情報保護學會論文誌
第20卷 第2號, 2010. 4

민간기업과 공공기관의 정보보호 관리체계 차이 비교

김 지 숙,† 이 수 연, 임 종 인‡
고려대학교 정보경영공학전문대학원

Comparison of The ISMS Difference for Private and Public Sector

Ji-sook Kim,† Soo-yeun Lee, Jong-in Lim‡
Korea University, Graduate School for Information Management Engineering

요 약

정보보호 관리체계 구축을 지원하기 위해 민간기업 대상으로는 "정보통신망 사용 촉진 및 정보보호 등에 관한 법률"에 근거하여 한국인터넷진흥원이 인증하는 ISMS제도가 있으며 공공기관 대상으로는 아직 인증제도는 없으나 "전자정부법"에 근거하여 국가정보원이 '정보보안 관리실태 평가제도'를 운영하고 있다. 본 논문에서는 민간부문과 공공부문에서 시행하고 있는 정보보호 관리체계 통제항목에 대한 비교와 함께 그간 실시한 평가 미흡사항을 분석하여 이를 토대로 효율적인 정보보호 관리체계 구축방안을 살펴보고자 한다.

ABSTRACT

To support the establishment of Information Security Management System, the private sector and the public sector have taken some measures. In the private sector, KISA(Korea Internet & Security Agency) has certified ISMS system based on "The Act on Communication Network Use Promotion and Information Security etc.". In the public sector, No authentication system has been established. Instead, NIS(National Intelligence Service) has enforced 'Information Security Management Condition Evaluation' based on "Electronic Government Act". This article compared ISMS control parts of the private sector with that of the public sector and analyzed the non-enforcement parts of ISMS implementing two sectors for years. Based on this, I would like to consider the method of establishment for efficient ISMS.

Keywords: Information security, Information security management system, Information security management condition evaluation

I. 서 론

정보통신 네트워크가 집적화·고도화됨에 따라 해킹 피해, 개인정보 유출 등 정보침해 사고가 증가 일로에 있다. 이에 대해 민간 및 공공부문은 시스템에 대한 투자를 확대하고 있지만 사고를 막기에는 역부족이다. 첨단화·지능화 되어가는 정보통신망에 대한 보안위협에 대처하는 최선의 방법은 정보보호를 체계적이면서 지속적으로 수행하는 것이다. 최근 정보보호 관리체계 방법론에 대한 관심이 커지고 있는 것도 이를 반영한 것이라 볼 수 있다.

조직은 각각의 목적과 특성, 운영방식이 있다. 어떤 제도가 민간 기업에게 효율적일지라도 공공기관에 그대로 적용하기 곤란한 측면이 있으며 그 반대의 경우도 있을 것이다. 정보보호도 마찬가지이다. 정보시스템에 대한 기밀성, 무결성, 가용성을 확보한다는 목적은 같지만 수행방법에 있어서는 어느 것을 우선순위에 둘 것인지, 어떤 방법을 사용할 것인지는 차이가 있을 수 있다. 특히 공공기관은 독립된 특수목적의 정보통신시스템을 운영하거나 국가안보와 관련된 데이터베이스를 암호화하여 운용하는 등 별도의 보호 정책을

접수일(2009년 11월 15일), 게재확정일(2010년 2월 2일)
† 주저자, scales12@korea.ac.kr
‡ 교신저자, lsyeon@empal.com

적용해야 할 필요가 있다.

정보보호를 위한 절차와 과정을 체계적으로 수립하여 지속적으로 관리·운영하는 정보보호 관리체계(Information Security Management System, ISMS)는 모든 영역에서 필요하며 효율적으로 이행되어야 한다. 하지만 민간영역과 공공영역은 그 특성이 다르므로 관리체계를 동일하게 적용할지, 아니면 별도의 체계로 운영할 지에 대해서는 많은 검토가 필요하다.

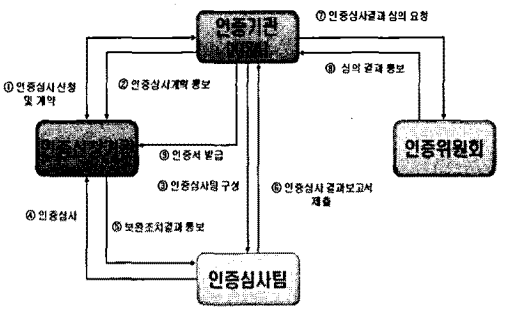
본 논문에서는 민간영역과 공공영역의 정보보호 관리체계 평가 제도를 비교해 보고 그간 실시한 결과에서 나타난 양 영역의 정보보호관리 실태의 미흡사항을 분석하여 문제점과 개선방향 제시를 통해 효율적인 정보보호 관리체계 확립 방안을 마련하기 위한 연구의 밑거름이 되고자 한다.

II. 민간기업 정보보호 관리체계 인증제도

2.1 개 요

정보화 역기능으로 인해 기업 손실이 늘어나자 많은 기업들이 정보보호 활동을 사업수행의 지원요소가 아니라 사업목표를 달성하기 위한 핵심요소로 인식하기 시작하였다. 이에 영국(BS7799, 1998년)을 필두로 독일(IT Baseline Protection Qualification, 2001년), 싱가포르(Singapore Standard), 일본(ISMS 적합성 평가제도, 2002년) 등에서 정보보호 관리체계 인증 제도를 도입하였다[1]. 하지만 나라마다 상이한 인증제도는 상호 호환을 어렵게 함에 따라 국제 표준화 필요성이 제기되어 2005년 국제표준화기구(ISO)와 국제전기기술위원회(IEC)가 영국의 BS7799를 보완, ISO/IEC 27000 시리즈를 국제표준으로 채택하였다. 27001은 PDCA (Plan-Do-Check-Act) 프로세스에 의한 정보보호 요구서에 해당되며, 27002는 정보보호 관리를 위한 실행지침서이다. 27003은 PDCA에 대한 실행지침서이며, 27004는 정보보호 매트릭스와 측정에 관한 표준이고, 27005는 위험관리에 대한 표준이다(이중 27004와 27005는 현재 draft 상태이다)[2].

우리나라도 정보통신망에 대한 예방중심의 체계적이고 지속적인 정보보호 관리모델이 필요하게 되었고 기업에서 자율적으로 높은 수준의 보호조치를 취할 수 있는 제도가 요구되었다. 이에 '정보통신망 이용 촉진 및 정보보호 등에 관한 법률' 제47조에[3] 근거하여



[그림 1] 인증절차 기본 흐름도

'02.7 정보보호 관리체계 인증제도가 도입되었으며 한국인터넷진흥원(KISA)이 민간기업을 대상으로 인증서를 심사·발급하며 2009.12월까지 발급된 인증서는 77건에 이른다[4].

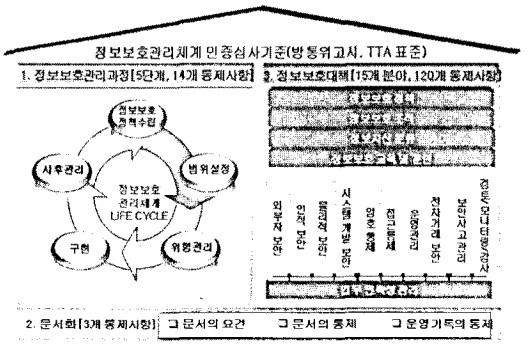
2.2 정보보호 관리체계 인증 절차 [5]

인증을 원하는 기업은 조직 전체 또는 조직단위별, 지역별, 시스템별로 인증범위를 선정하여 인증기관에 심사를 신청한다. 인증기관은 신청기관에 대해 인증심사를 실시한 후 인증위원회의 심의를 받아 인증서를 발급하는데 신청부터 인증서 발급까지 3개월이 소요된다. 인증절차는 [그림1]과 같다.

