情 報 保 護 學 會 誌
第 13 券 第 2 號, 2003. 4

국외 정보보호 자격제도에 대한 현황 및 분석

나 현 미*, 한 호 현**, 김 종 배***

요 약

본 연구에서는 국제적으로 통용되고 있는 정보보호 자격에 대하여 운영기관, 응시자격, 검정방법, 시험과목, 합격결정기준, 합격률, 합격자수에 대하여 상세히 분석한다. 정보보호 분야의 국제통용 자격으로 CISSP, SSCP, CISA, ISO17799/BS7799, GIAC, CBCP, CIA 등 7개의 자격에 대한 분석을 통하여 국외 정보보호 자격의 추세와 흐름을 고찰한다.

Ⅰ. 서 론

21세기 지식정보화사회로의 진입은 사회 전 분야에서 정보기술이 핵심 기반이 되어 있는 등 새로운 패러다임을 형성하고 있다. 특히 우리 나라는 세계 최초로 전 가구수의 70%가 초고속 인터넷망에 연결되고 2,600만명의 국민이 인터넷을 이용하는 등 명실상부한 세계 최고 수준의 정보통신 인프라를 갖추고 있다. 이렇듯 우리 나라의 정보화가 국가 전반에 크게 확산된 반면 그 이면에는 정보화의 부산물로 컴퓨터바이러스, 해킹, 개인정보 침해 등 정보화 역기능이 증가하고 있다. 정보화 역기능을 극복하는 여러 가지 방법으로 정보보호에 대한 인식의 제고 및 관련 분야에 대한 기술개발과 투자가 확대되어야 한다.

정보보호산업은 전자적 침해로부터 정보 주권을 지키는 정보사회의 방위산업으로 〔표 1〕에 제시한 것처럼 다른 IT 산업 분야에 비해 약 2.5배 이상의 고성장을 기록할 것으로 전망되는 미래의 유망·전략산업이다.

세계 정보보호 시장규모는 〔표 2〕에서와 같이 연평균 28.8% 성장하여 2007년에는 766억달러로 약

〔표 1〕 정보보호산업과 다른 IT 산업의 성장률(2001~2007) 비교

구 분	정보통신산업	소프트웨어산업	정보보호산업
세 계	11.7%	16.3%	28.8%
국 내	19.5%	26.8%	36.2%

※ 자료 : 한국전자통신연구원(2002)

〔표 2〕 세계 정보보호시장 전망 (단위 : 백만달러)

분 류	2001	2002	2003	2004	2005	2006	2007	연평균성장률
제 품	8,533	11,181	14,785	19,217	24,606	32,582	43,222	30.8%
서비스	5,739	7,152	8,869	11,341	14,085	17,361	21,402	24.5%
기 타	2,532	3,285	4,270	5,554	7,118	9,230	11,968	29.5%
합 계	16,804	21,618	27,924	36,112	45,809	59,173	76,592	28.8%

※ 자료 : 한국전자통신연구원(2002)

* 한국직업능력개발원 e-Learning센터
** C&C엔터프라이즈(주)(rhhan@cncen.com)
*** (주)이엔터프라이즈(kjb@eenterprise.co.kr)

〔표 3〕 국내 정보보호시장 전망 (단위 : 억원)

분 류	2001	2002	2003	2004	2005	2006	2007	연평균 성장률
제 품	3,530	4,721	7,003	9,772	13,254	17,178	21,887	35.5%
서비스	191	275	450	610	911	1,241	1,685	43.8%
기 타	34	56	110	195	280	320	365	48.5%
합 계	3,755	5,052	7,563	10,577	14,445	18,739	23,937	36.2%

※ 자료 : 한국정보보호산업협회(2002)

4.6배 성장할 전망이다.

국내 정보보호시장도 〔표 3〕에 제시한 것과 같이 연평균 성장률 36.2%로 2007년 2조 4천억원 수준으로 6.4배 성장이 예상된다.

이와 같이 정보보호산업의 급성장과 더불어 인력 수요는 급증하고 있으나, 필요한 인력 공급이 제대로 이루어지지 못해 향후 인력수급 불균형 현상이 심화될 전망이다.

정보보호 전문 인력 양성은 대학 및 대학원 등의 정규 교육기관과 교육훈련기관을 통해 이루어지거나 자격 제도를 통한 전문 인력을 양성할 수 있다. 현재까지 국내의 정보보호 자격제도는 활발하게 운영되고 있지 않은 상태에서 외국의 자격제도인 CISSP와 CISA 자격 등이 주요 정보보호 자격제도로 인식되고 있다. 특히 '1.25 인터넷 대란' 이후 정보통신부는 정보보호 강화 대책의 방안으로 정보보호에 대한 투자확대 및 정보보호 자격의 활성화를 통해 인력 양성 방안을 추진하고 있다. 이러한 시점에서 국외 정보보호 자격에 대한 체계적이고 정확한 고찰을 통해 그 시사점을 살펴보는 것은 국내 정보보호 자격 제도의 도입 및 활성화에 주는 의미가 매우 크다고 할 수 있다.

Ⅱ. 국외 정보보호 자격제도

정보보호 분야의 국외 자격은 정보보호 산업을 주도하고 있는 미국을 중심으로 영국 및 국제표준 자격 등이 있다. 현재 우리 나라는 정보통신기반보호법에서 정보보호 기술 인력을 초급, 중급, 고급 인력으로 나누어 제시하고 있으며 이를 분류하는 기준으로 학력과 정보보호 분야의 자격취득으로 규정하고 있다. 그러나 우리 나라는 정보보호 관련 국가자격이 없으므로 국외자격인 CISSP와 CISA자격 취득자를 고급 기술 인력으로 인정하고 있다. 이와 같이 정보보호 분야의 자격은 이미 국내에서 통용되고 있으므로 정보보호 분야에 대한 국외 자격제도의 고찰은 매우 필요하다고 하겠다.

1. CISSP

CISSP(Certified Information System Security Professional)는 정보보호 전문가 자격에 관심 있는 국제 조직들이 1988년에 컨소시엄 형태로 설립한 국제정보시스템보안자격협회((ISC)^2 : International Information Systems Security Certification Consortium)에서 운영하는 자격이다.

CISSP 자격 취득을 위한 응시 자격은 정보 시스템 보안과 연관된 지식과 기술을 요구하는 보안업무 종사자, 보안 감시자, 보안 컨설턴트, 보안 제공업자, 컴퓨터 범죄수사관, 보안제품 개발자 등 실제로 보안과 관련하여 정규직원으로 만 3년 이상 근무한 경력자만 시험에 응시할 수 있다. 보안 관련 경력은 CBK(Common Body of Knowledge)의 10개 영역에서 근무한 경력을 모두 합하여 3년 이상이 되어야 응시할 수 있으며, CISSP에 응시하기 위해서는 (ISC)^{2}의 직업윤리 강령을 준수하여야 한다. (ISC)^{2}가 인증한 모든 보안 전문가들은 CISSP 자격을 취득하기 위해 시험과 자격심사를 통과해야 하며 CISSP 응시료는 450$이다.

CISSP 검정 방법은 사지선다형으로 250문항이 출제지만, 그 중 25문제는 다음 시험을 위한 테스트 시험이므로 점수에는 반영되지 않는다. 시험 시간은 6시간이 소요되며, 시험은 영문으로만 가능하다. 필기 시험 검정 내용은 (ISC)^{2}가 제공하는 CBK의 10개의 영역에서 무순위로 출제된다. 10개의 영역은 다음과 같다.

1.1 접근 제어 시스템 및 방법론

접근 통제는 정보의 특정 항목이나 사용자의 신분 및 다양하게 미리 정의된 그룹의 권한에 근거하여 특정 기능에 대한 시스템의 접근을 제한 및 통제, 감시하는 메커니즘을 말한다. 이는 시스템 관리자들이

가용성, 무결성, 비밀성을 위해 시스템의 행위 및 사용, 내용에 대해 감독 및 금지 권한을 행할 수 있도록 한다. 이 영역에서는 다음 사항을 다룬다.

