안전하고 신뢰할 수 있는 전자상거래 정보시스템 인증·평가모델에 관한 연구

조영훈*, 김석우*

*한세대학교, 정보보호공학과

The Study of Safety and Trust Certification Evaluation Model of Electronic Commerce System

Yeong-hoon Cho*, Seok-woo Kim*

*Department of Information Security Engineering, HANSEI Univ.

요 약

이 논문에서는 전자상거래에서의 안전하고 신뢰할 수 있는 이용여건을 마련하기 위해 자율규제로 추진되고 있는 국내외 인터넷 평가모델에 대한 분석과 효율적인 전자상거래 인증·평가모델을 제시한다.

I. 서론

2000년 들어서 빈번하고 있는 인터넷을 이용한 정보시스템에 대한 해킹사건은 전문가를 중심으로 그 중요성이 인식되어 온 정보보안에 대한 관심을 일반인까지 확산시키는데 크게 기여하였다.

현재 OECD는 개인정보 보호를 위한 시스템 구비와 관련한 권고를 정보, 컴퓨터, 통신위원회(ICCP)가 중심이 되어 추진하고 있다. 동 위원회는 정보보안 문제에 대한 각종 지침 제정 및 시행을 주도하였는데, 1980년 「프라이버시보호와 개인정보 국가간 이동에 관한 가이드라인」, 1992년 「정보시스템보안에 관한 가이드라인」, 1997년 「암호화정책에 관한 가이드라인」 등이 대표적이다. 이외에도 BT, HSBC 등과 영국 상무성이 함께 연구한 「정보보안관리 실무규범(A Code of Practice for Information Security Management)」이 있다. 이 권고안은 조직의 정보보안을 구현하고 유지하는 관리자들이 참조할 수 있도록 보편적 문서로 개발되었다. 현재 이 권고안은 1999년 10월 ISO 표준으로 제안되어 ISO/IEC DIS 17799-1으로 채택되었으며, 유럽, 북미, 환태평양권을 중심으로 높은 관심을 보이고 있다.[1]

하지만 국내의 경우 인터넷 운영기관 및 사업자의 정보보호에 대한 마인드 부족과 미비한 수준의 대응으로 해킹사고가 빈발하고 있으며, 이에 따른 인터넷에 대한 이용자의 불신이 높아지고 있다. 특히 국가 주요 정보통신기반에 대한 공격과 위협이 증가함에 따라 이에 대한 보호를 위한 다각적인 절차의 개발과 관련기술의 연구가 여러 관련기관을 통해 진행되고 있다. 그 결과 2001년 7월 제정된 정보통신기반보호법에 따라 주요 정보통신 기반에 대한 취약성 평가를 의무적으로 실행하게 되었다.

이와같은 정부주도의 정책이 제대로 시행되기 위해서는 인터넷 운영 부처 및 기관이 보유하고 있는 정보시스템의 보안에 대한 이해와 정보시스템의 해킹방지를 평가하는 인터넷 제3자 인증제도의 개발 및 시행이 요구된다.

이에 본 논문에서는 안전하고 신뢰할 수 있는 인터넷 사용여건을 마련하기 위해 민간자율규제 형태의 국내외 인터넷 평가모델에 대한 분석과 효율적인 전자상거래 인증·평가모델을 제시한다.

II. 국내외 인터넷자율규제 평가모델 도입현황

1. 개요

인터넷은 정보통신 기술의 발전에 따라 비약적인 성장을 거듭하여 전자상거래를 비롯하여 사회 각분야에서 활용되고 있으나 개인정보 침해 및 유출 등 역기능으로 공급자와 이용자간 불신의 벽이 높아지고 있다. 이에 세계각국은 인터넷상의 개인정보를 보호하고 소비자 피해문제를 최소화하기 위해 다양한 제도를 연구, 시행하고 있다. 이러한 움직임은 크게 경제협력개발기구(OECD) 등 국제기구를 중심으로 회원국가에 권고하는 방식과 민간 자율적으로 제3자 인증신뢰마크 제도를 마련하고 시행하는 것으로 나타난다.[2]

본 논문에서는 후자를 중심으로 서술한다.

