웹기반 서비스 인증·평가제도 발전방향에 관한 연구

- A Study on the Improvement of Web-based Services Evaluation and Certification Program -

서 광 규 *
Seo Kwang Kyu

Abstract

Web-based services have fundamentally confidential problems due to characteristics of internet environment such as anonymity. These problems are serious obstacles to grow the web-based services. The security and confidence of web-based services rely on both service provider and users' opinion. But the former has difficulty in trusting the service provider and the latter takes too long time to propagete all users after converging their opinion. Therefore it is necessary to establish the objective and confidential evaluation and certification program for web-based service. In this paper, the internal and external web-based services evaluation and certification programs are compared and analyzed. The critical factors and evaluation methodology for secure and confidential web-based service are identified. Finally, this paper provides the improvement and strategy for web-based services evaluation and certification program.

Keyword : Web-based Services, Evaluation, Certification

† 본 논문은 상명대학교 2004학년도 연구소 학술지원 연구비에 의해 연구되었음.
* 상명대학교 산업정보시스템공학과

1. 서 론

기업은 자신이 가지고 있는 컨텐츠 등을 이용하여 개발한 비즈니스 모델을 웹기반으로 전환하여 일반인 및 다른 기업에게 제공하거나 판매가 가능하며, 이용자는 이를 구매하거나 인터넷을 매체로 하여 서비스를 이용할 수 있다. 그러나 웹기반 서비스는 익명성이 보장된 인터넷 환경의 특성상 근본적으로 신뢰의 문제를 안고 있으며, 이는 웹기반 서비스가 활성화 되는데에 중요한 장애요소로 작용하고 있는게 사실이다 [2].

급속히 확장되고 있는 인터넷은 인터넷 이용자로 하여금 정보통신 기술의 양면성을 경험하도록 하고 있다. 생활은 편리해졌지만, 정보통신 기술을 악용한 개인 신상정보, 거래정보 등의 유출 및 침해도 빈번하게 나타나고 있다. 따라서 객관적이고 공정한 절차를 통하여 공신력 있는 제3자로부터 웹기반 서비스를 평가·인증하는 제도가 필요하다.

이러한 인증·평가제도는 객관적이고 공정한 평가를 통하여 공신력 있는 제3자로부터 웹기반 서비스에 대한 안전성과 신뢰성이 검증된 웹기반 서비스를 권장함으로써 정보의 불법적 유출, 정보의 위·변조, 바이러스, 서비스 방해, 불건전 정보의 유출, 해킹 등의 정보화 역기능으로부터 안전한 정보화 사회 구축에 기여하고 있다 [4].

본 논문에서는 현재 국내·외 웹기반 서비스 인증·평가제도를 비교 분석한다. 더불어 급변하는 국제 환경에 적합한 안전하고 신뢰할 수 있는 웹기반 서비스 구축시 고려해야 할 평가방법론과 웹 환경에서의 평가요인을 도출하여 웹기반 서비스 인증평가 업체의 인증업무 담당자와의 인터뷰를 통하여 평가요인 적용의 타당성을 분석한다. 마지막으로 국제환경과 웹 환경에 적합한 웹기반 서비스 인증·평가체계를 재정립함으로써 안전하고 신뢰할 수 있는 웹기반 서비스 인증·평가 제도의 발전방향을 제시하고자 한다.

2. 국내·외 웹기반 서비스 인증·평가 제도

급속히 확장되고 있는 인터넷 통신망은 인터넷 이용자로 하여금 정보통신 기술의 양면성을 경험하도록 하고 있다. 필요한 자료나 정보를 얻기 위해 또는 물품을 구매하기 위해 과거처럼 다리품을 팔지 않아도 되는 등 생활은 편리해졌지만, 정보통신 기술을 악용한 개인 신상정보, 거래정보 등의 유출 및 침해도 빈번하게 나타나고 있다.

