https://doi.org/10.14400/JDC.2017.15.5.197

웹방화벽의 보안성 평가 기준의 구축

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

Construction of Security Evaluation Criteria for Web Application Firewall

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

요 약 웹방화벽이 정보유출방지 등의 웹 보안 기능을 효과적으로 제공하여 웹 애플리케이션 보안이라는 목표를 달성하기 위해서는 웹사이트 보안 강화와 안전한 서비스 제공이라는 목표를 달성할 수 있어야 한다. 따라서 관련된 표준을 근간으로 웹방화벽시스템의 보안성 평가를 체계적으로 수행할 수 있는 연구가 필요하다. 본 논문에서는 웹방화벽시스템의 기반 기술과 웹방화벽의 보안성 품질에 관한 요구사항을 분석하고 소프트웨어 제품평가에 관한 국제표준과 정보보안 관련 제품의 평가에 관련된 표준을 근간으로 보안성 품질을 평가하는 기준을 구축하였다. 본 연구를 통해 웹방화벽시스템의 보안성 품질수준을 확인하고 품질향상을 제고할 수 있는 기준의 확보를 기대할 수 있을 것으로 사료된다. 향후 연구과제로 지속적으로 변화하고 있는 국제표준에 따라 평가기준을 지속적으로 업그레이드할 필요가 있다.

주제어 : 웹방화벽, 보안성, 품질 요구사항, 정보보안, 품질 평가

Abstract To achieve web application security goals effectively by providing web security features such as information leakage prevention, web application firewall system must be able to achieve the goal of enhancing web site security and providing secure services. Therefore, it is necessary to study the security evaluation of web application firewall system based on related standards. In this paper, we analyze the requirements of the base technology and security quality of web application firewall, and established the security evaluation criteria based on the international standards for software product evaluation. Through this study, it can be expected that the security quality level of the web application firewall system can be confirmed and the standard for enhancing the quality improvement can be secured. As a future research project, it is necessary to continuously upgrade evaluation standards according to international standards that are continuously changing.

Key Words : Web Application Firewall, Security, Quality Requirements, Information Security, Quality Evaluation

1. 서론

정보시스템을 구축하고 있는 많은 기업들은 정보보안 관련 기술을 필요로 한다. 최근에는 인터넷의 발달로 업무처리 능력이 획기적으로 향상되었으나 데이터에 대한 보안위협과 정보유출 피해가 커지고 있으며[1], DDoS 공

Received 8 March 2017, Revised 4 April 2017
Accepted 20 May 2017, Published 28 May 2017
Corresponding Author: Hyo-Sik Yang
(Seoul(Samil PricewaterhouseCoopers IT Risk & Security)
Email: hyosyang@samil.com

격을 통해 원활한 서비스를 방해하는 등의 보안 위협이 증가하고 있다[2].

정보보안 관련 기술 중에서 주된 관심의 대상이 되고 있는 기술이 웹방화벽(WAF:Web Application Firewall)이다. 대부분의 기업들이 고객을 대상으로 하는 업무를 웹 기반으로 운영하고 있고 정부의 행정서비스도 많은 부분이 웹기반으로 운영되고 있어 안전한 웹서버의 운영에 대한 관심이 제고되었다. 더구나 웹서비스는 외부에 노출되어 있다는 특징이 있어 보호 받기가 더 어려운 성격을 가진 서비스이다. 이러한 웹 기반 서비스는 웹 애플리케이션에 의해 이루어지며 이를 보호하는 역할을 하는 것이 웹방화벽이다.

최근 국내에서 발생하는 개인정보유출 및 해킹, 인터넷뱅킹에 대한 해킹 등은 개인 및 기업의 정보유출과 더불어 막대한 금전적 피해를 주는 등 웹 보안에 대한 관심이 증대되었다[3]. 최근에는 IoT의 발전에 따라 활성화되고 있는 U-헬스 기기의 보안[4]이나 IoT 기기에 대한 공격 대응 방안에 대한 연구[5] 등이 이루어지고 있다. 보안에 대한 관심 증대로 정보보호 제품에 대한 수요가 급증하였으며 정보보호 제품의 품질수준이 중요해졌으며 기능적합성 평가[6]나 효율성 평가[7], 사용성 평가[8] 등도 중요하지만 무엇보다도 보안성에 관한 평가가 우선이라 할 것이다.

