https://doi.org/10.14400/JDC.2017.15.12.303

통합보안관리시스템의 보안성 메트릭 개발

양효식
삼일회계법인 IT Risk & Security

Development of Security Metrics of Enterprise Security Management System

Hyo-Sik Yang
Samil PricewaterhouseCoopers IT Risk & Security

요 약 신생 정보기술의 등장에 따른 새로운 보안 위협에 대처하기 위해 기업은 통합보안괸리(Enterprise Security Management)시스템을 도입하고 솔루션 간 상호연동을 통해 중복투자나 자원 낭비를 줄이고 보안 위협에 대처하고 있다. 이에 따라 통합보안관리시스템이 보안성을 충족시킴을 입증하기 위해 관련 표준을 근거로 한 보안성 평가 메트릭의 구축이 필요한 실정이다. 따라서 본 연구에서는 통합보안괸리시스템에 대한 보안성을 평가할 수 있는 메트릭을 구축하기 위해 통합보안괸리시스템의 보안성 품질 관련 요구사항을 분석하고 충족 정도를 측정할 수 있는 메트릭을 구축하였다. 본 메트릭을 통해 ISO/IEC 15408과 ISO/IEC 25000 표준에 부합하는 보안성 평가의 일원화를 통한 시너지 효과를 얻을 수 있다. 이를 통해 통합보안관리시스템의 보안성 품질수준을 평가하는 모델을 구축하고, 향후 통합보안괸리시스템에 대한 평가방법의 표준화를 기할 수 있을 것으로 사료된다.

주제어 : 통합보안관리, 보안성, 메트릭, 품질평가, 품질 요구사항

Abstract As new information technology emerges, companies are introducing an Enterprise Security Management system to cope with new security threats, reducing redundant investments and waste of resources and counteracting security threats. Therefore, it is necessary to construct a security evaluation metric based on related standards to demonstrate that the Enterprise Security Management(ESM) System meets security. Therefore, in order to construct a metric for evaluating the security of the ESM, this study analyzed the security quality related requirements of the ESM and constructed a metric for measuring the degree of satisfaction. This metric provides synergies through the unification of security assessments that comply with ISO/IEC 15408 and ISO/IEC 25000 standards. It is expected that the evaluation model of the security quality level of ESM will be established and the evaluation method of ESM will be standardized in the future.

Key Words : Enterprise Security Management, Security, Merics, Quality Evaluattion, Quality Requirements

1. 서론

보안이 이슈화되고 관리해야 할 보안장비가 늘면서 장비들의 로그가 증가하고 이에 따라 효과적인 관리 및 모니터링 방안이 요구되었다. 고성능 보안 솔루션들을 어떻게 체계적으로 중앙집중적으로 운영・관리하여 전

Received 11 October 2017, Revised 27 November 2017
Accepted 20 December 2017, Published 28 December 2017
Corresponding Author: Hyo-Sik Yang
(Samil PricewaterhouseCoopers IT Risk & Security)
Email: hyosyang@samil.com

ISSN: 1738-1916

문화되고 단일화된 관리를 통해 양질의 보안 서비스를 제공하는가에 대한 새로운 요구가 발생하여 통합된 모니터링 및 관리의 필요성에 따라 ESM(Enterprise Security Management : 통합보안관리) 시스템이 도입되었다[1].

방화벽(Firewall), 침입탐지시스템(IDS), 침입방지시스템(IPS), 분산서비스거부(DDoS) 장비 등 보안 관련 장비는 계속 늘고 있지만 보안 업무를 수행하는 자원에는 한계가 있기 마련이며 이러한 제한적인 환경에서 효율적으로 보안관리 업무를 제공할 수 있도록 하려면 통합관리 방안이 필요하다. ESM은 보안장비를 통합·관리할 수 있도록 하기 위하여 보안 이벤트를 수집하고 관리하며 수집된 이벤트를 통합적으로 관리하고 분석하는 시스템이라 할 수 있다[2].

이러한 중요한 역할을 하는 ESM 시스템의 가장 핵심적으로 평가해야 할 부분은 보안성 품질에 대한 수준을 어느 정도 보증하는가일 것이다.

