2005 한국경영과학회/대한산업공학회 춘계공동학술대회
2005 년 5 월 13 일~14 일, 충북대학교

전자상거래를 위한 웹사이트 보안 평가에 관한 연구
Website Security Evaluation for Electronic Commerce

김현우, 이근수, 김세헌
한국과학기술원 산업공학과

Abstract

최근 몇 년 동안 전자상거래는 새로운 비즈니스 환경으로 인식되어 급속하게 성장하고 있다. 온라인 상거래가 활성화 되면서 전자상거래를 위한 웹사이트도 많이 생겨나고 있지만, 사기, 개인 및 신용정보 노출, 개인의 사회적 신뢰도 저하 등 전자상거래 보안에 관련된 문제들이 전자상거래 시장의 활성화를 위협하고 있다. 따라서 본 논문에서는 웹 기반의 전자상거래 발전에 있어 보안 문제의 해결이 가장 중요함을 인식하고 전자상거래 웹사이트에 대한 보안 평가 모델을 제시하고자 한다. 이를 위해 전자상거래 보안과 관련한 다수의 보안 평가 항목을 선정하고, AHP(Analytic Hierarchy Process)를 사용하여 영역별 가중치를 산정한 모델을 설계한다. 본 논문에서 제시한 보안 평가 모델은 안전한 전자상거래 웹사이트 설계, 구축 및 운영에 필요한 보안 가이드라인으로 활용될 수 있다.

1. 서론

IT기술의 급속한 발전은 전자상거래라는 새로운 개념의 상거래의 생성과 활성화를 가져왔다. 개인으로부터 기업에 이르기까지 과거 현실 세계에서 오프라인으로 이뤄졌던 상거래를 이제는 웹사이트라는 사이버 매개체를 통해 수행하고 있다. 온라인 상거래가 활성화 되면서 전자상거래를 위한 웹사이트도 많이 생겨나고 있다.

인터넷 쇼핑몰이라는 가상의 공간에서 물건을 고르고 주문하며 값을 지불하는 형태의 전자상거래는 편리함과 시간 및 노력 절약 등 많은 유익함을 제공하는 반면 기존의 오프라인 거래와 달리 온라인 거래의 특성상 거래 당사자의 익명성에 기인한 사기, 개인 신상 및 신용 정보 등의 노출로 인한 사회적 문제들 또한 야기시키고 있다. 이는 전자상거래 웹사이트의 보안 관련 문제로서 전자상거래 비즈니스의 성장을 위해 가장 우선적으로 해결해야 할 문제로 인식되고 있다 [5]. 이런 보안 취약성을 극복하기 위해서는 전자상거래 사업자가 웹사이트 설계, 구축 단계부터 실제 운영까지의 전 단계에서 지속적으로 보안 취약성에 대한 평가와 보완을 해야 한다. 따라서 안전한 전자상거래 웹사이트 설계, 구축 및 운영에 필요한 보안 가이드라인과 평가 기준의 중요성이 부각되고 있다. 그러나, 전자상거래 보안의 중요성이 크게 대두되고 있는 가운데에도 지금까지 전자상거래 웹사이트에 대한 전반적인 평가를 위한 연구는 많이 수행되어 왔지만 웹사이트의 보안 취약성 측면에 중점을 둔 연구는 거의 없는 실정이다.

본 논문에서는 웹 기반의 전자상거래 발전에 있어 보안 문제의 해결이 가장 중요함을 인식하고 전자상거래 웹사이트에 대한 보안 평가 모델을 제시하고자 한다. 이를 위해 전자상거래 환경에서 고객과 사업자에게 위협 요소가 될 수 있는 취약점을

본 연구는 정보통신부 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음

중심으로 다수의 평가 항목을 선정하고, 보안 평가 항목으로 구성된 보안 평가 모델의 개발을 위해 AHP(Analytic Hierarchy Process)를 사용하여 영역별 가중치를 산정한 모델을 설계한다.