- 책임 추적성(Accountability)
- 접근 제어 기술/관리/모델(Access Control Techniques /Administration/Model)
- 식별 & 인증 기술(Identification & Authentication Techniques)
- 접근 제어 방법론 & 구현(Access Control methodologies & Implementation)
- 파일 & 데이터 소유권 & 관리인의 임무(File & Data Ownership & Custodianship)
- 공격의 도구(Methods of Attack)
- 감시(Monitering)
- 침입 테스트(Penetration Testing)

1.2 통신망 및 네트워크 보안

통신 및 네트워크 보안 영역은 사설 및 공개 네트워크를 통한 전송에 무결성, 가용성, 인증, 비밀성을 제공하기 위한 구조, 전송 방법, 전송 형식, 보안 대책을 다룬다.

- ISO/OSI Layers & Characteristics
- 통신 네트워크 보안
- Internet/Intranet/Extranet
- Firewalls, Routers, Switches, Gateways, Proxies
- 프로토콜, 서비스, 보안 기술
- 메일/FAX 보안
- 안전한 음성 통신
- 네트워크 공격 & 대책

1.3 보안 관리

보안 관리는 조직의 정보 자산 및 비밀성, 무결성, 가용성을 보증하는 정책, 기준, 절차, 지침의 개발 및 문서화, 이행을 포함한다. 데이터 분류 및 위험 진단, 위험 분석 등의 관리도구들을 사용하여 위협을 정의하고, 자산을 분류하며, 취약성을 평가하여 효과적인 보안 통제를 구축할 수 있다.

- 보안 관리 개념 & 원칙
- 변경 제어/관리
- 데이터 분류
- 정책, 표준, 가이드라인 과 절차
- 권한, 책임, 교육, 보안 관리 계획

1.4 응용 프로그램 및 시스템 개발

응용프로그램 및 시스템 개발 보안은 시스템 및 응용 소프트웨어와 그 개발 단계에 대한 통제를 말한다. 응용프로그램은 분산 또는 집중 환경에서 사용되는 에이전트 및 애플릿, 소프트웨어, 데이터베이스, 데이터 창고, 지식기반 시스템 등을 말한다.

- 응용 프로그램 이슈
- 데이터베이스 & DW
- 데이터/정보 저장소
- 지식 기반 시스템
- 시스템 개발 제어
- 악의적인 코드(Malicious Code)
- 공격의 도구

1.5 암호

암호 영역은 정보의 무결성, 비밀성, 인증을 보증하기 위한 이론 및 수단, 방법을 말한다.

- 암호의 사용
- 암호의 개념, 방법론과 훈련
- 개인키 알고리즘
- 공개키 알고리즘
- PKI
- 암호의 기능 구현을 위한 시스템 구조
- 공격의 도구

1.6 보안 아키텍쳐 및 모델

보안 아키텍처와 모델 영역은 다양한 수준의 비밀성, 무결성, 가용성을 부여하기 위해 운영체제, 장비, 네트워크, 어플리케이션과 그 통제를 설계·구축하고, 감시 및 보안하기 위한 개념 및 이론, 구조, 기준을 포함하고 있다.

- 컴퓨터와 네트워크 조직, 구조와 설계의 원칙
- 보안 모델(BLP 등), 구조(IPSEC 등), 검증 조건(ITSEC 등)의 원칙
- 시스템 구조와 설계와 관련된 보안 이슈와 흐름

1.7 컴퓨터 운용 보안

운영 보안은 하드웨어, 미디어, 운영자에 대한 모든 자원에의 접근 권한에 대한 통제를 정의한다.

- 관리자 관리(Administrative management)
- 개념(Concepts)
- 제어 타입(Cntrol Types)
- 운영 제어(Operation Controls)
- 자원 보호(Resource protection)
- 감사(Auditing) /모니터링(Monitoring)
- 모니터링 도구와 기술(Monitoring tools and techniques)
- 침입 탐지(Intrusion Detection)
- 침투 테스트 기술(Penetrating testing techniques)
- 위협과 대책(Threat and countermeasures)

1.8 사업 연속 계획 및 비상 복구 계획

사업 연속 계획과 재해 복구 계획 영역은 정상 사업 운영의 중대한 중단에 대처하여 사업을 보전하기 위한 특정 활동에 대한 준비를 말한다. 이는 자연적이거나 인위적인 사건과 즉시 또는 효과적으로 수행되지 않았을 때의 결과를 다룬다.

- BCP/DRP
- 비즈니스 연속 계획 요소(Element of business continuity planning)
- BCP/DRP 이벤트

1.9 법 · 수사 및 윤리

법과 수사, 윤리 영역은 컴퓨터 범죄의 법과 규정을 말한다. 범죄가 일어났는지에 대한 판단, 증거가 있다면 수집 방법을 결정하기 위한 조사 방법 및 기술, 보안 전문가를 위한 규약을 제공하는 윤리적 제약을 다룬다.

- 법
- 법의 주요 분류와 형태
- 심사(Investigation)
- 컴퓨터 범죄의 주요 분류
- 윤리

1.10 물리적 보안

물리적 보안은 기업의 자원 및 중요한 정보를 물리적으로 보호하는데 사용되는 위협 및 취약성, 대응책을 말한다. 이러한 자원에는 인원, 그 안에서 작업이 일어나는 설비, 데이터, 그리고 장비, 지원 시스템, 미디어, 이들이 이용하는 공급품들을 포함한다.

- 시설 요구사항
- 기술 제어
- 환경(Environment)/라이프(Life) 안전성
- 물리적 보안 위협과 요소

CISSP 필기 시험은 응시생 전체 평균의 70%이상의 득점 시 합격한다. 즉 시험 응시생들의 전체 평균이 90점인 경우, 63점 이상이면 합격하게 된다. 불합격하여 재시험을 보게되는 경우, 최소 3 개월간은 재 응시할 수 없다. 최근 CISSP는 시험과목이 지나치게 광범위하고 출제문제가 최근의 기술발전 추세를 제대로 반영하지 못하고 있다는 지적과 함께 현실적으로 실무능력 배양에 큰 도움을 주지 못한다는 비판이 제기되면서 2002년 6월 1일부터 자격 검증에 대한 제도가 신설되었다. 또한 2003년부터는 경력 기준을 강화하여 검증을 할 예정이다.

현재까지 알려진 CISSP 자격의 평균합격률은 30%정도이며, 2002년 8월까지 전 세계 33개국에서 활동하고 있는 $(ISC)^2$에 등록한 CISSP 자격 취득자는 6,839명으로 추산된다. 국내에는 1995년 첫 CISSP 취득자를 필두로 현재 약 107명의 CISSP 합격자가 있다.

CISSP 자격을 유지하기 위해서는 자격증 취득 후 매 3년간 120시간 상당의 재교육을 실시하는데, 재교육 정도에 따라 전문적 활동의 영역이 달라진다. 만일 120시간의 재교육을 받지 못할 경우, 3년마다 재시험을 통과하여야 한다. 또한 자격증을 취득한 후에도 3년마다 재심사를 받아야만 자격증의 효력이 유지된다. 재교육 기준도 $(ISC)^2$에서 제시하는 CPE(Conrivuing Professional Education) 기준을 120 지수 이상 달성해야 하는 등 매우 까다롭다.

2. SSCP

SSCP(Systems Security Certified Practitioner)는 CISSP와 같은 국제정보시스템보안자격협회($(ISC)^2$: International Information Systems

Security Certification Consortium)에서 2000년 11월에 처음 검정을 시행한 자격이다. SSCP는 정보보안 정책, 표준, 절차를 개발하고 도구를 경영하는 역할을 담당하는 IT 전문가에게 주어지는 CISSP 자격증과는 달리, 방대한 하드웨어와 소프트웨어 프로그램 상의 정책, 표준, 절차들을 구성하는 네트워크 및 시스템 관리자를 양성하는 자격제도이다. SSCP 응시 자격은 7개 도메인과 관련한 1개 이상의 분야에서 1년간의 경력자이며 응시 전에 $(ISC)^2$ 윤리 강령을 준수하여야 한다. SSCP 자격 취득을 위한 응시료는 295$이다.

