The Journal of Digital Policy & Management 2013 Oct; 11(10): 1-16

중소기업 산업보안 강화를 위한 지방정부의 역할 분석연구
-경기도 사례에 대한 실증분석을 중심으로-

박태형*, 임채홍**, 이기오***, 임종인****
고려대학교 정보보호대학원*, 고려대학교 정부학연구소**, 경기도청 정보보호팀***, 고려대학교 정보보호대학원****

Analysis on Local Governmental Role for Strengthening of Industry Security in Small and Medium-sized Businesses
-Focused on Empirical Analysis of Case of Gyeonggido-

Tae-Hyoung Park*, Chae-Hong Lim, Kee-O Lee***, Jong-In Lim****
Graduate School for Information Security, in Korea University*
Institute of Government Studies, in Korea University**
Team for Information Security, in GyeongGi-Do Provincial Government***
Graduate School for Information Security, in Korea University****

요 약 본 연구는 중소기업 산업보안 강화를 위해서 지방정부에 해야 할 역할에 대해서 경기도 사례를 중심으로 분석하였다. 특히, 경기도가 해당 지역의 중소기업 산업보안 강화를 위해 추진하고 있는 다양한 사업(사이버안전기업 구축 및 민관보안관제센터 활성화 등)에 대해서 중소기업의 담당자를 대상으로 다양한 측면에서 분석 및 평가함으로써, 향후 이러한 수요에 맞게 경기도가 담당해야할 역할이 무엇인지를 탐색해보는데 초점을 두었다. 이상의 연구결과를 바탕으로 산업보안의 사업에 대한 홍보극대화, 보다 현실적인 사업운영 및 중장기적인 전략수립에 대해해서 논의하고, 추후 후속연구의 필요성에 대해서 제시하였다.

주제어 : 중소기업, 산업보안, 지방정부 역할

Abstract This study analyzed on local governmental role for strengthening of industry security in small and medium-sized businesses, Focused on case of Gyeonggido. In particular, Gyunggi-do evaluates various businesses (construction for cyber security businesses and revitalization of the private security control centers) which are promoted to strengthen industrial security in the region, by targeting SME representatives in various aspects. We focused on finding what role Gyeonggido can take to meet this demand has been explored. Based on the above research result, discuss ways to maximize promotion effects about industry security's activites, and more realistic business management. Futhermore, The need for further follow-up studies are presented.

Key Words : Small and medium-sized businesses, Industrial security, Local government's roles

* 본 논문은 미래창조과학부 및 정보통신산업진흥원의 '지식정보보안인력양성 최고정보보안전문가과정' 사업의 연구결과로 수행되었음(과제번호: NIPA-H2102-13-1002)"
Received 24 June 2013, Revised 22 July 2013
Accepted 20 October 2013
Corresponding Author: Jong-In Lim(Graduate School for Information Security, in Korea University)
Email: jilimr@korea.ac.kr

ISSN: 1738-1916

1. 서론

일반적으로 산업기술보안은 국가경쟁력차원에서 다루어져야할 문제로 인식되고 있다. 그러나, 최근에 국가의 역할과 더불어, 지방정부의 역할이 점차 강조되고 있는 추세이다. 즉, 국가차원에서의 전체적인 전략을 지역수준에서 보다 구체화시키는데 있어서 해당 지역의 다양한 주체(학교, 기업, 지방정부 등)의 협력이 중요하게 부각되었고, 이들 사이에 지방정부가 어떠한 역할을 수행해야 하는지에 대한 고민이 요구되고 있다. 이에 본 연구는 중소기업 산업보안 강화를 위해서 지방정부에 해야할 역할에 대해서 경기도 사례를 중심으로 실증적으로 분석하는데 목적이 있다.

최근, 경기도에서는 사이버공격 등 보안이슈 증가로 인해서, 개인정보보호법 대응, 60만 중소기업 산업보안 강화, 민간 보안관제 서비스 확대지원과 더불어, 중소기업 산업기술 유출 방지 및 개인 정보보호 지원 대민서비스 강화가 요구되고 있다. 이에 따라서 경기도에서는 경기도 정보보안 최고책임자(CSO)협의체 구성('12. 5), 사이버안전기업 대상 중소기업 지원(포천 킹유전자)('12. 8), 경기도·17개 보안업체 사이버안전기업 구축지원 MOU('12. 9), 사이버안전기업 구축 대상기업 보안컨설팅(김포, 안산)('12. 12), 경기도 산업보안포럼 개최(민관보안관제센터 연계 협약)('12. 12) 등과 같은 지속적인 노력을 추진 중에 있다(경기도, 2012a; 2012b; 2012c; 2012d; 2012e; 2013).

이러한 상황에서 경기도가 해당 지역의 중소기업 산업보안 강화를 위해 추진하고 있는 다양한 사업(사이버안전기업 구축 및 민관보안관제센터 활성화 등)에 대해서 개괄적으로 분석 및 평가하는 작업은 중요하다. 왜냐하면 해당 사업의 중장기적인 방향을 모색하는데 고려되어질 투입, 산출, 결과, 고객, 외적요인 등의 요소를 반영한 사업을 추진하는데 점검이 반드시 필요하기 때문이다. 이러한 측면에서 본 연구는 중소기업의 담당자를 대상으로 인식 및 견해를 실증적으로 살펴봄으로써, 향후 고객의 입장에 맞게 경기도가 담당해야할 역할이 무엇인지를 탐색해보는데 초점을 둔다.

서론에 이어 2장에서는 산업보안과 관련된 이론적 논의 및 기존연구의 경향을 심층적으로 분석하고 본 연구의 차별성에 대해 논의한다. 3장에서는 경기도 사례의 개요를 소개하고, 2장의 논의를 바탕으로 연구설계 및 조사방법을 자세히 설명한다. 4장에서는 다양한 측면에서 경기도 중소기업 담당자의 의견을 실증적으로 분석한다. 마지막으로 5장에서는 본 연구 결과를 요약하고 이를 통한 정책적 시사점에 대해서 논의한다.

2. 이론적 논의 및 선행연구 검토

2.1 산업보안에 대한 이론적 논의

2.1.1 산업보안에 대한 개념적 논의

산업보안(Industry Security)은 산업기술의 경제적 중요도의 증가에 따라 국가 및 기업 등에 의해 산업기술을 보호하기 위한 다양한 활동이 수행되면서 등장한 광의적인 개념이다. 그동안 일반적으로 산업기술 보호 활동이 주로 기업 실무적 측면에서 수행됨에 따라, 국내 학계에서는 산업보안에 대한 개념 및 정의에 대해 일관된 합의가 이루어지지 않았다(노호래, 2008; 최순호, 2009; 노민선, 2010; 정덕영, 2010; 최선태, 2010; 최진혁, 2010; 이하섭, 2012; 정병수, 2012). 하지만 최근에 IT 등의 첨단산업이 기업의 경제활동을 넘어 국가의 사회, 경제, 안보 등에 광범위한 영향을 미치면서, 산업보안에 대한 다각적인 논의가 추진되고 있다. 이에 따라 산업보안의 개념 및 이론이 정립되는 등 산업보안의 학문적·이론적 특성이 점차 구체화되고 있는 추세이다(정병수, 2012).

그동안 국내에서 산업보안의 핵심 역할을 담당해온 국가정보원에서는 산업보안을 '산업과 관련된 기밀(산업과 관련된 것으로 외부에 드러내서는 안될 국가기관이나 기타 조직체의 비밀)의 안전을 유지하는 일'로 정의하였으며, 구체적으로 산업보안을 '산업체·연구소에서 보유하고 있는 기술·경영상 정보 및 이와 관련된 인원·문서·시설·통신 등을 경쟁 국가 또는 업체의 스파이나 전·현직 임직원, 외국인 유치과학자 등 각종 위해요소로부터 침해되지 않도록 보호하는 활동'으로 제시하였다(국가정보원, 2002; 2008). 그 외에도 산업보안 정의는 다양하게 정의되고 있다.