인증절차는 준비→심사→인증→사후관리의 4단계로 나뉜다. 준비단계는 신청서류를 접수하고 부족한 서류 보완 및 심사 계획에 대한 협의 단계이다. 심사단계는 제출문서를 검토하는 서면심사와 네트워크·시스템 취약점 점검, 보호대책 수립과 이행여부 확인 등의 기술심사가 있다. 인증단계는 심사보고서 작성과 인증위원회의 심사결과에 대한 검토 및 심의를 거쳐 결과를 통보하고 인증서를 교부하는 단계이다. 인증서 유효기간은 3년이다. 마지막으로 사후관리 단계는 인증 유지 상태를 매년 1회 확인하는 사후관리 심사와 재심사 및 갱신심사가 있다. 재심사는 인증을 받은 정보보호 관리체계 범위 내에서 중대한 변경이 발생한 경우에 하는 심사이며 갱신심사는 유효기간 만료시 유효기간 연장을 위해 받는 심사이다.

2.3 정보보호 관리체계 인증 심사기준 [6]

ISMS 인증심사 기준은 방송통신위원회(舊 정통부)가 2002.2월 고시하였고 필수사항인 관리과정 14개 항목, 문서화 요구사항 3개 항목과 선택사항인 정



〔그림 2〕 정보보호 관리체계 구성요소

보보호 대책 120개 항목 등 총 137개로 구성되어 있으며 〔그림2〕와 같다. 인증 신청기업은 137개 심사기준의 요구사항을 충족하여야 인증을 받을 수 있다.

ISMS는 정보보호 정책수립→정보보호 관리체계 범위 설정→위험관리→구현→사후관리의 라이프사이클을 가지고 있다. 정보보호 관리과정은 여기에 해당되는 5단계 14개 통제항목으로 구성되어 있다. 문서화 요구사항은 3개 통제항목으로 정보보호 관리체계를 수립하고 이행관련 내용을 문서화하는 문서요건과 문서관리 통제에 대한 절차 수립 및 문서 통제, 정보보호 관리체계 운영기록 절차 수립, 유지관리에 대한 운영기록의 통제가 요구된다. 정보보호 대책은 정보보호 관리체계의 세부 통제항목으로 15개 분야 120개 항목으로 구성된다.(부록 표 1 참조)

2.4 정보보호 관리체계 인증심사 판정

137개 통제항목 각각에 대해 심사를 실시하여 인증심사 기준에 규정된 요구사항을 충족할 경우에는 '적합' 판정을 하고, 인증심사 기준을 충족하지 못하는 사항에 대해서는 발견된 문제점이 정보보호 관리체계에 미치는 영향에 따라 '중결함' 또는 '결함' 판정을 하며, 요구사항을 충족하지 않아 인증을 부여할 수 없을 때는 '부적합'으로 판정한다. '중결함'과 '결함' 사항에 대해서는 신청인에게 보완 조치토록 하고 그 결과에 대해 적합 여부를 결정한다.

ISMS 인증서를 취득한 기업은 내부적으로 직원들의 정보보호 마인드 변화, 정보보호 활동에 대한 자생력 확보, 자체 보안관리체계 수립방법 습득 및 능력 배양, 고객 신뢰성 제고 및 기업 이미지 제고 등의 효과가 있는 것으로 나타났으며〔7〕 외적인 면에서는 인증서를 취득한 해에는 정보보호 안전진단이 면제되고 신용평가기관의 기업 신용평가시 가점이 부여되며 중소기업에 대한 정부예산 지원업체 선정시 가산점 부여 등의 인센티브가 주어진다〔8〕.

III. 공공기관 정보보호 관리체계 운영 실태

3.1 개 요

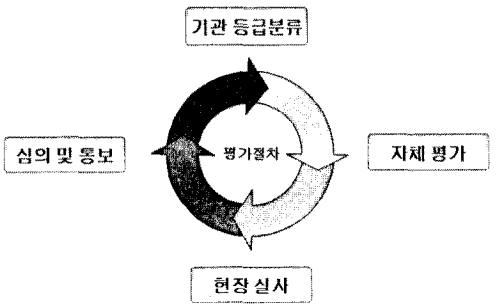
영국, 독일, 일본 등은 민간·공공영역에 동일한 ISMS 인증제도를 적용하고 있다. 특히 일본의 "ISMS 적합성 평가제도"는 영국의 BS7799와 동일하여 1회의 심사로 2개의 인증서가 발급된다〔1〕. 반면 미국, 캐나다 등의 국가는 공공영역과 민간영역에 대해 각각 다른 인증제도를 운영하고 있다. 미국은 연방 정보보호 관리법(FISMA)을 제정하고 2002.12 표준기술원(NIST)이 개발한 정보보호관리 표준에 의해 예산관리국(OMB)이 매년 81개 연방정부기관을 심사한다. 심사결과는 "통과 또는 탈락" 형태가 아닌 미흡한 부분을 보완하고 결과를 예산에 반영하는 방식이다〔9〕.

우리나라는 전자정부법 제 27조 제3항(정보통신망 등의 보안대책 수립·시행)〔10〕 동법 시행령 제 35조(전자문서의 보관유통 관련 보안조치) 및 제 36조(이행여부 확인), 공공기록물 관리법 시행령 제 5조(전자기록물 보안관리)〔11〕에 의거하여 국가정보원이 공공기관 대상으로 '정보보안 관리실태 평가'를 실시하고 있다. 동 제도는 해당기관의 정보통신시스템에 대한 인증이 아니라 보안관리 체계가 제대로 구축, 운영되는지 실태를 확인하고 미흡한 부분은 보완 및 보안대책을 지원하는 형식으로 운영되고 있으며 미국의 FISMA와 유사한 방식이다. 국정원은 2007년 99개 국가·공공기관 대상 최초 평가를 실시한데 이어 2008년에는 117개 기관에 대해 평가를 실시하였다.

3.2 정보보안 관리실태 평가 절차 〔12〕

정보보안 관리실태 평가는 기관 보안등급 분류→평가항목 자체평가→ 자체평가 내용 현장실사→ 평가결과 심의·통보의 4단계로 구분된다. 이는 〔그림3〕과 같이 나타낼 수 있다. 평가 결과를 토대로 미비점 개선 및 기관 실정에 맞는 보안대책이 지원된다.

먼저, 기관의 보안등급은 수행업무의 중요도, 정보시스템, 피해에 따른 영향력 등에 해당하는 14개 평가요소에 따라 가·나·다급으로 분류한다. 가급기관은 매



〔그림 3〕 정보보안 관리실태 평가 절차

우 높은 수준의 보안관리가, 나급 기관은 높은 수준의 보안관리가, 다급 기관은 보통 수준의 보안관리가 요구되는 기관이다.

2단계는 국가정보원이 마련한 평가항목에 대해 각 기관이 자체평가를 실시한다. 국가정보원은 ISO/IEC 27002를 토대로 한 평가항목에 보안환경 변화를 고려하여 매년 새로운 평가항목을 제시한다.[1] 공공기관 평가를 처음 실시한 2007년도에는 분야별 보안정책과 관련규정 보유여부에 중점을 두어 9개 분야 246개 항목을 제시하였다. 2008년도 평가항목에는 전년도 평가결과를 반영하여 거의 모든 기관이 시행하고 있는 항목은 제외하고 신규 취약점 점검항목을 추가하여 8개 분야 135개 항목을 제시하였다.[2] 평가항목 8개 분야는 정책 및 업무수행, 정보자산 관리, 비밀관리, 인적보안, 침해사고 대응체계 구축, 접근보안, 운영관리, 물리적 보안으로 구성되어 있다.(부록 표 2 참조)

3단계는 민·관 전문가 합동으로 현장 실사를 실시하여 자체평가 결과와 관련된 증빙자료를 확인한다.