필기 시험 검정 방법은 사지선다형 방식으로 125문제가 출제되며, 시험 소요 시간은 3시간이다. SSCP의 시험 과목은 7개의 도메인(CBK : Common Body of Knowledge)에서 출제된다. 도메인은 업무를 수행하기 위해 필요한 조건, 실질적 업무, 원칙, 과정 및 개념 등으로 이루어져 있다. CISSP의 10개의 도메인과는 3개의 도메인이 다르며 나머지는 CISSP와 유사하다.

2.1 접근 통제

사용자가 할 수 있는 것, 그들이 접근할 수 있는 자원, 그리고 그들이 수행할 수 있는 작동들을 특화시키기 위하여 시스템 경영을 가능하게 해 주는 메커니즘을 다룬다.

- 최소 권한의 규칙
- 이행하는 최소 권한
- 다중 요소 인증(Multi-facter Authentication)
- proactive access control
- AC & Privacy Issues
- 시스템 책임 추적성(System Accountability)
- 접근 통제 모델(DAC/MAC/formal Models)
- ACL(Access Control Lists)
- 물리적 접근 통제(Physical Access Control)
- SSO(Single Sign On)
- Kerboros/RSA

2.2 관리

조직의 정보 자산에 관한 문서, 통합, 유용성 등을 정립, 층화, 보강하는데 필요한 보안 원칙, 정책, 표준, 절차 등을 포함한다. 역할, 의무, 통합 경영, 변화 통제, 보안 경고, 승인된 산업 업무의 적용 등에 대하여 다룬다.

- 보안 관리 원칙
- 인증
- 어플리케이션 시스템 전개(Application System Development)
- 프로그램/데이터 공격
- 가능한 취약점
- 운영 모델
- 통제, 변경 통제/관리
- 보안 통제 구조(Security Control Architecture)
- 하드웨어 세그먼테이션(Segmentation)
- 데이터 보호 메카니즘
- 데이터 분류
- 직원 정책 & 이행(직무 분리/교육)
- 보안 관리 계획
- 악의적인 공격

2.3 심사와 모니터링

심사는 시스템이 승인된 산업 절차와 특수한 조직화 정책, 표준, 절차 등에 따라 작동되는 시스템 하에서 결정하는 능력과 모니터링은 보안 사고, 취약성에 관하여 정립, 계층화, 우선 사항을 결정하고, 반응·보고할 수 있는 기제, 도구, 설비 등을 포함하여 다룬다.

- 보안 감사
- 침입 탐지
- 침입 테스트(Penetration Testing)
- Sniffing
- Radiation Monitoring
- Dumpster Diving
- Social Engineering

2.4 위험, 반응 및 복구

위험 분석, 응급 조치, 재해 복구, 사업 연속성 유지 등의 역할 및 시스템 취약성에 관한 평가, 안전성에 관한 선택과 평가, 복구 계획과 절차 평가 등을 포함하며, 예방, 증거 저장, 기억장치를 포함하고 위험 처리 등을 다룬다.

- 위험 관리 도표
- Cyclical/교육/분석/테스트
- 검증/위협
- 위험 완화/분석, 위험 평가
- DR(Disater Recovery)/DRP

- BCP(Business Continuty Planning)

2.5 암호

통합성, 기밀성, 신빙성 등을 보강하기 위하여 정보를 가공하는데 사용되는 방법, 원칙, 수단 등을 다룬다.

- 암호의 사용
- 암호의 개념, 방법론 과 훈련
- 개인키 알고리듬
- 공개키 알고리듬
- PKI
- 암호의 기능 구현을 위한 시스템 구조
- 공격의 도구

2.6 데이터 통신

통신의 경로 사이의 데이터 변환을 위한 통합성, 가용성, 신빙성, 기밀성 등을 제공하는 구조, 전달 방법, 전달 경로 및 보안 방법 등을 다룬다.

- OSI 모델
- 네트워크 하드웨어 식별
- LAN Topologies
- Protocols, Routing
- IP 어드레스 스키마
- 방화벽 구조(Firewall Architecture)
- 통신 보안 이슈

2.7 악성 코드

시스템이나 네트워크 정보의 적합한 작동을 감염시키고, 오용하거나 강요하는 프로그램, 적용, 코드 구획 등을 해결하기 위한 원칙, 수단, 방법 등을 다룬다.

- 악성 코드(Malicious Code)
- 컴퓨터 바이러스/이메일 바이러스
- Salami Attacks
- 컴퓨터 Trojans/Worms

2002년 11월까지 전 세계에서 활동하고 있는 $(ISC)^2$에 등록한 SSCP 자격증 취득자는 106명으로 추산되며, 국내에는 SSCP합격자가 아직까지는 없다. SSCP 자격을 유지하기 위해서는 자격을 취득한 후, 매 3년에 한 번씩 CPE(Continuing Professional Education)를 이수하여야 한다.

3. CISA

CISA(Certified Information Systems Auditor)는 정보시스템감사통제협회(ISACA : Information Systems Audit & Control Association), 정보시스템감사통제재단(ISACF : Information Systems Audit & Control Foundation)에서 운영하고 있다.

CISA 시험에 응시하는데 특별한 자격 제한은 없다. 정보 시스템 감사, 통제 및 보호 분야에서 최소한 5년의 경력이 있어야 한다. 이러한 경력은 다음의 경력으로 대체할 수도 있다.

첫째, 1년 이상의 정보 시스템 운영, 프로그래밍 경력 또는 회계감사 경력은 정보 시스템 감사·통제·보안 경력 1년으로 인정

둘째, 전문대학 또는 대졸 학력은 각각 1년 또는 2년의 정보 시스템 감사·통제·보안 경력으로 인정

셋째, 전산과학, 회계, 정보처리 감사 등의 관련 분야에서의 대학 전임강사 이상의 경력은 매 2년 당 정보 시스템 감사, 통제, 보안 경력 1년으로 대체될 수 있다.

CISA 자격(증) 신청은 시험 합격 후 5년 이내에 해야 하며, 경력은 자격 신청일 기준으로 과거 10년 이내 또는 최초 시험의 합격일로부터 5년 이내의 경력이어야 한다. CISA 시험은 사지 선다형 방식으로 200문항이 출제되며, 시험 소요시간은 4시간이다. CISA시험은 별도의 과목이 지정되어 있지 않으며, 다음과 같은 1 프로세스(process)+6 컨텐츠(contents) 영역으로 구성되며 괄호안의 퍼센트는 시험 문제 출제 구성비이다.

3.1 프로세스 영역

(1) IS 감사 프로세스(10%)

조직의 정보기술과 사업 시스템이 적절하게 통제되고, 모니터 되고 평가되는 것을 보증하기 위하여 일반적으로 받아들여지는 IS 감사 기준 및 지침에 대하여 평가한다.

3.2 내용 영역

(1) IS(Information Security)의 관리, 계획 및

조직(11%)
IS의 관리, 계획 및 조직을 위한 전략, 정책, 표준, 절차 및 관련된 실무에 대하여 평가한다.

(2) 기술 인프라와 운영 실무(13%)
조직의 사업목적이 적절하게 지원됨을 보증하기 위하여 조직의 기술 및 운영 인프라의 구현, 수행중인 관리의 효과성과 효율성에 대하여 평가한다.

(3) 정보자산의 보호(25%)
정보자산을 허가받지 않고 사용하거나, 노출시키고, 변경함에 따른 피해 및 손실로부터 보호하기 위한 논리적, 환경적 IT 인프라의 보안에 대하여 평가한다.

(4) 재해 복구 및 사업 연속성(10%)
재해 발생시 사업 운영 및 IS 프로세스의 지속을 위한 계획의 개발과 유지 프로세스에 대하여 평가한다.

(5) 사업 응용 시스템 개발, 취득, 구현 및 유지(16%)
사업 응용 시스템 개발, 취득, 구현 및 유지가 조직의 사업 목표 충족을 보장하기 위하여 이에 사용된 방법론 및 프로세스에 대하여 평가한다.

