Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.5, Oct. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.5.847

Anti-Virus 성능 시험을 위한 평가 기준 수립 연구*

이 정 호,[1†] 신 강 식,[2] 유 영 락,[2] 정 동 재,[1] 조 호 묵[3‡]
[1,2,3]KAIST 사이버보안연구센터 (선임연구원, 연구원, 책임연구원)

A Study on Establishment of Evaluation Criteria for Anti-Virus Performance Test*

Jeongho Lee,[1†] Kangsik Shin,[2] Youngrak Ryu,[2] Dong-Jae Jung,[1] Ho-Mook Cho[3‡]
[1,2,3]KAIST Cyber Security Research Center (Senior Researcher, Researcher, Principle Researcher)

요 약

최근 국내에서 소프트웨어의 취약점을 이용한 악성코드로 피해가 증가하는 가운데 악성코드를 막기 위한 안티바이러스 설치는 필수사항이라 할 수 있다. 하지만 일반 사용자는 어떠한 안티바이러스 제품의 성능이 좋은지 자신의 환경에 적합한지를 알기란 쉽지 않다. 국외에 안티바이러스 성능에 대한 정보를 제공해주는 기관이 다수 존재하고 이런 기관들은 자체 테스트 환경과 시험평가 항목을 수립하여 테스트를 진행하고 있으나, 자세한 테스트 환경 정보, 세부적인 시험평가 항목 및 결과는 공개하지 않는다. 또한 기존 품질평가 연구들은 안티바이러스 제품 평가에는 부합되지 않는 평가 기준이 다수 존재하는 등의 이유로 최신 안티바이러스 평가에는 적절하지 않다. 그래서 본 논문에서는 최신 안티바이러스 평가에 적합한 세부적인 안티바이러스 평가지표를 수립하고 이를 국내외 9종의 안티바이러스 제품에 적용하여 안티바이러스의 기능 및 성능을 검증하였다.

ABSTRACT

With the recent increase in damage caused by malcious codes using software vulnerabilities in Korea, it is essential to install anti-virus to prevent malicious codes, However, it is not easy for general users to know which anti-virus product has good performance or whether it is suitable for their environment. There are many institutions that provide information on anti-virus performance outside of korea, and these institutions have established their own test environments and test evaluation items, but they do not disclose detailed test environment information, detailed test evaluation items, and results. In addition, existing quality evaluation studies are not suitable for the evaluating the latest anti-virus products because there are many evaluation criteria that do not meet anti-virus product evaluation. Therefore, this paper establishes detailed anti-virus evaluation metrics suitable for the latest anti-virus evaluation and applies them to 9 domestic and foreign anti-virus products to verify the functions and performance of anti-viruses.

Keywords: Anti-Virus, Malware, Performance Evaluation

I. 서 론

최근 국내에서 MagicLine4NX(매직라인)의 취약점을 이용하여 북한 정찰총국이 기업 및 정부 기관 50여 곳을 대상으로 한 악성코드를 유포하는 사건이 발생하였다. 매직라인은 국가, 공공기관, 금융

Received(08. 18. 2023), Modified(09. 07. 2023), Accepted(09. 07. 2023)
* 본 논문은 과학기술정보통신부 글로벌사이버보안기술연구(과제고유번호: 1711177169) 사업의 지원을 받아 수행된 연구임
† 주저자, ddanzit@gmail.com
‡ 교신저자, chmook79@kaist.ac.kr(Corresponding author)

기관 등의 홈페이지에 공동인증서로 로그인할 때 본인 인증을 위해 개인용 컴퓨터에 설치되는 프로그램이다. 이 프로그램은 한번 설치되면 사용자가 별도로 업데이트하거나 삭제하지 않는한 자동실행되며, 취약점이 존재한다면 해커의 해킹 경로로 악용되기 쉽다.

또 다른 사건으로는 한글 2022 크랙 설치파일로 위장한 암호화폐 채굴 및 원격제어 악성코드가 국내 파일공유사이트를 통해 유포되었는데, 이 악성파일은 사용자가 다운로드 한 후 압축을 해제하고 설치할 때 사용자 컴퓨터에 안티바이러스가 설치되어 있지 않을 경우 한글 2022 크랙 설치파일과 함께 원격제어 악성코드인 오르쿠스(Orcus) RAT이 다운로드 되어 해커가 사용자 컴퓨터를 원격으로 제어할 수 있는 권한을 획득할 수 있다.

이처럼 안티바이러스 프로그램이 설치되어 있지 않는다면 악성코드로 인한 감염에 노출될 위험이 높아질 수 있으므로 컴퓨터에 안티바이러스 프로그램을 설치하는 것은 컴퓨터를 보호하기 위해 최소한의 필수사항이라 할 수 있다.

하지만 수많은 안티바이러스 프로그램 중 어떠한 제품의 기능 및 성능이 좋은지, 자신의 환경에 적합한지는 일반 사용자가 알기란 쉽지 않다. 이런 안티바이러스 성능에 대한 정보를 제공해주는 기관들이 국외에 여러 곳이 존재하는데 이러한 기관들은 다양한 안티바이러스 제품의 성능을 테스트하고 인증해주는 역할을 하고 있으며, 국내 안티바이러스 제품들도 일부 기관에 인증을 받아 품질을 인정받고 있다.

