http://dx.doi.org/10.14400/JDC.2016.14.5.341

VPN의 보안성 평가를 위한 CC와 ISO 관련 표준의 융합

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

Convergence of Related Standard of CC and ISO for Security Evaluation of VPN

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

요 약 VPN은 인터넷망을 이용하므로 데이터를 암호화하는 보안기술이 뒷받침되어야 하며 보안성에 대한 확신을 줄 수 있도록 표준에 기반을 둔 평가 기술이 뒷받침되어야 한다. 그러므로 연관된 표준을 기반으로 VPN의 보안성을 평가할 수 있는 방법을 체계화할 필요가 있다. 따라서 본 연구에서는 정보보호시스템의 인증을 위한 평가기준인 CC(Common Criteria)와 소프트웨어 품질평가 표준인 ISO의 보안성(기밀성, 무결성, 부인방지, 책임성, 인증성) 평가 부분을 접목하여 이를 통합한 보안성 평가 모델을 구축하고자 하였다. 이를 위해 VPN의 기반 기술과 보안성에 관한 품질 요구사항을 분석하여 두 국제표준의 품질특성과의 연관성을 고려한 평가모델을 개발하였다. 이를 통해 VPN의 보안성 품질수준을 평가하는 융합 모델을 구축할 수 있을 것으로 사료되며, 향후 VPN에 대한 평가사례의 축적을 통해 평가모델의 적합성과 타당성을 제고할 필요가 있다.

주제어 : 융합, 품질평가 모델, 보안성, 가상사설망, 평가모듈

Abstract Because VPN(Virtual Private Network) uses internet network, the security technique should support it and evaluation technique based on standard should support it. Therefore the method should be organized that can evaluate the security of VPN based on the related standard. In this study, we intended to construct the security evaluation model through combining CC(Common Criteria) which is a evaluation standard and a part of security(Confidentiality, Integrity, Non-repudiation, Accountability, Authenticity) evaluation of ISO which is the standard of software quality evaluation. For this, we analyzed the quality requirements about intra-technology and security of VPN and constructed the evaluation model related to the quality characteristics of two international standard. Through this, we are able to construct a convergence model for security evaluation of VPN. Through accumulating the evaluation practices for VPN in the future, the suitability and validity of the evaluation model must be improved.

Key Words : Convergence, Quality Evaluation Model, Security, Virtual Private Network, evaluation module

Received 4 April 2016, Revised 1 May 2016
Accepted 20 May 2016, Published 28 May 2016
Corresponding Author: Hyo-Sik Yang
(Samil PricewaterhouseCoopers IT Risk & Security)
Email: hyosyang@samil.com

ISSN: 1738-1916

1. 서론

VPN은 공중망 인프라를 공유하여 구축된 망으로 가상사설망(Virtual Private Network)을 의미한다. IP VPN으로 기업은 본사와 자사를 연결하는 인트라넷(intranet), 협력사와 연결되는 익스트라넷(extranet), 그리고 최근 들어 급증하고 있는 이동근무자와 재택근무자를 회사에 안전하게 연결시킬 수 있는 원격 접속망 등을 경제적으로 구축할 수 있게 되었다[1].

많은 기업들은 공중망을 이용하여 자사의 WAN을 백본처럼 이용하는 네트워크인 VPN을 구축하여 사용하고 있는데, 별도로 값비싼 장비나 소프트웨어를 구입・관리할 필요가 없어 비용 절감효과를 기대할 수 있다[2].

VPN은 정보보호를 위한 시스템으로서 제 역할을 다할 수 있도록 보안 요구사항을 국제 공통 평가 기준(CC : Common Criteria, ISO/IEC 15408)에 따라 작성된 보호프로파일(Protection Profile)[3]에 입각하여 제품을 개발하고 평가를 받거나, 혹은 개발된 제품의 제원을 보호 프로파일로 등록하고 평가를 받게 된다.

본 논문에서는 VPN의 기능성에 관한 품질평가를 위해 CC를 기반으로 한 VPN에 관한 보호프로파일과 ISO/IEC 25010 소프트웨어 제품평가에 관한 국제표준의 품질 체계를 기준으로 VPN의 보안성에 관한 품질 모델을 구축하였다.

