ISSN 1229-1889(Print)
ISSN 2287-9005(Online)
J Korean Soc Qual Manag Vol. 41, No. 4: 649-658, December 2013
http://dx.doi.org/10.7469/JKSQM.2013.41.4.649

산업보안 역량 수준평가 및 개선방안

김문선 * · 전대성 **† · 남경현*** · 김규로 **** · 한찬명 *****

* (사)정보통신연구원
** 대구미래대학교
*** 경기대학교
**** 경기과학기술대학교
***** ㈜엠플러스비전

Implication of Industrial Security Capacity Based on Level Evaluation

Moon Sun Kim * · Dae-Seong Jeoune **† · Kyung H. Nam ***
Gyu-Ro Kim **** · Chan-Myeong Han *****

* IMRC(Information and Management Research Consortium), First Author
** Department of Media Design, Daegu Future College, Corresponding Author
*** Department of Applied Information Statistics, Kyonggi University
**** Department of Mechatronics, Gyeonggi College of Science and Technology
***** CEO, M+ Vision Co. Ltd.

Abstract

Purpose: In this study, the actual situation of domestic firms vulnerable to industrial security competence will be discussed. And accordingly be discussed for effective response measures.

Methods: Using a structured questionnaire by mail, fax, e-mail and fill method was used respondents. By the end of '10 R&D Center, which holds 15,247 companies(population) among the 95% level of confidence, tolerance ±3% p-level corporate type, sector, region extraction method stratified multi-level companies were investigated through the final 1529.

Results: The average level of industrial security capabilities 43.8%(out of 100) is very weak, so urgent and positive response measures also need to be investigated sought.

Conclusion: we propose the effective management framework and improvement plans to prevent illegal industrial leakage are to be made.

Key Words: SMEs Survey, Statistic Quality, Quality Control, QMS(Quality Management for Statistics)

• Received 6 December 2013, revised 18 December 2013, accepted 19 December 2013
† Corresponding Author(dsjeoune@dfc.ac.kr)

1. 서 론

최근 잇따른 불법적인 산업스파이 활동 및 기술유출 사건들로 인해 산업보안 및 핵심기술 보호에 대한 사회경제적 관심이 높아지고 있다. 특히 이러한 크고 작은 사건들로 인한 피해사례가 여러 가지로 열세적 위치에 있는 중소기업에게는 그 영향력과 피해 정도가 심각해 사회경제적 관심 외에도 정책적으로 주요 관심과 지원의 대상이 되고 있다[1, 2, 5. 10]. 국내 기업의 기술유출 비율과 피해금액은 최근의 IT융합 환경 속에서 기업의 지속가능한 성장을 저해하고 있다는데 그 심각성이 크다. 지난 3년간('08~'10) 기술유출 경험이 있는 국내 기업은 13.2%로 기업성장을 저해하는 가장 주요한 요인으로 조사된 바 있다[12].

구체적으로 기술유출 1건당 평균 16.7억원의 피해가 발생하고, 이러한 실태는 점차 감소추세인 사고건수에 비해 건당 피해규모는 계속 증가 추세라는데 문제가 있다. 그리고 이와 함께 기업들의 산업보안 역량수준은 매우 취약한 것으로 나타나 그 심각성이 더욱 우려되고 있는 실정이다[12].

이에 본 연구는 국내 기업의 취약한 산업보안 역량실태와 수준을 업종별, 기업유형별로 살펴보고, 이에 따른 효율적인 대응방안에 대해 살펴보고자 한다. 이는 기업의 핵심자산인 산업기술의 불법적인 유출을 선제적으로 방지하고 이에 대한 효과적인 관리방안 모색을 가능하게 하며, 나아가 기업경쟁력 저해요소를 제거함과 동시에 이를 혁신적으로 개선할 수 있는 기회를 제공해 줄 수 있을 것이다.

2. 연구 방법 및 범위

본 연구는 국내 기업을 대상으로 기업유형별, 업종별 산업보안 역량수준을 진단, 평가하는데 1차적인 목적이 있다. 중소기업의 산업보안 정책은 기술적인 관점에서 뿐만 아니라 심리학적, 사회적, 조직적 관점에서도 고려되어야 하며, 이는 기업의 산업보안 정책에 많은 영향을 주는 것으로 보고되고 있다[16, 17, 18]. 이에 본 연구에서는 이러한 사항들을 종합적으로 고려하여 <Figure 1>과 같이 중소기업에 적합한 산업보안 관점의 3개 분야(정책분야, 적용분야, 대응분야)별로 산업보안 구성요소에 대한 수준을 평가하였다. 그리고 각 분야별 내 항목별로 0~3점을 부여한 후 항목별 점수를 합산하여 해당 분야의 산업보안 수준을 산출하였다.