이런 기관들은 자체 테스트 환경과 시험평가 항목을 수립하고 테스트하고 있으나, 자세한 테스트 환경, 세부적인 시험평가 항목 및 결과는 공개하지 않고 큰 범주의 시험평가 항목에 대한 평가 결과만을 공개하고 있다. 또한 기존 품질평가 연구들은 안티바이러스 제품 평가에는 부합되지 않는 평가 기준이 다수 존재하는 등의 이유로 최신 안티바이러스 제품을 평가하기에 적절하지 못하다. 그래서 본 논문에서는 최신 안티바이러스 제품 평가에 적합한 세부적인 평가지표를 수립하고, 이를 국내외 9종의 안티바이러스 제품에 적용하여 기능 및 성능을 분석하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대해 기술하고, 3장에서는 안티바이러스 평가 기준을 수립하고 이에 대한 검증을 진행하고, 4장에서는 결론 및 향후 연구 방향에 대해 논한다.

II. 관련연구

2.1 안티바이러스 성능테스트 기관

2.1.1 ICSA Labs[1]

1991년에 설립된 미국의 사설 시험기관으로 암호장비, 침입차단시스템, 침입탐지시스템, 안티바이러스 등 다양한 정보보호제품에 대한 인증을 실시하고 있으며, 미국 국방성과 정부 인증 보안규격 테스트 및 암호검증(CVP) 평가 업무도 함께 수행하고 있어 세계적으로 신뢰성이 높은 인증기관이다. 안티바이러스 평가는 In-the-Wild, Common Infectors, Zoo 3가지 형태의 악성코드 샘플 수만개를 가지고 이루어지며 100% 정확히 탐지해 오탐이 없어야 인증 획득이 가능한 까다롭고 권위 있는 인증 기관이다.

2.1.2 Comparitech[2]

VPN, 안티바이러스, 네트워크 모니터링 도구, 방화벽 등을 포함한 광범위한 제품에 대한 테스트를 진행하는 영국에 소재하고 있는 2015년에 설립된 기관이다.

각 안티바이러스에 대해 장점, 단점, 가격 등을 자세히 소개하며 두 개의 안티바이러스 간의 비교, 안티바이러스 순위 및 테스트 결과를 공개하고 있다. 안티바이러스 테스트는 탐지, 치료, 자동갱신 정책, 시스템 영향, 기본기능, 고급기능 등 다양한 방법으로 샌드박스 환경에서 테스트를 진행하고, 탐지의 경우 EICAR 테스트 악성코드 및 실제 악성코드를 이용하여 테스트를 진행하며 실시간 스캔 및 전체 시스템 스캔을 이용하여 평가를 진행한다.

2.1.3 AV-Comparatives[3]

오스트리아에 위치한 비영리 보안 제품 테스트 기관으로 실제 환경과 동일한 상황에서 테스트를 진행하며 자체 크롤링 시스템을 사용하여 악성 사이트 샘플을 수집하여 테스트를 진행한다. 기관에서 제시하는 신뢰성 및 안정성에 해당하는 13개의 요구사항을 충족해야 인증을 획득할 수 있다. AV-Comparatives의 Real-World Protection Test 방법론은 오스트리아 정부에서 수여하는 Constantinus Award, standortagentur Tirol에서 수여하는 Cluster

Award 등의 다양한 상을 수상하였다.

2.1.4 AV-TEST[4]

여러 안티바이러스 제품을 테스트하고 순위를 매기는 독일 소재의 글로벌 보안제품 성능평가 기관이며, 보호(탐지/치료), 사용성, 성능 3가지 범주에 대해 테스트를 진행하여 각각 최대 6점을 획득할 수 있으며 총 10점 이상을 획득하고 각 범주에서 최소 1점 이상은 획득해야 인증이 된다. Android, MacOS, Windows 등 OS 제품군별, 개인용, 기업용 등 사용자별 등 다양한 형태의 테스트를 진행하며 테스트 결과는 홈페이지를 통해 공개하고 있다. 이 연구소는 2021년 스위스 IT 보안 그룹에 인수되었다.

2.1.5 Virus Bulletin[5]

악성코드 전문 매거진을 발행하는 영국의 민간 보안 연구 단체이다. 1989년부터 매거진을 발행했으며 2006년에 인쇄 잡지로 배포되던 것을 중단하고 완전히 디지털화하였다. 2014년 이후로는 월간 간격이 아닌 독립형 기사 형태로만 웹사이트에 게시한다. 인증 프로그램인 VB100은 1998년도부터 운영되어 왔으며 Windows 엔드포인트 보안 솔루션에 대한 인증 테스트이다. 전 세계 지역을 기준으로 최소 2개 지역 이상에서 실제 감염이나 발견 보고가 있었던 최근 악성코드 1,000~2,000개, 정상 어플리케이션 100,000개로 가상머신에서 테스트를 진행하며 평가 기간은 약 1개월이 소요된다. 인증된 제품 및 결과는 최신순으로 홈페이지를 통해 공개한다.

2.1.6 MRT Effitas[6]

2009년 웹사이트 포럼으로 시작하여 성장한 영국의 독립적인 성능 평가기관으로 자체적인 Level을 만들어 평가를 진행하며, 최신 악성코드 동향을 반영한 악성 앱을 직접 만들어 평가에 활용한다. 평가 결과는 분기별로 홈페이지를 통해 공개하며 정상 애플리케이션 500개 샘플, 익스플로잇, 랜섬웨어, 봇넷, 애드웨어 등의 다양한 악성코드 샘플로 테스트를 진행하며 악성 정탐율 99% 이상인 경우에 인증을 획득할 수 있으며, 4개의 분기별 테스트를 모두 통과하면 Effitas 상을 수여한다.

