DOI: 10.3745/KIPSTC.2008.15-C.3.173

정보보호 수준평가 적정화 방안 연구

허 순 행[†] · 이 광 우[††] · 조 혜 숙[††] · 정 한 재[††] · 전 웅 렬[††] · 원 동 호[†††] · 김 승 주[††††]

요 약

국내에서는 정보보호 수준평가를 위해 정보보호 관리체계 인증제도와 정보보안 관리수준평가를 운영하고 있다. 하지만 정보보호 관리체계 인증제도와 정보보안 관리수준평가는 기존의 평가인증제도, 정보통신기반보호제도, 정보보호 안전진단제도 등과의 유기적인 연결성이 부족하여 중복 진단, 비효율적인 진단 방법 등의 문제점이 있다. 또한 기존 제도들은 주로 주요정보통신기반시설의 보호에 초점을 맞추고 있어 공공기관의 수준평가에는 적합하지 않다. 본 논문은 공공기관의 정보보호 목표를 효과적으로 달성하기 위해서 기존의 다양한 정보보호제도를 분석하여 새로운 모델을 제안한다.

키워드 : 정보보호, 정보보호제도, 정보보호 수준평가, 정보보호 인증제도, 정보보호 안전진단, 정보보호 관리체계, 수준평가 적정화 방안

A Study on Development of Information Security Evaluation Model

Soonhaeng Hur[†] · Kwangwoo Lee[††] · Heasuk Jo[††] · Hanjae Jeong[††] · Woongryul Jeon[††] · Dongho Won[†††] · Seungjoo Kim[††††]

ABSTRACT

The purposes of this study is development of information security evaluation model for governments to analyze domestic and foreign existing models. Recent domestic information security certification systems have several problems, because shortage of organic connectivity each other. Therefore we analysis on domestic and foreign existing models, specify security requirements, evaluation basis and other facts of models, optimize these facts for governments, and develop new model for domestic governments.

Key Words : Information Security, Information Security System, Information Security Evaluation, Information Security Check, Information Security Management System, Information Security Evaluation Model

1. 서 론

정보화의 급속한 발달로 정보보호의 중요성에 대한 인식이 증가하고 있으며, 이에 따라 조직은 정보보호정책을 수립하고 다양한 정보보호제품을 활용하여 정보보호수준을 향상시키기 위해 노력하고 있다. 이러한 조직의 정보보호수준을 평가하고 향상시키기 위해 국내·외 정보보호 관련기관에서는 다양한 제도를 개발하여 적용하고 있다. 국내에서는 한국정보보호진흥원이 정보보호 관리체계 인증제도를 2002년부터 운영하고 있으며, 국가정보원에서도 공공기관의 정보보안 관리수준평가를 2006년부터 시범 운영하고 있다. 하지만 이들은 평가인증제도, 정보통신기반보호제도, 정보보호 안전진단제도 등 기존 제도와의 유기적인 연결성 부족으로 중복 진단 및 효율적인 보안수준 제고 방법론의 부재와 같은 문제점들을 가지고 있다. 또한 기존 제도들은 주로 주요 정보통신기반기설의 보호에 초점을 맞추었기 때문에 공공기관, 특히 정부부처 산하기관의 정보보호 수준평가에는 적합하지 않다. 따라서 공공기관의 정보보호 목표를 효율적·효과적으로 달성하기 위해서 다양한 기존의 정보보호제도를 통합 및 개선하여 공공기관 평가에 최적화된 모델의 제시가 필요하다[1].

이에 본 연구에서는 국내 공공기관에 적합한 정보보호 수준평가 모델을 개발하는 것을 목표로 한국정보보호진흥원의 정보보호 관리체계인증과 영국의 BS7799, 독일의 IT 베이스라인 보호매뉴얼, 일본의 정보보호 관리체계, 그리고 미국의 DITSCAP을 자세히 분석할 것이다[2][3]. 분석한 내용을 토대로 공공기관에 특화된 정보보호 수준평가 모델을 개발하고 공공기관의 정보보호방법 평가와 보안수준 검증을 통하여 시스템 장애나 침해사고의 피해를 감소시키는 효과를 기대할 수 있을 것이다.

* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-C1090-0801-0028)
† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 석사과정
†† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 박사과정
††† 종신회원 : 성균관대학교 정보통신공학부 교수
†††† 종신회원 : 성균관대학교 정보통신공학부 부교수(교신저자)
논문접수 : 2008년 2월 21일, 심사완료 : 2008년 3월 4일

2. 관련 연구

2.1 주요 정보보호 인증제도 동향

2.1.1 국내 정보보호 인증제도

2.1.1.1 정보보호 관리체계인증

기관이 정보자산의 비밀성, 무결성, 가용성을 지키기 위한 절차 및 과정을 문서화하고 이를 관리하는 시스템을 운영한다면, 정보보호 관리체계인증은 기관이 운영하는 시스템이 기준에 적합한지 평가하고 이에 대한 적합성을 인증하는 제도이다. 기관에서 정보자산의 보호를 위해 관리 및 운영하는 시스템은 정책 수립, 위험 관리, 대책 구현, 사후 관리 등의 여러 정보보호 대책들의 유기적인 결합이며 이를 정보보호 관리체계(ISMS)라 한다. 정보보호 관리체계의 평가는 한국정보보호진흥원과 같이 객관적이며 독립적인 제 3자의 인증기관에서 이루어진다[4].

2.1.1.2 보안성평가 및 평가인증

정보보호제품 보안성평가 및 평가인증은 민간업체가 개발한 정보보호제품의 보안기능을 검증하여 국가차원에서 안전성과 신뢰성을 보증하는 제도이다. 우리나라는 1998년 2월부터 정보보호제품 평가·인증제도를 실시하고 있으며 2002년도부터 국제공통평가기준(Common Criteria)에 따라 정보보호제품을 평가·인증하고 있다. 또한, 2006년 5월 국제상호인정협정에 회원국으로 가입함으로서, 기존의 평가·인증제도를 국제기준에 맞게 개선하여 시행하고 있다. 보안성평가 및 평가인증 체계는 인증기관, 평가기관, 평가신청인으로 이루어지며 인증기관은 국가정보원, 평가기관은 한국정보보호진흥원, 한국산업기술시험원, 한국시스템보증이다[5][6].

2.1.1.3 정보통신기반보호

국가 주요정보통신기반시설을 침해 사고 등의 위협으로부터 보호할 수 있도록 취약점 분석·평가, 보호대책 수립 등에 필요한 기술을 지원하여 동 기반시설의 안정적인 운영을 도모하기 위한 제도이다. 주요정보통신기반시설의 안정적 운영과 동 시설에 내장된 중요 정보의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 전자적 침해행위 등 다양한 위협을 파악하고 이들 위협에 대하여 주요정보통신기반시설에 침해사고 발생 시 파급효과 및 대책을 식별·분석 및 평가한다[6][7].

2.1.1.4 정보보호 안전진단제도

정보보호 안전진단제도는 주요정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC), 쇼핑몰 등의 정보통신망에 대한 침해사고 예방을 위하여 관리적·기술적·물리적 정보보호 지침(안전진단 기준)을 이행하고, 안전진단 수행기관으로부터 안전진단을 받음으로써 정보통신망 및 정보통신서비스에 대한 안정성 및 신뢰성을 확보하기 위한 제도이다. 안전진단 대상자는 매년 1월 1일부터 12월 31일 사이의 기간 내에 안전진단 수행기관으로부터 정보보호 안전진단을 받아야 한다. 정보보호 안전진단제도의 체계는 안전진단 대상자와 안전진단 수행기관으로 구성되며 안전진단 수행기관으로 한국정보보호진흥원이 있다[8].

2.1.1.5 정보보호 수준평가 방법론

정보보호 수준평가 방법론은 한국정보보호진흥원에서 개발한 통신, 금융 등 정보통신기반 및 서비스의 정보보호 수준을 평가하기 위한 방법론이다. 정보보호 정책, 위험평가, 구성관리, 유지보수, 매체보호, 보안 인식과 교육, 비상계획·업무 연속성 계획, 물리적·환경적 보호, 인적보안, 사고대응, 감사 및 책임 추적, 시스템 접근통제 및 통신보호 부분의 성숙도를 평가하며 평가체계는 평가기관과 평가대상기관으로 이루어진다[9].

2.1.2 국외 정보보호 인증제도

2.1.2.1 영국 BS7799

1995년에 BSI(British Standard Institution)에서 처음으로 BS7799 Part 1을 발표하였다. 그 후, 2007년 7월에 ISO/IEC 27002로 명칭이 변경되었다. BS7799 Part 2는 "정보보안 관리시스템 - 사용 안내 명세서(Information Security Management Systems - Specification with guidance for use)"란 명칭으로 1999년 BSI에 의해 처음 발표되었고 2005년 11월에 ISO/IEC 27001로 채택되었다. BS7799의 인증 절차는 정보보호 관리체계의 범위 설정, 정보보호 경영시스템의 방침 설정, 위협평가를 위한 체계적 접근방법 설정, 위협 파악, 위협 평가, 위협 처리를 위한 대안 파악 및 평가, 위협 처리를 위한 통제목표 및 통제항목 선택, 적용성 보고서 작성의 인증 준비 단계와 추진팀 구성 및 전략 합의, 컨설팅의 필요성 검토, 위험평가 수행, 방침문서 개발, 지원문서 개발, 정보보호 경영시스템 실행, 인증등록, 사후관리심사의 인증 단계로 나누어진다[10][11].

2.1.2.2 독일 IT 베이스라인 보호매뉴얼

독일의 연방보안기술청(Bundesamt Fűr Sicherheit in der Informationstechnik, BSI)에서 개발한 IT 베이스라인 보호 매뉴얼은 IT시스템 차원에서 접근하고 있으며, 조직구조, 인력, 기반구조와 기술적인 차원을 적절하게 조화시켜 IT시스템에 대하여 정보보호 수준을 세 단계로 분류하여 선택할 수 있도록 구성되어 있다. 매뉴얼은 자산별로 세부적인 설명을 하고 자산별로 가능한 위협들의 명세를 나열하였으며, 이러한 위협에 따른 위험을 줄이기 위한 가능한 통제사항들을 제시하고 있다[12].

2.1.2.3 일본 정보보호 관리체계

일본 통산성은 기존의 정보시스템 안전대책 인증제도의 개선을 공표하고, 일본 정보처리 개발협회(JIPDEC)를 인정기관으로 지정하여 2001년 4월 6일, 정보시스템 안전대책 인증제도를 정보보호 관리체계 인증제도로 개정 시행 공표하였다. 2002년 4월 1일부터 일본 산업현황을 반영한 독자적

인 인증기준 version 1.0을 시행하다가 2003년 4월 1일부터는 BS 7799-2:2002 에 기반을 둔 version 2.0을 시행하고 있다. 일본의 정보보호 관리체계는 정보보호 관리체계 범위 및 정책 수립, 위협 평가에 기반을 둔 통제 목록 선택, 위험 관리 대책의 세 단계로 나뉜다[13][14].

2.1.2.4 미국 DITSCAP

미 국방부(Department of Defense, DoD)에서는 국방 정보시스템 정보보호 프로그램(Defense Wide Information Systems Security Program, DISSP)을 발족시켜 컴퓨터와 시스템 그리고 네트워크에 대한 평가와 승인을 위한 표준화된 요구사항과 프로세스의 개발을 지원해 왔다. 이러한 표준 평가 및 승인 프로세스는 DoD와 OMB(Office of Management Budget)의 정책과 조화되도록 만들어졌다. 이와 같은 환경에서 개발된 DITSCAP은 DoD 산하 정보시스템의 표준 평가 및 승인 프로세스로써 사용되고 있다. DITSCAP은 정보보증(Information Assurance)과 국방정보기반구조(Defense Information Infrastructure)를 보호하기 위해 정보시스템 평가 및 승인을 위한 표준적인 프로세스, 활동, 태스크와 관리적 책임 및 역할을 포함하고 있다. DITSCAP은 조직의 임무와 전산 환경, 그리고 정보보호 아키텍처에 중점을 두고 있으며 정보시스템과 관련 전산환경과의 통합적 관점에서 접근하는 기반구조 지향의 접근방식을 특성으로 하고 있다. DITSCAP의 평가 체계는 관리역할을 하는 프로그램 매니저, 정보보호 역할을 하는 승인기관과 평가자, 그리고 사용자 역할을 하는 사용자대표로 구성된다. 평가 단계는 정의단계, 검증단계, 확인단계, 사후승인 단계로 나뉜다[15][16][17].