연구방법으로는 구조화된 설문지를 활용한 우편, 팩스, 이메일 등을 이용하였고, '10년말 기준 기업부설연구소를 보유하고 있는 15,247개 기업(모집단) 가운데 95% 신뢰수준, 허용오차 ±3%p 수준에서 기업유형별, 업종별, 지역별 다단계 층화추출방법을 통해 최종 1,529개의 기업을 조사하였다. 표본크기는 조사여건과 비용을 고려하여 Neyman의 최적배분법과 비례배분법의 장점을 이용한 Power Allocation을 활용하였다.

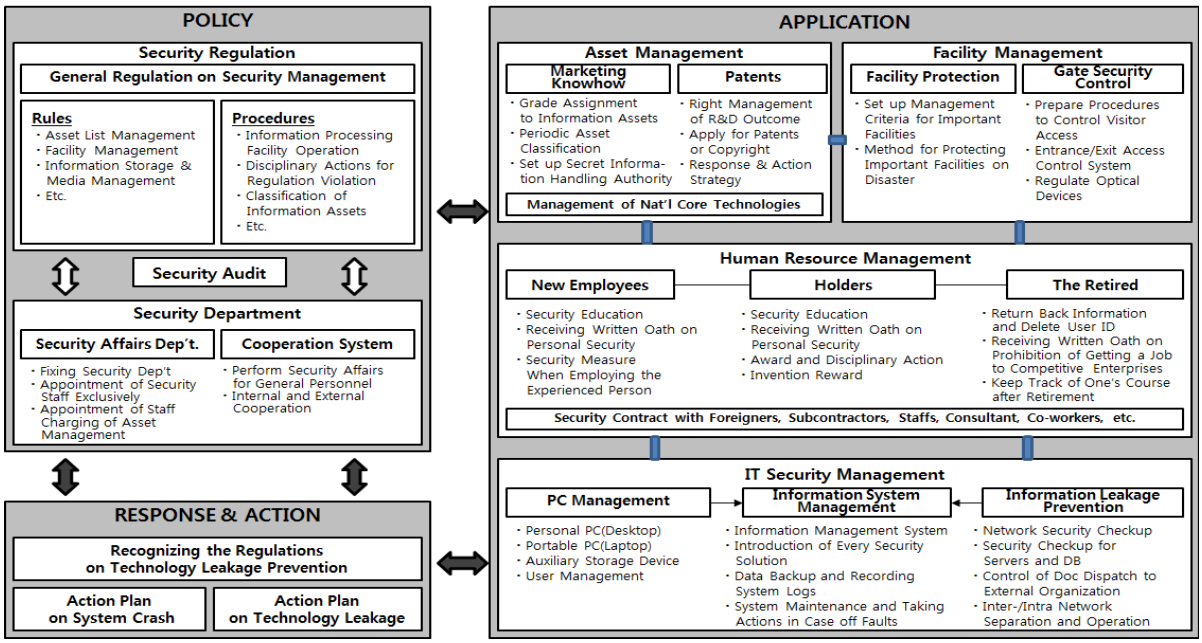


Figure 1. Research model for level evaluation on industrial security capability

3. 산업보안 역량수준 평가

본 연구에서 논의되는 산업기술에 대한 정의는 공공연하게 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 상당한 노력에 의하여 비밀로 유지된 유·무형의 기술 또는 경영정보를 말한다. 아울러 보안비용이라 함은 산업기술 관리시스템 구축, 보안 전담인력에 대한 인건비, 보안교육, 보안홍보 등 산업기술 보호를 위해 기업이 지출하는 비용을 일컫는다. 그리고 본 연구에서는 산업보안 역량수준은 세 분야의 점수를 합하여 측정하며 점수별로 우수(Excellent), 양호(Good), 보통(Normal), 취약(Weak), 위험(Dangerous) 등의 5단계로 성숙도(Maturity Score)를 평가한다.

