通信情報保護學會誌
第 11 券 第 2 號, 2001. 4

국내 정보보호제품의 표준 적합성 시험과 인증 체계

장 청 룡*, 김 학 범**, 이 홍 섭**

요 약

사이버 패러다임으로 의하여 지식기반사회에서 요구되는 신뢰성과 안전성을 실현하기 위하여 정보보호 기능 이용이 대중화됨에 따라 이러한 기능을 구현한 제품의 제조와 활용이 보편화되고 있다. 이에 따라 정보보호 제품에 대하여서도 이를 이용하는 사용자들은 일반적인 개방형 시스템의 적합성 시험과 유사한 수준의 시험을 통과한 제품을 구매하여 자신에게 적절한 안전한 시스템을 구축하여 운용하기를 원하게 된다. 이를 위하여 본 고에서는 정보보호제품의 표준적합성 시험과 관련된 국내외 동향을 살펴보고 국내 환경에 적용가능한 정보보호 제품의 적합성시험 및 인증 체계의 수립시의 고려사항들을 제안하고자 한다.

Ⅰ. 서 론

정보통신 제품들을 구매 또는 조달하는 사용자들은 표준에 준거하여 구현된 제품들을 구매하여 운용하기를 원한다. 그러나, 일반 사용자들의 대부분은 구매 제품이 표준에 적합하게 구현되었음을 판단한다는 것이 그리 쉽지는 않다. 또한 제조회사 자체도 기술 환경이 급속하게 변화됨에 따라 표준의 적합 시험을 위한 시험환경을 모두 갖추어 시험하기도 어려운 실정이다. 이를 위하여 일반적으로는 시험 서비스 기관에 의뢰하여 시험을 받아 이의 결과를 인증받는다. 그리고, 적합성 시험에 대한 인증 제품이라 할지라도 다양한 벤더들의 생산 제품들간에 상호 운용성을 보장할 수 없다. 따라서, 적합 인증 제품들을 상호 접속하여 그들 제품간에 상호운용이 가능함을 보여주어야 하며 이러한 결과를 공개함으로써 사용자들의 운용 편의성을 증진시켜 제품간의 상호 접속시 야기 될 수 있는 인터페이스 비용을 최소화하여 이를 이용하여 개발하는 제품 또는 서비스의 경쟁력을 제고시킬 수 있게 된다[1, 2].

지식기반사회에서 사이버 패러다임으로 의한 정보보호 기능 이용의 대중화로 이러한 기능을 구현한 제품의 제조와 활용이 보편화됨에 따라 정보보호 제품에 대하여서도 앞서 언급한 바와 같은 일반적인 개방형 시스템의 적합성 시험과 유사한 수준의 시험과 인증 체계가 요구되고 있다. 이를 위하여 본 고에서는 국내에서 정보보호제품의 표준적합성 시험과 인증 체계의 수립시의 고려사항들을 제안하고자 한다.

Ⅱ. 정보보호제품 표준 적합성 시험 동향

1. 국제 동향

정보보호 제품의 평가와 적합성 시험에 대한 오랜 경험을 갖고 있는 미국의 경우는 연방 정부를 포함하는 정보보호 제품의 조달을 위한 정부 기관 중심 프로그램과 순수한 민수용 정보보호 제품에 대한 민간 업체 중심 프로그램으로 대별된다. 먼저, 상무성 산하인 NIST가 CFR(Code of Federal Regulation) Title 15 Part 285에 근거한 민간의 자발적인 시험기관 인정 프로그램인 NVLAP(National Voluntary Laboratory Accreditation Program)중 보안 기술 평가 프로그램(TTAP : Trusted Technology Assessment Program)을 운영하고 있다. 이의 세부 운영지침으로서는 NIST Handbook 150이 있으며 최근 암호기술 표준에 근거한 제품의 구현 기능의 적합성 시험을 위하여 암호 모듈의 검증

* 경동대학교 (crjang@kyungdong.ac.kr)
** 한국정보보호센터

(CMV: Cryptographic Module Validation)과 연방 PKI 프로그램을 운영하고 있다[3]. 또한, 국방성 산하의 DISA(Defence Information Systems Agency)에서도 국방정보기반과 관련한 국방 PKI 프로그램을 운영하고 있다[4].

