情 報 保 護 學 會 誌
第23卷 第5號, 2013. 10

국외 평가 인증 체계 현황 분석

최 명 길*, 나 학 연**, 정 재 훈***

요 약

본 연구는 국제 공통평가기준 상호인정협정의 중요성에 대해 소개하고, 적절한 정보보호 평가체계의 대책에 대해 알아보기 위해 국외의 CCRA 표준화 활동에 대해 조사 연구하였다. 미국, 캐나다, 영국, 독일, 일본은 각각 고유의 스킴을 통해 평가인증제도 운영과 관련되어 체계적인 시스템을 마련하고 있으며, 그 효과에 대해 면밀히 검토하여 우리나라에 적용할 수 있는 방안을 모색해보고자 한다.

Ⅰ. 서 론

국제 공통평가기준 상호인정협정(CCRA : common criteria recognition arrangement)은 인터넷 확산과 정보보호 제품 시장의 글로벌화에 따라 미국, 영국, 독일 등 IT 보안 분야의 선진국들이 자국의 제품을 수출하기 위해 수출대상 국가에서 또 다른 평가를 받아야했으므로, 평가에 따른 소요 시간, 인력, 비용을 절약하기 위한 대책 마련 필요성에 의해 생겨나게 되었다.

우리나라도 '06년 5월 CCRA에 가입하여, 국내 제품의 경쟁력을 제고하고, 안전성 검증을 강화하고 있다. CCRA 정책은 우리나라 정보보호에 미치는 영향이 크므로 CCRA 정책을 지속적으로 분석할 필요가 있으며, 많은 관심을 가지고 지속적으로 개선책을 제시할 필요가 있다. 이를 위해서는 정보보호 평가체계의 감독 체계의 확립이 필요하다.

CCRA 정책은 각 나라의 국제공통평가기준(CC: common criteria)으로 인증된 제품을 동일한 수준으로 인정한다는 것을 의미한다. 특히, 정보보호 시스템 사용환경에서 보안 문제를 해결하기 위해서 보안 요구 사항을 국제 공통 평가 기준 내에서 선택하여 작성한 제품 · 시스템별 보안기능 · 보안요구사항을 보호프로파일(PP: protection profile)이라고 한다.

따라서 본 논문에서는 국외 CCRA 국가가 시행하고 있는 인증체계 분석 및 국내 인증체계 발전방안을 제시하고, 특히 CCRA 인증서 발행국의 평가 · 인증 체계를 분석 및 정보보호제품 평가현황을 분석해보고자 한다.

Ⅱ. 미국/캐나다 CCRA 표준화 활동 분석

2.1 미국의 평가 인증 · 체계

미국의 평가 · 인증체계 및 제도를 규정하는 스킴(scheme)은 CCEVS(common criteria evaluation and validation scheme)로 평가 · 인증제도 운영과 관련된 사항을 규정하고 있다. 미국의 평가 · 인증 체계는 [표 1]과 같다. 인증기관은 NSA와 NIST가 공동으로 운영하는 NIAP CCEVS로 정보보호제품평가에 대한 인증 관련 역할을 담당하고 있다. 평가기관으로는 현재 9개의 민간평가기관이 지정되어 운영되고 있다.

NIAP CCEVS는 미국 정부가 정보통신기술에 있어서 정부부문과 민간부문의 긴밀한 협조를 도모하기 위한 노력의 일환으로 NIAP를 설립하게 되는데, NIAP은 평가 및 인증에 대한 새로운 스킴으로서 CCEVS를 제정하였으며, 동 스킴은 평가 기준으로서 CC를 채택하였다. CCEVS는 NIAP에 의해 운영되는 평가·인증제도에 대한 기본지침으로서 인증기관, 평가기관 및 인정기관 설립과 그 역할 및 책임 등에 대해서는 'Scheme

* 중앙대학교 경영학과 교수 (mgchoi@cau.ac.kr)
** ETRI, 부설연구소, 선임연구원 (hyna3800@naver.com)
*** 중앙대학교 일반대학원 경영학과 박사과정 (selpine@naver.com)

〔표 1〕 미국의 평가 · 인증 체계

인증기관	NIAP CCEVS
인정기관	NVLAP
평가기관	· Arca CCTL · atsec information security corporation · Booz Allen Hamilton Common Criteria Testing Laboratory · COACT Inc. CAFE Laboratory · Computer Sciences Corporation · CygnaCom Solutions, Inc · DSD Information Assurance Laboratory · InfoGard Laboratories, Inc · SAIC Common Criteria Testing Laboratory

Publication #1'에서 규정하고 있다. 이에 따라 NIAP 인증기관은 CCEVS의 최종 책임기관으로서 CCEVS의 정책과 절차에 따라 동 제도가 원활하게 운영되어 평가 및 인증제도가 정부 및 민간 모두에게 효율적으로 운영하는 것을 목적으로 하고 있다.