웹방화벽은 일반 네트워크 방화벽(Firewall)과는 다르다. 주로 앱 애플리케이션 보안 솔루션의 성격을 가지고 있으며 SQL Injection이나 Cross-Site Scripting 같은 웹 공격을 감지하여 차단한다. 그 외에도 정보유출 방지 솔루션이나 부정 로그인 방지 솔루션, 웹사이트 위변조 방지 솔루션으로 활용할 수 있다[9].

웹방화벽의 보안 기능이 제 역할을 수행해야 웹 공격에 대응하고 정보유출을 방지하며 부정 사용자의 로그인을 차단하고 웹 사이트에 대한 위변조를 방지할 수 있다.

따라서 본 논문에서는 웹방화벽에 대한 보안성 품질에 중점을 두고 품질 수준을 측정할 수 있는 방법에 대해 고찰하고자 한다.

본 논문의 구성은 2장에서는 웹방화벽에 관련된 기술과 동향을 다루고 3장에서는 웹방화벽의 품질 요구사항을 분석하고 4장에서는 웹방화벽의 보안성에 관한 품질특성에 따라 평가 모델을 구축하고 5장에서 결론과 함께 향후 연구 과제를 제시하였다.

2. 웹방화벽 관련 기술과 시장 동향

2.1 웹방화벽 관련 기술 동향[10]

보안 관련 기업의 담당자들은 웹방화벽으로 자동적으로 방어되는 비율을 20~30% 정도로 보고 있으며 이것은 웹방화벽에 대한 설정이 중요하다는 의미이다.

최근 웹방화벽 관련 이슈는 해커의 잠입시도를 차단하는 능력, SSL(Secure Sockets Layer) 속도 성능, 클라우드 관련 기술이다. 차단 성능과 속도 간의 균형이 중요한데 기존의 보안이 침해를 피할 수 없는 감시・차단을 중점으로 하는데 반해 웹방화벽에서는 빠른 선 조치를 위한 실시간성 확보와 개인정보 유출을 탐지하고 실시간으로 차단하는 것이 강조되고 있다. 또한, 웹방화벽에 필요한 정책으로서 실시간 탐지 및 차단, 예외처리, 리포트 기능 등을 제공하고 있다.

침입탐지에 관한 정확도를 높이기 위한 기술로 기존의 패턴매칭 방식이 아닌 논리분석을 통한 지능형 탐지 엔진도 적용된 바 있으며, 이를 통해 네트워크의 성능저하도 최소화하고 있다.

웹방화벽의 효율 향상 기법으로 웹 트래픽 선별만 웹방화벽에게 맡기고 나머지 패킷은 서버로 신속히 전달하며 선별된 웹 트래픽을 웹보안 전용엔진이 검사하도록 해서 CPU의 효율적 사용을 지원한다.

향후 웹방화벽은 인공지능과 머신러닝이 결합되는 양상으로 진화될 것이며 이를 위한 관련 기업들 간의 협력과 공동 개발이 예상된다.

2.2 웹방화벽 시장 동향[11]

웹방화벽 관련 시장은 2011년에 100억원 정도의 규모에서 2015년에 285억원 정도의 규모로 성장했다. IDC(International Data Corporation)는 2016년 웹방화벽 시장 규모가 358억원에서 꾸준히 성장해 2019년에 658억원 규모에 이를 것으로 예측하고 있으며, F5(F5 Networks)는 좀 더 긍정적으로 전망하여 2017년에 700억원, 2019년에 1,000억원 규모에 이를 것으로 전망하고 있다.

3. 웹방화벽의 품질 요구사항과 품질특성

이 절에서는 웹방화벽의 보안성을 중심으로 웹방화벽

이 갖추어야 할 요구사항을 분석하고 보안성에 관련된 품질특성 체계를 구축하였다.