2.2. 국내·외 정보보호제도 비교·분석

2.2.1 국내 정보보호제도 관련 인증구조 현황 분석

국내 정보보호제도 인증구조를 비교·분석하면 <표 1>과 같다.

2.2.2 국외 정보보호 제도 관련 인증구조 현황 분석

국외 정보보호제도 인증구조를 비교·분석하면 <표 2>와 같다. 일본의 정보보호 수준평가제도는 영국의 BS7799 기반이다.

2.2.3 국내·외 정보보호 제도의 문제점

국내 정보보호 관리체계는 영국의 BS7799보다 기술적 측면이 추가되었지만 DITSCAP보다 불충분하며 인증과정에서의 상호의견 교류도 부족하고 자산의 사전평가가 없다. 영국의 BS7799는 관리적 측면이 강하지만, 기술적 측면이 불충분하며 국내 정보보호 관리체계와 마찬가지로 상호의견 교류와 자산의 사전평가가 부족하다. 그리고 DISTCAP과 보안성 평가 및 평가인증은 기술적 부분은 중점적으로 다루지만 관리적 측면이 불충분하다. 따라서 국내·외 제도들의 문제점을 해결하고 공공기관에 적합한 정보보호 수준평가 방법론을 도출하기 위해서 자산의 중요도 파악하고 관리적·기술적 측면을 총체적으로 다룰 수 있는 새로운 공공기관 정보보호 수준평가 방법론이 필요하다[2][3].

〈표 1〉 국내 정보보호제도 관련 인증구조 현황분석

구분	정보보호 관리체계	보안성 평가 및 평가인증	정보통신 기반보호	정보보호 안전진단제도	정보보호 수준평가 방법론
기준구조	- 5단계 관리과정 - 15개 통제영역 - 120개 세부통제사항	- 1,2,3부로 구성 - 11개 보안기능요구사항 클래스 - 10개 보증요구사항 클래스	- 평가는 크게 계획, 심사, 종료 3단계로 진행 - 세부 5단계의 취약성 분석 및 평가 절차로 구성	- 4단계 과정 - 3개 통제영역 - 48개의 관련된 업무 단위 - 시설 및 설비에 대한 안전진단	- 5단계 과정 - 12개 통제영역 - 89개의 관련된 업무 단위 - 통신 및 금융 서비스에 특화한 평가방법론
관리과정	① 정보보호 정책수립 ② ISMS 범위 설정 ③ 위험관리 ④ 구현 ⑤ 사후관리	① PP/ST 소개 ② TOE 설명 ③ 보안환경 ④ 보안목적 ⑤ 보안요구사항 ⑥ 이론적 근거	① 취약성 분석 평가 대상 선별 ② 현 보호대책 및 취약성 평가 ③ 취약성 분석 평가 ④ 보호대책 수립 ⑤ 전담반 구성 분석/평가 계획 수립	① 정보보호지침 이행 ② 안전진단 ③ 개선권고 ④ 개선명령	① 현재 확립된 세부통제항목 이행 중 ② 새로운 세부통제항목 시행계획 수립 및 문서화 ③ 문서화된 계획에 따라 세부통제항목 시행 ④ 일정기간 검증 ⑤ 개선작업 수행
수립 프로세스 차이	기술적 정보보호 측면 강조	기술적 정보보호 측면 강조	기술적 정보보호 측면 강조	관리적 정보보호 측면 강조	관리적 정보보호 측면 강조
세부통제항목	전자상거래 보안, 데이터 센터 보안 등의 통제항목 강화	평가제품의 보안요구사항 항목들을 세부적으로 제공	정보통신설비에 대한 통제항목 강화	정보보호조직의 구성 및 운영과 정보통신설비에 대한 통제항목 강화	정책, 운영, 관리 등의 통제항목 강화
인증심사방법	BS7799 기준으로 하되, 기술심사를 추가	평가·인증제도 절차를 따름	정해진 평가·인증제도 절차를 따름	정해진 평가·인증제도 절차를 따름	정해진 평가·인증제도 절차를 따름

〈표 2〉 국내외 정보보호 수준평가 인증 구조 비교

구분	BS7799 기반형		BS7799 독자형
	영국	독일	DITSCAP
기준구조	- 6단계 관리과정 - 11개 통제영역 - 133개 세부 통제 사항	- 4단계 정보 수집, 4단계 자격 취득의 총 8단계로 구성 - 62개의 세부 모듈로 구성, 모듈 단위 심사	- 4단계 관리과정 - 16개 통제영역 - 39개의 관련된 업무 단위
관리과정	① 정책 정의 ② 영역 설정 ③ 위험분석 및 평가 ④ 위험관리 ⑤ 정책 및 통제목적 일치 ⑥ 보안통제사항 문서화 및 정의	① 조사대상 정의 ② 선행작업 ③ 기본 보안 검사 ④ 추후 활동 명시 ⑤ 타당성 검사 ⑥ 구현 검사 ⑦ 자체선언/인증 ⑧ 재자격 취득	① 정의 ② 확인 ③ 검증 ④ 사후관리
수립 프로세스의 차이	관리적 정보보호 측면 강조	기술적 정보보호 측면 강조	기술적 정보보호 측면 강조
세부통제항목	정보보호관리를 위한 최선의 실무 권고 사항을 제공	IT 인프라 구조와 모듈을 대응시키는 방법을 제공	정보시스템과 국방정보기반구조를 구성하는 요소를 보호
인증심사방법	PDCA(Plan, Do, Check, and Act) 모델을 적용한 일반적인 싸이클 개념	BSI가 허가한 감사인이 인증 수행, 인증결과는 웹을 통해 공시	인증·인가 제도 프로세스를 따름

3. 공공기관에 특화된 정보보호 수준평가 모델 연구

3.1 공공기관에 특화된 정보보호 수준평가 모델 개발

현재 국내 정부부처 산하에는 직할기관 및 사단·재단법인을 포함하여 많게는 수백여 개의 공공기관이 있다. 그러나 규모, 특성, 주요 처리 업무 및 자산이 모두 다른 기관들을 한 가지 기준으로 평가하는 것은 어렵다. 기관에 따라 중요한 자산, 즉 보호해야 할 대상이 다르고 정보보호를 위한 목적 및 수단 역시 차이가 있기 때문이다. 앞서 분석한 국내·외 정보보호 수준평가제도들을 보았을 때 정보보호 관리체계는 평가대상기관이 가지고 있는 자산 파악이 힘들다는 단점을 가지고 있었다. 따라서 정보보호 관리체계의 단점을 보완하기 위해 평가대상기관의 자산평가 체크리스트에 DITSCAP의 인증-인가수준 결정 기준의 가중치를 적용하고 가중치 합으로 기관의 등급을 결정하는 방법을 적용시킨다. 이를 통해 수백여 개에 이르는 공공기관들을 보호하고자 하는 자산에 따라 구분할 수 있도록 적합한 기준을 확립한다. 그리고 그 기준에 따라 공공기관을 몇몇 범주로 구분하여 각 범주에 알맞은 정보보호 수준평가를 수행하는 모델을 개발한다[18].

공공기관에 특화된 정보보호 수준평가 관리 과정은 5단계로 구성한다. 각 단계는 준비단계, 문제정의단계, 사전평가단계, 정보보호 수준평가단계, 그리고 사후 관리 단계로 구성된다.

첫 번째 단계는 준비 단계로 기관의 등급을 결정하는 단계이다. 이 단계는 기관 평가에 앞서 평가에 적합한 평가기준을 확립하는 것이 목적이다. 기관의 등급은 인적/물리적 규모, 기관의 정보시스템 의존도, 기관이 다루는 정보의 중요도 세 가지 기준으로 구분한다. 각 항목에 가중치가 두어 특정 항목의 비중을 조절할 수 있다.

두 번째 문제정의단계는 기관의 정보보호 수준평가를 위한 기반사항을 정립하는 단계이다. 이 단계는 기관의 정보보호 수준을 평가하기 위해 필요한 정보 획득, 평가 및 승인 활동의 전체적인 계획 확립, 그리고 정보보호 수준평가 사전분석서의 작성이 주요 활동이다. 이 단계의 목적은 기관을 평가하기에 앞서 기관의 상황을 정확히 파악하고 기관에 요구되는 보안 요구사항을 정립하는 것이다.

세 번째 단계는 사전평가단계로 두 번째 단계에서 작성한 정보보호 수준평가 사전분석서를 바탕으로 기관을 평가하는 과정이다. 초기 평가활동 수행단계로 기관에 요구되는 정보보호 수준과 현재 기관이 시행 중인 정보보호 수단의 비교 및 검증이 목적이다.

네 번째 단계는 정보보호 수준평가 단계로 실제 기관의 정보보호 수준을 평가하는 단계이다. 이 단계에서 기관은 첫 번째 단계에서 구분한 등급에 적합한 기준으로 평가 받는다. 평가결과를 바탕으로 현존하는 위협을 도출하고 위협을 해결하기 위한 방안을 수립하며 위협 해결을 위한 방안을 적용하고 재평가를 통해 잔재위협의 여부를 판단한다.

마지막 단계는 사후 관리 단계로 정보보호 수준평가를 받은 기관의 사후 정보보호수준 유지 및 관리에 대한 절차와 방법을 정의한다.

3.2 공공기관의 등급을 구분하기 위한 기분

기관을 분류하는 기준은 크게 인적/물리적 규모, 기관의 정보시스템 의존도, 기관이 다루는 정보의 중요도로 구분할 수 있다. 세 범주의 기준에 의거하여 상세기준을 도출하고 그 기준에 따라 기관을 3개의 등급으로 분류한다. 공공기관을 등급 구분 기준은 <표 3>과 같다.

각 기준은 가중치를 지닌다. 가중치의 비중이 큰 항목으로 기관이 소요하는 연간 예산 항목과 기관이 다루는 개인정보의 중요 수준 항목을 들 수 있다. 그 이유는 규모가 작은 기관이라 해도 많은 예산을 보유하거나 다수의 주요 개인정보를 다룬다면 그 기관의 기준은 높게 측정되어야 하기 때문이다. 가중치는 추후 다각도의 분석을 통해 세분화 되

〈표 3〉 공공기관의 등급 구분 기준

대분류	소분류	점검 항목수	문항 점수
기관의 인적/물리적 규모	I-1. 기관에 배정된 예산	5	4.0
	I-2. 기관에 근무 중인 직원 수	5	3.0
	I-3. 국내 또는 국외 하부기관/부속기관의 여부	5	2.5
	I-4. 기관의 정보시스템(PC, 서버, 네트워크 등)을 활용한 업무환경	3	5.5
	I-5. 기관이 사용하는 네트워크 장비(라우터, 허브, 스위치, 서버 등)	5	5.5
	I-6. 정규 직원의 비율	5	6.0
	I-7. 통제구역의 비율	5	5.5
기관의 정보시스템 의존도	II-1. 기관 구성원들의 컴퓨터 시스템 의존도	5	4.5
	II-2. 기관 네트워크 장비가 업무에 미치는 영향	5	5.0
	II-3. 소프트웨어 오류가 작업에 미치는 영향	5	4.5
	II-4. 백업 데이터 비중	5	5.0
	II-5. 외부 IT시스템의 장애가 기관의 IT시스템에 미치는 영향	5	7.0
기관이 다루는 정보의 중요도	III-1. 기관을 감사하는 검사역 담당직원의 비율	5	6.5
	III-2. 기관의 정보가 침해사고로 유출될 경우, 피해복구에 대한 시급 정도	5	9.0
	III-3. 기관이 다루는 개인정보의 수준	5	8.0
	III-4. 기관이 다루는 기관 및 기업정보의 수준	4	8.5
	III-5. 기관의 정보가 정보침해사고로 유출될 경우, 국가의 사회, 경제 기반에 주는 영향	5	10.0
합계		82	100

거나 조정될 수도 있다. 기관의 등급은 기준에 의거하여 기관이 획득한 총점에 따라 구분된다. 즉, 등급의 구분은 기관의 중요정도에 기반을 둔다고 할 수 있다. <표 4>~<표 20>은 공공기관의 등급 구분 기준 항목이다.