이에 대해 정부는 정보통신망 및 시스템 운영자가 지켜야할 안전성과 신뢰성 기준을 마련하는 연구를 추진하여 그 결과로 "정보통신기반 보호법"을 마련하고 2001년 7월 1일부터 시행하고 있으며, "정보통신망 이용촉진 및 정보보호등에 관한 법률"상의 개인정보보호규정 신설과 개인정보보호지침을 통해 개인정보 보호의 제도적 장치를 마련하여 시행하고 있다. 또한 인터넷을 이용한 전자상거래 과정에서 발생하는 소비자피해를 최소화하기 위해 공정거래위원회는 "전자상거래상에서의소비자보호등에관한법률"과 "사이버몰 표준이용약관"을 마련하여 시행하고 있다.

이러한 정부 주도의 정책이 제대로 시행되기 위해 웹기반 서비스 운영기관과 사업자가

왜 웹기반 서비스 이용자의 개인정보를 보호해야하며 어떻게 보호해야하는지에 대한 이해와 웹기반 서비스 이용자의 개인정보 유출이나 침해를 최소화하기 위해 노력하는 웹기반 서비스 운영기관 및 사업자를 선별할 수 있는 웹기반 서비스 평가모델에 대한 연구가 시급하게 요구되고 있다. 이와 유사한 연구는 한국을 비롯하여 미국, 일본, 영국, 싱가포르, 노르웨이, 유럽연합(EU) 등의 인터넷 선진국에서 수행되고 있으며, 제3자 인증·평가제도를 도입하여 시행하고 있다.

이 제도는 크게 인터넷쇼핑몰과 같이 상거래를 하는 웹사이트를 대상으로 소비자보호지침의 준수 여부를 평가하여 인증마크를 부여하는 소비자 신뢰인증제도(Customer Trust Seal)와 전체 웹사이트를 대상으로 개인정보보호 혹은 시스템 보안지침의 준수 여부를 평가하여 마크를 부여하는 개인 신뢰인증제도(Privacy Trust Seal)로 구별할 수 있다.

전자의 예로는 미국 BBB*Online* 신뢰(Reliability) 마크, 영국 TrustUK 마크, 일본 온라인 마크, PWC BetterWeb 마크, 한국 eTRUST 마크 등이 있다. 후자의 예로는 미국 TRUSTe 마크, 미국 BBB*Online* 프라이버시 마크, 일본 프라이버시 마크, 한국 i-Safe 인증, ePRIVACY 인증 등이 있다.

이러한 추세에 발맞추어 국내 인터넷산업의 경쟁력 강화의 기틀을 마련하고자 공급자와 이용자, 사업자와 소비자간의 신뢰관계 형성을 위해 인터넷사이트 운영기관 및 사업자에 대한 이용자 보호를 위한 민간 자율적인 규제로 다양한 제도가 도입되어 시행되어 오고 있다. 국내에는 전자거래진흥원의 eTrust, 한국정보통신산업협회의 ePRIVACY(개인정보보호마크), i-Safe(인터넷사이트안전마크) 등 공신력있는 공공기관에서의 평가제도가 시행되고 있다.

eTrust의 경우 상업적인 웹사이트를 대상으로 업종별로 구분하여 평가기준을 달리 적용하고 있으며 소비자보호, 개인정보보호, 시스템보안 부문을 모두 고려하고 있다. 하지만 주로 웹사이트에서의 이용자 편리성과 소비자보호에 대한 평가를 중점적으로 시행하고 있어 보안부문에 대한 평가가 취약하다고 할 수 있다.

ePRIVACY의 경우 개인정보를 수집하는 모든 웹사이트를 대상으로 주로 관련법 및 지침의 준수에 대한 적합성 여부를 평가항목으로 하여 인증·평가하고 있다. 웹사이트상에서의 개인정보보호정책 등 관련법 준수 등 관리적인 측면을 고려하고 있으며 이 또한 보안부문에 대한 평가는 전무한 상태라 할 것이다.

i-Safe의 경우 보안요구수준에 따라 고도의 보안을 요구하는 업종과 그렇지 않은 업종으로 구분하여 평가기준을 달리적용하여 시스템 보안, 개인정보보호, 소비자보호 부문을 모두 평가하고 있다.

3. 정보시스템 평가방법론

본 장에서는 안전하고 신뢰할 수 있는 웹기반 서비스 인증·평가제도 개선을 위하여 고려해야 할 요소를 도출하고 적용하기 위하여 정보시스템 및 정보보호시스템 평가방법론 연구에 대하여 비교 분석을 수행한다.

