석사학위논문

중소기업의 산업정보 유출사고에 관한 실증분석 연구

2021년

한성대학교 지식서비스&컨설팅대학원

스마트융합컨설팅학과

스마트융합보안컨설팅전공

고 찬 석

석 사 학 위 논 문
지도교수 장석은

중소기업의 산업정보 유출사고에 관한 실증분석 연구

An Empirical Analysis of Industrial Information Leakage Accidents in Small and Medium-sized Enterprises

2020년 12월 일

한성대학교 지식서비스&컨설팅대학원

스 마 트 융 합 컨 설 팅 학 과

스마트융합보안컨설팅전공

고 찬 석

석 사 학 위 논 문
지도교수 장석은

중소기업의 산업정보 유출사고에 관한 실증분석 연구

An Empirical Analysis of Industrial Information Leakage Accidents in Small and Medium-sized Enterprises

위 논문을 컨설팅학 석사학위 논문으로 제출함

2020년 12월 일

한성대학교 지식서비스&컨설팅대학원

스 마 트 융 합 컨 설 팅 학 과

스마트융합보안컨설팅전공

고 찬 석

고찬석의 컨설팅학 석사학위 논문을 인준함

2020년 12월 일

심사위원장 _____(인)

심사위원 _____(인)

심사위원 _____(인)

국 문 초 록

중소기업의 산업정보 유출사고에 관한 실증분석 연구

한성대학교 지식서비스&컨설팅대학원
스 마 트 융 합 컨 설 팅 학 과
스 마 트 융 합 보 안 컨 설 팅 전 공
고 찬 석

4차 산업혁명 시대의 도래와 함께 다양한 산업 분야 기술 발전으로 인한 IoT, 클라우드 등 정보사회 고도화로 산업정보 유출경로 및 유출정보의 범위가 확대되면서 각 기업의 고유한 기술력과 지식재산권이 중요시되고 있다. 기술 경쟁력이 곧 국가 경쟁력이라는 인식이 확대되면서 국내뿐만 아니라 전 세계적으로 각국의 지식재산 보호 강화에 주력하고 있으며 산업 경제에 상당히 중요한 부분을 차지하고 있다. 실제로 반도체, 디스플레이 산업과 같은 고부가가치를 창출하는 기술력을 토대로 우리나라의 산업이 세계적 시장에서 경쟁 우위를 점했고 이는 곧 경제 발전으로 이어졌다. 그러나 우리나라는 여전히 주요국 대비 지식재산 보호 수준이 낮은 것으로 평가되고 있으며, 기업의 기술력 및 영업비밀 등의 산업정보 유출 사례가 매년 증가하고 있다.

산업통상자원부에서 제공한 산업정보보안 역량 수준 실태조사 통계에 따르면 국내 중소기업의 정보보안 체계 및 중요 기술력 보호가 가장 취약한 것으로 확인되었다. 주요 문제점으로는 핵심기술 및 중요정보에 대해 체계적인 관리보호 미흡, 보안에 대한 인식과 역량 취약, 정보유출에 대해 신속한 대응 미흡, 정보유출에 대한 처벌수준 미흡 등이 있다. 대기업의 경우 지속적인 투

자를 통해 내부 보안 인프라 구성 및 관리를 체계화함으로써 산업정보 유출 사례가 감소하고 있지만, 중소기업의 경우 예산문제로 인한 보안 인프라 구성 및 보안전문 인력 투자가 어려워지면서 자연스럽게 산업정보보안에 관한 관심이 줄어들고 그로 인해 매년 산업기밀정보 유출사례가 증가하고 있다. 이러한 환경을 종합적으로 살펴보았을 때, 우리나라 국가 및 경제의 지속적인 성장을 위해서는 기업의 지식재산권이 유출되지 않도록 철저한 보호관리가 이루어져야 할 필요성이 있다.

본 연구는 산업정보 및 기술 유출 사고가 빈번하게 발생하고 있는 중소기업을 대상으로 연구를 진행하였다. 산업정보 유출 사고가 발생하는 사례를 살펴보고 중소기업에 적합한 산업정보 관리체계를 제시하였으며, 2018~2019년 사이에 수집한 데이터를 기반으로 산업정보 유출 실증분석을 진행하였다. 업종별 산업정보가 몇 건이 반출되었고 유출의심은 몇 건인지 수치를 나타냈으며 어떤 방법으로 유출 시도하였는지에 대한 결과를 도출하였다. 또한, 산업보안 관리체계와 접목해서 중소기업별 산업정보보안 관리구성 현황에 대한 평가지표를 명시하였다.

해당 연구 결과를 토대로 중소기업의 산업정보 및 핵심 기술정보를 물리적 보안영역 · 관리적 보안영역 · 기술적 보안영역 관점에서 체계적으로 구성하는 방안과 중소기업 분야별 산업정보 유출 실증분석을 통해 산업보안 가이드를 제시함으로써 산업정보 유출사고를 감소시킬 수 있도록 이바지하고자 한다.

【주요어】 지식재산권, 산업정보보안, 산업정보, 물리적 보안영역, 기술적 보안영역, 관리적 보안영역, 중소기업, 실증분석, 유출

목 차

표 목 차

그 림 목 차

제 1 장 서 론

제 1 절 연구 배경

산업정보가 국가의 핵심 경제자원으로 인식되면서 국가와 기업에서 산업정보 보안에 대한 중요성이 강조되고 있다. 산업보안이 기업의 주 경쟁력으로 급부상하면서 전 세계적으로 산업보안 인프라 구축과 전문 인력 양성에 많은 투자를 하고 있다. 국내 산업보안의 경우, 산업정보 및 첨단기술 유출 사고가 매년 꾸준히 증가하고 있다.

국내 산업기술보호 동향을 살펴보면 2010년 이후 산업정보 및 기술 유출 사고가 증가하고 있다. 국가정보원에서 제공한 산업스파이[1] 해외 유출 사고 적발 건수에 따르면 10~14년도에 229건이었으며 과거 대기업, IT 분야 중심에서 최근에는 중소기업, 정밀기계 분야까지 확대되었다. 산업정보 유출 사고는 중소기업 64%, 대기업 16%, 기타 연구기관 20% 비율로 발생했으며 주로 내부 임직원에 의한 기밀정보 유출이 80%를 차지했다(산업통상자원부, 2019).

이러한 산업기술 유출 사고의 발생은 국내의 여러 기업이 첨단 기술을 보유하고 막대한 예산과 인력을 투입하여 기술개발에 투자하고 있지만, 기술 개발에 관한 관심과 투자보다 산업기술 유출에 대한 대응능력, 보안의식 등 정보보호에 대한 투자가 상대적으로 많이 부족하기 때문이다. 우리나라 기업의 90% 이상의 비중을 차지하는 중소·중견기업은 대기업보다 보안에 대한 투자가 매우 부족하므로 더욱 산업기술 유출에 대한 사고는 지속해서 증가하고 있다(김광민, 2019).

대기업의 경우 예산투자와 법률적 규제를 통해 산업유출방지를 위한 시스템을 마련하여 운영하고 있다. 하지만 중소기업의 경우 산업보안 유출에 대한 위험과 위협은 느끼고 있으나 산업보안에 대한 인식 부족, 예산 등의 문제로 인해 산업기밀유출방지를 위한 대응방안이 부족하여 여러 방면에서 취약점을 가지고 있다(김태균, 2014).

특히 산업정보보안에 관한 인프라 및 관리체계가 열악한 중소기업은 산업정

1) 산업스파이 : 경쟁국이나 기업이 비밀로 관리하는 중요 산업정보를 부정한 목적과 수단으로 정탐하고 유출하는 일체의 행위를 하는 사람을 말한다(국가정보원, 2016).

보보안을 어떻게 받아들이는가가 향후 기업, 나아가 국가의 발전에 막대한 영향을 미친다는 점에서 산업보안 강화를 위해 어떠한 대응방안이 필요한지에 대한 연구가 필요하다(허재영, 2009).

중소기업의 산업보안은 건강한 산업의 생태계 조성 및 지식 기반 신산업 육성의 필수조건으로, 세계적으로 확대되는 신기술과 원천기술에 대한 보안에 대해서도 선제로 대응할 필요가 있다. 또한, 중소기업이 보유하는 기술은 해당 기업의 자산이며 기업 운영과 발전을 위해서도 그 보호가 필요하지만, 중소기업의 산업기술 보호 역량을 강화하여 안정적인 기술 개발 여건을 조성하고 기업의 기술 경쟁력을 제고 하여 관련 산업 발전과 나아가 국가 발전에 기여 한다는 점에서 지속적인 관리와 보호 그리고, 꾸준한 지원이 필요하다(이호준, 2020).

오늘날 우리는 첨단 지식정보 시대에 살고 있다. 산업정보는 중소기업의 존폐에 영향을 미칠 수 있으므로 산업보안의 중요성은 증대 될 수밖에 없다. 그러나 끊임없이 증가하는 수많은 산업기술 관련 정보들을 제대로 보호하고 관리한다는 것은 거의 불가능하므로 기업에서는 먼저 보호해야 할 대상과 그 관리범위를 먼저 정한 후 체계적이고 효율적인 보안체계가 정착될 수 있도록 각별한 관심과 노력을 기울여야 할 것이다(김중배, 2009).

제 2 절 연구 목적

산업정보보안을 강화하기 위해서는 과거에 국내에서 발생했던 산업정보 유출 사례에 대한 실태 분석을 통해 유출 사고가 발생한 원인을 파악해야 하며, 현업에서 실제로 얼마만큼의 산업정보가 반출되고 유출되고 있는지 실증분석을 통해 중소기업의 전반적인 산업보안에 대한 점검이 필요하다. 또한, 산업정보보안 관리 방안 프로세스 확립을 통해 산업정보 유출에 대한 대응방안 체계 마련이 필요하다.

본 연구에서는 대기업과 비교했을 시, 산업정보보안 수준 및 환경이 상대적으로 미흡한 국내 중소기업을 대상으로 연구를 진행했으며, 물리적 보안, 기술적 보안, 관리적 보안 영역으로 접근하여 중소기업에 적합한 산업보안 관리체계 구성 및 산업정보 유출 실증분석에 관한 연구를 진행하였다.

제1장에서는 산업정보보안에 관한 연구 배경 및 연구 목적을 정의하고자 한다.

제2장에서는 산업보안·산업기술에 대한 개념을 정의하고 산업정보보안의 필요성을 살펴보고자 하며 본 논문에서 연구하고자 하는 중소기업에 대한 정의와 중소기업 지식재산권 보호에 대한 개념을 정리하였다. 또한, 산업정보보안 관련 법률에 대한 정보를 명시하였다.

제3장에서는 국내 중소기업에서 발생한 산업정보 유출 현황 및 유출 사례에 대한 분석을 진행하였다.

제4장에서는 중소기업에 적합한 산업보안 관리체계를 구성하기 위해 물리적 보안·기술적 보안·관리적 보안 영역으로 접근하여 산업정보보안을 체계적으로 구성할 수 있도록 관리방안을 명시하였다.

제5장에서는 국내 중소기업 중 제조사, 서비스사를 대상으로 현업에서 수집한 데이터를 통해 산업정보 반출 및 유출의심 건에 대한 실증분석을 진행하였으며 산업보안 관리체계와 접목하여 산업정보보안 관리구성 현황에 대한 평가지표를 명시하였고 산업정보 유출 실증분석 결과를 도출하였다.

제6장에서는 본 논문의 결론 및 시사점과 연구의 한계점 및 향후 과제를 제시하였다.

제 2 장 이론적 배경

제 1 절 산업정보보안 개요

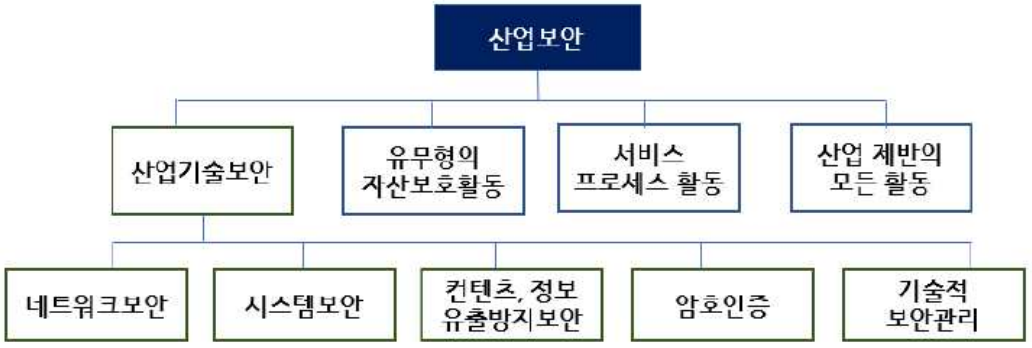
1) 산업보안 정의

산업보안이란 기업 활동을 위해 보호해야 할 인원·문서·시설·기술 등 산업정보의 침해 방지 및 외부로 유출되지 않도록 보호하는 활동이며 국가산업발전의 이윤을 위한 산업기술 및 각종 침해요소로부터 보호하는 자율적이고 예방의 조치를 말한다. 즉 기업이 보유한 기술·지적 재산·영업 비밀과 같은 산업기술을 보호하기 위해 정해진 목적 외에 사용하려는 내외부인으로부터 보호하는 것을 말한다(신현구, 2014).

세계적으로 산업보안의 중요성이 대두되면서 비교적 최근에서 보편화되고 사람들의 주목을 받게 되었다. 국가정보원에서 2013년 10월'산업기밀보호센터'가 설립되면서부터, 산업보안의 중요성이 점차 강조되면서 용어에 대한 정의와 개념이 일반에 알려지기 시작했고, 2016년 '산업기술의 유출방지 및 보호에 관한 법률'제정으로 인해 동법의 제18조와 제20조 등에 산업보안과 산업기술, 기술유출, 영업비밀 등의 법률용어로서 구체화 되었다. 주로 산업 분야 기술유출의 심각성이 문제도 대두되기 시작하면서, 산업보안이란 용어도 언론을 중심으로 사용되기 시작했다. 또한, 산업보안에 대한 국가적 차원에서 관심이 높아지면서 사회적 이슈로 나타났다(이호준, 2020).

산업보안은 정보보안, 물리보안, 융합보안으로 나눌 수 있으며, 3가지 보안을 합쳐서 통칭한다. 정보보안이란 사이버공간에서 이루어지는 정보유출 및 범죄행위로부터 보호하는 방법으로 보안솔루션, 네트워크 장비 등을 의미한다. 물리보안이란 출입통제, 기업자산 절도행위 등 물리적인 위협으로부터 보호하는 방법으로 CCTV, 임직원 인식카드, 자물쇠 등을 의미한다. 융합보안이란 정보보안 및 물리보안을 융합해서 네트워크 구성부터 시작하여 프로그램 개발, 정책 수립, 시스템 운영 등 산업보안을 통합으로 관리하는 것을 의미한다(허재영, 2009).

산업보안 구조는 아래의 [그림 2-1]을 통해 살펴볼 수 있다.



[그림 2-1] 산업보안 정의 (한국산업기술보호협회, 2016)

2) 산업기술 정의

산업기술이란 제품 또는 용역의 개발·생산·보급 및 사용에 필요한 제반 방법 내지 기술상의 정보를 말한다. “산업기술의 유출방지 및 보호에 관한 법률”의 최초 법률안을 살펴보면, ‘산업기술’의 정의에서 부정경쟁방지법상의 ‘영업비밀’에 대한 개념을 차용하여 “공연히 알려졌지 아니하고, 독립된 경제적 가치를 지니는 것으로서, 상당한 노력으로 비밀로 유지된 유무형의 기술정보” 라고 규정하였다. 이후 수정안에서 ‘산업기술’을 보다 추상적인 용어로 규정하되, 법 적용대상을 명확하게 확정하기 위해 산업발전법 제5조에 규정한 첨단기술, 국내에서 개발된 독창적인 기술로써 선진국 수준과 동등 또는 우수하고 산업화가 가능한 기술, 기존제품의 원가절감이나 성능 또는 품질을 현저하게 개선할 수 있는 기술, 기술적·경제적 파급효과가 커서 국가기술력 향상과 대외 경쟁력 강화에 이바지할 수 있는 기술, 위 기술의 응용 또는 활용기술, 기타 산업기술보호 위원회가 보호지원을 할 필요가 있다고 인정한 기술에 한하여 동법상의 보호를 받을 수 있도록 하고 있다(김중배, 2009).

중앙행정기관이 법령에 따라 지정·고시·인증하는 산업기술의 종류는 [표 2-1]과 같다.

[표 2-1] 지정·고시·인증하는 기술의 종류

기술종류	근거법률	기술의 정의	소관기관
첨단기술	산업발전법 (제5조)	기술집약도가 높고 기술혁신 속도가 빠른 기술로서 산업구조 고도화에 대한 기여도가 높으며 신규수요 및 부가가치 창출 효과, 산업간 연관 효과가 큰 기술	산업통상자원부 (고시)
고도기술	조세특례 제한법 (제18조)	국내에서의 개발수준이 낮거나 개발이 되지 아니한 기술로서 대통령령으로 정하는 기술	기획재정부 (지정)
신기술(1)	산업기술혁신 촉진법 (제15조의 2)	국내에서 최초로 개발된 기술 또는 기존 기술을 혁신적으로 개선·개량한 우수한 기술	산업통상자원부 (인증)
신기술(2)	환경기술 및 환경산업 지원법 (제7조)	국내에서 최초로 개발된 환경 분야 공법 기술과 그에 관련된 기술 또는 도입한 기술의 개량에 따른 새로운 환경 분야 공법기술과 그에 관련된 기술	환경부 (인증)
전략물자	대외무역법 (제19조)	대통령령으로 정하는 다자간 국제수출 통제체제에서 정하는 물품의 제조·개발 또는 사용 등에 관한 기술	산업통상자원부 (고시)
전력 신기술	전력기술 관리법 (제6조의2)	국내에서 최초로 개발한 전력기술이나 외국에서 도입하여 개량한 것으로서 국내에서 신규성·진보성 및 현장 적용성이 있다고 판단되는 전력기술	산업통상자원부 (고시)

부품소재 기술	부품·소재전문기업 등의 육성에 관한 특별조치법 (제2조)	상품의 제조에 사용되는 원재료 또는 중간 생산물 중 대통령령이 정하는 것	산업통상자원부 (고시)

※ 출처 : 이영일 (2012)

3) 산업정보보안의 필요성

오늘날 산업기술은 국가 및 국민경제에서 핵심요소라고 할 수 있다. 각종 산업기술을 통한 경제적 가치가 창출되고 있다. 고부가가치를 창출하는 산업기술로 인해 우리나라의 산업이 세계적으로 경쟁 우위를 지닐 수 있었고 국가 및 기업 발전에 이바지했으며 국민 경제를 활성화 시키는 원동력이 되었다. 이에 따라 경제적 가치의 관점에서 산업정보 및 산업기술은 우리나라 성장을 위해 중장기적 관점에서 최우선으로 관리되고 보호되어야 하는 요소이다. 첨단산업정보 및 기술을 보유하고 있는 중소기업의 경우 산업정보 유출사고가 증가하고 있다. 중소기업의 경우, 기업의 핵심기술에 대한 보호 및 관리체계가 대기업보다 상대적으로 부족하다. 실제로 중소기업청에서 실시한 조사에 따르면, 중소기업의 12.5%가 기술유출을 경험하였고, 건당 피해 금액은 2009년 10.2억 원에서 2012년 약 15.7억 원으로 증가한 것으로 나타났다. 중소기업 산업정보보호 정책 및 실태를 파악하고 정부의 지원을 통해 중소기업 산업보호 대책 마련이 시급하다(안성진, 2016).

이처럼 중소기업 산업정보 및 기술 유출에 대한 위협을 대비하기 위해 기업은 중요 지식자산에 대한 기술적·물리적·관리적 보안 관리체계의 수립이 필요하며, 기업의 보안관리 노력은 보안역량을 제고하는 방향으로 이루어지는 것이 바람직하다. 또한, 대기업보다 상대적으로 보안역량이 부족하고 비용에 투자하기 어려운 중소기업에 대한 정보보안 관리방안이 강화될 필요가 있으며 중소기업의 입장에서 필요한 부분을 보완하는 방식으로 이루어지는 것이 필요하다(김광민, 2019).

제 2 절 중소기업 개요

1) 중소기업 정의

국내의 중소기업을 구분하는 기준은 「중소기업 기본법」 제2조 및 동법 시행령 제3조에 상세하게 규정해 놓았다. 기업 중에서도 흔히 규모가 작은 사업장을 중소기업이라 부르며, 중소기업으로의 구분 대상은 영리를 목적으로 사업을 영위하는 기업이다. 즉, 개인사업자와 법인인 기업이다. 규모상의 기준과 독립성 기준 두 가지 모두 충족해야 중소기업에 해당하며, 우리나라 중소기업은 2017년 기준의 자료에서 전체 기업규모 중에서 99.9%를 차지하고 있고, 국내 기업 종사자 중의 89.8%가 일하고 있다. 중소기업은 상대적으로 투하자본이 적으며 결과적으로 독점이윤의 형성을 이룩하는 역할을 한다(이호준, 2020).

기업의 기준을 정의하는 매출액 기준은 [표 2-2]와 같다.