이에 따라 ESM 시스템이 보안성 품질 수준을 어느 정도 충족시키는가를 검증하기 위한 타당성 있는 근거가 요구된다. 따라서 보안성 품질 관련 표준을 근거로 한 품질측정 메트릭을 구축할 필요가 있다.

따라서 본 연구에서는 ESM 시스템의 보안성을 측정할 수 있는 메트릭을 구축하기 위해 ESM 시스템에 관한 품질표준들을 기반으로 통합 모델을 구축하고자 하였다. 이를 위해 ESM 시스템의 보안성 품질 관련 요구사항을 분석하여 요구사항의 충족 정도를 측정할 수 있는 메트릭을 구축하였다. 이를 통해 통합보안관리시스템의 보안성 관련 품질수준 평가 모델을 구축하고, 향후 통합보안관리시스템에 대한 평가방법의 표준화를 기할 수 있을 것으로 사료된다.

본 논문의 2장에서는 기업의 사이버 보안 실태에 대해 소개하고 3장에서는 ESM 시스템의 보안성 특성과 관련된 평가항목을 분석하고 4장에서는 ESM 시스템의 보안성에 대한 평가 메트릭을 구축하며 5장에서 결론과 향후 연구 과제를 기술하였다.

2. 기업 보안 실태 및 동향

2.1 사이버 위협 동향[3]

2017년도 1분기에는 랜섬웨어(ransomware), 피싱(phishing)·스미싱(smishing), IoT(Internet of Things) 취약점 등 기존의 사이버 위협이 계속되었다. 2분기에는 해커들의 사이버 공격으로 정상 운영되던 인터넷 서비스의 종료나 회사의 파산 위기 등이 발생하였으며 1분기와 마찬가지로 랜섬웨어, APT(Advanced Persistent Threat) 공격, IoT 악성코드 및 제로데이 취약점을 이용한 해커의 공격 등 다수의 사이버 위협들이 실제 사고로 이어졌다.

<Table 1>에서처럼 2017년도 2분기에 가장 유행한 악성코드는 랜섬웨어로서 1분기 972건 대비 약 3.5배 증가한 3,542건으로 집계되었다.

<Table 1> Status of Ramsomeware Complaints Received

Division	2015 (Quarter)				2016 (Quarter)				2017 (Quarter)	
	1	2	3	4	1	2	3	4	1	2
Complaints received	0	127	58	585	176	353	197	712	972	3,542
Sum	770				1,438				4,514	

2.2 기업의 사이버 보안 실태

보안감사 업체인 Positive Technologies는 2016년에 수행한 보안감사에서 기업 시스템 중 47%에서 심각한 취약점이 발견되었다고 발표하였다[4].

그 중에서 시스템의 잘못된 설정 및 구성 취약점이 40%, 웹 응용프로그램 소스코드 오류가 27%, 보안 업데이트 및 패치 미흡이 20% 순으로 나타났다. 외부자 침입 테스트에서는 55%의 시스템에서 기업 인프라를 완전히 제어할 수 있었으며, 내부 침입 테스트에서는 거의 모든 시스템을 제어하는데 성공하였다.

최근에는 MS 윈도의 취약점을 악용한 워너크라이(wannacry) 랜섬웨어로 인해 보안 업데이트 및 패치에 대한 중요도가 부각되었다.

보안감사의 대상 중 취약한 시스템들에서 마지막 업데이트 날짜는 평균 9년 전으로 관리자들의 정보보안 인식의 변화가 필요한 상황이었다. 해당 취약점에 대한 피해 예방을 위해서는 관리자 및 담당자들의 보안인식 제고가 가장 선행 되어야 할 점이다.

3. ESM의 보안성 평가항목

소프트웨어 제품평가에 관련된 국제표준은 ISO/IEC 9126[5, 6]으로부터 발전한 25010[7]이며 본 연구에서는 이 표준의 보안성 품질특성을 근간으로 하고 CC(Common Criteria(공통 평가기준))[8, 9]로부터 도출된 ESM 시스템에 대한 보호프로파일[10]을 융합하여 ESM 시스템에 대한 평가체계와 메트릭을 구축하였다. CC와 ISO/IEC 25000 시리즈 표준을 통합하기 위한 연구는 최근에 활발히 이루어지고 있다[11, 12].

