

운영체제(OS) 기술 지원 종료에 따른 안내

<‘25.6.2(월), 의료정보보호센터>

□ 개요

- 2025년 10월 14일 윈도우(Windows)10의 기술지원 종료와 함께 보안 업데이트 중단
- 이에 종료일 이후 새로운 보안 취약점을 악용한 사이버공격에 대한 사전 대비 필요

□ 주요 내용

- 윈도우즈10을 윈도우즈11 혹은 윈도우즈 상위 버전으로 업그레이드
 - (기한) 2025년 10월 14일까지
 - (기술지원) 마이크로소프트 누리집(<https://support.microsoft.com/ko-kr/windows>)를 통해 윈도우11로 업그레이드 진행

□ 주의 사항

- 업그레이드 조건
 - 사용하는 PC가 윈도우11의 최소 시스템 요구사항을 만족하지 못할 경우, 업그레이드가 어려울 수 있으므로 신규 PC로 교체 필요(필요 시, 마이크로소프트 고객지원 누리집으로 기술지원 요청)
- ※ 윈도우11 최소 시스템 요구사항은 [붙임1] 참조

□ 참고 사항

- 2024년 6월 30일 리눅스 종류인 **CentOS 7**의 단종 및 기술지원이 종료¹⁾ 되었으나 현재까지 미조치 의료기관이 확인되어 조속한 조치 필요
※ 대체 가능한 OS 내역은 [붙임2] 참조

□ 기타

- (출처)
 - <https://www.krcert.or.kr/kr/bbs/view.do?searchCnd=&bbsId=B0000132&searchWrd=&menuNo=205022&pageIndex=1&categoryCode=&nttId=71761>
 - 윈도우10 기술지원 종료와 관련하여 자세한 사항은 한국인터넷진흥원 (☎118 또는 보호나라 누리집), 카카오톡 “보호나라” 채널 챗봇문의, 마이크로소프트(고객지원 누리집)으로 연락하시면 도움을 받으실 수 있습니다.
- (연락처) 의료정보보호센터
 - email : cert@hisac.or.kr - Tel : 02-6360-6280

1) 기술지원이 종료된다는 것은 새로 발견되는 보안 취약점에 대한 보안 업데이트가 중단됨을 의미

붙임1

윈도우11 최소 시스템 요구사항

○ 윈도우10 Vs. 윈도우11 최소 요구 사양 비교

| 구분 | 윈도우10 | 윈도우11 |
|---------------|-----------------|-----------------------------------------------------------------|
| 중앙처리장치(CPU) | 1GHz, 1개 이상의 코어 | 1GHz, 2개 이상의 코어 |
| 메모리(RAM) | 1GB | 4GB |
| 저장공간(HDD,SSD) | 16GB | 64GB |
| 보안 기능 | 별도 요구사항 없음 | TPM*(Trusted Platform Module) 필수 * 비밀번호, 인증서 등을 저장하는 보안 전용 칩 |

- PC가 요구사항을 충족하는지 확실하지 않을 경우 PC OEM(주문자 상표 부착 방식) 구매처에 문의하거나, 해당 PC에서 윈도우10을 이미 사용 중이면 마이크로소프트에서 제공하는 PC 상태 검사 앱을 사용하여 호환성을 확인 가능

* <https://www.microsoft.com/windows/windows-11#pchealthcheck>

붙임2

CentOS 7과 호환되는 리눅스 버전

○ Rocky8~9, RHEL7로 변경 및 교체 권고

- 무료 버전 Rocky²8 혹은 Rocky9(2032년까지 지원) 운영체제로 변경하거나 유료 버전인 RHEL³7버전으로 교체 권고

※ Rocky, RHEL 리눅스는 개발 시 같은 코드체계를 사용하여 호환성과 안정성이 뛰어남

- OS 변경 설치 시 既 서버 환경 파악 및 백업 필요, 既 설치된 어플리케이션과 신규 OS의 호환성을 확인하기 위해 테스트 장비에서 설치 및 정상동작 확인 후, 본 장비에 설치 권고

