2022년

영업비밀 보호 가이드 연구

국내 판례 분석 및
비대면 근무환경을 중심으로

2022. 12. 2.

특허청
Korean Intellectual Property Office

K-ip care
한국지식재산보호원
Korea Intellectual property Protection Agency

영업비밀보호센터
Trade SEcret Protection center

제 출 문

한국지식재산보호원장 귀하

본 보고서를 “영업비밀 보호 가이드” 발간 연구과제의 보고서로 제출합니다.

2022년 12월 2일

| 주관연구기관명 | 법률사무소 데이터로

| 연 구 기 간 | 2022. 10. 21. ~ 2022. 12. 2.

| 주관연구책임자 | 정관영(법률사무소 데이터로 대표변호사)

| 참 여 연 구 원 | 김성용(법률사무소 데이터로 전문위원)

남연식(법률사무소 데이터로 독일변호사)

최희정(법무법인 별 구성원변호사)

정민경(법무법인 별 송무팀 직원)

목 차

표 목차

그림 목차

Ⅰ. 서 론

1. 연구 추진목표
2. 연구 추진범위 및 내용

Ⅰ. 서 론

1. 연구 추진목표

가. 국내 판결조사·분석을 통한 데이터베이스

부정경쟁방지 및 영업비밀보호에 관한 법률(이하 '부정경쟁방지법') 개정으로 영업비밀 인정요건이 완화된 후 최근 5년간(선고일 기준 2017년 1월 1일부터 2021년 12월 31일까지 영업비밀 관련 민·형사 판결 약 1,980 여건) 전국 각급 법원에서의 영업비밀 관련 판결을 전수 조사하고, 이에 대한 정량적·정성적 분석을 통해 영업비밀 관련 주요 쟁점별(ex, 비밀관리 충족을 위한 판단 요소 등 영업비밀 성립요건, 침해행위, 민사구제, 형사구제 등) 색인화를 하여 최신 판결 데이터를 구축한다.

나. 비대면 근무환경을 포함한 포괄적 영업비밀 보호 가이드

최신 판결에 대한 주요 쟁점별 데이터베이스화 작업으로 마련된 자료를 기초로 영업비밀 보호 표준서식을 구축하고, 원격근무 등 디지털기반 근무환경에서 사용자·피용자가 준수해야 할 주의사항 및 조치를 도식화하여 원격근무 등 변화된 환경에 맞는 이른바 포괄적 영업비밀 보호 표준서식과 규정을 마련한다. 이는 지적재산을 보호하고 비즈니스 관행의 적절성을 유지하기 위해 사용할 수 있는 보호조치의 초석을 마련하기 위함이다.

다. 해외사례 조사를 통한 최신 동향

최근 미국 펜실베니아 동부지방법원(U.S. District Court for the Eastern District of Pennsylvania)의 판결로 원격근무 시 기업의 영업비밀 침해에 대한 문제점을 확인할 수 있었다. 법원 판결과 해외 학술지 등 기타 자료를 참고하여 원격근무 등 비대면 근무환경에서 해외 각국은 영업비밀 보호를 위해 어떠한 관리조치를 하고 있는지 영업비밀 유출(해외)사례를 조사하여 최신 동향을 파악한다.

2. 연구 추진범위 및 내용

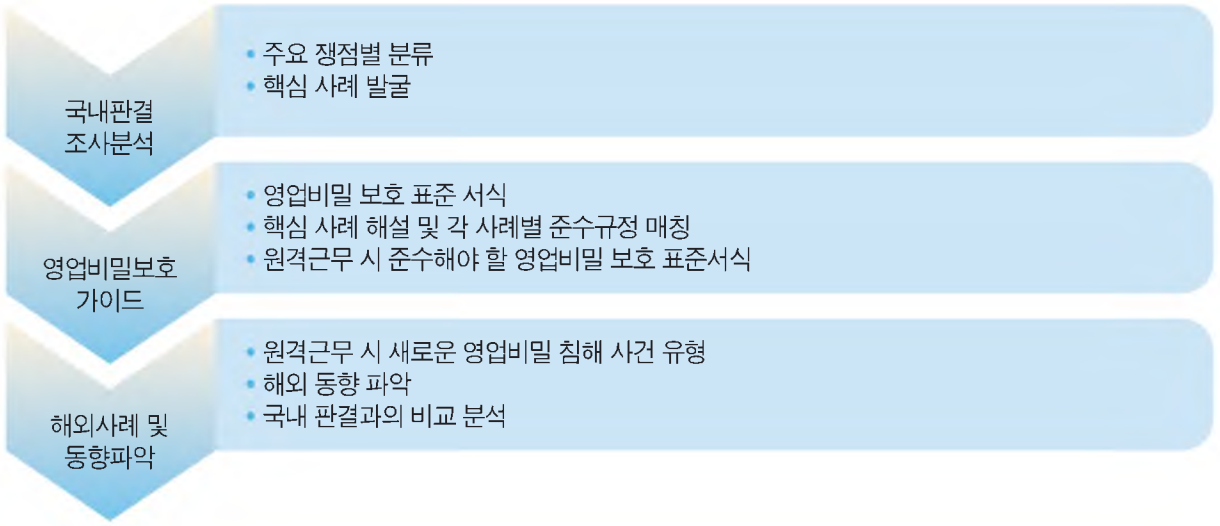
가. 연구 추진범위

2017년 1월 1일부터 2021년 12월 31일까지 최근 5년간 전국 각급 법원의 영업비밀 관련 판결 전체(민·형사 1,980여 건의 판결문 및 결정문) 분석.

표 1. 분석대상 기준

분석대상	기간	선고일 기준 2017년 1월 1일 ~ 2021년 12월 31일
	심급	1심, 2심, 3심 전체
	확정	확정 여부에 관계없이 해당 기간 선고 사건 전체
	민사	본안(영업비밀 침해행위 금지, 손해배상 등) 및 가처분
	형사	부정경쟁방지 및 영업비밀보호에 관한 법률 위반 사건

그림 1. 연구 추진범위 개요



나. 연구 추진내용

- 현행 부정경쟁방지법은 제2조 제2호에서 영업비밀에 대한 정의 규정을, 제2조 제3호에서는 "영업비밀 침해행위 6가지(가.목 내지 바.목)를 유형화하고 있다.
- 민사상 조치로는 영업비밀 침해행위의 금지 및 예방, 부대 청구(물건의 폐기 등), 손해배상, 신용회복 청구를 규정하고 있다.
- 형사상 제재로는 동법 제18조(벌칙)에서 규정하고 있으며, 특히 국내외를 구분하여 영업비밀 침해 행위에 대한 형량을 달리하고 있다. 아울러 미수 및 예비·음모에 관한 처벌 규정도 두고 있다.
- 본 연구는 위와 같은 현행 법률규정을 반영하여, 이하와 같은 기준으로 판결을 분석한다.

1) 영업비밀 침해행위 관련 국내 판결 분류 및 색인화 작업

가) 1차 분류- 부정경쟁방지법 제2조 제2호의 '영업비밀'에 해당하는지 최초 분류

표 2. 부정경쟁방지법 제2조 제2호에 따른 분류

영업비밀	성립요건(특히 비밀관리성 판단 기준), 민사구제, 형사제재, 침해행위 유형

나) 2차 분류- 민사와 형사사건으로 분류

표 3. 민사와 형사 분류

민사사건	보전처분(가처분 등) / 본안(금지, 제거, 예방, 손해배상)
형사사건	부정경쟁방지법 제18조 제1·2항, 제19조 / 형법 업무상배임

다) 3차 분류- 세부 핵심어 태그별 분류

영업비밀 사건은 성립요건, 침해행위, 민사구제, 형사제재별 세부 핵심어 태그별로 분류한다(아래 표 참조).

표 4. 세부 핵심 태그별 분류

영업비밀	성립요건	비공지성, 경제적 유용성, 비밀관리성
	비밀관리성	비밀관리성 판단 요소, 판단 요소별 검토
	침해행위	침해행위의 주체, 부정취득, 부정사용
	민사구제	금지대상, 금지기간, 폐기청구, 경업금지, 손해배상
	형사제재	공소사실 특정, 실행의 착수·기수, 업무상배임

2) 주요 사항에 대한 사례 분석 작업

부정경쟁방지법상 영업비밀 관련 판례 중 1·2심에서 '비밀관리성' 판단이 뒤바뀐 사례, 비밀관리성 판단 기준 완화 여부, 비밀관리성 판단 요소에 대한 비교·분석, 기술탈취 관련 판례 중 영업비밀과 타법(형법, 산업기술보호법 등)과의 관계 등 분석.

3) 핵심 요소별 보호 사례

영업비밀 침해관련 각 판결문에 대해 침해행위 유형·주요쟁점 등 세부 기준에 의한 집행통계를 산출하는 것을 기본 방향으로 하여 영업비밀 침해행위 관련 판결을 기초로 영업비밀 보호 가이드 마련.

- 영업비밀 - 영업비밀 판결문을 민사 판결문 5가지(청구취지, 손해배상액 등), 형사판결문 5가지(죄목, 형량 등) 유형으로 분류하여 분석 진행(아래 표 참조).

표 5. 영업비밀 성립요건에 따른 민사/형사 사건의 주요쟁점 등 분류

구분		주요내용
민사	청구취지	손해배상, 전직금지, 침해금지, 침해예방, 폐기 등
	주요쟁점	비공지성, 경제적 유용성, 비밀관리성, 전직금지 등
	사건결과	인용, 일부인용, 기각, 각하
	유형별 결과	손해배상, 영업비밀 침해금지 등, 가처분
	손해배상액	손해배상 청구액·인용액 최고값, 중앙값, 평균 등
형사	주요쟁점	비공지성, 경제적 유용성, 비밀관리성, 업무상 배임 등
	사건결과	유죄, 무죄, 선고유예 등
	죄목분류	영업비밀 취득, 사용, 제3자 누설
	무죄사유	비공지성, 경제적 유용성, 비밀관리성 등
	형량	기간별 형량

4) 포괄적 영업비밀 보호 관리 가이드라인

기업이 도입하여야 할 영업비밀 보호조치를 유형화하여 각 유형별 사례를 소개하고 이에 대한 해설을 적시하여 비대면 환경을 전제로 한 포괄적 영업비밀 보호 가이드를 마련한다.

- 최종 선정된 주요 판결문에 대한 요약문을 지정된 양식과 항목에 맞추어 작성하되 주요 판결 선정은 아래의 기준으로 한다.

기업이 도입하여야 할 영업비밀 보호조치에 부합하되 '비밀관리성'이 쟁점이 된 사안을 우선 추려 그 중에서 각 심급에서 판단이 달라진 사건, 영업비밀과 타법(형법, 산업기술보호법 등)과의 관계로 유의미한 결과를 도출시킬 수 있는 사건을 우선 선정한다. 아울러 비밀관리성 인정요건 완화로의 법 개정을 반영할 수 있는 사례와 원격근무 확대로 도입이 시급한 영업비밀 관리방안 관련 사례도 우선순위로 선정한다.

5) 원격근무에 따른 규정 정비 및 서식 마련

영업비밀이 기업마다 고유한 것으로 인정되듯이 이러한 비밀을 보호하기 위한 정책 역시 일관성 있게 진행되어야 한다. 따라서 COVID-19 이전의 근무조건에서의 영업비밀 보호 가이드와 융합될 수 있는 원격근무 등의 상황을 가정한 영업비밀 보호 가이드를 새롭게 마련함으로써 이른바 포괄적 영업비밀 보호 가이드라인에 부합하는 영업비밀 보호 규정, 영업비밀 보호 관련 각종 서식(원격근무 신청서, 원격근무 관리대장 등)을 마련한다.

Ⅱ. 영업비밀 판결 분석

1. 분석의 목적
2. 판결 분석 개요 및 현황
3. 영업비밀 침해 민사 판결 분석
4. 영업비밀 침해 형사 판결 분석
5. 의의 및 한계

Ⅲ. 영업비밀 판결 분석

1. 분석의 목적

본 연구는 2017년 1월 1일부터 2021년 12월 31일까지 5년 간 「부정경쟁방지 및 영업비밀보호에 관한 법률」 관련하여 영업비밀 분야에서 선고된 민·형사 판결문(가처분 결정문 포함. 이하 같음) 1,980여 건을 분석 대상으로 삼아 영업비밀 성립요건, 비밀관리성 인정 요소, 침해의 대상이 된 정보의 유형, 손해배상액 판단 근거 등 주요 쟁점별로 분류하고, 이러한 분류에 따라 데이터를 체계적으로 구축하는 것을 주요 내용으로 한다.

판결문 전수 분석을 통해 부정경쟁방지법 제2조 제2호에서 정의하고 있는 영업비밀로 인정되기 위한 3요소(비밀관리성, 비공지성, 경제적 유용성)와 각 요소별 판단기준, 법원의 비밀관리성 판단 요소, 판단 요소별 빈도와 상관관계, 분쟁 대상 정보 유형에 따른 사건 결과, 영업비밀 침해유형에 따른 민·형사적 책임 등 법원의 전체적인 판결 동향과 흐름을 파악하고자 하였다.

표 6. 영업비밀 판결 분석 기준 대분류

구 분		주 요 내 용
민 사	청구취지	침해금지·예방, 폐기·제거, 손해배상, 전직금지 등
	영업비밀 요건	비밀관리성, 비공지성, 경제적 유용성
	침해유형	가. 제3자에 의한 부정취득행위 나. 부정취득자로부터의 악의취득행위 다. 부정취득행위자의 사후적 관여행위 라. 비밀유지의무자에 의한 부정공개행위 마. 부정공개자로부터의 악의취득행위 바. 부정공개행위에 관한 사후적 관여행위
	손해배상	금액별, 손해액 산정 방법, 인용률
	사건결과	인용, 기각, 각하
형 사	영업비밀 요건	비밀관리성, 비공지성, 경제적 유용성
	사건결과	유죄, 무죄, 집행유예 등
	죄목	영업비밀 국외유출 영업비밀 국내유출 법인 양벌규정 업무상 배임
	무죄사유	비공지성, 경제적 유용성, 비밀관리성 등
	형량	자유형, 벌금 / 실형, 집행유예

판결문 전수 분석의 궁극적인 목적은 기업의 사용자와 피용자가 영업비밀 보호를 위해 지켜야 할 핵심 요소를 추출하고 그에 따른 관리 방안을 제시하고자 함에 있다.

한편 영업비밀로 인정받기 위한 요건 중 하나인 '비밀관리성' 요건과 관련하여 부정경쟁방지법 제2조 제2호는 "'합리적인 노력'에 의하여 비밀로 유지"되어야 할 것을 요구하였으나, 2019. 1. 8. 법률 제16204호로 개정된 부정경쟁방지법은 단순히 "비밀로 관리"하기만 하면 되는 것으로 변경하였다. 또한 위 개정 법률은 영업비밀 침해행위에 대한 벌칙 조항(제18조)을 개정하여 통해 법정형을 상당히 강화하였다. 이는 조직력이나 자금력 면에서 상대적으로 취약한 중소기업이 자사의 영업비밀을 충분히 보호받지 못하는 사례가 많아 이에 대응하기 위한 입법이다. 본 연구를 통해 위 개정법 조항에 따라 변경된 판단 기준을 적용하여 판시한 사례가 있는지 찾아보았다.

2. 판결 분석 개요 및 현황

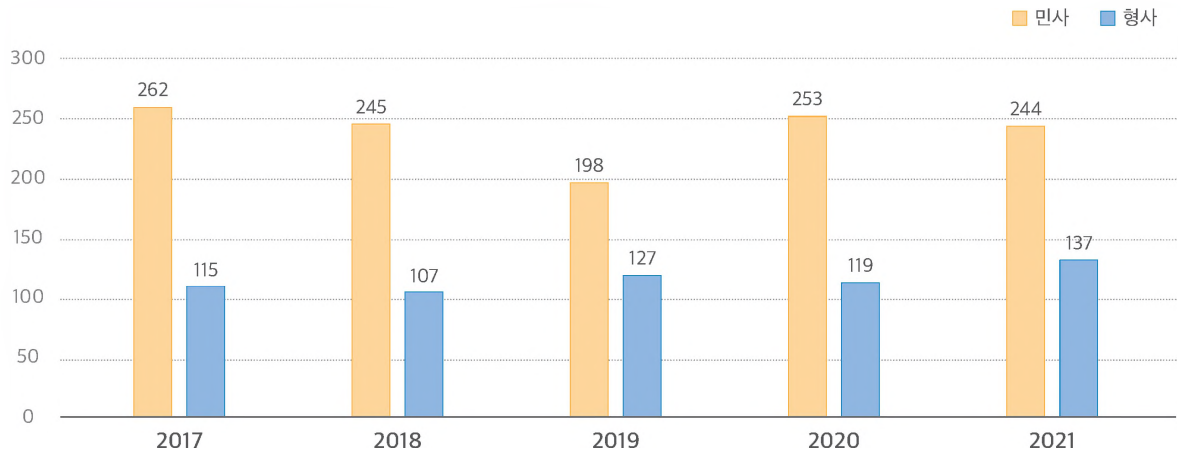
가. 분석대상 판결

분석 대상은 선고일 기준 2017년 1월 1일부터 2021년 12월 31일 까지 전국 각급 법원에서 선고된 판결문과 결정문이다. 수집된 판결·결정문 중에서 무관 판결을 제외한 영업비밀 관련 판결은 총 1,807건으로 파악되었다.

수집한 판결문을 연도별로 구분하면 아래 표와 같다.

표 7. 영업비밀 관련 판결 총 집계

선고년도	2017	2018	2019	2020	2021	합계
민사	262	245	198	253	244	1202
형사	115	107	127	119	137	605

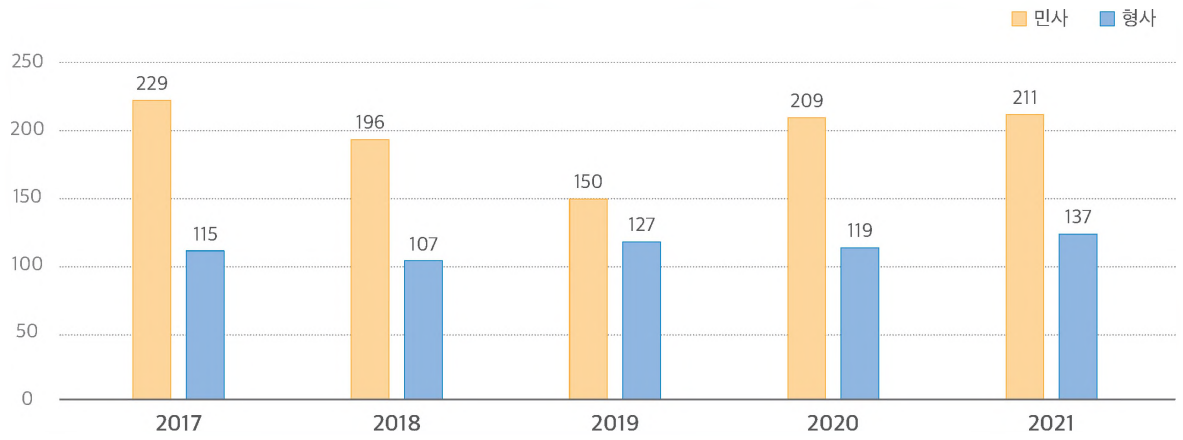


영업비밀 관련 판결은 민·형사 합하여 총 1,807건이었고, 이 중 민사사건은 1,202건, 형사사건은 605건이었다. 전체 판결 중 민사사건이 66.52%, 형사사건이 33.48%를 차지하였다.

한편, 민사에서 영업비밀 관련 판결 중 오직 전직금지·경업금지만을 쟁점으로 한 사건이 207건이었는바 이 사건들을 제외하고 부정경쟁방지법상 영업비밀 침해 판결만을 집계하면 아래 표와 같다.

표 8. 부정경쟁방지법상 영업비밀 침해 판결 집계

선고년도	2017	2018	2019	2020	2021	합계
민사	229	196	150	209	211	995
형사	115	107	127	119	137	605

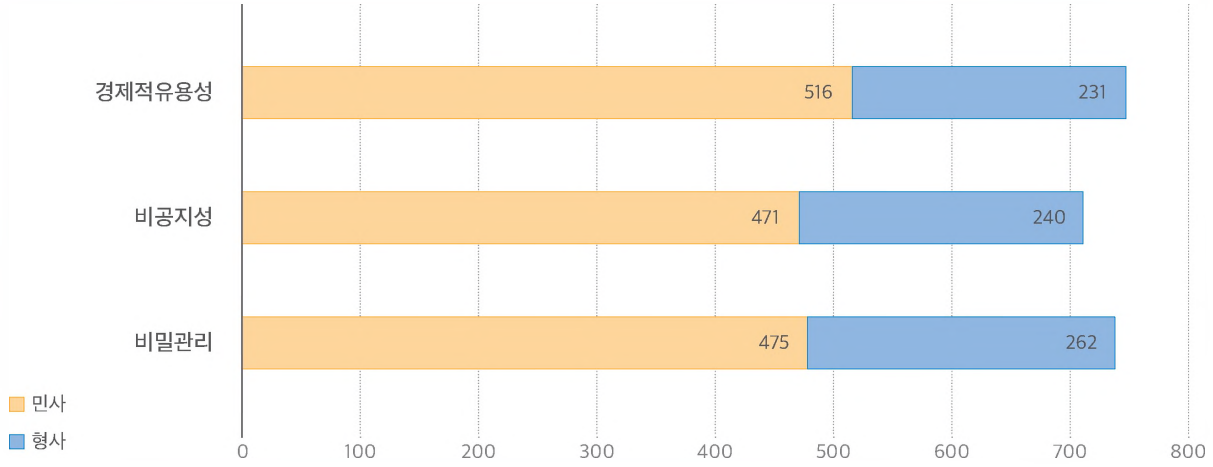


나. 영업비밀 성립요건별 현황

부정경쟁방지법상 영업비밀로 보호받기 위해서는 해당 정보가 공공연히 알려지지 아니하여야 하고(비공지성), 영업활동에 유용한 기술상 혹은 경영상의 독립된 경제적 가치를 가져야 하며(경제적 유용성), 영업비밀 보유자가 비밀로 관리한 것이어야만 한다(비밀관리성). 이러한 성립요건에 따라 판결문을 분류한 결과는 아래 표와 같다.

표 9. 주요 쟁점별(영업비밀 성립요건별) 총 집계

구분	비밀관리	비공지성	경제적 유용성
민사	475	471	516
형사	262	240	231
비율	40.79%	39.51%	41.33%

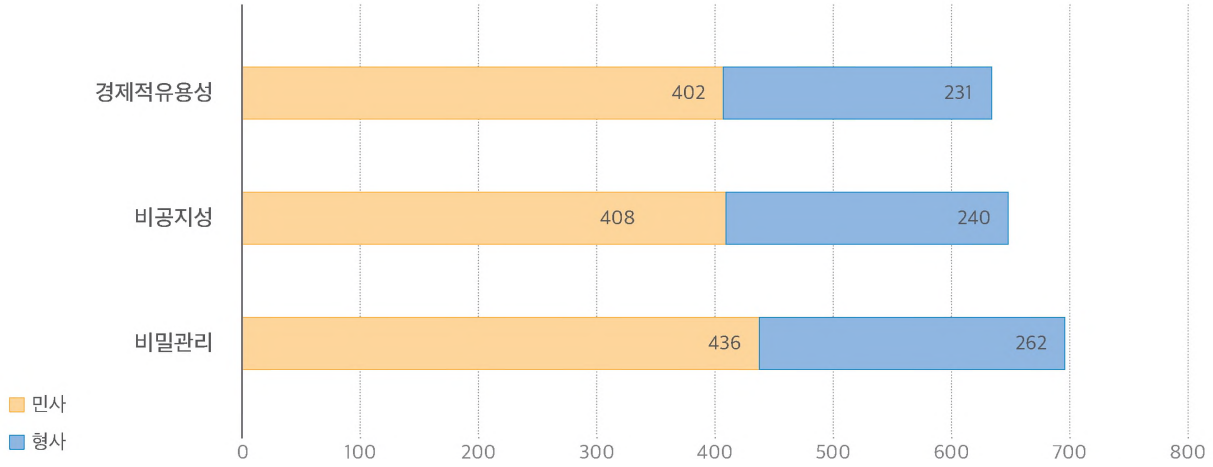


분석결과 민·형사 사건을 통틀어 "경제적 유용성" 쟁점이 41.33%로 가장 비율이 높았고, 다음으로 "비밀관리성" 40.79%, "비공지성" 39.51% 순으로 나타났다. 경제적 유용성 쟁점이 가장 많이 나타난 이유를 살펴본 결과, 민사 경업금지·전직금지 사건에서 경제적 유용성(보호할 가치 있는 이익)이 자주 언급되었기 때문으로 파악되었다.

이에 민사 경업금지·전직금지를 제외하고 오로지 부정경쟁방지법상 영업비밀 침해 사건에서의 쟁점 비율을 집계한 결과, 민·형사 사건에서 공히 가장 주요하게 다루어진 쟁점은 "비밀관리성"으로 나타났다.

표 10. 주요 쟁점별(영업비밀 성립요건별) 총 집계 : 경업금지·전직금지 제외

구분	비밀관리	비공지성	경제적 유용성
민사	436	408	402
형사	262	240	231
비율	43.62%	40.50%	39.56%



민·형사 사건을 통틀어 영업비밀 보유자가 어느 정도 노력을 기울여 영업비밀로 관리하였는지 여부를 판단하는 "비밀관리성"쟁점이 43.62%로 가장 비율이 높았고, "비공지성" 40.5%, "경제적 유용성" 39.56%로 나타나 영업비밀 3요소 모두 쟁점으로 폭넓게 다루어지고 있는 것으로 파악되었다.

다. 침해행위 주체 및 유형별 쟁점 현황

민사사건의 침해 유형·주체

부정경쟁방지법 제2조 제3호는 영업비밀 침해행위를 가. 제3자에 의한 부정취득행위, 나. 제3자로부터의 악의취득행위, 다. 부정취득행위에 관한 사후적 관여행위, 라. 비밀유지의무위반자의 부정공개행위, 마. 부정공개자로부터의 악의취득행위, 바. 부정공개행위에 관한 사후적 공개행위로 분류하고 있다. 각 목의 의미는 아래와 같다.

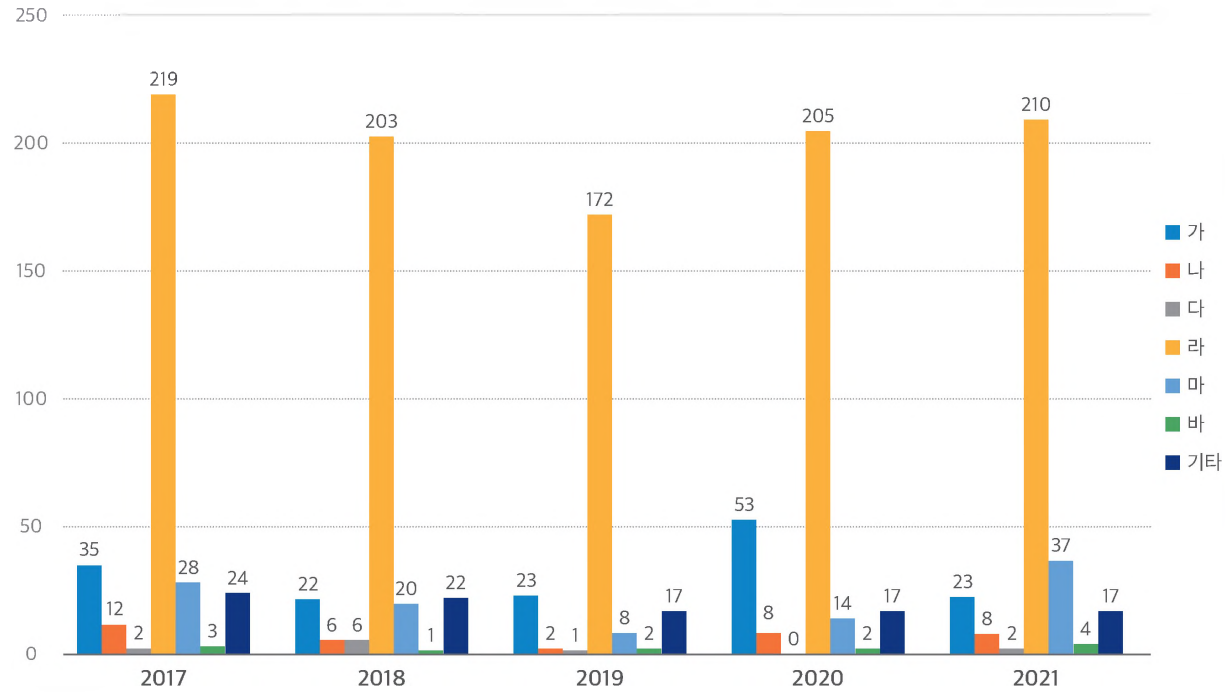
- 가목 제3자의 부정취득행위 등 : 절취, 기망, 협박 그 박의 부정한 수단으로 영업비밀을 취득하거나 취득한 영업비밀을 사용하거나 공개하는 행위
- 나목 부정취득자로부터의 악의취득행위 : 영업비밀에 대하여 부정취득행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 취득하는 행위 또는 그 취득한 영업비밀을 사용하거나 공개하는 행위
- 다목 부정취득행위에 관한 사후적 관여행위 : 영업비밀을 취득한 후에 그 영업비밀에 대하여 부정취득행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 사용하거나 공개하는 행위
- 라목 비밀유지의무자의 부정공개행위 : 계약관계 등에 따라 영업비밀을 비밀로서 유지하여야 할 의무가 있는 자가 부정한 이익을 얻거나 그 영업비밀의 보유자에게 손해를 입힐 목적으로 그 영업비밀을 사용하거나 공개하는 행위
- 마목 부정공개자로부터의 악의취득행위 : 영업비밀이 라목에 따라 공개된 사실 또는 그러한 공개행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 취득하는 행위 또는 그 취득한 영업비밀을 사용하거나 공개하는 행위를 말한다.
- 바목 부정공개행위에 관한 사후적 관여행위 : 영업비밀을 취득한 후에 그 영업비밀이 라목에 따라 공개된 사실 또는 그러한 공개행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 사용하거나 공개하는 행위

조사기간 동안 입수한 영업비밀 침해행위 관련 민사 판결을 위 침해행위유형별로 분석한 결과는 아래 표와 같다.

표 11. 침해행위 유형별 민사 판결 쟁점(연도별)

연도 / 침해유형	2017	2018	2019	2020	2021	합계[1]
가	35	22	23	53	23	156
나	12	6	2	8	8	36
다	2	6	1	-	2	11
라	219	203	172	205	210	1,009
마	28	20	8	14	37	107
바	3	1	2	2	4	12
기타[2]	24	22	17	17	17	97
합계	323	280	225	299	301	1,428

민사사건에서는 비밀유지의무 위반자의 부정공개행위인 "라"목이 70.66%(1,009/1,428), 부정취득행위인 "가"목이 10.92%(156/1.428)를 차지하여 비밀유지의무위반자의 부정공개행위인 "라"목이 가장 높은 비율을 차지하는 것으로 분석되었다.

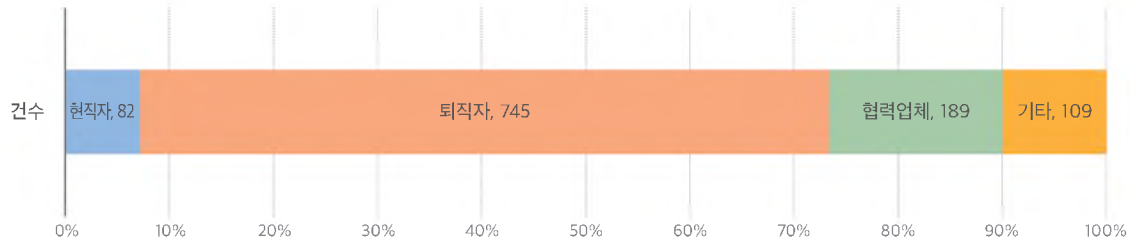


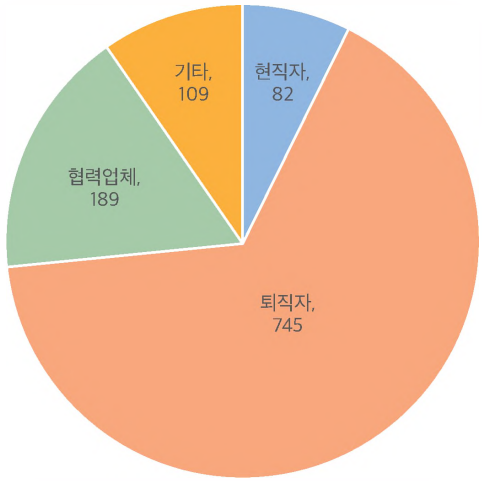
1) 동일 사건이라도 쟁점 유형이 여럿인 경우 개별적으로 행위 유형 적용해서 중복데이터 발생.
2) 유형을 알 수 없거나 불분명한 경우

이해를 돕기 위해 영업비밀 침해행위 민사사건에서 침해행위 주체별로 분석한 결과는 아래와 같다.

표 12. 침해행위 주체별 민사 판결

침해주체	현직자	퇴직자	협력업체	기타	합계
건수	82	745	189	109	1,125
비율	7.29%	66.22%	16.8%	9.69%	100%





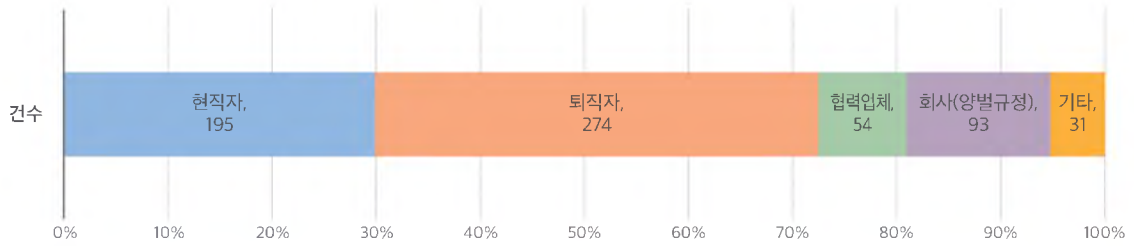
조사 결과 영업비밀 침해행위 민사사건의 주체는 퇴직자가 66.22%(745/1,125) 이상으로 가장 많았고, 현직자보다는 협력업체 임직원이 그 다음으로 많았다. 이는 재직 중 영업비밀 침해행위를 하기 보다는 퇴직 전후로 영업비밀 침해행위를 계획하고 퇴직 후 회사를 설립하거나 경쟁업체에 취업하여 영업비밀을 누설하는 경우가 많기 때문인 것으로 추측된다.

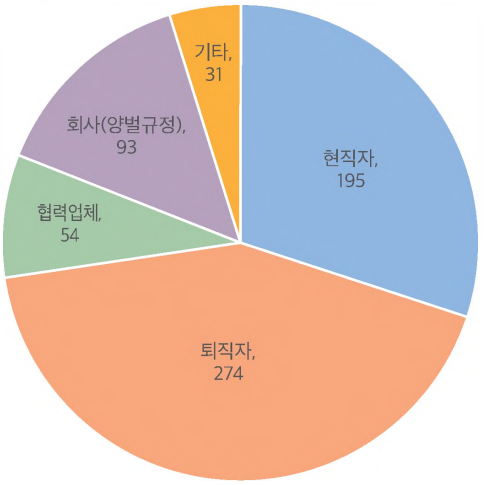
형사사건의 침해 유형·주체

영업비밀침해 형사사건(업무상배임 포함)을 침해 주체별로 살펴본 현황은 아래 표와 같다.

표 13. 침해행위 주체별 형사 판결

침해행위주체	현직자	퇴직자	협력업체	회사(양벌규정)	기타	합계[3]
건수	195	274	54	93	31	647
비율	30.1%	42.3%	8.3%	14.4%	4.8%	100%





조사 결과 영업비밀 침해행위 형사사건의 주체는 퇴직자가 42.3%로 가장 많았고, 다음으로 현직자도 30.1%로 매우 많았다. 그리고 협력업체 임직원이 그 다음으로 많았다. 이는 재직 중 영업비밀 침해행위를 하기 보다는 퇴직 전후로 영업비밀 침해행위를 계획하고 퇴직 후 회사를 설립하거나 경쟁업체에 취업하여 영업비밀을 누설하는 경우가 많기 때문인 것으로 추측된다.

구체적으로 보면 영업비밀 침해행위자가 퇴직자인 경우가 현직자인 경우보다 더 많은 것으로 분석되었고, 퇴직자와 현직자를 합하면 72.4% 정도에 이르러 사실상 회사 내부사정을 잘 알고 있는 직원이 침해행위를 할 가능성이 매우 높다는 것을 알 수 있다. 기타는 동종업체 운영자가 가장 많았고, 그 외에는 경쟁업체 임직원, 경쟁사업 제안자 등이다.

한편 부정경쟁방지법 상 영업비밀 침해 사건에서는 법인 양벌규정이 존재하는바, 양벌규정에 의해 법인도 벌금형으로 처벌된 비율은 14.4%에 달하였다.

3) 현직자·퇴직자 등 주체가 다수이거나 피고인이 다수인 경우 개별적으로 산정하여 중복데이터 발생.

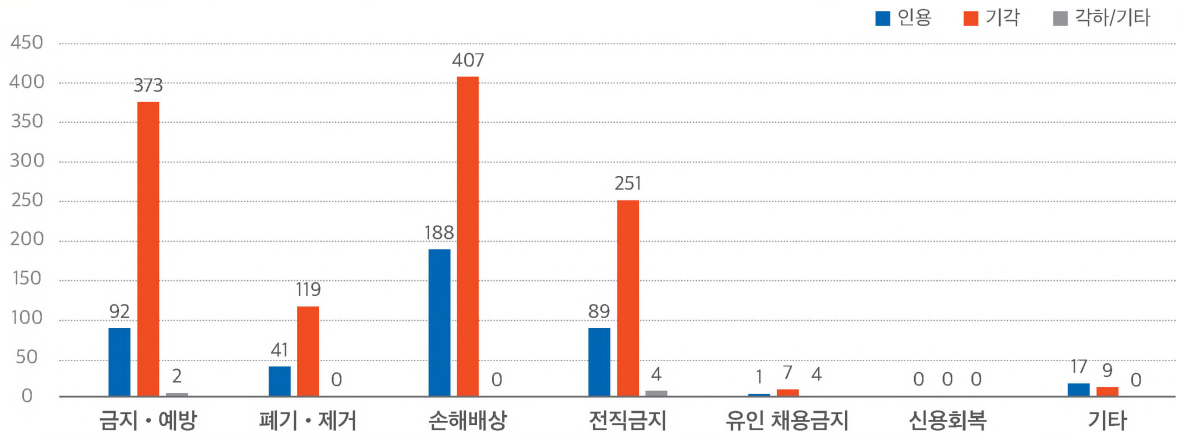
라. 민사 구제수단별 현황

영업비밀 침해행위로 인해 영업상의 이익이 침해되거나 침해될 우려가 있는 경우 피해자는 그 행위의 금지 또는 예방을 청구할 수 있고, 금지 또는 예방과 더불어 영업비밀 침해행위로 조성한 물건의 폐기나 영업비밀 침해행위에 제공된 설비의 제거, 그 밖의 영업비밀 침해행위의 금지 또는 예방을 위하여 필요한 조치를 청구할 수 있다. 또한 고의 또는 과실에 의한 영업비밀 침해행위로 영업비밀 보유자의 영업상의 신용이 실추된 경우, 피해자는 침해자를 상대로 영업상의 신용을 회복하는 데에 필요한 조치를 청구할 수도 있다.[4)]

위와 같은 구제수단 중 영업비밀 침해 피해자들이 어떤 구제수단을 선택하였고 그 결과는 어떠했는지 현황을 살펴본 바 그 결과는 아래 표와 같다.

표 14. 민사 구제수단별 판결 현황

구제수단	금지·예방	폐기·제거	손해배상	전직금지	유인 채용금지	신용회복	기타[5)]	합계[6)]
인용	92	41	188	89	1	-	17	428
기각	373	119	407	251	7	-	9	1,166
각하/기타	2	-	-	4[7)]	-	-	-	6
합계	467	160	595	344	8	-	26	1,600



구제수단 중 손해배상을 청구한 경우가 37.19%(595/1,600)로 가장 높은 비중을 차지하고, 영업비밀 침해행위의 금지·예방을 구하는 경우는 29.19%(467/1,600), 전직금지를 구하는 경우는 21.5%(344/1,600), 폐기·제거를 구한 경우는 10.0%(160/1,600), 유인채용금지를 구한 경우는 0.5%로 나타났고, 신용회복을 구한 경우는 이번 조사결과에서는 나타나지 않았다. 신용회복 청구는 사실상 사문화된 것으로 보인다.

4) 부정경쟁방지법 제10조 제1항, 제2항 및 제12조 참조.
5) 채권가압류, 전직금지가처분 상 간접강제금에 대한 집행분부여의 소 등.
6) 동일사건에서 당사자가 다수이거나 구제수단을 중복청구한 경우 개별적으로 분석하여 중복데이터 발생.
7) 이 중에서 원심의 전직금지 가처분 결정에 대하여 채무자들이 항고하였으나, 항고심 재판부는 채무자 중 일부에 대한 전직금지기간이 도과하여 보전의 필요성이 없다고 보아 각하 결정한 사례가 있었음(서울고등법원 2018라21359).

마. 형사 유죄 현황

부정경쟁방지법 제18조 제1항 및 제2항 유죄 판결 현황

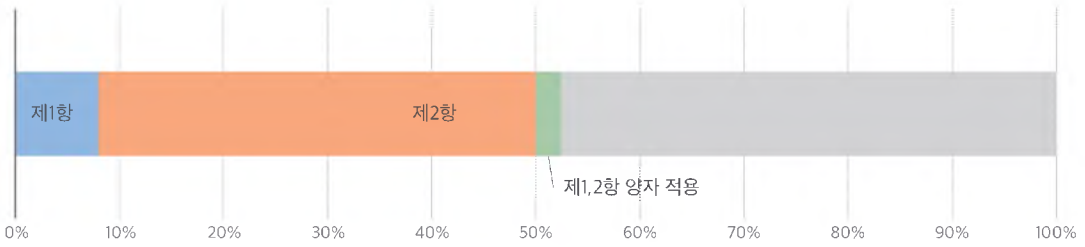
부정경쟁방지법상 영업비밀침해죄는 부정한 이익을 얻거나 영업비밀 보유자에 손해를 입힐 목적으로 ⅰ) 영업비밀을 취득·사용 또는 제3자에게 누설하거나(제18조 제1항 제1호 가목), ⅱ) 영업비밀을 지정된 장소 밖으로 무단으로 유출하거나(같은 호 나목), ⅲ) 영업비밀 보유자로부터 영업비밀을 삭제하거나 반환할 것을 요구받고도 이를 계속 보유함으로써 성립한다(같은 호 다목). 그 외에 ⅳ) 절취·기망·협박, 그 밖의 부정한 수단으로 영업비밀을 취득하거나(제18조 제1항 제2호), ⅴ) 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 알면서도 그 영업비밀을 취득하거나 사용(제18조 제1항 제3호)하는 행위도 처벌 대상이다.

또한 부정경쟁방지법 제18조는 영업비밀 침해행위에 대해 부정 이익 취득 또는 영업비밀 보유자에게 손해 입힐 목적으로 그 영업비밀 침해행위를 외국에서 하거나 외국에서 침해행위 할 것임을 알면서 취득 등 행위는 제1항으로, 국내에서의 영업비밀 침해행위는 제2항으로 각 규율하고, 외국에서 사용하거나 사용될 것임을 알면서 영업비밀 침해행위 하는 것에 대해서는 가중 처벌하고 있다.

조사기간 동안 입수된 영업비밀 침해행위 전체 형사사건 중에서 부정경쟁방지법 제18조 제1항 및 제2항을 적용하여 유죄판결이 선고된 결과를 분석한 결과는 아래 표와 같다.

표 15. 부정경쟁방지법 제18조 제1항 및 제2항 각 적용 유죄 현황

제18조 적용 현황	건수	비율
제1항	47	7.8%
제2항	255	42.1%
제1, 2항 양자 적용	15	2.48%
합계	317	52.4%



제18조 적용 유죄 판결 자유형 양형(연도별)

영업비밀 침해행위 형사사건 중 유죄로 선고된 사건을 제18조 제1항, 제2항으로 구분하여 연도별로 분석한 결과는 아래 표와 같다.

표 16. 부정경쟁방지법 제18조 제1항 유죄 자유형 양형 현황(연도별)

양형 \ 연도	2017	2018	2019	2020	2021	합계
유죄 건수[8]	7	1	14	9	12	43
자유형 평균(개월)[9]	23.86	12	15.73	15.1	16	

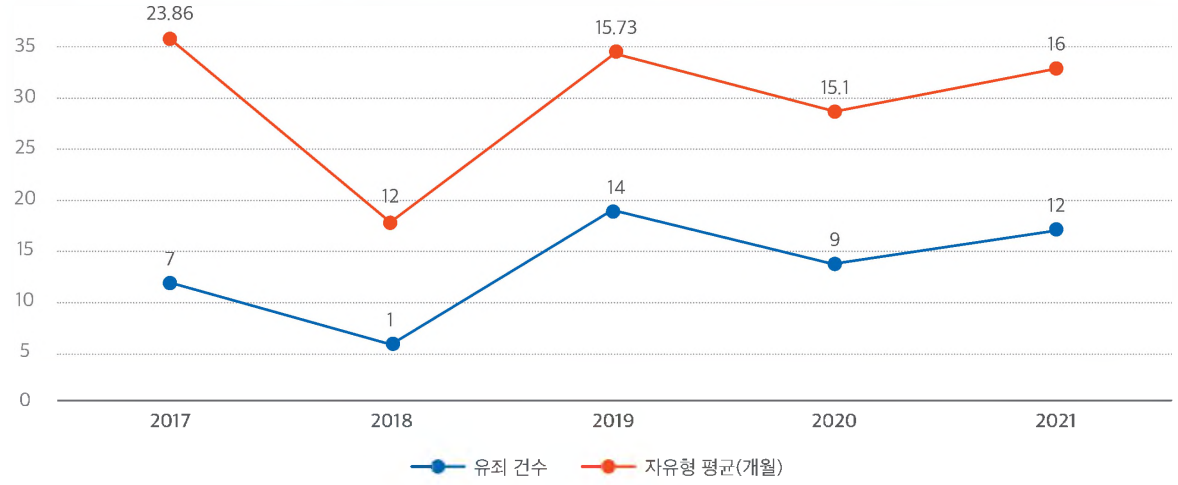
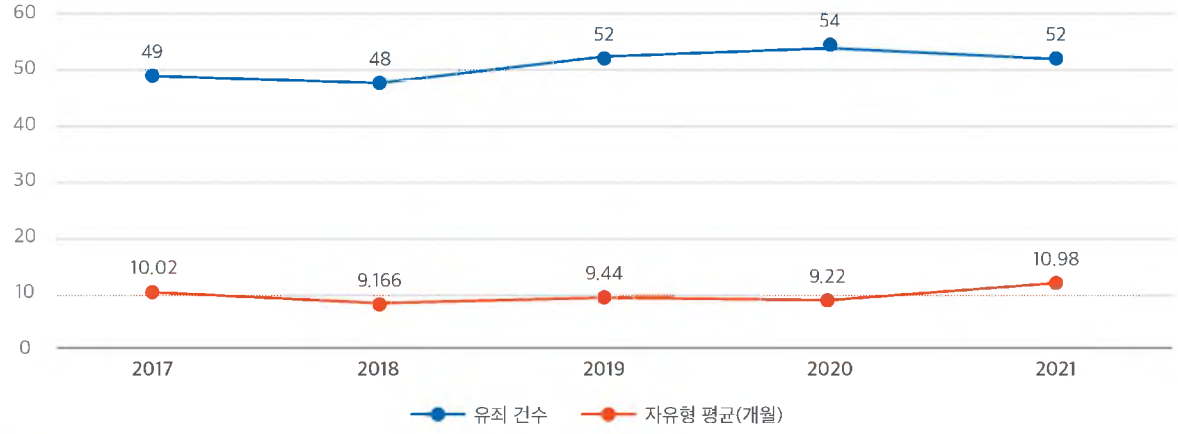


표 17. 부정경쟁방지법 제18조 제2항 유죄 자유형 양형 현황(연도별)

양형 \ 연도	2017	2018	2019	2020	2021	합계
유죄 건수[10]	49	48	52	54	52	255
자유형 평균(개월)[11]	10.02	9.166	9.44	9.22	10.98	



8) 대법원 판결 등 양형 확인 불가능한 판결 제외.
9) 업무상배임 등 타 법률 동시 적용 건 포함.
10) 대법원 판결 등 양형 확인 불가능한 판결 제외.
11) 업무상배임 등 타 법률 동시 적용 건 포함.