ESM 시스템의 보안성에 관한 품질특성과 메트릭을 구축하기 위해 먼저 ESM의 보안성에 관한 평가항목을 체계화하였다.

3.1 보안감사성

보안감사는 보안과 연관된 행동에 대한 사건의 탐지, 감사데이터의 생성과 저장 및 분석, 보안을 위반한 사건에 대한 분석 및 대응 등과 관련된 감사이다. 감사데이터의 예에는 특정 기간에 대한 시스템 활동, 특정 각간 중에 수정된 개체의 목록, 사용자에게 할당된 역할, 특정 사용자 계정에 대해 수행된 작업, 실패한 프록시 세션 등이 있다.

ESM 시스템에서의 보안감사 관련 측정항목으로는 보안 경보, 보안 대응, 감사 데이터 수집, 감사 데이터 생성, 사용자 신원 연관, 잠재적 위반 분석, 복잡공격 학습, 감사 검토, 선택 가능한 감사검토, 감사 증적 저장소 보호, 감사 데이터 손실 예측시 대처 행동, 감사 데이터의 손실 방지 등의 평가항목이 있다. <Table 2>에 보안감사성에 관한 평가항목을 기술하였다.

<Table 2> Table of Security Auditability

No.	Characteristic	Sub-Property	valuation Item Name	Meaning
1	Security	Security Audit	Security alarm	A list of actions should be taken when detecting potential security violations against audit data.
2			Security Response	A list of actions to minimize confusion should be taken when detecting security violations.
3			Audit data collection	Provide the ability to collect audit data information.
4			Audit data generation	Audit record generation and related audit information of auditable events should be recorded.
5			User identity association	It should be possible to correlate the identity of the triggering user with the event.
6			Potential violation analysis	A set of rules for audited events should be applied to indicate potential violations.
7			Complex attack learning	When a signature case or sequence of events is compared and matched, a potential violation should be indicated.
…			…	…

3.2 사용자 데이터의 보호

사용자 데이터에 대한 보호와 관련된 핵심 활동은 사용자 데이터 보호정책이나 형태의 수립, 사용자 데이터의 유출 방지, 전송되는 사용자 데이터의 비밀성과 무결성 보호 등을 들 수 있다.

ESM 시스템에서의 사용자 데이터 보호 관련 측정항목으로는 부분적인 접근통제, 보안속성에 따른 접근통제, 보안속성 없는 사용자 데이터 유입, 기본적인 내부전송 보호 등의 평가항목이 있다. <Table 3>에 사용자 데이터 보호에 관한 평가항목을 기술하였다.

<Table 3> Table of User Data Protection

No.	Characteristic	Sub-Property	valuation Item Name	Meaning
1	<Security>	<User data protection>	Partial Access Control	The access control security policy should be enforced on the list of operations between subjects and objects covered by subject, object, and security function policy.
2				
3			Access Control based on security attributes	For each object, list of subjects, objects, and objects, you should enforce the Asymptotically Controlled Security Function policy on the object based on the appropriate security attributes.
4			User Data Flow-in without Security Attribute	The security policy for access control should be enforced when the user data which were controlled by the security function policy is imported from outside the evaluation target.

5			Basic internal transport protection	Access control is essential to prevent exposure or alteration of user data transmission.
…			…	…

3.3 식별과 인증

식별 및 인증에 관련된 핵심 활동은 사용자의 신원을 식별하거나 인가된 사용자를 인증하고 사용자에게 부여된 권한을 결정하거나 사용자에게 관련된 보안속성을 정확하게 연결하는 것 등을 들 수 있다.

ESM 시스템에서의 식별 및 인증 관련 측정항목으로는 인증 실패 대처, 사용자 속성 정의, 비밀정보 검증, 인증, 식별 등의 평가항목이 있다. <Table 4>에 식별과 인증에 관한 평가항목을 기술하였다.

