

IP카메라 보안강화 체크리스트



사업장명	소재지	점검일시/점검자
점검유형	<input type="checkbox"/> 전문업체 점검 (설치업체, 유지보수업체 등) <input type="checkbox"/> 자체점검 (전담부서, 담당자 점검 등) <input type="checkbox"/> 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	아니요	비고
1-1. 사업장 내에 CCTV를 설치한 업체 또는 CCTV에 대한 유지보수를 담당하는 업체를 알고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>	
1-2. 사업장 내에 CCTV 설치·운영을 담당하는 전담부서가 있는가?	<input type="checkbox"/>	<input type="checkbox"/>	

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	아니요	비고
2-1. 사업장 내 설치된 CCTV 중에서 외부 인터넷을 통해 접근 가능한 IP카메라가 있는가? ※ CCTV와 IP카메라는 화선 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)	<input type="checkbox"/>	<input type="checkbox"/>	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	<input type="checkbox"/>	<input type="checkbox"/>	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 기능 차단
- ▶ 특히, 은밀한 신체적 노출이 예상되는 민감한 장소에는 반드시 외부 인터넷에서 접근 불가능하도록 조치(네트워크 화선/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	아니요	비고
3-1. 모든 IP카메라와 영상저장장치의 사용자 계정(ID) 및 비밀번호를 누구나 쉽게 유추할 수 없는 문자열로 변경하였는가? <small>※ IP카메라와 저장장치별로 ID/비밀번호가 각각 존재할 수 있으므로 확인 후 모두 변경</small>	<input type="checkbox"/>	<input type="checkbox"/>	비밀번호 변경 IP카메라 00대, 저장장치 00대

조치사항

- ▶ 사용자 계정(ID)과 비밀번호는 제조업체에서 제공한 **전용 앱(App)**이나 **전용 S/W** 또는 **웹브라우저**를 통해 변경 가능. 다만, 기기별로 다른 경우가 있으므로 필요시 제조업체 문의 필요
- ▶ admin, root, user1, user2, user3과 같이 실제 **해킹 사례**가 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 이상**의 문자열로 변경
- ▶ 기존에 설정되어 있는 비밀번호를 알 수 없어 **초기화**하는 경우에는 현재 설정값이나 영상이 모두 삭제될 수 있으므로 반드시 제조업체 또는 설치업체에 확인 필요

4단계 기타 보안조치

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

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

