내 PC지키미 사용자 매뉴얼

Version 1.0

목차

1. 개요

본 문서는 “내 pc 지키미 V1.0” 제품에 대한 매뉴얼이다. 본 문서는 “내 pc 지키미 V1.0” 제품을 사용하는 고객을 그 대상으로 한다. 본 문서에서 모든 내용은 “Microsoft Windows 7”에서 작성되었으며 사용자의 운영 체제에 따라 용어와 그림에 약간의 차이가 있을 수 있다.

2. 설치하기

2.1. 내 PC 지키미 클라이언트 권장 사양

내 PC 지키미 클라이언트 설치와 정상적인 동작을 위해서 시스템은 다음 사양을 만족해야 한다.

운영체제

- Microsoft Windows XP (SP2 이상) 이상
- Microsoft Windows Server 2003 (SP1 이상) 이상

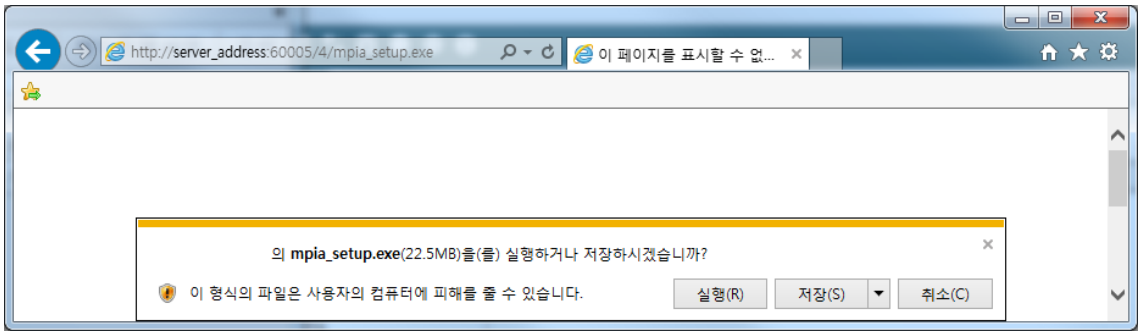
2.2. 내 PC 지키미 설치하기

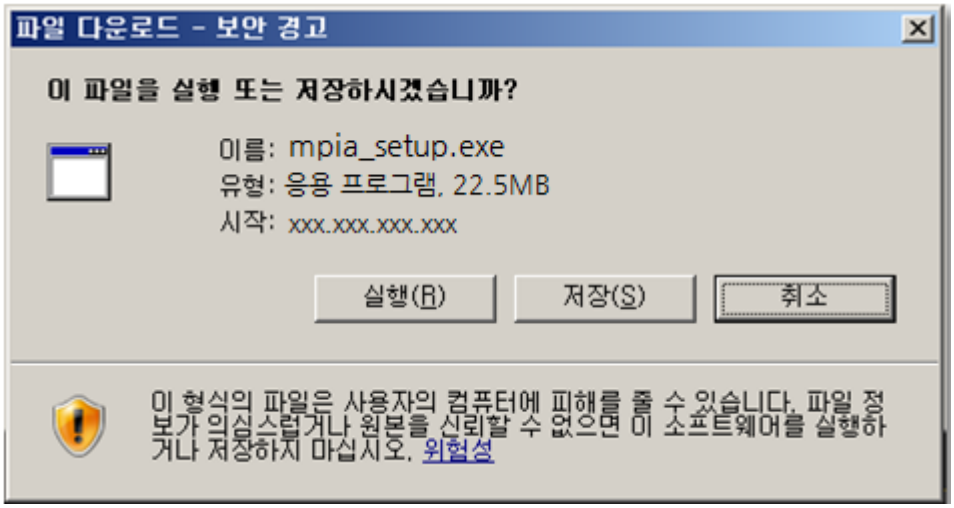
“내 pc 지키미” 클라이언트를 설치하는 방법은 아래와 같다.

Step 1 .

내 PC 지키미 다운로드 페이지에서 파일 다운받기

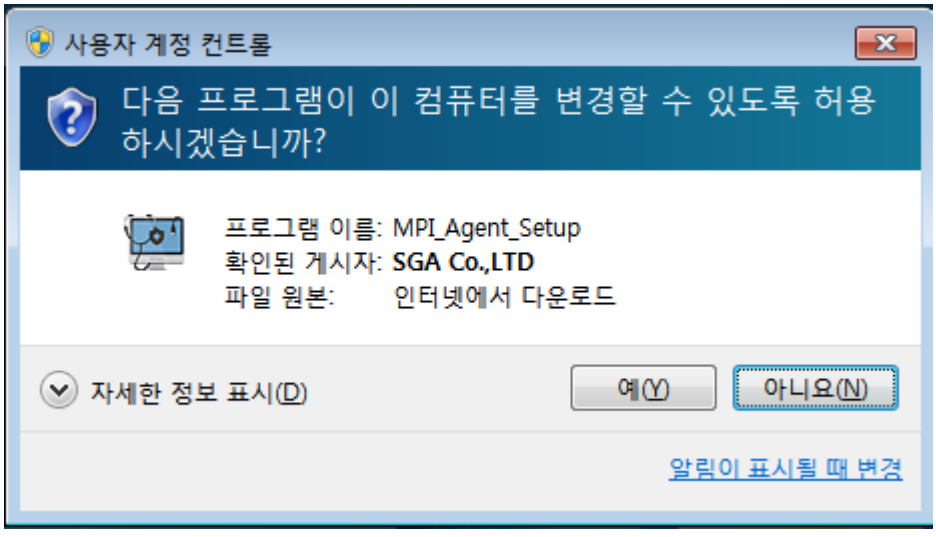
관리자가 제공한 주소를 웹브라우져 주소창에 붙여 넣기하여 파일을 다운로드 받는다. 보안경고 창이 나타나면 저장이나 실행을 클릭한다.(네트워크가 불안정하거나 느린 경우엔 저장 후, 실행을 권장한다.





[그림 2.22-1] 내 PC 지키미 다운로드

다운받은 파일을 실행시, 다음의 경고창이 또 나타난다. 이는 윈도우 시스템에서 실행파일을 실행 시, 발생하는 창으로 "실행"을 클릭하여 설치를 진행한다.



[그림 2.22-2] 내 PC 지키미 실행

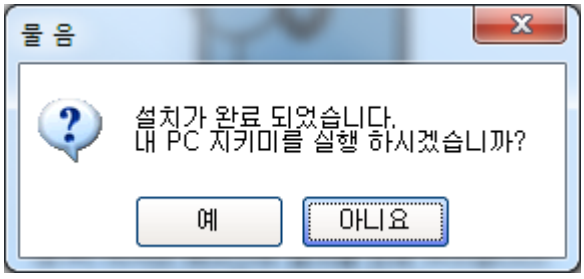
Step 2 .

실행을 확인하면, 내 PC 지키미의 설치가 시작된다. 최초 설치 시, 시스템에 따라 1~2 분의 지연이 발생할 수 있으며, 설치과정은 수초 / 수분 내에 완료되며, "[그림 2.2-3] 내 PC 지키미 설치완료" 와 같이 메시지가 출력되면 정상적으로 설치된 것이다.

[그림 2.22-3] 내 PC 지키미 설치완료

Step 3 .

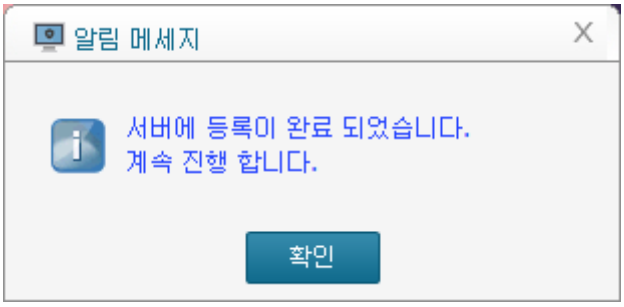
"마침"을 누를 경우 아래와 같은 메시지가 발생되고 내 PC 지키미 실행여부에 대하여 묻는다. 해당 화면에서 아무런 이벤트를 하지 않을 경우 10 초 후 자동 종료된다.



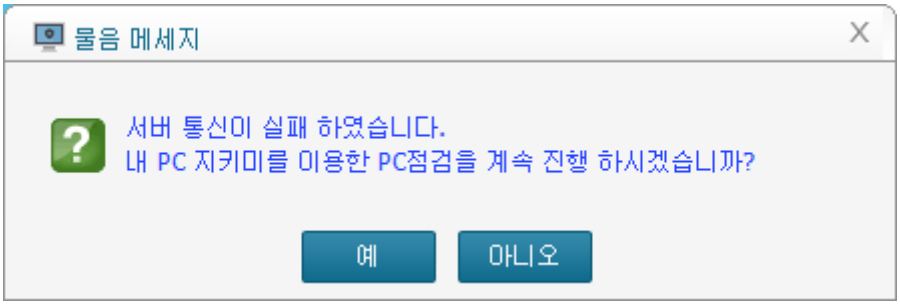
[그림 2.22-4] 설치완료 후 내 PC 지키미 자동실행

Step 4 .

최초 내 PC 지키미 실행시 "[그림 2.2-5] 서버 등록 성공" 과 같은 메시지가 발생한다. 1 회에 한하여 발생된다. 또한 서버에 연결되지 않을 경우엔 "[그림 2.2-6] 서버 연결 실패"와 같은 메시지가 발생되며 자동 종료됩니다. "서버에 연결 할 수 없습니다"의 경우 관리자에게 확인하시기 바랍니다.



[그림 2.22-5] 서버 등록 성공



[그림 2.22-6] 서버 연결 실패

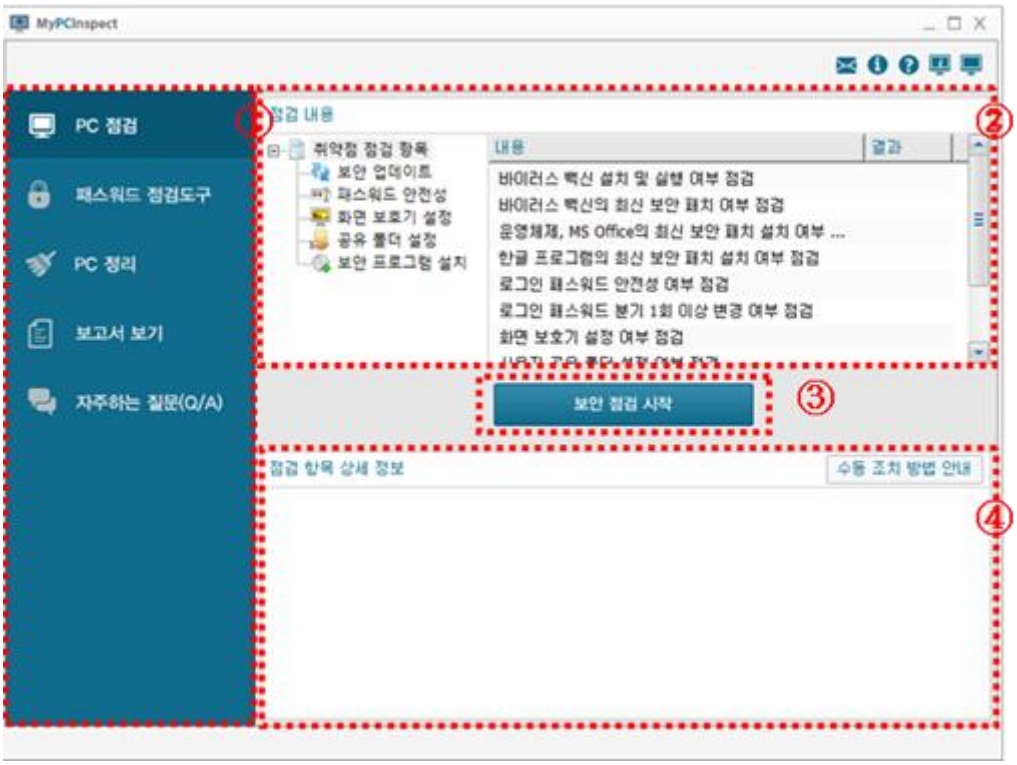
Step 5 .

