http://dx.doi.org/10.14400/JDC.2014.12.9.159

NAC 시스템의 시험방법과 평가사례에 관한 연구

양효식*, 전인오**
호서대학교 벤처전문대학원 융합공학과*, 호서대학교 벤처전문대학원 정보경영학과**

A Study the Test Methods and Evaluation Practices of Network Access Control System

Hyo-Sik Yang*, In-Oh Jeon**
Dept. of Fusion Engineering, Graduate School of Venture, Hoseo University*
Dept. of Information Management, Graduate School of Venture, Hoseo University**

요 약 인터넷과 이동통신 기기의 발전으로 인해 개인의 경제활동에 관련된 인터넷뱅킹, 인터넷대출, 스마트폰등과 같은 이동통신기기를 이용한 모바일 뱅킹이 활성화되고 있다. 이에 따라 신종 범죄를 막기 위해 보안 시스템들이 새롭게 선보이고 있으며, 앞으로 보안 시스템의 시장은 날로 늘어날 것으로 보고 이에 따른 보안 시스템들에 대한 질적인 발전이 지속적으로 요구되고 있다. 따라서 보안시스템 제품의 시장이 지속적으로 성장할 것으로 예상되는 시점에서 보안 시스템의 품질평가 요구에 대응하기 위해 본 논문에서는 보안 시스템중의 네트워크 접근제어시스템 분야의 기반기술과 표준을 조사하고, 동향을 분석하여 관련 시스템의 시험과 평가방법을 제안하여 네트워크 접근제어시스템의 품질평가 방법과 체계를 제안하였다.

주제어 : 네트워크 접근제어시스템, 보안시스템, 평가방법, 품질평가

Abstract With the advancement of internet and mobile communication devices, mobile banking such as internet banking, internet loan and smart phones related to the people's economic activities using mobile communication devices is becoming increasingly more popular. Various security systems to prevent such new crimes are being introduced and the security system market is anticipated to continuously increase substantially in the future. Accordingly, qualitative advancement of the security systems are also in continuous demand. Therefore, this thesis proposes the method and system for quality evaluation of the network access control system by proposing testing and evaluating method for the relevant system through surveying and analyzing the tend in the foundation technologies and standards in the area of network access control system, which is one of the security systems, in order to cope with the demands for the evaluation of the quality of the security system as the security system product market is anticipated to grow continuously.

Key Words : Network Access Control System, Security System, Evaluation Methods, Quality Evaluation

Received 7 July 2014, Revised 18 August 2014
Accepted 20 September 2014
Corresponding Author: In-Oh Jeon(Graduate School of Venture, Hoseo University)
Email: eric@hoseo.edu

ISSN: 1738-1916

1. 서론

보안시스템 제품은 양적으로 빠른 성장세를 보이고 있으나, 그 동안 질적인 성장과 품질을 높이기 위한 노력이 미흡한 것으로 나타나고 있다.

일반적으로 보안시스템은 웹 방화벽시스템, 가상사설망시스템, 기업정보보안시스템, 네트워크 접근제어시스템으로 크게 4가지로 구분되어 있다. 본 논문에서는 보안시스템 중 IT 인프라 관리, BYOD (Bring your own device), 클라우드 등 다양한 IT 환경에서 안전하게 이용할 수 있도록 하는 네트워크 접근제어시스템을 선택하여 제품의 질적인 면을 평가하고 품질 수준을 파악하여 개선방향을 도출함으로써 네트워크 접근제어시스템의 품질향상을 지원할 수 있는 평가모델을 개발하고자 한다.

본 논문에서는 네트워크 접근제어시스템 제품의 동향 및 기술적인 요소들을 조사 분석하고, 평가방법론 구축의 기본이 되는 국제표준의 최신동향을 분석하였다. 또한 네트워크 접근제어시스템 제품의 특성을 고려하여 각 제품별 일반 품질 요구사항으로 커버되는 품질 요소와 네트워크 접근제어시스템 제품의 고유한 품질 요구사항을 도출하고 분류하여 분석함으로써 품질 항목 중 보안성 및 보안성능이 네트워크 접근제어시스템 제품의 품질평가에서 비중 있게 다루어질 필요성을 제안하였다.

본 논문의 2장에서는 네트워크 접근제어시스템 품질평가 모델을 개발하기 위해 제품의 특성 및 핵심 기술 요소를 조사/분석하였다. 또한, 네트워크 접근제어시스템의 구조 및 중요 기술 분석하고 네트워크 접근제어시스템의 품질평가에 고려할 국제표준 ISO/IEC 25000시리즈[1], 소프트웨어 테스트에 대한 표준 ISO/IEC 29119의 최신 국제 표준 동향을 조사/분석하였다.

3장에서는 2장에서 분석된 동향과 기술특성 및 국제표준을 바탕으로 네트워크 접근제어시스템의 품질특성 및 품질 요구사항을 도출하였다.