본 논문의 구성은 다음과 같다. 2장에서는 전자상거래 보안 위협 요소와 지금까지 전자상거래 웹사이트 평가에 대한 관련 연구를 고찰해보고 3장에서는 보안 평가 모델을 구성하는 세부 보안 평가 항목을 선정하여 제시한다. 4장에서는 AHP를 사용한 데이터 수집과 분석 방법을 설명하며, 5장에서 분석 결과와 최종 웹사이트 보안 평가 모델을 제시한 후 6장에서 결론을 맺는다.

2. 관련 연구

2.1 전자상거래 보안

전자상거래의 성공을 위한 가장 중요한 요소는 보안이며, 이와 관련한 전자상거래 시스템을 위협하는 보안 요소에 관한 많은 연구가 진행되었다.

개인정보보호는 전자상거래에 있어 가장 일반적인 보안 이슈이며, 전자공간에서의 신뢰 구축에 필수적인 거래 당사자의 신분 확인도 전자상거래의 활성화를 위한 주요 기반요소가 된다 [10]. 현재 암호기술이 개인정보를 보호하기 위한 수단으로 널리 이용되고 있으며, 암호기법에 기반한 디지털 서명 방식, 사람의 생체특성 방식 등의 기술이 전자상거래 거래 행위의 신뢰성 보장을 위한 거래 당사자 신분확인에 활용되고 있다.

네트워크와 전자상거래 웹사이트에 대한 해킹과 바이러스 공격 또한 전자상거래의 중요한 위협요소이다 [7]. 방화벽 시스템을 비롯한 침입탐지시스템, 정보복구시스템 등의 기술이 웹 기반의 시스템 보안을 위해 주로 사용되고 있으며, 이들 요소들을 결합한 통합시스템의 개발로 보안취약성을 해결하려는 연구가 활발하게 진행되고 있다. 전자상거래의 보안 위협 요소들로부터 안전한 전자상거래 환경을 확보하기 위해 개인정보보호기술, 지불 보안기술, 웹 보안기술, 인증기술 등의 보안기술을 개발하고 활용하는 것도 중요하지만, 제도 및 정책, 관리 및 운영측면의 보안요소들 또한 함께 고려되어야 한다 [4]. 이러한 요소들은 조직 구성원을 포함한 내부로부터 기인한 취약성을 보완하고 최소화시킬 수 있는 방편으로써 현재 발생하고 있는 전자상거래 보안사고의 가장 큰 부분을 차지하고 있는 비기술적인 보안위협에 대한 대비책이 될 수 있다.

2.2 전자상거래 웹사이트 평가

전자상거래에서 웹사이트는 쇼핑몰의 성공여부를 결정하는 중요한 요소이다. 그 외에도 인터넷 쇼핑몰의 성공에 영향을 미치는 요소들은 매우 다양하며 이와 관련한 많은 연구들이 수행되었다.

전자상거래를 일반적인 상거래 입장에서 본다면 가격, 제품의 질, 편리성, 쇼핑의 즐거움, 정보제공의 다양성, 소비자 맞춤형 거래, 안전성, 신속한 배달, 용이한 반품 등의 요소가 기본적인 인터넷 쇼핑몰의 성공요인으로 분석될 수 있다 [6]. 여기에 인터넷 쇼핑몰을 이용하는 소비자의 사용 편리성 측면을 추가한다면 사용자 인터페이스를 강조할 수 있는 기본 컨텐츠가 도출될 것이다. 또한 쇼핑몰의 고객 만족도를 분석하기 위해 위험성과 경제성, 윤리성을 독립변수로 설정하여 만족도와의 영향 관계를

분산분석을 통해 설명하기도 하였으며 만족도가 높을수록 재구매 의도가 높음을 보인 연구도 있다 [3].