내 PC 지키미가 실행되면 "[그림 2.2-7] 내 PC 지키미 실행"과 팝업 창이 발생되며 "내 PC 지키미 시작하기"를 통해 검사가 진행된다.

[그림 2.22-7] 내 PC 지키미 실행

Step 6 .

"내 PC 지키미 시작하기" 클릭시 다음과 같은 창이 나타나며 검사를 진행하면 된다.



[그림 2.22-8] 내 PC 지키미 검사하기

항목	내용
1. 메인 메뉴	내PC지키미의 주요기능을 사용할 수 있는 메뉴이다.
2. 점검항목/결과 표시창	각 점검항목과 점검결과를 확인 할 수 있다.
3. 점검시작 버튼	점검 시작 버튼을 통해 점검을 진행 한다.
4. 점검결과/조치방법안내/바로조치	점검 결과에 따른 조치 방법안내와 자동 조치 가능하도록 바로조치기능을 제공한다.

3. 보안 점검

3.1. 보안점검 항목 및 점검내용

내 PC 지키미에서는 다음과 같은 점검기능을 제공한다.

3.1.1 바이러스 백신 설치 및 실행 여부 점검

시스템에 바이러스 백신이 설치되어 있고 현재 실행되고 있는지 점검한다.

3.1.2 바이러스 백신의 최신 보안 패치 여부 점검

바이러스 백신이 실행되어 있고 최신 업데이트 상태를 유지하고 있는지 점검한다.

3.1.3 운영체제, MS Office 의 최신 보안 패치 설치 여부 점검

운영체제(Windows) 및 MS Office 의 보안 패치를 점검하여 최신 보안 업데이트 상태를 유지하고 있는지 점검한다.

3.1.4 한글프로그램의 최신 보안 패치 설치 여부 점검

아래한글 보안 패치를 점검하여 최신 보안 업데이트 상태를 유지하고 있는지 점검한다.

3.1.5 로그인 패스워드 안정성 여부 점검

Windows 로그인 패스워드의 안전성을 점검한다.

3.1.6 로그인 패스워드의 분기 1 회 이상 변경 점검

Windows 로그인 패스워드를 마지막 변경한 후 사용기간이 90 일이 지났는지 점검한다.

3.1.7 화면보호기 설정 여부 점검

화면 보호기 설정 여부를 점검한다.

3.1.8 사용자 공유 폴더 설정 여부 점검

사용자 공유 폴더가 설정되어 있는지 점검한다.

3.1.9 USB 자동 실행 허용 여부 점검

USB 의 자동 실행이 허용되어 있는지 점검한다.

3.1.10 미사용(3 개월) ActiveX 프로그램 존재 여부 점검

3 개월 동안 사용하지 않은 ActiveX 프로그램이 존재하는지 점검한다.

3.1.11 PDF 프로그램의 최신 보안 패치 설치 여부 점검

PDF 프로그램의 최신 보안 패치 설치 여부를 점검한다.

3.1.12 편집 프로그램 (MS Office, 한글, PDF) 설치 여부 점검

편집 프로그램 (MS 워드, 한글, PDF, 엑셀, PPT) 설치 여부를 점검한다.

3.1.13 무선 네트워크 카드 설치 여부 점검

무선 네트워크 카드 설치여부를 점검한다.

3.1.14 보안 USB SW 설치 여부 점검

보안 USB SW 설치 여부를 점검한다.

3.1.15 비인가 프로그램 설치 여부 점검

비인가 프로그램 설치 여부를 점검한다.

3.1.16 프로세스 목록 수집 기능

프로세스 목록 수집을 한다.

3.2. 보안점검 하기

내 PC 지키미에서 제공하는 보안점검 방식은 두가지가 있다.

첫째, 매월 세번째 수요일에 시행되는 사이버보안 진단의 날에 수행되는 것으로 내 PC 지키미가 설치된 단말은 자동으로 수행된다.

둘째, 단말사용자가 수행하는 방식으로 사용자가 원하는 시기에 수행 할 수 있으며, 점검하는 내용은 사이버보안 진단의 날에 수행하는 정책과 동일하게 수행된다.

3.2.1 사이버보안 진단의 날 점검

매월 세번째 수요일이 되면, 단말에 내 PC 지키미가 자동으로 실행되므로 사용자는 사용자는 공지사항 창의 화면 확인을 통해 수행됩니다. 보안점검 시작을 클릭하시면 자동으로 점검을 시작하고, 결과가 관리자에게 자동 전송됩니다.

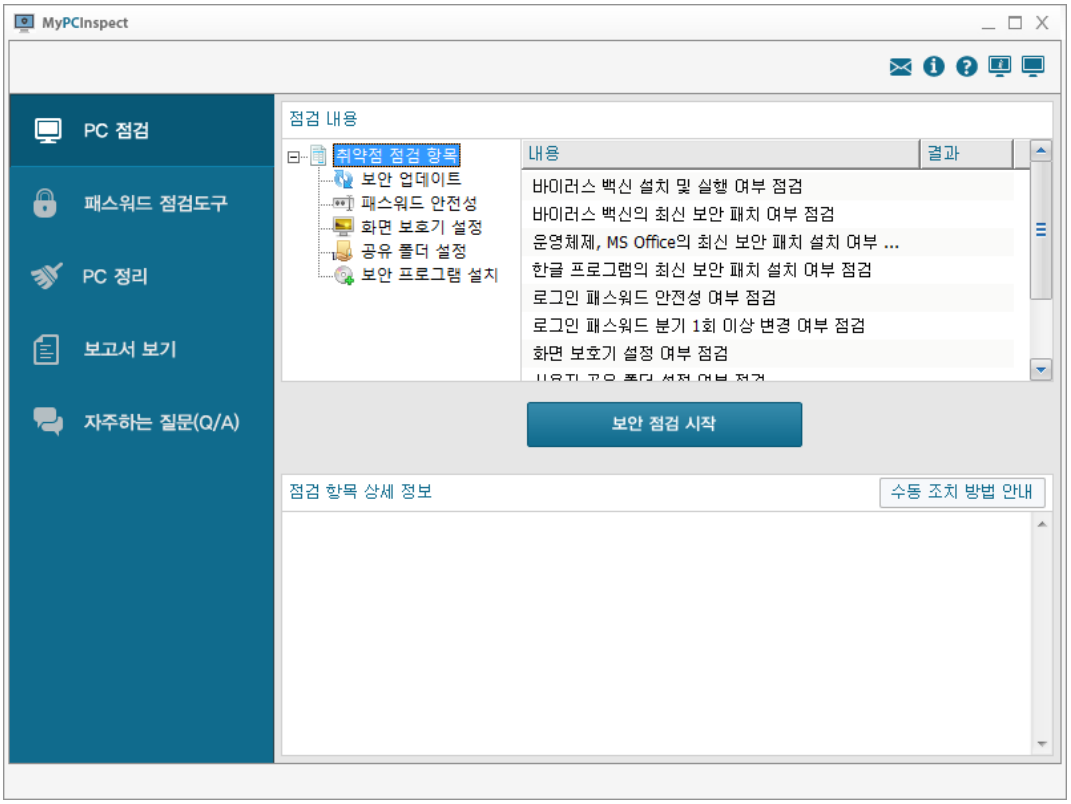
[그림 3.2-1] 내 PC 지키미 점검

3.2.2 사용자 자가 점검

내 PC 지키미는 사용자가 사이버보안 진단의 날과 무관하게 단말의 상태를 점검 할 수 있는 기능을 제공한다.

Step 1 .

바탕화면에 있는 “내 PC 지키미” 아이콘을 더블클릭 하면 다음과 같이 내 PC 지키미 창이 나타난다.

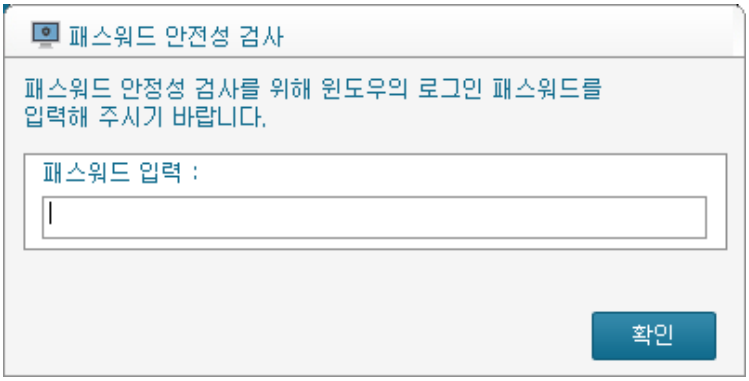


[그림 3.2-2] 내 PC 지키미

Step 2 .

“보안 점검 시작” 버튼을 클릭하면 점검을 시작한다.

◎ 점검 과정 중, 윈도우 로그인 패스워드 점검안내 “[그림 3.2-3]로그인 암호 입력”

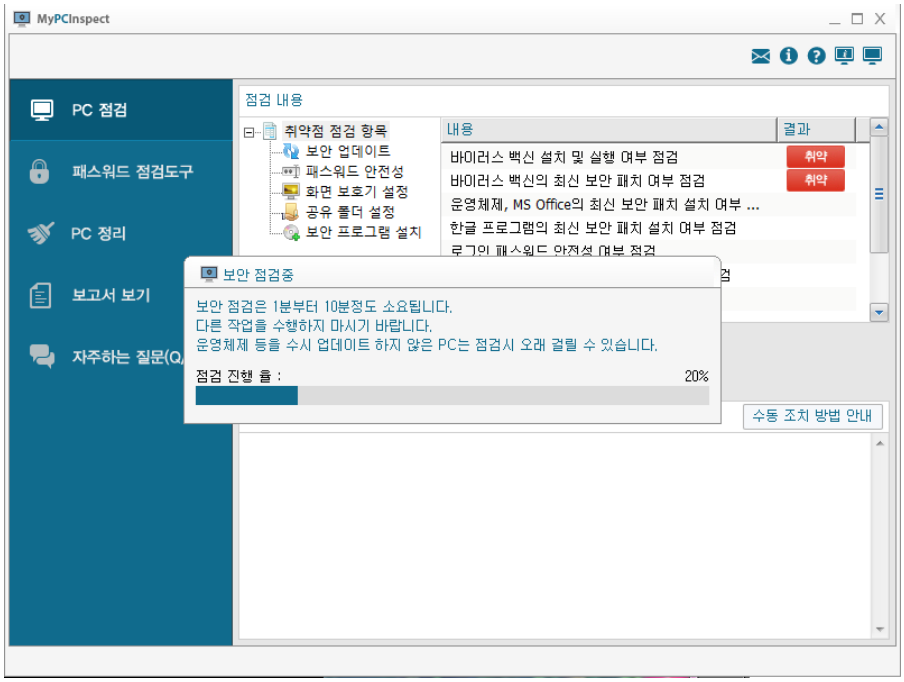


[그림 3.2-3] 로그인 암호 입력

점검이 시작되면, 거의 모든 과정은 자동으로 진행되지만, 사용자의 확인이 필요한 윈도우 로그인 패스워드 점검시엔 윈도우 로그인 패스워드를 정확히 입력해야 한다. 이는 윈도우 로그인 패스워드의 보안등급을 점검하기 위한 과정으로, 아직 패스워드를 설정하지 않으셨다면, 그대로 두고 “확인” 버튼을 클릭하면 된다.

