

MyV3

사용설명서

2004.10.11 , Version 1.0

문서 정보



Copyright ©, (주)안철수연구소, 1988-2004, All rights reserved.

이 사용설명서의 내용과 MyV3 프로그램은 저작권법과 컴퓨터 프로그램 보호법에 의해서 보호받고 있습니다.

또한, 이 사용설명서에 표기된 각 제품명은 각 회사의 등록상표입니다.

2004년 10월 15일 제 1판 발행

표기법

표기 규칙	내용
<창 이름>	창에 나타나는 문구 및 프레임, 윈도우의 이름
시작->프로그램	실행 순서 설명
확인	버튼 이름
추가/수정/삭제	추가 또는 수정 또는 삭제 의미
 참고	사용자가 알아 두면 좋은 부가적인 사용법 설명
 주의	프로그램 사용시 반드시 주의해야 할 점 경고 이 사항을 무시하고 사용할 경우, 예기치 못한 상황에 처할 수 있습니다.

목차 설명

장	설명
1. 제품 소개	MyV3 서비스에 대해 소개합니다.
2. 기능 및 특징	MyV3의 기능과 특징에 대해 설명합니다.
3. 설치/삭제하기	MyV3를 설치, 삭제하는 방법을 설명합니다.
4. 검사/치료하기	MyV3를 통해서 바이러스를 검사하고 치료하는 방법을 설명합니다.
5. 검역소에 보관하기	치료 과정에서 손상된 데이터나 기타 이유로 감염된 원본 파일을 보관해 두는 검역소 기능을 설명합니다.
6. 검사 기록보기	바이러스 감염 경향이나 횟수를 확인하는 방법을 설명합니다.
7. 환경 설정하기	실행 환경을 설정하는 방법을 설명합니다.
8. 부록	FAQ, 색인

고객 지원 서비스

MyV3 서비스를 신청하고 나면 1년 동안 서비스를 받을 수 있으며 제품 서비스는 물론, 고객 지원 서비스도 받을 수 있습니다. 1년이 지나면, 서비스를 받을 수 없으니 다시 신청하시기 바랍니다.

고객 지원 연락처

MyV3의 사용법 및 서비스 신청 방법에 대한 문의는 아래 연락처로 연락하십시오.

(주)안철수연구소 고객만족센터	
주소	150-869 서울시 영등포구 여의도동 12번지 CCMM빌딩 6층 안철수연구소
홈페이지	http://www.ahnlab.com
이메일	customer@ahnlab.com
전화	02-2186-3000 (고객만족센터: 고객등록방법문의)
팩스	02-2186-6100 (대표) 02-2186-3001 (고객만족센터)

(주)안철수연구소 해외 지사	
China, Beijing	Rm 1701, Modern Qing Yun Building No34 BeiSanHuanXi Road, Haidian District, Beijing , P.R.C china 100086 Tel : +86-10-6219-6008 Fax : +86-10-6219-6003
China, Shanghai	No.2602 Lippo Plaza, No222Huaihaizhong Road , Luwan District Shanghai, China 200021 Tel : +86-21-5396-6132 Fax : +86-21-5396-6020
Tokyo, Japan	3F Daiichi-Denpa Bldg., 2-4-4 Sotokanda Chiyoda-ku, Tokyo, Japan 101-0021 Tel. +81-3-5209-8601 Fax. +81-3-5294-7307 Web : http://www.ahnlab.co.jp

목차

1. 제품 소개	6
2. 기능 및 특징	7
2.1. 기능	7
2.2. 특징	8
3. 설치/삭제하기	9
3.1. 시스템 요구 사양	9
3.2. 설치	9
3.3. 삭제	12
4. 검사/치료하기	14
4.1.1. 바이러스 감염 파일 검사/치료하기	14
4.1.2. 검사하는 도중에 검사 중단하기	15
4.1.3. 감염 파일 목록 확인하기	16
4.1.4. 발견된 바이러스를 한꺼번에 치료하기	17
4.1.5. 발견된 바이러스를 선택해서 치료하기	17
5. 검역소에 보관하기	18
5.1.1. 검역소에 있는 파일 목록 확인하기	18
5.1.2. 백업 파일 복원하기	18
5.1.3. 알려지지 않은 바이러스나 새로운 바이러스를 신고센터로 보내기	19
5.1.4. 목록에 있는 파일 삭제하기	19
6. 검사 기록 보기	20
6.1.1. 발견된 바이러스 목록 확인하기	20
6.1.2. 상세 정보	20
6.1.3. 목록에 있는 파일 삭제하기	21
7. 환경 설정하기	22
7.1. 검사 설정	22
7.1.1. 검사할 파일 선택하기	22
7.1.2. 검사 방법 선택하기	23
7.1.3. 설정값 되돌리기	23
7.2. 치료 설정	23
7.2.1. 치료할 수 있는 바이러스 처리하기	24
7.2.2. 치료할 수 없는 바이러스 처리하기	24
7.2.3. 감염된 파일이 실행중인 파일인 경우 치료하기	24
7.2.4. 치료하거나 삭제하기 전에 감염 파일 복사본을 검역소에 보관하기	25
7.2.5. 설정값 되돌리기	25
8. 부록	26
8.1. FAQ	26
8.2. Index	27

그림 목차

[그림 3-1] 스마트 업데이트 실행	10
[그림 3-2] Speed Up 시작 가이드.....	10
[그림 3-3] Speed Up 로그인.....	11
[그림 3-4] 트레이 아이콘에서 바이러스 검사 선택-개인 고객용	11
[그림 3-5] 트레이 아이콘에서 바이러스 검사 선택-기업 고객용	11
[그림 3-6] 트레이 아이콘에서 MyV3 종료-개인 고객용.....	12
[그림 3-7] 트레이 아이콘에서 MyV3 종료-기업 고객용.....	12
[그림 3-8] MyV3 제거 프로그램.....	13
[그림 4-1] 바이러스 검사 대상 선택	14
[그림 4-2] 바이러스 검사 진행 창	15
[그림 4-3] 바이러스 검사 일시 중지	16
[그림 4-4] 바이러스 검사 완료	16
[그림 4-5] 바이러스 치료 완료 창	17
[그림 5-1] 검역소에 있는 바이러스 확인	18
[그림 5-2] 바이러스 감염 파일 복원 여부 확인	18
[그림 5-3] 바이러스 감염 파일을 임의의 폴더에 저장.....	19
[그림 6-1] 날짜 별 바이러스 감염 정보 기록 확인.....	20
[그림 6-2] 바이러스 검사 기록 상세 정보	21
[그림 6-3] 검사 기록 삭제 여부 확인	21
[그림 7-1] 바이러스 검사 환경 설정	22
[그림 7-2] 바이러스 치료 환경 설정	24

1. 제품 소개

(주)안철수연구소 보안클리닉에서는 다양한 보안 관련 ASP제품을 서비스하고 있습니다.

바이러스 치료를 위해서는 **MyV3** 서비스를, 해킹 차단을 위해서는 **MyFirewall** 서비스를, 바이러스 침입 실시간 감지를 위해서는 **MyV3 RTS** 서비스를 사용자 컴퓨터의 보안 취약점을 알려주는 **보안경고리포트** 서비스를 제공합니다.