3.1 웹방화벽의 품질 요구사항

이 절에서는 ISO/IEC 15408[12]과 ISO/IEC 18045[13]를 기반으로 웹방화벽과 관련된 품질 요구사항을 분석하였다.

3.1.1 보안감사

보안 관련 행동의 책임을 추적하기 위해 감사 레코드를 생성하고 기록하고 검토하며 감사된 사건에 대한 보안 위반을 탐지하며 대응행동을 수행하는 능력으로 <Table 1>에 보안감사에 관한 요구사항을 정리하였다.

<Table 1> Requirements for Security Audit

Requirements	Content
Security Alert	The system should take action when security violations are detected.
Audit data generation	The creation of audit records for the event to be audited.
Correlation of event and user	It is able to correlate the identity of the user who caused the audit event and the event to be audited.
Pointing out the violation of rules	When the audit event is inspected it is able to apply the set of rules and point the potential violation.
Audit review	The system should provide the administrator with the function which read the audit data.
Storage protection	The system should protect the audit record from a unauthorized deletion and change.
Reaction against loss prediction	The system should inform and react when the audit trail exceeds the limit.
loss prevention of audit data	The system should carry out the prescribed action against the unintended audit store failure.

3.1.2 사용자 데이터의 보호

정보보안 제품에 장애가 발생했을 때 안전한 상태를 유지하고 보안과 관련된 데이터와 실행코드의 무결성 검증을 위한 자체시험 수행 및 사용자가 일정한 기간동안 컴퓨터를 사용하지 않고 있는 상황이 발생하였을 때 세션 관리 기능을 제공하는 능력으로 <Table 2>에 사용자 데이터 보호에 관한 요구사항을 정리하였다.

<Table 2> Requirements for User Data Protection

Requirements	Content
Information Flow Control	The system should control the information flow of the operation that occur a information flow.
Control based on security attributes	The system should control the information flow base on the controlled subject and the security attribute type of information.
Integrity inspection and reaction	The system should Inspect the user data stored in controlled storage about integrity errors of an entity.

3.1.3 식별 및 인증

정보보안 제품의 관리자를 포함하여 사용자 신원의 식별·인증 및 인증 실패시의 대응행동을 제공하는 능력으로 <Table 3>에 식별 및 인증에 관한 요구사항을 정리하였다.

<Table 3> Requirements for Identification and Authentication

Requirements	Content
Authentication failure handling	The system should detect a specified number of unsuccessful authentication attempts.
Maintaining user security attributes	The system should maintain a list of security attributes belonging to each user.(default value, query, modification, deletion etc.)
User authentication	The system should authenticate the users successfully.
Autentication Feedback Protection	The system should provide only the feedback list to the users.
User identification	The system should identify the user before allowing the functions.

3.1.4 보안 관리

정보보안 제품의 보안기능이나 보안속성, 보안에 관련된 데이터, 보안 역할과 관련된 사항을 관리하는 능력으로 <Table 4>에 보안 관리에 관한 요구사항을 정리하였다.

<Table 4> Requirements for Security Management

Requirements	Content
Security Function Management	The determination, suspension, initiation, and alteration of actions according to the security function should be limited to those who are authorized.

Providing Default Values	The system should control the access to provide limited default values for the security attributes.
Data Management Restrictions	The modification and deletion of identification and authentication data should be limited to those who are authorized.
Performing management functions	The system should perform the prescribed administrative functions.
Maintaining Security role	The system should maintain the authorized role.

3.1.5 보안기능 보호

보안기능에 대해 주기적으로 수행하거나 관리자의 요구가 있을 때 무결성을 검증하는 능력으로 <Table 5>에 보안기능 보호에 관한 요구사항을 정리하였다.

<Table 5> Requirements for the Protection of the Security Function

Requirements	Content
Keeping Safe State	The system should remain secure in the event of a failure.
Self Test	The system should perform self-tests to demonstrate the correct operation of the security functions.

3.1.6 접근통제

시스템이 정보흐름을 중재하기 위해 보안정책에 따라 패킷필터링 등을 통해 외부망으로부터 내부망을 보호하는 능력으로 <Table 6>에 접근통제에 관한 요구사항을 정리하였다.

