내 PC 지키미 – 국내용

설명서 V3.0

<목 차>

<표 목차>

<그림 목차>

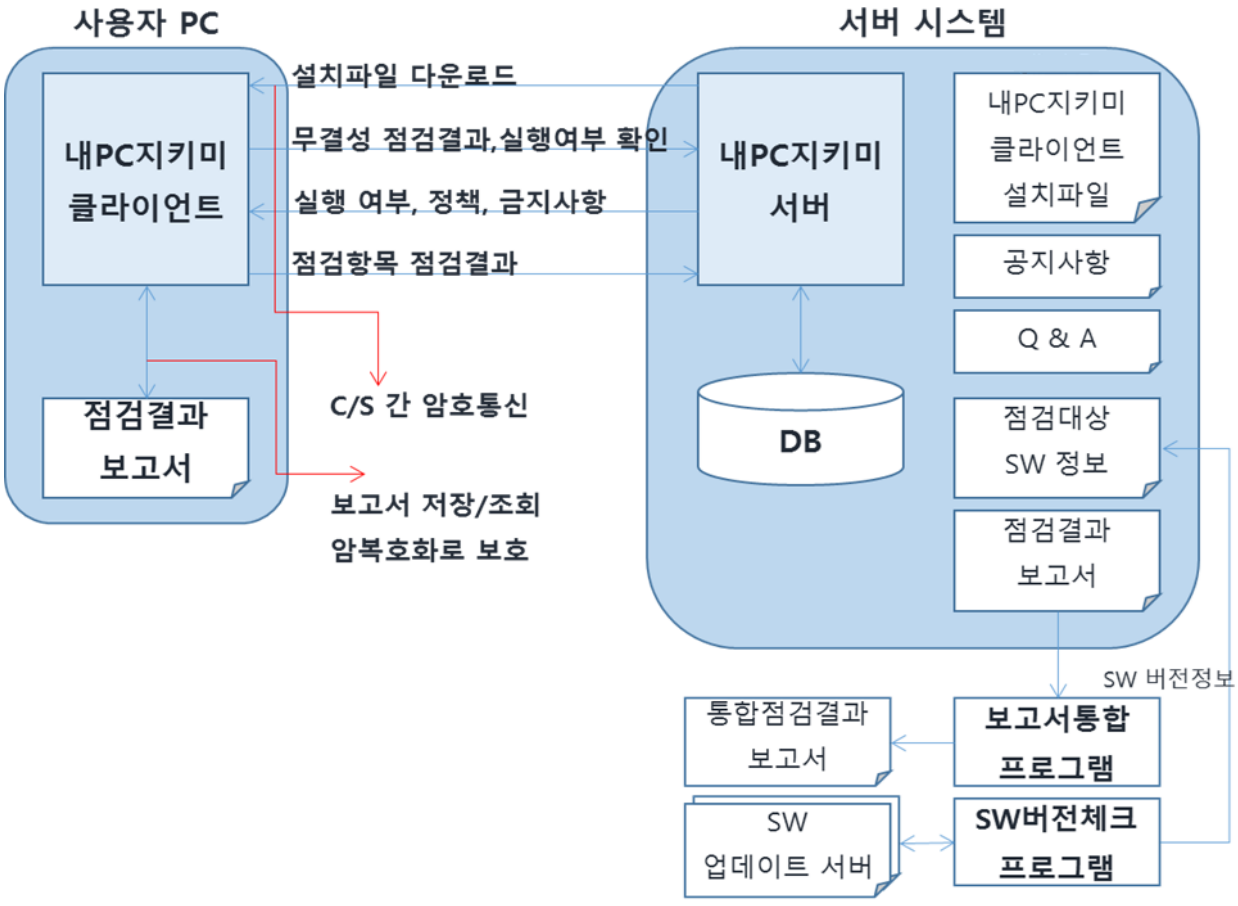
1. 개요

내 PC 지키미는 해킹으로 인한 사용자 PC 정보 유출 피해예방과 보안의식 제고를 위해 매월 "사이버 보안 진단의날"을 수립하여 PC 사용자가 PC 의 보안 수준을 스스로 확인하고 보완하도록 안내하는 소프트웨어입니다. 내 PC 지키미는 클라이언트-서버 구조의 프로그램이며, 본 문서에서는 내 PC 지키미 클라이언트 프로그램의 사용설명서를 기술하였습니다.

1.1 목적

이 문서는 개인용 PC 의 보안 수준을 고취하기 위한 ㈜하우리의 내 PC 지키미와 관리 프로그램인 내 PC 지키미 Console 의 설명서로 모든 사용자가 숙지하여야 할 사항을 운영과 각 구성요소의 기능, 배포로 나누어 설명하고 있습니다.

1.2 제품 운영 환경



[그림] 1 제품 운영환경

1.3 제품 설치 환경

1.3.1 제품 구동 최소 요구사항

- 내 PC 지키미를 구동하기 위한 최소하드웨어/소프트웨어 최소 요구사항은 다음과 같습니다.

구 분	내PC지키미
CPU	Intel Atom 1.8 GHz 이상
Memory	1GB 이상
HDD	1GB 이상 여유공간
NIC	10/100/10000MB
OS	XP SP2/SP3 Windows 8 Windows 8.1 Embedded Standard 7 Embedded POSReady 2009

[표] 1 설치 운영환경

1.3.1 제품 통신 포트

구 분	포트	포트 설명
내PC지키미 SERVER	60005	내PC지키미 서버를 구성하는 서비스 포트 중 하나로 Server가 Agent에게 정책 배포를 위한 통신 채널을 말한다.
	5432	내PC지키미 서버가 PostgreSQL과 통신하기 위한 채널을 말한다.

[표] 2 내PC지키미 통신 포트

2. 내PC지키미 PC점검 및 조치 기능

2.1 PC 점검 기능

- 내PC지키미의 주 기능은 PC점검 기능이며 점검 항목은 [표] 3과 같습니다.
- [표] 3의 15개 점검 항목에 대해서 사용자PC의 보안상태를 점검하고 결과를 표시합니다.
- 점검 완료 후 점검 결과는 서버로 전송됩니다.

번호	점검항목(대분류)	점검항목(소분류)
1	보안 업데이트	바이러스 백신 설치 및 실행 여부 점검
2		바이러스 백신의 최신 보안 패치 여부 점검
3		운영체제, MS Office의 최신 보안 패치 설치 여부 점검
4		한글프로그램의 최신 보안 패치 설치 여부 점검
5	패스워드 안전성	로그인 패스워드 안전성 여부 점검
6		로그인 패스워드의 분기 1회 이상 변경 여부 점검
7	화면보호기 설정	화면보호기 설정 여부 점검
8	공유 폴더 설정	사용자 공유 폴더 설정 여부 점검
9	보안프로그램 설치	USB 자동 실행 허용 여부 점검
10		미사용(3개월) ActiveX 프로그램 존재 여부 점검
11	추가점검기능	PDF 프로그램의 최신 보안 패치 설치 여부
12		편집 프로그램(MS워드, 한글, PDF, 엑셀, PPT) 설치 여부 점검
13		무선 랜카드 설치 여부 점검
14		보안USB 설치 여부 점검 기능
15		비인가 프로그램 설치 여부 점검

[표] 3 내PC지키미 PC 점검항목

- 1번 항목부터 15번 항목까지는 필수 점검 항목으로써 반드시 점검이 수행되어야 하는 항목입니다.
- 하지만, 고객사의 많은 요구로 인해 검사 제외 가능하며, 필수 항목이므로 제품에 항목이 나타나며, 검사결과는 "점검불가"로 표시됩니다.
- 11번 항목부터 15번 항목까지는 관리자가 선택적으로 추가할 수 있는 점검 항목으로써 관리자의 설정에 따라 점검을 수행할 수도 안 할 수도 있습니다.
- 11번 항목부터 15번 항목 에 대해서 관리자과 추가하지 않은 항목은 제품에 표시되지 않으며, 검사 또한 하지 않습니다.

2.2 PC 점검 후 취약점 조치 기능

- 점검항목에 대해 "취약"으로 판정되었을 경우 조치 방법을 안내하고 조치 기능을 수행 합니다.
- 조치 기능에 대해서는 3장을 참고하시기 바랍니다.

2.3 내PC지키미 점검일 자동실행

□ 내PC지키미 클라이언트 프로그램은 관리자가 설정한 점검일에 윈도우 부팅 시 자동실행 됩니다.

- 예를 들어 관리자가 점검일을 "매월 세 번째 수요일" 이라고 지정하면 내PC지키미는 매월 그달의 첫 번째 수요일을 기준으로 하여 세 번째 수요일마다 윈도우가 로그인 되자마자 실행됩니다.
- 관리자가 설정한 "강제 점검 수행"으로 인해 PC점검이 자동으로 시작될 수 있습니다.

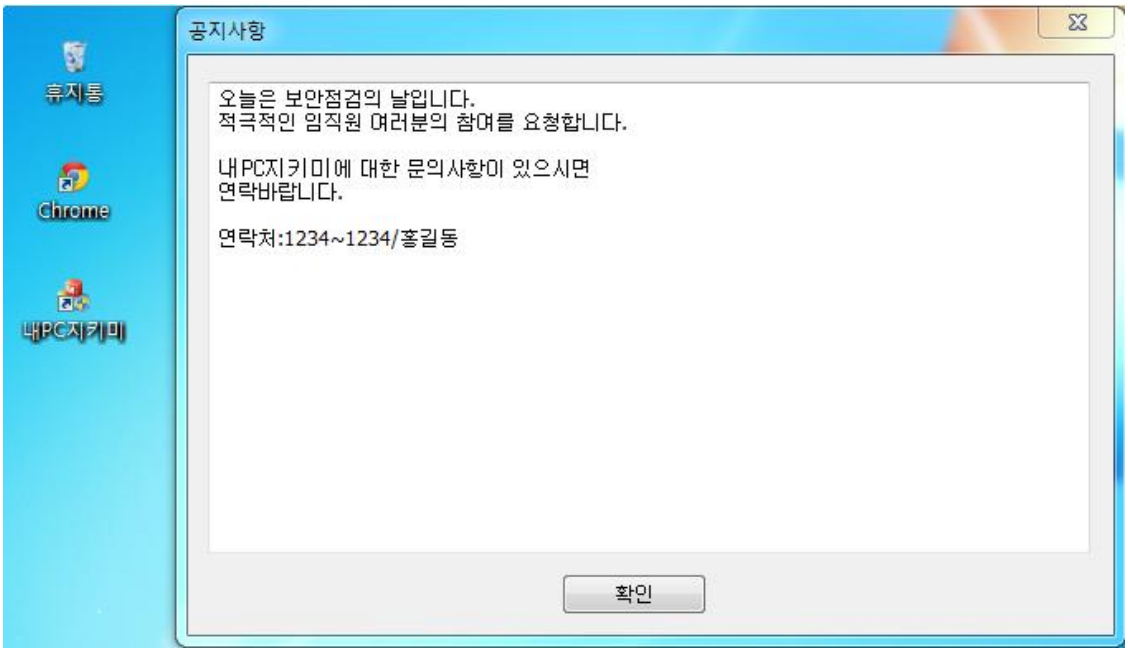
□ 관리자가 점검일을 복수일자로 설정할 수 있기 때문에 내PC지키미는 한달에도 여러 번 실행될 수 있습니다.

- 예를 들어 관리자가 점검일을 기준으로 "매주 화요일" 이라고 설정하면 매주 화요일 마다 한 달에 4번 이상 자동 실행될 수 있습니다.

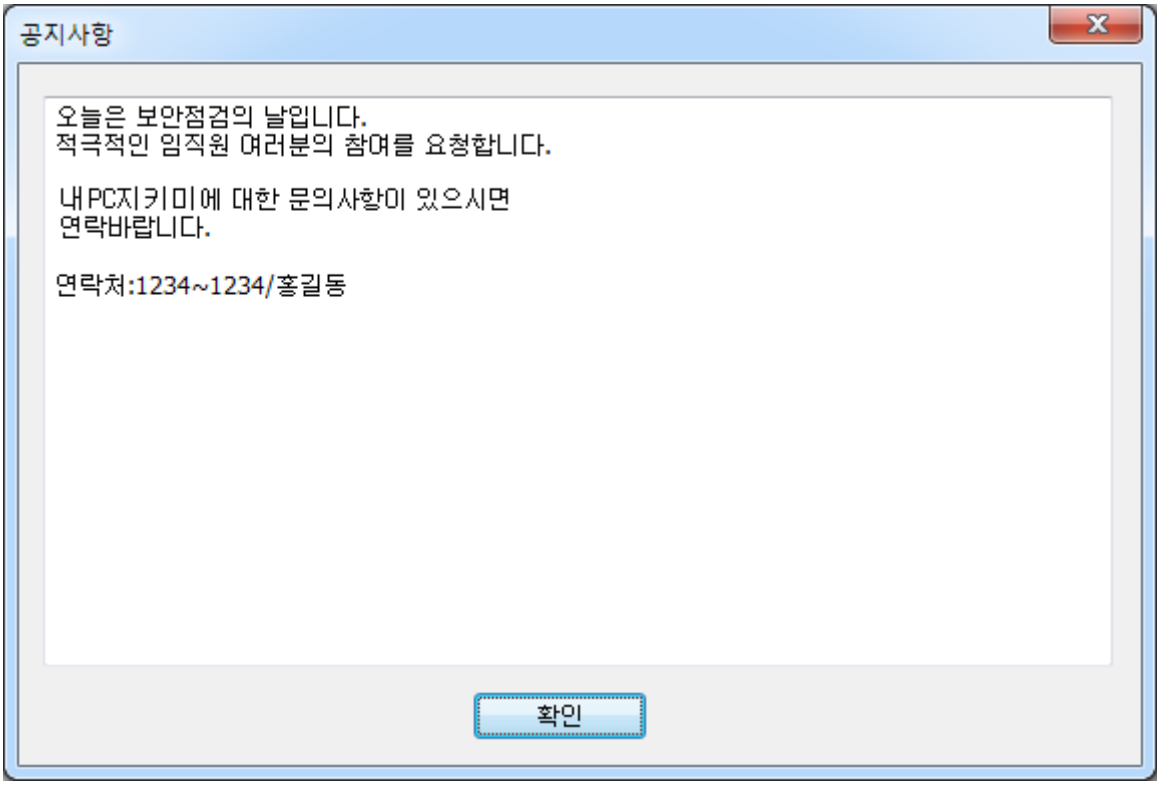
□ 관리자가 설정한 점검일에 내PC지키미를 설치했다면 설치된 후에 돌아오는 주기에 자동 실행됩니다.

2.4 내PC지키미의 실행

□ 내PC지키미가 처음 실행되면 사용자의 적극적인 보안취약점 해소에 대한 참여를 위해 안내 페이지를 나타나도록 하였습니다.

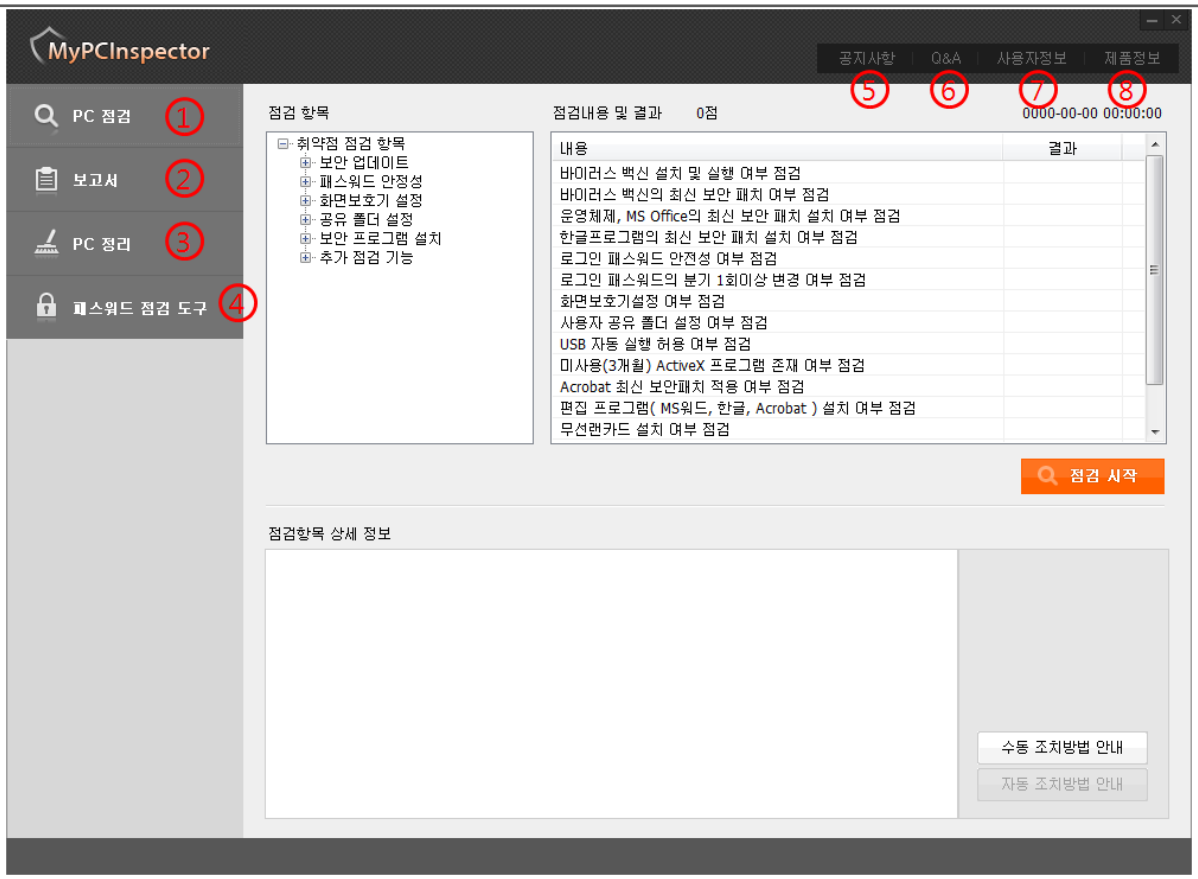


[그림] 2 시작 안내 화면



[그림] 3 공지사항 화면

□ 이때, 관리자가 설정한 공지사항이 있으면 공지사항이 먼저 떠서 사용자에게 안내를 하고 다음을 진행하면, 메인 화면이 생성됩니다.



[그림] 4 메인 화면

□ [그림] 4에서 각 메뉴는 다음과 같은 기능을 수행합니다.

① PC 점검 메뉴 – 15개 PC 점검항목에 대해서 점검을 수행합니다.

② 보고서 보기 메뉴 - PC점검에 대한 결과를 확인할 수 있습니다.

③ PC 정리 메뉴 - 윈도우 시스템 및 인터넷 익스플로러의 임시 파일 정리를 수행합니다.

④ 패스워드 점검도구 메뉴 – 패스워드의 강도를 점검합니다.

⑤ 공지사항 메뉴 – 관리자로부터의 공지사항 내용을 확인합니다.

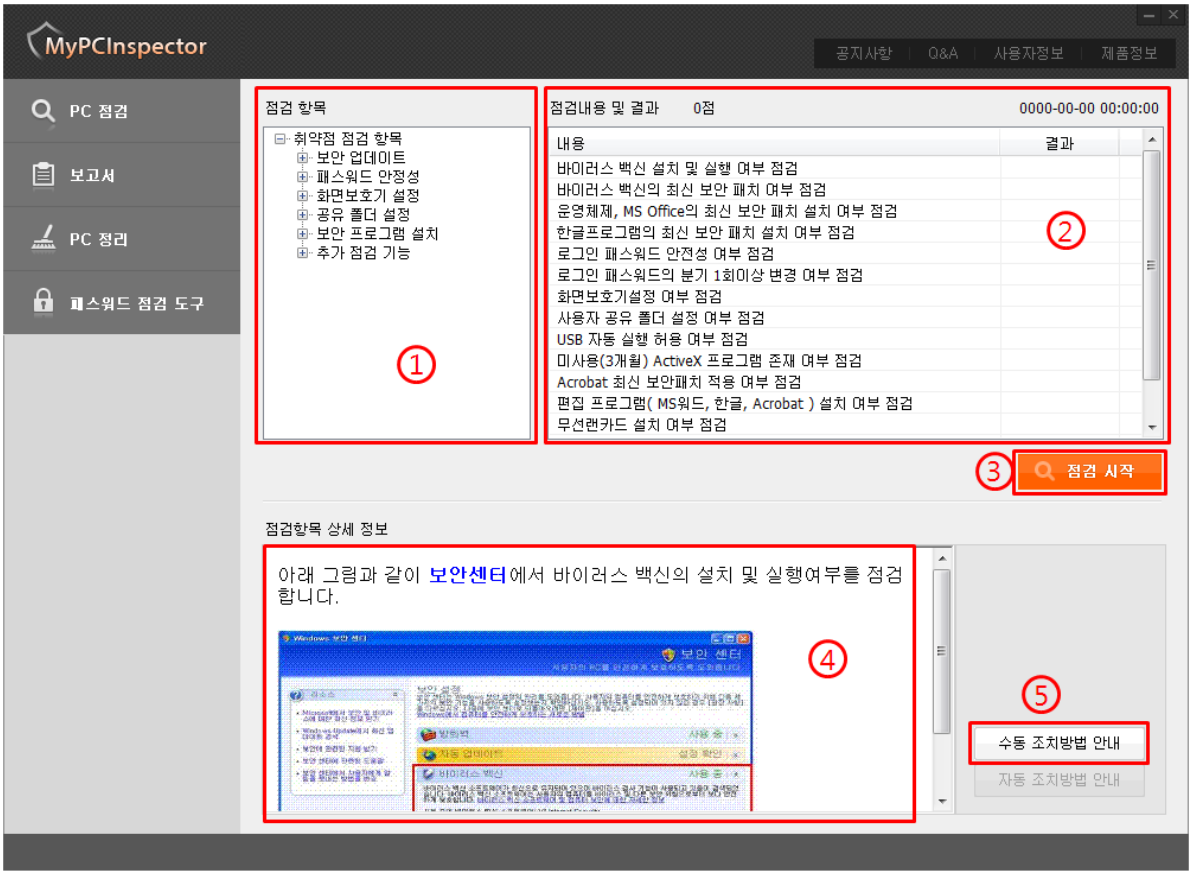
⑥ Q&A 메뉴 – 관리자 제공 Q&A를 표시합니다.

