한국경호경비학회 – 제42호(2015): 155–178
투고일 2015. 01. 31, 심사일 2015. 02. 25, 게재확정일 2015. 03. 23

# 산업보안 지원 정책 결정의 우선 순위
## – 기업 수요와 효율성을 중심으로 –

김 창 호·유 재 환

# 산업보안 지원 정책 결정의 우선 순위 - 기업 수요와 효율성을 중심으로 -

김창호*·유재환**


## 〈요 약〉

본 연구는 산업보안의 주체인 기업을 대상으로, 기업의 기밀 보호를 위한 정부 정책의 우선 순위가 무엇인지, 산업보안을 위한 정부 지원 규모의 확대가 필요한지를 조사하였다. 우선 순위를 결정하는데 있어 기밀 보호와 관련된 기업, 개인, 사회, 정부 등의 의견과 입장을 모두 고려해야 할 것이나, 산업보안 특히 기밀 보호의 주체, 기밀 보호 정책의 수혜자, 수요자로 가장 중요하고 직접적인 당사자인 기업이 요구하는 것들이 지원 정책 결정의 기초가 될 수 있을 것으로 보았다.

이에 따라, 우리나라 기업의 보안 부서 근무자 또는 보안 담당자에게 설문지 발송을 통해 회수된 설문지중 유효한 것으로 판단된 50개를 분석하였으며, '교육 및 인력육성(On/Off-Line) 지원 강화,' '보안관련 관리 및 대책수립,' '자격/검정제도를 통한 보안전문가 위상 강화'가 기업의 기밀(고객 개인정보 포함) 보호를 위해 정부차원에서 가장 우선적으로 지원해야 할 정책 방향 1, 2, 3 순위로 조사되었다. 산업보안을 위한 정부 지원의 확대가 필요한지에 대해서는 조사 대상자 모두 필요하다고 응답하였다.


**주제어 : 산업보안, 기업 기밀, 지원 정책 우선순위, 보안 교육, 보안 인력 육성, 보안 관리, 보안 대책, 보안 자격/검정 제도**

* 경기대학교 경호보안학과 교수
** 경기대학교 경호보안학과
*** 본 연구는 2013학년도 학습연구비 (교내연구) 과제 지원에 의하여 수행되었음

목 차



# Ⅰ. 서 론

기업[1]의 기밀은 기업의 지속적인 영업 또는 수익 활동, 기업의 존속, 발전을 위해 보호되어야 할 기업의 중요한 자산이다. 기업의 기밀은 기밀 보호로 인한 이익을 얻게 되는 직접 당사자인 기업이 보호해야 한다. 기업은 기밀 보호를 위해 스스로 보안 정책을 수립하고, 수립된 정책을 실행하고, 실행에 있어 문제가 없는지 주기적으로 점검하고, 문제가 발견될 경우 보완해야 한다. 이같이 기업의 기밀 보호는 기업 자체의 기밀 보호 활동이 원칙이나, 기업 기밀의 유출이 해당 기업에 손실을 입히는 것을 넘어 국가의 기술 경쟁력 저하 등 그 기업이 속한 국가, 사회에까지 피해가 발생 될 수 있으므로 기업의 기밀 유출 방지를 위해 정부의 정책적 지원이 필요하다고 볼 수 있다(노민선·이삼열, 2010). 또한, 산업과 기업이 발전할 수 있도록 지원하는 것을 정부의 역할로 본다면, 기업의 발전에 필수 불가결한 기밀 보호 또한 정부의 정책 범위에 포함될 수 있을 것이다.

정부가 기업의 기밀 보호 활동을 위해 지원할 수 있는 자원에는 한계가 있으므로, 정책 결정과 집행에 있어 활용 가능한 정책 수단의 우선 순위가 중요할 것이다. 우선 순위를 결정하는데 있어 기밀 보호와 관련된 기업, 개인, 사회, 정부 등의 의견과

1) 본 연구에서 기업은 공기업, 사기업, 공기업과 사기업의 연구소를 의미한다. 연구소가 기업에 속한 경우 기업의 근본적 특색을 공유하는 것으로 보아 연구 대상에 같이 포함하였다.

입장을 모두 고려할 수 있겠으나, 가장 중요하고 직접적인 당사자는 기밀 보호의 주체, 기밀 보호 정책의 수혜자, 수요자인 기업으로 판단되므로 기업이 필요로 하는 것들을 기초로 지원 정책을 결정할 수 있을 것으로 본다.

본 연구는 기밀 유출로 인한 기업의 손실, 기밀 유출 방지 등 자산 보호를 위한 산업 보안 현황, 산업보안과 기업 기밀 보호를 위한 정부의 지원 정책을 살펴보고, 정부나 제3자가 아닌, 산업 보안 지원 정책의 직접 수혜자인 기업이 판단하는 정책 우선 순위가 무엇인지를 설문 조사를 통해 조사하였다. 이는, 기업의 기밀 유출 피해, 보안 실태를 기초로 바로 정책 대안을 제시하거나 수립하는 단계로 가지 않고, 정책 적용의 직접 당사자인 기업이 필요하다고 판단하는 정책 대안에 기초하여 정부가 지원 정책 우선 순위를 결정하는 것이 적합한 과정이라고 보았기 때문이다.

또한, 그간의 산업보안에 대한 연구는 기술 분석이나 발전적 대안의 제시보다 기업 기밀 유출 단속 법규, 법적 보호 등에 대한 연구가 주로 이루어지고 있는데(최진혁, 2010) 반해, 이 연구는 법적인 측면보다 기밀보호 정책의 수요자인 기업의 요구에 대해 사실적, 정책적 관점에서 분석하였다.

# Ⅱ. 문헌 연구

## 1. 이론적 배경

### 1) 산업보안, 기밀의 개념

산업보안의 개념은 국내에서 명확히 정의되어 있지 않지만 정부기관, 기업 등이 국가의 핵심 기술이나 중요 산업 기밀 또는 기업의 영업 비밀 등을 보호하기 위한 모든 예방적, 보호적 활동을 포괄하는 것으로 볼 수 있으며 특허보다는 영업비밀과 관련되어 있다(노민선·이삼열, 2010; 최진혁, 2010).

산업보안은 정부기관의 보안과 공·사기업의 보안으로 나눌 수 있는데(Kovacich & Halibozek, 2003), 정부 기관의 보안을 제외한 기업 보안은 기업의 인적 자원, 정보, 물리적 자산을 보호하고 기업의 자산에 대한 위험을 감소시키는 것이라고 할 수 있다(Halibozek & Kovacici, 2005).

