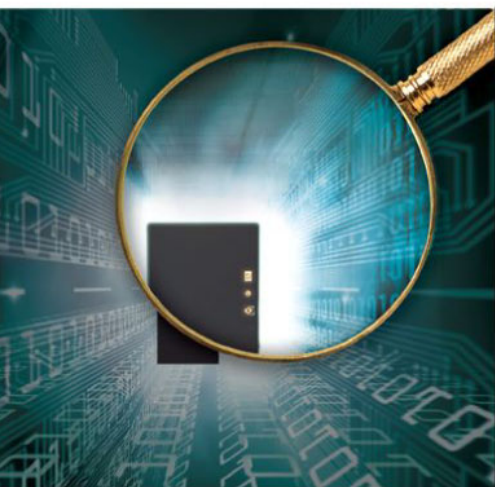




# V3 Net

for Windows Server 6.0

## 사용설명서

# 사용설명서 소개

---

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

이 V3Net for Windows Server 6.0 사용설명서의 내용과 프로그램은 저작권법과 컴퓨터프로그램보호법에 의해서 보호받고 있습니다. 이 사용설명서에 표기된 제품명은 각 사의 등록상표입니다.

2005년 12월 5일 제 2판 발행

## 내용 구성

### 1장 제품 소개

V3Net for Windows Server 6.0의 기능 및 특징을 소개합니다.

### 2장 시작하기

V3Net for Windows Server 6.0을 설치하고 삭제하는 방법을 순서대로 설명합니다.

### 3장 최신 엔진 업데이트

최신 엔진을 업데이트하는 방법을 설명합니다. 최신 엔진으로 업데이트하지 않으면 새로 발견된 신종 바이러스를 치료할 수 없습니다.

### 4장 바이러스 검사 및 치료

사용자의 시스템을 검사하여 감염된 파일을 치료하는 방법을 설명합니다.

### 5장 둘러보기

V3Net for Windows Server 6.0을 구성하는 메뉴를 살펴보고 각 메뉴의 사용법을 설명합니다.

### 6장 환경 설정

바이러스 검사 및 치료하는 방법 등을 사용자가 원하는 대로 직접 설정하는 방법을 설명합니다. 알람 메시지를 보이지 않게 하는 등 다양한 환경 설정 옵션을 선택할 수 있습니다.

### 7장 부록

V3Net for Windows Server 6.0을 사용하는 데 도움이 될 수 있는 용어를 설명합니다. 색인을 사용하면 원하는 기능만 바로 찾아서 볼 수 있습니다.

## (주)안철수연구소 고객만족센터

E-Mail : customer@ahnlab.com

홈페이지 : <http://www.ahnlab.com>

Tel : 02-2186-3000

Fax : 02-2186-3001

주소 : 150-869 서울시 영등포구 여의도동 12번지 CCMM빌딩 6층  
(주)안철수연구소

## 온라인(제품)등록

V3Net for Windows Server 6.0을 설치한 사용자는 반드시 온라인(제품)등록을 해야 합니다. 온라인 등록을 하지 않으면, 최신 엔진을 업데이트할 수 없으며, 그 이외에도 다양한 고객지원서비스를 받을 수 없습니다.

### 재계약

고객 지원 기간(1년)이 만료되면 재계약을 해야 합니다. 재계약을 하지 않으면 최신 엔진 업데이트 서비스 등의 고객지원서비스를 받을 수 없으며 설치된 제품도 더 이상 사용할 수 없습니다. 현재 설치된 제품의 고객지원서비스 만료일은 (주)안철수연구소 홈페이지(<http://www.ahnlab.com>)의 [고객 지원 > 등록제품확인] 메뉴에서 확인할 수 있습니다.

### (주)안철수연구소 고객만족센터

(주)안철수연구소 인터넷 쇼핑몰 <http://shop.ahnlab.com> [재계약] 메뉴에서 재계약 제품을 구입하십시오. 재계약에 대해서 궁금한 점이 있으면 고객만족센터로 연락하시기 바랍니다.

- 재계약 안내: 02-2186-3090
- 고객만족센터: 02-2186-3000
- E-Mail: customer@ahnlab.com

**!** 주의 고객지원서비스 기간(1년)이 만료되면 반드시 시스템에서 이 제품을 삭제해야 합니다. 사용 기간이 만료된 제품을 삭제하지 않으면 불법 소프트웨어 사용으로 간주되어 민, 형 사상의 처벌을 받을 수 있습니다.

## 고객지원서비스

V3Net for Windows Server 6.0을 설치한 사용자는 반드시 온라인 고객 등록을 해야 합니다. 이 제품을 설치했으나 온라인 고객 등록을 하지 않은 사용자는 고객 지원서비스를 받을 수 없습니다. 제품을 설치하고 온라인 고객 등록을 한 사용자는 고객지원서비스 기간(1년) 동안 다음과 같이 다양한 고객지원서비스를 이용할 수 있습니다.

- 전화, 팩스, 온라인을 통한 제품 상담 서비스
- 매주(수요일) 최신 엔진 업데이트 서비스
- E-Mail을 통한 엔진 업데이트 소식 및 신종 바이러스 정보 서비스
- 디지털 바이러스 캘린더(스크린 세이버)제작 배포
- 보안 세미나, 교육 프로그램 행사 시 무료 참가 서비스

**!** 주의 제품을 설치할 때 제품 번호를 입력하지 않으면, 평가판으로 설치됩니다. 평가판은 일정 기간(30일) 동안만 사용할 수 있으며, 사용 기간이 만료되면 반드시 시스템에서 삭제해야 합니다. 사용 기간이 만료된 평가판을 삭제하지 않으면 불법 소프트웨어 사용으로 간주되어 민, 형사상의 처벌을 받을 수 있습니다.

# 목 차

---

|                              |           |
|------------------------------|-----------|
| 사용설명서 소개 .....               | 2         |
| 내용 구성 .....                  | 2         |
| (주)안철수연구소 고객만족센터 .....       | 3         |
| 온라인(제품)등록 .....              | 3         |
| 고객지원서비스 .....                | 4         |
| <b>1장 제품 소개 .....</b>        | <b>11</b> |
| 기능 소개 .....                  | 12        |
| 시스템 사양 .....                 | 15        |
| <b>2장 시작하기 .....</b>         | <b>17</b> |
| 설치하기 .....                   | 18        |
| 삭제하기 .....                   | 26        |
| <b>3장 최신 엔진 업데이트 .....</b>   | <b>29</b> |
| 스마트 업데이트 .....               | 30        |
| 업데이트 환경 설정 .....             | 32        |
| <b>4장 바이러스 검사 및 치료 .....</b> | <b>39</b> |
| 한번 따라하기 .....                | 40        |
| 시스템 검사 .....                 | 41        |
| 사용자 검사 목록 .....              | 42        |
| 빠른 검사 .....                  | 43        |
| 실시간 감시 .....                 | 44        |
| 바이러스 치료 .....                | 46        |
| 시스템 검사/치료 .....              | 46        |
| 실시간 감시/치료 .....              | 48        |
| <b>5장 둘러보기 .....</b>         | <b>51</b> |
| Home .....                   | 52        |
| 시스템 검사 .....                 | 54        |
| 이벤트 기록 .....                 | 56        |
| 검사 기록 .....                  | 58        |
| 검역소 .....                    | 61        |

---

|                    |    |
|--------------------|----|
| 보안 경고 리포트 .....    | 64 |
| 메뉴 .....           | 66 |
| 기본 메뉴 .....        | 66 |
| 상단 메뉴 바 .....      | 67 |
| 상단 도구 모음 .....     | 68 |
| 웹 링크 .....         | 68 |
| 알림 메시지 .....       | 69 |
| 보안 경고 메시지 .....    | 69 |
| 자체 보호 알림 메시지 ..... | 69 |
| 포트 차단 알림 메시지 ..... | 70 |
| 도구 모음 .....        | 71 |
| 탐색기 도구 모음 .....    | 71 |
| 알림 도구 모음 .....     | 71 |

## 6장 환경 설정 .....73

|                  |     |
|------------------|-----|
| 환경 설정 시작 .....   | 74  |
| 쉬운 설정 .....      | 75  |
| 시스템 검사/감시 .....  | 77  |
| 시스템 검사/감시 .....  | 77  |
| 시스템 검사 .....     | 79  |
| 예약 검사 .....      | 81  |
| 화면 보호기 검사 .....  | 84  |
| 시스템 감시 .....     | 86  |
| 인터넷 감시 .....     | 88  |
| 시작 프로그램 감시 ..... | 90  |
| 비검사 영역 .....     | 92  |
| 고급 설정 .....      | 94  |
| 고급 검사 설정 .....   | 97  |
| 네트워크 차단 .....    | 99  |
| 포트 차단 .....      | 100 |
| 포트 추가 .....      | 101 |
| 포트 차단 기록 .....   | 103 |

---

|                    |            |
|--------------------|------------|
| 포트 차단 알림 메시지 ..... | 103        |
| 예외 포트 .....        | 104        |
| 경보 메일 .....        | 105        |
| 메일 계정 설정 .....     | 106        |
| 바이러스 경보 메일 .....   | 107        |
| 업데이트 경보 메일 .....   | 107        |
| 시스템 감시 경보 메일 ..... | 107        |
| 보안 설정 .....        | 109        |
| 보호 대상 설정 .....     | 109        |
| 암호 설정 .....        | 110        |
| 기타 설정 .....        | 111        |
| 알림 환경 .....        | 111        |
| 디스크 공간 지정 .....    | 112        |
| <b>7장 부록 .....</b> | <b>113</b> |
| 용어 .....           | 114        |
| 색인 .....           | 118        |

## 그림 목차

---

|                                                |    |
|------------------------------------------------|----|
| 그림 1 V3Net for Windows Server 6.0 설치 시작 .....  | 18 |
| 그림 2 사용권 계약 .....                              | 19 |
| 그림 3 다른 제품 설치 확인 .....                         | 19 |
| 그림 4 사용자 정보 .....                              | 20 |
| 그림 5 설치 폴더 선택 .....                            | 21 |
| 그림 6 파일 복사 .....                               | 21 |
| 그림 7 설치 진행 .....                               | 22 |
| 그림 8 V3Net for Windows Server 6.0 설치 완료 .....  | 22 |
| 그림 9 스마트 업데이트 유틸리티 .....                       | 23 |
| 그림 10 환경 설정 마법사 .....                          | 24 |
| 그림 11 시스템 검사 .....                             | 25 |
| 그림 12 V3Net for Windows Server 6.0 설치 완료 ..... | 25 |
| 그림 13 V3Net for Windows Server 6.0 삭제 시작 ..... | 26 |
| 그림 14 V3Net for Windows Server 6.0 삭제 .....    | 26 |
| 그림 15 V3Net for Windows Server 6.0 삭제 완료 ..... | 27 |
| 그림 16 업데이트 정보 .....                            | 30 |
| 그림 17 업데이트 제품 선택 .....                         | 32 |
| 그림 18 업데이트 방법 .....                            | 33 |
| 그림 19 인터넷 설정 .....                             | 33 |
| 그림 20 공유 폴더 설정 .....                           | 34 |
| 그림 21 일반 설정 .....                              | 35 |
| 그림 22 예약 설정 .....                              | 36 |
| 그림 23 예약 주기 설정 .....                           | 36 |
| 그림 24 시스템 검사 .....                             | 41 |
| 그림 25 사용자 검사 목록 .....                          | 42 |
| 그림 26 빠른 검사 줄 .....                            | 43 |
| 그림 27 Home 작업 창 .....                          | 44 |
| 그림 28 시스템 감시 알림 .....                          | 45 |
| 그림 29 시스템 검사 결과/치료 .....                       | 46 |
| 그림 30 바이러스 치료 전 주의 .....                       | 47 |
| 그림 31 바이러스 치료 완료 .....                         | 47 |
| 그림 32 시스템/인터넷 감시 결과 .....                      | 48 |
| 그림 33 치료 전 주의 .....                            | 49 |
| 그림 34 바이러스 치료 완료 .....                         | 49 |
| 그림 35 Home 작업 창 .....                          | 52 |

|                              |     |
|------------------------------|-----|
| 그림 36 시스템 검사 .....           | 54  |
| 그림 37 이벤트 기록 .....           | 56  |
| 그림 38 검사 기록 .....            | 58  |
| 그림 39 검역소 .....              | 61  |
| 그림 40 보안 경고 리포트 .....        | 64  |
| 그림 41 보안 경고 리포트 등록 정보 .....  | 65  |
| 그림 42 화면 구성 .....            | 66  |
| 그림 43 보안 경고 리포트 알림 메시지 ..... | 69  |
| 그림 44 자체 보호 알림 메시지 .....     | 69  |
| 그림 45 포트 차단 알림 메시지 .....     | 70  |
| 그림 46 탐색기 도구 모음 .....        | 71  |
| 그림 47 쉬운 설정 .....            | 75  |
| 그림 48 시스템 검사/감시 환경 설정 .....  | 77  |
| 그림 49 시스템 감시 종료 알림 .....     | 78  |
| 그림 50 시스템 검사 환경 설정 .....     | 79  |
| 그림 51 예약 검사 .....            | 81  |
| 그림 52 화면 보호기 검사 .....        | 84  |
| 그림 53 시스템 감시 .....           | 86  |
| 그림 54 인터넷 감시 .....           | 88  |
| 그림 55 시작 프로그램 감시 .....       | 90  |
| 그림 56 비검사 영역 .....           | 92  |
| 그림 57 고급 검사 설정 .....         | 94  |
| 그림 58 고급 검사 설정 .....         | 97  |
| 그림 59 자체 보호 알림 메시지 .....     | 98  |
| 그림 60 네트워크 차단 .....          | 99  |
| 그림 61 포트 차단 .....            | 100 |
| 그림 62 포트 정보 입력 .....         | 101 |
| 그림 63 포트 차단 기록 .....         | 103 |
| 그림 64 포트 차단 알림 메시지 .....     | 103 |
| 그림 65 경고 메일 .....            | 105 |
| 그림 66 메일 계정 설정 .....         | 106 |
| 그림 67 바이러스 경고 메일 편집 .....    | 107 |
| 그림 68 보안 설정 .....            | 109 |
| 그림 69 기타 설정 .....            | 111 |



# 1장

---

## 제품 소개

기능 소개 /12

시스템 사양 /15

V3Net for Windows Server 6.0의  
기능 및 특징을 소개합니다.

## 기능 소개

V3Net for Windows Server 6.0의 기능을 소개합니다.

### 감염자 추적

사용자의 시스템에 바이러스를 감염시킨 사용자의 정보를 확인하여 바이러스 확산으로 인한 피해를 줄일 수 있습니다. 네트워크 공유 폴더를 통해서 확산되고 있는 악성 바이러스의 감염 경로를 확인할 수 있습니다. FTP 프로그램 등을 통해서 받은 파일은 추적하지 않습니다.

☑참고 감염자 추적 기능을 사용하려면 <환경 설정>의 **시스템 감시** 메뉴에서 **고급...**을 눌러서 **검사 방법>검사 범위**에서 **로컬 드라이브 쓰기 검사**를 선택해야 합니다.

### 감염 위험 영역 추적 감시

(주)안철수연구소가 독자적으로 개발한 백신 알고리즘과 특정 위치 추적 검사 기술을 사용하여 바이러스 감염 위험이 높은 영역만을 집중적으로 감시합니다. 바이러스 감염 위험이 높은 특정 영역만을 감시하므로 사용자 컴퓨터의 동작에는 거의 영향을 미치지 않고 효과적으로 동작합니다.

### 사용자 시스템 취약점 보고

사용자 컴퓨터 상태를 확인하여 시스템에서 취약점이 발견되면 이를 실시간으로 알려줍니다. 보안 경고 리포트(64쪽)를 수시로 확인하여 바이러스의 침입에 대비하고 시스템의 취약점을 해결하여 피해를 최소화 할 수 있습니다.

### 바이러스 활동 예보

바이러스 캘린더(68쪽)에서 각 날짜 별로 활동이 예측되는 바이러스에 대한 정보를 제공합니다. (주)안철수연구소에서 분석한 바이러스 예보를 미리 확인하여 바이러스의 침입에 대비하는 것이 좋습니다.

### 치료 전 데이터 백업

바이러스에 감염된 파일이 발견되면 치료를 시작하기 전에 원본이 검역소(61쪽)에 백업됩니다. 바이러스 치료 도중에 중요한 데이터가 손상되었을 경우, 검역소에서 원본 파일을 복원하여 사용할 수 있습니다.

## **쉬운 설정**

<환경 설정> 창의 **쉬운 설정(75쪽)**에서 시스템 보호 수준(높음, 보통, 낮음)을 지정하면, 각 기능 별 검사/치료 환경을 일일이 지정하지 않아도 됩니다.

## **시스템 감시 자동 다시 시작**

사용자가 시스템을 다시 시작하거나 지정한 시간(분)이 지나면 **시스템 감시**를 자동으로 다시 시작할 수 있습니다.

## **알림 메시지**

작업 표시줄에 V3Net for Windows Server 6.0의 현재 동작 상태를 나타내는 알림 아이콘이 나타납니다. 작업 표시줄에는 알림 메시지가 수시로 보여지고 알림 아이콘을 마우스 오른쪽 버튼으로 선택하면 **알림 도구 모음(71쪽)**이 나타납니다. 알림 도구 모음을 사용하면 바이러스 검사를 바로 수행할 수 있습니다.

## **보안 설정(109쪽)**

실시간 감시 종료, 프로그램 삭제와 같은 주요 기능은 지정된 암호를 아는 사용자만 사용하도록 설정할 수 있습니다.

## **자체 보호(98쪽)**

V3Net for Windows Server 6.0를 구성하는 실행 파일들에 접근하는 프로세스를 실시간으로 감시하여 악성 코드의 접근을 차단합니다.

## **고급 검사 설정(97쪽)**

시스템 검사/감시 중에 메모리, 부트 영역, 시작 프로그램 V3Net for Windows Server 6.0 관련 실행 파일 등을 함께 검사할 수 있습니다.

## **긴급 바이러스 경보(52쪽)**

최근 확산되는 위험 바이러스에 대한 정보를 제공합니다. 긴급 경보 바이러스의 이름을 선택하면 (주)안철수연구소 홈페이지(<http://www.ahnlab.com>)에서 제공하는 바이러스 정보를 자세히 확인할 수 있습니다.

## **네트워크 차단(99쪽)**

네트워크를 통해서 신종 바이러스가 급속히 확산될 경우 감염 경로로 추정되는 특정 포트를 일시적으로 차단할 수 있습니다. 새로운 최신 엔진이 업데이트되기 전까지는 특정 포트를 차단하여 시스템을 안전하게 보호하는 것이 좋습니다.

### 경보 메일(105쪽)

사용자가 지정한 기간 동안에 지정한 숫자 이상의 바이러스가 발견되면 즉시 경보 메일을 받아볼 수 있습니다. 업데이트를 성공적으로 완료했거나 실패한 경우 또는 시스템 감시 재시작이 실패한 경우에도 경보 메일을 받아볼 수 있습니다.

## 시스템 사양

V3Net for Windows Server 6.0을 위해서는 다음과 같은 사양을 갖춘 시스템이 필요합니다.

### 하드웨어

| 항목         | 권장 사양                                                                                                                          | 최소 사양                            |
|------------|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| CPU        | Pentium III, IA 64, AMD 64 이상                                                                                                  | Pentium 150MHz, IA 64, AMD 64 이상 |
| RAM        | 256MB                                                                                                                          | 32MB 이상                          |
| HDD        | 200MB                                                                                                                          | 30MB 이상                          |
| CD-ROM     | 24배속 이상                                                                                                                        | 4배속 이상                           |
| Resolution | 1024 * 768                                                                                                                     | 800 * 600 이상                     |
| 운영 체제      | Windows NT Server 4.0(SP6 이상), Windows 2000 Server/Advanced Server/DataCenter Server, Windows 2003 Server Standard/Enterprise. |                                  |

**!** 주의 이 프로그램은 Windows NT/2000 Server/2003 Server에만 설치할 수 있습니다.  
Windows NT Server 4.0(SP6 이상)에 이 프로그램을 처음으로 설치한 경우에는 시스템을 다시 시작해야 할 수도 있습니다.



## 2장

---

# 시작하기

설치하기 /18

삭제하기 /26

V3Net for Windows Server 6.0을  
설치하고 삭제하는 방법을  
순서대로 설명합니다.

## 설치하기

**!** 주의 터미널 서비스를 사용해서 원격으로 V3Net for Windows Server 6.0을 설치할 경우에는 시스템을 다시 시작해야 합니다.

1. V3Net for Windows Server 6.0의 설치 CD를 CD-ROM 드라이브에 넣습니다. 아래와 같은 <V3Net for Windows Server 6.0 설치> 창이 나타납니다.

### 제품 설치

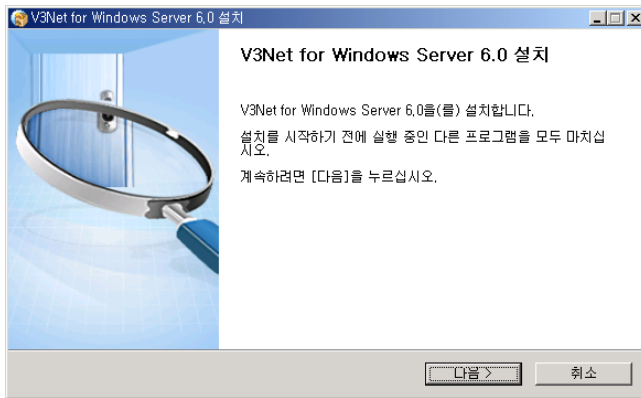


그림 1 V3Net for Windows Server 6.0 설치 시작

2. 다음 >을 누릅니다. <사용권 계약> 창이 나타나고 이 프로그램의 사용권 계약을 보여줍니다.

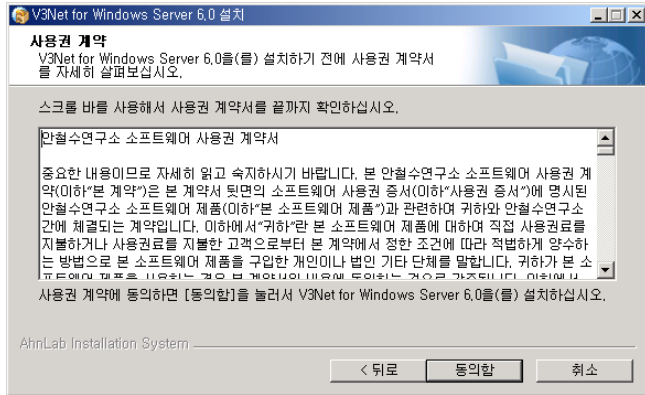


그림 2 사용권 계약

3. 사용권 계약서를 확인하고 계약서에 동의하면 **동의함**을 누르십시오. <다른 제품 설치 확인> 창이 나타납니다. 사용자의 컴퓨터에 다른 백신 제품이 설치되어 있지는 확인합니다. 다른 백신 제품이 설치되어 있으면 오류가 발생할 수 있으므로 **취소**를 눌러서 설치를 중지하고, 다른 백신 제품을 삭제한 다음 다시 설치하십시오.

