과학기술정보통신부 **보도자료** 대체불가 대한민국

보도 시점 2026. 11. 12.(목) 12:00 (2026. 11. 13.(금) 조간) **배포** 2026.11.11.(수) 14:00

사물인터넷 제품, 제조사의 적극적 보안 강화와 소비자의 보안 수칙 실천이 필요

- 보안점검 결과와 유럽 냉장·냉동설비 제어시스템 해킹 사고를 계기로 사물인터넷 제품 보안관리 중요성 강조 -

- 안전한 비밀번호 설정, 주기적 보안 최신화 등 안전한 디지털 생활을 위한 소비자와 제조사의 관심 또한 필수적 -

과학기술정보통신부(부총리 겸 과학기술정보통신부 장관 배경훈, 이하 '과기정통부')는 한국인터넷진흥원(이하 'KISA')과 한국소비자원(원장 윤수현)의 **보안 실태 점검 결과 발표**와 유럽 냉장·냉동설비 **제어시스템 해킹 사고**를 계기로 **사물인터넷(IoT) 제품 보안 강화 필요성을 강조**하고, **제품 보안성 제고**를 위한 지속적인 노력을 추진하겠다고 밝혔다.

IP카메라를 비롯한 **IoT 제품**은 최근 몇 년간 시장 규모가 급속히 확대되어 상당수 가정에 보급되는 등 **국민 생활에 가장 밀접한 제품**으로 자리 잡았으나, IoT 제품의 보안 취약점과 해킹사례가 빈번히 보도되어, 보안에 대한 소비자의 우려도 커지고 있다.

이에 더하여, 유럽에서는 정보통신망과 연결된 **냉장·냉동설비 제어시스템을 해킹**하고 원격으로 온도를 조절하여 매장 700여곳의 식료품이 대량 폐기된 사건이 발생하였다. 인터넷과 제품·설비 등의 연결이 확대되고 IoT 제품과 산업현장의 제어시스템 등을 노리는 해킹이 증가함에 따라 **해킹이 사이버 공간에서만 머무는 것이 아닌, 국민 생활에도 직접적 영향을 미칠 수 있음**을 시사한다.

한편, 과기정통부는 **소비자에게 정확한 보안정보를 제공**하고 **제품 보안 수준을 제고**하고자 소비자 권익 보호 및 제품 안전성 검사에 전문성을 갖춘 한국소비자원과 협력하여 정보보호 전문기관인 KISA와 함께 작년 로봇청소기에

이어 올해 **IP카메라를 대상**으로 보안 실태점검을 수행하였다.

한국소비자원과 KISA에서 발표한 이번 실태점검 결과에 따르면, KISA는 **일부 제품에서 사생활 침해**로 이어질 수 있는 **주요 취약점을 발견하고, 기업에 통보하여 개선 조치를 요청하였다.** 해당 기업은 주요 취약점에 대해 현재 조치중에 있으며, 그 외 보안 취약점은 **각 제조사가 개선계획을** 한국소비자원에 **제출**하였다.

과기정통부는 이번 IP카메라 보안 실태점검 결과를 바탕으로 **주요 제조사·유통사**와 연내 간담회 개최를 시작으로 **소통을 강화**하여 이번 점검 대상이었던 제품에 대한 **보안성 개선을 요구**할 예정이다.

또한, **소비자** 생활 속에서 실천할 수 있는 **보안 수칙**과 **제조·유통사**가 제품을 안전하게 제조·납품하기 위한 **보안 수칙을 마련**한 후에 이번 보도자료를 계기로 **보안수칙을 주기적으로 개정하고 홍보**할 예정이다. 보안수칙의 **주요 내용**은 다음과 같다.

< IoT 보안수칙 주요 내용 >

◈ **(사용자 보안 수칙)** ①구매 및 설치 시 **기본 비밀번호 변경**, ②사용 과정에서 **최신 보안 업데이트 항시 적용**, ③중고거래 및 폐기 시 **공장 초기화**

◈ **(제조사 보안 수칙)** ①설계 및 개발 단계에서 **불필요한 서비스·기능 비활성화**, ②제품 출시 이후 **지속적 취약점 관리·보안 업데이트 제공**

과기정통부 임정규 정보보호네트워크정책관은 "이번 IP카메라 보안 실태점검이 **제품 보안성 향상과 소비자 인식제고에 중요한 역할**을 할 것으로 기대한다."라며, "제품 **보안성을 지속적으로 제고**하기 위해 **보안 수칙을 주기적으로 환기**하고, **관련 제도 개선**을 추진하기 위한 노력을 지속하겠다."라고 밝혔다.

담당 부서	정보보호네트워크정책실 정보보호산업과	책임자
		담당자

대체불가 대한민국 내실을 만드는 과학기술 내삶을 채우는 디지털·AI 대한민국 정책브리핑

붙임 1 사용자 보안 수칙

안전한 IoT 사용을 위한 사용자 보안 수칙



01 구매 및 설치 시 IoT 기기를 사용하기 전에 꼭 확인하세요.