〈표 4〉 기관의 인적/물리적 규모 : 예산

I-1. 기관에 배정된 예산				
주요점검내용		▶ 산하기관의 예산 현황	가중치	4.0
점검 항목	1	100억 미만	0	
	2	100 ~ 500억 미만	0.25	
	3	500 ~ 1000억 미만	0.50	
	4	1000 ~ 3000억 미만	0.75	
	5	3000억 이상	1.00	
참조	중소기업 정보보호 수준 자가 측정[19] The US-CCU Cyber-Security Check List[20]			

〈표 5〉 기관의 인적/물리적 규모 : 직원 수

I-2. 기관에 근무 중인 직원 수				
주요점검내용		▶ 산하기관의 직원 수 현황	가중치	3.0
점검 항목	1	30명 이하	0	
	2	31 ~ 50명	0.25	
	3	51 ~ 100명	0.50	
	4	101 ~ 300명	0.75	
	5	301명 이상	1.00	
참조	중소기업 정보보호 수준 자가 측정[19] The US-CCU Cyber-Security Check List[20]			

〈표 6〉 기관의 인적/물리적 규모 : 부속기관

I-3. 국내 또는 국외 하부기관/부속기관의 여부				
주요점검내용		▶ 산하기관의 조직구성(산하기관 하에 하부기관이나 부속기관이 있는지 없는지, 있다면 조직도)	가중치	2.5
점검 항목	1	없음	0	
	2	국내 또는 국외 1	0.25	
	3	국내 또는 국외 2	0.50	
	4	국내 또는 국외 3	0.75	
	5	국내외 다수	1.00	
참조	중소기업 정보보호 수준 자가 측정[19] 취약점 분석 평가를 위한 분석 지침[7]			

〈표 7〉 기관의 인적/물리적 규모 업무환경

I-4. 기관의 정보시스템(PC, 서버, 네트워크 등)을 활용한 업무환경				
주요점검내용		▶ 기관의 정보시스템 활용 범위	가중치	5.5
점검 항목	1	일부에 머무름(LAN환경의 내부 네트워크 기반으로 인사, 재무 등의 단위업무 처리)	0.30	
	2	약간 의존하고 있음(독립적 PC환경에서 사내 업무 등이 PC 중심으로 처리)	0.60	
	3	대부분이 의존하고 있는(외부 네트워크를 통해 기타 산업체 및 기관과 다양한 수준의 정보를 주고받는 처리환경)	1.00	
참조	중소기업 정보보호 수준 자가 측정[19] The US-CCU Cyber-Security Check List[20]			

〈표 8〉 기관의 인적/물리적 규모 : 네트워크 장비

I-5. 기관이 사용하는 네트워크 장비(라우터, 허브, 스위치, 서버 등)				
주요점검내용		▶ 산하기관이 사용하는 네트워크 장비의 수	가중치	5.5
점검 항목	1	없음	0	
	2	기자재의 25% 미만	0.25	
	3	기자재의 50% 미만	0.50	
	4	기자재의 75% 미만	0.75	
	5	기자재의 75% 이상	1.00	
참조	중소기업 정보보호 수준 자가 측정[19] 취약점 분석 평가를 위한 분석 지침[7]			

〈표 9〉 기관의 인적/물리적 규모 : 정규직원 비율

I-6. 정규직원 비율				
주요점검내용		▶ 전체 직원 중 정규직원의 비율	가중치	6.0
점검 항목	1	전체 직원의 40% 미만	0	
	2	전체 직원의 55% 미만	0.25	
	3	전체 직원의 70% 미만	0.50	
	4	전체 직원의 85% 미만	0.75	
	5	전체 직원의 85% 이상	1.00	
참조	중소기업 정보보호 수준 자가 측정[19] 취약점 분석 평가를 위한 분석 지침[7]			

〈표 10〉 기관의 인적/물리적 규모 : 통제구역

I-7. 통제구역의 비율				
주요점검내용		▶ 기관에서 물리적으로 접근통제가 이루어지는 영역의 비율	가중치	5.5
점검항목	1	20% 미만	0	
	2	30% 미만	0.25	
	3	50% 미만	0.50	
	4	70% 미만	0.75	
	5	70% 이상	1.00	
참조	정보보호 관리체계인증[4] 취약점 분석 평가를 위한 분석 지침[7] 정보보안점검항목[21]			

〈표 11〉 기관의 정보 의존도 : 컴퓨터 시스템 의존도

II-1. 기관 구성원들의 컴퓨터 시스템 의존도				
주요점검내용		▶ 기관에서 사용하는 컴퓨터 시스템에 장애가 발생하였을 때 구성원들의 정상적인 업무에 미치는 영향	가중치	4.5
점검항목	1	전혀 영향을 끼치지 않음(0%)	0	
	2	약간 영향을 끼침(25%)	0.25	
	3	보통 영향을 끼침(50%)	0.50	
	4	많은 영향을 끼침(75%)	0.75	
	5	매우 많은 영향을 끼침(100%)	1.00	
참 조	중소기업 정보보호 수준 자가 측정[19] The US-CCU Cyber-Security Check List[20] 정보보호 관리체계인증[4] 취약점 분석 평가를 위한 분석 지침[7] 기업의 정보보호 거버넌스 본연의 자세에 관한 연구회 보고서[22]			

〈표 12〉 기관의 정보 의존도 : 네트워크 장비

II-2. 기관 네트워크 장비가 업무에 미치는 영향				
주요점검내용		▶ 기관에서 사용하는 네트워크 장비에 장애가 발생하였을 때 구성원들의 정상적인 업무에 미치는 영향	가중치	5.0
점검항목	1	전혀 영향을 끼치지 않음(0%)	0	
	2	약간 영향을 끼침(25%)	0.25	
	3	보통 영향을 끼침(50%)	0.50	
	4	많은 영향을 끼침(75%)	0.75	
	5	매우 많은 영향을 끼침(100%)	1.00	
참 조	The US-CCU Cyber-Security Check List[20] 정보보호 관리체계인증[4] 취약점 분석 평가를 위한 분석 지침[7] 기업의 정보보호 거버넌스 본연의 자세에 관한 연구회 보고서[22]			

〈표 13〉 기관의 정보 의존도 : 소프트웨어 오류

II-3. 소프트웨어 오류가 작업에 미치는 영향				
주요점검내용		▶ 소프트웨어에 오류가 발생할 경우, 구성원들이 정상적인 업무에 미치는 영향	가중치	4.5
점검항목	1	전혀 영향을 끼치지 않음(0%)	0	
	2	약간 영향을 끼침(25%)	0.25	
	3	보통 영향을 끼침(50%)	0.50	
	4	많은 영향을 끼침(75%)	0.75	
	5	매우 많은 영향을 끼침(100%)	1.00	
참 조	중소기업 정보보호 수준 자가 측정[19] The US-CCU Cyber-Security Check List[20] 정보보호 관리체계인증[4] 취약점 분석 평가를 위한 분석 지침[7] 기업의 정보보호 거버넌스 본연의 자세에 관한 연구회 보고서[22]			

〈표 14〉 기관의 정보 의존도 : 백업 데이터

II-4. 백업 데이터 비중				
주요점검내용		▶ 기관의 중요자산이 되는 주요정보들을 제2의 저장 공간에 백업하는 비율을 검사	가중치	5.0
점검항목	1	전체의 10% 미만	0	
	2	전체의 10~20%	0.25	
	3	전체의 20~50%	0.50	
	4	전체의 50~80%	0.75	
	5	전체의 80% 이상	1.00	
참 조	중소기업 정보보호 수준 자가 측정[19] The US-CCU Cyber-Security Check List[20] 정보보호 관리체계인증[4] 정보보호 수준평가방법론[9] 기업의 정보보호 거버넌스 본연의 자세에 관한 연구회 보고서[22]			

〈표 15〉 외부 시스템 장애

II-5. 외부 IT시스템의 장애가 기관의 IT시스템에 미치는 영향				
주요점검내용		▶ 기관의 IT시스템을 활용한 업무가 외부에 존재하는 IT시스템으로부터 받는 영향	가중치	7.0
점검항목	1	외부 IT시스템 장애 발생 시 모든 업무가 마비됨	0	
	2	외부 IT시스템 장애 발생 시 상당부분 업무에 영향이 있음	0.25	
	3	외부 IT시스템 장애 발생 시 일부 IT 업무에 영향이 있음	0.50	
	4	기관 내 IT시스템은 필요에 따라 외부 IT시스템과 연관됨	0.75	
	5	기관 내 IT시스템은 외부 IT시스템과 무관하게 정상 동작됨	1.00	
참 조	국가사이버안전매뉴얼[23] 정보보안점검항목[21] 정보시스템 장애관리 지침[24] 기업의 정보보호 거버넌스 본연의 자세에 관한 연구회 보고서[22]			

〈표 16〉 기관이 다루는 정보의 중요도 : 검사역직원 비율

III-1. 기관을 감사하는 검사역 담당직원의 비율				
주요점검내용		▶ 전체 직원 중 기관 내 각 기관부서를 감사하는 검사역의 비율	가중치	6.5
점검항목	1	전체 직원의 0.5% 미만	0	
	2	전체 직원의 1% 미만	0.25	
	3	전체 직원의 1.5% 미만	0.50	
	4	전체 직원의 2% 미만	0.75	
	5	전체 직원의 2% 이상	1.00	
참조	정보보호 관리체계인증[4] 정보보안점검항목[21] 정보보호 수준평가방법론[9] 전산감리 효과 연구[25]			

〈표 17〉 기관이 다루는 정보의 중요도 : 피33해복구

III-2. 기관의 정보가 침해사고로 유출될 경우, 피해복구에 대한 시급 정도				
주요점검내용		▶ 기관이 침해사고를 당했을 때, 이에 대한 피해복구 업무가 기관의 전체 업무 순위에서 차지하는 정도	가중치	9.0
점검항목	1	전혀 영향을 미치지 않음(0%)	0	
	2	약간 영향을 미침(25%)	0.25	
	3	보통 영향을 미침(50%)	0.50	
	4	많은 영향을 미침(75%)	0.75	
	5	매우 많은 영향을 미침(100%)	1.00	
참조	국가사이버안전매뉴얼[23] 정보보안점검항목[21]			

〈표 18〉 기관이 다루는 정보의 중요도 : 개인정보

III-3. 기관이 다루는 개인정보의 수준				
주요점검내용		▶ 기관이 보유하고 있는 개인정보의 수준	가중치	8.0
점검 항목	1	낮은 수준-익명이 보장된 온라인 정보(홈페이지주소, IP주소 등)	0	
	2	약간 낮은 수준-익명이 보장된 오프라인 정보(전화번호, 주소, 이메일주소 등)	0.25	
	3	보통 수준-개인정보(이름, 회사명, 핸드폰번호)	0.50	
	4	약간 높은 수준-개인 식별 정보(주민등록번호, 사회보장번호 등)	0.75	
	5	높은 수준-개인 금융 관련 정보(카드번호, 통장번호 등)	1.00	
참조	정보보호 관리체계인증[4]			

〈표 19〉 기관이 다루는 정보의 중요도 : 기업정보

III-4. 기관이 다루는 기관 및 기업정보의 수준				
주요점검내용		▶ 기관이 보유하고 있는 전산화된 기밀자료와 전체 기밀자료의 비율	가중치	8.5
점검 항목	1	낮은 수준·공개 정보(홈페이지주소, IP주소, 전화번호 등)	0	
	2	약간 낮은 수준·공개 정보(연봉수준, 인사 계획 등)	0.33	
	3	보통 수준·중요사업 기밀정보(기업의 중요사업 계획 등)	0.66	
	4	약간 높은 수준·핵심기술 기밀정보(기업의 원천기술 등)	1.00	
참조	정보보호 관리체계인증[4]			