단계별 특성을 보면, 먼저 1단계(위험, 40점 미만)는 보안에 대해 심각한 결점 및 취약성이 상존하고, 기술유출 및 침해 정도에 따라 치명적인 피해가 우려되는 상태이며, 2단계(취약, 40점 이상 55점 미만)는 보안에 대해 다소 심각한 결점 및 취약점을 내포하고, 기술의 유출 및 침해 정도에 따라 치명적인 피해를 가져올 수 있다. 3단계(보통, 55점 이상 70점 미만)은 보안에 대해 일반적인 결점 및 취약성을 내포하고, 기술의 유출 및 침해 정도에 따라 피해가 커질 수 있는 상태이며, 4단계(양호, 70점 이상 85점 미만)는 보안에 대해 심각하지 않은 결점 및 취약성을 내포하고, 회사차원의 보안업무가 일정부분 이루어지고 있는 상태를 나타낸다. 마지막으로, 5단계(우수, 85점 이상)는 보안에 대한 결점 및 취약성이 거의 없고, 기술의 유출 및 침해사고 발생 시 피해가 최소화되는 상태를 의미한다.

4. 조사결과 분석

4.1 산업보안 역량

전반적으로 산업보안 역량수준이 '10년 대비 소폭 하락한 가운데, 평균 43.8점(100점 만점)으로 취약한 수준으로 나타났다. 이는 기업유형별로 다소 차이가 있는데, 대기업은 75.4점으로 양호한 수준인 반면, 중소기업(벤처기업 제외)은 42.6점, 벤처기업은 42.8점으로 위험에 가까운 매우 취약한 수준인 것으로 조사되었다. 특이사항으로는 일반 중소기업에 비해 상대적으로 기술이 집약된 벤처기업의 수준이 2010년과는 큰 차이가 없다는 점이다(<Figure 2(a)>).

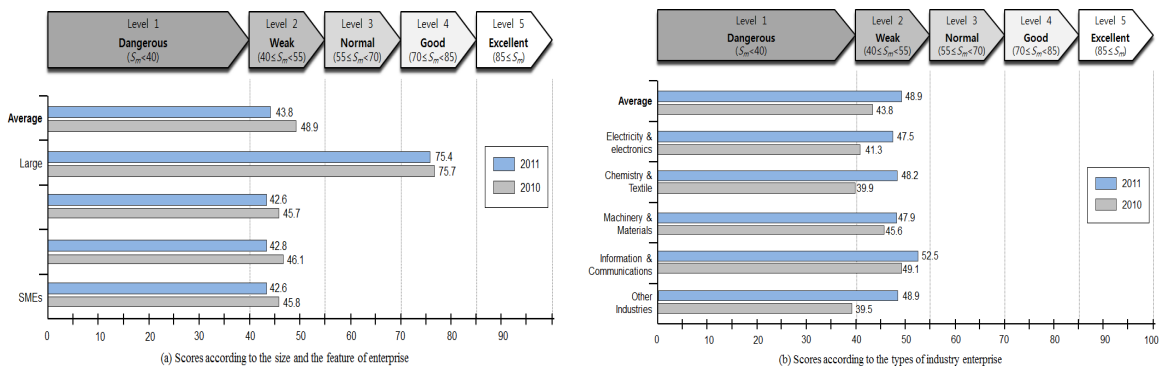
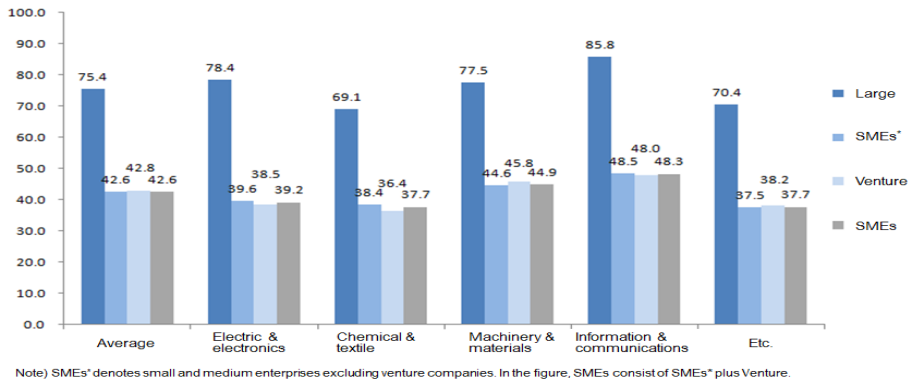


Figure 2. Maturity score for industry security capability

이러한 결과는 기술응집형 벤처기업이 경기침체와 영세성 등으로 인하여 산업보안 역량수준 제고노력이 상대적으로 미흡했던 것으로 풀이된다. 이를 업종별로 살펴보면, 화학섬유(39.9점), 기타(39.5점)가 위험수준, 그 외 전기전자(41.3점), 기계소재(45.6점), 정보통신(49.1점)으로 나타났다. '10년 결과와 비교했을 때, 상대적으로 전기전자 및 화학섬유, 기타업종이 5점 이상의 하락폭을 보여 시급한 대응책 마련이 필요한 것으로 보인다(<Figure 2(b)>).

