전자상거래 환경하에서의 신용인증 서비스에 관한 비교 분석

김정덕*, 김도일**, 박현출***

A Comparative Analysis for Website Certification Service in the Context of Electronic Commerce

Jungduk Kim*, Doil Kim, Hyunchul Park*****

요 약

전자상거래에 있어서 인증 서비스는 크게 신원인증, 내용인증(전자공증), 신용인증 등 세 가지로 나눌 수 있다. 전자상거래가 활성화됨에 따라 여러 인증기관에서 신용인증 서비스를 제공하고 있으나, 인증기관의 성격에 따라 인증 실무기준을 달리한다. 따라서 본 논문에서는 현재 신용인증 서비스를 제공하는 인증기관의 성격별로 각 신용인증 서비스를 비교 분석한 후, 신용인증 서비스의 종합적인 인증 실무기준 framework 제시에 초점을 둔다.

Key words: 인증(Authentication), 인증(Certification), 신용인증

1. 서론

최근 개방 네트워크가 확산되고 새로운 정보기반구조가 형성됨에 따라 전자상거래가 급격히 활성화되고 있다. 전자상거래의 범세계적 가능성은 높아졌지만 정보보호 측면에서는 심각한 역기능이 나타나고 있다. 따라서 정보기반구조의 원활한 확산을 위해서는 정보기반구조의 신뢰성과 보안을 보장해 주어야 한다.

예를 들어 전자상거래에서 표시·광고한 것과 다른 불량제품의 배송, 반품과 환불의 거절 및 회피, 거래했던 쇼핑몰의 웹사이트 폐쇄, 대금을 지급했음에도 불구하고 제품을 배달하지 않는 경우, 이용하지 않은 제품과 서비스 등에 대한 대금청구, 소비자의 개인정보 유출 등의 경우에 소비자를 보호할 수 있는 제도적 장치가 마련되어야 한다. 따라서 전자상거래는 전통적인 거래 방식과 달리 비대면 상태에서 이루어지기 때문에 문제점이나 제약을 해소하기 위해서는 거래의 성립뿐만 아니라 거래 후 생겨날 수 있는 제반 분쟁해결에 인증 서비스가 요구된다.

2. 인증의 정의 및 종류

우선 인증(Authentication)이란 정보나 통신시스템에서 사용자, 주변장치, 혹은 다른 실체의 주장된 신원의 정당성을 확립하는 기능을 말한다[1]. 즉 요구된 자원이나 주체의 신원이 주장된 신원임을 보장하는 특징을 가지며, 사용자, 절차, 시스템, 정보 같은 실체에 적용된다.

이에 반해 인증(Certification)이란 거래와 관련된 사람, 서비스, 정보 등의 진정성을 검증하는 것으로 어떤 사실을 증명하거나 사실이라는 것을 보장하는 기능이다[2]. 본 논문에서는 인증(Certification)에 초점을 두고자 한다.

전자상거래에 있어서 인증 서비스의 목표는 크게 3 가지로 압축하여 설명할 수 있다[3]. 첫째는 안전한 전자상거래의 보장이며, 둘째는 개인 및 기업의 비밀 보장이며, 셋째는 거래 사실에 대한 증명을 제공하는 것이다.

이러한 목표를 달성하기 위해 전자상거래에 적용되는 인증 기능은 일반적으로 다음과 같이 구분할 수 있다.

① 신원인증: 상대방의 본인성을 확인하는 기능으로 거래 당사자간의 신원 확인을 목적으로 한다.

② 내용인증(전자공증): 거래 내용, 일시 등을 확인하는 기능으로 누가 누구와 함께 언제 무엇을 거래하였는가를 증명한다.

③ 신용인증: 거래 상대의 신용 능력을 확인하는 기능으로 사용자 및 웹 사이트의 신용도를 평가한다.

전자상거래가 발전하고, 응용 서비스의 범위가 넓어짐에 따라 현재 공개키 기반구조를 바탕으로 한 신원인증과 더불어 안전한 전자상거래를 위해 내용인증과 신용인증의 필요성도 더욱 더 커지고 있다.