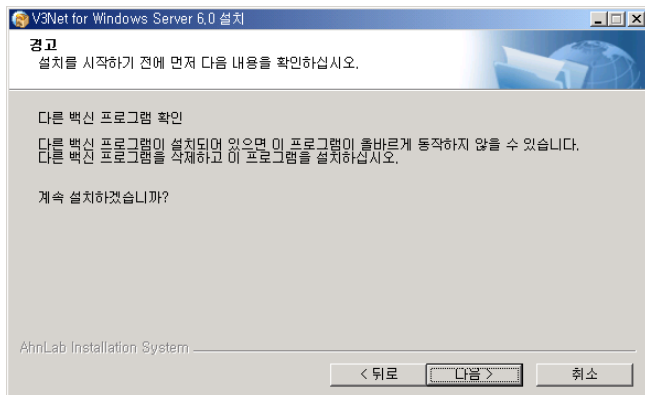


그림 3 다른 제품 설치 확인

4. 다른 백신 제품이 설치되어 있지 않으면 <다음>을 누르십시오. <사용자 정보> 창이 나타납니다. 제품을 구입한 사용자의 이름, 회사 이름, 제품 번호를 입력하십시오. 제품 번호는 제품 설치 CD에 적혀 있으며 하이픈(-)으로 구분하지 않고 입력해도 됩니다.

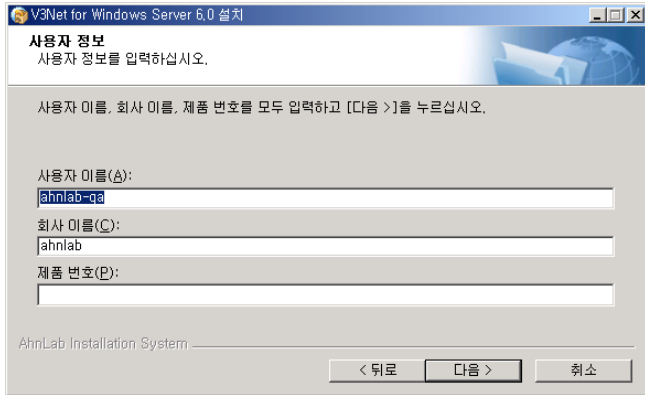
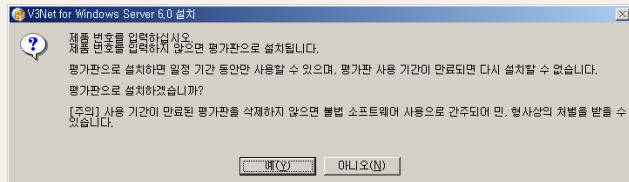


그림 4 사용자 정보

- ! 주의** 제품 번호를 입력하지 않고 평가판으로 설치하면 아래와 같은 창이 나타납니다. 평가판으로 설치하면 정해진 기간 동안만 이 제품을 사용할 수 있으며 사용 기간이 지난 제품은 [제어판]-[프로그램 추가/제거]에서 삭제해야 합니다. 사용 기간이 지난 제품을 삭제하지 않으면 불법 소프트웨어 사용으로 간주되어 민, 형사상의 처벌을 받을 수 있습니다.



5. 사용자 정보를 입력하고 **다음** > 을 누르십시오. <설치 폴더 선택> 창에 V3Net for Windows Server 6.0이 설치될 폴더 경로(C:\Program Files\Ahnlab\WV3)가 나타납니다. 설치 폴더를 바꾸려면 **찾아보기...**를 눌러서 설치할 폴더를 직접 선택하십시오.

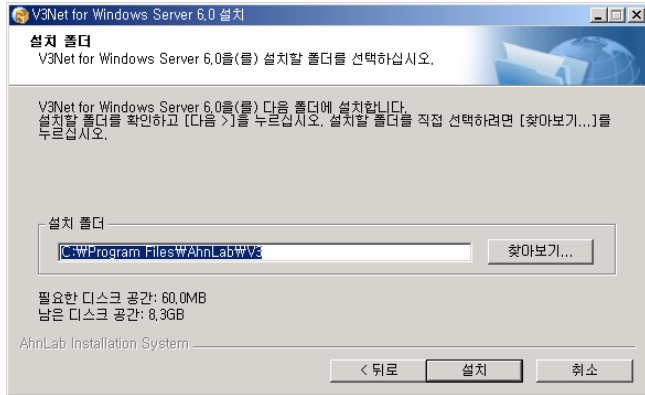


그림 5 설치 폴더 선택

6. 설치 폴더를 선택하고 **다음** > 을 누릅니다. <파일 복사> 창이 나타나서 설정 사항을 보여줍니다. 설치 폴더 및 설치 제품 이름을 확인합니다.

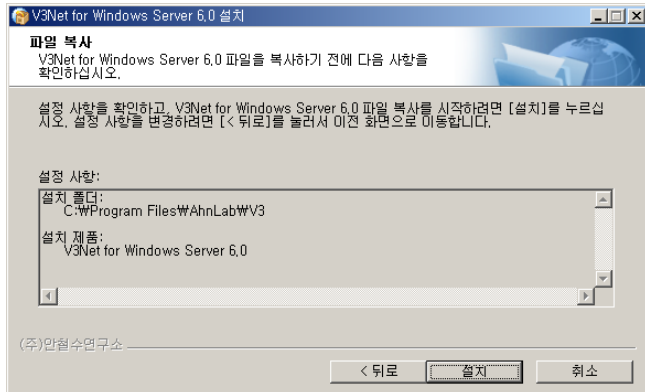


그림 6 파일 복사

7. 설정 사항을 확인하고 **설치**를 누릅니다. <설치 진행> 창이 나타나고 설치가 진행되고 있는 상황을 보여줍니다.

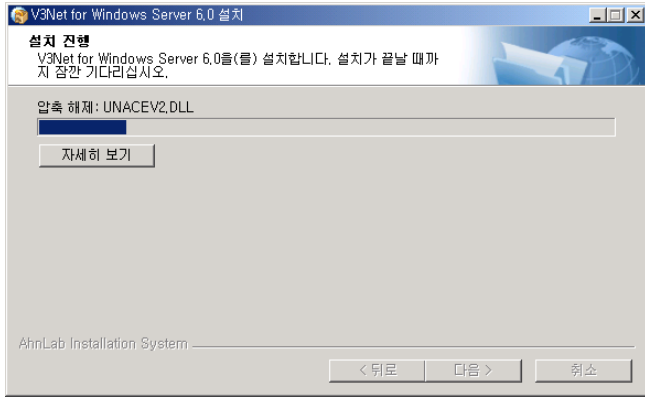


그림 7 설치 진행

8. 제품 설치가 완료되면 <V3Net for Windows Server 6.0 설치 완료> 창이 나타납니다. 제품 설치가 완료된 다음에 바로 실행할 항목만 선택하고, **마침**을 누르십시오.

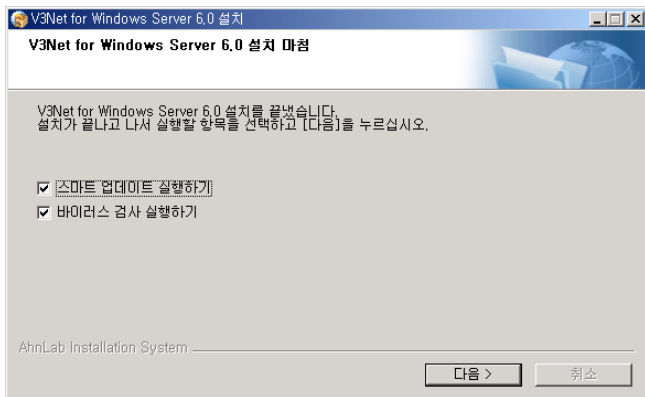


그림 8 V3Net for Windows Server 6.0 설치 완료

- 스마트 업데이트 실행하기: <스마트 업데이트 유틸리티> 창이 나타나고 최신 엔진을 다운로드 받습니다. 업데이트를 수행하려면 사용자의 컴퓨터가 인터넷과 연결되어 있어야 합니다.

- 바이러스 검사 실행하기: <시스템 검사> 창이 나타나고 바로 사용자의 시스템을 검사합니다.

9. <V3Net for Windows Server 6.0 설치 완료> 창에서 **스마트 업데이트 실행하기**를 선택했으면, <스마트 업데이트 유틸리티> 창이 나타납니다.

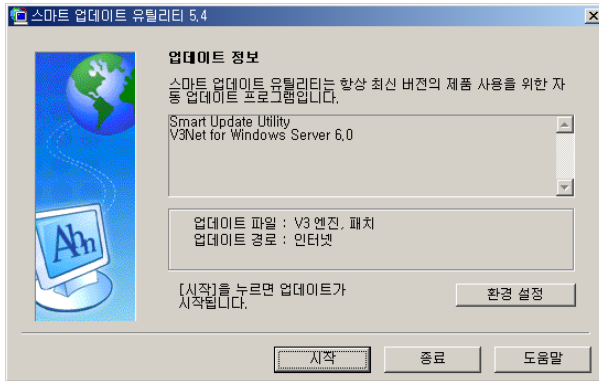


그림 9 스마트 업데이트 유틸리티

10. **시작**을 눌러서 최신 엔진으로 업데이트합니다. 최신 엔진 업데이트가 완료되면 업데이트 정보 파일 readme.txt가 나타납니다. 스마트 업데이트에 대한 자세한 내용은 최신 엔진 업데이트(30쪽)를 참고하십시오.

11. 스마트 업데이트가 완료되면 <환경 설정 마법사> 창이 나타납니다. 쉬운 설정에서 시스템 보호 수준을 선택합니다. 시스템 보호 수준을 선택하고 **완료**를 누릅니다.

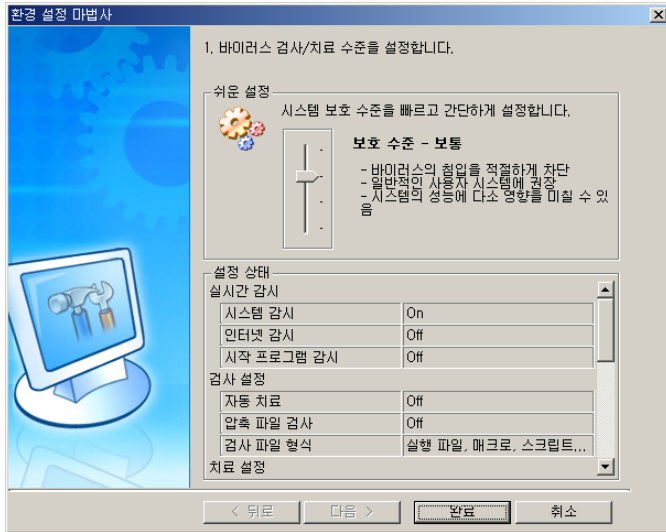


그림 10 환경 설정 마법사

### 환경 설정 - 쉬운 설정

- **높음**: 바이러스의 침입을 완벽하게 차단합니다. 바이러스 감염 위험이 높은 시스템에서 선택하는 것이 좋습니다. 시스템의 성능에 영향을 미칠 수도 있습니다.
- **보통**: 바이러스의 침입을 적절하게 차단(일반 사용자 시스템에 권장)
- **낮음**: 바이러스의 침입을 최저 수준으로 차단(바이러스 감염 위험이 낮은 시스템에 권장)
- **사용자 정의 설정**: 사용자가 직접 바이러스 검사/치료 환경을 설정할 수 있습니다. 이 항목을 선택하면 **다음**을 눌러서 자세한 검사 치료 방법을 설정할 수 있습니다. 자세한 방법은 환경 설정>쉬운 설정(75쪽)을 참고하십시오.

12. 환경 설정 정보가 저장되고 <환경 설정 마법사> 창이 닫힙니다. <V3Net for Windows Server 6.0 설치 완료> 창에서 **바이러스 검사 실행하기**를 선택했으면 <시스템 검사> 창이 나타납니다.

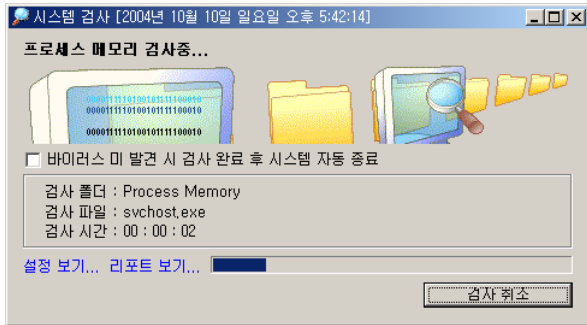


그림 11 시스템 검사

13. 시스템 검사가 완료되어 사용자의 시스템에 감염된 바이러스가 없으면 닫기를 눌러서 시스템 검사를 종료합니다. 발견된 바이러스가 있으면 **바이러스 검사/치료 > 시스템 검사/치료(46쪽)**를 참고하여 치료하십시오. <V3Net for Windows Server 6.0 설치 완료> 창이 나타납니다.



그림 12 V3Net for Windows Server 6.0 설치 완료

14. **마침**을 눌러서 V3Net for Windows Server 6.0 설치를 끝냅니다.

## 삭제하기

1. 작업 표시줄에서 실행을 누르고 프로그램을 선택합니다. 메뉴에서 V3Net for Windows Server 6.0을 선택하고 V3Net for Windows Server 6.0 제거를 누릅니다. 아래와 같은 <V3Net for Windows Server 6.0 삭제> 창이 나타납니다.

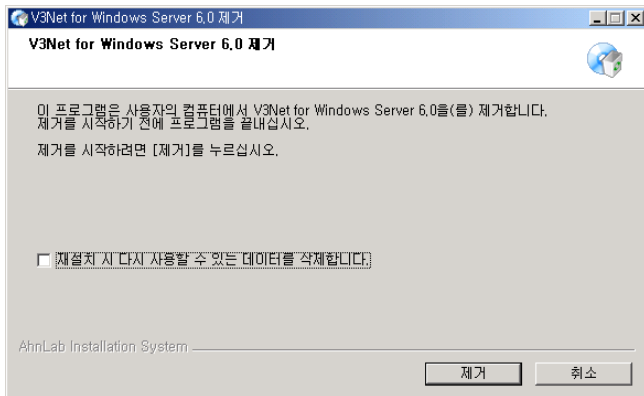


그림 13 V3Net for Windows Server 6.0 삭제 시작

2. V3Net for Windows Server 6.0을 삭제하려면 예를 누르십시오. 이벤트 기록, 검사 기록, 검역소 백업 파일 삭제를 선택하면 이 프로그램과 관련된 데이터들도 모두 완전히 삭제됩니다. V3Net for Windows Server 6.0을 다시 설치하여 사용할 경우에는 이 항목을 선택하지 않아도 됩니다. 아래와 같은 창이 나타납니다.

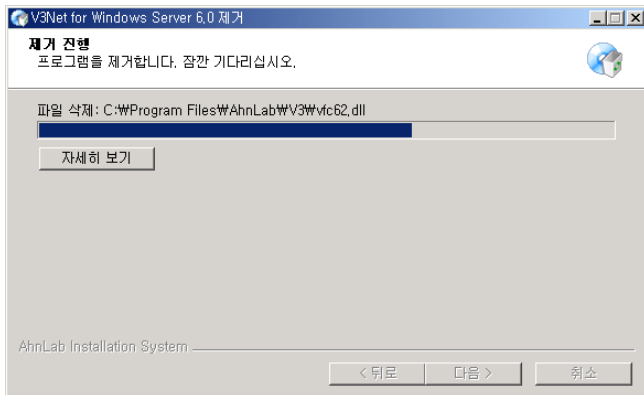


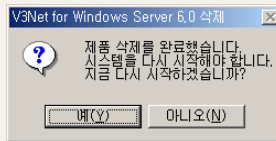
그림 14 V3Net for Windows Server 6.0 삭제

3. 삭제를 끝낼 때까지 잠깐 기다리십시오. 완료되면 다음과 같은 창이 나타납니다.



그림 15 V3Net for Windows Server 6.0 삭제 완료

**!** 주의 탐색기 검사나 오피스 프로텍터를 실행하고 있었거나 윈도우즈 탐색기나 Microsoft Internet Explorer를 실행하고 있었을 경우에는 제품 삭제가 완료되면 다음과 같은 창이 나타날 수 있습니다. 시스템을 다시 시작하지 않으려면 제품 삭제를 취소하고 탐색기 검사나 오피스 프로텍터를 중지하고 윈도우즈 탐색기나 Microsoft Internet Explorer를 종료한 다음 제품 삭제를 다시 시도하십시오.



4. **확인**을 눌러서 V3Net for Windows Server 6.0 삭제를 끝냅니다.



## 3장

---

# 최신 엔진 업데이트

스마트 업데이트 /30

업데이트 환경 설정 /32

V3Net for Windows Server 6.0의

최신 엔진을 업데이트하는 방법을 설명합니다.

최신 엔진으로 업데이트하지 않으면

새로 발견된 신종 바이러스를 치료할 수 없습니다.

## 스마트 업데이트

V3Net for Windows Server 6.0을 설치한 사용자는 반드시 다음과 같은 방법으로 최신 엔진으로 업데이트해야 합니다. 최신 엔진으로 업데이트하지 않으면 기존 엔진으로는 검사/치료가 되지 않는 새로운 바이러스에 감염될 수 있습니다. 매주 새롭게 업데이트 되는 엔진을 수시로 다운로드 받으십시오.

**! 주의** 최신 엔진을 업데이트하기 위해서는 반드시 사용자의 컴퓨터가 인터넷에 연결되어 있어야 합니다.

1. 다음과 같은 방법 중으로 <스마트 업데이트 유틸리티> 창을 실행합니다.

- 메뉴 바: 파일(F)>스마트 업데이트(U) 선택
- 도구 모음: 업데이트 선택
- 작업 표시줄: 알림 아이콘을 마우스 오른쪽 버튼으로 선택하고 스마트 업데이트... 선택
- 윈도우즈 탐색기/Microsoft Internet Explorer(5.0 이상): V3 도구 모음에서 스마트 업데이트... 선택

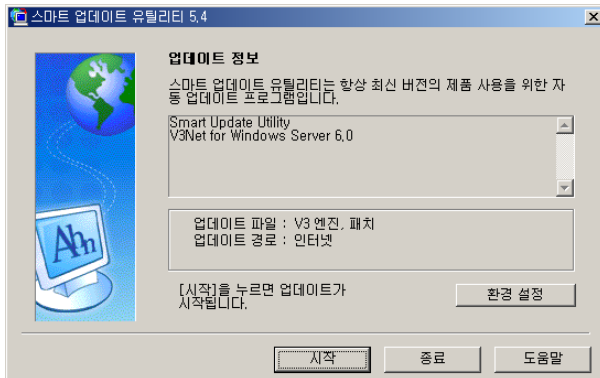


그림 16 업데이트 정보

2. 시작을 누르면, 업데이트할 최신 엔진 파일을 분석합니다. 시스템 분석 작업은 시스템 환경에 따라서 몇 분이 걸릴 수 있습니다. 모든 작업이 끝날 때까지 기다려 주십시오.

3. 사용자의 시스템에 최신 엔진 파일이 업데이트되면, 업데이트 정보 파일 `readme.txt`가 자동으로 나타납니다. 업데이트된 최신 엔진 정보를 확인하고, `readme.txt`을 닫습니다. Home 메뉴에서 **엔진 업데이트 내용보기**를 선택하면 `readme.txt` 파일을 다시 확인할 수 있습니다.

**!** 주의 탐색기 검사와 관련된 파일이 실행 중에 업데이트되었을 경우에는, 시스템을 다시 시작해야 합니다.

## 업데이트 환경 설정

1. 다음과 같은 방법으로 스마트 업데이트를 실행하면 <스마트 업데이트 유틸리티> 창이 나타납니다.

- 메뉴 바: 파일(F)>스마트 업데이트(U) 선택
- 도구 모음: 업데이트 선택
- 작업 표시줄: 알림 아이콘을 마우스 오른쪽 버튼으로 선택하고 스마트 업데이트... 선택
- 윈도우즈 탐색기/Microsoft Internet Explorer(5.0 이상): V3 도구 모음에서 스마트 업데이트... 선택

2. 환경 설정을 누르면, <업데이트 제품 선택> 창이 나타납니다.

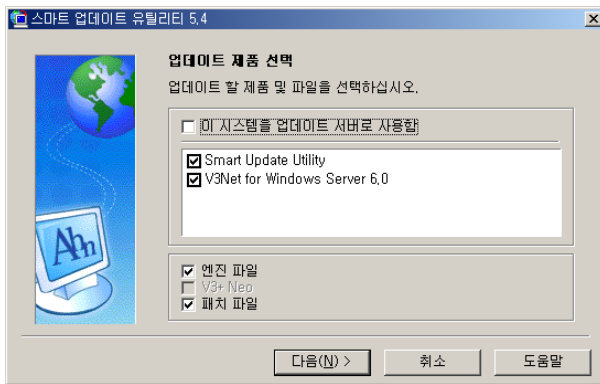


그림 17 업데이트 제품 선택

3. 업데이트할 제품 및 유틸리티를 선택하고, 다음(N) >을 누릅니다. <업데이트 방법> 창이 나타납니다.

### 업데이트 제품 선택

- 이 시스템을 업데이트 서버로 사용함: 사용자의 시스템에 연결된 다른 시스템들도 이 컴퓨터를 통해서 최신 엔진을 업데이트 받을 수 있습니다.
  - V3Net for Windows Server 6.0 기능과 관련된 파일들
  - Smart Update Utility: 최신 스마트 업데이트 유틸리티를 업데이트합니다.
- 엔진 파일: 최신 엔진 파일을 업데이트합니다.
- 패치 파일: 엔진 업데이트 패치 파일들을 업데이트합니다. (권장 사항)

4. 최신 엔진을 업데이트할 때 사용할 방법을 선택하고, **다음(N) >**을 누릅니다.

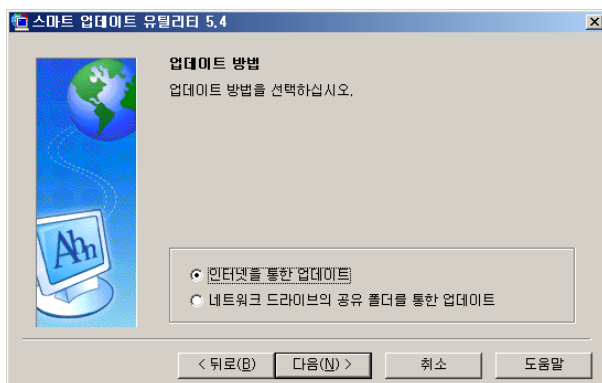


그림 18 업데이트 방법

### 업데이트 방법

- 인터넷을 통한 업데이트: 인터넷을 사용해서 ㈜안철수연구소의 인터넷 서버로부터 최신 엔진 파일을 직접 업데이트합니다.(개인 사용자 권장)
- 네트워크 드라이브의 공유 폴더를 통한 업데이트: 최신 엔진 파일을 다운로드 받은 컴퓨터를 업데이트 서버로 설정하여, 로컬 네트워크를 통해서 연결된 여러 시스템들이 공유합니다.(기업 네트워크 사용자 권장)

5. 이전 단계에서 인터넷을 통한 업데이트를 선택했으면 <인터넷 설정> 창이, 네트워크 드라이브의 공유 폴더를 통한 업데이트를 선택했으면, <공유 폴더 설정> 창이 나타납니다. 필요한 정보를 입력하고 **다음(N) >**을 누릅니다.