Step 3 .

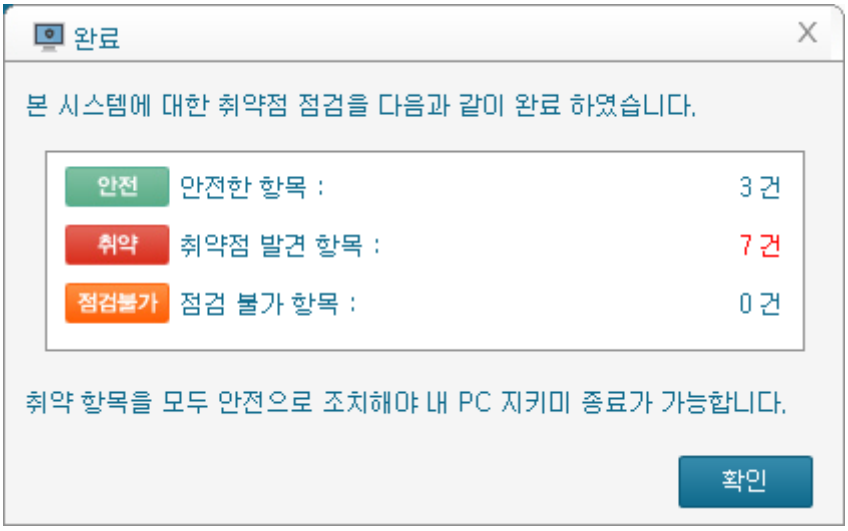
운영체제, MS Office 의 최신보안 패치설치여부를 점검시엔, MS 사의 Update 사이트와 확인하여 점검하므로 업데이트 할 내용이 많거나 네트워크 연결이 원할하지 않을 경우, 다소 지연시간이 발생 할 수 있다.



[그림 3.2-4] 보안 검사 중

Step 4 .

점검이 완료되면 자동으로 중앙관리서버로 전송된다. 전송내역은 메인메뉴의 왼쪽 “보고서보기”에서 확인 할 수 있다.



[그림 3.2-5] 점검 완료 메세지

3.3. 보안점검 결과에 따른 조치하기

보안점검이 완료되면 PC 의 점검 항목에 따른 결과를 확인 할 수 있다.

[그림 3.3-1] 점검 결과

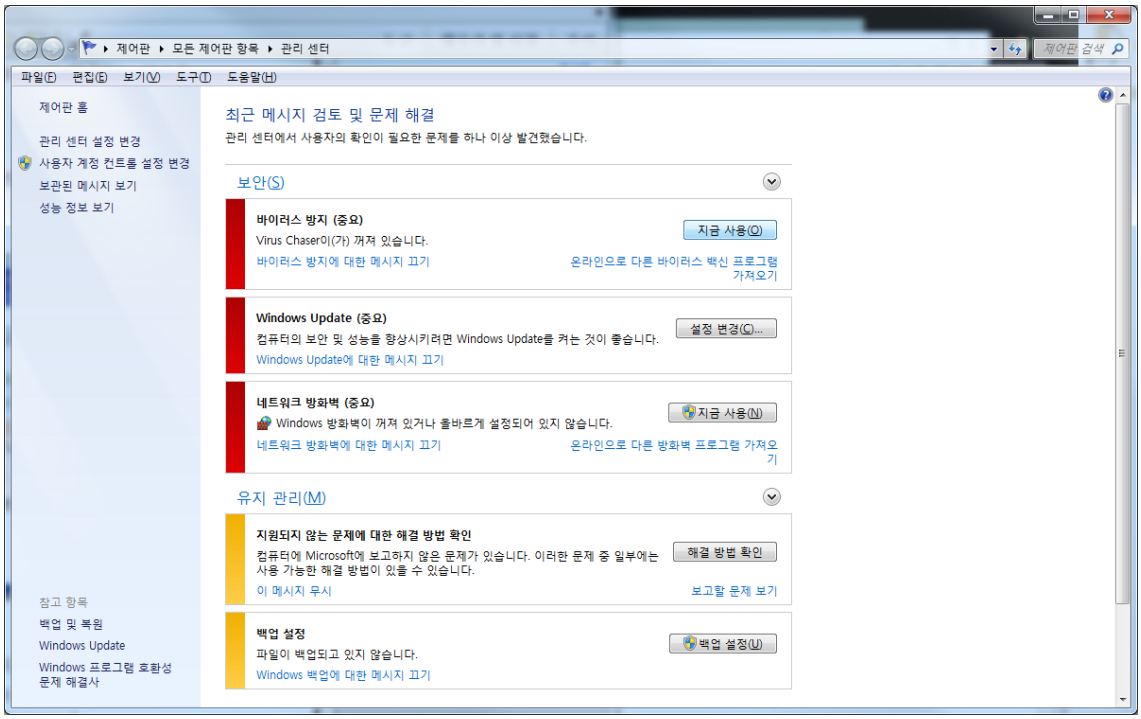
◎ 취약으로 판정된 항목은 결과가 붉은색으로 표시된다.

항목	내용
①	취약으로 결과가 나온 항목을 선택한다.
②	점검결과에 대한 내역을 간략히 확인한다.
③	편의를 위해 1회성의 조치가 가능한 부분은 각 탭의 “버튼”을 통해 제공한다. 조치가 되지않는 부분은 프로그램 상의 조치방법 안내를 확인 하거나, 내PC지키미 프로그램의 상단부의 “기술지원탭”  을 선택하여 지원 받기를 권장한다.
④	조치방법 안내를 통해 상세히 조치하는 방법을 열람 한다.

첫째, 취약으로 결과가 나온 항목을 선택하고, 둘째, 점검 결과에 대한 내역을 간략히 확인한 이후 셋째, 보안점검이 완료되면 P

3.3.1 바이러스 백신 설치 및 실행 여부 점검

바이러스 백신이 설치되어 있지 않거나, 미동작시 “취약”으로 점검된다. 백신이 설치되어 있는 PC 의 경우, “보안센터 실행하기” 버튼을 클릭 Windows 보안센터로 이동하셔서 권장사항버튼을 클릭 하신 후, 조치한다.



[그림 3.3-2] 보안센터 등록

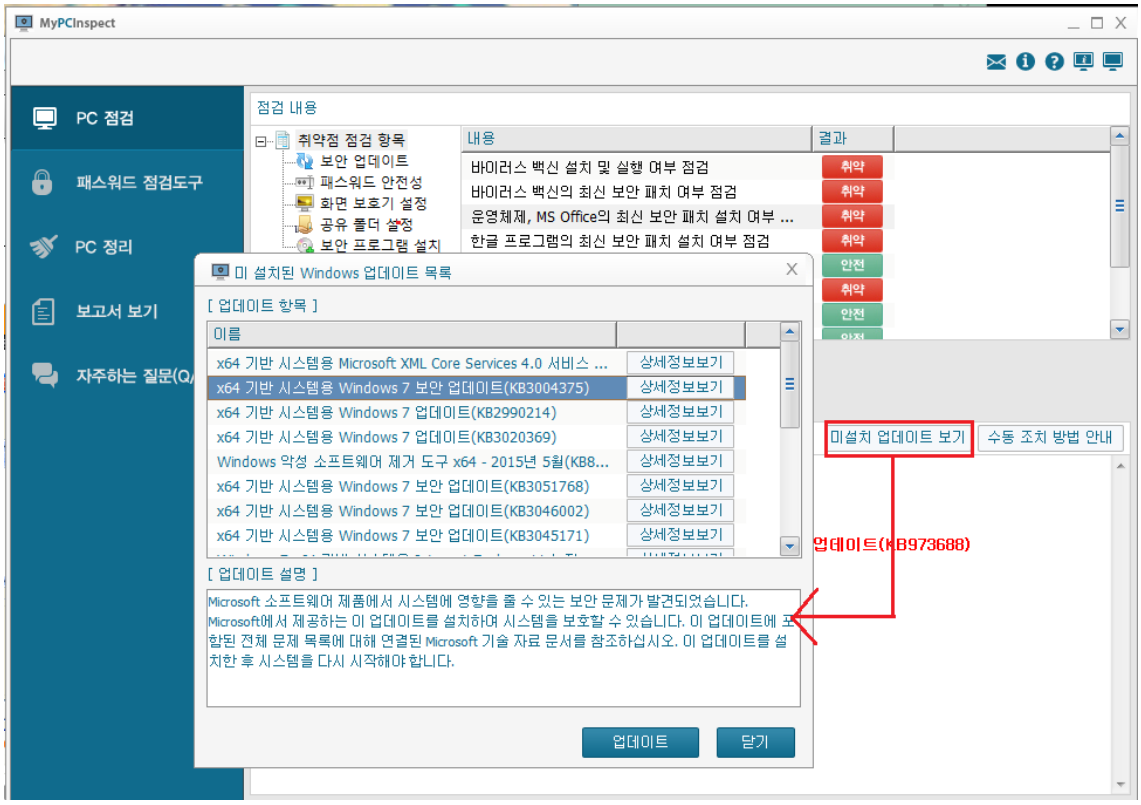
3.3.2 바이러스 백신의 최신 보안 패치 여부 점검

바이러스 백신이 설치되지 않은 단말이거나, 바이러스 백신은 설치 되어 있지만 최신보안 패치가 적용되지 않았을 경우 “취약”으로 점검된다.

