공공기관의 정보보호관리체계 감사시스템의 설계 및 구현

A Design and Implementation of Information Security Management and Audit System for Government Agencies

전 용 준* 조 기 환** 김 원 규***
Jun, Yong Joon Cho, Gi Hwan Kim, Won Kyu

요 약

오늘날 정보기술은 모든 산업분야에서 경영의 근간을 이루고 있다. 특히 공공기관들은 민감한 데이터를 다루기 때문에 공정하고 효율적인 정보보호 체계를 갖추어야 한다. 현재 공공기관 대부분이 정보보호 소프트웨어 및 하드웨어를 보유하고 일상적인 감사를 받으며 운영 하고 있지만 관리 정책에 대한 감사체계가 마련되어 있지 않거나 형식에 그치고 있다. 본 논문은 BS7799에 근거한 감사체계를 이용하여 현재 공공기관의 업무환경에 적합한 감사시스템의 설계와 구현을 제시한다. 특히 광역시, 도, 시군구 공공기관에 있어 객관적이고 수치화된 정보보호 업무를 할 수 있는 정보보호 관리체계의 통제에 목적을 두었다. 업무감사시 주관적인 감사자의 이해관계를 통제하고 감사기관의 여건에 맞는 맞춤식 감사 도구를 설계하고 구현할 수 있는 기반을 제공한다.

Abstract

Recently, information technology is considered as a basement of management for industries as well as administrations. Especially, government agencies deal with more high sensitive and important data than other businesses, so, their security managements should be fair and efficient. At present, most government agencies possess and operate their own information security systems, but apply them for the sake of formality only , even do not adapt an audit system for management polices. This paper presents a design and implementation of an automated audit system which is suitable for the operation environment in government agencies, using the audit system based on the BS7799. The proposed system aims to objectively, numerically and daily control the ISMS (Information Security Management System) for different level of government agencies. In addition, it permits to design and implement an adaptive audit tool, in order to meet a given condition of audit organization and guard the personal relationship between the auditor and its counterpart.

☞ keyword : BS7799, ISMS, 정보보안관리체계, Control Object, 통제항목

1. 서 론

최근 인터넷이 일반화 되면서부터 공공기관에 보급되어온 보안장비 및 소프트웨어는 국가기관의 인증 제도를 통하여 국가기관에서 원하는 최소한의 기술적인 기준에 부합하는 제품들이 공급 활용 되어 왔다. 그러나 정보보안 전반에 걸쳐 체계적인 관리에 대한 정리된 지침, 제도 및 도구는 사실상 마련되어 있지 않아 시스템의 운용상에 미비점이 자주 지적되는 실정이다. 국가기관에서 인증하는 정보보호 관리체계인증 제도 또한 자체적인 정보보호 관리체계의 상시적인 운영이라기보다는 서류 및 실사를 통한 일시적인 정보보호 관리체계의 검사 업무에 불과한 수준으로 알려져 있다.

공공기관에서 정보보호 관리 및 감독의 업무는 각종 지침을 통해서 지침의 준수 여부에 대해 정

* 준 회 원 : 전라북도청 정보통신담당관
yjjun@ejeonbuk.net
** 정 회 원 : 전북대학교 전자정보공학부 부교수
ghcho@chonbuk.ac.kr
*** 준 회 원 : 나일소프트 정보보안 컨설팅 근무
kwk@nilesoft.co.kr
[2006/05/22 투고 - 2006/06/14 심사 - 2006/07/28 심사완료]

기 혹은 비정기적으로 수행되고 있는데 이는 업무담당자의 잦은 교체로 인해 지침의 이해 및 활용도가 낮아 지침의 준수 여부를 수치적으로 판단하기 어려우며, 이를 관리 감독하는 감사자의 성향에 따라 감사 결과가 상이하게 평가 될 수도 있다[1]. 따라서 공공기관에 적합한 정보보호 관리체계와 이를 통제하고 감독할 수 있는 체계적인 감사제도가 절실한 상황이다.

감사업무는 정보보호 혹은 정보보안시스템의 보안위험을 식별하고 이러한 위험을 효과적으로 관리할 수 있는 대책을 포함한다. 이를 위하여 BT, HSBC, Marks and Spencer, Shell International, Unilever 등 주요 업체와 더불어 영국의 상무성 주관으로 "정보보안관리 실무 규범(A Code of Practice for Information Security Management)"이라는 제목으로 제시된 BS7799[2][3]를 기반으로 설계한다. BS7799는 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용하도록 개발되었으며, 조직의 보안 표준의 기반이 되도록 고안되었다. 즉, 기업이 고객 정보의 비밀성, 무결성 및 가용성을 보장한다는 것을 공개적으로 확인하는데 초점을 둔다. 물론 이 표준에서 제시하고 있는 통제들 모두가 모든 상황에 적용될 수 있는 것은 아니며, 개별적인 환경적 또는 기술적 제약조건을 고려하여 선택하여야 할 것이다. 따라서 이 표준은 지침과 권고안의 성격을 가진다.

본 논문은 상기의 문제점을 정보보호관리 체계의 시스템화와 체계적인 관리 감독을 위한 도구의 설계 및 구현을 제시한다. 정보보호 업무의 설계, 업무범위 담당자별 할당, 업무 수행 결과의 수치화를 통한 객관화된 평가 결과를 도출 할 수 있게 하여 자동화된 도구에 의한 업무를 수행 할 수 있는 기반을 다음의 세 가지의 구성 요소로 구성한다.

1.1. 감사업무의 설계

BS7799에서는 10 영역, 36 통제 목표(Control Objectives)와 127 통제항목을 준거로 공공기관에 적합한 정보보안관리시스템(Information Security Management System : ISMS)를 구축할 수 있도록 하였으며, 준거 틀을 기반으로 설계된 업무는 전체 혹은 부분적으로 재활용이 가능하게 하였다. 이러한 설계 결과를 Database화하여 감사업무의 지식 기반을 축적할 수 있도록 구현한다.

1.2. 업무(감사)수행 부분

사용자에 의해 설계된 통제 항목을 이용한 업무(감사)수행부분으로 업무 담당자 단독 혹은 팀 단위로 업무를 수행 할 수 있도록 통제항목의 배분 및 수집을 가능하게 하여 감사(업무)부문별 전문성 혹은 편의성에 의한 업무의 분담 수행을 가능 하게 한다.