2) Rocky Linux는 CentOS의 대안으로 만들어진 RHEL 호환 배포판으로, CentOS 창립자인 Gregory Kurtzer 주도하여 개발 이름 "Rocky"는 CentOS 공동 창립자였던 "Rocky McGaugh" 이름을 따서 명명함

3) Red Hat Enterprise Linux로 Red Hat社의 상용리눅스로 기업환경에서 안정성과 보안, 기술 지원 중시

< 윈도우 10 지원 종료 대응 메뉴얼 >

■ 개요

- 마이크로소프트에서는 2025년 10월 14일부로 윈도우(Windows)10의 기술 지원 종료를 발표하였습니다. 이에 따라, 윈도우 10 운영 체제를 사용하는 PC는 공식적인 보안 업데이트와 기술 지원이 중단됩니다.
- 이에, [윈도우 10]을 [윈도우 11]로 업그레이드하여야 하며, 윈도우 업그레이드가 불가능한 경우, 기업용 백신 프로그램을 운용하여 보안을 강화하고 추후에 윈도우 11로 대체하십시오

■ 주요 내용

- 윈도우 10 기술 지원 종료일에 따라, 상위 버전으로 업그레이드
 - (기한) 2025년 10월 14일까지
 - **[붙임2]** 윈도우 11 설치 방법을 참조하여 업그레이드 진행

■ 주의 사항

- 윈도우 11 최소 시스템 요구 사항 점검
 - PC 상태 검사를 통하여 PC가 업그레이드 할 수 있는지 확인이 필요함.
 - ※ PC 상태 검사 바로가기 (**[붙임1]** 윈도우11 최소 시스템 요구사항 참조)
- 윈도우 11 업그레이드 불가 시, 백신 사용
 - 사용하는 PC가 윈도우 11의 최소 시스템 요구 사항을 충족하지 못할 경우에는 업그레이드가 불가하기에, **신규 PC로 교체** 혹은 **백신 프로그램을 사용**해야 보안유지 및 개인정보보호법을 준수함.
 - ※ 단, 기업용 백신으로 사용 (무료 알약 및 V3을 회사에서 운용할 경우 불법)

■ 기타

- 출처
 - [한국인터넷진흥원\(공지 - PC 운영체제 윈도우10 기술지원 종료 안내\)](#)

[붙임1]

윈도우 10, 윈도우 11 최소 PC 요구사항

| 구분 | 윈도우10 | 윈도우11 |
|---------------|-----------------|-----------------------------------------------------------------|
| 중앙처리장치(CPU) | 1GHz, 1개 이상의 코어 | 1GHz, 2개 이상의 코어 |
| 메모리(RAM) | 1GB | 4GB |
| 저장공간(HDD,SSD) | 16GB | 64GB |
| 보안 기능 | 별도 요구사항 없음 | TPM*(Trusted Platform Module) 필수 * 비밀번호, 인증서 등을 저장하는 보안 전용 칩 |

- 1) CPU : 1GHz 이상, 2개 이상의 코어를 갖춘 호환되는 64비트 프로세서 또는 시스템 온 칩(SoC)
- 2) RAM : 4GB 이상의 RAM
- 3) HDD/SSD : 64GB 이상의 저장 공간 (업데이트와 앱을 설치하기 위해 필요한 추가 공간이 있을 수 있음)
- 4) 보안기능(TPM) : TPM 2.0은 하드웨어 기반 보안을 제공하며, 윈도우 11에서 필수로 요구됨
※ TPM 확인 방법 : [Win + R] → [tpm.msc 입력 Enter] → [TPM 확인]

[붙임2]

