한국경호경비학회 – 제61호(2019): 203–234
https://doi.org/10.36623/KSSR.2019.61.9

투고일 2019. 11. 07 심사일 2019. 11. 26 게재확정일 2019. 12. 10

대·중소기업 동반성장과 상생을 위한 중소 협력업체의 보안인증 제도 도입 방안

신 현 구

대·중소기업 동반성장과 상생을 위한 중소 협력업체의 보안인증 제도 도입 방안

신 현 구*

〈요 약〉

최근 협력업체의 기술유출로 인하여 고객사인 대기업의 경영에 위험을 초래하고 나아가 이미지와 신뢰도가 추락하는 등 보안사고 피해가 지속적으로 증가하고 있다. 그러나 현대 산업구조는 대기업의 독자적인 기업형태는 현실적으로 불가능하고 협력업체와의 전략적 제휴가 필수적이라 할 수 있는데 이에 따른 정보의 교환이 증가되고 정보시스템의 사무의 존도가 극대화됨은 물론 업무프로세스의 복잡화와 보안관련 법률의 강화에 따른 법적 요구와 이해관계자의 요구사항이 증대되고 있는 산업구조 형태로 변화되고 있다.

중소기업의 기술보호 실태를 보면 대기업에 비하여 상대적으로 열악한 환경과 재정적 어려움으로 인하여 보안체계를 갖추지 못하고 있는 실정인데 반하여 대기업과 중소 협력업체간의 산업구조가 IT시스템 공유가 필수 불가결하여 중소협력업체의 보안수준 향상 없이는 고객사인 대기업의 보안관리는 불가능한 현실을 감안하여 고객사인 대기업과 중소협력업체 간의 보안체계구축 인증제도를 도입하므로써 대기업에 비하여 열악한 보안수준을 향상하여야 하는 시점이다. 이에 그간의 대중소기업 동반성장을 위한 제도와 여러 기관의 정보보호 역량 평가 모형을 살펴보고, 중소협력업체 인증제도 도입 방안을 제시하고자 한다.

주제어 : 대중소기업, 협력업체, 기술유출, 보안실태, 정보보호 인증제도, 보안측정

* 중부대학교 경찰경호학부 교수

목 차

Ⅰ. 서 론

최근 정부가 대기업의 사회적 책임과 대 · 중소기업 상생을 강조함에 따라 상생협력에 대한 관심이 높다. 기업의 역할은 생산의 범주에서 벗어나 조달-운영-유통의 과정을 거치게 되는 사슬로 확대되어 얼마나 효율적으로 운영하고 차별적인 경쟁력을 갖추고 있는지에 따라 기업 성패가 좌우된다. 이러한 사슬을 구성하는 전략에 따라 기업의 경쟁력이 달라지고 전체적인 운영에 영향을 미치게 되고 이러한 사슬이 점차 커짐에 따라 기업이 관리해야 할 차원이 늘어나면서 하나의 기업이 모든 기능을 수행할 수 없으므로 현실적으로 기업은 아웃소싱 또는 더 나은 파트너십을 구축한 협력업체와 함께 사슬을 구성하게 되고 이러한 경쟁력 있는 사슬을 구성하기 위해 협력업체의 중요성은 점점 확대되고 있다. 협력의 모습은 기업규모로 볼 때 대기업과 대기업, 중소기업과 중소기업, 대기업과 중소기업의 형태로 이루어 질 수 있는데 이 중에서 힘의 균형이 한쪽으로 치우치게 되는 대기업과 중소기업의 관계에 있어서는 힘이 월등히 강한 대기업과 종속적인 위치에 있는 중소기업의 관계에서 불합리성과 비효율성이 발생하게 되고, 이를 극복하여 대등한 관계가 형성되어야 win-win 또는 동반성장의 성과를 나타낼 수 있다. 즉 대기업과 중소기업이 함께 협력

할 수 있는 기업생태계를 구축해야 경쟁력을 갖출 수 있다.

이런 배경으로 보안 측면을 살펴보면, 대기업과 중소 협력업체간 기술정보 및 IT 시스템의 공유가 증가함에 따라 고객사인 대기업의 기술정보 또는 영업비밀 등이 협력업체를 통해 유출되는 일이 빈번히 발생하고 있음은 물론 중소협력업체의 보안수준을 향상시키고 정형화하여 안정화된 협력업체 보안관리 체계를 구축하고 나아가 동반성장과 상생협력의 기초를 마련해야 할 시점이다. 특히 최근 협력업체의 기술유출로 인하여 고객사인 대기업의 경영에 위험이 초래되고 나아가 이미지와 신뢰도가 추락하는 등 보안사고 피해가 지속적으로 증가하고 있다. 그러나 현대산업구조는 대기업의 독자적인 기업형태는 현실적으로 불가능하고 협력업체와의 전략적 제휴가 필수적이라 할 수 있는데 이에 따른 정보의 교환이 증가되고 정보시스템의 사무의존도가 극대화됨은 물론 업무 프로세스의 복잡화와 보안관련 법률의 강화에 따른 법적 요구와 이해관계자의 요구사항이 증대되고 있는 산업구조 형태로 변화되고 있다.

중소기업이 보유하는 기술은 고객사인 대기업의 자산일 수도 있고, 해당 기업의 자산일 수도 있으나 기업운영과 발전을 위해서도 그 보호가 필요하다,

따라서 중소기업의 기술보호 역량을 강화하여 안정적인 기술개발 여건을 조성하고 기업의 기술 경쟁력을 제고하며 관련 산업발전과 나아가 국가발전에 기여하는 정보는 무체재산권이라는 점에서 지속적인 관리와 보호 및 그 지원이 필요하다고 할 수 있다.

Ⅱ. 협력업체의 정보보호 상생평가 개념과 중소기업의 보안실태 및 보안인증제도 도입의 필요성

1. 대중소 협력과 대중소기업 동반성장 지수 평가 현황

실제 산업현장에서 대중소기업 협력의 필요성에 대하여 이종욱 외(2016)는 상생협력을 통한 대중소기업 동반성장 해외진출은 간접수출의 편승 모형으로 상대적으로 투입 비용이 적어, 위험이 적다고 하였다. 최근 대부분의 기업들은 전략적 시장 대응을 위해 외부조달과 아웃소싱을 확대하고 있으며, 협력업체와의 협력과 조정을 통해

공급체인의 효율성과 효과를 기대할 수 있으며, 이를 통해 수요예측을 통한 신속대응, 품질향상을 통한 경쟁우위 확보와 같은 다양한 성과를 얻을 수 있다는 송혁준(2014)의 연구가 있다.

실제로 삼성전자는 협력사들과 정보를 공유하기 위한 다양한 활동을 하고 있다. 뉴데일리(2017)에 따르면 삼성전자 상생협력 아카데미는 협력사 임직원들의 역량 향상을 위해 계층별 특화 교육을 무상으로 지원하고 있고, 2015년 보유 특허 2만7000여 건을 개방하고 이를 대구경북창조경제혁신센터 홈페이지에 게시하였으며, 중소기업이 필요로 하는 기술 분야에 대한 특허 매칭 및 특허 출원지원, 활용방법 등에 대한 컨설팅을 지원하였다(매일경제(2017)). 중부일보(2016)에 따르면 삼성전자는 수원에서 '2016 협력사 소통의 장' 행사를 열었으며, 이 행사 이외에도 환경안전센터에 협력사 환경안전 지원 전담부서를 설치하고 가이드와 체크리스트 등을 제공하고 하고 있다.

대중소기업상생협력촉진에 관한 법률 제2조제10호 "동반성장지수"란 대중소기업 간 동반성장을 촉진하기 위하여 동반성장의 수준을 평가하여 계량화한 지표를 말하는 것으로 동법 제10조 제1항 및 제3항 중소벤처기업부장관은 대중소기업 상생협력을 촉진하기 위하여 대중소기업 상생협력의 수준을 평가하여 계량화한 대중소기업 상생협력 지수를 산정하여 공표할 수 있고, 필요하다고 인정될 경우 상생협력 지수를 동반성장위원회가 산정, 공표하는 동반성장지수로 대체할 수 있도록 하고 있다.

