기업규모와 특성에 따른 정보보호 관리체계(ISMS) 적용 방안 연구

서동호*, 신현민**
*고려대학교 컴퓨터정보통신대학원 컴퓨터정보통신공학과
**위즈시큐리티 주식회사
e-mail:bbanana86@korea.ac.kr

A Study on the application of Information Security Management System(ISMS) according to size and characteristics of company

Dong-Ho Seo*, Hyun-Min Shin**
*Department of Computer and Information Technology, Korea University Graduate School Computer and Information Technology
**WhizSecurity Corporated

요 약

ICT산업의 발전과 전자상거래의 대중화에 따라 정보시스템에 대한 지능·고도화 된 사이버위협이 증가되고 있고, 개인 및 기업정보 유출의 피해규모가 커짐에 따라 정보보호의 중요성이 한층 더 부각되고 있다. 이미 세계 각국에서는 ISO27001, BS10012 등 정보보호 관리 제도를 구축하여 운영하고 있다. 이에 국내에서도 미래창조과학부 주관 정보보호 관리체계(ISMS:Information Security Management System) 인증제도를 비롯한 정보보호 제도를 구축하여 기업 정보자산의 안전과 신뢰성 향상 등의 목적으로 자율과 의무 대상을 구분하여 운영하고 있다. 하지만 기업의 규모와 환경, 매출 등에 따라 형평성 있게 구분하지 않은 현재의 정보보호 관리체계 인증제도에는 여러 모순이 존재한다. 통제항목을 비롯한 세부점검항목을 인증 기업을 대상으로 모두 공통으로 적용하기 때문이다. 본 논문에서는 정보보호 관리체계 인증제도와 유사 인증체계를 비교하여 인증기준 항목을 기업의 규모와 특성에 따라 유형별로 구분하여 적용하는 방안을 연구하였다.

1. 서론

ICT산업의 발전과 전자상거래의 대중화에 따라 온라인상에는 많은 개인정보 및 기업정보가 유통되면서 이 정보들을 대상으로 다양한 형태의 IT기술을 활용한 범죄가 급속도로 증가하고 있다. 정보보안의 위협은 시간이 지날수록 지능적이고 대규모로 조직화되면서 기업에 많은 피해를 입히고 있다. 아래 [표1]을 보면 정보보안 사고와 피해가 매년 끊이지 않고 지속적으로 발생하는 것을 볼 수 있다.[1]

[표1] 대한민국 정보보안 사고 현황

시기	기관	유형	피해규모
2016. 07	인터파크	개인정보유출	1,030만건
2015. 09	뽐뿌	개인정보유출	200만명
2014. 03	KT	개인정보유출	1,200만명
2014. 03	SKT, LG U+ 등	개인정보유출	1,230만명
2014. 03	국토교통부	개인정보유출	2,000만명
2014. 01	KB국민카드,롯데카드, NH농협은행	개인정보유출	2,000만명
2013. 06	새누리당,군장병,청와대,주한미군	개인정보유출	294만명
2013. 05	민족문제연구소	개인정보유출	912명
2013. 04	SC제일은행,씨티은행	개인정보유출	13만명
2013. 03	MBC, KBS, 농협등	전산망 마비	
2012. 07	KT	개인정보유출	870만명
2012. 06	코웨이	개인정보유출	198만명
2012. 05	EBS	개인정보유출	400만명
2012. 03	SK텔레콤,KT	개인정보유출	20만명
2011. 11	넥슨	개인정보유출	1,320만명
2011. 10	선거관리위원회	사이트 마비	
2011. 08	한국앱손	개인정보유출	35만명
2011. 07	SK컴즈	개인정보유출	3,500만명
2011. 05	네이버,다음,네이트	개인정보유출	3500만명
2011. 04	현대케피탈	개인정보유출	175만명
2011. 04	농협	전산망 마비	수백억원 추정
2011. 03	정부기관,포털,은행	사이트 마비	
2010. 03	신세계몰	개인정보유출	820만명
2009. 07	정부기관,포털,은행	사이트 마비	
2009. 04	네이버	명의도용	9만명
2008. 09	GS칼텍스	개인정보유출	1125만명
2008. 04	하나로텔레콤	개인정보유출	600만명
2008. 02	옥션	개인정보유출	1863만명
2005. 05	엔씨소프트	개인정보유출	50만명
2003. 01	KT	DNS서버공격	9시간마비

때문에 각종 정보보안 사고의 사전 예방을 위해 해당 기업규모에 적합하고 체계적인 정보보호 관리 체계 수립이 매우 중요하다.[1] 이에 정부는 각종 위협으로부터 주요 정보자산을 보호하고 궁극적으로 중요 정보들을 안전하게 지키기 위해 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조에 의거한 정보보호 관리체계(ISMS:Information Security Management System) 인증제도를 구축하여 운영하고 있다.[2] 하지만 기업의 정보보호 관리체계의 적합성을 판단하는 인증기준은 기업의 규모나 특성을 고려하지 않고 모든 통제항목과 세부점검항목을 공통으로 적용하기 때문에 중소기업이나 소상공인에게는 불합리한 모순이 존재한다. 본 논문의 2장에서는 정보보호 관리체계 인증제도를 유사 인증체계와 비교하여 인증대상의 유형별로(공공기관, 대기업, 중소기업, 소상공인) 분류하였고 각각의 인증기준을 차등 적용시켜 중소기업과 소상공인의 부담을 완화하기 위한 방안을 제시하였다. 끝으로 본 논문의 3장에서 결론 및 향후 연구로 끝을 맺는다.