(6) 사업 프로세스 평가와 위험 관리(15%)
조직의 사업 목표에 상응하여 위험이 관리됨을 보장하기 위하여 사업 시스템과 프로세스에 대하여 평가한다.

시험 문제는 총 200문항이며 해당 연도 응시생의 성적을 기준으로 최저 25부터 최고 99의 스케일 비율로 측정하여 75점 이상이 되어야 합격이 된다.

2002년 현재까지 CISA시험 합격자는 총 1739명이며, 전 세계적으로는 18,000여명이 활동하고 있다. CISA 자격을 유지하기 위해서는 매년 최소 20시간, 3년간 최소 120시간 이상의 계속교육(CPE : Continuing Professional Education)이 요구되고 있다. CPE는 ISACA의 CISA 자격취득자들이 자격을 계속 유지하기 위하여 매년 감사 통제 분야에서 활동한 결과를 인정받아야 한다. CPE 시간은 국내외 교육을 받는 방법 외에도 논문, 출판, 강연, 협회 활동에 참여 등 다양한 방법이 있다.

4. ISO 17799/BS7799 심사원

ISO 17799/BS7799 심사원은 BS7799에 기술한 정보보안 표준 규정에 근거하여 업무 및 서비스 활동을 지원하는 통신 및 컴퓨터 시스템을 각종 재해와 위험으로부터 보호하여 가용성을 높이고, 이를 통하여 처리되는 정보의 유실 또는 불법적 사용을 방지하고자 하는 역할을 수행한다. BSI(The British Standards Institution)는 1901년 영국의 국가규격을 작성 보급하기 위해 설립된 국가표준 제정 발행기관으로 1929년 영국 황실로부터 비영리 국가단체로 허가를 받아 우리 나라의 국가기술표준원과 한국표준협회 두 기관의 역할을 모두 수행하는 조직이다.

ISO 17799/BS7799 심사원은 별도의 응시자격 및 제한은 없으며, 특정 분야의 기술 및 경험이 중시되는 직무이므로 해당 교육과 평가 및 심사 경험 과정을 통과하면 자격을 부여한다.

ISO 17799/BS7799 심사원은 예비 심사원(provisional auditor) → 심사원(auditor) → 선임 심사원(lead auditor)의 세 단계로 나뉘어진다.

심사원의 첫 단계는 5일 과정의 교육을 받고, 이에 관하여 평가를 실시함으로써 예비 심사원이 되고, 둘째 단계로 심사 경험을 기준으로 평가하여 심사원이 되며, 마지막으로 심사의 제반 모든 사항을 경험하는 것으로 선임 심사원 자격을 획득하게 된다.

예비 심사원이 되기 위한 교육과정의 내용은 다음과 같다.

(1) 정보보안 개념
(2) 정보보안 경영 시스템
(3) ISO 17799 : 2000 (2002년 현재 BS7799 Part 1에서 명칭 변경됨)
- ISO 자격인정 획득
- 참조 문서로 사용할 수 있음
- 보안 관리에 대한 포괄적인 세트 제공
- 현재 사용중인 최상의 정보보안 실행 지침
- 10개의 부분으로 구성
- 심사 및 인증으로의 사용은 불가

(4) BS7799 Part 2 : 2002
- 정보보안 관리 시스템 문서화 수립 실행에 대한 요구사항 규정
- 개별 조직의 필요성에 따라 실행될 수 있는 보안 관리 요건을 규정

(5) 정보보안의 사례 연구
(6) 위험성 평가 및 관리
(7) 정보보안기술
(8) 소프트웨어 제품 및 시스템 평가
(9) 심사기술

교육과정을 통한 평가는 관련 내용을 설명, 실행 실습, 사례 연구, 역할 연기, 시험 평가 등을 통해 수행된다. 교육과정 중에 이루어지는 지속적인 평가에서는 과정 참여와 팀 활동, 필기시험, 태도 및 개별적인 기여도, 참석율 및 시간 관념, 역할 연기, 언어구사 능력, 1일 평가 등에 관하여 평가한다. 교육과정 이수 후 실시하는 평가에서 필기시험 100점 만점에 70점 이상, 1일 지속평가 16점 만점에 10점 이상, 사례 연구 20점 만점에 13점 이상을 획득하게 되면 합격하여만 예비 심사원 자격을 획득하게 된다. 국내에서 2000년에는 24명, 2001년에는 70명, 2002년에는 40명이 합격하였다.

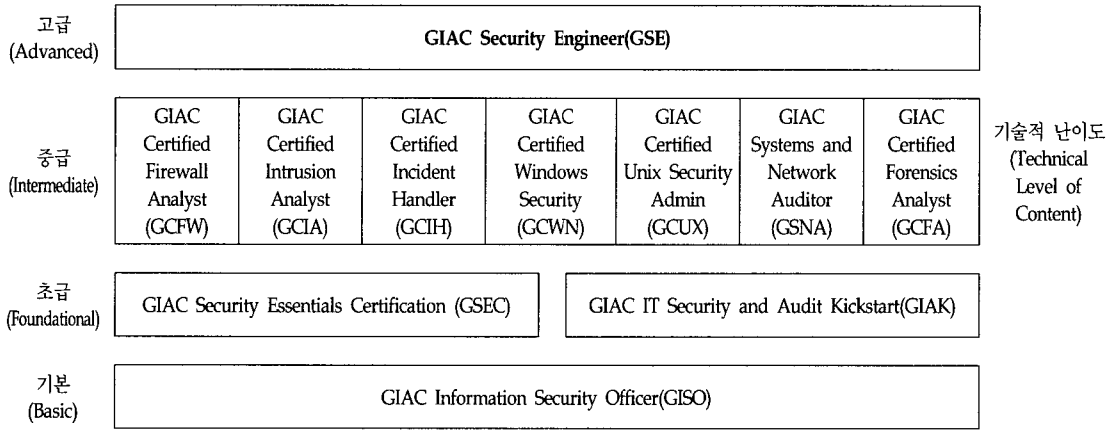
5. GIAC

GIAC(Global Information Assurance Certifications)은 2000년 2월에 정보시스템 공급자로부터 중립적이고 독립적인 보안 자격증으로 시작하였다. GIAC 자격을 운영하고 있는 SANS(SysAdmin, Audit, Network, Security)는 1989년 미국에 설립된 연구·교육훈련 조직이다. GIAC 자격을 취득하기 위한 응시대상에 대하여서 특별히 자격을 제한하고 있지는 않지만 정보보안의 실제 경험과 이에 대한 지식과 기술에 대한 것으로 검정 내용이 구성되어 진다.

GIAC 자격은 11개의 개별적인 자격증이 존재하며 응시자들은 현업이나 자신의 경력과 연관된 자격증을 취득할 수 있다. 기본 자격(GISO)과 10개의 초급·중급·고급 자격으로 이루어 졌으며 이들 자격 가운데 5개 이상 과정의 자격증을 취득하면 최상의 고급 자격증인 GSE(GIAC Security Engineer)를 응시할 수 있다. [그림 1]은 GIAC의 11개의 자격에 대한 자격체계를 나타내고 있다.

GIAC 자격은 인터넷을 이용한 온라인으로 자격검정을 시행하므로 별도의 자격검정 일자를 지정하고 있지 않다. 다만 자격을 취득하기 위해서는 인터넷으로 자격 검정을 신청하고 응시료를 지불하면 등록이 된다. GIAC 자격은 다음과 같은 6단계의 절차를 통해 취득하게 된다.