NIAP의 내부규정들은 CC 및 CEM에 근거한 민간기관의 평가와, 이에 대한 NIAP 산하의 인증기관(validation body)의 인증을 중심내용으로 하고 있다.

NIAP 인증기관은 평가 및 인증제도, 즉 CCEVS의 책임주체로서 CCEVS의 내용을 정하고 이를 집행하며, 평가기관에 대한 감독 및 지원을 행하며, NVLAP에 의해 인정된 평가기관을 승인하는 역할을 담당하고 있다. 인증기관의 역할은 구체적으로 다음과 같으며, 이러한 업무를 수행하기 위하여 필요한 전문기술 및 능력을 가지고 평가기관 및 신청자에 대해 기술적으로 지원할 수 있어야 한다.

(1) CCEVS의 운영에 관한 정책과 절차의 수립
(2) CCEVS 규정에 따른 정책과 절차의 운용 및 공중에 대한 정보공개의 보장
(3) CCEVS에 참여하고자 하는 평가기관(CCTL)의 승인
(4) 평가기관(CCTL)의 업무수행, 특히 평가기준(CC) 및 평가방법(CEM)의 해석, 적용, 준수 여부에 대한 감독

평가기관은 인정기관인 NVLAP(NIST's voluntary laboratory accreditation program)에 의해 인정을 받고 인증기관의 승인을 얻어야 한다. 이렇게 승인을 얻은 평가기관을 CCTL(common criteria testing laboratory)라 한다. 평가기관에 관한 규정은 다음과 같다.

2.1.1 평가기관의 설립

정보보호시스템에 대한 평가기관은 상업적 시험연구소로서, CCEVS상의 평가기관(CCTL)으로 역할을 하기 위해서는 NVLAP의 인정을 얻고, NIAP 인증기관의 승인을 얻어 승인된 시험소의 명단에 등록이 되어야 한다. 평가기관의 조직 및 운영에 대해서는 ISO/IEC Guide 25의 내용을 포함하고 있는 NIST Handbook 150 및 NIST Handbook 150-20의 규정을 준수해야 하며, 이에 대한 준수여부에 대해 인정기관의 인증 및 인증기관의 승인을 얻어야 한다.

2.1.2 평가기관의 역할 및 책임

평가기관은 평가 신청인과의 계약을 통해 IT제품 및 PP에 대한 평가업무를 수행하며 반드시 NIAP의 승인을 얻은 평가기준(CC) 및 평가방법(CEM)을 통해 평가를 행해야 한다. 또한, 평가의 수행은 반드시 CCEVS에서 규정하는 절차를 준수해야 한다.

평가는 공정해고 투명해야 하며 상업적 비밀을 보장할 수 있어야 한다. 특히 상업적 비밀과 관련하여 평가기관은 IT제품 및 PP의 중요정보 등을 보호하기 위한 정책 및 절차를 강구해야 하며, 이에 대해서 NIAP 인증기관의 감사를 받는다.

평가기관이나 평가기관의 직원의 특정 평가결과에 대해 이해관계를 가져서는 안되며, 자신이 개발한 제품이나 평가에 관한 컨설팅을 행한 제품에 대한 평가에 참여할 수 없다. 이에 따라 평가기관은 자신이 평가하는 제품에 대해 이해관계를 가지지 않는다는 사실을 보장할 수 있는 방안을 강구해야 한다.

NIAP 인증기관과 NVLAP는 평가의 공정성을 해칠 수 있는 평가기관의 이해관계가 발생하거나 발생할 가능성이 있는 경우 이를 중재해야 할 책임이 있다.

CCEVS의 평가기관에서 탈퇴를 하고자 하는 자는 탈퇴하기 30일 전까지 인증기관에 대해 그 사실을 통보해야 한다.