전자상거래 활성화를 위한 위와 같은 연구 외에도 인터넷 쇼핑몰이 성공하기 위한 최상위 수준의 요인은 소비자의 쇼핑몰에 대한 trust임을 인식하고 이에 따른 영향 요소를 분석한 연구도 있다 [6]. Trust와 위험인지는 서로 상반된 의미로서 소비자들이 인터넷 쇼핑몰에 대한 위험을 인지하는 여러 요인들 중에서 쇼핑몰의 물리적 존재 여부 및 규모, 쇼핑몰의 인지도(reputation) 등이 소비자의 trust에 가장 큰 영향을 미치는 요인들이다. 이와 더불어 소비자들의 사이버 쇼핑몰 선택에 미치는 요인 분석에서 정보보안 요인이 가장 중요하며 카드결제, 회원등록 정보 등의 유출에 대한 안심도가 가장 많은 영향을 미친다. 소비자들의 trust를 얻기 위해서는 결과적으로 신용과 정보 노출에 대한 안전감을 느낄 수 있도록 배려하는 사이트 구축이 필요하다 [2].

Stephen R.E. et al.은 다양한 종류의 전자상거래 웹사이트에 적용할 수 있는 평가 모델을 개발하기 위해 이론적 연구와 실제 웹사이트에 대한 실증적 연구를 통해 6개의 평가분야에 대한 세부 평가 요소를 제시하였다 [9]. 더불어 웹사이트 평가의 공정성을 기하기 위해 구분된 평가 요소들에 AHP 기법을 사용한 연구도 진행되었다 [1]. 평가 요소들에 각 항목별, 분야별 가중치를 적용하여 평가 요소들의 중요도 차별화를 이용하면 더욱 객관적인 웹사이트 평가 결과를 얻을 수 있다.

3. 웹사이트 보안 평가 요소

이상의 관련 연구에서와 같이 전자상거래 환경에서 보안의 중요성과 이에 대한 실질적인 대책의 필요성은 점점 크게 인식되고 있는 상황이다. 본 논문에서는 전자상거래 웹사이트 개발자나 운영자, 관리자들이 실제 활용할 수 있는 실질적이고 체계화된 보안 기준을 제시하기 위해 기존의 연구 및 자료를 통해 전자상거래 웹사이트 보안 평가에 적용할 수 있는 보안 평가 요소들을 도출하였다. 보안 평가 요소들은 크게 보안 기술, 보안제도 및 정책, 보안관리 및 운영의 세 영역으로 나뉘며, 각 영역별 세부 평가 항목들을 살펴보면 다음과 같다.

1) 보안기술

▪인증

거래 고객 본인 인증, 고객이 사용하는 신용카드 등 지불 수단에 대한 인증과 고객과 거래를 위해 전송되는 거래 정보에 대한 인증을 포함한다.

▪응용프로그램 보안

전자상거래 서비스를 제공하는 응용프로그램의 알려진 또는 알려지지 않은 보안 취약성 및 안정성(stability) 결함에 대한 즉각적이고 지속적인 보완을 통한 안정적인 서비스 제공으로 신뢰도를 향상시킨다.

▪로그 및 감사

서버에서 일어나는 모든 이벤트에 대한 기록과 임의 삭제 또는 변경을 방지하고 지속적인 감사를 통한 보안 대책으로 로그 자료에 대한 접근 통제 또는 별도의 로그 기록 장치를 통한 로그의 무결성을 보장한다.

▪사용자 접근통제

전자상거래 업무 외의 인원에 대한 계정 부여를 금지하고 각 계정별 리소스 접근권한

을 차등적으로 부여하여 불필요한 인원에 대한 접근을 차단, 보안 툴을 통한 원격접속(텍스트 환경에서 원격접속 금지) 및 퇴근 후 사외(社外)로부터의 원격접속을 차단하여 보안 취약 요소를 사전에 제거한다.

▪통신보안

제 3자에 대한 고객과 웹 서버간 전송되는 모든 데이터의 노출을 방지해야 하며, 이를 위해 키 로깅(key logging) 보안 프로그램 및 전송 데이터에 대한 암호화 통신 서비스를 제공한다.