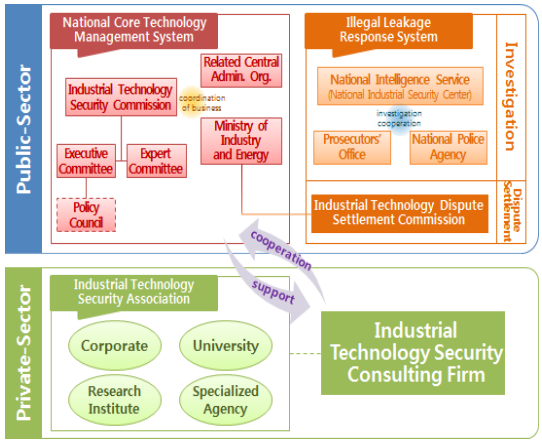
기존연구들은 보호의 대상 및 범위와 활동의 범주에 있어 다소 차이가 존재하지만, 산업활동과 관련하여 자산 보호를 위해 수행하는 일련의 활동을 산업보안으로 정의하고 있다. 이러한 기존연구들은 주로 정진홍(2006)

의 산업보안의 정의를 주로 인용하고 있는데, 본 연구에서도 이에 근거하여 "첨단기술 뿐만 아니라 산업활동에 유용한 기술상, 경영상의 모든 정보나 인원, 문서, 시설, 자재 등을 산업스파이나 경쟁관계에 있는 기업은 물론이고 특정한 관계가 없는 자에게 누설 또는 침해당하지 않도록 보호·관리하기 위한 대응방안이나 활동"을 산업보안의 개념으로 정의하고자 한다(정진홍, 2006; 노호래, 2008; 이준복, 2009; 최순호, 2009; 정덕영, 2010).

2.1.2 산업보안에 대한 공공부문과 민간부문의 연계 필요성

산업보안은 활동의 주체와 지원 범위에 따라, 정부기관이 국익 보호를 목적으로 산업기밀 해외유출 차단을 위해 수행하는 교육·컨설팅 지원 등 유출 예방활동 및 산업스파이 색출활동인 '국가차원의 산업보안'과 기업·연구소 등이 자체적으로 보유하고 있는 기술·경영상 정보 및 이와 관련된 인원·문서·시설·전산·통신 등을 경쟁국가 또는 업체의 산업스파이 등 위해 요소로부터 보호하는 일체의 활동 '기업차원의 산업보안'으로 분류할 수 있다(국가정보원, 2008).

하지만 국가의 연구개발이 대부분 기업에 의해 수행되고 있고 기업의 첨단산업기술 보유가 국가 경제에 미치는 영향이 상당함을 고려할 때, 산업보안은 국가나 기업의 개별적인 활동의 수행으로 이루어지는 것이 아닌, 국가와 정부기관을 대표로 하는 공공부문에 의한 지원과 기업, 연구기관 등의 민간부문에 의한 협조를 기반으로 하는 공공-민간의 파트너십을 통해 추진되어야 하는 특성을 가진다. 특히, 국가의 산업 발전에 있어 산업보안의 대상인 첨단 산업에 대한 의존도가 높아지고 있는 현실을 고려한다면, 산업보안의 핵심인 첨단 산업기술 유출의 방지와 보호를 위한 범정부 차원의 대응이 산업보안에 있어서 가장 우선적으로 논의되어야 하며, 이와 함께 민간 기업의 산업보안을 지원하는 정부기관 내 유관부처가 민간 부문과의 유기적 공조 하에 실효성 있는 정책과 계획을 수립하여 민간 기업의 산업보안을 지원해야할 필요가 있다. 더 세부적으로 살펴보면, 공공부문에서는 산업보안을 위한 국가핵심기술 관리체계와 불법유출 대응체계가 명확하게 구축되어야 하며, 이러한 국가적 산업보안 활동이 민간부문의 산업기술보호협회를 통해 기업, 연구기관 등에 대해 연계되어 추진되어야 한다.



[Fig. 1] Industrial technology security policy implementation system

이러한 국가 중심의 산업보안 추진체계의 실질적 구현을 위해서는 핵심 산업 기술의 관리, 기술유출의 대응, 협력·공조 등 정부기관의 역할·책임과 산업기술 유출에 대한 규제가 법제도적 측면에서 규정되어야 하며, 이를 기반으로 각 부처 및 기관들이 국가 및 기업의 산업보안 활동을 효과적으로 지원할 수 있도록 하는 관리적 측면의 다양한 국가 정책이 수립되어야 한다. 또한 산업기술을 보유한 민간 기업 차원에서는 산업보안을 위해 필요한 관리적·기술적 보호 조치의 도입을 고려해야하며, 산업보안 관련 기술의 연구개발, 도입 등에 대한 국가의 지원이 연계되어야 한다.

2.2 선행연구 검토와 본 연구의 차별성

2.2.1 산업보안에 대한 선행연구 경향

국내에서 1990년대부터 국가정보원의 주도로 산업보안 활동이 시작된 이후 2003년에 국정원 산하에 산업기밀보호센터가 설립되면서 산업기술의 보호를 위한 보안기술 및 법제도에 대한 연구들이 시작되었으며, 2007년 수립된 「산업기술의 유출방지 및 보호에 관한 기본계획」에 따라 지식경제부, 중소기업청, 한국산업기술보호협회 등을 통해 산업보안 강화를 위한 실태조사 및 정책연구과제가 추진되면서 산업보안 관련 기반이 구축되었다. 따라서 한국산업보안연구학회 등의 학회를 통해 산업보안에 대한 학문적 연구가 본격화되고 있다.[1)]

1) 정병수(2012)에서는 국내 산업보안의 연구가 2006년 이후부

본고에서는 산업보안의 주로 2000년 이후 발표된 산업보안 관련 선행연구를 다양하게 분석하여 국내 산업보안 연구 경향을 파악하고자 한다. 특히, 본고에서는 한국연구재단의 한국학술지인용색인(KCI) 사이트(www.kci.go.kr)와 한국교육학술정보원의 학술연구정보서비스(RISS) 사이트(www.riss.kr)에서 산업보안, 산업기술유출, 산업스파이, 기술유출 등의 산업보안 관련 키워드로 검색된 국내 등재학술지 및 등재후보학술지를 중심으로 분석한다.[2)]

산업보안 강화를 위한 정책 방안을 제시한 연구를 살펴보면, 정덕영(2007)은 산업스파이와 이를 통한 기술유출 및 산업기밀관리의 실태 분석을 통해 산업보안을 위협하는 주요원인이 산업스파이임을 확인하고, 이에 대한 대응방안으로 기업의 산업보안시스템 구축, 효과적인 민관협력체계의 구축, 기술인력 관리체계의 구축, 산업보안 교육 및 전문가양성과정 운영을 제시하였다. 이훈재(2011)는 국내 산업스파이 범죄의 실태 및 대응정책의 문제점 분석과 외국의 산업스파이 범죄 대응정책의 검토를 통해 산업스파이 대응의 시급성을 식별하고, 산업스파이 대응을 위한 정책으로 관련법규 정비(산업기술 유출 처벌 강화, 소송내용의 비공개, 피해산정 방법 마련), 국가대응기관 간 공조 활성화를 위한 제도적 장치 마련, 산업기술 보안교육 및 보유주체의 보호기능 강화, 국제공조체제 확립이 필요함을 제시하였다.

노호래(2008)는 산업보안의 위협요인을 산업기술 유출범죄로 인식하고, 산업기술유출 범죄의 특성과 관련 법제도 및 사례 분석을 통해 산업기술유출 방지를 위한 정책적 대응방안으로 관련법규 정비(법률의 명확한 이원화), 기업의 산업보안활동(보안시스템구축, 계약 관계 강화, 기술인력 보상)에 대한 국가의 지원, 국가기관의 역할(경찰의 산업보안기능 강화, 국가정보원과 경찰의 사이버 산업스파이신고센터운영 활성화, 국가정보대학원 등의 산업보안 전문교육 강화, 산업보안협의회를 통한 산업체 및 유관기관 공조 강화, 중소기업청의 중소기업 산업보안 지원) 제안 등의 해결방안을 제시하였으며, 이희선(2012)도 산업보안과 관련된 기술유출 범죄 관련 이론의 고찰과 범죄 실태 분석을 통해, 기술유출 범죄 대응을 위한 법제도 장치(피해산정방안 마련, 유출범죄 형량 강화, 소송 중 영업비밀 비공개, 정부기관 역할 강화) 마련, 국가 및 기업의 산업보안인식 제고, 기업의 보안관리 감독체계 구축 및 이에 대한 국가 지원의 대응방안이 필요함을 제시하였다. 주일엽(2008)은 산업보안의 위협요인을 외국 정보기관의 인간정보활동으로 설정하고, 산업기술정보유출과 관련된 외국 정보기관의 인간정보(HUMINT) 활동 사례 분석을 통해, 국내 산업기술을 보호하기 위한 정책적 방안으로 인원보안의 중요성 인식, 인원보안의 관리수단(신원조사, 동향파악, 보안교육, 보안서약 등) 확보, 국가 정보·보안기관의 방첩능력 제고의 방안을 제시하였다.