[표 2-2] 업종별 매출액 기준

<table>
<tr><th>분류</th><th>중소기업</th><th>중견기업</th><th>대기업</th></tr>
<tr><td rowspan="2">규모기준</td><td>주된 업종
3년 평균 매출액 기준</td><td>업종별 평균매출액 등이 규모 기준에 초과</td><td rowspan="4">상호출자 제한 기업 집단 또는 채무보증제한 기업집단 소속회사

자산총액 10조원 이상인 법인의 피출자기업</td></tr>
<tr><td>상한기준
자산총액 5천억 원 미만</td><td>자산총액 5천억원이상</td></tr>
<tr><td rowspan="3">독립성 기준</td><td>상호출자 제한기업 집단 또는 채무보증제한 기업집단이 아닐 것</td><td>좌동</td></tr>
<tr><td>자산총액 5천억 원 이상인 법인이 피 출자기업이 아닐 것</td><td>자산총액 10조원 이상인 법인의 피 출자기업이 아닐 것</td></tr>
<tr><td>관계기업의 경우 평균 매출액 등이 중소기업 규모 기준 충족하는 기업</td><td>관계기업의 경우 평균 매출액 등이 중소기업 규모 기준 초과하는 기업</td></tr>
</table>

소관	중소기업청 (정책총괄과)	중소기업청 (중견기업정책과)	공정거래위원회 등
확인방법	중소기업확인서	중소기업확인서	지정 및 통지 등
관련법률	중소기업 기본법	중견기업 성장촉진 및 경쟁력 강화에 관한 별법	공정거래법 등

※ 출처 : 중소벤처기업부 (2018)

2) 중소기업 지식재산권 보호

지식재산이란 무형자산을 의미하며 지식재산권이란 사람의 두뇌 활동을 통해 이루어진 무형적 이익을 독점적으로 이용할 수 있는 것을 의미한다. 지식재산권은 보호의 목적에 따라 산업발전에 이바지할 수 있는 창작물 등을 객체로 하는 권리인 산업재산권과 인간의 문화생활 향상에 이바지할 수 있는 창작물을 객체로 하는 권리인 저작권으로 구분된다. 산업재산권은 발명, 고안, 디자인, 상표 등을 보호하는 권리인 특허권, 실용신안권, 디자인권, 상표권으로 다시 분류할 수 있다. 대표적인 예로서, 반도체배치설계, 데이터베이스, 컴퓨터프로그램 등이 해당한다(고려대학교 세종산학협력단, 2020).

우리나라는 여전히 주요국 대비 중소기업 지식재산 보호 수준이 낮은 것으로 평가되고 있으며, 기업의 기밀·기술 등 영업비밀 유출 사례가 지속해서 증가하고 있다.

[표 2-3]을 통해 국내 중소기업의 기술보호 역량 수준을 살펴볼 수 있다.

[표 2-3] 기술보호 역량수준

구분	기술보호 역량수준		기술보안 담당인력	
	대기업	중소기업	대기업	중소기업
‘16	67.2점	49.3점	8.3명	1.0명
‘17	67.9점	51.3점	4.6명	2.0명
‘18	70.3점	44.9점	6.5명	2.0명

※ 출처 : 중소벤처기업부 (2018)

중소기업의 경우 기술분쟁이 발생하더라도 피해 사실 입증이 어렵고 손해배상액이 불충분하여 소송을 포기하는 예도 다수 발생한다. 하여 지식재산 침해 입증을 위한 증거확보 제도 개선, 손해배상제도 개선 등 민·형사 규제 강화가 필요하며 산업정보보호법에 근거하여 산업정보 유출에 대한 처벌을 강화해야 한다.

제 3 절 산업정보보안 관련 법률

1) 국내 산업보안 법률

국내의 산업기술 관련 법률은 국가핵심기술, 첨단기술, 신기술, 새로운 전력기술, 새로운 건설기술, 보건 신기술, 핵심 뿌리기술 및 그 밖의 법률 또는 해당 법률에서 위임한 명령에 따라 지정하는 기술 중 산업통상자원부 장관이 관보에 고시하는 기술로 규정되어 있다. 산업기술의 유출방지 및 보호에 관한 법률은 2006년 제정되어 국내 산업의 핵심기술 보호 및 국가 산업 경쟁력 강화에 목적을 두고 있으며, 2016년에 기술유출에 대한 형량 강화 등을 담아 개정되었다. 부정경경쟁방지 및 영업비밀보호에 관한 법률은 상표 및 상호와 관련한 부정경쟁이나 영업비밀 침해 등을 방지하기 위해 1998년 제정되었다. 그 밖에도 중소기업 보호지원에 관한 법률은 2014년 제정되어 중소기업의 기술보호와 중재를 지원하고 분쟁을 조정하는 등의 역할을 수행하고 있다(이호준, 2020).

[표 2-4]를 통해 주무부처별 중소기업 기술 법률 현황을 확인할 수 있다.

[표 2-4] 주무부처별 중소기업 기술 법률

법률 명	보호대상	주무부처
중소기업기술 보호 지원에 관한 법률	중소기업기술	중소벤처기업부
산업 기술의 유출방지 및 보호에 관한 법률	산업기술, 국가핵심기술	산업통상자원부
대·중소기업 상생 협력 촉진에 관한 법률	기술자료	중소벤처기업부

하도급 거래 공정화에 관한 법률	기술자료	공정거래위원회
부정 경쟁 방지 및 영업 비밀 보호에 관한 법률	영업비밀	특허청
대외무역법	전략물자	산업통상자원부
산업 발전법	첨단기술, 첨단제품	산업통상자원부
방위 산업 기술보호법	방위산업기술	산업통상자원부

※ 출처 : 이호준 (2020)

가) 부정경쟁방지 및 영업비밀보호에 관한 법률

기술발전과 사회·경제 구조 변화를 통한 경제적 가치를 창출할 수 있는 자산의 유형이 급증하고 있으며, 기존의 법질서로 규제하기 어려운 다양한 유형의 부정경쟁행위가 등장하고 있다. 이와 같은 다양한 유형의 부정한 경쟁행위를 효율적으로 규제할 수 있는 일반적이고 포괄적인 법적 근거를 마련해야 할 필요성이 대두되었다(이경환, 2016).

부정경쟁방지 및 영업비밀보호에 관한 법률(이하 영업비밀 보호법)은 상표법이나 특허법 등의 다른 산업재산권법이 미치지 않는 영역의 지적재산권까지 포함하는 지적재산권법의 일반법이라고 할 수 있다(윤선희, 2007).

1961년 12월 30일에 처음으로 제정되어 1962년 1월 1일 자로 시행된 법률로서 국내에 알려진 타인의 상표·상호 등을 부정하게 사용하는 부정경쟁행위와 타인의 영업비밀을 침해하는 행위를 방지하여 건전한 거래질서를 유지함을 목적으로 하는 법률이다. 이러한 부정경쟁방지법은 제정 이후 수차례 개정이 되었는데, 개정과 관련된 주요 내용은 다음과 같다(이형진, 2018).

우선, 영업비밀 침해행위에 대한 벌칙 규정이 개정되었다. 이와 관련하여 대표적으로 국외로의 영업비밀 유출에 대한 형량이 기존의 7년 이하에서 10년 이하로 강화되었다. 그리고 영업비밀 보호대상이 기존의 기업에서 영업비밀보유자로 확대되었다. 그리고 소송 과정에서 알게 된 영업 비밀을 부정 사용하거나 누설하는 행위를 막기 위해 부정경쟁방지법에 비밀유지명령제도를 도입하도록 하는 개정안 역시 2011년에 도입되었다. 그리고 최근에는 영업비밀 구성요건 중 비밀유지 관리 성이 완화되어 부정경쟁방지법을 통한 보호대상의 범위를 넓힐 수 있게 되었다(안성진, 2016).

나) 산업기술의 유출방지 및 보호에 관한 법률

산업기술보호법은 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내 산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지함을 목적으로 하는 법률로 2007년 4월에 제정되어 발효되었다.

이러한 산업기술보호법에 의거하여 산업기술보호위원회의 구성 및 운영을 통한 산업기술유출방지 종합계획, 산업기술 유출방지·보호, 기본 목표와 단계별 목표 및 추진방안, 홍보·교육, 기반구축, 기술개발, 정보수집 및 분석에 대한 시행계획이 수립되고 시행된다. 그리고 본 법률의 9조~11조를 통하여 국가핵심기술의 지정 및 매각·이전 등을 통한 수출 시, 사전승인 또는 사전신고 제도 도입과 관련된 사항을 명시하였다. 또한, 산업기술의 유출·침해 행위에 대한 징역·벌금형 등의 형사적 책임을 강화하고 산업기술분쟁조정제도가 운영될 수 있는 법적 근거를 제시하고 있다.

산업기술은 다음의 추가적인 요건 중 하나 이상을 만족하면 산업기술유출방지법의 보호대상이 될 수 있다. 산업기술유출방지법에 규정된 국가핵심기술을 살펴보면 국가핵심기술은 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장 잠재력이 높아 해외로 유출될 때 국가의 안전보장 및 국민경제의 발전에 심각한 악영향을 줄 우려가 있는 산업기술로서 지식경제부 장관이 관계 중앙행정기관의 장으로부터 그 소관의 국가핵심기술로 지정되어야 할 대상 기술을 통보받아 산업기술보호위원회의 심의에 의해 “국가핵심기술로 지정된 산업기술을 말한다”라고 되어 있다. 국가핵심기술로 지정되기 위해서는 국내·외적에서 기술적·경제적으로 경쟁력 있는 산업기술이거나 관련 산업의 성장 잠재력으로 인해 장래에는 특별한 가치를 갖게 될 것으로 여겨지는 산업기술이어야 하며, 해외유출 시 국익에 심각한 악영향을 줄 우려가 있는 산업기술도 국가핵심기술로 지정될 수 있다(이경환, 2016).

다) 중소기업 기술 보호 지원에 관한 법률

중소기업기술보호법은 2014년 5월 28일에 제정되어 2014년 11월 29일 자로

발효가 된 법령이다. 본 법령은 중소기업 기술 보호를 지원하기 위한 기반을 확충하고 관련 시책을 수립·추진함으로써 중소기업의 기술보호 역량과 기술경쟁력을 강화하고 국가 경제의 발전에 이바지함을 목적으로 하는 법령이다.

중소기업기술보호법은 제5조를 통하여 3개년 지원계획을 수립, 중소기업의 기술 보호 역량 강화를 목표로 하는 중소기업 기술 보호 정책 추진, 기술보호정책 수립과 관련된 자문·협의, 중소기업 기술 보호 실태조사, 일련의 기술보호 추진체계 수립을 뒷받침하고 있는 법적 근거를 제공하고 있다. 또한, 중소기업기술보호법의 제정을 통하여 보안설비 구축, 보안관제서비스, 기술자료 임치 등 중소기업 기술보호를 위한 지원근거가 마련되었고, 기술보호지원 전담기관 지정·기술보호 전문 인력 양성·보안관제서비스 및 보안시스템 구축 지원 등의 인프라 조성에 대해서도 법적 근거가 마련될 수 있었다.

중소벤처기업부장관은 중소기업기술의 유출방지와 보호를 위하여 기술자료 임치제도 지원, 국가연구개발사업의 성과물 보호, 중소기업기술보호 진단 및 자문, 해외진출 중소기업의 기술보호 등 다양한 사업을 지원하도록 하고 있다. 중소기업 기술보호 기반조성과 관련해서 중소벤처기업부장관은 중소기업 보안기술 개발의 보급 및 촉진, 기술보호 전담기관의 지정, 중소기업 기술보호 교육 및 홍보, 기술보호 인력의 양성, 기술보호 관제 서비스 및 보안시스템 구축 지원, 기술보호 상생협력, 중소기업기술 보호 포상, 국제협력 등의 사업을 시행할 수 있다. 그리고 중소기업기술의 보호 지원에 관한 업무를 전담하는 기관을 지정하고, 그 경비 등을 지원하며 중소기업의 기술 유출로 인한 분쟁의 조정 및 중재를 위한 '중소기업기술분쟁조정·중재위원회'를 설치하여 운영하도록 하였다(이찬우, 2018).

라) 방위산업기술 보호법

방위산업기술 보호법은 2015년 12월 29일에 제정되었다. 방위산업기술 보호법은 방위산업기술을 체계적으로 보호하고 관련 기관을 지원함으로써 국가의 안전을 보장하고 방위산업기술의 보호와 관련된 국제조약 등의 의무를 이행하여 국가신뢰도를 제고하는 것을 목적으로 하는 법률이다.

방위산업기술 보호법은 방위산업기술보호위원회를 구성 및 운영하고 방위산업기술의 보호에 관한 종합계획과 시행계획 수립·시행할 수 있도록 하는 법적 근거를 제시하고 있다. 그리고 방위산업기술의 지정 및 수출, 국내 이전 시 보호대책 수립·시행 의무 부과, 방위산업기술 보호를 위한 제도적 틀을 제시하고 있다. 또한, 방위산업기술 유출에 대한 사후 제재 및 사전 예방적 차원에서 방위산업기술의 유출·침해 행위에 대한 징역·벌금형 등의 형사적 책임 강화 조항도 있다(안성진, 2016).

방위산업기술을 효율적으로 보호하고 관리하기 위한 종합계획으로 5년마다 수립하며, 방위산업기술의 보호에 관한 기본목표와 추진방향, 단계별 목표와 추진방안, 구축에 관한 사항, 연구개발 및 지원에 관한 사항, 정보의 수집·분석·가공 및 보급에 관한 사항, 국제협력에 관한 사항, 대상기관의 방위산업기술 보호체계 구축·운영 및 지원에 관한 사항 등을 포함한다(이찬우, 2018).

[표 2-5]를 통해 중소기업 기술보호를 위한 법령을 파악할 수 있다.

[표 2-5] 중소기업 기술보호를 위한 법령 비교

구분	산업기술보호법	영업비밀보호법	중소기업기술보호법	방위산업기술 보호법
소관 부처	산업부	특허청	중기청	국방부
보호 대상	국가핵심기술 산업기술	영업비밀	중소기업기술	방위산업기술
주요 내용	국가핵심기술 지정·수출신고 산업기술의 부정 취득 금지	영업비밀의 부정취득 금지	지원계획 수립 기술자료 임치제도 전담기관 설치 상담·교육 지원	방위산업기술 지정 및 수출·국내이전 관리 방위산업기술의 부정 취득 금지
피해 구제	X	손해배상	X	X
	형사처벌	형사처벌	X	형사처벌
	금지청구	금지청구	X	X
	산업기술분쟁	산업재산권분쟁	중소기업기술분쟁	

	조정	조정	조정 · 중재	
형벌	5년 이하 징역 또는 5억원 이하 벌금	5년 이하 징역 또는 5천만원 이하 벌금	X	7년 이하 징역 또는 7천만원 이하 벌금

※ 출처 : 국가지식재산위원회 (2016)

제 3 장 산업정보 유출 현황

제 1 절 중소기업 산업정보 유출 현황

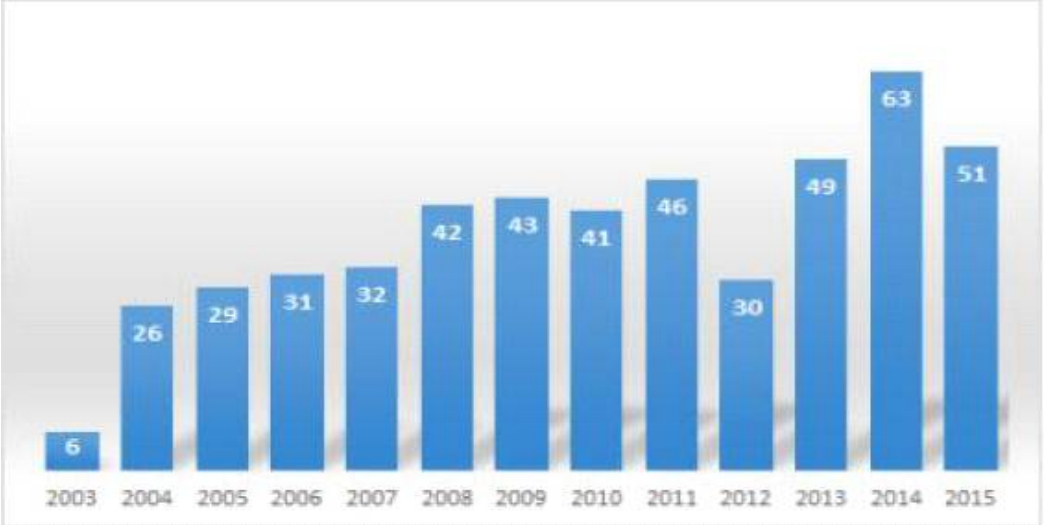
21세기 첨단과학 기술의 발전과 함께 국내 중소기업 산업기밀 정보·기술을 보호하기 위해 산업보안에 대한 국가 법률제정 및 정부 지원 활동이 지속해서 이루어지고 있음에도 불구하고 [표 3-1]과 같이 매년 산업정보·기술 유출 사고는 꾸준하게 증가하고 있다.

[표 3-1] 연도별 산업정보·기술 적발 실적

구분	계	2005	2006	2007	2008	2009	2010	2011	2012
건수	294	29	31	32	42	43	41	46	30

※ 출처 : service12.nis.go.kr (2013)

국정원 산업기밀보호센터의 기술유출 통계에 따르면 [그림 3-1]과 같이 산업정보·기술 유출 사고가 매년 증가하고 있으며 2003년도와 2014년도 비교 시 약 10배 이상 산업정보·기술 유출 적발 건수가 증가했음을 확인할 수 있다.



[그림 3-1] 기술유출 연도별 적발 현황 (산업기밀보호센터, 2016)

산업기밀보호센터에 따르면 산업정보 유출의 동기는 인사·처우에 대한 불만, 금전적인 유혹, 개인의 영리 등 다양하게 나타났고 유출한 기밀을 매수하거나 이직하는 등 향후에 개인적인 목적으로 소속된 기업의 기밀을 유출하여 무단 보관하는 사례도 많은 비중을 차지하고 있어 결국 유출 동기나 유출된 기밀의 활용목적은 다양하지만, 조직 애착이 낮은 상태에서 이직을 결심하고 기업의 산업기술을 유출한다고 할 수 있다. 또한, 산업기술유출의 약 60%는 전직 직원의 퇴사 후 회사 설립 등 이직 시 발생하는 것으로 나타났다(장항배, 2015).

대부분 이직 1개월 전에 기밀을 유출한 후 이직 의사를 밝히는 경향이 있으며, 대부분 기업에서 임직원이 이직 의사를 밝힌 후 집중적으로 관리하기 때문에 기술유출 여부를 적발하더라도 유출된 자료를 회수하기 어려운 문제가 발생한다(현미분, 2016).

중소기업의 기술보호 역량과 관련해서도 국가핵심기술 보유기관별 실태조사를 통해 제시된 통계자료가 있다. [표 3-2]에 따르면, 2012년 기준으로 보안 역량 수준이 평균 71점이었으나, 2014년에는 2012년에 비해 5점가량이 상승한 76점인 것으로 나타났다. 국가핵심기술 보유기관의 기술보호 역량이 다소 향상되었음에도, 중소·중견기업의 경우에는 여전히 기술보호 역량이 취약한 것으로 확인되었다(안성진, 2016).

[표 3-2] 국가핵심기술보유기관 보안역량 수준 현황

구분	대기업	중견기업	중소기업	연구기관	전체평균
12년도	92점	74점	58점	83점	71점
14년도	93점	76점	61점	92점	76점

※ 출처 : 산업통상자원부 (2014)

[그림 3-2]에 의하면 2014년 기준으로 중소기업의 기술보호 역량 점수는 45.6점으로 대기업 기술보호 역량 점수인 65.6점의 약 70% 수준에 불과하다. 중소기업의 기술보호 역량은 2012년 34.9점과 비교해볼 때, 10점 넘게 상승한 것으로 나타났다. 하지만 여전히 대기업보다는 현저하게 낮은 기술보호 역량을 보이기 때문에 중소기업의 경우 산업정보보안이 취약하며, 이에 대한 지속적인

지원책 마련이 필요하다.

[그림 3-2] 중소기업 기술보호 역량 (중소기업청, 2014)

산업통상자원부에서 제공한 [표 3-3] 산업정보·기술 유출 현황에 따르면 2013년~2018년 사이에 발생한 국내 산업정보·국가핵심기술 해외유출 및 시도 적발 건수는 총 158건, 연평균 26건 이상 발생하였다. 2014년도와 2015년도에 30건 이상의 산업기술 유출을 적발하였다. 2014년부터 2018년도까지 산업기술 유출 적발 건수는 점차 감소하는 것을 확인할 수 있다.

[표 3-3] 산업정보·국가핵심기술 유출 적발 건수

연도	2013	2014	2015	2016	2017	2018	합계
산업기술	29	31	30	25	24	19	158
국가핵심기술	2	4	3	8	3	5	25

※ 출처 : 산업통상자원부 (2020)

디스플레이 분야를 중심으로, 국내 기업이 경쟁력을 보유한 자동차, 조선, 전기, 전자 등의 업종에서 주로 유출이 발생했음을 [표 3-4]를 통해 확인할 수 있다.

[표 3-4] 업종별 산업정보·기술 유출 적발 건수

업종	전기전자	기계	조선 · 자동차	정보 통신	화학 · 생명 공학	기타	합계
건수	67	31	24	14	16	6	158

※ 출처 : 산업통상자원부 (2020)

보안역량이 열약한 중소기업에서 대기업 대비 산업정보 · 기술 유출이 높은 비중을 차지하고 있는 것을 [표 3-5]을 통해 확인할 수 있다.