그 비율을 보면, 전체 유죄사건은 2017년 56건, 2018년 49건, 2019년 67건, 2020년 64건, 2021년 64건으로 나타났다.

각 연도별 평균 양형은 자유형의 경우 제18조 제1항은 2017년 23.86개월, 2018년 12개월, 2019년 15.73개월, 2020년 15.1개월, 2021년 16개월로 나타났고, 제18조 제2항은 2017년 10.02개월, 2018년 9.166개월, 2019년 9.44개월, 2020년 9.22개월, 2021년 10.98개월로 나타났다. 제18조 제1항의 양형이 제2항보다 더 강한 것으로 확인되었으나, 영업비밀 침해로 인한 피해와 상응하는 수준의 형량이 선고되는지에 관해서는 여전히 의문이 있다.

한편, 개정 부정경쟁방지법[법률 제16204호, 2019. 1. 8., 일부개정]은 제18조 제1항과 제2항을 개정하여 ㉠ 침해행위에 대한 법정형을 대폭 상향하였고, ㉡ 침해 예비·음모죄에 대한 벌금액도 상향하였으며, ㉢ 침해행위의 유형을 추가하고 구체화하였다(아래 참조).

표 18. 부정경쟁방지법 제18조 신·구 조문 대조표

제18조(벌칙) ① 부정한 이익을 얻거나 영업비밀 보유자에게 손해를 입힐 목적으로 그 영업비밀을 외국에서 사용하거나 외국에서 사용될 것임을 알면서 취득·사용 또는 제3자에게 누설한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. 다만, 벌금형에 처하는 경우 위반행위로 인한 재산상 이득액의 10배에 해당하는 금액이 1억원을 초과하면 그 재산상 이득액의 2배 이상 10배 이하의 벌금에 처한다.	제18조(벌칙) ① 영업비밀을 외국에서 사용하거나 외국에서 사용될 것임을 알면서도 다음 각 호의 어느 하나에 해당하는 행위를 한 자는 15년 이하의 징역 또는 15억원 이하의 벌금에 처한다. 다만, 벌금형에 처하는 경우 위반행위로 인한 재산상 이득액의 10배에 해당하는 금액이 15억원을 초과하면 그 재산상 이득액의 2배 이상 10배 이하의 벌금에 처한다.
〈신 설〉	1. 부정한 이익을 얻거나 영업비밀 보유자에 손해를 입힐 목적으로 한 다음 각 목의 어느 하나에 해당하는 행위 가. 영업비밀을 취득·사용하거나 제3자에게 누설하는 행위 나. 영업비밀을 지정된 장소 밖으로 무단으로 유출하는 행위 다. 영업비밀 보유자로부터 영업비밀을 삭제하거나 반환할 것을 요구받고도 이를 계속 보유하는 행위
〈신 설〉	2. 절취·기망·협박, 그 밖의 부정한 수단으로 영업비밀을 취득하는 행위
〈신 설〉	3. 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 알면서도 그 영업비밀을 취득하거나 사용(제13조제1항에 따라 허용된 범위에서의 사용은 제외한다)하는 행위
② 부정한 이익을 얻거나 영업비밀 보유자에게 손해를 입힐 목적으로 그 영업비밀을 취득·사용하거나 제3자에게 누설한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. 다만, 벌금형에 처하는 경우 위반행위로 인한 재산상 이득액의 10배에 해당하는 금액이 5천만원을 초과하면 그 재산상 이득액의 2배 이상 10배 이하의 벌금에 처한다.	② 제1항 각 호의 어느 하나에 해당하는 행위를 한 자는 10년 이하의 징역 또는 5억원 이하의 벌금에 처한다. 다만, 벌금형에 처하는 경우 위반행위로 인한 재산상 이득액의 10배에 해당하는 금액이 5억원을 초과하면 그 재산상 이득액의 2배 이상 10배 이하의 벌금에 처한다.
③ ~ ⑤ (생 략)	③ ~ ⑤ (현행과 같음)

제18조의3(예비·음모) ① 제18조제1항의 죄를 범할 목적으로 예비 또는 음모한 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. ② 제18조제2항의 죄를 범할 목적으로 예비 또는 음모한 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.	제18조의3(예비·음모) ① 제18조제1항의 죄를 범할 목적으로 예비 또는 음모한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. ② 제18조제2항의 죄를 범할 목적으로 예비 또는 음모한 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

그러나 영업비밀의 비밀관리 요건을 완화('합리적인 노력에 의해 비밀로 유지' ➜ '비밀로 관리')하였음에도 불구하고 비밀관리성이 부인되어 영업비밀로 인정받지 못해 무죄가 선고된 판결이 2건 있을 뿐, 개정법 제18조 제1항·제2항 그리고 제3항을 적용한 유죄 판결은 발견되지 않아 개정법 시행에 따른 법원의 선고형 변화 추이는 살펴볼 수 없었다. 따라서 향후 법원의 개정법 적용에 따른 양형 추이를 면밀하게 관찰할 필요가 있다.

제18조 적용 유죄 판결 실형 선고 비율

한편, 부정경쟁방지법상 영업비밀 침해로 자유형(집행유예 포함)이 선고된 300건을 실형과 집행유예로 분석한 결과는 아래 표와 같다.

표 19. 부정경쟁방지법 제18조 제1항 유죄 실형 선고 현황

자유형		합계
실형	집행유예	
15	28	43

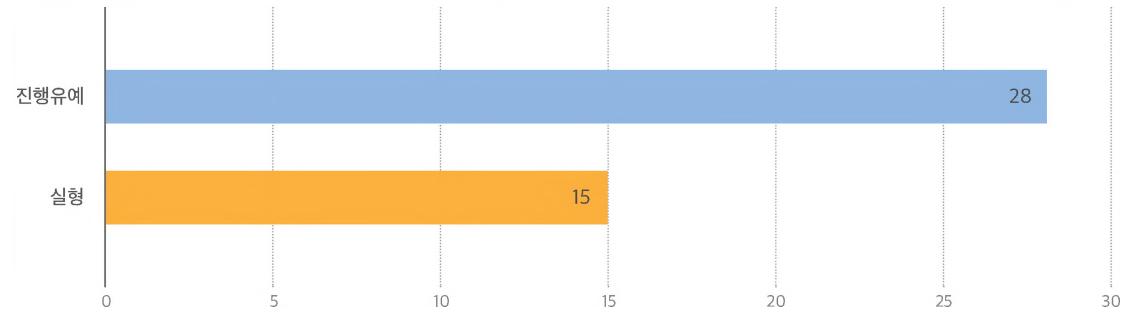
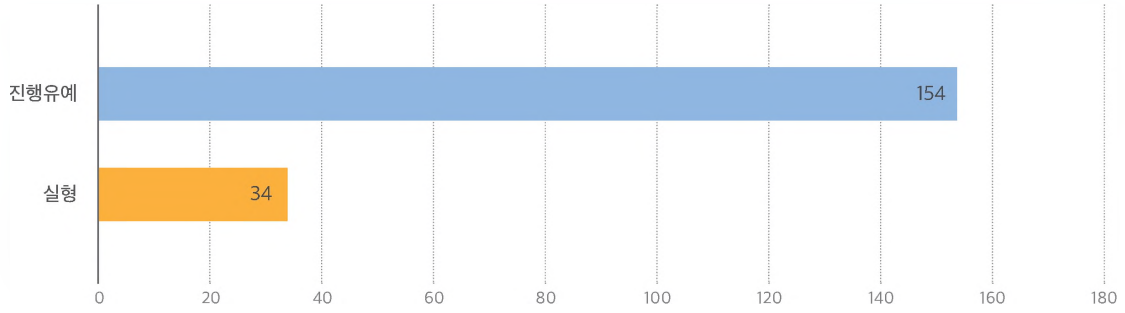


표 20. 부정경쟁방지법 제18조 제2항 유죄 실형 선고 현황

자유형		합계
실형	집행유예	
34	154	188



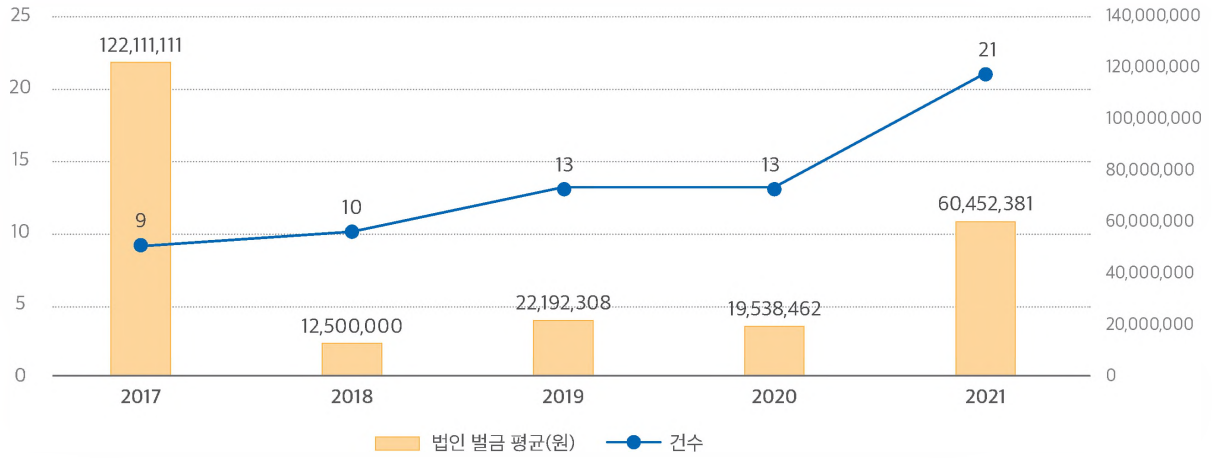
그 비율을 보면, 자유형이 선고된 사건 중 제1항의 실형이 선고된 사건의 비율은 34.88%(15/43), 제2항의 실형이 선고된 사건의 비율은 18.09%(34/188)로 조사되어 제1항의 실형 선고율이 훨씬 높은 것으로 조사되었다.

제19조 법인 양벌규정 적용 현황(연도별)

부정경쟁방지법상 양벌규정에 의한 법인 처벌 양형 수준을 연도별로 분석한바 아래와 같다.

표 21. 부정경쟁방지법 제19조 법인 양벌규정 유죄 양형 현황(연도별)

양형 \ 연도	2017	2018	2019	2020	2021
건수	9	10	13	13	21
법인 벌금 평균(원)	122,111,111[12]	12,500,000	22,192,308	19,538,462	60,452,381[13]



12) 법인 벌금 10억원 선고 사건(서울서부지방법원 2016노1185)이 있어서 평균 상향.

13) 법인 벌금 10억원 선고 사건(대법원 2017도16441)이 있어서 평균 상향.

바. 기타 참고사항

비대면 근무환경에서 비밀관리조치가 고려된 사례 여부

이번 조사에서 법원이 비대면 디지털 근무환경을 감안하여 비밀관리성의 성립 여부를 판단한 판결은 발견되지 않았다. 검사가 피고인이 회사의 중요한 자산을 반출한 행위를 업무상배임으로 의율하여 기소한 사건에서 당해 피고인이 '재택근무를 하기 위해 자료를 반출하였다'고 변소한 건이 있었지만(수원지방법원 2018노4562) 코로나19 이후 비대면 디지털 근무환경으로의 패러다임 변화를 고려한 판결은 아니었다.

다만 주목할 점은 이번 조사 결과 회사 외부에서 원격 근무를 하는 과정에 비밀 유출이 일어난 사건들을 발견할 수 있었다. 재택근무를 하면서 회사 서버에 접속하여 영업비밀 파일을 다운로드 받는다든지(수원지방법원 안산지원 2019고단3178 판결. 피고인에게 징역 1년 6월과 집행유예 3년이 선고되었다. / 수원지방법원 2017노1620 판결. 다만 이 사건에서 영업비밀로 인정받지 못해 피고인에게 무죄가 선고되었다), 회사 영업비밀을 개인 클라우드에 업로드 하거나 사진으로 촬영하여 클라우드 서비스에 업로드 하는 방식으로 유출하는 등 클라우드컴퓨팅을 이용하는 사례도 여러 건 발견되었다(수원지방법원 2021노2618 판결, 수원지방법원 안산지원 2020고단4438 판결, 의정부지방법원 고양지원 2018고단2917 판결, 수원지방법원 2020고단2902 판결, 수원지방법원 2020고단1120 판결, 수원지방법원 2019고단5986 판결, 대전지방법원 2020고단3803 판결, 서울동부지방법원 2018고단2485 판결, 대전지방법원 2018노2528 판결 등).

따라서 팬데믹 이후 비대면 근무환경이 보편적으로 자리 잡은 점, 특히 정보통신 분야나 전기전자 업종, 인터넷 서비스 기반 업종에서 이와 같은 비대면 디지털 근무환경의 추세가 역전되지는 않을 것이므로, 향후 법원의 판결 동향을 면밀하게 추적할 필요가 있다.

기업의 업종과 영업비밀과의 관계

전체 1,808건의 판결에서 나타난 영업비밀 정보의 내용에 따라 산업분류를 준용하여 총 8개 분야로 나누어 분석을 진행하였다. 그 결과 기계/소재는 361건, 전기/전자 295건, 정보통신 93건, 화학 109건, 바이오/의료 84건, 에너지/자원 39건, 일반서비스[14] 419건, 기타[15] 360건으로 확인되었다.

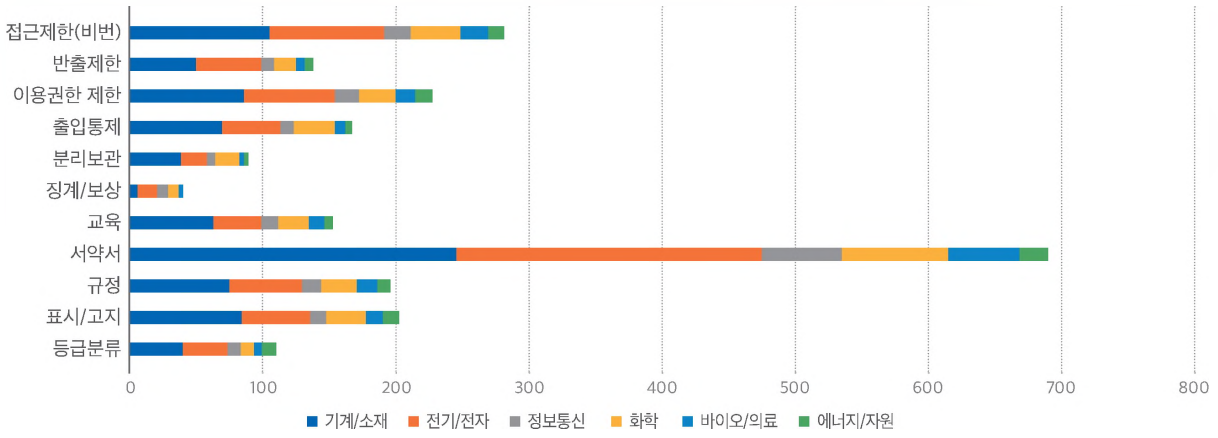
본 연구에서는 주요 업종 위주로 영업비밀 보호 조치의 빈도수를 분석하였다(아래 표).

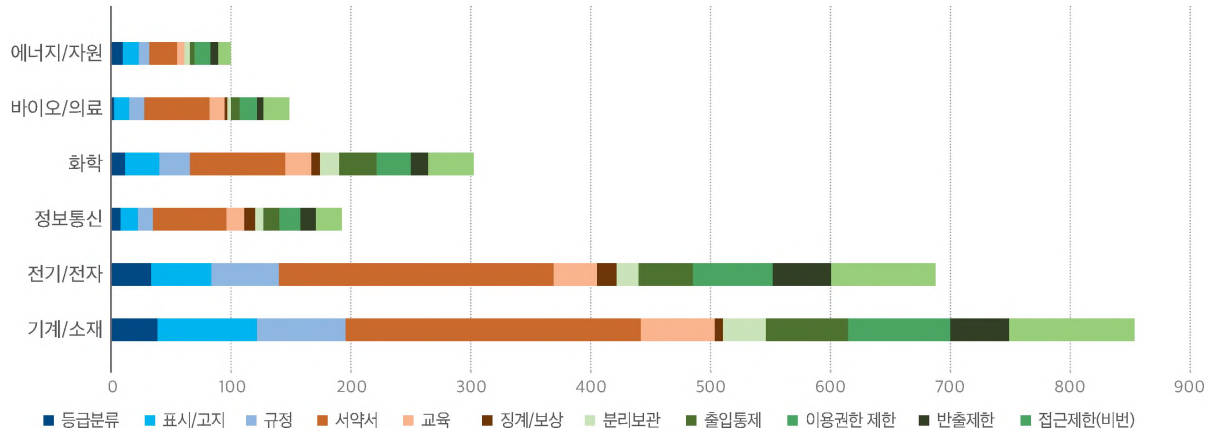
14) 산업기술혁신사업 공통 운영요령의 산업기술분류표를 준용하되, 프랜차이즈와 도소매업은 '기타'로 분류하였다. 가맹사업, 공인중개사, 꽃배달 등 배달업, 보안서비스, 보험, 산후조리, 쇼핑몰, 온라인 교육, 영상, 음식점, 식품 등 유통, 주류업 등을 일반서비스로 포섭하였다.

15) 가구점, 농수산물, 피트니스센터, 출판업 등을 기타 업종으로 포섭하였다.

표 22. 기업 업종과 영업비밀 보호 조치별 빈도 수(민·형사 통합)

구분	제도적 관리			인적 관리			물리적 관리				
판단 요소	등급분류	표시/고지	규정	서약서	교육	징계/보상	분리보관	출입통제	이용권한 제한	반출제한	접근제한(비번)
기계/소재	40	83	74	246	62	5	38	68	84	50	104
전기/전자	33	52	56	230	36	15	19	44	69	48	87
정보통신	10	13	14	61	14	9	8	12	19	11	21
화학	12	29	27	79	22	7	17	30	28	15	37
바이오/의료	3	12	15	54	12	2	2	8	14	7	20
에너지/자원	11	13	10	22	6	-	4	5	13	6	12
합계	109	202	196	692	152	38	88	167	227	137	281





전체 민·형사 사건 중 법원이 서약서 징구를 비밀관리 요소로 언급한 사건은 692건으로 가장 많았다. 그 다음으로 접근제한(비밀번호 등)이 281회, 이용권한제한은 227회로 나타났다.

분석 결과 기계/소재와 전기/전자 분야에서 영업비밀 보호 조치를 많이 취하였다는 점이 확인되었다. 하지만 법원이

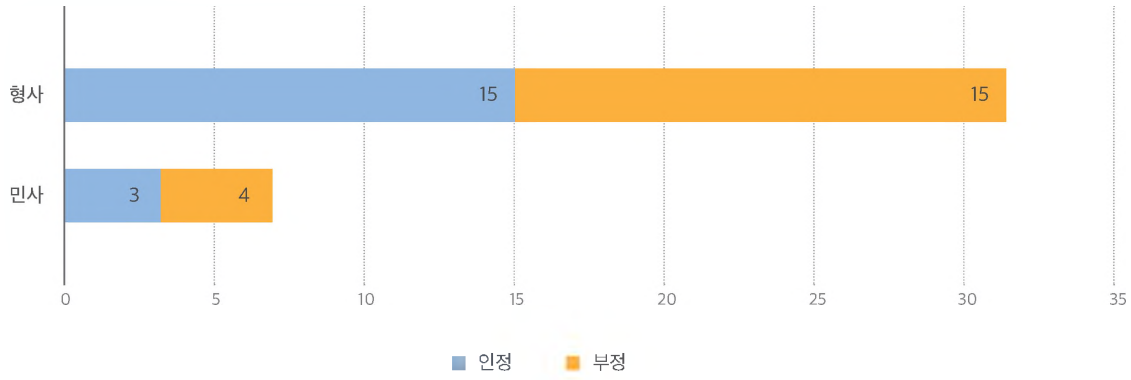
고려하는 영업비밀 관리 조치의 내용이나 빈도가 업종별로 각각 다른지 여부까지 구체적으로 확인되지는 않는다.

기업의 규모와 영업비밀 성립의 상관관계

분석 결과 법원이 비밀관리성 여부를 판단함에 있어 종업원 수나 자본금 등 기업의 규모를 고려하여 비밀관리성을 인정한 사건은 18건, 기업 규모를 고려하더라도 비밀관리성을 인정할 수 없다고 판단한 사건은 19건으로 확인되었다.

표 23. 기업 규모를 고려한 판결 결과

구분		인정	부정	전체
전체	민사	3	4	7
	형사	15	15	30
	합계	18	19	37



분석 대상 판결만으로는 법원이 기업 규모 등을 고려하여 비밀관리성을 완화할 경우 구체적으로 어떤 요소를 어느 정도 완화하는지, 기업 규모 등을 고려하더라도 반드시 취해야 할 조치가 무엇인지까지는 명확하게 나타나지 않았다.

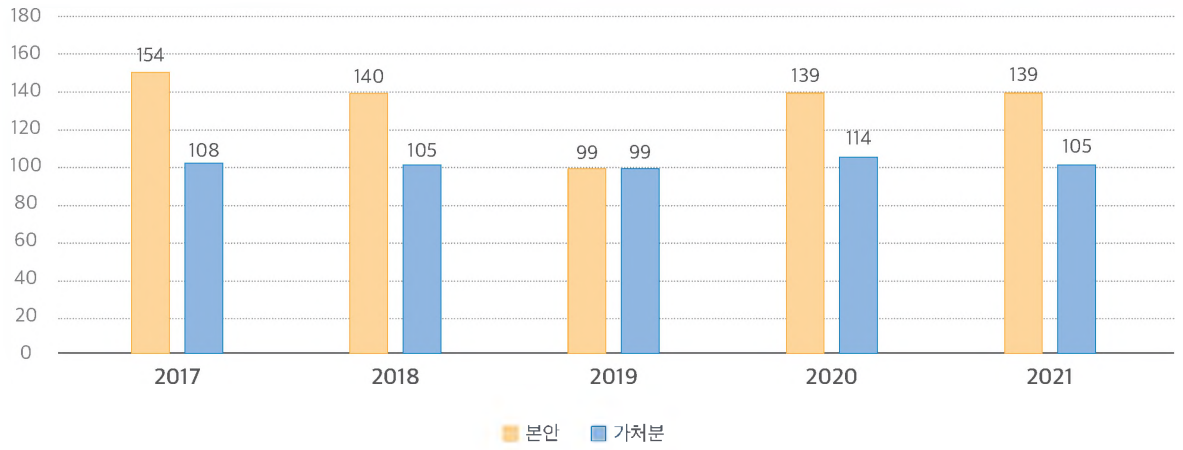
3. 영업비밀 침해 민사 판결 분석

가. 분석대상 판결

2017. 1. 1.부터 2021. 12. 31.까지 선고된 영업비밀 침해 관련 민사 판결은 총 1,249건이다. 분석대상 판결 1,249건 중 본안 사건과 가처분 사건의 수를 사건접수 연도에 따라 분류하면 아래 표와 같다.

표 24. 영업비밀 민사 판결 본안/가처분 집계

구분	민사		합계
	본안	가처분	
2017	154	108	262
2018	140	105	245
2019	99	99	198
2020	139	114	253
2021	139	105	244
합계	671	531	1,202



영업비밀 침해 민사 판결 중 본안 사건은 55.8%, 가처분 등 보전처분 사건은 44.2%로 나타났다.

영업비밀 침해 민사사건의 경우 가처분 사건의 비율이 일반 민사사건보다 현저히 높은 것으로 보인다. 이는 전체 영업비밀 침해 사건의 경우 부정경쟁방지법에서 구제수단으로 손해배상 외에 금지청구와 예방청구 등을 명시적으로 규정하고 있고, 사건의 성격상 신속한 권리구제의 필요성이 크기 때문으로 이해된다.

나. 연도별 비밀관리성 쟁점 판결

조직력이나 자금력이 상대적으로 부족한 중소기업 입장에서는 법정에서 "합리적인 노력에 의하여 비밀로 유지"해야 한다는 조건 성취를 입증하는 것이 쉽지 않았다. 이에 영업비밀로 보호받지 못하는 사례가 많았는바, 이에 2019. 1. 8. 법률 제16204호 부정경쟁방지법 개정을 통해 비밀관리성 요건을 완화하여 "비밀로 관리"만 하면 되는 것으로 요건을 완화하였다.

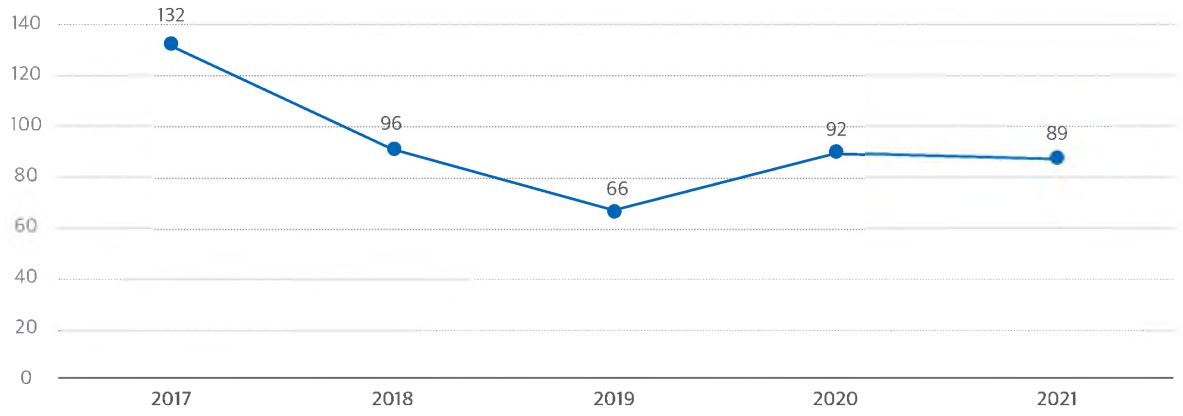
그러나 이번 조사에서 위 개정법상 "비밀로 관리" 요건을 적용하여 판결한 민사 사건은 10건밖에 없었다. 그리고 그

중에서도 비밀관리성을 인정하여 영업비밀 침해를 인정한 건은 단 1건 뿐이었다(수원지방법원 2020카합10357). 그마저도 영업비밀로서 보호받기 위한 어느 정도의 노력이 '비밀로 관리'한 것으로 인정받을 수 있는지에 대한 명확한 기준은 아직까지 제시되지 아니한 상황이다.

이에 개정법(2019. 1. 8. 법률 제16204호 부정경쟁방지법)을 적용한 유의미한 민사 판결이 아직 없는 가운데 연도별로 비밀관리성이 쟁점이 된 판결 비율을 분석한바 아래와 같다.

표 25. 연도별 비밀관리성 쟁점 판결(민사)

연도 / 비밀관리	2017	2018	2019	2020	2021	합계
건수	132	96	66	92	89	475



비밀관리성은 회사의 노력 여하에 따라 "영업비밀"로 인정받을 수 있는 가능성을 끌어올릴 수 있는 가장 중요한 요건이다. 따라서 개발 사건들에서 꾸준히 주요 쟁점으로 부각되고 있다.

다만 개정법상 완화된 비밀관리 요건 관련하여 충분한 데이터가 아직까지 축적되지 않은 관계로, 어느 정도면 "비밀로 관리"했다고 인정받을 수 있을지 향후 지속적인 판결 동향 분석을 통해 법원의 판단 기준을 확인할 필요가 있다.

다. 영업비밀 보호 조치별 비밀관리성 분석

본 연구에서는 기업의 영업비밀 관리·조치를 아래 기준에 따라 구분하였다. 크게 제도적 관리, 인적 관리, 물리적 관리로 분류하고, 다시 세부 내용에 따라 하위 조치를 구분하였다.

표 26. 영업비밀 보호 조치 분류

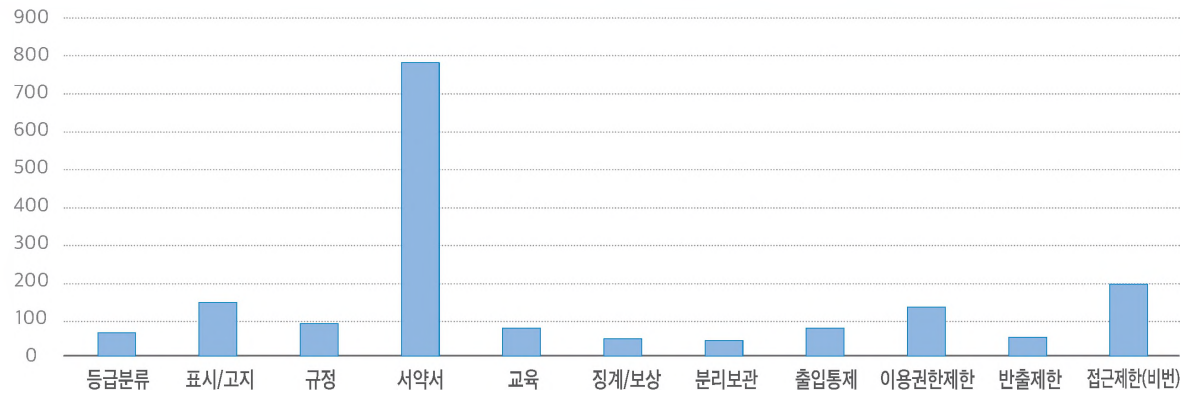
보호조치		내용
제도적 관리	등급분류	영업비밀 또는 중요한 자산을 중요도에 따라 분류
	표시/고지	영업비밀임을 인식할 수 있는 표시를 하였거나 고지
	규정	각종 영업비밀 보호 규정

보호조치		내용
인적 관리	서약서	영업비밀 보호 서약서, 계약 등 영업비밀 보호 약정
	교육	영업비밀 보호 관련 교육
	징계/보상	영업비밀 보호 관련 징계 또는 보상
물리적 관리	분리보관	영업비밀을 일반 정보와 분리된 장소에 보관
	출입통제	영업비밀이 보관된 장소에 대한 출입 통제
	이용제한	영업비밀 접근·권한을 임직원 별로 구분·제한
	반출제한	영업비밀 외부 반출 통제
	접근제한	영업비밀에 대한 접근 방법을 제한(비밀번호 등)

법원이 민사 사건에서 비밀관리성 판단을 하면서 가장 많이 언급한 영업비밀 보호관리 조치는 "서약서"와 "접근제한(비밀번호 등)"이었으며, 다음으로는 이용권한 제한 여부와 표시/고지 순으로 나타났다. 보호 조치별 빈도수를 분석한 결과는 아래와 같다.

표 27. 영업비밀 보호 조치별 빈도 수(민사)

구분	제도적 관리			인적 관리			물리적 관리				
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용권한 제한	반출 제한	접근제한 (비번)
민사	65	152	96	784	78	53	47	74	139	62	195

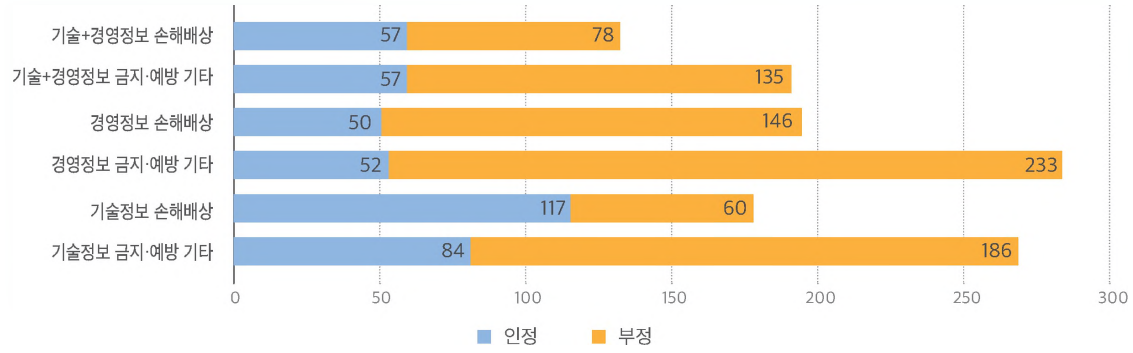


라. 영업비밀 정보 유형별 분석

법원 판결에서 쟁점이 된 영업비밀을 정보 유형별로 나누어 분석한바, 경영정보가 364건, 기술정보가 350건으로 나타났다. 기술정보와 경영정보 모두 침해되었다고 주장된 사건도 291건에 달하였다. 이를 통해 기술정보와 경영정보 모두 폭넓게 유출 대상이 되고 있음을 확인할 수 있었다.

표 28. 정보 유형별 영업비밀성 분석(민사)

구분	전체	소송물	인정	부정
기술정보	350	금지·예방 기타	84	186
		손해배상	117	60
경영정보	364	금지·예방 기타	52	233
		손해배상	50	146
기술+경영정보	291	금지·예방 기타	57	135
		손해배상	57	78



기술정보가 유출된 350건의 판결 중에서 금지·예방 기타 청구가 인용된 비율은 32.2%(84건/270건), 손해배상 청구가 인용된 비율은 66.1%(117건/177건)였다.[16]

경영정보가 유출된 364건의 판결에서 금지·예방 기타 청구가 인용된 비율은 18.25%(52건/285건), 손해배상 청구가 인용된 비율은 25.5%(50건/196건)로 나타났다.

그리고 기술정보와 경영정보 전부가 유출된 291건의 사건에서 금지·예방 기타 청구가 인용된 비율은 29.7%(57건/192건), 손해배상 청구가 인용된 비율은 29.1%(57건/196건)로 나타났다.

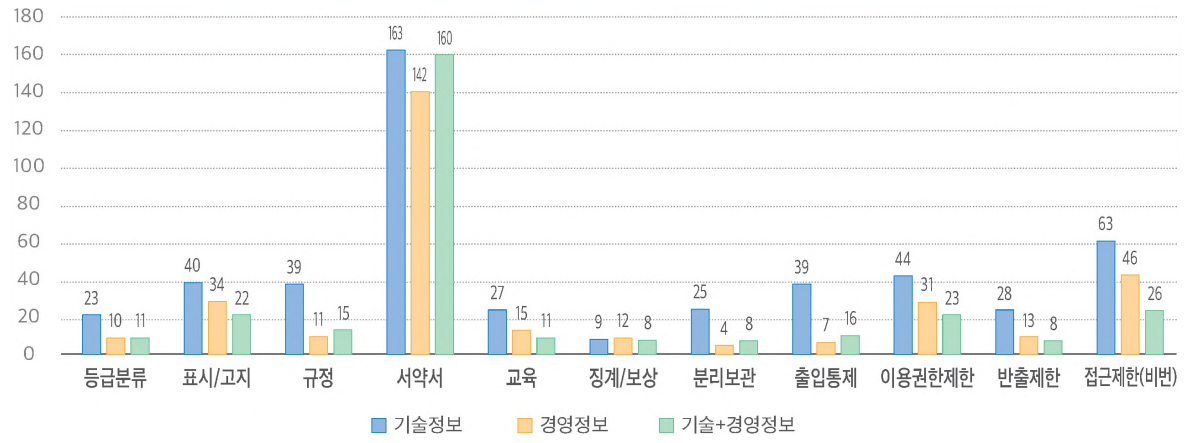
영업비밀 정보 유형별 보호관리 조치의 빈도수를 살펴보면, 기술정보와 경영정보 통틀어 공히 서약서 징구가 많이 활용되었다. 그 다음으로는 기술정보와 경영정보 모두에서 접근제한 조치(비밀번호 등)이 많이 활용되었다. 다음으로 기술정보에서는 이용권한 제한(44건)이, 경영정보에서는 표시/고지(34건)가 활용된 것으로 나타났다.

정리하면 서약서, 접근제한 조치, 표시/고지가 영업비밀 보호관리 조치로 자주 활용되었고, 기술정보의 경우'출입통제'가 이루어졌는지 여부도 자주 언급된 것으로 나타났다.

16) 금지·예방 기타 청구와 손해배상 청구를 중복하여 제기한 소송이 있어서 일부 데이터가 중복되었다.

표 29. 영업비밀 정보 유형별 빈도 수(민사)

구분	제도적 관리			인적 관리			물리적 관리				
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용권한 제한	반출 제한	접근제한 (비번)
기술정보	23	40	39	163	27	9	25	39	44	28	63
경영정보	10	34	11	142	15	12	4	7	31	13	46
기술+경영 정보	11	22	15	160	11	8	8	16	23	8	26
합계	44	96	65	438	53	29	37	62	98	49	135



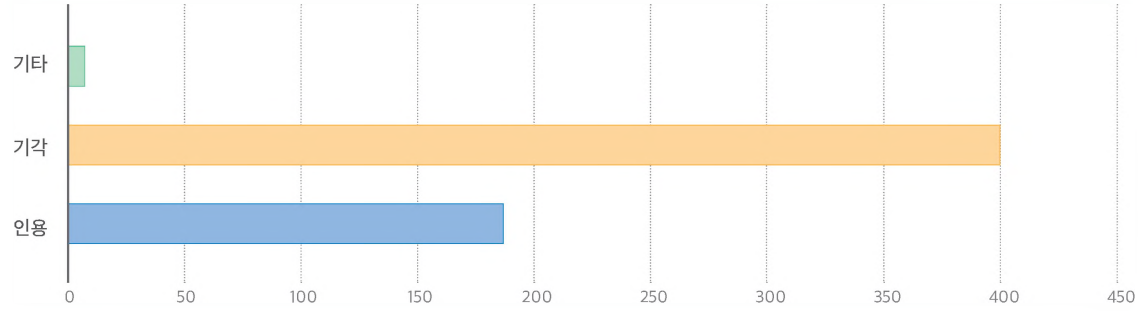
마. 손해배상 사건 분석

인용율 및 손해배상액 분석

영업비밀 침해행위 민사사건에서 구제수단으로 손해배상을 택한 경우 총 595건의 처리결과는 아래 표와 같다.

표 30. 영업비밀 민사 손해배상 청구 인용율

사건결과	인용	기각	기타	합계
건수	188	401	6	595

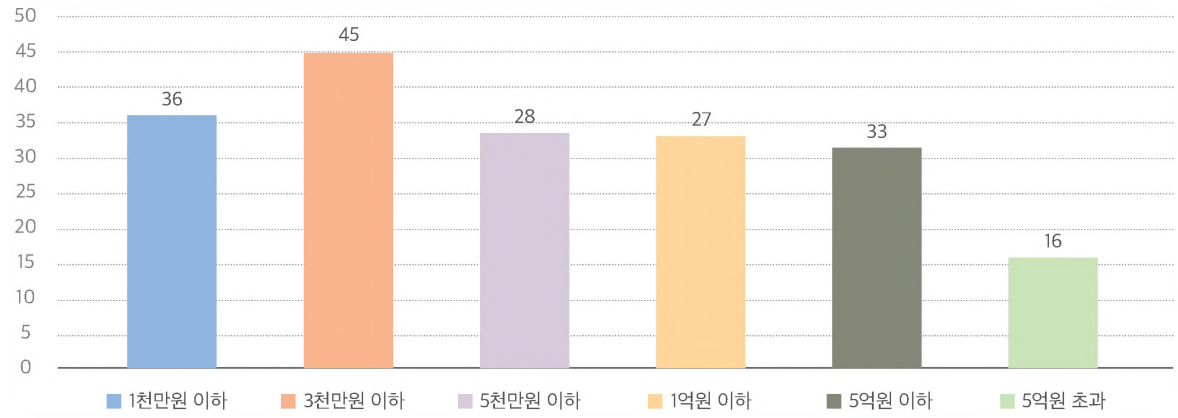


그 구체적 비율을 보면, 손해배상청구 사건에서 인용 비율은 31.60%(188건/595건), 기각 비율은 67.39%(401건/595건)인 것으로 분석되었다.

한편, 손해배상이 인정된 사건에서 손해배상액을 1천만원 이하, 5천만원 이하, 5천만원 내지 1억 원 이하, 1억 원 내지 5억 원 이하, 5억 원 초과로 구간을 나누어 분석한 결과는 다음과 같다.

표 31. 영업비밀 침해행위 민사사건 손해배상 사건 분석

손해배상액	1천만 원 이하	3천만 원 이하	5천만 원 이하	1억 원 이하	5억 원 이하	5억 원 초과	합계
건수	36	45	28	27	33	16	167[17]



3천만 원 이하의 배상액이 45건으로 그 비율이 가장 높게 나타났다. 인용된 손해배상액 중 가장 큰 금액은 금 85억 여 원이었다(대구고등법원 2016나1602 판결).

손해배상액 산정 근거

부정경쟁방지법 제11조는 고의 또는 과실에 의한 영업비밀 침해행위로 영업비밀 보유자의 영업상 이익을 침해하여 손해를 입힌 자는 그 손해를 배상할 책임을 진다고 규정하고 있다. 그리고 손해배상액에 관하여 이를 명확히 할 수 없는 경우 동법 제14조의2 손해배상액의 추정을 규정하고 있다.

민사상 불법행위에 기한 손해배상청구의 원칙은 불법행위와 상당인과관계가 있는 손해를 배상하는 것이다. 이는 부정경쟁방지법상 영업비밀 침해로 인한 손해에 있어서도 마찬가지다. 하지만 일반 불법행위와 달리 영업비밀 침해로 인한 손해, 특히 소극적 손해(불법행위로 인하여 얻지 못하게 된 이익)를 산정함에 있어서는 침해가 없었을 경우를 가정한 전형적인 사상경과를 추론하는 것이 쉽지 않다. 이에 부정경쟁방지법 제14조의2는 손해액 산정에 관한 특칙을 규정하여 원고의 입증책임을 완화하고 있는 것이다.

부정경쟁방지법 제14조의2에 따른 손해배상액의 추정방법은 아래와 같다.

17) 대법원 판결 등 판결금 확인이 안 되는 사건 제외.

1) 제1항 - 영업상의 이익을 침해한 자가 영업비밀 침해행위를 하게 한 물건을 양도하였을 때 손해액

ⅰ) (침해당한 자가 생산할 수 있었던 물건의 수량 - 실제 판매한 물건의 수량) × 영업상의 이익을 침해당한 자가 영업비밀 침해행위가 없었다면 판매할 수 있었던 물건의 단위수량당 이익액

ⅱ) 침해당한 자가 생산할 수 있었던 물건의 수량에서 실제 판매한 물건의 수량을 뺀 수량을 넘는 수량 또는 영업비밀 침해행위 외의 사유로 판매할 수 없었던 수량이 있는 경우, 이들 수량에 대해서는 '영업상의 이익을 침해당한 자가 부정경쟁행위등침해행위가 없었으면 합리적으로 받을 수 있는 금액'

2) 제2항 - 영업상의 이익을 침해한 자가 그 침해행위에 의하여 이익을 받은 것이 있으면 그 이익액을 영업상의 이익을 침해당한 자의 손해액으로 추정

3) 제3항 - 영업비밀 침해행위 대상이 된 영업비밀의 사용에 대하여 통상 받을 수 있는 금액에 상당하는 금액(실시료)

4) 제5항 - 법원이 변론 전체의 취지와 증거조사의 결과에 기초하여 상당한 손해액 인정(손해발생은 인정되나 그 손해액을 입증하기 위하여 필요한 사실을 입증하는 것이 해당 사실의 성실상 극히 곤란한 경우)

영업비밀 침해행위 민사사건 손해배상액 산정근거 분석결과 부정경쟁방지법 제14조의2 제5항이 적용된 사건이 가장 많았으며, 제1항과 제2항이 적용된 사건이 일부 있었고, 제3항이 적용된 사건도 1건 있었다.

[주요판결]

아래 판결은 부정경쟁방지법 제14조의2 제1항 및 제5항의 손해배상액 산정에 관한 리딩 케이스가 될 것으로 판단된다. 주요 부분을 발췌하면 아래와 같다.

대구고등법원 2017. 5. 11. 선고, 2016나1602 손해배상(기) 판결

[표] 부정경쟁방지법 제14조의2 제1항에 의한 손해액 산정

제1항 전문	원칙	손해액 = 침해품의 양도수량 × 피침해자의 제품 단위수량당 이익액
제1항 후문	한도	피침해자의 생산능력(피침해자가 생산할 수 있었던 물건 수량 - 실제 판매한 물건 수량)
제1항 단서	공제	침해행위 외의 사유로 판매할 수 없었던 사정 부분 공제

[손해배상액의 산정]

가) 피고 회사의 매출액

- 피고 회사는 원고 회사의 영업비밀을 침해하여 원고 회사와 같은 초경합금 제품을 생산·판매하여 2021년부터 영업비밀 보호기간 범위 내인 2015년까지 계속 매출을 올렸다. 피고 회사는 위 초경합금 제품 외에 다른 제품을 생산하거나 판매한 사실은 없다. 따라서 피고 회사의 위 연간 매출액을 피고 회사가 원고 회사의 영업비밀을 침해하여 생산한 제품의 총판매액으로 본다.
- 피고 회사의 매출액 : 피고 회사의 매출액을 부정경쟁방지법 제14조의2 제1항에 따른 '침해자의 양도수량' 총액으로 평가할 수 있다.