최순호(2009)는 산업보안 활동에 있어 경찰의 역할이 중요함을 제시하며, 국내 경찰의 산업보안활동의 실태분석을 통해 경찰의 산업보안활동 활성화 및 산업보안 수사 역량 강화를 위한 정책 방안으로 경찰의 산업보안 수사 활동 강화, 사이버 산업스파이신고센터 운영/활성화, 경찰의 산업보안 전문 인력 확보를 위한 산업보안 전문교육 강화 및 외부 위탁교육 강화 등의 정책 방안을 제시하였으며, 이하섭(2012)은 국내 산업보안 실태에 대한 문헌 연구를 통해 산업보안 유출의 해결을 위한 방안으로 경찰의 산업보안 수사요원 보강/교육 강화, 산업보안 수사전문기관 통합, 경찰의 산업보안의식 변화, 민관 협조체제 구축의 산업보안 예방활동 강화 방안을 제시하였다.

노민선(2010)은 산업보안에 있어 중소기업의 문제가 심각함을 지적하며, 중소기업의 산업보안 역량에 대한 영향요인의 통계적 분석을 통해, 중소기업 지원범위의 구체화를 통한 핵심 중소기업의 산업보안 강화, 기술유출 경험 중소기업에 대한 보안컨설팅 지원을 통한 보안역량 강화, 혁신형 중소기업 인증 시 보안관리 항목의 평가지표 반영, 해외 수출·진출·기술이전 중소기업 대상 보안컨설팅·보안교육 및 실태 관리 등의 국가 대응책 마련, 국가연구개발사업 참여기업에 대한 보안조치 강화, 중소기업 CEO의 보안 인식제고를 위한 다양한 정책수단 강

터 급증하였으며, 대부분 정책 대안을 제시하는 유형이었으나 2008년부터 산업보안의 이론 소개·검증·적용에 대한 연구가 등장하고 있어, 국내 산업보안의 연구가 실무적 측면에서 학문적 영역으로 자리 잡고 있음을 밝히고 있다.

2) 학술연구정보서비스(RISS)를 통해 조회된 결과 산업보안과 관련된 선행연구 중 「산업기술의 유출방지 및 보호에 관한 법률」 등에 관한 법제도 측면의 연구가 다수 존재하나, 본 논문의 초점에서 벗어나므로 분석대상에서 제외하였다. 더불어, 산업보안과 관련된 국내 석사/박사 학위논문이 다수 존재하고 있으나, 보다 본 논문의 분석대상에서는 제외하였다.

구, 중소기업 기술유출방지 예산 확대 등을 중소기업 산업보안 역량강화를 위한 정부의 정책 방안으로 제시하였으며, 이와 유사하게 남재성(2012)도 중소기업의 산업기술 유출의 원인 및 피해 실태 분석을 통해 중소기업에 대한 산업보안문제의 심각성을 확인하고, 중소기업의 산업기밀 유출범죄 피해 감소를 위한 법제도적 방안으로 중소기업의 보안시스템 구축을 위한 국가적 차원의 지원 확대, 보안종합관제센터 등 중소기업 대상의 상시 종합적 대응 시스템 지원, 산업기술 유출 사고 수사 강화를 위한 민간조사제도 도입 및 활성화, 정부 주도형 산업기밀 유출 피해보상 보험제도 도입, 경찰, 국가정보원 등의 수사체계 강화, 산업기밀 유출 억제를 위한 기소전 몰수보전제도 활용, 중소기업 산업기술 보호를 위한 산업기술 임치제도 활성화 등을 제시하였다.

정태황(2010)은 공공기관/대기업/중소기업의 관리적 보안실태에 관한 설문조사를 통해 산업기술보호 활성화를 위한 관리적 측면의 정책적 방안으로 보안 규정, 조직문화 등 보안정책의 효과적 실행 기반 조성, 보안 활성화를 위한 보안투자 확보, 인적 측면의 관리적 산업보안 방안(인력 관리 보안의식 향상) 강화, 중요 자산의 통제/관리 강화를 위한 정책 방안 마련의 방안이 필요함을 제시하였으며, 최응렬(2011)도 첨단산업기술 보유 기업의 보호실태 자료 분석과 설문 조사를 통하여 기술 보유 기업의 보안요인과 핵심기술의 보호수준과의 관계를 통계적으로 분석하고, 국가핵심기술의 보호수준에 대한 개선방향으로 국가핵심기술에 대한 국가적 지원, 국가핵심기술에 대한 정확한 성과관리, 국가핵심기술 보호수준의 측정을 위한 최소수준 등의 기준 수립 등이 필요함을 제시하였다.

김순석(2010)은 산업기술유출의 주요 요인인 핵심인력 유출의 문제점을 분석하고, 이를 해결하기 위한 핵심인력의 관리방안으로 기업환경의 개선, 기업 내 인적 내부위협에 대한 관리적 보안대책 수립, 핵심인력 분류·보안체계·보상·관리로 구성된 핵심인력 관리시스템의 구축, 핵심인력의 양성 및 교육, 기업체와 유관기관의 공조체제 구축을 제시하였으며, 최응렬(2012)은 산업기술의 유출 경로를 분석하기 위한 전문가조사를 통해 산업기술 유출 경로를 식별하고 이를 방지를 위한 정책적 대응 방안으로 정보보호정책 수립, 정보보호기술 도입 등의 정보보호 강화, 내부구성원 인적관리 및 성과관리·보상체계 강화, 산업보안 수준의 정확한 측정, 경찰의 산업기술 유출 수사역량 강화의 방안을 제시하였다. 채정우(2012)는 국내 산업기술 유출의 사고사례 분석을 통해 산업기밀 유출요인을 분석하고 이에 대한 대응방안으로 기술매력도, 유출행위자, 보안정책, 가상 공간 통제, 물리 공간 통제의 요인으로 구성된 산업기술유출방지 관리프레임워크를 제시하였다.

김경규(2009)는 산업 보안기술 관련 수요·공급기업의 인터뷰를 통해 산업보안 기술의 요구사항을 분석하고 이를 기반으로 산업기술 유출통제/접근통제/모니터링으로 구성된 기술적 산업보안기술 체계를 설계하고, 산업기술의 개발과제로 이기종 이동저장장치 통제시스템, 산업기술 문서 통합보안 시스템, 고성능 데이터베이스 보안시스템, 역할기반 네트워크 종단 보안시스템을 설정하는 산업보안 기술개발 전략을 제시하였으며, 정덕영(2010)은 산업보안활동의 실태 및 대학 내 산업기술 유출사례 분석을 통해, 대학 내 산업보안활동의 활성화를 위한 정책방안으로 연구개발성과 보상, 보안관리 인식제고, 체계적 보안시스템 구축, 대학산업보안협의회의 활성화를 제시하였다. 최선태(2010)는 산업보안업무의 효과적 수행을 위한 산업보안 관련 전문자격을 비교하고 산업보안 전문자격 제도의 필요성을 제시하였고, 이와 함께 산업보안 전문인력 양성을 위한 국내외 산업보안 관련 교육과정을 분석하고, 국내 환경에서 요구되는 산업보안교육 프로그램 정립의 필요성을 제시하였다. 최진혁(2010)은 제도·정책 측면의 미국 산업보안 대응체계 사례 분석과 국내 산업보안의 문제점 분석을 통해 국내 산업보안에 대한 포괄적 접근과 연구를 위한 제도적 발전방안이 필요함을 논의하며, 국내 산업보안의 제도적 발전방안으로 정부부처 및 기업의 전반적인 산업보안 인식 제고, 산업보안 관련 왜곡된 이해와 편향된 투자의 교정, 국가 주도의 총체적이인 장기 산업보안 프로그램 운영, 산업보안 기능 중심의 국가 중추적 조정기관의 설립·운영, 중소기업 보안체계 확립을 위한 국가적 지원, 수요 맞춤형 산업보안 전문 인력 양성 및 다학제간 연계 연구 추진, 민관협의체 구축 등을 통한 민관 협조체제 구축의 방안을 제시하였다.

산업보안 대응의 관점에 따라 기존연구에서 제시하고 있는 산업보안 강화 방안과 그에 따른 핵심적인 내용을 정리하면 다음과 같다.

첫째, 법제도적 측면에서는 산업기술 유출 범죄에 대한 처벌의 강화와 산업기술 유출로 인한 피해의 합리적 산정 기준 마련, 소송 중 산업기술 유출 방지를 위한 비공개 규정의 보완을 제시하고 있다(이훈재, 2010; 이희선, 2012).

둘째, 국가 정책적 측면에서는 기업의 산업보안관련 보안시스템 등 보안체계 구축에 대한 국가의 지원이 제시되고 있으며(노호래, 2008; 최진혁, 2010; 남재성, 2012; 이희선, 2012; 최응렬, 2011), 경찰, 국가정보원 등 산업보안과 관련된 국가 정부기관의 역할 및 역량 강화도 제시되고 있으나(노호래, 2008; 주일엽, 2008; 최순호, 2009; 남재성, 2012; 이하섭, 2012; 최응렬, 2012), 일부 연구자들은 산업보안 관련 정부기관의 공조와 일관된 산업보안활동을 위한 담당기관의 일원화를 제시하기도 한다(이훈재, 2010; 최진혁, 2010; 이하섭, 2012). 또한 산업보안 강화를 위한 민간과 공공의 협력체계 구축도 국가정책 측면에서 공통적으로 제시되고 있다(정덕영, 2007; 김순석, 2010; 최진혁, 2010; 이하섭, 2012).