⑦ 사용자 정보 메뉴 – 사용자 정보 및 컴퓨터 정보를 확인합니다.

⑧ 제품정보 메뉴 – 내PC지키미 버전 정보를 확인할 수 있습니다.

3. 내PC지키미의 화면 구성

- [그림] 4의 PC점검버튼(①)을 클릭하면 다음과 같은 PC점검 화면이 보여집니다.



[그림] 5 PC점검 화면 구성

3.1 PC 점검 화면 구성

□ [그림] 5에서 표시되는 내용의 세부사항은 다음과 같습니다.

① PC 점검 항목 대분류
- PC 점검 항목의 대분류를 표시합니다.
- 각 항목 선택 시 ②에서 해당 대분류에 속한 소분류가 표시됩니다.

② PC 점검 항목 소분류
- PC 점검 항목의 소분류를 표시합니다.
- PC점검 수행 후 점검 결과를 표시합니다. (안전/취약/점검불가)
- 각 항목 선택 시 ④에서 상세정보가 표시됩니다.

③ 보안 점검 시작 버튼
- 해당 버튼을 클릭하면 PC 점검을 시작합니다.

④ 점검항목 상세 정보 표시
- ②에서 각 항목 선택 시 선택된 항목의 상세 정보를 표시합니다.
- PC점검 수행 후 점검 결과가 "취약"인 경우 취약 원인을 표시합니다.

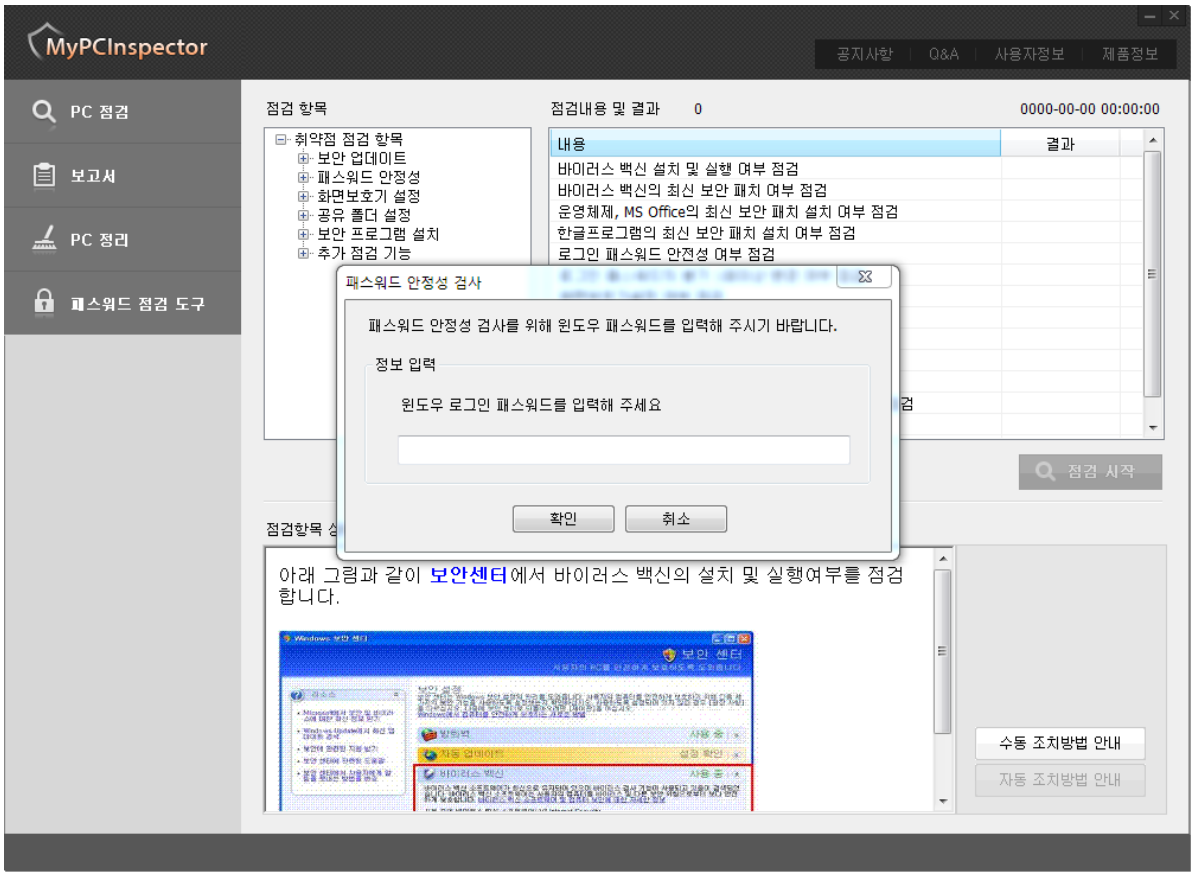
⑤ 수동조치방법안내 버튼

- 버튼 클릭 시 ②에서 선택한 점검 항목의 점검 결과가 "취약"으로 판별된 경우 수동으로 수정하는 방법을 안내합니다.

3.2 PC 점검 수행 화면

□ "보안 점검 시작"버튼([그림] 5의 ③)을 클릭하여 PC 점검을 시작합니다.

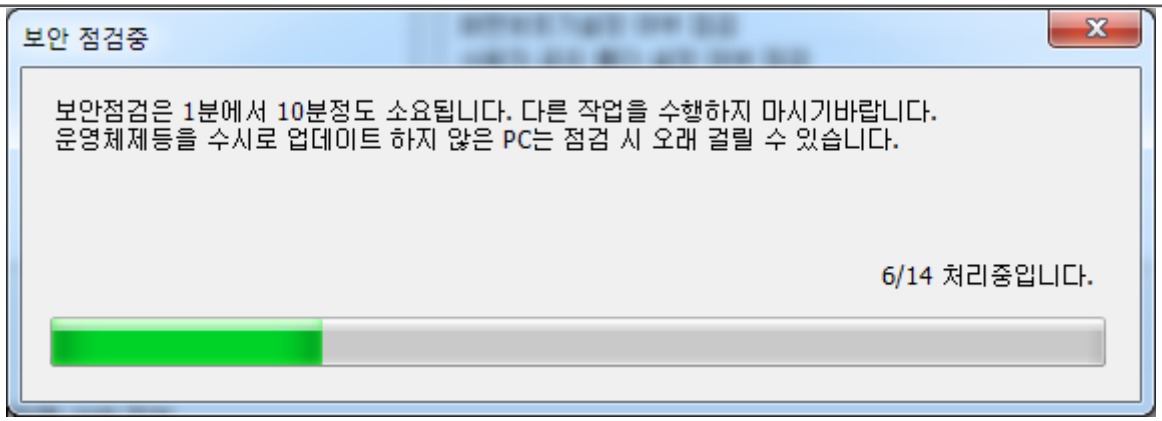
- 관리자가 설정한 "강제 점검 수행"으로 인해 PC점검이 자동으로 시작될 수 있습니다
- 그러면 점검항목 중 "로그인 패스워드 안전성 여부 점검" 항목을 점검하기 위해 사용자의 윈도우 로그인 패스워드 입력창이 생성됩니다.



[그림] 6 PC점검 수행 화면 구성

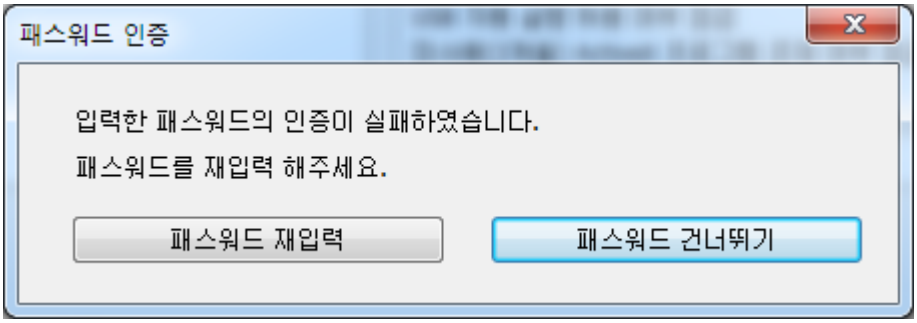
□ 윈도우 로그인 패스워드를 입력하고 "확인" 버튼을 클릭합니다.

□ 로그인 패스워드를 정확히 입력했을 경우 PC 점검이 시작되며 다음과 같은 진행 사항이 보여집니다.



[그림] 7 PC점검 진행 사항 표시

□ 로그인 패스워드를 잘못 입력한 경우 다음과 같은 메시지 창이 생성됩니다.



[그림] 8 PC점검 윈도우 패스워드 불일치 알림 창

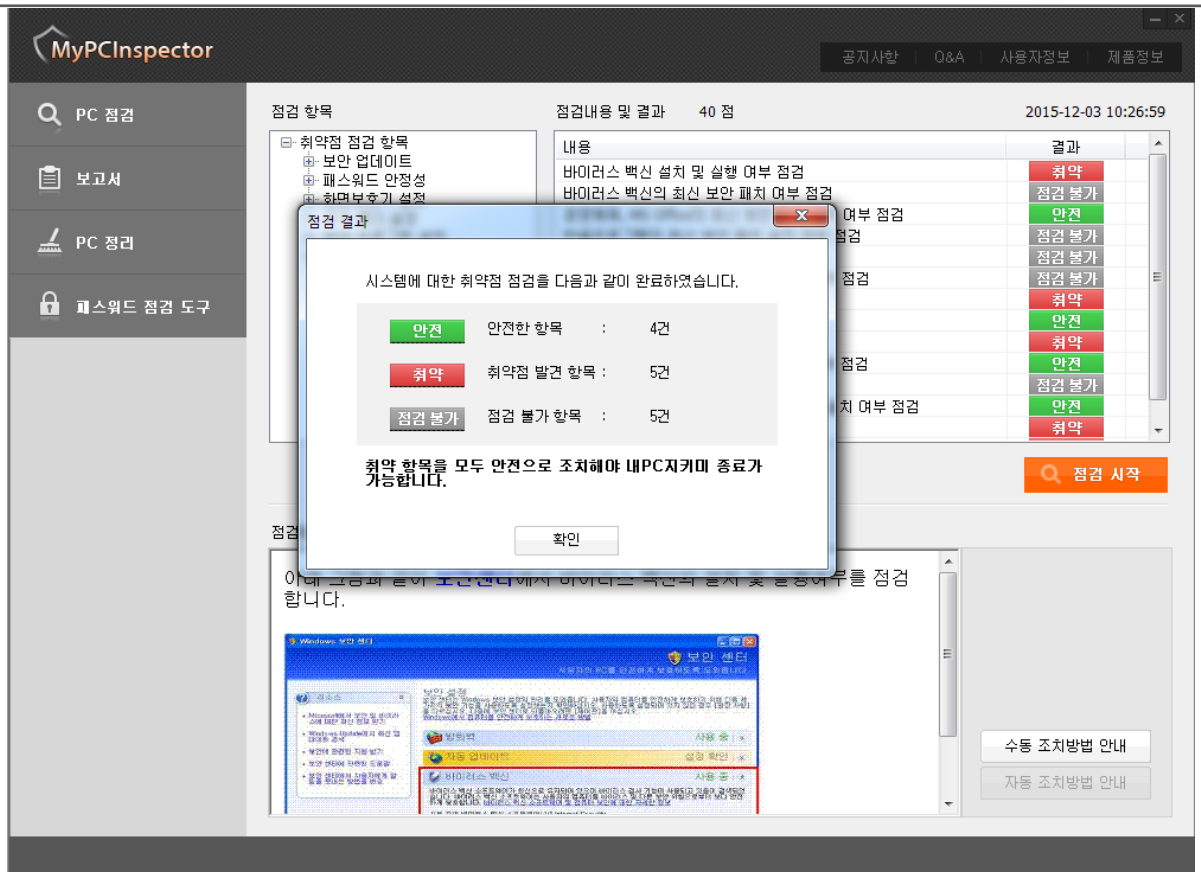
○ 패스워드를 다시 입력하려면 "패스워드 재입력" 버튼을 클릭합니다. [그림] 6의 패스워드 입력창이 다시 보여집니다.

○ 로그인 패스워드 안전성 여부 점검을 수행하지 않고 넘어가려면 "패스워드 검사 건너뛰기" 버튼을 클릭합니다. 단 점검결과는 "점검불가"로 표시됩니다.

○ 패스워드를 정확히 다시 입력하거나 로그인 패스워드 안전성 여부 점검을 건너뛰면 PC 점검이 시작되며 [그림] 7과 같은 진행 사항이 보여집니다.

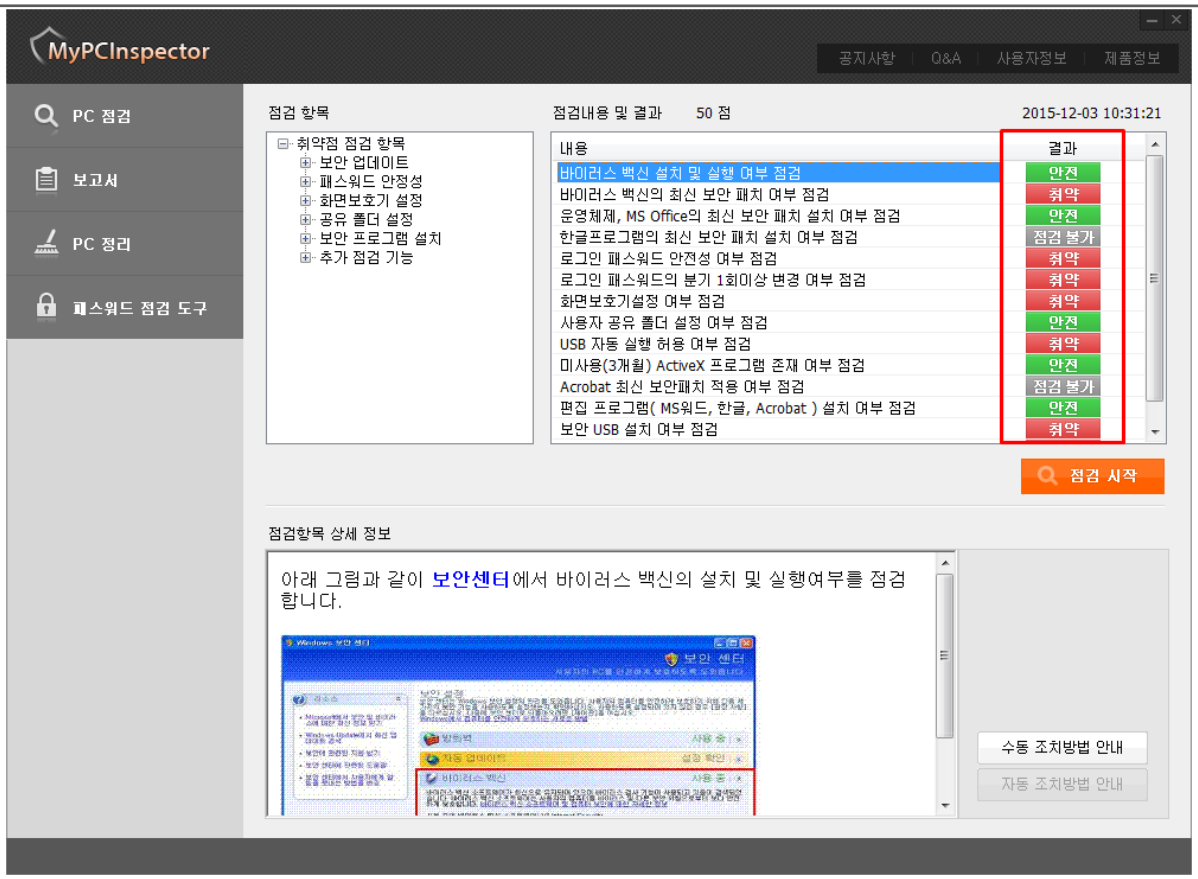
□ PC 점검은 몇 분 정도 걸리며 점검시간에는 다른 작업을 수행하지 마십시오.

□ PC 점검이 완료되면 [그림] 9와 같이 점검 결과 요약 창이 생성됩니다.



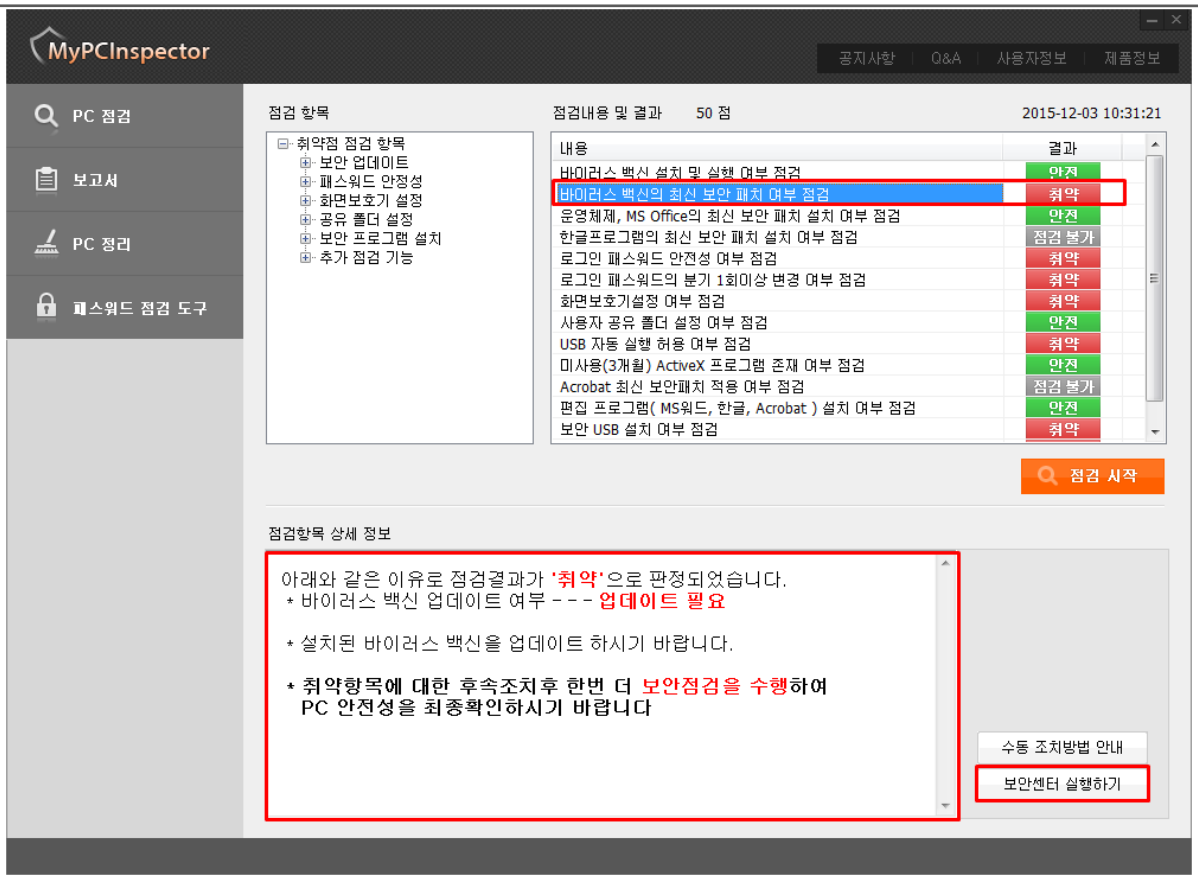
[그림] 9 PC점검 완료 화면

□ 읽어 보신 후 "확인" 버튼을 클릭합니다.