2. 제3자 인터넷 인증 신뢰마크제도

1) 운영기관

현재 세계각국의 민간기구는 인터넷사이트를 신뢰할 수 있는 평가모델을 개발하고 심사결과 적합여부를 판정한 후 마크를 부여하고 있다. 대표적인 단체가 미국의 TRUSTe이다. TRUSTe는 1997년 OECD 소비자보호정책위원회를 중심으로 연구중이었던 『전자거래 소비자보호 가이드라인』과 다른 민간자율의 가이드라인을 제시하였다. 이러한 움직임은 미국 경영개선이사회(BBB), 일본통신판매협회, 일본정보처리개발협회, 한국정보통신산업협회, 전자거래진흥원 등으로 이어졌다.[3]

현재 인터넷사이트에 대한 제3자 인증신뢰마크는 인터넷쇼핑몰과 같이 상거래를 하는 웹사이트를 대상으로 소비자보호지침의 준수 여부를 평가하여 마크를 부여하는 소비자 신뢰마크(Customer Trust Seal)와 전체 웹사이트를 대상으로 개인정보보호 혹은 시스템 보안지침의 준수 여부를 평가하여 마크를 부여하는 개인 신뢰마크(Privacy Trust Seal)로 구분된다. 전자의 대표적인 마크가 미국 BBBOnline 신뢰(Reliability) 마크, 한국 인터넷사이트안전마크이며, 후자의 대표적인 마크는 미국 TRUSTe 마크, 미국 BBBOnline 프라이버시 마크, 일본 프라이버시 마크, 한국 인터넷사이트안전마크이다.[4]

세계각국의 기관이 운영하고 있는 제3자 인증신뢰마크제도를 살펴보면, 운영기관은 한국과 영국의 경우 정부가 직 간접적으로 관여하고 있다. 그러나 일본과 미국의 신뢰마크제도는 공공민간단체들에 의하여 운영되고 있다. 영국 제도의 경우 정부가 간접적으로 관여하고 기업과 소비자가 연합하여 인증기관을 만들었다.

2) 심사기준

세계각국의 제3자 인증 신뢰마크제도 심사기준은 지역적·문화적 차이에 따라 차이는 있지만 크게 개인정보 보호에 관한 항목, 시스템의 안정성과 보안에 관한 항목, 그리고 소비자에게 정보제공 및 선택에 관한 항목, 불만처리항목으로 구성되어 있다.

특히 현재 전세계에서 운영되고 있는 제3자 인증신뢰마크를 심사기준을 살펴보면 개인정보 보호 또는 소비자거래정보 보호를 위해 최소한의 시스템 안정성과 보안을 요구하고 있음을 알 수 있다. ([표 1] 참조)

[표 1] 시스템 보안 관련 심사기준

구분		심사기준
한국	eTrust	시스템 성능 및 안정성 : 13개
	iSafe	시스템보안 : 금융. 의료 73개, 일반 66개
일본	Online Shopping Trus	시스템보안 : 충분한 안전대책
	Privacy	시스템보안 : 개인정보안전조치
미국	TRUSTe	시스템보안 : 정보안정성 35개
	BBB Privacy	시스템보안 : 암호화된 보안 시스템, 보안대책 점검
	CPA Webtrustg	거래의 무흠성 : 거래를 완벽하게 할 수 있는 시스템
영국	TrustUK	시스템보안 : 정보의 안정성 (BS7799사용), 수시안전 점검

3. 효율적 전자상거래 자율규제 방안

1) 자율규제 원칙

제3자 인증 신뢰마크제도는 소비자들이 믿고 거래할 수 있는 인터넷사이버몰에 대한 정보를 제공해 주고 이들 사업자와의 거래를 유도함으로써 소비자들로 하여금 인터넷을 통한 전자상거래가 편리하고 저렴하며 신뢰할 수 있는 새로운 상거래 방식이라는 인식을 갖을 수 있도록 해주어 소비자의 이용을 촉진하고 동시에 소비자의 불만과 피해를 사전에 예방할 수 있게 해준다는 것에 그 의의가 있다.[5]

이처럼 전자상거래에서의 민간중심적인 자율적 인증제도의 도입은 소비자의 신뢰도를 높일 뿐만 아니라 아직 그 체계가 확실히 잡혀 있지 않은 전자상거래관련 업계에 전자상거래의 모범적인 비즈니스 모델을 제시하는 효과를 주어 사업자의 올바른 기업관을 정립할 수 있도록 도와줄 것이며 이러한 소비자 참여의 활성화와 사업자의 올바른 기업관 정립은 국내 전자상거래의 경쟁력 강화에 기틀을 마련할 수 있는 하나의 기반이 될 수 있을 것이다.

인증제도를 자율규제방안으로 도입하려면 다음의 효율적인 자율규제방안 원칙에 부합한 제도를 추진해야한다. 첫째, 사업자에게 인센티브를 제공 즉, 자율규제의 인센티브는 정부 규제에 대한 두려움이 될 수 있으며 경제적으로 인센티브를 제공할 수 있다. 둘째, 자율규제 기관이 감사할 능력이 있어야 한다. 셋째, 평가 기준이 객관화되어야 한다. 넷째, 소비자 참여가 필요하다. 다섯째, 인증제도의 효율적 관리를 위해 소수 사업자의 참여가 필요하다.[6]