4단계는 평가위원회의 심의를 거쳐 최종결과를 기관에 통보한다. 여기에는 평가점수와 함께 항목별 미비점 및 개선대책이 포함되며 취약기관 대상으로 보안컨설팅을 지원한다. 또한 평가결과는 국무총리실(중앙행정부처), 행정안전부(지자체)의 '기관 업무평가'에 반영되고 있다.

IV. 민간〔13〕·공공영역〔14〕 ISMS 비교

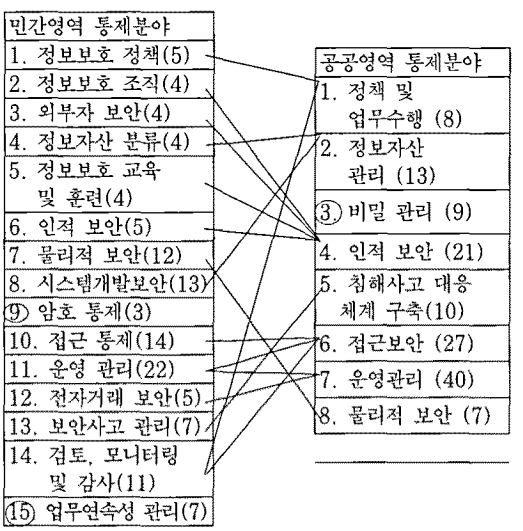
이 장에서는 민간영역과 공공영역의 정보보호 관리체계를 비교하고자 한다. 비교분석 프레임은 양 영역의 통제항목에 대한 매핑을 실시하는 방식을 취할 것이며 이를 통해 영역별 특성을 알아보고자 한다.

한국인터넷진흥원이 수행하는 ISMS 인증제도는 필수사항인 관리과정 14개 항목과 문서화 요구사항 3개 항목 및 선택사항인 정보보호 대책 120개 항목으로 구성되어 있다. 이 중 정보보호 관리체계의 세부 통제항목인 15개 분야 120개 항목을 2008년도 국가정보원이 공공기관 대상으로 실시한 정보보안 관리실태 평가항목 8개 분야 135개 항목과 비교하였다. 세부 통제항목 내용은 본 논문 끝부분에 별도 수록하였다.

매핑 결과, 민간영역에서는 공공영역에서 시행하고 있는 비밀관리 분야에 대한 대책이 포함되어 있지 않으며 공공영역에서는 암호통제와 업무 연속성 관리에 대한 평가가 이루어지지 않는 것으로 확인되었다.

민간영역 120개 항목 중 공공영역 평가항목과 일치하는 항목은 97개(81%)이며 공공영역 135개 항목 중 민간영역 심사항목과 일치하는 항목은 108개(80%)로 나타나 민간영역과 공공영역의 정보보호 관리체계에 있어 약 80%가 일치하고 20%만이 차이가 있는 것으로 확인되었다.

세부 통제항목을 비교한 결과, 민간영역의 정보보호 정책, 조직, 외부자 보안, 정보자산 분류, 교육 및 훈련, 인적 보안, 시스템 개발 보안, 보안사고 관리 항목은, 통제 분야에 대한 분류가 공공영역과 동일하지



〔그림 4〕 민간영역과 공공영역 정보보호관리 통제항목 매핑도

1) 이 부분이 민간영역의 정보보호 관리체계 인증제도와 가장 큰 차이점이라 할 수 있다. 민간영역에서는 고정된 통제항목을 제시하고 있지만 공공영역은 정보통신 환경 및 국가 보안정책의 변화상을 적시 반영하여야 하기 때문이다.

2) 본 절에서는 2008년도 평가항목 중심으로 서술하고자 한다.

〔표 1〕 민간과 공공영역 통제항목 유형

구분	공공영역		민간영역	
	항목수	비율 (%)	항목 수	비율 (%)
전체 항목 수	152	—	133	—
WKA대응항목	36	23.69	17	12.78
UKA대응항목	17	11.18	13	9.77
해당없는 항목	99	65.13	103	77.44

않아도 통제 목적과 통제 내용이 유사하여 큰 차이를 보이지 않은 것으로 나타났다.

반면, 접근 통제 분야 중 네트워크·운영체제·응용프로그램·데이터베이스에 대한 접근 통제, 물리적 보안 분야 중 사무실 보호, 운영관리 분야 중 운영절차의 문서화 및 시스템 보안, 전자거래 보안 분야 중 교환합의서 및 전자거래 보안관리·이용자 공지사항, 검토·모니터링 및 감사 분야의 법적 요구사항 준수 검토 등은 공공영역과 부분일치 하는 것으로 확인되었다.

한편, 공공영역의 보안관리 평가 항목 중에는 정책 및 예산 등의 정보보안 계획과 기관장 관심도 등을 파악하는 정보보안 업무수행, 운영관리 분야의 정보통신기기 관리 항목은 민간영역과는 차별을 나타내어 공공의 특성이 반영된 것으로 보인다.

또한, 민간영역과 공공영역의 정보보호 관리체계에 대한 통제내용 중 평가방법이 프로세스를 평가하는지 아니면 이행여부 자체만을 평가하는지 분석한 결과, 민간영역에서는 120개 통제항목 중 39개(32%)가 이행여부를 확인하고 81개(68%)는 통제사항에 대한 프로세스를 확인하는 것으로 나타났으며, 공공영역에서는 135개 항목 중 61개(45%)가 이행여부를 확인하고 프로세스에 대한 평가는 74개(55%)인 것으로 나타나 민간영역의 정보보호 관리체계가 프로세스에 더 치중하고 있는 것으로 확인되었다.

나아가, 민간영역과 공공영역 각각의 통제항목이 알려진 공격(Well Known Attack, WKA)에 대응하기 위한 통제 사항인지, 알려지지 않은 공격(Un Known Attack, UKA)에 대응하기 위한 통제 사항인지를 분석한 결과는 〔표1〕과 같았다.

〔표1〕에서 각 영역별 전체 통제항목 수가 늘어난 것은 알려지지 않은 공격에 대응하는 통제항목이 알려지지 않은 공격에 대응하기 위한 통제사항과 함께 알려진 공격에 대응하기 위한 통제사항도 포함하고 있어 중복되기 때문이다.

〔표1〕에서 보는 것처럼 공공영역의 통제항목에는 알려진 공격에 대응하는 통제항목이 23.69%이며 알려지지 않은 공격에 대응하는 통제항목이 11.18%로 전체 34.87%의 통제항목이 공격에 대응하는 항목이다. 민간영역은 알려진 공격에 대응하는 통제항목이 12.78%이고 알려지지 않은 공격에 대응하는 통제항목이 9.77%로 전체 22.55%의 통제항목이 공격에 대응하는 항목으로 나타나, 사이버 공격에 대응하기 위한 통제항목은 공공영역이 민간영역보다 12.32% 더 많은 것으로 확인되었다.