<Table 6> Requirements for Access Control

Requirements	Content
Session Lock	The system should lock the administrator session after the administrator inactivity period.

3.2 웹방화벽의 보안성 품질특성

국내 소프트웨어 시험・인증서비스 기관에서는 보안용 소프트웨어를 포함한 소프트웨어 전 분야에 대해 ISO/IEC 9126[14], 25041[15], 25051[16] 등의 국제표준을 기반으로 품질특성에 대한 평가를 수행한다.

보안용 시스템의 평가를 위한 공통기준(Common Criteria, ISO 15408)이 있으나 ISO 표준과는 체계가 달라 시험・인증을 위한 일원화된 체계가 요구된다.

이 절에서는 웹방화벽의 요구사항을 바탕으로 웹방화벽의 보안성(security)에 관련된 특성을 분류하고 분석하고자 한다. 본 연구에서는 ISO/IEC 15408의 보안성 체계와 특성을 근간으로 ISO/IEC 25000 표준의 보안성 평가 체계에 따른 평가 기준을 구축하고자 한다. 즉, ISO/IEC 25000 표준을 근간으로 하는 보안성에 관련된 부특성인 기밀성(Confidentiality)과 무결성(Integrity), 책임성(Accountability), 인증성(Authenticity)의 체계에 따라 보안성을 평가하기 위한 기준을 구축하고자 한다.

3.2.1 웹방화벽의 기밀성 품질특성

기밀성이란 데이터가 액세스할 권한이 있는 것에만 액세스할 수 있다는 것을 보증하는 정도를 의미하며 기밀성에 관련된 웹방화벽의 특성에 속하는 항목에는 다음과 같은 것들이 있다.

① 웹방화벽은 인가된 관리자에게 감사 레코드로의 모든 감사 데이터를 읽을 수 있게 하는 기능을 제공해야 한다. 또한, 사용자가 정보를 해석하기에 적합하도록 감사 레코드를 제공해야 한다.(보안감사)
② 웹방화벽은 정보흐름을 일으키는 모든 오퍼레이션에 관한 정보흐름을 강제적으로 통제해야 하며 정보흐름을 일으키는 모든 오퍼레이션의 정보흐름을 통제해야 한다.(사용자 데이터 보호)
③ 웹방화벽은 적어도 통제되는 주체와 정보의 목록, 주체와 정보 각각에 대한 보안속성과 같은 주체 보안속성 및 정보 보안속성 유형에 기반하여 정보흐름통제를 강제해야 한다.(사용자 데이터 보호)
④ 웹방화벽은 기능목록에 있는 기능에 대한 행동을 결정하거나 중지하고 개시 및 변경하는 능력을 허가된 관리자로 한정해야 한다.(보안 관리)
⑤ 웹방화벽은 다음 방법에 의해 인가된 관리자 비활동 기간 후 상호 작용하는 인가된 관리자 세션을 잠가야 한다.(접근통제)

3.2.2 웹방화벽의 무결성 품질특성

무결성이란 시스템이나 제품 또는 컴포넌트가 컴퓨터 프로그램이나 데이터에 권한이 없는 액세스나 수정을 하지 못하게 하는 정도를 의미하며 무결성에 관련된 웹방화벽의 특성에 속하는 항목에는 다음과 같은 것들이 있다.

① 웹방화벽은 인가되지 않은 삭제에 대응하여 감사 증적에 저장된 감사 레코드를 보호할 수 있어야 한다. 또한, 저장된 감사 레코드에 관한 인가되지 않은 변경을 방지해야 한다.(보안감사)
② 웹방화벽은 감사증적이 미리 정의된 한도를 초과할 경우 인가된 관리자에게 통보하고 결정되어 있는 대응행동을 취해야 한다.(보안감사)
③ 웹방화벽은 특별 권한을 갖는 인가된 사용자에 의해 취해진 행동을 제외한 감사 저장 실패의 경우에 취해야 할 그 밖의 행동을 수행해야 한다.(보안감사)
④ 웹방화벽은 모든 객체에 대한 무결성 오류에 대하여 보안기능에 의해 통제된 저장소 내에 저장된 사용자 데이터를 검사해야 한다.(사용자 데이터 보호)
⑤ 웹방화벽은 규정된 관리 기능을 수행할 수 있어야 한다.(보안 관리)

3.2.3 웹방화벽의 책임성 품질특성

책임성이란 한 객체(entity)의 행위(action)가 그 객체로 유일하게 추적될 수 있는 정도를 의미하며 책임성에 관련된 웹방화벽의 특성에 속하는 항목에는 다음과 같은 것들이 있다.