4장에서는 도출된 요구사항을 바탕으로 ISO/IEC 25000시리즈와 ISO/IEC 29119를 참조하여 네트워크 접근제어시스템의 품질평가 항목과 기준을 개발하였다.

5장에서는 4장에서 개발된 네트워크 접근제어시스템 평가 항목과 평가 방법의 실제적용 여부 및 타당성을 입증하기 위하여 시중의 베타버전인 네트워크 접근제어시스템을 직접 시험 평가하여 적용성을 확인하였다.

2. 관련 연구

2.1 네트워크 접근제어시스템

IT 분야는 물론 물리적 보안 시스템까지 네트워크 기반으로 급격히 변화하면서 네트워크를 통한 침입과 정보유출이 날로 심각해지고 있다. 이에 대응하기 위해 네트워크 접근제어(Network Access Control, 이하 NAC)시스템이라는 개념이 등장[2]하였으며, 최근 들어 IT 보안 분야의 주요 이슈로 부상하고 있다.

2.1.1 인증

네트워크 접근제어시스템이 접근제어를 위하여 사용하는 방안의 대표적인 것이 인증방법이다. 즉, 사용자에 대한 인증, 단말에 대한 인증, 트래픽에 대한 인증을 네트워크 접근제어시스템이 수행하게 된다. 네트워크 접근제어시스템은 모든 네트워크를 경계선으로 본다. 어떤 사용자가 어떠한 경로를 통하여 들어오든지, 사용자 및 단말은 검사를 통과해야 내부 네트워크로 진입할 수 있다. 네트워크를 사용하기에 앞서 사용자에 대한 인증을 받아야 하며, 사용하는 노트북을 네트워크에 연결해도 안전하다는 검사를 받아야 한다[3]. 또한, 네트워크를 사용하면서 조금이라도 이상한 통신(Traffic)을 수행한다면 이는 바로 NAC에 의해 감지되어 외부의 IP는 네트워크로부터 격리시키게 된다.

2.1.2 네트워크 사용 모니터링

사용자 및 단말 인증을 거쳐 네트워크에 접속한 단말은 이제 네트워크를 이용할 수 있다. 하지만 자신에게 허용된 범위 내에서만 사용이 가능하다. 사용할 수 있는 범위는 사용자 인증 과정에서 미리 정해질 수도 있으며, 진입한 후에 정해질 수도 있다. 예를 들어, 사용자가 네트워크 진입과정에서 외부 협력업체 직원으로 인증을 받았다고 하면, 그 사용자는 내부 네트워크는 사용할 수 없고 인터넷만 사용이 가능하게 사용범위가 제한될 수 있다.

전체 네트워크를 사용할 수 있는 사용자라고 하더라도 정책에 위반되는 통신 또는 유해 트래픽을 발생시킨다고 하면 NAC는 그 단말을 검출하여 네트워크로부터 격리시키는 작업을 수행하게 된다[4]. 이를 위하여 NAC는 내부 네트워크에서 통신되는 모든 트래픽을 감시하는 기능을 가지고 있다. 제품의 종류에 따라 간단한 정책위

반을 검사할 수도 있고, 어떤 제품은 단말에 Backdoor가 설치되어 내부의 데이터를 외부로 유출하려는 시도까지도 검출이 가능하다.

2.2 네트워크 접근제어시스템 기술 요소

2.2.1 게이트웨이 인포서

게이트웨이 인포서는 네트워크 경계 지점에 설치되는 어플라이언스 장비로, 원격 엔드포인트의 정책 준수 여부를 기준으로 트래픽 흐름을 통제 또는 차단한다. 여기서 '경계 지점'이란 WAN 링크, VPN과 같은 네트워크 진입 지점일 수도 있고, 핵심 비즈니스시스템이 운영되는 네트워크 부분일 수도 있다. 게이트웨이 인포서는 자원에 대한 접근을 효과적으로 통제하고, 정책을 준수하지 않는 엔드포인트를 정책 준수 상태로 되돌리기 위한 조치를 자동으로 수행한다[5].

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.

2.2.2 DHCP 인포서

DHCP 인포서는 엔드포인트와 기업의 DHCP 서비스 인프라스트럭처 중간 지점에 설치된다. DHCP 인포서는 엔드포인트가 NAC 에이전트를 실행하고 있지 않거나, 정책을 준수하지 않고 혹은 정책 준수 여부를 확인할 수 없는 경우, '제한적 DHCP 주소 할당((restrictive DHCP lease assignment)'을 수행하게 된다.

제한적 DHCP 주소 할당을 통해 발급되는 IP 주소는 하우팅이 지원되지 않으며 네트워크 접근이 제한된다. DHCP 인포서는 엔드포인트 에이전트와의 커뮤니케이션을 통해 엔드포인트에 정책 준수 할당을 요청한다[6]. 새로운 주소 할당 요청을 수신한 DHCP 인포서는 엔드포인트가 정책을 준수하고 있음을 확인한 후 운영 네트워크에 정상적으로 접근할 수 있는 IP 주소를 할당한다.

