

보도시점 2025. 12. 7.(일) 12:00
(2025. 12. 8.(월) 조간) 배포 2025. 12. 7.(일) 09:00

IP카메라 피해 최소화 및 예방을 위해 후속대책 즉시 마련·추진

< 관계부처 합동 IP카메라 보안강화 방안 후속대책 발표 >

- 추가 해킹 피해에 노출된 IP카메라 이용자에 대한 보안조치 이행 권고
- 설치업체 보안조치 요구 및 범정부 합동 사전 점검 등 기존 이용 환경 보완 추진
- 생활밀접시설 IP카메라는 보안인증 제품 사용을 의무화하는 법령 제정 추진

과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈, 이하 ‘과기정통부’), 개인 정보보호위원회(위원장 송경희, 이하 ‘개인정보위’), 방송미디어통신위원회(위원장 직무대행 반상권, 이하 ‘방미통위’), 경찰청(청장 직무대행 유재성)은 지속되는 IP카메라 해킹과 영상 유출로 인한 피해를 최소화하고 국민의 사생활을 안전하게 보호하기 위해 작년 11월에 발표한 「IP카메라 보안강화 방안」의 후속대책을 수립하여 추진한다고 밝혔다.

※ IP카메라 : 유무선 인터넷에 연결되어 다른 기기로 영상 전송이 가능한 카메라로 가정, 사업장, 의료기관, 공공시설 등 안전관리용으로 활용

정부는 작년 11월 관계부처 합동으로 IP카메라 제조/수입 → 유통 → 이용의 단계별 보안 강화를 위한 「IP카메라 보안강화 방안」을 마련하고 정책과제를 추진 중이나, 실제 IP카메라 이용자 등 국민이 체감하는 정책 효과가 신속하게 나타나지 않고 있으며 IP카메라 해킹 및 영상 유출 범죄가 지속 발생하여 많은 국민이 위협에 노출되어 있다고 판단하여 신속하게 후속대책을 마련하였다.

<< 해킹 피해 보안 조치 >>

우선, 해킹에 취약한 IP카메라에 대한 보안조치 이행 안내와 피해자 보호를 추진한다.

최근 경찰청에 의해 검거된 IP카메라 해킹 피의자들이 침입한 12만여 대의 IP카메라가 단순한 형태 또는 공격자들에게 알려진 비밀번호를 사용하고 있어 추가 해킹 피해에 노출되어 있다고 판단됨에 따라 통신사와 협력하여 IP 정보를 바탕으로 신속하게 이용자를 식별하고 ID/PW 변경 등의 보안조치 이행을 권고한다.

IP카메라 해킹으로 인한 피해자를 보호하기 위해 △ 성착취물 영상 삭제·차단 △ 피해자 법률·의료·상담을 지원하고 △ 고위험·대규모 영상유출 사업장에 대한 개인정보보호법 위반 여부 우선 조사를 추진하며 △ IP카메라 해킹 및 영상유출 △ 불법 촬영물 등 성착취물 영상 판매·유통 사이트 운영 △ 해당 영상 구입·소지 등 관련 범죄에 대해 수사를 강화한다.

<< 기존 이용자·제품 대상 보안 대책 >>

다음으로 다양한 이해관계자를 대상으로 한 맞춤형 인식 제고와 기존 이용 환경에 대한 사전 점검을 추진한다.

‘24.11월 「IP카메라 보안강화 방안」의 일환으로 실시한 ‘IP카메라 보안 실태조사’를 통해 IP카메라 설치를 대행하는 업체들이 보안조치 필요성에 대한 인식이 낮다는 것을 파악하였으며, IP카메라 이용자들 또한 IP카메라 보안 조치 이행에 관심이 높지 않음이 확인되었다.

이에, 다중이용시설 등에 IP카메라 설치를 대행하는 업체들이 설치·유지 보수 과정에서 활용할 수 있는 ‘IP카메라 설치·운영 보안 가이드’를 마련·배포하고 오프라인 설명회를 개최하여 업체들의 보안조치 이행력을 확보할 계획이다.

범죄 가능성이 큰 주요 업종을 대상으로 개인정보보호법 상의 ‘안전성 확보 조치 의무’*를 고지하고 IP카메라 보안수칙도 지속 안내한다. 이와 함께 디지털 접근·이용이 어려워 IP카메라 보안수칙 인지가 용이하지 않은 고령자·농어민 등의 디지털 취약계층을 대상으로 찾아가는 교육을 제공하는 디지털배움터를 활용하여 IP카메라 피해 사례와 보안수칙 안내를 추진한다.