① 웹방화벽은 잠재된 보안 위반을 탐지했을 때 혼란을 최소화하는 대응행동 목록을 취해야 한다.(보안감사)
② 웹방화벽은 감사대상 사건들에 대한 감사 레코드를 생성해야 한다.(보안감사)
③ 웹방화벽은 식별된 사용자의 행동으로 발생한 감사 사건에 관하여, 사건을 일으킨 사용자의 신원과 대상 사건을 관련시킬 수 있어야 한다.(보안감사)
④ 웹방화벽은 감사된 사건을 검사하는 경우에 규칙 집합을 적용할 수 있어야 하고, 이 규칙에 기반을 두고 잠재적인 위반을 지적할 수 있어야 한다.(보안감사)

3.2.4 웹방화벽의 인증성 품질특성

인증성이란 주체(subject)나 리소스(resource)의 정체(identity)가 요구된 바로 그것이라는 것이 증명될 수 있는 정도를 의미하며 인증성에 관련된 웹방화벽의 특성에 속하는 항목에는 다음과 같은 것들이 있다.

① 웹방화벽은 인증 사건의 목록과 관련된 규정진 횟수의 인증시도 실패가 발생하면 이를 탐지해야 한다.(식별 및 인증)
② 웹방화벽은 각 사용자에 속한 질의 , 변경, 디폴트값, 삭제, 기타 연산 같은 보안속성 목록을 유지해야 한다.(식별 및 인증)
③ 웹방화벽은 사용자를 대신하여 보안기능이 중재하는 다른 모든 행동을 허용하기 앞서 사용자를 성공적으로 인증해야 한다.(식별 및 인증)
④ 웹방화벽은 인증이 진행되는 동안 사용자에게 피드백 목록만을 제공해야 한다.(식별 및 인증)
⑤ 웹방화벽은 사용자를 대신하여 보안기능이 중재하는 다른 모든 행동을 허용하기 앞서 각 사용자를 성공적으로 식별해야 한다.(식별 및 인증)
⑥ 웹방화벽은 보안속성 목록의 보안속성을 디폴트값 변경, 질의, 삭제, 기타 연산하는 능력을 인가된 관리자로 제한하도록 접근통제, 정보흐름통제를 강제해야 한다.(보안 관리)

4. 웹방화벽의 보안성 평가모델

웹방화벽의 보안성 평가모델은 부특성 체계와 평가척도(metrics, measure), 품질검사표, 점검표로 구성하였다. 평가모듈은 평가 관련 사항을 문서화한 것으로 ISO/IEC 25042(Evaluation Modules)에 정의된 구성을 바탕으로 한다. 이 표준에는 평가방법에 관한 전반적인 사항을 기술하기 위해 사용되는 문서의 구성과 내용을 정의하고 있다. 이를 바탕으로 평가모듈을 다음과 같이 구성하였다.

4.1 평가모듈의 체계

평가모듈은 품질시험 관련 제반 사항을 문서화한 것으로 평가 개요, 기법, 메트릭 상세 내용, 메트릭 적용 절차, 도출된 결과에 대한 해석 등을 포함하고 있고 품질평가 프로세스에 대한 국제표준인 ISO/IEC 25042 평가모듈의 형식에 근거하여 작성하였다. 품질평가 모듈의 체계는 <Table 7>과 같다.

