http://dx.doi.org/10.14400/JDC.2015.13.2.121

개인정보보호를 고려한 중소기업 정보화 수준 분석 설계

김병철
백석대학교 정보통신학부

The SME Informatization Level Analysis and Design for Privacy

Byung-chul Kim
Dept. of Information and Communication, Baekseok University

요 약 중소기업 정보화 수준 분석은 기업의 성과 분석과 경쟁력 강화를 위한 지표로써 의미가 크다. 그런데 최근에는 개인정보보호의 중요성이 부각되면서 보안 및 정보보호를 위한 인프라 및 마인드도 매우 중요한 지표로 인식되고 있다. 따라서 본 연구에서는 중소기업의 정보화 수준 분석에 있어서 개인정보보호 관련 활동을 어떻게 평가할 수 있는지의 여부에 중점을 두고 연구를 수행하였다.

주제어: 정보화 수준, 중소기업 정보화, 개인정보보호, 정보화 측정 지표

Abstract SME informatization level analysis is significant as an indicator for analyzing the performance and competitiveness of enterprises. However, as has recently been highlighted, the importance of privacy recognized as infrastructure, and mindset are very important indicators for security and privacy. Therefore, In this study, analysis of SMEs at the informatization level, with a focus on how we can assess whether the privacy-related activities were carried out.

Key Words : Informatization level, small business information, privacy, information measures

1. 서론

IT를 통한 기업의 정보화는 기업 경쟁력을 확보하는데 필수적 요소이다[1]. 그러나 중소기업의 경우 인력과 비용의 문제로 인하여 정보화에 대한 적극적인 투자를 하기가 쉽지 않은 현실이다. 이러한 정보시스템 투자와 인력문제는 한편 대기업과 중소기업의 정보화 수준 격차 발생의 근원적 원인이 되어 왔으며 중소기업 성과 향상에 병목 현상이 되어왔다[2].

또한 현대는 정보화 사회로서 정보의 중요성이 강조되고 IT 기술발전으로 필요한 정보를 쉽게 실시간으로 얻을 수 있다. 하지만 정보취득의 용이성은 개인정보침해라는 부작용의 측면도 존재한다[3]. 정보기술(Information Technology)의 발전으로 인해 개인의 삶의 방식, 기업활동, 공공부문에서 효율성과 편리성이 제고된 반면에, 이러한 발전 과정에 개인정보의 오·남용의 가능성이 증가하였다. 개인정보의 사용이 증가함에 따라 개인정보의 유출가능성이 증가하였고 해킹기술도 고도로 발전하여

* 이 논문은 2014년도 백석대학교 대학연구비에 의하여 수행된 것임
Received 19 December 2014, Revised 29 January 2015
Accepted 20 February 2015
Corresponding Author: Byung-chul Kim(Baekseok University)
Email: bckim@bu.ac.kr

ISSN: 1738-1916

대규모 개인정보 침해사건들이 자주 일어나고 있다[4].

개인정보보호는 이용자의 프라이버시 보호목적 뿐만 아니라 기업의 위험관리 차원에서도 중요하다. 기업이 개인정보를 부실하게 관리할 경우에 고객의 신뢰 성 저하로 인하여 기업이미지가 크게 타격받을 수 있다. 최근 들어 기업의 개인정보 유출 사건에 대해 개인정보 유출 피해자들이 대규모 소송을 제기하고 있고 일부 소송에서는 기업의 손해배상이 판결되는 점을 감안할 때 개인정보보호는 기업의 경영과도 직결된다고 볼 수 있다[5].

이에, 본 논문에서는 중소기업의 정보화 수준 분석에 있어서 개인정보보호 관련 활동을 어떻게 평가할 수 있는지에 대하여 개인정보보호법을 기준으로 하여 분석하였다.

2. 관련 연구

2.1 국내 중소기업 정보화 수준 조사

중소기업에 대한 정보화 수준 분석 방법은 여러 가지가 제시되어 있지만, 최근 우리나라에서는 중소기업기술정보진흥원에서 분석 방법을 개발하여 중소기업 정보화 수준 분석을 지속해 오고 있다.

2.1.1 중소기업기술정보진흥원 조사 배경

중소기업청 및 중소기업기술정보진흥원에서는 중소기업의 정보화를 앞당기기 위해 다양한 정책적 지원을 수행해 오고 있다.