2.1.7 SE Labs[7]

다양한 안티바이러스 테스트를 진행하며 개인 및 기업 대상의 보안 제품 컨슈머 리포트를 제공하는 영국의 민간 테스트 기관이다. 테스트는 Windows 10 기반의 PC에 VLAN을 이용하여 다른 대상 시스템과 격리하여 진행하며 샘플 악성코드 중 널리 퍼진 것으로 판단된 악성코드는 가중치를 부여하여 테스트된다. 테스트는 분기별로 실행되며 엔터프라이즈, 소기업 및 소비자 제품으로 구분하여 진행한다.

2.2 기존 평가기준 연구

윤여웅 등은 정보보호 제품에서는 일반 소프트웨어와 달리 가장 중요한 품질이 보안성이며 낮은 성능을 가진 정보보호 제품은 대용량 네트워크 환경에서 운영되지 않을 수 있으므로 성능적인 요소를 포함한 정보보호 특성이 고려되어야 하며 이러한 특성에는 안전한 자산 보호 기능, 높은 성능, 사용편의성, 신뢰성, 유지보수성, 통합 호환성이 있다고 하였다[8].

맹두열 등은 국제표준 ISO/IEC 품질인증 시스템을 기반으로 국내외 기관 및 연구소에서 품질에 대한 많은 방법론이 연구 및 적용되고 있으나, 다양한 속성을 지닌 소프트웨어를 정해진 기준에 맞추어 품질 및 성능을 평가하기에는 무리가 따라 품질평가를 위한 정량화 방안 마련을 위해 계층적 분석 방법(AHP 기법)을 이용하여 복잡한 다수의 평가요인을 범주화하며 가중치 정보를 마련하고 주특성 평가항목을 기능성, 성능성, 편의성으로 구분하여 공개용 안티바이러스 70여종에 대한 리얼 테스트 환경에서 품질평가를 수행하였다[9].

강득수 등은 국제표준인 ISO/IEC 9216과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 기능성, 신뢰성, 효율성, 사용성, 유지보수성, 이식성 6가지 항목으로 분류하고 ESM 소프트웨어의 시험평가 모델을 개발하여 성능시험을 진행함으로써 자원 효율성과 시간 효율성을 측정하는 방안을 모색하였다[10].

이완석은 IT인증사무국에 등록된 공통평가기준(Common Criteria) 인증 제품을 기준으로 각 제품의 보안목표명세서(Security Target)의 보안기능 요구사항을 기반으로 분석하여 안티바이러스 시스템에 대한 S-SLA(Security Service Level Agreement) 지표를 개발하였다. 시스템 등급은

A-D까지 총 4등급으로 분류하여 등급화하였다[11].

정혜정은 소프트웨어 품질 평가를 위해 국제 표준인 ISO/IEC 9126 평가 모델과 ISO/IEC 25023의 평가 모델에 대한 차이점을 비교, 분석하고 기능성, 신뢰성, 사용성, 유지보수성, 이식성, 효율성, 상호운영성, 보안성 등 8가지의 품질 특성 측면에서 평가 지표를 수립하고 융합 소프트웨어 331개를 분류하여 테스트하고 차이점을 분석하였다[12].

Dunham은 안티바이러스 평가시 비용, 시스템 요구사항, 인터페이스와 리더쉽, 성능, 스캔 옵션, 제거와 복구 옵션, 지원, 호환성 등이 중요한 요소라고 제시하였다[13].

Eddy Willems는 "The Antivirus Companies"에서 안티바이러스 테스트 표준 조직인 AMTSO(Anti-Malware Testing Standards Organization)를 소개하였는데 AMTSO는 안티바이러스 9가지 테스트 원칙을 제시하였다. 그 내용은 다음과 같다.

① 테스트는 대중을 위험에 빠뜨리지 않아야 한다.
② 테스트는 편파적이지 않아야 한다.
③ 테스트는 합리적으로 공개되고 투명해야 한다.
④ 안티바이러스 제품의 효과와 성능은 균형잡힌 방식으로 측정되어야 한다.
⑤ 테스트는 테스트 샘플 또는 테스트 사례가 악의적인지, 무해한지 또는 유효하지 않은지 정확하게 분류되었는지 확인하기 위해 주의를 기울여야 한다.
⑥ 테스트 방법론은 테스트 목적과 일치해야 한다.
⑦ 테스트의 결론은 테스트 결과를 기반으로 해야 한다.
⑧ 테스트 결과는 통계적으로 유효해야 한다.
⑨ 벤더, 테스터 및 퍼블리셔는 테스트 관련 내용을 주고받을 수 있는 유효한 연락처를 보유해야 한다.

이 9가지 원칙은 안티바이러스 테스트가 일관되고 유용하며 효율적임을 확인하기 위해 기본적으로 지켜져야 하며 이 기준을 모두 충족하는 테스트 제품의 경우 테스트 목표에 부합된다고 하였다[14].

III. 평가 기준 수립 및 검증

이전 연구들에서 제시한 품질평가 기준들은 일반 소프트웨어, 정보보호제품, ESM 소프트웨어 등에 대한 평가 방법으로 안티바이러스 제품 평가에는 부합되지 않는 평가 기준이 다수 존재하거나, 안티바이러스 평가 기준의 경우에도 보안 기능 위주의 평가기준으로 안티바이러스 성능에 대한 평가가 제대로 이루어지지 못하는 한계가 존재한다. 이런 안티바이러스 제품 평가에 부합되지 않고, 보안기능 위주의 평가 기준이 대다수인 기존 평가 방법을 개선하기 위하여 본 논문에서는 국내 "소프트웨어 기술성 평가 기준 지침", ISO/IEC 25010[15], ISO/IEC 25020[16], ISO/IEC 25023[17], ISO/IEC 25041[18] 및 각 안티바이러스 제품의 메뉴얼을 바탕으로 종합적으로 공통 평가항목 및 기능을 분류하고, 평가항목을 단순화하여 평가 기준을 수립하였다.