나) 원고 회사의 이익액

- 부정경쟁방지법 제14조의2 제1항의 피침해자의 '단위수량당 이익액'은 피침해자의 매출액에서 비용을 공제하여 산출된 이익액을 판매제품의 수량으로 나눈 것으로, 여기서 이익액은 제조원가와 함께 그 제품의 판매를 위하여 추가로 지출하였을 것으로 보이는 변동비를 공제한 금액(한계이익)으로 보아야 한다.
- 피침해자인 원고 회사의 한계이익률을 부정경쟁방지법 제14조의2 제1항에 따른 '단위수량당 이익액'으로 평가한다.

다) 손해배상액의 한도

- 피침해자인 원고 회사의 생산능력에 따른 금액을 원고 회사의 2011년 매출액으로 보고, 위 매출액에서 원고 회사의 2012년부터 2015년까지 각 해당연도의 매출액을 뺀 금액에 원고 회사의 한계이익률을 곱한 금액을 부정경쟁방지법 제14조의2 제1항의 피침해자가 '생산할 수 있었던 물건의 수량에서 실제 판매한 물건의 수량을 뺀 수량에 단위수량당 이익액을 곱한 금액'으로 평가하고, 이를 원고 회사의 손해배상액 한도로 본다.

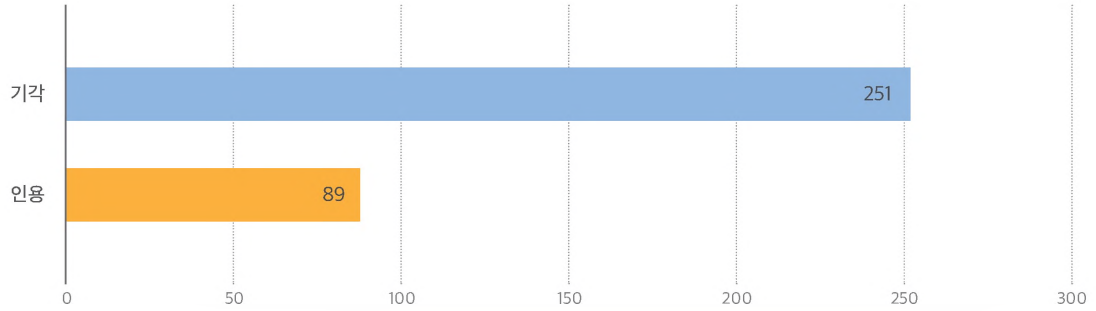
부정경쟁방지법 제14조의2 제5항을 적용하여 법원이 직권으로 손해액을 산정하는 경우가 가장 많은 이유는 제1항 내지 제3항에 의한 손해액 또는 이익액 산정을 위한 구체적인 증거에 의한 입증하는 것이 용이하지 않기 때문으로 추측된다. 이로 인하여 현실적인 손해액에 미치지 못하는 경우가 많을 것으로 생각되므로, 위에서 본 판결(대구고등법원 2016나1602 판결)과 같이 피해자와 법원 모두 현실적인 손해액을 입증하기 위한 적극적인 대책과 전향적인 자세로 실질적 손해배상이 이루어지게끔 할 필요가 있다.

바. 경업금지 및 전직금지 사건

경업금지와 전직금지도 넓게 보아 영업비밀을 보호하기 위한 구제수단의 하나로 보아 분석대상 판결에 포함하였다. 조사기간 중 수집한 전직금지가처분 신청 등 사건의 판결을 분석한 결과는 아래 표와 같다.

표 32. 경업금지/전직금지 인용율

인용여부	인용	기각
건수	89	251



구체적으로 살펴보면 전직금지청구를 인용한 경우는 25.14%(89건/354건), 기각한 경우는 70.9%(251건/354건)로 기각률이 더 높다. 이는 사용자에게 보호할 만한 경제적 이익이 있고 이를 보호하기 위하여 필수적이고 불가피할 경우 경업금지나 전직금지 신청을 받아들이기 때문으로 추측된다. 다만 법원 판결은 근로자에게 보장된 헌법상 직업선택의 자유를 고려하여 전직금지의 기간을 일부 제한하는 경향을 띤다.

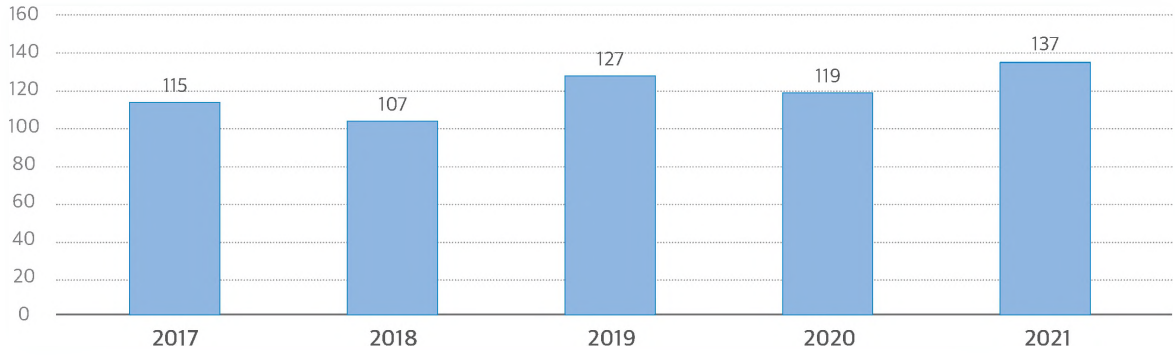
4. 영업비밀 침해 형사 판결 분석

가. 분석대상 판결

2017. 1. 1.부터 2021. 12. 31.까지 선고된 형사사건 중 영업비밀 침해행위 관련 판결로는 총 605건이 입수되었고 이를 사건접수연도에 따라 분류하면 아래 표와 같다.

표 33. 영업비밀 형사 판결 연도별 집계

선고년도	판결 수
2017	115
2018	107
2019	127
2020	119
2021	137
합계	605



나. 연도별 비밀관리성 쟁점 비율

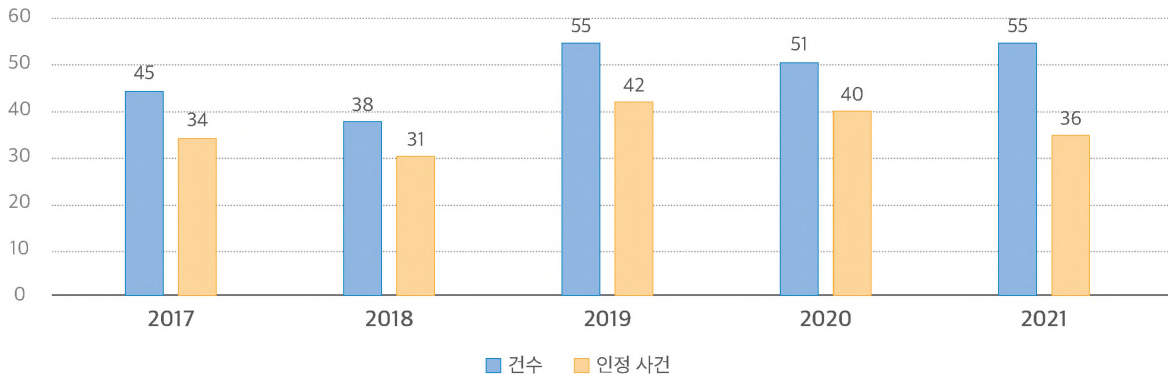
영업비밀 유출 의심자를 상대로 형사 고소를 하더라도, 중소기업 입장에서는 "합리적인 노력에 의하여 비밀로 유지"하는 것이 쉽지 않아 영업비밀로 보호받지 못하는 경우가 많았다. 이에 2019. 1. 8. 법률 제16204호 부정경쟁방지법 개정을 통해 비밀관리성의 요건을 완화하여 "비밀로 관리"만 하면 되는 것으로 요건을 완화하였다.

그러나 이번 조사에서 위 개정법상 "비밀로 관리" 요건을 적용하여 판결한 형사 건은 2건밖에 없었다. 그리고 그 중에서도 비밀관리성을 인정하여 영업비밀 침해를 인정한 건은 한 건도 없었다. 비밀관리 요건을 완화하였음에도 불구하고 해당 사건들에서 법원은 비밀관리성을 인정하지 아니하였다(인천지방법원 2020고단2847 판결, 서울동부지방법원 2021노333 판결).

이에 개정법(2019. 1. 8. 법률 제16204호 부정경쟁방지법)을 적용한 유의미한 판결이 아직 없는 가운데 연도별 비밀관리성을 인정한 형사 판결 비율을 분석한바 아래와 같다.

표 34. 연도별 비밀관리성 쟁점 판결 비율(형사)

연도 / 비밀관리	2017	2018	2019	2020	2021	합계
건수	45	38	55	51	55	244
인정 사건	34	31	42	40	36	183
인정 비율	75.55%	81.58%	76.36%	78.43%	65.45%	



검사가 기소한 영업비밀 침해 사건에서 영업비밀로 인정된 비율은 대체로 70~80% 선에 달하였다. 다만 개정법 관련하여 충분한 데이터가 아직까지 축적되지 않은 관계로, 어느 정도면 "비밀로 관리"했다고 인정받을 수 있을지 향후 지속적인 판결 동향 분석을 통해 법원의 판단 기준을 확인할 필요가 있다.

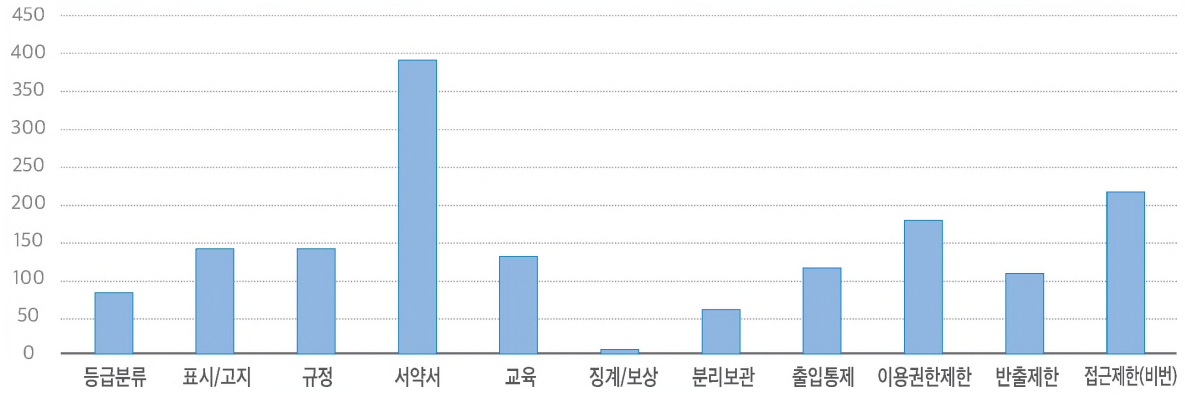
다. 영업비밀 보호 조치별 분석

법원이 형사 사건에서 비밀관리성 판단을 하면서 가장 많이 언급한 영업비밀 보호관리 조치는 "서약서"와 "접근제한(비밀번호 등)"이었고, 다음으로는 이용권한 제한 여부와 영업비밀 보호 규정 순으로 나타났다. 그 외에도 영업비밀 "보호 규정", 영업비밀의 "표시 또는 고지"가 보호 조치로 많이 언급되었다.

보호 조치별 빈도수를 분석한 결과는 아래와 같다.

표 35. 영업비밀 보호 조치별 빈도 수(형사)

구분	제도적 관리			인적 관리			물리적 관리				
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용권한 제한	반출 제한	접근제한 (비번)
형사	78	144	149	388	128	6	65	117	178	110	216

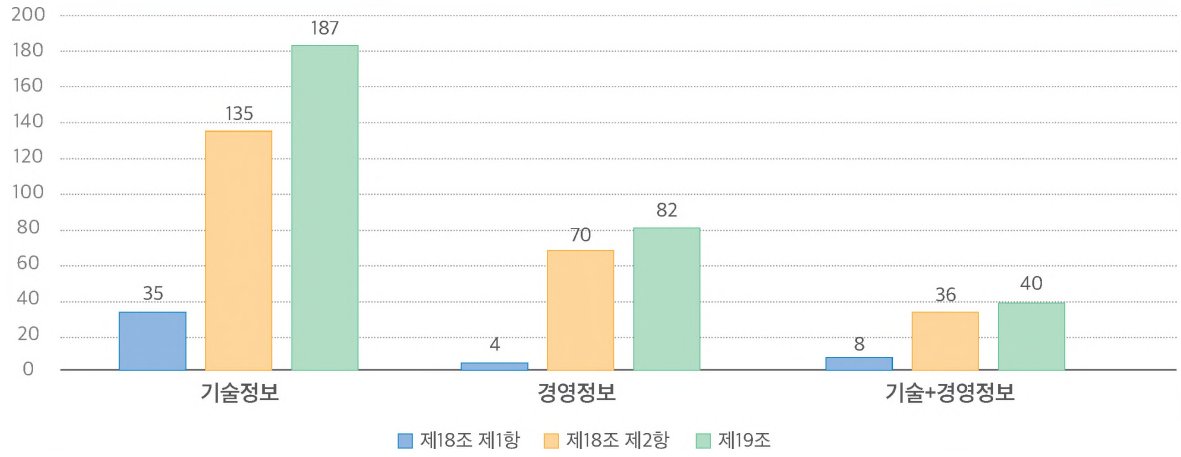


라. 영업비밀 정보 유형별 분석

법원의 형사 판결에서 쟁점이 된 영업비밀을 정보 유형별로 나누어 분석한바, 기술정보가 319건으로 압도적으로 많았고, 경영정보는 148건, 기술정보와 경영정보 모두 유출된 것으로 기소된 건은 86건으로 나타났다. 이를 통해 검찰은 영업비밀 침해 형사 사건에서 주로 기술정보 유출을 더 중요하게 다루고 기소하고 있음을 확인할 수 있었다.

표 36. 정보 유형별 영업비밀 유죄 판결 분석(형사)

구분	전체	제18조 제1항	제18조 제2항	제19조
기술정보	319	35	135	187
경영정보	148	4	70	82
기술+경영정보	86	8	36	40



기술정보가 유출된 319건의 판결 중에서 제18조 제1항 유죄가 선고된 사건은 35건, 제2항 유죄가 선고된 사건은 135건, 제19조(양벌규정) 유죄 선고 사건은 187건에 달하였다.

경영정보가 유출된 148건의 판결 중에서 제18조 제1항 유죄가 선고된 사건은 4건, 제2항 유죄가 선고된 사건은 70건, 제19조(양벌규정) 유죄 선고 사건은 82건으로 나타났다.

그리고 기술정보와 경영정보 전부가 유출된 86건의 사건에서 제18조 제1항 유죄가 선고된 사건은 8건, 제2항 유죄가 선고된 사건은 36건, 제19조(양벌규정) 유죄 선고 사건은 40건으로 나타났다.

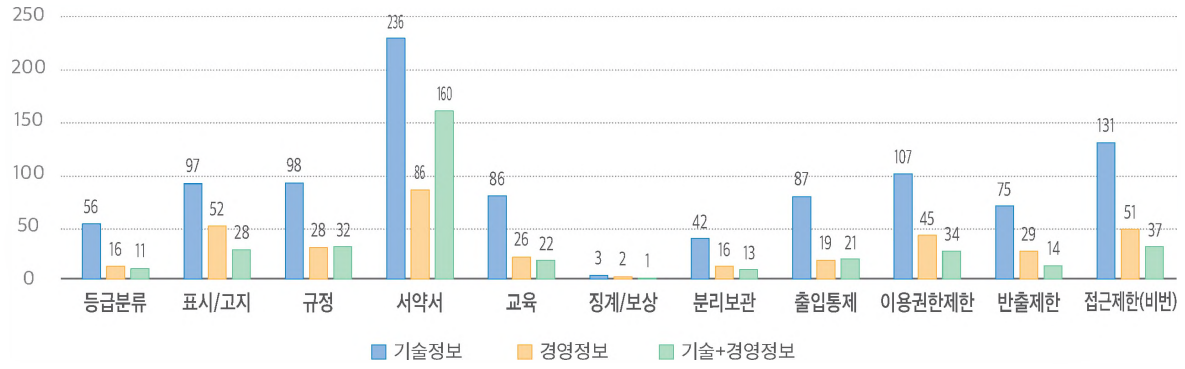
영업비밀 정보 유형별 보호관리 조치의 빈도수를 살펴보면, 기술정보와 경영정보 통틀어 공히 서약서 징구가 많이 활용되었다. 그 다음으로는 기술정보와 경영정보 모두에서 접근제한 조치(비밀번호 등)이 많이 활용되었다. 이는 민사 사건 분석과도 일치하는 결과다.

다음으로 기술정보과 경영정보에서 이용권한 제한이 많이 활용되었다(기술정보 : 107건 / 경영정보 : 45건).

정리하면 서약서, 접근제한 조치, 이용권한 제한이 영업비밀 보호관리 조치로 자주 활용되었고, 기술정보의 경우'표시/고지'와 '규정'이 자주 언급된 것으로 나타났다.

표 37. 영업비밀 정보 유형별 빈도 수(형사)

구분	제도적 관리			인적 관리			물리적 관리				
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용권한 제한	반출 제한	접근제한 (비번)
기술정보	56	97	98	236	86	3	42	87	107	75	131
경영정보	16	32	28	86	26	2	16	19	45	29	51
기술+경영 정보	11	28	32	67	22	1	13	21	34	14	37
합계	83	157	158	389	134	6	71	127	186	118	219



마. 부정경쟁방지법 제18조 무죄 판결 비율 및 이유 분석

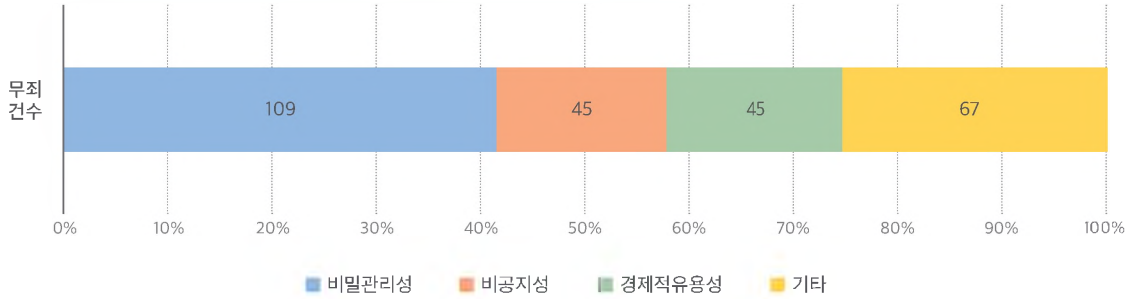
제18조 무죄 이유 비율

영업비밀 침해행위 형사판결 605건 중 업무상배임죄 등을 제외하고 순수하게 부정경쟁방지법위반죄로 기소되어 무죄가 선고된 판결은 173건으로 파악되었다. 이 중에서 유/무죄를 분석한 결과는 아래 표와 같다.

표 38. 부정경쟁방지법 제18조 무죄 이유 분석

무죄 사유*	비밀관리성	비공지성	경제적 유용성	기타[18]
무죄 건수[19]	109	45	45	67
비율	63%	26%	26%	38.7%

* 위 각 무죄사유는 하나의 사건 내에서 중복될 수 있다.



18) 영업비밀이 특정되지 아니하였거나, 법원이 단순히 증명 부족으로 무죄 판결하거나, 영업비밀 보호기간이 도과하였거나, 상급심에서 기각되는 등으로 유무죄를 분석하지 못한 경우.
19) 피고인이 복수일 경우 주범인 피고인을 중심으로 분석하였다.

분석 결과 검사가 기소한 부정경쟁방지법상 영업비밀 침해 전체 사건 중 "비밀관리성" 요건 불충족으로 무죄가 선고된 비율은 63%, "비공지성"과 "경제적 유용성" 요건 탈락으로 무죄가 선고된 비율은 각각 26%, 기타 영업비밀 불특정 또는 영업비밀 보호기간 도과, 부정한 목적의 부존재, 입증 부족으로 무죄가 선고된 비율은 38.7%로 나타났다.

이러한 결과는 영업비밀 성립요건 중 "비밀관리성"이 중요하다는 점을 단적으로 보여준다.

5. 의의 및 한계

영업비밀 관련 판례의 분석은 부정경쟁방지 및 영업비밀 보호에 관한 법률의 법 집행의 실효성을 제고하기 위해 반드시 필요한 작업이다. 그동안 영업비밀 침해 사건의 유형 및 쟁점, 기업의 규모·업종별, 비밀관리성 판단 요소별 빈도 중심으로 연구가 이루어져 왔다.

본 연구는 2014년도에 발행된 영업비밀 보호 가이드가 2008년부터 2012년까지 선고·결정 판결문을 토대로 도출된 관계로, 개정된 법률과 판례 등을 반영하여 현행화 할 필요에서 추진되었다. 구체적으로는 영업비밀 비밀관리성 인정요건 완화,[20] 3배 손해배상제도 도입, 벌칙 강화 등에 따른 법원의 판결 동향에 따른 비밀관리체계를 재설정하는 데 필요한 데이터를 구축하기 위함이다. 또한 본 연구는 2019 코로나 팬데믹 이후 급속히 확산된 비대면 디지털 근무환경에서 비밀관리조치가 고려된 사례를 분석하여 원격 접속 이용 시 필요한 조치 및 주의사항을 도출하는 것에도 그 의의를 두었다.

연구 결과, 영업비밀 성립요건별, 침해행위 주체 및 유형별, 민사 구제수단별로 법원이 고려하는 영업비밀 관리 조치가 내용적으로나 빈도상으로 어떤 차이를 보이는지를 살펴볼 수 있었다. 또한 부정경쟁방지법 제18조 제1항 및 제2항 유죄 판결의 양형과 제19조 양벌규정 적용 현황을 연도별로 정리할 수 있었다.

그 외에도 분쟁의 대상이 되는 정보의 유형, 기업의 규모와 업종별로 법원이 고려하는 영업비밀 보호 조치가 빈도 상으로 어떤 의미를 보이는지를 살펴보았다. 비록 확연하게 눈에 띄는 데이터를 확인하지는 못했지만, 형사 사건에서 검사는 경영정보 보다 기술정보를 훨씬 더 의미 있게 바라보아 소추를 하는 경향이 있다는 점, 민·형사를 불문하고 서약서 등 영업비밀 보호 약정은 비밀관리 조치를 판단함에 있어 아주 기본적인 사항이라는 점 등을 확인할 수 있었다.

나아가 지난 수년 간 영업비밀 침해행위에 대한 양형에 거의 변화가 없어 처벌 수위는 여전히 낮은 것으로 나타났다.

다만 본 연구에서는 2019. 7. 9. 시행된 개정법에 따른 비밀관리성 요건을 적용한 판결이 많이 발견되지 않은 관계로, 개정법 시행 후 법원에서 비밀관리성을 인정하는 비율이 높아지고 있는지 여부까지는 확인할 수 없었다. 향후 판례 동향을 지속적으로 추적함으로써 법률 개정으로 비밀관리성 요건이 완화된 것과의 관련성을 관찰하여야 할 것이다.

또한 2019. 7. 9. 시행된 개정법에 따라 강화된 벌칙 조항이 적용되어 양형이 상향되었다고 볼 만한 의미 있는 판결도 발견되지 않았는바 마찬가지로 판결 동향에 대한 추적 관찰이 필요하다.

한편 이번 조사에서 법원이 비대면 디지털 근무환경을 감안하여 비밀관리성의 성립 여부를 판단한 판결은 발견되지 않았다. 그러나 이번 조사 결과 회사 외부에서 원격 근무를 하는 과정에 비밀 유출이 일어난 사건들을 다수 발견할 수

20) (2019. 7. 9. 시행) 합리적인 노력에 의하여 비밀로 유지된 → 비밀로 관리된

있었다. 재택근무를 하면서 회사 서버에 접속하여 영업비밀 파일을 다운로드 받거나, 회사 영업비밀을 개인 클라우드에 업로드 하거나 사진으로 촬영하여 클라우드 서비스에 업로드 하는 방식으로 유출하는 등 클라우드컴퓨팅을 이용하는 사례가 다수 확인되었다.

아직 비대면 디지털 근무환경이 직접적인 쟁점으로 부각된 사례는 없지만, 다음 장에서 소개할 미국과 일본, 유럽의 비대면 근무환경에서의 영업비밀 유출 사건·판례 및 방지 대책과 더불어 이번 조사에서 발견한 판결들을 통해, 팬데믹 이후 보편화된 비대면 근무환경과 관계된 영업비밀 비밀관리 조치 요소에 관한 법원 판단을 예측하고 대비하는 데 도움이 될 것으로 기대한다.

Ⅲ. 비대면 근무환경에서의 영업비밀 보호 최신동향

1. 미국, 일본의 비대면 근무환경에서의 영업비밀 유출 사건·판례 및 방지 대책
2. 유럽의 비대면 근무환경에서의 영업비밀 유출 사건·판례 및 방지 대책
3. 비대면 근무환경에서 영업비밀 보호를 위한 동향 및 정책

Ⅲ. 비대면 근무환경에서의 영업비밀 보호 최신동향

1. 미국, 일본의 비대면 근무환경에서의 영업비밀 유출 사건·판례 및 방지 대책

가. 서설

2020년 3월 세계보건기구(WHO)가 감염병의 세계적 유행을 뜻하는 팬데믹을 선언한 가운데, 이는 기업으로 하여금 비대면 디지털 기반 근무로의 환경변화를 가속화시켰다. 물론 2020년 이전에도 비대면 디지털 기반 근무가 존재하지 않은 것은 아니다. 다만 종래의 비대면 디지털 기반 근무의 도입·활용은 업무의 효율화나 근로방식 개혁 등을 목적으로 일부 기업과 '일부' 피용자가 이용하는 근무 형태로서 예외적인 선택지 중 하나에 머물러 있었을 뿐이었다. 그러나 2020년 이후를 기점으로 비대면 디지털 근무는 감염증 대응을 계기로 피용자가 일제히 장기간에 걸쳐 이용하고 있는 상황이어서 현재의 디지털 기반 근무는 과거와는 차이가 있다. 즉 현재의 디지털 기반 근무는 대기업뿐만 아니라 소규모 회사에까지 두루 실시하는 표준적·일반적인 업무·근무형태 중 하나가 되어가고 있다. 특히 미국은 COVID-19 전파 차단을 위해 약 42개 주에서 3억 1천 6백만 명 이상의 주민들이 집에 머물도록 하는 등 고강도 정책을 실시하였다.[21] 이로 인해 미국 내 거의 모든 회사가 재택근무(work from home, 'WFH')를 실시하는 등 비대면 방식으로의 시스템 전환을 실시하였다. 이에 따라 미국 노동력의 42%가 가정에서 일하고 있을 정도로 비대면 근무가 일상화되었고,[22] 그러는 사이 사이버 범죄가 300% 증가했다는 발표가 있었다.[23] 이와 같은 결과는 우리나라의 경우도 크게 다르지 않다.24) 그 이유는 비대면 디지털 기반 근무에 대한 충분한 사전준비 없이 사무실에서의 업무가 개인 가정으로 옮겨졌고, 이에 따라 상대적으로 공격에 취약한 가정용 네트워크가 해커들의 표적이 되었다는 점과 최소한의 감독만으로 느슨하게 이루어진 근무 환경으로 인한 피용자의 과실, 즉 부주의를 그 이유로 꼽고 있다. 이처럼 오늘날 비대면 디지털 기반 근무로의 전환은 대세적 흐름으로 자리하게 되었고, 이로 인하여 기업은 기술 및 경영상 정보인 영업비밀(confidential information and trade secrets)유출 등 사고 예방과 수습에 집중할 수밖에 없는 비상 상황에 직면한 것이다.

21) Sarah Mervosh, 'See Which States and Cities Have Told Residents to Stay at Home'. (New York Times, 7 April, 2020)https://www.nytimes.com/interactive/2020/us/coronavirus-stay-at-home-order.htmlAccessed on Nov. 22, 2022.
22) Stanford News, Stanford research provides a snapshot of a new working- from-home economy, <https://news.stanford.edu/2020/06/29/snapshot-new-working -home-economy/>.(last visited Nov. 22, 2022).
23) Jenna Walter, COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes, IMC Grupo, <https://www.imcgrupo.com/covid-19-news-fbi-reports -300-increase-in-reported-cybercrimes/>,(last visited Nov. 22, 2022).
24) 서울경제, "코로나 악용 해킹시도 폭증", <https://www.sedaily.com/NewsView/ 1Z59WJ20'O>,(last visited Sep. 26, 2020). ; ChosunBiz, "코로나 악용 메시지 이용 해킹 96% 증가", <https://biz.chosun.com/site/data/html_dir/2020/07/12/2020071200224.html?utm_source=naver&utm_medium=original&utm_campaign=biz>.(last visited Nov. 22, 2022).

그런데 비대면 디지털 기반 근무와 영업비밀은 구체적으로 무슨 관련이 있는 것일까? 앞서 잠깐 언급한 비대면 디지털 기반 근무와 사이버 범죄와의 연관성을 생각해 보면 해답을 찾을 수 있다. 사실 제품 또는 서비스의 기술적 측면에서 가격구조, 시장 분석, 비즈니스 전략 및 고객 목록에 이르기까지 광범위한 정보가 보호 대상이 될 수 있는 기업의 영업비밀은 지적재산에서 중요한 부분을 차지한다. 그런데 영업비밀이 비밀로서 보호받기 위해서는 법적 요건, 즉 비밀을 유지하여 경쟁사에 일반적으로 알려지지 않은 정보로 경제적(상업적)가치가 있는 것이어야 하는데, 비대면 근무환경으로 인해 영업비밀이 유출될 가능성이 높아진 것이다. 아래에서는 미국과 일본을 중심으로 비대면 근무환경과 관련한 미국과 일본의 법원 판단 등 기업의 영업비밀 침해 사례 및 방지대책(예방법)에 대해 살펴보기로 한다.

나. 비대면 근무환경에서의 영업비밀 유출 사례

(1) 미국

우리나라를 비롯한 대부분의 국가는 Facebook, Skype, Zoom, Microsoft Teams, Line 등 다양한 온라인 회의 플랫폼 기기로 눈을 돌리며 '비대면 디지털 기반 근무'(이하, '원격근무')[25]로의 전환하였는데, 이 역시 영업비밀보호법의 통제를 받고 있다. 미국의 경우 연방법과 주법 2가지 범주에서 보호되는데, 우선 영업비밀 관련 연방법은 컴퓨터 사기 및 남용법(Computer Fraud and Abuse Act, 18 U.S.C § 1030), 경제간첩법(Economic Espionage Act, 18 U.S.C § 1031) 그리고 2016년 오바마 행정부에서 제정된 연방 영업비밀보호법(DTSA, Defend Trade Secret Act, 18 U.S.C § 1036)이 있다. 그리고 주법으로는 뉴욕주를 제외한 49개주에서 채택한 통일영업비밀보호법(Uniform Trade Secret Act)이 있다. 아울러 그 외에 각 주에서 독자적으로 제정한 법령들이 추가적으로 적용된다.

여기서 DTSA에 따르면, 영업비밀은 "유/무형 여부와 상관없이 패턴(patterns), 계획(plans), 편집(compilations), 프로그램 장치(program devices), 공식(formulas), 설계(designs), 프로토타입(prototypes), 방법(methods), 프로세스, 절차(procedures), 프로그램 또는 코드(programs, or codes)를 포함한 재무(financial), 비즈니스(business), 과학(scientific), 기술(technical), 경제 또는 엔지니어링 정보(economic, or engineering information)의 모든 형식 및 유형, 물리적 저장, 컴파일 또는 기억 방법으로 (A) 해당 정보의 보유자가 해당 정보를 비밀로 유지하기 위한 합리적인 조치(reasonable measures)를 취한 경우, 그리고 (B) 정보가 일반적으로 알려져 있지 않거나 적절한 수단을 통해 쉽게 확인할 수 없는 다른 사람으로부터 실제 또는 잠재적 독립적인 경제적 가치를 얻을 수 있는 것으로 정의하고 있다. 이러한 정의는 통일영업비밀법을 모델로 한 수많은 주 법령에 의해 성문화되었으며 2016년 U.S.C. 1839(3)에 따라 연방 차원에서 채택되었다. 이처럼 미국의 경우 주마다 영업비밀보호법이 조금씩 다르지만, 모든 주에서는 영업비밀 보유자가 해당 정보의 비밀성을 보장하기 위해 "합리적인 조치"를 취할 것을 요구한다.[26]

25) 비대면 디지털 기반 근무란, 정보통신기술(ICT: Information and Communication Technology)을 활용하여 장소나 시간을 효율적으로 활용할 수 있는 유연한 근무 방식을 말한다. 비대면 디지털 기반 근무의 형태는 업무를 수행하는 장소에 따라 '재택근무'(집에서 일하는 방식), '위성 오피스 근무'(자택 근처나 통근 도중의 장소 등에 설치된 새틀라이트 오피스(메인 오피스 이외에 설치된 공유 오프스 등 오피스 쉐어 코워킹 스페이스를 포함)에서 일하는 방식), '모바일 근무'(노트북 등을 활용하여 임기응변으로 선택한 장소에서 일하는 방식)로 분류된다.

26) Accordingly, to qualify as a 'trade secret,' information must both derive independent economic value from not being generally known or readily ascertainable and be subject to reasonable efforts to maintain its secrecy. Beard Research, Inc. v. Kates, 8 A.3d 573, 589 (Del. Ch.), ASDI, Inc. v. Beard Research, Inc., 11 A.3d 749 (Del. 2010).

이에 과거 미국에서 발생한 고전적인 영업비밀 사건을 소개하면 아래와 같다.

customer or pricing lists (Cytodyne Techs., Inc. v. Biogenic Techs., Inc., 216 F.R.D. 553 (M.D. Fla. 2003))

proprietary software (telSPACE, LLC v. Coast to Coast Cellular, Inc., No. 2:13-CV01477 RSM, 2014 WL 4364851 (W.D. Wash. Sept. 3, 2014))

unique formulas or products (Del Monte Fresh Produce Co. v. Dole Food Co., Inc., 136 F. Supp. 2d 1271 (S.D. Fla. 2001))

specially developed processes and custom machinery (Premier Lab Supply, Inc. v. Chemplex Indus., Inc., 10 So. 3d 202 (Fla. 4th Dist. Ct. App. 2009))

한편, 연방 영업비밀보호법 및 대부분 주에서의 영업비밀 법령은 어떠한 일정 기준이 충족될 경우 사용자가 명령적 및 금전적 구제(injunctive and monetary relief)를 요구할 수 있도록 허용한다. 그런데 위에서 말한 '일정 기준'이란 기업이 민감 정보를 보호하기 위해 "합리적인 조치"를 취했다는 것을 의미한다. 즉 법이 정한 기준에 따라 영업비밀로서 보호받을 요건을 갖추기 위해서는 "합리적인 조치(reasonable measures)"를 취했음을 입증하여야 한다. 그런데 합리적인 조치는 본질적으로 주관적이기 때문에 비밀로서 유지하기 위해 합리적인 조치를 취했는지 여부를 입증하거나 반증하는 것은 영업비밀 소송에서 복잡한 문제이며, 이는 당사자들이 소송에서 승소하기 위해 반드시 넘어야 할 산이라고 할 수 있다. 어떤 경우가 합리적인 것으로 간주되는 것인지는 지리적 위치, 시대, 산업 구조 등에 따라 바뀔 수 있다. 예를 들어 어떤 기업이 20년 전 영업비밀을 비밀로 관리한 경우 그 당시 기술 수준으로 오늘날의 영업비밀을 관리하였을 경우 합리적 조치를 인정받을 수 있을까? 현재의 기준으로 보면 그때의 그 보호조치는 상당히 구식이어서 효과적이지 않을 수 있고, 따라서 당시에는 합리적인 조치로 볼 수 있었어도 지금은 그렇게 간주되지 않을 수 있다. 합리적 조치에 대한 기준은 가변적이어서 실제 사례별로 다시 검토되어야 하지만, 그 간 축적된 판례는 우리에게 어떤 조치가 "합리적 조치"인지에 대해 판단할 수 있는 기준을 제시해준다고 할 수 있다. 아래에서 살펴볼 판결이 그러한데, 팬데믹 이전과 이후 원격근무와 관련한 영업비밀 침해 사건은 어떤 유형의 것이 있었는지 살펴보기로 하자.

1) 팬데믹 이전 '비대면 근무환경'에서의 영업비밀 사건

가) Computer Associates International v. Quest Software, Inc.[27]

i) 사실관계

1996년 소외회사 Platinum Technology International, Inc.(이하, 'Platinum')는 소프트웨어 프로그램 Enterprise Database Administrator(EDBA)의 첫 번째 버전을 출시했다. 당시 이 사건 피고들[Quest Software Inc.(Quest), Michael J. Friel, Debra A. Jenson, Robert M. Mackowiak, Elizabeth W. Wahlgren 및 Frank L. Bisotti, 이하 피고들]은 Platinum의 EDBA 개발 연구소 관리자, 개발팀의 책임자 등으로 근무하였다. 데이터베이스 관리자는 Platinum

27) 333 F.Supp.2d 688 United States District Court, N.D. Illinois, Eastern Division.

의 프로그램을 통해 이전에 많은 시간이 소요되었던 수많은 공정을 자동화할 수 있었다. 그러던 1999년 봄 소프트웨어 제조업체인 Computer Associates International, Inc.(CA)(이하 '원고')는 Platinum을 인수하였는데, 이 무렵 피고 Wahlgren을 비롯한 많은 피용자가 해고되었고, 다른 피고들 4명 역시 회사를 떠나기로 결정했다. 피고들은 해고/퇴사 후 원고와 경쟁회사인 Quest Software, Inc.(이하, 피고회사)로 이직하였는데, 피고회사는 피고들이 Platinum에서 수행한 작업과 거의 동일한 작업에 근무하도록 했다. 이에 원고는 2002년 7월 피고가 EDBA 소스 코드 사본을 피고회사로 가져가 원고의 영업비밀을 침해했다고 주장하며 피고를 상대로 금지명령을 구하는 영업비밀 침해 소송을 제기했다.

ii) **법원 판단**

일리노이주 영업비밀보호법(The Illinois Trade Secrets Act, ITSA)은 "영업비밀 침해가 실제적 또는 위협적(actual or threatened)"인 경우 법원으로 하여금 금지 명령을 내릴 수 있도록 허용한다.[28] 따라서 원고는 승소하기 위해 (1) 소스코드가 ITSA에 따라 보호할 수 있는 영업비밀이며, (2) 피고가 비즈니스 과정에서 소스코드를 사용했을 가능성이 높다는 점을 입증해야 한다.

한편 위 사건을 심리한 일리노이 법원은 영업비밀 여부를 판단할 때 다음과 같은 6가지 지침을 고려하였다.

(1) 해당 정보가 사업 외부에 알려진 범위
(2) 해당 정보가 기업 내의 피용자 및 기타 사람들에게 알려진 정도
(3) 해당 정보를 보호하기 위해 취한 조치
(4) 경쟁자에 대한 정보의 가치
(5) 정보 개발에 소요된 시간, 비용 및 노력의 양
(6) 다른 사람들이 쉽게 정보를 얻을 수 있었는지 여부

위 지침을 고려하여 법원은 원고가 원격근무를 위해 시행한 정책이 영업비밀을 보호하기 위한 "합리적인 조치"와 일치한다고 그 이유를 밝히며 아래와 같이 적시하였다.

비록 피고들이 원고의 정책에 따라 원격근무를 하였고, 형식적으로 특별한 부담감 없이 서약서에 서명하였을 뿐이었다는 항변을 했지만,

(1) 피고들은 서약서 등 매뉴얼에 명시된 비밀 정책의 대상
(2) 원고는 피고들에게 퇴사 시 비밀유지 의무를 상기시킴
(3) 원고의 주요 시설에 대한 접근은 키(Key) 카드 사용에 의해 제한
(4) 영업비밀로 추정되는 영업상 정보는 일반 대중이 결코 이용할 수 없었음
(5) 피고들은 비밀유지 조치를 알고 있거나 인식할 수 있었음

이라며 피고의 항변을 받아들이지 않았다.

한편 증거에 따르면, 원고는 정보가 외부인의 손에 들어가지 않도록 보호 조치를 취했음을 보여주었고, 기밀 유지 정

28) PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1267 (7th Cir.1995).

책은 서약서에 명시되어 있었다. 이러한 정책은 외부인이 소스 코드에 접근하는 것을 방지하고 회사 내 코드에 대한 접근도 제한했다. 또한 원고는 직원들로 하여금 회사를 떠날 때 이러한 의무를 상기시켰는데, 원고의 Oak Brook 시설에 대한 접근은 보안 카드가 있는 직원으로 제한되었다. 아울러 소스 코드는 프로그램과 함께 배포되거나 일반 대중에게 공개되지 않았고, 이러한 절차는 소스 코드를 비밀로 유지하기 위한 합리적 노력으로 보는 것이 타당하다. 나아가 포렌식 분석에 따르면 피고는 EDBA 코드 사용을 은폐하기 위해 컴퓨터에서 파일을 지우려고 시도했는데, 이러한 피고의 행동은 영업비밀 침해의 증거가 될 수 있다.

iii) 생각해 볼 사항

이 사건에서 피고들은 원고회사에서 원격근무 형태로 근무하였던 바, 이는 비밀을 관리해야 하는 원고회사 입장에서 영업비밀 관리 측면에서 분명 분리한 점이었다. 원고회사에 원격근무 수칙이 있었는지, 있었다면 어느 정도 수준이었는지 등 이로 인해 피고가 원격근무 중 회사 정보를 어떻게 취급하였는지 여부에 따라 법적 요건으로부터 멀어 질 수 있으므로 원격근무가 원고에게 약점으로 작용할 수 있었다. 그러나 법원은 ITSA 하에서 영업비밀보호는 완벽(perfection)이 아닌 합리적인(reasonable) 수준으로의 합리적 조치를 요구하므로 원고의 EDBA 소스 코드에는 ITSA에 따라 보호할 수 있는 영업비밀이 포함되어 있다고 판단하였다(즉, 합리적 조치가 이루어진 것). 실제 이 사건에서 법원은 원고회사가 원격근무 시 어떠한 수준으로 피고들에게 비밀 준수 의무를 부과했는지 등에 대해 구체적으로 판단을 하지 않은 것으로 보인다. 이에 피고는 이 점을 공격 포인트로 삼아 허술한 원고의 원격근무 조치로 비밀관리에 대한 합리적 조치가 이루어지지 않은 점을 적극 주장한 것으로 보인다. 앞서 어떤 경우가 영업비밀보호를 위한 합리적인 조치인 것인지는 지리적 위치, 시대, 산업 구조 등에 따라 가변적일 수 있다고 언급한바 있다. 이 사건은 지금으로부터 20년 전의 사건이다. 따라서 이 사건이 팬데믹 이후인 오늘날의 기술수준에서 발생하였다면 이와 동일한 판단이 나왔을지 의문이 든다. 그 이유는 현재의 기술기준으로 보면 당시의 기술적 보호조치는 상당히 구식이어서 비밀보호에 효과적이지 않을 수 있고, 그 결과 당시 원고가 취한 보호조치는 합리적인 수준으로 볼 수 없을 가능성이 있기 때문이다.

나) API Americas Inc. v. Miller

i) 사실관계

API Americas(이하, '원고')는 핫 스탬핑 호일(hot stamping foils) 및 기타 제품을 설계, 제조, 유통하는 회사로 미국 전역에 고객을 확보하고 있다. 한편 Miller(이하, '피고')는 캔자스주 존슨 카운티(Johnson County, Kansas)에 거주하는 개인으로 원고 회사에서 2007년 6월 고객 서비스 담당자로 일하기 시작하면서 원고 제품 공식/레시피, 가격 책정, 품질 관리를 포함하는 중요한 기밀정보 및 영업비밀(고객과의 비즈니스에 관한 정보와 지식)을 얻게 되었다. 이후 피고는 고객 서비스 관리자로 승진한 후 기술 서비스 및 계정 관리자로 근무하였고, 2011년 7월 6일 원고와 기밀(Confidentiality), 유인 및 경쟁행위 금지계약(Non-Solicitation and Non-Competition Agreement)을 체결하고, 2016년 3분기부터 원고의 주 고객사인 Hallmark의 계정 관리자로 일했다. 그러던 2017년 9월 피고는 원고 회사에서 퇴사하였고, 원고회사를 떠나기 전 원고의 영업비밀 및 기타 독점 정보를 다운로드하여 자신의 개인 이메일 계정으로 전송하여 정보를 유출했다. 현재 피고는 원고의 경쟁사인 UNIVACCO Foils Corporation 중서부 영업 관리자로서 과거 원고에서 근무했던 동일한 영역에서 일하고 있다.

ii) 법원판단

이 사건에서 캔자스 주(District of Kansas) 법원은 원고가 피고와 비밀유지협약(confidentiality agreement) 및 비경쟁 계약(noncompete agreement)을 체결했기 때문에 피고로 하여금 원격으로 근무하도록 허용하는 것은 영업비밀 보호를 위한 "합리적인 조치(reasonable measures)"였다고 판결하였다.[29] 그러면서 법원은 피고가 원고로부터 가지고 나온 것으로 의심되는 영업비밀의 반환과 함께 사용을 금지하고, 원고 고객 특히 소외 Hallmark Cards Incorporated와의 연락을 금지하는 제한조치를 명령하였다.

iii) 생각해 볼 사항

이 사건에서 원고는 "원고의 비지니스는 자체적으로 보유한 고유기술, 제조 프로세스, 마케팅 전략, 고객 및 잠재 고객 관계, 비즈니스 모델 및 전략에 달려 있다"고 주장하면서 피고가 원고의 귀중한 정보와 지식을 사용하여 원고와 비지니스 경쟁을 한다면 원고에게 심각하고 돌이킬 수 없는 피해가 발생할 것이라고 주장했다. 물론 이 사건 역시 팬데믹 이전의 사건으로 원격근무가 주요 쟁점은 아니었고, 따라서 원격근무에 대한 구체적인 판단을 하지 않았다. 다만 법원은 피고가 원고와의 계약에 따라 원격근무를 하였고, 원격 근무자인 피고가 자신의 개인 이메일 계정으로 빈번하게 원고가 관리하고 있는 영업비밀을 전송했음을 인정하면서 피고의 원격근무로 인하여 발생할 수 있는 사항들과 연계한 비밀관리성에 대한 합리적인 조치에 의문을 제기하지 않았다. 위에서 살펴본 Computer Associates International v. Quest Software, Inc.과 마찬가지로 원격근무 과정에서 발생할 수 있는 다양한 쟁점에 대해 살펴보았다면 어떠한 판단이 나왔을지 의문이 든다고 할 수 있다.