▪침입탐지/방지 시스템

외부 또는 내부로부터의 불법적인 침입을 차단 또는 탐지하고 각종 바이러스, 웜 등으로부터 내부 망과 웹 서버를 보호하기 위해서 침입탐지시스템(Intrusion Detection System), 방화벽(Firewall), 백신 프로그램(Anti-virus program)을 설치한다.

▪고객 정보보호

고객 및 거래 정보를 웹 서버에 보관 시에는 고객의 동의를 얻어 암호화해서 저장 관리하며, 백업 장치로 유사시 정보의 손실을 방지한다.

2) 보안제도 및 정책

▪정보보호정책

전자상거래를 위한 정보보호정책이 수립되어 있으며 안전한 서비스 제공을 위한 환경에 적합하고 실행 가능해야 한다.

▪보안사고 처리

고객 관련 보안 사고가 발생할 경우, 고객에 대한 피해 보상과 적절한 포상과 처벌로 유사 사고 재발을 방지하고 보안의식을 고취시킨다.

3) 보안관리 및 운영

▪보안통제관리

사용자 계정과 패스워드의 안전한 관리 및 갱신, 휴면 계정의 삭제, 로그인 연속 실패 시 벌점(penalty) 적용과 웹 서버에 대한 비인가자의 물리적인 접근 제한 및 관리 활동을 포함한다.

▪서비스관리

시스템 및 네트워크에 대한 항시 모니터링(monitoring) 체계와 웹 서버의 멀티 서비스(multi service)의 통제, 대용량 트래픽에 대한 효과적인 처리로 고객에 대한 차원 높은 전자상거래 서비스를 제공한다.

▪조직 및 인력관리

전자상거래 보안을 위한 전담 조직을 구성하고 책임자 임명 및 보안 역할에 따른 업무의 할당, 보안 교육과 훈련의 지속적인 실시로 전반적인 보안 수준의 제고를 위한 인적/조직적 관리 활동을 포함한다.

