 제129조 내지 제132조를 적용함에 있어서는 이를 공무원으로 본다. 1.·2. (생략) 3. <u>제15조의 규정에 따라 침해행위의 접수 및 방지 등의 업무를 수행하는 자</u> 4. ~ 6. (생략) 제39조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자는 1천만원 이하의 과태료에 처한다. 다만, 제4호의 경우에는 국가를 제외한다. 1. ~ 5. (생략) 6. <u>제15조제1항의 규정에 따른 산업기술 침해신고</u>를 하지 아니한 자 7. (생략)	-----. 제34조(비밀유지의무) ----- ----- ----- -----. 1. ~ 3의3. (현행과 같음) 4. <u>제15조제1항에 따른 침해행위나 같은 조 제2항에 따른 침해사고</u>----- ----- 5. ~ 10. (현행과 같음) 제35조(벌칙 적용에서의 공무원 의제) ----- ----- ----- -----. 1.·2. (현행과 같음) 3. <u>제15조제1항에 따른 침해행위나 같은 조 제2항에 따른 침해사고의</u>----- ----- 4. ~ 6. (현행과 같음) 제39조(과태료) ① ----- ----- -----. -----. 1. ~ 5. (현행과 같음) 6. <u>제15조제1항 및 제2항의 규정에 따른 신고</u>----- 7. (현행과 같음)
--	--

현행법 제14조1)에서는 누구든지 절취·기망·협박 그 밖의 부정한 방법으로 대상기관의 산업기술을 취득하는 행위 또는 그 취득한 산업기술을 사용하거나 공개하는 행위 등 산업기술의 유출 및 침해행위를 금지하는 사항을 규정하고 있음.

1) 「산업기술의 유출방지 및 보호에 관한 법률」

제14조(산업기술의 유출 및 침해행위 금지) 누구든지 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 절취·기망·협박 그 밖의 부정한 방법으로 대상기관의 산업기술을 취득하는 행위 또는 그 취득한 산업기술을 사용하거나 공개(비밀을 유지하면서 특정인에게 알리는 것을 포함한다. 이하 같다)하는 행위
2. 제34조의 규정 또는 대상기관과의 계약 등에 따라 산업기술에 대한 비밀유지의무가 있는 자가 대상기관의 산업기술을 유출하거나 그 유출한 산업기술을 사용 또는 공개하거나 제3자가 사용하게 하는 행위
3. 제34조 또는 대상기관과의 계약 등에 따라 산업기술에 대한 비밀유지의무가 있는 자가 산업기술에 대한 보유 또는 사용 권한이 소멸됨에 따라 대상기관으로부터 산업기술에 관한 문서, 도화(圖畵), 전자기록 등 특수매체기록이나 원시코드 등의 반환이나 산업기술의 삭제를 요구받 고도 이를 거부 또는 기피하거나 그 사본을 보유하는 행위
4. 대상기관의 계약 등에 따라 산업기술에 대한 접근 권한이 있는 자가 산업기술을 지정된 장소 밖으로 무단으로 유출하거나 목적 외로 사용·공개하는 행위
5. 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 취득·사용·공개하거나 산업기술을 취득한 후에 그 산업기술에 대하여 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 사용하거나 공개하는 행위
6. 제1호부터 제4호까지의 어느 하나에 해당하는 행위를 소개·알선·유인하는 행위
7. 제11조제1항의 규정에 따른 승인을 얻지 아니하거나 부정한 방법으로 승인을 얻어 국가핵심 기술을 수출하는 행위
8. 제11조제4항에 따른 신고를 하지 아니하거나 거짓이나 그 밖의 부정한 방법으로 신고를 하고 국가핵심기술을 수출하는 행위
9. 제11조의2제1항에 따른 승인을 받지 아니하거나 거짓이나 그 밖의 부정한 방법으로 승인을 받아 해외인수·합병등을 하는 행위
10. 제11조의2제5항 및 제6항에 따른 신고를 하지 아니하거나 거짓이나 그 밖의 부정한 방법으로 신고를 하고서 해외인수·합병등을 하는 행위
11. 제11조제6항·제8항 및 제11조의2제8항·제10항에 따른 산업통상부장관의 명령을 이행하지 아니하는 행위
12. 산업기술 관련 소송 등 대통령령으로 정하는 적법한 경로를 통하여 산업기술이 포함된 정보를 제공받은 자가 정보를 제공받은 목적 외의 다른 용도로 그 정보를 사용하거나 공개하는 행위
13. 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 취득·사용 및 공개하거나 산업기술을 취득한 후에 그 산업기술에 대하여 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 사용하거나 공개하는 행위

또한, 현행법 제15조²⁾에서는 국가핵심기술 및 국가연구개발사업으로 개발한 산업기술을 보유한 대상기관의 장으로 하여금 제14조에 따른 금지 대상 행위가 발생할 우려가 있거나 발생한 때에는 즉시 산업통상부장관 및 정보수사기관의 장에게 그 사실을 신고하도록 의무화하고 있음.