3.1 정보보호수준 평가방법론

3.1.1 BS7799

BS 7799는 정보자산관리의 개념을 떠나 체계적이고 표준적인 관리지침 및 방법을 마련하고자 영국 표준기관(British Standard Institution)이 1995년에 제정한 평가체계다. BS 7799 Part 1은 총 10개의 주요 분야, 36개의 세부분야(통제목적), 그리고 127개의 보안통제항목을 정의하고 있다. 그 중 10개의 분야는 보안정책, 보안조직, 자산분류 및 통제, 인적보안, 물리적 및 환경적 보안, 통신 및 운영관리, 접근통제, 시스템 개발 및 유지보수, 업무 지속성 관리, 준수(부합성)로 구성된다. Part 2(Specification for information security management systems)에서는 정보보호관리체계를 구축하는 절차(프레임워크)를 제시하고 있다 [1].

3.1.2 GMITS

보안관리 체계의 국제표준으로 대표적인 것이 ISO/IEC TR 13335 GMITS(Guidelines for the Management of Information Technology Security)에서 제시하는 정보보호관리 프로세스이다. GMITS은 국제 표준기구인 ISO/IEC JTC1 SC27 (정보보안기술 표준화 분과위원회) WG1에서 작성한 표준문서로 ISO/IEC TR 13335, "Guidelines for the Management of IT Security"의 5부로 구성되어 있다 [8]. GMITS에서는 일반적인 위험관리 과정을 소개하고 있어 구체적인 위험관리 방법론의 개발 또는 선정시 기본적인 틀(framework)로서 활용될 수 있다.

3.1.3 FITSAF(연방정보기술 보안평가 프레임워크)

미 CIO(Chief Information Officers)협의회내의 보안소위원회에 의해 개발된 연방정보기술 보안평가 프레임워크(Federal Information Technology Security Assessment Framework)는 각 기관의 담당자들이 기존의 정책과 관련하여 그들의 보안 프로그램의 현재 상태를 결정하고, 필요한 경우 향상 목표를 수립하기 위한 방법을 제공한다. 하지만 프레임워크가 새로운 보안 요구사항을 수립하지는 않는다 [3].

3.2 정보보호시스템 평가방법론

3.2.1 TCSEC (Trusted Computer System Evaluation Criteria)

미국은 컴퓨터시스템이 처리하는 비밀정보를 보호하기 위한 대책을 수용하고 있는 국방부 지침(DoD Directive 5200.28)이 1972년 발표된 이후로 1981년 국방부 컴퓨터보

안센터(DoD Computer Security Center)가 설립되고 국방부지침 5125.1에 안전한 컴퓨터 평가기준 제정 및 평가업무에 대한 내용이 명시되면서 1983년 TCSEC(Trusted Computer System Evaluation Criteria)의 초안(Orange Book)이 제작되었고, 2년 뒤인 1985년에 미 국방성 표준(DoD STD 5200.28)으로 채택되었다.

이후 1987년 네트워크 제품에 대한 평가기준 TNI(Trusted Network Interpretation of the TCSEC) [9]의 제정에 이어 1991년 DBMS에 관한 평가기준 TDI(Trusted DataBase Management System Interpretation of the TCSEC) [10]이 제정되었다.

3.2.2 ITSEC (Information Technology Security Criteria)

유럽의 ITSEC는 영국, 프랑스, 독일, 네덜란드 등 자국의 정보보호시스템 평가기준을 제정하고 시행하던 4개국이 평가제품의 상호인정 및 평가기준이 상이함에 따라 정보보호 제품의 중복평가에 허비되는 시간, 인력, 및 소요비용을 절감하기 위하여 개발된 공동의 기준이다. 4개국은 1989년 소위 "일치된 평가체계(Harmonized Criteria)"를 작성하기로 합의하고 1991년 공동의 평가기준으로 ITSEC 버전 1.2를 제정하였다. ITSEC을 적용하고 있는 국가는 영국, 독일, 프랑스, 네덜란드, 이태리, 스웨덴, 호주 등 7개국이다 [7]. ITSEC는 TCSEC와 달리 단일기준으로 모든 정보보호 제품을 평가한다. 따라서 보안기능은 개발자가 제품에 미리 정의한 보안기능은 개발자가 제품이 사용될 환경을 고려하여 보안기능을 설정하거나 미리 정의한 보안기능을 사용토록 하였으며, 제품평가는 보증부분만 가지고 수행된다.