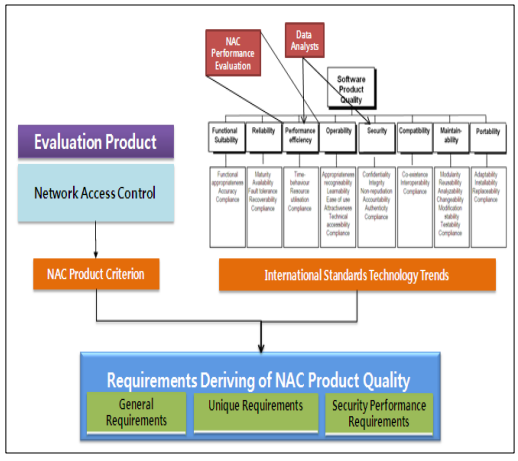
DHCP 인포서는 기본적으로 인라인 DHCP 프록시(in-line DHCP proxy)로 동작하므로, 기존 DHCP 인프라스트럭처와 호환된다. 또한 별도의 하드웨어/소프트웨어 업그레이드가 불필요하다.

DHCP 인포서 어플라이언스의 대안으로, 마이크로소프트 DHCP 서버에 직접 설치할 수 있는 DHCP 인포서 플러그인을 제공하기도 한다[7]. DHCP 인포서 플러그인을 사용할 경우에는 마이크로소프트 DHCP 서버가 정책 실행 포인트의 역할을 담당하게 된다.

3. 네트워크 접근제어시스템의 품질요구

이 장에서는 도출된 NAC 시스템의 요구사항은 아래의 그림에서와 같이 제품의 특징 및 품질평가 및 보안관련 국제표준인 ISO/IEC 25010 보안성능 관련 기술 동향에 근거를 두고 있다.

NAC 시스템의 품질 요구사항은 일반 품질요구사항과 고유 품질 요구사항으로 구분된다. 일반 품질 요구사항은 기능성, 신뢰성, 사용성, 효율성의 품질 요구사항을 도출하였으며, 고유 품질 요구사항은 ISO/IEC 2500시리즈에서 보안성과 효율성의 부특성인 보안성능을 중심으로 구성하였다.



[Fig. 1] Requirements of NAC System Quality

3.1 NAC 시스템의 일반 품질요구

2장에서의 관련연구의 NAC 제품의 특성과 기술 요소를 분석된 데이터를 가지고 국제표준인 ISO/IEC 25000 시리즈에서 NAC 시스템의 고유 특성인 보안성을 제외한 기능성, 신뢰성, 사용성, 효율성[8], 통합성, 안정성 주 특성별로 NAC 시스템의 일반 요구사항을 도출하여 NAC 시스템의 품질평가 기준 및 방법론을 구축하기 위한 기반을 확립하고자 한다.

3.1.1 기능성에 관한 요구사항

- 제품에 관한 설명서나 사용자 매뉴얼에 기술된 기능이 전체적으로 완전하게 구현되어 있어야 한다.
- 제품을 구성하는 각 기능이 제품별로 기능 구성요소로서 적절한 기능이어야 한다.
- 제품의 각 기능이 관련 설명서에 명세된 정확성에 관한 요구사항 대로 구현되어 요구하는 수준에 부합해야 한다.
- 서술된 정보대로 데이터의 상호 교환이나 표준화된 자료의 교환 등 다른 제품과의 상호작용을 통한 데이터 교환 기능이 동작해야 한다.

3.1.2 신뢰성에 관한 요구사항

- 제품에서 이전 제품에 존재하던 결함이 개선되었다면 명시적으로 해결이 확인되는 사항에 대해 기술하고 있어야 한다.
- 제품에 결함이 발생하더라도 관련 데이터가 정상상태로 완전히 복구될 수 있어야 한다.
- 제품에 결함이 발생되었을 경우 목표하거나 규정된 시간 내에 복구가 가능해야 한다.

3.1.3 사용성에 관한 요구사항

- 제품 설명서와 사용자 문서는 사용자가 기능을 이해하기 쉽게 작성되어 있어야 한다.
- 제품의 입력 및 출력에 사용되는 데이터는 그 의미를 쉽게 이해하고 사용할 수 있도록 구성되어 있어야 한다.
- 제품의 운영 절차는 전체 제품에 걸쳐 일관성 있게 구성되어 제품 사용시 사용자에게 혼동을 주지 않도록 구조화 되어 있어야 한다.

