

AHP 기법을 이용한 안티바이러스 소프트웨어 평가 요인 분석

김종기* · 황숙연** · 이동호***

<목 차>

I. 서 론	IV. 실증분석
II. 이론적 배경	4.1 계층구조별 평가기준의 중요도 산출
2.1 컴퓨터 바이러스에 대한 연구	4.2 1차 요인에 대한 분석결과
2.2 안티바이러스 소프트웨어에 대한 연구	4.3 2차 요인에 대한 분석결과
2.3 안티바이러스 소프트웨어 평가요인 에 관한 연구	4.4 3차 요인에 대한 분석결과
2.4 소프트웨어 품질 평가에 대한 연구	4.5 평가요인에 대한 집단별 우선순위 비교
III. 연구모델	V. 결론
3.1 안티바이러스 소프트웨어 평가를 위 한 AHP기법	참고문헌
3.2 연구모형	Abstract

I. 서 론

네트워크의 발전과 개방화는 인터넷을 이용한 정보기술의 확산을 촉진시키는 계기를 마련해주었지만, 역으로 인터넷을 통한 의도적이거나 비의도적인 해킹, 정보 유출, 변조, 파괴 등 조직의 목표와 이익을 침해하거나 업무를 마비시키는 보안 사고들이 증가하게 되었다. 정보기술의 발전이 역으로 보안과 개인 정보보호에 더 큰 위협 요소가 되어버린 것이다. 그 중에서도, 바이러스(virus)는 시스템의 데이터를 파괴하는 바이러스부터 매크로 바이러스(macro virus) 그리고 웜(worm)의 형태에 이르기까지 광범위한 피해를 주고 있다(정관진과 이희조, 2003).

현재의 컴퓨터 바이러스는 초기의 단순한 형태를 벗어나 상당히 다양한 특성을 가지고 있으며 그 피해의 정도도 기업과 개인에게 금전적, 시간적 차원의 심각한 영향을 미친다(Mamaghani,

* 부산대학교 경영학부 교수, jkkim1@pusan.ac.kr

** 부산대학교 대학원 경영학과, syhwang@pusan.ac.kr

*** 동명정보대학교 유통경영학과 전임강사, dhlee@tit.ac.kr

2002; Dunham, 2003). 이러한 이유로, 정보자산에 심각한 악영향을 미치는 바이러스나 악성코드의 피해를 줄이기 위한 보안대책이 필요하다. 바이러스의 피해를 막기 위한 하나의 방법으로 안티바이러스 소프트웨어(anti-virus software)를 구입하여 사용하고 있다.

안티바이러스 소프트웨어를 선택하는 것은 여러 가지 요인들이 고려되어야 하는 어려운 의사 결정의 문제이다(Dunham, 2003). 즉, 안티바이러스 소프트웨어를 선택하는 과정은 안티바이러스 소프트웨어의 기능과 성능, 가격 등의 차원에서 상당히 다양한 특성을 지니고 있다는 점과 사용하는 기업이나 조직 혹은 개인이 요구하는 사항이 차별적인 성격을 가지기에 상당히 복잡한 문제로 간주된다(Mamaghani, 2002).

한편, 소프트웨어의 품질을 향상시키기 위한 품질평가에 관한 연구는 다수의 소프트웨어 평가 모형이 개발되었으며, ISO에서도 품질인증 시스템을 개발하였다. 하지만, 이런 표준안이 있음에도 불구하고 일반적으로 소프트웨어 제품의 측정과 평가는 여러 가지 고려사항이 있기 때문에 소프트웨어 제품의 평가와 선정 문제는 구조상 다속성 의사결정(multiple attribute decision making)의 성격을 가지게 된다(박호인과 정호원, 1997). 기업이나 개인 측면에서 안티바이러스 소프트웨어의 선택과 사용도 대표적인 다속성 의사결정으로 볼 수 있다. 본 연구의 목적은 안티바이러스 소프트웨어의 평가요인에 대한 문제를 중심으로 효과적인 평가요인 분석을 통해 평가요인의 구체적인 우선순위를 모색하는 것이며, 이를 위해 연구에서는 안티바이러스 소프트웨어의 평가에 영향을 미치는 요인들을 범주화하여 계층적 분석과정(analytic hierarchy process: AHP) 기법을 통한 각 요인간의 상대적 중요도를 분석하고자 한다.

II. 이론적 배경

2.1 컴퓨터 바이러스에 대한 연구

2.1.1. 컴퓨터 바이러스의 정의와 유형

컴퓨터 바이러스를 한마디로 정의한다는 것은 상당히 어려운 일이며, 실제 이론적으로나 실무적으로도 상당히 다양한 정의가 존재한다(Highland, 1997; Brunnstein, 1999). 바이러스의 개념을 최초로 언급하고 있는 Cohen(1984)은 바이러스에 대해 자신을 복제하며 변조를 통해서 다른 프로그램을 감염시키는 프로그램이라고 정의하였다. Cohen의 정의는 오늘날 많은 문제를 야기하고 있는 웜과 같은 네트워크를 통한 자기복제를 포함하는 악의적인 소프트웨어에 적용할 수가 없다. 따라서 오늘날에는 컴퓨터 바이러스를 보다 넓은 의미로 해석하여 적용하고 있다.

즉, 초기의 바이러스라는 개념은 다른 악성코드(malware)와 명확한 구분이 되는 경우가 상당히 많았으나, 최근의 안티바이러스 소프트웨어의 개발자 혹은 사용자의 인지 측면에서 볼 때, 바이러스 이외의 다른 악의적인 코드를 포함하는 개념으로 바이러스라는 용어를 사용하고 있다(Brunnstein, 1999). 따라서 본 연구에서 컴퓨터 바이러스는 웜이나 트로이 목마, 논리폭탄, 혹스

(hox), 조크, 에드웨어(ad-ware) 같은 것들을 모두 포함하여 사용자가 인지하지 못하거나 원하지 않는 시스템 작동을 유발하는 모든 형태의 악성코드로 정의한다.

이런 여러 가지 악성코드들 중 대표적인 컴퓨터 바이러스, 트로이 목마, 웜에 대한 비교하면 다음의 <표 1>과 같다. 아래 표에서 나타난 것처럼, 트로이목마는 바이러스나 웜과는 달리 자기 복제 능력이 없으며, 사용자가 트로이목마 프로그램이 아무른 해가 없는 응용프로그램으로 오인하도록 하여 이를 실행시키도록 유도한다.

<표 1> 악성코드의 비교

	자기복제	직접감염	형태	복구방법
컴퓨터 바이러스	○	○	기생/겹침	치료
트로이목마	×	×	독립	삭제
웜	○	×	독립	삭제

좁은 의미의 컴퓨터 바이러스는 트로이목마나 웜과는 달리 시스템 파일이나 응용프로그램을 변조시켜서 그 안에 기생하거나 끝에 부가된 형태로 존재함으로 공격대상 파일이나 프로그램에 직접적인 영향을 미친다. 따라서 컴퓨터 바이러스를 제거하기 위해서 감염된 파일 자체를 삭제한다면 시스템 자체가 운영이 불가능하게 될 우려가 있어 해당 파일에서 바이러스 부분만 선택적으로 삭제해야 하지만, 트로이목마나 웜은 독립적으로 존재함으로 그 자체를 삭제함으로써 복구가 가능하다.