<Table 4> Table of Identification and Authentication

No.	Characteristic	Sub-Property	valuation Item Name	Meaning
1	<Security>	<Identification and Authentication>	Handling of Authentication failure	The administrator shall detect a specified number of failed authentication attempts.
2			Define user attributes	You should maintain a list of identities, roles, and user security attributes for each user.
3			Verification of confidential information	Provide a mechanism to verify that the secret information satisfies the defined acceptance criteria(minimum length of password, combination rule, change period, etc.)
4			Authentication	Before the administrator authentication, the administrator should be allowed to list the actions to be performed on behalf of the administrator and successfully authenticate the administrator before allowing any action other than the action list.
5			Identification	Before administrators can be identified, a list of actions to be performed on behalf of the administrator is allowed, and the administrator must be successfully identified before any action other than the action list is allowed.
…			…	…

3.4 보안관리성

보안관리성에 관련된 핵심 활동은 보안기능, 보안속성, 데이터 관리 및 보안역할 정의 등을 들 수 있다.

ESM 시스템에서의 보안관리성 관련 측정항목으로는 보안기능의 관리, 보안속성 관리, 정적 속성 초기화, TSF 데이터 관리, 관리기능 명세, 보안역할 등의 평가항목이 있다. <Table 5>에 보안관리성에 관한 평가항목을 기술하였다.

<Table 5> Table of Security Manageability

No.	Characteristic	Sub-Property	valuation Item Name	Meaning
1	<Security>	<Security Manageability>	Security Function Management	It should be possible to determine, suspend, initiate, and change the behavior of only the authorized roles for the function of the function list.
2			Security Attribute Management	It should be possible to query, modify and delete the security attributes of the security attribute list only within the authorized role.
3			Static attributes initialization	You must enforce access control to provide a limited default value for security attributes.
4			Data Management	Only authorized roles should be able to query, modify, delete, and delete data lists.
5			Management Functional Specification	It shall be able to perform the management function of the management function list provided by the security function.
6			Security Role	It should be able to maintain authorized roles and associate roles with administrators.
…			…	…

3.5 보안기능(TSF) 보호

보안기능 보호에 관련된 핵심 활동은 보안기능을 제공하는 메커니즘과 데이터에 대한 무결성 및 보안기능과 상호작용하는 외부 실체에 대한 시험 등을 들 수 있다.

ESM 시스템에서의 보안기능 보호 관련 측정항목으로는 내부전송 TSF 데이터의 기본적인 보호, TSF 자체 시험 등의 평가항목이 있다. <Table 6>에 보안기능(TSF)보호에 관한 평가항목을 기술하였다.

<Table 6> Table of Security Function Protection

No.	Characteristic	Sub-Property	valuation Item Name	Meaning
1	<Security>	<Security Function Protection>	Basic Protection	Protect your security function data from nannies or changes.
2			TSF Self Test	Self-test should be executed at start-up, periodically, and at the request of the administrator.

3.6 접근통제성

접근통제성에 관련된 핵심 활동은 사용자 세션에 대한 통제이다. 즉, 사용자와 컴퓨터 간에 활성화된 접속 상태에 대한 통제를 말한다.

ESM 시스템에서의 접근통제성 관련 측정항목으로는 TSF에 의한 세션 잠금 평가항목이 있다. <Table 7>에 접근통제성에 관한 평가항목을 기술하였다.

<Table 7> Table of Access Control

No.	Characteristic	Sub-Property	valuation Item Name	Meaning
1	<Security>	<Access Control>	Session Locking	If there is no authorized administrator activity for a fixed time, the interactive session should be locked.

4. ESM 시스템의 보안성 평가모델

ESM 시스템은 정보보호시스템의 일종으로서 본 연구에서는 ESM 시스템을 평가하기 위해 공통 평가기준을 기반으로 하고 ISO/IEC 25000[13, 14, 15, 16] 관련 품질평가 모델도 아울러 고려해야 한다. 본 연구에서는 ISO/IEC 25000과 공통 평가기준의 관련 품질평가 체제를 함께 참조하여 보안성 품질에 연관된 부특성인 기밀성(Confidentiality) 및 무결성(Integrity), 그리고 책임성(Accountability) 및 인증성(Authenticity)에 관해 평가 가능한 모델을 구축하였다. <Table 8>에 보안성에 관한 부특성의 개념을 정리하였다.