2) 추진 방안

전자상거래의 제3자 인증 신뢰마크제도 방안은

인터넷사이트안전마크, e트리스트마크, 미국 TRUSTe마크, BBB Onlinc마크, 일본 Onlinc Shopping Trust마크, 일본 프라이버시마크에 대한 분석과 현재 정부에서 추진중인 전자상거래등에서의소비자보호에관한법률제정 흐름을 감안하여 준사법기관인 공정거래위원회에서 권장할 수 있는 최소한의 가이드라인에 초점을 맞추었다. 이는 사업자에게 참여할 수 있는 인센티브를 제공하기 위한 것이다. 또한 소비자보호문제에 접근함에 있어 전자상거래 환경에 적합하고 이미 운영중인 국내 제3자 인증 신뢰마크제도와 차별화될 수 있는 평가기준이 될 수 있도록 하였다. 평가척도를 O, X로 단순화 한 것은 이 연구에서 제시하는 평가기준이 최소한의 가이드라인이기 때문이다. 이 가이드라인은 이해 당사자인 정부, 사업자단체, 소비자단체, 사업자 대표, 소비자 대표 등이 참여하여 사업 실정에 적합한 자율규제로 가시화될 것이다.

추진방안을 정함에 있어 가장 큰 어려움은 법령 준수 여부만으로 사업자별 소비자보호를 확인하는데는 한계가 있다는 것이다. 이 문제는 사업현실에 맞는 자율규제를 검토하는 과정에서 사업자가 스스로 판단하고 결정할 수 있지 않을까 한다. 또한 연구의 범위를 거래과정에서의 소비자보호로 한정할 것인지, 아니면 소비자 개인정보보호, 거래정보보호까지 확대할 것인지의 검토도 있었다. 소비자 개인정보보호는 인터넷사이버몰사업자가 대부분 회원제로 운영하는 현실을 감안하고 소비자 거래정보보호는 결제수단이 무통장입금에서 신용카드 결제, 온라인입금 결제로 확대되는 현실을 감안하여 소비자 개인신상정보를 보호하기 위한 최소한의 정보시스템 보안정책 수립 및 시행이 요구되어 최소기준으로 포함시켜야 한다는 의견을 반영하였다. 일부에서는 내부자에 의한 정보유출이 70%이상의 비중을 차지하고 있음을 감안하여 제3자 해킹은 고려할 필요가 없다고 하지만, 이러한 조치없이 소비자 정보가 안전하게 보존될 수 없어 최소 기준으로 적용하였다.

3) 심사기준

심사기준은 크게 사업자 등록 및 온라인 정보제공, 상품주문 및 거래정보 보호, 소비자피해구제 등 3개분야 7개 그룹 30개 항목으로 구성하였다.([표 2] 참조)

[표 2] 인터넷사이버몰 제3자 인증 신뢰마크 심사기준 총괄표

구 분		항목수
I. 사업자 등록 및 온라인 정보제공	1. 사업자 등록	2
	2. 사업자 신원정보 제공	2
	3. 소비자 개인 신상정보보호	9
	4. 거래정보 충실성	4
소 계		17
II. 상품주문 및 거래 정보보호	1. 상품주문 및 반품환불	4
	2. 소비자 거래정보 보호	5
소 계		9
III. 소비자 피해구제	1. 불만처리	4
소 계		4
총 계		30

전체 30개 평가기준은 전기통신사업법, 정보통신망이용촉진 및정보보호등에관한법률, 개인정보보호지침, 소비자보호법, 전자거래기본법, 방문판매등에관한법률, 약관의규제에관한법률, 할부거래에관한법률, 표시 광고의공정화에관한법률, 전자상거래 등에서의소비자보호에관한법률(안), 청소년보호법, 전자거래 소비자보호지침, 인터넷사이버몰 이용표준약관, 소비자피해보상규정 등을 근거로 개발되었다.

이중 소비자 거래정보 보호 심사기준은 전자상거래상에서의 최소한의 시스템 보안 심사항목으로 구성했다. 실제로 전자상거래의 활성화를 위해서는 소비자의 거래정보를 보호를 하기 위한 대책의 수립 및 시행이 요구된다. 하지만 소비자 거래정보 보호는 사업자의 의지와 함께 이를 위한 환경과 시스템이 구축되어야 가능하다. 보안은 단순한 의지로만 달성할 수 없기 때문이다. 따라서 인프라의 보안을 위해 보안 시스템을 설치하며, 현재 가장 보편적으로 사용하는 것이 침입탐지시스템이다.

침입탐지시스템은 필터링 기능을 가진 것과 프락시 기능을 가진 것 그리고 두 가지를 모두 가진 시스템으로 구분된다.

침입차단시스템은 그러나 필터링 기능을 가지고 있으면 많은 부분을 커버할 수 있으므로 심사항목에서는 필터링의 기능을 최소 요건으로 한다. 실제로 프락시 기능은 성능을 저하시킬 수 있으며 NT의 경우에는 필터링 기능만을 가진 시스템이 현재 국내에 개발되어 인증을 취득하였다.