본 논문의 2장에서는 VPN의 필요성과 보안성에 관한 품질평가 모델의 표준 동향에 대해 살펴보고 3장과 4장에서는 VPN의 보안성 품질특성과 이에 따른 보안성 평가 모델을 구축하고 5장에서 결론과 향후 연구 과제를 제시하였다.

2. VPN 품질평가 연구동향 및 관련 표준

2.1 VPN의 품질평가에 관한 연구동향

VPN의 품질평가와 관련해서 CC(ISI/IEC 15408)와 ISO/IEC 25000 시리즈의 소프트웨어 품질평가 표준을 기반으로 한 효율성 평가 융합 모델에 관한 연구로서 VPN의 시간반응성(Time Behavior), 자원효율성(Resource Utilization), 보안성능(Security Performance)에 대한 메트릭과 품질검사표 및 점검표를 구축한 연구가 있다[4].

또한, VPN 소프트웨어의 품질 특성에 따른 수준을 도출하기 위한 지표 개발 연구로 소프트웨어 품질평가 관련 표준인 ISO/IEC 9126과 패키지 소프트웨어 품질시험 지침에 관한 표준인 ISO/IEC 12119를 기반으로 하여 시험을 위한 표준 환경을 구축하고 결함내역을 도출하며 속성분석을 통해 VPN 소프트웨어의 품질수준을 평가하여 피드백하는 체계를 구축한 연구가 있다[5, 6].

VPN 같은 정보보안시스템에 대한 품질평가 관련 연구로는 지문인식 시스템의 성능효율성에 관한 연구[7]와 DRM 소프트웨어의 품질평가 모델 개발에 관련된 연구[8, 9]가 있으며, 그 밖에 ISO/UEC의 소프트웨어 품질평가 표준을 적용한 연구들이 다수 있다[10].

2.2 보안성 평가 모델의 표준 동향

소프트웨어 품질평가 관련 표준인 International Standard ISO/IEC 9126과 ISO/IEC 12119에서는 소프트웨어 품질특성으로 기능성(Functionality), 신뢰성(Reliability), 사용성(Usability), 효율성(Efficiency), 유지보수성(Maintainability), 이식성(Portability)의 6개 품질특성 중 기능성 품질특성에 부특성으로 보안성이 포함되어 있었으나 ISO/IEC 25010에서는 보안성이 품질특성으로 격상되고 그 부특성으로 기밀성(Confidentiality), 무결성(Integrity), 부인방지(Non-repudiation), 책임성(Accountability), 인증성(Authenticity)으로 변화되었다.

3. VPN의 보안성 평가항목

이 절에서는 ISO/IEC 25010 표준에 입각하여 보안성에 관한 품질특성을 VPN의 특성에 기반하여 구축하기 위해 VPN의 보안성에 관한 전반적인 평가항목을 체계화하였다.

3.1 VPN의 보안감사성

VPN의 보안감사성이란 보안과 관련된 행동에 대한 책임을 추적하기 위해 지식정보보안 제품에서 발생하는 관련 사건들의 감사 레코드를 생성, 기록, 검토하고 감사된 사건에 대한 잠재적 보안 위반을 탐지하고 대응행동을 수행하는 능력을 의미한다. 보안감사성은 보안 경보,

감사 데이터 생성, 사건과 사용자 연관, 규칙 위반 지적, 감사 검토, 저장소 보호, 대응 행동, 손실 방지의 평가항목을 가진다.

<Table 1> Security Audit Table

No.	Characteristics	Subcharacteristics	Name of Evaluation Item	Object of Evaluation Item
1	Security	Security Audit	Security Alert	When detecting security violations, VPN should get the reaction list.
2	Security	Security Audit	Audit data generation	The creation of a regulatory audit data
3	Security	Security Audit	Pointing out the violation of rules	When examining the case , system applys a set of rules and assess whether it can indicate a potential violation based on rules.
…	…	…	…	…

3.2 VPN의 암호지원

VPN의 암호지원이란 인터넷과 같은 공중망을 이용하여 사설 전용망의 효과를 얻기 위해서 VPN을 사용할 때 외부에 대한 보안을 통해 정보가 노출되는 것을 막기 위해 지원된다. 암호지원은 암호키 생성, 암호키 분배, 암호키 파기, 암호 연산의 평가항목을 가진다.