평가모듈은 평가 척도에 대해 ISO/IEC 25041[17]의 평가모듈(evaluation module) 형식에 입각해서 소프트웨어 품질을 평가하기 위한 방법을 문서로 구축하는 형식을 정리한 체계이다.

<Table 8> Quality Characteristics System about Security

Quality Characteristic	Quality Sub-Property	meaning
Security	Confidentiality	Only those authorized by the owner of the information to protect sensitive information from unauthorized individuals or organizations have access to the information.
	Integrity	Accuracy and completeness should be protected so that information is not altered or destroyed in an unauthorized manner when storing and transmitting information.
	Accountability	This means the degree of ensuring that the behavior of each individual can be tracked uniquely.
	Authenticity	It means the degree to which a subject or object can be guaranteed to be correct.

4.1 평가모듈의 형식

평가모듈은 평가방법에 관한 제반 사항에 대해 문서화한 결과물이다. 즉, 평가모듈이란 메트릭의 개념은 무엇이고 메트릭을 이용해 어떻게 평가할 것인가, 평가결과로 도출된 값에 대해 어떻게 평점을 매기고 그 의미를 해석할 것인가 등에 대해 전반적인 내용을 정리하여 품질평가 시 활용할 수 있도록 만들어진 문서라 할 수 있다. ISO/IEC 25041에는 평가모듈의 제반사항을 어떤 구성과 내용으로 만들어야 하는가를 <Table 9>와 같은 내용으로 정의하고 있다.

<Table 9> The Content of Quality Evaluation Module

Configuration	Content
Outline	In the outline, the concept of the metric and the purpose of what to obtain through the measurement, which category of the metric belongs, and the explanation of the new term constituting the metric.
Coverage	In the scope of the application, what kind of documents or software should be applied to the metrics, what tools and resources are needed to apply the metrics, techniques to be applied when testing the metrics, and considerations when applying the evaluation module .
Reference	The reference document describes from which basis the metric is derived.
Metric	This section defines what data to measure, how to measure specifically for each data item, and how to derive the results from the data to derive the results of the metric.
Application Procedures	This section describes the specific procedures and methods to be applied in the course of performing the test.
Result interpretation and reporting	The measured values as a result of the measurement can be expressed in various ranges. Determine the range of values to be rated for this value, present how the value should be interpreted, and summarize the key findings presented in the evaluation process.

4.2 메트릭의 개발 내역

본 연구에서는 ESM 시스템을 대상으로 ISO/IEC 25010의 품질특성 중 하나인 보안성 품질특성을 기반으로 그 특성을 구성하는 서브 특성인 기밀성, 무결성, 책임성, 인증성을 바탕으로 하여 공통 평가기준(CC)과의 통합을 시도한 메트릭을 구축하였다.

4.2.1 기밀성 관련 메트릭

<Table 10>에는 ESM 시스템의 보안성(품질특성) - 기밀성(부특성)에 관한 메트릭을 나타내었다.

<Table 10> The Metrics about Confidentiality of ESM

Characteritic	Sub-Property	Item	Related Items
Security	Confidentiality	Audit review	ESM system should offer the authorized system administrator with the ability to read audit records that are made suitable for interpretation.
		Selectable audit review	ESM system should provide audit data selection based on logical criteria.
		Partial access control	ESM system must control access to the operations list between subjects and objects by force.
		Access control based on security attributes	ESM system must enforce information flow control according to the list of controlled subjects and objects, the subject security attributes, and the types of information security attributes.
		User data entry without security attributes	ESM system must forcibly enforce user data coming from the outside and ignore the related security attributes.
		Basic internal transport protection	When user data is transferred between physically separate parts, ESM system should control access so that user data is not exposed or altered.
		Confidential Information Verification	ESM system should provide the capability to verify that confidential information conforms to defined acceptance criteria.
		Managing Security Features	ESM system should allow only authorized administrators to enforce, stop, initiate, and modify actions on the functionality of the feature list.
		Session lock by security function	ESM system should lock the authorized administrator session when the administrator's activity continues to be in the specified inactive state.
		…	…

4.2.2 무결성 관련 메트릭

<Table 11>에는 ESM 시스템의 보안성(품질특성) - 무결성(부특성)에 관한 메트릭을 나타내었다.