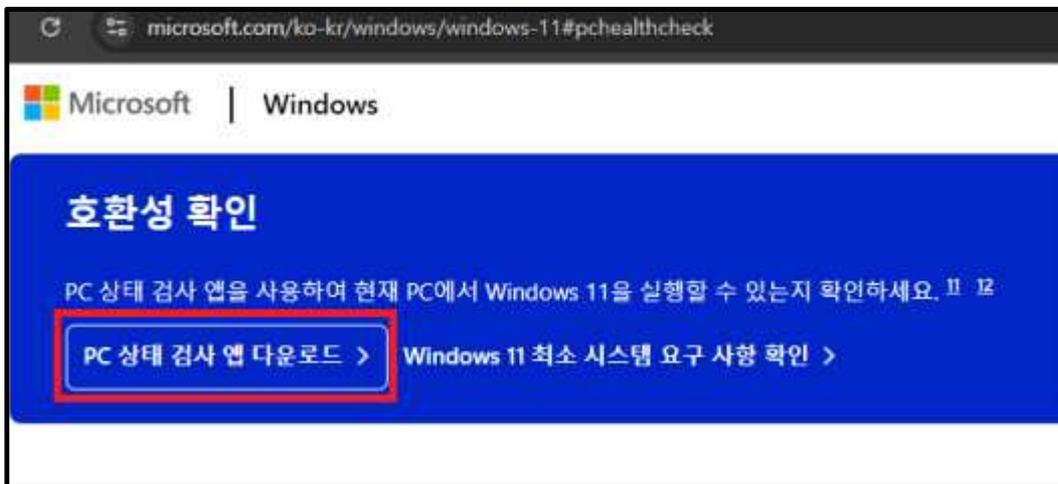
윈도우 11 설치 방법

■ [1단계] 윈도우 운영체제(OS) 확인

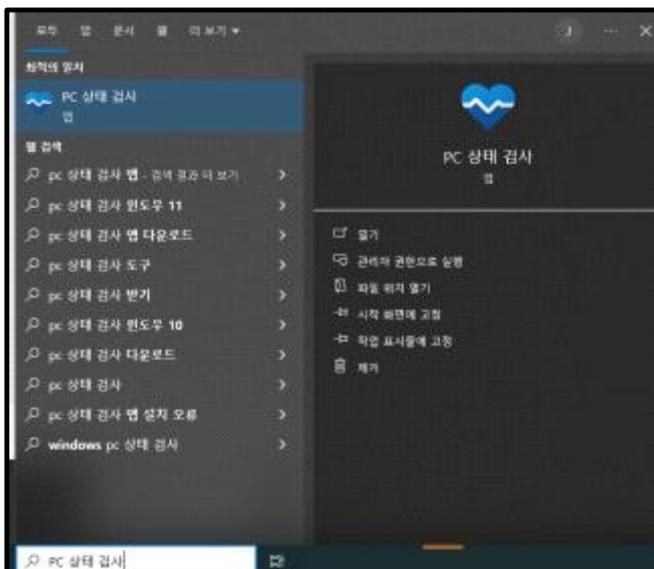
- 1) [바탕화면 or 파일] → [내 PC or 내 컴퓨터] 마우스 오른쪽 클릭 → [속성] 클릭
- 2) Windows 10 이라고 표시되어 있으면 대응 대상입니다.
※ Windows 11이 설치되어 있으면 별도 조치가 필요하지 않습니다.

■ [2단계] 윈도우 11 업그레이드 진행하기

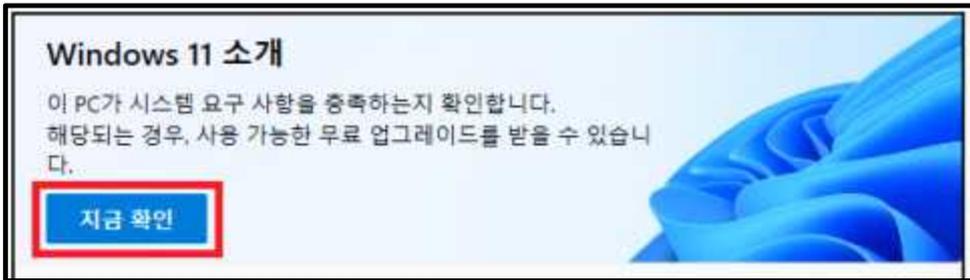
- 1) 마이크로소프트에서 지원하는 '[PC 상태 검사 도구](#)'를 설치합니다.



- 2) 윈도우 검색기에서 [PC 상태 검사]를 입력한 뒤 실행합니다.



3) Windows 11 소개 하단의 [지금 확인]을 클릭합니다.