한편, 민간 업체들에 의한 시험과 인증체계로는 자사 개발 표준인 S/MIME과 PKCS에 대한 시험을 하는 RSA사[5], 다양한 벤더들로부터 암호 제품, 침입차단시스템, 침입탐지시스템, IPSec 제품, PKI 제품 등에 대한 제 3자 시험의뢰를 받아 시험과 인증을 하는 TruSecure사[6], VPN 제품에 대한 시험을 하는 VPN 컨소시움이 설립되어 운영되고 있다[7].

유럽에서는 주로 ITSEC에 의하여 정보보호 제품의 평가를 하지만 이도 최근 국제 공통기준(CC, ISO/IEC 15408)에 근거하여 처리하고 있다. 더욱이, 정보보호 표준에 대한 구현의 적합성에 대하여는 영국의 상무성 산하 NPL에서 기존의 개방형 시스템에 적용한 적합성 시험 기법을 정보보호제품에 적용할 수 있도록 SCT(Strict Conformance Test)에 대한 관련 기술을 개발하고 이의 표준화를 위한 노력을 해오고 있는 실정이며 이 결과에 대한 인증은 평가 체계의 일부에 포함하여 처리하고 있다[8].

또한, 국제표준화 기구인 ISO/IEC JTC 1/SC27에서는 정보기술의 보안 보증 프레임워크(ISO/IEC WD 15443)에서 보증을 위한 시험의 하나로서 적합성 시험을 수용하는 입장을 취하고 있다.

2. 국내 현황

국내의 적합성 시험 및 인증은 개방형 정보통신 제품에 대하여 '93년부터 적용되기 시작하였다(전기통신표준재정 및 적합인증에 관한 시행 세칙). 이후 전기통신표준화지침(정보통신부고시 제1994-97호, '94. 12)에 의하여 적합인증 업무를 한국통신기술협회에서 운영하고자 하였으나, WTO와 같은 통신시장 정책의 변화 등으로 개방형 정보통신 시스템의 적합인증에 대한 것은 민간의 자발적 참여로 유도하고 관이 주도하는 정책을 최소화였다. 이 결과 정보통신 표준화지침(정보통신부 고시 제1997-29호, 1997. 5)에서는 이와 관련된 적합 인증에 관한 조항이 모두 삭제되기에 이르렀다.

한편, 정보의 안전한 유통을 위하여 정보보호에 필요한 시책의 수립과 시행을 통하여 건전한 지식정보화 사회의 발전과 정보화의 역기능을 최소화하기 위한 취지를 포함하는 정보화촉진기본법(법률 제5669 호, '99. 1개정, '95. 8 제정)이 제정되었다. 이 법률의 시행을 위한 시행령(대통령령 제16,458호, '99, 6) 제15조(한국정보보호센터의 업무등)와 제16조(정보보호시스템의 보완등)에서는 정보시스템의 안전 운영에 필요한 보안요구 수준에 상응하고 신뢰성 있는 정보보호시스템 보급 확대를 도모하고 정보보호시스템의 성능과 신뢰도에 대한 평가기준을 제공하여 이용자의 인지도 및 선택상의 편익을 향상시키기 위하여 관련 기술 기준에 대한 합치여부 평가 또는 인증 업무를 한국정보보호센터가 수행하도록 하고 있다.

이에 따라, 정보통신망 침입차단시스템 평가지침서(정보통신부고시 제1998-20호('98.2.23))를 운영하여 오다가 침입차단시스템을 포함한 정보통신망에 사용하는 정보보호시스템으로 확대 적용하기 위하여 이를 정보보호시스템 평가·인증지침(정보통신부고시 제 2000-15 호, 2000. 2)으로 개정하여 운영하여 오고 있다. 이의 세부 기술 기준으로서는 정보통신망 침입차단시스템 평가기준 (2000. 2. 개정), 정보통신망 침입탐지시스템 평가기준 (2000. 7.)이 고시, 운영되고 있다.

이와 같은 정보보호시스템의 평가·인증지침에서는 평가대상 제품에 대하여 주로 보안 기능과 보증에 관한 시험을 하여 그 결과를 인증하게 된다. 그러나, 이 지침에서도 정보보호시스템에서 정보보호 기능의 구현과 관련하여 해당 표준에 대한 적합성 시험은 별도의 조항으로 규정하지는 않고 있다. 사이버 패러다임에 따른 정보보호 기능 이용의 대중화로 이러한 기능을 구현한 제품의 제조 및 활용이 보편화됨에 따라 정보보호 제품에 대하여서도 본 고의 서두에 언급한 바와 같은 일반적인 개방형 시스템의 적합성 시험과 유사한 수준의 시험과 인증 체계가 요구될 것이다. 다만, 정보보호 기술 또는 기능이라는 특수성으로 어느 정도의 제도권 하에서 운영됨이 바람직할 것으로 사료된다.