<Table 7> System of Quality Evaluation Module

Item		Content
Outline	Concept of metric	
	Measurement purposes	
	Metric category	Characteristic - Subcharacteristic - Metric
	Term Explanation	
Coverage	application target	Product Description, User Document, Program & Data
	Necessary resources	Resources which is needed to apply the metric
	Techniques	Testing techniques
Reference		Where is the metric derived from?
Metric	Measurement items	
	Measurement method	
	Expression	Expressions of metrics
Application Procedures		Description about the specific procedures and method for performing the test
Results interpretation & report	Mapping of the measurement	The range of metric result
	Interpretation of the measurement result	Provide instructions on how to interpret the measured results
	Reporting requirements	Items to document and report on measurement results

4.2 메트릭 개발 내역

본 연구에서 웹방화벽의 보안성에 대한 부특성인 기밀성, 무결성, 부인방지, 책임성, 인증성에 관한 메트릭을 개발하였다.

4.2.1 기밀성에 관한 메트릭

기밀성에 관한 메트릭은 <Table 8>과 같이 구축하였다.

<Table 8> The Measures about Confidentiality

Characte rities	Subchara cteristics	Item	Related Items
Security	Confident iality	Ability to read audit data	Web application firewall should provide the ability to read all audit data and provide audit records to facilitate interpretation of information.
		Mandatory information flow control	Web application firewall should enforce information flow control for all operations that cause information flow.
		Security attribute-b ased control	Web application firewall should enforce information flow control based on subject security attributes and information security attribute types.
		Restrict to authorized administrat or	Web application firewall should allow authorized administrators to determine, suspend, initiate, and modify actions on the function list.

4.2.2 무결성에 관한 메트릭

무결성에 관한 메트릭은 <Table 9>와 같이 구축하였다.

<Table 9> The measure about integrity

Characte ritics	Subchara cteristics	Item	Related Items
	Integrity	User data inspection	Web application firewall should check the user data stored in the repository controlled by the security function for integrity errors on all objects.
		Keeping the safe state	Web application firewall should remain in a safe state in the event of a specified type of failure.
		Audit record protection	Web application firewall system should protect the audit records of the audit trail from illegal deletion and prevent unauthorized changes to the stored audit records.
		Reaction	Web application firewall should notify the administrator and take action if the audit trail exceeds the defined limit.
		…	…

4.2.3 책임성에 관한 메트릭

책임성에 관한 메트릭은 <Table 10>과 같이 구축하였다.

<Table 10> The measure about Accountability

Characte ritics	Subchara cteristics	Item	Related Items
	Accounta bility	Acquisition of a reaction list	Web application firewall should minimize the confusion by taking a reaction list when detecting potential security violations.
		Creating audit records	Web application firewall should be able to generate audit records of auditable events.
		Associating events with users	The system should be able to correlate the auditable event with the identity of the user who generated the audit event.
		Pointing out potential violations	Web application firewall should be able to apply a set of rules to inspect audit cases and to point out potential violations based on these rules.
		…	…

4.2.4 인증성에 관한 메트릭

인증성에 관한 메트릭은 <Table 11>과 같이 구축하였다.

<Table 11> The measure about Authenticity

Characteristics	Subcharacteristics	Item	Related Items
	Authenticity	Providing default values	Web application firewall should enforce access control and information flow control to provide a limited default value of security attributes and shall allow authorized administrators to specify optional initial values to override default values when creating objects or information.
		Detection of authentication attempts	Web application firewall should detect if a certain number of authentication failures occur.
		Keeping security attributes	Web application firewall should maintain a list of security attributes such as default values, queries, changes, deletions, and other operations for each user.
		User Authentication	Web application firewall should successfully authenticate the user before allowing any action.
		…	…

4.3 품질검사표

품질검사표는 품질평가에 관한 전반적인 사항을 정의한 평가모듈을 실제 평가과정에서 편리하게 활용할 수 있도록 핵심적인 사항을 정리한 것으로 ISO/IEC <Table 12>와 같은 형태로 구성하였다.

