사물인터넷 소형 스마트 홈·가전 보안 가이드 [이용자용]

2016. 12.

미래창조과학부
Ministry of Science, ICT and Future Planning

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

제1장
개요

제1장 개요

1. 필요성 및 목적

스마트 홈은 가정 내 스마트 디바이스들을 유·무선 네트워크로 연동하여 자동화, 원격 제어, 에너지 관리 등을 통해 이용자의 편의성을 제공하며 삶의 질 향상과 비용 절약 측면에서 새로운 가치를 제공하고 있다.

또한 스마트 디바이스 보급률의 증가와 무선 통신 기술, 센서 기술 등의 발전으로 인해 스마트 홈 구축비용이 감소하고, 가정 내의 에너지 관리에 대한 관심이 높아짐에 따라, 미래창조과학부, ETRI, 한국스마트홈산업협회 중심으로 하는 사물인터넷 기반의 스마트 홈 관련 사업 등이 활발하게 진행되고 있다.

하지만 이러한 발전의 이면에는 “2016년 초, 전세계 7만 3천여 대의 IP 카메라 해킹”, “2015년 12월 아파트 도어락 해킹하여 출입문 개방”, “2016년 2월 네트워크 카메라 영상 불특정 다수에게 유포”, “2016년 10월 26일 발생된 미국의 대규모 DDoS 공격” 등 스마트 디바이스를 대상으로 하는 침해사고가 지속적으로 발생되고 있다.

특히 스마트 홈에서 수집되는 데이터는 사람과 사물간의 데이터 교환을 기반으로 개인정보(이름, 생년월일, 전화번호, 주소 등), 개인 영상 정보 등 사생활에 대한 정보가 포함하고 있어 유출시 프라이버시 침해 위험성이 높다.

만약 스마트 도어락이 해킹된다면 무단침입이 가능하고, 스마트 디바이스들 역시 해킹되어 개인정보가 유출된다면 2차, 3차 피해가 발생할 수 있다. 이처럼 스마트 홈 침해 사고는 금전적, 물리적, 정신적인 피해가 발생될 수 있어 파급력이 매우 크다.

이에 제조사, 서비스 제공자 등을 중심으로 정보 보호를 위한 데이터 신뢰성, 무결성, 가용성 강화를 위해 노력하고 있지만, 무엇보다 스마트 홈 환경에서 가장 효율적인 정보 보안 방법은 스마트 홈을 활용하고 있는 이용자들에 대한 보안 인식 제고이며, 이를 통해 침해 사고를 사전 예방할 수 있도록 해야 한다.

본 가이드에서는 스마트 홈가전에서 발생 가능한 보안 위협에 대해 침해 사고를 사전에 예방할 수 있도록 이용자 입장에서 보안위협과 대응방안을 제시하며, 최근 침해사고가 자주 발생하고 있는 IP 카메라의 실제 보안 설정화면을 통해 이용자의 이해를 돕는다.

2. 가이드 목적 및 구성

목적	- 스마트 홈·가전에 대한 보안 위협의 심각성을 인지하여 보안 인식 제고 - 안전한 스마트 디바이스 이용으로 침해 사고 예방
대상	- 사물인터넷 기반 스마트 홈·가전 이용자
범위	- 스마트 홈·가전 디바이스 이용 시 지켜야 할 사항
구성	- [1장] 개요 1.1 필요성 및 목적 1.2 가이드 목적 및 구성 - [2장] 스마트 홈·가전 보안 위협 및 대응방안 2.1 정보유출 2.2 비 인가자 접속 가능 2.3 DDoS 공격 악용 - [3장] 스마트 홈·가전 보안 가이드 3.1 패스워드 설정 3.2 암호화 설정 3.3 접근제어 설정 – IP/MAC 주소 인증 3.4 펌웨어 업데이트

제2장

스마트 홈·가전 보안 위협 및 대응방안

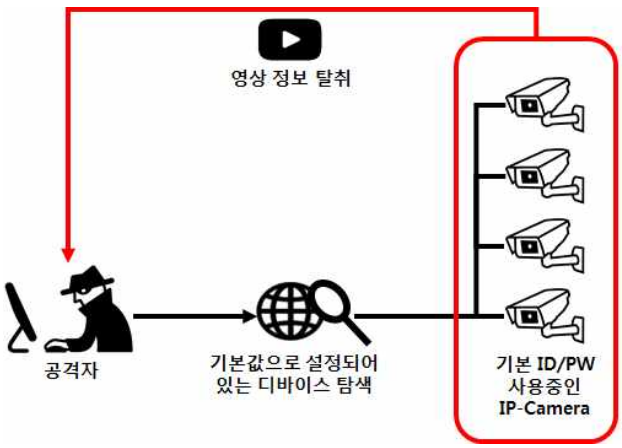
제2장 스마트 홈 · 가전 보안 위협 및 대응방안

2.1 정보 유출

대부분의 사물인터넷 디바이스 이용자의 경우 관리자 혹은 접속 가능한 계정의 패스워드를 디바이스 출고 당시 기본 패스워드 그대로 사용하거나, 안전하지 않는 패스워드를 사용하고 있다. 공격자는 자동화된 공격 툴을 통해 패스워드가 기본적으로 설정되어 있는 취약한 디바이스에 접속하여 전력 사용량, 영상정보 등을 탈취할 수 있다. 전력 사용량은 시간대별 이용자의 생활 형태를 파악하는 데이터로, 영상정보는 이용자의 일거수일투족이 외부에 노출될 수가 있어 심각한 사생활 침해를 유발할 수 있다.

위 보안위협에 대한 실제 사례로, 얼마전 전 세계 약 7만 3천여 대의 IP 카메라가 해킹되어 '인세캠' 이라는 사이트를 통해 생중계 되었다. 한국에서는 약 6000여개의 IP 카메라가 해킹되었으며 '인세캠' 이라는 사이트 운영자가 '보안 설정의 중요성' 을 알리기 위해 해킹한 것으로 밝혀졌다. 공격자는 공장 출고 당시 설정된 아이디와 비밀번호를 바꾸지 않은 IP 카메라를 해킹 대상으로 하였다. 이를 통해 공개된 장소는 가정집과 공연장, 사무실, 공장, 슈퍼마켓, 미용실, 헬스클럽, 수영장, 카페, 피부 관리실 등 다양하며 사이트에는 IP 카메라가 설치된 위도와 경도가 나와 있고 구글 지도를 이용해 해당 위치를 추적할 수 있어, 이를 악용할 경우 개인프라이버시가 침해되고 더 나아가 금전적, 물리적 피해까지 발생할 수 있다.

이와 같은 점을 이용한 공격 시나리오는 <그림 2-1>과 같다.



<그림 2-1> 취약한 패스워드를 사용할 경우의 보안 위협

이와 같은 보안 위협을 방지하기 위하여 최초 패스워드는 충분한 보안성을 지닌 패스워드로 변경하여 사용하여야 한다. 또한 같은 패스워드를 장기간 사용할 경우 보안이 취약해질 수 있으므로 주기적으로 변경하여야 한다. <표 2-1>은 안전한 패스워드를 설정할 수 있는 방법의 예시이다.

<표 2-1> 안전한 패스워드를 설정할 수 있는 방법

예측이 어려운 비밀번호	
1.	영문자(대·소문자), 숫자, 특수 문자들을 혼합한 구성 예시) '10H+ 20Min', 'I!Can&9it' 등과 같은 구성
2.	특수 문자 활용 시, 비밀번호 시작 혹은 끝 부분이 아닌 위치에 삽입하여 설정 예시) 'Security1!' 이 아니라 'Securi2t&&y' 와 같은 형태로 설정
3.	영문자(대·소문자)를 구분할 수 있을 경우, 대·소문자를 혼합하여 설정 예시) 'gksrnrdlsxjsptwjdqh' -> 'gkSrnSdlSxJspTwjDqH' 등

