https://doi.org/10.14400/JDC.2017.15.6.219

네트워크 접근제어 시스템의 보안성 메트릭 개발

이하용*, 양효식**
서울벤처대학원대학교 융합산업학과*, 삼일회계법인 IT Risk & Security**

Development of Security Metric of Network Access Control

Ha-Yong Lee*, Hyo-Sik Yang**
Dept. of Fusion Industry, Seoul Venture University*
Samil PricewaterhouseCoopers IT Risk & Security**

요 약 네트워크 접근제어(Network Access Control)를 통해 IT 인프라에 대한 보안위협 즉, 비인가 사용자, 단말의 네트워크 무단 접속, 직원의 내부 서버 불법접근 등을 효과적으로 차단할 수있어야 한다. 이러한 관점에서는 보안성을 충족시키고 있음을 확실히 하기 위해 관련 표준에 기반을 둔 메트릭 구축이 요구된다. 그러므로 관련 표준에 따른 NAC의 보안성 평가를 위한 방법의 체계화가 필요하다. 따라서 이 연구에서는 네트워크 접근제어시스템의 보안성 메트릭 개발을 위해 ISO/IEC 15408(CC:Common Criteria)과 ISO 25000 시리즈의 보안성 평가 부분을 융합한 모델을 구축하였다. 이를 위해 네트워크 접근제어시스템의 품질 요구사항을 분석하고 두 국제표준의 보안성에 관한 융합 평가메트릭을 개발하였다. 이를 통해 네트워크 접근제어시스템의 보안성 품질수준 평가 모델을 구축하고, 향후 네트워크 접근제어시스템에 대한 평가방법의 표준화에 적용할 수 있을 것으로 사료된다.

주제어 : 네트워크 접근제어, 품질평가 모델, 보안성, 메트릭, 품질 요구사항

Abstract Network access control should be able to effectively block security threats to the IT infrastructure, such as unauthorized access of unauthorized users and terminals, and illegal access of employees to internal servers. From this perspective, it is necessary to build metrics based on relevant standards to ensure that security is being met. Therefore, it is necessary to organize the method for security evaluation of NAC according to the related standards. Therefore, this study builds a model that combines the security evaluation part of ISO / IEC 15408 (CC: Common Criteria) and ISO 25000 series to develop security metric of network access control system. For this purpose, we analyzed the quality requirements of the network access control system and developed the convergence evaluation metric for security of the two international standards. It can be applied to standardization of evaluation method for network access control system in the future by constructing evaluation model of security quality level of network access control system.

Key Words : Network Access Control, Quality Evaluation Model, Security, Metric, Quality Requirements

1. 서론

네트워크 및 인터넷의 발전으로 보안위협과 정보유출에 대한 피해는 계속 커지고 있다[1]. 과거 IT 분야의 보안은 외부 침입에 대한 방어에 집중되어 있었으나 현재는 기업 업무환경의 변화로 모바일 기기까지 보안을 챙

Received 16 March 2017, Revised 28 May 2017
Accepted 20 June 2017, Published 28 June 2017
Corresponding Author: Hyung-Sik Yang
(Samil PricewaterhouseCoopers IT Risk & Security)
Email: hyosyang@samil.com

ISSN: 1738-1916

겨야 하는 상황에 도달하였다.

네트워크 접근제어(이하 NAC)는 네트워크에 접속하려는 단말의 보안정책 준수 여부를 검사하여 인가를 받지 않았거나 악성코드에 감염된 단말이 네트워크에 접속하는 것을 원천 차단하여 시스템을 보호하는 형태로 보안성을 강제할 수 있는 보안 인프라이다[2]. 2010년대 후반부터 국내의 NAC 시장은 높은 성장률과 더불어 APT(Advalced Persistent Thread) 같은 보안 공격에 대한 대안으로 새롭게 자리잡고 있다. APT는 공격 대상에 침입 후 잠복하여 때를 기다리다가 적정 시점에 정보를 빼가는 방식을 사용하는 공격 방법이다[3].

NAC 시스템은 정보보호 시스템으로서 자신의 역할을 제대로 수행하기 위해서는 준수해야 할 기준을 구축하여 적용해야 한다. 이를 위해 네트워크 집근제어시스템에 대한 보안 요구사항을 CC(ISO/IEC 15408, Common Criteria)라는 국제 공통 평가 기준에 따라 작성된 보호 프로파일[4]에 따라 제품을 개발하여 평가받게 된다.