- 시스템 요구 사항이 충족하는 경우, 업그레이드 진행
- 시스템 요구 사항이 충족하지 않은 경우, 업그레이드 불가 → [3단계 진행]

※ [붙임2] 윈도우11 최소 시스템 요구사항 참조



4) [마이크로소프트 사이트](https://www.microsoft.com/ko-kr/software-download/windows11)를 통하여 윈도우 11 설치 도우미를 [다운로드] 합니다.



5) 윈도우 11 설치 도우미를 [실행] - [수락 및 설치] - 자동 진행



■ [3단계]

1) 윈도우 보안 기능 활용

- Windows Defender (기본 백신) → 켜짐 상태 유지
 - ※ 단. 백신 사용의 경우 꺼짐 상태 유지
- 윈도우 방화벽 : 반드시 켜져 있어야 함
- 윈도우 업데이트 : 최신 업데이트를 유지
 - ※ [붙임3] 윈도우 10·11 보안 업데이트 방법 참조

□ 업그레이드가 불가능한 경우

1) 윈도우 10을 유지할 경우, 백신 프로그램 사용은 필수

- 기업용 백신 프로그램 설치
- 무료 백신이 아닌, 유료 기업용 백신 설치
 - ※ [기업용 V3](#), [알약](#) 등 (클릭 시, 사이트로 이동)
- 백신 자동업데이트 설정 및 유지
 - ※ 백신 사용기한 만료 시, 업데이트가 중단되므로, 정기적인 확인 필요

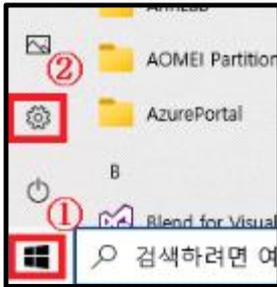
2) 추후 윈도우 11이 탑재된 PC로 교체

[붙임3]

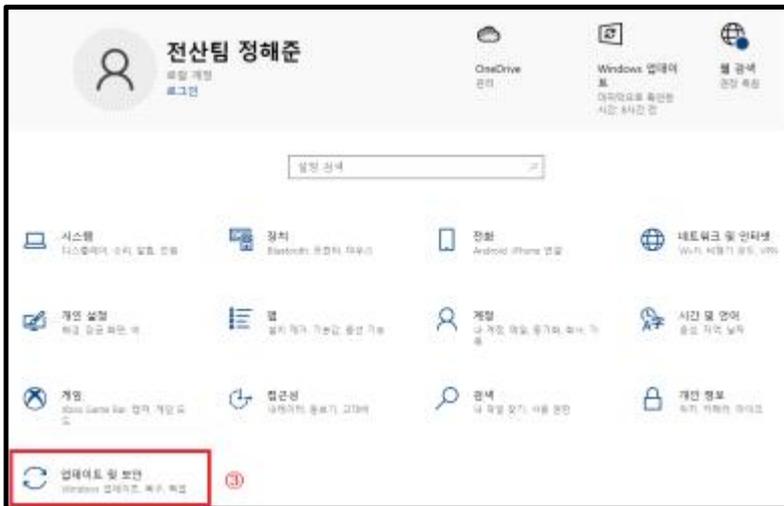
윈도우 10·11 보안 업데이트 방법

■ 윈도우 10

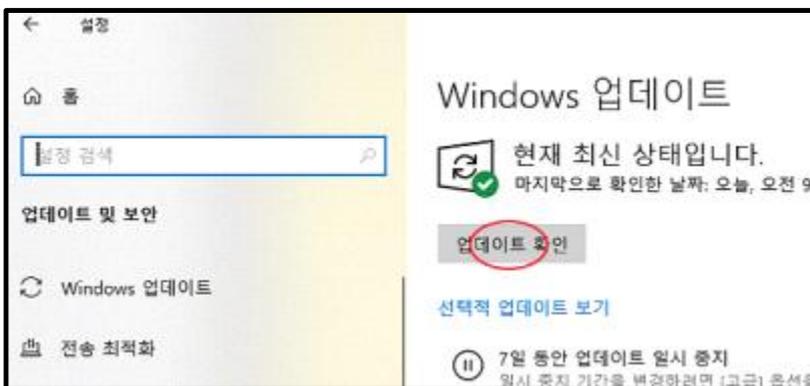
1. 아래 그림과 같이 ①[윈도우 버튼] - ②[설정]을 클릭합니다.



