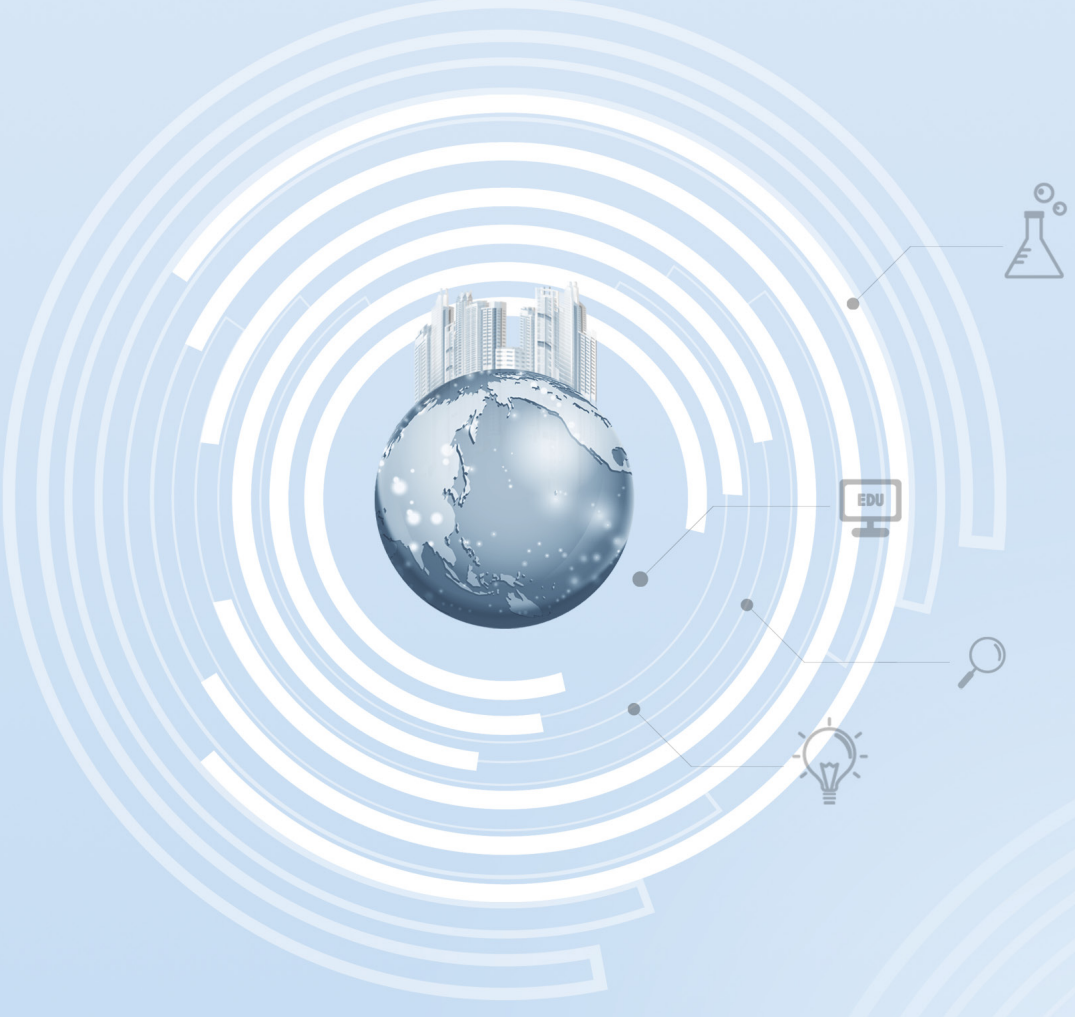
발 간 등 록 번 호
11-1430000-001718-01

기업 규모·업종별 영업비밀 표준관리체계 마련 연구



특허청

제 출 문

특허청장 귀하

본 보고서를 2019년 **“기업 규모·업종별 영업비밀 표준관리체계 마련 연구”** 과제의 최종보고서로 제출합니다.

주관연구기관명 : 법무법인(유한) 다래

연구기간 : 2019. 8. 19. ~ 2019. 12. 31.

주관연구책임자 : 박지환(법무법인(유한) 다래 변호사)

참여 연구원 : 민현아(법무법인(유한) 다래 변호사)

정영선(법무법인(유한) 다래 변호사)

윤정근(법무법인(유한) 다래 변호사)

최재혁(법무법인(유한) 다래 기술경영팀 부장)

서지영(법무법인(유한) 다래 기술경영팀 계장)

정용식(법무법인(유한) 다래 기술경영팀 연구원)

서대연(법무법인(유한) 다래 기술경영팀 연구원)

이현진(법무법인(유한) 다래 기술경영팀 연구원)

목 차

Ⅰ. 개요

1. 연구의 필요성 ····· 2
2. 연구의 목표 ····· 4

Ⅱ. 판례 분석

1. 개요 ····· 6
1.1 분석 대상 판례 ····· 6
1.2 분석 항목 ····· 7
2. 분석 결과(개요) ····· 9
2.1 연도별 비밀관리성 인정 비율 ····· 9
2.2 영업비밀 보호관리 조치별 분석 결과 ····· 10
2.3 영업비밀 정보 유형별 분석 결과 ····· 11
2.4 기술 분야별 분석 결과 ····· 13
2.5 기업 규모를 고려한 판결 ····· 16
2.6 의의 및 한계 ····· 17
3. 분석 결과(상세) ····· 19
3.1 영업비밀 보호관리 조치별 분석 ····· 19
3.2 영업비밀 정보 유형별 분석 ····· 21
3.3 기술 분야별 분석 ····· 31
3.4 기업 규모를 고려한 판결 ····· 47

Ⅲ. 영업비밀 표준 관리 체계

1. 필요성 및 배경 ····· 54
1.1 영업비밀의 정의 및 보호 요건의 완화 ····· 54
1.2 비밀관리성 판단 기준(판례) ····· 55
1.3 기존 영업비밀 보호관리 체계 ····· 57
1.4 중소기업 기술 보호 체계 ····· 58
1.5 정리 ····· 60

2. 영업비밀 표준 관리 체계 ····· 61
2.1 도출 방법 ····· 61
2.2 업종·규모별 영업비밀 표준 관리 체계 ····· 62
2.3 영업비밀 표준 관리체계의 내용 ····· 67
2.4 영업비밀 보호·관리 체계 구축을 위한 컨설팅 추진 방안 ····· 71

Ⅳ. 영업비밀 등급 분류 체계

1. 개요 ····· 80
1.1 등급 분류의 필요성 ····· 80
1.2 영업비밀 등급 분류 기준 ····· 82
1.3 기타 등급 분류 기준 ····· 85
2. 중소기업을 위한 영업비밀 등급 분류 체계 ····· 88
2.1 유형별 영업비밀 등급 분류 체계 ····· 88
2.2 약식 영업비밀 등급 분류 체계 ····· 89
2.3 영업비밀 정의 기반 등급 분류 체계 ····· 89
2.4 영업비밀 등급 분류의 실무 ····· 92

Ⅴ. 주요 국가의 영업비밀 보호 체계 (비밀관리성을 중심으로)

1. 개요 ····· 96
2. 국가별 규정 및 판례 ····· 97
2.1 일본 ····· 97
2.2 중국 ····· 101
2.3 미국 ····· 104
2.4 베트남 ····· 108
3. 정리 ····· 109

Ⅵ. 결론

[붙임 1] 영업비밀 관리 규정(일반형) ····· 116
영업비밀 관리 규정(소규모기업용) ····· 130
[붙임 2] 비밀유지 서약서 ····· 142

[표] 목 차

[표 1] 전체 수집된 판례 ····· 6
[표 2] 비밀관리성이 쟁점이 된 판례 ····· 6
[표 3] 영업비밀 보호 조치 분류 ····· 7
[표 4] 정보 유형 분류 ····· 8
[표 5] 기술 분야 분류 ····· 8
[표 6] 연도별 비밀관리성 인정 비율 ····· 9
[표 7] 영업비밀 보호관리 조치별 빈도 수 ····· 10
[표 8] 영업비밀 정보 유형별 분석 결과 ····· 11
[표 9] 영업비밀 정보 유형별 빈도 수 ····· 12
[표 10] 기술 분야별 분석 결과 ····· 13
[표 11] 기술 분야별 빈도 수 ····· 13
[표 12] 기업 규모를 고려한 판결 분석 결과 ····· 16
[표 13] 기업 규모를 고려한 판결 빈도 수 ····· 16
[표 14] 법원의 비밀관리성 판단 시 고려 요소 ····· 52
[표 15] 부정경쟁방지 및 영업비밀보호에 관한 법률 개정 이력 ····· 54
[표 16] 원심 및 항소심 판결 비교 ····· 56
[표 17] 비밀 관리성 판단 요소별 검토 빈도율 및 상관계수(민·형사 통합) ····· 57
[표 18] 영업비밀 보호 10계명 ····· 58
[표 19] 기업 성장 단계별 구분 ····· 58
[표 20] 중소기업 성장 단계별 기술 보호 ····· 59
[표 21] 중소기업 기술보호 10대 핵심 수칙 ····· 59
[표 22] 표준 체계(1차) – 규모·업종(분야)별 기업 분류 ····· 63
[표 23] 중소기업 기본법 시행령에 따른 중소기업 분류 ····· 64
[표 24] 중소기업 기본법 시행령에 따른 소기업 분류 ····· 65
[표 25] 기업체당 평균 매출액/총자산/자본 ····· 65
[표 26] 표준 체계(2차) – 규모에 따른 기업 분류 ····· 66
[표 27] 표준체계에 따른 제도적 보호·관리 조치 ····· 67
[표 28] 표준체계에 따른 인적 보호·관리 조치 ····· 68
[표 29] 표준체계에 따른 물적 보호·관리 조치 ····· 70
[표 30] 현행 영업비밀 보호컨설팅 현황 점검표 일부 (관리자용) ····· 72

[표 31] 현행 영업비밀 보호관리 수준 분류 기준 ····· 74
[표 32] 영업비밀 컨설팅 추진 시 확인 사항 ····· 75
[표 33] 영업비밀 지정 기준(2012) ····· 83
[표 34] 영업비밀 등급 분류 가이드(2016) ····· 84
[표 35] 영업비밀 정보 유형별 등급 분류 ····· 88
[표 36] 약식 영업비밀 등급 분류 ····· 89
[표 37] 영업비밀 정의 기반 등급 분류 ····· 90
[표 38] 영업비밀 등급 분류의 절차 ····· 92
[표 39] 영업비밀 등급 분류의 실무상 절차(예) ····· 93
[표 40] 주요 국가의 영업비밀 비밀관리성 관련 규정 ····· 96

[그 림] 목 차

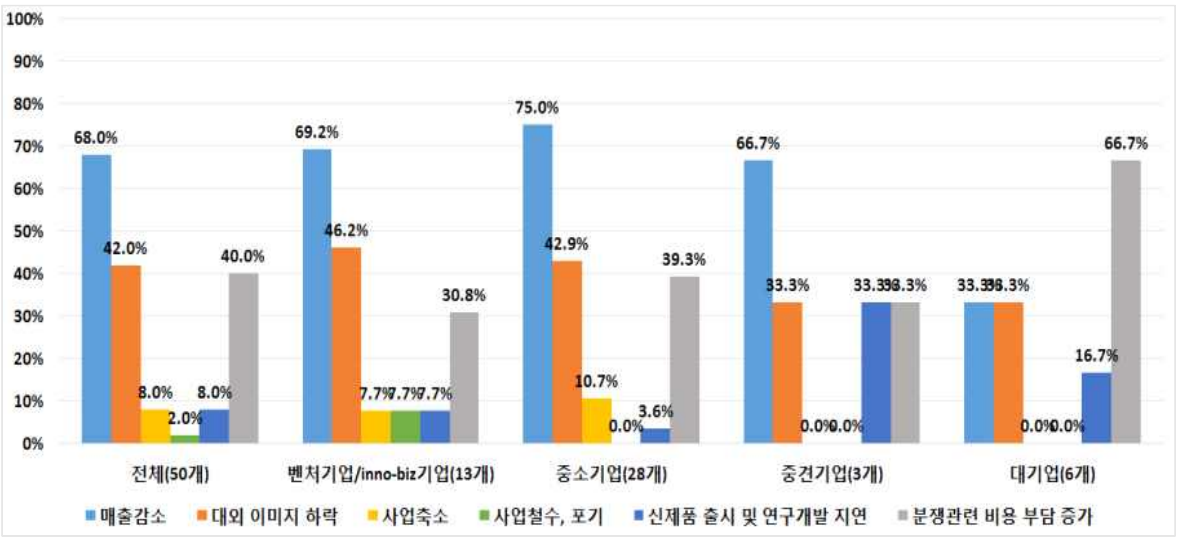
[그림 1] 국내 영업비밀 유출에 따른 피해 항목 ····· 2
[그림 2] 영업비밀 보호 및 관리의 애로 사항 ····· 3
[그림 3] 기업의 영업비밀 전담부서 보유 여부 ····· 3
[그림 4] 기업 규모별 중요하게 생각하는 영업비밀 ····· 4
[그림 5] 현행 영업비밀 보호 컨설팅 내용 ····· 4
[그림 6] 영업비밀 보호관리 조치별 빈도 수 ····· 11
[그림 7] 기술 분야별 사건 수 ····· 15
[그림 8] 매출액 규모별 기업체 분포 ····· 66
[그림 9] 자산 규모별 기업체 분포 ····· 66
[그림 10] 현행 영업비밀 관리 체계 구축 단계별 세부 사항 ····· 73

Ⅰ. 개요

1. 연구의 필요성

○ (영업비밀의 중요성 증대) 기업에서 영업비밀을 포함한 무형자산이 차지하는 비중이 날로 증대됨에 따라 영업비밀 유출로 인한 매출 감소, 대외 이미지 하락 등의 피해가 발생하고 있으며, 미국·중국·EU 등 해외 주요국들도 영업비밀 보호 제도를 강화하고 있는 추세이다.

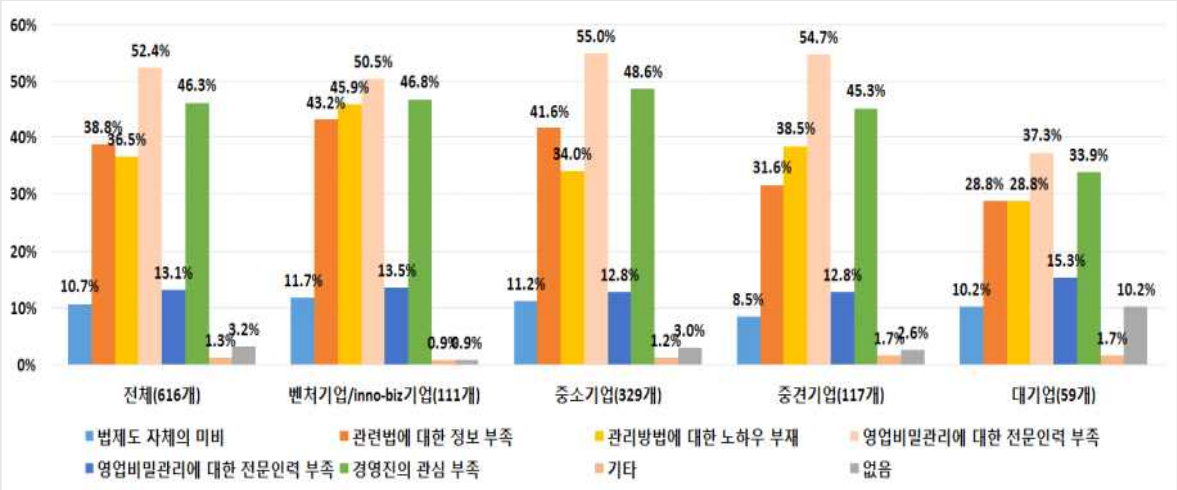
* 국내 기업 중 52.9%가 영업비밀을 보유하고 있으며, 이 중 14%(86개 기업)가 영업비밀 유출로 인한 피해를 보았다고 응답 (출처: 2016. 우리기업의 국내외 영업비밀 피침해 실태 조사, 특허청/한국지식재산연구원)



[그림 1] 국내 영업비밀 유출에 따른 피해 항목(출처: 상동)

○ (영업비밀 관련 정보 부족) 영업비밀은 법률상 “비밀로 관리”된 기술상·경영상의 정보에 한해 보호가 가능하나, 구체적으로 어떤 방법으로 관리해야 하는지에 대한 기업 규모·업종별 세분화·표준화된 정보가 부족한 실정이다.

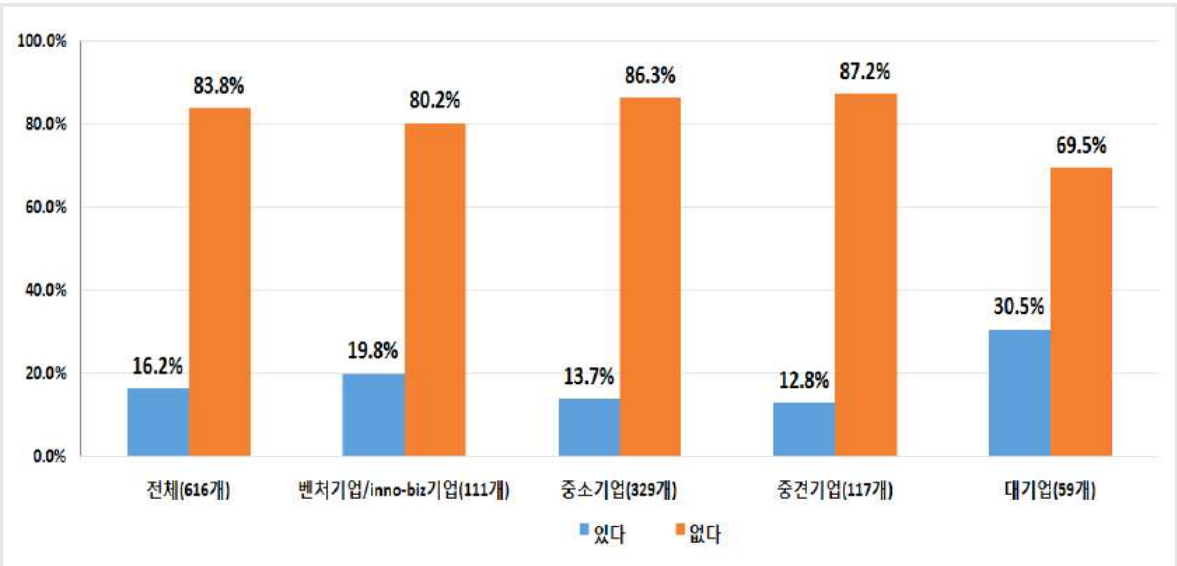
* 특허청 조사 결과 약 40%에 달하는 기업이 영업비밀 보호 및 관리의 애로 사항으로 관련 정보가 부족하다고 응답 (출처: 상동)



[그림 2] 영업비밀 보호 및 관리의 애로 사항 (2016, 특허청)

○ (영업비밀 보호·관리 역량 미흡) 국내 기업의 상당수가 영업비밀 보호를 위한 전담 인력이나 부서를 보유하고 있지 않아, 체계적이고 지속적인 영업비밀 보호·관리 활동이 이루어지지 못하고 있을 뿐만 아니라 영업비밀 유출로 인한 피해가 발생해도 효과적으로 대응하지 못하고 있는 상태이다.

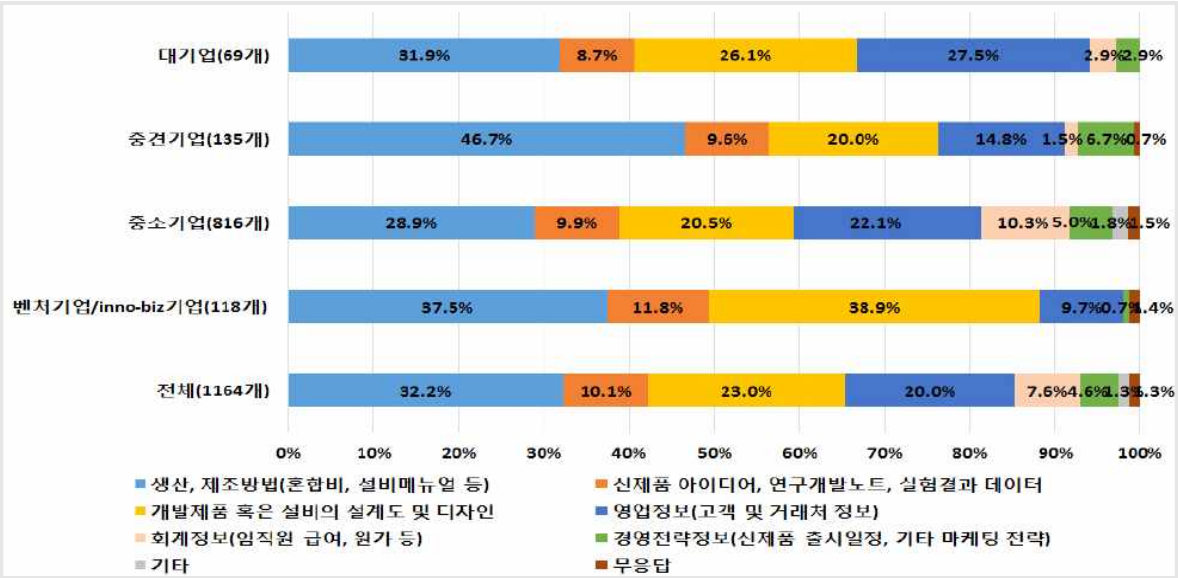
* 영업비밀 전담 부서가 있는 기업은 전체의 13.5%에 불과하며, 영업비밀 관리를 위한 별도 예산이 없거나 1천 만원 이하라고 응답한 기업이 각 25.2%와 상당수에 이르며, 영업비밀 유출 사건 발생 시 아무런 대응을 하지 못한 비율이 42%에 달함 (출처: 상동)



[그림 3] 기업의 영업비밀 전담부서 보유 여부(출처: 상동)

2. 연구의 목표

○ (영업비밀 보호·관리 방법 표준화) 기업의 규모나 업종에 따라 중요 영업비밀의 종류가 상이할 뿐만 아니라 관련 예산이나 전담 부서/인력의 유무 등 차이가 있으므로, 유형별 영업비밀 보호·관리 방법을 표준화함으로써 기업이 보다 용이하고 체계적으로 영업비밀을 보호·관리할 수 있도록 방법론을 제시하고자 한다.



[그림 4] 기업 규모별 중요하게 생각하는 영업비밀 (출처: 상동)

○ (영업비밀 보호 컨설팅 체계 구축) 영업비밀 보호 컨설팅의 프로세스와 방법론을 매뉴얼화하여 컨설팅 수행 전문가에 따른 편차를 최소화함으로써 컨설팅 품질을 제고하고 기업 만족도를 최대화 하고자 한다.

[그림 5] 현행 영업비밀 보호 컨설팅 내용 (출처: 영업비밀보호센터)

Ⅱ. 판례 분석

1. 개요

1.1 분석 대상 판례

선고일을 기준으로 2015년 1월 1일부터 2019년 6월 30일까지 선고된 영업비밀 관련 민·형사(가처분 포함) 판결 총 1,596건을 대상으로 하였다.

[표 1] 전체 수집된 판례

구분	민사	형사	합계
2015년	144	120	264
2016년	189	155	344
2017년	286	123	409
2018년	303	129	432
2019년 상반기	85	62	147
합계	**1007**	**589**	**1596**

위 판례에 대한 전수 분석을 통해 1) 영업비밀 보호 요건과 직접적 관련이 없는 손해배상, 부당이득반환 청구, 불법행위 등이 쟁점이 된 사건이나 단순 전직(경업) 금지가 쟁점이 된 사건 등 무관한 사건은 분석 대상에서 제외하고, 2) 비밀관리성에 대한 구체적 판단이 없거나 일반적 설시만 있는 판례(예를 들어, '사정을 종합하여 보면, 본 안 정보는 영업비밀이라고 볼 수 없으므로', 혹은 '사건 기록을 살펴보면, 본 안 정보가 객관적으로 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태에 있었다고 볼 자료가 없다' 등) 역시 분석 대상에서 제외한 후, 영업비밀 보호 요건 중 '비밀관리성'에 관해 구체적으로 판단하고 있는 판례 368건을 선별하여 최종 분석 범위로 하였다.

[표 2] 비밀관리성이 쟁점이 된 판례

구분	민사	형사	합계
2015년	38	36	74
2016년	37	45	82
2017년	58	39	97
2018년	33	44	77
2019년 상반기	15	23	38
합계	**181**	**187**	**368**

1.2 분석 항목

‘비밀관리성’ 판단의 실질적 의미를 파악하기 위하여 1) 어떤 보호조치를 취했기 때문에 법원이 비밀관리성을 인정 또는 부정하였는지(보호 조치별), 2) 영업비밀 정보가 어느 유형에 속하는지(정보 유형별), 3) 해당 영업비밀 정보가 속하는 기술 분야가 무엇인지(기술 분야별)로 나누어 분석을 진행하였다. 이 외에, 법원이 비밀관리성 판단에 있어 기업 규모 등을 고려하였음을 명시적으로 밝히고 있는 판례에 대해서는 추가적인 분석을 진행하였다.

