전자상거래를 위한 보안 항목 우선순위 분석: 연구자그룹과 실무자그룹을 중심으로†

(A Priority Analysis on E-Commerce Security Factors - Focused on Researchers and Practitioners)

김 현 우*
(Hyunwoo Kim)

요 약 인터넷의 발달로 새로운 비즈니스 환경으로 인식되어 급속하게 성장한 전자상거래가 최근 WiFi의 보급과 모바일 폰 등으로 결제 수단이 다양해지면서 더욱 가파르게 진화하고 있지만 사기, 개인 및 신용정보 노출, 개인의 사회적 신뢰도 저하 등 전자상거래 시장의 활성화를 위협하는 보안 문제는 여전한 상황이다. 본 논문에서는 웹 기반의 전자상거래 발전에 있어 보안 문제의 해결이 가장 중요함을 인식하고 전자상거래 활성화를 위한 보안 요구사항을 도출하고 분석하고자 한다. 이를 위해 전자상거래 보안과 관련한 다수의 보안 항목을 선정하고, 연구자그룹과 실무자그룹을 대상으로 AHP(Analytic Hierarchy Process)를 사용하여 영역별 가중치를 산정한 모델을 설계한다. 또한 향후 안전한 전자상거래 시스템 설계, 구축 및 운영에 필요한 보안 가이드라인으로 활용될 수 있도록 두 그룹을 통해 나타난 상대적인 우선순위를 비교하여 분석한다.

핵심주제어 : 전자상거래, 보안 항목, 우선순위, AHP

Abstract In e-commerce environment, security should be considered as an essential factor for success. In this paper, we analyze security requirements for e-commerce system, and it is focused on the practical usage, not theoretical contribution, in the field of e-commerce security. To identify the security requirements being specific to e-commerce environment, the researches related to e-commerce security are surveyed and a phase of Delphi method and Analytic Hierarchy Process(AHP) are used to determine the relative importance of e-commerce security factors. Since researchers and practitioners can have significantly different views because of each different work environment, we divide the professionals into two respondents' group. This survey result can be useful security guidelines in the development of e-commerce service system from the initial system development step to the completion.

Key Words : E-Commerce, Security Factor, Priority, Analytic Hierarchy Process(AHP)

1. 서 론

인터넷의 발달과 더불어 성장한 전자상거래는 최근 WiFi의 보급이 확대되고 다양한 모바일 기기가 기존의 개인용 컴퓨터를 대신하게 되면서 또 다시 성장의 확대일로에 있게 되었다. 하지만, 전자상거래가 많은 유익함을 제공하는 반면 기존의 오프라인 거래와 달리 온라인 거래의 특성상 거래 당사자의 익명성에 기

† 이 논문은 2011년도 경일대학교 신임교원정착연구비 지원에 의하여 수행된 것임.
* 경일대학교 경영학부 조교수

인한 사기, 개인 신상 및 신용 정보 등의 노출로 인한 사회적 문제들은 여전히 해결되지 않고 있는 상황이다[1, 2]. 이는 전자상거래 시스템의 보안 관련 문제로서 전자상거래 비즈니스의 발전을 위해 가장 우선적으로 해결해야 할 문제로 인식되고 있다[3]. 이러한 보안 취약성을 극복하기 위해서는 전자상거래 사업자가 시스템 설계, 구축 단계부터 실제 운영까지의 전 단계에서 지속적으로 보안 취약성에 대한 평가와 보완을 해야 한다[4]. 따라서 안전한 전자상거래 시스템 설계, 구축 및 운영에 필요한 보안 가이드라인과 평가 기준의 중요성이 부각되고 있다[5]. 그러나 전자상거래 보안의 중요성이 크게 대두되고 있는 가운데에도 지금까지 전자상거래 시스템에 대한 전반적인 평가를 위한 연구는 많이 수행되어 왔지만 전자상거래 시스템의 보안에 초점을 맞추고 보안 요구사항 측정 및 평가에 중점을 둔 연구는 많지 않은 실정이다.