동반성장지수의 평가는 공정거래위원회(이하 '공정위')의 '공정거래협약 이행평가'와 동반성장위원회(이하 '동반위')의 '동반성장 종합평가' 등 두 위원회의 지수를 합산하여 평가하며, 평가대상은 사회적 관심이 크고, 동반성장의 파급효과가 큰 대기업이고, 평가주체는 공정위와 동반위에서 실시한다.

동반성장 종합평가는 크게 중소기업 체감도 조사(거래관계, 협력관계, 동반성장 체제 등)와 대기업실적평가항목으로 공평한 성과의 배분, 상생협력기금, 임금격차 해소, 창업기업 지원, 국내 및 해외 판로 지원, 기술보호 지원 등의 평가항목이 있으며, 감점항목으로 적합업종 위반, 중소기업 전문인력 및 기술탈취, 법위반에 따른 처분 항목이 있다. 여기에서 주목하여야 할 것은 기술보호지원은 평가항목에, 중소기업 전문인력 및 기술탈취는 감점항목에 있는 점에 주목하여야 한다.

따라서 상생협력은 대기업이 주도적으로 진행하고 중소기업은 시혜를 받는 형태이므로 대중소기업의 상생을 위한 대기업의 중소기업 협력업체에 대한 기술보호지

원은 어떤 방법으로든 이루어져야 하는 시점에 도달하였으며, 나아가 중소협력업체의 보안체계 구축에도 관심을 갖고 지원하여야 할 것이다.

2. 중소기업의 보안실태

'중소기업기술 보호 수준 실태조사(2018)'에 의하면 최근 3년간(2015~2017) 기술유출 경험이 있는 것으로 조사된 중소기업은 1.9%로 나타났고, 이는 전년도조사 결과(3.8%)보다 1.9%가 감소된 수치를 보이고 있다.

〈표 1〉 중소기업 경험(기술유출 건수 및 피해금액)

구분	피해 경험률 (%)	총 (건수)	평균 (건수)	총 피해금액 (억원)	평균 피해금액 (억원)
중소기업	1.9	67	2.1	1,119	16.7
수혜기업	2.8	46	2.1	1,063	23.1
비수혜기업	1.2	21	2.2	56	2.6

* 응답그룹별 사례수 = (중소기업 2,179개, 수혜기업 924개, 비수혜기업 1,255개)
* 평균 기술유출 건수 = 유출 총 건수 / 유출 총 기업 수
* 평균 기술유출 금액 = 유출 총 금액 / 유출 총 건수
* 기술유출 건수 및 피해금액은 기술유출 피해 경험이 있다고 응답한 중소기업 41개사 중 기술유출 건수와 기술유출 피해금액에 응답한 32개사 기준임

또한 최근 4년간(2015~2018년)의 기술유출 피해금액을 살펴보면 총 1,119억원으로 전년도(1,022억원) 대비 97억원 가량 증가하였고, 평균 피해금액 역시 전년(13.1억원) 대비 3.6억원이 증가한 16.7억원으로 조사 되었다.

〈표 2〉 중소기업 기술유출 현황

구분	피해 경험률 (%)	총 (건수)	평균 (건수)	총 피해금액 (억원)	평균 피해금액 (억원)
2018년	1.9	67	2.1	1,119	16.7
2017년	3.8	78	1.5	1,022	13.1
2016년	3.5	58	1.1	1,097	18.9
2015년	3.3	66	1.1	902	13.7

기술유출의 피해 유형은 경쟁사로의 기술유출(50.0%)과 내부직원의 기술유출(47.1%)이 많았으며, 그 다음으로 거래 관계에서의 기술유출(26.5%), 기술인력 유출(20.6%) 등의 순으로 나타나고 있다.

〈표 3〉 중소기업 기술유출 피해유형 (복수응답, 단위:(%))

구분	경쟁사로의 기술유출	거래관계에서의 기술유출	기술인력유출	내부직원의 기술유출	해킹 등으로 인한 피해
2018년	50.0	26.5	20.6	47.1	5.9
2017년	42.0	23.9	27.3	25.0	3.4
2016년	21.2	1.9	3.8	76.9	0.0
2015년	20.6	13.2	38.9	17.0	4.1

기술자료를 외부로 유출시킨 자는 전직원(퇴사자)이 91.2%로 가장 많이 나타났고 다음으로 현직원이 11.8%를 보이고 있다.

〈표 4〉 중소기업 기술유출시킨 관계자

구분	현직원(인턴, 임시직포함)	전직원 (퇴사자)	대기업 (납품관계)	협력업체 (하도급)	경쟁기업	용역업체
2018년	11.8	91.2	5.9	2.9	8.8	2.9
2017년	14.8	69.3	-	8.0	6.8	2.3
2016년	11.5	69.2	-	5.8	17.3	0.0
2015년	11.7	75.8	-	5.5	4.4	0.0

* 납품관계 대기업은 2018년 신규 보기항목임

기술자료의 유출수단으로는 휴대용 저장장치(USB, 외장하드 등)이 58.8%로 가장 많이 사용되었으며 다음으로 복사절취가 47.1%, 이메일이 20.6% 등으로 많이 사용되고 있다.

〈표 5〉 중소기업 기술자료 유출 수단

구분	복사 절취	이메일	해킹	휴대폰 저장장치	스카웃 매수	관계자 매수	기술교류
2018년	47.1	20.6	2.9	58.8	14.7	5.9	5.9
2017년	18.2	14.8	4.5	38.6	19.3	2.3	3.4
2016년	17.3	17.3	5.8	30.8	36.5	0.0	1.9
2015년	25.9	9.2	5.1	39.8	19.5	0.0	3.0

기술유출 방생 이후 내부적으로 취한 조치는 보안관리 강화와 직원 보안욕육 강화가 가장 많았고, 다음으로 보안장치 설치강화 순으로 나타나고 있다.

〈표 6〉 중소기업 기술유출 현황

구분	보안관리 강화	보안장치 설치	직원교육	사후조치 않음	기타
2018년	47.1	17.6	41.2	14.7	5.9
2017년	26.1	9.1	39.8	45.5	4.5
2016년	40.4	19.2	61.5	5.8	0.0
2015년	67.7	25.1	23.4	16.0	1.9

* 보안관리강화 : 자료관리, 출입자 통제 등 관리 강화를 뜻함

중소기업에서 유출사고가 발생하는 주된 이유는 보안관리감독체계 미흡이 44.4%로 가장 높고, 다음으로 임직원 보안의식 부족이 35.9%, 보안투자미흡이 24.5% 순으로 나타나고 있다.

〈표 7〉 중소기업 기술 유출 사고발생 주된 이유

구분	보안관리 감독체계 미흡	보안 투자 미흡	임직원보안 의식 부족	임직원금전 이익 추구	회사 처우 불만	보안 전임자 부재	회사운영난 따른 감원 등 직업 불안정	기타
2018년	44.4	24.5	35.9	20.2	17.0	14.5	5.9	0.3
2017년	46.5	11.6	23.5	5.1	3.1	3.8	3.0	1.5
2016년	45.8	26.5	43.1	20.2	11.9	6.9	21.0	0.0
2015년	47.9	26.0	36.7	14.4	15.4	14.8	7.8	1.0

3. 대중소기업의 상생을 위한 중소협력업체 보안인증제도 도입의 필요성

최근 주요 고객사인 대기업(이하 '대기업')과 중소기업인 협력업체(이하 '협력업체') 간 기술정보 및 IT시스템 공유가 증가함에 따라 대기업의 기술정보 또는 영업비밀 등이 협력업체를 통해 유출되는 일이 빈번히 발생하고 있어 대기업의 정보보호는 물론이고 협력업체 전반의 보안수준을 향상시키고 정형화하여 안정화된 협력업체 보안관리 체계를 구축하므로써 동반성장과 상생협력의 기초를 마련해야 할 시점이다.