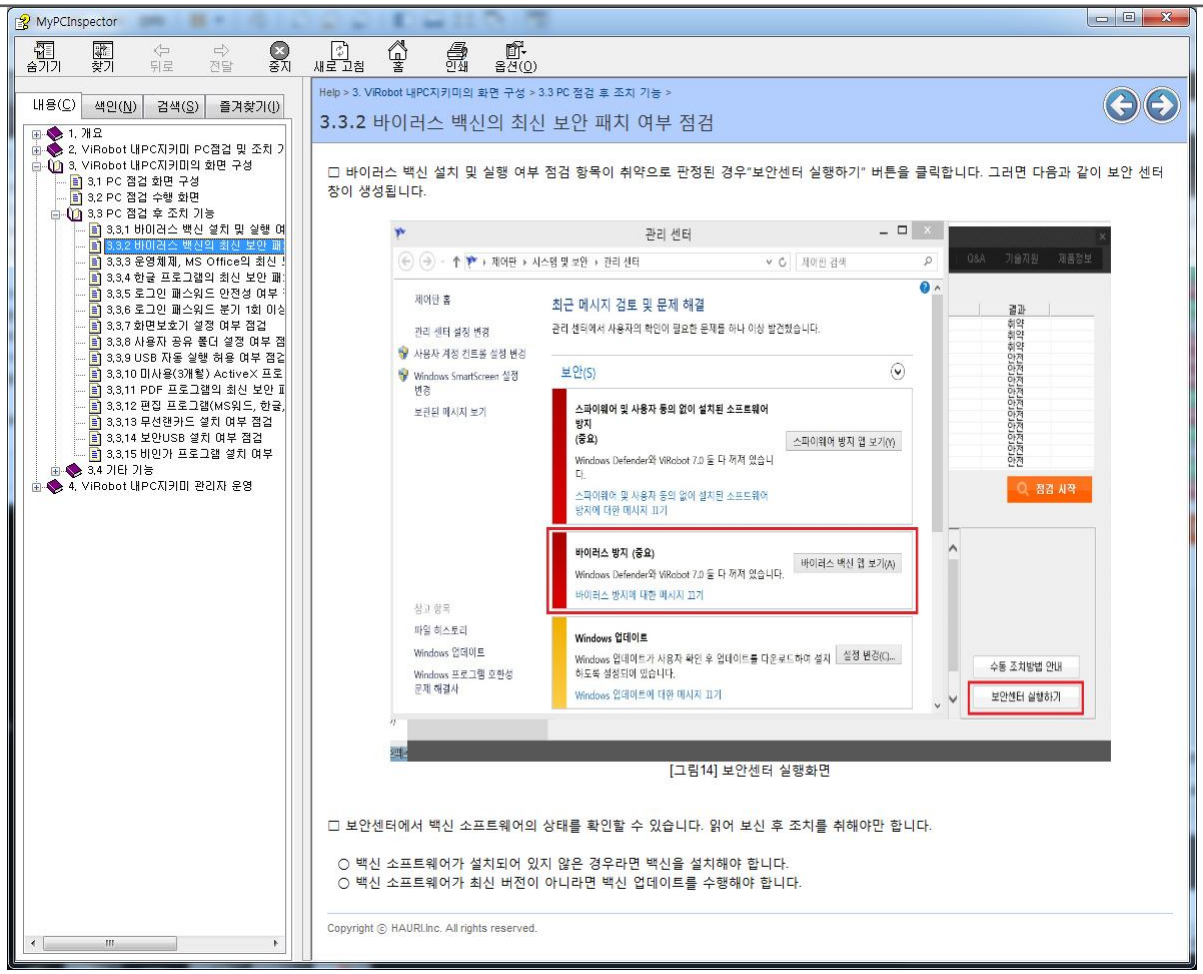
[그림] 10 취약 항목 정보 표시

□ 취약한 항목에 대해서는 조치가 필요합니다.



[그림] 11 점검결과 취약 항목 및 원인 표시

□ "수동조치방법안내" 버튼을 클릭하면 취약점을 제거하는 조치방법을 안내하는 창이 생성되니 읽어 보신 후 취약점을 제거하시기 바랍니다.

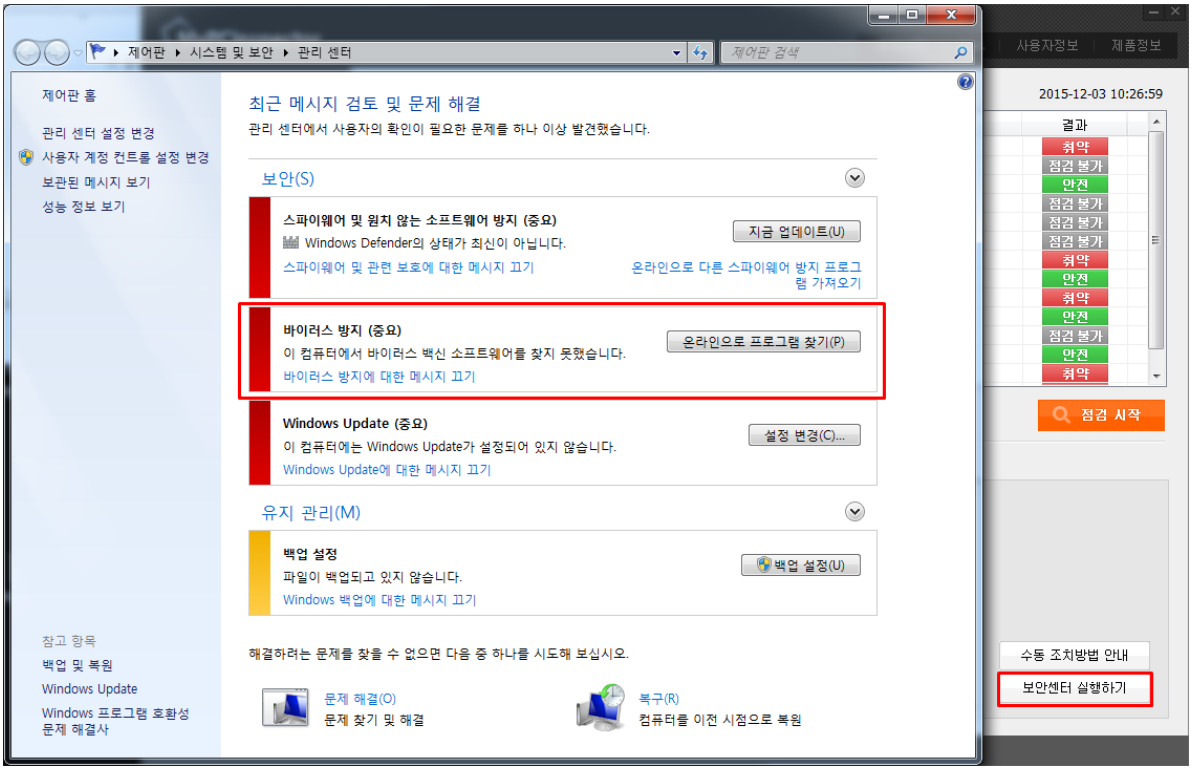


[그림] 12 수동 조치방법 안내 창 표시 화면

3.3 PC 점검 후 조치 기능

3.3.1 바이러스 백신 설치 및 실행 여부 점검

□ 바이러스 백신 설치 및 실행 여부 점검 항목이 취약으로 판정된 경우 "보안센터 실행하기" 버튼을 클릭합니다. 그러면 다음과 같이 보안 센터창이 생성됩니다.



[그림] 13 보안센터 실행화면

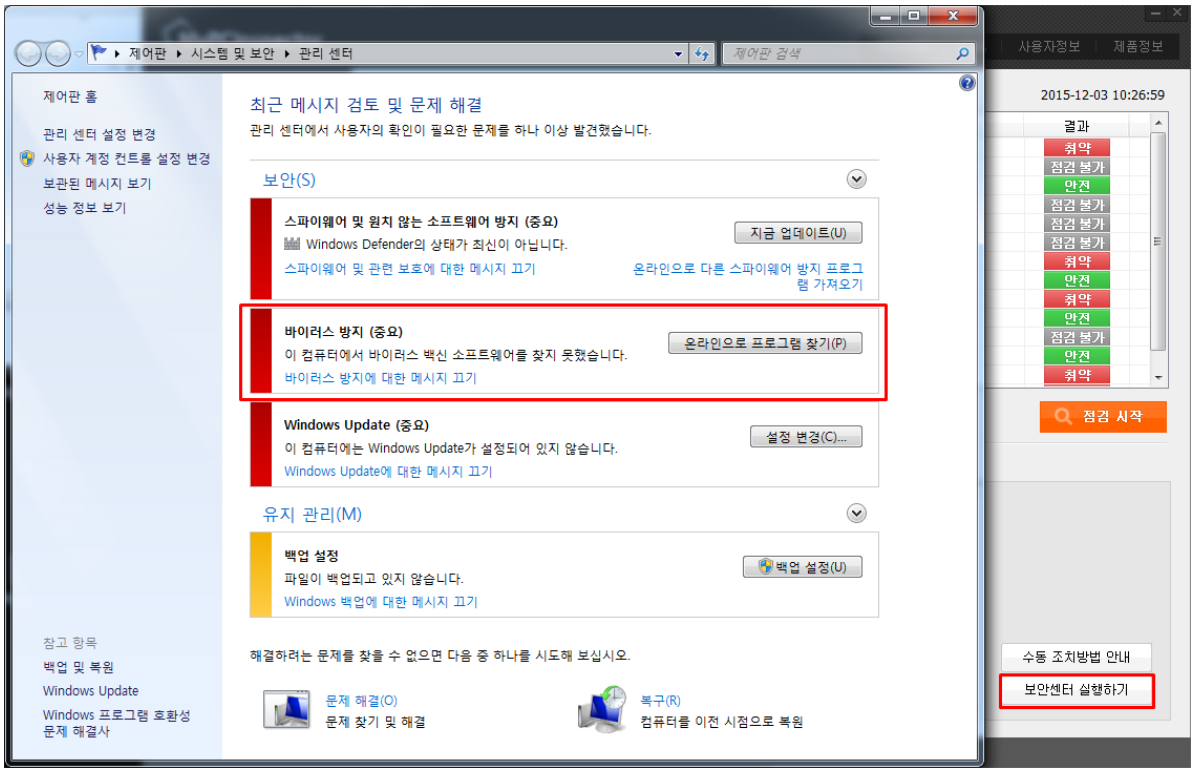
□ 보안센터에서 백신 소프트웨어의 상태를 확인3)할 수 있습니다. 읽어 보신 후 조치를 취해야만 합니다.

○ 백신 소프트웨어가 설치되어 있지 않은 경우라면 백신을 설치해야 합니다.

○ 백신 소프트웨어가 동작중이 아니라면 동작시켜야 합니다.

3.3.2 바이러스 백신의 최신 보안 패치 여부 점검

□ 바이러스 백신 설치 및 실행 여부 점검 항목이 취약으로 판정된 경우"보안센터 실행하기" 버튼을 클릭합니다. 그러면 다음과 같이 보안 센터창이 생성됩니다.



[그림] 14 보안센터 실행화면

□ 보안센터에서 백신 소프트웨어의 상태를 확인할 수 있습니다. 읽어 보신 후 조치를 취해야만 합니다.

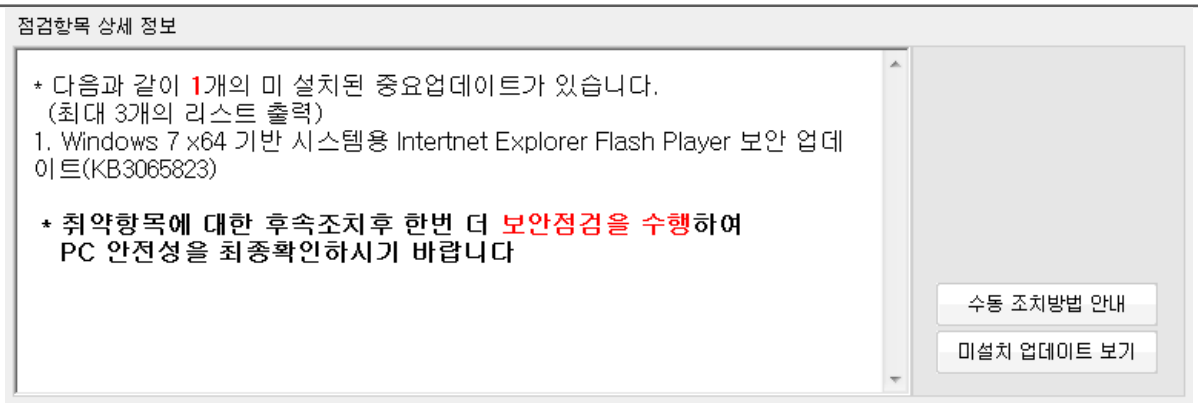
○ 백신 소프트웨어가 설치되어 있지 않은 경우라면 백신을 설치해야 합니다.

○ 백신 소프트웨어가 최신 버전이 아니라면 백신 업데이트를 수행해야 합니다.

3.3.3 운영체제, MS Office의 최신 보안 패치 설치 여부 점검

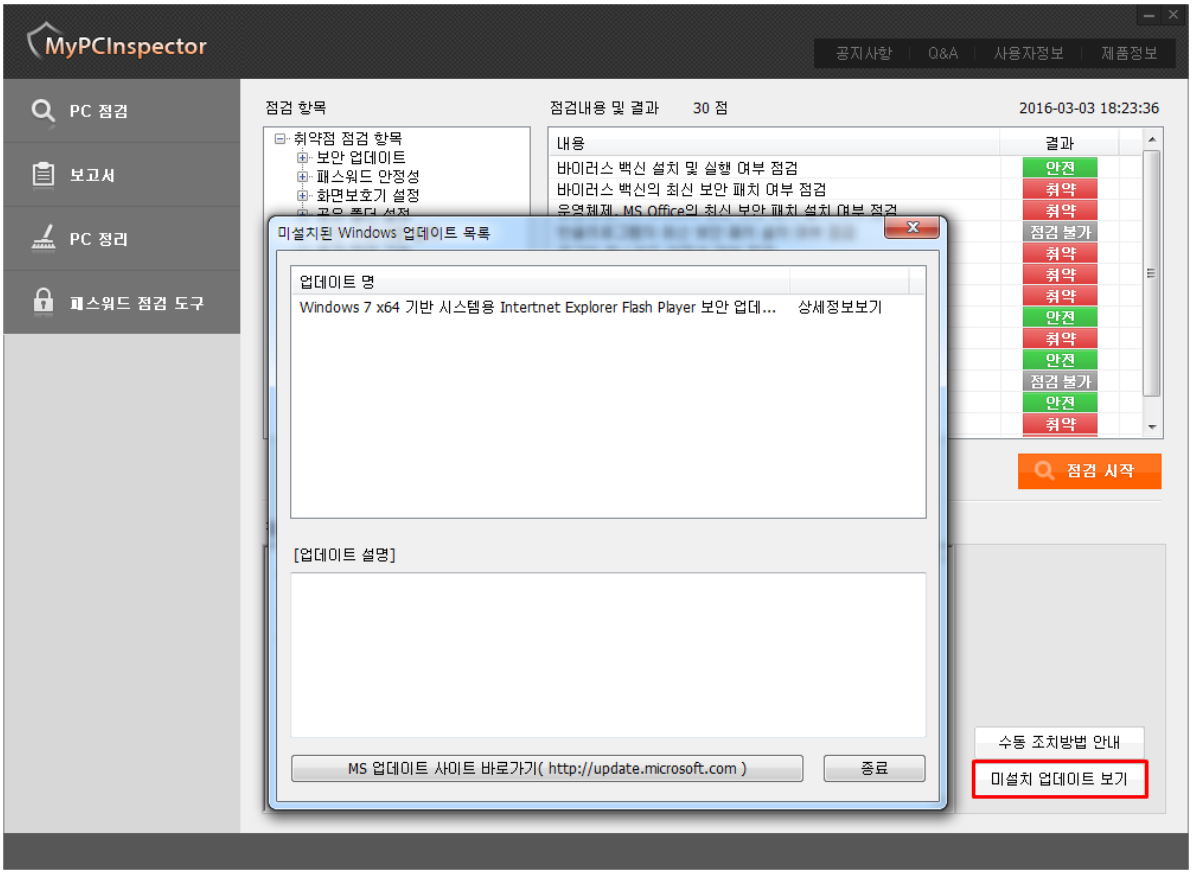
□ 운영체제, MS Office의 최신 보안 패치 설치 여부 점검 항목이 취약으로 판정된 경우는 설치되지 않은 중요 업데이트가 존재할 때 판정됩니다.

□ 조치를 하기 위해서는 [그림] 15에서 "미 설치 업데이트 보기"버튼을 클릭 합니다.



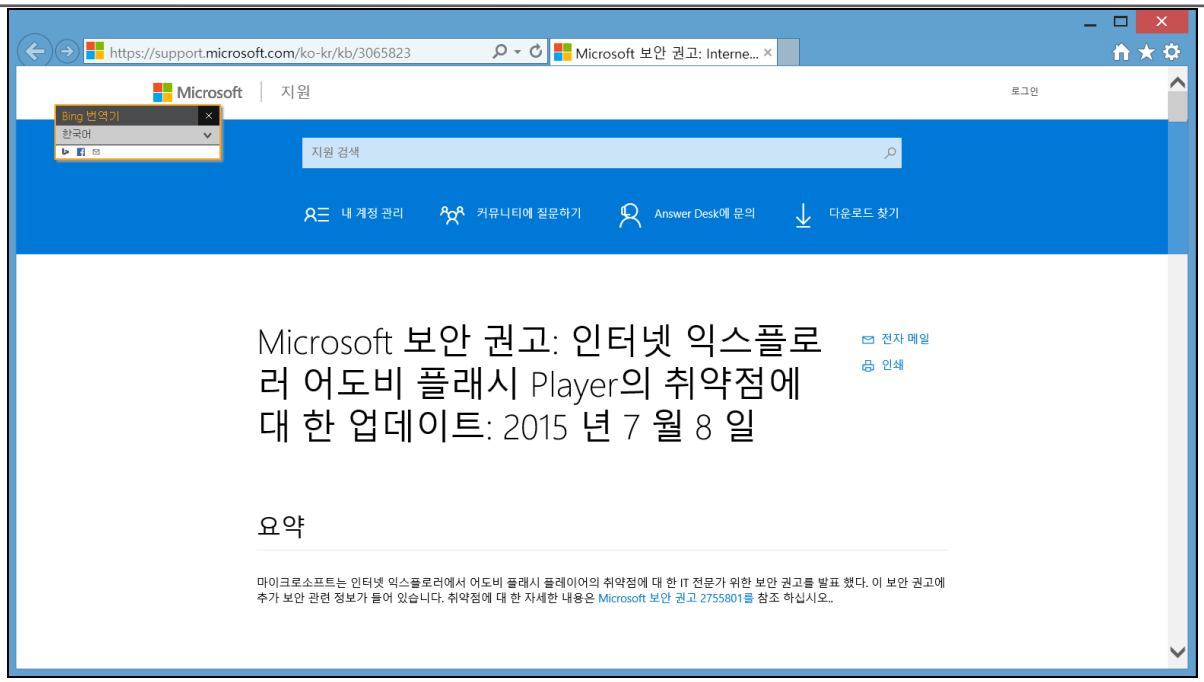
[그림] 15 운영체제, MS Office의 최신 보안 패치 설치 여부 취약 원인

□ 그러면 현재 설치 되지 않은 윈도우 업데이트 항목을 확인할 수 있는 창이 생성 됩니다.



[그림] 16 미설치 업데이트 보기 화면

□ [그림] 16에서 "상세정보보기" 버튼을 선택하면 마이크로소프트(MS) 사이트로 연결되어 해당 항목에 대한 자세한 설명을 볼 수 있습니다.



[그림] 17 상세 정보 보기 화면

□ [그림] 16에서 "MS업데이트 사이트 바로가기"버튼을 클릭하면 마이크로소프트 업데이트 사이트로 연결됩니다. 해당 업데이트 사이트에서 업데이트를 수행해야 합니다.

[그림] 18 마이크로소프트 업데이트 사이트

3.3.4 한글 프로그램 의 최신 보안 패치 설치 여부 점검

□ 한글프로그램의 최신 보안 패치 설치 여부 점검 항목이 취약으로 판정된 경우 한글 프로그램의 업데이트가 필요합니다. 다음과 같이 PC에 설치된 한글 프로그램의 버전을 확인하시고 업데이트를 수행해야 합니다.