업종별, 기업유형별 산업보안 역량수준을 살펴보면, 대기업의 경우 정보통신(85.8점)이 가장 우수한 가운데, 대체로 양호한 수준을 보였다. 반면, 중소(벤처기업 제외) 및 벤처기업은 전 업종에 걸쳐 매우 취약한 수준을 보였다. 업종 특성상 정보통신이 상대적으로 높긴 하지만 각각 45.8점, 48.0점 등으로 취약수준이었고, 이외의 업종들은 이들보다 더욱 낮은 매우 취약 및 위험수준으로 진단돼 매우 심각한 상태임을 나타내었다(<Figure 3>)



Note) SMEs* denotes small and medium enterprises excluding venture companies. In the figure, SMEs consist of SMEs* plus Venture.

Figure 3. Industrial security capacity level according to the size, feature and industry enterprise

4.2 산업보안 역량수준별 기업 분포

먼저 보안역량 수준별 기업분포를 살펴보면, 위험수준 영역에 가장 많은 기업이 분포해 있으며(46.4%), 다음으로 취약(24.2%), 보통(15.3%) 순이었다. 대기업은 우수기업이 37.0%로 가장 많고, 다음으로 양호(29.6%), 보통(20.4%), 취약수준 이하(13.0%) 순이었다. 중소(벤처기업 제외) 및 벤처기업은 모두 절반가량(각각 47.7%, 46.4%)이 위험수준인 것으로 나타나(<Figure 4(a)>), 위험군의 중소/벤처기업을 대상으로 하는 수준향상 지원책 마련이 우선적으로 필요한 것으로 분석되었다.

업종별 보안역량 수준을 살펴보면, 대부분의 업종에서 80% 내외가 취약수준 이하인 것으로 조사되었다. 특히 전기전자, 화학섬유, 기타업종은 과반 이상이 위험수준에 노출되어(<Figure 4(b)>), 정확한 실태 파악과 함께 시급한 대응책 마련이 필요함을 알 수 있었다.