3.2.3 CC (Common Criteria)

국제 공통평가기준(Common Criteria)은 컴퓨터시스템의 발달과 이에 따른 자료의 저장, 전송 등의 신뢰성에 대한 요구의 증가에 의해 1983년 미국의 TCSEC(Trusted Computer System Evaluation Criteria)을 시작으로 1991년 유럽(영국, 프랑스, 독일, 네덜란드)의 ITSEC(Information Technology Security Evaluation Criteria), 1993년 캐나다의 CTCPEC(The Canadian Trusted Computer Product Evaluation Criteria) 등의 평가기준들의 개발을 통해 가시화되었다. 현재는 이러한 각국의 평가기준들을 상호인정하기 위한 표준화작업이 수행되어 국제 공통평가기준이 1999년에 ISO 15408 국제표준으로 제정된 상태이다[6].

이상에서 기술한 선행연구들에 대한 비교 결과를 표 1에 나타내었다.

< 표 1 > 정보시스템 평가방법론의 비교결과

인증대상	평가방법론	특징(장점)	한계점(단점)
보안관리 체계	BS7799	- 조직의 보안수준평가 - 국제표준 ISO17799-1	- 높은 수준의 기준을 제공 - 대상이 IT보안에 집중 - 시스템의 기능평가 미흡
	GMITS	- 일반적인 위험관리 - 국제표준 ISO13335	- 구체적인 평가모델을 제시하지 못함
	FITSAF	- 보안관리의 현재상태 평가	- 새로운 보안 요구사항을 제공하지 못함
제품/ 시스템	TCSEC	- 세계 최초의 평가기준 - 기밀성 강조	- 무결성, 가용성을 강조하는 민간기업에서 적용곤란
	ITSEC	- 세계 최초의 국제통합기준 - TCSEC 수용	- 단일기준으로 모든 제품을 평가하고자함
	CC	- 국제상호인증을 위한 공통기준 - 국제표준으로 추진중(ISO15408)	- 평가대상이 제품 및 시스템에 한정되어 있음

4. 웹기반 서비스 인증·평가제도 개선방안

4.1 웹기반 서비스 인증·평가제도 개선의 필요성

국내에서는 1999년부터 인터넷쇼핑몰을 대상으로 인터넷모범상점인증제도라는 웹기반 서비스 인증·평가제도를 도입 시행하여 왔으며[5], 2001년에는 이의 평가대상을 확대하여 포털, 커뮤니티, 은행 등 업종구분없이 인터넷 전사이트를 대상으로 인증·평가하고 있다. 기존 웹기반 서비스 인증·평가제도의 평가기준이 국내 관련법 및 지침을 기반으로 일반적이고 보편적으로 구성되어 있음을 감안할 때 평가방법론 및 평가기준 구성의 타당성 검증이 부재한 상태이다. 평가방법론의 적용이나 타당성이 검증된 평가기준을 구성하는 인증·평가체계의 구축은 단순히 인증·평가제도를 설명하는 역할뿐 아니라 실제로 웹기반 서비스를 이용하는 이용자에게 인증·평가제도에 대한 신뢰를 얻기 위하여 중요한 역할을 수행한다.

기존의 평가기준이 조직 전체의 보편적인 보안요구에 대한 사항으로 구성되어 있어 웹기반 서비스를 제공하는 업체 및 이용자의 보안요구사항에 적절히 대처하지 못한다는 단점도 가지고 있다. 따라서 위의 분석결과를 종합하여 볼 때 웹기반 서비스 인증·평가제도의 평가방법론 및 평가기준의 타당성 확보를 위해서는 인증·평가체계의 구축이 필요하다. 그러나 새로운 인증·평가체계를 만드는 데에는 많은 시간, 노력 및 예산이 소요된다. 따라서 국제적으로 표준화된 인증·평가체계를 활용함으로써 이러한

문제를 해결할 수 있고 향후 웹기반 서비스 업체들이 해외시장 진출시 다른 국가들로부터 신뢰를 얻기위한 중요한 도구가 될 것이다. 더불어 국내 웹기반 서비스 이용자에게도 신뢰도 향상에 크게 기여할 것이다.

