情 報 保 護 學 會 誌
第17卷 第4號, 2007. 8

정보보호관리체계(ISMS) 구축 시 일반적으로 나타나는 결함사례에 관한 분석

고규만*, 김재성*, 장상수*

요 약

한국정보보호진흥원이 정보통신망이용촉진및정보보호등에관한법률 제47조에 근거를 두고 시행하고 있는 정보보호관리체계(ISMS) 인증제도는 2002년 제도가 시행된 이후 현재까지 44개 기업이 인증을 취득하였다. 본 고에서는 그동안 인증취득기관의 정보보호관리체계(ISMS) 인증 심사과정에서 지적된 결함사례를 분석함으로써, 국내 중소, 대기업들이 정보보호관리체계를 수립하여 운영하는 과정에서 공통적으로 나타나는 결함사항을 정리하고, 향후 기업들이 정보보호관리체계를 수립하는 과정에서 중점적으로 고려해야 할 사항들이 무엇인지 고찰하고자 한다.

Ⅰ. 서 론

초고속 인터넷의 빠른 보급과 더불어 인터넷의 사용은 개인, 기업, 공공분야 등 전 분야에 걸쳐 보편화되었고, 급속한 정보화의 물결과 맞물려 고객의 개인정보 및 산업기밀 유출 등 다양한 역기능으로 인해 기업의 손실이 점차 늘어나고 있는 것이 현실이다. 이에, 많은 기업들은 정보보호활동이 단지 기업의 사업을 수행하기 위한 지원요소가 아니라, 기업의 사업목표를 달성하기 위한 핵심적인 요소로 인식하기 시작했다. 이제 기업의 사업목표 달성과 직접적으로 연계되어 있는 정보보호 목표를 달성하기 위해서는 그동안 수행되어 왔던 단편적인 정보보호활동만으로는 한계에 다다른 것이 사실이다. 이에 국내·외적으로 정보보호에 대한 체계적이고 조직적인 관리를 위한 노력이 확산되고 있으며, 국내에서도 정보보호관리체계 인증제도에 대한 연구를 2000년부터 진행하여 2001년 "정보통신망이용촉진 및 정보보호 등에 관한 법률"을 개정하여 정보통신부가 인증제도 시행을 공표함으로서, 2002년부터 정보보호관리체계(Information Security Management System) 인증제도를 본격적으로 시행하는 계기가 되었다. 도입배경으로는 국내 환경에 적합한 정보보호관리 모델을 개발·보급함으로써 국내 기업들의 정보보호관리체계 수립을 지원하고 정보통신망의 안전·신뢰성을 강화하는데 있다. 또한 현재까지, 한국정보보호진흥원이 인증기관으로서 인증심사, 지침배포, 기술자문, 인증심사원 양성 및 교육 등 국내 정보보호관리 수준 향상을 위해 다양한 노력하고 있다. 특히, 게임, 포털, 의료, 학교 등 다양한 분야에서 개인정보 관리의 중요성이 부각됨에 따라, 기업들이 고객 신뢰성 확보 및 이미지 제고 방안으로 정보보호관리체계 수립을 택하는 사례가 늘어날 전망이다. 본 논문에서는 먼저 국내 정보보호관리체계 인증제도에 대한 개요, 절차, 현황 등을 살펴보고, 실제 기업들이 정보보호관리체계 수립하여 운영하는 과정에서 발견되었던 결함사례를 다양한 형태로 분석함으로써, 향후 기업들이 정보보호관리체계 수립 시 중점적으로 고려해야할 요구사항이 무엇인지에 대해 알아본다.