1.2.1 영업비밀 보호 조치별 분석

우선, 법원이 ‘비밀관리성’을 판단하면서 영업비밀 보유자 또는 피해 기업이 어떤 조치를 취했거나 취하지 않았기 때문이라고 판시하고 있는지를 분석하였다. 관련 영업비밀 관리·보호 조치는 제도적·인적·물적 관리로 구분하여 각 구분별로 총 11가지의 구체적 보호관리 조치로 나누어 그 빈도수를 살펴보았다.

[표 3] 영업비밀 보호 조치 분류

보호조치		내용
제도적 관리	등급분류	영업비밀의 중요도 등에 따른 등급 분류
	표시/고지	영업비밀임을 인식할 수 있는 표시/고지
	규정	영업비밀 관리규정(문서관리규정, 비밀관리규칙 등)
인적 관리	서약서	영업비밀보호약정 등
	교육	영업비밀 보호 의무와 위반 시 책임 등을 주지시키는 교육
	징계/보상	영업비밀 보호 의무 위반에 대한 징계 등
물리적 관리	분리보관	영업비밀 자료를 일정한 장소 등에 분리하여 보관
	출입통제	영업비밀 자료가 보관된 장소에 대한 출입 제한
	이용제한	영업비밀 이용 방법 혹은 이용 권한을 제한
	반출제한	영업비밀 대외 반출에 대한 제한
	접근제한 (패스워드)	영업비밀에 대한 접근 방식 및 접근할 수 있는 자를 제한

1.2.2 영업비밀 정보 유형별 분석

각 판례에서 쟁점이 된 영업비밀을 유형별로 나누어 기술정보 또는 경영정보가 문제된 사건과 기술정보 및 경영정보가 모두 문제된 사건으로 구분하여 분석하였다.

[표 4] 정보 유형 분류

분류	내용
기술정보	도면, 배치도, 방법, 연구개발 보고서, 실험정보, 아이디어 등
경영정보	고객명부, 원가 정보, 제품개발계획, 구입처, 가격표, 계산표 등
기술정보+경영정보	기술정보와 경영정보 모두를 포함하는 경우

1.2.3 기술 분야*별 분석

종래 영업비밀 관련 분석에서 업종을 기준으로 한 결과 대부분의 기업이 '제조업'에 속하기 때문에 분석의 실익이 없다고 판단하여, 이번 연구에서는 해당 영업비밀 정보가 속한 (기술) 분야가 무엇인지에 따라 8개 분류로 나누어 분석하였다. (산업기술분류표를 준용하되, '지식서비스'는 1차 분석 결과, 분류 실익이 없다고 판단되어 '일반 서비스'로 변경함)

[표 5] 기술 분야 분류

분류	내용
기계·소재	정밀생산기계, 산업/일반기계, 조선/해양시스템 등
전기·전자	반도체장비, 가정용기기, 디스플레이 등
정보통신	이동통신, 소프트웨어, 디지털콘텐츠 등
화학	고분자재료, 화학공정, 화학제품, 섬유제품 등
바이오·의료	의약/산업 바이오, 치료기기, 의료정보 등
에너지·자원	자원, 원자력, 신재생에너지, 에너지효율향상 등
일반 서비스	유통/물류/마케팅 서비스, 여행업체, 배달업, 학원 등
기타	상기 분류에 속하지 않거나, 명확한 분류를 할 수 없는 경우

* 통상적인 방법으로 '업종'을 분류할 경우 대부분의 영업비밀 보유자 또는 피해 기업이 '제조업'에 속하는 문제가 있어, 대안적인 접근으로 영업비밀에 해당하는 정보의 내용에 따라 산업 분류를 적용함

1.2.4 기업규모를 고려한 판례 분석

이 외에, 법원이 비밀관리성의 '상당성' 또는 '합리적 수준'을 판단함에 있어 기업 규모(인원 수, 매출 등)를 고려하였음을 명시적으로 밝히고 있는 판례(예를 들어, '그룹 전체의 규모 등에 비추어 볼 때 상대적으로 높은 수준의 비밀관리 노력이 요구된다고 봄이 상당한 점 등을 고려하여 보면', '대표와 대표 부인 2명으로 구성된 회사여서 회사 내부적으로 특별한 보안조치가 필요하지는 않았다고 보인다' 등)에 대해서는 추가적인 분석을 진행하였다.

2. 분석 결과 요약

2.1 연도별 비밀관리성 인정 비율

[표 6] 연도별 비밀관리성 인정 비율

연도	구분	사건수	인정(비율)	부정(비율)
2015	전체	74	33 (44.6%)	41 (55.4%)
	민사	38	14 (36.8%)	24 (63.2%)
	형사	36	19 (52.8%)	17 (47.2%)
2016	전체	82	37 (45.1%)	45 (54.9%)
	민사	37	14 (37.8%)	23 (62.2%)
	형사	45	23 (51.1%)	22 (48.9%)
2017	전체	97	47 (48.5%)	50 (51.5%)
	민사	58	24 (41.4%)	34 (58.6%)
	형사	39	23 (59.0%)	16 (41.0%)
2018	전체	77	40 (51.9%)	37 (48.1%)
	민사	33	15 (45.5%)	18 (54.5%)
	형사	44	25 (56.8%)	19 (43.2%)
2019 (상반기)	전체	38	21 (55.2%)	17 (44.7%)
	민사	15	5 (33.3%)	10 (66.7%)
	형사	23	16 (69.6%)	7 (30.4%)
전체	민사	**181**	72 (39.8%)	109 (60.2%)
	형사	**187**	106 (56.7%)	81 (43.3%)
	합계	**368**	**178 (48.4%)**	**190 (51.6%)**

전체 판례에서 영업비밀 관리성이 인정된 비율은 48.4%, 부정된 비율은 51.6%, 민사 판례에서 영업비밀 관리성이 인정된 비율은 39.8%, 부정된 비율은 60.2%, 형사판례에서 영업비밀 관리성이 인정된 비율은 56.7%, 부정된 비율은 43.3%이다.

연도별로 비밀관리성 인정 비율을 살펴보면, 2015년의 경우 전체 쟁점 사건 중 비밀관리성이 인정된 비율이 44.6%이며(33건/74건), 2016년 45.1%(37건/82건), 2017년 48.5%(47건/97건), 2018년 51.9%(40건/77건)로 비밀관리성 인정 비율이 높아지는 추세에 있다는 것을 알 수 있는데, 이는 법률 개정을 통해 비밀관리성 요건을 완화한 것과 관련이 있는 것으로 보인다.

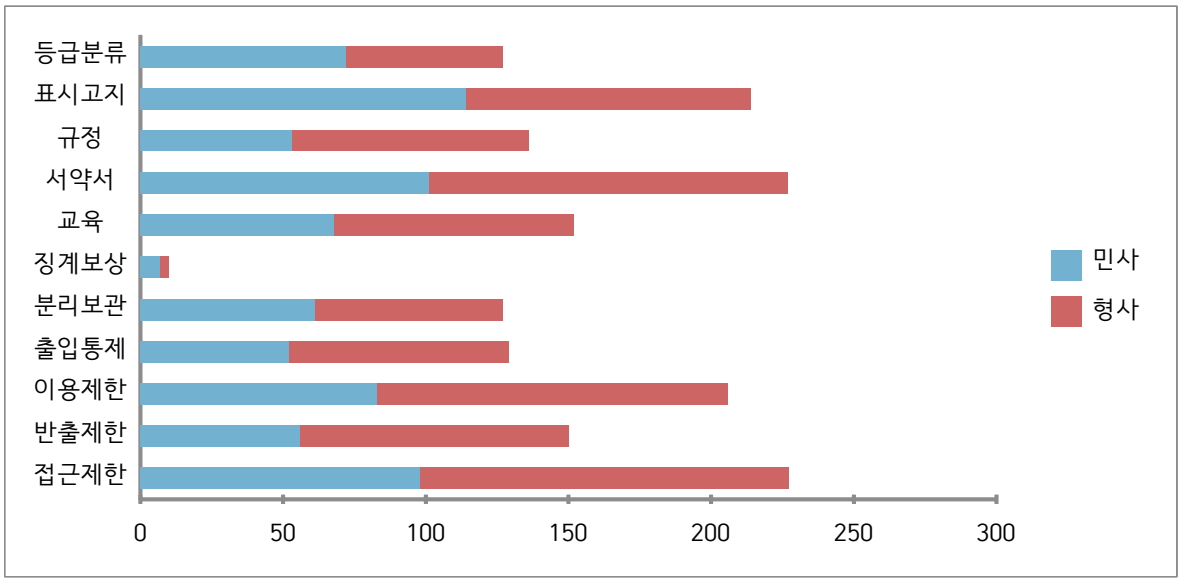
2.2 영업비밀 보호관리 조치별 분석 결과

전체 사건에서 법원이 비밀관리성 판단을 하면서 가장 많이 언급한 보호관리 조치는 민·형사 사건 모두 “서약서”와 “접근제한”이였으며, 다음으로 영업비밀임을 표시 또는 고지했는지 여부와 이용제한 조치 순으로 나타났다. 가장 빈도가 높은 4개의 조치는 영업비밀 보유자가 반드시 취해야 하는 필수적인 조치라 할 수 있다.

[표 7] 영업비밀 보호관리 조치별 빈도 수

구분	제도적 관리			인적 관리			물적 관리				
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
민사	76	**118**	62	**133**	70	7	62	58	85	57	**102**
형사	59	**106**	95	**155**	96	3	71	84	**127**	96	**140**
합계	135	**224**	157	**288**	166	10	133	142	212	153	**242**

이 중, 제도적·인적 관리조치 5가지의 전체(징계/보상 제외) 빈도수는 970회인데 반해, 물리적 관리조치의 전체 빈도수는 882회인 것으로 나타나 비밀관리성 인정에 있어 상대적으로 제도적·인적 관리조치를 취했는지 여부가 훨씬 더 빈번하게 언급되었다는 것을 알 수 있다.



[그림 6] 영업비밀 보호관리 조치별 빈도 수

2.3 영업비밀 정보 유형별 분석 결과

판례에서 문제된 영업비밀을 정보 유형별로 나누어 살펴보면, 경영정보가 105건, 기술정보가 202건으로 기술정보의 유출 사건이 약 2배에 달했다.

[표 8] 영업비밀 정보 유형별 분석 결과

구분		인정	부정	전체
민사	경영정보	16	43	59
	기술정보	45	47	92
	기술+경영정보	11	19	30
	합계	72	109	**181**
형사	경영정보	26	20	46
	기술정보	66	44	110
	기술+경영정보	14	17	31
	합계	106	81	**187**
전체	경영정보	42 (40.0%)	63 (60.0%)	**105**
	기술정보	111 (54.9%)	91 (45.1%)	**202**
	기술+경영정보	25 (41.0%)	36 (59.0%)	**61**
	합계	178	190	**368**

경영정보가 유출된 105건의 판결에서 비밀관리성이 인정된 비율은 40%(42건/105건)인데 반해, 기술정보가 유출된 202건의 판결에서 비밀관리성이 인정된 비율은 54.9%(111건/202건)로, 경영정보에 대한 비밀관리성 인정 비율이 상대적으로 낮은 것으로 나타났다.

영업비밀 정보 유형별 보호관리 조치의 빈도수를 살펴보면, 경영정보의 경우에는 서약서 징구, 표시 또는 고지, 접근제한과 이용제한이 중요하며, 기술정보의 경우에도 거의 동일하지만 '출입통제'가 이루어졌는지 여부가 자주 언급된 것으로 나타났다.

[표 9] 영업비밀 정보 유형별 빈도 수

구분	판단	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
경영 정보	관리성 인정	14	15	13	**34**	18	1	9	5	**23**	8	**28**
	관리성 부정	25	**49**	17	**39**	29	1	14	10	31	24	**39**
기술 정보	관리성 인정	36	52	54	**103**	51	4	51	**62**	61	47	**75**
	관리성 부정	40	**72**	43	**64**	40	1	41	39	56	45	**61**

그 중, 민사 판례(181건)의 유형별 보호조치 빈도수를 분석한 결과는 다음과 같다.

민사	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
경영 정보	26	**38**	12	**38**	26	1	13	6	25	16	**31**
기술 정보	39	**63**	36	**70**	33	3	40	44	43	31	**55**
합계	76	**118**	62	**133**	70	7	63	59	85	58	**103**

형사 판례(187건)의 유형별 보호조치 빈도수를 분석한 결과는 다음과 같다.

형사	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
경영 정보	13	26	18	**35**	21	1	10	9	**29**	16	**36**
기술 정보	37	61	61	**97**	58	2	52	57	**74**	61	**81**
합계	59	106	95	**155**	96	3	71	84	**127**	96	**140**

2.4 기술 분야별 분석 결과

영업비밀에 해당하는지 여부가 쟁점이 된 정보가 속한 (기술)분야별로 살펴본 결과, 기계소재 분야가 133건으로 가장 많았고, 다음으로 서비스업, 전기전자, 정보통신, 화학 순으로 많았다. 이 중, 서비스업의 경우 관리성 인정 비율이 다른 분야에 비해 낮은 것으로 파악되었다.

[표 10] 기술 분야별 분석 결과

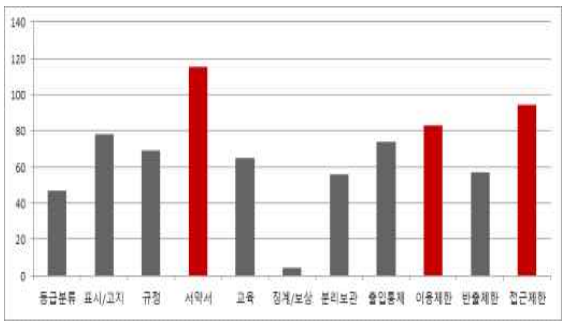
구분	예시/설명	인정(비율)	부정(비율)	전체
기계소재	정밀생산기계, 산업/일반기계, 조선/해양시스템 등	**72 (54.1%)**	**61 (45.9%)**	**133**
바이오의료	의약/산업 바이오, 치료기기, 의료정보 등	6 (37.5%)	10 (62.8%)	16
에너지자원	자원, 원자력, 신재생에너지, 에너지효율향상 등	2 (50.0%)	2 (50.0%)	4
전기전자	반도체장비, 가정용기기, 디스플레이 등	**34** (63.0%)	**20** (37.0%)	**54**
정보통신	이동통신, 소프트웨어, 디지털콘텐츠 등	**15** (42.9%)	**20** (57.1%)	**35**
서비스업	유통/물류/마케팅 서비스, 여행업체, 배달업, 학원 등	**16** (25.4%)	**47** (74.6%)	**63**
화학	고분자재료, 화학공정, 화학제품, 섬유제품 등	**20** (58.8%)	**14** (41.2%)	**34**
기타	상기 분류에 속하지 않거나, 명확한 분류를 할 수 없는 경우	13 (44.8%)	16 (55.2%)	29
합계		**178(48.4%)**	**190(51.6%)**	**368**

보호관리 조치를 기준으로 살펴볼 때, 모든 분야에서 서약서 징구 여부의 빈도가 가장 높았으며, 서비스 분야의 경우 표시/고지 여부의 빈도수가 상대적으로 높은 점이 특징적이었다. 분리·보관 등 물적 관리 조치 중에서는 공통적으로 접근 제한과 이용 제한의 빈도가 가장 높았으며, 기술 분야별로 관리 조치의 내용에 현저한 차이를 보이지는 않는다.

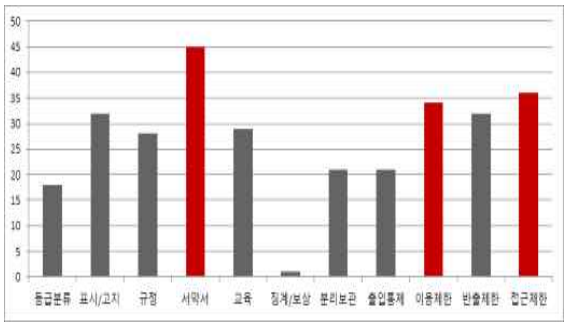
[표 11] 기술 분야별 빈도 수

구분	사건 수	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
기계 소재	133	47	78	69	**115**	65	4	56	74	**83**	57	**94**
전기 전자	54	18	32	28	**45**	29	1	21	21	**34**	32	**36**
정보 통신	35	17	**23**	16	**28**	15	2	18	13	18	20	**21**
서비스	63	17	**42**	12	**40**	24	1	15	4	35	15	**40**

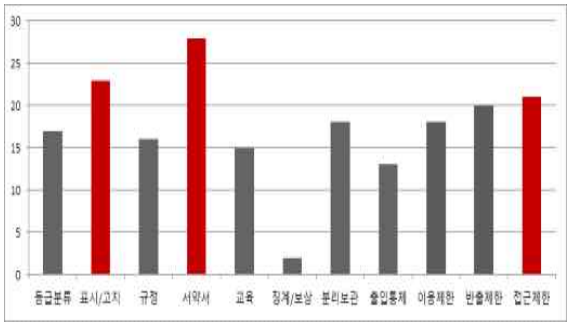
기계소재



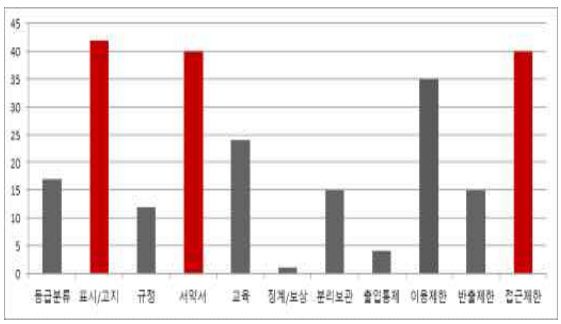
전기전자



정보통신



서비스



기술 분야별 민사 사건(181건)의 보호조치 빈도수를 분석한 결과는 다음과 같다.

민사	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
기계 소재	25	**34**	27	**53**	26	3	26	32	30	18	**37**
전기 전자	7	**9**	8	**11**	**9**	0	4	4	7	8	**9**
정보 통신	11	**15**	10	**17**	9	2	9	8	**12**	9	11
일반 서비스	16	**34**	9	**31**	19	1	12	4	24	13	**28**

기술 분야별 형사 사건(187건)의 보호조치 빈도수를 분석한 결과는 다음과 같다.

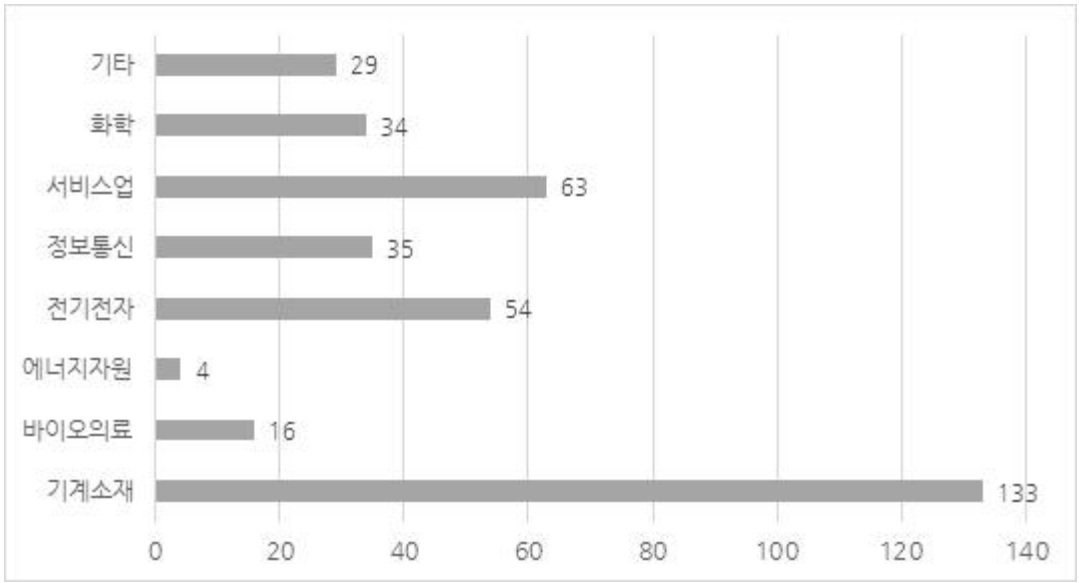
형사	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
기계 소재	22	44	42	**62**	39	1	30	42	**53**	39	**57**
전기 전자	11	23	20	**34**	20	1	17	17	**27**	24	**27**
정보 통신	6	8	6	**11**	6	0	9	5	6	**11**	**10**
일반 서비스	1	8	3	**9**	5	0	3	0	**11**	2	**12**

위 분석은 기술 분야별로 민사 사건과 형사 사건에 어떤 차이가 있는지를 알아보기 위한 것이었으나, 기술 분야별로 민사 사건과 형사 사건 간에 뚜렷한 차이가 나타나지는 않았다.

다만, 민사 사건의 경우 전체 181건 중 서약서를 징구하였는지 여부는 112회(약 61%), 표시/고지가 92회(약 50%)이고, 접근제한은 85회(약46%), 이용제한은 73회(약 40%)인데 반해, 형사 사건(총 187건)에서는 서약서가 116회(62%), 표시/고지가 83회(약 44%). 접근제한이 106회(약 56%), 이용제한이 97회(약 51%)로 나타나, 형사 사건에서 조금 더 물적 관리 조치에 대한 언급이 많은 편이라 할 수 있다.

본 연구에서 기술 분야별로 영업비밀 관리 조치를 분석한 이유는 업종별로 영업비밀 보호·관리에 차이가 있다는 경험적 가설 때문이었다. 다만 종전과 같이 표준산업분류에 따를 경우 대부분의 기업이 제조업에 속하는 관계로 '업종'별 특성을 파악하기 어렵기 때문에, 이 연구에서는 판결문에 기재된 내용을 기초로 – 예컨대, 영업비밀인지 여부가 쟁점이 된 정보가 "플라스틱 성형 가공법", "금형설계자료" 이면 기술 분야를 "기계 소재"로 하고, "소스코드", "센서제조방법" 등인 경우 "전기전자"로 하는 등 – 기술 분야별 특징을 살펴보고자 하였다. 결과론적으로는 대상 판결 분석을 통해서는 기계 소재 분야의 사건이 가장 많았다는 점을 제외하고는 기술 분야를 불문하고 법원이 고려하는 영업비밀 관리 조치의 내용이나 빈도는 대동소이한 것으로 보인다.

[그림 7] 기술 분야별 사건 수



2.5 기업 규모를 고려한 판결

법원이 비밀관리성 여부를 판단함에 있어 종업원 수나 자본금 등 기업의 규모를 고려할 때 비밀관리성이 인정된다고 판단한 사건이 20건, 기업 규모를 고려하더라도 비밀관리성이 인정되지 않는다고 판단한 사건이 20건으로 확인되었다.

[표 12] 기업 규모를 고려한 판결 분석 결과

구분		인정	부정	전체
전체	민사	8	10	18
	형사	12	10	22
	합계	**20**	**20**	**40**

기업 규모 등을 고려하여 비밀관리성을 인정한 사건의 경우 서약서 징구, 표시/고지와 이용제한 및 접근 제한 조치를 취했는지 여부를 가장 자주 언급하였고, 규모 등을 고려하더라도 비밀관리성을 부정한 사건에서도 서약서, 접근제한, 등급분류, 표시/고지가 가장 자주 언급되었다.

[표 13] 기업 규모를 고려한 판결 빈도 수

구분	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	5	**14**	7	**18**	8	4	9	6	**12**	7	**13**
관리성 부정	**15**	**15**	10	**18**	12	0	8	6	13	8	**16**
전체	20	**29**	17	**36**	20	4	17	12	**25**	15	**29**

다만, 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 무엇인지 까지는 명확하게 나타나지 않았다.

2.6 의의 및 한계

영업비밀 관련 판례의 분석은 부정경쟁방지 및 영업비밀 보호에 관한 법률 집행 현황 차원이나[1], 영업비밀 침해 사건의 유형 및 쟁점, 사건 처리 기간 및 법원 등에 관해[2], 또는 비밀관리성의 판단 요소별 빈도 중심으로 이루어진 바 있다[3].

본 연구를 통해 목표한 바는 영업비밀 관련 판결 분석을 통해 기업의 규모·업종별로 영업비밀 관리 조치가 어떤 차이가 있는지를 중심으로, 법원이 비밀관리성을 판단함에 있어 고려하는 요소가 기술 분야별로, 정보의 유형별로, 민사·형사 사건에 따라 어떤 차이를 보이는지 등을 종합적으로 분석해보고자 한 것이다.

앞서 살펴본 바와 같이, 연도별 추이를 볼 때 비밀관리성이 인정되는 비율이 다소 높아지고 있는 것은 법률 개정으로 비밀관리성 요건이 완화된 것과 일정 부분 관련이 있는 것으로 보이며, 비밀관리성 판단에 있어 기업의 규모나 업종 등을 고려한 사건이 40건 가량 확인되었고, 특히 최근 판결에서는 법원이 명시적으로 “비밀관리성의 상대성”에 관해 구체적으로 판시하고 있는 것은 주목할 만하다(보고서 50페이지 참조)[4].