<Table 2> Encryption Support Table

No.	Characteristics	Subcharacteristics	Name of Evaluation Item	Object of Evaluation Item
1	Security	Encryption support	Encryption Key Generation	Evaluate whether system generates an encryption key according to the specified encryption key generation algorithm and the encryption key length.
2	Security	Encryption support	Encryption Key Distribution	Evaluate whether system distributes an encryption key according to the specified encryption key distribution method.
3	Security	Encryption support	Encryption Key Destruction	Evaluate whether system destroys encryption keys in accordance with a specified encryption key destruction method.
…	…	…	…	…

3.3 VPN의 사용자 데이터 보호

VPN의 사용자 데이터 보호란 정보흐름 관련 기능의 정보호름을 통제하고 객체에 대한 무결성 오류에 대해 사용자 데이터를 검사하고 오류 탐지시 대응행동을 수행하는 능력을 의미한다. 사용자 데이터 보호는 정보흐름 통제, 보안속성에 따른 통제의 평가항목을 가진다.

<Table 3> User Data Protection Table

No.	Characteristics	Subcharacteristics	Name of Evaluation Item	Object of Evaluation Item
1	Security	User data protection	Information Flow Control	Evaluate whether system controls information flow of information flow related functions.
2	Security	User data protection	Control based on security attributes	Evaluate whether system controls information flow based on security attributes.

3.4 VPN의 식별 및 인증

VPN의 식별 및 인증이란 해당 정보보호 제품의 관리자를 포함한 사용자의 신원을 식별 및 인증하고 인증 실패시 대응 행동을 제공하는 능력을 의미한다. 식별 및 인증은 인증실패 처리, 사용자 보안속성 유지, 비밀정보 생성, 사용자 인증, 인증 피드백 보호, 사용자 식별의 평가항목을 가진다.

<Table 4> Identification and Authentication Table

No.	Characteristics	Subcharacteristics	Name of Evaluation Item	Object of Evaluation Item
1	Security	Identification and Authentication	Authentication failure handling	Evaluate whether system detects a authentication failure and perform reactions.
2	Security	Identification and Authentication	Maintaining user security attributes	Evaluate whether system maintains regulatory security attribute lists for each user.
3	Security	Identification and Authentication	Generating secret information	Evaluate whether system provides a mechanism to verify to meet the regulatory permission criteria.
…	…	…	…	…

3.5 VPN의 보안관리성

VPN의 보안관리성이란 해당 지식정보보안 제품의 보안기능, 보안속성, 보안 관련 데이터, 보안 역할 등과 관련된 사항을 관리하는 능력을 의미한다. 보안관리성은 보안기능 관리, 보안속성 관리, 디폴트값 제공, 데이터 관

리 제한, 한계치 관리 제한, 관리기능 수행, 관리자 역할 유지의 평가항목을 가진다.

<Table 5> Security Manageability Table

No.	Characteristics	Subcharacteristics	Name of Evaluation Item	Object of Evaluation Item
1	Security	Security Manageability	Security Function Management	Evaluate whether system restrict so that only authorized administrators can manage the security functions.
2	Security	Security Manageability	Security Attribute Management	Evaluate whether system restricts so that only authorized administrators can manage the security attributes.
3	Security	Security Manageability	Provide Default Values	Evaluate whether system forces to provide the default values of security attributes.
…	…	…	…	…

3.6 VPN의 보안기능 보호

VPN의 보안기능 보호란 주기적 또는 관리자의 요구에 따라 무결성을 검증하는 능력을 의미한다. 보안기능 보호는 재사용 탐지, 재사용 대응, 자체 시험의 평가항목을 가진다.