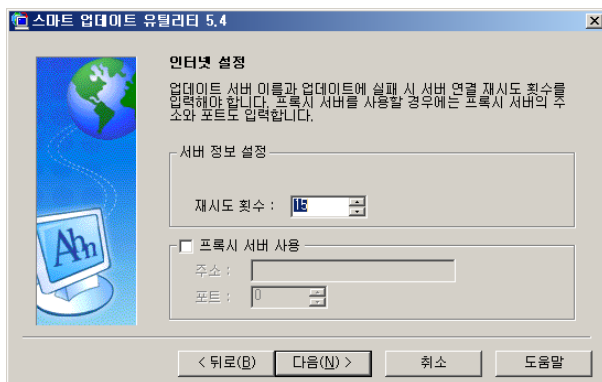


그림 19 인터넷 설정

## 인터넷 설정

- 서버 정보 설정
  - 위치: 인터넷 업데이트 서버가 속한 국가/지역
  - 다시 시도 횟수: 웹 서버 접속을 실패했을 경우 서버 연결 다시 시도 횟수 (기본 값: 15)
- 프록시 서버 사용: 프록시 서버를 사용해서 홈페이지에 접속
  - 주소: 프록시 서버의 주소
  - 포트 : 프록시 서버에서 사용하는 포트

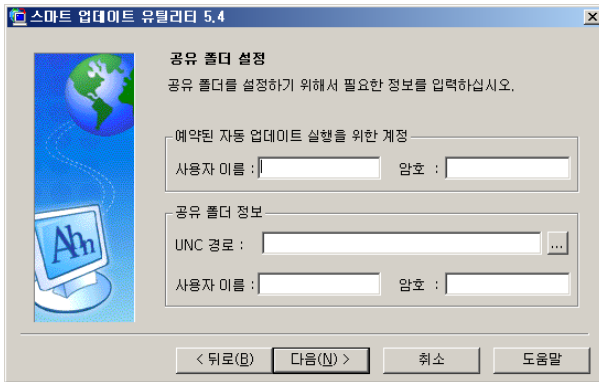


그림 20 공유 폴더 설정

## 공유 폴더 설정

- 예약 자동 업데이트 실행을 위한 계정
  - 사용자 이름: 예약 자동 업데이트를 위해서 필요한 네트워크에 접속할 수 있는 사용자 ID
  - 암호: 예약 자동 업데이트를 위해서 필요한 네트워크에 접속할 수 있는 암호
- 공유 폴더 정보
  - UNC(Universal Naming Convention)경로: 네트워크 드라이브를 통해서 공유된 폴더의 경로. [...]을 눌러서 경로를 지정할 수 있습니다.
  - 사용자 이름: 공유 폴더에 접속할 수 있는 사용자 ID
  - 암호: 공유 폴더에 접속할 수 있는 암호

6. 엔진 업데이트를 수행하기 위해서 필요한 일반 옵션을 설정하고 **다음(N) >**을 누릅니다.

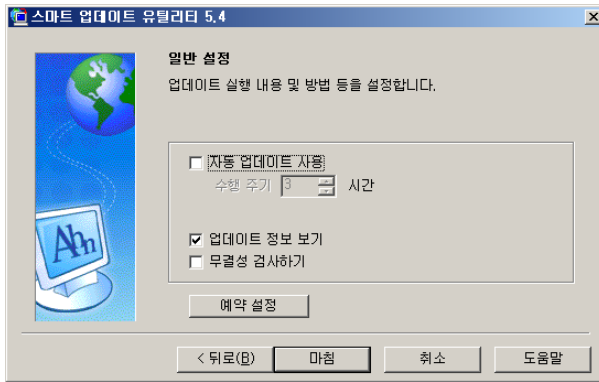


그림 21 일반 설정

### 일반 설정

- 자동 업데이트 사용: 설정된 시간마다 자동으로 엔진 버전을 확인하고 최신 엔진을 업데이트합니다.
  - 수행 주기(시간): 엔진 자동 업데이트 주기
- 업데이트 정보 보기: 최신 업데이트에서 추가 및 변경된 내용이 적힌 readme.txt 파일을 보여줍니다.
- 무결성 검사하기: 다운로드 한 최신 엔진 파일을 적용하기 전에 무결성을 검사합니다.

7. 스마트 업데이트 환경 설정을 완료했으면 **마침**을 눌러서 끝냅니다. 엔진 업데이트 일정을 예약해 두려면 **예약 설정**을 누르십시오. <예약 설정> 창이 나타납니다. Home 메뉴에서 **예약 설정>엔진 업데이트 예약 more**을 선택해도 <예약 설정> 창을 열 수 있습니다.

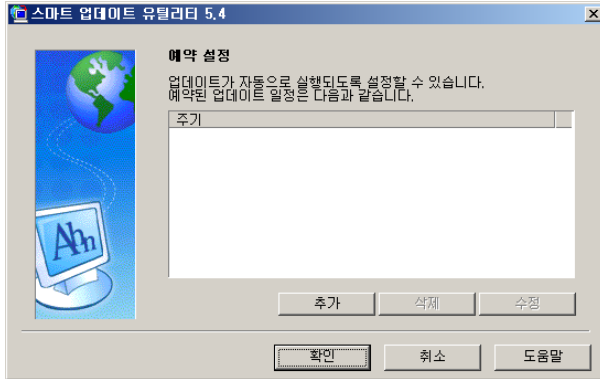


그림 22 예약 설정

8. **추가**를 누르십시오. <예약 설정> 창이 나타납니다.

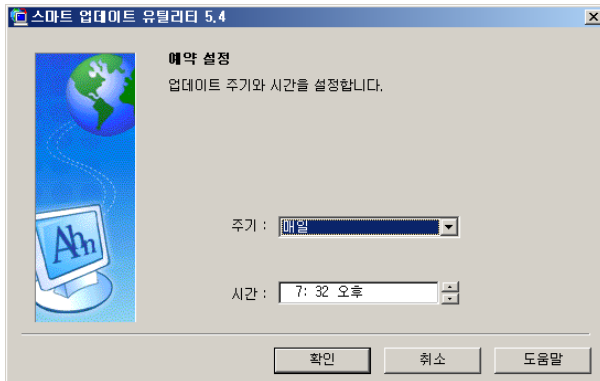


그림 23 예약 주기 설정

9. 엔진 업데이트 주기 및 시간을 설정한 다음 **확인**을 누릅니다. 등록된 엔진 업데이트 일정을 수정 또는 삭제하려면, 일정을 선택하고 **수정** 또는 **삭제**를 누릅니다.

#### 예약설정

- 주기
  - 매일  
시간 예) 5:14 오후
  - 매주  
요일 예) 금요일  
시간 예) 5:14 오후
  - 매달  
일 예) 15일  
시간 예) 5:14 오후
  - 한번  
날짜 예) 2004년 11월 06일  
시간 예) 5:14 오후

10. 엔진 업데이트 예약 설정을 완료했으면 **확인**을 눌러서 스마트 업데이트 <일반 설정> 창으로 되돌아갑니다. **미침**을 누르면 <업데이트 정보> 창이 열리고 **종료**를 누르면 창이 닫힙니다.



---

## 바이러스 검사 및 치료

한번 따라하기 /40

시스템 검사 /41

실시간 감시 /44

바이러스 치료 /46

V3Net for Windows Server 6.0으로

사용자의 시스템을 검사하여

감염된 파일을 치료하는 방법을 설명합니다.

## 한번 따라하기

---

기본 기능을 사용해서 쉽고 빠르게 이 제품을 사용하는 방법은 다음과 같습니다.

1. 상단 도구 모음에서 **업데이트(30쪽)**를 선택합니다. : 최신 엔진을 업데이트 받습니다.
2. 왼쪽에 있는 기본 메뉴에서 Home을 누르고 **실시간 감시(44쪽)**를 실행(On)합니다. : 바이러스 침입을 사전에 차단합니다.
3. 왼쪽에 있는 기본 메뉴에서 **시스템 검사(41쪽)**를 선택하고 **검사 실행**을 누릅니다. : 이 제품을 설치하기 전에 이미 바이러스에 감염된 파일이 없는지 확인합니다. 바이러스에 감염된 파일이 발견되면 **바이러스 치료(46쪽)**를 수행합니다.
4. 상단 도구 모음에서 **환경 설정**을 선택하고, <환경 설정> 창의 **쉬운 설정(75쪽)** 메뉴에서 시스템 보호 수준(높음, 보통, 낮음, 사용자 정의)을 지정합니다.

☒ **참고** 각 검사/감시 방법에 대한 자세한 검사/치료 설정은 **환경 설정(73쪽)**을 참고하십시오.

## 시스템 검사

시스템 검사를 실행하여 사용자의 시스템에서 바이러스에 감염된 파일은 없는지 수시로 확인합니다.

1. 왼쪽 프레임에 있는 기본 메뉴에서 **시스템 검사**를 선택합니다.
2. 상단에 있는 버튼을 눌러서 검사할 영역을 지정합니다.
  - 사용자 검사 목록: 자주 검사하는 대상(드라이브, 폴더 등)을 선택해서 사용자 검사 목록으로 설정해 둡니다.
  - 드라이브 단위로 검사: 검사할 드라이브를 선택합니다.
  - 폴더 단위로 검사: 검사할 폴더만 선택합니다.
  - 로컬 하드 드라이브: 로컬 하드디스크 드라이브만 검사합니다.
3. **검사 실행**을 누릅니다. <시스템 검사> 창이 나타나고, 바이러스 검사가 시작됩니다.

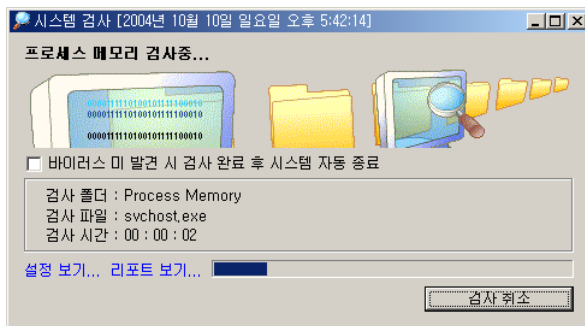


그림 24 시스템 검사

4. 바이러스 검사 진행 상태를 확인합니다. **검사 취소**를 누르면 검사를 중지할 수 있습니다.
  - 바이러스 미 발견 시 검사 완료 후 시스템 자동 종료: 검사 결과 발견된 바이러스가 없으면 시스템을 자동으로 종료합니다.
  - 설정 보기...: 바이러스 검사/치료 설정 내역을 확인할 수 있습니다. 시스템 검사에 대한 검사/치료 설정은 환경 설정의 **시스템 검사(79쪽)**에서 변경할 수 있

습니다.

- 리포트 보기...: 바이러스 검사 진행 상태를 각 영역 별(메모리/주 부트 섹터/도스 부트 섹터/실행 프로세스/파일)로 자세히 확인할 수 있습니다.

5. 바이러스 검사가 완료되고 발견된 바이러스가 없으면 **닫기**를 눌러서 <시스템 검사> 창을 닫습니다. 발견된 바이러스가 있으면 바이러스 치료 > 시스템 검사 (46쪽)를 참고하여 치료하십시오.

## 사용자 검사 목록

자주 검사하는 영역은 사용자 검사 목록으로 저장하여 검사할 때 사용할 수 있습니다.

1. 시스템 검사 메뉴에서 **사용자 검사 목록**을 누릅니다. 다음과 같은 <사용자 검사 목록> 창이 나타납니다.

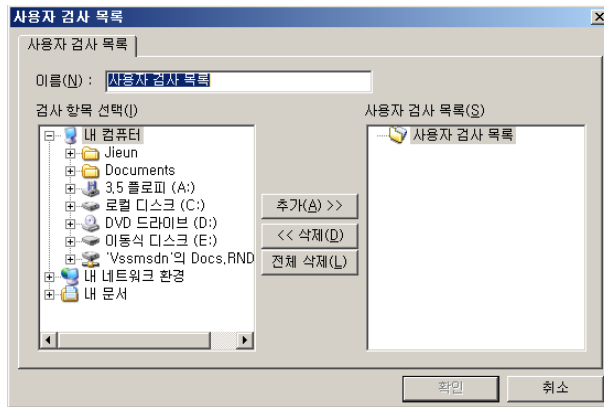


그림 25 사용자 검사 목록

2. 검사 항목 선택에서 자주 검사하는 영역을 선택하고, **추가(A) >>**를 누릅니다.
3. 사용자 검사 목록에 새로운 검사 목록이 등록되어 나타납니다.
4. 검사할 영역을 모두 추가했으면 **확인**을 눌러서 <사용자 검사 목록> 창을 닫습니다.
5. 사용자 검사 항목을 선택하고, **검사 실행**을 누르면 추가한 영역을 검사합니다.

## 빠른 검사

상단 도구 모음에 있는 빠른 검사 줄에 검사할 영역을 바로 입력해서 빠르게 검사할 수도 있습니다.

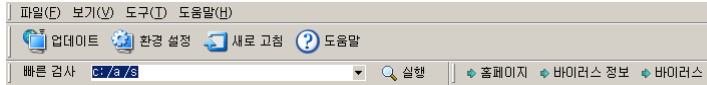


그림 26 빠른 검사 줄

1. 빠른 검사 줄에 다음과 같은 형식으로 검사할 영역을 지정합니다. 여러 개의 폴더를 한꺼번에 검사할 경우에는 공백으로 구분해서 입력합니다. 폴더 이름에 공백이 포함되어 있을 경우에는 큰 따옴표(“”)로 구분해서 입력합니다.

### [드라이브] [폴더] [파일] [옵션]

- 드라이브 : 예) C:
- 폴더 : 예) C:\winnt
- 파일 : 예) D:\data\homework.txt
- 옵션
  - 하위 폴더 포함: /s
  - 여러 개의 폴더: 공백으로 구분
  - 모든 파일 검사: /a
  - 압축 파일 검사: /c
  - 네트워크 공유 폴더: \\로 구분 예) \\ABC\l
  - 옵션 확인: /?

2. 실행을 누릅니다. <바이러스 검사> 창이 나타나서 지정한 영역을 검사한 결과를 보여줍니다.
3. 발견된 바이러스가 없으면 닫기를 눌러서 바이러스 검사를 마칩니다.

## 실시간 감시

사용자의 시스템에 바이러스가 침입하지 못하도록 Home 메뉴에서 실시간 감시를 실행(On) 시켜 둡니다.



그림 27 Home 작업 창

실시간 감시는 다음과 같은 방법으로도 실행할 수 있습니다.

- 메뉴 바의 도구(T)>실시간 감시(A)를 실행합니다.
- 작업 표시줄에 있는 V3 알람 아이콘을 마우스 오른쪽 버튼으로 선택해서 실시간 감시를 실행합니다.
- <환경 설정> 창의 시스템 검사/감시(77쪽) 메뉴에서 실행할 실시간 감시 기능을 선택합니다.

## 시스템 감시

사용자 시스템의 일반 응용 프로그램에서 접근하는 모든 파일 및 데이터를 실시간으로 검사합니다. 바이러스의 침입을 실시간으로 차단하기 위해서는 시스템 감시 기능을 항상 실행해 두는 것이 좋습니다. 시스템 감시 기능을 중지하면 다음과 같은 <알림> 창이 나타나고 작업 표시줄에 있는 V3Net for Windows Server 6.0 알림 아이콘이 와 같이 회색으로 표시됩니다.

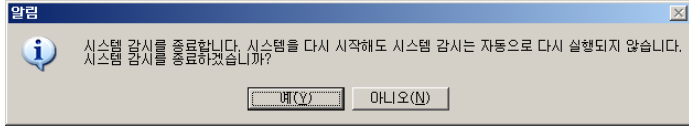


그림 28 시스템 감시 알림

## 인터넷 감시

인터넷 웹 브라우저를 통해서 다운로드되는 모든 데이터 및 파일들을 실시간으로 검사합니다.

## 시작 프로그램 감시

시작 프로그램의 레지스트리, 시작 프로그램 폴더, 시스템 파일에 등록된 시작 프로그램들을 윈도우즈를 시작할 때마다 자동으로 검사합니다.

**! 주의** 시작 프로그램 감시 기능이 동작 중일 때 새로운 사용자 계정이 등록되면 등록된 계정에 대한 시작 프로그램 폴더 및 레지스트리는 시작 프로그램 감시 대상에 바로 포함되지 않습니다. 추가된 사용자 계정에 대한 시작 프로그램 폴더 및 레지스트리도 시작 프로그램 감시 대상에 포함시키려면 시작 프로그램 감시 기능을 중지하고 다시 실행하십시오.

## 바이러스 치료

실시간 감시, 인터넷 감시 등을 실행(On)시켜 두었거나 시스템 검사를 실행하여 바이러스가 발견되면 다음과 같은 방법으로 치료합니다.

- ☑참고 바이러스에 감염된 파일은 복사되어 검역소에 저장됩니다. 치료 도중에 파일이 손상되었거나 치료하지 못한 경우에는 검역소에서 백업 파일을 복원하여 사용할 수도 있습니다.

### 시스템 검사/치료

1. 시스템 검사 중에 바이러스에 감염된 파일이 발견되면, 다음과 같은 창이 나타납니다.

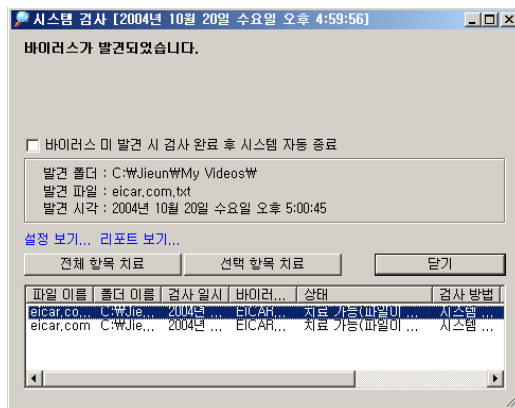


그림 29 시스템 검사 결과/치료

2. 바이러스에 감염된 파일 정보를 확인하고 치료합니다.

- 파일 이름: 바이러스에 감염된 파일의 이름
- 폴더 이름: 감염된 파일이 위치한 폴더 경로
- 검사 일시: 검사한 날짜 및 시각
- 바이러스 이름: 감염된 바이러스의 이름
- 상태: 치료 예정
- 검사 방법: 시스템 검사 / 시스템 감시 / 인터넷 감시 등
- 소유자: 감염된 파일을 읽고 쓸 수 있는 권한을 가진 사용자

3. 다음 링크를 누르면 바이러스 검사/치료 방법 및 검사 진행 상태를 확인할 수 있습니다. 자세한 검사/치료 방법은 환경 설정 > 시스템 검사(79쪽)를 확인하십시오.

- 설정 보기...: 바이러스 검사/치료 환경 설정 내용
- 리포트 보기...: 바이러스 검사 수행 내용

4. 감염 파일 목록 중에서 치료할 파일만 선택해서 치료합니다. 여러 개의 파일을 선택할 경우에는, 마우스 또는 Ctrl 키를 누르고 선택합니다.

- 전체 항목 치료: 시스템 검사 결과 발견된 모든 감염 파일을 치료합니다.
- 선택 항목 치료: 감염 파일 목록에서 특정 파일만 선택하여 치료합니다. 여러 개의 파일을 선택하려면 마우스로 드래그하거나 Ctrl 키를 누르고 선택합니다.
- 닫기: 바이러스 치료가 끝나면 검사 창을 닫습니다.

5. 전체 항목 치료 또는 선택 항목 치료를 누르면 다음과 같은 <주의> 창이 나타납니다.

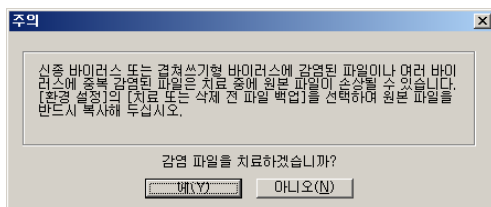


그림 30 바이러스 치료 전 주의

6. 치료 중에 파일이 손상될 수도 있으므로 감염된 파일을 복사해 둔 다음 예(Y)를 눌러서 치료합니다. 아래와 같은 창이 나타나면 **확인**을 누릅니다.

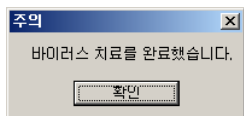


그림 31 바이러스 치료 완료

## 실시간 감시/치료

1. 실시간 감시 중에 바이러스에 감염된 파일이 발견되면, 다음과 같은 창이 나타납니다.

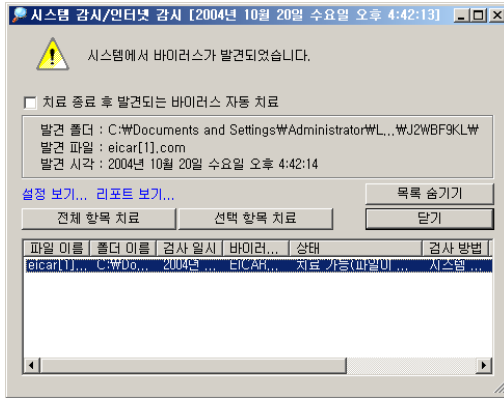


그림 32 시스템/인터넷 감시 결과

2. 바이러스에 감염된 파일 정보를 확인하고 치료합니다.
  - 파일 이름: 바이러스에 감염된 파일의 이름
  - 폴더 이름: 감염된 파일이 위치한 폴더 경로
  - 검사 일시: 검사한 날짜 및 시간
  - 바이러스 이름: 감염된 바이러스의 이름
  - 상태: 치료 예정
  - 검사 방법: 시스템 검사 / 시스템 감시 / 인터넷 감시 등
  - 소유자: 감염된 파일을 읽고 쓸 수 있는 권한을 가진 사용자
3. 다음 링크를 누르면 바이러스 검사/치료 방법 및 검사 진행 상태를 확인할 수 있습니다. 보다 자세한 검사/치료 방법은 환경 설정 > 시스템 감시/인터넷 감시/시작 프로그램 감시(90쪽)를 확인하십시오.
  - 설정 보기...: 바이러스 검사/치료 환경 설정 내용
  - 리포트 보기...: 바이러스 검사 수행 내용

4. 감염 파일 목록 중에서 치료할 파일만 선택해서 치료합니다. 여러 개의 파일을 선택할 경우에는, 마우스로 드래그하거나 Ctrl 키를 누르고 선택합니다.

- 전체 항목 치료: 시스템 검사 결과 발견된 모든 감염 파일을 치료합니다.
- 선택 항목 치료: 감염 파일 목록에서 특정 파일만 선택하여 치료합니다. 여러 개의 파일을 선택하려면 마우스 또는 Ctrl 키를 누르고 선택합니다.
- 닫기: 바이러스 치료가 끝나면 검사 창을 닫습니다.

5. 전체 항목 치료 또는 선택 항목 치료를 누르면 다음과 같은 <주의> 창이 나타납니다.