〈표 20〉 기관이 다루는 정보의 중요도 : 정보유출

III-5. 기관의 정보가 정보침해사고로 유출될 경우, 국가의 사회, 경제 기반에 주는 영향				
주요점검내용		▶ 기관의 정보가 침해사고로 유출되었을 경우, 그 피해가 사회, 경제 전반에 미치는 영향의 정도	가중치	10
점검 항목	1	영향을 미치지 않음(0%)	0	
	2	거의 영향을 미치지 않음(25%)	0.25	
	3	일정수준 영향을 미침(50%)	0.50	
	4	상당한 영향을 미침(75%)	0.75	
	5	매우 큰 영향을 미침(100%)	1.00	
참조	국가사이버안전매뉴얼[23] 정보보안점검항목[21] 정보보호 수준평가방법론[9] 정보시스템 장애관리 지침[24]			

3.3 공공기관의 등급 구분

공공기관의 등급은 각 항목의 점수에 가중치를 곱한 점수에 따라 결정된다. 기관의 등급은 세 등급으로 높은 수준의 정보를 다루는 기관, 보통 수준의 정보를 다루는 기관, 낮은 수준의 정보를 다루는 기관으로 구분된다. 구분 기준 75점 이상 100점 사이는 A 등급, 55점 이상 80점 이하의 점수는 B 등급, 60점 이하의 점수는 C 등급의 기관을 나타낸다. A, B, C 등급 간에 가중치는 크게는 5 ~ 10점의 점수가 중첩되는데, 그 이유는 평가대상기관과 평가위원회 간의 협의에 의하여 평가 수준을 조정할 수 있는 기회를 부여하기 위해서이다. 그리고 이러한 기관의 등급에 따라 추후 세부 체크리스트의 기준이 정해진다.

3.4 공공기관의 정보보호 수준평가 기준

기관 등급 구분 기준을 통해 산정된 기관의 등급을 바탕으로 실제 공공기관의 정보보호 수준을 평가하기 위한 기준을 제안한다. 본 공공기관 정보보호 수준평가 기준에서는 기관의 정보보호 수준을 평가하기 위해 공공기관이 만족해야 하는 정보보호 수준을 기관의 등급에 일대일로 대응하도록 부여함으로써 기관이 다루는 정보의 중요도에 따라 평가 기준을 달리하도록 하였다. 따라서 기관은 평가를 통해 기관에 부여된 기준 등급 이상을 획득해야 하며, 이를 통해 기관의 정보보호수준이 우수함을 입증할 수 있다. 평가기관은 경우에 따라 통제 분야 및 세부 항목을 추가할 수 있으므로 각 기관의 특성에 맞게 유연하게 적용할 수 있다. 평가 결과가 기관에 적합한 정보보호 등급에 미치지 못하는 경우, 기관은 네 번째 단계인 정보보호 수준평가 단계에서 기관의 부족한 부분을 보완하여 재평가 되어야 한다. 예를 들어, 공공기관 '가'가 있다고 가정할 경우, 본 모델을 적용하여 정보보호 수준을 평가하기 위한 첫 단계로 기관이 다루는 정보의 자산 가치를 통해 기관을 등급화 한다. 이 때 "기관의 등급을 구분하기 위한 기준"에는 인적/물리적 규모, 기관의 정보 의존도, 기관이 다루는 정보의 중요정도 등이 가중치에 따라 계산된다. 이 계산된 결과는 <표 22>의 세 등급 중 하나에 속하게 된다. 만약 '가' 기관의 등급이 B 등급 즉, "보통 수준의 정보를 다루는 중간 규모의 기관"에 속한다면 B 등급에 해당하는 공공기관의 정보보호 수준 등급 기준인 "보통 수준의 정보를 다루는 기관이 수행되어야 할 항목"을 만족시켜야 한다. 이때 그 기준을 모두 만족시킨다면 '가' 기관은 B 등급의 정보보호 수준으로 인증 받을 수 있게 된다. 이 때 평가 기준은 그 기관의 특성에 맞게 추가될 수 있으며, 이 평가 기준에 충족되지 않을 때에는 평가 모델 관리과정에 따라 피드백을 통해 보완과정을 거치게 된다.

〈표 21〉 공공기관의 정보보호 수준 등급 분류

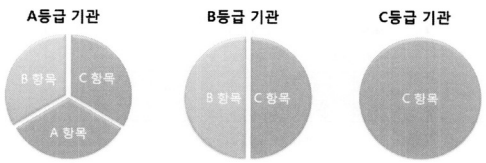
등급 (Level)	내 용
A	높은 수준의 정보를 다루는 기관이 수행되어야 할 항목
B	보통 수준의 정보를 다루는 기관이 수행되어야 할 항목
C	낮은 수준의 정보를 다루는 기관이 수행되어야 할 항목

3.4.1 정보보호 수준평가를 위한 체크리스트

체크리스트는 크게 관리적 보호, 기술적 보호, 물리적 보호의 세 영역으로 구성되어 있으며, 세부적으로 180개의 세부 체크리스트 항목으로 구성된다. 이를 통해 산정된 공공기관의 정보보호 수준 등급은 A, B, C 등급으로 구분되

며, 기관이 다루는 정보의 중요도에 따라 체크리스트 항목이 정해진다. 체크리스트 각 항목은 (그림 1)과 같이 포함관계를 가지는데, A 등급 기관은 체크리스트의 A, B, C 항목을 모두 점검해야 하고, B 등급 기관은 B, C 항목을 선택하여 점검하며, C 등급 기관은 C 항목에 해당하는 항목만을 선택하여 점검하면 된다. 이 때 평가대상기관은 체크리스트 항목 중 "필수"로 표시된 문항에 대해서는 반드시 수행하고 있어야 한다.

정보보호 수준평가를 위한 체크리스트는 평가대상기관 스스로가 자가 테스트를 할 수 있게 구성되었다. 자가 테스트를 할 수 있음으로써 기관을 스스로 평가 할 수 있는 장점이 있는 반면, 평가받기 위해 평가위원회에 제출하는 체크리스트 점검 결과의 점수를 조작하여 임의의 항목을 선택해 높은 등급을 취할 수 있는 단점이 발생할 수 있다. 따라서 이를 방지하기 위해 본 연구에서는 "필수" 항목을 제시하였는데, 이는 평가대상기관의 등급에 따라 기관에 반드시 요구되는 항목으로 반드시 수행되고 있어야 하며, 만일 "필수" 항목이 수행되고 있지 않을 경우에는 그 등급을 취할 수 없어 재평가되어야 한다. 하지만 유연한 평가제도가 되기 위해, 평가위원회와 평가대상기관은 기관의 특성상 "필수"항목을 수행하지 않아도 되는 경우 협의를 통해서 "필수" 항목을 제거할 수 도 있다. 정보보호 수준평가를 위한 체크리스트 기준은 <표 22>이고, <표 23>~<표 63>은 체크리스트이다. <표 64>는 각 체크리스트의 항목별 등급에 따른 필수 항목의 총점과 등급에 대한 전체 총점을 나타낸다.



(그림 1) 각 기관별 수행해야하는 항목

〈표 22〉 공공기관의 정보보호 수준평가 체크리스트

대분류	중분류	소분류	항목수
1.관리적보호	1.1 정보보호조직의 구성·운영	1.1.1 정보보호조직의 구성 1.1.2 정보보호책임자의 선정 1.1.3 정보보호조직 구성원의 역할	17
	1.2 정보보호계획 등의 수립 및 관리	1.2.1 정보보호방침의 수립 및 수행 1.2.2 정보보호실행계획의 수립 및 수행 1.2.3 정보보호실무지침의 마련 및 준수	21
	1.3 인적보안	1.3.1 내부인력 관리 및 보안 1.3.2 주요/민감한 직무 담당자에 대한 관리 1.3.3 외부 인력에 대한 보안지침 1.3.4 위탁운영 관련 보안지침	13
	1.4 사용자 지침	1.4.1 정보보호 지침 제공	5
	1.5 침해사고 대응	1.5.1 침해사고 대응계획의 존재여부 1.5.2 침해사고 대응체계 1.5.3 유사 침해사고 방지를 위한 노력 1.5.4 침해사고의 기록 및 관리 1.5.5 사고의 복구 1.5.6 유사 사고 방지를 위한 대책	19
	1.6 정보자산 및 설비의 관리	1.6.1 정보통신설비 및 시설 관리	7
2. 기술적 보호	2.1 네트워크 보안	2.1.1 트래픽 모니터링 2.1.2 무선서비스 보안 2.1.3 정보보호시스템 설치 및 운영 2.1.4 정보보호시스템 보안	19
	2.2 정보시스템 보안	2.2.1 정보시스템 취약점 점검 2.2.2 웹 서버 보안 2.2.3 DNS 서버 보안 2.2.4 DHCP 서버 보안 2.2.5 DB 서버 보안 2.2.6 라우터/스위치 보안	36
	2.3 접근통제	2.3.1 접근통제 관리	4
	2.4 식별 및 인증	2.4.1 관리자 및 사용자 계정 관리 2.4.2 사용자 식별 및 인증	11
	2.5 패치관리	2.5.1 패치 관리	2
3.물리적 보호	3.1 물리적 보호구역의 출입 및 접근보안	3.1.1 물리적 보호구역의 정의와 보안대책 수립 및 이행 3.1.2 물리적 보호구역에 대한 접근통제	7
	3.2 물리적 보호구역의 백업 및 복구	3.2.1 물리적 보호구역 내의 자산에 대한 백업 장비 및 시설 3.2.2 물리적 보호구역 내의 자산에 대한 백업 및 복구 절차	6
	3.3 물리적 보호구역의 유지보수 및 관리	3.3.1 물리적 보호구역의 위치 및 구조 3.3.2 물리적 보호구역에서 사용하는 장비들에 대한 안전한 폐기 및 정책 3.3.3 물리적 보호구역에서 사용하는 장비들에 대한 유지보수 및 관리 3.3.4 물품 배달 및 수령에 대한 통제 여부 3.3.5 전원 공급 및 통신회선 보호	13
계			180

〈표 23〉 관리적 보호 : 정보보호조직 구성

1.1.1 정보보호조직의 구성					
주요점검내용		▶ 정보보호조직(정보보호책임자, 정보보호관리자, 정보보호담당자) 운영 여부 ▶ 정보보호관리 활동에 도움을 받기 위해 외부 전문가의 조언을 받았는지 여부	해당등급	항목점수	필수항목
점검 항목	1	정보보호책임자, 정보보호관리자, 정보보호담당자로 구성된 정보보호조직이 운영되고 있는가?	A, B, C	2.0	
	2	실무적인 보안 관리를 총괄 수행하는 정보보호관리자가 지정되어 있는가?	A, B, C	2.5	
	3	주요시설 및 주요정보자산의 보안운영 실무를 담당하는 정보보호담당자가 지정되어 있는가?	A, B, C	2.5	필수
	4	정보보호조직이 별도의 전담팀으로 구성되어 있는가?	A, B	2.0	
	5	정보보호관리자와 정보보호담당자는 겸직할 수 있으나 별도로 지정되어 있는가?	A, B	1.5	
	6	중요한 정보보호관리 활동에 도움을 얻기 위해 외부 전문가의 조언을 받았는가?	A, B	1.5	
	7	외부 전문지식을 보유하고 있는가?	A, B	1.5	
참조		정보보호 안전진단기준[26] 정보보호 관리체계인증[4]			