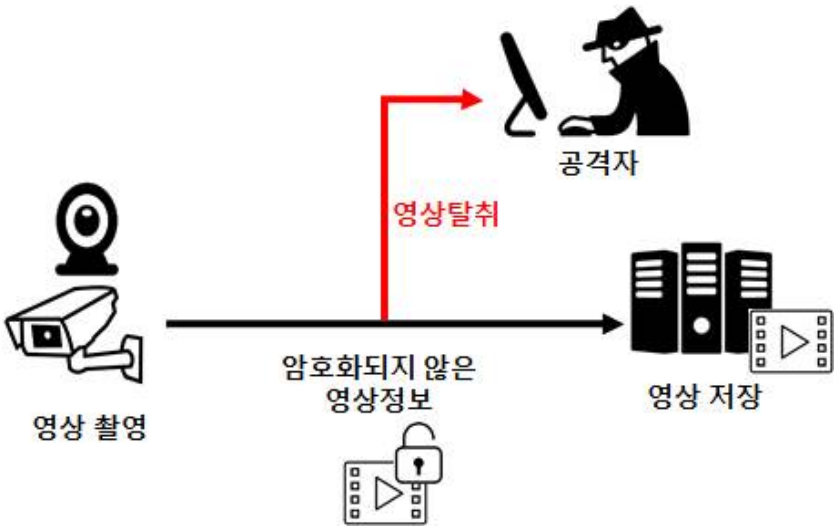
※ 안전한 패스워드 생성 및 관리에 대한 세부적인 사항은 한국인터넷진흥원의 패스워드 선택 및 이용 가이드를 참고
https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=6&mode=view&p_No=259&b_No=259&d_No=32&ST=T&SV=

또한 사물인터넷 디바이스 통신에 암호화를 이용하지 않거나, 취약한 암호방식을 사용할 경우, 공격자는 암호 알고리즘의 취약점을 이용하여 디바이스에 접근하여 사용자의 특정 정보를 탈취할 수 있다.

위 보안 위협에 대한 실제 사례로, 트렌드넷의 웹 기반 모니터링 카메라 단말기인 시큐어뷰어가 촬영한 동영상이 온라인상에 노출되는 사건이 발생하였다. 이는 트렌드넷이 2010년 4월 펌웨어 업데이트 버전을 상용화할 때 고객의 로그인 계정 정보를 암호화하지 않고 인터넷상에서 동영상을 전송 및 저장하여 발생한 문제로 파악되었다. 또한 트렌드넷 전용 모바일 앱에서도 고객이 로그인 시 계정 정보가 지속적으로 단말기에 저장되어 보안에 취약한 구조인 것으로 확인되었다.

이처럼 공격자는 보안 취약점을 통해 IP주소로 접속하여 별도의 인증 절차 없이 영상을 다운로드 받는 등 침해 사고를 발생시킬 수 있다.

이와 같은 점을 이용한 공격 시나리오는 <그림 2-2>와 같다.



<그림 2-2> 암호화 절차가 없는 경우의 보안 위협

이와 같은 보안 위협을 방지하기 위하여 사물인터넷 디바이스간 송/수신하는 데이터의 암호화가 필요하며, 사물인터넷 디바이스에서는 HTTPS(SSL/TLS)기반 보안 설정이 가능한 제품 이용을 권고한다. 만약 공유기를 이용할 경우 무선 암호화는 보안 강도에 따라 WEP, WPA, WPA2 등으로 분류되는데, 보안강도가 낮을수록 보안상 문제가 발생할 소지가 높기 때문에, 데이터 암호화 WPA2로 변경하여 보안을 강화하도록 한다.

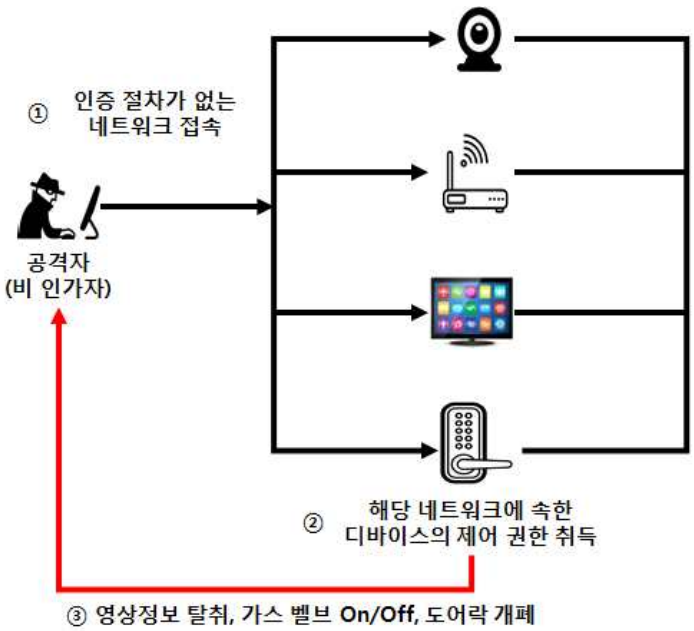
<표 2-2> (공유기)무선 인증/암호화 기술별 특징

구분	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access2)
인증	• 사전 공유된 비밀키 사용 (64비트, 128비트)	• 사전에 공유된 비밀키를 사용하거나 별도의 인증서버를 이용	• 사전에 공유된 비밀키를 사용하거나 별도의 인증서버를 이용
암호화	• 고정 암호키 사용 (인증키와 동일) • RC4 알고리즘 사용	• 암호키 동적 변경(TKIP) • RC4 알고리즘 사용	• 암호키 동적 변경 • AES 등 강력한 블록 암호 알고리즘 사용
보안성	• 64비트 WEP 키는 수분내 노출 • 취약하여 널리 쓰이지 않음	• WEP 방식보다 안전하나 불완전한 RC4 알고리즘 사용	• 가장 강력한 보안기능 제공

2.2 비 인가자 접속 가능

사물인터넷 디바이스는 실생활과 밀접한 관련을 가진다. 베이비 모니터, 도어락 등 비 인가자가 제어 권한을 탈취하게 될 경우, 홈 컨트롤러에 접속하여 가스밸브를 On/Off 시키거나, 전기료 과다 청구 유발, 도어락 개폐, IP 카메라의 관리자 페이지에 접속 및 영상 정보 탈취 등이 가능하다.

이와 같은 점을 이용한 공격 시나리오는 <그림 2-3>와 같다.



<그림 2-3> 접근제어가 없는 경우의 보안 위협

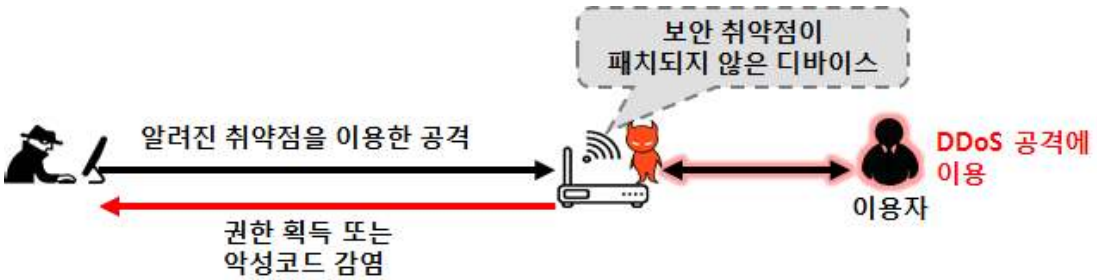
따라서 사물인터넷 디바이스는 인가된 이용자만이 이용 및 관리하여야 하며, 보안 위협을 방지하기 위하여 인가된 이용자인지 확인하고, 비 인가자의 보안 위협에 대응할 수 있도록 ID, 패스워드, RFID 태그, MAC 주소 등 다양한 인증 수단을 이용하여야 한다.

2.3 DDoS 공격 악용

일반적으로 사물인터넷 디바이스에 취약점이 발견되면, 이를 해결한 보안 업데이트가 이루어져야 한다. 하지만 보안 업데이트가 이루어 졌음에도 불구하고 이용자들이 해당 업데이트를 적용시키지 않는다면, 알려진 취약점이 무방비상태로 노출되게 된다. 알려진 취약점으로 인하여 해당 디바이스에 악성코드가 감염되면 DDoS 공격에 활용되어 이용자 모르게 타인을 공격하게 된다.

위 보안 위협에 대한 실제 사례로, 16년 10월 주요 도메인 네임 시스템(DNS) 제공업체인 DYN(딘)을 대상으로 한 분산 서비스 거부공격이(DDoS)[1] 발생하였다. DNS는 웹 라우팅 시스템으로 kisa.or.kr과 같은 웹사이트 이름을 203.255.210.86과 같이 컴퓨터가 읽을 수 있는 숫자로 된 인터넷 프로토콜 주소로 변환해주는 역할을 한다. DNS가 없으면 웹 브라우저는 사용자가 보고자 하는 웹사이트를 찾을 수 없는데, 이러한 서비스를 제공해주는 DYN의 서버에 DDoS 공격이 발생하여 한동안 수백만 명의 인터넷 사용자들이 불편을 겪었다. 공격자는 많은 사물인터넷 디바이스들이 알려진 취약점과 출고 당시 기본 패스워드를 사용하고 있는 점을 이용하여 악성코드를 감염시켜 DDoS 공격에 이용하였다.

