AhnLab
V3 Internet Security 8.0

사용설명서

무게감이 다르다! 가벼운 V3

V3 뉴 프레임워크 적용을 통한 경량화 실현
복합적 위협에 대응하기 위한 다양한 보안 기능 제공

- V3 뉴 프레임워크 적용을 통한 경량화
- Anti-Virus와 Anti-Spyware 기능의 완벽한 통합
- 개인 방화벽과 네트워크 침입 차단 기능을 통한 네트워크 보안 기능
- 웹 보안 및 메일 보안 기능
- 안정적 시스템 운영을 위한 프로세스 실행 차단 기능
- PC 최적화, 파일 완전 삭제 등 다양한 부가 기능

일러두기

2009년 4월 24일 제 1판 발행

표기 규칙	표기 규칙 내용
V3 IS 8.0, V3 Internet Security 8.0	AhnLab V3 Internet Security 8.0 프로그램의 약칭입니다.
< >	창의 이름입니다.(예: <설치 확인>)
->	메뉴 실행 순서입니다.(예: **시작->프로그램**)
굵은 글꼴	버튼 이름, 창에 나오는 메시지입니다.(예: **확인**)
참고	프로그램을 사용할 때 참고할 사항입니다.
주의	프로그램을 사용할 때 주의해야 할 사항입니다.

고객지원

(주)안철수연구소에서는 고객만족센터와 홈페이지를 통해 정품 등록 사용자가 프로그램을 사용하면서 느끼는 의문 사항이나 사용 방법, 프로그램 오류에 대하여 상담 서비스를 제공하고 있습니다. 상담을 요청하기 전에 다음과 같은 내용을 미리 확인하면 더 빠르고 정확하게 문제를 해결할 수 있습니다.

고객 지원을 요청하기 전에 확인할 사항

- ❖ 온라인 도움말이나 사용설명서를 확인하십시오. 온라인 도움말과 사용설명서는 V3 IS 8.0의 사용과 관련하여 많은 정보를 담고 있어 고객님의 문제를 상담 전에 해결할 수도 있습니다.
- ❖ 사용하고 있는 제품이 정식으로 등록된 제품인지 확인하십시오. 제품 번호를 정식으로 등록하지 않고 사용할 경우 정품 사용자에게 제공하는 상담 서비스를 이용할 수 없습니다.
- ❖ 제품과 엔진을 최신 버전으로 업데이트했는지 확인하십시오. 프로그램의 잘못된 동작은 제품과 엔진을 최신 버전으로 업데이트하면 해결되는 경우가 많습니다.

고객만족센터 연락처

- ❖ 안철수연구소 홈페이지: http://www.ahnlab.com
- ❖ 기업고객 핫라인: 02-2186-3082
- ❖ 1:1 메일 상담: http://www.ahnlab.com의 고객지원->1:1 메일 상담
- ❖ 주소: 150-869 서울시 영등포구 여의도동 12번지 CCMM빌딩 6층 (주)안철수연구소 고객만족센터 담당자앞

목차

1장
V3 Internet Security 8.0 소개

새로운 기능

V3 IS 8.0은 악성코드를 더 효과적으로 진단/치료하고 사용자 편의성을 높이기 위해 다음과 같은 기능을 새롭게 추가하고 성능을 대폭 향상 하였습니다.

가벼워진 리소스 점유율과 바이러스와 스파이웨어 엔진의 완벽한 통합

차세대 플랫폼인 V3 뉴 프레임워크를 적용하여 검사 속도를 향상시키고 메모리 점유율도 감소시켰습니다. 이 플랫폼은 시스템 부하를 최소화할 수 있게 설계된 독립적인 콤포넌트 구조로 기존 구조보다 160%~300% 향상된 경량화와 빠른 속도를 지원하며, 안티바이러스, 안티스파이웨어 엔진을 통합하여 리소스 점유율을 개선하고 매일 발견되는 새로운 보안 위협에 대한 대응 속도도 향상 시켰습니다.

TrueFind(은폐진단) 기능

TrueFind는 은폐하거나 악성코드 스스로 자기를 보호하고 있는 경우를 찾아내어 진단하고 치료할 수 있도록 해 주는 새로운 기술입니다. 최근의 악성코드는 감염 후 자신의 감염 사실을 숨기고 오랫동안 동작하기 위해 자신의 파일, 프로세스, 레지스트리 정보를 숨깁니다. 악성코드가 자신을 은폐하면 백신이나 Windows의 탐색기, 작업 관리자에서 해당 악성코드를 찾지 못해 사용자의 피해가 더욱 증가합니다. V3 IS 8.0은 TrueFind(은폐진단)라는 신기술을 도입하여 지능적으로 은폐된 악성코드의 파일, 프로세스 레지스트리를 찾아서 치료합니다. TrueFind(은폐진단)는 모든 은폐형 악성코드와 앞으로 나타날 가능성이 있는 악성코드까지 대응하므로 사용자 PC의 안전성이 더욱 높아질 수 있습니다.

USB 드라이브 검사

저장 매체를 통한 악성코드 감염은 초기의 플로피 디스켓을 통한 바이러스 감염에서 시작하여 현재는 USB 드라이브를 통한 악성코드 전파가 일반화되고 있습니다. 가지고 있는 USB 드라이브를 무심코 PC에 연결하여 악성코드에 감염된 파일을 실행하면 해당 PC에 악성코드가 감염되기 쉽습니다. V3 IS 8.0은 최근의 이러한 추세를 반영하여 USB 미디어에 저장된 데이터의 악성코드 감염 여부를 검사합니다. USB 드라이브 검사를 선택한 후 USB 미디어를 연결하면 자동으로 PC 검사가 실행되어 저장된 폴더나 파일의 악성코드 감염 여부를 검사하고 설정된 방법에 따라 치료하므로 USB 미디어를 통한 악성코드 감염을 사전에 차단할 수 있습니다.

Hosts 파일 변조 방지

사용자 PC의 네트워크 연결 정보가 저장된 Hosts 파일을 변조하여 개인 정보를 유출하는 파밍(Pharming)공격에 대응하기 위해 Hosts 파일의 변경이 있는 경우 차단합니다. Hosts 파일이 변경되어 저장되려고 할 때 사용자에게 파일 변조를 알려주면 사용자는 Hosts 파일 변조를 확인한 후에 변경을 차단하거나 허용할 수 있으므로 악성코드로 인한 Hosts 변조를 예방하여 개인 정보 유출과 같은 피해를 사전에 차단할 수 있습니다.

블랙리스트(BlackList)기반의 실행 차단 기능

회사나 단체에서 업무에 필요하지 않은 프로그램을 차단하고 원격 키로거등 악용 가능한 프로그램의 실행을 차단하여 안정적인 컴퓨터 사용을 도와줍니다. 실행 차단 기능은 사용자가 직접 차단할 폴더나 프로그램을 등록하면 해당 파일이 실행될 때 차단해 줍니다.

이럴 땐 이렇게

V3 IS 8.0을 다음과 같은 경우에 활용하면 다양한 보안 위협과 PC 문제를 해결하는데 도움이 될 수 있습니다.

바이러스나 스파이웨어와 같은 악성코드 감염이 의심되는 경우

빠른 검사, 정밀 검사, 사용자 목록 검사, USB 드라이브 검사, 실시간 검사, 탐색기 검사, 예약 검사 등 다양한 검사 방법을 활용하여 사용자 상황에 맞는 검사를 실행할 수 있습니다. 악성코드는 파일을 복사, 이동, 실행, 다운로드하는 경우에 V3 IS 8.0이 제공하는 다양한 검사 기능이 악성코드 감염 여부를 검사합니다.

메신저를 통해 파일을 받는 경우

메신저를 통한 감염이 일반화된 상황에서 V3 IS 8.0의 메신저 실시간 검사를 사용하면 상대방이 보낸 파일을 무심코 수락하여 악성코드에 감염되는 치명적인 실수를 예방할 수 있습니다.

메일을 통해 첨부 파일을 보내거나 받는 경우

메일 검사의 받는 메일 실시간 검사(POP3)와 보내는 메일 실시간 검사(SMTP)를 사용하면 감염된 첨부 파일을 보내거나 받는 위험을 예방할 수 있습니다. 메일을 통한 악성코드 전파는 감염된 메일을 보낸 사람의 신뢰도 뿐만 아니라 보낸 사람이 속한 회사나 단체의 신뢰도에 영향을 끼치므로 메일 실시간 검사를 사용하면 이러한 위험을 최소화하는데 도움이 됩니다.

스팸 메일을 차단하고 싶은 경우

사용자가 입력한 스팸 차단 규칙에 따라 스팸 메일을 효과적으로 걸러낼 수 있습니다. 스팸 메일 차단을 사용하면 사용자가 직접 설정한 스팸 차단 규칙에 따라 스팸 메일을 자동으로 차단하여 불필요한 스팸으로 인한 불편을 최소화할 수 있습니다. 또한, 허용/차단 메일을 설정해 두면 사용자가 설정한 주소에서 온 메일을 허용하거나 차단하여 꼭 필요한 메일을 받는데 도움이 됩니다.

인터넷을 통해 다양한 웹사이트에 접속하는 경우

인터넷 상거래가 활성화되면서 사기 사이트나 불법적인 사이트 접속으로 사용자들이 피해를 보는 경우가 증가하고 있습니다. 웹 보안에서 제공하는 피싱 사이트 차단은 피싱으로 알려진 일반적인 사이트에 대한 데이터베이스를 바탕으로 사용자들이 접속하는 사이트가 피싱 사이트인지 알려줍니다. 웹사이트 필터링을 사용하면 성인 사이트나 도박과 같은 불건전한 사이트 접속을 차단하고 회사나 단체에서 사용이 금지된 웹사이트에 접속하는 것을 차단할 수 있습니다.

중요한 파일을 깨끗하게 지우고 싶은 경우

개인 정보가 담겨 있는 파일이나 업무상 중요한 파일을 삭제할 때 Windows에서 제공하는 삭제를 사용하면 하드 디스크에 해당 파일의 정보가 남아 있어 복구 프로그램으로 파일을 복구하여 사용할 수 있습니다. 파일 완전 삭제를 사용하면 삭제한 파일을 복구할 수 없거나 복구하더라도 원본과 다른 내용으로 복원을 합니다. 사용하던 하드 디스크를 버리거나 교체하는 경우에 파일 완전 삭제로 파일을 삭제하면 남아 있는 정보를 불법으로 복구하여 사용하는 악의적인 사용자로부터 개인 정보와 소중한 업무 정보를 보호할 수 있습니다.

컴퓨터의 속도가 느려지거나 임시 파일을 정리하고 싶은 경우

웹사이트에 접속하면 다른 사람은 보이지 않는 이상한 그림이나 메뉴가 보이거나 컴퓨터의 실행 속도가 예전보다 느려졌다고 느껴진 경우에는 PC 최적화를 실행해 보시기를 권장합니다. 웹사이트 접속 시에 저장되는 쿠키 정보와 같은 임시 인터넷 파일을 통해 웹사이트 접속이 느려지거나 남들과 다른 증상이 발생할 수도 있습니다. PC 최적화는 시스템 영역과 임시 인터넷 파일 청소, 메모리 최적화 등을 실행하여 PC 성능을 높이는 데 도움이 됩니다.

1

보안 요건

V3 IS 8.0을 설치하기 전에 먼저 다음과 같은 보안 사항을 확인하십시오.

운영체제 패스워드 규칙(Microsoft Windows XP Professional)

본 제품을 CC인증의 EAL 3 레벨에서 요구하는 보안환경에서 사용하기 위해서는 Microsoft Windows XP Professional 운영체제의 패스워드 규칙에 대해 다음과 같은 규칙을 적용해야 합니다.

Microsoft Windows XP Professional 운영체제의 패스워드 길이는 8자리 이상 40자 이하로 다음 최소 요구 사항을 만족해야 합니다.

- 사용자 계정의 이름의 전부 또는 일부를 포함하지 않아야 합니다.
- 다음 네 범주 중 세 범주의 문자를 포함해야 합니다.
- 영어 대문자(A-Z)
- 영어 소문자(a-z)
- 기본 10 숫자(0-9)
- 기호 문자(예:!,$,#, %)

Microsoft Windows XP Professional 운영체제의 패스워드 규칙을 변경하려면 제어판에서 다음과 같이 설정해야 합니다.

1 **제어판->관리도구->로컬 보안 정책**을 누릅니다.

2 <로컬 보안 설정>이 나타나면, **보안 설정**의 **계정 정책**을 선택합니다.

3 **암호 정책**을 선택합니다.

4 오른쪽 창에 나타난 정책 목록에서 **암호는 복잡성을 만족해야 함**에서 더블 클릭한 후 **사용**을 선택하고 **확인**을 누릅니다.

5 오른쪽 창에 나타난 정책 목록의 **최소 암호 길이**에서 더블 클릭한 후 암호 최소 길이인 8문자를 설정하고 **확인**을 누릅니다.

신뢰된 관리자

- V3 IS 8.0을 사용하는 사용자는 악의가 없으며, 적절한 교육을 받고 사용 지침을 모두 준수해야 합니다.

- V3 IS 8.0은 Administrator 권한이 있는 계정으로 로그인한 사용자만 프로그램을 설치하거나 V3의 정책(환경 설정)을 변경, PC 검사 및 치료 등 V3의 모든 기능을 사용할 수 있습니다.
- Administrator 이외 유형의 계정으로 로그인한 사용자는 V3의 기능 중 PC 검사 및 치료 요청, 이벤트 기록 및 검사 기록의 조회/삭제/저장, 검역소 정보의 복원/삭제/임의의 폴더로 이동/바이러스 신고센터로 전송만 사용할 수 있습니다.

참고

검역소의 복원, 임의의 폴더로 이동은 로그인한 계정이 복원할 폴더나 임의의 폴더에 쓰기 권한이 있어야 합니다.

신뢰된 서버

- V3 IS 8.0이 설치되면 기본적으로 안철수연구소 업데이트 서버에 대한 도메인 주소를 갖게 되며 소프트웨어 배포 과정에 신뢰성이 있다면 업데이트 서버에 대한 도메인 주소를 신뢰합니다.

네트워크 환경

- 사용자 시스템 위치는 네트워크 공격으로부터 내부망을 보호하는 네트워크 보안 장비(방화벽, IDS등)가 설치/운영되는 신뢰된 네트워크 환경에 위치해야 하며 네트워크 보안 장비의 보안정책에 따라 동일한 보안 수준으로 통제 운영되어야 합니다.

물리적 접근제한

- V3 IS 8.0이 설치된 컴퓨터는 물리적으로 안전해야 합니다.
- 허가받지 않은 사용자가 V3 IS 8.0에 접근할 수 없도록 운영체제에서 제공하는 화면 보호기 기능을 사용해야 합니다. 화면 보호기를 해제하려면 암호를 입력하도록 설정해야 합니다.

운영체제 보강

- V3 IS 8.0이 설치된 컴퓨터에서는 필요없는 서비스를 실행하지 않습니다.
- V3 IS 8.0이 설치된 컴퓨터에는 필요없는 프로그램을 설치하지 않습니다.
- 운영체제의 취약점을 보완하는 패치를 주기적으로 실행하여 운영체제가 최신의 상태를 유지하도록 합니다.

시그너처 갱신

- V3 IS 8.0의 인가된 사용자는 시그너처 등 보안 기능 데이터를 최신의 상태로 유지해야 합니다.

2장
설치하기

시스템 사양

2

V3 IS 8.0을 설치하기 위해서는 다음의 시스템 사양 이상의 컴퓨터와 소프트웨어 환경을 만족해야 합니다. 시스템 사양을 확인하신 후에 설치하여 주시기 바랍니다.

하드웨어 환경

- CPU: Intel Pentium III 500MHz 이상
- 메모리: 256MB 이상
- HDD: 300MB 이상의 여유 공간
- 해상도: 800x600 256 컬러 이상

웹브라우저

- Microsoft Internet Explorer 5.0 이상

지원 언어

- 한글
- 영어

참고

V3 IS 8.0을 설치할 수 있는 소프트웨어 환경 중 해당 운영체제가 한글이면 한글 버전으로 설치되고, 해당 운영체제가 영어인 경우 영어 버전의 V3 IS 8.0이 설치됩니다.

소프트웨어 환경

❖ 32 비트 계열

- Windows 2000(SP 4 이상) Professional
- Windows XP(SP 2 이상) Professional
- Windows XP(SP 2 이상) Home Edition
- Windows XP(SP 2 이상) Media Center Edition
- Windows Vista(SP 1 이상) Home Basic Edition
- Windows Vista(SP 1 이상) Home Premium Edition
- Windows Vista(SP 1 이상) Business Edition
- Windows Vista(SP 1 이상) Enterprise Edition
- Windows Vista(SP 1 이상) Ultimate Edition

❖ 64 비트 계열

- Windows XP Professional x64 Edition
- Windows Vista Home Basic Edition
- Windows Vista Home Premium Edition
- Windows Vista Business Edition
- Windows Vista Enterprise Edition
- Windows Vista Ultimate Edition

설치 전 확인사항

2

V3 IS 8.0을 설치하기 전에 설치할 때의 주의 사항과 패키지 구성 내용 등을 먼저 확인해 주시기 바랍니다.

제품 구성물 확인

V3 IS 8.0을 구입하면 제품이 들어있는 패키지 박스와 박스 안에 제품 설치 CD와 사용설명서 등이 포함되어 있습니다. 프로그램 패키지 내용물을 확인하시고 제품 구성물에 이상이 없는지 확인해 주시기 바랍니다.

- V3 IS 8.0 프로그램 설치 CD 1장
- CD 케이스 1개
- 사용설명서
- 제품 번호 스티커
- 소프트웨어 사용권 증서
- 패키지 박스

시스템 사양 및 사용자 계정

V3 IS 8.0을 설치하기 전에 시스템 사양과 사용자 계정 권한을 확인하십시오.

❖ 시스템 사양을 먼저 확인하십시오. V3 IS 8.0을 설치하려는 대상 시스템이 V3 IS 8.0이 지원하는 사양 이상의 컴퓨터인지 확인해 주십시오. 시스템 사양을 충족하지 못할 경우 설치가 정상적으로 되지 않거나 설치 후에 프로그램이 정상 실행되지 않을 수도 있습니다.

❖ V3 IS 8.0을 설치하려는 사용자 계정이 Administrator 이거나 동등한 권한이 있는 계정인지 확인하십시오.

❖ Administrator 이외 유형의 계정으로 로그인한 사용자는 V3 IS 8.0의 일부 기능을 사용할 수 없습니다. 실행 가능한 기능에 대해서는 보안 요건을 확인하십시오.

방화벽 사용 여부 확인

V3 IS 8.0을 설치하기 전에 Windows 방화벽이나 타 사에서 제공하는 방화벽 프로그램이 작동하고 있는지 확인하십시오. 방화벽이 설치되어 있거나 작동하고 있는 경우 해당 프로그램을 삭제하거나 작동을 중지한 후에 V3 IS 8.0을 설치하시기 바랍니다. V3 IS 8.0의 개인 방화벽 기능은 설치할 때 설치 여부를 사용자가 직접 선택할 수 있습니다.

네트워크 연결 상태 확인

V3 IS 8.0을 설치 후 엔진 업데이트와 네트워크 침입 차단 등 네트워크 기반의 기능이 정상 동작하려면 사용자 컴퓨터의 인터넷 연결이 정상적이어야 합니다. 회사나 단체의 경우 내부 프록시 서버 설정이나 방화벽, 기타 다른 웹사이트 접속 등 전반적인 인터넷 연결 상태에 문제가 없는지 확인하여 주십시오.

실행 중인 다른 응용 프로그램 종료

V3 IS 8.0을 설치하기 전에 설치 프로그램을 제외한 다른 응용 프로그램의 실행을 먼저 종료할 것을 권장합니다.

업그레이드

2

안철수연구소에서 제작한 V3 IS 8.0 이전의 보안 프로그램이 설치되어 있는 경우라면 다음 제품에 한하여 해당 프로그램을 자동 삭제하고 V3 IS 8.0을 설치합니다.

자동 삭제 후 기존에 사용하던 데이터를 활용할 수 있는 제품

V3 Internet Security 7.0 제품군을 사용하고 있었다면 V3 IS 8.0을 설치하면서 이전 제품의 이벤트 로그, 검사 로그, 검역소 백업 정보 등을 V3 IS 8.0에서 다시 사용할 수 있습니다. 이전 제품의 정보를 다시 사용하려면 삭제할 때 **다시 설치할 때 사용할 수 있는 데이터를 삭제합니다.**를 선택하지 않고 삭제하면 필요한 데이터를 그대로 사용할 수 있습니다.

- V3 Internet Security Enterprise 7.0
- V3 Internet Security Platinum Enterprise 7.0

자동 삭제 후 기존에 사용하던 데이터를 활용할 수 없는 제품

다음 제품들이 설치된 상태에서 V3 IS 8.0을 설치하면 자동으로 삭제하고 V3 IS 8.0을 설치합니다. 다음 제품들을 사용하면서 저장된 이벤트 로그, 검사 로그, 검역소 백업 정보 등은 프로그램 삭제와 함께 모두 삭제되며 V3 IS 8.0에서 해당 정보를 가져와서 사용할 수 없습니다.

- V3Pro 2002
- V3Pro 2004
- AhnLab SpyZero
- AhnLab Security Pack

설치

V3 IS 8.0을 설치하는 방법은 다음과 같습니다.

참고

V3 Internet Security 7.0/2007을 사용하고 있었다면, V3 IS 8.0을 설치하면서 이전 제품을 삭제할 수 있습니다. V3 IS 8.0을 설치하면서 이전에 설치된 V3 Internet Security 7.0/2007을 삭제하면 방화벽 규칙이나 검역소 백업 정보 등을 그대로 사용할 수 있습니다.

1 V3 IS 8.0의 CD-ROM을 CD-ROM 드라이브에 넣습니다.

2 자동 실행 화면이 나타나면 **V3 Internet Security 8.0 설치하기**를 누릅니다.

- V3 Internet Security 8.0 설치하기: V3 IS 8.0을 설치합니다.
- Adobe Reader 설치하기: V3 IS 8.0의 사용설명서를 볼 수 있는 Adobe Reader 프로그램을 설치합니다.
- 사용설명서 보기: V3 IS 8.0의 사용설명서를 볼 수 있습니다.
- 설치 CD 열기: V3 IS 8.0 설치 CD의 내용을 볼 수 있습니다.
- 안철수연구소 홈페이지 방문하기: (주)안철수연구소 홈페이지를 엽니다.
- 끝내기: 자동 실행 화면을 닫습니다.

3 <AhnLab V3 Internet Security 8.0 설치>가 나타나면 **다음**을 누릅니다.

4 <사용권 계약>이 나타납니다. V3 IS 8.0의 사용권 계약서를 확인하고 계약에 동의하면 **동의함**을 눌러서 설치를 시작합니다.

5 <사용자 정보>가 나타납니다. **사용자 이름***, **회사 이름**, **제품 번호***를 입력하고 **다음**을 누릅니다.

- 사용자 이름*: 제품을 사용할 사용자의 이름을 입력합니다.
- 회사 이름: 사용자가 속한 부서나 회사의 이름을 입력합니다.
- 제품 번호*: 제품을 구입하고 받은 제품 번호를 입력합니다. 제품 번호를 입력하지 않으면 평가판으로 설치됩니다.

참고

* 표시는 반드시 입력해야 하는 필수 항목입니다.

⚠ 주의

올바른 제품 번호를 입력하지 않으면 일정한 기간 동안만 사용할 수 있는 평가판이 설치됩니다. 평가판 사용 기간이 지나면 엔진을 업데이트할 수 없고 V3 IS 8.0 기능을 대부분 사용할 수 없습니다.

6 <구성 요소>가 나타납니다. 설치할 구성 요소에서 V3 IS 8.0과 같이 설치할 구성 요소를 선택합니다.

- AhnLab Personal Firewall: 개인 방화벽을 설치합니다. 개인 방화벽을 설치하면 방화벽 규칙에 따라 프로그램의 인터넷 연결을 제어하고 네트워크 침입을 탐지할 수 있습니다.

7 <설치 폴더>가 나타납니다.
설치 폴더의 기본 값은 \Program Files\AhnLab\V3IS80 입니다. 다른 폴더에 설치하려면 **찾아보기**를 눌러 설치할 폴더를 직접 선택하고 **설치**를 누릅니다.

8 <설치 진행>이 나타납니다. 설치가 끝날 때까지 기다리십시오.

9 <AhnLab V3 Internet Security 8.0 설치 마침>이 나타납니다. **마침**을 누릅니다.

삭제

V3 IS 8.0을 삭제하는 방법은 V3 IS 8.0이 제공하는 제거 기능을 사용하거나 제어판의 프로그램 추가/제거에서 선택하여 삭제할 수 있습니다.

1 Windows의 작업 표시줄에서 **시작**을 누르고 **모든 프로그램->AhnLab->AhnLab V3 Internet Security 8.0->AhnLab V3 Internet Security 8.0 제거**를 선택합니다.

2 <프로그램 제거>에서 다시 설치할 때 사용할 수 있는 데이터 삭제 여부를 확인하고 **제거**를 누릅니다.

- 다시 설치할 때 사용할 수 있는 데이터를 삭제합니다. V3 IS 8.0이나 V3 Internet Security 7.0 제품군 사용 중에 저장된 방화벽 규칙, 검역소 백업 정보들을 모두 삭제합니다. 이 정보를 삭제하지 않으면 V3 IS 8.0을 다시 설치했을 때 이전에 사용하던 규칙과 검역소 백업 정보들을 다시 사용할 수 있습니다.

3 <제거 진행>에서 V3 IS 8.0에 관련된 폴더와 파일을 삭제합니다.

4 삭제를 마치면, **AhnLab V3 Internet Security 8.0 제거를 끝냈습니다.** 라는 메시지가 나타납니다.

5 **확인**을 누릅니다.

참고

회사나 단체에서 원격 관리 프로그램인 AhnLab Policy Center를 사용하고 있는 경우 AhnLab Policy Center 관리자에 의해 V3 IS 8.0을 설치하거나 삭제할 수도 있습니다.

참고

제어판의 프로그램 추가/제거에서 AhnLab V3 Internet Security 8.0을 선택하고 제거를 눌러도 삭제할 수 있습니다.

제품 번호 등록

평가판으로 V3 IS 8.0을 사용 중인 경우 제품 번호를 등록하면 업데이트와 등록 고객에게 제공하는 다양한 고객 지원 서비스를 이용하실 수 있습니다. 평가판은 사용 기간이 제한되어 있으므로 사용 기간이 지나면 V3 IS 8.0을 정상적으로 사용할 수 없습니다. 제품 구입 시에 받으신 제품 번호를 꼭 등록하여 정품 사용자로서의 혜택을 누리시기 바랍니다.

1 바탕 화면의 V3 IS 8.0 아이콘( )을 더블 클릭합니다.

2 HOME의 제품 사용 기간 옆에 있는 **제품 번호 등록**을 누릅니다.

참고

이미 제품 번호를 등록한 경우에는 HOME에 제품 사용 기간이 표시되지 않습니다.

3 <제품 번호 등록>에서 제품 번호를 입력합니다.

4 **확인**을 누릅니다.

5 **제품 번호를 등록했습니다.** 라는 메시지가 나옵니다. **확인**을 누릅니다.

6 HOME의 제품 사용 기간 영역이 사라지고 실시간 검사 설정, 마지막 검사 날짜, 엔진 버전만 보입니다.

3장
둘러보기

화면 설명

V3 IS 8.0은 사용자가 편리하고 쉽게 프로그램을 이용할 수 있도록 하였습니다. V3 IS 8.0의 주 화면을 실행하면 다양한 기능을 손쉽게 실행할 수 있습니다. V3 IS 8.0 주 화면에서는 각각의 기능을 손쉽게 실행하거나 도움말을 확인할 수 있으며, 사용자에게 맞는 보안 환경을 설정할 수 있습니다.

1. 주요 기능

- HOME: V3 IS 8.0의 주요 기능을 실행할 수 있으며 보안 상태와 프로그램 정보, 빠른 검사, PC 최적화를 간단히 실행할 수 있습니다.
- PC 검사: 바이러스나 스파이웨어 감염이 의심되는 경우 PC 검사의 다양한 검사 방법을 선택하여 검사할 수 있으며 검사에 대한 상세 설정을 할 수 있습니다.
- 네트워크 보안: 해킹 프로그램과 허가하지 않은 인터넷 연결 차단을 위해 네트워크 침입 차단, 개인 방화벽, 허용/차단 IP 주소 사용 여부를 선택하고 상세 설정을 할 수 있습니다.
- 웹 보안: 유해 사이트 차단을 위해 피싱 사이트 차단, 웹사이트 필터링의 사용 여부를 선택하고 상세 설정을 할 수 있습니다.

- 메일 보안: 메일을 통한 악성코드 감염을 차단하기 위해 메일 검사와 스팸 메일 차단, 허용/차단 메일 주소 관리를 통해 안전하게 메일을 사용할 수 있습니다.
- PC 도구: 컴퓨터가 더 안전하고 빠르게 동작할 수 있도록 PC 최적화, 파일 완전 삭제, 실행 차단 목록을 설정하고 실행할 수 있습니다.