3.1.4 효율성에 관한 요구사항

- 제품 사용시 사용자의 처리 요구에 대한 반응이 나타나기까지의 평균 반응 시간은 명시된 규정을 준수하거나 최소화되어야 한다.
- 제품의 I/O자원 사용은 시스템의 전체적인 성능에 영향을 미칠 수 있으므로 가능한 최소화되어야 한다.
- 제품의 CPU 사용은 시스템의 성능에 영향을 미칠 수 있으므로 가능한 최소화되어야 한다.

3.1.5 안정성에 관한 요구사항

- 발생된 문제에 대한 분석을 수행할 수 있도록 상태를 모니터링하기 위한 필요한 데이터를 기록 저장하는 기능을 제공해야 한다.
- 제품에서 환경 설정에 관해 사용자가 쉽게 이해하고 파악하여 변경하기 용이하게 구현되어 있어야 한다.

3.1.6 통합성에 관한 요구사항

- 제품이 설치될 환경에서의 데이터 구조에 영향을 미치지 않고 정상적으로 작동할 수 있어야 한다.
- 제품이 설치매뉴얼 등의 설치 정보에 따라 정상적으로 설치되어 동작할 수 있도록 설치 프로그램과 설치 매뉴얼이 구성되어 있어야 한다.
- 기존의 제품을 대체하여 새로운 제품을 설치하고자 하는 경우, 이전에 사용하던 제품의 데이터를 제거하거나 변경하지 않고 사용할 수 있도록 유연성이 있어야 한다.

3.2 NAC 시스템의 고유 품질요구

이절에서는 NAC 시스템의 품질 고유 요구사항에 관련해서 시스템의 고유한 특성이 보안성에 관한 요구사항을 분석하여 NAC 시스템의 품질평가 기준 및 방법론을 구축하기 위한 기반을 확립하고자 한다.

3.2.1 보안감사

보안감사는 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안 제품에서 발생하는 관련 사건들의 감사 레코드를 생성, 기록, 검토하고 감사된 사건에 대한 잠재적 보안 위반을 탐지하고 대응행동을 수행하는 능력을 의미하며, 보안감사에 관한 요구사항은 다음과 같다.

- NAC 시스템은 잠재적인 보안 위반을 탐지한 경우 혼란을 최소화하는 대응행동의 목록을 취해야 한다.
- NAC 시스템은 식별된 사용자의 행동으로 인해 발생한 감사 사건에 대하여, 사건을 발생시킨 사용

자의 신원과 감사 대상 사건을 연관시킬 수 있어야 한다.

- NAC 시스템은 인가되지 않은 삭제로부터 감사 증적 내에 저장된 감사 레코드를 보호해야 한다. 또한, 저장된 감사 레코드에 대한 비인가된 변경을 방지해야 한다.
- NAC 시스템은 특별 권한을 갖는 인가된 사용자가 수행한 행동에 의한 감사 저장 실패가 아닌 경우에 손실 방지를 위한 행동을 취해야 한다.

3.2.2 사용자 데이터 보호

사용자 데이터 보호란 보안 제품 장애 발생시 안전한 상태를 유지하고 보안 관련 데이터 및 실행코드의 무결성을 검증하기 위하여 자체 시험을 수행하며 사용자가 일정기간 컴퓨터를 사용하지 않는 상황이 발생했을 때 세션 관리 기능을 제공하는 능력을 의미한다.

- NAC 시스템은 정보흐름을 유발하는 모든 오퍼레이션에 대하여 정보흐름통제를 강제해야 하며 모든 정보흐름을 유발하는 모든 오퍼레이션들의 정보흐름을 통제해야 한다.
- NAC 시스템은 지문정보와 관련된 객체, 보안목표 명세서 작성자에 의해 결정된 기타 목록에 자원을 할당 및 회수하는 경우에 자원의 모든 이전 정보 내용이 가용하지 않음을 보장해야 한다.

3.2.3 식별 및 인증

- NAC 시스템은 인증 사건의 목록에 관련된 정해진 횟수의 실패한 인증 시도가 발생한 경우 이를 탐지해야 한다.
- NAC 시스템은 각 사용자에 속한 디폴트값, 질의, 변경, 삭제, 연산 등의 보안속성 목록을 유지해야 한다.

3.2.4 보안관리

- NAC 시스템은 기능목록의 기능에 대해 행동을 결정, 중지, 개시, 변경하는 능력을 인가된 관리자로 제한해야 한다.
- NAC 시스템은 인가된 사용자와 연관된 보안속성 목록을 관리자만이 폐지할 수 있어야 한다.
- NAC 시스템은 식별 및 인증 데이터를 변경, 삭제하는 능력을 인가된 관리자로 재한해야 한다.

4. NAC 시스템 시험 평가방법

이장에서는 소프트웨어 품질평가 통합모델 표준인 ISO.IEC 25000 시리즈와 소프트웨어 테스트에 대한 표준 기준인 ISO/IEC 29119를 참조하여 평가방법을 구축하였고 보안제품의 특성과 ISO/IEC 25000시리즈를 참조하여 주특성에 보안성과 안정성, 통합성을 주특성으로 반영하였다.