〈표 24〉 관리적 보호 : 정보보호책임자

1.1.2 정보보호책임자의 선정					
주요점검내용		▶ 침해사고 발생 시 정보보호 조직이 긴급조치 권한을 행사할 수 있는 자를 지정하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	정보보호에 대한 업무를 총괄하는 정보보호책임자가 지정되어 있는가?	A, B, C	2.0	
	2	정보보호책임자는 최고경영층의 공식적인 지정을 받아 모든 임직원에게 공표되어 있는가?	A, B, C	1.5	
	3	정보보호책임자는 침해사고 등 비상상황 발생 시 대책반을 구성할 수 있는 권리가 있는가?	A, B, C	1.5	
	4	정보보호책임자는 정보보호 활동 및 직무를 수행하기 위한 충분한 경험과 지식을 보유하고 있는가?	A, B, C	3.0	필수
	5	정보보호책임자는 CIO(Chief Information Officer) 또는 CSO(Chief Security Officer)등 임원급으로 지정되어 있는가?	A	2.0	
참조		정보보호 안전진단기준[26]			

〈표 25〉 관리적 보호 : 조직 구성원

1.1.3 정보보호조직 구성원의 역할					
주요점검내용		▶ 정보보호책임자가 정보보호 업무와 조직을 총괄 지휘하는지 여부 ▶ 정보보호관리자가 정보보호 업무의 실무를 총괄하고 관리하는지 여부 ▶ 정보보호담당자가 정보보호 업무의 분야별 실무를 담당하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	정보보호책임자, 정보보호관리자, 정보보호담당자의 업무를 정의한 업무분장 문서가 있는가?	A, B, C	2.5	필수
	2	정보보호담당자의 업무분장 문서에는 각 업무별 실무에 대한 역할 및 책임이 명시되어 있는가?	A, B, C	2.5	필수
	3	정보보호책임자, 정보보호관리자, 정보보호담당자 각자의 업무분장 문서와 실제 업무는 일치하는가?	A, B	2.0	
	4	정보보호책임자, 정보보호관리자, 정보보호담당자의 세부 역할과 책임을 정보보호실무지침에 반영하였는가?	A, B	1.5	
	5	정보보호 조직의 각 주체의 업무분장 문서는 매년 검토되어 갱신되고 있는가?	A, B	1.0	
참조		국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]			

〈표 26〉 관리적 보호 : 정보보호방침

1.2.1 정보보호방침의 수립 및 수행					
주요점검내용		▶ 정보보호 목표, 범위, 책임 등을 포함한 정보보호방침(policy)이 수립되어 있는지 여부 ▶ 최고경영층(임원급 이상)의 승인이 있는지 여부 ▶ 기관의 경영목표를 지원할 수 있도록 정보보호의 법적, 규제적 요건과, 전략적이고 조직적인 위험관리를 기술한 정보보호정책을 수립되어 있는지 여부	해당등급	항목점수	필수항목
점검 항목	1	회사의 정보보호의 목적, 범위, 책임 등을 포함한 정보보호방침(Policy)이 수립되어 있는가?	A, B, C	2.5	필수
	2	정보보호방침은 최고경영층(임원급 이상)이 승인하였는가?	A, B, C	2.0	
	3	정보보호방침은 모든 임직원 및 관련자에게 공표되어 이를 준수하고 있는가?	A, B, C	1.5	
	4	정보보호방침은 주기적으로 검토되어 갱신되고 있는가?	A, B, C	1.5	
	5	정보보호방침은 모든 임직원 및 관련자가 쉽게 열람할 수 있도록 비치되어 있는가?	A, B	1.0	
	6	정보보호 방침에는 정보보호의 목적을 지지하기 위한 최고경영자의 의지가 표명되어 있는가?	A, B	1.0	
	7	정보보호방침을 알리기 위해 소책자, 전자 문서 등 다양한 방법을 사용하고 있는가?	A, B	1.0	
	8	정보보호정책은 국가나 관련 산업에서 정하는 정보보호의 법이나 규제사항을 만족하고 있는가?	A, B, C	3.0	필수
	9	정보보호정책은 전략적이고 조직적인 위험관리를 기술하고 있는가?	A, B	2.5	
	10	정보보호정책에서 다루는 적용범위가 적절한가?	A, B	2.0	
	11	전년도 보안활동 추진 결과에 대한 심사분석을 하고 있는가?	A	1.5	
참조		국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26] 정보보호 관리체계인증[4]			

〈표 27〉 관리적 보호 : 정보보호실행계획

1.2.2 정보보호실행계획의 수립 및 수행					
주요점검내용		▶ 정보보호방침을 토대로 예산, 일정 등을 포함한 당해 연도의 정보보호실행계획이 수립되어 있는지 여부 ▶ 최고경영층이 실행계획을 승인하고 정보보호책임자가 추진 상황을 매 분기마다 점검하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	정보보호방침을 토대로 예산, 일정 등을 포함한 당해 연도의 정보보호 실행계획을 수립하고 있는가?	A, B, C	2.5	필수
	2	정보보호실행계획은 최고경영층이 승인하고 있는가?	A, B, C	1.5	
	3	정보보호책임자는 반기별로 정보보호 실행계획을 검토하고 있는가?	A, B, C	1.5	
	4	정보보호실행계획에 안전진단계획이 포함되어 있는가?	A, B, C	2.5	필수
	5	정보보호실행계획이 정보보호방침과 명확한 관계가 있는가?	A	2.0	
참조	정보보호 안전진단기준[26]				

〈표 28〉 관리적 보호 : 정보보호실무지침

1.2.3 정보보호실무지침의 마련 및 준수					
주요점검내용		▶ 정보통신설비 및 시설에 대한 관리적·기술적·물리적 보호조치의 구체적인 시행 방법·절차 등을 규정한 정보보호실무지침을 마련하였는지 여부 ▶ 정보보호책임자가 실무지침을 승인하고 관련 법·제도, 설비의 교체 등 변경사유가 발생할 경우 보완하여 관리하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	정보보호방침 및 정보보호실행계획을 구체적으로 수행하기 위한 정보보호활동의 세부적인 방법 및 절차를 구체화시킨 정보보호실무지침들이 있는가?	A, B, C	2.5	필수
	2	정보보호실무지침들은 관리적·기술적·물리적 보호조치에 합당한 내용을 포함하고 있는가?	A, B, C	2.5	필수
	3	각 정보보호실무지침들은 정보보호책임자의 승인을 득하였는가?	A, B, C	1.5	
	4	각 정보보호실무지침들은 수시·주기적으로 검토되어 변경되고 있는가?	A, B, C	1.5	
	5	정보보호실무지침들은 각 해당자에게 적절한 방법을 통해 배포되고 준수되고 있는가?	A, B	1.0	
참조	정보보호 안전진단기준[26]				

〈표 29〉 관리적 보호 : 내부인력

1.3.1. 내부인력 관리 및 보안					
주요점검내용		▶ 임직원의 전보 또는 퇴직시 관련 계정 등에 대한 접근 권한을 제거하는지 여부 ▶ 임직원에게 정보보호 인식을 제고할 수 있는 홍보(정보보호 실천수칙 보급 등)를 실시하는지 여부 ▶ 정보보호조직의 구성원 및 정보보호와 관련된 업무에 종사하는 자에게 정기적으로 정보보호 교육을 실시하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	임직원의 전보 또는 퇴직 시 해당자의 계정 등에 대한 접근 권한을 즉시 제거하고 있는가?	A, B	3.0	필수
	2	임직원의 정보보호인식을 제고할 수 있는 홍보(정보보호 실천수칙 보급 등)를 실시하고 있는가?	A, B	1.5	
	3	모든 임직원에게 정기적으로 정보보호 교육을 실시하고 있는가?	A	1.5	
	4	정보보호담당자들이 외부 전문교육 또는 세미나 등에 참석하고 있는가?	A, B	1.5	
참조	The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]				

〈표 30〉 관리적 보호 : 직무 담당자

1.3.2. 주요/민감한 직무 담당자에 대한 관리					
주요점검내용		▶ 정보시스템 접근권한을 포함하는 업무가 새로이 할당될 때, 특히 재무정보나 비밀정보와 같이 중요한 정보를 처리하는 담당자에 대해서는 별도의 관리를 수행하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	주요/민감한 직무에 대한 정의가 이루어지고 있는가?	A, B, C	2.0	
	2	민감한 직무 담당자에 대해서는 강화된 적격심사가 이루어지고 있는가?	A, B	2.0	
	3	민감한 정보를 취급하는 직원들에 대한 비밀유지서약이 이루어지고 있는가?	A	2.5	필수
참조	The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]				

〈표 31〉 관리적 보호 : 외부 인력

1.3.3. 외부 인력에 대한 보안지침					
주요점검내용		▶ 계약직 및 임시 직원은 물론 정식직원 채용 시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어지는지 여부 ▶ 직원들이 용역회사를 통해 충원되는 경우 용역회사의 계약서의 적격심사에 따르는 책임사항을 명문화하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	계약직 및 임시 직원 채용 시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어지는가?	A, B	3.0	필수
	2	직원들이 용역회사를 통하여 충원되는 경우, 용역회사와의 계약서에 적격심사에 따른 책임사항이 명문화되어 있는가?	A, B, C	2.5	필수
참조	The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]				

〈표 32〉 관리적 보호 : 위탁운영

1.3.4. 위탁운영 관련 보안지침					
주요점검내용		▶ 전산업무를 외부에 위탁할 경우 보안계약서 또는 서비스 수준협약 등에 '정보보호에 관한 위탁업체의 책임범위', '위탁업무 중단에 따른 비상대책' 등을 반영하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	전산업무를 외부 업체에 위탁할 경우 계약서 또는 서비스 수준 협약 내에 정보보호에 대한 위탁업체의 책임범위가 반영되어 있는가?	A, B, C	2.5	필수
	2	전산업무를 외부 업체에 위탁할 경우 업무 중단에 따른 비상대책이 반영되어 있는가?	A, B	2.5	필수
	3	계약서 또는 서비스수준협약 내에 명시된 내용이 정보보호관련 법률 또는 제도 등을 만족하고 있는가?	A, B, C	3.0	필수
	4	위탁운영 계약서 또는 서비스수준협약서 상의 정보보호 준수사항을 주기적으로 점검하기 위하여 절차가 마련되어 있는가?	A, B	1.5	
참조	The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]				

〈표 33〉 관리적 보호 : 정보보호지침

1.4.1. 정보보호지침 제공					
주요점검내용		▶ 사용자에게 침해사고 예·경보, 보안취약점, 계정·비밀번호 관리방안 등의 정보를 지속적으로 제공하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	사용자에게 개인정보보호정책, 보안취약점, 계정 및 비밀번호 관리방안 등을 제공하는가?	A, B, C	2.5	필수
	2	사용자에게 수시·정기적으로 정보보호 관련 정보를 제공(메일, 홈페이지 게시, 또는 SMS 등)하고 있는가?	A, B, C	2.0	
	3	사용자에게 정보를 제공하기 위해 사용자의 연락처를 확보하고 있는가?	A, B, C	2.0	
	4	사용자에게 정보보호정보를 제공하는 담당자가 지정되어 있는가?	A, B	1.5	
	5	사용자의 정보보호 관련 문의사항이나 조치를 취하기 위한 헬프데스크가 운영되고 있는가?	A, B	3.0	필수
참조	The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]				

〈표 34〉 관리적 보호 : 침해사고 대응계획

1.5.1. 침해사고 대응계획의 존재여부					
주요점검내용		▶ 보안사고의 정의 및 범위, 긴급연락체계 구축, 보안사고 발생 시 보고 및 대응절차, 사고 복구조직의 구성, 교육계획 등을 포함한 보안사고 대응계획을 수립 및 시행하고 있는지 여부	해당등급	항목점수	필수항목
점검 항목	1	보안사고 대응계획이 수립되어 있는가?	A, B, C	3.0	필수
	2	보안사고가 중요도에 따라 분류되어 있고 이에 따른 보고라인이 정의되어 있는가?	A, B, C	2.5	
	3	사고대응계획은 기관의 업무연속성계획과 일관성이 있는가?	A, B	2.0	
참조	The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]				

〈표 35〉 관리적 보호 : 침해사고 대응체계

1.5.2. 침해사고 대응체계					
주요점검내용		▶ 보안사고의 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하였는지 여부 ▶ 대응체계에는 내부 직원 뿐 아니라 외부기관의 전문가와 협조체계를 반영하고 있는지 여부	해당등급	항목점수	필수항목
점검 항목	1	보안사고를 모니터링하고 대응할 수 있는 중앙집중적인 대응체계가 구축되어 있는가?	A, B	2.5	필수
	2	보안사고의 모니터링, 대응 및 처리와 관련되어 전문가, 전문기관, 전문정부기관 등과의 협조체계를 구축하고 있는가?	A	2.0	
참조	The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]				