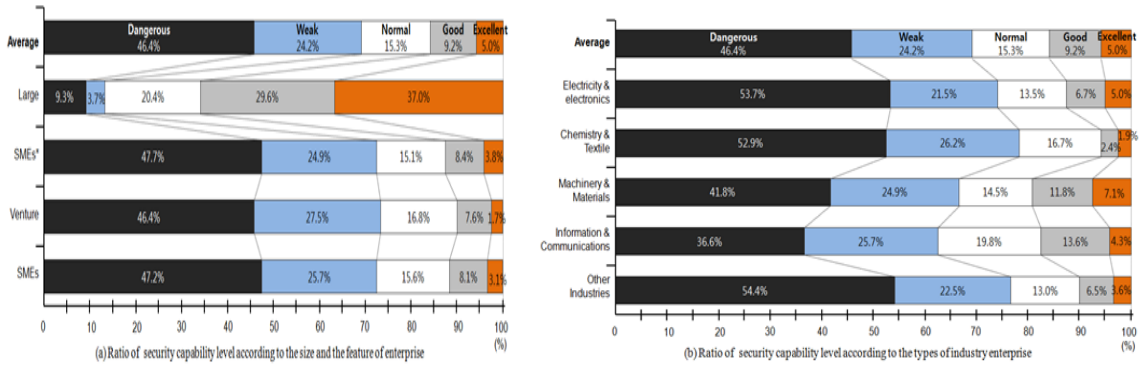


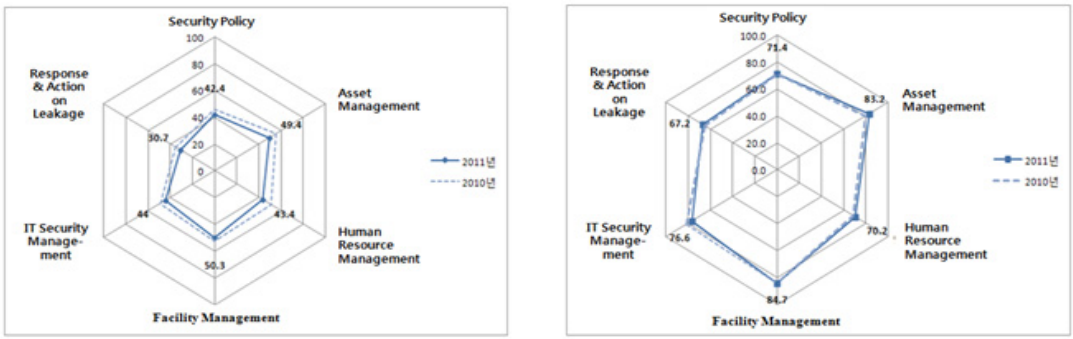
Figure 4. Distribution of industrial security capacity level according to the size, feature and industry enterprise

4.3 영역별 산업보안 역량

영역별 산업보안 역량점수의 경우, 유출사고 대응(30.7점)이 위험 수준, 나머지 5개 분야는 모두 취약한 것으로 조사되었다. '10년 대비 하락세를 보이는 가운데, 인적자원관리 및 자산관리에서의 하락이 5점 이상으로 크게 나타

났다(<Figure 5(a)>).

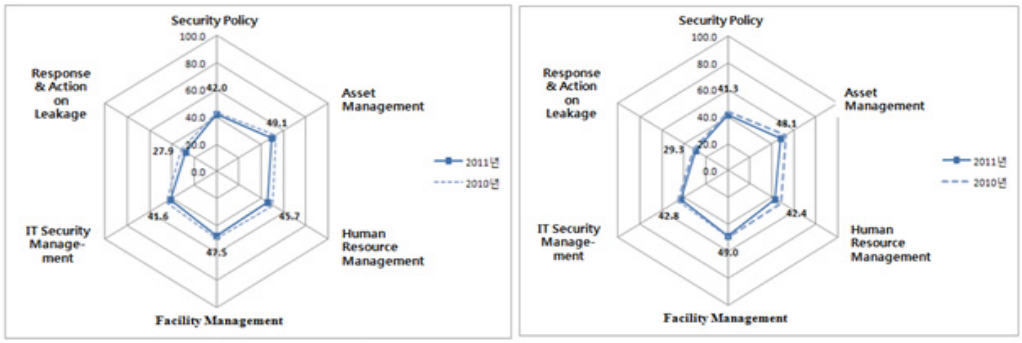
기업유형별로 보면, 대기업은 유출사고 대응이 67.2점으로 보통수준이고, 그 외는 모두 양호하였는데, 특히 시설관리(84.7점) 및 자산관리(83.2점)는 80점 이상으로 높은 보안역량 수준을 보였다. '10년과 비교해 보면 큰 차이 없이 보안수준이 유지되는 것을 알 수 있었다(<Figure 5(b)>).



(a) Total including large and SME enterprises (b) Large enterprises

Figure 5. Security capability in various areas of industrial security

그러나 중소기업 및 벤처기업은 모두 전반적으로 보안수준이 취약하며 유출사고 시 대응수준이 가장 위험한 수준인 것으로 조사되었다(<Figure 6>). 결론적으로, 대기업을 비롯한 대부분의 한국기업들이 최근 큰 관심과 이슈를 보이는 산업스파이 및 불법 기술유출 사건 발생 시 매우 취약하고 위험한 상태임을 알 수 있다.



(a) SMEs excluding venture companies (b) Venture companies

Figure 6. Security capability of SMEs versus venture companies

업종별·영역별 산업보안 역량수준은 전기전자 및 화학섬유업종이 가장 취약한 것으로 조사되었다. 그리고 6대 영역 가운데 유출사고 대응이 가장 취약해 구체적이고 시급한 대책 마련이 필요한 것으로 분석되었다. 반면 시설관리와 자산관리 영역은 타 영역에 비해 다소 나은 수준이었는데, 이는 유형 자산에 대한 파악과 관리가 용이하기 때문으로 풀이된다. 한편 정보통신업종은 인적자원관리에 대한 보안수준이 다소 높은 것으로 나타났는데 이는 업종특성에 기인하는 것으로 볼 수 있다(<Figure 7>).