(1) 1단계 - 등록
자격증 취득을 위한 응시료를 지불하고 등록한다
(2) 2단계 - GIAC계정 취득
ID(user name)와 비밀번호(password)를 교부받는다.
(3) 3단계 - 코스 과정 이수
SANS의 자격증 관련코스 과정을 이수를 희망하는 경우 온라인이나 컨퍼런스(미국 정부관련 컨퍼런스, 국제 컨퍼런스, 지역별 컨퍼런스등), 온라인 교육(25명 이상인 경우 방문교육), 그룹 라이센싱(온라인 과정을 20명 이상 구매한 경우), 각 나라별 인증된 멘토 프로그램 등을 이용하여 학습 과정에 참여할 수 있다.
자격증에 따라 코스과정이 필수적인 것도 있다. 온라인 자료나 실제 문제와 유사한 퀴즈도 선택적으로 이용할 수 있다. 일부 과정은 수업에서 다루지 않은 보충 자료도 온라인에서 구할 수 있다. GSEC, GCFW, GCIA, GCIH, GCUX는 SANS의 교육을 꼭 이수하지 않아도 개인적으로 이와 관련한 공부를 하고 시험에 응시할 수 있다.



[그림 1] GIAC자격체계

(4) 4단계 - 논문 작성 및 제출
계정 취득 후 5개월 이내 논문 시험을 치루어야 한다. 논문은 필드의 경험을 바탕으로 한 실제적인 연구물이어야 하며 논문 작성시 표절은 절대 허용되지 않는다.
(5) 5단계 - 시험
필기 시험은 GIAC 웹사이트를 통해 온라인으로 시행된다. 자격증에 따라 한 과목 혹은 두 과목의 시험을 치른다.
(6) 6단계 - 합격 통보
시험 합격 여부에 관한 통보를 받으며 인증서를 받게 된다. 논문 점수와 이름 등이 웹사이트에 기록된다.

GIAC 자격은 먼저 제출한 논문에 대한 평가를 받아야 하는데 논문주제의 분석에 대한 정확성, 간결성, 완성도, 보안 방어기술에 실질적인 기여도 등을 평가하여 100점을 만점으로 하여 점수가 매겨지며 합격, 불합격, 우수 등으로 구분된다. 논문 점수가 70점 이상 되어야 합격되며 90점 이상인 경우는 우수로 분류된다. 우수에 대한 평가는 SANS 자문위원회를 통해 이루어지며 90점 이상이 아니더라도 실질적인 업무와 연관한 공헌도 등을 평가하여 우수논문으로 분류한다. 논문 시험이 통과되면 온라인 필기 시험을 치를 수 있다. 모든 시험은 사지 선다형 객관식으로 75문제이며 2시간 동안 진행된다. 몇몇 다른 시험은 3시간 동안 90문항이 출제되며 오픈 북(open book)으로 진행된다. 시험 합격 점수는 70점 이상이다. 시험은 GIAC 계정 발생 후 6개월 이내 마쳐야 한다.

GIAC자격이 시행된 2000년 첫해에 1,000여명이 자격증을 취득하였으며 2002년 3월까지 3,000여명이 자격증을 취득하였고 2002년 12월 3일까지 4,170명의 합격자가 있다. 우리나라에는 2명의 GCIH 자격취득자가 있다. GIAC의 개별적인 모든 자격증은 정기적으로 재 시험에 응시하여 합격하여야만 자격이 갱신된다.

6. CBCP

CBCP(Certified Business Continuity Professional)는 미국의 비영리 기관인 DRI International(Disaster Recovery Institute International)에서 재난복구 전문가 양성교육 및 인증을 주된 목적으로 운영하고 있다. CBCP 자격은 각종 재해 발생시 비즈니스 연속성을 유지하기 위한 방법론으로 9·11 미국 테러사건 이후 크게 주목받기 시작했다. BCP는 재해·재난으로 인해 정상적인 운용이 어려운 시스템의 복구, 데이터 백업, 원상회복 같은 단순복구 뿐 아니라 고객 서비스의 지속성 보장, 고객신뢰도 유지, 핵심 업무기능 지속 등을 위한 환경을 조성해 기업의 가치를 최대화하는 방법론을 자격의 검정 내용으로 구성되어 있다. 즉, 관리적, 기술적, 물리적(환경적)인 요소에서 발생하는 사고 또는 비상사태로 인하여 사업상의 일부 요소 또는 전체 체계가 마비되어 원활한 사업 지속에 장애가 발생하는 것에 대비하기 위해, 이를 사전에 분석하고, 이에 대한 예방(Prevention), 억제(Deterrent), 탐지(Detect), 복구(Recovery), 재개(Resumption)와 관련된 관리적, 기술적, 물리적 체계를 구축하는 일련의 과정을 의미한다. 따라서 CBCP의 대상은 단순히 전산 시스템에 한정되는 것이 아니라, IT 인프라, 정보자원, 임직원, 건물 등 사업수행과 관련된 모든 요소가 그 대상이 된다 .

CBCP자격을 취득하기 위한 응시자격은 사업 연속성 또는 재난복구 관련 분야로 다음에 열거된 10개 분야중에서 3개 이상의 분야에 대해서 2년 이상의 실무경험을 가진 자를 대상으로 한다.

(1) 프로젝트 관리(project initiation and management)
(2) 위험평가 및 통제(risk evaluation and control)
(3) 사업 영향력 분석(business impact analysis)
(4) 사업 연속성 전략 개발(developing business continuity strategies)
(5) 비상대책 수립(emergency response and operations)
(6) 사업 연속성 개발과 구현(developing and implementing business continuity plans)
(7) 교육훈련 프로그램(awareness and training programs)
(8) 사업연속성 계획의 연습과 관리(maintaining and exercising business continuity plans)
(9) 공공관계 및 위기 통신(public relations and crisis communication)
(10) 공공기관과의 협조(coordination with public authorities)

자격 검정은 상기의 응시자격을 충족하는 자에 대하여 교육이수와 시험통과를 통해서 이루어진다. CBCP 자격을 취득하기 위하여서는 시험에서 75점 이상을 획득해야 하며 점수는 총점으로 계산된다. 시험 분야(domain)별로 과락이 존재하지는 않으며, 시험 분야별로 응시하거나 합격이 인정되지 않는다. 국내에서는 2002년에 처음으로 시행되었으며 50명이 지원하여 2명이 합격하였다. 전 세계적으로 1988년부터 2,500여명의 합격자가 있다.

CBCP 자격을 유지하기 위하여서는 2년 동안 80점의 교육훈련 점수를 누적하여야 한다. 첫해 30점은 재난관리에 관한 직무를 수행하여 점수를 취득하여야 하며 10점은 전문적인 지식과 기술을 배양하기 위한 교육훈련을 통하여 취득하여야 한다. CBCP 자격을 유지하기 위해서는 매달 일정금액을 DRII에 납부하도록 되어 있다.

7. CIA

CIA(Certified Internal Auditor)는 국제 내부 감사인 협회(IIA :The Institute of Internal Auditors)에서 공인하는 내부감사사 전문 자격증을 말한다. 국제 내부 감사인 협회(IIA) 주관으로 1974년부터 시행되고 있는 CIA는 외부감사업무를 수행하는 CPA와 더불어 감사분야의 대표적인 자격증이다. 현재 35,000명 이상의 CIA 자격 취득자가 전 세계에서 기업의 내부감사 전문가로 활동하고 있으며 국내에는 현재 약 20명 정도가 자격증을 보유하고 있다.

CIA 자격취득을 위한 응시 자격은 4년제 대학 졸업자 및 졸업예정자(4학년)면 경력에 관계없이 누구나 응시가능 하다. 응시자는 IIA에서 정한 서식에 따라 소속기관장, 매니저, 학술인 및 CIA 자격을 취득자와 같은 책임 있는 사람으로부터 추천서를 받아야 한다. 실무경력(Professional experience)에 대하여 응시자는 24개월 간의 내부감사 혹은 동등한 경력(품질보증, 회계감사, IS 감사, 준법감시, 내부 통제 등)을 갖고 있어야 한다. 석사학위보유자, 회계/법무/재무 경력자는 1년의 직무경력으로 인정된다. 직무경력증명서(IIA 양식)는 응시원서와 함께 송부하거나 합격 후 송부할 수 있다. 즉, 응시 시점에서는 실무경력은 없어도 무방하다.