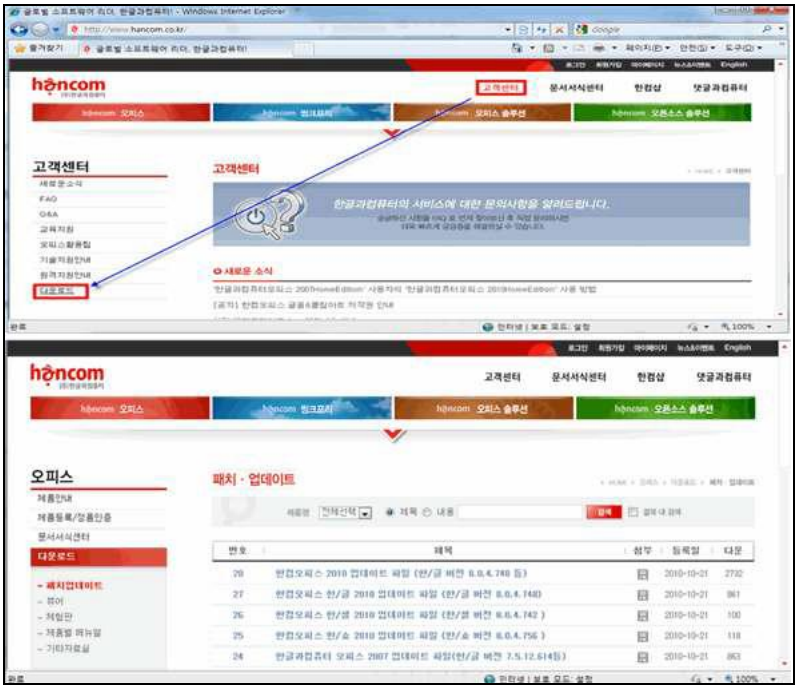
[그림] 19 한글 프로그램 취약버전 확인

□ 한글 프로그램의 업데이트 방법은 다음과 같습니다.

○ 한글 프로그램의 자동 업데이트 기능을 수행합니다.

[그림] 20 한글 자동업데이트 메뉴

○ 한글과 컴퓨터 홈페이지(http://www.hancom.co.kr)에서 업데이트를 수행합니다.



[그림] 21 한글과 컴퓨터 홈페이지

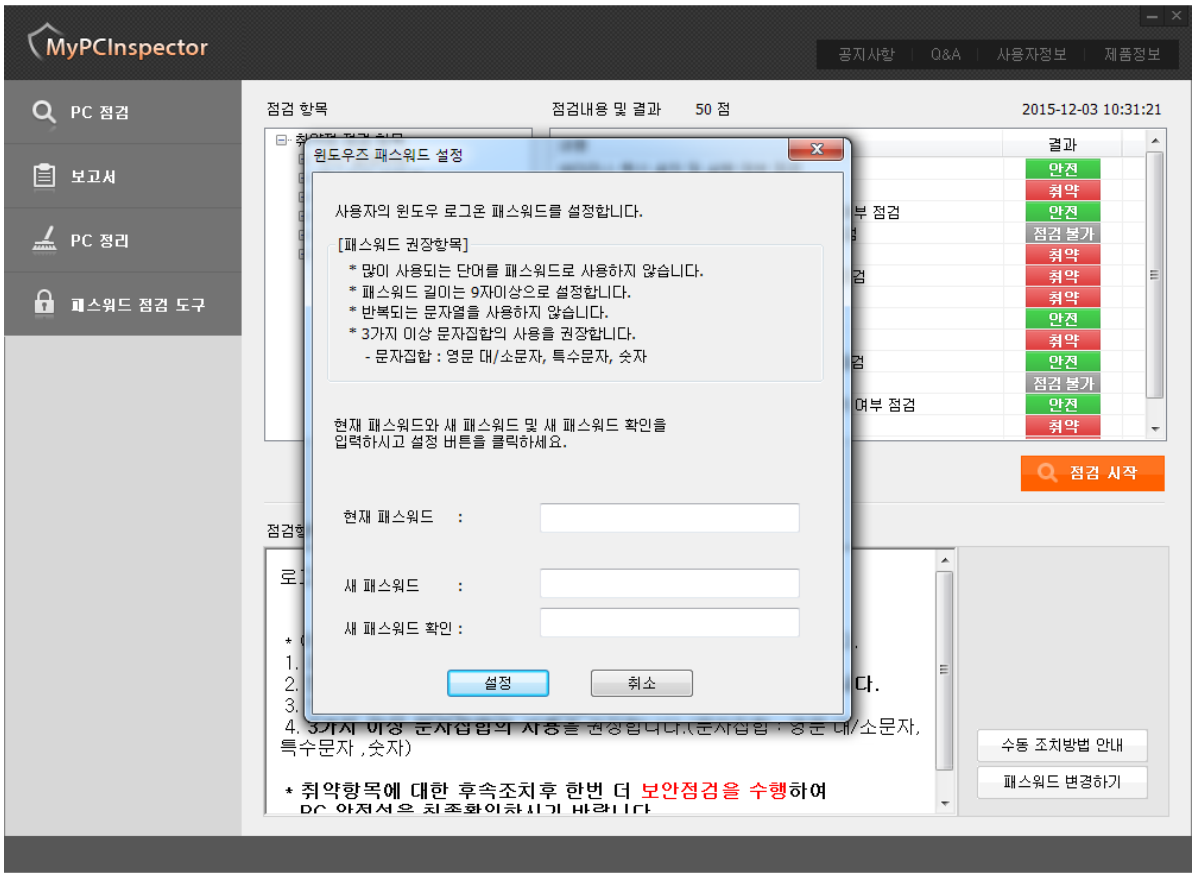
3.3.5 로그인 패스워드 안전성 여부 점검

□ 로그인 패스워드 안전성 여부 점검 항목이 취약으로 판정된 경우의 취약원인은 다음과 같습니다.

번호	로그인 패스워드 안전성 여부 점검 "취약" 원인
1	Windows로그인 패스워드를 사용하지 않는 경우
2	로그인 패스워드 길이가 9자 이하인 경우
3	패스워드에 문자 또는 숫자를 연속한 단어가 포함되어 있지 않은 경우

[표] 4 로그인 패스워드 안전성 여부 점검 "취약" 원인

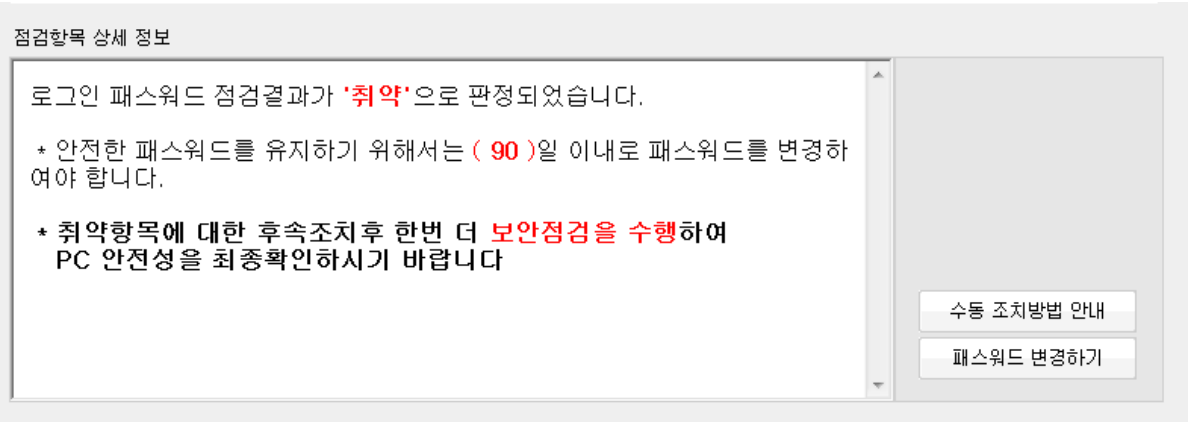
□ 이 경우 "패스워드 변경하기"버튼을 클릭하여 패스워드를 재설정해야 합니다.



[그림] 22 패스워드 변경하기 화면

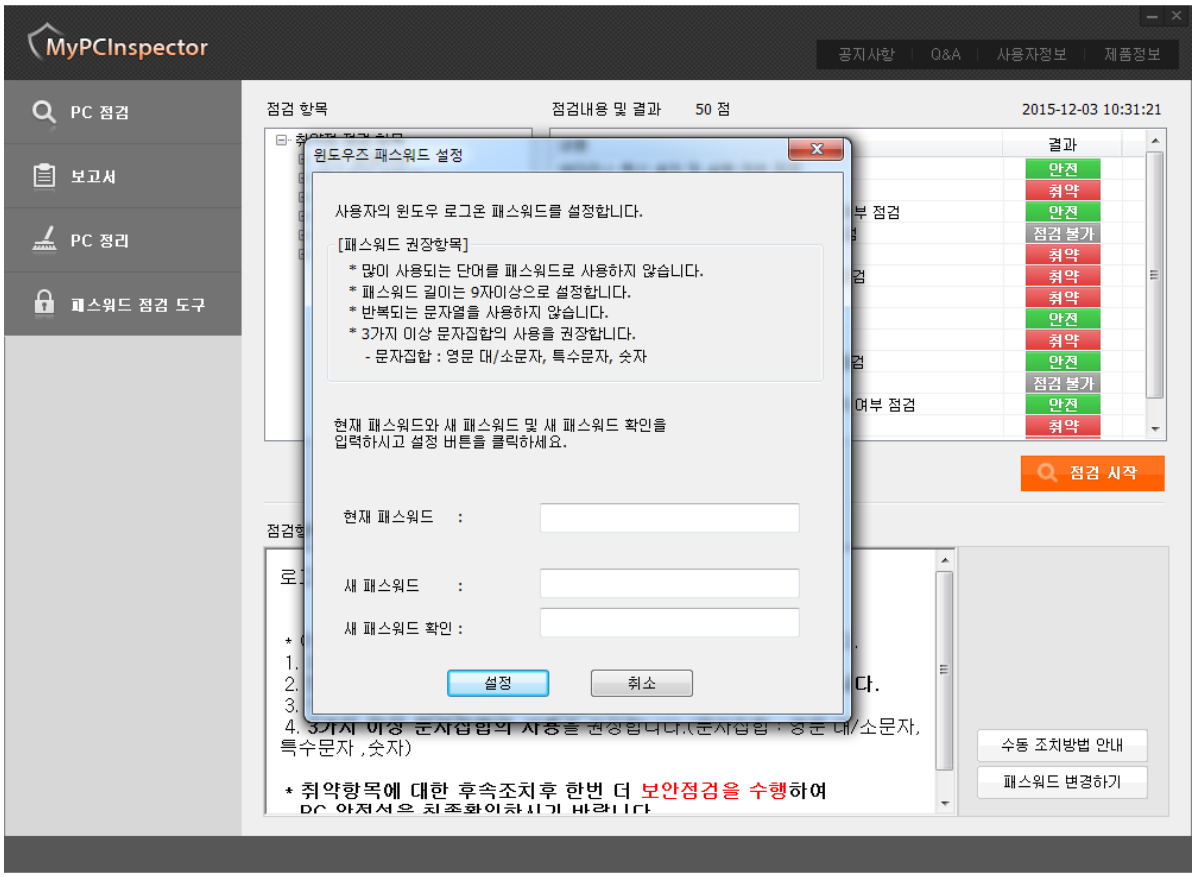
3.3.6 로그인 패스워드 분기 1회 이상 변경 여부 점검

□ 로그인 패스워드 분기 1회 이상 변경 여부 점검이 취약으로 판정되는 경우는 윈도우 로그인 패스워드를 90일 이상 변경하지 않은 경우에 해당됩니다.



[그림] 23 로그인 패스워드 분기 1회 이상 변경 여부 점검 취약 원인

□ 이 경우 패스워드 변경하기"버튼을 클릭하여 패스워드를 재설정해야 합니다.



[그림] 24 패스워드 변경하기 화면

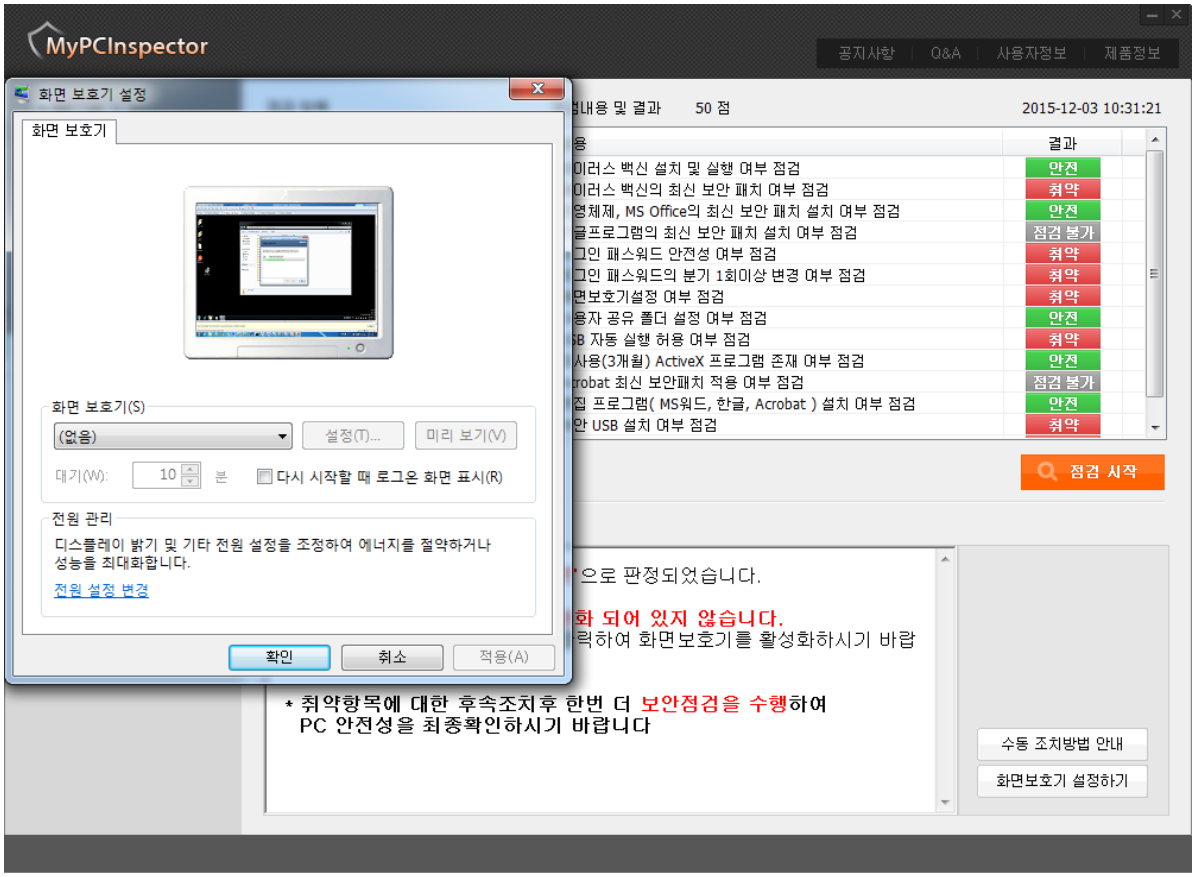
3.3.7 화면보호기 설정 여부 점검

□ 화면 보호기 설정 여부 점검이 취약으로 판정되는 경우는 다음과 같습니다.

번호	화면보호기 설정 여부 점검 "취약" 원인
1	화면보호기가 활성화 되어 있지 않은 경우
2	부재시 화면보호기 자동실행시간이 10분 초과인 경우
3	화면보호기 해제를 위한 비밀번호를 사용하고 있지 않은 경우

[표] 5 화면보고시 안전성 여부 점검 "취약" 원인

□ 이 경우 "화면보호기 설정"버튼을 클릭하여 화면보호기를 설정해야 합니다.

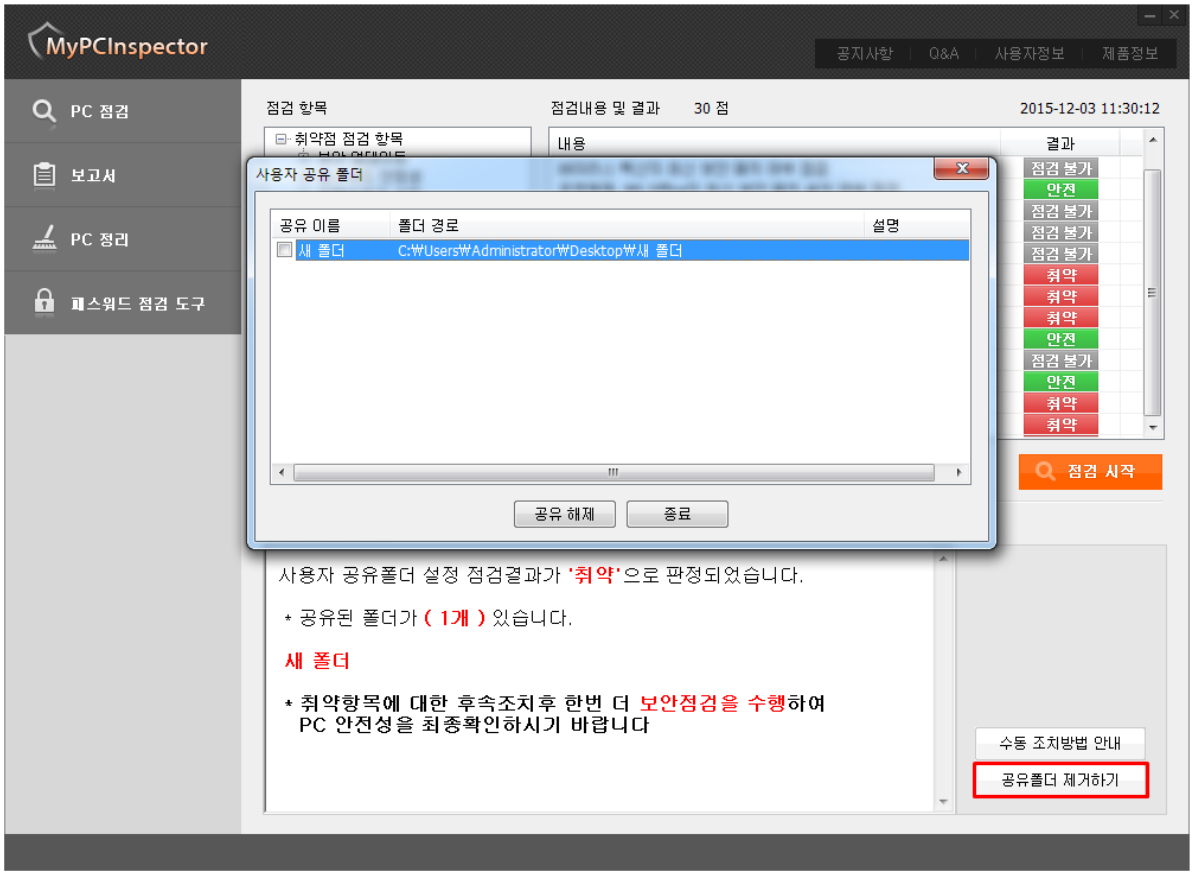


[그림] 25 화면보호기 설정하기 화면

□ 화면보호기 설정창에서 정상적으로 설정 변경을 하고 확인을 해야 합니다.

3.3.8 사용자 공유 폴더 설정 여부 점검

□ 사용자 공유 폴더 설정 여부 점검 항목이 취약으로 판정된 경우 "공유폴더 제거하기"버튼을 클릭합니다. 그러면 현재 설정된 공유폴더를 확인할 수 있습니다.

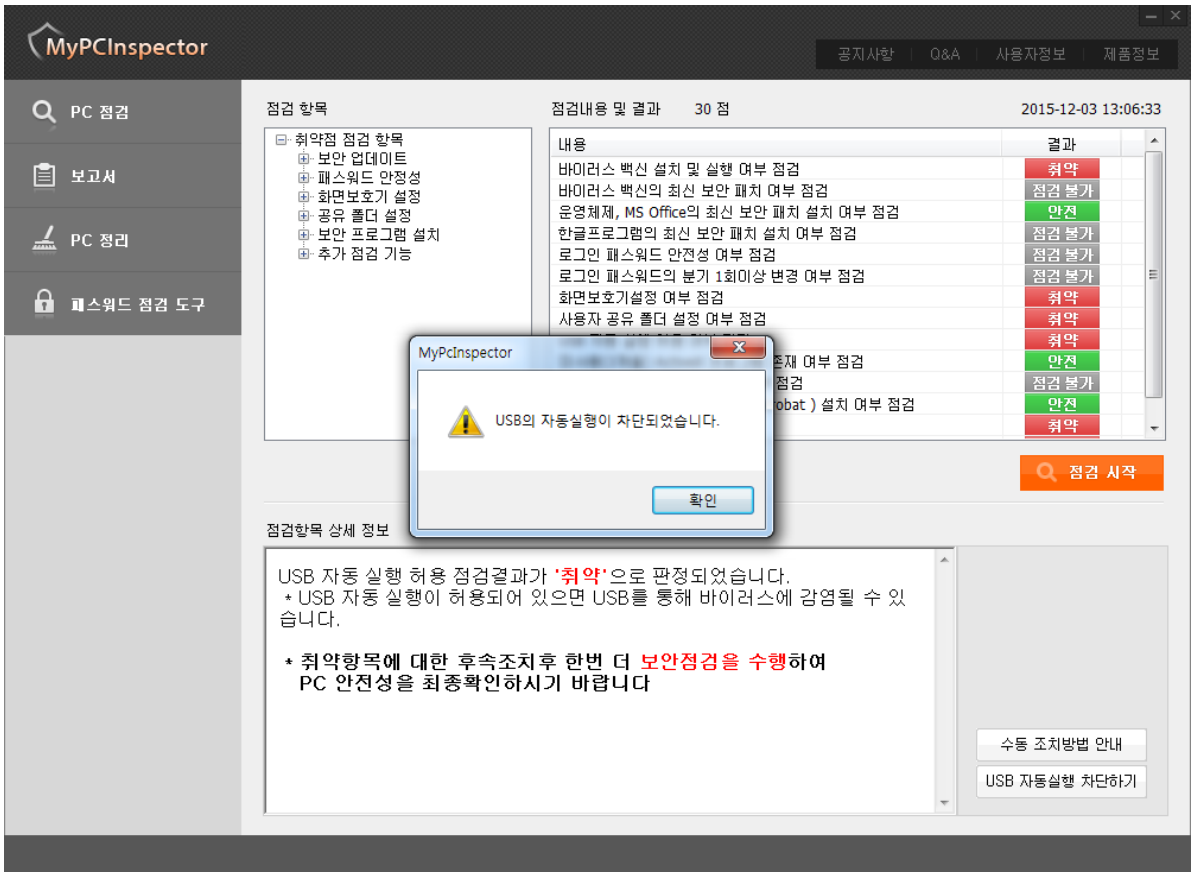


[그림] 26 공유폴더 제거하기 화면

□ "모든 공유 폴더 공유 해제"를 클릭하여 시스템에 설정된 모든 공유 폴더를 해제해야 합니다.