본 논문에서는 웹 기반의 전자상거래 발전에 있어 보안 문제의 해결이 가장 중요함을 인식하고 전자상거래 활성화를 위한 보안 요구사항을 도출하고 분석하고자 한다. 이를 위해 전자상거래 보안과 관련한 주요 분야별로 다수의 보안 항목을 선정하고, AHP (Analytic Hierarchy Process)를 사용하여 영역별 가중치를 산정한 모델을 설계한다. 또한 업무특성을 고려하여 연구자그룹과 실무자그룹으로 전문가를 나누고 두 그룹을 통해 제안된 보안 요구사항들을 대상으로 상대적인 우선순위를 비교, 분석하여 향후 안전한 전자상거래 시스템 설계, 구축 및 운영에 필요한 보안 가이드라인으로 활용될 수 있도록 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 전자상거래 보안 위협 요소와 관련한 기존 연구를 고찰해 보고 3장에서는 전자상거래 보안 항목을 세부적으로 선정하여 제시한다. 4장에서는 AHP를 사용한 데이터 수집과 분석 방법을 설명하고 전자상거래 보안 요구사항 계층 모델을 제안하며, 5장에서 분석 결과를 제시한 후 6장에서 결론을 맺는다.

2. 전자상거래 보안

전자상거래의 성공을 위한 가장 중요한 요소는 보안이며, 지금까지 전자상거래 시스템의 안전을 위협하는 취약점과 보안 요소에 관한 많은 연구가 진행되었다.

개인정보보호는 전자상거래에 있어 가장 일반적인 보안 이슈이며, 전자공간에서의 거래 당사자의 신분확인을 하는 것은 전자상거래의 활성화를 위한 주요 기반요소가 된다[6]. 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[7].

네트워크와 전자상거래 시스템에 대한 해킹과 바이러스 공격 또한 전자상거래의 중요한 위협요소이다[8]. 방화벽을 비롯하여 침입탐지시스템, 정보복구시스템 등의 기술이 웹 기반의 시스템 보안을 위해 주로 사용되고 있으며, 이들 요소들을 결합한 통합시스템의 개발로 보안 취약성을 해결하려는 연구가 활발하게 진행되고 있다[9].

전자상거래의 보안 위협요소들로부터 안전한 전자상거래 환경을 확보하기 위해 암호화기술, 인증기술 등의 보안기술을 개발하고 활용하는 것도 중요하지만 제도 및 정책, 관리 및 운영측면의 보안요소들 또한 함께 고려되어야 한다[10]. 이러한 요소들은 조직 구성원을 포함한 내부로부터 기인한 보안 취약성을 보완하고 최소화시킬 수 있는 방편으로써 현재 발생하고 있는 전자상거래 보안사고의 가장 큰 부분을 차지하고 있는 비기술적인 보안위협에 대한 대비책이 될 수 있다[11].

3. 전자상거래 보안 항목

전자상거래 환경에서 보안의 중요성과 이에 대한 실질적인 대책의 필요성이 점점 크게 인식되고 있는 상황에서 본 논문은 전자상거래 시스템 개발자나 운영자, 관리자들이 실제로 활용할 수 있는 실질적이고 체계화된 보안 기준을 제시하기 위해 기존의 연구와 도서 등의 자료를 통해 전자상거래 보안에 필요한 요구사항들을 도출하였다[12, 13]. 보안 요구사항들은 크게 보안 기술, 보안제도 및 정책, 보안관리 및 운영의 세 영역으로 나뉘며, 각 영역별 세부 항목들을 살펴보면 다음과 같다.

3.1 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 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 접근권한을 차등적으로 부여하여 불필요한 인원에 대한 접근을 차단, 보안 툴을 통한 원격접속 및 퇴근 후 사외로부터의 원격접속을 차단하여 보안 취약 요소를 사전에 제거한다.

○통신보안

제3자에 대한 고객과 웹 서버 간 전송되는 모든 데이터의 노출을 방지해야 하며, 이를 위해 키 로깅 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 위해 침입탐지시스템, 방화벽, 백신 프로그램 등을 설치한다.