본 논문에서는 NAC 시스템의 보안성 품질에 관한 평가를 위해 CC를 기반으로 한 NAC 시스템에 관한 보호 프로파일 및 ISO/IEC 25010[5] 소프트웨어 제품평가 관련 국제표준 품질체계를 기준으로 NAC 시스템의 보안성 품질 모델을 구축하였다.

본 논문의 2장에서는 NAC 시스템의 기술동향 및 시장동향을 살펴보고 3장에서는 NAC 시스템의 보안성 특성 관련 평가항목을 분석하고 4장에서는 보안성 평가모델을 구축하며 5장에서 결론과 함께 향후 연구 과제를 제시하였다.

2. NAC 시스템 시장 동향 및 평가 동향

2.1 NAC 시스템 시장 동향

가트너(2016)[6]에 따르면, 전 세계의 NAC 관련 시장은 상위 글로벌 3사인 Cisco, FOreScout, HPE의 자료로 볼 때, 2014년 대비 18% 성장률과 약 5억 4,300만불의 시장 규모였다. NAC 시장은 성숙단계에 접어 들었지만 여전히 BYOD, IoT와 연관해서 지속적인 수요의 증가를 보이고 있으며 급변하는 보안위협에 대한 모니터링과 네트워크의 가시성(network visibility)를 개선하기 위해 SIEM, EMM 솔루션 등의 다른 보안 솔루션과의 통합이 주요 이슈로 등장하고 있다.

2016년 국가정보보호백서[7]에 따르면 정보보안 제품 분야가 전체의 75.7%, 정보보호 서비스 분야가 나머지 24.3%를 차지하고 있다. 이 중에서 정보보안 제품으로 네트워크보안, 시스템(단말) 보안, 콘텐츠/정보유출 방지 보안, 암호/인증, 보안관리 등을 분류하고 있으며 NAC 시스템은 네트워크보안에 속하는 제품으로서 정보보안 산업 전체의 26%를 차지하고 있는 네트워크보안 분야의 일부로서 관련 산업 전체의 2.6%, 네트워크 보안 분야의 9.8%를 차지하고 있다.

2.2 NAC 시스템의 품질 관련 연구 동향

NAC 시스템에 대한 기존의 품질평가 관련 연구[8, 9]에서는 보안성을 근간으로 하고 이를 평가하기 위해 ISO/IEC 25010의 기능성, 신뢰성, 사용성, 효율성의 품질 요구사항을 NAC 시스템에 적용할 수 있도록 도출하여 일반 품질 요구사항으로 삼고 이들 이외의 순수 보안성에 관련된 품질 요구사항을 NAC 시스템 고유의 품질 요구사항으로 구분하여 체계를 구성한 바 있다.

NAC 시스템의 성능 향상을 통한 의료정보 유출 방지를 위한 네트워크 이중 접근통제 모델에 관한 연구[10]에서는 NAC 센서를 통해 내부의 네트워크 접근을 원하는 디바이스를 식별하고 NAC 서버를 통해 접근통제 정책을 수립 및 실행하는 시스템을 구축하였다. 이 시스템에서는 실제 사용자가 조직 내 어디에 위치하는가를 기준으로 하여 네트워크 접근통제 정책을 실행한다.

3. NAC의 보안성 평가항목

이 절에서는 소프트웨어 제품평가에 관련된 ISO/IEC 25010 표준을 기반으로 보안성(security)에 관한 품질특성을 NAC의 특성에 입각하여 구축할 수 있도록 NAC의 보안성에 관련된 전반적인 평가항목을 체계화하였다.

3.1 NAC의 보안감사성

NAC의 보안감사성이란 보안 관련 행동에 대한 책임 추적을 위해 정보보안 제품에서 발생하는 사건들에 관한 감사 레코드를 생성하거나 기록・검토하고 감사 사건에 관련된 잠재적 보안 위반을 탐지 및 대응행동 수행 능력

을 의미한다. 보안감사성은 감사 데이터의 생성, 보안 경보, 사건과 사용자의 연관, 규칙 위반의 지적, 저장소 보호, 감사 검토, 감사 데이터 손실 예측 시 대응 행동, 감사 데이터 손실 방지의 평가항목을 가진다.