이외에도 이번 연구에서는 기술 분야별, 민사·형사 사건별, 정보 유형별, 기업 규모·업종별로 법원이 고려하는 영업비밀 관리 조치가 내용적으로나 빈도상으로 어떤 차이를 보이는지를 살펴보았는데, 단정적인 결론을 내릴 수 있을 정도로 현저한 차이를 확인하지는 못했지만 몇 가지 의미 있는 단서를 확인할 수 있었다.

즉, 정보의 유형별로 볼 때 경영정보 보다 기술정보가 문제된 사건에서 법원이 접근 제한 등 물적 관리 조치를 더 자주 언급했다는 것의 의미는 영업비밀 보유자인 기업 등이 보유한 주요 정보가 기술정보인지 경영정보인지에 따라 비밀 관리 조치의 내용을 달리해야 한다, 즉 기술정보에 대해서는 물적 관리 조치를 강화해야 한다는 의미로 해석할 수 있다.

---

1) 부정경쟁방지 및 영업비밀보호에 관한 법률 집행 현황 연구, 특허청, 2014
2) 영업비밀 및 부정경쟁행위 국내 판결문 구축, 특허청, 2016 및 부정경쟁방지법 관련 국내 판결문 분석 연구, 특허청, 2017
3) 꼭 알아야 할 영업비밀 보호 가이드, 특허청, 2014
4) 서울동부지방법원 2019. 3. 13. 선고 2018고단2485 판결

또, 기술 분야별로 볼 때도 장비 설계도 등이 문제된 기계소재 분야 대비 소스 코드 등이 문제된 전기전자, 정보통신 분야의 영업비밀 사건에서 접근 제한 등 물적 관리 조치를 취했는지 여부의 빈도가 조금 더 높게 나왔다는 점은, 정보의 속성, 즉 도면이나 문서와 같은 유형물의 형태로 존재하는 정보와 코드 등 디지털 형태의 정보가 가지는 성질상의 차이에 기인한 것으로 생각할 수 있다.

이번 연구를 통해 민사 사건 보다는 형사 사건에서 비밀관리성이 인정되는 비율이 더 높은 것으로 확인되었으나[5], 사건 유형별로 영업비밀 관리 조치의 내용이나 빈도가 크게 다르지는 않은 것으로 보인다[6]. 어느 경우에 있어서나 법원은 사실 관계 및 증거 등을 종합적으로 고려하여 판단하고 있기 때문으로 추정된다.

판결은 구체적인 사안에서 법원이 당사자의 주장 및 사실 관계, 증거 등을 종합적으로 고려한 결과물이라는 점에서 판결문에 기재된 문구만으로 그 의미를 일반화하는 것은 매우 어려운 일이다. 게다가, 비밀관리성은 대법원이 일관된 입장을 견지하고 있는 것처럼, '객관적으로 인식 가능한 상태'에 이르렀는지 여부를 판단하기 위해 영업비밀 보유자가 어떤 조치를 취했는지를 종합적으로 판단할 수밖에 없기 때문에, 더더욱 명쾌한 결론을 도출하기 어려운 본질적인 한계가 있다.

본 연구는 2015년부터 2019년 상반기까지 선고된 영업비밀 관련 판결 1,596건 중 비밀관리성이 쟁점이 된 판결 368건을 분석한 것으로, 정보 유형별, 기술분야별, 기업 규모·업종별 관리 조치의 구체적인 차이를 확인하고자 했다는 점에서 의미를 찾을 수 있지만, 내용이나 방법 등 모든 측면에서 후속 연구를 통해 이번 연구의 결과물에 대한 검증 및 보완, 추가 분석이 필요함은 물론이다.

5) 형사 사건의 경우 경찰이나 검찰에서 비밀관리성 요건을 충족하지 못한 것으로 판단될 경우 무혐의 처분 등을 통해 기소가 되지 않으므로, 기소된 사건에 대한 판결만을 기준으로 민사 사건에 비해 형사 사건의 비밀관리성 인정 비율이 더 높다고 단정하기 어렵다. 더구나, 형사 사건에서는 무죄추정의 원칙 등에 따라 엄격한 입증이 요구되기 때문에 민사 사건에 비해 비밀관리성이 더 쉽게 인정되는 것은 아니라고 할 수도 있다.

6) 민사 사건 대비 형사 사건에서 법원이 접근 제한 등 물적 관리 조치를 고려한 빈도가 조금 더 높게 나타났지만 (10페이지 표 7 참조), 이것만으로는 형사 사건에서는 물적 관리 조치가 더 중요하다고 단정하기는 어렵다.

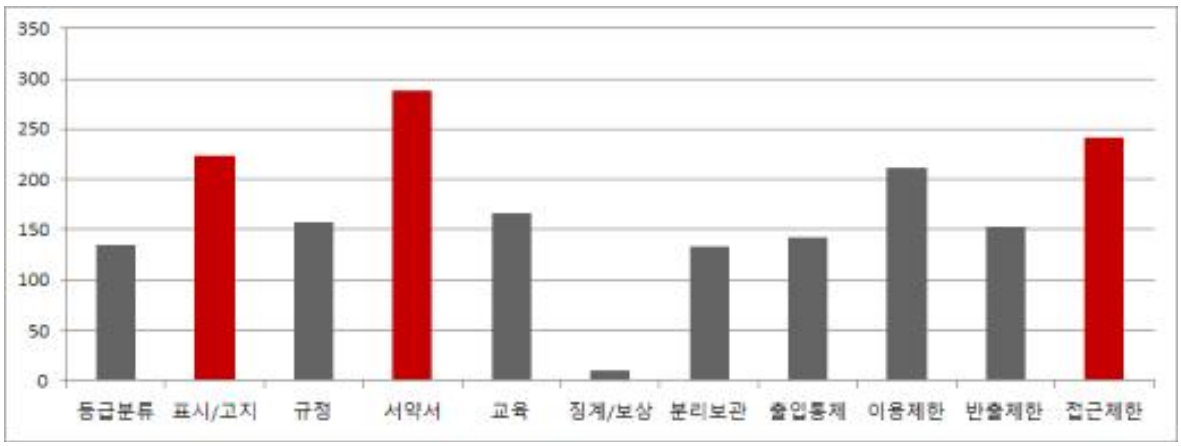
3. 분석 결과(상세)

3.1 영업비밀 보호관리 조치별 분석

3.1.1 전체 판례 보호관리 조치별 빈도수 분석

- 전체 368건 판례에서 가장 많이 언급된 영업비밀 보호관리 조치는 서약서 징구 여부였으며, 다음으로 접근제한, 표시/고지 순으로 나타났다.

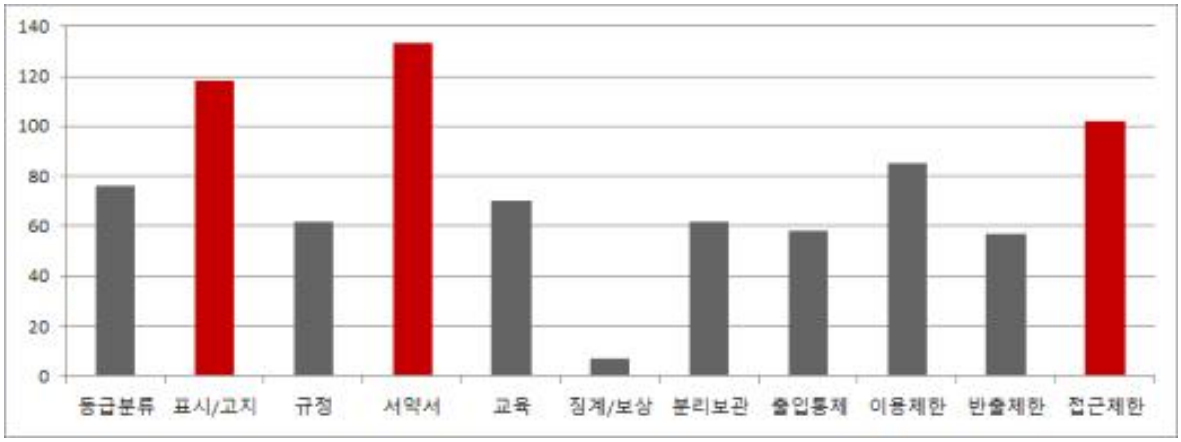
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	135	**224**	157	**288**	166	10	133	142	212	153	**242**
순위	9	**3**	6	**1**	5	11	10	8	4	7	**2**



3.1.2 민사 판례 보호관리 조치별 빈도수 분석

- 민사 181건의 보호관리 조치별 빈도수를 살펴보면, 서약서, 표시/고지, 접근제한 순으로 나타났다.

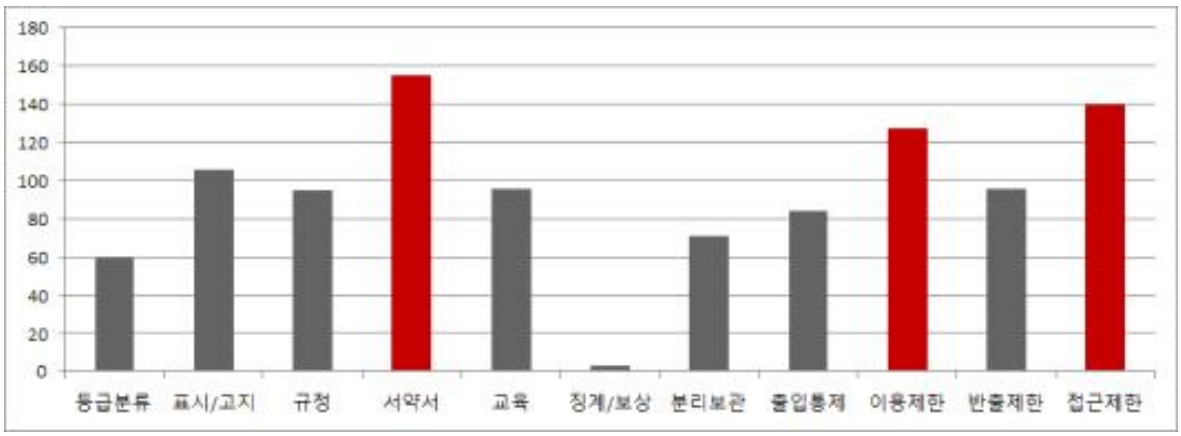
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	76	**118**	62	**133**	70	7	62	58	85	57	**102**
순위	5	**1**	7	**2**	6	11	7	9	4	10	**3**



3.1.3 형사 판례 보호관리 조치별 빈도수 분석

- 형사 187건의 보호관리 조치별 빈도수를 분석한 결과, 민사와 마찬가지로 서약서 징구여부가 가장 많이 언급되었고, 다음으로는 접근제한, 이용제한 순인 것으로 분석되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	59	106	95	**155**	96	3	71	84	**127**	96	**140**
순위	10	4	7	**1**	5	11	9	8	**3**	5	**2**



3.2 영업비밀 정보 유형별 분석

3.2.1 분석 대상 판례

- 전체 368건 판례의 영업비밀 유형을 경영정보(105건), 기술정보(202건), 기술정보와 경영정보가 모두 포함된 건(61건)으로 나누어 보호관리 조치별 빈도수를 분석하였다.

구분		인정	부정	전체
민사	경영정보	16	43	59
	기술정보	45	47	92
	기술+경영정보	11	19	30
	합계	72	109	**181**
형사	경영정보	26	20	46
	기술정보	66	44	110
	기술+경영정보	14	17	31
	합계	106	81	**187**
전체	경영정보	42 (40.0%)	63 (60.0%)	**105**
	기술정보	111 (54.9%)	91 (45.1%)	**202**
	기술+경영정보	25 (41.0%)	36 (59.0%)	**61**
	합계	178	190	**368**

- 전체 대상 판결 중 고객명부 등 경영정보가 유출된 사건에서 법원이 해당 정보의 비밀관리성을 인정한 비율은 40%(42건/105건)이며, 설계도면 등 기술정보가 유출된 사건의 경우에는 54.9%, 경영정보와 기술정보가 모두 유출된 사건의 경우에는 40.9%로 나타났다.

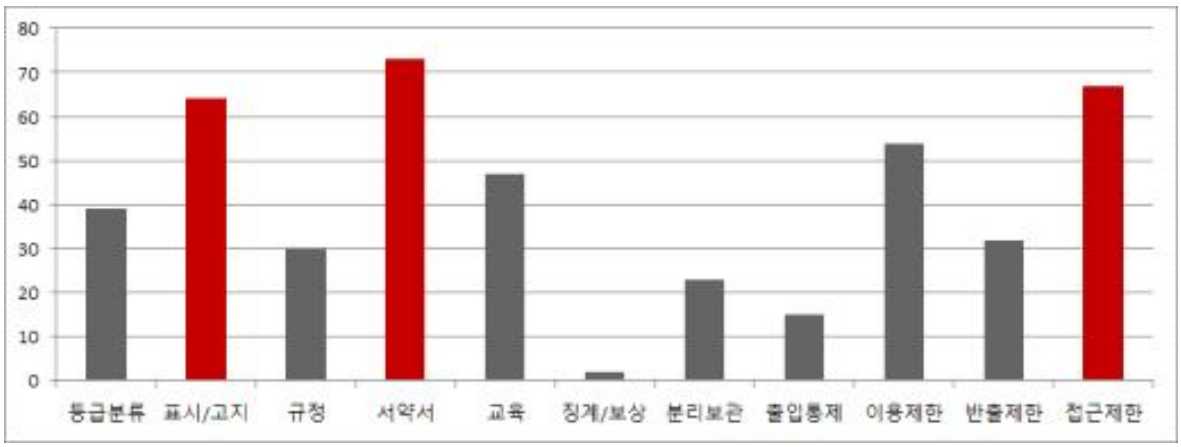
- 민/형사 사건을 나누어 보면, 기술정보가 유출된 민사 사건의 경우 관리성 인정 비율이 48.9%(45건/92건)인데 반해 기술정보가 유출된 형사 사건은 54,5%(66건/110건)이며, 경영정보가 유출된 민사 사건의 관리성 인정 비율은 27.1%(16건/59건), 형사 사건은 56.5%(26건/46건)인 것으로 나타났다.

3.2.2 전체 판례 분석

가. 경영정보

- 영업비밀 유형이 경영정보에 해당하는 105건 판례의 보호관리 조치별 빈도수를 분석한 결과, 서약서 징구여부가 가장 많이 언급된 것으로 나타났다. 이는 대법원이 일관되게 제시하고 있는 “객관적으로 정보가 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태”, 즉 “객관적 인식 가능성”을 확보하기 위해 기업 등 영업비밀 보유자가 취할 수 있는 가장 기본적인 조치이자 실제로도 가장 흔히 취해지는 조치이기 때문으로 보인다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	39	**64**	30	**73**	47	2	23	15	54	32	**67**
순위	6	**3**	8	**1**	5	11	9	10	4	7	**2**



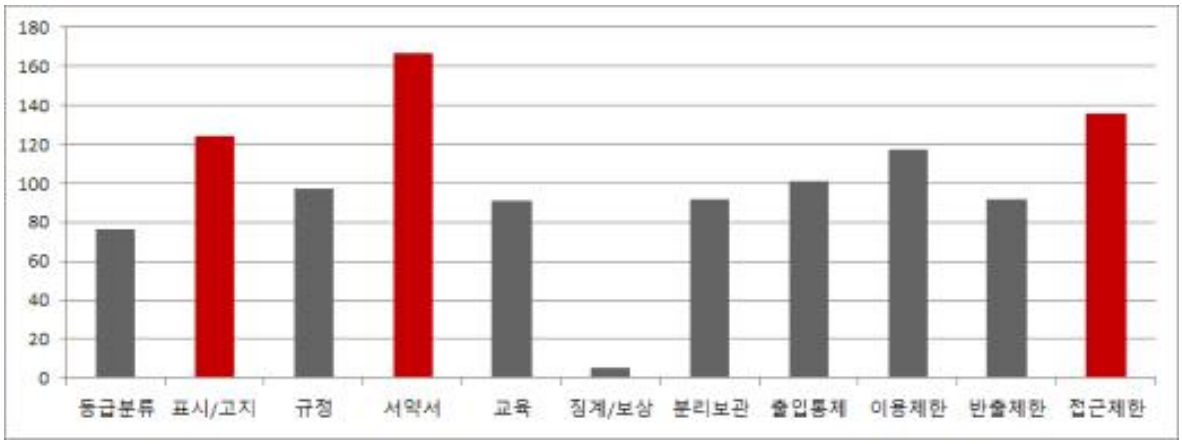
- 유출된 경영정보의 비밀관리성을 인정한 판례에서는 서약서 징구여부, 부정한 판례에서는 표시/고지 여부의 언급 빈도가 가장 높은 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	14	15	13	**34**	18	1	9	5	**23**	8	**28**
관리성 부정	25	**49**	17	**39**	29	1	14	10	31	24	**39**

나. 기술정보

- 영업비밀 유형이 기술정보에 해당하는 202건 판례를 분석한 결과, 서약서 징구 여부, 접근제한이 이루어졌는지 여부, 표시/고지 여부 순으로 많이 언급된 것으로 나타났다. 경영정보의 경우 전체 105건 중에 접근 제한 여부를 언급한 판결이 67건(약 63%)인데 반해, 기술정보의 경우 접근 제한 여부를 언급한 판결이 136건(약 67%)으로 조금 더 높고, 분리보관 등 다른 물적 관리 조치들의 경우에도 기술정보가 문제된 사건이 경영정보가 문제된 사건에 비해 빈도가 높게 나타났다. 이것은 설계도, 소스코드 등 기술정보의 경우 고객정보와 같은 경영정보에 비해 그 속성상 영업비밀로 특정하기 쉽고, 자주 변경되지 않는데다, 해당 정보에 접근하는 임직원의 수가 상대적으로 더 적은 경우가 많기 때문인 것으로 추정된다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	76	**124**	97	**167**	91	5	92	101	117	92	**136**
순위	10	**3**	6	**1**	9	11	7	5	4	7	**2**



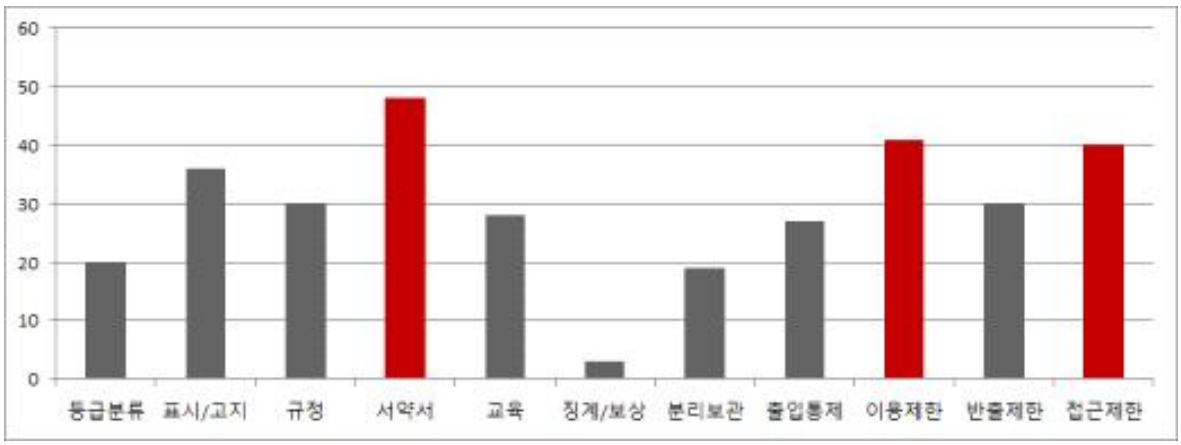
- 유출된 기술정보의 비밀관리성을 인정/부정한 판례의 보호관리 조치별 빈도수에 있어서는, 인정한 판례에서는 서약서 징구여부가, 부정한 판례에서는 표시/고지 여부가 가장 많이 언급되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	36	52	54	**103**	51	4	51	**62**	61	47	**75**
관리성 부정	40	**72**	43	**64**	40	1	41	39	56	45	**61**

다. 기술정보 및 경영정보

- 영업비밀 유형이 기술정보와 경영정보 모두에 해당하는 61건 판례의 보호관리 조치별 빈도수를 분석한 결과, 다른 경우와 마찬가지로 서약서 징구여부의 빈도수가 가장 높았다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	20	36	30	**48**	28	3	19	27	**41**	30	**40**
순위	9	4	5	**1**	7	11	10	8	**2**	5	**3**



- 유출된 기술/경영정보의 비밀관리성을 인정/부정한 판례의 보호관리 조치별 빈도수를 분석한 결과 경영정보 또는 기술정보와 마찬가지로 서약서와 표시/고지가 가장 자주 언급된 것으로 나타났다.

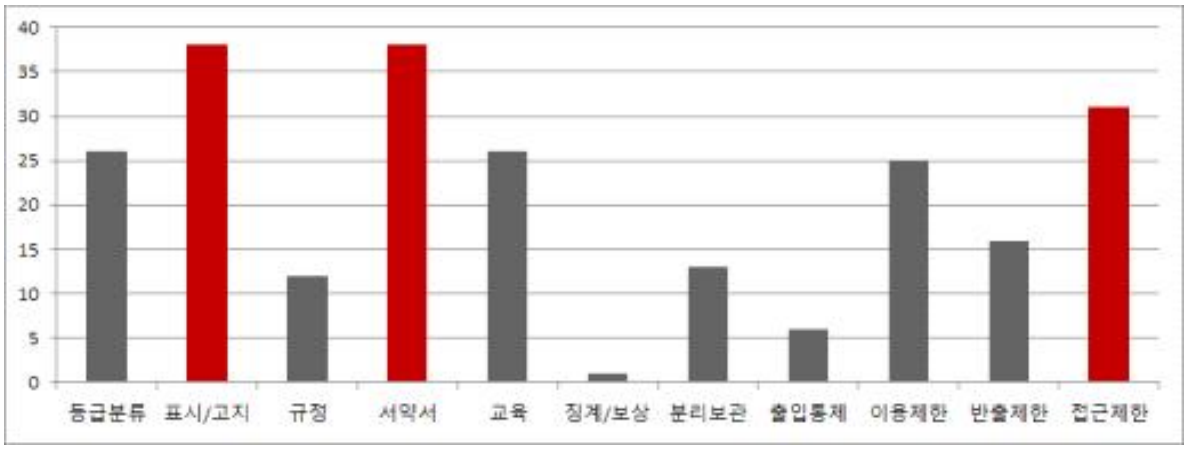
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	6	8	12	**23**	10	3	9	12	**15**	9	**14**
관리성 부정	14	**28**	18	25	18	0	10	15	**26**	21	**26**

3.2.3 민사 판례 분석

가. 경영정보

- 영업비밀 유형이 경영정보에 해당하는 105건 판례 중 민사 59건 대한 빈도수를 분석한 결과, 표시/고지 여부와 서약서 징구여부의 언급 빈도가 가장 높았다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	26	**38**	12	**38**	26	1	13	6	25	16	**31**
순위	4	**1**	9	**1**	4	11	8	10	6	7	**3**



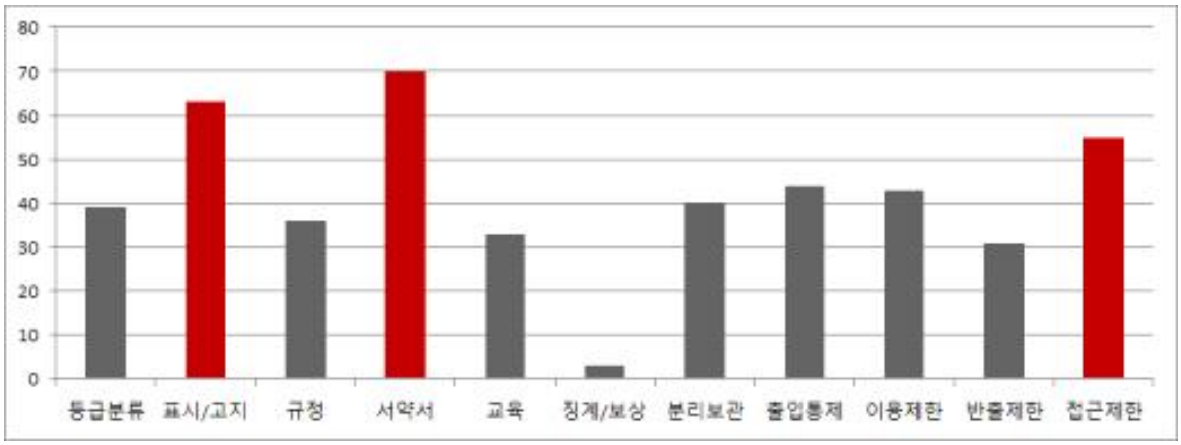
- 이 중, 유출된 경영정보의 비밀관리성을 인정한 판례에서는 서약서 징구여부가, 부정한 판례에서는 표시/고지 여부가 가장 많이 언급된 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	7	7	3	**15**	**8**	0	3	1	6	2	**9**
관리성 부정	19	**31**	9	**23**	18	1	10	5	19	14	**22**

나. 기술정보

- 영업비밀 유형이 기술정보에 해당하는 202건 판례 중 민사 92건에 있어서는 서약서 징구, 표시/고지, 접근제한 순으로 언급 빈도가 높은 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	39	**63**	36	**70**	33	3	40	44	43	31	**55**
순위	7	**2**	8	**1**	9	11	6	4	5	10	**3**



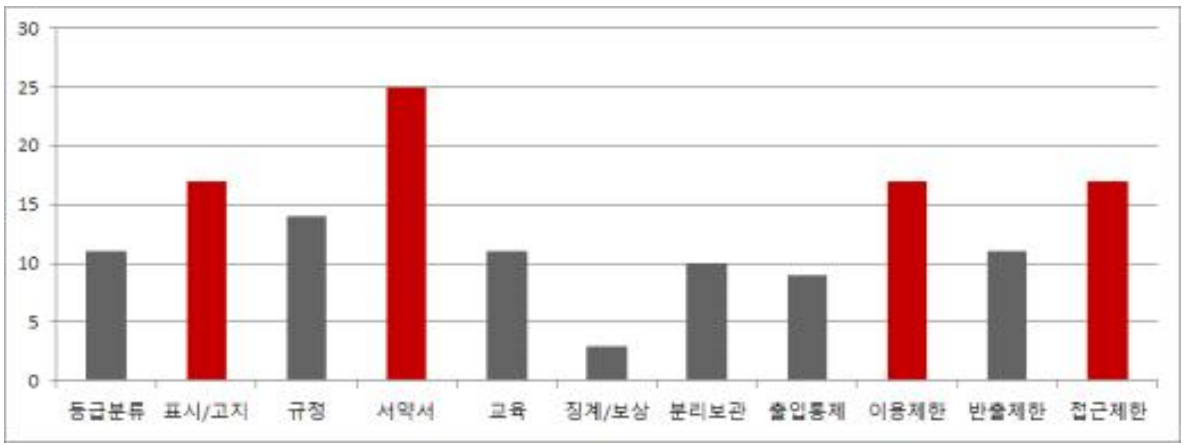
- 이 중, 유출된 기술정보의 비밀관리성을 인정한 판례에서는 경영정보의 경우와 마찬가지로 서약서 징구 여부가, 부정한 판례 역시 경영정보의 경우와 마찬가지로 표시/고지 여부가 가장 많이 언급된 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	20	23	21	**41**	20	2	22	**31**	18	15	**26**
관리성 부정	19	**40**	15	**29**	13	1	18	13	25	16	**29**

다. 기술정보 및 경영정보

- 영업비밀 유형이 기술정보 및 경영정보 모두에 해당하는 61건 판례 중 민사 30건에 대한 빈도수를 분석한 결과, 서약서 징구여부가 가장 자주 언급되었고, 표시/고지, 이용제한, 접근제한이 그 다음으로 자주 언급되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	11	**17**	14	**25**	11	3	10	9	**17**	11	**17**
순위	6	**2**	5	**1**	6	11	9	10	**2**	6	**2**



- 이 중, 유출된 기술/경영정보의 비밀관리성을 인정/부정한 경우 모두 서약서 징구여부가 가장 자주 언급된 것으로 나타났다.

