전자상거래 보안전문가 자격인증제도 도입에 관한 탐색적 연구

노 규 성† 하 태 현†

요 약

전자상거래 보안은 전자상거래의 성공여부를 결정할 수 있는 신뢰성 확보를 위한 기반기술로서 인식되고 있다. 이러한 보안 서비스의 문제는 전자상거래 활성화의 가장 큰 요소 중의 하나로서 정보기술과 인터넷 기술의 발전과 함께 꾸준히 연구 및 보완되어야 할 중대한 이슈가 되었다. 특히 전자상거래의 급성장과 함께 보안사고가 잇따르고 있는 상황에서 이를 대처하기 위한 전문인력이 절대적으로 부족함에도 불구하고 이런 상황을 타개하기 위한 전문인력 양성제도나 기관은 극히 취약한 실정이다. 이와같은 상황에서 보안 전문인력의 양성을 위한 자격인증 제도의 도입이 절실히 요구되고 있다.

따라서 본 연구는 전자상거래 보안 전문가를 양성하기 위한 연구로서 자격증 인증제도의 도입에 관하여 실무적으로 접근한다는 점에서 그 의의를 갖는다. 즉 본 연구는 전자상거래 보안전문가 자격제도의 도입, 관련 교육에 관한 이론적, 실무적 체계 마련 등 전자상거래 보안전문가 자격인증제도의 기반을 연구함으로써 국내 전자상거래 보안 수준을 향상시키고 나아가 전자상거래 발전에 기여하게 될 것이다.

1. 서 론

전세계는 인터넷을 매개로 시공을 초월한 하나의 전자시장으로 발전해 가고 있다. 직접 대면하는 일반 상거래와는 다르게 전자상거래는 전자적 매개체를 이용하여 상품과 서비스 판매방식의 변화를 추구하여 효율성과 비용절감을 가능케 하였다. 예를 들면, 판매자는 고객에 대한 정보를 입수하여 차별화된 마케팅을 할 수 있으며, 인터넷을 새로운 유통 채널로 대신하여 제품의 원가를 낮추어 경쟁력을 가질 수 있게 되었다. 또한 소비자는 다양한 제품의 가격을 실시간 적으로 정보를 입수하여 최적의 선택을 할 수 있다. 이와 같이 가격이 신속하게 결정되고 거래비용을 감소시켜 효율적 시장을 쉽게 형성할 수 있게되었다(노규성 · 조남재, 2000).

그러나 인터넷의 속성인 개방성에 따라 해커(hacker)의 공격에 쉽게 노출되며 또한 자연재앙, 인간의 실수, 하드웨어와 소프트웨어의 결함 등으로 인한 많은 보안상의 위협이 있으

†선문대학교 경영학부 ‡우석대학교 컴퓨터교육과

며, 전세계의 불특정 다수가 참여하는 가상 공간에서는 사기와 속임수가 발생할 가능성이 높다.

따라서 전자상거래 전반에 걸쳐 보안이 필요하지 않은 곳이 없다고 해도 지나치지 않을 정도로 핵심적인 요소이고 적절한 보안 장치가 없다면 전자상거래 자체가 존재하기 어렵다. 결국 전자상거래 보안은 전자상거래의 성공여부를 결정할 수 있는 신뢰성 확보를 위한 기반 기술로서 인식되고 있다.

특히 전자상거래의 급성장과 함께 보안사고가 잇따르고 있는 상황에서 이를 대처하기 위한 전문인력이 절대적으로 부족함에도 불구하고 이런 상황을 타개하기 위한 전문인력 양성 제도나 기관은 극히 취약한 실정이다. 이와 같은 상황에서 보안 전문인력의 양성을 위한 자격인증 제도의 도입이 절실히 요구되고 있다.

따라서 본 연구는 전자상거래 보안 전문가를 양성하기 위한 자격인증제도의 도입에 관한 탐색적 연구로서 그 의의를 갖는다. 즉 본 연구는 전자상거래 보안전문가 양성을 위한 자격제도의 도입, 관련 교육에 관한 이론적, 실무적 체계 마련 등 전자상거래 보안전문가 자격인증 제도의 기반을 연구함으로써 국내 전자상거래 보안수준을 향상시키고 나아가 전자상거래 발전에 기여하게 될 것이다.