침입탐지시스템은 침입차단시스템과 함께 인프라 보안의 주축을 이루는 시스템이다. 네트워크 기반과 시스템 기반이 있으며, 침입자의 행위를 실시간에 탐지하거나 혹은 로그 파일을 분석하여 침입의 사실을 찾아내기도 한다.

침입차단시스템이 정책에 의거한 정적인 보안의 구현이라고 하면, 침입탐지시스템은 동적으로 침입의 여부를 판단할 수 있으므로 침입차단시스템과 상호 보완적으로 사용할 수 있다. 이러한 시스템은 또한 침입차단시스템이 간과한 사실을 탐

지하여 보안 기능의 향상을 가져오므로 꼭 필요한 시스템이다.

취약성 분석을 위한 소프트웨어는 침입을 당할 우려가 있는 시스템의 부분들을 점검하는 소프트웨어를 말하며 이를 점검함으로서 시스템 전체의 보안성을 향상시킬 수 있다. 일반적으로 패스워드 파일, 접근 제어 혹은 원격 접근 관련 시스템 파일 등을 점검한다. 취약점 분석을 통해 발견된 문제들을 수정 보완하는 기능까지도 포함하고 있다. 이러한 소프트웨어의 설치 혹은 동일한 기능을 제공할 수 있도록 준비하는 것은 전자상거래의 인프라 보안을 위해 필수적인 요소라 할 수 있다.

Ⅲ.결론

본 논문에서 기술한 것과 같이 민간자율규제 형태인 인터넷 제3자 인증신뢰마크는 불모지에 가까웠던 국내 개인정보 보호, 시스템 보안, 소비자 보호분야에 대한 중요성을 민간업계에 전파하고 이에 대한 대책수립을 촉진하는 계기를 마련하는데 기여하였다.

하지만 안전하고 신뢰할 수 있는 인터넷 사용 여건을 조성하기 위해 필수적으로 요구되는 개인정보의 유출 및 침해방지대책 등을 자율적으로 마련하고 준수할 수 있도록 정부의 보다 강력한 정책의지가 요구된다. 또한 현재 개인정보 보호에 대한 연구가 정책적 제도적 측면으로 치중하고 있어 별도 기술적 대책에 대한 연구가 필요하다. ▲ 익명성을 보장한 개인정보 보호방법으로 논의되고 있는 remailer center, AT&T crowd, anonymous user 등 ▲ CC의 보안기능 요구사항 중 프라이버시 기능을 구현한 기술제품 ▲ 기타 기술적 대책에 대한 연구 등은 대표적인 예이며, 현재 선진각국에서 관심을 보이고 있는 분야임을 감안하여 신속하고 적극적인 대처가 요구된다.

또한 민간분야에서 시행하고 있는 인터넷 제3자 신뢰인증마크가 정부 및 공공기관에 대한 정부 전문조직의 평가후 제3자 "validation" 차원에서 적용 시행된다면, 선진각국에서와 같이 모범적인 국가 정보시스템의 개인정보 보호 및 시스템 보안 사이트 구축의 시금석을 마련하는데 이바지 할 것으로 보인다. 현재 대부분의 국가기관, 공공기관의 경우에 각 기관의 특성에 맞게 안내 및 홍보 홈페이지를 인터넷으로 연결할 수 있도록 운영하고 있어 해킹에 취약한 구조 - FTP, telnet 등을 비롯하여 많은 포트를 열어 놓고 작업하는 현실에 대한 대책도 필요할 것으로 생각된다.

본 논문이 보다 발전된 인터넷 제3자 인증제도로 마련하고 정착하는 계기로 나타나길 바라며, 그간의 기타 다른 연구결과들과 기술적인 보안대책이 어우러져 종합적인 인터넷 신뢰환경 구축에 기여할 수 있기를 기대한다.

참고문헌

[1] 김종기, BS7799 정보기술 보안관리 지침 표준화동향, 부산대, 2000

[2] 한태인, 조영훈외 3인, 인터넷사이트안전마크 인증제도 도입방안에 관한 연구, 한국정보통신진흥협회, 2000

[3] 김철완, 조영훈외 7인, 건전한 정보통신윤리 확립과 개인정보보호대책 방안 연구, 정보통신정책연구원, 2001

[4] 한국인터넷백서 2001, 한국전산원, 2001

[5] 김경신, 전자상거래 소비자보호를 위한 사업자자율규제에 관한 연구(석사학위 논문), 경희대, 2001

[6] 조영훈, 김석우외 3인, 전자상거래에서의 효율적인 자율규제방안 및 신종거래분야 법규범 적용방안 연구, 공정거래위원회, 2001