〈표 36〉 관리적 보호 : 유사 침해사고 방지

1.5.3. 유사 침해사고 방지를 위한 노력					
주요점검내용		▶ 보안사고 대응 계획, 절차 및 방법에 대하여 정기적으로 교육을 실시하는지 여부 ▶ 사고 처리 후 재발 방지를 위한 교육 및 훈련을 실시하고 있는지 여부	해당등급	항목점수	필수항목
점검 항목	1	보안사고 대응방법 및 절차에 관한 적절한 교육 계획이 존재하고, 이에 따라 정기적으로 교육을 실시하고 있는가?	A	2.5	필수
	2	보안사고 처리 후 재발방지를 위하여 교육, 훈련이 실시되고 있는가?	A	2.5	
참조	The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]				

〈표 37〉 관리적 보호 : 침해사고 관리

1.5.4. 침해사고의 기록 및 관리					
주요점검내용		▶ 사고의 징후 또는 보안사고 발생을 인지한 때에 보고체계에 따라 적절하고 신속히 보고되는지 여부 ▶ 시스템이나 네트워크 보안취약점과 소프트웨어 기능장애의 보고 여부	해당등급	항목점수	필수항목
점검 항목	1	보안사고의 징후 또는 보안사고 발생을 인지한 경우, 정의된 보안사고보고절차에 의해 신속하게 보고가 이루어지고 있는가?	A, B, C	2.5	필수
	2	보안사고의 징후 또는 발생을 문서화한 보안사고보고서가 존재하는가?	A, B	2.0	
	3	주요 사고로 지정된 사고의 경우 최고경영층에 까지 신속히 보고되고 있는가?	A, B	1.5	
	4	보안사고 보고에 관해 관계기관의 법률이나 규정 등이 존재하는 경우, 보고되어야 할 내부의 보안사고가 관계기관 등에 적절히 보고되고 있는가?	A, B, C	3.0	필수
	5	시스템이나 네트워크의 보안취약점과 소프트웨어 기능장애 또한 신속히 보고되고 있는가?	A, B, C	2.0	
참조		The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]			

〈표 38〉 관리적 보호 : 보안사고 복구

1.5.5. 보안사고의 복구					
주요점검내용		▶ 보안사고 발생 시 처리, 복구 절차에 따라 처리와 복구를 신속히 수행하는지의 여부	해당등급	항목점수	필수항목
점검 항목	1	보안사고 처리 및 복구 절차가 존재하는가?	A, B, C	2.5	필수
	2	절차에 따라 보안사고 처리 및 복구가 이루어지며 처리결과가 반영된 보고서가 존재하는가?	A	2.0	
	3	모든 보안사고는 발생부터 해결될 때까지 기록 및 감사되고 있는가?	A	2.0	
참조		The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]			

〈표 39〉 관리적 보호 : 보안사고 방지

1.5.6. 유사 사고 방지를 위한 대책					
주요점검내용		▶ 보안사고가 처리되고 종결된 후 이에 대한 분석이 수행되는지 여부 ▶ 보안사고로부터 얻은 정보는 관련조직 및 인력이 공유하고, 유사 사고가 발생하지 않도록 대책을 수립하는지 여부 ▶ 유사사고 방지를 위한 정책, 절차, 조직 등 보안체계가 필요에 의해 변경되고 적용되는지의 여부	해당등급	항목점수	필수항목
점검 항목	1	보안사고는 보안사고의 유형, 유사 사고의 발생빈도, 사고 처리 비용 등 다양한 관점으로 분석되어 보고되고 있는가?	A	2.0	
	2	보안사고 정보와 발견된 취약성들이 관련조직과 인력에 공유되고 있는가?	A	1.5	
	3	보안사고 분석을 통해 얻어진 정보를 활용하여 유사사고가 반복되지 않도록 하는 재발방지 대책이 수립되었는가?	A, B	2.5	필수
	4	분석된 결과에 의해 보안사고 대응절차, 보안대책, 보안정책 및 절차 등을 변경하는 절차가 존재하며, 필요 시 이에 따라 변경이 이루어지는가?	A, B	1.5	
참조		The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]			

〈표 40〉 관리적 보호 : 정보통신설비 관리

1.6.1. 정보통신설비 및 시설 관리					
주요점검내용		▶ 정보통신망 구성도를 마련하고 변경사항이 있을 경우 보완·관리 여부 ▶ 정보통신설비 및 시설의 목록(용도 및 위치 등 포함) 작성·관리 여부	해당등급	항목점수	필수항목
점검 항목	1	정보통신망 구성도가 작성되어 관리되고 있는가?	A, B, C	2.5	필수
	2	정보통신설비 및 시설의 목록이 작성되어 관리되고 있는가?	A, B, C	2.5	필수
	3	정보통신망 구성도와 정보통신설비 및 시설 목록은 최신버전이 관리되고 있는가?	A, B, C	2.0	
	4	정보통신설비 및 시설의 목록에는 자산의 형태, 특성, 소유자, 관리자, 용도, 식별번호 및 위치 등이 표시되어 있는가?	A, B, C	2.0	
	5	정보보호설비 및 시설 목록을 통해 자산에 대한 위험 분석을 실시하고 있는가?	A, B	2.0	
참조		The US-CCU Cyber-Security Check List[20] 취약점 분석 평가를 위한 분석 지침[7] 정보보호 관리체계인증[4] 중소기업 정보보호 수준 자가 측정[19]			

〈표 41〉 기술적 보호 : 트래픽 모니터링

2.1.1 트래픽 모니터링					
주요점검내용		▶ 정보통신시설(주요내부노드, 외부망 등)의 트래픽을 24시간 모니터링 하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	네트워크 모니터링 도구를 이용하여 주요내부노드 구간에서 소통되는 트래픽을 상시 모니터링하고 있는가?	A, B	1.5	
	2	네트워크 모니터링 도구를 이용하여 외부망과 연결되는 주요 회선에서 소통되는 트래픽을 모니터링하고 있는가?	A, B, C	2.5	필수
	3	네트워크 트래픽 모니터링 중 이상 징후가 발생해도(해킹시도 또는 시설장애) 서비스를 정상적으로 제공할 수 있는 방안을 가지고 있는가?	A	2.5	필수
	4	네트워크 트래픽 모니터링 중 이상 징후 발생 시 이를 관리자에게 SMS, 메일 또는 경보 등을 통하여 통보하고 있는가?	A, B	1.5	
	5	정보통신시설이 로드 밸런싱을 하도록 구성되어 있는가?	A, B	2.0	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]				

〈표 42〉 기술적 보호 : 무선서비스

2.1.2. 무선서비스 보안					
주요점검내용		▶ 무선서비스(무선랜, 무선인터넷)를 제공할 경우 보안조치가 마련되어 있는지 여부	해당등급	항목점수	필수항목
점검 항목	1	무선서비스를 제공할 때 신뢰할 수 있는 사용자 인증 등의 보안조치를 수행하고 있는가?	A, B, C	2.5	필수
	2	무선서비스를 제공할 때 도청, 전파월경 등에 대한 대책이 마련되어 있는가?	A, B	1.5	
	3	무선서비스를 제공할 때 데이터 보호를 위하여 데이터암호화 등의 보안조치를 수행하고 있는가?	A, B, C	2.5	필수
	4	무선서비스에 대한 보안방법, 수행절차, 사용자 인증, 데이터 암호화, 무선랜 장비관리 등이 기관 내 규정으로 명시되어 있는가?	A	2.0	
	5	무선서비스에 대한 보안대책 및 보안조치가 적절한지 주기적(매월 1회 이상)으로 점검하고 있는가?	A, B	2.0	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]				

〈표 43〉 기술적 보호 : 정보보호시스템 운영

2.1.3. 정보보호시스템 설치 및 운영					
주요점검내용		▶ 정보시스템을 외부망과 연결 시 침입차단/탐지시스템 등의 정보보호시스템을 설치·운영하고 있는지 여부	해당등급	항목점수	필수항목
점검 항목	1	국가기관용의 정보보안 요구사항을 만족하는 인가, 승인된 정보보호제품을 사용하고 있는가?	A, B, C	2.5	필수
	2	외부망과 연결된 모든 구간에 침입탐지시스템(IDS)이 설치·운영되고 있는가?	A, B, C	2.0	
	3	외부망과 연결된 중요 노드에 침입탐지시스템(IDS) 또는 침입차단시스템(IPS)이 설치·운영되고 있는가?	A, B, C	3.0	필수
	4	정보보호시스템이 정보보호시스템 설치로 인한 통신속도 저하 등의 문제가 발생하지 않도록 구성되어 있는가?	A	1.5	
	5	가상사설망(VPN) 또는 바이러스월 등이 설치·운영되고 있는가?	A, B	2.0	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26] 정보보호 관리체계인증[4]				

〈표 44〉 기술적 보호 : 정보보호시스템 보안

2.1.4. 정보보호시스템 보안					
주요점검내용		▶ 정보보호시스템을 설치하였다면, 정보보호시스템이 정상적으로 작동하는지 확인하고 주기적으로 점검하고 있는지 여부	해당등급	항목점수	필수항목
점검 항목	1	정보보호시스템의 이상 징후에 대한 경고 기능이 설정되어 운영되고 있는가?	A, B, C	2.0	
	2	정보보호시스템이 새로 발생하는 공격 기법에 대한 이상 징후를 탐지하기 위해 주기적으로 업데이트되고 있는가?	A, B	1.5	
	3	정보보호시스템의 보안기능 정상작동 여부를 주기적으로(매월 1회 이상)점검하고 있는가?	A, B, C	2.5	필수
	4	정보보호시스템의 로그를 주기적으로(매월 1회 이상) 점검하고 있는가?	A, B	1.5	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]				

〈표 45〉 기술적 보호 : 정보시스템 점검

2.2.1. 정보시스템 취약점 점검					
주요점검내용		▶ 정보시스템의 취약점 점검 주기적으로 실시하고 발견된 취약점을 보완하고 있는지 여부	해당등급	항목점수	필수항목
점검 항목	1	기관 내 취약점 점검과 관련된 규정을 가지고 있는가?	A	1.5	
	2	주기적으로 취약점 점검을 수행하고 있는가?	A, B	2.0	필수
	3	정보시스템에서 발견된 취약점 또는 취약점 점검의 결과가 정보보호책임자에게 보고되고 있는가?	A, B	2.0	
	4	취약점 점검으로 파악된 취약점에 대한 대응책이 적용되고 있는가?	A, B, C	3.0	필수
	5	취약점 점검의 결과가 DB, 보고서 등의 파일로 기록·보관되고 있는가?	A, B, C	2.0	필수
	6	취약점 점검이 정보시스템, 네트워크, DB, 웹 서비스 등 여러 영역으로 나누어져 이루어지고 있는가?	A	1.5	
	7	취약점 점검에 자동화된 도구 등을 사용하고 있는가?	A, B	1.5	
	8	취약점 점검이 외부의 전문 기관에 의해 수행되어 객관성을 확보하고 있는가?	A	1.0	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]				

〈표 46〉 기술적 보호 : 웹 서버

2.2.2. 웹 서버 보안					
주요점검내용		▶ 웹 서버가 안전하게 구성되어있고 관리되고 있는가?	해당등급	항목점수	필수항목
점검 항목	1	웹 서버가 단독 서버로 운영되고 있는가?	A, B	2.0	
	2	취약점이 알려진 서비스들을 웹 서버에서 제거했는가?	A, B, C	2.5	필수
	3	웹 서버가 내부망과 분리된 DMZ에 설치되어 운영되고 있는가?	A	2.0	
	4	침입차단시스템을 통해 웹 서버로의 불필요한 트래픽을 제한하고 있는가?	A, B, C	3.0	필수
	5	웹 서버의 로그를 주기적으로(월 1회 이상) 분석하여 침해사고에 대응하고 있는가?	A, B	1.5	
	6	웹 취약점을 이용한 웹 해킹 등을 점검하고 이를 위한 보안조치를 취하고 있는가?	A	1.5	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]				