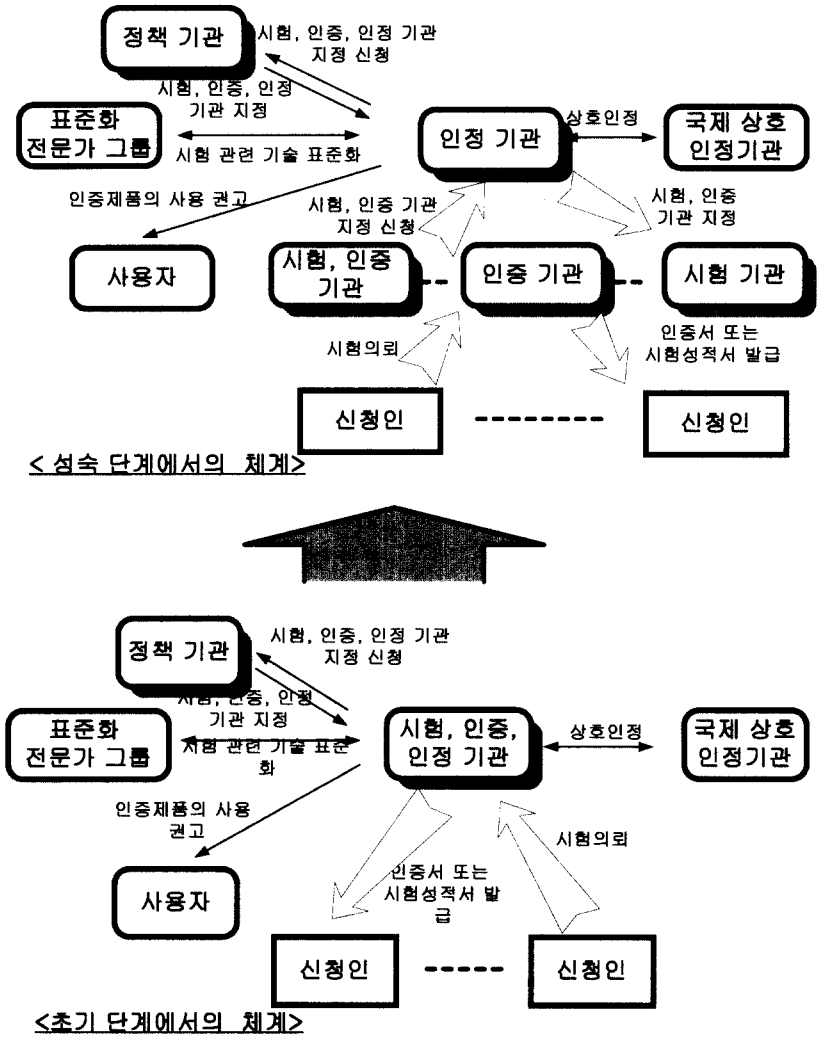
Ⅲ. 국내의 정보보호제품의 표준적합성 시험 및 인증 체계의 제안

정보보호 제품에 대한 국내의 표준 적합성과 상호운용성 시험과 이에 대한 인증 체계의 수립을 위하여 먼저, 기존의 정보보호시스템 평가·인증지침에 수용하여 관련 사항을 별도의 조항으로 하여 추진하

는 제 1안과 가칭 "정보보호시스템의 기술기준 적합 인증"을 별도로 고시하여 운영하는 제 2안이 있을 수 있겠다.

제 1안의 경우는 적합성 시험을 보증을 위한 하나의 시험 수단으로 수용하는 ISO/IEC 모델이며 제 2안의 경우는 미국 NIST의 NVLAP과 유사하다. 그러나, 두 모델에서 적합성 시험을 위한 시험 주체, 시험 방법, 시험 규격 등은 동일하다.