2.1.2. 컴퓨터 바이러스의 영향

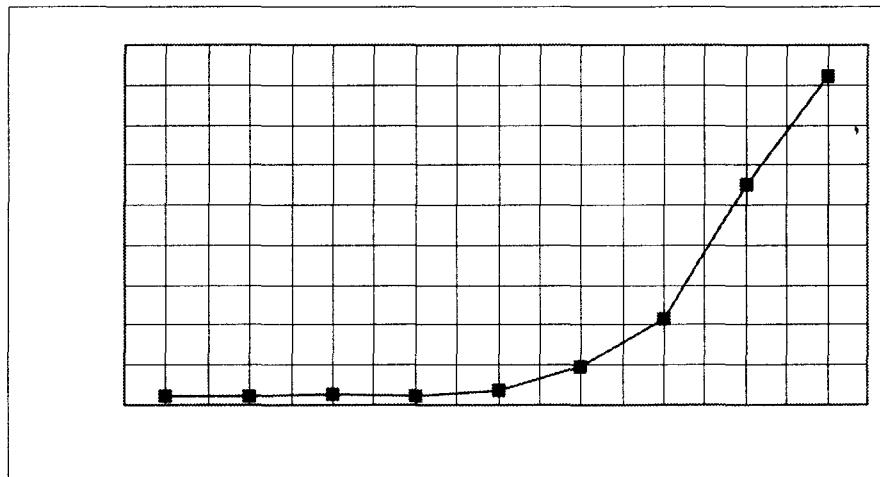
컴퓨터 바이러스의 감염 경로 중 가장 빈번한 경우는 소프트웨어의 불법 복사에 의한 감염이다. 또한 네트워크를 통해서 다운로드 받은 소프트웨어에 의하여 바이러스가 감염되기도 한다. 최근에는 인터넷을 이용하는 인구가 빠른 속도로 증가하고 있기 때문에 네트워크를 관리하는 관리자뿐만 아니라 컴퓨터를 사용하는 모든 사용자들도 컴퓨터 바이러스에 대한 주의를 기울여야 한다. 다음의 <표 2>는 ICSA 연구소에서 바이러스가 감염되는 원천에 대한 설문조사를 복수응답을 허용하여 조사한 결과를 보여주고 있는데, 표에서 보면 근래 대부분의 바이러스 감염원천이 e-mail을 비롯한 인터넷을 통하는 것으로 추세가 변화되고 있다.

최근의 컴퓨터 바이러스는 웜과 백도어가 결합된 형태나 네트워크 전파와 같이 복합적인 형태를 가진 바이러스가 많이 나타나고 있으며, 일반적으로 웜이나 트로이목마 제작에 고급언어를 사용하여 바이러스 보다 제작이 쉬운 것도 확산이유 중의 하나이다. 즉, 현재의 컴퓨터 바이러스는 컴퓨터를 사용하는 사람의 숫자와 네트워크의 규모가 증가할수록 바이러스의 확산 속도도 같이 증가하고 있는 추세이다(Hubbard & Forcht, 1998). 따라서 현재의 바이러스는 네트워크를 통하여 스스로 전파되고 피해를 입히는 웜 형태로 변화해 나가고 있다. <그림 1>에서 보는 것과 같이 컴퓨터 바이러스의 침해사건 수는 계속해서 증가하고 있다.

<표 2> 바이러스의 감염원천

바이러스 감염원천	1996	1997	1998	1999	2000	2001	2002
E-mail	9%	26%	32%	56%	87%	83%	86%
인터넷 다운로드	10%	16%	9%	11%	1%	13%	11%
웹 브라우징	0%	5%	2%	3%	0%	7%	4%
알 수 없음	15%	7%	5%	9%	2%	1%	1%
다른 경로	0%	5%	1%	1%	1%	2%	3%
소프트웨어 배포	0%	3%	3%	0%	1%	2%	0%
디스켓 및 기타	71%	84%	64%	27%	7%	1%	0%

자료원 : ICSA Labs(2003), p.24 인용



<그림 1> 컴퓨터 바이러스 침해 사건 수

자료원 : CERT(2003)

2.2 안티바이러스 소프트웨어에 대한 연구

안티바이러스 소프트웨어는 컴퓨터 시스템에서 바이러스, 트로이목마, 웜 등의 악성코드를 진단하고 복구해 주는 프로그램으로, 현재까지 악성 코드 예방과 퇴치에 가장 효과적인 것으로 평가되고 있다(차민석, 2002; Hubbard & Forcht, 1998; Mamaghni, 2002; Larry, 2002). 이런 종류의 프로그램에 관한 시장은 점차 확대되고 있으며, 안티바이러스 소프트웨어는 일반적으로 다음과 같이 크게 세 가지로 구분된다.

- ① 바이러스 감염을 사전에 방지하기 위한 예방 프로그램

- ② 바이러스에 감염이 되었는지를 검사하는 진단 프로그램
- ③ 바이러스에 감염된 파일을 원래의 상태로 복구하는 치료 프로그램

일반적으로 사용자는 안티바이러스 소프트웨어를 설치하는 것으로 바이러스의 침해 사고를 예방할 수 있다고 생각한다. 하지만, 안티바이러스 소프트웨어는 새로운 바이러스에 대한 정보를 가지고 있지 않기 때문에 기능을 수행하는데 여러 가지 한계점을 가지고 있다.

첫째, 안티바이러스 소프트웨어의 가장 큰 한계는 해당 프로그램이 식별할 수 있는 바이러스만 진단, 퇴치가 가능하다는 점이다. 사용자가 소프트웨어를 설치한 후에도 신종 바이러스는 계속 제작되고 유포되기 때문에 안티바이러스 소프트웨어의 엔진을 계속 업데이트 해주어야 한다. 안티바이러스 소프트웨어 제작사들은 신종 바이러스의 진단/치료 기능이 추가될 때마다 이에 대한 정보를 개신해서 고객들에게 제공한다.

둘째, 시스템 감시기능은 바이러스의 접근을 차단하는 것이지, 네트워크를 통한 바이러스의 공격을 예방하는 것은 아니다. 시스템 감시기능은 사용자가 접근하는 파일의 감염 여부를 검사해 사전에 사용자가 감염된 파일에 접근하는 것을 차단해준다. 이런 특징으로 인해 바이러스에 감염된 파일을 다른 컴퓨터의 공유 폴더를 이용하여 파일을 복사할 때, 파일을 받는 컴퓨터 쪽 백신의 시스템 감시 기능은 파일이 전송되는 중간에 파일을 검사하지 않고 파일이 모두 복사되고 파일이 닫히는 시점에서 파일을 검사/진단하여 바이러스 유무를 사용자에게 알려준다. 이렇게 악성코드 감염여부를 검사하는 시점이 파일에 대한 모든 작업이 완료된 후이다 보니, 사용자는 현재 사용하는 프로그램의 문제로 악성코드의 감염을 차단하지 못했다고 오해할 수 있는 것이다. 그 외에도 안티바이러스 소프트웨어 제품마다 바이러스 분류가 다르기 때문에 나타날 수 있는 점이나, 안티바이러스 소프트웨어도 하나의 프로그램이기 때문에 바이러스에 감염될 수 있다는 한계를 가지고 있다.

2.3 안티바이러스 소프트웨어 평가요인에 관한 연구

Dunham(2003)은 안티바이러스 소프트웨어 선정에 있어서 다음의 다섯 가지 주요한 고려사항들을 설명하고 있다.

- ① 안티바이러스 프로그램의 인지도
- ② 주요 소프트웨어에 대한 인식과 개인적인 테스트
- ③ 안티바이러스 소프트웨어의 기능과 이해에 대한 평가
- ④ 안티바이러스 소프트웨어의 기능성에 대한 검정
- ⑤ 개인적인 필요를 위한 최선의 안티바이러스 소프트웨어의 선정

또한 비용, 시스템 요구사항, 인터페이스, 성능, 스캔(scan) 옵션, 제거와 복구 옵션, 지원 등이 안티바이러스 소프트웨어의 주요한 평가 기준으로 제시되고 있다. Sherif & Gilliam(2003)의 연구에서는 안티바이러스 소프트웨어 폐기지에 대한 평가 항목으로, 멀티 플랫폼 지원, 업데이트, 지속적인 개발, 헬프데스크 지원, 스캐닝, 치료, 시스템 감염에 대한 응답, 스캔율, 메모리 요구

수준 등의 평가 기준을 제시하고 있으며, 주된 평가기준으로 기능, 신뢰, 유지, 비용의 네 가지의 기준을 제시하고 있다.