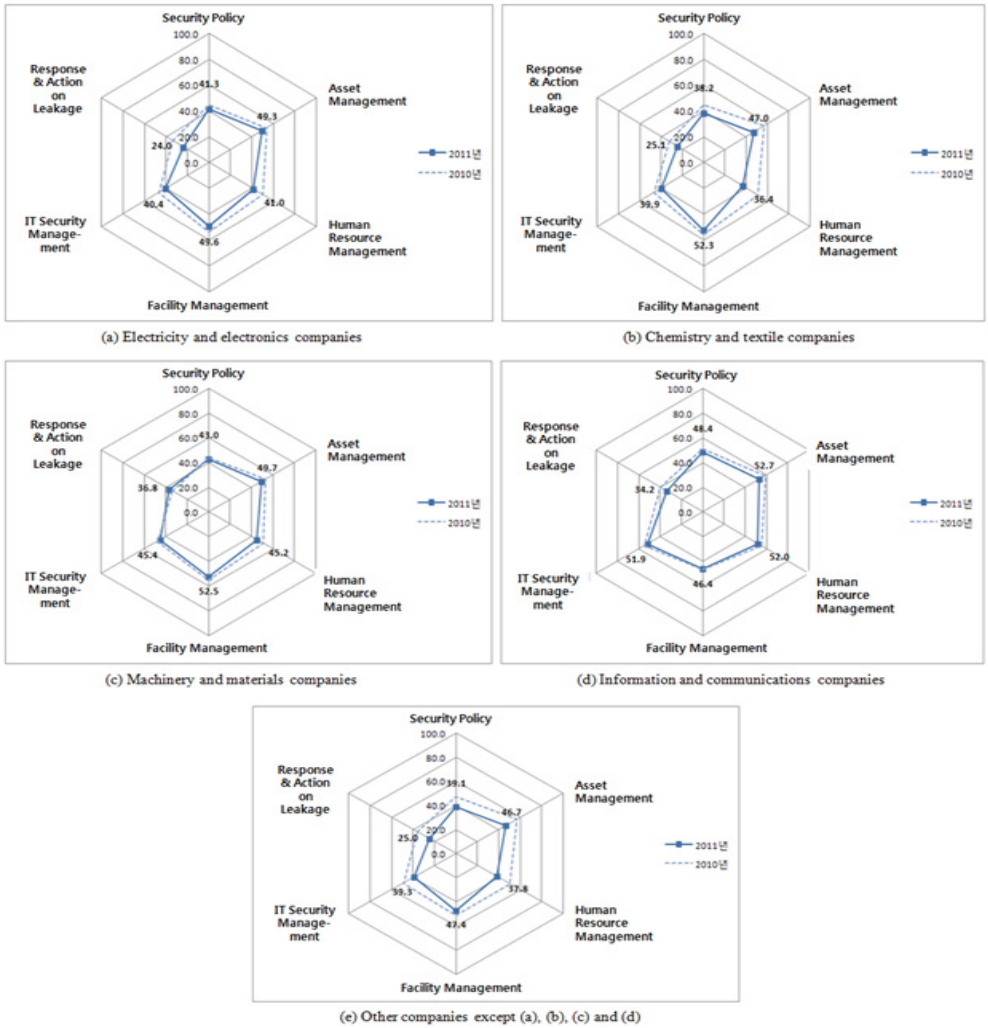


Figure 7. Security capability in various areas of industrial security according to their belonging industry enterprise

5. 개선방안 및 시사점

본 연구에서는 분석결과를 토대로 한국 중소기업의 혁신적인 산업보안 역량 강화를 위한 세 가지의 정책적 개선방안 및 지원방안을 제시한다.

첫째, 중소기업형 기술보호 참조모델 개발이 필요하다[3, 8, 13]. 금번 조사결과에 따르면, 대다수의 중소기업이 산업보안 역량수준이 매우 취약함(평균 43.8점/100점 만점)과 동시에 내·외부 여건 또한 영세하고 위험수준으로 스스로 이를 해결 또는 해소하기에는 역부족인 것을 잘 알 수 있었다. 따라서 현재 중소·벤처기업의 보안역량 개선을 위해서는 우선적으로 수시로 참고하고 활용할 수 있는 참조모델이나 지침, 가이드라인 등의 제작과 이의 보급이 필요하다고 판단된다. 그리고 이를 위해 먼저 역량과 기반이 어느 정도 갖춰진 기업부설연구소 보유기업에 대한 기술보호 참조모델을 개발, 보급하는 것을 제안한다. 아울러 보다 쉽게 이용, 적용 가능한 보안매뉴얼을 제작하고, 보안지침 이행여부를 자동 측정하는 도구를 개발, 보급하며, 보안활동 투자대비 성과개선 편익을 가시화할 수 있는 방법

론 등을 개발하고 이에 대한 교육이 필요하다 하겠다[2, 6, 11].