이러한 시험과 인증 체계를 운영을 함에 있어 이의 서비스를 위한 설비투자가 초기 단계에서 일반 벤더 또는 제 3의 시험 기관이 부담하여 추진한다는 것이 상당한 무리가 있을 것으로 사료된다. 즉, 정보보호 기술력과 이의 구현에 대한 검증에 대한 know-how를 갖춘 전문 인력을 확보하기가 그리 쉬운 것이 아니기 때문이다. 따라서, 이의 추진은 초기단계에서 정부 산하 기관으로서 정보보호 기술력의 인력 확보가 가능하여 관련 전문 교육이 원활하고 평가 업무에 관한 경험이 있는 기관의 참여가 필수적이다. 그리고 나서, 시험 서비스 시장이 어느 정도 규모가 커지고 민간의 시험 전문 능력과 경험이 확보되는 성숙 단계에서는 시험소의 인정 프로그램에 의한 제 3의 시험기관 또는 자체 시험소를 인정하여 운영하게 한다. 그리고, 정부 산하 기관은 적합성 시험을 위한 시험 환경에 요구되는 참조 구현의 확보, 시험 표준, 시험 방법 등을 조정하고 표준화하는 업무와 시험 결과에 대한 인증업무를 수행



〔그림 1〕 국내 정보보호제품에 대한 단계별 적합성 시험 및 인증 체계(안)

하도록 하여야 함이 바람직할 것이다.

국내의 정보보호 제품의 적합성 시험 및 인증 체계는 그림 1에 보여지는 바와 같이 초기 단계에서는 정보보호제품의 시험에 관한 총괄적인 정책을 수립하여 시행하는 업무를 정보통신부에서 담당함으로써 정보통신 산업의 균형적인 발전은 물론 정보보호산업의 진일보에 기여가 가능할 것이다. 이의 실제 업무인 시험과 인증 서비스를 위한 실질적 업무는 시험 환경의 구축 운용 즉, 시험 설비와 전문 인력의 확보가 비교적 용이한 정보통신부 산하 기관인 한국정보보호센터에서 그 기능을 수행하도록 하고 그 결과에 대한 인증업무와 국외 인증 결과의 상호인정 등을 위한 업무도 병행하도록 함이 바람직할 것이다. 그리고, 성숙 단계에서 정보보호 산업의 성숙으로 인한 적합성시험 및 인증 서비스 시장이 커지면 한국정보보호센터는 시험소와 인증기관에 대한 평가기관으로서 신청기관에 대하여 그 자격을 심사하여 자격이 되면 인정 프로그램에 의해 이들 기관을 인정하는 인정업무를 수행하게 된다. 또한, 시험 기술 관련 표준화 전문가 그룹과 시험 규격과 참조 구현의 확보에 주력하는 기능을 수행함이 바람직 할 것이다. 한편 적합성시험 및 인증 서비스 시장의 성숙으로 일반 업체 또는 제3의 기관에서는 시험소 및 인증 기관 인정 프로그램에 의한 시험소 또는 인증기관 또는 이 두 가지 기능을 모두 수행하는 시험 및 인증 기관으로서의 서비스를 할 수 있을 것이다.

각 단계에서 적합성 시험과 인증을 위한 기능 주체와 이들의 역할 및 이를 수행할 주무 기관들이 표 1에 설명되어 진다.

〔표 1〕 정보보호제품의 단계별 적합성 시험 및 인증 업무 수행(안)

기 능	역 할	주무 부처 또는 기관	
		초기 단계	성숙 단계
정책 시행	- 정책의 입안 - 정책 수립 및 시행	정보통신부	좌 동
인정	- 인정 프로그램의 수립 및 시행 + 시험소 및 인증 자격 평가 및 인정 + 국제 상호 인정	한국정보보호센터	한국정보보호센터 또는 제 3의 독립기관
인증	- 시험 결과의 평가 및 인증서 발급 - 인증 제품의 공고 및 사용 권고		한국정보보호센터 또는 제 3의 독립기관
시험	- 시험 환경 확보(설비, 기술, 인력) - 시험 규격 및 참조 구현 확보 - 시험 기술 및 방법 자문		한국정보보호센터 또는 제 3의 독립기관
시험 의뢰	- 제품 개발 - 시험 의뢰	제조 업체 및 수출입 업체	좌 동
제품 사용자	- 인증 제품의 활용	정부, 지방자치단체, 기업, 일반인	좌 동
표준화	- 기험 기술 표준화 - 표준화 시험 기술 홍보 및 워크샵 운영	한국정보통신기술협회	좌 동

Ⅳ. 상호운용성 시험

정보통신 제품의 시험으로서 표준에 대한 준수여부를 시험하기 위하여 적합성 시험(conformance testing)이 시행되고 이에 대한 시험 방법의 표준화, 시험 도구의 개발, 시험 서비스가 국제적으로 추진되고 있다. 그러나, 정보통신 제품의 구매조건으로 적합성 시험만을 통과하여 인증된 제품이 실제의 정보통신 환경에 사용하기에는 충분치 않으며 상호운용성 시험(interoperability testing)의 실시를 요구하는 추세이다.

