네트워크접근제어(NAC) 제품의 신뢰성 평가 모델

강상원*, 전인오**, 양해술**
*호서대학교 혁신기술경영융합대학원
**호서대학교 벤처전문대학원
e-mail:myksangwon@paran.com, hsyang@office.hoseo.ac.kr

Reliability Evaluate Model of Network Access Control (NAC) Product

Sang-Won Kang*, In-Oh Jeon**, Hae-Sool Ynag*
*Graduate School of Multidisciplinary Technology and Management, Hoseo Univ
**Graduate School of Venture, Hoseo Univ

요 약

인터넷의 대중화 이후에 불어온 방화벽시스템의 바람은 정보보안 솔루션의 보통명사처럼 여겨질 정도로 국내 시장에서 확실히 자리를 잡고 있다. 인터넷을 확장시켜 편리함을 추구할 수 있는 모든 종류의 것들을 향유하기 위해서는 즉, 정보화 사회를 제대로 구현하기 위해서는 정보보안이라는 파수꾼의 역할이 매우 중요한 것이다. 본 연구에서는 네트워크접근제어(NAC) 시스템에 대해 특성과 기술 요수를 분석하고 이를 바탕으로 네트워크접근제어 시스템 제품의 신뢰성 품질평가 모델을 개발하였다.

1. 서론

국내의 암호화 기술은 기술선진국에 비해 상당히 낙후되어 있는 편이다. 이와 같은 이유로 암호화라는 것이 발달할 수 있던 배경은 군사적 목적에 의해 발전시켜온 것이 대부분이기 때문이다.

그러나 국내의 정보보안 시스템에 대해 그다지 큰 우려를 해야만 하는 상황은 아니다. 최근 정부의 정보화 육성책에 의해 한국인터넷진흥원, 한국정보화진흥원 등의 기관에서 암호화, 보안 시스템에 대한 기술연구와 인증절차 등이 진행 중이며 국내 순수기술로 만들어진 방화벽시스템의 인기가 갈수록 상승되고 있는 상황이기 때문이다.

이상과 같이 정보보안 제품의 시장이 지속적으로 성장할 것으로 예상되는 시점에서 이에 따른 지식정보보안 제품의 품질평가 요구에 대응이 필요하다.

본 연구에서는 정보보안 제품 중 네트워크접근제어(NAC-Netwok Access Control) 시스템의 신뢰성 품질평가에 대해 연구를 하였다. 본 연구는 네트워크접근제어 시스템 제품의 기반기술을 조사하고 관련 제품의 기술, 표준과 소프트웨어 관련 품질평가 동향을 조사하여 네트워크접근제어(NAC) 시스템 제품의 신뢰성 품질 평가모델을 개발하였다.

2. 네트워크접근제어 시스템 특징

2.1 경계선 보안

네트워크 환경에서는 소위 경계선이라는 것이 있었다. 현재의 네트워크 환경에서 외부 사용자 혹은 외부 데이터(유해데이터, 바이러스, 웜 등)가 내부로 들어올 수 있는 경로는 많다. 무선의 사용이 증가했고, 노트북 이용자가 늘었으며 여기에 이동형 저장장치(USB 등)사용과 IP를 가진 단말기의 종류가 증가하고 있다. 경계선을 침입할 수 있는 새로운 기술들이 늘어나고 있어 이에 보안할 수 있는 기술들이 개발되고 있다.

2.2 인증

NAC(Network Access Control)를 우리말로 번역하면 네트워크 접근제어로서 NAC가 접근제어를 위

하여 사용하는 방법은 인증이다. 사용자에 대한 인증, 단말에 대한 인증, 트래픽에 대한 인증을 NAC가 수행하게 된다.

2.3 사용자 인증 및 단말 인증

NAC 솔루션은 항시 네트워크를 감시하고 있다. 이 과정에서 무언가 새로운 단말이 네트워크로 진입하게 되면 이를 감지하고 우선적으로 사용을 차단하게 된다. 그리고는 접근하려는 사용자에게 인증을 요청한다. 인증을 수행하는 방법은 주로 내부에 존재하는 인증 DB에 있는 사번과 해당 비밀번호를 입력해야 한다.