1.3. 업무(감사)결과의 출력

업무(감사)의 수행 결과를 분석하여 수치화된 경과를 도출하여 Reporting을 하며, 설계된 통제항목을 별도로 출력할 수 있도록 하여 전체 통제항목에 대한 사전 검토 및 감사대상 인원 및 기관에 사전 통보가 가능하게 한다.

위에서 살펴본 정보보호 감사시스템의 구성 요소 세가지중 가장 중요한 요소는 감사 업무설계 부분이라고 할 수 있다. 설계부분은 BS7799와 같은 준거 틀을 활용한 새로운 감사기준(Audit Template)의 설계를 할 수 있어 공공기관에 적합한 통제항목의 생성과 통제항목에 대한 감사상세항목(Audit Check List) 및 감사방법(Audit Method) 등을 생성할 수 있다. 설계의 구현은 감사자기준으로 도구를 실제로 구현 하였으며, 이를 활용한 보안 감사 항목의 생성, 감사의 수행, 수행결과의 도출을 할 수 있도록 한다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 본 논문에서 설계되고 구현된 감사업무 시스템의 근간이 되는 BS7799에 대해 개략적으로 살펴보고, 3장에서는 BS7799에 기반 하여 공공기관의 업무특성 및 환경에 적합한 감사업무 시스템을 설계한다. 4장에서는 3장의 설계내용에 기반하여 각각의 기능별 구현과정을 상세히 기술한다. 5장에서는 구현된 감사업무시스템의 활용이 기대되는 분야를 기술 하였다. 마지막으로 6장에서는 결론을 내린다.

2. BS7799

1995년에 처음 제정된 BS7799는 1999년에 개정되었으며, 영국 이외에 호주, 브라질, 네덜란드, 뉴질랜드, 노르웨이 등에서 사용되고 있다. 1999년 10월에 ISO 표준으로 제안되어 ISO/IEC DIS 17799-1이 되었다. 영국 정부에서는 전자정부를 향한 노력을 뒷받침하기 위하여 대부분의 정보시스템에 대하여 BS7799 인증을 받도록 하여 국가 핵심 정보 기반구조를 보호하기 위한 수단으로 활용하고 있다. 산업계에서는 정보보안이 국제시장에서 경쟁 우위를 제공하는 경영전략이 될 수 있다고 인식하고 있으며, 유럽, 북미, 환태평양권 등 전 세계적으로 BS7799에 대한 높은 관심을 보이고 있다.

BS7799는 기업들이 부딪치는 대부분의 상황에 필요한 통제를 식별하기 위한 중요한 참조사항을 제공함으로써 중소기업은 물론 대기업까지 광범위한 범위에 적용될 수 있도록 하는 공통적인 정보보안관리 문서는 기업들 간의 네트워킹에 있어서 상호 신뢰 가능기반을 제공한다.

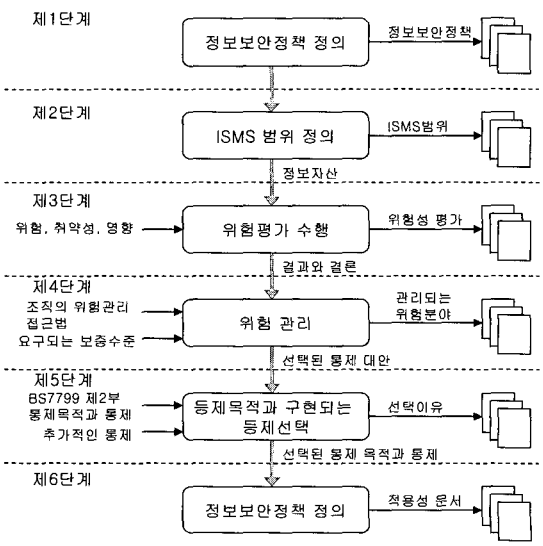
권고안으로써 BS7799는 두 부분으로 구성된다. 제1부는 표준적인 실무 지침이며 종합적인 보안통제 목록을 제시하고, 제2부는 정보보안관리시스템(ISMS)에 대한 표준적인 명세이다. 또한 ISO9000과 유사하게 운영되는 "c: cure"라는 인증 시스템이 있다. 사실 ISO9000과 BS7799 사이에는 많은 유사성이 있는데, 예를 들어 ISO9000에서의 품질 정책과 품질관리시스템 대신에 BS7799에는 정보보안 정책과 ISMS가 존재한다.

2.1. 보안통제

보안통제 부분은 10개의 주요 분야로 나누어진 127개의 통제 항목으로 구성되어 있으며, 현재 사용되고 있는 최선의 정보보안 실무들로 구성된 종합적인 보안통제 목록을 제공한다. 이중에서 10개의 통제 항목들은 핵심 통제들로서 필수적인 요구사항이거나 정보보안을 위한 기초적인 구성요소이며, 조직이 정보보안 통제를 구현하는데 기반이 된다.

2.2. 관리표준

BS7799는 체계적이고 효율적인 정보보호를 위해 ISMS를 구현하도록 요구하고 있다. 관리표준 부분은 위험관리의 중요성을 강조하며, 보안통제 부분에 수록된 모든 통제 항목들을 구현할 필요는 없다는 점을 명확히 강조하고 있다.



(그림 1) ISMS 구축 단계

(그림 1)은 관리표준 부분에서 명시한 ISMS를 어떻게 구축하는지에 관한 여섯 단계로 구성된 구체적인 구축단계를 제시한다. 먼저 모든 정보자산과 조직에 있어서 그들의 가치를 분석하고, 어떤 정보가 왜 중요한지를 식별하는 정책을 고안하도록 한다. 2 단계에서는 낮은 가치를 가진 정보를 제외하여 관리 대상의 범위를 정의한다. 다음으로, 가치를 상실하는데 따른 위험을 분석하며, 그 위험을 어떻게 관리할지를 결정한다. 여기에는 물리적, 인적, 절차적인 측면을 고려하여야 하며, 효과적인 업무 지속성 계획의 개발도 포함된다. 그 다음 단계는 위험을 관리하기 위한 보안대책을 선정한다. 구체적인 보안대책이 BS7799에 열거되어 있으나 완전한 것이 아니며, 원하는 경우에는 추가적인 보안대책이 포함될 수 있다. 이러한 이유로 BS7799의 적용성에 관한 명제는 특정한 보안 통제가 선택된 이유를 기술할 뿐만 아니라 BS7799에서 열거한 보안 통제 중에서 제외된 항목이 특정 조직에 관련이 없는 이유를 서술하고 있다.