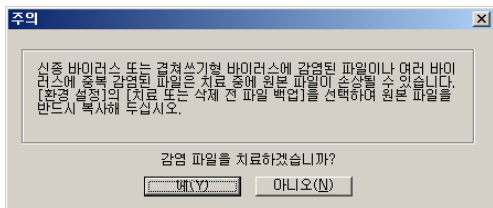


그림 33 치료 전 주의

6. 치료 중에 파일이 손상될 수도 있으므로 감염된 파일을 복사해 둔 다음 예(Y)를 눌러서 치료합니다. 아래와 같은 창이 나타나면 **확인**을 누릅니다.

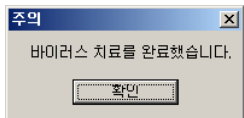


그림 34 바이러스 치료 완료



## 5장

---

# 둘러보기

Home /52

시스템 검사 /54

이벤트 기록 /56

검사 기록 /58

검역소 /61

보안 경고 리포트 /64

메뉴 /66

알림 메시지 /69

도구 모음 /71

V3Net for Windows Server 6.0를 구성하는  
메뉴를 살펴보고 각 메뉴의 사용법을 설명합니다.

# Home

V3Net for Windows Server 6.0을 실행하면 처음 나타나는 Home 작업 창입니다.



그림 35 Home 작업 창

## 최신 긴급 바이러스

오른쪽 상단 긴급 경고 창에는 최근 급속히 확산되고 있는 바이러스에 대한 정보가 나타납니다. 바이러스 이름을 누르면, ㈜안철수연구소 홈페이지의 긴급 경고 바이러스 메뉴로 바로 연결됩니다.

**! 참고** 긴급 바이러스 경고 창 오른쪽 상단의 x를 누르면 긴급 경고 창을 닫을 수 있습니다. 긴급 경고 창을 다시 보려면, **환경설정 > 기타 설정(111쪽)**을 누르고 **Home 창에 긴급 경고 표시**를 선택하십시오.

## 엔진 업데이트

- 엔진 날짜: 마지막으로 업데이트 된 엔진의 날짜
- 엔진 업데이트 내용 보기 more: 엔진 업데이트를 한번 이상 수행하면 마지막으로 업데이트된 엔진에 대한 자세한 내용이 적힌 readme.txt를 확인할 수 있습니다.

## 실시간 감시

실시간 감시 기능을 실행(On) 또는 중지(Off)할 수 있습니다. <환경 설정> 창의 시스템 검사/감시 (77쪽)나 작업 표시줄에 있는 알림 메뉴에서도 실시간 감시 기능을 실행(On) 또는 중지(Off)할 수 있습니다. 각 감시 기능 별로 **more**를 누르면 <환경 설정> 창이 나타나서 검사/치료 설정을 할 수 있습니다.

## 네트워크 차단

**포트 차단** 기능을 실행(On) 또는 중지(Off)할 수 있습니다. **more**를 누르면 <환경 설정> 창의 **네트워크 차단** > 포트 차단 (99쪽)이 나타나고 차단할 포트를 직접 선택 및 등록할 수 있습니다.

## 예약 설정

- 엔진 업데이트 예약 **more**: 주기를 설정해 두면 자동으로 최신 엔진을 업데이트할 수 있습니다.
- 예약 검사 **more**: 주기를 설정하여 자동으로 특정 폴더를 검사할 수 있습니다.

## 마지막 검사 수행 내용

최근에 수행한 검사 시간, 검사한 영역 및 검사 결과 발견된 감염 파일 개수 등을 자세히 확인할 수 있습니다. 각 날짜 별로 수행한 검사 결과는 왼쪽에 있는 검사 기록 (58쪽) 메뉴에서 자세히 확인할 수 있습니다.

## 시스템 검사

시스템 검사를 실행하여 사용자의 시스템에서 바이러스에 감염된 파일은 없는지 수시로 확인합니다.

1. 왼쪽 프레임에 있는 기본 메뉴에서 **시스템 검사**를 선택합니다.
2. 상단에 있는 다음과 같은 버튼을 눌러서 검사할 영역을 지정합니다.
  - 사용자 검사 목록: 자주 검사하는 대상(드라이브, 폴더 등)을 선택해서 사용자 검사 목록으로 설정해 둡니다.
  - 드라이브 단위로 검사: 검사할 드라이브를 선택합니다.
  - 폴더 단위로 검사: 검사할 폴더만 선택합니다.
  - 로컬 하드 드라이브: 로컬 하드 드라이브만 검사합니다.
3. **검사 실행**을 누릅니다. <시스템 검사> 창이 나타나고, 바이러스 검사가 시작됩니다.

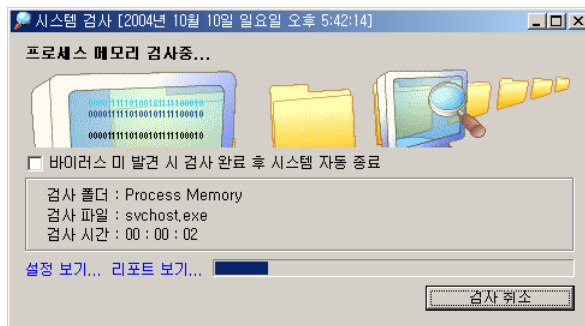


그림 36 시스템 검사

4. 바이러스 검사 진행 상태를 확인합니다. **검사 취소**를 누르면 검사를 중지할 수 있습니다.
  - 바이러스 미 발견 시 검사 완료 후 시스템 자동 종료: 검사 결과 발견된 바이러스가 없으면 시스템을 자동으로 종료합니다.
  - 설정 보기...: 바이러스 검사/치료 설정 내역을 확인할 수 있습니다. 시스템 검사에 대한 검사/치료 설정은 환경 설정의 시스템 검사(79쪽)에서 변경할 수 있습니다.

- 리포트 보기...: 바이러스 검사 진행 상태를 각 영역 별(메모리/주 부트 섹터/도스 부트 섹터/실행 프로세스/파일)로 자세히 확인할 수 있습니다.

5. 바이러스 검사가 끝나고 발견된 바이러스가 없으면 **닫기**를 눌러서 <시스템 검사> 창을 닫습니다. 발견된 바이러스가 있으면 바이러스 치료 > 시스템 검사 (46쪽)를 참고하여 치료하십시오.

## 이벤트 기록

왼쪽 메뉴에서 **이벤트 기록**을 누르면 이 프로그램을 사용한 작업 내역을 날짜 별로 확인할 수 있습니다.

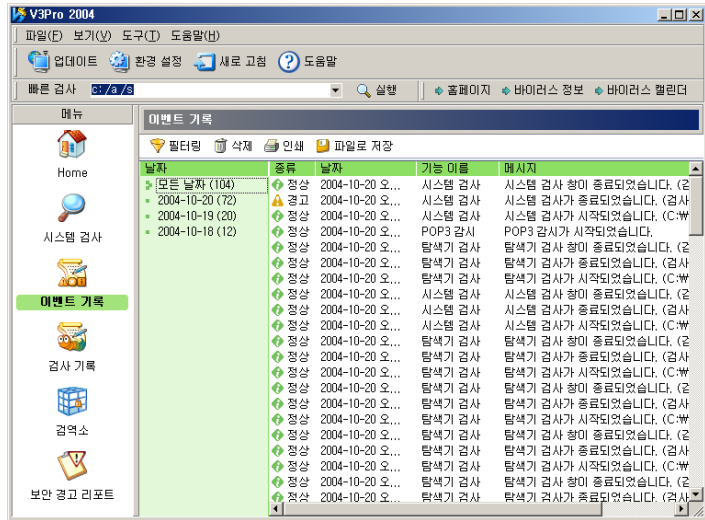


그림 37 이벤트 기록

이벤트 기록은 각 날짜 별로 필터링, 삭제, 인쇄, 파일로 저장할 수 있습니다.

- ☒ **참고** 이벤트 기록은 <환경 설정> 창의 **기타 설정(111쪽)** > **디스크 공간 지정** > **이벤트 기록 저장 공간**에서 지정한 개수를 초과하면 자동으로 삭제됩니다.

### 필터링

1. 이벤트 기록을 검색할 날짜를 선택하고, 상단의 **필터링**을 누릅니다.
2. <이벤트 기록 필터링> 창이 나타납니다. 필터링할 이벤트 기록 종류를 선택합니다.

• 기간: 처음부터와 마지막까지를 선택하거나 직접 날짜를 선택할 수 있습니다.

- 종류: 필터링할 이벤트 기록의 종류를 선택합니다.
  - 정상
  - 에러
  - 경고

3. **확인**을 누르면 필터링 조건에 맞는 이벤트 기록만 검색되어 나타납니다.

## 삭제

1. 이벤트 기록을 삭제할 날짜를 선택하고, 상단에 있는 **삭제**를 누릅니다.
2. <확인> 창이 나타나서 선택한 날짜의 이벤트 기록이 모두 지워짐을 알려줍니다.
3. **확인**을 누르면, 선택한 날짜에 등록된 이벤트 기록이 모두 삭제됩니다.

## 인쇄

1. 인쇄할 이벤트 기록이 있는 날짜를 선택하고, 상단에 있는 **인쇄**를 누릅니다.
2. <인쇄 설정> 창이 나타납니다. 프린터 및 용지 설정을 확인하고 **확인**을 누릅니다.
3. 선택한 날짜에 등록된 모든 이벤트 기록이 인쇄됩니다.

## 파일로 저장

1. 하나의 파일로 저장할 이벤트 기록이 있는 날짜를 선택하고, 상단의 **파일로 저장**을 누릅니다.
2. <다른 이름으로 저장> 창이 나타납니다. 이벤트 기록을 저장할 파일의 경로와 이름, 형식을 입력하고, **저장**을 누릅니다.
  - 파일 이름: 선택한 날짜를 yyyyymmdd와 같은 형식으로 입력하는 것이 좋습니다.  
예) 2004년 11월 6일의 이벤트 기록을 저장한 파일 이름: 20041106log
  - 파일 형식: 확장자가 CSV인 Excel 파일/확장자가 txt인 텍스트 파일 등으로 저장할 수 있습니다.
3. 선택한 날짜에 등록된 모든 이벤트 기록은 지정한 파일에 저장됩니다.

## 검사 기록

왼쪽 메뉴에서 검사 기록을 누르면 이 프로그램을 사용해서 바이러스 검사한 내역을 날짜 별로 확인할 수 있습니다.

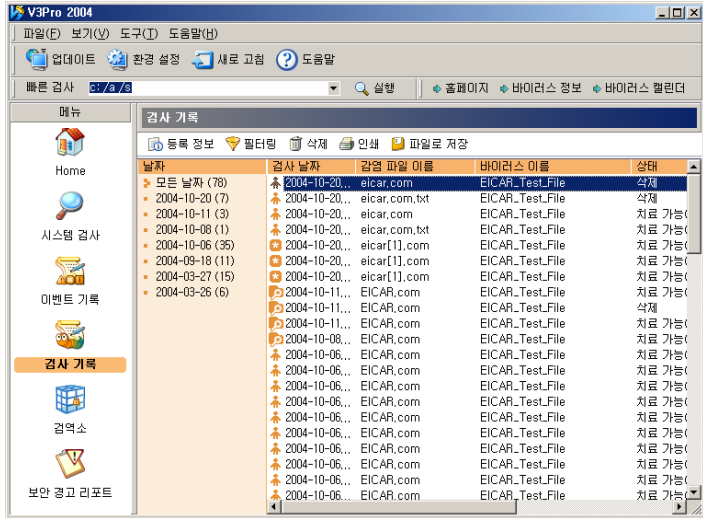


그림 38 검사 기록

검사 기록은 각 날짜 별로 필터링, 삭제, 인쇄, 파일로 저장할 수 있습니다.

☒ 참고 검사 기록을 보관하지 않으려면 <환경 설정> 창의 **기타 설정 (11쪽)** > **디스크 공간 지정** 에서 **검사 기록 보관**을 선택 해제 하십시오. 검사 기록은 **검사 기록 저장 공간**에서 지정한 용량을 초과하면 자동으로 삭제됩니다.

### 등록 정보

1. 각 날짜 별로 등록된 바이러스 검사 기록 중에서 하나를 선택합니다.
2. 상단에 있는 등록 정보를 누릅니다.

**3. 선택한 바이러스 검사 기록에 대한 자세한 등록 정보가 나타납니다.**

- 검사 날짜: 검사 날짜 및 시각
- 바이러스 이름: 감염된 바이러스 이름
- 감염 파일 이름: 감염된 파일이 저장된 폴더 경로 및 이름
- 상태: 치료 가능/치료 불가/치료 예정/치료 완료/삭제
- 검사 방법: 시스템 검사/시스템 감시/탐색기 검사 등
- 소유자: 감염된 파일을 읽고 쓸 수 있는 권한을 가진 사용자
- 접근자: 해당 파일에 접근 가능한 권한이 있는 로그인한 사용자
- 감염자: 해당 파일을 감염시킨 사용자

## 필터링

**1. 바이러스 검사 기록을 필터링할 날짜를 선택합니다.**

**2. <검사 기록 필터링> 창이 나타납니다. 필터링할 검사 기록 종류를 선택합니다.**

- 기간: **처음부터와 마지막까지**를 선택하거나 직접 날짜를 선택할 수 있습니다.
- 상태: 필터링할 검사 기록의 상태를 선택합니다.
- 치료 전
  - 치료 가능: 치료할 수 있음
  - 신종 바이러스: 치료할 수 없음(신고 센터로 전송 가능)
  - 압축 파일: 압축된 파일
- 치료 후
  - 치료 완료
  - 삭제됨: 성공적으로 치료되어 시스템에서 삭제됨
  - 치료 실패
  - 이름 변경: 치료된 결과 이름이 변경됨

**3. 확인**을 누르면 필터링 조건에 맞는 기록만 검색되어 나타납니다.

## 삭제

**1. 검사 기록을 삭제할 날짜를 선택하고, 상단에 있는 **삭제**를 누릅니다.**

**2. <확인> 창이 나타나서 선택한 날짜의 검사 기록이 모두 지워짐을 알려줍니다.**

**3. 확인**을 누르면, 선택한 날짜에 등록된 검사 기록이 모두 삭제됩니다.

## 인쇄

1. 인쇄할 검사 기록이 있는 날짜를 선택하고, 상단에 있는 **인쇄**를 누릅니다.
2. <인쇄 설정> 창이 나타납니다. 프린터 및 용지 설정을 확인하고 **확인**을 누릅니다.
3. 선택한 날짜에 등록된 모든 검사 기록이 인쇄됩니다.

## 파일로 저장

1. 하나의 파일로 저장할 검사 기록이 있는 날짜를 선택하고, 상단의 **파일로 저장**을 누릅니다.
2. <다른 이름으로 저장> 창이 나타납니다. 검사 기록을 저장할 파일의 경로와 이름, 형식을 입력하고, **저장**을 누릅니다.
  - 파일 이름: 선택한 날짜를 yyyyymmdd와 같은 형식으로 입력하는 것이 좋습니다.  
예) 2004년 11월 6일의 이벤트 기록을 저장한 파일 이름: 20041106log
  - 파일 형식: 확장자가 CSV인 Excel 파일/확장자가 txt인 텍스트 파일 등으로 저장할 수 있습니다.
3. 선택한 날짜에 등록된 모든 검사 기록은 지정한 파일에 저장됩니다.

## 검역소

왼쪽 메뉴에서 **검역소**를 누르면 바이러스에 감염된 원본 파일을 백업해 둔 백업 파일 목록을 확인하고 필요할 경우에 복원하여 사용할 수 있습니다.

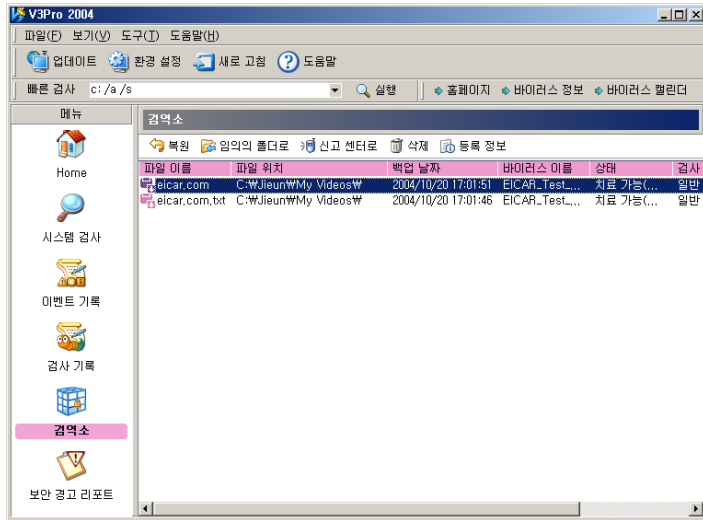


그림 39 검역소

**! 주의** 백업 파일은 바이러스 치료를 시작하기 전에 복사되므로 바이러스에 감염된 상태입니다. 바이러스에 감염된 백업 파일을 복원하면 바이러스가 계속 전파될 수 있으며, 사용자의 시스템에 치명적인 손상을 입힐 수도 있습니다.

### 복원

1. 백업 파일을 복원하기 전에 시스템 감시를 중지합니다. 시스템 감시가 실행 (On) 중이고 시스템 감시의 검사 설정이 자동 치료로 설정되어 있으면, 바이러스에 감염된 백업 파일을 복원하면 바로 다시 검역소로 백업됩니다.
2. 복원할 백업 파일을 선택하고 **복원**을 누릅니다. 마우스 또는 Ctrl 키를 사용하여 여러 개의 파일을 한꺼번에 선택할 수도 있습니다.

3. <백업 파일 복원> 확인 창이 나타납니다.

4. **확인**을 누릅니다. 선택한 백업 파일이 원래 있던 위치로 복원됩니다.

### 임의의 폴더로

중요한 데이터가 저장된 파일이 치료 도중에 손상된 경우에는, 백업 파일을 복원해서 사용할 수 있습니다.

**!** 주의 백업 파일은 바이러스 치료를 시작하기 전에 복사되므로 바이러스에 감염된 상태입니다. 바이러스에 감염된 백업 파일을 복원하면 바이러스가 계속 전파될 수 있으며, 사용자의 시스템에 치명적인 손상을 입힐 수도 있습니다.

1. 백업 파일을 복원하기 전에 시스템 감시를 중지합니다. 시스템 감시가 실행 (On) 중이고 시스템 감시의 검사 설정이 자동 치료로 설정되어 있으면, 바이러스에 감염된 백업 파일을 복원하면 바로 다시 감염소로 백업됩니다.

2. 복원할 백업 파일을 선택하고, **임의의 폴더로**를 누릅니다.

3. <폴더 찾아보기> 창이 열립니다.

4. 백업 파일을 복원할 폴더를 지정하고 **확인**을 누릅니다. 선택한 백업 파일은 사용자가 지정한 임의의 폴더로 복원됩니다.

### 신고 센터로

바이러스 감염 파일의 상태가 **치료 불가** 또는 **신종 바이러스**일 경우에는 치료 중에 데이터가 손상될 수도 있으므로 (주)안철수연구소의 신고 센터로 보내 주시기 바랍니다.

1. 신고 센터로 전송할 백업 파일을 선택합니다. 신고 센터로는 치료 불가 또는 신종 바이러스 상태인 파일만 전송할 수 있습니다. (주)안철수연구소의 신고 센터로는 치료 불가 또는 신종 바이러스 상태인 파일만 전송할 수 있습니다. 치료 가능 상태의 파일을 선택하고 **신고 센터**를 누르면 오류 메시지가 나타납니다.

2. 상단 메뉴에서 **신고 센터**를 누릅니다. <확인> 창이 나타납니다.

3. **확인**을 누르면 <백업 파일 전송> 창이 나타납니다.

4. 보내는 사람의 정보를 자세히 기록하고 **전송(S)**을 누릅니다.

- 이름: 보내는 사람 이름
- 전화: 보내는 사람 전화번호
- E-Mail: 보내는 사람의 E-Mail 주소
- 주소: 보내는 사람의 주소
- 바이러스 증상: 바이러스에 감염된 파일 및 시스템의 증상을 자세히 기록합니다.

5. 검역소에서 선택한 백업 파일은 (주)안철수연구소의 신고 센터로 전송되고 완료 메시지가 나타납니다.

## 삭제

치료 완료 상태인 백업 파일은 다음과 같은 방법으로 삭제할 수 있습니다.

1. 검역소 작업 창에서 치료 완료 상태인 백업 파일을 선택합니다.
2. 상단 메뉴에서 **삭제**를 선택합니다.
3. <확인> 창이 나타납니다.
4. **확인**을 누르면 선택한 백업 파일은 삭제됩니다.

## 등록 정보

검역소에 백업된 파일을 선택하고 상단의 **등록 정보**를 누르거나 더블 클릭하면 <백업 파일 등록 정보> 창이 나타납니다.

다음과 같은 자세한 등록 정보를 확인할 수 있습니다.

- 파일 이름: 백업된 파일 이름
- 파일 위치: 백업된 파일의 원래 위치
- 파일 크기: 백업된 원본 파일의 크기
- 백업 날짜: 백업된 날짜 및 시간
- 만든 날짜: 원본 파일을 만든 날짜
- 바이러스 이름: 감염된 바이러스 이름
- 바이러스 상태: 치료 예정/치료 불가/치료 완료 등
- 속성: 원본 파일의 속성
  - 읽기 전용
  - 숨김
  - 기록
  - 시스템

# 보안 경고 리포트

<보안 경고 리포트> 창에 나타난 링크를 누르면 보안 경고 리포트 메뉴로 바로 이동합니다.

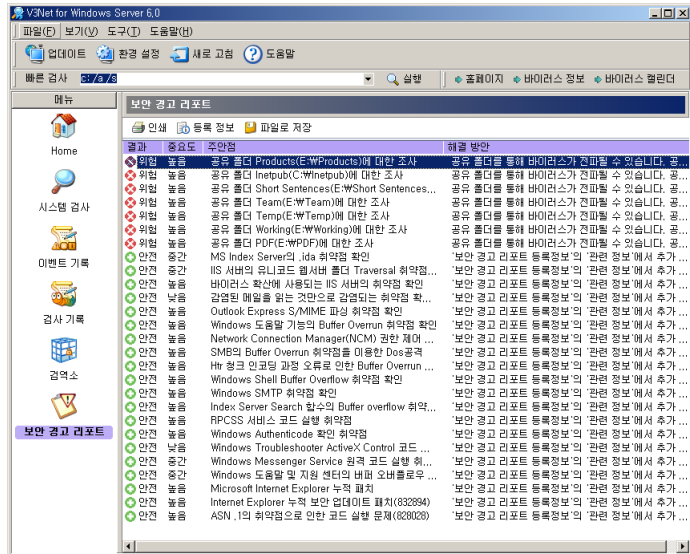


그림 40 보안 경고 리포트

결과 및 중요도를 확인하고 위험한 항목이나 중요도가 높은 항목은 주안점 및 해결 방안을 참고하여 필요한 조치를 취해야 합니다. 보안 경고 리포트에서 권장하는 적절한 조치를 취하지 않으면 바이러스에 감염되어 큰 피해를 입을 수도 있습니다. 보안 경고 리포트 작업 창 상단에는 다음과 같은 메뉴가 있습니다.