[그림 3.3-3] 바이러스 최신 보안패치

3.3.3 운영체제, MS Office 의 최신 보안 패치 설치 여부 점검

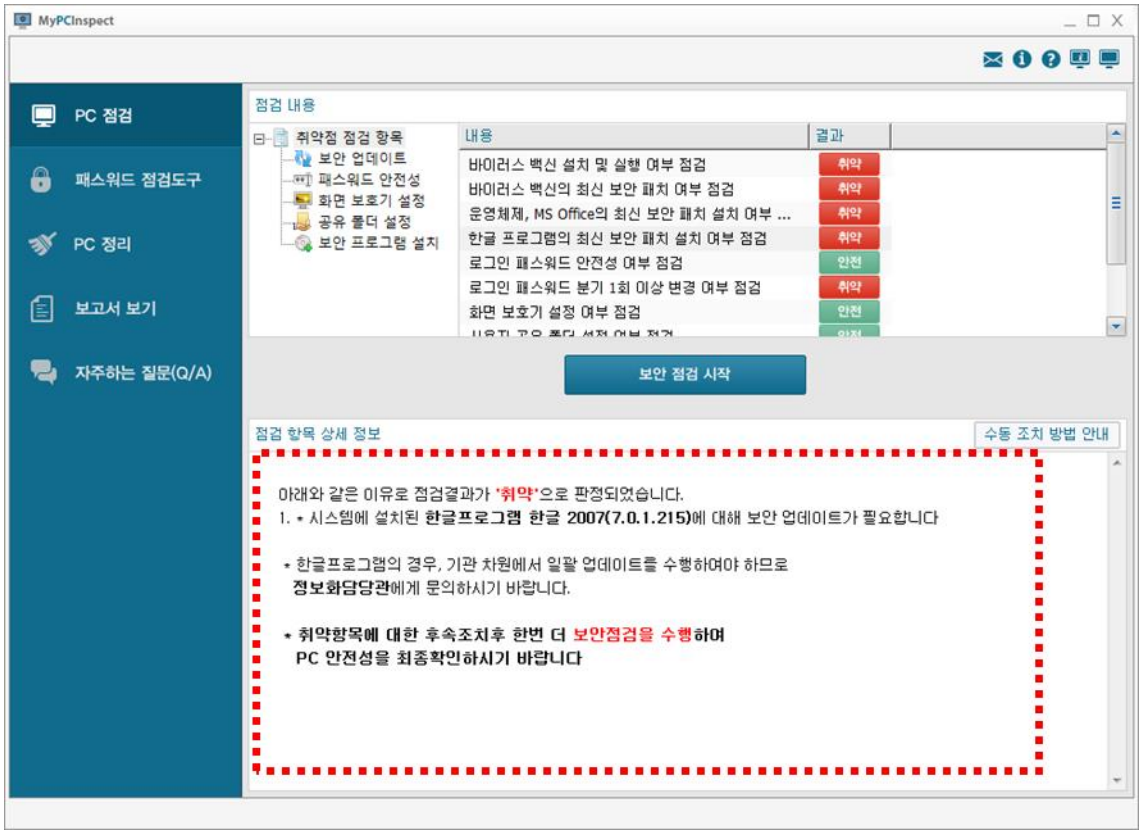
현재사용중인 단말의 운영체제와 MS Office 군 제품에 대한 최신패치적용 여부를 점검하는 기능으로 점검 시, MS 사의 최신 업데이트 정보와 비교하여 누락, 미적용된 패치항목이 있으면 “취약”으로 점검된다.



[그림 3.3-4] 보안패치 점검

3.3.4 한글프로그램의 최신 보안 패치 설치 여부 점검

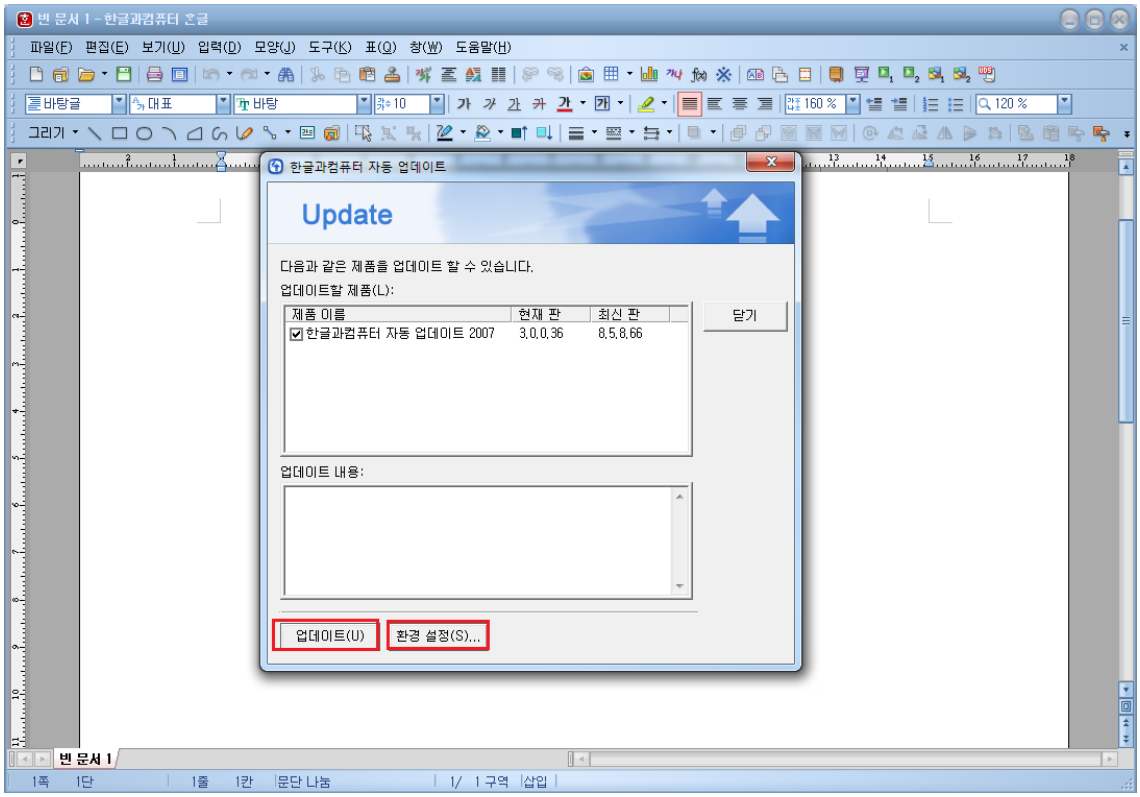
아래한글 제품 군의 최신보안패치 적용여부를 점검하는 기능으로, 아래한글이 설치되지 않은 단말에 대해서는 “점검불가”로 판정되며, 아래한글 제품만 설치하고 보안 패치가 적용되지 않은 단말은 “취약”으로 점검한다.



[그림 3.3-5] 한글 패치 점검

조치 방법 안내에 따라 업데이트를 진행하거나, 아래 한글 제품을 통해서도 업데이트는 진행이 가능하다. (제품자체에서 지원하는 기능이 편리하며, 자동업데이트 설정을 할수 있다)

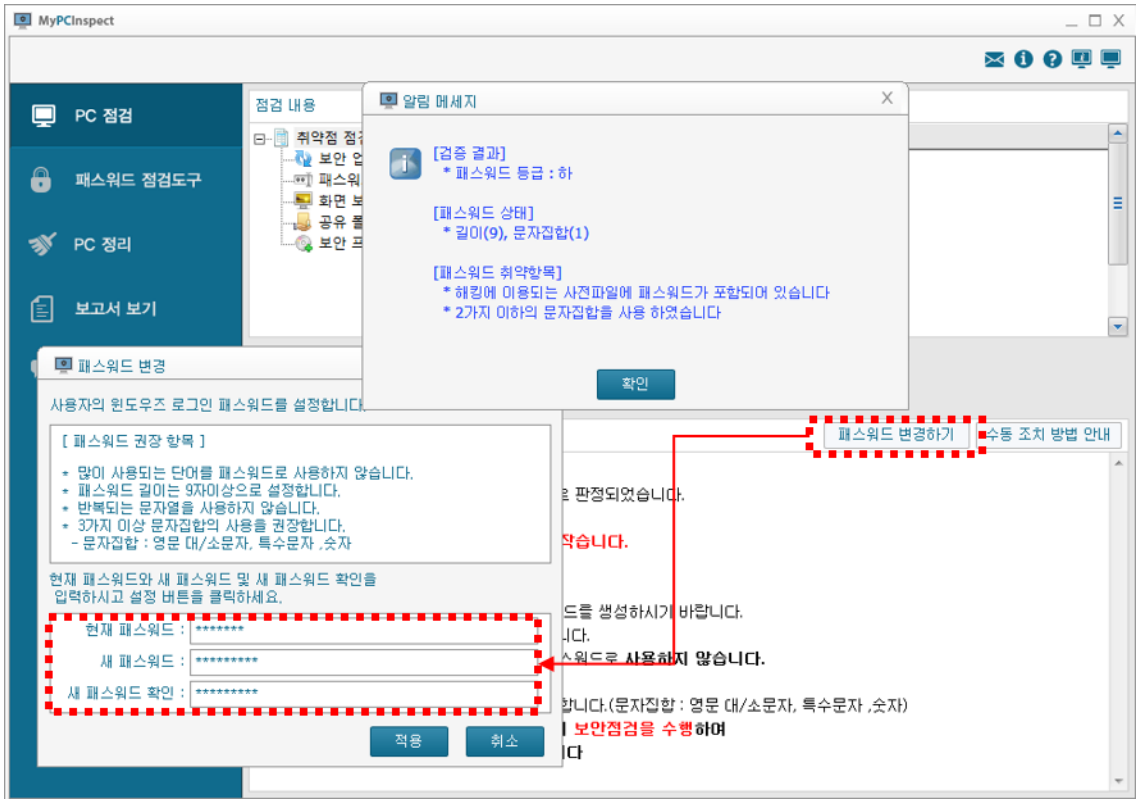
한글 실행 -> 도움말 -> 한컴 자동 업데이트 선택시 아래와 같은 창이 나타납니다. 업데이트 버튼을 클릭하거나, 환경설정에서 자동업데이트 설정을 하면 된다.



[그림 3.3-6] 한글 자동 업데이트

3.3.5 로그인 패스워드 안정성 여부 점검

윈도우 계정의 로그인 패스워드의 안정성을 점검하는 항목으로 패스워드 설정이 안되어 있거나, 보안 수준이 낮은 패스워드를 사용할 때 “취약”으로 점검된다. “패스워드 변경하기” 버튼을 클릭하면 패스워드를 즉시 설정, 변경 할 수 있는 창이 팝업되며 패스워드에 대한 보안 수준 레벨을 즉시 측정하여 설정이 가능하다.



[그림 3.3-7] 로그인 패스워드 안전성

3.3.6 로그인 패스워드의 분기 1 회 이상 변경 점검

로그인 패스워드를 설정한 후, 분기별로 변경하기를 권장하며, 90 일 동안 패스워드를 변경하지 않은 단말에 대하여 “취약”으로 점검된다.