V. 민간·공공영역 ISMS 평가결과 분석

5.1 민간영역 결함항목 분석〔15〕

민간기업 대상의 ISMS 인증 심사에서 도출된 결함사항에 대한 분석은 고규만, 김재성, 장상수의 "ISMS 구축시 일반적으로 나타나는 결함사례에 관한 분석"(정보보호 학회지 제 17권 제 4호, 2007.8)의 내용을 인용한다. 여기서는 2002.1~2007.8간 정보보호 관리체계 인증을 취득한 33개 업체를 대상으로 최초 인증심사, 1·2차 사후관리 심사, 갱신 심사에서 발견된 전체 결함사항과 세부 통제항목별로 발생빈도가 높은 결함사항을 분석한 것이다.

5.1.1 인증심사별 결함사항

최초 인증심사, 1·2차 사후관리 심사, 갱신심사별 결함수를 조사한 결과는 〔표2〕와 같았다. 표를 보면 최초 인증심사 때보다 1차·2차 사후관리 심사시 업체당 결함 수가 현저히 줄어든 것을 볼 수 있다. 이는 인증을 취득한 업체가 지속적으로 정보보호 관리체계를 운영함으로써 업체의 정보보호 수준이 향상되었음을 보여주는 것이라 볼 수 있다. 다만, 유효기간 연장을 목적으로 하는 갱신심사의 경우 업체당 결함수가 다소 증가한 것은 갱신심사시 인증범위가 확대·변경되어 신규 결함수가 증가되었기 때문으로 분석된다.

다음은 정보보호 관리체계 수립 후 개선효과를 객

〔표 2〕 정보보호 관리체계 인증심사별 결함수

심사 구분	업체 수	총 결함수	업체당 결함수
최초 인증심사	33개	574건	17.4건
1차 사후관리 심사	25개	150건	6건
2차 사후관리 심사	15개	83건	5.5건
갱신 심사	6개	52건	8.7건

〔표 3〕 정보보호 관리체계 결함 개선율 비교

구 분	최초 인증심사	1차 사후관리심사	2차 사후 관리심사
전체 결함수	243건	94건	83건
업체당 결함수	16.2건	6.3건	5.5건

관적으로 분석하기 위해 인증 유효기간 3년에 걸쳐 최초인증심사, 1·2차 사후관리심사를 모두 수행한 15개 업체들의 결함수를 비교해 보고 결함 개선율을 확인한 결과, 〔표3〕에서처럼 사후관리 심사에서는 최초인증심사시보다 매년 결함수가 줄어들고 있음을 알 수 있다. 즉, 1차 사후관리 심사에서는 최초인증심사 결함수 243건보다 61%가 감소한 94건이 발견되었으며 2차 사후관리 심사에서는 1차 사후관리 심사 결함수 94건보다 12%가 감소한 83건의 결함이 발견되었다. 이는 기업들이 최초심사에서는 정보보호 관리체계 수립운영에 관한 경험 부족으로 결함이 많이 발견되나 향후 지적된 결함을 보완하고 지속적으로 관리함으로써 사후관리 심사에서는 결함수가 현저히 줄어들고 있는 것으로 분석된다.

5.1.2 세부 통제항목별 결함수

최초 인증심사 33회, 1·2차 사후관리 심사 40회, 갱신심사 6회 등 총 79회에 걸친 인증심사에서 발견된 결함을 분석한 결과, 상위 10위에 해당하는 결함발생율을 보인 세부 통제항목은 〔표4〕와 같다. 결함발생빈도는 아래와 같이 계산하며 이는 인증심사시 137개 세부 통제항목별로 얼마나 자주 결함사항이 발견되었는지를 나타낸다.

결함발생 빈도 = 발견된 총 결함수/인증심사 횟수

세부 통제항목 중 결함 발생빈도가 가장 높은 것, 즉 항목에 규정된 요구사항을 충족하지 못한 1위는 백업 및 복구관리로 나타났으며 이는 기업들이 사전에 시스템 장애 및 재해를 대비하는데 소홀하다는 것을 알 수 있다.

두 번째로 잘 지켜지지 않는 항목은 정보자산에 대한 보안등급 표시 및 취급절차이며 3위는 시스템에 대한 사용자 접근권한 관리로 주요시스템을 공동계정으로 사용하거나 사용자 계정 등록 및 해지 절차가 잘 지켜지지 않고 신규 사용자계정 발급에 대한 책임자의 승인 누락, 사용자 권한 변경내역에 대한 주기적인 점검이 미흡한 것으로 나타났다.

그 다음으로는 정보자산 분류와 변경관리 및 보안

〔표 4〕 세부 통제항목별 결함수 비교

순위	세부 통제사항	통제 내용	결함 건수	발생 빈도
1	백업 및 복구 관리	데이터·장비의 무결성과 가용성을 유지하기 위해 백업계획을 수립·이행하고 사고발생시 적시 복구할 수 있도록 관리한다.	34	43%
2	정보 자산 보안 등급과 취급	중요도에 따라 분류된 정보자산에 보안등급을 부여하고 물리적·전자적 보안등급 표시를 부착 관리하며 보안등급의 부여에 따른 취급절차도 정의하여 이행한다.	23	29%
3	시스템 사용자 등록	정보시스템 및 서비스에 대한 접근을 통제하기 위한 공식적인 사용자 등록 및 해지절차를 마련한다.	19	24%
4	정보 자산 분류	정보자산이 기관에서 차지하는 가치와 기관에 미치는 영향을 고려하여 분류방식을 선택하고 분류한다.	18	23%
5	정보 자산 변경 관리	정보시스템 관련 자산들을 조사하고 모든 변경사항을 반영할 수 있는 공식적인 관리책임과 절차를 수립한다.	18	23%
6	보안 사고 대응 계획 수립	보안사고의 정의 및 범위, 긴급 연락체계 구축, 사고 발생시 보고 및 대응절차, 사고 복구조직 구성, 교육계획 등을 포함한 보안사고 대응계획을 수립, 이행한다.	18	23%
7	정보 보호 교육시행 및 평가	교육·훈련은 정기적으로 실시하며 정보보호 정책, 절차, 역할에 변경이 있는 경우는 수시 실시하고 기록을 남긴다. 교육훈련 종료후 검토를 통해 차기 교육에 반영한다.	17	22%
8	물리적 보호 구역	물리적 보호구역 출입은 적절한 출입통제절차에 의하여 통제되고 출입자를 식별하고 기록, 관리한다.	16	20%
9	업무 연속성 계획 시험	환경 변화나 부정확한 전제 등으로 인한 오류를 제거할 수 있도록 지속적인 시험을 수행하며 시험계획에는 시기, 방법, 절차 등을 포함한다.	16	20%
10	위험 분석	식별된 정보자산에 영향을 줄 일 수 있는 모든 위협, 취약성, 위험을 식별하여 분류하며 정보자산의 가치와 위험을 고려하여 잠재적 손실의 영향을 식별, 분석한다.	15	19%

사고 대응계획 수립 항목으로 모두 23%의 결함 발생 빈도를 갖고 있는 것으로 나타났는데 정보자산 분류와 관련된 주된 결함은 정보자산 분류기준 부재, 정보자산 분류기준에 부합하지 않는 정보자산 관리, 전자정보와 문서자산의 정보자산 분류 누락 등이 발견되며 정보자산 변경관리와 관련하여서는 절차의 부재 및 절차준수 미흡, 변경에 대한 정식 승인절차 미준수 등이 지적되었다.

보안사고 대응계획 수립과 관련된 결함으로는 해킹, 웜·바이러스 등에 의한 보안사고 발생시 긴급 연락체계 작성 미흡, 보안사고 중요도에 따른 보고라인 및 처리방법 부재 등이 문제시 되었다.