2.3. 국내 인증 현황 및 만족도

국내인증 현황은 BS7799가 2001년 한빛은행(현 우리은행)을 필두로 현재까지 40여 기관에서 BS7799인증을 획득 하였다. 인증 기업들의 중 상당수가 금융권이며 이는 금융권이 정보보호관리체계의 확립을 통한 은행업무의 안전성 확보에 노력함을 알 수 있는 증거라고 할 수 있다. 몇몇 대기업의 경우도 BS7799인증을 획득하여 보안업무의 체계적인 수행을 확보하고 있는 상태이다.

인증을 받은 기업들은 정기적으로 업무수행 절차에 및 수행 결과물에 대한 서면 감사 등을 통해서 지속적으로 정보보호관리 체계의 안정적인 수행상태를 점검 받고 있어 업무의 안정성을 제고하고 있다. 해당 업무담당자 또한 체계적인 업무 수행으로 업무의 효율성을 확보하고 있다.

BS7799인증을 획득한 기업의 부가적인 효과는 정보보호에 대한 국제표준(BS 7799)에 적절하게 부합되는지 해당조직의 정보보호경영시스템을 제3자가 독립적이고 객관적으로 검증함으로써, 해당조직의 보안수준을 지속적으로 개선하고 이의 인증을 통하여 고객 및 비즈니스 파트너로부터 신뢰감이 확보되고 있다는 것이며 또한 이에 만족하고 있는 상태이다.

2.4. 유사제품의 분석

정보보호관리 체계를 유지 관리하기 위한 도구는 있지만, 정보보호관리 체계만을 위한 도구는 아니며 주로 위험 분석 업무 지원 도구에 가깝다고 할 수 있다. 불과 2년 내지 3년 전에 BS7799에 대한 감사 기능을 보강한 제품 들이 출현 되고 있으나 감사도구로서는 적절하지 못하다. 영국의 경우 CRAMM이라는 도구가 가장 유사한 도구라 할 수 있으나 위험 분석에 치중되어 있다. 미국의 경우 Buddy, Expert 라는 도구로 국내에 소개된 적이 있으며 BS7799에 대한 내용을 담고 있으나 고객지원의 부재 및 국내현실에 부합되지 못하여 적용에 실패 하였다. 국내에서는 한국전산원에서 1990년대 중반 이를 도입 연구 하여 HWAK라는 위험 분석 시스템을 만들었으나 현실에 적용 되지는 못하고 있다. 최근 금융권을 중심으로 위험관리 체계 시스템 구축이 일부 이루어 졌으나 일반적으로 활용이 불가한 해당 기관만의 전용 시스템으로 봐야 할 것이다. 정보보호 진흥원에서도 정보보호관리 체계인증을 위한 도구를 개발 적용 하고 있으나 인증을 위한 내용만을 담고 있어 일반 기관에서의 감사도구로 활용에 적절하지 못하다.

본 논문을 통하여 설계 구현한 도구는 BS7799의 정보보호관리체계의 감사기능에 한정 되어 있지 않고 공공기관의 감사업무에 적합하도록 감사자에 의한 감사 통제항목의 자유로운 설계와 재활용이 가능하다. 따라서 외국의 유사제품과의 직접적인 기능상의 특성 및 차이점에 대한 비교는 의미를 같지 못할 것으로 판단된다.

3. 감사시스템 설계

감사시스템 설계에 있어 우선 적으로 고려된 사항은 정보보호관리 체계에 대한 통제항목의 구축 및 감사에 중점을 두고, 공공 기관에 있어 다양한 부분에 감사기능의 적용이 가능하도록 감사 통제 항목의 자유로운 설계 및 재활용이 가능하도록 한다.

3.1. 시스템 설계의 특징

시스템의 설계에 있어 공공기관에 적당한 정보보호관리 체계의 준거 틀이 현재 국내 공공기관에 적용되어 있는 것이 없다. 정보보안 관련 공공기관에서 사용 되는 중앙정부의 지침은 존재하나 부분별로 분리되어 있는 것이어서 종합된 정보보호 관리를 위한 지침 및 체계로 볼 수 없다. 따라서 세계적으로 인정되고 있는 영국의 BS7799를 정보보호관리 체계 상시운영 및 감사시스템 설계에 정보보호 관리의 체계성과 일반성을 제고한다.

그러나 공공기관의 사용자가 신규로 감사통제 항목의 생성을 준거 틀을 이용하지 않고 생성이 가능하도록 하여 BS7799에 대한 확장성은 설계과정에서 고려한다. 또한 기 작성된 보안업무(감사) 기준을 활용하여 새로운 기준을 생성 할 수 있도록 하여 변화되는 공공기관의 업무환경에 적합하게 운영 될 수 있는 시스템을 구조에 적응성을 포함한다.

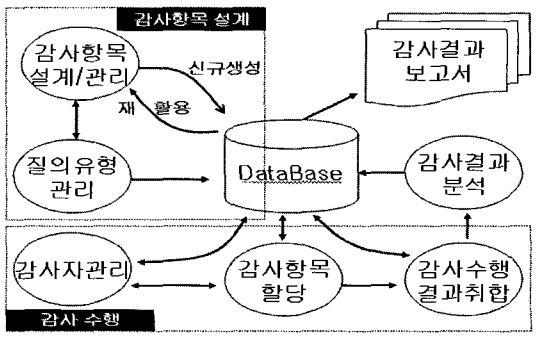
이러한 설계의 기본 방향으로 구현된 도구는 정보보호관리 체계만을 대상으로 감사하는 도구가 아니고 정보시스템에 대한 감리, 일상 감사 업무 등에도 폭넓게 활용할 수 있도록 하기 위함이다. 이러한 기능의 구현은 Database를 이용하여 감사 통제항목의 재활용 측면과 활용된 감사 기준의 DB축적기능을 포함하고 있어 감사통제 기준에 대한 지식 기반을 마련할 수 있도록 한다[4 - 11].