평가 기준은 악성코드 탐지, 속도 등 안티바이러스 성능을 평가하기 위한 ***기능성***, 시스템의 과도한 자원 사용을 확인하기 위한 자원 ***효율성***, 안티바이러스의 안정성을 평가하기 위한 ***신뢰성***, 전반적인 UI/UX와 편의성을 평가할 수 있는 ***사용성***, 추가적인 기능 제공을 평가하기 위한 ***부가 기능***, 업데이트 및 장애 지원을 확인하기 위한 ***공급업체 지원*** 등 크게 6가지로 구분하여 수립하였다.

평가에 대한 결과는 순서와 상관없이 안티바이러스의 제품명을 표기하지 않고 A-I로 표기하였다.

3.1 평가 기준 검증을 위한 환경

기존 성능테스트 기관들의 경우 테스트 환경을 공개하지 않거나 AV-Comparatives, Comparitech, Virus Bulletin, MRT Effitas 등과 같이 가상환경에서 테스트를 진행하여 가상환경을 인식하는 악성코드의 경우 테스트에서 제외하거나 탐지하지 못하는 문제가 존재한다. 또한 악성코드 샘플의 경우도 대부분의 성능테스트 기관이 1,000개 미만으로 테스트를 수행하고 가장 많은 악성코드 샘플로 테스트하는 AV-Comparatives도 약 10,000개의 악성코드 샘플로 테스트를 수행하는데 그치고 있다. 본 논문에서는 복원시점을 설정한 실제 PC를 이용하여 테스트를 진행함으로써 가상환경을 인식하는 악성코드도 테스트를 진행할 수 있으며 대량의 악성코드 샘플 테스트의 경우 약 20,000개를 이용하였으며 확장자별 악성코드 샘플 및 상용 패킹도구로 패킹된 악성코드를 이용하여 테스트함으로써 좀 더 다양한 악성코드에 대한 안티바이러스 성능테스트가 이루어질 수 있도록 평가 기준 검증 환경을 구축하였다.

수립한 평가 기준을 검증하기 위한 안티바이러스는 국내의 경우 V3, 알약 제품을 선정하고 국외에는 카스퍼스키, 노턴, 맥아피, 윈도우 디펜더 등 7종의

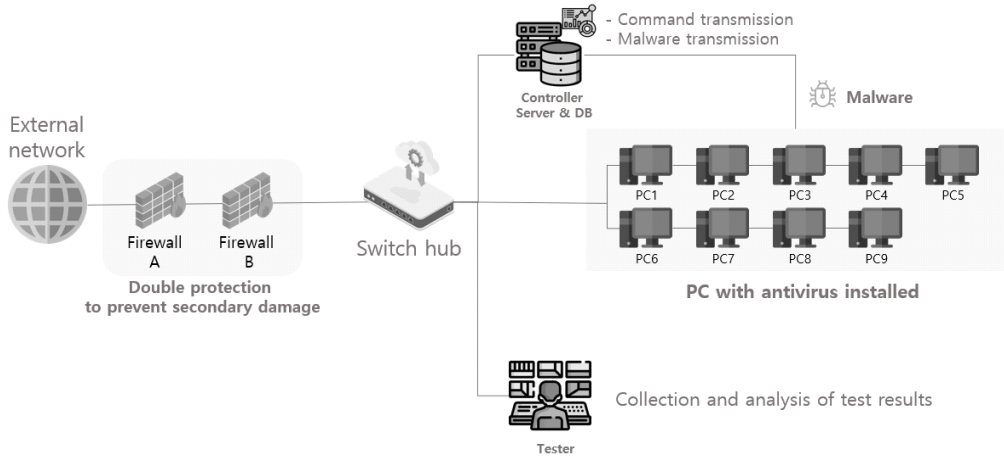

Fig. 1. Architecture of the test bed environment

제품을 선정하여 총 안티바이러스 9종의 제품을 선정하고 동일한 성능의 PC 9대에 제품을 설치하여 평가를 진행하였다. 안티바이러스 선정 기준은 다음과 같다[19][20].

- 국내 및 국외 시장 점유율이 높은 안티바이러스
- 고유한 엔진을 보유한 제품
- Windows 운영체제에 설치가 가능한 제품
- 비교 다양성을 위해 무료 안티바이러스 포함

성능 평가에 사용할 악성코드는 연구 목적으로 바이러스토탈[21]에서 제공 받은 대량의 악성코드, 공공기관, 보안기업, 자체 크롤링 시스템에서 유입된 악성코드, MalShare[22], VirusShare[23]와 같은 악성코드 DB 사이트에서 수집한 악성코드를 종합하여 유형, 출현시기, 특징 등을 고려하여 선별하였다. 또한 평가 시나리오에 따라 아래와 같은 총 6개의 악성코드 샘플로 구성해 각 시나리오에 맞는 샘플로 사용하였다[19][20].