그런데, 최근 산업기술의 유출 양상이 고도화·간접화됨에 따라, 산업기술을 직접 보유한 기관뿐만 아니라 그 협력망(supply chain)에 포함된 중소 협력업체를 경유한 해킹·사이버 공격 사례³⁾가 발생하고 있음.

이러한 공급망 기반의 해킹 시도는 개별 사례에 그치지 않고, 국내 전체 침해사고 통계에서도 확인되는데, 실제로 한국인터넷진흥원(KISA)에 신고된 국내 해킹 등 침해사고 추이를 보면 신고 건수가 2021년 640건에서 2024년 1,887건으로 약 3배 증가하는 등 최근 4년간 큰 폭으로 증가하였고,

2) 「산업기술의 유출방지 및 보호에 관한 법률」

제15조(산업기술 침해신고 등) ①국가핵심기술 및 국가연구개발사업으로 개발한 산업기술을 보유한 대상기관의 장은 제14조 각 호의 어느 하나에 해당하는 행위가 발생할 우려가 있거나 발생한 때에는 즉시 산업통상부장관 및 정보수사기관의 장에게 그 사실을 신고하여야 한다.

②산업통상부장관 및 정보수사기관의 장은 제1항의 신고를 받은 경우 또는 제14조에 따른 금지행위를 인지한 경우에는 필요한 조사 및 조치를 하여야 한다.

③ 산업통상부장관 및 정보수사기관의 장은 제2항에 따른 조사 및 조치를 한 경우에 그 결과를 정보수사기관의 장 또는 산업통상부장관에게 각각 통보하여야 한다. 다만, 정보수사기관의 장이 국가안전보장을 위하여 필요하다고 인정하는 경우에는 통보하지 아니할 수 있다.

3) ‘TSMC “협력사 해킹 피해”…랜섬 해커그룹, 923억원 요구’ (연합뉴스, 2023. 7. 2.)

최근 4년간 민간기업 대상 사이버 해킹 침해사고 신고 현황

구 분	2021년	2022년	2023년	2024년
신고 건수	640건	1,142건	1,277건	1,887건

자료: 한국인터넷진흥원

2025년 1월부터 8월 말까지 신고된 총 1,410건 중 85.5%인 1,205건이 중소기업에서 발생한 것으로 나타나⁴⁾, 침해사고가 상대적으로 보안이 취약한 중소기업에 집중되고 있음을 확인할 수 있음.

2025년 8월 기준 기업 규모별 사이버 해킹 침해사고 신고 현황

구 분	대기업	중견기업	중소기업	합 계
신고 건수	53건 (3.7%)	152건 (10.8%)	1,205건 (85.5%)	1,410건 (100%)

자료: 한국인터넷진흥원

또한, 현행법 제10조⁵⁾ 및 시행령 제14조⁶⁾는 국가핵심기술을 보유·관

4) "최근 5년 국내기업서 발생한 사이버 해킹 6447건"…기하급수 증가 (뉴스1, 2025. 9. 21)

5) 「산업기술의 유출방지 및 보호에 관한 법률」

제10조(국가핵심기술의 보호조치) ① 국가핵심기술을 보유·관리하고 있는 대상기관의 장은 국가핵심기술의 유출을 방지하기 위하여 다음 각 호에 따른 조치를 하여야 한다.

1. 보호구역의 설정·출입허가 또는 출입 시 휴대품 검사
2. 국가핵심기술을 취급하는 전문인력의 이직 관리 및 비밀유지 등에 관한 계약 체결
3. 그 밖에 국가핵심기술 유출 방지를 위하여 대통령령으로 정하는 사항

② 제1항의 규정에 따른 조치에 관하여 필요한 사항은 대통령령으로 정한다.
 ③ 누구든지 정당한 사유 없이 제1항의 보호조치를 거부·방해 또는 기피하여서는 아니 된다.

6) 「산업기술의 유출방지 및 보호에 관한 법률 시행령」

제14조(국가핵심기술의 보호조치) 법 제10조제1항제3호에서 “대통령령으로 정하는 사항”이란 다음 각 호의 사항을 말한다.