○고객정보 보호

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

3.2 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.

3.3 보안관리 및 운영

○보안통제관리

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

○서비스관리

시스템 및 네트워크에 대한 항시 모니터링 체계와 웹 서버의 멀티 서비스 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 시스템 보안 요구사항을 실제 시스템에 효과적으로 적용하여 활용하기 위해서는 세부 보안 항목들 간의 상대적인 가중치가 필요하다. 이를 위해 본 연구에서는 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 하게 함으로써 조사하려는 요소들 사이의 상대적 중요도 판단을 명확하고 용이하게 할 수 있게 해 준다[14, 15]. 또한 요소들 사이의 상대적 중요도를 판단할 때 판단의 일관성 정도를 알려주어 일관성이 결여

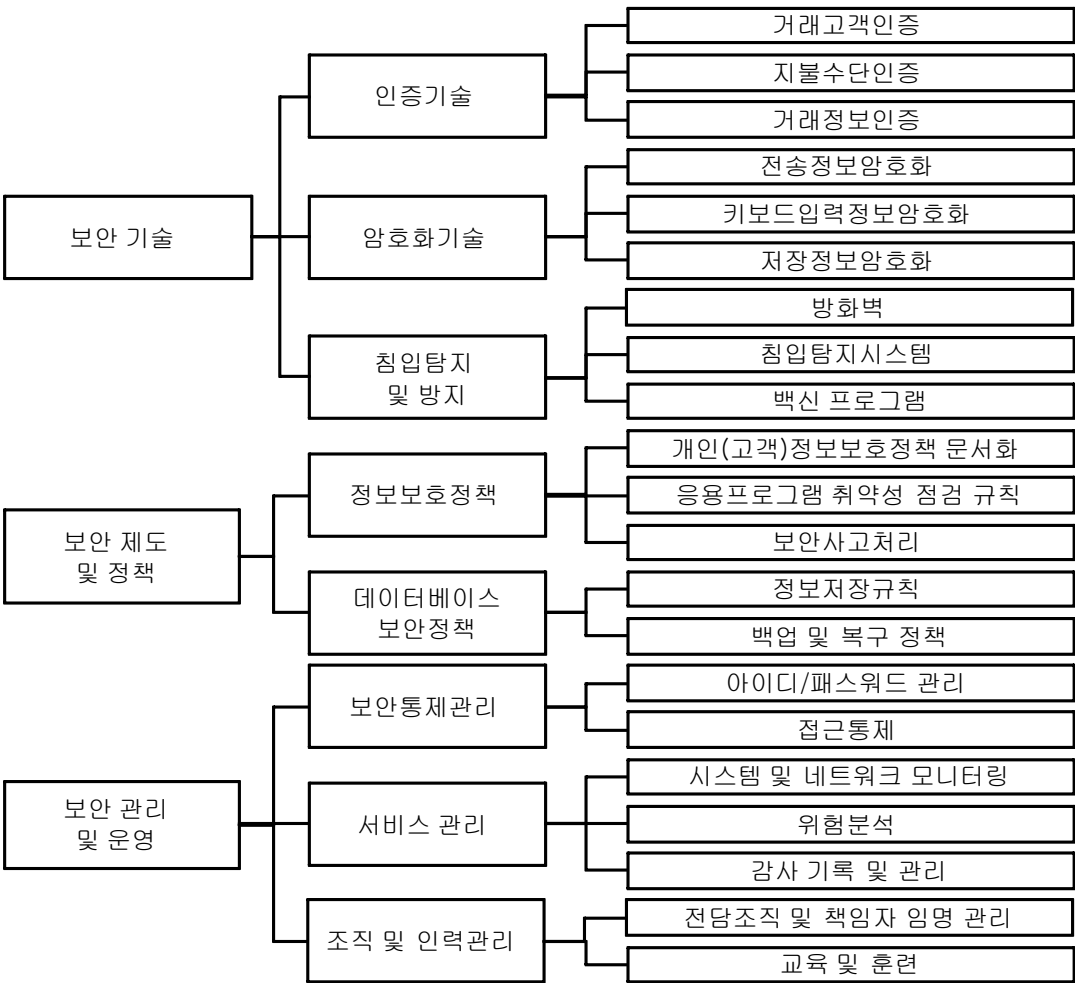
되었을 때에는 수정작업을 가능하게 해 준다.