2) 팬데믹 이후 비대면 근무환경에서의 영업비밀 사건

가) Smash Franchise Partners, LLC v. Kanda Holdings, Inc.

i) 도입

2020년 8월 델라웨어 법원(Court of Chancery of Delaware) 판결은 인터넷을 통해 교환되는 정보를 보호하기 위해 사용 가능한 모든 보안 기능을 활용하지 못할 경우 기업은 영업비밀보호에 있어 위험에 빠질 수 있음을 강조하였다. 2020년 8월 13일 델라웨어 법원의 Smash Franchise Partners, LLC v. Kanda Holdings, Inc. 사건은 원고가 해당 플랫폼에서 적용 가능한 보안 기능을 적절히 활용하지 않았기 때문에 웹 기반 화상 회의 플랫폼 줌(Zoom)에서 논의하며 오고간 정보에 대해 영업비밀로서 보호되지 않는다고 결정했다. 즉 법원은 영업비밀 보유자인 원고가 줌 개인정보보호 및 보안 기능을 통합하지 못하고 공개 줌 통화에서 기밀 및 독점 사업 전략을 공개함으로 인해 영업비밀을 보호하기 위한 합리적인 조치를 취하지 않았다고 판결했다.

ii) 사실관계

Smash Franchise Partners(이하, '원고')는 고객이 현장에서 쓰레기를 압축해 폐기물 관리 및 처리에 들어가는 비

29) 380 F. Supp. 3d 1141, 1149 (D. Kan. 2019).

용을 절약할 수 있는 '모바일 쓰레기 압축기(mobile trash compactors)' 기술(이하 '이 사건 기술')을 보유하고 있는 가맹본부(franchisor)이다. 이 장치는 트럭의 침대에 장착되며 운전실과 롤러 암에 부착된 톱니 모양의 무게가 있는 드럼으로 구성되는데, 운전자는 운전실에서 롤러 암을 제어하고 이를 사용하여 드럼을 쓰레기 수거통으로 내리며, 그런 다음 운전자는 쓰레기통을 가로질러 드럼을 이동하여 압축하는 기능을 갖고 있다. 원고는 전술한 기술로 2019년 4월에 첫 번째 가맹사업을 체결했고, 해당 가맹사업자는 2019년 10월에 운영을 시작하였다. 원고는 자사의 압축기와 비즈니스 모델을 지역의 가맹사업자(franchisees)에게 판매하기로 하였는데, 다만 가망 예비 가맹사업자(prospective franchisees)는 상품과 사업모델을 소개받기 전에 비공개계약서(non-disclosure agreement, NDA)를 체결해야 했다.

이에 따라 이 사업에 관심을 보인 Kanda Holdings, Inc.(이하 '피고')는 2019년 12월 NDA에 서명하고 사업 수행비용, 사업 전략 및 대상 고객에 대한 웹 기반 화상 회의 애플리케이션인 Zoom의 Founder Call에 참여했다. Zoom에는 액세스를 위해 비밀번호를 요구하고 호스트가 신원 확인 후 개별적으로 허용할 수 있도록 참가자를 대기실에 배치하는 등 호스트가 회의에 참여하는 사람을 제어하는 데 사용할 수 있는 기능이 있지만, 원고의 Zoom 회의는 이러한 기능을 사용하지 않았다. 다시 말해 원고가 개최한 회의는 회의 ID가 있는 모든 사람에게 열려 있었다. 원고의 후속 미팅은 모두 동일한 회의 ID를 사용했으며 암호가 필요하거나 대기실(waiting room)을 사용하는 미팅은 없었다. 원고는 비즈니스 모델의 일환으로 기업가들에게 가맹계약을 체결하도록 홍보하여 다양한 지역에서 콤팩트화 하는 작업을 수행하였다. 이에 다양한 기업들이 NDA를 체결한 후, 가맹사업 체결을 원하는 가망고객들로 하여금 줌(Zoom)을 통해 매주 "파운더스 콜(Founders Calls)[30]"에 참여하도록 초대했고, 여기서 원고회사 대표는 자사에서 비밀로 유지되고 있는 사업계획을 포함하여 고객목록에 대한 정보를 제공했다. 피고는 10시간가량 원고가 주최한 줌 미팅에 참여하였다.

그런데 피고는 궁극적으로는 향후 원고와 경쟁관계에 있는 이 사건 기술 회사를 설립할 목적으로 원고 가맹사업에 관심이 있는 척하며 원고에게 접근하여 중요정보의 수집을 시도한 것이었다. 결국 피고는 원고와 가맹사업 계약을 체결하기보다는 그와 동일한 아이템으로 경쟁 사업을 하기로 마음먹고 원고 사업과 동일한 사업을 공개적으로 시작하였다. 이에 원고는 피고를 상대로 NDA에 따른 계약 위반과 영업비밀 침해를 이유로 하는 예비 금지명령 신청을 하였다.

iii) **법원판단**

우선 예비명령(preliminary injunction)의 인용을 이끌어내기 위해서는 원고가 회사의 기밀이라고 주장하는 정보가 무엇인지 살펴보아야 했는데, 공개한 정보는 아래와 같은 내용의 것들이었다.

- 품목별 가맹사업에 필요한 초기 투자
- 가맹사업 재무성과에 대한 광범위한 내용
- 원고사업 장비 제조의 정체성

30) 예비 가맹사업자는 두 가지 유형의 화상 회의에 참여할 수 있다. 첫 번째로 "Franchisee Forum Call" 또는 "Validation Call"이라고 하는 한 가지 유형은 매주 목요일에 진행되었으며 현재 가맹점이 진행하며 프랜차이즈 운영 방법을 설명하고 비즈니스에 대한 질문에 답변한다. 두 번째로 "Founder Call"이라고 하는 다른 유형의 전화는 매주 수요일에 진행되었으며 회사의 역사와 전망에 대해 이야기하고 질문에 답변한다. 이 과정이 끝나면 예비 가맹사업자가 가맹점 계약을 신청할 수 있고, Smash가 신청서를 승인하면 예비 가맹사업자와 Smash는 가맹계약에 서명한다.

- 인구에 따른 원고 가맹사업 영역의 추정 크기
- 서비스를 제공하기 위해 가맹사업자가 구매해야 하는 트럭의 수
- 수행한 사업 규모에 따라 가맹사업자가가 구매해야 하는 트럭의 수
- 원고 가맹사업자 수

이에 델라웨어 법원은 공개 줌 통화에서 피고가 빼돌린 것으로 알려진 영업비밀이 공개됐다는 점을 강조한 뒤 원고가 영업비밀을 비밀로서 보호하기 위한 합리적인 조치를 취하지 않았다는 이유로 영업비밀 예비명령 가처분 신청을 기각하였다. 여기서 법원이 말한 합리적인 조치란 원고가 플랫폼에서 사용할 수 있는 보안 기능을 사용하지 아니하여 줌 통화 중에 전술한 바와 같이 논의된 정보에 대해 영업비밀보호를 주장할 수 없음을 언급한 것으로, 구체적으로 법원은 ① 원고는 자신의 가맹사업 계약에만 열을 올린 나머지 줌 미팅 코드를 변경하지 않은 채 당사자들에게 줌에 접속하기 위한 정보를 자유롭게 제공했다는 점, ② 회의 접근 코드 외에도 비밀번호를 부여하지 않았다는 점, ③ 호스트가 미팅 참석자를 허락할 때까지 배제하는 줌 "대기실(waiting room)" 기능을 사용하지 아니하였다는 점, ④ 호스트가 각 회의에 참석하고 소속되지 않은 사람들을 제거하도록 요구하는 자체 절차를 따르지 않았다는 점 등을 지적했다.

이처럼 앞서 논의된 바와 같이 원고가 영업비밀이라고 주장하는 중요정보의 대부분은 공개 문서에서 공개적으로 사용할 수 있도록 했으며, 프레젠테이션 자료, 소개 전화, Unit Economics Call 및 Unit Economics Worksheet에서 무료로 사용할 수 있도록 함으로써 영업비밀의 비밀관리성 내지는 비공지성을 상실하여 더 이상 비밀이 아니었다. 따라서 공개회의에서 공유된 정보를 보호하지 못한 것은 영업비밀보호법에 따라 요구되는 합리적인 조치를 취하지 못한 것이다. 결국 법원은 비록 피고가 줌 파운더 콜에 참여함으로써 부정직하고 부당한 행동을 했다고 언급하면서도 위와 같은 여러 이유를 설시하며 원고의 피고에 대한 예비명령 신청을 기각하였다.

iv) 시사점

델라웨어 영업비밀보호법의 '합리적 (보호)조치'는 2016년 발효된 연방 영업비밀보호법과 크게 다르지 않다. 앞으로 팬데믹 상황이 아니더라도 원격근무는 새로운 근무형태로 계속 이어질 것으로 예측된다. 이런 상황에서 줌과 같은 소셜미디어 애플리케이션은 원격 작업 환경에서 아이디어와 비즈니스 정보를 원활하고 즉각적으로 전송하는 데 있어 매우 중요한 것으로 평가받는다. 그런 만큼 영업비밀 보유자는 많은 주의가 필요하다. 분명 피고의 행동이 이중적이고 사악한 것이라는 점에는 의심의 여지가 없을 것이다. 그러나 델라웨어 법원은 원격 작업에 사용할 수 있는 보안 조치를 구현하지 않고서는 원활한 기업 활동을 할 수 없음을 기업들에게 경고하는 메시지를 주었다고 할 것이다.

아울러 이 사건을 통하여 원격근무의 편리성 등 오늘날 새로운 형태의 비즈니스 동향을 이해할 수 있다.

v) 영업비밀 유출 방지 대책(예방책)

이 사건이 주는 교훈을 통해 향후 기업들은 아래와 같은 방지 대책(예방법)의 시행으로 원격근무로 인한 영업비밀 침해의 위험에 대비할 수 있을 것이다.

첫째, 줌 호스트는 허가받지 않은 참가자의 참여를 막기 위해 암호를 요구하는 비공개 회의를 개최하여야 한다. 그러

나 이 사건에서 원고는 줌 미팅에 참석하지 말았어야 할 사람들을 분류하고 차단하여야 할 작업을 하지 않았다. 따라서 사용자는 줌과 다른 도구의 사용이 영업비밀 보호의 손실을 초래하지 않도록 보안 조치를 취해야 한다. 기업은 부득이 줌 회의를 개최해야 하는 경우 비밀번호로 보호된 회의 링크를 허용하는 보안 기능을 사용해야 하며, 무단 참석자 제거 등의 다른 절차도 시행해야 한다.

- 원치 않는 "Zoomboming"[31] 이나 불쾌한 자료의 공유를 방지하기 위해 호스트 전용 도구 개발
- 줌 미팅에 참석하는 참가자들의 발언을 보호하기 위해 자동 음소거 기능을 사용
- 파일공유 비활성화 작업으로 악성파일이 전송되지 않도록 설정
- "far-end camera"[32] 제어를 사용 불가능으로 설정하여 참가자가 자신의 카메라 이외의 카메라를 제어할 수 없도록 함
- 스트리밍 프레젠테이션을 위해 등록이 필요하며, 가능하다면 참가자 전원에게 미팅 시작 시 청중에게 자신을 소개하도록 요청

둘째, Zoom, Teams 또는 기타 화상 회의 시스템에서 제공하는 보안 기능을 활용하는 것 외에도, 기업은 원격 작업을 위해 쉽게 사용할 수 있는 다른 보안 기능을 활용하도록 보장해야 한다. 예를 들어 VPN과 같은 안전한 암호화된 네트워크에 대한 민감한 정보의 교환을 제한하고 이중 인증 방법을 사용할 수 있다. 협업 플랫폼은 정기적으로 업데이트하여 새로운 보안 기능이 모두 갖춰지도록 해야 하며, 직원들은 회사에서 검증하고 승인한 플랫폼만 사용하도록 제한해야 한다. 영업비밀은 기밀 정보에 액세스한 사람을 식별하기 위한 액세스 로그와 함께 액세스가 합법적으로 필요한 사람에게만 공개되어야 한다.

- 사용자는 전사적으로 사용할 수 있는 가장 높은 보안 조치를 구현하여야 함
- 피용자에게 보안 조치를 구현하도록 지시, 예를 들어 가능한 한 개인실(private room)을 사용하도록 권고하고, 개인 공간을 찾을 수 없다면 헤드폰을 사용하고 화면 시야를 제한해야 함
- 피용자에게 특정 플랫폼을 회사 업무에 사용해야 한다는 회사의 요구 사항을 정기적으로 상기시키고, 의무 플랫폼 사용이 중요한 이유를 설명
- 피용자가 사내 업무에 복귀하기 시작하면 영업비밀과 관련된 논의 중 기록한 모든 메모를 사무실 파일에 보관하거나 전문적인 파쇄를 위해 가져오도록 지시

마지막으로, 전직 피용자나 전직 비즈니스 협력자와 같이 더 이상 기밀 정보를 볼 수 없어야 하는 사람들이 후속 접근(접속)을 할 수 없도록 차단해야 한다.

31) 줌부밍(Zoomboming)이란? 온라인 강의 또는 미팅 룸 진행시 불특정 인원이 난입하여 이용행위를 방해하는 것을 말한다. 따라서 온라인상에 공개된 SNS 또는 게시글에 Zoom 초대링크를 공개하는 것은 매우 위험하므로 초대링크를 공유할 때는 발송자의 신원을 꼭 확인하거나 비공개 SNS 게시글 형태로 공개하여야 한다.

32) 파 엔드 카메라(far-end camera)이란? 원격 카메라 제어를 통해 다른 미팅 참여자로 하여금 본인 카메라를 제어하도록 허용하고, 카메라의 pan-tilt-zoom(PTZ) 기능을 사용하는 것을 말한다. 이 기능이 작동하려면 웹캠에 이러한 PTZ 기능이 있어야 한다. 이 기능은 화상 회의 미팅 또는 프리젠테이션으로 다른 참가자로부터 원격 도움말을 받는 데 유용하다.

나) M3 USA Corporation v. Karie Hart, et al[33]

i) 도입

이 사건은 연방 영업비밀보호법(Defend Trade Secrets Act of 2016) 위반, 펜실베니아 통일영업비밀보호법(Pennsylvania Uniform Trade Secret Act) 위반, 불공정 경쟁, 충실의무 및 비밀유지 위반으로 인한 민사상 부당이득 청구 등 다양한 쟁점이 포함된 사건이지만 원격근무로 인한 유출을 주요쟁점으로 하고 있지는 않다. 다만 이 사건은 피고가 원고 회사에 근무하며 10여 년 동안 원격근무를 하며 타 회사로 이직을 하고 나서도 원고회사 영업비밀 파일에 접근하는 등의 내용이 담긴 사건으로 디지털 기반 근무환경에서의 영업비밀 사건으로 살펴볼 의미가 있다. 아울러 이 사건은 피고가 영업비밀을 유출하며 제기된 소송에서 관할권 문제를 다룬 사건으로 우리의 경우와 달리 주 간에 법이 상이하고 영토가 넓어 관할권 문제가 발생할 수 있는 미국의 경우에서만 발생할 수 있는 독특한 사건이다. 따라서 피고는 원고의 이 사건 청구는 펜실베니아주 포트워싱턴에 고용된 후 뉴저지 주에서 원격근무하는 피고에 대하여 속인적 관할권(personal jurisdiction)이 없으므로 그 청구는 배척되어야 한다는 주장을 하였다.

ii) 사실관계

M3(이하, 원고)는 미국, 유럽, 아시아에서 의료 산업과 제약 회사에 시장 조사 모집, 데이터 수집 및 지원 서비스를 제공하는 의료 시장 조사 기관으로 "특정 프로젝트에 대한 입찰 및 견적"을 요청하는 잠재 고객에게 연락을 한다. 이때 원고는 "기밀 및 독점 공식"을 사용하여 입찰가를 계산하는데, 이런 입찰가 계산 공식, 가격 정보 및 고객 정보를 영업비밀로 관리하고 있다. 구체적인 관리 방식으로 원고는 이 정보들을 암호로 보호된 네트워크, 서버 및 장비에 저장하고 이 정보에 접근할 수 있는 사람에게 기밀 유지 및 비공개 계약(non-disclosure agreements)에 서명하도록 하였다. 아울러 원고가 비밀로 관리한 해당 정보를 개발하는 데에는 많은 시간과 비용이 투여되었다. 2009년 5월 29일 원고는 Karie Hart(이하, 피고)를 내부 영업 관리자로 고용하여 같은 해 6월 1일부터 근무하도록 했다. 피고는 원고의 독점 계약에 서명하고 회사에 업무범위를 제외하고 기존 또는 장래의 가망고객에게 독점 정보를 공개하거나 사용하지 않기로 하는 기밀유지에 동의하였다.

피고는 원고의 포트 워싱턴 본사에서 약 50마일 떨어진 뉴저지 집에서 WFH 형태로 일을 했다. 2020년 피고는 포트 워싱턴 본부에 접근하기 위해 키 리모컨을 요청하고 받았고, 캘리포니아, 코네티컷, 델라웨어, 워싱턴 D.C., 플로리다, 조지아, 아이다호, 일리노이, 메릴랜드, 미네소타, 매사추세츠, 뉴햄프셔, 뉴저지, 오하이오, 펜실베이니아, 사우스캐롤라이나, 유타, 텍사스, 버지니아, 위스콘신 등 미국 전역의 고객들과 함께 원고를 대표했다. 또한 피고는 인도, 독일, 프랑스, 영국, 스페인, 이탈리아, 스웨덴, 노르웨이, 핀란드, 덴마크, 일본을 포함한 원고의 국제적인 고객들을 위해 서비스를 제공하였다. 원고는 피고가 재직하는 동안 기밀 및 독점 정보를 제공했고, 이런 피고는 2014년 3월 수석 관리자에 이어 영업부 수석 부사장으로 승진했다. 이 과정에서 피고는 원고의 BluePrint Research Group 계정을 감독하고 BluePrint Research Group의 주요 연락처 역할을 했다. 그러던 2020년 원고 고위 임원인 Das Gupta와 Savanah Haunert는 원

33) 516 F.Supp.3d 476 United States District Court, E.D. Pennsylvania.

고의 경쟁사인 Atlas Primary, Inc.(이하 '피고회사')로 이직하기 위해 원고회사에서 퇴직하였다.

피고회사는 원고와 유사한 서비스를 동일한 고객에게 제공하는 의료 연구 회사로서 델라웨어에 설립되었으며 조지아주에 본사를 두고 있다. 한편 2020년 2월과 2020년 6월 사이 Das Gupta는 원고의 블루프린트 계정(BluePrint account)을 가져오기 위하여 피고를 영입하기로 했다. 그런데 피고에 대한 이런 유인행위가 이어지던 2020년 4월부터 7월까지 원고의 블루프린트 입찰(BluePrint bids)은 매달 "실질적인 감소"가 있었는데, 이는 2019년 4월부터 2019년 7월까지의 블루프린트 입찰과 비교했을 때 현저히 낮은 수치였다. 원고회사는 2019년부터 2020년까지 블루프린트 입찰에서 7.69%의 "승률" 감소에 따른 42건의 입찰 감소를 겪었다. 원고는 피고가 2020년 7월 원고에서 퇴직하여 업무가 종료됐음에도 원고 계정과 관련된 정보에 계속 접근하여 2020년 7월 31일 금요일 9시 27분에서 17시 28분 사이, 원고의 블루프린트 계정 및 아델파이 계정(Adelphi account)과 연결된 노트북에서 파일에 접속하였고, 내장 하드 드라이브의 "블루프린트" 폴더에 접속하는 등 이 시간 동안 피고의 노트북에 USB가 꽂혔다고 주장하였다. 원고는 피고 때문에 사업 손실이 있었다고 의심한다. 이런 과정에서 피고는 뒤늦게 피고회사에서 일하던 첫날 노트북과 휴대전화를 원고의 펜실베니아 본사에 반납했지만, USB는 반납하지 않았다.

결국 피고는 원고의 경쟁 회사인 피고회사에 고용되었을 때 원고의 영업비밀을 가져갔다는 혐의를 받았다. 원고는 2020년 7월 30일 피고가 사직서를 제출했음에도 불구하고, 그 후 나흘 동안 피고가 원고회사 로그인 자격 증명과 회사에서 발급한 노트북을 사용하여 프로젝트, 입찰 및 가격 정보에 접속하고 그 정보를 피고회사에게 가져가는 동안 어떠한 조치도 취하지 못했다. 이에 원고는 2020년 9월 1일 피고회사의 고위 임원 Das Gupta에게 정지 서한을 보내 피고가 원고회사의 규정을 위반하는 것을 중단하고 원고의 기밀 정보와 영업비밀을 반환할 것을 요구했다.

iii) **법원판단**

펜실베니아 지방법원은 원고의 주장에 대해 일부승소 판결을 내렸다. 상황의 전체성을 분석하면서, 법원(맥휴 판사)은 다음과 같은 사법적으로 관련된 몇 가지 사실들을 고려하였다.

피고는 원고가 제공한 노트북과 휴대전화를 이용하여 원격근무를 했는데 ① 회사는 펜실베니아에서 직원을 관리했다. ② 피용자들은 근무하는 동안 급여, 복리후생 또는 기타 문제를 해결하기 위해 펜실베니아 사무소에 연락할 필요가 있었다. ③ 의료 보장, 의료 급부금 및 퇴직 계획은 펜실베니아에서 관리되었다. ④ 사용자는 시간 기록, 각 직원의 고객 청구서 및 펜실베니아 사무소의 이메일을 관리했다. ⑤ 사용자는 펜실베니아 은행을 사용하여 급여를 지불했다. 그리고 ⑥ 사용자와의 계약 상 법률 조항에는 펜실베니아 근무 선택사항이 포함되어 있었다. 간단히 말해, 피고 등 원격근무 직원들이 생계를 유지할 수 있도록 하는 모든 필수 기능은 펜실베니아를 통해 전달된 것이다. 이런 상황에서 2020년 8월 3일 피고는 원고회사를 퇴사하였음에도 뉴저지 주 자신의 집에서 원고의 영업비밀이 담긴 파일에 접속하여 기존 원고의 고객을 자신과 피고회사의 이익을 위해 반출해 가 피고회사 고객 유인 용도로 사용한 불법행위를 저지른 것이다. 피고는 원고로부터 받은 기기를 펜실베니아 사무실에 즉시 반환하지 않고 이를 사용하여 기밀 고객정보에 접근한 것이다. 이에 법원은 피고의 뉴저지 거주권 때문에 피고에 대한 일반적인 개인적(속인적) 관할권을 행사할 수 없었지만, 피고의 영업비밀 유용에 대해 피고와 피고회사에 대한 사법권을 행사할 수 있었다. 따라서 법원은 피고와 피고회사에게 소송비

용과 기타 비용으로 30만 8,000달러를 지급하라고 판결했다.

iv) 시사점

이 사건은 피용자의 실제 원격근무로 중 발생한 것으로 관할권이 주 쟁점이다. 따라서 이 건으로 원격근무와 영업비밀과의 관계를 정리하기에는 무리가 있다. 다만 피고가 퇴사 후 나흘 동안 원고회사의 로그인 자격 증명과 회사로부터 발급받은 노트북을 사용하여 프로젝트, 입찰 및 가격 정보에 접근하고 나아가 그 정보를 피고회사에게 가져간 것은 분명 원고가 원격근무자인 피고에 대한 보안 문제를 철저하게 관리하지 않았음을 짐작하게 한다. 즉 원고는 피고에게 10년이라는 장기간 동안 원격근무를 허용하였음에도, 원격근무 시 준수해야 할 중요사항뿐 아니라 정보보안 등 기술적 보안조치를 하지 않은 것으로 판단된다. 기업이 원격 작업자에게 회사 소유 노트북을 발급하면 개인 소유 노트북에 비해 회사 자산 등 중요한 정보의 유지와 해킹 및 기타 유형의 기업 스파이 활동을 차단하는데 효과적일 수 있다. 그러나 여기에 그쳐서는 안 된다. 사용자는 피용자가 퇴사할 때는 물론 이 사안과 같이 장기간 원격근무를 할 경우를 대비해 정기적으로 기기를 회수하여 디지털 포렌식 등의 방법으로 보안점검을 했어야 했으나, 그렇게 하지 아니하였다. 이는 대부분의 정보 유용과 무단 공개가 피용자들이 기기를 갖고 새로운 일자리로 가져갈 때 발생하기 때문이다. 사실 정보가 이미 피용자의 개인 노트북에 저장되어 사용자에게 반환할 필요가 없는 경우(반환하지 않은 경우) 해당 정보에 대한 유용은 기하급수적으로 쉬워질 것이다. 반복해서 강조하지만 이 사건에서 피고는 10여 년이라는 장기간 동안 원격근무를 하였다. 따라서 원고는 모든 업무에 관한 정보를 지급한 노트북이 아닌 회사 서버에 저장되도록 물리적 조치를 취했어야 하며, 부득이 그렇게 할 수 없는 경우라면 퇴사 즉시 원격으로 저장된 정보를 "삭제"할 수 있었어야 했다. 이를 위해 사용자가 컴퓨터 또는 기타 전자 장치를 피용자들에게 발급하는 경우 그러한 자산을 추적하기 위한 시스템을 갖추었어야 했다. 아울러 피용자에게 장치를 사용하지 않을 때 홈 오피스 문을 잠그도록 하고, 장치를 안전한 곳에 보관하거나 여행할 때 휴대하고, 컴퓨터에서 손을 떼기 전에 화면을 잠그도록 하는 교육을 주기적으로 하였어야 한다.

v) 영업비밀 유출 방지 대책(예방책)

아무리 기술수준이 급변하는 사회라고 하더라도 중요정보 또는 제품에 대하여 영업비밀로서 보호받고자 하는 기업은 일반적으로 다음과 같은 조치를 취해야 한다. ① 영업비밀에 접근할 수 있는 사람들에게 비공개 또는 비밀유지 계약에 서명하도록 요구하여야 하며, ② 특별히 의미 있는 자료에 접근을 제한하여야 하며, ③ 영업비밀이 저장된 위치 또는 위치를 보호하기 위해 최첨단 물리적 보안 조치를 유지하여야 한다. 이를 위해 사용자는 원격근무와 회사의 기밀정보 취급에 대한 기대 정도를 설명하는 독립적 정책 발행을 고려할 수 있다. 최소한 그러한 정책은 피용자로 하여금 모든 의무를 상기시켜야 하며, 이는 피용자가 회사의 비밀을 보호하기 위해 적절한 예방 조치를 취할 것으로 기대할 수 있다. 비록 이러한 제안된 조치들은 사용자를 영업비밀 유용의 위협으로부터 완전히 보호할 수는 없지만, 그 보호 가능성을 크게 증가시킨다. 또한 제안된 정책을 이행하면 정보 도용으로 인하여 향후 발생 가능한 소송에 대해 사용자에게 많은 도움이 될 수 있다.

(2) 일본

1) 텔레워크 방식 등 현황(テレワークの現状, 원격근무)

2020년에 발생한 신종 코로나 바이러스 감염증(新型コロナウイルス)의 증가로 일본은 재택근무를 포함한 텔레워크 리모트워크(在宅勤務などを含むテレワーク・リモートワーク; 이하 "원격근무") 추진을 단숨에 가속화시켰다. 일본 총무성(総務省)의 '2021년판 정보통신백서(令和3年版　情報通信白書)'에 따르면, 기업의 원격근무 실시율은 2020년 1차 긴급사태 선포 당시 17.6%에서 56.4%로 증가하였다. 해제 후에는 이 수치가 저하되었지만, 그 후에도 비상사태 선포나 증가 방지 등 중점 조치, 오미크론의 유행 등으로 인해 원격근무를 선택하는 기업은 증가 추세에 있다. 중소기업의 원격근무 실시율은 대기업에 비해 낮은 경향이 있지만, 도쿄상공회의소(東京商工会議所)의 '중소기업의 원격근무 실시상황에 관한 조사'에서는 2022년 2월 실시상황이 전회 조사 때보다 6%포인트 이상 증가해 전체의 37.8%로 나타났다. 신종 코로나 바이러스의 증가를 계기로 계속 원격근무를 실시하는 기업은 증가하고 있어 앞으로도 근무방식 개혁으로 일관되게 원격근무 방향으로 진행될 것으로 예상된다.

한편 팬데믹 이전 전통적인 근무 방식이었던 오피스 근무(オフィス勤務)라면 기업은 일괄적인 보안 대책을 강구할 수 있지만, 원격근무의 경우는 각 사원에 따라 근무환경이 다르다. 따라서 보안 대책의 내용은 개인에게 맡겨지곤 한다. 원격근무에 의한 정보 유출이 발생하는 요인으로는 취약성이 있는 공공 Wi-Fi 등의 이용, PC나 태블릿 등 디바이스 분실 등의 물리적인 이유 외에 클라우드 서비스 이용 등을 들 수 있다. 우선은 컴퓨터 바이러스의 감염이나 부정 접속, 기기 도난 등의 외적요인을 들을 수 있다. 바이러스나 악성 프로그램 등의 악성 프로그램은 무차별적으로 공격하는 유형과 어느 정도 표적을 좁혀 공격하는 유형으로 나눌 수 있는데, 타깃을 좁힌 범행의 경우 악성코드가 첨부된 메일을 상대방에게 직접 송신하는 등의 수법이 일반적이다.

어쨌든 이 모든 것은 누구도 예상하지 못했던 상황에서 취업환경이 통일되지 않은 채 출발한 원격근무 때문에 발생하는 사안이라고 할 수 있다. Information-technology Promotion Agency, Japan(IPA, 독립행정법인 정보처리추진기구; 独立行政法人情報処理推進機構)가 정리한 '정보보안 10대 위협 2022'에 따르면 4위에 '원격근무 등 비정형 근로방식을 노린 공격'이 랭크되어 있어 원격근무 환경 하에서의 보안대책은 기업에 있어서 중요한 위치를 차지하고 있다.[34] 그 결과 최근 몇 년간 원격근무에 대한 수요가 높아지고 있는 현상을 노린 사이버 공격 등도 증가하고 있어 더욱 경계가 필요하다. 그럼에도 불구하고 원격근무는 시간과 장소를 효율적으로 활용하여 유연하고 균형 잡힌 근무방식을 실현하는데 매우 도움이 되는 근로방식임에 틀림없다. 근무방식의 편리성과 유연함 그리고 정해진 사무실 이외의 장소에서 일을 진행함으로써 지금까지와 같은 보안 대책의 양면성은 풀어야 할 과제이다. 따라서 원격근무 방식과 일본에서 발생한 최신 보안사고 사례에 대해 확인하고 대책의 필요성에 대해 검토하도록 하는 것이 필요하다.

우선 원격근무 방식(시스템 구성 방식)은 다양한 패턴으로 이루어지고 있는데, 2021년 5월 일본 총무성(総務省)이 발표한 바에 따르면 기본적인 원격근무 방식으로 아래 7종류로 정리하고 있다.

34) 企業における営業秘密管理に関する実態調査 2020調査実施報告書, 独立行政法人情報処理推進機構（実施：みずほ情報総研株式会社).

	방식(方式)	해 설
①	VPN (バーチャルプライベートネットワーク)	원격 단말기에서 오피스 네트워크에 VPN 접속을 실시하고, 그 VPN을 통해 사무실 서버 등에 접속하여 업무를 수행하는 방법
②	원격 데스크톱 (リモートデスクトップ)	원격 단말기에서 사무실에 설치된 단말기(PC 등)의 데스크톱 환경에 접속을 실시하고, 그 데스크톱 환경을 원격 조작해 업무를 수행하는 방법
③	VDI (仮想デスクトップ)	원격 단말기에서 가상 데스크톱 기반 상의 데스크톱 환경에 접속하여 데스크톱 환경을 원격으로 조작하여 업무를 수행하는 방법
④	시큐어 컨테이너 (セキュアコンテナ)	원격 단말기에 로컬 환경과는 독립된 시큐어 컨테이너라는 가상경계를 설정하고, 그 환경 내에서 애플리케이션을 움직여 업무를 수행하는 방법
⑤	시큐어 브라우저 (セキュアブラウザ)	원격 단말기에서 시큐어 브라우저라고 불리는 특수 인터넷 브라우저를 이용하여 사무실 시스템 등에 접속하여 업무를 수행하는 방법
⑥	클라우드 서비스 (クラウドサービス)	사무실(오피스) 네트워크에 접속하지 않고, 원격 단말기에서 인터넷상의 클라우드 서비스에 직접 접속하여 업무를 수행하는 방법
⑦	스탠드얼론 (スタンドアロン)	사무실(오피스) 네트워크에는 접속하지 않고, 미리 원격 단말기나 외부 기록매체에 필요한 데이터를 저장해 두고 그 저장 데이터를 사용하여 업무를 수행하는 방법

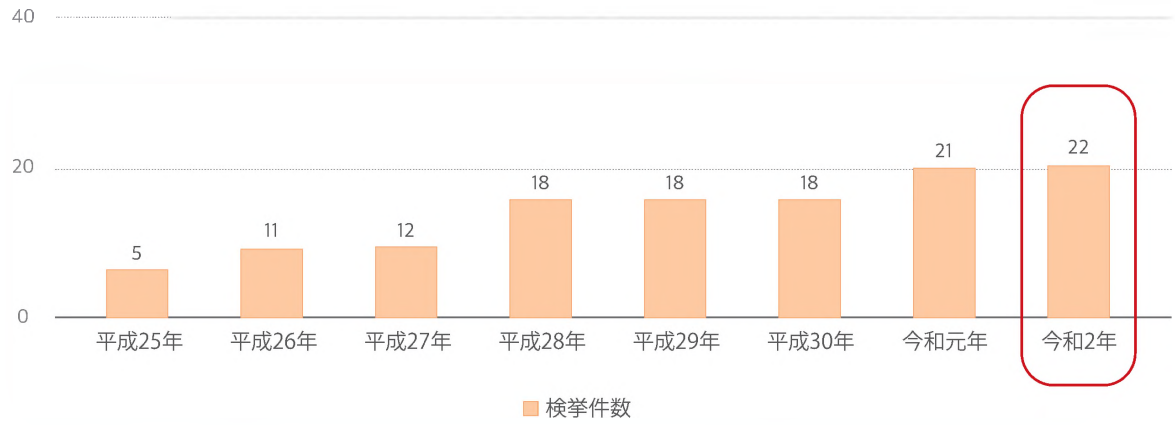
일본에서도 위와 같이 다양한 방식으로 원격근무를 실시하고 있는 기업들이 많다. 하지만 보안 대책이 마련되지 아니하여 사고로 이어진 사례들도 있으므로, 이하에서는 일본에서 원격근무 시 발생(또는 발생이 예상되는)한 보안사고 사례에 대해 살펴본다.

2) [2022 최신] 원격근무로 인한 보안사고 사례[35)]

기업에서의 비밀정보 유출 대책은 대체로 착실하게 진전되고 있다고 생각되지만, 여전히 종업원·퇴직자에 의한 국내외 유출 사건은 증가하고 있는 추세이다. 이는 令和 3 年(2021년) 일본 경제산업성(経済産業省)에서 통계로 산출한 "최근 영업비밀침해죄 검거건수 추이(近年の営業秘密侵害罪 検挙件数の推移)" 그래프를 보면 알 수 있다.

35) 総務省, テレワークセキュリティガイドライン第 5 版(令和 3 年 5 月).

그림 2. 近年の営業秘密侵害罪 検挙件数の推移[36]



이러한 영업비밀 범죄 건수에는 원격근무가 보편화된 가운데 발생한 사건도 포함하고 있는바, 도쿄 상공 리서치(東京商工リサーチ)의 조사에 따르면 영업비밀 유출은 전자기기의「바이러스 감염·부정 액세스」에 의한 정보 누설이 49.5%로 전체의 절반가량의 비율을 차지하고 있고, 이중「바이러스 감염·부정 접속」에 의한 정보 누설에서는 1개의 사고 당 누설·분실 건수가 평균 57만 8,714건으로 상당한 양을 차지한다고 발표한바 있다.

바이러스의 감염 경로로서는 컴퓨터의 기본 OS나, 인터넷 관련 프로그램의 취약성을 노리고 바이러스가 침입하는「네트워크 감염형(ネットワーク感染型)」이나 Web 사이트상의 링크 등에서 컴퓨터 바이러스를 다운로드 시키는「Web 열람 감염형(Web閲覧感染型)」등이 있는데, 웹 열람 감염형의 경우 정상 웹 사이트가 부정 침입을 받아 변조되는 경우도 있기 때문에「수상한 웹 사이트에 접속하지 않으면 감염을 막을 수 있다」라고 단언할 수도 없다.

이처럼 원격근무가 보편화된 환경에서 피용자에 대한 정보보안 교육만으로 비밀유출을 막을 수 없는 것은 비대면 근무환경에서의 영업비밀 유출에 대해 우리가 풀어야 할 숙제이다. 2021년 5월 31일 일본 총무성은 원격근무 가이드라인(제5판)(「テレワークセキュリティガイドライン（第５版）」)을 발표하며 원격근무 전자 단말기기를 중심으로 발생하는 부정접속에 대해 경고하기도 하였다.

이에 정보유출의 절반가량을 차지하는 바이러스 감염·부정 접속으로 인한 피해 등 원격근무 시 발생한 보안사고 사례를 크게 5가지 경우로 정리할 수 있는데, ①전적으로 피용자의 부주의로 컴퓨터 USB 를 분실하는 경우, ②바이러스에 감염되어 개인정보 유출, ③팝업 표시에 의해 컴퓨터가 탈취당하는 경우, ④업데이트를 게을리 하여 VPN 비밀번호가 유출되는 경우, ⑤VPN 비밀번호가 유출되어 부정 접속이 일어나는 경우가 그것이다.

가) 패턴① 피용자의 과실에 의한 정보유출(분실·도난·착오전송 등)

2021년 2월 16일 오사카부에 위치한 마쓰시타기념병원(松下記念病院)에서 사용하던 노트북이 분실되는 사고가 발

36) 그림2. 출처 経済産業省, 最新の営業秘密侵害事例から見えてくる「営業秘密」保護のポイント(令和３年６月２日).

생했다. 이 기기에는 방사선과에서 엑스레이 촬용을 위해 사용하던 것으로 환자 1,971명의 환자 ID, 이름, 생년월일, 촬영부위 및 이미지 등 다양한 (개인)정보가 저장되어 있었다. 그런데 기기가 분실된 장소는 외부인이 출입할 수 없는 공간으로 이는 곧 피용자의 과실로 분실·도난당한 사고라고 할 수 있다.

이처럼 휴대가 용이한 PC나 USB 등 외부저장장치는 원격근무를 위해 부득이 회사 밖으로 반출하여야 할 수밖에 없는바,[37] 이때 중요정보가 담긴 PC나 USB를 분실하거나 도난당함으로써 보안 사고가 일어나는 패턴이다. 자택이나 카페, 공공 작업 공간 등 사무실 이외의 장소에서 업무를 수행하기 위해서는 종이문서 또는 전자 단말기를 사외로 반출하거나 사외에서 사무실 공유 폴더 등에 접속하여야 하는바, 이 같은 경우 제3자로부터 도난 등 사고와 피용자의 부주의는 각별히 경계해야 할 사항이다.

이에 원격근무 중 피용자의 부주의한 실수로 인해 발생하는 각종 보안사고 사례에 대해 알아보겠다.

ⅰ) 원격근무 장소로 이동 중, 개인정보가 담긴 USB 등 전자 단말기기 분실

피해 내용	개인정보가 담긴 USB 분실
후속 피해	신뢰성 실추
원　　인	원격근무 장소로 이동 중 허가 없이 반출한 USB 분실

원격근무를 위해 이동 중 휴대한 노트북과 USB 등 전자 단말기기를 분실해 버렸는데, USB에 들어있던 정보는 다름 아닌 회사가 중요 정보로 관리하는 것일 경우이다.[38] 전형적인 피용자 과실에 의한 물리적 매체 유출 사례이지만, 물리적 매체의 분실을 넘어 그 안에 저장된 정보 유출로 이어지는 사례에 해당한다.

회사 밖으로 회사 정보를 반출할 경우 허가를 받도록 하는 규칙이 있었으나, 이런 규칙이 지켜지지 아니하여 사고가 발생하였다.

- 종이로 된 파일과 같은 물리적 문서나 컴퓨터, USB 등 전자 단말기를 전철이나 공공장소에 두고 내려 분실한다.
- 원격근무 장소에서 공유 컴퓨터에 USB 등 전자 단말기를 분리하지 않고 퇴실하여 분실한다.

ⅱ) 원격근무 장소로 이동 중이거나 공유 공간에서 작업 중 불특정다수에 의해 정보 유출

피해 내용	회사의 고객정보 등 중요정보 유출
후속 피해	불특정 다수에 의한 2차 피해
원　　인	피용자의 정보보안 의식 부족

37) 2020年 6 月、ある教育機関で児童や関係者延べ3000人以上の氏名や住所、電話番号等を含む個人情報を記録したUSBメモリを紛失する事故が発生しました。テレワークを実施するため、USBメモリを外部に持ち出した際に紛失が発生したとのことで、当該教育機関は、関係者に向け謝罪を表明しています. 総務省, “テレワークセキュリティガイドライン” 第 5 版（令和 3 年 5 月).

38) 2018年に日本ネットワークセキュリティ協会（JNSA）が発表した調査によると、「紛失・置き忘れ」による情報漏洩が最も多く、1年間で116件も発生していました.

공유 공간에서 원격회의 중 회사정보를 포함한 각종 정보가 주변사람에게 노출된 사례이다.[39] 이와 유사한 사례로 출장으로 신칸센(新幹線)으로 이동 중 차내에서 미발표 신제품에 관한 프리젠테이션 자료를 작성하고 있었는데, 누군가 그 내용을 보고 「모회사의 신제품에 관한 유출정보」라는 제목으로 SNS에 유출된 사례가 있었다.[40]

이를 예방하기 위해서는 노트북 등 단말기기에 프라이버시 필터를 장착하는 것을 의무화해야 하고, 아울러 단말기기에 회사 기밀 등 중요정보 파일이 열려있는 채로 컴퓨터를 놔두고 이동하지 말도록 하여야 하며, 부득이 자리에서 이동할 경우(이동하지 않더라도) 컴퓨터 화면이 제3자에게 노출되지 않도록 주의해야 한다.

- 전자 단말기기의 화면이 제3자에게 열람 가능한 상태로 되어 있어 화면에 표시돼 있던 정보가 유출된다.
- 원격근무 시 외부와의 웹 회의 중 카메라에 회사 기밀문서가 찍히는 경우.

iii) **원격근무 장소로 도착 후, 정보전송 과정에서의 부주의**

피해 내용	중요정보가 섞인 정보를 잘못 전송
후속 피해	신뢰성 실추
원　　인	작업환경의 변화로 생긴 부주의 및 정보 관리부실

원격근무를 위해 노트북, USB 등 전자단말 기기를 안전하게 집으로 가져왔으나, 작업 중 수신자 지정을 잘못하여 엉뚱한 곳으로 전송한 경우이다. 일반적으로 회사에서는 작업하던 파일을 이메일로 전송할 때 2개의 화면으로 확인하지만, 원격근무로 가정 등 회사 이외의 장소에서 근무할 때에는 작은 노트북 화면으로 작업하기 때문에 확인하는 과정에서 주의를 소홀히 할 수 있다. 즉 중요정보 등이 포함된 파일을 다른 곳으로 잘못 전송한 사례이다.

이 외에도 원격근무 중 회사에 기 도착한 서류를 확인하지 못하여 보내지 말아야 할 사람에게(예, 퇴사자, 계약이 철회된 회사 등) 메일을 보내거나, 원격근무로 회사에 부재중인 상황에서 담당자에게 서류가 장시간 전달되지 않아 분실되는 사례도 발생하고 있다.

아래 사례 역시 전형적인 피용자의 부주의로 발생한 사례인데, 작업환경이 바뀌어 실수를 범하거나 작업자의 정보관리 의식 부족을 그 원인으로 꼽을 수 있다.

- 근무 시간 외이기는 하지만 원격근무 중 자택에서 촬영한 사진파일에 회사의 기밀문서가 들어간 사실을 인지하지 못하고, 해당 정보가 포함된 사진을 SNS에 업로드하여 정보가 유출된다.

나) 패턴①-1 피용자의 고의에 의한 정보유출(내부자 부정)

정보 유출은 위와 같은 피용자의 부주의로 발생하는 경우에만 국한되지 않는다. 피용자가 고의로 기업의 영업비밀

39) 従来、業務環境はオフィス等、周囲にいる人間が自組織内の関係者等に限定される環境でした。しかし、テレワークを活用し、在宅勤務やモバイル勤務、サテライトオフィス勤務を行う場合、家族を含む、業務に関係のない第三者に囲まれた環境で業務を行うことが想定されます。そのため、第三者にPCの画面が見られてしまうことや、家族が偶然撮影しSNS等に投稿した写真にPCの画面が映りこんでしまう等、意図しない情報漏えいにつながるリスクが高まります。 総務省, "テレワークセキュリティガイドライン" 第 5 版 (令和 3 年 5 月).

40) 総務省, テレワークセキュリティガイドライン第 4 版.

을 제3자에게 누설시킬 가능성도 있다. 트렌드 마이크로(トレンドマイクロ)의 조사에서는 법인 조직의 보안사고 중 10.2%를 「내부 부정」이 차지하고 있을 정도라고 밝히고 있다.

원칙적으로 사외비 정보나 문서를 원격근무를 핑계로 회사 밖으로 반출하고 있거나, 회사 밖에서 정보에 접근할 수 있는 상황이 있음으로써 평상시보다 쉽게 사외로 기업비밀을 반출할 수 있기 때문에 고의에 의한 제3자에 대한 정보유출 위험도 높아진다고 할 수 있다. 최근까지 발생한 내부부정에 의한 정보유출은 아래와 같다.

내부(자)부정에 의한 정보 유출 사례		
기업 조직명	공표일	피해내용
アイディホーム 株式会社	2021. 6. 23.	누군가에 의해 반출된 고객 리스트가 외부 기업으로 반입되어 약 7,000건의 개인 정보가 유출
株式会社東急コミュニティー	2021. 3. 29.	전직 종업원이 고객 약 5,000명분의 개인정보를 부정 유출하여 외부 유출
SCSK株式会社	2021. 3. 24.	마쓰이 증권의 거래 시스템 개발을 수탁한 전직 사원이 210명분의 고객 정보를 빼돌려 약 2억엔을 부정하게 출금

다) 패턴② 바이러스 감염에 의해 정보 유출

보안사고 중에서도 피해가 크고 기업의 신뢰성에도 큰 피해를 주는 것이 개인정보를 포함한 회사의 기술상 경영상 정보 유출이다. 마땅히 지켜져야 할 기술상 경영상 정보가 바이러스 감염에 의해 유출되는 패턴은 많이 보인다. 바이러스에 감염되는 경로는 Web에 접속하거나 파일을 다운로드 하는 등 다양하지만, 원격근무 시에는 보안 대책 등 통신 환경이 사내에서 정상근무를 했을 때만큼 적절히 강구되어 있지 않다는 점 등으로 바이러스 감염의 위험성이 높아진다.