☑ **참고** MyV3 서비스를 이용하기 위해서는 (주)안철수연구소 보안클리닉 PC 보안 서비스를 신청해야 합니다. 기업 고객의 경우, 전산 관리자가 구매한 개수만큼 서비스를 이용할 수 있습니다.

MyV3는 온라인 백신 프로그램으로 바이러스를 검사/치료할 수 있으며 프로그램을 실행할 때마다 자동으로 엔진 업데이트를 하기 때문에 고객이 별도의 엔진 업데이트를 실행하지 않아도 되는 편리한 제품입니다.

2. 기능 및 특징

MyV3는 (주)안철수연구소에서 개발한 보안 관련 ASP 제품입니다. 보안클리닉 PC 보안 서비스 유료 회원으로 등록하면 여러 가지 기능들을 이용할 수 있으며, MyV3는 바이러스를 검사/치료하는 기능입니다.

참고 기업 고객의 경우 관리자가 등록된 개수만큼 사용할 수 있으며, 관리자가 지정해 준 웹페이지에 접속함으로써 제품을 설치할 수 있습니다.

2.1. 기능

MyV3는 아래와 같은 기능들이 있습니다.

최신 검사 상태 확인하기

창 오른쪽 위에 마지막 검사 내용에서 가장 최신의 검사 상태를 확인할 수 있습니다. **마지막 검사일, 검사 대상** 드라이브나 폴더, **검사 결과**를 볼 수 있습니다.

바이러스를 검사하고 치료하는 방법

창 오른쪽 아래에 있는 **검사 대상 선택**에서 검사하고자 하는 폴더를 선택한 다음, **검사/치료를** 누릅니다. <검사/치료> 창이 뜨면서 자동으로 검사를 시작합니다. 바이러스가 발견되면 감염된 파일이나 악성 코드 목록이 창에 실시간으로 나타납니다.

검역소

바이러스 치료 과정에서 손상된 데이터를 복구하거나 기타 이유로 감염 파일 원본이 필요할 때 **검역소**에서 보관해둔 파일을 복구할 수 있습니다.

바이러스 검사/치료 환경 설정

MyV3는 중소 규모 비즈니스 환경에 가장 적합한 상태로 설정되어 있습니다. 그러나 특수한 상황에서 설정을 다르게 해야 할 필요가 있다면 **환경 설정**을 누릅니다. 환경 설정에는 **검사 설정**과 **치료 설정**이 있습니다.

바이러스 검사 기록 보기

검사 기록은 시스템 사용자의 바이러스 감염 경향이나 회수 등을 확인할 수 있습니다. 검사 결과 바이러스가 발견된 경우에 한해, 날짜 별로 그 결과를 볼 수 있습니다.

2.2. 특징

MyV3는 (주)안철수연구소에서 개발한 보안 관련 ASP 제품입니다. 보안클리닉 서비스 유료 회원으로 등록하면 여러 가지 컴퓨터 보안 기능들을 이용할 수 있습니다.

바이러스의 진단과 치료에는 (주)안철수연구소의 엔진을 사용하여 안정적이고 빠른 진단과 치료가 가능하며, 서비스를 이용할 때마다 항상 최신 버전의 엔진을 사용하므로 기존 패키지 제품과 같이 엔진 업데이트를 별도로 수행해야 하는 불편함이 없습니다.

3. 설치/삭제하기

이 장에서는 MyV3를 설치하기 위한 시스템 요구 사양과 설치하는 방법, 부득이하게 MyV3를 사용하지 않고 삭제해야 할 경우 보안클리닉 Speed Up을 삭제하는 방법을 소개합니다.

먼저, MyV3를 실행하기 전에 시스템 요구 사양을 확인하십시오.

3.1. 시스템 요구 사양

지원 운영체제(OS)

Windows 98, Windows 98 SE, Windows ME, Windows 2000 Professional, Windows XP Home, Windows XP Professional

웹 브라우저

Windows Internet Explorer 5.0 이상

지원 언어

한글

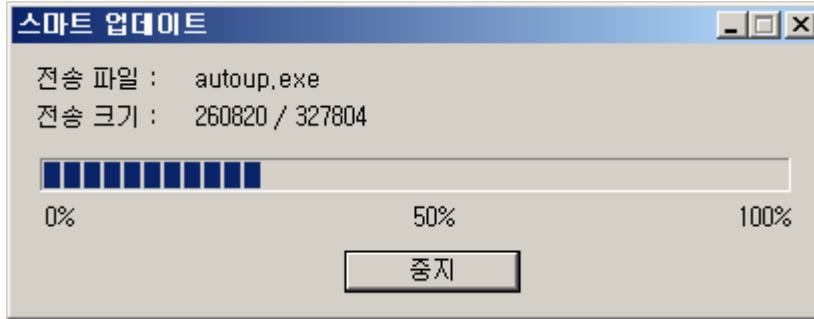
3.2. 설치

MyV3는 보안클리닉 Speed Up을 통해서 실행되는 프로그램입니다. MyV3를 설치하기 위해서는 보안클리닉 Speed Up을 설치해야 합니다.

① 보안클리닉 Speed Up을 설치하기 위해서는 브라우저를 실행한 다음 (주)안철수연구소 홈페이지(<http://www.ahnlab.com>)에 접속합니다. 보안클리닉 PC 보안 서비스를 신청하고, 가입한 사용자 ID로 로그인한 다음 보안클리닉->PC 보안->Speed Up 설치/삭제를 누릅니다.

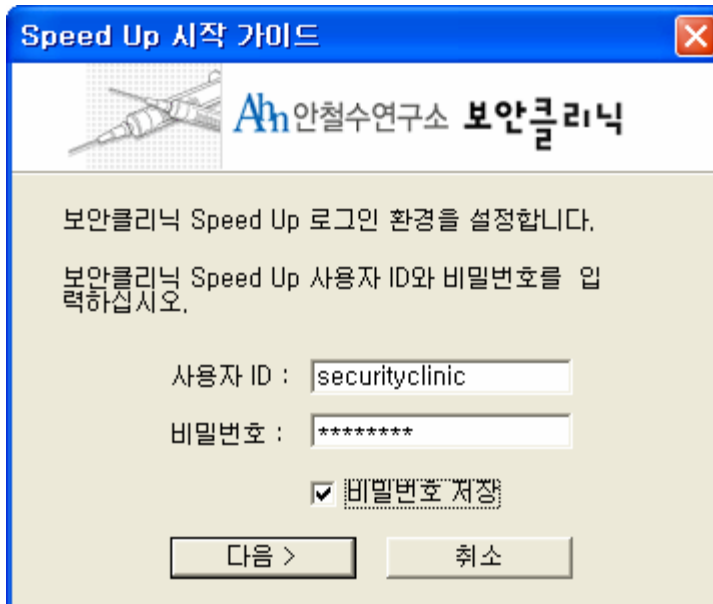
참고 기업 고객용의 경우, 관리자가 등록한 개수만큼 설치할 수 있으며, 관리자가 지정해 준 웹페이지를 통해서 설치할 수 있습니다.

② 보안클리닉 Speed Up 설치하기를 누르면 스마트 업데이트가 실행되면서 엔진이나 프로그램을 업데이트합니다.



[그림 3-1] 스마트 업데이트 실행

- ③ 스마트 업데이트가 실행되면서 엔진 다운로드가 끝나면 <Speed Up 시작 가이드> 창이 뜹니다. 사용자 ID와 비밀번호를 입력하고 <다음 >을 누르면 보안클리닉 Speed Up이 실행됩니다. **비밀 번호 저장** 체크 박스()를 선택하면 이후부터 <Speed Up 시작 가이드> 창이 뜨지 않고 자동으로 로그인합니다.