중소기업이 정보화를 추진·구축하여 운영하기 위해서는 자사의 현재 정보화 추진현황을 영역별 분야별로 진단하고 발전단계 수준을 진단함으로써 미진한 부문에 대한 구체적인 개선방안을 도출할 수 있도록 하며, 한편으로는 그동안 정부에서 진행해온 여러 가지 정보화 정책에 대한 평가를 통한 개선 방향을 제시할 수 있도록 하는 것이 필요하다. 이를 통하여 중소기업에게는 정보화 투자의 타당성 및 추진전략을 제시함으로써 정보화 추진에 대한 의지를 고취시키며, 정부에게는 중소기업들이 원하는 현실적이고도 고객지향적인 지원방안을 위한 기초자료를 제공한다.

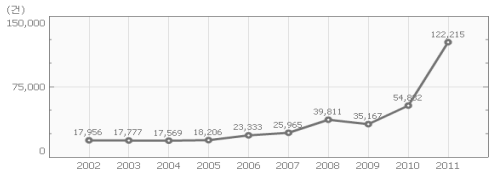
이에 중소기업 정보화수준 조사는 국내 중소기업의 정보화수준을 보다 체계적으로 과학적인 기법을 이용하여 조사·분석하고 있으며, 특히, 2012년도에는 변화하는 정보화 환경을 적절히 반영하기 위하여 새롭게 개편된 정보화수준 체계에 맞춘 신지수를 산출하였고, 새로운 지표를 제시하였다[6].

2.2 개인정보보호 관리과정 및 필요성

개인정보보호를 위해서는 다음의 관리과정을 고려하는 것이 필요하다. 개인정보보호 관리과정은 크게 4단계로 구성할 수 있다. 첫째, 개인정보보호의 목표와 기본적으로 수행해야 할 사항들을 포함하는 개인정보보호 정책을 수립하는 것이다. 둘째, 보호해야 할 개인정보와 관련된 업무와 자산을 식별하고 개인정보영향평가 및 위험분석을 통해 개인정보의 수집, 이용, 보관, 파기 등 전주기에 대한 유출가능성을 파악하고 대안들을 선택하는 위험관리활동이 있다. 다음으로, 선택된 개인정보 보호대책을 집행하고 개인정보 관련 교육을 통해 인식변화와 문제해결을 위해 노력하는 활동이 있다. 마지막으로 개인정보보호과정에서 성과측정을 통해 문제점을 해결하고 개선점을 파악 및 보완 하는 활동이 있다[7].

개인정보를 수집하고 이용하는 활동이 사회 전 영역에서 다양한 형태로 증가하고 있기 때문에 개인정보의 유출로 인한 금전적·비금전적 피해는 심각한 수준이라고 할 수 있다. 궁극적으로 개인정보의 오·남용과 유출에 의한 피해를 사전에 예방하고 침해된 경우에 사후적으로 구제하는 것은 인간의 존엄성의 실현을 위해 필요하다고 하겠다. 우리나라에서는 식별된 또는 식별가능한 개인에 관한 정보인 개인정보의 침해가 2010년 5만 4천 건에서 2011년도 12만 2천 건으로 급격하게 증가하는 것을 볼 수 있다[Fig. 1]. 개인정보보호의 필요성이 증대되면서 세계 각국은 개인정보 보호를 위한 기본법을 제정하고, 이에 따른 개인정보보호 전담조직을 설치하였다[8].

우리나라의 경우도 2012년 3월 30일부터 개인정보보호법을 시행해 오고 있다.



[Fig. 1] The number of privacy

〈Table 1〉 SME Informatization area and detailed factors

Domain	Details factor	History
Information strategy	Information Mind of the CEO / staff	CEO / Employee Information willingness care and support
	Vision Information	Establish ICT plans
	ICT Investment Feasibility Analysis	ICT investment feasibility study conducted
Promoting environmental information	Informatization Promotion staff	ICT plays workforce
	ICT investment	ICT investment to sales ratio
	IT training	ICT training or not, subject and scope
Construction and Application Information	Business Management Systems Maintenance	Standardized and documented level of business procedures
	Information Systems business area	Information Systems Development and Application Range
	New information technology adoption aggressiveness	Willingness to adopt new information technologies to improve information systems