2. 연구 배경

2.1 전자상거래 보안 필요성

전자상거래는 네트워크를 통하여 형성되므로 사용자들은 서로 만나지 않고 거래하게 된다. 이는 전자상거래의 장점이기도 하지만 반대로 상호간의 신분에 대한 확인이 쉽지 않다는 단점이 되기도 한다.

인터넷에서 안전한 전자상거래를 위해서는 우선 거래 상대가 본인인가를 확인함과 아울러 거래 정보의 복사에 의한 정보의 부당한 취득을 방지하는 대책이 필요하다. 즉 거래 상대의 본인 인증을 행하고 거래 내용에 부정이 없는 것을 증명하는 구조가 있어야 하고, 거래 내용을 제 3자에게 노출되지 않게 기밀성을 보장하는 암호화와는 다른 사람에 의한 개조 또는 본인이 작성한 사실이나 내용을 부정할 수 없게 하는 전자서명기능을 채택한 프로토콜 등이 절실하다(조남재 · 노규성, 2000).

인터넷 특성에 기인한 전자상거래의 취약성과 이를 보호하기 위한 기본적인 대책을 기반으로 하여 전자상거래 보안 필요성을 정리하면, 다음과 같다.

첫째, 정상적인 정보의 기능유지 측면에서 볼 때 정보는 고유한 사용 목적과 기능을 유지해야하고 필요한 장소, 필요한 사람, 필요한 시점에 정확히 전달되어야 한다. 그러나 정보자체가 무결성이나 비밀성 등을 보장하지 못하며 무용지물이 될 소지가 많으므로 정상적인 정보의 기능 유지를 위해 정보보안이 필요하다.

둘째, 자산의 보호측면에서 정보는 정보에 관련된 모든 자산, 즉 하드웨어, 소프트웨어, 데이터 등의 손실과 왜곡으로 막대한 재정적 손실을 초래할 수 있으므로 정상적인 정보통신망

운영과 정보에 관련된 모든 재산권 보호를 위해 정보보안이 필요하다.

셋째, 개인정보의 보호측면에서 정보는 정보통신망의 확대와 컴퓨터 보급확장 등으로 인해 개인정보의 침해 가능성도 증가되어 가고 있어 개인의 프라이버시(privacy)보호를 위해 정보보안이 필요하다.

넷째, 국가안전에 관한 측면에서 정보통신망의 보안 허점으로 인한 국가기밀정보의 위협은 국가 경쟁력 약화까지 초래할 수 있으므로 국가의 안전보장을 유지하기 위해서 정보 보안이 필요하다.

다섯째, 정보윤리의 확보 측면에서의 정보의 건전한 유통질서와 안전한 거래를 보장할 수 있는 유통질서 확립과 정보의 역기능을 예방·방지할 수 있는 정보윤리의 확보를 위해 정보보안이 필요한 것이다.

결국 위와 같이 전자상거래 보안의 필요성이 향후 큰 부분을 차지할 것으로 보아 보안 관련 자격증 도입은 매우 중요한 사안이라고 볼 수 있다.

2.2 전자상거래 보안 관련 현황

2.2.1 국제 동향

전자상거래 관련 기술중에서도 가장 기초가 되는 기반 기술로는 암호화 기술과 인증기술이라고 할 수 있다. 암호화와 인증기술은 기술수준의 성숙도면에서 볼 때, 다수의 기술이 경쟁적으로 개발되고 표준화가 진행되는 유아기 단계에서 표준화된 기술들이 확실한 사용자층을 확보하고 범위를 넓혀 가는 단계인 성장기 단계로 정의되는 과정에 있다고 볼 수 있다. 암호 알고리즘은 이미 DES나 RSA 등이 사실상의 표준으로 널리 사용되고 있으며 키 관리를 위한 절차나 메커니즘도 표준화가 진행중이다. 인증기술은 암호화 메커니즘(공개키 기반)을 사용하고 인증서에 대한 표준은 ITU-T의 X.509에 규정되어 있으며 사실상의 표준(de facto standards)으로 그 영역을 넓혀가고 있다(한국전산원, 1998).