* 중앙대학교 정보시스템학과 부교수
** 중앙대학교 상경학부 교수
*** 중앙대학교 정보시스템학과 석사과정

3. 기존 주요 인증 서비스 현황

3.1 AICPA/CICA 의 Webtrust 인증 서비스

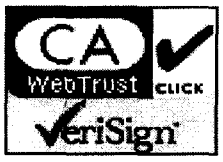
AICPA(American Institute of Certified Public Accountants)는 미국의 공인회계사 단체이며, CICA(Chartered Accountants of Canada)는 캐나다의 공인회계사 단체이다. 이 두 기관에서는 공동으로 'WebTrust'라는 이름의 웹 사이트 신용인증 서비스를 제공하고 있다. 이를 위해 크게 3 가지의 'WebTrust 원칙'을 수립하고 이에 따라 평가기준을 제시하고 있다[4].

업무 공개: 인터넷 상점은 전자상거래와 관련된 업무 절차를 공개하여야 하며, 공개된 내용에 따라 업무를 수행해야 한다. 거래에 대한 소비자의 신뢰를 높이기 위해서는 소비자가 본래 주문했던 물건, 정보, 또는 서비스를 정확하게 제공받는 것이 매우 중요하다. 따라서 인터넷 상점은 주문, 반환, 보증과 관련된 업무 절차를 공개하고 이에 따라 업무를 수행하여야 한다.

거래의 무결성: 인터넷 상점은 주문과 지불 처리가 소비자가 동의한 방법에 의해 이루어지도록 해야 한다. 이것은 거래 확인, 거래의 유효성 및 정확성, 거래의 처리, 지불 처리 등과 관련되는 사항이다

정보의 보호: 인터넷 상점은 소비자의 개인정보가 거래와 관련되지 않는 용도로 사용되지 않도록 보호해야 한다. 이것은 신용카드 정보와 같은 소비자의 개인정보보호를 위한 암호화 기술 및 기타 보호 방법에 대한 사항이다. 소비자의 정보는 네트워크를 통해 전송되므로 이때 공격 위험이 매우 많다. 따라서 소비자의 정보는 누출, 변경, 재전송 등으로부터 보호되어져야 한다. 또한 인터넷 상점은 자신의 시스템에 대한 공격에 대해서도 적절한 방어대책을 수립하여야 한다.

(그림 1) AICPA 인증마크



(그림 2) CICA 인증마크

3.2 미국 ICSA 의 인증 서비스

ICSA(International Computer Security Association)은 1989 년 NCSA(National Computer Security Association)이라는 이름으로 조직된 컴퓨터 보안에 관련된 여러 분야에 대해 연구하는 기관이다. ICSA 에서는 방화벽, Anti-Virus 소프트웨어 등 컴퓨터 보안과 관련된 여러 분야에 대해 인증 서비스를 제공하고 있는데, 웹 사이트 인증 서비스도 그 중 하나이다.

(그림 3) ICSA 인증마크

웹 사이트 인증을 위한 평가원칙은 다음과 같다[5].

네트워크 보안: 웹사이트는 네트워크를 통한 공격에 견디어 낼 수 있어야 한다.

안전한 통신 (Secure Connection): 웹 사이트 사용자들에게 신뢰감을 주고, 사용자 수를 늘리기 위해서 중요한 정보의 전송에는 반드시 적절한 암호화 기술이 사용되어야 한다.

중요한 정보 (Sensitive Data): 개인의 주소나 신용카드 정보와 같은 중요한 정보는 보호되어야 한다.

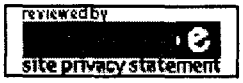
물리적인 보안: 접근 제한 구역을 통제하고, 적절한 장비로 응급 복구대책 등을 세워야 한다.

논리적인 보안: 안전한 패스워드 정책을 구현, 서버 관리를 위해 최소한의 권한 설정 등의 활동을 하여야 한다.

운영상의 보안: 시스템의 운영과 관련된 정보는 반드시 기록되어야 하며, 시스템의 운영 정책은 문서화되어 존재해야 한다.

3.3 미국의 TRUSTe 의 인증 서비스

TRUSTe 는 CommerceNet 과 EFF(Electronic Frontier Foundation)에서 설립한 비영리 기관으로, 인터넷 상에서의 거래에서 신뢰할 수 있는 환경 구축을 그 목적으로 하고 있다. TRUSTe 는 특히 웹을 통한 전자상거래에서 개인정보보호에 중점을 두고 TRUSTe Privacy Program 을 서비스하고 있다.



(그림 4) TRUSTe 인증마크

TRUSTe 의 평가기준은 다음과 같다[6].

① 정보의 공개: 웹 사이트는 자신의 정보 수집 활동에 대해 설명해야 하고, 수집된 개인의 정보를 어떠한 용도로 사용하며, 이 정보를 공유하는 자는 누구인가에 대해 설명해야 한다. 또한 웹 사이트는 사용자가 원하는 경우 저장된 정보를 지우거나, 변경할 수 있는지에 대해 설명해야 한다.

