[솔루션 기능 테스트]
리눅스 PC보안용 LAV 테스트
(부요 데스크탑) 기능 테스트 결과서

한국소프트웨어진흥원
공개SW기술지원센터

<Revision 정보>

일자	VERSION	변경내역	작성자
2007. 6.20	0.1	초기 작성	양선주
2007. 7. 4	0.2	테스트 완료 내용 추가	양선주

목 차

표 차례>

1. 문서 개요

본 문서는 리눅스 PC보안용 솔루션인 LAV를 Booyo Desktop 2.0 OS(kernel 2.6.15-1)에서 호환성 및 기능성 검증을 중심으로 테스트 하였으며, 관련 솔루션 업체의 참고자료 활용을 위해 제작되었다.

가. 문서의 목적

다음과 같은 세부적인 목적을 달성하기 위하여 작성되었다.

- 리눅스 PC보안 솔루션 LAV와 Booyo Desktop 2.0 OS(kernel 2.6.15-1) 기능성 결과
- 진행 중 문제 발생 사항과 각각의 진행사항

나. 본 문서의 사용방법

다음과 같은 방법으로 사용할 수 있다.

- Booyo Desktop 2.0 OS(kernel 2.6.15-1)에서 LAV의 설치, 구동 및 기능 실행 결과를 확인한다.

2. 테스트 완료 사항

이하의 내용은 기능성 테스트 결과와 문제 발생 사항, 진행사항을 기술한다.

가. 테스트 항목

항목		방법
LAV 설치	lkd 설치	LAV 설치 스크립트로 설치 후 결과 확인
	LAV 설치	
LAV 기동		프로그램 시작 버튼을 선택하여 기동
LAV 기능 테스트	실시간 검사	실시간 시스템 검사 기능을 이용하여 검사
	수동 검사	시스템 검사 기능을 이용하여 수동으로 검사
	예약 검사	시스템 검사를 위해 특정 일자를 설정하여 해당 시간에 시스템 검사를 수행
	비검사 영역	바이러스 파일을 포함하고 있는 특정 영역을 설정하여 검사 대상에서 제외하고 시스템 검사를 수행
	검역소	수동 검사 결과로 치료된 바이러스 파일들이 검역소에 보관되어 있는지 확인하고, 파일을 선택하여 복원
	로그보기	이벤트 로그 및 바이러스 로그의 정상적인 출력 여부 확인
	업데이트	백신 엔진의 업데이트 수행 후 로그 확인

