eScan 매뉴얼

- Internet Security Suite -

2015. 5.

에프이에이코리아(주)

<목 차>

1. 설치 준비

1.1 설치 준비 사항

설치를 하시기 전에 다음 사항을 확인해 주시기 바랍니다.

처음 설치하시는 경우라면,

- 관리자 권한으로 윈도우에 로그인 해 주세요.
- 다른 프로그램들은 종료해 주시고, 다른 백신프로그램을 사용 중이라면 삭제해 주세요.
- Windows Defender를 비활성화 시키거나 삭제해 주세요.
- Windows Firewall을 포함하여 방화벽 프로그램을 비활성화 시키거나 삭제해 주세요.

기타

- 이스캔을 설치할 컴퓨터가 인터넷에 연결되어 있으면 백신 데이터베이스가 최신 상태로 유지됩니다.
- 메일 서버 사용과 관련한 정보를 등록하시면 경고 (알림) 메시지를 메일로 보내드립니다.
- 운영 체제와 관련한 최신 보안패치가 설치되어 있는 것이 좋습니다.

재설치 혹은 업그레이드를 설치하는 경우

- 기존 설치된 eScan을 제거하지 않고 바로 업그레이드를 수행할 수 있습니다.

기존 eScan 삭제 후 다시 설치하는 경우

- 기존 eScan을 삭제하고 다시 설치하는 경우에는 반드시 재부팅을 하셔야 설치하실 수 있습니다.

1.2 시스템 요구사항

운영체제

- Windows® 8 Family
- Windows® 7 Family
- Windows Vista®Family
- Windows® XP Family Service Pack 2 or higher
- Windows® 2000 Professional Service pack 4 Rollup patch 1

Tip. 기업용 제품이 아니면 윈도우 서버운영체제는 지원하지 않습니다.

CPU

- Windows 8requires 1 GHz
- Windows 7 requires 1 GHz
- Windows Vista requires 1GHz
- Windows XP requires 450MHz (1 GHz recommended)

메모리

- Windows 8 requires 1 GB
- Windows 7 requires 1 GB
- Windows Vista requires 1GB
- Windows XP requires 512MB (1GB recommended)

하드디스크

- 750 MB

기타

- Web Browser:Microsoft Internet Explorer 7.0 or 8.0 or higher.
- Display:High-color display with a resolution of 640x480 pixels or higher

1.3 사용자 환경

GUI

GUI는 처음 사용자이건 익숙한 사용자이건 쉽게 사용할 수 있도록 구성하였습니다. 사용언어를 변경해야 한다면, 키보드에서 **Shift + F12 로 영어**로, **Shift + F5 로 설치할 때 선택한 언어**로 환경이 변경됩니다.

첫 화면을 [대시보드]라고 합니다. 대시보드는 각 모듈별 주요 정보를 종합하여 표시하며, 제품명, 버전, 실시간 보호 상태, 최근 검사일, 최근 백신업 데이트일 등을 표시합니다.

오른쪽 위의 ? (Help)를 클릭하면 아래와 같은 화면이 표시됩니다.

- **실시간 채팅 :** 인터넷에 연결되어 있으면, 24시간 실시간채팅으로 질의하실 수 있습니다. 현재는 영어/독일어를 지원하고 있습니다.
- **온라인 도움말** : 인터넷에 연결되어 있다면, eScan wiki에서 다양한 정보를 통해 도움을 받으실 수 있습니다. 연결되는 사이트는 http://www.escanav.com/wiki 입니다.
  이용 중에 F1을 누르면, 현재 이용 중인 서비스와 가장 가까운 도움말을 표시해 드립니다.
- **이스캔포럼** : 이스캔 포럼에서 다른 사용자들과 의견을 교환하실 수 있습니다.
- **이스캔 원격지원** : 고객 컴퓨터에 원격으로 접속하기 위한 아이디와 비번이 표시됩니다. 원격지원을 요청하실 때 전화/메일/채팅 등으로 알려 주시기 바랍니다.
- **피드백** : 링크에 연결된 이스캔 홈페이지에서 제품에 대해 평가를 해 주시면, 품질관리팀에 전송됩니다.

모듈

대시보드에는 아래의 각 모듈들을 선택하여 설정을 변경할 수 있습니다. 기본값으로는 파일 안티바이러스, 방화벽, 엔드포인트 보안, 클라우드 보안이 활성화 상태에 있습니다.

- **파일 안티바이러스** : 파일과 폴더에 대한 실시간 감시 기능을 제공합니다.
- **메일 안티바이러스** : 감염된 메일, 첨부파일 등이 컴퓨터에 저장되기 전에 차단합니다.
- **안티 스팸** : 키워드나 문장을 검사하여 스팸 메일을 필터링합니다.
- **웹 보호** : 웹 브라우저에 폭력적이거나 선정적인 콘텐츠가 표시되지 않도록 보호합니다.

- **방화벽** : 포트, 프로그램, 기타 서비스를 차단하는 전문가용 기능을 설정합니다.
- **엔드포인트 보안** : USB, DVD, SD, 웹캠 등에 의한 감염을 보호하며, 프로그램 혹은 장치에 대한 차단 리스트 혹은 허용 리스트를 관리합니다.
- **사생활 보호** 웹브라우저 캐시, 이력, 쿠키 등 개인정보 유출의 위험이 있는 임시 파일들을 제거합니다.
- **클라우드 보안** : 세계 이스캔 사용자 네트워크에 연결되어 백신이 미처 준비되기 이전의 위험요소들을 경고하고 차단합니다.

기타 옵션버튼

왼쪽 아래에 2개의 버튼이 있습니다.

- **검사** : 즉시검사, 예약검사 등을 실행하거나 설정합니다.
- **업데이트** : 매일/매주/매월 정기적인 업데이트를 설정합니다.

빠른 메뉴

오른쪽 아래에는 몇 가지 빠른 메뉴들이 준비되어 있습니다.

- **eScan 원격지원** : 원격지원으로 지원을 받으실 필요가 있을 때 클릭하시면, 원격접속을 위해 저희에게 알려주셔야 하는 아이디와 비번이 표시됩니다. 자세한 내용은 http://wiki.escanav.com/wiki/index.php/Remote_Support 를 참고 하세요.
- **비밀번호** : 이스캔 관리자 비밀번호를 변경할 수 있습니다.
- **라이선스 정보** : 라이선스키를 등록하고 정품인증을 수행합니다.
- **툴** : 응급 복구 디스크 생성, 이스캔 업그레이드 (핫픽스 다운로드), 안전모드 보호, 윈도우 최신패치 (핫픽스 다운로드), 바이러스 샘플 보고, USB 예방접종 등의 기능이 제공됩니다.
- **보고서** : 각 모듈의 활동상황에 대한 보고서를 작성합니다.

툴

오른쪽 아래에 있는 [툴] 메뉴에서 사용할 수 있는 기능들입니다.

- **응급 복구 디스크 생성**

응급 복구용 디스크 파일을 생성하는 마법사가 시작됩니다.
윈도우 운영체제가 감염 되었을 때 CD로 부팅해서 루트킷과 같이 일반적인 부팅 상태에서 치료할 수 없는 바이러스를 치료할 수 있으며, 이러한 CD를 생성하기 위한 이미지 파일(image file)을 생성하거나 다운로드 받게 됩니다.
http://download1.mwti.net/download/wikifiles/eScan_Rescue_Disk.pdf 참조.

- **이스캔 최신 핫픽스 다운로드**

이스캔 최신 버전을 다운로드 합니다. 이미 최신 버전이 사용 중인 경우에는 회색으로 비활성화 됩니다.

- **안전모드 보호**

안전모드를 사용할 수 있는 운영체제인 경우에는 안전모드 실행에 대해 비밀번호를 설정하여 다른 사용자가 임의로 안전모드로 들어가는 것을 금지 시킬 수 있습니다. 안전모드는 드라이버 상당수가 실행되지 않는 상태로 보안이 취약한 상태이므로, 다른 사람이나 프로그램이 임의로 진입하여 시스템 설정을 변경하는 것을 예방하는 것입니다.

- **윈도우 최신 핫픽스 다운로드**

윈도우 운영체제의 최신 버전이나 버그 패치를 다운로드하여 설치합니다.

● **디버그**

이스캔 사용 중 문제점을 발견했을 때 이 메뉴를 실행시키면, debugs.zip 파일이 생성되어 아래 경로에 저장됩니다.

- 32비트컴퓨터 : [Disk Drive]\Program Files\eScan\Debug
- 64비트컴퓨터 : [Disk Drive]\Program Files (x86)\eScan\Debug

이 파일을 이스캔 기술팀으로 보내 주시면, 이 파일을 분석하여 문제점을 해결할 수 있도록 도움을 드리게됩니다.

다른 메일 서비스를 사용하셔서 보내주시면 되나, 이스캔 프로그램에서 바로 보내기 위해서는 아래와 같이 메일을 발송하는 메일서버 정보가 입력되어야 합니다.

- Mail From : 발송자 메일주소
- Mail To : 수신자 메일 주소. support@escanav.com 로 발송하면 됩니다.
- SMTP Server : 메일 서버의 아이피주소
- SMTP Port : 메일 서버의 메일 발송용 포트번호 (기본값 25)
- User Authentication (선택적) : 메일 발송을 위해 사용자 인증이 필요한 경우 사용자 아이디
- Authentication Password (선택적) : 메일 발송을 위해 사용자 인증이 필요한 경우 비밀번호

● **윈도우 기본설정 복원**

바탕화면 설정을 포함하여 바이러스로 인하여 수정되었을 수 있는 모든 변경사항을 윈도우 운영체제의 기본설정으로 복원시킵니다. 시스템을 검사하고 각종 시스템 운영 관련 변수들도 기본값으로 설정합니다.

● **샘플 업로드**

바이러스 샘플을 이스캔 기술팀에게 보내어 점검하도록 요청 하실 수 있습니다.

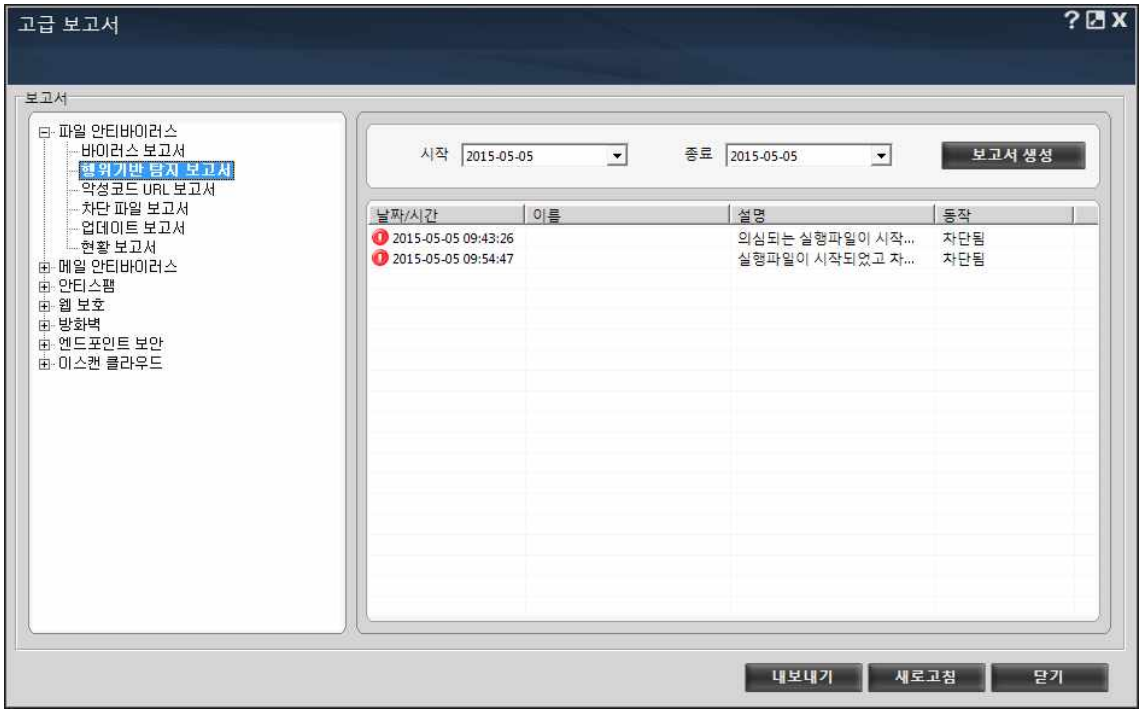
● **USB 예방접종**

USB는 다양한 목적으로 사용이 되는데, USB 로부터 바이러스가 감염되기도 하고, USB 장치가 감염되기도 합니다. 예방접종을 수행한 USB 장치는 바이러스에 감염된 시스템에 접속을 하더라도 바이러스에 감염되지 않게 됩니다.

컴퓨터에 USB 장치를 연결하면, [예방접종] 버튼이 활성화 되는데, USB 장치가 연결된 드라이브를 선택하고 [예방접종] 버튼을 눌러 주면 완료됩니다.

활동보고서작성

각 모듈별로 보호활동에 대한 보고서를 생성합니다.



1.4 설치확인

설치가 완료되면, 윈도우 오른쪽 아래 트레이에  아이콘이 표시되는데, 활동 중이 아닐 때에는  와 같이 X 표가 같이 표시 됩니다. 여기에서 마우스 왼쪽을 클릭하면 기본 GUI환경 (eScan 보호센터)이 실행되며, 오른쪽을 클릭하면 아래와 같은 팝업메뉴가 나타납니다.

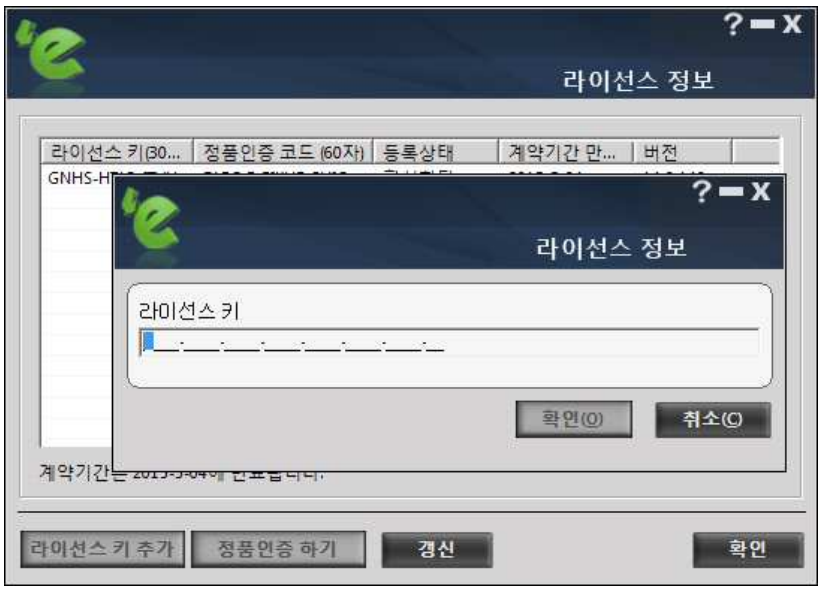
[eScan보호센터]를 열려면 관리자 비밀번호가 설정된 경우에는 이를 입력해야 하며, 기본 설정된 비밀번호는 [admin]입니다.

1.5 라이선스키 관리

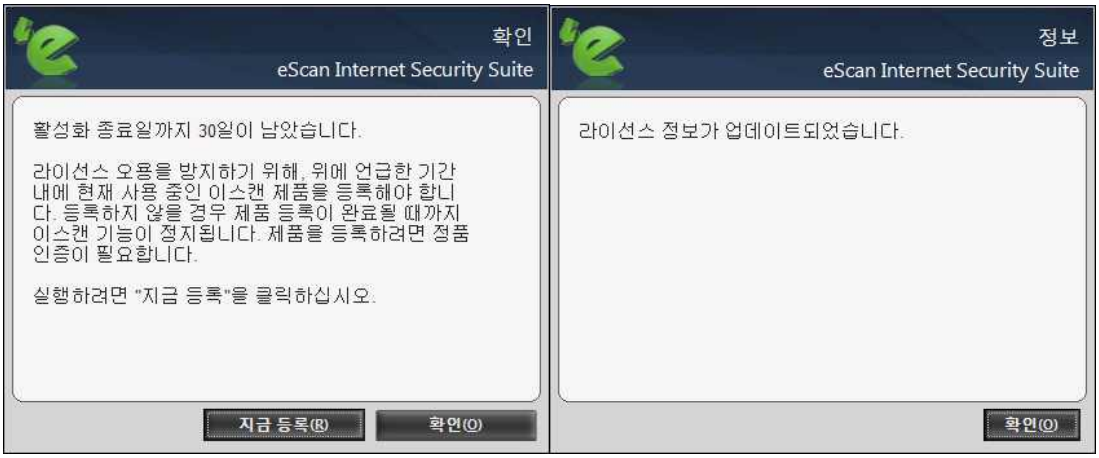
라이선스키를 입력하고 정품인증(Activation)을 수행하는 과정을 다룹니다.
License Key 없이 30일 동안은 사용하실 수 있는데, 이 기간 이내에 정품을 구매하셔서 License Key를 등록하고 정품인증을 하셔서 이스캔으로 시스템을 계속 보호하시기를 바랍니다.

라이선스키 입력

라이선스키는 최대 2개까지 입력할 수 있으며, 하나의 라이선스키가 정품인증까지 완료된 이후에 다음 라이선스키를 입력할 수 있게 됩니다.
라이선스키는
1. [시작 >모든프로그램 >eScan for Windows >eScan 등록] 클릭
2. 아래 대화창에서 License Key 입력



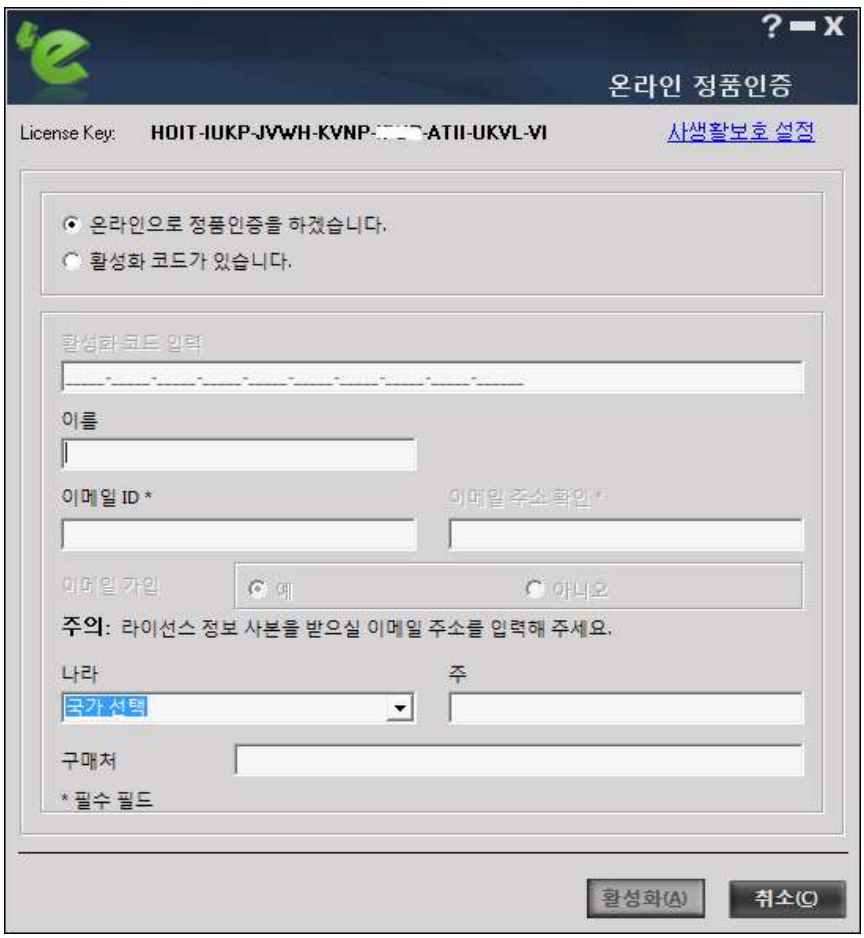
– 공백은 없이 입력합니다.
– 정확하게 입력해야 다음 단계로 넘어갈 수 있으며, 간혹 잘못된 입력임에도 다음 단계로 넘어가는 경우에는 그 다음 단계에서 오류가 발생합니다.
– 다음 단계로 넘어가면, 아래와 같은 메시지가 나타납니다.



– [확인]을 클릭하면, 라이선스 정보가 갱신됩니다.

정품인증 (또는 활성화, Activation)

유효한 라이선스키를 입력하였다면, 이 정보를 토대로 정품인증을 수행합니다. 정품인정은 앞서 [라이선스키 입력] 과정 마지막 단계에서 [지금 등록]을 클릭하면 아래와 같은 대화창에서 [정품인증하기] 버튼으로 수행합니다.



[정품인증 하기]를 클릭하면, 아래의 대화창이 표시됩니다.

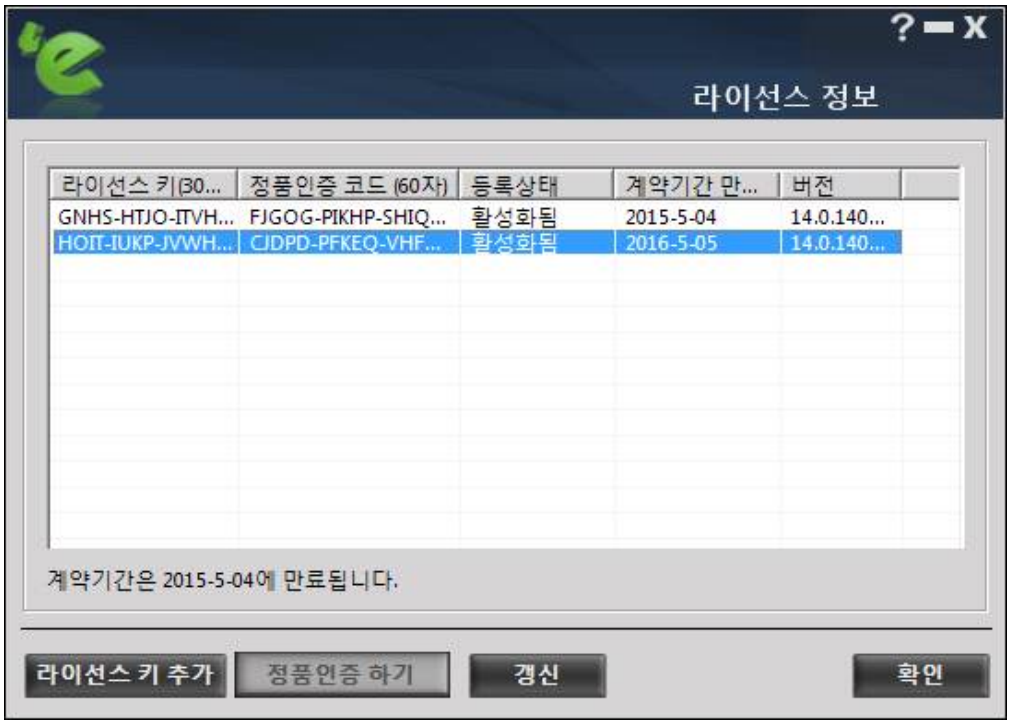
- **[온라인으로 정품인증을 하겠습니다.]**

기본설정은 이것으로 되어 있으며, 이름, 메일 주소 등을 입력할 수 있으며, 인터넷에 연결되어 있으면 온라인으로 정품인증이 완료됩니다.