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 전자상거래 보안 요구사항의 계층 모델을 나타낸 것이다.

AHP를 사용하여 세부 보안 항목들 간의 중요도를 도출하기 위해서는 전문가조사를 통해서 관련 데이터를 수집하여야 한다. 본 논문에서는 전자상거래 기업의 관리자와 시스템 개발자를 비롯하여 정보보호 연구기관 연구원 및 정보시스템 분야 교수를 대상으로 각 계층에 속하는 보안 요구사항간의 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.

전문가 설문조사를 통해 획득한 결과는 AHP 방법론을 적용하여 분석하는데, 각 보안 항목들 간의 우선순위를 결정하기 위해 영역별 가중치를 산정한다. 이 과정에서 사용한 AHP 방법론을 간단히 설명하면 다음과 같다.

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



<그림 1> 전자상거래 보안 요구사항의 계층 모델

$$A=\begin{pmatrix} w_1/w_1 & w_1/w_2 \cdots & w_1/w_n \\ w_2/w_1 & w_2/w_2 \cdots & w_2/w_n \\ \vdots & & \vdots \\ w_n/w_1 & w_n/w_2 \cdots & w_n/w_n \end{pmatrix}$$

여기서 w_i와 w_j는 i번째 속성과 j번째 속성의 가중치를 나타내는데, w_i/w_j는 i가 j에 미치는 상대적인 우월성을 나타내게 되므로, 주 대각선의 원소들이 모두 1이 되는 역수행렬이 된다.

이원비교의 결과를 나타내는 행렬의 고유벡터를 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 A에 대하여 $AW = \lambda W$를 만족하는 스칼라 λ와 $n \times 1$의 고유벡터 $W(=(W_1, W_2, \cdots, W_n)^T)$가 존재하는데, 이러한 경우 $\lambda_{\max}$ 에 대응하는 고유벡터 W 가운데에서 $\Sigma W_j = 1$을 만족하는 고유벡터가 그 계층 내의 요소들 간의 가중치가 된다.

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

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

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

5. 분석 결과

본 연구에서는 업무특성에 따라 전자상거래 보안에 대한 인식이 다르다고 판단하고 조사 대상 그룹을 연구자그룹과 실무자그룹으로 나누어 각 그룹별로 전자상거래 보안 항목의 우선순위를 도출하였다. 그룹별 우선순위는 비교를 통해 분석하고 시사점을 도출하였다. <표 1>은 관련 데이터를 얻기 위해 실시한 설문조사의 대상 분포를 나타낸 것이다.

<표 1> 설문조사 대상 분포

설문 응답자		응답자 (명)	분포 (%)
연구자 그룹	정보보호 연구기관 연구원	17	32.7
	정보시스템 분야 교수	6	11.5
실무자 그룹	전자상거래 기업 관리자	18	34.6
	전자상거래 기업 시스템 개발자	11	21.2
합 계		52	100

<표 2>는 연구자그룹을 대상으로 전자상거래 보안 요구사항의 영역별 가중치를 계산한 결과이다. 상위 계층에서는 보안 기술의 중요도가 매우 크게 나타났으며, 보안 기술의 중간 계층에서는 인증기술이 암호화기술이나 침입탐지 및 방지기술에 비해 중요한 요소임을 알 수 있다. 하위 계층에서는 영역별로 거래고객인증, 전송정보암호화, 백신 프로그램, 보안사고처리, 백업 및 복구 정책, 접근통제, 시스템 및 네트워크 모니터링, 전담조직 및 책임자 임명 관리가 높은 가중치를 나타낸다.