<표 1> 기능 테스트 항목

나. 테스트 결과

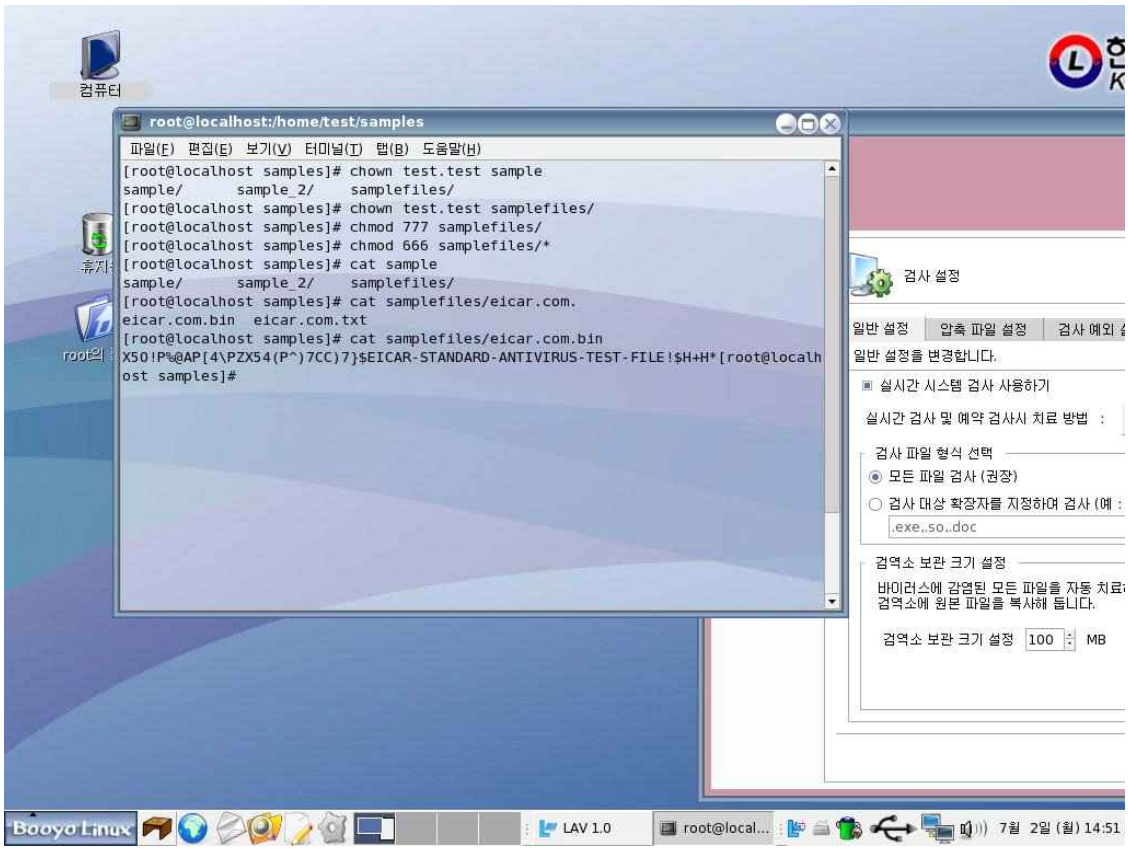
항목			일자 / 결과									
			6/20	6/21	6/22	6/25	6/26	6/27	6/28	6/29	7/2	7/3
LAV 설치		lkd 설치	PASS	생략	생략	생략	생략	생략	생략	생략	생략	생략
		LAV 설치	PASS	생략	생략	생략	생략	생략	생략	생략	생략	생략
LAV 기동테스트			PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
LAV 기능테스트	실시간검사	자동치료오프	일반사용자 & 퍼미션(777/666)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			일반사용자 & 퍼미션(777/444)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			root & 퍼미션(777/444)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			root & 퍼미션(555/444)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			일반사용자 & 퍼미션(777/777)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			일반사용자 & 퍼미션(777/555)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			root & 퍼미션(777/555)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			root & 퍼미션(555/555)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			CD 미디어	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
		파일삭제	일반사용자 & 퍼미션(777/666)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			일반사용자 & 퍼미션(777/444)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			CD 미디어	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			일반사용자 & 퍼미션(777/777)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
		그대로두기	일반사용자 & 퍼미션(777/777)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			일반사용자 & 퍼미션(777/555)	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
			CD 미디어	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F

항목			일자 / 결과									
			6/20	6/21	6/22	6/25	6/26	6/27	6/28	6/29	7/2	7/3
LAV 기능 테스트	수동 검사	압축파일 오프	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
		zip 파일	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
		lzh 파일	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
		이중 zip 파일	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
	예약 검사	매일	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
		특정 요일	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
		비특정 요일	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
	비 검사 영역	실시간 검사	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
		사용자 지정검사	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
		사용자 목록지정검사	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
		예약 검사	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
		비검사 오프	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F
	검역소	복원	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
		삭제	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
		검역소 용량초과	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
	로그 보기	이벤트 로그	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
		바이러스 로그	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
	업데이트		FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL

<표 2> (smp kernel ver.) 일자별 호환성 및 기능 테스트 결과

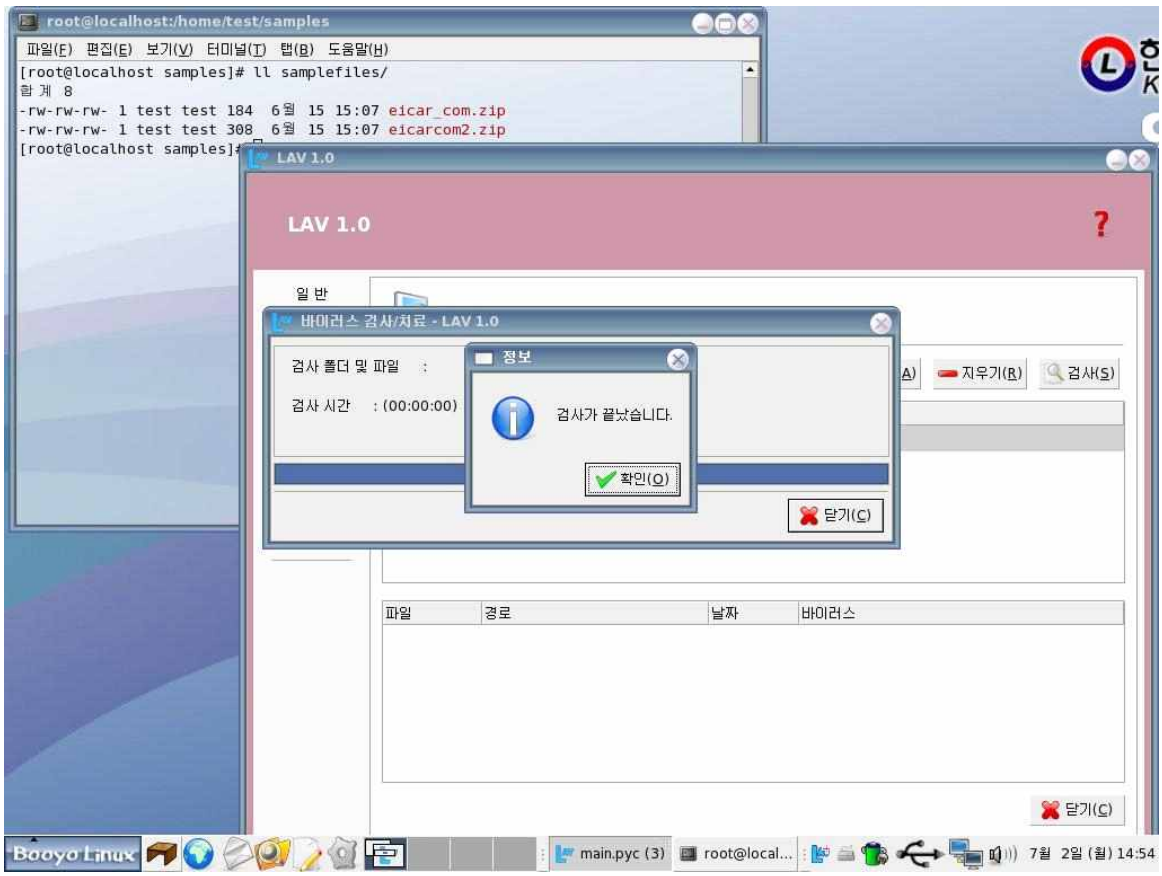
다. 문제 발생 및 진행 사항

항목	문제점	진행사항	최종 수정일
실시간 검사	일반 커널에서 실시간 감시 기능이 동작되지 않음(application/octet MIME 형태인 바이러스 파일을 text/plain 파일로 인식하며 실시간 감시가 되지 않는 문제 발생)		