더욱이 적합성 시험은 시험 도구를 이용하여 미리 준비되어 있는 시험항목(test case) 만을 시험함으로써 주어진 특정 조건하에서의 프로토콜 측면만을 고려한 시험이기 때문에 정보통신 서비스의 실용화를 위한 시험으로서는 불충분하다는 의견이 있다.

이에 비해 상호운용성 시험은 상이한 벤더들의 인증된 제품간에 실제 운용에 가까운 환경을 설정하여 실제의 동작 및 효과를 시험하는 서비스 중심의 시험이다.

이와 같은 정보통신 제품에 적용한 상호운용성 시험의 개념을 특히 통신 프로토콜을 기반으로 하는 정보보호 제품에도 동일하게 적용할 수 있어 적합성 시험을 통과한 상이한 벤더들의 인증 제품들을 상호운용성 시험 환경 하에서 시험을 하게 된다.

정보보호 제품에 대한 상호운용성 시험에 대한 사례로는 미국의 NIST에서 주관하는 MISPC(Minimum Interoperability Specification for PKI Component) 프로그램, DoD의 PKI 상호운용성 프로그램, NIST와 RSA사의 S/MIME 상호운용성 프

로그램, NIST와 TruSecure사의 IPSec 상호운용성 프로그램이 운영되고 있는 실정이다[3, 5, 6, 9].

이와 같은 상호운용성을 위한 시험 환경을 구성하기 위하여 시험 방법, 시험 도구, 시험 규격 등이 시험에 참여하는 업체, 그리고 이들의 견해를 적절히 수용하거나 조정할 수 있는 기관 또는 협의체가 요구된다. 특히 초기 단계에서의 이를 위한 기관으로서는 정보보호시스템 평가인증 업무를 수행하여온 정부 산하기관인 한국정보보호센터가 적절할 것이다.

또한, 이러한 시험을 위하여 초기 단계에서는 특정 장소에서 시험을 원하는 제품들을 집중시켜 시험을 하겠지만 점차 통신망을 통한 시험이 보편화될 것으로 예상되어 이를 위한 상호운용성 시험망을 구축 운용함이 바람직하다.

그리고, 상호운용성 시험 결과는 적합성 시험 결과의 평가인 인증과는 다소 다르게 다루어 져야 한다. 즉, 상호운용성은 두 제품들간의 상호운용성이 가능함을 보여 주는 것이다. 비록 상호운용 시험 대상의 제품들이 그러한 시험을 실패하였더라도 해당 제품들에 기능상의 문제가 있다는 것이 아니므로 일반 정보통신 제품의 상호운용성 시험과 같이 이들이 시험을 성공적으로 마치었을 경우 상호운용성 시험의 운영 기관에서 상호운용성이 가능한 제품들의 리스트를 공고하는 것이 바람직하다.

V. 결 론

안전성과 신뢰성이 요구되는 사이버 패러다임에서 다양한 형태의 경제사회 활동을 수행하기 위하여 정보보호제품의 활용은 보다 보편화될 것이다. 그리고, 이를 이용하는 이용자는 자신이 처리해야하는 경제사회 활동에서 정보보호 기능을 구현한 제품을 구매하여 이용하려 할 것이다. 더욱이, 이용자의 대부분은 정보보호에 대한 전문 지식의 결여로 정보보호 기능이 표준 또는 규격에 규정된 바와 같이 구현되어 관련 제품들간에 무리 없이 연동되어 사용될 수 있음이 확인된 제품을 선호하게 된다.