3.2 시스템의 기본구조

정보보호 관리체계의 상시운영 및 감사시스템의 구성의 요구사항을 기반으로 구성된 시스템 구조는 (그림 2)와 같다. 감사 항목의 설계/관리는 기 생성된 자료를 기반으로 순환적 과정을 통하여 이루어지도록 함으로써 설계의 일관성과 관리의 편의성을 제고하고 있다. 또한 감사 항목설계와 수행과정에서 생성된 자료를 저장하는 데이터베이스를 중심으로 감사결과 분석이 피드백되며 최종결과는 보고서로 출력되어 근거 자료로 활용되도록 한다.

업무(감사)기준설계, 업무(감사), 결과보고서부분은 데이터베이스 내에서 상호 연동 되어 처리될 수 있도록 설계되어 있어야 하므로 각 부분별로 별도의 요구사항이 존재하고 상호연계처리 되어야 한다. 따라서 시스템 관점에서 이러한 요구사항은 세 가지 부분으로 구성된다. 업무(감사)기준설계 부분의 필수적인 기본 요구사항을 다음과 같이 정의한다.

가. BS7799와 같은 준거 틀의 재활용을 통한 파생기준 생성
나. 신규업무(감사)기준의 자유로운 생성
다. 업무(감사) 방법의 생성 관리
라. 생성된 기준의 담당자별 할당



(그림 2) 시스템 구조

업무(감사)수행 부분의 기본 요구사항은 다음과 같이 정의한다.

가. 업무(감사) 결과의 입력
나. 업무(감사) 진행사항의 표시
다. 기 수행한 업무(감사)결과의 조회
라. 할당된 업무(감사)결과의 취합

결과보고 부분의 기본 요구사항은 다음과 같이 정의한다.

가. 설계된 업무(감사) 양식 보고서
나. 결함 내역, 이행 비율에 대한 정량분석 보고서
다. 기간별 결과 분석 결과 비교 보고서

3.3. 감사결과의 분석

감사결과의 분석은 본 논문에서 제안한 제반 과정의 궁극적인 과정으로 가장 중요한 단계이다. 한편 분석 결과에서 오류 최소화는 물론 항목의 정의가 명료하게 제시되어야 한다. 정량적으로 분석하기 위해서 통제항목을 분류하여 처리하며, 이는 다음과 같이 분류 정의하여 처리하였다.

3.3.1 평가그룹

평가하기 위한 목적을 기준으로 감사결과는 통제항목을 묶어서 그룹으로 정의하였다.

3.3.2 평가비중

각 평가그룹에 어느 정도의 비중을 두어 정보보호관리 체계를 평가하는지를 나타내는 척도로 식 (1) 과 같이 정의하였다.

$$\text{평가비중} = \frac{\text{해당 평가그룹의 평가총점}}{\sum(\text{각 평가그룹의 평가총점})} \quad (1)$$

3.3.3 평가그룹의 평가점수와 평가 총점

통제항목의 평가총점은 정보보호관리 체계에서 해당 통제항목이 차지하는 비중을 정량화한 개념이다. 평가점수는 평가총점 중에서 통제항목에 대한 감사결과 획득한 점수화한 것으로 통제항목의 답변 형식이 선택형인 경우, 식 (2)와 식 (3)을 통해 평가 총점과 평가 점수를 정의하였다.

$$\text{통제항목의 평가총점} = (\text{통제항목의 중요도}) \times \sum(\text{각 보기항목에 할당된 점수}) \quad (2)$$

$$\text{통제항목의 평가점수} = (\text{통제항목의 중요도}) \times \sum(\text{심사결과에서 선택된 보기항목에 할당된 점수}) \quad (3)$$

답변형식이 선택형이 아니고 서술형태인 경우는 정략분석자(감사자)가 통제항목의 평가 총점과 평가 점수를 직접 표시하며, 식 (4)와 식 (5)와 같이 평가 점수와 평가 총점을 정의하였다.

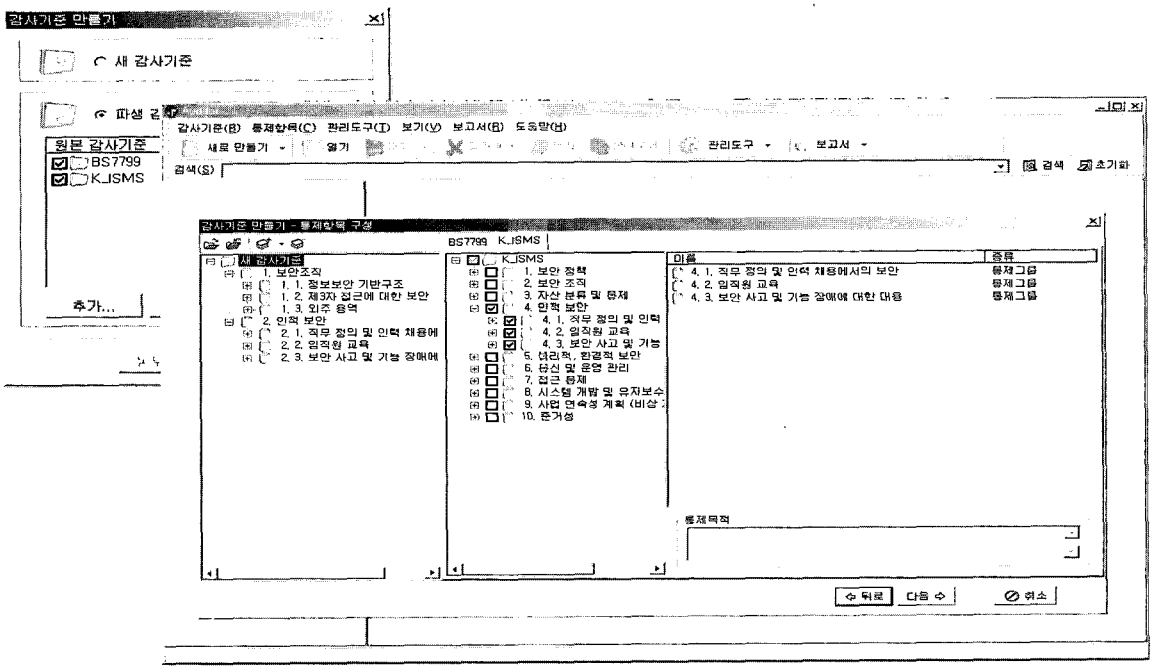
$$\text{평가그룹의 평가총점} = \sum(\text{하위 통제항목의 평가총점}) \quad (4)$$