그러나 인증절차나 인증기관의 역할, 그리고 인증기관간 상호운용성의 확보 등의 법/제도적 문제는 새로운 국제적 현안으로 대두되고 있으며 이에 대한 해결이 전자상거래의 범세계적 확산에 매우 중요한 역할을 하게 될 것이다. 또한 암호키 위탁 및 복구 등 암호화된 정보에 대한 정부의 접근권 보장을 포함하는 암호화 기술의 사용과 수출입용 보안제품에 사용되는 키의 크기를 제한하는 수출입 정책은 현재 국가간 그리고 정부와 민간간의 핵심 현안으로 대두되고 있다. 현재 미국은 암호화된 정보에 대한 정부의 접근 권한 보장 여부 및 그 방식에 대해 행정부와 입법부에서 활발한 정책과 입법방안이 검토되고 있으며, 암호장비의 수출입 규제와 함께 민간 산업계와 많은 논란이 야기되고 있다. 이에 대한 대응방안으로 국제적으로는 OECD에서 '97년 "암호정책 지침"을 발표하여 전자상거래의 촉진 및 프라이버시 보호를 고려하면서도 정부의 적법한 접근권을 보장하는 암호 정책을 권고하고 있다.

현재 보안기술 수준은 개발 또는 개선될 여지는 많으나 상당 부분 표준화가 진전되고 있으며 안정화되고 있다. 그러나 법/제도적인 면에서는 아직도 해결해야 할 많은 문제를 내포

하고 있고 국가간의 기술수준과 환경의 차이로 인해 합의도출 가능성이 용이하다고 볼 수 없다. 따라서 기술적인 면과 법/제도적인 면을 고려한 전체 환경적인 측면에서는 유리하지도 그렇다고 불리하지도 않은 중간 수준이라고 볼 수 있다.

2.2.2 국내 현황

국내 전자상거래 정보 보안 현황은 외국에 비해 취약한 상태이다. 또한 지불 프로토콜 분야에서만 개발이 이루어지고 있는 상태이며, 이러한 현황은 시급한 정부 지원하에 정책 마련 및 민간부문에 대한 지원이 시급하다는 것을 나타내고 있다. 국내 보안기술의 수준은 자체 기술을 일부 보유하고 있으나 성능면에서 미약한 수준이라고 할 수 있는 소화모방 단계에 있고 인증기술은 선진국의 기술을 이해하고 이를 구현하고자 노력하는 독자복제 단계라고 할 수 있다(김정덕, 1999).

1) 보안관련 기술분야의 현황

전자상거래 보안부분에서 가장 취약한 분야가 기술분야이다. 거의가 외국의 기술을 도입하여 사용하고 있다. 따라서 국내 현실에 맞지 않거나. 특수한 상황을 해결하지 못해서 사용자들이 이에 적응하여 사용하는 경우도 있는데, 이러한 기술분야에 대한 추진현황을 보안 프로토콜, 지불 프로토콜, 전자화폐 시스템, 인증서비스로 나누어 살펴보면 다음과 같다(한국전산원, 1998).

첫째, 보안 프로토콜 분야는 인터넷의 TCP/IP를 기반으로 한 고도의 웹 기반기술(웹서버 및 웹브라우저 제작 기술)을 요구하기 때문에 국내에서는 개발하기 어려운 실정이다. 보안 프로토콜 분야는 미국의 넷스케이프나 마이크로소프트와 같은 웹 관련 핵심기술을 보유하고 있는 기업체나 IETF와 같은 인터넷 관련 표준 단체등에 의해 이루어지고 있으며, 국내 기업체나 연구기관의 참여도는 거의 없는 실정이다.

둘째, 지불 프로토콜 분야는 SET과 Non-SET으로 분류되며, 국내에서는 SET 1.0사양에 따른 제품 개발이 완료 또는 진행되고 있는 상태이고, 일부 업체등은 자사만의 Non-SET을 개발하고 있는 상황이다. 현재 지불 프로토콜의 대표적인 예로는 비자와 마스터카드를 주축으로 개발된 SET 1.0이 있으며, Non-SET으로는 미국의 Cyber Cash, First Virtual 등이 있다. 국내의 경우 SET 관련하여 커머스넷 코리아에서 한국형 전자상거래 산업을 추진하고 있으며, 데이콤 등이 기술개발을 담당하여 SET시스템을 구축하고 현재 운영 중이다.