대기업에 비하여 협력업체의 보안사고 비율은 월등히 높게 나타나고 있고, 유출사고의 발생은 협력업체 정보 뿐 아니라 고객사인 대기업의 정보까지도 포함되어 있어 협력업체의 정보유출은 곧 산업계 전체 이미지와 신뢰도가 추락할 수도 있는 실정이다. 특히 정보자산 및 시스템의 대량화와 복잡화 등으로 협력업체와의 전략적 제휴

에 따른 정보교환은 증가되고 있으며, 정보시스템의 사무의존도도 극대화되고 있고 유출에 대한 위험은 상존하고 있다고 해도 과언이 아닐 것이다. 더불어 정보보호 관련 법률의 개정과 제정은 물론 대내외 이해관계자의 보안요구 사항은 높아지고 있는 실정이다.

따라서, 고객사인 대기업이 중소기업인 협력업체에 대해 관리적, 물리적, 기술적 보안성 검증을 시행할 수 있는 권한을 명시하고 이행하여 협력업체가 적정한 보안수준을 지속적으로 유지할 수 있도록 유도함으로써 협력업체를 통한 대기업의 설계 및 기술자료 등의 유출방지는 물론 협력업체 자체의 보안수준 향상에 기여하는 등 지적재산권 보호가 반드시 필요한 상황이다.

Ⅲ. 보안평가에 대한 선행연구 및 선행평가 모형

우선적으로 대기업을 고객사로 두고 있는 중소협력업체의 보안평가모형을 개발하기 위하여 어떤 항목을 평가하고, 어떤 가점을 부여하여야 하는지를 규정하여야 한다. 이를 위해 기존 제도나 실태조사 항목 등을 살펴보았다.

1. ISMS

1) 개요

국내 정보보호 관리체계로써 'ISO27001'과 유사하지만 국내환경에 맞게 적용한 정보보호 관리체계로써 '기업이 주요정보자산을 보호하기 위해 수립, 관리, 운영하는 정보보호관리체계가 기준에 적합한지를 심사하여 인증을 부여하는 제도'로써 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법') 제47조 및 시행령 제47조~54조에 근거하고 있다. K-ISMS는 기업(조직)이 각종의 위험으로부터 주요 정보자산을 보호하기 위해 수립、관리、운영하는 종합적인 관리체계(정보보호 관리체계)의 적합성에 대해 인증을 부여하는 제도이다. 2001년부터 제도가 도입 되어, 2002년부터 인증서 발급되기 시작되었다. 2018년 12월 현재 ISMS 인증기관은 한국인터넷진흥원(KISA)이며, 인증심사기관은 한국정보통신진흥협회(KAIT)와 한국정보통신기술협회 (TTA), 금융보안원(FSI) 등 3개 기관이다.

2) 인증대상자

정보보호 관리체계를 구축, 운영하는 기관(기업)은 의무 대상이 아니더라도 인증 취득을 희망하는 경우 자발적으로 신청하여 인증 취득이 가능하고, 정보통신망법 제47조2항에 의하면 인증 의무대상자를 아래와 같이 정하고 있다. 이를 어길 경우 동법 제76조의 의거하여 3,000만원 이하의 과태료를 부과하도록 하고 있다.

〈표 8〉 정보보호관리체계 구축 운영 의무대상자

전기통신사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자	인터넷접속서비스, 인터넷전화서비스 등	서울 및 모든 광역시에서 정보통신망 서비스 제공
집적된 정보통신 시설을 운영 관리하는 사업자	서버호스팅, 코로케이션 서비스 등	정보통신서비스부문 전년도 매출액 100억 이하인 영세 VIDC 제외
연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 매출액 100억 또는 이용자수 100만명 이상인 사업자	인터넷쇼핑몰, 포털, 게임, 예약, 케이블-SO 등	정보통신서비스부문 전년도 매출액 100억 이상 또는 전년도말 기준 직전 3개월간 일일평균 이용자수100만명 이상
	상급종합병원, 대학교	직적연도 12월31일 기준 재학생 수가 1만명 이상인 대학교

3) 인증 혜택

ISMS 인증취득시 혜택으로는 아래 표와 같다.

〈표 9〉 ISMS 인증 취득시 혜택

구분	시행기관	혜택
평가 항목	과학기술정보통신부	공공부문 정보시스템기획·구축·운영 사업자, SW개발사업자 선정 시 '소프트웨어 기술성 평가 기준'의 평가항목(기밀보안)에 ISMS 인증취득시 만점(최대5점)부여
		보안관제 전문업체 지정시 '보안관제수행능력평가기준'의 정보보호 인증기업(보안관리체계 보유기업)항목에 만점(최대5점)부여
		정보보호 전문 서비스 기업 지정시 '업무수행 능력심사 세부평가 기준'의 정보보호 인증기업(보안관리체계 보유기업)항목에만점(최대5 점)부여
	2015 KISA	정보보호대상 평가 시 가점 부여
	한국기업지배구조원	상장기업대상 ESG(환경, 사회, 지배구조)평가 일부항목 대체

구분	시행기관	혜택
요금 할인	보험사	정보보호 관련 보험(배상책임보험 등)가입시 할인
권고	국토교통부	유비쿼터스 도시 기반 시설에 대해 정보보호 관리체계(ISMS)인증취득을 권고
	교육부	사이버 대학에 대하여 정보보호 관리체계 인증의 취득을 권고
ISMS 인증 수수료 할인	KISA	중소기업 기업 할인(매출액 100억 미만, 30%)

4) ISMS-P

ISMS-P 인증은 기존 ISMS와 PIMS의 통합으로써 정보보호 및 개인정보보호관리체계인증이라는 명칭으로 기존 정보통신망법 제47조의 3(과학기술정보통신부)과 개인정보보호법 제32조의 2(행정안전부)의 통합인증이라고 할 수 있으며 2018년 11월7일자로 시행되기 시작하였다.

2. ISO/IEC 27001 국제 표준

ISO 27001 인증은 국제표준 정보보안 경영시스템으로 정보보안 분야에서 가장 권위 있는 인증으로, 조직 전체적인 비즈니스 위험 환경 내에서 문서화된 ISMS를 수립, 구현, 운영, 모니터링, 검토, 유지 및 개선하기 위한 요구사항을 규정한다. 또한 이 규격은 개별 조직 또는 조직 일부의 요구에 따른 보안통제의 구현을 위한 요구사항을 규정한다. ISO 27001은 영국 BSI인증원의 BS7799 규격을 따르며 PDCA 모델 개념에 따라 ISMS 시스템 구축과 실행, 그리고 지속적 향상 달성을 위한 요구사항으로 구성되어 있다. P단계에서는 ISMS 수립 및 관리, D단계에서는 ISMS 구현 및 운영, C단계는 ISMS 모니터 및 검토, A단계는 ISMS 유지 및 개선의 단계별 활동으로 구성되어 있다. ISO 27001은 정보보호 관리과정 4개의 도메인과 Annex 14개 도메인 114개 세부 통제항목으로 구성되어 있고, 6개월 주기의 사후심사, 3년 주기 재심사를 진행하여야 한다. ISO 27001의 관리항목은 <표 10>과 같다.