<Table 1> Table of Security Auditability

No.	Characteristic	Subcharacteristic	Name of Evaluation Items	Meaning of Evaluation Item
1	Security	Security Audit	Audit data generation	The generation of a regulatory audit data
2			Correlation of event and user	The system can correlate the identity of the user who caused the event and the audited event.
3				
4			Pointing out the violation of rule	When examining a case, system applies a set of rules and evaluates whether it can point out a latent vidation based on rules.
…			…	…

3.2 NAC의 사용자 데이터 보호

NAC의 사용자 데이터 보호는 정보흐름과 관련된 기능의 정보흐름을 통제하고 객체에 관한 무결성 오류에 관해 사용자 데이터를 검사하고 오류를 탐지했을 때 대응행동을 수행하는 능력을 의미한다. 사용자 데이터 보호에는 정보흐름 통제, 부분적인 접근통제, 보안속성에 따른 통제, 보안속성 없는 사용자 데이터 접근통제, 잔여정보 보호의 평가항목이 있다.

<Table 2> Table of User Data Protection

No.	Characteristic	Subcharacteristic	Name of Evaluation Items	Meaning Evaluation Item
1	<Security>	<User data protection>	Information Flow Control	The system must evaluate if system controls information flow of functions related to information flow.
2			Partial Access Control	The System must control the access about the operation lists between the subject and the object.
3			Control based on security attributes	The system should evaluate if it controls information flow according to security attributes.
4			User Data Access Control without Security Attribute	The System must control the access forcibly and ignore the security attribute related to user data when the user data controlled with security function come in from outside.
…			…	…

3.3 NAC의 식별 및 인증

NAC의 식별 및 인증은 해당 정보보호 제품의 관리자 및 사용자의 신원을 식별하고 인증하며 인증 실패시 대응할 수 있는 능력을 의미한다. 식별 및 인증은 인증실패시 처리, 사용자 보안속성의 유지, 비밀정보 검증, 사용자 인증, 인증 피드백의 보호, 사용자 식별 등의 평가항목을 가진다.

<Table 3> Table of Identification and Authentication

No.	Characteristic	Subcharacteristic	Name of Evaluation Items	Meaning of Evaluation Item
1	<Security>	<Identification and Authentication>	Authentication failure handling	The system must evaluate if system detects a authentication failure and perform reactions.
2			Maintaining user security attributes	The system must evaluate if system maintains a list of security attribute for each user.
3			Verifying secret information	The system must evaluate if system provides a mechanism which verify to satisfy the regulatory permission criteria.
4			User authentication	The system must evaluate if system certifies a user successfully before permitting any action.
5			Autentication Feed -back Prote -ction	The system must provide a user with only the feedback list during the authentication.
…			…	…

3.4 NAC의 보안관리성

NAC의 보안관리성은 해당 정보보안 제품의 보안기능과 속성, 보안 관련 데이터 및 보안 역할 등에 관한 사항을 관리하는 능력이다. 보안관리성은 보안기능 관리, 보안속성의 관리, 보안속성의 폐지 권한, 데이터 관리의 제한, 관리기능의 수행, 관리자 역할의 유지 등의 평가항목을 가진다.

<Table 4> Table of Security Manageability

No.	Characteristic	Subcharacteristic	Name of Evaluation Items	Meaning of Evaluation Item
1	<Security>	<Security Manageability>	Security Function Management	The system must evaluate if system restrict so that the only authorized administrator can manage the security functions.

2			Security Attribute Management	The system must evaluate if system restricts so that the only authorized administrator can manage the security attributes.
3			Rights for Security Attribute Abolition	Only the administrator can abolish the list of the authorized user and the related security attribute list.
4			Limit Data Management	The system must evaluate if system restricts so that the only authorized administrator can manage the identification and authentication data.
…			…	…

3.5 NAC의 보안기능 보호

NAC의 보안기능 보호란 보안기능에 대해 주기적이거나 관리자의 요구가 있을 때 무결성을 검증하는 말한다. 보안기능 보호성은 자체 시험의 평가항목을 가진다.

<Table 5> Table of Security Function Protection

No.	Characteristic	Subcharacteristic	Name of Evaluation Items	Meaning of Evaluation Item
1	<Security>	<Security Function Protection>	Self Test	The system can do the self-test to prove the accurate operation of the security functions.

3.6 NAC의 접근통제성

NAC의 접근통제성은 시스템이 정보흐름을 중재할 수 있도록 관련 보안 정책에 따라 패킷필터링 등을 통해 외부망으로부터 내부의 망을 보호하는 능력이다. 접근통제성은 세션 잠금의 평가항목을 가진다.