Mamaghani(2002)는 안티바이러스와 필터링 소프트웨어의 평가와 선택에 관한 연구를 통해 선택의 주요한 기준으로 설치, 운영, 관리, 통보/로그, 안티바이러스, 내용 필터링의 6가지의 기준을 제시하고 있다. 이러한 기준들 중 연구 결과를 통해 안티바이러스와 내용필터링이 안티바이러스 선택에 가장 주요한 기준이었다. 황진욱(2002)은 안티바이러스 소프트웨어를 소비자 관점에서 선호도 분석을 하였다. 인터넷을 사용하는 기업 및 사용자를 대상으로 설문조사가 실시되었고, 제품인지도가 도출되었으며, 인지도를 구성하기 위해 요인 분석과 선호도 회귀 분석 (preference regression analysis)이 사용되었다.

황진욱(2002)의 연구에서 사용되고 있는 선호도 회귀 분석은 사용자의 선호도 항목을 요인점수와 상관계수의 관계식으로 표현하고 있는 모델로 설명되고 있는데, 사용자의 선호도를 중요한 항목의 요인점수와 상관계수로 회귀방정식을 도출하고 그 회귀식을 통해서 특정의 개별 소프트웨어에 대한 선호도를 분석하고 있다. 요인 분석 결과, 핵심품질, 효율성, 주변요소의 3가지 공통 요인이 도출되었다. 그 중에 핵심품질은 세가지요인 중에서 가장 중요한 것으로 나타났다. 안티바이러스 소프트웨어평가와 관련된 선행연구를 표로 정리해 보면 <표 3>과 같이 나타난다.

<표 3> 안티바이러스 소프트웨어 평가요인관련 선행 연구

연구자/연구기관	평가기준
Dunham(2003)	비용, 시스템 요구사항, 인터페이스, 성능, 스캔 옵션, 제거와 복구옵션, 지원
Sheirf & Gilliam(2003)	기능, 신뢰, 유지, 비용
Larry(2002)	설치, 인터페이스, 지원, 바이러스 스캐닝, 스캐줄 스캐닝, 업데이트
Managhani(2002)	설치, 운영, 관리, 통보/로그, 안티바이러스, 내용 필터링
황진욱(2002)	온라인지원, 신종바이러스에 대한 신속한 대응, 편리한 메뉴구성, 디자인, 프로그램 업데이트, CPU 및 메모리 점유율, 스캔 시간, 프로그램 습득, 스캔 엔진의 업데이트, 가격대비 성능

2.4 소프트웨어 품질 평가에 대한 연구

2.4.1 Boehm의 연구

Boehm(1978)은 최초로 소프트웨어 제품의 품질을 정량적으로 측정 및 평가 할 수 있는 품질 모형을 제시하였다. 이 모형에 의하면 품질을 외부 관점에서 본 중간구조와 내부관점의 기초구조의 2차원으로 구성되어 있다(Gilles, 1992).

이 모형에서 품질특성은 초기운용, 유지보수, 이식성의 세 가지로 분류하고 중간구조에서는 이식성, 신뢰성, 효율성, 인간공학, 시험성, 이해성, 변경성으로 품질특성과 연관지어 분류하였다. 내부특성으로는 장치 독립성, 자기 포함성, 완전성, 확고 및 무결성, 일관성, 설명성, 장치 효율성, 통신성, 자기 기술성, 구조성, 간결성, 명료성, 확대성 등 14가지로 분류하고 중간구조와의 연관성을 나타내었다.

2.4.2 McCall의 연구

McCall(1978)은 미 공군의 요청으로 연구를 시작하여 미 국방성의 품질표준으로 채택되어 현재 많은 품질측정 기초로 이용되고 있다. McCall의 모형은 소프트웨어 품질 요구사항을 명확히 설정하고 개발된 제품의 품질을 평가관리하기 위한 방안으로, 사용자 관점에서 요구된 품질 수준을 구체화하고 소프트웨어 개발과정 중 요구된 품질의 평가 가능성을 판단하는 지침으로 활용되기도 한다.

그의 연구에서는 11 가지의 품질요인을 소프트웨어 제품의 개정, 전이 및 운용의 관점에서 구분하여 제안하였다. 제품제정에는 유지보수성, 유연성, 시험성이 있고, 제품전이에는 상호 운용성, 재사용성, 이식성이 있으며, 제품운영을 위해서는 정확성, 효율성, 무결성, 신뢰성, 사용성의 품질특성이 있다.

2.4.3 Evans의 연구

Evans(1987)는 12개의 품질특성을 선택한 후, 소프트웨어 개발 수명주기를 중심으로 성능, 설계, 개선의 3개 범주로 구분하였다. 성능은 사용자에 의해 언급된 요건들이 소프트웨어의 운영방법을 구체적으로 설명하는가의 측면을 다루고, 설계에서는 사용자의 소프트웨어 요구사항을 구현하기 위한 종합적인 설계과정, 개선은 사용자와 유지/보수자에게 영향을 주는 수명주기 상에서 고려되는 사항으로, 소프트웨어가 얼마나 용이하게 사용자의 요건을 추가·변경하고 다른 프로그램에서 재사용이 가능할 것인가를 다루고 있다.

2.4.4. 소프트웨어 평가 관련 국제표준

ISO/IEC 9126(Information Technology - Software Quality Characteristics and Metrics)은 품질특성 및 메트릭을 정의하고 있는 표준으로 각 품질 특성별로 세부 메트릭을 제시하고 있다 (ISO/IEC 9126, 1995). ISO/IEC 9126에서는 소프트웨어 품질 특성 및 품질 부특성의 항목들을 계층구조로 표현하는 품질 모델을 제시하고 있다. 이는 소프트웨어 품질과 관련된 체크리스트로써 사용 가능하고 품질 부특성들은 내부 메트릭이나 외부 메트릭에 의해 측정 가능하다. 각 품질 특성 및 부특성들을 정의하면 <표 4>와 같다.

<표 4> ISO/IEC 9126 품질 특성에 대한 정의

품질 특성	부특성	정의
기능성(Functionality): 소프트웨어가 특정조건에서 사용될 때, 명시된 요구와 내재된 요구를 만족하는 기능을 제공하는 소프트웨어 제품의 능력	적합성 (suitability)	명시된 과업과 사용자 목적에 적합한 기능의 집합들을 제공해 줄 수 있는 능력
	정확성 (accuracy)	정확한 규격, 일치된 결과, 정확한 효과를 나타내는 소프트웨어의 능력, 계산에 있어서의 정확성
	상호운용성 (interoperability)	명시된 하나 또는 그 이상의 시스템들과 상호운영 될 수 있는 능력
	부합성 (compliance)	관련 표준, 법률상의 규칙 또는 협정·규정 등에 부합되는 능력
	보안성 (security)	정보나 프로그램에 대한 권한 없는 접근을 방지하는 능력
신뢰성(Reliability): 명시된 조건에서 사용될 때, 성능 수준을 유지할 수 있는 소프트웨어 제품의 능력	성숙성 (maturity)	소프트웨어의 결함으로 인한 오류를 회피하는 능력
	오류허용성 (fault tolerance)	명시된 인터페이스의 위반 또는 소프트웨어의 오류 발생시에 소프트웨어가 명시된 수준으로 성능을 유지하는 능력
	복구성 (recoverability)	고장시에 소프트웨어가 직접 피해를 입은 데이터를 복구하고 성능수준을 회복하는 능력
사용성 (Usability): 명시된 조건에서 사용될 경우, 사용자에 의해 이해되고, 학습되고, 사용되고 선호될 수 있는 소프트웨어 제품의 능력	이해성 (understandability)	특정 과업과 사용 환경에서 어떻게 사용되는지와 적합한지를 사용자가 이해할 수 있도록 하는 능력
	학습성 (learnability)	사용자에게 소프트웨어 적용법을 학습하도록 하는 소프트웨어의 능력
	운용성 (operability)	사용자가 운영하고 통제하도록 하는 소프트웨어의 능력
효율성 (Efficiency): 명시된 조건에서 사용되는 자원의 양에 따라 요구된 성능을 제공하는 소프트웨어 제품의 능력	시간효율성 (time behavior)	명시된 조건하에서, 기능 수행시 적절한 응답과 처리시간 또는 처리율을 제공해 주는 능력
	자원 활용도 (resource utilization)	명시된 조건하에서, 기능 수행시 적절한 시간동안 적절한 자원을 사용하는 능력
유지보수성 (Maintainability): 소프트웨어 제품이 변경되는 노력. (환경과 요구사항 및 기능적 명세에 따른 소프트웨어의 수정, 개선, 혹은 개작 등)	해석성 (analysability)	소프트웨어의 고장원인 또는 결함을 진단하거나, 수정되어야 할 부분을 찾아내는 능력
	변경성 (changeability)	소프트웨어가 명시된 수정을 이행하는 능력, 코딩, 설계·문서화의 변경 포함
	안정성 (stability)	소프트웨어의 수정에 의해 야기되는 예기치 못한 영향을 최소화하는 능력
	시험성 (testability)	수정된 소프트웨어의 타당성을 시험하는 능력
이식성 (Portability): 한 환경에서 다른 환경으로 전이될 수 있는 소프트웨어 제품의 능력	적응성 (adaptability)	이식 목적에 해당되는 작업이나 수단 이외의 것은 이용하지 않고, 명시된 다른 환경으로 이식될 수 있는 능력
	설치성 (installability)	소프트웨어가 명시된 환경에서 설치되는 능력
	부합성 (conformance)	소프트웨어가 이식성에 관련된 표준이나 협정에 부합하는 능력
	치환성 (replaceability)	소프트웨어가 명시된 다른 소프트웨어와 치환되어 그 환경에서 사용되는 능력