산업보안은 광의의 의미로 '범죄로부터 모든 경제 활동을 보호하는 일체의 노력

(한국산업보안연구학회, 2011:6), ‘자산을 지키는 자산 보호와 피해를 막는 손실 방지(Cunningham & Taylor, 1985: 39)’, ‘산업 자산의 안정성을 유지하는 모든 활동이나 상황(최선태, 2009: 36)’ 등으로 표현되며, 협의의 산업보안은 ‘산업 활동에 유용한 기술·경영상의 모든 정보나 인원·문서·시설·자재 등을 산업 스파이나 경쟁 관계에 있는 기업은 물론이고 특정한 관계가 없는 자에게 누설 또는 침해당하지 않도록 보호·관리하기 위한 방안이나 활동(국가정보원, 1999: 1)’, ‘국가 발전에 유용한 기술이나 경영상에 필요한 정보 및 기술을 각종 침해 행위로부터 안전하게 보호·관리하기 위한 대책(민병설, 2002: 24)’ 등으로 정의되며 산업 기술이나 기밀의 유출을 방지하는데 초점을 두고 있다.

시만텍, 안철수 연구소 등 기밀 보호나 보안을 필요로 하는 기업에 보안 서비스를 제공하는 보안 산업은 본 연구의 산업보안 개념과는 그 관점이 다르다. 그러나 산업보안을 위한 정책적 고려에 기업에 보안 서비스를 제공하는 보안 산업 업체의 활동을 활성화해야 산업보안도 강화된다는 점을 검토할 필요성은 존재한다고 볼 수 있을 것이다.

산업보안과 기업 보안은 유사하나 또 다른 개념인 정보 보안(Information Security)은 정보 시스템 자원의 가용성(Availability), 기밀성(Confidentiality), 무결성(Integrity)을 유지하기 위해 정보 시스템에 취해진 보호 조치를 뜻한다(NIST, 1996; ISO 17799, 2005).

산업보안과 관련된 법률을 살펴보면 ‘산업기술의 유출방지 및 보호에 관한 법률’은 중앙 행정 기관이 지정 고시하는 산업 기술 및 국가 핵심 기술 보호가 주목적인데 ‘부정경쟁방지 및 영업비밀보호에 관한 법률’은 이러한 기술 외에도 외부의 침해로부터 보호해야 할 기업의 다른 기술 또는 경영관련 정보를 ‘영업비밀’로 규정하고 부정한 수단에 의한 침해를 금지하고 있다(임창묵, 2013). ‘산업기술의 유출방지 및 보호에 관한 법률’은 기업의 이익을 우선하여 기업 기밀을 보호하는 것보다 기업 기밀 유출로 인해 사회, 국가가 입게 될 피해를 예방하는데 초점이 있는 것으로 보인다. 이에 반해 ‘부정경쟁방지 및 영업비밀보호에 관한 법률’은 사회, 국가를 논하기 전에 기밀의 소유자인 기업이 기밀 보호로 인해 얻게 되는 이익을 보호하는데 주된 목적이 있는 것으로 이해할 수 있을 것이다.

본 연구는 산업보안의 주체인 기업, 연구소 등이 산업보안, 특히 기밀 보호를 위해 우선적으로 정부가 지원할 방향이 무엇인지에 대해 조사하였다. 여기에서 산업보안은 인적, 물적 자산, 정보 보호와 관련된 모든 요소를 포괄하는 광의의 의미가 아니

고, 기업의 정보, 기술 즉, 기업의 기밀이 외부로부터 침해당하지 않도록 하기 위한 일련의 활동을 의미하는 협의의 산업보안이다.

연구 대상은 정책을 집행하는 정부 기관을 제외하고 정책의 수혜를 받게 되는 공기업, 사기업, 공기업과 사기업의 연구소 등을 포괄하여 조사하였다. 정부의 정책을 결정하는데 있어 중소기업과 대기업, 공기업과 사기업, 기업과 연구소 등으로 나누어 정책을 집행할 필요성이 있는데, 본 연구는 이를 나누어 분석하지 않고 산업보안 정책의 수혜자가 되는 조직에 전체적으로 적용될 수 있는 정책 방향을 알아보고자 하였다. 이는 산업보안의 범주에 포함되는 조직들에 공통적, 통합적으로 적용되는 정책 수립과 집행을 할 필요성도 존재한다고 판단하였기 때문이다.

본 연구에서 기밀은 '산업기술의 유출방지 및 보호에 관한 법률'의 산업 기술 및 국가 핵심 기술 개념이 아닌, 「부정경쟁방지 및 영업비밀보호에 관한 법률」의 '영업비밀'의 개념으로 보았다. 또한, 정보 보안 3요소 중 기밀성에 초점을 두고 조사하였다. 이러한 기밀은 기업이 관리 주체인 모든 개인 정보, 고객 정보를 포함한다. 개인정보, 고객 정보의 유출이 큰 사회적 반향을 일으키고 심각한 문제로 대두되었고, 심각한 문제로의 부상 여부를 떠나, 기업이 존재하는 기초가 되고 영업 활동의 원천이 되는 개인 정보, 고객 정보는 기업이 보호해야 할 기업의 기밀 정보에 당연히 포함되는 것으로 보아야 할 것이다.

### 2) 기업 기밀 유출 및 보안 현황

우리나라는 국제전기통신연합 (ITU, 2013)가 발표하는 정보 통신 발전지수는 1위이지만, 사이버 보안이 기업에서 적절히 다뤄지는 정도를 나타내는 스위스 국제경영개발원(IMD, 2013)의 사이버 보안지수(cyber security index)[2]는 58개국 중 23위에 그치고 있다. 정보 통신의 발전으로 점점 많은 양의 정보가 정보 통신을 통해 생산, 보관, 전달되고 이 과정에서 기밀 유출의 가능성 또한 증가된다는 점에서, 정보 통신 발전에 따른 보안 리스크에 대한 대비 및 투자 또한 증대되어야 할 것으로 판단되나, 현실은 그렇지 않은 것으로 보여 진다. 국가정보원 기술 유출 통계(2013)에 따르면 연도별 해외 기술 유출 적발 건수는 2012년 30건으로 전년도인 2011년 46건에 비해 줄었으나, 2003년 6건에서 2013년 49건으로 전체 연도를 보면 증가 추세이다. 2009년

2) 국가 경쟁력 지수의 기술·인프라 부문에 포함된 지식정보 보안 관련 항목으로 사이버 보안이 기업에서 다루어지는 비중을 말한다.

부터 2013년까지의 기술 유출 209건 중에서 유출 주체는 전직 직원 60.8%, 현직 직원 19.6%, 협력업체 9.6%로 기업의 내부 직원과 기업에 우호적이어야 할 업체가 오히려 90%를 차지하고 있다. 기술 유출의 피해자는 중소기업 73%, 대기업 19%로 기업의 보안 시스템에 투자할 자금이 부족하고 기술 보호 의식이 대기업보다 상대적으로 낮은 것으로 추정되는 중소기업의 기술 유출 건수가 지속적으로 증가하는 것으로 보이며, 기술 유출을 한 이유는 금전 유혹, 개인 영리가 약 80%, 인사, 처우 불만이 약 15%이다.