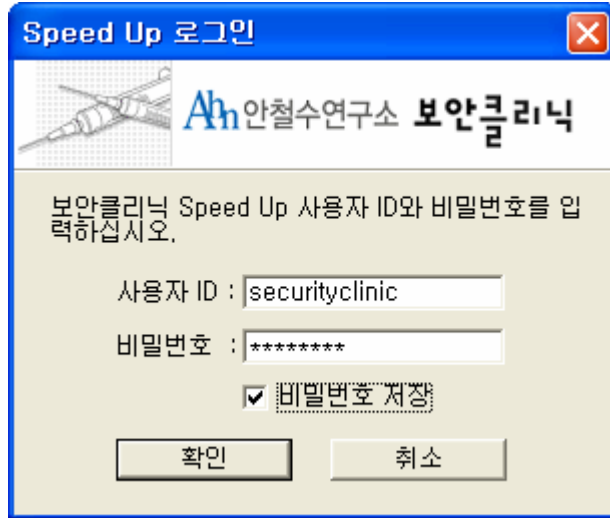


[그림 3-2] Speed Up 시작 가이드


- 참고** 기업 고객용의 경우 <Speed Up 시작 가이드> 창이 뜨지 않고 진행됩니다.

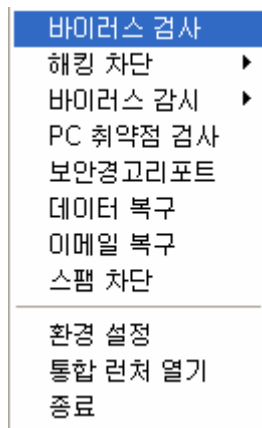
- ④ 작업 표시줄에 보안클리닉 Speed Up 트레이 아이콘()이 나타납니다.

- ⑤ 설치를 한 이후부터는 보안클리닉 Speed Up을 종료하고 나서 다시 실행할 때, <Speed Up 로그인> 창이 뜨며 사용자 ID와 비밀번호를 입력해서 로그인합니다. 비밀번호 저장을 선택했을 경우에는 로그인 과정 없이 바로 실행됩니다.



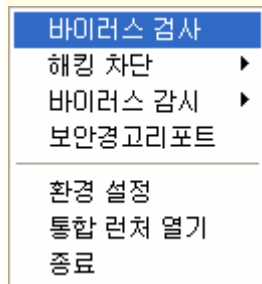
[그림 3-3] Speed Up 로그인

⑥ 작업 표시줄 오른쪽 트레이 아이콘에서 Speed Up 트레이 아이콘()에 마우스를 대고 오른쪽 버튼을 눌러 바이러스 검사를 실행시킵니다.



[그림 3-4] 트레이 아이콘에서 바이러스 검사 선택-개인 고객용

☑ 참고 기업 고객용의 경우 트레이 아이콘 메뉴가 다르게 나타납니다.



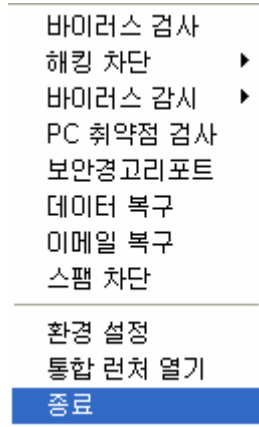
[그림 3-5] 트레이 아이콘에서 바이러스 검사 선택-기업 고객용

MyV3 프로그램은 윈도우즈에서 ActiveX 프로그램이 위치하는 C:\Windows\W

Download Program Files 폴더에 설치됩니다.

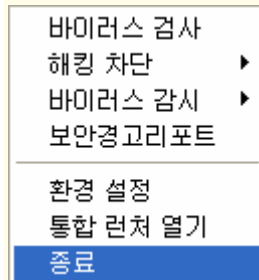
3.3. 삭제

① MyV3를 삭제하기 위해서는 먼저 보안클리닉 Speed Up을 종료해야 합니다. <보안클리닉>이나 <바이러스 검사 (MyV3)> 창이 열려 있지 않더라도 실행중인 경우가 있으므로, 작업 표시줄에 있는 MyV3 트레이 아이콘에 마우스를 대고 오른쪽 버튼을 눌러 **종료**를 누릅니다.



[그림 3-6] 트레이 아이콘에서 MyV3 종료-개인 고객용

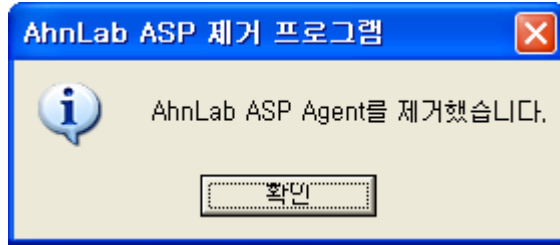
☑ **참고** 기업 고객용의 경우 트레이 아이콘에 마우스를 대고 오른쪽 버튼을 누르면 메뉴가 다르게 나타납니다.



[그림 3-7] 트레이 아이콘에서 MyV3 종료-기업 고객용

② 삭제를 하기 위해서는 **시작->모든 프로그램->Ahnlab->Speed Up->Speed Up 삭제**를 누릅니다. 삭제를 누르면 AhnLab ASP 제거 프로그램 다운로드 웹페이지로 연결이 되고 제거 프로그램을 다운로드하는 창이 나타납니다.

③ 제거 프로그램을 저장하거나 아니면 **열기(O)**를 눌러서 실행시킵니다. 제거 프로그램이 실행되고 나면 AhnLab ASP Agent를 제거했다는 메시지가 나타나고 **확인**을 누르서 프로그램 삭제 과정이 끝납니다.