[표 3-5] 기업규모별 산업정보 · 기술 유출 적발 건수

구분	대기업	중소기업	기타	합계
건수	36	107	15	158

※ 출처 : 산업통상자원부 (2020)

산업정보 · 기술의 유출 주체의 대부분은 전 · 현직 직원으로부터 발생하는 기술유출 사고가 80%를 차지하고 기타 협력업체, 유치과학자 등을 포함할 시 총 93%를 차지할 정도로 기업의 내부정보를 손쉽게 이용할 수 있는 관계자들에 의해 대부분의 기술 유출범죄가 이루어지고 있는 것으로 [그림 3-3]을 통해 확인되었다. 이는 사내 정보에 접근하기 위해서는 일정 수준의 접근권한을 가지고 있어야 하며 일반적으로 기업들은 접근제어정책을 시행하고 있으므로 사내 정보에 대한 접근권한이 부여된 임직원이 아니면 기술의 유출이 힘든 환경이 되었다고 볼 수 있다. 즉 기술적 부분으로 인한 산업정보 · 기술 유출 사고가 관리적 부분으로 인한 산업정보 · 기술 유출 사고가 발생하고 있다. 또한, 몇몇 연구·개발자들은 본인이 개발한 기술은 자신이 소유할 권리가 있다는 생각을 가지고 죄의식 없이 회사의 기술을 유출하여 사업화하거나 지속해서 내부 직원과의 관계를 활용하여 기술유출의 통로로 이용하기도 하였으며, 유출 동기는 개인의 이윤추구를 위함이었다. 또한, 기술유출 피해 기업의 규모를 보면 중소기업이 70%로 제일 높은 비중을 보였고 기술에 대한 보호 수준도 종업원 수를 기준으로 기업의 규모가 작을수록 보호에 대한 수준이 미흡한 것으로 나타난 결과도 볼 수 있었다. 기술 유출의 가장 높은 유형으로는 중요자료의 무단보관으로 인한 기술유출 사고가 46%로 주요기술을 취급하는 직원들의 보안의식 부족이 가장 큰 문제점으로 확인되었다(김광민, 2019).

[그림 3-3] 기술유출 주체 · 규모 현황 (산업기밀보호센터, 2019)

제 2 절 중소기업 산업정보 유출 사례 분석

1) 산업정보 유출 원인

산업기술의 유출 범죄가 발생하는 이유는 개인 혹은 조직적인 차원에서 부당한 경제적 이득을 충족시키기 위한 것이 대부분이다. 기술유출 대상은 핵심 산업기술뿐만 아니라 부수적으로 관련된 영업 기밀까지 포함하고 있음을 알 수 있다. 이는 기술을 실제로 사업화하기 위해서는 경영상의 제반 정보를 함께 탈취해야만 실질적인 수익을 조기에 보장하기 위한 것으로 해석된다. 이와 같은 산업기술 유출 범죄는 국내 기업의 단순한 기술 투자비용에 대한 피해뿐만 아니라 기술을 빼내간 경쟁업체가 얻게 될 이익까지 합하면 그 손해액은 천문학적인 액수일 것으로 예상된다(김광민, 2019).

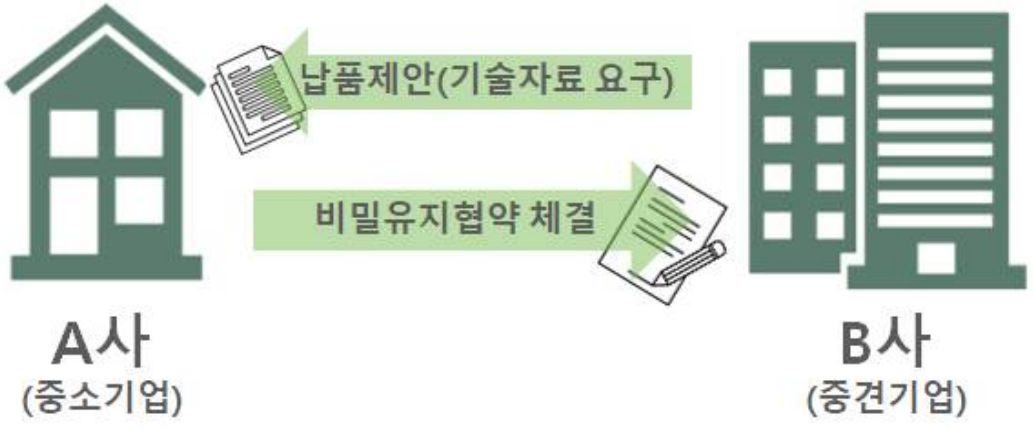
산업기술 정보 유출 원인 요인 중 국가 차원의 기술보호 종합시스템 및 체계적 관리 부재도 큰 원인으로 파악된다. 중소기업 산업기술 보호 정책을 살펴보면 여러 부처에서 많은 정책적 방안을 제공하고 있지만, 기업에서는 정책에 대한 인지를 못 하고 있는 실정이다. 이러한 점을 볼 때, 정부 차원의 산업기술보호 체계가 존재하지 않는다는 것을 파악할 수 있다. 이와 관련하여 조사결과에 따르면 기업 입장에서의 각종 지원정책에 대한 기업 인지도는 24.5%로 낮은 상

황이다(안성진, 2016).

2) 산업정보 유출 사례

가) 납품제안 중 산업정보 유출

2018년 금형 제조업체 A사는 중견기업 B사로부터 납품계약을 제안받으면서 도면, 기계 사양 등의 기술 자료 제공을 요구받았다. A사는 2014년도 타 기업과 납품계약을 맺으면서 기술 자료를 제공한 적이 있는데 자료 제공 후에 거래가 단절되고 기술이 유출된 경험이 있어 B사와의 거래 전 중소벤처기업부에 상담을 요청하였다. A사는 법률자문을 받고 B사와 납품계약을 맺으면서 거래 시 영업비밀이나 기술 자료를 타인에게 공개하지 않도록 하는 비밀유지협약(NDA)[2]도 함께 체결하여 기술유출을 예방하였다.



[그림 3-4] 납품제안 과정에서 산업기술 유출

[그림 3-4]의 산업정보 유출 대응전략으로 기업 간 거래 전에 비밀유지협약 체결 없이 유출된 산업기술정보는 A사에서 B사로 문제없이 제공한 것으로 해석되고, 결국 법적 분쟁에서 불리해지므로, 산업기밀 정보를 외부에 제공하는 경우

2) 비밀유지협약(NDA) : 상호 간에 기술제휴, 이전 및 동업 등의 합의된 목적을 달성하기 위해 당사자 간 비밀을 유지한다는 내용을 기재한 문서로 위반할 경우 민사상 손해배상 대상(IPR Helpdesk, 2008).

사전에 반드시 비밀유지협약서를 작성해서 기업 간에 문제가 없도록 조치하는 것이 바람직하다.

나) 계열사를 통한 산업정보 유출

소프트웨어 개발업체 A사는 스마트폰 요금부과 서비스 개발과 관련하여 대기업 B사의 요청으로 정식계약을 체결하지 않고 B사의 계열사인 C사를 통해 개발을 진행하도록 요구받았다. 개발이 완료된 2014년부터 B사에 라이선스 계약을 요청했으나, C사를 통한 단순 용역개발로만 계약을 체결하였다. 2016년 용역계약이 만료됨에 따라 개발기술이 무단으로 사용하게 되는 피해가 발생할 수 있어 중소벤처기업부 기술보호 법무지원단[3]의 법률자문을 지원받아 B사와 상호협의를 통해 정식 계약을 체결하였다.

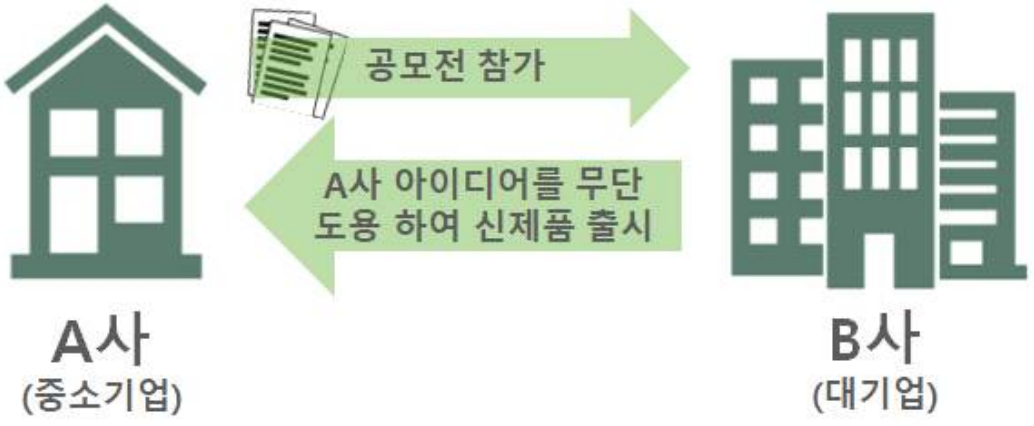
[그림 3-5] 계열사를 통한 산업기술 유출

[그림 3-5]의 산업정보 유출 대응전략으로 대기업과의 기술 개발사업은 계열사와 같이 진행하는 경우가 많으므로 의사결정에 대한 어려움이 증가한다. 따라서 사전에 개발될 기술에 대해 명확하게 범위를 지정하고, 각 이해 관계자들과의 미팅을 통해 개발될 기술에 대한 권리 귀속을 명확하게 정의해야 한다.

3) 기술보호 법무지원단 : 중소기업의 1:1 법률주치의로 기술보호를 위한 맞춤형 법률서비스 지원(중소기업기술보호울타리, 2020).

다) 공모전 아이디어 도용

그래픽 디자인 회사인 A사는 2016년 대기업 B사가 주최하는 콘텐츠 공모전에 참가하여 제품디자인, 광고기획 등의 아이디어를 제출하였다. 그러나 B사는 A사의 사전 동의 없이 제출한 아이디어를 무단으로 도용하여 A사가 제출했던 제품디자인, 광고기획을 B사의 신제품에 적용하여 출시하였다.



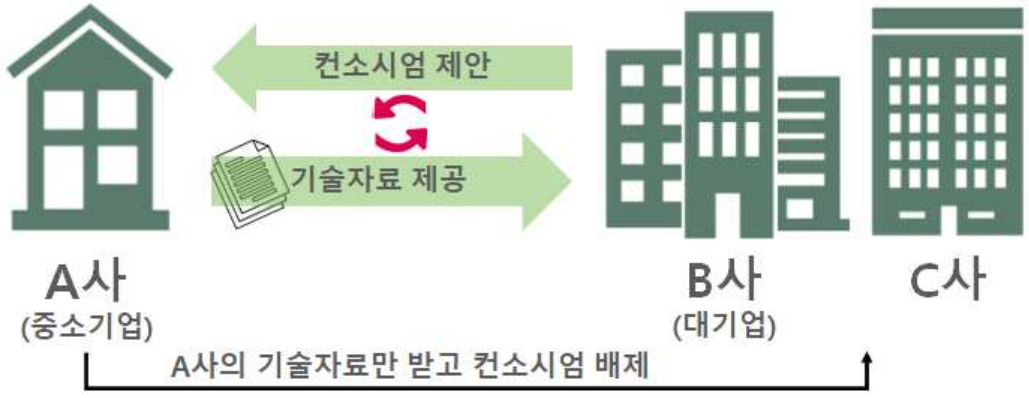
[그림 3-6] 공모전 아이디어 도용

[그림 3-6]의 산업정보 유출 대응전략으로 공모전 주최 측의 제안 아이디어 권리 소유, 상금 대가로 권리 이전 등 아이디어 권리 귀속에 대한 공모전 세부 규정의 사전검토가 필요하다. 아이디어의 핵심적인 내용을 사전에 저작권 등록하거나 핵심 기술의 특허출원을 통해 불법·도용·탈취에 대한 법적 보호 장치를 사전에 마련한 이후 공모전에 참가하는 것이 바람직하다.

라) 핵심 영업비밀 유출

교량 시공 전문 업체인 A사는 2016년 도로건설 설계 입찰에 참가한 대기업 B사의 컨소시엄 제안을 받고 핵심 기술자료를 B사에 제안했다. B사는 A사에 아이디어, 핵심기술 등을 추가로 요구하였고, 이를 활용하여 낙찰에 성공하였으나,

B사는 핵심 기술을 제공한 A사가 아닌 C사와 함께 사업을 진행하였다.

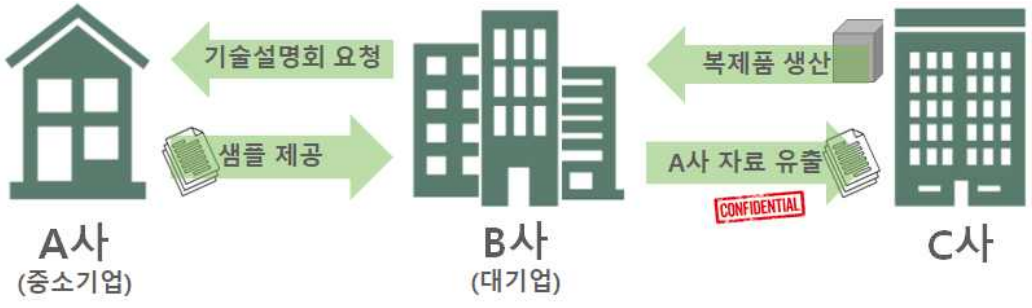


[그림 3-7] 컨소시엄 제안과정에서의 기술탈취

[그림 3-7]의 산업정보 유출 대응전략으로 외부로 기술이 공개되거나 상대방에게 제공하기 전에 자사의 기술임을 입증받을 수 있도록 제3의 신뢰성 있는 기관에 임치하여 안전하게 관리해야 한다.

마) 부품 샘플을 통한 산업정보 유출

2012년 대기업 B사는 선박부품 제조업체 A사에 기술 설명회를 요청하여 부품 샘플을 받고, 타 기업인 C사에 제공하여 복제품을 생산하도록 지시하였다. B사는 C사를 통해 생산된 복제품을 직접 사용하였다.



[그림 3-8] 부품 샘플을 복제품으로 제작

[그림 3-8]의 산업정보 유출 대응전략으로 중소기업의 경우 자사의 산업기술 정보를 기술설명회에서 공개 후, 타사에서 기술을 모방해서 복제품을 생산 시 빠른 대처가 미흡하므로 기술임치제도, 특허출원 등 보호수단을 마련한 후, 핵심 기술자료를 제공해야 산업정보 보호가 가능하다.

바) 입찰과정 산업정보 유출

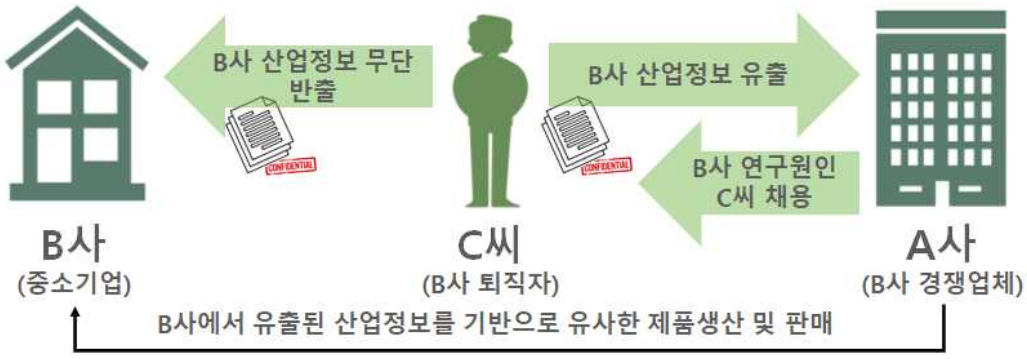
설비 성능평가 및 검증업무를 수행하는 기관인 A사는 공공기관인 B사의 용역을 수행하면서 기술 절차서, 보고서 등 영업비밀을 제출하였다. B사는 추가 용역발주 과정에서 A사의 영업비밀을 C사에 제공하여 저가로 입찰에 참여하였다. 영업비밀 유출 손해를 입은 A사는 중소벤처기업부의 법률자문을 지원받아 B사에 관련 문건 폐기처리를 요청하였다.

[그림 3-9] 입찰을 통해 산업정보가 경쟁사로 유출

[그림 3-9]의 산업정보 유출 대응전략으로 기술용역의 경우, 발주처에서 사후관리를 명목으로 기술거래계약에서 명확하게 규정하지 않은 핵심기술정보를 요구하는 경우가 많으므로 기술자료를 제공할 시, 개별적인 비밀유지협약서를 작성하거나 기술거래를 통해 해당 기술정보의 정당한 대가를 받는 것을 고려해야 한다.

사) 경쟁사 인력 채용

2016년 A사는 경쟁사인 B사의 핵심 연구인력을 유인하여 채용함으로써, B사의 영업비밀에 해당하는 기술자료와 정보를 부당하게 취득하였다. A사는 B사의 영업비밀을 부당하게 이용하여 B사가 제조한 제품과 유사한 제품을 생산·판매함으로써, B사는 매출액이 급감하는 손해를 입었다.



[그림 3-10] 경쟁사 직원 채용을 통한 산업정보 유출

[그림 3-10]의 산업정보 유출 대응전략으로 유출된 영업비밀의 비밀관리 성이 부정되는 경우에 근로자와 '경업금지약정[4]"을 체결했다면 전직 금지 가처분 수단을 활용할 수 있다.

아) 퇴직자 기술 유출

2018년 A사는 의료용 소프트웨어 출시를 앞두고 연구소장 B씨가 갑작스레 퇴직하는 일이 발생하였다. 연구소장은 퇴직 전 임직원들 몰래 기술자료를 개인 외장 하드에 복사하여 유출하고 직원들 모르게 경쟁업체인 중국기업과 빼돌린 기술로 사업을 추진하였다.

4) 경업금지약정 : 근로자가 경쟁업체에 취업하거나 스스로 경쟁업체를 설립·운영하는 등의 행위를 하지 않을 것을 약속하는 것으로, 이를 위반 시 손해배상 청구 가능(국가법령정보센터, 2020).

[그림 3-11] 퇴직자를 통한 산업정보 유출

위의 산업정보 유출 대응전략으로 중소기업의 기술유출 예방은 퇴직자 관리가 우선이다. 우선 업무 인수인계 리스트를 충실히 작성하도록 하고 경업금지 및 비밀유지 특약이 포함된 사직서를 징구하여야 하며, 영업비밀 보유자 등 핵심인력인 경우 영업비밀 유출 시 관련 법규에 따라 처벌받을 수 있다는 사실을 사전에 고지해야한다. 또한, 퇴사자가 재직 시 작성한 서약서나 프로젝트 투입기록, 전자파일 등을 해당 부서 팀장 또는 보안담당 부서에서 확인하고 반드시 보존 허락을 득해야 한다.

자) 현직 임직원 산업정보 유출

A사의 직원 B씨는 자사의 영업 비결인 휴대전화 지식 서비스 기술을 협력사인 C사에 유출했고 C사는 같은 서비스를 유사한 이름으로 사용하였다.

[그림 3-12] 현직 임직원 산업정보 유출

[그림 3-12]의 산업정보 유출 대응전략으로 영업비밀을 취급하는 임직원은 반드시 보안서약서를 징구해야한다. 임직원의 재직 중에 중요 프로젝트에 참여하거나 승진 또는 인사이동으로 업무 내용이 변경되었을 경우 영업비밀 보안서약서를 징구하고 정기면담을 시행하여 근무여건 등 애로사항을 파악하여 사전에 산업정보 유출을 예방해야 한다.

차) 개인 SNS를 통한 산업정보 유출

2016년 광고영화를 제작하는 A사에서 2년간 재직한 B씨는 퇴직 시 임금체납에 대한 불만으로 컴퓨터 그래픽 소스, 촬영본, 결과물 등을 개인 SNS에 무단으로 게시하여 거래처들의 기술자료를 유출하였다. 이를 확인한 거래처 C사 등은 A사와의 거래를 단절하여 지속해서 피해가 발생하였다.

위의 산업정보 유출 대응전략으로 보안서약서 작성과 임직원 산업정보보호 교육을 의무화해야 한다. 회사에서 습득한 사업상의 모든 정보 및 영업기밀 등을 외부로 유출·누설하지 않겠다는 보안서약서를 입사·퇴직 시 체결하고, 임직원들에게 산업보안을 인식시킬 수 있도록 정기적인 보안교육을 시행해야 한다. 퇴사 의사를 밝힌 직원에게 퇴직자 비밀유지 서약서를 징구하고 퇴직자가 개발한 기술의 일체 권리는 회사에 있음을 인식시켜야 한다.

제 4 장 중소기업에 적합한 산업보안 관리체계

제 1 절 산업보안 관리체계 구성 개요

첨단산업이 지속해서 발전하고 있는 오늘날에는 경제적 가치를 지닌 산업정보 유출로 인해 국가의 재산과 기업의 가치가 외부로 유출될 위험이 점점 더 커지고 있다. 이에 따라 우리나라 국가 및 국민경제에 악영향이 생기게 될 것이고, 결과적으로 우리나라 경제 성장 동력을 떨어뜨릴 수 있다.

산업현장에서 다양한 연결기기 사용 및 사물인터넷을 통한 설계부터 생산·유통·서비스 과정이 연속되면서 산업정보 유출의 위험성이 더욱 커지고 있다. 4차 산업혁명 시대에 맞춰 기업들은 산업현장의 보안을 위협하는 요소들을 파악하여 체계적이고 효율적인 사이버 보안 전략수립이 중요해졌다. [그림 4-1]을 통해 산업정보보안 영역을 확인할 수 있다.