III. 연구모델

3.1 안티바이러스 소프트웨어 평가를 위한 AHP기법

Saaty(1972)에 의해 창안된 AHP 기법은 다속성 의사결정도구로, 기업이나 군사에 관련된 계획, 의사결정, 제한된 자원의 배분 등과 관련된 문제를 해결하기 위하여 개발되었다. AHP기법은 객관적인 평가요인은 물론 주관적인 평가요인도 수용하는 매우 유연한 의사결정기법으로서 수학적인 이론보다도 직관을 바탕으로 하기 때문에 그 논리가 매우 쉽다는 장점을 가지고 있다(윤재곤, 1997; Scholl et al., 2004).

AHP는 특히 집단의사결정 문제 등에 유용하여 1980년대 이후 경영과학 분야의 주요 의사결정기법으로 인정받아 왔다. 일반적으로 의사결정 문제는 서로 불완전한 정보와 제한된 자원 하에서 목적과 기준에 일치되는 최적의 대안을 선택해야 하는 문제를 가지고 있다. 이러한 관점에서 AHP는 최종적인 목적아래 하위기준들을 수립하고, 상위 목표의 관점에서 하위 기준을 평가하여 가중치를 부여하는 방식이다.

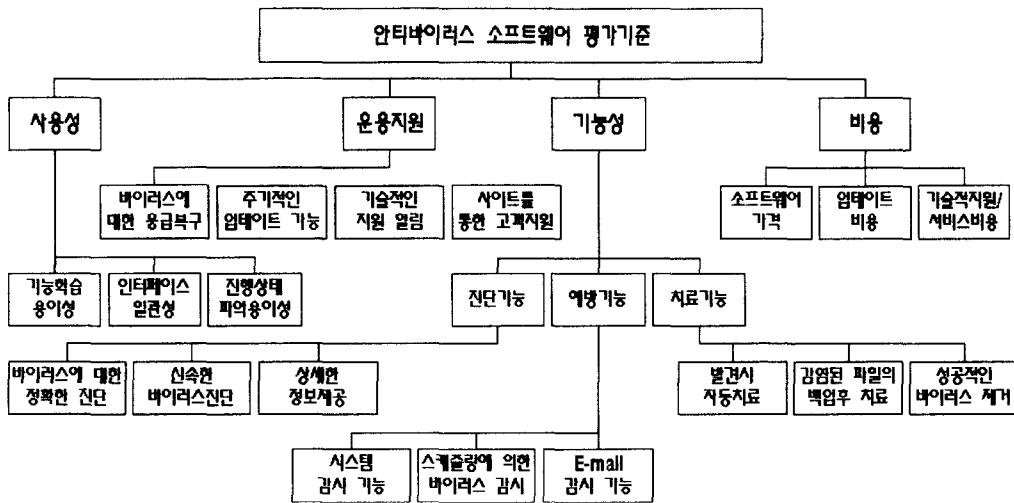
3.2 연구모형

본 연구에서 안티바이러스 소프트웨어의 평가요인 분석을 위한 평가기준의 작성은 먼저 소프트웨어 품질 평가에 관한 국제표준인 ISO/IEC 9126에서 제시하고 있는 소프트웨어 품질기준을 충족할 수 있는 기준을 도출하였다. 다음으로 안티바이러스 소프트웨어 평가측면에서 평가요인을 선정하였으며, <그림 2>와 같이 AHP기법 적용을 위한 계층도를 도출하였다.

본 연구에서 측정하고자 하는 안티바이러스 소프트웨어 평가 요인을 분석하기 위해 평가기준으로 ISO/IEC 9126의 주 품질특성 요인 중에 사용성과 기능성의 사용자 측면에서 측정 가능한 품질특성을 채택하였고, 안티바이러스 소프트웨어의 특성에서 운영지원과 비용의 주 품질평가 요인을 채택하였다.

기존의 ISO/IEC 9126은 기존의 모형에서 개발자 관점의 많은 특성이 제거되었고, 사용자 관점의 품질특성이 보다 많이 구체화되어 있다. 따라서 연구에서는 ISO/IEC 9126의 품질평가기준과 Dunham(2003)에서 논의된 설문의 세부항목을 참조하여 대폭적으로 수용하였으며 운영비용과 지원 부분은 다수의 문헌(황진숙, 2002; Dunham 2003; Sheirf & Gilliam, 2003)에서 언급되고 있는 항목들 중에서 공통적으로 논의되는 부분을 포괄적으로 구성하도록 하였다.

하부 품질특성으로는 사용성에서는 기능학습의 용이성(McCall, 1978; Evans, 1987)과 인터페이스 일관성(Boehm, 1976; Evans, 1987; ISO/IEC, 1995, Dunham, 2002), 진행상태 파악의 용이성의 세 가지의 안티바이러스 소프트웨어의 사용과 관련된 사항을 평가기준으로 하였다.



<그림 2> 안티바이러스 소프트웨어 평가 계층구조

운용지원의 하부 측정변수로는 바이러스에 대한 응급복구, 주기적인 업데이트, 기술적인 지원, 고객 트레이닝이 평가기준이 되며, 지원부분에 있어서는 Larry(2002)의 문헌과 Dunham(2002)에서 언급하고 있는 내용을 참고하여 항목들을 구성하였다. 기능성에서는 진단기능, 예방기능, 치료기능의 2차 요인으로 나눴다. 비용 측면에서는 구입비용, 업데이트 비용, 기술적인 지원/서비스 비용의 세 가지 하부평가요인으로 분리하였다. 본 연구의 측정변수를 종합하면 다음의 <표 5>와 같다.