CIA 검정 방법은 4과목이며, 사지선다형으로 각 과목당 80문항이 출제된다. 시험 시간은 각 과목당 210분이 주어진다. 시험 언어는 영어, 불어, 스페인어 중 선택한다. 응시자는 4과목을 모두 치를 수도 있고, 유효기간(3년)안에 능력에 맞게 선택해서 시험을 칠 수 있다. 시험 과목은 4개의 Part로 구분된다.

(1) Part I 내부 감사자 프로세스(Internal auditing Process)
내부 감사 이론과 실무를 측정한다. 감사(Auditiong), 전문적인 감사실무(Professionalism), 부정(Fraud) 적발 등이 해당된다.

(2) Part II 내부 감사 기술(Internal Audit Skills)
사고력, 의사소통 기법, 피감사인을 다루는 능력에 대한 기술을 측정한다. 감사 성적의 평가와 문제 해결법, 데이터 수집·문서화와 보고, 샘플링과 수학능력 등이 해당된다.

(3) Part III 경영관리와 정보 기술(Management Control and Information Technology)
내부 감사 실무에 필수적으로 기본이 되는 경영 분야를 측정한다. 경영관리(Management Control), 운영관리(Operations Management), 정보기술(Information Technology)이 해당된다.

(4) Part IV 감사환경(The Audit Environment)
재무회계와 재무, 경영, 내부 감사 실무와 관련 있는 법과 제도 분야를 측정한다. 재무회계(Finacil Accounting), 재무(Finance), 관리회계(Management Accounting), 법적 환경(Regulatory Environment)이 해당된다. 이 부분은 CISA나 AICPA 소지자가 응시시 시험이 면제된다.

합격 결정 기준은 응시자가 한 과목만 응시할 수도 있고, 4과목 모두 한꺼번에 응시할 수도 있으므로 과목별 부분 합격이 인정된다. 각 Part 별 600점(750점 만점)이상이 되어야 합격이며, 불합격된 Part는 재응시가 가능하다. CISA와 AICPA 합격자는 파트 IV 응시가 면제된다. CIA 자격을 유지하기 위하여서는 시험을 합격한 후 3년 이내 2년 감사업무를 수행한 경력이 필요하며 이를 증명하지 못할 경우에는 자격이 취소된다. 2002년 5월까지 전 세계적으로 CIA 자격증 취득자는 35,000여명으로 추산되며, 국내에는 25명의 합격자가 있다.

Ⅲ. 국제 통용 자격에 대한 비교

정보보호분야의 7개의 국제 통용 자격들에 대하여 살펴보았던 내용을 표로 정리하면 다음 〔표 4〕와 같다. GIAC 자격의 경우 다른 6개의 내용 및 운영이 매우 다르므로 〔표 5〕에 제시하고 있다.

정보보호 분야의 국외 자격들을 비교하면 다음과 같은 몇 가지의 공통점들이 발견된다.

첫째, 자격의 운영기관에 대한 것이다.

모든 국외 정보보호 자격은 비영리 단체에서 운영이 되고 있다. CISSP와 SSCP는 $(ISC)^2$, CISA는 ISACA에서 운영하고 있으며 ISO 17799/BS7799 심사원은 BSI, GIAC는 SANS, CBCP는 DRI International, CIA는 IIA에서 운영되고 있다. 이들 자격운영 기관은 해당 분야의 전문가들로 조직이 구성되어 자격운영 기관에 대한 공신력을 인정받고 있다. 또한 영리를 목적으로 하는 기관이나 단체가 아니므로 자격운영 기관으로서의 공정성과 투명성을 갖추고 있음을 알 수 있다.

둘째, 자격 응시 대상을 정보보호 관련 분야의 경험을 전제조건으로 하고 있음을 알 수 있다.

응시대상에 대한 명확한 규정을 제시하여 반드시 해당 분야에서 업무를 수행하는 사람에게만 응시 기회를 부여하고 있다. 이러한 점은 GIAC의 경우 해당 분야를 매우 구체적이고 세분화하여 제시하고 있으며 CISSP의 경우에는 응시 대상에 대한 규제를 더욱 강화하여 자격을 취득한 사람들에 대한 검증을 실시하기도 한다. 그러나 CISA의 경우는 응시대상을 제한을 두고 있지는 않지만 시험을 합격한 후 5년 이내에 관련 업무 경험을 객관적으로 인정 받아야하며, 경력은 자격 신청일 기준으로 과거 10년 이내 또는 최초 시험의 합격일로부터 5년 이내 획득하여야 한다.

세째, 시험 문제의 유형이 대부분 객관식으로 이

〔표 4〕 국제 통용 자격 제도 비교표

자격명	응시자격	운영기관	시험과목(교육내용)	문항수	제한시간	출제방법	합격결정 기준	자격유지
CISSP	· 보안과 관련하여 정규직원으로 3년 이상 근무한 경력자 · 직업윤리강령에 서명	$(ISC)^2$	$(ISC)^2$가 제공하는 CBK의 10개의 도메인에서 무순으로 출제 ①접근제어시스템 및 방법론 ②통신망 및 네트워크보안 ③보안관리 ④응용프로그램 및 시스템 개발 ⑤암호학 ⑥보안 아키텍처 및 모델 ⑦컴퓨터 운용 보안 ⑧사업연속계획 및 비상복구계획 ⑨법·수사 및 윤리 물리적 보안 ⑩물리적 보안	250문항	6시간	사지선다	70% 이상 득점	3년간 120시간의 재교육
SSCP	· 관련분야 1년이상 경력 · 직업윤리강령에 동의		$(ISC)^2$가 제공하는 CBK의 7개의 도메인에서 무순으로 출제 ① 접근통제 ② 관리 ③ 심사, 모니터링 ④ 위험, 반응 및 복구 ⑤ 암호학 ⑥ 데이터 커뮤니케이션 ⑦ 악성코드	125문항	3시간	사지선다	70% 이상 득점	3년간 120시간의 재교육
CISA	제한없음	ISCA	· 정보시스템 감사 기준 및 실무, 정보시스템 보안, 통제 실무 · 정보시스템 조직과 관리 · 정보시스템 운영 · 정보보안 소프트웨어 개발, 구입, 유지보수 · 정보시스템 무결성, 기밀성, 가용성	200 문항	4 시간	사지 선다	75% 이상 득점시 합격	3년간 120시간의 재교육

〔표 4〕 국제 통용 자격 제도 비교표(계속)

BS7799 심사원	BSI	제한없음	· 정보보안개념 · 정보보안 경영시스템 · ISO 17799 · BS7799 Part 2 : 2002 · 정보보안의 Best Practice · 위험성 평가 및 관리 · 정보보안 기술 · 소프트웨어 제품 및 시스템 평가 · 심사기술				· 필기시험 100점 만점, 70점 이상 · 일일지속평가 16점 만점, 10점 이상 · 사례연구 20점 만점, 13점 이상	심사업무수행 실적에 따라서 예비심사원, 심사원, 선임사사원의 자격취득
CIA	IIA	· 학사학위 또는 이와 동등한 학위 소지자 · IIA에 정한 서식에 따라 소속기관장, 매니저, 학술인 및 CIA와 같은 책임있는 사람으로부터의 추천서 · 24개월간의 내부감사 혹은 동등한 경력	Part 4로 구분하며, 각 과목은 객과목 80문항이 출제 Part I. 내부 감사자 프로세스 (Internal auditing Process) Paer II. 내부 감사 기술 (Internal Audit Skills) Part III 경영관리와 정보 기술 (Management Control and Information Technology) Part IV. 감사환경(The Audit Environment)	각 과목당 80문항	각 과목당 210분	사지선다	과목당 75점 이상 득점	3년이내 2년 동안의 감사업무경력필요
CBCP	DRI	· 사업의 연속성 또는 재난복구 관련 2년 이상의 실무경험을 가진 자	① 프로젝트 착수와 관리 ② 위험평가와 통제 ③ 비즈니스 영향 평가 ④ 사업 연속성 전략 개발 ⑤ 비상사태 처리와 대처 ⑥ 사업 연속성 개발과 구현 ⑦ 교육훈련 프로그램 ⑧ 사업연속성 계획의 연습과 관리 ⑨ 위기발생시 언론 통제 ⑩ 공공기관과의 협조	200문항	3시간 30분	사지선다형	75점 이상을 획득	2년동안80점의점수필요

루어져 있다.