- Exe, Pdf, Hwp 등 확장자 별로 분류된 악성코드 100개
- 랜덤 샘플링하여 선정한 대량의 악성코드 20,330개
- 공공기관 및 자체 크롤링 시스템에서 수집한 최근 3개월내 악성코드 151개
- 보안기업에서 제공한 분석된 악성코드 6,363개
- 상용 패킹 도구로 패킹된 악성코드 50개
- 악성 행위를 하는 실행 가능한 악성코드 25개

성능 평가를 진행할 테스트 베드는 Fig. 1.과 같이 2차 피해를 방지하기 위하여 이중으로 방화벽을 구성하였으며 평가 기준별 명령 수행 및 악성코드 배포를 자동으로 수행할 Controller와 Agent는 자체

Table 1. Version for each Anti-Virus

Anti-Virus	Version
ESTsecurity Alyac	5.1.22
Avast Premium Security	23,3,6058
Kaspersky Antivirus	21.3.10
McAfee Total Protection	16.6.161
MS Defender	4.18.2303
ESET Nod32 Antivirus	16.1.14
Norton Antivirus	22.23.3
TrendMicro Internet Security	17.7.1827
AhnLab V3 Internet Security	9.0

Table 2. Specifications of the PC used in the evaluation

	Specification
CPU	i5-12400
Graphics	On-board Intel UHD Graphics 730
Memory	16GB
Storage	SSD 500GB
OS	Windows 10 Pro (64bit)

개발하였다. 각 PC가 수행한 명령 및 다운로드된 파일에 대한 로그는 데이터베이스에 저장하여 추후 확인할 수 있도록 구성하였다[19][20].

성능평가에 사용된 각 PC의 사양은 Table 2.에서 보는 바와 같다.

3.2 평가 기준 및 검증

3.2.1 기능성

기능성 평가 항목은 정확성과 신속성을 평가하기 위한 항목으로 안티바이러스 제품이 악성코드를 제대로 탐지하고 얼마나 빠르게 동작하는지 평가하는 항목이다.

정확성의 대표적인 평가 기준은 악성코드 100개를 네트워크를 통하여 컴퓨터에 전송했을 때 안티바이러스 제품이 실시간으로 올바르게 악성코드로 탐지하는 것이 목적이다. 정확성은 70%이상 정확히 탐지하였을 경우 Good, 50%이상 70%미만일 경우 Average, 50% 미만일 경우 Bad로 평가하였다.

신속성의 경우에는 위에서 언급한 정확성 평가와 동일한 방식으로 테스트가 이루어지는데, 악성코드 100개를 네트워크로 전송시 안티바이러스 제품이 실시간으로 얼마나 빠르게 탐지하는 것이 목적이다. 신속성은 악성코드 수가 증가할수록 탐지시간이 오래걸리는 것을 감안하여 악성코드 200개 미만 평가시험의 경우 평균 탐지시간이 10초이내일 경우 Good, 10분 이내일 경우 Average, 10분 이상일 경우 Bad로 평가하였고, 자세한 신속성 평가 기준은 Appendix A에 자세히 표기하였다.

기능성 평가의 총 13개의 세부 평가 항목 중 A가 안티바이러스가 6개의 우수를 받아 가장 우수한 결과가 나왔다. 기능성에서 A의 가장 큰 장점은 빠른 탐지 속도에 있었다. E, F, G의 일부 항목은 실시간 탐지가 동작하지 않거나 탐지된 개수가 0인 이유로 인하여 탐지속도를 측정하지 못하거나 하여 테스트 결과에 반영하지 않았다.

기능성 관련 자세한 평가 항목은 Appendix B에서 찾아볼 수 있다.

Table 3. Overall Evaluation Table(Functionality)

	Good	Average	Bad
A	6	4	3
B	3	8	2
C	5	4	4
D	1	5	6
E	3	3	5
F	2	1	6
G	4	4	5
H	4	4	5
I	4	4	5

Table 4. Overall Evaluation Table(Resource Efficiency)

	Good	Average	Bad
A	4	4	
B	4	4	
C	2	5	1
D	4	4	
E	2	6	
F	2	6	
G	2	4	2
H	3	5	
I	1	7	

3.2.2 자원 효율성

자원 효율성 평가 항목은 안티바이러스가 악성코드 탐지시 시스템의 CPU 및 메모리의 자원을 얼마나 사용하는지를 평가하는 항목이다. 이 항목은 동일한 조건에서 CPU 및 메모리 사용률이 낮을수록 안티바이러스 성능이 좋다고 할 수 있다. CPU 사용률의 평가 기준은 일반검사시 CPU 사용 증가율이 0.2% 이내이면 Good, 1% 이내이면 Average, 1% 이상이면 Bad로 평가하였으며 메모리 사용률은 20% 이내이면 Good, 40% 이내이면 Average, 40% 이상이면 Bad로 평가하였다.

자원 효율성 평가 항목의 총 8개의 세부 평가 항목 중 A, B, D의 안티바이러스 제품이 우수 4개와 평균 4개를 받아 가장 좋은 결과를 얻었으며, 전체적으로 거의 모든 제품이 평균 이상의 결과를 보여주었다.

자원 효율성과 관련된 평가 항목은 Appendix C에 첨부하였다.

3.2.3 신뢰성

신뢰성 평가 항목은 시스템에 장애를 발생하지 않

Table 5. Overall Evaluation Table(Reliability)

	Good	Bad
A	1	
B	1	
C	1	
D	1	
E	1	
F	1	
G	1	
H	1	
I	1	

고 안티바이러스가 얼마나 안정적으로 동작하는지를 평가하는 항목이다.

단일 평가항목으로 A-I까지 모두 장애를 발생하지 않고 안정적으로 동작함을 보여주었다.

신뢰성에 대한 자세한 평가 항목은 Appendix D에서 볼 수 있다.

3.2.4 사용성

사용성 평가 항목은 사용자 학습 용이성, 인터페이스 조정 가능성, 입력데이터 지원, 진행상태 파악 용이성, 설치 환경 적합성, 설치제거 용이성, 보고서 생성, 사용자 정의 탐지/검사, 유/무료 여부 등으로 구분된다.