[그림 3.3-8] 로그인 패스워드 분기별 변경

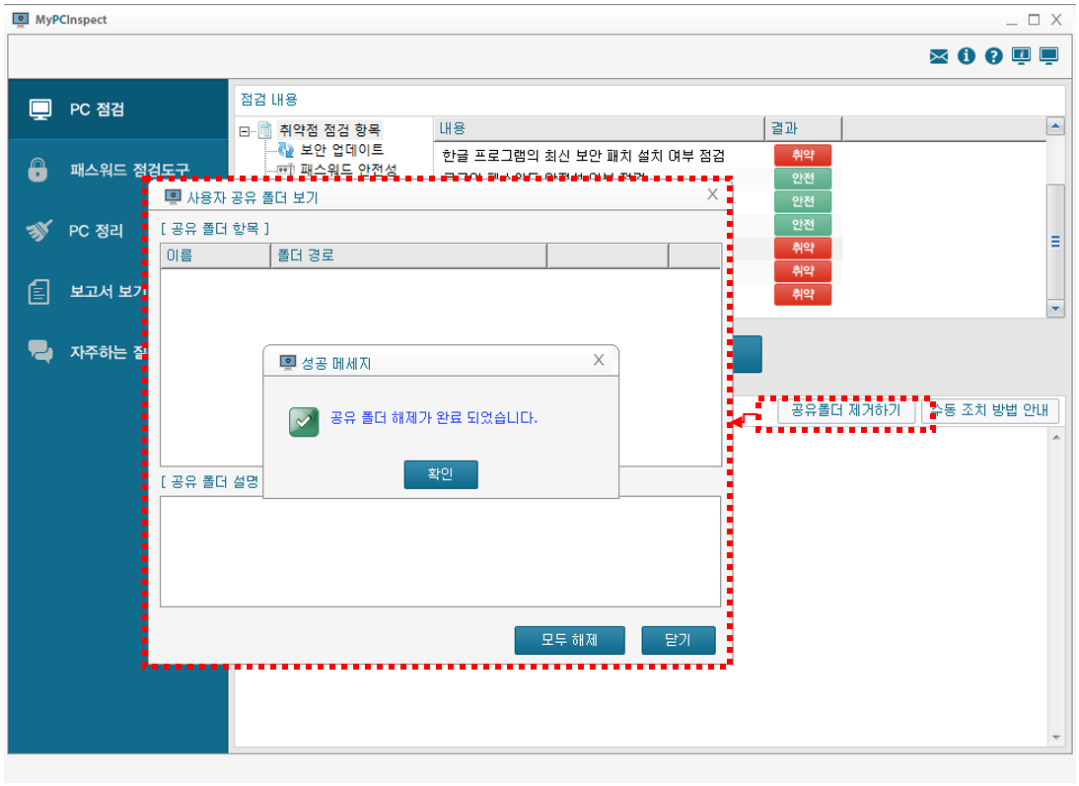
3.3.7 화면보호기 설정 여부 점검

단말에 화면보호기가 설정되어 있는지 여부와 화면보호기를 해제할 때, 암호로 보호되어 있는지 점검하여, 누락된 사항이 있으면 “취약”으로 점검된다. 취약으로 판정된 경우 “화면보호기 설정하기” 버튼을 통해 자동으로 변경한다.

[그림 3.3-9] 화면보호기 설정

3.3.8 사용자 공유 폴더 설정 여부 점검

사용자 단말에 공유설정이 되어있는 폴더 유무를 점검하여, 공유 폴더가 있는 경우, “취약”으로 점검된다. “점검 항목 상세 정보” 란에서 공유된 폴더 내용이 나오며, 조치를 위해 “공유폴더 제거하기”를 클릭하면, 단말내 공유 폴더의 전체목록이 나열되며 공유해제 할 폴더를 선택하거나, 하단 부의 모두 해제 버튼을 눌러 해제한다.



[그림 3.3-10] 사용자 공유 폴더

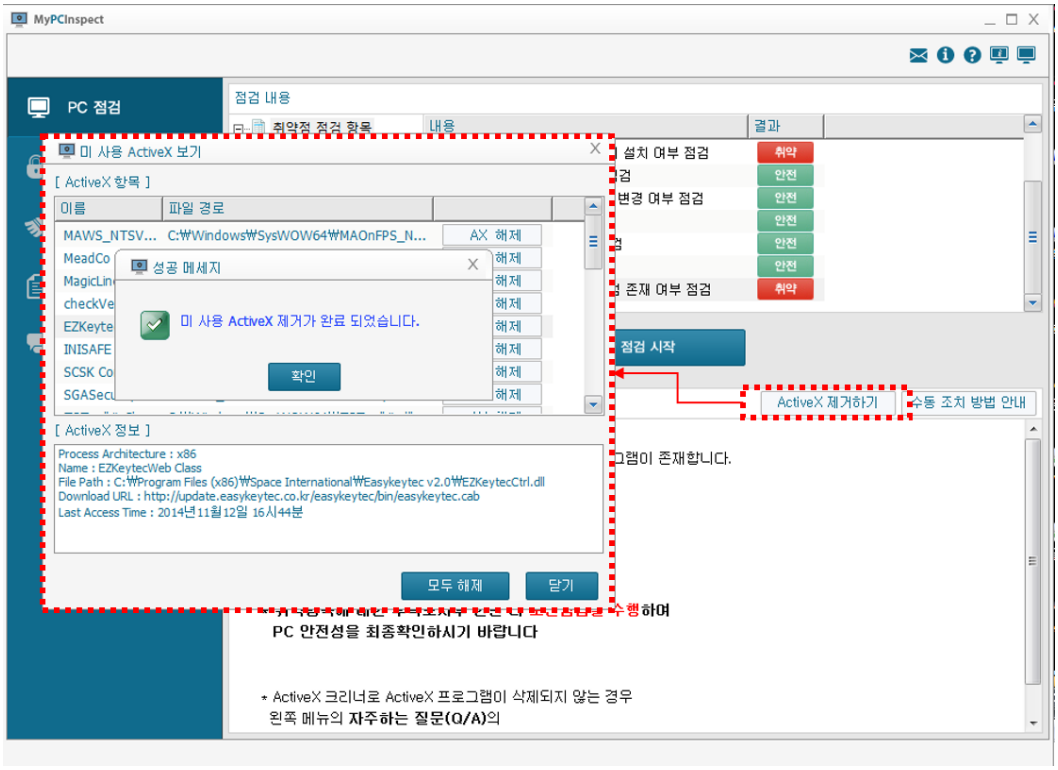
3.3.9 USB 자동 실행 허용 여부 점검

USB 포트를 통해 연결되는 USB 메모리, 휴대기기 등의 자동실행 방지기능이 활성화 여부를 점검하며, 자동실행이 가능한 상태이면 “취약”으로 점검된다. “USB 자동실행 차단” 버튼을 통해 즉시 조치가 가능하다.

[그림 3.3-11] USB 자동 실행 여부

3.3.10 미사용(3 개월) ActiveX 프로그램 존재 여부 점검

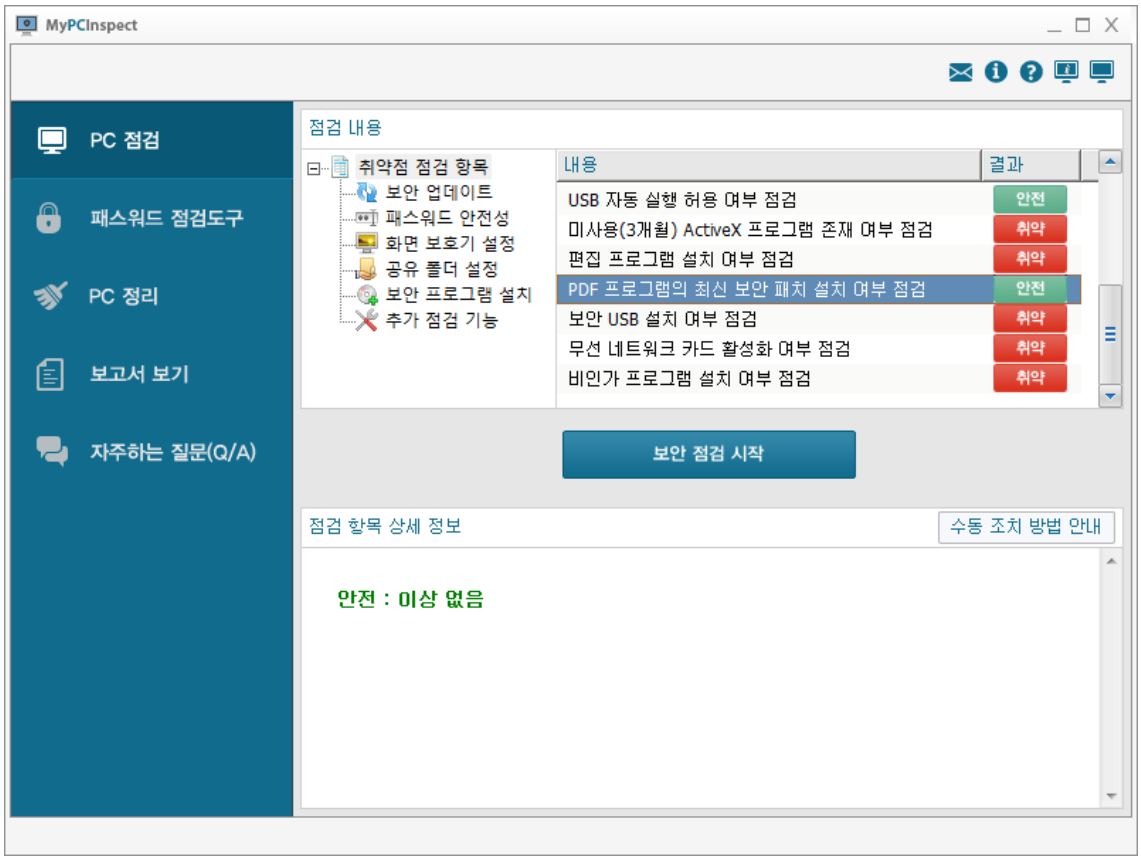
단말의 사용하지 않은지 3 개월이 경과한 ActiveX 에 대한 점검항목이다. 90 일을 기준으로 90 일이 초과된 ActiveX 가 존재하는 경우 “취약”으로 점검된다.
“ActiveX 제거하기” 버튼을 통해 즉시 조치가 가능하다.