3. 네트워크접근제어 시스템 기술

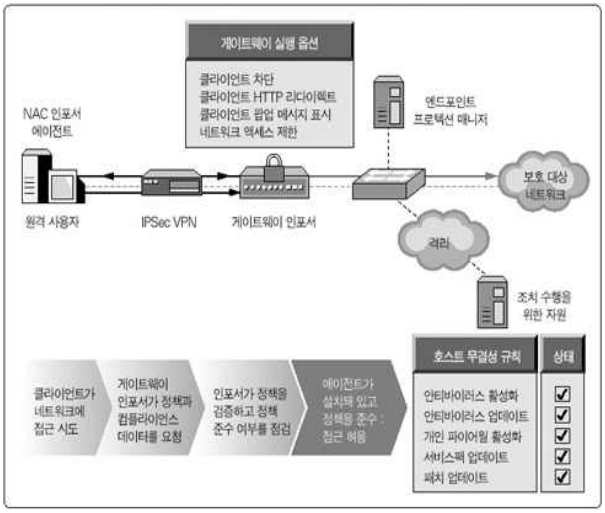
3.2 DHCP 인포서

DHCP 인포서는 기본적으로 인라인 DHCP 프록시(in-line DHCP proxy)로 동작하므로, 기존 DHCP 인프라스트럭처와 호환된다. 또한 별도의 하드웨어/소프트웨어 업그레이드가 불필요하다. DHCP 인포서 어플라이언스의 대안으로, 마이크로소프트 DHCP 서버에 직접 설치할 수 있는 DHCP 인포서 플러그인을 제공하기도 한다. DHCP 인포서 플러그인을 사용할 경우에는 마이크로소프트 DHCP 서버가 정책 실행 포인트의 역할을 담당하게 된다.

3.1 게이트웨이 인포서

게이트웨이 인포서는 네트워크 경계 지점에 설치되는 어플라이언스 장비로, 원격 엔드포인트의 정책 준수 여부를 기준으로 트래픽 흐름을 통제 또는 차단 한다. 여기서 '경계 지점'이란 WAN 링크, VPN과 같은 네트워크 진입 지점일 수도 잇고, 핵심 비즈니스 시스템이 운영되는 네트워크 부분일 수도 있다. 게이트웨이 인포서는 자원에 대한 접근을 효과적으로 통제하고, 정책을 준수하지 않는 엔드포인트를 정책 준수 상태로 되돌리기 위한 조치를 자동으로 수행한다.

게이트웨이 인포서는 일반적으로 원격 지사 사무실과 본사를 연결하는 IPSec VPN, WAN 연결, 또는 컨퍼런스 룸의 무선 네트워크, 중요 서버 시스템이 설치된 네트워크, 소규모 데이터 센터의 경계 지점 등에 설치된다.



[그림 1] 게이트웨이 인포서 흐름

4. 네트워크접근제어 신뢰성 평가방법

신뢰성이란 명세된 조건에서 사용될 때, 성능 수준을 유지할 수 있는 제품의 능력을 의미한다. 신뢰성은 성숙성, 오류허용성, 회복성, 준수성 등의 품질 부특성으로 세분화된다.

4.1 성숙성 평가항목

성숙성이란 제품 내의 결함으로 인한 장애를 피해가는 제품의 능력을 의미한다. 성숙성은 문제 해결률, 결함 회피율, 결함발생 평균시간 등의 평가항목을 가진다.

[표 1] 성숙성 평가항목

부특성	평가 항목명	평가항목의 목적
성숙성	문제 해결률	이전 버전의 네트워크접근제어시스템에 존재하던 문제에 대하여 명시적으로 해결이 확인되는 정도를 평가
	결함 회피율	일정한 운용 시간 내에 결함이 발생하지 않는 정도를 평가
	결함발생 평균시간	네트워크접근제어 시스템의 결함발생 평균시간(MTBF)를 평가

4.2 오류허용성 평가항목

오류허용성이란 명세된 인터페이스의 위반 또는 제품 결함이 발생했을 때 명세된 성능 수준을 유지할 수 있는 제품의 능력을 의미한다. 오류허용성은 다운 회피율, 장애 회피율 등의 평가항목을 가진다.