<Table 12> An example of quality testing table

Measure name		Can a authorized administrator read all audit data from the audit record?		
Audit Review				
Measurement items	A	The number of audit data		
		- data no.1 - data no.2		
	B	The number of audit data which a authorized administrator can read		
Formula		Audit Review = B/A		
Range of results		0 ≤ Audit Review ≤ 1	result value	
problem				

품질검사표의 측정항목은 메트릭에 따라 다수의 항목으로 구성되어 항목에 대한 개념과 그 개념에 따른 세부 측정항목으로 구성된다. 계산식은 측정항목의 값으로부터 정해진 식에 의해 결과값을 도출하며 결과 영역은 메트릭 전반에 대해 0~1 사이의 값으로 결정될 수 있도록 조정된다.

4.4 점검표

측정항목의 값을 도출하려면 세부 측정항목을 설정하여 도표화하고 각 세부항목에 대해 평가대상을 검토하여 가부를 결정해야 하며, 이 세부 측정항목에 대한 표를 점검표라 한다.

점검표의 도출은 웹방화벽의 보안성에 관한 요구사항을 기반으로 한다. 웹방화벽의 보안성에 관한 요구사항으로부터 특정 메트릭의 개념에 맞는 내용을 도출하여 점검표 항목을 구성한다. <Table 13>은 '감사 검토' 메트릭의 점검표를 나타내고 있다.

<Table 13> Checklist of 'Audit Review'

No	Data to be checked	Audit data which an authorized administrator can read
1	Audit Data 1	√
2	Audit Data 2	
…	…	…
The number of Audit Data		A
The number of audit data which an autorized administrator can read		B
Result		B/A

4.5 기존 평가 기준과의 비교

보안성에 관한 품질평가 표준은 소프트웨어 제품평가에 관련하여 ISO/IEC 9126과 ISO/IEC 12119에서 정의하고 있고 이 두 표준과 품질평가 프로세스에 관한 표준인 ISO/IEC 14598을 통합하여 구축한 ISO/IEC 25000 시리즈가 있다. 그러나 9126과 12119 표준에서는 보안성이 품질특성 레벨이 아니라 6개의 품질특성 중 하나인 기능성의 부특성으로 적합성, 정확성, 상호운영성, 보안성, 준수성을 정의하고 있어 상대적으로 보안성에 관한 중요성이 낮다고 볼 수 있다. ISO/IEC 25000 시리즈에서 보안성을 품질특성으로 격상시키고 그 부특성으로 기밀성, 무결성, 부인방지, 책임성, 인증성 등을 정의하고 있지만 전문 정보보호 관련 제품에 대한 평가에 적용하기에는 부족한 부분이 있다.

ISO/IEC 15408 표준(공통 평가기준)은 정보보안 제품의 평가에 특화된 표준으로서 보안성 평가에 대한 전문성은 ISO/IEC 25000 표준에 비해 높다고 할 수 있지만 소프트웨어 제품의 전반적인 품질특성의 평가에는 적용할 수 없다.

국내의 소프트웨어 제품평가・인증 기관에서는 ISO/IEC 25000을 근간으로 정보보안 제품의 평가도 병행하여 실시하고 있고 보안성의 중요성이 품질특성 체계에도 반영되고 있는 만큼 평가 의의를 제고하기 위해서라도 도 표준을 통합한 보안성 평가기준의 구축이 필수적이라 사료된다.

5. 결론

다양한 보안 관련 이슈들이 매스컴을 통해 보도되고 정보보안 관련 사고들이 끊임없이 발생하고 있는 현실에서 정보보안을 위한 대책을 수립하는 문제는 정보시스템을 구축하고 있는 기업이나 조직에서 매우 중요한 선택사항일 수밖에 없을 것이다. 하지만 다양한 정보보안 제품 중에서 기업이나 조직의 목적과 용도에 맞는 제품을 선택하기 위해서는 관련 제품에 대한 적절한 판단 기준이 필요할 수밖에 없다. 따라서 정보보안 제품의 선택에 있어서 핵심이 되는 보안성 품질에 대해 판단하는 올바른 기준을 구축해야 하며 가능한 한 관련 표준을 준수한 평가체계의 구축이 바람직하다고 할 것이다.