〈표 10〉 ISO27001 관리항목

Annex	비고
Information security policies	보안정책의 경영진 승인, 효과성
Organization of information security	내부조직, 모바일기기 및 원격근무
Human resource security	고용전, 재직중, 고용후
Asset management	자산책임, 정보분류, 매체관리
Access control	접근제어, 사용자 관리 및 책임
Cryptography	암호화제어
Physical and environmental security	보안영역,보호설비
Operations security	운영절차와 책임, 악성코드, 백업등
Communications security	네트워크보안, 정보전송
System acquisition, development and maintenance	시스템보안 요구사항, 개발지원보안
Supplier relationships	공급업체와 정보보호
Information security incident management	정보보안 사고와 개선
Information security aspects of business continuity management	정보보안 연속성, 중복성
Compliance	법률 및 계약요구사항 준수

3. 산업기술보호지침 자가진단표

산업기술유출방지법에 근거하여 마련된 산업기술보호지침 및 매뉴얼(2017)에 의하면 산업기술의 보호수준을 측정하는 자가진단표는 총 5개 영역으로 질문을 통해 진단이 필요한 사항이 무엇인지 알 수 있도록 하고 있다. 각각의 답에 점수가 부여되어 있으며 점수들의 총합은 대상기관의 산업기술 보호수준을 알 수 있는 지표로 사용된다. 자가진단표의 점수는 다음과 같이 매겨진다.

〈표 11〉 산업기술보호지침 자가진단표 점수 기준

구 분	내 용
우수 수준(10점)	보안에 대한 취약한 부분이 없으며, 산업기술을 보호하기 위한 현행 노력을 지속하면 산업기술의 유출 및 침해사고 발생에 대한 피해가 없는 수준이다.
양호 수준(8점)	보안에 대한 점검 및 취약성이 거의 없지만, 유출 및 침해의 가능성이 내재해 있는 수준이다.
보통 수준(6점)	회사 차원의 보안업무가 나름대로 시행되어 왔으나 전문적인 진단과 조치가 필요하다.
미흡 수준(4점)	산업기술의 유출 및 침해에 따라 심각한 피해를 가져올 수 있는 수준이다.
위험 수준(2점)	보안에 대해 심각한 결점 및 취약성이 상존하며, 보유한 주요 산업기술은 이미 공개되었다고 생각해도 무방한 수준이다.

세부적 자가진단 리스트의 항목과 점수분포는 다음 표와 같다

〈표 12〉 산업기술보호지침 자가진단 리스트 점수 분포

구분	대분류	중분류	내용	점수
운영	규정지침	제개정	규정/지침 정책반영 여부, 승인여부, 공지배포	50
		검토	환경변화시 규정의 지침 검토 실시	20
	조직	회의	실무협의회 운영여부	20
		부서	부서의 존재와 업무분담	20
자산	문서	등급	등급분류 및 부여	20
		접근	열람기록 및 반출입 승인	20
		관리	비밀문서 관리, 세단기사용, 문서방치여부	40
	자재	점검	보안자재 보유 및 주기확인여부	30
		관리	보안자재 취급 관리책임	40
	인력	계약	고용계, 보안서약, 신원조회	40
		교육	교육정책 및 주기적 실시여부	20
		퇴직	퇴사자의 책임, 반납절차, 동향파악 여부	30
		관리	외부인력 신원확인, 인사이동 후 변경조치	40
	시설	접근	시설분류, 보호구역 출입통제, 휴대물품	50
		장비	CCTV, 화재 및 누수여부	50
		관리	구역설정 관리, 출입자 로그관리	50
IT	전산	프로그램	운영체계 및 보안업데이트	20
		보호	비밀번호변경, 화면보호기 작동여부	40
		대비	외부수리의뢰시 보안대책 등	30
		자료	서버 내 저장자료 중요도에 따른 권한설정	20
		관리	저장장치 폐기 및 반출입 승인관리	40
	네트워크	통신망	내외부 통신망 분리	30
		점검	무선네트워크, 인터넷 보안성 검토	50
외부	계약		계약시 보안관련 절차, 권리설정	60
	해외진출		정보보호예산, 준수사항, 점검사항, 교육	50
사고대응	사고대응	교육	보안취약점 등 절차 교육	20
		외부	사이버 위협정보, 탐지기술 공유	40
		관리	보안관제센터 운영, 모의훈련	60
합계				1,000

※ 200점 미만(위험), 400점 미만(미흡), 600점 미만(보통), 800점 미만(양호), 800점 이상(우수)

4. 국가핵심기술 실태조사 배점 기준

평가 모형의 개발을 위하여 정부에서 범용하고 있는 국가핵심기술 평가 모형을 살펴보면, 전반적으로 관리적 보안 점수(50점)에 치중하고 나머지 영역인 물리적 보안 점수(8점), 기술적 보안 점수(30점), 기타 점수(12점)로 배점기준을 정하여 조사하고 있는 실정이다(표3). 이는 보안정책 및 인원관리, 조직관리, 문서관리 등 관리부문의 중요성을 의미함을 알 수 있다.

〈표 13〉 '10 국가핵심기술 실태조사 배점기준

구분 \ 설문영역	배점	항목
1. 보호등급 및 보안정책	20점	자가진단법활용여부, 기술관련 보안규정 운영여부, 보안규정의 활용 정도 등 7개 영역
2. 인적 자원 관리	30점	보호업무 담당조직유형, 부서책임자 직급, 직급별 인지, 보안교육실시등 10개 영역
3. 주요 보호 시설관리	8점	보호구역 지정영부, 관리주체, 주요 시설에 대한 정도, 시설 및 장비 활용등 5개 영역
4. IT관련 S/W 및 H/W	17점	규정의 보유유무, 통신망 분리운영, 접근법위, 주기적 확인 등 7개 영역
5. 정보처리 및 자료보안	13점	정보시스템 처리규정, 권한 관리, 운영솔루션 유형 등 5개 영역
6. 유출사고 대응 영역	12점	기술유출여부, 대응방안의 유무, 대처방안에 체계성 등 5개 영역
총점	100점	

5. 영업비밀보호센터의 보안측정지표 배점 기준

국내기업의 영업비밀보호 주무기관인 특허청 산하기관인 영업비밀보호센터의 보안 측정지표에서도 관리적 보안이 65점의 가중치를 부여하고 나머지 물리적 보안과 기술적 보안은 총 35점으로 관리 보안의 중요성을 강조한다고 할 수 있다.

〈표 14〉 영업비밀보호센터 보안측정지표

항 목		배점	내 용
관리적 보안 - 정책 관리		20	접근제한 정책, 교육, 경영자태도, 규정준수 및 감사활동, 관리조직 및 운영, 홍보물통제
관리적 보안 - 취급 관리		20	비밀등록 및 표시, 보관, 생성 및 취급이력, 열람 및 사용, 복사인쇄, 반출절차, 폐기
관리적 보안 - 인적 관리		25	서약서, 협력업체, 퇴직자, 징계절차
물리적 관리		20	통제구역, 출입절차, 감시장치, 기기반출입
기술적 관리		15	서버 및 DB, 방화벽, 전자기록매체, 전자문서, 패스워드, 화면보호기, 망분리, 로그기록
계		100	
보안 등급 산정 기준			
A 등급	80점 이상	양호	보안관리체계를 잘 구비하고 이행하고 있음
B 등급	71-80 점	보통	유출시 법적으로 보호받을 정도로 이행하고 있지만 유출방지 대책은 보통임
C 등급	61-70 점	취약	유출시 법적으로 보호받기 다소 미흡하고 유출에 취약하므로 관리체계구축 필요
D 등급	41-60 점	위험	유출시 법적으로 보호가 어렵고, 유출 위험에 상시 노출되어 있어 시급한 관리체계 구축이 필요함
F 등급	40점 이하	무관심	상시 유출에 노출

6. 정보보호준비도평가(SECU-STAR) 자가 진단

기업의 통합적인 정보보호 수준을 향상시키기 위하여 정보보호 준비도 수준을 자율적으로 진단받을 수 있는 제도로 '정보보호 준비도 평가'등급을 해당 기업 전체 등급으로 부여하여 이용자에게는 기업 선택의 기준을 제공하고, 정보보호 활성화 및 투자 확대를 유도하는 목적으로 세부평가기준은 다음과 같다.