다음으로는 정보보호 교육 시행 및 평가 항목으로 기업들이 연간 정보보호 교육계획서를 작성하지 않으며 교육 후 참석자 서명·강사 평가 등 기록관리가 미흡하고 교육 및 훈련내용에 대한 효과 측정 및 분석절차를 누락하는 것으로 나타났다.

그 다음으로 잘 지켜지지 않는 항목은 물리적 보호구역 분야로 물리적 보호구역 구분 및 정의 누락, 물리적 보호구역 경고표시 미부착, 물리적 보호구역 내 장비·문서·매체 반출입 절차 부재 등이 문제시 되었다.

결함 발생빈도가 9위인 업무 연속성 계획 시험분야에서는 시험계획에 필요한 시기·방법·절차 등이 구체화되지 않으며 시험실시 후 결과에 대한 반영이 미흡할 뿐 아니라 시험계획에 따라 주기적으로 시험을 시행하지 않는 것으로 나타났다.

마지막으로 위험분석 분야에서는 위험분석 범위 내에 고객정보 등 중요자산이 누락되고 위험분석 및 평가방법론이 정의되지 않으며 지침에 명시되어 있는 자산가치 산정기준, 취약성 및 위험평가 기준을 따르지 않으며 목표위험수준에 대해 최고책임자의 승인이 없는 것이 결함으로 나타났다.

5.2 공공영역 미흡항목 분석

5.2.1 개 요

2007년도 평가한 99개 공공기관(47개 중앙부처, 16개 광역지자체, 16개 광역교육청, 20개 정부출연기관 및 국공립대학)과 2008년도 평가대상 117개중 59개 기관(43개 중앙부처, 16개 광역지자체)의 평가결과를 분석하였다.

우선, [표5]에서 보듯이 평가점수를 비교해 보면

[표 5] 보안관리실태 평가 점수

구분	2007년	2008년	비 고
전체	80.01점	86.32점	6.31점 ↑(7.88%)
중앙행정기관	80.85점	86.60점	5.75점 ↑(7.11%)
광역지자체	77.56점	85.58점	8.02점 ↑(10.34%)

07년도에는 중앙부처가 80.85점에서 08년도 86.6점으로 5.75점(7.11%) 상승하였으며 광역지자체는 77.56점에서 85.58점으로 10.34%인 8.02점이 상승하였다. 이는 정보보안 관리실태평가 시행으로 중앙기관과 광역지자체 모두 보안관리 역량이 개선되었으며 중앙행정기관보다 광역지자체 상승폭이 더 크다는 것을 알 수 있다. 광역지자체 상승폭이 더 큰 것은 08년도부터 정보보안 관리실태평가가 지자체 업무평가(행안부 시행)에 반영되고 그 결과가 지방교부금 액수에 영향을 미침에 따라 광역지자체에서 동 평가에 더 많은 노력을 기울인 데 기인한 것으로 판단된다.

세부적으로 8개 분야별 평가결과는 [표6]과 같다. 여기에서 보듯이 모든 분야가 상승하였으며 가장 큰 폭의 상승률을 보인 분야는 운영관리 분야로 07년도 75.93점에서 08년도 87.42점으로 15.13%가 상승하였다. 이는 공공기관이 운영관리에 포함되는 전자우편, 홈페이지 관리 및 PC·노트북· USB 관리, 로그관리 등을 적극 시행한 것으로 볼 수 있다. 그 다음은 정보자산 관리 분야로 07년 78.59점에서 08년 87.5점으로 11.34% 상승하였다. 또 비밀관리 분야가 07년도에 이어 08년도에도 높은 점수를 획득한 것을 알 수 있는데 이는 비밀관리가 공공영역에서 보안의 핵심으로 인식이 확고하게 자리 잡고 있어 오랜 경험과 노하우가 축적되어 있을 뿐만 아니라 비밀관리 부실은 징계나 문책으로 연결될 수 있어 관리가 비교적 잘되고 있기 때문으로 분석된다. 반면 접근보안은 08년도 평가분야 중 가장 점수가 낮아 정보통신망 및 정보시스템, 정보보호시스템에 대한 관리가 여전히 부실한

[표 6] 세부 분야별 정보보안 관리실태 평가 점수

분 야	2007년	2008년	상승률
운영관리	75.93	87.42	15.13%
정보자산 관리	78.59	87.5	11.34%
인적 보안	80.72	86.25	6.85%
침해사고 대응체계 구축	82.41	88.0	6.78%
물리적 보안	87.32	92.02	5.32%
정책 및 업무수행	83.39	86.13	3.29%
접근 보안	81.23	83.33	2.59%
비밀 관리	89.18	91.4	2.49%

것으로 나타나고 있다.

5.2.2 공공영역 '미흡' 평가항목 분석

공공영역은 업무 특성과 중요도에 따라 기관의 보안등급을 가·나·다급으로 분류하고 보안등급에 따라 평가요건을 차등 적용하였다. 평가항목 중 대분류 항목(8개 분야)은 국제표준에 의한 분류방식을 적용하고 중·소분류 항목은 정보통신 환경과 국가의 보안정책 적용을 위해 매년 변경하고 있다.

2007년도에는 공공영역에 대한 최초평가인 만큼 보안관리 체계에 필요한 내부 규정을 마련하고 이를 적용하는지에 중점을 두어 소분류 평가항목을 246개로 세분화하고 항목별 수준을 구별하여 A항목(173개, 70%)은 가·나·다급 기관 모두가 확인하는 항목으로, B항목(48개, 20%)은 가·나급 기관이 추가로 확인하는 항목, C항목(25개, 10%)은 가급 기관이 추가로 확인하는 항목으로 분류하였다. 즉, 가장 높은 보안수준을 필요로 하는 가급 기관은 246개 전 항목을 평가해야 하며 높은 수준의 보안을 요구하는 나급 기관은 221개 항목을, 보통의 보안수준이 필요한 다급 기관은 173개 항목만 평가하게 되었다.

그러자, 기관들은 적은 수의 항목만을 평가받기 위해 기관의 보안등급을 분류하는 1단계 평가시 의도적으로 보안수준을 낮게 평가하여 기관의 보안등급을 하위등급으로 분류하는 문제점이 나타났다. 이에 2008년도에는 모든 기관의 평가항목 수를 동일하게 적용하되 특정 항목에는 등급별로 만점지표를 다르게 적용하는 방식으로 전환하였다. 즉 〔그림5〕의 예시에서 보듯이 가급 기관은 전담조직이 구성되어 있어야 이 항목에 대해 만점을 받지만 나급 기관은 ①번 또는 ②번에 해당하면 만점을 획득하고 다급 기관은 ①번, ②번, ③번 중 하나를 선택해도 만점을 받는다.

〔표7〕은 2007년도 99개 기관이 수행한 평가항목 중 수행률이 낮은 항목 10개를 보여준다.

〔표7〕에서 보듯이 가급으로 최고의 보안수준을 요하는 기관은 상용 전자우편을 사용하지 않도록 정책화

* 기관의 특성에 맞춰 정보보안업무를 수행하는가?
① 전담조직이 구성되어 있다.
② 1명 이상의 정보보안 전담직원이 있다
③ 정보보안과 일반업무를 병행하는 인원이 있다.
④ 정보보안 인원이 없다.
⑤ 해당 없다.