Ⅱ. 정보보호관리체계 인증제도

2.1. 개 요

정보보호관리체계 인증제도란, 정보보호를 위한 기업 내의 일련의 활동을 137개 심사기준 적합성 여부를 한국정보보호진흥원이 객관적인 심사를 거쳐 인증을 부여하는 제도이다. 2006년까지는 인증대상을 정보통신서비스제공자, '정보통신서비스제공자에게 물리적 시설을 제공하는 자'로서 집적된 정보통신시설을 운영·관

* 한국정보보호진흥원 IT기반보호단 기반보호팀(kmko@kisa.or.kr, kimjs@kisa.or.kr, ssjang@kisa.or.kr)

리하는 자, 정보통신망을 운영하는 민간사업자로 크게 3개 대상으로 구분하였으나, 2007년에는 대상자 규정을 삭제하여 정보보호관리체계를 수립·운영하고 있는 자는 모두 인증을 받을 수 있도록 정보통신망법을 개정하였다. 정보통신망법에서는 정보보호관리체계를 정보통신망의 안정성을 확보하고 조직의 정보자산을 보호하기 위해 기술, 관리, 물리적 정보보호대책을 구현하여 지속적으로 관리·운영하는 종합적 시스템으로 정의하고 있다.

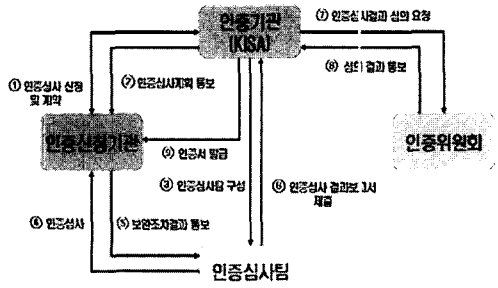
2.2. 인증절차

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(보완조치 기간 : 1개월)하는 심사단계, 인증위원회가 인증심사결과를 심의하여 인증서를 교부하는 인증단계, 인증취득 기관이 정보보호관리체계를 지속적으로 운영하는 지를 심사하는 사후관리단계로 구분된다. 이상의 절차를 기본적인 흐름으로 도식화하면 〔그림 1〕과 같다.

2.3. 인증심사의 종류

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

- 최초인증심사
  기업이 수립하여 운영하는 정보보호관리체계가 정보통신부장관이 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 인증받은 정보보호관리체계 범위 내에서 중대한 변화가 발생하였을 경우, 신청인의 신청에 의해 인증기관이 실시하는 심사를 말한다.



〔그림 1〕 인증절차의 기본 흐름

2.4. 인증서 발급 현황

2002년 5월 첫 인증서를 발급한 이후 2007년 8월 현재까지 33개 업체 총 44건의 인증서를 발급하였다. 2004년까지 통신, 금융, 정보보호컨설팅 전문업체에 집중되던 인증분야가 2005년 이후 특히, 개인정보보호가 중요시 되고 있는 대형포탈, 금융, 의료, 교육분야 등의 인증분야로 확대하고 있다. 본 연구에서는 33개 업체의 인증심사 결과 발견된 결함사항에 대한 분석을 진행한다.

Ⅲ. 정보보호관리체계 인증 요구사항

정보보호관리체계 인증심사 기준은 정보통신부가 2002년 2월 고시(제2002-32호)하였고, 필수사항인 관리과정 14개 항목, 문서화 요구사항 3개항목과 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.

3.1. 정보보호관리과정 5단계

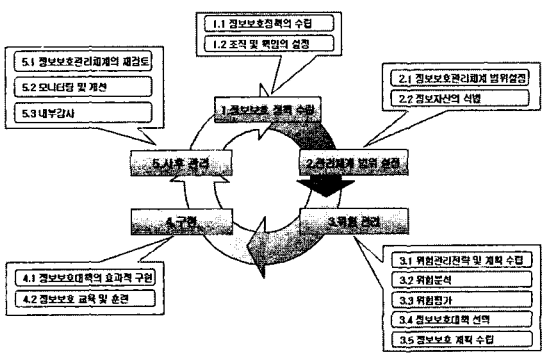
정보보호관리체계는 ①정보보호정책 수립 ②정보보

호관리체계 범위 설정 ③위험관리 ④구현 ⑤사후관리의 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.

3.2. 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.