[그림 4-1] 산업정보보안 영역

하지만 중소기업의 경우 대기업과 비교하면 더욱이 기술보호 관점에서 충분한 역량이 갖추어지지 못하는 경우가 많다. 핵심기술을 보유하고 있다고 하더라도 산업정보 자산이 유출되지 못하도록 기업 차원에서 지속적인 투자를 할 재정적 여건이 부족하다. 또한, 사후 대응도 충분한 역량을 갖추지 못하고 있어서 산업정보 유출사고가 발생 시 대응방안 체계가 미흡하다. 그리고 인식적 측면에서도 산업정보보호를 위한 대비가 충분하지 않다. 임직원들에 대한 정보보호 교육이 부족하며 정보보안 인력에 대한 투자도 역시 부족하다. 산업정보·기술유출의 경우 대부분 내부 구성원에 의한 유출이 빈번하므로 이를 방지하기 위해서는 인적자산에 대해 지속적이고 충분한 관리가 이루어져야 한다.

하여 본 연구에서는 중소기업에 적합한 산업보안 관리체계에 대해 물리적 보안영역·기술적 보안영역·관리적 보안영역으로 정의하고 각 영역에서 어떤 보안이 필요하며 산업정보 유출사고 예방을 위한 방안을 살펴보고자 한다.

[그림 4-2]를 통해 산업 정보보안 프레임워크를 살펴볼 수 있으며 보안영역별로 관리해야 할 프로세스를 확인할 수 있다.

[그림 4-2] 정보보안 프레임워크

제 2 절 물리적 보안

1) 물리적 보안 정의

물리적 보안이란 기업의 설비 및 시설 자산을 지칭하며 각종 물리적 위협요소로부터 기업의 자산을 보호하며 정보 자산에 가해질 수 있는 피해를 최소화하고 정보 시스템에 관련된 전반적인 물리보안을 의미한다.

물리적 보안 관리체계로 생체인식, 출입통제, 시설보호, 물리시스템 백업, 휴대장치 통제 등이 있으며 [표 4-1]을 통해 확인할 수 있다.

[표 4-1] 물리적 보안 관리체계

항목	목적
생체인식 보안	지문인식, 얼굴인식, 홍채인식, 음성인식 등 사람의 생체를 통해 개인 식별을 함으로써 외부인은 출입할 수 없도록 통제
출입통제 보안	보안카드로 게이트를 통과할 수 있으며 사전에 허가된 인가자만 출입할 수 있도록 통제
시설보호 보안	기업의 중요시설을 감시하며 비인가자는 접근할 수 없도록 물리적으로 통제
물리시스템 백업 보안	재해복구센터를 통해 기업의 자산을 보호하고 이중화 구성을 통해 문제가 발생 시, 즉시 복구 조치
휴대장치 통제 보안	기업에 출입 시 휴대장치에 보안스티커, 보안 애플리케이션 설치 등을 통한 통제

2) 생체인식 보안

생체인식 보안이란 사람의 생체 및 행동을 측정해서 개인 고유의 식별 수단으로 활용하는 것이다. 생체인식 보안기술은 지문인식기술 · 얼굴인식기술 · 홍채인식기술 · 음성인식기술이 있다.

지문인식기술은 사람의 지문을 기반으로 임직원임을 식별하거나 인지하는 기술이다. 편리하고 안전한 인증보안 방법으로 다양한 장치에서 사용할 수 있으며

정확도가 우수하다.

얼굴인식기술은 카메라로 입력되는 영상을 분석하여 얼굴의 위치와 얼굴 여부를 판단하여, 데이터베이스에 있는 값과 비교하여 임직원의 얼굴인지 식별하는 기술이다. 비접촉식으로 인증이 진행되므로 편리하며 시스템 구축비용이 저렴하고 원격을 통해 인증이 가능하다.

홍채인식기술은 사람마다 고유의 홍채패턴(무늬 · 형태 · 색 · 모세혈관)을 구분해서 임직원의 얼굴인지 식별하는 기술이다. 낮은 오 인식률과 위조가 불가하므로 보안성이 좋고 비접촉식의 장점이 있다.

음성인식기술은 사람마다 고유한 음성을 이용하여 임직원의 음성인지 식별하며 소리 센서를 통해 얻은 음성의 특징을 데이터베이스값과 비교하는 기술이다.

3) 출입통제 보안

출입통제 보안이란 기업과 서버 실에 출입하기 위한 보안절차를 의미한다. 출입통제 보안기술로는 보안카드 기술이 있다.

보안카드 기술은 특정 건물 및 장소에 출입 시, 출입 허가된 인원임을 인증하기 위한 기술로 보안카드 안에 인증할 수 있는 칩을 넣어서 보안카드 칩을 인식할 수 있는 게이트만 통과할 수 있다.

4) 시설보호 보안

시설보호 보안이란 기업 내의 중요한 시설이 있는 장소는 물리적으로 차단하여 비인가자에 대해 접근 통제하고 관련 있는 임직원만 출입할 수 있도록 허용한다. 비인가자에 대한 접근 통제를 통해 기밀데이터 유출방지 및 중요 자산에 대한 물리적인 보안을 강화할 수 있다. 또한, CCTV를 통해 인가자 및 비인가자에 대한 모니터링이 필요하며 녹화된 영상을 증거자료로 사용할 수 있다.

5) 물리시스템 백업 보안

물리시스템 백업 보안은 기업의 물리시스템 백업 자산을 다른 지역에 보관하거나 재해복구센터를 통해 기업의 자산을 보호하고 안정성을 확보하는 기술이다. 물리시스템이 있는 기업 본사에 문제가 발생하더라도 동일한 구성의 백업 자산을 신속하게 확보할 수 있고 재해복구센터를 통해 이중화가 되어 있으므로 기업에서 운영하는 서비스에 문제가 없도록 할 수 있다.

6) 휴대장치 통제 보안

휴대장치 통제 보안은 기업에 출입 시, 휴대장치 카메라에 보안스티커를 붙여서 기업 내부에서 카메라를 사용할 수 없도록 하거나 휴대장치에 기업에서 제공하는 보안 애플리케이션을 설치 후 카메라 및 데이터 전송에 대해 일시적 잠금을 할 수 있도록 하는 기술이다. 휴대장치 카메라를 통해 산업정보를 탈취할 수 있으므로 대중적으로 보편화 되어있는 휴대장치 통제에 대한 보안이 필수적이다. 또한, WIPS[5]를 통해 모바일 무선 네트워크를 이용한 데이터 유출을 차단하고 비인가 무선 네트워크 접근을 사전에 예방해야 한다.

제 3 절 기술적 보안

1) 기술적 보안 정의

기술적 보안이란 정보자산에 대한 보안으로 다양한 보안기술을 통해 산업정보를 보호할 수 있는 것을 의미하며 외부 위협으로부터 기업의 자산을 보호하고 내부 위협으로부터 기업의 가치를 지키는 것을 의미한다.

기술적 보안 관리체계로 네트워크 보안, 엔드포인트[6] 보안, 시스템 보안이 있

---

5) WIPS : Wireless Intrusion Prevent System 약자로 공격 및 자료유출에 대해 비인가 무선단말기 접속을 차단하고 보안에 취약한 무선공유기를 탐지하는 소프트웨어다(SECUI, 2020)

6) 엔드포인트 : 데스크탑, 노트북 등 사용자가 사용하는 Device를 지칭한다(Symantec, 2018)

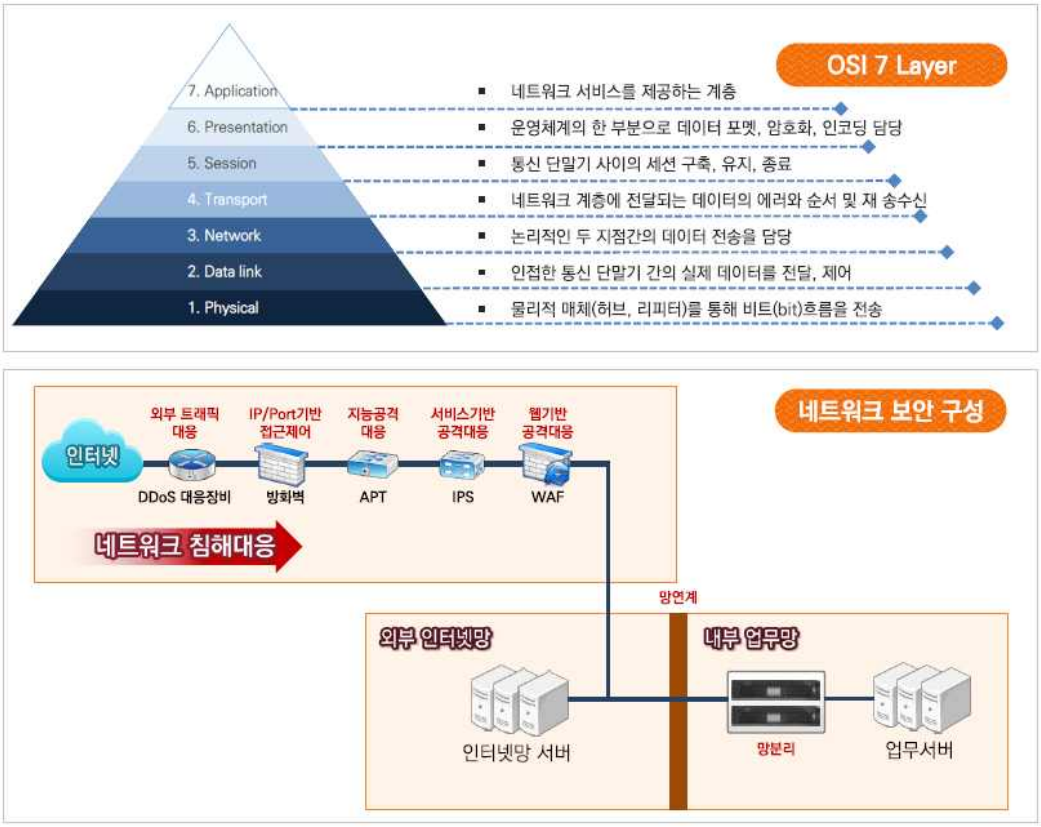
으며 [표 4-2]를 통해 확인할 수 있다.

[표 4-2] 기술적 보안 관리체계

항목	목적
네트워크 보안	기업 네트워크에 허가되지 않은 엑세스 또는 외부 위협요소로부터 데이터 및 인프라 보호. DDoS, Firewall, NAC, APT, IPS 등의 보안장비를 네트워크 구간별로 구성하여 네트워크 보안 강화
엔드포인트 보안	기업에서 업무 목적으로 사용하는 PC에 대한 보안 통제. 문서파일 암호화, 개인정보 탐지, 매체제어, 출력물 보안, 패치관리, 문서 중앙화, 악성코드 탐지 등의 보안 소프트웨어를 통한 엔드포인트 보안 강화
시스템 보안	기업 내부에 있는 서버에 접근 가능한 경로를 통제하며 계정관리, 접근통제, 데이터베이스 암호화, 명령어 통제, 본인인증 등을 통한 서버 시스템 보안 강화

2) 네트워크 보안

네트워크 보안은 기업 네트워크에 허가되지 않은 엑세스 또는 외부 침입을 사전에 방지하며 외부의 위협으로부터 네트워크 데이터와 인프라를 보호하는 최상단 보안이다. 네트워크 구간별로 필요한 보안 솔루션을 도입함으로써 보다 안전하고 강화된 기업 네트워크를 구축할 수 있다. 또한, 네트워크 보안영역을 단순히 솔루션으로 구분하면 외부위협을 방지할 수 없으며, 보안솔루션 구축 및 기능을 고도화하여 네트워크 침해 위협으로부터 보안을 강화해야 한다. 보안솔루션 구축 및 데이터 보안정책, 긴급재난복구계획, 정기적인 취약점 점검, 모의해킹 등을 통해 한층 더 강화된 기업의 네트워크 보안을 구성할 수 있다.



[그림 4-3] 네트워크 보안 영역 구성 (SKinfosec, 2019)

[그림 4-3]을 통해 네트워크 보안 영역 구성을 확인할 수 있다. 기본적으로 OSI 7 Layer 모형을 통해 프로토콜을 기능별로 나눌 수 있으며 기업 네트워크 보안을 구성하는데 참조하는 핵심 지표이다. 주로 DDoS, Firewall, Network Access Control(NAC), Advanced Persistent Threat(APT), Intrusion Prevention System(IPS) 보안장비를 기업의 네트워크 구간에 설치하여 네트워크 보안을 강화할 수 있다(SKinfosec, 2019).

DDoS 보안장비는 끊임없이 진화하고 다양한 기술을 사용하는 DDoS 공격을 국가별, IP 그룹, URL 평판분석을 통해 차단하며 DNS 요청 트래픽에 대한 탐지 및 방어를 수행한다.

Firewall 보안장비는 사전에 정의된 보안 규칙을 통해 Inbound/Outbound 네트워크 트래픽을 모니터링하고 제어한다. 인가된 내부 네트워크, 인가되지

않은 외부 네트워크를 구분하고 신뢰할 수 있는 트래픽만 허용하며 나머지 트래픽은 차단함으로써 네트워크 보안의 기본구성을 수행한다.

Network Access Control 보안장비는 네트워크 접근제어 솔루션으로 일련의 프로토콜을 사용해 엔드포인트가 기업의 네트워크망에 접근시도 할 때, 악성코드 검사와 기업의 보안 컴플라이언스 정책에 적합한지 판단하여 부적합 시 엔드포인트 네트워크를 차단하고 강제로 필수 소프트웨어를 설치하도록 통제한다.

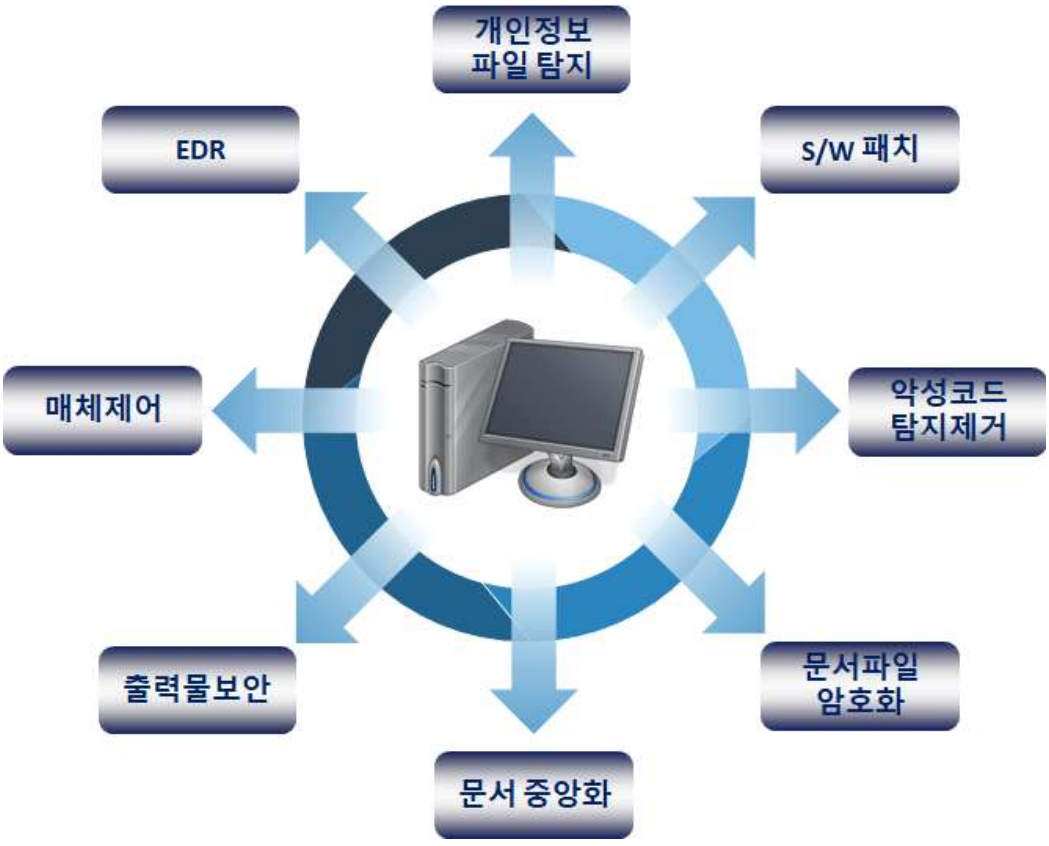
Advanced Persistent Threat 보안장비는 패턴, 시그니처 기반의 알려진 공격에 대한 대응으로 지능형 지속 위협 공격에 대응하는 솔루션으로 기존의 보안 솔루션을 우회하는 공격에 대응하며 가상 머신 기반으로 신종 악성 파일을 분석하고 파일 유입 및 유출의 양방향 트래픽 모니터링, 유해 사이트 접근 및 차단을 한다.

Intrusion Prevention System 보안장비는 기존 트래픽 흐름에 직접 관여하여 실시간으로 외부침입을 통제하며 유해 트래픽을 차단한다. OS나 Application의 취약점을 능동적으로 사전에 예방하며 외부에서 내부 네트워크로의 침입을 방지하고 비정상적인 트래픽을 차단한다.

3) 엔드포인트 보안

엔드포인트 보안은 사용자 PC를 안전하게 사용하기 위해 악성 코드 예방치료 및 기밀 정보유출 사전대응, 필수 소프트웨어 및 보안패치 설치 유도, 물리적 매체에 대한 보호활동 등을 통해 사용자 PC의 보안통제를 지원한다. [그림 4-4]를 통해 엔드포인트 시스템 보안 영역을 확인할 수 있다. 엔드포인트 보안의 경우 특성상 하나의 소프트웨어만으로는 통제가 어려우므로 기능별로 다양한 소프트웨어를 PC에 설치해서 관리와 통제가 필요하다. 엔드포인트 보안은 사용자 업무 PC에 소프트웨어를 설치하기 때문에 업무적으로 잦은 이슈가 발생하는 단점이 있지만, 끝단에서 상시 기업의 보안을 책임지는 핵심 보안 영역이다. 중앙에서 엔드포인트 소프트웨어 삭제 패스워드 관리와 설치 배포를 통해 사용자가 임의로 소프트웨어를 삭제할 수 없도록 통제 가능하며 문서를 암호화하여 기밀문

서가 외부로 유출되더라도 열람할 수 없게끔 보안을 구성하고 있다. 엔드포인트 보안영역으로는 악성 코드 탐지, 개인정보 탐지, 문서 보안, 출력물 보안, 매체제어, 패치 관리, 문서 중앙화, Endpoint Detection and Response, Automated Detection and Response가 있다(SKinfosec, 2019).



[그림 4-4] 엔드포인트 보안 영역 구성

악성 코드 탐지 소프트웨어는 외부 악성 코드 침해위협 대응으로 실시간 PC 내의 악성코드 탐지 및 감염 방지, 랜섬웨어 진단 및 처단, 사이버 침해사고를 예방한다. 최근에는 행위 및 평판 분석을 통해 Zeroday[7] 위협으로부터 대응할 수 있다.

개인정보 탐지 소프트웨어는 PC 내의 개인정보 탐지에 따른 개인정보 유출

7) Zeroday : 알려지지 않은 보안취약점을 이용한 공격(Symantec, 2017)

을 모니터링 및 차단하며 각 산업에 맞는 정책을 사전 정의하여 산업기밀 정보 유출을 최소화할 수 있다.

문서 보안 소프트웨어는 PC 내에 저장된 파일을 암호화, 권한제어, 유효기간 관리를 통해 실제로 문서가 유출되더라도 외부에서 문서를 열람할 수 없도록 보안 기능을 제공한다. 외부인력과 협업으로 인한 문서유출 사고에 대응하며 반도체, 자동차, 조선, 철강 등의 중요 산업기술에 대한 문서보안을 강화한다.

출력물 보안 소프트웨어는 출력되는 프린트 용지 내용을 통제하며 출력 내용에 기업 로고, 이미지, 출력자 정보 등을 워터마크로 남기고 출력 이력을 추적할 수 있으며 기밀정보가 포함된 문서는 출력을 차단할 수 있다.

매체제어 소프트웨어는 CD, USB 등 각종 매체 연결을 제어함으로써 이동식 저장장치에 의한 정보유출을 방지하며 정책적으로 사전에 허가된 매체만 사용할 수 있다.

패치 관리 소프트웨어는 중앙에서 PC OS 및 소프트웨어 보안 패치를 진행함으로써 취약점을 사전에 조치하고 상시 최신 보안 업데이트를 유지하여 PC 보안을 강화한다.

문서 중앙화 소프트웨어는 PC 내에 문서를 저장하는 것이 아닌, 중앙서버에 모든 문서를 저장 및 관리함으로써 사전에 랜섬웨어 등 보안위협에 대응한다. 클라우드 서버와 연계해서 사용할 수 있는 장점이 있다.

Endpoint Detection and Response 소프트웨어는 엔드포인트의 행위기반 악성 코드 탐지 대응 솔루션으로 알려지지 않은 악성 코드를 탐지 및 제거하고 위험요소를 분석함으로써 외부 사이버 공격을 사전에 예방할 수 있다. 또한, 비정상적이거나 의심스러운 동작에 대한 엔드포인트 모니터링을 하며 분석을 수행하여 위협요소에 대한 패턴을 식별하고 포렌식을 위한 수집된 데이터를 제공한다.

Automated Detection and Response 소프트웨어는 AI 및 머신러닝과 같은 고급 기술을 활용하여 위협 데이터를 선별하고 사전에 자동으로 차단하며 위협요소 조사, 검증 프로세스를 자동화할 수 있고 탐지 정확도가 높아 오 탐지가 적으며 운영 효율성을 향상시킨다. 또한, 인가되지 않은 장치를 네트워크에 연결했을 경우 검색해서 조치를 한다.