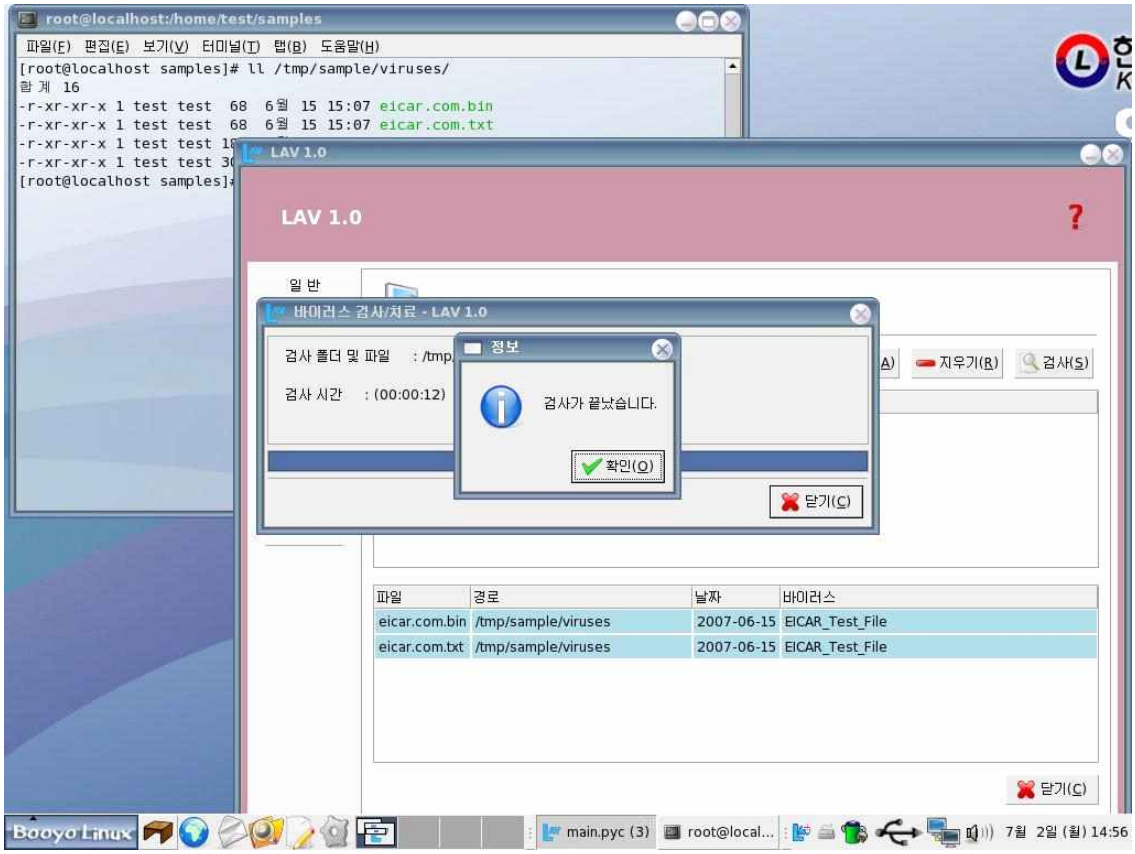
<표 3-1> 문제 발생 및 진행 사항

항목	문제점	진행사항	최종 수정일
실시간검사 / 수동검사 / 예약검사 / 비검사 영역 등 모든 검사항목 공통 사항	커널과 상관없이, 바이러스를 포함하여 압축된 파일은 압축 해제하여 바이러스 파일에 직접 접근하기 이전에는 바이러스로 검출되지 않음		