인증·평가체계 개선을 위하여 먼저 기존 인증·평가체계와 국제 표준화된 인증·평가체계를 비교 분석하여 수정·보완할 사항을 도출하고 그 타당성을 분석하여 개선된 웹기반 서비스 인증·평가 체계를 제시하고자 한다.

4.2. 인증·평가체계의 평가지표 타당성 분석

웹기반 서비스 인증·평가 체계의 평가지표 개선에 대한 타당성 분석을 위하여 기존 웹기반 서비스 인증업체의 인증업무 담당자를 대상으로 인터뷰를 실시하였다.인터뷰 대상업체는 웹기반 서비스 인증·평가제도를 신청 및 인증받은 업체 100개사를 대상으로 실시하였으며 응답한 업체는 57개사였다.

4.2.1. 평가범위 변경을 위한 타당성 분석

현행 인증·평가제도(i-Safe)의 평가범위는 업종별로 크게 A그룹 및 B그룹으로 구분하여 평가범위를 설정하였다. A그룹은 금융, 병원 등 고도의 보안을 요하는 업종이며, B그룹은 A그룹을 제외한 일반 업종을 의미한다. 먼저 업종별로 웹사이트를 통하여 정보를 수집하거나 취급하는 정보의 중요도(수준)를 분석해 보았는데, 분석결과를 보면 B그룹이라 할 지라도 수집·취급하는 정보가 높은 수준의 정보를 수집·취급하고 있다는 것을 알 수 있었다. 따라서 적용하는 평가범위를 A그룹과 동일하게 적용하여야 할 필요성이 있으며 또한 A그룹이라 할 지라도 웹사이트를 통하여 수집·취급하는 정보의 수준이 낮을 수도 있다는 것이다. 따라서, B그룹에 적용하는 평가기준을 A그룹에 적용할 수도 있다는 것을 알 수 있었다.

4.2.2 위험평가 변경을 위한 타당성 분석

적절한 보안체계를 수립하기 위해서는 보호가 필요한 대상과 관리가 필요한 위험이 무엇인지를 파악하여 이에 대한 적절한 보안대책을 수립하는 위험평가가 수행되어야 한다. 안전하고 신뢰할 수 있는 웹기반 서비스의 보안관리체계를 마련하기 위해서는 위험평가가 필요하지만, 사고발생 빈도 및 손상정도에 대한 데이터가 제한되기 때문에 정확한 위험평가가 어려운 상황이며, 이러한 제한으로 인해 위험평가 자체에 대한 불필요성이 제기되기도 한다. 이러한 한계를 극복하기 위해 다양한 위험평가 방법 및 기법 즉, 인터뷰, 설문지, 체크리스트, 문서검토, 자동화된 점검도구, 모의해킹, 위험 시나리오 기법, 위험수준 매트릭스 등이 사용되고 있다.

본 연구에서 수행한 설문결과를 분석해보면 업체의 인증업무담당자의 보안업무 경력이

낮은데다가 업무범위 역시 넓은 것으로 나타나 적용하고 있는 위험평가 방법은 국내 현실을 반영하지 못한 것이라 할 수 있겠다 (표 2, 표 3, 표 4 참조). 따라서, 인증기관 위주로 신청기관을 평가하여 피드백해줄 수 있는 위험평가방법을 도입할 필요가 있다.

< 표 2 > 업종별 정보수집 내용

업종별 / 정보의 중요도별	A그룹	B그룹	계
High	5개사	5개사	10
Medium	2개사	41개사	43
Low	-	4개사	4
계	7	50	57

< 표 3 > 인증업무 담당자의 IT경력

업종별 / 경력	A그룹(중요)	B그룹(보통)	계
5년 이상	3명	6명	9명
2년이상~5년미만	3명	17명	20명
2년 미만	1명	27명	28명
계	7명	50명	57명

< 표 4 > 인증 업무 담당자의 위험평가 대응정도

업종		A그룹			B그룹			계
경력		2년이하	2년~5년	5년이상	2년이하	2년~5년	5년이상	
수준	D(어렵다)	1명	3명	1명	22명	14명	4명	45명
	M(보통)	-	-	2명	5명	3명	2명	12명
	E(쉽다)	-	-	-	-	-	-	-
계		1명	3명	3명	27명	17명	6명	57명

4.3 웹기반 서비스 인증·평가체계 제시

본 절에서는 기존의 보안 인증·평가체계를 비교 분석한 결과를 토대로 보안전문가의 인터뷰를 통하여 문제점을 객관화시키고 인증·평가체계의 평가지표 변경에 대한 타당성을 검증하여, 국제환경에 맞는 국제 표준수용을 반영하여 안전하고 신뢰할 수 있는 웹기반에서의 인증·평가 체계를 제시하고자 한다.