2. 본론

2..1 정보보호 관리체계 인증제도의 정의

조직의 중요한 정보자산에 대해 안전성을 확보하고 신뢰성을 높이기 위한 절차적 단계를 체계적으로 문서화하여 지속적으로 정보자산의 관리·운영을 통하여 정보의 무결성, 기밀성, 가용성을 지키기 위해 일련의 과정을 지속적으로 정보보호 개선 활동을 하는 것을 정보보호 관리체계라고 한다. 인증제도의 관점에서 살펴보면, 기업이 운영하는 정보보호 관리체계가 일정한 인증심사 기준에 적합하는지의 여부를 제3자의 인증기관이 독립적이고 객관적으로 평가하여 보증해주는 제도를 정보보호 관리체계 인증제도라고 의미한다. 또한 정보보호 관리체계 인증제도는 각 기관이 정보보호를 위한 적합한 기술적·관리적·물리적 기준에 따라 정보보호 관리체계를 적용했는지 심사하여 인증기준에 맞게 운영되고 있는 경우 인증서를 부여하고 계속적으로 사후관리를 수행하는 제도이다.[3]

2..2 정보보호 관리체계 인증제도의 심사기준

정보보호 관리체계 인증제도는 2002년 미래창조과학부(구 정보통신부)에서 주관하고 한국인터넷진흥원(KISA)과 한국정보통신진흥협회(KAIT) 등 네 곳의 인증 기관을 통해 [표2]와 같이 104개의 통제항목과 253개의 세부점검 항목으로 심사를 하여 이를 보증한다.[4]

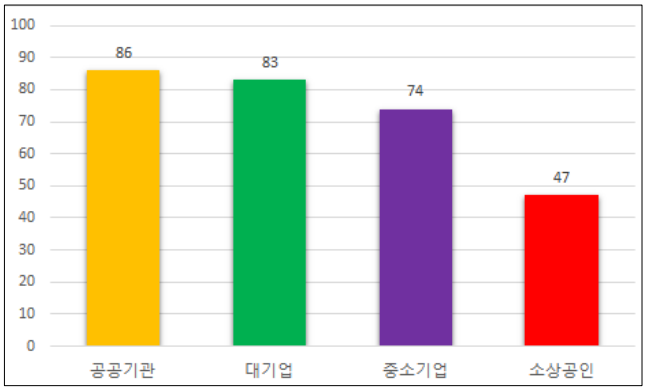
[표2] 정보보호 관리체계 인증기준 항목

분야		통제항목	세부점검항목
정보보호 관리과정	정보보호 정책 수립 및 범위 설정	2	4
	경영진 책임 및 조직 구성	2	4
	위험 관리	3	11
정보보호 대책	정보보호대책 구현	2	3
	사후관리	3	6
	정보보호 정책	6	13
	정보보호 조직	4	7
	외부자 보안	3	4
	정보자산 분류	3	7
	정보보호 교육	4	10
	인적보안	5	11
	물리적 보안	9	21
	시스템 개발 보안	10	22
	암호통제	2	8
	접근통제	14	46
	운영 보안	22	56
	침해사고 관리	7	14
	IT재해복구	3	6
총 계		**104**	**253**

세부 내용을 살펴보면 정보보호 관리과정의 경우, 정보보호정책 수립 및 범위설정, 경영진 책임 및 조직 구성, 위험관리, 정보보호대책 구현, 사후관리의 5단계 과정을 거쳐 수립, 운영. 관리 과정은 일회적인 단계가 아니라 지속적으로 유지 관리되어야 하며 정보보호대책은 정보보호에 관련된 위험을 통제하기 위한 요구사항으로 13개 통제분야, 92개 통제사항, 225개 세부점검 항목으로 구성된다.

2..3 유사 인증체계와의 비교 분석

정보보호 관리체계 인증과 유사한 제도로써 2011년 방송통신위원회 주관으로 시작된 개인정보보호 관리체계(PIMS:Personal Information Management System) 인증제도는 기업이 전사차원에서 개인정보보호 활동을 체계적·지속적으로 수행하기 위해 필요한 일련의 개인정보 보호조치 체계로써 기업이 개인정보보호를 위해 무엇을, 어떻게 조치하여야 하는지에 대한 기준을 제시하는 인증제도이다. 개인정보보호 관리체계는 2016년부터 개인정보보호 인증(PIPL)과 통합되었으며 기업의 혼란과 부담을 해소하기 위해 [그림1] 및 [표3]과 같이 기관 및 기업의 유형에 따라 인증기준을 차등 적용하였다.[5]



[그림1] 개인정보보호 관리체계의 유형별 인증기준

[표3] 적용 유형별 인증기준

구분	적용 유형별 인증기준			
	공공기관	대기업 및 정보통신 서비스제공자	중소기업	소상공인
개인정보보호 관리과정(16개)	16	16	15	4
생명주기 및 권리보장(20개)	20	19	19	19
개인정보 보호조치(50개)	50	48	40	24
총 계	86	83	74	47

개인정보보호 관리체계 인증심사 항목은 개인정보 사이클(생명주기 및 권리보장)이 포함된 것을 제외하면 [표4]와 같이 정보보호 관리체계(ISMS) 심사항목과 중복되는 것을 볼 수 있다.

