



제 428회 국회 (임시회)
제2차 과학기술정보방송통신위원회

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

검 토 보 고

〈IoT 보안인증제도 실효성 제고〉

■ 이정현의원 대표발의(의안번호 제2208928호)

2025. 8.

과학기술정보방송통신위원회

수석전문위원 이복우

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	2
1. IoT 보안인증제도 실효성 제고(안 제48조의6 제7항 신설 등)	2

I. 제안경위

가. 발 의 자 : 이정현의원 등 14인

나. 발 의 일 : 2025. 3. 14.

다. 회 부 일 : 2025. 3. 17.

II. 제안이유 및 주요내용

현행법에 따르면 과학기술정보통신부장관은 정보통신망연결기기등이 정보통신망의 안정성 및 정보의 신뢰성 확보 등에 관한 인증기준에 적합한 경우 정보보호인증을 할 수 있음.

그런데, 현행법상 정보보호인증제도가 의무인증제도가 아닌 임의인증제도로 규정되어 있어 해외 기업이 제조한 정보통신망연결기기등이 정보보호인증을 받지 않고 수입되고 있는 등 정보보호인증 실적이 저조함.

이에 정보보호인증을 받은 자는 정보보호인증의 내용을 표시하거나 홍보할 수 있도록 하고, 과학기술정보통신부장관이 중앙행정기관 등에 정보보호인증을 받은 정보통신망연결기기등의 우선구매 등을 요청할 수 있도록 하며, 정보보호인증을 받으려는 자에 대한 지원 근거를 마련함으로써 기업 등이 정보보호인증을 받을 유인을 높여 정보보호인증제도의 실효성을 제고하려는 것임(안 제48조의6제7항부터 제9항까지 신설 등).

Ⅲ. 검토의견

1. IoT 보안인증제도 실효성 제고(안 제48조의6 제7항 신설 등)

가. 개정안 요지

- 정보통신망연결기기등에 대한 정보보호인증을 받은 자는 대통령령으로 정하는 바에 따라 정보보호인증의 내용을 표시하거나 홍보할 수 있으며, 정보보호인증을 받은 자가 아니면 정보보호인증의 내용 또는 이와 비슷한 표시를 하거나 홍보하여서는 아니 됨(안 제48조의6 제7항 신설).
- 정보보호인증을 받지 아니하고 정보보호인증의 내용을 표시 또는 이와 비슷한 표시를 하거나 홍보한 자에 대하여 1천만원 이하의 과태료를 부과함(안 제76조 제3항 제12호의2 신설).
- 과학기술정보통신부장관은 중앙행정기관, 지방자치단체, 공기업·준정부 기관 등에 정보보호인증을 받은 정보통신망연결기기등의 우선구매 등 필요한 조치를 요청할 수 있음(제8항 신설).
- 과학기술정보통신부장관은 정보보호인증을 받으려는 자에 대하여 관련 비용 및 기술 등 필요한 지원을 할 수 있음(제9항 신설).

나. 개정안 조문대비표

현 행	개 정 안
제48조의6(정보통신망연결기기등에 관한 인증) ① ~ ⑥ (생략)	제48조의6(정보통신망연결기기등에 관한 인증) ① ~ ⑥ (현행과 같음)

현행	개정안
<u><신 설></u> ⑦ (생략) 제76조(과태료) ①·② (생략) ③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다. 1. ~ 12. (생략) <u><신 설></u> 12의2. (생략) 12의3. (생략) 13. ~ 25. (생략) ④ (생략)	<u>인정하는 기관</u> ⑨ 과학기술정보통신부장관은 정보보호인증을 받으려는 자에 대하여 정보보호인증에 관련된 비용 및 기술 등 필요한 지원을 할 수 있다. ⑩ (현행 제7항과 같음) 제76조(과태료) ①·② (현행과 같음) ③ ----- ----- -----. 1. ~ 12. (현행과 같음) 12의2. 제48조의6제7항을 위반하여 정보보호인증의 내용을 표시 또는 이와 비슷한 표시를 하거나 홍보한 자 12의3. (현행 제12호의2와 같음) 12의5. (현행 제12호의3과 같음) 13. ~ 25. (현행과 같음) ④ (현행과 같음)

다. 검토사항

- 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”) 제48조의6은 과학기술정보통신부장관이 정보통신망의 안정성 및 정보의 신뢰성 확보 등에 관한 인증기준을 정하고,

해당 기준에 적합한 정보통신망연결기기등에 대하여 정보보호인증(이하 “IoT 보안인증”)을 할 수 있도록 하고 있음¹⁾²⁾.