〔그림 2〕 정보보호관리체계 5단계 관리과정

3.3. 정보보호대책

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

Ⅳ. 결함사항 분석

4.1. 분석 방법

인증제도가 시행된 2002년부터 2007년 8월 현재까

〔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

지 정보보호관리체계 인증을 취득한 33개 업체를 대상으로 최초인증심사, 1/2차 사후관리심사, 갱신심사에서 발견된 전체 결함사항을 조사하고 세부통제항목별 특징을 살펴보도록 한다. "결함"이라 함은 기업이 수립한 정보보호관리체계가 인증심사기준 137개 항목에 규정된 요구사항을 충족하지 못할 경우 지적된 사항을 말하고, 결함사항은 인증심사팀이 인증심사과정(문서/기술심사)을 통해 발견하게 된다. 먼저, 정보보호관리체계 인증심사별 결함 개선율을 비교해보고, 다음으로는, 137개 세부통제항목별(관리과정 14개, 문서화 3개, 정보보호대책 120개) 결함빈도수를 도출한 후 그 순위에 따라 결함사항의 특징을 살펴보도록 한다.

4.2. 결함내역 및 분석

4.2.1. 인증심사별 결함 수

최초인증심사, 1/2차 사후관리심사, 갱신심사별 결함수를 조사한 결과 〔표 2〕와 같았다. 최초인증심사 시 업체당 결함수는 평균 17.4건이 발견되었으나, 1차/2차 사후관리심사 시에는 발견된 업체당 결함수가 각각 평균 6건과 5.5건으로 현저히 줄어든 것을 볼 수 있다. 이는 인증을 취득한 업체가 지속적으로 정보보호관리체계를 관리 운영함으로 인해 업체의 자체 정보보호수준이 향상되었음을 간접적으로 보여주는 것이라 할 수 있다.

다만, 갱신심사의 경우 업체당 결함수가 다소 증가한 원인은 업체의 갱신심사 시 인증범위 확대로 인한 신규 결함수가 증가요인으로 포함되었기 때문이다.

〔표 2〕 정보보호관리체계 인증심사별 결함 수

심사구분	업체수	총 결함수	업체당 결함수
최초인증	33개	574건	17.4건
1차 사후관리	25개	150건	6건
2차 사후관리	15개	83건	5.5건
갱신	6개	52건	8.7건

4.2.2. 결함 개선율 비교

다음은 정보보호관리체계 수립 후 개선효과를 객관적으로 분석하기 위해 인증유효기간 3년에 걸쳐 최초인증심사, 1/2차 사후관리심사를 모두 수행한 15개 업체들의 결함수를 비교해보고 결함 개선율을 살펴보기로 한다.

〔표 3〕 정보보호관리체계 결함 개선율 비교

구 분	최 초	1차 사후관리	2차 사후관리
전체 결함수	243건	94건	83건
업체당 결함수	16.2건	6.3건	5.5건

〔표 3〕에서처럼 사후관리심사에서는 최초인증심사 시보다 매년 결함수가 줄어들고 있음을 발견할 수 있다. 즉, 1차 사후관리심사에서는 최초인증심사 결함수 243건보다 61%가 감소한 94건이 발견되었으며, 2차 사후관리심사에서는 1차 사후관리심사 결함수 94건보다 12%가 감소한 83건의 결함이 발견되었다. 이는, 기업들이 초반 정보보호관리체계 수립 운영에 관한 사전 경험 부족으로 인한 시행착오가 결함이 많이 발견되는 원인으로 보인다. 하지만, 향후 지적된 결함을 적절히 보완하고 지속적으로 관리함으로써, 사후관리심사에서는 결함수가 현저히 줄어들고 있음을 볼 수 있다. 이러한 결함율 개선요인으로는 다음과 같은 사항들을 대표적으로 들 수 있다.

① 주기적인 위험관리, 내부감사, 보안점검 시행
② 정보보호조직 구성으로 인한 체계적인 정보보호 활동
③ 경영층의 적극적인 관심과 실무진의 지속적인 노력
④ 직원들의 정보보호인식 수준 향상
⑤ 체계적인 정보보호 교육 및 훈련

4.2.3. 세부통제항목 별 결함 수

최초인증심사 33회, 1/2차 사후관리심사 40회, 갱신심사 6회, 총 79회 걸친 인증심사에서 발견된 결함을 분석한 결과 Top 12에 해당하는 세부통제사항은 아래 〔표 4〕와 같다. 결함발생빈도는 아래와 같이 계산하고 이는 인증심사 시 137개 세부통제항목별로 얼마나 자주 결함사항이 발견되었는지를 나타낸다. 본 절에서는 조사된 결함발생빈도수 순위에 따라 12개 통제사항을 선택하여 그 특징을 살펴보고 그동안 심사과정에 주로 발견되는 결함을 보여주고자 한다.