〈표 15〉 정보보호 준비도 자가진단표

NO	항목	평가 점수	
1	정보보호 리더십	· 정보보호최고책임자 지정 · 의사소통 · 운영방침	14점
2	정보보호 자원관리	· 정보보호 추진계획 · 인력 및 조직 · 예산수립 및 집행 · 이행점검	16점

NO	항목	평가 점수	
3	관리적 보안	· 교육의 수행 · 자산관리 · 인적보안 · 외부자 보안	18점
4	물리적 보안	· 시설환경 보안 · 출입관리 · 사무실 보안	12점
5	기술적 보안	· 취약점 점검 · 사고탐지 및 대응 · 시스템 개발 보안 · 네트워크 보안 · 정보시스템 및 응용프로그램 인증 · 자료유출방지 · 시스템 및 서비스 운영 보안 · 백업 및 IT 재해 복구 · PC 및 모바일 기기 보안	40점
합계			100점

* 100~90점(AAA), 89~80점(AA), 79~60(A), 59~40(BB), 39~23(B)

7. 중소기업 기술보호 역량 측정

기술보호 역량 측정모형(2018년)과 중소기업 기술보호 수준 측정개선(안)을 살려보면 아래표와 같다.

〈표 16〉 2019년 중소기업 기술보호 수준 실태조사 개선 최종보고서

2018년 기술보호역량 측정 모형			신규 중소기업 기술보호 수준 측정 개선(안)			
분야	설문문항수	분야별 배점	영역		세부영역	
			구분	배점	구분	배점
보안정책수립 및 집행	8개	30점	정책	46점	정책 수립 및 운영	34점
					정책관리	12점
보안관리	13개	45점	관리보안	25점	인력관리	15점
					외부자관리	10점
인력관리	8개	20점	물리보안	9점	자산및장비관리	4.5점
					출입통제	4.5점

2018년 기술보호역량 측정 모형			신규 중소기업 기술보호 수준 측정 개선(안)			
분야	설문문항수	분야별 배점	영역		세부영역	
			구분	배점	구분	배점
보안사고재해관리	2개	5점	기술보안	12점	운영관리	6점
					IT보안	6점
			사고,재해관리	8점	사고대응	6점
					재해관리	2점
총계		100좀	총계			100점

8. D사의 협력업체 보안인증 평가측정 적용사례

중소협력업체와의 시스템을 운영하고 있는 D사의 경우를 살펴보면, 협력업체의 보안평가 배점도 관리보안에 치중한 배점을 볼 수 있다.

〈표 17〉 D사 보안인증제도 배점 현황

분류	번호	점검항목	배점			판단근거
			우수	보통	미흡	
도면 및 기술자료 (40점)	1	도면관리규정	10	5	0	규정유무
	2	도면접수대장	10	5	0	대장유무
	3	담당자 지정	5	2.5	0	샘플링
	4	도면분류기준	5	2.5	0	시건여부
	5	도면 보관	5	2.5	0	분류기준
	6	사용자 관리	5	2.5	0	최신사용자
인적자원 (40점)	7	사내 담당자	5	2.5	0	조직도
	8	일일보안당직	5	2.5	0	당직일지
	9	보안점검 및 교육	10	5	0	교육자료
	10	입퇴사 서약서	10	5	0	서약서
	11	출입	5	2.5	0	규 및 및 대장
	12	관리규정	5	2.5	0	전산장비
기술보안 (15점)	13	PC계정관리	3	1.5	0	
	14	백신관리	3	1.5	0	
	15	화면보호기	3	1.5	0	
	16	보안패치	3	1.5	0	
	17	공유폴더	3	1.5	0	공유폴더
물리(5점)	18	출입감시장치	5	2.5	0	시설
총점			100			

Ⅳ. 보안인증제도 도입방안

1. 중소협력업체 보안현황 및 평가인증 배경

협력업체의 기술유출이 곧 고객사인 대기업의 경쟁력에 지대한 영향을 미치고 있는 것이 사실이다. 따라서 협력업체의 보안수준을 향상하는 것이 곧 대기업의 보안수준 향상이며, 나아가 중소기업 지원을 통해 함께 성장하는 문화의 하나로 보안이 진행되어야 한다.

2. 평가모형의 개발

선행연구 및 평가 모델을 종합하여 볼 때, 다양한 평가도구가 활용되고 있으나 대기업의 정보(설계도면 및 정보자료)를 활용하여 제작납품하거나 용역을 제공하는 중소협력업체의 평가 모형은 아직 그 사례를 찾아보기 어려웠다. 따라서 선행 평가모형들을 종합하여 아래와 같은 결론을 도출하기에 이르렀다.

〈표 18〉 중소 협력업체 평가모형(안)

영역	통제분야	통제항목	세부항목	필수/권유	점수	%
관리부문	1. 보보안관리체계	1.1 보안 조직	1.1.1	필 수	5	
		1.2 보안 정책	1.2.1	필 수	5	
	2. 보안계획및활동	2.1 보안계획	2.1.1	필 수	5	
		2.2 개인활동	2.2.1	필 수	5	
		2.3 보안점검	2.3.1	필 수	5	
	3. 정보자산통제	3.1 정보자산분류	3.1.1	필 수	5	
			3.1.2	필 수	5	

영역	통제분야	통제항목	세부항목	필수/권유	점수	%
		3.2 폐기	3.1.1	필 수	5	
	4. 인적보안	4.1 인원보안	4.1.1	필 수	5	
			4.1.2	필 수	5	
			4.1.3	필 수	5	
			4.1.4	필 수	5	
		4.2 보안교육	4.2.1	필 수	5	
			4.2.2	필 수	5	
	4개 분야, 9개 통제 항목, 14개 세부 통제 항목(필수 14개)				70	45.16%
물리 부문	5. 출입통제	5.1 출입관리	5.1.1	필 수	5	
			5.1.2	필 수	5	
	6.보호구역 및 관리	6.1 보안구역설정	6.1.1	필 수	5	
		6.2 접근 감시 추적	6.2.1	권 유	5	
	7. 반출입관리	7.1 반출입	7.1.1	필 수	5	
	3개 분야, 4개 통제 항목, 5개 세부 통제 항목 (필수 4개, 권유 1개)				25	16.13%
기술 부문	8. 사용자 기능	8.1 윈도우업데이트	8.1.1	필 수	5	
		8.2 바이러스 탐지	8.2.1	필 수	5	
			8.2.2	필 수	5	
	9. 시스템 컴퓨터	9.1 합관리	9.1.1	권 유	5	
		9.2 자료보호	9.2.1	필 수	5	
			9.2.2	필 수	5	
	10. 네트워크	10.1 공유자원관리	10.1.1	필 수	5	
		10.2 무선보안	10.2.1	권 유	5	
		10.3 예방통제	10.3.1	권 유	5	
			10.3.2	권 유	5	
	11. 서버관리	11.1 서버보안	11.1.1	권 유	5	
			11.1.2	권 유	5	
	4개 분야, 8개 통제 항목, 12개 세부 통제 항목 (필수 6개, 권유 6개)				60	38.71
합 계	11개 분야, 21개 통제 항목, 31개 세부 통제 항목 (필수24개, 권유 6개)				155	100%

단, 여기에서 중요한 것은 대기업에 비하여 중소협력업체는 자금력이나 전문인력 면에서 열악한 측면을 감안하여 기술적 보안분야에 대한 평가(38%)보다는 보안정책 및 경영자의 의지 등 관리적 보안 점수(45%)에 치중하여 가점을 부여하는 방식을

고려하여야 할 것이며, 특히 여러 가지의 보안 평가 모형들은 기업의 규모와 관계없이(사실상 대기업에 요구되는 항목임) 평가를 하고 있는 모형이지만, 중소협력업체의 보안인증을 위한 평가는 기초적인 보안 점검에 대한 평가받을 수 있는 평가 모형이 필요하다고 할 수 있다. 다만, 업무특성상 협력업체와 공동으로 프로젝트를 수행함에 있어 도면 및 기술자료를 공유할 수밖에 없기 때문에 보관, 활용 및 전송 시 외부로부터 보호하기 위한 기술적 보안 시스템 적용을 영업비밀보호센터 기준치(15%)로 낮추기에는 무리가 있어 30%의 가중치를 두었다.