$$\text{평가그룹의 평가점수} = \sum(\text{하위통제항목의 평가점수}) \quad (5)$$

3.3.4 평가 그룹의 이행비율

평가그룹의 하위 통제항목들에 대하여 조직이 요구하는 통제수준의 몇 %가 실제로 이행되고 있는지를 나타내는 척도이며, 식 (6)과 같이 정의하였다.

$$\text{평가그룹의 이행비율}(\%) = \frac{\text{평가그룹의 평가점수}}{\text{평가그룹의 평가총점}} \quad (6)$$



(그림 3) 파생 감사기준 생성

3.3.5 평균 이행 비율

모든 평가 그룹의 이행 비율을 평균한 개념으로 식 (7)과 같이 정의하였다.

$$\text{평가이행비율} = \frac{\sum(\text{평가그룹의 평가점수})}{\sum(\text{평가그룹의 평가총점})} = \frac{\sum(\text{통제항목의 평가점수})}{\sum(\text{통제항목의 평가총점})} \quad (7)$$

3.3.6 감사 결과의 적합성 평가

모든 평가그룹의 이행 비율이 '최소 기준값' 이상이고 평균 이행비율이 '평균 기준값' 이상인 경우에만 감사 대상 조직의 정보보호 관리체계가 '적합' 혹은 '부적합'하다는 평가를 할 수 있도록 감사자가 '이행비율의 최소 기준값과 평균 기준값을 지정할 수 있도록 하였다.

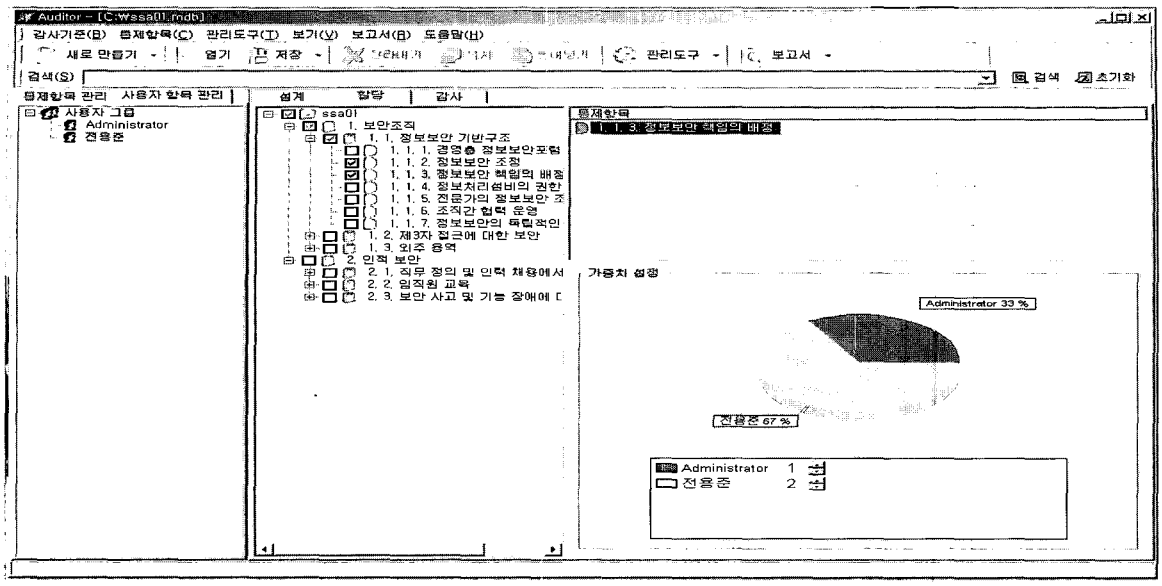
4. 구 현

시스템 구현은 감사자 단독 혹은 감사팀 단위로 업무를 수행할 수 있도록 하여 상황에 적합하게 활용 할 수 있게 구현하는 것을 목표로 하여 구현한다. 감사 기준(통제항목)의 생성, 배분, 취합은 직관적으로 조작이 가능하게 하였지만 감사결과의 평가는 정량 평가를 할 수 있도록 구현한다.