② 웹 사이트는 반드시 홈페이지에 TRUSTe 의 인증 마크를 표시하여야 하며, 이 인증마크는 TRUSTe 의 페이지로 연결시켜 놓아야 한다.

③ 웹 사이트는 법 또는 웹 사이트의 유지를 위해 필요한 경우를 제외하고는 전자우편과 같은 통신 내용을 모니터 할 수 없다.

④ 웹 사이트는 자신들이 기술한 개인정보보호 정책을 반드시 준수해야 한다.

⑤ 웹 사이트는 고객의 동의가 없는 한 TRUSTe 의 프로그램에서 탈퇴한 후에도 자신들이 기술한 개인정보보호 정책을 반드시 준수해야 한다.

⑥ 웹 사이트는 TRUSTe 의 감사 활동에 협조해야 한다.

3.4 일본의 프라이버시 마크 제도

1997 년 일본 통상산업성은 '민간부문에 있어서 전자계산기처리에 관계된 개인정보의 보호에 관한 지침'(통상산업성 고시 98 호, 이른바 '개인정보보호지침')을 제정하여, 민간부문에 있어서 개인정보 관리의 가이드라인을 제시한 바 있다[7].

이 가이드라인이 제정되고 난 뒤, 민간사업자가 이 가이드라인에 따라 개인정보관리를 하도록 유도하기 위해서는

인증마크 제도의 도입이 필요하다는 논의가 제기되었다. (재)일본정보처리개발협회가 이러한 논의를 구체화하여 도입한 제도가 1998 년 4 월부터 시행한 '프라이버시 마크제도'이다.

(그림 4) 일본 프라이버시 마크

일본 프라이버시 마크 심사기준은 별도로 규정되어 있는 프라이버시 마크부여 인정기준에 따라 접수된 신청서류의 기재내용을 심사한다. 기본적으로는 앞에서 말한 '프라이버시 마크를 신청할 수 있는 사업자'의 두 가지 조건을 만족시켜야 하는데, 특히 다음 사항은 중요한 조건이 된다.

① 개인정보 관리자를 지정하고 개인정보보호에 대해 회사 내에서 책임과 역할 분담이 명확하며, 개인정보를 적절히 취급하는 체계를 정비해야 한다.

② 년 1 회 이상, 개인정보 수집, 이용 및 제공에 종사하는 자에게 개인정보의 기밀보존과 관련된 교육 및 연수 등을 실시해야 한다.

③ 년 1 회 이상, 사업자 내부의 개인정보보호 상황을 감사해야 한다.

④ 개인정보보호에 관한 상담창구를 상설하고, 이를 소비자에게 명시해야 한다.

⑤ 당사자가 소유한 개인정보에 대해 외부의 침입 또는 내부로부터 누설되지 않도록 적정한 안전조치를 강구해야 한다.

⑥ 기업 외부에 개인정보의 제공, 취급을 위탁할 때에는 책임분담 및 비밀보장과 관련된 계약을 체결하는 등, 개인정보에 대해 적절한 보호를 할 수 있는 조치를 마련해야 한다.

3.5 미국의 BBB Online 마크제도

미국 경영개선협회 이사회(Council of Better Business Bureaus)가 운영하는 BBB 온라인마크는 신뢰성마크(reliability seal)과 프라이버시 마크(privacy seal) 등 두 개의 마크로 구성된다.

BBB 는 민간사업자의 회비로 운영되는 비영리단체로서, 소비자가 구매를 하기 전에 도움이 되도록 회원사에 대한 자료를 작성하여 제공하고, 자선단체에 관한 정보를 제공하며, 조정 및 중재제도를 통하여 소비자의 불만을 해결하는 등의 사업을 수행한다.

(그림 5) BBB Online 마크

신뢰성마크의 부여 조건은 다음과 같다[8].

① 해당 지역 BBB 의 회원이어야 한다.

② 업체 대표자의 성명, 영업, 주소 전화번호 등에 관한 정보를 BBB 에 제공해야 하고, BBB 가 방문을 통해 확인할 수 있는 물리적인 영업소를 가지고 있어야 한다.

③ 최소한 일년 이상 영업을 지속적으로 해야 한다.

④ BBB 가 만족할만한 불만처리절차를 갖추어야 한다.