<표 3>은 실무자그룹을 대상으로 전자상거래 보안 요구사항의 영역별 가중치를 계산한 결과로서 연구자그룹의 영역별 가중치와는 다른 결과가 나타나는 것을 확인 할 수 있다. 상위 계층에서 보안 기술이 가장 중요하게 나타난 연구자그룹과 달리 실무자그룹에서는 보안 관리 및 운영을 가장 중요하게 평가했는데, 이는 전자상거래 기업의 실무자들이 이론적인 기술보다는 시스템을 직접 관리하고 운영하는 것이 전자상거래 보안에 있어 중요한 요소라고 판단한 결과이다. 보안 기술의 중간 계층에서도 인증기술이 중요하다고 평가한 연구자그룹과 달리 침입탐지 및 방지가 가장 중요한 것으로 나타났다. 하위 계층에서는 영역별로 거래고객인증, 저장정보암호화, 침입탐지시스템, 응용프로그램 취약성 점검 규칙, 백업 및 복구 정책, 아이디/패스워드 관리, 위험분석, 전담조직 및 책임자 임명 관리가 높은 가중치를 받아 역시 연구자그룹의 결과와는 차이가 있는 것으로 나타났다.

<표 2> 전자상거래 보안 요구사항의 영역별 가중치 (연구자그룹)

구분	보안 요구사항	보안 항목
보안 기술 (0.549)	인증기술 (0.629)	거래고객인증 (0.532)
		지불수단인증 (0.227)
		거래정보인증 (0.241)
	암호화기술 (0.186)	전송정보암호화 (0.603)
		키보드입력정보암호화 (0.158)
		저장정보암호화 (0.239)
	침입탐지 및 방지 (0.185)	방화벽 (0.273)
		침입탐지시스템 (0.189)
		백신 프로그램 (0.539)
보안 제도 및 정책 (0.167)	정보보호정책 (0.700)	개인(고객)정보보호정책 문서화 (0.140)
		응용프로그램 취약성 점검 규칙 (0.307)
		보안사고처리 (0.553)
	데이터베이스보안정책 (0.300)	정보저장규칙 (0.383)
		백업 및 복구 정책 (0.617)
보안 관리 및 운영 (0.284)	보안통제관리 (0.556)	아이디/패스워드 관리 (0.416)
		접근통제 (0.584)
	서비스 관리 (0.160)	시스템 및 네트워크 모니터링 (0.438)
		위험분석 (0.402)
		감사 기록 및 관리 (0.160)
	조직 및 인력관리 (0.284)	전담조직 및 책임자 임명 관리 (0.600)
		교육 및 훈련 (0.400)

<표 3> 전자상거래 보안 요구사항의 영역별 가중치 (실무자그룹)

구분	보안 요구사항	보안 항목
보안 기술 (0.324)	인증기술 (0.246)	거래고객인증 (0.571)
		지불수단인증 (0.172)
		거래정보인증 (0.257)
	암호화기술 (0.250)	전송정보암호화 (0.303)
		키보드입력정보암호화 (0.335)
		저장정보암호화 (0.362)
	침입탐지 및 방지 (0.504)	방화벽 (0.285)
		침입탐지시스템 (0.378)
		백신 프로그램 (0.336)
보안 제도 및 정책 (0.223)	정보보호정책 (0.436)	개인(고객)정보보호정책 문서화 (0.222)
		응용프로그램 취약성 점검 규칙 (0.450)
		보안사고처리 (0.327)
	데이터베이스보안정책 (0.564)	정보저장규칙 (0.183)
		백업 및 복구 정책 (0.817)
보안 관리 및 운영 (0.453)	보안통제관리 (0.303)	아이디/패스워드 관리 (0.558)
		접근통제 (0.442)
	서비스 관리 (0.335)	시스템 및 네트워크 모니터링 (0.316)
		위험분석 (0.393)
		감사 기록 및 관리 (0.291)
	조직 및 인력관리 (0.362)	전담조직 및 책임자 임명 관리 (0.583)
		교육 및 훈련 (0.417)