<Table 6> Table of Access Control

No.	Characteristic	Subcharacteristic	Name of Evaluation Items	Meaning of Evaluation Item
1	<Security>	<Access Control>	Lock Session	The system must evaluate if system emasculates the action by locking the interacting sessions after a period of inactivity of the administrator.

4. NAC의 보안성 평가모델

NAC은 정보보안 시스템으로서 이에 대해 평가하기 위해서는 공통 평가기준(CC)을 바탕으로서 ISO/IEC 25000 시리즈[11, 12, 13]의 품질평가 모델도 더불어 고려해야 한다. 따라서 본 논문에서는 공통 평가기준과 ISO/IEC 25000 표준의 품질평가 체계를 함께 고려하여 보안성의 품질특성에 관련된 부특성들인 기밀성(Confidentiality), 무결성(Integrity), 책임성(Accountability), 인증성(Authenticity)에 관한 평가모델을 구성하였다. <Table 7>에 보안성에 관한 부특성의 개념을 정리하였다.

<Table 7> Quality Characteristics System about Security

Quality Characteristic	Quality Subcharacteritic	Concept
Security	Confidentiality	The degree to which the product or system can access data only to users with access
	Integrity	The degree to which a system or product prevents unauthorized access or modification of computer programs or data.
	Accountability	The degree to which the behavior of an entity can be traced to an entity uniquely.
	Authenticity	The degree to which the identity of the subject or resource can be proved as the very subject

평가모듈은 평가 척도에 대해 ISO/IEC 25041[14]의 평가모듈(evaluation module) 형식에 의거해서 소프트웨어 품질평가에 대한 제반 사항을 문서화하는 형식에 관한 체계이다. 평가모듈에 관련된 기본 사항들을 4.1에서 기술하였다.

4.1 평가모듈의 구성

평가모듈은 메트릭의 개념 및 메트릭을 이용한 평가방법과 평가결과에 대한 해석 등에 관해 전반적인 사항을 문서화하여 평가시 참고할 수 있는 문서이다. 평가모듈은 ISO/IEC 25041을 기반으로 <Table 8>과 같은 구성으로 작성한다.

<Table 8> The Construction of Quality Evaluation Module

Configuration	Content
Outline	The basic concept of evaluation modules
	What you want to get by measuring the evaluation module
	where the metric belongs
	explanation of related terms

Coverage	target such as document or software
	Tools/resources required to apply the metric
	Testing techniques that can be applied
	Information to consider when applying the assessment module
Reference	Related Documents that metrics are derived
Metric	Data items to be measured
	Specific metrics for metrics for configuring metrics
	Definition of a formula using data items
Application Procedures	Description on specific procedure and method to perform the test
Result interpretation and reporting	The range of metric results
	Provide guidance on how to interpret measurement results
	Items you need to create and report

4.2 메트릭 개발 내역

본 연구에서는 NAC의 보안성에 관한 부특성인 기밀성, 무결성, 책임성, 인증성에 관한 메트릭을 개발하였다.

4.2.1 NAC의 기밀성에 관한 메트릭

<Table 9>에는 NAC의 보안성의 부특성 중 기밀성에 관한 메트릭을 나타내었다.

<Table 9> The Metrics about Confidentiality of NAC

Characteritic	Subcharacteristic	Item	Related Items
Security	Confidentiality	Mandatory access control	The system must forcibly control access to the list of operations between the subject and the object.
		Ignoring Security Attributes	The system must forcibly control access when the user data controlled by the security function is imported from the outside and ignore the security attributes related to the user data when the user data is inputted from the outside.
		Ensuring the unavailability of previous information	The system should ensure that all prior information content of the resource is not available when assigning and retrieving resources to the object associated with the fingerprint information, or to the list of other objects determined by the security target author.
		Providing validation mechanism	The system should provide a mechanism to verify that the secrets meet the defined tolerance criteria.
		Ability to read audit data	The system should provide the authorized administrator with the ability to read all audit data from the audit records. In addition, an audit record should be provided to allow the user to interpret the information.
		…	…

4.2.2 NAC의 무결성에 관한 메트릭

<Table 10>에는 NAC의 보안성의 부특성 중 무결성에 관한 메트릭을 나타내었다.