- ‘정보통신망연결기기등’이란 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 것으로서³⁾, 정보통신망에 연결되어 정보를 송·수신할 수 있는 사물인터넷(IoT) 기기와, 관리·제어 등의 목적으로 IoT 기기와 연동하는 IoT 앱을 의미함.

- 2025년 6월 기준 IoT 보안인증을 받은 정보통신망연결기기등은 총 441개임.

-
- 1) 제48조의6(정보통신망연결기기등에 관한 인증) ① 과학기술정보통신부장관은 제4항에 따른 인증시험대행기관의 시험 결과 정보통신망연결기기등이 제2항에 따른 인증기준에 적합한 경우 정보보호인증을 할 수 있다.
- ② 과학기술정보통신부장관은 제1항에 따른 정보보호인증(이하 “정보보호인증”이라 한다)을 위하여 정보통신망의 안정성 및 정보의 신뢰성 확보 등에 관한 인증기준을 정하여 고시할 수 있다.
- ③ 과학기술정보통신부장관은 정보보호인증을 받은 자가 다음 각 호의 어느 하나에 해당하는 경우에는 그 정보보호인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 그 정보보호인증을 취소하여야 한다.
1. 거짓이나 그 밖의 부정한 방법으로 정보보호인증을 받은 경우
 2. 제2항에 따른 인증기준에 미달하게 된 경우
- ④ 과학기술정보통신부장관은 정보통신망연결기기등이 제2항에 따른 인증기준에 적합한지 여부를 확인하는 시험을 효율적으로 수행하기 위하여 필요한 경우에는 대통령령으로 정하는 지정기준을 충족하는 기관을 인증시험대행기관으로 지정할 수 있다.
- ⑤ 과학기술정보통신부장관은 제4항에 따라 지정된 인증시험대행기관(이하 “인증시험대행기관”이라 한다)이 다음 각 호의 어느 하나에 해당하면 인증시험대행기관의 지정을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 그 지정을 취소하여야 한다.
1. 거짓이나 그 밖의 부정한 방법으로 지정을 받은 경우
 2. 제4항에 따른 지정기준에 미달하게 된 경우
- ⑥ 과학기술정보통신부장관은 정보보호인증 및 정보보호인증 취소에 관한 업무를 한국인터넷진흥원에 위탁할 수 있다.
- ⑦ 정보보호인증·정보보호인증 취소의 절차 및 인증시험대행기관의 지정·지정취소의 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.
- 2) IoT 보안인증에 대한 세부내용은 참고자료 참조
- 3) 제45조(정보통신망의 안정성 확보 등) ① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.
2. 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 기기·설비·장비(이하 “정보통신망연결기기등”이라 한다)를 제조하거나 수입하는 자

<IoT 보안인증 대상>

분야	내용
가전	스마트 홈네트워크에 연결되는 멀티미디어 제품, 주방가전 제품 또는 생활가전 제품 등의 가전제품 또는 그 제품에 사용되는 기기·설비·장비
교통	지능형교통체계, 드론, 자동차, 선박 등에 사용되는 기기·설비·장비
금융	「전자금융거래법」 제2조제8호에 따른 전자적 장치
스마트 도시	「스마트도시 조성 및 산업진흥 등에 관한 법률」 제2조제2호에 따른 스마트도시서비스에 사용되는 기기·설비·장비
의료	「의료기기법」 제2조제1항에 따른 의료기기 중 통신기능을 보유한 기기·설비·장비
제조·생산	제품의 제조·생산 또는 용역을 관리하기 위하여 제어·점검·측정·탐지 등의 용도로 사용되는 기기·설비·장비
주택	「건축법」 제2조제1항제4호에 따른 건축설비 중 지능형 홈네트워크에 연결되는 기기·설비·장비
통신	「전파법」 제2조제16호에 따른 방송통신기자재 중 무선 또는 유선으로 통신이 가능한 방송통신기자재