4) 시스템 보안

시스템 보안은 기업의 내부에 있는 서버에 접근 가능한 파일, 폴더, 장치제어를 통제하는 보안이다. 서버는 기업의 자산이며 중요한 데이터를 저장하고 서비스를 운영하는 데 있어서 핵심적인 역할을 수행하므로 서버 취약점을 이용한 다양한 공격 및 해킹이 발생할 수 있으며 산업기밀정보가 유출될 가능성이 높다. 하여 침해사고에 대응하기 위해 주로 계정관리 및 접근통제, 데이터베이스 암호화, 비밀번호관리 등의 기능을 사용하며 [그림 4-5]를 통해 시스템 보안의 워크플로를 확인할 수 있다(SKinfosec, 2019).

[그림 4-5] 시스템 보안 영역 구성

계정관리 및 접근통제는 시스템 계정 생성, 변경, 삭제에 대해 자동화 관리를 수행하며 계정별로 권한을 부여해서 서버접근 권한을 통제한다. 기업에는 다양한 용도의 서버들이 많으므로 계정관리가 용이하지 않다. 중앙에서 서버별로 계정의 권한을 통제함으로써 악성 코드 실행, 데이터 삭제 등의 불필요한 행위를 원천적으로 차단할 수 있다.

데이터베이스 암호화는 데이터베이스 내의 중요 데이터를 암호화하여 정보유출에 대해 근원적으로 데이터를 보호할 수 있다. 알고리즘, 데이터베이스 유형별로 암호화 기술을 적용하며 서버마다 암호화 방식 및 복호화 키 값이 상이하므로 데이터베이스 안에 저장된 기밀정보에 대한 보안을 강화할 수 있다.

비밀번호관리는 시스템 계정 및 관리자 계정의 패스워드를 주기적으로 일괄

변경하고 프로세스를 통해 권한이 부여된 사용자에게 패스워드를 생성 및 발급하여 비밀번호 관리의 보안성과 통합을 제공한다. 패스워드가 외부로 유출되더라도 주기적인 패스워드 변경을 통해 시스템 접근 보안을 강화할 수 있다.

제 4 절 관리적 보안

1) 관리적 보안 정의

관리적 보안이란 인적 자산에 대한 보안으로 기업 내 인적 자산 관리 절차 및 규정을 말하며 조직 내부의 정보 보호 체계를 정립, 임직원 관리, 정보 시스템의 이용 및 관리에 대한 절차 수립, 비상사태 발생을 대비하여 계획을 수립 등의 대책을 의미한다.

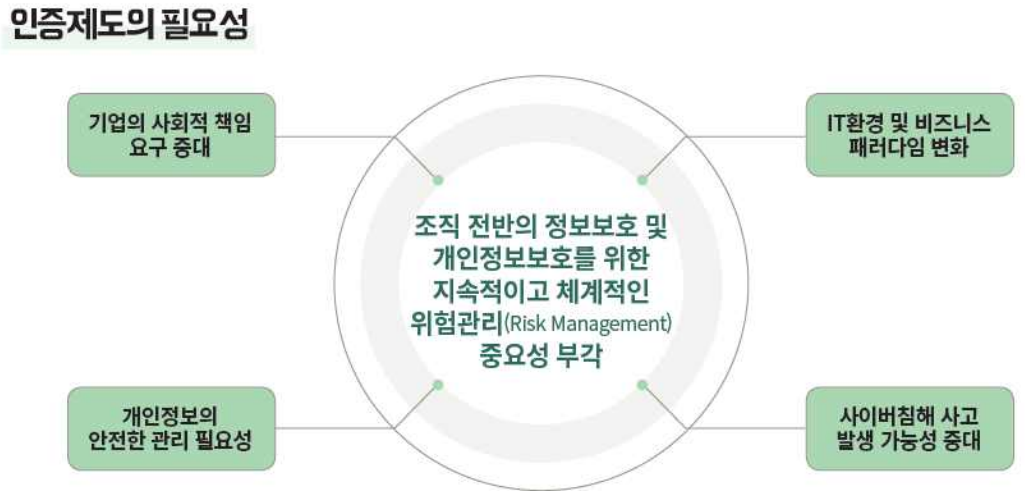
관리적 보안 관리체계로 보안정책 관리, 보안조직구성 및 운영, 인력보안 관리, 보안 감사, 침해사고 대응 등이 있으며 [표 4-3]을 통해 확인할 수 있다.

[표 4-3] 관리적 보안 관리체계

항목	목적
정보보호 관리체계 인증제도	ISMS, ISO27001 인증제도를 통한 기업의 산업보안 실태 확인 및 통제 항목을 기준으로 적합성 평가
산업정보보안 정책	기업환경에 맞는 산업정보보안 정책을 구성하고 전체적인 보안영역 관리 및 통제. 영역별로 정책이 상이하므로 명확한 근거와 데이터를 기반으로 정책 구성 필요
산업정보보호 조직체계	기업 내 산업정보보호 조직체계 구성을 통한 조직별로 산업보안에 대한 역할 및 책임을 부여함으로써 거버넌스 프로세스 확립
산업정보보안 교육	입사 시부터 퇴사 시까지 지속적인 산업정보보안 교육을 통한 임직원 보안의식 강화 및 유출 사고 개선
퇴직 대상자 관리	퇴직 대상자를 집중적으로 모니터링하고 산업정보 유출사고가 발생하지 않도록 관리 및 통제
침해사고 대응	침해사고 발생 시 빠른 대응 및 복구를 통해 기업의 피해를 최소화하는 목적

2) 정보보호 관리체계 인증제도

산업보안을 강화하기 위해서는 정확한 지표가 있는 관리체계 인증제도가 필요하다. [그림 4-6]을 통해 살펴보면 정보보호 관리체계 인증제도를 통해 조직의 전반적인 정보보호를 지속적이고 체계적으로 관리해야 하며 기업의 사회적 책임 요구를 증대하고 기밀정보의 안전한 관리 필요성을 중요시함으로써 인증제도의 필요성을 확인할 수 있다.



[그림 4-6] ISMS 인증제도 필요성 (KISA, 2020)

정보보호 관리체계 인증제도는 국내 표준인 ISMS 인증이 있으며 국제 표준 인증제도인 ISO27001 인증이 있다.

ISMS란 정보보호 관리체계 수립 및 운영을 위한 5단계 관리과정, 문서화, 정보보호대책에 대하여 기업의 특성 및 환경에 부합되도록 유지하고 관리하는지 평가하여 인증을 부여하는 제도를 말한다. 정보보호를 해야 하는 기업에 대한 인증을 통하여 인증받은 기업이 보유하고 있는 정보자산의 안전성, 신뢰성, 정보보호 관리 인식 제고, 정보보호서비스 산업의 활성화를 목적으로 하고 있다. 인증 기준은 '관리체계 수립 및 운영', '보호 대책 요구사항' 2개 영역에서 80개의

인증 항목에 대한 적합성 평가이다. [표 4-4]를 통해 ISMS 정보보호 관리체계 인증 항목을 확인할 수 있다(KISA, 2019).

[표 4-4] ISMS 정보보호 관리체계 인증 항목

영역	분야	인증 항목 수
1. 관리체계 수립 및 운영 (16개)	1.1. 관리체계 기반 마련	6
	1.2. 위험관리	4
	1.3. 관리체계 운영	3
	1.4. 관리체계 점검 및 개선	3
	소계	16
2. 보호대책 요구사항 (64개)	2.1. 정책, 조직, 자산 관리	3
	2.2. 인적 보안	6
	2.3. 외부자 보안	4
	2.4. 물리 보안	7
	2.5. 인증 및 권한관리	6
	2.6. 접근통제	7
	2.7. 암호화 적용	2
	2.8. 정보시스템 도입 및 개발 보안	6
	2.9. 시스템 및 서비스 운영관리	7
	2.10. 시스템 및 서비스 보안관리	9
	2.11. 사고 예방 및 대응	5
	2.12. 재해복구	2
	소계	64
합계		80

※ 출처 : KISA (2019)

ISO27001은 국제 표준에 근거하여 만든 인증 제도이며 조직 내·외부의 다양한 이슈와 이해관계자 등의 요구사항을 기반으로 한 정보보호 관리체계의 수립, 이행, 지속적 관리 및 개선을 수행할 수 있도록 표준 요구사항이다. 또한, 조직에 직·간접적으로 영향을 미치는 이슈와 이해관계자 등의 요구사항을 기반으로 위험 관리를 수행함으로 조직의 위험을 현실적이고 효과적으로 관리하도록 요구하고 있다. 국내에서는 글로벌 기업 위주로 ISO27001 인증심사를 진행하고 있다. 인증 기준은 114개의 통제 항목에 대한 적합성 평가이다. [표 4-5]를 통해 ISO27001 국제 표준 통제 항목을 확인할 수 있다(김광민, 2019).

[표 4-5] ISO27001 국제 표준 통제 항목

분야	통제 항목 수
정보보안 정책	2
정보보안 조직	7
자산 관리	10
인적자원 보안	6
물리적 및 환경적 보안	15
통신 보안	7
접근 통제	14
정보시스템 취득, 개발 및 유지보수	13
정보보안 사고 관리	7
업무연속성 관리	4
준수	8
공급자 관계	5
암호 통제	2
운영 보안	14
합계	114

※ 출처 : 김광민 (2019)

3) 산업정보보안 정책

산업정보보안 정책에 대한 프로세스를 확립함으로써 유출 사고를 사전에 예방할 수 있다. 산업기술자산을 구체적으로 규정하고 분류하는 기준이 필요하며 기술자산의 위험 도출 및 대책 마련 방안이 사전에 정의되어야 한다. 또한, 기술자산 유출 및 침해 예방방법에 대한 내부 지침을 수립하고 정보보안 조직에 역할 및 책임을 부여해서 관리하도록 해야 한다. 다양한 보안솔루션을 통해 산업보안 관리 및 통제를 하고 보안관리에 대한 세부규정을 운영해야 하며, 내부·외부 인력관리를 통한 산업정보 유출사고를 사전에 예방하며 노후되거나 폐기해야 할 장비에 대한 대책 마련 방안도 마련이 되어야 한다. 정보보안 기준점인 ISO27001과 ISMS 통제항목을 통해 정보보안 정책을 세분화해서 관리할 수 있다.

4) 산업정보보호 조직체계 구성

산업기술 유출방지 및 보호를 위해서는 기업별로 체계적으로 정보보호 조직이 구성되어야 한다. 정보보호 조직을 통해 산업기술 보호와 유출대응 등의 업무를 수행해야 하지만 중소기업의 경우 정보보호 조직체계를 구성하고 운영하는 것은 인력과 비용적인 부분에서 현실적으로 어렵다. 하지만 기업의 규모가 작아도 산업기밀정보가 유출될 가능성이 크기 때문에 보호업무 수행의 기능은 필요하다. 정보보호 조직을 구성하기 어려운 중소기업은 산업기술 유출방지 및 보호조직의 업무 내용을 숙지하고 보안 담당자에게 관련 업무를 수행하도록 해야 한다. 인력과 비용적인 부분에서 여유가 있는 중소기업의 경우 최고 경영자 밑에 산업기술 유출방지 및 보호 총괄 책임자를 임명하여 관리해야 한다. 총괄 책임자 밑에 산업기술관리 책임자를 임명하고 부서별 산업정보보호 및 유출 사고를 예방할 수 있는 활동업무를 해야 한다. 심의, 결정사항이나 규정 제정 등의 역할은 위원회를 두어 운영해야 한다. 산업기술관리 책임자의 밑에는 산업기술 관리자, 산업기술보호 책임자, 산업기술관리 담당자를 산업기술관리 책임자가 임명하도록 하여 산업정보보호 관련 업무를 수행하도록 한다. [표 4-6]과 같이 산업기술보호 조직의 역할 및 책임을 구분할 수 있다(산업통상자원부, 2017).

[표 4-6] 산업기술보호 조직 역할 및 책임

구분	역할 및 책임
산업기술보호위원회	산업기술보호 규정 제정, 주요계획, 주요정책 결정
	기밀정보 취급자 및 퇴직자의 관리정책, 비밀보호와 관련된 임직원 관리
산업기술관리 책임자	조직 전체 산업기술 관리에 대한 총괄적인 조정 통제 업무
	산업기술 관리 지침 및 계획 작성
	산업기술 보호의 총괄 조정, 감사업무
	유출사고 조사 보고 및 대응조치
산업기술 관리자	부서 내 산업기술 문서 보관 및 관리
	소속지원에 대한 산업정보보안 교육
산업기술보호 책임자	산업기술 관리자를 보조하는 총괄 실무 담당

	산업기술 취급과 관리를 위한 실무 책임자
	소관장비, 시설관리 실무책임, 모든 안전조치 및 보호의 실행
산업기술관리 담당자	산업기술 관련 문서 정리, 출입자 관리, 장비 관리
	산업기술 관리자, 산업기술보호 책임자의 보조 역할 수행

※ 출처 : 산업통상자원부 (2017)

5) 산업정보보안 교육

기업 내의 임직원에 대한 산업정보보안 교육은 지속해서 필요하며 보안의식을 강화할 수 있도록 자체교육 및 외부교육을 병행해야 할 필요가 있다. 자체교육의 경우 임직원을 대상으로 입사 시부터 퇴사 시까지 지속해서 이루어져야 하는 매우 중요한 산업정보보안 강화 수단이다. 이러한 교육을 통해 산업정보 유출을 감소시킬 수 있으며 유출 사고 발생 시 법적 증거로도 활용할 수 있다. 외부교육의 경우 기업 내 자체교육이 어렵거나 임직원들의 참여가 저조할 경우, 외부기관을 통해 위탁교육을 받을 수 있다. [표 4-7]과 [표 4-8]을 통해 산업정보보안 교육 내용을 확인할 수 있다(산업통상자원부, 2017).

[표 4-7] 산업정보보안 자체교육

구분	내용
시 기	정기교육 - 신규 채용 시 직원교육
	수시교육 - 연말, 연초에 집중적으로 실시 - 신규 사업 및 프로젝트 시작 시 - 외부에서 매수 등의 징후가 포착되었을 때 - 정보유출 방지에 관한 지침 제·개정시
대 상	전 임직원(파견근로자 및 외국인 포함)

내 용	산업정보보호 세부규정
	산업정보보호 관련 법률
	산업정보보호 서약서 작성요구의 이유 및 내용 설명
	생활보안 행동준칙(기관별 작성)
	기타 경영진의 판단 하에 교육하여야 할 내용들

※ 출처 : 산업통상자원부 (2017)

[표 4-8] 산업정보보안 외부교육

구분	내용
국가정보원 산업기밀보호센터	국가정보대학원 산업보안교육 - 외국의 산업정보 탐지동향 - 산업보안관리 실무 - 산업기밀 유출 사례 및 대책 - 사이버 보안관리 - 보안관리 우수업체 사례
	기업체 / 연구소 방문 교육 - 최근 산업스파이 사건 사례 - 산업체 종사자들의 산업기술 보호의식 함양 - 산업기술 보호 경각심 제고 - 보안관리 능력 - 해당 기업체에서 특별히 요청하는 분야
산업기술보호협회	교육내용 - 산업기술 유출방지 및 보호에 관한 법규와 보호지침 - 산업기술 유출방지 및 보호와 관련된 기술유출 현황과 대응방안
	관련법령 ‘산업기술 유출방지 및 보호에 관한 법률 시행령’ 제24조 (산업기술보호교육 실시)

※ 출처 : 산업통상자원부 (2017)

6) 퇴직 대상자 관리

산업정보 유출은 퇴직자에 의해 발생하는 사례가 많다. 그만큼 기업에서는

퇴직자에 대한 지속적인 관리 및 모니터링이 필요하다. 대기업의 경우 퇴직자에 대한 관리 프로세스가 정립되어있지만, 중소기업은 퇴직자에 대한 관리가 부족한 것이 현실이다. 우선 계약서에 입사 시부터 퇴직 시까지 보안 정책상 모니터링 대상임을 명시하고 임직원이 모니터링에 대한 거부감이 없도록 해야 한다. 또한, 퇴직예정자는 현업부서에서 모니터링 강화 통지 및 산업정보 유출 시, 민·형사상 손해배상책임을 묻는 것을 내용으로 하는 비밀유지서약서, 퇴직자보안서약서 작성이 필요하다. 단 퇴직대상자에 대한 인권침해가 되지 않는 조건에서 사후관리를 더욱 철저하게 하는 것이 산업기밀정보 유출 예방에 큰 도움이 될 것이다.

7) 침해사고 대응

산업정보 침해사고 대응 및 복구 계획은 침해예방 계획, 사고조치 계획, 복구계획 등으로 구분할 수 있으며 침해사고 대응 및 복구를 통해 기업의 피해를 줄이는 것을 목적으로 한다. 침해예방 계획에는 산업정보 유출 및 침해를 예방하기 위해 지켜야 할 사항들이 포함되어야 하며, 임직원들은 침해예방 계획을 잘 따르도록 해야 한다. 사고조치 계획에는 산업정보 유출 및 침해사고 발생을 대비해서 부서 및 임직원들이 조치해야 할 사항들을 미리 규정하고 침해사고 발생 시 사전에 정의한 규정에 따라 신속히 대응함으로써 이른 시일 안에 사고조치를 해야 한다. 복구계획은 관련된 내용을 따로 규정하고 기업의 업무 정상화를 위해 우선으로 노력해야 할 사항들을 확인할 수 있도록 해야 한다. 침해사고 대응 및 복구는 기업 내부적으로 훈련을 통해서 피해를 최소화하도록 노력해야 하며 [표 4-9]를 통해 침해사고 대응 및 복구 훈련방법을 확인할 수 있다(한국산업기술보호협회, 2017).

[표 4-9] 침해사고 대응 및 복구 훈련방법

구분	역할 및 책임
Table-top 훈련	대표이사 등의 경영진만 참여하여 메시지 위주로 시행하는 훈련이며 메시지에 대한 조치는 구두 혹은

	문서로 시행하고 조치에 따른 영향도를 미리 산정하여 메시지로 부여
Drill 훈련	메시지 및 모형을 이용하는 훈련
Exercise 훈련	산업정보 유출 및 침해상황을 실제 행동으로 조치하는 훈련

※ 출처 : 한국산업기술보호협회 (2017)

제 5 장 산업정보 유출 실증분석

제 1 절 산업정보 유출 실증분석 정의

산업정보·기술유출은 제조업, 서비스업에서 지속해서 발생하고 있다. 금융업의 경우 산업정보 유출과 비교하면 개인정보에 대한 유출이 더욱 빈번하므로 본 연구에서 다루고자 하는 산업정보 유출 실증분석은 금융업을 제외한 국내 중소기업에 속하는 제조업 세 곳과 서비스업 두 곳을 기준으로 실증분석을 진행하였다.

본 연구에서는 2018년~2019년 2년 동안 현업에서 정보보안 컨설팅을 진행한 중소기업 및 내부 산업정보 유출의심 사례가 발생하여 데이터 분석을 요청한 중소기업을 대상으로 실증분석을 진행하였다. 정보보안책임자 동의하에 수집한 반출 데이터를 기준으로 실제 유출로 의심되는 데이터에 대한 실증분석을 진행하였으며, 유출로 의심되는 데이터는 중소기업 정보보안담당자와 협업을 통해 확인하였고, 해당 데이터를 수집한 엔드포인트 보안 프로그램은 다음과 같다.

첫 번째로 중요정보유출방지솔루션[8] 을 통해 각 기업에서 취급하는 고유한 제품정보, 기술정보, 기밀키워드 등을 데이터 식별자 패턴 기반으로 정책구성 및 모니터링을 통해 임직원이 외부로 산업정보 반출 시, 저장되는 로그를 수집하여 실증분석을 진행하였다.

두 번째로 매체제어솔루션[9] 을 통해 각 기업에서 사전에 제공 및 인가된 이동식저장장치 외에 개인이 소유한 이동식저장장치 연결 및 업무용 문서파일 반출 시, 저장되는 로그를 수집하여 실증분석을 진행하였다.

실증분석 대상 업종별 외부로 반출한 데이터 중에 산업정보 유출·기술 유출로 의심되는 데이터로 판별한 기준은 [표 5-1]을 통해 명시하였으며, 현업에서 중소기업 정보보안 컨설팅과 산업정보 유출 데이터 분석 시 표준 지표로 활용하고 있다.

---

8) 중요정보유출방지솔루션 : PC 내의 중요정보유출방지 보안 솔루션(Symantec, 2018).

9) 매체제어솔루션 : 이동식저장장치 등 다양한 매체제어 보안 솔루션(Symantec, 2018).