2. 공통 기능

- 환경 설정: V3 IS 8.0의 주요 기능을 실행하기 위한 세부 조건을 설정할 수 있습니다.
- 업데이트: 악성코드를 치료하는 검사 엔진을 최신 버전으로 업데이트하고 프로그램 변경 사항이 있는 경우 패치 파일도 함께 업데이트합니다.
- 도움말: V3 IS 8.0의 온라인 도움말을 확인할 수 있으며, 안철수연구소 홈페이지 연결, 최신 바이러스/스파이웨어 정보, 온라인 제품 등록, 제품 정보를 실행하거나 확인할 수 있습니다.

3. 보안 상태 및 프로그램 정보

- 실시간 검사 설정: 실시간 검사 사용 현황을 보여줍니다. 전체 보안 설정에서 모든 보안 기능을 선택했다면 모두 사용 중, 일부만 선택한 경우에는 일부 사용 중, 모두 선택하지 않은 경우에는 사용 안 함으로 표시됩니다.
- 마지막 검사 날짜: V3 IS 8.0으로 PC 검사를 마지막으로 실행한 검사 날짜를 보여줍니다. 검사 기록이 없는 경우 **정보 없음**으로 표시됩니다.
- 엔진 버전: 현재 사용 중인 V3 IS 8.0의 검사/치료 엔진의 버전을 보여줍니다. 엔진 업데이트는 수시로 진행되므로 오늘 날짜가 아닌 경우 업데이트를 실행하시기 바랍니다.
- 제품 사용 기간: 프로그램을 설치할 때 제품 번호를 입력하지 않고 평가판으로 설치한 경우에만 보입니다. 평가판으로 설치한 경우에는 남은 제품 사용 기간과 제품 번호를 등록할 수 있는 링크가 보입니다.

4. 실시간 검사 사용 여부

- PC 실시간 검사: 바이러스와 악성코드를 차단해주는 PC 실시간 검사 사용 여부를 보여줍니다. 사용 안 함인 경우 ▾ 를 눌러 사용을 선택합니다.
- 네트워크 침입 차단: 웜이나 트로이목마와 같은 해킹 프로그램의 침입을 차단해 주는 네트워크 침입 차단의 사용 여부를 보여줍니다. 사용 안 함인 경우 ▾ 를 눌러 사용을 선택합니다.

- 개인 방화벽: 네트워크 규칙과 프로그램 규칙에 따라 허가하지 않은 인터넷 연결을 허용하거나 차단합니다. 사용 안 함인 경우 ▾ 를 눌러 사용을 선택합니다.

참고

개인 방화벽을 설치하지 않은 경우 개인 방화벽 실시간 검사 사용 여부는 표시되지 않습니다.

5. 빠른 검사

V3 IS 8.0이 선정한 주요 폴더에 대한 바이러스와 스파이웨어 감염 여부를 검사합니다.

6. PC 최적화

시스템 영역 청소, Internet Explorer 임시 인터넷 파일 청소, 메모리 최적화 등을 실행하여 필요없는 파일을 정리하고 PC 성능 향상을 도와줍니다.

업데이트와 검사

V3 IS 8.0 설치를 마쳤으면 가장 먼저 최신 엔진으로 업데이트할 것을 권장합니다. 백신 프로그램은 최신 엔진의 업데이트를 적용한 후에 악성코드를 검사해야 새로 발견된 악성코드까지 검사/치료할 수 있습니다. 최신 엔진으로 업데이트한 후에는 바로 컴퓨터 전체를 검사하여 백신 프로그램 설치 이전에 감염된 파일이 있는지 확인하는 것이 좋습니다.

업데이트하기

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 HOME의 오른쪽 위에 있는 **업데이트**를 누릅니다.

3 **업데이트를 준비하고 있습니다.** 라는 메시지가 나타납니다.

4 **업데이트 파일을 다운로드하고 있습니다.** 라는 메시지가 나타나면서 파일 다운로드 상황을 알려줍니다.

5 업데이트 파일을 적용하는 화면이 나타난 후 업데이트를 마치면 창이 자동으로 사라집니다.

6 현재 엔진 버전은 HOME의 엔진 버전이나 화면 오른쪽 위의 도움말의 제품 정보, 작업 표시줄의 V3 알림 아이콘()에 마우스를 위치하면 현재 엔진 버전을 볼 수 있습니다.

검사하기

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**의 **정밀 검사**를 선택합니다.

3 검사 대상 목록에서 검사할 폴더나 파일을 선택합니다.

참고

설치 후 처음하는 검사라면 내 컴퓨터에 연결된 모든 하드 디스크의 모든 폴더와 파일을 검사하는 것이 좋습니다.

4 **검사하기**를 눌러 검사를 실행합니다.

참고

정밀 검사의 자세한 방법이나 내용은 정밀 검사를 참고하십시오.

안전 모드

컴퓨터가 안전 모드 상태로 동작하는 경우, V3 IS 8.0에서는 다음과 같은 기능을 사용할 수 있습니다.

- ❖ 빠른 검사: 사용자 컴퓨터의 중요 폴더와 파일의 악성코드 감염 여부를 검사할 수 있습니다.
- ❖ 보안 설정: 전체 보안 설정에서 자동으로 실행할 보안 기능을 선택하거나 선택을 해제할 수 있습니다.

작업 표시줄

V3 IS 8.0을 설치하면 작업 표시줄에 알림 아이콘()이 등록됩니다. V3 IS 8.0은 작업 표시줄의 알림 아이콘 색상이나 모양에 따라 현재 V3 IS 8.0의 상태를 표시합니다. 작업 표시줄의 알림 아이콘에서 마우스 오른쪽을 누르면 V3 IS 8.0의 주요 기능을 간단히 실행할 수 있습니다.

작업 표시줄의 알림 아이콘

-  : V3 IS 8.0의 실시간 검사가 동작하고 있는 경우입니다.
-  : 예약 검사에서 설정한 주기에 예약 검사를 실행하고 있는 경우입니다.
-  : PC 실시간 검사가 꺼져 있는 경우입니다.
-  : PC 실시간 검사가 꺼진 상태에서 예약 검사에서 설정한 주기에 따라 예약 검사를 실행하고 있는 경우입니다.

작업 표시줄에서 실행할 수 있는 기능

- V3 Internet Security 열기: V3 IS 8.0 프로그램의 HOME 화면을 보여줍니다.
- 빠른 검사: 빠른 검사를 실행하여 바이러스와 스파이웨어 감염 위험이 높은 중요 폴더와 파일을 검사합니다.
- PC 최적화: PC 최적화를 실행합니다. PC 최적화는 필요없는 파일과 레지스트리 정보, 임시 파일을 청소하고 메모리 사용을 최적화합니다
- 실시간 검사
  - PC 실시간 검사: 바이러스와 스파이웨어 같은 악성코드를 다운로드하거나 복사, 이동, 실행하는 경우 PC 실시간 검사가 검사하고 치료합니다. 검사 대상과 범위, 치료 방법은 PC 실시간 검사 설정에 따라 처리합니다.
  - 네트워크 침입 차단: 네트워크 침입 차단을 사용합니다. 네트워크 침입 차단을 사용하면, 네트워크를 통해 웜이나 트로이목마와 같은 악성코드가 침입하는 것을 탐지하여 차단합니다.
  - 개인 방화벽: 개인 방화벽을 사용합니다. 개인 방화벽을 사용하면 네트워크 규칙과 프로그램 규칙에 따라 허가하지 않은 인터넷 연결을 차단하여 컴퓨터를 더 안전하게 유지할 수 있습니다.

❖ 환경 설정: V3 IS 8.0에서 제공하는 모든 기능의 설정을 할 수 있습니다. PC 검사, 네트워크 보안, 웹 보안, 메일 보안, PC 도구 등 각 기능별로 사용자 환경에 맞게 설정할 수 있습니다.

❖ 업데이트: 업데이트를 즉시 실행합니다.

❖ 알림 아이콘 숨김: 작업 표시줄의 알림 아이콘()을 보이지 않게 합니다. 알림 아이콘을 다시 표시하려면, 알림 설정에서 **작업 표시줄에 V3 알림 아이콘 표시**를 선택합니다.

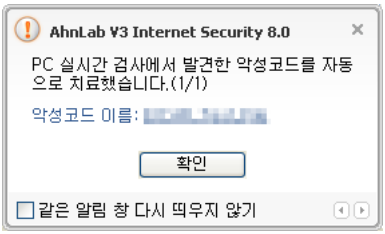
알림 창

알림 창은 환경 설정의 알림 설정에서 설정한 상황이 발생한 경우 알림 창으로 악성코드나 외부의 침입, 파일의 변경 사실을 사용자에게 즉시 알려줍니다.

3

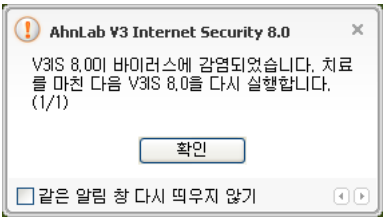
PC/메신저 실시간 검사의 악성코드 치료 알림

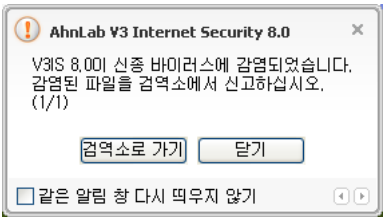
PC/메신저 실시간 검사에서 악성코드를 발견하여 치료했음을 사용자에게 알려줍니다. 알림 창에서는 감염된 악성코드의 이름을 확인할 수 있습니다. 악성코드 이름을 누르면 해당 악성코드의 이름과 감염된 파일의 상세 경로를 확인할 수 있습니다.



V3 감염 여부 검사 후 알림

V3 IS 8.0의 악성코드 감염 여부를 검사하고 감염되었을 경우 다음과 같이 사용자에게 알려줍니다. V3 IS 8.0이 감염되면 자체 검사와 치료 모듈이 감염된 파일을 치료하고 V3 IS 8.0을 다시 실행합니다. V3 IS 8.0이 알려지지 않은 새로운 바이러스에 감염된 경우에는 **검역소로 가기**를 눌러 감염된 파일을 안철수연구소로 즉시 신고하여 주시기 바랍니다.



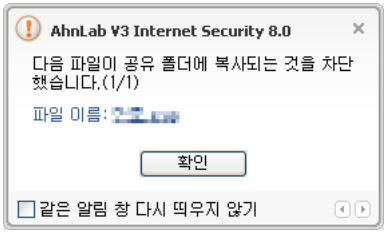


hosts 파일 변경 알림

Windows의 hosts 파일의 변경을 시도한 프로그램이 있는 경우 사용자에게 알려줍니다.

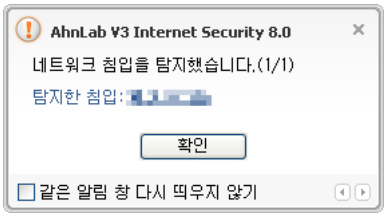
실행 파일이 공유 폴더에 복사되는 것을 차단했을 때 알림

사용자 PC의 공유 폴더에 네트워크를 통해 다른 사용자가 실행 파일을 복사할 때 차단했음을 알려줍니다.



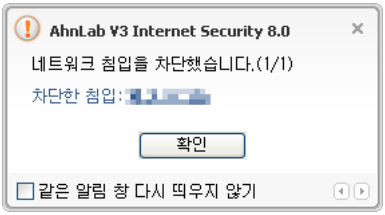
네트워크 침입 탐지 알림

네트워크를 통해 사용자 PC에 침입을 시도한 것을 탐지했을 때 탐지한 침입의 이름과 탐지 사실을 사용자에게 즉시 알려줍니다.



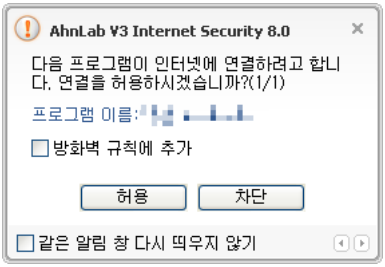
네트워크 침입 차단 알림

네트워크를 통해 사용자 PC에 침입을 시도한 것을 차단했을 때 차단한 침입의 이름과 차단 사실을 사용자에게 즉시 알려줍니다.



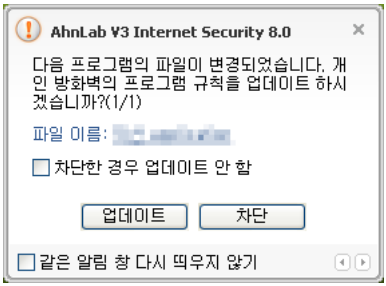
프로그램이 인터넷 접근을 시도할 때 알림

개인 방화벽의 프로그램 규칙에 허용하거나 차단하도록 설정되어 있지 않은 프로그램이 인터넷에 연결하려고 하면 사용자에게 허용/차단 여부를 확인합니다. 인터넷에 연결하려는 프로그램 이름을 확인하고 허용이나 차단을 선택하면 프로그램 규칙에 추가합니다.



프로그램 규칙 업데이트가 필요할 때 알림

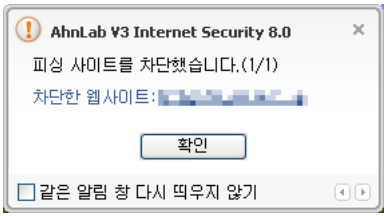
개인 방화벽의 프로그램 규칙에서 인터넷 연결을 허용하도록 설정되어 있는 프로그램이 규칙을 만든 시점과 달리 파일의 고유 정보가 변경된 경우에 다음과 같이 알려줍니다. 프로그램 변경은 악성코드에 의한 변경이나 해당 프로그램 제작사에서 업데이트나 패치를 하기 위해 변경하는 경우가 있습니다. 변경 내용을 잘 확인한 후에 업데이트 여부를 선택해야 합니다.



- 업데이트 선택: 차단한 경우 업데이트 안 함에 영향을 받지 않고 기존 프로그램 규칙에서 파일 고유 정보를 업데이트하여 인터넷 연결을 계속 허용합니다.
- 차단한 경우 업데이트 안 함을 선택하고 차단을 선택한 경우: 프로그램 규칙을 만들 때와 달리 파일 고유 정보가 변경된 이 파일의 인터넷 연결을 차단하고 프로그램 규칙은 변경하지 않습니다. 프로그램 규칙의 인터넷 연결은 이전에 등록한 파일 정보에 따라 인터넷 연결을 허용합니다.
- 차단한 경우 업데이트 안 함을 선택하지 않고 차단을 선택한 경우: 기존의 프로그램 규칙에서 파일 고유 정보를 업데이트하고 인터넷 연결이 모두 허용에서 모두 차단으로 변경됩니다.

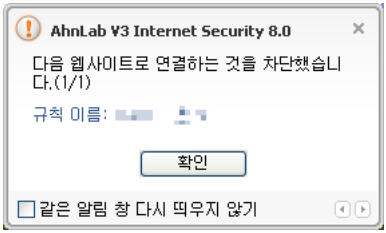
피싱 사이트 차단 알림

피싱으로 알려진 사이트에 접속하려고 할 때 차단한 웹사이트 이름과 차단 사실을 알려줍니다.



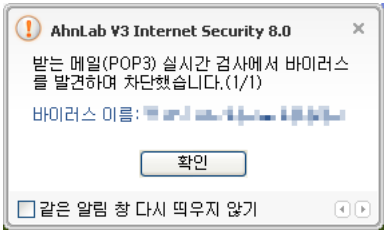
웹사이트 필터링 알림

웹사이트 필터링 규칙에서 차단 웹사이트로 등록된 사이트에 접속하려고 하면 알려줍니다.



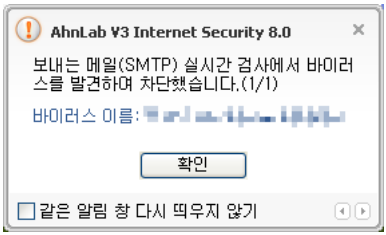
감염된 메일이 들어올 때 알림(POP3)

POP3를 통해 받는 메일이 바이러스에 감염된 경우 알려줍니다.



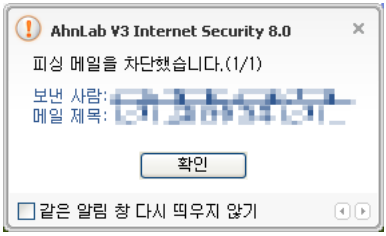
감염된 메일이 나갈 때 알림(SMTP)

SMTP를 통해 보내는 메일이 감염되었을 때 알려줍니다.



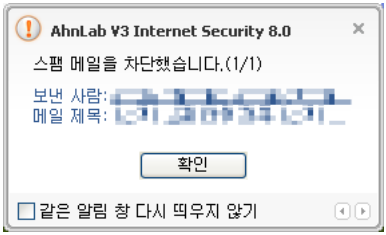
피싱 메일을 차단했을 때 알림

피싱 메일을 차단했을 때 알려주며 알림 창에서는 피싱 메일을 보낸 사람과 메일 제목을 확인할 수 있습니다.



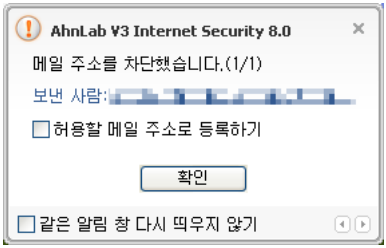
스팸 메일을 차단했을 때 알림

스팸 메일 차단 규칙에 정의된 스팸 키워드를 메일의 제목이나 본문에 포함하고 있는 경우 차단합니다. 알림 창에서는 스팸 메일을 보낸 사람의 메일 주소와 메일 제목을 확인할 수 있습니다.



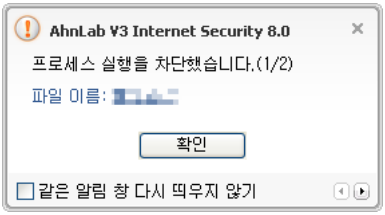
차단 목록에 등록된 메일 주소를 차단할 때 알림

차단 목록에 등록된 메일 주소에서 보낸 메일을 받으려고 할 때 알려줍니다. 알림 창에서는 보낸 사람의 메일 주소를 확인할 수 있으며 메일을 허용하고 싶으면 **허용할 메일 주소로 등록하기**를 선택하면 허용 메일 주소로 등록됩니다.



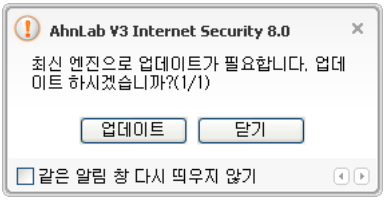
프로세스 실행 차단 알림

사용자가 선택한 폴더나 파일의 실행을 차단했을 때 차단 내용을 알려줍니다.



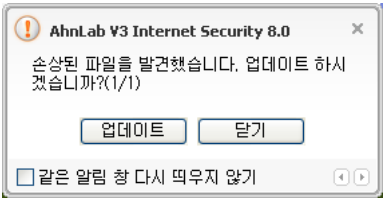
업데이트가 필요할 때 알림

현재 사용하고 있는 엔진 파일이 7일 이상 지난 경우에 알려줍니다. 업데이트를 누르면 최신 엔진을 다운로드합니다.



손상된 파일이 있을 때 알림(무결성 검사)

컴퓨터를 시작할 때 V3 IS 8.0 관련 파일의 손상 여부를 확인하고 손상된 파일이 있는 경우 알려줍니다. 파일이 손상된 경우 업데이트를 실행해야 합니다.



온라인 도움말 사용

V3 IS 8.0 온라인 도움말은 제품의 기능을 설명합니다. 제품 사용법에 대해 궁금한 점이 있으면 온라인 도움말을 확인하십시오.

온라인 도움말 보기

1 바탕 화면의 V3 IS 8.0 아이콘( )을 더블 클릭합니다.

2 HOME의 오른쪽 위에 있는 도움말을 누르고 **도움말**을 선택합니다.

- 도움말: AhnLab V3 Internet Security 8.0 온라인 도움말을 엽니다.
- (주)안철수연구소 홈페이지: (주)안철수연구소의 홈페이지를 엽니다.
- 최신 바이러스 정보: 최신 바이러스 정보를 확인할 수 있는 웹페이지를 엽니다.
- 최신 스파이웨어 정보: 최신 스파이웨어 정보를 확인할 수 있는 웹페이지를 엽니다.
- V3 파일 무결성 검사: V3 IS 8.0 프로그램 자체의 손상된 파일이나 감염된 파일이 없는지 확인합니다.
- 온라인 제품 등록: 온라인으로 제품을 등록할 수 있는 웹페이지를 엽니다.
- 제품 정보: AhnLab V3 Internet Security 8.0의 제품 정보를 확인할 수 있습니다.

3 도움말이 나타납니다.

현재 화면의 도움말 보기

현재 사용하고 있는 화면의 오른쪽 위에 있는 도움말을 누르면 해당 화면의 도움말을 확인할 수 있습니다.

참고

키보드에서 F1 키를 누르면 도움말을 볼 수 있습니다.

악성코드 예방법

악성코드라고 불리는 컴퓨터 바이러스와 스파이웨어는 사용자 몰래 자신을 실행하여 사용자가 원하지 않는 결과를 초래한다는 공통점이 있습니다. 컴퓨터 바이러스는 컴퓨터 프로그램이나 실행 가능한 부분을 변형하여 여기에 바이러스 자신 또는 자신의 변형을 복사하는 명령어의 조합으로 사용자 몰래 스스로 복제하는 프로그램입니다. 바이러스는 자기 복제를 위해 실행 가능한 파일(예: .exe, .com, .dll 등)에 바이러스 코드를 삽입하여 프로그램이 실행될 때마다 자신을 실행합니다. 스파이웨어는 사용자의 허락을 받지 않거나 사용자의 정확한 이해없이 설치되어 컴퓨터에 저장된 개인 정보를 수집하고 유출하는 프로그램입니다. 스파이웨어는 사용자가 방문한 웹사이트의 목록부터 사용자의 이름이나 ID, 비밀번호와 같은 아주 중요한 개인 정보까지 다양한 정보를 수집합니다. 수집한 정보는 일반적으로 마케팅 자료로 사용하지만 ID나 비밀번호를 이용하여 개인 정보를 도용할 위험도 있습니다. 특정한 광고를 보는 것을 조건으로 일반인에게 무료로 배포하는 프로그램인 애드웨어도 중요한 개인 정보를 사용자의 동의없이 수집하는 경우가 있어 스파이웨어에 포함하기도 합니다. V3 IS 8.0은 기존의 바이러스 검사와 스파이웨어 검사를 기능적으로 완벽히 통합하여 바이러스 따로 스파이웨어 따로 검사하는 불편을 최소화하였습니다. 악성코드 검사는 백신 프로그램을 사용하여 사용자 컴퓨터에 감염된 파일이나 사용자가 원하지 않거나 유해 가능성이 있는 프로그램을 찾아내어 컴퓨터를 치료하고 보호하기 위한 검사입니다. 악성코드를 발견하면 V3 IS 8.0의 기본 설정에 의해 치료하거나 삭제, 검역소에 격리 보관합니다. 따라서, 악성코드 진단/치료를 위해 항상 최신 엔진 업데이트 파일을 사용해야 합니다.

악성코드 예방법

- ❖ PC 검사를 정기적으로 실행하고 PC 실시간 검사를 항상 실행해 놓으십시오.
- ❖ 네트워크 침입 탐지 기능을 항상 실행하여 웜이나 트로이목마가 설치되는 것을 예방하십시오.
- ❖ 개인 방화벽을 항상 실행하여 컴퓨터에 허가받지 않은 접근을 차단하십시오.
- ❖ Microsoft Windows 업데이트를 정기적으로 실행하여 사용하고 있는 운영체제의 보안 상태를 항상 최신으로 유지하십시오.
- ❖ 출처가 확실하지 않거나 믿을 수 없는 웹사이트에서는 실행 가능한 파일을 다운로드하지 마십시오.
- ❖ 출처가 확실하지 않거나 의심스러운 메일의 첨부 파일을 열지 말고 삭제하십시오.

❖ P2P(Peer-to-Peer) 파일 공유 프로그램을 사용하지 않습니다. 파일 공유 프로그램을 설치할 때 스파이웨어와 같은 악성코드가 함께 설치되는 경우가 많습니다.

❖ 스팸 메일을 열어 보지 않습니다. 스팸 메일은 사용자가 스파이웨어와 같은 악성코드를 다운로드하도록 유도합니다.

❖ 의심스러운 프로그램은 설치하지 않습니다. 프로그램을 설치할 때에는 사용권 계약을 모두 읽고 조건에 동의하는 경우에만 설치합니다.

❖ 요청하지 않은 ActiveX 콘트롤의 설치 허가 요구는 거부합니다.

악성코드의 차이점

악성코드로 대표되는 컴퓨터 바이러스, 웜, 트로이목마 프로그램은 크게 자기 복사 능력과 정상적인 프로그램에 기생하여 다른 프로그램을 감염시키는가에 따라 다음과 같이 구분합니다.

	컴퓨터 바이러스	웜	트로이목마 프로그램
자기 복사	O	O	X
다른 프로그램에 붙음	O	X	X
부작용	있을 수도 있고, 없을 수도 있음	있을 수도 있고, 없을 수도 있음	있음

일반적으로 컴퓨터 바이러스는 자기 복사 능력이 있고, 단독 파일로 실행되지 않으며, 정상적인 다른 파일에 붙어서 감염을 확산시키는 특징을 가진 악성코드를 말합니다. 인터넷의 대중화로 급속도로 확산된 웜은 자기 복사 능력은 있지만, 다른 프로그램의 도움 없이 웜 프로그램 자체적으로 실행되는 특징이 있습니다.

컴퓨터 바이러스와 웜은 종류에 따라 감염에 따른 부작용이 나타날 수도 있고 나타나지 않을 수도 있지만 최근에 발견되는 악성코드는 대부분 부작용을 동반합니다. 트로이목마 프로그램은 자기 복사 능력도 없고 다른 프로그램에 붙어서 실행되지 않는 단독 프로그램으로 제작된 목적이 사용자 컴퓨터에 부작용을 유발하기 위해 만들어진 악성코드입니다.

4장
HOME

전체 보안 설정

전체 보안 설정에서는 악성코드와 네트워크를 통한 각종 침입을 실시간 자동 차단할 수 있는 기능을 제공합니다. 전체 보안 설정에서 제공하는 보안 기능을 사용하면 사용자 PC에 접근하는 악성코드와 네트워크를 통한 침입을 차단하므로 악성코드로 인한 PC 감염 위험을 최소화할 수 있으며 보다 안전하게 인터넷을 이용할 수 있습니다. 전체 보안 설정에서 선택한 보안 기능이 동작하고 있으면 악성코드나 외부의 침입이 있는 경우 사용자에게 알림 창으로 해당 내용을 알려줍니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **HOME**의 실시간 검사 설정의 상태 값 중 **모두 사용 중, 일부 사용 중, 사용 안 함**을 누릅니다.

3 <전체 보안 설정>이 나타납니다. PC 검사, 네트워크 보안, 웹 보안, 메일 보안에서 필요한 보안 기능을 선택합니다.

- PC 실시간 검사: 사용자 PC에서 복사, 이동, 실행, 저장되는 파일을 검사하여 해당 파일이 바이러스와 스파이웨어와 같은 악성코드에 감염되었는지 검사합니다. 감염된 파일은 PC 실시간 검사에서 설정한 치료 방법에 따라 처리합니다.
- 메신저 실시간 검사: V3 IS 8.0에서 지원하는 메신저를 통해 받은 파일에 대해 악성코드 감염 여부를 검사하고 치료합니다. 감염된 파일은 메신저 실시간 검사에서 설정한 치료 방법에 따라 처리합니다.
- USB 드라이브 검사: USB 미디어에 저장된 파일의 감염 여부를 검사합니다. USB 드라이브에 USB 미디어를 연결하여 인식하는 순간 저장된 파일의 감염 여부를 검사합니다.
- V3 자체 보호: 악성코드가 V3 IS 8.0에 관련된 파일이나 레지스트리 변경을 차단합니다. V3 자체 보호는 악성코드로 인한 V3 IS 8.0 관련 정보의 변형을 차단함으로써 V3 감염으로 인한 피해를 차단할 수 있습니다.
- 네트워크 침입 차단: 인터넷과 같은 네트워크를 이용하여 사용자 PC에 접근하는 웜이나 트로이목마 같은 해킹 프로그램의 침입을 차단합니다.
- 개인 방화벽: 설정된 개인 방화벽 규칙에 따라 인터넷 연결을 허용하거나 차단합니다.

- 피싱 사이트 차단: V3 IS 8.0의 피싱 규칙 정보에 따라 사용자가 접속하는 사이트가 피싱 사이트인지 판단합니다. 피싱 사이트인 경우 해당 웹사이트 접근을 차단합니다.
- 웹사이트 필터링: 필터링할 웹사이트 목록에 등록한 웹사이트에 접속하면 접속을 차단하고 웹사이트 차단 페이지가 나타납니다.
- 받는 메일 검사: POP3를 통해 받는 메일의 악성코드 감염 여부를 검사합니다.
- 보내는 메일 검사: SMTP를 통해 보내는 메일의 악성코드 감염 여부를 검사합니다.
- 피싱 메일 차단: V3 IS 8.0의 피싱 규칙 정보에 따라 피싱 메일 여부를 판단하고 피싱 메일인 경우 차단합니다.
- 스팸 메일 차단: 스팸 차단 규칙에 등록한 키워드를 메일의 제목이나 본문에 포함한 메일이 있는 경우 차단합니다.