## 인쇄

1. 인쇄할 보안 경고 리포트를 선택하고, 상단에 있는 **인쇄**를 누릅니다.
2. <인쇄 설정> 창이 나타납니다. 프린터 및 용지 설정을 확인하고 **확인**을 누릅니다.
3. 선택한 보안 경고 리포트가 인쇄됩니다.

## 등록 정보

선택한 보안 경고 리포트의 등록 정보를 보여줍니다.

1. 자세한 정보를 확인할 보안 경고 리포트를 선택합니다.
2. 상단에 있는 **등록 정보**를 누릅니다.
3. 선택한 보안 경고 리포트에 대한 자세한 등록 정보가 나타납니다.

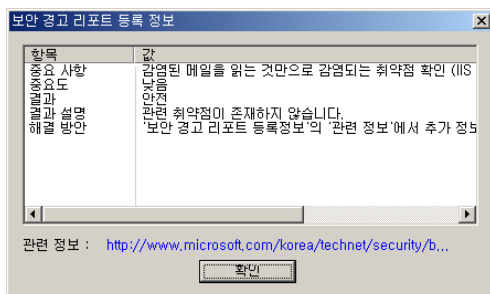


그림 41 보안 경고 리포트 등록 정보

- **중요 사항**: 해당 보안 경고 리포트의 주안점을 자세히 보여줍니다.
- **중요도**: 높음/중간/낮음
- **결과**: 위험/안전
- **결과 설명**: 위험 정보에 대해서 설명합니다.
- **해결 방안**: 위험 상황을 해결하는 방안을 설명합니다.

## 파일로 저장

1. 상단의 **파일로 저장**을 누릅니다.
2. <다른 이름으로 저장> 창이 나타납니다. 저장할 파일의 경로와 이름, 형식을 입력하고 **저장**을 누릅니다.
  - **파일 이름**: 선택한 날짜를 yyyyymmdd와 같은 형식으로 입력하면 좋습니다.  
예) 2004년 11월 6일의 이벤트 기록을 저장한 파일 이름: 20041106log
  - **파일 형식**: 확장자가 CSV인 Excel 파일/확장자가 txt인 텍스트 파일 등으로 저장할 수 있습니다.
3. 지금까지 보고된 모든 보안 경고 리포트가 지정한 파일로 저장됩니다.

## 메뉴

V3Net for Windows Server 6.0을 제품을 실행하면 왼쪽 프레임에는 다음과 같은 기본 메뉴가 나타납니다.



그림 42 화면 구성

## 기본 메뉴

- **Home(52쪽):** 실시간 감시 기능을 실행(ON) 또는 중지(OFF)하거나, 예약 검사 및 엔진 업데이트 예약 일정을 설정할 수 있습니다. 최근에 수행한 엔진 업데이트 날짜 및 검사 날짜도 확인할 수 있습니다.
- **시스템 검사(54쪽):** 사용자가 지정한 영역을 검사하여, 바이러스에 감염된 파일을 찾아냅니다.
- **이벤트 기록(56쪽):** 이 제품에서 수행한 작업 내역을 날짜 별로 확인할 수 있습니다.
- **검사 기록(58쪽):** 바이러스 검사를 수행한 기록 및 검사 결과를 각 날짜 별로 확인할 수 있습니다.
- **검역소(61쪽):** 바이러스 검사로 발견한 감염 파일을 치료하기 이전 상태로 복원할 수 있습니다.
- **보안 경고 리포트(64쪽):** 사용자의 시스템에 바이러스가 침입 및 전파될 수 있는 위험이 있을 경우 나타나는 보안 경고 메시지를 확인할 수 있습니다.

## 상단 메뉴 바

상단에 있는 메뉴 바에 다음과 같이 메뉴가 있습니다. 각 메뉴를 사용하면 다음과 같은 기능을 수행할 수 있습니다.

### 파일(F)

왼쪽 프레임에 있는 기본 메뉴에 따라서 메뉴 구성이 변경됩니다.

- 스마트 업데이트(U): 최신 엔진 다운로드
- 끝내기(X): 프로그램 종료

### 보기(V)

도구 모음, 웹 링크, 빠른 검사 줄을 숨기거나 보이게 설정할 수 있으며, 각 메뉴별 작업 창으로 이동할 수 있습니다.

- 도구 모음(T): 업데이트/환경설정/새로고침/도움말 버튼 보이기/숨기기
- 웹 링크(W): 홈페이지/바이러스 정보/바이러스 캘린더 보이기/숨기기
- 빠른 검사 줄(Q): 빠른 검사 줄 보이기/숨기기
- Home(H): Home 작업 창 열기
- 시스템 검사(M): 시스템 검사 작업 창 열기
- 이벤트 기록(E): 이벤트 기록 작업 창 열기
- 검사 기록(L): 검사 기록 작업 창 열기
- 검역소(R): 검역소 작업 창 열기
- 보안 경고 리포트(S): 보안 경고 리포트 작업 창 열기

### 도구(T)

다음과 같은 주요 기능을 바로 실행 및 중지할 수 있습니다.

- 화면 보호기 검사(S)
- 탐색기 검사(E)
- 실시간 감시(A)
  - 시스템 감시
  - 인터넷 감시
  - 시작 프로그램 감시
- 예약 검사(C)
- 네트워크 차단
  - 포트 차단
- 환경 설정(P)

## 도움말(H)

이 프로그램에 대한 정보와 웹 링크 도움말을 보여줍니다.

- 도움말 항목(H): V3Net for Windows Server 6.0 도움말을 보여줍니다.
- 바이러스 정보(I): ㈜안철수연구소 홈페이지의 바이러스 정보 페이지로 이동합니다.
- 바이러스 캘린더(C): ㈜안철수연구소 홈페이지의 바이러스 캘린더 페이지로 이동합니다. 날짜 별로 활동 가능성이 높은 바이러스 정보를 알려줍니다.
- 홈페이지(W): ㈜안철수연구소의 홈페이지로 이동합니다.
- 온라인 등록(R): ㈜안철수연구소 홈페이지의 고객 지원 > 온라인제품등록 페이지로 이동합니다.
- V3Net for Windows Server 6.0정보(A): 이 제품을 설치한 사용자 정보 및 제품 버전 정보, 저작권 등을 보여줍니다.

## 상단 도구 모음

상단에 있는 도구 모음을 사용하면 주요 기능을 바로 실행할 수 있습니다.

- 업데이트: 최신 엔진 업데이트
- 환경 설정: 바이러스 검사/치료 설정
- 새로 고침: 각 작업 창 새로 고침
- 도움말: 이 제품에 대한 도움말 보기

## 웹 링크

V3Net for Windows Server 6.0을 실행하면 상단에 다음과 같은 웹 링크가 있습니다. 각 버튼을 누르면 해당 웹 페이지로 이동합니다.

**!** 주의 웹 링크를 사용하려면 사용자의 시스템이 인터넷과 연결되어 있어야 합니다.

- 홈페이지: ㈜안철수연구소의 홈페이지로 이동합니다.
- 바이러스 정보: ㈜안철수연구소에서 바이러스를 분석한 결과를 자세히 확인할 수 있습니다.
- 바이러스 캘린더: ㈜안철수연구소에서 각 날짜 마다 활동할 가능성이 높은 것으로 예측한 바이러스에 대한 정보를 확인할 수 있습니다.

## 알림 메시지

V3Net for Windows Server 6.0을 설치하면 오른쪽 하단 작업 표시줄에 다음과 같은 알림 메시지가 나타납니다.

### 보안 경고 메시지

사용자의 시스템에서 보안상 취약점이 발견되면 작업 표시줄에 다음과 같은 보안 경고 리포트 알림 메시지가 나타납니다.

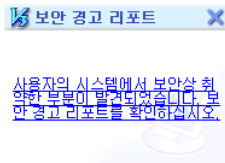


그림 43 보안 경고 리포트 알림 메시지

보안 경고 리포트 알림 메시지를 보지 않으려면 **환경 설정>기타 설정>알림 환경 (111쪽)**에서 **작업 표시줄에 알림 아이콘 표시>보안 경고 메시지 보임**을 선택 해제 하십시오.

### 자체 보호 알림 메시지

V3Net for Windows Server 6.0 제품과 관련된 파일에 특정 프로세스가 접근할 경우에 이를 차단하고 사용자에게 실시간으로 알려줍니다.

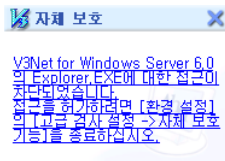


그림 44 자체 보호 알림 메시지

자체 보호 알림 메시지를 보지 않으려면, **환경 설정>고급 검사 설정(97쪽)**에서 **자체 보호>사용자에게 알림 메시지 보이기를** 선택 해제 하십시오.

## 포트 차단 알림 메시지

<환경 설정> 창의 네트워크 차단 > 포트 차단 메뉴에 등록된 포트들이 차단되면 작업 표시줄에 다음과 같은 알림 메시지가 나타납니다.

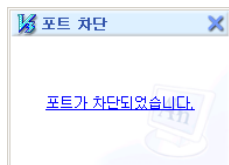


그림 45 포트 차단 알림 메시지

포트 차단 알림 메시지를 보지 않으려면, **환경 설정>네트워크 차단>포트 차단(100 쪽)**에서 **포트 차단 알림 메시지 보이기**를 선택 해제 하십시오.

## 도구 모음

### 탐색기 도구 모음

윈도우즈 탐색기 또는 Microsoft Internet Explorer(5.0 이상)의 메뉴에서 보기(V)  
> 도구 모음(T) > V3를 선택하면 다음과 같은 V3 도구 모음이 나타납니다.

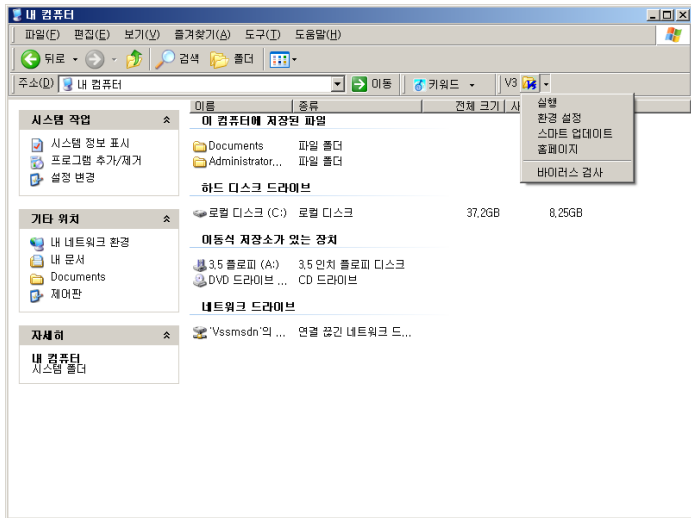


그림 46 탐색기 도구 모음

- 실행: Home 작업 창 열기
- 환경 설정: <환경 설정> 창 열기
- 스마트 업데이트: 최신 엔진 업데이트
- 홈페이지: (주)안철수연구소 홈페이지로 이동
- 바이러스 검사: 해당 폴더에 대한 바이러스 검사 실행

### 알림 도구 모음

작업 표시줄에 있는 알림 아이콘을 마우스 오른쪽 버튼으로 선택하면, 아래와 같은 알림 도구 모음이 나타납니다.

- 열기: Home 작업 창 열기

- 실시간 감시: 각 감시 기능 실행 및 중지
  - 시스템 감시
  - 인터넷 감시
  - 시작 프로그램 감시
- 환경 설정...: <환경 설정> 창 열기
- 네트워크 차단
  - 포트 차단
- 스마트 업데이트...: 최신 엔진 업데이트
- 닫기: 작업 표시줄에 알람 아이콘이 없어집니다. 알람 아이콘을 다시 나타내려면 바탕 화면 또는 프로그램 목록에서 이 프로그램을 다시 실행시키십시오.

## 6장

# 환경 설정

환경 설정 시작 /74

쉬운 설정 /75

시스템 검사/감시 /77

고급 설정 /94

고급 검사 설정 /97

네트워크 차단 /99

경보 메일 /105

보안 설정 /109

기타 설정 /111

바이러스 검사 및 치료하는 방법 등을

사용자가 원하는 대로

직접 설정하는 방법을 설명합니다.

알림 메시지를 보이지 않게 하는 등

다양한 환경 설정 옵션을 선택할 수 있습니다.

## 환경 설정 시작

---

바이러스 검사/감시 기능 별로 검사/치료 환경을 설정하려면 다음과 같은 방법으로 <환경 설정> 창을 실행합니다.

- 상단 메뉴 바에서 도구(T) > 환경 설정(P)을 선택합니다.
- 도구 모음에서 **환경 설정**을 누릅니다.
- 작업 표시줄에서 V3Net for Windows Server 6.0 알림 아이콘을 마우스 오른쪽 버튼으로 선택하고 알림 메뉴에서 **환경 설정...**을 선택합니다.

 **참고** 원격 데스크톱 웹 연결 등을 사용해서 관리자(Administrator) 권한을 가진 여러 명의 사용자가 환경 설정 값을 변경할 경우에는 마지막에 설정한 값이 적용됩니다.

## 쉬운 설정

1. <환경 설정> 창의 왼쪽 메뉴에서 쉬운 설정을 선택합니다.

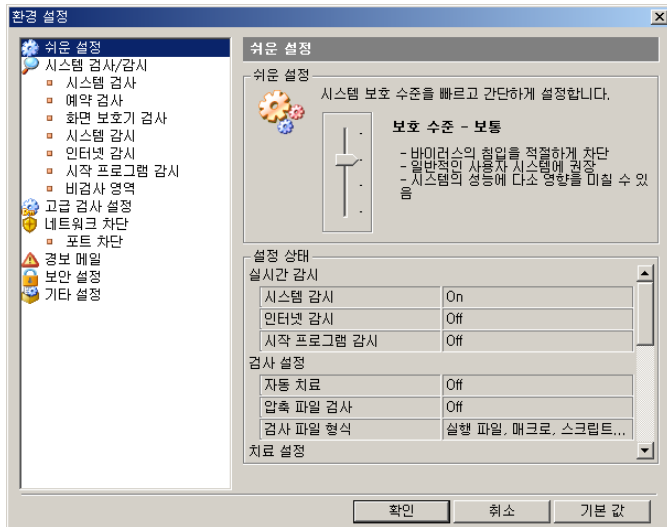
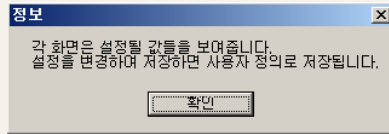


그림 47 쉬운 설정

2. 시스템 보호 수준을 높음, 보통, 낮음 중에서 하나를 선택하여 적용하거나 또는 사용자 정의를 선택하여 직접 일일이 각 기능 별로 검사/치료 설정을 합니다.

- 높음: 바이러스의 침입을 완벽하게 차단 및 치료(바이러스 감염 위험이 높은 시스템에 권장)합니다. 시스템의 사양에 따라서 시스템 보호 수준을 높음으로 할 경우에 성능에 영향을 미칠 수도 있습니다.
- 보통: 바이러스의 침입을 적절하게 조정하여 검사 및 치료(일반 사용자 시스템에 권장)합니다.
- 낮음: 바이러스의 침입을 최저 수준으로 검사 및 치료(바이러스 감염 위험이 낮은 시스템에 권장)합니다.
- 사용자 정의: 사용자가 직접 각 기능 별로 검사/치료 설정을 변경합니다.

- ✓참고 시스템 보호 수준을 **높음**, **보통**, **낮음** 중에서 하나를 선택하고 왼쪽 메뉴를 선택할 경우 아래와 같은 <정보> 창이 나타나고 시스템 보호 수준이 자동으로 **사용자 정의**로 전환됩니다. 왼쪽 메뉴 별로 직접 환경 설정을 할 경우에는 **사용자 정의**를 선택하십시오.



3. **확인**을 누르면 선택한 시스템 보호 수준이 사용자의 시스템에 적용됩니다. 기본 값을 누르면 시스템 보호 수준이 **보통**으로 설정됩니다.

# 시스템 검사/감시

## 시스템 검사/감시

1. <환경 설정> 창의 왼쪽 메뉴에서 시스템 검사/감시 메뉴를 선택합니다.

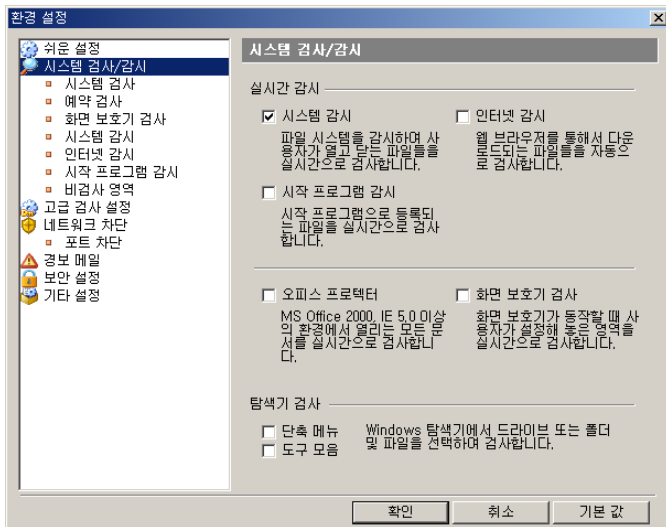


그림 48 시스템 검사/감시 환경 설정

2. 각 검사/감시 기능에 대한 설명을 읽고 실행할 기능만 선택한 다음 확인을 누릅니다. 기본 값을 누르면 처음 설정으로 돌아갑니다.

### 시스템 감시(86쪽)

사용자 시스템의 일반 응용 프로그램에서 접근하는 모든 파일 및 데이터를 실시간으로 검사합니다. 바이러스의 침입을 실시간으로 차단하기 위해서는 시스템 감시 기능을 항상 실행해 두는 것이 좋습니다. 시스템 감시 기능을 중지하면 다음과 같은 <알림> 창이 나타나고 작업 표시줄에 있는 V3Net for Windows Server 6.0 알림 아이콘이 와 같이 회색으로 표시됩니다.

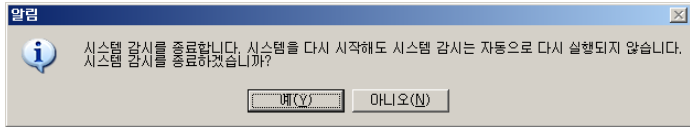


그림 49 시스템 감시 종료 알림

## 인터넷 감시(88쪽)

인터넷 웹 브라우저를 통해서 다운로드되는 모든 데이터 및 파일들을 실시간으로 검사합니다.

## 시작 프로그램 감시(90쪽)

시작 프로그램의 레지스트리, 시작 프로그램 폴더, 시스템 파일에 등록된 시작 프로그램들을 윈도우즈를 시작할 때마다 자동으로 검사합니다.

**! 주의** 시작 프로그램 감시 기능이 동작 중일 때 새로운 사용자 계정이 등록되면 등록된 계정에 대한 시작 프로그램 폴더 및 레지스트리는 시작 프로그램 감시 대상에 바로 포함되지 않습니다. 추가된 사용자 계정에 대한 시작 프로그램 폴더 및 레지스트리도 시작 프로그램 감시 대상에 포함시키려면 시작 프로그램 감시 기능을 중지하고 다시 실행하십시오.

## 오피스 프로텍터

Microsoft Office 2000 또는 Microsoft Internet Explorer 5.0 이상의 오피스 프로그램을 사용해서 OLE (Object Linking & Embedding) 파일 열기 등을 시도하면 해당 파일을 자동으로 검사합니다.

**! 주의** 오피스 프로텍터 관련된 파일이 패치되었을 경우에 시스템을 다시 시작해야 할 수도 있습니다.

## 화면 보호기 검사(84쪽)

화면 보호기가 실행될 때마다 검사 목록에 등록된 영역을 자동으로 검사 및 치료합니다.

## 탐색기 검사(71쪽)

윈도уз 탐색기와 Microsoft Internet Explorer(5.0 이상)에서 단축 메뉴 및 도구 모음을 바로 실행할 수 있도록 합니다.

- 단축 메뉴: V3 바이러스 검사 등을 바로 실행할 수 있는 메뉴입니다.
- 도구 모음: Windows NT Server 4.0(SP6 이상)에서는 V3 도구 모음을 실행할 수 없습니다.

**!** 주의 탐색기 검사와 관련된 파일이 패치 되었을 경우에 시스템을 다시 시작해야 할 수도 있습니다.

## 시스템 검사

시스템 검사, 탐색기 검사, 빠른 검사, 예약 검사에 적용할 검사/치료 옵션을 설정합니다.

1. <환경 설정> 창의 왼쪽 메뉴에서 **시스템 검사/감시** 시스템 검사를 선택합니다.

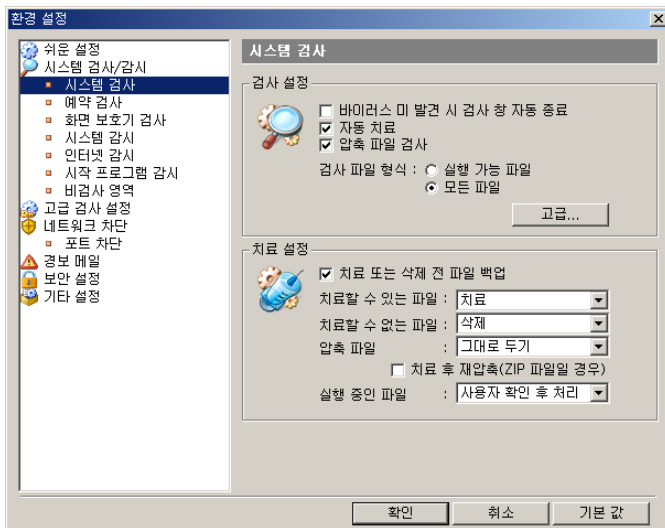


그림 50 시스템 검사 환경 설정

2. 시스템 검사에 적용할 검사/치료 설정을 선택하고 **확인**을 누릅니다. 기본 값을 누르면 처음 설정으로 돌아갑니다.

## 검사 설정

- 바이러스 미 발견 시 검사 창 자동 종료: 발견된 바이러스가 없이 바이러스 검사가 끝나면 검사 창을 자동으로 닫습니다.
- 자동 치료: 바이러스가 발견되면 사용자에게 알리지 않고 자동으로 치료합니다.
- 압축 파일 검사: 압축된 파일도 검사합니다.
- 검사 파일 형식:
  - 실행 가능 파일: 실행 파일, 매크로, 스크립트 등 바이러스가 실행될 수 있는 파일만 검사합니다.
  - 모든 파일: 형식에 상관없이 모든 파일을 검사합니다.
- 고급...(94쪽): 검사 파일 형식, 검사 방법, 압축 파일 검사 등에 대한 옵션을 자세히 설정할 수 있습니다.