3.3.9 USB 자동 실행 허용 여부 점검

□ USB 자동 실행 허용 여부 점검 항목이 취약으로 판정된 경우는 USB 자동 실행 차단하기" 버튼을 클릭하여 USB 자동실행을 차단해야 합니다.

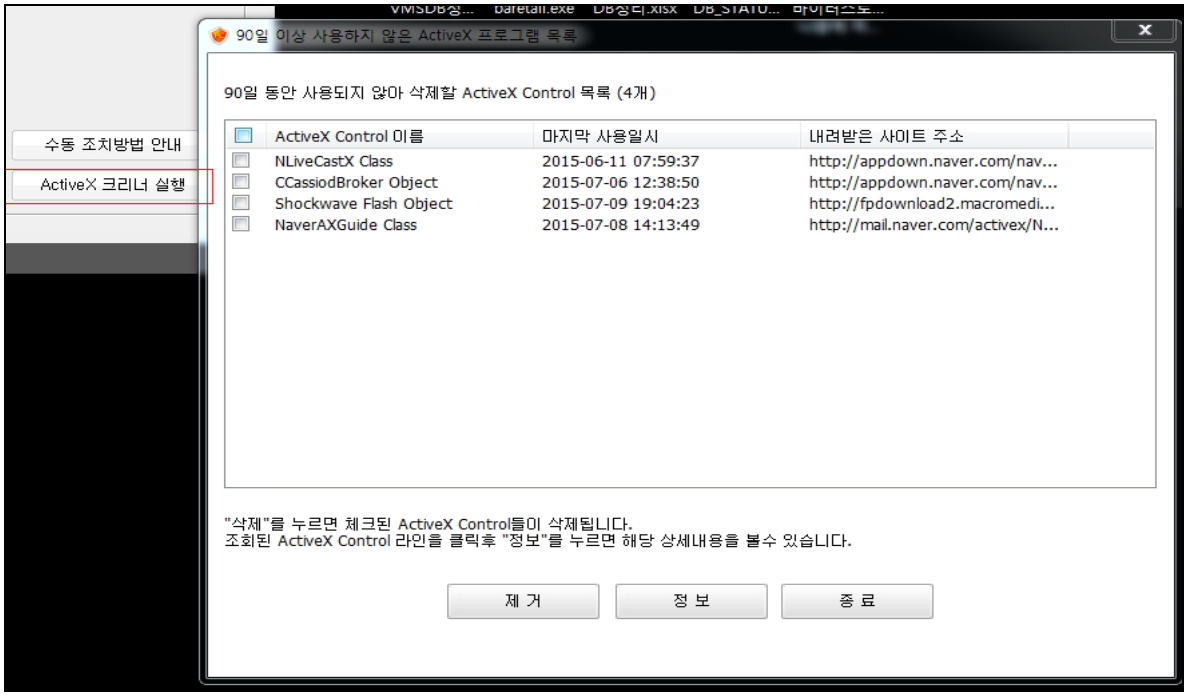


[그림] 27 USB 자동실행 차단 화면

3.3.10 미사용(3개월) ActiveX 프로그램 존재 여부 점검

□ 미사용(3개월) ActiveX 프로그램 존재 여부 점검 항목이 취약으로 판정된 경우 "ActiveX 크리너 실행" 버튼을 클릭합니다. 그러면 3개월 이상 사용하지 않은 ActiveX 프로그램을 확인 할 수 있는 창이 생성됩니다.

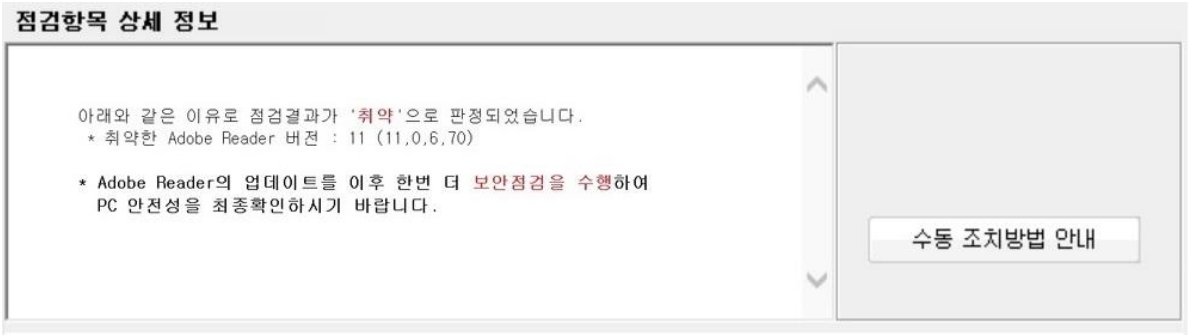
□ [그림] 28에서 제거하고자 하는 ActiveX 프로그램을 선택 후 "제거" 버튼을 클릭하여 ActiveX를 제거합니다.



[그림] 28 ActiveX 제거 화면

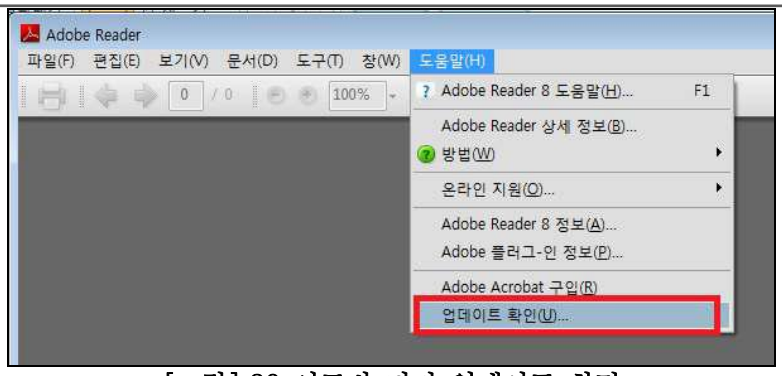
3.3.11 PDF 프로그램의 최신 보안 패치 설치 여부

□ PDF 프로그램의 최신 보안 패치 설치 여부 점검 항목이 취약으로 판정된 경우 어도비 리더 프로그램의 업데이트가 필요합니다. [그림] 29의 취약원인에서 PC에 설치된 어도비 리더의 버전을 확인하고 업데이트를 수행합니다.



[그림] 29 PDF 프로그램의 최신 보안 패치 설치 여부 점검 취약 원인

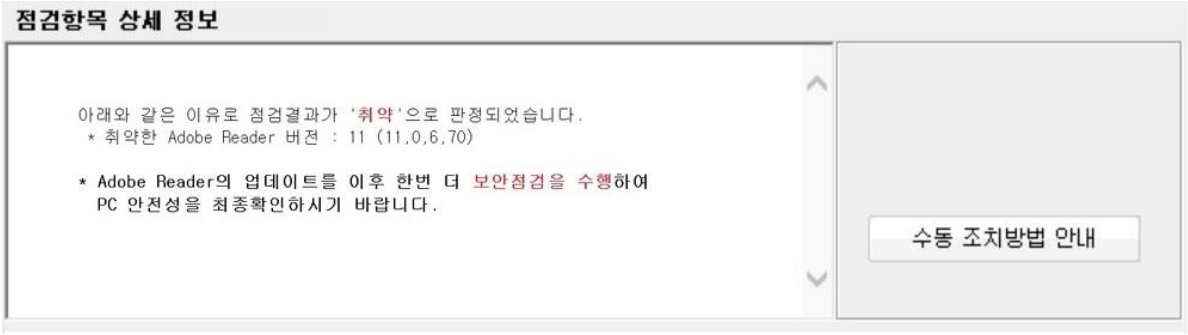
□ 업데이트 방법은 다음과 같이 어도비 리더 프로그램 실행 후 [도움말]-[업데이트 확인] 메뉴를 이용하면 됩니다.



[그림] 30 어도비 리더 업데이트 화면

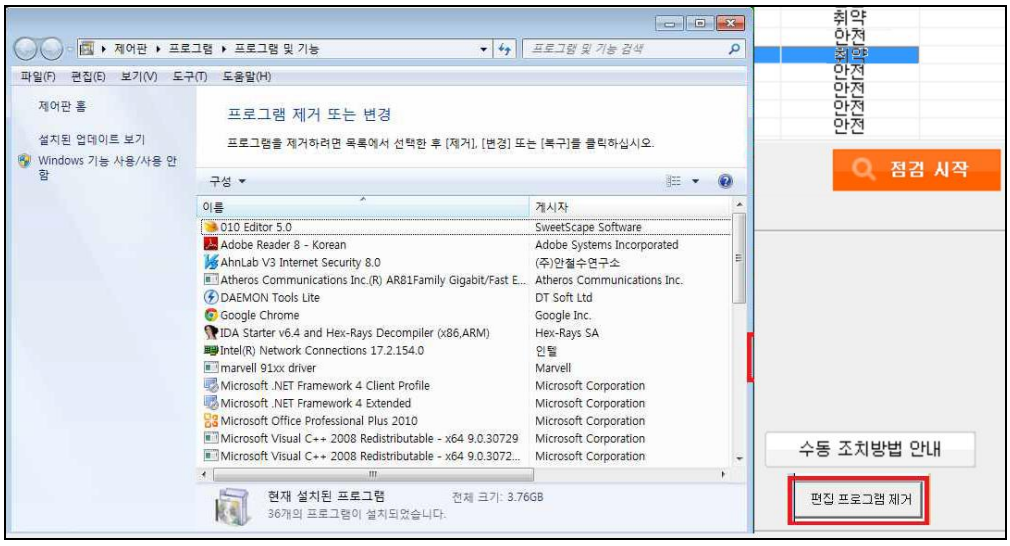
3.3.12 편집 프로그램(MS워드, 한글, PDF, 엑셀, PPT) 설치 여부 점검

□ 편집 프로그램(MS워드, 한글, PDF, 엑셀, PPT) 설치 여부 점검 항목이 취약으로 판정된 경우는 다음과 같이 관리자가 허용하지 않은 편집프로그램이 설치되어 있기 때문입니다.



[그림] 31 편집 프로그램(MS워드, 한글, PDF) 설치 여부 점검 항목 취약 원인

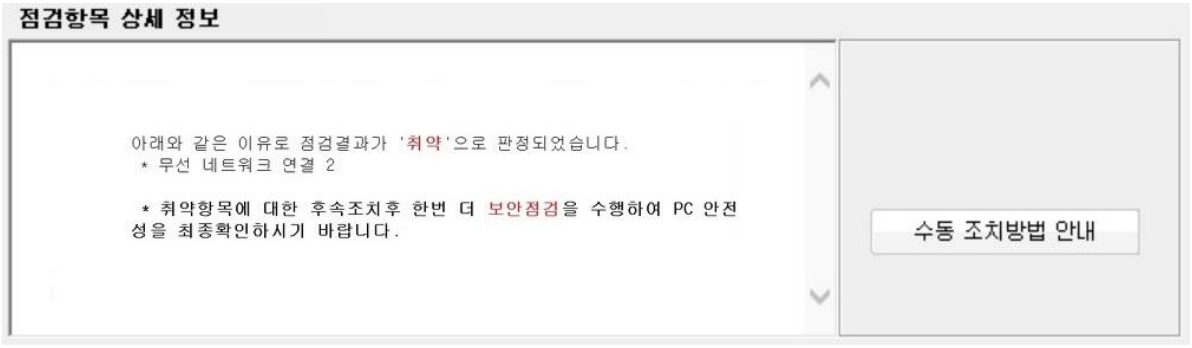
□ "편집 프로그램 제거" 버튼을 클릭하면 "프로그램 제거 또는 변경"창이 생성 됩니다. 프로그램 제거 기능으로 해당 편집 프로그램을 제거해야 합니다.



[그림] 32 편집 프로그램 제거

3.3.13 무선랜카드 설치 여부 점검

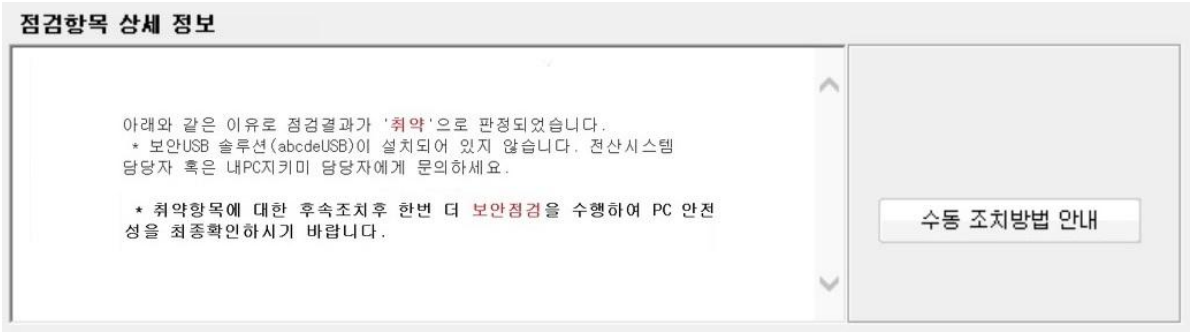
□ 무선랜카드 설치 여부 점검 항목이 취약으로 판정된 경우 다음과 같이 현재 PC에 설치된 무선랜카드가 설치되어 있는 경우이며 해당 무선랜카드를 물리적으로 제거 해야합니다.



[그림] 33 무선랜카드 설치 여부 점검 취약 원인

3.3.14 보안USB 설치 여부 점검

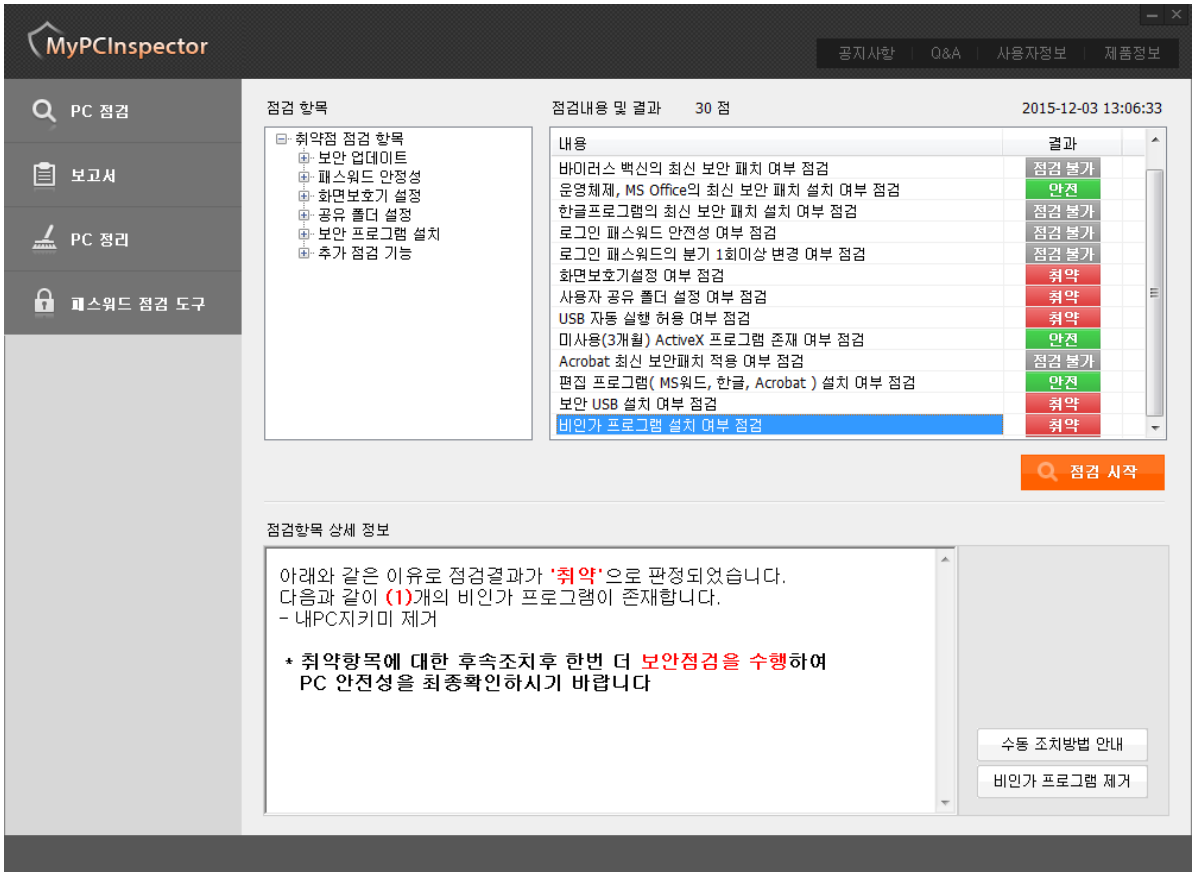
□ 보안USB 설치 여부 점검 항목이 취약으로 판정된 경우는 다음과 같이 기관에서 설치해야 하는 보안USB가 설치 되지 않은 경우이며 해당 보안USB를 설치해야 합니다.



[그림] 34 보안 USB 솔루션 미설치 취약 원인

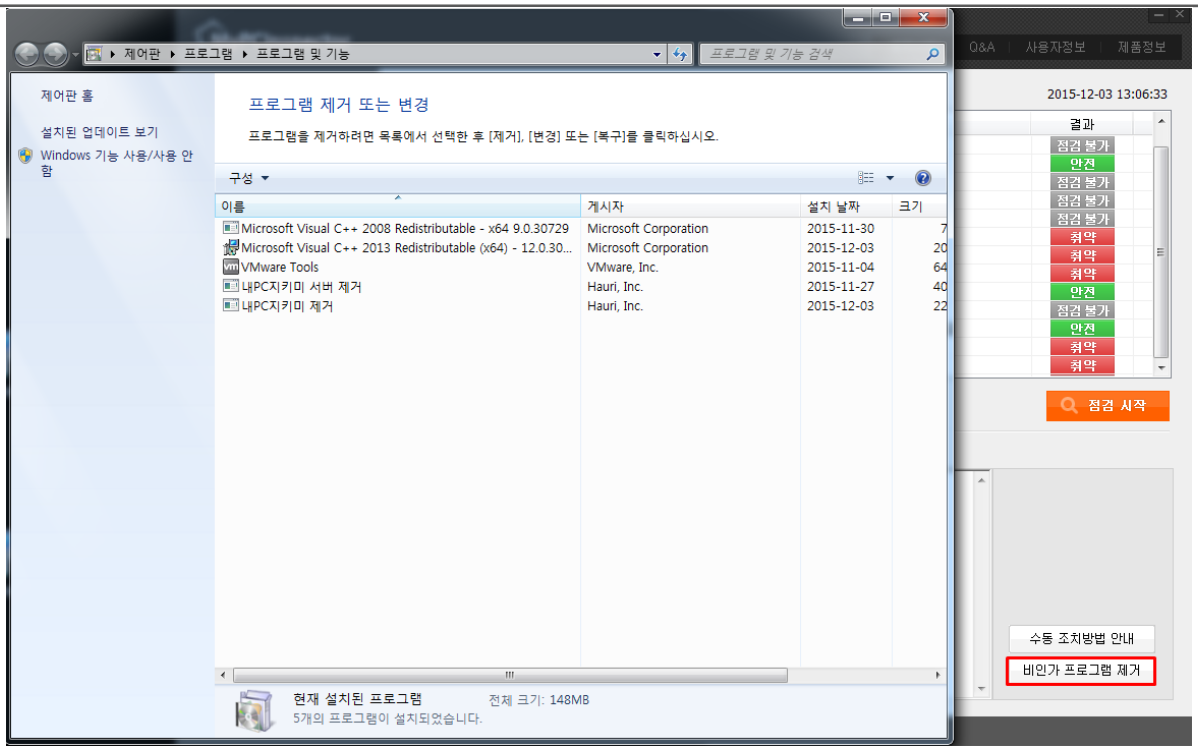
3.3.15 비인가 프로그램 설치 여부

□ 비인가 프로그램 설치 여부 점검 항목이 취약으로 판정된 경우 다음과 같이 비인가 프로그램이 설치되어 있기 때문입니다.