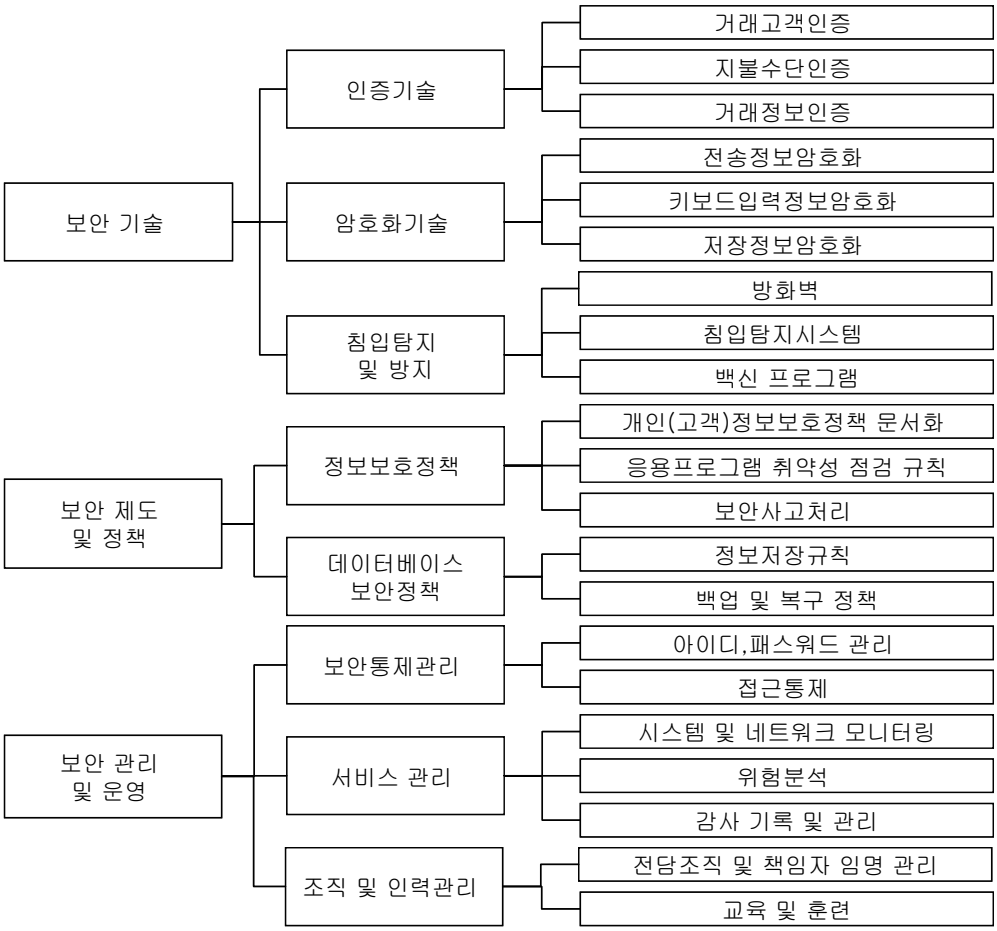
4. 연구방법론

전자상거래 웹사이트 보안 평가 모델을 실제 시스템에 효과적으로 적용하기 위해서는 보안 평가 항목들간의 상대적인 가중치가 필요하다. 이를 위해 본 연구에서는 보안 평가 항목들의 우선 순위를 결정하기 위해 과학적 타당성을 인정받고 있는 AHP 방법론을 이용하였다. AHP는 복잡한 문제를 단순화시켜 합리적인 의사결정이 가능하도록 지원해주는 계층적 분석 방법론으로 복수의 요소들에 대한 가중치를 동시에 고려하기 보다는 두 개씩 짝을 지어 이원비교를 하게함으로써 조사하려는 요소들 사이의 상대적 중요도 판단을 명확하고 용이하게 할 수 있게 해 준다 [8]. 또한, 요소들 사이의 상대적 중요도를 판단할 때 판단의 일관성 정도(consistency ratio)를 알려주어 일관성이 결여되었을 때에는 수정작업을 가

능하게 해 준다.

AHP를 사용하기 위해서는 먼저 해결하고자 하는 문제를 하위의 구성 요소들로 분해하여 계층적으로 나타내어야 하는데, 이를 위해 본 연구에서는 3장의 보안 요소들을 실제 평가에 적용할 수 있도록 세부 항목으로 재분류하여 계층적인 모델을 작성하였다. <그림 1>은 3계층으로 구분한 웹사이트 보안 평가 항목의 계층 모델을 나타낸 것이다.

AHP를 사용하여 보안 평가 항목들 간의 우선 순위를 도출하기 위해서는 전문가조사(Delphi approach)를 통해서 관련 데이터를 수집하여야 한다. 본 논문에서는 전자상거래 기업의 관리자와 개발자를 비롯하여 정보보호 연구기관 연구원을 대상으로 각 계층에 속하는 보안 평가 항목간의 상대적 중요도를 측정하는 설문조사를 실시하였다. 설문척도는 의사결정 요인의 이원비교를 위해 1점에서 9점까지의 수치로 표현하였는데, 1은 비교하는 두 보안 평가 항목의 동등한 중요도를 나타내고, 9는 한 평가 항목이 절대적으로 중요함을 나타낸다.



<그림 1> 웹사이트 보안 평가 항목의 계층 모델

전문가 설문조사를 통해 획득한 결과는 AHP 방법론을 적용하여 분석하는데,

각 보안 평가 항목간의 우선 순위를 결정한 후 영역별 가중치를 산정한다. 이 과정에서 사용한 AHP 방법론을 간단히 설명하면 다음과 같다.

설문조사를 통해 우선 순위를 체계적으로 구하기 위해서는 중요도 척도에 따른 이원비교행렬을 다음과 같이 구성해야 한다.

$$A=\begin{bmatrix} w_1/w_1 & w_1/w_2 & \mathrm{L} & w_1/w_n \\ w_2/w_1 & w_2/w_2 & \mathrm{L} & w_2/w_n \\ \mathrm{M} & & & \mathrm{M} \\ w_n/w_1 & w_n/w_2 & \mathrm{L} & w_n/w_n \end{bmatrix}$$

여기서 w_i 와 w_j 는 i번째 속성과 j번째 속성의 가중치를 나타내는데, w_i/w_j 는 i 가 j 에 미치는 상대적인 우월성을 나타내게 되므로, 주 대각선의 원소들이 모두 1이 되는 역수행렬이 된다.