이와 같이 알려진 취약점을 이용한 공격 시나리오는 <그림2-4>와 같다.



<그림 2-4> 보안 취약점을 가진 디바이스에 대한 보안 위협

이와 같은 보안 위협을 방지하기 위하여 펌웨어를 최신 버전으로 유지해야 한다. 제조사에서 알려진 취약점을 해결한 버전을 배포하였는지 제조사의 보안 공지 내용을 정기적으로 확인하여 보안 업데이트를 적용해야 한다.

---

1) 분산 서비스 거부 공격(DDoS) : 수십~수백만 대의 PC(디바이스)를 특정 서버(웹사이트)에 동시에 접속시킴으로써 단시간 내에 과부하를 일으켜 서버를 마비시키는 공격

제3장

스마트 홈·가전 보안 가이드

제3장 스마트 홈·가전 보안 가이드

본 장에서는 사물인터넷 소형 스마트 홈·가전 기기들 중에서, IP 카메라 기준으로 실제 설정 화면을 통해 보안위협에 대한 대응 방안을 제시한다.

※ 제품마다 설정 화면과 설정 방법의 차이가 있으며, 본 가이드의 설정 화면과 다를 수 있음

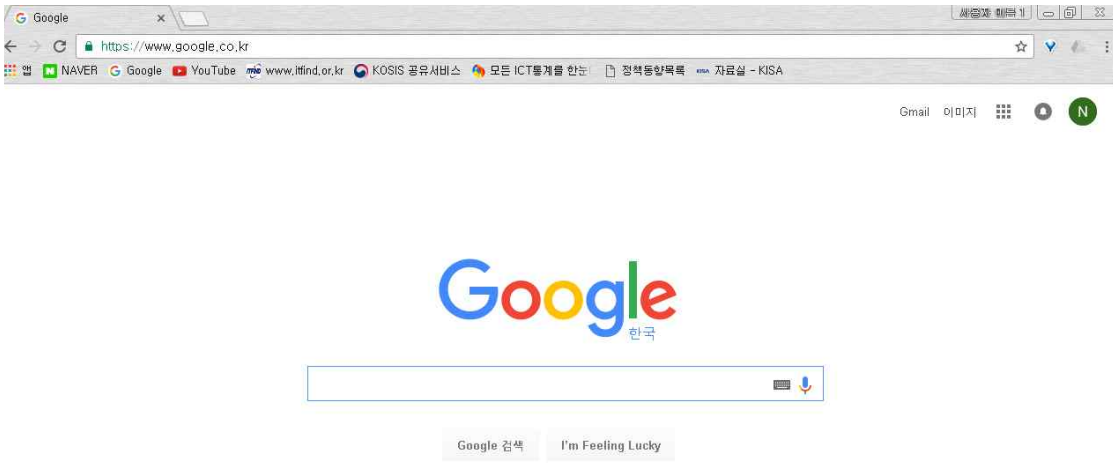
3.1 패스워드 설정

패스워드 설정 미흡으로 인한 정보 유출을 방지하기 위하여 초기 패스워드 변경, 주기적인 패스워드 변경, 접속 기록 관리 등을 수행하여야 한다.

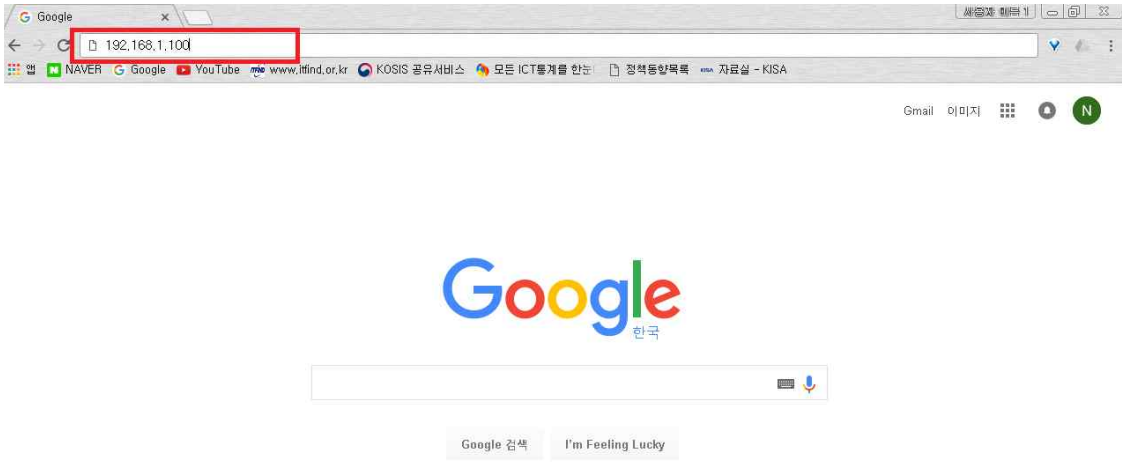
디바이스 초기 작동 시 기본 값으로 설정된 패스워드를 변경하여야 하며, 악의적인 목적을 가진 비 인가자가 관리자 페이지에 접근할 수 없도록 이용자는 추측이 어려운 비밀번호로 설정해야 한다.

[초기 패스워드 설정 방법 예시]

① 인터넷 브라우저를 실행한다.



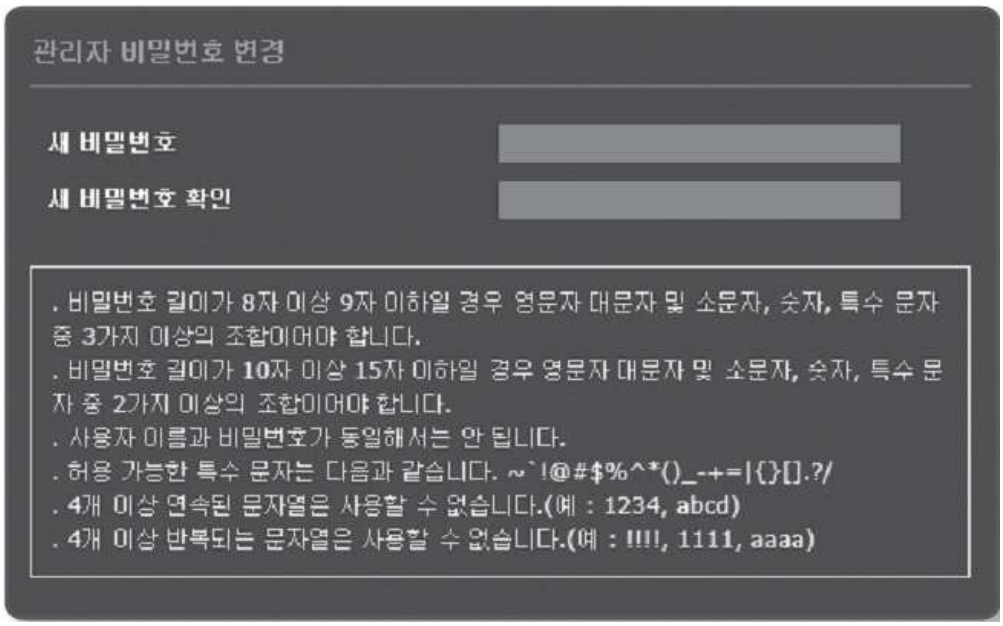
② 주소 입력란에 디바이스의 IP주소를 입력 하고 Enter 키를 입력한다.



예시1) IP주소 (IPv4) : 192.168.1.100인 경우
- http://192.168.1.100

예시2) IP주소 (IPv6) : 2001:230:abcd:ffff:0000:0000:ffff:1111인 경우
- http://[2001:230:abcd:ffff:0000:0000:ffff:1111]

③ 초기 패스워드 설정 창이 뜨면 사용하실 비밀번호를 입력하신 후 Enter 키를 입력한다.