- 전자 단말기기 OS나 앱 업데이트를 하지 않아 외부로부터 공격을 받는다.
- 공공장소에서 제공되는 공공 와이파이에 접속하여 정보가 유출된다.
- 업무와 관계없는 웹사이트를 열람하여 악성코드에 감염된다.

i) SNS 접속으로 바이러스 감염 중요정보 유출

피해 내용	- 종업원의 성명·이메일 주소 등 개인정보, - 서버의 로그, 통신 패킷, - 서버 정보 설정 등의 정보 유출
후속 피해	정보 유출로 인한 기업에 대한 신뢰성 저하
원　　인	원격근무 시 사내 네트워크를 경유하지 않고 SNS에 접속하여 바이러스에 감염됨

원격근무를 실시하고 있던 회사의 종업원이 회사 PC로 사내 네트워크를 경유하지 않고 SNS에 접속하여 제3자로부터 받은 파일을 다운로드함으로써 회사 PC가 컴퓨터 바이러스에 감염되었다. 이후 직원이 출근해 바이러스에 감염된

기업용 PC를 사내 네트워크에 연결하면서 사내의 다른 PC로도 감염이 확대됐다는 것이다.[41] 이 경우 유출된 정보는, 종업원의 개인정보(이름·메일 주소), 서버의 로그, 통신 패킷, 서버 정보 설정 등 다양하다. 거래처나 관계회사 등 기밀성이 높은 정보는 누설되지 않았지만, 큰 보안 사고의 사례가 되었다.

- 사용이 인정되지 않은 앱이나 소프트웨어를 전자 단말기에 설치하여 악성코드에 감염된다.

라) 패턴③ 팝업 사기 등에 의한 정보탈취

팝업 사기란 웹사이트에 접속했을 때 표시되는 팝업 기능을 사용하여 사용자를 속이는 사기를 말한다. 악의적인 광고를 클릭하는 등의 이유로 애드웨어(アドウェア)라고 불리는 프로그램을 다운로드하면 「바이러스에 감염되었습니다(ウイルスに感染しました)」라고 하는 내용의 팝업창이 표시된다. 그 팝업의 지시에 따라 작업을 수행하게 되면 컴퓨터가 탈취당하거나 중요정보가 유출되어 금전 등의 피해를 입게 되는 것이다. 무엇보다 원격근무를 할 경우에는 가정 등에서 혼자 근무하기 때문에 주변 동료의 시선을 신경 쓸 필요가 없는 만큼 업무와 관계없는 웹 사이트에 부담 없이 접속하게 되어 팝업 사기 등을 당할 가능성이 높다. 게다가 팝업이 떴을 때 주변에 도움을 요청하는 등 처한 상황에 대해 상담할 수 있는 사람이 없기 때문에 피해가 커질 수 있는 문제가 있다. 이 외에도 가짜 이메일을 보내 상대방을 속여 금전을 절취하는 비즈니스 메일 사기도 이와 유사한 범주의 사건으로 분류할 수 있다.[42]

i) 팝업 표시에 따라 PC 통제권을 탈취 당함

피해 내용	- 제3자에게 컴퓨터의 통제권을 탈취 당함
후속 피해	- 개인정보 등 회사의 중요정보 유출 가능성 - 신뢰성의 저하
원　　인	- 원격근무 시 바이러스 감염 - 팝업창이 표시됨 - 컴퓨터가 이른바 좀비 PC 화 됨

직원이 원격근무를 실시하던 중 바이러스 감염을 전하는 팝업이 나타난바, 직원이 팝업의 지시에 따라 컴퓨터 조작을 실시했을 뿐인데 약 10분간 제3자에게 PC의 통제권을 빼앗겨 버렸다는 보안사고 사례이다. 다행히도 직원은 PC 통제권을 빼앗긴 후 금전을 요구하는 표시가 나오자 사기를 의심하고 인터넷 접속을 끊고 탈취를 해제했다. 그 후 전문 업체에 의해 실시된 조사 결과 정보 유출 등은 없었지만 통제 불능상태에서 수십 분 동안 단말기에 표시되어 있던 피험자의 개인정보가 열람되었을 가능성이 보고되었다. 기존 오피스 근무 형태였더라면 네트워크에서의 적절한 보안대책이 갖추어져 애초에 발생하지 않았을 사건이나, 근무환경의 변화로 발생한 사건으로 보인다.

41) 2020年５月、グループ会社の従業員がフリーメールに添付されたファイルを開封し、PC１台がマルウェアに感染する事件が発生しました。マルウェア検知システムは導入していたものの、メールに添付されたファイルに仕込まれたマルウェアが新種であったためにマルウェア検知が遅れ、氏名やメールアドレス等を含む個人情報１万件以上が漏えいしました。総務省, “テレワークセキュリティガイドライン” 第５版（令和３年５月).

42) 偽の電子メールを送り付け、従業員をだまして資金を窃取する「ビジネスメール詐欺（＝BEC）」が、財務部門の従業員等、セキュリティ意識の甘い末端の個人を標的に増加しています31。また、IPAが提供している「サイバー情報共有イニシアティブ（J-CSIP）運用状況[2020年７月- ９月]」32の中で、BECの事例の１つとして、実在するCEOを詐称し、　出張中であるが、企業買収について協力して欲しいことがある」といった内容で連絡を取るようなものが紹介されています。総務省, “テレワークセキュリティガイドライン” 第５版（令和３年５月).

마) 패턴④/⑤ VPN 비밀번호 유출로 부정 접속 피해

VPN(バーチャルプライベートネットワーク)의 취약성으로 인해 이를 이용하는 기업을 대상으로 아이디와 비밀번호가 전 세계로 유출된 사건이 발생하였다. 이 중 2020년 8월 미국 Pulse Secure(펄스 시큐어)사의 VPN 기기의 취약성으로부터 히타치카세이(日立化成), 스미모토 임업(住友林業) 등 복수의 기업이 부정 액세스를 이유로 JPCERT/CC로부터 주의를 요하는 당부를 받은 사실이 있었다.[43] 이러한 취약성에서는 사내 네트워크 접속에 필요한 '인증 정보'가 절취되었을 가능성이 있어, 부정 접속이 사고의 원인으로 보인다.

여기서 VPN이란 Virtual Private Network(가상 프라이빗 네트워크)의 머리글자로, 「가상공간에 만들어진 전용 회선」을 말한다.[44] 인터넷으로 통신할 때 상대방을 아이디와 패스워드로 인증하고 정보를 암호화해 보내면 정보가 새지 않도록 할 수 있다. VPN을 사용하여 가정의 PC와 회사를 연결함으로써 안전하게 기밀성이 높은 정보를 주고받고 일을 진행할 수 있기 때문에 원격근무에 필수적인 기술이 되고 있는 것이다. 그런데 VPN 아이디와 비밀번호가 유출되면서 기업의 기밀정보가 유출되는 보안사고 사례가 많이 일어나고 있다. 일단 VPN의 아이디와 비밀번호가 유출되면 기업의 기밀정보에 누구나 접근할 수 있는 상태가 되기 때문에 매우 위험한 상황에 처할 수 있다.

이에 아래에서 VPN 비밀번호 유출로 인한 정보유출 사례를 소개한다.

i) 업데이트를 게을리 하여 VPN 비밀번호 유출

피해 내용	VPN 비밀번호가 유출되어 기업의 기밀 정보에 누구나 접근할 수 있는 상태
후속 피해	기업의 기밀 정보가 유출되었을 가능성
원 인	VPN 전용기기의 업데이트를 게을리 하여 패스워드가 유출

2020년 5월 원격 접속을 이용한 개인 단말기를 통해 정규 계정과 비밀번호를 도난당하고, 이어 사무실 네트워크에까지 불법 접속이 이루어진 사건이 발생하였다.[45] 전용 단말기기의 업데이트를 게을리 하여 VPN 비밀번호가 유출된 사례이다. 당시 정보가 유출된 기업은 특정 VPN 기기를 사용하고 있었지만, 특정 VPN 기기 제조업체가 기기의 취약성을

43) 2020年８月に、VPN機器のIDやパスワードが世界中から流出する事件が発生しました。既知の脆弱性を放置したまま運用を続けていたVPN機器が攻撃を受け、日本でも40社近くの企業等に対して、不正アクセスが行われました。2019年には、この脆弱性を悪用する攻撃が既に発生しており、該当のVPN機器の製造ベンダー側でファームウェアの修正が行われていますが、ファームウェアを最新にアップデートしていない機器が攻撃を受けました。総務省, "テレワークセキュリティガイドライン" 第５版（令和３年５月).

44) 가상 개인 네트워크(Virtual Private Networks) 사무실에서 재택근무 등 원격으로 업무를 처리함에 따라 회사 정보가 사이버 공격으로부터 도난당할 위험이 높아졌다. 가정용 무선 네트워크는 기업의 보안 네트워크보다 훨씬 더 쉽게 침입할 수 있는데, 개인 무선 네트워크는 일반적으로 보안 프로토콜이 적기 때문이다. 회사 서버에 원격으로 액세스하는 직원에게는 일반적으로 VPN(가상 사설 네트워크)에 대한 액세스 권한이 부여된다. VPN은 직원들이 회사의 기밀 정보와 영업비밀에 대한 위험을 크게 최소화하는 동시에 회사의 네트워크에 직접 액세스할 수 있도록 하는 사설 암호화된 채널이다. VPN은 또한 고용주가 원격 작업자의 액세스 로그를 만들고 모니터링 하여 각 직원이 파일을 열거나 사용하고 전송하는 과정을 추적할 수 있기 때문에 유용하다.

45) 総務省, "テレワークセキュリティガイドライン" 第５版(令和３年５月).

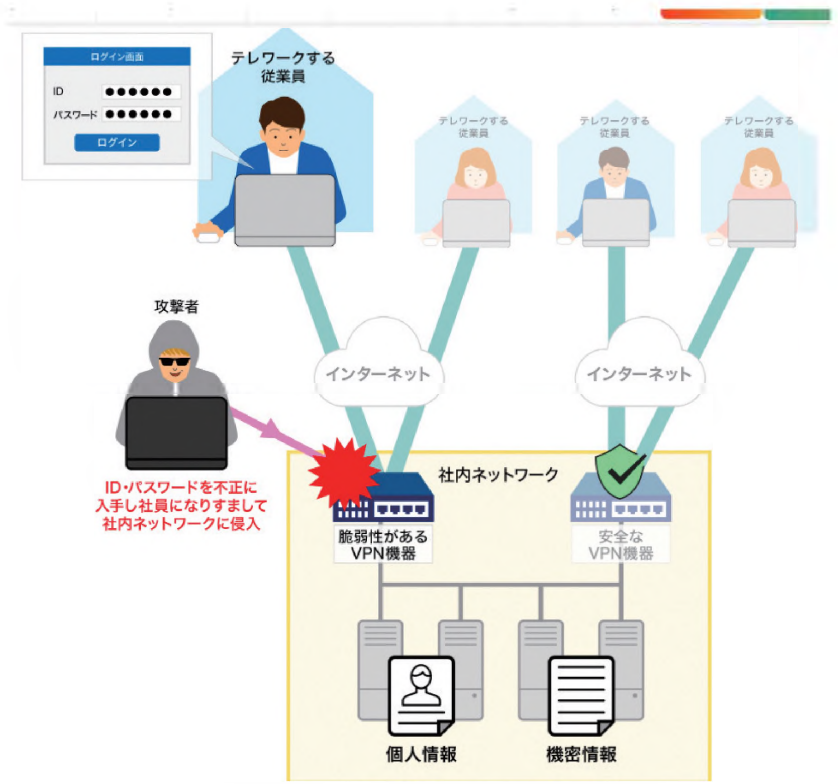
발표하고 수정 프로그램을 공개하며 주의를 당부했음에도 기업에서는 수정 프로그램을 반영하지 않았다. 결국 그 틈을 타 사이버 공격을 받아 VPN 비밀번호와 기업의 기밀 정보가 유출된 사례이다.

ii) VPN 비밀번호 유출로 인한 부정접속

피해 내용	VPN 암호가 유출되어 PC 한 대에 부정 접속
후속 피해	- 기밀 정보가 유출되었을 가능성 - 기업의 신뢰성의 실추
원 인	VPN 전용 기기의 취약성으로 패스워드 유출

VPN의 취약성에서 드러난 허점에 따른 보안 사고는 많은 기업에서 일어나고 있다. 기업에서 사용하던 VPN 기기의 취약성으로 말미암은 사이버 공격으로 VPN 암호가 유출되고, 기업의 PC 1대에 대해 부정 액세스가 이루어지고 있었다는 것이다(비록 불법 접속에 의한 정보 유출은 확인되지 않았지만). 이런 경우 대개 괜찮다고 안심하면서 평소와 같이 컴퓨터를 사용하곤 하나, 사실 보안 대책이 충분히 이루어지지 않았을 수 있다.

그림 3. VPN 기기의 취약성으로 인한 정보탈취 사례[46]



46) 그림3. 출처, コラム, “テレワークにおける情報漏洩リスクはどのように防ぐのか？事例からセキュリティ対策を解説”, <https://www.magicconnect.net/column/keyword_vol5.php?utm_source=google&utm_medium=display&utm_campaign=regad&utm_content=pmax&gclid=CjwKCAjw-rOaBhA9EiwAUkLV4mU_OiAWfSPRLA0fORxZfAPxDkyK4n7kGjpsqFOlQD5PZdcvuWdmdRoCjXYQAvD_BwE>,(last visited Nov. 28, 2022).

원격근무에서 VPN은 통신의 안전을 확보하기 위한 일반적인 수단인 만큼 미국 Pulse Secure(펄스 시큐어)사 사례는 일본 내에서 뿐만 아니라 전 세계적으로 큰 충격을 주었다. 이에 JPCERT/CC는 납품업체가 제공하는 업데이트를 이용하는 것은 물론 이러한 사태에 대비해 원 타임 패스워드(ワンタイムパスワード) 등의 인증을 도입하는 등 인증 레벨의 강화가 바람직하다고 하고 있다.

원격근무는 지금까지 사무실에서 실시하고 있던 일을 회사외의 장소에서 실시하는 것이기 때문에, 정보유출의 위험에 더해 바이러스 감염이나 도청 등에도 주의를 기울여야 한다. 바이러스 감염이나 도청을 차단하려면 원격근무 단말기와 사내 네트워크(또는 회사에 있는 자석 PC 등) 사이의 통신 경로를 암호화하는 것이 효과적이다. 암호화 통신로를 확립하는 수단으로 VPN이나 리모트 데스크톱(화면 전송형)이 있는바, 안전한 원격근무를 실시하는 방안으로 VPN 또는 리모트 데스크톱(화면 전송형)을 이용하는 것을 추천할 수 있다. 이렇게 하면 바이러스 침입에 의한 정보 누설이나 도청에 의한 데이터의 조작을 막는 대책으로 효과가 있다.

위의 그림3.은 보안 대책으로 VPN을 이용하고 있었다고 생각되지만, 다음과 같은 문제로 정보 유출이 일어난 사안으로 추정된다. 첫째 견고한 인증 방식의 채택과 디바이스 제한이 이루어지지 않았고, 둘째 보안 패치 적용 등을 포함한 기기 관리 요소가 부족했기 때문에 부정 접속이 이루어졌다.

이처럼 기업에서의 원격근무 정착은 '원격근무에 사용하는 툴에 편승한 사이버 공격'을 증가시키는 원인이 되었고, 이러한 정보유출 패턴이 사고발생의 최신 동향이라고 하겠다.

앞선 살핀 VPN 부정 접속 외에도 VDI(仮想デスクトップ),[47] Web Outlook(메일 서비스), Office 365(Office 제품 구독 서비스), Zoom(웹 회의 서비스), Salesforce(클라우드형 고객 관계 관리 도구), Trello(프로젝트 관리 도구), Amazon Web Services(클라우드 컴퓨팅 서비스)와 같은 경로로 정보유출이 발생하고 있다는 점도 유념해야 한다.

다. 법원 판결 및 기업 사례로부터 추론해 본 비대면 근무환경에서의 영업비밀 보호 방향(방지 대책)

만일 누군가 "원격근무는 회사 영업비밀이 노출될 위험을 높일 수 있나?"라고 질문했을 경우, 이에 가장 적절한 답은 무엇일까?

팬데믹 시대에 원격근무로의 빠른 전환, 화상 회의에 대한 새로운 의존, Amazon Alexa 또는 Google Home과 같은 장치와 함께 사이버 보안 공격의 위험이 증가했음은 누구나 예상할 수 있다. 따라서 위와 같은 질문의 중요성은 여러 번 강조해도 지나치지 않을 것이다.

우선 위 질문에 대한 적절한 답은 "여러 가지 면에서 원격근무에 대한 적절한 예방책이 없으면 '그렇다'"고 말하는

47) VDI(Virtual Desktop Infrastructure) 서버 상에 가상의 PC를 여러 대 준비하여 서버 단말의 이용자로부터는 마치 개별적으로 PC가 준비되어 있는 것과 같은 효과를 주어 편리하게 이용할 수 있도록 하는 환경으로 클라이언트의 실현 방식 중 하나이다.

것이 가장 합리적인 답이 될 것이다. 그 이유는 원격근무의 경우가 회사 내에서 네트워크를 통한 파일 접속(접근)보다 문제가 생길 가능성이 높기 때문이다. 종종 직원들은 원격으로 근무할 때 접속시간이 더 많이 걸린다고 불평하는 경우가 많다. 때문에 피용자들은 회사 자료를 다운로드하기 위해 외장 하드 드라이브와 같은 개인장치를 사용하는 경우가 많아졌다. 그렇지만 이러한 관행은 기업의 영업비밀보호에 큰 문제를 야기할 수 있다. 원격근무 시대, 기업은 자사의 영업비밀 보호정책이 충분한지, 또는 사이버보안 보험이 회사 네트워크를 통한 외부 정보 전송 위반을 보장하는지 여부를 평가해야 한다. 사실 많은 기업이 USB나 클라우드 네트워크와 같은 원격 저장장치로의 정보 반출을 금지하지만, 직원과의 네트워크 연결을 위해 보안 네트워크를 사용하고 특정 디지털 파일에 대한 개인별 접속을 제한하는 것에는 소홀한 면이 없지 않다.

이제는 암호로 보호된 서버에 기밀 및 독점 정보를 저장하도록 하는 것만으로는 충분하지 않을 수 있다. 이는 아래의 사례에서 확인할 수 있는바, 식품의 품목을 분리하고 무게를 측정하는 척도, 제어 및 표시 시스템을 조립, 제조, 설치하고 서비스하는 기업이 위와 같은 조치를 수행했지만, 사건을 심리한 법원은 해당 정보는 부품실, 회계 부서, 서비스 부서 및 기타 관리 부서에서 근무한 직원을 포함하여 여러 부서에서 사용할 수 있었다는 이유로 위와 같은 조치만으로는 대상 정보가 영업비밀로 간주되는 것에 유리하게 작용하지 않는다고 판단하였다.[48] 정리하면 독점 및 기밀 정보가 있는 네트워크에 대한 관리 접근은 "최소한의 접근 권한"으로 제한되어야 하며, 절대적으로 필요한 사람만 접근 가능하게끔 정보 접근권을 제한하는 실천이 필요하다. 또한 기업은 직원들이 보안 네트워크 접근(접속)을 통해 업무용으로 발급된 장치에만 민감한 정보를 저장하게 하는 명확한 정책을 마련해야 한다.

결론적으로 기업은 다음과 같은 작업을 수행해야 한다.

- 회사 영업비밀 파악
- 영업비밀 및 기타 기밀 및 독점 정보의 공개를 금지하는 기밀 또는 비공개 계약에 서명
- 영업비밀 및 정보보안 정책, 특히 가정 내 Wi-Fi 네트워크 비밀번호로 보호하도록 교육
- 최신의 안전한 시스템이 갖춰져 있는지 확인(직원들이 팀과의 구두 및 전자 통신을 유지할 수 있도록 안전하고 보호되는 수단을 제공)
- 전자 통신의 경우 직원들에게 회사 이메일 계정, 보안 공유 드라이브 또는 보안파일 전송 시스템만 사용하도록 지시하고, 가능한 경우 개인 단말 기기나 계정을 사용하지 않도록 주의
- 인쇄물 또는 물리적 자료를 집으로 가져와야 하는 경우, 해당 정보를 안전하게 보관하도록 지시
- 중요한 정보 및 독점 정보에 대한 접근(접속)을 필요한 경우로 제한
- 퇴사 시 각종 문서(documents, notebooks, files), 랩탑(laptops), 썸 드라이브(thumb drives), 외장 하드 드라이브(external hard drives) 또는 기타 회사 전자 단말기기를 회수하고 회사 정보에 대한 접근(접속)을 종료하는 계획 수립

48) Weight Systems South Inc. v. Mark's Scale &Equipment Inc., 347 Arc. 868, 68 S.W.3d 299(2002).

- 법률 고문 및 IT 전문가의 도움을 받아 사이버 보안 프레임워크 및 위험 관리계획 개발
- 피용자의 이메일 또는 다른 계정의 스냅샷을 보존
- 특히 중요한 정보에 가장 쉽게 접근할 수 있는 직원 및/또는 경쟁업체에 합류할 가능성이 있는 직원의 경우 피용자가 사용한 기기를 만지기 전에 보존하고 이미징 하는 것을 고려

라. 맺음말

팬데믹으로 수많은 직원들이 원격근무를 시작해야 했고, 이른바 하이브리드 작업 환경이라는 새로운 이슈에 대비해야 하는 상황에 직면한 우리가 영업비밀 보호를 위해 할 수 있는 일은 무엇일까? 기업은 유례없는 위험에 대비하기 위해 원격근무라는 근무형태를 선택해야했지만, 새로운 환경으로부터 발생하는 바이러스 감염 및 해킹 등으로부터 영업비밀을 보호해야 하는 방안에 대해 고민해야 했다.[49] 즉 COVID-19 대유행으로 인하여 원격근무가 권장되는 등 기업의 근로방식 변화로 정보관리 방법에 있어 많은 변화가 나타났다. 한편 과거에도 원격근무는 존재했지만, 이는 일부 피용자에 한하여 필요시에만 존재했던 제도였다. 그러나 오늘날과 같은 팬데믹 상황에서의 원격근무는 과거와 달리 선택이 아닌 필수로 거의 모든 피용자가 행해야 하는 기업의 근무형태로 자리하여 결과적으로 일과 삶의 균형에 공헌한 것으로 볼 수 있다. 분명 원격근무는 직장과 주택을 이동하면서 생기는 통근 스트레스를 해방시켜주었고, 출퇴근 시간을 절약하여 시간을 효율적으로 배분하도록 함으로써 업무 효율성을 높여주는 장점이 있다. 이외에도 육아·돌봄과 일을 양립할 수 있도록 하여 다양하고 유연한 노동 근무방식 개혁에 기여하는 수단으로서도 주목을 끌기에 충분하다.

그러나 향후 지금의 팬데믹과 유사한 감염병 등 긴급사태가 올 수 있다는 세계보건기구(WHO)의 경고는 원격근무의 편리성보다 바이러스 감염 및 해킹 등으로부터 영업비밀의 유출로 이어질 수 있다는 불안감에 기업경영을 위축시킬 수 있다. 따라서 원격근무 중 발생했거나 또는 발생할 가능성이 있는 사례를 통해 기술적·물리적·인적 문제에 대해 되돌아보고, 영업비밀 보유자인 기업은 물론 국가, 지방자치단체 등 관련기관 역시 기업이 비대면 근무환경에서의 문제점에도 불구하고 경영의 연속성을 확보할 수 있도록 공헌하는 수단과 방법 등 디지털 생태계 조성에 만전을 기하여야 할 것이다.

49) 김성용, "사이버 공간에서 디지털 자구행위(Digital self-help) 법제도화를 위한 해킹백(Hacking Back)에 관한 소고", 『법학논총』 제34권 제1호(2021), "능동적 사이버 방어 행위"는 현실세계에서는 상대 공격(이를테면 폭행에 대한 정당방위 등)에 대한 자위권적 대응으로 자구행위를 인정하지만, 사이버 공간에서는 이를 인정하고 있지 않기 때문에 나온 이론이다. 즉 진화하는 해킹기술과 그로 인한 피해에 적극적으로 대응해야할 필요성이 제기되면서 공격자(해커)를 식별하고 도난당한 데이터를 찾아오거나 파괴하는 등의 적극적 대응을 말한다.

2. 유럽의 비대면 근무환경에서 영업비밀 유출 사건·판례 및 방지 대책

가. 유럽의 영업비밀보호 개관

(1) 2019년 이후 영업비밀보호에 관한 법제 및 판례 동향

- 유럽에서는 기업의 핵심 노하우 및 기밀을 불법 탈취하는 침해행위가 증가함에 따라 이에 대한 대책의 일환으로 유럽시장을 규율하는 통합 법률을 제정할 것을 EU 회원국에 권유하기 위해 입법지침을 마련하였다. 민사 구제를 원칙으로 하는 이 입법지침은 영업비밀을 불법 취득, 사용, 공개로부터 보호하려는 것을 목적으로 한다.

- 그동안 독일을 포함한 일부 유럽연합 회원국들은 영업비밀을 규정하는 고유한 법률이 없었으며, 유럽 전체를 대상으로 통일된 보호범위를 정립하지 못하였다. 더구나 구체적인 침해 형태에 따른 통합된 법적 규제의 부재로 효과적으로 영업비밀 침해행위에 대처해 오지 못하고 있다는 비판이 제기되어 왔다. 이에 따라 유럽연합 의회는 회원국의 관련 법규를 통일해서 균등한 규제를 위하여 "노하우 및 영업비밀에 관한 입법지침"을 2016년 4월 16일 승인하고, 6월 8일 통과시켰다.[50] 이 입법지침에 따라 모든 회원국은 국내법을 제정하도록 하였다.[51]

- 2016년 EU 입법지침에 기초하여 독일을 비롯한 모든 회원국이 국내법으로 영업비밀보호를 위한 특별법을 제정하거나 관련 법률을 대폭 수정하였다. 영국은 EU 회원국에서 탈퇴를 선언하기 직전이었으므로 EU 입법지침에 따라 특별법을 제정하였고, 오스트리아는 자국의 부정경쟁방지법 등의 개정으로 입법지침을 수용하였으며, 프랑스 역시 상법전을 개정하여 영업비밀 보호 규정을 담아냈다. 스위스의 경우 EU 회원국이 아님에도 자국 기업의 영업비밀을 보호하기 위해서는 이 입법지침의 영향으로부터 자유롭지 못하다고 할 것이다.

- 코로나 팬데믹 이후 홈오피스를 비롯한 재택 및 원격근무에 따른 영업비밀보호와 관련된 유럽 각국의 최근 동향을 검토한다. 이와 관련된 판례들이 현재 축적된 상태가 아니므로 향후 유럽 국가들의 국내법원의 견해와 유럽사법재판소의 판단을 눈여겨보아야 할 것이다.

(2) 코로나 팬데믹과 홈오피스에서의 영업비밀 유지조치 사례

- 오늘날 국경을 초월해서 문제 되고 있는 코로나 팬데믹은 개인의 일상생활뿐만 아니라 기업의 업무환경에도 큰 변화를 불러왔다. 홈오피스 (Home Office), 재택근무, 원격근무 등의 비대면 근무 형태가 평범한 기업의 업무문

50) EU Directive 2016/943 (Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure).

51) EU(유럽연합)는 2016년 제정한 영업비밀에 관한 입법지침을 2018년 6월까지 EU 회원국에게 국내법을 제정하도록 기한을 명시했다.

화로 자리 잡기에 이르렀다. 이는 국가 정책과 법적 요구에 의해 또는 회사의 방침에 따라 직원의 건강과 회사의 주의의무를 실현하려는 노력의 결정체로 등장한 근무형태라 할 것이다.

- 그런데 비대면 근무환경에서 제대로 된 회사의 정보와 비밀관리 조치가 영업비밀 관련 법률의 규정에서 요구하는 일정한 수준을 갖추지 못한 경우에는 특히 유럽에서 새로운 규정에 의해 영업비밀로 인정받을 수 없고, 막대한 법적 결과를 초래할 수 있다. 현재 코로나 팬데믹 상황으로 인해 재택근무가 점점 더 활성화되고 있는 것을 고려할 때, 재택 및 원격근무에 따른 적절한 정보의 보호조치는 필수적 최소 요건이라고 할 것이다.[52] 이러한 배경에서, 회사 업무 또는 공무를 수행하면서 개인소유의 기기 사용은 비밀보호 조치에 반하는 것으로 보아야 한다. 따라서 비대면 근무에서 기업정보의 사용에 대한 적절한 비밀성 유지조치를 취할 수 있도록 법적, 기술적 제한도 적극적으로 요구되는 실정이다.

- 엄밀하게 말하면, 비대면 근무의 유형은 다양하기 때문에 이를 구별하여야 한다. 넓은 의미에서 홈오피스는 종전의 비대면 근무를 모두 (모바일근무, 재택근무, 원격근무 등) 포함하는 개념이지만, 계약의 유형(계약직, 정규직, 임시직, 영구직 등)과 사용하는 인터넷 및 IT 체계 (공용 WLAN 네트워크, 개인 PC 사용방식 등) 등에 따라서 구별하기도 한다.

- 유럽뿐만 아니라 세계적으로 COVID-19 여파가 공공의 일상생활을 제한하면서 언제까지 지속될지, 언제 제한이 풀릴지 불분명한 상황에서 기업들은 재택근무로 인해서 발생될 법적 위험을 방지 또는 예방하기 위한 "적절한 정보보호 조치"를 강구해야 할 시점에 이르렀다. 재택근무는 직원의 단순한 "귀가조치"가 아니기 때문이다. 재택근무로 인해 개인 생활과 회사의 공적 업무가 혼재될 가능성이 높아지고 있다. 이에 따라 데이터 보호와 관련된 법률, IT 보안 또는 영업비밀 보호 영역에서 경제적·기술적·법적 위험이 증가하고 있고, 이에 대한 대책이 국가 차원에서 또는 회사별로 진행 중이다.

- 여기서는 우선 원격 및 재택근무를 위한 가이드라인, 특히 독일연방 중소기업협회(BVMW)에서 제시한 "기업의 정보보호를 위한 가이드라인"을 대표적으로 소개하고, 홈오피스로 인한 영업비밀보호와 관련된 유럽 국가들의 법적 분쟁을 검토한다. 이를 통해 우리나라에서 영업비밀 보호조치를 위한 국가 정책 기획 및 기업별 대책 마련에 일정한 시사점을 줄 수 있기를 기대한다.

나. 독일의 영업비밀보호에 관한 법률 분석 및 판례 동향

- 2016년 EU 입법지침에 따라 독일에서는 관련 국내법을 제정하였다. 2019년 6월 독일은 "영업비밀보호를 위

52) https://www.cmshs-bloggt.de/rechtsthemen/coronavirus-handlungsempfehlungen-fuer-unternehmen/covid19-schutz-von-geschaeftsgeheimnissen-im-home-office-das-ist-zu-tun/

한 법률"이라는 명칭[53]으로 입법지침을 수용하여 특별법을 발효하였다. 국내법 제정 전부터 독일 연방대법원은 2018년 3월 22일 판례[54] 등을 통해 영업비밀보호에 대한 요건들을 규명하였고, 부정경쟁방지법(UWG)[55] 및 민법(BGB)과 형법(StGB) 등의 규정에 따라 영업비밀을 충분히 보호할 수 있다고 보았다. 그러나 독일 입법부는 EU 입법지침과 지금까지 국내에서 이와 같은 법률을 통한 보호가 산재되어 있고, 모호한 부분도 묵과할 수 없어, 좀 더 체계적으로 영업비밀을 보호하기 위한 새로운 법 제정이 불가피하다고 보았다. 또한 이 법률에서 처음으로 영업비밀의 정의를 규정하였다.

- 2020년 KPMG 회계법인에서 발표한 연구[56]에 따르면 독일에서 일어난 경제범죄 중 84%가 영업비밀 유출 및 침해에 관한 사건(Verrat von Geschäfts- und Betriebsgeheimnissen)이 차지하는 것으로 나타났다.

(1) 비대면 근무환경에서의 보호조치

- 독일 기업들이 원격근무(Remote Work) 환경에서도 영업비밀을 유지하고, 보호가 가능하도록 "적절한 영업비밀 보호조치"에 대하여 연방정부 기관인 독일 연방중소기업협회(BVMW)[57]는 2019년 4월 26일 기업의 정보보호를 위한 가이드라인[58]을 설정하여 공개하고 있다. 이 조치는 원격근무 및 재택근무의 경우에도 적용된다.

이 협회에서 제시한 10가지 가이드라인은 다음과 같다.

① 회사의 비밀보호 담당자 또는 책임자를 지정한다.
② 보호할 가치가 있는 회사의 정보를 확인한다.
③ 보호받을 가치가 있는 식별된 정보에 대하여 보호권 신청을 고려할 수 있는지 여부를 확인한다.
④ 식별된 보호 가능한 지식을 여러 가지 범주로 분류한다.
⑤ 보호 조치에 대한 규정을 확립한다.
⑥ 확립된 보호 조치를 이행한다.
⑦ 예방 및 대응적 보호 조치를 문서화한다.
⑧ 교육을 실시하고 직원들의 경각심을 높인다.
⑨ 타인이 보호하는 비밀에 감염되지 않도록 예방한다.
⑩ 1번부터 9번까지 정기 점검하며, 최신화한다.

53) Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG).
54) 독일 연방법원 판결에서 영업비밀보호에 관한 일정한 기준과 원칙이 마련되어 있었다. (BGH Urteil vom 22.03.2018 - I ZR 118/16 참조).
55) 독일의 부정경쟁방지법은 2019년 영업비밀보호를 위한 법률의 제정으로 전면 개정이 단행되었다.
56) https://www.kosmicon.de/kpmg-studie-zu-wirtschaftskriminalitaet-belegt-notwendigkeit-von-cyber-defense-massnahmen-fuer-kmu-und-onlinehandel/
57) BVMW는 독일 중견 기업들을 대표하는 협회로서 900,000명 이상의 회원으로 구성되어 있다. 300명이 넘는 이 협회의 대표단은 매년 약 800,000 건에 걸쳐 직접적인 경영전략을 협의하며, 매년 2,000 여개의 크고 작은 기업 관련 행사를 개최하고 있다.
58) https://www.bvmw.de/fileadmin/03-Themen/Recht/Dateien/checkliste-10_Tipps_zum_Gescha_ftsgeheimnisgesetz.pdf

이를 구체적으로 기술한다.

- 독일에서 2019년 4월 26일, 영업비밀보호법(GeschGehG)이 발효됨으로써 제3자의 무단 엑세스로부터 보호받을 가치가 있는 정보를 보유하는 모든 기업은 이 법의 대상이 되었다. 이미 언급한 바와 같이 독일은 기업의 영업비밀을 위한 장치를 여러 법률에서 구현해왔으나, 이제는 특별법의 제정으로 더 높은 요구조건을 갖추어야 한다.

- 지금까지 기업의 정보가 비밀로 보호되어야 할 정보들은 거의 자동적으로 법적으로 기업비밀로 간주되고, 악용되지 못하도록 보호를 받아왔으나, 이제는 비밀정보의 보유자(소유자)는 해당 정보가 경우에 따라 적절한 비밀 조치의 대상이라는 점을 입증하여야만 비로소 영업비밀보호법의 보호 대상이 될 수 있다.

- 따라서 독일 기업은 자신들의 비밀이 영업비밀보호법의 규정에 따라 일정한 요건을 구비하지 않을 경우에는 법적 보호를 더 이상 받지 못할 상황이 발생할 수도 있게 되었다. 더구나 이 특별법은 적절한 비밀유지조치에 관해 명백하게 구체적으로 규정하고 있지 않다. 문제는 지금부터 모든 기업들이 스스로 비밀유지 조치를 단행해야 한다는 점이다. 더구나 이와 같은 안전 조치를 실현하는 것은 기업 스스로 세심한 기획을 세워야 구현될 수 있는 것이다. 이제부터 보호 개념과 범위를 설정하고 보호조치를 실행하는 것은 기업에게 커다란 도전이 아닐 수 없게 되었다. 이를 위해 독일의 BVMW는 중소기업별로 정보보호 조치를 마련하도록 권유하면서 일정한 메뉴얼을 작성하여 다음의 10가지로 나누어 공개하고 있다.

① 회사의 비밀보호 담당자 또는 책임자를 지정한다. 지정된 담당자는 법정에서 입증된 정보보안 관리시스템을 설정하고 체계화하는 일을 총괄하며, 비밀보호에 필요한 권한을 갖고, 그의 대리인도 지정하여야 하며, 회사 내의 각종 부서의 책임자 및 직원들과 협력하여야 한다.

② 보호할 가치가 있는 회사의 정보를 확인하고 식별한다. 이러한 정보에는 기술정보 (예: 발명품, 건설계획, 공식 등) 뿐만 아니라 상업 정보(예: 가격목록, 조건, 재무 데이터)가 비밀이 될 수 있다. 보호할 가치가 있는 정보의 흐름도(지도)를 작성하여, 그 정보가 어디에서 발생되며, 어디로부터 기업으로 유입되는지, 그 정보가 어느 곳에 저장되고 그리고 어떻게 기업 내에 배포되는지를 일목요연하게 파악할 수 있는 "지도"를 작성하여야 한다. 그 정보들을 분류하고 체계화하기 위해서는 문서화시스템(Dokumentationssystem)을 활용하여야 한다.

③ 보호받을 가치가 있는 식별된 정보에 대하여 어떤 보호권리를 신청하는 것이 유리한지 확인한다. 일부 발명품은 제조법이나 제품 분석만으로는 알아낼 수 없는 경우에는 특허출원이 유리하고 그 밖의 경우에는 영업비밀보호로 처리하는 것이 더 유리할 것이다.

④ 식별된 보호 가능한 지식(정보)을 여러 가지 범주로 분류한다. 이와 같은 정보가 손실되면 회사의 존립이 위태로워질 수 있는 경우에는 가장 높은 범주 A에 할당하고, 전략적으로 중요하고 손실로 인한 충격이 큰 경우의 정보는 범주 B로 분류하고, 다른 회사와의 경쟁에서 요구되는 중요한 지식으로 어느 정도 감당할 수 있는 정보는 범주 C

로 분류한다. 여기에서도 문서화시스템을 활용하여 기록한다.

⑤ 보호조치에 대한 회사 자체 규정을 확립한다. 먼저 총체적이고 지속 가능하며 법정에서 문제 될 수 없는 입증된 보안 개념을 설정한다. 이 보호조치는 구체적인 상황에 따라 적절하게 처리한다. 범주 A는 상상할 수 있는 가장 엄격한 보안 조치를 요구하고, 범주 B는 일반적으로 엄격한 단계의 보안 조치를 요구하나, 최고 수준일 필요는 없다. 범주 C에는 효과적이고 어느 정도 관리 가능한 조치를 취할 정도의 것으로 분류한다. 이때 생각할 수 있는 모든 기술적, 조직적 조치와 계약상의 조치를 결합할 수 있다. 한편으로는 비용, 편익 및 현실 타당성과 다른 한편으로는 기업의 규모와 기업이 갖는 비밀의 의미를 적절히 파악하여 반영하여야 한다. 보호조치는 모든 위험성을 판단하고 고려해서 구축하여야 한다.

⑥ 정확하게 확립된 보호 조치를 구현한다. 기업은 직원 및 거래처 상대방은 물론 알려지지 않은 제3자, 즉 산업스파이 등과 관련해서 일정한 조치를 취해야 한다. 특히 기업에서는 근무하는 직원들에게 "알 필요가 있는 원칙 need-to-know-prinzip"을 준수하도록 하여야 한다. 예를 들어, 업무상 필요로 한다면 그 정보에 접근할 수 있도록 한다, 접근방식의 예로는 공간적 분리, 공간과 저장 장소를 위한 접근 규정, 차별화된 권한을 가진 잠금 체계, 암호화, 비밀번호 규정, 디지털 권한 관리, 메타데이터에 대한 식별 등을 들 수 있다. 기업의 정보에 접근하는 것을 피할 수 없는 경우에는 그 정보를 받는 접근자(수신자)가 어떻게 비밀을 다루어야 하는지, 공개 가능 여부도 정확하게 정해야 한다. 이것은 일반적이고 포괄적으로 이루어져서는 안된다. 이른바 포괄 규정(catch-all-clause)[59]으로 작성되어서는 안된다. 이와 같은 조치는 구체적인 정보에 적절하게 적용되어야 한다. 주의할 점은 구조적이고 기술적이며 조직적으로 융합된 상호작용에 유의하여야 한다. 적은 것이 때로는 더 큰 효과를 발휘할 수 있다는 점을 명심해야 할 것이다.

⑦ 예방 및 대응적 보호조치를 문서화한다. 비밀 보유자(소유자)는 분쟁이 발생할 경우 자신이 "상황에 따라 적절한 비밀유지 조치"를 취했음을 입증해야 한다. 그러므로 이 조치들이 언제든지 "적절"하기 위해서는 보호조치가 정기적으로 재검토되고 경우에 따라 조율되어야 한다. 그래서 정보 취급을 명백하고 이해하기 쉽고, 그리고 법원에서 이미 확인된 법적 증거로 간주되는 정보로 인정받을 수 있도록 육하원칙에 의거해 문서화하여야 한다 (누가, 무엇을, 언제, 어디서, 왜, 그리고 어떻게).

a) 새로 제정된 영업비밀보호법을 이행하기 위해서 프로젝트의 범위와 내용을 기술한다.

b) 새로운 정의에 따라 분류된 영업비밀 목록을 작성한다.

c) 정보보호 컨셉을 구현하기 위한 조치 카탈로그를 작성한다.

d) 검토보고서를 작성하여 보호조치의 이행을 입증한다.

e) 내부와 외부의 기업비밀에 대한 내부 지식을 가진 것에 대한 자료들을 포렌식 방식으로 활용할 수 있는 충분한 양의 데이터를 생성하여 확보한다.

59) 2022년 1월 독일 아헨 노동법원에서는 고용계약서에 명시한 포괄규정(catch-all-clause)은 비밀유지조치에 해당하지 않는다고 판시하였다 (ArbG Aachen Urteil vom 13.1.2022 - 8 Ca 1229/20),

f) 내부 및 외부 기업비밀 보유자(보유 장치)와의 모든 계약 내용을 조율한 회의록을 작성한다.

g) 목적에 적확한 증거 자료를 항상 확보한다.

h) 직원을 대상으로 실시하는 교육자료는 백업해야 한다.

⑧ 정보보안에 대한 교육을 실시하고 직원들의 경각심을 높인다. 매일 민감한 정보를 다루는 직원들에게 정보의 중요성을 환기시킨다. 이를 위해 정기적인 교육을 실시한다. 특히 메뉴얼 및 규정집을 숙지시키고, 구체적인 계약 내용을 점검하며, 제재와 지시 권한의 여부를 확인시키고, 비밀보호에 대한 의사소통으로 신뢰를 형성하여, 의식적으로 비밀유지에 대한 감각을 유지하는 기업의 분위기를 조성한다.

⑨ 타인이 보호하는 비밀에 감염되지 않도록 예방한다. 신입사원 채용이나 신규 협력 관계가 이루어지면 다른 회사의 비밀 지식이 빠르게 자신의 기업으로 유입되기 마련이다. 타인이나 다른 회사의 비밀일 경우에는 그 비밀의 활용 여부를 명확히 해야 한다. 그렇지 않을 경우에는 기업이 비밀 소유자에게 책임을 진다. 경영진이 알지 못한 경우에도 부분적으로 책임을 진다.

⑩ 정기적으로 1번부터 9번까지 재점검하며, 최신화하고, 반복하여야 한다. 보안은 상태가 아니라 프로세스이다. 기밀 유지 조치가 항상 적절하다고 평가받기 위해서는 그 보호 기능과 상태를 정기적으로 점검하고 조율하여야 한다.

(2) 홈오피스로 인한 법적 분쟁 전망

- 홈오피스를 비롯한 원격근무, 재택근무 등은 '재택 사무실'에서 회사의 데이터를 처리하는 작업이므로 개별 사안에 따라 이에 대응하는 적절한 비밀유지 조치 역시 방법을 달리해야 한다. 홈오피스 작업을 통제하려면 먼저 회사 내의 네트워크 전체를 체계적으로 기획하여야 한다. 이를 위해 데이터 보안을 위한 충분한 수준의 버전을 제공하는지의 여부와 재택 직원은 자신이 사용하는 커뮤니케이션 수단에 대해서도 충분히 숙지하는 것이 중요하다.

- 2016년 EU 영업비밀에 관한 입법지침에 따라 회원국인 서유럽뿐만 아니라 중유럽과 동유럽 국가들 사이에도 이를 바탕으로 영업비밀 보호 규정을 자국의 법률에 반영하여 시행하고 있다. 홈오피스에서의 작업이 회사의 영업비밀을 다루는 경우에도 이 영업비밀보호와 관련된 법률이 적용된다. 2022년 현재 EU 회원국은 물론 영국에서도 EU 입법지침을 수용하여 자국의 법률에 적용하고 있다.[60] 결국 유럽 전역에서 영업보호와 관련된 사안은 EU 입법지침을 바탕으로 동일한 내용으로 균등하게 규율되므로, 영업비밀 침해행위와 그 대처 방안은 거의 유사한 것으로 귀결될 것이다. 아직 2022년 11월 현재 EU 회원국 사이의 첨예한 분쟁 사례는 발견되지 않는다. 향후 회원국

60) 영국에서도 코로나 팬데믹 이후 영업비밀과 관련된 판례들이 공개되었다. Travel Counsellors Ltd v Trailfinders Ltd [2021] EWCA Civ 38 (19 January 2021), Celgard LLC v Shenzhen Senior Technology Material Co Ltd [2020] 5 WLUK 45 (07 May 2020), Shenzen Senior Technology Material Co Ltd v Celgard LLC [2020] EWCA Civ 1293.

사이의 분쟁은 유럽사법재판소의 몫이기는 하지만, 현행 영업비밀보호에 관한 입법지침이 판단기준이 될 것으로 전망한다.

(3) 코로나 팬데믹 이후 최근 독일의 판례 동향

- 독일은 2019년 영업비밀보호법을 제정하여 실행하는 가운데 코로나 팬데믹 현상과 중첩되면서, 한편으로는 정보보호 조치가 비대면 근무환경에서 더욱 강구될 필요성이 있다는 점을 인식하고 이에 대응하고 있으며, 다른 한편으로는 영업비밀보호법에서 규정하는 "정보의 적절한 보호유지 조치"의 범위와 한계 설정 등이 예민한 문제로 부각되고 있다.[61]

- 그러나 코로나 팬데믹으로 인한 비대면 근무환경이 활성화된 후 이에 관한 판례는 아직 찾아보기 힘든 실정이다. 또한, 이러한 판례를 논의하기에는 시기상조인 것도 사실이다. 원격근무 활성화가 더 많은 영업비밀 보호 침해를 야기시켰다고 볼 수도 없으며, 이와 관련해 분쟁이 발생한다고 해도 판례가 확립되기까지의 절차와 과정이 있기 때문이다.

다. 오스트리아의 영업비밀보호 관련 판례 현황

오스트리아는 부정경쟁방지법(UWG)과 민법(ABGB) 조항들을 개정함으로써 2016년 EU 입법지침을 수용하였다.[62] 오스트리아에서의 영업비밀 침해행위에 대한 분쟁 사례는 독일의 영업비밀 관련 법률 규정과 동일하기 때문에 독일과 오스트리아 사이의 법원 결정이 서로 상당한 영향을 미칠 것으로 전망된다.[63]

- 원격근무와 영업비밀 관련 최근 판례 신문보도 기사(2022년 4월 8일 공개).