이원비교의 결과를 나타내는 행렬의 고유벡터(eigenvector)를 이용하면 어느 한 계층 내의 요소들 사이의 가중치를 구할 수 있는데, 이 가중치는 각 요소들 간의 상대적 중요도를 나타낸다. 일반적으로 $n\times n$ 의 행렬 A 에 대하여 $[AW=\lambda W]$ 를 만족하는 스칼라 λ 와 $n\times 1$ 의 고유벡터 $W(=(W_1,W_2,\cdots,W_n)^T)$ 가 존재하는데, 이러한 경우 $\lambda_{\max}$ 에 대응하는 고유벡터 W 가 운데에서 $\Sigma W_j=1$ 을 만족하는 고유벡터가 그 계층 내의 요소들 간의 가중치가 된다.

행렬 A 의 일관성의 정도가 클수록 $\lambda_{\max}$ 는 n 에 가까워지며, 이러한 특성을 이용하여 일관성 지수(consistency index: CI)를 다음의 식을 통해 구할 수 있다.

$$CI=(\lambda_{\max}-n)/(n-1)$$

CI와 경험적 자료로 얻어진 평균 무작위 지수(random index: RI)의 비율을 일관성 비율이라 하는데, 일관성 비율이 10% 이내인 경우에 우선순위에 무리가 없는 신뢰할 수 있는 결과라 할 수 있다.

5. 전자상거래 웹사이트 보안 평가 모델

전자상거래 웹사이트 보안 평가는 다양한 평가 항목들을 차별적으로 적용시킴으로써 더욱 객관적인 결과를 얻을 수 있다. 이를 위해 본 연구에서는 AHP 기법을 이용하여 웹사이트 보안 평가 모델을 구성하는 보안 평가 항목들의 영역별 가중치를 산정하였다. <표 1>은 관련 데이터를 얻기 위해 실시한 설문조사의 대상 분포를 나타낸 것이다.

<표 1> 설문조사 대상 분포

설문 응답자	응답자	분포(%)
정보보호 연구기관 연구원	7	26
전자상거래 기업 관리자	9	33
전자상거래 기업 개발자	11	41
합 계	27	100

<표 2>는 웹사이트 보안 평가 항목의 영역별 가중치를 계산한 결과이다. 최상위 계층에서는 보안 기술 항목의 중요도가 매우 크게 나타났으며, 보안 기술의 두 번째 계층에서는 인증기술이 암호화 기술이나 침입탐지 및 방지기술에 비해 중요한 요소임을 알 수 있다.

<표 2> 웹사이트 보안 평가 항목의 영역별 가중치

구분	평가 영역	세부 평가 항목
보안 기술 (0.630)	인증기술 (0.600)	거래고객인증 (0.568)
		지불수단인증 (0.231)
		거래정보인증 (0.201)
	암호화 기술 (0.200)	전송정보암호화 (0.630)
		키보드입력정보암호화 (0.188)
		저장정보암호화 (0.182)
	침입탐지 및 방지 (0.200)	방화벽 (0.297)
		침입탐지시스템 (0.086)
		백신 프로그램 (0.617)
보안 제도 및 정책 (0.188)	정보보호정책 (0.833)	개인(고객)정보보호정책 문서화 (0.142)
		응용프로그램 취약성 점검 규칙 (0.429)
		보안사고처리 (0.429)
	데이터베이스보안정책 (0.167)	정보저장규칙 (0.750)
		백업 및 복구 정책 (0.250)
보안 관리 및 운영 (0.182)	보안통제관리 (0.584)	아이디,패스워드 관리 (0.250)
		접근통제 (0.750)
	서비스 관리 (0.135)	시스템 및 네트워크 모니터링 (0.099)
		위험분석 (0.797)
		감사 기록 및 관리 (0.104)
	조직 및 인력관리 (0.281)	전담조직 및 책임자 임명 관리 (0.750)
		교육 및 훈련 (0.250)