셋째, 전자화폐 시스템 분야는 몇몇 연구기관에 의해 일부 연구되고 있는 실정이다. 전자화폐 분야는 인터넷 기반이 아닌 오프라인 방식의 일반 직불카드와 유사한 기능을 갖는 시스템으로 개발되기 시작하였으나, 현재는 인터넷 전자상거래와 접목되어 개발 전개되고 잇는 추세이며, 유럽의 Mondex나 Ecash가 가장 앞선 기술을 보유하고 있다. 일본 NTT는 1997년부터 전자화폐 시스템 개발을 추진하고 있으며, 1999년부터 시범 서비스를 실시하고 있다.

넷째, 인증서비스 분야에서 국내 인증관련 기술 개발은 SET규격 또는 미국의 연방 공개키 기반구조(PKI. Public Key Infrastructure)규격에 따른 시스템 개발이 주류를 이루고 있

으며, 시스템공학연구소, ICEC(International Center for Electronic Commerce)등은 SET규격에 따른 인증시스템을 개발하였으며, Metaland에서는 ICEC에서 개발한 인증시스템을 운영하고 있다.

2) 전자상거래 보안 관련 법제도의 현황

인터넷의 빠른 보급에 따라 이를 이용한 네트워크상의 거래에 대한 신뢰 및 소비자를 보호하고자 전자상거래를 활성화시킬 목적으로 정부에서는 1998년 12월 전자거래기본법과 전자서명법을 제정·공포하였으며, 1999년 7월 1일부터 시행되고 있다. 이와 관련되는 법제도를 보안문제나 정보보호 등의 주제로 한정하여 살펴보면 다음과 같다.

가. 전자거래기본법

전자거래기본법은 전자문서가 서면문서와 동일한 수준의 법률적 효력을 부여받는 것은 전자상거래에 있어서 신뢰성 확보 및 소비자 보호 그리고 전자상거래의 촉진을 위해 안전하게 거래를 할 수 있도록 하는 것을 기본방침으로 하고 있다.

전자상거래의 안전성과 신뢰성을 확보하기 위해서는 전자 거래 당사자간의 신원을 확인해 주는 공인 인증기관을 전자서명법의 규정에 따라 지정할 수 있도록 하였으며(제16조·17조) 이와 아울러 전자거래를 이용하는 소비자의 기본권익을 보호하기 위해서는 관계 법령에 따라 소비자에의 정보제공, 소비자피해보상기준의 적용 등 필요한 시책을 마련하도록 하였다(제29조 또는 32조).

나. 전자서명법

전자서명법의 내용은 총칙, 공인인증기관, 인증서, 인증 업무의 안전 및 신뢰성확보, 보칙, 벌칙 등 6개장으로 구성되어 있는데, '전자서명'을 비대칭 암호기술을 활용한 digital signature로 정의하고, 전자서명과 전자문서의 법적 효력을 부여하며(제3조), 안전한 전자서명의 이용 기반을 조성할 수 있도록 공인인증기관 같은 기관을 두어 객관성 있는 전자서명상의 인증을 하도록 하며(제4조), 공인 인증 업무의 적절성 및 지속성을 확보하기 위하여 필요한 규정(제6조 또는 14조)을 두고 있다. 또한 인증서의 신뢰성 확보를 위하여 인증서에 포함할 내용을 명확히 하고(15조), 인증서의 발급·효력정지·폐지절차 및 방법 등에 관한 세부적인 사항을 규정하고 있다(제 16조 또는 18조). 또한 전자서명을 안전하게 사용할 수 있는 환경 조성 및 효율적인 공인인증기관 관리를 위하여, 한국정보보호센터로 하여금 전자서명 인증관리 업무를 수행하도록 하였다(제25조). 마지막으로 국가간의 전자적 거래에 대비하여 정부가 외국 인증기관이 발행한 인증서를 상호 인정하는 협정을 체결할 수 있도록 규정하고 있다(제26조).