중소기업연구원(2014)은 중소기업의 기술 유출 비중이 대기업보다 높고, 중소기업의 기술유출 비율은 감소하고 있으나 기술유출 1건당 피해 금액은 2008년 9.1억원에서 2013년 16.9억원으로 지속적으로 증가하고 있는 것으로 조사하였다. 중소기업 1개사가 지출하는 보안 관리 비용은 평균 3,530만원, 기업 매출액의 0.24%였다.

한국산업기술진흥협회(2010)의 2010년 10월 1,500개 중소기업 대상 조사 결과에 따르면 13.0%의 기업이 기술 유출로 인한 피해를 경험했고 건당 피해 금액은 평균 16억원으로 나타났다. 조사 대상 중 54.0%의 기업만이 보안 규정을 가지고 있었고 보안 관련 조직이나 직원이 없는 기업이 41.5%에 달하였으며, 53.8%가 산업보안 관련 애로 사항으로 투자 곤란을 언급하였다. 정기적으로 임직원 교육을 실시하는 기업은 12.7%에 불과하였다.

한국인터넷진흥원의 정보 보안 실태조사(2010)에 의하면 국내 기업의 85.5%가 정보 보안 전담 조직을 운영하지 않는 등 지속적인 정보 보안 관리를 위한 전담 부서가 부족했고, 정보 보안 업무를 책임지는 CSO, CISO가 형식적으로 운영되거나 임명되지 않는 것으로 나타났다.

시만텍(2010)의 기업 현황 보고서에 따르면, 2년간의 추이를 분석한 결과 75% 이상의 기업의 사이버 공격을 당하였고, 이로 인한 기업의 피해액은 연평균 약 23억원으로 추산되며, 모바일, 클라우드, SNS 등 새로운 서비스가 확산됨에 따라 공격 대상이 확대되고 기법도 지능화되고 있다. Sarbanes-Oxley Act[3], Basel II[4], 개인정보보호법[5] 등 보안 관련 법규 도입, 시행으로 보안 환경이 달라지고 있어 보안과 관련된

3) 엔론(Enron)사와 월드콤(WorldCom)사의 회계 부정 사건 이후 재무 조작과 회계 스캔들을 방지하기 위해 2002년 미국에서 제정된 법으로 2002년 기업책임성법(Corporate Responsibility Act of 2002)으로 불리기도 한다.

4) 은행 건전성 기준인 자기자본 비율(BIS)인 바젤1을 강화한 새로운 BIS협약으로 신바젤협약이라고도 한다. 은행 내부규정, 임직원 업무행위, IT시스템의 운영 리스크 등을 규정하고 있다.

접근 방법도 변화해야 한다(김정덕, 2012).

한국인터넷진흥원의 지식정보보안 분야 인력 현황 및 중장기 인력 수급 전망 분석(2010)은 향후 2018년까지 매년 지식정보보안 인력의 신규 수요보다 신규 공급이 부족할 것으로 예측하고 있다.

위와 같이 기업 기밀 유출로 인한 피해가 증가하고, 기밀 유출의 경로가 다양해지고 있으므로 이에 대비하여 기업은 기밀 보호 활동에 변화가 필요한지 분석해야 할 필요가 있고, 정부는 기밀 유출 방지를 위해 기업의 요청 사항을 고려하여 어느 분야에 정책적 지원의 우선순위를 둘 것인지를 검토해야 할 것으로 보인다.

### 3) 산업보안 및 기업 비밀 보호를 위한 정부의 정책 및 지원

정부 차원의 산업보안 내지 기업 보안 활동이 본격적으로 시작된 것은 2003년 10월 국가정보원에 '산업기밀보호센터'가 설립되면서부터, 국가정보원을 제외한 정부의 산업보안 활동은 '부정경쟁방지 및 영업비밀보호에 관한 법률'의 한계를 보완하기 위해 지식경제부가 주도한 '산업기술의 유출 방지 및 보호에 관한 법률' 시행과 '한국산업기술보호협회'가 설립된 2007년 이후라고 볼 수 있다(노민선·이삼열, 2010).

기술 유출 방지를 위한 정부의 산업보안 정책은 관련 기업의 특정한 행위를 유도하거나 권장할 수도 있으나, 상당 부분은 기업의 행위를 제한하는 규제적 성격을 가질 수 있다. '산업기술의 유출방지 및 보호에 관한 법률'은 국가 핵심 기술 관련 수출 및 해외 인수·합병의 경우에 정부의 승인 또는 사전 신고를 요구하는 등 유인 또는 정보 제공 보다 규제 측면이 강하다고 볼 수 있다(정병일, 2008: 86; 한희원, 2009: 273). 같은 맥락으로 규제개혁위원회는 '산업기술의 유출방지 및 보호에 관한 법률'에 규정되어 있는 각종 정책을 행정적 규제(administration regulation)로 분류하고 있으며, 국가안보에 미치는 영향 등 특정한 경우에는 수출 및 인수·합병이라는 기업의 영업 활동을 직접적으로 제한하는 경우도 있다는 점에서 경제적 규제(economic regulation)의 성격도 일부 포함하고 있다. 산업보안 정책의 규제방식은 강제력을 행사하여 사회적 가치를 실현시키거나 또는 이의 실현을 방해하는 행위를 직접적으로 금지 또는 제한하는 '명령지시적 규제(regulation by directives)' (최병선,

5) 이 법 적용 대상은 공공·민간의 모든 개인정보처리자로, 개인정보의 수집·이용·제공 등에 대한 보호기준을 규정하고, 고유식별정보의 처리 제한을 강화하고, 영상정보처리기기의 설치 제한에 대한 근거를 마련하였다.

1992: 457-458), 개인이나 기업에 어떤 의무를 부과하기는 하지만 경제적 유인책을 제시함으로써 부여된 의무를 이행하도록 유도하는 '시장유인적 규제'(최병선, 1992: 458; 김용우, 2010: 322), 정부 주도의 일률적 규제로는 복잡 다양한 모습을 갖고 있는 기업을 효과적으로 규제하는데 한계가 있으므로(곽관훈, 2009: 28) 집단이 그 구성원의 행위를 스스로 규제하는 자율규제(self-regulation)(최병선, 1992)등으로 구분할 수 있다.

김정덕(2012)은 정부의 평가 및 인증 제도에 중복 규제가 존재하며, 기업의 자율통제(self-control) 역량을 강화하고 보안 수준 향상을 위한 당근과 채찍 정책 재검토가 필요하다고 보았다. 정보보안전문가(SIS), 산업보안관리사, 정보시스템보안전문가(CISSP), 정보시스템 감리사(CISA), 정보보안관리자(CISM) 등 국내, 국외 자격증이 존재하나 국가 공인 정보보안 자격제도가 요구되고, 공통적으로 습득해야 할 필수 요구 지식(EBK: Essential Body of Knowledge)에 대한 정의가 필요하며, 민간 기업이나 공공 기관의 CSO, CISO 임명 권고 내지 의무화 도입 검토를 제안하였다. 그리고 '정보통신망 이용촉진 및 정보보안등에 관한 법률', '정보통신기반보호법', '신용정보의 이용 및 보호에 관한 법률', '전자서명법', '위치정보의 보호 및 이용 등에 관한 법률' 등 보안과 관련된 여러 개별법이 있으나 법률 적용의 사각 지대 및 개별법 간의 충돌을 해결하기 위한 일반법이 필요한 것으로 보았다.