2. ③[업데이트 및 보안]을 클릭합니다.

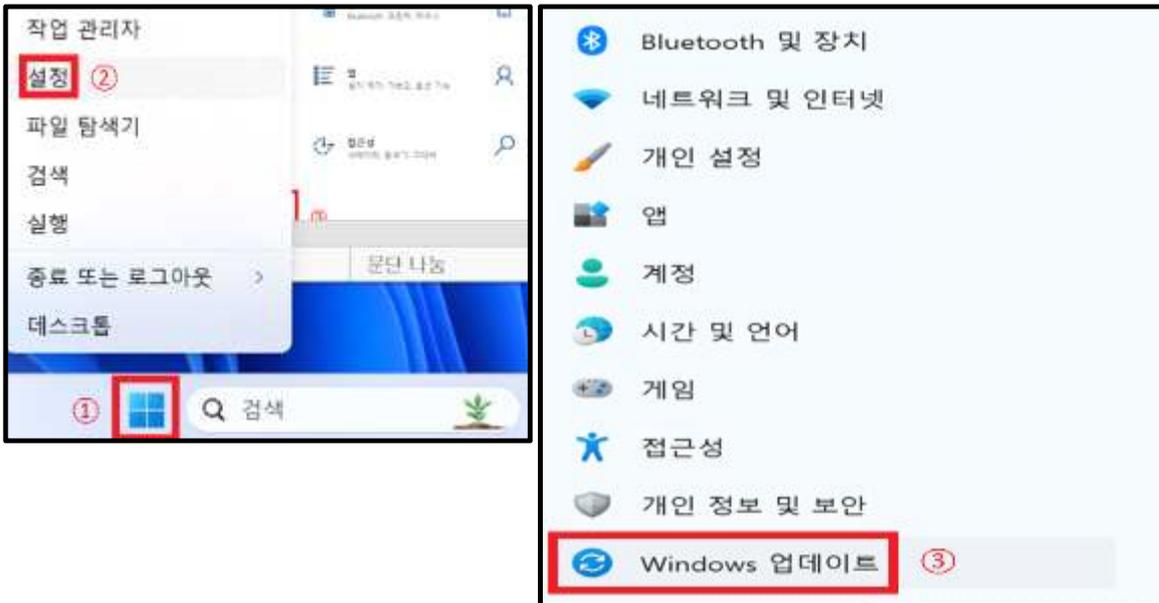


3. ④[Windows 업데이트] 선택 후 ⑤[업데이트 확인]을 클릭합니다.