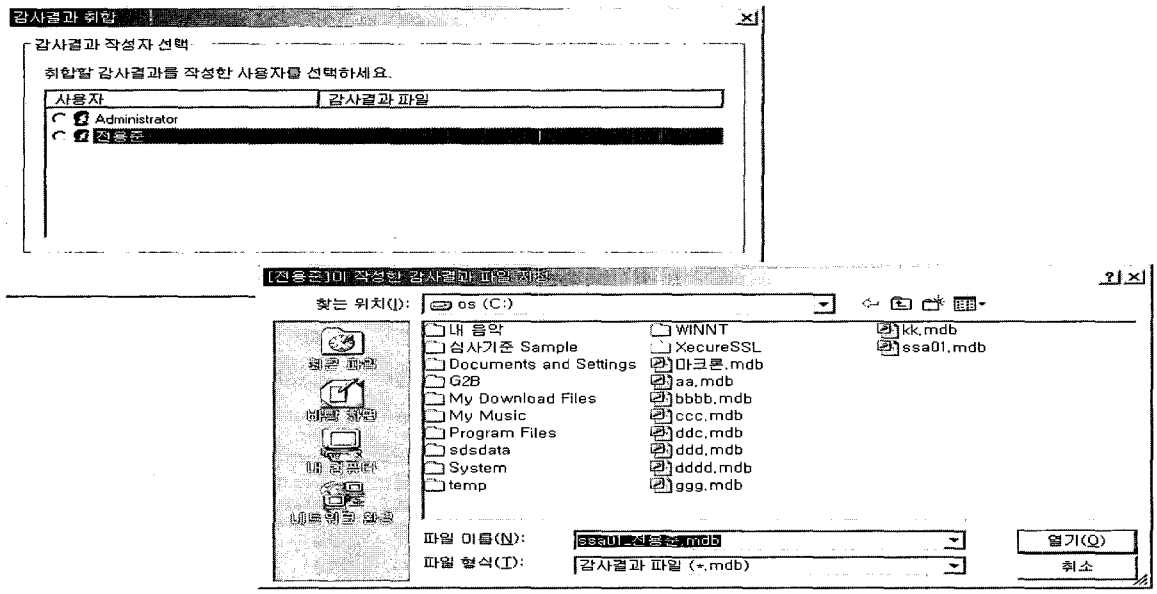
4.1. 감사기준의 구축

업무(감사)기준 생성은 두 가지 방법으로 가능하다. 통제항목이 전혀 포함되어 있지 않은 '새 감사기준'을 생성할 수 있을 뿐 아니라, 기존 감사기준들로부터 일부 내용을 복사하고 재구성하여 어느 정도 구축 과정이 진행되어 있는 '파생 감사기준'을 생성하는 것도 가능하도록 한다. (그림 3)은 기존의 감사기준에 의거하여 필요한 감사기준을 시스템에 포함시키는 과정을 보여준다.

이렇게 생성된 감사기준에 통제항목을 추가,

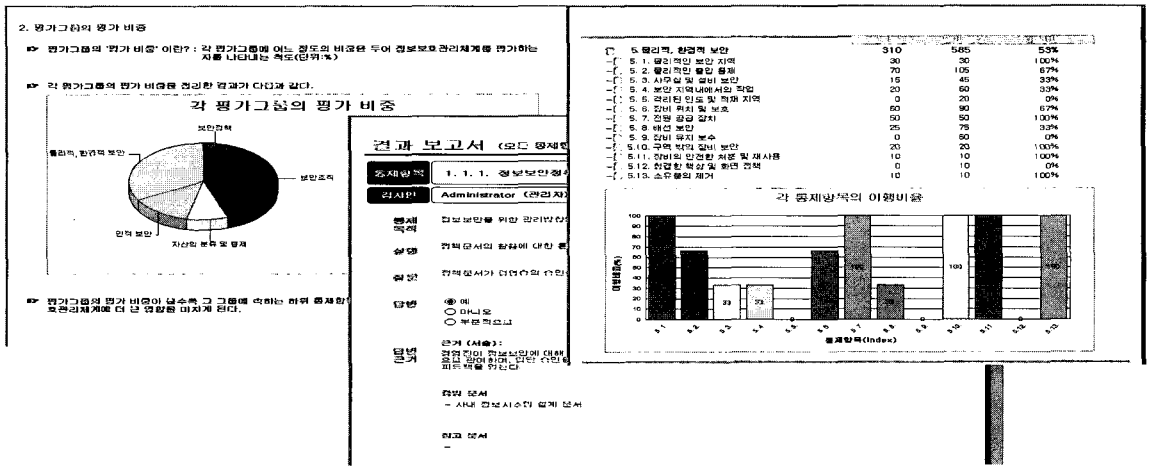


(그림 4) 역할분담 및 기준배분



(그림 5) 감사결과의 취합

삭제, 삽입하는 등 기본적인 편집 작업을 통해서 감사기준을 자유롭게 편집할 수 있도록 하였고, 각 통제항목에는 질문, 답변 유형 및 감사 방법(참고 문서, 면담 대상자, 자동화 도구), 중요도를 입력할 수 있으며 입력 과정의 편의를 위해 한번 입력된 답변 유형의 재사용을 지원할 수 있게 한다. 통제항목의 중요도 입력은 감사 결과 분석 과정에서 통제항목별 가중치를 부여하는 기준을 제공하여 감사보고서에 제시되는 분석 결과의 신뢰성을 확보하도록 한다.



(그림 6) 결과 보고서

4.2. 역할분담 및 감사기준 배정

감사를 직접 수행할 감사자를 등록하고 등록된 감사자들에게 통제항목을 할당하는 과정을 지원한다. 감사자에 관한 제반 정보를 관리하고 접근권한을 조정하는 등의 작업이 가능하고, 하나의 통제항목을 여러 명의 감사자들에게 할당하는 '공유 할당'을 지원하여 감사 결과가 특정 감사자의 의견에 편중되는 것을 예방할 수 있는 장치를 마련한다. 감사자 등록 및 통제항목 할당이 완료된 후, '감사기준 배분'이라는 절차를 통해 각 감사자가 감사를 수행하고 그 결과를 직접 입력할 감사기준을 생성할 수 있도록 한다. (그림 4)는 임의의 감사자에게 통제항목이 할당되고 감사기준이 배분되는 과정을 보여준다.

4.3. 감사결과 입력 및 취합

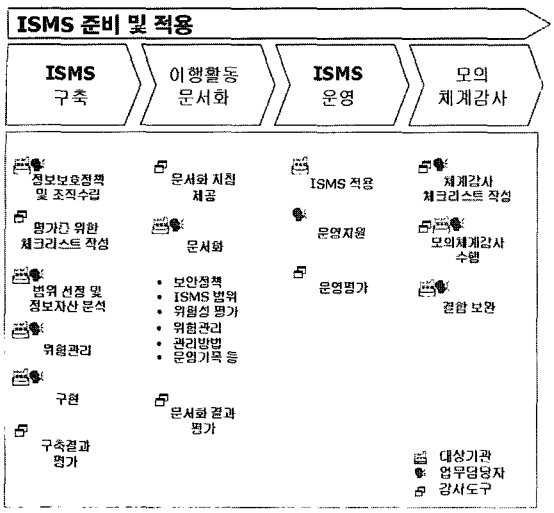
해당 감사기준을 배포 받은 감사자들이 할당받은 통제항목에 대하여 감사를 수행하고 감사 결과를 입력할 수 있는 기능을 구현 한다. 감사 결과의 객관성을 확보하기 위하여 근거를 서술하거나 증빙 문서를 첨부할 수 있도록 하였으며, 모든 감사자들의 감사 결과 입력이 완료된 후, '감사결과 취합'이라는 절차를 통해 각 감사자들이 입력한 부분적인 감사결과를 하나의 감사 결과에 통합할 수 있도록 한다. (그림 5)는 각 감사자들의 감사결과를 취합하기 위한 화면이다.