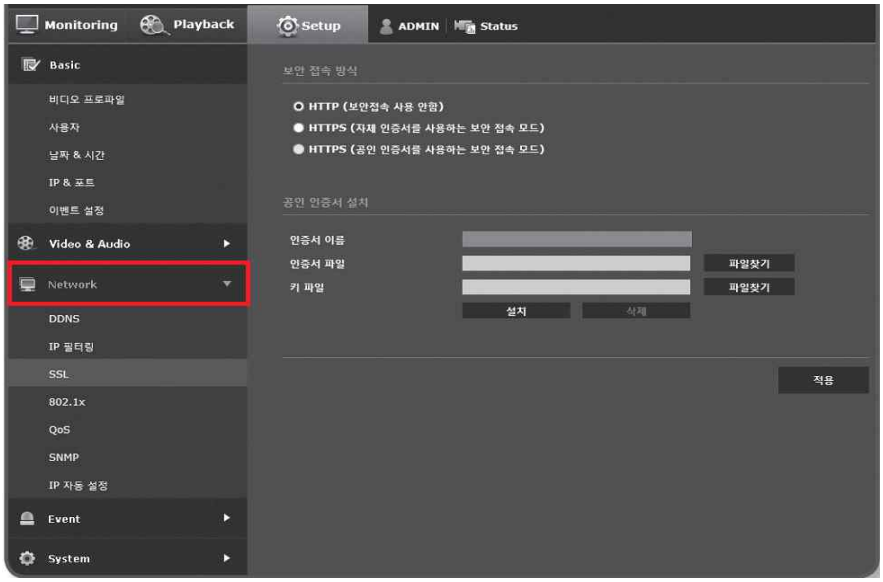


3.2 암호화 설정

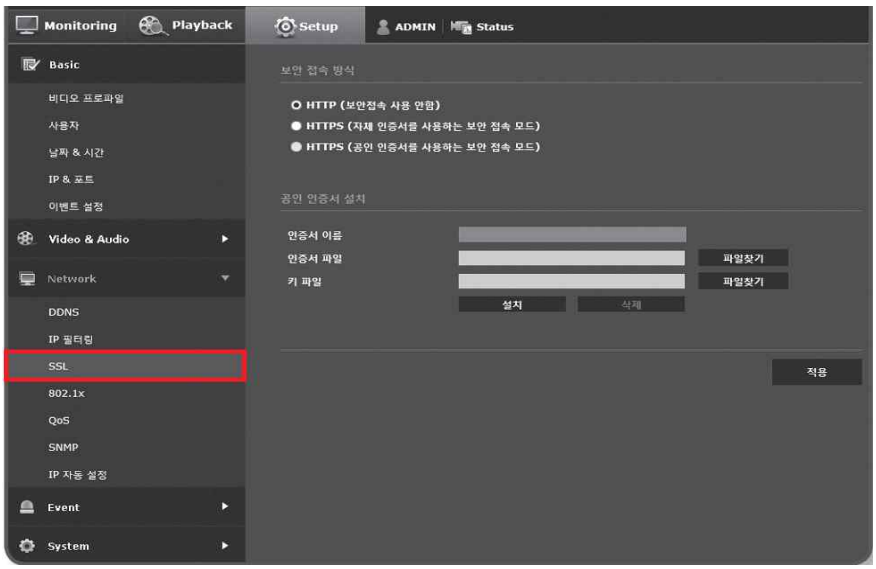
암호화 관련 취약점으로 인한 영상 정보 유출을 방지하기 위하여 SSL, TLS, SRTP 등의 보안 통신 프로토콜을 적용하여야 한다.

[SSL 적용 방법 예시]

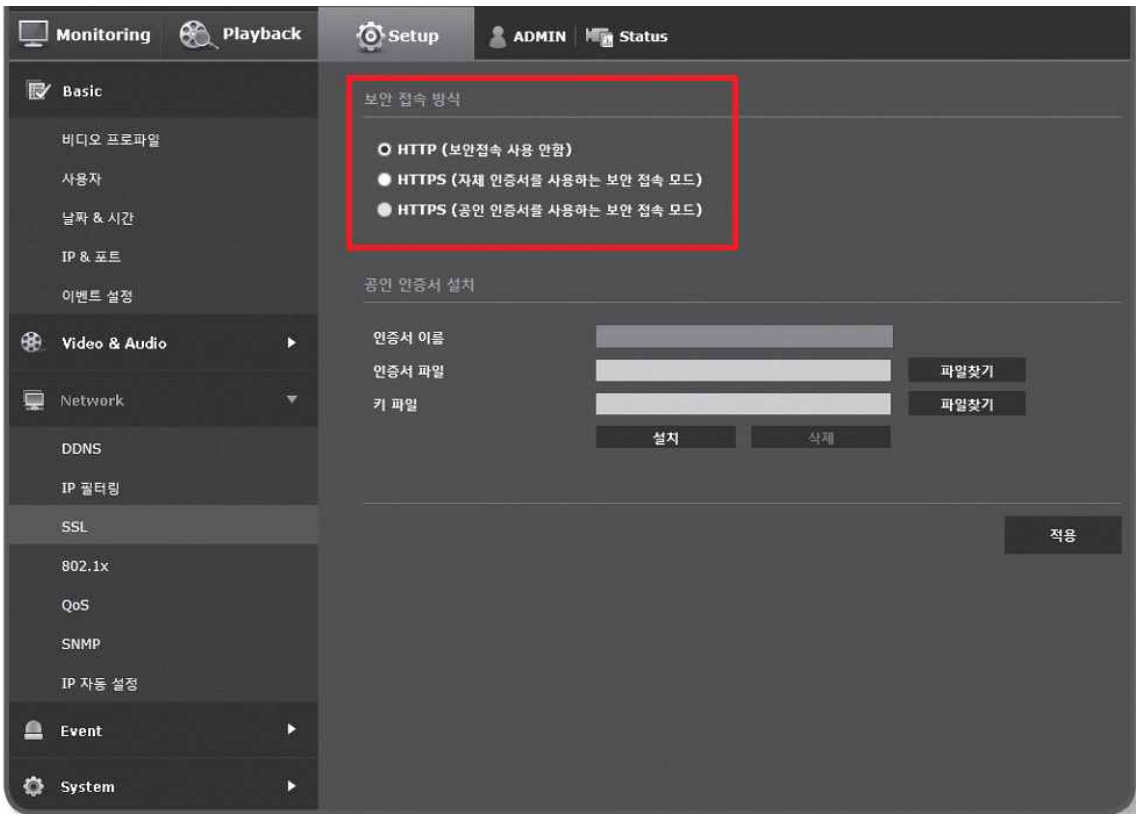
① 설정 메뉴에서 <Network> 탭을 선택한다.



② <SSL>을 클릭한다.

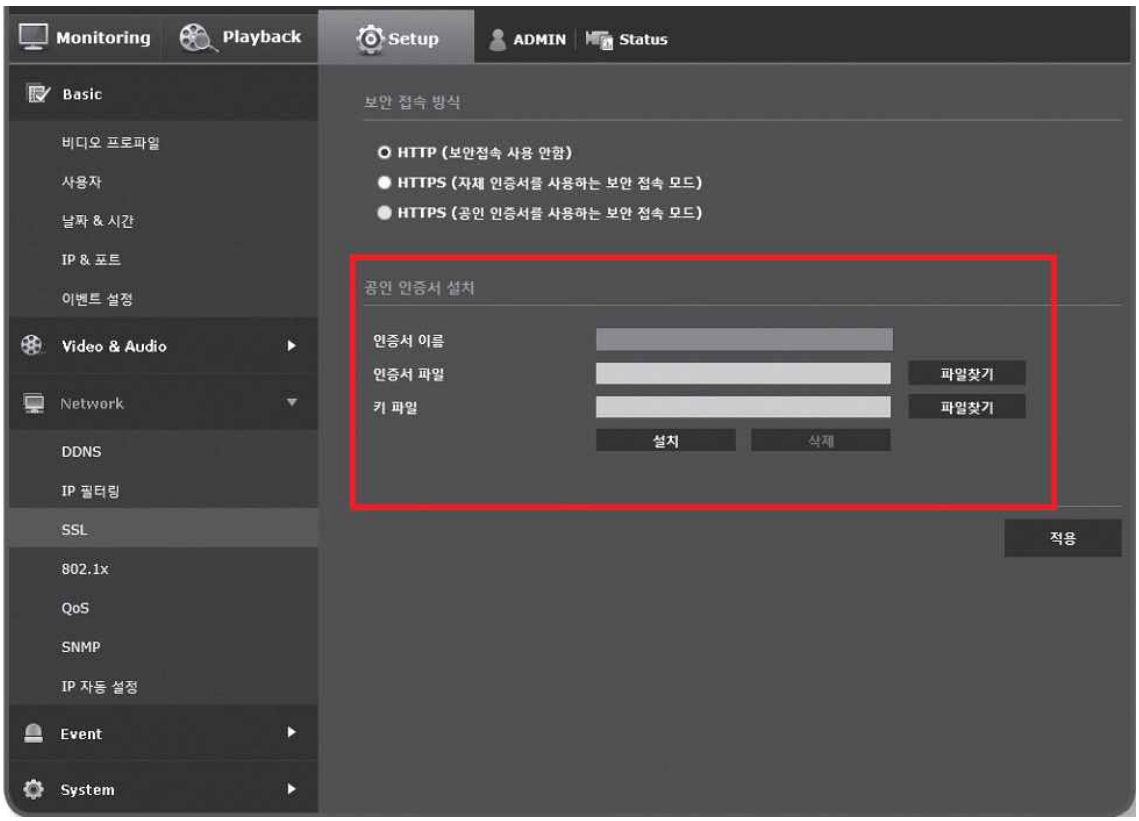


③ 보안 접속 방식을 선택한다.