인터넷에 연결되어 있지 않거나, 다른 문제가 있는 경우에는 아래와 같은 대화창이 표시되는데, [아니오]를 선택하면 정품인증을 위한 Onlineregister.txt 파일이 생성됩니다. 이 파일을 register@escanav.com (본사) 혹은 info@escan.co.kr (한국지사)로 메일로 보내면, 정품인증을 위한 코드를 회신으로 보내드립니다.

● **[정품인증코드로 인증하기] :**

메일로 받은 정품 인증코드를 입력하여 인증을 완료할 수 있습니다.



2. 파일 안티바이러스

컴퓨터를 실시간으로 모니터링하고 보호하는 모듈입니다. 행위기반 검사기능을 포함하고 있어서 수상한 활동을 하는 프로그램의 실행을 차단하며, 파일 보호 기능으로 특정 파일들을 내/외부 접근으로부터 보호할 수 있으며, 폴더 단위로 생성/삭제/수정 등의 활동을 차단시킬 수도 있습니다.

2.1 메인

구성

파일 안티바이러스 상태 : 파일 안티바이러스 기능의 실행 상태
행위기반 탐지기능 상태 : 행위기반 탐지기능 활성화 여부
감염 발견 시 수행할 작업 : 감염된 파일에 대한 작업 설정 상태

시작/중지

파일 안티바이러스 기능을 시작하거나 중지

설정

파일 안티바이러스와 관련한 옵션들을 설정할 수 있습니다.

- **기본값** : 최초 기본설정으로 옵션들을 설정합니다.
- **적용** : 변경한 옵션설정을 적용합니다
- **확인** : 현재 설정을 저장하고 창을 닫습니다.
- **취소** : 창을 닫습니다.

보고서

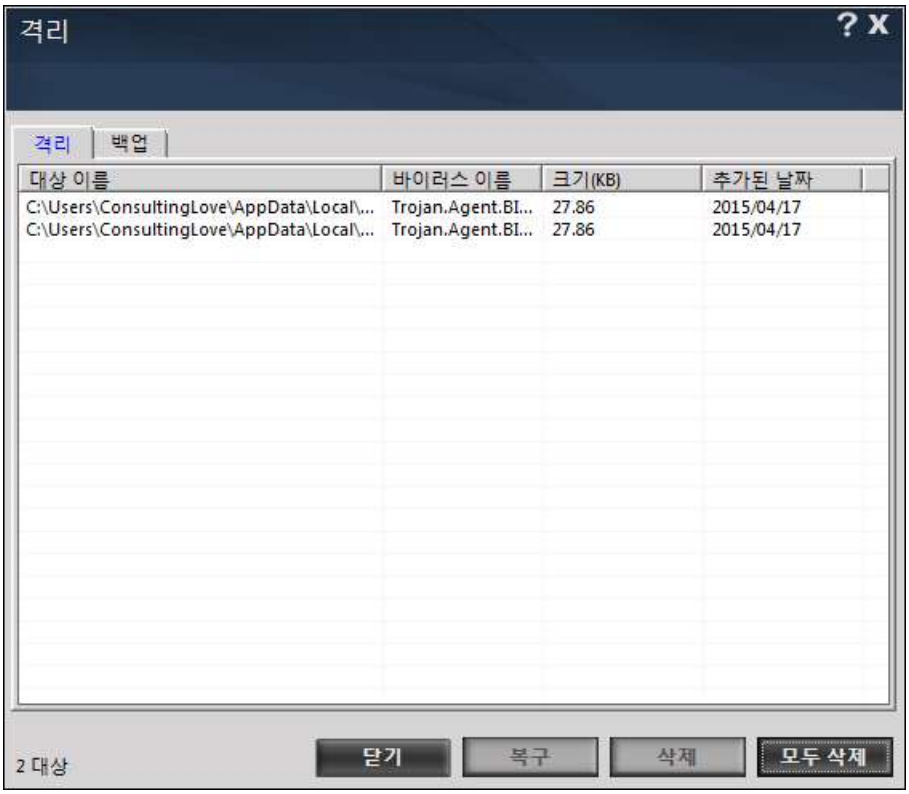
검사된 파일 개수 : 실시간 감시로 점검된 파일의 개수를 표시
위험 요소 발견 개수 : 실시간 감시에 의해 발견된 바이러스나 멀웨어 개수를 표시
가장 최근 검사된 파일 : 가장 최근에 검사된 파일 이름

통계 보기

아래 그림과 같이 실시간 감시 현황을 요약하여 표시합니다.

격리 처리된 파일 보기

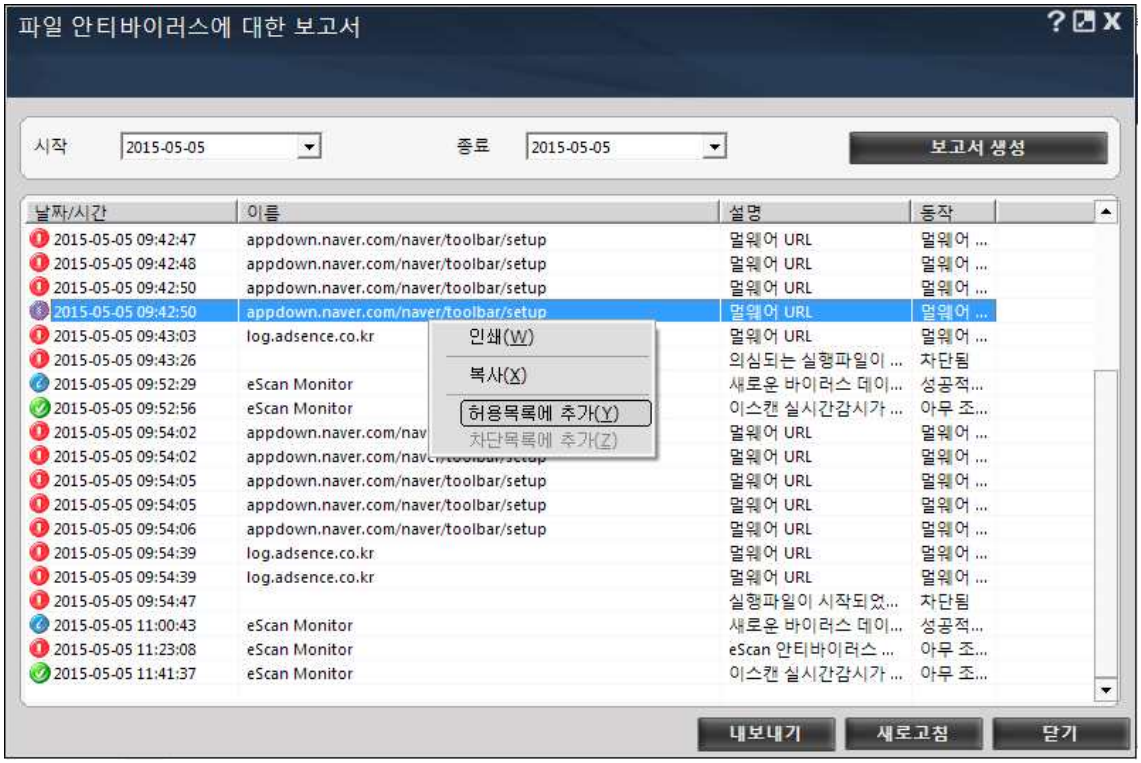
아래 그림과 같이 격리 되었거나 백업된 파일목록을 표시합니다.



- **격리** : 바이러스 검사에 의해 격리된 파일목록입니다. 목록을 선택하고 마우스 오른쪽을 클릭하면 원래위치로 복원시키거나 삭제하는 등의 작업을 수행할 수 있습니다.
- **백업** : 감염된 파일을 치료할 때 치료에 앞서 원본파일을 백업해 둔 목록입니다. 목록을 선택하고 마우스 오른쪽을 클릭하면 원래 위치로 복원시키거나 삭제하는 등의 작업을 수행할 수 있습니다.

보고서

파일 안티바이러스 활동에 의한 날짜별 활동내용을 조회 할 수 있습니다.



- **허용목록에 추가**

보고서 내 항목을 선택하고 마우스 오른쪽을 클릭하면 선택할 수 있습니다. 혹 정상적인 것으로 확신하는 파일이 바이러스 감염으로 보고되면, 다음부터 오진하지 않도록 허용목록에 추가합니다.

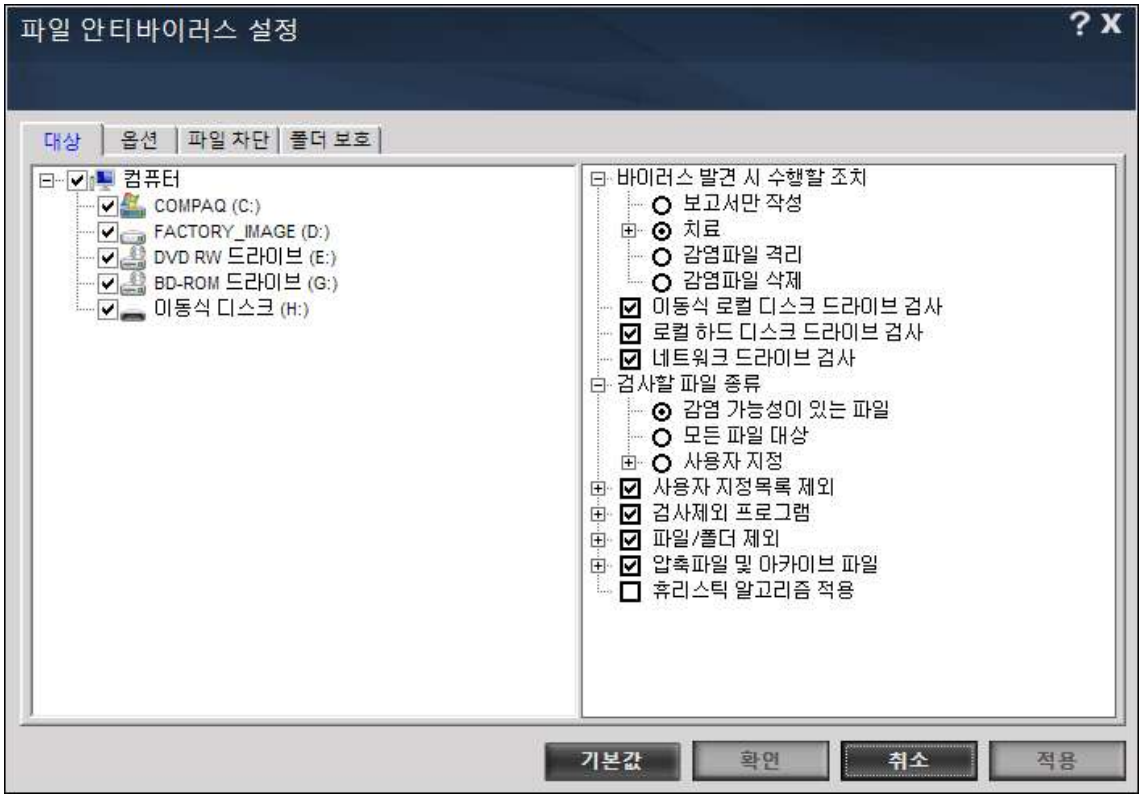
- **차단목록에 추가**

보고서 내 파일을 선택하고 마우스 오른쪽을 클릭하면 선택할 수 있습니다. 의심스러운 파일로 분류된 것이지만, 앞으로 실행되지 않도록 차단목록에 추가합니다.

2.2 설정

파일 안티바이러스와 관련한 상세기능을 조율합니다.

대상



- **바이러스 발견 시 수행할 조치**

기본 설정은 [치료]이며, 치료가 되지 않는 파일들은 c:\Program Files\eScan\Infected folder 에 저장 됩니다.

- **이동식 로컬 디스크 드라이브 검사 (기본선택)**

실시간 감시기능을 이동식 저장장치에도 적용시키려면 선택합니다.

- **로컬 하드 디스크 드라이브 검사 (기본선택)**

실시간 감시기능을 컴퓨터에 장착된 하드 디스크에 적용시키려면 선택합니다.

- **네트워크 드라이브 검사 (기본선택)**

실시간 감시기능을 컴퓨터에 연결된 네트워크 드라이브에 적용시키려면 선택합니다.

- **검사할 파일 종류**

실시간 감시기능이 감시할 파일 형태를 지정합니다. [사용자 지정>추가/삭제]를 더블클릭하면 이스캔이 지정한 파일 형태가 기록되어 있으며, 사용자가 추가하거나 삭제할 수 있습니다.

- **사용자 지정목록 제외 (기본선택)**

실시간 감시기능을 적용하지 않고자 하는 파일 형태를 [추가/삭제]를 더블클릭하여 추가하거나 삭제할 수 있습니다.

- **검사제외 프로그램 (기본선택) :**

파일 안티바이러스는 유해한 프로그램의 실행을 차단할 수 있는데, 감염을 목적으로 하는 파일 혹은 운영체제에 보안측면에서 해로울 수 있는 프로그램이 포함됩니다. 유해한 프로그램이 아니라고 확신할 수 있는 프로그램들은 [추가/삭제]를 더블클릭하여 추가하여 차단되지 않도록 할 수 있습니다.

- **파일/폴더 제외 (기본선택)**

특정 파일이나 특정 폴더 및 그 하위 폴더를 실시간 감시 혹은 바이러스 검사에서 제외하고자 하는 목록을 관리합니다.

- **압축 파일 및 아카이브 파일 (기본선택)**

압축된 파일이나 아카이브 파일을 검사할지 여부를 선택합니다. 아카이브 파일을 선택하면 몇 단계 깊이까지 검사할 지를 지정할 수 있습니다. 기본값으로는 압축파일을 검사하도록 지정되어 있습니다.

- **휴리스틱 알고리즘 적용**

실시간 감시에 휴리스틱 알고리즘을 적용하여 명확히 바이러스로 보고되지는 않았으나 의심스러운 파일이나 감염이 의심되는 파일들도 찾아내도록 합니다.

옵션

로그 파일의 크기, 로그 파일/격리 파일/보고서의 위치 등 파일 안티바이러스 모듈의 기본설정을 지정합니다.

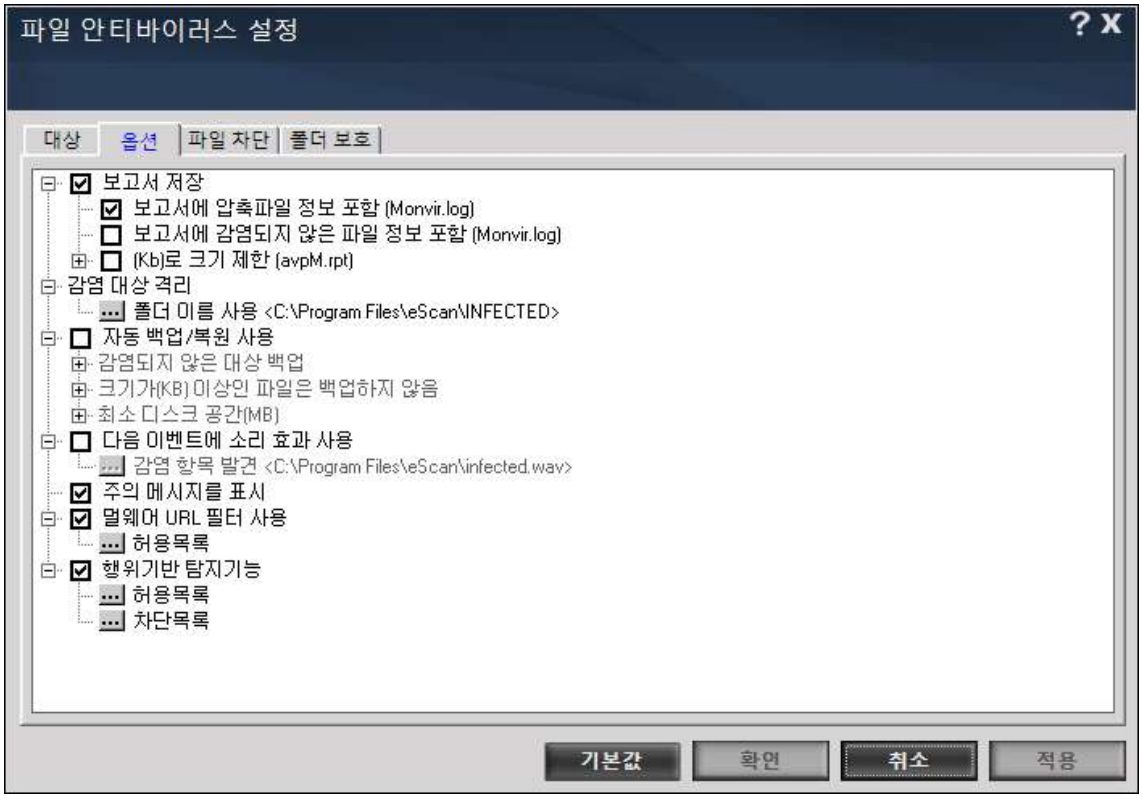
- **보고서 저장 (기본설정)**

검사된 파일, 감염 파일 조치사항 등 검사 과정에서 발견되거나 취해진 조치내용을 기록한 보고서를 저장합니다.

- 보고서에 압축파일 정보 포함 (기본선택) :
  zip, rar 파일과 같은 압축파일에 대한 검사기록을 Monvir.log 파일에 기록합니다.
- 보고서에 감염되지 않은 파일 정보 포함 :
  검사 하였으나 감염되지 않은 파일 목록도 Monvir.log 파일에 기록합니다.
- (Kb)로크기제한 :
  로그파일 (avpM.rpt)의 크기를 제한할 수 있습니다. 기본값은 50kb 로 제한되어 있습니다.

- **감염 대상 격리**

감염된 파일을 격리시킬 폴더를 선택합니다.



● **자동 백업/복원사용**

운영체제 중 중요한 파일들은 자동으로 백업해 두었다가, 감염 사고가 있는 경우 깨끗한 파일로 복원합니다.

- 감염되지 않은 대상 백업 :
  감염되지 않은 파일들을 백업해 둘 폴더를 지정합니다.
- 크기가 (kb)이상인 파일은 백업하지 않음 :
  파일의 크기가 큰 파일은 백업에서 제외하도록 합니다. 기본값은 32768kb입니다.
- 최소 디스크 공간 (MB) :
  이스캔이 백업 파일을 저장하기 위한 최소 공간을 확보해 두도록 합니다. 기본값 500MB.
- 파일 크기 제한
  지정한 크기보다 큰 크기의 파일에 대해서는 바이러스 검사를 수행하지 않도록 합니다.
  기본값은 20480KB입니다.

● **다음 이벤트에 소리 효과 사용**

각 이벤트에 사용할 소리 종류를 지정합니다.

● **주의 메시지를 표시 (기본설정)**

바이러스에 감염된 파일이 발견되었을 때 파일의 경로와 이름을 메시지로 표시합니다.

● **멀웨어 URL 필터사용 (기본설정)**

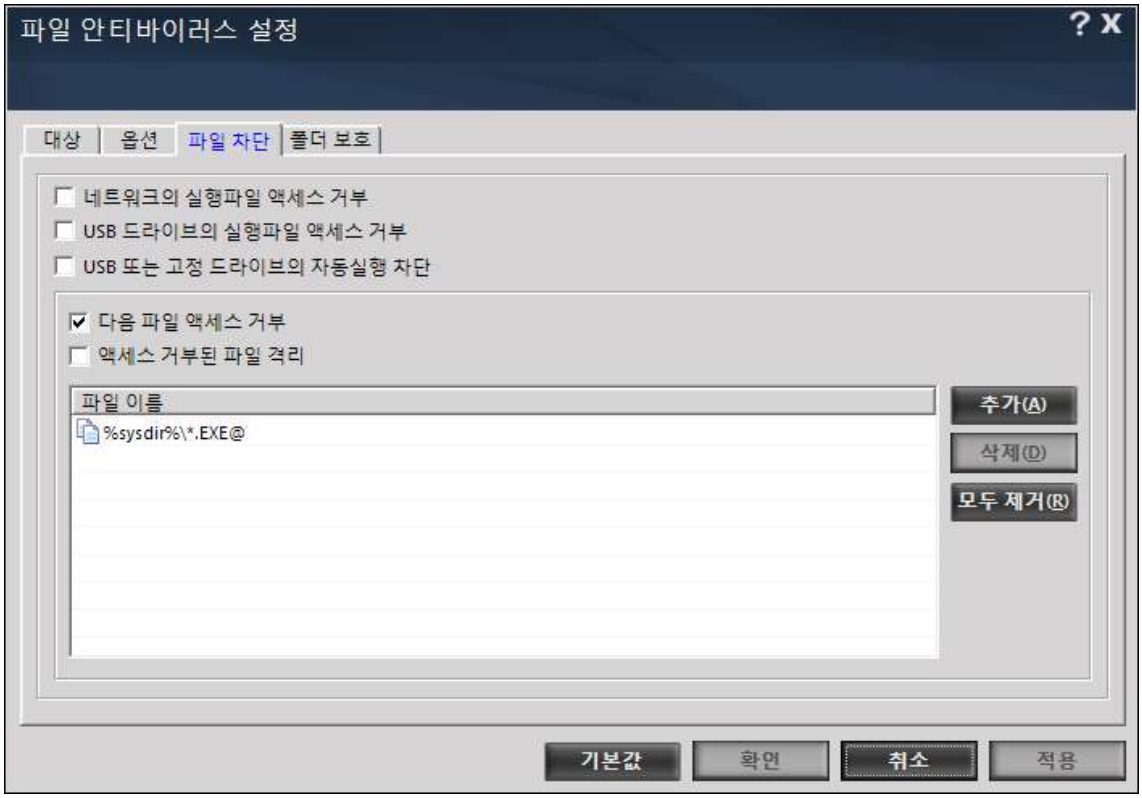
바이러스에 감염되었거나 배포하는 것으로 알려진 URL 접속을 차단합니다. 허용목록 버튼을 클릭하여 차단하지 않고자 하는 웹사이트 주소를 추가할 수 있습니다.