⑤ BBB 의 광고 자율 규제 프로그램 (truth-in-advertising standards)에 참여하는데 동의하고, BBB 에 의해 지적을 받았을 때 온라인 광고를 수정하거나 취소할 수 있어야 한다.

⑥ 모든 소비자들의 불만에 즉각적으로 대응해야 한다.

또한 프라이버시 마크 부여조건은 다음과 같다.

① 엄격한 수준의 개인정보보호 원칙(privacy principles)에 따라 개인정보를 관리해야 한다.

② 공신력 있는 기관으로부터 정기적으로 개인정보 관리 상태에 대해 점검을 받아야 한다.

③ 소비자불만처리 절차를 갖추고 있음을 표시한다.

3.6 영국의 Hall 마크제도

Hall 마크는 IMRG(Interactive Media in Retail Group)가 회원사를 대상으로 IMRG 의 전자상거래 영업규정 (IMRG Code of Practice for Electronic Commerce)에 적합한 영업활동을 하는 업체를 대상으로 부여하는 마크제도로서 1997 년 10 월 14 일부터 시행되었다. IMRG 는 쌍방향미디어를 이용해 소매를 하는 회사(Interactive Media in Retail)들의 단체로 1990 년 영국에서 설립되었다. 현재 20 개 국가에 걸쳐 400 개의 회원사가 참여하고 있으며, 주기적인 시장조사와 보고서의 발간, 업계 자문, 공동프로젝트의 수행과 같은 임무를 수행한다.

(그림 6) 영국의 Hall 마크

영국의 Hallmark 인증기준은 다음과 같다[7].

① 모든 전자상거래 서비스는 합법적이고, 착실하며, 공정하고, 정직하고 진실해야 한다.

② 모든 전자상거래 서비스 소비자와 사회에 대한 책임감에 따라 운영되어야 한다. 전자상거래 서비스는 공평하며, 신속하고 효율적으로 수행되어야 하며, 소비자와 공정하고 올바르게 거래가 이루어져야 한다. 사업자는 불필요한 실망을 야기 시키지 않도록 해야 한다.

③ 모든 전자상거래 서비스는 공정한 경쟁의 원칙을 존중해야 한다.

④ 어떤 사업자도 전자상거래가 악평을 받도록 해서는 안된다.

4. 신용인증 서비스 비교

앞에서 살펴 본 주요 신용인증 평가 제도를 비교, 분석해 보면 <표 1>과 같이 정리할 수 있다.

<표 1> 주요 신용인증 제도 비교

국가	미국				일본	영국
신용인증명칭	WebTrust	ICSA	TRUSTe	BBB Online	Privacy 마크	Hall 마크
관련기관	미국/캐나다 공인회계사 단체	컴퓨터 보안연구기관	Commerce NET/EFF 비영리 단체	BBB (Better Business Bureau) 경영개선 협회	(재)일본정보처리개발협회	IMRG 소매회사 단체
주요 인증 실무기준	업무공개, 거래 무결성, 정보보호	NW 보안, 안전한 통신, 정보보호	개인정보보호	개인정보보호	개인정보보호	거래 무결성
초점	업무절차	시스템 보안	Privacy	Privacy	privacy	소비자 보호

<표 1>과 같이 현재까지 신용인증 제도는 인증 Seal을 제공하는 인증기관의 성격에 따라 인증 실무기준은 차이점을 보이고 있다. 기존 Off-line 상의 소비자 보호단체 및 비영리 기관을 중심으로 전자상거래에서도 똑같이 소비자의 주권 또는 권익 보호와 개인정보의 불법 유출 문제에 초점을 두는 그룹과 정보기술 측면으로 정보보호 차원에서 웹사이트의 안전성에 초점을 두는 그룹으로 나눌 수 있다.

5. 신용인증 서비스 통합 Framework

신용인증 기관이 웹사이트의 신용도를 효과적으로 평가하기 위해서는 신용인증의 다양한 측면을 고려하고 전반적인 웹사이트의 신뢰수준을 제고 시키는 방향으로 인증 실무기준이 제시되어야 한다. 이를 위해서는 각 인증 실무기준에 대한 개념 공유가 선행되어야 한다.

5.1 신용인증 서비스 통합 Framework 개발을 위한 배경

앞에서 살펴본 대로 현재 신용인증 서비스를 위한 인증 실무기준들은 다양하게 존재하고 있다. 본 논문에서는 앞에서 분석한 신용인증 관련 실무기준들을 바탕으로 공통요소를 도출하고자 한다.