셋째, 기업의 관리적·기술적 보호조치 측면에서는 기업의 산업보안 체계 구축과(정덕영, 2007; 2010; 정태황, 2010; 이훈재, 2011; 이희선, 2012; 최응렬, 2012), 더불어 산업보안 인식제고, 보안교육, 전문인력 양성 등 인적 측면에서의 산업보안 강화 방안이(정덕영, 2007; 2010; 최선태, 2010; 이훈재, 2011; 정태황, 2010) 공통적으로 제시되고 있다.

2.2.2 중소기업 관련 산업보안 선행연구 경향

본 연구의 대상이 되는 중소기업 관련 산업보안에 대한 기존연구를 살펴보면 다음과 같다. 중소기업의 정보보호관리체계와 관련된 연구로, 김정덕(2006)은 중소기업의 정보보호 현황 분석과 전문가 설문을 기반으로 중소기업의 정보화 특성에 적합한 정보보호 관리체계를 개발, 실증적 검증을 수행하였으며, 장항배(2010)도 중소기업의 산업보안 현황 및 산업기술유출 사례 분석을 통해 중소기업의 산업보안 강화를 위한 정보보호 관리체계를 제시하고, 전문가회의를 활용한 델파이 기법을 통한 검증을 수행하였다.

중소기업의 일반적인 정보보호와 관련된 연구로, 김종기(2006)는 컴퓨터 바이러스를 중심으로 대기업과 중소기업 간 보안요소에 대한 사용자의 인지도 차이 분석을 통해 기업보안 강화를 위한 보안인지와 보안정책의 중요성을 고찰하였으며, 여상수(2009)는 중소기업의 보안사고 예방을 위해 기업의 조직, 업무, 자산, 기술의 네 가지 관점에서 보안 이슈를 분석하고 이를 기반으로 중소기업의 안정적인 정보시스템 운영을 위한 보안대책과 전략을 제시하였다. 강종구(2011)는 소규모 IT 기업의 정보보호를 위해, 소규모 IT의 특성과 핵심 정보 자산 유형을 분석 제시하였으며, 이와 유사하게 김양훈(2012)은 소규모 IT 서비스 기업의 보안관리 요구사항 분석을 통해 소규모 IT 서비스 기업의 보안대책 수립을 위한 보안관리모델을 개발, 실증 분석을 통해 기업보안 관리를 위한 추진전략을 제시하였다.

중소기업의 산업보안에 대한 정책적 방안을 제시하고 있는 보다 구연구로는, 앞서 살펴본 노민선(2010)과 남재성(2012)의 연구가 있다. 노민선(2010)은 기술유출 사고가 발생한 중소기업의 48.4%에서 사고가 재발생하며 유출기업의 59.3%가 유출 전후의 보안관리 개선여부에 변화가 없음을 근거로, 기업의 자율적인 산업보안 활동의 효과성이 낮기 때문에 정부에 의해 조율된 정책이 필요하고, 특히 취약한 보안역량을 가진 중소기업에 대해서 정부의 역할이 중요하기 때문에 이와 관련된 정부 예산 확대가 필요하고 중소기업의 보안역량 제고에 산업보안 지원 정책의 주안점을 둘 필요가 있음을 주장하며 이를 위한 다양한 정책적 방안을 제시하였다. 남재성(2012)은 그동안의 중소기업 관련 산업보안 연구가 제한적이며, 내부자 통제, 자체 보안 강화 등 기업 자체의 역량에만 초점을 두고 있음을 지적하고, 중소기업의 보안시스템 구축, 보안기술 도입에 관한 지식 부족이 중소기업 산업기술 유출의 주된 원인 중 하나이며 이를 해결하기 위한 다양한 정책적 방안을 제시하였다.

산업보안 강화를 위한 정책 방안을 제시하는 연구들에서도 중소기업의 산업보안에 대한 분석과 해결방안이 일부 다루어졌는데, 노호래(2008)는 산업기술유출 방지를 위한 정책적 대응방안 중 하나로 중소기업의 산업기술 유출 방지를 위한 중소기업청의 정책적 역할로 제시하면서, 이를 위해 산업보안 교육의 확대, 실태조사 및 대응매뉴얼 개발, 민간의 보안기술 연구개발 지원, 보안컨설팅 및 보안시스템 구축 지원이 요구됨을 제시하였으며, 정태황(2010)은 산업기술보호 활성화를 위한 관리 정책 방안의 하나로 보안정책 운영실태가 미흡한 중소기업의

보안관리 능력 보강을 위해 국가적 차원의 지원시스템 확장이 필요함을 제시하였다. 이외에도 정덕영(2007)과 이희선(2012)은 규모가 영세한 중소기업의 경우 자체 보안 관리 시스템 구축에 어려움을 겪을 수 있으므로, 핵심 기술의 보안 관리에 대한 정부의 예산 지원의 방안을 고려할 필요가 있음을 주장하였고, 최진혁(2010)은 중소기업의 산업보안 활동에 있어 재정적 환경적 제약 외에도 인식의 부족을 문제점을 분석하고 중소기업의 산업보안을 위해 정부 차원의 장려 및 체계적 지원이 시급하며, 이와 관련하여 관련 정부부처 간 분산된 지원으로 인한 비효율성과 단발성 정책의 한계를 벗어나기 위한 통일되고 일관성 있는 정책적 제도적 방안 마련과 효율적 지원이 필요함을 논의하였다.

2.2.3 기존연구와 본 연구의 차별성

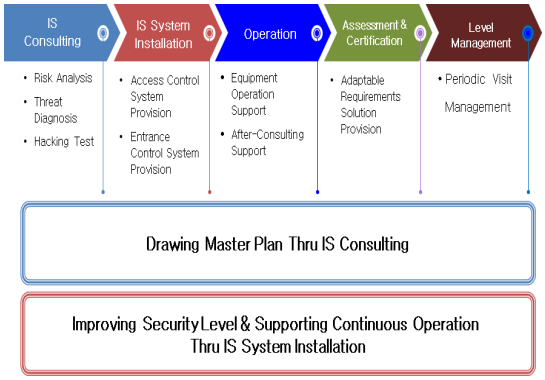
기존연구들은 각종 국내 산업보안 관련 현황에서는 산업기술 유출 중 중소기업에서 비교적 많은 사고가 발생하며 중소기업의 산업보안 수준이 턱없이 부족함을 밝히고 있다. 하지만 위에서 살펴본 바와 같이, 중소기업의 산업보안 관련 국내 선행연구는 산업보안 관련 선행연구에 비해 그 수도 적을 뿐 아니라, 내용에 있어서도 주로 기업 내 역량 강화를 중점으로 정보보호관리체계 구축, 기업 내 정보시스템의 보안정책 강화 등에 한정되고 있다. 이러한 역량 강화에 있어 국가적 지원이 필요함을 밝히고 있지만 보안교육 확대, 보안시스템/컨설팅 지원 등 일반적인 수준의 국가적 지원만을 제시하고 있어, 실질적으로 요구되는 국가 정부부처의 구체적인 지원 활동 등에 대한 연구가 이루어지지 않음을 확인할 수 있다. 이러한 기존연구의 한계를 보완하기 위해서 본 연구에서는 경기도 사례를 중심으로 사업운영 과정에서 요구되는 보다 구체적인 시사점을 제공할 수 있을 것으로 판단된다.

3. 사례개요 및 연구설계

3.1 경기도 중소기업 산업보안 사례 개요

경기도에서는 사이버공격 등 보안이슈 증가로 인해서, 개인정보보호법 대응, 60만 중소기업 산업보안 강화, 민간 보안관제 서비스 확대지원과 더불어, 중소기업 산업기술 유출 방지 및 개인 정보보호 지원 대민서비스 강화가 요구되고 있다. 이에 따라서 경기도에서는 경기도 정보보안 최고책임자(CSO)협의체 구성('12. 5), 사이버안전기업 대상 중소기업 지원(포천 킹유전자)('12. 8), 경기도·17개 보안업체 사이버안전기업 구축지원 MOU('12. 9), 사이버안전기업 구축 대상기업 보안컨설팅(김포, 안산)('12. 12), 경기도 산업보안포럼 개최(민관보안관제센터 연계 협약)('12. 12) 등과 같은 지속적인 노력을 추진중에 있다(경기도, 2012a; 2012b; 2012c; 2012d; 2012e; 2013).