현재의 지원 정책 현황을 살펴 보면, 산업기술보호협회에서 기업 임직원 대상의 산업보안 교육, 통합보안 컨설팅, 산업 보안 관리사 시험, 산업기술 유출 상담을 제공하고 있다. 산업기술 유출 분쟁을 신속하게 조정하기 위해 산업기술분쟁조정위원회가 운영되고 있으며, 중소기업청에서는 보안시스템 구축 지원, 해외 진출 기업을 포함한 기술보호 상담, 핵심 기술 자료를 임치 기관에 보관하여 기술보호를 위한 증빙자료로 활용하게 하는 기술 자료 임치, 정보시스템에 대한 보안관제 서비스를 시행하고 있다. 중소기업연구원(2014)에 따르면, 중소기업 기술보호 지원예산은 2009년 약 30억원에서 2014년 65.7억원으로 증가하였고, 중소기업청 전체 예산 대비 기술보호 지원예산 비율 또한 증가하고 있지만 2014년 기준 0.33%에 그치고 있다. 한편, 2014년 제정된 '중소기업기술보호 지원에 관한 법률'에 따라, 중소기업 기술보호 관련 국세 및 지방세 감면이 가능하고, 중소기업 기술분쟁조정·중재위원회가 운영되고 있다.

## 2. 선행 연구

노민선·이삼열(2010)은, 2007년 중소기업청 주도로 산업보안 통계조사가 실시되었고 기업을 대상으로 한 보안 교육과 보안 시스템 구축 지원 사업이 시행되고 있으나, 예산 부족으로 일회성 교육 또는 가이드북 발간에 그치고, 보안 컨설팅이나 보안 시스템 구축 지원은 부족한 것으로 보았다.

기업이 정부에 요청한 지원 분야의 연구 결과를 보면, 보안 컨설팅 및 시스템 구축 전반에 대한 지원 확대를 가장 우선적으로 요구했고(중소기업청, 2009a), 산업보안 우수 기업에 대해 정부의 인증 및 인증기업에 대한 정부의 우대(한국산업기술진흥협회, 2006; 한국산업기술보호협회, 2008; 중소기업청, 2009a), 산업보안 전문인력 양성의 필요성도 요구되었다(한국산업기술보호협회, 2008; 중소기업청, 2009a, 2009b). 중소기업청(2008)은 벤처기업과 이노비즈 등 혁신형 중소기업의 인증 평가 지표에 '기업의 보안관리 노력'을 포함시켜 중소기업의 보안관련 투자활성화 및 인식 제고를 도모할 필요가 있음을 제시하고 있다.

중소기업청(2012)은 중소기업을 대상으로 산업기밀 유출로 인한 피해, 기밀 유출자, 유출 후 조치, 보안 규정을 갖추고 있는지 여부, 기타 보안 인프라 등에 대한 기술보호 역량 및 수준조사를 하고 있다. 이 조사를 바탕으로 정부 기관 등이 지원 정책 대안을 제시할 수는 있으나, 기업이 필요하다고 판단하는 지원 정책의 우선 순위를 중심으로 조사하지는 않았다. 본 연구는 정책 결정의 우선 순위를 정책의 수혜 당사자인 기업을 대상으로 조사하는데 중점이 있다는 점과 조사 대상이 중소기업에 한정되어 있지 않다는 점에서 중소기업 기술보호 역량 및 수준조사와 차이가 있다.

임창묵(2013)에 의하면, 학계 및 연구기관, 지식경제부, 경찰청, 민간 협회, 민간기업 대상 조사에서 명령 지시적 규제, 시장 유인적 규제, 자율 규제 정책 수단 중, 시장 유인적 수단을 바탕으로 기업의 능동적인 참여를 유도하는데 주력하면서 보조금 지원 및 보안규정 수립과 부분적인 자율규제의 방법을 병행하는 정책의 우선순위가 높게 조사되었다

위와 같이 기밀 보호를 위한 정부의 그간의 지원 규모는 기업이 만족할 만한 수준이었다고 보기 어렵다. 정부의 지원 정책은 상당 부분 법률 등을 통한 규제적 정책이었다고 볼 수 있겠으며 기밀 보호를 위한 기업의 활동을 장려하는 정책 수단의 강화가 고려될 필요가 있을 것으로 판단된다. 또한 보안 전문가에 대한 인증, 자격증,

검정에 대한 국가의 공인 내지 지원이 필요한 것으로 보이고, 이를 위해 기본적으로 보안 전문가가 갖추어야 할 공통적 필수 지식을 정립하는데 정부가 일조해야 한다는 요구도 있어 왔다.

선행 연구는 중소기업을 분리하여 연구 대상으로 한 경우가 상당수 있었으나, 본 연구는 대기업과 중소기업을 나누지 않고 같은 분석의 대상에 포함하였다. 중소기업과 대기업, 또는 기업과 연구소가 서로 성격이 다른 부분이 있으므로 정책 또한 달리 설계되어야 할 것이나, 중소기업과 대기업이 같은 기업이라는 속성을 갖고, 기업의 연구소인 경우 기업과 연구소는 근본적 특색을 공유하므로 정책의 수립, 적용에 있어 공통적인 부분 또한 갖고 있는 것으로 보았다. 산업보안의 이해 당사자인 정부, 사회, 기업, 학계, 개인 등등에서 산업보안 강화, 기밀 보호 강화의 주체인 기업과 주체의 활동에 도움을 줄 수 있는 정부의 역할 관계에 초점을 두었기 때문에 기업을 대기업, 중소기업과 같이 한 단계 더 나누어 조사, 분석하지는 않았다.

본 연구는 기업 기밀 보호를 위해 정부의 지원 규모 확대가 필요한지를 지원 정책의 수요자인 기업을 대상으로 조사하였고, 위에서 언급된 교육, 보안 시스템 구축 지원, 인증 제도와 유인적 수단 같은 다양한 정책 수단을 설문지에 포함시켜 기밀 보호 정책 방향 조사에 반영하였다.