* 개인정보보호법 제25조(고정형 영상정보처리기의 설치·운영 제한) 및 제29조(안전 조치의무)에 따라 영상정보처리기기운영자와 개인정보처리자는 안전성 확보에 필요한 조치를 이행하여야 함

또한, 현재의 일회성·사후적 점검으로는 이용자의 경각심 제고와 해킹 사고 사전 예방·개선에 한계가 있다고 판단하여 △ 범정부적 합동 사전 점검과 개선조치 실시 △ 공통 위반사항 및 조치 필요사항의 안내·제도 △ 주요 제품에 대한 보안성 점검 및 결과 공표 등 기존 출시 제품과 이용 환경에 대한 점검도 전면 실시한다.

<< 신규 이용자·제품 대책 신속 추진 >>

아울러, 기존 대책의 효과성 확보를 위해 정책 과제 이행에 박차를 가할 계획이다.

민간부문에서도 생활밀접시설(병원, 수영장, 산후조리원 등 신체적 노출 시설)의 IP카메라는 보안인증을 받은 제품을 사용토록 의무화하는 법률안 제정과 제품 설계 단계에서부터 복잡한 비밀번호 설정 기능 등*을 탑재하는 법령 개정을 신속하게 추진한다. 이와 더불어, 기존에 출시된 제품에 대해서도 복잡한 비밀번호 설정 기능 탑재가 적용될 수 있도록 제조사와 협의해 나갈 계획이다.

- * ① 대문자, 소문자, 숫자, 특수문자 중 3조합 8자리 이상 또는 2조합 10자리 이상
- ② 비밀번호 연속하여 일정 횟수(최대 5회) 잘못 입력 시 일정시간(30초~60분) 접속 차단

다수의 관계부처에서 불법 사이트 차단을 위해 노력하고 있으나 차단 기법을 회피하여 사이트 접속이 가능한 상황을 고려하여 차단 기술 고도화 방안을 강구하고, IP카메라를 구매하는 단계에서부터 보안수칙이 잘 전달될 수 있도록 제조사 및 온라인플랫폼사와의 협의를 지속 추진할 계획이다.

과기정통부 최우혁 네트워크정책실장은 “국내에서 취약한 상태로 운영 중인 IP카메라에 대한 보안 조치가 무엇보다 중요함에 따라 IP카메라를 이용하는 국민들께서는 꼭 ID/PW 변경 등의 보안조치를 이행해주시길 당부한다”라고 언급하며, “관계부처와 협력하여 국민 생활과 직결되는 IP카메라의 안정성 확보를 위해 책임을 다하겠다”라고 강조하였다.

붙임 : IP카메라 보안 관리체계 고도화 방안

담당부서	과학기술정보통신부 사이버침해대응과	책임자	과 장	최광기 (044-202-6460)
		담당자	사무관	안희남 (044-202-6465)
< 공동 >	과학기술정보통신부 정보보호산업과	책임자	과 장	최영선 (044-202-6450)
		담당자	사무관	김소완 (044-202-6451)
< 공동 >	과학기술정보통신부 정보보호기획과	책임자	과 장	김연진 (044-202-6440)
		담당자	사무관	정준환 (044-202-6448)
< 공동 >	개인정보보호위원회 신기술개인정보과	책임자	과 장	고낙준 (02-2100-3061)
		담당자	서기관	정종일 (02-2100-3068)
< 공동 >	방송미디어통신위원회 디지털유해정보대응과	책임자	과 장	김우석 (02-2110-1560)
		담당자	사무관	박상현 (02-2110-1567)
< 공동 >	경찰청 국가수사본부 사이버테러대응과	책임자	과 장	주진화 (02-3150-0053)
		담당자	계 장	이승운 (02-3150-3071)
< 공동 >	국립전파연구원 기술기준과	책임자	과 장	배석희 (061-338-4600)
		담당자	사무관	박문철 (061-338-4610)
< 공동 >	한국인터넷진흥원 위협대응단 탐지대응팀	책임자	단 장	임진수 (02-405-6610)
		담당자	팀 장	조정식 (02-405-5263)

내일을 만드는 과학기술
내일을 채우는 디지털·AI

대한민국
지능정보화



IP카메라 보안 관리체계 고도화 방안

2025. 12월



관계부처 합동

1

추진배경

- 정부는 안전한 IP카메라 이용환경을 조성하기 위해 '24년 11월 'IP카메라 보안 강화 방안*'을 수립하고 정책과제를 이행 중이나,
 - * 비밀번호 설정 강화, 민간 분야 보안인증 제품 사용, 보안수칙 개발안내 영상 차단 및 집중 수사
- 다양한 이해관계 및 정책시차 등으로 가정 및 소상공인 등 실제 이용자들이 체감할 수 있는 정책 효과 미미
- 유출 영상이 게시되는 불법 사이트가 지속 운영되고 있으며 추가 피해 사례*가 다양한 경로로 노출되는 등 국민 불안 가중
 - * IP카메라 해킹에 의한 것으로 추정되는 상업시설에서의 솔자리 영상이 SNS를 통해 확산(25.9월)
- 특히, IP카메라 해킹과 불법촬영물 등 성착취물 유통 피의자 검거·조사 과정에서 국내 다수의 IP카메라가 해킹에 취약*한 것으로 파악
 - * 아이디와 비밀번호가 동일 글자 단순반복, 순차적 숫자나 문자의 조합 등 단순한 형태로 설정

2

현황 및 문제점

- 검거된 피의자에 의해 해킹된 12만대 기기의 이용자 등이 추가 피해에 노출
 - 피해 규모가 12만대로 크고 피해자를 특정할 수 있는 정보가 한정



민관 협업으로 피해사실 통지 및 조치방안 안내 등 피해자 보호 추진 필요

- 제품 자체의 보안성 강화, 이용자의 보안조치 이행 유도, 신규 제품 출시 및 설치하는 경우를 중심으로 기존 대책 설계

- ① (기존대책) IP카메라 제품 제조·수입 → 유통 → 이용의 단계별 보안 강화
방안에 집중, (한계) 해킹 사고는 제품 외적 요인에 의해서도 발생

※ 보안조치를 필수적으로 수행하는 설치업체는 59.0%, 복수고객을 대상으로 동일유사한 비밀번호를
설정한 경험이 있는 설치업체는 23.4%으로 설치업체의 보안조치 미흡(실태조사, '25.10월)

※ IP카메라 관련 네트워크 보안의 주체가 명확하지 않고 보안 기능도 제품 자체 적용을 규율하고
있는 등 이용자 및 제조사 중심의 보안 책임 구조로 중요 이해관계자인 설치업체통신사 제외

설치·운영 단계에서의 보안성 강화와 위험요인 통제 방안 필요

- ② (기존대책) 이용자의 보안조치 이행 유도를 위해 보안수칙을 마련·안내,
(한계) 비용 발생에 따른 제조사의 비협조*로 이용자에게 전달 미흡

* 8개 제조사 중 설명서 내 보안수칙 QR코드 삽입은 2개社, 앱 내 팝업 보안수칙 안내는 1개社

※ 비밀번호를 직접 설정하는 이용자는 81.0%, 최근 6개월 이내 비밀번호를 변경한 경우는
30.8%로 사업장 및 개인은 안전성 확보 조치 이행에 관심 저조(실태조사, '25.10월)

다양한 이용자 대상으로 보안수칙의 맞춤형 안내 방안 필요

- ③ (기존대책) 영상 유출 시 안정성 확보 조치 조사 추진, (한계) 일회성·
사후적 점검으로 이용자 경각심 제고 및 사전 예방·개선에 효과 부족

※ 경찰청에서 검거한 피의자 2명에 의해 해킹된 IP카메라가 각각 약 6만 3천대, 7만대대로
영상 유출 규모(불법사이트에 판매된 영상 1,193개)보다 더 많음

다중 이용 환경 등에 대한 사전적인 현장 계도·점검·단속 필요

- 불법사이트 운영 수법의 고도화, 다양한 이해관계 발생 등으로 일부
기존 대책의 정책 효과 기대 곤란

※ 법령 개정은 국회 및 관계부처 사정으로 개정 지연 가능성 존재, 불법사이트 차단
회피 사례 등장, 제조사 및 온라인쇼핑몰의 공감대 부족

기존 대책의 효과성 확보를 위해 보완 방안 필요

- (취약한 기기 조치) 피해기기 IP를 통신사에 공유, 통신사를 통해 이용자에게 ID/PW 변경 등 보안조치 이행을 권고하고 이행사항 점검(11월~)
 - 통신사 고객 대응팀 구성·운영*을 통해 피해기기 이용자 및 일반 국민 대상 응대 등 혼란 최소화(11월~)
 - * 피해기기 IP 정보를 바탕으로 피해가 확인된 이용자 이외의 경우로, IP카메라 이용자가 직접 통신사에 문의할 때 ID/PW 변경 등 보안조치 사항을 안내
 - 통신사와 함께 IP 이용자 정보를 분석하여 피해가 집중된 주요 업종 확인(11월~)
- (영상물 피해자 보호) IP카메라 해킹으로 유출된 불법 촬영물 등 성착취물 영상 삭제·차단 지원 등 피해자 보호 추진
 - 고위험·대규모 영상유출 처리자(사업자 등)에 대한 개인정보보호법 위반 여부 우선 조사 추진(12월~)
 - ※ 경찰청 협조를 통해 다중이용시설(상가, 숙박 등) 등 당해 개인정보처리자 특정, 위반사실 확인, 증거확보 등 추진
 - 불법 촬영물 등 성착취물 영상 삭제·차단 요청 및 해당 피해자 대상 법률·의료·상담 지원* 등 피해자 보호 추진(연중)
 - * '디지털성범죄 피해자 지원센터'(d4u.stop.or.kr)와 연계
- (해킹·사이트 수사 강화) 해외 기관과의 공조 수사를 통해 불법 사이트 운영자 수사 및 사이트 폐쇄 추진(계속)
 - △ IP카메라 해킹 및 영상유출 △ 불법 촬영물 등 성착취물 영상 판매·유통 사이트 운영 △ 영상 구입·소지 등 관련 범죄에 대해 집중수사 지속('25.11월~)

4

기존 이용자·제품 대상 보완 대책

< 국내 IP카메라 현황('24년 기준) >

○ 전국 약 2,037만대 이상*, 공공기관 약 195만대 CCTV 설치·운영 중('25.7월, 개보위)

* '24년 '개인정보보호 및 활용조사'를 바탕으로 추정

□ (설치·운영 보안조치) 설치업체를 대상으로 보안 조치 가이드라인을 마련·배포하고 기존 설치 공사에 대한 보안 조치를 요청(11월)

○ 설치업체, 제조사 대상으로 오프라인 설명회 추진(12월~)

○ 통신사를 통해 기업용 상품 가입자, 다중이용시설 사업장 등을 대상으로 IP카메라 보안수칙 안내 추진(12월~)

□ (이용자 인식 제고) 범죄 가능성이 큰 주요 업종을 도출하여 업종별 소관 부처를 통한 사업장의 안정성 확보 조치 의무* 안내(12월~)

* 개인정보보호법 제25조(고정형 영상정보처리기의 설치·운영 제한) 및 제29조(안전조치의무)에 따라 영상정보처리기기운영자와 개인정보처리자는 안전성 확보에 필요한 조치를 이행하여야 함

○ 중앙행정기관을 통해 국민 일상생활과 밀접한 분야를 대상으로 IP카메라 정보보호 조치의 중요성 및 보안 수칙* 안내 확대(상시)

* 보인인증 제품 사용, 초기 계정 및 비밀번호 변경, 펌웨어 최신 상태 유지, 사용 후 전원 차단 등

○ 디지털 취약계층을 대상으로 디지털 배움터*를 활용하여 IP카메라 피해사례 전파 및 보안수칙 안내(12월~)

* 디지털 활용에 어려움을 느끼는 국민 누구나를 대상으로 쉽고 편리하게 배울 수 있는 디지털 실생활 역량 교육을 제공하는 사업으로 전국 3,000개소 운영 중

□ (레거시 환경 점검) 각 부처별로 취약분야(병·의원, 마사지샵 등)를 선정하여 범부처(지방정부 포함) 합동 사전 점검 및 개선조치 실시(12월~)

※ 관련 협·단체(정보통신공사업협회 등) 공동 추진, 개인정보위는 전문인력 지원

○ 공통 위반사항 또는 즉시 조치 필요사항에 대한 안내·계도(12월~)

○ 소비자원 협력을 통한 주요 제품에 대한 보안점검·공표·개선권고 등을 추진, 과기정통부 자체 점검 및 개선권고를 위한 법적 근거 마련 추진(10월~)

5

신규 이용자 · 제품 대책 신속 추진

- (법령 개정 조속 추진) 생활밀접 시설 영상유출 예방을 위한 IP카메라 보안인증 제품 사용을 의무화하는 법안* 제정 적극 추진(~'26)

* (주요 내용) 요가, 필라테스, 병원, 헬스클럽, 수영장, 산후조리원 등 신체적 노출 시설 등 주요 민간시설에 IP카메라를 설치·운영하는 경우 보안인증을 받은 제품 사용

- 무차별 대입(Brute Force) 공격에 대응 가능한 복잡한 비밀번호 설정 원칙*이 제품 설계 단계에서 적용되도록 법령 개정** 신속 추진(~12월)

* ① 대문자, 소문자, 숫자, 특수문자 중 3조합 8자리 이상 또는 2조합 10자리 이상
② 비밀번호 연속하여 일정 횟수(최대 5회) 잘못 입력 시 일정시간(30초~60분) 접속 차단

** 방송통신기자재등의 적합성평가(전파법 제58조의2) 관련 단말장치 기술기준(고시)

- 既 출시 제품에 대해서도 복잡한 비밀번호 설정 원칙 및 강화된 보안 기능* 탑재를 제조사에 협조 요청(10월~)

* 메일 등 이중 인증 설정, 펌웨어 업데이트 알림 등

- (불법 사이트 차단) 영상 노출 사이트 모니터링 및 차단 신속 수행(연중)

- 차단 기법을 회피하는 사례*에 대응하여 비복호화 기반 트래픽 분석 등 차단 기술 고도화 방안 검토('26~)

* 현재는 통신 연결에 필요한 암호화되지 않은 서버 이름을 식별하고 불법 사이트 목록과 비교하여 차단 중이나, 서버 이름까지 암호화하는 보안 프로토콜을 사용하는 불법 사이트 등장

- 오픈된 IP 정보를 제공하는 해외사이트에 대한 모니터링 및 기술적 대응 방안 마련('~26)

※ 해커들이 취약한 IP카메라를 식별하는 수단으로 악용되는 해외사이트에서 국내 IP 카메라의 정보가 제공되는 것을 차단

- (이용자 실천 제고) 제품 설명서에 보안수칙 QR코드 삽입, 앱 내 보안수칙 팝업 안내 등을 제조사에 지속 요청(연중)

- 온라인쇼핑 플랫폼의 제품 검색 단계에서 보안수칙이 안내될 수 있는 방안에 대해 온라인플랫폼사와 지속 협의(연중)

주요 과제

일정

소관

□ 해킹 피해 보안 조치

■ 이용자 보안 조치 이행 권고	‘25.11월~	과기정통부
■ 고위험·대규모 영상유출 처리자 우선 조사	‘25.12월~	개보위
■ 성착취물 영상 피해자 보호	연중	경찰청
■ 불법 사이트 운영자 수사 및 사이트 폐쇄	계속	경찰청
■ IP카메라 해킹 및 영상유출 등 집중수사	‘25.11월~	경찰청

□ 기존 제품·이용자 대상 보완 대책

■ 설치업체 대상 보안 조치 가이드 마련·배포	‘25.11월	과기정통부
■ 업종별 사업장 안전성 확보 조치 의무 안내	‘25.12월~	과기정통부·관계부처
■ 국민 일상생활 밀접 분야 보안 수칙 안내	연중	과기정통부·관계부처
■ 디지털 취약계층 대상 피해사례 전파 및 보안수칙 안내	‘25.12월~	과기정통부
■ 취약분야 합동 사전 점검, 위반사항 안내·계도	‘25.12월~	개보위·관계부처
■ 주요 제품 보안점검·개선 권고 법적 근거 마련	‘25.10월~	과기정통부

□ 신규 제품·이용자 대책 신속 추진

■ 생활밀접분야 보안인증 제품 사용 의무화	~‘26	개보위
■ 제품에 복잡한 비밀번호 설정 적용	~‘25.12월	과기정통부
■ 불법 사이트 차단 기술 고도화 방안 검토	‘26~	과기정통부
■ 취약한 IP 스캔 해외사이트 모니터링 및 대응 방안 마련	~‘26	과기정통부
■ 제조사 및 온라인플랫폼을 통한 보안수칙 안내	연중	과기정통부