첫째, 경기도 CSO협의회를 통해 선정된 중소기업을 대상으로 개인정보보호 및 산업보안에 대한 취약점 진단 및 컨설팅을 통해 현장에 필요한 보안장비 및 솔루션을 기부하여 중소기업의 개인정보보호 및 산업보안에 대한 정보보호 의식 고취와 기업의 중요 데이터를 보호하게 함으로써, 경쟁력 있는 중소기업을 육성 발전시키는 프로그램이다. 사이버 안전기업 구축 프로세스는 <그림 2>와 같이 5단계에 거쳐 진행되며, 개인정보보호법 위반에 따른 불이익 감소 및 예방, 출입통제 시스템을 통한 외부 위험 대응, 자동화 시스템을 통한 불필요한 경비 및 인력 비용 감소, 중소기업 전반의 보안강화 도모 및 업무효율성 증대를 추구할 것으로 기대하고 있다.



[Fig. 2] Construction for cyber security businesses

둘째, 산업보안관리센터(단국대) 및 통합보안관제센터(경기대) 구축은 전산망·인터넷 등에 의한 기술자료 유출 감시, PC 서버 등에 대한 바이러스 감염 사전차단 등 토탈 관제서비스 제공(예방·탐지·분석·대응)하는 프로그램으로 '12.3~9월까지 기반시설을 구축하고 '12년 10월부터 정식서비스를 제공하고 있다. 특히, 보안관제서비스,

내부정보유출 방지, 홈페이지 관제, 시스템 관제, 네트워크 관제, 보안수준 점검, 이상징후 분석 등 다양한 서비스를 제공하며, 향후 발전을 위해서 융합보안 관제체계 수립, 모바일 보안관제 실시, 내부정보유출방지, 관제센터 인프라 구축, 서비스 운영절차 확립 등의 다양한 전략을 중장기적으로 실시할 계획이다.

3.2 연구설계 및 조사 방법

본 연구에서는 경기도 중소기업 중 명단이 확보된 770여개 가운데 조직의 대표 또는 실무진을 대상으로 2013년 4월 1일부터 5월 31일까지 약 2개월간 직접 설문조사를 실시하였다. 이 가운데 설문조사에 불성실하게 응답한 표본을 제외하고 49개의 중소기업의 산업보안 담당자에 대한 자료를 최종적으로 분석에 활용하였다.

경기도의 사업추진 내부자료와 기존연구 들의 핵심적인 내용을 참조하여 산업보안 강화 프로그램에 대한 인지도, 운영상 다양한 측면에 대한 중요도, 프로그램 대상 여부, 프로그램의 필요성, 향후 기대효과, 전반적인 만족도 및 확대의사, 향후 계획의 상대적 중요도, 프로그램 운영의 문제점과 활성화 방안 등 다양한 문항을 조사하였으며, 주로 1-5점 척도방식(해당 수치가 높을수록 긍정적으로 인식)으로 진행하였다. 실증분석을 위해서 정확성을 검증하고 SPSS 21.0과 EXCEL 2010 프로그램을 활용하여 분석하였다.

〈Table 1〉 Status of sample

		Frequency (person)	Percent (%)
Gender	Male	39	86.7
	Female	6	13.3
	Total	45	100.0
	Missing data	4	
Education level	Less than high school	1	2.2
	College graduates	8	17.8
	4-year college graduates	29	64.4
	Master degree or higher	7	15.6
	Total	45	100.0
	Missing data	4	
Ages	Less than 20s	3	6.7
	30s	11	24.4
	40s	20	44.4
	50s or older	11	24.4
	Total	45	100.0
	Missing data	4	
Position	Employee	4	8.9
	Assistant manager	5	11.1
	Team manager	8	17.8
	Section chief	20	44.4
	Head of department	5	11.1
	Director	3	6.7
	Total	45	100.0
	Missing data	4	
Seniority	Less than 1 year	1	2.2
	1 year ~ 5 years	11	24.4
	5 years ~ 10 years	5	11.1
	10 years ~ 15 years	9	20.0
	More than 15 years	19	42.2
	Total	45	100.0
	Missing data	4	
Total		49	

4. 분석결과 및 해석

4.1 표본의 현황

분석에 활용된 표본은 49개로, 표본의 주요 현황을 살펴보면 <Table 1>과 같다. 각각의 주요 특성별로 살펴보면 성별의 경우 남자(86.7%)가 많은 비중을 차지하고 있으며, 학력수준은 주로 4년제 대졸자(64.4%)에 해당되는 비중이 가장 많았다. 연령대는 주로 30대부터 50대이상 사이에 많이 분포하였으며, 40대(44.4%)가 가장 많은 비중을 차지하였다. 직급은 과장급(44.4%)이 가장 많았으며, 근속기간은 15년 이상(42.2%)의 비중이 가장 높은 것으로 나타났다. 결과적으로 각 중소기업별로 조직의 전반적인 사항을 잘 아는 대표자 또는 경력이 오래된 상위직급의 실무진이 조사에 응답한 것으로 판단된다.

4.2 경기도 산업보안 사례 인지도 및 운영측면 분석

<Table 2>는 경기도 산업보안 프로그램에 대한 인지도를 분석한 것이다. 경기도 “중소기업 산업기술 유출방지를 위한 산업보안 강화 프로그램 운영”에 대한 인지도는 보통(평균=3)인데 반해서, 세부적인 사이버안전기업 구축 프로그램(평균=2.62)과 산업보안관리센터(단국대) 및 통합보안관제센터(경기대) 프로그램(평균=2.61)에 대한 인지도는 보통보다 낮은 수준임을 알 수 있다. 이러한 결과는, 경기도의 중소기업들이 산업보안 프로그램에 대해서 잘 인지하지 못하고 있음을 보여주며, 해당 프로그램에 대한 홍보노력이 필요함을 시사한다.

〈Table 2〉 Awareness about Gyeonggido industrial security program

	N	Average	Standard deviation
The awareness for program about strengthen of industry security in SME	49	3.00	1.19
The awareness for construction for cyber security businesses	47	2.62	1.05
The awareness for industry security management center and integrated security control centers	49	2.61	1.02

<Table 3>은 경기도 산업보안 프로그램의 다양한 운영측면에서의 상대적 중요도를 분석한 것이다. 즉, 법제도, 조직 및 인력, 재정, 거버넌스 측면에서의 현재수준과 향후 수준에 대한 상대적 중요도를 분석한 것으로, 대체로 보통(3점)이상의 평균을 보이고 있으며, 현재수준과 향후수준의 상대적인 차이는 통계적으로 유의미한 것을 알 수 있다. 현재수준에서는 재정적 측면에 중요도가 가장 높으며(평균=3.17), 조직 및 인력 측면에 중요도가 가장 낮은(평균=3.04)은 반면에, 향후 수준에서는 조직 및 인력적 측면의 중요도가 가장 높고(평균=4.05) 재정적 측면과 법제도적 측면의 중요도가 가장 낮은(평균-3.93)은 것으로 나타났다. 결과적으로 향후수준과 현재수준의 상대적 차이를 고려할 때, 조직 및 인력적 측면(평균=1.00), 거버넌스적 측면(평균=0.85), 법제도적 측면(평균=0.80), 재정적 측면(평균=0.76)의 순으로 상대적 중요도를 우선순위를 고려할 필요가 있음을 잘 보여준다.

〈Table 3〉 Importance of the Gyeonggido industrial security program operating aspects

	N	Present		Hereafter		Gqp (Hereafter - Preswent)	
		Avg	Std dev	Avg	Std dev	Avg	p -value
Legal system	46	3.13	1.02	3.93	1.21	0.80	0.00
Organization and HR	46	3.04	1.15	4.05	1.18	1.00	0.00
Finance	46	3.17	1.04	3.93	1.00	0.76	0.00
Governance	46	3.13	0.93	3.98	0.98	0.85	0.00

4.3 사이버안전 기업 구축, 산업보안관리센터 및 통합보안관제센터 프로그램에 대한 분석

<Table 4>는 경기도 산업보안 프로그램의 지원여부를 분석한 것이다. 즉, 조사에 응답한 중소기업들이 사이버안전기업 구축 프로그램 또는 산업보안관리센터(단국대) 및 통합보안관제센터(경기대)에 해당여부를 잘 보여준다.

사이버안전기업 구축 프로그램의 지원을 받은 경험이 있는 중소기업 표본은 6.5%로 거의 소수에 해당된다. 실제로 사이버안전 기업 구축에는 참여한 기관은 14개로 소수에 해당된다. 따라서, 본 프로그램이 경기도 내 중소기업의 적극적인 참여를 전제로 한다는 점에서 홍보와 참여유도가 핵심이 되는 것으로 판단된다.