<Table 10> The Metrics about Integrity of NAC

Characteritic	Subcharacteristic	Item	Related Items
	Integrity	Abolition of security property list	Only the administrator should be able to abolish the security property list associated with the authorized user.
		Audit record protection	The system should protect the audit records stored in the audit trail from unauthorized deletion.
		reaction	If the audit trail exceeds the predefined limit, the system should notify the authorized administrator and take the determined reaction.
		Loss prevention behavior	The system should take action to prevent loss if audit storage failure is not the actions performed by an authorized user with special authority.
		Performing administrative functions	The system should be able to perform the prescribed management functions.
		…	…

4.2.3 NAC의 책임성에 관한 메트릭

<Table 11>에는 NAC의 보안성의 부특성 중 책임성에 관한 메트릭을 나타내었다.

<Table 11> The Metrics about Accountability of NAC

Characteritic	Subcharacteristic	Item	Related Items
	Accountability	Acquisition of a reaction list	The system should take a reaction list that minimize confusion if it detects potential security violations.
		Creating audit records	The system should be able to create audit records of auditable events.
		Associating events with users	The system should be able to associate the auditable event with the identity of the user who generated the event for the audit event that occurred due to the behavior of the identified user.
		Pointing out potential violations	The system should be able to apply a set of rules when examining audited events and be able to point out potential violations based on these rules.
		…	…

4.2.4 NAC의 인증성에 관한 메트릭

<Table 12>에는 NAC의 보안성의 부특성 중 인증성에 관한 메트릭을 나타내었다.

<Table 12> The Metrics about Authenticity of NAC

Characteritic	Subcharacteristic	Item	Related Items
	Authenticity	Detection of authentication attempts	The system should detect if a specified number of unsuccessful authentication attempts have occurred related to the authentication events list.
		Keeping security attributes	The system should keep a list of security attributes such as default values, queries, changes, deletions, and other operations belonging to each user.
		User Authentication	The system should successfully authenticate the user on behalf of the user before allowing any other behavior that the security function mediates.
		Providing a feedback list	The system should provide only the feedback list to the user during the authentication.
		User identification	The system should successfully identify each user before allowing any other behavior that the security function mediates on behalf of the user.
		…	…

4.3 품질검사표

품질검사표는 메트릭의 의미와 측정 항목의 개념 및 방법, 메트릭의 계산식과 결과값의 범위 등으로 구성하여 평가현장에서 손쉽게 활용할 수 있도록 한 도표이다. 품질검사표는 소프트웨어 품질평가 방법에 관한 전반적인 사항을 문서화할 때 활용할 수 있는 표준인 ISO/IEC 25041의 평가모듈 구성체계를 기반으로 필수적인 사항을 추출하여 간편한 활용을 위해 만든 것이다. <Table 13>에 품질검사표의 예를 나타내었다.

<Table 13> An Sample of Quality Inspection Table

Measure name		Are the prescribed audit data generated?		
Audit Data Generation				
Measurement items	A	the number of audit data to be generated		
	B	the number of audit data generated		
expression		- Audit Data Generation = B/A		
The range of results		0 ≤ Audit Data Generation ≤ 1	result value	
problem				

품질검사표의 결과를 도출하기 위해서는 측정 항목(measurement items)의 값을 구하기 위해 체크리스트 형태의 점검표를 구축하여 측정 항목에 대한 결과를 얻어야 한다. 결과값이 일정한 범위로 사상될 수 있도록 하기 위해 계산식은 0~1 사이의 결과를 도출할 수 있도록 구성하였다.

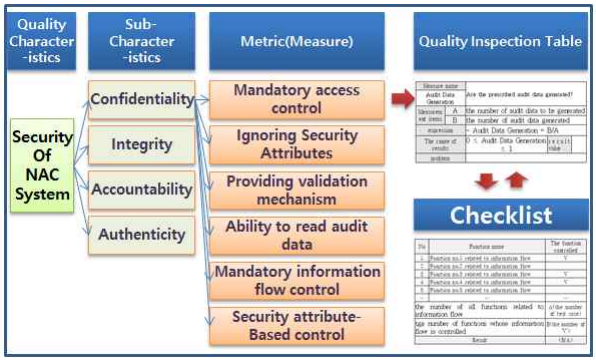
4.4 점검표

점검표는 품질검사표의 결과를 도출하기 위해 체크리스트 형태로 구성하여 품질검사표의 측정 항목에 대한 값을 도출하기 위해 활용한다. <Table 14>에 NAC의 기밀성 부특성의 '정보흐름 통제' 메트릭에 대한 점검표의 구성을 나타내었다.