사용자 학습 용이성은 제품에 대한 다양한 언어를 제공하고 변경할 수 있는지 또한 외부연결 없이 제품 내에서 사용자 메뉴얼을 제공하는지에 대해 평가하고 인터페이스 조정 가능성은 사용자가 자신에게 맞은 메뉴 선택과 화면 배치 등을 변경할 수 있는지에 대해 평가하며 입력데이터 지원 항목은 간편 및 정밀 검사에서 다양한 검사 대상을 지정할 수 있는지를 평가한다.

Table 6. Overall Evaluation Table(Usability)

	Good	Average	Bad
A	7	3	3
B	7	2	4
C	7	1	5
D	10	1	2
E	9	2	2
F	6	2	5
G	4	2	7
H	9	1	3
I	7	2	4

Table 7. Overall Evaluation Table(Add-Ons)

	Good	Average	Bad
A	16		3
B	15	2	2
C	15	1	3
D	13		6
E	11	2	6
F	10		6
G	4	2	13
H	12		7
I	8	1	10

설치 환경 적합성 및 설치제거 용이성은 다양한 OS에 설치가 가능하고 제거가 쉬우며 불필요한 외부 프로그램 설치를 권유하지 않는지를 평가한다.

보고서 생성 항목은 탐지 및 치료 결과에 대해 보고서 생성 유무 및 다양한 포맷으로 제공하는지를 평가하며 사용자 정의 탐지/검사 항목은 탐지/검사시 특정 조건을 제외하고 검사할 수 있는지에 대해 평가한다.

마지막으로 유/무료 여부는 안티바이러스에 대한 무료 버전을 제공하여 사용자가 구입전 미리 사용해 볼 수 있도록 하여 불필요한 구입이 발생하지 않는지 여부를 판단한다.

사용성은 총 13개의 세부항목이 있으며 안티바이러스 D가 가장 우수한 결과를 얻었다. D의 경우 다양한 검사 대상 지정 및 언어를 제공하고 있었으며

Table 8. Overall Evaluation Table(Support from the Vendor)

	Good	Bad
A	4	
B	4	
C	4	
D	4	
E	4	
F	4	
G	4	
H	4	
I	4	

총 5가지의 OS(Windows, Linux, Mac, Android, iOS) 설치를 지원하였다.

사용성에 대한 자세한 평가 항목은 Appendix E에 첨부하였다.

3.2.5 부가 기능

부가 기능은 악성코드 탐지 및 치료 이외에 네트워크 보안, 시스템 보안, 개인정보 보호 등 기본 보안 기능 이외의 기능을 제공하는지 평가하는 항목이다.

부가 기능은 총 19개의 세부 평가 항목이 있으며 안티바이러스 A, B, C의 제품이 우수한 결과를 나타냈다. 이 제품들은 AMSI(AntiMalware Scan Interface), 방화벽 설정, 랜섬웨어 탐지, 레지스트리 정리 등의 부가적인 보안 기능을 제공하고 있다.

부가 기능에 대한 자세한 평가 항목은 Appendix F에 첨부하였다.

3.2.6 공급업체 지원

공급업체 지원 항목은 안티바이러스 제품에 대해 주기적인 업데이트가 이루어지고 사용자가 주기를 설정할 수 있으며 안티바이러스에 문제가 발생했을 때 업체의 지원을 받을 수 있는지를 평가하는 항목이다.

A부터 I까지 모든 안티바이러스의 업체들이 적절한 지원을 제공하고 있었다.

공급업체 지원에 대한 자세한 평가 항목은 Appendix G에 첨부하였다.

IV. 결 론

본 논문에서는 기존 품질평가 기준의 불필요한 항목을 제거/개선 및 단순화하여 기능성, 자원효율성, 신뢰성, 사용성, 부가기능, 공급업체 지원 등 크게 6가지 평가항목으로 분류하고, 각각의 세부적인 평가 기준을 수립하여 최신 안티바이러스 제품 평가를 위한 객관적이고 정량적인 기준을 제시하였다. 이렇게 제시한 기준을 토대로 실제 안티바이러스 제품의 품질평가를 위한 환경을 구축한 후 국내외 안티바이러스 9종을 대상으로 평가함으로써 평가기준 및 세부 평가 항목에 대한 유효성을 검증함과 동시에 여러 안티바이러스의 기능 및 성능에 대한 상대적 우열을 검증할 수 있었다.

향후 연구에서는 수립된 평가 기준을 바탕으로 주기적으로 새로운 안티바이러스 제품을 평가함으로써 미흡한 부분을 도출하고 보완하며 신속성 평가시 탐지된 파일만을 대상으로 평가하여 신속성 평가에 대한 신뢰도를 향상하고 관리서버에 대부분의 기능이 들어가 있는 기업용 버전에 대한 평가도 포함하여 평가 기준을 고도화할 예정이며, 더 나아가 윈도우 안티바이러스 제품의 평가 기준 및 항목을 벤치마킹하여 모바일 안티바이러스 기능 및 성능 검증 연구로 확장할 예정이다.