<Table 6> Protection of Security Functions

No.	Characteristics	Subcharacteristics	Name of Evaluation Item	Object of Evaluation Item
1	Security	Security Function Protection	Detection of Reuse	Evaluate whether system detects the reuse of identified entity lists.
2	Security	Security Function Protection	Response to Reuse	Evaluate whether system implements the reaction when it detects the reuse of identified entity lists.
3	Security	Security Function Protection	Self Test	Evaluate whether system can test itself to verify the integrity of data and execution code.

3.7 VPN의 접근통제성

VPN의 접근통제성이란 시스템이 정보흐름을 중재하기 위해 관련 보안정책에 기반하여 패킷필터링 등을 통하여 외부망으로부터 내부망을 보호하는 능력을 의미한다. 접근통제성은 세션 잠금의 평가항목을 가진다.

<Table 7> Access Control Table

No.	Characteristics	Subcharacteristics	Name of Evaluation Item	Object of Evaluation Item
1	Security	Access Control	Lock Session	After a period of inactivity of administrator, Evaluate whether system emasculates the action by locking the interacting sessions

4. VPN의 보안성 평가모델

VPN은 지식정보보안 시스템으로서 이에 대한 평가는 공통 평가 기준(Common Criteria)을 근간으로 하면서 ISO/IEC 25000 시리즈[11, 12, 13, 14]의 품질평가 모델도 함께 고려되어야 한다. 따라서 본 연구에서는 ISO/IEC 25000 시리즈의 품질평가 모델과 공통 평가 기준을 함께 고려하여 보안성에 관한 부특성인 기밀성(Confidentiality), 무결성(Integrity), 부인방지(Non-repudiation), 책임성(Accountability), 인증성(Authenticity)을 포함하는 평가모델을 구성하였다.

본 논문에서는 ISO/IEC 25010의 보안성에 관한 품질특성을 도입하여 VPN의 보안성 평가를 위한 품질특성을 구축하는데 적용하였다. <Table 8>에 보안성에 관한 부특성의 개념을 정리하였다.

<Table 8> Quality Characteristics System about Security

Quality Characteristics	Quality Subcharacteritics	Concept
Security	Confidentiality	Degree to which a product or system ensures that data are accessible only to those authorized to have access.
	Integrity	Degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data.
	Non-repudiation	Degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later.
	Accountability	Degree to which the actions of an entity can be traced uniquely to the entity.
	Authenticity	Degree to which the identity of a subject or resource can be proved to be the one claimed.

평가모듈은 메트릭에 대해 ISO/IEC 25041의 평가모듈 형식에 의거하여 소프트웨어 품질평가에 관한 제반

사항을 문서화하는 형식에 관한 체계이다. 평가모듈에 대해 기본적인 사항을 4.1에서 기술한다.

4.1 평가모듈의 체계와 개발 내역

4.1.1 평가모듈의 체계

평가모듈은 품질시험에 관한 제반사항을 문서화한 것으로 ISO/IEC 25041의 평가모듈 구성에 따라 작성하였다. 품질평가 모듈의 체계는 <Table 9>와 같다.

<Table 9> The System of Quality Evaluation Module

Configuration Item		Contents
Outline	Concept of metric	The basic concept of evaluation modules
	Measurement purposes	what you want to get through the measurement of the evaluation module
	Metric category	where the metric belongs
	Term Explanation	explanation of related terms
Coverage	application target	target such as document or software
	Necessary resources	Tools/resources required to apply the metric
	Techniques	Testing techniques that can be applied
	Considerations	Relevant information to be considered when apply evaluation modules
Reference		Related Documents that metrics are derived
Metric	Measurement items	Data items to be measured
	Measurement method	specific measure for the measure item to configure the metric
	Expression	definition of expression using the data items
Application Procedures		Description on specific procedures and method to perform the test
Results interpretation and reporting	Mapping of the measurements	The range of metric results
	Interpretation of the measurement results	Provide guidance about how to interpret the measurement results
	Reporting requirements	items to be reported as a document on the measurement results

4.1.2 메트릭 개발 내역

본 연구를 통해 <Table 10>에 나타낸 것처럼 VPN의 보안성에 관한 메트릭을 개발하였다.