<Table 14> Checklist of Information Flow Control

No	Function name	The function controlled
1	Function no.1 related to information flow	V
2	Function no.2 related to information flow	
3	Function no.3 related to information flow	V
4	Function no.4 related to information flow	V
5	Function no.5 related to information flow	
…	…	…
the number of all functions related to information flow		A(the number of test case)
tge number of functions whose information flow is controlled		B(the number of 'V')
Result		(B/A)

4.5 평가 방법 종합



[Fig. 1] Analysis and evaluation process of security evaluation model

지금까지 제시한 NAC의 보안성 평가모델의 전체적인 분석 및 평가 과정은 [Fig. 1]과 같다. 메트릭의 값을 도출하기 위한 품질검사표의 세부 측정항목은 점검표를 이용하여 NAC 시스템의 실행을 통해 검토한다. 품질검사표의 계산식에 의해 메트릭의 값이 도출되면, 하나의 부특성을 구성하는 메트릭들의 값이 집계되어 부특성의 결과가 도출되고 최종적으로 부특성의 결과를 집계하여 보안성의 결과를 얻을 수 있다.

4.6 평가모델의 유용성

소프트웨어 제품의 품질특성으로서 ISO/IEC 25000 시리즈에서 기능적합성(Functional Suitability), 신뢰성(Reliability), 성능효율성(Performance Efficiency), 운영성(Operability), 보안성(Security), 호환성(Compatibility), 유지보수성(Maintainability), 이식성(Portability)을 정의하고 각 품질특성에 관한 부특성을 정의하고 있다. 이전 표준인 ISO/IEC 9126에서는 보안성을 기능성의 부특성으로 정의했으나 빈번한 보안 관련 개인정보 유출이나 해킹사고 등으로 보안성의 중요성이 제고되면서 다른 품질특성과 동등한 레벨로 격상되었다.

보안성의 중요성을 인식하여 품질평가 과정에서 중요도가 높아지고 좀 더 세분화된 평가가 가능해졌지만, 국내 소프트웨어 제품에 대한 품질평가 및 인증과정에서 활용하는 ISO/IEC 25000 시리즈 표준과 정보기술 보안 제품에 대한 평가에 관련된 ISO/IEC 15408 표준으로 이원화되어 있는 상황이다.

따라서 국내 소프트웨어 제품 시험·인증 기관에서도 기존에 기반을 두고 있는 표준인 ISO/IEC 9126[15, 16]과 ISO/IEC 25000 시리즈뿐만 아니라 ISO/IEC 15408 표준의 좀 더 체계적이고 세분화된 기준에 따라 보안성 평가 체계를 보완할 필요가 있다고 본다.

따라서 본 연구에서는 ISO/IEC 15408(공통 평가 기준)을 기반으로 한 NAC에 대한 보호 프로파일을 근간으로 소프트웨어 제품평가 관련 표준인 ISO/IEC 25000 계열의 품질특성/부특성 체계를 도입하여 보안성 메트릭을 구축하였다. 더불어 ISO/IEC 25041에 정의된 평가모듈 구성에 따른 품질검사표와 점검표를 구성하여 보안성 평가의 일원화를 통한 시너지 효과를 얻고자 하였다.

4.7 평가모델의 차별성과 의의

ISO/IEC 25000 모델을 이용한 소프트웨어 품질평가에서는 소프트웨어의 전반적인 특성을 망라한 품질특성·부특성 체계에 따라 평가를 수행할 수 있다는 장점이 있으나 정보보안이라는 분야에 특화된 제품을 평가하는 관점에서는 충분히 상세한 평가항목을 구축하고 있지 못하다는 약점이 있다. ISO/IEC 15408은 정보보안 제품의 특성을 충분히 반영한 평가체계를 구축하고 있으나 동시에 정보보안 제품의 특성에 치중하고 있다는 약점이 있다.

기존의 소프트웨어 품질인증은 보안성의 평가가 부특성 레벨에서 이루어졌다는 점에서 높아진 보안성의 위상을 충분히 반영하지 못하고 있다고 할 수 있다. 본 연구에서는 보안성의 위상을 품질특성 레벨로 격상한 ISO/IEC 25000 표준의 최근 동향을 반영하고 ISO/IEC 15408의 보안제품 평가에 대한 전문성을 고려하여 통합된 모델을 구축함으로써 품질평가의 표준화 동향을 반영하고 전문성 향상을 추구했다는 점에서 의미가 있다고 본다. <Table 15>에 기존의 평가기준과 제안하는 방법의 차별성과 장점에 대해 정리하였다.