〈Appendix〉

A. Evaluation Criteria

Evaluation Items			Good	Average	Bad
Detection Accuracy			70%〈=	40%〈=, 〈70%	〈40%
Detection Speed	Number of Malwares	〈 200	〈=10sec.	10sec.〈, 〈=10min.	10min.〈
		6,363	〈=1min.	1min.〈, 〈=30min.	30min.〈
		20,330	〈=10min.	10min.〈, 〈=30min.	30min.〈
		20,330(USB)	〈=1hour	1hour〈, 〈=6hour	6hour〈
CPU Usage	Scan Method	Manual Scan	0.2%〈=	0.2%〈=, 〈1%	〈1%
		Real-time Detection	1%〈=	1%〈=, 〈10%	〈10%
		Deep Scan	10%〈=	10%〈=, 〈30%	〈30%
Memory Usage			〉=20%	20%〈, 〈=40%	40%〈

B. Evaluation Area 1: Functionality

Area	Item	Criteria
Functionality	Accuracy	(1) Real-time detection accuracy on a single, individually sent (per piece) for total 100 malwares.
		(1)-1 Detection accuracy for Decompressing 100 malwares
		(2) Detection accuracy with 25 malwares executions
		(3) Detection accuracy for USBs containing a large number of malwares (20,330)
		(4) Real-time detection accuracy for decompressing a large number of malwares (20,330)
		(5) 151 malwares detection accuracy for the latest malware (within three months)
		(6) Detection accuracy of analyzed malwares (6,363)
		(7) Detection accuracy of 50 packed malwares
		(7)-1 Detection accuracy for 50 unpacked malwares
	Time Efficiency	(8) Average rate of real-time detection speed on a single, individually sent (per piece) for total 100 malwares
		(9) Average rate of detection speed for USBs containing a large number of malwares (20,330)
		(10) Average rate of detection speed for decompressing a large number of malwares (20,330)
		(11) Average rate of 151 malwares detection speed for the latest malwares (within three months)
		(12) Average rate of detection speed of analyzed malwares (6,363)
		(13) Average rate of detection speed of packed malwares

C. Evaluation Area 2: Resource Efficiency

Area	Item	Criteria
Resource Efficiency	#1 CPU Usage	(14) Average CPU usage before evaluation item (1) on a PC with the same conditions
	#1 Memory Usage	(15) Average Memory usage before evaluation item (1) on a PC with the same conditions
	#2 CPU Usage	(16) Average CPU usage before evaluation item (3) on a PC with the same conditions
	#2 Memory Usage	(17) Average Memory usage before evaluation item (3) on a PC with the same conditions
	CPU Usage on Real-time Detection	(18) Real-time CPU usage when evaluating item (1)
	Memory Usage on Real-time Detection	(19) Real-time memory usage when evaluating item (1)
	CPU Usage on Deep Scan	(20) CPU usage when evaluation item (3) on a PC with the same conditions
	Memory Usage on Deep Scan	(21) Memory usage when evaluation item (3) on a PC with the same conditions

D. Evaluation Area 3: Reliability

Area	Item	Criteria
Reliability	Operational Safety	(22) Did the antivirus cause any failures after installation?

E. Evaluation Area 4: Usability

Area	Item	Criteria
Usability	Usability of User Learning	(23) Possibility to change other languages while using the product?
		(24) How many languages does the antivirus offer?
		(25) Does the antivirus provide help service inside the software except by linking the website?
	Interface Adjustability	(26) Possible to modify the menu and structure to the user's desire?
	Input Data Support	(27) How many ways to specify the target to scan for in a quick and deep scan? (e.g., email files, other folders, compressed files, etc.)
	Easily Track Progress	(28) Does the antivirus provide a UI/UX to understand the current progress of the tasks being performed?
	Installation Environment Suitability	(29) What types of operating system environments are available (Windows/Linux/Unix/Mac/Android/iOS)?
		(30) Does it encourage the installation of external programs?
	Usability of Uninstallation	(31) Does the product uninstall correctly?
	Generate reports	(32) Possible to generate reports on detection and quarantine results?
		(33) How many formats can be generated as reports?
	User-Defined Detection/Inspection	(34) Possible to exclude certain conditions (folder, filename, extension, detection name, etc.) from detection and scanning?
	Free or not	(35) Is there a free version of the antivirus product?

F. Evaluation Area 5: Add-Ons

Area	Item	Criteria
Add-Ons	Real-time Detection	(36) Possible to specify a location (entire system, specific folder, etc.) for real-time detection?
		(37) Does it have Antimalware Scan Interface (ASMI)* capabilities? * Detects obfuscated scripts such as JavaScript, VBScript, Powershell, etc.
		(38) Possible to set actions (quarantine and delete) for detected malware after real-time detection?
	Manual Scanning	(39) How many manual scanning methods does the antivirus offer?
		(40) Possible to specify a location (file, drive, specific folder, etc.) to scan during a manual scan?
		(41) Possible to scan for specific malicious behavior (Anti Rootkit, process, memory)?
		(42) Does it have a scheduling inspection feature?
	Network Security	(43) Possible to set up a firewall within the antivirus?
		(44) Possible to block harmful sites or manage custom sites?
		(45) Possible to prevent or detect specific network-based intrusions (spoofing, remote, etc.)?
		(46) Does it have a VPN or proxy?
	System Security	(47) Possible to look up a history of recently created files?
		(48) Does it have ransomware-specific detection or blocking capabilities?
		(49) Possible to access to storage media (USB, external hard, CD/DVD, etc.)?
		(50) Does it have a registry cleanup feature?
	Privacy Protection	(51) Does it have the ability to delete temporary files?
		(52) Possible to delete my browsing history?
		(53) Possible to delete traces of the user (recently opened files, list of running documents, etc.)?
		(54) Possible to completely erase files from recovery (BCWipe, CCleaner, etc.)?

G. Evaluation Area 6: Support from the Vendor

Area	Item	Criteria
Support from the Vendor	Maintenance	(55) Are there regular product updates and feature additions?
	Set Update Frequency	(56) Possible to update the engine automatically, manually, or on demand?
	Troubleshooting and Support	(57) Does it have a Q&A or FAQ on its website or within its antivirus product?
		(58) Does it have such a quick contacting service system (such as a chatbot)?