1 기본 비밀번호 즉시 변경
- 초기 제공 비밀번호를 그대로 사용하지 않기
- 영문 대소문자·숫자·특수문자를 조합해 설정

2 공식 앱만 설치
- 구글 플레이, 앱 스토어 등 공식 배포처 이용
- 출처가 불분명한 앱은 설치하지 않기

3 안전한 공유기에 연결
- WPA3 또는 WPA2 등 안전한 무선 보안 방식 사용
- 공유기 관리자 비밀번호도 함께 변경

4 보안 인증 제품 확인
- KISA IoT 보안인증 등 여부 확인
- 신뢰할 수 있는 제조사의 제품 선택

02 사용 중 평소 사용하면서 습관처럼 점검하세요.

5 최신 보안 업데이트 적용
- IoT 기기, 연동 앱을 최신 버전으로 유지
- 자동 업데이트 기능 켜 두기

6 저장 데이터 안전하게 관리
- 필요 없는 영상과 데이터는 정기적으로 삭제

7 2단계 인증 설정 및 접속 알림 확인
- 의심스러운 접속이 있으면 비밀번호 즉시 변경
- 비밀번호 외에 추가 인증 수단을 함께 사용

8 사용하지 않는 원격 접속 끄기
- 사용하지 않는 원격 접속 기능은 꺼 두기
- 외부 공개 설정은 필요한 범위로 제한

03 중고 거래 및 폐기 시 마지막으로 한번 더 확인하세요.

9 중고 거래 전 공장 초기화
- 계정 연동을 해제하고 저장 영상과 개인 설정 삭제
- 공장 초기화를 확인한 뒤 중고 거래 진행

10 폐기 시
- 기기 내 저장된 영상·개인정보 완전 삭제
- 저장매체가 있으면 초기화 후 폐기

작은 보안 습관이 해킹과 개인정보 유출을 예방합니다.

과학기술정보통신부 Ministry of Science and ICT | 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY | 한국소비자원 Korea Consumer Agency

붙임 2 제조 · 유통사 보안 수칙

안전한 IoT 보급을 위한 제조·유통사 보안 수칙



01 설계 및 개발 처음부터 보안을 적용하여 안전한 IoT 제품을 설계하세요.

1 기본 계정·비밀번호 정책 강화
- 제품마다 서로 다른 초기 비밀번호 적용
- 처음 사용할 때 비밀번호를 반드시 변경하도록 설정

2 전용 앱·펌웨어 위·변조 방지
- 전용 앱의 위·변조 탐지 및 방지 기능 적용
- 펌웨어의 전자서명을 검증하고 불법 시험·변조 여부 확인

3 안전한 통신 및 암호화 방식 적용
- 전송 계층 보안(TLS) 1.2 이상, WPA3 지원
- 취약하거나 지원이 종료된 암호·통신 방식 사용 금지

4 불필요한 서비스·기능 비활성화
- 출하 제품의 개발·점검용 접속 기능 제거 또는 비활성화
- 사용하지 않는 외부 공개 기능·경로 비활성화

02 검증 및 인증 출하 전 보안 검증을 빠짐없이 수행하세요.

5 안전한 업데이트 체계 구축
- 보안 업데이트를 안전하고 신속하게 배포하는 체계 운영
- 전자서명이 확인된 펌웨어만 설치되도록 제한

6 보안 인증 및 표준 준수
- 제품에 해당하는 보안인증을 출하 전에 획득
- 국내외 보안 표준의 요구사항 충족

03 제조자 개발생산(ODM) 제품 유통 시 제품을 유통하거나 변경할 때도 보안을 유지하세요.

7 도입 및 맞춤 변경 시 보안확인
- 도입하는 하드웨어·소프트웨어의 보안취약점 존재 여부 점검
- 보안 패치·업데이트 지원 여부 점검
- 보안설정을 임의로 낮추지 않기
- 자체 변경한 프로그램과 설정에 대해 보안점검 수행

8 외부 서비스 연동 시 보안 검증
- 외부 서비스·클라우드 연동 구간 보안점검
- 연동 구간 인증·권한 관리 검증

04 운영 및 지원 관리 출시 이후에도 책임 있게 관리하세요.

9 지속적인 취약점 관리
- 공개 취약점을 확인한 후 보안업데이트를 신속히 배포
- 제품 지원 기간 및 종료기간 안내
- 취약점 신고 창구 등 대응체계 마련

안전한 제품과 책임 있는 유통이 신뢰받는 IoT 시장을 만듭니다.

과학기술정보통신부 Ministry of Science and ICT | 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY | 한국소비자원 Korea Consumer Agency