그림 5 정보보안 관리실태 평가항목 예시

〔표 7〕 2007년도 평가항목 중 미흡항목

순위	세부 평가항목	수행률 (%)	대상기관
1	상용 전자우편 사용금지의 기술적 구현	7.14	가급
2	인사 이동시 자료 등 불법반출 차단대책	11.25	가·나급
3	기록된 로그의 비인가 열람 및 훼손 방지대책	17.50	가·나급
4	사용자 로그인시 이전 로그인 정보 제공	17.50	가·나급
5	카메라 폰, 디지털카메라 소지 및 촬영 제한	21.05	가급
6	재난·재해 대비 미러시스템, 백업시스템 등 강구	21.21	가·나·다급
7	RFID 태그 발급기, 리더기 접근 통제 규정	23.08	가·나·다급
8	사이버 침해사고 대비 비상연락망 유지	23.23	가·나·다급
9	기관장에게 정보보안 계획 정기적 보고	26.25	가·나급
10	인가된 장비(H/W, S/W) 사용 위반시 책임 규정	26.25	가·나·다급

하였음에도 이를 기술적으로 구현·적용하고 있는 기관은 7.14%에 불과하며, 보직변동이나 퇴직 등 인사이동시 업무자료 등의 불법반출 차단대책을 마련하고 있는 기관은 11.25%에 그치고 있다. 또한 로그 관리도 17.5%만이 수행하고 있는 것으로 나타나고 있으며 재난·재해 발생에 대비하여 미러시스템 또는 백업시스템 등 대책을 강구하고 있는 공공기관은 21.21%로 99개 기관 중 21개 기관에 불과하다. 또 해킹 등 사이버 침해사고 발생에 대비하여 비상연락망을 유지하고 있는 기관은 23.23%였으며 기관장에게 정보보안 계획에 대해 정기적으로 보고하는 기관은 26.25%에 그치는 등 10개 항목의 수행률이 30% 미만으로 낮은 것을 알 수 있다.

〔표8〕은 2008년도 59개 기관이 수행한 평가항목 중 수행률이 낮은 10개 항목을 나타낸다.

2008년도에는 무선랜 무단사용 여부를 확인·점검하는 항목의 수행률이 40.34%로 가장 낮게 나왔으며 보직변경 또는 퇴직직원의 보안관리는 미흡항목 2위를 차지하고 있으나 인사이동과 관련된 보안관리가 2007년 11.25%에서 2008년 52.81%로 크게 개선되었음을 알 수 있다. 또한 로그의 비인가 열람 및 훼손 방지대책은 2007년 17.5%에서 2008년 62.07%

〔표 8〕 2008년도 평가항목 중 미흡항목

순위	세부 평가 항목	수행률 (%)
1	무선랜 무단사용 여부 확인 점검	40.34
2	보직변경·퇴직직원 보안관리	52.81
3	로그의 비인가 열람·훼손방지 대책 수립	62.07
4	정보화예산 대비 정보보호예산 8%이상	64.14
5	중요 업무시스템 로그인 실패횟수 제한	68.00
6	업무용시스템 패스워드 주기적 변경	68.49
7	자택 등 외부에서의 기관메일 사용 차단	68.51
8	정보시스템 소스코드 관리	68.60
9	스캐너 이용 시스템 취약점 매월 점검	68.79
10	USB 관리시스템 도입 등 대책 수립	69.31

로 수행률이 급증하였다. 그 다음으로 수행률이 낮은 항목은 정보화예산 대비 정보보호 예산 8% 이상 확보, 중요 업무시스템 로그인 실패횟수 제한, 업무용시스템 패스워드 주기적 변경 순이었다.

2007년도와 2008년도에 걸친 공공기관 대상 정보보안 관리실태 평가를 통해 공공기관의 보안관리 필요성에 대한 인식이 높아지고 관리기법을 터득하여 기관의 정보보안 수행 역량이 크게 개선되었음을 알 수 있으며 특히 2007년도에 비해 2008년도에는 개별 항목별로 미흡분야 수행률이 현저히 개선되어, 가장 낮은 항목이 40.34%이며 나머지 8개 항목은 60% 이상 70% 미만의 수행률을 나타내고 있어 동 평가로 인해 공공영역의 정보보안 관리체계에 많은 발전이 있었다고 판단된다.

5.3. 민간·공공영역 정보보안 관리체계 부실분야 분석

민간영역과 공공영역의 정보보안 관리체계 부실 분야에 대해 분석한 결과, 민간영역에서 부실한 정보자산의 보안등급과 취급, 정보자산 분류 및 변경·관리 등은 공공영역에서는 비교적 잘 수행되고 있는 것으로 나타났다.

민간영역에서는 비밀유지 서약서 징구, 정보보호 교육, 물리적 보호구역 보안관리 분야의 수행률이 낮은 반면 공공영역에서는 보직변경이나 퇴직 등 인사이동시 자료 반출 차단대책과 용역 등 외부인력에게 제공하는 자료에 대한 보안대책 수행률이 낮은 것으로 확인되었다.

공공영역에서는 정책 및 업무 수행 분야에서 기관장에게 정보보안 계획을 정기적으로 보고하는 기관이 적으며 기관장도 보안관련 지시를 거의 하지 않는 등 기관장의 보안에 대한 관심도가 낮은 것으로 나타났다. 또한 로그의 비인가 열람 방지대책이 미흡하고 중요업무시스템에 대한 로그인 실패횟수를 제한하지 않으며 패스워드를 주기적으로 변경하지 않는 등 접근통제가 부실한 것으로 확인되었다. 또 운영관리적 측면에서는 USB 등 보조기억매체에 대한 관리가 부실하여 보조기억매체 등록 및 관리번호 부여, 보조기억매체 분실 대비 대책 및 관리시스템 도입 등이 저조한 것으로 나타났다.

한편, 백업 및 복구관리, 시스템 사용자 등록 관리, 보안사고 대응계획 수립 분야는 민간영역과 공공영역 모두 관리가 제대로 되지 않는 것으로 확인되었다.

5.3.1 정보보호 관리체계 부실 원인

민간영역에서 정보자산 분류 및 관리, 시스템 사용자 등록, 정보보호 교육 분야에 대한 관리체계가 부실한 것은 급변하는 정보통신 환경에 기인한다고 본다. 기업들은 정보통신기기 관련 시스템 또는 제품을 수용하는 순환체계가 빠르고 입·퇴사 등 인적교류가 공공영역보다 빈번하다. 이에 따라 정보자산에 대한 관리가 체계화되어 있지 않은 것으로 보이며, 빈번한 인원교체와 맞물려 이루어져야 하는 시스템 사용자 등록과 정보보호 교육이 부실해지기 쉽다.

공공영역은 무선랜 무단사용에 대한 점검, 보직변경 및 퇴직직원에 대한 보안관리, 사용자 로그 및 패스워드 관리가 부실하다. 이러한 현상은 공공영역에 대한 사이버침해사고의 주된 원인이 되고 있는 실정으로 공직사회의 특성에 기인한 바 크다. 즉 공공영역은 법과 절차에 대한 준수를 중요시하기 때문에 침해사고 발생시 대응시간이 민간영역에 비해 상대적으로 길고 담당 직무 외의 사안에 대해 책임지지 않으려는 특성으로 인해 유연성이 떨어지게 된다. 이러한 점은 최근 사회적 이슈가 된 "7.7 DDoS 공격"에 대한 대응에서도 나타나고 있다. 일례로 DDoS 공격 발생시 긴급히 도메인을 전환하면 빨리 복구할 수 있음에도 이에 대한 대처가 늦었던 측면이 있다.

민간영역과 공공영역 모두 관리체계가 부실한 백업 및 복구관리, 보안사고 대응계획 수립, 시스템 취약점 점검 분야는 당면 문제가 아니라 미래 발생 가능한 위협에 대한 대비이기 때문에 정보보호 우선순위에서 밀려 관리가 부실한 것으로 판단된다.