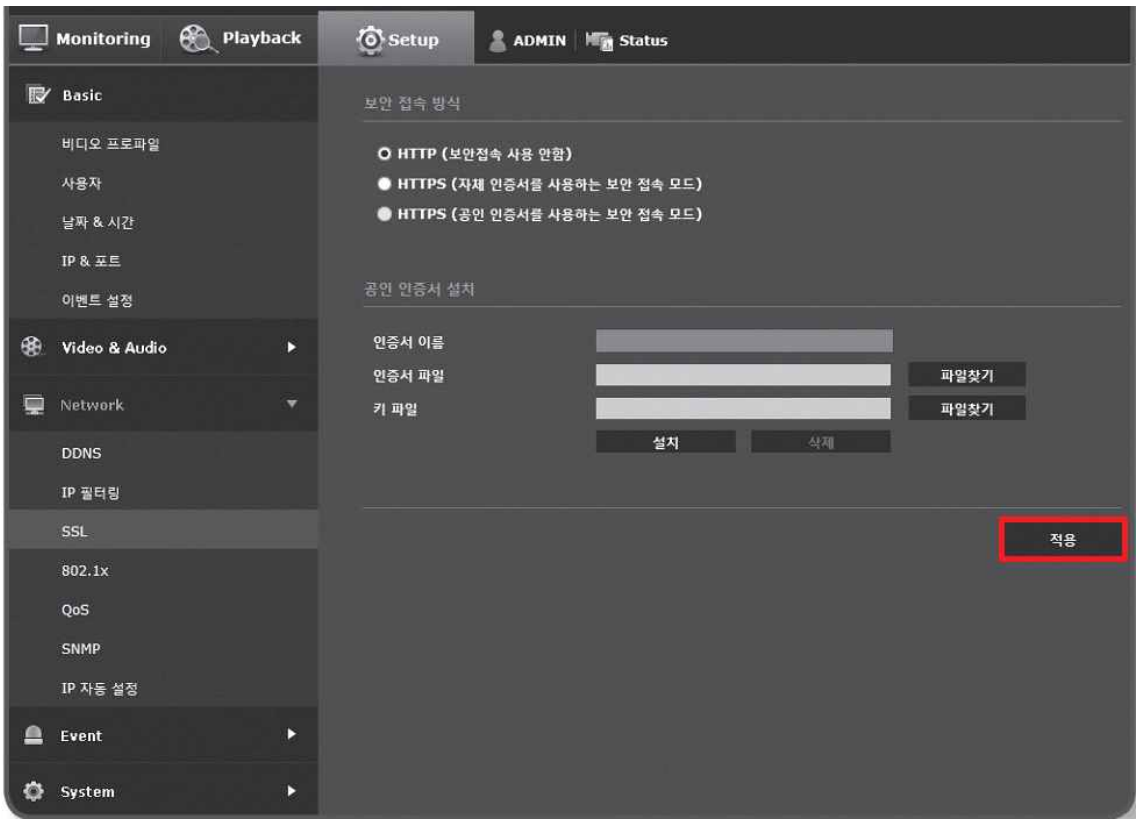
- HTTPS 모드를 사용해 카메라에 접속하기 위해 카메라의 IP 주소를 https://<카메라의 IP>로 입력한다.
- Internet Explorer에서 HTTPS모드에서 웹뷰어 설정이 안되는 경우 다음과 같이 인터넷 옵션을 변경한다.
  - <메뉴 → 도구 → 인터넷 옵션 → 고급 → 보안 → TLS 1.0 선택 해제 및 TLS 1.1, TLS 1.2 선택>

④ 카메라에 설치할 공인 인증서를 검색하여 등록한다.



- 카메라에 인증서를 설치하기 위해 (사용자가 임의 지정 가능한) 인증서 이름, 인증기관에서 발행한 인증서 파일, 키 파일을 입력한다.
- <HTTPS (공인 인증서를 사용하는 보안 접속 모드)> 항목은 등록된 공인 인증서가 있을 경우만 선택할 수 있다.

⑤ 설정이 완료되면 [적용] 버튼을 클릭한다.