● **행위기반 탐지기능 (기본설정)**

시스템에서 실행되고 있는 실행파일들을 감시하고자 할 때 선택합니다. 시스템에 위협이 되거나 의심스러운 실행파일들이 발견되면 차단여부를 확인하는 메시지를 표시하게 되며, 허용목록에 추가하면 실행되는 것을 허용하게 됩니다. 차단목록을 보면, 이러한 활동으로 차단된 파일목록을 조회할 수 있으며, 필요에 따라 허용목록과 차단목록을 조정하실 수 있습니다.

파일차단

네트워크 드라이버나 USB 드라이브, 고정 장치 등에서 실행파일 혹은 자동실행을 유도하는 autorun.inf 파일들이 컴퓨터에 접근하는 것을 차단할 수 있습니다.



선택할 수 있는 옵션들은 다음과 같습니다.

● **USB 드라이브의 실행파일 엑세스 거부**

네트워크로 연결된 곳에서 실행 파일이 실행되는 것을 금지합니다.

● **USB 또는 고정 드라이브의 자동실행 차단**

USB의 AUTORUN.INF 나 실행파일들이 자동으로 실행되는 것을 금지합니다.

● **네트워크의 실행파일 엑세스 거부**

네트워크로 연결된 폴더에서 실행파일이 실행되지 않도록 합니다. 실행이 필요한 파일이 있는 경우 허용목록에 추가합니다.

- **다음 파일 엑세스 거부**

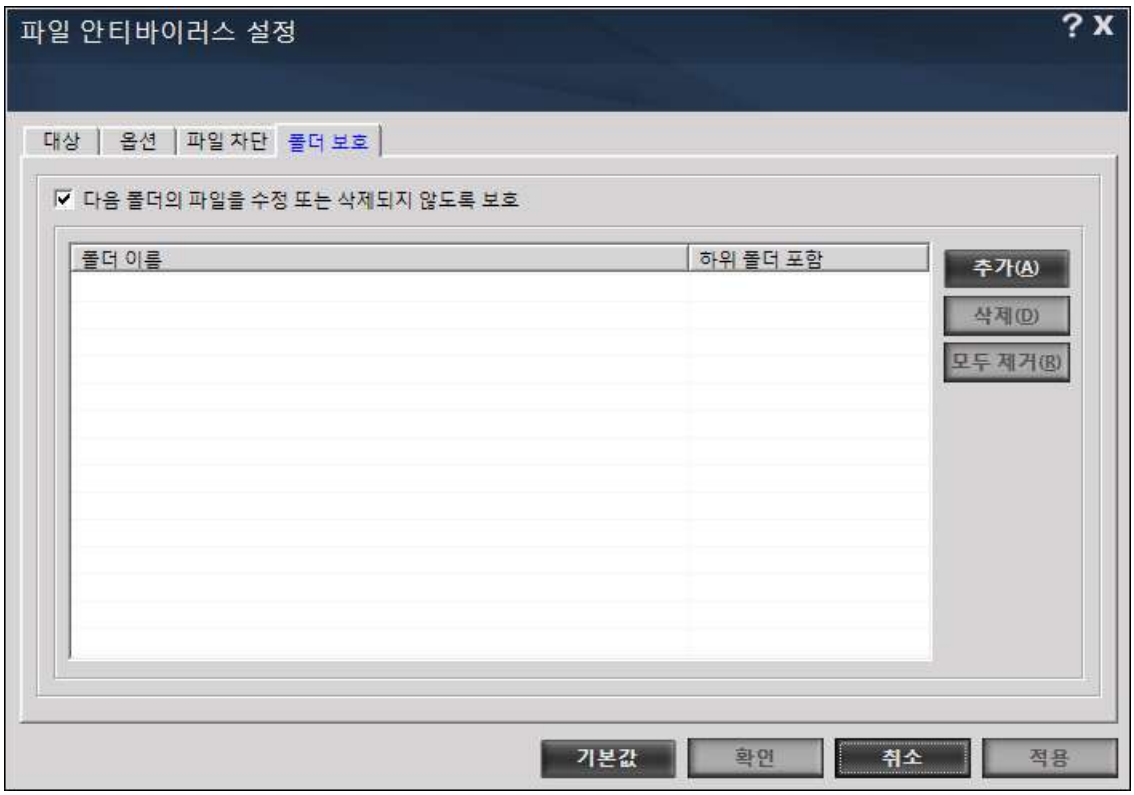
아래 목록에 기록된 파일들이 시스템 상에서 실행되지 않도록 지정합니다. 기본값으로 시스템 폴더에 있는 EXE 확장자의 파일들이 지정되어 있습니다.

- **엑세스 거부된 파일 격리**

실행을 시도했다가 거부된 파일들은 별도로 격리시켜 두도록 지정할 수 있습니다. 특정 파일이 실행되지 않도록 하려면, 목록에 기록해 둡니다.

폴더보호

여기에 지정한 폴더의 하위 폴더들은 수정되거나 삭제되지 않도록 보호합니다.



- **다음 폴더의 파일을 수정 또는 삭제되지 않도록 보호 (기본설정)**

여기에 지정한 폴더 (하위 폴더 포함 여부 선택)는 수정되거나 삭제되지 않도록 보호합니다.

3. 메일 안티바이러스

이 모듈은 수신하거나 발신하는 모든 이메일에 대하여 바이러스, 스파이웨어, 에드웨어, 기타 의심스런 내용에 대해 검사를 수행합니다. 기본값으로는 수신되는 이메일과 첨부파일에 대해서만 검사하도록 지정되어 있습니다만, 필요에 따라 설정을 바꾸어 발송되는 메일에 대해서도 검사하도록 지정하시면 됩니다. 메일 발송자나 시스템 관리자에게 감염된 이메일을 받았을 때 안내문을 보내도록 설정할 수 있습니다.

3.1 메인

구성

메일 안티바이러스 상태 : 메일 안티바이러스 기능이 사용 중인지 여부를 표시
감염발견 시 수행할 작업 : 감염된 메일 발견 시 수행하도록 지정한 조치사항을 표시

시작/중지

메일 안티바이러스기능을 시작하거나 중지시킬 수 있습니다.

설정

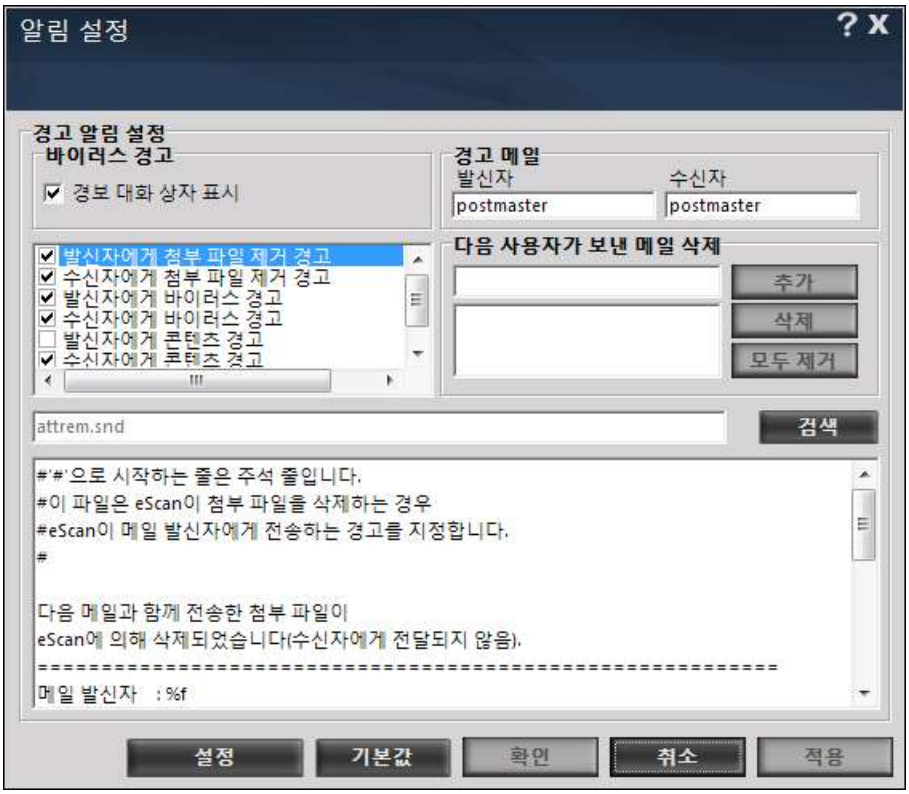
메일 안티바이러스 기능과 관련한 옵션들을 설정합니다.

- **기본값** : 최초 기본설정으로 옵션들을 설정합니다.

- **적용** : 변경한 옵션설정을 적용합니다
- **확인** : 현재 설정을 저장하고 창을 닫습니다.
- **취소** : 창을 닫습니다.

알림

유해요소가 포함된 메일이 발견되었을 때 누구에게 어떤 알림 메시지를 보낼 것인가를 지정합니다.



- **경보 대화 상자 표시 (기본설정)**

유해요소 발견 사실에 대한 안내창을 표시합니다.

- **발신자에게 첨부 파일 제거 경고 (기본설정)**

발신자에게 메일에 감염된 첨부파일이 있었음을 알리는 메일을 발송합니다. 메일 미리보기에 발송된 메일 내용 일부가 표시됩니다.

- **수신자에게 첨부 파일 제거 경고 (기본설정)**

수신자에게 메일에 감염된 첨부파일이 있었음을 알리는 메일을 발송합니다. 메일 미리보기에 메일 내용 일부가 표시됩니다.

- **발신자에게 바이러스 경고 (기본설정)**

발신자에게 감염된 메일이 발송되었음을 알리는 메일을 발송합니다. 메일 미리보기에 발송된 메일 내용 일부가 표시됩니다.

- **수신자에게 바이러스 경고 (기본설정)**

수신자에게 감염된 메일이 수신되었음을 알리는 메일을 발송합니다. 메일 미리보기에 메일 내용 일부가 표시됩니다.

- **발신자에게 콘텐츠 경고 (기본설정)**

발신자에게 부적절한 내용의 메일이 발송되었음을 알리는 메일을 발송합니다. 메일 미리보기에 발송된 메일 내용 일부가 표시됩니다.

- **수신자에게 콘텐츠 경고**

수신자에게 부적절한 내용의 메일이 발송되었음을 알리는 메일을 발송합니다. 메일 미리보기에 메일 내용 일부가 표시됩니다.

- **경고메일**

유해요소가 발견된 메일이 있었음을 알리는 메일을 특정인에게 보내고자 할 때 설정합니다. 기본값은 수신자/발신자 모두 postmaster입니다.

- **다음 사용자가 보낸 메일 삭제**

특정한 메일 계정에서 오는 메일은 삭제하도록 지정합니다. 수신을 원하지 않는 발송자의 메일 주소를 추가합니다.

보고서

총 검사 메일 수 : 실시간 검사를 통해 검사된 메일의 개수 표시
총 감염 대상 수 : 실시간 검사를 통해 유해요소가 발견된 메일의 개수 표시

보관된 메일 보기

[설정>보관] 관련 매뉴얼 참조

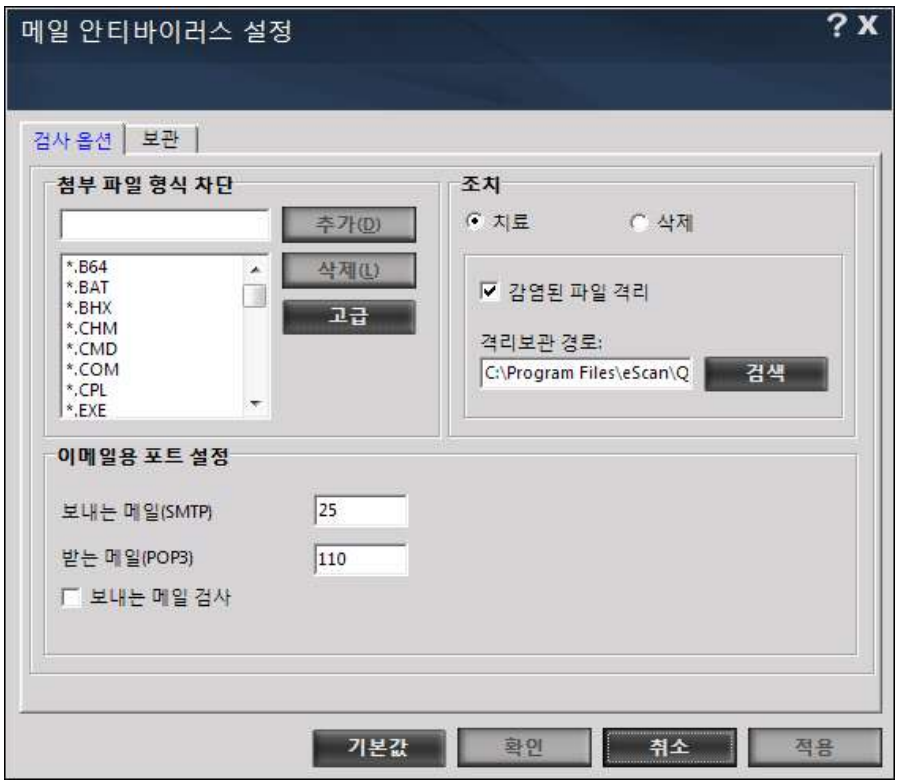
보고서

메일 안티바이러스 활동에 의한 날짜별 활동내용을 조회할 수 있습니다.

3.2 설정

검사옵션

검사를 수행할 이메일 종류를 선택하고, 유해사항 발견 시 조치 사항을 지정합니다.



● **첨부 파일 형식 차단**

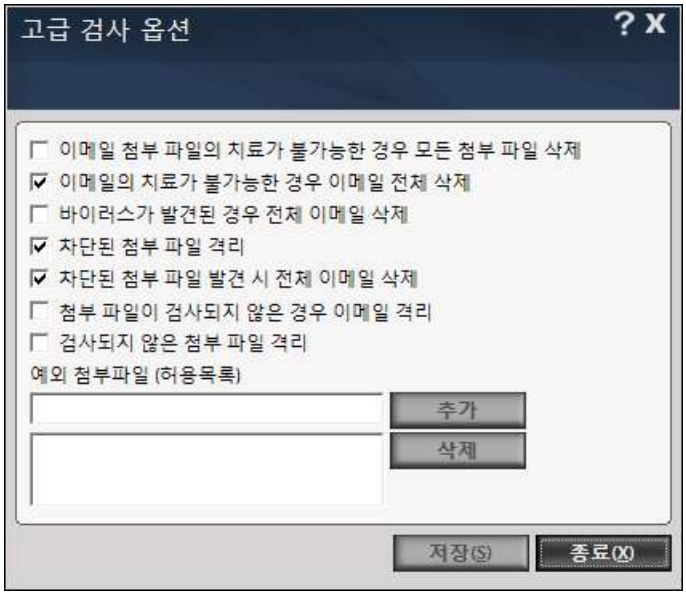
바이러스가 많이 이용하는 파일형태들을 사전에 정의하여, 이러한 파일이 첨부되는 메일들은 사용자에게 전달되기 전에 차단하거나 삭제하도록 합니다. 필요에 따라 확장자를 추가하거나 삭제할 수 있습니다. 필요에 따라 조정하시되, 최초에는 현재 정의된 확장자를 그대로 유지하시는 것이 좋겠습니다.

● **고급**

메일 검사와 관련하여 아래와 같은 옵션을 선택할 수 있습니다.

- 이메일 첨부파일의 치료가 불가능한 경우 모든 첨부파일 삭제
- 이메일의 치료가 불가능한 경우 이메일 전체 삭제 (기본설정)
- 바이러스가 발견된 경우 전체 이메일 삭제
- 차단된 첨부 파일 격리 (기본설정)
- 차단된 첨부 파일 발견 시 전체 이메일 삭제 (기본설정)
- 첨부 파일이 검사되지 않은 경우 이메일 격리
- 검사되지 않은 첨부 파일 격리
- 예외 첨부 파일 (허용목록) : 특정한 형태의 첨부 파일에 대해서는 수신을 허용하도록 설정합니다. 앞서의 차단 목록에 대해 우선합니다. 예를 들어 PIF 확장자를 가진 파일을 수신하기를 원한다면 *.PIF를 목록에 추가하면

되나, 가급적이면, ABC.PIF 와 같이 구체적인 이름을 넣어 주는 것이 좋겠습니다.



● **조치**

감염된 메일 발견 시 조치사항

- 치료 (기본설정) : 이메일 혹은 첨부파일을 치료하도록 합니다.
- 삭제 : 감염된 메일이나 첨부파일은 삭제하도록 합니다.
- 감염된 파일 격리 (기본설정) : 감염된 파일을 지정한 경로에 격리시켜 보관하도록 합니다. 보관 경로 초기값은 C:\Program Files\eScan\QUARANT 폴더이며 변경할 수 있습니다.

● **이메일용 포트 설정**

이메일을 발송/수신 할 때 사용할 포트 번호를 지정하면, 앞으로 메일 수발신에 이 포트를 사용하게 됩니다.

- 보내는 메일 (SMTP) : 기본값 25. SMTP 사용을 위한 포트 번호
- 받는메일 (POP3) : 기본값 110. POP3 메일을 위한 포트 번호
- 보내는 메일 검사 : 보내는 메일에 대해서도 검사를 수행하려면 선택

보관

이메일을 보관하는 방식에 대해 설정합니다.

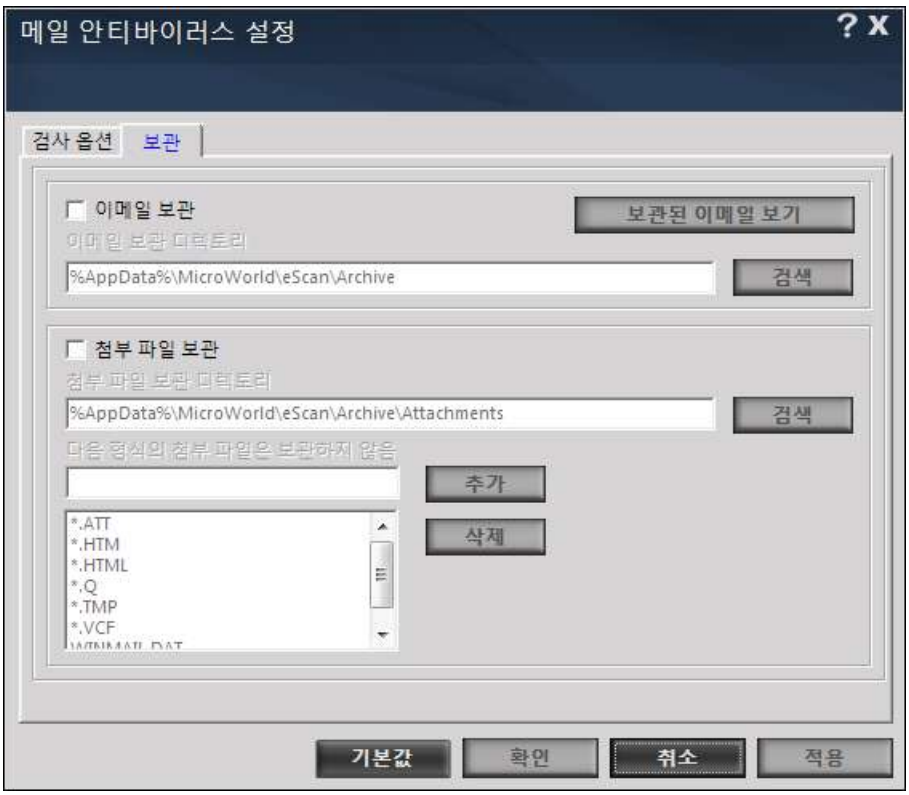
● **이메일 보관**

바이러스 검사를 수행한 메일들을 별도로 보관해 두도록 지정할 수 있습니다.

기본값으로는 선택이 되어 있지 않으나, 기능을 활성화 시키면 보관경로를 변경할 수 있으며 [보관된 메일 보기] 버튼으로 보관된 메일들 목록을 볼 수 있습니다.

- **첨부 파일 보관**

발송하거나 수신한 첨부 파일들을 별도의 폴더에 저장해 둘 수 있습니다. 기본값으로 선택이 되어 있지 않으나, 기능을 활성화 시키면 보관경로를 변경할 수 있습니다.



4. 안티스팸

정크메일이나 스팸메일을 인공지능 기반의 NILP 기술로 필터링하고 지정한 메일로 알림을 발송합니다.

4.1 메인

구성

안티스팸 상태 : 안티스팸 기능이 사용 중인지 여부를 표시
메일 피싱 필터 : 피싱 메일 감시 기능이 사용 중인지 여부를 표시
감염 발견 시 수행할 작업 : 감염된 메일 발견 시 수행하도록 지정한 조치사항을 표시

시작/중지

안티스팸 기능을 시작하거나 중지시킬 수 있습니다.

설정

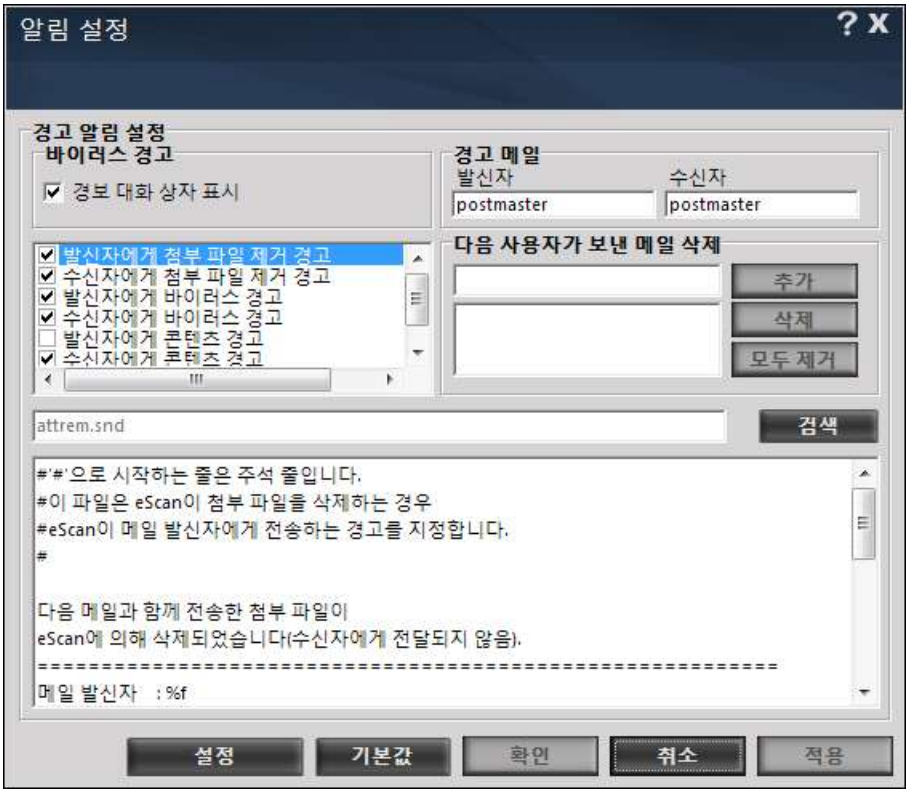
안티스팸 기능과 관련한 옵션들을 설정합니다.