4 **모두 선택**을 누르면 보안 기능을 모두 선택하고, **모두 취소**를 누르면 선택한 보안 기능을 모두 선택하지 않습니다.

5 **확인**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

빠른 검사

빠른 검사를 사용하면 바이러스와 스파이웨어를 하나의 검사 창에서 검사할 수 있으며, 중요한 시스템 폴더에서 감염 확률이 높은 파일과 스파이웨어 감염 위험이 높은 영역을 검사하고 치료할 수 있습니다. 바이러스와 스파이웨어를 하나의 검사 창에서 검사하면 컴퓨터에 감염된 악성코드를 빠르게 검사하고 발견한 악성코드 또한 하나의 검사 창에서 손쉽게 치료할 수 있습니다. 빠른 검사에서 발견한 바이러스나 스파이웨어는 PC 검사 설정에서 사용자가 선택한 치료 방법에 따라 치료합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **HOME**의 **빠른 검사**를 누릅니다.

3 <PC 검사/치료>에서 사용자 컴퓨터의 바이러스와 스파이웨어를 검사합니다.

- 검사 폴더: 현재 검사하고 있는 파일의 경로명을 보여줍니다. 스파이웨어 감염 위험이 높은 영역을 검사할 때는 현재 검사하고 있는 스파이웨어의 이름을 보여줍니다.

참고

빠른 검사는 레지스트리 영역, Windows 설치 경로, Program Files 경로, V3 IS 8.0 설치 경로와 스파이웨어 감염 위험이 높은 영역을 검사합니다.

- 검사 파일: 현재 검사하고 있는 경로에서 검사하고 있는 파일 이름을 보여줍니다.
- 일시 중지: 검사가 진행되는 중에 검사를 잠시 멈추려고 할 때 사용합니다. 일시 중지를 누르면 검사를 잠시 멈춥니다.
- 다시 시작: 일시 중지를 누른 경우에 나타납니다. 일시 중지된 검사를 다시 시작하려고 할 때 선택합니다.
- 멈춤: 현재 실행 중인 검사를 끝내려고 할 때 선택합니다. 멈춤을 선택하면, **PC 검사를 멈추시겠습니까?** 라는 창이 나타납니다. 검사를 멈추려면 **예**를 누르고, 계속하려면 **아니오**를 누릅니다.
- 감염 수: 바이러스에 감염된 파일, 메모리, 주 부트 영역, 도스 부트 영역, 실행 프로세스, 레지스트리와 스파이웨어에 감염된 파일과, 레지스트리의 전체 감염 개수를 합쳐서 보여 줍니다.
- 치료 수: 치료한 바이러스 및 스파이웨어의 개수를 합쳐서 보여줍니다.

- 보고서 보기: 검사 영역별로 검사한 개수, 감염된 개수, 치료 수를 요약하여 보여줍니다.
- 이름: 바이러스나 스파이웨어의 이름을 보여줍니다.
- 상태: 감염된 파일의 치료 가능 여부를 표시합니다.
  - 치료 가능: 현재 버전에서 치료 가능한 바이러스에 감염되었으므로 치료하기를 눌러 치료할 수 있습니다.
  - 치료 예정: 현재 버전에서 치료할 수 없는 바이러스에 감염되었으므로 감염된 파일을 (주)안철수연구소로 보내거나 새로운 엔진으로 업데이트한 후에 치료할 수 있습니다.
- 파일 경로: 감염된 파일이 실제 위치하고 있는 경로를 보여줍니다.
- 악성코드가 발견되지 않으면 검사 창 그대로 두기: 악성코드 검사를 끝낸 후에 발견된 악성코드가 없는 경우 현재 보고 있는 검사 창을 닫지 않고 그대로 둡니다.
- 악성코드가 발견되지 않으면 검사 창 닫기: 악성코드 검사를 끝낸 후에 발견된 악성코드가 없는 경우 현재 보고 있는 검사 창을 닫습니다.
- 악성코드가 발견되지 않으면 컴퓨터 자동으로 끄기: 악성코드 검사를 끝낸 후에 발견된 악성코드가 없는 경우 컴퓨터를 자동으로 종료합니다. 검사 결과 바이러스나 스파이웨어가 발견되지 않으면 컴퓨터를 종료하는 기능으로 검사 시간이 오래 걸리는 경우 검사를 실행하고, 장시간 자리를 비우거나 더 이상 컴퓨터를 사용하지 않는 경우에 활용하면 편리합니다.
- 치료하기: 검사가 끝나면 치료하기 버튼이 나타납니다. 검사 창에 발견된 악성코드가 있다면 감염된 파일을 선택하고 치료하기를 눌러 악성코드를 제거할 수 있습니다.
- 닫기: 검사를 진행하는 동안은 닫기 버튼으로 나타납니다. 닫기를 누르면 현재의 검사를 중지하고 검사 창을 닫습니다.
- 마침: 검사를 모두 마치면, 닫기 버튼이 마침으로 변경됩니다. 마침을 누르면 현재의 검사 창을 닫습니다.

PC 최적화

PC 최적화를 실행하면 필요없는 파일과 레지스트리 정보, 임시 파일을 청소하고 메모리 사용을 최적화합니다. PC 최적화는 하드 디스크 드라이브의 저장 공간을 차지하는 필요 없는 파일이나 임시 파일, 필요없는 레지스트리 정보를 청소하고 메모리 사용을 최적화하여 컴퓨터의 실행 속도를 빠르게 합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **HOME**에서 **PC 최적화**를 누릅니다.

참고

PC 도구의 PC 최적화에서 실행하기를 눌러도 PC 최적화를 실행할 수 있습니다.

3 <PC 최적화>에서 **최적화 항목**과 **진행 상태**를 보여줍니다.

4 PC 최적화를 마치면 **닫기**를 누릅니다.

참고

PC 최적화 항목은 PC 최적화 설정에서 선택할 수 있습니다.

업데이트와 설정

V3 IS 8.0을 설치하면 가장 먼저 엔진 업데이트를 실행해야 합니다. 매일 새로 발견되는 악성코드와 네트워크를 통한 보안 위협을 차단하기 위해서는 백신 프로그램을 설치하고 엔진 업데이트를 주기적으로 실행하는 것이 가장 중요합니다.

업데이트하기

사용자가 직접 업데이트를 실행하여 최신 엔진을 다운로드하는 방법입니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 HOME의 오른쪽 위에 있는 **업데이트**를 누릅니다.

3 **업데이트를 준비하고 있습니다.** 라는 메시지가 나타납니다.

4 **업데이트 파일을 다운로드하고 있습니다.** 라는 메시지가 나타나면서 파일 다운로드 상황을 알려줍니다.

5 업데이트 파일을 적용하는 화면이 나타난 후 업데이트를 마치면 창이 자동으로 사라집니다.

6 현재 엔진 버전은 HOME의 엔진 버전이나 화면 오른쪽 위의 도움말의 제품 정보, 작업 표시줄의 V3 알림 아이콘()에 마우스를 위치하면 현재 엔진 버전을 볼 수 있습니다.

참고

작업 표시줄의 아이콘()에서 마우스 오른쪽을 눌러 **업데이트**를 선택해도 최신 엔진을 다운로드할 수 있습니다.

업데이트 설정

업데이트 설정에서는 하루에도 몇 번씩 업데이트를 해야 하는 번거로움을 줄이기 위해 자동 업데이트 주기를 선택하거나 정해진 시간에 엔진 업데이트를 실행할 수 있도록 예약할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **HOME**에서 **환경 설정**을누릅니다.

3 <환경 설정>의 **업데이트 설정**을 누릅니다.

4 **업데이트 방법**을 설정합니다.

- 자동 업데이트 사용(권장): PC를 부팅한 후 5분~30분 사이에 업데이트 서버에 접속하여 업데이트 여부를 확인합니다. 부팅 이후에는 예약한 시간과 관계없이 자동 업데이트 주기의 주기에 따라 업데이트 여부를 확인하여 업데이트합니다.
- 자동 업데이트 주기: 지정한 시간마다 업데이트 서버를 검사하여 업데이트를 실행합니다. 자동 업데이트 주기는 1시간 부터 24시간까지 숫자로 설정할 수 있으며, 기본 값은 3시간입니다.
- 예약 업데이트 사용: 일정한 주기와 시간을 설정하여 예약한 시간에 업데이트를 자동으로 실행합니다. 시스템을 시작할 때나 매일, 매주, 매월 단위로 지정한 날짜와 시간에 업데이트를 실행하도록 예약할 수 있습니다.
  - 매일: 매일 지정한 시간에 업데이트를 실행합니다.
  - 매주: 매주 지정한 요일과 시간에 업데이트를 실행합니다.
  - 매월: 매월 지정한 날짜와 시간에 업데이트를 실행합니다.
  - 한 번만 지정한 날짜와 시간에 업데이트를 한 번만 실행합니다.

5 **프록시 서버 설정**을 설정합니다.

- 프록시 서버 사용: 프록시 서버를 통해 인터넷에 연결할 때 선택합니다.
  - 서버 주소: 프록시 서버의 주소를 입력합니다.
  - 포트 번호: 프록시 서버에서 사용하는 포트 번호를 입력합니다.

⚠ 주의

프록시 서버의 주소를 입력할 때에는 "http://"를 제외한 주소를 입력하십시오.

6 **고급 설정**을 설정합니다.

- 업데이트할 때 패치 파일 다운로드: 최신 엔진을 업데이트할 때 V3 IS 8.0의 변경 사항이 반영된 패치 파일을 다운로드합니다.
- 업데이트 정보 보기: 업데이트를 마친 다음 업데이트 정보를 보여줍니다. 업데이트한 제품과 엔진에 대한 정보를 확인할 수 있습니다.
- 업데이트 무결성 검사: 다운로드한 업데이트 파일의 손상 여부나 감염 여부를 검사합니다.

7 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0 설정된 기본 값을 적용합니다. 기본 값은 자동 업데이트 사용, 자동 업데이트 주기 3시간, 업데이트할 때 패치 파일 다운로드, 무결성 검사입니다.
- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

5장
PC 검사

정밀 검사

정밀 검사는 사용자가 검사할 폴더나 파일을 직접 선택하거나 사용자 컴퓨터 전체를 선택하여 바이러스와 스파이웨어를 검사할 수 있습니다. 정밀 검사는 사용자가 선택한 폴더나 파일을 검사하므로 실시간 검사와 달리 백신 프로그램이 설치되기 이전에 감염된 파일을 검사할 수 있는 장점이 있지만, 선택한 파일의 개수와 종류에 따라 검사 시의 컴퓨터 속도가 달라질 수도 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**의 **정밀 검사**를 선택합니다.

3 검사 대상 목록에서 검사할 폴더나 파일을 선택합니다.

4 **검사하기**를 누릅니다.

5 <PC 검사/치료>에서 사용자 컴퓨터의 바이러스와 스파이웨어를 검사합니다.

참고

폴더를 선택하면, 해당 폴더의 모든 파일과 하위 폴더의 모든 파일까지 검사합니다.

- 검사 폴더: 현재 검사하고 있는 파일의 경로명을 보여줍니다. 스파이웨어 감염 위험이 높은 영역을 검사할 때는 현재 검사하고 있는 스파이웨어의 이름을 보여줍니다.
- 검사 파일: 현재 검사하고 있는 경로에서 검사하고 있는 파일 이름을 보여줍니다.
- 일시 중지: 검사가 진행되는 중에 검사를 잠시 멈추려고 할 때 사용합니다. 일시 중지를 누르면 검사를 잠시 멈춥니다.
- 다시 시작: 일시 중지를 누른 경우에 나타납니다. 일시 중지된 검사를 다시 시작하려고 할 때 선택합니다.
- 멈춤: 현재 실행 중인 검사를 끝내려고 할 때 선택합니다. 멈춤을 선택하면, **PC 검사를 멈추시겠습니까?** 라는 창이 나타납니다. 검사를 멈추려면 **예**를 누르고, 계속하려면 **아니오**를 누릅니다.
- 감염 수: 바이러스에 감염된 파일, 메모리, 주 부트 영역, 도스 부트 영역, 실행 프로세스, 레지스트리와 스파이웨어에 감염된 파일과, 레지스트리의 전체 감염 개수를 합쳐서 보여 줍니다.

- 치료 수: 치료한 바이러스 및 스파이웨어의 개수를 합쳐서 보여줍니다.
- 보고서 보기: 검사 영역별로 검사한 개수, 감염된 개수, 치료 수를 요약하여 보여줍니다.
- 이름: 바이러스나 스파이웨어의 이름을 보여줍니다.
- 상태: 감염된 파일의 치료 가능 여부를 표시합니다.
  - 치료 가능: 현재 버전에서 치료 가능한 바이러스에 감염되었으므로 치료하기를 눌러 치료할 수 있습니다.
  - 치료 예정: 현재 버전에서 치료할 수 없는 바이러스에 감염되었으므로 감염된 파일을 (주)안철수연구소로 보내거나 새로운 엔진으로 업데이트한 후에 치료할 수 있습니다.
- 파일 경로: 감염된 파일이 실제 위치하고 있는 경로를 보여줍니다.
- 악성코드가 발견되지 않으면 검사 창 그대로 두기: 악성코드 검사를 끝낸 후에 발견된 악성코드가 없는 경우 현재 보고 있는 검사 창을 닫지 않고 그대로 둡니다.
- 악성코드가 발견되지 않으면 검사 창 닫기: 악성코드 검사를 끝낸 후에 발견된 악성코드가 없는 경우 현재 보고 있는 검사 창을 닫습니다.
- 악성코드가 발견되지 않으면 컴퓨터 자동으로 끄기: 악성코드 검사를 끝낸 후에 발견된 악성코드가 없는 경우 컴퓨터를 자동으로 종료합니다. 검사 결과 바이러스나 스파이웨어가 발견되지 않으면 컴퓨터를 종료하는 기능으로 검사 시간이 오래 걸리는 경우 검사를 실행하고, 장시간 자리를 비우거나 더 이상 컴퓨터를 사용하지 않는 경우에 활용하면 편리합니다.
- 치료하기: 검사가 끝나면 치료하기 버튼이 나타납니다. 검사 창에 발견된 악성코드가 있다면 감염된 파일을 선택하고 치료하기를 눌러 악성코드를 제거할 수 있습니다.
- 닫기: 검사를 진행하는 동안은 닫기 버튼으로 나타납니다. 닫기를 누르면 현재의 검사를 중지하고 검사 창을 닫습니다.
- 마침: 검사를 모두 마치면, 닫기 버튼이 마침으로 변경됩니다. 마침을 누르면 현재의 검사 창을 닫습니다.

사용자 목록 검사

사용자 목록 검사는 사용자가 검사할 폴더를 선택하여 검사 목록에 추가한 후 필요할 때 사용자 검사 목록을 선택하여 검사하고 치료할 수 있는 기능입니다. 사용자 목록 검사는 다운로드하는 파일을 저장하는 폴더나 공유 폴더, 파일 변경이 잦은 프로그램 폴더 등을 추가하여 필요할 때 검사하면 악성코드 감염으로 인한 피해를 빠르고 간단하게 검사할 수 있습니다.

사용자 검사 목록 추가

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**의 **사용자 목록 검사**를 선택합니다.

3 **추가**를 누릅니다.

4 <사용자 검사 목록 추가/수정>이 나타납니다.

- 검사 이름: 사용자 검사 목록에 추가하려는 검사 대상을 구분할 수 있는 이름을 입력합니다. 검사 이름은 한글, 영문, 숫자, 특수 문자 모두 입력 가능하며 1~30 글자 사이에서 입력할 수 있습니다.
- 검사 대상 선택: 검사할 폴더를 선택합니다. 상위 폴더를 선택하면, 해당 폴더의 하위 폴더까지 모두 검사 대상으로 선택됩니다.

5 **확인**을 누릅니다.

6 검사 목록에 입력한 검사 이름이 등록되었는지 확인합니다.

사용자 검사 목록 수정

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**의 **사용자 목록 검사**를 선택합니다.

3 검사 목록에서 수정할 **검사 이름**을 선택합니다.

4 **수정**을 누릅니다.

5 <사용자 검사 목록 추가/수정>이 나타납니다. **검사 이름**이나 **검사 대상**을 변경합니다.

6 **확인**을 누릅니다.

7 수정한 내용이 검사 목록에 반영되었는지 확인합니다.

사용자 검사 목록 삭제

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**의 **사용자 목록 검사**를 선택합니다.

3 검사 목록에서 삭제할 **검사 이름**을 선택합니다.

4 **삭제**를 누릅니다.

5 삭제한 내용이 검사 목록에서 지워졌는지 확인합니다.

사용자 목록 검사하기

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**의 **사용자 목록 검사**를 선택합니다.

3 사용자 검사 목록에서 검사할 이름을 선택합니다.

4 **검사하기**를 누릅니다.

5 <PC 검사/치료>에서 사용자 목록을 검사합니다. 감염된 파일이 있는 경우 PC 검사 설정의 옵션에 따라 치료합니다.

USB 드라이브 검사

USB 미디어에 저장된 파일의 감염 여부를 검사할 수 있습니다. 환경 설정에서 USB 드라이브 검사 옵션을 선택해 두면, USB 드라이브에 USB 미디어를 연결하여 인식하는 순간 저장된 파일의 감염 여부를 확인할 수 있습니다.

USB 드라이브 검사 설정하기

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 환경 설정의 **PC 검사 설정**을 누릅니다.

3 **PC 검사** 탭을 선택합니다.

4 PC 검사의 고급 설정에서 **USB 드라이브 검사**를 선택합니다.

참고
전체 보안 설정에서도 USB 드라이브 검사를 선택할 수 있습니다.

5 **적용**을 누릅니다.

6 **확인**을 누릅니다.

USB 드라이브 검사하기

1 USB 드라이브에 USB 미디어를 연결합니다.

2 사용자 PC에서 USB 드라이브를 인식하는 과정이 나타납니다.

3 <PC 검사/치료>에서 USB 미디어에 저장된 폴더와 파일을 검사합니다. 감염된 파일이 있는 경우 PC 검사 설정의 옵션에 따라 치료합니다.

참고
USB 드라이브 검사를 사용하려면 사용자가 Windows에 로그인 상태여야 합니다. 로그인 상태가 아닌 경우 USB 드라이브 검사를 실행하지 않습니다. 로그인 상태 이전에 연결한 USB 미디어에 대해서는 USB 드라이브 검사가 자동으로 실행되지 않습니다. 이런 경우, 사용자가 직접 정밀 검사나 사용자 목록 검사, 탐색기 검사에서 USB 드라이브를 선택한 후 검사해야 합니다.

참고

USB 드라이브 검사를 진행하는 도중에 USB 미디어를 제거해도 별도의 오류 창은 발생하지 않고 검사를 마칩니다.

참고

사용설명서에서 말하는 USB 미디어란 USB 드라이브에 연결할 수 있는 모든 매체를 지칭합니다.

실시간 검사

PC 실시간 검사와 메신저 실시간 검사를 사용하면 악성코드에 감염된 파일을 실행, 복사하거나 메신저를 통해 감염된 파일을 받는 경우에 감염 여부를 사용자에게 즉시 알려줍니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 PC 실시간 검사 설정에서 **PC 실시간 검사 사용**을 선택하고 검사 설정을 설정합니다.

참고

메신저 실시간 검사는 메신저 실시간 검사 설정에서 **메신저 실시간 검사 사용**을 선택하고 검사 설정을 설정합니다.

3 PC 실시간 검사나 메신저 실시간 검사가 작동 중인 상태에서 파일을 실행하거나 복사, 다운로드할 때 악성코드에 감염된 파일을 발견하면 악성코드 발견 창이 나타납니다.

- 발견한 악성코드 수: PC 실시간 검사나 메신저 실시간 검사가 발견한 악성코드의 개수를 보여줍니다.
- 악성코드 이름: 감염된 바이러스나 스파이웨어의 이름을 보여줍니다.
- 상태: 감염된 파일의 치료 가능 여부를 보여줍니다.
- 감염된 파일 경로: 감염된 파일이 실제 위치하고 있는 경로를 보여줍니다.
- 다음부터 자동 치료하기: PC 실시간 검사나 메신저 실시간 검사가 악성코드를 발견한 경우 자동으로 치료합니다.
- 치료하기: 현재 발견된 악성코드를 치료합니다.
- 닫기: 악성코드 감염 발견 창을 닫습니다.

탐색기 검사

윈도우 탐색기에서 마우스 오른쪽 버튼을 눌러 사용자가 선택한 폴더나 파일을 간단하게 검사할 수 있습니다.

탐색기 검사 설정하기

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 환경 설정의 **기타 설정**에서 **탐색기 설정**을 누릅니다.

3 **Windows 탐색기 메뉴 사용**을 선택합니다. Windows 탐색기 메뉴 사용을 선택하면, PC 검사와 파일 완전 삭제를 선택할 수 있습니다.

- PC 검사: 탐색기에서 사용자가 선택한 드라이브, 폴더, 파일에 대한 악성코드 감염 여부를 검사합니다. 탐색기에서 대상을 선택하고 마우스 오른쪽을 누르면 **V3 PC 검사**로 나타납니다.
- 파일 완전 삭제: 탐색기에서 사용자가 선택한 폴더나 파일을 완전 삭제합니다. 탐색기에서 대상을 선택하고 마우스 오른쪽을 누르면 **V3 파일 완전 삭제**로 나타납니다.

탐색기에서 PC 검사하기

1 사용자 PC에서 검사할 폴더나 파일을 선택합니다.

2 선택한 대상에서 마우스 오른쪽을 눌러 **V3 PC 검사**를 선택합니다.

3 <PC 검사/치료>에서 선택한 폴더나 파일을 검사합니다. 감염된 파일이 있는 경우 PC 검사 설정의 옵션에 따라 치료합니다.

참고

탐색기 검사는 사용자가 선택한 폴더나 파일만을 검사하고 다른 영역은 검사하지 않습니다.

보고서 보기

보고서 보기는 검사 실행 정보를 정리해서 보여줍니다. 실행한 검사 내용에 따라 검사한 영역과 해당 영역에서 발견한 악성코드의 개수와 치료 개수를 확인할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 빠른 검사, 정밀 검사, 사용자 목록 검사, USB 드라이버 검사, 탐색기 검사 중에서 필요한 검사를 실행합니다.

3 <PC 검사/치료>에서 검사를 진행합니다. 검사를 마치고 창을 닫기 전에 **보고서 보기**를 누릅니다.

- 검사 영역: V3 IS 8.0으로 검사한 영역을 영역별로 구분하여 보여줍니다.
  - 파일: 사용자 PC에 저장된 파일을 검사합니다.
  - 메모리: 사용자 PC의 메모리를 검사합니다.
  - 주 부트 섹터: 사용자 PC의 주 부트 섹터를 검사합니다.
  - 도스 부트 섹터: 사용자 PC의 도스 부트 섹터를 검사합니다.
  - 실행 중 프로세스: 검사 당시 실행되고 있었던 프로세스를 대상으로 검사합니다.
  - 레지스트리: 사용자 PC의 레지스트리를 검사합니다.
- 검사 수: 각 영역별로 검사한 개수를 보여줍니다.
- 감염 수: 각 영역별로 감염된 개수를 보여줍니다.
- 치료 수: 각 영역별로 치료한 개수를 보여줍니다.

PC 검사 설정

PC 검사의 정밀 검사나 사용자 목록 검사를 할 때 검사할 영역이나 감염된 파일을 치료하는 방법을 설정합니다. 정밀 검사나 사용자 목록 검사는 사용자가 직접 검사 대상을 선택하여 검사하는 방식으로 사용자가 선택한 검사 대상과 PC 검사 설정에서 설정한 내용에 따라 검사합니다. PC 검사 설정은 감염 위험이 높은 영역이나 파일 확장자에 따른 검사 등 다양한 옵션을 사용자가 직접 선택하여 PC 환경에 맞는 검사를 실행할 수 있습니다. 감염된 파일을 발견한 경우 선택한 치료 방법에 따라 처리합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **설정하기**를 누릅니다.

3 **PC 검사 설정**에서 **PC 검사** 탭을 누릅니다.

4 사전 검사 대상 선택, 검사 대상 선택, 치료 방법 선택에서 필요한 옵션을 선택합니다.

5 **홈페이지 바꾸기**에서 필요한 옵션을 선택합니다.

- 홈페이지 바꾸기 사용: 악성코드를 치료한 다음 Microsoft Internet Explorer의 홈페이지를 바꿉니다. 악성코드가 Microsoft Internet Explorer의 홈페이지를 바꾸어 놓은 경우 사용자가 입력해 둔 홈페이지로 변경하는 기능으로 홈페이지 바꾸기를 선택하고 홈페이지로 설정할 웹사이트의 주소를 입력합니다.
- 빈 페이지로 설정: 홈페이지 바꾸기를 선택하고 빈 페이지로 설정을 하면 Microsoft Internet Explorer 홈페이지를 빈 페이지로 바꿉니다.

6 **고급 설정**에서 필요한 옵션을 선택합니다.

- CPU 점유율 선택: PC 검사를 할 때 평균적인 CPU 사용율을 조정합니다. 기본 값은 높음입니다. 보통과 낮음을 선택하면 높음을 선택했을때보다 평균적으로 CPU를 적게 사용합니다.
- 프로세스 우선 순위 선택: 여러 프로세스가 동시에 동작할 때 V3의 PC 검사 우선 순위를 결정합니다. 기본 값은 보통이며, 보통을 선택하면 우선 순위의 변경없이 PC 검사를 실행하고, 아주 높음이나 높음을 선택하면 보통보다 높게 PC 검사의 우선 순위를 부여합니다. 낮음이나 아주 낮음을 선택하면 PC 검사의 우선 순위를 보통보다 낮게 순위를 부여하여 다른 프로세스보다 PC 검사가 늦게 처리될 수 있습니다.

- 스파이웨어 감염 위험이 높은 영역: V3 IS 8.0이 지정한 스파이웨어 감염 위험이 높은 레지스트리와 기타 영역을 별도로 검사합니다.
- 공유 폴더 해제 후 검사: 사용자 PC에 설정되어 있는 공유 폴더의 공유를 모두 해제한 후 PC 검사를 실행합니다.
- 쉘 프로세스 멈추고 검사: 사용자 PC에 실행 중인 쉘 프로세스를 종료하고 검사를 실행합니다. PC 검사를 마치면, 종료했던 쉘 프로세스를 다시 실행합니다.

7 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

PC 실시간 검사 설정

PC 실시간 검사는 알려지거나 알려지지 않은 악성코드를 지속적으로 탐지하여 차단합니다. V3 IS 8.0 사용자는 PC 실시간 검사가 실행될 때 검사하는 파일 형식과 검사 대상, 검사 범위, 치료 방법 등을 직접 설정하여 사용자에게 맞는 실시간 검사를 실행하도록 설정할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘( )을 더블 클릭합니다.

2 **PC 검사**에서 **설정하기**를 누릅니다.

3 **PC 검사 설정**에서 **PC 실시간 검사** 탭을 누릅니다.

4 **PC 실시간 검사 사용**을 선택합니다.

- PC 실시간 검사 사용: 바이러스와 스파이웨어를 실시간으로 검사하는 실시간 검사를 실행합니다.
- PC 실시간 검사를 끝내더라도 자동으로 다시 시작: PC 실시간 검사를 실행 종료한 상태에서 사용자가 선택한 시간이나 상황에 따라 PC 실시간 검사를 자동으로 다시 시작합니다.
  - 사용 안 함: PC 실시간 검사를 자동으로 다시 시작하지 않습니다.
  - 10분 후: PC 실시간 검사를 종료하고 10분이 지나면 PC 실시간 검사를 다시 실행합니다.
  - 30분 후: PC 실시간 검사를 종료하고 30분이 지나면 PC 실시간 검사를 다시 실행합니다.
  - 1시간 후: PC 실시간 검사를 종료하고 1시간이 지나면 PC 실시간 검사를 다시 실행합니다.
  - 컴퓨터 다시 시작할 때: PC 실시간 검사를 종료하고 컴퓨터를 다시 시작하면 PC 실시간 검사를 실행합니다.

⚠ 주의

PC 실시간 검사를 사용하지 않으면, 바이러스와 스파이웨어를 실시간으로 검사하여 차단하는 실시간 검사가 작동하지 않아 악성코드의 위험에 노출될 수 있습니다.

5 검사 설정의 **사전 검사 대상 선택**에서 검사 여부를 선택합니다.

- 사전 검사 사용: PC 실시간 검사를 시작할 때 사용자가 선택한 사전 검사 영역을 검사합니다.
- 사용자 지정: 사전 검사 대상을 선택할 수 있습니다.

참고

사전 검사 대상에 대한 자세한 설명은 사전 검사 대상 선택을 참고하십시오.

6 **검사 대상 선택**을 설정합니다.

7 **검사 범위 선택**을 설정합니다.

- 플로피 디스크 부트 영역: 플로피 디스크를 사용할 때 플로피 디스크 부트 영역의 감염 여부를 먼저 검사합니다.
- 네트워크 드라이브: 사용자가 네트워크 드라이브에 있는 파일을 실행하거나 저장하는 경우에 감염 여부를 검사합니다.