(정보통신망법 시행령 [별표 1의3])

○ 개정안은 최근 침해사고 증가에 따라 정보통신 기기·설비 등에 대한 보안의 중요성이 증가하고 있음을 감안하여,

IoT 보안인증을 받은 자가 그 내용을 표시·홍보할 수 있도록 하고, 중앙행정기관, 지방자치단체, 공기업·준정부기관 등이 IoT 보안인증을 받은 제품을 우선적으로 구매하도록 과학기술정보통신부장관이 요청할 수 있도록 하며,

IoT 보안인증에 관한 비용 및 기술 등을 지원할 수 있도록 함으로써 민간기업들이 자발적으로 보안인증을 받을 유인을 제공하고 IoT 보안인증을 활성화하려는 것으로 그 취지가 타당하다고 보임.

- 참고로, 현행 정보통신망법은 유사한 인증제도인 정보보호 관리체계 인증 및 정보보호 관리등급에 대하여 이를 받은 자가 해당 사실을 표시·홍보할 수 있도록 하고 있으며⁴⁾,
- 소기업 등에 대해서는 정보보호 관리체계 인증에 관련된 비용·기술 등을 지원할 수 있도록 하고 있음⁵⁾.
- 다만, IoT 보안인증을 받은 제품의 우선구매에 대해서는 다음 사항을 검토할 필요가 있음.

4) **제47조(정보보호 관리체계의 인증)** ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 “정보보호 관리체계”라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

1. 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”라 한다)
2. 집적정보통신시설 사업자
3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

⑨ 제1항 및 제2항에 따라 정보보호 관리체계의 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.

제47조의5(정보보호 관리등급 부여) ① 제47조에 따라 정보보호 관리체계 인증을 받은 자는 기업의 통합적 정보보호 관리수준을 제고하고 이용자로부터 정보보호 서비스에 대한 신뢰를 확보하기 위하여 과학기술정보통신부장관으로부터 정보보호 관리등급을 받을 수 있다.

③ 제1항에 따라 정보보호 관리등급을 받은 자는 대통령령으로 정하는 바에 따라 해당 등급의 내용을 표시하거나 홍보에 활용할 수 있다.

5) **제47조의7(정보보호 관리체계 인증의 특례)** ① 과학기술정보통신부장관은 제47조제1항 및 제2항에 따른 인증을 받으려는 자 중 다음 각 호의 어느 하나에 해당하는 자에 대하여 제47조에 따른 인증기준 및 절차 등을 완화하여 적용할 수 있다.

1. 「중소기업기본법」 제2조제2항에 따른 소기업
2. 그 밖에 정보통신서비스의 규모 및 특성 등에 따라 대통령령으로 정하는 기준에 해당하는 자

② 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 제1항에 관련된 비용 및 기술 등 필요한 지원을 할 수 있다.

□ IoT 보안인증 제품에 대한 우선구매 요청(안 제48조의6 제8항)

- 안 제48조의6 제8항은 중앙행정기관, 지방자치단체, 공기업·준정부기관 등이 IoT 보안인증을 받은 제품을 우선적으로 구매하도록 하려는 것으로서, 현행 「정보통신망연결기기등 정보보호인증에 관한 고시」(과학기술정보통신부고시) 제33조⁶⁾를 법률에 상향하여 규정하려는 것임⁷⁾.
- 다만 안 제4호는 ‘그 밖에 과학기술정보통신부장관이 인증기기등의 구매촉진 등을 위하여 필요하다고 인정하는 기관’에 대해 우선구매를 요청할 수 있도록 하고 있는데, 해당 기관에 민간기관도 포함될 수 있을 것으로 보임.
- 우선구매에 관한 타 입법례가 대부분 우선구매 요청 대상을 정부, 지자체, 공공기관 등 공공부문으로 한정하고 있는 점, 민간기관에게 사업 여건, 요구 사양, 다른 시스템과의 호환성 등을 고려하지 않고 인증기기등을 우선적으로 구매하도록 하는 것은 영업의 자유를 제한할 수 있는 점 등을 고려하여, 우선구매 요청 대상 기관을 공공부문으로 한정하여 규정하는 방안을 고려할 필요가 있음.