- **기본값** : 최초 기본설정으로 옵션들을 설정합니다.
- **적용** : 변경한 옵션설정을 적용합니다
- **확인** : 현재 설정을 저장하고 창을 닫습니다.

- **취소** : 창을 닫습니다.

알림

유해요소가 포함된 메일이 발견되었을 때 누구에게 어떤 알림 메시지를 보낼 것인가를 지정합니다.



- **경보 대화 상자 표시 (기본설정)**

유해요소 발견 사실에 대한 안내창을 표시합니다.

- **발신자에게 첨부 파일 제거 경고 (기본설정)**

발신자에게 메일에 감염된 첨부파일이 있었음을 알리는 메일을 발송합니다. 메일 미리보기에 발송된 메일 내용 일부가 표시됩니다.

- **수신자에게 첨부 파일 제거 경고 (기본설정)**

수신자에게 메일에 감염된 첨부파일이 있었음을 알리는 메일을 발송합니다. 메일 미리보기에 메일 내용 일부가 표시됩니다.

- **발신자에게 바이러스 경고 (기본설정)**

발신자에게 감염된 메일이 발송되었음을 알리는 메일을 발송합니다. 메일 미리보기에 발송된 메일 내용 일부가 표시됩니다.

- **수신자에게 바이러스 경고 (기본설정)**

수신자에게 감염된 메일이 수신되었음을 알리는 메일을 발송합니다. 메일 미리보기에 메일 내용 일부가

표시됩니다.

- **발신자에게 콘텐츠 경고 (기본설정)**

발신자에게 부적절한 내용의 메일이 발송되었음을 알리는 메일을 발송합니다. 메일 미리보기에 발송된 메일 내용 일부가 표시됩니다.

- **수신자에게 콘텐츠 경고**

수신자에게 부적절한 내용의 메일이 발송되었음을 알리는 메일을 발송합니다. 메일 미리보기에 메일 내용 일부가 표시됩니다.

- **경고메일**

유해요소가 발견된 메일이 있었음을 알리는 메일을 특정인에게 보내고자 할 때 설정합니다. 기본값은 수신자/발신자 모두 postmaster입니다.

- **다음 사용자가 보낸 메일 삭제**

특정한 메일 계정에서 오는 메일은 삭제하도록 지정합니다. 수신을 원하지 않는 발송자의 메일 주소를 추가합니다.

보고서

격리 처리된 메일 수 : 실시간 검사를 통해 검사되어 격리 처리 된 메일의 개수 표시
정상 처리된 메일 수 : 실시간 검사를 통해 검사되어 정상 처리 된 메일의 개수 표시

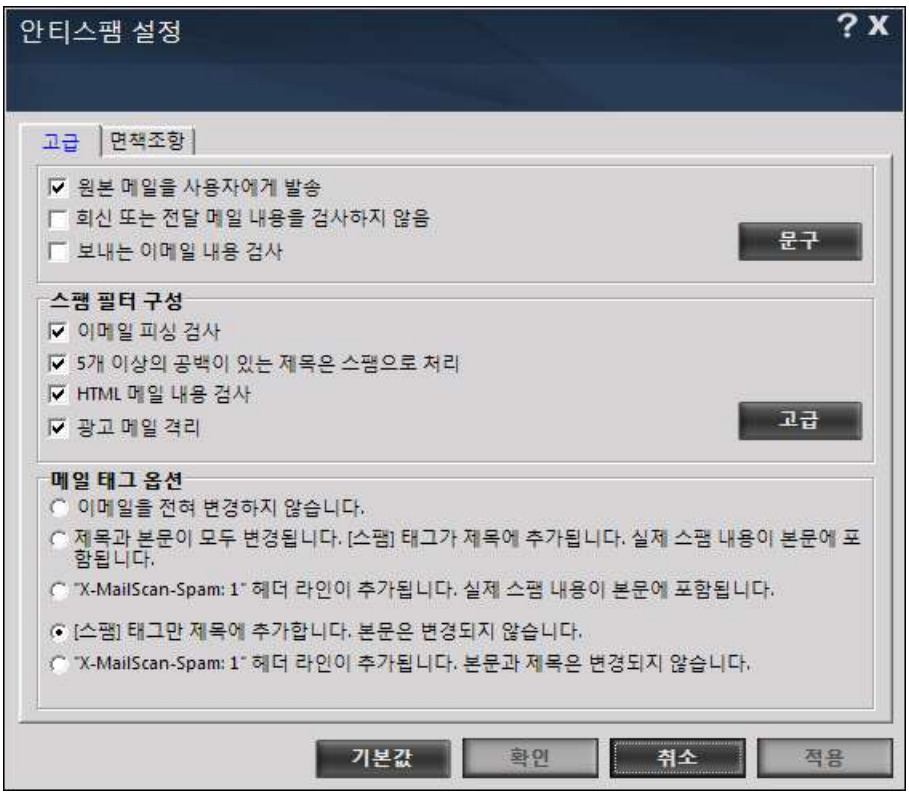
격리된 메일 보기

스팸메일로 분류되어 격리 처리 된 메일들을 조회할 수 있습니다.
스팸메일 : 스팸메일로 분류된 메일들을 조회할 수 있습니다.

보고서

안티스팸 활동에 의한 날짜별 활동내용을 조회할 수 있습니다.

4.2 설정



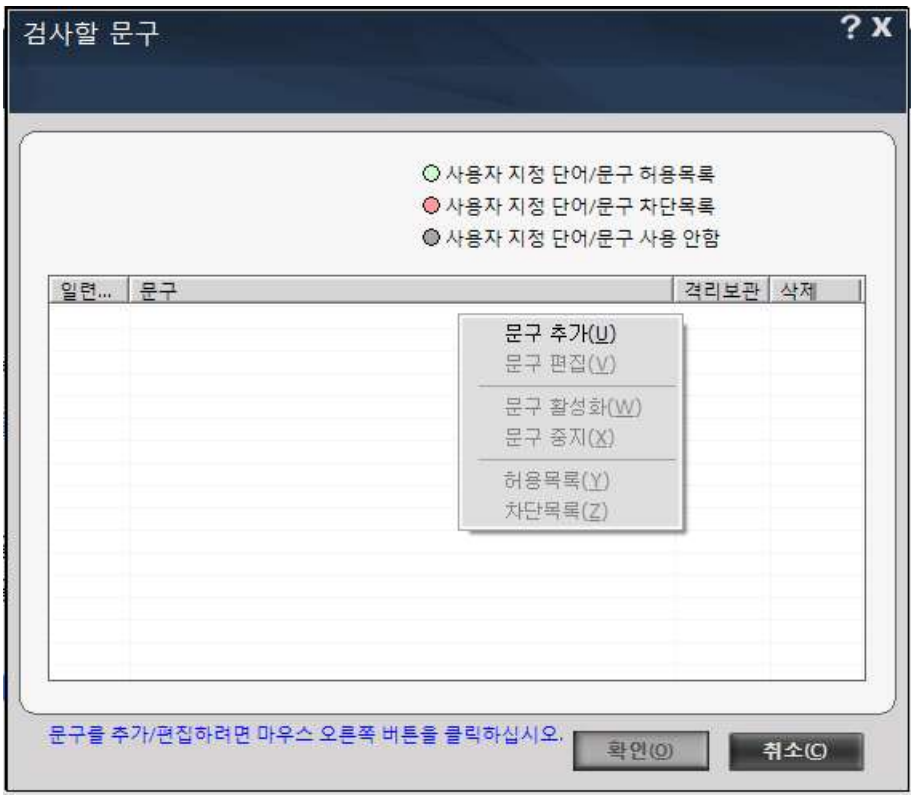
고급

일반 메일, 스팸 메일, 메일 태그와 관련된 옵션을 설정합니다.

- **안티스팸 설정**

– 원본 메일을 사용자에게 발송 (기본설정) : 스팸으로 분류되는 메일도 수신자에게 전달하고자 할 때 선택
– 회신 또는 전달메일을 검사하지 않음 : 사용자가 회신 또는 전달하는 메일은 검사하지 않도록 설정
– 보내는 이메일 내용 검사 : 사용자가 발송하는 메일도 검사하고자 할 때 선택

- [문구] 버튼을 클릭하여 스팸으로 필터링 할 단어나 문장을 추가할 수 있습니다.

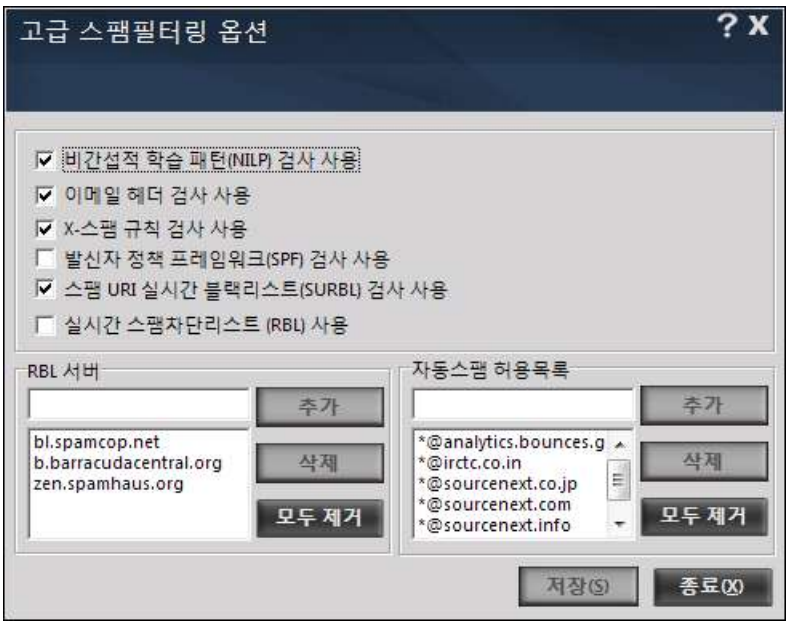


: 사용자 지정 단어/문구 허용목록 : 클릭하면 필터링 제외목록이 선택됩니다.
: 사용자 지정 단어/문구 차단목록 : 클릭하면 필터링 대상목록이 선택됩니다.
: 사용자 지정 단어/문구 사용 안함 : 클릭하면 필터링에 사용하지 않도록 지정한 목록이 선택됩니다.
: 기타 : 마우스 오른쪽을 클릭하면, 필터링 대상 단어/문구를 추가할 수 있습니다.

● **스팸 필터 구성**

- 이메일 피싱 검사 (기본설정) :
  사기성 이메일을 검사하여 격리 시킵니다.
- 5개 이상 공백이 있는 제목은 스팸으로 처리 (기본설정) :
  스팸 메일을 분석한 결과에 따르면 제목에 5개 이상의 공백이 포함되는 메일은 스팸인 경우가 많았으며, 이를 스팸 필터링에 적용하는 것입니다.
- HTML 메일 내용 검사 (기본설정) :
  일반 텍스트 메일 이외 HTML 메일도 검사합니다.
- 광고 메일 격리 (기본설정) :
  광고성 메일을 검사하여 격리 처리 합니다.

● **고급 설정**



– 비간섭적 학습패턴 (NILP) 검사 사용 (기본설정) :

NILP는 이스캔의 혁신적인 기술로 Bayesian 필터링과 인공지능 기법으로 각 메일을 분석하여 스팸메일이나 피싱 메일이 사용자에게 전달되지 않도록 차단하는 기법입니다. 자기학습 기능과 이스캔 서버의 스팸 메일 연구결과를 필터링에 반영합니다.

– 이메일 헤더 검사 사용 (기본설정) :

메일헤더를 분석하여 메일의 유효성을 검사합니다.

– X-스팸규칙검사사용 (기본설정) :

이스캔 데이터베이스에 저장되어 있는 스팸메일의 특성을 기반으로 검사를 수행합니다. 메일헤더, 메일내용, 첨부파일 등에 대하여 단어/문장별로 지수화된 데이터베이스를 통해 스팸지수를 산정하고, 이를 바탕으로 스팸을 걸러냅니다.

– 발신자정책프레임워크 (SPF) 검사사용 :

SPF는 발신자 정보를 속이지 못하도록 하기 위한 국제표준으로 피싱 메일 차단에 효과적입니다. 발신자 서버도메인의 SPF 레코드를 대조하게 되므로 인터넷에 연결되어 있는 경우에만 사용할 수 있는 옵션입니다.

– 스팸 URI 실시간 블랙리스트 (SURBL) 검사 사용 (기본설정) :

이메일 내용에 포함된 URL들을 점검하여 SURBL에 스팸 발송지로 등록된 것이 있으면 차단합니다. 인터넷에 연결되어 있는 경우에 사용할 수 있는 옵션입니다.

– 실시간 스팸차단리스트(RBL) 사용 :

RBL은 스팸을 발송하는 것으로 알려진 서버의 아이피 주소 목록입니다. 여기에 등록된 아이피에서 발송되는 메일은 스팸으로 간주하고 차단합니다.

– RBL 서버 :

RBL 목록을 관리하는 사이트를 추가하거나 삭제할 수 있습니다.한국인터넷정보진흥원에서 관리하는 목록의 주소는 spamlist.or.kr 입니다.

– 자동스팸 허용목록 :

스팸 필터링을 하지 않고 수신을 허용할 메일주소나 도메인 목록을 지정합니다.

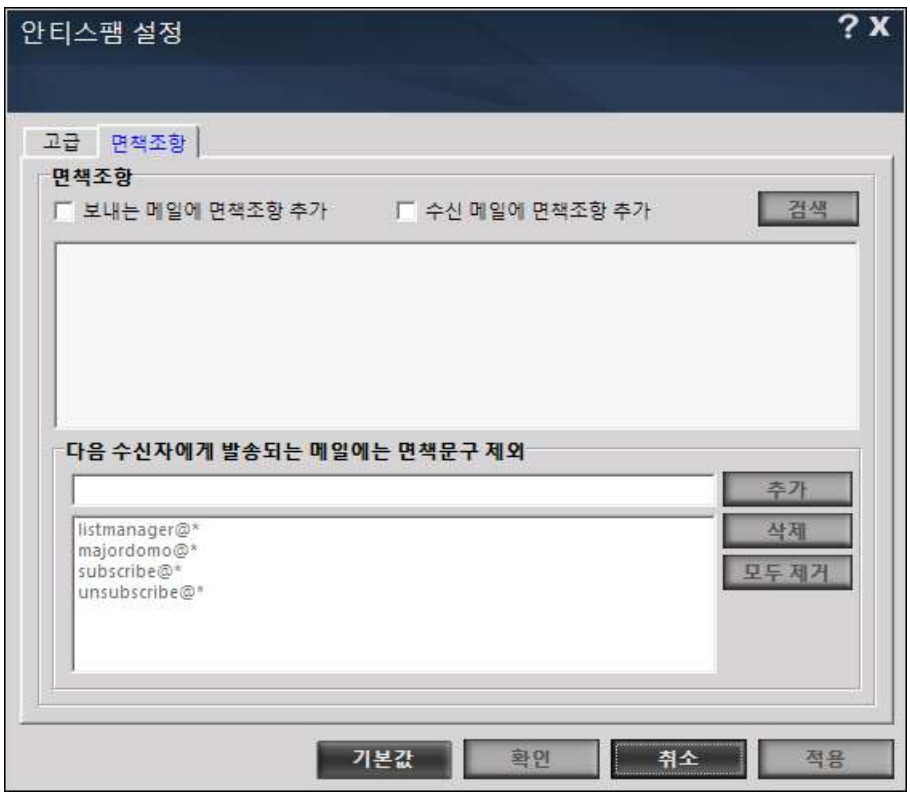
● **메일 태그 옵션**

스팸 메일이지만 사용자에게 전달하도록 설정한 경우, 스팸 메일이라는 표시를 추가할 수 있습니다.

- 이메일을 전혀 변경하지 않습니다 :
  받은 메일 그대로 전달되도록 합니다.
- 제목과 본문이 모두 변경됩니다. :
  제목에 [SPAM] 태그를 붙여서 메일이 전달됩니다. 본문 중에도 스팸 부분에 태그가 붙습니다.
- X-MailScan-Spam:1 헤더라인이 추가됩니다. :
  메일헤더에 스팸임을 알리는 내용이 추가되며, 본문에도 [SPAM] 태그가 붙습니다.
- [스팸] 태그만제목에추가합니다. (기본설정) :
  제목에 [SPAM] 태그를 붙여 메일을 전달합니다. 본문은 변경되지 않습니다.
- X-MailScan-Spam:1 헤더라인이 추가됩니다. 본문과 제목은 변경되지 않습니다.:
  메일헤더에 스팸임을 알리는 내용이 추가되며, 본문이나 제목은 그대로 유지하여 메일을 전달합니다.

면책조항

메일을 발송할 때에, 메일 하단에 지정한 문장이 추가되어 발송 되도록 합니다.



- 보내는 메일에 면책조항 추가 :
  보내는 메일에, 그 메일이 발송 전에 바이러스 검사를 마쳐 깨끗한 메일이라는 것을 안내하는 문장을 추가하여 발송되도록 합니다.

– 수신 메일에 면책조항 추가 :

컴퓨터를 이용하는 다른 사용자들이 수신하는 모든 메일에, 그 메일들은 바이러스 검사를 마쳐 깨끗한 메일이라는 것을 안내하는 문장을 추가되도록 합니다. 안내문장은 위 입력란에 직접 입력을 하거나, 문장 내용을 저장한 텍스트 파일을 [검색] 버튼으로 불러 들여서 지정합니다.

– 다음 수신자에게 발송되는 메일에는 면책문구 제외 :

아래 지정하는 메일 수신자에게 발송되는 메일에는 안내문장이 포함되지 않도록 합니다.

5. 웹 보호

웹 사이트에 포함된 단어나 문장을 검사하여 포르노성이거나 폭력적이거나 하는 등 사용자가 지정한 특정 형태의 사이트 접속을 차단합니다. 컴퓨터를 자녀들과 같이 사용하는 부모, 혹은 적절하지 못한 사이트 접속을 차단하고자 하는 회사에서 활용할 수 있습니다.

5.1 메인

구성

웹 보호 상태 (또는 자녀보호) : 웹 보호 기능이 사용 중인지 여부를 표시
웹 피싱 필터 상태 : 웹 피싱 감시 기능이 사용 중인지 여부를 표시
악성코드 URL 필터상태 : 악성코드를 배포하는 URL을 걸러내는 필터 사용 여부 표시

웹 보호 (자녀보호) 시작/중지

웹 보호 (또는 자녀보호) 기능을 시작하거나 중지시킬 수 있습니다.

피싱 필터 시작/중지

피싱 필터 기능을 시작하거나 중지시킬 수 있습니다.

•

악성코드 URL 필터시작/중지

악성코드 URL 필터 기능을 시작하거나 중지시킬 수 있습니다.

보고서

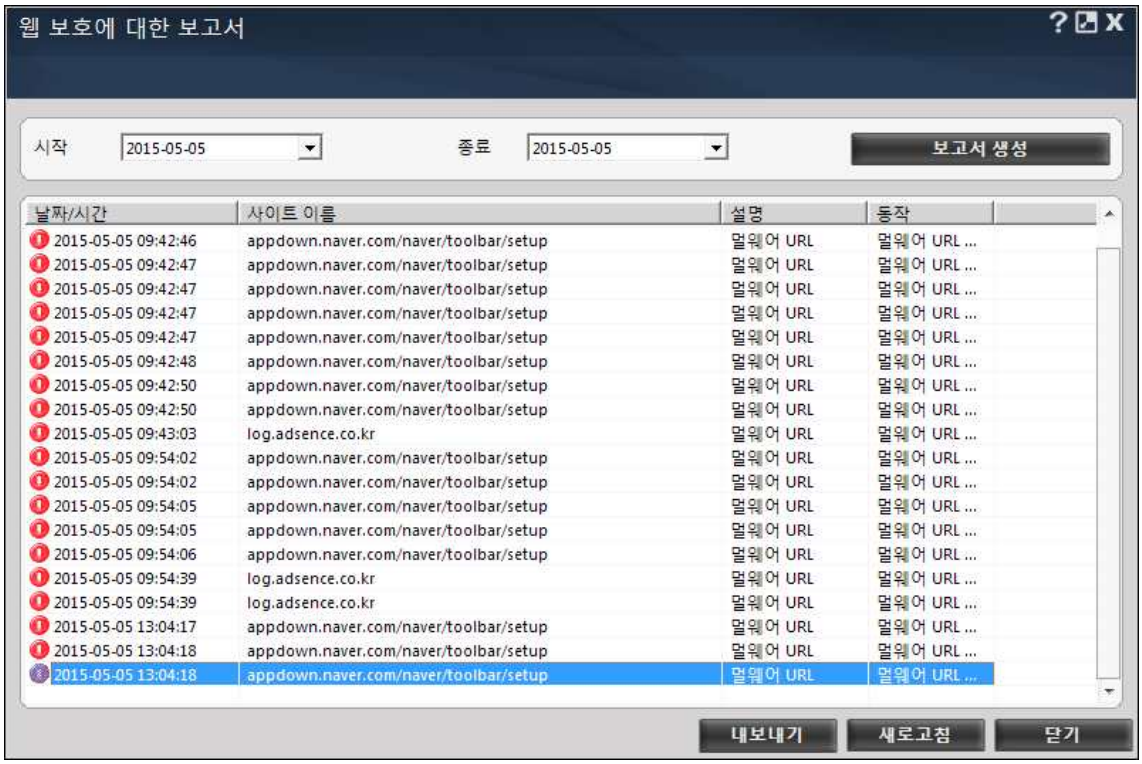
총 검사 사이트 수 : 검사가 이루어진 사이트 수
총 차단 사이트 수 : 검사되어 차단된 사이트 수
가장 최근 검사된 사이트 : 가장 최근 검사된 사이트 주소 표시

웹 보호 로그 보기

접속이 차단된 사이트에 대한 기록이 표시됩니다.