[그림] 35 비인가 프로그램 설치 여부 점검 항목 취약 원인

□ "비인가 프로그램 제거" 버튼을 클릭하면 "프로그램 제거 또는 변경"창이 생성됩니다. 프로그램 제거 기능으로 비인가 프로그램을 제거해야 합니다.

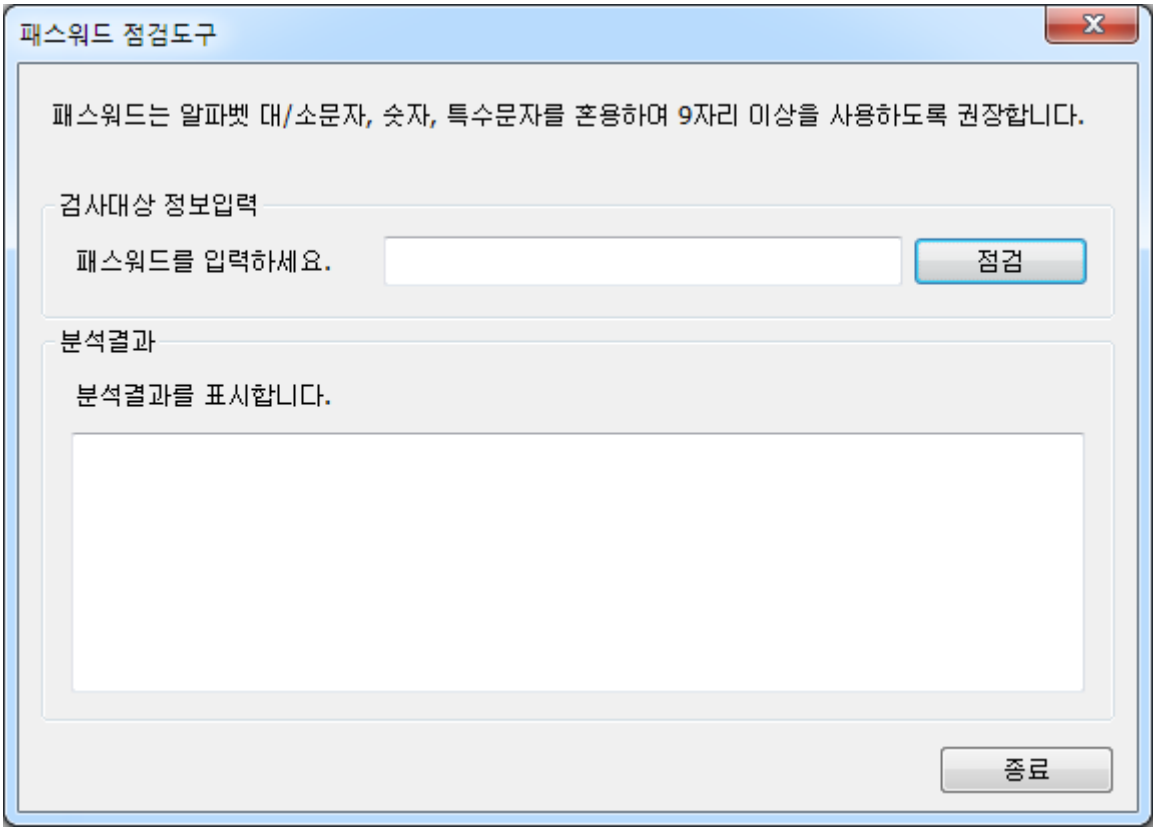


[그림] 36 비인가 프로그램 제거

3.4 기타기능

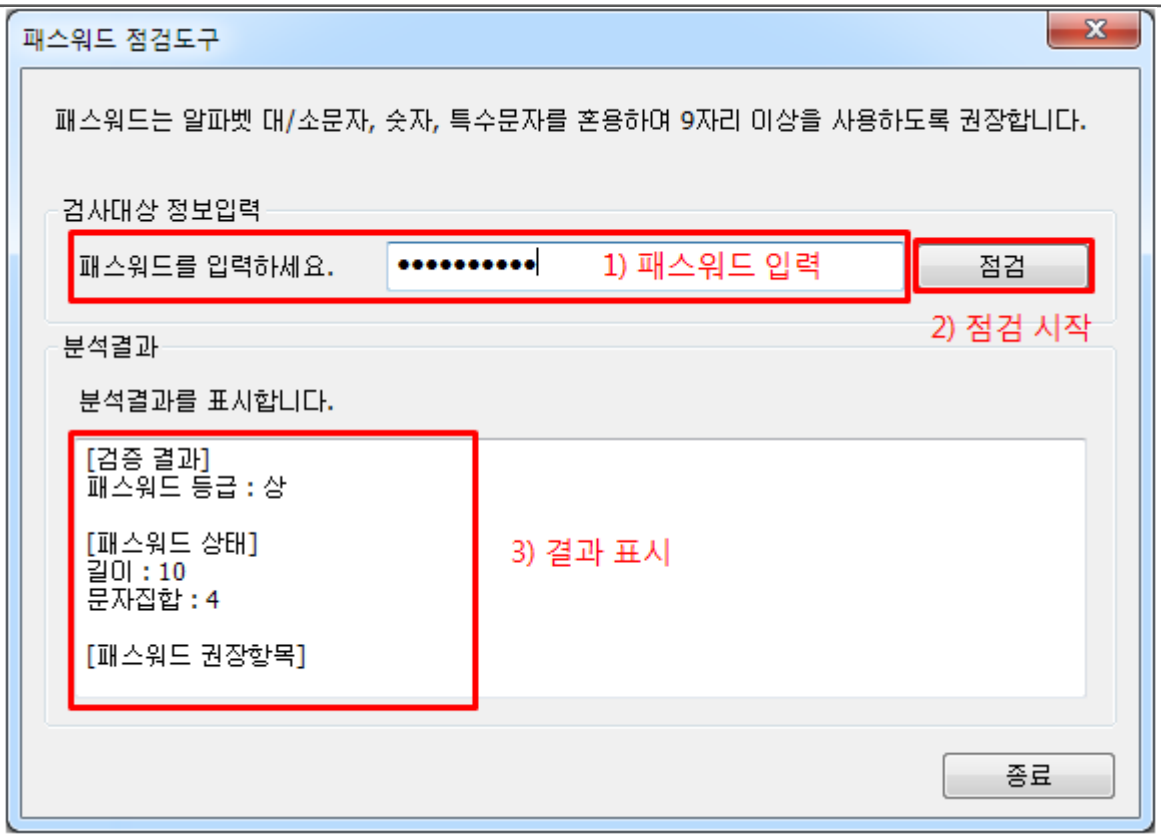
3.4.1 패스워드 점검기능

□ 프로그램 메인화면 메뉴에서 "패스워드 점검도구" 버튼을 클릭하면 다음과 같이 패스워드 점검도구 창이 생성됩니다.



[그림] 37 패스워드 점검도구 실행화면

□ 패스워드 입력창에 패스워드를 입력하고 "점검" 버튼을 클릭합니다. 그러면 패스워드의 점검결과가 "분석결과"에 표시됩니다.



[그림] 38 패스워드 점검 기능 수행

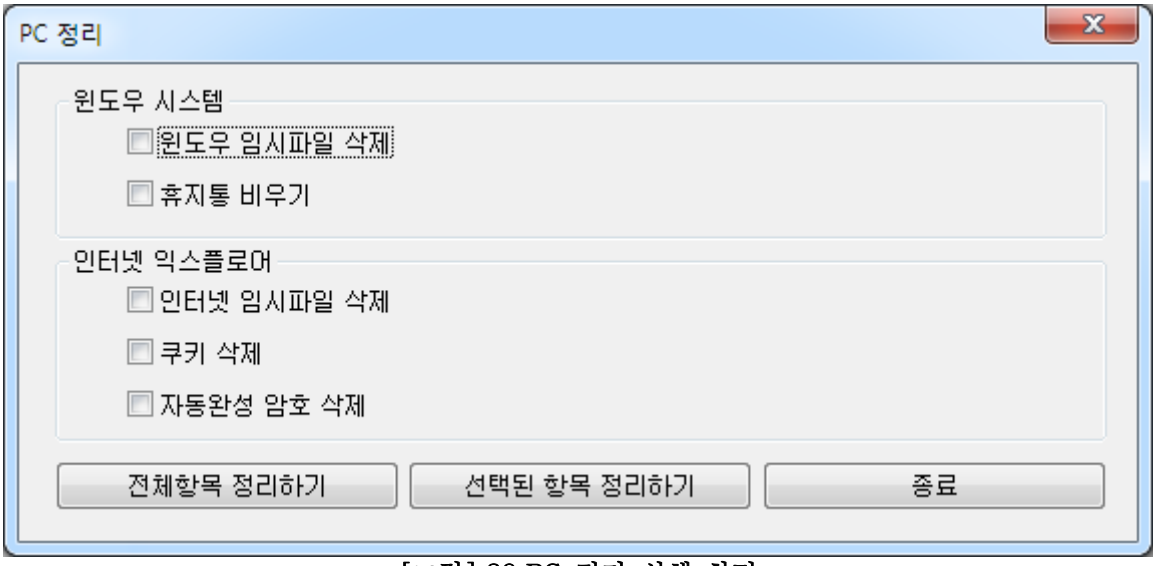
□ 분석 결과에 표시되는 내용에 대한 자세한 설명은 다음과 같습니다.

항목	설명	내용
[검증 결과]	패스워드 등급 표시	최상/상/중/하
[패스워드 상태]	패스워드 길이 표시	길이를 숫자로 표시
	패스워드 문자집합 개수 표시 (영문 대/소문자/숫자/특수문자)	문자집합 개수를 숫자로 표시
[패스워드 취약항목]	취약항목에 대한 원인 표시	▪ 해킹에 이용되는 사전파일에 패스워드가 포함되어 있습니다. ▪ 패스워드의 길이가 X 입니다.(8자 이상권장) ▪ 반복되는 문자열이 포함되어 있습니다. ▪ 사용된 문자 집합의 종류가 X가지입니다.

[표] 6 패스워드 점검 결과 표시 내용

3.4.2 PC 정리 기능

□ 프로그램 메인화면 메뉴에서 "PC 정리" 버튼을 클릭하면 다음과 같은 PC 정리창 이 생성됩니다.



[그림] 39 PC 정리 실행 화면

□ 원하는 기능을 선택합니다.

○ 전체항목 정리하기: 5가지 전체 항목에 대해 PC 정리를 수행합니다.

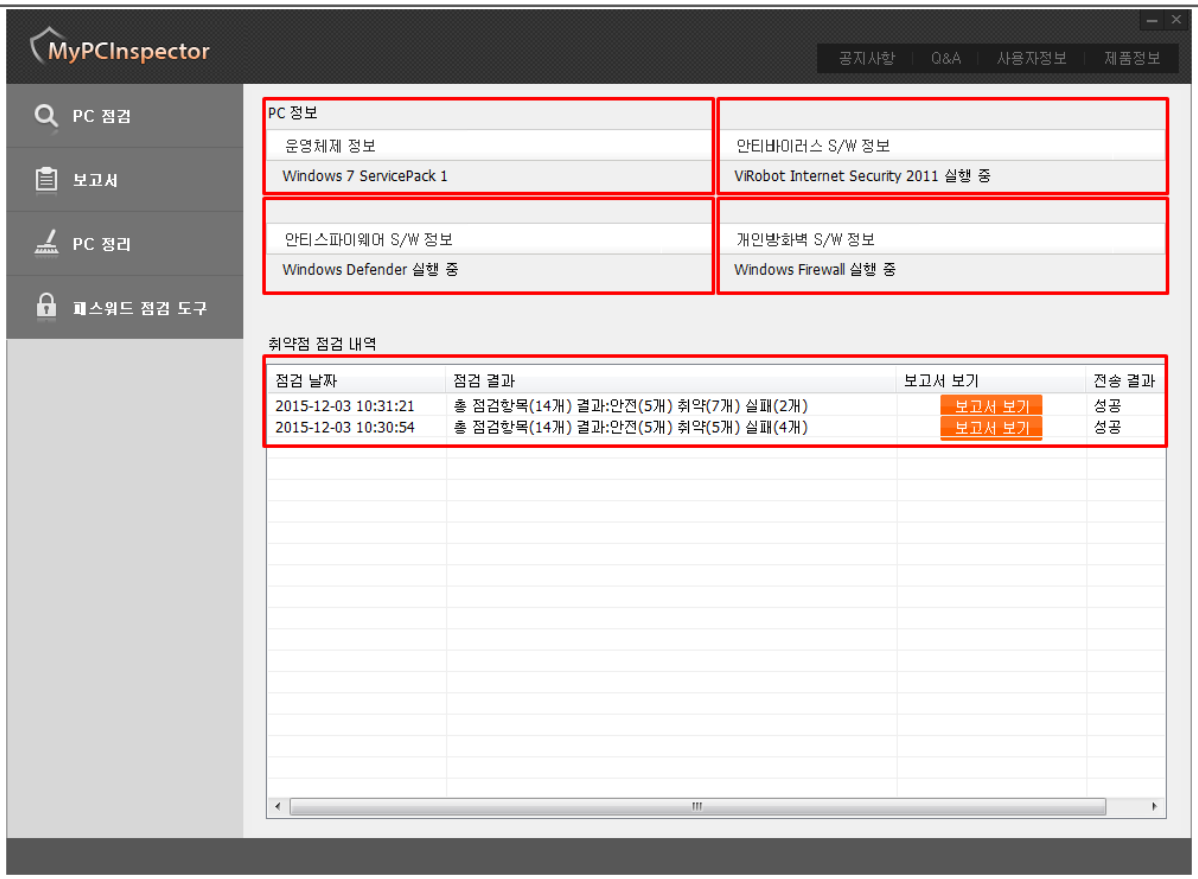
○ 선택항목 정리하기: 선택된 항목에 대해 PC 정리를 수행합니다.

○ 종료: PC 정리를 종료합니다.

3.4.3 보고서 보기 기능

□ 보고서는 사용자 정보 및 점검 결과 상세내역을 보여주는 기능입니다.

□ 프로그램 메인화면 메뉴에서 "보고서 보기" 버튼을 클릭합니다. 그러면 다음과 같은 화면이 표시됩니다.



[그림] 40 보고서 보기 화면

□ 표시되는 내용에 대한 설명은 다음과 같습니다.

① 운영체제 버전 정보를 표시합니다.

② 안티스파이웨어 소프트웨어 정보를 표시합니다.

③ 안티바이러스 소프트웨어 정보를 표시합니다.

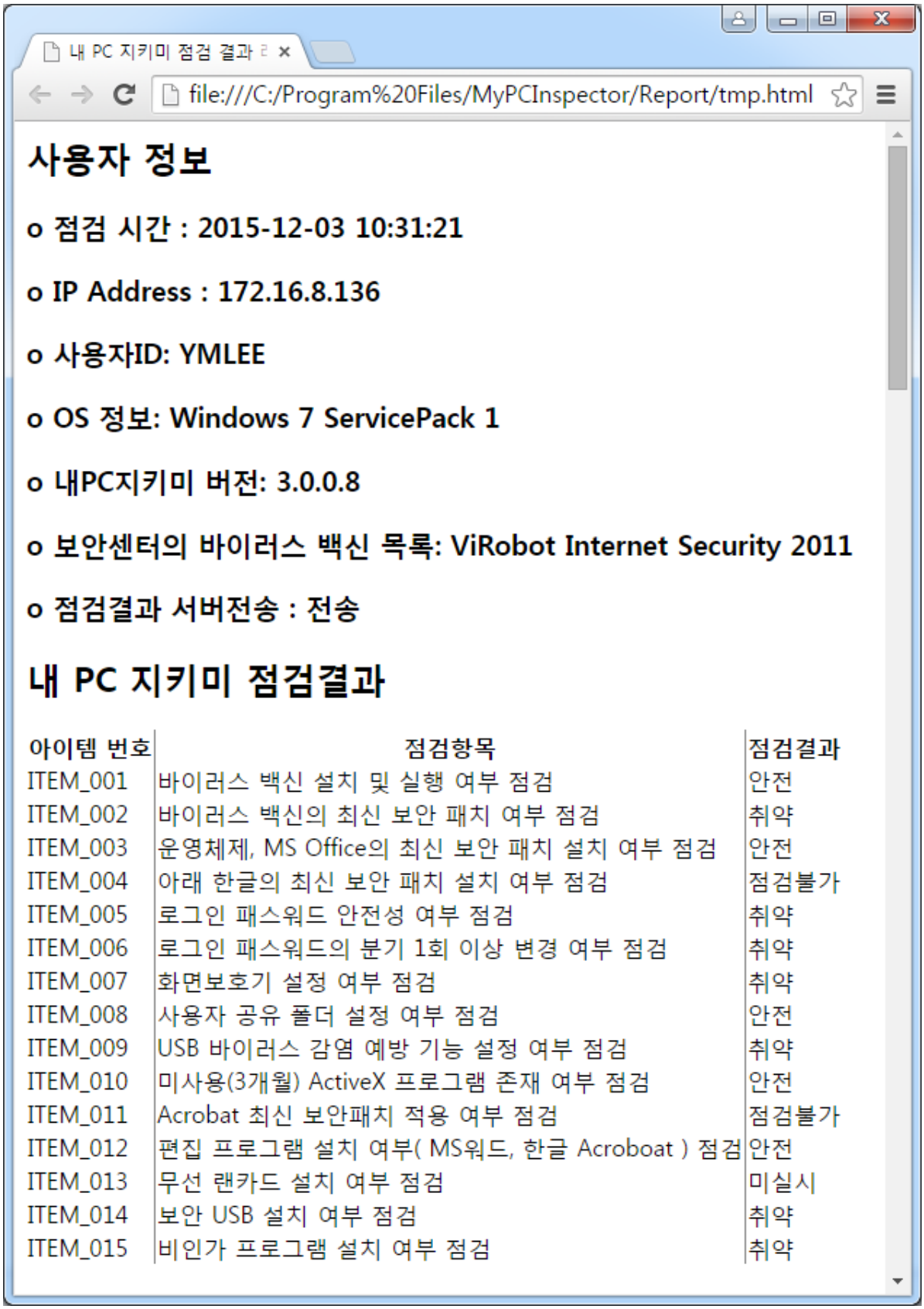
④ 개인방화벽 소프트웨어 정보를 표시합니다.

⑤ PC 점검 결과 요약 정보를 표시합니다.(점검 시간, 점검항목 개수, 안전항목 개수, 취약항목 개수, 점검불가 개수)

⑥ "보고서 보기" 클릭시 사용자 정보 및 PC 점검 결과 세부 내용을 표시합니다.

⑦ 점검결과의 서버 전송 여부를 표시합니다.(전송 결과: "성공", "실패")

□ [그림] 40에서 "보고서 열기" 버튼을 클릭하면 [그림] 41과 같은 보고서를 확인 할 수 있습니다.