4.4. 보고서

보고서의 양식은 세 가지 형태를 구현 한다. 첫째, 모든 통제항목의 양식(질문, 답변 유형, 감사 방법, 중요도)을 보기 쉽게 출력하는 양식 보고서로 설계된 감사내용을 감사자가 사전에 확인할 수도 있으며 피감사 대상에게 제시 사전 준비를 할 수 있는 기능을 할 수 있다. 둘째, 양식 보고서에 감사 결과까지 표시하여 출력하는 결과 보고서로 감사자가 감사한 결과를 출력해서 확인할 수 있도록 한다. 셋째, 정량 분석 보고서로 감사 결과에 대한 정량적인 분석을 통해 정보보호관리 체계에 대한 종합적인 평가를 제시할 수 있도록 한다. (그림 6)은 구현된 감사시스템의 출력 예를 보이고 있다.

5. 활용 방안

감사도구의 활용은 정보보호관리 체계의 감사를 기본으로 하고 있으나 통제항목의 자유로운



(그림 7) ISMS 준비 및 적용 과정

편집을 통해서 IT 분야 감리 및 일반 감사 등에도 활용 될 수 있으며, 공공기관 및 일반 업체에서의 감사 감리업무에 활용이 가능하다. 본 논문을 통해 구현 된 도구는 감사자, 감리자, 관련 컨설팅 회사의 컨설턴트에 의해 전유되는 것이 아니고 일반 실무 업무 담당자 또한 자체적인 감사, 감리도구로 활용이 가능하다.

감사도구의 활용은 정보보호관리 체계의 구축을 준비하는 기관에서도 유용하게 활용될 수 있다. 정보보호관리 체계의 구축은 해당 기관의 업무 범위, 형태에 따라 달라질 수 있지만 도구가 제공하는 BS7799 기반의 통제항목을 준거 틀로 삼아서 해당 기관에 적합한 정보보호관리 체계의 구축하는데 활용 될 수 있다.

5.1 공공기관에서 활용

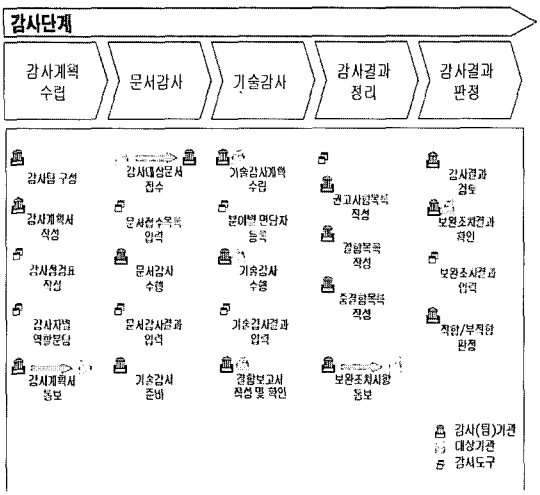
정보보호관리 체계의 구축은 조직의 자산에 대한 안전성 및 신뢰성을 향상시키기 위한 절차와 과정을 체계적으로 수립하고 문서화하여 지속적으로 관리, 운영하고 정보보호 목표인 정보의 비밀성, 무결성, 가용성을 실현하기 위한 일련의 과정 및 활동이다. 다양한 형태로 존재하는 실제 상황에 이를 조직 자체적으로 체계적인 구축을 한다는 것은 결코 쉽지 않은 일이다. 일반적으로 정보보호관리 체계를 구축하는 과정은 정보보안 컨설팅 전문업체의 컨설팅을 통하여 수행되어 지는데 이는 최소 3개월 이상의 전문 컨설팅이 필요한 부분으로 많은 비용과 시간이 필요하다.

(그림 7)은 감사도구를 활용 정보보호관리 체계를 자체적으로 수행 구축하는 과정을 나타낸 것이다. ISMS의 구축을 기관 자체적으로 구축하고 이를 이행, 운영하고 자체적으로 정보보호관리 체계에 대한 감사를 실시하는 과정을 감사도구를 활용 적용한 것이다.

자체적인 ISMS의 구축은 전문분야 컨설턴트에 의해 실시되는 것이 좋을 수도 있지만 조직의 특성에 적합한 정보보호관리 체계를 구현하는데 있어서는 해당 기관의 조직원에 의해 해당 조직의 특성에 적합한 정보보호관리 체계를 구축하는 것이 효과적일 수 있다. 자체적인 구축의 단점으로 비전문가에 의한 정보보호체계의 구축이라는 위험 부담이 있지만 조직의 정보보호관리 체계에 대한 업무 역량 강화와 비용 절감이라는 장점도 가지고 있다. 전문 컨설턴트의 도움을 부분적으로 수용하고 자체인력과 협업을 통한 정보보호관리 체계의 구축은 이러한 장단점을 감안하면 좋은 대안이 될 수도 있을 것이다. 정보보호관리 체계의 구축후 이를 상시 운영 하는데 있어 감사도구의 활용은 업무의 전문성과 효율성을 확보한다는 차원에서 도움이 될 것으로 보인다.

5.2. 도구의 적용

정보보호관리 체계에 대한 감사는 감사계획의 수립, 문서 감사, 기술 감사, 감사 결과 정리 및 판정이라는 일련의 과정이라 볼 수 있다. 감사도구를 이러한 일련의 과정에서의 활용은 감사자의 개인역량에 의해서 수행되어오던 감사와 달리 감사의 객관성과 전문성을 도구를 통하여 강화할 수 있어 감사 결과에 대한 신뢰를 확보 할 수 있다.