1. 국가핵심기술에 대한 보호 등급의 부여와 보안관리규정의 제정
2. 국가핵심기술 관리책임자 및 보안 전담인력의 지정

리하고 있는 대상기관⁷⁾으로 하여금 의무적으로 국가핵심기술의 유출을 방지하기 위한 다양한 보호조치를 취하도록 하여 높은 보안 관리 수준을 유지하도록 요구하고 있으나,

대상기관의 협력업체⁸⁾는 이러한 보호조치의 의무 대상에 포함되어 있지 않음에 따라, 상대적으로 보안 관리 수준이 낮은 협력업체의 정보망을 우회경로로 활용하여 국가핵심기술을 탈취하는 ‘공급망 공격(supply chain attack)⁹⁾’이 큰 위협으로 부상하고 있음.

이에 개정안은 국가핵심기술을 보유한 대상기관의 협력업체에 대해서

-
3. 국가핵심기술 보호구역의 통신시설과 통신수단에 대한 보안
 4. 국가핵심기술 관련 정보의 처리 과정과 결과에 관한 자료의 보호
 5. 국가핵심기술을 취급하는 전문인력의 구분 및 관리
 6. 국가핵심기술을 취급하는 전문인력에 대한 보안교육 실시
 7. 국가핵심기술의 유출 사고에 대한 대응체제 구축

7) 「산업기술의 유출방지 및 보호에 관한 법률」

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

2. “국가핵심기술”이라 함은 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술로서 제9조의 규정에 따라 지정된 것을 말한다.
4. “대상기관”이란 산업기술을 보유한 기업·연구기관·전문기관·대학 등을 말한다.

- 8) 안 제15조제2항에서는 국가핵심기술을 보유한 대상기관의 협력업체를 대상기관에 국가핵심기술 관련 물품·용역을 공급하거나 대상기관과 「하도급거래 공정화에 관한 법률」 제2조제1항*에 따른 하도급거래에 관한 계약을 체결한 자 중 대통령령으로 정하는 자로 정의하고 있음.

* 「하도급거래 공정화에 관한 법률」

제2조(정의) ① 이 법에서 “하도급거래”란 원사업자가 수급사업자에게 제조위탁(가공위탁을 포함한다. 이하 같다)·수리위탁·건설위탁 또는 용역위탁을 하거나 원사업자가 다른 사업자로부터 제조위탁·수리위탁·건설위탁 또는 용역위탁을 받은 것을 수급사업자에게 다시 위탁한 경우, 그 위탁(이하 “제조등의 위탁”이라 한다)을 받은 수급사업자가 위탁받은 것(이하 “목적물등”이라 한다)을 제조·수리·시공하거나 용역수행하여 원사업자에게 납품·인도 또는 제공(이하 “납품등”이라 한다)하고 그 대가(이하 “하도급대금”이라 한다)를 받는 행위를 말한다.

- 9) 공급망 공격(supply chain attack)이란 공격자가 조직의 소프트웨어, 하드웨어, 또는 서비스 공급망 내의 취약한 요소를 이용해 침입하는 사이버 공격을 의미하며, 신뢰할 수 있는 제3자 소프트웨어 업데이트나 부품을 통해 악성코드를 유포하거나, 소프트웨어 개발 및 유통 과정에 침투해 정상적인 제품인 것처럼 위장한 악성 소프트웨어를 유포하는 방식으로 이루어짐.

도 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”) 제2조제7호¹⁰⁾에 따른 침해사고(이하 “침해사고”) 발생 시 신고의무를 부과하고,

침해사고로 인한 협력업체의 보안시스템 복구 비용 지원 등 정부의 침해사고 대응·방지 지원 근거를 마련함으로써 국가핵심기술 보유기관으로의 피해 확산을 예방하고 국가핵심기술의 공급망 보안을 체계적으로 강화하려는 것임.

협력업체가 보유·처리하는 정보에는 단순한 거래·생산 데이터뿐만 아니라 설계도면, 제조공정, 기술사양 등 국가핵심기술과 직·간접적으로 연관된 데이터가 포함되는 경우가 많아 협력업체에 대한 해킹 등 침해사고는 곧바로 산업기술 보유기관의 기술유출 피해로 직결될 수 있음.

그럼에도 불구하고 현행법은 산업기술을 직접 보유한 대상기관만을 신고 의무자로 한정하고 있어, 협력업체 단계에서 발생하는 침해사고를 조기에 탐지하거나 정부가 선제적으로 대응할 수 없는 한계가 있음을 고려해 볼 때,

10) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

7. “침해사고”란 다음 각 목의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.