<Table 11> The Metrics about Integrity of ESM

Characteritic	Sub-Property	Item	Related Items
	Integrity	Security Response	The ESM system should select a list of actions to minimize confusion when a security breach occurs.
		Audit data collection	ESM system must have the ability to collect audit data generated by the target system.
		Protecting the audit trail store	ESM system shall prevent unauthorized deletion or alteration of the audit records of the audit trail.
		Action in case of audit data loss forecast	ESM system should notify the administrator when the audit trail is over the specified limit and take appropriate action.
		Preventing Loss of Audit Data	ESM system should perform a loss prevention action when audit storage fails, except for the intended behavior of an authorized user when the audit trail is saturated.
		Management Functional Specification	ESM system should perform the prescribed management functions.
		Security Role	ESM system must maintain an authorized role.
		Basic protection of internal transport security functions data	ESM system should protect the security function data as it is transmitted between the separate parts.
		Security function self test	ESM system should perform self-tests at startup, periodically during operation, when an authorized user requests, and where self-tests are required.
		…	…

4.2.3 책임성 관련 메트릭

<Table 12>에는 ESM 시스템의 보안성(품질특성) - 책임성(부특성)에 관한 메트릭을 나타내었다.

<Table 12> The Metrics about Accountability of ESM

Characteritic	Sub-Property	Item	Related Items
	Accountability	Security alarm	ESM system should determine a list of actions that have not yet occurred but reduce the confusion to a cancellation in the event of a security breach.
		Generating audit data	ESM system should be able to make audit records for events to be audited.
		User identity association	ESM system should be able to correlate the relevant user's identity with the target event when an audit event occurs.
		Potential violation analysis	ESM system should apply a set of rules when inspecting audited events and be able to indicate potential violations in accordance with these rules.
		Complex attack learning	ESM system should maintain an internal representation of successive events and signature events of known intrusion scenarios.
		…	…

4.2.4 인증성 관련 메트릭

<Table 13>에는 ESM 시스템의 보안성(품질특성) - 인증성(부특성)에 관한 메트릭을 나타내었다.

<Table 13> The Metrics about Authenticity of ESM

Characteritic	Sub-Property	Item	Related Items
	Authenticity	Authentication failure handling	ESM system should detect when a specified number of authentication failures occur.
		Defining user attributes	ESM system should maintain a security attributes list such as queries, default values, changes, and deletions related to the user.
		certification	ESM system must allow a list of actions to be performed on behalf of the administrator before authenticating the administrator.
		Identification	ESM system must allow a list of actions to be performed on behalf of the administrator before identifying the administrator.
		Managing Security Attributes	ESM system should allow only authorized administrators to change, query, and delete default values for security attributes in the security attributes list.
		Initializing static properties	ESM system should control the provision of default values for security attributes and shall allow the authorized administrator to specify the initial values for the substitution of the default values.
		Security function data management	ESM system should allow only authorized administrators to change and delete identification and authentication data.
		…	…

4.3 품질검사표

평가모듈은 품질평가에 관한 제반 사항을 정의하고 있으나 품질평가에 적용하기 위해서는 필요한 최소한의 사항을 활용하기 쉽도록 정리하여 문서화할 필요가 있다. 이렇게 문서화한 것이 품질검사표로서 여기에는 메트릭의 명칭과 개념, 측정 항목(measurement items)의 개념 및 측정 방법, 메트릭이 어떤 계산에 의해 그 결과가 도출되는가와 결과값이 어떤 범위로 매핑되는가, 그리고 메트릭을 적용하는 과정에서 발생한 문제점은 무엇인가 등을 구성하여 정리한다. 품질검사표는 품질평가 모듈을 구성하는 기준인 ISO/IEC 25041을 기반으로 핵심 사항을 선정하여 활용이 용이하도록 정리한 것이다. <Table 14>는 품질검사표의 예를 보여주고 있다.