(그림 8) ISMS 감사

(그림 8)은 도구의 특성상 감사의 계획수립에서부터 감사결과의 판정에 이르기까지 도구를 활용 하는 것을 일반적인 감사 과정의 예를 들어 표현한 것이다. 도구의 활용은 전문성과 객관성의 확보에 있어 감사 자료의 생성과 감사 결과의 판정에 있어 도구에 근거를 두고 있기 때문에 감사자의 주관, 성향, 개인적인 감사 능력에 의한 결과보다는 객관적일 수 있다.

5.3. 감리 업무의 적용

도구가 가지고 있는 감사 통제 항목이 정보보호관리 체계에 대한 것으로 구성 되어 있긴 하지만 일반적인 IT업무에 대한 운영 및 보안 감리업무도 수행이 가능하다. 감사 통제 항목의 부분적 편집이나 새로운 통제항목의 생성은 도구가 지원하고 있어 상당 부분의 BS7799통제 항목들이 약간의 편집 과정만 있으면 정보시스템 운영 및 보안 감리에 활용이 가능하기 때문이다.

감리인에 의한 공인 감리 또는 기관 자체적인 감리에 있어서도 정보보호관리 체계의 감사와 유사한 과정을 가지고 있어서 도구의 활용은 시간, 인원, 비용의 절감 효과와 관련 업무의 효율성을 확보할 수 있을 것이다.

6. 결 론

본 논문에서는 공공기관에서의 정보보호관리 체계의 상시 운영과 이를 관리, 감독할 수 있는 감사시스템에 대한 설계와 구현을 하였다. 정보보호관리 체계에 대한 준거는 세계적으로 인정받고 있는 BS7799를 활용 하였으나 공공기관의 특성에 따라 편집할 수 있도록 설계하였다. 따라서 새로운 정보보호관리 체계의 생성과 새로운 감사기준의 생성이 자유롭게 설계, 구현되어 있어 변화되는 감사기준, 관리체계에 유연하게 대처할 수 있다. 한번 생성된 기준은 추후 편집을 통한 재활용도 가능하게 되어 있다. 이러한 감사도구의 적용은 감사부서에서는 감사도구로 일반 업무 부서에서는 평소 반드시 준수하여야 할 상시 시스템으로 적용 할 수 있다. 또한 통제 항목의 자유로운 생성과 편집을 통해 감리회사, 컨설팅 회사 등에서도 유용하게 활용할 수 있도록 하였다.

또한 도구를 통한 객관화된 감사는 피감사자에게는 결과의 신뢰성을 제고할 수 있으며, 감사자는 다양한 상황에 적합한 감사 통제항목의 설계 및 시행을 통해 감사방법에 대한 지식의 축적을 통해 보다 효과적인 감사를 수행할 수 있는 지식기반을 확보 할 수 있다. 제안된 감사 자동화 시스템은 정보보안 장비 및 소프트웨어는 많이 보급되어 있지만 이를 관리 감독하기위한 도구화된 관리체계가 없는 우리나라 공공기관에 정보보호관리 체계의 구축 적용 및 관리 감독에 활용될 수 있다. 또한 공공기관의 정보보안 관련된 업무담당자, 감사부서, 감사기관, 감리회사 등에서도 활용될 수 있다. 더불어 개발된 시스템은 감사기준의 생성, 수정, 삭제를 통해 일반 기업들의 정보보안 업무의 체계화 및 효율화에 적용될 수 있다.

참 고 문 헌

[1] (사)한국정보시스템감리인협회, "정보시스템 운영. 보안 감리지침," 2002.

[2] BS7799-1:1999, "Information Security Management - Part 1: Code of practice for information security management," 1999.

[3] BS7799-2:1999, "Information Security Management - Part 2: Specification for information security management systems," 1999.

[4] 금융감독원, "검사업무 편람VI-정보기술(IT)부분 검사업무," 2000.12

[5] COBIT 운영위원회 및 정보시스템감사 . 통제재단, "COBIT 프레임워크," 1998. 4.

[6] COBIT 운영위원회 및 정보시스템감사 . 통제재단, "COBIT 프레임워크: 경영자를 위한 요약," 1998. 4.

[7] ISO/IEC TR 13335-1, "Information Technology-Guidelines for the Management of IT Security - Part 1 : Concepts and models for IT Security," 1996.

[8] ISO/IEC TR 13335-2, "Information Technology-Guidelines for the Management of IT Security - Part 2 : Managing and planning IT Security," 1997.

[9] ISO/IEC TR 13335-3, "Information Technology-Guidelines for the Management of IT Security - Part 3 : Techniques for IT Security," 1998.

[10] ISO/IEC TR 13335-4, "Information Technology-Guidelines for the Management of IT Security - Part 4 : Selection of Safeguards," 2000.

[11] ISO/IEC TR 13335-5, "Information Technology-Guidelines for the Management of IT Security - Part 5 : Management guidance on network security," 2001.

◐ 저 자 소 개 ◑

전 용 준

1988년 한국방송통신대학 전자계산학과 졸업(학사)
2003년 전북대학교 대학원 컴퓨터 과학과 졸업(석사)
2006년 전북대학교 대학원 정보보호공학과 수료(박사)
1992년 전라북도청 전산사무관
1998년~2005년 정보통신 담당관실 관리계장, 행정정보계장
2005년~2006년 전라북도청 지방서기관
2006년 현재 전라북도청 정보통신담당관
관심분야 : 정보보안, 이동컴퓨팅, 무선인터넷
전자우편 : yjjun@ejeonbuk.net

조 기 환

1987년 서울대학교 계산통계학과 졸업(석사)
1996년 영국 Newcastle 대학교 전산학과 졸업(박사)
1987년~1997년 한국전자통신연구원 선임연구원
1997년~1999년 목포대학교 컴퓨터과학과 전임강사
1999년~현재 전북대학교 전자정보공학부 부교수
관심분야 : 이동컴퓨팅, 무선인터넷, 네트워크보안, 컴퓨터통신
전자우편 : ghcho@chonbuk.ac.kr

김 원 규

1991년 한국외국어대학교 컴퓨터공학과 졸업(학사)
1990년~1995년 LG히다찌 개발팀 근무
1995년~1998년 메리츠 증권 전산실 근무
1998년~현재 나일소프트 정보보안 컨설팅 근무
관심분야 : 보안, etc.
전자우편 : kwk@nilesoft.co.kr