<표 4> 보안 항목 우선순위 (연구자그룹)

우선순위	보안 항목	중요도
1	거래고객인증	0.1835
2	접근통제	0.0923
3	거래정보인증	0.0833
4	지불수단인증	0.0781
5	아이디/패스워드 관리	0.0657
6	보안사고처리	0.0647
7	전송정보암호화	0.0616
8	백신 프로그램	0.0547
9	전담조직 및 책임자 임명 관리	0.0485
10	응용프로그램 취약성 점검 규칙	0.0359
11	교육 및 훈련	0.0324
12	백업 및 복구 정책	0.0309
13	방화벽	0.0277
14	저장정보암호화	0.0244
15	시스템 및 네트워크 모니터링	0.0199
16	정보저장규칙	0.0192
17	침입탐지시스템	0.0192
18	위험분석	0.0183
19	개인(고객)정보보호정책 문서화	0.0164
20	키보드입력정보암호화	0.0161
21	감사 기록 및 관리	0.0073

산정된 영역별 가중치를 이용하면 세부 보안 항목들이 전체 계층 모델에서 차지하는 상대적인 우선순위를 구할 수 있다. <표 4>와 <표 5>는 각각 연구자그룹과 실무자그룹을 대상으로 전체 중요도가 큰 순서로 세부 보안 항목들을 나열한 것으로 보안 항목의 전체 우선순위를 나타낸다.

<그림 2>는 2차원 평면 위에 연구자그룹과 실무자그룹을 대상으로 분석한 전자상거래 보안 항목의 우선순위를 비교하여 나타낸 것이다. 그림을 통해 연구자그룹과 실무자그룹이 중요하게 생각하는 보안 항목에는 다소 차이가 있다는 것을 쉽게 확인할 수 있다.

연구자그룹과 실무자그룹은 공통적으로 접근통제, 아이디/패스워드 관리, 전담조직 및 책임자 임명 관리, 백신 프로그램을 전자상거래 보안을 위해 중요한 항목으로 인식하고 있으며 이들은 모두 평면의 1사분면 위에 위치하고 있다. 거래고객인증과 교육 및 훈련도 공통적으로 중요한 항목으로 인식되고 있다. 그리고, 연구자그룹은 실무자그룹에 비해 거래정보인증, 지불수단인증, 보안사고처리, 전송정보암호화, 응용프로그램 취약성 점검 규칙을 중요한 항목으로 생각하는 반면 실무자그룹은 백업 및 복구 정책, 침입탐지시스템, 위험분석, 시스템 및 네트워크 모니터링, 방화벽 등과 같이 시스템 방어 및 관리와 관련된 항목을 더 중요한 항목으로 인식하고 있다.

<표 5> 보안 항목 우선순위 (실무자그룹)

우선순위	보안 항목	중요도
1	백업 및 복구 정책	0.1026
2	전담조직 및 책임자 임명 관리	0.0958
3	아이디/패스워드 관리	0.0766
4	교육 및 훈련	0.0685
5	침입탐지시스템	0.0618
6	접근통제	0.0606
7	위험분석	0.0596
8	백신 프로그램	0.0550
9	시스템 및 네트워크 모니터링	0.0479
10	방화벽	0.0466
11	거래고객인증	0.0455
12	감사 기록 및 관리	0.0442
13	응용프로그램 취약성 점검 규칙	0.0438
14	보안사고처리	0.0318
15	저장정보암호화	0.0293
16	키보드입력정보암호화	0.0271
17	전송정보암호화	0.0245
18	정보저장규칙	0.0230
19	개인(고객)정보보호정책 문서화	0.0216
20	거래정보인증	0.0205
21	지불수단인증	0.0137

이상의 결과를 통해 업무특성에 따라 전자상거래 보안 강화를 위해 필요한 항목에 대한 인식이 다르게 나타나는 것을 확인할 수 있었다. 특히 전자상거래 시스템을 실질적으로 운영하는 경우에는 1사분면과 2사분면에 위치한 보안 항목들을 강화할 필요가 있는데 이 항목들은 모두 실무자그룹에서 중요하게 생각하는 것들이다. 또한 한정된 자원을 통해 전자상거래 시스템의 보안을 강화해야 하는 경우에는 먼저 1사분면에 위치한 항목들의 보안 강화를 하는 것이 보다 실질적인 효과가 있을 것으로 생각된다.