국민을 대상으로 한 정부의 서비스나 고객을 대상으로 한 기업의 서비스가 웹을 통해 제공되고 메일, 전자상거래, 블로그, 게임 등 다양한 기능들이 웹 애플리케이션을 통해 제공되면서 대부분의 웹사이트들이 웹 취약점으로 인해 악성해커와 유해 코드로부터 공격받는 위협에 항시 노출되어 있을 수밖에 없게 되었다. 이러한 웹 애플리케이션에 대한 공격을 방어하기 위해 웹방화벽이 필수인 만큼 웹방화벽의 품질 수준을 평가하기 위한 체계적인 방법의 구축이 필수적이다.

웹방화벽의 품질 수준에 대한 평가의 핵심은 보안성 평가로서 보안성 평가를 위한 체계 구축을 위해서는 관련 표준을 근거로 하는 보안성 품질의 평가기준 구축이 필수적이다. 본 논문에서는 ISO/IEC 25000 표준의 보안성 품질특성과 ISO/IEC 15408을 근간으로 웹방화벽의 보안성 평가를 위한 통합체계를 구축하였다.

웹방화벽의 보안성 평가모델 개발 연구로서 웹방화벽 관련 기술을 분석하고 웹방화벽의 보안성 평가모델을 개발하기 위해 웹방화벽에 관한 보안성 품질 요구사항을 분석하고 주요 품질요소를 분석하여 평가 기준을 구축하였다.

향후, 웹방화벽의 보안성에 대한 평가사례를 구축하고 이를 축적하여 타당성과 객관성을 갖춘 평가기준으로 확립될 수 있도록 지속적인 연구가 필요하다.

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.

[2] Sunghyuck Hong, "DDos attack traffic through the analysis of responses to research", Journal of Convergence Society for SMB, Vol. 4, No. 3, p. 1, 2014. 8.

[3] Bae-Keun Kang, "Research about Quality Analysis of Web Fire Wall System", The Graduate School of Hoseo University, 2009.

[4] Yun-A Hur, Keun-Ho Lee, "A Study on Countermeasures of Convergence for Big Data and Security Threats to Attack DRDoS in U-Healthcare Device", Journal of the Korea Convergence Society, Vol. 6, No. 4, pp. 243-248, 2015. 8.

[5] Ju-Hye Oh, Keun-Ho Lee, "Attack Scenarios and Countermeasures using CoAP in IoT Environment", Journal of the Korea Convergence Society, Vol. 7, No. 4, pp. 33-38, 2016. 7.

[6] Ha-Young Lee, Hyo-Sik Yang, "Development of Functional Suitability Evaluation Measure of DRM Software", Journal of digital Convergence , Vol. 14, No. 5, pp. 293-300, 2016.

[7] Ha-Yong Lee, Jung_Gyu Kim, "Quality Evaluation Model about Efficiency for Fingerprint Recognition System", Journal of digital Convergence, Vol. 12, No. 6, pp. 215-216, 2014.

[8] 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.

[9] Wikipedia, https://ko.wikipedia.org/wiki/%EC%9B%

B9%EB%B0%A9%ED%99%94%EB%B2%BD, 2017. 2. 9.
[10] Sang-Soo Hong, http://www.ciociso.com/news/articleView.html?idxno=11072, 2017. 2. 9.
[11] You-Ji Lee, http://byline.network/2016/06/1-206/, 2017. 2. 10.
[12] ISO/IEC 15408, Information technology -- Security techniques -- Evaluation criteria for IT security, 1999.
[13] ISO/IEC 18045, Information technology == Security techniques -- Methodology for IT security evaluation, 2005.
[14] ISO/IEC 9126-1, 2, 3, 4, Software engineering -- Product quality -- Part 1, 2, 3, 4, 2001.
[15] ISO/IEC 25041, Systems and software engineering -- Systems and software Quality Requirements and Evaluation(SQuaRE) -- Evaluation guide for developers, acquirers and independent evaluators, 2012.
[16] ISO/IEC 25051, Systems and software engineering -- Systems and software Quality Requirements and Evaluation(SQuaRE) -- Requirements for quality of Ready to Use Software Product(RUST) and instructions for testing, 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 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