한편, 산업보안관리센터(단국대) 및 통합보안관제센터(경기대) 프로그램의 경우 53.2%를 제외하고 나머지 중소기업이 대상이 되는 것으로 나타났으며, 둘다 대상(21.3%), 통합보안관제센터(경기대)(19.1%), 산업보안관리센터(단국대)(6.4%)의 순으로 나타났다.

〈Table 4〉 The availability of Gyeonggido industrial security program support

		Frequency (person)	Percent (%)
The availability of industrial security program support	No	44	93.6
	Yes	3	6.4
	Total	47	100.0
	Missing data	2	
The presence of industry security management center's target and integrated security control centers's target	No	25	53.2
	Industry security management center	3	6.4
	Integrated security control centers	9	19.1
	Both	10	21.3
	Total	47	100.0
	Missing data	2	
Total		49	

<Table 5>는 경기도 사이버안전 기업 구축 프로그램의 세부 단계별 필요성에 대한 분석결과이다. 필요성에 대한 응답은 보통(3점)과 그렇다(4점) 사이에 주로 분포하고 있으며, 상대적으로 정보보호컨설팅_위험분석(평균

=3.98), 정보보호컨설팅_취약점 진단(평균=3.98)에 대한 필요성이 가장 높으며, 그 다음으로는 운용_추후 컨설팅 지원(평균=3.94), 수준관리_정기적 방문관리(평균=3.94) 등의 순으로 나타났다. 한편, 상대적 필요성이 가장 낮은 단계는 정보보호시스템 설치_출입통제 시스템 제공(평균=3.79)임을 알 수 있다. 이러한 경기도 사이버안전 기업 구축 프로그램의 세부 단계별 필요성의 수요를 고려하여 향후 프로그램의 서비스 공급 등을 방향을 조정하는 전략이 요구되는 것으로 판단된다.

〈Table 5〉 The need for detailed step of construction program for cyber security businesses in gyeonggido

		N	Average	Standard deviation
Information security consulting	Risk analysis	47	3.98	0.79
	Vulnerability diagnosis	47	3.98	0.77
	Simulation hacking	47	3.81	0.77
Information security system installation	Provision of access control system	47	3.81	1.01
	Provision of entry access control system	47	3.79	1.08
Operation	Support of equipment management	47	3.85	0.83
	Support of after consulting	47	3.94	0.87
Evaluation and certification	Provision of adapted solution for requirements	47	3.91	0.97
Level management	Periodic visit management	47	3.94	0.92

<Table 6>은 경기도 사이버안전 기업 구축 프로그램의 세부 예상 효과에 대한 인식을 분석한 것이다. 응답은 보통(3점)과 그렇다(4점) 사이에 주로 분포하고 있으며, 상대적으로 산업보안 강화(평균=3.88)에 대한 인식이 가장 높으며, 그 다음으로는 개인정보 보안(평균=3.86), 업무 효율성 증가(평균=3.61), 비용 절감(평균=3.31)의 순으로 나타났다. 결과적으로 산업보안 강화(출입통제 시스템을 통한 외부 위험에서 대응)가 가장 효과적이며, 상대적으로 비용 절감(자동화 시스템을 통한 불필요한 경비 및 인력 감소)이 가장 효과적이지 않은 것으로 중소기업 실무진은 인식하고 있음을 잘 보여준다.

〈Table 6〉 Details expected effect of construction program for cyber security businesses in gyeonggido

	N	Average	Standard deviation
Personal information security	49	3.86	0.84
The strengthen of industry security	49	3.88	0.86
Cost reduction	49	3.31	0.96
Increase in business efficiency	49	3.61	0.89

<Table 7>은 경기도 산업보안관리 센터 및 통합보안 관제센터 프로그램의 서비스 필요성에 대한 인식을 분석한 것이다. 응답은 보통(3점)과 그렇다(4점) 사이에 주로 분포하고 있으며, 상대적으로 내부정보유출 방지(평균=3.83), 보안수준 점검(평균=3.83)이 가장 필요하다고 인식하고 있으며, 반면에 홈페이지 관제(평균=3.67), 시스템 관제(평균=3.67)이 상대적으로 필요성이 낮은 것으로 인식하고 있었다. 결과적으로 내부정보유출 방지(온라인 및 이동형 저장매체를 통한 핵심기술유출 시도를 실시간으로 감시), 보안수준 점검(중소기업들의 보안취약점 파악을 우한 전산장비 점검, 악성 코드 탐지 등 현장 조사)이 가장 핵심적인 서비스임을 시사하고 있다.

〈Table 7〉 The need for gyeonggido industry security management center and integrated security control center program

	N	Average	Standard deviation
Service related security	46	3.72	0.91
Prevention of the leaking of internal information	46	3.83	0.88
Homepage control	46	3.67	0.87
System control	46	3.67	0.79
Network control	46	3.72	0.75
Check the security level	46	3.83	0.82
Analysis of symptom	46	3.78	0.79

<Table 8>은 경기도 산업보안관리 센터 및 통합보안 관제센터 프로그램의 향후 발전을 위한 중요도를 분석한 것이다. 대체로 보통(3점)이상의 평균을 보이고 있으며, 현재수준과 향후수준의 상대적인 차이는 통계적으로 유의미한 것을 알 수 있다. 현재수준에서는 내부정보유출방지 서비스 실시(평균=3.55)가 가장 중요하며, 모바일 보안관제 실시(평균=3.26)이 가장 중요도가 낮은 것으로 나타났다. 반면에, 향후 수준에서는 내부정보유출방지 서비스 실시(평균=4.09)가 가장 중요한 것으로 인식하고 있으며, 관제센터 인프라 구축(평균=3.91)을 가장 중요도가 낮게 인식하고 있음을 알 수 있다. 결과적으로 향후 수준과 현재수준의 상대적 차이를 고려할 때, 서비스 운영절차 확립(평균=0.76)이 가장 중요하며, 융합보안 관제체계 수립(평균=0.43)이 상대적 중요도가 가장 낮은 것으로 분석되었다.

〈Table 8〉 Importance for the future development about gyeonggido industry security management center and integrated security control center program

	N	Present		Hereafter		Gap (Hereafter - Present)	
		Average	Standard deviation	Average	Standard deviation	Average	p-value
Establishment of convergency security control system	46	3.52	1.01	3.96	1.07	0.43	0.00
Implementation of mobile security control	47	3.26	1.01	3.98	1.13	0.72	0.00
Implementation of service for prevent the leaking of internal information	47	3.55	1.08	4.09	1.02	0.53	0.00
Control center construction of infrastructure	47	3.30	0.98	3.91	1.04	0.62	0.00
Establishment of service operation procedure	46	3.28	0.98	4.04	0.94	0.76	0.00

4.4 전반적 평가 및 향후 수요에 대한 분석

<Table 9>는 경기도 산업보안 프로그램에 대한 전반적 만족도와 확대의사를 분석한 것이다. 대체로 보통(3점)이상의 평균을 보이고 있어 전반적 만족도와 확대의사가 높은 편임을 알 수 있다.

〈Table 9〉 Overall satisfaction levels and intention to expand about gyeonggido industry security program

	N	Average	Standard deviation
Overall satisfaction	46	3.57	1.03
The need for expanding	49	4.02	0.78

〈Table 10〉 The relative importance about future plans of gyeonggido industry security program

	N	Present		Hereafter		Gap (Hereafter - Present)	
		Average	Standard deviation	Average	Standard deviation	Average	p-value
Academic publication	45	3.33	0.88	3.80	0.92	0.47	0.00
Liaison between MOU	45	3.44	0.81	3.93	0.84	0.49	0.00
Support of private security service	45	3.58	0.87	3.89	0.98	0.31	0.01
Support of handling a problem and difficulties technique	45	3.62	0.89	3.98	0.94	0.36	0.00
Study on management system	45	3.49	0.94	4.07	0.86	0.58	0.00
Operation of supporting program	45	3.58	0.84	4.07	0.86	0.49	0.00
construction of security industry cluster	45	3.47	0.87	3.96	0.88	0.49	0.00

<Table 10>은 경기도 산업보안 프로그램 향후 계획

에 대한 상대적 중요도를 분석한 것이다. 대체로 보통(3점)이상의 평균을 보이고 있으며, 현재수준과 향후수준의 상대적인 차이는 통계적으로 유의미한 것을 알 수 있다. 현재수준에서는 도내 중소기업의 산업기술 유출신고, 국정원연계 사고처리 및 애로기술 지원(평균=3.62)이 가장 중요하며, 사이버안전기업 Before & After 사례 발표, 정보보호 자문교수단 학술발표 등(평균=3.33)이 가장 중요도가 낮은 것으로 나타났다. 반면에, 향후 수준에서는 사이버안전기업 확산위한 지원 프로그램 운영(장비지원, 기업인증, 지원연계)(평균=4.07), 중소기업 지원 사이버안전기업 관리체계 연구용(평균=4.07)가 가장 중요한 것으로 인식하고 있으며, 사이버안전기업 Before & After 사례 발표, 정보보호 자문교수단 학술발표 등(평균=3.80)을 가장 중요도가 낮게 인식하고 있었다. 결과적으로 향후수준과 현재수준의 상대적 차이를 고려할 때, 중소기업 지원 사이버안전기업 관리체계 연구용(평균=0.58)을 우선적으로 고려할 필요가 있음을 잘 보여준다.