NAC 시스템의 일반 요구사항과 고유 품질 요구사항으로부터 품질평가를 위한 특성과 NAC 시스템의 품질평가 기준을 도출하였다.

〈Table 1〉 Quality Characteristics and Negative Characteristics

Quality Characteristics	Negative Characteristics
Security	Security Audit, User Data Protection, Identification and Certification, Security Manageability, Security Protection Access Control
Reliability	Maturity, Fault tolerance, Recoverability
Usability	Understandability Learnability, Operability
Functionality	Suitability, Accuracy, Interoperability
Stability	Analyzability, Changeability, Maintainability
Efficiency	Time efficiency, Resource efficiency, Security Performance
Integrity	Adaptability, Installability, Replaceability, Co-existence

4.1 보안성

보안성이란 승인 혹은 권한이 없는 사람 또는 시스템이 필요한 정보를 불러오거나 변경하지 못하게 하고, 승인 혹은 권한이 있는 사람 또는 시스템이 필요한 정보에 대한 접근이 거부되지 않도록 하는 제품의 능력이다.

〈Table 2〉 Evaluation Items and Purposes of Security

Evaluation items	Evaluation purpose	Domain of the results
Security information	Evaluate whether cases of security infringement is recorded in the list of occurrences	0 ≤ Security alarm ≤ 1
Prevention of data loss	Evaluate whether the records taken at the time of failure to save auditing are being executed	Prevention of loss = Yes or No
Control for flow of information	Evaluate whether the flow of information or data is being controlled	0 ≤ Control the flow of information ≤ 1
Control of security function	Evaluate whether only the approved user can manage the security function	Control the security function = Yes or No

4.2 신뢰성

신뢰성이란 명시된 조건에서 시스템 또는 소프트웨어가 사용되어질 때, 성능 수준을 유지할 수 있는 제품의 능력이다.

〈Table 3〉 Evaluation Items and Purposes of Reliability

Evaluation items	Evaluation purpose	Domain of the results
Rate of possibility of restoration	Evaluate possibility of restoration in the event of occurrence of defect or error in the system	0 ≤ Possibility of restoration ≤ 1
Data restoration rate	Evaluate the extent of restoration in the event of occurrence of defect or error in the system	0 ≤ Data restoration rate ≤ 1
Avoidance of disability	Evaluate the extent of ensuring that defect does not occur in the event of occurrence of serious disability among the defects or errors generated	0 ≤ Avoidance of disability ≤ 1

4.3 사용성

사용성이란 명시된 조건에서 사용 할 경우 사용자가 학습, 이해, 선호 할 수 있는 제품의 능력이다.

〈Table 4〉 Evaluation Items and Purposes of Usability

Evaluation items	Evaluation purpose	Domain of the results
Functional learning	Evaluate whether the user can easily learn the functions for the product	0 ≤ Functional learning ≤ 1
Understanding of function	Evaluate the extent of understanding of the functions offered by the product through the manual provided	0 ≤ Understanding of function ≤ 1
User guidance	Evaluate the extent of provision of the functions of the product or system that can be used in accordance with the level of the user	0 ≤ Guidance of user ≤ 1
Consistence in operational procedures	Evaluate whether the operational procedure of the product or system has been uniformly structuralized	0 ≤ Consistency in operational procedure ≤ 1

4.4 기능성

제품 혹은 시스템이 특정한 상황에서 사용될 때, 명시된 요구와 내재된 요구를 만족하는 기능을 제공하는 제품의 능력이다.

〈Table 5〉 Evaluation Items and Purposes of Functionality

Evaluation items	Evaluation purpose	Domain of the results
Precision	Evaluate whether the result value of the product coincides with the result value described in the user document	0 ≤ Precision ≤ 1
Completeness of the function	Evaluate whether the functions stipulated in the document are realized or not	0 ≤ Completeness of function ≤ 1
Consistence of operational procedure	Evaluate whether the operational procedures of the product or the system has been uniformly structuralized	0 ≤ Consistency in operational procedure ≤ 1

4.5 안정성

제품이 변경되어도 안정적으로 운영 될 수 있는 능력을 의미하며, 변경에는 환경과 요구사항, 기능적 명시에 따른 제품의 수정, 개선 등이 포함된다.

〈Table 6〉 Evaluation Items and Purposes of Stability

Evaluation items	Evaluation purpose	Domain of the results
Possibility of modification	Evaluate whether setting of the environment is easy in the product or system	0 ≤ Possibility for modification ≤ 1
Support diagnosis function	Evaluate whether diagnostic function that can solve the defect or error that occurs	0 ≤ Support diagnosis function ≤ 1
Success rate of modification	Evaluate the extent of prevention of the unexpected results due to changes in the environment setting	0 ≤ Success rate of modification ≤ 1

4.6 효율성

명시된 조건에서 사용되는 자원의 양에 따라 요구된 성능을 제공하는 능력을 말한다.