<표 5> 안티바이러스 소프트웨어의 평가기준별 내용

	평가기준	내용
사용성	기능학습의 용이성	안티바이러스 소프트웨어의 기능을 학습하는 용이성
	인터페이스 일관성	안티바이러스 소프트웨어의 프로그램 화면의 일관성
	진행상태 파악 용이성	안티바이러스 소프트웨어의 설치, 검사 기능과정에서 어떤 진행상태가 되고 있는지에 대한 것
운용지원	바이러스에 대한 응급복구	바이러스 감염 시 치료해 줄 수 있는 시간
	주기적인 업데이트	새로운 바이러스에 대한 계속적인 최신의 치료나 스캔 정보의 제공
	기술적인 지원	바이러스를 자동으로 치료하지 못했을 때 공급업체에서 치료를 위해 기술적 지원을 제공
	고객 트레이닝	이메일이나 알림을 통한 고객에게 바이러스 위험에 대한 정보제공 정도

	바이러스 발견시 자동치료	바이러스가 발견되면 자동으로 치료하는 기능
기능성	바이러스에 감염된 파일의 백업 후 치료	감염된 파일을 치료하기 전에 파일을 저장해 주는 기능
	성공적인 바이러스 제거	바이러스 감염 시 바이러스가 제거된 것
	시스템 감시기능	컴퓨터가 켜짐과 동시에 계속적으로 바이러스에 대한 감시를 실시
	스케줄링 스캐닝	사용자가 지정한 시간에 맞추어 바이러스의 유무에 관한 검사를 실시
	E-mail 스캐닝	컴퓨터로 E-mail을 확인하기 전 바이러스의 유무에 관한 체크
	바이러스에 대한 정확한 진단	바이러스에 감염 되었을 때 감염된 바이러스의 이름과 치료 방법을 정확하게 진단하는 기능
	신속한 바이러스 진단	바이러스에 감염 되었을 때 감염된 바이러스를 시간의 지체없이 빠른 시간 내에 진단하는 기능
	침입 바이러스에 대한 상세한 정보제공	감염된 바이러스에 대한 상세한 정보가 제공되는 기능
비용	구입비용	안티바이러스 소프트웨어의 구입비용
	업데이트 비용	안티바이러스 소프트웨어를 업데이트할 때 드는 비용
	기술적인 지원/서비스 비용	고객이 기술적인 지원과 서비스를 받을 때 지출되는 비용

IV. 실증분석

본 연구에서 설문 대상은 안티바이러스 소프트웨어를 사용하고 있는 대학원생 이상의 일반 사용자 집단과 회사와 대학의 전산관리자 집단, 그리고 국내 A사의 안티바이러스 소프트웨어 개발 담당자로 구성된 전문가 집단의 세 그룹으로 이루어졌다. 연구는 설문지를 통한 실증조사의 방법이 적용되었다. 설문조사는 2004년 10월부터 11월까지 실시되었으며 개발 담당전문가들은 국내의 바이러스 개발 기업인 A회사에 근무하는 관리자급 이상을 선정하도록 하였다. 설문응답자와 관련된 기술통계와 사용자의 특성은 다음의 <표 6>과 같이 요약할 수 있다.

<표 6> 표본의 기술통계 요약

	구분	빈도	비율
성별	남	8	66.7%
	여	4	33.3%
연령	20대	7	58.3%
	30대	5	41.7%
전산경력/ 인터넷사용경력	3년~5년	2	16.7%
	5년 이상	10	83.3%
	합계	12	100.0%

4.1 계층구조별 평가기준의 중요도 산출

본 연구에서 사용되어지는 안티바이러스 소프트웨어의 평가요인 분석을 위한 계층분석은 Expert Choice 2000 프로그램을 사용하였다. 측정도구의 신뢰성 검증을 먼저 살펴보면, AHP모델은 설문자료를 토대로 통제요소들에 대한 쌍대비교과정에서 응답자들이 일관성을 가지고 평가하였는지를 판단하는 지수로서 일관성비율(consistency ratio; CR)을 산출하였다. 일반적으로 CR이 0.1 이하이면 의사결정자가 행한 쌍대비교는 합리적인 일관성을 갖는 것으로 판단하고 0.2 이내일 경우에는 용납할 수 있으나, 그 이상이면 일관성이 부족한 것으로 판단한다(Saaty, 1990). 본 연구에서는 Saaty(1990)의 연구에서 언급하고 있는 CR의 허용적인 수준인 0.2를 기준으로 적용하였다.

신뢰성 검증을 위한 일관성 비율의 분석결과를 보면 <표 7>과 같다. 표에서 나타난 바와 같이 일반사용자와 전산관리자, 전문가의 CR이 각각 0.16, 0.10, 0.08을 보여 전문가집단의 CR이 일반 사용자 집단의 CR보다 낮게 나타나는데 이는 전문가집단이 일반 사용자집단에 비해 보다 일관성 있게 응답하였다는 것을 의미한다.

<표 7> 측정도구의 신뢰성 분석

	CR ≤ 0.1	0.1 < CR ≤ 0.2	전체평균 CR
일반사용자	0	4	0.16
관리자	3	1	0.10
개발자(전문)	4	0	0.08
전체	7	5	0.11

4.2 1차 요인에 대한 분석결과

1차 요인에 대한 설문지 분석결과는 <표 8>과 같다. 1차 요인에 대한 분석 결과, 일반사용자는 “비용”을 상대적으로 중요하다고 생각하고 있는 반면에 관리자는 “기능성”을, 전문가는 “서비스 지원”을 상대적으로 중요한 것으로 판단하고 있다. 일반사용자는 안티바이러스 소프트웨어를 자신이 부담하여 구입해야 되기 때문에 관리자나 전문가에 비해 비용에 대한 관심이 크다고 볼 수 있다.

관리자의 경우 소프트웨어가 설치되고 난 후 바이러스 침해 예방을 위한 소프트웨어 자체의 기능적인 측면을 더 중요하게 생각한다고 볼 수 있으며, 전문가의 경우에는 소프트웨어를 개발하고 난 후 고객을 위한 운용지원이 가장 중요한 평가요인으로 나타났다. 다음으로 일반사용자는 “기능성”的 요인을 중요하게 생각하고 있으며 전문가 역시 “기능성”的 요인을 두 번째로 중요하게 생각하고 있다. 전체적으로 볼 때, 일반사용자, 관리자, 전문가 모두 “기능성”에 대해 상대적으로 높은 우선순위를 보여주고 있다.

<표 8> 1차 요인에 대한 분석 결과

평가요인	일반사용자		전산관리자		전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
사용성	0.111	3	0.326	2	0.165	3
운용지원	0.105	4	0.122	4	0.340	1
기능성	0.372	2	0.390	1	0.335	2
비용	0.412	1	0.163	3	0.160	4
합계	1.000		1.000		1.000	
일관성지수	0.190		0.088		0.078	

4.3 2차 요인에 대한 분석결과

앞에서 분석한 안티바이러스 소프트웨어의 1차 요인에 대한 분석에 이어 이들의 세부구성항 목인 2차 요인들에 대한 분석을 각 1차 요인 별로 실시하였다.

4.3.1 평가기준 “사용성”의 하위 평가 기준들 간의 상대적 중요도

“사용성” 요인의 2차 세부 평가요소들에 대한 우선순위를 살펴보면 <표 9>와 같다. 전체적으로 보면, 일반사용자와 관리자의 경우 사용성의 세부 평가항목의 중요도는 같은 것으로 나타났다. 그 중에서 “기능 학습의 용이성” 요인이 상대적으로 가장 중요한 것으로 나타났으며, 전문가의 경우 “진행상태를 파악하는 용이성”이 상대적으로 가장 중요한 것으로 나타났다. 사용자, 관리자, 전문가 모두 “인터페이스 일관성” 항목에 대해서 가장 낮은 중요도를 보였는데, 이것은 현재 안티바이러스 소프트웨어 제품의 인터페이스 자체가 워낙 잘 갖추어져 있기 때문에 상대적으로 낮은 중요도를 보인 것으로 보인다.