2.3 전자상거래 보안 인력 현황과 양성과제

전자상거래를 비롯한 인터넷 산업의 급속한 발전으로 이 분야의 전문인력 수요가 폭주하지만 인력공급은 좀처럼 늘지 않아 갈수록 인력부족 현상이 심화될 것으로 분석됐다. 산업연구원(KIET)이 펴낸「인터넷산업의 현황과 발전방안」 보고서에 따르면 올해 전자상거래

분야의 인력수요는 1만6천여명인 반면 공급은 5천5백여명에 불과, 1만명 이상이 부족할 것으로 예상됐다(hani.co.kr). 인터넷산업 전체분야에서, 특히 소프트웨어와 컨텐츠 분야에 비해 전자상거래 분야의 인력부족 현상이 가장 심각한 것으로 보이는데 2001년 전자상거래 분야 인력 수요는 2만6천여명으로 추산되지만 공급은 6천5백여명에 불과, 2만명 가량의 수급 부족이 우려된다. 또 2002년에는 수요가 3만7천여명으로 늘지만 공급은 6천6백여명에 그쳐 3만명이상이 부족하고 2003년에는 인력부족 규모가 4만6천여명에 이를 전망이다.

그러나 이러한 견해는 단지 전자상거래 관련 모든 분야를 합친 전망이며 보안 분야에 국한할 경우 상황은 더욱 심각하다 해도 과언이 아니다. 이와같이 전자상거래 보안인력이 절대적으로 부족한 상황에서 정보통신부가 향후 5년간 정보보호 교육과정 및 연구센터 등을 대폭 확충해 2만 4천여명의 정보보호인력을 공급하고 2천8백여억원을 투자해 정보보호기술을 적극 개발하는 등 정보보호산업을 중점 육성할 계획을 발표하였다(etnews, 2000.9.29). 즉 보안 대책의 필요성과 중요성을 감안할 때 정보보호 분야의 인력을 집중 양성하는 것은 국가적으로 올바른 정책이라고 볼 수 있다.

2.4 전자상거래 보안 자격 제도의 필요성

인터넷의 개방성으로 인하여 개인 및 기업의 보안 문제가 사회적 관심사로 대두되고 있는 가운데 국내외적으로 해킹사건이 급증하고 있다(joins.com, 2000.9.30). 최근의 전자상거래 활동을 살펴보면 전자상거래를 위한 기술발전 및 법/규제 제거 등 공급자위주의 관점으로부터 소비자의 요구사항(신뢰, 편의성) 등을 고려해야 전자상거래 확산이 가능하다는 점이 강조되었다. 즉 신뢰의 중요성이 점증되고 있으며 이는 보안, 인증, 암호화 등을 통한 신뢰를 바탕으로 소비자들이 거래에 대한 통제수준, 평판, 품질보증 등을 통한 신뢰를 제고시키는 것이 전자상거래의 성공여부를 결정할 수 있는 주요한 기반기술로서 인식되고 있다.

결국 전문적 보안 지식을 가진 전문가의 인력 양성이 매우 시급하다 할 수 있는데, 국내에서는 아직 전자상거래 보안 전문가 자격증 제도가 시행되고 있지 않고 있어 인력양성이 활발하게 전개되지 못하고 있다. 따라서 전자상거래 보안자격제도가 시급히 도입되어 관련 인력양성을 위한 제도적 기반이 마련되어야 하겠다.

3. 전자상거래 보안 전문가의 자격구조와 인증체계

3.1 전자상거래 보안관련 자격제도의 국내현황

현재 국내에서 시행되고 있는 보안 관련 전문 자격증으로서 알려져 있는 것은 두가지가 있다. 먼저 미국 정보시스템 감사통제협회(ISACA)에서 부여하는 정보시스템 감사사(CISA:Certified Information System Auditor) 자격증을 들 수 있다. CISA 자격증은 정보시스템 감사분야의 전문자격증으로 정보시스템 통제, 보안 및 감사분야의 전문가임을 국제적으로 인정받게 된다. 그러나 이 자격증에서 보안은 정보시스템 감사의 한 부분으로 다룬다

고 볼 수 있으며, 특히 전자상거래와 관련해서는 직접적으로 관련시키고 있다고 볼 수 없다.