8 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

예약 검사 설정

사용자 컴퓨터에 저장된 파일과 데이터를 바이러스와 스파이웨어로 부터 보호하고, 이미 감염된 상태로 저장되어 있는 파일을 검사하기 위하여 백신 프로그램을 주기적으로 사용하는 것이 좋습니다. 예약 검사를 사용하면 설정한 날짜와 시간에 자동으로 컴퓨터를 검사합니다. V3 IS 8.0의 예약 검사는 사용자의 필요에 따라 검사 예약을 할 수 있도록 다양한 기능을 제공합니다.

참고

실시간 검사는 실시간 검사가 실행된 이후에 실행되는 파일을 감시하므로 이미 감염된 파일이 사용자 컴퓨터에 저장되어 실행되지 않는다면, 감염된 파일을 찾을 수 없습니다. 정밀 검사나 예약 검사를 사용하면, 현재 실행되지 않은 감염된 파일까지 찾을 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **예약하기**를 누릅니다.

3 **예약 검사 사용**을 선택합니다.

4 예약 검사 목록에서 **추가**를 누릅니다.

5 <예약 검사 추가/수정>에서 **예약 검사 이름**을 입력합니다. 예약 검사 이름은 1~30자 까지 입력할 수 있습니다.

참고

기업이나 단체에서 AhnLab Policy Center를 사용하고 있다면, AhnLab Policy Center에서 사용자 PC에 설치된 V3 IS 8.0의 예약 검사를 설정할 수 있습니다. PC 사용자가 설정한 검사 이름과 관리자가 설정한 검사 이름이 동일한 경우 사용자가 설정한 예약 검사는 삭제되며, AhnLab Policy Center 관리자가 설정한 예약 검사를 사용자가 수정하거나 삭제할 수도 없습니다.

6 **예약 시간 설정**에서 검사할 시간을 설정합니다.

- 매일: 바이러스나 스파이웨어를 검사할 시간을 설정합니다. 설정한 시간에 자동으로 PC 검사를 실행합니다.
- 매주: 바이러스나 스파이웨어를 검사할 요일과 시간을 설정합니다. 매주 설정한 요일의 시간에 자동으로 PC 검사를 실행합니다.

- 매월: 바이러스나 스파이웨어를 검사할 날짜와 시간을 설정합니다. 매월 선택한 날짜와 시간에 PC 검사를 실행합니다.
- 한 번만: 선택한 날짜와 시간에 한 번만 PC 검사를 실행합니다.

참고

예약 검사는 동시에 2개 이상 실행되지 않습니다. 하나의 예약 검사가 실행되고 있다면, 다른 예약 검사는 실행되지 않습니다. 따라서 예약 검사를 추가할 때 검사 시간이 중복되지 않도록 하는 것이 좋습니다.

7 검사 대상 선택에서 검사할 드라이브나 폴더, 파일을 선택합니다.

참고

예약 검사는 USB 미디어와 같은 외부 저장 장치는 검사하지 않습니다. 예약 검사는 C 드라이브나 D드라이브와 같이 항상 사용자 PC에 고정 장착된 디스크만 검사합니다.

8 검사 설정에서 사전 검사 대상 선택, 검사 대상 선택, 치료 방법 선택을 설정합니다.

9 **고급 설정**에서 필요한 옵션을 선택합니다.

- CPU 점유율 선택: PC 검사를 할 때 평균적인 CPU 사용율을 조정합니다. 기본 값은 높음입니다. 보통과 낮음을 선택하면 높음을 선택했을때보다 평균적으로 CPU를 적게 사용합니다.
- 프로세스 우선 순위 선택: 여러 프로세스가 동시에 동작할 때 V3의 PC 검사 우선 순위를 결정합니다. 기본 값은 보통이며, 보통을 선택하면 우선 순위의 변경없이 PC 검사를 실행하고, 아주 높음이나 높음을 선택하면 보통보다 높게 PC 검사의 우선 순위를 부여합니다. 낮음이나 아주 낮음을 선택하면 PC 검사의 우선 순위를 보통보다 낮게 순위를 부여하여 다른 프로세스보다 PC 검사가 늦게 처리될 수 있습니다.
- 스파이웨어 감염 위험이 높은 영역 검사: V3 IS 8.0이 지정한 스파이웨어 감염 위험이 높은 레지스트리와 기타 영역을 별도로 검사합니다.

10 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

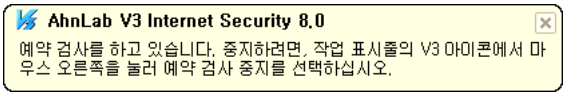
참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

예약 검사를 실행하는 경우

설정된 예약 검사를 실행하는 경우 작업 표시줄의 V3 알림 아이콘( )에 다음과 같은 풍선 도움말이 나타납니다.



메신저 실시간 검사 설정

메신저를 통해 받는 파일의 악성코드 감염 여부를 실시간으로 검사합니다. 메신저 사용이 보편화 되어 있어 대화 중에 받는 파일은 무심코 다운로드하지 않아야 합니다. 대화 상대에게 해당 파일을 보냈는지를 먼저 확인하고 해당 파일을 다운로드하는 것이 안전합니다. 또한, 대화 상대가 보낸 파일이라 하더라도 감염 여부는 확인할 수 없으므로 메신저 실시간 검사를 항상 실행하여 메신저를 통해 악성코드에 쉽게 노출되지 않도록 주의해야 합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **설정하기**를 누릅니다.

3 **PC 검사 설정**에서 **메신저 실시간 검사** 탭을 누릅니다.

4 **메신저 실시간 검사 사용**을 선택합니다.

- 메신저 실시간 검사를 끝내더라도 자동으로 다시 시작: 메신저 실시간 검사를 실행 종료한 상태에서 사용자가 선택한 시간이나 상황에 따라 메신저 실시간 검사를 자동으로 다시 시작합니다.
  - 사용 안 함: 메신저 실시간 검사를 자동으로 다시 시작하지 않습니다.
  - 10분 후: 메신저 실시간 검사를 종료하고 10분이 지나면 메신저 실시간 검사를 다시 실행합니다.
  - 30분 후: 메신저 실시간 검사를 종료하고 30분이 지나면 메신저 실시간 검사를 다시 실행합니다.
  - 1시간 후: 메신저 실시간 검사를 종료하고 1시간이 지나면 메신저 실시간 검사를 다시 실행합니다.
  - 컴퓨터 다시 시작할 때: 메신저 실시간 검사를 종료하고 컴퓨터를 다시 시작하면 메신저 실시간 검사를 실행합니다.

5 **검사 대상 메신저 선택**에서 메신저 실시간 검사를 적용할 메신저를 선택합니다. 검사 대상 메신저는 **MSN 메신저, 네이트온 메신저, 다음 메신저, 야후! 메신저, AOL 메신저, Windows 메신저, ICQ Lite 메신저, IP 메신저**입니다.

참고

검사 대상 메신저 중 사용자가 선택한 메신저를 통해 받는 파일의 감염 여부를 검사합니다. 사용자가 선택한 메신저를 통해 받는 파일 중 메신저 실시간 검사의 검사 설정에서 선택한 검사 대상에 따라 검사하고 감염된 파일이 있는 경우 치료 방법 선택에서 선택한 방법에 따라 치료합니다.

6 검사 설정의 검사 대상 선택, 치료 방법 선택을 설정합니다.

7 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

고급 설정

고급 설정에서는 은폐된 악성코드를 진단 치료하는 TrueFind(은폐진단)와 악성 ActiveX 콘트롤 설치 차단, V3 IS 8.0 자체 보호 기능 등을 설정할 수 있습니다. 또한, PC 검사 시에 사용자가 지정한 영역은 검사를 하지 않도록 하는 검사 예외 영역과 허용할 악성코드 이름을 설정할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **환경 설정**을 선택합니다.

3 PC 검사에서 **고급 설정**을 선택합니다.

4 필요한 옵션을 선택합니다.

- TrueFind(은폐진단) 사용: 악성코드가 자신의 정보를 사용자가 발견할 수 없도록 은폐했을 때 V3 IS 8.0이 탐지하는 기능입니다. 은폐된 악성코드에 감염된 파일은 컴퓨터를 다시 시작할 때 치료합니다. TrueFind(은폐진단)는 사전 검사 영역의 프로세스나 레지스트리, PC 검사와 예약 검사에서 파일을 검사할 때 은폐된 악성코드에 감염되었는지 검사하며, 이 기능을 선택하지 않으면 일반적인 악성코드 검사 방법을 사용합니다.

참고

TrueFind(은폐진단)는 64Bit 운영체제는 지원하지 않습니다.

- 악성 ActiveX 콘트롤 설치 차단: V3 IS 8.0에 등록된 알려진 악성코드의 고유 값을 Internet Explorer에 등록하여 Internet Explorer를 통한 악성 ActiveX 콘트롤 설치 시도를 차단합니다. 악성코드의 고유 값은 이 기능을 선택한 시점과 엔진 업데이트를 마친 후에 Internet Explorer에 악성코드의 고유 값을 새로 등록합니다. 이 기능을 선택해제하거나 V3 IS 8.0을 삭제하면 Internet Explorer에 등록한 악성코드의 고유 값을 제거하여 악성 ActiveX 콘트롤의 설치를 차단할 수 없습니다.
- 컴퓨터 시작할 때 V3 파일 무결성 검사: 컴퓨터를 시작할 때 V3 관련 파일의 손상 여부를 검사합니다. 파일이 손상된 경우 V3 IS 8.0 실행을 마치고 엔진 업데이트를 해야 합니다.

주의

V3 파일 무결성이 손상되어 엔진 업데이트를 할 때는 반드시 패치 파일을 다운로드하도록 선택해야 합니다. 패치 파일을 선택하지 않으면 손상된 프로그램 파일을 업데이트할 수 없습니다.

- V3 감염 여부 검사: PC 검사 실행, V3 IS 8.0의 메인 화면 실행, 작업 표시줄에 V3 아이콘을 등록할 때와 같이 해당 기능이 실행될 때 메모리와 실행 파일의 감염 여부를 검사합니다. 검사한 파일이 악성코드에 의해 감염된 경우 V3 IS 8.0을 종료하고 치료한 후에 프로그램을 다시 시작합니다.
- V3 자체 보호: 다른 프로그램이 V3의 동작을 방해하거나 중지할 목적으로 V3가 사용하는 프로세스를 종료하거나 V3 관련 파일이나 레지스트리를 변경하거나 삭제하는 것을 차단합니다. **사용자 지정**을 누르면 V3 관련 자체 보호 대상을 사용자가 직접 선택할 수 있습니다. V3 자체 보호 대상의 기본 값은 파일, 프로세스, 레지스트리 모두 선택입니다.
  - 파일: V3 관련 파일을 변경하거나 삭제하는 것을 차단합니다.
  - 프로세스: 다른 프로그램이 V3 관련 프로세스를 종료하는 것을 차단합니다.
  - 레지스트리: V3 관련 레지스트리를 변경하거나 삭제하는 것을 차단합니다.

참고

V3 자체 보호의 프로세스는 64Bit 운영체제에서는 지원하지 않습니다.

5 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

검사 예외 설정

PC 검사를 할 때 사용자가 지정한 특정 폴더나 파일, 확장자에 대해서는 바이러스나 스파이웨어 등의 악성코드 감염 여부를 검사하지 않는 기능입니다. 또한, 허용할 악성코드에 등록한 악성코드나 유해 가능 프로그램에 대해서도 감염 여부를 검사하지 않습니다.

1 바탕 화면의 V3 IS 8.0 아이콘( )을 더블 클릭합니다.

2 **환경 설정**을 선택합니다.

3 PC 검사의 **고급 설정**에서 **검사 예외 설정**을 선택합니다.

4 **선택한 대상 검사하지 않기**를 선택합니다. 이 옵션을 선택하면, 검사 예외 영역에 추가한 폴더나 파일, 확장자에 대해서는 검사를 하지 않습니다.

5 **검사 예외 영역**에 검사를 하지 않을 대상을 등록합니다.

- 폴더 추가: 검사 예외 영역에 등록할 폴더를 추가합니다. 폴더 추가를 누르면 <폴더 찾아보기>에서 검사를 하지 않을 폴더를 직접 선택할 수 있습니다.
- 파일 추가: 검사 예외 영역에 등록할 파일을 추가합니다. 파일 추가를 누르면 <열기>에서 필요한 파일 이름을 직접 선택할 수 있습니다.
- 확장자 추가: 검사 예외 영역에 등록할 확장자를 직접 입력합니다. 확장자 추가를 누르면 검사 예외 확장자 입력란에 검사를 하지 않을 확장자를 직접 입력할 수 있습니다. 확장자는 최대 260자 까지 입력할 수 있습니다.(영문자 기준)

참고

확장자를 두 개 이상 설정할 때에는 '/'로 구분하십시오.(예: bmp/gif/txt)

참고

\ : * ? " . < > |와 같은 문자는 확장자에 사용할 수 없으며, exe, dll, ocx와 같은 실행 파일은 검사 예외 확장자로 입력할 수 없습니다.

- 시스템 복원 폴더 검사하지 않기: 시스템 복원 폴더는 Microsoft Windows가 시스템 복원을 위해 컴퓨터를 손상시킬 수 있는 변경 내용을 추적할 수 있도록 제공하는 기능입니다. 시스템 복원 폴더는 Microsoft Windows만 해당 폴더를 생성하고 파일을 저장할 수 있기 때문에 복원 폴더에서 발견된 바이러스에 감염된 파일은 백신이 쓰기 권한이 없으므로 치료할 수 없습니다. 시스템 복원 폴더에 바이러스가 발견되는 이유는 Microsoft Windows가 시스템 복원 폴더에 파일을 백업할 때 이미 감염된 파일을 백업했기 때문입니다. 따라서, 시스템 복원 폴더에서 바이러스가 발견되었을 경우에는 치료할 수는 없지만, 시스템 복원을 할 때 해당 파일이 바이러스에 감염되었음을 사용자가 알고 있는 것이 중요할 수도 있습니다.

  Microsoft Windows XP의 경우 시스템 복원 폴더는 Microsoft Windows 설치 드라이브:\WINDOWS\system32\Restore 입니다.

참고

Windows 2000에서는 시스템 복원 폴더 검사하지 않기를 지원하지 않습니다.

6 검사에서 제외할 바이러스/스파이웨어가 있다면, **허용할 악성코드 영역**에 대상을 **추가**합니다.

7 <허용할 악성코드 추가/수정>에서 허용할 악성코드나 유해 가능 프로그램 이름을 입력합니다.

참고

악성코드 이름은 V3 IS 8.0에서 진단한 이름을 입력해야 하며, 입력한 악성코드는 검사에서 제외합니다.

8 **확인**을 누릅니다.

9 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

검사 설정

사전 검사 대상 선택

사전 검사 영역은 V3 IS 8.0이 PC 검사를 위해 파일 검사 이전에 검사해야 하는 컴퓨터의 주요 영역을 사용자가 직접 설정하는 기능입니다. 대부분의 경우 사전 검사 영역은 모두 선택하여 검사할 것을 권장합니다.

참고

사전 검사 영역은 PC 검사와 PC 실시간 검사, 예약 검사 설정에서 설정할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **설정하기**를 누릅니다.

3 **PC 검사 설정**의 PC 검사, PC 실시간 검사나 예약 검사 설정을 선택합니다.

4 **검사 설정**의 **사전 검사 대상 선택**에서 사전 검사 사용 옵션을 선택합니다.

- PC 실시간 검사가 꺼진 경우 사전 검사 사용: PC 검사나 예약 검사에서는 실시간 검사가 꺼진 경우에 사전 검사를 사용할 것인지를 선택할 수 있습니다. PC 실시간 검사가 꺼진 경우에 정밀 검사나 사용자 목록 검사, 예약 검사를 실행하면 사용자가 선택한 사전 검사 영역을 검사합니다.

5 **사용자 지정**을 누릅니다.

- 메모리: 컴퓨터의 메모리에 실행 중인 프로그램을 검사합니다. 악성코드가 실행되면, 대부분 메모리에 로드되어 다른 프로그램을 감염시키는 경우가 많으므로 메모리 검사는 항상 선택하는 것이 좋습니다.
- 부트 영역: 하드 디스크의 부트 영역에 대한 악성코드 감염 여부를 검사합니다.
- 프로세스: 현재 실행 중인 프로세스를 검사합니다. 프로그램은 디스크에 저장된 파일이고, 프로세스는 메모리에서 실행 중인 복사된 프로그램입니다. 따라서, 악성코드가 실행되면 악성코드가 실행한 프로세스가 실행 중일 가능성이 높습니다. 현재 실행 중인 프로세스는 Microsoft Windows의 작업 관리자를 실행(Ctrl+Alt+DEL키를 누름)하여 **[프로세스]**에서 확인할 수 있습니다.

- 시작 프로그램: 컴퓨터가 부팅된 후 항상 실행되는 시작 프로그램을 검사합니다. 악성코드 중에는 시작 프로그램을 감염시키거나 시작 프로그램에 자신을 등록하여 컴퓨터가 실행될 때마다 자신을 실행하여 다른 프로그램을 쉽게 감염시킬 수 있습니다.

참고

고급 설정에서 TrueFind(은폐진단) 사용을 선택했다면 사전 검사 영역을 검사할 때 TrueFind(은폐진단) 기능을 활용하여 은폐된 악성코드 감염 여부를 검사합니다.

6 **확인**을 누릅니다.

7 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

검사 대상 선택

악성코드 검사 대상은 V3 IS 8.0이 지원하는 모든 파일과 감염되기 쉬운 실행 파일, 매크로 파일, 스크립트 파일입니다. 또한, 사용자가 추가로 검사할 확장자가 있는 경우 직접 검사할 확장자를 입력하면, 해당 확장자에 대한 검사를 실행합니다. V3 IS 8.0이 지원하는 정밀 검사나 실시간 검사 등 검사 종류에 맞게 검사 대상을 선택하면 검사의 효율성이 높아질 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **설정하기**를 누릅니다.

3 **PC 검사 설정**의 PC 검사, PC 실시간 검사, 메신저 실시간 검사나 예약 검사 설정을 선택합니다.

4 **검사 설정**의 **검사 대상 선택**에서 필요한 옵션을 선택합니다.

- 모든 파일: V3 IS 8.0이 지원하는 모든 파일을 검사합니다.

- 감염되기 쉬운 파일: 악성코드의 감염 위험이 높은 실행 파일, 매크로 파일, 스크립트 파일 등을 검사합니다.
  - 실행 파일: 실행 가능한 확장자를 가진 파일을 검사합니다. 대표적으로 EXE, DLL, OCX, SCR, COM 등의 실행 가능한 확장자를 가진 파일을 검사합니다.
  - 매크로 파일: XLS, SHS, DOT 등의 확장자를 가진 매크로 파일을 검사합니다.
  - 스크립트 파일: PIF, VBS, JS, BAT, INI 등의 확장자를 가진 스크립트 파일을 검사합니다.
- 추가로 검사할 확장자: 감염되기 쉬운 파일과 사용자가 입력한 확장자를 검사합니다. 입력한 확장자간의 구분은 '/' 를 입력해야 합니다. (예: dat/txt/tmp)
- 압축 파일 검사: 사용자가 선택한 압축 파일을 검사합니다. 사용자 지정을 누르면, 검사할 압축 파일 형식과 압축 파일 검사 설정을 선택할 수 있습니다.

5 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

압축 파일 검사 설정

압축 파일 검사는 사용자가 설정한 검사할 압축 파일 형식과 압축 회수에 따라 파일이 악성코드에 감염되었는지를 검사합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **설정하기**를 누릅니다.

3 **PC 검사 설정**의 PC 검사, 메신저 실시간 검사나 예약 검사 설정을 선택합니다.

4 **검사 설정**의 **추가 검사에서 압축 파일**을 선택합니다.

5 **사용자 지정**을 누릅니다.

6 <압축 파일 검사 설정>에서 압축 파일 형식과 압축 파일 검사 방법을 선택합니다.

- 압축 파일 형식 선택: V3 IS 8.0이 지원하는 압축 파일 중에서 사용자가 검사할 압축 파일 확장자를 직접 선택할 수 있습니다. 선택할 수 있는 압축 파일은 ARJ, BZIP2, CAB, LZH, RAR, TAR, ZIP, Z, ALZ이며, 기본 값은 ARJ, LZH, RAR, ZIP, ALZ입니다.
- 압축 파일 검사 방법 선택
  - 검사할 수 있는 최대 다중 압축 횟수 선택: 압축 파일 검사를 사용자가 설정한 최대 다중 압축 횟수에 따라 압축을 풀어 검사합니다. 다중 압축 횟수는 1부터 10까지 설정할 수 있습니다. 다중 압축 횟수가 높은 파일이 있는 경우 검사 시간이 오래 걸릴 수 있습니다. 기본 값은 1(회)입니다.
  - 검사할 압축 파일의 최대 크기: 압축 파일의 크기에 따라 검사를 할 수 있습니다. 선택 가능한 파일의 크기는 1MB 부터 10MB 까지 이며, 기본 값은 5MB 입니다.

참고

파일을 압축하는 경우 대부분 한 번만 압축하는 것이 일반적입니다. 예를 들어, sample.zip이 sample1.txt, sample2.txt, sample3.txt를 포함하고 있다면 이는 한 번만 압축된 경우입니다. 만약, sample.zip을 한 번 더 압축하여 newsample.zip을 만든다면 newsample.zip은 두 번 압축된 경우입니다. 예제와 같이 두 번 이상 압축된 파일을 다중 압축 파일이라고 부릅니다.

7 **확인**을 누릅니다.

- 기본 값: V3 IS 8.0에 정의된 기본 설정 옵션으로 압축 파일을 검사합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 저장하고 창을 닫습니다.
- 취소: 설정한 내용을 저장하지 않고 창을 닫습니다.

치료 방법 선택

악성코드에 감염된 파일을 치료하는 방법을 선택할 수 있습니다. 사용자가 선택한 치료 방법에 따라 감염된 파일을 치료하거나 삭제하고 검역소로 보내도록 선택할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **설정하기**를 누릅니다.

3 PC 검사**,** PC 실시간 검사, 메신저 실시간 검사, 예약 검사 설정을 선택합니다.

4 **검사 설정**의 **치료 방법 선택**에서 필요한 옵션을 설정합니다.

- 악성코드: 바이러스나 스파이웨어에 감염된 파일을 발견했을 때 치료하는 방법을 설정합니다.
  - 그대로 두기: 감염된 파일을 치료하지 않고 감염된 상태 그대로 둡니다.
  - 치료하기: 치료 가능한 파일인 경우 감염된 파일을 치료합니다. 단, 검사 결과 감염된 파일이 치료 불가 상태인 경우에는 해당 파일을 삭제합니다. 악성코드 치료 방법 선택의 기본 값입니다.
  - 삭제하기: 감염된 파일을 치료하지 않고 삭제합니다.
- 감염된 압축 파일: 압축 파일이 악성코드에 감염된 경우 치료하는 방법을 설정합니다.
  - 그대로 두기: 감염된 압축 파일을 치료하지 않고 감염된 상태 그대로 둡니다. 감염된 압축 파일 치료 방법 선택의 기본 값입니다.
  - 삭제하기: 감염된 압축 파일을 치료하지 않고 삭제합니다.

참고

감염된 압축 파일 치료 방법 선택은 PC 실시간 검사에서는 지원하지 않습니다.

- 실행 중인 감염 파일: 감염된 파일이 현재 실행 중인 경우, 실행 중인 파일을 치료하는 방법을 설정합니다.
  - 그대로 두기: 감염된 파일을 치료하지 않고 감염된 상태 그대로 둡니다.
  - 강제로 멈추고 치료하기: 실행 중인 파일을 V3 IS 8.0이 강제로 실행을 종료한 후에 치료합니다. 단, Microsoft Windows의 시스템 프로세스(smss.exe, csrss.exe, winlogon.exe, lsass.exe, services.exe)는 컴퓨터를 다시 시작할 때 치료합니다.
  - 탐색기/Internet Explorer만 멈추고 치료하기: explorer.exe, iexplore.exe만 강제로 멈추고 치료합니다.
  - 컴퓨터를 다시 시작할 때 치료하기: 감염된 파일을 컴퓨터를 다시 시작할 때 치료합니다.
  - 사용자 확인 후 치료하기: 사용자가 직접 감염된 파일을 치료하는 방법을 검사할 때 마다 선택하여 처리합니다.

참고

실행 중인 감염 파일 치료 방법 선택은 메신저 실시간 검사에서는 지원하지 않으며, 사용자 확인 후 치료하기는 PC 검사에서만 설정할 수 있습니다.

- 자동 치료: V3 IS 8.0이 악성코드에 감염된 파일을 발견한 후 사용자에게 치료 여부를 묻지 않고 바로 치료합니다. 자동 치료를 선택하면, 치료를 위한 화면이 나타나지 않고 감염된 파일을 자동 치료하고, 감염 파일의 치료 여부는 검사 기록을 통해 확인할 수 있습니다.
- 치료나 삭제 전 감염된 파일을 검역소로 보내기: 설정된 치료 방법에 따라 감염된 파일을 치료 또는 삭제할 경우, 해당 파일을 미리 검역소에 백업합니다. 검역소 백업은 지정한 폴더에 감염된 원본 파일을 실행 불가능한 형태로 변경하여 보관합니다. 감염된 원본 파일을 검역소에 그대로 백업할 경우 해당 파일을 다시 실행하여 다른 파일을 감염시킬 수 있기 때문입니다.
- hosts 파일 보호: 악성코드가 hosts 파일을 변경하려고 할 때 차단합니다. hosts 파일의 변경 시도가 있는 경우 사용자에게 알림 창으로 변경 시도를 차단했음을 알려줍니다.

참고

hosts 파일 보호는 PC 실시간 검사에서만 설정할 수 있습니다.

5 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

실행 중인 감염 파일 치료

PC 검사 설정의 치료 방법 선택에서 실행 중인 감염 파일의 치료 방법을 사용자 확인 후 치료하기를 선택하면 감염된 파일의 치료를 위해 사용자에게 치료 방법을 물어보는 창이 나타납니다.

실행 중인 감염 파일 발견

- 감염된 파일 이름: V3 IS 8.0이 악성코드에 감염되었다고 진단한 파일 이름을 보여줍니다.
- 실행 중인 파일 이름: 감염된 파일 이름과 같은 경우도 있지만, DLL이나 실행 파일과 관련된 다른 파일이 감염된 경우 실제 감염된 파일을 사용하는 파일의 이름을 보여줍니다.

❖ 치료 방법 선택

- 강제로 멈추고 치료하기: 실행 중인 파일을 강제로 멈추고 치료합니다.

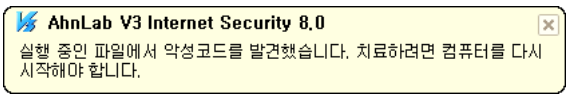
⚠ 주의

실행 중인 파일을 종료하기 전에 저장하지 않은 데이터는 복구할 수 없습니다.

- 탐색기/Internet Explorer만 멈추고 치료하기: 실행하고 있던 모든 탐색기/Internet Explorer를 종료한 후에 감염된 파일을 치료합니다.
- 컴퓨터 다시 시작할때 치료하기: 현재 상태에서 감염된 파일을 종료할 수 없는 경우에 컴퓨터를 다시 시작할 때 감염된 파일을 치료합니다.
- 그대로 두기: 감염된 파일을 치료하지 않고 그대로 둡니다.
- 현재 검사를 마칠 때까지 감염된 파일은 모두 같은 방법으로 치료: 실행 중인 파일 여러 개에서 악성코드가 발견된 경우 검사를 마칠 때까지 사용자가 선택한 치료 방법으로 계속 치료합니다.

실행 중인 파일에서 악성코드를 발견한 경우

실행 중인 파일에서 악성코드를 발견하면 V3 IS 8.0의 알림 아이콘에 다음과 같은 풍선 도움말이 나타납니다. 실행 중인 감염 파일은 실행 중인 감염 파일 치료에 설정된 방법에 따라 처리합니다.



6장
네트워크 보안

개인 방화벽 규칙의 우선 순위

개인 방화벽 규칙을 설정하면 다음과 같은 순서로 규칙을 적용하여 트래픽을 허용하거나 차단합니다.

1 허용 주소에 등록되어 있는 IP 주소인지 확인합니다.

2 차단 주소에 등록되어 있는 IP 주소인지 확인합니다. 계속 차단 IP 주소나 임시 차단 IP 주소에 있으면 차단합니다.

3 네트워크 침입 차단에서 차단하는 패킷을 보냈는지 확인합니다.

4 개인 방화벽의 네트워크 규칙에서 허용하거나 차단하도록 설정한 IP 주소인지 확인합니다.

5 개인 방화벽의 프로그램 규칙에서 허용하거나 차단하도록 설정한 IP 주소인지 확인합니다.

네트워크 침입 차단 사용하기

네트워크를 통해 웜이나 트로이목마와 같은 악성코드가 침입하는 것을 탐지하여 차단합니다. 악성코드에 감염된 컴퓨터는 네트워크로 연결된 다른 컴퓨터를 감염시킵니다. 네트워크에 감염된 컴퓨터가 있으면 사용자의 컴퓨터도 악성코드에 감염될 위험이 있습니다. 특히 인터넷에 연결된 컴퓨터는 항상 악성코드에 감염될 위험이 있습니다. 네트워크 침입 차단을 사용하면 악성코드가 침입하는 것을 차단하여 컴퓨터를 보호할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 네트워크 침입 차단은 다음의 3가지 방법 중에서 선택하여 실행할 수 있습니다.