<표 3-2> 문제 발생 및 진행 사항

항목	문제점	진행사항	최종 수정일
비검사 영역	검사 예외 영역으로 설정한 디렉토리에서도 바이러스 검출함		



<표 3-3> 문제 발생 및 진행 사항

항목	문제점	진행사항	최종 수정일
업데이트	GUI에서는 정상적으로 업데이트 된 것처럼 나오지만, update.log 파일에서는 Failed 로 기록됨		

```
[root@localhost log] tail -f /usr/share/lavscan/log/update.log
**********************
** UPDATE LOG BEGINE **
**********************
2007-07-02 17:02:46      Update/Start
2007-07-02 17:02:46      Product Name : KIPAV
2007-07-02 17:02:46      Product Update Code : 0
2007-07-02 17:02:46      Product Serial Number :  35640010-50510004
2007-07-02 17:02:46      Product Version :
2007-07-02 17:02:46      Product Information : /etc/smartupdate.conf
2007-07-02 17:02:46      *** Product Number is vaild

2007-07-02 17:02:46      Update/Autocopy/Start
2007-07-02 17:02:46      Backup/Background Information : /usr/share/lavscan/log/updat
e.log/ahn.unix, Backup Directory : /usr/share/lavscan/update/backup
2007-07-02 17:02:46      Backup/ahn.unix(Error)
2007-07-02 17:02:46      Backup/Autocopy(Failed)
2007-07-02 17:02:46      Copy/Background Information : /usr/share/lavscan/log/update.l
og/ahn.unix
2007-07-02 17:02:46      Copy/ahn.unix(Error)
2007-07-02 17:02:46      Restore/Background Information : /usr/share/lavscan/update/b
ackup/ahn.unix
2007-07-02 17:02:46      Restore//usr/share/lavscan/update/backup/ahn.unix(Error)
2007-07-02 17:02:46      Restore/Autocopy(Failed)
2007-07-02 17:02:46      Update/Exit(Failed)
end
[test@localhost log]$
```

<표 3-4> 문제 발생 및 진행 사항

3. 테스트 환경

가. 데스크탑 구성

항목	내역	수량	비고
CPU	Intel Pentium(R) 4 2.8GHz	1개	
Memory	512MB	1개	
HDD	WD 80GB	1개	
OS	Booyo Desktop 2.0	N/A	

<데스크탑 구성 내역>

나. 테스트 방법

항목	테스트 프로그램	방법론	비고
Application (백신 솔루션)	LAV	Booyo Linux 데스크탑에 LAV 설치 후 바이러스 검역, 로그 확인, 백신 엔진 업데이트 등의 기능 확인	

<테스트 방법>

다. 기타 환경

4. OS, Driver 정보

구분	(Driver) 이름	Version	구분	Driver 이름	Version
OS	Booyo Desktop 2.0	kernel : 2.6.15-1.2054_bone21			

<각 version>

5. 테스트 절차 내역

- 테스트 요청서와 절차서는 이하의 첨부 파일을 참조

테스트 요청서	테스트 절차서
	중앙기술지원-BO-20070703-리눅스

6. 테스트 완료 의견

이하의 내용은 테스트 완료 후 테스트 수행자의 의견을 기술한다.

항목	결과
실시간 검사	일반 커널에서 바이러스 검출되지 않음
실시간/ 수동/ 예약 검사	압축파일을 해제한 후 바이러스 파일에 접근하지 않으면, 바이러스로 검출되지 않음
비검사 영역	① /tmp 를 비검사 영역으로 설정하고 검사 시, /tmp/sample 하위의 바이러스 검출됨 ② /tmp/sample 을 비검사 영역으로 설정하고 /tmp 검사 시, /tmp/sample 하위의 바이러스 검출됨 ③ 비검사 오프 후 /tmp 검사 시 /tmp/sample 하위의 바이러스 파일을 포함한 압축파일은 바이러스로 검출 안됨 ④ /tmp/sample 을 비검사 영역으로 설정하고 /tmp/sample 및 여러 디렉토리를 함께 검사 시, /tmp/sample 하위의 바이러스 검출됨 ⑤ /tmp 를 비검사 영역으로 설정 후 예약검사 시, 스케줄링은 정상동작하나 /tmp/sample 하위의 바이러스 검출함
수동 검사	/proc 하위의 정상적 파일에 대해 바이러스로 인식함

<표 4> 테스트 완료 의견