<Table 10> The Measure about Security of VPN

Characteritics	Subcharacteristics	Item	Related Items
Security	Confidentiality	Encryption Key Generation	Evaluate whether system generates an encryption key according to the specified encryption key generation algorithm and the encryption key length.
		Encryption Key Distribution	Evaluate whether system distributes an encryption key according to the specified encryption key distribution method.
		…	…
	Integrity	Detection of Reuse	Evaluate whether system detects the reuse of identified entity lists.
		Response to Reuse	Evaluate whether system implements the reaction when it detects the reuse of identified entity lists.
		…	…
	Non0repudiation	Nonrepudiation of Origin	It provides the ability to prevent a sender from denying sending behavior.
		Nonrepudiation of Receipt	It provides the ability to prevent a receiver from denying receiving behavior.
		…	…
	Accountability	Security Alert	When detecting security violations, VPN should get the reaction list.
		Audit data generation	The creation of a regulatory audit data
		…	…
	Authenticity	Authentication failure handling	Evaluate whether system detects a authentication failure and perform reactions.
		Maintaining user security attributes	Evaluate whether system maintains regulatory security attribute lists for each user.
		…	…

4.2 품질검사표

소프트웨어의 품질을 평가하기 위해서는 품질평가 현장에서 용이하게 적용할 수 있도록 ISO/IEC 25041의 평가모듈 구성체계에 따른 품질검사표를 구성하여 적용할 필요가 있다. 품질검사표에는 <Table 11>과 같이 메트릭명과 개념, 측정항목, 메트릭의 계산식, 결과의 영역, 결과값, 문제점 기술 부분 등으로 구성되어 있다.

<Table 11> An Example of Quality Inspection Table

Measure name		How many list of response action are taken when security violation was detected?		
Security Alert				
Measurement items	A	the number of detection of security violation		
	B	the number of case that is taken of list of response action		
expression		- Security Alert = B/A		
The range of results		0 ≤ Security Alert ≤ 1	result value	
problem				

품질검사표는 다수의 측정항목으로 구성되어 점검표를 통해 측정항목의 값을 도출하고 측정항목으로 구성된 계산식을 통해 메트릭의 결과값을 도출한다. 결과값의 범위는 정규화하여 0과 1 사이의 값으로 사상될 수 있도록 계산식을 결정하는 것이 좋으며 그렇지 못할 경우에는 계산식의 값에 대한 범위에 따라 평점 수준을 결정하고 결과값에 대해 평가모듈에 정의한 바에 따라 해석할 수 있다.

4.3 점검표

점검표는 품질검사표를 이용하여 측정항목에 대한 측정을 수행하기 위해 작성된 테스트 케이스의 시험 목록이다. <Table 12>는 VPN의 책임성 부특성의 '보안경보' 메트릭에 대한 점검표의 예를 보여주고 있다.

<Table 12> Checklist of TCP Process Performance

No	Test case	Test result
1	Detection of security violation : 1st	V
2	Detection of security violation : 2nd	
3	Detection of security violation : 3rd	V
…	…	…
the number of detection of security violation		A(the number of test case)
the number of case that is taken of list of response action		B(the number of 'V')
Result		(B/A)

4.4 평가모델의 평가 과정

4.4.1 점검표와 품질검사표의 작성

평가에서 첫 번째 과정은 <Tab.le 12>와 같은 점검표를 이용하여 사례를 테스트하고 체크리스트 형태로 작성하는 것이다. 작성된 점검표에 의해 측정 항목의 값(A, B 등)이 도출되고 <Table 11>과 같은 품질검사표에 제시된 계산식(expression)에 따라 메트릭의 결과값이 산출된다.

4.4.2 부특성의 결과 도출

품질검사표에 따른 메트릭의 결과값을 이용하여 <Table 13>과 같이 보안성의 각 부특성들에 대한 메트릭의 평균을 구하여 부특성의 결과값을 도출한다.