  - 2022년 4월 8일 오스트리아 일간지 보도[64]에 등장한 최근 오스트리아 비엔나 법정에서 진행되고 있는 코로나 팬

61) 코로나 팬데믹 이후 독일법원에서 영업비밀과 관련된 상당한 분량의 판례들이 공개되었다. 이 판례들 가운데 주된 법적 이슈가 되었던 판례들을 구체적으로 정리한다. 먼저 영업비밀이 도출될 수 있는 파일의 외부 특성에 대한 접근 또한 금지대상이 될 수 있음을 명시한 판례 (BVerwG, Beschluss vom 05.03.2020 - 20 F 3/19), 영업비밀보호법 적용범위에 대한 판례 (OLG Düsseldorf, Beschluss vom 11.01.2021 - 20 W 68/20), 개인적으로 기록한 정보의 경우에도 영업비밀에 해당한다고 간주한 판례 (LAG Düsseldorf, Urteil vom 03.06.2020 - 12 SaGa 4/20), '비밀유지조치'를 위한 최소한의 보호조치에 관한 판례 (OLG Stuttgart, Urteil vom 19.11.2020 - 2 U 575/19), OLG Hamm, Beschluss vom 27.01.2021 - 20 W 48/20, "보호의 적절성"의 평가 기준을 설정한 판례 (OLG Hamm, Urteil vom 15.09.2020 - 4 U 177/19), 적합한 비밀관리성에 대한 기준을 제시한 판례 (LAG Baden-Württemberg, Urteil vom 18.8.2021 – 4 SaGa 1/21, LAG Rheinland-Pfalz Urt. vom 25.1.2021 - 3 SaGa 8/20), 고용계약서에 명시한 포괄규정 (catch-all-clause)은 비밀유지조치에 해당하지 않는다는 판례 (ArbG Aachen Urteil vom 13.1.2022 – 8 Ca 1229/20), 비밀유지조치 기준에 대한 판례 (OLG Düsseldorf Urteil vom 11.03.2021 – 15 U 6/20), 영업비밀로 보호받을 수 있는 기간에 대한 판례 (OVG Münster Urteil vom 04.07.2022 – 15 A 4113/19), 영업비밀보호법을 기초로 청구권을 행사하기 위한 요건에 대한 판례 (OLG Frankfurt am Main, Beschluss vom 27.11.2020 - 6 W 113/20) 등을 들 수 있다.

62) https://www.wko.at/service/wirtschaftsrecht-gewerberecht/schutz-von-geschaeftsgeheimnissen.html

63) 최근 영업비밀보호와 관련된 비엔나 법원의 판결 참조 (OGH Wien, Urteil vom 26.01.2021, 4 Ob 188/20f).

64) 새로운 영업비밀보호 규정과 코로나팬데믹 동안에 원격근무로 인해 발생한 영업비밀 분쟁 사례를 신문보도에서 다루고 있다. GERICHTSREPORTAGE, Prozess um Geheimnisverrat in der Instrumentenbranche, Michael Möseneder 8. April 2022, (https://www.derstandard.de/consent/tcf/story/2000134789239/prozess-um-geheimnisverrat-in-der-instrumentenbranche).

데믹과 관련된 원격근무로 말미암아 발생한 영업비밀 관련 소송이 주목받고 있다. 원격근무로 인해 개인정보와 회사의 기밀에 해당될 수도 있는 영업상 업무 내용을 동일 노트북에 저장함으로써, 영업비밀 유출 또는 폭로로 이어진 분쟁이 현재 진행 중이다.

- 이와 같은 법원에서의 소송은 2016년 EU 입법지침을 수용하여 오스트리아에서 영업비밀보호에 관한 입법체제를 새롭게 갖추었기 때문에 새로운 영업비밀 보호 규정과 코로나 팬데믹 동안에 원격근무로 발생한 영업비밀 분쟁 사례로 주목받고 있는 것이다.[65]

사건 개요

- 3년 반 동안 비엔나 소재 악기 회사의 재무담당이사(CFO)였던, Mr. Z가 2020년 11월 26일에 회사 측과 고용계약을 상호 합의로 해지하였다. 그는 같은 날 저녁 자신의 팩스로 가장 치열한 경쟁상대인 다른 회사에게 대가를 받고 자신이 취득한 그동안의 기업비밀을 누설하고, 향후 정보를 더 제공하겠다는 약속을 하였다는 혐의를 받고 있다. 그는 외국을 위한 기업비밀을 유출했다는 범죄로 기소되었다.

- 현재 Mr. Z는 무죄를 항변하고 있다. 그는 그가 다니던 회사의 사내 분위기는 좋지 않았고, 부서 간 협력이 좀처럼 원활하지 못하였다고 주장하였다. 더구나 코로나 팬데믹 상황에서 자신은 상부의 지시를 받고 직원 150명의 근무시간을 단축시켜야만 했고, 따라서 자신의 이와 같은 혐의는 지난 시기 자신의 업무에서 빚어진 음모라고 주장하였다.

- 퇴직 당일 오전에 그는 기업의 IT 담당자에게 자신의 업무용 휴대폰과 노트북을 반환하였다고 주장했다. 그리고 회사의 IT 담당자가 노트북을 재설정할 수 있도록 그에게 자신의 비밀번호(password)를 알려주었다. Mr. Z는 그동안 코로나로 인한 재택근무를 자주했기 때문에 자신의 인터넷 사용기록에 개인적으로 접속한 사이트들도 함께 저장되어 있었다. 저장되어 있던 비밀번호 중에는 인터넷으로 팩스를 보낼 수 있는 어플리케이션도 깔려있었다. 그리고 이 어플리케이션에 연결된 팩스를 통해 해당 경쟁 회사에게 2통의 팩스가 전송되었는데 그 중 하나는 11월 26일 저녁에, 그리고 다른 하나는 12월 초에 전송된 것으로 나타났다. 첫 번째 팩스 내용은 2013부터 2019년까지 판매한 상품 개수가 기록되어 있었다. Mr. Z는 이 정보는 아무런 가치가 없다고 주장했는데, 위와 같은 정보는 도매상들에게 문의하면 쉽게 파악할 수 있기 때문이라고 그 이유를 설명했다(이하, 기술적인 분쟁 내용은 생략한다).

- Mr. Z는 개인 메일로 회사정보를 다른 경쟁회사로 전송했다는 주장과 재택근무 간에 개인 메일을 회사 업무용 노트북을 통해 사용했으나, 그 내용은 영업비밀에 해당하지 않는다는 주장이다. 현재 오스트리아 법원 담당판사

65) https://www.derstandard.de/consent/tcf/story/2000134789239/prozess-um-geheimnisverrat-in-der-instrumentenbranche

Katharina Bogner는 IT 전문가에게 정보 전달 또는 유출 경로를 파악하도록 의뢰한 상태이다.

라. 평가

- 최근 홈오피스 작업에서의 영업비밀 보호조치의 문제는 코로나 팬데믹 현상과 2019년 이후 유럽에서 새로운 영업비밀보호법이 발효되면서 세계적으로 관심이 주목되고 있다. 유럽에서 2016년 EU 입법지침이 발효된 이후, 이를 수용하기 위해 유럽 회원국들은 자국의 관련 법규를 다듬어 새로운 법적 체계를 갖추었다. 따라서 독일을 비롯한 대부분의 국가에서 '비대면 근무환경'에서의 '영업비밀 침해'가 발생하여 판례로 확립이 되기까지 그 경과를 지켜보아야 할 것이다.

- 또한, 유럽 대부분의 국가에서도 정부 차원에서, 협회 차원에서 또는 기업별로 영업비밀 유지 조치에 심혈을 기울이고 있다. 여기서 소개한 바와 같이 정보 유출 방지를 위해 정신적 인식 고취 및 교육적 차원에서뿐만 아니라, 기술 보안 차원에 이르기까지 다양한 조치가 제시되고 실행하고 있다. 그럼에도 불구하고 코로나 팬데믹 현상에서 빚어지는 홈오피스 작업 시 대처할 정통한 매뉴얼을 갖고 있지 못한 상황이므로 향후 홈오피스를 비롯한 비대면 근무환경에서 이와 관련된 법적 분쟁이 크게 야기될 것이다. 따라서 유럽 국가들의 이에 대한 법적 해결 과정을 면밀히 주시해야 할 것이다.[66]

마. 참고문헌

연구논문

Möhrenschlager in : Wabnitz/Janovsky/Schmitt, Handbuch Wirtschafts- und Steuerstrafrecht, 5. Auflage 2020 Rn. 9-20

Böhm/Brams: Aktuelle Entscheidungen der Arbeitsgerichte zum Beschäftigtendatenschutz, NZA-RR 2021, 521

Lunze/Rektorschek: Auswirkungen von COVID-19, PharmR 2021, 629

Gilga: Beschäftigtendatenschutz und Covid-19: Daten sicher im Homeoffice?, ZD-Aktuell 2020, 07113

Ohly: Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, 441

Kraus/Leister: Daten und Geheimnisschutz im Homeoffice – Schutzkonzept zur Vermeidung von Bußgeld- und Haftungsrisiken, CCZ 2021, 111

Picker: Arbeiten im Homeoffice – Anspruch und Wirklichkeit NZA-Beilage, 2021, 4

Kurt Pärli / Jonas Eggmann, Ausgewählte Rechtsfragen des Homeoffice, Jusletter 22. Februar 2021

66) 현재 유럽에서 홈 오피스를 비롯한 원격 또는 자택근무 등과 관련된 영업비밀 침해에 관한 소송은 아직 미미한 실정이고, 그 내용이나 결과도 대부분 공개되지 않고 있는 실정이다.

Bildhäuser/Reinhardt: Das neue GeschGehG: Systematik, Rechtsprechung
und Unternehmenspraxis, GRUR-Prax 2020, 576
Krüger/Wiencke/Koch: Der Datenpool als Geschäftsgeheimnis, GRUR 2020, 578
Bräutigam/Habbe: Digitalisierung und Compliance – Rechtliche Herausforderung für die Geschäftsleitung, NJW 2022, 809
Stilz: Strafbarkeit des auf digitale Werte bezogenen Insiderhandels auf NFT-Handelsplattformen RDi 2022, 404
Holthausen: Big Data, People Analytics, KI und Gestaltung von
Betriebsvereinbarungen – Grund-, arbeits- und datenschutzrechtliche An- und Herausforderungen, RdA 2021, 19
Wilske/Markert/Ebert: Entwicklungen in der internationalen Schiedsgerichtsbarkeit im Jahr 2021 und Ausblick auf 2022, SchiedsVZ 2022, 111
Generalanwalt beim EuGH (Rantos), Schlussantrag vom 20.09.2022 – C-252/21, BeckRS 2022, 24109
Wysk: Planungssicherstellung in der COVID-19-Pandemie, NVwZ 2020, 905
Klaas: Unternehmensinterne Verstöße und „Whistleblowing“: Zum Grundrechtsschutz der Beteiligten und den Anforderungen an eine einfachrechtliche Regelung, CCZ 2019, 163

참고판례

[독일]

BVerfG, 14.03.2006 - 1 BvR 2087/03
BVerwG, Beschluss vom 05.03.2020 – 20 F 3/19
BGH, Hinweisbeschluss vom 16.12.2021 – I ZR 186/20
OLG Düsseldorf, Beschluss vom 11.01.2021 - 20 W 68/20
LAG Düsseldorf, Urteil vom 03.06.2020 - 12 SaGa 4/20
OLG Stuttgart, Urteil vom 19.11.2020 - 2 U 575/19
OLG Hamm, Beschluss vom 27.01.2021 - 20 W 48/20
OLG Hamm, Urteil vom 15.09.2020 - 4 U 177/19
LAG Baden-Württemberg, Urteil vom 18.8.2021 – 4 SaGa 1/21
LAG Rheinland-Pfalz Urt. vom 25.1.2021 - 3 SaGa 8/20
ArbG Aachen Urteil vom 13.1.2022 – 8 Ca 1229/20
OLG Düsseldorf Urteil vom 11.03.2021 – 15 U 6/20
OVG Münster Urteil vom 04.07.2022 – 15 A 4113/19
OLG Frankfurt am Main, Beschluss vom 27.11.2020 - 6 W 113/20

[오스트리아]

OGH Wien (Urteil vom 26.01.2021, 4 Ob 188/20f).

[영국]

Shenzen Senior Technology Material Co Ltd v Celgard LLC [2020] EWCA Civ 1293

Celgard LLC v Shenzhen Senior Technology Material Co Ltd [2020] 5 WLUK 45 (07 May 2020)

Travel Counsellors Ltd v Trailfinders Ltd [2021] EWCA Civ 38 (19 January 2021)

인터넷사이트

https://www.boehmert.de/update-brexit-und-schutz-von-geschaeftsgeheimnissen-im-vereinigten-koenigreich/

https://www.kosmicon.de/kpmg-studie-zu-wirtschaftskriminalitaet-belegt-notwendigkeit-von-cyber-defense-massnahmen-fuer-kmu-und-onlinehandel/

https://www.cmshs-bloggt.de/rechtsthemen/coronavirus-handlungsempfehlungen-fuer-unternehmen/covid19-schutz-von-geschaeftsgeheimnissen-im-home-office-das-ist-zu-tun/

https://www.bvmw.de/fileadmin/03-Themen/Recht/Dateien/checkliste-10_Tipps_zum_Gescha__ftsgeheimnisgesetz.pdf

https://ey-law.de/de_de/rechtsberatung/catch-all-klausel-ist-keine-angemessene-geheimhaltungsmassnahme

https://gowlingwlg.com/en/insights-resources/articles/2018/trade-secrets-directive-becomes-directly-effective/

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/schutz-von-geschaeftsgeheimnissen.html

https://www.derstandard.de/consent/tcf/story/2000134789239/prozess-um-geheimnisverrat-in-der-instrumentenbranche

https://www.mll-news.com/update-eu-richtlinie-zum-schutz-von-geschaeftsgeheimnissen-tritt-in-kraft/

https://www.srd-rechtsanwaelte.de/blog/krisenratgeber-homeoffice-datenschutz/

https://booster-magazine.ch/know-how/

https://www.boehmert.de/update-brexit-und-schutz-von-geschaeftsgeheimnissen-im-vereinigten-koenigreich/

https://www.infosec.ch/blog/tag/home-office/

http://ukscblog.com/case-comment-vestergaard-frandsen-v-bestnet-europe-2013-uksc-31/

3. 비대면 근무환경에서 영업비밀 보호를 위한 동향 및 정책

가. 영업비밀 보호 강화 사례

지금부터는 실제로 원격근무를 실시하고 있는 기업이 어떤 보안 대책을 세우고 있는지 구체적인 사례를 소개하겠다. 2017년~2019년 사이에 일본 총무성이 실시하고 있는 「원격근무 선구자 백선(テレワーク先駆者百選)」에서 총무대신상(総務大臣賞)을 수상한 사례로부터, 보안 대책에 힘쓰고 있는 아래 3개 기업(NTT東日本, アフラック生命保険株式会社, ネットワンシステムズ株式会社)이 선정되었다.

NTT東日本

동일본전신전화주식회사(東日本電信電話株式会社, NTT東日本) NTT 도코모에서는 2010년부터 근무방식의 재검토를 실시해, 2018년에는 도코모의 본사나 지사에서 약 80%의 재택 근무율을 달성했다. 오피스 워크에 필요한 애플리케이션은 모두 모바일 단말기에서 사용할 수 있으며 플로우 승인이나 스케줄 관리, 웹 회의 등을 간편하게 할 수 있도록 고안되어 있다. 이러한 정보는 일절 단말기에 남지 않는 구조로 되어 있어 보안 대책도 만전을 기하고 있다. 원격근무로 과제가 되는 오피스 워크의 보안이나 구조 만들기가 완성되어 실제로 원격근무를 경험한 사원의 80%가 「평소와 다름없이 업무를 할 수 있었다(通常と変わらず業務ができた)」「생산성이 향상되었다(生産性が向上した)」라고 회답하고 있다.[67] 한편 최근에는 정보보호를 강화하기 위해 클라우드 서비스를 도입하는 것을 추천하고 있는데, 그 이유로 첫째, 기업 규모에 따라 차이가 있겠지만 IT에 정통한 담당자가 없기 때문에 전면적으로 원격근무 보안 사고에 능동적인 대책을 실시하는 것은 어려우며 둘째, 보수나 운용의 필요성은 알고 있지만 막상 추진하기 쉽지 않다는 점을 들고 있다. 이에 NTT東日本은 원격근무 시 보안사고 대책으로 최신의 보안패치와 365일 24시간 감시·대응이 가능한 '클라우드 도입·운용 지원 서비스'를 추천하며 자체 클라우드 도입 및 운영 지원 서비스를 통해 원격근무에 필요한 데이터 환경뿐만 아니라 보안 대책도 포함한 종합적인 지원을 한다고 설명하고 있다.

Aflac Insurance Services アフラック保険サービス株式会社

애플락 생명보험 주식회사(アフラック生命保険株式会社)에서는 원격근무를 시작할 때 모델 부문을 마련해 문제점이나 대책을 밝혀내기 시작함으로써 전사원이 원격근무에 참가할 수 있는 환경이 마련되어 순조롭게 진전되고 있다고 한다. 보안 대책에서는 화상회의 시스템 등 ICT 툴을 정비함으로써 장소를 가리지 않고 안심하고 업무를 할 수 있는 환경을 만들었다. 또한 PC나 USB등의 대여도 실시하고 있어 일정한 보안 기준을 지킨 상태에서 원격근무를 할 수 있도록 고

67) 総務省, 平成29年度テレワーク先駆者百選 総務大臣賞事例のご紹介.

안하고 있다.[68] 그 외에도 원격근무에서 사용하는 툴의 사용법이나 e러닝 등 지식의 공유도 적극적으로 실시하고 있다.

net one

넷원시스템즈 주식회사(ネットワンシステムズ株式会社)는 2011년부터 이용 횟수나 이용자를 제한하지 않는 텔레워크 제도를 도입해 왔다. 전 사원에게 가상 데스크톱 환경을 제공해 어디에 있어도 사무실과 동등한 환경에서 일을 할 수 있도록 고안하였다. 보안 대책으로는 지정한 디바이스의 PC만 사용할 수 있도록 허용하고 구입비는 특별 상여금으로 지급하며 보안을 담보한 후 클라우드 서비스나 인트라넷을 이용함으로써 원활한 업무를 실현했다. 또한 24시간 체제의 헬프 데스크를 설치하여, 원격근무 중 사고가 일어났을 경우에도 즉시 대응할 수 있도록 하고 있다. 보안 대책을 하면서 오피스 근무 등의 환경을 실현함으로써 잔업 시간의 감소 등 업무 체제의 향상으로 이어졌다.[69]

大塚商会

오오츠카상회(大塚商会)에서는 원격근무 상황에서도 영업비밀 보호를 강화하기 위한 다각적인 보안 대책을 마련하여 영업비밀 보호 강화를 하고 있다. 특히 기술적 보호조치에 방점을 두어 정보보호를 강화하고 있는바, 아래와 같은 기술적 운용을 통해 공격자에 대한 초기 침입으로부터 내부 확산방지, 단말기 감염, 서버 통신 간 차단 등 중요정보가 누설로 이어지는 다양한 위험을 회피하는 방안을 마련하고 있다.

- Cyber Cleaner LE(サイバークリーナーエルイー) : 잘못된 통신을 감지하여 자동으로 차단하는 어플라이언스(アプライアンス) 제품으로 인터넷으로부터의 공격이나 내부로부터 인터넷의 부정한 통신을 차단해 표적형(標的型) 공격에 의한 정보 유출로부터 중요정보를 보호한다.

- FortiGate(フォーティゲート) : 외부로부터의 보안 위협과 내부로부터의 정보누설 양쪽으로부터 사내 네트워크를 보호한다. 1대의 몸체에 여러 보안 기능을 탑재하고 있으면서도 가성비가 뛰어난 특징이 있다.

- Palo Alto(パロアルト) : 애플리케이션을 식별하고 제어할 수 있는 차세대 방화벽이다. 바람직하지 않은 애플리케이션 통신을 차단하고 허가된 애플리케이션에 대해서도 위협이 숨어 있지 않은지 체크하여 표적형 공격의 위협으로부터 사내 네트워크를 보호한다.

68) 総務省, 令和元年度テレワーク先駆者百選 総務大臣賞事例のご紹介.
69) 総務省, 平成29年度テレワーク先駆者百選 総務大臣賞事例のご紹介.

나. 영업비밀 보호 동향 및 정책

IPA에 따르면, 원격근무에 대한 대응 내지는 내부자 부정행위에 대해서는 여전히 과제라는 점을 분명히 하고 있다.[70] 원격근무에서의 정보관리 규칙을 정하지 않은 기업이 상당수 존재(29.5%)하고, 사내 규정의 재검토는 진행되고 있지만 개별 피용자 등 퇴직자로부터의 서면 징구는 낮은 수준으로 조사되었다. 원격근무 도입으로 정보의 디지털화, 이른바 탈종이화(페이퍼리스)가 본격화되었고, 앞으로 더욱 가속화 될 것으로 예측되는 가운데 발생 가능성이 있는 정보보안에 대한 대책이 강구되지 않을 경우 기업이 보유한 비밀에 대한 영업비밀 해당성이 훼손될 가능성이 높아질 것이다. 그럼에도 불구하고 이를 계속 방치한다면 최종 수단인 법적 구제마저 불가능하게 될 것이다. 물리적 기술적으로 클라우드를 통한 부정한 정보 유출이 발생했을 경우 로그 기록 확보, 책임 명확화 등의 대책을 강구하고 있는 기업은 극히 일부일 것으로 예상되는바, 최근 비대면 근무환경에서 아래와 같은 정보보안 대책으로 영업비밀을 보호하고 있다.

(1) 영업비밀 보호 동향

가) 다요소 인증(多要素認証)

사내 네트워크나 회사에 있는 PC 등에 접속할 때의 사용자 인증을 철저하게 함으로써 위장에 의한 정보유출 위험을 회피할 수 있다. 이렇듯 인증을 확실하게 하기 위해서는 ID나 패스워드에 PC의 고유 정보나 사용자의 지문 정보 등의 다른 요소를 조합한 인증 방식인 이른바 「다요소 인증(多要素認証)」이 유효하다. 다요소 인증의 구조를 채용하고 있으면 앞서 사례에서 언급한 그림 3.과 같이 ID와 패스워드가 제3자에게 유출되었다고 해도 원격 단말기(원격 리모트워크에서 사용하는 수중 PC)의 하드웨어 고유정보나 피용자의 지문정보 등이 인증 시에 필요하기 때문에 제3자에 의한 부정접속의 위험 가능성은 낮아진다.

나) 원격 단말기기 제한

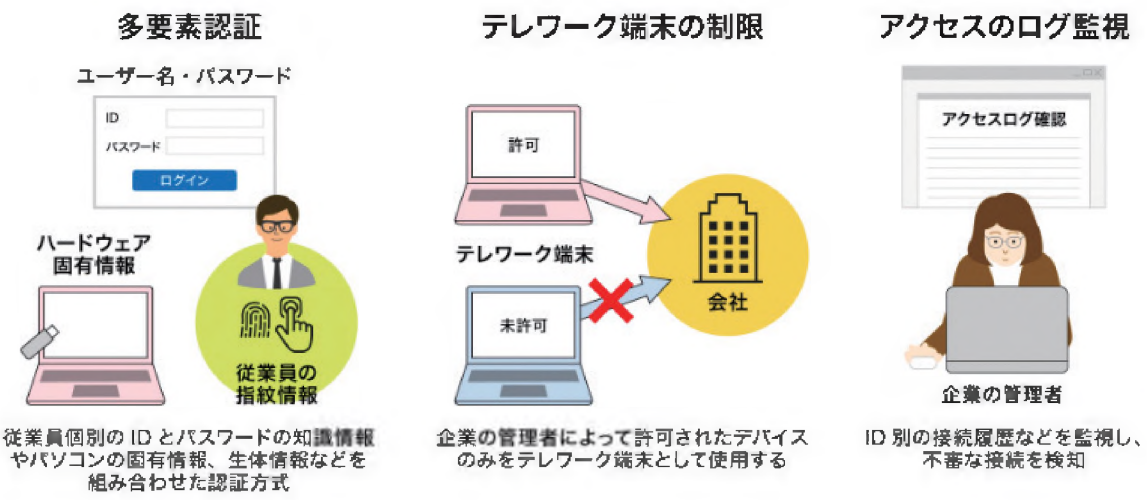
부정 접속(접근) 방지에는 기업의 관리자가 원격 단말기기를 제한하는 방안도 효과적이다. 단말기를 제한한다는 것은 기업의 관리자에 의해 허가된 PC나 태블릿 등의 기기만을 원격 수단으로 사용할 수 있음을 의미한다. 따라서 원격 단말기를 제한하면 위 그림 3.의 경우와 같이 ID와 패스워드가 제3자에게 유출되었다고 해도 기업의 관리자가 미리 허가한 PC를 입수하지 않는 한 악의적 제3자는 사내 네트워크에 접근할 수 없다.

70) 企業における営業秘密管理に関する実態調査 2020調査実施報告書, 独立行政法人情報処理推進機構（実施：みずほ情報総研株式会社).

다) 접속 로그 감시

접속 로그 감시도 효과가 있다. 피용자에게 할당된 ID별의 접속 이력 등을 감시하는 것으로, 수상한 접속의 감시가 가능하다. 제3자에 의한 부정 접속(접근)의 조기 발견이 가능하면, 중요 정보에 대한 누설을 최소한으로 막을 수 있다.

그림 4. 정보 유출 방지에 효과적인 보안 대책[71]



라) 제로 트러스트(ゼロトラスト)

알려진 공격기법에 대한 방어를 염두에 두고 구성된 보안 대책만으로는 충분한 방어가 어려워지고 있다. 따라서 오피스 네트워크 내에 공격자가 침입하는 것을 전제로 보안 대책을 재검증하는 이른바 제로 트러스트(ゼロトラスト)라는 생각에 관심이 쏠리고 있다. 먼저 이 개념은 전술한 바와 같이 다양화되는 시스템 구성이나 이용 형태에 대한 보안 향상이라는 관점에서도 주목받고 있다.

(2) 영업비밀 보호 정책(사람·규칙·기술 3가지의 조화)

COVID-19 대유행으로 인한 봉쇄조치로 사업장이 폐쇄되고 더 많은 피용자들이 홈 VPN 또는 무선 네트워크를 통해 개인 컴퓨터나 휴대폰으로 업무를 처리하면서 해킹에 더 취약할 수 있다는 사실은 누구나 예상할 수 있는 시나리오다. 이런 상황에서 기술에 정통하지 못하고 신기술의 보안 요구사항에 적응하는 데 어려움을 겪는 피용자에 의해(의도와는 무관하게) 관리되는 영업비밀이 유출될 가능성이 높다. 그렇다면 영업비밀 보유자는 영업비밀을 보호하기 위한 합

71) 그림4. 출처 : <https://www.magicconnect.net/column/keyword_vol5.php?utm_source=google&utm_medium=display&utm_campaign=regad&utm_content=pmax&gclid=CjwKCAjw-rOaBhA9EiwAUkLV4mU_OiAWfSPRLA0fORxZfAPxDkyK4n7kGjpsqFOlQD5PZdcvuWdmdRoCjXYQAvD_BwE>,(last visited Nov. 28, 2022).

리적 보호조치와 관련하여 팬데믹 이전에 시행했던 (보안)수준만으로도 충분한 것인가? 아니면 좀 더 엄격한 수준의 조치를 해야 하는가?라는 의문이 들 수 있다. 영업비밀 관리자는 원격근무 정책을 추진하면서 기존 정책을 다시 검토하고 업그레이드해야 할 필요가 있다. 이를테면 비밀계약 검토 및 업데이트, 특정 비밀정보에 대한 접근 추적, 영업비밀 보호 정책에 대한 문서화와 같은 몇 가지 간단한 조치만으로도 기업(회사)의 영업비밀 보호를 크게 강화할 수 있다.

다만 최근 영업비밀 보호 정책수립을 위해서는 어림잡아 대충하는 주먹구구식의 검토와 업그레이드가 아닌 아래의 3가지 측면에서 체계적으로 접근해야 할 필요가 있음이 강조되고 있다.[72]

가) '사람' 측면에서의 접근

정보보안 정책 추진을 위해 크게 「사람」·「규칙」·「기술」 등 3가지로 분류하는데, 이 중 「사람」측면에서의 접근이 가장 실시하기 어려운 부분이라고 할 수 있다. 왜냐하면 아무리 철저한 규칙을 정해도 실제 원격 근무자나 시스템 관리자가 이를 지키지 않으면 규칙에 의한 효과가 발휘되지 않기 때문이다. 특히 원격 근무자는 사무실에서 눈이 잘 닿지 않는 곳(가정 등)에서 작업을 하게 되므로 규칙이 지켜지고 있는지 여부를 기업·조직이 확인하기 어렵다는 점에 유의할 필요가 있다.[73] 따라서 어렵게 정한 규칙을 정착시키기 위해서는 관계자에 대한 교육이나 자기계발을 통해 규칙의 취지를 스스로 이해하고 규칙을 준수하는 것이 자신에게 이점이 된다는 것을 자각하게 하는 것이 중요하다. 또한 원격 근무자가 정보보안에 관한 필요한 지식을 습득하고 있으면 이른바 피싱이나 표적형 공격 등의 피해를 방지할 수 있다. 이는 곧 잘 정비된 보안 규정 등 규칙을 수행하기 위해 피용자 교육이 필요한 이유이기도 하다.

나) '규칙' 측면에서의 접근

업무를 진행함에 있어 정보보안 측면에서 안전한지 여부를 그때그때 판단하고 필요한 대책을 강구해 나가는 것이 반드시 효율적인 것은 아니며, 이 또한 전문가가 아니면 적절한 판단을 내릴 수도 없다. 그래서 '이렇게 일을 하면 안전을 확보할 수 있다'라고 하는 일의 방식을 규칙으로 정해 놓으면 피용자는 규칙을 지키는 것만을 의식함으로써 안전하게 일을 진행할 수 있다. 다시 말해 원격근무를 실시할 경우 오피스 근무와는 다른 환경에서 일을 하게 되므로 보안 확보를 위해 새로운 규칙을 정할 필요가 있다. 따라서 조직으로서 어떤 규칙을 정하고 지켜나가면 좋을지에 대해 임직원간 대화와 협의가 필요하다.

---

72) コラム, "テレワークにおける情報漏洩リスクはどのように防ぐのか？事例からセキュリティ対策を解説", <https://www.magicconnect.net/column/keyword_vol5.php?utm_source=google&utm_medium=display&utm_campaign=regad&utm_content=pmax&gclid=CjwKCAjw-rOaBhA9EiwAUkLV4mU_OiAWfSPRLA0fORxZfAPxDkyK4n7kGjpsqFOlQD5PZdcvuWdmdRoCjXYQAvD_BwE>,(last visited Nov. 28, 2022).

73) 이와 관련하여 사용자는 피용자가 가정에서 일을 하는지 감시하여 원격근무로 인한 프라이버시 문제가 발생하기도 하며 실제로 이러한 문제가 노동문제로 확대되어 일본 법원으로부터 나온 판결이 있다.

다) '기술' 측면에서의 접근

기술적 대책은 앞서 언급한 '규칙'이나 '사람'으로는 대응할 수 없는 부분을 보완하는 것이다. 따라서 어떻게 보면 가장 실현가능한 정책방향이라고 할 수 있다. 기술적 대책은 여러 가지 위협에 대해 '인증', '검지', '제어', '방어'를 자동적으로 실시하는 것으로 원격근무 장소의 환경 다양성을 고려하여 각각의 환경에서의 정보보안 유지를 위해 적절히 대책을 강구해 둘 필요가 있다.

이렇듯 비대면 근무환경에서의 영업비밀 보호 정책은 ①사람 ②규칙 ③기술 등 3가지 방향에서 종합적·체계적으로 접근하는 방법으로 추진되어야 하는바, 이를 구체적으로 풀어 정리하면 아래와 같다.

- 원격근무를 해야 할 경우
  - 개인용도의 PC 등 전자 단말기 접속 제한을 실시하여야 함
  - 자택이나 공공장소의 네트워크 회선을 사용하지 않고 회사 대여 Wi-Fi 단말기만을 사용하여야 함
  - 기존에 사용하던 비밀유지 계약을 검토하여 최신의 것으로 업데이트 하되, 원격 작업 계약서는 사용자가 피용자에게 요구하는 사항을 구체적으로 명시한다.

- 이러한 계약서는 적절한 인사 파일과 계약 관리 시스템에 저장되도록 하고. 비밀로 관리하는 정보에 접근 할 수 있는 직원, 협력업체 또는 잠재적인 비즈니스 파트너는 모두 비밀유지계약에 따르도록 주지시켜야 한다.

- 사용자는 원격근무 계약을 통해 피용자가 지켜야 할 사항, 즉 비밀유지 의무에 대해 반복하여 교육하여야 한다. 아울러 원격 등 재택 작업 환경에 대한 사용자의 피용자에 대한 기대치를 설정하고, 정보보호의 중요성을 반복하며 네트워크 허용범위의 사용 정책을 반복하여 교육한다.

- 원격작업 시 이중 요소 인증을 사용하는 보안 VPN을 통해서만 원격 접근이 허용 되도록 한다. 특히 민감 정보의 경우 사용자는 개별화된 워터마크, 접근 로깅 및 기타 전자 보안 기능을 구현할 수 있도록 한다.

- 정보의 중요도에 따라 접근권한을 회사의 고위 임원으로 차등화하는 작업을 고려할 수 있다. 또한 특정 정보에 대한 접근을 위해 결정을 내릴 담당자를 지정한다. 이렇게 하면 업무상 중요한 이유로만 정보가 제공되고, 접근 기록이 유지된다.

- 사용자는 피용자가 퇴사할 때에는 이른바 퇴사 인터뷰를 시행하여 비밀로 관리되는 정보가 반환됐는지 확인하며, 부득이한 경우 가상공간을 통해서라도 퇴사하는 직원을 만나야 한다.

- 협력업체 및 파트너에 대한 지침을 업데이트하고, 제3자와의 비밀정보 공유는 비밀유지계약에 따르도록 한다.

Ⅳ. 결론

첨부1. 영업비밀 보호 가이드라인

첨부2. 직무발명(직원소유) vs 영업비밀(회사소유)

첨부3. 비대면 근무환경에서 영업비밀 보호를 위한 조치

Ⅳ. 결론

영업비밀 침해행위는 경제적 이득을 목적으로 하는 재산적 침해 및 범죄의 특성을 띠고 있다. 따라서 침해행위로 인해 얻는 이득이 발각되어 치러야 할 대가보다 크면 발생할 소지가 높다. 그런데 본 조사결과 중소기업의 경우 법원에서 요구하는 영업비밀 유지관리 수준을 충족하는 데 여전히 어려움을 겪고 있고, 침해행위자 입장에서는 영업비밀 침해행위를 통해 얻을 수 있는 이득에 비하여 손해배상액수나 처벌 수위가 낮아 범죄에 대한 위하(威嚇)력이 약한 것으로 확인되었다.

기업은 많은 시간과 노력을 투자하여 기술 또는 경영적인 정보를 개발하고 축적한다. 그리고 그러한 정보를 영업비밀로 보호하여 장기 지속적인 발전을 꾀한다. 하지만 영업비밀의 침해와 유출은 이런 기업의 노력을 한순간에 물거품으로 만들어버린다는 점에서 그 해악은 이루 말할 수 없다. 따라서 기업은 영업비밀 침해 방지를 위해 관리시스템을 미연에 구축하여 놓고, 정부는 침해행위에 대한 신속하고 효과적인 구제가 이루어질 수 있도록 제도적인 개선에 진력해야 할 것이다.

주지하다시피 영업비밀 관리의 수준에 관해 개정 전 법률에서 "합리적인 노력"으로 규정하였음에도 불구하고 가시적인 변화가 보일 정도는 아니어서 "비밀로 관리"로 변경하였으나, 아직 관련 판결이 충분히 선고되지 않은 관계로 향후 추이를 지켜볼 필요가 있다. 또한 코로나19 팬데믹이 촉발한 비대면 디지털 근무환경을 맞이하여 정부는 선제적으로 대응책을 마련해야 하겠다.

이에 본 연구는 최근 5년간 법원에서 선고된 영업비밀 관련 민·형사 판결을 전수 분석하여 영업비밀 3요소와 비밀관리성 쟁점을 조사하였고, 미국과 일본, 유럽에서 비대면 근무환경에 관한 최신 법제도 및 동향 조사를 통해 국내법의 제도 개선과 사법기관에 제시할 시사점을 발굴하였다. 그 결과 기업의 사용자와 피용자, 그리고 수사기관과 사법당국이 영업비밀 관리성 여부를 판단함에 도움이 될 수 있는 가이드라인을 마련하였다.

깊은 샘에서 물을 퍼 올리려면 한 바가지의 마중물이 필요하다. 본 연구를 통해 소개된 미국과 일본·유럽의 최신 사례와 판례·동향을 통해 비대면 근무라는 변화된 환경을 맞이하여 정부가 어떤 방향으로 제도를 개선해야 할지 알려주는 이정표가 되기 바란다.

또한 본 연구에서 제시한 가이드라인을 통해 우리 기업들의 영업비밀 관리 시스템 구축에 실천적인 도움이 되기를 기대한다.

첨부1. 영업비밀 보호 가이드라인

사용자·피용자가 지켜야 할 영업비밀 보호 핵심 요소 및 관리방안

영업비밀 보호 가이드라인

— 사용자·피용자가 지켜야 할 영업비밀 보호 핵심 요소 및 관리방안을 중심으로 —

【① 사용자가 지켜야 할 영업비밀 핵심 요소 및 관리방안】

[회사의 자산 보호]

1. 기본사항 : 비밀유지약정을 체결하거나 보안서약서를 징구하라!

- 보안서약서조차 징구해두지 않았다면 인적 관리를 한 것으로 인정받기 어려움

"약정서 없이 근로계약서 부수의무 등을 주장하는 것으로는 영업비밀로 인정받지 못한다."

2. 비밀서약서는 추상적 문구가 아닌, 함축적이고 구체적인 사항으로 특정 하라!

흔히 기업비밀 보호서약서, 독점정보 약정서, 윤리 경영 실천 서약서, 정보보호 서약서, 비밀약정서 등의 이름으로 작성되는 서약서는 그 내용이 포괄적이고 추상적이면 이를 준수해야하는 자(피용자) 입장에서는 무엇이 비밀로 유지·관리되고 있는 것인지 알기 어려울 수 있다. ex) "일체의 회사 내 업무상 정보나 비밀을 유출하지 않겠다."

아울러 서약서의 내용이 포괄적이고 추상적이면 최후의 수단인 법적 절차에서도 무엇이 관리되는 정보인지 입증이 곤란하다.

- 수원지방법원 성남지원 2017카합50049 결정

〈참고판례 : 서울중앙지방법원 2020가합519081〉

이 사건 채무자는 채권자를 퇴사한 이후에도 채권자의 업무용 이메일 계정을 사용하면서 채권자의 업무용 이메일 계정에서 채무자 개인의 이메일 계정으로 채권자의 중요한 영업비밀에 해당하는 고객의 자산현황 정보, 입찰제안서 등을 유출하여 영업을 위하여 사용하였다. 그런데 채무자는 채권자와 근로계약 체결 당시 아래와 같이 독점정보 약정서를 작성하여 제출한 사실이 있다.

- 독점정보 약정서 -

• 채권자와의 고용관계로 인해 채무자가 채권자에 중요한 가치가 있는 기밀이나 독점정보를 개발 또

는 지득하거나 그러한 정보에 접근할 수 있음을 인정한다. 이에 채무자는 고용조건으로, 채권자에 고용되어 있는 한 다음의 사항들을 준수할 것에 동의한다.

- 채무자가 채권자에 고용됨으로써 영업상 유리한 고지를 채권자에 부여하는 기밀, 독점 또는 영업비밀의 성격을 가진 특정 정보에 관하여 채권자와 채무자 사이에 확신과 신뢰의 관계가 형성된다. 본 약정에서 모든 기밀, 독점 및 영업비밀 정보는 '독점정보'라고 한다.
- 독점정보란 다음의 사항을 포함하되 이에 국한되지 아니한다.

채권자에 의해 또는 채권자를 위해 개발하거나 라이센스한 모든 소프트웨어와 기타 기술(중략) 고객 정보를 포함하는 모든 정보를 포함하나 이에 국한되지 않는다. 마케팅과 영업계획, 제품 개발 계획, 경쟁력 분석, 벤치마크 검사결과, 사업 및 재정계획과 예측, 비공식적인 재무정보, 합의서, 채권자의 고객과 직원 명단, 계약서, 계약서신, 주문서, 승인서 양식과 승인단계, 자문제안, 입찰, 작업현황, 가격제안과 견적 또는 구매주문 등

이에 법원은 채권자가 채무자를 포함한 임직원들로부터 이 사건 독점정보 약정서를 징구하고 있는 점은 인정하면서도 채권자가 직원들로부터 징구하는 위 독점정보 약정서의 내용이 포괄적이고 추상적이어서 직원들이 해당 약정서의 기재만 보고 위와 같은 정보들이 비밀로 유지, 관리되는 대상이라고 인식하기는 어려울 것으로 보인다는 점을 들어 이 사건 정보가 부정경쟁방지법 제2조 제2호의 영업비밀에 해당한다고 보기 어렵다며 채권자의 신청을 기각하였다.

3. 회사 업무관련 파일의 보관책임자를 지정하고, 중요도에 따른 분류 또는 대외비 표시를 하라!

- 법원은 '접근대상자나 접근방법 등을 제한하기 위한 별도의 조치를 취했는지 여부'를 비밀관리성 판단하는 근거 중 하나로 삼고 있다.

- 서울동부지방법원 2016가단136874 판결

이 사건에서 원고는 (원고 회사)퇴직자인 피고들이 원고의 영업비밀인 "Tizen TV 내장형 매뉴얼의 프로토타입"(이하 프로토타입 기술)을 이용하여 Tizen OS의 내장형 매뉴얼 제공 사업을 수주하고, 역시 원고의 영업비밀인 "DITA를 이용한 InDesign 자동 조판 기술" (이하 DITA 기술)을 이용하여 영업을 하는 등 원고의 영업비밀을 침해하고 이 사건 약정에 따른 비밀유지서약 내지 전직금지약정을 위반하였다고 주장하며 부정경쟁방지법 제11조에 따른 손해배상책임 또는 이 사건 약정상 비밀유지서약 위반에 따른 손해배상책임을 주장하였다.

이에 법원은 프로토타입 기술 및 DITA 기술 및 거래처 명단 등이 부정경쟁방지법상 영업비밀에 해당하는지에 관하여 판단하였는바, 원고 회사는 프로토타입 기술 및 DITA 기술에 대하여 보관책임자를 지정하거나 비밀 또는 보안을 유지할 필요가 있는 대상이라고 별도의 표시(중요도에 따른 분류 또는 대외비, 기밀자료의 표시)를 하지 않았다고 지적하였다. 즉 피용자들이 취득 사용한 회사의 업무 관련 파일은 회사 내에서 일반적으로 자유롭게 접근/열람/복사할 수 있었고, 따라서 원고 주장의 정보는 비밀로 유지되었다고 볼 수 없다며 판단 근거를 제시하였다.

결국 법원은 원고의 프로토타입 기술 및 DITA 기술이 부정경쟁방지법 제2조 제2호에 정한 영업비밀에 해당하지 않는다며 원고의 청구를 기각하였다.

4. 비밀로 관리하기 위한 일련의 정책들, 이를테면 대외비 표시 문구는 사후적으로 쉽게 만들 수 없는 것으로 기안하라!

- 부산지방법원 2015가합44659 판결

법원은 영업비밀로 관리되었다고 주장하는 회사의 중요정보에 대하여 지켜지고 있는 다양한 보안조치(예컨대 '원고로부터 취득한 도면 및 금형 등을 이용하여 원고 회사 외에 타 회사에 기술을 유출하거나 공급할 경우 민형사상 이의가 없음을 협약합니다'라는 내용의 협약서를 제출 받은 사실, 원고가 원고 회사 사무실 내에 CCTV를 설치한 사실)에도 불구하고, 도면에 표시된 '대외비' 표시가 사후적으로도 쉽게 만들 수 있는 것으로 보인다고 하면서 비밀관리성을 부정한 바 있다.

"원고가 제출한 도면에 존재하는 '대외비' 표시는 사후적으로도 쉽게 만들 수 있는 것으로 보이고, 원고가 주장하는 영업비밀 침해 기간 동안 피고에게 이 사건 도면이 비밀이라고 인식될 수 있도록 고지를 하였다거나 이 사건 도면이 대외비로 관리되고 있었다는 점을 뒷받침할 다른 증거를 제출하고 있지 못한 점"

따라서 피용자의 비밀침해 행위 이전부터 꾸준히 비밀로 관리되고 있었다는 점을 입증하기 위해서는 비밀로 관리하기 위한 일련의 정책들이 사후적으로 추가·삭제·수정 등의 방법으로 급조될 수 없는 방법들로 추진되어야 한다.

5. 영업비밀 관리규정을 제정하여 동종의 경쟁업체로 하여금 자사의 경영상 정보가 비밀로 유지·관리되고 있다는 사실을 인식 가능하도록 하라!

- 부산지방법원 2017가단317132 판결

원고는 자신들의 '거래처별 단가 및 적용 할인율'(이하, 이 사건 경영상 정보)은 국내에서 수십 년간 "해도(海圖, charts)[74]" 판매를 하면서 수입처 인증, 거래처별 거래기간 등을 고려하여 작성한 노하우에 해당하는 영업자산으로서 영업비밀에 해당한다고 주장한다. 그런데 피고는 원고 회사에서 퇴사하면서 원고들의 이 사건 경영상 정보를 유출한 후 소외 회사로 이직하였고, 원고에서 하던 업무와 동일한 업무(해도 판매)를 하면서 거래업체들에게 원고들의 단가 및 할인율보다 적은 금액으로 판매를 제의했다. 이에 원고는 기존 거래업체로부터 항의를 받고 피고들이 제시한 금액 상당으로 추가 할인된 금액으로 판매할 수밖에 없었고, 거래처별로 추가할인을 요청받아 손해가 발생했다며 추가 할인율에 따른 손해의 배상을 구하기 위해 이 건 손해배상 청구를 하였다.

이에 법원은 부정경쟁방지법이 규정한 영업비밀로서 보호되기 위해서는 원고들이 거래하는 거래처별로 다른 단가와 다른 할인율이 적용되는 특정된 이 사건 경영상의 정보가 존재하고 객관적으로 그 정보가 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태에 있어야 하는데, '해도(海圖, charts) 등 품목을 매입해 오는 제품의 원가는 회사 내에 사용 중인 프로그램에서 한 번에 알 수는 없고, 각각 개별적인 업무 내에서 개별적인 판매 품목에 접근했을 때 "매입가"로 표기되는 항목을 원고 대표가 지정하는 원가이다'라고 진술한 사실에 주목했다.

따라서 법원은 원고의 이 사건 경영상 정보는 여러 품목별로 산재된 정보로서 원고가 거래하는 거래업체들과의 계약서를 취합하여 알 수 있는 정보로 그 정보가 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태에 있다고 보기 어렵다고 하였다.

