정보보호관리체계를 활용한 기업 내부 시스템 보안성 향상방안에 관한 연구

신예나*, 최진영**
*고려대학교 컴퓨터정보통신대학원 디지털정보·미디어공학과
**고려대학교 컴퓨터정보통신공학과
e-mail : syena@korea.ac.kr, choi@formal.korea.ac.kr

A Study on the Security Improvement of Enterprise Internal System Using Information Security Management System

Yena Shin* and Jinyoung Choi**
*Dept of Digital Information & Media Engineering,
Graduate School of Computer & Information Technology, Korea University
**Dept of Computer & Communication Engineering, Korea University

요 약

기업의 정보자산에 대한 위협이 날로 증대하고 있다. 따라서 기업의 중요한 정보를 보호 및 관리하는 정보보호관리체계 (Information Security Management System; ISMS)에 대한 필요성과 중요성이 더욱 증가하고 있다. 정보보호관리체계란 조직의 주요 정보자산을 보호하기 위해 정보보호관리 절차와 과정을 체계적으로 수립하여 지속적으로 관리·운영하기 위한 종합적인 체계를 의미한다. 본 논문에서는 국내 기업의 정보보호관리체계에 대한 문제점 및 필요성 등을 분석하여 기업 내부 시스템의 보안성 향상을 위한 효율적인 정보보호관리체계 수립방안을 제안한다.

1. 서 론

최근 들어, 공공 및 민간기업의 정보기술에 대한 의존도가 높아지고, 정보화의 역기능들이 위험 요소로 등장하면서 정보보호에 대한 인식이 증가하고 있다. 미국, 영국, 독일 등 선진국들은 1980년대부터 제품과 서비스뿐만 아니라 정보보호관리시스템 자체에 대한 체계적인 절차를 수립하여 시행하고 있다. 이러한 추세에 발맞추어 국내에서도 기업 내부의 보안 정책과 관리 측면의 중요성이 부각되어 정보보호관리체계 (Information Security Management System; ISMS)의 필요성과 중요성이 대두되고 있다. 국내에서는 2002년 5월, 한국정보보호진흥원이 주축이 되어 국제표준 및 국내의 실정을 고려한 ISMS의 통제항목 및 인증절차를 제정하여 업체의 ISMS를 평가할 수 있도록 하였으며, 관련 법·제도 및 지침을 개정, 고시하는 등 ISMS의 국내 활성화를 위한 다양한 노력이 진행되고 있다[1]. 본 논문에서는 국내 기업의 정보보호관리체계에 대한 문제점 및 필요성 등을 분석하여 기업 내부 시스템의 보안성 향상을 위한 효율적인 정보보호관리체계 수립방안을 제안한다.

2. 정보보호관리체계 개요

ISMS는 조직의 전반적인 관리시스템의 일부로서 비즈니스 위험에 기반하여 정보보호를 계획, 구현, 운영, 검토 및 개선시키기 위해 조직체계 및 정책, 정보보호 프로세스 및 절차, 정보보호통제 등으로 구성된 종합적인 관리체계이다.

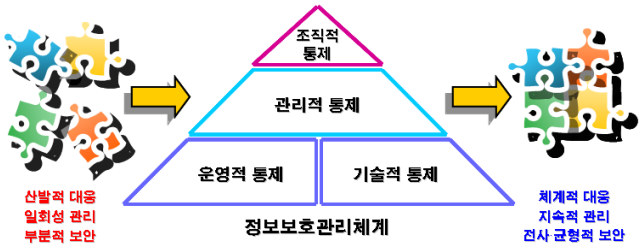

그림 1. 정보보호관리체계의 개념

2.1 국·내외 정보보호관리체계 연구동향

ISMS의 요구사항을 포함하는 ISO 27001 (BS 7799 part 2 : 2002 수정판)과 ISMS의 기초적인 통제수단을 수록한 ISO 27002 (ISO 17799 : 2005)가 국제표준화에 성공하여 최근 전 세계적으로 ISMS에 대한 인증 노력이 빠르게 확산되고 있다[2]. 한국정보보호진흥원에서는 BS 7799의 내용을 기본으로 하여 정보 기술적 측면보다는 조직이나 환경적 측면에서의 관리적 방식을 강조하면서 다양한 환경에 종합적으로 적용할 수 있도록 정보보호관리체계를 개발하였다[1].

2.2 국내 기업의 정보보호 문제점 및 필요성

정보통신망의 발전과 함께, 사회 전반의 정보화가 진행되면서 정부, 공공기관 및 기업 등 국가 사회 각 분야의 업무들이 오프라인 환경에서 온라인 환경으로 전환되었지만 보안 대책 미비로 인한 해킹이나 바이러스 등에 의한

보안 위협도 증가하였다. 국내 D사의 경우 대·내외적으로 표 1과 같은 문제점으로 인해 ISMS 인증획득을 필요로 하고 있다.