<Table 14> A Sample of Quality Inspection Table

Measure name		How closely can the user's identity be related to the event being audited?		
User Identity Association				
Measurement items	A	the number of events to be audited		
	B	the number of events that can associate the user that generated the event		
expression		- User Identity Association = B/A		
The range of results		0 ≤ User Identity Association ≤ 1	result value	
problem				

품질검사표의 결과는 측정 항목(measurement items) 각각의 값을 측정한 후 메트릭의 계산식에 따라 계산하여 도출한다. 결과값은 메트릭에 따라 서로 다른 범위의 값으로 나타날 수 있다. 결과값을 서로 비교할 수 있으려면 동일한 범위의 값(0≤값≤1)으로 매핑될 수 있도록 계산식을 구성하면 된다.

4.4 점검표

메트릭의 측정항목들의 값을 도출하기 위해 검토해야 할 체크리스트 형태의 점검항목을 표로 구성한 것이다. <Table 15>에 ESM 시스템의 보안성(품질특성) - 기밀성(부특성)의 '보안속성에 따른 접근 통제' 메트릭에 대해 구성한 점검표를 나타내었다.

<Table 15> Checklist of Information Flow Control

No	Function name	The function controlled
1	Operation no.1 related to data flow	V
2	Operation no.2 related to data flow	
3	Operation no.3 related to data flow	V
4	Operation no.4 related to data flow	V
5	Operation no.5 related to data flow	
…	…	…
The number of all operations related to data flow		A(the number of case)
The number of operations whose data flow is controlled by security attributes		B(the number of chech 'V')
Result		(B/A)

4.5 연구 결과의 유용성과 의의

정보보안 분야에 대한 평가는 특화된 공통평가 기준이 존재하며 소프트웨어 전반에 관한 품질평가는 ISO/IEC 25000 모델을 기반으로 이루어진다. 각각의 표준은 사용에 따른 장단점이 있으나 이원화된 체계로 인해 전문성을 살리면서 표준을 통합적으로 수용한 평가방법의 필요성이 제기된다.

본 연구에서는 보안성 제품에 대한 전문성을 추구하는 ISO/IEC 15408 공통 평가기준과 소프트웨어 전반에 대한 평가 체계를 구축하고 있는 ISO/IEC 25000 모델의 보안성 체계를 통합 수용한 메트릭 모델을 구성함으로써 관련 표준의 수용과 전문성을 함께 추구한 보안성 평가 방법을 구축하였다고 볼 수 있다.

또한, 기존의 보안성은 기능성이라는 품질특성의 부특성 범주에 속해 있었으므로 그 중요성을 충분히 살리지 못하였으나 본 연구에서는 최근의 표준화 동향에 부응하여 보안성을 품질특성 범주로 격상하고 그 부특성을 체계화함으로써 품질평가 분야의 트렌드를 반영하였다는 점에서 의의가 있고 활용성을 높였다고 할 수 있다.

5. 결론

오늘날의 거의 모든 비즈니스는 정보기술(Information Technology)을 기반으로 하지 않는 경우가 없다고 할 수 있을 정도로 대부분의 비즈니스 업무에는 IT가 근간이 되고 있다. 더구나, 인터넷을 매개로 하는 컴퓨팅 환경이 일반화된 현재, 개방된 환경에서 정보자산을 지키기 위해 정보보호 솔루션들에 대한 관심이 급증하고 있다. 또한, 기업에 있어서 정보보호 솔루션의 도입은 필수가 되었다.

정보보호의 필요성이 제고되면서 화두가 되는 부분은 바로 보안 시스템들의 통합을 통한 보안 정책의 통일, 보안 시스템 간의 상호 운용성 및 보안성의 극대화를 통한 위협요소의 최소화이다. 이러한 목적으로 등장한 것이 바로 ESM 시스템이다.