결함발생빈도 = 발견된 총결함수 / 79회(인증심사회수)

〔표 4〕 세부통제항목 별 결함수 비교

순위	세부통제사항	통제내용	결함건수	발생빈도
1	백업 및 복구관리	데이터 및 장비의 무결성과 가용성을 유지하기 위해 백업 계획을 수립하여 이행하고 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.	34	43%
2	정보자산의 보안등급과 취급	중요도에 따라 분류된 정보자산에 보안등급을 부여하고, 물리적, 전자적 보안등급 표시를 부착, 관리하여야 한다. 또한 보안등급의 부여에 따른 취급절차도 정의하여 이행하여야 한다.	23	29%
3	시스템 사용자 등록	정보시스템 및 서비스에 대한 접근을 통제하기 위한 공식적인 사용자 등록 및 해지 절차를 마련하여야 한다.	19	24%
4	정보자산의 분류	정보자산이 신청기관에서 차지하는 가치와 신청기관에 미치는 영향을 고려하여 분류방식을 선택하고 분류하여야 한다.	18	23%
5	정보자산의 변경관리	정보시스템 관련 자산들을 조사하고, 모든 변경사항들을 반영할 수 있는 공식적인 관리책임 및 절차를 수립하여야 한다.	18	23%
6	보안사고 대응계획 수립	보안사고의 정의 및 범위, 긴급연락체계 구축, 보안사고 발생 시 보고 및 대응 절차, 사고 복구조직의 구성, 교육계획 등을 포함한 보안사고 대응 계획을 수립, 이행하여야 한다.	18	23%
7	정보보호 교육 시행 및 평가	교육 및 훈련은 정기적으로 실시하여야 하며, 정보보호정책이나 절차 및 역할의 변경이 있는 경우에는 수시로 실시하고 이에 대한 기록을 남겨야 한다. 또한 교육훈련 종료 후 검토를 통하여 차기 교육에 반영하여야 한다.	17	22%
8	물리적 보호구역	물리적 보호구역에 대한 출입은 적절한 출입통제절차에 의하여 통제되어야, 출입자를 식별하고 기록·관리하여야 한다.	16	20%
9	업무연속성 계획 시험	환경의 변화 또는 부정확한 전제 등으로 인한 오류를 제거할 수 있도록 지속적인 시험을 수행하며, 시험 계획에는 시기, 방법, 절차 등을 포함하여야 한다.	16	20%
10	위험분석	식별된 정보자산에 영향을 줄 수 있는 모든 위협, 취약성, 위험을 식별하여 분류하여야 하며, 이 정보자산의 가치와 위험을 고려하여, 잠재적 손실에 대한 영향을 식별·분석하여야 한다.	15	19%
11	내부감사	기업은 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되는 지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 계획된 주기로 내부감사를 수행하여야 한다.	15	19%
12	비밀유지 서약서	직원으로부터 비밀유지 서약서에 서명을 받아야 하며, 임시직원이나 제3자에게 정보에 대한 접근 권한을 부여할 경우에도 그들로부터 비밀유지 서약서에 서명을 받아야 한다.	15	19%

① 백업 및 복구 관리

백업 및 복구는 예상치 않았던 재해 및 장애 등의 문제로 시스템이 손상되었을 경우 업무 연속성을 보장하기 위해 가장 기본적으로 구현해야 하는 정보보호대책 중 하나이다. 하지만 〔표 4〕에서 보는 것처럼 발생빈도가 43%로 인증심사 2회당 거의 1번꼴로 결함이 발견되고 있어, 기업들이 사전에 시스템 장애 및 재해를 대비하는데 소홀하다는 것을 알 수 있다. 백업 및 복구관리와 관련하여 주로 발견되는 결함을 살펴보면 다음과 같다.