둘째, 기술유출 사고대응 체계를 수립하는 것이 시급하다. 조사결과에서 볼 수 있듯이 국내 기업의 보안사고 및 기술유출 시 대응수준은 30.7점으로 매우 위험한 수준으로, 이는 중소기업뿐만 아니라 벤처기업까지 마찬가지로 나타났다. 대기업은 보통수준(67.2점)이라고 하나, 이 또한 글로벌 경쟁력을 가져야할 입장에서는 매우 취약하고도 위험한 수준이라 할 수 있다. 따라서 국내기업들 모두 사후예방을 위한 대응체계로서 기술유출 사고대응 체계 마련이 중요하고도 필요하다 하겠다. 현재 가장 취약한 유출사고 대응역량 개선을 위해 기술유출 사전예방 활동과 연계한 사후 대응처리 과정을 수립, 홍보, 활용토록 한다. 이 때 기술유출 예방교육은 근무기간 및 조직 내 직급에 따라 차별화하여 맞춤형 교육이 이루어져야 할 것이다[6]. 특히, 인적자원 유출이 많으므로 표준화된 퇴직자 보안교육 교재 및 온라인 콘텐츠 개발, 유출사고자 또는 보안규정 위반자에 대한 사례별 처리 가이드라인[6, 9] 등을 제공하는 구체적 실행방안도 필요하다.

마지막으로 내부 유출방지에 특화된 보안기술 개발 지원이 요구된다. 산업보안 관리 및 개선을 위해서는 가장 우선적으로 내부의 인적자원관리가 가장 중요하다는 조사결과가 많다. 이는 상당수의 기술유출 및 산업보안 관련 사건, 사고가 주로 내부 임직원에 의해 발생하고 있기 때문이다. 그럼에도 불구하고 금번 조사결과에 의하면, 중소기업의 인적자원관리 수준은 43.4점, 대기업은 70.2점으로 취약 또는 보통 수준에 불과한 것으로 나타났다. 이에 최소한 내부직원에 의한 유출사고 정도는 스스로 사전예방 및 통제관리할 수 있도록 방안 마련이 필요하다 하겠다. 이에 산업보안에 특화된 보안시스템 지원요청에 부응하기 위해 내부 유출방지 기술개발에 중점적으로 지원하고, 특히 최근 이슈화되고 있는 서비스지향형 보안서비스(Service-oriented Security Service)를 제안한다.

6. 결 론

산업보안 역량수준이 평균 43.8점으로 매우 취약하고 '10년에 비해 5.1점 하락한 가운데, 향후 국내 기업의 경쟁력 있는 지속성장의 큰 걸림돌로 작용할 것이 예상된다. 대기업의 경우 75.4점으로 상대적으로 양호한 수준이나, 글로벌 경쟁시대를 감안할 때 안심할만한 수준은 아니므로 국내 기업의 산업보안 경쟁력은 전반적으로 매우 심각한 수준으로 분석할 수 있겠다. 이렇게 취약한 산업보안 역량수준은 위험수준의 기업 비중이 46.4%라는 점에서 매우 시급하고도 구체적인 대안 마련의 필요성이 제기된다 하겠다. 그리고 무엇보다 최근 경기침체 및 글로벌 금융위기로 인해 경기대응력이 취약[14, 15]한 중소기업 및 벤처기업의 타격이 클 것으로 예상되는바, 가장 기본적이고 근원적인 자기방어 전략으로서 산업보안 역량강화의 필요성은 매우 절실하고도 생존과 직결된 필수 과제라 할 것이다[3, 4, 6, 7]. 그러나 한국기업의 절대 다수는 유출사고 발생 시 대응역량이 30.7점에 불과하며, 실제로 현장에서 이루어지는 보안수준은 눈에 보이는 시설관리와 자산관리 정도에 그치는 것으로 조사결과 나타났다. 이 또한 최소한의 자산파악 및 목록 구성 정도의 기초적인 수준으로 취약한 실태(50점 내외)를 보여, 결국 한국기업의 산업보안 역량수준은 총체적 난국으로 획기적인 대응책 및 개선책 마련이 필요한 시점이다.