[표 5-1] 산업정보 유출로 의심되는 데이터 판별 기준

산업정보 유출의심 영역	산업정보 유출의심 기준
이동식저장장치	개인 이동식저장장치를 통해 기밀키워드/제품정보/기술정보가 포함된 다수의 문서 반출
	문서, 도면 파일 확장자를 알 수 없는 확장자로 변경 후 반출
	퇴직 대상자 모니터링 시 개인 이동식저장장치를 통한 다수의 문서, 파일 반출
프린트	기밀키워드/제품정보/기술정보가 포함된 문서 출력
웹사이트	카페, 블로그, 커뮤니티에 기술정보가 포함된 문서 업로드
	구인·구직 사이트에 기술정보가 포함된 문서 업로드
	개인 NAS 서버에 다수의 업무 문서파일 저장
메일	경쟁사로 기밀키워드/제품정보/기술정보가 포함된 문서 및 파일 전송
	개인 메일로 기밀키워드/제품정보/기술정보가 포함된 문서 및 파일 전송
	알 수 없는 메일주소로 다수의 업무 문서파일 전송
클라우드	개인 클라우드로 기밀키워드/제품정보/기술정보가 포함된 다수의 문서 및 파일 저장
	퇴직 대상자 모니터링 시 개인 클라우드로 다수의 문서, 파일 저장
응용프로그램	메신저로 업무용 사진 및 중요정보가 포함된 파일 전송
	메신저로 기밀 문서파일 암호화 후 전송

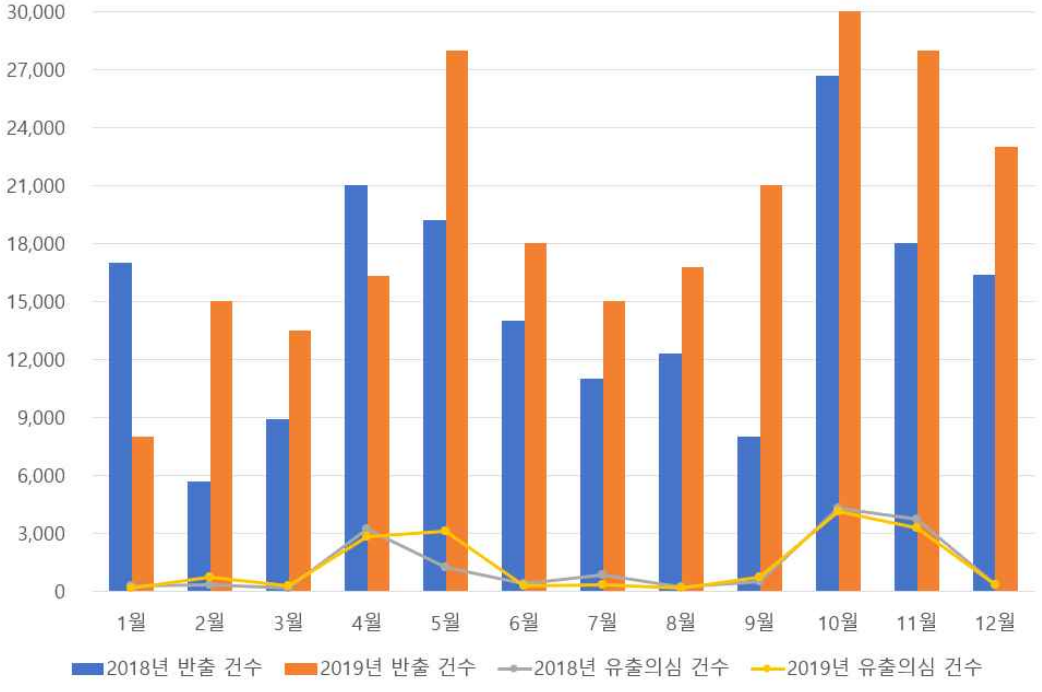
2018년~2019년에 수집한 반출데이터와 [표 5-1]의 기준을 통해 판별된 유출의심 데이터는 실증분석 대상인 중소기업별 그래프형식으로 월별 추이를 나타냈으며 유출의심 영역별 수치화하여 표로 작성하였다. 또한, 실증분석 대상인 중소기업 정보보안담당자와 설문조사를 통해 수집한 데이터를 기준으로 4장에서 제시한 산업보안 관리체계와 접목해서 기업별 산업정보보안 관리구성 현황에 대한 평가지표를 작성하였다. 등급은 총 6단계이며 가중치는 100% 기준으로 작성하였으며 정보보안담당자 주관적인 평가가 반영되었다.

제 2 절 중소 제조업 산업정보 유출 실증분석

국내 중소 제조업 A사, B사, C사에서 2년 동안 수집한 산업정보 반출 데이터 통계를 기준으로 산업정보 유출로 의심되는 데이터에 대한 실증분석을 진행하였다.

1) A제조사

국내에서 인지도가 높은 의약품 제조사이며 임직원들의 해외 출장이 잦고 기업 외부에서 근무하는 환경이 많아서 산업기밀정보 유출에 대한 위험도가 높으며 의약품 사업 특성상 영업비밀 자료 및 고유기술이 경쟁사로 유출될 경우, 기업의 존속 여부에 영향을 미치기 때문에 실증분석 대상으로 선정하였다.



[그림 5-1] A제조사 연도별 산업정보 반출, 유출의심 현황

[그림 5-1]을 통한 A제조사 실증분석 결과, 2018년도에는 총 178,200건의 데이터 반출이 있었고 그중에 약 15,540건은 데이터 유출의심으로 판단되었다. 또한, 2019년도에는 총 232,600건의 데이터 반출이 있었고 그중에 약 16,220건은 데이터 유출의심으로 판단되었다. 2018년 ~ 2019년도 사이 산업정보 반출 및 유출의심 건수가 동일 연도 기준 타 제조사보다 월등하게 높은 수치임을 확인할 수 있다. 의약품 제조기업 특성상 산업기밀정보로 정의된 다수의 제품번호 및 영업비밀 키워드로 인해 매월 평균 약 17,100건의 데이터를 반출했으며 유출로 의심되는 건수는 매월 평균 약 1,320건임을 확인할 수 있다. 그래프 추이를 살펴보면 상반기, 하반기 공개채용 이후 이직 시기인 4월, 5월, 10월, 11월에 데이터 반출 및 유출의심 건수가 가장 많았으며 11월에는 약 3,500건 이상의 산업정보 유출의심 현황이 확인되었다. 또한, 지속적인 기업의 성장으로 인한 임직원 수가 늘어나면서 2018년도(평균 1,295건)에 비해 2019년도(평균 1,352건)에 유출의심 건수가 평균 57건 정도 증가했음을 확인할 수 있다.

[표 5-2] A제조사 연도별 산업정보 반출, 유출의심 대상

대 상	2018년			2019년		
	비율(%)	반출 건	유출 건	비율(%)	반출 건	유출 건
이동식저장장치	17 %	30,297	2,642	15 %	34,890	2,433
프린트	2 %	3,564	311	6 %	13,956	973
웹사이트	15 %	26,733	2,331	12 %	27,912	1,946
메일	35 %	62,377	5,439	38 %	88,388	6,164
클라우드	23 %	40,990	3,574	22 %	51,172	3,569
응용프로그램	8 %	14,259	1,243	7 %	16,282	1,135
합 계	100 %	178,200	15,540	100 %	232,600	16,220
평 균(월)	-	14,852	1,295	-	19,383	1,352

[표 5-2]를 통해 2년 동안 임직원들이 어떤 영역을 통해 산업정보를 반출, 유출했는지 확인할 수 있다. 2018년도와 2019년도의 수치를 비교해보면 영역별로 비중은 비슷하며 메일을 통해 가장 많은 데이터를 반출, 유출하였다. 업무 특성상 메일로 데이터 및 정보를 주고받을 일이 많으므로 각각 35%, 38%를 차지하였고 클라우드를 통해서도 많은 비중의 데이터를 반출 및 유출했음을 확인하였다. 또한, 개인이 소지한 이동식저장장치를 연결해서 대량의 파일을 반출하였고

업무 목적 사이트가 아닌 비인가 사이트를 통해 내부기밀정보 및 업무용 문서를 업로드 했음을 확인하였다.

2018년 대비 2019년도에 데이터 반출 및 유출의심 건수가 지속해서 증가하고 있으므로 임직원들 대상으로 정보보안 교육을 통해 보안인식 향상이 필요할 것으로 판단되며, 업무 특성상 해외출장 및 외근이 잦으므로 엔드포인트 보안을 강화하고 사내·사외정책을 구분하여 모니터링 및 차단 정책을 운영해야 한다. 또한, 업무용 문서는 외부 반출 시, 사전에 부서장을 통해 승인을 받고 반출해야 하며 대외비 문서의 경우 마스킹처리 또는 암호화를 통해 보안을 강화하여 내부적인 프로세스 확립을 통한 효과적인 산업기밀정보 유출 대응방안이 필요하다.

[표 5-3] A제조사 산업보안 관리체계 평가지표

물리적 보안 관리체계		
항목	등급	가중치(%)
생체인식 보안	D	5%
출입통제 보안	A	40%
시설보호 보안	A	40%
물리시스템 백업 보안	B	15%
휴대장치 통제 보안	F	0%
기술적 보안 관리체계		
항목	등급	가중치(%)
네트워크 보안	B	35%
엔드포인트 보안	B	55%
시스템 보안	C	10%
관리적 보안 관리체계		
항목	등급	가중치(%)
정보보호 관리체계 인증제도	F	0%
산업정보보안 정책	B	20%
산업정보보호 조직체계	B	20%
산업정보보안 교육	A	25%
퇴직 대상자 관리	B	15%
침해사고 대응	B	20%

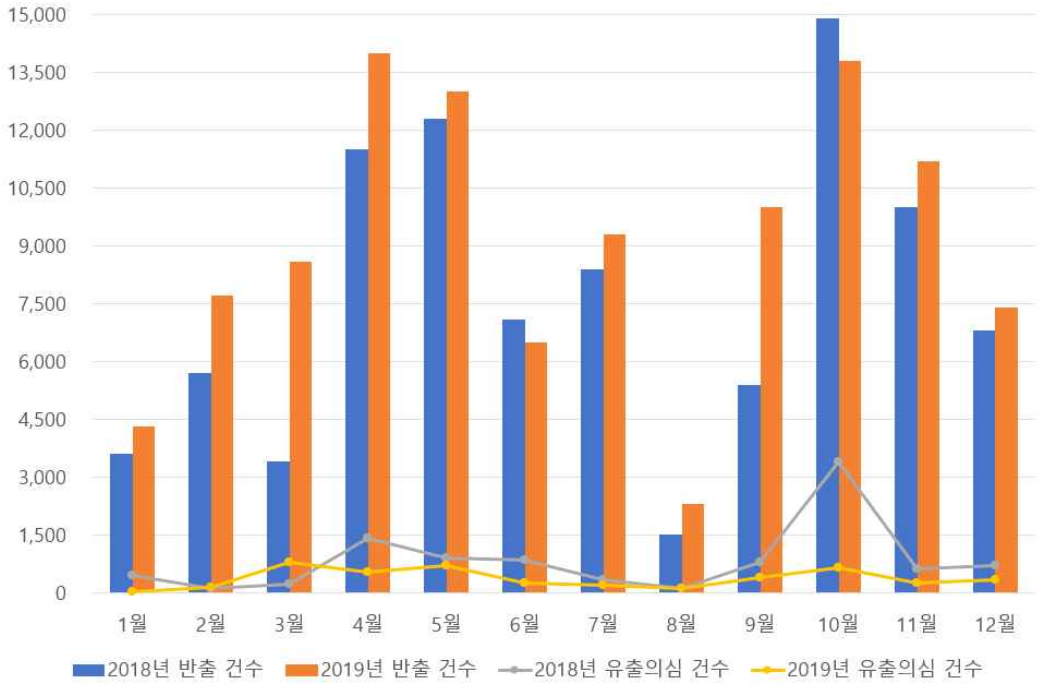
*등급 = A(100점), B(80점), C(60점), D(40점), E(20점), F(0점)

[표 5-3]의 A제조사 산업보안 관리체계 평가지표 설문 결과, 물리적 보안 관리체계에서 출입통제와 시설보호 보안은 철저한 관리가 이루어지고 있지만,

휴대장치는 전혀 통제가 없는 것으로 조사되었다. 개인 휴대장치를 통해 산업정보 유출사고가 지속적으로 발생할 수 있으므로 통제방안이 필요하다. 기술적 보안 관리체계에서는 엔드포인트 보안 가중치가 가장 높았으며 네트워크 보안과 시스템 보안에 대한 가중치 증가가 필요한 것으로 확인되었다. 관리적 보안 관리체계는 평균적으로 평가 등급이 높았으나 정보보호 관리체계 인증심사는 등급이 'F'이고 가중치는 0%인 것으로 확인되었다. 인증 통제항목을 통해 사전에 산업정보를 강화해야 할 필요성이 있다. 또한, 내부적으로 산업정보보호 조직체계가 확립되어있고 임직원들 대상으로 산업정보보안 교육을 주기적으로 실시함으로써 장기적인 관점에서 임직원들의 정보보안 수준 향상을 기대할 수 있다. A제조사는 전반적으로 산업보안 관리체계 평가 등급이 높지만 지속해서 유출의심 건수가 발생하고 있으므로 휴대장치 통제와 기술적 보안 강화가 필요하며 퇴직 대상자 관리에 대한 가중치가 낮으므로 지속해서 퇴직 대상자 관리가 필요하다는 결과를 도출할 수 있다.

2) B제조사

엘리베이터 제조사이며 사무직보다 현장에서 근무하는 인원들이 많아서 산업정보 유출 사고가 빈번하게 발생하며, 국내에 경쟁사가 많으므로 내부 중요 기술정보 및 기밀자료가 유출될 시 기업의 가치가 하락하고 경쟁력이 떨어질 수 있으므로 실증분석 대상으로 선정하였고 수집한 데이터를 기준으로 실증분석을 진행하였다.



[그림 5-2] B제조사 연도별 산업정보 반출, 유출의심 현황

[그림 5-2]를 통해 B제조사 실증분석 결과, 2018년도에는 총 90,600건의 데이터 반출이 있었고 그중에 약 9,950건은 데이터 유출의심으로 판단되었다. 또한, 2019년도에는 총 108,100건의 데이터 반출이 있었고 그중에 약 4,370건은 데이터 유출의심으로 판단되었다. 산업기밀정보로 정의된 설계도면 파일에 대한 반출 건수가 많았으며 사업 금액, 제품 단가 등 영업비밀 내용이 포함된 문서도 반출 및 유출의심 건수가 많았다. 매월 평균 약 8,200건의 데이터를 반출했으며 유출로 의심되는 건수는 매월 평균 약 600건임을 확인할 수 있다. 그래프 추이를 살펴보면 날씨가 좋은 3월, 4월, 5월, 9월, 10월, 11월에 사업이 진행되면서 동시에 내부적으로 데이터 반출 및 유출의심 건수가 가장 많았으며 2018년 10월에는 약 3,400건 이상의 산업정보 유출의심 현황이 확인되었다. 8월에는 데이터 반출 및 유출의심 건수가 가장 적었는데 업무 특성상 현장에서 근무하는 직원이 많고 8월에 현장 직원 모두 하계휴가를 떠나서 수집된 데이터가 다른 월에 비해 적음을 알 수 있으며, 2018년도(평균 829건)에 비해 2019년도(평균 364건)에 유출의심 건수가 대폭 감소했음을 확인할 수 있다.

[표 5-4] B제조사 연도별 산업정보 반출, 유출의심 대상

대 상	2018년			2019년		
	비율(%)	반출 건	유출 건	비율(%)	반출 건	유출 건
이동식저장장치	32 %	28,992	3,184	28 %	30,268	1,224
프린트	39 %	35,334	3,881	33 %	35,673	1,442
웹사이트	10 %	9,060	995	16 %	17,296	699
메일	13 %	11,778	1,293	15 %	16,215	655
클라우드	4 %	3,624	398	5 %	5,405	219
응용프로그램	2 %	1,812	199	3 %	3,243	131
합 계	100 %	90,600	9,950	100 %	108,100	4,370
평 균(월)	-	7,550	829	-	9,008	364

[표 5-4]를 통해 B제조사 임직원들이 어떤 영역을 통해 산업정보를 반출, 유출했는지 확인할 수 있다. 2018년도와 2019년도 모두 이동식저장장치 및 프린트를 통해 데이터 반출 및 유출을 하였다. 업무 특성상 현장직이 많고 메일보단 문서를 직접 출력해서 업무를 진행하거나 이동식저장장치로 자료를 전달하기 때문에 두 가지 영역의 점유율이 높았다. 웹사이트, 메일, 클라우드, 응용프로그램으로 데이터를 반출 및 유출한 직원은 대부분 사무직으로 확인되었다. 프린트를 통해 도면이나 제품정보 등을 출력하는 사례가 많았기 때문에 출력물에 대한 보안 강화가 필요하다고 판단된다. 출력 시 워터마크를 통해 어느 부서 직원이 해당 문서를 출력했는지 문서에 표기해야 하며, 내부 기밀정보가 포함된 문서를 출력 시 출력이 차단되도록 정책을 운영해야 한다. 사무직과 현장직에 대한 구분을 통해 산업정보보안을 강화해야 할 필요성이 있다.

[표 5-5] B제조사 산업보안 관리체계 평가지표

물리적 보안 관리체계		
항목	등급	가중치(%)
생체인식 보안	F	0%
출입통제 보안	A	45%
시설보호 보안	A	50%
물리시스템 백업 보안	E	5%
휴대장치 통제 보안	F	0%
기술적 보안 관리체계		

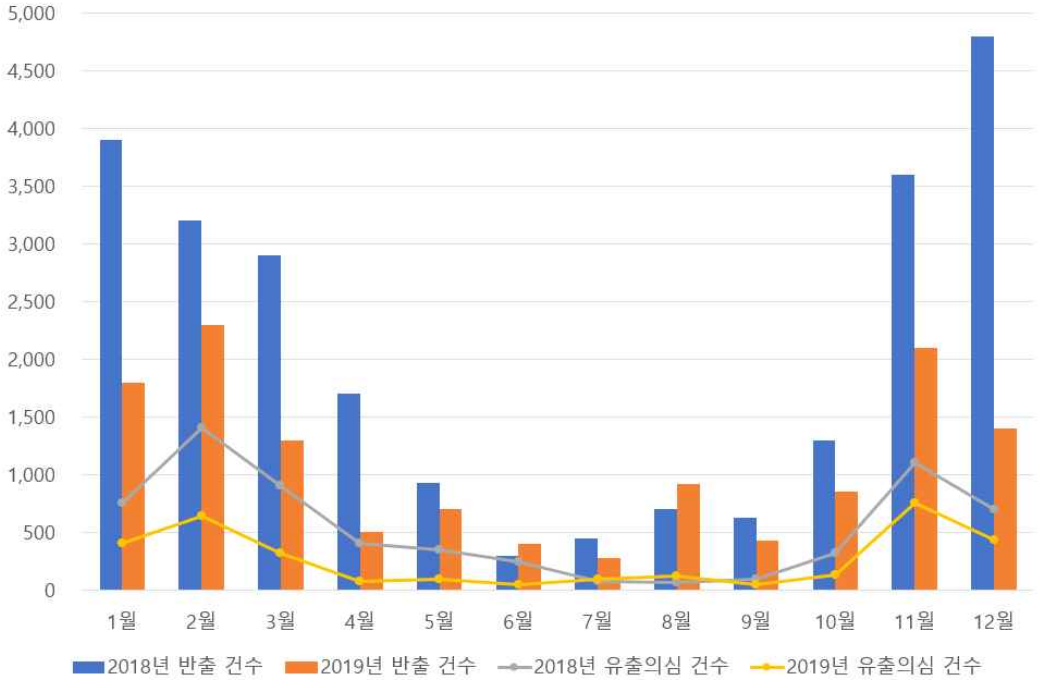
항목	등급	가중치(%)
네트워크 보안	C	35%
엔드포인트 보안	B	60%
시스템 보안	E	5%
관리적 보안 관리체계		
항목	등급	가중치(%)
정보보호 관리체계 인증제도	F	0%
산업정보보안 정책	C	20%
산업정보보호 조직체계	E	5%
산업정보보안 교육	D	10%
퇴직 대상자 관리	A	45%
침해사고 대응	C	20%

*등급 = A(100점), B(80점), C(60점), D(40점), E(20점), F(0점)

[표 5-5]의 B제조사 산업보안 관리체계 평가지표 설문 결과, 물리적 보안 관리체계에서 출입통제와 시설보호 보안은 철저한 관리가 이루어지고 있지만, 휴대장치 통제와 생체인식 보안은 관리체계가 없는 것으로 조사되었다. A제조사와 마찬가지로 휴대장치를 통해 다양한 산업정보 유출사고가 지속해서 발생할 수 있으므로 통제방안이 필요하며, 기업 자산에 접근 시, 생체인식을 통해 정확한 임직원 식별 보안기술이 필요하다. 기술적 보안 관리체계에서는 엔드포인트 보안 가중치가 가장 높았으며 네트워크 보안 가중치는 상대적으로 낮은 것으로 확인되었다. 시스템 보안의 경우 없다고 해도 무방할 정도로 가중치가 낮으므로 시스템 보안에 대한 대책 마련이 시급한 것으로 판단된다. 관리적 보안 관리체계는 평균적으로 평가 등급이 낮으며 A제조사와 동일하게 정보보호 관리체계 인증심사는 등급이 F이고 가중치는 0%인 것으로 확인하였다. B제조사도 인증통제항목을 통해 사전에 산업정보 강화가 필요하며 기업의 보안 수준에 대한 점검이 필요하다. 산업정보보호 조직의 경우, 조직이 별도로 구성되어 있지 않으며 전산실에서 정보보안 업무를 처리하고 있으므로 산업정보보호 조직을 체계적으로 구성해야 할 필요성이 있다. B제조사는 전반적으로 산업보안 관리체계 평가등급이 낮고 매월 꾸준히 산업정보 유출의심 건이 발생하고 있지만, 퇴직 대상자 관리를 통해 2018년 대비 2019년에는 산업정보 유출의심 건수가 대폭 감소한 결과를 도출하였다.

3) C제조사

자동차 부품 제조사이며 부품정보 및 산업 기술정보를 중요하게 다루고 있다. 국내에 다양한 경쟁업체가 있고 특허받은 제품에 대한 데이터를 소유하고 있으며 점차 임직원들의 보안의식이 강화됨을 확인할 수 있었으므로 실증분석 대상으로 선정하였다.