- HOME의 네트워크 침입 차단에서 **사용 안 함**에서 마우스를 눌러 **사용**을 선택합니다.
- 네트워크 보안의 개인 방화벽에서 **사용 안 함**에서 마우스를 눌러 **사용**을 선택합니다
- 환경 설정의 네트워크 침입 차단에서 **네트워크 침입 차단 사용**을 선택합니다.

참고

네트워크 침입 차단 상세 규칙의 사용 여부를 선택하려면 네트워크 침입 차단에서 설정할 수 있습니다.

개인 방화벽 사용하기

개인 방화벽을 사용하면 네트워크 규칙과 프로그램 규칙에 따라 허가하지 않은 인터넷 연결을 차단하여 컴퓨터를 더 안전하게 유지할 수 있습니다. 방화벽은 다른 컴퓨터에서 사용자의 컴퓨터로 들어오는 데이터와 사용자의 컴퓨터에서 다른 컴퓨터로 나가는 데이터를 제한합니다. 허가없이 컴퓨터에 접근하려는 사람이나 바이러스와 웜과 같은 악성코드가 사용자의 컴퓨터에 침입하는 것을 막을 수 있습니다. 또한 사용자의 컴퓨터에 감염된 악성코드가 컴퓨터에서 정보를 유출하는 것을 막을 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 개인 방화벽은 다음의 3가지 방법 중에서 선택하여 실행할 수 있습니다.

- HOME의 개인 방화벽에서 **사용 안 함**에서 마우스를 눌러 **사용**을 선택합니다.
- 네트워크 보안의 개인 방화벽에서 **사용 안 함**에서 마우스를 눌러 **사용**을 선택합니다.
- 환경 설정의 개인 방화벽에서 **개인 방화벽 사용**을 선택합니다.

참고

개인 방화벽의 규칙은 개인 방화벽에서 설정할 수 있습니다.

네트워크 침입 차단

사용자가 직접 네트워크 침입 차단 기능을 사용하거나 사용하지 않도록 선택할 수 있으며, 네트워크 침입 차단을 사용하지 않으면 웜이나 트로이목마와 같은 해킹 위험에 노출될 수 있습니다. 네트워크 침입 차단에서 제공하는 상세 차단 규칙은 사용자가 사용 여부를 직접 선택할 수 있고 공격자의 IP 주소를 허용/차단 IP 주소에 등록하여 해당 IP에서 들어오는 공격은 계속 차단하거나 임시로 차단할 수 있습니다. 네트워크 침입 차단에서 제공하는 차단 규칙은 엔진 업데이트에 의해 업데이트 되므로 항상 최신 버전의 엔진을 사용해야 합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **네트워크 침입 차단**에서 **설정하기**를 누릅니다.

3 **네트워크 침입 차단 사용**을 선택합니다.

- 네트워크 침입 차단 사용: V3 IS 8.0이 제공하는 네트워크 침입 차단 규칙에 의해 규칙에 해당하는 공격이 있을 경우 차단합니다.
  - 이름: 악성코드를 차단하는 규칙의 이름입니다.
  - 사용 여부: 해당 네트워크 침입 차단 규칙을 사용하고 있는지 보여 줍니다. 마우스 오른쪽 버튼을 눌러 **사용**이나 **사용 안 함**을 선택할 수 있습니다.

⚠ 주의

사용 여부를 **사용 안 함**으로 설정하면 해당 규칙이 차단하는 악성코드가 컴퓨터에 침입해 피해를 입힐 위험이 있습니다.

  - 규칙 분류: 규칙이 차단하는 악성코드의 유형으로 트로이목마, 웜, 스캐닝 등이 있습니다. 스캐닝의 경우 네트워크 침입을 탐지하여 알려주고, 트로이목마나 웜과 같은 공격은 해당 공격을 탐지하여 차단합니다. 네트워크 침입 탐지와 네트워크 침입 차단 알림 창을 보려면 알림 설정에서 해당 항목을 선택해야 합니다.
  - 설명: 악성코드를 차단하는 규칙에 대한 설명입니다.

4 **공격자 IP 주소 임시 차단**이 필요한 경우 선택합니다.

- 공격자 IP 주소 임시 차단: 악성코드에 감염되어 접근을 차단한 IP 주소로 허용/차단 IP 주소에 임시 차단 IP로 등록한 주소를 차단합니다. 차단할 IP 주소는 허용/차단 IP 주소에서 설정한 규칙에 따르며, 임시 차단 만료 시간은 30분입니다.

- 임시 차단 IP 보기: 허용/차단 IP 주소의 임시 차단 IP 주소 목록에 등록된 IP 주소를 확인할 수 있습니다.

5 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

개인 방화벽 설정

방화벽 정책

개인 방화벽 정책은 네트워크 규칙과 프로그램 규칙을 하나로 묶은 것으로 네트워크 규칙과 프로그램 규칙을 설정하기 전에 먼저 방화벽 정책을 설정해야 합니다. 네트워크 규칙과 프로그램 규칙에서는 선택한 방화벽 정책의 세부 규칙을 설정하는 기능이므로 먼저 방화벽 정책을 세운 후에 네트워크 규칙과 프로그램 규칙을 설정해야 합니다. 따라서, 네트워크 규칙과 프로그램 규칙을 다르게 설정한 방화벽 정책을 여러 개 추가하면 상황에 따라 적절한 방화벽 정책을 적용하여 컴퓨터를 더욱 효과적으로 보호할 수 있습니다. 또한, 이동이 잦아 다양한 네트워크 환경에서 컴퓨터를 사용해야 하는 사용자는 방화벽 정책 자동 전환 기능을 활용하여 상황에 맞는 방화벽 정책을 자동 적용할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **개인 방화벽**에서 **설정하기**를 누릅니다.

3 **개인 방화벽 사용**을 선택합니다.

4 **방화벽 정책** 탭을 선택합니다.

5 방화벽 정책 목록에서 **추가**를 누릅니다.

6 <방화벽 정책 추가>에서 방화벽 정책을 설정합니다.

- 방화벽 정책 이름: 새로 만드는 방화벽 정책의 이름을 입력합니다. 방화벽 정책 이름은 63자까지 입력할 수 있습니다.
- 정책 가져오기: 이전에 설정한 정책의 규칙을 복사해서 사용하거나 기본으로 제공하는 정책을 가져오지 않고 직접 다시 설정할 수 있습니다.
  - 사용 안 함: 기존의 방화벽 정책을 가져오지 않고 사용자가 새로운 정책 이름을 만들고 방화벽 정책을 수립합니다.
  - 사무실: 사무실과 같은 네트워크 환경에서 권장할 만한 방화벽 정책으로 외부로 나가는 접근은 허용되지만 내부로 접근하는 들어오는 접근은 사용자의 개인 방화벽 설정 규칙에 따라 허용하거나 차단합니다. 기본적으로 제공하는 네트워크 규칙을 모두 사용합니다.

- 집: 가정과 같은 네트워크에 환경에서 권장할 만한 방화벽 정책입니다. 기본적으로 제공하는 네트워크 규칙 중 Microsoft Directory Service 나가기 허용만 사용하지 않고 모든 규칙을 사용합니다.

참고

Microsoft Directory Service는 회사와 학교 같은 단체 네트워크 환경에서 주로 사용하는 프로토콜이므로 기본적으로 제공된 집 방화벽 규칙에서는 사용 안 함으로 설정되어 있습니다.

- 노트북(무선랜): 노트북과 같은 무선 네트워크 환경에서 권장할 만한 방화벽 정책으로 사무실에서의 정책과 동일하지만 모든 나가기 허용, DNS 나가기 허용, ICMP 나가기 허용만 기본적으로 사용합니다.
- 직접 접속(방화벽 없음): 인터넷 환경에 직접 연결하는 환경에서 권장할 만한 방화벽 정책으로 회사나 단체처럼 방화벽 장비가 설치되지 않아 높은 보안 수준이 요구되는 환경에서 사용을 권장합니다. 무선랜 환경과 동일하게 모든 나가기 허용, DNS 나가기 허용, ICMP 나가기 허용만 기본적으로 사용하고 나머지 규칙은 사용자가 직접 사용 여부를 결정해야 합니다.

- 네트워크 장치 이름: 정책을 적용할 네트워크 카드의 이름을 선택합니다. 사용자 PC에 장착되어 있는 네트워크 카드 이름이 나타나므로 해당 장치를 선택합니다.
- 정보 가져오기: 네트워크 장치 이름을 선택하고 정보 가져오기를 누르면 게이트웨이 주소를 자동으로 불러옵니다.
- 게이트웨이 주소: 게이트웨이 IP 주소를 직접 입력하거나 정보 가져오기를 눌러 주소를 자동으로 입력합니다.

7 **확인**을 누릅니다.

8 방화벽 정책 이름에 새로 추가한 방화벽 정책이 등록되었는지 확인합니다.

9 **방화벽 정책 자동 전환**이 필요한 경우 선택합니다.

- 방화벽 정책 자동 전환: 네트워크 환경이 변경되면 이를 감지해서 자동으로 방화벽 정책을 변경합니다. 방화벽 정책 자동 변환은 게이트웨이 주소에 따라 네트워크 환경의 변화를 감지하며 방화벽 정책 자동 전환 상태에서도 사용자가 직접 방화벽 정책을 선택할 수 있습니다.

참고

Windows 2000에서는 방화벽 정책 자동 전환을 지원하지 않습니다.

10 **고급 설정**에서 필요한 옵션을 선택합니다.

- IPX 프로토콜 허용: IPX 프로토콜을 사용하는 트래픽을 허용합니다.
- IGMP 프로토콜 허용: IGMP 프로토콜을 사용하는 트래픽을 허용합니다.
- 포트 숨김 사용(스텔스 포트 기능): 포트 스캐닝 기법을 이용한 해킹 시도를 방지합니다.

11 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

네트워크 규칙

네트워크 규칙은 IP 주소, 프로토콜, 포트 번호, 인터넷 연결 방향으로 구성된 방화벽 규칙으로 인터넷이나 네트워크를 통하여 다른 컴퓨터와 데이터를 주고 받는 것을 허용하거나 차단하도록 규칙을 설정할 수 있습니다. 개인 방화벽의 네트워크 규칙을 이용하면 믿을 수 있는 컴퓨터만 데이터를 주고 받는 것을 허용하고 해킹과 같은 위험을 막아 컴퓨터를 보호할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **개인 방화벽**에서 **설정하기**를 누릅니다.

3 **개인 방화벽 사용**을 선택합니다. 개인 방화벽을 사용하면, 개인 방화벽이 동작하여 설정된 규칙에 따라 접근을 허용하거나 차단합니다.

4 **네트워크 규칙** 탭을 선택합니다. 네트워크 규칙은 인터넷을 통하여 다른 컴퓨터가 사용자의 컴퓨터에 접근하여 데이터를 주고 받는 것을 허용하거나 차단하도록 규칙을 설정합니다. 규칙에 없는 컴퓨터에서 사용자의 컴퓨터에 접근하면 알림 창이 나타납니다.

참고

프로그램 규칙은 컴퓨터에 설치된 프로그램이 인터넷에 연결하는 것을 허용하거나 차단하도록 규칙을 설정하는 기능으로 프로그램 규칙을 참고하십시오. 방화벽 정책은 컴퓨터에 적용할 방화벽 정책을 설정하는 것으로 방화벽 정책을 참고하십시오.

5 **규칙에 적용할 방화벽 정책 선택**에서 **적용할 정책**을 선택합니다.

- 적용할 정책: 현재 새로 만들거나 수정할 네트워크 규칙에 적용할 방화벽 정책을 선택합니다. 방화벽 정책은 방화벽 정책에서 새로 만들 수 있으며 V3 IS 8.0이 제공하는 기본 방화벽 정책을 선택할 수도 있습니다. 기본적으로 제공하는 방화벽 정책은 사무실, 집, 노트북(무선랜), 직접 접속(방화벽 없음)이 있으며 사용자가 만든 방화벽 정책이 있는 경우 적용할 정책 목록에 지정한 이름으로 나타납니다.
- 방화벽 정책 설정: 적용할 정책 목록에 새로운 네트워크 규칙을 적용할 정책이 없는 경우 방화벽 정책 설정을 눌러 방화벽 정책을 만들 수 있습니다.

6 **네트워크 규칙 설정**을 설정합니다.

- 우선 순위 조정: 여러 개의 네트워크 규칙에 설정된 내용이 서로 충돌할 경우에는 우선 순위에 따라 규칙을 적용합니다. 네트워크 규칙 설정 목록에서 위에 보이는 것이 규칙의 우선 순위가 가장 높고 밑으로 갈수록 우선 순위가 낮아집니다. V3 IS 8.0이 제공하는 기본 방화벽 정책에 따른 네트워크 규칙 우선 순위의 기본 값은 모든 나가기 허용>DNS 나가기 허용>DNS 들어오기 허용>NetBIOS Name Service 나가기 허용>NetBIOS Name Service 들어오기 허용>NetBIOS Datagram Service 나가기 허용>NetBIOS Datagram Service 들어오기 허용>NetBIOS Session Service 나가기 허용>Microsoft Directory Service 나가기 허용>ICMP 나가기 허용>ICMP 들어오기 허용입니다.
  - ▲: 선택한 규칙의 우선 순위를 높입니다.
  - ▼: 선택한 규칙의 우선 순위를 낮춥니다.
- 추가: <네트워크 규칙 추가/수정>에서 추가할 규칙을 새로 만들 수 있습니다.
- 수정: 네트워크 규칙 목록에서 수정할 규칙을 먼저 선택하고 수정을 누르면 <네트워크 규칙 추가/수정>에서 해당 규칙을 변경할 수 있습니다.

- 삭제: 네트워크 규칙 목록에서 삭제할 규칙을 먼저 선택하고 삭제를 누르면 **선택한 네트워크 규칙을 삭제하시겠습니까?** 라는 메시지가 나타납니다. 삭제할 규칙이 맞다면 **예**를 누릅니다.
- 사용 여부: 선택한 방화벽 정책에서 해당 규칙을 사용하고 있는지를 나타냅니다. 사용 여부를 변경하려면 해당 규칙에서 더블 클릭하거나 수정 버튼을 누르면 나타나는 <네트워크 규칙 추가/수정>에서 **네트워크 규칙 사용**을 선택하거나 선택을 해제합니다. 네트워크 규칙 사용을 선택하면 사용 여부가 **사용**으로 나타나고 선택을 해제하면 **사용 안 함**으로 나타납니다.
- 규칙 이름: 네트워크 규칙의 이름입니다. 규칙 이름은 <네트워크 규칙 추가/수정>의 공통 설정에서 설정할 수 있습니다.
- 설명: 네트워크 규칙의 설정 상태를 간단히 보여줍니다.

7 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

네트워크 규칙의 기본 값

규칙 이름	기본 값
모든 나가기 허용	모든 IP주소, TCP, UDP, ICMP 프로토콜, 모든 포트 번호
DNS 나가기 허용	모든 IP 주소, TCP, UDP 프로토콜, 특정 원격 포트 번호:53
DNS 들어오기 허용	모든 IP 주소, TCP, UDP 프로토콜, 특정 로컬 포트 번호:53
NetBIOS Name Service 나가기 허용	모든 IP 주소, TCP, UDP 프로토콜, 특정 원격 포트 번호:137

규칙 이름	기본 값
NetBIOS Name Service 들어오기 허용	모든 IP 주소, TCP, UDP 프로토콜, 특정 로컬 포트 번호:137
NetBIOS Datagram Service 나가기 허용	모든 IP 주소, UDP 프로토콜, 특정 원격 포트 번호:138
NetBIOS Datagram Service 들어오기 허용	모든 IP 주소, UDP 프로토콜, 특정 로컬 포트 번호:138
NetBIOS Session Service 나가기 허용	모든 IP 주소, TCP 프로토콜, 특정 원격 포트 번호:139
Microsoft Directory Service 나가기 허용	모든 IP 주소, TCP, UDP 프로토콜, 특정 원격 포트 번호:445
ICMP 나가기 허용	모든 IP 주소, ICMP 프로토콜, 모든 포트 번호
ICMP 들어오기 허용	모든 IP 주소, ICMP 프로토콜, 모든 포트 번호

네트워크 규칙 추가/수정

인터넷으로 데이터를 주고 받을 때 허용하거나 차단할 네트워크 규칙을 설정할 수 있습니다. 네트워크 규칙은 인터넷 연결 방향, IP 주소, 프로토콜, 포트 번호를 직접 선택하여 규칙을 만들 수 있습니다.

네트워크 규칙 추가

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **개인 방화벽**에서 **설정하기**를 누릅니다.

3 **개인 방화벽 사용**을 선택합니다.

4 **네트워크 규칙** 탭을 선택합니다.

5 **규칙에 적용할 방화벽 정책 선택**에서 **적용할 정책**을 선택합니다.

6 **네트워크 규칙 설정**에서 **추가**를 누릅니다.

7 <네트워크 규칙 추가/수정>의 **공통 설정**에서 규칙에 사용할 이름과 인터넷 연결 방향을 선택합니다.

- 규칙 이름: 네트워크 규칙 이름을 입력합니다. 규칙 이름은 63글자까지 입력할 수 있습니다.
- 인터넷 연결: 인터넷에 연결할 때 규칙에서 설정한 IP 주소, 프로토콜, 포트를 사용한 연결을 허용하거나 차단하도록 설정합니다.
  - 들어오기 허용: 연결한 IP 주소에서 데이터를 받는 것을 허용합니다.
  - 나가기 허용: 연결한 IP 주소로 데이터를 보내는 것을 허용합니다.
  - 모두 허용: 연결한 IP 주소와 데이터를 주고 받는 들어오기와 나가기를 모두 허용합니다.
  - 들어오기 차단: 연결한 IP 주소에서 데이터를 받는 것을 차단합니다.
  - 나가기 차단: 연결한 IP 주소로 데이터를 보내는 것을 차단합니다.
  - 모두 차단: 연결한 IP 주소와 데이터를 주고 받는 들어오기와 나가기를 모두 차단합니다.

8 <네트워크 규칙 추가/수정>의 **IP 주소**에서 규칙을 적용할 주소를 지정합니다.

- 모든 IP 주소: 모든 IP 주소를 대상으로 합니다.
- 특정 IP 주소: 사용자가 입력한 IP 주소 목록을 대상으로 합니다. 특정 IP 주소 목록에는 최대 8개까지 추가할 수 있습니다.
- 특정 IP 주소 목록: 사용자가 입력한 IP 주소 목록을 보여줍니다. **추가**를 누르면 <IP 주소 설정>에서 IP 주소를 설정할 수 있으며, **수정**을 누르면 선택한 IP 주소를 수정할 수 있습니다. **삭제**를 누르면, 선택한 IP 주소를 목록에서 지웁니다.

9 <네트워크 규칙 추가/수정>의 **프로토콜**에서 인터넷이나 네트워크를 통해서 데이터를 주고 받을 때 허용하거나 차단할 프로토콜을 선택합니다.

- TCP: TCP 프로토콜을 이용하여 주고 받는 데이터를 허용하거나 차단합니다.
- UDP: UDP 프로토콜을 이용하여 주고 받는 데이터를 허용하거나 차단합니다.
- ICMP: ICMP 프로토콜을 이용하여 주고 받는 데이터를 허용하거나 차단합니다.

10 <네트워크 규칙 추가/수정>의 **포트 설정**에서 인터넷이나 네트워크를 통해서 데이터를 주고 받을 때 허용하거나 차단할 포트를 설정합니다.

- 모든 포트 번호: 모든 포트에 대해 사용을 허용하거나 차단합니다.
- 특정 포트 번호: 특정 포트에 대해 사용을 허용하거나 차단합니다. **특정 포트**를 선택하고 **추가**를 누르면 <포트 설정>에서 규칙을 적용할 포트를 설정할 수 있습니다.

11 **로그 남김**을 선택합니다. 로그 남김을 선택하면, 설정한 네트워크 규칙에 의해 차단할 경우 로그를 남깁니다. 단, UDP 프로토콜에 대해서는 로그를 남기지 않습니다.

12 **확인**을 누릅니다.

IP 주소 설정

특정 IP 주소를 직접 입력하거나 수정할 수 있습니다.

1 <IP 주소 설정>의 **IP 주소 입력**에서 IP 주소나 IP 주소 범위를 입력합니다.

- 단일 IP 주소: 특정한 IP 주소를 허용하거나 차단합니다.
  - 호스트 이름: 허용하거나 차단할 컴퓨터의 호스트 이름을 입력합니다. 호스트 이름을 입력하고 **IP 주소로 변환**을 누르면 입력한 호스트의 IP 주소를 자동으로 찾아서 변환합니다.
  - IP 주소: 허용하거나 차단할 컴퓨터의 IP 주소를 입력합니다.
- IP 주소 범위: 시작 IP 주소와 종료 IP 주소 사이에 있는 IP 주소를 허용하거나 차단합니다.
  - 시작 IP 주소: 허용하거나 차단할 IP 주소 범위의 처음 IP 주소를 입력합니다.
  - 종료 IP 주소: 허용하거나 차단할 IP 주소 범위의 마지막 IP 주소를 입력합니다.
- 서브넷 마스크: IP 주소와 서브넷 마스크를 입력하여 IP 주소 범위를 지정합니다.
  - IP 주소: IP 주소를 입력합니다.
  - 서브넷 마스크: 서브넷 마스크를 입력합니다.

2 **방화벽 규칙 적용 방법 선택**에서 규칙을 적용하는 방법을 선택합니다.

- 입력한 IP 주소에만 규칙 적용: 설정한 IP 주소나 IP 주소 범위에 해당하는 컴퓨터에만 방화벽 규칙을 적용합니다.
- 입력한 IP 주소만 제외하고 규칙 적용: 설정한 IP 주소나 IP 주소 범위에 해당하는 컴퓨터를 제외한 다른 모든 컴퓨터에 방화벽 규칙을 적용합니다.

3 **확인**을 누릅니다.

포트 설정

네트워크 규칙을 적용할 포트를 지정합니다. 모든 포트나 사용자가 특정 포트를 지정하여 규칙을 적용할 포트를 설정할 수 있습니다.

1 <포트 설정>의 **포트 종류 선택**에서 **로컬 포트**나 **원격 포트**를 선택합니다.

- 로컬 포트: 사용자 컴퓨터에서 규칙을 적용할 포트 번호입니다.
- 원격 포트: 네트워크를 통해 접근하는 다른 컴퓨터의 포트 번호입니다.

2 **포트 입력**에서 입력 방법과 포트 값을 입력합니다.

- 단일 포트(기본): 단일 포트에 입력한 특정 포트를 허용하거나 차단합니다.
  - 단일 포트: 허용하거나 차단할 포트 번호를 입력합니다.
- 포트 범위: 시작 포트와 종료 포트 사이에 있는 포트 번호를 허용하거나 차단합니다.
  - 시작 포트: 허용하거나 차단할 포트 범위의 처음 포트 번호를 입력합니다.
  - 종료 포트: 허용하거나 차단할 포트 범위의 마지막 포트 번호를 입력합니다.

3 **방화벽 규칙 적용 방법 선택**에서 규칙을 적용하는 방법을 선택합니다.

- 입력한 포트에만 규칙 적용: 설정한 포트나 포트 범위에 해당하는 포트 번호에만 네트워크 규칙을 적용합니다.
- 입력한 포트만 제외하고 규칙 적용: 설정한 포트나 포트 범위를 제외한 다른 모드 포트에 네트워크 규칙을 적용합니다.

4 **확인**을 누릅니다.

프로그램 규칙

컴퓨터에 설치된 프로그램이 인터넷에 연결하는 것을 허용하거나 차단하도록 규칙을 설정합니다. 컴퓨터에 설치된 프로그램에는 웹브라우저와 같이 인터넷에 연결되어 데이터를 주고 받는 프로그램이 있습니다. 웹브라우저 외에도 프로그램의 최신 버전을 확인하거나 프로그램이 열고 있는 파일의 정보나 저작권을 확인하기 위해 인터넷에 연결하여 데이터를 주고 받아야 하는 프로그램이 있습니다. 그러나 악성코드는 컴퓨터에 있는 사용자의 정보를 몰래 유출하거나 악성코드를 설치하기 위해서 인터넷에 연결합니다. 개인 방화벽의 프로그램 규칙을 설정하면, 믿을 수 있는 프로그램이 인터넷에 연결하는 것만 허용하고 악성코드가 인터넷에 연결되는 것을 막아 컴퓨터를 보호할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **개인 방화벽**에서 **설정하기**를 누릅니다.

3 **개인 방화벽 사용**을 선택합니다. 개인 방화벽을 사용하면, 개인 방화벽이 동작하여 설정된 규칙에 따라 접근을 허용하거나 차단합니다.

4 **프로그램 규칙** 탭을 선택합니다.

5 **규칙에 적용할 방화벽 정책 선택**에서 **적용할 정책**을 선택합니다.

- 적용할 정책: 현재 새로 만들거나 수정할 프로그램 규칙을 적용할 방화벽 정책을 선택합니다. 방화벽 정책은 방화벽 정책에서 새로 만들 수 있으며 V3 IS 8.0이 제공하는 기본 방화벽 정책을 선택할 수도 있습니다. 기본적으로 제공하는 방화벽 정책은 사무실, 집, 노트북(무선랜), 직접 접속(방화벽 없음)이 있으며 사용자가 만든 방화벽 정책이 있는 경우 적용할 정책 목록에 지정한 이름으로 나타납니다.
- 방화벽 정책 설정: 적용할 정책 목록에 새로운 프로그램 규칙을 적용할 정책이 없는 경우 방화벽 정책 설정을 눌러 방화벽 정책을 만들 수 있습니다.

6 **프로그램 규칙 설정**을 설정합니다.

- 추가: <프로그램 규칙 추가>에서 규칙을 적용할 프로그램을 선택하고 인터넷 연결을 허용하거나 차단하도록 선택합니다.

참고

프로그램 규칙은 최대 256개까지 추가할 수 있습니다.

- 수정: 프로그램 규칙 목록에서 수정할 규칙을 먼저 선택하고 수정을 누르면 <프로그램 규칙 수정>에서 이 프로그램에 대한 규칙 사용 여부와 인터넷 연결을 허용하거나 차단하도록 변경할 수 있습니다.
- 삭제: 프로그램 규칙 목록에서 삭제할 규칙을 먼저 선택하고 삭제를 누르면 **선택한 프로그램 규칙을 삭제하시겠습니까?** 라는 메시지가 나타납니다. 삭제할 규칙이 맞다면 **예**를 누릅니다.
- 사용 여부: 선택한 방화벽 정책에서 해당 규칙을 사용하고 있는지를 나타냅니다. 사용 여부를 변경하려면 해당 규칙에서 더블 클릭하거나 수정 버튼을 누르면 나타나는 <프로그램 규칙 수정>에서 **프로그램 규칙 사용**을 선택하거나 선택을 해제합니다. 프로그램 규칙 사용을 선택하면 사용 여부가 **사용**으로 나타나고 선택을 해제하면 **사용 안 함**으로 나타납니다.

- 프로그램 이름: 프로그램 규칙을 적용하는 프로그램의 이름입니다.

참고

프로그램 규칙은 동일한 경로의 동일한 파일 이름을 중복해서 추가할 수 없으며, 파일 이름이 같더라도 파일 경로가 다르면 규칙에 추가할 수 있습니다.

- 인터넷 연결: 이 프로그램의 인터넷 연결 허용과 차단 여부, 사용자 정의 상태인지를 보여줍니다.
- 프로그램 규칙 자동 추가로 알림 창 발생 최소화하기: V3 IS 8.0이 안전하다고 판단하는 프로그램이 인터넷에 연결하려 할 때 알림 창을 보이지 않고 자동으로 연결을 허용하고 프로그램 규칙에 추가합니다.
- 파일 고유 정보 확인: 프로그램 규칙에 추가된 프로그램의 파일 버전과 파일 크기를 비교하여 규칙을 만들 때와 정보가 다른 경우 사용자에게 인터넷 연결 여부를 물어봅니다. 파일 고유 정보 확인을 선택하면, 파일 버전과 파일 크기 외에 파일의 해쉬(Hash) 값까지 비교하여 프로그램 규칙을 만들 때와 파일 정보가 다른 경우 인터넷 연결 허용 여부를 사용자에게 확인합니다. 프로그램 규칙이 모두 차단으로 설정된 경우에는 사용자에게 확인하지 않고 모두 차단합니다.

7 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

프로그램 규칙 추가/수정

사용자 컴퓨터에 설치된 프로그램 중 인터넷 연결을 허용하거나 허용하지 않을 프로그램을 선택할 수 있습니다. 프로그램 규칙에 추가한 프로그램은 사용자가 선택한 규칙에 따라 인터넷 연결을 허용하거나 차단합니다. 또한 규칙에 추가된 프로그램이라 하더라도 규칙을 만들 당시와 파일 정보가 다른 프로그램이 인터넷에 연결하려고 하면 사용자에게 알림 창으로 연결 허용 여부를 확인한 후에 인터넷 연결을 할 수 있습니다.

프로그램 규칙 추가

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **개인 방화벽**에서 **설정하기**를 누릅니다.