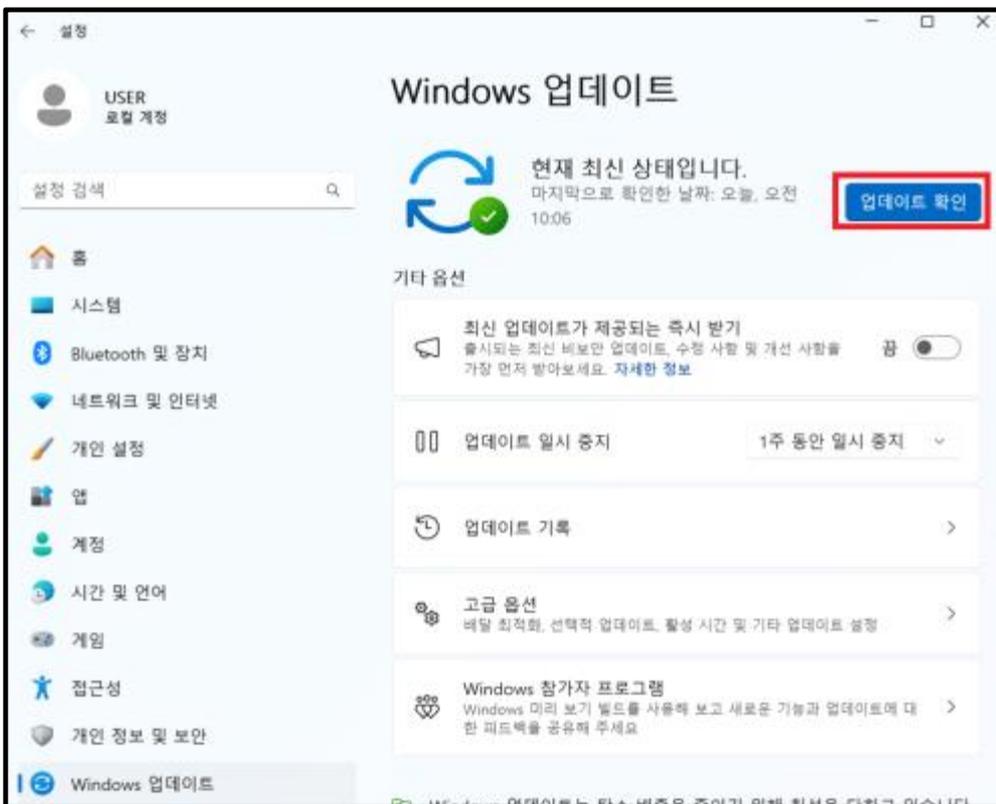


■ 윈도우 11

1. 아래 그림과 같이 ①[윈도우 오른쪽 버튼 클릭] - ②[설정] - ③[Windows 업데이트]를 클릭합니다.

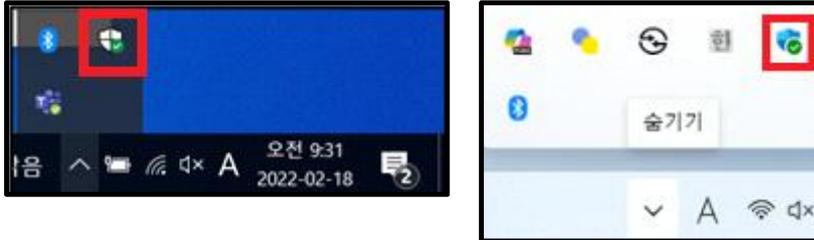


2. ④[업데이트 확인]을 클릭합니다.



윈도우 10·11 보안 간단 설정방법

1. 우측 하단 메뉴바에서 ‘^’ 를 클릭하여 윈도우 보안을 바로 확인하실 수 있습니다. 아래와 같이 보안 아이콘이 녹색, 노란색, 빨간색으로 표시되며 [녹색]으로 설정되어 있어야 윈도우 디펜더가 정상적으로 작동합니다.



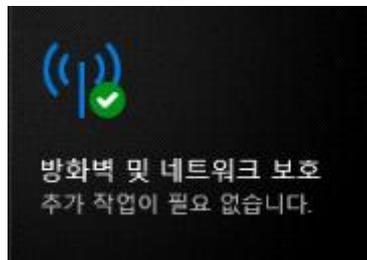
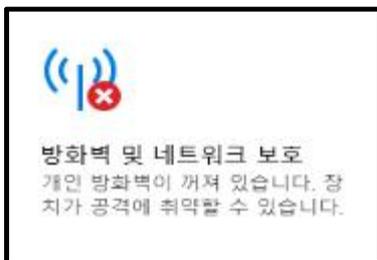
2. 메뉴바에서 확인할 수 없을 경우

  [검색] - “Windows 보안” 검색 - [홈]

- “바이러스 및 위협 방지”, “계정 보호”, “방화벽 및 네트워크 보호”, “앱 및 브라우저 컨트롤”, “장치 보안” 등 녹색블로 유지하여 주시기 바랍니다.



3. 아래와 같이 “X 표시” 혹은 노란색으로 표시되어 있을 경우, 윈도우 보안 권고에 맞게 설정하여 주신 후 녹색블로 표시될 수 있도록 변경하여 주시기 바랍니다.



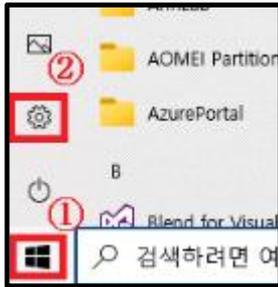
※ 참고링크 : 윈도우 보안 설정의 자세한 사항은 아래 링크를 참고하여 주시기 바랍니다.