보고서

웹 보호 활동에 의한 날짜별 활동 내용을 조회할 수 있습니다.



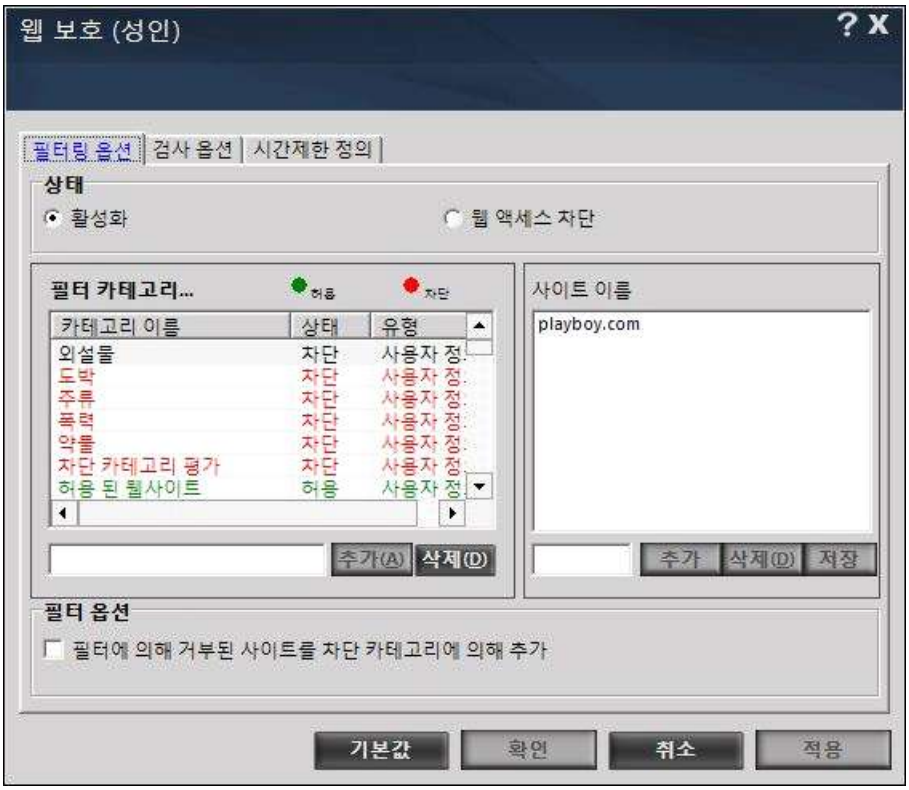
5.2 웹 보호 (또는 자녀보호) 설정

자녀보호 기능을 시작하면, 상세 기능을 설정할 수 있게 됩니다.

컴퓨터에 로그인 할 수 있는 계정들이 나타납니다.

1) 계정명을 선택하고, [프로필 선택]에서 성인/청소년/십대/어린이 로 계정 이용자의 특성을 지정합니다.
2) 왼쪽 위에 [사용/중지]를 메뉴을 클릭하여, 선택한 계정에 대한 웹 보호 기능 적용 여부를 지정합니다.
3) [프로필 편집]을 클릭하면, 웹 보호 기능의 상세 옵션들을 설정할 수 있습니다.

필터링 옵션



◆ **상태**

웹 사이트 카테고리별로 웹사이트 접속 차단 기능을 사용할 것인지를 선택합니다.

– 활성화 : 카테고리별로 허용/차단기준에 따라 사이트 접속을 허용 또는 차단하도록 설정합니다.

– 웹 엑세스 차단 : 지정한 사이트 이외의 모든 사이트 접속을 차단하도록 설정합니다.

◆ **필터카테고리**

각 웹 사이트를 카테고리별로 분류하여, 접속을 허용하거나 차단할 수 있습니다.

카테고리 이름을 더블클릭하면 허용/접속 설정이 바뀝니다.

– 녹색표시 : 접속을 허용하는 카테고리입니다.

– 적색표시 : 접속을 차단하는 카테고리입니다.

카테고리를 추가할 수 있으며, 각 카테고리별로 사이트를 추가/삭제 할 수 있습니다.

◆ **필터옵션**

– 필터에 의해 거부된 사이트를 차단카테고리에 추가 :

웹 보호기능에 의해 차단된 사이트를 차단카테고리에 추가하여 관리하도록 합니다.

이 사이트를 다시 접근할 때에는 사이트검사를 수행하지 않고 카테고리분류에 따라 차단됩니다.

검사옵션

◆ ActiveX 차단

ActiveX는 웹브라우저에 의해 자동으로 다운로드 되어 실행되는 컴포넌트 프로그램을 의미합니다. 악성코드가 유포되기도 하므로 주의가 필요합니다.

- 자바애플릿 :

자바로 씌어진 프로그램으로 HTML 페이지에 숨어 있으며, 자바 프로그램을 확인할 수 있는 브라우저에서 코딩을 볼 수 있습니다. 이 프로그램은 웹브라우저에서 사용자와 대화형으로 쉽게 사용할 수 있게 도움을 주지만, 역시 악성코드가 포함되어 있으면 운영시스템에 장애를 유발하거나 민감한 정보를 탈취하는데도 사용될 수 있습니다. 자바프로그램이 자동으로 다운로드 되는 것을 차단하고자 할 때 선택합니다.

- 스크립트 (Java &VB) :

스크립트는 JavaScript 혹은 VBScript 와 같은 언어로 쓰여진 것으로 사용자의 입력없이 수행될 수 있는 명령문들입니다. 웹사이트내에서 사용자편의를 위한 프로그래밍에 사용되나, 해커들이 악성스크립트를 사용하여 사용자 정보를 탈취하는 목적으로도 사용되므로, 이의 다운로드와 실행을 차단하고자 할 때 선택합니다.

- 바이러스검사 (기본설정) :

악성코드가 포함된 웹사이트 여부를 검사하고 차단합니다.

◆ 조치

- 위반로그 (기본설정) :

보안에 위협이 되는 웹사이트 방문에 대한 기록을 저장하여 다음 정책을 설정할 때 참고할 수 있도록 합니다.

- 30초 이내에 프로그램 종료 :

사용자가 지정한 설정에 저촉되는 경우 30초 이내에 브라우저를 닫아 버립니다.

◆ **포트설정**

컴퓨터에 드나드는 정보를 모니터링 할 포트번호를 지정합니다. 웹 브라우저들은 통상 80. 8080, 3128, 6588, 4480, 88번 포트를 인터넷 접속의 목적으로 사용합니다. 기타 점검하고자 하는 다른 포트가 있다면 같이 기록하여 모니터링 되도록 합니다.

◆ **콘텐츠 유형**

이미지 / 오디오 / 비디오 / 이메일 / 프로그램 등 지정한 형태의 자료가 다운로드 되는 것을 차단합니다.

시간제한정의

컴퓨터를 사용하는 다른 사용자에 대한 웹 사용 시간, 또는 웹 보호 기능의 적용 여부를 통제할 수 있습니다. 휴면상태 / 웹엑세스 차단을 선택한 상태에서 주간 일정표 상에 마우스로 선택하여 기능을 조절합니다.

- 활성화 : 웹 보호 기능을 사용하는 시간대를 지정합니다.
- 휴면상태 : 웹 보호 기능을 일시적으로 해제하는 시간대를 지정합니다.
- 웹 엑세스 차단 : 웹 사이트 접속을 전면 차단하는 시간대를 지정합니다.

6. 방화벽

방화벽은 컴퓨터로 들어오고 나가는 모든 데이터를 모니터링하여 네트워크를 통해 침입하는 모든 유해요소로부터 컴퓨터를 보호하기 위한 모듈입니다. 이스캔이 설정한 기본적인 통제규칙에 사용자의 필요에 의한 규칙을 추가하거나 삭제하여 운영합니다. 방화벽은 사용자가 지정한 규칙을 확인하고, 네트워크를 통해 전송되어지는 데이터패킷을 분석하여 규칙에 위배되는 데이터 이동을 차단합니다.

◆ **방화벽의 잇점**

컴퓨터가 인터넷에 연결되면 여러 가지 보안 위협에 노출 됩니다.
방화벽은 아래와 같은 다양한 형태의 네트워크 사용 활동에서 사용자의 데이터를 보호하게 됩니다.

- 인터넷을 통한 채팅으로 여러 경로를 통해 접속한 다른 사람들과 연결될 때
- 텔넷으로 원격지 서버에 접속을 하여 작업을 수행할 때
- FTP 로 서버에서 컴퓨터로 파일을 전송할 때
- LAN으로 연결된 다른 네트워크 사용자와 데이터를 주고 받을 때
- VPN (Virtual Private Network)에 연결된 컴퓨터를 사용할 때
- 인터넷을 사용하거나 이메일을 주고 받는 목적으로 컴퓨터를 사용할 때

◆ **방화벽 모드의 종류**

- 모두 허용 : 방화벽을 사용하지 않고, 들어오거나 나가는 모든 데이터를 허용합니다.
- 제한된 필터 (기본설정) : 들어오는 데이터를 필터링 합니다.

– 양방향 필터 : 들어오거나 나가는 모든 데이터 흐름을 필터링하되, 필요할 때 사용자 확인을 요청합니다.
– 모두 차단 : 모든 네트워크 접속을 차단 합니다.

6.1 메인

구성

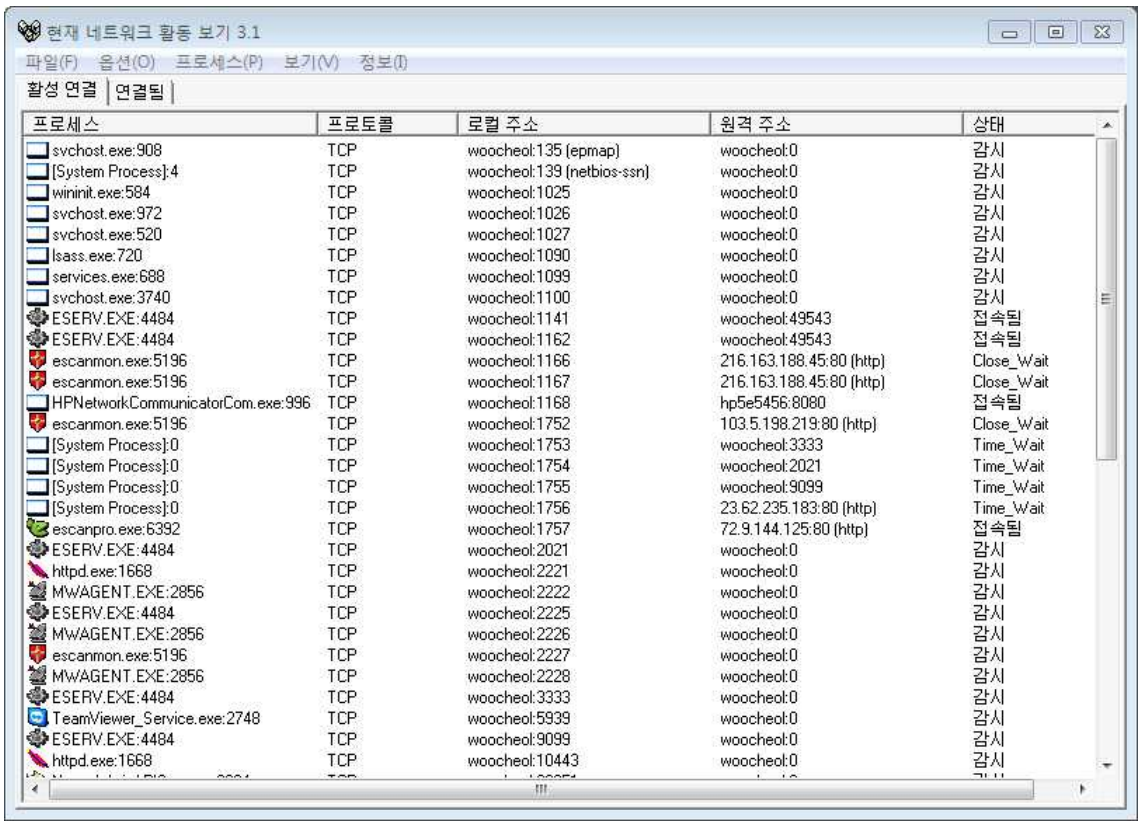
방화벽 상태 : 방화벽 설정 상태를 표시
필터링 시스템 : 선택된 방화벽 모드의 종류를 표시

보고서

인바운드 패킷 차단 : 방화벽에 의해 차단된 인바운드 패킷 수
아웃바운드 패킷 차단 : 방화벽에 의해 차단된 아웃바운드 패킷 수

현재 네트워크 활동 보기

현재 활성 상태에 있는 네트워크 연결을 실시간으로 표시합니다.



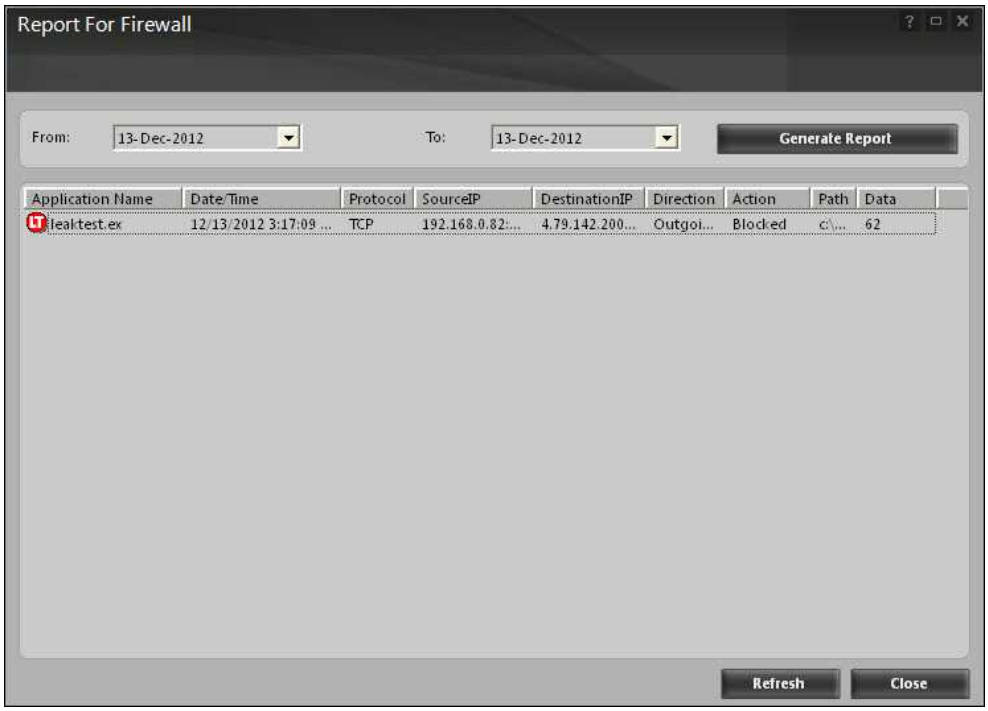
요약보기

방화벽의 활동에 대한 요약으로 활동별로 적용된 규칙을 표시합니다.

보고서

웹 보호 활동에 의한 날짜별 활동 내용을 조회할 수 있습니다.

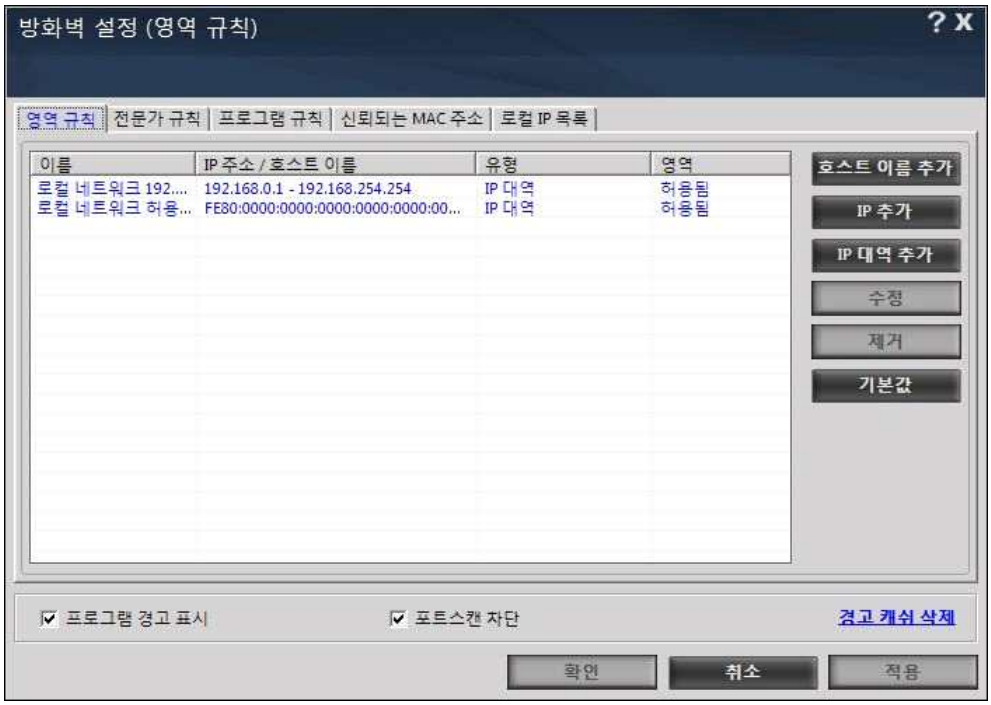
보고서는 네트워크 트래픽 그래프를 포함하며, 그래프의 단위는 KBps (초당전송되는 KB 단위 데이터량)입니다.



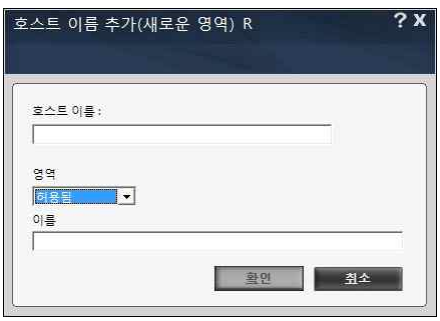
6.2 설정

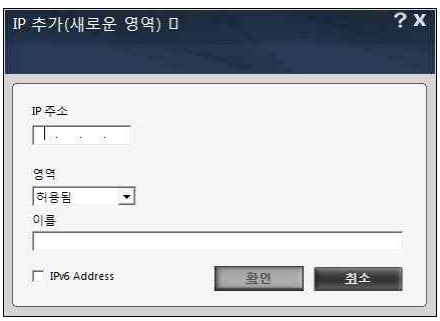
영역규칙

컴퓨터에 네트워크를 통해 접속할 수 있도록 허용할 아이피주소, 호스트명 등을 정의합니다.



- **호스트 이름 추가 :** 호스트 이름을 추가하고, 접속을 허용할지 차단할지 지정합니다.
- **IP 추가 :** 아이피 주소를 추가하고, 접속을 허용할지 차단할지 지정합니다.
- **IP 대역추가 :** 아이피대역을 추가하고, 접속을 허용할지 차단할지 지정합니다.

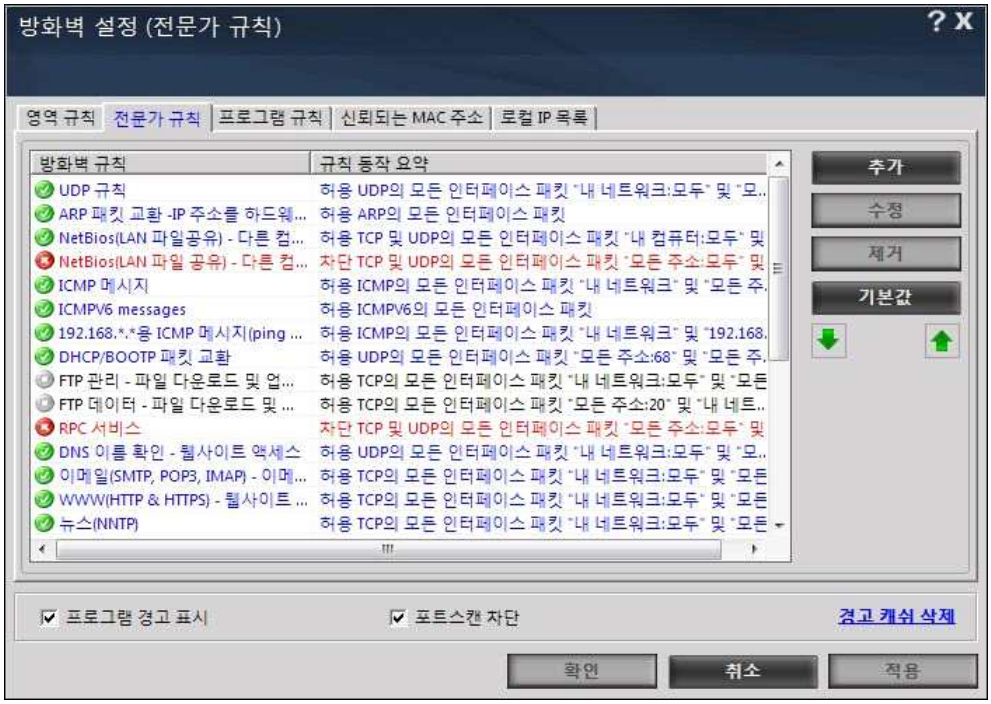




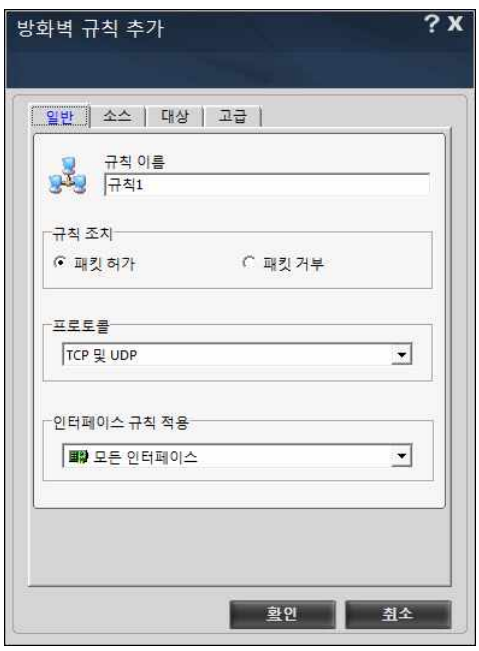
- **수정 :** 선택된 설정 내용을 수정합니다.