<표 9> “사용성”의 하위 평가기준들의 상대적 중요도

사용성	일반사용자		전산관리자		전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
기능을 학습하는 용이성	0.569	1	0.513	1	0.392	2
인터페이스 일관성	0.181	3	0.231	3	0.146	3
진행상태 파악 용이성	0.250	2	0.256	2	0.462	1
합계	1.000		1.000		1.000	
일관성지수	0.098		0.070		0.088	

4.3.2 평가기준 “운용지원”의 하위 평가 기준들 간의 상대적 중요도

“운용지원” 요인의 2차 세부 평가요소들에 대한 우선순위를 살펴보면 <표 10>과 같다. 일반 사용자와 관리자는 “주기적인 업데이트” 요인이 가장 중요하다고 나타나고 있으며, 전문가의 경우 “사이트를 통한 고객지원”이 가장 중요한 것으로 나타나고 있다. 일반사용자와 관리자의 경우 새로운 바이러스의 생성과 침입에 대비하기 위한 것으로 주기적인 업데이트가 가장 중요한 요인으로 나타나며, 전문가의 경우 소프트웨어의 구입 사후의 고객에 대한 지원이 가장 중요한 요인으로 생각하고 있는 것이다. 하지만, 전문가의 경우 우선순위의 평가요인으로 “사이트를 통한 고객지원”을 인지하고 있지만, 나머지 평가요인인 “주기적인 업데이트 가능”과 “기술적인 지원”역시도 가중치에서 비슷한 수치를 보이고 있다.

<표 10> “운용지원”的 하위 평가 기준들 간의 상대적 중요도

운용지원	일반사용자		전산관리자		전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
바이러스에 대한 응급복구	0.385	2	0.279	2	0.085	4
주기적인 업데이트 가능	0.403	1	0.469	1	0.265	3
기술적인 지원	0.136	3	0.122	4	0.312	2
사이트를 통한 고객지원	0.076	4	0.131	3	0.338	1
합계	1.000		1.000		1.000	
일관성지수	0.138		0.095		0.075	

4.3.3 평가기준 “기능성”的 하위 평가 기준들 간의 상대적 중요도

“기능성” 요인의 2차 세부 평가요소들에 대한 우선순위를 살펴보면 <표 11>과 같다. “기능성”的 경우에는 전체적으로 세무항목간의 중요도에 큰 차이가 없는 것으로 나타났다. 먼저 전체적인 관점에서 보면, “치료기능”이 가장 중요한 요인으로 나타났으며, “진단기능”과 “예방기능”이 다음으로 중요한 항목으로 나타났다. 전문가의 경우 우선순위는 “치료기능”이 상대적으로 가장 중요하다고 나타나고 있지만, “진단기능”과 “예방기능”과의 가중치는 크게 차이가 나지 않는 것을 볼 수 있다. 이것은 전문가가 진단기능, 예방기능, 치료기능을 전부 중요하게 생각하고 있다고 할 수 있다. 반면에 관리자의 경우는 “치료기능”的 기능성에 대해 다른 기능성보다 상대적으로 높은 가중치를 주고 있는 것으로 나타났다. 이는 바이러스가 침입하고 난 후의 사후 치료기능만을 중요하게 생각하고 있는 것으로 볼 수 있다.

<표 11> “기능성”의 하위 평가 기준들 간의 상대적 중요도

기능성	일반사용자		전산관리자		전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
진단기능	0.388	2	0.276	2	0.324	2
예방기능	0.164	3	0.228	3	0.284	3
치료기능	0.448	1	0.496	1	0.393	1
합계	1.000		1.000		1.000	
일관성지수	0.105		0.015		0.058	

4.3.4 평가기준 “비용”의 하위 평가 기준들 간의 상대적 중요도

2차 평가요인의 마지막으로 “비용” 요인의 2차 세부 평가요소들에 대한 우선순위를 살펴보면 <표 12>와 같다. 일반사용자의 경우 “소프트웨어가격” 요인이 가장 중요하다고 나타났으며, 관리자와 전문가는 “업데이트 비용”이 상대적으로 가장 중요하다고 나타나고 있다. 이것은 앞에 1차 요인에서 살펴보았듯이 사용자의 경우 “비용” 요인을 상대적으로 가장 중요하다고 나타났으며, 그것이 곧 소프트웨어의 가격에 대한 비용이라는 것을 알 수 있다. 반면, 관리자와 전문가의 경우 계속적인 개선을 통한 새로운 바이러스 검색과 진단, 치료에 효율적으로 대처할 수 있는 것을 중요하게 생각하고 있다.

<표 12> “비용”의 하위 평가 기준들 간의 상대적 중요도

비용	일반사용자		전산관리자		전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
소프트웨어가격	0.575	1	0.301	2	0.180	3
업데이트비용	0.186	3	0.487	1	0.427	1
기술적 지원 서비스 비용	0.239	2	0.213	3	0.393	2
합계	1.000		1.000		1.000	
일관성지수	0.115		0.065		0.083	

4.4 3차 요인에 대한 분석결과

마지막으로 2차 요인의 “진단기능”, “예방기능”, “치료기능”에 대한 각각의 세부 항목 평가요인에 대해 살펴보면 다음과 같다.

4.4.1 2차 평가기준 “진단기능”의 하위 평가 기준들 간의 상대적 중요도

“진단기능”에 대한 하위 세부 평가요인의 상대적인 중요도는 <표 13>과 같다. 일반사용자와 관리자의 경우 평가요인에 대한 상대적 중요도의 순위가 같이 나타나고 있다. 바이러스에 대한 “정확한 진단”이 가장 중요하고, 다음으로 바이러스에 대한 “신속한 진단”이 중요하다고 나타나고 있다. 반면, 전문가의 경우 바이러스에 대한 “상세한 정보제공”이 가장 중요한 평가요인으로 나타나고 있다.

<표 13> “진단기능”의 하위 평가 기준들 간의 상대적 중요도

진단기능	일반사용자		전산관리자		전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
바이러스에 대한 정확한 진단	0.546	1	0.510	1	0.188	3
신속한 바이러스 진단	0.342	2	0.410	2	0.256	2
상세한 정보제공	0.112	3	0.080	3	0.557	1
합계	1.000		1.000		1.000	
일관성지수	0.148		0.080		0.158	

4.4.2 2차 평가기준 “예방기능”의 하위 평가 기준들 간의 상대적 중요도

“예방기능”的 세부 하위 평가요인에 대한 중요도는 <표 14>와 같다. 사용자와 관리자의 경우 바이러스에 대해 “시스템 감시기능”이 가장 중요한 평가요인으로 나타나고 있다. 이는 바이러스 침입에 대비하여 시스템을 계속적으로 감시하는 것이 중요시 되고 있음을 알 수 있다. 반면에 전문가의 경우 “스케줄링에 의한 감시”가 가장 중요한 평가요인으로 나타나고 있는데, 이것은 예약된 시간에 맞춰서 지속적인 바이러스에 대한 예방차원이 중요하다는 것을 나타나는 것이다.

<표 14> “예방기능”的 하위 평가 기준들 간의 상대적 중요도

예방기능	일반사용자		전산관리자		전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
시스템 감시기능	0.682	1	0.680	1	0.200	3
스케줄링에 의한 바이러스 감시	0.161	2	0.100	3	0.515	1
E-mail 감시기능	0.157	3	0.220	2	0.286	2
합계	1.000		1.000		1.000	
일관성지수	0.170		0.090		0.028	

4.4.3 2차 평가기준 “치료기능”의 하위 평가 기준들 간의 상대적 중요도

“치료기능”的 세부 하위 평가요인에 대한 중요도는 <표 15>와 같다. 전문가의 경우 바이러스에 대한 “자동치료,” “파일백업 후 치료,” “바이러스 제거”的 순으로 중요도를 나타내고 있다. 반면에 일반사용자의 경우 반대로 “바이러스 제거,” “파일백업 후 치료,” “자동 치료”的 순으로 중요도를 평가하고 있다.