- 백업대상, 백업방법, 백업주기 등을 명시한 백업관련 지침 및 구체적인 백업 계획 부재
- 백업관련 지침 및 계획 미준수 및 백업관리대장 관리 미흡
- 백업매체의 소산 미흡 및 소산장소 미지정

② 정보자산의 보안등급과 취급

기업의 주요정보자산을 안전하게 보호하기 위해서는 정보자산을 중요도에 따라 분류하여야 하며, 그 중요도에 따라 보안등급을 표시하고 취급절차를 마련하여야 한다. 기업들은 자산의 중요도 산정은 하고 있으나, 실제로 그 중요도에 따른 처리절차가 명확하지 않거나, 절차를 준수하지 않는 경우가 많다. 정보자산의 보안등급과 취급 관련하여 주로 발견되는 결함을 살펴보면 다음과 같다.

- 정보자산에 해당 보안등급의 물리적, 전자적 표시 미흡

- 문서자산의 경우 자산의 중요도 산정(1/2/3등급 등)과 문서자산 보안등급(기밀, 대외비, 사외비 등) 간의 일관성 결여
- 정보자산 보안등급에 따른 취급절차 미흡

③ 시스템 사용자 등록

주요 시스템의 가용성을 보장하거나 시스템에 저장되어 있는 고객정보 등 기업의 민감한 정보 유출을 방지하기 위해서는 사용자 계정의 접근 권한관리를 통한 통제가 필수적으로 필요하다. 특히, 정보의 유출이 내부자에 의해 발생되는 사례가 많으므로, 자칫 소홀하기 쉬운 내부자 접근에 대한 관리도 특히 주의를 기울여야 한다. 시스템 사용자 등록과 관련하여 주로 발견되는 결함을 살펴보면 다음과 같다.

- 주요시스템의 공동계정 사용
- 사용자 계정 등록 및 해지절차 미흡
- 신규 사용자 계정 발급에 대한 책임자의 승인 누락
- 사용자 권한 변경내역에 대한 주기적인 점검 미흡

④ 정보자산의 분류

정보보호관리체계 범위내의 주요 자산을 효율적이고 안전하게 관리하기 위해서는 자산을 모두 파악한 후 적절한 분류기준에 따라 분류하고 자산의 가치를 중요도에 따라 산정하여야 한다. 하지만, 정보자산의 분류기준이 정책, 지침에 구체적으로 명시가 되어 있지 않거나, 분류기준에 따라 정보자산을 분류하고 있지 않은 경우가 많다. 분류기준을 명확히 정의하고 이에 따라 정보자산을 식별하고 관리한다면 이 통제항목에 대한 결함은 현저히 줄일 수 있을 것이다. 예를들어, 정보자산은 데이터, 문서, 하드웨어, 소프트웨어, 설비, 인적자산으로 분류할 수 있다. 정보자산의 분류와 관련하여 주로 발견되는 결함을 살펴보면 다음과 같다.

- 정보자산의 분류 기준 부재
- 정보자산의 분류 기준에 부합하지 않는 정보자산 관리
- 전자정보(고객정보 DB 등)와 문서(기밀문서, 보고서 등)자산의 정보자산 분류 누락

⑤ 정보자산의 변경관리

'정보자산 식별'에 관한 요구사항에 따라 정보보호관리체계를 수립한 기업들은 보호받을 가치가 있는 정보자산을 식별하여 자산목록으로 관리하고 있다. 하지만, 새로운 소프트웨어, 하드웨어 설치 등으로 인한 정보자산의 변경 시 준수해야 하는 변경 관리절차가 부재하거나 있더라도 따르지 않는 경우가 결함으로 종종 발견되고 있다. 초기 정보자산의 식별뿐만 아니라, 정보보호관리체계의 운영과정에서 발생하는 자산의 변경에 대해서 그 내역을 철저히 관리하고 점검할 필요가 있다. 정보자산의 변경관리와 관련하여 주로 발견되는 결함을 살펴보면 다음과 같다.