4.5 정보보호 서비스 수요에 대한 분석결과

<Table 11>은 경기도 산업보안 프로그램의 정보보호 서비스의 수요를 분석한 결과이다. 「개인정보보보호법」 제33조 제1항 및 「개인정보보보호법」 시행령 제35조 상의 개인정보 영향평가 대상에 해당되는 기관은 52.2%로 과반수 이상이며, 향후 1~2년 내 「개인정보보보호법」 제33조 제1항 및 「개인정보보보호법」 시행령 제35조 상의 개인정보 영향평가 대상에 해당된다는 표본도 54.3%(그렇다 32.6% + 매우 그렇다 21.7%)로 과반수 이상에 해당된다.

한편, 산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따라 지정된 국가핵심기술을 보유한 기관도 52.2%로 과반수 이상이며, 보유한 기술은 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따라 지정된 국가핵심기술은 아니지만, 그에 해당하는 가치있는 기술로서 보호되어야 한다는 항목에서도 57.4%가 긍정적으로 응답하였다. 더불어, 산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따라 지정된 국가핵심기술을 보유한 기업과 함께 업무수행여부에 대해서도 그렇다는 응답이 52.2%로 과반수 이상에 해당됨을 알 수 있다.

결과적으로 분석에 포함된 중소기업 담당자의 정보보호 서비스 수요는 상당히 높으며, 이에 따라서 경기도의 산업보안 정책도 중장기적으로 보다 수요대응적인 관점에서 활성화될 필요가 있을 것으로 보여진다.

〈Table 11〉 Demand for information security service of gyeonggido industry security program

		Frequency (person)	Percent (%)
The presence of privacy impact assessment's target	Disagree	22	47.8
	Agree	24	52.2
	Total	46	100.0
	Missing Data	3	
The possibility for becoming target on the privacy impact assessment	Strongly Disagree	3	6.5
	Disagree	6	13.0
	Neutral	12	26.1
	Agree	15	32.6
	Strongly Agree	10	21.7
	Total	46	100.0
	Missing Data	3	
The presence of national core technology	Disagree	22	47.8
	Agree	24	52.2
	Total	46	100.0
	Missing Data	3	
The need to protect technology in retention	Strongly Disagree	3	6.5
	Disagree	3	6.5
	Neutral	9	19.6
	Agree	16	34.8
	Strongly Agree	15	32.6
	Total	46	100.0
	Missing Data	3	
Whether perform business with other companies	Disagree	22	47.8
	Agree	24	52.2
	Total	46	100.0
	Missing Data	3	
Total		49	

5. 결론

5.1 요약 및 시사점 논의

본 연구는 중소기업 산업보안 강화를 위해서 지방정부에 해야 할 역할에 대해서 경기도 사례를 중심으로 분

석하였다. 특히, 경기도가 해당 지역의 중소기업 산업보안 강화를 위해 추진하고 있는 다양한 사업(사이버안전기업 구축 및 민관보안관제센터 활성화 등)에 대해서 중소기업의 담당자를 대상으로 다양한 측면에서 분석 및 평가함으로써, 향후 이러한 수요에 맞게 경기도가 담당해야할 역할이 무엇인지를 탐색해보는데 초점을 두었다.

경기도 산업보안 프로그램에 대한 중소기업의 인지도는 상대적으로 낮은 반면에, 해당 서비스에 대한 필요성, 기대효과 등은 상당히 높은 것으로 나타났다. 특히, 정보보호 수요가 증대될 가능성이 높은 시점에서 중장기적인 단계별 우선순위를 고려한 경기도의 역할은 매우 중요할 것으로 판단된다. 따라서 본 연구결과를 바탕으로 향후 경기도 산업보안 강화 프로그램 운영을 확대 및 활성화하기 위해서는 다음과 같은 방안이 모색될 필요가 있을 것이다.

첫째, 정보화 사회에서 기업의 산업재산권 및 기술 관련하여 외부 유출 등 산업보안의 중요성이 대두됨에 있는 상황에서 중소기업의 인력, 비용, 정보 등은 많이 부족한 실정이다. 따라서, 산업보안에 대한 인식의 필요성과 사전적인 예방을 위해서 운영에 대한 홍보를 강화할 필요가 있다. 실제 정보보안의 중요성은 아무리 강조해도 끝이 없은 상황이나, 중소기업에서 필요성을 느끼는 만큼 관련된 사업이나 지원을 알 수 있도록 하는 홍보전략은 많이 부족한 실정이다. 따라서, 지방정부 수준에서 중소기업은 정보보안의 필요성을 인지하고 관련된 사업에 참여할 수 있도록 하는 홍보함으로써, 자체적으로 해결하지 못하는 문제에 지원을 해야 할 것이다.

둘째, IT산업의 활성화가 이루어지고 있는 현 시점에서 중소기업의 필수요소인 비용 등에 재투자가 이루어지고 있는 실정이며, 현실적으로 악성 바이러스 및 무분별한 보안 프로그램의 설치제한 및 필터링 등의 상황속에서 중소기업은 자체적 산업보안 강화에 대해서는 대책이 없는 실정이다. 이러한 측면에서 중소기업의 다양한 측면의 수요, 필요한 서비스, 향후 단계별 우선순위 등을 고려한 차등적인 서비스를 지방정부가 중앙정부 및 대기업과 연계하여 지원할 수 있도록 하는 노력이 필요하다. 특히, 보안과 관련된 막연한 설명이 아니라 컨설팅을 통한 각 중소기업에 맞는 자세한 구성과 CEO 등의 인식을 재고시킬 수 있도록 해야 할 것이다.

5.2 연구의 한계와 후속연구의 방향

본 연구는 방법론상에서 다음과 같은 한계를 가질 수 있어 향후 해석상의 주의와 추가적인 보완 연구 등이 이루어져야 한다.

본 연구의 방법론적 측면에서 경기도 사례에 대해 일부 중소기업만을 대상으로 조사한 결과라는 점에서 이를 모든 지방정부에 일반화하기에는 어려움이 존재한다. 특히, 본 연구는 인과관계를 파악하기 보다는 전체적인 측면에서 경기도 사례에 대한 산업보안의 실태를 다양하게 분석하는데 초점을 두고 있다. 따라서, 일차적으로 경기도 내의 중소기업에 대한 정보구축을 통해 보다 충분한 표본을 확보하여 다양한 측면에 심층적인 연구가 이루어질 필요가 있다. 나아가, 중장기적으로는 다른 지방정부의 외생적, 내생적 환경과 수요를 반영하여 추가적인 연구가 이루어질 필요가 있다.

한편, 본 연구에서 활용한 양적인 방법론이 가지는 근본적인 한계를 보완하기 위해서 중소기업 담당자에 대한 심층적인 인터뷰나 관련 분야 전문가를 대상으로 한 조사 등을 통해서 보완적인 연구가 이루어질 필요가 있다. 특히, 본 연구는 전체적인 측면에서 경기도에 대한 개괄적인 실태를 파악하는 수준에서 이루어진 연구라는 점에서, 보다 구체적인 시사점을 제공하기 위해서는 반드시 후속연구를 통한 보완이 필요할 것이다.