1) 정보보호 관점

조직 내 정보보호의 조기 정착과 확산을 위해 영국은 정보보호 관리 지침인 BS7799(British Standard, Code of Practice for Information Security management)를, 독일은 'IT Baseline Protection Manual'을 제정하여 시행하고 있다. 또한 정보보호 관리 지침의 국제표준 ISO/IEC JTC1 SC 27 TR13335, GMITS : Guidelines for Management of Information Technology Security)도 제정되었다.

국내에서는 이러한 국제적인 추세에 발맞추어 정보보호를 위해 개별 조직에 적합한 보안정책 및 보안지침을 수립하였으며 공공기관의 경우 1997 년 '국가전산 보안업무 기본지침'이 제정되어 수행되고 있다.

이러한 정보보호 관리 수준을 평가하기 위한 방법은 대부분 단순한 체크리스트 접근 방법을 이용한 취약성 평가가 주류를 이루었다. 체크리스트 방법 중에서 Krauss(1972:1980)가 개발한 'SAFE 체크리스트'는 시스템 평가에 대해서 점수법을 이용했다. Hoyt(1973)와 Hutt et al(1988)이 개발한 '컴퓨터 보안 편람(Computer Security Handbook)'은 경험이 없는 위험분석가도 기존 시스템을 감사할 수 있도록 만들어졌다[9].

정보보호 평가를 위한 이들 체크리스트들은 공통적으로 물리적 보안, 논리적 보안, 관리적 보안으로 나누어 평가항목을 제시하고 있다.

물리적 보안은 전산실이나 통신실 등의 시설물과 정전압/ 무정전 설비, 공기정화 설비, 집진 장치 등 물리적 시설과 장비에 대한 물리적 침입과 파괴, 자연재해 등의 위협요인으로부터 자산을 보호하기 위한 정보통신시설, 설비의 위치설정, 기계적 기준 등을 말한다.

논리적 보안은 소프트웨어와 데이터를 대상으로 불법적이고 의도적인 접근 또는 비의도적인 실수나 오용으로부터 보호하기 위해서 인증, 암호화 등 접근통제나 통신보안을 하는 것을 말한다.

관리적 보안은 물리적 및 논리적 자산을 다루는 사람과 조직 그리고 행정에 관한 것으로 인간에 의한 의도적 및 비의도적 위협으로부터 보호하는 것이다.

2) 소비자 관점

전자상거래에 관한 국제적 논의를 주도하고 있는 그룹은 국제 기구인 경제협력개발력기구(OECD)이다. OECD 는 이미 수년 전부터 전자상거래에 있어 소비자 보호 문제와 더불어 프라이버시 보호, 보안과 인증, 지적재산권 보호, 내용물 규제, 접근성 확대, 사회경제적 영향 등에 관심을 가지고 연구를 계속해 왔다.

OECD 가이드라인은 가이드라인이 적용되는 범위와 전자상거래에 있어 소비자 보호를 위한 다음과 같은 일반 원칙들을 제시하고 있다.

투명하고 효과적인 소비자 보호: 전자상거래에 참여하는 소비자는 일반 거래 소비자와 동등한 수준의 보호를 받아야 하며 이러한 동등한 수준의 소비자 보호를 위해 정부, 사업자 및 소비자의 세 주체가 협력적으로 노력을 기울여서 소비자보호를 투명하고 효과적으로 하여야 한다.

공정한 영업 행위, 광고 및 마케팅 관행: 공정한 영업 관행으로써 사업자가 준수하여야 할 사항으로는 사기·기만적 거래 행위 금지, 소비자에 대한 위해 행위 금지, 소비자 정보의 충실한 제공 및 사업자의 자율 규약 준수 의무, 전자상거래의 범세계적 특성과 관련 규제의 특성 이해와 전자상거래의 특성을 이용한 부당 거래 행위 금지, 불공정 계약서의 사용 금지 등이 있다. 광고 및 마케팅에 관해서는 먼저 광고와 마케팅이 서로 구별될 수 있어야 하고 각각의 주체를 밝혀야 한다고 하였으며 광고와 마케팅 시 사용한 표현에 대해서는 입증할 수 있어야 한다고 한다. 또한 원치 않는 광고성 전자우편 수신 거절을 위한 절차를 개발·시행해야 하며 원치 않는 광고성 전자우편의 발송은 금지하고 그런 전자우편에 대한 각국의 법적, 자율적 규제를 준수해야 한다고 한다. 그리고 어린이 등 취약 계층을 대상으로 한 광고 및 마케팅에 대해서는 특별한 주의를 기울여야 한다고 명시되어 있다.