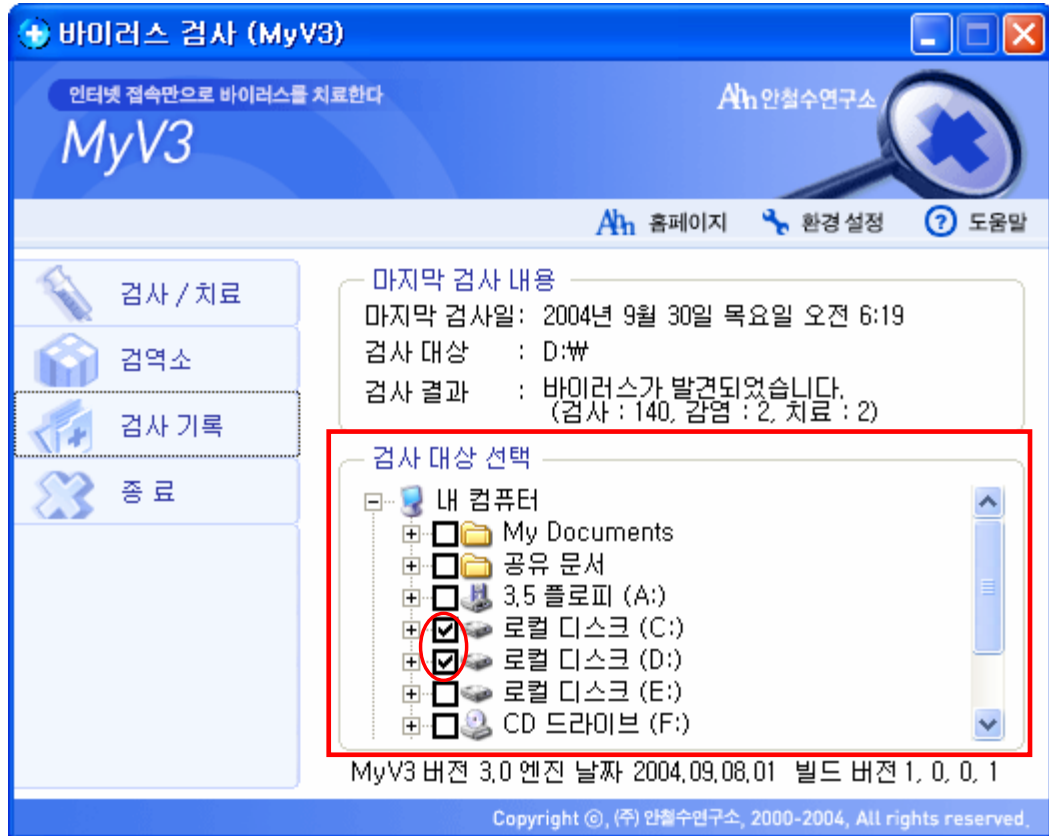
[그림 3-8] MyV3 제거 프로그램

4. 검사/치료하기

다음은 검사/치료 과정에서 알아두면 편리한 기능입니다.

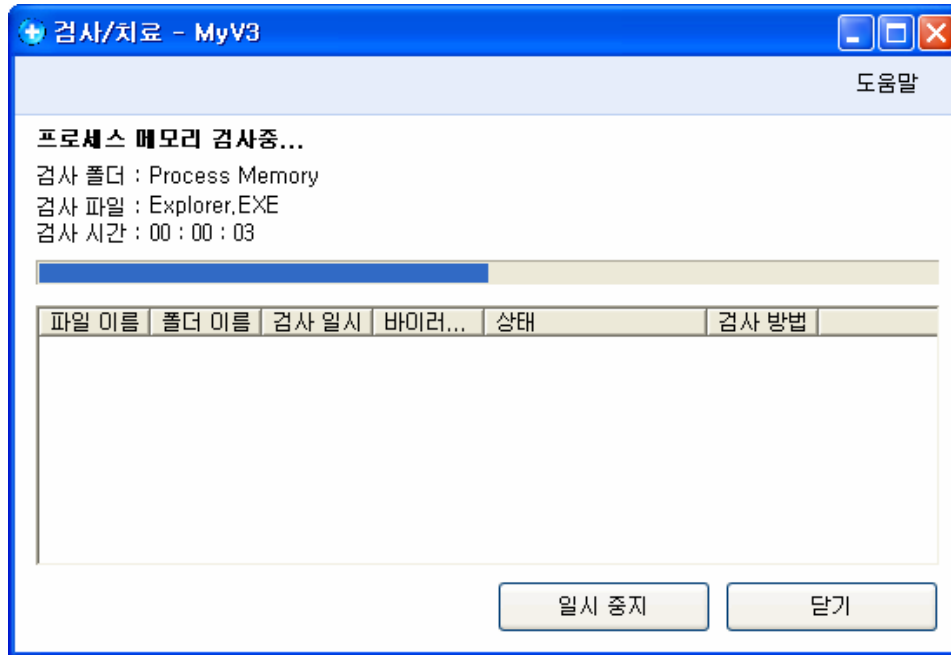
4.1.1. 바이러스 감염 파일 검사/치료하기

바이러스를 검사하기 위해서는 먼저, 검사할 대상을 선택합니다. 검사할 드라이브나 폴더 앞에 있는 체크 박스()를 선택합니다.



[그림 4-1] 바이러스 검사 대상 선택

왼쪽 메뉴에서 검사/치료를 누르면, <검사/치료 - MyV3> 창이 나타나면서 바이러스를 검사하는 진행 과정을 볼 수 있습니다.

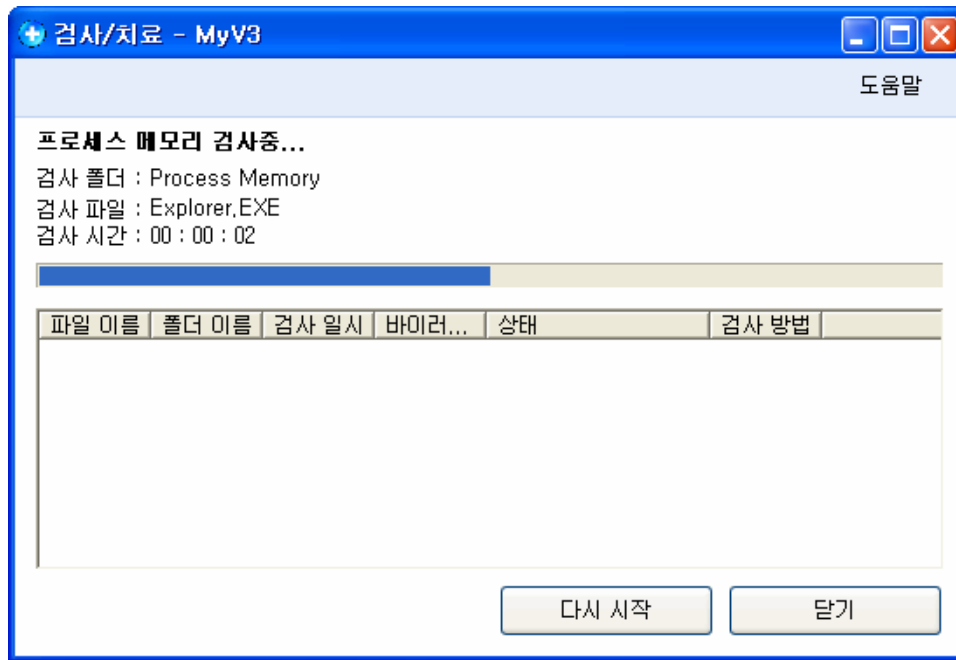


[그림 4-2] 바이러스 검사 진행 창

4.1.2. 검사하는 도중에 검사 중단하기

일시 중지를 선택하여 검사를 잠시 중단합니다. 바이러스를 검사하는 도중에는 다른 응용프로그램을 실행하지 않는 것이 안전합니다. 그러므로 검사 도중 다른 프로그램을 실행하려면 **일시 중지** 기능을 사용하는 것이 좋습니다. [그림 4-2]에서 일시 중지를 눌러서 검사를 잠시 중지한 다음 다른 응용 프로그램을 닫습니다.