아이템 번호	점검항목	점검결과
ITEM_001	바이러스 백신 설치 및 실행 여부 점검	안전
ITEM_002	바이러스 백신의 최신 보안 패치 여부 점검	취약
ITEM_003	운영체제, MS Office의 최신 보안 패치 설치 여부 점검	안전
ITEM_004	아래 한글의 최신 보안 패치 설치 여부 점검	점검불가
ITEM_005	로그인 패스워드 안전성 여부 점검	취약
ITEM_006	로그인 패스워드의 분기 1회 이상 변경 여부 점검	취약
ITEM_007	화면보호기 설정 여부 점검	취약
ITEM_008	사용자 공유 폴더 설정 여부 점검	안전
ITEM_009	USB 바이러스 감염 예방 기능 설정 여부 점검	취약
ITEM_010	미사용(3개월) ActiveX 프로그램 존재 여부 점검	안전
ITEM_011	Acrobat 최신 보안패치 적용 여부 점검	점검불가
ITEM_012	편집 프로그램 설치 여부(MS워드, 한글 Acroboat) 점검	안전
ITEM_013	무선 랜카드 설치 여부 점검	미실시
ITEM_014	보안 USB 설치 여부 점검	취약
ITEM_015	비인가 프로그램 설치 여부 점검	취약

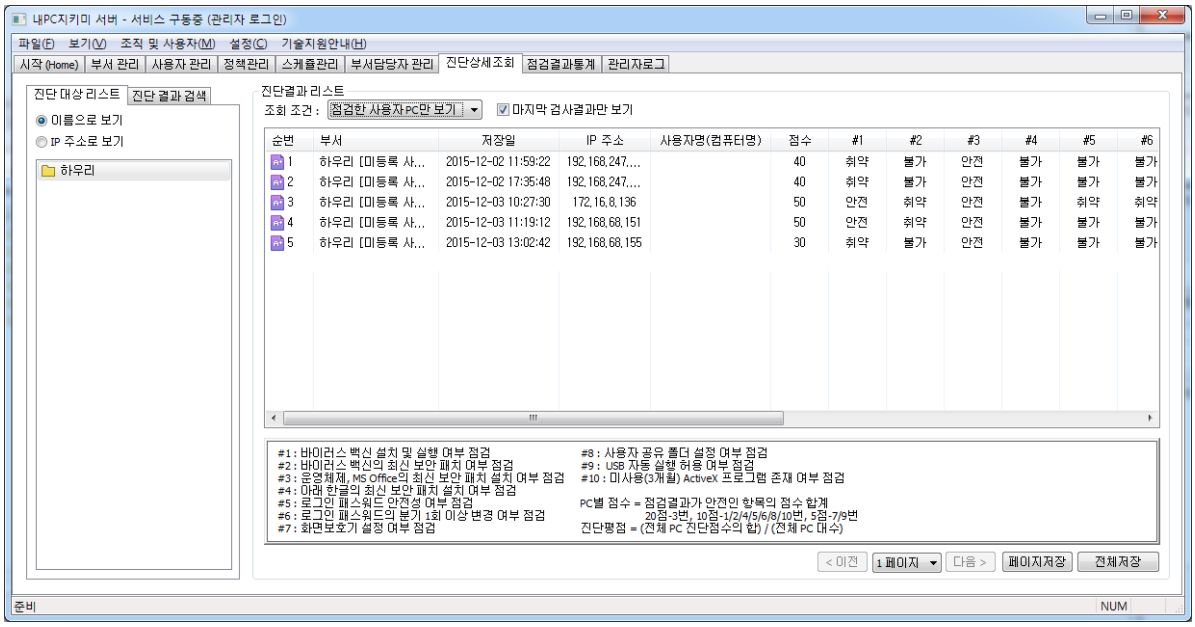
[그림] 41 PC점검 결과 보고서

4. 내PC지키미 관리자 운영

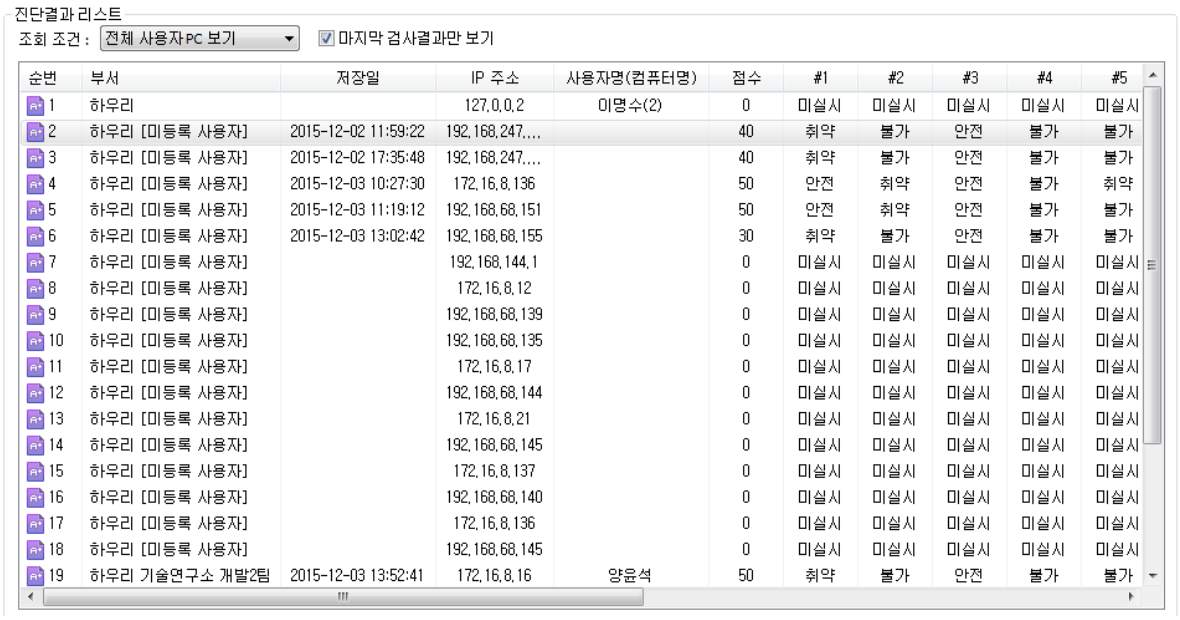
4.1 내PC지키미 Console 주요 기능

4.1.1 취약점 점검 결과 통계

□ Console 메뉴에서 [그림] 42와 같이 "관리 탭" → "진단상세조회"을 클릭하면 오른쪽 조직도에서 선택한 부서의 취약점 점검 통계를 [그림] 43처럼 볼 수 있습니다.

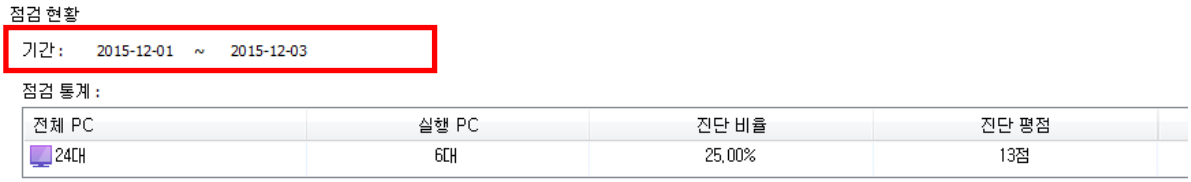


[그림] 42 취약점 점검 통계 결과 실행



[그림] 43 취약점 점검 통계 결과 전체화면

□ 조회기간의 기본값은 [그림] 44처럼 조회시작일은 콘솔이 실행된 달의 1일이고, 조회종료일은 콘솔의 실행 일자로 설정됩니다.


점검 현황

기간 : 2015-12-01 ~ 2015-12-03

점검 통계 :

전체 PC	실행 PC	진단 비율	진단 평점
24대	6대	25,00%	13점

[그림] 44 취약점 점검 통계 날짜 지정 화면

○ 전체 PC: 선택한 조직의 PC 수량
○ 실행 PC: 선택한 조직의 보안점검 실행 PC 수량
○ 진단 비율: 보안점검을 실시한 PC 의 비율(실행 PC/선택한 조직의 PC 수량 * 100)
○ 진단 평점: 보안점검을 실시한 PC 의 평균점수(실행 PC 기준)
○ 하단의 버튼 [페이지 저장] 또는 [전체 저장]을 클릭하여 파일로 결과를 저장 할 수 있습니다


상세 통계 :

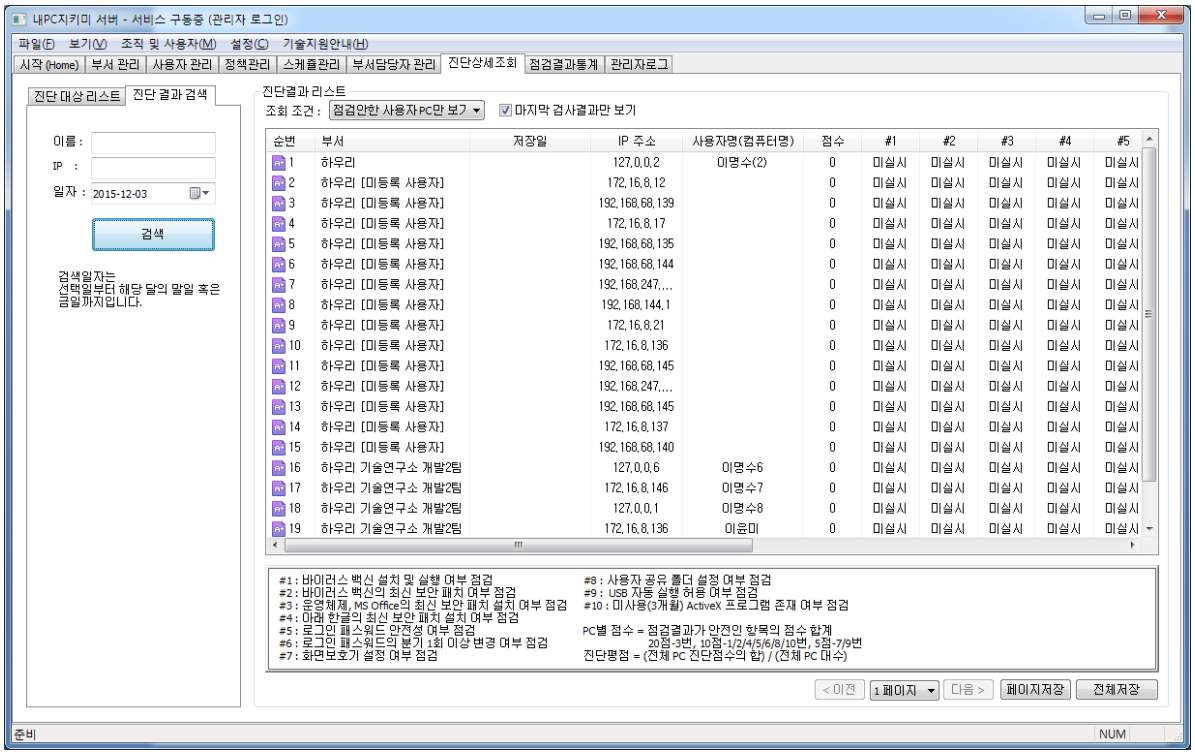
점검 항목	안전 PC	취약 PC	안전/전체	안전/실행
#1. 바이러스 백신 설치 및 실행 여부 점검	2	4	8,33%	33,33%
#2. 바이러스 백신의 최신 보안 패치 여부 점검	0	6	0,00%	0,00%
#3. 운영체제, MS Office의 최신 보안 패치 설치 여부 점검	6	0	25,00%	100,00%
#4. 아래 한글의 최신 보안 패치 설치 여부 점검	0	6	0,00%	0,00%
#5. 로그인 패스워드 안정성 여부 점검	0	6	0,00%	0,00%
#6. 로그인 패스워드의 분기 1회 이상 변경 여부 점검	0	6	0,00%	0,00%
#7. 화면보호기 설정 여부 점검	1	5	4,17%	16,67%
#8. 사용자 공유 폴더 설정 여부 점검	5	1	20,83%	83,33%
#9. USB 자동 실행 허용 여부 점검	0	6	0,00%	0,00%
#10. 미사용(3개월) ActiveX 프로그램 존재 여부 점검	6	0	25,00%	100,00%
#11. 편집프로그램(한글, MS워드, PDF) 설치 여부 점검	6	0	25,00%	100,00%
#12. 무선랜카드 점검	0	6	0,00%	0,00%
#13. 보안USB 설치여부 점검	0	6	0,00%	0,00%
#14. PDF 업데이트 여부 점검	0	6	0,00%	0,00%
#15. 비인가 프로세스 목록 점검	2	4	8,33%	33,33%

[그림] 45 취약점 점검 통계 결과 화면

○ 점검코드: 점검항목의 코드
○ 점검항목: 보안점검에 대한 제목
○ 안전 PC: 해당 보안점검을 실행한 PC 중 안전 진단을 받은 PC 의 수량
○ 취약 PC: 해당 보안점검을 실행한 PC 중 취약 진단을 받은 PC 의 수량
○ 안전/전체: 선택한 조직의 전체 PC 에 대한 안전 비율
○ 안전/실행: 선택한 조직의 보안점검을 실행한 PC 에 대한 안전 비율

4.1.2 취약점 점검 미실행 PC 관리

□ [그림] 42에서 미실행 PC 클릭시 선택한 조직에서 보안점검을 실행 하지 않은 PC의 정보를 보여줍니다.

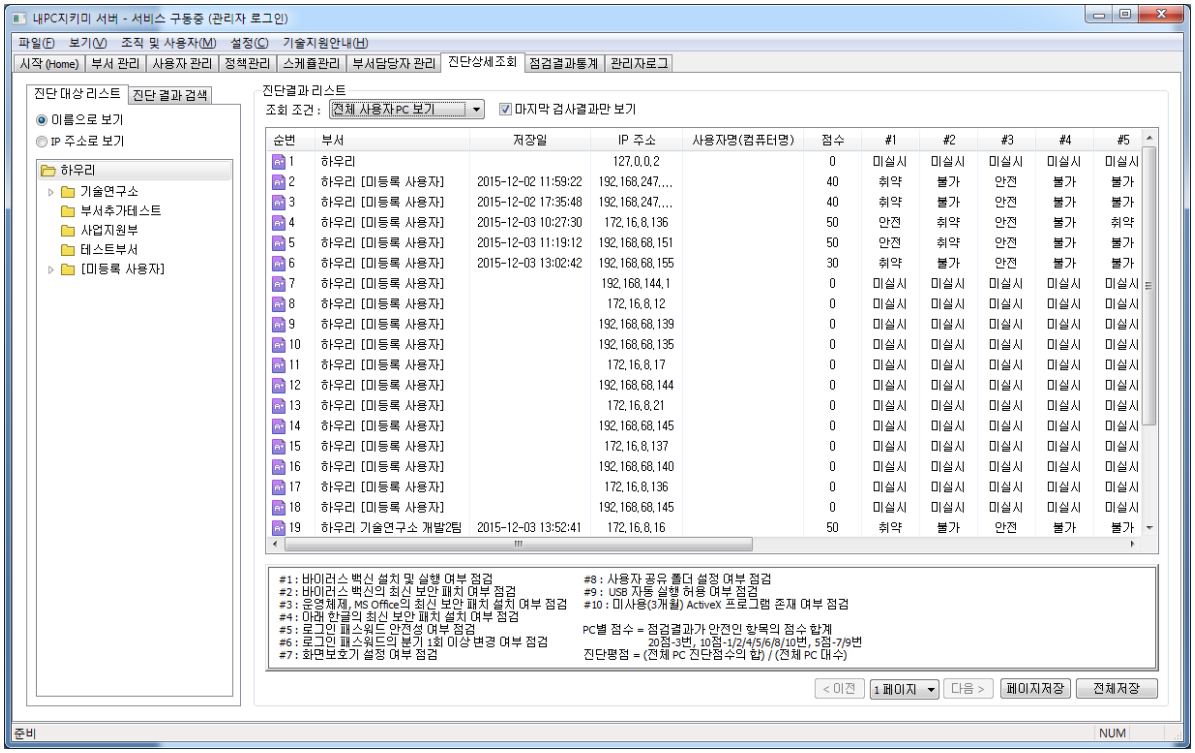


[그림] 46 취약점 점검 미실행 PC 정보 화면

□ [그림] 46에서 저장 버튼을 클릭하면 해당내용을 파일로 저장 할 수 있습니다.

4.1.3 취약점 진단 상세로그

□ [그림] 47 은 콘솔의 "관리 탭" → "진단상세조회" 선택하면 화면의 중간에 결과를 출력합니다.

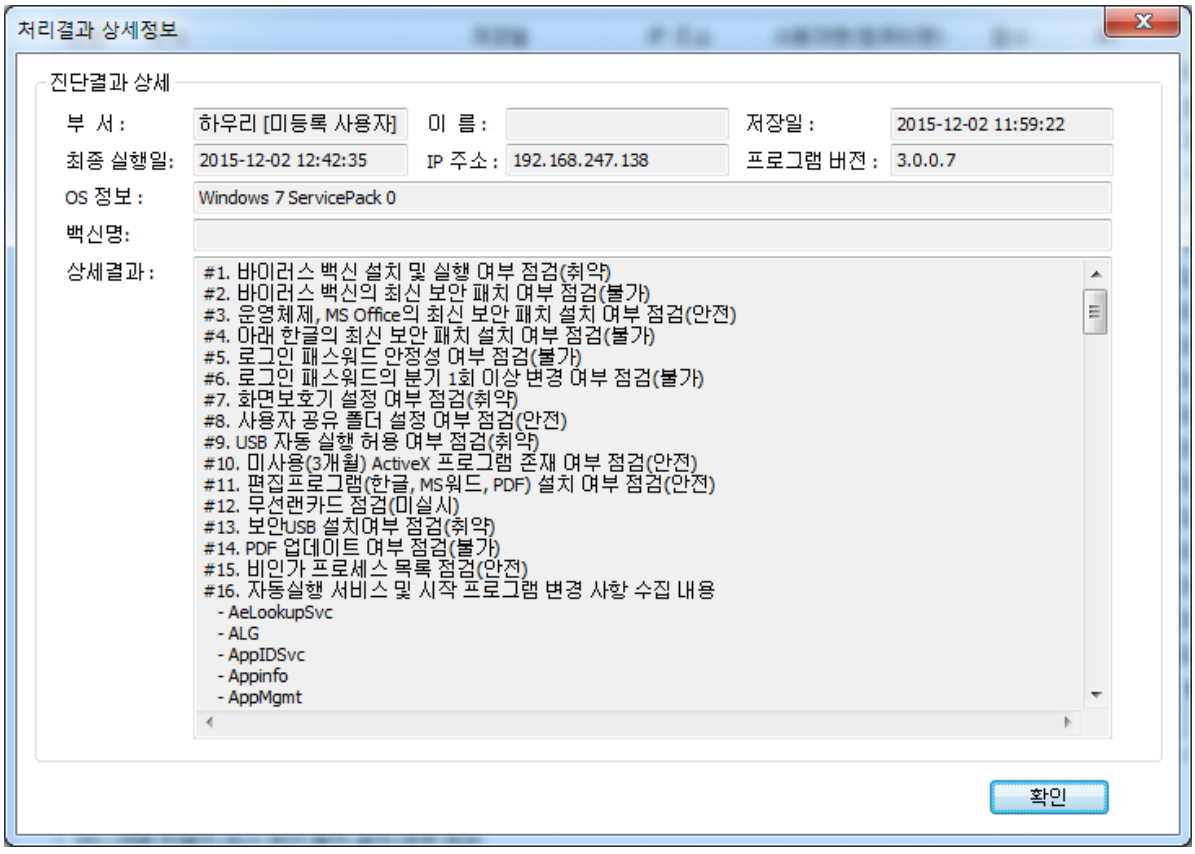


[그림] 47 취약점 진단 상세로그 화면

□ 오른쪽 조직도에 해당하는 노드들의 검사 일시와 보안점수, 점검항목의 위약여부를 [그림] 48 처럼 한눈에 볼 수 있습니다. 열람하고 싶은 노드를 마우스로 **더블 클릭하면** [그림] 49처럼 **상세내용을 볼 수 있습니다.**

순번	부서	저장일	IP 주소	사용자명(컴퓨터명)	점수	#1	#2	#3	#4	#5
1	하우리		127.0.0.2		0	미실시	미실시	미실시	미실시	미실시
2	하우리 [미등록 사용자]	2015-12-02 11:59:22	192.168.247....		40	취약	불가	안전	불가	불가
3	하우리 [미등록 사용자]	2015-12-02 17:35:48	192.168.247....		40	취약	불가	안전	불가	불가
4	하우리 [미등록 사용자]	2015-12-03 10:27:30	172.16.8.136		50	안전	취약	안전	불가	취약
5	하우리 [미등록 사용자]	2015-12-03 11:19:12	192.168.68.151		50	안전	취약	안전	불가	불가
6	하우리 [미등록 사용자]	2015-12-03 13:02:42	192.168.68.155		30	취약	불가	안전	불가	불가
7	하우리 [미등록 사용자]		192.168.144.1		0	미실시	미실시	미실시	미실시	미실시
8	하우리 [미등록 사용자]		172.16.8.12		0	미실시	미실시	미실시	미실시	미실시
9	하우리 [미등록 사용자]		192.168.68.139		0	미실시	미실시	미실시	미실시	미실시
10	하우리 [미등록 사용자]		192.168.68.135		0	미실시	미실시	미실시	미실시	미실시
11	하우리 [미등록 사용자]		172.16.8.17		0	미실시	미실시	미실시	미실시	미실시
12	하우리 [미등록 사용자]		192.168.68.144		0	미실시	미실시	미실시	미실시	미실시
13	하우리 [미등록 사용자]		172.16.8.21		0	미실시	미실시	미실시	미실시	미실시
14	하우리 [미등록 사용자]		192.168.68.145		0	미실시	미실시	미실시	미실시	미실시
15	하우리 [미등록 사용자]		172.16.8.137		0	미실시	미실시	미실시	미실시	미실시
16	하우리 [미등록 사용자]		192.168.68.140		0	미실시	미실시	미실시	미실시	미실시
17	하우리 [미등록 사용자]		172.16.8.136		0	미실시	미실시	미실시	미실시	미실시
18	하우리 [미등록 사용자]		192.168.68.145		0	미실시	미실시	미실시	미실시	미실시
19	하우리 기술연구소 개발2팀	2015-12-03 13:52:41	172.16.8.16		50	취약	불가	안전	불가	불가

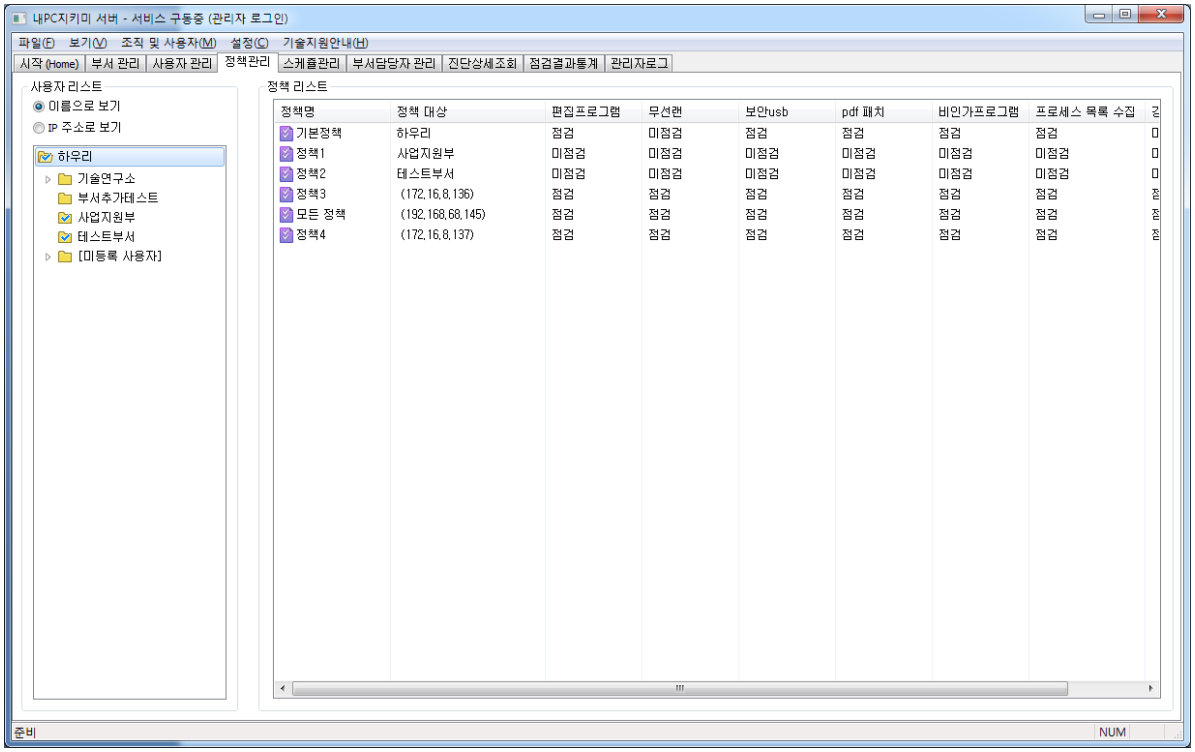
[그림] 48 취약점 진단 상세로그 화면



[그림] 49 노드의 취약점 진단 상세로그 화면

□ [그림] 48, 49에서 저장 버튼 클릭 시 결과 자료를 파일로 생성 할 수 있습니다.