6. 영업비밀 보호 및 누출방지에 관하여 정기적, 비정기적 교육을 실시하라!

- 교육의 방식은 집합교육이 가장 바람직하되 입증할 수 있어야 함(교육을 받은 기억은 없다고 임직원이 진술하여 패소한 사례가 있음)

74) 바다 속에 직접 들어가 보지 않고도 그곳에 무엇이 있는지 각종 정보를 수록해 놓은 것이 있는데 이를 해도(charts)라고 한다. 해도에는 바다의 깊이, 해저의 지질, 섬의 모양, 장애물, 해류나 조류의 성질, 해안의 지형, 항로 표지, 등대나 부표 등 바다를 항해하는 데 필요한 여러 가지 사항이 기록되어 있다.

- 창원지방법원 2021노654 판결

"규정 등 관리 조치들 있으나 직원은 법정에서 진술하면서 '보안교육 없었고, 대외비도 일률적으로 다 찍었다"고 진술하였으나, 법원은 비밀관리를 하였다고 믿기 어렵다고 판단하여 영업비밀성을 부정하였다.

7. 업무용 기본 인프라는 회사 소유로 제공하라!

- 관련판례 : 대구지방법원 2019노398 판결

"먼저 피고인의 노트북에 저장되어 있었던 별지 범죄일람표 기재 각 자료(이하 '이 사건 각 자료'라고 한다)가 피해회사의 합리적인 노력에 의하여 비밀로 유지된자료인지에 관하여 살펴보건대, 원심 및 당심에서 적법하게 채택하여 조사한 증거들에 의하여 인정되는 아래와 같은 사정들 즉, ① 피해회사는 설립 당시부터 상당한 기간 동안 업무를 위한 컴퓨터를 별도로 마련하지 않아 피고인 개인 소유의 노트북 컴퓨터를 업무용으로 사용하였고 , 그에 따라 이 사건 각 자료 등 업무용 자료들이 자연스럽게 피고인의 노트북에 저장된 점, ② 위 노트북 컴퓨터에는 비밀번호가 설정되어 있거나 별도의 잠금장치도 없었고, 피해회사의 작업장에는 위 노트북 컴퓨터 외에 다른 컴퓨터가 없어 업무시간 중에는 피고인 외에도 피해회사의 직원들이 업무용 또는 개인용도로 위 노트북 컴퓨터를 사용한 것으로 보이는 점, ③ 위 노트북 컴퓨터에 저장된 업무용 자료에 관하여 별도로 권한 없는 사람의 접근이 제한되도록 관리되거나 비밀로 분류·표시하여 관리되는 등의 조치도 없었던 것으로 보이는 점, ④ 피고인은 피해회사에 근무하는 중에도 위 노트북 컴퓨터를 소지하고 퇴근하는 등 이를 반입·반출하는 데 있어서 별다른 제한이 있었던 것으로 보이지도 않는 점, ⑤ 피해회사와 피고인 사이에 별도의 명시적인 비밀유지 약정이 있었다거나 피해회사에 보안관리에 관한 내부 규정 등이 있었다는 자료가 없고, 고소인의 진술 외에 피해회사가 직원들에게 보안교육을 하였다는 객관적인 자료도 없는 점 , ⑥ 피해회사는 원청회사의 공장 내부에 위치하였는데, 출입문에 시정장치가 설치되어있기는 하였으나 대부분 잠금이 해제된 상태에 있었고 실질적으로 출입통제가 이루어지지는 않은 것으로 보이는 점 등을 종합해 보면, 이 사건 각 자료가 합리적인 노력에 의하여 비밀로 유지된 자료라고 보기 어렵다."

8. 기술적 보안장치인 VDI 시스템에서 실행되는 보안조치와 회사의 정보보호 규정을 혼동하지 말라!

- 서울중앙지방법원 2016노4792 판결

VDI(virtual desktop infrastructure) 시스템을 적용하여 원격근무를 할 경우 권한 있는 자만이 인증 절차를 거쳐 시스템에 접속할 수 있고, 가상 컴퓨터에 저장된 파일은 승인절차 없이는 외부저장장치에 저장할 수 없다. 또한 이러한 시스템 하에서는 외부메일로 파일을 전송할 경우 필터링이 되는데, 이 모든 보안조치는 VDI 시스템에 저장되는 모든 파일에 대하여 일반적으로 적용되는 것일 뿐 이러한 조치를 취했다고 비밀로 유지하였다고 볼 수 없다. 즉 피해 회사의 정보보호 규정에 따르면 보안 규정으로 정보보호 서약서 외 비밀문서에 '대외비' 표시를 하도록 하고 있으나, 이 사건 자료에는 이와 같은 표시가 전혀 되어 있지 않았다.

따라서 기술적인 시스템 상 보안이 잘 지켜졌다고 하더라도 이는 시스템 설계상 당연히 이뤄지는 보안 절차일 뿐, 회사의 정보보호 규정을 지키지 않아도 되는 것은 아니다. 즉 시스템 상 기술적 보안조치와 사내 정보보호 규정은 함께 준수되어야 한다.

9. (개인용)외장 저장장치에 의한 파일 복제 및 유출 방지, 퇴직자 계정의 접근 제한 등을 위한 대책을 수립하라!

- 수원고등법원 2020나13492 판결

피고는 경쟁회사로 이직할 것을 염두에 둔 상태에서 원고 회사의 변속기 검사장비제작과 관련된 기술상의 정보가 담긴 파일을 외장하드에 저장해두었다. 피고는 원고 회사가 저장매체의 반납을 요청하자 추후 외장하드를 반환받아 복구할 의도로 '빠른 포맷'을 하여 반납하였으며 이후 원고 회사로부터 외장하드를 돌려받아 중국 소재 컴퓨터 전문업체를 통하여 자료를 복구하였다. 피고는 경쟁회사로 이직한 후 복구한 자료를 수주업무에 사용하였고, 담당직원 및 엔지니어에게 파일을 전송하여 누설하였다.

따라서 퇴직자로부터 반환받은 개인용 외장하드 등 저장장치에 회사의 중요정보가 저장되어 있는지 확인 할 경우 단순히 중요 파일이 삭제되었다는 점만 확인할 것이 아니라, 향후 복구가 불가능하도록 조치를 취해야 한다. 이를테면 피용자가 퇴직 시 근무기간 동안 사용한 개인 저장매체에 대한 물리적 파쇄

또는 디가우징[75] 방법으로 포맷 시키는 등의 방지대책이 필요하다.

10. 신규채용인의 적법한 자료사용 등에 관한 관리감독을 확실히 하라!

- 수원지방법원 안산지원 2019고단3178 판결

- 피용인의 영업비밀 침해행위에 대해 사용자(새 직장)의 법적 책임을 인정한 사례로서 "법인 피고인의 양벌규정적용 및 항변" 등에 대해 상세하게 판단
- 법인이 영업비밀 침해행위 사전예방 주의감독 의무를 소홀히 한 책임을 인정

"채용 시 영업비밀 침해금지 서약서를 징구한 사실은 있으나, 서약서만 징구하고 그 이행 여부를 확인하지 아니하였으며, USB등 이동식 저장매체의 사용을 제한하지 않은 점 등을 감안할 때 상당한 주의의무를 이행하지 않았다"

"양벌규정에 있어서 법인이나 사용인 등이 상당한 주의 또는 관리감독 의무를 게을리 하였는지 여부는 당해 위반행위와 관련된 모든 사정 즉, 당해 법률의 입법 취지, 처벌조항 위반으로 예상되는 법익 침해의 정도, 그 위반행위에 관하여 양벌조항을 마련한 취지 등은 물론 위반행위의 구체적인 모습과 그로 인하여 실제 야기된 피해 또는 결과의 정도, 법인의 영업 규모 및 행위자에 대한 감독가능성 또는 구체적인 지휘감독관계, 법인이 위반행위 방지를 위하여 실제 행한 조치 등을 전체적으로 종합하여 판단하여야 한다.

증인 H , L, O의 법정진술과 서약서 (검사 신청 증거서류 등 목록 순번 97) 의 기재 등에 의하면, 피고인 A가 H 등을 채용함에 있어 기존 회사의 영업비밀, 지적재산권 등을 침해하지 않겠다는 취지의 서약서를 징구한 사실을 인정할 수는 있다. 그러나 피고인 A가 경쟁관계에 있는 피해회사에 근무하고 있는 직원들을 단기간에 채용함에 있어서 위와 같은 내용의 서약서만을 징구하고(더구나 H 등이 영어로 기재되어 있는 서약서의 내용을 충분히 이해했다고 보기 어려운데도 이를 제대로 이해하였는지에 관한 조치를 취하지도 않았다), 이동식 저장매체를 사용하는데 별다른 제한을 두지 않아 H으로 하여금 손쉽게 피해회사의 영업비밀 자료가 저장된 휴대전화를 피고인 A에서 사용하는 업무용 노트북에 연결하여 사진 파일을 복제, 저장할 수 있도록 한 것을 두고 영업비밀 침해행위를 방지하기 위한 상당한 주의와 감독을 게을리 하지 아니한 경우에 해당한다고 보기 어려우므로, 이 부분 주장 또한 받아들이지 않는다."

75) 강력한 자기장을 이용해 하드디스크에 저장된 데이터를 물리적으로 삭제하는 기술로, 사실상 데이터 복구가 불가능한 방법이다. 일반적으로는 하드디스크의 파일을 지워도 흔적이 남기 때문에 복구 프로그램을 돌리면 복원이 가능하다. 하지만 디가우징은 디가우저라는 박스형 장치에 하드디스크를 넣어 모든 기록을 영구 삭제시키기 때문에 복구가 불가능한 것으로 알려져 있다.

【② 임직원이 지켜야 할 영업비밀 핵심 요소 및 관리방안】

<법적 분쟁으로부터의 예방>

회사의 임직원은 아래 사항들을 이행하거나 회사에 제안함으로써 본인에게 닥칠 법적 위험까지도 미연에 예방하는 효과를 가져 올 수 있음

1. 절대 비밀번호를 공유하지 않도록 하라!

- 비밀번호는 정보보호에 가장 기본적인 사항이기는 하지만, 의외로 지켜지지 않는 경우가 있다.

- 의정부지방법원 2017가합56117 판결

이 사건에서 원고는 자신이 개발한 메뉴(이하 '이 사건 레시피')의 제조법이 부정경쟁방지법 제2조 제2호에 따른 영업비밀에 해당한다고 주장하며 피고들이 이 사건 레시피를 비밀로 유지해야 할 의무가 있음에도, 가맹계약을 체결할 것처럼 원고를 기망하여 부정한 방법으로 이 사건 레시피를 알아내어 자신들의 영업에 그대로 사용하여 영업비밀을 침해하였다고 주장하였다. 즉 피고들이 원고의 웹하드에 자유로이 접속하여 이 사건 레시피를 부정한 방법으로 취득하였다는 취지로 주장하였다.

그러나 법원은 피고들이 이 사건 레시피를 부정한 방법으로 취득하여 사용하였다고 보기 어렵다고 판단하여 원고의 청구를 기각하였는데, 그 이유 중 하나가 피고 배우자와 컴퓨터 비밀번호 및 웹하드 비밀번호를 공유하였다는 점이다. 비록 원고는 피고에게 직접적으로 이 사건 레시피가 저장된 컴퓨터 등의 비밀번호를 공개하지는 않았지만, 피고의 배우자인 소외인에게 공개한 사실이 있었고 법원이 이를 지적하며 영업비밀을 부정하였다. 이는 영업비밀 성립요건인 비밀관리성과 비공지성을 충족하지 못한 것으로 중요정보를 관리해야하는 사용자 입장에서는 각별히 주의해야 할 사항이다.

2. 입수하게 된 정보의 출처를 확인하라! – 적법한 정보사용인지 반드시 확인하라

- 의정부지방법원 고양지원 2019고단3415 판결 : 가맹점 관련 식자재 단가를 입수하고 사용한 것이 문제된 사례
- 스스로 부정취득 또는 계약위반 행위를 한 것이 아니라, 비밀성 자료를 취득한 것을 기화로 활용한 것을 형사 처벌한 예
- 항소심도 유죄 유지

"피고인은 2018. 5.경 피해자 주식회사 E에서 운영하는 'F'이라는 상호의 음식점 가맹점을 운영하는 성명 불상자로부터 피해자 회사에서 가맹점 주들에게 제공하는 영업비밀인 'F 식재료공급단가'를 수기로 기재한 문건을 소지하게 된 것을 기화로 위 회사 가맹점주들을 찾아가 위 단가표보다 낮은 가격으로 식재료를 공급해주는 방법으로 거래처를 확장하고자 2018. 6. 4.경 고양시 소 F 일산중산점에서 해당 가맹점을 운영하는 G에게 위와 같이 소지한 식재료 공급단가를 정리한 문건을 제시하는 등 같은 날부터 같은 해 6.경까지 별지 1 범죄일람표 기재와 같이 총 4개 가맹점주들에게 피해자 회사에서 공급하는 식재료의 단가보다 자신이 더 낮은 가격에 공급한다는 점을 알려 가맹점주들에게 식재료를 공급하기 위하여 4개의 가맹점들을 상대로 총 4회에 걸쳐 영업비밀인 'F 식재료공급단가'를 사용하였다. 이로써 피고인은 부정한 이익을 얻거나 피해자 회사에 손해를 입힐 목적으로 영업비밀을 사용하였다."

3. 직무와 관계된 영업비밀 관리 시스템 이행 여부를 점검하라!

- 영업비밀 유출 관련 보고 시스템과 규정이 갖추어져 있는지 점검하라
- 본인의 직무와 관계된 영업비밀의 범위를 조사하고 파악하라
- 직무 관련 영업비밀의 유출 가능성을 식별하고, 가능성을 점검하라
- 영업비밀 유출 취약점을 회사에 정식으로 보고하고, 기록을 남겨라

4. 전직 시 회사에 정확하게 알리고 가급적이면 전직 동의서를 확보하라!

- 전직으로 인하여 회사에 손해가 발생할 가능성이 있는지 여부를 점검하라
- 동의를 받을 수 없더라도, 적어도 거짓 진술을 하지는 말라
- 업무 인수인계를 위한 행동강령, 방침과 절차를 이행하라

5. 퇴사 시 기존 회사에서 사용하던 문서와 각종 전자기기는 신속하게 반환하고 개인용 외부저장 기기에 저장된 파일을 포맷하라!

퇴사(또는 이직)시 기존에 사용 중이던 각종 문서(documents, notebooks, files), 랩탑(laptops), 썸 드라이브(thumb drives), 외장 하드 드라이브(external hard drives) 또는 기타 회사 전자 단말기기를 즉시 반환한다. 재직 당시 개인용 외부 저장기기는 복구가 되지 않도록 포맷 처리하고 이를 회사 보안담당자에

게 확인시키도록 한다. 혹시라도 개인용 저장기기를 복구하는 과정에서 전 회사의 정보가 발견되었다면 인지한 즉시 삭제한다.

6. 원격 화상회의 시 참석자의 신원을 파악하고, 해당자에게만 비밀번호를 부여하라!

- 화상회의에서는 정보 유출이 빈번하게 일어날 수 있는 만큼 링크전송 과정에서부터 암호 설정까지 참가자의 신원을 확실하게 점검하는 것이 필요하다.

- Smash Franchise Partners, LLC v. Kanda Holdings, Inc.

이 사건은 미국 델라웨어 법원에서 나온 판결이지만, 만일 이와 유사한 사안이 국내에서 발생하였다고 하더라도 동일하게 판결하였을 것으로 판단되는 팬데믹 시대의 주요 사건이라고 할 수 있다.

이 사건에서 Smash Franchise Partners(이하, '원고')는 '모바일 쓰레기 압축기(mobile trash compactors)' 기술을 보유하고 있는 가맹본부이고, Kanda Holdings, Inc.(이하 '피고')는 원고의 사업에 관심을 보이며 원고가 개최한 줌 회의에 참여한 자이다. 사실 피고는 원고와 가맹계약을 체결하기 보다는 원고와 경쟁관계에 있는 회사를 설립할 목적으로 줌 미팅에 참여한 것으로 원고 가맹사업에 관심이 있는 척하며 줌 미팅 중 원고의 중요정보 수집을 시도한 것이다. 이에 원고는 피고를 상대로 NDA에 따른 계약 위반과 영업비밀 침해를 이유로 하는 예비 금지명령 신청을 했다. 그러나 법원은 피고의 행위가 부당하다고 지적하면서도 원고가 회의 접속을 위한 비밀번호를 부여하지 않았다는 점, 관리자가 미팅 참석자를 허락할 때까지 배제하는 줌 "대기실(waiting room)" 기능을 사용하지 않았다는 점, 관리자가 회의 참석에 부적절한 사람들을 제거하도록 요구하는 자체 절차를 따르지 않았다는 점 등의 이유로 줌 회의 시 공개한 품목별 가맹사업에 필요한 초기 투자 등 정보는 더 이상 비밀로서 관리되었다고 볼 수 없다고 판단하여 원고의 금지명령을 기각하였다.

따라서 원격회의를 개최하는 과정에서 줌 관리자는 허가받지 않은 자의 참여를 막기 위해 암호를 요구하는 비공개 회의를 개최하여야 하며 필요시 회의 중이라고 하더라도 참석 대상자가 맞는지 참석자 신원을 점검할 필요가 있다.

7. 중요정보를 공유 폴더에 보관하지 마라!

- 백 번의 철통보안을 유지했어도 단 한 번의 느슨한 관리는 앞선 모든 노력을 물거품으로 만들 수 있다.

- 서울중앙지방법원 2016가단5165584 판결

〈참고판례 : 서울중앙지방법원 2020가합519081, 서울중앙지방법원 2018가합587135〉

원고 회사의 퇴직자인 피고는 원고 회사의 국내 거래처 정보, 공급자·별거래처별 판매수수료 등 원고의 영업비밀을 취득한 상태에서 원고 회사를 사직하고 곧바로 원고와 관련 회사이며 경쟁 회사로 이직하여 위 영업비밀 등을 사용함으로써 원고의 영업비밀 등을 침해하였다. 이에 원고는 이 사건 손해배상 청구를 제기하였다.

그러나 법원은 원고 회사가 영업비밀 보호를 위해 철저한 보안을 유지했다고 인정하면서도 단 한 번의 이해할 수 없는 관리시스템에 문제를 지적하며 비밀관리성을 부정하였다. 즉 법원은 원고 회사가 1차 보안(방화문-디지털키), 2차 보안(내부 강화 유리문-지문), 3차 보안(CCTV), 4차 보안(개인컴퓨터 비밀번호 사용), 5차 보안(NAS 서버 비밀번호 사용-외부 접속 불가능) , 6차 보안(무역팀 이메일 비밀번호 사용)등의 조치에도 불구하고 자료를 업무용 공유 폴더에 보관하고 단일한 도메인의 이메일 주소로 모든 직원들이 이를 공유할 수 있도록 하는 등의 납득하기 어려운 조치로 보건데 보안조치가 충분한지 의문이 있다며 원고의 청구를 기각하였다.

이 사건에서 공유폴더에 업무용 파일을 저장한 것은 단 한 번의 느슨한 관리라고 할 수 있다.

8. 중요정보가 저장된 컴퓨터를 켜 놓은 채로 자리를 이탈하지 마라!

거래업체에 기술적 보안 서비스를 담당하는 자가 업데이트 등 기술지원을 위해 노트북을 소지하고 거래업체에 방문하였는데, 거래업체 직원이 담당자가 컴퓨터를 켜 놓은 상태에서 잠시 자리를 비운 틈을 이용해 노트북에 저장된 중요정보를 개인소유 USB에 그대로 옮겨 저장하여 유출한 사안이다. 이와 유사한 사건으로 일본에서는 공유 공간에서 원격회의 중 회사정보가 포함된 각종 정보가 주변사람에게 노출된 사례가 있다. 그리고 출장으로 신칸센(新幹線)으로 이동 중 차내에서 미발표 신제품에 관한 프리젠테이션 자료를 작성하던 중 누군가 그 내용을 보고 「모회사의 신제품에 관한 유출정보」라는 제목으로 SNS에 유출된 사례도 있었다.

이를 예방하기 위해서는 노트북 등 단말기기에 프라이버시 필터를 장착하는 것을 의무화해야 하며, 아울러 원칙적으로는 회사 기밀 등 중요정보 파일이 열려있는 상태에서 컴퓨터를 놔둔 채 이동하지 말아야 하며 부득이 자리에서 이동할 경우 전원을 OFF시켜 제3자에게 노출되지 않도록 주의해야 한다.

9. 회사가 지정한 자료전송시스템에 의해서만 정보전송을 허용하고, 업무용 e-mail을 외부로 발신할 때에는 보안책임자 또는 관리책임자에게 승인을 받도록 하라!

- 가능하면 피용자 각자 자리에 있는 PC는 인터넷 사용이 불가하도록 차단하고, 지정된 PC에서만 인터넷이 가능하도록 하는 것도 생각해 볼 수 있다.

- 대구지방법원 김천지원 2017가합15013 판결

원고가 영업비밀이라고 주장하는 이 사건 정보는 암호가 설정되어 접근대상자나 접근방법이 제한되었다. 원고는 회사에서 관리하는 도면 등 정보를 외주 업체(내지 거래처)에 이메일로 전송할 경우 캐드 파일이 아닌 PDF 문서 파일을 첨부하도록 하였고, 부득이 캐드 파일을 전송하여야 할 경우 원고 대표이사에게도 참조 형태로 그 이메일을 전송하도록 하였다. 또한 보낸 이메일에는 "본 도면은 원고의 자산이며 임의 사용 및 배포를 금합니다."라는 문구를 기재하였다. 이외에도 원고는 피용자들에 대한 보안 교육과 함께 퇴사자로부터 '재직시 업무상 지득한 회사의 제반 비밀사항을 타인에게 일체 누설하지 않겠습니다'는 문구가 삽입되어 있는 사직서를 받았다.

이에 법원도 원고는 규모가 크지 않은 중소기업으로서 '합리적인 노력'에 의하여 이 사건 설계도면을 '비밀로 유지'하여 온 것으로 보인다고 판단하였다. 그럼에도 불구하고 원고는 피고가 원고의 영업비밀을 다른 피고에게 이메일로 전송하여 비밀 유출을 차단하지 못했다고 할 것인바, 기술적보안 조치에 문제가 있었을 것으로 추정된다. 따라서 소규모 회사의 경우 비용이 많이 드는 기술적 보안조치가 힘들다면 피용자 개인 자리에서 자유롭게 인터넷이 가능할 수 없도록 할 필요가 있다.

10. 회사에서 개인용 이동식 저장장치의 사용은 삼가고, 개인 클라우드에 회사의 중요정보를 저장해두지 마라!

수많은 영업비밀 유출 사건에서 개인용 이동식 저장장치(USB, 외장하드, 스마트폰 등)가 활용되고 있다. 그리고 클라우드컴퓨팅이 보편화된 이후에는 개인용 클라우드 서비스에 회사의 중요정보를 유출하는 사례가 증가하고 있다.

그러나 특정 시기(퇴사 직전, 중요 프로젝트 시작 후·종료 전)에 회사에서 이동식 저장장치로 접속하였다는 사실 자체로 오해를 살 수 있다는 사실을 명심하라. 또한 재택근무 등을 대비해 편의상 개인 클라우드 서비스에 회사의 중요정보를 올려두었다가 개인용 PC에 다운로드 받는 경우도 많으나, 이 또한 회사에 영업비밀 유출 사고가 발생했을 때 불필요한 오해의 소지가 될 수 있음을 유념하라.

첨부2. 직무발명(직원소유) vs 영업비밀(회사소유)

직무발명과 영업비밀의 관계

직무발명(직원소유) vs 영업비밀(회사소유) — 직무발명과 영업비밀의 관계 —

회사는 임직원들의 인적인 집합체이며 임직원들의 연구개발로 기술이나 정보자산 등을 생성한다. 임직원이 업무수행 과정에서 발명 또는 생성한 아이디어 등은 "직무발명"이 될 수 있는데 아래에서"직무발명"의 개념에 대하여 살펴보고 이에 대한 권리는 누구에게 있는지, 이것이 "영업비밀"과 어떠한 차이가 있으며 직무발명을 발명한 임직원이 당연히 발명을 사용할 권리가 있는 것인지에 대해 살펴본 후 직무발명의 권리 귀속과 관련하여 임직원과 회사 간 발생될 수 있는 분쟁을 예방하기 위한 조치를 알아본다.

1. 직무발명의 개념

직무발명이란 '종업원, 법인의 임원 또는 공무원(이하 종업원등)이 그 직무에 관하여 발명한 것이 성질상 사용자·법인 또는 국가나 지방자치단체(이하 사용자등)의 업무범위에 속하고 그 발명을 하게 된 행위가 종업원 등의 현재 또는 과거의 직무에 속하는 발명'을 말한다. 이는 우리나라에서 직무발명에 관하여 규정하는 발명진흥법에 정의된 내용이다. 여기서의 '발명'은 특허법, 실용신안법, 디자인보호법에 따라 보호 대상이 되는 발명, 고안 및 창작을 의미[76]하고 '발명'은 '자연법칙을 이용한 기술적 사상의 창작으로서 고도한 것', '고안'은 '자연법칙을 이용한 기술적 사상의 창작'이라고 개념 정의되어 있다[77].

직무발명으로 인정되기 위해서는 ① 발명이 종업원에 의한 것일 것, ② 발명의 성질상 사용자의 업무범위에 속할 것, ③ 발명을 하게 된 행위가 당해 종업원의 과거 또는 현재의 직무에 속하는 것일 것이라는 요건을 충족해야 한다. 일반적으로 임직원이 자신에게 부여된 업무와 관련하여 어떠한 새로운 기술을 발명하였다면 그것은 직무발명에 해당될 가능성이 높다고 보면 된다.

2. 직무발명에 대한 권리귀속

발명진흥법에서 직무발명의 권리귀속 및 법률관계에 대하여 규정된 내용은 아래와 같다. '직무발명에 대하여 종업원등이 특허등을 받았거나 특허등을 받을 수 있는 권리를 승계한 자가 특허등을 받으면 사용자등은 그 특허권 등에 대하여 통상실시권을 가진다. 다만, 사용자등이 중소기업기본법 제2조에 따른 중소기업이 아닌 기업인 경우 종업원등과의 협의를 거쳐 미리 다음 각호의 어느 하나에 해당하는 계약 또는 근무규정을 체결 또는 작성하지 아니한 경우에는 그러하지 아니하다. 1. 종업원등의 직무발명에 대하여 사용자등에게 특허등을 받을 수 있는 권리나 특허권 등을 승계시키는

76) 발명진흥법 제2조 제1호, 제2호
77) 특허법 제2조 제1호, 실용신안법제2조 제2호

계약 또는 근무규정, 2. 종업원의 직무발명에 대하여 사용자등을 위하여 전용실시권을 설정하도록 하는 계약 또는 근무규정'[78]. '종업원이 직무발명을 완성한 경우에는 지체없이 그 사실을 사용자등에게 문서로 알려야 한다.[79]', '통지를 받은 사용자 등은 그때로부터 4개월 이내에 그 발명에 대한 권리의 승계 여부를 종업원 등에게 문서로 알려야 한다.[80]' '종업원 등은 직무발명에 대하여 특허등을 받을 수 있는 권리나 특허권 등을 계약이나 근무규정에 따라 사용자에게 승계하거나 전용실시권을 설정한 경우에는 정당한 보상을 받을 권리를 가진다.', '사용자등은 직무발명에 대한 권리를 승계한 후 출원하지 아니하거나 출원을 포기 또는 취하하는 경우에도 정당한 보상을 하여야 한다.[81]'

위 규정들에 따르면 사전 승계약정이나 근무규정이 없는 경우 종업원이 직무발명을 하였다면 그 사실을 회사에 통지해야 하고 회사는 직무발명에 대한 권리 승계여부를 결정해 근로자에게 통지해야 하는데, 사용자가 직무발명에 대한 권리를 승계하지 않기로 하였다면 당해 근로자가 해당 발명에 대한 특허권자 등 권리자가 될 수 있다. 다만, 사용자는 법에 따라 통상실시권을 법에 따라 당연히 가지게 된다. 반면 직무발명에 대한 권리를 사용자에게로 승계하기로 하는 승계약정이나 이를 내용으로 한 근무규정이 있는 경우 사용자는 이와 같이 사전에 마련된 승계약정이나 근무규정에 근거하여 그 임직원의 직무발명에 대한 정당한 특허권자가 될 수 있되, 다만 종업원에게 정당한 보상을 실시할 의무를 부담한다.

기업 실무상, 대부분의 회사는 근로계약서나 서약서(영업비밀보호서약서 등) 또는 근무규정에 '**근무중 업무와 관련하여 개발한 발명, 고안 등 일체의 아이디어 또는 취득한 회사의 영업비밀, 연구개발 영업자산 등에 영향을 미칠 수 있는 유무형의 정보 기타 회사의 주요 영업자산에 대한 모든 권리를 회사에 귀속시킬 것을 서약합니다**'와 같은 조항을 두는 것이 일반적이다. 이와 같이 근로자의 업무상 발명이나 일체의 정보를 회사에 승계시킨다는 점을 명시한 조항이 있다면 그 내용이 발명진흥법에서 말하는'사용자에게 권리를 승계시키기로 하는 계약'이 되는 것이고 위 조항이 포함된 계약서류를 작성하였거나 그러한 내용의 근무규정이 있는 회사라면 위 내용에 따라 자신의 직무발명에 대한 특허를 받을 권리를 회사에 승계한 것으로 해석된다. 따라서 회사는 임직원의 직무발명에 대한 특허권자가 될 수 있고 근로자는 사규에 정한 보상금 청구권을 취득하게 된다. 즉 이때 근로자는 보상금 청구권만 가질 뿐 직무발명 자체에 대한 특허권 또는 실시권이 없다.

한편, 특허는 기술을 공개하여 일정기간 독점하는 것을, 영업비밀은 기술을 외부에 공개하지 않고 비밀로 관리하여 독점적 보호를 받는 것을 각 그 본질로 한다. 기업이 어떠한 발명을 확보하게 된 경우 그것을 특허권으로 할 것인지 영업비밀로 관리할 것인지는 기업에서 전략적으로 정할 문제이다. 종업원이 발명한 기술을 통지받은 회사는 그것을 특허권으로 출원할 경우에도 '정당한 보상'을 하여야 하고, 영업비밀로 관리하면서 출원하지 않기로 한 경우(출원유보)에도 '정당한 보상'을 해야 한다.

이상의 내용들을 종합하면, 직무발명을 완성한 근로자가 (회사가 승계를 거부하여) 특허권자가 되었다면 회사는 통

78) 발명진흥법 제10조 (직무발명)
79) 발명진흥법 제12조 (직무발명 완성사실의 통지)
80) 발명진흥법 제15조 (직무발명에 대한 보상)
81) 발명진흥법 제16조 (출원 유보시의 보상)

상실시권을 법에 따라 확보하고, 사규 또는 근로계약서에서 '직무발명에 대한 사용자 승계권'을 미리 정하여 회사가 특허권자가 되었다면 직무발명을 한 근로자는 보상청구권을 획득한다는 것이다. 즉 미리 권리승계 여부를 사규 또는 계약서에 규정해 두었는지 여부에 따라 권리 귀속 주체를 달리 하되 근로자 또는 회사 모두 해당 발명에 이해관계를 가지는 만큼 각 상대방에게 일정한 권리(통상실시권 또는 보상청구권)를 법으로서 보장한 것이다. 기업 실무상 대부분의 회사에서 직무발명에 대한 사전승계약정을 두는 만큼 근로자가 업무 수행 중 발명한 그 어떠한 발명은 회사에게 권리가 귀속된다고 이해하는 것이 적절하다.

3. 영업비밀의 개념

영업비밀이란 '공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 비밀로 관리된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보'를 말한다[82]. 영업비밀로 인정받기 위하여 ① 공공연히 알려져 있지 않을 것, ② 독립된 경제적 가치를 가질 것, ③ 비밀로 관리될 것의 요건이 필요하다. 이는 영업비밀보호법이라는 법에 의한 보호를 받기 위하여 요구되는 요건이다. 영업비밀보호법 위반행위가 있는 경우 영업비밀보유자는 위반행위의 유형에 따라 위반행위자에 대하여 형사처벌, 손해배상, 사용금지요구, 신용회복조치청구 등을 요구할 수 있다.

4. 영업비밀에 대한 권리귀속 및 직무발명과의 관계

영업비밀은 그것을 보유하는 자에게 그 권리가 있다. 위에서 살펴본 직무발명에 대한 권리귀속과 같이 영업비밀에 대한 권리귀속 주체가 누구인지에 관하여 법에서 명문으로 정하는 바는 없다. 영업비밀 보유자가 누구인지는 영업비밀의 개념을 유추하여 상식적으로 판단할 수밖에 없다. 법률에서 말하는 보유자에는 회사와 같은 법인 또는 자영업자와 같은 자연인 개인이 모두 해당될 수 있다. 즉, 영업을 영위하는 법인 또는 자연인이 자신의 영업을 위하여 다른 사람은 알지 못하는 경제적 가치 있는 정보를 비밀로 관리하고 있다면 영업비밀을 보유하고 있는 자가 된다. 영업성 정보자산을 비밀을 관리할 정도의 영업을 하는 자는 대부분 직원을 수인 채용한 규모가 있는 법인 또는 영업주일 것이다.

영업비밀이 생성되는 과정은 다양하다. 일반적으로는 처음 창업을 한 영업주(또는 회사대표)가 자신의 창업 및 성공노하우를 비밀로서 관리하여 '영업비밀'로 인정받는 경우가 많을 것이고, 채용된 직원이 업무수행 과정에서 새로운 기술상, 경영상 정보를 창출하여 회사 영업을 위하여 비밀로 관리하여 '영업비밀'로 인정받는 경우가 있을 것인데 후자의 경우 직무발명의 개념과 연결지어 생각해 볼 수 있을 것이다.

우리나라 발명진흥법이나 영업비밀보호법에는 후자, 즉 직원이 창출한 영업비밀의 권리귀속에 대해 명확히 규정하고 있지는 아니하다. 발명진흥법 제16조 출원유보 보상 규정을 참조할 수 있을 따름이다. 회사가 직무발명을 특허권 등으로 권리화하지 않고 출원을 유보하였다면 이를 외부에 알리지 않고 영업비밀로 관리하겠다는 의사를 나타낸 것이라

82) 부정경쟁방지 및 영업비밀보호법(이하 영업비밀보호법) 제2조 제2호

고 볼 수 있고 그렇다면 정당한 보상을 할 의무가 있다는 내용이 그것이다.

영업비밀은 공지되지 않은 경제적 가치를 가지는 경영상, 기술상 정보를 포괄한다. 따라서 특허나 실용신안의 요건이 되는'자연법칙을 이용한 기술적 사상의 창작'보다는 보다 넓게 인정될 수 있다. 이에 고객정보나 고객명단, 제조법 등 취합된 정보 그 자체로서도 영업비밀로 인정받을 수 있고 많은 판례에서 위와 같은 정보가 영업비밀로 인정된 바 있다.

종업원이 창출한 영업비밀의 귀속에 관하여 명시적 규정이 없는 이상 종업원이 근무 중에 특허나 실용신안으로 보호받을 정도에 이르지는 못하지만 경제적 가치가 있는 어떤 기술상 경영상 정보를 창출한 경우 그에 대한 권리귀속이 어떻게 되는지는 종업원과 그 사용자 간 계약에 의해 정해질 수밖에 없다. 영업비밀을 관리할 정도의 회사라면 근로자와 근로계약을 체결하였을 것이고 이때 근로계약서나 별도의 서약서 등에서 '**근무중 개발한 발명 기타 일체의 정보에 대한 권리가 회사에 귀속된다**'는 취지의 규정을 포함하였을 가능성이 있다. 그렇다면 근로자가 생성한 영업비밀은 당연히 회사에 귀속되는 것이 된다. 다만, 위와 같은 약정이 없다면 그 정보에 대한 사용권은 사용주와 근로자 간의 근로계약의 취지, 신임관계라는 일반적인 법리에 따라 판단될 것이고 해당 정보가 근무 과정에서 회사의 업무수행을 위하여 창출된 것임을 고려하면 명시적인 약정이 없다고 하더라도 당해 정보에 대한 정당한 권리자는 사용주가 된다고 봄이 타당할 것이다.

5. 영업비밀 침해사건에서 직무발명에 의한 사용권 항변을 배척한 사례

의정부지방법원 고양지원 2014고단2481[83] 영업비밀 누설 등 사건에서 피고인이 침해대상 영업비밀이 자신이 발명한 것이기 때문에 사용할 권리가 있다고 주장한 바 있는데 위 법원은 대상 영업비밀에 관한 권리는 회사에 있는 점, 피고인들 스스로 대상 영업비밀이 회사에 승계되었다고 진술한 점 등을 적시하며 피고인들의 항변을 부정하였다. 이 판결은 항소심 및 상고심에서까지 유지되었다.

2. 범죄사실

피고인들은 공모하여 2011. 11. 3.경 피해자 회사와 동종제품을 생산하는 주식회사 C를 설립하고 피해자 회사에서 근무하면서 습득한 피해자 회사의 영업비밀인 T 제조기술을 사용하여 I를 제작한 후 2012. 6.경 판매하였다. 이로써 피고인들은 공모하여 부정한 이익을 얻거나 피해자 회사에 손해를 입힐 목적으로 피해자 회사의 영업비밀을 사용함과 동시에 위 영업비밀 액수 미상 시장 교환가격 상당의 재산상 이익을 취득하고 피해자 회사에 액수 미상의 이익감소분 상당의 손해를 가하였다.

83) 위 사건의 항소심(의정부지방법원 2017노412) 및 상고심 (대법원 2017도16521 판결)

3. 이 사건 제조기술이 피고인들의 직무발명에 해당하여 피고인들이 이 사건 제조기술을 사용할 권리가 있는지 여부

이 법원이 적법하게 채택하여 조사한 증거들에 의하여 알 수 있는 다음과 같은 사정 즉, 이 사건 제조기술에 관한 권리는 피해자 회사에 있는 점(설령 피고인들이 이 사건 제조기술 개발에 기여가 있다고 하더라도 피고인들 스스로도 이 사건 제조기술에 관한 권리는 피해자 회사에 승계되었다고 진술하고 있다), 관련 민사소송에서 인정된 피고인 A의 직무발명은 이 사건 제조기술이 아닌 I 상부에 니켈분말과 다이아몬드 코팅 필름을 부착하여 I수명을 연장시키는 기술에 관한 것이고 그 권리도 피해자 회사에 승계된 점을 보면 피고인들에게 이 사건 제조기술을 사용할 권리가 있다고 볼 수 없다.

6. 결어

근로자들은 직무발명에 대하여 근로자 본인에게 당연히 권리가 있는 것으로 인지하고 있는 경향이 있다. 그러나 직무발명은 그 개념상 회사의 업무와 관련하여 자신의 직무 범위 내에서 발명을 한 것을 의미하는 것으로서 회사에 일정한 권리가 있을 수밖에 없다. 발명진흥법 등 법에서도 이 점을 인정하여 사전 예약승계 규정에 의하여 회사가 특허권자가 될 수 있음을 규정하고 있고 회사가 특허권자가 되지 않더라도 적어도 통상실시권을 가질 수 있음을 규정하고 있다.

한편, 영업비밀 등 정보자산을 관리할 규모의 회사라면 근로자와의 근로계약서 또는 영업비밀보호 서약서 등에 근무 중 발명하는 그 어떠한 정보나 아이디어에 대하여 회사에 권리가 귀속된다는 점에 대한 명문의 약정서 또는 근무규정을 보유하고 있는 경우가 많은데 이러한 경우 직무발명에 대한 권리는 사전승계 약정에 따라 회사에게 권리가 당연히 이전되고 근로자 개인은 특별한 사정이 없는 한 그 발명을 스스로 사용할 권리는 없다. 이러한 법리는 특허권이 아닌 영업비밀로 정보자산을 보호하는 경우에도 동일하게 적용되는데 최근 판결은 영업비밀 침해사건에서 직무발명에 의한 근로자의 사용권 항변을 부정함으로써 그 점을 명확히 하였다. 따라서 자신이 개발한 것이라고 하여 당연히 근무 중이나 퇴사 후에도 자신이 당연히 사용권을 보유하고 있는 것이라고 단정해서는 안 된다는 점을 유념할 필요가 있다.

사용자 입장에서도 근로자와의 법적 분쟁을 최소화하고 사용자의 권리를 확실히 하기 위하여서는 사전에 예약승계 규정을 명확히 해두는 것이 필요하다. 일반적으로 기업에서는 취업규칙만을 사내 규정의 전부로 알고 있는 경향이 있는데, 취업규칙은 근무, 휴가 등 근태에 관한 일반적인 사항만 있을 뿐 영업비밀 등 회사의 정보자산 보호를 위한 예약승계 규정이 당연히 포함되어 있지 않다[84]. 회사의 정보자산 등 보호를 위한 예약승계 규정은 별도의 규정으로 마련해 두어야 한다. 또한 회사가 정하는 위와 같은 규정 이외에도 하여 근로자와의 직접 체결 또는 징구하는 근로계약서 또는 영업비밀 보호 서약서에 정보자산의 귀속 주체에 대하여 명시적 규정을 두어 근로자들의 인지가능성을 높이는 것이고 해당 내용을 특히 굵게 표시하는 등 명확하게 표현하여 두는 것이 좋을 것이다.

84) 고용노동부에서 제공하는 표준 취업규칙에 영업비밀 등 정보자산 보호에 관하여 전혀 규정되어 있지 아니하다.

첨부3. 비대면 근무환경에서 영업비밀 보호를 위한 조치

1. 원격근무 영업비밀보호규정
2. 원격근무 관련 각종 서식

비대면 근무환경에서 영업비밀 보호를 위한 조치

1. 들어가기에 앞서

영업비밀 보호규정은 기업의 영업비밀 관리 의사를 드러내는 사내 규정이다. 다수의 판례에서 당해 기업이 영업비밀 보호를 위한 사내 규정이 있는지 여부를 기준으로 당해 기업의 '비밀관리성'을 판단하는 것이 확인되기도 한다. 따라서 영업비밀을 비밀로서 관리하여 법의 보호를 받고자 하는 기업은 영업비밀 보호규정을 사내 규정으로 제정하여 이를 임직원들에게 공포하고 임직원들이 잘 볼 수 있는 곳(인트라넷 등)에 게시하여 임직원들로 하여금 수시로 확인하고 회사의 영업비밀보호 및 관리 의지를 확인할 수 있도록 해야 한다.

또한 최근의 사회적 분위기 및 코로나 팬데믹 등으로 기업의 근무형태가 변화한바 기업에 출근하여 기업에서 집중적으로 근무하는 방식에서 탈피하여 재택근무, 거점오피스 근무 등 근로자들의 근무방식도 다양해지고 있으므로 기존의 영업비밀보호 방식 또는 기존의 규정만으로 해결할 수 없는 다양한 상황이 있다. 근무방식이 변화하였음에도 기존의 방식대로만 정보보호 체계를 유지한다면 과연 기업이 정보를 "비밀"로서 관리하고자 하는 의지가 있는지에 대한 의구심을 불러일으킬 수 있다.

우리나라의 영업비밀보호법은 계속하여 개정되고 있는데 2019. 7. 9. 시행된 법률부터는 영업비밀의 개념이 기존보다 완화되어 '공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서 비밀로 관리된 생산방법, 판매방법, 그밖에 영업활동에 유용한 기술상 또는 경영상 정보'라고 규정되어 있다. 위 법 시행 전에는 "상당한 노력에 의하여 비밀로 관리된" 또는 "합리적 노력에 의하여 비밀로 관리된"이라는 요건이 요구되었다. 그러나 많은 중소기업이 '상당한 노력' 또는 '합리적 노력'의 수준을 충족하지 못하여 법의 보호를 받지 못한 사례가 자주 발생되어 중소기업의 영업비밀을 보호하기 위하여 영업비밀의 요건이 완화되었다. 다만, 그렇다고 하더라도 최소한 영업비밀 보호법의 적용을 받기 위하여 "비밀로 관리"된다는 요건이 기본적으로 필요하다. 최근 5년간의 영업비밀 관련 판례를 분석하여 본 바로도 다수의 판결례에서 개정법을 감안하더라도 영업비밀 보호법의 적용을 받기 위하여 기본적인 "비밀관리성"이 필요함을 지적하며, '자료가 비밀이라고 인식될 수 있도록 고지를 하지 않고 비밀유지약정을 하지 않으며, 자료에의 접근을 물리적으로 허용하지 않는 장치를 하지 않았다면 영업비밀이라고 볼 수 없다'고 판시하고 있음을 확인할 수 있었다[85].

기업이 원격근무를 허용하였음은 기업의 자료를 임직원 이외 다른 사람들이 볼 수 있는 환경에 노출시켰다는 것인데

85) 인천지방법원 부천지원 2019가합101938판결 등

기업이 이러한 상황에 대비한 정보 보호를 위한 노력을 하지 않는다면 '비밀관리'를 다하지 못한 것으로 인정받을 가능성이 높다. 따라서 원격근무에 대비한 영업비밀 관리규정을 추가하거나 새로 정비할 필요성이 있다.

아울러, 영업비밀 보호 규정이 있는지 여부가 여러 판례에서 영업비밀 관리의 징표 중 하나로 확인되기도 하지만 그 규정이 형식적으로 만들어 둔 것에 불과한 경우 규정의 존재에도 불구하고 회사의 "비밀관리"노력이 없는 것으로 판단한 다수의 판결례를 확인할 수 있다. 따라서 영업비밀 보호 규정은 제정이 중요한 것이 아니라 실제 그 내용대로 이행되도록 하는 것이 더욱 중요하다. 규정의 내용대로 보안관리 책임자를 지정하고 보안교육 및 서약서 징구 등 지침의 내용을 실천하며 보안관리 상황을 주기적으로 경영진에 보고하고 개선해 나가는 것이 규정을 제정하여 두는 것만큼이나 중요하다.

모든 기업에는 당해 기업을 성장시킨 고유한 핵심 노하우 또는 영업비밀이 있게 마련이다. 이러한 영업비밀을 법적인 보호 범위로 끌어들이는 노력은 각 회사가 스스로 해야 할 수밖에 없다. 규정이나 시스템이 체계적으로 갖춰진 대기업 이외의 기업들은 사내 규정으로는 취업규칙 이외에 별다른 것이 없을 가능성이 높은데 아래 제시하는 영업비밀보호 규정 등을 자체 규정으로 채택하여 활용함으로써 기업의 영업비밀 관리노력을 다하는 것이 매우 중요하다 하겠다. 아래에서 원격근무를 채택한 기업이 영업비밀 보호를 위하여 활용할 수 있는 세부 규정이나 서식을 참조 양식으로 제공한다. 영업비밀을 보호하고자 하는 기업들이 유용하게 활용할 수 있을 것이다. 이하에서 제공하는 서식 및 관련 자료는 다음과 같다.