[그림 3.3-12] 미사용 ActiveX 프로그램 여부

3.3.11 PDF 프로그램의 최신 보안 패치 설치 여부 점검

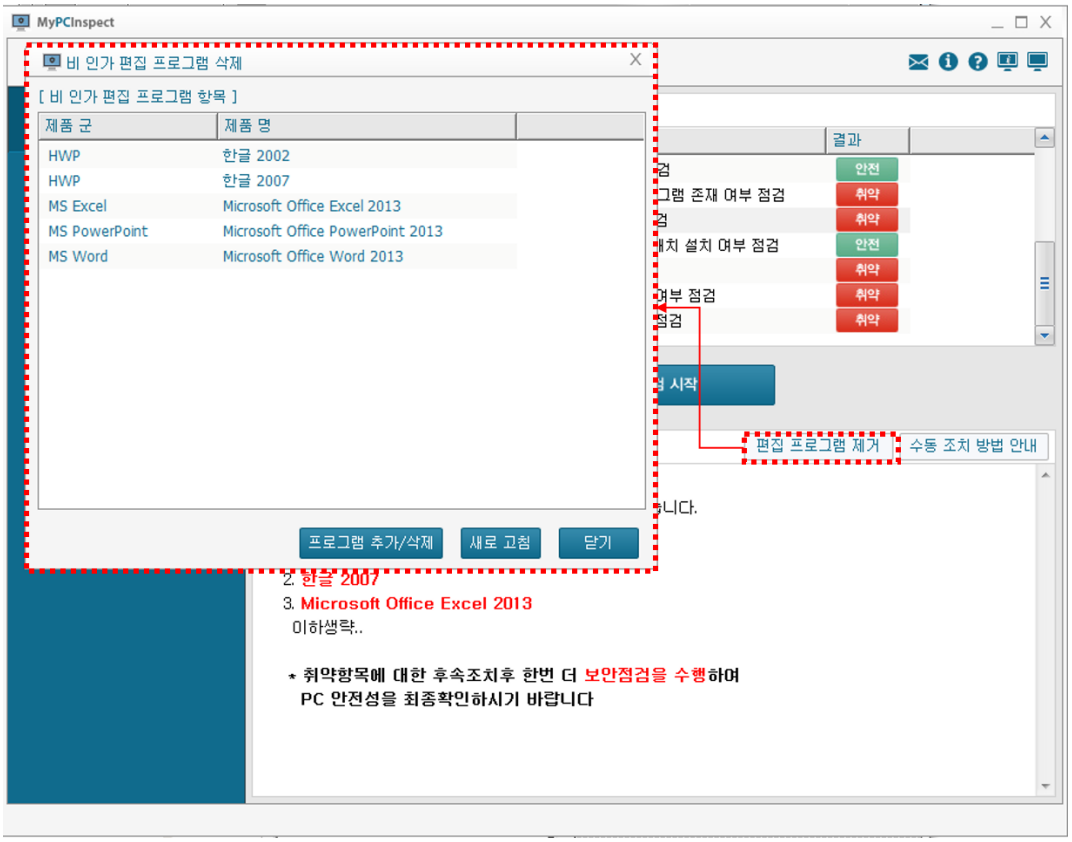
PDF 프로그램에 대한 최신보안 패치 적용여부를 점검하여, 패치가 적용되지 않은 단말에 대해서 “취약”으로 점검된다. (설치하지 않은 단말에 대해서는 안전으로 표시됩니다.)



[그림 3.3-13] PDF 프로그램 보안패치 여부

3.3.12 편집 프로그램 (MS Office, 한글, PDF) 설치 여부 점검

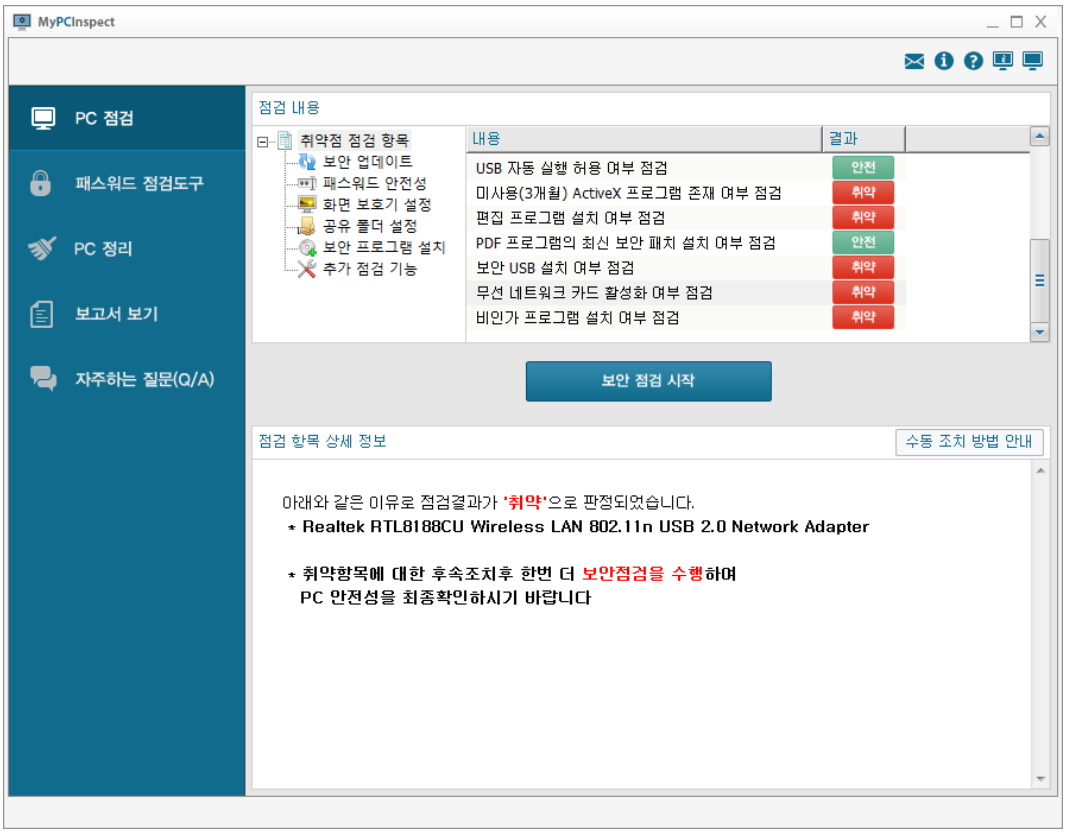
편집프로그램이 설치된 내역을 검사하여 설치되어 있으면 "취약"으로 점검된다. (단, 관리자가 정책에 의해서 예외 처리한 항목은 결과에 반영하지 않음)



[그림 3.3-14] 편집 프로그램 설치 여부

3.3.13 무선 네트워크 카드 설치 여부 점검

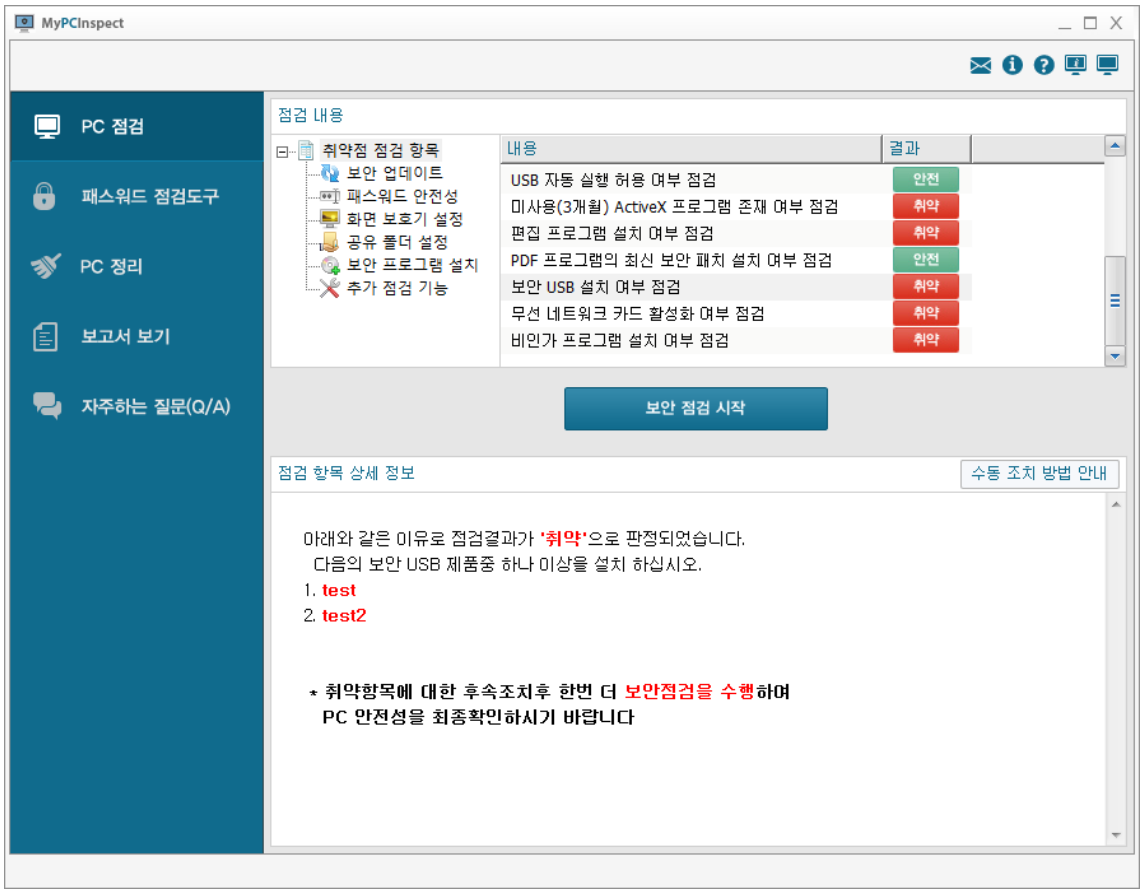
무선 네트워크 카드가 사용가능하도록 되어 있는지 여부를 점검한다. 무선 네트워크 카드가 사용가능하면 “취약”으로 점검된다.



[그림 3.3-15] 편집 프로그램 설치 여부

3.3.14 보안 USB SW 설치 여부 점검

보안 USB 가 설치되어 있는지 여부를 점검한다. 관리자 설정에 의해 미리 설정한 보안 USB 에 대해서 점검하며 보안 USB SW 설치가 되어있지 않을 경우 “취약”으로 점검된다.

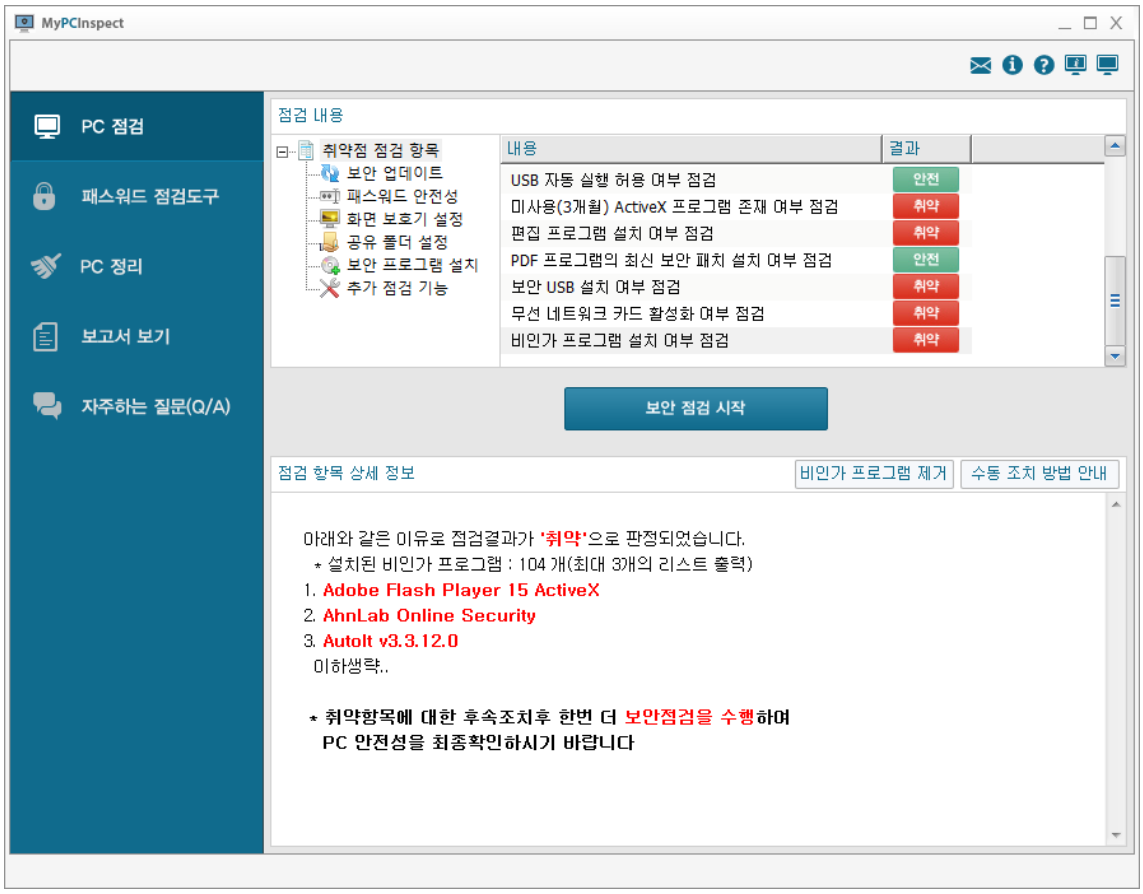


[그림 3.3-16] 보안 USB 설치 여부

3.3.15 비인가 프로그램 설치 여부 점검

인가되지 않은 프로그램이 설치된 것에 대한 점검이다. 취약으로 나온 프로그램이 있을 경우, 삭제하거나 업무상 필요한 소프트웨어에 대해서는 관리자의 승인이 필요하므로