<표 1> 국내 D사의 정보보호 문제점 및 필요성

정보시스템의 중요성 증가	▪ 정보시스템에 대한 비즈니스 의존도 증가 ▪ 시간과 공간 제약이 없는 실시간 업무처리 필요 ▪ 정보시스템 손상시 비즈니스 프로세스 마비
대외 신뢰도 저하	▪ 내부직원에 의한 고객정보유출 및 보안사고 증가 ▪ 외부자에 의한 전자적 침해 행위의 증가
대규모 인프라 사용	▪ 프로세스 구축 미비 ▪ 정보보호에 대한 인식 미비

3. 정보보호관리체계 수립방안

앞장에서 언급한 정보보호에 따른 문제점을 해결하고 국내 D사와 같이 일정한 규모를 가진 기업이나 조직이 경쟁력 있게 살아남기 위해서는 여러 가지 안전장치가 마련되어야 한다. 특히 기업들은 새롭게 증가하는 정보보호 위협을 대비하기 위하여 내부적으로 통제를 강화하고 다양한 정책, 지침, 절차를 만들어 갈 필요가 있으며, 이러한 일련의 정보보호 활동의 체계적인 관리를 위해서는 그림 2와 같은 단계를 거쳐 ISMS를 수립하는 것은 필수적이다.

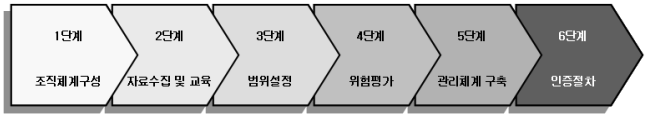

그림 2. 정보보호관리체계의 수립단계

ISMS 수립에 필요한 조직체계를 구성하고 관련 자료수집 및 구성된 조직에 대하여 충분한 교육을 실시한다. 단계수립을 위한 범위를 설정한 후 정보자산에 대한 위험평가를 실시하여 문제점을 도출한다. 다음으로 이에 대한 대응책들을 체계적으로 구성하고 관련 보안 프로세스들을 수립하여 정보보호관리체계를 수립한 후 인증을 획득한다. 본 논문에서는 ISMS 수립 후 기업에서 ISMS 인증 시 취약점으로 지적되는 사항을 보완하기 위해 다음과 같은 사항을 제안한다.

- 데이터·장비의 가용성 유지를 위한 백업 계획 수립
- 정보자산에 보안등급을 부여하고 물리적·전자적 표시
- 정보시스템·서비스 접근 통제를 위한 사용자 정책 마련
- 정보시스템의 변경사항을 반영할 수 있는 관리 절차 수립
- 보안사고의 정의 및 범위, 대용 절차 등에 관한 계획 수립
- 정책·역할의 변경이 있을 경우 수시로 교육 실시
- 적절한 절차로 보호구역을 통제하고 출입자 기록
- 정보자산에 영향을 줄 수 있는 위협, 취약성 분류
- 감사의 기준, 방법을 규정하고 계획된 주기로 수행
- 직원에게 비밀유지 서약서를 받고 임시직도 동일

이와 같이, ISMS 수립에 따른 기업 내부 보안성 향상을 통하여 표 1에 나타낸 문제점을 해결함으로써 다음과 같은 효과를 기대할 수 있다.

<표 2> ISMS 수립에 따른 효과

대고객 및 감독기관 신뢰도 향상	▪ 안정적인 E-Biz 사업의 전개 ▪ KISA-ISMS 인증 획득을 통한 회사 이미지 향상 ▪ 대외 비즈니스 경쟁력 강화
안정적인 정보시스템의 운영	▪ 정보시스템의 취약점 제거 및 보완 프로세스 확립 ▪ 정보시스템의 가용성, 무결성 확보

표 3은 ISMS 인증을 통하여 국내 D사 뿐만 아니라 여러 분야의 기업들이 얻을 수 있는 인증 효과를 나타낸 것이다.

<표 3> ISMS 인증사례로 바라본 인증효과

업 체	인증 효과
N사 (은행)	▪ ISMS 인증을 계기로 정보보호조직 구성의 발판 마련
K사 (IDC)	▪ 모든 임직원의 정보보호 마인드의 확연한 변화 및 정보보호 활동을 자체적으로 수행할 수 있는 자생력 확보 ▪ 고객의 신뢰성 제고 및 기업 이미지 제고
K사 (통신)	▪ 정보자산에 대한 체계적인 보안관리로 보안사고 최소화 ▪ 정보보호수준 향상 및 정보보호관리 절차를 정착시킬 수 있는 환경 조성
정보보호컨설팅 전문업체	▪ 자사 ISMS 컨설팅에 대한 고객 신뢰감 향상
H그룹 (항공, 운송)	▪ ISMS 수립 시작부터 마무리까지 TFT 구성을 통한 자체 수립 ▪ 기업 이미지 제고를 통한 매출 증대

4. 결 론

본 논문에서는 기업 내부 시스템의 보안성 향상을 위한 정보보호관리체계 수립방안을 제안하였다. 이를 바탕으로 기업의 보안성 향상을 통하여 대외적인 신뢰도를 향상시키고, 총체적인 관리와 체계적인 관리를 할 수 있을 것으로 사료된다.

참고문헌

[1] http://isms.kisa.or.kr/isms.html

[2] A. Plate and O. Weissman, "ISO/IEC FCD 17799," *ISO/IEC JTC 1/SC27 NC394*, Jun. 2004.