2.1.3 CCEVS 기술동향

2008년 9월에 Publication #1~5가 V2.0으로 개정되

〔표 2〕 미국 CCEVS

구분	주요내용
Publication #1	· CCEVS – Organization, Managment and Concept of Operations
Publication #2	· CCEVS – Quality Manual and Standard Operating Procedures
Publication #3	· CCEVS – Guidance to Validators
Publication #4	· CCEVS - Guidance to CCEVS Approved Common Criteria Testing Laboratories
Publication #5	· CCEVS - Guidance to Sponsors
Publication #6	· CCEVS – Assurance Continuity: Guidance for Maintenance and Re-evaliation

었으며, 최신 평가 인증 현안의 반영 및 불필요한 내용들에 대한 삭제 등이 이루어졌다.

2008년 9월에 Publication #6 보증 연속성(보증유지 및 재평가에 대한 지침 V2.0)에 대한 내용을 신규로 등재하였다.

또한, 2008년 3월에 Validation Oversight Review (VOR) Evaluators and Validators Guide 2.0이 등재되었으며, 이 문서에는 초기, 시험, 최종 인증보고서 작성 관련 평가자/인증자 행동 및 각 인증보고서에 포함되어야 하는 항목에 대한 지침을 제공하고 있다.

〔표 3〕 미국 인증보고서 구성

구분	주요내용
IVOR (Inital VOR)	· ST 평가결과에 대한 검토
TVOR (Test VOR)	· 개발(ADV) 및 시험(ATE) 평가결과에 대한 검토
FVOR (Final VOR)	· 최종 평가결과(ETR)에 대한 최종 검토

2.2 캐나다의 평가 인증 · 체계

캐나다는 CC제도에 대하여 문서로 정의하고 EAL5 이상 등급 평가방법에 대해서도 자국의 평가방법론을 규정하고 있다. [표 4]와 같이 인증기관은 CSE 이며 인정기관은 SCC 이다. 평가기관은 현재 공공 평가기관과 민간 평가기관을 모두 합하여 총 4개의 평가기관이 지정되어 운영되고 있다.

〔표 4〕 캐나다의 평가 · 인증 체계

인증기관	CSE
인정기관	SCC
평가기관	· CGI Information Systems · Management Consultants Inc · DOMUS IT Security Laboratory · EWA-Canada

캐나다의 스킴은 CCS(canadian common criteria evaluation and certification scheme)로 2005년 이후 변경사항이 없다.

〔표 5〕 캐나다의 CCS

구분	주요내용
CCS Guide #1	· Scheme Description
CCS Guide #2	· Quality Manual
CCS Guide #3	· Evaluation Facility Approval
CCS Guide #4	· Technical Oversight for TOE Evaluation
CCS Guide #5	· Technical Oversight for PP Evaluation
CCS Guide #6	· Technical Oversight for Assurance Continuity of a Certified TOE

캐나다는 암호기능성 평가조건, CC 평가 대상이 되는 암호 알고리즘 식별, 인증기관, 평가기관 역할 정의 등을 기술한 CCS Instruction #4 암호 기능성 평가 및 인증 지시서가 2008년 7월에 등재되었다.

Ⅲ. 유럽 CCRA 표준화 활동 분석

3.1 영국의 평가 인증 · 체계

영국은 미국과 함께 평가 제도를 먼저 도입한 국가이다. 영국은 인증기관인 CESG(communications electronic security group)에서 평가 · 인증제도 운영과 관련된 사항을 규정하고 있으며, 민간 평가 기관들을 승인하기 위하여 UKAS(UK accreditation service)라는 인정기관을 두고 있다.

영국은 공공 평가기관과 민간 평가기관을 모두 합하여 [표 6]과 같이 현재 4개의 평가기관을 보유하고 있다. 미국과 유사하게 유럽의 평가 제도를 선도하는 국가로 정보보호제품 평가에 대한 관심이 많은 나라 중 하나이다.

〔표 6〕 영국의 평가·인증 체계

인증기관	CESG
인정기관	UKAS
평가기관	· BT · EDS · Logica · SiVenture

영국의 평가기관에 의한 평가는 평가대상의 보안목표(ST)에 대한 평가와 함께 제품 개발환경 등에 대한 평가도 함께 이루어지게 된다. 영국의 평가 및 인증제도의 주체인 CESG는 평가를 진행하는 과정에 있어 모든 평가절차를 총괄 할 수 있는 프로젝트 관리자(project manager)를 선임할 것을 권고하고 있다. 평가기관에 의해 행해지는 구체적인 평가의 내용은 다음과 같다.