전문가의 경우는 바이러스가 침입하면 바이러스에 대해 자동적인 치료가 가능해야 사용자가 소프트웨어에 대해 만족 할 것이라고 생각하고 있으며, 일반사용자와 관리자의 경우 바이러스가 성공적으로 제거하는 것이 더 중요하다고 생각하고 있다. 그리고 일반사용자는 “파일백업 후 치료”的 요인이 두 번째로 중요하다고 생각하고 있는 반면에 관리자는 가장 낮은 중요도를 보이고 있는데, 이것은 일반사용자는 개인의 파일이 중요한 것으로 인식되며, 관리자는 컴퓨터를 전체적으로 관리하는 입장에서 파일보다는 전체적으로 바이러스의 침입에 대해 치료되는 것이 더 중요시 되고 있음을 알 수 있다.

<표 15> “치료기능”的 하위평가 기준들 간의 상대적 중요도

치료기능	일반사용자		전산관리자		전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
발견시 자동 치료	0.191	3	0.310	2	0.422	1
감염된 파일백업 후 치료	0.393	2	0.170	3	0.330	2
성공적인 바이러스 제거	0.417	1	0.520	1	0.248	3
합계	1.000		1.000		1.000	
일관성지수	0.138		0.100		0.038	

4.5 평가요인에 대한 집단별 우선순위 비교

앞에서 AHP분석을 통하여 안티바이러스 소프트웨어에 대한 일반사용자, 전산관리자, 전문가의 평가요인에 대한 상대적인 중요도를 산출하였다, 전체적인 결과는 <표 16>에 나타나 있다. 결과들을 비교 편의를 위해 평가요인별로 세부 항목들을 순위화해서 배열하였다. 여기서 중요도 항목은 각 세부항목이 속한 1차 평가기준 내에서 세부 평가항목들 간의 상대적 중요도를 나타내고, 합성중요도 항목은 전체 세부항목 중에서 각 세부항목이 가지는 상대적인 중요도를 나타낸다.

표에서 보면, 일반사용자와 전산관리자가 중요하게 생각하고 있는 평가요인은 대동소이한 것으로 나타났다. 상위 순위 10개중 7개의 공통요인이 나타난 것을 볼 수 있다. 세부적으로 살펴보면, 일반사용자는 평가항목들 중에서 특히 비용에 관련된 요인에 대해 상대적으로 중요하게 생각하고 있고, 관리자들은 운용지원 요인을 제외한 모든 요인에 대해서 중요도를 높게 평가하였다. 반면에 전문가 집단은 바이러스의 치료기능과 고객을 위한 운용지원에 관한 요인에 대해 상

대적으로 더 중요하게 평가하였다. 특히 운용지원 항목은 다른 두 집단에서 하나의 세부항목도 상위 10위안에 평가하지 않았다.

<표 16> 집단별 세부 평가요인 항목들의 순위비교

순위	일반사용자			전산관리자			전문가		
	세부항목	중요도	합성 중요도	세부항목	중요도	합성 중요도	세부항목	중요도	합성 중요도
1	소프트웨어 가격	0.575	0.224	바이러스 제거	0.520	0.139	자동치료	0.422	0.101
2	정확한 진단	0.546	0.103	정확한 진단	0.510	0.109	고객지원	0.388	0.097
3	신속한 진단	0.342	0.102	자동치료	0.310	0.100	기술적 지원	0.312	0.094
4	기술적지원/서비스비용	0.239	0.076	기능학습 용이성	0.513	0.086	주기적인 업데이트	0.265	0.081
5	바이러스 제거	0.417	0.071	시스템 감시기능	0.680	0.082	상세한 정보제공	0.557	0.080
6	업데이트 비용	0.186	0.060	신속한 진단	0.410	0.074	파일백업 후 치료	0.330	0.078
7	시스템 감시기능	0.682	0.052	소프트웨어 가격	0.301	0.061	스케줄링에 의한 감시	0.515	0.058
8	기능학습 용이성	0.569	0.051	진행상태파악 용이성	0.256	0.060	바이러스 제거	0.248	0.057
9	응급복구	0.385	0.048	인터페이스 일관성	0.231	0.051	기술적/서비스 비용	0.393	0.051
10	파일백업 후 치료	0.393	0.042	업데이트비용	0.487	0.049	진행상태파악 용이성	0.462	0.045
11	자동치료	0.191	0.032	파일백업 후 치료	0.17	0.040	업데이트 비용	0.427	0.045
12	주기적인 업데이트	0.403	0.032	주기적인 업데이트	0.469	0.036	신속한 진단	0.256	0.039
13	진행상태 파악용이성	0.250	0.024	기술적/서비스 비용	0.213	0.025	e-mail 감시	0.286	0.036
14	상세한 정보제공	0.112	0.017	응급복구	0.279	0.025	기능학습 용이성	0.392	0.036
15	인터페이스 일관성	0.181	0.017	e-mail 감시	0.22	0.022	시스템 감시기능	0.200	0.025
16	e-mail 감시	0.157	0.014	상세한 정보제공	0.08	0.015	응급복구	0.085	0.025
17	기술적 지원	0.136	0.011	스케줄링에 의한 감시	0.10	0.014	정확한 진단	0.188	0.024
18	스케줄링에 의한 감시	0.161	0.010	기술적 지원	0.122	0.009	소프트웨어 가격	0.180	0.017
19	고객지원	0.076	0.009	고객지원	0.131	0.009	인터페이스 일관성	0.146	0.013

결론적으로, 일반사용자와 전산관리자는 안티바이러스 소프트웨어 평가요인들 간에 차이가 거의 없지만, 전문가와 비교해 볼 때 항목들 간에 큰 차이가 있었다.

V. 결 론

본 연구에서는 안티바이러스 소프트웨어의 평가기준을 도출하여 사용자, 관리자 및 전문가 집단을 대상으로 평가항목의 상대적 중요도에 대한 설문조사를 수행하고, 그 결과에 대하여 AHP 기법을 이용하여 분석하였다. 전반적인 분석 결과를 살펴보면, 전문가 집단은 사용자와 관리자 집단과는 평가요인의 상대적인 중요성에 대해 다른 견해를 보였다. 특히 운용지원과 관련된 평가 요인은 사용자와 관리자 집단에서는 상대적으로 중요하지 않다고 생각하고 있는 평가요인이다.

연구의 분석 결과를 통해서 일반사용자와 관리자 집단을 포함하는 안티바이러스 소프트웨어의 소비자는 개발자인 전문가 집단과는 안티바이러스 소프트웨어를 바라보는 관점이 다르다는 점을 발견할 수 있다. 부연하면, 소비자는 가격에 상대적으로 더 민감하다. 또한, 다양하고 방대한 기능을 가진 다른 응용프로그램과는 달리 안티바이러스 소프트웨어에 대해서 바이러스 방지 및 치료라는 명확하게 정의된 기능을 소비자는 인지하고 있다. 개발자의 입장에서 생각하면, 당연히 비용보다는 해당 소프트웨어가 제공하는 기능이 더 우선시될 것이고, 현재 시중에 나와 있는 여러 안티바이러스 소프트웨어의 기능이 비슷한 수준에 있음을 감안한다면, 운영지원 부분에 보다 더 많이 치중함으로써 다른 제품과의 차별적 특성을 부여할 수 있을 것이다.

개발자가 운영지원 관련 사항들을 중요하게 생각하는 다른 이유로는 안티바이러스 소프트웨어가 제공하는 기능이 적절히 유지되기 위해서는 소프트웨어 제작사의 지원이 뒷받침되어야 하기 때문이라고 판단된다. 이것은 현재의 안티바이러스 소프트웨어가 새로 만들어지는 컴퓨터 바이러스에 효과적으로 대응하기에는 한계가 있기 때문이다. 신종 바이러스는 날이 갈수록 기술적으로 보다 더 정교해지고 다양한 변종이 만들어지고 있지만, 패턴 매칭 기법을 위주로 하는 현재의 바이러스 검색 알고리즘으로는 대응하기에는 한계가 있다(Nachenberg, 1997). 따라서 소프트웨어 업데이트와 고객 지원과 같은 운영지원은 바이러스 검색 알고리즘의 한계를 보완할 수 있는 중요한 수단이다.