한편 본 논문은 몇 가지 측면에서 한계가 있음을 밝혀둔다. 먼저 본 논문에서 산업보안 역량평가모델로 사용한 연구프레임에 대한 풍부하고도 정교한 이론적 기반연구에 대한 아쉬움이 있다. 본 모델은 정책적 요구사항 반영과 지난 3년간의 조사결과를 기초로 하여 구상, 개발된 연구모델이다. 산업보안 및 정보보안 분야의 많은 선행・최신 연구의 결과를 검토 분석하여 본 모델을 보다 정교화, 체계화할 필요성이 있다. 그리고 본 연구는 제조업 대상에 국한되어 있어, 향후 조사대상의 업종 확대가 필요하다. 물론 산업보안역량이 매우 취약한 현재의 우리나라 상황에서는 그나마 기본적인 인프라 및 주변 여건이 안정적인 제조업을 연구대상으로 할 수밖에 없었던 이유가 있긴 하다.

그러나 점차 산업보안에 대한 인식 증가, 인프라 개선 등의 추세를 반영한다면 향후 도소매를 비롯한 서비스업이나 건설, 유통 등에 대한 연구대상 확대도 가능하리라 보여진다. 모쪼록 이러한 한계점들이 후속연구자들의 활발한 추가연구를 통해 개선 및 해결될 수 있기를 희망한다.

REFERENCES

Anderson, R. 2008. Security Engineering: A Guide to Building Dependable Distributed Systems 2nd Ed., John Wiley & Sons.

Baek, Min-Jeong, and Shon, Seung-Hee. 2011. "A Study on the Effect of Information Security Awareness Behavior on the Information Security Performance in Small Medium Sized Organization." Korean Small Business Review 33:113-32.

Heo, Jaeyoung. 2008. "An Empirical Study on Industrial Security of Small-to-Medium Companies." MBA Thesis, Hanyang University.

Hwang, Soon-Hwan. 2003. "An Analysis on the Heightening of Capability to Cope with Depression through Informatization." Proceedings of 2003 Fall Conference, The Korea Society of IT Services in Fall 309-15.

Hwang, Soon-Hwan, and Kim, Moon-Sun. 2005. "Analysis of Relation between the Informatization Level Evaluation and Performance of Small and Medium Enterprises." Korean Management Review 43:549-68.

Jang, Hang-Bae. 2010. "The Design of Information Security Management System for SMEs Industry Technique Leakage Prevention." Journal of Korea Multimedia Society 13:111-21.

Kim, In-Kwan. 2011. "A Study Affecting the ISMS Certification by Security Awareness of Industrial Technology and Investment of Information Security." M.S. Thesis, Konkuk University.

Kim, Jongki, and Jeon, Jinhwan. 2006. "Comparison of Users' Perception of Information Security Elements on Computer Virus between Large and Small-and-Medium Companies." Journal of the Korea Institute of Information Security & Cryptology 16:72-92.

Kim, Kwan-Soo. 2009. "A Study on the Information Leakage Prevention appropriate to the Small and Medium Enterprises." M.S. Thesis, Konkuk University.

Kim, Kyung-Kyu, Ryoo, Sung-Yul, Shin, Ho-Kyoung, and Kim, Moon-Sun. 2007. "Evaluation of the Level of Informatization for Small and Medium Enterprises." Korean Small Business Review 29:41-71.

Korea Technology and Information Promotion Agency. 2012. Survey Report on 2011 Technology Protection Capability and Level Evaluation. Small and Medium Business Administration. TIPA.

Lee, Yeong-Kyu. 2008. "An Empirical Study on the Coincidence and the Importance of the Evaluation Indicators for Information Security." Ph.D. Dissertation, Kwangwoon University.

Moon, Hyun-Jeong. 2009. "Present State and Problems on Educational Training for Strengthening Information Protection Capability of Korean SMEs." Review of the Korea Institute of Information Security & Cryptology 19:29-39.

Noh, Min-Sun, and Lee, Sam-Yeol. 2010. "Explaining Industrial Security of SMEs in Korea: An Ordered Logit Analysis." Proceedings of the Korean Association for Public Administration 44:239-59.

Pipkin, D. L. 2000. Information Security: Protecting the Global Enterprises. Prentice Hall PTR.

Shin, Gyo-Sun. 2008, "A case study on the applicability of large-scale security system to the small and medium sized business." MBA Thesis, Kookmin University.

Weippl, E., and Klemen, M. 2006. Implementing IT Security for Small and Medium Enterprises. New York: Information Science reference.

Yeo, Sangsoo, and Hwang, Suchul. 2009. "A Safe Operating Strategy for Information System of Small & Medium Enterprises." Journal of the Korea Society of Computer Information 14:105-12.