온라인 정보 제공의 강화: 온라인 정보에는 사업자에 대한 정보와 제품 및 서비스에 관한 정보, 거래에 관한 정보가 있다. 먼저 사업자에 대한 정보의 경우 전자상거래는 인터넷이라는 비대면적 통신매체를 사용하기 때문에 소비자는

자신이 거래하는 사업자에 대해 명확히 알기가 어려우며 사업자가 신원을 밝히지 않을 경우에 소비자의 불신을 초래 등 전자상거래 장애가 될 수 있다. 따라서 사업자의 신원에 관한 정보의 제공은 소비자의 신뢰제고와 보호를 위해 가장 중요한 요소가 될 수 있다. 제품 및 서비스에 관한 정보의 경우 전자상거래 사업자가 소비자에게 제품과 서비스에 관한 정보를 제공할 경우 소비자가 해당 정보에 쉽게 접근할 수 있어야 하고, 정확하고, 충분해야 한다. 거래에 관한 정보의 경우 거래 정보 제공의 원칙과 종류를 규정하고 있다.

거래 확인 절차의 구축·운영: 전자상거래에 참여하는 소비자들은 컴퓨터를 통해 상품을 주문하기 때문에 최종 주문 전에 자신이 구매하고자 하는 제품과 서비스가 무엇이며, 그 내용을 정정하고 필요하다면 거래를 취소할 수 있어야 할 것이다. 주문확인과 관련하여 소비자는 계약 체결 전에 구매하고자 하는 제품 및 서비스를 확인할 수 있어야 하며 주문을 수정할 수 있으며 충분한 정보가 제공되고 숙고한 끝에 구매에 대한 동의를 표시해야 하며 거래에 관한 정확한 기록을 보유할 수 있어야 한다고 소비자의 주문확인 절차에 관한 규정을 두고 있다.

안전한 대금지급 체계: 대금지급 메커니즘이 간편성과 안전성 등 두 가지 요건을 구비해야 한다고 명시하였으며 소비자에게 대금지급과 관련한 보안 수준에 대해 정보를 제공해야 한다고 규정하고 있다.

분쟁 해결 및 피해구제의 강화: 분쟁 해결 및 피해구제를 위해서는 준거법 및 재판관할에 관한 검토와 대안적 분쟁해결 및 피해구제 등의 사항에 대한 원칙을 제시하고 있다. 분쟁해결 및 그 전 단계인 소비자 불만의 처리에 있어서 공정하며(fair), 신속하고(timely), 부당한 비용과 부담이 없어야 함(without undue cost or burden)을 분명히 밝히고 있다.

프라이버시의 보호: 프라이버시 보호를 위한 8 원칙은 다음과 같다.

첫째 개인정보의 수집에는 제한이 있어야 하며, 개인정보는 적법하고 공정한 방법으로 그리고 정보주체의 동의하에 수집되어야 하는 자료수집의 제한(Collection Limitation)이다.

둘째 개인정보는 사용목적에 부합하여야 하며, 그 목적에 필요한 범위 내에서 정확성, 무결성, 최신성이 유지되어야 하는 정보의 질 유지(Data Quality)다.

셋째 개인정보의 수집 전에 수집 목적을 정확하게 명시하여 사용목적을 구체화(Purpose Specification)하여야 한다.

넷째 개인정보는 이용자의 동의나 법률에 의하지 않고서는 특정된 목적 이외의 목적을 위해 공개되거나 유출·이용되어서는 안된다는 이용의 제한(Use Limitation)이다.

다섯째 개인정보는 누출, 무단접근, 파괴, 불법사용, 변조, 공개 등의 위험으로부터 보호하기 위하여 합리적인 보안장치가 강구되어야 하는 보안장치(Security Safeguards) 마련이다.

여섯째 개인정보에 관한 정책·관행이 공개되어야 하고, 개인정보 수집자의 신원·주소 뿐만 아니라 개인정보의 사용목적 등을 쉽게 확인할 수 있어야 하는 공개성(Openness)이다.

일곱째 정보주체는 정보관리자가 자신에 관한 정보를 소유하고 있는지 여부를 확인할 권리가 있고, 합리적인 기간 내에, 합리적인 방법으로, 이해하기 쉬운 형태로, 무상으로 자신에 관한 정보를 통보 받을 권리가 있으며, 정보주체의 이와 같은 요구가 받아들여지지 아니한 때에는 그 이유를 설명 받을 권리와 함께 이의를 제기할 권리를 가지도록 개인의 참여(Individual Participation)가 가능해야 한다.