ACKNOWLEDGMENTS

This research was supported by s grant from the Information Security Expert Course in Knowledge Information Security (NIPA-H2102-13-1002) sponsored by 'Ministry of Science ICT and Future Planning' and 'National IT Industry Promotion Agency'

REFERENCES

[1] Gyeonggi-do, Introduction to gyeonggi-do industry security management center, Inside data, 2012a

[2] Gyeonggi-do, Introduction to cyber security business program, Gyeonggi-do of chief security

officers's inside data, 2012b
[3] Gyeonggi-do, Guidance on prevention and protection of national core technology, Inside data, 2012c
[4] Gyeonggi-do, Gyeonggi-do hold prevention of small and medium-sized businesses's industrial technology industry security forum, The press release, 2012d
[5] Gyeonggi-do, The construction case of cyber security business, Gyeonggi-do of chief security officers's presentation material, 2012e
[6] Gyeonggi-do, The plan for private information security governance and strengthen of industry security, Gyeonggi-do Inside data, 2013
[7] Joon-cheol Koh, Tae-soo Kim, Yong-ma Joo, Woo-hyun Kim, Kyung-sik Kang, A study of asset and risk assessment for established of industrial security management system, Applied Journal of the Korea safety management & science, Vol. 12, No. 4, pp. 1-11, 2010
[8] National intelligence service, A business guide of industry security, 2002
[9] National intelligence service, The theory and practice for industry security, The series of National intelligence service industiral secret protection center, 2008
[10] Kyung-kyu Kim, Seo-yun Chou, Sung-hye Hur, Exploratory study on R&D strategies industrial technology security, Applied Journal of Korea navigation institute, Vol. 13, No. 1 pp. 120-125, 2009
[11] Soon-seok Kim, Jae-chul Shin, The plans for core personnel management to prevent industrial technology leakage, Applied Korena security science review, No. 25, pp. 109-130, 2010
[12] Yang-hoon Kim, Young-sub Na, Hang-bae Chang, A study on information security reference model considering business process charateristics for samll IT service, Applied information systems review, Vol. 14, No. 3, pp. 131-141, 2012
[13] Jong-gu Kang, Jae-hwan Lim, Hong-joo Lee, Hang-bae Chang, A study on classification of information asset considering business process characteristics for small IT service organization, Apllied Journal of society for e-business studies, Vol. 106, No. 4, pp. 97-108, 2011
[14] Jung-duk Kim, Hang-bae Chang, Sung-yui Ryoo, Astudy of information security management system for small and medium enterprises, Appliedthe The korean association of small business studies, Vol. 28, No. 2, pp. 267-294, 2006
[15] Jong-ki Kim, Jin-hwan Jeon, Comparison of users' perception of information security elements on computer virus between large and small-and-medium companies, Appied Korea institute of information security and cryptology, Vol. 16, No. 5, pp. 79-92, 2006
[16] Jea-sung Nam, Actual condition of damage of industrial secrets leakage crime and its measures at small or medium sized business -Focusing on legal, systematic methods, Applied Korean academy of public safety and criminal justice, Vol. 46, pp. 45-75, 2012
[17] Mean-sun Noh, Sam-uel Lee, Explaning industrial security of SMEs in korea : An ordered logit analysis, Applied Public administration of korea, Vol. 44, No. 3, pp. 239-259, 2010
[18] Ho-rae Roh, A study on the countermeasure of industrial technology outflow, Applied Korean academy of public safety and criminal justice, Vol. 30, pp. 47-77, 2008
[19] Byung-seol, Min, A study of the establishment of the industrial security system, Ph.D. dissertation, Kyung-Hee University, 2002.
[20] Sang-soo Yeo, Su-chul Hwang, A safe operating strategy for information system of small and medium enterprise, Appied Journal of the korea society of computer and information, Vol. 14, No. 7, pp. 105-112, 2009
[21] Joon-bok Lee, A legal study on the protection of industrial techonology in corporate mergers and acquisitions(M&A), Appied World constitutional law review, Vol. 15, No. 3, pp. 295-324, 2009

[22] Chang-mu Lee, Conceptual research and the definition of industry security, Applied Korean society of safety, Vol. 2, No. 1, pp. 73-90, 2011

[23] Ha-sub Lee, A study on the activation plan of industry security by police, Applied Institute of police science, Vol. 7, No. 1, pp. 39-67, 2012

[24] Hun-jae Lee, A study on the situation of industiral espionage and improvement of related polices, Applied Institute of police science, Vol. 6, No. 1, pp. 179-202, 2011

[25] Hee-sun Lee, A study on counter-measures on the technology leakage crimes an their enhancement, Applied The korean society of private security, Vol. 11, No. 2, pp. 283-301, 2012

[26] Hang-bae Chang, The design of information security management system for SMEs industry technique leakage prevention, Applied Journal of korea multimedia society, Vol 13, No. 1, pp. 111-121, 2010

[27] Duke-young Jeong, Byung-soo Jung, Revitalization solutions for industrial security activities in universities, Applied The journal of the korea contents association, Vol. 10, No. 5, pp. 314-324, 2010

[28] Byeng-su Jeong, Sang-li Rye, Hwa-su Kim, Analysis of research trends in industrial security: cConcentrated on academic research information service (Year 2000 ~ 2011), Applied Journal of korean public police and security studies, Vol. 9, No. 2, pp. 195-215, 2012

[29] Jin-hong Jeong, Industry security in business, National information school, 2006

[30] Tea-hwang, Jung, Hang-bae Chang, Applied A study on the real condition and the improvement directions for the protection of industrial technology, Applied Korean security science review, No. 24, pp. 147-1701, 2010

[31] Il-yeob Joo, A research on the industry Technology protection way against foreign secret service's HUMINT activity, Appied Korean security science review, No. 17, pp. 317-336, 2008

[32] Jeong-woo Chae, Young-hee Ko, Exploring case study on security factors and strategy to precent leakage of corporate information for CEO, Applied The journal of professional management, Vol. 15, No. 1, pp. 87-113, 2012

[33] Seon-tae Choi, 21st century industy security: Global business and business security, Jinyoung Press, 2009

[34] Sun-tae Choi, A study on vocational qualification systems in the industrial security, Appied The korean association of police science review, Vol. 12, No. 4, pp. 221-255, 2010

[35] Sun-tae, Choi, Hyeong-chang, Yu, A study on the establishment of industrial security education programs in korea, Applied, Korean security science review, No. 25, pp. 185-208, 2010

[36] Sonn-ho, Choi, Woo-li, Jung, A review of enhancing industrial security policing, Appied The korean association of police science review, Vol. 11, No. 1, pp. 227-252, 2009

[37] Eung-ryul Choi, Yong-li, Rhee, Bong-gyu, song, Study about the relationship between the protective level of vational core technology and security factors, Applied Korean academy of public safety and criminal justice, Vol. 44, pp. 365-413, 2011

[38] Eun-rhul Choi, Bong-gui Song, Young-li Lee, Kyung-min Park, A study on the leaking channels of industrial technology, Applied Reasherch police science, Vol. 26, No. 1, pp. 225-259, 2012

[39] Justin Jin-hyuk, Choi, A study on the institutional improvement directions of industrial security program: Focused upon policies and practives in the U.S., Applied Korean security science review, No. 22, pp. 197-230, 2010

[40] Jin-hyuk, Choi, Jun-Seok Park, An empirical study on the recognition of CPTED strategy's usefulness to enhance the effectiveness in industrial security, Appied The korean association of police science review, Vol. 12, No. 2, pp. 283-320, 2010

[41] Industry security, The korea association for industrial security, Parkyoung Press, 2011

박 태 형(Tae-Hyoung Park)

- 2002년 2월 : 고려대학교 서양사학(행정학부전공)(학사)
- 2004년 2월 : 고려대학교 행정학(석사)
- 2011년 2월 : 고려대학교 정보보호대학원 정보보호공학(정보보호정책 전공)(박사)
- 2011년 3월~ 현재 : 고려대학교 정보보호대학원 연구교수
- 2013년 3월~ 현재 : 고려대학교 사이버국방연구센터
- 관심분야 : 정보보호정책, 성과평가, 사이버국방, 방위사업
- E-Mail : mosto2004@korea.ac.kr

임 채 홍(Chae-Hong Lim)

- 2003년 2월 : 광운대학교 행정학(경영학 부전공)(학사)
- 2005년 2월 : 고려대학교 행정학(계량행정)(석사)
- 2008년 8월 : 고려대학교 행정학(정책분석평가)(박사수료)
- 2008년 9월~ 현재 : 고려대학교 정부학연구소 연구원
- 관심분야 : 정책분석평가(과학기술정책, 정보화정책 등), 계량분석 및 방법론
- E-Mail : dlacoghd@hanmail.net

이 기 오(Kee-O Lee)

- 2000년 2월 : 숭실대학교 컴퓨터공학(공학박사)
- 2008년 11월~2011년 1월 : 유비즈텍 대표
- 2009년 3월~2011년 1월 : 숭실대학교 컴퓨터공학과 겸임교수
- 2011년 1월~현재 : 경기도청 정보통신보안담당관 정보보호팀장
- 관심분야 : 융합·산업보안 정책 및 거버넌스, 정보보안서비스(SaaS), IT 보안컨설팅(ISO27001) 및 컴플라이언스
- E-Mail : koleesys@hotmail.com

임 종 인(Jong-In Lim)

- 1980년 2월 : 고려대학교 수학(학사)
- 1982년 2월 : 고려대학교 수학(석사)
- 1986년 2월 : 고려대학교 수학(박사)
- 1986년 3월~ 현재 : 고려대학교 교수/정보보호대학원장
- 관심분야 : 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등
- E-Mail : jilim@korea.ac.kr