[그림 5-3] C제조사 연도별 산업정보 반출, 유출의심 현황

[그림 5-3]을 통한 C제조사 실증분석 결과, 2018년도에는 총 24,410건의 데이터 반출이 있었고 그중에 약 6,380건은 데이터 유출의심으로 판단되었다. 또한, 2019년도에는 총 12,980건의 데이터 반출이 있었고 그중에 약 3,130건은 데이터 유출의심으로 판단되었다. 매월 평균 약 1,550건의 데이터를 반출했으며 유출로 의심되는 건수는 매월 평균 약 400건임을 확인할 수 있다. 유출로 의심되는 데이터는 대부분 특허받은 부품정보. 설계도면, 영업 기밀문서로 확인되었

다. 그래프 추이를 살펴보면 자동차 부품 제조업 특성상 연말부터 연초까지 데이터 반출 및 유출의심 건수가 가장 많았으며 2019년 11월에는 약 1,100건 이상의 산업정보 유출의심 현황이 확인되었다. 7월, 8월 여름 휴가 시즌에는 수집된 데이터가 미미했으며 지속해서 임직원 정보보안 교육 및 관리, 보안솔루션 도입 등을 통한 산업정보보안을 강화함으로써 2018년도(평균 532건)에 비해 2019년도(평균 261건)에 유출의심 건수가 대폭으로 감소했음을 확인할 수 있다. 또한, 퇴직 예정자는 별도로 관리하여 산업정보 유출 건수를 감소시켰다.

[표 5-6] C제조사 연도별 산업정보 반출, 유출의심 대상

대 상	2018년			2019년		
	비율(%)	반출 건	유출 건	비율(%)	반출 건	유출 건
이동식저장장치	57 %	13,914	3,636	62 %	8,048	1,941
프린트	19 %	4,638	1,213	9 %	1,168	282
웹사이트	8 %	1,953	510	7 %	909	219
메일	13 %	3,173	829	17 %	2,207	532
클라우드	2 %	488	128	4 %	519	125
응용프로그램	1 %	244	64	1 %	129	31
합 계	100 %	24,410	6,380	100 %	12,980	3,130
평 균(월)	-	2,034	532	-	1,082	261

[표 5-6]을 살펴보면 이동식저장장치를 통해 가장 많은 데이터를 반출, 유출하였다. 개인이 소지한 이동식저장장치를 연결해서 대량의 파일을 반출하였고 경쟁사 또는 알 수 없는 메일로 업무자료를 전송하였다. 또한, 부품정보를 대량으로 출력한 이력도 확인할 수 있었다.

2018년 대비 2019년도에는 데이터 반출 및 유출의심 건수가 대폭 감소했으며 임직원들이 산업정보보안에 대한 의식을 강화하고 있다는 것을 알 수 있었다. 하지만 이동식저장장치를 통한 데이터 반출 및 유출의심 건수가 많으므로 내부적으로 이동식저장장치에 대한 보안체계를 확립해야 할 필요성이 있다.

[표 5-7] C제조사 산업보안 관리체계 평가지표

물리적 보안 관리체계		
항목	등급	가중치(%)

생체인식 보안	F	0%
출입통제 보안	A	30%
시설보호 보안	A	50%
물리시스템 백업 보안	B	15%
휴대장치 통제 보안	D	5%
기술적 보안 관리체계		
항목	등급	가중치(%)
네트워크 보안	B	50%
엔드포인트 보안	C	35%
시스템 보안	D	15%
관리적 보안 관리체계		
항목	등급	가중치(%)
정보보호 관리체계 인증제도	F	0%
산업정보보안 정책	B	20%
산업정보보호 조직체계	D	5%
산업정보보안 교육	A	35%
퇴직 대상자 관리	B	20%
침해사고 대응	B	20%

*등급 = A(100점), B(80점), C(60점), D(40점), E(20점), F(0점)

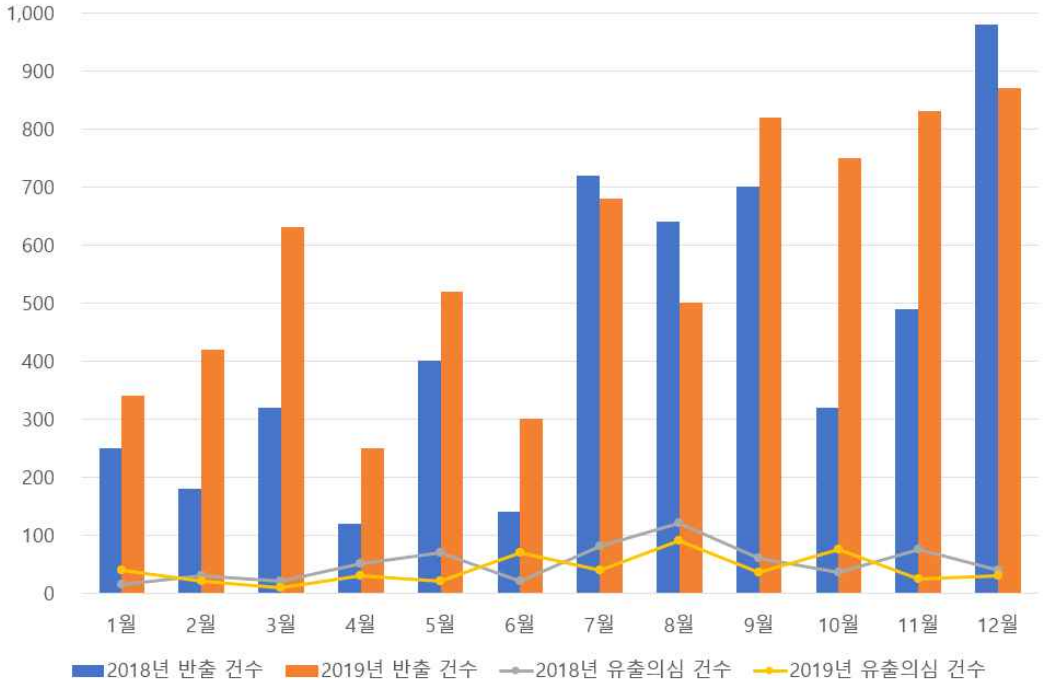
[표 5-7]의 C제조사 산업보안 관리체계 평가지표 설문 결과, 물리적 보안 관리체계에서 출입통제와 시설보호 보안은 철저한 관리가 이루어지고 있지만, 생체인식 보안은 관리체계가 없는 것으로 조사되었다. 임직원들은 카드키를 통해 출입하고 있으며, 카드키 분실 시 외부인 출입 가능성이 존재하므로 생체인식을 통해 정확한 임직원 식별 보안기술이 필요하다. 휴대장치 통제의 경우 휴대장치 카메라에 보안스티커를 부착하여 불법촬영 및 산업정보 유출을 통제하였다. 기술적 보안 관리체계에서는 네트워크 보안 가중치가 가장 높았으며 엔드포인트 보안과 시스템 보안 가중치 증가가 필요한 것으로 확인되었다. 관리적 보안 관리체계에서 정보보호 관리체계 인증심사는 A제조사와 B제조사와 동일하게 등급이 F이고 가중치는 0%인 것으로 확인하였다. 산업정보보호 조직체계 구성은 D등급으로 평가되었으며 산업정보보호 인력도 부족한 것으로 확인되었다. C제조사는 산업보안 관리체계 평가 등급은 보통이지만 지속적인 보안솔루션 도입, 지속적인 산업정보보안 교육, 퇴직 대상자 관리를 통해 2018년 대비 2019년에는 산업정보 유출의심 건수가 대폭 감소한 결과를 도출하였다.

제 3 절 중소 서비스업 산업정보 유출 실증분석

국내 중소 서비스업 A사, B사, C사에서 2년 동안 수집한 산업정보 반출 데이터 통계를 기준으로 산업정보 유출로 의심되는 데이터에 대한 실증분석을 진행하였다.

1) A서비스사

국내에서 인지도가 있는 호텔을 운영 중이며 기업의 특성상 산업정보 유출에 대한 위험도는 적지만 기업에서 보유하고 있는 고객 개인정보 및 사업 관련 대외비 문서가 유출되고 있음을 확인하였기에 실증분석 대상으로 선정하였다.



[그림 5-4] A서비스사 연도별 산업정보 반출, 유출의심 현황

[그림 5-4]를 통한 A서비스사 실증분석 결과, 2018년도에는 총 5,260건의 데이터 반출이 있었고 그중에 약 610건은 데이터 유출의심으로 판단되었다. 또한, 2019년도에는 총 6,910건의 데이터 반출이 있었고 그중에 약 485건은 데이터 유출의심으로 판단되었다. 매월 평균 약 500건의 데이터를 반출했으며 유출로 의심되는 건수는 매월 평균 약 46건임을 확인할 수 있다. 그래프 추이를 살펴보면 여름인 7월, 8월, 9월과 겨울인 11월, 12월에 데이터 반출 및 유출의심 건수가 많았으며 2018년 8월에는 약 120건의 산업정보 유출의심 현황이 확인되었다. 2018년도(평균 51건)에 비해 2019년도(평균 40건)에 유출의심 건수가 감소했음을 확인할 수 있다. 반출 및 유출의심 데이터의 대부분은 고객 개인정보로 확인되었으며, 내부 대외비 문서도 경쟁업체 메일로 전달된 것을 확인하였다.

[표 5-8] A서비스사 연도별 산업정보 반출, 유출의심 대상

대 상	2018년			2019년		
	비율(%)	반출 건	유출 건	비율(%)	반출 건	유출 건
이동식저장장치	5 %	264	31	3 %	207	15
프린트	3 %	158	18	5 %	346	24
웹사이트	20 %	1,052	122	15 %	1,037	73
메일	70 %	3,682	427	75 %	5,182	363
클라우드	1 %	52	6	1 %	69	5
응용프로그램	1 %	52	6	1 %	69	5
합 계	100 %	5,260	610	100 %	6,910	485
평 균(월)	-	438	51	-	576	40

[표 5-8]을 살펴보면 A서비스사의 경우 메일과 웹사이트를 통해서 약 90%의 데이터가 반출 및 유출되었고 개인 메일을 통해 고객 개인정보가 포함된 문서를 전송한 사례가 많았으며 개인 블로그와 카페에 대외비 문서에 관한 내용을 업로드 한 것을 확인하였다.

기업의 특성상 외부로 산업정보를 반출할 사례가 적으며 다른 서비스사와 비교 시 산업정보보다는 개인정보 위주로 반출된 것을 확인하였지만, 내부 중요 대외비 문서도 유출되지 않도록 임직원에 대한 관리 및 정보보안 교육이 필요할 것으로 판단된다.

[표 5-9] A서비스사 산업보안 관리체계 평가지표

물리적 보안 관리체계		
항목	등급	가중치(%)
생체인식 보안	F	0%
출입통제 보안	B	90%
시설보호 보안	E	10%
물리시스템 백업 보안	F	0%
휴대장치 통제 보안	F	0%
기술적 보안 관리체계		
항목	등급	가중치(%)
네트워크 보안	C	60%
엔드포인트 보안	C	40%
시스템 보안	F	0%
관리적 보안 관리체계		
항목	등급	가중치(%)
정보보호 관리체계 인증제도	F	0%
산업정보보안 정책	D	20%
산업정보보호 조직체계	E	5%
산업정보보안 교육	F	0%
퇴직 대상자 관리	E	5%
침해사고 대응	B	70%

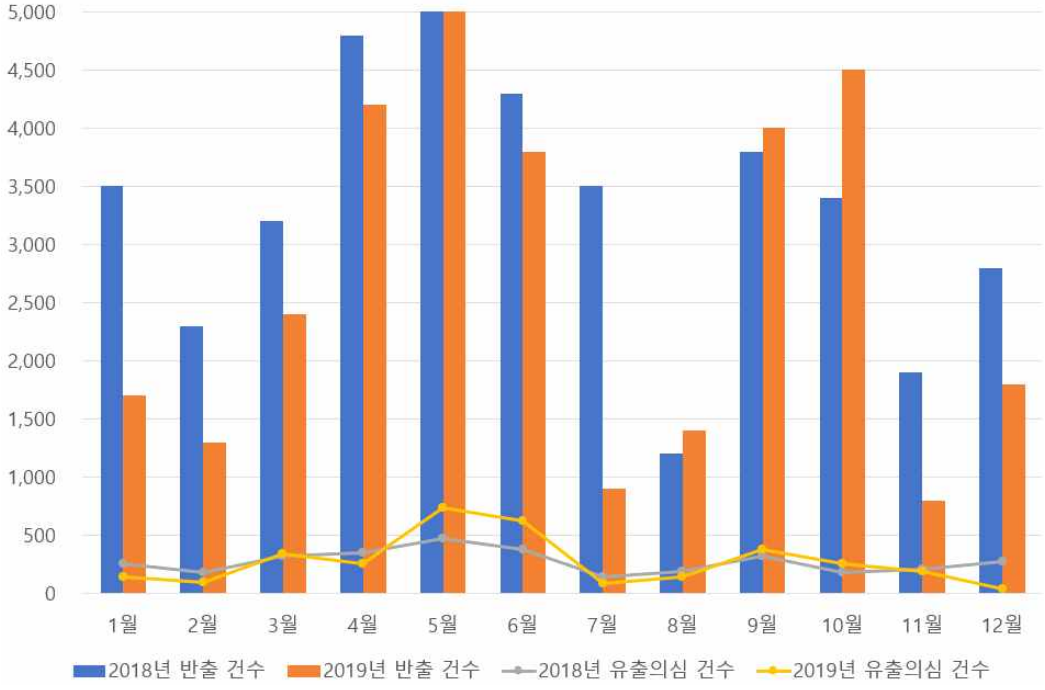
*등급 = A(100점), B(80점), C(60점), D(40점), E(20점), F(0점)

[표 5-9]의 A서비스사 산업보안 관리체계 평가지표 설문 결과, 물리적 보안 관리체계에서 업종 특성상 출입통제 보안은 가중치가 높지만, 시설보호 보안의 경우, 보호해야 할 시설이 많이 없으므로 가중치가 낮은 것으로 확인되었다. 생체인식 보안은 관리체계가 없는 것으로 조사되었다. 제조사와 동일하게 임직원들은 카드키를 통해 출입하고 있으며, 카드키 분실 시 호텔 방문 고객에게 영향이 생길 수 있으므로 정확한 임직원 식별 보안기술이 필요하다. 물리시스템 백업 보안의 경우 재해복구센터를 통한 이중화 구성 관리체계는 없었으며, 기업 내부 인프라 장애 발생 시, 대응방안 마련이 필요하다. 기술적 보안 관리체계에서는 전체적으로 평가등급이 낮았으며 기술적 보안에 관한 관심이 적은 것으로 확인되었다. 관리적 보안 관리체계도 전체적으로 평가등급이 낮지만, 침해사고 대응은 전반적으로 평가 등급이 높음을 확인할 수 있다. 또한, 임직원들 대상으

로 산업정보보안 교육은 진행된 사례가 없었다. A서비스사는 산업보안 관리체계 평가 등급이 매우 낮으며 물리적 보안 관리체계, 기술적 보안 관리체계, 관리적 보안 관리체계를 지속해서 관리하고 많은 개선이 필요하다는 결론이 도출되었다.

2) B서비스사

국내에서 구인·구직 사이트를 운영하는 기업이며 광고, 마케팅, 개발 소스 등의 산업정보들이 경쟁사로 유출되었을 경우 기업의 자산에 큰 영향을 미칠 수 있으므로 실증분석 대상으로 선정하여 분석을 진행하였다.



[그림 5-5] B서비스사 연도별 산업정보 반출, 유출의심 현황

[그림 5-5]를 통해 B서비스사 실증분석 결과, 2018년도에는 총 39,700건의 데이터 반출이 있었고 그중에 약 2,990건은 데이터 유출의심으로 판단되었다. 또한, 2019년도에는 총 31,800건의 데이터 반출이 있었고 그중에 약 3,250건은

데이터 유출의심으로 판단되었다. 영업 및 마케팅에 관한 내용이 포함된 문서를 대다수 반출했으며 업무와 연관된 개발 소스 파일도 반출한 것을 확인하였다. 매월 평균 약 3,000건의 데이터를 반출했으며 유출로 의심되는 건수는 매월 평균 약 270건임을 확인할 수 있다. 그래프 추이를 살펴보면 업종 특성상 구인·구직 시기인 4월, 5월, 6월, 9월, 10월에 데이터 반출 및 유출의심 건수가 많았으며 하계휴가인 07월, 08월에는 비교적으로 데이터 반출 및 유출의심 건수가 감소한 걸 확인할 수 있다. 2019년 05월에는 반출 건수가 가장 많았으며 약 730건 이상의 산업정보 유출의심 현황이 확인되었다. 2018년도(평균 249건)에 비해 2019년도(평균 270건)에 발생한 유출의심 건수는 증가한 것으로 확인되었다.

[표 5-10] B서비스사 연도별 산업정보 반출, 유출의심 대상

대 상	2018년			2019년		
	비율(%)	반출 건	유출 건	비율(%)	반출 건	유출 건
이동식저장장치	4 %	1,588	119	2 %	636	65
프린트	3 %	1,191	90	2 %	636	65
웹사이트	21 %	8,337	628	13 %	4,134	423
메일	19 %	7,543	568	18 %	5,724	584
클라우드	29 %	11,513	867	36 %	11,448	1,170
응용프로그램	24 %	9,528	718	29 %	9,222	943
합 계	100 %	39,700	2,990	100 %	31,800	3,250
평 균(월)	-	3,308	249	-	2,650	270

[표 5-10]을 통해 B서비스사 임직원들이 어떤 영역을 통해 산업정보를 반출, 유출했는지 확인할 수 있다. 기업 내부적으로 이동식저장장치와 프린트 출력에 대한 통제로 인해 해당 영역을 통한 데이터 반출은 비중이 작았고 업무 특성상 웹사이트 및 메일을 통해 데이터 반출 및 유출행위가 모니터링되었다. 또한, 개인 클라우드 및 메신저를 통해 대량의 업무용 파일을 전송한 행위를 확인했으며 퇴직대상자 모니터링 시, 업무용 PC에 저장된 데이터를 개인 클라우드로 업로드한 이력을 확인할 수 있었다. 업무용 PC에 저장된 데이터를 개인 클라우드로 업로드 하는 것은 명확한 산업정보 유출로 판단되며 웹사이트, 메일, 클라우드, 응용프로그램 통제를 통해 산업정보 반출 및 유출의심 건수가 감소할 수 있도록 기

업과 임직원들의 노력이 필요할 것으로 판단된다.

[표 5-11] B서비스사 산업보안 관리체계 평가지표

물리적 보안 관리체계		
항목	등급	가중치(%)
생체인식 보안	A	40%
출입통제 보안	B	20%
시설보호 보안	C	10%
물리시스템 백업 보안	A	30%
휴대장치 통제 보안	F	0%
기술적 보안 관리체계		
항목	등급	가중치(%)
네트워크 보안	B	45%
엔드포인트 보안	A	55%
시스템 보안	F	0%
관리적 보안 관리체계		
항목	등급	가중치(%)
정보보호 관리체계 인증제도	B	40%
산업정보보안 정책	B	10%
산업정보보호 조직체계	B	10%
산업정보보안 교육	B	10%
퇴직 대상자 관리	B	5%
침해사고 대응	B	25%

*등급 = A(100점), B(80점), C(60점), D(40점), E(20점), F(0점)

[표 5-11]의 B서비스사 산업보안 관리체계 평가지표 설문 결과, 물리적 보안 관리체계에서 생체인식 보안과 물리시스템 백업 보안 평가 등급이 높은 것을 확인할 수 있다. 기업 내 모든 출입은 생체인식을 통해 인증하였으며 재해복구센터를 통한 이중화도 다른 중소기업 대비 구성체계가 되어있다. 업종 특성상 개발 소스 및 영업기밀정보를 휴대장치를 통해 유출할 수 있으므로 휴대장치 통제 방안 마련이 시급하다. 기술적 보안 관리체계에서 네트워크 보안과 엔드포인트 보안은 가중치가 높고 관리체계에서 부족한 부분은 없었으며 중요 서버에 대한 시스템 보안은 필요한 것으로 확인되었다. 관리적 보안 관리체계에서 정보보호 관리체계 인증은 가중치가 높았으며 해마다 ISMS 인증심사를 진행하였으며 통제항목을 통해 보안영역 관리를 지속적으로 하였다. B서비스사는 전반적으로

산업보안 관리체계 평가 등급이 높았으며 평가 등급이 F인 휴대장치 통제 및 시스템 보안은 개선이 필요하다는 결론이 도출되었다.

제 4 절 산업정보 유출 실증분석 결과

국내 금융업의 경우 망분리 사업을 통해 업무망·인터넷망이 분리되어있고 다양한 보안솔루션 도입을 통해 개인정보 및 산업정보 유출 건수가 감소하고 있지만, 국내 중소기업 대다수의 제조업과 서비스업의 경우 망분리 환경이 구성되어 있지 않고 임직원들의 정보보안 의식이 낮으며 내부 정보보안 프로세스가 명확하게 확립되어있지 않아 산업정보 유출의심 건수가 매년 발생하고 있음을 위의 실증분석을 통해 확인할 수 있다. 물론 기업과 임직원들의 노력으로 2018년도 대비 2019년도에는 산업정보 유출의심 건수가 감소한 기업도 확인할 수 있었다.