6) 제33조(우선구매 촉진) 과학기술정보통신부장관은 정보통신망연결기기등 정보보호인증을 받은 제품 등의 수요를 창출하기 위해 다음 각 호에서 정하는 기관에 우선구매 등을 요청할 수 있다.

1. 중앙행정기관

2. 지방자치단체

3. 「공공기관의 운영에 관한 법률」 제5조에 따른 공기업 및 준정부기관

4. 그 밖에 과학기술정보통신부장관이 구매촉진을 위하여 필요하다고 인정하는 기관

7) 과학기술정보통신부에 따르면 현재 해당 고시에 따른 우선구매 요청 사례는 없음

○ 과학기술정보통신부는 IoT 보안인증의 유인책을 마련하여 보안이 내재화된 IoT 제품의 확산을 지원하려는 취지에 공감하여 개정안에 동의하는 입장임.

다만, 개정안의 우선구매 대상 중 공공기관은 공기업(31개)·준정부기관(57개)으로 한정되어 있는데, 개정안의 효과성 제고 차원에서 기타 공공기관(243개)을 추가할 필요가 있다는 입장임.

문 의 처
02)6788-5230

※참고: 정보통신망연결기기등에 관한 정보보호인증 개요

(출처: 과학기술정보통신부)

□ 개 요

- (개요) 국민의 일상생활과 밀접한 사물인터넷(IoT) 제품·앱이 일정 수준 이상의 보안 요구조건을 갖추도록 하여 국민의 사생활 보호 지원
- (현황) 정보통신망법 개정(제48조의6, '21.9월)을 통해 IoT 제조기업들이 자율적으로 신청하여 인증을 받을 수 있도록 운영 중
 - IoT 사용 비중이 높은 가전, 주택 등 8개 분야를 인증대상으로 규정, TTA·KTC·KTR을 시험대행기관으로 지정하고 KISA에서 인증서 발급

인증대상	가전, 교통, 스마트도시, 의료, 제조 및 생산, 주택, 통신 등(8개 분야)
인증기준	식별·인증(초기 PW 변경 등 6개 항목), 데이터보호(중요정보 저장시 암호화 등5개 항목), 암호(안전한 암호 알고리즘 사용 등 4개 항목), SW보안(알려진 취약점 조치 등 7개 항목), 업데이트(자동업데이트 등 7개 항목), 네트워크보안(원격접속 통제 등 12개 항목), HW보안(인터페이스 보호 등 9개 항목)등 총 7개 영역 50개 항목

- 대상기기 및 보안요구 조건(개인정보 취급 여부) 등에 따라 '라이트', '베이직', '스탠다드'로 구분하여 운영 중

< IoT 보안인증 종류 및 보안 요구수준 >

구분	보안 요구수준	평가 항목	실적	예시
라이트 (Lite)	단순 해킹공격에 대응할 수 있는 필수 보안조치 수준 (개인정보 수집·저장·전송 등 취급시 라이트 신청 불가)	10	233	도어락, 센서 등
베이직 (Basic)	중요정보의 불법적인 접근을 차단하고 노출방지에 대응할 수 있는 일반적인 보안조치 수준	29	204	IP카메라, 월패드 등
스탠다드 (Standard)	고도의 해킹공격에 대응할 수 있고 국제적인 요구사항을 포함한 종합적 보안조치 수준	43	4	스마트 가전 등

□ IoT 보안인증 연도별 취득 현황

연도	'18	'19	'20	'21	'22	'23	'24	'25.6	합계
합계	4	24	41	73	83	82	106	28	441