## Ⅲ. 연구방법

본 연구는 국내 학술지, 저서, 인터넷 등을 통한 문헌 연구를 통해 국내 현황을 알아보고, 우리나라 기업, 또는 연구소의 보안 부서 근무자 또는 보안 담당자에게 설문지를 발송하여, 회수된 설문지중 유효한 것으로 판단된 50개를 분석의 대상으로 양적 연구를 실시하였다. 우리나라 전체 기업, 연구소 중에서 무작위 등의 방법으로 표본을 추출하는 것이 원칙적인 연구 방법이나, 무작위로 표본을 추출하여 그 추출된 표본의 보안 담당자 모두에게 설문을 하는 것은 현실적으로 실행에 어려움이 있었다. 차선책으로, 가장 많은 응답을 받는 것을 우선으로 하여 응답지를 보낼 수 있는 113개 조직에 응답 요청을 하였고 그 중 71개의 응답지를 회수하였으나, 50개를 제외한 나머지는 응답지의 답변 내용이 상당수 공란으로 되어 있는 등, 유효한 응답지로 사용하기에 부적합하였다. 이러한 제약으로 인해, 이 연구에 사용된 응답이 우

리나라 기업, 연구소 등을 산업별, 규모별로 충분히 비례적으로 대표한다고 보기에는 어려운 한계점이 존재한다. 설문지에 대한 응답은 각각의 직원이 하였으나, 그 응답은 하나의 기업, 또는 연구소에 대한 것이므로 분석의 단위(unit of analysis)는 기업, 또는 연구소 단위의 조직(organization)이다. 응답 대상은 제조업체가 35개로 가장 많고, 연구소, 정보통신, 물류 운송 등이 포함되었고 <표 1>, 민간 기업 43개, 공기업 2개 연구소 5개로 민간 기업이 대다수를 차지하고 있다 <표2>. 응답 대상의 규모는, 중소기업기본법 제2조를 참조하여 직원수 1천명 이상, 매출액 1천 5백억원 이상을 기준으로 대기업, 중소기업 수준으로 나누어 보았고 대기업으로 볼 수 있는 규모의 응답 대상은 직원수 기준으로는 22개, 매출액으로는 29개였다 <표3-1, 표 3-2>. 설문지에 응답한 임직원은 그 직급이 다양하고 <표 4>, 각 응답자는 보안 책임자 또는 보안 부서에 근무하는 임직원으로 응답자가 속한 조직의 보안 현황을 알 수 있는 위치에 있었다.

산업보안[6]을 위한 정부 지원 규모의 확대에 대한 의견을 5점 척도로 조사하였다. 지원 규모의 확대에 대한 의견을 여러 개의 문항을 이용하여 질문하고 측정치를 합산하여 평가할 수도 있겠으나, 확대의 필요성에 대해 하나의 질문으로 직접적으로 측정이 가능하고, 응답자의 답변이 용이하여 응답율을 높일 수 있고 조사결과의 간단한 구성이 가능하다고 보았기 때문에 5점 척도를 사용하였다. 확대의 필요성이 어느 정도 있는지에 대한 답변을 등간 척도의 수준으로 인식할 수 없기 때문에 5점 척도보다 많은 구간으로 나누어도 많아진 구간간의 비교가 특별한 의미가 없어 7점 척도를 사용하지 않았다. 또한, 3개의 척도로 나누는 것은 확대의 필요성이 있다, 없다에 대한 조사는 할 수 있으나 필요성이 많은지 적은지에 대한 답을 얻을 수 없어 5점 척도가 가장 적절하다고 보았다.

기업의 기밀(고객의 개인정보 포함) 보호를 위해 정부 차원에서 가장 우선적으로 추진해야 할 정책 방향을 우선순위대로 5개 선택할 것을 설문하면서 다음과 같은 17개 항을 예시로 제시하였다. 17개항 작성은, 그간의 산업보안 통계 조사와 그 설문지 등을 참고 또는 원용하였는데(한국산업기술진흥협회, 2006; 한국산업기술보호협회, 2008; 중소기업청, 2008, 2009a, 2009b), 그 이유는 기존의 조사, 설문에서 제시한 각 항목이 이미 가능한 정책 수단, 분야를 포괄하고 있으므로 다른 수정을 할 필요성

6) 본 연구의 산업보안은, 정부기관을 제외한 공·사기업, 연구소 등의 기밀 유출 방지에 초점을 둔 협의의 산업보안을 의미한다.

이 없다고 보았고, 기존 설문지의 질문을 차용하는 것이 완전히 새로운 설문을 하는 것보다 기존 연구의 조사결과와 비교가 용이한 장점이 있는 것으로 판단하였기 때문이다.

(01) 보안관련 관리 및 대책수립
(02) 세부지침 제정 및 전파
(03) 보안상담지원
(04) 대국민 홍보문화 활동
(05) 침해신고. 관리 분쟁조정
(06) 실태조사
(07) 국제협력
(08) 교육 및 인력육성(On/Off-Line) 지원 강화
(09) 기술개발사업 지원
(10) 유공 포상 및 포상금 지원
(11) 보호설비구축 지원
(12) 인증시스템 구축/지원
(13) 자격/검정제도를 통한 보안전문가 위상 강화
(14) 정책연구개발 및 세미나, 포럼 등 활동지원
(15) 국내외 전시회 지원
(16) 보안관련 학과의 설립 지원
(17) 기타 (:_____)

〈표 1〉 설문조사 대상: 산업별

n=50

| | |
|---|---|
| 건설 (Construction) | 2 |
| 컨설팅 (Consulting) | 2 |
| 정보통신 (Information Technology) | 2 |
| 물류, 운송 (Logistics, Transportation) | 2 |
| 제조 (Manufacturing) | 35 |
| 전력 (Utilities) | 1 |
| 연구 개발 (Research & Development) | 5 |
| 기타 (Other) | 1 |

〈표 2〉 설문조사 대상의 성격 (종류)

n=50

| | |
|---|---|
| 민간 기업 | 43 |
| 공기업 | 2 |
| 연구소 | 5 |

〈표 3-1〉 설문조사 대상: 규모 (직원 수)

n=50

| 직원 1천명이상 | 직원 1천명 미만 |
|---|---|
| 22 | 28 |

〈표 3-2〉 설문조사 대상: 규모 (매출액)

n=50

| 매출액 1천 5백억 이상 | 매출액 1천 5백억 미만 |
|---|---|
| 29 | 21 |

〈표 4〉 설문조사 대상: 응답자의 직급

| | 빈도 | 퍼센티지 |
|---|---|---|
| 대표이사 | 1 | 2.0 |
| 본부장 | 1 | 2.0 |
| 이사 | 1 | 2.0 |
| 부장 | 6 | 12.0 |
| 차장 | 5 | 10.0 |
| 과장 | 14 | 28.0 |
| 주임 | 2 | 4.0 |
| 대리 | 6 | 12.0 |
| 사원 | 9 | 18.0 |
| 선임연구원 | 1 | 2.0 |
| 연구원 | 1 | 2.0 |
| 책임 | 1 | 2.0 |
| 무응답 | 2 | 4.0 |
| 합계 | 50 | 100.0 |

본 연구는 대기업과 중소기업, 민간 기업과 공기업, 기업과 연구소 등을 별도로 나누어 조사, 분석하지 않았다. 그 이유는 중소기업과 대기업의 직원수, 매출, 수익,

환경, 기밀 보호를 위한 투자 여력, 기밀 보호에 대한 직원 및 경영진의 관심에 차이가 있을 것이므로, 상당수 기존 연구와 같이 중소기업과 대기업을 나누어 각각 필요로 하는 지원 정책의 방향이 무엇인지를 조사하는 것이 유의미할 것이나, 기업 전체에 공통적으로 적용될 수 있는 정부의 정책 연구도 필요하다고 보았기 때문이다.