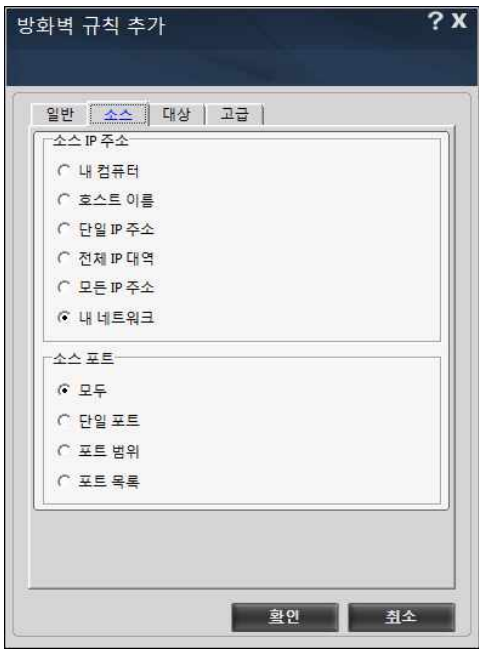
전문가 규칙

방화벽에 대한 이해가 있을 경우, 세부적인 규칙을 설정할 수 있습니다.

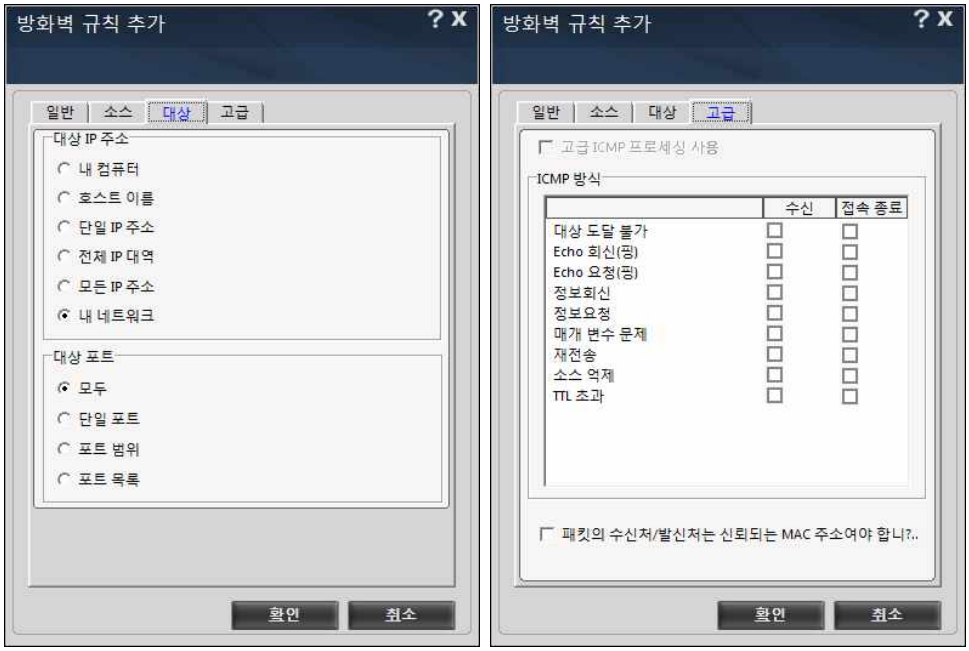


[추가] 버튼을 클릭하면 아래와 같은 대화창을 통해 규칙을 추가할 수 있습니다.





- 규칙이름은 임의로 지정합니다.
- 패킷을 허가하는 규칙인지 거부하는 규칙인지 지정합니다.
- 통신프로토콜과 인터페이스 규칙을 선택합니다.
- [소스]는 데이터 전송이 시작되는 곳에 대한 정보를 지정하기 위한 탭입니다.

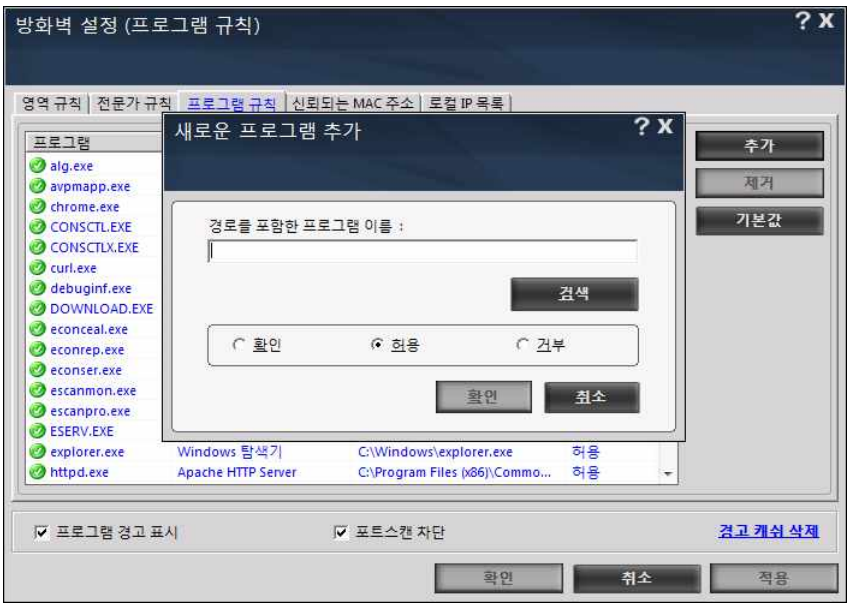


- [대상]은 데이터가 유입되는 위치에 대한 정보를 기록하기 위한 탭입니다.
- [고급] 탭은 프로토콜을 ICMP 로 선택한 경우에만 해당합니다.

프로그램 규칙

각 응용 프로그램별로 인터넷 접속에 대한 허용 여부를 설정합니다.

◆ **추가 :** 프로그램 규칙을 추가합니다.



추가하는 대화창에서 선택사항은 확인/허용/거부 중에서 선택합니다.

- 확인 : 프로그램이 네트워크에 접속하려고 할 때 사용자 승인을 구하도록 합니다.
- 허용 : 프로그램의 네트워크 접속을 허용합니다.
- 거부 : 프로그램의 네트워크 접속을 차단합니다.

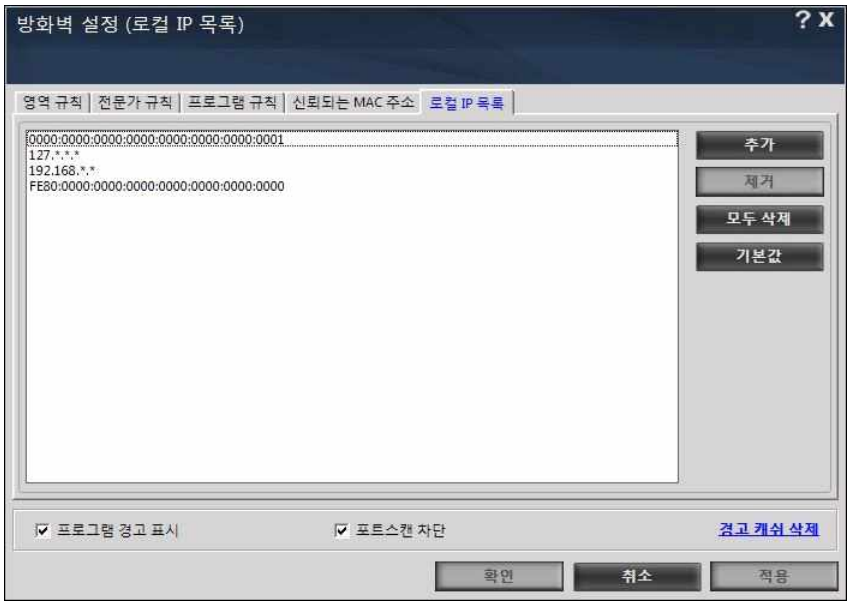
◆ **삭제 :** 프로그램 규칙을 삭제합니다.

신뢰되는 MAC 주소

MAC 주소는 네트워크 내에서 하드웨어를 인식하는 고유번호를 의미합니다.
[전문가규칙>고급]에서 [패킷의 수신처/발신처는 모두 신뢰 되는 MAC 주소여야 합니다] 가 선택 되었을 경우에만 필요하며, 패킷의 차단 여부는 전문가 규칙에서 설정한 바에 따릅니다.

로컬 IP 목록

로컬 아이피 주소목록을 표시합니다.



공통

- 프로그램 경고표시 (기본설정) :
  프로그램 규칙에 따라 프로그램의 실행이나 인터넷 접속이 차단될 때 안내창이 표시됩니다.
- 포트스캔차단 (기본설정) :
  내 컴퓨터에서 가용한 포트 정보를 추출하려는 해커의 시도가 발견되면 차단합니다.
- 경고 캐쉬 삭제 :
  방화벽에 의해 저장된 임시 기록 (프로그램 차단 등)을 삭제합니다.

7. 엔드포인트 보안

엔드포인트 보안은 USB 장치나 방화벽 기반의 이동식 저장 장치에 의한 정보 유출이나 보안 위협으로부터 컴퓨터를 보호하고자 하는 모듈로써, 응용 프로그램이 사용자도 모르는 사이에 실행되는 것도 차단할 수 있습니다. 외부 장치 혹은 응용 프로그램에 대한 보고서는 어떤 프로그램 혹은 어떤 장치를 사용하고 차단할지 선택하는데 큰 도움이 될 것입니다.

7.1 메인

구성

엔드포인트 보안 상태 : 엔드포인트 보안 활동 상태 표시
프로그램 관리 : 응용 프로그램에 대한 통제 기능 활동 상태 표시
장치 제어 : 장치 제어 기능 활동 상태 표시

보고서

허용된 프로그램 수 : 실행이 허용되고 있는 응용 프로그램의 수
차단된 프로그램 수 : 실행이 차단고 있는 응용 프로그램의 수

시작 / 중지

엔드포인트 보안 기능의 시작 또는 중지

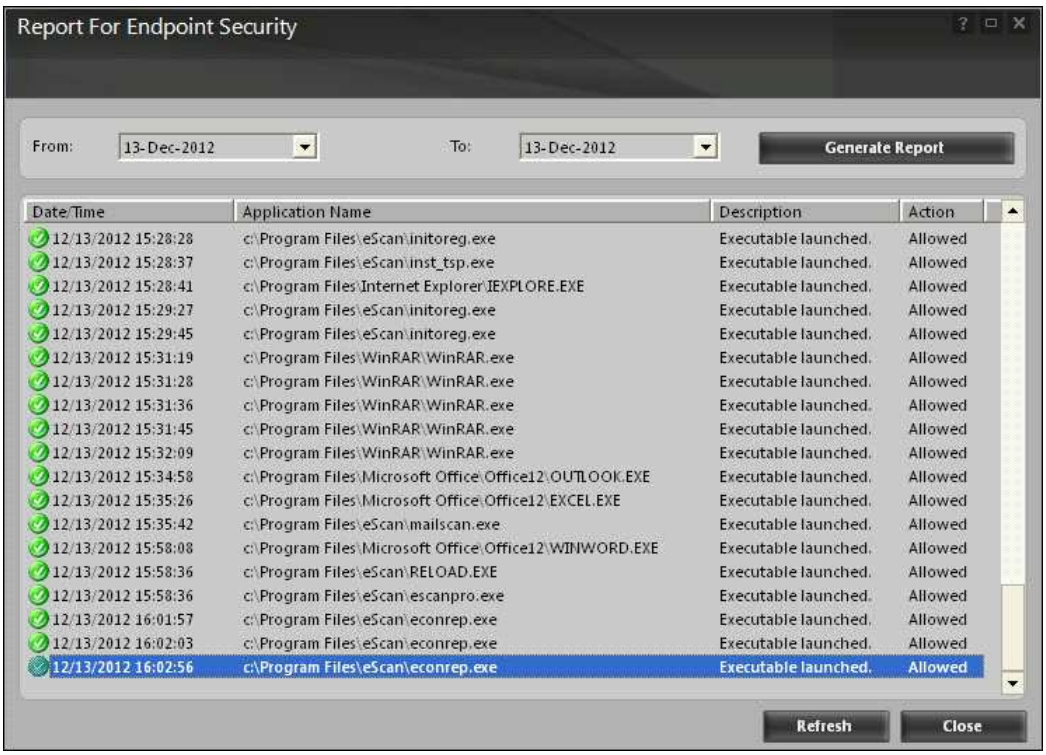
설정

엔드포인트 기능과 관련한 옵션들을 설정합니다.

- **기본값** : 최초 기본설정으로 옵션들을 설정합니다.
- **적용** : 변경한 옵션설정을 적용합니다
- **확인** : 현재 설정을 저장하고 창을 닫습니다.
- **취소** : 창을 닫습니다.

보고서

엔드포인트 보안 활동에 의한 날짜별 활동 내용을 조회할 수 있습니다.



7.2 설정

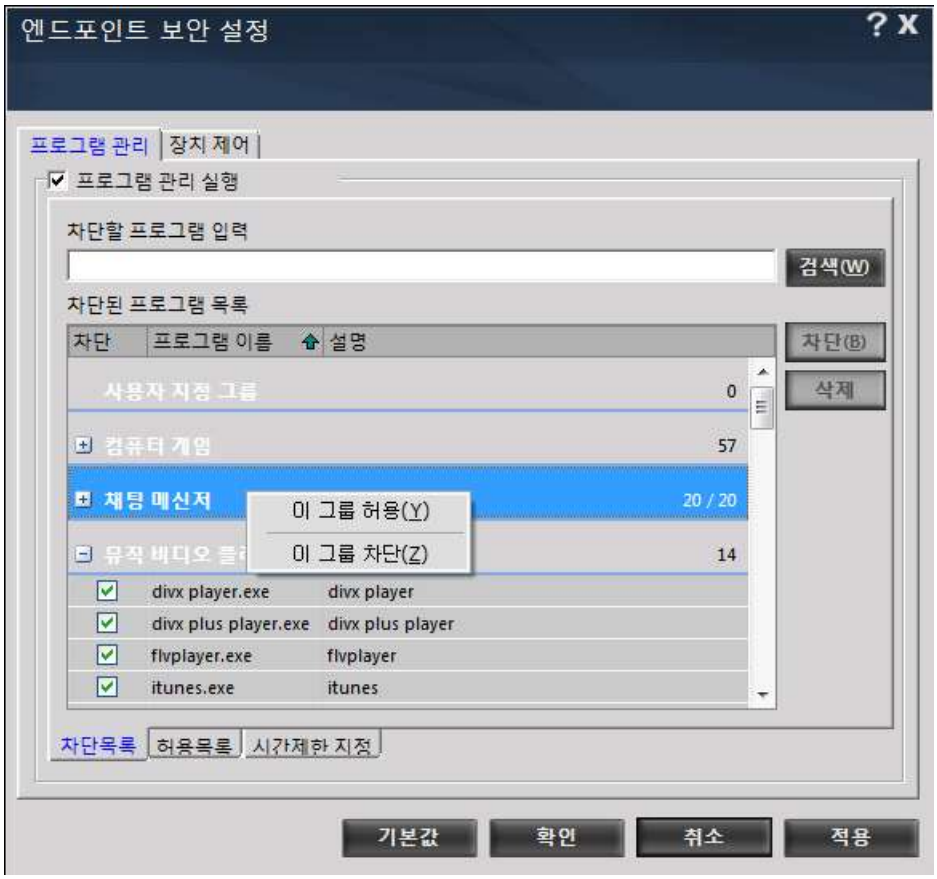
프로그램 관리

- **차단 목록**

실행을 차단하고 있는 프로그램 목록입니다.
차단된 프로그램 중 일부를 허용하려면, 프로그램명 앞에 선택을 해제하면 됩니다.

그룹별로 분류되어 있으며, 아래 그림과 같이 그룹별로 실행을 허용하거나 차단할 수 있습니다.
[이 그룹 허용]을 선택하면, 선택된 그룹 내 프로그램은 선택상태가 해제되어 차단되지 않게 됩니다.

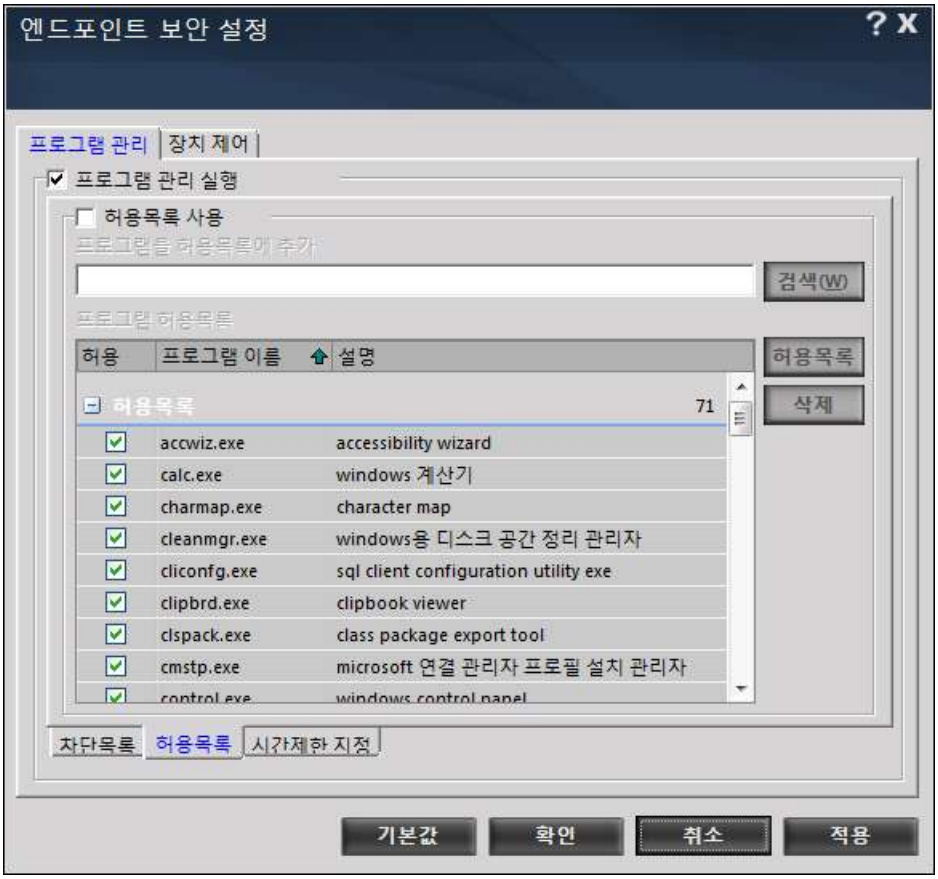
– 프로그램 관리 실행 :
선택되어 있지 않는 경우에는 프로그램 실행을 차단하지 않습니다.
부적절한 프로그램들을 목록에 추가하고, 실행을 차단하고자 하면 선택해 주세요.



[검색] 으로 차단시킬 프로그램을 선택하고, [차단] 버튼을 누르면 목록에 추가됩니다.

◆ **허용 목록**

[허용 목록 사용]을 선택하면, 목록에 있는 프로그램만 사용할 수 있게 되며,
나머지 프로그램들은 모두 실행되지 않도록 차단합니다.



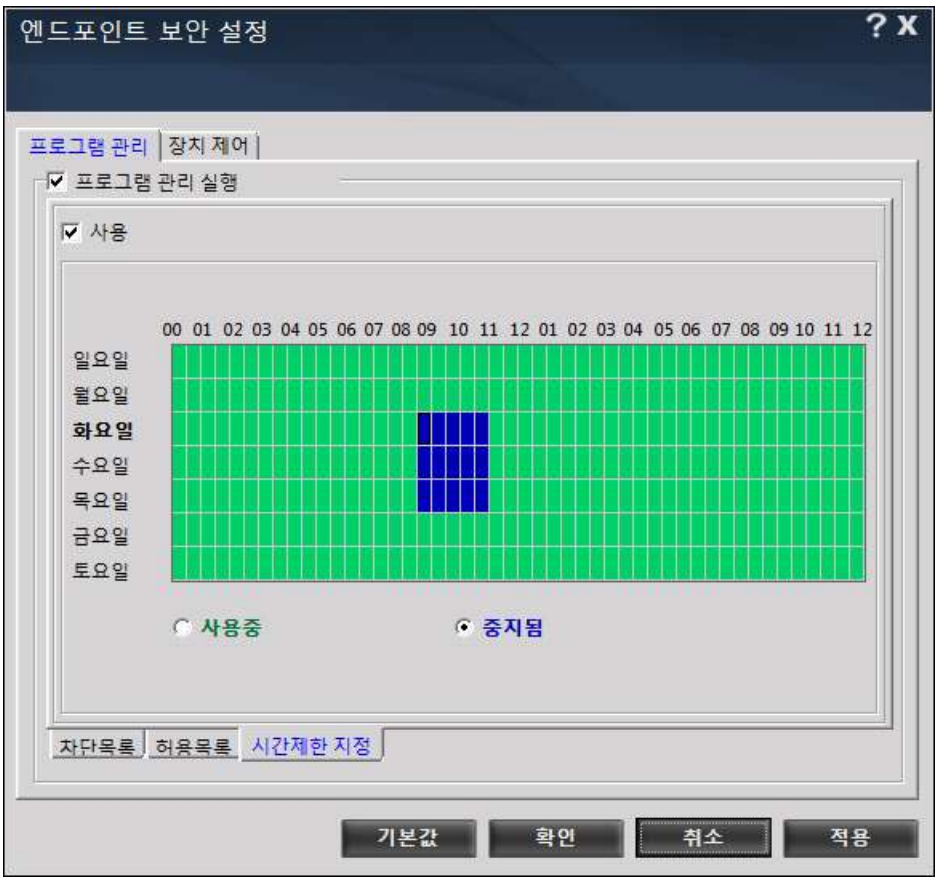
[검색] 으로 프로그램을 선택하고, [허용목록] 버튼을 누르면 목록에 추가됩니다.

◆ **시간제한 지정**

[프로그램 관리] 기능을 일정 기간 중지시킬 필요가 있을 때 설정합니다.

[중지됨] 을 선택한 상태에서 주간 단위 일정표에 마우스로 [프로그램 관리] 기능을 사용하지 않을 시간대를 마우스 클릭 또는 마우스 끌기로 선택합니다.