한편 한국정보통신자격협회에서 시행하는 민간자격증으로 인터넷보안전문가(Internet security professional) 자격증이 있다. 이는 인터넷보안에 필요한 전문지식을 가지고 서버관리, 보안설정, 서버보안분석, 정보보호, 서버 복구 등의 업무를 전문적이고 정확하게 수행할 수 있는 능력을 검정하여 1급, 2급, 3급으로 나누어 자격을 인증한다. 그러나 이 자격증은 인터넷과 관련되는 보안문제를 다루므로 전자상거래와 직접 관련되는 응용분야나 기술적 요소는 아직 다루고 있지 못한 실정이다. 따라서 전자상거래와 관련하여 발생할 수 있는 보안 피해 및 이의 대책에 관한 지식과 기술을 필요로 하는 전문자격 제도가 별도로 마련되어야 할 것이다.

3.2 직무분야, 검정기준 및 응시자격

3.2.1 직무분야

전자상거래 보안은 전자상거래를 활성화시키기 위한 기반 기술이라고 할 수 있다. 따라서 전자상거래 전문가가 알아야 할 보안 분야는 첫째, 암호기술의 이해, 둘째, 정보통신기술, 셋째, 인터넷 보안, 넷째, 전자상거래 응용 보안으로 구분할 수 있다.

3.2.2 검정기준 및 응시자격

검정기준은 기반 보안인 암호기술, 정보통신기술, 인터넷 및 시스템보안을 통하여 전자상거래의 응용보안을 이해할 수 있는 수준으로써 상당한 수준의 전문성을 요구해야한다. 따라서 향후 보안 인원의 수요에 따라 인력의 확산이 제기됨으로써 자격증을 제안하고자 하고 명칭은 전자상거래 보안 전문가로 이름을 붙인다.

전자상거래 보안 전문가 자격증 시험은 현업에서 보안과 관련하여 활동하는 인력이나 보안에 관심이 있는 인력이면 누구나 응시할 수 있으나 보안 기술에 대해 체계적인 교육을 받아 심도있는 지식을 갖춘 사람이어야 할 것이며, 보안전문 인력의 확충을 목적으로 하는 신설 자격증이어야 하므로 학력 및 경력에 대한 제한을 두어서는 안된다고 판단된다.

3.3 검정방법, 검정과목 및 합격기준

전자상거래 보안 전문가 검정방법은 필기시험과 실기시험으로 이루어진다. 필기시험 내용은 크게 전자상거래 정보보호 개론, 전자상거래 암호기술, 전자상거래 보안기술, 전자상거래 시스템 운영 및 관리, 전자상거래 응용보안의 5개 부문으로 나누어 시험이 치러지고 (김정덕, 1999) 실기시험은 전반적인 실무적 적용 기술을 파악한다. 검정과목에 따라 출제 비율을 다르게 할 수 있으며 아울러 대단원 및 중단원의 구성내용과 수준으로 과목을 세분할 수 있다.

현행 국가기술자격의 합격기준은 필기시험의 경우 과목별 중요도에 관계없이 전체 검정과목 점수의 평균 60점 이상의 획득과 과목별 최소 40점 이상의 획득을 합격기준으로 하고 있

다.

3.4 출제기준 및 채점 방법

출제기준은 직무분석에 의해 제시된 전자상거래 보안 전문가의 직무를 수행하기 위해 필요한 지식, 기술, 기능에 대한 사항은 전자상거래 보안기술 체계를 기준으로 작업별로 추출하여 이를 분류·종합하여 검정과목으로 제시한다. 또한 검정과목에서는 문제출제 기준을 만들기 위해 해당 지식, 기술, 기능을 대단원과 중단원 수준으로 분류하였다. 검정과목에 있어서도 단원별 중요도에 따라 배점기준을 달리하기 위해 대단원 수준에서 중요도를 평가하여 중요도에 따라 출제배점을 달리하도록 한다.

한편 실기시험은 전자상거래 보안 전문가가 알아야 할 실무지식으로서 시스템 보안관리, 시스템침해분석, 방화벽 구축, 시스템관리, 사용자관리, 보안관리, 서비스관리, 암호 및 코드, 바이러스 분석 등 전자상거래 보안실무 능력을 점검하도록 치뤄져야 할 것이다.

필기시험의 채점방법은 5지선다형의 경우, 여러 기본 개념에 대한 정확한 의미를 이해하고 있는지를 파악하기 위하여 올바른 문항을 객관식으로 출제하여 채점기준을 작성하며, 단답형 문항의 경우, 핵심 개념 및 기술과 밀접한 연관이 있는 중요 단어들을 중심으로 문항별로 상세한 채점기준을 작성한다.