협력업체 보안관리를 위해 정보보호 기초 생태계를 조성하는 것이 시급하며, 이를 위해 정보보호 교육 및 홍보, 규정 및 지침 정비 등 People, Process 측면의 기초 투자가 선행되어야 한다고 판단된다. 또한 협력업체들이 정보보호와 영업비밀 유출 사고 등에 대해 의식을 개선하고 공감할 수 있도록 가이드라인 및 홍보 자료, 교육 제공, 정기 점검(지도) 등을 통해 정보보호 상생협력 체계를 구축하는 데에 기여함이 바람직하며, 이 같은 대기업의 지원에 동참하여 중소협력업체에서도 정보보호 관련 정부의 지원제도(담당자 역량 강화, 장비 도입) 활용 등을 통해 자구 노력도 동반해야 한다고 판단된다.

3. 중소협력업체 보안 인증제도 도입 방안

1) 개요

국가핵심기술 실태조사(2010년)에 의하면 산업기술보호 정책의 우선순위에 대한 조사결과에서 산업기술보호 인증시스템 구축 및 지원에 대한 순위가 1순위로 답변(69.7%)한 것으로 나타난 것으로 보아 보안인증에 대한 수요는 물론 필요성을 공감하고 있다. 이에, 협력업체의 영업비밀과 기술정보 유출방지를 위해 최소한의 보안기준을 설정하고 객관적으로 평가하여 협력업체 보안 관리체계에 대한 수준과 적합성을 보증하기 위한 '협력업체 보안인증제도'를 권고하며 운영에 대한 모델을 제시하였다.

2) 도입 배경과 기대효과

협력업체의 자발적인 기술보호 노력 유도의 필요성과 고객사 정보(기술자료 및 영업비밀 자료 등)에 대한 보안이 필요하며, 특히 협력업체 전반의 보안수준 향상

유도를 위하여 대기업과 중소기업의 상생협력체계 구축을 통한 동반성장 기조에 발맞추어 나아가야 할 시점이다. 그러므로써 그간의 단편적, 일회성 대응체계에서 체계적, 지속적 보안관리체계를 수립하고 구축할 수 있으며, 부분적 보안에서 균형적 보안환경으로의 정착이 가능하며, 협력업체의 정보보호 자생력을 배양하고 나아가 보안사고를 예방하며, 사고 발생시 법적 근거자료 활용이 가능할 수 있다.

3) 대상 협력업체 선정 기준

인증대상업체의 선정 대상은 거래협력업체 중 기술 및 개발 용역 사업 유관 협력업체를 대상으로 할 수 있으며 아래와 같이 그 대상을 선별하여 우선 적용할 수 있을 것이다.

(1) 소기업, 중기업, 중견기업, 대기업 중 중기업 이상 협력업체 대상
(2) 협력업체 전체 매출 대비 매출비율 높은 순위로 대상 선정
(3) 보안사고 有경험 협력업체 및 발생가능성 잠재 협력업체
(4) 기타 대기업의 보안부서에서 지정한 협력업체

〈표 19〉 대상 협력업체 선정 기준 예시

평가항목	비중	중요도 평가 기준		
	(%)	10점	6점	3점
거래 비중	10	50% 이상	30% 이상	30% 미만
자료제공 형태	50	도면, 기술자료	경영, 마케팅	일반자료
사업장 규모	20	500명 이상	300명 이상	300명 미만
거래관계	10	출자한 협력업체	1차 협력업체	기타 협력업체
매출액(상위)	10	100억 이상	50억 이상	50억 미만

4) 보안평가 등급 및 인증

평가점수 산정방법은 보안 수준 평가 항목은 관리적 보안 부문 항목, 물리적 보안 부문 항목, 기술적 보안 부문 항목 등으로 구성되고 각 세부 평가 항목별로 보안관리 수준에 따라 1점부터 5점까지 5점 척도 기준으로 평가하여 합계점수를 산출하며 이 때 합계 점수는 백분율 점수이다.

〈표 20〉 평가등급 및 인증

구 분	보안수준 등급				비 고
A Class	A+	A0	A-	인증획득	ISO27001 국제 정보보호 표준인증 보유시 한전기술 보안부서 확인후 자동인증
	100	95이상	90이상		
B Class	B+	B0	B-		
	85이상	80이상	75이상		
C Class	C+	C0	C-		
	70이상	65이상	60이상		
D Class	D+	D0	D-		
	50이상	40이상	30이상		
E Class	E+	E0	E-	F	
	20이상	10이상	1이상	0	

5) 협력업체 보안 인증 구분

〈표 21〉 인증의 구분

구 분	내 용
최초 인증(Initial)	최초로 인증을 받는 경우
사후관리 인증(Surveillance)	인증 받은 협력업체의 보안관리 유지여부 평가 (1년 1회)
갱신 인증(Renewal)	· 인증범위 내에 중대 변화 (정보시스템의 중대한 변화, 사무실 이전 등) 발생하는 경우 실시 · 인증 유효기간 만료(3년)전에 유효기간의 연장 목적의 경우 실시

6) 운영 방법

(1) 평가 방법

선정된 보안관리 대상 협력업체에 인증제도 6개월 전 사전공지 → 실사평가 2주 전 고객사인 대기업에서 인증 평가전 평가 시트를 협력업체에 송부 → 협력업체 대표 또는 보안담당자가 자체평가 실시 → 평가 결과를 고객사인 대기업의 보안담당자에 통보 → 협력업체와 일정협의 후 보안담당자(또는 외부전문기관 의뢰) 현장방문실사 평가실시 → 최종평가 확정 및 협력업체 통보

(2) 등급판정 및 사후관리

인증 평가 결과를 <표 20> 상에 정의된 A+, A0, A-, B+, B0, B-, … 등의 결과로 표시하고 A- 이상 판정을 받은 협력사에 대해 인증을 부여함. 보안인증에 실패한

협력업체는 미흡한 점을 보완 후 6개월 이내 재평가를 의뢰할 수 있음. 국제 정보보호표준 ISO27001 인증 보유시 평가없이 자동인증 가능

(3) 인증실패에 대한 책임

보안인증에 실패한 협력업체가 인증을 포기하거나 재평가에서도 인증을 획득하지 못하면 고객사에서 보안 전문업체를 통한 보안교육 및 컨설팅 등의 지원을 고려하고 고객사의 지도, 지원에도 불구하고 협력업체의 자구 노력이 미미한 경우 거래제한 및 중단 등의 페널티 방안을 검토한다.

(4) 인증 유효기간

인증의 유효기간은 3년이며, 유효기간 만료 전 갱신인증을 받아야 인증의 효력이 유지되며 인증을 획득한 후 3년 미만 일지라도 정보시스템의 변화가 발생하였거나, 사무실 이전 등의 중대한 변화가 발생한 경우에도 갱인 인증을 받아야 한다.

(5) 인증의 취소

협력업체의 부도시, 사후관리 인증 거부시, 갱신 인증 거부시, 보안사고 발생 등과 같은 경우 인증을 취소할 수 있다.

4. 협력업체 인증 참여 동기부여 방안

기존 평가 모델 중에서 ISMS의 인증 취득시 여러 가지 혜택을 부여하여 인증참여를 유도하듯이 협력업체 보안인증에 따른 동기부여 방안을 아래와 같이 제시한다.