본 논문에서 제시하는 인증·평가체계는 기존 평가체계를 적용해 보았던 신청업체

및 인증 업체를 대상으로 인터뷰한 결과를 분석하여 웹의 발전과정에 따른 평가 요인을 반영하고 앞 장에서 연구·분석한 CC를 비롯, 영국의 BS 7799 등 정보시스템 평가방법론의 특성을 고려하여 작성하였다.

본 논문에서 제안하는 인증·평가체계는 크게 5단계로 구분할 수 있다. 1단계 보안정책 수립, 2단계 평가범위 설정, 3단계 위험평가·분석, 4단계 위험관리, 5단계 사후관리 등이다(표 5참조).

< 표 5 > 기존 및 개선된 웹기반 서비스 인증·평가체계 비교

구분	Task	기존 평가지표	개선 평가지표
1단계	보안정책	-	수집 / 취급하고 있는 정보의 중요도에 따라
2단계	평가범위	업종의 중요도에 따라 차등 적용	정보의 중요도에 따라 차등 적용
3단계	위험평가	자가점검 레포트 모의 해킹 현장실사 점검	·자동화된 위험평가 툴의 활용(BS7799위주로) ·개별 제품/서비스의 기능 평가(CC위주로)
4단계	위험관리	-	자체 취약성 점검보안관제서비스 활용
5단계	사후관리	-	자체 보안감사 제도 도입(자율규제로의 유도)

1) 1단계 : 보안정책 수립대상 지정

인증·평가체계의 평가지표를 위한 타당성 분석결과를 보면 웹사이트를 통하여 수집 및 취급되고 있는 정보는 업종별에 따라 구분하는데 에 한계가 있다는 것을 알 수 있었다. 따라서, 보안정책도 인증·평가 프레임워크 내에서 획일적으로 적용되어서는 안된다고 보며 취급하고 있는 정보의 중요도에 따라 각각 다르게 적용하여 작성·수행해야 한다. 인터넷뱅킹서비스 등 중요정보를 수집·취급하는 은행과 단순 정보를 수집·취급하는 포탈사이트에게는 다른 수준의 보안 요소가 요구되기 때문이다. 따라서 평가범위의 수정이 불가피하며 그에 따라 보안정책 수립단계에서부터 그 기준에 따라 적용되어야 할 것이다.

< 표 6 > 정보보호정책수립 대상분류

취급정보의 중요도	High	Medium	Low
정보의 종류	신용정보 등	개인정보 등	식별정보 등

2) 2단계 : 평가범위 지정

정보의 중요성에 따라 평가범위를 정하되 좀 더 세부적으로 구분을 지울 수 있다. 정보의 중요도를 High, Medium, Low로 정하고 평가항목 적용 범위는 현재 크게 물리

적 기준, 기술적 기준, 관리적 기준 등 3분야로 구분하여 적용하고 있다. 따라서, 이를 기준으로 정보보호 정책수립 대상이 관리하는 정보의 중요성에 따라 각기 다른 기준의 준용이 필요하다 하겠다. High는 물리적, 기술적, 관리적 기준을 모두 적용하여야 하나 Medium은 기술적, 관리적 기준을, Low는 관리적 기준만을 준용해도 된다.

이는 최소의 비용으로 최대의 효과를 얻을 수 있는 보안 대응책을 마련하기 위해서는 현재 보유하고 있는 정보 중에서 가장 중요한 순으로 최약점을 내포하는 부분을 해소하는 방안을 마련해야 하기 때문이다.