ISO1779/BS7799 심사원을 제외한 자격들의 시험은 사지선다형으로 출제되고 있다. GIAC의 경우도 1차 논문을 통과한 사람에게 온라인 필기시험을 치도록 하고 있으며 사지선다형 객관식으로 시행된다. CISSP, SSCP, CIA, CBCP 등은 모두 사지선다형 객관식으로 문제가 출제된다. 또한 객관식 시험문항의 개수는 75문항에서 320문항으로 구성되어 있으며 GIAC 자격의 2차 시험인 경우 11개의 각 자격별로 75문항에서 90문항까지 제출이 되며 CISSP는 250문항, SSCP는 125문항, CISA는 200문항, CIA는 문항 수 가 가장 많게 320 문항이 출제되고 있어서 시험을 치르는 시간도 이틀에 걸쳐 이루어지고 있으며 CBCP는 200문항이 출제되고 있다.

네째, 합격결정 기준이 유사하다.

앞에서 살펴본 대부분의 국제 통용 자격들의 합격결정 기준은 득점기준 70% 혹은 70점 이상을 받아야 합격을 할 수 있다. CISSP와 SSCP는 전체에서 70% 이상 득점을 하여야 하며 CISA는 75% 이상을 CIA는 네 개의 파트에서 각각 75점 이상 득점하여야 하고 CBCP는 전체에서 75점 이상을 획득하여야 한다. GIAC도 필기 시험은 70점 이상을 득점하여야만 한다.

다섯째, 자격을 유지하기 위하여서는 지속적인 교육 및 관련 분야 경력을 쌓아야 한다.

CISSP와 SSCP, CISA는 3년간 최소 120시간 이상의 계속 교육을 받아야 하며 CIA는 3년 이내 2년 동안 감사업무 경력이 없으면 자격이 취소된다. CBCP는 2년 동안 80학점을 취득하여야 하고 ISO1779/BS7799 심사원은 심사업무의 수행한 경력에

〔표 5〕 GIAC 자격 제도

자격명	운영 기관	등급	자격의 유지	응시 대상	검정내용	문항수	제한시간	출제 방법	합격결정기준	자격 유지
GSEC	SANS	초급 · 중급	2년	시스템, 네트웍관리자, 기술적 보안관련자, 보안 관리자, 보안직군, 보안관련 폭 넓은 지식을 갖으려 하는 기술직 관련 종사자	보안 실제 경험을 내용을 조직내에 통합하고 실질적인 보안 지식과 스킬을 테스트함	75문항 ~ 90문항	3시간	1차: 논문	논문 점수와 2차 필기도 70점 이상	재시험을 통하여 자격갱신
GCFW		중급	4년	전체적인 네트워크, 디자인 및 라우터, 방화벽, VPN/원격접근 장치와 같은 보안 장비를 구축, 설계, 구성, 모니터링하는 기술직	라우터, 방화벽, 과 같은 보안 경계 장비를 구성, 설계, 모니터하는 능력과 지식을 테스트함			2차사지선다형		
GCIA		중급 · 고급	4년	침임탐지 시스템, 네트워크, 호스트 모니터링, 트래픽 분석 관련 종사자	침입탐지시스템의 구성, 모니터능력 및 관련 로그 파일과 네트워크 트래픽을 분석, 해석 능력을 테스트 함					
GCIH		중급	2년	재난 사고 취급과 관련한 종사자, 효과적인 보안 대책수립자와 현재 시스템과 네트워크의 위협책임자	사고를 관리 능력, 공격 기법과 툴에 대한 이해, 공격에 대한 방어 관리능력을 테스트함					
GCWN		중급	2년	Windows XP, 2000, NT 시스템의 설치 및 구성과 서비스, 네트웍 관련 종사자	IIS와 인증 서비스를 포함한 추가 서비스 기능, 윈도우 시스템의 감사 기능을 테스트함					
GCUX		중급	2년	UNIX, Linux시스템의 설치, 구성 및 모니터 능력을 테스트함	UNIX와 Linux시스템의 보안 및 감사하는 지식과 능력을 테스트 함					
GISO-Basic		초급	2년	보안 관련 사무 관리직	정보 보안의 전체적인 이해, 위협/위험 및 best practice와 관련한 기본 지식, 보안 원리 기술적인 개념의 기본 이해도를 테스트함					
GSNA		중급	2년	정보시스템 보안,감사 기술직	기본적인 위험 분석 기술과 주요 정보 시스템의 기술 감사를 수행하는 방법을 테스트함					
GCFA	SANS	고급	4년	Forensic 조사자/분석가, 고급 사고 취급자 및 일반 사고 조사자	고급 사고 처리 시나리오 취급 방법, 사고 조사 수행방법, 네트워크와 호스트의 포렌직 조사 수행 방법을 테스트함	75문항 ~ 90문항	3시간	1차 논문	논문점수와 2차 필기모두70점 이상	재시험을 통하여 자격갱신
GCFA	SANS	고급	4년	Forensic 조사자/분석가, 고급 사고 취급자 및 일반 사고 조사자	고급 사고 처리 시나리오 취급 방법, 사고 조사 수행방법, 네트워크와 호스트의 포렌직 조사 수행 방법을 테스트함	75문항 ~ 90문항	3시간	1차논문	논문점수와 2차 필기모두70점 이상	재시험을 통하여 자격갱신

〔표 5〕 GIAC 자격 제도(계속)

GCFA	SANS	고급	4년	Forensic 조사자/분석가, 고급 사고 취급자 및 일반 사고 조사자	고급 사고 처리 시나리오 취급 방법, 사고 조사 수행방법, 네트워크와 호스트의 포렌직 조사 수행 방법을 테스트함	75문항 ~ 90문항	3시간	1차논문	논문점수와 2차 필기모두70점 이상	재시험을 통하여 자격갱신
GSLC		초급	2년	정보 보안직을 관리하는 관리자 및 감독자	현재 보안 관련 이슈, 모범사례 및 기술 관련 필수 지식을 테스트함			2차사지선다		
GSE		고급	N/A	5개 중급 자격증(GCFW, GCIA, GCIH, GCWN, GCUX)의 자격증을 취득하고 적어도 한 자격증에서 우수성적을 득한 개인	1시간의 기술 프리젠테이션 선다형 시험 장비 실습 시험 논술, 단답형 시험 cyber와 관련된 논문 및 간행물등 경력심사 2003년 하반기에 시행 예정					

따라서 예비심사원, 심사원, 선임심사원의 순으로 자격을 취득할 수 있도록 되어 있다. GIAC의 경우는 11개의 자격마다 자격의 유지기간이 2년~4년까지 다르며 재시험을 거쳐 자격을 갱신하여야 한다.

여섯째, 시험을 치르게 되는 제한 시간은 3시간에서 최장 14시간 동안 진행된다.

SSCP와 GIAC의 시험시간은 3시간이며 CBCP는 3시간 30분, CISA는 4시간의 제한 시간 동안 시험을 치르게 되며 CISSP는 6시간, CIA는 이틀에 걸쳐 하루에 7시간 동안 시험을 치르게 되어 있다.

Ⅳ. 결 론

인터넷이 전 산업 분야에 직접적으로 영향을 미치고 있으며 전자상거래의 확산 및 전자지불 등이 활발히 도입되고 있음에 따라 정보시스템에 대한 보안 관리는 매우 중요해졌다. 이에 따라서 정보시스템에 대한 보안 관리를 담당할 정보보호 인력이 필요하게 되었으며 정보보호 업무를 수행 할 수 있다는 능력의 객관적 증거로서 정보보호 자격이 유용하게 될 것으로 보인다. 앞에서 살펴본 여러 국제 통용 정보보호 자격의 흐름과 자격제도를 분석하여 보면 다음과 같다.