내 PC 지키미 상단메뉴의 기술지원 연락처  를 참고하기 바란다.

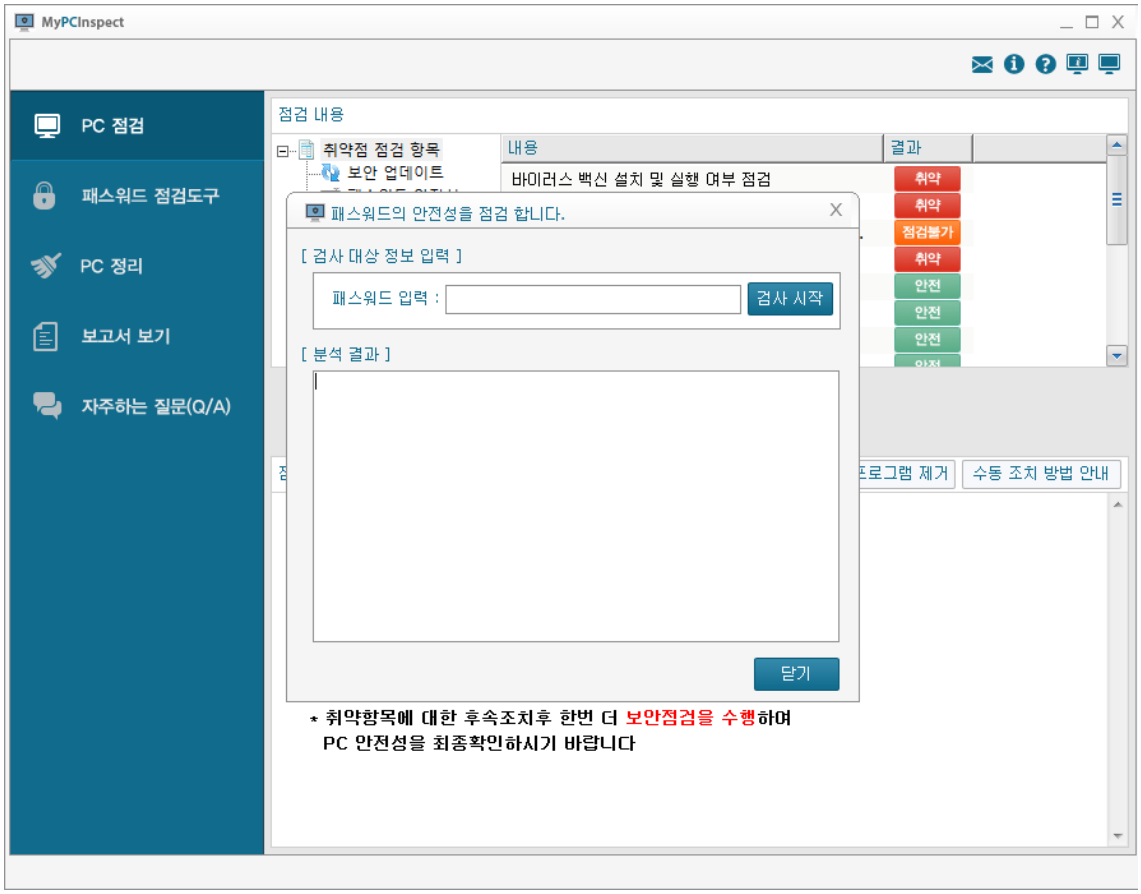


[그림 3.3-17] 비인가 프로그램 설치 여부

4. 관리 도구

4.1. 패스워드 점검도구

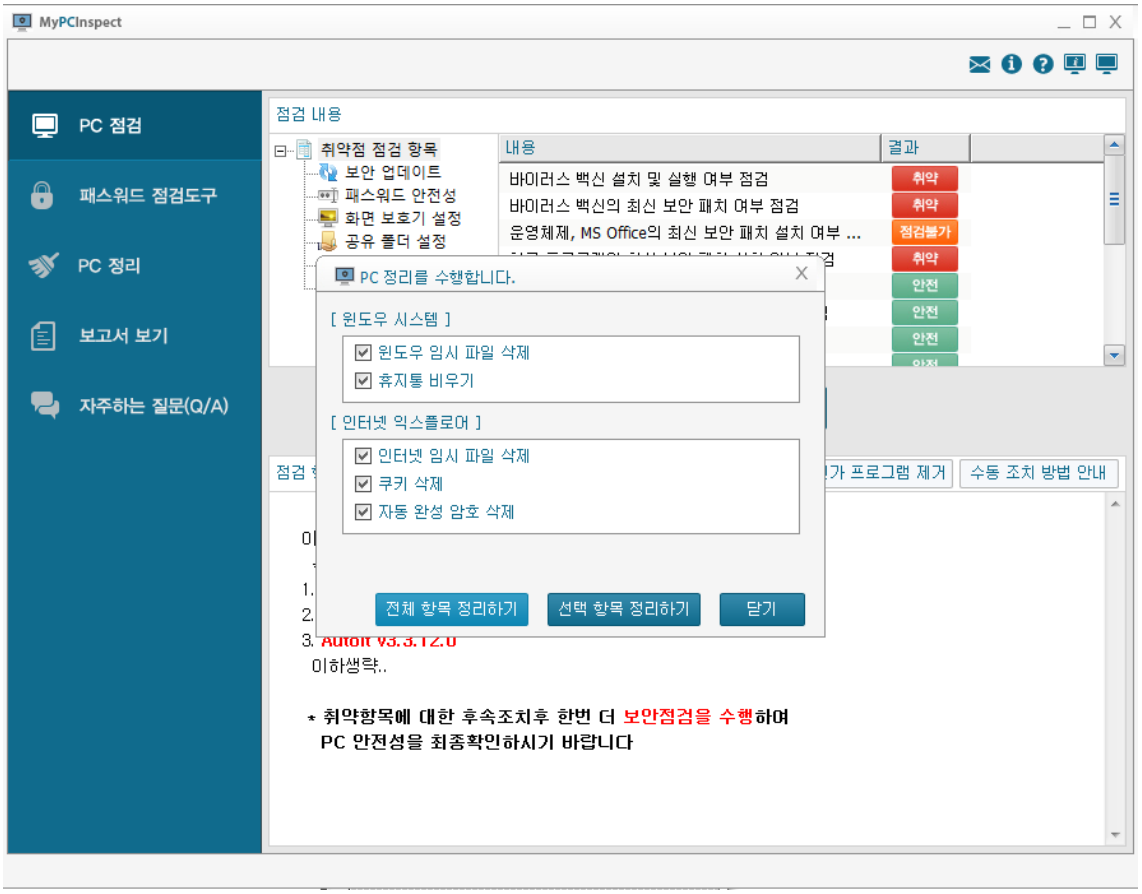
패스워드 수준을 점검 할 수 있도록 도와주는 도구이다. PC 뿐 아니라, 다른 곳에 활용하는 패스워드도 점검하는데 활용할 수 있다.



[그림 4.1-1] 패스워드 안전성 점검

4.2. PC 정리

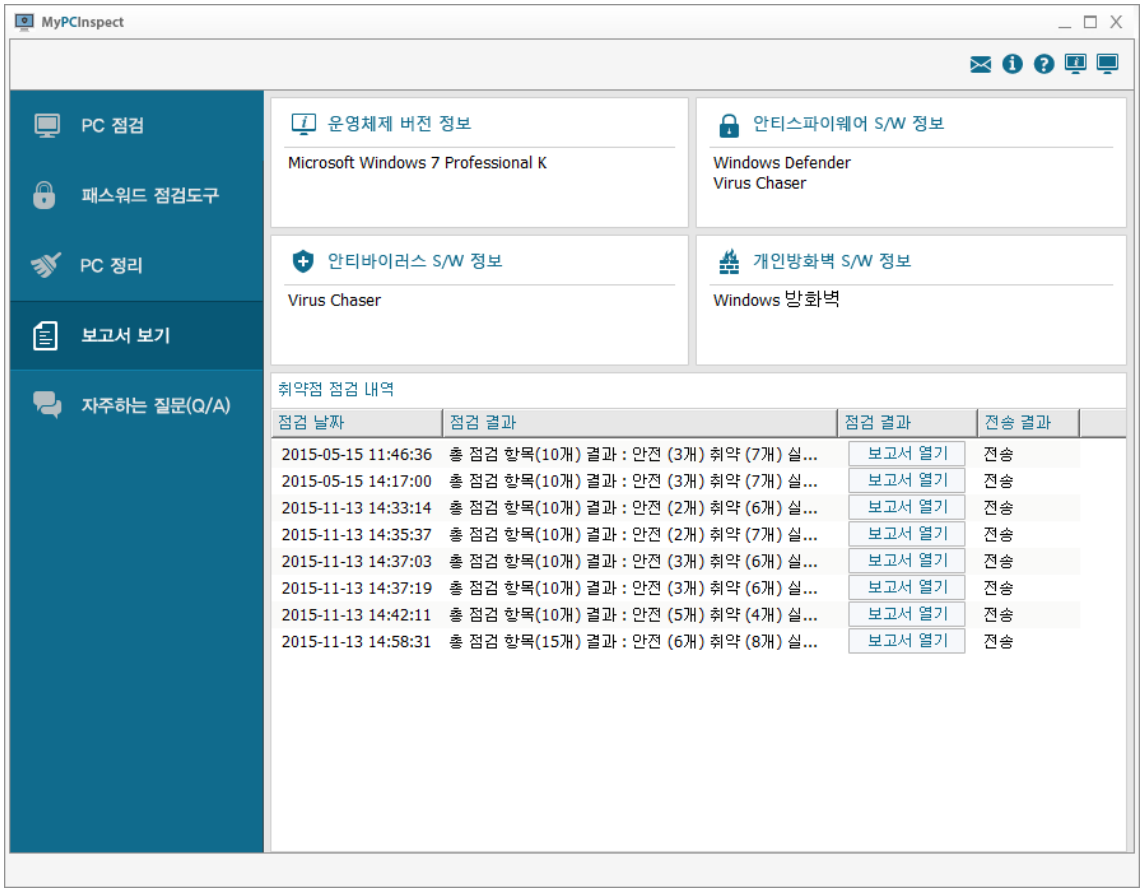
불필요하게 사용자 단말에 저장된 정보를 관리하여 단말을 최적화한다. 윈도우 시스템, 인터넷 익스플로어의 임시파일을 삭제하는 기능이며 개별로 선택 할 수 있고 하단에 "전체 항목 정리하기"를 통해 전체 정리가 가능하다.