여덟째 개인정보의 수집자는 위에서 언급된 기본원칙을 이행하기 위하여 마련된 조치에 따라 행동할 의무(Accountability) 사항이다.

소비자 교육의 강화: 소비자와 사업자를 대상으로 전자상거래에 대한 소비자 교육을 강화하기 위해 정부, 사업자, 소비자대표가 협력적으로 노력해야 함을 규정하고 있다.

3) 웹사이트 관점

전자상거래에서 웹사이트는 네트워크 거래에서 의문시되는 다음에 대한 보증을 제공해야 한다[10].

① 거래 상대방이 정말 그 사람인가?
② 인터넷 가상상점은 실제로 존재하는가?
③ 배달된 상품/서비스는 합법적인 것인가?
④ 배달은 제대로 되었는가?
⑤ 거래가 언제 이루어졌는가?
⑥ 거래 내용을 증명할 수 있는가?

이를 위해 웹사이트는 내부 부정방지 대책 및 업부 감사 등을 통한 내부통제 구조를 가지고 있어야 하며, 개인 및 기업 정보의 비밀의 보장, 업무 제공의 연속성, 기술적 안전성, 신뢰성 및 신속성을 확보해야 한다. 또한 고객으로부터 사회적 신뢰도와 손해배상, 보험 등에 대비한 재정적 능력을 갖추어야 한다.

미국의 공인회계사 단체인 AICPA 에서 수행한 CPA vision Project 에서는 소비자와 비즈니스 파트너의 주요 관심사항을 다음과 같이 제시했다.

정보 보호	Privacy
비즈니스 정책	거래 처리 무결성

(그림 7) 소비자와 비즈니스 관심사항

정보보호는 웹 사이트에 대한 의도적/ 비의도적인 공격으로부터의 보호를 통한 안전성을 의미하며, Privacy 는 소비자의 개인정보가 거래와 관련되지 않는 용도로 사용되지 않음을 의미한다. 비즈니스 정책은 웹사이트는 주문, 반환, 보증과 관련된 업무절차를 공개해야 함을 의미하고, 거래 처리상의 무결성은 거래 확인, 거래의 유효성 및 정확성 등과 관련된 사항이다.

5.2 신용인증 서비스 통합 Framework

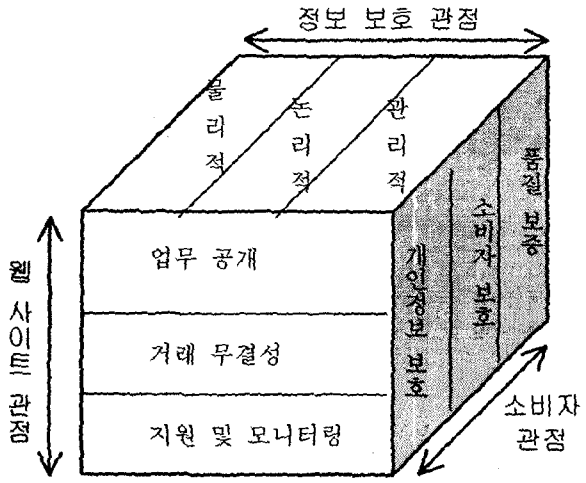
앞에서 살펴본 3 가지 관점에서의 이론적 배경을 바탕으로 신용인증 서비스 통합 Framework 을 제시하고자 한다.

정보보호 관점은 앞서 살펴 본 여러 체크리스트 비교연구를 바탕으로 물리적 보안, 논리적 보안, 관리적 보안의 3 가지 기준을 제시했다. 모든 시스템 보안 요소가 반드시 특정 기술에만 의존하는 것은 아니다. 단순한 논리(기술)상의 보안 요건만을 평가하는 것 보다는 포괄적으로 물리적, 관리적 보안요소까지 확대해서 평가하는 것이 바람직하다.

소비자 관점에서는 OECD 권고안을 바탕으로 소비자입장에서 전자상거래에서 중요시하는 요소를 고려하여 Privacy 보호, 소비자 보호, 품질 보증이라는 3 가지 기준을 제시했다. Privacy 보호는 소비자 자신의 신상정보가 웹사이트의 개인 정보보호 정책에 따라 불법 유출되지 않는가에 대한 요건이며, 소비자 보호는 Off-line 상의 기존 거래와 마찬가지로 On-line 상의 전자상거래에서도 동등하게 소비자 보호를

받을 수 있는가에 대한 요건이며, 품질 보증은 웹사이트가 제공하는 상품이나 서비스가 품질 요건이다.