운용지원 항목과 관련하여 다른 중요한 논의사항은 안티바이러스 소프트웨어의 사용에 관한 것이다. 흔히 100% 완벽한 정보보안은 달성이 불가능하다고 한다. 컴퓨터 바이러스 문제도 동일하다. 최근 실시된 국내외의 여러 조사에 따르면 대다수의 기업들이 안티바이러스 소프트웨어를 사용하고 있음에도 불구하고 많은 기업들이 바이러스 관련 피해를 입은 경험이 있다고 한다 (Bagchi & Udo, 2003; 한국전산원, 2003; CSI, 2003). 이것은 컴퓨터 바이러스에 의한 피해를 방지하기 위해서 단순히 안티바이러스 소프트웨어를 설치하여 운영한다고 해서 해결될 문제가 아니라라는 점을 시사한다. 다른 정보보안의 문제처럼 기술적인 측면과 더불어 관리적인 측면에서 포괄적으로 다루어져야 한다. 안티바이러스 소프트웨어 평가기준 중에서 운영지원 항목들은 관리적인 측면을 포함하고 있다는 점에서 사용자와 관리자들이 관심을 가져야 할 요소이다.

마지막으로, 본 연구의 한계점과 추후과제는 다음과 같다. 첫째, 본 연구에서는 전문가 집단을 구성하는 응답자를 한 회사에서만 선정하였기 때문에 그 회사의 개발전략이 응답자의 중요도 평가에 영향을 미칠 가능성을 배제할 수 없다. 따라서 향후 연구에서는 다수의 안티바이러스 소프

트웨어 업체에 소속된 전문가를 선정하여 실증분석을 실시하면 보다 일반화된 결과를 도출해 낼 수 있을 것이다. 둘째, 본 연구에서 안티바이러스 소프트웨어의 평가요인에 대하여 획단적 분석이 수행되었는데, 안티바이러스 관련 보안관리의 성숙도에 따라서 평가요인의 중요성에 대한 변화추이를 살펴보는 것도 의미가 있을 것으로 생각된다.

참 고 문 헌

- 박호인, 정호원, “소프트웨어 제품을 위한 평가 선정 모형의 조사 및 적용성에 관한 연구,” 한국 정보처리학회, 제4권 제7호, 1997, pp. 1706-1718.
- 윤재곤, “AHP기법의 적용효과 및 한계점에 관한 연구: MIS 성공요인평가를 위한 3가지 통계기법 비교중심,” 한국경영과학, 제 21권 제 3호, 1996, pp. 109-125.
- 정관진, 이희조, 인터넷 웹과 바이러스의 진화와 전망, 안철수 연구소, 2003.
- 차민석, 바이러스 백신과 악성코드에 대한 몇 가지 이해, 안철수 연구소, 2002. (http://info.ahnlab.com/security_info)
- 한국전산원, 국가정보화 촉진을 위한 품질정책연구, 한국전산원, 1997.
- 한국전산원, 2003 한국인터넷백서, 한국전산원, 2003.
- 황진욱, An Analysis of Consumers' Preference in Virus Vaccine Programs, 한국정보통신대학원 석사학위논문, 2002.
- Bagchi, K. and G. Udo, "An Analysis of the Growth of Computer and Internet Security Breaches," *Communications of the AIS*, Vol. 12, 2003, pp. 684-700.
- Boehm, B. W., J. R. Brown, and M. Lipow, "Quantitative Evaluation of Software Quality," *Proc. 2nd Int. Conf. on Soft.*, 1976, pp. 592-605.
- Brunnstein, K., "From AntiVirus to AntiMalware Software and Beyond : Another Approach to the Protection of Customers from Dysfunctional System Behaviour," *National Information Systems Security Conference Status*, Vol. 22, 1999.
- CERT, CERT/CC Overview, *Carnegie Mellon University*, 2003, pp. 1-29.
- Cohen, F., "Computer Viruses - Theory and Experiments," *7Th DOS/NBS Computer Security Conference*, 1984, pp. 143-158.
- CSI, 8th Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2003.
- Dunham, K., "Evaluating Anti-Virus Software: Which Is Best?," *Telecommunications and Network security*, Jul/Aug, 2003, pp. 17-28.

- Evans, M. W. and J. J. Marciniak, Software Quality Assurance and Management, John Wiley & Sons, 1987.
- Expert Choice Korea, Expert Choice Guide and Tutorial, 2002.
- Gilles, A. C., Software Quality : Theory and Management, Chapman and Hall, 1992.
- Highland, H. J., "A History of Computer Viruses : Three Special Viruses," *Computer & Security*, Vol. 16, No. 5, 1997, pp. 430-438.
- Hubbard, J. and K. Forcht, "Computer Viruses : How Companies Can Protect Their Systems," *Industrial Management & Data Systems*, Vol. 98, No. 1, 1998, pp. 12-16.
- ICSA Labs, Computer virus Prevalence Survey, 2003.
- ISO/IEC 9126, Information Technology—Software Product Evaluation Quality Characteristics and Guidelines for Their Use, Geneve, 1991.
- Larry, S., "Personal Antivirus : The One Utility You Can't Live Without," PC magazine, June 11, 2002, pp. 97-98.
- Mamaghani, F., "Evaluation and Selection of an Antivirus and Content Filtering Software," *Information Management & Computer Security*, Vol. 10, No. 1, 2002, pp. 28-32.
- McCall, J. A., P. K. Richards, and G. F. Walters, "A Framework for the Measurement of Software Quality," *The Proceeding of the ACM Software Quality Assurance*, 1978.
- Nachenberg, C., "Computer Virus - Anti Virus Coevolution," *Communications of the ACM*, Vol. 40, No. 1, 1997, pp.46-51.
- Saaty, T. L., "A Scaling Method for Priorities in Hierarchical Structures," *Journal of Mathematical Psychology*, Vol. 15, No. 3, 1977, pp. 234-281.
- Saaty, T. L., "How to Make a Decision : the Analytic Hierarchy Process," *European Journal of Operational Research*, Vol. 48, No. 1, 1990, pp. 9-26.
- Scholl, A., L. Manthey, R. Helm, and M. Steiner, "Solving Multi attribute Design Problems with Analytic Hierarchy Process and Conjoint Analysis: An empirical comparison", *European Journal of Operational Research*, Vol. 164, No. 3, 2005, pp. 760-777.
- Sherif, J. S. and D. P. Gilliam, "Deployment of Anti-Virus Software: a Case Study," *Information Management & Computer Security*, Vol. 11, No. 1, 2003, pp. 5-10.

<Abstract>

An Analysis of Evaluation Factors of Anti-Virus Software Using AHP Technique

Jong-Ki Kim, Suk-Yeon Hwang, Dong-Ho Lee

The history of computer virus comes along with that of computer. Computer virus has surfaced as a serious problem in information age. The advent of open network and widespread use of Internet made the problem even more urgent. As a method of defense for computer virus most companies use anti-virus software. Selecting appropriate anti-virus software involves various criteria and thus it is a multiple-attribute decision making problem. The purpose of this study is to prioritize anti-virus software evaluation factors. To do that, first of all, important evaluation factors are selected based on previous research on anti-virus software as well as general software evaluation models. Then, a questionnaire survey was conducted on end-users, system administrators and anti-virus software developers. The survey result was analyzed with ExpertChoice 2000 which is based on Analytic Hierarchy Process technique.

This study found that there are clear differences among three survey groups regarding the relative importance of overall evaluation factors. End-user group ranked "cost" first, but it was the least important factor to developer group. Developers pointed out "operational support" as the most important factor. There were also obvious differences in the relative importance of detail evaluation items. Both end-users and system administrators shared 7 common items among top 10 most important items. Moreover, neither of the two groups ranked any of the items in the "operational support" factor in top 10, whereas all 4 items in the factor were included in top 10 by developer group.

Keyword: Antivirus Software, AHP, Evaluation Factor, Information Security

* 이 논문은 2005년 1월 24일 접수하여 1차 수정을 거쳐 2005년 3월 22일 게재 확정되었습니다.