3 **개인 방화벽 사용**을 선택합니다.

4 **프로그램 규칙** 탭을 선택합니다.

5 **규칙에 적용할 방화벽 정책 선택**에서 **적용할 정책**을 선택합니다.

6 **프로그램 규칙 설정**에서 **추가**를 누릅니다.

7 <프로그램 규칙 추가>에서 **프로그램 규칙 사용**을 선택합니다.

8 규칙을 적용할 프로그램을 목록에서 선택하거나 **찾아보기**를 눌러 직접 파일 이름을 선택합니다.

9 선택한 프로그램에 대한 **인터넷 연결** 규칙을 선택합니다.

- 모두 허용: 선택한 프로그램의 인터넷 연결을 항상 허용합니다.
- 모두 차단: 선택한 프로그램의 인터넷 연결을 항상 차단합니다.
- 사용자 정의: 사용자가 직접 상세 규칙을 설정하여 선택한 프로그램의 인터넷 연결 규칙을 선택합니다. **상세 규칙 설정**을 누르면 <프로그램 상세 규칙 설정>에서 인터넷 연결 규칙을 설정할 수 있습니다.

10 **확인**을 누릅니다.

프로그램 규칙 수정

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **개인 방화벽**에서 **설정하기**를 누릅니다.

3 **개인 방화벽 사용**을 선택합니다.

4 **프로그램 규칙** 탭을 선택합니다.

5 **규칙에 적용할 방화벽 정책 선택**에서 **적용할 정책**을 선택합니다.

6 프로그램 규칙 목록에서 수정할 규칙을 선택하고 **수정**을 누릅니다.

7 <프로그램 규칙 수정>에서 수정할 내용을 선택합니다.

- 프로그램 규칙 사용: 이 프로그램 규칙을 사용할 것인지를 선택합니다.
- 프로그램 이름: 선택한 프로그램의 이름입니다.
  - 버전: 선택한 프로그램 자체의 버전입니다.
  - 회사: 선택한 프로그램을 만든 회사 이름입니다.
  - 실행 파일: 선택한 프로그램을 실행할 수 있는 실행 파일 이름입니다.
  - 파일 경로: 선택한 프로그램이 있는 실행 경로입니다.
- 인터넷 연결: 선택한 프로그램의 인터넷 연결 여부를 결정합니다.
  - 모두 허용: 선택한 프로그램의 인터넷 연결을 항상 허용합니다.
  - 모두 차단: 선택한 프로그램의 인터넷 연결을 항상 차단합니다.
  - 사용자 정의: 사용자가 직접 상세 규칙을 설정하여 선택한 프로그램의 인터넷 연결 규칙을 선택합니다. **상세 규칙 설정**을 누르면 <프로그램 상세 규칙 설정>에서 인터넷 연결 규칙을 설정할 수 있습니다.

8 **확인**을 누릅니다.

프로그램 규칙 삭제

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **개인 방화벽**에서 **설정하기**를 누릅니다.

3 **개인 방화벽 사용**을 선택합니다.

4 **프로그램 규칙** 탭을 선택합니다.

5 프로그램 규칙 목록에서 삭제할 규칙을 선택하고 **삭제**를 누릅니다.

6 **선택한 프로그램 규칙을 삭제하시겠습니까?** 라는 메시지가 나타납니다. 삭제하려면 **예**를 누르고, 삭제하지 않으려면 **아니오**를 누릅니다.

7 삭제한 프로그램 규칙이 프로그램 규칙 목록에서 삭제되었는지 확인합니다.

8 **확인**을 누릅니다.

프로그램 상세 규칙

선택한 프로그램에 대한 네트워크 규칙을 따로 설정할 수 있습니다. 일반적인 프로그램 규칙은 선택한 프로그램에 대한 인터넷 연결을 허용하거나 차단하도록 선택할 수 있습니다. 프로그램 상세 규칙에서는 선택한 프로그램에 대하여 IP 주소, 프로토콜, 포트 설정과 인터넷 연결 방향에 대하여 사용자 상황에 맞는 규칙을 설정할 수 있습니다.

프로그램 상세 규칙 추가

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **개인 방화벽**에서 **설정하기**를 누릅니다.

3 **개인 방화벽 사용**을 선택합니다.

4 **프로그램 규칙** 탭을 선택합니다.

5 **규칙에 적용할 방화벽 정책 선택**에서 **적용할 정책**을 선택합니다.

6 프로그램 규칙 목록에서 수정할 규칙을 선택하고 **수정**을 누릅니다.

7 **프로그램 규칙 설정**에서 **추가**를 누릅니다.

8 <프로그램 규칙 추가>에서 **프로그램 규칙 사용**을 선택합니다.

9 규칙을 적용할 프로그램을 목록에서 선택하거나 **찾아보기**를 눌러 직접 파일 이름을 선택합니다.

10 선택한 프로그램에 대한 **인터넷 연결** 규칙에서 **사용자 정의**를 선택합니다.

11 **상세 규칙 설정**을 누릅니다.

12 <프로그램 규칙 상세 설정>에서 선택한 프로그램의 네트워크 규칙을 설정하기 위해 **추가**를 누릅니다.

13 공통 설정, IP 주소, 프로토콜, 포트 설정을 설정합니다.

참고

프로그램 상세 규칙의 네트워크 규칙 설정에 대한 자세한 방법은 네트워크 규칙 추가/수정을 참고하십시오.

14 **로그 남김**을 선택합니다. 로그 남김을 선택하면, 설정한 네트워크 규칙에 의해 차단할 경우 로그를 남깁니다. 단, UDP 프로토콜에 대해서는 로그를 남기지 않습니다.

15 **확인**을 누릅니다.

프로그램 상세 규칙 수정

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **개인 방화벽**에서 **설정하기**를 누릅니다.

3 **개인 방화벽 사용**을 선택합니다.

4 **프로그램 규칙** 탭을 선택합니다.

5 **규칙에 적용할 방화벽 정책 선택**에서 **적용할 정책**을 선택합니다.

6 프로그램 규칙 목록에서 수정할 규칙을 선택하고 **수정**을 누릅니다.

7 <프로그램 규칙 수정>의 인터넷 연결에서 사용자 정의를 선택합니다.

8 **상세 규칙 설정**을 누릅니다.

9 <프로그램 상세 규칙 설정>에서 네트워크 규칙 목록에서 수정할 규칙을 선택하고 **수정**을 누릅니다.

10 공통 설정, IP 주소, 프로토콜, 포트 설정을 수정합니다.

참고

프로그램 상세 규칙의 네트워크 규칙 설정에 대한 자세한 방법은 네트워크 규칙 추가/수정을 참고하십시오.

11 **로그 남김**여부를 선택합니다. 로그 남김을 선택하면, 설정한 네트워크 규칙에 의해 차단할 경우 로그를 남깁니다. 단, UDP 프로토콜에 대해서는 로그를 남기지 않습니다.

12 **확인**을 누릅니다.

허용/차단 IP 주소 설정

허용 주소

허용 주소에 등록된 IP는 방화벽 규칙에 관계없이 항상 인터넷 연결이 허용됩니다. 허용 IP 주소는 방화벽 규칙에서 우선 순위가 가장 높으므로 방화벽의 네트워크 규칙과 프로그램 규칙에서 설정한 규칙과 관계없이 항상 연결을 허용하는 IP 주소를 등록하면 항상 인터넷 연결을 허용합니다.

> ⚠ **주의**
> 허용할 IP 주소로 등록하면 해당 IP 주소의 컴퓨터가 웜이나 트로이목마에 감염되어 악성코드를 보내더라도 차단하지 않습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **허용/차단 IP 주소**에서 **설정하기**를 누릅니다.

3 **허용 주소** 탭에서 **추가**를 누릅니다.

4 <IP 주소 추가/수정>의 **입력 방법**에서 IP 주소 입력 방법을 선택하고 입력 방법에 따라 **IP 주소**를 입력합니다.

- 단일 IP 주소: 허용할 특정 IP 주소를 입력합니다.
  - IP 주소: 허용할 컴퓨터의 IP 주소를 입력합니다.
- IP 주소 범위: 시작 IP 주소와 종료 IP 주소 사이에 있는 IP 주소를 허용합니다.
  - 시작 IP 주소: 허용할 IP 주소 범위의 처음 IP 주소를 입력합니다.
  - 종료 IP 주소: 허용할 IP 주소 범위의 마지막 IP 주소를 입력합니다.
- 서브넷 마스크: IP 주소와 서브넷 마스크를 입력하여 IP 주소 범위를 지정합니다.
  - IP 주소: IP 주소를 입력합니다.
  - 서브넷 마스크: 서브넷 마스크를 입력합니다.

5 **확인**을 누릅니다.

6 허용 IP 주소 목록에 입력한 IP 주소가 등록되었는지 확인합니다.

참고

허용 IP 주소 목록에서 수정할 목록을 선택하고 **수정**을 누르면 <IP 주소 추가/수정>에서 수정할 수 있습니다. 목록에 추가된 허용 IP 주소를 삭제하려면, 삭제할 목록을 누르고 **삭제**를 누릅니다. 삭제를 누르면, **선택한 IP 주소를 허용/차단 IP 주소 목록에서 삭제하시겠습니까?** 라는 메시지가 나타납니다.

7 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

차단 주소

차단 주소에 등록된 IP는 방화벽 규칙에 관계없이 항상 인터넷 연결을 차단합니다. 차단 IP 주소는 허용 IP 주소보다는 우선 순위가 낮지만 방화벽의 네트워크 규칙과 프로그램 규칙보다는 우선 순위가 높아서 방화벽 규칙과 관계없이 인터넷 연결을 차단하고 네트워크 침입 차단 규칙도 적용되지 않습니다.

참고

차단할 IP 주소로 등록해도 해당 IP 주소로 보내는 패킷은 차단하지 않습니다. 해당 IP 주소에서 들어오는 패킷만 차단합니다.

계속 차단 IP 주소 목록

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **허용/차단 IP 주소**에서 **설정하기**를 누릅니다.

3 **차단 주소** 탭의 **계속 차단 IP 주소 목록**에서 **추가**를 누릅니다.

4 <IP 주소 추가/수정>의 **입력 방법**에서 IP 주소 입력 방법을 선택하고 입력 방법에 따라 **IP 주소**를 입력합니다.

- 단일 IP 주소: 차단할 특정 IP 주소를 입력합니다.
  - IP 주소: 차단할 컴퓨터의 IP 주소를 입력합니다.
- IP 주소 범위: 시작 IP 주소와 종료 IP 주소 사이에 있는 IP 주소를 차단합니다.
  - 시작 IP 주소: 차단할 IP 주소 범위의 처음 IP 주소를 입력합니다.
  - 종료 IP 주소: 차단할 IP 주소 범위의 마지막 IP 주소를 입력합니다.
- 서브넷 마스크: IP 주소와 서브넷 마스크를 입력하여 IP 주소 범위를 지정합니다.
  - IP 주소: IP 주소를 입력합니다.
  - 서브넷 마스크: 서브넷 마스크를 입력합니다.

5 **확인**을 누릅니다.

6 계속 차단 IP 주소 목록에 입력한 IP 주소가 등록되었는지 확인합니다.

참고

계속 차단 IP 주소 목록에서 수정할 목록을 선택하고 **수정**을 누르면 <IP 주소 추가/수정>에서 수정할 수 있습니다. 목록에 추가된 차단 IP 주소를 삭제하려면, 삭제할 목록을 누르고 **삭제**를 누릅니다. 삭제를 누르면, **선택한 IP 주소를 허용/차단 IP 주소 목록에서 삭제하시겠습니까?** 라는 메시지가 나타납니다.

7 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

임시 차단 IP 주소 목록

<네트워크 침입 차단>에서 **공격자 IP 주소 임시 차단**을 선택하면 웜이나 트로이목마에 감염된 패킷을 보낸 컴퓨터의 접근을 임시로 차단합니다. 차단된 컴퓨터에서 보내는 패킷은 감염 여부를 확인하지 않고 무조건 차단합니다. 임시로 차단된 IP 주소는 30분이 지나면 임시 차단 목록에서 삭제됩니다. 임시 차단 목록에서 삭제되면 다시 패킷을 받아올 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **네트워크 보안**의 **네트워크 침입 차단**에서 **설정하기**를 누릅니다.

3 **네트워크 침입 차단 사용**을 선택합니다.

4 **공격자 IP 주소 임시 차단**을 선택합니다.

5 **임시 차단 IP 보기**를 누릅니다.

6 임시 차단 IP 주소 목록에서 등록된 IP 주소를 확인합니다.

- 임시 차단 IP 주소: 임시로 차단한 IP 주소를 보여 줍니다.
- 임시 차단 만료 시간: 임시로 차단한 IP 주소는 30분이 지나면 목록에서 자동으로 삭제됩니다. 자동으로 IP 주소가 삭제될 때까지 남은 시간을 보여줍니다.

참고

임시 차단 만료 시간이 지난 후에 동일한 IP 주소가 다시 등록될 경우 다시 등록된 시점부터 다시 30분간 임시 차단합니다.

- 새로 고침: 임시 차단 IP 주소 목록을 새로 고쳐서 가장 최근에 임시로 차단한 IP 주소 목록을 보여줍니다.
- 삭제: 임시 차단 IP 주소 목록에 등록된 IP 주소를 삭제하여 임시 차단하지 않습니다.
- IP 추적: 임시 차단 IP 주소에 등록된 IP 주소를 선택하면 <IP 주소 추적 결과>에서 차단한 컴퓨터에 대한 정보를 확인할 수 있습니다.
  - 추적 IP 주소: 차단한 컴퓨터의 IP 주소입니다.
  - NetBIOS 이름: 차단한 컴퓨터의 이름입니다.
  - IP 라우팅 정보: 차단한 컴퓨터가 지나온 라우터의 정보입니다.
- 계속 차단: 신뢰할 수 없는 IP 주소인 경우 계속 차단을 눌러 계속 차단 IP로 등록할 수 있습니다. 계속 차단으로 등록한 IP 주소는 임시 차단 IP 주소 목록에서 계속 차단 IP 주소 목록으로 이동하여 등록됩니다.

7 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

7장
웹 보안

피싱 사이트 차단 사용하기

피싱(Phishing)은 개인 정보(Private Data)와 낚시(Fishing)의 합성어입니다. 피싱은 유명 회사의 웹사이트를 위조한 피싱 사이트를 만든 다음 인터넷 이용자에게 메일을 보내 위조한 웹사이트에 계좌 번호나 비밀번호와 같은 개인 정보를 입력하도록 유인하고 인터넷 이용자가 위조된 웹사이트에 개인 정보를 입력하면 이를 수집해 계좌에서 돈을 빼내거나 개인 정보를 범죄에 악용하는 사기 행위입니다. V3 IS 8.0은 피싱 사이트라고 알려진 사이트에 대한 정보를 갖고 있습니다. 이 정보를 이용하여 웹브라우저에서 접속한 사이트가 피싱 사이트인지 확인하여 피싱 사이트인 경우 차단합니다.

참고

Microsoft Internet Explorer로 웹사이트에 접속할 때만 차단합니다.

참고

V3 IS 8.0은 피싱으로 알려진 사이트에 대한 정보를 항상 업데이트합니다. 그러나, 피싱 사이트였던 곳이 관리자나 회사의 변경으로 정상적인 사이트로 운영될 경우 해당 사이트에 대한 정보를 수집하지 못할 수도 있습니다.

7

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 피싱 사이트 차단은 다음의 2가지 방법 중에서 선택하여 실행할 수 있습니다.

- **웹 보안**의 피싱 사이트 차단에서 **사용 안 함**에서 마우스를 눌러 **사용**을 선택합니다.
- 환경 설정의 피싱 사이트 차단에서 **피싱 사이트 차단**을 선택합니다.

참고

피싱 예외 사이트를 등록하려면 피싱 사이트 차단에서 설정할 수 있습니다.

웹사이트 필터링 사용하기

필터링할 웹사이트 목록에 등록된 웹사이트에 접속하면 접속을 차단하고 웹사이트 차단 페이지가 나타납니다. 성인 사이트나 도박 사이트와 같은 유해한 웹사이트를 등록하거나 회사나 단체에서 접속이 금지된 사이트를 등록하면 유해 사이트 접속으로 인한 문제를 예방할 수 있습니다.

참고

Microsoft Internet Explorer로 웹사이트에 접속할 때만 차단합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 웹사이트 필터링은 다음의 2가지 방법 중에서 선택하여 실행할 수 있습니다.

- **웹 보안**의 웹사이트 필터링에서 **사용 안 함**에서 마우스를 눌러 **사용**을 선택합니다.
- 환경 설정의 웹사이트 필터링에서 **웹사이트 필터링 사용**을 선택합니다.

참고

필터링할 웹사이트 주소를 추가하려면 웹사이트 필터링에서 설정할 수 있습니다.

피싱 사이트 차단 설정

피싱 사이트 차단 여부를 선택하고, 피싱 사이트 차단에서 제외할 사이트를 등록하고 수정할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **웹 보안**의 **피싱 사이트 차단**에서 **설정하기**를 누릅니다.

3 **피싱 사이트 차단**을 선택합니다.

- 피싱 사이트 차단: V3 IS 8.0이 가지고 있는 피싱 사이트 정보에 따라 피싱 사이트로 알려진 경우 해당 웹사이트로 접근하는 것을 차단합니다.

4 피싱 사이트 차단에서 제외할 웹사이트가 있다면, **피싱 사이트 차단 예외 사용**을 선택합니다.

- 피싱 사이트 차단 예외 사용: 피싱 사이트로 알려진 웹사이트이더라도 차단하지 않습니다.

⚠ 주의

피싱 사이트로 알려진 웹사이트를 피싱 예외 사이트에 등록하면 V3 IS 8.0은 해당 사이트의 피싱 여부를 검사하지 않고 차단하지도 않습니다.

5 **피싱 예외 사이트 목록**에서 **추가**를 누릅니다.

6 <피싱 예외 사이트 추가/수정>에서 피싱 검사 예외 사이트를 입력합니다. 피싱 검사 예외 사이트에 입력한 웹사이트에 대해서는 피싱 사이트 여부를 판단하지 않습니다.

7 **확인**을 누릅니다.

8 피싱 예외 사이트 목록에 입력한 내용이 추가되었는지 확인합니다.

참고

피싱 예외 사이트 목록에 있는 웹사이트를 선택하고 **수정**을 누르면, <피싱 예외 사이트 추가/수정>에서 피싱 검사 예외 사이트 주소를 수정할 수 있습니다. 피싱 예외 사이트 목록에 추가된 웹사이트를 선택하고 **삭제**를 누르면, **선택한 웹사이트를 피싱 예외 사이트 목록에서 삭제하시겠습니까?** 라는 메시지가 나타납니다. 삭제하려면 **예**를 누릅니다.

9 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

웹사이트 필터링 설정

특정한 웹사이트의 연결을 차단하도록 웹사이트 주소를 추가하거나 등록된 주소를 수정할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **웹 보안**의 **웹사이트 필터링**에서 **설정하기**를 누릅니다.

3 **웹사이트 필터링 사용**을 선택합니다.

4 **필터링할 웹사이트 목록**에서 **추가**를 누릅니다.

5 <필터링할 웹사이트 추가/수정>에서 필터링할 웹사이트 주소를 입력합니다.

- 필터링할 웹사이트 입력: 차단할 웹사이트 주소를 입력합니다. 필터링할 웹사이트 주소는 URL이나 IP 주소로 입력할 수 있으며, 별표(*)를 사용하면 관련된 웹사이트를 한 번에 등록할 수 있습니다. http://*.example.com을 입력하면 http://www.example.com과 http://blog.example.com, http://mail.example.com를 모두 차단하지만, http://*와 같이 모든 사이트 차단은 사용할 수 없습니다.

참고

필터링할 웹사이트 주소는 http 이외의 프로토콜은 지원하지 않습니다.

- 최근 접속한 웹사이트: 최근에 접속한 웹사이트를 모두 차단할 때 선택합니다. **불러오기**를 누르면 Microsoft Internet Explorer로 최근에 접속한 웹사이트의 목록이 나타납니다. 목록에서 차단할 웹사이트의 주소를 선택합니다.
- 하위 웹사이트 추가: 필터링할 웹사이트의 하위 웹사이트까지 모두 차단합니다.

참고

웹사이트 필터링은 Microsoft Internet Explorer만 지원합니다.

6 **확인**을 누릅니다.

7 선택한 웹사이트가 필터링할 웹사이트 목록에 등록되었는지 확인합니다.

8 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

8장
메일 보안

스팸 메일 차단 사용하기

스팸 메일은 인터넷을 통하여 다수의 사람에게 대량 발송하는 원하지 않는 상업성 메일을 말합니다. 스팸 메일은 메일을 받는 사람이 원하지 않는 내용으로 보통 상업적 목적을 띄고 있는 경우가 많습니다. 또한, 메시지 내용과 더불어 일정 기간 동안 메일을 대량으로 발송하는 경우를 스팸 메일로 간주합니다. 스팸 메일의 문제점은 받는 사람의 시간을 낭비하고, 정신적인 피로와 사용자의 네트워크나 컴퓨터 자원을 낭비하는 정신적, 물질적인 피해를 야기합니다. 이러한 스팸 메일을 차단하기 위해 다양한 방법을 연구 개발하고 있으나, 인터넷의 특성으로 인해 완벽한 차단 기술 개발은 거의 가능하지 않은 것으로 알려져 있습니다. V3 IS 8.0의 스팸 메일 차단 기능은 사용자가 설정한 스팸 키워드와 스팸 필터링을 사용하여 스팸으로 알려진 단어를 포함한 메일이 있는 경우 실시간으로 차단하여 사용자 불편을 최소화하고 있습니다.

스팸 메일 차단 사용하기

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 스팸 메일 차단은 다음의 2가지 방법 중에서 선택하여 실행할 수 있습니다.

- 메일 보안의 스팸 메일 차단에서 **사용 안 함**에서 마우스를 눌러 **사용**을 선택합니다.
- 환경 설정의 허용/차단 메일 설정의 스팸 메일 차단에서 **스팸 메일 차단 사용**을 선택합니다.

참고

스팸 차단 규칙 설정과 허용/차단 메일에서 규칙을 설정할 수 있습니다.

스팸 메일 예방 방법

❖ 메일 주소를 공개적인 웹사이트에 올리거나 보내지 마십시오. 스팸 메일을 발송하는 사람들은 주로 인터넷에 공개된 메일 주소를 수집하여 스팸 메일을 발송합니다.

❖ 스팸 메일을 받은 후, 수신 거부를 요청하지 마십시오. 메일을 더 이상 받고 싶지 않으면 수신 거부를 누르십시오. 라고 안내하는 스팸 메일은 해당 메일 주소가 실제 사용하고 있는 주소인지 확인하기 위한 수단으로 악용되는 경우가 많습니다. 따라서, 자신이 직접 가입한 메일링 서비스가 아닌 경우에 수신 거부를 신청하면, 더 많은 스팸 메일을 받을 수 있습니다.

❖ 스팸 메일을 절대 열거나 읽지 마십시오. 메일에 응답하지 않고 살짝 열어보기만 해도 메일에 숨겨져 있는 특별한 html 코드를 통해 스팸 메일을 보낸 사람은 메일을 받는 사람이 열어본 것을 바로 알 수 있으며 사용 중인 메일 주소로 간주하여 더 많은 스팸 메일을 보내게 됩니다. 특히 메일 클라이언트 프로그램의 미리 보기 기능은 사용자가 메일을 열어 보는 것과 같으므로 이 기능을 끄고 사용하십시오.

❖ 웹사이트를 운영하거나 공개된 곳에 메일 주소를 올려야 하는 경우에는 메일 주소를 사람들은 읽을 수 있지만, 프로그램은 읽을 수 없는 형태로 변형하면, 스팸 메일을 보내는 사람들이 프로그램을 이용하여 메일 주소를 수집하는 것을 예방할 수 있습니다. 예를 들어 내 메일 주소가 myemail@sample.com이라면 myemail'at'sample'dot'com으로 변형할 수 있습니다.

❖ V3 IS 8.0의 PC 실시간 검사와 스팸 메일 차단을 항상 실행하여 악성코드의 설치를 예방합니다. 또한, 의심스러운 첨부 파일은 절대로 열지 말고 바로 삭제하십시오.

❖ 공짜 웹 메일 계정을 공개용 메일 주소로 사용합니다. 개인용 메일 주소는 친구나 업무용으로만 사용합니다. 개인용 메일 주소를 사용하여 웹 서비스에 가입하거나 특별 행사에 응모하지 않는 것이 좋습니다.

❖ 스팸 메일 발송자에게 수집된 메일 주소를 계속 사용하는 경우, 스팸 메일을 방지하는데 한계가 있습니다. 따라서, 스팸 메일이 급격하게 증가하고 있다면 메일 주소 변경을 고려하는 것이 좋습니다.

메일 검사 설정

POP3를 통해 받는 메일과 SMTP를 통해 보내는 메일에 첨부된 파일의 감염 여부를 실시간으로 검사하여 감염된 첨부 파일이 있으면 검사 설정에 따라 치료하거나 차단합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **메일 보안**의 **메일 검사**에서 **설정하기**를 누릅니다.

3 **받는 메일 실시간 검사(POP3)**를 선택합니다.

- 받는 메일 실시간 검사(POP3): POP3를 통해 받는 메일에 첨부된 파일을 실시간 검사합니다.

4 **보내는 메일 실시간 검사(SMTP)**를 선택합니다.

- 보내는 메일 실시간 검사(SMTP): SMTP를 통해 보내는 메일에 첨부된 파일의 감염 여부를 실시간 검사합니다.

5 메일 검사 설정에서 **검사 대상 선택**을 선택합니다.

- 모든 파일: 받는 메일과 보내는 메일에 첨부된 모든 종류의 파일을 검사합니다.
- 감염되기 쉬운 파일(실행 파일, 매크로 파일, 스크립트 파일): EXE, DLL, OCX, SCR, COM 등의 실행 파일, XLS, SHS, DOT 등의 매크로 파일, PIF, VBS, JS, BAT, INI 등의 스크립트 파일과 같이 악성코드 감염 위험이 있는 첨부 파일을 검사합니다.
  - 추가로 검사할 확장자(예: dat/txt/tmp): 감염되기 쉬운 파일과 사용자가 입력한 확장자를 가진 첨부 파일을 추가로 검사합니다. 입력한 확장자 간의 구분은 '/'를 입력해야 하며 최대 260자까지 입력할 수 있습니다.
- 유해 가능 프로그램: 첨부된 파일이 유해 가능 프로그램인지 검사합니다.
- 압축 파일: 메일에 첨부된 압축 파일의 감염 여부를 검사합니다. 검사하는 압축 파일 형식은 **사용자 지정**을 눌러 <압축 파일 검사 설정>에서 선택할 수 있습니다.

6 **받는 메일(POP3) 치료 방법 선택**을 선택합니다.

- 악성코드: 바이러스나 스파이웨어에 감염된 첨부 파일을 발견했을 때 치료하는 방법을 설정합니다.
  - 그대로 두기: 감염된 첨부 파일을 치료하지 않고 감염된 상태 그대로 둡니다.

- 치료하기: 치료 가능한 파일인 경우 감염된 첨부 파일을 치료합니다. 단, 검사 결과 감염된 파일이 치료 불가 상태인 경우에는 해당 첨부 파일을 삭제합니다. 악성코드 치료 방법 선택의 기본 값입니다.
- 삭제하기: 감염된 첨부 파일을 치료하지 않고 삭제합니다.

- 감염된 압축 파일: 첨부된 압축 파일이 악성코드에 감염된 경우 치료하는 방법을 설정합니다.
  - 그대로 두기: 메일에 첨부되어 있는 감염된 압축 파일을 치료하지 않고 감염된 상태 그대로 둡니다. 감염된 압축 파일 치료 방법 선택의 기본 값입니다.
  - 삭제하기: 메일에 첨부되어 있는 감염된 압축 파일을 치료하지 않고 삭제합니다.
- 치료나 삭제 전 감염된 파일을 검역소로 보내기: 설정된 치료 방법에 따라 감염된 첨부 파일을 치료 또는 삭제할 경우, 해당 파일을 미리 검역소에 백업합니다. 검역소 백업은 지정한 폴더에 감염된 원본 파일을 실행 불가능한 형태로 변경하여 보관합니다. 감염된 원본 파일을 검역소에 그대로 백업할 경우 해당 파일을 다시 실행하여 다른 파일을 감염시킬 수 있기 때문입니다.
- 경고 메일(POP3)보내기: 받는 메일 검사 중 악성코드를 발견하면, 해당 메일을 보낸 사람의 주소로 경고 메일을 발송합니다.
- 경고 메일 설정: 경고 메일을 보내는 사람의 메일 주소 및 경고 메일 발송 정보를 설정합니다.
  - 보내는 사람 메일 주소: 경고 메일을 보내는 사람의 메일 주소를 입력합니다.
  - SMTP 서버 주소: SMTP 서버 주소를 입력합니다.
  - SMTP 포트: SMTP 서버의 포트 번호로 기본적으로 25번 포트를 많이 사용합니다.
  - 서버 접속 ID: SMTP 서버에 접속할 수 있는 사용자 ID를 입력합니다.
  - 서버 접속 암호: SMTP 서버 사용자 ID의 비밀번호를 입력합니다.
  - 확인: 설정한 내용을 저장하고 창을 닫습니다.
  - 취소: 설정한 내용을 저장하지 않고 창을 닫습니다.