웹사이트 관점은 실제 전자상거래를 위해 운영되는 웹사이트가 자신의 업무 정책 및 절차를 반드시 공시하는 업무 공개 의무와 상품의 주문, 지불, 배송과 관련하여 거래의 무결성 유지 의무, 그리고 신용인증 기관에 대한 지원과 지속적인 모니터링 대한 협조 의무이다. 통합 Framework 은 3 가지 관점에서 9 가지 기준으로 다음 그림과 같은 입방체로 구성된다.



(그림 8) 신용인증 통합 Framework

본 통합 Framework 은 세 가지 관점으로 개별적인 신용 인증 실무기준으로 제시될 수도 있지만, 다른 관점과의 연관성을 강조하고 있다. 예를 들어 소비자 관점에서의 개인정보 보호문제는 웹사이트 관점의 업무 공개 기준내에 개인정보 보호정책이 반드시 웹사이트에 공개되어 있어야 하는 요건과 정보보호 관점의 논리적 보안으로 암호화가 이루어진 바탕 위에 개인정보 보호가 이루어질 수 있음을 보여준다.

따라서 본 통합 Framework 은 전자상거래 주체인 소비자 관점, 웹 사이트 관점, On-line 거래의 특징인 정보보호 관점 등에서 고려할 요소들을 보여줌으로써 종합적인 시각에서 신용인증 서비스를 위한 인증 실무기준을 제시할 수 있다.

5. 결론 및 향후 연구과제

비대면 전자상거래로 발생할 수 있는 문제 해결을 위해서 인터넷 상점 또는 고객에 대한 신용인증이 필요하며, 인터넷 상점 또는 고객에 제 3 의 기관에서 공증해 줌으로써 사용자가 브라우저를 통해 보여지는 인터넷 상점을 신뢰하거나 고객을 신뢰할 수 있게 되는 것이다.

본 논문에서는 현재 신용인증 서비스를 제공하고 있는 대표적인 6 개의 기관에 대해서 이들이 인증을 하기 위해 제시하고 있는 인증 실무기준을 중심으로 살펴보았다. 그리고 기관의 성격별로 달리했던 신용인증 실무기준을 통합하는 Framework 을 제시하였다. 이것은 신용인증에 대한 종합적인 이해에 도움을 줄 것이다.

본 연구를 수행하면서 인증마크에 대한 위조가능성에 대한 우려를 없애는 기술적 보완책 마련이 시급함을 인식했고, 고객이 직접 인증마크를 클릭하여 쇼핑몰의 신용도를 확인하거나, 신용상점 목록 디렉토리를 직접 비교해야 하는 부가적인 노력을 줄일 수 있는 연구가 뒷받침되어야 할 것이다. 그리고 전자상거래의 특성을 고려한 국제적 상호인증에 대한 논의가 필요할 것이다.

인터넷을 이용한 쇼핑이 중요한 구매 수단의 하나로 자리잡아 가고 있는 현 시점에서, "TRUST"문제는 전자상거래에서 가장 큰 이슈가 되고 있으며 따라서 이러한 문제를 해결하기 위한 신용인증 서비스는 기존의 CA 의 신원인증 및 내용인증 업무와 함께 간과할 수 없는 중요한 문제이다.

참고문헌

[1] Recommendation of OECD Council concerning Guideline for Cryptography Policy, 1997.3

[2] clause 1.15, Certification Authority Guideline, Alpha version, Electronic Commerce Promotion council of Japan(ECOM), 1997.3

[3] Warwick Ford and Michael S. Baum, Secure Electronic commerce, Prentice Hall, 1997

[4] Webtrust principles and criteria for B2C EC, 1999.10, http://www.cpawebtrust.org

[5] ICSA http://www.icsa.net.

[6] TRUSTe http://www.truste.org/join/guide.html

[7] 한국정보통신진흥협회, 인터넷 모범상점 인증제도도입 방안에 관한 연구, 1999.12, 한국정보통신진흥협회

[8] BBBOnlie http://www.bbbonline.com

[9] 김정덕, 김기윤, 정보보호지표 항목개발 및 계량화 연구, 한국정보보호센터, 1998.12

[10] 김지선, 인증서비스 기술동향, KRNET98, 1998