본 고에서는 이를 위하여 정보보호 제품의 적합성 시험과 이 결과에 대한 인증에 대하여 미국 등 선진국에서의 적합성 시험 동향을 소개하고 아울러 국내의 현황을 살펴보았다. 특히 국내의 경우는 아직 정보보호제품중 일부 제품에 대한 평가 제도는 시행되고 있으나 적합성시험에 관한 제도와 절차가 아직 준비되고 있지 않은 상태로 분석되었다. 이를 위한 하나의 방안으로 국내의 정보보호 제품에 관한 적합성 시험과 인증 체계를 현재의 국내 기술 및 산업 환경을 미성숙한 초기 단계와 향후의 성숙 단계로 구분하여 각 단계별로 해당 주체들의 기능과 역할을 정리하여 제안하였다.

아울러, 이렇게 적합성시험을 통과한 제품들간의 상호연동성을 보장하기 위한 상호연동성 시험에 대하여도 소개하였다.

참 고 문 헌

[1] Directory of Conformance Testing Programs, Products and Services, http://www.itl.nist.gov/div897/ctg/ctdhome.htm

[2] Hans Blick and Gert Vermeer, "The Way Towards Interoperability", 5th IWPTS, pp 148~152, 1992.

[3] Mission of the Computer Security Division (893), http://www.itl.nist.gov /div893/

[4] JEB(Center for Information Tech nology Standards) Projects, http:// www.itsi.disa.mil/whatshot.html

[5] PKCS Conformance Workshop, http://www.rsasecurity.com/rsalabs/pkcs/workshop/00conformance.html

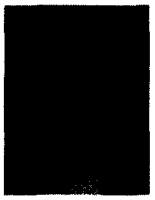
[6] ICSA Security Practitioner Certifications, http://www.trusecure.comhtml/secsol/practitioner.shtml

[7] Virtual Private Network Consortium,http://www.vpnc.org

[8] Information Security Engineering, "Stric Conformance Test", NPL, March 1997

[9] Joint Interoperability Test Command (JITC), http://jitc.fhu.disa.mil/

〈著者紹介〉



장 청 룡 (Chung-ryong Jang)
종신회원

1980년 2월 : 성균관대학교 전자공학과 졸업
1986년 8월 : 연세대학교 대학원 전자공학과 석사
1994년 2월 : 성균관대학교 대학원 정보공학과 박사

1979년 12월~1983년 12월 : 한국전자통신기술연구소(현, ETRI), 연구원
1984년 1월~1997년 1월 : 한국통신 연구개발본부 선임연구원
1997년 3월~현재: 경동대학교 정보보통신공학부 조교수
관심분야 : 보안제품의 시험, 통신망 보호, 블록암호,

김 학 범 (Hakbeom Kim)
종신회원

1990년 8월 : 중앙대학교 전자계산학과 졸업(석사)
2001년 2월 : 아주대학교 컴퓨터공학과 졸업(박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1997년 4월~1998년 12월 : TTA/SC10/SG3(시스템보안 연구반) 간사
2000년 1월~현재: TTA/TC10(정보보호 기술위원회) 간사,
TTA/TC10/시스템보안연구반 의장
1996년 7월~현재: 한국정보보호센터 기술표준팀장
관심분야 : 컴퓨터·네트워크 보안, 접근통제, 정보보호 표준화, 정보보호 관리체계 인증

이 홍 섭 (Hong-Sub Lee)
종신회원

1979년 : 한양대학교 전자공학과 졸업(학사)
1985년 : 한양대학교 전자공학과 졸업(석사)
1999년 : 대전대학교 컴퓨터공학과 졸업(박사)
1980년~1996년 : 한국전자통신연구원, 연구원~책임연구원, 실장
1996년~현재: 한국정보보호센터 기술부장
1996년~현재: 한국통신정보보호학회 상임이사
1997년~현재: 정보통신기술협회 정보보호기술위원회 의장
2000년 : NETSEC-KR 행사 조직위원장
2000년~현재: 전자거래분쟁조정위원회 조정위원(산자부), 금융분쟁조정위원회 조정위원(금감원), 개인정보분쟁조정위원회 조정위원(정통부), 인터넷보안기술포럼 초대의장, 한국ASP인증위원회 인증위원
2001년~현재: 인터넷사이트 안전마크위원회 위원, 대한전자공학회 회지편집위원회 위원, 국가과학기술표준분류전문위원회 위원, 사이버범죄 민간자문위원회 위원(서울지방경찰청)
관심분야 : 정보보호 관리, 정보보호기술 표준화, PKI, 시스템 및 네트워크 보안 등