- 정보자산 변경절차의 부재 및 절차준수 미흡
- 변경에 대한 정식적인 승인절차 미준수
- 신규 네트워크 장비 설치, 소프트웨어 설치 등 변경에 대한 사전 영향분석 미흡
- 정보자산 변경내용, 변경이유, 변경날짜 등 변경에 대한 기록 미흡

⑥ 보안사고 대응계획 수립

보안사고는 해킹, 바이러스, 웜, 사람 등의 다양한 위협요소로 인해 언제든지 발생할 수 있다. 2003년 1.25 인터넷 대란 당시 사실 많은 기업들이 보안사고에 대한 체계적인 대응절차를 수립하지 못했던 것이 사실이다. 하지만, 기업들이 1.25대란의 징후를 인지한 후 미리 마련된 보안사고 대응절차에 따라 신속하게 대응을 했었다면 피해를 많이 줄일 수 있었을 것이다. 이처럼, 국가 전체에 영향을 미치는 대규모 보안사고 뿐만 아니라, 단순 바이러스 감염 등에도 기업의 업무가 마비될 수 있으므로, 기업별로 업무특성에 적합한 보안사고 대응절차를 마련할 필요가 있다. 결국, 주기적인 보안점검을 통해 사전에 보안사고를 예방하는 것도 중요하지만, 보안사고 발생한 후 그 피해를 최소화하는 것도 그에 못지않게 중요한 일이다. 보안사고 대응계획 수립과 관련하여 주로 발견되는 결함을 살펴보면 다음과 같다.

- 보안사고 발생 시 긴급연락체계 작성 미흡
- 보안사고의 범위 및 정의 미흡
- 보안사고의 중요도에 따른 보고라인 및 처리방법 부재

⑦ 정보보호 교육 시행 및 평가

직원들에게 신규 취약점, 위협 등 최근 정보보호 관련 이슈를 공유하고 기업의 정보보호 정책, 지침, 절차를 숙지시키기 위해 기업들이 선택하는 가장 효과적인 방법이 바로 교육 및 훈련의 시행이다. 이를 통해 기업은 직원의 정보보호 인식수준을 기업이 원하는 적정수

준 만큼 높일 수 있다. 정보보호관리체계 인증 취득 업체 중 전반적으로는 연간 정보보호교육 계획을 수립하여 체계적으로 정보보호교육을 실시하고 있으나, 교육 실시 후 교육 내용에 대한 평가 및 분석을 하고 차기 계획에 결과를 반영하는 경우는 드물다. 정보보호 교육 시행 및 평가와 관련하여 주로 발견되는 결함을 살펴보면 다음과 같다.

- 연간 정보보호교육 계획서 미작성
- 교육 후 참석자 서명, 강사 평가 등 기록관리 미흡
- 교육 및 훈련 내용에 대한 효과 측정 및 분석 절차 누락

⑧ 물리적 보호구역

특별한 보호가 필요한 시설 및 장비를 비인가자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 보호하기 위하여 제한구역, 통제구역, 사무실 구역 등 보호구역을 정의하고 이에 따른 보안대책을 수립하여야 한다. 하지만, 물리적 보호구역에 대한 정의가 명확하게 되어 있지 않거나 보호구역에 따른 정보보호대책이 수립되어 있지 않은 사례가 발견된다. 물리적 보호구역과 관련하여 주로 발견되는 결함을 살펴보면 다음과 같다.

- 물리적 보호구역의 구분 및 정의 누락
- 물리적 보호구역 경고 표시 미부착
- 물리적 보호구역 내 장비, 문서, 매체 반출입 절차 부재

⑨ 업무연속성 계획 시험

기업은 업무 환경의 변화 또는 부정확한 전제 등으로 인해 발생되는 오류를 제거하고 수립된 업무연속성 계획에 대한 실행계획 차원에서의 구체적인 현실성을 점검하기 위해 업무연속성 계획 시험을 실시하여야 한다. 지속적인 시험을 통해서만이 업무연속성계획의 효과성을 확인할 수 있으며, 시험결과는 다시 업무연속성계획의 재정립에 필요하다. 하지만 기업의 업무연속성 계획 시험을 위해 시기, 방법, 절차 등이 포함된 구체적인 시험계획 등이 미흡하거나 시험 시행에 대한 관리가 이루어지지 않은 경우가 많다. 업무연속성 계획 시험과 관련하여 주로 발견되는 결함을 살펴보면 다음과 같다.