[표 2] 오류허용성 평가항목

부특성	평가 항목명	평가항목의 목적
결함 허용성	다운 회피율	발생되는 결함 중 시스템 다운을 가져오는 결함이 발생하지 않는 정도
결함 허용성	장애 회피율	발생되는 결함 중 장애를 발생시키는 정도의 심각한 결함이 발생하지 않는 정도

4.3 회복성 평가항목

회복성이란 장애 발생시 명세된 성능 수준을 회복하고 직접적으로 영향 받은 데이터를 복구하는 제품의 능력을 의미한다. 회복성은 데이터 복구율, 복구 가능률, 복구 효과율, 문제 해결 구현율 등의 평가항목을 가진다.

[표 3] 회복성 평가항목

부특성	평가 항목명	평가항목의 목적
회복성	데이터 복구율	결함이 발생할 경우에 데이터가 복구되는 정도
회복성	이용 가능률	일정 시간 사용중에 시스템이 다운이나 기타 이유로 인하여 사용할 수 없는 기간을 평가
회복성	평균 복구 시간	시스템에 결함이 발생되었을 경우 복구가 시작되어 완료되기까지 소요되는 복구 평균 시간을 평가
회복성	복구 가능률	제품에 결함이 발생되었을 경우 복구 할 수 있는 가능성 정도
회복성	복구 효과율	제품에 결함이 발생되었을 경우 목표 시간내에 복구하는 능력의 정도

4.4 준수성 평가항목

준수성이란 신뢰성과 관련된 표준, 관례 또는 규제를 고수하는 제품의 능력을 의미한다. 준수성은 신뢰성 표준 준수율의 평가항목을 가진다.

[표 4] 준수성 평가항목

부특성	평가 항목명	평가항목의 목적
준수성	신뢰성 표준 준수율	네트워크접근제어 시스템의 신뢰성 표준에 따라 시스템이 구현되어 있는지 평가

5. 네트워크접근제어 품질 점검표

본 장에서는 앞에서 네트워크접근제어 평가항목에 맞게 점검할 수 있는 점검표를 제시하였다.

[표 5] 문제해결률 점검표

측정 항목	A	시험 대상 문제 해결 항목수
		- 버그 레포트를 검토하여 시험 대상을 결정하고 테스트 케이스를 작성
	B	문제 해결이 확인된 항목수
		- 테스트케이스를 시험하여 문제가 해결되었는가를 검토
계산식	문제해결률 = B/A	
결과 영역	0 ≤ 문제해결률 ≤ 1	결과값

위 [표 5]는 문제 해결률의 점검표로 이전 버전의 시스템에 존재하던 문제에 대하여 명시적으로 해결이 확인되는 정도를 점검한다.

[표 6] 결함 회피율 점검표

측정 항목	A	단위 운용시간
	B	발견된 결함 수
		- 운용 시간 중 발견된 결함의 수를 측정
계산식	결함 회피율 = 1- min(1, B/A)	
결과 영역	0 ≤ 결함 회피율 ≤ 1	결과값

위 [표 6]은 결함 회피율 점검표로 일정한 운용시간내에 결함이 발생하지 않은 정도에 대해 점검한다.

[표 7] 결함발생 평균시간 점검표

측정 항목	A	결함발생 평균시간의 한계값
	B	(운용시간/결함수)
계산식	결함발생 평균시간 = min(1, B/A)	
결과 영역	0 ≤ 결함발생 평균시간 ≤ 1	결과값

위 [표 7]은 결함 발생 평균시간 점검표로 결함이

발생한 시간 간격의 평균의 정도를 점검한다.