4. 결 론

4.1 전자상거래 보안전문가 자격인증의 도입효과

현재 우리 나라에서 실시하고있는 인터넷 기술 자격 인증시험(민간자격)은 지난 3년 동안 10만 명에 이르는 인원이 응시, 약 2만5천 여명의 합격자를 배출하였고, 합격자들은 상대적으로 높은 취업률을 기록한 것으로 나타났다.

우리 나라는 지난 1997년부터 IMF 구제금융시대에도 불구하고 정보통신 분야의 경우 지속적인 고용환경을 유지하였고, 최근 들어 일부 전문직종에는 인력품귀 현상까지 일어나 타 업종과 대조를 보이고 있다. 이러한 정보통신, 특히 인터넷을 중심으로 하는 사이버 공간에 전자상거래, 인터넷서비스제공사업(ISP), 정보제공사업(IP), S/W, 컨텐츠 산업 등 다양한 정보산업에 대한 발전의 토대를 마련하여 2002년까지 이 분야에서만 약 70만 명의 새로운 일자리가 창출될 것으로 전망된다.

이는 보안 측면에서의 세부적인 자격증이라 할 수 있는 전자상거래 보안전문가 자격 제도의 도입을 절대적으로 필요로 하는 전자상거래 시장의 발전 추이라 할 수 있다. 전자상거래 보안 전문가 자격증은 이 인력부족 현상을 타개함과 동시에 전자상거래의 신뢰성을 높이는 차원에서 전자상거래 발전의 중대한 가교역을 할 것으로 기대한다.

4.2 전자상거래 보안전문가의 진출분야

전자상거래 보안 전문가의 진출분야는 전자상거래가 활발할수록 더욱 더 다양하며 앞으로도 계속적으로 새로운 분야들이 나타나고 있다.

현재까지 필요한 분야는, 첫 번째로 보안 컨설팅 사업으로 보안 분야 신제품 개발을 위한 기술 자문과 기존 기업의 보안 사업 확대 컨설팅에 참여할 수 있으며, 둘째로 시스템 개발 능력을 보유하여 정보보안 제품 및 서비스 개발분야로 진출하고, 셋째 해킹 방지 요원, 다섯째 금융기관에 진출하여 전자지불이 보편화되는 추세에 맞추어 지불 프로토콜 관리를 위한 운용 요원으로서의 역할이다. 여섯째 보안 교육 전문가로 그리고 마지막으로 인증업의 진출이다. 이는 전자서명법이 시행됨에 따라 공인인증기관의 저자서명이 분명한 법적 근거를 가지게 되고 공인인증기관의 활용이 활성화되면 거래상의 불확실성과 위험의 상당 부분이 극복되어, 중요한 거래 문서의 교환이 인터넷 상에서 활발히 이루어질 수 있을 것이다, 또한 이때를 기점으로 기존에 미미하거나 전무했던 새로운 인증 관련 산업이 촉발될 것으로 예상된다.

4.3 정책적 제언

현재 보안부문에서 국내 독자 개발한 기술(디지털 서명 기술 등)을 더욱 안정적으로 발전시켜 가면서 동시에 국가 안보차원에서 전략적 중요성을 지니는 암호화나 인증 기술에 더 많은 투자를 촉진하기는 하나, 위험을 최소화하기 위하여 선도적, 실험적 투자가 이루어지고 있는 해외 사례 등을 기다려 이를 분석하고 성공 가능성이 높은 방향을 선택하여 새로운 기술과 체제를 도입, 개발, 또는 실행할 필요가 있다. 즉, 보안 관련 표준 동향을 면밀히 분석하며 이를 우리의 역량과 결부시켜 빠른 시간내에 구현시키고 국제기구에서의 보안 관련 활동을 분석적으로 비교 검토하여 이를 우리의 보유 기술과 정책 환경에 적합하도록 유도할 필요가 있다. 이에따라 다음과같이 정책적 제안을 제시한다.