## Ⅳ. 연구 결과

조사 결과, 산업보안을 위한 정부 지원 규모가 확대되어야 한다는데에 대한 응답 비율이 '늘어야 한다' 55.3%, '많이 늘어야 한다' 44.7%에 이르는 등 모든 응답자(n=47)간에 이견이 없었다<표 5>. 이는 정부의 지원 규모가 부족했었다는 문헌 연구 내용과 같은 결과로 볼 수 있겠다.

기밀 보호를 위해 정부가 가장 우선적으로 추진해야 할 정책 방향이 무엇인지에 대해 응답자가 선택한 1순위부터 5순위까지 5개 답변 중에서 4순위, 5순위를 제외하고, 1순위 빈도에 가중치 3배, 2순위 빈도에 가중치 2배, 3순위 빈도에 가중치 1배로 계산하여 이를 합산, 가중치 적용 후 점수를 산출하여 순위 선정의 기준으로 하였다. 가중치 1,2,3배와 관련된 유사 사례를 선행 연구에서 발견하지 못 하여 다른 연구와 연계되는 객관적 수치를 적용하였다고 보기는 힘들고, 가중치 적용에 대해 연구자마다 달리 판단할 수 있을 것으로 본다.

기업의 기밀(고객 개인정보 포함) 보호를 위해 정부 차원에서 가장 우선적으로 추진해야 할 정책 방향에 대해, '교육 및 인력육성(On/Off-Line) 지원 강화'가 1순위 응답중 가장 높은 빈도로 조사되었고, 가중치 적용 후 응답에서도 가장 우선적으로 추진해야 할 정책 방향으로 나타났다. '보안관련 관리 및 대책수립'이 1순위 응답에서 '교육 및 인력육성(On/Off-Line) 지원 강화'과 같은 빈도(11)를 보였으나, 1, 2, 3순위 응답에 가중치를 적용한 결과 두 번 째 높은 점수로 나타났다. '자격/검정제도를 통한 보안전문가 위상 강화'는 1순위 응답에서 실태조사보다 빈도가 낮았으나, 가중치 적용 후 세 번째 높은 우선 순위로 조사되었다<표 6>.

〈표 5〉 산업보안을 위한 정부 지원 규모 확대에 관한 의견

| | 빈도 | 퍼센트 |
|---|---|---|
| 늘어야 한다 | 25 | 55.3 |
| 많이 늘어야 한다 | 21 | 44.7 |
| 합계 | 47 | 100.0 |

〈표 6〉 기업의 기밀(고객의 개인정보 포함) 보호를 위해 정부 차원에서 가장 우선적으로 추진해야 할 정책 방향 우선순위

n=50 (미응답 포함)

| 순위 (가중치 적용후) | 정책 방향 | 1 순위 | % | 2 순위 | % | 3 순위 | % | 가중치 적용후 점수[7] | % |
|---|---|---|---|---|---|---|---|---|---|
| 1 | (08) 교육 및 인력육성(On/Off-Line) 지원 강화 | 11 | 22 | 10 | 20 | 3 | 6 | 56 | 19 |
| 2 | (01) 보안관련 관리 및 대책수립 | 11 | 22 | 6 | 12 | 5 | 10 | 50 | 17 |
| 3 | (13) 자격/검정제도를 통한 보안 전문가 위상 강화 | 4 | 8 | 4 | 8 | 11 | 22 | 31 | 10 |
| 4 | (02) 세부지침 제정 및 전파 | 4 | 8 | 7 | 14 | | | 26 | 9 |
| 5 | (11) 보호설비구축 지원 | 3 | 6 | 5 | 10 | 4 | 8 | 23 | 8 |
| 6 | (12) 인증시스템 구축/지원 | 3 | 6 | 3 | 6 | 6 | 12 | 21 | 7 |
| 7 | (06) 실태조사 | 5 | 10 | 2 | 4 | 1 | 2 | 20 | 7 |
| 8 | (04) 대국민 홍보문화 활동 | 2 | 4 | 2 | 4 | 7 | 14 | 17 | 6 |
| 9 | (09) 기술개발사업 지원 | 1 | 2 | 2 | 4 | 5 | 10 | 12 | 4 |
| 10 | (03) 보안상담지원 | 1 | 2 | 2 | 4 | 2 | 4 | 9 | 3 |
| 11 | (16) 보안관련 학과의 설립 지원 | | | 4 | 8 | | | 8 | 3 |
| 12 | (05) 침해신고. 관리 분쟁조정 | | | 1 | 2 | 2 | 4 | 4 | 1 |
| 13 | (07) 국제협력 | 1 | 2 | | | 1 | 2 | 4 | 1 |
| 14 | (14) 정책연구개발 및 세미나, 포럼 등 활동 지원 | 1 | 2 | | | | | 3 | 1 |
| 15 | (10) 유공 포상 및 포상금 지원 | | | | | 1 | 2 | 1 | 0 |
| 16 | (15) 국내외 전시회 지원 | | | | | | | 0 | 0 |
| 17 | 미응답 | 3 | 6 | 2 | 4 | 2 | 4 | 15 | 5 |

7) 가중치 적용 후 점수 = 1순위 빈도*3 + 2순위 빈도*2 + 3순위 빈도*1

(08) ‘교육 및 인력 육성’과 (13) ‘자격/검정 제도를 통한 보안 전문가 위상 강화’는 그 목적이나 범위가 다소 다를 수 있으나, 큰 범주에서 유사한 유형이라고 볼 수 있다. ‘자격/검정 제도를 통한 보안 전문가 위상 강화’는 보안, 기밀 보호 업무를 전담하는 인력에 초점이 맞춰져 있다.

(01) ‘보안 관련 관리 및 대책’은 기밀 보호 조직을 어떻게 둘 것인지와 직원들에게 기밀 보호를 위해 어떤 행동을 요구할지를 규정하는 것으로 이해할 수 있다. 인사, 총무, 사내 IT 등 기업 내부의 지원 부서 중에 기밀 보호 활동을 전담하는 부서가 따로 없고 지원 부서중 하나에 소속된 직원이 업무를 처리하는 경우도 있고, 전담 부서가 별도로 구성된 기업도 있다. 기업의 직원수, 매출과 수익 규모, R&D 비중, 특허 등 보유 기술, CEO의 기밀 보호에 대한 의식 등에 따라 기밀 보호 업무를 수행하는 직원, 부서의 위치가 정해진다고 볼 수 있다. 기업 기밀 보호의 가치를 크게 본다면 기밀 보호를 담당하는 직원, 부서를 보다 독립적으로 둘 것이다.