(1) 평가대상의 보안목표에 대한 평가
(2) 시스템의 정확성에 대한 평가
(3) 보안성에 대한 시험
(4) 제품 개발환경에 대한 평가
(5) 제품의 사용환경에 대한 평가
(6) 예상되는 취약점에 대한 확인
(7) 침투 시험(penetration testing)
(8) 포괄적인 평가보고서의 작성

인정기관인 UKAS는 비영리민간조직으로, 통산성과의 양해각서(memorandum of understanding) 체결을 통하여 인정업무에 관한 유일한 정부기관으로 인정받고 있으며, 통산성으로 부터 일정한 지원 및 감독을 받고 있다.

평가기관은 인정기관인 UKAS에 의해 인정받은 기관을 의미하며, 인증기관인 CESG에 의해 감독을 받게 된다.

영국의 스킴은 UK Scheme(UKSP)로 2008년 10월 용어 명확화 등 경미한 내용에 대한 개정을 수행하였다.

〔표 7〕 영국의 UK Scheme (UKSP)

구분	주요내용
UKSP00	· Abbreviations and References
UKSP01	· Description of the scheme
UKSP02	· CLEF Requirements Part I – Start Up and Operation · CLEF Requirements Part II – Conduct of an Evaluation
UKSP03	· Sponsor's Guide (Role of Sponsor in IT Security Evaliation and Cetification)

3.2 독일의 평가 인증·체계

독일도 영국과 같이 스킴 문서에 평가 및 인증제도 운영과 관련된 사항을 규정하고 있다. [표 8]과 같이 독일의 인증기관은 정부기관인 BSI이며 인정기관은 DAR이다. 독일은 현재 CCRA CAP국 중 평가기관이 17개로 가장 많은 나라이다. 독일에서는 EAL5 이상의 고등급 평가·인증을 받은 경우 인증서가 이중으로 발행이 되는 경우가 있다. 이는 평가·인증 받은 정보보호제품의 수출입을 장려하기 위한 방안으로, CCRA 가입국들 간에 상호인정하지 않는 EAL5 이상 등급의 제품에 대하여 EAL4 등급의 인증서를 이중으로 발행하

〔표 8〕 독일의 평가·인증 체계

인증기관	BSI
인정기관	DAR
평가기관	· atsec information security GmbH · Brightsight BV · CSC Deutschland Solutions GmbH · T-Systems GEI GmbH · datenschutz nord GmbH · DFKI · SRC Security Research & Consulting GmbH · Tele-Consulting security / networking / training GmbH · IABG(Industriean lagen-Betriebsgesellschaft mbH · TUV Information Technology GmbH · Atos Origin GmbH · media transfer AG · Secunet Security Networks AG · secunet SwissIT AG · CETECOM ICT Services GmbH · Fraunhofer Institut für Angewandte · Optik und Feinmechanik

는 것이다. 상호인정하지 않는 고등급 평가는 각국의 평가방법론에 따라 평가를 진행하고 있으나, 공통평가방법론인 CEM을 기반으로 평가를 수행하므로 독일에서 EAL5 등급의 평가·인증에 대하여 EAL4 등급의 인증서를 발행하는 것이다. 이로 인해 다른 나라들에 비해 EAL5 이상의 고등급 평가·인증이 가장 많이 이루어지고 있으며, 독일정부가 고등급 평가에 대한 기술을 확보하고 있음을 알 수 있다.

독일의 BSI는 독일연방 내무성 산하 기관이지만 정보사회에서의 IT보안에 관련하여 독립적이고 중립적인 기관이며 유럽국가와 달리 유일한 정부기관이라는 특징이 있다. BSI는 IT보안의 확보를 위하여를 다음과 같은 내용을 주요업무로 하고 있다.