## 치료 설정

- 치료 또는 삭제 전 파일 백업: 바이러스에 감염된 파일을 치료 또는 삭제하기 전에 원본 파일을 백업합니다.
- 치료할 수 있는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 치료
  - 삭제: 삭제된 파일은 휴지통이나 검색소에서도 복구할 수 없습니다.
- 치료할 수 없는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 삭제: 삭제된 파일은 휴지통이나 검색소에서도 복구할 수 없습니다. 사용 중인 파일 또는 암호화된 파일일 경우에는 파일은 그대로 존재하지만 파일의 크기가 0 byte로 바뀝니다.
- 압축 파일: 압축 파일 처리 방법
  - 그대로 두기: 중요한 데이터일 경우
  - 삭제
- 치료 후 재압축(ZIP 파일일 경우): ZIP 형식으로 압축된 파일은 압축을 풀어서 치료하고 다시 ZIP 형식으로 압축합니다.
- 실행 중인 파일
  - 사용자 확인 후 처리
  - 그대로 두기: 중요한 데이터일 경우
  - 강제 종료 후 치료
  - 치료 후 시스템 재시작

## 예약 검사

예약 검사 일정을 등록해 두면, 예약된 시간에 맞추어 시스템 검사를 자동으로 수행할 수 있습니다.

1. Home 작업 창에서 **예약 검사>more**를 선택하거나 <환경 설정> 창의 왼쪽 메뉴에서 **예약 검사**를 선택합니다. <예약 검사> 창이 나타납니다.

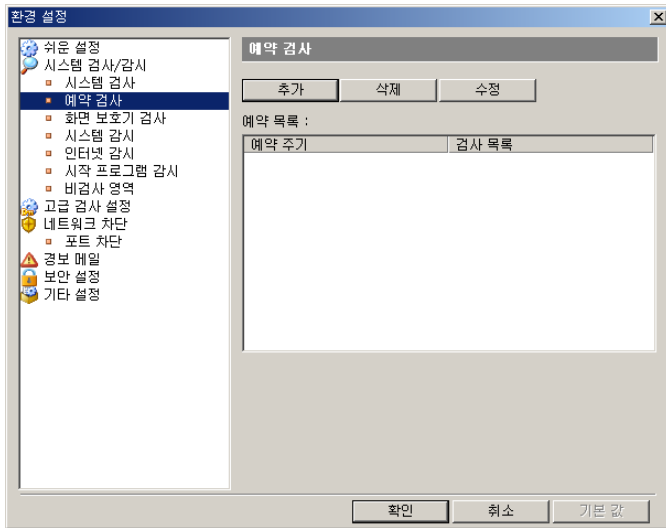


그림 51 예약 검사

2. 왼쪽 상단에 있는 **추가**를 누릅니다. <예약 검사 마법사>가 나타납니다.
3. 예약 검사를 수행할 검사 주기를 설정합니다.

### 주기

- 시스템 시작할 때 마다
- 매일;시간
- 매주;요일;시간
- 매월;날짜;시간
- 한 번;날짜;시간

4. 검사 항목 선택에서 검사할 폴더 및 드라이브를 선택하고 **추가 >>**를 눌러서 검사 항목으로 등록합니다.

5. 사용자의 시스템이 Windows NT 계열이거나 **검사 목록**에 특정 사용자만 접근할 수 있는 네트워크 경로를 등록했으면, **권한 설정**을 눌러서 해당 경로에 접근할 수 있는 사용자 계정 정보를 입력 합니다.
6. **다음** >을 누릅니다. 등록된 예약 검사에 대한 검사/ 치료 옵션을 설정하고 **확인**을 누릅니다. **기본 값**을 누르면 처음 설정으로 돌아갑니다.

### 검사 설정

- 바이러스 미 발견 시 검사 창 자동 종료: 발견된 바이러스가 없이 바이러스 검사가 끝나면 검사 창을 자동으로 닫습니다.
- 백그라운드 검사: 검사 창을 띄우지 않고 바이러스 검사를 수행합니다.
- 자동 치료: 바이러스가 발견되면 사용자에게 알리지 않고 자동으로 치료합니다.
- 압축 파일 검사: 압축된 파일도 검사합니다.
- 검사 파일 형식:
  - 실행 가능 파일: 실행 파일, 매크로, 스크립트 등 바이러스가 실행될 수 있는 파일만 검사합니다.
  - 모든 파일: 형식에 상관없이 모든 파일을 검사합니다.
- **고급...(94쪽)**: 검사 파일 형식, 압축 파일 검사 등에 대한 옵션을 자세히 설정할 수 있습니다.

 **참고** Windows NT 4.0 Workstation Service Pack 6에서는 바이러스 미 발견 시 검사 창 자동 종료, 백그라운드 검사, 자동 치료를 선택 해제 할 수 없습니다.

### 치료 설정

- 치료 또는 삭제 전 파일 백업: 바이러스에 감염된 파일을 치료 또는 삭제하기 전에 원본 파일을 백업합니다.
- 치료할 수 있는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 치료
  - 삭제: 삭제된 파일은 휴지통이나 검색소에서도 복구할 수 없습니다.

- 치료할 수 없는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 삭제: 삭제된 파일은 휴지통이나 검색소에서도 복구할 수 없습니다. 사용 중인 파일 또는 암호화된 파일일 경우에는 파일은 그대로 존재하지만 파일의 크기가 0 byte로 바뀝니다.
- 압축 파일: 압축 파일 처리 방법
  - 그대로 두기: 중요한 데이터일 경우
  - 삭제
- 치료 후 재압축(ZIP 파일일 경우): ZIP 형식으로 압축된 파일은 압축을 풀어서 치료하고 다시 ZIP 형식으로 압축합니다.
- 실행 중인 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 강제 종료 후 치료
  - 치료 후 시스템 재시작

7. 설정을 확인하고 **완료**를 누릅니다. 예약 검사 목록이 나타납니다. 예약 주기 및 검사 목록을 확인하고 수정 또는 삭제할 수 있습니다. 등록된 예약 검사 일정을 수행하지 않으려면 선택을 해제하십시오.

## 화면 보호기 검사

화면 보호기가 실행될 때마다 검사할 영역을 지정하고 검사/치료 옵션을 설정합니다.

1. <환경 설정> 창의 왼쪽 메뉴에서 **화면 보호기 검사**를 선택합니다. <화면 보호기 검사> 창이 나타납니다.

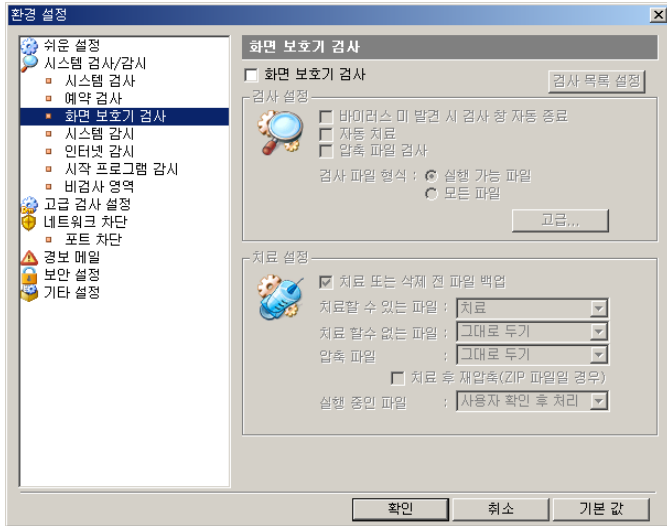


그림 52 화면 보호기 검사

2. **화면 보호기 검사**를 눌러서 화면 보호기 검사를 실행합니다.
3. 오른쪽 상단에 있는 **검사 목록 설정**을 누릅니다. <검사 목록 설정> 창이 나타납니다.
4. **검사 항목 선택**에서 검사할 폴더 및 드라이브를 선택하고, **추가 >>**를 눌러서 검사 목록으로 등록합니다. 검사 항목을 모두 지정했으면 **확인**을 누릅니다. 검사 영역을 지정하지 않으면 로컬 하드 드라이브를 검사합니다.
5. 검사/ 치료 옵션을 선택하고 **확인**을 누릅니다. **기본 값**을 누르면 처음 설정으로 돌아갑니다.

## 검사 설정

- 바이러스 미 발견 시 검사 창 자동 종료: 발견된 바이러스가 없이 바이러스 검사가 끝나면 검사 창을 자동으로 닫습니다.
- 자동 치료: 바이러스가 발견되면 사용자에게 알리지 않고 자동으로 치료합니다.
- 압축 파일 검사: 압축된 파일도 검사합니다.
- 검사 파일 형식:
  - 실행 가능 파일: 실행 파일, 매크로, 스크립트 등 바이러스가 실행될 수 있는 파일만 검사합니다.
  - 모든 파일: 형식에 상관없이 모든 파일을 검사합니다.
- 고급... (94쪽): 검사 파일 형식, 압축 파일 검사 등에 대한 옵션을 자세히 설정할 수 있습니다.

## 치료 설정

- 치료 또는 삭제 전 파일 백업: 바이러스에 감염된 파일을 치료 또는 삭제하기 전에 원본 파일을 백업합니다.
- 치료할 수 있는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 치료
  - 삭제: 삭제된 파일은 휴지통이나 검색소에서도 복구할 수 없습니다.
- 치료할 수 없는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 삭제: 삭제된 파일은 휴지통이나 검색소에서도 복구할 수 없습니다. 사용 중인 파일 또는 암호화된 파일일 경우에는 파일은 그대로 존재하지만 파일의 크기가 0 byte로 바뀝니다.
- 압축 파일: 압축 파일 처리 방법
  - 그대로 두기: 중요한 데이터일 경우
  - 삭제
- 치료 후 재압축(ZIP 파일일 경우): ZIP 형식으로 압축된 파일은 압축을 풀어서 치료하고 다시 ZIP 형식으로 압축합니다.
- 실행 중인 파일
  - 사용자 확인 후 처리
  - 그대로 두기: 중요한 데이터일 경우
  - 강제 종료 후 치료
  - 치료 후 시스템 재시작

## 시스템 감시

시스템 감시에 적용할 검사/치료 옵션을 설정하고 차단할 파일 형식을 지정합니다.

1. Home 작업 창에서 **시스템 감시>more**를 선택하거나, <환경 설정> 창에서 **시스템 검사/감시>시스템 감시**를 선택합니다.

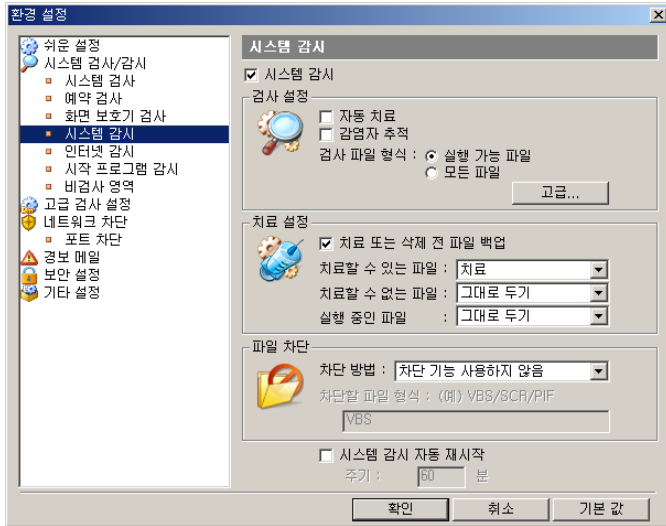


그림 53 시스템 감시

2. 시스템 감시를 눌러서 시스템 감시 기능을 실행합니다.
3. 시스템 감시에 적용할 검사/치료 옵션을 선택하고 **확인**을 누릅니다. **기본 값**을 누르면 처음 설정으로 돌아갑니다.

### 검사 설정

- 자동 치료: 바이러스가 발견되면 사용자에게 알리지 않고 자동으로 치료합니다.
- 감염자 추적: 네트워크 공유 폴더를 통해서 바이러스를 전파시킨 감염자의 시스템 이름과 IP 주소를 추적하여 알려줍니다.

- 검사 파일 형식:
  - 실행 가능 파일: 실행 파일, 매크로, 스크립트 등 바이러스가 실행될 수 있는 파일만 검사합니다.
  - 모든 파일: 형식에 상관없이 모든 파일을 검사합니다.
- 고급...(94쪽): 검사 파일 형식, 검사 방법 등에 대한 옵션을 자세히 설정할 수 있습니다.

## 치료 설정

- 치료 또는 삭제 전 파일 백업: 바이러스에 감염된 파일을 치료 또는 삭제하기 전에 원본 파일을 백업합니다.
- 치료할 수 있는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 치료
  - 삭제: 삭제된 파일은 휴지통이나 검색소에서도 복구할 수 없습니다.
- 치료할 수 없는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 삭제: 삭제된 파일은 휴지통이나 검색소에서도 복구할 수 없습니다. 사용 중인 파일 또는 암호화된 파일일 경우에는 파일은 그대로 존재하지만 파일의 크기가 0 byte로 바뀝니다.
- 실행 중인 파일
  - 그대로 두기
  - 강제 종료 후 치료
  - 치료 후 시스템 재시작

## 파일 차단

- 차단 방법:
  - 차단 기능 사용하지 않음: 특정 형식의 파일을 차단하지 않습니다.
  - V3F로 확장자 바꾸기: 바이러스에 감염된 파일은 바이러스가 활동할 수 없는 V3F 파일 형식으로 변환합니다.
  - 삭제: 삭제할 파일 형식(확장자)을 직접 입력합니다.
  - 차단: 차단할 파일 형식(확장자)을 직접 입력합니다.
- 차단 파일 형식: 차단 및 삭제할 파일 형식(확장자)을 입력합니다. 바이러스에 감염될 위험이 높은 파일의 확장자(CMD, PIF, SCR, VBS, VBE, JS, JSE, WSF, WSH 등)를 입력하십시오. 여러 조건에 맞는 파일을 한꺼번에 차단하려면 /로 구분하여 입력하십시오.

**주의** 차단 파일 형식에 실행 파일 확장자 EXE, DLL, COM, BAT를 입력하고 파일 차단 방법을 삭제로 선택하면 실행 파일들이 모두 삭제됩니다. 또한, 파일 차단 방법에서 **V3F로 확장자 바꾸기**를 선택하면 확장자가 V3F로 모두 변경됩니다.

- 시스템 감시 자동 재시작: 시스템 감시를 중지(Off)하면 사용자가 설정한 주기에 맞추어 자동으로 다시 시스템 감시를 시작합니다.
- 주기: 시스템 감시가 끝나면 자동으로 다시 실행될 시간을 설정합니다. 최소 10분에서 최대 10000분까지 값을 입력할 수 있습니다.

## 인터넷 감시

인터넷 감시에 적용할 검사/치료 옵션을 설정합니다.

1. Home 작업 창에서 **인터넷 감시>more**를 선택하거나, <환경 설정> 창에서 **시스템 검사/감시>인터넷 감시**를 선택합니다.

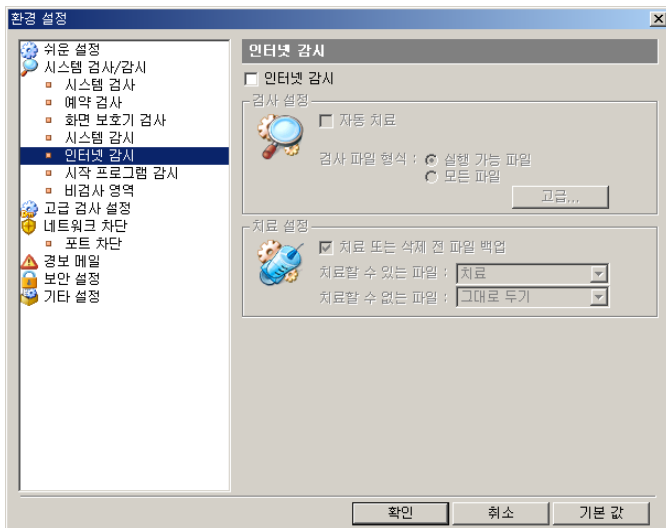


그림 54 인터넷 감시

2. 인터넷 감시를 눌러서 인터넷 감시 기능을 실행합니다.
3. 검사/치료 옵션을 선택하고 **확인**을 누릅니다. **기본 값**을 누르면 처음 설정으로 돌아옵니다.

## 검사 설정

- 자동 치료: 바이러스가 발견되면 사용자에게 알리지 않고 자동으로 치료합니다.
- 검사 파일 형식:
  - 실행 가능 파일: 실행 파일, 매크로, 스크립트 등 바이러스가 실행될 수 있는 파일만 검사합니다.
  - 모든 파일: 형식에 상관없이 모든 파일을 검사합니다.
- 고급...(94쪽): 검사 파일 형식에 대한 옵션을 자세히 설정할 수 있습니다.

## 치료 설정

- 치료 또는 삭제 전 파일 백업: 바이러스에 감염된 파일을 치료 또는 삭제하기 전에 원본 파일을 백업합니다.
- 치료할 수 있는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 치료
  - 삭제: 삭제된 파일은 휴지통이나 검역소에서도 복구할 수 없습니다.
- 치료할 수 없는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 삭제: 삭제된 파일은 휴지통이나 검역소에서도 복구할 수 없습니다. 사용 중인 파일 또는 암호화된 파일일 경우에는 파일은 그대로 존재하지만 파일의 크기가 0 byte로 바뀝니다.

## 시작 프로그램 감시

시작 프로그램 감시에 적용할 검사/치료 옵션을 설정합니다.

1. Home 작업 창에서 **시작 프로그램 감시>more**를 선택하거나 <환경 설정> 창에서 **시작 프로그램 감시**를 선택합니다.

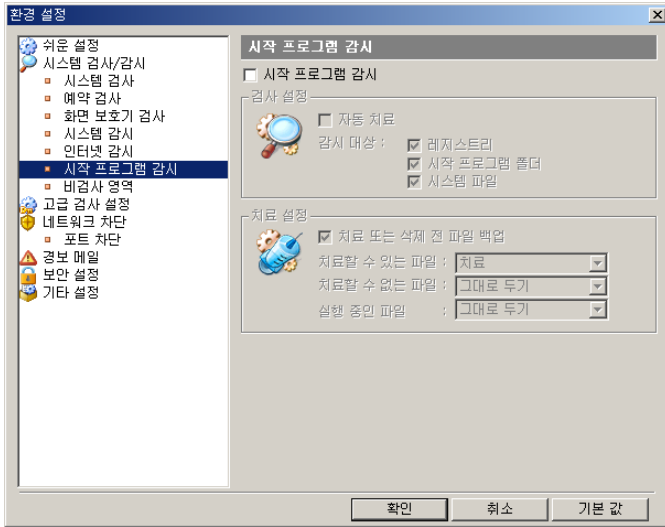


그림 55 시작 프로그램 감시

2. **시작 프로그램 감시**를 눌러서 시작 프로그램 감시 기능을 실행합니다.
3. 시작 프로그램 감시에 적용할 검사/치료 옵션을 선택하고 **확인**을 누릅니다. **기본 값**을 누르면 처음 설정으로 돌아갑니다.

### 검사 설정

- 자동 치료: 바이러스가 발견되면 사용자에게 알리지 않고 자동으로 치료합니다.
- 감시 대상
  - 레지스트리: 시작 프로그램 레지스트리에 등록된 파일들을 검사합니다.
  - 시작 프로그램 폴더: 시작 프로그램 폴더에 있는 파일들을 검사합니다.
  - 시스템 파일: 시스템 파일에 등록된 파일들을 검사합니다.
- 고급...(94쪽): 검사 파일 형식, 검사 방법 등에 대한 옵션을 설정할 수 있습니다.

## 치료 설정

- 치료 또는 삭제 전 파일 백업: 바이러스에 감염된 파일을 치료 또는 삭제하기 전에 원본 파일을 백업합니다.
- 치료할 수 있는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 치료
  - 삭제: 삭제된 파일은 휴지통이나 검색소에서도 복구할 수 없습니다.
- 치료할 수 없는 파일
  - 그대로 두기: 중요한 데이터일 경우
  - 삭제: 삭제된 파일은 휴지통이나 검색소에서도 복구할 수 없습니다. 사용 중인 파일 또는 암호화된 파일일 경우에는 파일은 그대로 존재하지만 파일의 크기가 0 byte로 바뀝니다.
- 실행 중인 파일
  - 그대로 두기
  - 강제 종료 후 치료
  - 치료 후 시스템 재시작

## 비검사 영역

검사 및 감시를 하지 않아도 바이러스 감염 위험이 없는 안전한 영역은 비검사 영역으로 지정할 수 있습니다.

**! 주의** 비검사 영역으로 설정된 영역은 어떤 검사/감시 기능에서도 제외됩니다. 바이러스에 감염될 위험이 조금이라도 있는 영역을 비검사 영역으로 설정하면 바이러스가 확산되어 피해를 입을 수 있습니다.

1. <환경 설정> 창의 왼쪽 메뉴에서 **비검사 영역**을 선택합니다.

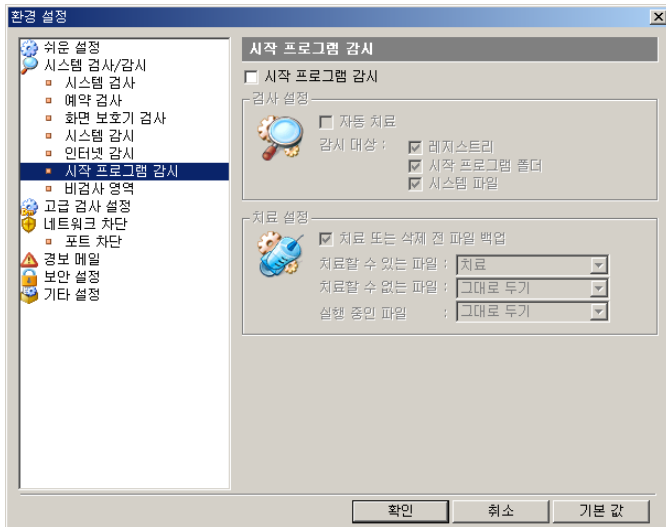


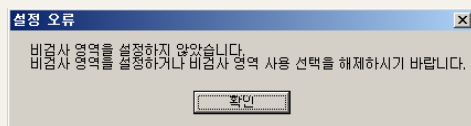
그림 56 비검사 영역

2. **비검사 영역 사용**을 선택합니다. 오른쪽에 있는 버튼들이 활성화됩니다.

3. 다음 버튼들을 사용해서 바이러스 감염 위험이 없는 안전한 영역을 비검사 영역으로 등록합니다.

- 폴더 추가: 비검사 영역으로 폴더 등록
- 파일 추가: 비검사 영역으로 파일 등록
- 확장자 추가: 비검사 영역으로 등록할 파일의 확장자 입력
- 삭제: 선택한 폴더 및 파일 비검사 영역에서 제외

✓참고 **비검사 영역 사용**을 선택했으나, 비검사 영역을 등록하지 않으면 다음과 같은 오류 창이 나타납니다.



## 고급 설정

<환경 설정> 창의 검사/감시 메뉴의 [검사 설정] 탭에 있는 **고급...**을 누르면, <고급 검사 설정> 창이 나타나고 다음과 같이 자세한 검사 방법을 설정할 수 있습니다. **기본 값**을 누르면 처음 설정으로 돌아갑니다.