[표4] ISMS와 PIMS의 비교

구분	정보보호 관리체계(ISMS)	개인정보보호 관리체계(PIMS)	유사 여부
관리 과정	정보보호 정책 수립 및 범위 설정	정책 수립 및 범위설정	○
	경영진 책임 및 조직 구성	경영진 책임 및 조직구성	○
	위험 관리	위협관리	○
	정보보호대책 구현	개인정보보호대책 구현	○
	사후관리	사후관리	○
보호 대책	정보보호 정책	개인정보보호 정책	○
	정보보호 조직	개인정보보호 조직	○
	외부자 보안	위탁업무 관리	○
	정보자산 분류	개인정보 자산분류	○
	정보보호 교육	개인정보보호 교육	○
	인적보안	인적 보안	○
	물리적 보안	물리적 보호조치	○
	시스템 개발 보안	개발 보안	○
	암호통제	암호화 통제	○
	접근통제	접근통제영역 관리	○
	운영 보안	운영보안	○
	침해사고 관리	침해사고 관리	○
	IT재해복구	관리적 보호조치	○
생명 주기	-	개인정보수집	X
	-	개인정보 이용 및 제공	X
	-	개인정보 관리 및 파기	X

이러한 비교 결과를 통해 살펴본 바와 같이 정보보호 관리체계도 개인정보보호 관리체계와 마찬가지로 유형별로 심사기준을 간소화하여 중소기업 및 소상공인의 부담을 완화시킬 수 있다. 더욱이 정보보호 관리체계 인증 의무 심사대상자(ISP, IDC, 정보통신사업자) 중 정보통신사업자로 분류되는 중소기업, 소상공인의 경우 재무재표, 회계장부상 100억원 이상 매출액, 사이트에 접속하는 고객의 Page View 증가 등의 이유로 인증 의무 대상자으로 지정되는 경우가 많다. 따라서 중소기업, 소상공인 기업의 유형별로 심사기준 간소화는 더욱 필요하다. 단, 인증심사의 기준이 간소화 되는 만큼 국제 인증제도인 ISO27001 심사주기와 같이 현행 1년에서 6개월로 단축하여 적용하는 방안을 세워 완화된 인증기준을 더욱 효과적으로 보완할 수 있다. 국내외 정보보호 관련 인증제도별 심사주기는 [표5]와 같다.

[표5] 각 인증별 심사주기

구분	PIMS	ISMS	ISO27001
심사주기	1년	1년	6개월

3. 결론 및 향후 연구

본 논문에서는 국내에서 최근 대두되고 있는 정보보호 관리체계(ISMS)를 유사 인증제도인 개인정보보호 관리체계(PIMS) 인증기준과 비교한 결과를 도출하여 인증기준을 기업 및 기관으로 구분하여 유형별로 적용하는 방안을 제안하였다. 정보보호 관리체계에서 모든 인증 대상에게 공통으로 요구하는 정보보안의 기준들은 중소기업이나 소상공인들이 운영 및 유지관리 하기에는 많은 비용과 인력, 시간이 투입되기에 많은 부담감이 존재할 수밖에 없기 때문이다. 또한 인증기준을 완화하는 대신에 ISO27001 인증제도처럼 심사주기를 6개월에서 1년사이로 단축 또는 유동성 있게 적용하여 완화된 부분을 보충하는 방안을 제시하였다. 아울러 기관 및 기업의 유형별 통제항목이나 세부점검항목을 차등적으로 적용하는 세부적인 방법이나 이를 보충하는 방법은 지속적인 연구 과제로써 연구되어야 할 것이다.

참고문헌

[1] Hyun-Sun Kang "An Analysis Information Security Management System and Certification Standard for Information Security" Journal of Security Engineering 2014.12

[2] http://isms.kisa.or.kr/kor/main.jsp

[3] 박종규 "The study on Improvement of Reinforcement of the Data Center Access Control using Information Security Management System(ISMS)" 건국대학교 2016.08

[4] 정보보호 관리체계(ISMS) 인증제도 안내서 http://isms.kisa.or.kr/kor/main.jsp 한국인터넷진흥원(KISA) 2016.03

[5] 김이준 "기업 정보보안 체계에 대한 연구 : ISMS와 PIMS의 비교 분석을 중심으로" 서울과학종합대학원 2013.02

[6] 개인정보보호 관리체계(PIMS) 인증제도 안내서 http://pims.kisa.or.kr/kor/main.jsp 한국인터넷진흥원(KISA) 2016.03