이렇게 파란색으로 선택한 시간대에는 엔드포인트 보안 중 프로그램 관리가 작동을 하지 않게 되므로, 모든 프로그램을 제한 없이 사용할 수 있게 됩니다.



장치 제어

이동식 장치를 통한 바이러스 확산과 데이터 유출을 방지하기 위한 기능입니다.

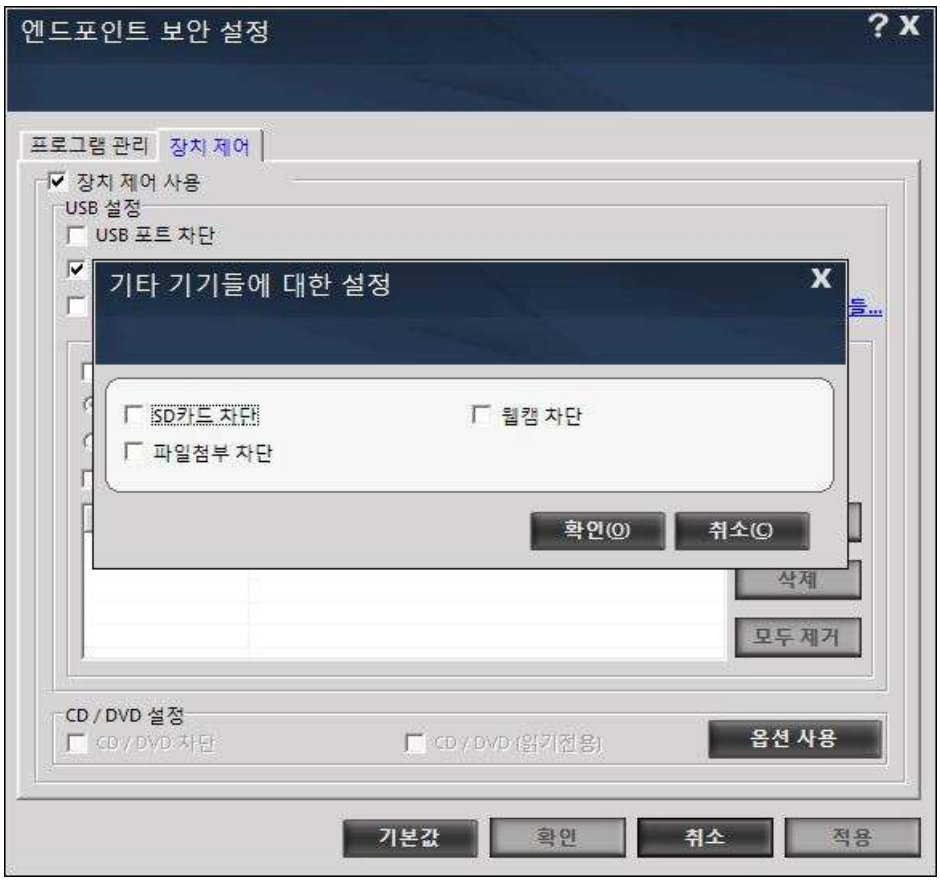
USB 장치가 연결될 때 비밀번호를 요구하게 하거나 연결을 차단시킬 수 있습니다.
필요에 따라 읽기만 허용하게 하여 데이터 유출을 예방하는 목적으로 활용합니다.
장치가 연결될 때마다 바이러스 검사를 수행하게 하여 이동장치에 의한 감염을 예방합니다.

- **장치 제어 사용 :** 장치 제어 기능을 사용하려면 선택합니다.
- **USB 포트 차단 :** USB 포트를 사용할 수 없도록 차단합니다. 다른 모든 옵션들은 비활성화 됩니다.
- **바이러스 검사 :** USB 장치가 연결되면 바이러스 검사를 자동 실행합니다.
- **자동재생 중지 :** USB 장치에 자동실행 파일이 있는 경우에 실행되지 못하도록 차단합니다.
- **읽기전용-USB :** USB 장치에 기록할 수 없도록 하여 데이터 유출을 방지합니다.
- **비밀번호 요청 :** USB 장치를 사용하기 위해서는 비밀번호를 입력해야만 하도록 설정합니다.
  - 이스캔 관리자 비밀번호 사용 : 이스캔 관리자 비밀번호를 입력하도로 합니다. (하단 [비밀번호] 메뉴에서 변경
  - 다른 비밀번호 사용 : USB 통제를 목적으로 하는 별도의 비밀번호를 입력
  - 허용목록의 USB 장치 검사 : 허용목록에 장치를 등록하면, 이들에 대해서는 비밀번호를 묻지 않게 됩니다.
- **CD/DVD 설정 :** CD/DVD를 차단하거나 읽기 전용으로만 사용하도록 설정합니다.

참고 : 이미 연결되어 사용 중인 USB 장치는 설정에 영향을 받지 않습니다.

◆ **기타 기기들**

[기타 기기들] 링크를 클릭하면, 아래와 같은 대화창이 나타납니다.



- SD 카드 차단 : SD 카드를 사용할 수 없도록 차단합니다.
- 웹캠 차단 : 웹캠을 사용할 없도록 차단합니다.
- 파일첨부 차단 : 이메일을 작성할 때 파일 첨부를 할 수 없도록 하여 정보유출을 예방합니다.

8. 사생활 보호

인터넷을 사용하는 동안에 컴퓨터에는 여러 가지 종류의 임시 파일들이 저장됩니다. 인터넷 속도를 빠르게 하기 위해서, 다음 번 로그인을 쉽게 하기 위해서 등의 목적으로 사용되나, 때로는 민감한 개인정보가 저장되었을 수도 있습니다. 이스캔의 사생활보호 모듈은 이러한 임시파일들을 삭제함으로써 개인정보가 탈취되거나 악용되는 것을 방지하는 기능입니다.

8.1 메인

구성

사생활보호 상태 : 수동으로 삭제하는지 예약된 시간에 정기적으로 삭제하는지를 표시 (수동 또는 예약)
다음 청소 일정 : 예약된 경우는 예약시간 표시

지금 청소

설정된 내용에 따라 임시저장 파일 삭제 진행

설정

사생활보호 기능과 관련한 옵션들을 설정합니다.

- **기본값** : 최초 기본설정으로 옵션들을 설정합니다.

- **적용** : 변경한 옵션설정을 적용합니다
- **확인** : 현재 설정을 저장하고 창을 닫습니다.
- **취소** : 창을 닫습니다.

보고서

최근 시스템 청소일 : 최근 임시파일 삭제 시간 표시

8.2 설정

브라우저

컴퓨터에 설치되어 있는 모든 브라우저들에 대한 정보를 표시합니다.

일반

웹 브라우저 혹은 다른 프로그램에 의해 생성된 임시 파일들의 종류가 나열되어 있으며, 삭제하고자 하는 종류의 파일을 선택합니다.

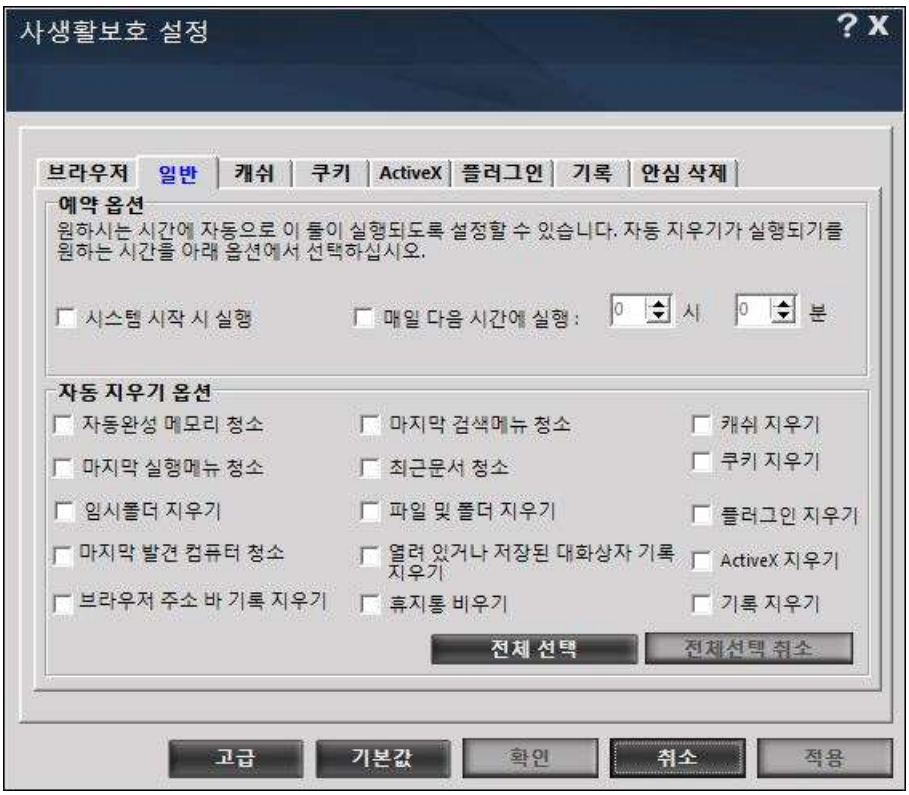
- **예약 옵션**

파일 삭제 작업을 진행할 시간을 예약합니다.
예약하지 않으면 별도로 관리되지는 않으며, 필요할 때 [사생활보호 > 지금 청소] 로 삭제하여야 합니다.

◆ **자동 지우기 옵션**

웹 브라우저는 사용자가 방문한 사이트들을 추적할 수 있는 정보를 특정 폴더에 저장합니다. 이 정보들은 다른 사람들에 의해 보여질 수 있는데, 이스캔은 이러한 정보들을 삭제할 수 있도록 하는데, 이를 위해서 컴퓨터에 설치되어 있는 모든 종류의 브라우저 정보를 파악하고, 저장된 정보의 종류와 경로를 표시합니다.

삭제할 임시파일의 종류를 선택하면, [지금 청소] 혹은 예약된 시간에 자동 삭제 됩니다.

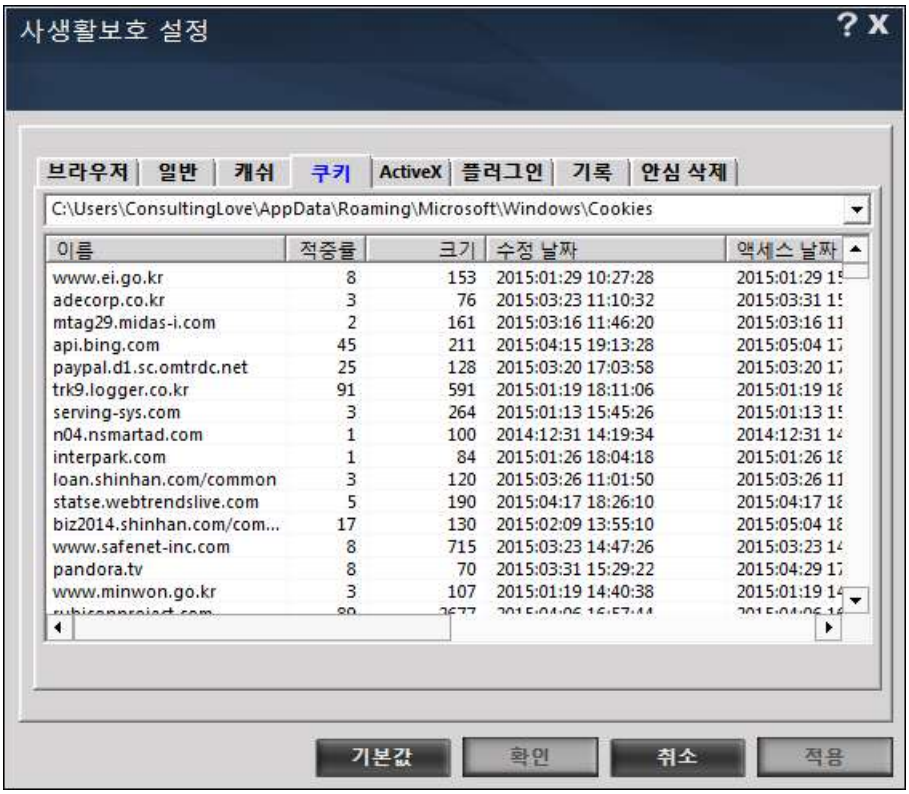


- 자동완성 메모리 청소 : 웹 사이트에서 검색/로그인 등을 위해 입력했던 정보로, 해커들은 이 정보로 로그인 정보를 얻거나 개인별 서핑 습관을 모니터링 합니다. 이런 정보들을 삭제합니다.
- 마지막 검색메뉴 청소 : 최근 검색에 사용하였던 키워드 정보 작세
- 캐쉬 지우기 : 웹 사이트 방문시 다음 방문 속도 향상을 위해 다운받아 저장된 임시 인터넷 파일 삭제
- 마지막 실행메뉴 청소 : 최근 실행한 프로그램 정보 삭제
- 최근 문서 청소 : 최근 수정한 문서 정보 삭제
- 쿠키 지우기 : 웹 사이트 방문 시 각 사이트가 생성한 파일들 삭제
- 임시폴더 지우기 : 웹 브라우저, 응용 프로그램들이 임시로 저장한 데이터를 보관하는 폴더 내용 삭제
- 파일 및 폴더 지우기 : [안심 삭제]에서 선택한 파일들을 복구 불능 상태로 완전히 삭제
- 플러그인 지우기 : 브라우저 플러그인 프로그램들을 삭제
- 마지막 발견 컴퓨터 청소 : 최근 검색한 네트워크 상 다른 컴퓨터 정보 삭제
- 열려있거나 저장된 대화상자 기록 지우기 : 현재 열려있거나 저장된 파일들의 링크 정보 삭제
- ActiveX 지우기 / 브라우저 주소 기록 지우기 / 휴지통 비우기 : 관련 내용 삭제
- 기록 지우기 : 최근에 방문했던 웹 사이트 정보 삭제

캐쉬 / 쿠키 / ActiveX / 플러그인 / 기록 (방문이력)

현재 컴퓨터에 기록되어 있는 정보들을 각 항목별로 표시합니다.
어떤 정보들이 저장되어 있는지 확인할 수 있습니다.

예를 들어
[캐쉬] 탭에는 각종 임시파일들 목록이,
[쿠키] 탭에는 쿠키를 저장한 사이트 목록이 표시됩니다.



9. 클라우드 보호

클라우드 보호는 신종 바이러스, 웜, 트로이목마 등이 널리 퍼지기 이전에 탐지하고 차단하는 기능으로, ESN (eScan Security Network) 기술을 사용합니다.

클라우드 보호의 내용을 정리하면 아래와 같습니다.
- 전 세계 이스캔 사용자에 기반한 보안 네트워크 (ESN) 를 통해 유해요소를 상시 모니터링합니다.
- ESN은 다운로드 된 파일이나 실행되고 있는 프로그램이 의심스러운 경우 이를 이스캔 연구소로 전송합니다. 이러한 파일은 웹 사이트, 이메일 첨부파일, P2P 채팅 등 다양한 경로를 통해 발견됩니다.
- ESN은 개인용 프로그램을 사용하는 모든 사용자들의 동의 하에 진행되며, 이러한 활동에 있어서 이름, 비밀번호 등 어떠한 개인정보도 수집하지 않습니다.
- 연구 대상이 된 프로그램 파일의 안전성은 유효한 디지털 시그니쳐의 여부와 함께 많은 요소들을 종합 검토하는 이스캔의 프로그램 분석 알고리즘을 통해 평가합니다.
- 프로그램이 안전하지 않거나 멀웨어라고 판단되면, 이에 대한 대책이 마련되기 이전에라도 모든 사용자에게 전파되어 사전 차단할 수 있도록 대비합니다.
- 전송된 유해요소에 대한 보호 대책 혹은 치료법을 마련하여 사용자에게 전송합니다.

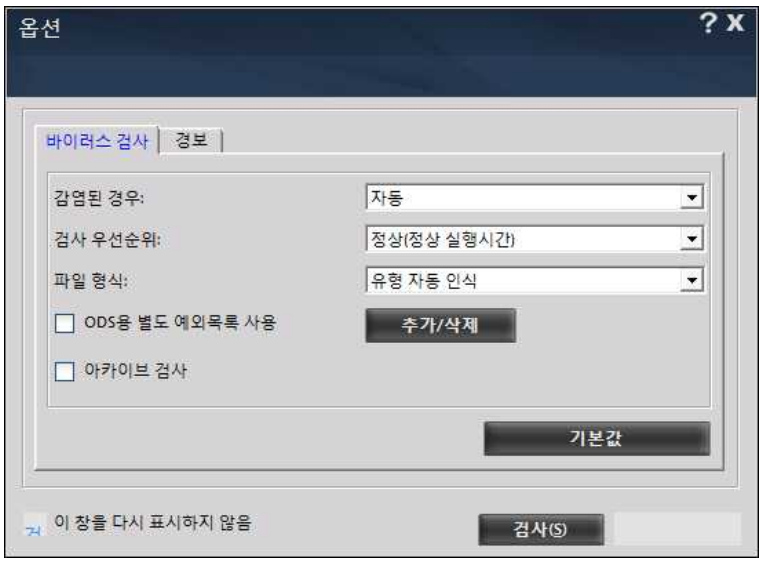
이를 통해서 이스캔은 새로운 사이버 공격에 대하여, 대응에 여러 시간이 걸리던 기존 시그니처 데이터베이스 업데이트 방식과 달리, 몇 분 이내에 인지하고 대비할 수 있게 되었습니다.

아래와 같이 클라우드 보안 네트워크에 참여한다는 내용에 체크만 해 주시면 됩니다.

10. 바이러스 검사

필요한 경우 언제든지 컴퓨터 내 폴더, 파일, 저장장치, 레지스트리 등에 대한 바이러스 검사를 수행할 수 있으며, 일정을 정하여 정기적으로 검사를 수행시킬 수 있습니다.

메뉴 중에서 검사 대상 링크을 클릭하면 아래와 같은 대화창을 통해 바이러스 검사를 진행하며, 바이러스, 멀웨어, 에드웨어 등을 탐색하여 치료하거나 격리하게 됩니다.



10.1 메인

메모리, 레지스트리, 서비스 및 시스템 폴더 검사

메모리, 레지스트리, 서비스 및 시스템 폴더에 대한 바이러스 검사
옵션 설명은 하기 [옵션] 메뉴 참조

컴퓨터 검사

컴퓨터 디스크 드라이브 대상 검사, 검사 옵션 설명은 하기 [옵션] 메뉴 참조

USB 드라이브 검사

USB 드라이브 검사, 검사 옵션 설명은 하기 [옵션] 메뉴 참조

CD-ROM 검사

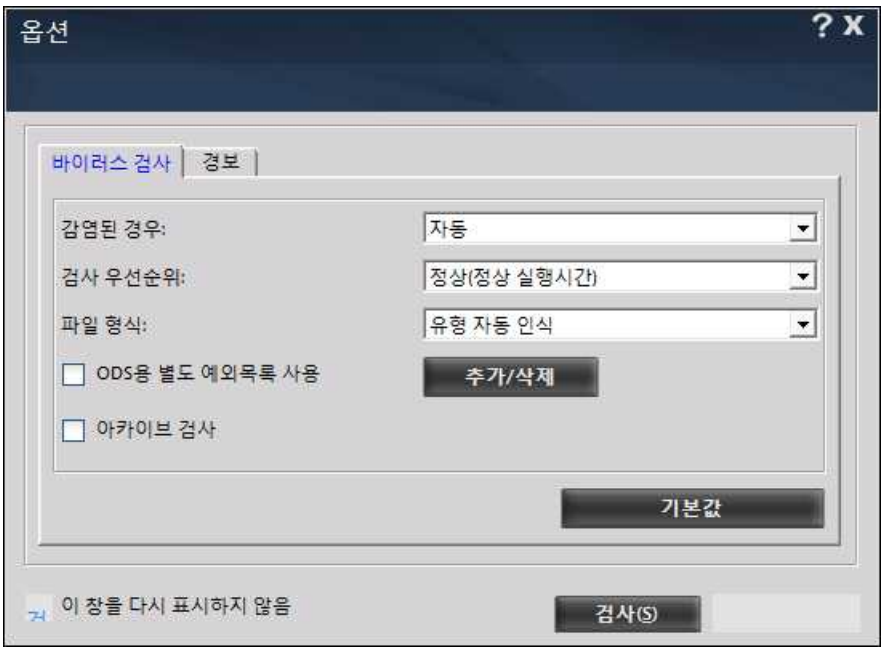
CD-ROM 검사, 검사 옵션 설명은 하기 [옵션] 메뉴 참조

사용자 지정 검사

검사 대상을 임의로 선택하여 검사 실행, 검사 옵션 설명은 하기 [옵션] 메뉴 참조

10.2 옵션

바이러스 검사



◆ **감염된 경우**

감염된 파일을 발견했을 때 조치 사항을 지정합니다.

- 로그전용 : 발견했다는 기록만 남깁니다. 로그 파일을 정기적으로 확인해 주셔야 합니다.
- 감염된 파일 삭제 : 감염된 파일을 삭제 처리합니다.
- 자동 (기본설정) : 발견되면, 치료를 시도합니다. 치료가 실패하면 실행되지 않도록 격리시켜 보관하거나 삭제 처리합니다.

◆ **검사 우선 순위**

- 높음 :

다른 프로그램 실행에 우선하여 검사를 수행합니다.
검사 시간은 짧으나, 컴퓨터 리소스가 부족하면 다른 프로그램의 실행 속도가 느려질 수 있습니다.

- 정상 (기본설정) :

다른 프로그램과 같은 조건으로 메모리를 할당받아 실행합니다.

- 낮은 순위 :

다른 프로그램들이 실행될 때 방해가 되지 않는 선에서 검사를 수행합니다.
실행하고 있는 프로그램이 많으면 검사 시간이 길어집니다.

◆ **파일 형식**

- 유형 자동 인식 (기본설정)
  모든 파일을 대상으로 검사를 수행하나, 감염이 될 수 없는 종류의 파일들은 검사를 생략합니다.
- 프로그램 파일만
  프로그램 파일이거나 실행 파일만을 대상으로 검사를 수행합니다.