- 시험계획에 필요한 시기, 방법, 절차 등이 구체화되지 않음
- 시험실시 후 결과에 대한 반영 미흡
- 시험계획에 따라 주기적으로 시험을 시행하지 않음

⑩ 위험분석

기업은 식별된 정보자산에 영향을 줄 수 있는 모든 위협, 취약성, 위험을 모두 식별하고 분류하여야 하며, 이 정보자산의 가치와 위험을 고려하여, 잠재적 손실에 대한 영향을 식별·분석하여야 한다. 하지만, 위험분석 범위에 중요자산이 누락되어 있거나 식별된 자산의 모든 위협요인이 고려되지 않고, 취약성 정도를 분석하기 위한 평가 방법에 문제가 있는 경우가 많음

- 위험분석 범위 내에 고객정보 등 중요자산 누락
- 위험분석 및 평가 방법론이 정의되지 않음
- 지침에 명시되어 있는 자산가치 산정기준, 취약성 및 위협 평가기준을 따르지 않음
- 목표위험수준(DoA)의 최고책임자 승인 누락

⑪ 내부감사

기업은 수립된 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되고 관리되고 있는 지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 규정에 따라 별도의 감사조직에 의해 내부감사를 수행하여야 한다. 하지만 조직에서 규정하고 있는 내부 감사 기준이 정보보호관리체계의 관리실태를 파악하기에 미흡한 사례가 많으며, 또한 규정된 기준에 의거 내부감사를 진행하고 있지 않은 경우가 많다. 주로 발견되는 결함은 다음과 같다.

- 구체적인 내부감사 규정 마련을 하고 있지 않음.
- 조직에서 규정하고 있는 감사기준에 따른 주기적 감사 미흡
- 독립된 감사조직에 의한 감사가 이루어지지 않음

⑫ 비밀유지서약서

기업의 중요 정보를 이용하고 있는 직원이나 임시직원, 제3자 등 정보에 대한 접근권한이 있는 자에 대해 정보 유출방지 등에 대한 비밀유지 서약서를 징구해야 한다. 하지만 정직원이 아닌 임시직 또는 제3자에 대한 비밀유지 서약서의 징구관리가 이루어지지 않은 조직이 많음

- 정규직원이외에 조직의 정보 접근권한을 갖고 있는 비정규직원, 제3자에게 비밀유지서약서 미 징구
- 신입직원에 대한 비밀유지서약서 미 징구
- 비밀유지서약서 관리 미흡

V. 결 론

2002년부터 2007년 8월 현재까지 인증을 취득한 33개 업체를 대상으로 인증심사 시 발견된 결함을 분석하고, 137개 통제사항 중 결함이 많이 발견된 순서대로 12개 세부통제항목을 선정하여 그 특징과 결함사례를 살펴보았다. 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. 향후, 국내 기업에 대한 정보보호관리체계 수립 활성화를 위하여 정보보호관리체계 수립에 대한 모범사례를 지속적으로 발굴하여 제시할 필요가 있다.

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.

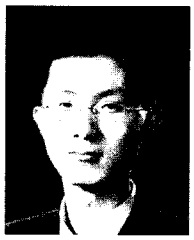
[4] 정보통신부, "정보보호관리체계 인증심사 기준", 정보통신부 고시 제2002-22호, 2002.

[5] 한국정보보호진흥원, "정보보호관리체계 인증업무지침", 2003

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

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

〈著者紹介〉



고 규 만 (Ko KyuMan)
1999년 2월 : 충북대학교 컴퓨터공학과 졸업
2002년 2월 : 연세대학교 컴퓨터과학과 석사
2002년 1월~현재 : 한국정보보호진흥원 IT기반보호단 기반보호팀
관심분야 : 정보보호관리, 내부감사, u-IT 서비스 정보보호

김 재 성 (Jason Kim)
2000년 2월 : 동국대학교 컴퓨터공학과 졸업
2002년 7월~현재 : 한국정보보호진흥원 IT기반보호단 기반보호팀
관심분야 : 정보보호관리, 정보보호 컨설팅

장 상 수 (Jang SangSu)
1989년 2월 : 한국항공대학교 항공정보통신공학과 졸업
2004년 2월 : 동국대학교 정보보호학과 석사
2006년 2월 : 전남대학교 정보보호학과 박사수료
2000년 1월~현재 : 한국정보보호진흥원 IT기반보호단 기반보호팀 팀장
관심분야 : 정보보호관리, 정보보호 안전진단, 네트워크 보안