- [마이크로소프트 윈도우 보안 설정방법 \(윈도우 11포함\)](#)

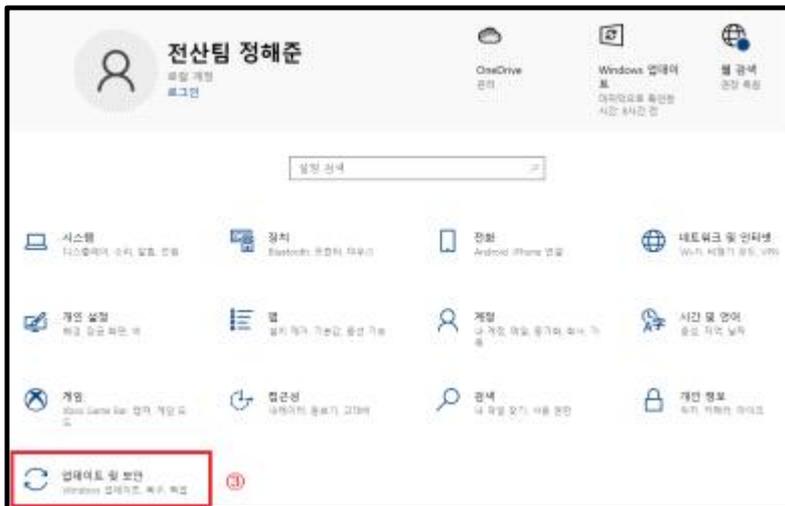
※ 위 방법으로 녹색으로 바뀌지 않을 경우, 윈도우 디펜더 상세 설정방법을 참고하여 주시기 바랍니다.

윈도우 10·11 보안 상세 설정방법

1. 아래 그림과 같이 ①[윈도우 버튼] - ②[설정]을 클릭합니다.



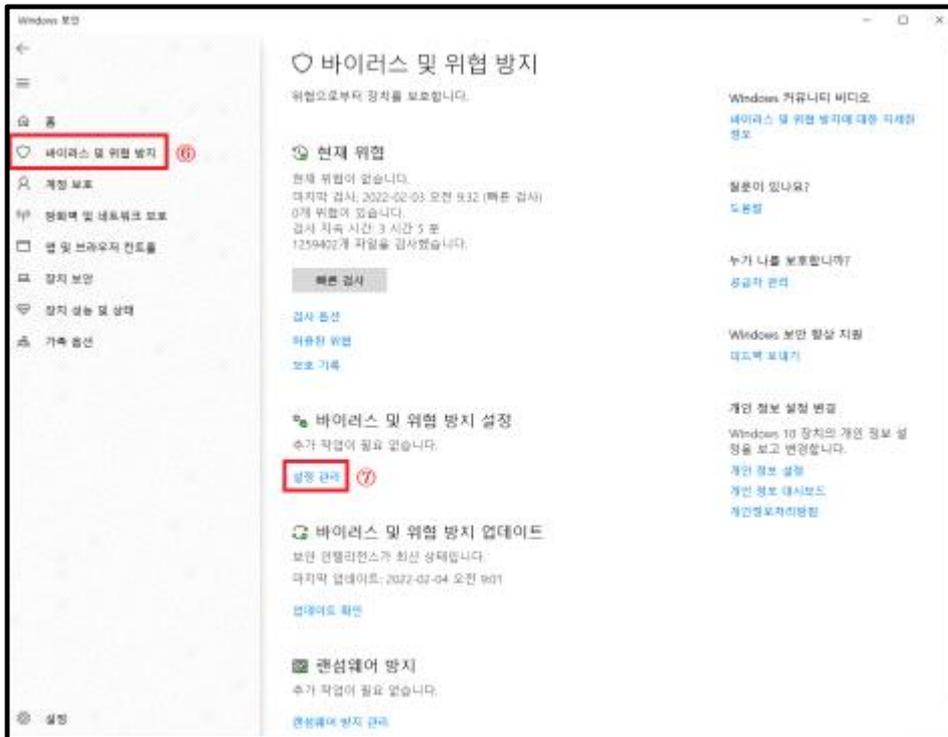
2. ③[업데이트 및 보안]을 클릭합니다.