1) 용역 입찰시 가점부여 및 제약 완화 : A– 등급 이상

- 용역내용 및 규모, 기간 제한 없음
- 용역 착수 사전 보안성 검토 bypass 가능
- 자료폐기 점검 생략
- 협력업체 보안우수업체 포상 후보 등록

2) 용역 규모 한정 : A– 미만 ~ C– 등급 이상

- 용역 분야 및 내용, 기간 한정

- 용역 착수 사전 보안성 검토 必
- 자료폐기 점검 실시(실무부서, 보안부서 수시 점검)
- 보안관리 취약분야 개선대책 수립

3) 용역 계약 제한 : C- 미만

- 용역 입찰 참여 제한 및 계약 불가
- 계약이 불가피한 경우 인증획득 및 사고 책임 명시 계약
- 대체 업체 확보 및 양성

5. 협력업체 보안인증제 제도 도입 추진 방안

1) 도입기

본 제도의 도입시 최소한의 비용만을 투자하는 방식으로 기존의 시스템을 이용하여 상호 협력체계를 이루는 시기를 말한다.

- 보안관리 인증제도 및 대상 협력업체 선정 기준 정립
  : 핵심분야 또는 매출액 분야 우선 대상 선정
- 협력업체 보안관리 인증제 설명회 개최
- 협력업체 보안관리 애로점 파악 및 개선 방안 수립
- 협력업체 보안관리 인증제도 가이드 북 제작 배포
- 협력업체별 방문 보안점검 및 취약점 개선 권고
- 자가·실사 평가 일정 및 내용 확정
- 고객사 내부 규정 및 지침 개정(협력업체 보안관리)
- 평가실시 및 인증 부여

2) 정착기

본 제도의 운영시 기존 시스템 혹은 신규 시스템을 활용하여 중규모 이상의 투자를 하는 적절한 시기로 본 제도의 안정화 정도를 의미하며, 정보유출의 피해를 최소화하는 시기라 할 수 있다.

- 내부 규정 및 지침 업무 반영
- 전체 협력업체 규모, 매출, 업종, 형태별 세분화

- 세분화된 협력업체별 연도별 목표 보안수준 등급 설정
- 대상 협력업체 대폭 확대 및 신규 대상 협력업체 방문 설명회 실시
- 객관성 및 공정성 확보를 위해 보안전문업체 동반 실사 수행
- 기 인증 획득 협력업체 중 사후관리 인증 및 갱신 인증 심사 수행
- 보안 문화정착을 위한 뉴스레터, 포스터, 교육자료 지원
- 정부의 제도 활용 인력 역량강화 및 보안시스템 구축 지원

3) 고도화기

본 제도의 실행에 따른 전 협력업체의 시스템 구축을 통하여 철저한 실행계획을 기반으로 안전성을 구축하고 완료하는 단계이다.

- 지속적 대상 협력업체 확대
- 기 인증획득 협력업체 사후관리 인증 및 갱신 인증 심사 수행
- 최신 보안트렌드 및 사고사례 전파
- 기존 평가모형(점검표)에 미반영 ISO27001 통제항목을 추가하여 평가모형 고도화 추진
- 인증획득 협력업체 중 보안관리 우수업체 ISO27001 인증 권고

6. 기술적 보안에 대한 협력업체 인증 착안점

중소협력업체의 기술적 보안에 대한 이해 수준이 대체적으로 낮으며, 인프라 조차 부족한 실정이며 기술적 정보보호 활동에 대한 준비가 마련되어 있지 않아 위험에 항상 노출되어 있는 상태로 보호되어야 하는 비밀을 취급하기에는 적합하지 않다. 따라서, 고객사인 대기업에서는 보호되어야 할 기밀 정보의 취급이 필요한 협력관계의 경우 외부 협력업체의 정보보호 준비 수준을 검토하고 평가 수준에 따른 비밀 공유의 범위와 업무 형태를 결정하여야 한다.

기업 내 기밀정보의 유출사례는 매년 급증하고 있으며 기밀정보 유출로 인한 피해규모 또한 증가하고 있다. 대부분의 정보유출의 주체는 내부 전/현직 직원 및 협력업체 직원 등 정보에 대한 접근권한이 있는 사용자가 90% 가량을 차지한다고 보고되고 있어 이러한 정보유출의 피해사례를 예방하기 위해 대기업의 협력업무 환경에 맞는 최적의 보안 기술 환경을 제공함으로써 원천적으로 보안사고 예방환경을

구현하여야 한다.

이를 위해서는 모든 비밀 데이터는 가급적 대기업인 고객사의 인프라 및 서버에 보관이 되도록 하고, 모든 작업 기록은 저장 보관 될 수 있는 환경의 구현이 필요하다. 특히, 문서의 생성에서 사용과 폐기에 이르는 과정에서 정보의 흐름을 식별하고 생명주기에 맞춘 적절한 보호대책이 구현되어야 한다. 문서의 생성부터 유통에 대한 전 과정에 대해 조직과 협력업체 사용자 권한에 대한 통합관리가 이루어져야 하며, 실사과정을 통해 가장 취약한 부분으로 확인된 출력물 통제 및 매체 통제를 포함한 자료 유통에 대한 통제 구현은 기술적, 재정적, 인적 분야에서 열악한 협력업체에서 자체적으로 보안대책을 구현하도록 하기보다는 중앙 통제가 가능한 대기업 고객사에서의 환경의 구현과 제공이 필요하다. 따라서 과도한 협력업체 대한 부담을 줄이고, 지원형식의 보안인증 제도로의 발전이 필요하다고 할 수 있다.

7. 보안인증을 위한 협력업체 지원

대중소기업 간의 상호 대등한 관계하에서의 인증제도는 오히려 우월적 지위를 이용한 횡포로 여겨질 수 있는 여지가 충분하고 실제 그런 오해로 인하여 문제가 야기된 경우도 나타나고 있다. 따라서 고객사인 대기업은 호혜와 평등에 입각하여 보안인증제도를 도입하고 정착하여야 할 것이며, 이는 어느 한쪽에서의 이익만을 위한 일방통행식의 제도여서는 도입취지에 맞지 않을 것이다. 따라서 아래와 같은 협력업체에 대한 보안관련 지원사업에도 게을리 하지 말아야 할 것이다.

1) 협력업체 보안 상생 이벤트 지원 : 보안선포식 및 선언문 낭독 등을 통하여 상생협력 및 공동체로서의 자부심과 노력으로 지속적인 보안활동을 전개하며 노력하고 자율적인 보안문화 확산을 실천하는 선언식 형태의 지원
2) 보안문화 홍보 및 정착을 위한 공모전 개최 지원 : 협력업체 임직원을 대상으로 보안표어, 포스터 및 아이디어 제안 공모 등을 통하여 포상하여 함께 참여할 수 있는 계기를 마련하는 지원
3) 협력업체 Best Practice 선정 지원 : 우수 협력업체에 대하여 포상하고 사례집을 발간하여 협력업체에 배포하고 보안문화 확산 및 인식제고 노력
4) 보안교육 지원 : 보안교육 및 보안교육비 지원
5) 보안관리 노하우 전수 : 보안 멘토링 및 자문 지원(규정, 지침 등)

6) 홍보자료 지원 : 보안영역별 가이드북 제작 및 배포
7) 기초 보안 자문 지원 : 고객사 대기업의 보안담당부서 또는 보안전문업체 등에 위탁하여 희망하는 협력업체에 방문하여 1~3일간의 기초적인 보안 컨설팅 지원
8) 정보보호인증 지원 : 인증 노하우 전수 및 인증비 지원

Ⅴ. 결론 및 제언

1. 결론

본 연구는 대기업을 고객사 가지고 있는 중소 협력업체의 보안인증제도 도입을 위한 평가모형과 도입절차에 대한 방안을 제시하였다. 그간 대기업은 독자적인 정보보호체계 구축에 노력은 하여 왔으나 실제 산업구조는 수많은 중소협력업체의 기술과 노하우가 없이는 사업목적 달성이 불가능하며, 특히 고객사인 대기업의 기술과 데이터 등의 정보제공으로 협력업체가 제작하여 완성 제품으로 공급하는 형태로 이어지고 있으므로 협력업체의 정보보호 필요성은 그 중요성이 강조되지 않을 수 없는 실정이다.