앞으로 전자상거래의 보안을 더욱 견고히 하기 위해서는 실무자들이 필요로 하고 중요하게 생각하는 보안 항목에 대한 관심과 연구가 절실하게 요구되며, 전자상거래 관련 연구자들과 실무자들이 공통적으로 관심을 가지면서도 실질적인 전자상거래 구축과 운영

에 필요한 요구사항들이 제시되어야 할 것이다.

6. 결론

본 논문에서는 웹 기반의 전자상거래 발전을 위해 가장 중요한 전자상거래 보안을 강화하기 위한 방편으로 전자상거래 보안 요구사항 모델을 제시하고 실제 시스템에 효과적으로 적용할 수 있도록 보안 항목들 간의 상대적인 가중치를 AHP 기법을 사용하여 산정하였다. 또한 본 논문에서는 조사 대상 그룹을 다양화하고 조사 대상 그룹에 따라 보안 요구사항에 대한 인식의 차이를 분석하였으며, 이를 통해 전자상거래 실무자들이 필요로 하는 보안 관리 및 운영 분야의 중요성을 확인하였다.

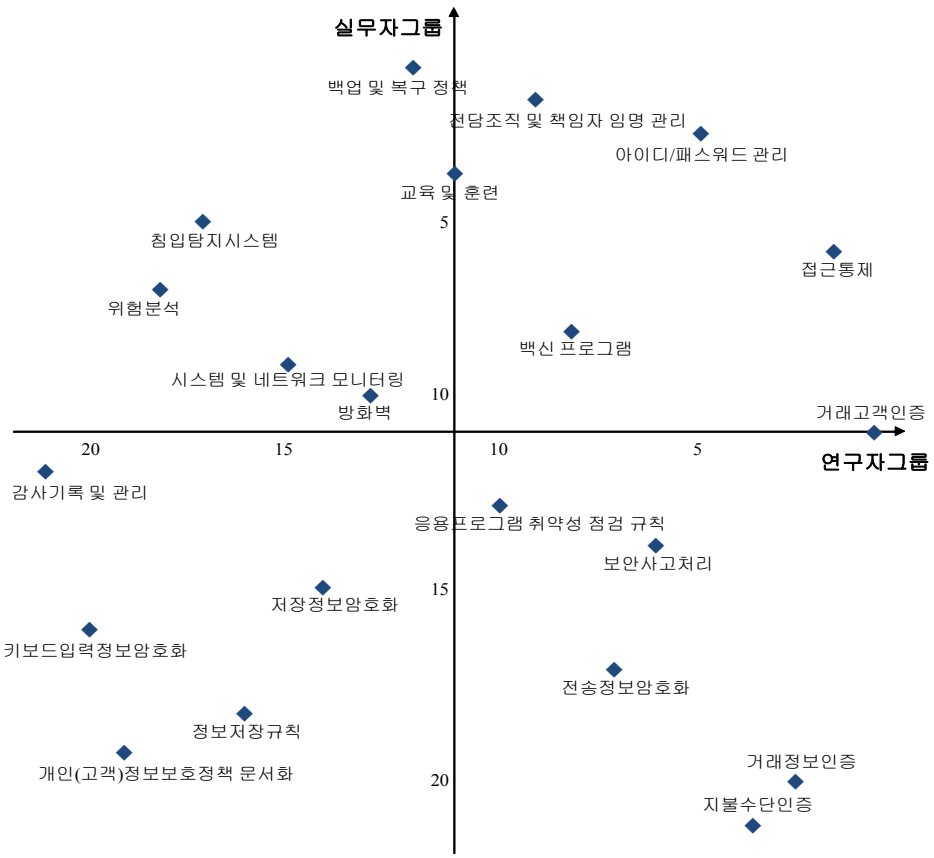
본 논문에서 제시한 전자상거래 보안 요구사항 모델과 분석 결과는 향후 안전한 전자상거래 시스템 설계, 구축 및 운영에 필요한 보안 가이드라인으로 활용될 수 있을 것으로 기대되며, 후속 연구를 통해 전자상거래 보안 관계자들이 공통적으로 관심을 가지면서도 실질적인 전자상거래 구축과 운영에 필요한 세부 요구사항들에 대한 도출이 필요하다.