〈Table 7〉 Evaluation Items and Purposes of Efficiency

Evaluation items	Evaluation purpose	Domain of the results
Data transmission rate	Evaluate the speed of data transmission	0 ≤ Data transmission rate ≤ 1
Appropriateness of the average processing time	Evaluate the average processing time that successfully execute particular tasks during the use of the product or system	0 ≤ Appropriateness of average processing time ≤ 1

4.7 통합성

시스템 혹은 제품이 새로운 환경으로 전이되거나 통합될 수 있는 제품의 능력이다.

〈Table 8〉 Evaluation Items and Purposes of Integrity

Evaluation items	Evaluation purpose	Domain of the results
Implant excellence	Evaluate whether easy adaption to new environment has been realized	0 ≤ Implant excellence ≤ 1
Installation functionality	Evaluate whether installation can be realized in accordance with the specified installation information	0 ≤ Possibility of installation ≤ 1
Sustaining of function	Evaluate whether the functions used before can be used when the product or system has been substituted	0 ≤ Sustaining of function ≤ 1

5. NAC 시스템의 시험평가 사례

NAC 시스템의 시험 평가에서는 현재 사용하고 있는 NAC 시스템 소프트웨어에 대해 시험 평가를 하였다. 그리고 제품의 품질을 측정하여 평가한 사례의 시험방법에 대해 품질평가 체계를 구축하였다.

5.1 NAC 시스템 제품

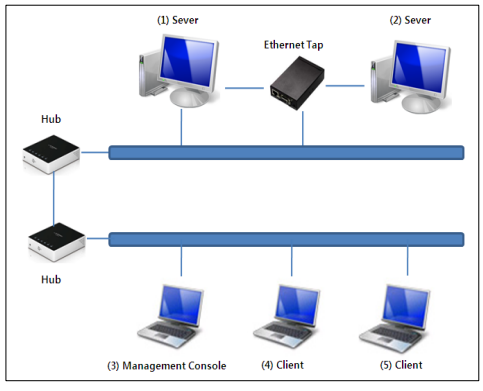
평가한 제품은 시중에 사용하고 있는 NAC 시스템 소프트웨어로서 기업의 보안 정책에 위배되는 PC에 대해 네트워크 접근을 통제할 수 있는 DB보안 솔루션으로 관리 모듈, 에이전트 모듈 및 네트워크 제어를 담당하는 어플라이언스(Appliance)로 구성되어 있는 시스템이다.

기능은 가음과 같다.

- 사용자/PC 인증 및 권한 관리
  : 등급(관리자, 사용자, 뷰어)별 로그인/로그아웃 등
- 실시간 모니터링
  : 로깅정책관리, 경고정책관리, 서버관리, DB관리, 사용자관리 등
- 보안 정책 관리 및 실행 기능 등
  : 실시간 감시, 감사데이터 생성, 로그검색, 패킷드랍 등
- 접근통제
  : 보안위반 감시, 경로제어, 세션차단 등

5.1 시험환경

시험환경은 다음과 같이 보이는 그림과 같이 구축하여 시험평가 하였다.



[Fig. 2] Test Environment

Ethernet Tap으로 (1)서버와 (2)서버를 묶어 스위치 허브에 연결하였으며 (3)관리콘솔, (4)클라이언트, (5)클라이언트에는 다른 스위치 허브에 연결하여 제품을 시험하였으며, (1)서버에 설치한 프로그램은 시험대상제품(관리모듈)과 JDK v1.5, Tomcat v4.1.31, MySQL v5.0.26, Apache Web Server v2.0, Oracle instant client v10.2.0를 설치하였으며, (2)서버에는 Oracle 10g R2를 설치하였다. (3)관리콘솔에는 시험 대상 제품 접속을 위한 프로그램인 Internet Explorer, 기타 응용 프로그램인 MS Office 2007, 한글 2005, PDF Viewer 등을 설치하였다.

그리고 (4)클라이언트와 (5)클라이언트에는 DBMS 접속을 위한 프로그램 : Windows Oracle Client 10g R2, Orange for Oracle v4.0, JLoader v1.0, Loop Runner v1.0과 기타 응용 프로그램을 설치하였다.

성능측정도구로는 TeamQuest v10.1(자원사용률 측정)를 사용하였으며, (1)번 서버와 (4)번 클라이언트에 각각 설치하였다.

5.2 시험결과

시험 결과 기능성에서는 경고 발생 시 이메일 발송 기능, 수동백업 기능, DB 리포트 생성 기능, DB Session 검색 기능 등에서 결함이 발생하였으며, 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 제품에서 제공하는 기능이 정상 동작함을 확인하였다.