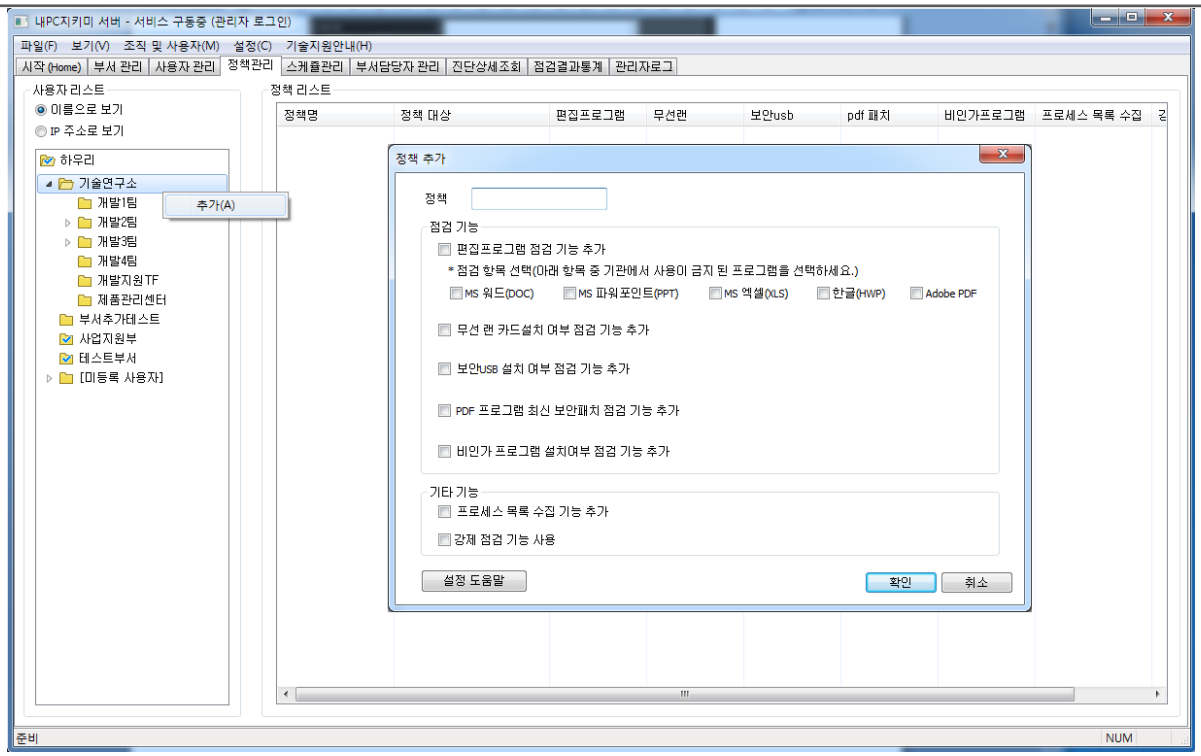
4.2 취약점 점검 정책 설정



[그림] 50 정책설정 메인 화면

4.2.1 정책 생성

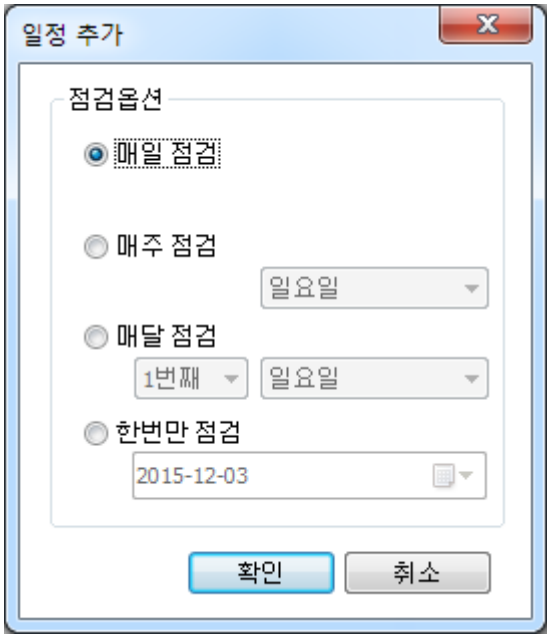
□ [그림] 50 의 화면에서 PC 보안점검정책을 선택 하고 오른쪽 상단의 [추가] 버튼을 클릭 하여 정책명과 설명을 입력하고 [확인] 버튼을 누른다. [그림] 51 참조



[그림] 51 정책설정 메인 화면

4.2.2 일반 설정

① 스케줄 설정



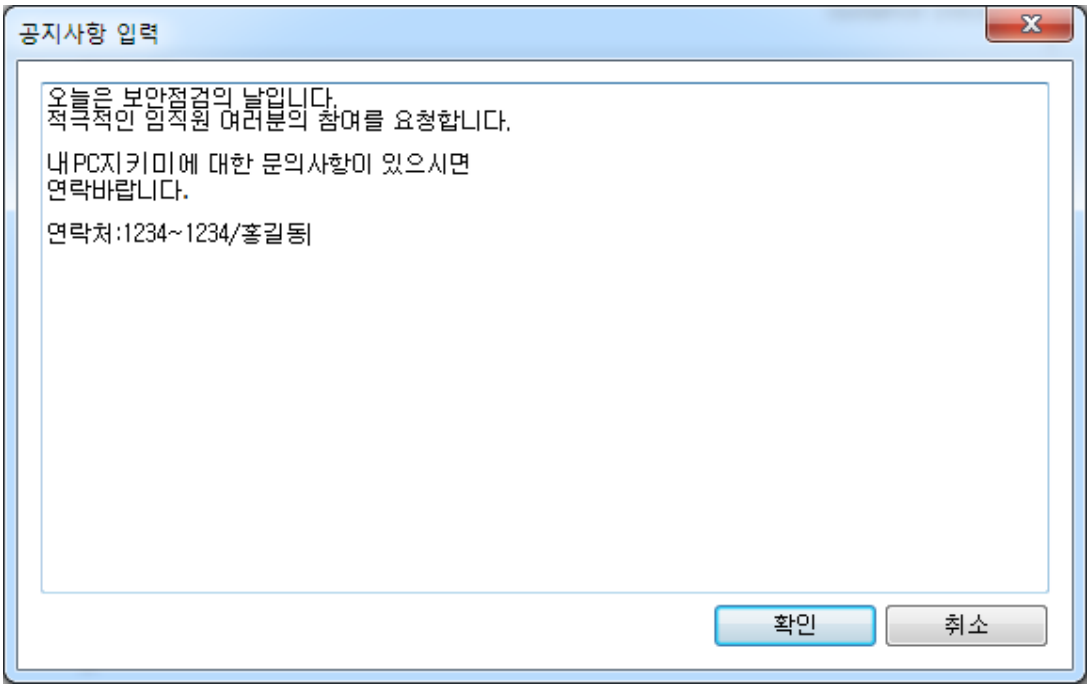
[그림] 52 스케줄 설정 화면

□ 스케줄이 등록되지 않으면 정책을 생성 할 수 없습니다. [그림] 52 화면에서 스케줄 추가 부분에 원하는 스케줄을 설정하여 추가합니다.

O 스케줄 추가: 주기에서 매달, 매주, 매일, 한번을 설정 할 수 있습니다.
매달 선택 시 시작주, 시작요일, 종료주, 종료요일을 선택합니다.
매주 선택 시 시작요일, 종료요일을 선택합니다.
매일, 한번은 시작주, 시작요일, 종료주, 종료요일을 선택 할 수 없습니다.

O 자동실행 옵션: 선택 시 사용자의 PC 에 정책 적용 시 패스워드 입력 없이 바로 취약점 점검을 실행합니다(강제검사). 미선택 시 사용자의 PC 에 정책 적용 시 화면전체에 점검시작 화면을 표시하여 사용자에게 취약점 점검을 유도합니다(수동검사).

② 공지사항



[그림] 53 공지사항 실행 화면

□ 각 에이전트에서 취약점 점검시작 시 사용자에게 작성한 공지사항을 [그림] 53 같이 보여줍니다.

③ 종료옵션

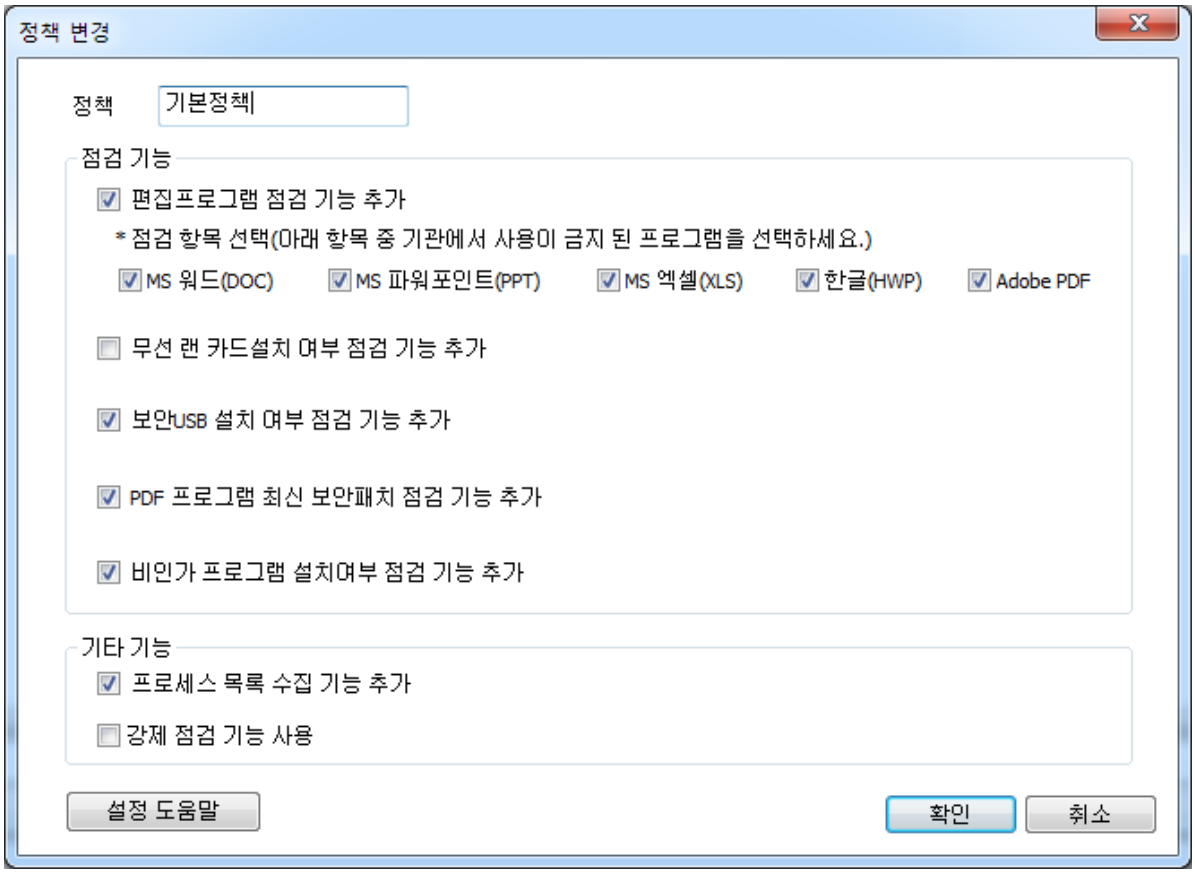
□ [그림] 52 화면에서 점수를 설정 할 수 있습니다. 각 에이전트에서 취약점점검 실행 시 설정한 점수 이상일 때 내 PC 지키미를 종료 할 수 있습니다.

④ 보안점검 시작화면 정렬

□ [그림] 52 화면에서 사용여부를 체크 할 수 있습니다. 선택 시 점검화면을 입력한 초마다 에이전트 점검화면을 최상위로 가져옵니다.

4.2.3 보안점검 항목 설정

□ 보안점검 항목 중 선택한 항목만 점검을 수행합니다.

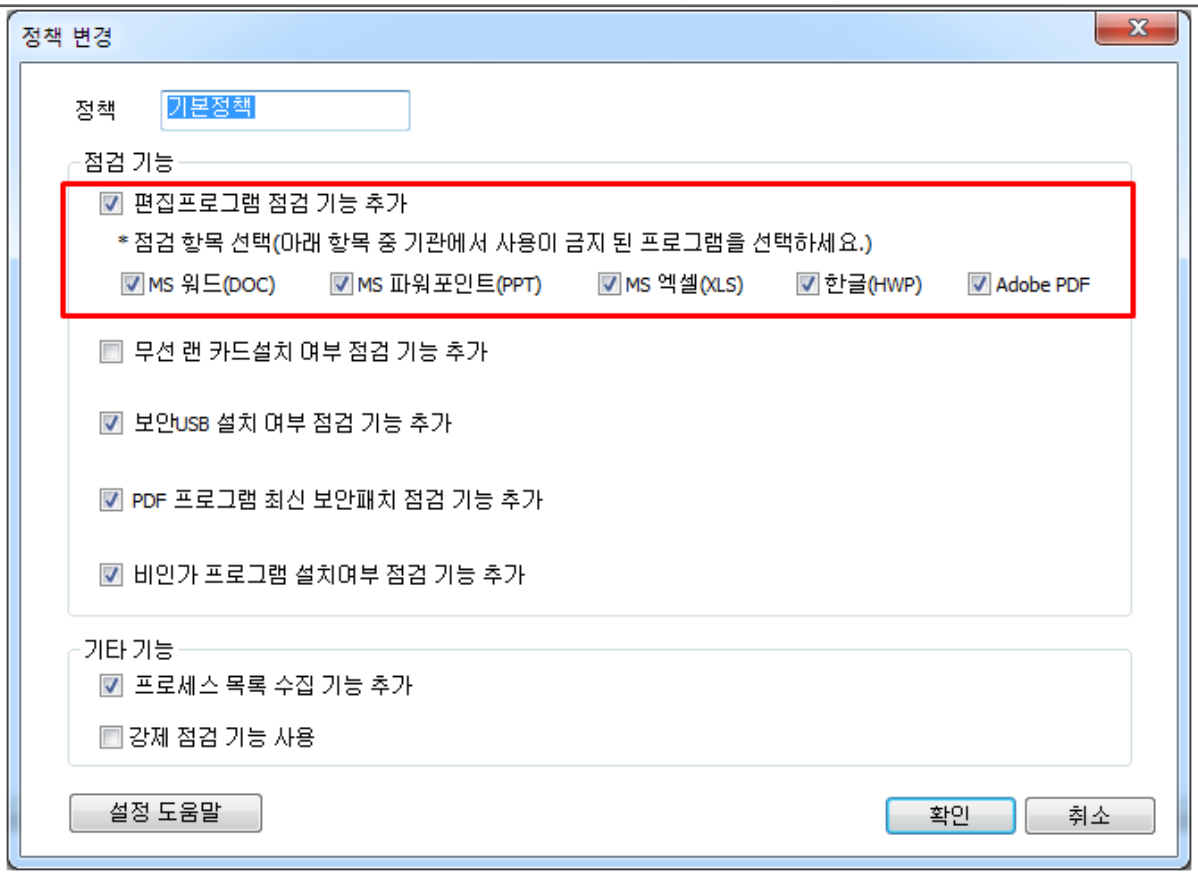


[그림] 544 보안점검 항목 선택 화면

□ 보안점검 항목 중 설정이 필요한 항목이 있습니다.

① 편집프로그램 설치 여부 점검

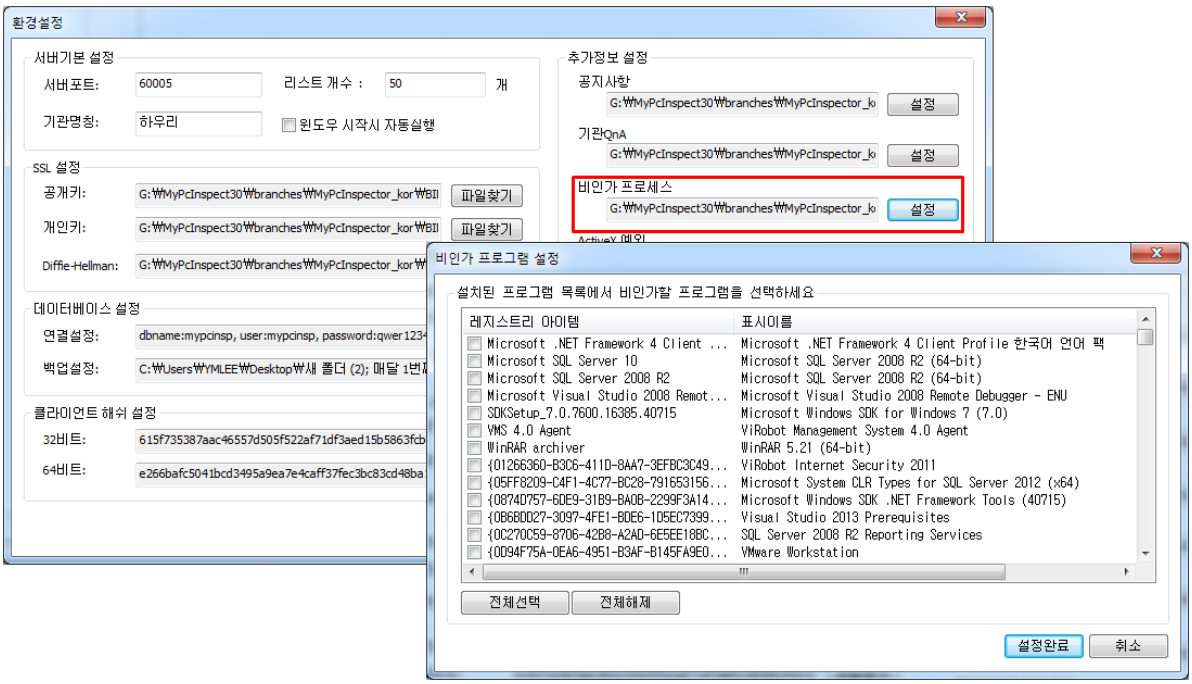
□ 기관에서 사용이 금지 된 편집 프로그램을 선택하여 해당 프로그램 존재 시 취약으로 판단합니다.



[그림] 55 편집 프로그램 설정 화면

② 비인가 프로그램 설치 여부

□ 사내에서 사용하고 있는 소프트웨어 목록을 클라이언트 에서 수집한 목록 중 비인가 프로그램을 등록하여 취약점 점검 시 삭제를 유도 합니다.



[그림] 556 비인가 프로그램 설정 화면