3. 개인정보보호 관련 평가 항목

3.1 중소기업 정보화 영역

관련 연구인 '중소기업 정보화 요인별 중요성, 현황 및 정책적 시사점[2]'에서는 일반적인 중소기업 경영성과 향상을 위한 정보화 핵심 요인으로 <Table 1>과 같이 정보화 전략, 정보화 환경, 그리고 정보화 구축과 활용 등 총 3개의 영역과 각 영역에서의 세부 항목으로 구분하였다. 이들 3개의 영역과 세부 항목은 중소기업 IT 거버넌스의 한계점인 이사회의 부재, 한정된 관리 구조, 소규모 혹은 존재하지 않는 IT 부서, 자원의 부족, 정보화에 대한 단순한 프레임웍 등과 연계된다[9]. 정보화 전략의 중요성은 비즈니스 전략과 IT의 연계와 실행을 강조하는 IT의 전략적 연계 모델(Strategic Alignment Model)[10]과 맥락을 같이 하며 중소기업의 IT관련 기획, 수행, 성과의 구조적 연계의 취약점을 메울 수 있는 IT 인력과 사용자 교육 등 CEO의 IT 역량 등 추진환경 영역에 영향을 받는다[11].

기존 정보화 수준 분석 항목에 개인정보보호 관련 내용이 없거나 충분하지 않은 경우가 많다. 또한 기업의 유형에 따라 개인정보보호 관련 활동에 대한 비중이 매우 다를 수 있으나 이를 고려한 연구는 충분하지 않다.

3.2 개인정보보호 평가 항목 도출

3.2.1 우리나라 개인정보보호정책의 현황

우리나라의 개인정보보호정책은 기본법이라고 할 수 있는 개인정보보호법이 2011년 3월 제정에 따라 이를 전후로 하여 정책을 구분할 수 있다. 우리나라는 해외주요국의 정책으로 구분한 것처럼 개인정보보호법 제정 이전에는 미국과 일본과 비슷하였으나, 개인정보보호법 제정 이후로는 유럽 국가들과 정책적으로 유사하게 되었다고 할 수 있다[4].

3.2.2 개인정보보호법을 통한 평가항목 도출

개인정보보호법은 2011년 3월 29일 제정되어 2012년 3월 30일에 시행되었다. 개인정보보호법의 구성체계는 총 본문 9장에 75개의 조문과 부칙 7개 조문으로 구성되어 있다. 제 1장은 '총칙'으로 목적, 정의, 개인정보보호 원칙, 정보주체의 권리, 국가 등의 책무, 다른 법률과의 관계로 구성되었고, 제2장은 '개인정보 보호정책의 수립 등'으로 개인정보 보호위원회, 보호위원회의 기능 등, 기본계획, 시행계획, 자료제출 요구 등, 개인정보 보호지침, 자율규제의 촉진 및 지원, 국제협력으로 구성되었다. 제3장은 '개인정보의 처리'로 제1절 개인정보의 수집, 이용, 제공 등과 제2절 개인정보의 처리 제한으로 구성되었고, 제4장은 '개인정보의 안전한 관리',제5장은 '정보주체의 권리 보장'으로 구성되었다. 제6장 개인정보 분쟁조정위원회, 제7장 개인정보 단체소송, 제8장 보칙, 제9장 벌칙으로 구성되었다. 이 논문에서는 개인정보처리자가 준수하여야하는 의무조항과 해서는 안되는 금지조항을 분류하였다<Table 2>.

개인정보처리자가 준수하여야 하는 의무사항과 해서는 안되는 금지사항에 관하여는 제 3장, 4장, 5장에 나타나며, 의무사항은 50개, 금지사항은 7개가 있다. 즉, 기업

〈Table 2〉 Classification obligations and prohibitions

Domain	Article	Obligations Clauses	Prohibitions Clauses
Processing of Personal Information - Collection of personal information, use, offer, etc.	Article 15 (Collection of Personal Information and use)	②	
	Article 16 (Limitation of collecting personal information)	①	②
	Article 17 (Provision of Personal Information)	②	③
	Article 18 (Use of Personal Information and providing limited)	③,④,⑤	①
	Article 19 (use of personal information provided to parties, provide limited)		Article 19
	Article 20 (collecting sources, including the highlands of personal information collected from other data subject)	20조	
	Article 21 (Disposal of personal information)	①,②,③	
	Article 22 (obtaining consent)	①,②,③,④,⑤	
Processing of personal information-processing limits of privacy	Article 23 (Limitation of handling sensitive information)		Article 23
	Article 24 (Limitation of unique identification process)	②,③	
	Article 25 (installation and operation limits of visual information processing equipment)	③,⑥,⑧	①
	Article 26 (Limitation of personal data processed in accordance with the business consignment)	①,②,③,④	⑤
	Article 27 (the previous limit the amount of personal information in accordance with such sales)	①	
	Article 28 (supervision of personal information handlers)	①,②	
Secure management of personal information	Article 29 (safeguards obligation)	29조	
	Article 30 (Establishment and disclosure of personal information handling policies)	①,②	
	Article 31 (Designation of the Chief Privacy Officer)	①,④	
	Article 32 (registration and disclosure of your personal information file)	①,④	
	Article 33 (Privacy Impact Assessment)	①,②,④,⑤,⑧	
	Article 34 (Notification disclosure of personal information, etc.)	①,②	
Protection of Rights of information processors	Article 35 (access of personal information)	③	
	Article 36 (correction of personal information, delete)	②,③,④	
	Article 37 (suspension of processing personal information, etc.)	②,③,④	
	Article 38 (Methods and procedures for the exercise of rights)	④,⑤	
Items Total		50	7