<Table 13> Result of Subcharacteristics

Characteritics	Subcharacteristics	Item			Mean
Security	Confidentiality	Encryption Key Generation	Encryption Key Distribution	…	0.85
		0.9	0.8	…	
	Integrity	Detection of Reuse	Response to Reuse	…	0.85
		0.8	0.9	…	
	Non0repudiation	Nonrepudiation of Origin	Nonrepudiation of Receipt	…	0.80
		0.7	0.9	…	
	Accountability	Security Alert	Audit data generation	…	0.78
		0.8	0.7	…	
	Authenticity	Authentication failure handling	Maintaining user security attributes	…	0.87
		0.9	0.9	…	

4.4.3 보안성 품질특성의 결과 도출

보안성 품질특성의 결과를 도출하기 위해 품질부특성의 결과값에 대해 백분율로 나타낸 값을 합산하여 평균을 산출하여 획득된 점수를 나타내면 <Table 14>와 같이 최종 점수를 획득할 수 있다. 평가 결과를 도출하는 과정에서 각 메트릭이나 품질부특성에 대해 중요도를 고려하여 가중치를 부여할 수도 있고 평가 결과값에 대한 해석은 평가 대상 시스템에 따라 평점수준을 설정하여 적용할 수 있다.

<Table 14> Result of Quality Characteristics about Security

Quality Subcharacteristics	Confidentiality	Integrity	Non0repudiation	Accountability	Authenticity
Result	85	85	80	78	87
Mean	83				

4.5 평가모델의 검토

소프트웨어 제품의 보안성에 관해 적용할 수 있는 품질평가 표준으로는 소프트웨어의 전반적인 품질특성을 다루는 체계 속에서 그 중 하나인 보안성 품질특성을 평가할 수 있는 ISO/IEC 9126, ISO/IEC 12119 그리고 이 표준들을 통합한 표준인 ISO/IEC 25000 시리즈가 있으며 정보보호 제품에 특화된 평가 기준을 제정한 ISO/IEC 15408(CC) 표준이 있다. 전자의 표준은 소프트웨어 제품의 보안성에 관한 상세한 품질수준을 평가하기 어려울 수 있고 후자의 경우엔 소프트웨어 제품의 품질을 포괄적인 시각에서 평가하기 어려운 단점이 있다.

기존의 선행연구에서는 ISO/IEC 9126이나 ISO/IEC 12119를 기반으로 한 VPN의 품질평가 모델을 구축함으로써 정보보호시스템의 보안성 품질평가라는 관점에서 상세한 수준의 평가를 하기에 다소 미흡한 점이 있었다.

본 연구에서 제안한 보안성 평가모델은 공통 평가 기준(ISO/IEC 15408)에 따른 VPN에 관한 보호 프로파일과 소프트웨어 제품평가에 관한 국제표준인 ISO/IEC 25010을 근간으로 하여 구성하였으며 보안성에 관한 25010 표준의 품질특성 체계를 기반으로 15408 표준의 품질요구사항을 융합하여 VPN에 관한 보안성 품질평가 모델의 체계화를 모색하였다. 또한, ISO/IEC 25041에 따라 평가모듈과 품질검사표를 구성하고 품질검사표의 측정항목을 도출하기 위한 점검표를 구성함으로써 타당성을 제고할 수 있도록 하였다.

소프트웨어 품질에 관한 표준의 최근 추세가 보안과 관련된 특성을 중요시한다는 점을 고려하여 보안성 모델을 구축하면서 공통평가 기준에 따른 보안성능을 포함하여 표준화의 추세를 반영한 보안성 평가 모델을 구축하였다는 점에서 의의가 있다고 본다.

5. 결론

인터넷의 발전과 보급은 다양한 보안 문제를 야기하였고 이로 인해 지식정보보안에 대한 인식제고로 VPN과 같은 보안 문제에 대처하는 시스템들이 개발되었다. 더불어 지식정보보안시스템 등에 대해 국제표준의 보안 요구 사항을 근간으로 품질수준을 평가하기 위한 다양한 노력이 활발히 진행되어 왔다.

지식정보보안 관련 제품의 용도 및 특성에 따라 적합한 보호 프로파일(protection profile)이 작성되었으며, 같은 유형의 지식정보보안 제품의 평가에 적용할 수 있다.