[표 8] 오류허용성 점검표

측정 항목	A	발견된 결함수
		- 운용 중 발견된 결함의 수를 측정 - 결함에 대한 명확한 정의가 필요
	B	다운 회수
		- 전체 시스템의 다운이 발생하는 경우의 수를 측정
계산식	다운회피율 = 1- B/A.	
결과 영역	0 ≤ 다운회피율 ≤ 1	결과값

위 [표 8]은 오류허용성 점검표로 발생되는 결함 중 전체 시스템의 다운을 가져오는 결함의 발생은 어느 정도인지를 점검한다.

[표 9] 장애 회피율 점검표

측정 항목	A	발견된 결함수
		- 운영 중 발견된 결함의 수 - 결함에 대한 명확한 정의가 필요
	B	장애 발생 회수(심각한 결함이 발생한 수)
		- 심각한 결함이 발생한 경우의 수를 측정 - 심각한 결함에 대한 정의가 필요
계산식	장애 회피율 = 1- B/A	
결과 영역	0 ≤ 장애 회피율 ≤ 1	결과값
문제점		

위 [표 9]는 장애 회피율 점검표로 장애를 발생시키는 정도의 심각한 결함은 전체 결함 중 어느 정도 발생되는 지를 점검한다.

[표 10] 데이터 복구율 점검표

측정 항목	A	데이터관련 오류 발생 수
		- 데이터의 망실, 손실, 잘못된 변경 등에 대한 발생 수를 측정
	B	성공적으로 데이터가 회복된 경우의 수
		- 데이터 회복을 시도하여 오류 이전의 상태로 회복된 경우의 수를 측정
계산식	데이터회복률 = B/A	
결과 영역	0 ≤ 데이터회복률 ≤ 1	결과값

위 [표 10] 데이터 복구율 점검표는 결함이 발생한 경우에 데이터 회복은 어느 정도인지를 점검한다.

6. 결 론

현재 보안장비는 날로 새로운 제품이 쏟아져 아노는 시점이다. 그러나 정작 이런 장비들을 질적인 면에서 품질을 고려하는 노력이 미흡하다. 따라서 본 연구에서는 보안장비 중 네트워크접근제어(NAC) 시스템 제품의 질적인 면에서 신뢰성을 평가하여 품질 수준을 파악하였다. 이를 통해 개선방향을 도출함으로써 품질향상을 지원할 수 있는 네트워크접근제어(NAC) 시스템 제품의 신뢰성 평가모델을 개발하기 위해 제품의 동향 및 기술적인 요소들을 조사 분석하였다.

본 연구가 네트워크접근제어(NAC) 제품의 품질 향상에 조금이나마 기여 할 수 있기를 바라며, 향후 연구에는 도출된 평가방법론에 대한 검증이 미흡한 부분이 있어, 지속적인 시험 평가방법을 통해 어려 사례를 축적함으로써 평가방법론에 대한 타당성을 제고하는 연구가 이루어져야 하겠다.

참고문헌

[1] ISO/IEC 9126, “Information Technology - Software Quality Characteris- tics and metrics - Part 1, 2, 3″

[2] ISO/IEC 14598, ″Information Technology - Software product evaluation - Part 1, 2, 3, 4, 5, 6″

[3] ISO/IEC 12119, ″Information Technology - Software Package - Quality requirement and testing″.

[4] S.E.Coull, M.P.Collins, C.V.Wright and F.Monrose, M.K.Reiter, ″On Web Browsing Privacy in Anonymized NetFlows″, 16Tth USENIX Security Symposium, 2007. 8.

[5] Gyoo-Yeong Jeong, Jeong-Ho Kim, ″Intranet Security Evaluation Using Hacking Techniques″, Vol 1, pp.162~182, 9th International Conference on Advanced Communication Technology, 2007. 2.

[6] 김동진, “기업환경의 내부보안을 위한 통합 보안관리 시스템의 설계 및 구현”, 창원대학교, 2008.

[7] 한국정보통신기술협회, “소프트웨어 테스트 전문기술”, 기초과정편, TTA, 소프트웨어시험인증센터, 2006.

[8] 한국정보통신기술협회, “소프트웨어 테스트 전문기술”, 응용과정편, TTA, 소프트웨어시험인증센터, 2006.