의 정보화 수준 분석에서 개인정보보호 영역에 대한 측정 항목은 앞의 57가지를 포함하여야 한다. 다만 기업의 유형에 따라 제외할 항목에 대한 구분과 각각의 가중치를 다르게 부여하는 문제에 대한 결정이 필요하다.

3.3 우리나라 개인정보보호정책의 과제

개인정보보호의 이해당사자인 시민, 기업, 공공기관이 함께 개인정보보호를 위한 생태계를 조성하는 측면에서 다음과 같은 법률 및 조직적 차원의 다수의 과제들을 추진하는 것이 필요하다.

먼저 법률적인 측면에서 IT기술의 발달에 따른 모바일 환경에 따라 새롭게 발생할 수 있는 개인정보 침해유형에 대비하여 일반법인 개인정보보호법에 공통된 기준마련 및 관련 영역별로 개별적인 법률 제・개정이 필요하다. 또한 일반법인 개인정보호호법과 기존의 다수 개별법 간에 상충되는 요소들에 대한 체계적인 정비도 하나의 과제라고 볼 수 있다.

다음으로 개인정보보호와 관련한 다수의 정부부처와

〈Table 3〉 Existing approaches Privacy Policy

Division	Policy aspects	Detailed policy
Legal and institutional aspects	Privacy and Personal Information Protection Policy	Protection of human rights as a fundamental right protected
	Intellectual Property Rights Policy	Guarantee and management of information resources, intellectual property rights
Technical aspects	Information Systems Security Policy	Security technologies, application services technology-based technologies
Industry and Economics	E-Commerce Policy	Electronic signature, encryption systems, Cyber Environment
	Information Security and Technology Policy	Development of information security technology, standardization, etc.
Administrative and cultural aspects	Information security culture and cooperation policy	Cyber promote healthy environments and Privacy Mind

공공기관들의 관계를 명확하게 하고 이들 기관들의 협조가 필요하다. 또한 개인정보보호위원회가 모든 것을 하기가 어렵기 때문에 개인정보보호를 위한 협회 등 민간 조직들을 활용하는 것도 필요하다.

마지막으로 개인정보보호가 전담 법률과 조직만으로 되는 것이 아니기 때문에 관련 인력과 산업에 대한 지원을 통해 개인정보보호와 관련된 생태계(eco-system) 조성 및 선순환 구조를 마련도 중요한 과제라고 [12].

<Table 3>에서 보는바와 같이 현재까지 개인정보 보호에 대한 연구들은 분야별로 많이 있었으며, 먼저 법률·제도적인 측면에서 개인정보 보호와 관련된 법률적인 해석을 위한 연구들이다. 두 번째로 기술적인 측면에서 보안기술, 컴퓨팅 보안과 관련된 연구들, 다음으로 산업적인 측면에서 민간기업의 소비자를 대상으로 한 개인정보보호에 관한 연구들과 기업의 전략이나 정책에 관한 연구들이 주를 이루어 왔다. 마지막으로는 공공기관의 개인정보보호에 관한 연구들이 수행되어 왔다.

4. 결론 및 시사점

개인정보보호정책을 역사적으로 보면 유럽 국가들은 다른 국가들에 비하여 개인정보를 보호하기 위한 법률 제정 노력이 먼저 되었고 또한 별도의 독립된 전담조직의 신설 등을 통해 개인정보보호를 위해 강화된 정책을 펴고 있다고 말할 수 있다. 미국과 일본은 유럽과 경제적 교류를 하기 위해 이러한 개인정보보호와 관련된 법률적 내용을 법률의 하위 부분인 지침 및 가이드라인의 제정 등을 통해 반영하는 측면이 있다[13].