신뢰성에서는 제품 관리를 위해서는 관리자 계정이 하나 이상 반드시 존재해야 하나, 모두 삭제 가능하고 이전 상태로 복구할 수 없는 신뢰성 결함이 발생하였으나, 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 제품이 정상 동작함을 확인하였다.

효율성에서는 제시된 시험환경(하드웨어 및 소프트웨어, 네트워크 환경에)에서 제품 운영시 CPU 사용률, 메모리 사용량 및 응답시간은 다음과 같이 나타났다.

제품이 Gateway 모드로 설정된 상태에서 클라이언트가 DB서버로 TPC-H Query(22개 Query)를 400회 반복하여 전송할 경우, 제품의 CPU 사용률은 7.2%까지 올라가나 처리완료 후 1% 미만으로 내려가고, 메모리 사용량은 3,401 ~ 3,430MB로 일정하게 유지되며, Query 처리시간은 평균 8.4초 소요되었다.

그리고 제품이 Sniffing 모드로 설정된 상태에서 클라이언트가 DB서버로 TPC-H Query(22개 Query)를 400회 반복하여 전송할 경우, 제품의 CPU 사용률은 6.7%까지 올라가나 처리완료 후 1% 미만으로 내려가고, 메모리 사용량은 3,514 ~ 3,538MB로 일정하게 유지되며, Query 처리시간은 평균 6.8초 소요되었다.

사용성에서는 도움말 실행 오류, 추이분석 그래프 X축 값 표시 오류, 경향 분석 그래프 표시 오류등의 결함이 발생하였으며, 최종적으로 정상 동작함을 확인하였다.

〈Table 9〉 Number of defects

Quality Characteristics	Defects
Security	3
Reliability	1
Usability	14
Functionality	13
Stability	1
Efficiency	0
Integrity	2
Total	34

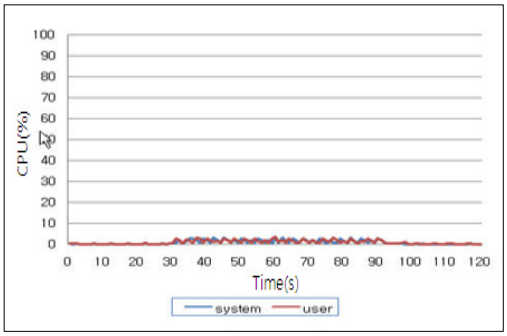
안정성에서는 네트워크를 통해 서버에 접근할 경우, 접근 로그를 기록하도록 환경설정을 변경해도 로그가 기록되지 않는 유지보수성 결함이 발생하였으나, 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 제품이 정상 동작함을 확인하였다.

통합성에서는 명시된 시험환경(하드웨어 및 소프트웨어, 네트워크 환경)에서 프로그램이 정상적으로 구동됨을 확인하였다.

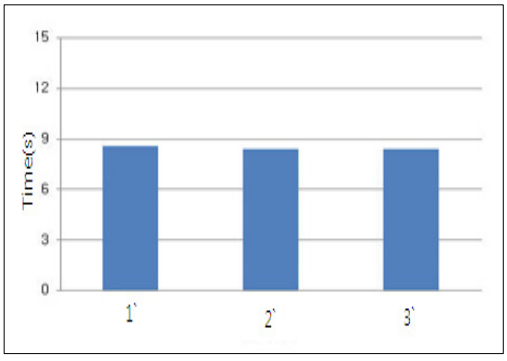
5.3 성능 시험결과

자원효율성에서 CPU 사용률은 제품이 Gateway 모드로 설정된 상태에서 클라이언트가 DB서버로 TPC-H Query(22개 Query)를 400회 반복하여 전송할 경우, (1)번 서버의 CPU 사용률은 7.2%까지 올라가나 처리완료 후 1% 미만으로 내려가고 이후 안정적으로 유지되었다.

시간효율성에서 처리시간은 제품이 Gateway 모드로 설정된 상태에서 클라이언트가 DB서버로 TPC-H Query(22개 Query)를 400회 반복하여 전송할 경우, Query 처리시간이 평균 8.4초 소요되었다.



[Fig. 3] Server - CPU



[Fig. 4] Server - Memory

6. 결론

NAC 시스템은 양적으로는 빠른 성장세를 보이고 있으나 질적인 품질을 고려하는 노력이 미흡하여 본 연구에서는 NAC 시스템의 질적인 면인 품질수준을 파악하여 개선방향을 도출함으로써 품질향상을 지원할 수 있는 평가모델을 개발하기 위해 동향 및 기술적인 요소들을 조사 분석하고, 평가방법론 구축의 근간이 되는 국제표준 ISO/IEC 25000시리즈와 테스트 표준인 ISO/IEC 29119의 동향을 분석하였다.