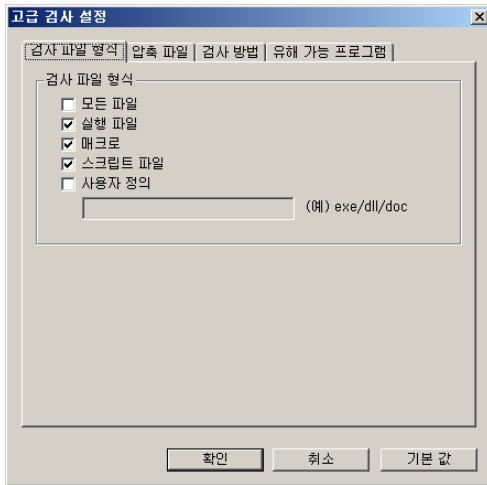


그림 57 고급 검사 설정

### 검사 파일 형식

| 항목      | 설명                                                           |
|---------|--------------------------------------------------------------|
| 모든 파일   | 형식에 상관없이 모든 파일을 검사합니다.                                       |
| 실행 파일   | 실행 파일을 검사합니다.                                                |
| 매크로     | 매크로 파일을 검사합니다.                                               |
| 스크립트 파일 | 스크립트 파일을 검사합니다.                                              |
| 사용자 정의  | 특정 확장자 파일을 지정해서 검사할 수 있습니다. 확장자를 여러 개 입력하려면, /로 구분해서 입력하십시오. |

## 압축 파일

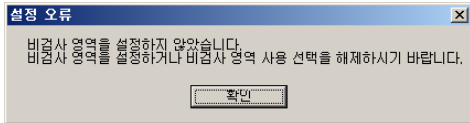
| 항목         | 설명                                                                  |
|------------|---------------------------------------------------------------------|
| 압축 파일 검사   | 압축 파일 검사를 실행합니다.                                                    |
| 다중 압축 파일   | 지정한 압축 횟수 이상 압축된 다중 압축 파일도 압축을 해제하고 검사합니다.                          |
| 실행 압축 파일   | PKLITE, LZEXE, DIET과 같은 프로그램을 통해서 만들어진 실행 압축 파일을 검사합니다.             |
| 처음 한 번만 검사 | 변경되거나 새로 만들어진 모든 파일은 맨 처음에 한 번만 검사합니다. 한 번 검사한 압축 파일은 다시 검사하지 않습니다. |
| 모든 압축 형식   | 모든 형식의 압축 파일을 검사합니다.                                                |
| 압축 형식 지정   | 지정한 형식(ace, arj, lzh, rar, zip와 같은 형식)의 압축 파일만 검사합니다.               |

## 검사 방법

시스템 검사(79쪽)에서 **고급...**을 누르면 다음과 같은 탭 메뉴가 나타납니다.

| 항목         | 설명                                                                                                                                                               |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 공유 해제 후 검사 | 사용자 시스템에서 다른 사용자와 공유된 폴더가 있으면 공유를 모두 해제하고 검사합니다. 공유 해제된 폴더는 검사가 끝나도 다시 공유되지 않습니다.                                                                                |
| 셸 종료 후 검사  | 현재 사용 중인 셸 프로세스(예: Explorer.exe 프로세스)를 끝내고 시스템 검사를 시작합니다. 이 항목을 선택하면 액티브 데스크 탐과 작업 표시줄에 있는 알람 아이콘 및 Explorer.exe 프로세스와 관련된 작업이 모두 끝나게 되며 검사가 끝나도 복구되지 않을 수 있습니다. |

시스템 감시(86쪽)에서 **고급...**을 누르면 다음과 같은 탭 메뉴가 나타납니다.

| 항목         | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 플로피 디스크 검사 | <ul style="list-style-type: none"> <li>• 플로피 디스크 부트 영역 검사</li> <li>• 윈도우즈 종료 시 플로피 디스크 검사</li> </ul>                                                                                                                                                                                                                                                                                                                                                         |
| 검사 범위      | <ul style="list-style-type: none"> <li>• 로컬 드라이브 읽기 검사</li> <li>• 로컬 드라이브 쓰기 검사: 감염자 추적 기능을 사용하기 위해서는 반드시 이 항목을 선택해야 합니다.</li> <li>• 네트워크 드라이브 읽기 검사</li> <li>• 네트워크 드라이브 쓰기 검사</li> </ul> <p>로컬 드라이브 읽기 검사 또는 로컬 드라이브 쓰기 검사 중에 하나는 선택해야 합니다. 둘 다 선택하지 않으면 아래와 같은 오류 창이 나타납니다.</p>  <p>설정 오류<br/>비검사 영역을 설정하지 않았습니다.<br/>비검사 영역을 설정하거나 비검사 영역 사용 선택을 해제하시기 바랍니다.<br/>확인</p> |
| 경고 메시지     | 바이러스 발견 시 경고 메시지 보이기(NT 계열에서만)                                                                                                                                                                                                                                                                                                                                                                                                                               |

## 유해 가능 프로그램

| 항목            | 설명                                                                                       |
|---------------|------------------------------------------------------------------------------------------|
| 유해 가능 프로그램 검사 | 정상적인 목적으로 만들었지만 악의적인 용도로 사용될 수 있는 유해 가능 프로그램을 검사하는 기능을 실행합니다.                            |
| 예외 프로그램       | 유해 가능 프로그램으로 진단하였지만 프로그램의 위험성을 알고 정상적인 목적으로 사용해야 하는 프로그램이 있다면 예외 프로그램으로 등록하여 사용할 수 있습니다. |

- ☑ **참고** 유해 가능 프로그램을 예외 프로그램으로 등록하는 방법은 두 가지가 있습니다.
- 시스템 감시를 실행하여 발견한 유해 가능 프로그램을 선택하고 마우스 오른쪽 버튼을 누른 다음 **예외 프로그램으로 등록**을 선택합니다.
  - 검사 기록 작업 창의 바이러스 검사 기록 중에서 유해 가능 프로그램을 검사한 기록을 선택하고 마우스 오른쪽 버튼을 누른 다음 **예외 프로그램으로 등록**을 선택합니다.

# 고급 검사 설정

1. <환경 설정> 창에서 고급 검사 설정을 선택합니다.

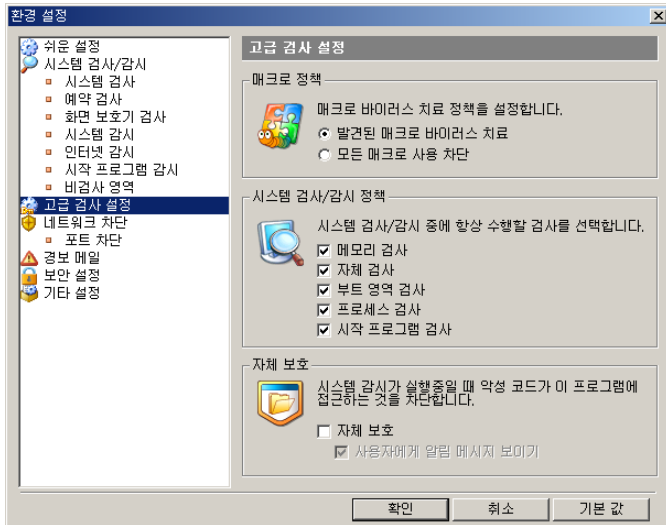


그림 58 고급 검사 설정

2. 각 항목 별로 실행할 기능만 선택하고 **확인**을 누릅니다. **기본값**을 누르면 처음 설정으로 돌아갑니다.

## 매크로 정책

오피스 프로텍터와 시스템 검사에 적용 될 매크로 차단 정책을 설정합니다. Microsoft Office 2000 또는 Microsoft Internet Explorer(5.0 이상)에서 OLE (Object Linking & Embedding) 파일 열기 등을 수행하면, 해당 파일을 자동으로 검사합니다.

- 발견된 매크로 바이러스 치료: 오피스 프로텍터 또는 시스템 검사 중에 발견된 매크로 바이러스를 치료합니다.
- 모든 매크로 사용 차단: 오피스 프로텍터 검사 또는 시스템 검사 중에 발견된 모든 매크로의 사용을 차단합니다.

## 시스템 검사/감시 정책

시스템 검사 또는 시스템 감시를 수행 할 때마다 항상 검사할 영역을 선택합니다.

- 메모리 검사: 메모리에 존재하는 감염 파일과 악성 프로그램들을 검사합니다. 발견된 감염 파일 및 악성 프로그램들은 시스템 검사/시스템 감시 환경 설정 값과는 상관없이 항상 자동으로 치료 및 차단됩니다.
- 자체 검사: V3Net for Windows Server 6.0를 실행하기 전에, V3Net for Windows Server 6.0 관련 파일이 바이러스에 감염되었는지 검사합니다.
- 부트 영역 검사: 부트 영역을 검사합니다.
- 프로세스 검사: 현재 실행 중인 프로그램의 프로세스를 검사합니다.
- 시작 프로그램 검사: 시작 프로그램으로 등록되어 있는 프로그램들의 파일을 검사합니다.

**! 주의** 시스템 검사/감시 정책은 탐색기 검사 또는 오피스 프로텍터에는 적용되지 않습니다.

## 자체 보호

시스템 감시 중에 이 프로그램의 실행 파일(예: Monsys32.exe)이나 스마트 업데이트의 실행 파일에 접근하는 프로세스를 실시간으로 감시하여 악성 프로그램을 사전에 차단합니다.

**! 주의** 자체 보호 기능은 시스템 감시를 실행해야만 동작합니다.

- 자체 보호: 이 항목을 선택하면 자체 보호가 실행됩니다.
  - 사용자에게 알림 메시지 보이기: 이 프로그램의 실행 파일들에 대한 접근이 발견될 경우 다음과 같은 자체 보호 알림 메시지를 사용자에게 보여줍니다.

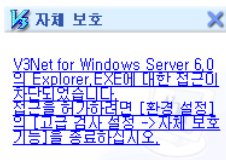


그림 59 자체 보호 알림 메시지

# 네트워크 차단

1. <환경 설정> 창의 왼쪽 메뉴에서 네트워크 차단을 선택합니다.

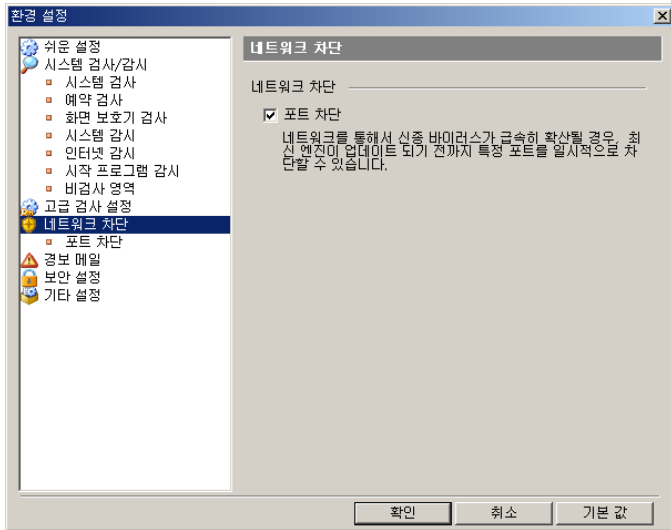


그림 60 네트워크 차단

2. 신종 바이러스가 급속히 확산되는 등의 위험이 있을 경우에는 왼쪽 상단에 있는 **포트 차단**을 눌러서 적용합니다.
3. 선택을 완료하면 **확인**을 누릅니다. **기본 값**을 누르면 처음 설정으로 돌아갑니다.

## 포트 차단

차단할 포트만 등록하고 나머지는 모두 허용하거나 허용할 포트만 등록하고 나머지는 모두 차단할 수 있습니다. 긴급 바이러스가 확산될 경우에는 일시적으로 모든 네트워크를 차단할 수도 있습니다.

1. <환경 설정> 창의 왼쪽 메뉴에서 **네트워크 차단** > **포트 차단**을 선택합니다.

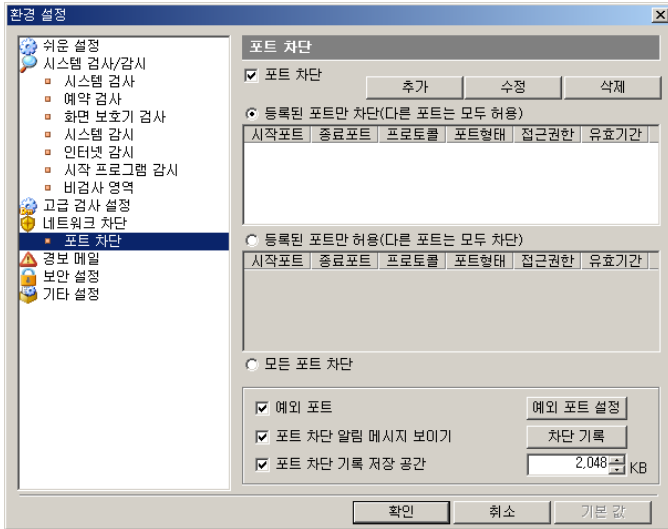


그림 61 포트 차단

2. 왼쪽 상단의 **포트 차단**을 눌러서 포트 차단 기능을 실행합니다. 이 체크 박스를 선택하지 않으면 포트 차단 설정을 등록해도 적용되지 않습니다.

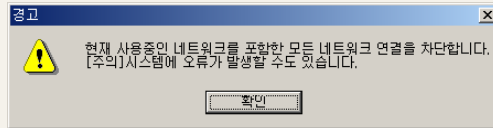
### 포트 허용/차단 설정

3. 아래 세 가지 항목 중에 하나만 선택하여 적용합니다.

- 등록된 포트만 차단(다른 포트는 모두 허용): 상단에 있는 **추가**를 눌러서 등록한 포트만 차단됩니다. 나머지 포트는 모두 허용됩니다.
- 등록된 포트만 허용(다른 포트는 모두 차단): 상단에 있는 **추가**를 눌러서 등록한 포트만 허용됩니다. 나머지 포트는 모두 차단됩니다.

- 모든 포트 차단: 현재 사용 중인 포트를 포함하여 연결된 모든 포트를 차단합니다. 시스템에 오류가 발생할 수 있으므로 네트워크 트래픽이 급증하거나 신종 바이러스가 급속히 확산될 경우에만 선택합니다.

**! 주의** 모든 포트 차단을 선택하면 아래와 같은 경고 창이 나타납니다. 현재 사용 중인 네트워크를 포함한 모든 네트워크 연결을 차단합니다. 현재 사용 중인 포트가 차단되면 시스템에 오류가 발생할 수도 있습니다.



## 포트 추가

1. 오른쪽 상단에 있는 **추가**를 누르면 <포트 정보 입력> 창이 나타납니다.

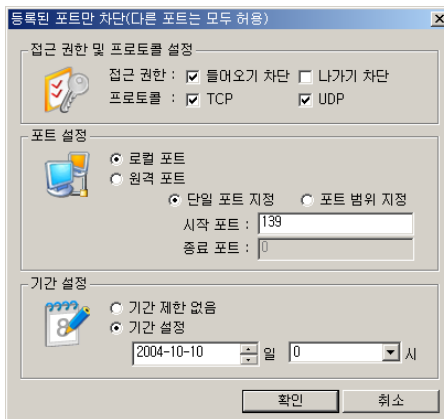


그림 62 포트 정보 입력

2. 차단 또는 허용할 포트 정보를 입력하고 **확인**을 누릅니다.

### 접근 권한 및 프로토콜 설정

둘 중에 하나는 반드시 선택해야 합니다. 둘 다 선택할 수도 있습니다.

- 접근 권한
  - 들어오기
  - 나가기
- 프로토콜
  - TCP
  - UDP

 **참고** TCP, UDP 프로토콜만 선택할 수 있습니다. TCP, UDP 프로토콜을 제외한 다른 프로토콜을 사용해서 통신하는 공유 폴더는 차단 또는 허용되지 않을 수 있습니다.

### 포트 설정

둘 중에 하나만 선택해야 합니다.

- 원격 포트
- 로컬 포트
- 단일 포트 지정
- 포트 범위 지정
  - 시작 포트
  - 종료 포트

### 기간 설정

- 기간 제한 없음: 등록된 포트를 계속 차단 또는 허용합니다.
- 기간 설정: 등록된 포트를 일시적으로 차단 또는 허용하려면 차단 기간을 설정할 수 있습니다.
  - 날짜/시간: 현재 등록하는 포트를 현재 시각부터 차단 또는 허용할 기간을 지정합니다.

3. **확인**을 눌러서 포트 차단 설정을 등록합니다.

4. 등록된 포트 정보를 수정하려면 더블 클릭하거나 상단에 있는 **수정**을 누르십시오. 상단에 있는 **삭제**를 누르면 등록된 포트 정보를 삭제할 수 있습니다. 여러 개의 포트를 한꺼번에 선택하려면 **Ctrl** 또는 **Shift** 키를 사용할 수 있습니다.

## 포트 차단 기록

오른쪽 하단에 있는 **차단 기록**을 누르면 아래와 같은 텍스트 파일이 나타납니다.  
등록된 포트들이 차단된 기록을 시간 순서대로 확인할 수 있습니다.

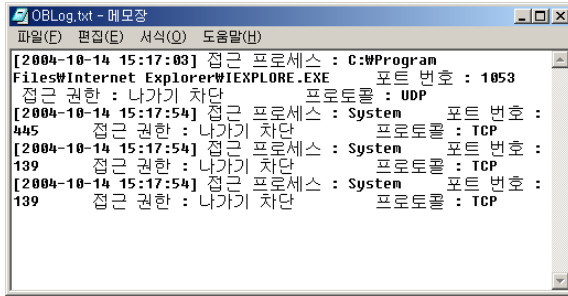


그림 63 포트 차단 기록

### 포트 차단 기록 저장 공간

포트 차단 기록을 저장할 텍스트 파일의 크기를 지정합니다. 최대 2048KB로 설정할 수 있습니다. 포트 차단 기록 파일이 지정한 용량보다 커지면 포트 차단 기록은 처음부터 시간 순서대로 삭제됩니다.

## 포트 차단 알림 메시지

**포트 차단 알림 메시지** 보이기를 선택하면 등록된 포트들이 차단될 때마다 작업 표시줄에 아래와 같은 이벤트 메시지가 나타납니다. 포트 차단 메시지를 확인하지 않으려면 이 항목을 선택 해제 하십시오.

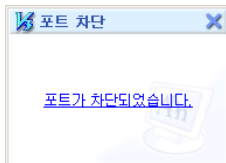


그림 64 포트 차단 알림 메시지

☒ 참고 기타 설정(111쪽)에서 **작업 표시줄에 알림 아이콘 표시**를 선택 해제하면, **포트 차단 알림 메시지** 보이기를 선택할 수 없습니다.

## 예외 포트

예외 포트 설정을 누르면 <예외 포트 설정> 창이 나타나고, 다음과 같은 예외 포트 목록을 확인할 수 있습니다. 예외 포트는 V3Net for Windows Server 6.0이 정상적으로 동작하기 위해서 항상 허용되어야 하는 포트들로서, 예외 포트를 선택하지 않으면 적용되지 않습니다.

| 예외 포트   | 프로토콜    | 포트형태     | 접근권한    | 설명                                                                                                                         |
|---------|---------|----------|---------|----------------------------------------------------------------------------------------------------------------------------|
| 80 ~ 83 | TCP     | 원격 포트    | 나가기 허용  | Windows Update와 스마트 업데이트를 통해서 최신 엔진을 업데이트 받기 위해서 항상 허용되어야 하는 예외 포트입니다.                                                     |
| 443     | TCP     | 원격 포트    | 나가기 허용  |                                                                                                                            |
| 1080    | TCP     | 원격 포트    | 나가기 허용  |                                                                                                                            |
| 8080    | TCP     | 원격 포트    | 나가기 허용  |                                                                                                                            |
| 8088    | TCP     | 원격 포트    | 나가기 허용  |                                                                                                                            |
| 11523   | TCP     | 원격 포트    | 나가기 허용  | Windows Update를 수시로 받기 위해서 항상 허용되어야 하는 예외 포트입니다.                                                                           |
| 2869    | UDP     | 원격 포트    | 나가기 허용  |                                                                                                                            |
| 25      | TCP     | 원격 포트    | 나가기 허용  | 지정된 관리자 계정으로 경보 메일을 보내기 위해서 항상 허용되어야 하는 예외 포트입니다.                                                                          |
| 2186    | TCP     | 원격 포트    | 나가기 허용  | (주)안철수연구소의 중앙 관리 방역 솔루션 AhnLab Policy Center의 통제를 받기 위해서 항상 허용되어야 하는 예외 포트입니다.                                             |
| 5465    | TCP     | 원격 포트    | 나가기 허용  |                                                                                                                            |
| 6063    | TCP     | 원격/로컬 포트 | 들어오기 허용 |                                                                                                                            |
| 8951    | TCP     | 원격 포트    | 나가기 허용  | (주)안철수연구소의 중앙 관리 방역 솔루션 AhnLab Policy Center의 통제를 받는 시스템에서는 이 포트를 항상 적용해야 합니다.                                             |
| 2191    | UDP     | 원격 포트    | 나가기 허용  | DNS 서버로부터 도메인 또는 호스트 이름을 IP 주소로 변환한 값을 받기 위해서 필요한 포트입니다.<br>도메인이나 호스트 이름으로 웹 사이트에 접속하거나 메일을 보내고 받기 위해서는 이 포트를 항상 허용해야 합니다. |
| 53      | TCP/UDP | 원격 포트    | 들어오기 허용 |                                                                                                                            |

## 경보 메일

1. <환경 설정> 창의 왼쪽 메뉴에서 **경보 메일**을 선택합니다.

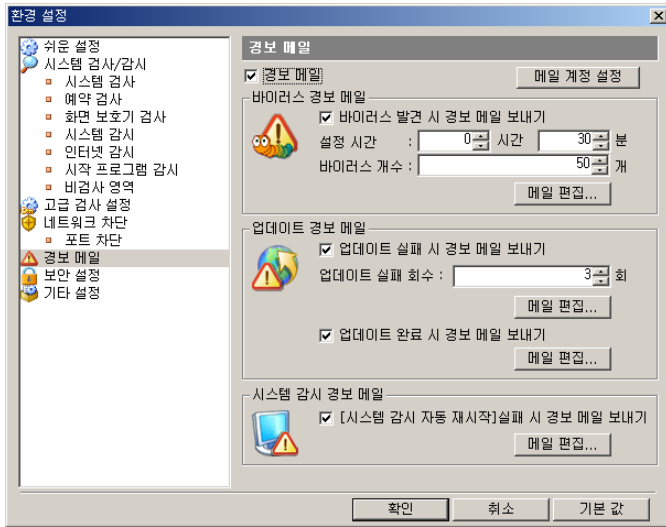


그림 65 경보 메일

2. 왼쪽 상단에 있는 **경보 메일**을 선택하면 모든 항목이 활성화됩니다.
3. 오른쪽 상단에 있는 **메일 계정 설정**을 누릅니다. <메일 계정 설정> 창이 나타납니다.