우리나라는 2011년도 개인정보보호법 제정 이전과 이후를 기점으로 하여 개인정보보호정책은 소위 전환기를 맞이하고 있다고 할 수 있다. 그러나 최근 개인정보를 이용한 범죄가 매우 많이 발생하고 있고, 그 피해규모도 크게 늘고 있는 추세이다. 개인정보보호법의 본래 취지와는 무관하게 현재 상황은 개인정보를 이용한 사고가 발생한 후 책임자 처벌을 위한 목적으로 사용되는 것이 많은 것이 현실이다.

하지만 이 법은 예방적 차원에서 사전적인 검증 역할을 하는데 쓰일 수 있도록 적극 활용하여야 한다[14].

정부 기관이나 민간 차원 등 여러 분야에서 기업의 정보화 수준을 분석하는 활동을 수행하고 있으므로 여기에 개인정보보호 활동에 대해 면밀히 검증할 수 있는 시스템을 확보하는 것이 필요하다[15].

즉, 개인정보보호 활동을 포함하는 기업의 정보화 수준 분석에서도 기 제정되어 시행되고 있는 개인정보보호법에 기반을 두고 측정항목을 도출하는 것이 바람직한 것으로 보인다.

본 논문에서는 중소기업의 정보화 수준 분석에 있어서 개인정보보호 관련 활동을 어떻게 평가할 수 있는지의 여부와, 일반 정보화 수준 분석에서 개인정보보호 활동이 차지하는 비중을 어떻게 도출할 것 인가를 알아보기 위해 연구를 수행하였으며, 개인정보보호법의 3장, 4장, 5장에 포함되어 있는 의무조항과 금지조항에 대해 해당 기업이 적절하게 대응하고 있는지, 그리고 시스템화

되어 있는지를 검토하도록 제안하였다. 그러나 본 연구에서는 질문항목 전부를 나열하지 않았고, 적용 사례를 들지도 않았으므로 향후 연구에서는 질문항목을 나열하고 전문가 집단을 통하여 각 항목의 중요도에 따라 가중치를 도출하여 실증분석을 수행하여 점검기준에 대한 신뢰성을 확보하고자 한다.

ACKNOWLEDGMENTS

This study was supported by the Research Program funded by the Baekseok University.

REFERENCES

[1] Valacich, J. and Schneider, J., Information Systems Today (5th Edition), Prentice Hall,2011.

[2] Hyun-Soo Han, Kiho Kim, Hee-Dong Yang, SME Informatization Attributes Based Analysis for their Criticalness, Status and Policy Implications, Journal Of Information Technology Applications & Management, 2013

[3] hyeong-seok Go, Study on privacy and remedies, Law Society, 2011

[4] Dae-kyeong Jeong, Comparative study of the privacy information protection policy, Privacy information basic laws and dedicated organizations, Information Security and Cryptology, 2012

[5] The Korea Communications Commission, MOPAS, Knowledge Economy, National Information Security White Paper, pp. 131-132, 2011

[6] TIPA, Survey on the Information Level of Korean Small and Medium Enterprises, 2012

[7] Jeong-deuk Kim, Management systems and governance for privacy, Information Security Journal, 2008

[8] Cheol Kim, Privacy and the role of government: the need for integrated privacy committee, Korea Society for Public Administration, 2003

[9] Koornhof, H., A Framework for IT Governance in Small Businesses, 2009

[10] Luftman, J. N., "Assessing Business-IT Alignment Maturity", Communications of the Association for Information Systems, 2000

[11] Levy, M. and Powell, P., Information Systems Strategy for Small and Medium sized Enterprises : An organizational perspective, Journal of Strategic Information Systems, 2000

[12] Sang-kwang Kim, The enactment of the Personal Information Protection and Policy Issues, Korea Policy Institute, Proceedings, 2011

[13] Korea Ministry of Information and Communication, Long-term data protection master plan for a safe and sound knowledge powerhouse implementation, 2002

[14] Keun-Ho Lee, A Measures to Converge Manage an Efficient Information Security Management System for Information Security Experts Manpower, Journal of the Korea Convergence Society, pp.81-86, 2014

[15] Myung-Seong Yim, Development of Measures of Information Security Policy Effectiveness To Maximize the Convergence Security, Journal of the Korea Convergence Society, pp. 27-32, 2014

김 병 철(Kim, Byung Chul)

- 2005년 8월 : 충북대학교 전자계산학과(이학박사)
- 2014년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 2007년 3월 ~ 2010년 11월 : 충남대학교 전기정보통신학부 겸임교수
- 관심분야 : 사물인터넷, 빅데이터, 융합기술, 영상처리
- E-Mail : bckim@bu.ac.kr