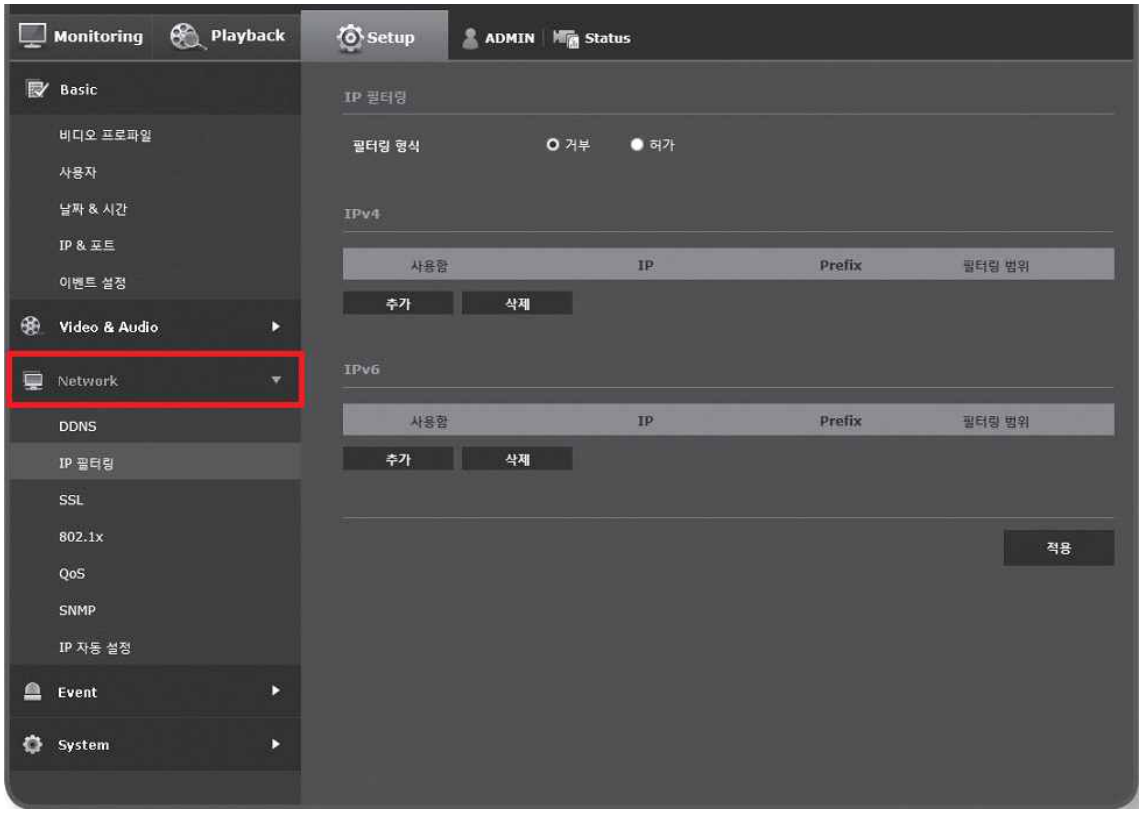


3.3 접근제어 설정 – IP/MAC 주소 인증

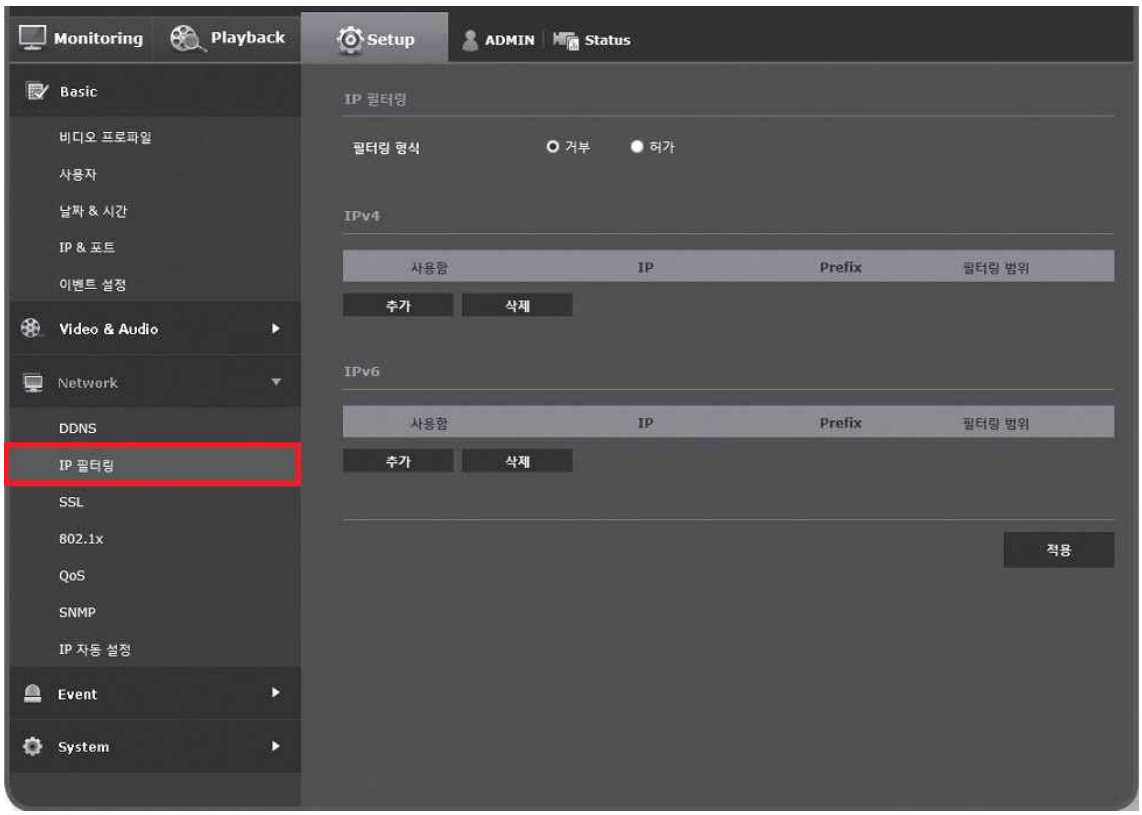
비 인가자 접속으로 인한 영상 정보 유출 등을 방지하기 위해 ID, 패스워드 외에 IP나 MAC주소 필터링 등을 이용하여 비 인가자의 접근을 제한하여야 한다.

[IP 필터링 적용 예시]

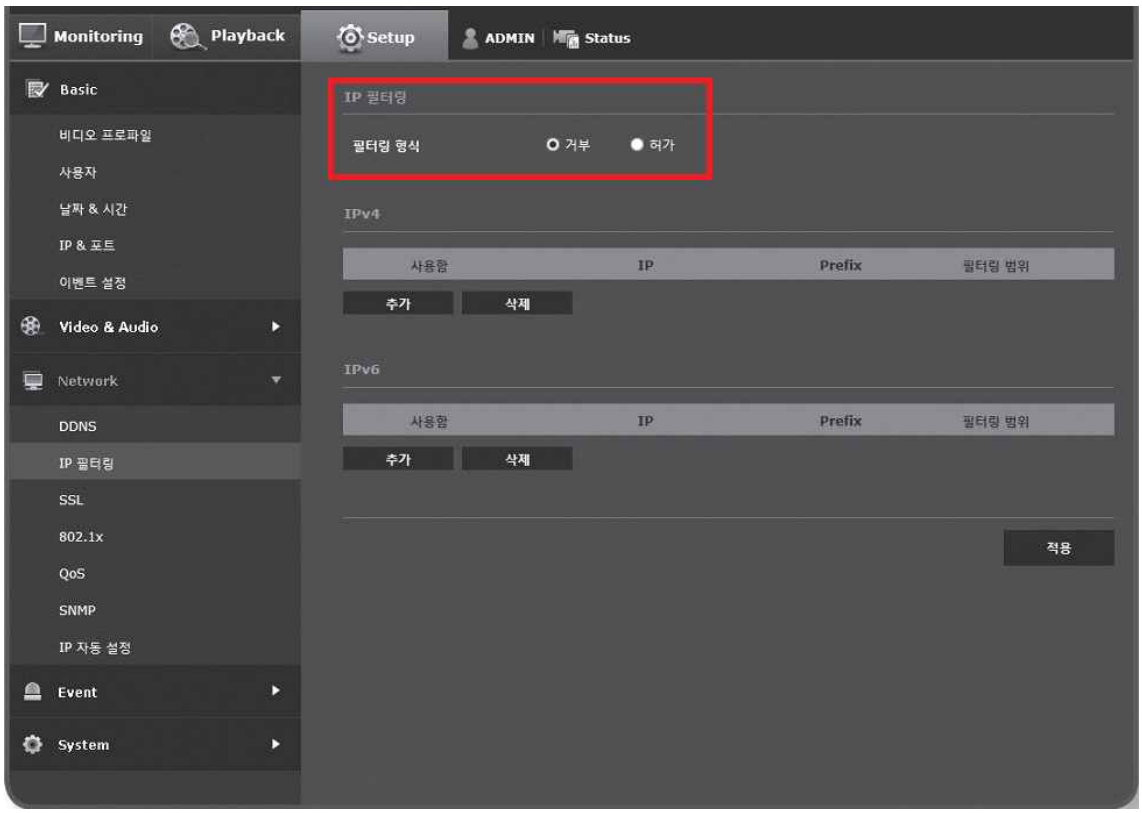
① 설정 메뉴에서 <Network> 탭을 선택한다.



② <IP 필터링>을 선택한다.

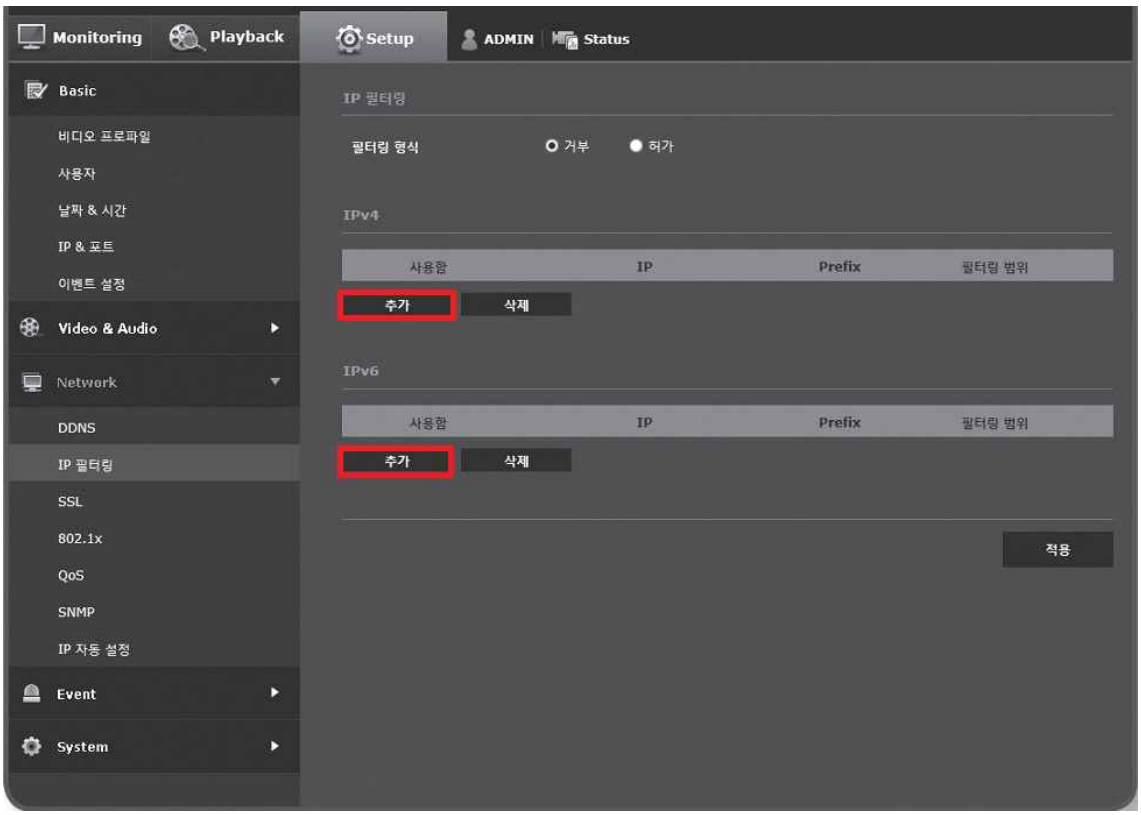


③ <필터링 형식>을 선택한다.

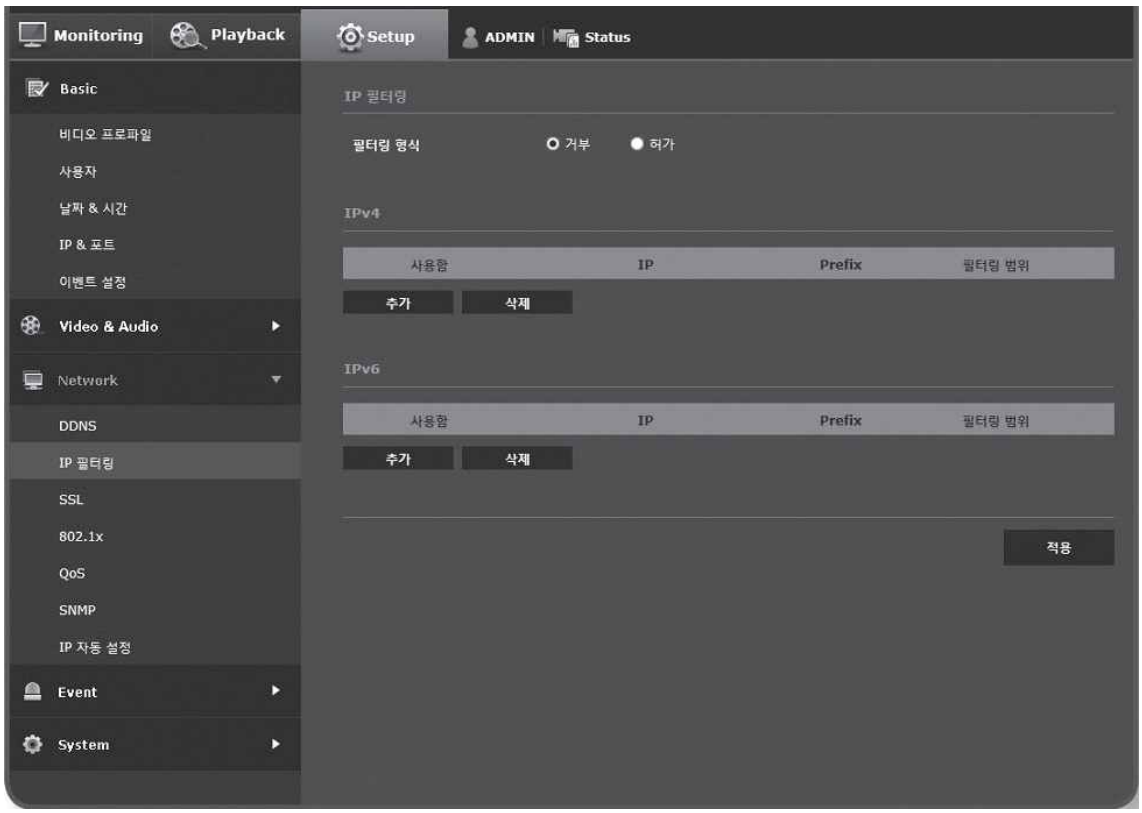


- <거부>를 선택할 경우 필터링에 등록된 IP의 접근을 제한한다.
- <허가>를 선택할 경우 등록된 IP의 접근만 허용한다.

④ <추가> 버튼을 클릭하면 IP 목록창이 생성된다.



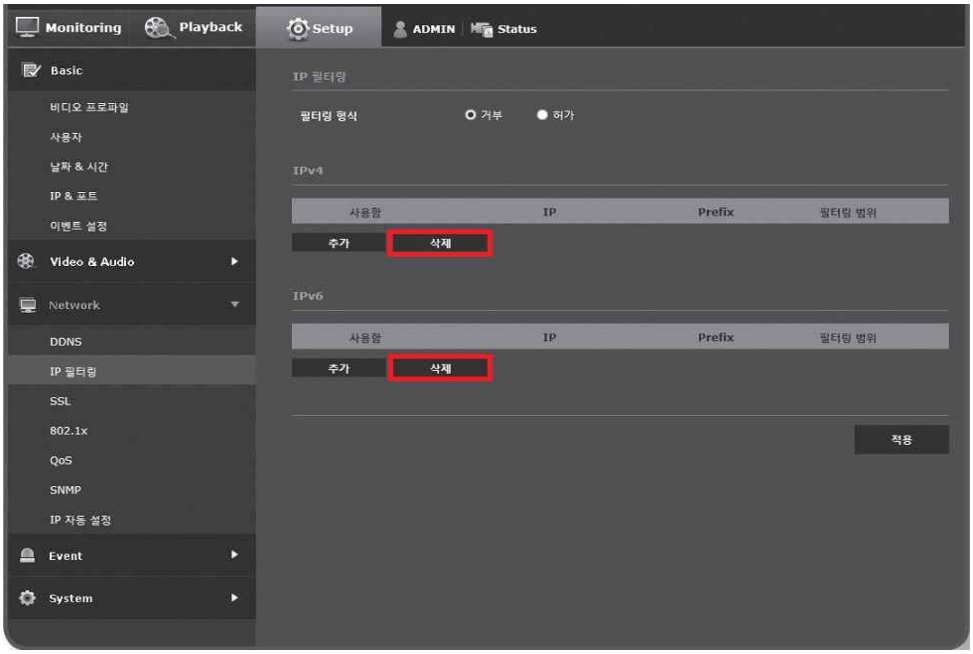
⑤ 허가 또는 거부할 IP를 입력한다.



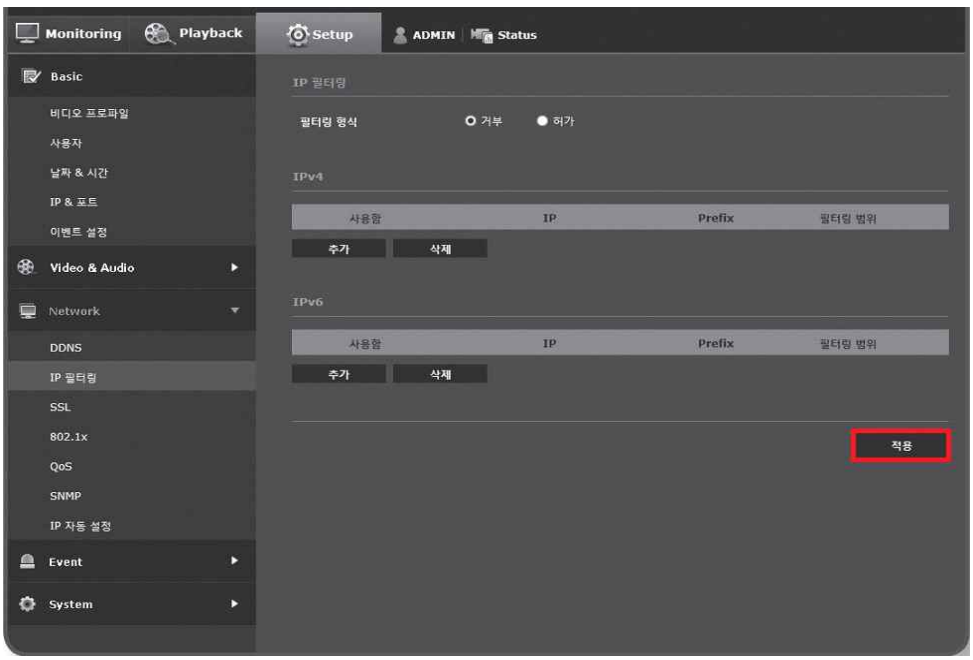
- IP 주소 및 Prefix를 입력하면 오른쪽의 필터링 범위 항목에 차단 또는 허용되는 IP 주소의 범위가 나타난다.

※ IP 필터링에서 <허가>를 선택하고, <IP & 포트>에서 <IPv6 설정>을 <사용함>으로 설정한 경우 현재 설정중인 PC의 IPv4 와 IPv6 주소를 모두 등록해야 한다.
※ 현재 설정중인 PC의 IP는 <거부>로 등록할 수 없으며, <허가>로 등록해야 한다.
※ <사용함>으로 설정한 IP들만 접속 가능하다.

⑥ IP 목록에서 삭제할 IP를 선택 후 <삭제> 버튼을 클릭하여 삭제한다.

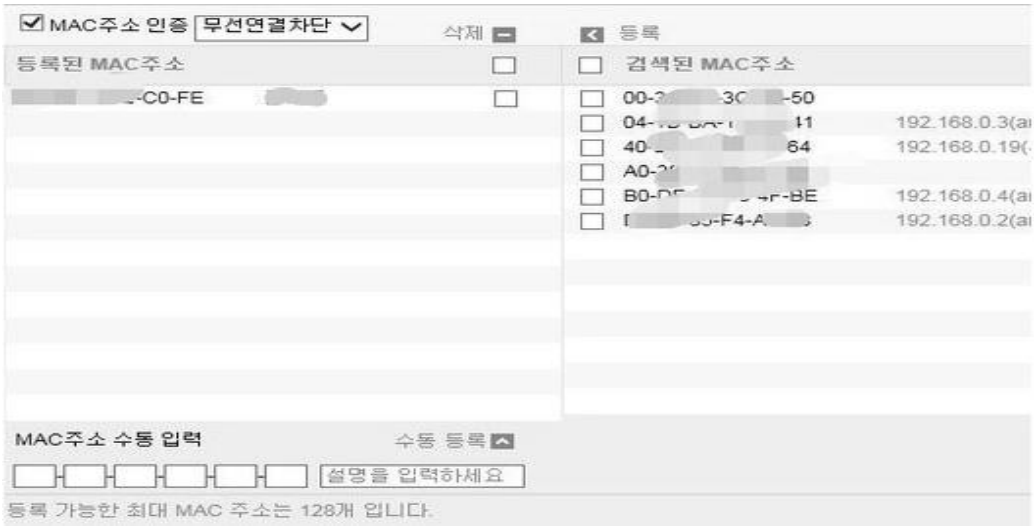


⑦ 설정이 완료되면 <완료> 버튼을 클릭한다.



[MAC 필터링 적용 예시]

이용하고 있는 디바이스에서 아래와 같이 MAC 주소 인증 기능이 있다면, 디바이스 별로 부여되어 있는 MAC 주소 인증 방식을 통해 디바이스의 비정상적인 접속을 필터링 하도록 설정한다.

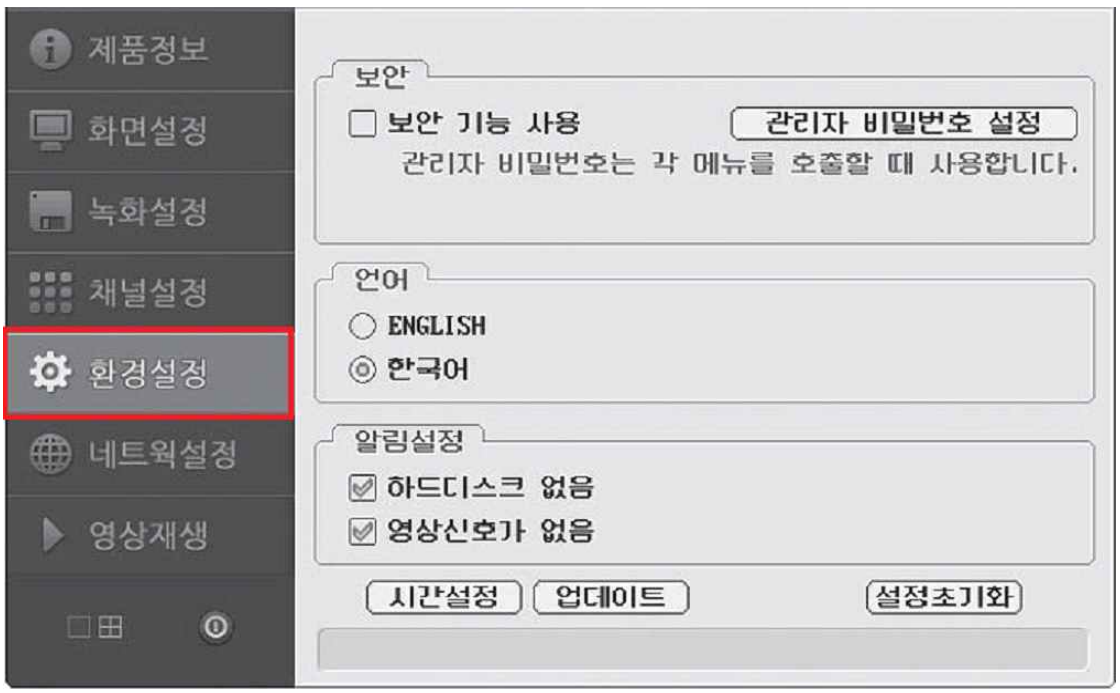


3.4 펌웨어 업데이트

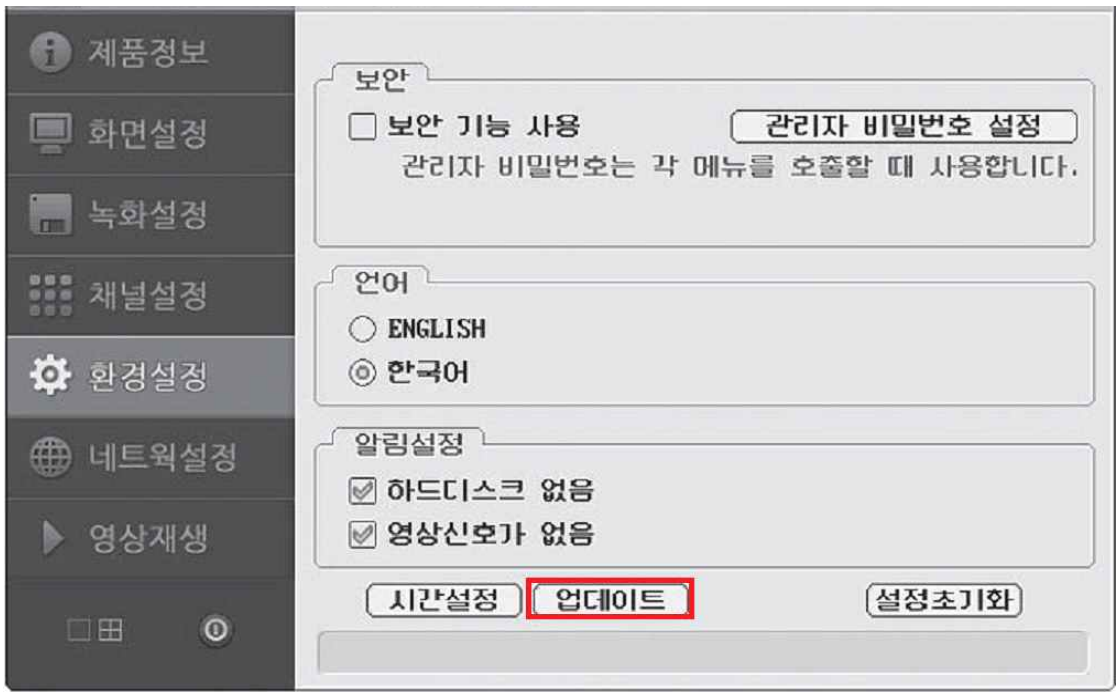
알려진 취약점으로 인한 악성코드 감염, 정보 유출 등을 방지하기 위하여 주기적인 펌웨어 업데이트 및 보안 패치를 진행하여야 한다.

[펌웨어 업데이트 예시]

① <환경설정> 탭을 클릭한다.



② <업데이트> 버튼을 클릭한다.



- 펌웨어가 최신 버전으로 업데이트된다. 업데이트는 인터넷이 연결되어있는 경우 업데이트를 실행하면 자동으로 설치되고, 인터넷이 연결되지 않은 경우 USB메모리카드나 외장하드 등을 이용 할 수 있다.

※ 펌웨어 업데이트는 다소 많은 시간이 소요될 수 있으며, 펌웨어 업데이트가 진행 중일 때에는 절대 시스템을 종료하지 않아야 한다. 강제 종료 시 시스템 고장의 원인이 될 수 있다.