<Table 15> Differentiation of Evaluation Model

	Existing evaluation model		The evaluation model of this study
ISO/IEC 25000	advantages	A comprehensive evaluation system for functionality, reliability, usability, efficiency, maintainability and portability	-Possession of expertise in security assessment of ISO/IEC 15408 -Reflecting recent trends in ISO/IEC 25000, which increased security to quality level -Combining the evaluation criteria of ISO/IEC 15408 and ISO/IEC 25000 security system
	Disadvantages	Not suitable for product evaluation that is specialized in information security	
		The quality certification authority has not yet reflected the latest standard trends that emphasize security.	
ISO/IEC 15408	advantages	Professional evaluation of information security products	
	Disadvantages	The evaluation of the overall characteristics of the product has not been performed and additional evaluation and certification is required.	

국내 소프트웨어 품질인증 기관에서는 ISO/IEC 9126, 25041, 25051 국제표준에 근거한 품질평가 모델을 기반으로 기능성, 신뢰성, 사용성, 효율성, 유지보수성, 이식성에 대한 시험을 실시하고 있다. 본 연구의 근간이 되는 ISO/IEC 25000 모델은 ISO/IEC 9126(품질특성 체계),

14598(품질평가 프로세스), 12119(소프트웨어 패키지 시험표준) 표준을 통합하여 재구성한 체계로서 보안성을 품질특성으로 격상하여 새로운 체계를 구축하였으므로 품질인증 기관에서 적용하기에도 무리가 없다는 점에서 활용성이 높다고 할 수 있다.

5. 결론

네트워크의 발전과 보급은 경제성을 제공하고 분산에 의한 신뢰성 향상 등 많은 장점을 제공하고 있지만 다양한 보안 문제가 야기되었고 이러한 보안 문제에 대처하기 위한 다양한 시스템들이 개발되어 활용되-고 있다.

과거의 정보보안은 대부분 외부로부터 유입되는 바이러스, 악성 코드, 해킹 등에 대응하는 것이 목적이었고 이를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템 등의 네트워크 보안 시스템이 주를 이루었다.

하지만 유·무선 네트워크 기술 발전, 다양한 단말기의 등장, 기업의 비즈니스 환경 확장 등의 변화로 유해 트래픽에 끊임없이 직면해야 하는 상황에 처하게 되었으며, 조직 내부에서의 공격에 의해 시스템 침해나 자산 유출 등이 발생하였다. 따라서 외부의 불법 접근을 차단하는 방법만으로는 내부 사용자로부터 전파되는 바이러스나 악성 코드, 주요 정보에 대한 불법적 접근 등에 대한 근본적인 차단이 어렵다. 이러한 한계를 극복하려는 대응으로 탄생한 것이 네트워크 접근제어(NAC) 이다.

NAC 시스템은 접근제어 및 인증, PC나 네트워크 장치의 통제, 해킹이나 웜, 유해 트래픽의 탐지 및 차단을 통해 보안사고를 방지한다. NAC 시스템이 본연의 역할을 제대로 수행하고 있는가를 평가하기 위해 정보보안 관련 제품의 보안 요구사항을 작성한 보호 프로파일이 구축되어 있다.

본 연구는 정보보안 제품 중 NAC의 보안성을 평가할 수 있는 메트릭의 개발에 관한 연구로서 NAC 시스템의 보호 프로파일 요구사항을 기반으로 ISO/IEC 25000 시리즈의 보안성 품질특성을 준용한 메트릭을 개발하였다.

본 연구를 통해 구축된 NAC 시스템에 대한 보안성 메트릭을 통해 정보보안 관련 제품의 보안성 평가를 관련 표준의 융합 체계를 통해 수행 가능할 것으로 기대하며, 평가 사례를 지속적으로 수집하여 보안성 메트릭의 검증을 통한 보안성과 타당성의 제고를 위해 지속적인 연구를 수행하고자 한다.

REFERENCES

[1] Byung-Jun Jeon, Deok-Byeong Yoon, Seung-Soo Shin, "Improved Integrated Monitoring System Design and Construction", Journal of Convergence Society for SMB, Vol. 7, No. 1, pp. 25-33, 2017.