References

[1] ICSA Labs, https://www.icsalabs.com/products, accessed Oct. 2022.

[2] Comparitech, https://www.comparitech.com/antivirus/, accessed Feb. 2023.

[3] AV-Comparatives, https://www.av-comparatives.org/consumer/test-methods/, accessed May. 2023.

[4] AV-TEST, https://www.av-test.org/en/antivirus/, accessed Jan. 2023.

[5] Virus Bulletin, https://www.virusbulletin.com/testing/, accessed Jan. 2023.

[6] MRT effitas, https://www.mrg-effitas.com/test-library/, accessed Dec. 2022.

[7] SE Labs, https://www.selabs.uk/security-vendors/, accessed Oct. 2022.

[8] Yeo-Wung Yun and Sang-Ho LEE, "A study on the quality model and metrics for evaluating the quality of information security products," Journal of Korea Institute of Information Security & Cryptology, 19(5), pp.134-135, Oct. 2009.

[9] Doo-lyel Maeng, Jong-kae Park and Sung-joo Kim, "A study on quality evaluation methodology establishment of anti-virus software based on the real test environment," The Journal of Korean Institute of Communications and Information Sciences, 35(3B), pp. 450-451, Mar. 2010.

[10] Deuk-Soo Kang and Hae-Sool Yang, "Evaluation items of ESM S/W by case analysis," The Journal of the Korea Contents Association, 10(8), pp.87-89, Aug. 2010.

[11] Wan-Suck Yi, Dong-Bum Lee, Dongho Won and Jin Kwak, "Development of S-SLA based on the analyses of security functions for anti-virus system," Journal of The Korea Institute of Information Security and Cryptology, 20(6), pp.240-245, Dec. 2010.

[12] Jung Hye Jung, "The software quality testing on the basis of the international standard ISO/IEC 25023," Journal of the Korea Convergence Society, 7(6), pp.38-40, Jul. 2016.

[13] Dunham, "Evaluating anti-virus software : which is best," Telecommunication and Network Securit, vol. 12, no. 3, pp.19-21, Dec. 2006.

[14] Eddy Willems, The antivirus companies, Springer Nature, pp.77-78, May. 2019.

[15] "Systems and software engineering: systems and software quality requirements and evaluation - system and software quality models," ISO/IEC 25010, Mar. 2011.

[16] "Systems and software engineering: systems and software quality requirements and evaluation - quality measurement framework," ISO/IEC 25020, Jul. 2019.

[17] "Systems and software engineering: systems and software quality requirements and evaluation - measurement of system and software product quality," ISO/IEC 25023, Jun. 2016.

[18] "Systems and software engineering: systems and software quality requirements and evaluation - evaluation guide for developers, acquirers and independent evaluators," ISO/IEC 25041, Oct. 2012.

[19] KAIST CSRC, "Antivirus function and performance analysis", https://csrc.kaist.ac.kr/blog/2023/03/27/%ec%95%88%ed%8b%b0%eb%b0%94%ec%9d%b4%eb%9f%ac%ec%8a%a4-%ea%b8%b0%eb%8a%a5-%eb%b0%8f-%ec%84%b1%eb%8a%a5-%eb%b6%84%ec%84%9d-2%eb%b6%80/, accessed Mar. 27. 2023.

[20] "Antivirus performance testing: why is it necessary and what are its limitations?", Boan News, Apr. 17. 2023., http

s://www.boannews.com/media/view.asp?idx=117042
〔21〕 VirusTotal, https://www.virustotal.com, accessed Jun. 2023.
〔22〕 MalShare, https://www.malshare.com, accessed Jun. 2023.
〔23〕 VirusShare, https://www.virusshare.com, accessed Jun. 2023.

〈저자소개〉

이 정 호 (Jeongho Lee) 정회원
2002년: 한남대학교 컴퓨터공학과 학사
2004년: 경희대학교 정보통신대학원 통신망관리공학과 석사
2017년~현재: 한국과학기술원 사이버보안연구센터 선임연구원
〈관심분야〉 웹보안, 시스템보안, 악성코드 분석

신 강 식 (Kangsik Shin) 정회원
2016년 2월: 충남대학교 컴퓨터공학과 학사
2018년 2월: 충남대학교 컴퓨터공학과 석사
2020년~현재: 한국과학기술원 사이버보안연구센터 연구원
〈관심분야〉 악성코드 분석, 사이버보안, 딥러닝 보안

유 영 락 (Youngrak Ryu) 정회원
2011년: 한밭대학교 컴퓨터공학과 학사
2021년: Technische Universität Berlin Computer Science 베를린공대 컴퓨터 사이언스 석사
2022년~현재: 한국과학기술원 사이버보안연구센터 연구원
〈관심분야〉 사이버보안, 악성코드 분석, 난독화

정 동 재 (Dong-Jae Jung) 종신회원
2011년: 아주대학교 정보 및 컴퓨터공학부
2013년: 한국과학기술원 정보보호대학원 석사
2020년: 한국과학기술원 정보보호대학원 박사
2020년~현재: 한국과학기술원 사이버보안연구센터 선임연구원
〈관심분야〉 악성코드 분석, 시스템보안, 흐름 분석

조 호 묵 (Ho-Mook Cho) 종신회원
2006년: 아주대학교 정보통신공학과 정보보호학 (공학석사)
2018년: 전남대학교 정보보안협동과정 (이학박사)
2014년~현재: 한국과학기술원 사이버보안연구센터 책임연구원/실장
〈관심분야〉 사이버보안, 악성코드 분석, XAI 보안