◆ **ODS 용 별도 예외 목록 사용 (기본설정)**

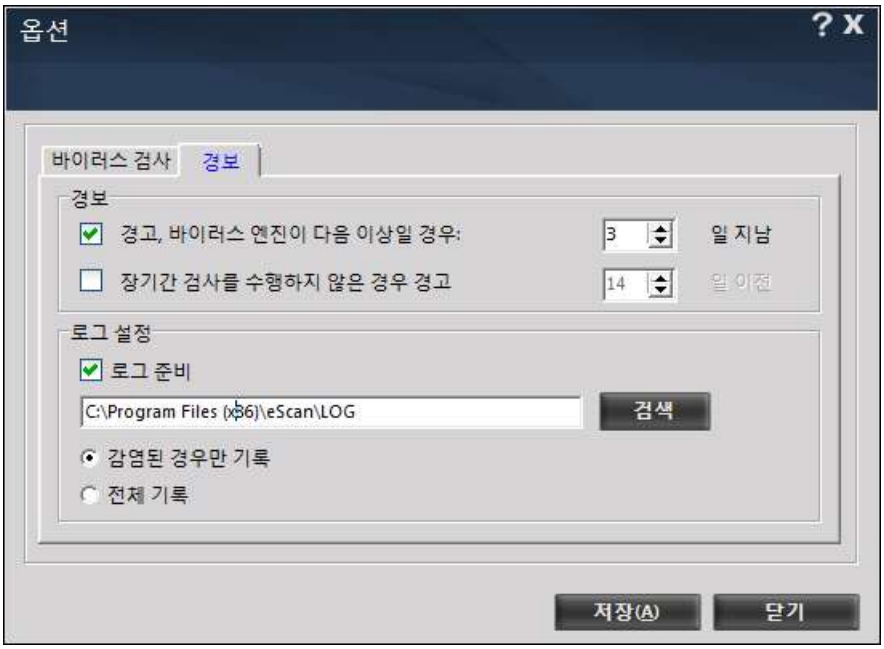
수동 혹은 예약으로 바이러스 검사를 수행 (ODS : On Demand Scanning) 할 때 지정한 폴더, 하위폴도, 파일들은 검사되지 않도록 지정합니다. 실시간 검사 예외목록과는 별개입니다.
[추가/삭제] 버튼을 클릭하여 목록을 추가합니다.

◆ **아카이브 검사**

압축되어 있거나 여러 파일을 묶어서 저장한 아카이브 파일도 검사하려면 선택합니다.

경보

바이러스 데이터베이스가 오래되었거나, 장기간 검사를 수행하지 않으면 사용자에게 안내메시지를 표시합니다.



◆ **경보**

– 경고, 바이러스 엔진이 다음 이상일 경우 (기본설정) :
바이러스 데이터베이스가 오래 되면 신종 바이러스에 대해 대비를 하지 못하게 됩니다.
지정한 기간 이상으로 데이터베이스가 업데이트 되지 않으면 경고창이 나타납니다.

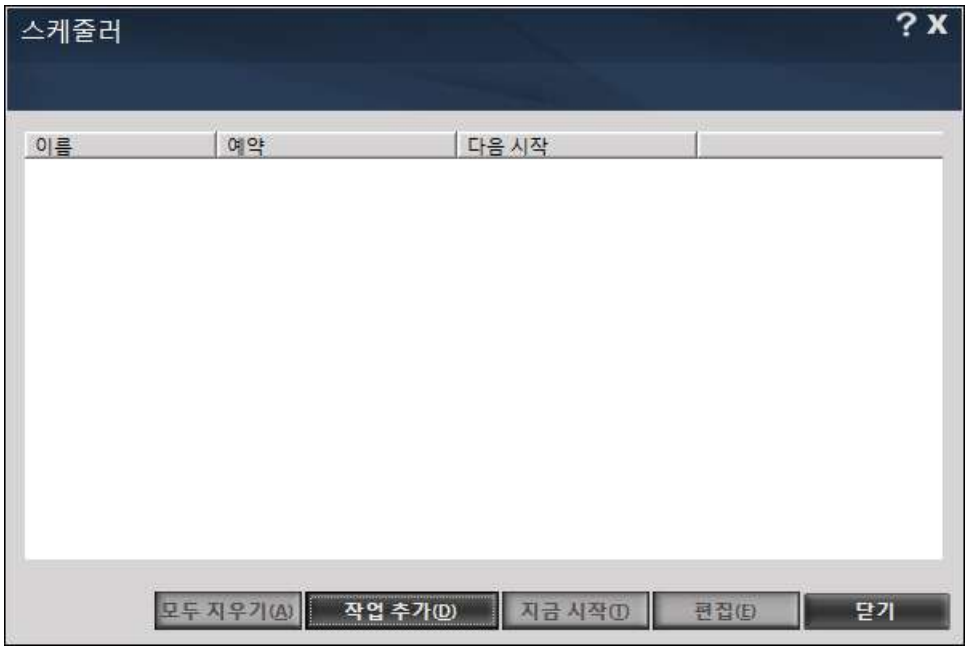
– 장기간 검사를 수행하지 않은 경우 경고
지정한 일수를 경과하여 오랫동안 컴퓨터에 대한 검사를 수행하지 않으면 경고창이 나타납니다.

◆ **로그 설정**

– 로그 준비 (기본설정) : 검사를 실행할 때 로그파일을 기록하도록 합니다. 경로는 변경할 수 있습니다.
– 감염된 경우만 기록 (기본설정) : 바이러스가 발견된 내용만 로그에 기록합니다.
– 전체 기록 : 검사를 수행한 모든 파일명과 검사결과를 로그에 기록합니다.

10.3 스케쥴러

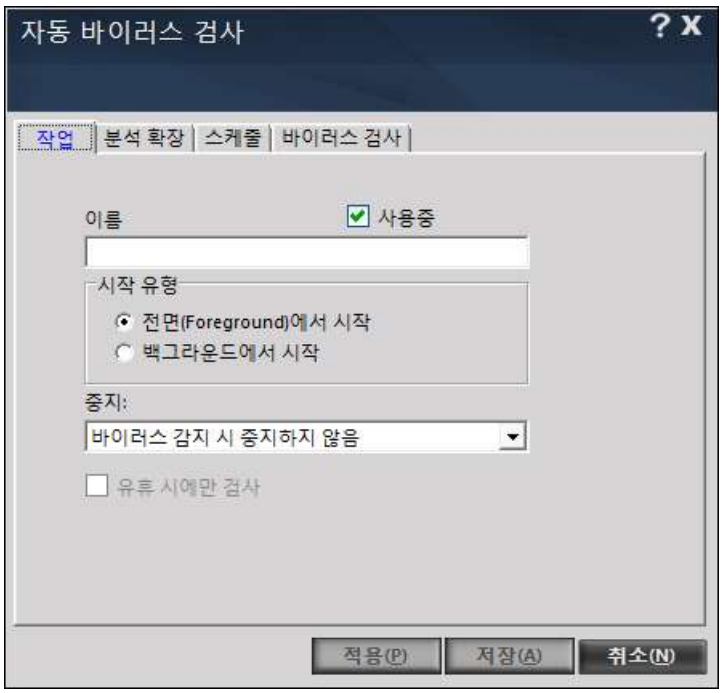
바이러스 검사를 예약하여 정기적으로 실행하도록 합니다.



[작업 추가] 버튼으로 정기적인 예약검사를 설정합니다.

작업

예약 검사 종류별로 이름을 지정하고 예약검사 조건을 지정합니다.



◆ **시작유형**

– 전면(Foreground)에서 시작 : 검사 창이 화면에 표시되어 진행됩니다.

– 백그라운드에서 시작 : 검사 창은 숨겨져 보이지 않도록 최소화된 상태에서 검사가 진행됩니다.

◆ **중지**

바이러스 검사가 완료된 후 검사창을 닫을지 여부를 지정합니다.

– 자동 멈춤 금지 : 검사 완료 후에도 검사창을 그대로 두어 사용자가 확인 후 닫도록 합니다.

– 바이러스 감지 시 중지하지 않음 (기본설정):

바이러스가 발견되면, 검사 완료 후에도 검사창을 닫지 않도록 합니다.

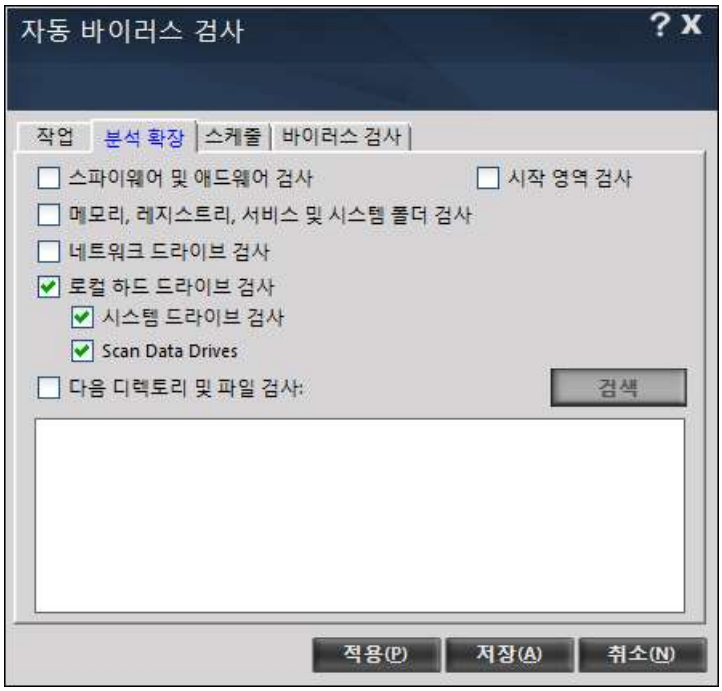
바이러스가 발견되지 않으면, 검사창을 닫습니다.

– 항상 종료 : 검사 완료 후 바이러스 발견 여부와 무관하게 검사창을 닫도록 합니다.

–

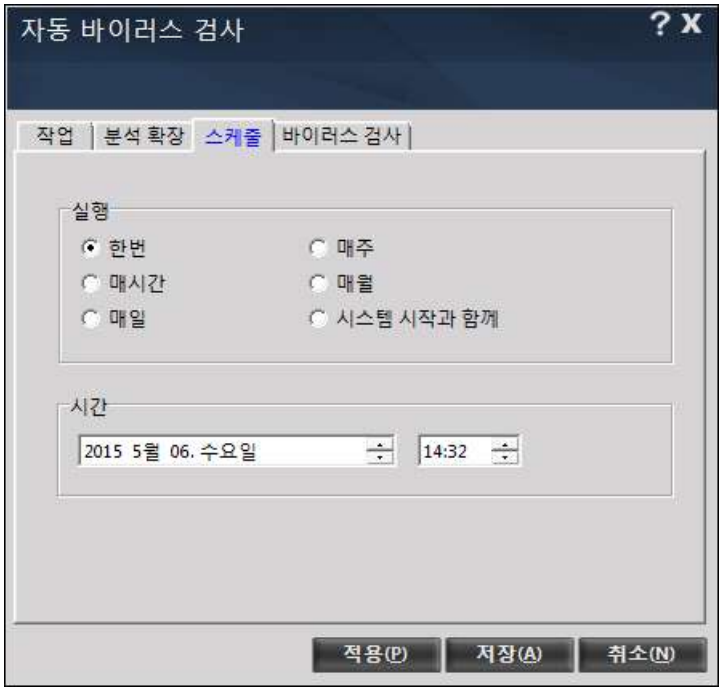
분석 확장

검사할 대상을 지정합니다.



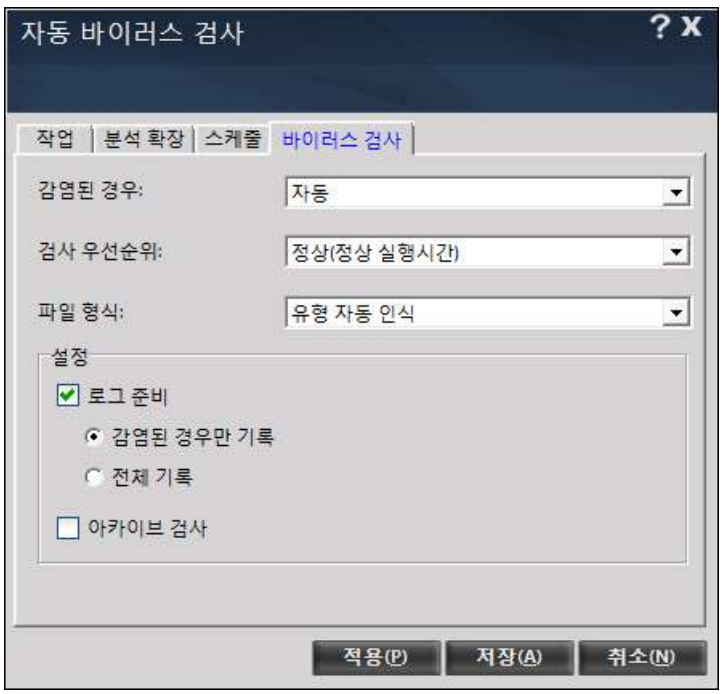
스케줄

예약 검사 주기와 시간을 설정합니다.



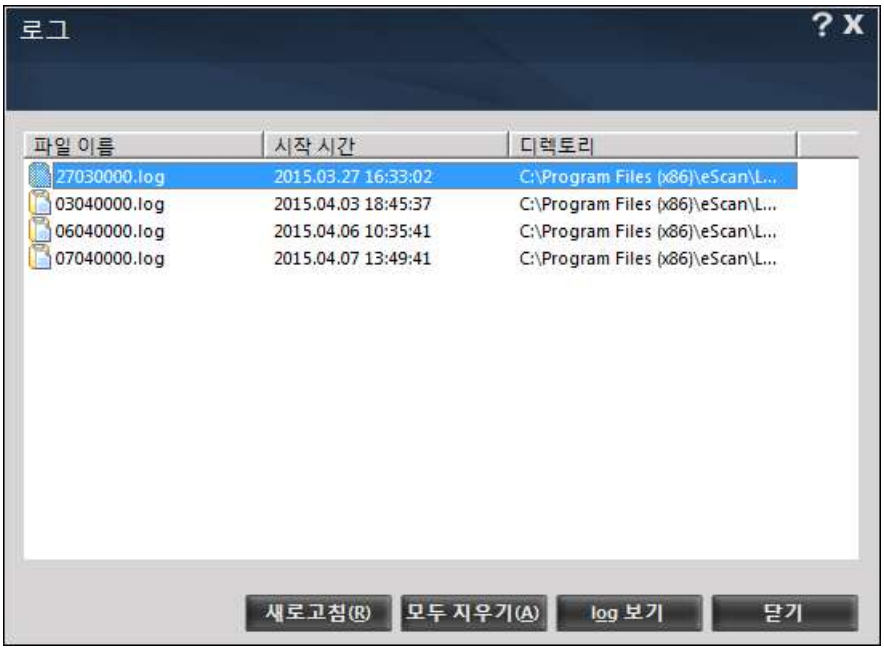
바이러스 검사

예약 검사에 적용할 검사 옵션을 지정합니다. [10.2 옵션]에서 안내한 내용을 참조합니다.



10.4 로그

바이러스 검사를 실행할 때 로그를 저장하게 한 경우에 확인할 수 있습니다.
기본설정은 바이러스가 발견되었을 때 그 내용만을 기록하게 되어있으며, 로그와 관련한 설정은 바이러스 검사 옵션에서 참조하시기 바랍니다.



11. 업데이트

컴퓨터를 유해요소로부터 보호하기 위해서는 바이러스 데이터베이스를 최신으로 유지하는 것이 중요합니다. 기본적으로 매 2시간 간격으로 업데이트 여부를 확인하여 최신 상태를 유지하도록 하고 있으나, 사용자의 환경에 따라 다운로드를 예약하거나, 별도의 업데이트 서버를 통해서 다운로드 받도록 설정할 수 있습니다.

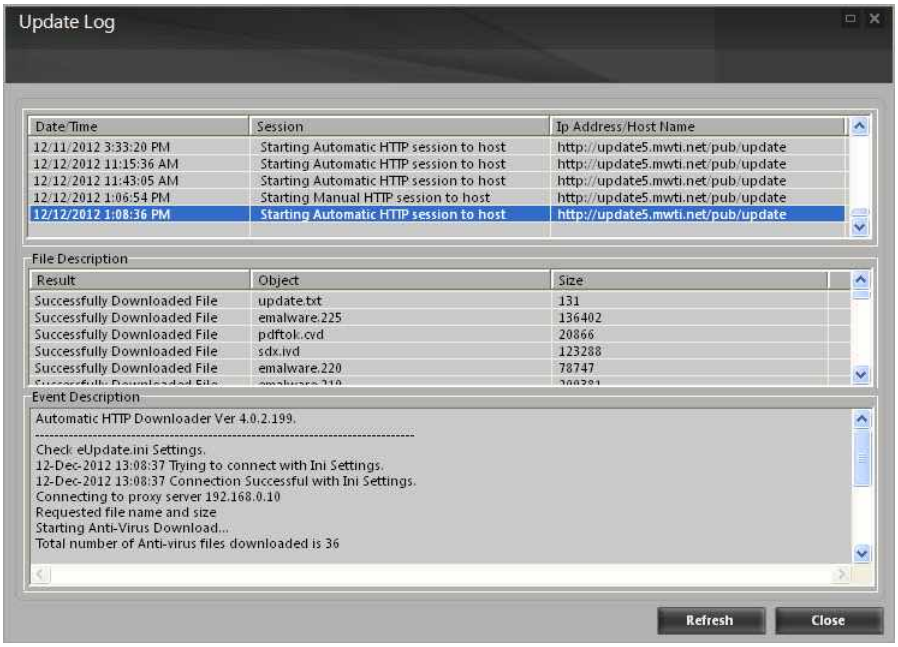
11.1 메인

구성

최근 데이터베이스 업데이트일 : 가장 최근 업데이트 한 일시
실행모드 : 현재 설정된 업데이트 예약 상태 (자동 / 예약)

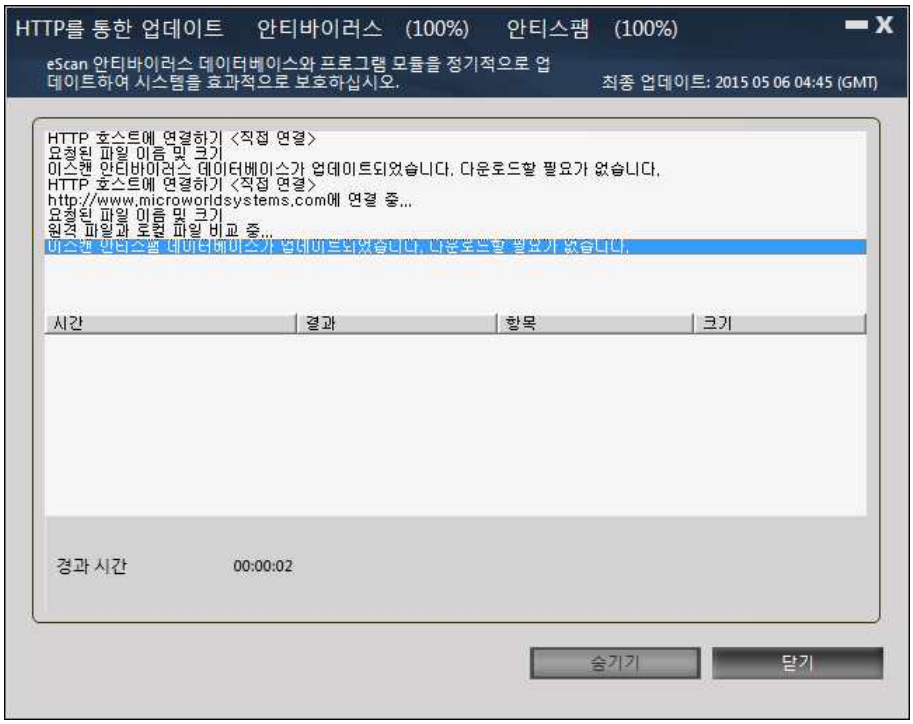
활동 보고

로그 보기 : 업데이트 이력을 조회할 수 있습니다.



지금 업데이트

최신 데이터베이스로 즉시 업데이트를 실시합니다.



11.2 설정

데이터베이스 업데이트 주기, 업데이트를 받을 서버 등을 설정합니다.

일반 구성

별도의 다운로드 서버를 지정하여 운영하는 경우에 설정합니다.

업데이트 후

바이러스 데이터베이스의 업데이트가 완료된 후 특정한 프로그램이 실행되기를 희망하는 경우에 설정합니다.

- **프로그램 이름 :** 실행시킬 프로그램을 선택합니다. 직접 경로를 입력하거나, 검색하여 선택합니다.
- **시작 :** 프로그램이 실행될 작업 폴더를 지정합니다. 직접 경로를 입력하거나, 검색하여 선택합니다.
- **매개변수 :** 프로그램 실행에 필요한 매개변수가 있다면 기록합니다.
- **실행**

프로그램이 실행될 창의 크기를 지정합니다.

– 정상 (기본설정) : 통상의 프로그램과 같이 프로그램에 따라 크기가 결정되도록 합니다.

– 최소화 / 최대화 / 숨김 : 필요에 따라 창의 크기를 이 중에서 선택합니다.

- **프로세스 강제 종료 :** 지정한 프로그램이 실행시키기 위해 다른 프로그램들은 모두 강제 종료 시킵니다.
- **프로세스 종료 기다리지 않기 :** 지정한 프로그램의 실행시간이 긴 경우, 실행 중인 다른 프로그램 혹은 프로세스도 같이 실행될 것을 허용합니다.
- **이 프로세스가 실행되는 동안 모든 작업을 일시 중단 :** 기본적으로 다른 프로세스도 정상적으로 작동하도록 하되, 현재 지정한 프로그램이 작동하는 일정 시간동안은 다른 프로그램에 의해 실행이 제한되거나 느려지는 일이 없도록 일정 시간 실행을 중지시키고자할 때 중지시킬 시간을 지정합니다.
- **업데이트 알림**

업데이트가 완료되면, 업데이트 완료 사실을 메일로 통보받고자 할 때 선택합니다.

– 발신자 : 발신자로 인식할 메일 주소를 기록합니다. 기본값은 escanuser@escanav.com 으로 설정됩니다.

– 수신자 : 안내메일을 받을 메일 주소를 기록합니다.

– SMTP 서버 / 포트 : 메일서버의 아이피 주소와 이메일 발송에 사용하는 포트 번호

스케쥴링

업데이트를 수행할 주기를 예약합니다.
기본값으로는 매 120분 마다 이스캔 서버로부터 최신 데이터베이스를 다운로드 받도록 설정되어 있습니다.

◆ **참고**

인터넷에 연결되어 있지 않은 컴퓨터라면, 아래 주소에서 업데이트 파일을 받은 후 해당 컴퓨터에서 실행하면 인터넷 연결 없이 수동으로 업데이트가 진행됩니다.

http://download1.mwti.net/download/updates/esupdatebd.exe