〈표 47〉 기술적 보호 : DNS 서버

2.2.3. DNS 서버 보안					
주요점검내용		▶ DNS 서버가 안전하게 구성되어있고 관리되고 있는가?	해당등급	항목점수	필수항목
점검 항목	1	DNS 서버의 CPU 사용률, Memory 사용률, 트래픽 양등을 주기적으로(월 1회 이상) 측정하고 있는가?	A, B	1.5	
	2	DNS 서버가 과부하에 견딜 수 있도록 구성되어 있는가?	A, B, C	1.5	
	3	DNS 서버의 설정 파일과 환경변수들을 정기적으로 백업하고 있는가?	A, B, C	2.0	
	4	DNS 서버가 사고로 사용할 수 없게 되었을 경우 사용할 수 있는 외부 공개 서버를 제공할 수 있는가?	A	2.5	필수
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]				

〈표 48〉 기술적 보호 : DHCP 서버

2.2.4. DHCP 서버 보안					
주요점검내용		▶ DHCP 서버가 안전하게 구성되어있고 관리되고 있는가?	해당등급	항목점수	필수항목
점검 항목	1	DHCP 서버의 CPU 사용률, Memory 사용률, 트래픽 양등을 주기적으로(월 1회 이상) 측정하고 있는가?	A, B	1.5	
	2	DHCP 서버의 부하를 측정하고 부하를 분산하기 위한 방법을 적용시키고 있는가?(이중화 or 로드밸런싱)	A	1.5	
	3	DHCP 사용자 정보와 설정파일과 환경변수들을 주기적으로 백업하고 있는가?	A, B, C	2.0	
	4	사용자별 할당된 IP 주소, Mac 주소, 사용시간 등의 로그를 남기고 있는가?	A, B, C	2.0	
	5	침입차단시스템 등을 사용하여 외부의 DHCP 서버 접근을 차단하고 있는가?	A, B, C	3.0	필수
	6	DHCP 서버의 취약점을 주기적(월 1회 이상)으로 점검하고 있는가?	A, B	1.5	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]				

〈표 49〉 기술적 보안 : DB 서버

2.2.5. DB 서버 보안					
주요점검내용		▶ DB 서버가 안전하게 구성되어있고 적절한 접근제어를 적용하여 운영하고 있는가?	해당등급	항목점수	필수항목
점검 항목	1	DB 서버가 단독 서버로 운영되고 있는가?	A, B	2.0	
	2	취약점이 알려진 서비스들을 DB 서버에서 제거했는가?	A, B, C	3.0	필수
	3	외부망에서 어떠한 사용자도 DB 서버로 직접 접근할 수 없도록 접근제어 되고 있는가?	A, B	3.0	필수
	4	내부망에서 인가된 사용자만이 DB서버로 접근할 수 있도록 접근제어 되고 있는가?	A, B	2.5	필수
	5	웹 서버와 DB 서버는 분리하여 운영하고 있는가?	A, B	1.5	
	6	DB 서버가 내부망과 분리된 DMZ에 설치되어 운영되고 있는가?	A	2.0	
	7	DB 서버로의 접근 및 데이터 변경이 항상 모니터링 되며 로그를 남기고 있는가?	A, B, C	1.5	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]				

〈표 50〉 기술적 보호 : 라우터/스위치

2.2.6. 라우터/스위치 보안					
주요점검내용		▶ 접근제어 기능을 가진 라우터/스위치 장비를 사용하고 있으며 보안기능을 적절히 활용하고 있는가?	해당등급	항목점수	필수항목
점검 항목	1	ACL 등의 접근제어 기능을 가진 라우터/스위치 장비를 사용하고 있는가?	A, B, C	2.0	
	2	라우터/스위치의 접근제어 기능을 이용하여 불필요한 트래픽 및 프로토콜 필터링과 비인가된 사용자의 접속제한을 하고 있는가?	A, B	2.5	필수
	3	취약점이 알려진 서비스를 라우터/스위치에서 제거하였는가?	A, B, C	3.0	필수
	4	라우터/스위치의 기본 계정 및 비밀번호를 제거하고 있는가?	A, B, C	1.5	
	5	라우터/스위치의 펌웨어 업그레이드 및 패치는 주기적으로(월 1회 이상) 수행하고 있는가?	A, B	1.5	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]				

〈표 51〉 기술적 보호 : 접근통제

2.3.1. 접근통제 관리					
주요점검내용		▶ 접근 보안대책을 통하여 비인가된 사용자 및 외부 접속으로부터 안전 여부 확인	해당등급	항목점수	필수항목
점검 항목	1	인가된 접속지로부터 인가된 사용자만이 접속할 수 있도록 통제되고 있는가?	A, B, C	3.0	필수
	2	인가된 사용자만이 정보통신설비에 접속할 수 있는지 주기적으로 점검하고 있는가?	A, B, C	2.0	
	3	외부에서 접속할 경우 신뢰할 수 있는 보안접속을 이용하고 있는가?	A, B	2.0	
	4	접근통제를 위한 프로토콜 외 프로토콜 및 서비스를 차단하고 있는가?	A, B, C	2.5	
참조		국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]			

〈표 52〉 기술적 보호 : 계정 관리

2.4.1. 관리자 및 사용자 계정 관리					
주요점검내용		▶ 관리자 및 사용자 계정 관련 절차 및 규정을 통하여 계정 관리에 관한 보안 조치가 마련되어 있는지 여부	해당등급	항목점수	필수항목
점검 항목	1	관리자 및 사용자 계정 관리에 관한 절차가 규정되어 있는가?	A	2.5	
	2	관리자 및 사용자 계정 발급 시 본인 여부를 파악하는가?	A, B	3.0	필수
	3	관리자 및 사용자 계정의 비밀번호는 적어도 3개월마다 1회 이상 변경되고 있는가?	A, B, C	1.5	
	4	관리자 및 사용자 계정의 비밀번호는 예측할 수 없는 비밀번호를 갖기 위한 방법을 권고하고 있고 그 방법을 제시하고 있는가?	A, B	1.5	
	5	관리자 계정 및 비밀번호에 대한 운영 및 승인 절차가 규정되어 있는가?	A	2.0	
	6	관리자 계정의 비밀번호를 알고 있는 직원이 퇴사할 경우 비밀번호를 즉시 변경하고 이러한 규정이 있는가?	A, B	2.5	필수
참조		국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]			

〈표 53〉 기술적 관리 : 식별 및 인증

2.4.2. 사용자 식별 및 인증					
주요점검내용		▶ 인증시 안전한 메커니즘의 사용과 인증 실패 시 대응 할 수 있는 규정 여부를 통하여 사용자 식별 및 인증의 안전성 조치 여부	해당등급	항목점수	필수항목
점검 항목	1	중요서비스 제공시 사용자 인증을 위해 안전성이 입증된 인증메커니즘을 사용하고 있는가?	A, B, C	3.0	필수
	2	전자서명인증체계를 사용하고 있는가?	A	2.5	
	3	인증 실패 시 대응 행동이 규정되어 있는가?	A, B	2.0	
	4	실패 인증 시도 한계치가 설정되어 있는가?	A, B, C	2.5	필수
	5	인증 시 모든 기록을 유지 관리하고 있는가?	A, B	1.5	
참조		국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]			

〈표 54〉 기술적 관리 : 패치

2.5.1. 패치 관리					
주요점검내용		▶ 정기적인 패치 및 규정을 통하여 보안사고 관련 사전 예방 조치 여부	해당등급	항목점수	필수항목
점검 항목	1	보안패치 설치에 관한 절차 및 규정이 있는가?	A, B, C	2.5	필수
	2	시스템 운영체제 및 중요 프로그램에 관한 보안패치 정보를 주기적으로 통보 및 패치를 시행하고 있는가?	A, B	2.0	
참조		국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]			

〈표 55〉 물리적 보호 : 물리적 보호구역 정의

3.1.1. 물리적 보호구역의 정의와 보안대책 수립 및 이행					
주요점검내용		▶ 특별한 보호가 필요한 시설 및 장비를 보호하기 위한 보호구역이 정의되어 있는지와 이에 따른 보안대책을 체계적으로 수립하여 수행하고 있는지 여부	해당등급	항목점수	필수항목
점검 항목	1	보호구역이 정의되어 있는가?	A, B, C	2.5	필수
	2	보호구역에 따른 보안대책을 수립하였는가?	A, B, C	2.5	필수
	3	보안대책을 등급별로 나눠 각각에 대한 보안대책을 체계적으로 수립하고 수행하고 있는가?	A, B	2.0	
참조		국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26] 정보보호 관리체계인증[4]			

〈표 56〉 물리적 보호 : 물리적 보호구역 접근통제

3.1.2. 물리적 보호구역에 대한 접근통제					
주요점검내용		▶ 물리적 보호구역에 대해 기관의 정책에 명시된 대로 물리적인 접근통제가 잘 수행되고 있는지와 주기적으로 검사하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	물리적인 접근통제에 대한 기관의 정책이 존재하는가?	A, B, C	2.5	필수
	2	물리적인 장비, 문서, 매체의 반출입 절차가 잘 지켜지고 있는가?	A, B, C	2.0	
	3	물리적으로 장비, 문서, 매체의 반출입에 대한 사항을 체계적으로 기록하고 있는가?	A, B, C	2.0	
	4	물리적인 접근통제 수행 내역을 주기적으로 검사하고 있는가?	A	1.5	
참조		국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26] 정보보호 관리체계인증[4]			

〈표 57〉 물리적 보호 : 물리적 보호구역 백업 장치

3.2.1. 물리적 보호구역 내의 자산에 대한 백업 장비 및 시설					
주요점검내용		▶ 물리적 보호구역 내의 자산에 장애가 발생 시, 피해를 최소화하기 위해 신속하게 서비스를 복구하기 위한 백업 장비 및 시설이 등급별로 갖추어져 있는지와 주기적으로 점검하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	백업 장비 및 시설이 갖추어져 있는가?	A, B, C	2.5	필수
	2	백업 장비 및 시설을 등급별로 나누고 있는가?	A, B	2.0	
	3	백업 장비 및 시설을 주기적으로 점검하고 있는가?	A, B, C	1.5	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26] 정보보호 관리체계인증[4]				

〈표 58〉 물리적 보호 : 물리적 보호구역 백업 절차

3.2.2. 물리적 보호구역 내의 자산에 대한 백업 및 복구 절차					
주요점검내용		▶ 물리적 보호구역 내의 자산에 장애가 발생 시, 피해를 최소화하기 위해 신속하게 서비스를 복구하기 위한 백업 장비 및 시설이 등급별로 갖추어져 있는지와 주기적으로 점검하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	백업 및 복구 절차가 있는가?	A, B, C	2.5	필수
	2	백업 및 복구 절차를 등급별로 분류하고 있는가?	A, B	2.0	
	3	백업 및 복구 절차를 주기적으로 테스트하고 있는가?	A, B, C	1.5	
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26] 정보보호 관리체계인증[4]				

〈표 59〉 물리적 보호 : 물리적 보호구역의 위치

3.3.1. 물리적 보호구역의 위치 및 구조					
주요점검내용		▶ 물리적 보호구역의 위치 및 구조가 안전한지와 그에 대한 대책 및 시설이 고려되었는지 여부	해당등급	항목점수	필수항목
점검 항목	1	안전성을 고려하여 물리적 보호구역의 위치 및 구조를 선정하였는가?	A, B, C	3.0	필수
	2	화재나 수재 등으로 인하여 재해 발생 시, 그에 따른 비상대책을 수립하여 수행하고 있는가?	A, B, C	3.0	필수
	3	화재나 수재 등으로 인하여 재해 발생 시, 그에 대비한 안전 장비 및 시설이 갖추어져 있는가?	A, B, C	2.5	
참조	중견기업을 위한 IBM 재해복구서비스[27] 국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26] 정보보호 관리체계인증[4]				