2. 원격근무 영업비밀보호규정

가. 영업비밀보호규정이 있는 경우, 하부 규정으로 신규 규정 추가…. 원격근무 보안관리지침 … ① 추가형

본 지침은 영업비밀관리규정을 이미 채택한 회사가 근무환경 변화로 원격근무를 실시할 경우 영업비밀 관리가 소홀해지지 않도록 원격관리시 기업의 정보보호를 위하여 기업 및 근로자가 준수해야 할 사항을 정한 것임

원격근무 보안관리지침(추가형)*

000주식회사는 20**. *. *. 부터 시행 중인 영업비밀 관리 규정의 세부 지침으로 2023. *. *. 부터 아래와 같은 원격근무 보안관리 지침을 시행한다.

[설명: *기존에 영업비밀규정을 채택한 회사가 추가로 원격근무를 실시할 경우 제정하는 규정]

- 아　　래 -

제1조 (목적)

이 지침은 000주식회사(이하 회사) 임직원이 회사 이외의 장소에서 근무를 할 경우(이하 원격근무) 회사의 영업비

밀을 포함한 정보 유출을 방지하기 위하여 필요한 세부 사항을 규정함을 목적으로 한다.

제2조 (적용범위)

이 지침은 회사의 원격근무 방침에 동의한 회사 소속 임직원에게 적용된다.*

[설명: * 근무의 형태와 관련된 것인 만큼 원칙적으로 회사소속 임직원에 적용되는 사내 규정임. 원격근무에 관한 내용이 취업규칙에 없다면 근로자와 협의 또는 동의없이 원격근무 실시는 불가능함. 협력사나 타사 직원에 대하여 본 지침이 바로 적용되기는 어려우므로, 협력사 인력 중 회사의 업무를 원격으로 실시하는 자에 대하여는 협력계약서에 지침의 내용을 계약내용으로 하기로 하는 별도의 조항이 필요함]

제3조 (정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. "원격근무"란 정보통신망을 활용하여 업무의 전체 또는 일부를 지정된 사무실 이외의 환경에서 수행하는 근무 형태로써 재택근무·파견근무·이동근무를 포함한다.
2. "재택근무"라 함은 자택에 업무공간을 마련하고 업무에 필요한 사무공간과 정보통신망을 구축하여 근무하는 행태를 말한다.
3. "파견근무"라 함은 일정기간 타 기관 파견 또는 타 시설에 사무환경과 정보통신망을 구축하여 근무하는 행태를 말한다.
4. "이동근무"라 함은 장소에 제약 없이 휴대용 단말기(휴대폰·태블릿·노트북PC 등)를 이용하여 이동하면서 업무를 처리하는 근무형태를 말한다.
5. "공개 원격근무"라 함은 처리되는 업무내용이 공개 가능한 원격근무를 말한다.
6. "비공개 원격근무"라 함은 처리되는 내용이 비공개 자료인 원격근무를 말한다.

제4조 (원격근무 목적과 원격근무 실시)

① 원격근무는 임직원이 자택이나 타 시설에서 정보통신망 등을 이용하여 업무를 수행함으로써 업무처리의 생산성 및 효율성을 높이기 위함에 목적이 있다.

② 원격근무는 임직원의 신청 또는 회사의 지정에 의해 시행한다. 회사는 임직원의 원격 근무신청이 있는 경우 다음의 사항을 고려하여 원격근무를 승인할 수 있다.

1. 당해 임직원의 재직 기간(최소 6개월 이상), 근태 및 업무처리 내역 등 근로자에 관한 제반 상황
2. 당해 임직원 소속 부서 및 회사의 업무 현황
3. 당해 임직원 업무의 성격상 원격근무가 가능한 것인지 여부

③ 아래의 업무는 원격근무 대상 업무에서 배제될 수 있다.

1. 대면상담이 필요한 업무
2. 업무수행을 위하여 반드시 특정 장소에 항상 위치해야 하는 경우
3. 그 밖에 원격근무를 허용할 경우 사업목적 달성에 현저한 지장이 우려되는 경우

[설명: * 원격근무 허용기준은 기업 인사관리 관점에서 명확하게 설정되는 것이 바람직함(예: 근속기간 6개월 이상인 사람 중에서)]

④ 원격근무는 임직원의 해지신청 및 이에 대한 회사의 승인으로 해지된다. 다만, 회사는 다음의 경우 임직원의 원격근무를 중단을 명하고 출근을 명할 수 있다.

1. 근무를 태만히 하거나 업무성과가 저해된 경우
2. 영리행위 등 재택근무 신청목적과 다른 행위를 한 경우
3. 정보 유출 등 보안사고를 일으킨 경우
4. 그 밖에 당해 원격근무의 필요성이 없다고 판단되는 경우

제5조 (원격근무 신청 절차)

① 임직원은 전항에 따라 원격근무를 신청할 경우 별지1의 원격근무 신청서를 회사 부서장의 승인을 얻어 제출한다.

② 부서장 및 보안관리책임자는 임직원의 신청을 검토하여 원격근무 여부를 심사하고 별지2의 보안서약서를 근로자로부터 받아야 한다.

제6조 (원격근무자 준수사항)

① 원격근무를 승인받은 임직원은 원격근무의 목적에 따라 업무를 수행한다.

② 원격근무자는 회사로부터 사용을 지정받은 컴퓨터나 장비를 이용해 업무를 수행하여야 하고 업무용으로 사용하는 이메일을 개인적 목적으로 사용하거나 개인이메일을 업무용으로 사용하여서는 아니된다.*

[설명: *개인 장비를 업무용으로 사용한 경우 영업비밀 관리성을 인정받지 못한 사례가 확인되는 만큼 업무용 PC는 별도로 지급해야 함. 업무용 이메일을 따로 사용하지 않는 것 역시 다수의 판례에서 영업비밀성을 인정받지 못하는 요소로 본 바 있으므로 업무용 PC ,업무용 이메일을 따로 쓰는 것이 중요함]

③ 원격근무자는 불특정 다수가 사용하는 장비를 이용하여서는 안 된다. 부득이하게 불특정 다수가 이용한 PC등 설비를 이용한 경우 즉시 보안담당관에게 별지3 상황보고서 내용에 따라 사용일시, 장소, PC 등 관련 정보를 보안관리책임자에게 보고하여야 한다.

④ 원격근무 중 이석하게 될 경우 반드시 비밀번호(8자리 이상)가 부여된 화면보호기능 구동, 사내 인트라넷에서 로그아웃 하거나 이에 준하는 보안조치를 하여야 한다.

⑤ 원격근무자는 업무와 무관한 자가 원격근무자가 작업 중인 화면을 열람 또는 화면 저장하거나 카메라 등을 이용하여 촬영하는 일이 없도록 하여야 한다. 사내 담당자와 통화를 하여야 할 경우 업무와 무관한 자가 청취할 가능성이 없는 별도의 공간에서 하여야 한다.

⑥ 원격근무자는 출력물 생성을 최소화해야 하고 출력물이 생성된 경우 즉시 보관 및 회수하여 부주의로 누출되지 않도록 하여야 한다.

⑦ 원격근무용 PC에 상용 P2P·메신저, 웹하드 등의 사용은 금지된다. 원격근무용 PC에는 불가피한 사정이 없는 한 가급적 업무용 파일을 저장하지 않는다.

⑧ 원격근무자는 업무용 PC에 보안프로그램을 상시 업데이트하여야 하고 바이러스 백신 프로그램으로 주기적 점검하여야 하며 불법소프트웨어를 사용하지 않도록 하여야 한다.

⑨ 원격근무자는 PC내 인증서나 PC비밀번호를 정당한 이유없이 제3자와 공유하여서는 아니 된다.

⑩ 원격근무자는 근무과정에서 정보가 유출되지 않도록 관리를 철저히 하고 정보누출의 우려가 있거나 정보 누출 등

보안사고가 발생된 때에 즉시 보안관리 책임자에게 알려야 한다.

제7조 (보안관리책임자의 원격근무 관리)*

① 보안관리책임자는 원격근무자의 담당직무에 따라 접근 및 사용권한을 구분하여 부여하고 본 지침의 실질적 운영을 담당한다.

[설명: *본 지침을 제정해 두는 것으로 그치는 것이 아니라 실제 이행되도록 하는 것이 중요함. 다수의 판례에서 '보안 규정은 있으나 실제 규정대로 이행된 것으로 보이지 않음' 등을 적시하며 비밀관리성을 부인한 바 있음. 보안담당관은 관리자급 이상으로 하되 임직원수 등 회사의 규모에 따라 겸임으로 할 수도 있음. 보안담당관은 정/부로 최소 2인 이상 지정하는 것이 바람직함]

② 보안관리책임자는 별지4 원격근무관리대장 양식을 이용하여 원격근무자의 이름과 부서, 기간, 담당업무, 사용장비 등에 관한 내역이 적힌 관리대장을 마련하고 각 대상자별로 별지5-1 원격근무 점검표에 따른 확인을 다하야야 한다.

③ 보안관리책임자는 원격근무시의 보안사고와 관련하여 아래 내용이 포함된 대응계획 및 처리 절차를 수립하여야 한다.

1. 보안사고의 정의: 업무용 PC 등 기기가 해킹되거나 업무상 정보가 누설 또는 분실된 경우
2. 처리 절차: 보안사고 발생시 사고를 인지한 즉시 회사 지원팀장(또는 대표이사)에게 보고

④ 보안관리책임자는 원격근무자에게 주기적 보안교육을 시행하여야 한다.

⑤ 보안관리책임자는 정보유출 방지를 위하여 '전자문서 보안대책(DRM) 등을 포함한 자료유출방지 시스템을 구축하고 비인가자의 접근 및 업무 정보 노출 방지대책을 수립해야 한다.

⑥ 보안관리책임자는 원격근무용 전산장비에 대해 최신 백신, 침입차단시스템 설치 및 보안패치를 실시하고 보안장비에 대해서는 담당자를 지정하여 관리토록 하여야 한다.

⑦ 보안관리책임자는 원격근무자에게 월1회 이상 별지5-2 원격근무 자가점검현황표를 송부하여 보안관리 현황을 점검하여야 한다.

⑧ 보안관리책임자는 전항의 정기점검 이외에 비정기적으로 원격근무자의 보안 준수사항을 점검할 수 있다.

⑨ 보안관리책임자는 원격근무자의 퇴직·전출·업무변경시 장보자산 사용권한 재설정 및 삭제절차를 마련하고 인증관련 정보나 매체 분실 또는 장기간 원격근무용 지원시스템 미사용의 경우 권한정지 등의 조치를 취하여야 한다.

⑩ 보안관리책임자는 연1회 이상 원격근무자 근무점검 및 관리현황을 대표이사에게 보고하여야 한다.

제8조 (원격근무 서비스 보안대책)

① 회사는 원격근무자에 대해 VPN(Virtual Private Network)시스템을 적용하여야 한다. 기술적, 경영적 상황으로 VPN시스템 적용이 어려운 경우로서 원격근로자의 정보통신망 사용이 불가피한 경우 근로자는 자신이 사용하게 되는 IP번호를 회사에 제출하여야 한다.

② 회사는 원격근무자에 대하여 '자료유출방지시스템' 구축 및 '전자문서 보안(DRM)' 대책, KeyLogging, ScreenCapture 등 자료유출 방지 대책을 수립하여 이행하여야 한다. 기술적, 경영적 상황으로 자료유출방지 관련한 시스템 또는 DRM을 적용할 수 없는 경우 원격근무자는 별지6의 원격근무 현장확인서를 회사에 제출하여

야 한다.

제9조 (효력)

본 지침은 회사의 영업비밀보호규정의 벗어나지 않는 범위에서 효력을 갖는다.

제10조 (시행)

본 지침은 대표이사의 결재를 얻는 즉시 시행한다.

나. 영업비밀보호 규정이 없는 경우, 영업비밀보호규정 내에 원격근무 관련 내용을 추가하여 (신)영업비밀보호규정을 마련… ② 신규 영업비밀보호 규정

영업비밀관리규정

제1장 총칙

제1조 (목적) 이 규정은 000주식회사(이하 '회사'라 함)의 정보자산, 보안사항, 영업비밀 및 기타 지식재산권의 관리 및 보호에 관한 필요한 사항을 정하여 회사의 발전을 도모함을 목적으로 한다.

제2조 (정의) 이 규정에서 사용되는 용어의 정의는 다음과 같다.

1. "정보"라 함은 회사의 경영 또는 활동에 필요한 일체의 지식을 말한다.
2. "정보자산"이라 함은 '정보와 정보시스템'을 포괄한 개념을 말한다.
3. "정보시스템"이라 함은 회사가 보유하고 있는 컴퓨터, 전산시스템, 네트워크, 소프트웨어 및 각종 영상매체시설물 등 "정보"를 관리하는데 필요한 모든 자산을 말한다.
4. "영업비밀"이라 함은 회사가 보유 또는 보유할 정보로서 공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로 비밀로 관리된 생산방법·판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.
5. "지식재산권"이란 인간의 창조적 활동 또는 경험 등에 의하여 창출되거나 발견된 지식·정보·기술, 사상이나 감정의 표현, 영업이나 물건의 표시, 생물의 품종이나 유전자원(遺傳資源), 그 밖에 무형적인 것으로서 재산적 가치가 실현될 수 있는 것에 관한 권리를 말한다.
6. "임직원"이라 함은 회사에 재직하는 임원과 직원을 말한다.
7. "원격근무"라 함은 정보통신망을 활용하여 업무의 전체 또는 일부를 지정된 사무실 이외의 환경에서 수행하는 근무 형태로써 재택근무·파견근무·이동근무를 포함한다.

제3조 (보안업무의 분류)

① 회사의 모든 "정보"에 대해 "일반업무"와 "보안업무"로 구분하고, "보안업무"는 다시 "시스템보안업무"와 "일반보안업무"로 구분된다.

② "시스템보안업무"는 컴퓨터, 정보통신망 등 주로 컴퓨터를 통하여 진행되는 정보시스템에 관한 보안업무를 말하며, "일반보안업무"는 그 이외의 모든 부문의 정보보안업무를 말한다.

제4조 (적용범위, 보호대상)

① 이 규정은 회사에 신규채용·재직·퇴직하는 모든 임직원과 외부 협력업체와 파트너 기타 회사를 출입하는 모든 사람에게 적용한다.

② 이 규정은 회사가 보유하고 있는 다음 각 호를 그 보호대상으로 한다.

1. 영업비밀 그 자체
2. 영업비밀이 화체된 물건 및 물체(예시 : 서류, 도면, 복사물, 자기테이프, 컴퓨터, CD, DVD, USB, 외장HDD, 전화기, 자재, 생산품, 등)
3. 영업비밀 생산설비와 장비
4. 영업비밀 통제구역
5. 지식재산권
6. 기타 회사 기밀과 관련된 정보자산

제2장 영업비밀의 보호관리

제5조 (보안업무의 조직 및 기능)

① 회사는 영업비밀 기타 정보자산의 관리와 보호를 위하여 회사 내 모든 보안업무를 총괄 담당하는 보안관리책임자를 지정한다.

② 보안관리책임자의 직무는 다음 각 호와 같다.

1. 부서별 영업비밀 보호 및 관리에 관한 계획 수립 및 조정
2. 소관 영업비밀의 등급분류
3. 영업비밀에 관한 교육 실시
4. 영업비밀 보유현황 조사 및 관리 감독
5. 비밀유지계약 및 서약서등의 집행
6. 보안관련 규정 및 지침 수립ㆍ조정
7. 회사가 원격근무를 실시하는 경우 원격근무자에 대한 제반 관리 및 지원
8. 기타 회사의 영업비밀 보호 기타 보안에 관하여 필요한 사항

③ 보안관리책임자는 분기별로 대표이사에게 보안업무의 현황을 보고하여야 하며, 임직원이 중요한 영업비밀을 개발하거나 창출하였을 경우에도 같다.

④ 회사의 각 부서장은 부서업무와 관련된 영업비밀(제6조의 1급비밀을 제외한다)의 관리책임자로서 제2항 제1호 내지 5호 및 제7호의 직무를 수행할 의무와 책임을 가진다.

⑤ 보안관리책임자는 각 부서장과 보안업무에 관한 협력체계를 수립하고 사내 주요 보안상황을 공유하며, 필요한 사항에 대해서는 전 임직원에게 공지한다.

제6조 (영업비밀의 분류와 기준)

① 회사는 영업비밀에 대해 그 중요성과 가치의 정도에 따라 "1급비밀", "2급비밀", "3급비밀" 등 3단계로 분류하고, 필요시 그 분류를 변경할 수 있다.

② "1급비밀"이란 경쟁사 또는 대외로 유출될 경우 회사가 막대한 손해를 입을 수 있는 다음 각 호의 영업비밀을 말한다.

1. 회사의 원천기술 및 이에 대한 지식재산권 출원과 관련된 사항

2. 세계 초일류 기술, 국방·안보관련 기술 또는 국가핵심기술과 관련되는 사항
3. 회사의 영업전략, M&A 기타 회사의 핵심 영업비밀에 해당하는 사항

③ "2급비밀"이란 경쟁사 또는 대외로 유출될 경우 회사에 피해를 줄 수 있는 영업비밀 중 "1급비밀"에 해당하지 않는 영업비밀을 말한다.

④ "3급비밀"이란 "1급비밀" 또는 "2급비밀"이 아닌 "영업비밀"을 말한다.

⑤ 영업비밀은 다음 각 호의 기간 동안 보존한다. 다만, 회사의 보안관리책임자 또는 각 부서장은 각 영업비밀의 특성을 고려하여 다음 제2호, 제3호의 보관기간보다 장기간을 보존기간으로 지정할 수 있다.

1. 1급비밀 : 영구보존
2. 2급비밀 : 10년
3. 3급비밀 : 5년

제7조 (영업비밀 표시 및 보관)

① 영업비밀은 그 표지에 "대외비" 표시와 함께 각 등급에 따라 아래와 같이 구분하여 표시하여야 한다.

1. 1급 비밀 : 대외비 | 1급
2. 2급 비밀 : 대외비 | 2급
3. 3급 비밀 : 대외비 | 3급

② 영업비밀이 화체된 서류, 물건 등은 일반 문서, 물건 등과 분리하여 별도의 보관함, 금고 등 보안장치를 구비하고 있는 용기에 넣어 특별히 관리해야 한다.

③ 영업비밀이 포함되어 있는 전자문서는 일반 전자문서와 분리하여 비밀번호를 설정하고, 영업비밀 취급자격이 있는 자 이외에는 열람할 수 없는 방법으로 보관하여야 한다.

제8조 (영업비밀 통제구역 설정)

① 영업비밀의 보호와 중요시설장비 및 자재의 보호를 위하여 필요한 경우 일정한 범위를 통제구역으로 지정하고, 필요 시 CCTV와 시건장치 기타 통제구역을 보호하기 위한 장치나 설비를 설치한다.

② 제1항의 통제구역에는 외부에서 인식할 수 있는 적절한 방법으로 "통제구역"임을 표시하고 회사로부터 사전에 허가 받은 관계자 이외의 출입을 통제하여야 한다.

③ 제1항의 통제구역에는 출입자 명부를 비치하여 출입자를 기록·보존하여야 하고, 필요할 경우 출입자로부터 영업비밀 보호에 관한 각서 또는 서약서를 징구해야 한다.

제9조 (관리대장)

각 영업비밀의 관리책임자는 제7조 제2항에 의하여 관리하고 있는 영업비밀에 대하여 등급별로 별지 제1호 서식의 영업비밀 관리대장(이하 '관리대장'이라 함)을 비치하고 변동사항 등에 대한 기록을 유지·관리하여야 한다.

제10조 (취급자격)

제6조에 의하여 분류된 영업비밀의 취급자격은 다음 각 호와 같다.

1. 1급 비밀 : 대표이사, 대표이사가 지정한 임직원, 보안관리책임자
2. 2급 비밀 : 1급 비밀 취급자, 해당 영업비밀이 속한 담당부서의 부서장 및 실무 담당자
3. 3급 비밀 : 2급 비밀 취급자와 동일

제11조 (보안점검)

① 보안관리책임자는 영업비밀을 취급하는 각 부서에 대하여 정기적으로 보안점검을 실시하여야 한다.

② 보안관리책임자는 영업비밀 보호를 위하여 필요한 경우 대표이사에게 그 사유를 보고한 이후 특정 임직원 및 부서를 선정하여 불시에 보안점검을 실시할 수 있다.

제12조 (복구)

각 영업비밀의 관리책임자는 영업비밀에 대한 위험이 발생하거나 발생할 우려가 있음을 알게 된 때에는 지체 없이 보안관리책임자 및 관련부서에 이를 통보하고 즉시 필요한 조치를 취하여야 한다.

제13조 (물품의 반입, 반출)

① 회사의 자산 및 물품을 반입·반출하는 임직원은 보안관리책임자 또는 관련부서 부서장의 사전승인을 얻어야 한다.

② 컴퓨터 등 정보처리장치(휴대용을 포함하며, 이하 '컴퓨터'라 한다) 및 USB메모리, 외장 HDD 등 전자기록매체(이하 '전자기록매체'라 한다) 등을 사용하고자 하는 임직원은 사전에 보안관리책임자 또는 담당부서장의 승인을 얻어야 하며, 회사의 업무를 위해서만 사용하여야 한다.

③ 컴퓨터 또는 전자기록매체를 반입·반출하는 경우, 이를 사용하는 사용자는 관련 규정에 따라 반입 반출일자, 기기사양, 사용용도, 사용자 정보 등을 작성하여 담당 부서장에게 제출하고, 담당 부서장은 이를 직접 확인한 이후 사용자가 제출한 서류를 보안관리책임자에게 제출하여야 한다.

④ 보안관리책임자는 제3항의 서류를 별도로 보관하고, 회사 내의 컴퓨터 및 전자기록매체 등의 존재 및 사용현황을 수시로 확인하여야 한다.

제14조 (비상대책)

① 영업비밀 관리책임자는 화재나 자연재해 등 비상상황에 대비하여 복사본 작성이 필요한 영업비밀에 대해서는 보안관리책임자와 협의하여 복사본을 작성하고, 이를 별도의 장소에 보관하여 정기적으로 관리하여야 한다.

② 보안관리책임자는 화재나 자연재해 및 회사의 기밀유출 등의 비상상황 발생시 회사의 피해를 최소화하기 위한 관련 규정 및 지침을 수립하고, 이를 전체 임직원에게 공지하여야 한다.

제3장 영업비밀의 생성과 취득

제15조 (영업비밀의 창출 및 귀속)

임직원이 직무와 관련하여 연구·개발하거나 취득한 영업비밀은 회사의 소유이며, 해당 임직원은 이를 회사에 귀속시켜야 한다. 다만, 임직원이 자신의 일반적 지식, 경험, 기술에 근거하여 창출한 영업비밀에 대해서는 특별한 약정이나

규정이 있을 경우 그 약정이나 규정에 따르고, 그 약정이나 규정이 없을 경우 해당 임직원의 소유로 한다.

제16조 (영업비밀 신고) ① 임직원이 재직 중 영업비밀을 창출한 경우에는 관련 부서의 장에게 신고하여야 한다.

② 임직원이 본 규정의 적용을 받지 아니하는 타인과 공동으로 회사의 업무와 관련된 영업비밀을 창출한 경우에도 제1항의 규정에 따라 신고하여야 한다.

제17조 (보상)

임직원이 창출한 영업비밀 중 이로 인하여 회사의 이익이 발생하고 상당한 가치가 있는 영업비밀에 대해서는 직무발명에 준하여 보상금을 지급하여야 한다.

제18조 (취득)

임직원이 영업비밀을 취득하였을 경우 소속 부서장에게 신고하고, 부서장은 이를 관리대장에 기재한다.

제4장 영업비밀의 사용

제19조 (사용)

① 회사의 영업비밀은 제10조에 따라 영업비밀 취급자격이 인정되는 영업비밀 관리책임자의 승인을 얻어 사용할 수 있다.

② 회사의 영업비밀을 사용하거나 이를 반출하는 경우에는 사전에 영업비밀 관리책임자에게 신청하여야 하고, 위 관리책임자는 신청인의 영업비밀 취급 자격을 확인한 이후 그 자격이 인정되는 경우에 한하여 별지 제2호 서식의 영업비밀 사용대장(이하 '사용대장'이라 함)에 신청내역을 기재한 이후 해당 영업비밀을 반출하거나 사용하도록 하여야 한다. 이때 제1급비밀의 사용 또는 반출에 대해서는 사전에 보안관리책임자의 동의를 얻어야 한다.

제20조 (양도)

① 영업비밀을 양도할 때에는 관련부서와 협의를 하고 영업비밀 관리책임자, 보안관리책임자 및 대표이사의 승인을 얻어야 한다.

② 영업비밀 관리책임자는 영업비밀을 양도한 후에도 필요에 따라 관계기록을 폐기하지 않고 영업비밀유지·관리를 수행해야 한다.

제21조 (부서간 사용)

회사 내부의 부서간 영업비밀을 대여·사용·유통을 위하여 이송할 때에는 제19조에 따라 부서 책임자간에 인수인계 절차를 거쳐야 하며, 영업비밀을 이송 받은 부서의 책임자는 해당 영업비밀의 사용이 종료되는 때에는 즉시 인수인계절차를 거쳐 해당 영업비밀을 원래 보관하고 있던 부서에 반환하여야 한다.

제22조 (이송방법)

① 영업비밀을 사내에서 대여·사용·유통을 위하여 이송할 때에는 밀폐포장이나 용기 등을 사용하여야 한다.

② 부득이 영업비밀을 통신수단에 의하여 이송할 때에는 보안이 설정된 파일 등을 활용하거나 주요내용 부분은 이를 분리하여 이송하는 등 필요한 보안조치를 취하여야 한다.

제23조 (관리, 폐기)

① 회사의 영업비밀은 별표1. 영업비밀별 관리기준에 따라 관리한다.

② 더 이상 활용가치가 없는 영업비밀은 일정한 절차에 의해 폐기할 수 있으며, 폐기 후에도 필요한 경우에는 계속하여 보호·관리한다.

제5장 임직원의 영업비밀 보호의무

제24조 (입사시)

회사가 신규로 채용한 임직원에 대해서는 별지 제3호의 비밀유지서약서를 작성하여 제출하게 해야 한다.

제25조 (재직 중 영업비밀누설 금지)

① 임직원은 재직 시 취득한 영업비밀에 대하여는 이 규정에 따라 취급·관리해야 하며 허가 없이 이를 유출·공개 또는 사용할 수 없다.

② 연구개발 결과, 신제품 등을 발표하거나 전람회 등에 출품하여 부득이 하게 영업비밀을 공개하게 되는 경우에는 사전에 해당 영업비밀의 관리책임자 및 보안관리책임자의 승인을 얻어야 한다.

③ 회사는 임직원의 재직 중에 정기적으로 별지 제4호의 비밀유지서약서를 징구할 수 있으며, 프로젝트 참여 등 필요 시에는 별지 제5호의 비밀유지서약서를 징구할 수 있다.

제26조 (퇴직 시)

① 회사의 임직원이었던 자는 회사의 사전승인 없이 재직 시 취득한 영업비밀을 공개·유출 또는 사용할 수 없다.

② 임직원이 퇴직할 경우 그 임직원이 보유하고 있는 모든 영업비밀을 반납 받고 별지 제6호 서식의 비밀유지서약서를 징구해야 한다.

제6장 협력업체 등에 대한 비밀관리

제27조 (협력업체 기타 제3자)

협력업체 기타 제3자에게 영업비밀을 제공하거나 영업비밀과 관련된 업무를 하게 할 경우 해당 협력업체 기타 제3자로 하여금 별지 제7호 서식의 비밀유지서약서를 작성하여 제출하도록 하여야 한다.

제28조 (공동 프로젝트, 기술제휴계약)

① 회사가 외부 기관 등에 연구개발 프로젝트를 의뢰하거나, 외부 기관과 사이에 기술제휴계약을 체결함에 있어서 회사의 영업비밀을 공개해야 하는 경우, 외부 기관의 참여 임직원에게는 별지 제8호 서식의 비밀유지서약서를 제출 받고, 외부 기관과 사이에는 별지 제9호 서식의 비밀유지 계약서에 따라 비밀유지계약을 체결한 이후에 영업비밀을 공개하여야 한다.

② 회사는 외부 기관과의 협의에 따라 제1항의 제8호 서식 또는 제9호 서식의 내용 중 일부를 변경할 수 있다.

제7장 시스템 보안관리

제29조 (컴퓨터 사용)

① 회사 내 모든 컴퓨터 사용자는 불법 소프트웨어를 사용해서는 안 되며, 불법 소프트웨어를 사용함으로 인한 모든 책임자는 사용자 본인에게 있으며, 회사는 책임이 없다.

② 회사 내 모든 컴퓨터 사용자는 바이러스 침입 및 해킹을 방지하기 위한 소프트웨어와 각종 보안 솔루션을 설치하고, 정기적으로 백업 및 업데이트 관리를 하여야 한다.

제30조 (통신망 사용)

① 임직원들은 회사 내에서 공통으로 사용하는 통신망만을 사용하여야 한다.

② 보안관리 부서 및 보안관리책임자는 회사의 영업비밀 보호 및 업무 효율성 확보를 위해 인터넷상의 특정 사이트 접속을 통제할 수 있다.

③ 임직원들은 회사에서 사용을 금지한 이메일을 사용해서는 안 된다.

④ 임직원들은 외부로 문서를 발송할 경우에는 부서장의 사전 승인을 받아야 한다. 단, 전결권한이 있는 임직원은 그렇지 아니하다.

제31조 (시스템 관리)

① 보안관리책임자는 회사의 보안시스템을 연1회 이상 정기적으로 점검하고, 그 결과를 전체 임직원에게 공개한다.

② 임직원들은 회사의 보안시스템에 대한 문제를 발견한 즉시 보안관리책임자에게 그 사실을 신고하여야 한다.

③ 시스템보안에 대해서는 이 규정에 의하는 외에 별도로 규정하는 바에 따른다.

제8장 원격근무와 정보보호

제32조 (원격근무의 승인과 보안서약서)

① 회사는 원격근무 제도를 도입할 수 있고 다음의 사항을 고려하여 신청한 임직원을 대상으로 별지 10 소정의 원격근무신청서에 따라 원격근무를 승인할 수 있다. 원격근무를 실시하고자 하는 자는 원격근무 신청절차에 따라 신청 후 별지 11 원격근무자 보안서약서를 작성하여 제출하여야 한다.

1. 당해 임직원의 재직 기간(최소 6개월 이상), 근태 및 업무처리 내역 등 근로자에 관한 제반 상황

2. 당해 임직원 소속 부서 및 회사의 업무 현황
3. 당해 임직원 업무의 성격상 원격근무가 가능한 것인지 여부

② 아래의 업무는 원격근무 대상 업무에서 배제될 수 있다.

1. 대면상담이 필요한 업무
2. 업무수행을 위하여 반드시 특정 장소에 항상 위치해야 하는 경우
3. 그 밖에 원격근무를 허용할 경우 사업목적 달성에 현저한 지장이 발생될 우려가 있는 경우

③ 원격근무는 임직원의 해지신청 및 이에 대한 회사의 승인으로 해지된다. 다만, 회사는 다음의 경우 임직원의 원격근무를 중단을 명하고 출근을 명할 수 있다.

1. 근무를 태만히 하거나 업무성과가 저해된 경우
2. 영리행위 등 재택근무 신청목적과 다른 행위를 한 경우
3. 정보 유출 등 보안사고를 일으킨 경우
4. 그 밖에 당해 원격근무의 필요성이 없다고 판단되는 경우

제33조 (원격근무자 준수사항)

① 원격근무자는 회사로부터 사용을 지정받은 컴퓨터나 장비를 이용해 업무를 수행하여야 하고 업무용으로 사용하는 이메일을 개인적 목적으로 사용하거나 개인 이메일을 업무용으로 사용하여서는 아니된다.

② 원격근무자는 불특정 다수가 사용하는 장비를 이용하여서는 안 된다. 부득이하게 불특정 다수가 이용한 PC등 설비를 이용한 경우 즉시 보안담당관에게 별첨의 서식에 따라 사용일시, 장소, PC 등 관련 정보를 보고하여야 한다.

③ 원격근무 중 이석하게 될 경우 반드시 비밀번호(8자리 이상)가 부여된 화면보호기능 구동, 사내 인트라넷에서 로그아웃 하거나 이에 준하는 보안조치를 하여야 한다.

④ 원격근무자는 업무와 무관한 자가 원격근무자가 작업중인 화면을 열람 또는 화면 저장하거나 카메라 등을 이용하여 촬영하는 일이 없도록 하여야 한다. 사내 담당자와 통화를 하여야 할 경우 업무와 무관한 자가 청취할 가능성이 없는 별도의 공간에서 하여야 한다.

⑤ 원격근무자는 출력물 생성을 최소화해야 하고 출력물이 생성된 경우 즉시 보관 및 회수하여 부주의로 누출되지 않도록 하여야 한다.

⑥ 원격근무용 PC에 상용 P2P·메신저, 웹하드 등의 사용은 금지된다. 원격근무용 PC에는 불가피한 사정이 없는 한 가급적 업무용 파일을 저장하지 않는다.

⑦ 원격근무자는 업무용 PC에 보안프로그램을 상시 업데이트 하여야 하고 바이러스 백신 프로그램으로 주기적 점검하여야 하며 불법소프트웨어를 사용하지 않도록 하여야 한다.

⑧ 원격근무자는 PC내 인증서나 PC비밀번호를 정당한 이유없이 제3자와 공유하여서는 아니 된다.

⑨ 원격근무자는 근무과정에서 정보가 유출되지 않도록 관리를 철저히 하고 정보누출의 우려가 있거나 정보 누출 등 보안사고가 발생된 때에 즉시 보안관리책임자에게 알려야 한다.

제34조 (보안관리책임자의 원격근무 관리)

① 보안관리책임자는 원격근무자의 담당직무에 따라 접근 및 사용권한을 구분하여 부여하고 본 지침의 실질적 운영

을 담당한다.

② 보안관리책임자는 별지12 원격근무관리대장 양식을 이용하여 원격근무자의 이름과 부서, 기간, 담당업무, 사용장비 등에 관한 내역이 적힌 관리대장을 마련하고 각 대상자의 별지13-1 원격근무 점검표 해당 여부를 상시 확인한다.

③ 보안관리책임자는 원격근무 관련 보안사고 발생시 대응계획 및 처리 절차를 수립하여야 한다.

1. 보안사고의 정의: 업무용 PC 등 기기가 해킹되거나 업무상 정보가 누설 또는 분실된 경우
2. 처리 절차: 보안사고 발생시 사고를 인지한 즉시 회사 지원팀장(또는 대표이사)에게 보고

④ 보안관리책임자는 원격근무자에게 주기적 보안교육을 시행하여야 한다.

⑤ 보안관리책임자는 정보유출 방지를 위하여 '전자문서 보안대책(DRM) 등을 포함한 자료유출방지 시스템을 구축하고 비인가자의 접근 및 업무 정보 노출 방지대책을 수립해야 한다.

⑥ 보안관리책임자는 원격근무용 전산장비에 대해 최신 백신, 침입차단시스템 설치 및 보안패치를 실시하고 보안장비에 대해서는 담당자를 지정하여 관리토록 하여야 한다.

⑦ 보안관리책임자는 원격근무자에게 월1회 이상 별지14 원격근무 자가점검현황표를 송부하여 보안관리 현황을 점검하여야 한다.

⑧ 보안관리책임자는 전항의 정기점검 이외에 비정기적으로 원격근무자의 보안 준수사항을 점검할 수 있다.

⑨ 보안관리책임자는 원격근무자의 퇴직·전출·업무변경시 사용권한 재설정 및 삭제절차를 마련하고 인증 관련 정보나 매체 분실 또는 장기간 원격근무용 지원시스템 미사용의 경우 권한정지 등의 조치를 취하여야 한다.

제35조 (원격근무 서비스 보안대책)

① 회사는 원격근무자에 대해 VPN(Virtual Private Network)시스템을 적용하여야 한다. 기술적, 경영적 상황으로 VPN시스템 적용이 어려운 경우로서 원격근로자의 정보통신망 사용이 불가피한 경우 근로자는 자신이 사용하게 되는 IP번호를 회사에 제출하여야 한다.

② 회사는 원격근무자에 대하여 '자료유출방지시스템' 구축 및 '전자문서 보안(DRM)' 대책, KeyLogging, ScreenCapture 등 자료유출 방지 대책을 수립하여 이행하여야 한다. 기술적, 경영적 상황으로 자료유출방지 관련한 시스템 또는 DRM을 적용할 수 없는 경우 원격근무자는 별지5의 원격근무 현장확인서를 회사에 제출하여야 한다.

제8장 영업비밀 침해구제

제36조 (구제조치)

① 보안관리책임자 및 각 부서장은 회사의 영업비밀을 침해 당했을 때에는 지체 없이 관계법령 및 사규에 의한 필요한 구제조치를 취하여야 한다

② 보안사고 발생시 업무담당자와 보안관리책임자 등 관련자는 사건 조사 및 해결에 성실히 협력하여야 한다.

제37조 (영업비밀누설자에 대한 징계)

영업비밀 누설자에 대해서는 제32조의 규정에 의한 조치를 취함과 동시에 별도로 사규에 따라 징계할 수 있다.

제38조 (관련자에 대한 징계)

영업비밀 누설을 부주의나 과실로 알지 못하였거나 막지 못한 관계자에 대해서도 사규에 의해 징계할 수 있다.

제9장 보칙

제39조 (교육)

① 보안관리책임자는 전체 임직원에 대해서 정기적으로 영업비밀에 관한 교육을 실시하여야 한다.

② 영업비밀 교육은 외부에 위탁하여 실시할 수 있다.

부칙

1. 이 규정은 20** 년 월 일부터 시행한다.
2. 이 규정 시행 전부터 보유하고 있는 영업비밀 중 주요 영업비밀에 대해서는 규정시행 후 1개월 이내에 등급분류(재분류)를 하여 등급을 지정(재지정)한다.

원격근무 관련 각종 서식

별지 양식

별지1 원격근무 신청서

별지2 원격근무 보안서약서

별지3 상황보고서

별지4 원격근무자 관리대장

별지5-1 원격근무 점검표

별지5-2 원격근무자 자가점검표

별지6 원격근무 현장확인서. 끝.

별지1 원격근무 신청서 **(임직원용)**

원격근무 신청서(신규)

소속/부서	
이름(생년월일)	
신청사유 (불허사유 해당여부)	
원격근무유형	
신청기간	
원격근무장소	
사용장비 현황	자산번호(PC 등)
연락처	본인 연락처 : 비상연락처 1: 비상연락처 2:

위와 같이 재택근무를 신청합니다.

20**년 **월 **일

위 신청인 - - - (인)

[결재]

승인	부서장	
합의	보안관리책임자	
통보	인사팀장/사업부장	

별지2 원격근무 보안서약서 **(임직원용)**

원격근무 보안서약서

(소속 / 직급) _____

(성명 / 생년월일) _____

1. 본인은 원격근무를 실시함에 있어 지정받은 장소에서 원격근무를 실시하고 회사의 원격근무 보안 지침을 철저히 준수할 것임을 서약한다.
2. 본인은 원격근무 수행 중 근무 장소에 외부인의 출입을 금지하며 출입문이나 사물함에 열쇠 등과 같은 시건 장치를 설치하도록 한다.
3. 본인은 원격근무 장소에 회사로부터 업무수행을 위하여 지정받은 장치 이외에 다른 카메라, 캠코더 등 촬영장치, 복합기나 프린터 등의 출력장치 반입을 금지한다.
4. 원격근무 수행 중 각종 문서 또는 파일, 각종 기록매체나 정보가 외부로 노출 또는 유출되지 않도록 각별히 한다.
5. 본인은 업무로 작성한 문서 또는 업무수행 중 알게 된 정보나 파일을 회사로부터 승인받지 않은 이메일 또는 저장매체에 저장하지 않는다.
6. 본인은 보안관리 강화를 위하여 매월 PC보안을 실시하고, 최신 상태의 백신 프로그램을 이용하여 주기적으로 검사를 실시한다.
7. 본인은 재택근무 수행용 컴퓨터에 로그인 암호, 화면보호기 패스워드를 사용한다.
8. 원격근무 점검을 위하여 회사의 보안담당자가 본인의 전산장치를 확인하고 본인의 업무 이메일을 열람함에 동의하고 원격근무 점검을 위하여 요청하는 사항에 적극 협조한다.
9. 본인은 기타 보안사항들을 성실히 준수하며 위반시 관련 규정에 따른 징계 등 법적 조치 대상이 될 수 있음을 인지한다.

위와 같이 원격근무를 위한 보안서약서를 작성하여 제출합니다.

20**. *. *.

(자필작성: 위 내용을 잘 읽고 이에 동의하고 이행을 다짐함, 서명)

(주) 0000 귀 중

별지3 상황보고서

수신 : (주) 0000 보안관리책임자

본인은 20**. *. *. 원격근무를 승인받은 원격근무자로서 다음과 같은 상황에 대하여 회사에 보고합니다.

보고내용: 특이상황 (예시)	내용	기타
사용 PC의 변경	기 승인 PC의 고장	
근무 장소의 변경		
기타		

20**.**.**.

위 보고자 _____부서 _____ (인/서명)

(주) 000 귀중

별지4 원격근무자 관리대장 **(보안관리책임자용)**

순번	성 명 (연락처: 전화번호/이메일)	원격근무기간	사용장비 현황 (자산번호)	VPN여부/ VPN미비시 IP	기타
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

㈜000주식회사 보안관리책임자 정:000/부:000

별지5-1 원격근무 점검표 (보안관리책임자용)

구분	점검사항	원격근무현황				
		공개	비공개			비고
			재택	파견	이동	
관리대책	1. 원격근무 업무 선정 기준이 존재하는가?					
	2. 원격근무 관련 보안관리지침이 존재하는가?					
보안계획 및 활동	1. 원격근무 보안사고 대응계획이 존재하는가?					
	2. 비상 연락체계가 존재하는가?					
	3. 원격근무 세부계획에 대하여 대표이사 확인을 받았는가?					
정보자산	1. 원격근무용 정보자산의 목록이 주기적으로 관리되는가?					
	2. 원격근무 관련문서의 반·출입 대장이 정기 점검되는가?					
	3. 중요문서의 반·출입 대장이 정기적으로 점검되는가?					
	4. 업무변경, 인사이동시 전산자료 인계인수절차가 있는가?					
	5. 장비 고장시 보안관리책임자 통보 및 후속대책 있는가?					
	6. 원격근무 종료시 보안관리책임자는 전산장비를 회수 등 관리조치를 하는가?					
원격 근무자 보안관리	1. 원격근무자의 정보보안 관련 직무·책임이 명확한가?					
	2. 원격근무자의 담당직무에 따라 정보에 대한 접근권한이 구분되어 있는가?					
	3. 원격근무자에게 보안서약서를 징구하는가?					
	4. 원격근무자에게 주기적 보안교육이 시행되는가?					
	5. 원격근무자는 회사가 제공한 원격근무용 전용장비(HW, SW)를 사용하는가?					
	6. 원격근무자가 장기간 작업을 하지 않을 경우 장비를 회수하거나 사용을 제한하는가?					
	7. 원격근무자가 인증정보 분실시 신속한 재인증 절차가 있는가?					
	8. 원격근무자의 보안규정 위반시 징계규정 절차가 있는가?					
	9. 정보보안 관련자료를 원격근무자에게 신속히 배포할수 있는 수단이 있는가?					

구분	점검사항	원격근무현황				
		공개	비공개			비고
			재택	파견	이동	
물리적 보안	1. 원격근무용 전산장비는 도난·분실·훼손 방지 대책이 있는가?					
	2. 근무시간 중 출입문 시건장치 등 비인가자의 접근방지 대책이 있는가?					
불법접근 차단대책	1. 이용권한에 따라 서버 및 네트워크 접근을 통제하고 내부망 접근을 제한하기 위한 침입차단시스템 등 검증필 정보보호시스템이 설치·운영되고 있는가?					
	2. 원격근무용 제반장비의 오(誤)사용 모니터링을 하는가?					
	3. 원격근무 전산장비에 전자문서 저장시 DRM 등 문서열람 제한시스템 또는 이에 준하는 관리를 하는가?					
	4. 승인되지 않은 프로그램 설치 금지 및 주기적 확인·삭제 절차가 있는가?					
	5. 원격근무 서버가 불필요한 서비스 포트를 개방하지 못하도록 보안설정을 하였는가?					
운영관리	1. 원격근무 전산장비에 부팅, 패스워드, 화면 보호기, 사용자인증 비밀번호가 작동중인가?					
	2. 원격근무 전산장비에 바이러스 백신, 침입 차단시스템이 운영되고 최신 업데이트를 유지하는가?					
	3. 원격근무 전산장비의 운영체제 패치 및 보안 관련 최신 업데이트를 유지하는가?					
	4. 원격근무 중 이석시 사전 화면보호기능 구동 등 보안조치가 실시되고 있는가?					
	5. 원격근무용 소프트웨어 설치시 시험평가 절차가 있는가?					
	6. KeyLogging, ScreenCapture 등 자료유출 방지 대책이 있는가?					

㈜000주식회사 보안관리책임자 정: 000/ 부:000

별지5-2 원격근무자 자가점검표

점검사항	확인(O/X)	비고
원격근무 승인절차는 준수하였음		
원격근무 보안서약서 작성하였고 내용 인지함		
원격근무용 장비는 회사로부터 지급받음		
회사 승인 이메일 사용중임(개인이메일 사용금지)		
업무 중 자료 생성후 자료의 등급표시를 함		
문서저장시 비밀번호나 DRM 등 적용함		
영업비밀자료를 개인저장매체에 저장하지 않음		
사용장비나 시스템에 비밀번호 설정함(이석시 PC잠금 여부포함)		
백신등 보안프로그램 정기적 업데이트 함		
원격근무장소에 제3자의 출입은 제한됨		
근무장소에 시건장치가 있음		
정보유출, 장비고장 등 보안사고 대처방법 알고 있음 (보안관리담당자 연락처 알고 있음		

2022. 00. 00.

원격근무자 _____부서 (서명)

㈜000주식회사

별지6 원격근무 현장확인서

원격근무 현장확인서

소속 및 직급 :

성　　명 :

본인은 원격근무를 절차에 따라 신청하였고 본인이 원격근무하는 공간은 다음과 같이 시건장치와 독립공간을 마련하고 있으며 DRM 등 자료 보안을 위한 회사 지시사항을 충실히 이행하고 있음을 확인함.

(현장 사진 첨부)

년　　월　　일

확인자

1. 독립공간 확보여부

독립공간 전경(방 전체)

2. 출입문 잠금장치 구비여부

출입문 잠금장치(외 · 내부 잠금장치)

3. 캐비넷 구비여부

비공개문서 보관용 캐비넷(잠금장치 포함)

㈜000주식회사

2022년

영업비밀 보호 가이드 연구

제 작 일 2022년 12월
발 행 일 2023년 10월
발 행 처 한국지식재산보호원 영업비밀보호센터
서울시 강남구 테헤란로 131 한국지식재산센터 6층
TEL (02) 1666-0521
FAX (02) 6196-2000

디자인·편집 박소연, 정하나, 최민아
인 쇄 (주)신성토탈시스템 T. 02-2277-5713