참 고 문 헌

[1] M. Warren, and W. Hutchinson, “A Security Risk Management Approach for E-Commerce”, Information Management & Computer Security, Vol. 4, No. 5, pp.238-242, 2003.

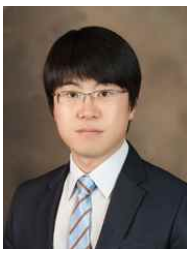
[2] 이동주, 김명수, “전자상거래 이용자들의 정보 프라이버시 우려와 반응 행동에 대한 실증 연구”, e-비즈니스연구, 제12권, 제2호, pp.365-383, 2011.

[3] N. F. Awad, and M. S. Krishnan, “The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the



<그림 2> 전자상거래 보안 항목 우선순위 비교

Willingness to be Profiled Online for Personalization", MIS Quarterly, Vol. 30, No. 1, pp.13-28, 2006.
[4] 전형구, 장화식, "전자상거래 정보보안 기술에 대한 연구", 인터넷비즈니스 연구, 제10권, 제1호, pp.43-55, 2009.
[5] 이선구, 임춘성, 서형식, "웹 사이트 발전단계에 따른 평가모형 구축과 활용에 관한 연구", 대한산업공학회 춘계학술대회논문집, pp.334-341, 2002.
[6] G. J. Udo, "Privacy and Security Concerns as Major Barriers for E-commerce: A Survey Study", Information Management & Computer Security, Vol. 9, No. 4, pp.165-174, 2001.
[7] 최성욱, 김기태, "안전하고 신뢰성 있는 전자상거래를 위한 키보드 입력 보안 시스템의 설계 및 구현", 정보처리학회논문지, 제13-C권, 제1호, pp.55-62, 2006.
[8] R. C. Marchany, and J. G. Tront, "E-Commerce Security Issues", 35th Hawaii International Conference on System Science, 2002.
[9] M. A. Patton, and A. Josang, "Technologies for Trust in Electronic Commerce. Electronic Commerce Research", Vol. 4, pp.9-21, 2004.
[10] I. Arce, "The Weakest Link Revisited. IEEE Security & Privacy Magazine", Vol. 1, No. 2, pp.72-76, 2003.
[11] A. Wright, "Controlling Risks of E-commerce Content", Computers & Security, Vol. 20, No. 2, pp.147-154, 2001.
[12] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영, 전자상거래 보안 기술, 생능출판사, 1999.
[13] 김세헌, 정보보호 관리 및 정책, 생능출판사, 2002.
[14] T. L. Saaty, Decision-Making for Leaders: The Analytical Hierarchy Process for Decisions in a Complex World, RWS Publications, 1995.
[15] 서수석, 이종호, "AHP를 이용한 전자상거래 웹사이트 평가모델 개발", 전자상거래학회지, 제5권, 제1호, pp.125-141, 2004.



김 현 우 (Hyunwoo Kim)

- 정회원
- 한국과학기술원 산업경영학과 공학사
- 한국과학기술원 산업공학과 공학석사
- 한국과학기술원 산업공학과 공학박사
- LG유플러스 기술연구원 책임연구원
- 경일대학교 경영학부 조교수
- 관심분야 : 보안성평가, e-business 전략, 정보보호, 서비스품질