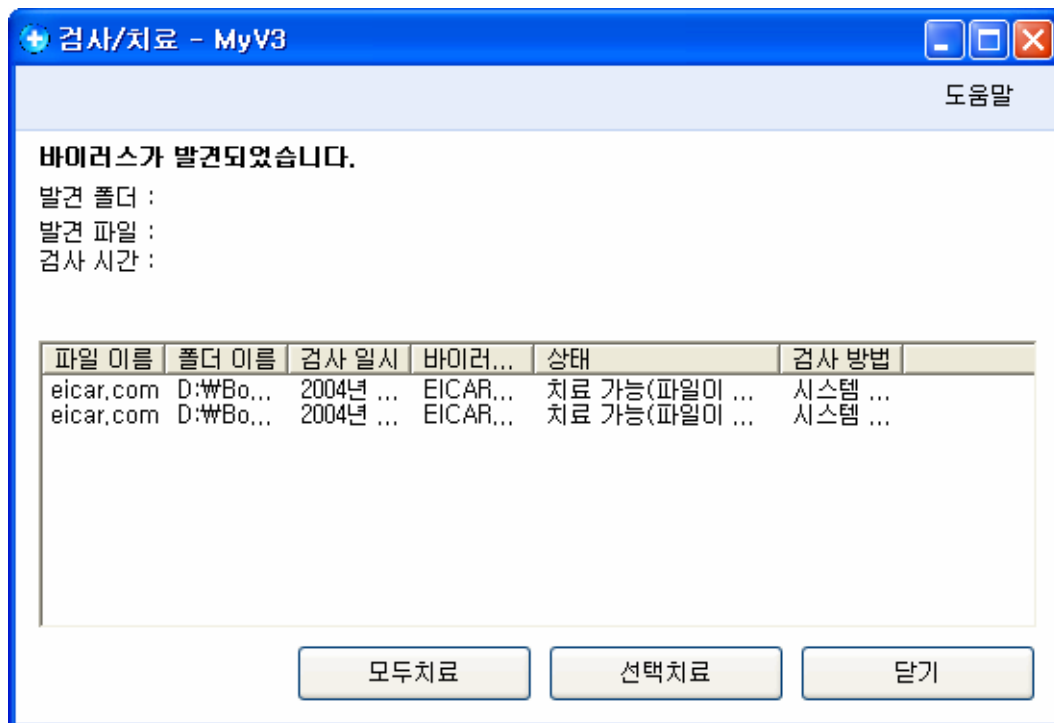
다시 검사를 시작하려면 **다시 시작**을 누르십시오.



[그림 4-3] 바이러스 검사 일시 중지

4.1.3. 감염 파일 목록 확인하기

바이러스 검사를 하고 나면 발견된 바이러스에 대한 목록을 보여줍니다. 감염 파일 목록은 파일 이름, 폴더 이름, 검사 일시, 바이러스 이름, 상태, 검사 방법을 보여줍니다.



[그림 4-4] 바이러스 검사 완료

여기서 상태란 감염 파일의 처리 상태를 말합니다. 예를 들어, 삭제인 경우 악성 코드이므로 삭제되었음을 의미합니다. 바이러스 치료를 마쳤거나 바이러스 검사/치료를 취소하려면 **닫기**를 누릅니다.

참고 사용자가 환경 설정에서 감염된 파일을 삭제하지 않도록 설정했다면 수동으로 파일을 삭제해야 합니다. 수동 삭제 방법은 감염된 파일을 선택한 다음 **선택치료**를 누르거나, **모두치료**를 눌러서 감염된 파일을 치료합니다. 감염된 파일을 자동으로 삭제하도록 설정하려면 **7.2 치료 설정**을 참고하십시오.

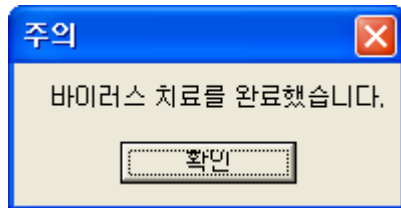
4.1.4. 발견된 바이러스를 한꺼번에 치료하기

모두치료를 누르면 한꺼번에 바이러스를 치료 또는 삭제할 수 있습니다. MyV3는 자동으로 감염 파일을 치료하고, 악성 코드를 삭제할 수 있습니다. 그러나 사용자가 환경 설정에서 자동 치료 옵션을 해제했다면, 감염 파일을 수동으로 치료 또는 삭제해야 합니다. 이 경우 **모두치료**를 사용하면 편리합니다.

4.1.5. 발견된 바이러스를 선택해서 치료하기

치료 혹은 삭제하고자 하는 파일을 선택한 다음 **선택치료**를 누르면 해당 파일만 치료 혹은 삭제합니다.

바이러스 치료가 끝나면 다음과 같이 치료가 완료되었다는 메시지를 보여줍니다.



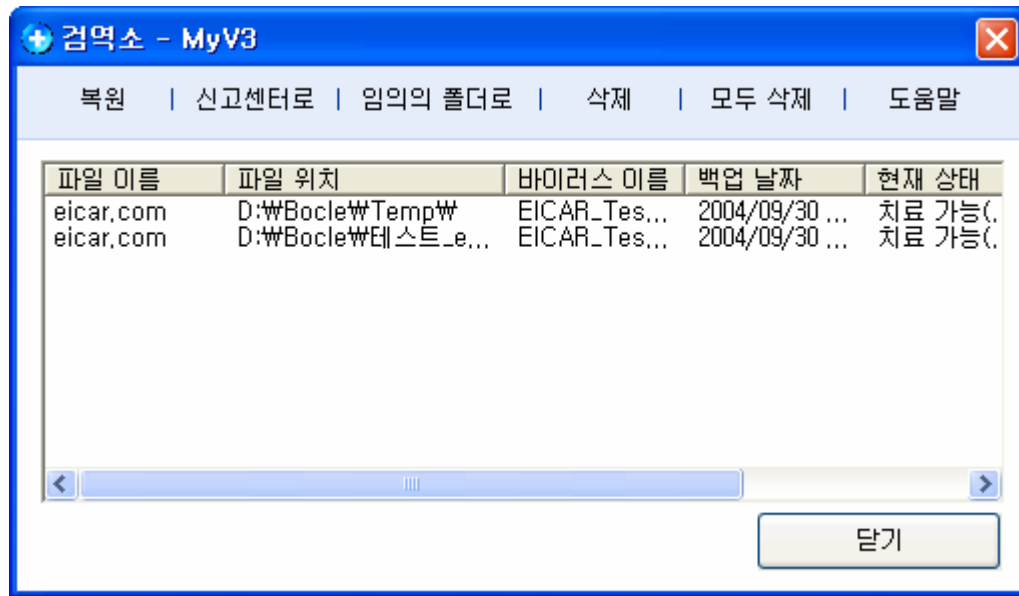
[그림 4-5] 바이러스 치료 완료 창

5. 검역소에 보관하기

바이러스를 치료하거나 악성 프로그램을 삭제하기 전에 감염 파일 복사본을 보관해두는 곳입니다. 여기에 보관된 파일은 여전히 감염된 상태에 있는 파일이지만, 격리되어 있기 때문에 시스템에 영향을 미치지 않습니다.

5.1.1. 검역소에 있는 파일 목록 확인하기

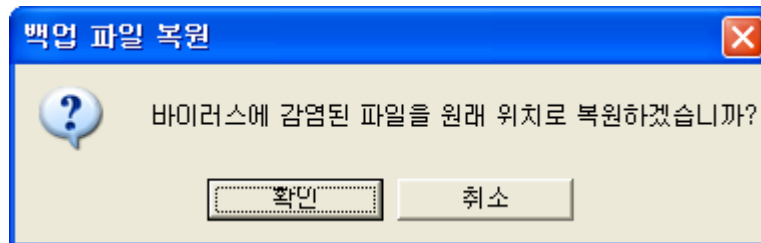
검역소에 있는 파일 목록은 치료 혹은 삭제한 파일 목록입니다. 바이러스에 감염되었지만 사용자 정의에 의해 치료 혹은 삭제되지 않은 파일은 검역소 목록에 나타나지 않습니다. 목록은 **파일 이름**, **파일 위치**, **바이러스 이름**, **백업 날짜**, 그리고 **현재 상태**를 보여줍니다. **백업 날짜**는 해당 파일을 치료 혹은 삭제한 날짜입니다. **현재 상태**는 원본 파일의 치료 여부 등 현재 처리 상태를 알려줍니다.