## 메일 계정 설정

경보 메일을 받아볼 관리자의 메일 계정 정보를 입력합니다. 메일 정보를 모두 입력했으면 **설정 테스트**를 눌러서 경보 메일이 제대로 전송되는지 확인하고 **확인**을 눌러서 닫습니다.

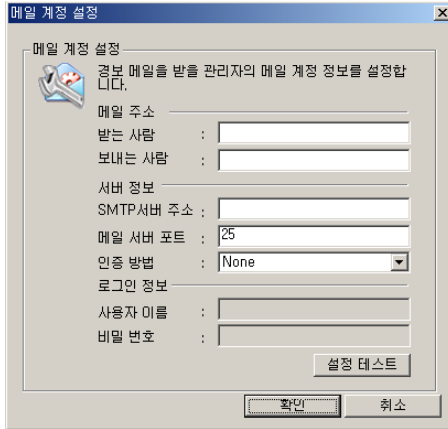


그림 66 메일 계정 설정

### 메일 정보

- 받는 사람: 경보 메일을 받아 볼 관리자 계정 정보
- 보내는 사람: 경보 메일을 보내는 사람의 메일 정보

### 서버 정보

- SMTP 서버 주소: 경보 메일을 보낼 때 사용할 SMTP 메일 서버 주소
- 메일 서버 포트: 경보 메일을 보낼 때 사용할 메일 서버의 포트 번호(기본 값 25번)
- 인증 방법: 경보 메일을 보낼 때 사용할 메일 서버의 인증 방법
  - NONE
  - AUTH LOGIN: 로그인 정보가 활성화됩니다. – 사용자 이름/비밀 번호
  - LOGIN PLAIN: 로그인 정보가 활성화됩니다. – 사용자 이름/비밀 번호

## 바이러스 경고 메일

4. 경고 메일을 받아볼 상황을 선택하고, 각 경우마다 필요한 값을 입력합니다.

- 바이러스 발견 시 경고 메일 보내기: 설정한 기간 동안 지정한 숫자 이상의 바이러스가 발견되면 등록된 관리자 계정으로 경고 메일을 보냅니다. 오른쪽
- 설정 시간: 바이러스 경고 메일 전송 시간 간격을 지정할 수 있습니다. (기본 값 30분)
  - 시간: 10분~336시간(2주)까지 설정할 수 있습니다.
  - 분: 10분~60분까지 설정할 수 있습니다.
- 바이러스 개수: 1~10000 사이의 값을 입력할 수 있습니다. (기본 값 50개)

## 업데이트 경고 메일

- 업데이트 실패 시 경고 메일 보내기: 엔진 업데이트를 완료하지 못하였을 경우에 관리자 계정으로 경고 메일을 보냅니다.
  - 업데이트 실패 회수: 기본 값 3회
- 업데이트 완료 시 경고 메일 보내기: 엔진 업데이트를 성공적으로 완료하였을 경우에 관리자 계정으로 경고 메일을 보냅니다.

## 시스템 감시 경고 메일

- [시스템 감시 자동 재시작] 실패 시 경고 메일 보내기: 시스템 감시 자동 재시작이 실패할 때마다 등록된 관리자 계정으로 경고 메일을 보냅니다.

5. 각 항목마다 **메일 편집...**을 누르면, 아래와 같은 <메일 편집> 창이 나타납니다.

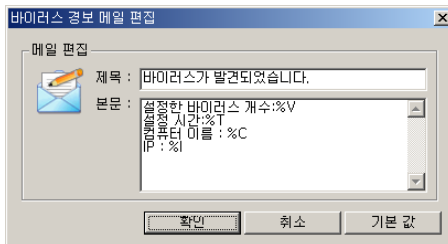


그림 67 바이러스 경고 메일 편집

6. 관리자가 받아볼 경보 메일의 제목 및 내용을 직접 입력하고, **확인**을 누르십시오.

- 제목

- 바이러스 경보 메일: 바이러스가 발견되었습니다.
- 업데이트 실패 경보 메일: 업데이트가 실패했습니다.
- 업데이트 완료 경보 메일: 업데이트가 성공적으로 완료되었습니다.
- 시스템 감시 경보 메일: 시스템 감시 자동 재시작이 실패했습니다.

- 본문

- 설정된 바이러스 개수: %V
- 설정 시간: %T
- 컴퓨터 이름: %C
- IP 주소: %I

## 보안 설정

1. <환경 설정> 창에서 **보안 설정**을 선택합니다. 다음과 같은 메뉴 중에서 필요한 기능만 선택합니다.

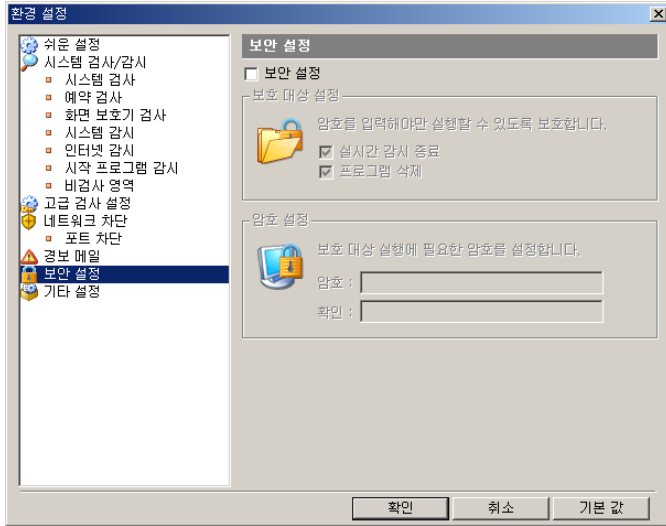


그림 68 보안 설정

2. 왼쪽 상단에 있는 **보안 기능 사용**을 선택합니다. 다음과 같은 작업은 암호를 알고 있는 사용자만 수행할 수 있도록 보호할 수 있습니다. 보호 대상으로 설정된 작업은 **쉬운 설정(75쪽)**에서 선택한 시스템 보호 수준(높음, 보통, 낮음)과 상관없이 계속 보호됩니다.

### 보호 대상 설정

- 실시간 감시 종료: 실시간 감시 기능을 중지(Off)하려면 설정된 암호를 입력해야 합니다.
- 프로그램 삭제: 이 프로그램을 삭제하려면 설정된 암호를 입력해야 합니다.

## 암호 설정

보호 대상으로 설정된 작업을 수행할 수 있는 필요한 암호를 입력합니다. 입력된 암호를 알지 못하는 사용자는 보호 대상으로 설정된 작업을 실행할 수 없습니다. 보안 기능 사용을 선택하고, 암호를 설정하지 않으면 오류 메시지가 나타납니다.

 **주의** 설정한 암호를 기억할 수 없을 경우에는 ㈜안철수연구소의 고객센터센터로 문의하십시오.

## 기타 설정

<환경 설정> 창에서 **기타 설정**을 선택합니다. 다음과 같은 메뉴 중에서 필요한 기능만 선택합니다.

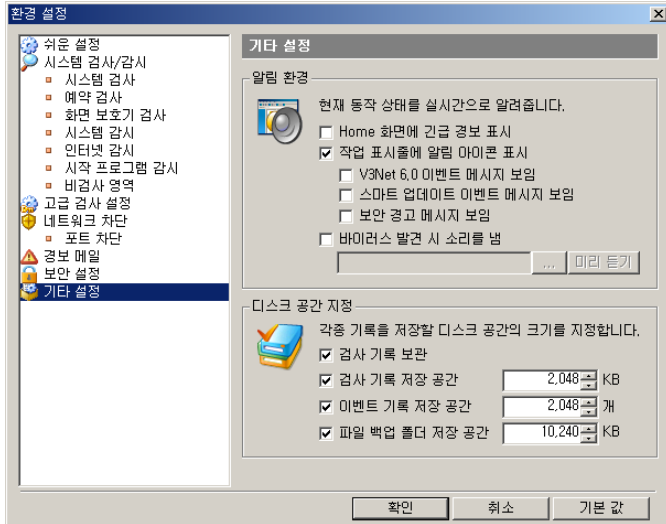


그림 69 기타 설정

### 알림 환경

다음과 같은 경우에 각각 작업 표시줄의 이벤트 메시지나 소리 등을 사용해서 사용자에게 이를 알려줍니다.

- Home 창에 긴급 경보 표시: Home 메뉴의 오른쪽 상단에 최신 긴급 바이러스 정보가 나타납니다.
- 작업 표시줄에 알림 아이콘 표시: 작업 표시줄 오른쪽 하단에 알림 아이콘이 표시되어, 다음과 같은 이벤트 메시지를 보여줍니다.
  - V3Net for Windows Server 6.0의 이벤트 메시지 보임: 엔진 업데이트 오류, 바이러스 발견 등 중요한 이벤트가 발생하면 사용자에게 이벤트 메시지를 보여서 알려줌
  - 스마트 업데이트 이벤트 메시지 보임: 스마트 업데이트 오류가 발생하면 사용자에게 이벤트 메시지를 보여서 알려줌

- 보안 경고 메시지 보임: 사용자의 시스템에서 보안 취약점이 발견되면 보안 경고 메시지를 보여서 알려줌

✓참고 작업 표시줄에 알림 아이콘 표시를 선택 해제하면, 포트 차단에서 작업 표시줄에 포트 차단 메시지 보임을 선택할 수 없습니다.

- 바이러스 발견 시 소리를 냄: 바이러스가 발견되었음을 사용자에게 알려 줄 때, 사용할 음악 파일을 지정합니다.
- ...을 눌러서 사용자의 시스템에 저장되어 있는 WAV 파일을 선택하고, 미리 듣기를 눌러서 소리를 확인할 수 있습니다.

## 디스크 공간 지정

검사 기록, 이벤트 기록 등을 저장할 디스크 공간을 지정합니다.

- 검사 기록 보관: 각 날짜 별로 수행한 검사 기록을 저장합니다. 검사 기록 메뉴에서 자세한 내용을 확인할 수 있습니다.
- 검사 기록 저장 공간: 검사 기록을 저장할 수 있는 디스크 공간의 크기 (512~4,194,303KB)
- 이벤트 기록 저장 공간: 저장할 수 있는 이벤트 기록의 개수 (512~4,194,303개)
- 파일 백업 폴더 저장 공간: 검역소에 백업할 수 있는 파일 백업 폴더의 크기 (512~4,194,303KB)

## 7장

# 부록

용어 /114

색인 /118

V3Net for Windows Server 6.0을 사용하는 데  
도움이 될 수 있는 용어를 설명합니다.  
색인을 사용하면 원하는 기능만  
바로 찾아서 볼 수 있습니다.

### D

**DNS:** (Domain Name Service: 도메인 네임 서비스) DNS는 인터넷상에서 통신을 하기 위해서는 각각의 주 컴퓨터를 식별할 수 있도록 사용하는 도메인이라는 단위를 관리하는 서비스입니다.

### I

**IGMP:** IGMP는 IP 멀티캐스트를 실현하기 위한 통신 규약입니다. 구내 정보 통신망(LAN)상에서 라우터가 멀티캐스트 통신 기능을 구비한 PC에 대하여 멀티캐스트 패킷을 분배하는 경우에 사용됩니다.

**IP:** 인터넷에 연결된 모든 통신망과 그 통신망에 연결된 컴퓨터에 부여되는 32비트의 고유한 숫자입니다. 일반적으로 8비트(1바이트)마다 마침표로 구분하여 4개의 10진수로 표현합니다.

**IP 주소:** IP 주소 (Internet Protocol Address)는 인터넷에 접근하는 각 시스템마다 할당된 정형화된 주소로서, 8 비트 단위마다 마침표로 구분된 32 비트의 숫자로 표현합니다. 우리 나라에서는 0.0.0.0 ~ 255.255.255.255 사이의 IP 주소를 사용할 수 있습니다.

**IPX:** IPX(Internetnetwork Packet eXchange) IPX는 미국 노벨사의 망 운영 체제인 넷웨어 (NetWare) 386의 네트워크 프로토콜입니다.

### O

**OLE:** 애플리케이션에 정보의 연계와 공유를 실현하는 기능의 한 가지로서, 윈도우즈 3.1부터 운영 체제(OS)의 표준 기능으로 제공됩니다. 객체 연계 매입(OLE)을 이용하여 어떤 애플리케이션에서 작성된 정보를 다른 애플리케이션에 연결시킵니다.

### S

**SMTP:** TCP/IP의 상위 층 응용 프로토콜의 하나로, 컴퓨터 간에 전자 우편을 전송하기 위한 프로토콜입니다.

**SPX:** (Sequenced Packet eXchange:순차 패킷 교환) SPX는 미국 노벨사(Novell, Inc.)의 망 운영 체제인 넷웨어(NetWare)의 상위 프로토콜의 하나입니다.

## T

**TCP:** TCP는 2개의 호스트간에 연결된 데이터 흐름에 신뢰성을 보장해주는 통신 프로토콜입니다.

**TCP/IP:** (Transmission Control Protocol/Internet Protocol) TCP/IP는 컴퓨터 간의 통신을 위해 TCP와 IP를 조합하여 미국 국방부에서 개발한 통신 프로토콜입니다.

**Telnet:** 컴퓨터를 이용해 상대방의 원격 컴퓨터에 접속하기 위한 프로토콜로서, 이 프로토콜을 사용하면 서로 다른 기종의 컴퓨터도 통신할 수 있습니다.

## U

**UDP:** IP를 사용하는 네트워크 내에서 컴퓨터 간에 메시지들이 교환될 때 제한된 서비스만을 제공하는 통신 프로토콜입니다.

**UNC:** (Universal Naming Convention) 컴퓨터 내의 공유 파일이 저장되어 있는 장치를 명시하지 않고, 그 파일을 확인하기 위한 방법입니다. 윈도우즈 운영 체제, 노벨 네트웨어와 같은 운영 체제들도, 자체적인 명명 시스템 대신 사용될 수 있습니다.

## ㄱ

**게이트웨이:** 다른 네트워크로 들어가는 관문의 기능을 수행하는 지점으로 볼 수 있습니다.

**공유:** 복수의 사용자가 네트워크상에서 중앙 컴퓨터 또는 공용 서버에 저장되어 있는 파일들을 요구, 열람, 변경하는 컴퓨터 파일 사용 방법입니다.

## L

**네트워크 마스크:** IP 주소에서 네트워크를 식별할 수 있는 부분과 호스트를 식별할 수 있는 부분을 나누어 주는 값으로서 일반적으로 서브넷 마스크라고도 합니다.

## ㄷ

**단편화:** 정보 송수신 시에 임의의 긴 데이터를 통신 프로토콜이 관리하기에 적절한 크기로 분할하는 것을 말합니다.

**데이터그램 서비스:** 패킷 통신망이 제공하는 서비스의 한 종류로, 가상 회선 서비스에 대응되는 개념입니다. 가상 회선 서비스와는 달리, 패킷을 전송하기 전에 회선을 설정하지 않고 전송할 각 패킷에 수신 측의 주소를 명시하여 전송

하는 방식을 취합니다.



**매크로:** 표 계산 소프트웨어인 엑셀(Excel)이나 문서 처리 소프트웨어인 워드(word) 등의 매크로 기능을 악용한 바이러스를 의미합니다.

**무결성:** 정보 및 자원을 불법적으로 변경하여 사용할 수 없도록 보호하는 성질을 의미합니다.



**부트 바이러스:** 컴퓨터를 처음 켜면 처음으로 실행되는 하드 디스크의 부트 섹터(Boot Sector)에 위치한 바이러스를 의미합니다. 대표적인 부트 바이러스는 브레인(Brain) 바이러스와 미켈란젤로(Michelangelo) 바이러스 등이 있습니다.



**서브 네트워크:** 통신망의 일부로 구성되어 있는 망을 서브네트워크(부분망)라 말합니다. 중계 기능을 제공하는 하나 또는 복수의 개방형 시스템 집합으로 되어 있고, 말단의 개방형 시스템은中间的의 개방형 시스템을 이용하여 망 이동을 할 수 있는 망입니다. 패킷 교환망, 회선 교환망, 구내 정보 통신망(LAN) 등이 있습니다.

**서브넷 마스크:** 라우터가 IP 주소 중의 부분망 주소를 식별하기 위한 정보입니다. 부분망을 이용하여 통신을 하는 경우 IP 주소 중 어느 부분이 부분망 번호인지를 식별할 수 있도록 하기 위해서는 부분망 번호의 위치를 판단하는 템플릿(패턴 인식에 사용되는 원형 패턴)을 라우터에 설정합니다.

**세션:** 프로세스들 사이에 통신을 수행하기 위해서 메시지 교환을 통해 서로를 인식한 이후부터 통신을 마칠 때까지의 기간을 말합니다.

**세션 서비스:** 세션 계층은 응용 계층 간의 통신을 위한 제어 구조를 제공합니다. 또한 상호 통신을 하고 있는 응용 계층 간을 연결, 관리하고 연결을 종료시키는 역할을 합니다.

**스크립트:** 소프트웨어를 실행시키는 처리 절차를 문자(텍스트)로 기술한 것으로서, 일종의 프로그램이라고 할 수 있습니다. 응용 프로그램이나 운영 체제(OS)에서 사용자가 제어할 수 있는 일련의 처리 과정을 조합하여 자동화하기 위해서 사용합니다.

## ○

**원격 컴퓨터:** 중앙 처리 장치, 통신 장치, 단말 장치, 사용자 등 4가지 요소로 구성되는 시스템을 원격 컴퓨터라 말합니다. 이들의 상호 연관 동작으로 작업을 수행합니다.

**웜:** Worm 바이러스: 컴퓨터 내부 시스템에 직접적인 피해를 입히지는 않지만, 허용된 범위 내에서 계속 자신을 복제하는 프로그램을 의미합니다. 대표적인 웜으로 HLLC.AIDS\_II, HLLC.Even\_Beeper, HLLC.Laufwerk가 있습니다.

**응용 프로그램:** 컴퓨터로 사용자의 업무를 처리하기 위해 작성된 프로그램을 말합니다. 응용 프로그램은 게임, 그래픽과 컴퓨터 이용 설계(CAD), 통신, 문서 처리, 사무 계산, 데이터베이스, 과학 기술용 수치 해석 등 수많은 분야가 있습니다.

## ㄷ

**트래픽:** 전신, 전화 등의 통신 시설에서 통신의 흐름을 지칭하는 말입니다. 개개의 호 보류 시간에 관계없이 발생한 호의 수를 호 수라고 하고 호 수와 평균보류 시간의 곱을 트래픽량, 단위 시간당 트래픽량을 호량 또는 트래픽 밀도라 합니다.

**트로이 목마 프로그램:** 바이러스의 이름 중에 Trojan이 포함되어 있는 프로그램으로서, 시스템 메모리 영역에 상주하여 사용자의 컴퓨터 작업을 방해합니다.

**패킷:** 데이터 전송에서 사용되는 데이터의 묶음을 말합니다. 패킷 전송은 두 지점 사이에 데이터를 연속적으로 전송하지 않고, 전송할 데이터를 적당한 크기로 나누어 패킷의 형태로 구성한 다음 패킷들을 하나씩 보내는 방법을 씁니다.

## ㄹ

**프로토콜:** 컴퓨터와 컴퓨터 또는 컴퓨터와 단말기 등의 정보 기기간의 정보 교환을 위해서 미리 정해 놓은 여러 가지 통신 규칙과 방법에 대한 약속 즉, 통신 규약을 의미합니다. 대표적인 예로 인터넷에서 사용하고 있는 TCP/IP를 들 수 있습니다.

**프록시 서버:** 내부의 클라이언트를 대신해서 외부 서버와 통신하는 컴퓨터를 의미합니다. 프록시 서버는 클라이언트로부터 요청을 받고 이를 통과시킬 것 인지를 결정하고 서버에 요청합니다. 또한, 서버로부터 응답을 받아서 다시 클라이언트에 전달합니다.

# 색인

|                   |        |
|-------------------|--------|
| ㄱ                 |        |
| 감염자 추적 .....      | 12, 86 |
| 검사 기록 보관 .....    | 112    |
| 검사 기록 저장 공간 ..... | 112    |
| 공유 해제 후 검사 .....  | 95     |

|             |                |
|-------------|----------------|
| ㄴ           |                |
| 단축 메뉴 ..... | 79             |
| 도구 모음 ..... | 67, 68, 71, 79 |

|                     |    |
|---------------------|----|
| ㄷ                   |    |
| 로컬 드라이브 쓰기 검사 ..... | 96 |
| 로컬 드라이브 읽기 검사 ..... | 96 |

|                |     |
|----------------|-----|
| ㄹ              |     |
| 매크로 정책 .....   | 97  |
| 메모리 검사 .....   | 98  |
| 메일 계정 설정 ..... | 106 |

|                              |            |
|------------------------------|------------|
| ㅁ                            |            |
| 바이러스 경보 메일 .....             | 107        |
| 바이러스 미 발견 시 검사 창 자동 종료 ..... | 80, 82, 85 |
| 백그라운드 검사 .....               | 82         |
| 백업 파일 등록 정보 .....            | 63         |
| 보안 경고 메시지 보임 .....           | 69, 112    |
| 보안 기능 .....                  | 109, 110   |
| 보호 대상 설정 .....               | 109        |
| 부트 영역 검사 .....               | 96, 98     |

|                        |            |
|------------------------|------------|
| ㅂ                      |            |
| 사용자 검사 목록 .....        | 41, 42, 54 |
| 사용자에게 알림 메시지 보이기 ..... | 69, 98     |
| 서버 정보 설정 .....         | 34         |
| 웹 종료 후 검사 .....        | 95         |
| 시스템 감시 경보 메일 .....     | 107        |
| 시스템 감시 자동 재시작 .....    | 13, 88     |

|                    |                |
|--------------------|----------------|
| 시스템 검사/감시 정책 ..... | 98             |
| 시스템 보호 수준 .....    | 13, 24, 40, 75 |
| 시작 프로그램 검사 .....   | 98             |
| 신고 센터로 전송 .....    | 59, 62         |

|                     |     |
|---------------------|-----|
| ㅇ                   |     |
| 알림 도구 모음 .....      | 71  |
| 알림 환경 .....         | 111 |
| 업데이트 경보 메일 .....    | 107 |
| 엔진 업데이트 내용 보기 ..... | 52  |
| 예약 설정 .....         | 53  |
| 오피스 프로텍터 .....      | 78  |
| 유해 기능 프로그램 .....    | 96  |
| 이벤트 기록 저장 공간 .....  | 112 |

|                         |     |
|-------------------------|-----|
| ㅈ                       |     |
| 자체 검사 .....             | 98  |
| 자체 보호 .....             | 98  |
| 작업 표시줄에 알림 아이콘 표시 ..... | 111 |

|                        |                        |
|------------------------|------------------------|
| ㅊ                      |                        |
| 최신 긴급 바이러스 .....       | 52                     |
| 치료 또는 삭제 전 파일 백업 ..... | 80, 82, 85, 87, 89, 91 |

|                 |    |
|-----------------|----|
| ㅌ               |    |
| 탐색기 도구 모음 ..... | 71 |

|                      |     |
|----------------------|-----|
| ㅍ                    |     |
| 파일 백업 폴더 저장 공간 ..... | 112 |
| 프로세스 검사 .....        | 98  |