가. 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법

나. 정보통신망의 정상적인 보호·인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하는 방법

개정안의 내용은 산업기술 보호의 실질적인 범위를 기술 보유기관에서 협력 생태계 전체로 확장하여 국가핵심기술의 유출 위험을 선제적·실효적으로 차단하려는 것으로서 합리적이고 시의적절한 조치로 보임.

산업통상부는 개정안에 찬성하면서도, 국가핵심기술이 침해되었거나 침해될 우려가 있는 경우 국가핵심기술 보유기관의 침해신고를 의무화하고 있는 현행법의 입법취지와 관계기관의 전문성¹¹⁾ 및 의견¹²⁾ 등을 종합적으로 고려해 볼 때,

침해사고 신고의무가 부과되는 협력업체의 기준¹³⁾을 ‘국가핵심기술 관련 정보를 제공받아 대상기관에 소재·부품·장비를 공급하거나 국가핵심기술 관련 제조·수리·시공 또는 용역수행을 위탁받은 자’로 법률에 명시하고,

11) 침해신고가 있는 경우, 신고를 받은 기관은 필요한 조사 및 조치를 하여야 하는 바, 산업통상부장관 및 정보수사기관의 장이 해킹 등 「정보통신망법」상 침해사고*에 대응한 조사 및 조치 전문성에도 한계

* 침해사고 : 해킹, 컴퓨터바이러스, 메일폭탄, 보호·인증절차 우회프로그램 설치등의 방법으로 정보통신망 등을 공격하는 행위로 인해 발생한 사태(「정보통신망법」 제2조제7호)
→ 침해사고 발생 시 과학기술정보통신부장관 및 한국인터넷진흥원에 신고하도록 하고, 침해신고를 받은 기관은 필요한 조치를 취하도록 규정(「정보통신망법」 제48조의3)

12) 국가정보원 입장: 기관별 전문성을 고려하여 해킹 등 침해사고 발생 시에는 과학기술정보통신부장관 및 한국인터넷진흥원이, 국가핵심기술 침해사고 발생 시에는 산업통상부장관 및 정보수사기관의 장이 필요한 조치를 취하도록 하는 것이 바람직함.

13) 안 제15조제2항에서는 국가핵심기술을 보유한 대상기관의 협력업체를 대상기관에 국가핵심기술 관련 물품·용역을 공급하거나 대상기관과 「하도급거래 공정화에 관한 법률」 제2조제1항*에 따른 하도급거래에 관한 계약을 체결한 자 중 대통령령으로 정하는 자로 정의하여 협력업체의 세 부 기준을 대통령령에 위임하고 있음.

신고 대상이 되는 침해사고의 범위¹⁴⁾를 「정보통신망법」에 따른 침해사고의 발생으로 인해 국가핵심기술이 침해되었거나 침해될 우려가 있는 경우에 해당되는 경우로 그 범위를 한정하는 것이 바람직해 보인다는 입장임.

한편, 개정안에서는 현행법 제34조¹⁵⁾의 비밀유지의무 대상과 제35조¹⁶⁾의 벌칙 적용에서의 공무원 의제 대상에 침해사고의 접수 및 방지 등의 업무를 수행하는 자를 추가하고,

침해사고의 신고의무를 이행하지 않는 경우 1천만원 이하의 과태료를 부과하고 있는데, 이는 산업기술 유출 방지 및 신고 절차 이행의 실효성을 확보하기 위해 필요한 조치로 보임.

14) 안 제15조제2항에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제7호에 따른 침해사고가 발생한 때에는 즉시 산업통상부장관 및 정보수사기관의 장에게 그 사실을 신고하도록 하여, 신고 대상이 되는 침해사고의 범위를 한정하지 않고 있음.

15) 「산업기술의 유출방지 및 보호에 관한 법률」 제34조(비밀유지의무) 다음 각 호의 어느 하나에 해당하거나 해당하였던 자는 그 직무상 알게 된 비밀을 누설하거나 도용하여서는 아니 된다.

4. 제15조의 규정에 따라 침해행위의 접수 및 방지 등의 업무를 수행하는 자

16) 「산업기술의 유출방지 및 보호에 관한 법률」 제35조(벌칙 적용에서의 공무원 의제) 다음 각 호의 업무를 행하는 자는 「형법」 제129조 내지 제132조를 적용함에 있어서는 이를 공무원으로 본다.

3. 제15조의 규정에 따라 침해행위의 접수 및 방지 등의 업무를 수행하는 자

문 의 처
02)6788-5457