[그림 5-1] 검역소에 있는 바이러스 확인

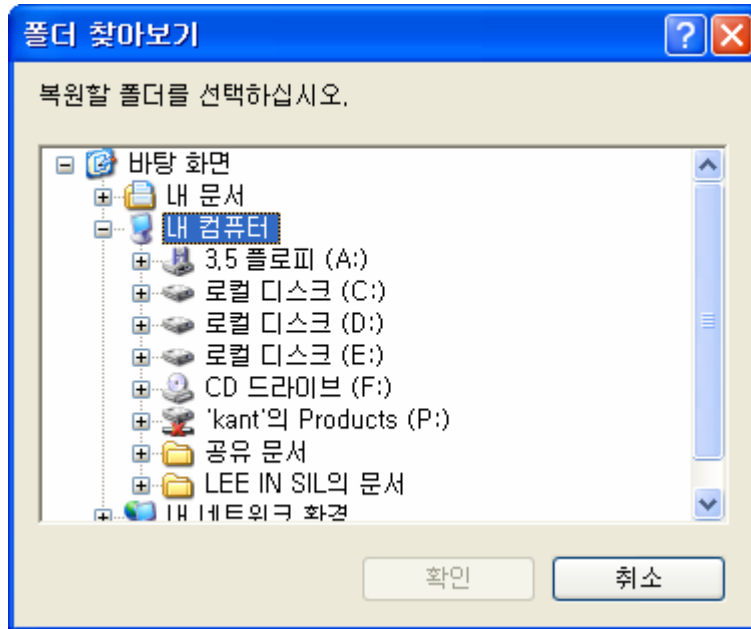
5.1.2. 백업 파일 복원하기

매우 드문 일이지만, 바이러스에 중첩 감염된 파일은 치료 과정에서 손상될 수 있습니다. 이렇게 손상된 파일을 반드시 복구해야 할 경우 **복원**을 누르면 감염 파일이 원래 있던 폴더로 복원됩니다.



[그림 5-2] 바이러스 감염 파일 복원 여부 확인

임의의 폴더를 누르면 사용자가 지정하는 폴더에 복원됩니다. 사용자가 파일을 저장할 폴더를 선택할 수 있습니다.



[그림 5-3] 바이러스 감염 파일을 임의의 폴더에 저장

주의 이렇게 복원된 파일은 여전히 바이러스에 감염된 상태이므로 시스템에 영향을 미칠 수 있습니다. 그러므로 꼭 필요한 경우가 아니라면 감염된 파일을 복원하지 마십시오.

5.1.3. 알려지지 않은 바이러스나 새로운 바이러스를 신고센터로 보내기

알려지지 않은 바이러스나 새로운 바이러스가 발견되면 검역소 파일 목록의 현재 상태 항목에 '새로운 바이러스'라고 표시됩니다. 해당 파일을 선택한 다음 신고센터로 누르십시오. 신고센터로 보내주신 바이러스 샘플은 더 좋은 백신을 만드는데 도움이 될 것입니다.

5.1.4. 목록에 있는 파일 삭제하기

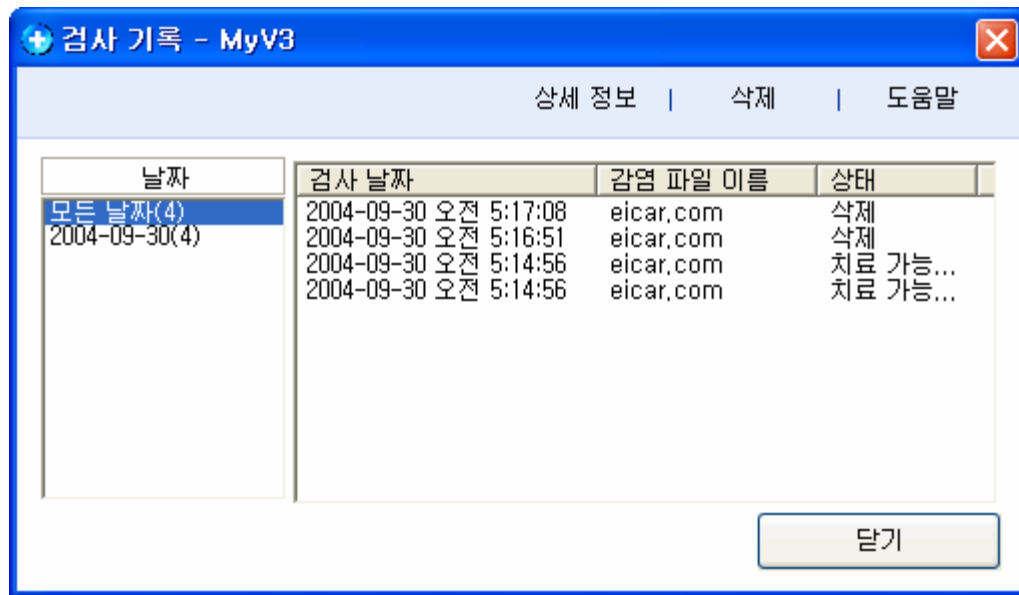
삭제하고자 하는 파일을 선택한 다음 삭제를 누릅니다. 파일을 선택하지 않고 한꺼번에 삭제하려면 모두 삭제를 누르십시오.

6. 검사 기록 보기

검사 기록은 시스템 사용자의 바이러스 감염 경향이나 횟수 등을 보여줍니다. 검사 결과 바이러스가 발견된 경우에 한해, 검사 기록에서 날짜 별로 그 결과를 볼 수 있습니다.

6.1.1. 발견된 바이러스 목록 확인하기

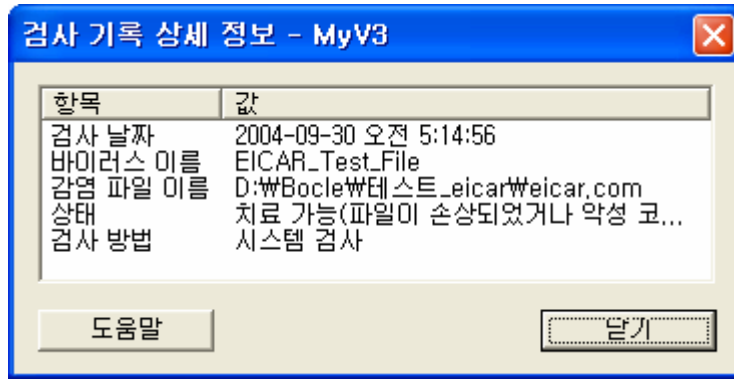
왼쪽 창의 날짜 목록 가운데 하나를 누르면 오른쪽 창에 해당 날짜의 검사 날짜, 감염 파일 이름, 상태를 볼 수 있습니다. 보안클리닉을 설치한 이후 바이러스에 감염된 적이 없다면 목록에 아무 것도 나타나지 않습니다.