본 논문에서는 NAC 시스템의 특성과 국내 현황을 분석하여 네트워크 접근제어시스템의 일반 요구사항과 고유 품질 요구사항을 도출하였으며, 도출된 요구사항과 국제표준 소프트웨어 품질평가 통합 모델인 ISO/IEC 2500시리즈와 소프트웨어 테스트에 대한 표준인 ISO/IEC 29119를 참조하여 NAC 시스템의 평가기준과 평가방법을 구축하였다.

그리고 구축된 평가방법의 적용성을 확인하기 위해 실제로 사용하고 있는 NAC 시스템을 직접 시험 평가하여 방법을 확인하였다.

본 논문에서 실제 시험 평가한 사례는 실용적으로 현장에서 적용가능하다는 점에서 실질적인 NAC 시스템의 품질향상에 도움이 될 것으로 판단된다.

기술적으로 NAC 시스템의 활용성이 높아지고 있는 시점을 생각하면 NAC 시스템의 평가체계 확립은 필요하며, 본 논문에서 구축한 평가방법에 통해 다양한 상황의 사용되는 NAC 시스템의 다양한 요구사항을 반영하여 정량적으로 평가할 수 있는 방법과 검증이 필요하다.

향후 연구과제로는 NAC 시스템의 평가체계를 업데이트되는 국제표준을 반영하여 NAC 시스템의 평가방법에 대한 신뢰성을 높이는 노력이 필요하고 정도를 높이기 위한 지속적인 연구수행이 필요하다고 본다.

REFERENCES

[1] ISO/IEC 25000, SQuaRE - Software Product Quality Requirements and Evaluation Part 1,2,3,4,5.

[2] Keith N. Hampton, Chul-joo Lee, and Eun Ja Her, How new media affords network diversity: Direct and mediated access to social capital through participation in local social settings, TELECOMMUNICATIONS POLICY. Vol. 35, No. 9-10, pp. 883-894, 2011

[3] William H. Lehr, John M. Chapin , “On the convergence of wired and wireless access network architectures”, Information Economics and Policy. Vol. 22, No. 1, pp. 33-41, 2010.

[4] Growitsch, Christian, Network access charges, vertical integration, and property rights structure--experiences from the German electricity markets, Energy Economics. Vol. 27, No. 2, pp.257, 2005.

[5] Henrike Hannemann-Weber, Maura Kessel, Carsten Schultz , Research performance of centers of expertise for rare diseases : The influence of

network integration, internal resource access and operational experience, Health policy. Vol. 105 No. 2-3, pp. 138-145, 2012.

[6] Chang-Hun Lee, Ok-Hyun Ha, A Study on Convergence of Cyber Security Monitoring and Industrial Security, Journal of Information and Security, Vo.l10, No.4, pp. 61-67, 2010. 12.

[7] Seung-Hyun Paik, Sung-Kwang Kim, Hong-Bae Park, Design and Implementation of Network Access Control for Security of Company Network, Journal of the institute of electronics engineers of Korea, Vol.47, No.12, 2010. 12.

[8] Sang-Won Kang, Hae-Sool Yang, Quality Evaluation of Criterion Construction for Open Source Software", The journal of digital policy & management, Vol.11, No.2, 2013. 2.

양 효 식(Yang, Hyo-Sik)

- 2008년 2월 : 호서대학교 컴퓨터공학과 졸업(학사)
- 2012년 2월 : 호서대학교 벤처전문대학원 정보경영학과 졸업(석사)
- 2012년 3월 ~ 현재 : 호서대학교 벤처전문대학원 융합공학과 박사과정 재학중
- 2009년 1월 ~ 2011년 1월 : KITT 한국IT진흥(주) 근무
- 2011년 3월 ~ 2013년 3월 : KT네트웍스(주) 근무
- 2013년 4월 ~ 2014년 2월 : UL Korea(주) 재직중
- 관심분야 : 소프트웨어 프로세스 인증 및 시험, 물리보안 시스템, 소프트웨어 및 네트워크 보안, 정보서버 보안관리
- E-Mail : scaglietti.hs@hanmail.net

전 인 오(Jeon, In-Oh)

- 1998년 2월 : 호서대학교 전자공학과 졸업(학사)
- 2000년 2월 : 중앙대학교 경영학과 졸업(석사)
- 2005년 2월 : 호서대학교 소프트웨어공학전공(공학박사)
- 1998년 1월 ~ 2004년 12월 : (주)씨아이정보기술 대표이사
- 2010년 3월 ~ 2011년 2월: 호서대학교 글로벌창업대학원 부원장
- 2005년 3월 ~ 현재 : 호서대학교 글로벌창업대학원 교수
- 2005년 3월 ~ 현재 : 호서대학교 벤처전문대학원 교수
- 2012년 2월 ~ 현재 : 호서대학교 창업지원단 단장
- 관심분야 : 벤처창업론 및 컨설팅, 소프트웨어공학(특히, SW품질보증과 평가 및 품질감리), 전시/컨벤션산업
- E-Mail : eric@hoseo.ac.kr