7 검사 포트 설정을 설정합니다.

- 검사할 POP3 포트: POP3를 통해 메일을 받을 때 사용하는 통신 포트를 감시합니다. 기본 값은 110번입니다.

- 검사할 SMTP 포트: SMTP를 통해 메일을 보낼 때 사용하는 통신 포트를 감시합니다. 기본적으로 25번 포트를 많이 사용합니다. 통신 포트가 여러 개인 경우, 포트 간의 구분은 '/'를 사용해서 입력합니다. (예)25/119/50

참고

검사 포트에 값을 잘못 입력하면 **포트 번호는 1~65534까지 입력할 수 있습니다.** 라는 메시지가 나타납니다.

8 **기타 설정**을 설정합니다.

- 검사할 메일의 최대 크기: 첨부 파일의 크기가 큰 경우 파일 검사 시간이 많이 소요될 수 있습니다. 메일을 통해 전파되는 악성코드들은 대체로 크기가 크지 않으며, 실시간 검사를 실행한 상태에서 첨부 파일을 다운로드하여 실행하면 다시 한번 실시간 검사가 감염 여부를 검사할 수 있습니다. 따라서, 사용자가 적절한 크기의 메일 용량을 지정하여 메일 검사를 위한 시스템 자원의 낭비를 최소화하고, 메일 서버와 메일 클라이언트 사이의 통신 문제를 해결하는데 도움이 될 수 있습니다. 검사할 메일의 최대 크기는 1~10MB 사이에서 입력할 수 있으며 기본 값은 3MB입니다.

참고

검사할 메일의 최대 크기에 잘못 값을 입력하면, **검사할 메일의 최대 크기는 1~10MB 범위에서 입력할 수 있습니다.** 라는 메시지가 나타납니다.

- POP3 타임 아웃 방지 시간: 첨부 파일의 용량이 큰 경우 검사 시간이 오래 걸려 받은 메일이 취소될 수 있으므로 검사를 마칠 때까지 POP3 서버와 클라이언트에 타임 아웃 방지 메시지를 보냅니다. 타임 아웃 방지 메시지를 보내는 시간은 3초에서 20초 사이에서 설정할 수 있으며 기본 값은 10초 입니다.

참고

POP3 타임 아웃 방지 시간에 잘못된 값을 입력하면, **POP3 타임 아웃 방지 시간은 3~20초 범위에서 입력할 수 있습니다.** 라는 메시지가 나타납니다.

9 피싱 메일을 차단하려면 **피싱 메일 차단**을 선택합니다.

10 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

허용/차단 메일 설정

스팸 메일 차단

POP3를 통해 받는 메일을 Regular Expression(정규식)이나 사용자가 추가한 특정 단어, 특정 메일 주소를 포함한 메일을 스팸으로 판단하여 메일 수신을 차단합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **메일 보안**의 **스팸 메일 차단**에서 **설정하기**를 누릅니다.

3 **스팸 메일 차단 사용**을 선택합니다.

4 **스팸 메일 차단 규칙 설정**에서 스팸으로 분류할 단어를 입력한 후 **추가**를 누릅니다.

- 추가: 스팸으로 분류할 단어를 입력하고 추가를 누르면 스팸으로 분류할 단어에 입력한 단어가 추가됩니다.
- 삭제: 스팸으로 분류할 단어에 추가된 규칙 중 삭제할 항목을 선택하고 삭제를 누르면 **스팸 메일 차단 규칙을 삭제하시겠습니까?** 라는 메시지가 나타납니다. 삭제할 항목이 맞으면 **예**를 누릅니다.
- 상세 설정: 특정 단어가 메일 제목이나 본문, 메일 주소에 포함되어 있는 경우 스팸 메일로 차단하도록 설정합니다. 상세 설정을 누르면, <스팸 차단 규칙 설정>에서 상세 규칙을 설정할 수 있습니다.
- 스팸으로 분류된 메일 주소를 자동 차단 메일 목록에 추가: 스팸 메일 차단 규칙에 의해 스팸 메일로 처리된 메일 주소를 자동으로 차단 메일 목록에 추가합니다.

5 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

스팸 차단 규칙 설정

사용자가 직접 스팸으로 분류할 차단 규칙을 설정합니다. 스팸 차단 규칙 설정에서는 차단할 특정 단어를 입력하거나 차단할 규칙 범위와 스팸 메일로 판단하기 위한 문자열 검색 방식을 선택할 수 있습니다. 스팸 차단 규칙에 따라 메일의 제목이나 본문을 검사해서 스팸 차단 규칙에 해당 되는 메일은 제목에 [SPAM]이라는 표시를 합니다.

참고

스팸 메일 차단은 POP3 프로토콜로 받는 메일에 대해서만 사용할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘( )을 더블 클릭합니다.

2 **메일 보안**의 **스팸 메일 차단**에서 **설정하기**를 누릅니다.

3 **스팸 메일 차단 사용**을 선택합니다.

4 **스팸 메일 차단 규칙 설정**에서 **상세 설정**을 누릅니다.

5 <스팸 차단 규칙 설정>에서 스팸 차단 규칙을 만듭니다.

- 우선 순위 조정: 스팸 차단 규칙의 차단 우선 순위를 조정합니다. ▲을 누르면, 현재 선택한 내용이 한 단계 위로 이동합니다. ▼을 누르면, 현재 선택한 내용이 한 단계 아래로 이동합니다.
- 추가: <스팸 차단 규칙 상세 설정>에서 선택한 규칙 범위에 따라 스팸 차단 규칙을 등록합니다.
- 수정: 스팸 차단 규칙에 등록된 규칙을 수정합니다.
- 삭제: 선택한 스팸 차단 규칙을 삭제합니다.
- 규칙 사용 여부: 현재 규칙을 사용하고 있는지 보여줍니다. 규칙을 사용하는 경우 사용으로 표시하고, 사용하지 않는 경우 사용 안 함으로 표시합니다. 사용 여부 선택은 해당 규칙을 더블 클릭하거나 수정 버튼을 누르고 <스팸 차단 규칙 상세 설정>에서 스팸 차단 규칙 사용을 선택하거나 선택 해제합니다.
- 규칙 내용: <스팸 차단 규칙 상세 설정>에서 설정한 규칙 내용을 보여줍니다.
- 불러오기: 사용자가 미리 만들어 둔 스팸 차단 규칙을 불러와서 차단 규칙에 등록합니다.
- 저장하기: 현재 만든 스팸 차단 규칙을 저장합니다. 저장하기를 누르면 저장할 위치와 파일 이름을 지정하여 저장할 수 있으며, 파일 형식은 rul 파일로 저장됩니다.

- 확인: 현재 내용을 저장하고 창을 닫습니다.
- 취소: 현재 내용을 저장하지 않고 창을 닫습니다.

참고

스팸 차단 규칙은 여러 개를 등록할 수 있으며, 스팸 차단 규칙 적용 순서를 변경할 수 있습니다. 우선 순위가 높은 스팸 차단 규칙에 의해 먼저 차단되면 우선 순위가 낮은 나머지 규칙은 비교하지 않습니다.

스팸 차단 규칙 상세 설정

<스팸 차단 규칙 설정>에서 추가를 눌러 사용자가 직접 차단할 규칙 범위와 차단할 단어를 입력합니다.

- 스팸 차단 규칙 사용: 사용자가 입력한 규칙 범위와 차단할 단어로 만들어진 차단 규칙을 스팸 차단 규칙으로 사용합니다.
- 규칙 범위 선택: 스팸 메일을 차단할 규칙의 범위를 선택하고, 차단할 단어를 입력합니다.
- 규칙 범위 선택
  - 메일 제목에 특정 단어 포함: 메일 제목에 사용자가 입력한 차단할 단어가 포함된 경우 해당 메일을 스팸 메일로 판단하여 차단합니다.
  - 메일 내용에 특정 단어 포함: 메일 내용에 사용자가 입력한 차단할 단어가 포함된 경우 해당 메일을 스팸 메일로 판단하여 차단합니다.
  - 보낸 사람에 특정 단어 포함: 보낸 사람 주소에 사용자가 입력한 차단할 단어가 포함된 경우 해당 메일을 스팸 메일로 판단하여 차단합니다.
  - 받는 사람에 특정 단어 포함: 받는 사람 주소에 사용자가 입력한 차단할 단어가 포함된 경우 해당 메일을 스팸 메일로 판단하여 차단합니다.
- 차단할 단어 입력: 규칙 범위 선택을 한 후, 차단할 단어를 입력하고 **추가**를 누릅니다.
  - 세부 조건 설정: <스팸 차단 세부 조건 설정>에서 차단할 단어에 입력한 단어를 스팸으로 판단하기 위한 문자열 검색 방식을 선택합니다.
- 규칙 조건 선택
  - 하나라도 포함되면 차단함: **차단할 단어 입력**에 입력한 단어가 메일 중에 하나라도 포함되어 있으면 해당 메일을 스팸 메일로 판단하여 차단합니다.

- 모두 포함되면 차단함: **차단할 단어 입력**에 입력한 단어가 메일 중에 모두 포함되어 있으면 해당 메일을 스팸 메일로 판단하여 차단합니다.

- 완성된 스팸 차단: 선택한 스팸 차단 규칙을 조합하여 문장으로 보여줍니다. 선택한 규칙이 여러 개 있는 경우 고급 설정에서 선택한 **그리고, 또는**으로 규칙들을 조합합니다.
- 고급 설정: <스팸 차단 고급 설정>에서 규칙 조건 설정을 할 수 있습니다.

스팸 차단 추가 조건 설정

스팸 차단 규칙의 **차단할 단어 입력**에 입력된 단어를 스팸 메일로 판단하기 위한 문자열 검색 방식을 선택합니다.

- 기본 문자열 검색 방식 사용: 입력한 문자열 그대로 검색합니다.
- 사용자 정의 정규 표현식(Regular Expression) 사용: 사용자가 직접 정규 표현식 문법에 맞도록 정규 표현식을 만들어서 문자열 검색 규칙을 설정하는 방법입니다.
- 기본 정의 정규 표현식(Regular Expression) 사용: V3 IS 8.0에 정의되어 있는 정규 표현식입니다. V3 IS 8.0에 정의되어 있는 정규 표현식은 다음과 같습니다.
  - 모두 빈 칸인 경우 차단: 사용자가 선택한 규칙 범위에 있는 단어가 모두 빈 칸인 경우 해당 메일을 스팸 메일로 판단하여 차단합니다.
  - 모두 영어인 경우 차단: 사용자가 선택한 규칙 범위에 있는 단어가 모두 영어인 경우 해당 메일을 스팸 메일로 판단하여 차단합니다.
  - 모두 숫자인 경우 차단: 사용자가 선택한 규칙 범위에 있는 단어가 모두 숫자인 경우 해당 메일을 스팸 메일로 판단하여 차단합니다.
  - HTML을 포함하고 있는 경우 차단: 사용자가 선택한 규칙 범위에 있는 단어에 HTML 코드가 있는 경우 해당 메일을 스팸 메일로 판단하여 차단합니다.
  - URL을 포함하고 있는 경우 차단: 사용자가 선택한 규칙 범위에 있는 단어가 URL(예:http://www.aaa.com)이 있는 경우 해당 메일을 스팸 메일로 판단하여 차단합니다.
- 대소문자 구분: 차단할 단어 입력에 입력한 문자의 대소문자를 구분하여 차단합니다.

스팸 차단 고급 설정

<스팸 차단 고급 설정>에서 규칙 조건 설정을 설정할 수 있습니다. 규칙 조건은 <스팸 차단 규칙 상세 설정>의 규칙 범위에서 여러 개의 규칙을 만든 경우에 여러 개의 규칙들을 그리고(AND) 조건으로 조합해서 적용할 것인지 또는(OR) 조건으로 조합해서 적용할 것인지를 선택할 수 있습니다.

- 그리고(모든 조건이 일치하는 경우): 스팸 차단 규칙 상세 설정에서 선택한 여러 가지 규칙 중 여러 가지 규칙의 공통 조건을 가진 메일을 스팸 메일로 판단하여 차단합니다.
- 또는(한 조건이라도 일치하는 경우): 스팸 차단 규칙 상세 설정에서 선택한 여러 가지 규칙 중 한 조건이라도 일치하는 내용이 있는 경우 스팸 메일로 판단하여 차단합니다.

허용/차단 메일

스팸 메일을 차단하기 전에 사용자가 입력한 메일 주소에서 오는 메일을 허용하거나 차단합니다. 차단하는 경우 스팸 메일과 동일하게 메일 제목에 [SPAM]이라는 표시를 합니다.

허용 메일

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **메일 보안**의 **허용/차단 메일 주소**에서 **설정하기**를 누릅니다.

3 **허용 메일** 탭을 선택합니다.

4 **추가**를 누릅니다.

5 <메일 주소 추가/수정>에서 허용할 메일 주소를 입력합니다.

6 **확인**을 누릅니다.

7 허용 메일 주소 목록에 입력한 메일 주소가 등록되었는지 확인합니다.

차단 메일

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **메일 보안**의 **허용/차단 메일 주소**에서 **설정하기**를 누릅니다.

3 **차단 메일** 탭을 선택합니다.

4 **추가**를 누릅니다.

5 <메일 주소 추가/수정>에서 차단할 메일 주소를 입력합니다.

6 **확인**을 누릅니다.

7 차단 메일 주소 목록에 입력한 메일 주소가 등록되었는지 확인합니다.

참고

<메일 주소 추가/수정>에 입력한 메일 주소의 일부 문자열이 일치하는 경우에도 해당 메일을 허용하거나 차단합니다.

9장
PC 도구

PC 최적화

PC 최적화를 실행하면 필요없는 파일과 레지스트리 정보, 임시 파일을 청소하고 메모리 사용을 최적화합니다. PC 최적화는 하드 디스크 드라이브의 저장 공간을 차지하는 필요 없는 파일이나 임시 파일, 필요없는 레지스트리 정보를 청소하고 메모리 사용을 최적화하여 컴퓨터의 실행 속도를 빠르게 합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **HOME**에서 **PC 최적화**를 누릅니다.

참고

PC 도구의 PC 최적화에서 실행하기를 눌러도 PC 최적화를 실행할 수 있습니다.

3 <PC 최적화>에서 **최적화 항목**과 **진행 상태**를 보여줍니다.

4 PC 최적화를 마치면 **닫기**를 누릅니다.

참고

PC 최적화 항목은 PC 최적화 설정에서 선택할 수 있습니다.

파일 완전 삭제

파일 완전 삭제는 사용자가 선택한 파일이나 폴더를 완전히 삭제하여 불법 데이터 복구로 인해 개인 정보가 유출될 위험을 없애줍니다.

파일 완전 삭제 실행하기

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 도구**의 **파일 완전 삭제**에서 **실행하기**를 누릅니다.

3 <파일 완전 삭제>에서 **추가**를 누릅니다.

4 <찾아보기>에서 삭제할 폴더나 파일을 선택합니다. 폴더를 선택하면 해당 폴더 안에 있는 모든 파일이 삭제 대상으로 등록됩니다.

5 <파일 완전 삭제> 목록에 선택한 대상이 추가되면, **시작**을 누릅니다.

6 **파일 완전 삭제로 지운 파일은 복구할 수 없습니다. 계속 하시겠습니까?** 라는 메시지가 나타납니다. 삭제해도 되는 파일인지 확인한 후에 **예**를 누르면 삭제합니다.

7 **파일 완전 삭제를 마쳤습니다. 계속하려면, 폴더나 파일을 마우스로 끌어당겨 놓거나 추가 버튼을 누르십시오.** 라는 메시지가 나타나면 선택한 파일의 완전 삭제를 마치고 새로운 파일이나 폴더를 추가하여 파일 완전 삭제를 계속할 수 있습니다.

참고
네트워크 드라이브에 저장되어 있는 파일은 완전 삭제를 실행할 수 없습니다.

8 **마침**을 누릅니다.

탐색기에서 파일 완전 삭제하기

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **환경 설정**의 **기타 설정**에서 **탐색기 설정**을 선택합니다.

3 **Windows 탐색기 메뉴 사용**을 선택합니다.

4 **파일 완전 삭제**를 선택합니다.

5 **적용**을 누릅니다.

6 탐색기나 바탕 화면 등에서 삭제할 폴더나 파일에서 마우스 오른쪽을 눌러 **V3 파일 완전 삭제**를 선택합니다.

7 <파일 완전 삭제> 목록에 선택한 대상이 추가되면, **시작**을 누릅니다.

8 **파일 완전 삭제로 지운 파일은 복구할 수 없습니다. 계속 하시겠습니까?** 라는 메시지가 나타납니다. 삭제해도 되는 파일인지 확인한 후에 **예**를 누르면 삭제합니다.

9 **마침**을 누릅니다.

참고

파일 완전 삭제 수준은 파일 완전 삭제 설정에서 선택할 수 있으며, 탐색기 설정에서 파일 완전 삭제를 선택하면 탐색기에서 바로 **V3 파일 완전 삭제**를 사용할 수 있습니다. 단, 파일 완전 삭제는 폴더나 파일만 선택할 수 있으며, C나 D와 같은 드라이브를 선택하면 마우스 오른쪽 버튼을 눌러도 V3 파일 완전 삭제 메뉴가 나타나지 않습니다.

주의

파일 완전 삭제로 지운 파일은 다시 복구할 수 없으며 복구가 되더라도 원본 파일과 내용이 다르므로 삭제 전 반드시 지워도 되는 폴더나 파일인지 확인하십시오.

참고

파일을 완전히 지우려면 존재하고 있는 파일을 새로운 데이터로 반복해서 덮어 써야 합니다. Windows에서 파일을 삭제할 때마다 파일을 완전히 지우기 위해 파일을 반복해서 덮어 쓴다면 모든 작업이 매우 느려질 것입니다. 그래서 Windows는 파일을 삭제할 때 파일이 있는 위치만 표시되지 않도록 하고 원본 데이터는 삭제하지 않습니다. 파일 복구 프로그램은 이런 특징을 이용해 잘못 삭제한 파일을 다시 복구합니다. 삭제한 파일에 중요한 정보가 있다면 다른 사람이 파일을 복구해서 내용을 볼 수 있습니다. V3 IS 8.0은 중요한 정보가 있는 파일을 복구할 수 없도록 완전히 삭제합니다.

PC 최적화 설정

컴퓨터를 사용하면서 여러 프로그램을 설치하고 제거하면 하드 디스크 드라이브에 사용하지 않는 파일이 남거나 레지스트리에 필요없는 정보가 남을 수 있습니다. 그리고 웹 브라우저를 이용해 웹사이트를 열면 임시로 저장하는 파일이 하드 디스크 드라이브에 쌓입니다. 사용하지 않는 파일이나 레지스트리 정보, 임시 파일은 컴퓨터의 저장 공간을 낭비하고 컴퓨터의 실행 속도를 느리게 할 수 있습니다. 또한, 스파이웨어와 같은 악성 코드는 임시 파일에 남아 있는 개인 정보를 사용자 모르게 유출하기도 합니다. PC 최적화에서 최적화 대상을 선택하면 사용자가 선택한 영역을 청소하여 컴퓨터의 저장 공간을 늘리고 개인 정보가 유출되는 것을 예방할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 도구**의 **PC 최적화**에서 **설정하기**를 누릅니다.

3 **최적화 대상 선택**에서 청소 대상을 선택합니다.

- 시스템 영역: 컴퓨터에서 사용하지 않는 파일이나 레지스트리 정보를 청소합니다.
  - 설치/삭제: 프로그램을 설치하고 제거하는데 필요한 정보만 있고 실제로 컴퓨터에는 설치되어 있지 않은 프로그램에 대한 기록과 파일을 찾아서 청소합니다.
  - 레지스트리: 필요없는 레지스트리 정보를 지우거나 잘못된 레지스트리 정보를 원래 상태로 복원합니다.
  - 시작 프로그램: Windows의 시작 프로그램으로 등록되어 있지만 실제로 컴퓨터에는 설치되어 있지 않은 프로그램에 대한 기록을 찾아서 청소합니다.
- Internet Explorer 임시 인터넷 파일: Microsoft Internet Explorer가 저장한 다음과 같은 임시 파일을 청소합니다.
  - 쿠키: 쿠키는 웹사이트를 사용할 때 필요한 정보를 사용자의 컴퓨터에 작은 텍스트 파일 형태로 저장한 것입니다. 쿠키를 저장하도록 허용하지 않으면 웹사이트의 내용을 볼 수 없거나 사용자 지정 기능(지역 뉴스, 날씨, 주식 주문 등)을 사용하지 못할 수도 있습니다.

- 임시 인터넷 파일: Microsoft Internet Explorer에서 한 번 열어 본 웹페이지는 다음에 보다 빨리 열어 볼 수 있도록 Temporary Internet Files 폴더에 저장됩니다. 이 기능을 사용하면 사용자가 한 번 접속했던 웹페이지를 다시 열 때 하드 디스크 드라이브에 저장된 파일을 열기 때문에 오프라인 상태나 네트워크가 불안정한 상태일 때에도 웹페이지를 빠르게 볼 수 있습니다.
- 열어본 페이지 목록: Microsoft Internet Explorer에서 최근에 열어 본 페이지 목록입니다. Microsoft Internet Explorer의 보기->탐색 창->열어본 페이지 목록(ctrl+H)을 누르면 지난 며칠, 몇 주 동안 방문한 웹사이트 및 페이지가 링크된 열어본 페이지 목록 창이 나타납니다.
- 암호 자동 완성 기록: 웹사이트에서 입력한 비밀번호를 저장해 둔 기록입니다. 웹사이트의 주소와 입력한 아이디가 비밀번호를 저장할 때와 같으면 이전에 입력한 비밀번호를 자동으로 입력합니다.
- 폼 자동 완성 기록: 웹페이지의 입력 상자에 입력한 정보를 저장해 둔 기록입니다. 입력 상자에 정보를 입력할 때 이전에 입력했던 정보 중에서 일치할 가능성이 있는 정보를 보여 줍니다.

- Windows 임시 파일: Windows 운영체제가 임시로 저장한 파일을 청소합니다.
  - 임시 파일: Windows에서 최근에 사용한 파일을 임시로 저장해 둔 것입니다.
  - 내 최근 문서: 사용자가 최근에 열어 본 문서의 목록입니다. 내 최근 문서는 작업 표시줄에서 **시작->내 최근 문서**를 선택하면 확인할 수 있습니다.
  - 휴지통: 사용자가 컴퓨터에서 삭제한 파일이나 폴더를 임시로 보관하는 곳입니다. 휴지통을 비우면 휴지통에 보관하고 있던 파일이나 폴더가 사용자의 컴퓨터에서 완전히 삭제됩니다.

참고

Windows NT Workstation에서는 **휴지통**을 선택할 수 없습니다.

- 최근에 사용한 파일 목록: 컴퓨터에 설치된 프로그램에서 사용한 파일 목록을 청소합니다.
  - RealPlayer: RealPlayer에서 최근에 사용한 파일 목록입니다. RealPlayer의 **파일** 메뉴를 선택하면 확인할 수 있습니다.
  - 워드패드: 워드패드에서 최근에 사용한 파일 목록입니다. 워드패드의 **파일** 메뉴를 선택하면 확인할 수 있습니다.
  - 그림판: 그림판에서 최근에 사용한 파일 목록입니다. 그림판의 **파일** 메뉴를 선택하면 확인할 수 있습니다.

    - Windows Media Player: Windows Media Player에서 최근에 사용한 파일 목록입니다. Windows Media Player의 **파일** 메뉴를 선택하면 확인할 수 있습니다.
- 기타 실행 목록: 사용자가 컴퓨터에서 실행한 작업을 기록한 정보를 청소합니다.
    - 실행: **시작->실행** 메뉴에서 최근에 실행했었던 프로그램, 폴더, 문서, 웹사이트 목록입니다. <실행>의 **열기**에서 드롭다운()을 누르면 나타납니다.
    - 파일 찾기: **시작->검색** 메뉴에서 최근에 찾아본 파일 목록입니다.
    - 컴퓨터 찾기: **시작->검색** 메뉴에서 최근에 찾아본 컴퓨터 이름 목록으로 입력 상자에 나타납니다.
    - 텔넷: 텔넷 명령 모드로 원격 호스트에 접속한 기록입니다.
- 메모리 최적화: 프로그램이 사용하지 않는 메모리를 사용할 수 있도록 하여 메모리의 양을 늘립니다.
    - 사용자 메모리: 운영체제가 프로세스에서 사용하고 있는 사용자 영역의 메모리를 사용할 수 있도록 합니다.
    - 작업 집합(Working Set): 작업하고 있지 않는 프로세스가 가진 메모리를 사용할 수 있도록 합니다.
    - 캐시(Cache): 시스템 파일 캐시를 사용할 수 있도록 합니다.

4 **임시 파일 보관 기간**을 선택합니다. 임시 파일 보관 기간은 0~30일을 선택할 수 있으며, 기본 값은 7일입니다.

- 임시 파일 보관 기간: 임시 파일을 보관하는 기간을 설정합니다. 임시 파일을 삭제할 때 사용자가 설정한 보관 날짜를 지난 파일만 삭제합니다.

5 청소한 파일을 백업하려면, **청소한 대상 검역소로 보내기**를 선택합니다.

6 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

파일 완전 삭제 설정

Windows의 삭제와 달리 파일이 남기는 흔적까지 모두 지워서 복구 툴을 이용하여 해당 파일을 다시 복구할 수 없도록 합니다. 파일 완전 삭제로 지운 파일은 복구를 할 수 없거나 복구를 하더라도 원본 파일과 내용이 달라집니다. 따라서, 파일 완전 삭제로 필요한 파일만 지울 경우, 개인 정보 유출의 위험이 매우 낮아집니다. 파일 완전 삭제 설정에서는 사용자가 직접 삭제할 파일의 삭제 수준을 설정할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 도구**의 **파일 완전 삭제**를 누릅니다.

3 파일 완전 삭제 설정에서 슬라이더를 움직여 삭제 수준을 설정합니다. 기본 값은 보통입니다.

- 삭제할 수준 선택: 슬라이더를 움직여 파일을 삭제하는 수준을 선택합니다.
  - 아주 높음: P.Gutmann 알고리즘을 사용하여 파일을 35번 덮어 씁니다. 파일을 삭제하는 속도가 가장 느립니다.
  - 높음: US NSA Erasure 알고리즘을 사용하여 파일을 7번 덮어 씁니다. 파일을 삭제하는 속도가 느립니다.
  - 보통: US DoD 5220.22-M Standard(8-306/E, C and E)알고리즘을 사용하여 파일을 7번 덮어 씁니다.
  - 낮음: US DoD 5220.22-M Standard(8-306/E)알고리즘을 사용하여 파일을 3번 덮어 씁니다. 파일을 삭제하는 속도가 빠릅니다.
  - 아주 낮음: Single Pass 알고리즘을 사용하여 1번 덮어 씁니다. 파일을 삭제하는 속도가 가장 빠릅니다.

4 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

실행 차단 목록 설정

프로세스 실행 차단은 사용자가 선택한 폴더나 파일의 실행을 차단합니다. 회사나 단체에서 사용을 금지한 프로그램이 있는 경우 프로세스 실행 차단에 등록해 두면, 해당 프로그램이 PC에 설치되더라도 사용하지 못하게 할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 도구**의 **실행 차단 목록**을 누릅니다.

3 **프로세스 실행 차단 사용**을 선택합니다.

- 프로세스 실행 차단 사용: 실행 차단 목록에 추가한 폴더나 파일의 실행을 차단합니다.
  - 차단할 프로세스가 이미 동작 중일 때 그대로 두기: 실행 차단 목록에 등록된 파일이 차단 전에 이미 실행되어 있는 경우 해당 프로세스를 종료하지 않고 그대로 둡니다.
  - 차단할 프로세스가 이미 동작 중일 때 강제로 멈추기: 실행 차단 목록에 등록된 파일이 차단 전에 이미 실행되어 있는 경우 해당 프로세스를 강제로 멈추어 실행을 종료합니다.

4 실행 차단 목록에 차단할 폴더나 파일을 추가합니다.

- 폴더 추가: 차단할 폴더를 선택할 수 있습니다. 선택한 폴더의 파일만 차단하고 해당 폴더의 하위 폴더는 차단하지 않습니다.
- 파일 추가: 차단할 파일을 선택할 수 있습니다. 파일을 선택하고 나면 <실행 차단할 프로그램 내용>에서 차단할 파일에 대한 차단 방법을 선택할 수 있습니다.
- 삭제: 실행 차단 목록에 추가한 폴더나 파일을 목록에서 삭제하여 실행을 차단하지 않습니다. 차단할 프로그램을 선택하고 삭제를 누르면 **선택한 실행 차단 목록을 삭제하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면, 해당 프로그램을 목록에서 삭제합니다.

참고

실행 차단 목록에는 최대 30개까지 등록할 수 있습니다. 실행 차단 목록에는 %WINDIR%, %WINDIR%\System32, V3 IS 8.0 설치 폴더와 AhnLab Policy Center 관련 폴더나 파일은 등록할 수 없으며 사용자가 등록하더라도 차단하지 않습니다. 또한, USB 드라이브와 네트워크 경로에 있는 파일이나 폴더는 차단 목록에 등록할 수 없습니다.