[그림 6-1] 날짜 별 바이러스 감염 정보 기록 확인

6.1.2. 상세 정보

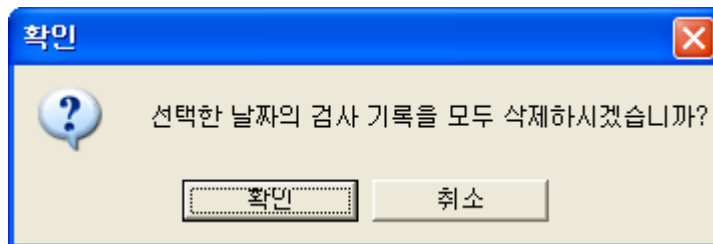
목록에 있는 파일의 자세한 정보를 보고 싶으면, 목록에서 해당 파일을 선택한 다음 창 위쪽의 상세 정보를 누릅니다. 검사 날짜, 바이러스 이름, 감염 파일 이름, 상태, 검사 방법(부트섹터 검사, 메모리 검사, 파일 검사 등 바이러스가 검출된 장소)에 대해 더 많은 정보를 확인할 수 있습니다.



[그림 6-2] 바이러스 검사 기록 상세 정보

6.1.3. 목록에 있는 파일 삭제하기

삭제하고자 하는 파일을 선택한 다음 **삭제**를 누르십시오. 날짜 목록에서 특정 날짜를 선택하고 **삭제**를 누르면 모두 삭제할지를 묻습니다. **확인**을 누르면 해당 날짜의 파일이 모두 삭제됩니다.



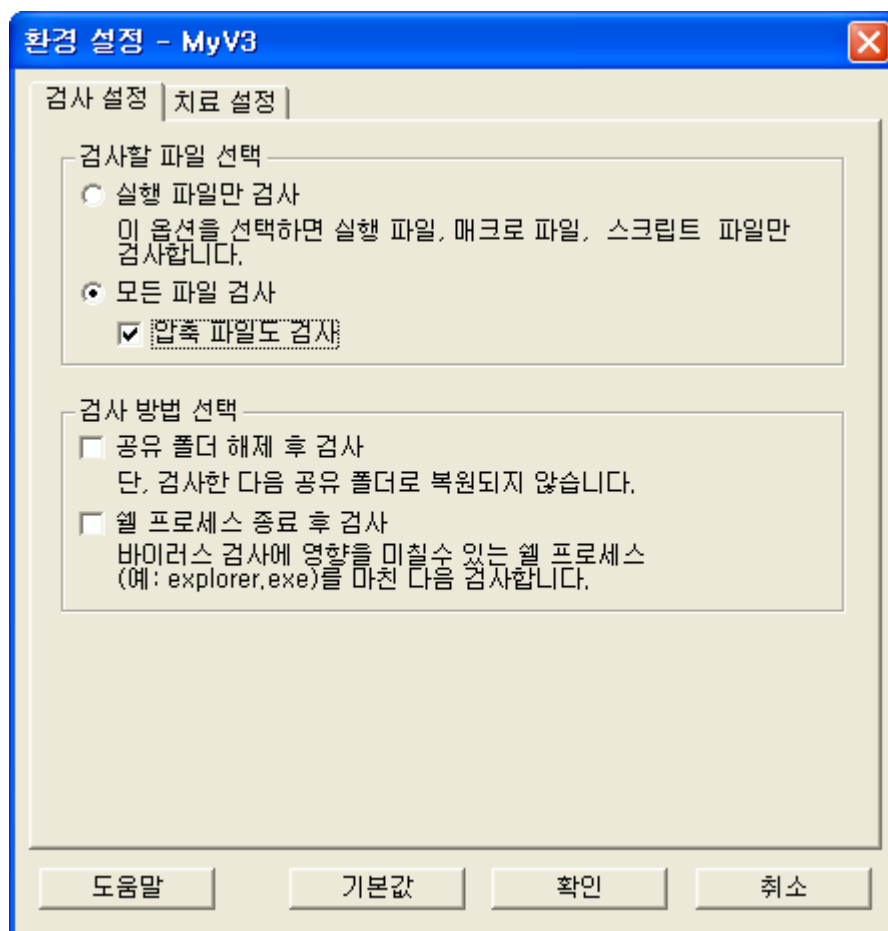
[그림 6-3] 검사 기록 삭제 여부 확인

7. 환경 설정하기

환경 설정에는 **검사 설정**과 **치료 설정**이 있습니다. 검사 설정은 바이러스를 검사하기 위한 방법을 사용자가 설정할 수 있으며, 치료 설정은 바이러스에 감염된 파일을 치료하는 방법을 설정할 수 있습니다.

7.1. 검사 설정

환경 설정에 있는 탭 메뉴 가운데 **검사 설정**을 누르면 아래와 같은 설정을 할 수 있습니다.



[그림 7-1] 바이러스 검사 환경 설정

7.1.1. 검사할 파일 선택하기

모든 파일을 검사하는 것이 좋습니다. 실행 파일만 검사하면 모든 파일을 검사하는 것보다 바이러스 검사 속도가 빠릅니다. 그러나 압축 파일 등 실행 파일이 아닌 파일에 들어 있는 바이러스나 악성코드를 찾아낼 수 없습니다. **모든 파일 검사->압축 파일도 검사**를 선택하면 1단계 압축까지 해제해서 바이러스 감염

여부를 검사합니다.

☑ **참고** 압축 파일이 ZIP 파일인 경우에는 검사 혹은 치료가 끝난 다음 파일을 원래대로 다시 압축합니다. 기타 압축 파일은 다시 압축하지 않습니다.

7.1.2. 검사 방법 선택하기

바이러스 검사 결과와 현재 시스템 상태에 차이가 생기지 않도록 공유 폴더를 해제하고 검사하는 것이 좋습니다. 공유 폴더를 해제하지 않고 바이러스를 검사하면, 공유 폴더를 검사 한 다음 다른 폴더를 검사하는 동안 네트워크를 통해 공유 폴더가 다시 감염될 수 있기 때문입니다.

