

내 일상이 실시간으로 중계된다고? IP카메라 비밀번호 당장 바꾸세요

- 개인정보보호위원회, IP카메라 보안 강화를 위한 민관협력 캠페인 전개
- 비밀번호는 문자, 특수문자, 숫자 등을 혼합하여 최소 8자리 이상으로 변경 안내

개인정보보호위원회(위원장 송경희, 이하 ‘개인정보위’)는 지난해 12월 관계부처 합동으로 발표한 「IP카메라* 보안 관리체계 고도화 방안」의 후속 조치로 관계부처, 지자체, 주요 직능단체 등과 함께 ‘IP카메라 보안 강화를 위한 민관협력 캠페인’을 추진한다.

* IP카메라(Internet Protocol Camera) : 유무선 인터넷에 연결되어 영상 전송 및 확인이 가능한 카메라로 가정집이나 사업장, 의료기관, 공공시설 등에서 활용

아이피(IP)카메라는 스마트폰 등을 통해 언제 어디서나 영상을 확인할 수 있고, 저렴한 비용으로 쉽게 설치 가능해 가정집이나 소규모 사업장 등에서 널리 사용되고 있다. 다만 최근 IP카메라의 보안 취약점을 노린 해킹 사고가 지속적으로 발생*하고 있어 이용자들의 각별한 주의 또한 요구되고 있는 상황이다.

* '25. 12. 1., 경찰청은 국내 IP카메라 12만 대를 해킹하여 영상을 탈취한 피의자 4명을 검거하였다고 발표(일부 영상물은 해외 불법사이트에 판매하여 가상자산 취득).
해킹된 IP카메라는 아이디와 비밀번호가 단순한 형태로 설정되어 있었음

특히, IP카메라 구입 시 기본으로 설정되어 있는 사용자 계정(ID)이나 초기 비밀번호를 변경하지 않고 계속 사용하는 경우*에는 해커들이 인터넷을 통해 쉽게 침입할 수 있으며, 이로 인해 가정집 내부나 사업장 이용객들의 일상이 실시간으로 외부에 중계되는 등 심각한 사생활 침해가 발생할 수 있다.

* (예시) admin, root, user1, user2, user3 등은 실제 해킹 사례가 있는 사용자 계정.
0000, 123456, abcd 등 연속된 문자, 숫자는 손쉽게 유추 가능한 비밀번호

이에 개인정보위는 소규모 사업장 등에서 이행할 수 있는 ‘IP카메라 점검 체크리스트’를 마련한다. 또한, 관계부처(문화체육관광부, 보건복지부 등), 지방자치단체, 주요 직능단체 등과 협력하여 공공시설물, 의료기관, 소규모 사업장(헬스장, 노래방 등) 등에 대한 IP카메라 자율점검 및 보안조치 이행을 적극 추진한다.

개인정보위에서 IP카메라 해킹 예방과 보안강화를 위해 이행 권고하는 사항은 다음과 같다.

첫째, IP카메라 사용 시에는 초기 사용자 계정(ID)과 비밀번호를 반드시 변경하고 사용해야 하며 이후에도 주기적인 변경을 통해 안전성을 확보하여야 한다. 특히 비밀번호는 다른 사람이 쉽게 유추할 수 없도록 문자, 특수문자, 숫자 등 3가지 유형을 혼합한 8자리 이상으로 변경해야 한다.

※ 사용자 계정(ID) 변경이 불가능한 IP카메라의 경우에는 우선 보다 복잡한 비밀번호를 사용하고, 이후 사용자 계정(ID) 변경이 가능한 제품으로 교체 권고

둘째, 사업장(병·의원, 필라테스학원, 요가학원, 악성샵, 피부관리실, 마사지샵 등) 내 신체 노출이 현저히 예상되는 장소에서는 IP카메라의 인터넷 접근을 제한(인터넷 선 분리 또는 가상사설망 구축 등)하여, 외부에서 해당 장소를 이용하는 사람의 영상에 접근할 수 없도록 조치하여야 한다.