그러나 우리나라 중소협력업체 대부분은 상대적으로 열악한 노동환경과 재무환경 등으로 정보보호에 대한 투자나 관심은 저조하여 유출의 심각성은 더해지고 있어 자사정보는 물론이고 고객사인 대기업의 기술정보 마저도 위협받고 있어 이에 대한 개선을 통하여 정보보호의 수준을 한단계 높일 수 있는 방안이 모색되어야 하는 시점이다.

이에, 협력업체의 보안인증 제도 도입을 통하여 중소협력업체에 대한 정보보호 업무 활동 지원의 계기를 마련하고, 고객사의 기술자료 유출 등 보안사고를 예방함은 물론 협력업체 임직원의 보안에 대한 중요성을 인식하는 계기를 마련하고, 나아가 협력업체 별로 보안활동을 통하여 보안사고 예방은 물론이고 보안사고 발생 시 법적 조치를 위한 근거자료 활용이 가능해지는 등 협력업체의 보안수준 향상에 크게 기여할 수 있을 것으로 판단된다.

2. 제언

본 연구는 협력업체 입장에서는 자칫 우월적 지위에 있는 '갑'의 일방적인 강제성으로 받아들이지 않도록 충분한 홍보가 필요하며, 보안측정의 공정성 문제가 야기될 수도 있어 주요 협력업체에게 공정하게 적용하기 위하여는 기존의 보안조직으로 운영, 유지하기에는 인적자원, 노하우 및 소요예산 등의 어려움이 수반될 수 있는 만큼 제3의 보안전문업체에 일부 또는 전부를 위탁하여 운영하는 등 제3자 평가(Third Party Assessment)방법을 통해 공정한 평가를 유도하여야 한다.

본 인증제도의 성공적인 수행을 위하여는 고객사인 대기업의 전향적인 자세가 우선시 되어야 하며 제도의 도입기 → 정착기 →고도화기 등의 체계적 발전 단계 적용 등 점진적 고도화로 발전시켜 나아가는데 고객사가 주도적으로 지원 성격을 유지하여야 할 것이다. 또한 인증제의 성격상 점수화하여 미달업체에 대해 불이익을 주기 위한 제도의 도입보다는 우수업체(Best Practice)에 대한 지원과 관심을 통하여 동화될 수 있는 분위기 조성이 필요하고, 성공적인 과제의 구현을 위하여는 협력업체 보안체계 구축을 위한 전담팀(또는 전담인력) 및 예산확보가 필요하고, 특히 공정한 제도의 운영 및 정착과 협력업체의 오해를 불식시키기 위해서 별도 보안전문업체에 위탁 운영하는 것이 바람직하다고 할 수 있을 것이다. 또한 인증제도가 시행될 경우, 최종적으로 인증 수준이 높은 것이 기술이 유출되지 않는다고 보장하지는 않는다는 점을 간과하여서는 안 될 것이며, 인증을 위한 수준평가 결과로써 기업의 보호 요소를 진단하여 개선방향을 권고 할 수 있는 것이며, 장기적으로 기업의 기술보호 수준을 향상시키는 효과를 얻을 수 있을 것으로 예상된다.

참고문헌

1. 논문

고형석 (2016). 정보보호인증제도의 확대에 관한 연구. **법과정책연구**, 16(2), 411-441.

공희경, 전효정, 이송하, 강민성, 김태성 (2016). 보안인증의 경제적 효과에 대한 연구동향 분석: ISMS를 중심으로. **정보보호학회논문지**, 26(3), 821-835.

김지성 (2018). 생태계기반 대중소기업 상생협력방안: 삼성전자 사례를 중심으로. **로지스틱연구**, 26(1), 95-112.

김진민, 박광태 (2014). 대기업과 중소기업의 협력을 위한 성공요인. **한국기업경영학회지**, 21(6), 25-38.

박성규, 김태성, 김진석, 유성재 (2018). 차세대 보안리더 양성프로그램의 성과평가 지표 개발. **정보보호학회논문지**, 28(2), 501-511.

송혁준 (2014). 국내대기업 상생협력 사례비교 및 시사점 도출. **한국경영학회 2014년 통합학술발표논문집**, 4149-4169.

안선주, 권순만 (2005). 의료기관의 정보보안 수준 측정을 위한 평가모형 개발. **한국병원경영학회지**, 10(4), 98-112.

오남석, 한영순, 엄찬왕, 오경석 (2011). 정보보호 수준평가 방법 개선에 관한 연구. **한국전자거래학회**, 16(2), 159-169.

유병홍, 김동원 (2012). 대중소기업상생협력 연구:LG전자 사례. **중소기업연구**, 34(1), 4-21.

이동현, 김성준 (2015). 정보보호인증심사 과정에 발생할 수 있는 피심사기관의 정보유출 방지대책. **한국산업보안연구**, 5(2), 141-165.

이종욱, 강명수, 송상연, 박지윤 (2016). 중소기업협력사 글로벌화와 기업가 정신: 동서발전 협력사 서베이자료를 중심으로. **한국경영학회 2016년 제18회 경영관련학회 통합학술대회**, 2091-2114.

장항배, 송지훈 (2009). 산업기술유출방지를 위한 보안시스템 평가 탐색적 연구. **한국산업보안연구**, 1(1), 50-61.

정세은, 정승일 (2013). 완성차 업체와 1차 대규모 협력업체와의 동반성장 실태 연구. **중소기업연구**, 35(2), 187-212.

최원녕, 김우제, 국광호 (2018). 기업의 정보보호활동의 효율성 평가. **융합보안**, 83, 25-32.

한도석, 염흥열 (2016). 산업보안에 특화된 정보보호 관리체계 제안. **한국산업보안연구**, 6(1), 153-154.

2. 기타자료

중소기업기술 보호 수준 실태조사 (2018)

중소기업 기술보호 수준 실태조사 개선 최종 보고서 (2019)

뉴데일리(2017). 삼성전자, 인력관리 협력사로 확대…"신입사원 입문교육 지원.
http://biz.newdaily.co.kr/news/article.html?no=10127355.

매일경제(2017). 협력사 손잡고 글로벌로 뛴다…삼성전자의 상생.
http://news.mk.co.kr/newsRead.php?&year=2017&no=199343.

중부일보(2016). 삼성전자, 470개 1차 협력사와 '소통의 장' 마련.
http://www.joongboo.com/?mod=news&act=articleView&idxno=1075640.

【Abstract】

Introduction of Security Certification System for Shared Growth and Co-prosperity of Small and Medium Businesses

Shin, Hyungoo

The damages from security accidents continue to increase as technology leaks from suppliers cause risks to the management of large companies, which are their customers, and their image and reliability to fall. However, the current industrial structure is practically impossible for large companies to form their own businesses and strategic alliances with business partners are essential, but it is changing into an industrial structure where the exchange of information is increased and the dependence of the information system is maximized, as well as legal demands and demands from stakeholders are increasing due to the complexity of the work process and the strengthening of security-related laws.

The status of technology protection of small and medium-sized enterprises shows that they are not equipped with a security system due to relatively poor environment and financial difficulties compared to large enterprises, whereas the industrial structure between large and small business partners is indispensable for sharing the IT system, and the security system of large business, which is a customer company, should be improved by considering the fact that it is impossible to maintain security system between large businesses. Thus, the government intends to examine the system for shared growth of small businesses and the model for evaluating the capabilities of various agencies for information protection, and propose measures to introduce the certification system for small business partners.

Keywords: Large and small businesses, Suppliers, Technology leaks, Security practices, Information protection certification systems, Security measures