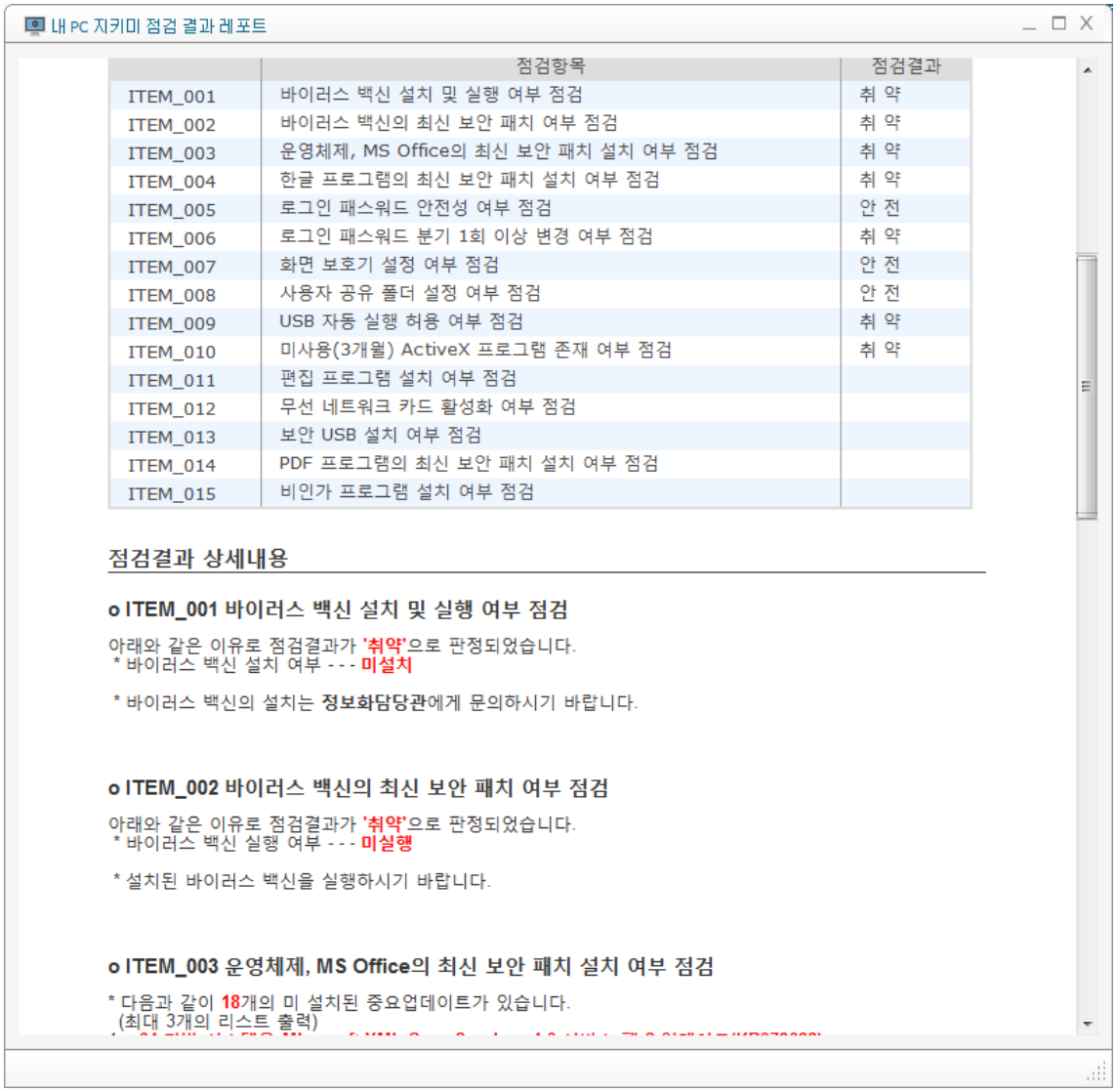
[그림 4.2-1] PC 정리

4.3. 보고서 보기

내 PC 지키미의 보고서를 확인하고, 중앙관리 서버로의 전송여부를 확인할 수 있는 항목이다. 화면상단에 운영체제 정보 , 안티 바이러스 S/W 정보, 안티 스파이웨어 S/W 정보, 개인방화벽 S/W 정보를 간략히 확인할 수 있다. 해당 검사의 "보고서 열기"를 클릭하면 제출된 보고서를 확인 할 수 있다.


MyPCInspect
PC 점검
패스워드 점검도구
PC 정리
보고서 보기
자주하는 질문(Q/A)
운영체제 버전 정보
Microsoft Windows 7 Professional K
안티스파이웨어 S/W 정보
Windows Defender
Virus Chaser
안티바이러스 S/W 정보
Virus Chaser
개인방화벽 S/W 정보
Windows 방화벽
취약점 점검 내역
점검 날짜
점검 결과
점검 결과
전송 결과
2015-05-15 11:46:36 총 점검 항목(10개) 결과 : 안전 (3개) 취약 (7개) 실... 보고서 열기 전송
2015-05-15 14:17:00 총 점검 항목(10개) 결과 : 안전 (3개) 취약 (7개) 실... 보고서 열기 전송
2015-11-13 14:33:14 총 점검 항목(10개) 결과 : 안전 (2개) 취약 (6개) 실... 보고서 열기 전송
2015-11-13 14:35:37 총 점검 항목(10개) 결과 : 안전 (2개) 취약 (7개) 실... 보고서 열기 전송
2015-11-13 14:37:03 총 점검 항목(10개) 결과 : 안전 (3개) 취약 (6개) 실... 보고서 열기 전송
2015-11-13 14:37:19 총 점검 항목(10개) 결과 : 안전 (3개) 취약 (6개) 실... 보고서 열기 전송
2015-11-13 14:42:11 총 점검 항목(10개) 결과 : 안전 (5개) 취약 (4개) 실... 보고서 열기 전송
2015-11-13 14:58:31 총 점검 항목(15개) 결과 : 안전 (6개) 취약 (8개) 실... 보고서 열기 전송

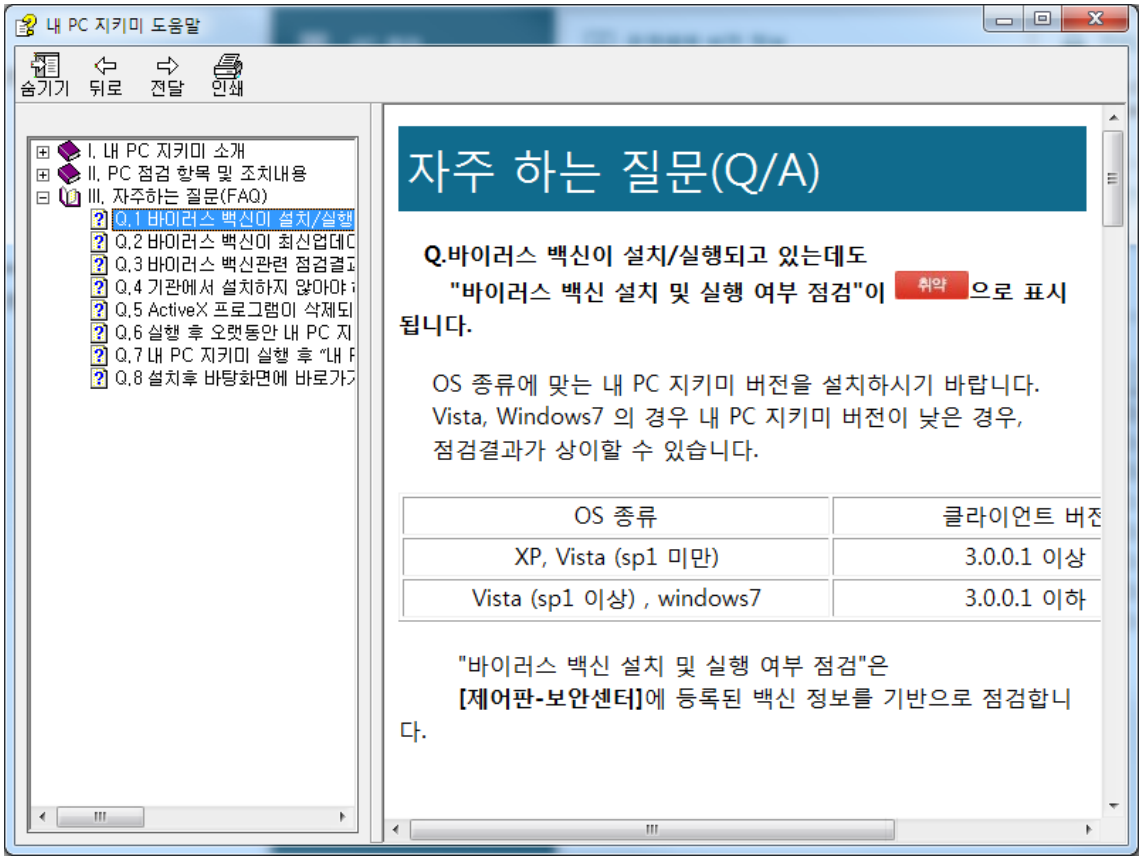
[그림 4.3-1] 보고서 보기



[그림 4.3-2] 보고서 견본

4.4. 자주하는 질문(Q/A)

내 PC 지키미에 도움말 화면이다. 각 항목에 대한 설명 및 조치방법에 대하여 상세 기록되어있으며 관리자에 의해 추가로 등록된 질문이 포함되어 각 고객사 별로 Q/A 를 작성하여 사용할 수 있다.



[그림 4.4-1] 자주하는 질문 (QnA)

5. 내 PC 지키미 삭제

5.1. 삭제하기

내 PC 지키미는 사용자 임의로 삭제 할 수 없으며, 삭제시 관리자의 허가를 승인 받은 이후, 삭제가 가능하다.

6. 솔루션 및 고객 지원

6.1. 고객 지원

자사에서는 “내 PC 지키미 1.0” 제품을 구매한 고객이 제품을 사용하며 발생하는 프로그램 문제, 제품에 대한 문의 등에 대한 기술 지원을 제공한다.

고객 지원 센터 연락처

홈페이지: http://www.viruschaser.com