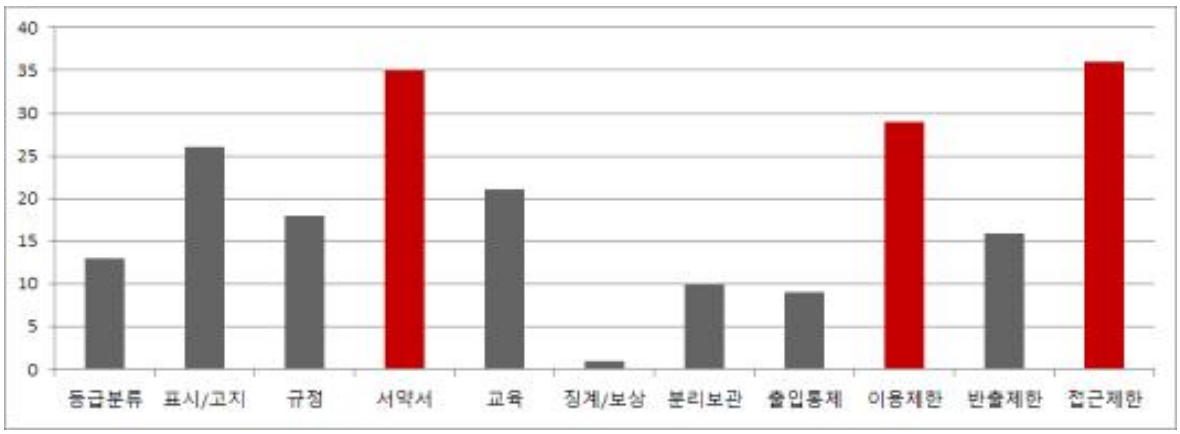
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	4	4	**7**	**10**	2	3	4	3	**6**	3	5
관리성 부정	7	**13**	7	**15**	9	0	6	6	11	8	**12**

3.2.4 형사 판례 분석

가. 경영정보

- 영업비밀 유형이 경영정보에 해당하는 105건 판례 중 형사 46건에 있어서는 접근제한 조치를 취했는지 여부가 가장 자주 언급된 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	13	26	18	**35**	21	1	10	9	**29**	16	**36**
순위	8	4	6	**2**	5	11	9	10	**3**	7	**1**



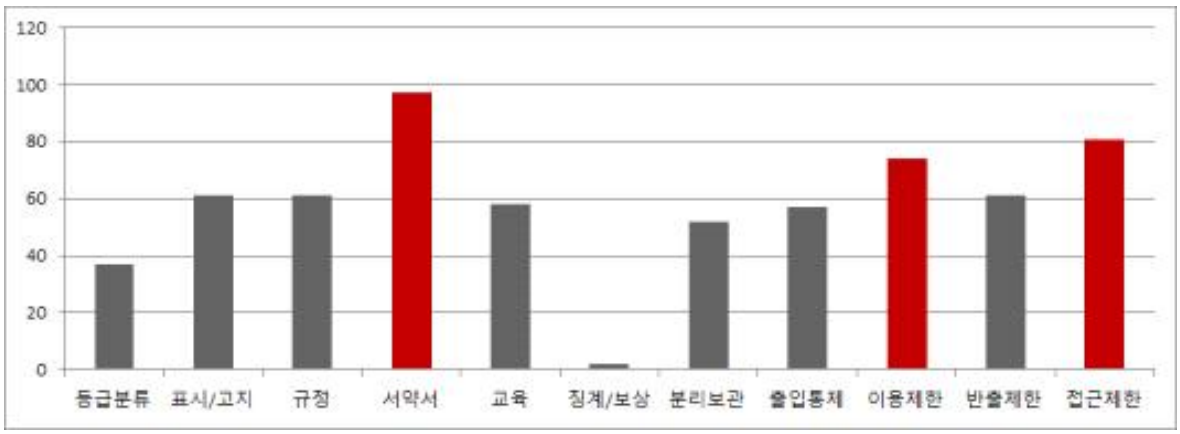
- 이 중, 유출된 경영정보의 비밀관리성을 인정한 판례에서는 서약서 징구여부와 접근제한 조치 여부, 부정한 판례에서는 표시/고지 여부의 언급 빈도가 가장 높았다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	7	8	10	**19**	10	1	6	4	**17**	6	**19**
관리성 부정	6	**18**	8	**16**	11	0	4	5	12	10	**17**

나. 기술정보

- 영업비밀 유형이 기술정보에 해당하는 202건 판례 중 형사판례를 분석한 결과, 서약서 징구여부, 접근제한 조치여부, 이용제한여부 순으로 언급 빈도가 높은 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	37	61	61	**97**	58	2	52	57	**74**	61	**81**
순위	10	4	4	**1**	7	11	9	8	**3**	4	**2**



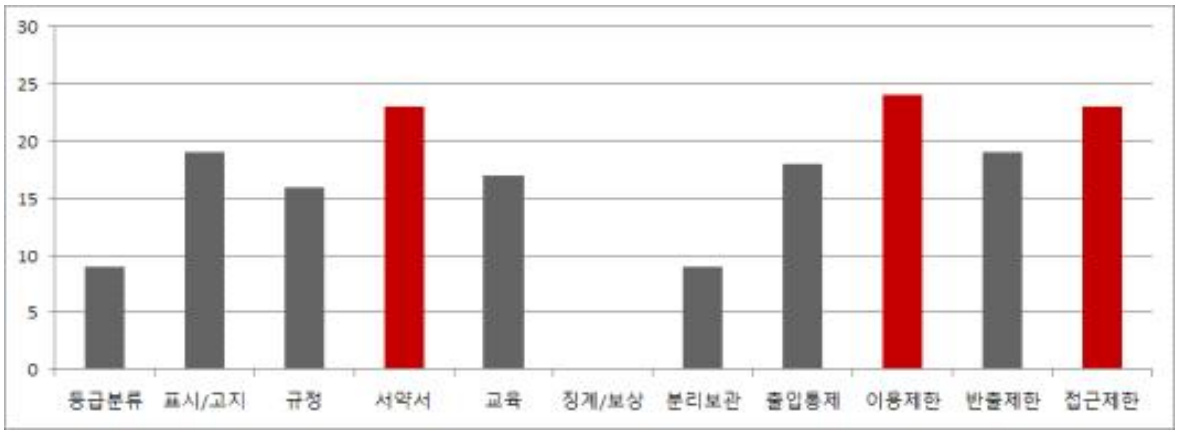
- 이 중, 유출된 기술정보의 비밀관리성을 인정한 판례와 부정한 판례 모두 서약서 징구여부가 가장 자주 언급되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	16	29	33	**62**	31	2	29	31	**43**	32	**49**
관리성 부정	21	**32**	28	**35**	27	0	23	26	31	29	**32**

다. 기술정보 및 경영정보

- 영업비밀 유형이 기술정보 및 경영정보 모두에 해당하는 61건 판례 중 형사 31건에 대한 보호관리 조치별 빈도수 분석

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	9	19	16	**23**	17	0	9	18	**24**	19	**23**
순위	9	4	8	**2**	7	11	9	6	**1**	4	**2**



- 이 중, 유출된 기술/경영정보의 비밀관리성을 인정한 판례는 서약서 징구여부를, 부정한 판례는 표시/고지여부와 이용제한 조치여부를 가장 자주 언급하였다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	2	4	5	**13**	8	0	5	**9**	**9**	6	**9**
관리성 부정	7	**15**	11	10	9	0	4	9	**15**	13	**14**

3.3 기술 분야별 분석

3.3.1 분석 대상 판례

- 전체 368건 판례에서 나타난 영업비밀 정보의 내용에 따라 산업분류를 준용하여 총 8개 분야, 즉 기계소재(133건), 바이오의료(16건), 에너지자원(4건), 전기전자(54건), 정보통신(35건), 일반서비스(63건)*, 화학(34건), 기타(29건)로 나누어 분석을 진행하였다.

* 산업기술혁신사업 공통 운영요령의 산업기술분류표를 준용하되, '지식서비스'는 분류 실익이 적어 '일반 서비스'로 변경함

- 이 중, 주요 분야(기계소재, 전기전자, 정보통신, 일반서비스, 화학 5개 분야)에 대한 보호관리 조치별 빈도수를 분석하였다.

구분	인정	부정	전체
기계소재	**72 (54.1%)**	**61 (45.9%)**	**133**
바이오의료	6 (37.5%)	10 (62.8%)	16
에너지자원	2 (50.0%)	2 (50.0%)	4
전기전자	**34 (63.0%)**	**20 (37.0%)**	**54**
정보통신	**15 (42.9%)**	**20 (57.1%)**	**35**
일반서비스	**16 (25.4%)**	**47 (74.6%)**	**63**
화학	20 (58.8%)	14 (41.2%)	**34**
기타	13 (44.8%)	16 (55.2%)	29
합계	**178 (48.4%)**	**190 (51.6%)**	**368**

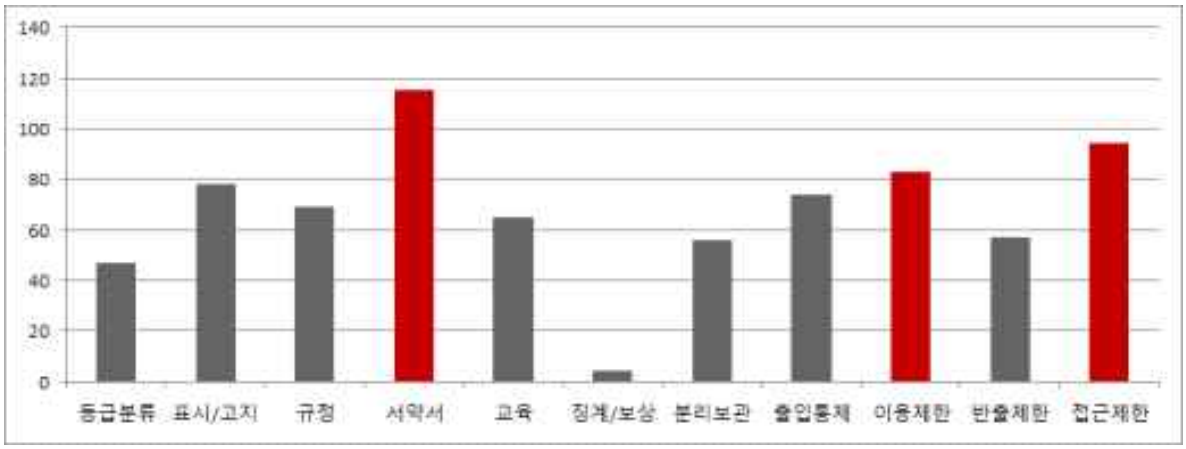
- 분석 대상 판례 중, 기계소재 분야의 사건 수가 가장 많았고, 다음으로는 일반서비스, 전기전자, 정보통신 순으로 나타났다.

3.3.2 전체 판례 분석

가. 기계소재

- 영업비밀이 기계소재 분야에 속하는 133건 판례의 보호조치 빈도수를 분석한 결과, 서약서, 접근제한, 이용제한 순으로 자주 언급된 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	47	78	69	**115**	65	4	56	74	**83**	57	**94**
순위	10	4	6	**1**	7	11	9	5	**3**	8	**2**



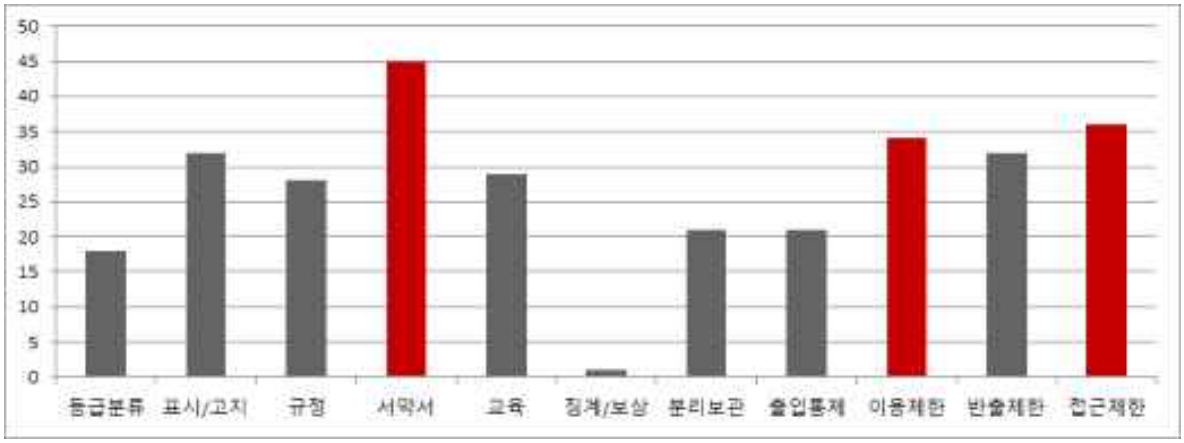
- 이 중, 비밀관리성이 인정된 판례에서는 서약서 징구여부의 언급 빈도가, 부정된 판례에서는 서약서 징구여부와 표시/고지여부의 언급 빈도가 가장 높았다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	25	31	36	**68**	34	3	30	**42**	**42**	26	**50**
관리성 부정	22	**47**	33	**47**	31	1	26	32	41	31	**44**

나. 전기전자

- 영업비밀이 전기전자 분야에 속하는 54건 판례에서는, 서약서 징구여부, 접근제한 조치여부, 이용제한여부 순으로 자주 언급된 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	18	32	28	**45**	29	1	21	21	**34**	32	**36**
순위	10	4	7	**1**	6	11	8	8	**3**	4	**2**



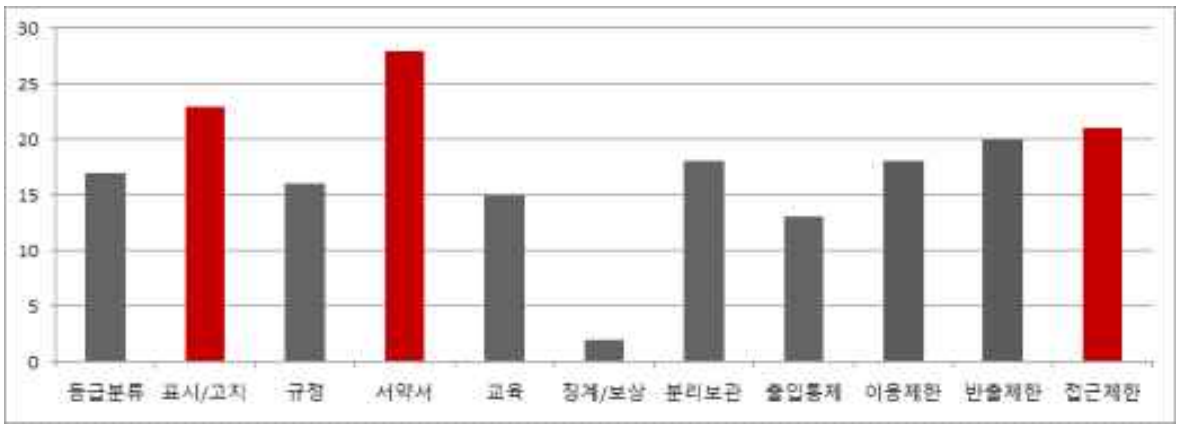
- 이 중, 비밀관리성이 인정된 판례에서는 서약서 징구여부가, 부정된 판례에서는 표시/고지여부 및 이용제한여부가 가장 자주 언급되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	11	17	16	**31**	**20**	1	14	12	19	18	**22**
관리성 부정	7	**15**	12	**14**	9	0	7	9	**15**	**14**	**14**

다. 정보통신

- 영업비밀이 정보통신 분야에 속하는 35건 판례를 분석한 결과, 기계소재나 전기전자와 마찬가지로 서약서 징구여부의 언급 빈도가 가장 높은 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	17	**23**	16	**28**	15	2	18	13	18	20	**21**
순위	7	**2**	8	**1**	9	11	5	10	5	4	**3**



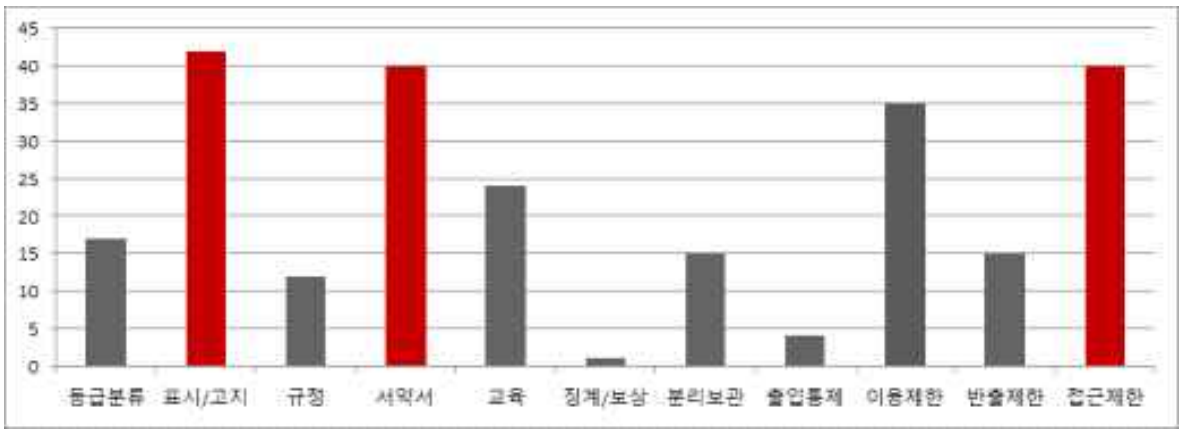
- 이 중, 비밀관리성을 인정한 판례는 서약서 징구여부를, 부정한 판례는 표시/고지 여부를 가장 많이 언급한 것으로 분석되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	4	6	**7**	**14**	3	2	**8**	4	6	**7**	**7**
관리성 부정	13	**17**	9	**14**	12	0	10	9	12	13	**14**

라. 일반서비스

- 영업비밀이 일반서비스 분야에 속하는 63건 판례의 빈도수를 분석한 결과, 표시/고지여부가 가장 많이 언급되었고 다음으로 서약서 징구여부와 접근제한 조치여부 순으로 자주 언급된 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	17	**42**	12	**40**	24	1	15	4	35	15	**40**
순위	6	**1**	9	**2**	5	11	7	10	4	7	**2**



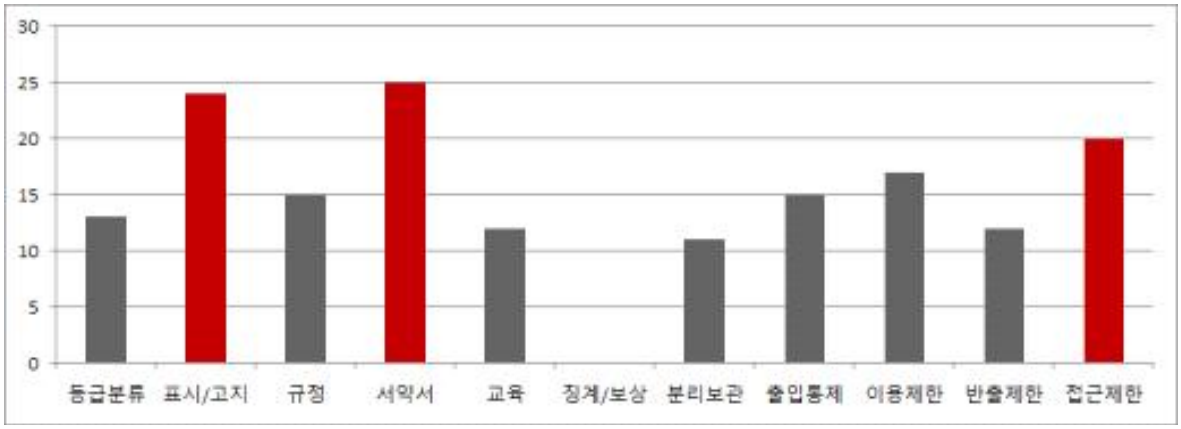
- 이 중, 비밀관리성이 인정된 판례에서는 서약서 징구여부가, 부정된 판례에서는 표시/고지여부가 자주 언급되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	4	6	3	**12**	4	0	5	2	**9**	1	**11**
관리성 부정	13	**36**	9	**28**	20	1	10	2	26	14	**29**

마. 화학

- 영업비밀이 화학 분야에 속하는 34건 판례의 경우, 서약서 징구여부, 표시/고지 여부, 접근제한 조치여부 순으로 언급 빈도가 높았다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	13	**24**	15	**25**	12	0	11	15	17	12	**20**
순위	7	**2**	5	**1**	8	11	10	5	4	8	**3**



- 이 중, 비밀관리성이 인정된 판례에서는 서약서 징구여부가, 부정된 판례에서는 표시/고지여부가 가장 많이 언급되었다.

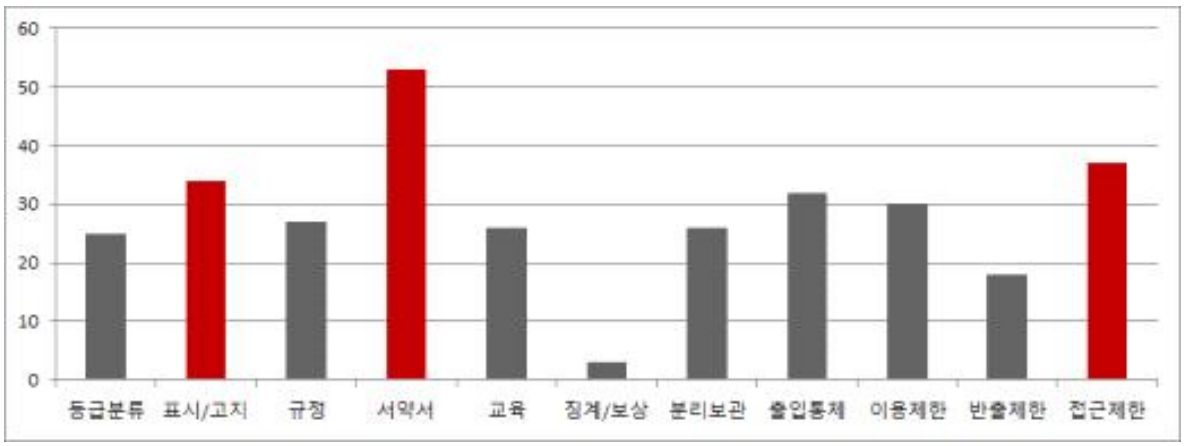
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	6	**11**	7	**17**	7	0	7	10	8	4	**11**
관리성 부정	7	**13**	8	8	5	0	4	5	**9**	8	**9**

3.3.3 민사 판례 분석

가. 기계소재

- 영업비밀이 기계소재 분야에 속하는 58건 판례의 경우, 서약서 징구여부, 접근제한 조치여부, 표시/고지여부 순으로 언급 빈도가 높은 것으로 분석되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	25	**34**	27	**53**	26	3	26	32	30	18	**37**
순위	9	**3**	6	**1**	7	11	7	4	5	10	**2**



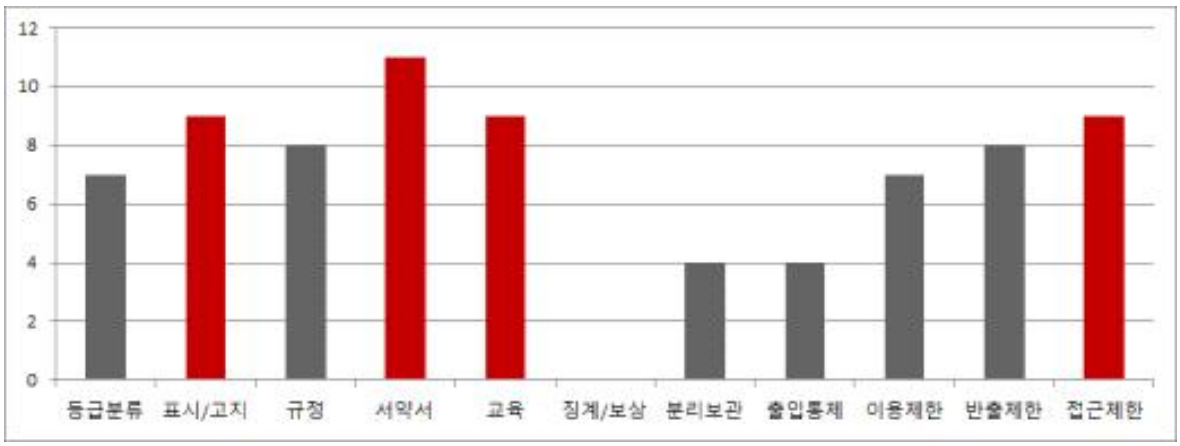
- 이 중, 비밀관리성이 인정/부정된 판례 모두 서약서가 가장 자주 언급되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	14	13	15	**30**	14	2	13	**21**	16	8	**20**
관리성 부정	11	**21**	12	**23**	12	1	13	11	14	10	**17**

나. 전기전자

- 영업비밀이 전기전자 분야에 속하는 16건 판례의 보호조치 빈도수를 분석한 결과, 서약서 징구여부가 가장 자주 언급되었고, 표시/고지, 교육, 접근제한이 그 다음으로 자주 언급된 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	7	**9**	8	**11**	**9**	0	4	4	7	8	**9**
순위	7	**2**	5	**1**	**2**	11	9	9	7	5	**2**



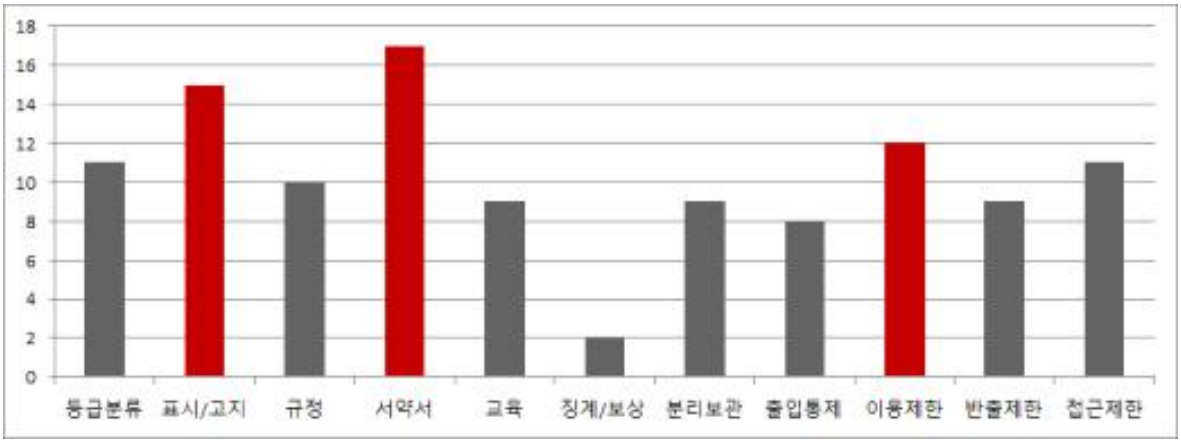
- 이 중, 비밀관리성을 인정한 판례에서는 서약서 징구여부를 가장 많이 언급한 것으로 나타났으나, 다른 보호조치들도 비슷한 빈도로 언급되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	**5**	**5**	**5**	**9**	**7**	0	3	2	3	**5**	**5**
관리성 부정	2	**4**	3	2	2	0	1	2	**4**	3	**4**

다. 정보통신

- 영업비밀이 정보통신 분야에 속하는 20건의 판례에서는, 서약서, 표시/고지, 이용제한 순으로 자주 언급된 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	11	**15**	10	**17**	9	2	9	8	**12**	9	11
순위	4	**2**	6	**1**	7	11	7	10	**3**	7	4



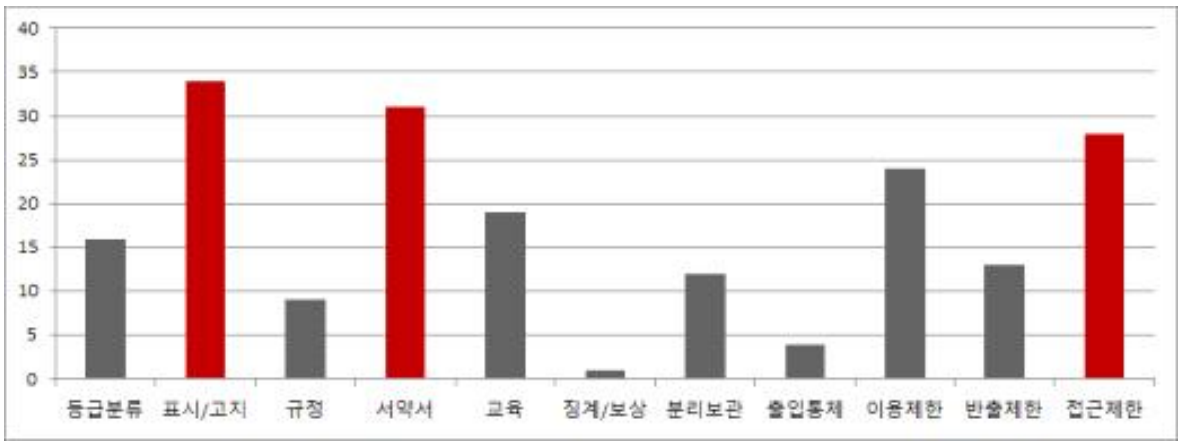
- 이 중, 비밀관리성을 인정한 판례에서는 서약서에 대한 언급 빈도가, 부정한 판례에서는 표시/고지 여부에 대한 언급 빈도가 가장 높은 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	3	**4**	**4**	**7**	1	2	**5**	3	3	3	2
관리성 부정	8	**11**	6	**10**	8	0	4	5	**9**	6	**9**

라. 일반서비스

- 영업비밀이 일반서비스 분야에 속하는 50건 판례에 있어서는, 표시/고지 여부가 가장 자주 언급되었고, 그 다음으로는 서약서 징구여부, 접근제한 조치여부의 언급 빈도가 높았다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	16	**34**	9	**31**	19	1	12	4	24	13	**28**
순위	6	**1**	9	**2**	5	11	8	10	4	7	**3**



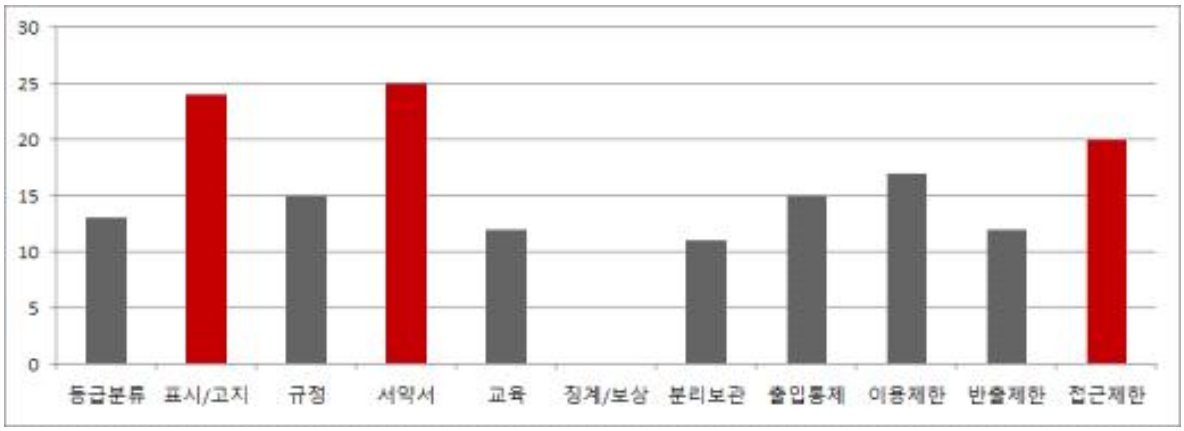
- 이 중, 비밀관리성을 인정한 판례는 서약서를, 부정된 판례는 표시/고지를 가장 많이 언급하였다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	4	**5**	3	**9**	4	0	3	2	4	1	**5**
관리성 부정	12	**29**	6	**22**	15	1	9	2	20	12	**23**

마. 화학

- 영업비밀이 화학 분야에 속하는 18건 판례를 분석한 결과, 표시/고지여부, 서약서 징구여부, 접근제한 조치여부 순으로 언급 빈도가 높은 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	8	**13**	4	**10**	3	0	6	6	6	6	**9**
순위	4	**1**	9	**2**	10	11	5	5	5	5	**3**



- 이 중, 비밀관리성이 인정된 판례는 서약서 징구여부를, 부정된 판례는 표시/고지 여부를 가장 자주 언급하였다.

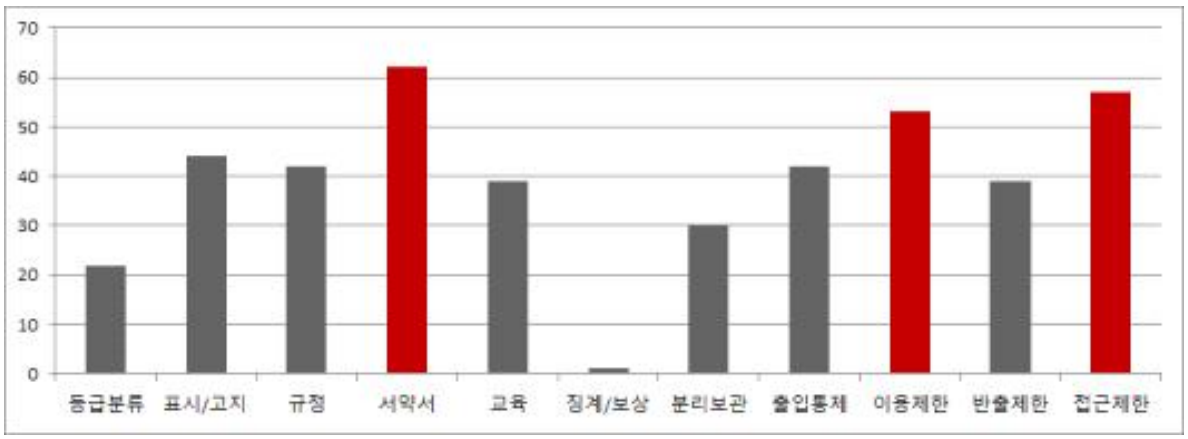
판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	4	**6**	2	**7**	1	0	4	4	2	2	**5**
관리성 부정	**4**	**7**	2	3	2	0	2	2	**4**	**4**	**4**

3.3.4 형사 판례 분석

가. 기계소재

- 영업비밀이 기계소재 분야에 속하는 75건의 형사판례를 분석한 결과, 서약서 징구여부, 접근제한 조치여부, 이용제한여부 순으로 언급 빈도가 높았다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	22	44	42	**62**	39	1	30	42	**53**	39	**57**
순위	10	4	5	**1**	7	11	9	5	**3**	7	**2**



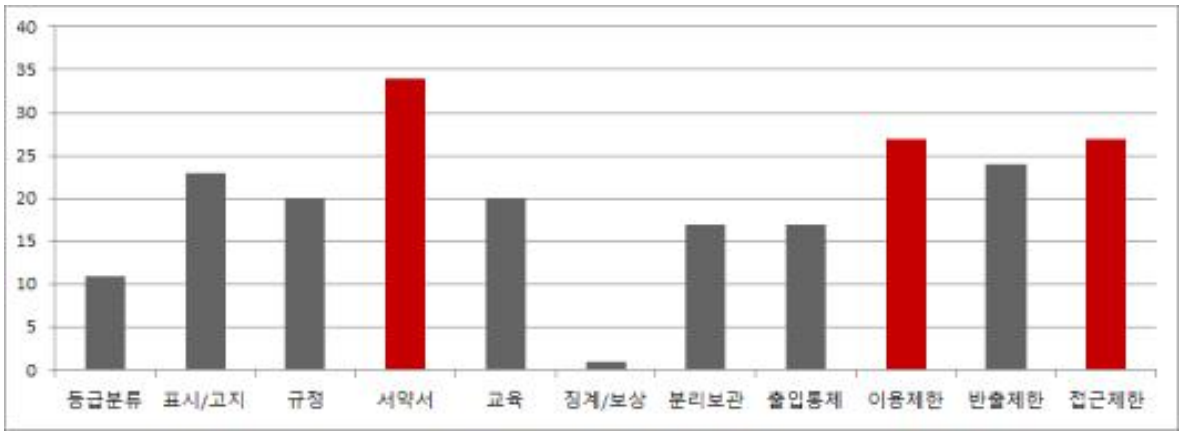
- 이 중, 비밀관리성이 인정된 판례에서는 서약서 징구여부가, 부정된 판례에서는 이용제한여부와 접근제한 조치여부가 가장 자주 언급되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	11	18	21	**38**	20	1	17	21	**26**	18	**30**
관리성 부정	11	**26**	21	24	19	0	13	21	**27**	21	**27**

나. 전기전자

- 영업비밀이 전기전자 분야에 속하는 38건 판례의 빈도 수를 분석한 결과, 서약서, 이용제한 및 접근제한 순으로 자주 언급된 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	11	23	20	**34**	20	1	17	17	**27**	24	**27**
순위	10	5	6	**1**	6	11	8	8	**2**	4	**2**



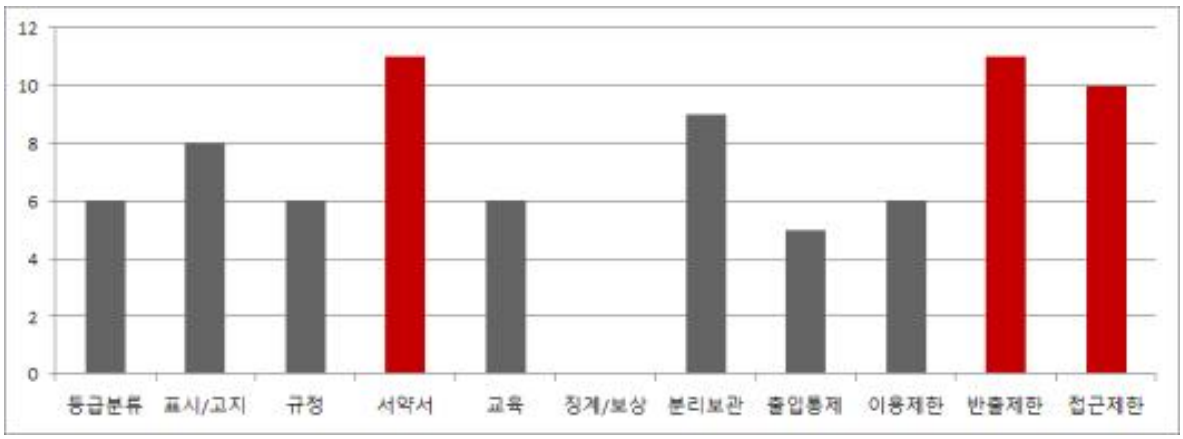
- 이 중, 비밀관리성을 인정한 판례와 부정한 판례 모두 서약서 징구여부를 가장 자주 언급하였다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	6	12	11	**22**	13	1	11	10	**16**	13	**17**
관리성 부정	5	**11**	9	**12**	7	0	6	7	**11**	**11**	10

다. 정보통신

- 영업비밀이 정보통신 분야에 속하는 15건의 판례에서는 서약서와 반출제한의 언급 빈도가 가장 높은 것으로 나타났고, 접근제한도 비슷한 수준으로 자주 언급되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	6	8	6	**11**	6	0	9	5	6	**11**	**10**
순위	6	5	6	**1**	6	11	4	10	6	**1**	**3**



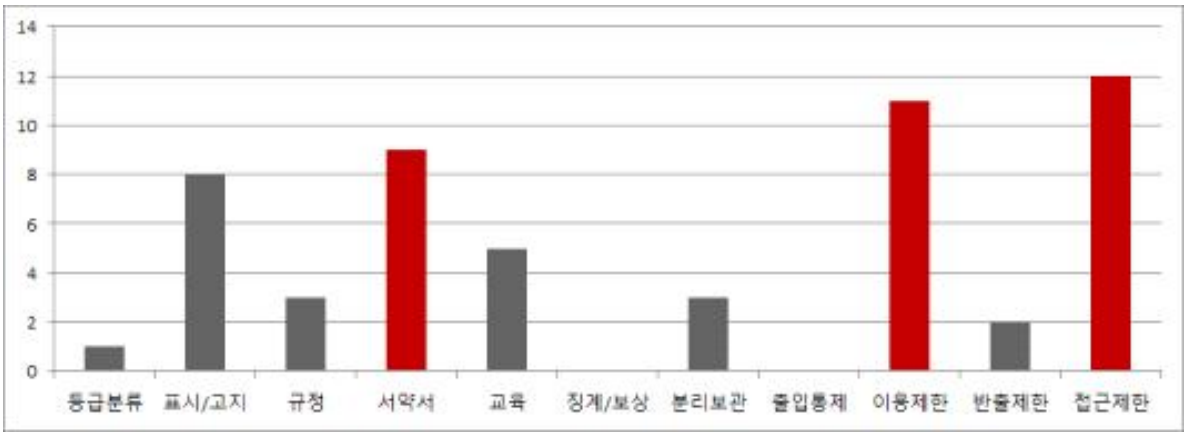
- 이 중, 비밀관리성을 인정한 판례는 서약서를, 부정한 판례는 반출제한을 가장 자주 언급하였다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	1	2	3	**7**	2	0	3	1	3	**4**	**5**
관리성 부정	5	**6**	3	4	4	0	**6**	4	3	**7**	5

라. 일반서비스

- 영업비밀이 일반서비스 분야에 속하는 13건 판례의 빈도수를 분석한 결과, 접근제한, 이용제한, 서약서 순으로 자주 언급된 것으로 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	1	8	3	**9**	5	0	3	0	**11**	2	**12**
순위	9	4	6	**3**	5	10	6	10	**2**	8	**1**



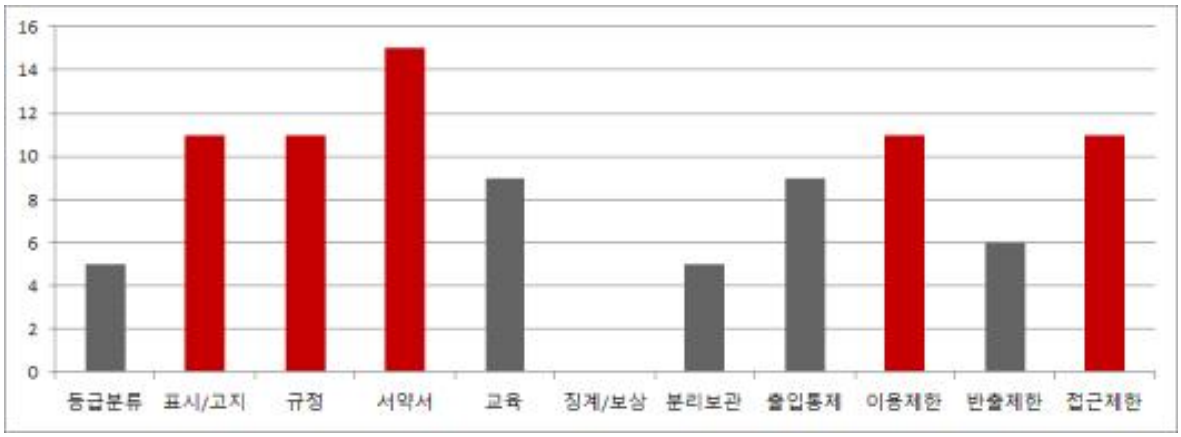
- 이 중, 비밀관리성이 인정된 판례에서는 접근제한이, 부정된 판례에서는 표시/고지가 가장 많이 언급되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	0	1	0	**3**	0	0	2	0	**5**	0	**6**
관리성 부정	1	**7**	3	**6**	5	0	1	0	**6**	2	**6**

마. 화학

- 영업비밀이 화학 분야에 속하는 16건 판례의 경우, 서약서 징구여부의 언급 빈도가 가장 높게 나타났다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
빈도수	5	**11**	**11**	**15**	9	0	5	9	**11**	6	**11**
순위	9	**2**	**2**	**1**	6	11	9	6	**2**	8	**2**



- 이 중, 비밀관리성을 인정한 판례는 서약서 징구여부를, 부정한 판례는 표시/고지 여부 및 규정 구비여부를 가장 자주 언급하였는데, 다른 보호조치에 대해서도 비슷한 빈도로 언급하고 있는 것으로 분석되었다.

판단 요소	등급 분류	표시/ 고지	규정	서약서	교육	징계/ 보상	분리 보관	출입 통제	이용 제한	반출 제한	접근 제한
관리성 인정	2	5	5	**10**	**6**	0	3	**6**	**6**	2	**6**
관리성 부정	3	**6**	**6**	**5**	3	0	2	3	**5**	4	**5**

3.4 기업 규모를 고려한 판결

3.4.1 분석 대상 판례

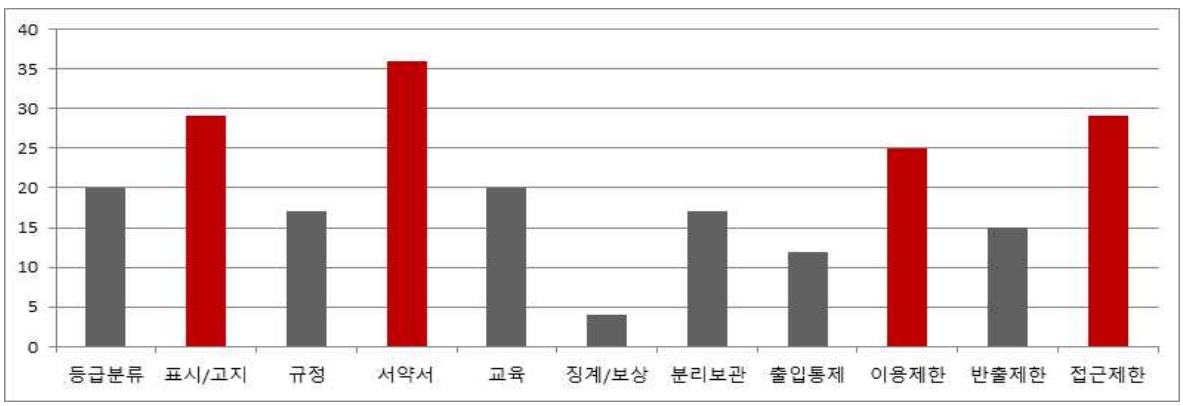
- 법원이 비밀관리성 여부를 판단함에 있어 종업원 수나 자본금 등 기업의 규모를 고려할 때 비밀관리성이 인정된다고 판단한 사건이 20건, 기업 규모를 고려하더라도 비밀관리성이 인정되지 않는다고 판단한 사건이 20건으로 확인되었다.

구분		인정	부정	전체
전체	민사	8	10	18
	형사	12	10	22
	합계	**20**	**20**	**40**

3.4.2 기업 규모를 고려한 판례 분석

- 기업 규모 등을 고려하여 비밀관리성을 인정한 사건의 경우 서약서 징구, 표시/고지와 이용제한 및 접근 제한 조치를 취했는지 여부를 가장 자주 언급하고 있으며, 규모 등을 고려하더라도 비밀관리성을 부정한 사건에서도 서약서, 접근제한, 등급분류, 표시/고지를 가장 자주 언급하고 있는 것으로 나타났다.

구분	등급분류	표시/고지	규정	서약서	교육	징계/보상	분리보관	출입통제	이용제한	반출제한	접근제한
관리성 인정	5	**14**	7	**18**	8	4	9	6	**12**	7	**13**
관리성 부정	**15**	**15**	10	**18**	12	0	8	6	13	8	**16**
전체	20	**29**	17	**36**	20	4	17	12	**25**	15	**29**
순위	5	**2**	7	**1**	5	11	7	10	**4**	9	**2**



3.4.3 기업 규모를 고려한 판례의 의의

가. '비밀관리성' 판단 기준 (판례)

1) '상당한 노력'의 의미

- 대법원은 2008. 7. 10. 선고된 2008도3435 판결[7]을 통해 영업비밀의 보호 요건으로서 "상당한 노력에 의하여 비밀로 유지된다"(이하, '비밀관리성')는 것은 비밀로 유지·관리되고 있다는 사실이 객관적으로 인식 가능한 상태를 말한다는 입장을 취하고 있으며, 이후 다수의 판결[8]에서 이와 동일·유사한 취지로 판단하고 있다.

> **대법원 2008. 7. 10. 선고 2008도3435 판결 외 다수**
>
> 구 부정경쟁방지 및 영업비밀보호에 관한 법률(2007. 12. 21 법률 제8767호로 개정되기 전의 것, 이하 같다) 제2조 제2호의 '영업비밀'이란 공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 상당한 노력에 의하여 비밀로 유지된 생산방법, 판매방법 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보를 말하는 것인바 (대법원 1999. 3. 12. 선고 98도4704 판결 등 참조), 여기서 '공연히 알려져 있지 아니하다'는 것은 그 정보가 간행물 등의 매체에 실리는 등 불특정 다수인에게 알려져 있지 않기 때문에 보유자를 통하지 아니하고는 그 정보를 통상 입수할 수 없는 것을 말하고(대법원 2004. 9. 23. 선고 2002다60610 판결 참조), '독립된 경제적 가치를 가진다'는 것은 그 정보의 보유자가 그 정보의 사용을 통해 경쟁자에 대하여 경쟁상의 이익을 얻을 수 있거나 또는 그 정보의 취득이나 개발을 위해 상당한 비용이나 노력이 필요하다는 것을 말하며(대법원 2008. 2. 15. 선고 2005도6223 판결 참조), '상당한 노력에 의하여 비밀로 유지된다'는 것은 그 정보가 비밀이라고 인식될 수 있는 표시를 하거나 고지를 하고, 그 정보에 접근할 수 있는 대상자나 접근 방법을 제한하거나 그 정보에 접근한 자에게 비밀준수의무를 부과하는 등 객관적으로 그 정보가 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태인 것을 말한다.

- 다만 '상당한 노력'의 구체적인 의미, 즉 '비밀관리성'이 기업 규모에 따라 다를 수 있다는 점에 관해 일부 하급심 판결[9]을 제외하면, 대법원이 이를 구체적으로

---

7) 이 판결 이전에는 '비밀관리성'에 관해 구체적으로 언급하지 않고, 영업비밀의 정의에 관해 아래와 같이 판시하는 정도였음 (대법원 1999. 3. 12. 선고 98도4704 판결 : 영업비밀이라 함은 일반적으로 알려져 있지 아니하고 독립된 경제적 가치를 가지며, 상당한 노력에 의하여 비밀로 유지·관리된 생산방법, 판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말하고, 영업비밀의 보유자인 회사가 직원들에게 비밀유지의 의무를 부과하는 등 기술정보를 엄격하게 관리하는 이상, 역설계가 가능하고 그에 의하여 기술정보의 획득이 가능하더라도, 그러한 사정만으로 그 기술정보를 영업비밀로 보는 데에 지장이 있다고 볼 수 없다.)

8) 대법원 2009. 7. 9. 선고 2006도7916 판결 등

9) 부산고등법원 2015. 1. 29. 선고 2012나5445 판결 [원고의 규모나 종업원 수, 이 사건 자료의 성격과 중요성 등 원고가 처한 구체적인 상황 아래서 원고는 특허등록된 유산균 이중코팅기술과는 별개의 것으로서 특정 · 구별되는 이 사건 자료에 대하여 비밀이라고 인식될 수 있는 표시를 하거나 고지를 하고,

판단한 사례는 찾아보기 어려우며, 일부 판결에서 '기업 규모를 고려하더라도'라는 표현을 사용하는 정도이다.

대법원 2009. 9. 10. 선고 2008도3436 판결

원심이 적법하게 채택한 증거들에 의하면, 피해회사가 피고인의 퇴직 전날인 2005. 7. 14. 피고인으로부터 '피해회사에서의 업무수행과 관련하여 습득한 제반 정보 및 자료에 대한 기밀을 유지하겠다'는 내용의 회사기밀유지각서를 제출받은 사실을 알 수 있으나, 다른 한편, 위 각 증거에 의하면, 이 사건 자료는 피해회사의 직원인 공소외인이 사용하는 컴퓨터에 저장되어 있었는데, 위 컴퓨터는 비밀번호도 설정되어 있지 않고 별도의 잠금장치도 없어 누구든지 위 컴퓨터를 켜고 이 사건 자료를 열람하거나 복사할 수 있었던 사실, 또한 위 컴퓨터와 네트워크를 통해 연결된 피해회사 내의 다른 컴퓨터를 통해서도 별도의 비밀번호나 아이디를 입력할 필요 없이 누구든지 쉽게 공소외인의 컴퓨터에 접속하여 이 사건 자료를 열람·복사할 수 있었던 사실, 공소외인은 이 사건 자료를 정기적으로 CD에 백업하여 사무실 내 서랍에 보관해 두었는데, 공소외인이 그 서랍을 잠그지 않고 항상 열어두었기 때문에 누구든지 마음만 먹으면 그 백업CD를 이용할 수 있었던 사실을 알 수 있는바, 이러한 사정들과 앞서 본 법리에 비추어 보면, 피해회사가 피고인으로부터 위와 같이 일반적인 회사기밀유지각서를 제출받은 사실만으로는, **피해회사가 소규모 회사라는 점을 고려하더라도**, 이 사건 자료가 상당한 노력에 의하여 비밀로 유지되었다고 보기는 어렵다고 할 것이고, 달리 그와 같은 점을 인정할 증거도 없다.

2) '합리적 노력'의 의미

- 2015년 부정경쟁방지법의 개정으로 종래 '상당한 노력'에서 다소 완화된 '합리적 노력'의 구체적인 의미에 대해 현재까지 확인된 대법원 판결은 없으며, 2016. 9. 27.자 의정부지방법원 2016노1670 판결[10]에서 처음으로 '합리적 노력'에 대해 판시한 이후 일부 하급심 판결에서 동일한 취지의 판단을 하고 있다.

의정부지방법원 2016. 9. 27. 선고 2016노1670 판결

비밀로 유지하기 위한 '합리적인 노력'을 기울였는지 여부는 해당 정보에 대한 접근을 제한하는 등의 조치를 통해 객관적으로 정보가 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태가 유지되고 있는지 여부(= 접근 제한 + 객관적 인식가능성)를, 해당 정보에 대한 ① 물리적, 기술

이 사건 자료에 접근할 수 있는 대상자나 접근 방법을 제한하고 그 자료에 접근한 자에게 비밀준수의무를 부과하는 등 원고 나름의 합리적인 노력을 기울임으로써 객관적으로 그 자료가 비밀로 유지・관리되고 있다는 사실이 인식 가능한 상태에 있게 되었음을 알 수 있으므로 (이하 생략))

10) 이 사안은 여행업체인 피해자 회사에서 해외 전시회 참관행사를 담당하던 피고인이 퇴사하면서 피해자 회사의 고객정보를 취득·사용한 것과 관련하여, 원심(의정부지방법원 고양지원 2016. 6. 17. 선고 2015고정1353 판결)은 해당 고객정보에 대하여 특별히 접근 제한을 하거나 비밀준수의무를 부여하지 않았다는 이유로 비밀관리성을 부정하여 피고인에 대해 무죄를 선고하였으나, 항소심 판결에서는 법률 개정의 취지 및 기업 규모 등을 고려할 때 비밀관리성이 인정된다고 하여 피고인에게 벌금 400만원을 선고한 사건임

적 관리, ② 인적, 법적 관리, ③ 조직적 관리가 이루어졌는지 여부에 따라 판단하되, 각 조치가 '합리적'이었는지 여부는 영업비밀 보유 **기업의 규모, 해당 정보의 성질과 가치, 해당 정보에 일상적인 접근을 허용하여야 할 영업상의 필요성이 존재하는지 여부, 영업비밀 보유자와 침해자 사이의 신뢰관계의 정도, 과거에 영업비밀을 침해당한 전력이 있는지 여부 등을 종합적으로 고려**해 판단해야 할 것이다.

합리적 노력의 판단 기준: 접근 제한 + 객관적 인식가능성		
① 물리적, 기술적 관리	**② 인적, 법적 관리**	**③ 조직적 관리**
영업비밀 보유 기업의 규모, 해당 정보의 성질과 가치, 해당 정보에 일상적인 접근을 허용하여야 할 영업상 필요성이 존재하는지 여부, 영업비밀 보유자와 침해자 사이의 신뢰관계, 과거에 영업비밀을 침해당한 전력이 있는지 여부 등에 기초하여 판단함.		

서울중앙지방법원 2017. 2. 15. 선고 2016노3163 판결[11]

피해자 회사의 규모와 자금력이 그리 큰 수준은 아니라고 보이고, 피해자 회사와 같은 규모의 중소기업은 자금력의 한계 등으로 인하여 대기업과 같은 수준으로 영업비밀을 완벽하게 유지·관리하는 것이 사실상 불가능하다. 이와 같은 상황에서 대기업과 같은 수준의 비밀 유지·관리를 요구한다면, 중소기업은 영업비밀에 대한 보호를 받기 어려울 것이다. 따라서 비밀 유지·관리에 일부 미흡한 부분이 있다 하더라도, 다른 요건들을 모두 충족하는 것을 전제로, **기업의 규모, 자금력 등에 비추어 영업비밀을 유지·관리하기 위한 노력을 게을리하지 않았음이 인정되는 경우**, 부정경쟁방지법상 영업비밀로 인정할 수 있다.

인천지방법원 2018. 5. 4. 선고 2017노4721 판결[12]

법률 제13081호로 개정된 부정경쟁방지 및 영업비밀보호에 관한 법률 (이하 '부정경쟁방지법'이라 한다) 은 위 '상당한 노력'을 '합리적인 노력'으로 완화하였다. 개정이유에 의하면 이는 자금사정이 좋지 않은 중소기업이 영업비밀 보호를 위한 충분한 시스템을 구비하지 못하여 보호받지 못하는 사례를 시정하기 위한 것이다. 따라서 현행 부정경쟁방지법상 영업비밀에 해당하는지를 판단하기 위해서는 그 정보가 비밀이라고 인식될 수 있는 표시 또는 고지가 있었는지, 그 정보에 접근할 수 있는 대상자나 접근 방법이 제한되어 있었는지, 그 정보에 접근한 자에게 비밀준수의무가 부과되어 있었는지 등을 여전히 그 기준으로 삼을 수 있겠으나, 다만 그 **노력의 정도는 기업의 규모 등에 비추어 그 시스템이 합리적이라고 판단될 수 있을 정도이면 충분하다**고 할 것이다.

11) 소스코드에 접근할 수 있는 권한을 가진 직원이 2명밖에 없었고, 개인종합평가에서 '보안관리' 부분을 평가하고, 직원들에게 이메일로 보안에 만전을 기할 것을 수차례 당부하였으며, 피고인도 이 사건 파일이 피해자 회사의 영업비밀임을 알고 있었다는 취지로 진술한 점 등을 고려하여 비밀관리성을 인정한 사안임

12) 이 사안의 경우 비밀로 표시하거나 고지된 바가 없고, 개인노트북에 보관되어 접근대상이나 방식이 제한되지 않았으며, 대표이사실이 연구소 내부에 있어 일단 손님이 사무소 내부에 들어오면 별다른 제한 없이 출입할 수 있었다는 등의 이유로 비밀관리성을 부정함

- 이번 연구를 통해 확인한 최근의 하급심 판결에서도 '비밀관리성'의 판단은 기업 규모 등을 고려하여 사안별로 판단해야 한다고 명시하고 있는 것으로 확인되었다.

대전지방법원 2018. 12. 13. 선고 2017노3469 판결[13)]

비밀관리성을 충족하기 위해 요구되는 조치의 수준은 절대적인 수준은 아니고, 보유자의 능력에 걸맞는 '합리적인 수준'에 이를 것이 요구된다. 따라서 **합리적인 수준**은 당해 정보에 대한 보유자의 비밀관리의사", 즉 '당해정보는 보유자가 비밀로서 관리하고 있음'을 객관적으로 충분히 나타낼 수 있는 정도에 이르러야 하나, 해당 정보의 내부에서의 사용에 지나친 제한을 야기하거나 보유자로 하여금 과도한 비용을 투입하여야 하는 정도에 이르러서는 안 된다. 따라서 **상당성의 수준은 보유자인 기업의 업종, 규모, 종업원의 수, 해당 영업비밀이 속한 기술분야 또는 성질, 침해방법의 수단과 방법, 영업비밀이 사용되는 업무의 특징, 침해자와 보유자 회사의 관계 등 제반 사정을 종합하여 사안별로 판단**하여야 할 것이다.

서울동부지방법원 2019. 3. 13. 선고 2018고단2485 판결[14)]

합리적 노력을 기울였는지 여부는 정보에 대한 접근제한조치 등으로 객관적으로 정보가 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태가 유지되고 있는지 여부 (접근 제한 + 객관적 인식가능성) 를 해당 정보에 대한 ① 물리적, 기술적 관리, ② 인적, 법적 관리, ③ 조직적 관리가 이루어졌는지 여부에 따라 판단하되, **각 조치가 "합리적"이었는지 여부는 영업비밀 보유 기업의 규모, 해당 정보의 성질과 가치, 해당 정보에 일상적인 접근을 허용하여야 할 영업상 필요성이 존재하는지 여부, 영업비밀 보유자와 침해자 사이의 신뢰관계의 정도, 과거에 영업비밀을 침해당한 전력이 있는지 여부 등을 종합적으로** 고려해 판단할 것이다.

※ 비밀 관리성의 상대성

비밀 관리성으로서 접근 제한과 객관적 인식 가능성 (표시) 은 침해 행위자와 목적물에 따라 상대적으로 판단할 수밖에 없다. 이 사건에서 피고인 B와 같은 개발자의 경우 평소 프로그램의 핵심 자료에 아무런 제한 없이 접근이 가능할 것이므로 퇴근, 외부 업무, 퇴직 시 등에 외부 반출을 못하도록 하는 규정과 물적 시설을 충분히 운영하더라도 의도하기에 따라서 얼마든지 회피가 가능하므로 (굴지의 대기업에서 끊임없이 침해와 경쟁사로의 유출 사건이 일어나고 있는 것이 현실이다) 이미 회사 내부적으로 업무상 접근 권한이 주어진 직원이 행위자인 경우 그에 대한 접근 제한 조치의 상당성을 따지는 것은 무의미할 뿐 아니라 개념적으로도 모순이다. 마찬가지로 비밀로서의 표시도 영업비밀의 나머지 요건 즉, 외부에 알려져 있지 않고 경제적 가치를 가지며 유출될 경우 큰 손해를 가져오는 자산이라는 것을 충분히 알고 있는 직원과의 관계에서 표시를 하지 않았다고 하여서 인식의 흠결로 인정할 수는 없는 것이다.

13) 피해자 회사의 직원이 약 10~15명 정도이고, 도료 레시피에 대한 열람 및 출력 권한을 제한하고 있었고, 이 사건 이전에 도료 레시피가 유출된 적이 없으며, 피고인들이 퇴사시 영업비밀보호서약서를 제출한 점 등을 고려하여 비밀관리성을 인정한 사안임

14) 피해자 회사는 외부인이나 거래 업체 직원들이 방문할 일이 거의 없고, 사무실 출입시설이나 보안장비, 로그인 계정 등을 통해 외부인의 접근을 차단한 점, 소스코드에 영업비밀이라고 별도로 표시할 방법도 없으며, 과거 영업비밀 침해 사고가 전혀 발생하지 않았던 점 등을 고려하여 비밀관리성을 인정함

나. 비밀관리성 판단에 영향을 미치는 요인

- 이상과 같은 판결 분석 결과를 종합해 보면, 법원은 기업 등 영업비밀 보유자의 업종, 규모 뿐만 아니라 영업비밀인지 여부가 문제되는 정보의 가치나 성질, 침해 또는 유출 경험 등의 사정을 종합적으로 고려하고 있다는 것을 알 수 있다.

[표 14] 법원의 비밀관리성 판단 시 고려 요소

구분	비밀관리성 강화	비밀관리성 완화
업종	- 영업비밀 침해/유출 사건의 빈도가 높은 업종	- 영업비밀 침해/유출 사건의 빈도가 낮은 업종
규모	- 종업원 수가 많은 경우 - 자본금이 많은 경우 - 매출액/시장점유율이 높은 경우	- 종업원 수가 적은 경우 - 자본금이 적은 경우 - 매출액/시장점유율이 낮은 경우
영업비밀의 성질	- 영업비밀이 속한 기술 분야의 발전 속도가 빠른 경우 (예: 반도체장비 > 농기구) - 영업비밀의 가치가 클 경우 - 영업비밀이 사용되는 업무의 특성상 소수의 인원만 열람/접근해도 될 경우	- 영업비밀이 속한 기술 분야의 발전 속도가 느린 경우 - 영업비밀의 가치가 낮을 경우 - 업무의 특성상 해당 영업비밀을 다수의 임직원이 공유해야 할 경우
침해 방법 및 수단	- 용이한 방법과 수단에 의해서도 영업비밀 침해가 가능한 경우	- 영업비밀 침해의 방법이나 수단이 고도한 경우
침해자와 보유자의 관계	- 침해자와 보유자간에 신뢰 관계가 낮은 경우 - 침해자에게 접근 권한이 없는 경우	- 침해자와 보유자간의 신뢰관계가 높은 경우 (예: 공동창업자, 장기근속자) - 침해자가 접근 권한을 가지고 있었던 경우
침해/유출 경험	- 영업비밀 유출 사고가 있었던 경우	- 영업비밀 유출 사고가 없었던 경우

Ⅲ. 영업비밀 표준 관리 체계

1. 필요성 및 배경

1.1 영업비밀의 정의 및 보호 요건의 완화

영업비밀의 정의 규정은 1991. 12. 31.자로 일부 개정되고, 1992. 12. 15.자로 시행된 '부정경쟁방지법'에서 신설한 이래, 보호 요건으로서 '비밀관리성'은 "상당한 노력에 의하여 비밀로 유지"될 것을 요하다가, 2015년 개정을 통해 "상당한 노력"이 "합리적 노력"으로 요건이 완화되었었고[15], 2019년 개정에서는 "합리적 노력"을 삭제하고 "비밀로 관리"될 것을 요건으로 하고 있다.[16]

[표 14] 부정경쟁방지 및 영업비밀보호에 관한 법률 개정 이력

구분	1991. 12. 31. 일부 개정 1992. 12. 15. 시행	2015. 1. 28. 일부 개정 2015. 7. 29. 시행	2019. 1. 8. 일부 개정 2019. 7. 9. 시행
정의	"영업비밀"이란 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, **상당한 노력**에 의하여 비밀로 유지된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.	"영업비밀"이란 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, **합리적인 노력**에 의하여 비밀로 유지된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.	"영업비밀"이란 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, **비밀로 관리**된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.
개정 이유	최근 과학기술투자의 확대와 기술혁신에 따라 산출되는 기술상·경영상 유용한 정보(營業秘密)의 중요성이 높아지고 있는바, 영업비밀의 도용등 침해행위를 방지하여 기업간의 건전한 경쟁질서를 확립하고자, 영업비밀 보호에 관한규정을 신설	영업비밀로 보호받기 위해서는 "상당한 노력"으로 비밀을 유지하여야 하는데, 자금사정이 좋지 않은 중소기업은 영업비밀 보호를 위한 충분한 시스템을 구비하지 못하여 영업비밀로 보호받지 못하는 사례가 발생하고 있음. (중략) 이에 비밀유지에 필요한 "상당한 노력"을 "합리적인 노력"으로 완화 (이하, 생략)	일정한 요건을 갖춘 생산방법, 판매방법 및 영업활동에 유용한 기술상 또는 경영상의 정보가 합리적인 노력에 의하여 비밀로 유지되어야만 영업비밀로 인정받던 것을, 합리적인 노력이 없더라도 비밀로 유지되었다면 영업비밀로 인정받을 수 있도록 영업비밀의 인정요건을 완화함.

15) 미국 Uniform Trade Secrets Act (UTSA) 등 영업비밀보호 법제에서의 "Reasonable effort"와 "상당한 노력"을 요구하지 않는 일본의 입법례를 참고한 것임 (법안설명자료)

16) 일본의 부정경쟁방지법(不正競争防止法) 제2조에서도 영업비밀을 '합리적 노력' 등의 요건 없이 "비밀로 관리된 생산방법, 판매방법..."이라고만 정의하고 있음 (この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。)

그러나, 법 개정에도 불구하고 '상당한 노력'과 '합리적인 노력'의 차이 및 현행 '비밀로 관리된'의 의미, 즉 영업비밀 보유자, 특히 중소기업이 어떤 조치를 취했을 때 '비밀관리성'이 인정되는지 여부는 여전히 명확하고 구체적으로 판단하기 어렵다.

1.2 비밀관리성 판단 기준(판례)

앞서 살펴본 바와 같이 대법원은 '상당한 노력에 의하여 비밀로 유지된다'는 것은 해당 정보 보유자의 주관적 인식만으로는 부족하고, 객관적으로 그 정보가 비밀임을 인식 가능한 상태에 이른 것을 의미한다고 보고 있으며, '비밀관리성'을 판단할 때 기업 규모 등을 고려할 수 있다는 것을 부정하지는 않으나, 구체적으로 판시하고 있는 사례는 없다.

> '상당한 노력에 의하여 비밀로 유지된다'는 것은 그 정보가 비밀이라고 인식될 수 있는 표시를 하거나 고지를 하고, 그 정보에 접근할 수 있는 대상자나 접근 방법을 제한하거나 그 정보에 접근한 자에게 비밀준수의무를 부과하는 등 객관적으로 그 정보가 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태인 것을 말한다. (대법원 2008. 7. 10. 선고 2008도3435 판결 외 다수)

2015년 '합리적인 노력'으로 개정된 이후, 의정부지방법원 2016. 9. 27.선고 2016노1670 판결에서 '합리적 노력'은 개정 전 '상당한 노력'에 비해 완화된 것이라는 점을 분명히 하면서, 어떤 조치가 '합리적'이었는지 여부는 기업 규모 등을 고려하여 종합적으로 판단해야 한다고 명시하였다.

> 각 조치가 '합리적'이었는지 여부는 영업비밀 보유 **기업의 규모, 해당 정보의 성질과 가치, 해당 정보에 일상적인 접근을 허용하여야 할 영업상의 필요성이 존재하는지 여부, 영업비밀 보유자와 침해자 사이의 신뢰관계의 정도, 과거에 영업비밀을 침해당한 전력이 있는지 여부 등을 종합적으로 고려**해 판단해야 할 것이다. (의정부지방법원 2016. 9. 27.선고 2016노1670 판결)

상기 의정부지방법원의 2016노1670 판결은, 영업비밀 보유자/피해 회사가 종래 일반적으로 제시되어 온 영업비밀 보호·관리조치라고 할 수 있는 서약서 징구, 교육 등을 하지 않았음에도 불구하고(이 때문에 원심에서는 비밀관리성을 부정함), 기업 규모나 피고인과 피해자 회사의 신뢰관계 등을 고려하여 원심을 파기하고 비밀관리성을 인정하였다는 점에서 매우 주목할 만한 판결이라고 할 수 있다.

[표 16] 원심 및 항소심 판결 비교

	원심 (2015고정1353)	항소심 (2016노1670)
주문	무죄	유죄 (벌금 400만원)
판단	비밀관리성 부정	비밀관리성 인정
법리	“상당한 노력”과 “합리적 노력”은 동일하게 해석	“합리적 노력”은 “상당한 노력”에 비해 완화된 기준
판단 근거	• 해당 정보는 직원들 모두 공유 • 피고인에게 정보접근권한을 부여하거나 비밀준수의무를 부과하지 않음 • 비밀표시 또는 고지하지 않음 • 정보의 등록이나 수정에 별다른 제한이 없었음	• 고객정보를 별도 관리하면서 직원들에게만 접근을 허용 **(합리적 구분)** • 네이버 주소록은 법인계정으로 관리하고 구글 스프레드쉬트 정보는 직원들만 초대**(기술적 관리)** • 네이버와 구글 계정은 대표가 관리**(조직적 관리)** • 피해자 회사는 직원 4명, 연매출액 약 2억원의 소규모 회사 • 피고인을 제외하면 전원이 대표자와 그 가족들로 구성 • 피고인은 고객정보의 중요성을 충분히 인식 할 수 있었음 • 피고인과 고소인은 25년간 알고 지냈고, 근속기간이 10년을 초과하여 상당한 신뢰관계가 형성됨 • 고객정보에 직원들이 접근하도록 한 것은 업무상 밀접한 관련이 있고, 지속적인 업데이트가 필요하기 때문 • 피고인이 퇴사한 직후 고객정보에 대한 접근을 차단함 • 과거 영업비밀이 침해당한 적이 없음

이외에도 이번 연구를 통해 확인한 다수의 결에서도 영업비밀 보유 기업의 규모, 해당 정보의 성질과 가치, 해당 정보에 일상적인 접근을 허용할 영업상 필요성이 존재하는지 여부, 영업비밀 보유자와 침해자 사이의 신뢰관계정도, 과거에 영업비밀을 침해당한 전력이 있는지 여부 등을 종합적으로 고려해야 한다고 판시하고 있다.

그러나, 이러한 판례를 통해서도 기업의 규모나 업종별로 영업비밀 보호관리 조치가 다를 수 있음은 분명하지만, 구체적으로 어떻게 다른지 또는 달라야 하는지를 명확히 구분하기는 어렵다.

1.3 기존 영업비밀 보호관리 체계

종래에도 영업비밀 관련 판결 분석을 통해 법원이 비밀관리성을 판단할 때 고려하는 요소별로 빈도와 상관계수를 분석하여[17], 가장 중요한 보호관리 조치 10가지를 제시한 바 있으나, 이는 기업의 규모나 업종 등을 고려한 것은 아니다.

[표 17] 비밀관리성 판단 요소별 검토 빈도율 및 상관계수(민·형사 통합)

대분류	소분류	비밀 관리성 판단 시 검토되는 빈도율	비밀 관리성 판단 결과와의 상관계수
표시/고지	1-1. 영업비밀 표시	**33 %**	**0.88**
	1-2. 영업비밀 등급 분류	26 %	**0.93**
	1-3. 보안 교육	22 %	0.72
	1-4. 영업비밀 고지	7 %	0.67
계약	2-1. 직원 대상 서약서 등 징구	**58 %**	0.50
	2-2. 거래업체와 비밀유지계약 체결	15 %	0.75
행정조치	3-1. 보안규정 시행	30 %	0.69
	3-2. 보안담당자 지정	14 %	**0.87**
	3-3. 영업비밀 열람/접근 제한	**38 %**	**0.89**
출입 제한	4-1. 보안장치 설치 운영	22 %	0.58
	4-2. 개발실/보관실 분리 및 출입 제한	28 %	0.79
	4-3. 출입 시 보안 검사	6 %	0.70
IT 보안	5-1. 영업비밀 복사/전송 제한	22 %	**0.91**
	5-2. 컴퓨터/네트워크 암호 설정	24 %	0.66
	5-3. 보안프로그램 및 파일 암호화	18 %	**0.86**
기타 요소	6-1. 기타	16 %	**0.89**

17) 영업비밀 보호 가이드, 영업비밀보호센터, 2013

[표 18] 영업비밀 보호 10계명

1.	접근 가능성 있는 자에게 영업비밀 보호의무를 부과해야 합니다.
2.	일반 정보와 영업비밀을 구분해야 합니다.
3.	누구나 알 수 있도록 영업비밀임을 표시해야 합니다.
4.	영업비밀 접근·사용자의 권한을 제한해야 합니다.
5.	영업비밀 개발·보관 장소를 별도로 만들어 관리해야 합니다.
6.	보안관리 전담인력을 지정해야 합니다.
7.	분쟁에 대비한 영업비밀관리 증거를 확보해야 합니다.
8.	정기적인 보안교육을 실시해야 합니다.
9.	보안 관련 규정을 만들어 시행해야 합니다.
10.	영업비밀 해당 여부 및 영업비밀 보호의무를 고지해야 합니다.

1.4 중소기업 기술 보호 체계

중소기업기술 보호 지침[18]에서는, 기업의 성장 단계별 특성을 고려한 기술보호 방안과 중소기업 기술보호 10대 핵심 수칙을 제시하고 있다. 다만, 창업 시점을 기준으로 3년 미만과 그 이후인 성장기로만 구분하고 있기 때문에, 영업비밀 보호관리 표준 체계 수립에 그대로 적용하기는 다소 한계가 있다.

[표 19] 기업 성장 단계별 구분 (출처: 중소기업기술보호 지침)

구분	창업기	초기 성장기	고도 성장기	성숙기	쇠퇴기
단계 특성	회사 창업 제품/서비스개발	제품/서비스 시장 출시 매출 발생	후속 신규 제품/서비스 출시 매출액 증가	매출 활동이 감소하는 비율로 지속	매출 활동의 정체 또는 지속적 감소
경영 특성	사업 구상과 개발	상업화	기업성장	안정화	퇴보
핵심 과제	제품개발, 자금 확보, 시장 기회 포착	개발된 제품의 시장 도입	매출 증대, 고용 인력 확보	매출과 성장률 유지	기업 존속과 성장 기회 확보
핵심 경영 문제	제품 개발과 고객 판매	생산 설비 취득, 판매망, 자금 조달	제품 생산에 대한 자원 배분	제품 다각화, 조직 안정화	기업 재도약

18) 중소기업기술 보호지침, 중소벤처기업부/대·중소기업·농어업협력재단, 2018.11.

[표 20] 중소기업 성장 단계별 기술 보호 (출처: 상동 / 발췌 정리)

구분		내용
창업기	특징	• 창업 후 3년 미만, 시제품 출시 • 주요 이슈는 투자 자금의 부족 • 사업 아이템 선정과 활용 방법 결정
	기술보호	• 기술 보호를 위한 내부 지침이나 자산 보호 수단을 강구할 여력이 부족함 • 자체 개발 기술의 경우 산업 재산이나 기술 자료 또는 영업비밀 중 하나로 보호 • 특허 등록과 관리에 주의하고, 연차료 납부 관리와 전담 인원 배정이 필요
성장기	특징	• 창업기 이후 • 성공적 시장 진입을 위한 기술 확보, 조직 시스템의 구축, 효율적 자원 배분, 중장기 경영 전략이 필요 • 사업 부진 시, 비즈니스모델 재점검, 투자 자금 조달, 신제품 개발 및 마케팅 전략 구상
	기술보호	• 미래 기술 예측과 연구개발을 통한 원천 기술 확보에 비중 • 기술 유출 및 기술 침해에 따른 분쟁에 대응할 수단을 마련 • 산업기술, 국가핵심기술, 영업비밀 등 각종 제도에 부합하는 기술 보호 전략 및 보안의 체계적 관리 시스템 구축 • 내부 인력에 의한 기술 유출 대응 수단 검토 • 미활용 기술을 매각하거나 관리에서 제외

[표 21] 중소기업 기술보호 10대 핵심 수칙 (출처: 상동)

1. 기술 보호를 위한 관리 규정을 갖추고 실시해야 한다.	
	기술 보호 관리 규정을 제정하여 영업 비밀 분류 및 취급, 종업원의 의무, 영업비밀 보관·파기, 출입자 통제 등에 관하여 정리하고 관리해야 한다.
2. 보안 관리 전담 인력은 반드시 지정해야 한다.	
	보안 담당자를 지정하여 기술 보호 감사를 정기적으로 실시해야 한다.
3. 전 직원을 대상으로 정기적인 기술 보호 교육을 실시해야 한다.	
	반기별 또는 분기별로 정기적인 교육을 통해 기술 보호 중요성을 알려준다.
4. 전 직원 비밀 유지 서약서, 핵심 직원은 전직 금지 서약서를 체결해야 한다.	
	모든 직원과 비밀 유지 서약서 체결, 핵심 개발자 및 임원과 전직 금지 서약서를 체결해 기술을 지켜야 한다.

5. 핵심 기술 인력이 퇴직할 경우 철저한 사후 관리를 해야 한다.	
	인력의 퇴직 시 영업 비밀 인수인계를 철저히 하고, 서류/기술 정보 반납 및 파일 삭제 확인서를 받고 영업 비밀 준수 의무 및 처벌 규정 상시시켜 주어야 한다.
6. 중요 기술은 영업 비밀로 분류하고 별도로 관리해야 한다 .	
	기업 자산(기술) 중 영업 비밀을 파악하고 등급(극비/비밀/대외비)을 부여하고 표시하여 관리해야 한다.
7. 중요 서류는 별도 보관하고, 접근·복제·반출은 철저히 관리해야 한다.	
	중요 서류는 별도 잠금 장치가 있는 곳에 보관하고, 자료를 임의로 복제와 반출할 수 없도록 관리 번호를 부여한 후 관리해야 한다.
8. 중요 설비·장치가 설치된 곳은 통제구역으로 설정하고 관리해야 한다.	
	개발 및 제조 설비 지역은 '출입통제구역'으로 정하고, 카메라 및 스마트폰의 반입을 금지하며 감시 카메라를 설치하여야 한다.
9. 중요한 기술은 특허나 기술 자료 임치로 보호해야 안전하다.	
	개발한 기술을 특허 등록하고, 영업비밀은 기술자료 임치로 보호해야 안전하다.
10. 정보시스템에 대한 보안을 철저히 해야 한다.	
	네트워크 인증, 데이터 암호화, 비밀번호의 주기적 변경, 허가된 USB 사용하기, 기술 지킴이(보안관제) 서비스를 활용해 기술 자료를 지켜야 한다.

1.5 정리

정리하면 부정경쟁방지법의 개정을 통해 비밀관리성 요건을 완화하였으나 구체적인 내용에 대해서는 정하는 바가 없고, 판례는 기업의 규모나 업종 등을 고려하여 종합적으로 판단한다는 입장이기는 하지만 기업 등 영업비밀 보유자 입장에서는 자신이 취하고 있는 영업비밀 보호·관리 조치가 비밀관리성을 충족할 만큼 충분한지에 대해서는 확신하기 어렵다. 나아가, 영업비밀 보호나 기술보호를 위한 기존의 가이드라인은 기업의 규모나 업종을 고려한 탄력적 기준을 제시하지 못하고 있다.

이에, 기업의 규모나 관련 영업비밀이 속한 기술 분야 등의 개별 기업의 특성을 고려했을 때, 어느 정도 수준의 보호조치를 취해야 영업비밀로서 인정을 받을 수 있는지에 대한 실효성 있는 표준 관리체계의 구축이 필요하다.

2. 영업비밀 표준 관리 체계

2.1 도출 방법

이번 연구를 통해 확인한 판결에 따르면, 법원은 비밀관리성 요건을 판단함에 있어서 기업의 규모, 해당 정보의 성질과 가치, 해당 정보에 일상적인 접근을 허용할 영업상 필요성이 존재하는지 여부, 침해의 방법과 수단, 영업비밀 보유자와 침해자 사이의 신뢰관계정도, 과거에 영업비밀을 침해당한 전력이 있는지 여부 등을 종합적으로 고려해야 한다고 판시하고 있다.

서울동부지방법원 2019. 3. 13. 선고 2018고단2485 판결

합리적 노력을 기울였는지 여부는 정보에 대한 접근제한조치 등으로 객관적으로 정보가 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태가 유지되고 있는지 여부 (접근 제한 + 객관적 인식가능성) 를 해당 정보에 대한 ① 물리적, 기술적 관리, ② 인적, 법적 관리, ③ 조직적 관리가 이루어졌는지 여부에 따라 판단하되, **각 조치가 "합리적"이었는지 여부는 영업비밀 보유 기업의 규모, 해당 정보의 성질과 가치, 해당 정보에 일상적인 접근을 허용하여야 할 영업상 필요성이 존재하는지 여부, 영업비밀 보유자와 침해자 사이의 신뢰관계의 정도, 과거에 영업비밀을 침해당한 전력이 있는지 여부 등을 종합적으로** 고려해 판단할 것이다.

※ 비밀 관리성의 상대성

비밀 관리성으로서 접근 제한과 객관적 인식 가능성 (표시) 은 침해 행위자와 목적물에 따라 상대적으로 판단할 수밖에 없다. 이 사건에서 피고인 B와 같은 개발자의 경우 평소 프로그램의 핵심 자료에 아무런 제한 없이 접근이 가능할 것이므로 퇴근, 외부 업무, 퇴직 시 등에 외부 반출을 못하도록 하는 규정과 물적 시설을 중분히 운영하더라도 의도하기에 따라서 얼마든지 회피가 가능하므로 (굴지의 대기업에서 끊임없이 침해와 경쟁사로의 유출 사건이 일어나고 있는 것이 현실이다) 이미 회사 내부적으로 업무상 접근 권한이 주어진 직원이 행위자인 경우 그에 대한 접근 제한 조치의 상당성을 따지는 것은 무의미할 뿐 아니라 개념적으로도 모순이다. 마찬가지로 비밀로서의 표시도 영업비밀의 나머지 요건 즉, 외부에 알려져 있지 않고 경제적 가치를 가지며 유출될 경우 큰 손해를 가져오는 자산이라는 것을 충분히 알고 있는 직원과의 관계에서 표시를 하지 않았다고 하여서 인식의 흠결로 인정할 수는 없는 것이다.

하지만, 앞서 살펴본 바와 같이 기업의 규모 등을 명시적으로 고려한 판결의 수가 충분하지 않을 뿐만 아니라, 침해의 방법과 수단, 영업비밀 보유자와 침해자의 신뢰관계 등의 사정은 영업비밀 침해가 발생하기 전에는 알 수 없기 때문에 표준 관리체계 수립에 고려할 수 없는 본질적인 한계가 있고, 무엇보다 사안별로 구체적인 사정을 종합적으로 고려하는 판결의 특성상 특정한 기준 – 예를 들어, 전기장비

제조업에 속한 기업의 매출이 10억원 미만이면 서약서 징구와 접근 제한 조치를 취하면 비밀관리성이 인정된다 등 -을 도출하기는 매우 어렵다.

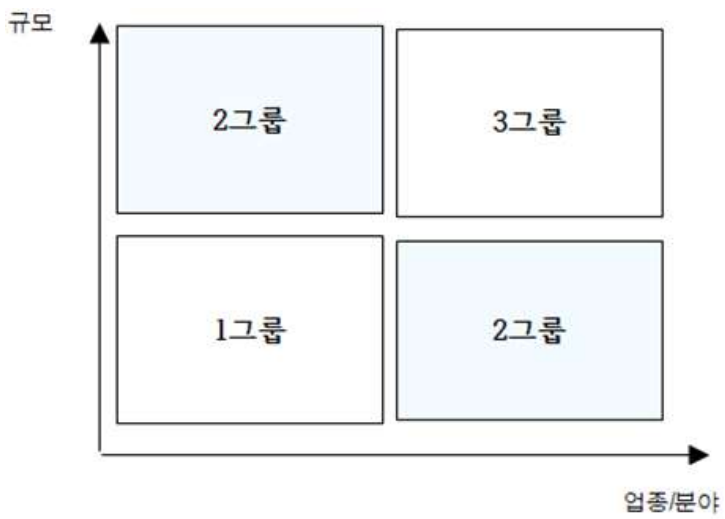
그럼에도 불구하고, 법원이 비밀관리성을 판단함에 있어서 기업의 규모나 업종 등을 고려하는 것이 분명하고, 기업 등 영업비밀 보유자 입장에서는 규모나 업종에 따른 특성을 고려하지 않는 일반적인 기준을 모두 따르기가 현실적으로 불가능한 경우가 많기 때문에, 일정한 한계가 불가피하더라도 기업 규모 및 업종을 고려한 영업비밀 표준 관리 체계가 필요하다.

이에 이번 연구에서는 앞서 살펴본 영업비밀 관련 판결의 분석 결과와 영업비밀 보호센터를 통해 수행한 기업 대상 영업비밀 보호관리 컨설팅 경험 등을 종합적으로 고려하여 다음과 같은 표준 관리 체계를 제시하고자 한다.

2.2 업종·규모별 영업비밀 표준 관리 체계

2.2.1 1차 도출 체계

기업 규모 등을 고려하여 비밀관리성을 판단한 판결을 종합해 보면, 법원은 기업의 자본금이나 종업원 수, 매출, 시장점유율 등 규모가 클수록 비밀관리성 요건을 엄격하게 판단하며, 이러한 규모와 관련된 요소는 필연적으로 해당 기업이 속한 업종에 따라 달라진다는 점을 고려하여, 다음과 같이 3개의 그룹으로 구분하여 표준체계를 마련하였다.



여기에서 ‘규모’는 영업비밀 보유 기업의 종업원 수, 매출액, 자본금 등을 기준으로 하며, ‘업종’ 또는 ‘분야’는 영업비밀 보유 기업이 속한 업종을, ‘분야’는 영업비밀에 해당하는 정보가 속한 (기술) 분야의 특성을 고려하여 3개 그룹으로 분류하였다.

[표 22] 표준 체계(1차) - 규모·업종(분야)별 기업 분류

구분	관리수준	정의 / 관리 수준	설명
1그룹	제도적·인적 관리 중심	규모가 작고 업종/(기술)분야의 특성상 고도한 영업비밀 보호관리 조치를 할 수 없거나, 필요하지 않은 경우	▪ 종업원 수 10명 미만, 매출액 5억원 이하 / 소상공인·스타트업일반 제조업(기계 등) 또는 서비스업 ▪ 경영정보 위주이거나 영업비밀의 가치/유출 위험이 크지 않은 경우
2그룹	제도적·인적 관리 + 일부 물적 관리	1그룹 대비 규모가 크거나 업종/(기술)분야의 특성상 주요 영업비밀 관리조치를 취할 필요가 있는 경우	▪ 종업원 수 10~50명, 매출액 20억원 이하 / 소기업 ▪ 전기전자/정보통신/바이오/첨단기계소재 분야 ▪ 영업비밀의 가치/유출 위험성이 1그룹 대비 큰 경우
3그룹	제도적·인적·물적 관리	(상대적으로) 규모가 크고 업종/(기술)분야의 특성상 상당한 정도의 보호관리 조치가 필요한 경우	▪ 종업원 수 50명 이상 / 매출액 20억원 이상 / 중기업 ▪ 화학/전기전자/정보통신/첨단기계소재 분야 ▪ 영업비밀의 가치(개발비용/피해액)가 크고, 유출 위험성도 높은 경우

다만, 이 체계에 의할 경우 어떤 기업이 종업원 수로는 1그룹에 속하지만 매출 기준으로는 3그룹에 속하는 경우 어떤 체계를 적용할지 판단하기 어렵다는 단점이 있고, 그룹의 정의 자체가 각 그룹간의 상대적 비교를 통해 이루어지므로 비교 대상이 없는 특정 기업이 ‘상대적으로’ 규모가 어느 정도인지를 판단하기 곤란하다는 등의 단점이 있다.

2.2.2 2차 도출 체계

법원이 비밀관리성을 판단함에 있어 고려하는 여러 가지 요소 중에 상대적으로 가장 객관화할 수 있는 지표가 자본금, 매출, 종업원 수 등 기업의 규모나 업종이라고 할 수 있는데, 중소기업기본법(제2조) 및 동법 시행령(제3조)에서도 자산총액이

5천억원 미만인 기업으로서 주된 업종에 따른 기업의 평균매출액 또는 연간매출액을 기준으로 대기업과 중소기업을 나누고 있으며, 중소기업 중 해당 기업이 영위하는 주된 업종별 평균매출액 등이 별도의 기준에 맞는 기업을 소기업으로, 소기업이 아닌 중소기업을 중기업으로 분류하고 있다는 점에서[19] 일응 표준 체계 개발의 기준으로 활용할 수 있다. 물론, 중소기업 육성을 목적으로 통계적 데이터를 기반으로 한 중소기업 분류 기준을 영업비밀 표준 체계에 그대로 적용하기에 한계가 분명하다. 그러나, 표준 체계 자체가 규범적 효력을 가지기 보다는 좀더 구체화된 형태의 가이드라인이라는 의미일 수 밖에 없고, 중소기업 분류는 보편적으로 사용되는 명확한 기준이라는 점에서 장점도 있기 때문에 이를 기반으로 2차 표준 체계를 도출하였다.

[표 23] 중소기업 기본법 시행령에 따른 중소기업 분류

해당 기업의 주된 업종	중소기업 규모 기준
의복, 의복액세서리 및 모피제품 제조업 / 가죽, 가방 및 신발 제조업 / 펄프, 종이 및 종이제품 제조업 / 1차 금속 제조업 / 전기장비 제조업 / 가구 제조업	평균매출액등 1,500억원 이하
농업, 임업 및 어업 / 광업 / 식료품 제조업 / 담배 제조업 / 섬유제품 제조업(의복 제조업은 제외) / 목재 및 나무제품 제조업(가구 제조업은 제외) / 코크스, 연탄 및 석유정제품 제조업 / 화학물질 및 화학제품 제조업(의약품 제조업은 제외) / 고무제품 및 플라스틱제품 제조업 / 금속가공제품 제조업(기계 및 가구 제조업은 제외) / 전자부품, 컴퓨터, 영상, 음향 및 통신장비 제조업 / 그 밖의 기계 및 장비 제조업 / 자동차 및 트레일러 제조업 / 그 밖의 운송장비 제조업 / 전기, 가스, 증기 및 공기조절 공급업 / 수도업 / 건설업 / 도매 및 소매업	평균매출액등 1,000억원 이하
음료 제조업 / 인쇄 및 기록매체 복제업 / 의료용 물질 및 의약품 제조업 / 비금속광물제품 제조업 / 의료, 정밀, 광학기기 및 시계 제조업 / 그 밖의 제품 제조업 / 수도, 하수 및 폐기물 처리, 원료재생업(수도업은 제외) / 운수 및 창고업 / 정보통신업	평균매출액등 800억원 이하
산업용 기계 및 장비 수리업 / 전문, 과학 및 기술 서비스업 / 사업시설관리, 사업지원 및 임대 서비스업(임대업은 제외) / 보건업 및 사회복지 서비스업 / 예술, 스포츠 및 여가 관련 서비스업 / 수리(修理) 및 기타 개인 서비스업	평균매출액등 600억원 이하
숙박 및 음식점업 / 금융 및 보험업 / 부동산업 / 임대업 / 교육 서비스업	평균매출액등 400억원 이하

19) 중소기업 기본법 시행령 별표 1 및 별표 3 참조 (2019. 2. 15. 시행)

[표 24] 중소기업 기본법 시행령에 따른 소기업 분류

해당 기업의 주된 업종	소기업 규모 기준
식료품 제조업 / 음료 제조업 / 의복, 의복액세서리 및 모피제품 제조업 / 가죽, 가방 및 신발 제조업 / 코크스, 연탄 및 석유정제품 제조업 / 화학물질 및 화학제품 제조업(의약품 제조업은 제외) / 의료용 물질 및 의약품 제조업 / 비금속 광물제품 제조업 / 1차 금속 제조업 / 금속가공제품 제조업(기계 및 가구 제조업은 제외) / 전자부품, 컴퓨터, 영상, 음향 및 통신장비 제조업 / 전기장비 제조업 / 그 밖의 기계 및 장비 제조업 / 자동차 및 트레일러 제조업 / 가구 제조업 / 전기, 가스, 증기 및 공기조절 공급업 / 수도업	평균매출액등 120억원 이하
농업,임업 및 어업 / 광업 / 담배 제조업 / 섬유제품 제조업(의복 제조업은 제외) / 목재 및 나무제품 제조업(가구 제조업은 제외) / 펄프, 종이 및 종이제품 제조업 / 인쇄 및 기록매체 복제업 / 고무제품, 및 플라스틱제품 제조업 / 의료, 정밀, 광학기기 및 시계 제조업 / 그 밖의 운송장비 제조업 / 그 밖의 제품 제조업 / 건설업 / 운수 및 창고업 / 금융 및 보험업	평균매출액등 80억원 이하
도매 및 소매업 / 정보통신업	평균매출액등 50억원 이하
수도, 하수 및 폐기물 처리, 원료재생업(수도업은 제외) / 부동산업 / 전문·과학 및 기술 서비스업 / 사업시설관리, 사업지원 및 임대 서비스업 / 예술, 스포츠 및 여가 관련 서비스업	평균매출액등 30억원 이하
산업용 기계 및 장비 수리업 / 숙박 및 음식점업 / 교육 서비스업 / 보건업 및 사회복지 서비스업 / 수리(修理) 및 기타 개인 서비스업	평균매출액등 10억원 이하