5.3.2 미흡사항에 대한 정보보호 관리체계 개선 방향

민간·공공영역 모두 관리체계 도입으로 정보보호

대책에 있어 많은 개선이 이루어지고 있음은 앞에서 다루었다. 그렇지만 여전히 관리체계가 부실한 것도 사실이다. 더욱이 최근 사이버침해 양태는 복잡화·지능화 되고 있을 뿐만 아니라 새로운 형태의 공격유형이 계속 출현하고 있다. 즉 기존에 나온 위협이 아니기 때문에 사이버 침해에 대한 대응이 어렵고 피해 규모도 갈수록 커지고 있다.

이러한 현상은 현행 대응체계가 차단 중심이며 알려진 공격 위주의 대응을 하기 때문에 더욱 심각해지고 있다. 제 4장의 민간·공공영역의 관리체계 비교에서 살펴보았듯이 공공영역과 민간영역의 알려진 공격에 대응하기 위한 통제항목이 각각 23.69%와 12.78%를 나타내고 있으며 알려지지 않은 공격에 대응하기 위한 통제항목은 11.18%와 9.77%에 불과하다.

이에 따라 정보통신망에 대한 보안위협에 효율적으로 대처하기 위해서는 정보보호 관리체계를 사이버 공격에 대한 대응역량을 높이는데 주안점을 둬야 할 것이다. 알려진 공격에 대비하여 동일한 사고가 재발하는 것을 방지하는 것도 중요하지만 사이버 침해 양상이 갈수록 알려지지 않은 공격이 심화되고 있는 만큼 상시 모니터링 체계를 구축하여 평상시 접근하는 IP 정보 수집을 통한 IP 접속평판(Reputation)에 의한 접근 허용 등 고급화된 관리기술을 적용하는 방안도 강구해야 할 것이다.

이와 더불어 각 기관에서 정보통신 환경 변화를 현장에 적기 적용할 수 있도록 통제항목을 보강하고 정보보호 관리 프로세스가 제대로 가동되는지를 점검하는 방향으로 나아가는 것이 타당할 것이다. 나아가 공공분야는 사이버 침해사고 발생시 즉응태세를 높이기 위해서 직무 담당관이 자발적으로 업무처리를 할 수 있는 범위를 확대하여 조직의 유연성을 넓히도록 제도적 뒷받침이 되어야 할 것이다.

VI. 결 론

정보통신기술이 발전할수록 새로운 보안취약 요인도 빠르게 늘어나고 있다. 어제까지 안전한 대책이 이제는 더 이상 안전하지 않는 대책이 되고 있는 실정이다. 이에 따라 주요 기관은 보안을 더욱 강화해야 하며 그 기준도 갈수록 엄격해지고 있다. 나아가 정보통신 환경 변화에 적시 대응할 수 있는 정보보안 관리체제가 필요하다고 본다. 고정된 항목만으로 정보보안 관리체계를 유지하여서는 급변하는 정보통신망에 대한 안전성을 확보하기 어렵기 때문이다.

최근 민간영역에서는 ISO/IEC 27001 또는 국내 ISMS 인증에 대한 관심이 높아지고 있으며 일부 공공기관에서 국제인증을 취득하거나 민간 인증제도의 공공기관 도입을 추진하려는 움직임이 있다.

그러나, 민간영역과 공공영역은 조직 운영의 특성과 목적이 다르고 정보보안 관리체계 이행에 있어서도 차이를 보이고 있음에 따라 각각의 특성에 맞는 보안관리 목표를 수립하고 정보보안 정책과 부합되는 효율적인 관리체계를 확립해 나가는 것이 필요하다. 더불어 이러한 차이점을 충분히 수용할 수 있도록 민간영역과 공공영역의 정보보안 관리체계 인증제도에 대한 많은 연구가 진행되어야 할 것이다. 본 논문이 향후 공공기관 정보보안 관리체계 인증제도 도입에 밑거름으로 사용되기를 바란다.

참 고 문 헌

[1] 장상수, 김학범, 이홍섭, "정보보호관리체계 인증제도 소개 및 추진방향," 정보보호학회지, 11(3), pp. 1-15, 2001년 6월.

[2] D. Holden, "ISO17799 Security Standard -How will It fit with other standards," www.issa-ne.org, pp. 5-15, Jan. 2006.

[3] 방송통신위원회, "정보통신망 이용촉진 및 정보보호등에 관한 법률," 법률 제9637호, 2009년 4월.

[4] http://isms.kisa.or.kr/isms/jsp/isms_2020jsp

[5] http://isms.kisa.or.kr/isms/jsp/isms_0020jsp

[6] http://isms.kisa.or.kr/isms/jsp/isms_0010jsp

[7] 한국정보보호진흥원, "정보보호관리체계 인증제도 소개," p. 25, 2008년 12월.

[8] http://isms.kisa.or.kr/isms/jsp/isms_0000jsp

[9] NIST Technology Administration, "An Intro- duction to Computer Security: The NIST Hand book," NIST USA, Jan. 1998.

[10] 행정안전부, "전자정부법," 법률 제9932호, 2010년 1월.

[11] 행정안전부, "공공기록물 관리에 관한 법률 시행령," 대통령령 제21473호, 2009년 5월.

[12] 국가정보원, "정보보안 관리실태 평가 해설," 2007년 9월.

[13] 한국정보보호진흥원, "정보보호 관리체계 교육," pp. 76-111, 2008년 12월.
[14] 국가정보원, "2008 보안관리실태 평가 해설," 2008년 9월.
[15] 고규만, 김재성, 장상수, "ISMS 구축시 일반적으로 나타나는 결함사례에 관한 분석," 정보보호학회지, 17(4), pp. 34-41, 2007년 8월.

〈著者紹介〉

김 지 숙 (Ji-sook Kim) 학생회원
2008년 3월~현재: 고려대학교 정보경영공학과 박사과정
〈관심분야〉 정보보호, 정보보호 정책, 정보보호 관리체계

이 수 연 (Su Yeon Lee) 학생회원
2009년 2월: 고려대학교 정보경영공학전문대학원 박사 수료
〈관심분야〉 정보보호정책, 네트워크 포렌식

임 종 인 (Jongin Lim) 종신회원
1986년 2월: 고려대학교 대학원 수학과 박사(암호학)
2000년 8월: 고려대학교 정보보호대학원/CIST 원장(센터장)
2004년 1월: 국가정보원 정보보호정책 자문위원
2005년 7월: 대통령 자문 전자정부 특별위원
2005년 12월: 국회 과기정위원회 정보통신 정책 자문위원
〈관심분야〉 정보보호기술, 정보보호정책, PET, 컴퓨터 포렌식

부 록

〔표 1〕 한국인터넷진흥원의 정보보호 관리체계 통제항목(120개)