※ 목욕실이나 화장실, 탈의실, 발한실 등의 경우에는 「개인정보 보호법」상 고정형 영상정보처리기기 설치·운영이 금지되는 장소이므로 IP카메라 또한 설치 금지

셋째, IP카메라 구입 시에는 국내 전문기관의 정보보호 관련 인증*을 받은 제품인지를 확인하고 보다 안전한 제품을 선택할 필요가 있다. 특히 해외 직구 등을 통해 별도의 검증절차 없이 구입한 제품은 향후 보안 업데이트 또는 A/S 지원이 어려울 수 있어 신중히 사용하여야 한다.

* 과기부 정보통신망연결기기등 정보보호 인증(CIC), 한국정보통신기술협회 IP카메라 보안성능 인증(TTA Verified), 개인정보위 개인정보보호중심설계 시범인증(PbD) 등

앞으로도 개인정보위는 관계부처, 지자체 등과 협력하여 모든 공공시설물과 사업장, 가정 등에 IP카메라 위험성을 널리 알리고 비밀번호 변경 등의 보안 조치 이행이 정착될 수 있도록 지속적인 홍보와 안내 등을 추진할 계획이다.

양청삼 개인정보위 사무처장은 “IP카메라가 국민 일상에 편리하게 사용되고 있지만, 영상 유출시 사생활을 심각하게 침해하는 결과를 초래할 수 있다.”라며, “사용자 계정(ID)와 비밀번호를 주기적으로 변경하는 것 만으로도 대부분의 피해를 예방할 수 있으므로 꼭 보안조치를 이행해 주시기를 당부한다”고 강조했다.

담당 부서 <총괄>	개인정보정책국 신기술개인정보과	책임자	과장(직무대리)	원세연 (02-2100-3071)
		담당자	서기관	정종일 (02-2100-3066)
			주무관	이선아 (02-2100-3064)
<공동>	한국인터넷진흥원 AI데이터정책팀(TF)	책임자	팀 장	박상준 (061-820-2990)
		담당자	책임연구원	고재우 (061-820-2992)



IP카메라 보안강화 체크리스트



사업장명	소재지	점검일시/점검자
점검유형	☐ 전문업체 점검 (설치업체, 유지보수업체 등) ☐ 자체점검 (전담부서, 담당자 점검 등) ☐ 외부기관 현장점검 (지자체, 복지부 등)	
종합의견	※ 신체적 노출이 예상되는 민감한 장소에 IP카메라가 설치되어 있는지 여부와 네트워크 차단 또는 비밀번호 변경 등 점검에 따른 조치사항을 포함하여 종합의견 작성	

1단계 IP카메라 점검을 위한 사전 정보 확인

점검사항	점검결과		
	예	아니오	비고
1-1. 사업장 내에 CCTV를 설치한 업체 또는 CCTV에 대한 유지보수를 담당하는 업체를 알고 있는가?	☐	☐	
1-2. 사업장 내에 CCTV 설치-운동을 담당하는 전담부서가 있는가?	☐	☐	

조치사항

- IP카메라 점검 가능한 전문업체(설치업체, 유지보수업체) 또는 전담부서가 있는 경우 과기정통부가 IP카메라 설치업체 대상으로 발간한 "2025년 IP카메라 설치-운영 보안가이드(2025.11.)"에 따른 정밀점검 실시
- 사업장내 네트워크 구성 방법 및 네트워크 카메라 기종에 따라 다양한 취약점이 존재할 수 있으므로 가능한 과기정통부 가이드 라인에 따른 정밀점검 권장
- IP카메라 정밀점검이 가능한 전문가(설치업체, 유지보수업체, 전담부서 등)가 없거나 정밀점검이 어려운 소규모 사업장은 다음 단계에 따른 점검을 실시하고 조치

2단계 IP카메라 운영 현황 및 필요성 점검

점검사항	점검결과		
	예	아니오	비고
2-1. 사업장 내 설치된 CCTV 중에서 외부 인터넷을 통해 접근 가능한 IP카메라가 있는가? ※ CCTV와 IP카메라는 회선 구성 방식에 차이가 있을 뿐 외관은 실질적으로 동일함 ※ 이에 본 체크리스트에서는 스마트폰 앱 또는 웹브라우저를 통해 실시간 또는 저장된 영상을 확인할 수 있는 IP카메라를 대상으로 함(이하 같음)	☐	☐	CCTV 00대 중 IP카메라 00대
2-2. 은밀한 신체적 노출이 예상되는 장소에 설치된 CCTV 중 IP카메라가 있는가? ※ 외부 인터넷 접근이 불가능하도록 VPN 접속 등을 통해 폐쇄회로 텔레비전으로 설치한 경우 제외	☐	☐	인터넷 접근 차단 IP카메라 00대

조치사항

- 외부 인터넷을 통해 접근 가능한 IP카메라가 있을 경우 이를 계속 운영해야 할 필요가 있는지 확인하고, 불필요한 경우 인터넷 접속 가능 차단
- 특히, 은밀한 신체적 노출이 예상되는 민감한 장소에는 반드시 외부 인터넷에서 접근 불가능하도록 조치(네트워크 회선/카드 분리, 저장장치 WAN 분리 등)
※ 가상사설망(VPN) 등을 통해 외부 인터넷에서 접근할 수 없도록 폐쇄회로 구성 가능

IP카메라 보안강화 체크리스트



3단계 사용자 계정(ID) 및 비밀번호 변경

점검사항	점검결과		
	예	아니오	비고
3-1. 모든 IP카메라와 영상저장장치의 사용자 계정(ID) 및 비밀번호를 누구나 쉽게 유추할 수 없는 문자열로 변경하였는가? ※ IP카메라와 저장장치별로 ID/비밀번호가 각각 존재할 수 있으므로 확인 후 모두 변경	☐	☐	비밀번호 변경 IP카메라 00대, 저장장치 00대

조치사항

- 사용자 계정(ID)과 비밀번호는 제조업체에서 제공한 전용 앱(App)이나 전용 S/W 또는 웹 브라우저를 통해 변경 가능. 다만, 기기별로 다른 경우가 있으므로 필요시 제조업체 문의 필요
- admin, root, user1, user2, user3과 같이 실제 해킹 사례가 있는 사용자 계정(ID)은 반드시 다른 이름으로 변경해야 함. 다만, ID 변경이 불가능한 제품의 경우에는 우선 보다 복잡한 비밀번호를 사용하여 안전성을 강화하고, 향후 ID 변경이 가능한 다른 제품으로 교체 권고
 ※ IP카메라를 교체하려는 경우에는 비밀번호를 연속으로 틀릴 경우 일정시간 접속을 차단하는 기능이 포함된 제품으로 교체 권고(비밀번호 자동 대입 공격을 원천적으로 차단)
- 비밀번호는 문자, 특수문자, 숫자 등 3가지 유형을 혼합하여 8자리 이상의 문자열로 변경
- 기존에 설정되어 있는 비밀번호를 알 수 없어 초기화하는 경우에는 현재 설정값이나 영상이 모두 삭제될 수 있으므로 반드시 제조업체 또는 설치업체에 확인 필요

4단계 기타 보안조치

점검사항	점검결과		
	예	아니오	비고
4-1. IP카메라 또는 영상저장장치에는 등록된 사용자 외 임의로 접근할 수 없도록 조치하였는가? ※ 게스트 모드 차단, 펌웨어 업데이트 등(필요시 제조사 협조)	☐	☐	
4-2. IP카메라 접근 가능한 단말기(스마트폰, 노트북, PC 등)에 대한 보안조치를 하였는가? ※ 자동 로그인 비활성화, 백신 설치 및 업데이트 등	☐	☐	

조치사항

- 게스트 모드 활성화시 비인가자가 무단으로 영상에 접근할 수 있어 반드시 차단 필요
- 단말기가 악성코드에 감염될 경우 IP카메라에 대한 통제 권한이 함께 탈취될 수 있음