산정된 영역별 가중치를 이용하면 세부 평가 항목들이 전체 웹사이트 보안 평가 모델에서 차지하는 가중치를 구할 수 있다. 실제 웹사이트 보안 평가에 세부 평가 항목들을 가중치 별로 적용한다면 보다 객관적인 보안 평가 결과를 얻을 수 있을 것이다. <표 3>은 전체 가중치가 큰 순서로 세부 보안 평가 항목들을 나열한 것으로 보안 평가 항목의 전체 우선 순위를 나타낸다.

6. 결론

본 논문에서는 웹 기반의 전자상거래 발전을 위해 가장 중요한 전자상거래 보안 문제를 해결하기 위한 방편으로 전자상거래 웹사이트에 대한 보안 평가 모델을 제시하였다. 보안 평가 모델은 전자상거래 보안과 관련한 다수의 보안 평가 항목으로 구성되었으며, 실제 전자상거래 웹사이트 보안 평가에 효과적으로 적용될 수 있도록 AHP를 사용하여 영역별 가중치를 산정하였다.

본 논문에서 제시한 전자상거래 웹사이트 보안 평가 모델을 실제 전자상거래 웹사이트의 관리에 적용하면 고객에게 안전한 전자상거래를 통한 신뢰감을 조성하여

웹 기반 비즈니스의 활성화를 도모할 수 있으리라 기대된다.

<표 3> 보안 평가 항목 우선 순위

보안 평가 항목
거래고객인증
지불수단인증
접근통제
전송정보암호화
백신 프로그램
거래정보인증
응용프로그램 취약성 점검 규칙
보안사고처리
전담조직 및 책임자 임명 관리
방화벽
아이디,패스워드 관리
키보드입력정보암호화
정보저장규칙
저장정보암호화
개인(고객)정보보호정책 문서화
위험분석
교육 및 훈련
침입탐지시스템
백업 및 복구 정책
감사 기록 및 관리
시스템 및 네트워크 모니터링

참고 문헌

[1] 서수석, 이종호, "AHP 를 이용한 전자상
거래 웹사이트 평가 모델 개발", 한국전자상거래학회, 하계학술대회, 2004, pp. 1-17.

[2] 유한종, "사이버쇼핑몰의 소비자행동에 관한 연구", [한국인터넷정보학회], 제 3 권, 1 호(2002), pp.11-16.

[3] 이경원, 지용선, "전자상거래 쇼핑몰의 고객만족에 미치는 영향에 관한 연구", [전자상거래학회지], 제 2 권, 2 호(2001), pp.3-19.

[4] Arce, I., "The Weakest Link Revisited", *IEEE Security & Privacy Magazine*, Vol. 1, Issue 2(2003), pp. 72-76.

[5] Hopwood, W. S., "Security in a Web-Based Environment", *Managerial Finance*, Vol.26, No.11(2000), pp.42-54.

[6] Jarvenpaa, S. L., Tractinsky, N., and Vitale, M., "Consumer trust in an Internet store', *Information Technology & Management*, Vol. 1, No.1/2(1999), pp.45-71.

[7] Marchany, R. C., and Tront, J. G., "E-commerce Security Issues", Proc. 35th Hawaii Intl. Conf. on System Science, 2002.

[8] Saaty, T. L., *Decision-Making for Leaders: The Analytical Hierarchy Process for Decisions in a Complex World*. RWS Publications, 1995.

[9] Stephen, R. E. et al., 'Towards a framework for evaluation of commercial Web sites', 13th International Bled Electronic Commerce Conference, June, (2000), pp.69-86

[10] Udo, G. J., "Privacy and Security Concerns as Major Barriers for E-commerce: A Survey Study", *Information Management & Computer Security*, Vol.9, No.4(2001), pp.165-174.