문헌 연구에서 언급한 한국산업기술진흥협회(2010)의 중소기업 대상 조사 결과, 조사 대상 중 54.0%의 기업만이 보안 규정을 보유하고, 정기적으로 임직원 대상 보안 교육을 실시하는 기업이 12.7%에 그친 것과 본 연구의 응답 선택 항목 순위를 볼 때, 기업 보안 담당 직원 및 관련 직원들은 현실의 보안 규정 부재와 낮은 교육 빈도가 개선되어야 할 중요 항목으로 판단하고 있는 것으로 해석할 수 있겠다.

기업이 기밀 보호를 담당하는 직원의 채용이 필요한지를 판단하고, 채용 여부를 결정할 때 해당 직원의 전문성에 대한 자료가 유용할 것이다. 이미 채용되어 근무하는 기밀 보호 담당 직원의 경우, 기밀 보호 활동을 보다 효과적으로 하기 위해 지속적인 교육과 개발이 요구될 것이다. (13) ‘자격/검정제도를 통한 보안 전문가’의 식별과 능력 개발은 기업의 입장에서, 기밀 보호 담당 직원의 위치에서도 모두 도움이 될 것으로 판단되며, 조사결과에 의하면 이에 대한 요구가 상당히 강한 것으로 보인다(가중치 적용 후 점수 31, 응답자의 선택 비율 10%).

(01) ‘보안 관련 관리 및 대책 수립’ 은 가중치 적용 후 점수 56(19%)이나 (02) ‘세부 지침 제정 및 전파’는 가중치 적용 후 점수 26(9%)로 조사되었다. ‘세부적’인 지침을 제정, 전파하는 경우 기업의 자율성이 줄어 들 수 있다고 보면, (01) ‘보안 관련 관리 및 대책 수립’이 (02) ‘세부 지침 제정 및 전파’보다 높은 응답을 기록한 것은 정부의 지원을 희망하나, 그 정도가 지나치게 규제적이거나 기업의 자유를 훼손하는 정도가 되어서는 안 된다는 것으로 이해할 수 있을 것이다. 이와 별도로 (02) ‘세부 지침 제정

및 전파' 자체로는 4번째 순위로 기밀 보호 정책의 고려 사항중 상위에 위치하였다.

(12) '인증시스템 구축/지원', (06) '실태조사', (04) '대국민 홍보문화 활동', (09) '기술개발사업 지원' 은 가중치 적용 후 점수 23～12 (8%～4%)로 지원 정책시 고려할 사항으로 어느 정도 응답자의 선택을 받았으나, (08) '교육 및 인력육성 지원 강화', (01) '보안관련 관리 및 대책수립', (13) '자격/검정제도를 통한 보안전문가 위상 강화' 보다 적은 선택 비율을 보였다.

(16) '보안관련 학과의 설립 지원'은 가중치 적용 후 점수 8(3%)의 응답을 보였으며, 기업 또는 기업의 직원은 보안 관련 학과의 설립이 기업의 기밀 보호와 큰 관련이 없다고 보는 것으로 해석될 수 있고, 보안 학과의 설립 또는 설립 지원이 장기적으로 기업 기밀 보호에 긍정적 효과를 줄 수 있겠으나, 단기적인 상관 관계나 필요성은 크지 않다고 응답자들이 판단한 것으로 추정할 수 있다.

(05) '침해 신고, 관리 분쟁 조정'은 가중치 적용후 점수 4(1%)로, 침해 신고나 관리 분쟁 조정은 이미 기밀 침해, 누출이 발생한 후의 조치이고 예방적 활동이 아니며, 주된 기밀 보호 활동으로 응답자들이 보지 않은 것으로 이해할 수 있을 것이다.

(07) '국제협력' 또한 기업의 기밀 보호를 위한 정부 지원 정책 항목으로서 특별히 중요하지 않은 것으로 보이며 (가중치 적용후 점수 4, 1%), (14) '정책연구개발 및 세미나, 포럼 등 활동지원', (10) '유공 포상 및 포상금 지원', (15) '국내외 전시회 지원' 또한 1% 또는 0%의 응답율을 보여 지원 정책의 수립시 주된 고려 사항에 포함하지 않아도 될 것으로 조사되었다.

위와 같은, 각 항목의 순위에 따른 분석은, 응답자들이 특정 항목을 어떤 이유로 선택하고, 다른 항목을 어떤 이유로 선택하지 않았는지를 구체적으로 물어보고 답을 받지 않은 상태에서 각 항목에 대한 선택 비율을 다른 항목과 비교하여 해석하였으므로, 이 해석들이 얼마나 유의미한지에 대해 한계나 오류가 존재할 수 있다는 점을 참고해야 한다.

## Ⅴ. 결 론

정부가 지원할 수 있는 예산과 투입 인력 등 자원은 한정되어 있어 정책 수단을 결정할 때 우선순위의 선택은 불가피한데, 정책의 수요자이자 기밀 보호의 직접적

주체인 기업이 판단하는 우선 순위를 정책 방향 수립의 가장 기초가 되는 자료로 활용할 수 있을 것이다. 이러한 측면에서, 본 연구가 진행되었고, 기업이 정부에 요청하는 기업 기밀 보호를 위한 정책 방향 우선순위는, '교육 및 인력육성 (On/Off-Line) 지원 강화', '보안관련 관리 및 대책수립', '자격/검정제도를 통한 보안전문가 위상 강화', '세부 지침 제정 및 전파' 등의 순으로 조사되었다.

위 4개의 항목을 대별하면, 교육과 관리 정책으로 크게 분류할 수 있다. 교육은 기업의 보안 담당자, 직원, CEO 등의 보안 의식과 관련되고, 관리 정책은 어떻게 기밀 보호를 할 것인지 방향과 실천 내용 등을 담고 있는 것이 보통이다. 결국, 기밀 보호에 대한 인식과 회사의 기밀 보호 대책이 정부가 가장 주의를 기울여 지원해야 할 분야로 볼 수 있고, 기업 스스로도 가장 중요한 두 가지 영역으로 판단하고 있다고 추정할 수 있을 것이다.

기업은 기밀 보호를 위해 침입감지 등 네트워크 보안, 바이러스/악성 코드에 대한 기술적 차단, CCTV 등 물리적 기계 경비 등, 기술적 수단을 이용하고 있다. 이러한 기술적 수단을 이용한 기밀 보호 활동은 최종적으로 사람이 운영하는 것이므로, 기업의 직원이 어떠한 보안 의식을 갖고 있는지가 최종적인, 그리고 근본적인 기밀 보호 활동의 출발점으로 볼 수 있을 것이다. 기업의 보안 담당자들의 답변중에 최상위를 차지한 '교육 및 인력 육성 강화'은 이러한 의미에서 해석될 수 있는 것으로 보인다. 기밀 보호는 기밀 보호 활동을 업무로 수행하는 직원에게만 해당되는 것이 아니라 해당 기업의 모든 직원이 책임을 갖고 기밀 보호를 위한 행위를 해야 하므로, 보안 관련 교육은 기밀 보호를 주 업무로 하는 사람에게만 제공되어서는 안되고, 기업의 모든 직원이 대상이 되는 것으로 이해되어야 할 것이다.