< 표 7 > 정보보호정책수립 대상별 관리범위

구분		정보보호정책수립 대상		
		High	Medium	Low
관리 범위	물리적 기준	○		
	기술적 기준	○	○	
	관리적 기준	○	○	○

3) 3단계 : 위험 평가·분석 실시

위험분석은 크게 사전위험분석과 상세위험분석으로 구분한다. 사전위험분석은 기본통제로 웹사이트를 통해 자가점검이 가능하도록 평가기준을 설문화하여 추진한다. 또한 모의해킹테스트를 통해 원격 취약성 점검을 진행한다.

전자의 예는 미국의 소비자보호단체인 TRUSTe가 운영하고 있는 인터넷 소비자보호에 대한 자율규제 제도인 TRUSTe마크이다. 동 기관은 웹사이트상에서 TRUSTe마크를 신청접수를 받으면서 자가점검 방식을 사용하여 소비자보호의 중요성을 홍보하고 있다. 이 같은 웹사이트상 자가점검방식의 사전위험분석은 웹 사이트를 운영하고 있는 국가기관, 금융기관, 인터넷사업자, 단순정보제공자에게 정보보호의 중요성과 관심을 유도할 수 있는 계몽적 성격도 나타낸다.

반면 후자의 모의 해킹테스트는 관련기관이나 사업체의 보안실태를 띄고 있어 특별한 보안이 요구된다. 현재 해킹은 사전에 해킹사실을 통보했든, 자신의 해킹기술을 점검하기 위해 실수로 했든 형사입건이 된다. 정보보호시스템에 대한 사전위험분석을 위한 모의해킹은 사전에 모의해킹 동의서를 작성하고 스캐닝 툴을 이용하여 패스워드를 유추하고 원격적으로 침투를 시도하여 Local Root 권한을 확보하고 모의 Backdoor를 설치하고 주위 네트워크로 추가 해킹을 시도한 후 침투 경로 및 취약성관련 레포트를 제출하는 것으로 이루어진다.

위험분석단계에서 자가점검보고서 및 모의해킹 대신 자동화된 위험분석 툴을 도입 시행하는 방안이 있을 수 있다. 특히 국제표준인 BS7799를 적용한 툴을 적용한다면 국제환경에 맞는 웹기반 서비스를 제공할 수 있다.

또한 현재 웹의 발전과정을 반영하여 웹서비스(소프트웨어) 도입이 가속화 되고 있

는 현실을 감안할 때 국제표준인 CC를 기반으로 소프트웨어 평가기법을 도입하여 인증·평가할 필요성도 있다.

4) 4단계 : 위험관리 수행

위험관리방법은 크게 자체 원격 취약성 점검결과를 분석하고 이에 따른 보안대책을 선택하고 검증하는 방법과 외부 전문기관에 보안관제서비스를 의뢰하고 추가적인 관리사항을 점검하는 방법이 있다. 보안관제서비스는 공공기관이나 대기업을 중심으로 적극 활용되고 있다.

인증업체의 방문실사 및 인터뷰 결과 인증업무 담당자 1명의 전담인력이 서버 60대를 운영하는 경우도 있고, 수십대 서버의 비밀번호를 모두 1234로 기억시켜 놓은 경우도 있고, 방화벽 설치를 웹서버 앞단에 설치하여 인터넷 접속부하를 가중시키는 등 시스템에 대한 지식이 부족한 인력으로 정보시스템을 운영하는 경우도 있고, 시스템 관리 전담이 아닌 다른 행정적인 업무를 겸직하는 경우도 많아 패치를 할 수 있는 시간이 없는 경우도 많은 것이 우리의 현실이다. 이에 위험분석을 통한 효율적인 위험관리를 위해서는 전문인력의 추가 배정 또는 보안관제서비스 전문업체를 선정하든지 해야만 해킹을 통한 고급 기밀정보의 유출을 최소화시킬 수 있다.

5) 5단계 : 사후관리

사후관리는 보안대책 수립과 관리를 통하여 수행할 수 있다. 보안대책 수립은 크게 3가지로 구분한다. 첫째, 지침서 개발 및 총괄계획 수립 둘째, 교육 및 훈련실시 셋째, 잔류 위협 평가이다. 보안대책 관리는 자체 유지보수 및 보안감사 실시(모니터링 포함)방법과 외부 전문기관의 보안관제서비스를 이용하여 유지보수 및 보안감사를 실시하는 방법이 있다.

5. 결론 및 향후연구

본 논문은 정보보호의 중요성이 과거 공공기관에서 민간기관으로 확산되고 있으며 웹기반으로 하는 다양한 서비스의 확대에 따른 신뢰문제를 감안하여 웹기반 서비스 시스템의 인증·평가제도 개선방향을 제시하였다. 그러나 웹기반 서비스 인증·평가모델 작성이 기존의 인증·평가제도를 기반으로 보안관리체계 인증의 대표적인 평가방법론인 BS 7799와 시스템/제품 기능의 인증 평가방법론으로 새로 부각되고 있는 CC를 이용하여 각색하였지만, 향후 제안된 평가모델의 검증이 객관적으로 실증 검토되어야 할 것이다. 이를 위하여 다음과 같은 추가적인 연구가 수행되어야 할 것이다.

웹 서버 및 웹 서비스 등 웹 환경에서의 보안기능을 요구하는 제품에 대한 평가하기 위한 구체적인 CC기반의 평가항목를 개발해야 하며, 평가항목별 가중치 적용을 통한 평가대상 서비스의 정보보호수준을 구체적으로 제시하여 피드백할 수 있는 기회를 제공하여야 한다.

웹기반 서비스는 인터넷을 매체로 활용하기 때문에 전 세계적으로 모든 이용자들에게 서비스의 개방성과 접근성을 제공한다. 예를들어 다국적 은행기업인 시티뱅크는 매우 높은 브랜드파워를 지니고 있기 때문에 서비스를 제공할 때 직면하는 신뢰의 문제를 무색하게 만든다. 하지만 국내 어느 중소기업이 개발한 웹기반 서비스를 외국의 다른 이용자에게 판매하고자 한다면, 상황은 전혀 달라질 것이다. 외국의 소비자는 무명의 국내기업을 신뢰하지 못할 것이기 때문이다. 따라서, 국제간 인증·평가제도의 상호인정에 대한 노력도 필요할 것이다.

6. 참 고 문 헌

[1] 강행연, 남길현, "정보보호관리규격(BS7799)을 적용한 국방정보체계 정보보안관리모델에 관한 연구", 2001년도 한국정보보호학회 학술대회논문집, 2001 : 459-460

[2] 김승렬, 김현수, 엄익천, "웹 서비스의 평가인증 제도에 관한 탐색적 연구", 한국전산원 정보화정책, 2003 : 99

[3] 이병욱, "정보보호관리체계 인증제도 추진현황", 정보보호심포지움 자료집, 한국정보보호진흥원, 2002 : 341-342

[4] 이창길, 조영훈, 김석우, 서창호, "안전하고 신뢰할 수 있는 인터넷사이트 평가 가이드라인 도입에 대한 연구", 제13회 정보보호 및 암호에 관한 학술대회 논문집, 한국전자통신연구원 부설 국가보안기술연구소, 2002 : 494-504

[5] 이창길, 조영훈, 한태인, 정재연, "인터넷모범상점인증제도 도입방안에 관한 연구", 정보통신부 연구보고서, 1999 : 37-68

[6] Common Criteria Editorial Board, "Common Criteria for Information Technology Security Evaluation, Part 1-4 : Introduction and General Model, Version 2.1", 1999

[7] France, Germany, The Netherlands, and The United Kingdom, "Information Technology Security Evaluation Criteria(ITSEC) V.3.0", 1993

[8] ISO/IEC, "ISO/IEC TR 13335-1:1996(E)~1998(E) : Information Technology - Guidelines for the Management of IT Security part 1", 2000

[9] National Computer Security Center, "Trusted Network Interpretation of The TCSEC(TNI), NCSC-TG-005", 1987

[10] National Computer Security Center, "Trusted Database Management System Interpretation of The TCSEC(TDI), NCSC-TG-02", 1992

저 자 소 개

서 광 규 : 고려대학교 산업시스템정보공학과에서 박사학위취득,
한국과학기술연구원(KIST) 시스템연구부 연구원으로 재직,
현재 상명대학교 산업정보시스템공학과 교수로 재직중.
관심분야는 정보시스템, 생산시스템, 멀티미디어, e-business 등이다.