〈표 60〉 물리적 보호 : 물리적 보호구역 장비 폐기

3.3.2. 물리적 보호구역에서 사용하는 장비들에 대한 안전한 폐기 및 정책					
주요점검내용		▶ 물리적 보호구역 내에 사용하는 장비 파기 시, 장비들의 중요 정보가 새어 나가지 않도록 잘 파기하고 폐기 정책 및 절차가 갖추어져 있으며 주기적으로 점검하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	장비 파기에 대한 확인 및 점검이 이뤄지고 있는가?	A, B, C	2.5	
	2	장비 파기에 대한 확인 및 점검 절차 및 정책이 존재하는가?	A, B, C	3.0	필수
	3	파기할 장비에 대해 주기적으로 점검하고 있는가?	A, B, C	1.5	
참조	정보보호 안전진단기준[26] 정보보호 관리체계인증[4]				

〈표 61〉 물리적 보호 : 물리적 보호구역 장비 유지보수

3.3.3. 물리적 보호구역에서 사용하는 장비들에 대한 유지보수 및 관리					
주요점검내용		▶ 물리적 보호구역 내에 사용하는 장비들에 대해서 유지보수 및 관리가 주기적으로 점검되는지 조사	해당등급	항목점수	필수항목
점검 항목	1	물리적 보호구역에서 사용하는 장비들에 대한 유지보수 및 관리 비용이 예산에 잡혀 있는가?	A, B, C	2.5	
	2	물리적 보호구역에서 사용하는 장비들에 대한 유지보수 및 관리 정책이 존재하는가?	A, B, C	3.0	필수
	3	물리적 보호구역에서 사용하는 장비들을 주기적으로 점검하고 있는가?	A, B, C	2.0	
참조	국가사이버안전매뉴얼[23] 정보보호 관리체계인증[4] 정보보호 안전진단기준[26] 중소기업 정보보호 수준 자가 측정[19]				

〈표 62〉 물리적 보호 : 물품 수령 통제

3.3.4. 물품 배달 및 수령에 대한 통제 여부					
주요점검내용		▶ 기관의 직원들에게 오는 물품 배달 및 수령에 대한 통제가 제대로 수행되는지와 기록 및 절차의 여부	해당등급	항목점수	필수항목
점검 항목	1	물품 배달 및 수령에 대한 통제가 제대로 수행되고, 기록 및 관리되고 있는가?	A	2.5	
	2	물품 배달 및 수령에 대한 통제 절차가 체계적으로 수립되어 있는가?	A	3.0	필수
참조	국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26] 정보보호 관리체계인증[4]				

〈표 63〉 물리적 보호 : 전원/통신회선

3.3.5. 전원 공급 및 통신회선 보호					
주요점검내용		▶ 기관의 장비에 공급되는 전원 및 통신회선에 대한 보호대책이 수립되고 주기적으로 검사하는지 여부	해당등급	항목점수	필수항목
점검 항목	1	전원 공급 및 통신회선 보호대책이 수립되어 있는가?	A, B	3.0	필수
	2	기관의 장비에 공급되는 전원 공급 및 통신회선에 대해 주기적으로 검사하고 있는가?	A, B	1.5	
참조	중견기업을 위한 IBM 재해복구서비스[27] 국가사이버안전매뉴얼[23] 정보보호 안전진단기준[26]				

〈표 64〉 항목별 등급에 따른 점수표

분류 \ 등급	A등급		B등급		C등급	
	필수	전체	필수	전체	필수	전체
관리적 보호	76.5	170	69	143.5	50	85.5
기술적 보호	66.5	150	61.5	123	46	68.5
물리적 보호	30.5	60	27.5	53	24.5	42.5

4. 결 론

본 논문에서 제안한 평가 모델은 국내·외 공공기관의 정보보호 수준평가제도 현황을 분석하여 공공기관의 정보보호 수준평가를 위한 관리·기술 대책에 대하여 연구하고 국내 조직에 적합한 정보보호 수준평가 방안을 제시하는 것을 목적으로 하였다. 따라서 공공기관에 특화된 정보보호 수준평가 모델 개발을 위해 공공기관의 등급을 구분하기 위한 기준 산정 및 등급 구분과 정보보호 수준평가 기준을 제시하였다. 이에 따라 기관의 유연한 정보보호 평가를 위해 평가결과를 수치화하여 기관의 등급에 일대일로 대응하는 평가등급의 도출을 목표로 하였다. 예를 들어 A, B, C 등급 중 A 등급이 가장 높은 정보보호 수준의 기관이라 가정할 때, A 등급의 기관이 B 등급의 정보보호 수준을 획득하였다면 해당 기관은 정보보호 수준이 요구되는 정도에 비해 현저히 낮은 수준이며 정보보호 수준 B 등급 이상, 즉 A 등급을 획득하기 위해 위험요소들을 분석하고 이를 제거하기 위한 대책을 수립 및 이행해야 한다. 이를 위한 기초 연구로 국내 정보보호 인증제도인 정보보호 관리체계, 보안성 평가 및 평가인증, 정보통신기반보호, 정보보호 안전진단제도, 정보보호 수준평가 방법론에 대해서 분석하고, 국외 제도로써 영국의 BS7799, 독일의 IT 베이스라인 보호매뉴얼, 일본의 정보보호 관리체계, 미국의 DITSCAP의 세부적인 절차와 방법론을 살펴보았다. 또한 분석한 자료를 비교함으로써 이를 우리나라 공공기관에 어떻게 적용할지에 대해 살펴보고, 새로운 정보보호 수준평가를 위한 모델 개발을 위해 어떠한 절차와 기준이 필요한지에 대해서 분석하였다. <표 65>는 기존 제도와 본 논문에서 제안한 공공기관에 특화된 정보보호 수준평가 모델을 비교·분석한 것이다. 본 평가 모델은 공공기관이 정보보호 목표를 효율적이고 효과적으로 달성할 수 있게 있고, 정보보호 능력 검증을 통해 공공기관의 신뢰도를 향상시킬 수 있을 것이다. 또한 정보보호 수준 개선을 위한 방법론으로도 활용 가능할 것이다.

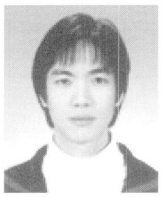
〈표 65〉 기존 제도와 새로운 모델의 비교

구분	정보보호 관리체계	영국 BS7799	미국 DITSCAP	보안성 평가 및 평가인증	새로운 모델
기술적 측면	보통	불충분	충분	충분	충분
관리적 측면	충분	충분	불충분	불충분	충분
자산의 사전평가 여부	불충분	불충분	충분	충분	충분
상호협의기준 문서	없음	없음	존재 (SSAA)	존재 (PP or ST)	존재

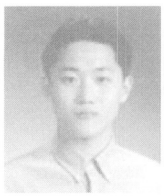
참 고 문 헌

[1] 한국정보보호센터, *정보보호평가기준개발*, 1999.
[2] 한국정보보호진흥원, *정보보호 관리체계인증 동향*, 2002.
[3] 한국정보보호진흥원, *정보보호관리기술 동향 및 사례 연구 연구보고서*, 2001.
[4] 한국정보보호진흥원, *정보보호 관리체계인증*, 2004.
[5] Common Criteria, http://www.commoncriteriaportal.org.
[6] 한국정보보호진흥원, http://www.kisa.or.kr.
[7] 한국정보보호진흥원, *취약점 분석 평가를 위한 분석 지침*, 2004.
[8] 한국정보보호진흥원, *정보보호 안전진단기준*, 2004.
[9] 한국정보보호진흥원, *정보보호 수준평가방법론*, 2006.
[10] BSI, *BS7799 Part 1: Code of Practice for Information Security Management, British Standards Institute*, 1999.
[11] BSI, *BS7799 Part 2 revised version: Specification for Information Security Management Systems British Standards Institute*, 2002.
[12] BSI, *IT Baseline Protection Manual*, 2000.
[13] Japan Information Processing Development Corporation, http://www.jipdec.or.jp/
[14] Japan Conformity Assessment Scheme for Information Security ManagementSystems, http://isms.jipdec.or.jp/en/
[15] Assistant Secretary of Defense for Command, Control, Communications and Intelligence, *DoD Information Technology Security Certification and Accreditation Process*, 1997.
[16] Assistant Secretary of Defense for Command, Control, Communications and Intelligence, *DITSCAP Application manual*, 2000.
[17] DITSCAP online, http://iase.disa.mil/ditscap/Ditscap Frame.html/
[18] 한국정보보호진흥원, *취약점 분석 평가 모델*, 2004.
[19] 한국정보보호진흥원, *중소기업 정보보호 수준 자가 측정*, 2007.
[20] U.S Cyber Consequence Unit, *The US-CCU Cyber-Security Check List*, 2007.
[21] 한국정보보호진흥원, *정보보안점검항목*, 2001.

[22] Japan Information-Technology Promotion Agency, *기업의 정보보호 거버넌스 본연의 자세에 관한 연구회 보고서*, 2006.
[23] 국가사이버안전센터, *국가사이버안전매뉴얼*, 2005.
[24] 한국전산원, *정보시스템 장애관리 지침*, 2005.
[25] 한국전산원, *전산감리 효과 연구*, 1995.
[26] 한국정보보호센터, *정보보호 관리기준*, 2001.
[27] IBM, *중견기업을 위한 IBM 재해복구서비스*, 2005.



허 순 행
e-mail : shhur@security.re.kr
2007년 성균관대학교 정보통신공학부 (학사)
2007년~현 재 성균관대학교 대학원 전자전기컴퓨터공학과 석사과정
관심분야 : 정보보호, 보안성 평가 등



이 광 우
e-mail : kwlee@security.re.kr
2005년 성균관대학교 정보통신공학부 (학사)
2007년 성균관대학교 대학원 전자전기 컴퓨터공학과(공학석사)
2007년~현 재 성균관대학교 대학원 전자전기 컴퓨터공학과 박사과정
관심분야 : 암호이론, 정보보호, 네트워크 보안, 전자투표, 워터마킹

조 혜 숙
e-mail : hsjo@security.re.kr
2003년 한성대학교 멀티미디어정보처리과 (학사)
2005년 성균관대학교 대학원 전자전기 컴퓨터공학과(공학석사)
2006년~현 재 성균관대학교 대학원 전자전기 컴퓨터공학과 박사과정
관심분야 : 정보보호, 보안성평가, 무선네트워크

정 한 재
e-mail : hjjeong@security.re.kr
2006년 성균관대학교 정보통신공학부 (학사)
2008년 성균관대학교 대학원 전자전기 컴퓨터공학과(공학석사)
2008년~현 재 성균관대학교 대학원 전자전기 컴퓨터공학과 박사과정
관심분야 : 정보보호, 보안성평가, 무선네트워크

전 웅 렬
e-mail : wrjeon@security.re.kr
2006년 성균관대학교 정보통신공학부 (학사)
2008년 성균관대학교 대학원 전자전기 컴퓨터공학과(공학석사)
2008년~현 재 성균관대학교 대학원 전자전기 컴퓨터공학과 박사과정
관심분야 : 보안성평가, 데이터베이스 보안

원 동 호
e-mail : dhwon@security.re.kr
1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1985년~1986년 일본 동경공업대 객원연구원
1988년~2003년 성균관대학교 교학처장, 전기전자 및 컴퓨터 공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년 국무총리실 정보화추진위원회 자문위원
2002년~2003년 한국정보보호학회장
2002년~현 재 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원
현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, 정보통신대학원장
관심분야 : 암호이론, 정보이론, 정보보호

김 승 주
e-mail : skim@security.re.kr
1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년 한국정보보호진흥원(KISA) 팀장
2004년~현 재 성균관대학교 정보통신공학부 부교수
2001년~현재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년~현 재 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년~현 재 교육인적자원부 유해정보차단 자문위원, 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
2007년~현 재 대검찰청 디지털수사 자문위원, KISA VoIP 보안기술 자문위원, 기술보증기금 외부 자문위원, 전자정부서비스보안위원회 사이버침해사고대응 실무위원회 위원
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET