情 報 保 護 學 會 誌
第20卷 第1號, 2010. 2

정보보호관리체계(ISMS) 인증심사 결함사항 분석에 관한 연구

장 상 수*, 이 호 섭*

요 약

인터넷이 급속하게 확산되면서 그 동안 오프라인 환경에서만 가능하던 많은 일들을 사이버 상에서도 가능하게 해준 반면에 해킹이나 바이러스 등 새로운 보안위협도 증가하게 되었다. 최근 기업이나 조직에서는 산발적인 보안 관리에서 종합적이고 체계적인 정보보호관리체계가 요구되고 있으며 국내에서도 2001년 7월부터 정보보호관리체계(ISMS) 인증제도가 시행되어, 2009년 12월 현재 77개 업체(기관)가 인증을 받았으며, ISO27001 인증 건수도 100여건에 이르고 있다. 이와 같이 ISMS 인증제도가 국내에 도입된 이래 인증수요는 꾸준히 증가하여 기업경쟁력의 중요한 수단으로 인식되어 가고 있는 추세인 반면 ISMS 인증의 실수요자가 인식하는 인증의 효과성 등의 질적인 측면이 미흡하다는 문제는 끊임없이 제기되어 오고 있다. 본 고에서는 그동안 인증취득기관의 정보보호관리체계(ISMS) 인증 심사과정에서 지적된 결함사례를 분석하고, 국내 중소, 대기업들이 정보보호관리체계를 수립하여 운영하는 과정에서 공통적으로 나타나는 결함사항을 도출함으로써, 향후 기업들이 정보보호관리체계를 수립하는 과정에서 중점적으로 고려해야 할 사항들이 무엇인지 고찰하고자 한다.

Ⅰ. 서 론

정보통신기술의 발전 및 인터넷의 확산으로 개개인의 생활양식이 현격하게 바뀌고 있고 기업의 비즈니스 양태도 획기적으로 변화되고 있을 뿐만 아니라 새로운 비즈니스가 폭발적으로 창출되고 있다. 그러나 이러한 변화의 이면에는 해킹, 바이러스, 개인정보 유출 등의 역기능 또한 비약적으로 커지고 있다.

따라서 이러한 역기능에 효과적으로 대응하는 것이 정부, 기업, 개인 등의 각 행위주체들에게 핵심적인 과제로 대두되고 있다. 특히 현대사회의 중추라고 할 수 있는 기업들에게 경영에 있어서 보안관리(Information Security Management)는 하나의 경영관리요소로 인식되어 가고 있다. 이러한 보안 관리에 대한 외부의 독립적인 평가 또는 인증의 필요성도 점차 강조되고 있으며, 국내에서도 2001년 7월부터 정보보호관리체계(ISMS) 인증제도가 시행되어 오고 있으며 2009년 12월 현재 77개 업체(기관)가 인증을 받았으며, ISO27001 인증건수도 100여건에 이르고 있다. 이와 같이 ISMS 인증제도가 국내에 도입된 이래 인증수요는 꾸준히 증가하여 기업경쟁력의 중요한 수단으로 인식되어 가고 있는 추세이다.

그러나 ISMS 인증제도는 기업의 정보자산을 보호하고 기업경쟁력을 강화하는 방안으로 활용되고 있으나 인증의 실수요자가 인식하는 인증의 효과성 등의 질적인 측면이 미흡하다는 문제가 제기되고 있다. 특히, 인증기업들이 인증을 통하여 기업의 서비스의 질을 향상시켜 고객만족과 대외적인 신뢰 구축을 이루어 경영혁신의 기회로 삼아야 함에도 인증 획득 자체에만 몰두하여 인증의 본래 의미가 많이 상실되어 가는 실정이다.

이런 이유로 국내 ISMS 인증 기업수가 크게 증가하지 않는 것으로 보이며, 이는 인증을 통한 기업경쟁력 강화의 실효성을 느끼지 못하거나 인식하지 못하기 때문인 것으로 판단된다. 따라서 기업이 ISMS 인증획득만을 목적으로 삼기보다는 기업의 생존여부의 수단으로 확실히 자리매김할 수 있도록 하는 유인책이 요구되는

* 한국인터넷진흥원(KISA) 인터넷 · 정보보호본부 기업보안관리팀(isms@kisa.or.kr)

시점이다. 즉, 기업은 정보보호 활동의 기반을 마련하고 조직의 지속성장이 가능하도록 비즈니스와 연계된 정보보호관리체계 구축이 필요한 것이다.

본 논문에서는 먼저 국내 정보보호관리체계 인증제도에 대한 개요, 절차, 현황 등을 살펴보고, 실제 기업들이 정보보호관리체계를 수립하여 운영하는 과정에서 발견되었던 결함사례를 분석하고, 주요 결함을 도출함으로써, 향후 기업들이 정보보호관리체계 수립 시 중점적으로 고려해야할 요구사항이 무엇인지에 대해 알아본다.

Ⅱ. 이론적 배경

2.1 정보보호관리체계 인증제도

2.1.1 개요

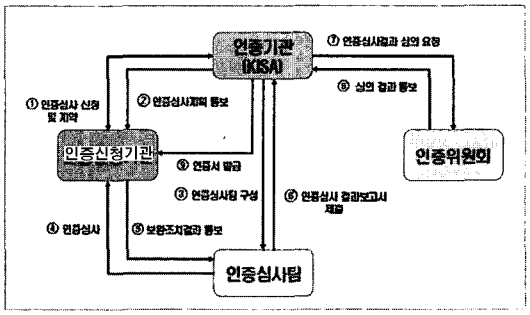
조직의 자산에 대한 안전성 및 신뢰성을 향상시키기 위한 절차와 과정을 체계적으로 수립하고 문서화하여 지속적으로 관리·운영하고 정보보호의 목표인 정보의 기밀성, 무결성, 가용성을 실현하기 위한 일련의 과정 및 정보보호에 대한 지속적인 개선활동을 정보보호관리체계(ISMS)라고 한다.

또한 기업(조직 또는 사업장의 일부 또는 전체)이 수립하여 운영하고 있는 이러한 정보보호관리체계가 일정한 인증심사기준에 적합한지 여부를 제3자인 인증기관이 객관적이고 독립적으로 평가하여 기준에 대한 적합여부를 보증해주는 제도를 정보보호관리체계 인증제도라고 할 수 있다.

우리나라에서는 「정보통신망이용촉진및정보보호등에관한법률」 제47조에 [정보보호관리체계의 인증] 이라는 법적 근거를 두고 기술적·물리적 보호조치를 포함한 종합적 관리체계가 인증심사기준에 적합한지 여부를 방송통신위원회 산하기관인 한국인터넷진흥원으로부터 인증 받도록 하고 있다.

2.1.2 인증절차

인증 취득을 원하는 기업이 인증심사를 신청하고 인증서를 발급받기까지는 약 3개월의 시간이 소요된다. 정보보호관리체계 인증은 크게 4단계로 진행된다. 첫째, 인증신청 및 계약을 준비하는 준비단계, 심사팀(기본 4명으로 구성)이 문서심사 및 기술심사를 한 후 그 결과 발견된 결함사항을 신청기관이 보완조치(보완조치기간 : 1개월)하는 심사단계, 인증위원회가 인증심사결과를 심의하여 인증서를 교부하는 인증단계, 인증취득기관이 정보보호관리체계를 지속적으로 운영하는 지를 심사하는 사후관리단계로 구분된다. 이상의 절차를 기본적인 흐름으로 도식화하면 [그림 1]과 같다.



〔그림 1〕 인증절차의 기본 흐름

2.1.3 인증심사의 종류

인증심사에는 최초인증심사, 사후관리심사, 갱신심사, 재심사의 4가지로 구분된다.

• 최초인증심사

기업이 수립하여 운영하는 정보보호관리체계가 방송통신위원회에서 고시한 정보보호관리체계 인증심사기준에 적합한지에 대하여 최초로 확인하는 심사를 말한다.

• 사후관리심사

인증을 취득한 기관이 인증심사기준에 적합하게 정보보호관리체계를 운영 및 유지하고 있는 지 1년에 1회 이상 점검하는 심사를 말한다.

• 갱신심사

인증을 취득한 기관이 3년의 인증유효기간 만료일 이전에 인증 유효기간을 연장하기 위한 심사를 말한다.

• 재심사

인증을 취득한 기관이 인증의 유효기간 내에 인증 받은 정보보호관리체계 범위 내에서 중대한 변화가 발생하였을 경우, 신청인의 신청에 의해 인증기관이 실시하는 심사를 말한다.

2.1.4 인증서 발급 현황

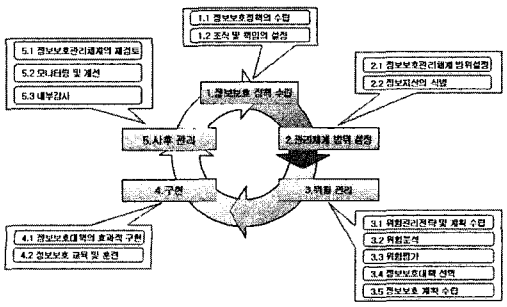
2002년 5월 첫 인증서를 발급한 이후 2009년 12월 현재까지 총 77건의 인증서를 발급하였다. 2004년까지 통신, 금융, 정보보호컨설팅 전문업체에 집중되던 인증분야를 2005년 이후 특히, 개인정보보호가 중요시 되고 있는 대형포탈, 금융, 의료, 교육분야 등으로 인증분야를 확대하고 있다. 본 연구에서는 77개 업체(기관)에 대한 인증심사 진행 시 발견된 결함사항을 활용하여 분석을 진행한다.

2.2 정보보호관리체계 인증 요구사항

정보보호관리체계 인증심사 기준은 2008년 5월 방송통신위원회 고시(제2008-11호)로 공표하였으며, 필수사항인 정보보호 5단계 관리과정 요구사항 14개 항목, 문서화 요구사항 3개 필수항목과 선택사항인 정보보호대책 120개 항목으로 총 137개로 구성되어 있다. 인증신청 기업은 137개 심사기준의 요구사항을 충족하여야 인증을 받을 수 있다. 실제로는 137개 심사기준에 대한 세부통제사항 수는 446개로 세분화될 수 있다.

2.2.1 정보보호관리과정 5단계

정보보호관리체계는 ① 정보보호정책 수립 ② 정보보호관리체계 범위 설정 ③ 위험관리 ④ 구현 ⑤ 사후관리의 5단계 과정을 거쳐 수립·운영된다. 새로운 위협요소 및 취약성 발견 등 지속적으로 변화하는 IT 및 인터넷 환경에서 업체 내부의 주요 정보자산을 효과적으로 보호하고 관리하기 위해서는 주기적인 위험분석을 통한 지속적인 사후관리가 필요하다. 이 관리과정은 일회적인 단계가 아니라, 지속적으로 유지 관리되어야 하는 순환 주기의 형태를 가진다. [그림 2]에서 이러한 관리과정의 순환적 절차를 보여준다. 정보보호관리과정 5단계에 대한 심사기준은 총 14개 통제사항으로 구성되어 있다.



〔그림 2〕 정보보호관리체계 5단계 관리과정

2.2.2 문서화 과정

정보보호관리체계 수립 및 운영의 근거는 정책, 지침, 절차 등으로 항상 문서화되어야 한다. 이러한 문서 관리에 대한 요구사항을 인증심사 기준에는 다음과 같이 3개 사항으로 제시하고 있다.

• 문서요건

정보보호관리체계와 관련한 문서는 기업의 모든 임직원 및 관련자들이 쉽게 이용할 수 있도록, 해당 기업의 규모 기능 등을 고려하여 문서화해야 한다.

• 문서의 통제

작성된 문서는 문서의 발생 타당성 승인, 갱신, 개정, 배포, 폐기 등의 통제를 위한 절차를 수립하여야 한다.

• 운영기록의 통제

정보보호관리체계를 효과적, 효율적으로 운영하기 위해서 기록을 확인, 유지보수, 보존, 폐기하는 문서화된 절차를 수립하고 유지·관리하여야 한다.

2.2.3 정보보호대책

정보보호관리체계는 쉽게 말해 정보보호에 관련된 위험을 통제하기 위한 대책을 수립하고 관리하는 체계라고 할 수 있다. 따라서, 인증심사 기준에서는 15개 통제분야에 대해 120개 세부통제사항을 제시하고 있다.

2.3 국외 ISMS

국제 표준화 기구 ISO(International Organization for Standardization)와 IEC(International Electrotechnical Commission)는 연합위원회(Joint Technical Committee)를 구성하여 2005년에 ISMS(Information Security Management System)에 대한 국제 표준인 ISO/IEC 27001(Information security management systems-Requirement)과 ISO/IEC 27002(Code of practice for

〔표 1〕 정보보호관리체계 인증 정보보호대책

통제분야	세부통제사항	항목수
1. 정보보호 정책	정책의 승인 및 공표, 체계, 유지관리	5
2. 정보보호 조직	조직의 체계 및 책임과 역할	4
3. 외부자 보안	계약 및 서비스 수준협약 등	4
4. 정보자산 분류	정보자산의 조사 및 책임할당, 정보자산의 분류 및 취급	4
5. 정보보호 교육 및 훈련	교육 및 훈련프로그램 수립, 교육훈련의 시행 및 평가	4
6. 인적보안	책임할당 및 규정화, 직원의 적격심사, 주요직무담당자 관리, 비밀유지	5
7. 물리적 보안	물리적 보호구역, 물리적 접근통제, 데이터 센터 보안, 장비보호, 사무실 보호 등	12
8. 시스템개발 보안	분석 및 설계, 구현 및 이행, 변경관리	13
9. 암호통제	암호정책, 암호사용, 키관리	3
10. 접근통제	접근통제 정책, 사용자접근관리, 접근통제 영역 등	14
11. 운영관리	운영절차와 책임, 시스템/네트워크 운영관리, 악성소프웨어 통제 등	22
12. 전자거래 보안	교환합의서, 전자거래, 전자우편, 공개서버의 보안관리, 이용자 공지사항	5
13. 보안사고 관리	대응계획 및 체계, 대응 및 복구	7
14. 검토, 모니터링 및 감사	법적 요구사항 준수 검토, 정보보호정책 및 대책 준수 검토, 모니터링, 보안감사	11
15. 업무연속성관리	업무연속성 계획 수립과 구현, 시험, 유지관리	7

information security management)를 발표하였다.

이 표준은 원래 BS(British Standard) 7799에서 발전한 것으로, 모범사례는 BS 7799 Part 1, 인증 기준은 BS7799 Part 2로 나뉘어져 BS 7799 Part 1이 ISO/IEC 17799로 먼저 국제 표준이 되었고, BS 7799 Part 2가 뒤이어 국제 표준이 되었다. 개정 작업을 통하여 2005년에는 현재 인증기준을 위해 사용 중인 ISO/IEC 27001과 모범사례의 집합인 ISO/IEC 27002로 바뀌었다.

정보보호관리체계에 대한 국제인증을 받기 위해서는 Part 1의 실행지침(ISO27002)에 따라 자체적인 체계를 수립하고, 일정 기간 이행한 기록을 토대로 Part 2 규격(ISO27001)에 따라 심사를 받아야 한다.

2.4 국내외 ISMS비교

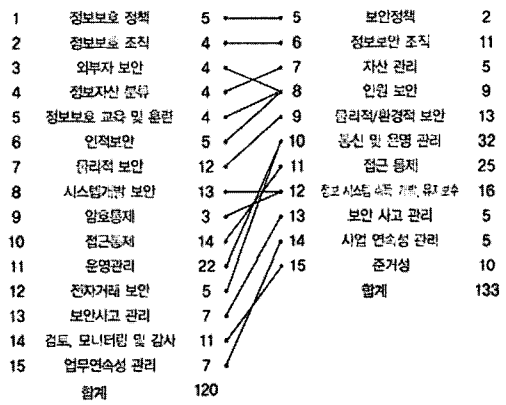
정보보호관리체계에 대한 국내외 인증을 받기 위해서는 각각의 인증심사 기준에 만족하도록 기관의 환경에 최적화된 정보보호관리체계 수립 및 운영이 이루어져야 한다. 여기서 말하는 국내외 인증심사 기준은 보안통제항목으로 구성되어 있으며, 각 보안통제항목에는 보안업무를 수행함에 있어서 요구되는 세부적인 보안요건 등을 정의하고 있다.

국내외 인증표준을 구성하고 있는 통제항목별 세부보안 요구사항들을 비교할 경우 [그림 3]과 같이 통제항목간의 매칭이 가능하다. 각각의 통제항목을 15개 또는 11개로 분류하고 세부항목을 정의하고 있지만 통제항목을 구성하고 있는 대부분의 보안요구사항이 비슷하게 구성되어 있다.

국내 ISMS의 경우 국제표준(ISO27001)을 모두 포함하면서 국내 환경에 적합하도록 모형을 개발하여 5개 관리과정(14단계), 문서화, 15개 분야로 세분화함에 따라 ISO27001의 11개 항목에 추가된 4개 분야(3. 외부자 보안 5. 정보보호 교육 및 훈련 9. 암호통제 12. 전자거래 보안)에 대해 보다 더 강조되어 설계되었다.

통제항목의 많고 적음이 보안수준을 높이거나 낮추는 것은 아니지만 국내 ISMS의 경우 세부체크리스트가 442개로 ISO27001보다 많은 통제항목으로 구성되었으며, 각 기업체의 정보보호관리체계에서 필요한 통제항목을 선택하고 각 보안요구사항에 대해 관리체계를 마련해 이행함으로써 보안수준을 체계적으로 향상시킬 수 있다.

국내에서는 ISMS와 ISO27001 인증제도가 공존하고



〔그림 3〕 국내 ISMS와 ISO27001 통제항목별 연관도

있는 실정으로 ISO27001 인증의 경우 BSI Korea (http://asia.bsi-global.com/Korea/index.xalter), DNV(http:// www.dnv.co. kr)와 같은 인증기관에, 국내 ISMS의 경우 KISA(Korea Internet & Security Agency, http://www.kisa.or.kr)에서 수행하고 있다. 신청기관은 인증범위, 인증심사 일정 등에 대해 인증기관과 협의해 인증심사에 대한 계약을 체결한다.

인증을 획득한 이후에도 ISO27001 인증의 경우 6개월 주기로, 국내 ISMS의 경우 1년 주기로 사후 심사를 받아야 인증을 유지할 수 있다. 사후심사는 지속적인 정보보호관리체계의 유지여부를 점검하기 위해 시행되며, 심사기간은 짧지만 본심사와 동일하게 이루어진다. 이때 중대한 문제가 발견된 경우 본심사와 동일하게 인증이 취소될 수 있다. 인증유효기간은 3년으로, 유효기간이 완료되는 시점에 재심사를 받아야 하며, 인증범위에 중대한 변경사항이 발생한 경우에도 재심사를 받아야 한다.

2.5 ISMS 인증 목적 및 기대효과

기업들이 ISMS 인증을 획득하게 되는 주요 동기나 기대효과로는 다음과 같이 정리할 수 있다.

첫째로 현재의 정보 시스템 운영상에 처해있는 위협으로부터 발생할 수 있는 손실 가능성을 정량적으로 예측/대처 하고 위험의 수준을 관리자나 사용자가 이해하고 위험 가능성을 줄일 수 있다. 둘째로 조직의 자산에 대한 안전성, 효과성, 효율성, 신뢰성을 향상시킬 수 있다. 셋째로 위험 분석 및 평가를 통한 위험수준의 가시적 표현으로 관리자와 사용자의 보안의식 고취를 할 수 있다. 넷째로 위험 발생 가능성이 높은 부분에 대해 우선순위와 비용/효과적인 측면을 고려하여 보안대책을 선정할 수 있도록 의사결정을 지원한다. 다섯째로 정보보호 관리를 제대로 하고 있다는 것을 국가인증기관으로부터 인정받게 되는 것이므로 대외적인 신뢰도와 경쟁력을 제고 할 수 있다. 여섯째로 관련 법규나 절차, 지침 등을 준수하고 있다는 것을 이용자 또는 거래 당사자에게 알려 기업의 이미지 제고를 할 수 있다. 일곱째로 기업 경영의 목표를 실질적으로 지원 할 수 있다.

하지만 위에서 살펴본 바와 같이 인증을 취득한 조직에게는 여러 가지 효과가 있지만 대부분의 효과가 눈에 보이지 않기 때문에 정보보호 관리체계 인증 제도를 통한 전통적 비용/효과 분석방법으로 정당화하기는 매우 어렵고 부가적으로 얻을 수 있는 유무형의 측정요소를 도출하여 분석하고 관리하기에는 많은 어려움이 있다.

Ⅲ. 결함사항 분석

3.1 분석 방법

한국인터넷진흥원에서 2009년도에는 (주)비씨카드, (주)모빌리언스 등 고객의 지불·결제정보를 취급하는 금융 및 전자결제 서비스 기업을 중심으로 인증 대상을 확대하여 총55건(신규19건, 사후31건, 갱신 5건)의 인증심사를 수행하였으며, 2009년 12월말까지 인증서 발급 누적 건수는 총 77건이 되었다. 2007년~2009년(3년)간 인증심사 수행결과를 토대로 주요 결함을 도출한 결과, 주요정보 유출, 보안사고 발생, 기업신뢰도의 저하를 가져 올 수 있는 심각한 결함들이 반복적으로 발생하고 있어, 기업의 효과적인 보안관리를 위해서는 아래 주요결함 분석결과를 고려하여 조직 환경에 적합한 보안관리 지침 및 절차를 체계적으로 수립하고, 이에 따른 실질적인 보안조치 이행이 중요할 것으로 보인다.

3.2 주요 결함 및 보안조치 방안

3.2.1 '07년~'09년 인증심사별 보안관리 결함 Top 10

'09년 40개 기업, '08년 44개 기업, '09년 50개 기업

〔표 2〕 2009년 ISMS 인증 기업 보안관리 결함 Top 10

Top 10	2009년 ISMS 인증 기업 보안관리 결함 (50개 기업)	결함 건수	발생 비율
1	관리자 계정 등 주요 패스워드 관리 미흡	14건	28%
2	개인정보보호법 등 법적 요구사항 준수 미흡	13건	26%
3	내부감사 규정 부재 및 주기적 감사 미흡	12건	24%
4	정보보호 직무에 대한 책임과 역할 불명확	11건	22%
5	사용자 접근권한에 대한 정기적인 점검 미이행	11건	22%
6	주요시스템 보호를 위한 네트워크 대책 미흡	11건	22%
7	주요 정보자산의 변경관리 절차 미흡	10건	20%
8	백업관련 지침(계획) 부재 및 미 준수	10건	20%
9	정보보호시스템 접근통제 정책(Rule Set) 검토 미흡	10건	20%
10	보안사고 정의, 대응 복구 절차 등 보안관리 미흡	10건	20%

〔표 3〕 2008년 ISMS 인증 기업 보안관리 결함 Top 10

Top 10	2008년 ISMS 인증 기업 보안관리 결함 (44개 기업)	결함 건수	발생 비율
1	정보자산의 보안등급 분류 미비, 취급절차 부재 및 미준수	20건	34%
2	사용자 계정 생성/변경/삭제 등 계정관리 절차 부재 및 관리자 계정 공동사용	18건	31%
3	주요정보의 저장, 전송 시 암호사용 절차 부재	15건	25%
4	백업관련 지침(계획) 부재 및 미준수	13건	22%
5	주요 정보자산에 대한 취약점/위협 분석 누락 등 위험분석 누락 등 위험분석 미흡	13건	22%
6	내부감사 규정 부재 및 주기적 감사 미흡	11건	18%
7	관리자 계정 등 주요 패스워드 관리 미흡	11건	18%
8	물리적 보호구역 미정의 및 반출입 절차 부재	11건	18%
9	환경변화에 따른 ISMS 효율성, 적절성 등 정기적 재검토 과정 미흡	10건	17%
10	보안사고 정의, 대응 복구 절차 등 보안관리 미흡	9건	15%

〔표 4〕 2007년 ISMS 인증 기업 보안관리 결함 Top 10

Top 10	2007년 ISMS 인증 기업 보안관리 결함(40개 기업)	결함 건수	발생 비율
1	백업관련 지침(계획) 부재 및 미준수	16건	40%
2	정보자산의 보안등급 분류 미비, 취급절차 부재 및 미준수	15건	37%
3	관리자 계정 등 주요 패스워드 관리 미흡	12건	30%
4	주요 정보자산의 변경관리 절차 미흡	10건	25%
5	보안사고 정의, 대응 복구 절차 등 보안관리 미흡	9건	22%
6	정보보호교육 계획 부재 및 교육 미실시	9건	22%
7	물리적 보호구역 미정의 및 반출입 절차 부재	8건	20%
8	주요 정보자산에 대한 취약점/위협 분석 누락 등 위험분석 누락 등 위험분석 미흡	7건	17%
9	내부감사 규정 부재 및 주기적 감사 미흡	7건	17%
10	기업의 주요정보 유출방지를 위한 비밀유지서약서 미 요구 (정규, 비정규직원, 제3자 등)	7건	17%

의 인증심사를 통해 도출된 결함을 분석한 결과 보안관리 결함 Top 10에 해당하는 세부통제사항은 [표 2]~[표 4]와 같다. 인증 업체(기관)의 결함 발생비율은 아래와 같이 15%~40%까지 나타남으로써, 기업 보안관리의 심각성을 보여주고 있다.

3.2.2 주요 결함 및 발생 사례

최근 3년간(2007년~2009년)의 ISMS 인증심사를 통해 도출된 결함 Top 10을 분석한 결과, 조사기간 중 빈번하게 나타나는 주요 결함이 있었다. 내용은 주요 시스템 패스워드의 공동사용, 유추하기 쉬운 패스워드(예: 1234, qwer, 유추하기 쉬운 단어 등), 보안사고 복구 대응 지침·절차 미 수립 등으로 인한 주요정보 유출, 보안사고 증가, 기업신뢰도의 저하를 가져 올 수 있는 결함들이 존재한다.

상기 주요 결함들은 보안관리자의 인식부족, 관리 지침 및 절차가 미흡하여 발생하는 결함들로 보안조치를 함으로써 예방이 가능하다.

〔표 5〕 주요 결함 및 발생 사례

주요 결함	발생 사례	연간 결함건수		
		'07년 (40개 기업)	'08년 (44개 기업)	'09년 (50개 기업)
백업관련 지침(계획) 부재 및 미 준수	시스템 접속 및 운영기록 등 주요 로그파일에 대한 백업이 이루어지고 있지 않아 침해사고 발생 시 사고조사 및 분석, 신속한 대응이 어려움	16 (40%)	13 (29%)	10 (20%)
관리자 계정 등 주요 패스워드 관리 미흡	주요 시스템 관리자 패스워드의 공동사용, 유추하기 쉬운 패스워드(예: 1234, qwer, 단어) 사용으로 시스템 침입 및 중요정보(내부정보, 개인정보 등)의 유출 가능성이 높아짐	12 (30%)	11 (25%)	14 (28%)
내부 감사 규정 부재 및 주기적 감사 미흡	구체적인 내부감사 규정이 없거나 주기적인 감사 미실시로 내부기밀의 유출 및 부정 사용 등의 피해 발생 및 적기 탐지가 이루어지지 않을 가능성이 있음	7 (17%)	11 (25%)	12 (24%)
보안사고 정의, 대응 복구 절차 등 보안관리 미흡	해킹, 바이러스, 웜 등의 다양한 위협요소로 인한 보안사고 발생 시, 신속한 사고대응 및 복구가 어려워 자산 손실, 기업신뢰도 저하 등의 피해를 입을 수 있음	9 (22%)	9 (20%)	10 (20%)

3.2.3 주요 결함에 대한 보안조치 방안

주요 결함 분석결과를 고려하여 조직환경에 적합한 보안관리 지침 및 절차를 체계적으로 수립하고, 이에 따른 실질적인 보안조치의 이행이 중요하다. 주요 결함에 대한 보안조치 방안은 [표 6]과 같다.

[표 6] 주요 결함에 대한 보안조치 방안

주요 결함	보안조치 방안
백업 관련 지침 (계획) 부재 및 미 준수	○데이터의 무결성 및 장비의 가용성을 유지하기 위해 백업/복구 지침 및 절차를 수립·문서화하고, 기 수립된 지침 및 절차에 따라 정기적인 백업과 주기적인 테스트를 실시해야 함 ○백업된 매체는 용이한 식별을 위해 현황관리가 이루어져야 하며, 보안사고 발생시 적시에 복구할 수 있도록 주기적인 관리가 필요함
관리자 계정 등 주요 패스워드 관리 미흡	○정보시스템 및 서비스에 대한 접근을 통제하기 위한 공식적인 사용자 등록 및 해지 절차를 마련하여야 하고, 정보유출(내부기밀, 고객정보 등) 사고에 대비하기 위한 패스워드 관리 지침 수립 및 정기 점검이 필요함 ※ 패스워드 관리 지침의 주요내용 : 최소길이, 영문 혼합, 변경 주기, 임계값 및 복잡도 설정 등 중요도 및 심각도에 따라 세부적 관리가 이루어지도록 지침 수립
내부 감사 규정 부재 및 주기적 감사 미흡	○기업의 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되는 지를 점검하기 위하여 감사의 대상, 기준, 범위, 절차, 감사자, 감사도구, 주기 및 방법 등을 구체적으로 규정하고, 계획된 주기로 내부감사를 수행하여야 함
보안 사고 정의, 대응 복구 절차 등 보안 관리 미흡	○보안사고의 정의 및 범위, 긴급연락체계 구축, 보안사고 발생 시 보고 및 대응절차, 사고 복구조직의 구성, 교육계획 등을 포함한 보안사고 대응 계획을 수립·시행하여야 함 ※ 침해사고 발생 시 파급영향의 정도에 따라 정의한 심각도별 대응 절차 수립시 보안특성인 기밀성, 무결성, 가용성 등을 종합적으로 고려해야 하며, 보안사고시 신속한 대응 및 복구를 위해 절차에 따른 정기적인 테스트 필요

Ⅳ. 결 론

2007년~2009년 12월 현재까지 ISMS 인증을 취득한 업체(기관)를 대상으로 인증심사를 통해 도출된 주요 결함을 선정하여 그 특징과 보안조치 방안을 제시하였다. 기업들은 정보보호관리에 대한 중요성을 이미 인식하고 있으나, 경영층의 지원 부족, 컨설팅 비용 부담, 전문적인 지식 부족 등의 이유로 정보보호관리체계를 구축하는데 어려움을 겪고 있다. 본 연구는 정보보호관리체계의 수립·운영 시 특히 고려해야 할 결함사례를 제시함으로서, 기업들이 정보보호관리체계를 수립하는데 도움이 될 것으로 판단된다. 기업의 보안관리 상 나타나는 결함들이 발생 또는 재발하지 않도록 지속적인 정보보호관리체계의 사후관리가 필요하고, 기업 스스로가 조직 환경에 적합한 보안관리를 하는 것이 중요하다. 향후 정보보호관리체계의 수준 향상 및 성과 측정 모델 지표를 개발하여 ISMS 인증제도의 수준을 평가하고 발전시킬 수 있는 연구가 필요하다.

참고문헌

[1] 정보통신부, "정보통신망 이용촉진 및 정보보호 등에 관한 법률 제7262호 제 47조", 2006.

[2] 정보통신부, "정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제23조의2", 2006.

[3] 정보통신부, "정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙 제6조", 2006.

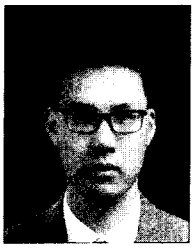
[4] 정보통신부, "정보보호관리체계 인증심사 기준", 정보통신부 고시 제2002-22호, 2002.

[5] 한국정보보호진흥원, "정보보호관리체계 인증업무 지침", 2003

[6] 한국정보보호진흥원, "정보보호관리체계 인증 가이드 5종", 2003

[7] 장상수, "정보보호관리체계 인증제도 시행", 한국정보보호진흥원, 2003.

〈著者紹介〉



장 상 수 (Jang SangSu)

1989년 2월: 한국항공대학교 항공정보통신공학과 졸업
2004년 2월: 동국대학교 정보보호학과 석사
2006년 2월: 전남대학교 정보보호학과 박사과정
2000년 1월~현재: 한국인터넷진흥원 인터넷기반개인정보보호단 기업보안관리팀 팀장
<관심분야> 정보보호관리, 정보보호 안전진단, 네트워크 보안

이 호 섭 (Lee HoSeop)

2009년 2월: 평택대학교 컴퓨터과학과 졸업
2009년 2월~현재: 한국인터넷진흥원 인터넷기반개인정보보호단 기업보안관리팀 주임연구원
<관심분야> 정보보호관리, 정보보호컨설팅, 내부감사, 웹 보안