본 연구에서는 지식정보보안 제품 중에서 VPN의 보안성 평가에 관한 모델 개발 연구로서 VPN의 보호 프로파일에 따른 요구사항을 준수하면서 소프트웨어 제품평가에 관한 국제표준인 ISO/IEC 25000 시리즈의 보안성 품질특성을 기반으로 평가모델을 구성하였다.

본 연구에서 제안된 VPN에 대한 보안성 품질평가 모델을 통해 일반적인 소프트웨어 제품의 보안성 평가에서 상세히 다룰 수 없는 지식정보보안 관련 제품의 보안성에 대한 평가를 국제표준의 체계를 반영하여 수행할 수 있을 것으로 기대한다.

향후, VPN의 보안성에 대한 평가사례의 수행을 통해 객관성과 타당성을 갖춘 보안성 평가체계로 발전시키기 위한 지속적인 연구를 수행할 필요가 있다.

REFERENCES

[1] Bong-Hyun Kim, Dong-Uk Cho, “Trend and Prospect of Network Security Technology”, The Journal of Korean Institute of Communications and Information Sciences(J-KICS)NIPA), Vol. 31, No. 4, 2014.

[2] Jong-Hoon Han, Jung-Woo Lee, Sung-Han Park, “A Dynamic Key Lifetime Change Algorithm for Performance Improvement of Virtual Private Networks”, Journal of the Institute of Electronics Engineers of Korea, Vol. 42, No. 10, p. 31, 2005. 10.

[3] Kang-Soo Lee, Young-Soo Kim et al.,, “Virtual Private Network Protection Profile V2.0”, Korea Information Security Agency & Hannam University, 2008. 4.

[4] Ha-Yong Lee, Jung-Gyu Kim, "Efficiency Evaluation Convergence Model of Virtual Private Network based on CC and ISO Standard", Journal of Digital Convergence, Vol.13, No.5, pp. 169-176, 2015. 5.

[5] Myung-Seong Yim, “Development of Measures of Information Security Policy Effectiveness To

Maximize the Convergence Security", Journal of the Korea Convergence Society, Vol. 5, No. 4, pp. 27-32, 2014.

[6] Kyung-Muk Kim, Hae-Sool Yang, "VPN(Virtual Private Network) SW's examination example analysis", Journal of academia-industrial technology, Vol.11, No.8, 2010.

[7] Ha-Yong Lee, Jung_Gyu Kim, "Quality Evaluation Model about Efficiency for Fingerprint Recognition System", Journal of digital Convergence, Vol. 12, No. 6, 2014.

[8] Ha-Yong Lee, Jung-Gyu Kim, "Quality Evaluation Model for Security of DRM Software", The Journal of Policy & Management, Vol. 11, No. 5, 2013. 5.

[9] Sang-Won Kang, In-Oh Jeon, Hae-Sool Yang, "Usability Quality Evaluation Plan of DRM Softwares", Proceedings of The Korea Academia-Industrial Cooperation Society, 2010. 11.

[10] 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, pp. 323-330, 2013.

[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 25040, "Systems and software engineering – Systems and software Quality Requirements and Evaluation(SQuaRE) -- Evaluation process", 2011.

[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] yong-won kim, "A study on Convergent & Adaptive Quality Analysis using DQnA model", Journal of the Korea Convergence Society, Vol. 5, No. 4, pp. 21-25, 2014.

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 ~ 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)

- 2008년 2월 : 호서대학교 컴퓨터공학과 졸업(학사)
- 2012년 2월 : 호서대학교 벤처전문대학원 정보경영학과 졸업(석사)
- 2015년 2월 : 호서대학교 벤처대학원 융합공학과 졸업(공학박사)
- 2003년 1월 ~ 2015년 12월 : 한국IT진흥(주), KT네트웍스(주), UL Korea(주), 이글루시큐리티(주) 근무
- 2016년 1월 ~ 현재 : 삼일회계법인 IT리스크&시큐리티 Senior Associate
- 관심분야 : 소프트웨어 프로세스 인증 및 시험, 물리보안 시스템, 소프트웨어 및 네트워크 보안, 정보서버 보안관리
- E-Mail : hyosyang@samil.com