참고

실행 차단 목록에는 32Bit, 64Bit 형식의 실행 파일만 등록할 수 있으며 16Bit 응용 프로그램을 실행 차단 목록에 등록하면 **프로세스 실행 차단은 16Bit 기반 응용 프로그램을 지원하지 않습니다.** 라는 메시지가 나타납니다.

주의

실행 차단 목록에 등록한 폴더나 파일이라도 사용자가 해당 폴더나 파일을 다른 위치로 복사해서 실행하는 경우에는 차단할 수 없습니다.

5 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

실행 차단할 프로그램 내용

실행 차단 목록에 파일을 추가하는 경우 실행 차단할 프로그램 내용에 대하여 선택할 수 있습니다.

- 파일 이름: 사용자가 선택한 경로에 있는 해당 파일의 실행만 차단합니다.
- 제품 이름: 차단할 프로그램의 제품 이름으로 실행을 차단합니다.
- 설명: 차단할 프로그램의 설명으로 실행을 차단합니다.

10장
환경 설정

알림 설정

Windows 작업 표시줄의 알림 영역에 알림 아이콘 표시 여부를 선택하고, 알림 창 표시 상황을 사용자가 직접 선택할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 환경 설정에서 **기타 설정**을 선택합니다.

3 **알림 설정** 탭을 누릅니다.

4 알림 아이콘과 알림 창 표시 여부를 선택합니다.

- 작업 표시줄에 V3 알림 아이콘 표시: Windows 작업 표시줄에 아이콘을 보여줍니다.
- 선택한 알림 상황에 알림 창 표시: 알림 설정에서 사용자가 선택한 상황이 발생했을 때 작업 표시줄에 알림 창을 보여줍니다. 알림 창에서는 발생한 상황에 따라 차단한 내용이나 감염된 악성코드 이름 등을 확인할 수 있습니다.
- 전체 화면 모드인 경우 알림 창 보이지 않기: 파워포인트에서 프리젠테이션을 하거나 워드나 게임 등에서 전체 화면 모드를 사용할 때 알림 창 발생을 금지합니다. 전체 화면 모드 상태에서 악성코드를 발견한 경우 모두 자동으로 치료하며 방화벽은 사용자에게 확인하지 않고 모두 차단 모드로 동작하여 사용자의 현재 작업을 방해하지 않습니다.

5 알림 설정에서 PC 검사, 네트워크 보안, 웹 보안, 메일 보안, PC 도구, 이벤트 메시지에서 알림이 필요한 상황을 선택합니다.

- PC 실시간 검사의 악성코드 치료 알림: PC 실시간 검사가 악성코드에 감염된 파일을 치료했을 때 알려줍니다.
- 메신저 실시간 검사의 악성코드 치료 알림: 메신저를 통해 받는 파일에 악성코드가 감염되었을 때 알려줍니다.
- 악성코드 치료 시 컴퓨터를 다시 시작해야 할 때 알림: 악성코드에 감염된 파일을 치료하기 위해 컴퓨터를 다시 시작해야 하는 경우에 알려줍니다.
- V3 감염 여부 검사 후 알림: V3 IS 8.0을 실행할 때 백신 자체가 악성코드에 감염되었는지 알려줍니다.
- hosts 파일 변경 알림: Windows의 hosts 파일의 변경이 있을 때 사용자에게 알려줍니다.

- 실행 파일이 공유 폴더에 복사되는 것을 차단했을 때 알림: 사용자 PC의 공유 폴더에 네트워크를 통해 다른 사용자가 실행 파일을 복사할 때 차단했음을 알려줍니다.
- 네트워크 침입 탐지 알림: 네트워크를 통해 사용자 PC에 침입 시도를 탐지했을 때 알려줍니다. V3 IS 8.0이 해당 공격을 탐지한 시점에 공격자 자체가 이미 연결된 세션을 종료한 경우에는 탐지했음을 알려줍니다. 네트워크 침입 탐지 알림 창에서는 V3 IS 8.0이 탐지한 침입의 이름과 상세 정보를 확인할 수 있습니다.
- 네트워크 침입 차단 알림: 네트워크를 통해 사용자 PC에 침입 시도를 차단했을 때 알려줍니다. V3 IS 8.0이 해당 공격을 탐지한 시점에 연결된 세션을 종료 가능한 경우에 침입을 차단하고 알려줍니다. 네트워크 침입 차단 알림 창에서는 V3 IS 8.0이 차단한 침입의 이름과 상세 정보를 확인할 수 있습니다.
- 프로그램이 인터넷 접근을 시도할 때 알림: 개인 방화벽의 프로그램 규칙 목록에 허용하거나 차단하도록 등록하지 않은 프로그램이 인터넷 연결을 시도하려고 할 때 알려줍니다. 알림 창에서 해당 프로그램의 인터넷 연결을 허용하거나 차단하도록 선택할 수 있습니다.
- 프로그램 규칙 업데이트가 필요할 때 알림: 개인 방화벽의 프로그램 규칙에 정의된 프로그램 중 규칙을 만들 때의 프로그램과 현재 네트워크에 연결하려는 프로그램이 다른 경우에 알려줍니다. 프로그램 규칙 업데이트가 필요할 때 알림은 규칙 생성 당시의 파일 경로, 파일 이름과 파일 고유 정보 확인을 선택한 경우 해당 정보들을 모두 비교하여 정보가 다른 경우 알림 창이 발생합니다.
- 피싱 사이트 차단 알림: 피싱으로 알려진 사이트에 접속하려고 할 때 해당 사이트 접속을 차단했음을 알려줍니다.
- 웹사이트 필터링 알림: 웹사이트 필터링 규칙에서 차단하는 웹사이트에 접근할 때 알려줍니다.
- 감염된 메일이 들어올 때 알림(POP3): POP3를 통해 사용자가 받는 메일이 감염되었을 때 알려줍니다.
- 감염된 메일이 나갈 때 알림(SMTP): SMTP를 통해 사용자가 보내는 메일이 감염되었을 때 알려줍니다.
- 메일 송수신 상태 알림: 받는 메일 실시간 검사(POP3)와 보내는 메일 실시간 검사(SMTP)에서 메일을 보내거나 받을 때 풍선 도움말로 메일의 송수신 상태를 알려줍니다. 메일을 받고 있는 경우에는 **POP3로 메일을 받고 있습니다.** 라는 풍선 도움말이 나타나고, 메일을 보내고 있는 경우에는 **SMTP로 메일을 보내고 있습니다.** 라는 풍선 도움말이 나타납니다.

- 피싱 메일을 차단했을 때 알림: 피싱 메일을 차단했을 때 알려줍니다.
- 스팸 메일을 차단했을 때 알림: 스팸 메일 차단 규칙에 스팸으로 분류한 단어가 제목이나 본문에 포함된 메일이 있는 경우 차단하여 알려줍니다.
- 차단 목록에 등록된 메일 주소를 차단할 때 알림: 차단하도록 등록한 주소에서 발송한 메일을 받으려고 할 때 차단하여 알려줍니다.
- 프로세스 실행 차단 알림: 사용자가 선택한 폴더나 파일의 실행을 차단했을 때 알려줍니다.
- 업데이트 시작/종료 알림: 업데이트를 시작할 때와 마쳤을 때 알려줍니다.
- V3 자체 보호 알림: 다른 프로그램이 V3의 동작을 방해하거나 중지하기 위해 V3 관련 파일, 프로세스, 레지스트리를 변경하거나 삭제를 시도할 경우 알려줍니다.
- 업데이트가 필요할 때 알림: 현재 사용하고 있는 엔진 파일이 7일 이상 지난 경우에 알려줍니다.
- 손상된 파일이 있을 때 알림(무결성 검사): 컴퓨터 시작할 때 V3 파일의 손상 여부를 확인하고 손상된 파일이 있는 경우 알려줍니다. 파일이 손상된 경우 V3 IS 8.0 실행을 마치고 엔진 업데이트를 해야 합니다.
- 예약 검사 알림: 사용자가 입력한 시간에 예약 검사를 시작할 때 알려줍니다.
- 백그라운드 검사 알림: 백그라운드 검사는 AhnLab Policy Center와 같은 관리 툴에 의해서 사용자에게 검사하는 화면이 보이지 않게 검사하는 기능입니다. 백그라운드 검사가 실행된 경우 관리 툴에서 설정한 상태에 따라 사용자가 백그라운드 검사를 멈추거나 멈추는 것이 금지될 수 있습니다.
- PC 검사/치료 알림: 정밀 검사나 사용자 목록 검사를 통해 검사하고 치료한 경우 알려줍니다. 검사 창을 최소화시켰거나 검사 후 다른 작업으로 검사와 치료 여부를 확인하기 힘든 경우에 사용하면 편리합니다.

6 **모두 선택**을 누르면 알림 설정에서 선택할 수 있는 알림 상황을 한 번에 모두 선택하고, **모두 취소**를 누르면 알림 설정에서 선택한 알림 상황을 모두 선택하지 않습니다.

7 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

보관 설정

PC 검사와 PC 최적화 등 V3 IS 8.0을 실행한 후 발생하는 각종 로그와 백업 파일을 저장할 디스크 공간 크기와 기간을 설정합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 환경 설정에서 **기타 설정**을 선택합니다.

3 **보관 설정** 탭을 누릅니다.

4 **보관 기간과 디스크 공간 설정**에서 필요한 값을 입력합니다.

- 바이러스 검역소 보관 공간: 바이러스에 감염된 백업 파일을 보관하는 검역소의 저장 공간 크기를 지정합니다. 기본 값은 10MB 입니다. 바이러스 검역소 보관 공간에는 1~4096MB 사이의 값을 입력할 수 있습니다. 값을 잘못 입력하였을 경우, **바이러스 검역소 보관 공간은 1~4096MB 사이에서 입력해야 합니다. 다시 입력하십시오.** 라는 메시지가 나타납니다.
- 스파이웨어 검역소 보관 기간: 스파이웨어를 검역소에 보관하는 기간을 지정합니다. 기본 값은 15일 입니다. 스파이웨어 검역소 보관 기간은 0~365일 사이의 값을 입력할 수 있습니다. 값을 잘못 입력하였을 경우, **스파이웨어 검역소 보관 기간은 0~365일 사이에서 입력해야 합니다. 다시 입력하십시오.** 라는 메시지가 나타납니다.
- PC 최적화 백업 파일 보관 공간: PC 최적화를 실행한 후 발생하는 백업 파일을 보관할 저장 공간 크기를 지정합니다. 기본 값은 10MB 입니다. PC 최적화 백업 파일 보관 공간은 1~4096MB 사이의 값을 입력할 수 있습니다. 값을 잘못 입력하였을 경우, **PC 최적화 백업 파일 보관 공간은 1~4096MB 사이에서 입력해야 합니다. 다시 입력하십시오.** 라는 메시지가 나타납니다.
- 검사 로그 보관 공간: 검사 로그를 저장할 공간의 크기를 지정합니다. 기본 값은 24MB 입니다. 검사 로그 보관 공간에는 4~256MB 사이의 값을 입력할 수 있습니다. 값을 잘못 입력하였을 경우, **검사 로그 보관 공간은 4~256MB 사이에서 입력해야 합니다. 다시 입력하십시오.** 라는 메시지가 나타납니다.

- 이벤트 로그 보관 공간: V3 IS 8.0을 실행한 이벤트 로그를 보관하는 공간의 크기를 지정합니다. 기본 값은 24MB 입니다. 이벤트 로그 보관 공간에는 4~256MB 사이의 값을 입력할 수 있습니다. 값을 잘못 입력하였을 경우, **이벤트 로그 보관 공간은 4~256MB 사이에서 입력해야 합니다. 다시 입력하십시오.** 라는 메시지가 나타납니다.

5 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

설정 잠금

허가받지 않은 사용자가 일부 기능을 임의로 중지하거나 환경 설정을 변경하는 것을 방지하고 V3 IS 8.0을 제거하는 것을 예방하기 위해 설정된 비밀번호를 입력한 후에 해당 기능을 이용할 수 있도록 합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 환경 설정에서 **기타 설정**을 선택합니다.

3 **설정 잠금** 탭을 누릅니다.

4 **설정 잠금 사용**을 선택합니다.

5 **비밀번호 설정**을 누릅니다.

6 <비밀번호 설정>에서 설정 잠금에서 사용할 비밀번호를 입력합니다. 비밀번호는 최소 1개 이상의 영문자, 숫자, 특수 문자 조합으로 8자 이상 30자 이하로 입력해야 합니다.

- 비밀번호 입력: 설정 잠금에서 사용할 비밀번호를 입력합니다.
- 비밀번호 확인: 비밀번호 입력에서 입력한 비밀번호를 다시 입력합니다.

⚠ 주의

비밀번호를 잘 기억하십시오. 비밀번호를 잊어버리면 다시 복구할 수 없습니다.

7 **확인**을 누릅니다.

8 비밀번호를 입력하지 않아도 실행해야할 기능이 있다면 **설정 잠금 예외 설정**에서 선택합니다.

- 예약 검사: 예약 검사는 설정 잠금 상태에서 비밀번호를 입력하지 않아도 실행합니다.
- 네트워크 규칙(개인 방화벽 기능): 개인 방화벽의 네트워크 규칙은 설정 잠금 상태에서 비밀번호를 입력하지 않아도 실행합니다.
- 프로그램 규칙(개인 방화벽 기능): 개인 방화벽의 프로그램 규칙은 설정 잠금 상태에서 비밀번호를 입력하지 않아도 실행합니다.

참고

관리 솔루션인 AhnLab Policy Center를 통해 회사나 단체의 관리자가 사용자 PC에 설치된 V3 IS 8.0의 설정 잠금 비밀번호를 설정할 수 있습니다. 설정 잠금 상태에서는 예약 검사, 개인 방화벽, 업데이트 기능은 사용할 수 있지만, V3 IS 8.0의 환경 설정이나 일부 기능의 실행 중지, 프로그램 제거는 비밀번호를 입력하지 않으면 사용할 수 없습니다.

9 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

비밀번호 확인

설정 잠금 상태에서 환경 설정을 선택하면 먼저 비밀번호 확인 창이 나타납니다. **비밀번호**란에 설정된 비밀번호를 입력하고 **확인**을 누르면, 환경 설정을 사용할 수 있습니다.

비밀번호 수정

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **환경 설정**을 누릅니다.

3 <비밀번호 확인>에서 **비밀번호**에 설정된 비밀번호를 입력하고 **확인**을 누릅니다.

4 <환경 설정>의 기타 설정에서 **설정 잠금** 탭을 누릅니다.

5 **비밀번호 설정**을 누릅니다.

6 <비밀번호 설정>에서 현재 비밀번호와 새 비밀번호를 입력합니다.

- 현재 비밀번호 입력: 사용하고 있는 설정 잠금 비밀번호를 입력합니다.
- 새 비밀번호 입력: 새로운 설정 잠금의 비밀번호를 입력합니다
- 새 비밀번호 확인: 새 비밀번호 입력에 입력한 비밀번호를 다시 입력합니다.

7 **확인**을 누릅니다.

탐색기 설정

V3 IS 8.0의 일부 기능 중 마우스 오른쪽 버튼을 누르면 프로그램을 직접 실행하지 않아도 선택한 기능을 사용할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 환경 설정에서 **기타 설정**을 선택합니다.

3 **탐색기 설정** 탭을 누릅니다.

4 Windows 탐색기 메뉴 사용을 선택합니다.

- Windows 탐색기 메뉴 사용: 마우스 오른쪽 버튼을 누르면 나타나는 탐색기 메뉴에서 V3 관련 메뉴를 바로 실행할 수 있습니다.
  - PC 검사: 검사할 드라이브나 폴더, 파일에서 마우스 오른쪽 버튼을 누르면 **V3 PC 검사**를 실행할 수 있습니다. V3 PC 검사를 선택하면, 선택한 대상에 대한 악성코드 감염 여부를 검사하고 치료합니다.
  - 파일 완전 삭제: 검사할 폴더나 파일에서 마우스 오른쪽 버튼을 누르면 **V3 파일 완전 삭제**를 실행할 수 있습니다. V3 파일 완전 삭제를 실행하면, 선택한 대상을 복구 불가능한 상태로 삭제합니다.

⚠ 주의

V3 파일 완전 삭제는 드라이브를 선택했을 경우에는 해당 기능을 사용할 수 없으며, 완전 삭제로 지운 파일은 복구할 수 없으므로 삭제 전 반드시 삭제 대상을 다시 확인하십시오.

5 **적용**을 누릅니다.

- 기본 값: V3 IS 8.0에 설정된 기본 값을 적용합니다.

참고

설정된 기본 값은 신종 바이러스의 등장과 V3 IS 8.0의 성능 개선에 따라 계속 업데이트 됩니다.

- 확인: 설정한 내용을 적용하고 창을 닫습니다.
- 취소: 설정한 내용을 적용하지 않고 창을 닫습니다.

11장
검역소

검역소

악성코드에 감염된 파일을 치료 이전의 감염된 상태 그대로 보관합니다. 검역소에서는 악성코드에 감염된 파일의 확장자를 변경하여 실행 불가능한 상태로 보관해 둡니다.

참고

검역소에 파일을 보관하려면 악성코드에 감염된 파일을 검사하기 전에 치료 방법 선택의 치료나 삭제 전 감염된 파일을 검역소로 보내기를 선택하고 치료해야 합니다.

신고하기

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **검역소**를 누릅니다.

3 **바이러스/스파이웨어**를 선택하고 마우스를 더블 클릭합니다.

4 검역소에 백업된 파일 목록이 오른쪽 백업 목록 창에 나타납니다. 백업 목록에서 신고할 파일을 선택하고 마우스 오른쪽을 눌러 **신고하기**를 선택합니다.

참고

신고하기는 최신 버전의 엔진에서 신종 바이러스나 치료할 수 없는 파일로 진단된 경우에만 바이러스 신고센터로 전송할 수 있습니다.

참고

검역소 백업 목록에서 백업 내용을 선택하고 더블 클릭하거나 마우스 오른쪽을 눌러 상세 보기를 선택하면 백업된 파일에 대한 자세한 정보를 확인할 수 있습니다.

5 <바이러스 신고하기>에서 **사용자 정보 수집 약관**을 자세히 읽으신 후에 내용에 동의할 경우 **동의함**을 선택합니다.

참고

사용자 정보 수집 약관의 내용에 동의하지 않을 경우 **동의 안 함**을 선택합니다. 동의하지 않는 경우 바이러스/스파이웨어 신고를 할 수 없습니다.

6 **사용자 이름, 전화 정보, 메일 주소**를 입력하고 신고할 증상을 자세히 입력하고 감염된 파일을 첨부합니다.

7 **신고하기**를 누릅니다.

복원하기

검역소에 저장된 파일을 복원하는 기능은 감염된 파일을 치료하거나 삭제함으로써 컴퓨터가 정상 동작하지 않는 경우, 악성코드에 감염되었지만 해당 파일의 중요성으로 인해 해당 파일을 사용해야 하는 경우에 활용할 수 있습니다. V3 IS 8.0은 악성코드의 종류에 따라 바이러스 검역소와 스파이웨어 검역소로 구분되어 있으며, PC 최적화를 실행하기 이전의 컴퓨터 상태를 저장해 두었다가 해당 컴퓨터에 문제가 발생했거나 해당 정보를 다시 사용해야 할 경우에 PC 최적화 검역소에 백업된 내용을 복원하여 사용할 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **검역소**를 누릅니다.

3 **바이러스/스파이웨어/PC 최적화**를 선택하고 마우스를 더블 클릭합니다.

4 오른쪽 백업 목록 창에서 복원할 항목을 선택하고 마우스 오른쪽을 눌러 **복원하기**를 선택합니다.
   - 원래 위치에 복원하기: 감염된 파일이 있던 원래 위치에 파일을 복원합니다.
   - 다른 위치에 복원하기: 다른 위치에 감염된 파일을 복원합니다. <폴더 찾아보기>에서 복원할 위치를 선택하고 **확인**을 누릅니다.

참고

다른 위치에 복원하기를 선택하면, **바이러스에 감염된 파일을 다른 위치로 복원하시겠습니까?** 라는 메시지가 나타납니다. 다른 위치에 복원하려면 **확인**을 선택하고, **아니오**를 누르면 선택한 백업 파일을 복원하지 않습니다. 다른 위치에 복원하기는 바이러스에 감염된 파일만 지원하고 스파이웨어, PC 최적화 백업 항목에서는 사용할 수 없습니다.

5 검역소의 백업 목록에서 파일이 사라집니다. 선택한 위치로 파일이 복원되었는지 확인합니다.

삭제하기

검역소에 백업된 파일을 사용자가 직접 삭제하는 기능입니다. 삭제한 파일은 다시 복원할 수 없으므로 삭제 전 주의해야 합니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **검역소**를 누릅니다.

3 **바이러스/스파이웨어**를 선택하고 마우스를 더블 클릭합니다.

4 오른쪽 백업 목록 창에서 삭제할 항목을 선택하고 마우스 오른쪽을 눌러 선택한 항목만 **삭제하기**를 선택합니다.

5 **선택한 항목을 삭제하시겠습니까?** 라는 메시지가 나타납니다. 삭제하려면 **예**를 선택하고, 삭제하지 않으려면 **아니오**를 선택합니다.

6 선택한 항목이 백업 목록에서 사라졌는지 확인합니다.

참고

검역소 항목에서 바이러스나 스파이웨어를 선택하고 도구 바의 **모두 삭제하기**를 누르면 백업 목록 창에 있는 모든 백업 목록을 삭제합니다.

관리자 권한으로 실행

검역소는 일반 사용자 계정으로도 실행할 수 있는 기능이지만, 사용자가 복원하려는 파일을 저장할 대상 폴더나 삭제하려는 파일이 있는 대상 폴더에 대한 권한이 없는 경우라면 관리자 권한으로 실행한 후에 검역소를 사용해야 합니다.

참고

관리자 권한으로 실행은 Microsoft Windows Vista에서만 사용할 수 있으며, 해당 운영체제에서 일반 사용자 계정으로 로그인하면 검역소의 **관리자 권한으로 실행** 버튼이 활성화되어 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 **PC 검사**에서 **검역소**를 누릅니다.

3 **관리자 권한으로 실행**을 누릅니다.

4 <사용자 계정 컨트롤>에서 **사용자가 다음 프로그램을 실행한 경우, 이 프로그램을 실행하려면 [계속]을 클릭하십시오. Quarantine Station AhnLab Inc.**가 나타나면, **계속**을 누릅니다.

5 검역소가 종료된 후 다시 실행되어 나타납니다.

참고

검역소가 관리자 권한으로 다시 실행되면, 관리자 권한으로 실행 버튼이 비활성화 되어 있습니다.

12장
로그 보기

검사 로그 보기

검사 로그는 바이러스나 스파이웨어를 진단 치료하기 위해 V3 IS 8.0을 이용하여 검사한 기록을 보여주는 기능입니다. 검사 로그는 PC 검사에서 발견한 악성코드에 대한 검사 날짜, 감염된 파일과 바이러스 이름, 감염시킨 컴퓨터 이름 등을 보여줍니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 V3 IS 8.0의 **PC 검사/네트워크 보안/웹 보안/메일 보안/PC 도구** 중 하나를 선택하고 **로그보기**를 누릅니다.

3 <로그 보기>가 나타납니다. 로그 선택 창에서 조회할 로그를 선택하고 더블 클릭합니다. 로그를 빨리 검색하려면, 빠른 검색 창에서 검색할 시작 날짜와 끝 날짜를 입력하여 원하는 날짜의 로그를 볼 수 있습니다.

검사 로그의 종류

- 바이러스 검사: 바이러스 검사 로그는 V3 IS 8.0을 이용하여 바이러스를 검사한 기록을 보여줍니다. 바이러스 검사 날짜, 감염된 바이러스 이름, 감염된 파일 이름, 감염 상태, 검사 방법 등의 상세 정보를 볼 수 있습니다.
- 스파이웨어 검사: 스파이웨어 검사 로그는 V3 IS 8.0을 이용하여 스파이웨어를 검사한 기록을 보여줍니다. 스파이웨어 검사 날짜, 감염된 스파이웨어 이름, 감염된 파일의 저장 경로 등의 상세 정보를 볼 수 있습니다.

검사 로그 창

검사 로그 창에서는 로그 선택 창에서 선택한 검사 로그 및 이벤트 로그의 내용을 보여줍니다. 바이러스와 스파이웨어의 검사 치료, 실시간 감시, 시스템 청소 등의 각종 기능을 실행한 작업 내역을 날짜 순서대로 볼 수 있습니다. 로그 창의 해당 항목에 대한 설명이 너무 길어서 모두 보이지 않을 경우에는 셀을 구분하는 선을 더블 클릭하십시오. 하단에 좌우 스크롤 바가 생겨서 모든 내용을 자세히 확인할 수 있습니다. 또한, 해당 항목을 누르면 비슷한 내용끼리 묶어서 쉽게 확인할 수 있도록 정렬 기능을 지원합니다. 단, 항목이 많은 경우 시간이 오래 걸릴 수도 있습니다.

- 검사 날짜: 바이러스와 스파이웨어를 검사한 날짜, 요일, 시간을 보여줍니다.

- 바이러스 이름/스파이웨어 이름: 감염된 바이러스와 스파이웨어 이름을 보여줍니다.
- 감염된 파일 경로: 감염된 파일이 저장된 위치와 파일 이름을 보여줍니다.
- 상태: 감염된 파일의 치료 가능 여부를 보여줍니다.
- 검사 방법: 바이러스와 스파이웨어를 검사한 방법을 보여줍니다.
- 감염된 파일 소유자: 감염된 파일을 가지고 있는 컴퓨터와 로그인 계정을 보여줍니다.
- 감염에 이용된 경로: 원격 컴퓨터에서 감염된 경우 감염된 파일에 접근할 때 이용한 네트워크 경로를 보여줍니다.
- 감염시킨 컴퓨터: 원격 컴퓨터에서 감염된 경우 감염된 파일을 가지고 있던 원격 컴퓨터의 이름을 보여줍니다.

이벤트 로그 보기

이벤트 로그는 V3 IS 8.0의 각 기능이 실행된 기록을 보여줍니다. PC 검사, 네트워크 보안, 웹 보안, 메일 보안, PC 도구 등을 실행한 기록과 작업 내역을 볼 수 있습니다.

1 바탕 화면의 V3 IS 8.0 아이콘()을 더블 클릭합니다.

2 V3 IS 8.0의 **PC 검사/네트워크 보안/웹 보안/메일 보안/PC 도구** 중 하나를 선택하고 **로그보기**를 누릅니다.

3 <로그보기>가 나타납니다. 로그 선택 창에서 **이벤트 로그**를 누릅니다.

4 이벤트 로그에서 조회할 이벤트 로그를 선택하고 더블 클릭합니다. 오른쪽 창에 나타나는 이벤트 로그의 상세 내용을 확인합니다.

이벤트 로그의 종류

- PC 검사: V3 IS 8.0의 각종 검사(정밀 검사, 사용자 목록 검사, 예약 검사, 메일 검사 등)와 실시간 검사를 실행한 내역 및 차단 기록 등을 보여줍니다.
- 네트워크 보안: 프로그램이 인터넷에 연결하려고 할 때 개인 방화벽이나 네트워크 침입 차단을 위해 프로그램을 실행한 내역과 접근, 차단, 설정 변경, 시작, 종료, 규칙의 추가/수정/삭제, 에러에 대한 내용을 보여줍니다.
- 웹 보안: 피싱 사이트 차단, 웹사이트 필터링을 실행한 내역을 보여줍니다.
- 메일 보안: 메일 보안을 위해 메일 검사, 스팸 메일 차단, 허용/차단 메일 주소 등을 실행한 내역을 보여줍니다.
- PC 도구: PC 최적화, 파일 완전 삭제, 실행 차단 목록 등을 실행한 내역을 보여줍니다.
- 업데이트: 업데이트를 실행한 내역을 보여줍니다.

이벤트 로그 창

이벤트 로그 창에서는 로그 선택 창에서 선택한 각종 이벤트 로그의 내용을 보여줍니다. V3 IS 8.0의 각종 기능을 실행한 작업 내역을 날짜 순서대로 볼 수 있습니다. 로그 창의 해당 항목에 대한 설명이 너무 길어서 모두 보이지 않을 경우에는 셀을 구분하는 선을 더블 클릭하십시오. 하단에 좌우 스크롤 바가 생겨서 모든 내용을 자세히 확인할 수 있습니다. 또한, 해당 항목을 누르면 비슷한 내용끼리 묶어서 쉽게 확인할 수 있도록 정렬 기능을 지원합니다. 단, 항목이 많은 경우 시간이 오래 걸릴 수도 있습니다.

- 날짜: 선택한 작업을 실행한 날짜, 요일, 시간을 보여줍니다.
- 수준: 수준 항목에는 출력된 이벤트 로그의 내용에 따라 일반, 경로, 에러, 정보, 중요 등을 표시합니다.
- 기능 이름: 실행한 기능 이름을 보여줍니다.
- 내용: 선택한 기능을 실행한 내역을 보여줍니다.

색인

ㅂ

ㅅ

ㅇ

ㅈ

ㅊ

ㅋ

ㅌ

ㅍ

ㅎ

C

H

I

P

R

S

T

U

V

W