

안내 사항

『의료법』 제23조(전자의무기록)제2항에 따라 전자의무기록이 **유무선 인터넷에 연결**된 경우 아래 안전성 확보 조치 필요

1. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
2. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
3. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
4. 개인정보에 대한 보안프로그램의 설치 및 갱신

더욱 강력한 안전성 확보 조치는 인터넷에 연결하지 않는 것 입니다.

의료기관 보안 설정 가이드

(공유기 및 Windows)

1. 공유기 보안 설정 미흡으로 인한 해킹 사고 사례

(사례1) 공유기 DMZ 기능 활성화로 취약 포트 외부 개방

- ▶ 000의원은 **공유기 DMZ 기능**이 PACS 서버로 지정되어 취약한 포트가 외부에 개방되어 **랜섬웨어 감염**
- ▶ 1차 랜섬웨어 감염 후 보안조치 없이, 단순 시스템 재 설치하여 운영 중 2차 랜섬웨어 감염 발생



* DMZ 기능: 지정된 IP로 모든 포트의 외부 접근을 허용하는 기능

1. 공유기 보안 설정 미흡으로 인한 해킹 사고 사례

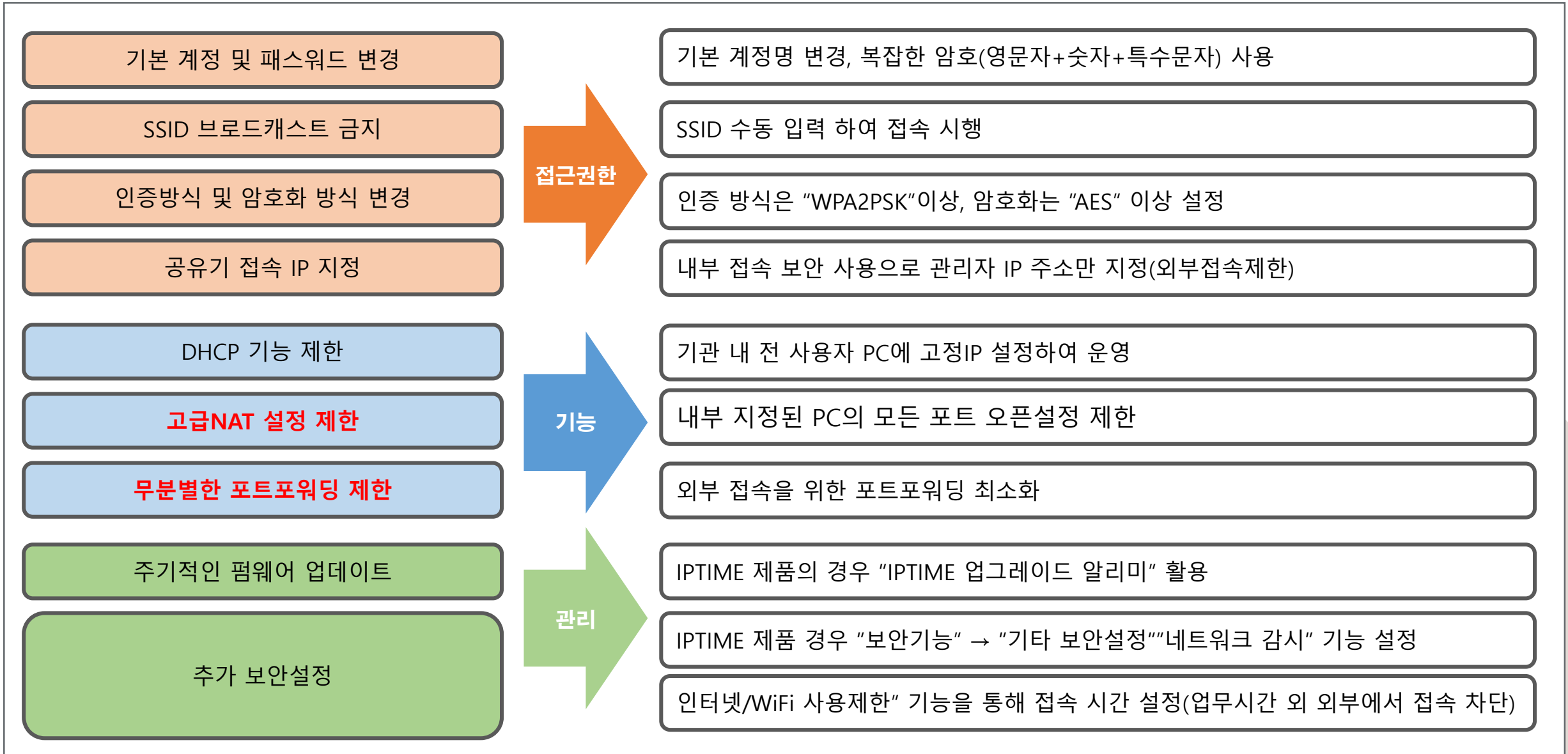
(사례2) 공유기 포트포워딩 기능을 통한 RDP 포트 외부 개방

- ▶ 000병원은 **공유기 포트포워딩 기능**을 통해 RDP 포트가 외부에 개방되어 랜섬웨어 감염
- ▶ 랜섬웨어 감염 후 보안조치 없이, 단순 시스템 재 설치하여 운영 중 RDP 포트를 통한 추가 공격 시도 확인