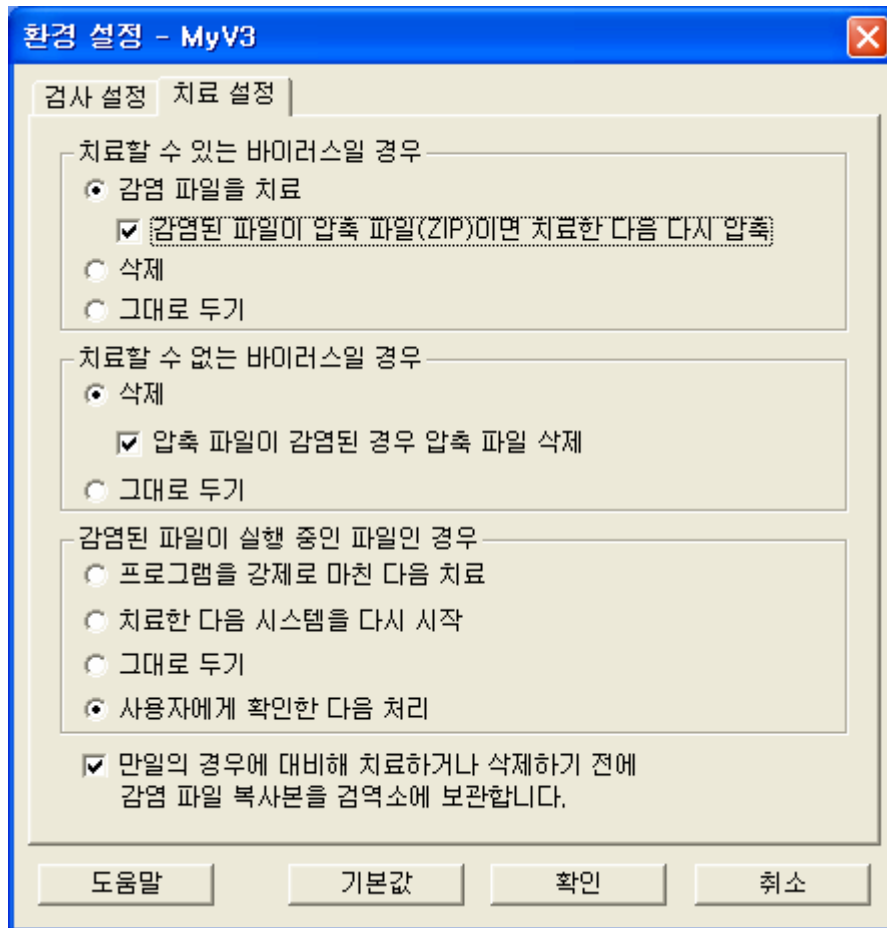
Windows 탐색기(explorer.exe)와 같은 쉘 프로세스도 프로그램을 마친 다음에 검사하는 것이 좋습니다. 바이러스 검사 과정을 방해하여 검사 속도를 떨어뜨리거나 검사 정확도를 낮출 수 있기 때문입니다.

7.1.3. 설정값 되돌리기

환경 설정을 바꾸었다가, 다시 MyV3가 추천하는 환경 설정으로 바꾸려면 언제든지 창 하단의 **기본값**을 누르십시오.

7.2. 치료 설정

환경 설정에 있는 탭 메뉴 가운데 **치료 설정**을 누르면 아래와 같은 설정을 할 수 있습니다.



[그림 7-2] 바이러스 치료 환경 설정

7.2.1. 치료할 수 있는 바이러스 처리하기

감염 파일을 치료를 권장합니다. 바이러스에 감염된 파일을 발견해서 치료하도록 알려줍니다. 감염된 압축 파일 중에서도 ZIP 형태로 압축된 1단계 압축 파일은 치료한 다음 다시 압축할 수 있습니다.

7.2.2. 치료할 수 없는 바이러스 처리하기

삭제를 권장합니다. 치료할 수 없는 바이러스는 크게 두 가지입니다. 악성코드와 ZIP 압축 파일 이외의 압축 파일에 들어있는 감염 파일입니다. 이 경우 유일한 치료 방법은 해당 파일을 삭제하는 것입니다.

참고 악성코드는 시스템에 악영향을 미치므로 반드시 삭제합니다. 대부분의 압축 파일은 그대로 두어도 시스템에 피해를 입히지 않습니다. 그러나 만일의 경우에 대비해 그대로 두지 말고 삭제할 것을 권장합니다.

7.2.3. 감염된 파일이 실행중인 파일인 경우 치료하기

사용자에게 확인한 다음 처리할 것을 권장합니다. 실행 중인 감염 파일은 치료할 수 없습니다. 실행을 마치고 치료하는 것이 가장 좋지만, 경우에 따라서 당장 실행을 마칠 수 없거나 지금 사용하고 있는 프로그램일 경우가 있습니다. 이런 경우

MyV3는 감염 파일 복사본을 만들어 치료한 다음, 시스템을 다시 시작할 때 감염 파일을 폐기하고 치료한 파일을 실행합니다.
이처럼 프로그램에 따라 대응 방법이 달라지기 때문에, MyV3가 가장 적절한 대응 방법을 선택해서 필요할 때마다 사용자가 확인해서 처리하도록 하는 것이 좋습니다.

7.2.4. 치료하거나 삭제하기 전에 감염 파일 복사본을 검역소에 보관하기

매우 드문 일이지만, 바이러스에 중첩 감염된 파일은 치료 과정에서 손상될 수 있습니다. 이것이 아주 중요한 데이터 파일이라면, 손상되는 것보다는 바이러스에 감염된 상태라도 그대로 보존하는 것이 낫다고 판단할 수 있습니다. 이후에 엔진 업데이트를 통해 손상 없이 치료할 수도 있으므로 만일의 경우에 대비해서 이 옵션을 선택합니다.

7.2.5. 설정값 되돌리기

환경 설정을 바꾸었다가, 다시 MyV3가 추천하는 환경 설정으로 바꾸려면 언제든지 창 아래쪽의 **기본값**을 눌러주십시오.

8. 부록

8.1. FAQ

MyV3를 어떻게 다운로드받고, 어떻게 업데이트하나요?

(주)안철수연구소 홈페이지(<http://www.ahnlab.com>)의 **보안클리닉->PC 보안->Speed Up 설치/삭제**에서 **보안클리닉 Speed Up 실행하기**를 누르면 MyV3가 자동으로 설치됩니다. 이후 MyV3에 접속할 때마다 자동으로 업데이트됩니다.

오프라인에서도 MyV3를 사용할 수 있나요?

아니오. MyV3는 온라인 백신 프로그램입니다. 오프라인에서는 사용할 수 없습니다.

MyV3 서비스를 신청하면 저절로 바이러스가 치료되나요?

아닙니다. 바이러스를 치료하려면 사용자의 컴퓨터에서 MyV3를 실행해야 합니다.

MyV3 서비스를 받고 있는데 바이러스에 걸렸어요. 어떻게 된 건가요?

바이러스 백신은 바이러스를 치료하는 프로그램이지 예방하는 프로그램이 아닙니다. 해킹 차단 (MyFirewall), 바이러스 감시 (MyV3 RTS)를 설치하여 바이러스나 악성 코드를 예방할 것을 권장합니다. 해킹 차단과 바이러스 실시간 감시 프로그램을 설치/동작해야 합니다. 계속해서 새로운 바이러스가 만들어지기 때문에 바이러스를 100% 예방하는 것은 불가능합니다. 바이러스 감염 피해를 최소화하려면 MyV3엔진 업데이트, 정기적인 바이러스 검사 등으로 시스템을 정기적으로 점검하는 습관을 들이는 것이 가장 좋습니다.

검역소가 뭔가요? 검역소 안에 있는 파일을 지워도 되나요?

바이러스를 치료하거나 악성 프로그램을 삭제하기 전에 감염 파일 복사본을 보관해두는 곳입니다.

감염된 파일을 치료/삭제한 다음 손상된 데이터가 없거나 시스템이 올바르게 동작하면 검역소 안에 있는 파일을 지워도 좋습니다. 그러나 지우지 않아도 상관없습니다. 여기에 보관된 파일은 여전히 감염된 상태에 있는 파일이지만, 격리되어 있어 시스템에 영향을 미치지 않기 때문입니다.

바이러스 검사 시간이 너무 오래 걸려요.

압축 파일까지 검사하려면 시간이 오래 걸립니다. 환경 설정에서 압축 파일 검사를 해제하고 검사하십시오. 또는 바이러스 감염 확률이 적은 폴더를 제외하고 검사하십시오.