본 연구에서 정부가 기업의 기밀 보호를 위해 정책 지원을 하고, 지원 우선 순위를 정해야 한다는 것은 단어 그대로 '지원'이며, 정부가 기업 기밀 보호의 주체가 되는 것을 의미하는 것은 아니다. 산업 보안, 기업 기밀 보호의 주체는 기업이고 기업이 주된, 그리고 근본적인 기밀 보호 활동을 해야 한다는 전제하에서, 정부의 지원 역할이 보다 효과적으로 이루어질 수 있는 방법을 모색한 것이 본 연구의 취지이다. 또한, 정부의 지원 정책이 지나치게 세부적이거나 규제적으로 되는 것은 기업의 자율성 측면에서 바람직하지 않을 것이므로 기업의 기밀 보호를 위해 정부가 어느 수준까지 개입할 것인지에 대해 주의 내지 숙고가 필요한 것으로 보인다. 지원 정책의 우선순위를 기업체를 대상으로 조사함에 있어 본 연구와 같이 중요 항목을 우선순위

로 선택하게 하는데서 더 나아가, 우선순위로 선택한 이유를 추가로 설문하는 방법도 고려할 수 있을 것이다. 설문 방식은 가급적 다른 유사 연구들과 같은 항목들을 응답자에게 제시하는 것이 다른 연구의 결과들을 비교하여 통합적인 해석을 하는데 유리할 것으로 보인다. 특정 연구자가 특정한 방법론을 정해 최초 조사한 경우, 이후 주기적으로 계속 조사를 한다면, 시간에 따른 사회, 기술의 변화와 기업이 원하는 지원 정책의 요구 사항의 변화 추이를 분석할 수 있을 것이다.

# 참고문헌

## 1. 국내문헌

국가정보원(1999). 산업보안실무

국가정보원(2014). 기술유출통계[On-line] http://service12.nis.go.kr/images/center/2014_infographic.pdf, 검색일 2014. 5. 12.

곽관훈(2009). 기업규제의 패러다임전환과 내부통제시스템, 경제법연구, 제8권 제1호.

김용우(2010). 정부규제와 규제행정, 대영문화사.

김정덕(2012). 국가 정보보안 이슈 및 정책방안에 관한 연구, 디지털정책연구, 제10권 제1호, 105-111.

남재성(2012). 중소기업의 산업기밀 유출범죄 피해실태와 대책 -법,제도적 방안을중심으로-, 한국 공안행정학회보, 46, 45-75.

노민선·이삼열(2010). 중소기업의 산업보안 역량에 대한 영향요인 평가, 한국행정학보, 44, 239-259.

민병설(2002). 산업보안체계의 정립에 관한 연구, 경희대학교 박사학위논문.

손경호(2010). 정보보안 산업현황 및 전망, 정보과학회지, 28, 72-78.

시만텍(2010). 기업현황 보고서

임창묵·박형준·김동현(2013). 효과적인 산업보안 규제정책 방향과 정책수단, 국정관리연구, 8, 123-151.

정병일(2008). 국가핵심기술의 수출규제보상에 관한 특허법적 연구, 산업재산권, 25, 85-131.

중소기업청(2009a). 중소기업 산업기밀관리 실태조사 보고서.

중소기업청(2009b). 산업보안 역량평가 및 발전방안.

중소기업청(2012). 중소기업 기술보호 역량 및 수준조사 결과 보고서

중소기업연구원(2014). 중소기업 기술보호 지원 정책의 현황 및 과제

한국산업기술보호협회(2008). 산업기술 보호를 위한 실태조사 보고서.

한국산업기술진흥협회(2006). 기업연구소 산업기밀 관리실태 및 개선방안.

한국산업기술진흥협회(2010). 산업기밀관리 실태조사 보고서.

한국산업보안연구학회(2011). 산업보안학, 박영사.

한국인터넷진흥원(KISA, 2010). 2010년 정보보안 실태조사

한국인터넷진흥원(KISA, 2010). 지식정보보안분야 인력현황 및 중장기 인력수급 전망 분석, 36-41.

한희원(2009). 정보보안의 규제 혁신에 대한 고찰, 법조, 제58권 제4호, 258-301.
최병선(1992). 정부규제론, 법문사.
최선태(2009). 21세기 산업보안론, 진영사.
최진혁(2010). 산업보안의 제도적 발전방안 연구, 한국경호경비학회지, 22, 197-230.

## 2. 국외문헌

Cunningham, W. C., & Taylor, T. H. (1985). Private security and police in America: The Hallcrest report. Portland, OR: Chancellor Press.

Halibozek, E. P. and Kovacici, G. L.(2005). Mergers and Acquisitions Security: Corporate Restructuring and Security Management, Amsterdam; Boston: Elsever Butterworth Heinemann.

International Institute for Management Development(IMD, 2013). World Competitiveness yearbook

ISO/IEC(2005) ISO17799, Code of Practice for Information Security Management

International Telecommunication Union (ITU, 2013). 정보통신발전지수(IDI).

Kovacich, G. L. and Halibozek, E. P.(2003). The manager's handbook for corporate security : establishing and managing a successful assets protection program. Boston, MA : Butterworth-Heinemann.

NIST(1996). An Introduction to Computer Security, The NIST Handbook.

【Abstract】

# Priority of the Government Policy to support Industrial Security

## – Focus on a companies' demand and efficiency of policy–

Kim, Chang–Ho
Yu, Jai–Hwan

This study surveyed the subject of companies' industrial security on priorities of the government policy for the confidentiality of corporate and the necessity of expanding the government support for the industrial security. In determining the priority, we should consider all opinions of companies, individuals, societies, and governments that associated with the confidentiality. Especially in industrial security, companies are the most significant beneficiaries and consumers of security policy and it would be the basis for supporting on policy-making. As a result, we analyzed the 50 valid questionnaires collected from security personnel of Korean corporations and 'Enhance support for education and promotion of human resource (On/Off-Line)', 'Establish Security management and Security measures', and 'Enhance Security professionals status via qualifications/certifications' are shown as 1st, 2nd, 3rd priority of government policy to protect Corporate confidential information including its customer information. All respondents of the study says that the Government support for Industrial Security should be enlarged.

Key words : Industrial Security, Commercial Confidentiality, Priority of Supporting Policy, Security Education and its Human Resource development, Security Policy, Security Measures, Security Qualifications and Certifications