(1) IT기술의 적용과정에서의 보안위험요소의 조사, 보안예방방안의 발전과 IT보안을 위한 장비 등의 발전업무 및 연방의 과제수행을 위해서 필요한 사항
(2) IT시스템과 IT관련 제품의 보안성 시험 및 평가를 위한 기준, 절차 및 장비의 발전
(3) IT시스템과 IT관련 제품의 보안성 시험 및 평가 및 보안인증서의 교부
(4) 연방 또는 연방의 용역에 의해서 이루어지는 사기업이 생산하는 행정상 비밀유지를 요하는 정보 및 그의 전달을 위해서 사용되어 질 암호화장비 등의 IT 시스템과 제품에 대한 허가
(5) 연방의 IT보안과 관련한 자문 및 통제에 관한 지원
(6) 경찰 및 형사사법기관에 대한 지원 및 테러관련 감시정보 또는 정보기관의 정보 분석과 평가에 관련한 지원
(7) IT 관련 생산, 판매 및 적용자에 대한 자문

BSI는 크게 4국으로 조직되어 각 국에 따라 그 업무를 달리하는 데 BSI의 일반 행정을 담당하는 행정사무국 과 다른 3개국으로 구성되어있다.

DAR은 독일국가인정기관으로서 독일 내 인정 업무에 관여하는 모든 기관의 활동을 조율하고 인정등록부를 관리한다. 이 기관은 독일연방경제부, 독일연방 노동부, 독일표준화기구(DIN) 등의 지원을 받는다.

Ⅳ. 일본 CCRA 표준화 활동 분석

4.1 일본의 평가 인증 · 체계

일본은 1998년부터 CC 평가·인증을 수행하였으며, [표 9]과 같이 인증기관은 IPA, 인정기관은 NITE이며 현재 3개의 평가기관이 운영되고 있다.

〔표 9〕 일본의 평가 · 인증 체계

인증기관	IPA
인정기관	NITE
평가기관	· ITSC · ECSEC · Mizuho Information & Research Institute

일본의 경제산업성은 '독립행정법 제품평가 기술기반 기구(NITE)'에 평가·인증사업을 위탁하여 2001년 4월부터 '정보보호시스템의 평가·인증제도'를 실시하고 있다. NITE가 법률의 위임을 받아 제정한 평가 및 인증제도의 지침의 경우도 CCRA의 요구사항을 반영하고 있으며, 이에 따라 인증기관, 평가기관 및 인정기관의 설립과 운영도 CCRA의 요건을 준수하도록 규정하고 있다.

일본은 정보화 및 정보보호전문기관인 정보처리추진기구(IPA)가 인증 기관, 경제산업성의 위탁을 받은 NITE가 인정기관으로서 역할을 하며, 평가기관은 민간이 담당한다.

민간 평가기관의 경우는, NITE에 의해 설립된 인정기관인 IA Japan(international accreditation japan)에 의해 심사 및 인정을 받고 인증기관(NITE)의 승인을 얻어야 한다. 아울러 인증기관인 IPA는 평가기관에 대한 기술지도와 감독의 의무가 부과된다.

Ⅴ. 국내 CC 인증 제도의 발전 방향

CC 인증은 제품의 보안성과 안전성을 검증받는 절차이나, 그동안 제품에 대한 보안성과 안전성에 대한 검증이라기 보단 공공기관의 사업에 참여하기 위한 하나의 방편으로 인식되어 왔다. 특히, 2009년 5월 이후에는 보안 적합성 검증이 사후검증으로 변화되면서 이러한 현상이 가속되어 왔다. 이러한 문제점을 해결해기 위해

그동안 국내의 CC인증은 변경 승인 절차의 간소화, EAL2 평가자의 간소화, 제출문의 간소화, 평가 수수료 할인등으로 진입장벽을 낮추고, 보안성 강화, CC 버전의 호환성 강화로 경쟁력을 가질 수 있도록 개선되어 왔다.

그러나, 다른 CCRA 발행국과 비교를 해본 결과, 국내의 CC 인증은 인증 제품의 수가 상대적으로 부족하며, 고등급의 인증에만 치우쳤다는 것을 알 수 있다. 이는, 일부 조건에 맞는 기업만이 CC인증에 참여하였다는 것을 알 수 있으며, 낮은 등급의 인증이 전무한 것으로 보아, 일정 수준이 안 되는 정보보안 제품은 아예 인증조차 시도 하지 않았다는 것을 의미한다. 이는 국내 CC인증의 높은 장벽을 의미하며, 결국 자본력이 있는 CC인증을 획득할 여력이 되는 업체만 CC 인증을 받게 된다는 것을 말한다. 이런 현상에 대한 해결책으로 CC 인증의 간소화, 수수료 할인등의 진입장벽을 낮춰야 하며, 특히 낮은 등급의 인증을 더욱 활성화 시킬 필요가 있다. 모든 정보보호관련 제품에 CC인증을 받도록 유도하여 국내의 정보보호제품의 경쟁력을 강화하고 안전성과 신뢰성을 보증하는 것이 중요하다. 공공기관과 일반기업이 안심하고 제품을 도입하여 사용할 수 있도록 지속적으로 상호보완적인 제도로서의 발전방향을 모색해가야 한다.