[2] Seung-Hyun Paik, Sung-Kwang Kim, Hong-Bae Park, "Design and Implementation of Network Access Control for Security of Campany Network", Journal of the Institute of Electronics Engineers of Korea, Vol. 47, No. 12, p. 91, 2010.

[3] Hyung-Jun Mun, Yooncheol Hwang, Ho-Yeob Kim, "Countermeasure for Prevention and Detection against Attacks to SMB Information System - A Survey", Journal of Convergence Society for SMB, Vol. 5, No. 2, p. 1, 2015.

[4] Kang-Soo Lee, Young-Soo Kim et al.,, "Label-based Access Control System Protection Profile V2.0", Korea Information Security Agency & Hannam University, April, 2008.

[5] ISO/IEC 25010, "Systems and software engineering -- Systems and software Quality Requirements and Evaluation(SQuaRE) -- system and software quality models", 2011.

[6] Garter, "Gartner Market Guide 2016 - Network Access Control", May, 2016.

[7] NIS, MSIP, KCC, MOI, KISA, NSR, "2016, A white paper on national information protection", 2016.

[8] Hyo-Sik Yang, In-Oh Heon, "A Study the Test Methods and Evaluation Practices of Network Access Control System", Journal of Digital Convergence, Vol. 12, No. 9, pp. 159-168, 2014.

[9] Sang-Won Kang, In-Oh Jeon, Hae-Sool Yang, "Reliability Evaluation Model of Network Access Control(NAC) Product", Proceeding of Korea Academia-Industrial Cooperation Society, pp. 159-168, 2011.

[10] Kyong-Ho Choi, Sung-Kwan Kang, Kyung-Yong Chung, Jung-Hyun Lee, "A Study of Network 2-Factor Access Control Model for Prevention the Medical_Data Leakage", Journal of Digital Convergence, Vol. 10, No. 6, pp. 341-347, 2012.
[11] ISO/IEC 25020, "Software product Quality Requirements and Evaluation(SQuaRE) -- Measurement reference model and guide", 2007.
[12] ISO/IEC 25030, "Soiftware product Quality Requirements and Evaluation(SQuaRE) -- Quality requirements", 2007.
[13] ISO/IEC 25051, "Software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing", 2014.
[14] ISO/IEC 25041, "Systems and software engineering -- Systems and software Quality Requirements and Evaluation(SQuaRE) -- Evaluation guide for developers, acquirers and independent evaluators", 2012.
[15] ISO/IEC 9126-1(2001), 2(2003), Software engineering -- Product quality, 2001.

이 하 용(Lee, Ha Yong)

- 1993년 2월 : 강원대학교 전자계산학과 졸업(이학사)
- 1995년 2월 : 강원대학교 대학원 전자계산학과 SW공학전공(이학석사)
- 2005년 2월 : 호서대학교 벤처전문대학원 컴퓨터응용기술학과졸업(공학박사)
- 1996년 3월 ~ 2005년 8월 : 경희대, 경원대, 선문대, 호서대 컴퓨터공학부강사
- 1995년 5월 ~ 2002년 12월 : 한국SW품질연구소 선임연구원
- 2005년 9월 ~ 현재 : 서울벤처대학원대학교 교수
- 관심분야 : 소프트웨어공학(특히, S/W 품질보증과 품질평가, 품질감리, 객체지향 프로그래밍, 객체지향 분석과 설계, 컴포넌트기반 S/W 개발방법론, 품질평가)
- E-Mail : lhyazby@svu.ac.kr

양 효 식(Yang, Hyo Sik)

- 2009년 2월 : 호서대학교 컴퓨터공학과 졸업(학사)
- 2012년 2월 : 호서대학교 벤처대학원 정보경영학과 졸업(석사)
- 2015년 2월 : 호서대학교 벤처대학원 융합공학과 졸업(공학박사)
- 2009년 1월 ~ 2015년 12월 : 한국IT진흥(주), KT네트웍스(주), UL Korea(주), 이글루시큐리티(주) 근무
- 2016년 1월 ~ 현재 : 삼일회계법인 IT리스크&시큐리티 Senior Associate
- 관심분야 : 정보시스템 위험 및 보안감사, 물리보안 시스템, 소프트웨어 및 네트워크 보안, 정보서버 보안관리
- E-Mail : hyosyang@samil.com