첫째 충분한 정보보안 전문인력의 양성 및 확보로 전자상거래의 활성화를 촉진하고 거래 당사자들에게 신뢰감을 주고, 둘째 정보보안의 윤리적 의식 확산으로 정보 및 정보사용의 의미에 대한 올바른 인식과 정보를 보존·보호할 수 있는 책임감을 확실하게 갖게한다. 세째 정보보안을 위한 전담기구의 설치 및 운영으로, 이는 개방 지향적인 전자상거래의 구성요소들을 통합 관리하고 각 분야별로 잔재해 있는 정보보안 요소들이 분석·평가되기 어려운 전자상거래상의 일련의 과정을 조정·관리하는 것이다. 넷째 정보보안을 위한 인력관리 및 교육으로 전자상거래상의 정보보안을 위해서는 관련자에 대한 엄격한 관리와 감시장치가 필요하다. 마지막으로 정보보안을 위한 정부의 역할로서, 전자상거래의 정보보안을 위해서는 정부의 역할이 필수적이다. 왜냐하면 정부도 이러한 전자상거래의 당사자가 될 뿐만 아니라, 이제 모든 사회 구성원의 생활 가운데 자리매김 하고 있는 전자상거래의 원활한 운영과 진행을 위한 기반조성의 책임이 있기 때문이다. 전자상거래의 주요 매체인 인터넷은 이미 각 개인이나 기업의 차원에서 통제될 수 없는 그야말로 세계적인 정보의 바다이다. 그러므로 정부가 할 수 있는 가능한 범위내에서 일관적이고 지속적인 통합적인 정책지원이 이루어 져

야 한다.

또한 전자상거래 관련 전문가들은 전자상거래 등 업체의 경우 사업을 하려면 의무적으로 정보보안 시설을 갖추도록 법제화하는 등의 제도적인 장치가 마련되어야 함을 강조하고 있다 (donga.com, 2000.7.31).

아울러 이러한 정보보안이 기업이나 개인 그리고 정부에게 주는 의미나 중요성 그리고 효과에 대한 홍보와 교육의 체계적 확립을 통해서 보다 활성화된 전자상거래가 이루어지도록 유도해야 할 것이다. 이에 따른 정보보안 마인드의 확산과 이에 대한 전자상거래 운영을 주도하여 전자상거래에 대한 회의적 또는 부정적 인식에 대한 변화를 촉발하여야 할 것이다. 이러한 일련의 정부의 역할은 단순한 전자상거래 만을 위한 정보보안이 아닌 정보사회의 총체적인 유지를 위한 정보보안 정책의 커다란 틀 속에서 이해되고 실행되어야 할 것이다.

참고 문헌

[1] 김정덕, "전자상거래 시스템 및 네트워크 보안기술', 한국전산원, 1999.

[2] 노규성 · 조남재, "전자상거래 관리사가 되는 길", 동광출판사, 2000.

[3] 동아일보, http://www.donga.com, 2000.7.31.

[4] 생산성본부. http://www.ecrc.kpc.co.kr

[5] 송유진 외, "전자상거래가 세상을 바꾼다", 1999.

[6] 이만영 외, "전자상거래 보안 기술", 생능출판사, 1999.

[7] 전자신문, http://www,.etnews.co.kr/

[8] 조남재 외. "전자상거래 보안기술", 1998.

[9] 조남재 · 노규성, "전자상거래 관리사 4권 시스템 운영 및 관리 ①", 한국전자상거래연구소, 2000.

[10] 조찬식, "전자상거래 정보보안", 한국직업능력개발원, 1999.

[11] 중앙일보, http://www.joins.com/

[12] 한겨레신문. http://www.hani.co.kr/

[13] 한국인터넷정보센타(KRNIC). http://www.nic.or.kr

[14] 한국전산원, "인증체계 분석 및 동향보고", 1998.

[15] 한국전산원, "전자상거래를 위한 보안기술 체계 및 요소기술에 대한 이해", 1998.

[16] 한국전산원. http://www.nca.or.kr

[17] 한국정보보호센타, http://www.kisa.or.kr

[18] 한국정보보호센터, "인증분야에 대한 OECD 국가의 주요 논의사항 및 접근방법", 1999.

[19] 한국정보통신자격협회, http://www.icqa.or.kr

[20] 홍승필 · 고재욱, "정보보안 기술과 구현", 파워북, 1998.