통제 분야	통제 항목	통제 사항	지표수
1. 정보보호 정책	1.1 정책의 승인 및 공표	정책의 승인, 정책의 공표	5
	1.2 정책의 체계	상위정책과의 일관성, 정책문서의 유형	
	1.3 정책의 유지관리	주기적 검토	
2. 정보보호 조직	2.1 조직의 체계	조직의 구성, 외부전문가 활용	4
	2.2 책임과 역할	정보보호 관리자, 정보보호 위원회	
3. 외부자 보안	3.1 계약 및 서비스수준협약	외부위탁·제3자와의 계약시 보안요구사항	4
	3.2 외부자보안 실행 관리	외부위탁 보안관리, 제3자 보안관리	
4. 정보자산 분류	4.1 정보자산 조사·책임할당	정보자산 조사, 정보자산별 책임 할당	4
	4.2 정보자산 분류 및 취급	정보자산 분류, 보안등급과 취급	
5. 정보보호 교육 및 훈련	5.1 교육 및 훈련프로그램 수립	교육 및 훈련 계획·대상·내용	4
	5.2 시행 및 평가	정기 및 수시 실시, 훈련결과 반영	
6. 인적 보안	6.1 책임할당 및 규정화	책임할당, 인사규정	5
	6.2 적격심사 및 담당자 관리	적격심사, 주요직무 담당자 관리	
	6.3 비밀유지	비밀유지 서약서	
7. 물리적 보안	7.1 물리적 보안대책	물리적 보호구역, 물리적 접근통제	12
	7.2 데이터센터 보안	위치 및 구조 조건, 출입통제, 내부 설비	
	7.3 장비 보호	주요시스템 보호, 장비 배치, 전원공급, 케이블 보호, 장비의 보수, 장비 폐기 및 재사용	
	7.4 사무실 보호	책상위 문서관리, 컴퓨터 화면 보호	
8. 시스템 개발 보안	8.1 분석 및 설계 보안관리	보안요구사항 정의, 입력데이터·내부처리·출력 및 데이터 검증, 인증·암호, 보안기록 관리	13
	8.2 구현 및 이행 보안관리	구현 및 시험, 운영환경 이행보안, 시험데이터 보안, 소스 프로그램 접근 보안	
	8.3 변경 관리	절차, 운영체계 변경시 검토, S/W패키지 변경	
9. 암호 통제	9.1 암호정책	암호사용 정책 수립	3
	9.2 암호 사용	암호 알고리즘 유형, 신뢰성, 키 길이	
	9.3 키 관리	키 관리지침, 절차, 방법 및 복구방안	
10. 접근 통제	10.1 접근통제 정책	정책의 문서화·내용, 접근통제 규칙·방법	14
	10.2 사용자 접근관리	사용자 등록, 특수권한 관리, 패스워드 관리, 사용자의 접근권한 검토, 사용자의 책임	
	10.3 접근통제 영역	네트워크·운영체제·응용프로그램·D/B 접근	
11. 운영 관리	11.1 운영절차와 책임	운영절차 문서화, 정보자산 변경관리, 직무분리, 개발과 운영환경 분리, 외부운영 설비관리	22
	11.2 시스템 운영	시스템 도입·인수, 성능·용량·백업 및 복구·장애관리, 로그관리, 보안시스템 운영	
	11.3 네트워크 운영	네트워크 운영대책, 인터넷 접속·원격운영 관리	
	11.4 매체 및 문서관리	매체 취급 및 보관·폐기, 시스템문서의 보안	
	11.5 악성 소프트웨어 통제	악성 소프트웨어 예방·탐지·대응 대책	
	11.6 이동컴퓨팅 및 원격 작업	휴대용 정보통신기기 보안정책, 원격 작업	
12. 전자거래 보안	12.1~12.5 전자거래 보안	교환합의서, 전자거래 보안관리, 전자우편, 공개서버의 보안관리, 이용자 공지사항	5
13. 보안사고 관리	13.1 대응계획 및 체계	대응계획 수립, 보안사고 대응체계 구축	7
	13.2 대응 및 복구	보안사고 대응교육 및 훈련·보고, 처리·복구	
	13.3 사후 관리	보안사고 분석 및 정보 공유, 재발방지	
14. 검토, 모니터링 및 감사	14.1 법적 요구사항 준수 검토	요구사항 명시, 준수 검토, 증거자료 수집	11
	14.2 정보보호 정책 준수 검토	검토 계획, 정책의 준수, 기술적 점검	
	14.3 모니터링	접근·사용 모니터링, 감사기록 분석·보관 등	
	14.4 보안 감사	보안감사 계획 및 이행, 감사결과 및 사후관리	
15. 업무 연속성 관리	15.1 관리체계 수립	업무연속성 관리과정·계획 프레임워크 수립	7
	15.2 계획 수립·구현	업무영향 분석, 업무연속성 계획 수립·구현	
	15.3 계획 시험·유지관리	업무연속성 계획 시험·유지관리	

〔표 2〕 국가정보원의 2008 보안관리실태 평가 항목(135개)

대분류	중분류	소분류	지표수
1. 정책 및 업무수행 (8)	1.1 정보보안 정책	1.1.1 정보보안 규정	2
	1.2 정보보안 계획	1.2.1 계획 수립	2
	1.3 정보보안 업무수행	1.3.1 업무 수행	2
		1.3.2 기관장 관심도	2
2. 정보자산 관리 (13)	2.1 정보자산 관리	2.1.1 정보자산 승인 및 관리	4
		2.1.2 정보시스템 수리 및 폐기	2
	2.2 시스템 개발 및 운용	2.2.1 시스템 개발	5
		2.2.2 시스템 유지 보수	2
3. 비밀 관리 (9)	3.1 비밀 관리	3.1.1 비밀취급 인가	1
		3.1.2 비밀문서 관리	4
		3.1.3 비밀 발간업체 관리	1
	3.2 국가용 보안시스템	3.2.1 보안시스템 운영관리	3
4. 인적 보안 (21)	4.1 정보보안 인력	4.1.1 정보보안 인력 구성	3
		4.1.2. 정보보안 인력 운영	3
	4.2 내부인원 관리	4.2.1 신입직원 관리	1
		4.2.2 재직직원 관리	2
		4.2.3 보직 변경 관리	2
	4.3 정보보안 교육	4.3.1 정보보안 인식	2
	4.4 외부인력 관리	4.4.1 외부인력 보안	6
		4.4.2 위탁운영 보안	2
5. 침해사고 대응체계구축(10)	5.1 사전 대응	5.1.1 대응체계 구축	4
	5.2 사후 대응	5.2.1 침해사고 긴급조치	2
		5.2.2 침해사고 처리	2
		5.2.3 재발방지 대책	2
6. 접근보안 (27)	6.1 정보통신망 보안	6.1.1 정보통신망 관리	5
		6.1.2 원격근무 보안관리	3
		6.1.3 무선랜 보안관리	2
	6.2 정보시스템 보안	6.2.1 정보시스템 관리	2
	6.3 정보보호시스템 보안	6.3.1 정보보호시스템 설치	2
		6.3.2 정보보호시스템 관리	6
	6.4 사용자 계정 및 인증	6.4.1 사용자 계정관리 및 인증	2
		6.4.2 패스워드 사용	2
		6.4.3 로그인 관리	3
7. 운영관리 (40)	7.1 서비스 관리	7.1.1 전자우편 보안관리	3
		7.1.2 홈페이지 게시물 관리	3
		7.1.3 홈페이지 운영관리	6
	7.2 정보통신기기 관리	7.2.1 PC 보안관리	8
		7.2.2 노트북 보안관리	3
		7.2.3 기타 정보통신기기 관리	1
	7.3 보조기억매체 관리	7.3.1 보조기억매체 관리	7
		7.3.2 디지털OA기기 관리	2
	7.4 로그 관리	7.4.1 로그 관리	4
	7.5 백업	7.5.1 백업	3
8. 물리적 보안 (7)	8.1 출입 통제	8.1.1 출입 통제	1
	8.2 시설 보안	8.2.1 통제구역 지정 및 관리	1
		8.2.2 작업 통제	1
	8.3 기반시설 보호	8.3.1 전원 및 통신회선 보호	2
		8.3.2 재난 대비	2