* 포트포워딩 기능: 공유기에서 특정 IP와 포트를 접근 허용하는 기능

2. 공유기 자체 보안 점검 리스트



3-1. 기본 계정 및 비밀번호 변경

기본 ID명 변경, 복잡한 암호(영문자+숫자+특수문자) 사용 권고

(위험)

- 공유기 기본 ID 및 PW 사용 시 내/외부 사용자가 무단으로 접근하여 공유기 설정을 임의로 변경가능

(권고)

○시스템 관리 - 관리자 설정

- **admin 계정명 변경** (변경 불가 시 복잡한 암호 설정)
- **복잡한 암호(영문자+숫자+특수문자) 사용**

(설명)

○공유기 기본 ID/PW 확인 필요

- admin/admin , root/root , root/toor 등 초기 패스워드 사용 확인

3-2. 기본 계정 및 비밀번호 변경

기본 ID명 변경, 복잡한 암호(영문자+숫자+특수문자) 사용 권고

메뉴탐색기

- 기본 설정
- 시스템 요약 정보
- 인터넷 연결 설정
- 무선 설정/보안
- 펌웨어 업그레이드
- 고급 설정

무선 설정/보안

동작 설정	☒ 실행 ☐ 중단
네트워크이름(SSID)	Marine ☐ 네트워크이름 알림
채널	11 [2.462 GHz, 상위] 채널 검색
인증 및 암호화	WPA2PSK + TKIP
네트워크 암호	 ☐ 암호보기

(위험)

- 기관에서 무선 네트워크 사용시 외부에 오픈된 SSID(Wifi 네트워크 이름)를 확인하여 외부 사용자가 패스워드 미사용 또는 취약한 패스워드 사용 시 쉽게 내부 네트워크 접속 가능

(권고)

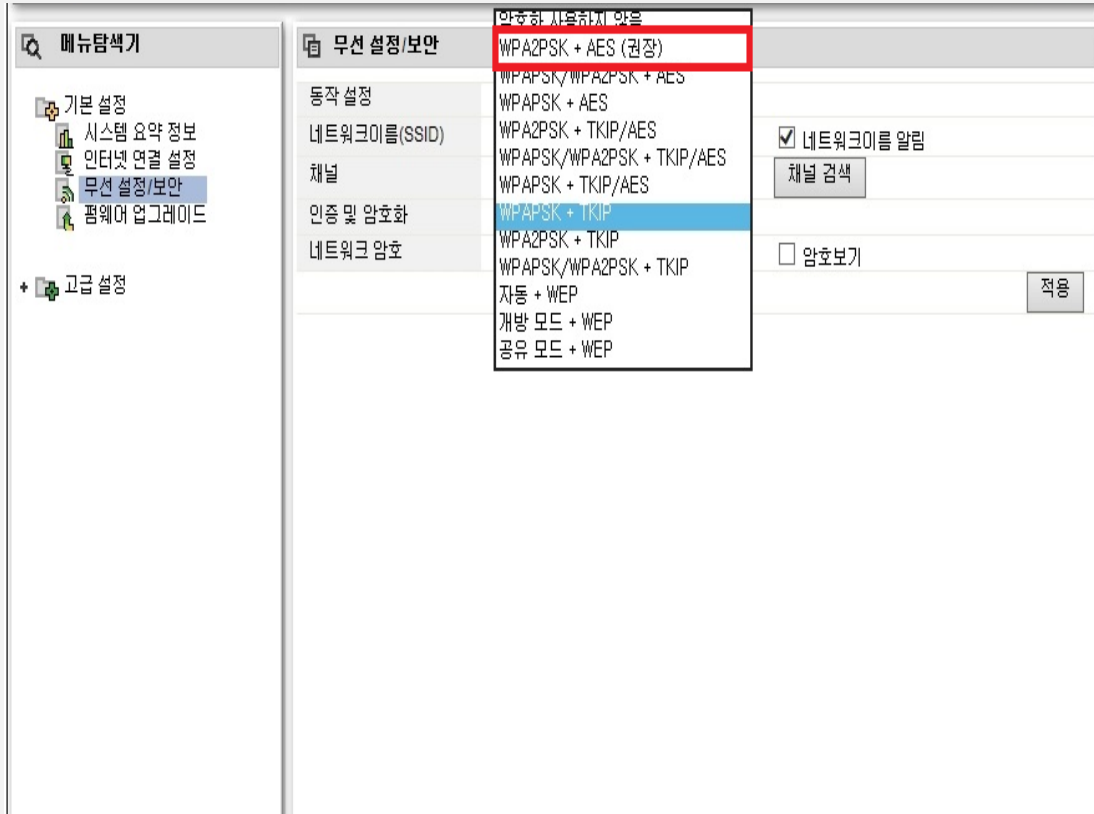
- 무선 네트워크 미사용 시 해당 기능 비활성화
- “네트워크이름 알림” 비활성화

(설명)

- SSID(Wifi 네트워크 이름) 숨김 처리 시 Wifi를 사용하려는 일반 사용자에게 해당 네트워크 이름이 검색되지 않음

3-3. 인증방식 및 암호화 방식 변경

기본 ID명 변경, 복잡한 암호(영문자+숫자+특수문자) 사용 권고



(위험)

○ 취약한 인증 및 암호화 방식을 설정하여 사용시 공격자가 무선 해킹 도구등을 이용하여 무선 AP 네트워크 키 획득을 통해 내부 네트워크 접속 가능

(권고)

○ **WPA2PSK + AES (권장)**

(설명)

○ **WPA2 (Wifi Protected Access 2)**

- AES-CCMP를 통한 암호화 기능 향상, EAP 사용자 인증 강화 등 포함

○ **AES (Advanced Encryption Standard)**

- CCM 모드를 이용한 데이터 암호화 방식 정의, 하드웨어 암호기법을 사용하여 TKIP보다 안전

3-4. 공유기 접속 IP 지정

내부 접속 보안 사용으로 관리자 IP 주소만 지정(외부접속제한)

메뉴탐색기

- 기본 설정
 - 시스템 요약 정보
 - 인터넷 설정 정보
 - 무선 설정/보안
 - 펌웨어 업그레이드
 - Easy Mesh
- 고급 설정
 - 네트워크 관리
 - 인터넷 설정 정보
 - 내부 네트워크 설정
 - DHCP 서버 설정
 - 무선랜 관리
 - 무선 설정/보안
 - 무선확장설정
 - MAC주소 관리
 - Easy Mesh
 - NAT/라우터 관리
 - 포트포워드 설정
 - 고급 NAT 설정
 - 라우터 데이터 관리

공유기 접속/보안관리

외부 접속 보안

☐ 원격 관리 포트 사용 원격 관리 포트 0 적용

☐ 외부 접속 보안 사용 허용 할 IP 주소 설명을 입력하세요 추가

IP 주소 최대 10개 추가 가능 설명 삭제

내부 접속 보안

☒ 내부 접속 보안 사용 허용 할 IP 주소 192.168.0.0 설명을 입력하세요 추가

IP 주소 최대 10개 추가 가능 설명 삭제

1	192.168.0.30	자동 항목	
---	--------------	-------	--

고급 보안 설정 ▲

on 악성 스크립트 접근 방지(CSRF)

(위험)

- 지정된 IP만 접근하도록 설정되어 있지 않을 경우 비인가자가 사전 대입 공격 등을 시도하여 접속 계정 패스워드 획득 후 공유기 접근 및 공유기 설정을 임의로 변경가능

(권고)

- 관리자 IP를 지정하여 공유기 접속 관리

(설명)

- 원격 관리 포트 사용
 - 외부 인터넷을 통해 공유기 관리 가능
- 외부 접속 보안
 - 외부 공인 IP를 지정하여 지정된 IP만 공유기 관리 가능
- 내부 접속 보안
 - 내부 IP를 지정하여 지정된 IP만 공유기 관리 가능

3-5. DHCP 기능 제한

기관 내 전 사용자 PC에 고정IP 설정하여 운영

메뉴탐색기

DHCP 서버 설정

DHCP 서버 동작 ☒ 실행 ☐ 중지 (10 개 IP주소 할당됨)

IP주소 대역 범위 192.168.0.2 ~ 192.168.0.254 ☐ 수동 지정

서브넷 마스크 255.255.255.0 ☐ 수동 지정

게이트웨이 주소 192.168.0.1 ☐ 수동 지정

기본 DNS 주소 8.8.8.8

보조 DNS 주소 168.126.63.2 ☒ 수동 지정

IP주소 대역 시간 2시간 DNS 서비스

DHCP서버충돌 ☐ 충돌 발견시 중단 적용

DHCP 서버 주소관리 ☐ 등록 주소만 인터넷 허용 ☐ 자동할당 주소만 인터넷 허용

등록된 주소 관리(최대 200 개) ☒ 삭제

사용중인 IP 주소 정보 ☒ 재검색 ☒ 등록

192.168.0.5	08-15-DC-04-ED-3D	무선:자동할당	☐
192.168.0.7	71-ED-08-08-1E-ED	--수동설정	☐
			☐
			☐
			☐
			☐

수동 주소 입력 192.168.0.0 설명을 입력하세요 ☒ 수동 등록

(위험)

○ DHCP 기능 사용으로 사용자 PC 및 공유기 재부팅 시 IP가 랜덤하게 변경 될 수 있으며 특정 서비스 사용 불가 등 네트워크 통신 오류 발생 가능

(권고)

○ 기관 사용자 PC 고정 IP 사용

- 사용자 PC의 고정IP 및 MAC 주소 확인 후 수동 등록 필요

(설명)

○ DHCP (Dynamic Host Configuration Protocol)

- 컴퓨터의 네트워크 접속 시 IP 주소와 게이트웨이를 자동으로 할당하는 기능

3-6. 고급NAT 설정 제한

내부 지정된 PC의 모든 포트가 외부에 오픈되어 고급NAT 설정 제한 권고

메뉴탐색기

- 기본 설정
 - 시스템 요약 정보
 - 인터넷 설정 정보
 - 펌웨어 업그레이드
 - Easy Mesh
- 고급 설정
 - 네트워크 관리
 - 인터넷 설정 정보
 - 내부 네트워크 설정
 - DHCP 서버 설정
 - NAT/라우터 관리
 - 포트포워드 설정
 - 고급 NAT 설정**
 - 라우팅 테이블 관리
 - 보안 기능
 - 특수기능
 - 트래픽 관리
 - 시스템 관리
 - 시스템 로그
 - 관리자 설정
 - 펌웨어 업그레이드
 - 기타 설정

Mobile UI

고급 NAT 설정

DMZ/Twin-IP	DMZ IP - 192.168.0.
FTP 비정규 포트	
인터넷 공유 기능	실행
포트포워드 UPnP 릴레이	실행

DMZ/Twin-IP

☒ 사용하지 않음

☒ DMZ (지정된 내부 IP 주소의 PC로 모든 포트를 개방합니다. 단, 포트포워드에 설정된 포트는 제외)

☐ Twin IP (지정된 MAC 주소의 PC가 공인 IP 주소를 사용하도록 합니다)

내부 IP주소: 192.168.0.1 ☐ 현재 접속된 PC의 IP 주소로 설정(192.168.0.4)

적용

(위험)

- 해당 기능 사용시 내부 지정된 PC의 모든 포트가 외부에 공개되어 공격자는 외부에 오픈된 포트를 스캔하고 해당 포트의 취약점을 악용하여 공격 시도

(권고)

- 고급NAT 설정 사용 제한 (**사용하지 않음** 설정)

(설명)

○ 사용하지 않음

- 고급 NAT 설정 기능 사용하지 않음

○ DMZ

- 지정된 내부 IP 주소의 PC로 모든 포트를 개방
단, 포트포워드에 설정된 포트는 제외

○ Twin IP

- 지정된 MAC 주소의 PC가 공인IP 주소를 사용하도록 함

3-7. 무분별한 포트포워딩 제한

외부 접속을 위한 특정포트(RDP,DB 등) 포트포워딩 제한

메뉴탐색기

- 기본 설정
 - 시스템 요약 정보
 - 인터넷 설정 정보
 - 펌웨어 업그레이드
 - Easy Mesh
- 고급 설정
 - 네트워크 관리
 - 인터넷 설정 정보
 - 내부 네트워크 설정
 - DHCP 서버 설정
 - NAT/라우터 관리
 - 포트포워딩 설정**
 - 고급 NAT 설정
 - 라우팅 테이블 관리
 - 보안 기능
 - 특수기능
 - 트래픽 관리
 - 시스템 관리
 - 시스템 로그
 - 관리자 설정
 - 펌웨어 업그레이드
 - 기타 설정

Mobile UI

포트포워딩 설정

사용자정의 규칙보기

순위	사용자 규칙	내부 IP	외부 포트	내부 포트	삭제
+	새규칙 추가				

규칙이름: [] 포트포워딩 사용자정의 [x] 규칙 비활성화 [] 순위: []

내부 IP주소: 192.168.0. [] 현재 접속된 IP 주소 [x] 순위높임 [x] 순위낮춤 [x]

프로토콜: TCP 외부 포트: [] ~ [] 내부 포트: [] ~ []

PC<-규칙저장 PC->규칙복원 파일 선택 선택된 파일 없음 새규칙 적용 취소

(위험)

- 해당 기능 사용시 내부 지정된 PC의 특정 포트(RDP,DB 등)가 외부 공개되어 공격자는 외부에 오픈된 포트의 취약점을 악용하여 공격 시도

(권고)

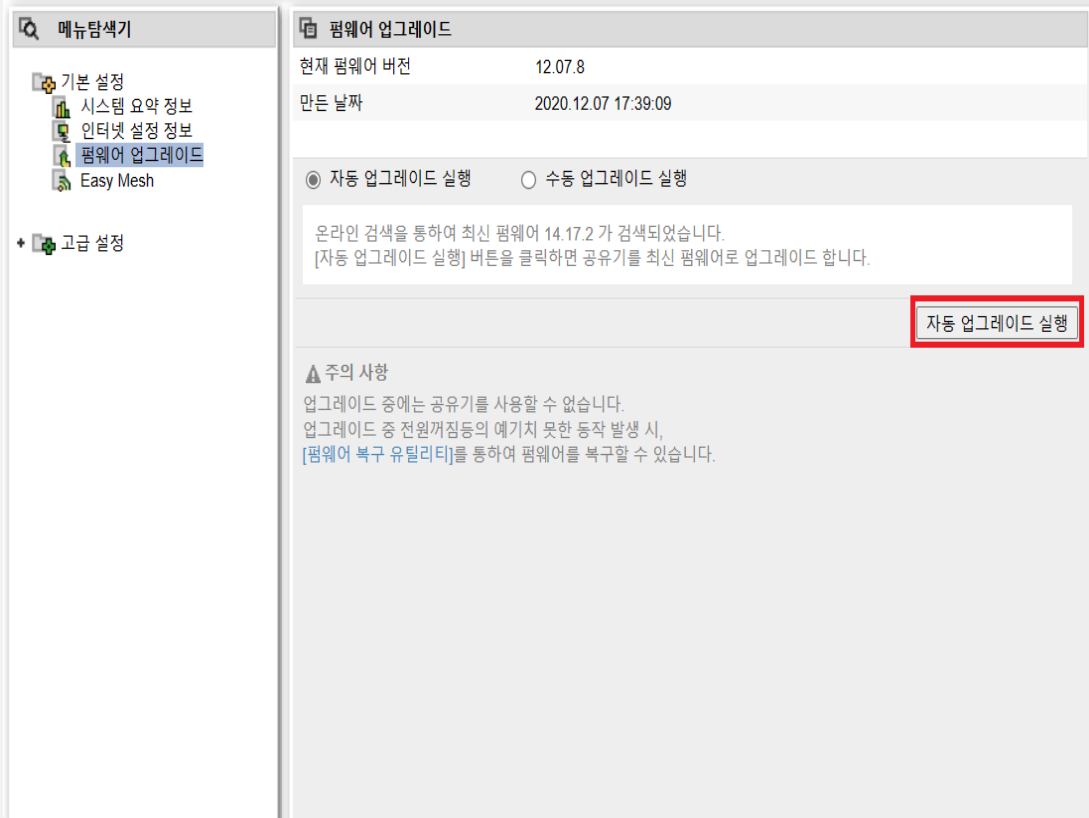
- **특정포트 포트포워딩(RDP, DB등) 설정 제한**

(설명)

- **내부 IP 주소**
 - 의료기관 EMR, PACS 시스템 관리를 위한 IP 지정
- **프로토콜**
 - 의료기관 접속 관리를 위한 원격 접속(RDP), DB포트 등을 지정

3-8. 주기적인 펌웨어 업데이트

주기적으로 최신 펌웨어 확인 및 최신 펌웨어 업데이트 실행 권고



The screenshot shows the '메뉴탐색기' (Menu Explorer) on the left with '펌웨어 업그레이드' (Firmware Upgrade) selected. The main panel is titled '펌웨어 업그레이드' and displays the current version (12.07.8) and creation date (2020.12.07 17:39:09). It has two radio buttons: '자동 업그레이드 실행' (selected) and '수동 업그레이드 실행'. Below them is a message: '온라인 검색을 통하여 최신 펌웨어 14.17.2 가 검색되었습니다. [자동 업그레이드 실행] 버튼을 클릭하면 공유기를 최신 펌웨어로 업그레이드 합니다.' A red box highlights the '자동 업그레이드 실행' button. At the bottom, a warning section '주의 사항' states that during the upgrade, the device cannot be used and that the recovery utility can be used if needed.

펌웨어 업그레이드	
현재 펌웨어 버전	12.07.8
만든 날짜	2020.12.07 17:39:09

☒ 자동 업그레이드 실행 ☐ 수동 업그레이드 실행

온라인 검색을 통하여 최신 펌웨어 14.17.2 가 검색되었습니다.
[자동 업그레이드 실행] 버튼을 클릭하면 공유기를 최신 펌웨어로 업그레이드 합니다.

자동 업그레이드 실행

주의 사항
업그레이드 중에는 공유기를 사용할 수 없습니다.
업그레이드 중 전원꺼짐등의 예기치 못한 동작 발생 시,
[펌웨어 복구 유틸리티]를 통하여 펌웨어를 복구할 수 있습니다.

(위험)

- 공유기의 최신 펌웨어 업데이트를 하지 않고 사용 시 공격자는 구 버전에 존재하는 취약점을 이용하여 공유기 접속 및 내부 네트워크 대역에 접속 가능

(권고)

- **최신 펌웨어 업데이트 권고**

(설명)

○ 자동 업그레이드 실행

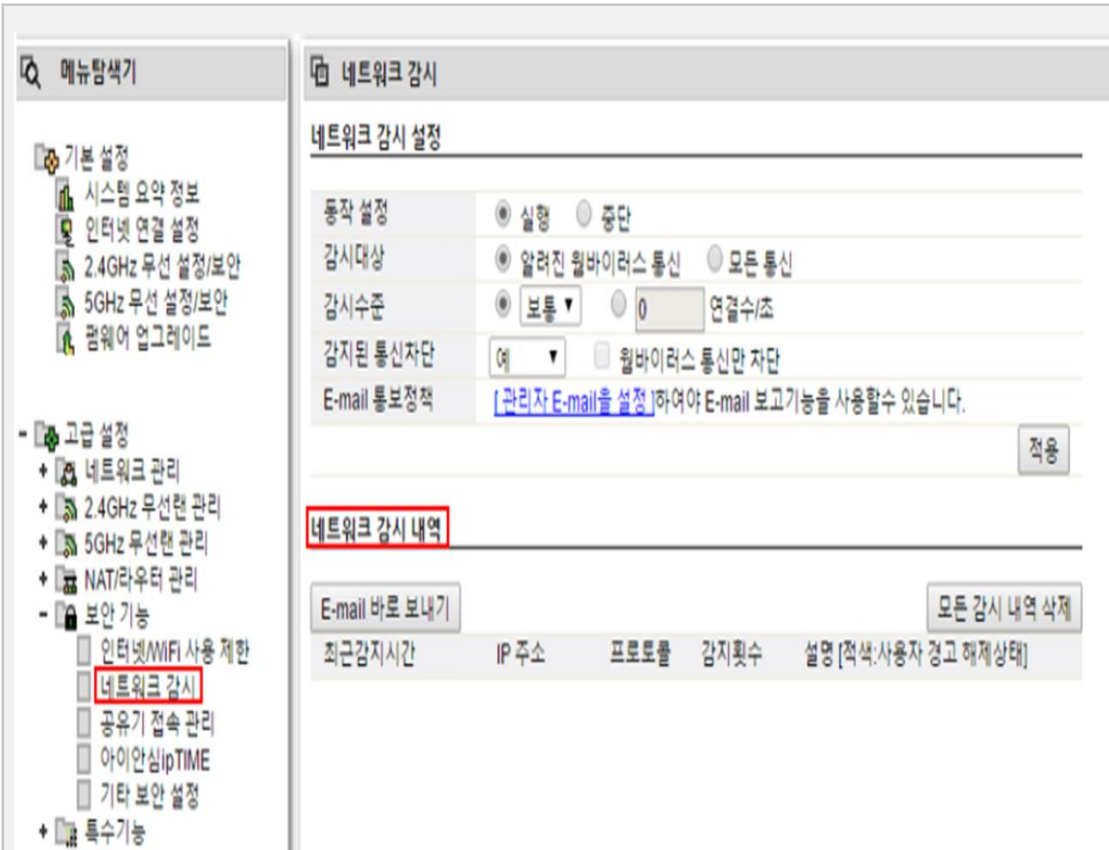
- 온라인 검색을 통하여 최신 펌웨어를 찾아 자동 업그레이드 실행

○ 수동 업그레이드 실행

- 공유기 홈페이지에서 제공하는 최신 펌웨어를 찾아 다운로드 후 다운로드한 펌웨어 파일 업로드를 통한 수동 업그레이드 실행

3-9. 추가 보안설정 권고

공유기 내 네트워크 감시 기능 활성화



메뉴탐색기

- 기본 설정
 - 시스템 요약 정보
 - 인터넷 연결 설정
 - 2.4GHz 무선 설정/보안
 - 5GHz 무선 설정/보안
 - 펌웨어 업그레이드
- 고급 설정
 - 네트워크 관리
 - 2.4GHz 무선랜 관리
 - 5GHz 무선랜 관리
 - NAT/라우터 관리
 - 보안 기능
 - 인터넷/WiFi 사용 제한
 - 네트워크 감시**
 - 공유기 접속 관리
 - 아이안심ipTIME
 - 기타 보안 설정
 - 특수기능

네트워크 감시

네트워크 감시 설정

동작 설정: ☒ 실행 ☐ 중단

감시대상: ☒ 알려진 웜 바이러스 통신 ☐ 모든 통신

감시수준: ☒ 보통 ☐ 0 연결수/초

감지된 통신차단: ☒ 예 ☐ 웜 바이러스 통신만 차단

E-mail 통보정책: [\[관리자 E-mail을 설정\]](#) 하여야 E-mail 보고기능을 사용할수 있습니다.

적용

네트워크 감시 내역

E-mail 바로 보내기 모든 감시 내역 삭제

최근감지시간	IP 주소	프로토콜	감지횟수	설명 [적색:사용자 경고 해제상태]
--------	-------	------	------	---------------------

(권고)

○ 네트워크 감시 설정 기능 실행 설정

- 동작 설정 : 실행
- 감시 대상 : 알려진 웜 바이러스 통신
- 감시수준 : 보통
- 감시 된 통신 차단 : 예

(설명)

○ 네트워크 감시

- 내부 네트워크에 연결되어 있는 모든 단말기 중 트래픽을 유발하거나 웜 바이러스 통신을 할 때, 해당 단말기를 차단 하는 기능

○ 네트워크 감시 내역

- 네트워크 감시 설정 실행을 통해 설정된 이벤트를 E-mail 발송 및 해당 내역 확인 가능

4. Windows 자체 보안 점검 리스트

Windows 패스워드 설정

Windows 패스워드 복잡성(영문자+숫자+특수문자) 설정 권고

백신 설치 및 실시간 감시 설정

바이러스 및 위협 방지를 위한 백신 활성화 및 실시간 보호 기능 설정

OS 최신 보안 업데이트

주기적으로 최신 보안 업데이트 확인 및 업데이트 실행 권고

Windows 방화벽 사용

Windows 방화벽 기능 사용 권고

관리

5-1. Windows 패스워드 설정

Windows 패스워드 복잡성(영문자+숫자+특수문자) 설정 권고



(위협)

- 패스워드 미사용 및 단순하게 설정하여 사용 시 패스워드 무작위 대입 공격 및 패스워드 추측 공격 등을 패스워드 탈취 및 비인가 접근이 가능

(권고)

○ 패스워드 복잡성(영문자+숫자+특수문자) 설정 권고

- (PC) 설정 > 계정 > 로그인 옵션 > '**비밀번호**' 변경
- (SERVER) 제어판 > 사용자 계정 > 계정 선택 > **암호변경**

(설명)

○ 무작위 대입 공격(Brute Force Attack)

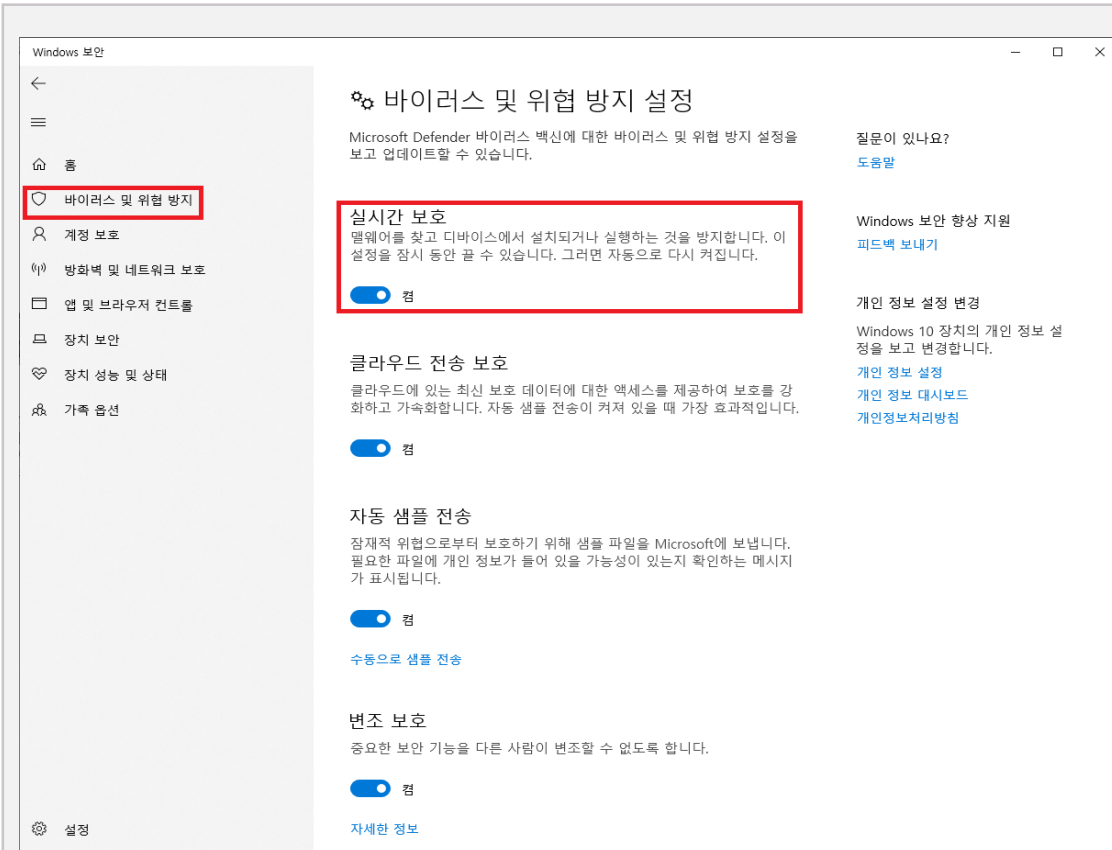
- 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도

○ 사전 공격(Dictionary attack)

- 사전에 있는 단어를 입력하여 암호를 알아내거나 해독하는 컴퓨터 공격법

5-2. 백신 활성화 및 실시간 보호 설정

바이러스 및 위협 방지를 위한 백신 활성화 및 실시간 보호 기능 설정



(위협)

- 백신 미설치 및 최신 업데이트가 이루어지지 않았을 경우 악성코드(바이러스, 웜, 랜섬웨어, 스파이웨어 등)의 감염이 발생하여 시스템의 중요한 파일이나 폴더의 유출 및 삭제가 발생할 위험이 존재

(권고)

○ 백신 및 실시간 보호 기능 활성화 권고

- (Windows Defender)

- ① Windows 보안 > '바이러스 및 위협 방지' > '켜기'

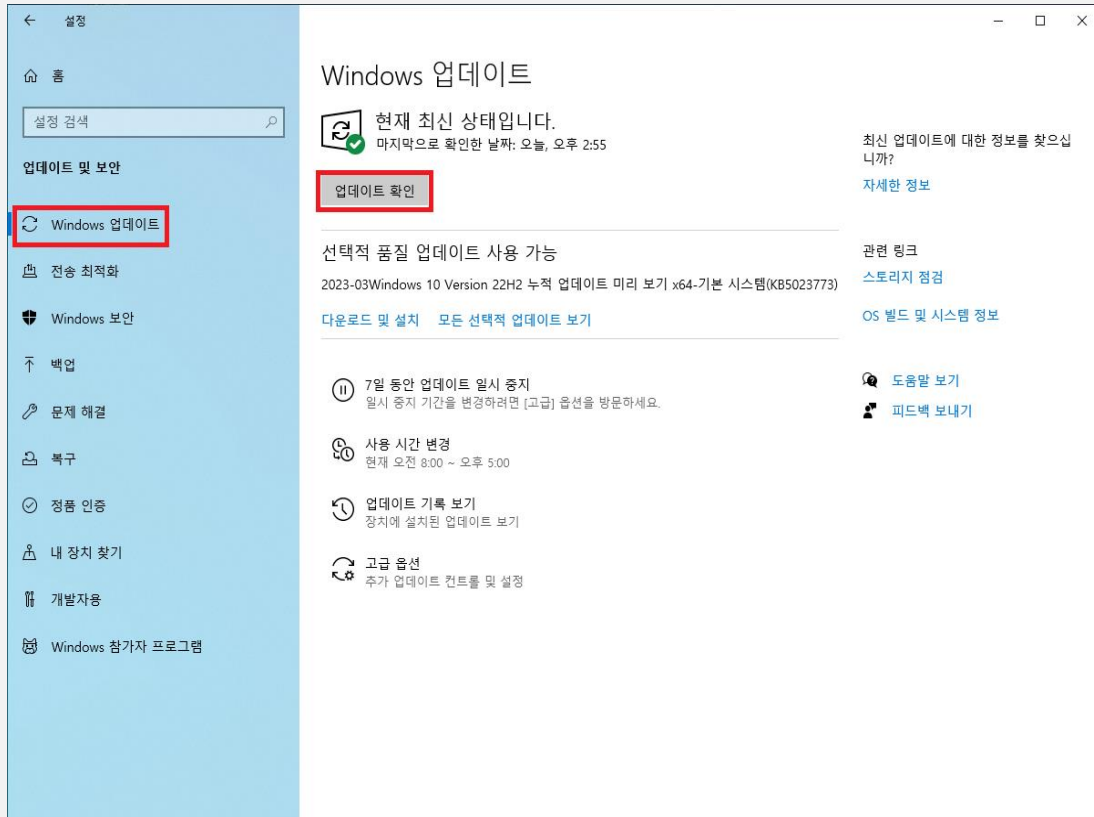
(실시간 보호 기능이 활성화 되어 있는 경우 해당 버튼 안 보임)

- ② '바이러스 및 위협 방지' > '설정 관리' > '실시간 보호' > '켄' 으로 설정

※ 해당 기관 환경에 맞는 백신 프로그램 사용 권고

5-3. OS 최신 보안 업데이트

주기적으로 최신 보안 업데이트 확인 및 업데이트 실행 권고



(위험)

- Hot Fix 및 최신 보안패치 적용을 시키지 않을 경우, 이미 공개된 취약점을 통하여 비인가자의 시스템 접근 및 관리자 권한 획득이 가능해짐

(권고)

○ 최신 보안 업데이트 권고

- ① 설정 > 업데이트 및 보안 > Windows 업데이트 → '**업데이트 확인**'
- ② 업데이트 확인 후 미 설치된 **HOT FIX, 최신 보안 업데이트 등의 설치**

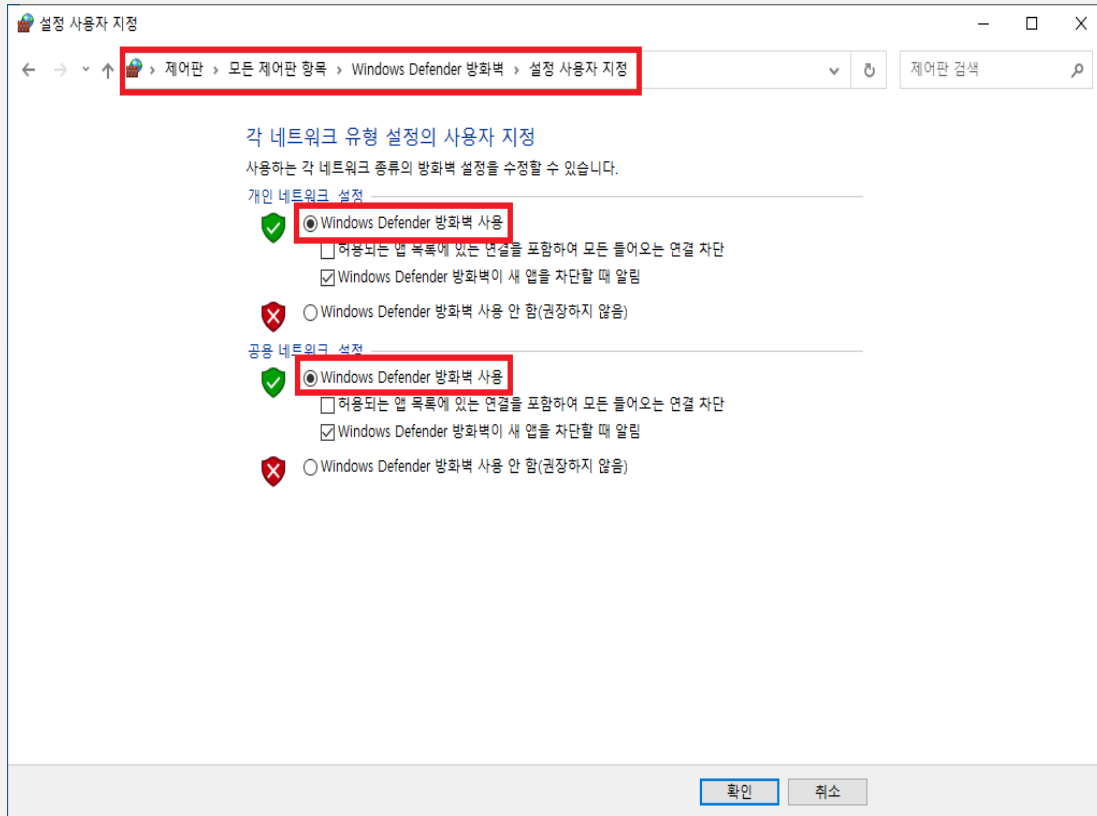
(설명)

○ Hot Fix

- 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련)을 패치하기 위해 배포되는 프로그램

5-4. Windows 방화벽 사용

Windows 방화벽 기능 사용 권고



(위험)

- 방화벽 기능이 비활성화되어 있을 경우, 외부 및 내부의 접근통제가 되지 않아 유해 정보가 유입되거나 시스템 사용자의 파일이나 폴더가 외부로 유출 될 위험이 존재

(권고)

○ Windows 방화벽 사용 권고

- ① 제어판 > Windows 방화벽 > Windows 방화벽 설정 또는 해제
(명령어를 통한 실행 방법: 시작 > 실행 > firewall.cpl 입력)
- ② '**Windows Defender 방화벽 사용**' 설정

(설명)

○ 방화벽

- 외부의 불법 침입으로부터 내부 정보 자산을 보호하고 외부로부터 유해정보 유입을 차단하기 위한 정책과 이를 지원하는 하드웨어와 소프트웨어를 총칭