즉, 전문적이고 다양한 보안 솔루션들을 체계적으로 운영·관리하는 문제에 직면하면서 각 보안 제품에 대한 중앙집중적 통합관리에 대한 요구에 부응하고 방어 체계의 고도화에 따른 복잡도를 유지하면서 전문화된 관리의 단일화를 통해 보안 서비스의 질을 높이기 위한 솔루션에 대한 새로운 니즈에 맞춰 등장한 것이 ESM 시스템이다.

ESM 시스템의 핵심은 보안성 관련 성능에 대해 어느 정도 수준을 보장하는가이고 이것을 평가하기 위해서는 ESM 시스템의 보안 요구사항을 도출해야 하며 이에 대해서는 보호 프로파일이 구축되어 있다.

본 연구는 정보보안 관련 제품 중 ESM 시스템의 보안성을 평가할 수 있도록 요구사항에 부합하는 메트릭을 개발하는 것으로 ESM 시스템 보호 프로파일을 기반으로 한 요구사항을 ISO/IEC 25000의 보안성 품질특성을 적용한 메트릭을 구축하였다.

본 연구를 통해 구축된 ESM 시스템에 대한 보안성 메트릭을 활용하여 ESM 제품의 보안성을 평가하고 향후, ESM 시스템의 보안성을 평가한 사례를 축적하여 ESM 보안성 메트릭을 검증하여 ESM 시스템의 보안성과 타당성 제고를 위한 지속적인 연구를 수행해 나갈 것이다.

REFERENCES

[1] Deuk-Soo Kang, Hae-Sool Yang, “Evaluation Items of ESM S/W by Case Analysis”, The Korea Contents Society, Journal of the korea contents association, p.84, August, 2010.

[2] Hyung-Ho Kang, “A Study on the Improvement of Alert Function in ESM for Effective Attack Detection”, Sungkyungkwan University, Thesis of Master's Degree, 2014.

[3] Korea Internet & Security Agency, “Cyber Threat Trend Report for the 2nd quarter 2017”, July, 2017.

[4] ComputerWeekly.com, “Security audits reveal poor state of corporate cyber defences”, August 4, 2017.

[5] ISO/IEC 9126-1:2001, Software engineering -- Product quality -- Part 1:Quality Model, 2001.

[6] ISO/IEC 9126-2:2003, Software engineering -- Product quality -- Part 2:External Metrics, 2003.

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

[8] ISO/IEC 15408, Information technology -- Security techniques -- Evaluation criteria for IT security, 1999.

[9] Jae-Woo Im, "Refining software vulnerability Analysis under ISO/IEC 15408 and 18045", Journal of the Korea Institute of Information Security & Cryptology, Vol.24, No.5, pp.969-974, October, 2014.

[10] Ji-Hoon Jeong, Goang-Taek Han, Heui-Bong Choi, Gang-Soo Lee, Young-Soo Kim, Gap-Seung Go, “Enterprise Security Management System Protection Profile V2.0”, National Security Research Institute & Hannam University, September, 2008.

[11] Ha-Yong Lee, Jung-Gyu Kim, “Efficiency Eval8uation Convergence Model of Virtual Private Network based on CC and ISO Standard”, The Journal of Digital Convergence, Vol.13, No.15, pp.169-176, 2015.

[12] Ha-Yong Lee, Hyo-Sik Yang, “Convergence Performance Evaluation Model for Intrusion Protection System based on CC and ISO Standard”, The Journal of Digital Convergence, Vol.13, No.15, pp.251-257, 2015.

[13] ISO/IEC 25020, “Software product Quality Requirements and Evaluation(SQuaRE) -- Measurement reference model and guide”, 2007.

[14] ISO/IEC 25030, “Software product Quality Requirements and Evaluation(SQuaRE) -- Quality requirements”, 2007.

[15] ISO/IEC 25040, “Systems and software engineering – Systems and software Quality Requirements and Evaluation(SQuaRE) -- Evaluation process”, 2011.

[16] 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.

[17] ISO/IEC 25041, “Systems and software engineering -- Systems and software Quality Requirements and Evaluation(SQuaRE) -- Evaluation guide for developers, acquirers and independent evaluators”, 2012.

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 감사, 소프트웨어 및 네트워크 보안, 기업보안시스템과 정보제품의 시험과 평가
- E-Mail : hyosyang@samil.com