실증분석을 진행한 다섯 곳의 중소기업 모두 이직 시기에는 데이터 반출 및 유출의심 건수가 많았으며, 하계휴가 시기에는 데이터 반출 및 유출의심 건수가 비교적 감소하였다. 제조사의 경우 평균적으로 데이터 반출 및 유출의심 건수가 많았으며, 대부분 이동식저장장치 및 프린트를 통해 데이터 반출이 되었음을 확인할 수 있었다. 서비스사의 경우 웹사이트, 메일, 클라우드를 통해 다수의 데이터가 반출되었으며 반출 건수에 비례해서 유출의심 건수가 높음을 확인할 수 있었다. 특히 다섯 곳의 기업 모두 퇴사 대상자를 모니터링 한 결과, 다양한 경로를 통해 데이터 반출 및 백업을 시도 하였고 일부 퇴사 대상자는 1,000건이 넘는 산업기밀정보를 유출 시도하였다. 또한, 클라우드 기술이 발전함에 따라 개인 클라우드에 산업기밀정보를 저장한 사례가 많았으며, 일부 사용자의 경우 개인 NAS 서버를 구축해서 데이터 백업을 진행했음을 확인하였다. 사내에 NAS[10] 서버가 있음에도 불구하고 개인 NAS 서버에 업무용 파일을 백업하는 행위는 명백하게 산업정보 유출로 판단할 수 있다. 이와 비슷하게 제조업의 경우 사내에서 인가된 보안 이동식저장장치가 아닌 개인 이동식저장장치를

10) NAS : 네트워크에 연결된 스토리지 기기로 클라우드와 비슷하며 데이터를 저장하고 검색할 수 있다 (SEAGATE, 2020)

연결하고 데이터를 전송하는 행위가 있었으며 개인 메일을 통해 경쟁사로 영업 비밀문서를 전송한 행위도 모니터링되었고 해당 건들은 산업정보 유출로 판단한 기준이 되었다. 서비스업의 경우 사내 메신저가 아닌 개인 메신저를 통해 업무용 문서를 업로드 한 행위가 다수 모니터링되었다.

추가로 실증분석 대상 기업의 정보보안담당자 설문을 통해 수집한 산업보안 관리체계 평가지표를 기반으로 해당 기업의 산업보안 현황을 분석하였다.

제조사의 경우 세 곳 모두 생체인식 보안 및 휴대장치 통제 보안 평가 등급이 'D'이하로 낮았으며 가중치는 5% 미만으로 확인되었다. 하지만 제조사 특성상 출입통제 보안 및 시설보호 보안은 모두 평가 등급이 'A'였으며 가중치도 평균 40% 이상으로 확인되었다. 생체인식과 휴대장치 통제 보안이 도입된다면 물리적 경로를 통한 산업정보 유출사고는 감소할 것으로 판단된다. 기술적 보안 관리체계의 경우 네트워크 보안과 엔드포인트 보안은 가중치가 높았지만, 시스템 보안영역은 가중치가 평균 10%로 확인되었으며 시스템 보안을 통한 기업 내 중요 서버들의 보호가 필요하다. 세 곳의 제조사 모두 정보보호 관리체계 인증제도는 평가받은 사례가 없었으며 전반적으로 관리적 보안 관리체계가 잘 이루어지고 있음을 확인할 수 있다. 특히 B제조사의 경우, 퇴직 대상자 관리를 통해 산업정보 유출 건수가 감소하였으며 세 곳의 제조사 모두 산업정보보호 조직체계가 명확히 구성된다면 전체적인 산업정보 관리체계가 향상될 것이라는 결론이 도출되었다.

서비스사 산업보안 관리체계 평가지표를 살펴보면 A서비스사는 물리시스템 백업, 휴대장치 통제, 네트워크 보안, 엔드포인트 보안, 산업정보보호 조직체계, 산업정보보안 교육, 퇴직 대상자 관리 등 전반적인 산업정보 관리체계가 미흡한 것으로 확인되었다. 아직 기업의 규모가 작아서 산업정보 유출의심 건수는 적었지만, 호텔 사업 특성상 영업비밀 및 고객 개인정보가 유출될 시 기업의 매출에 큰 손실이 생길 수 있으므로 지속적인 산업보안 관리체계를 구축해야 할 필요성이 있다. B서비스사의 경우 전반적으로 산업보안 관리체계가 구성되어 있으며 정보보호 관리체계 인증제도인 ISMS 인증심사를 통해 주기적으로 기업의 산업보안을 점검하고 취약한 부분은 개선할 수 있는 것을 확인하였다. 기술적 보안 관리체계에서 엔드포인트 보안에 가중치는 55%로 높았으며 평가

등급도 ‘A’였지만 산업정보 유출의심 건수는 2018년 대비 2019년에 증가한 것으로 확인되었다. B서비스사는 기술적 보안뿐만 아니라 관리적 보안을 통해 산업정보보호 조직체계를 강화하고 임직원들 대상으로 산업정보보안 교육을 주기적으로 실시하며, 퇴직 대상자를 철저하게 관리해야 할 필요성이 있다는 결론이 도출되었다.

위에서 사전에 정의한 산업정보 유출로 의심되는 데이터 기준으로 다섯 곳의 중소기업을 선정하여 산업정보 유출 실증분석을 진행하였으며 현업에서 종사하는 정보보안담당자 설문을 기반으로 작성된 산업보안 관리체계 평가지표를 통해 중소기업의 산업보안 실태를 파악할 수 있었으며 산업정보 유출을 감소시키기 위해 기업별로 어떤 관리체계가 필요한지 확인함으로써 의미 있는 결과를 도출하였다.

제 6 장 결 론

제 1 절 결론 및 시사점

중소기업 산업은 갈수록 고도화되고 산업정보·산업기술 유출 건은 매년 발생하고 있다. 산업보안에 대한 관리적 보안, 기술적 보안, 물리적 보안이 강화되고 있음에도 불구하고 중소기업 산업정보·산업기술 유출 건은 꾸준히 발생하고 있으며 이는 국내 중소기업 산업보안에 대한 한계점을 시사하고 있다.

국내의 경우 산업정보·산업기술 유출 심각성과 비교하면 처벌은 낮은 수준이다. 적발되더라도 기술유출 사범의 기소율이 낮고, 처벌도 벌금·집행유예가 대부분이다. 또한, 기술 침해 시 손해배상액 기준이 가해자의 이익액 기준이며, 기술유출로 인한 불법적 금전 이득 환수를 위한 법적 수단이 없다. 그리고 낮은 보안수준 및 인적 역량의 문제점도 있다. 국내 보안기술은 미국 대비 85.5%, 기술격차는 1년으로 지속적 보안기술 투자가 필요하나 정부 차원의 지원은 거의 없는 실정이다. 중소기업 내 보안전문가 채용의무는 없고, 보안업무도 비핵심 업무로 분류되어 기업 내 보안인력은 입지가 줄어들고 있으며 보안인력에 대한 처우가 낮고 중소기업 내 산업정보보안 관련 인력 및 설비투자 여력이 부족한 상황이다.

반면에 위의 실증분석을 통해 확인 결과, 산업정보보안에 인력 및 설비를 투자한 중소기업은 단기간에 산업정보 유출의심 건수가 줄어들었음을 데이터를 통해 확인할 수 있었다. 완벽한 보안은 없지만, 기업과 임직원들이 산업정보보안에 관해 관심을 조금이라도 가진다면, 점차 개선해 나갈 수 있다.

우선 출입통제, 시설보안 등 물리적 보안을 통해 최소한의 보안영역을 구성해야 한다. 보안에 대한 기본 틀이 세워지지 않으면 보안은 무너지게 되어있다. 기업 내에 물리적 보안이 기본적으로 구성되었다면 관리적 보안을 통해 내부 산업정보보안 프로세스를 확립해야 한다. 정보보호 조직체계를 구성하고 임직원들에게 역할을 할당해서 책임감을 느끼도록 해야 하며 ISMS, ISO27001 등 보안인증심사를 통해 통제항목을 기반으로 산업보안정책을 운영해야 한다. 보안기술이 발달한 현대시대에는 외부의 공격보단 내부 산업 스파이 및 내부 유출 사고

건수가 많다. 주기적인 산업정보보안 교육을 통한 임직원들의 보안의식을 향상시켜야 하며 산업기밀정보 유출 대상인 퇴직 대상자를 철저하게 모니터링 해야 한다. 내부 정보보안 프로세스가 갖춰졌다면 기업의 환경에 맞게 기술적 보안을 통해 네트워크 및 엔드포인트 영역에 대한 보안을 강화하고 임직원들을 모니터링하면서 데이터 유출에 대한 검증이 필요하며 포렌식을 통해 어떤 경로로 산업기밀정보가 유출되었는지 분석을 진행하고 대응방안을 마련해야 한다.

다양한 산업이 발전하면서 중소기업이 증가하고 있으며 기업마다 고유한 지식재산권이 매출의 핵심으로 자리 잡고 있다. 다른 측면으로 보면 기업의 존속 여부를 결정짓는 산업정보가 경쟁사에 유출되고 있다. 중소기업의 산업정보보안은 단기간에 큰 비용을 투자해서 프로세스를 확립할 수 없다. 장기간 지속적인 투자를 통해 보안 프로세스를 설계해야 할 필요성이 있다.

제 2 절 연구의 한계점 및 향후 발전방향

본 연구는 중소기업 산업정보 유출의 심각성을 알리고 지속해서 산업정보보안 프로세스를 확립하고자 연구를 진행하였다. 총 다섯 곳의 중소기업 제조사와 서비스사를 선정하여 현업에서 2년 동안 수집한 데이터를 기준으로 실증분석을 진행하였다. 산업정보 유출로 의심되는 항목을 기준으로 산업정보 반출 건수에 비례해서 유출의심 건수가 얼마만큼 발생했는지 분석하였으며, 어떤 영역을 통해 산업정보가 반출, 유출되었는지 실증분석을 진행하였다. 또한, 산업정보보안을 물리적 보안영역, 관리적 보안영역, 기술적 보안영역으로 구분하여 어떤 항목들을 점검하고 관리해야 하는지 제시하였다.

본 연구의 한계점으로는 수집한 데이터를 통해 통계치를 산정하는 과정에서 실제 유출의심 건인지에 대한 기준이 다소 부족하였다. 기준을 정하고 산업정보 반출 건과 유출의심 건을 정의했지만 오 탐지로 인한 실제 유출 건이 아님에도 불구하고 유출의심 건으로 판단한 데이터도 존재하였다. 수집된 모든 데이터를 확인하는 것은 한계였으며 유출의심 기준으로 정의한 조건에 따라 리포트를 구성해서 데이터를 취합했기 때문에 데이터 정합성에 대해 부족한 부분이 존재하였다. 실증분석 대상인 중소기업에서 근무하는 정보보안담당자와 협업을 통해

실제 산업정보 유출 건에 대한 데이터 검증이 필요했지만, 외부에 공개하기에는 내부적으로 민감한 대외비 산업정보도 많았으며, 모든 산업정보 유출의심 건에 대한 데이터 분석을 협업해서 진행하기에는 현실적으로 한계가 있었다. 일부 산업정보 유출의심 건은 정보보호담당자와 협업을 통해 분석을 진행하였고 실제 유출 데이터로 확인되었지만, 현업의 필요로 인해 분석을 진행하였기에 상시 분석을 진행하는 것은 한계점이었다. 또한, 산업보안 관리체계 평가지표 데이터의 경우, 설문 방식으로 진행되다 보니 정보보호담당자의 주관적인 의견이 반영되었으므로 신뢰성이 부족한 부분도 있었다.

본 연구에 대한 향후 발전방향으로는 다양한 산업 분야에 대한 데이터 수집 및 실증분석이 필요하며, 좀 더 명확한 기준을 가지고 산업정보 유출 판단을 정의해야 할 필요성이 있다. 또한, 중소기업 정보보호담당자와의 협업을 통해 주기적으로 유출의심 데이터에 대한 검증이 필요하며 물리적 보안영역, 관리적 보안영역, 기술적 보안영역을 기준으로 중소기업 산업정보보안 프로세스를 체계적으로 구성하는 모델을 제시할 필요성이 있다.

참 고 문 헌

1. 국내문헌

김광민. (2019). “중소·중견기업의 산업기술 보호를 위한 산업보안 관리체계에 관한 연구”. 건국대학교 정보통신대학원 석사학위논문

강기원. (2015). “제조기업 기술보호를 위한 ISMS 모델 기반의 정보시스템 보안 통제 실행에 관한 연구”. 연세대학교 공학대학원 석사학위논문

강푸름. (2013). “중소기업 기술유출 방지를 위한 핵심인력 관리 방안에 관한 연구”. 경기대학교 대학원 석사학위논문

고기철. (2015). “산업기술의 내부 유출방지 성과에 영향을 미치는 요인에 관한 연구”. 숭실대학교 대학원 박사학위논문

국가지식재산위원회. (2016).『중소기업 기술보호 역량강화 대응방안』

국회산업통상자원중소벤처기업위원회. (2020).『산업통상자원중소벤처기업위원회 정책현안 자료집』

김기권. (2009). “산업스파이의 대응 실태 및 대책에 관한 연구”. 동국대학교 행정대학원 석사학위논문

김윤성. (2015). “산업보안의 국내 입법 수요에 대한 연구: 선진사례 비교 및 적용모델 연구를 중심으로”. 국민대학교 법무대학원 석사학위논문

김중배. (2009). “산업기술 유출 대응방안에 관한 연구”. 성균관대학교 국가전략대학원 석사학위논문

김태균. (2014). “중소기업을_위한_산업기밀_보호체계_구축방안에_관한_연구”. 서울과학종합대학원대학교 석사학위논문

김태준. (2020). “정보보호 관리체계를 활용한 스마트팩토리 보안 관리 지표에 관한 연구”. 건국대학교 정보통신대학원 석사학위논문

김태형. (2019). “중소기업 산업기술유출방지 강화방안에 대한 연구”. 동국대학교 대학원 석사학위논문

김화영. (2011). “산업기술 유출방지 및 보호방안에 관한 연구: 산업보안 인력수

급과 직업도출을 중심으로". 고려대학교 정책대학원 석사학위논문
김화영. (2019). "산업보안 전문자격 활성화 방안 연구". 중앙대학교 대학원 박사학위논문
박낙규. (2014). "산업보안관리체계 인증 수립 방안 연구". 한국산업기술대학교 산업기술경영대학원 석사학위논문
박찬수. (2016). "산업기술유출범죄의 실태분석 및 대응방안". 용인대학교 일반대학원 석사학위논문
산업통상자원부. (2015).『제2차 산업기술의 유출방지 및 보호에 관한 종합계획』
산업통상자원부. 한국산업기술보호협회. (2017).『산업기술보호지침 및 매뉴얼』
송기현. (2011). "기업 내부 보안을 위한 정보보호 관리 연구". 성균관대학교 정보통신대학원 석사학위논문
신현구. (2015). "산업보안정책 준수의지의 영향요인에 관한 연구". 경기대학교 박사학위논문
양현정. (2018). "산업기술유출 범죄의 사례분석: 국내 포털 사이트 뉴스를 중심으로". 중앙대학교 대학원 석사학위논문
연희모. (2013). "내부자에 의한 산업기밀 유출방지 방안". 성균관대학교 국가전략대학원 석사학위논문
윤인수. (2007). "내부자에 의한 정보유출 방지를 위한 보안시스템 구축에 관한 연구". 강원대학교 산업대학원 석사학위논문
이경환. (2016). "산업기밀 유출 관련 법률의 문제점과 개선방안". 동국대학교 석사학위논문
이근주. (2014). "산업기술 유출 방지를 위한 보안 감사 시스템 개발". 남서울대학교 대학원 석사학위논문
이민혁. (2016). "주요국 산업보안체계 비교 및 발전방향 탐색". 상명대학교 대학원 석사학위논문
이성규. (2015). "산업보안정책 준수의지 결정요인 연구". 서울벤처대학원대학교 박사학위논문
이송미. (2018). "중소제조업 보안 강화를 위한 SECaaS 활용 방안 연구". 중앙대학교 대학원 석사학위논문

이순옥. (2019). 기업의 산업기밀 유출 방지를 위한 실효적 방안에 대한 연구.『중앙대학교 학술지』

이은섭. (2020). “정보시스템 구축·운영을 위한 외주용역기반 보안관리 강화에 관한 연구”. 한국산업기술대학교 지식기반기술·에너지대학원 박사학위논문

이정민. (2013). “산업기술 보호 및 유출 방지를 위한 내부통제 관리체계 설계 방안”. 고려대학교 정책대학원 석사학위논문

이태규. (2011). “산업정보유출 방지와 인적 보안관리”. 성균관대학교 국가전략대학원 석사학위논문

임창묵. (2012). “산업보안 정책설계에 관한 연구”. 성균관대학교 박사학위논문

이호준. (2020). “중소기업 산업보안 수준 개선에 관한 연구”. 동아대학교 대학원 석사학위논문

전승준. (2014). “산업기술 보호를 위한 기업의 보안수준 강화 연구”. 한국산업기술대학교 산업기술경영대학원 석사학위논문

전인호, 모수종, 빈기철, 이춘근. (2000). 제조산업의 실시간 전산망 보안을 위한 시스템설계에 관한 연구.『한국멀티미디어학회 학술지』

정병수. (2007). “산업스파이의 실태분석 및 대응방안에 관한 연구”. 동국대학교 석사학위논문

정성배. (2015). “산업보안 관리활동이 기업의 보안성과와 업무효율성에 미치는 영향”. 용인대학교 박사학위논문

중소벤처기업부. (2020).『기술탈취 · 기술유출 피해사례와 대응전략』

최성욱. (2016). “국내 중소기업 산업보안 향상 방안에 대한 연구: 기술보호통합센터 설립과 산업보안 지원방안을 중심으로”. 홍익대학교 대학원 석사학위논문

최판암. (2012). “기업정보보활동이 산업기밀 유출방지에 미치는 영향”. 경기대학교 박사학위논문

한국인터넷진흥원. (2019).『정보보호 및 개인정보보호 관리체계 인증제도 안내서』

한명수. (2010). “산업기밀 유출 방지에 대한 법적 고찰”. 충북대학교 석사학위

논문
한석호. (2019). “스마트 팩토리 보안관리 항목 연구”. 중앙대학교 대학원 석사 학위논문
허재영. (2009). “중소기업의 산업보안을 위한 실증적 연구”. 한양대학교 대학원 석사학위논문
현용태. (2017). “산업기술유출 사례분석을 통한 중소벤처기업 산업기술유출 방지시스템의 효율적 관리방안”. 건국대학교 대학원 석사학위논문
황현동. (2017). “산업기술유출의 원인 분석: 자기통제력과 조직몰입도를 중심으로”. 중앙대학교 대학원 석사학위논문
SKINFOSEC. (2019).『보안SI를 통한 IT정보보호 구축 가이드』

2. 국외문헌

Baum, F., & Bulthuis, W. (2014). *Managing security, safety and privacy in Smart Factories.* Smart Factory Innovation Forum
NIST, S. (2015). 800-82 Rev 2. Guide on industrial control systems security
Daniel J. Morris, Lawrence P. Ettkin, Mariyn M. (2000). *Issues in the illegal transference of US information technologies,* Information Management & Computer Security

ABSTRACT

An Empirical Analysis of Industrial Information Leakage Accidents in Small and Medium-sized Enterprises

Koh, Chan-Suk

Major in Smart Convergence Security Consulting

Dept. of Smart Convergence Consulting

Graduate School of Knowledge Service Consulting

Hansung University

With the advent of the fourth industrial revolution, the scope of information leakage routes and information leakage information is expanding due to the advancement of information society such as IoT and cloud due to the development of technologies in various industrial sectors, and each company's unique technology and intellectual property rights are becoming important. With the growing perception that technological competitiveness is national competitiveness, it is focusing on strengthening the protection of intellectual property in each country not only at home but also around the world, and is a significant part of the industrial economy. In fact, based on the technology that creates high value-added products such as semiconductors and display industries, Korea's industry has gained a

competitive advantage in the global market, which soon led to economic development. However, Korea is still considered to have a lower level of intellectual property protection compared to major countries, and the number of cases of leakage of industrial information such as corporate technical skills and trade secrets is increasing every year.

According to the survey statistics provided by the Ministry of Trade, Industry and Energy on the level of industrial information security capabilities, the information security system and important technical skills protection of domestic small and medium-sized enterprises were found to be the most vulnerable. Major problems include insufficient systematic management and protection of core technologies and important information, weak awareness and capacity of security, insufficient quick response to information leakage, and insufficient level of punishment for information leakage. In the case of large companies, the number of cases of industrial information leakage is decreasing by organizing and managing internal security infrastructure through continuous investment, but in the case of small and medium-sized companies, interest in industrial information security naturally decreases due to difficulties in constructing security infrastructure and investing security professionals due to budget problems, and thus the number of cases of industrial confidential information leakage is increasing every year. Taking a comprehensive look at this environment, it is necessary for thorough protection and management to be carried out to prevent the outflow of intellectual property rights of companies in order to ensure the continued growth of the nation's national and economic sectors.

This study was conducted on small and medium-sized enterprises with frequent industrial information and technology leakage incidents. It examined the cases of industrial information leakage accidents and presented an industrial information management system suitable for small and medium-sized enterprises, and conducted an empirical analysis of industrial

information leakage based on data collected between 2018 and 2019. Several cases of industrial information were taken out by industry, the number of suspected cases of leakage was shown, and the results of how the leak was attempted were derived. In addition, the evaluation index of the current status of industrial information security management by small and medium enterprises was specified in conjunction with the industrial security management system.

Based on the results of the study, the government intends to contribute to reducing industrial information leakage accidents by presenting industrial security guides by systematically organizing industrial information and key technical information of small and medium enterprises from the perspective of physical security areas, managed security areas, and technical security areas.

【Keyword】 Intellectual property rights, Industrial information security, Industrial information, Physical security area, Technical security area, Administrative security area, Small and medium business, Empirical analysis, Leakage