특히, IT보안인증사무국은 CCRA 인증서발행국으로서의 위상 제고를 위해 평가·인증제도를 국제수준에 맞도록 개선해 나아가야 한다. 향후에도 지속적으로 신종 정보보호제품에 대한 보호프로파일을 지속적으로 개발·배급하여 민간업체에서 제품 개발시 이를 참조, 국가 정보통신망 보호에 적합하고 국제적으로도 경쟁력 있는 제품을 개발할 수 있도록 유도·지원하여야 한다.

Ⅵ. 결 론

CC 기반의 평가·인증 제도를 사용하고 있는 국가들은 서로의 평가·인증 결과를 상호 인정해주기 위해서 공통평가기준 상호인정협약(CCRA)를 맺고 있다. 본 연구에서는 CCRA 발행국(CAP)간의 표준화 활동 분석을 통해 우리나라의 CC 인증의 발전 방향을 모색하였으며, 국내외 CC인증의 분석을 통해 개선 방향을 도출해내었다.

국제공통평가기준(CC)은 모든 정보보호시스템 유형을 포괄할 수 있는 보안 요구사항을 제시한 평가기준으로 정보보호시스템 보안요구사항의 집결체이다. 특히, 국내외에서 CC인증은 활발히 인증되고 있으며, 인증제품의 수는 시간이 지날수록 증가하고 있다. 정보보호시스템 사용환경에서 보안 문제를 서술하고 이를 해결하기 위한 보안요구사항을 국제공통평가기준에서 선택하여 평가기준으로 작성되는 보호프로파일의 분석은 필수라고 볼 수 있다.

본 연구는 특히 NIAP CCEVS가 제공하는 미국의 국가정보보증획득정책(national information assurance acquisition policy)에서 국내의 인증체계에서 이끌어내야 할 시사점을 도출한다. 향후 연구에서는 국외 CC 평가/인증의 프레임에 대하여 면밀한 분석이 필요할 것이다.

참고문헌

[1] *KISA, IT 보안성 평가인증 안내서, 2009년 12월*

[2] *BSI, http://www.bsi.de*

[3] *CC Portal, http://www.commoncriteriaportal.org*

[4] *Common Criteria for Information Technology Security Evaluation, CC v3.1. Release 3, 2009. 7*

[5] *Common Methodology for Information Technology Security Evaluation, CEM v3.1. Release 3, 2009. 7*

[6] *CCRA management committee, 'Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security', 2000. 5*

[7] *CESG, http://www.cesg.gov.uk*

[8] *CSEC, http://www.cse-cst.gc.ca*

[9] *DSD, http://www.dsd.gov.au/*

[10] *IPA, http://www.ipa.go.jp*

[11] *NIAP CCEVS, http://www.niap-ccevs.org*

〈著者紹介〉

최 명 길 (Myeonggil Choi)
종신회원

2004년 9월: 한국과학기술원 박사
1995년 9월~2000년 1월: 국방 과학연구소 연구원
2000년 2월~2005년 8월: 한국 전자통신연구원 선임연구원
2005년 9월~2008년 2월: 인제대학교 조교수
2008년 3월~현재: 중앙대학교 부교수
<관심분야> 보안성 평가, 정보보호정책 및 관리

나 학 연 (Hacyun Na)
장회원

1999년 2월: 숭실대학교 컴퓨터학부 학사
2001년 2월: 숭실대학교 대학원 소프트웨어공학 석사
2008년 9월: 충남대학교 컴퓨터공학 박사 수료
2000년 11월~현재: ETRI부설국가보안기술연구소 재직
<관심분야> 정보보호기술 및 취약성 평가, CC인증

정 재 훈 (Jaehun Jeong)
학생회원

2009년 2월: 인제대학교 시스템경영공학과 졸업
2011년 2월: 중앙대학교 경영학과 석사 졸업
2011년 3월~현재: 중앙대학교 경영학과 박사과정
<관심분야> 정보보호정책 준수, 거버넌스