첫째, 정보보호 자격취득자의 수가 매우 빠르게 증가하고 있다는 것으로 알 수 있다.

CISSP 자격의 경우 2002년 8월 기준으로 보면 전 세계적으로 자격 취득자의 수가 6,839명이며 그 중 우리 나라는 107명으로 4,552명의 미국, 442명의 캐나다, 303명의 홍콩, 145명의 싱가폴에 이어 6위를 차지하고 있다. CISSP 자격이 국내에 적극적으로 소개된 것이 불과 2년 정도의 기간임을 감안하여 볼 때 정보보호 자격에 대한 관심과 필요성은 매우 커졌다는 것을 알 수 있다. 이와 같은 사례는 CISA 자격에 대한 취득자의 수에서도 알 수 있는데 1998년 15명 합격자가 1999년에는 85명, 2000년에는 343명의 합격자가 2002년에는 837명의 합격자가 배출되었음을 통하여 정보보호 인력에 대한 필요성은 매우 높음을 알 수 있다.

또한, 정보보호 자격에 대한 관심과 필요성이 높아짐에 따라서 정보보호분야에 대한 새로운 자격이 국내에 소개되고 있음을 알 수 있다. CBCP와 CIA 자격은 최근 도입되어 이들 자격에 대한 인식의 부족으로 인하여 자격 취득자가 많지는 않다. 그러나 이들 자격에 대한 전 세계적인 자격취득자의 수를 감안하여 볼 때 정보보호 자격으로서 통용성과 활용성은 높다고 할 수 있다.

둘째, 국제 통용 자격 응시자 수의 증가에 따른 외화의 유출이 크다.

앞에서 살펴본 국제 통용 자격의 응시료는 모두 자격의 운영기관에 응시료를 납부하여야 만 응시할 수 있다. CISSP는 450$~550$, SSCP는 295$~395$이며, CISA는 415$~465$, GIAC은 250$~425$이다. 국외자격의 평균 합격률을 고려하여 보면 한 해에 자격 응시료로써 국외에 유출되는 금액은 매우 크다

는 것을 알 수 있다. 그러므로 국내 정보보호 자격이 활성화되기 위한 지원이 매우 절실하다고 할 수 있다. 우리 나라는 정보보호 분야에 대한 국가자격이 없으므로 현재 운영되고 있는 민간자격을 활성화하여 이를 국내 정보보호 시장에서 활용이 되도록 정책적 지원이 필요하다. 현재 국내에서 운영하고 있는 민간 자격에 대한 지원은 정보보호의 특성과 앞서 살펴본 국제 통용 자격의 운영기관과 같은 비영리 기관에서 운영되는 자격이어야 할 것이다.

세째, 정보보호 자격의 검정 내용이 변화되고 있음을 알 수 있다.

정보보호 산업과 밀접한 관련을 가지고 있는 정보보호 자격은 산업의 변화에 맞추어 자격 검정의 내용이 바뀌고 있음을 알 수 있다. BS 7799 자격은 국제 표준의 ISO 17799에 맞추어 자격의 명칭과 자격 검정의 내용을 변경하였다. 이러한 자격의 변화는 자격의 통용성을 국제적으로 높이고 현재 정보보호 산업에 맞추어 자격을 운영할 필요에 의한 것이다. CISA 자격 또한 검정 내용이 개정되어 2001년부터 시행이 되고 있다.

SSCP의 자격의 경우에도 기존의 CISSP 자격과 달리 정보보호 관리 자격에 대한 필요성에 의하여 개발이 되었다. 특히 2000년부터 운영된 GIAC 자격은 자격의 단계별로 총 11개의 자격으로 구성되어 구체적인 직무와 연결하여 자격을 취득할 수 있도록 자격을 설계하고 있다. 이와 같은 것으로 볼 때 정보보호 직무와 자격의 연결성이 매우 중요하다는 것을 알 수 있다. 정보보호 산업의 다양한 분야에서 실제 직무를 수행할 수 있는 인력에 대하여 자격을 부여함으로써 능력을 증명하는 자격이 필요하다는 것을 알 수 있다.

네째, 정보보호 자격에 대한 사후 관리가 엄격하다.

자격의 질은 자격의 유지기간과 매우 밀접한 관련이 있다. 정보보호 자격의 경우 자격을 유지하기 위하여서는 계속 교육을 모두 명시하고 있으며 이를 증명할 수 있어야 한다. 계속 교육에 대한 내용과 시간도 정보보호와 관련지어 엄격하게 규정하고 있으며 자체적으로 인터넷을 이용하여 교육훈련 프로그램을 운영하기도 하고 있다. GIAC을 운영하고있는 SANS는 정보보호 교육훈련 프로그램을 인터넷으로 운영하면서 자격을 취득하고자 하는 사람과 자격취득자를 대상으로 교육훈련을 시행함으로써 자격취득자에 대한 질 관리를 적극적으로 하고 있다.

다섯째, 자격취득자에 대한 지원책이 활발하게 이루어지고 있다.

자격을 운영하는 자격운영기관은 자격 검정의 운영과 관리뿐만 아니라 자격취득자에 대한 지원도 적극적으로 이루어지고 있다. 즉, 자격취득자에 대한 구인과 구직을 지원하기 위하여 자격운영기관의 홈페이지에 별도의 홈페이지를 운영하고 있으며 자격취득자에 대한 관리를 위하여 인터넷으로 교육훈련을 실시하거나 관련 교육훈련 프로그램에 대한 안내를 홈페이지를 통하여 정보를 제공하고 있다. CISA의 경우는 매우 적극적으로 이를 지원하고 있는데 ISACA에서는 한국지부를 운영하면서 자격에 대한 안내와 자격취득자에 대한 관리를 하고 있다. 또한, 자격취득자를 대상으로 하는 커뮤니티를 운영하여 자격취득자에 대한 지원을 하고 있다.

참 고 문 헌

[1] 한국전자통신연구원(2002). 2002 정보통신 기술·산업 전망.

[2] 한국정보보호산업협회(2002). 2001 정보보호 산업실태조사.

[3] 정보통신부(2002). 중장기 정보보호 기본 계획(안).

[4] 한국정보보호산업협회(2002). 2001 정보보호 산업실태조사.

[5] 한국직업능력개발원(2000). 정보통신관련 자격 종목 개발연구.

[6] www.bsikorea.co.kr

[7] www.ics2.org

[8] www.isaca.org.kr

[9] www.kies.co.kr

[10] www.kisa.or.kr

[11] www.sans.org

〈著 者 紹 介〉

나 현 미 (Rha Hyeon Mi)

1988년 2월 숭실대학교 전자계산학과 졸업(학사)
1991년 8월 동국대학교 컴퓨터교육학과 졸업(석사)
2002년 3월~현재 숭실대학교 컴퓨터학과 박사과정
1993년 7월~1997년 9월 한국교육개발원
1997년 10월~현재 한국직업능력개발원
관심분야 : IT 자격재도, IT 교육훈련, e-Leaning

한 호 현 (Han Ho Hyeorn)

1985년 2월 : 서울대학교 해양학과 졸업(학사)
1999년 8월 : 서강대학교 경영대학원 졸업(석사)
2002년 8월~현재 : 숭실대학교 대학원 컴퓨터학과 박사과정
1996년 11월~2003년 1월 : 정보통신부 전산사무관
2003년 1월~현재 : 씨엔씨엔터프라이즈 상무이사
정보통신기술사, 정보관리기술사, 전자계산조직응용기술사
관심분야 : 정보보호, 스마트카드 보안, 정보보호정책

김 종 배 (JongBae Kim)

1996년 2월 : 서울시립대학교 경영학과 졸업(학사)
2002년 8월 : 숭실대학교 정보과학대학원 정보산업학과 졸업(석사)
2002년 8월~현재 : 숭실대학교 대학원 컴퓨터학과 박사과정
1996년 1월~2001년 3월 (주)애드라닷컴 부설 연구소
2001년 4월~현재 (주)이엔터프라이즈 대표이사
관심분야 : 정보보호, 소프트웨어 개발 방법론, 에이전트 시스템