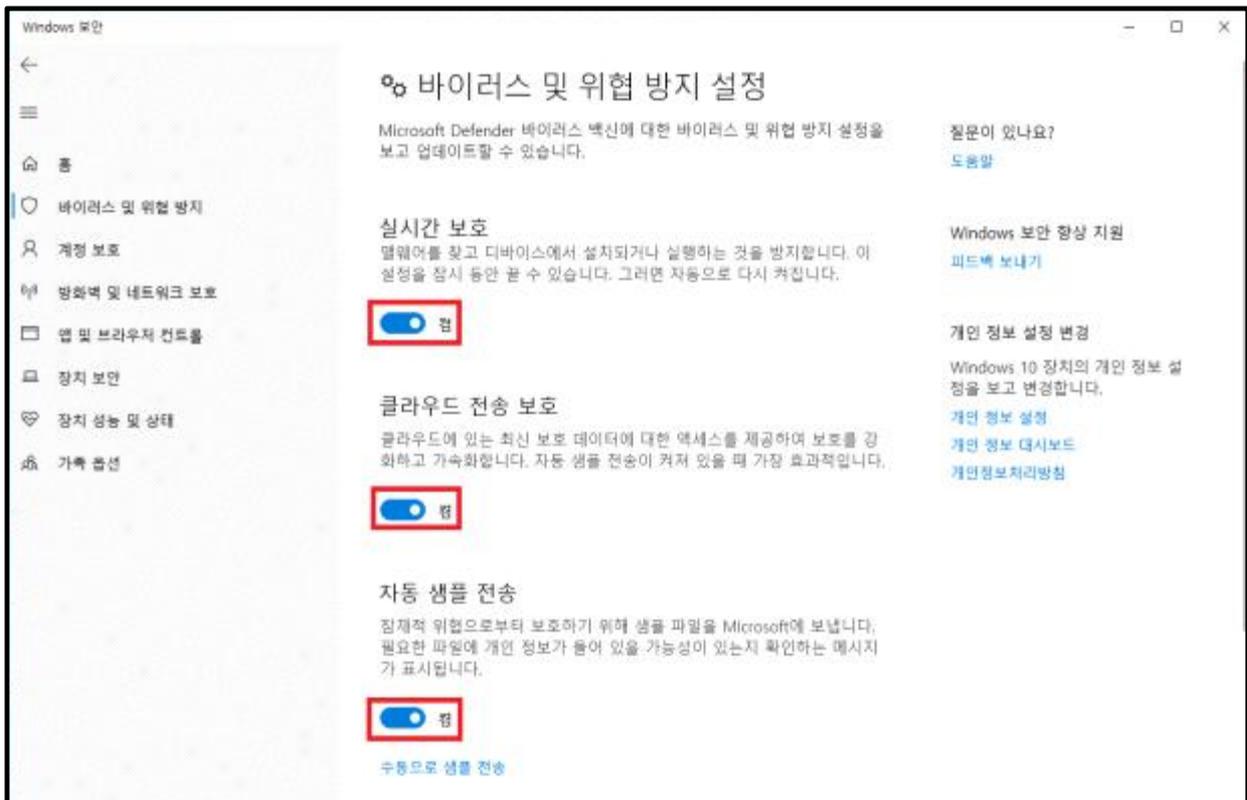
3. ④[Windows 보안] - ⑤[바이러스 및 위협방지]로 이동합니다.



4. ⑥[바이러스 및 위협 방지] - ⑦[설정 관리]로 이동합니다.



5. ⑧[실시간 보호], [클라우드 전송 보호], [자동 샘플 전송]를 모두 '켄'상태로 설정합니다.



6. ⑨[바이러스 및 위협 방지 업데이트]를 최신 상태로 업데이트 합니다.



5. ⑩[랜섬웨어 방지 관리] - ⑪[제어된 폴더 액세스]를 '켄'상태로 설정합니다.



6. ⑫[방화벽 및 네트워크 보호] - ⑬[도메인, 개인, 공용 네트워크]를 클릭하여 ⑭[Microsoft Defender 방화벽]을 '켄' 상태로 설정합니다.



3가지 모두 Microsoft Defender 방화벽을 '켄' 상태로 설정해주시기 바랍니다.