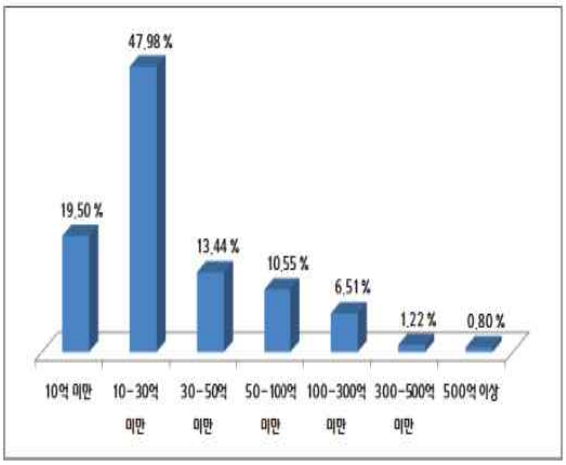
[표 25] 기업체당 평균 매출액/총자산/자본

단위 : 천원

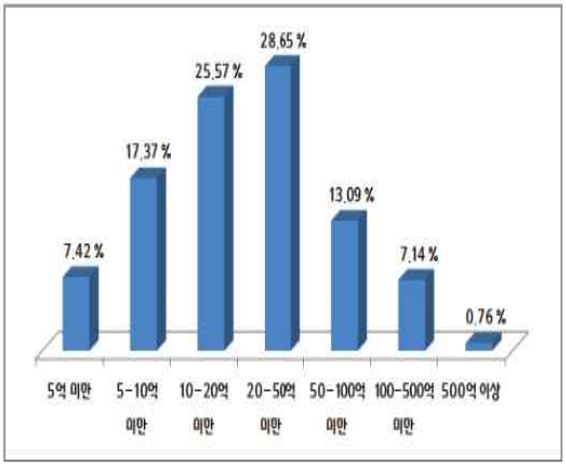
	제조업	소기업	중기업
평균 매출액	4.330.906	2.598.567	25.281.690
평균 총자산	4,348,068	2,713,692	23,896,397
평균 자본금	1,829,034	1,075,871	20,937,734

(출처: 2017년 기준 중소기업 경영지표/제조업, 중소기업중앙회, 2018)

[그림 8] 매출액 규모별 기업체 분포



[그림 9] 자산 규모별 기업체 분포



(출처: 상동)

[표 26] 표준 체계(2차) - 규모에 따른 기업 분류

구분	관리 수준	설명
소상공인[20] 소기업	제도적·인적 관리 중심 + 일부 물적 관리	상시 근로자가 10명 미만인 소상공인 또는 그에 준하는 규모의 소기업인 경우, 영업비밀 보호 관리를 위한 인적·물적 자원에 한계가 있기 때문에, 제도적·인적 보호 관리 조치를 위주로 표준 체계를 설계함
중소기업	일반적인 수준의 제도적·인적·물적 관리	소상공인이나 일부 규모가 매우 작은 소기업을 제외하면, 일반적인 수준의 제도적·인적·물적 보호관리 조치를 취하는 것이 가능하다고 보아, 상당한 정도의 인적·물적 투자가 필요 없는 보호 관리 조치 전반을 취하도록 체계를 설계함
중기업 중견기업	고도화된 수준의 제도적·인적·물적 관리	중견기업 및 이에 준하는 정도의 중기업의 경우 매출이나 자산, 종업원 수 등의 규모를 고려할 때 상당한 수준의 인적·물적 투자가 이루어질 수 있으므로, 보다 고도화된 수준의 영업비밀 보호관리 조치를 취하도록 표준 체계를 설계함

20) "소상공인"이란 소기업 중 상시 근로자가 10명 미만인 사업자로서 주된 사업에 종사하는 상시 근로자의 수가 광업·제조업·건설업 및 운수업의 경우에는 10명 미만, 그 외 업종의 경우에는 5명 미만인 사업자를 말한다(「소상공인 보호 및 지원에 관한 법률」 제2조 및 「소상공인 보호 및 지원에 관한 법률 시행령」 제2조제1항).

2차로 도출한 표준 체계의 경우, 가장 큰 문제는 중소기업에 해당하는 기업이 지나치게 많기 때문에, 같은 중소기업이라도 구체적인 여건은 전혀 다를 수 있어 규모나 업종을 고려한 실질적 체계를 도출한다는 취지에 반할 수 있다는 점인데, 이는 영업비밀 보호 컨설팅을 통해 개별적으로 기업의 여건을 고려하여 표준 체계를 수정하거나 탄력적으로 운영하고, 구체적인 적용 사례가 누적되는 과정에서 점진적으로 보완하는 것이 바람직하다.

2.3 영업비밀 표준 관리체계의 내용

2.3.1 제도적 보호·관리 분야

제도적 보호·관리 분야는 영업비밀 보호관리 규정을 기반으로 기업이 보유한 영업비밀을 일반 정보와 구분하여 표시하고, 담당 인력이나 조직을 갖추는 것을 내용으로 하며, 중소기업용 표준 체계를 기준으로 소상공인의 경우 다소 완화된 내용으로, 중기업 또는 중견기업의 경우 강화된 내용으로 구성된다.

[표 27] 표준체계에 따른 제도적 보호·관리 조치

구분	소상공인	중소기업	중견기업
관련 규정	• 영업비밀 보호관리 규정 제정	• 영업비밀 보호관리 규정의 세부 지침 - 관련 절차 규정	• 영업비밀 보호관리 규정 및 세부 지침에 대한 정기적 검토 및 개정
등급 분류	• ‘영업비밀’과 ‘일반정보’ 로 구분	• 영업비밀, 대외비, 일반정보로 구분 • 영업비밀 보유/이용 현황 조사	• 영업비밀의 중요도에 따라 1급, 2급, 3급으로 세분 • 정기적 보유/이용 현황 조사 • 등급별 보존기한/재분류 기한 관리 • 등급별 폐기 절차 및 방법 정의
표시 고지	• 영업비밀 문서 - 표지/본문 영업비밀임을 표시	• 문서 - 표지/본문에 영업비밀/대외비 표시	• 문서 - 표지/본문에 영업비밀/대외비 표시

	- (필요시) 보관함이나 바인더에 표시 • 전자 파일 - 파일명, 문서 상/하단에 표시	• 전자 파일 - 파일명, 문서 상/하단에 표시 • 주요 정보 - 영업비밀 원본 증명 이용 (권장)	• 전자 파일 - 파일명, 문서 상/하단에 표시 • 주요 정보 - 영업비밀 원본 증명, 기술자료임치
	* 정보나 저장매체의 특성상 '표시'가 어려운 경우(예: 데이터베이스 등) 임직원에게 고지하거나 시스템 로그인시 안내/주의 문구(팝업) 삽입		
인력 조직	• 영업비밀 담당자(겸직) 지정	• 영업비밀 담당자(겸직) - 2인(임원+담당자) • 각 부서별 담당자 지정 - 부서별 책임자 1인 이상	• 영업비밀 보호관리 전담 조직 설치 - 전담 인력 2인 이상 • 각 부서별 담당자 지정 - 부서별 책임자 및 실무자 • (필요시) 관련 위원회 설치/운영

2.3.2 인적 보호·관리 분야

인적 보호·관리 분야는 임직원 대상 서약서 징구와 영업비밀 보호 교육, 징계 및 보상 절차 마련, 퇴사자 인터뷰 등으로 구성되어 있으며, 기업의 규모를 불문하고 모두 필수적으로 취해야 할 조치들이다. 다만, 기업 여건에 따라 전체 임직원을 대상으로 할 것인지, 시기와 횟수, 절차의 완결성에서 다소 차이를 보일 수 있다.

[표 28] 표준체계에 따른 인적 보호·관리 조치

	소상공인	중소기업	중견기업
서약서	• 임원, 핵심/주요 인력 대상 - 입사 및 퇴사시(경업금지 약정 포함) • 외부인(거래처/협력업체) - 보안서약 또는 비밀유지 계약 체결	• 임직원 전체 - 입사 및 퇴사시(경업금지 약정 포함) • 외부인(거래처/협력업체) - 보안서약 또는 비밀유지 계약 체결	• 임직원 전체 - 입사 및 퇴사시(경업금지 약정 포함) • 정기적 징구 (연1회) • 주요 프로젝트 참여 인력 - 프로젝트 참여자용 서약서 징구 • 외부인(거래처/협력업체 등) - 비밀유지계약 체결

교육	• 전체 임직원 대상 정기 교육 (연 1회) • 온라인 교육 활용	• 정기 교육 (연 1~2회) - 외부 전문가 교육 포함 • 주요 인력 대상 교육 (연 2회) • 온라인 교육	• 정기 교육 (연2회) - 외부 전문가 교육 포함 • 입사자, 승진자 대상 교육 진행 • 부서/사업부분별 특화 교육 • 담당자 역량 강화 교육 • 영업비밀 보호 교육 이수 의무화
징계 보상	• 영업비밀 관련 징계/보상 규정 제정(인사/급여 규정에 포함 가능)	• 직무발명 규정 제정 - 발명/영업비밀 보상 제도 • 영업비밀 보호 우수 임직원 포상/표창	• 인사규정/직무발명 규정 정비 - 구체적인 징계/보상 기준 및 절차 마련 • 개인별 평가 (인사고과) - 우수 임직원 포상/표창 • 주요 인력 보안 수당 지급
기타	• 퇴사 인터뷰(Exit Interview) • 정기적 감사를 통한 규정 준수 확인		

2.3.3 물적 보호·관리 분야

물적 보호·관리 분야는 제도적, 인적 보호·관리에 비해 상대적으로 직접적인 비용 지출이 수반되는 경우가 많기 때문에, 기업의 규모나 자금 여력에 따라 관련 조치를 모두 취하기가 어려운 경우가 있다. 다만, 기업의 업무 환경이 컴퓨터나 네트워크를 기반으로 하고 있는데다, 기업이 보유한 정보의 대부분이 전자 파일 형태로 생성·보관되는 경우가 많기 때문에 영업비밀 보호를 위한 기본적인 물리적·기술적 보호 조치는 필수적이다. 또, 물적 보호·관리 조치가 수반되지 않는 경우 제도적·인적 보호·관리 조치의 실효성이 약화될 수 있으며, 업무 효율성도 저해될 가능성도 있다. 따라서 중소기업의 경우에도 기본적인 출입 통제나 개인용 컴퓨터에서도 충분히 가능한 수준의 물적 보호·관리 조치를 취하는 것으로 표준 체계를 구성하였다.

[표 29] 표준체계에 따른 물적 보호·관리 조치

<table>
<tr><th></th><th>소상공인</th><th>중소기업</th><th>중견기업</th></tr>
<tr><td rowspan="2">분리보관</td><td>• 주요 영업비밀 분리/보관
- 문서/유형물 : 잠금장치 캐비닛
- 전자 파일 : 별도 폴더</td><td>• 영업비밀 분리/보관
- 문서/유형물 : 캐비닛, 금고
- 전자 파일 : 별도 저장 장치/폴더
• 부서별 영업비밀 관리</td><td rowspan="2">• 영업비밀 분리/보관
- 문서/유형물 : 캐비닛, 금고
- 전자 파일 : 별도 저장 장치/폴더
• 전사적 영업비밀 보유/관리 현황 파악
• 부서별 영업비밀 정보 분리/보관
• 퇴사자 하드디스크/노트북 분리/보관
• 문서중앙화 솔루션 (권장)</td></tr>
<tr><td colspan="2">※ 저장매체, 정보의 특성 또는 업무상 필요에 따라 분리/보관이 불가능할 경우 접근/이용 권한 있는 자에게 영업비밀임을 고지하고, 해당 정보를 특정/명시하여 별도 서약서를 징구</td></tr>
<tr><td>출입통제</td><td>• 출입문 통제
• 외부인 출입 제한
- 임직원 동행
- 업무시간 외 출입 금지</td><td>• 출입문 및 주요 부서 (예: 연구소)
• 출입제한 구역 지정 및 표시
• 외부인 출입 제한
- 임직원 동행
- 업무시간 외 출입 금지
- 출입대장 작성/관리
• 주요 구역 CCTV, 지문인식 장치 등 설치</td><td>• 출입 제한 구역 지정 및 표시
• 외부인 출입 통제
- 출입대장 작성/관리
- (사전) 출입신청
- 접견 구역 설치
- 임직원 동행
- 출입증 발급
- 영업비밀 보호 서약(서)
• CCTV, 지문인식 장치 등 설치
- 출입구 및 엘리베이터, 비상계단 등</td></tr>
<tr><td>이용제한</td><td>• 업무상 필요에 따라 이용권한 부여
• PC/업무시스템/클라우드 - ID/PW 설정
• 암호화 (MS Office/한글 암호 설정)</td><td>• 업무상 필요에 따른 이용권한 세분화
• PC/업무시스템/클라우드 - ID/PW 정기적 변경
• 암호화 (DRM)</td><td>• 직급별, 업무별 이용권한 세분화
• 암호화 - DRM 솔루션 등(권장)
• 정보 이용 현황 모니터링 / 관제 시스템</td></tr>
<tr><td>반출제한</td><td>• 외부인에 의한 반출 제한
• 업무용 이메일 사용 권장
- 영업비밀 정보 발송 시 메일 제목 또는 본문에</td><td>• 이용/접근 권한 없는 자의 반출 제한
• 개인/비인가 이메일/클라우드 사용 제한</td><td>• USB, 외장 하드, 노트북, 태블릿 등 휴대용 저장 장치 이용 제한 및 반출 통제</td></tr>
</table>

	'영업비밀' 표시/주의 문구 삽입	• USB/외장하드 사용 제한 (반출 승인) • 휴대전화/태블렛 사용 제한(사전 승인) • 내부정보유출방지서비스 활용(권장) * 중소벤처기업부/한국산업기술보호협회	- 반출입대장 작성/관리 • 개인/비인가 이메일/클라우드 접근 차단 • 데이터유출방지(DLP) 솔루션 (권장) • 프린터/복합기 출력물 관리 (이용현황)
접근제한	• 외부인 접근 차단 (로그인 계정 관리) • 퇴사시 접근 차단 (ID/PW 변경/삭제)	• 이용 권한 없는 자의 접근 제한 • 퇴사 시 접근 차단 (ID/PW 삭제) • 운영체제(Windows 등) 방화벽 활용	• 영업비밀 등급별 접근 권한 부여 • 퇴사 시 접근 차단 (ID/PW 삭제) • 네트워크 방화벽 솔루션 (권장)
기타	• 「영업비밀 관리시스템」 도입 (선택) * 특허청/영업비밀보호센터	• 「영업비밀 관리시스템」 설치/운영 • 보안관제 서비스 활용 * 중소기업 기술지킴서비스 (중소벤처기업부/한국산업기술보호협회)	• DRM, DLP, 문서중앙화, 방화벽, 보안관제 등 정보보안 시스템/솔루션 권장 * 기술유출방지시스템 구축 지원 사업(중소벤처기업부/대중소기업농어업재단)

2.4 영업비밀 보호·관리 체계 구축을 위한 컨설팅 추진 방안

2.4.1 기존 영업비밀 보호 컨설팅의 개선 사항

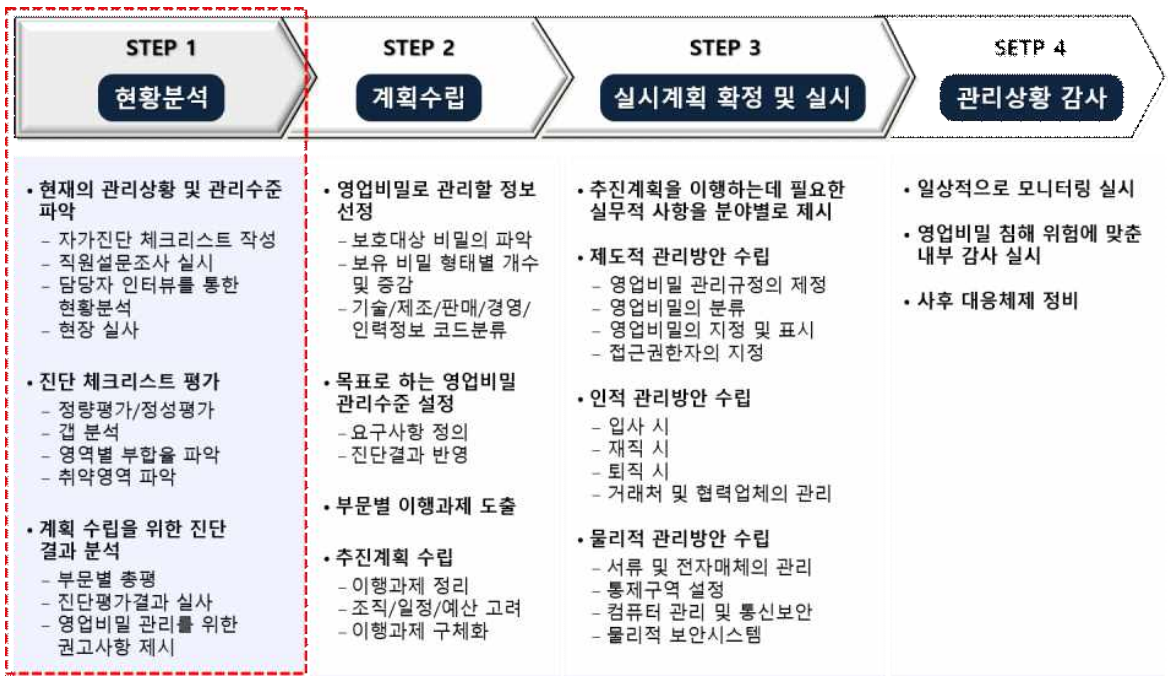
한국지식재산보호원 산하 영업비밀보호센터는 신청 기업에 대한 사전 설문 조사를 바탕으로 영업비밀 보호 컨설팅을 수행하고 있는데, 기업의 관리자나 임직원이 영업비밀에 대해 잘 알지 못하는 경우 설문에 대한 응답 결과만으로는 기업의 영업비밀 보호·관리 현황을 정확하게 알 수 없는 경우가 발생한다. 특히, 기업에 따라서는 '보안'과 '영업비밀 보호'를 같은 것으로 보거나, 반대로 지나치게 엄격하게 구분하는 경우에 더욱 그러하다. 추후 설문 조사 외에 현장 실사 및 면접 방식에 의한 조사를 보완할 경우 좀더 정확한 실태 파악이 가능할 것으로 보인다.

[표 30] 현행 영업비밀 보호컨설팅 현황 점검표 일부 (관리자용)

대분류	중분류	점검사항	선택
1. 제도적 관리	1.1. 최고경영자 태도	① 영업비밀 보호를 위한 감시설비, 보안솔루션 확충, 교육파견 등 영업비밀 보호 관련 예산을 당해 연도에 책정되어 있거나, 최근 1년간 영업비밀 보호에 비용을 지불한 실적이 있다.	□
		② 최고 경영자가 회의 시, 교육 시 등 수시(분기 1회 이상)로 영업비밀의 중요성을 강조하고 실행을 확인하는 등 적극적인 태도를 보인다.	□
		③ 최고경영자가 관심 없거나, 말로는 영업비밀의 중요성을 강조하지만 상기 내용을 실행하지 않는다.	□
	1.2. 접근권한 제한 정책	① 회사의 모든 영업비밀 정보에 대해 접근통제 기준을 가지고 통제하며 퇴직, 부서변경 등에 따른 권한 변경 시 접근권한을 회수한다.	□
		② 일부 중요 영업비밀에 대해 접근권한을 통제하고 있다.	□
		③ 영업비밀에 대한 접근통제 정책을 가지고 있지 않다.	□
	1.3. 비밀관리 규정 제정	① 영업비밀 관리규정 준수 여부에 대하여 매년 감사 활동을 하고 있다.	□
		② 영업비밀 관리규정이 사규에 포함되어 있으며, 배포, 게시, 교육 등의 방법으로 수시로 임직원들에게 그것의 이행을 공지하고 있다.	□
		③ 영업비밀 관리규정이 없거나, 있어도 사문화되어 준수하지 않고 있다.	□
	1.4. 관리책임자 지정	① 사내 전체 또는 부서별 영업비밀 관리책임자가 지정되어 있다.	□
		② 영업비밀 관리책임자가 지정되어 있지 않다.	□
	1.5. 비밀정보 구분·분류	① 회사에서 취급하고 있는 정보에 대해 일반 정보와 영업비밀 정보로 구분한다.	□
		② 영업비밀로 별도 구분하지 않는다.	□
	1.6. 비밀정보 표시	① 등록된 영업비밀 문서의 표지나 전자문서 폴더 등에 비밀임을 표시한다.	□
		② 비밀임을 표시하지 않는다.	□

	1.7. 법적 분쟁 발생 시 입증수단 이용여부	① 영업비밀 보유 여부에 대해 법적 효력을 갖는 입증 수단 (원본증명서비스, 기술 임치제도 등)을 이용하고 있다.	□
		② 입증 수단을 이용하고 있지 않다.	□

다음으로 기존 영업비밀 보호 컨설팅은 1회성으로 진행되는데, 이로써는 실질적인 영업비밀 보호관리 체계 구축이 매우 어려운 실정이다. 아래 그림에서와 같이 일반적인 컨설팅은 현황(AS-IS) 분석을 기반으로 한 실행 계획 수립, 실행 및 점검과 후속 조치 등의 순서로 수차례 이상 진행되는데 반해, 현재의 영업비밀 보호 컨설팅은 상당수의 경우 영업비밀에 대한 이해도가 부족한 중소기업들에게 영업비밀 보호의 중요성이나 필요성 정도를 인식하게 하는 수준에 머무르게 된다는 점에서 3회 이상의 실질적인 컨설팅의 추진이 필요해 보인다.



[그림 10] 현행 영업비밀 관리 체계 구축 단계별 세부 사항

기존 영업비밀보호컨설팅은 사전 설문조사 결과를 바탕으로 대상 기업의 영업비밀 보호관리 수준을 5단계로 구분하여, 단계적 개선 방안을 제시하는 방식으로 이루어지고 있는데, 기업의 규모나 업종에 따른 구체적인 사정을 감안한 보호관리 체계를 제시하는데 다소 한계가 있다.

[표 31] 현행 영업비밀 보호관리 수준 분류 기준

점수	등급	상 태
81점 이상	**양호(A)**	영업비밀 관리체계를 구비하여 잘 이행하고 있음
71~80점	**보통(B)**	영업비밀 유출 시 법적으로 보호받을 정도로 이행하고 있지만 유출방지 대책은 보통임
61~70점	**취약(C)**	영업비밀 유출 시 법적으로 보호받기 다소 미흡하고 유출에 취약하므로 관리체계 구축 필요
41~60점	**위험(D)**	영업비밀 유출 시 법적 보호가 어렵고, 유출 위험에 노출되어 있으므로 시급한 관리체계 구축 필요
40점 이하	**무관심(F)**	상시로 영업비밀 유출에 노출됨

2.4.2 영업비밀 표준 관리 체계를 활용한 컨설팅 추진 방안

이번 연구를 통해 도출한 기업의 규모·업종을 고려한 영업비밀 표준 관리 체계를 활용한 컨설팅 추진의 가장 큰 특징으로는 대상 기업의 여건을 고려한 실질적인 보호관리 체계 구축이 가능하다는 점을 들 수 있다.

즉, 이번 연구를 통해 분석한 판결에서 알 수 있는 바와 같이 법원이 비밀관리성 여부를 판단함에 있어서 고려하는 제반 사항들을 설문이나 면접, 현장 실사를 통해 컨설턴트가 파악한 후, 표준 관리 체계에서 제시하고 있는 제도적·인적·물적 보호관리 조치를 대상 기업의 여건에 맞게 제시할 수 있기 때문이다.

[표 32] 영업비밀 컨설팅 추진 시 확인 사항

구분	확인해야 할 사항
업종	✓ 영업비밀 침해/유출 사건의 빈도가 높은 업종인지 여부
규모	✓ 종업원 수, 자본금, 매출액/시장점유율
정보의 유형	✓ 기업이 보유한/보호하고자 하는 주요 정보가 설계도, 소스코드 등 기술정보인지, 고객/시장 정보, 경영계획 등 경영정보인지 ✓ 해당 정보가 전자 파일 형태로 생성/보관되는지, 문서 및 기타 유형물로 생성/보관되는지 여부
정보의 가치	✓ 기업에서 보호하고자 하는 정보의 가치를 평가 (비용 기준, 수익 기준, 시장 기준)
정보의 성격	✓ 대상 정보가 기업 내 소수 인원만 알고 있으면 되는지, 대다수 또는 상당수의 인원이 공유해야 하는지 여부
침해/유출 경험	✓ 과거 영업비밀 유출 사고가 있었는지 여부

영업비밀 표준 관리 체계는 소상공인, 중소기업, 중견기업을 기준으로 영업비밀 보호·관리를 위한 제반 조치에 일응 차이를 두고 있으나, 이는 절대적·규범적인 기준이 아니며 사안에 따라 탄력적·상대적으로 적용하는 것이 바람직할 것이다.

서울동부지방법원 2019. 3. 13. 선고 2018고단2485 판결

비밀 관리성으로서 접근 제한과 객관적 인식 가능성 (표시) 은 침해 행위자와 목적물에 따라 상대적으로 판단할 수밖에 없다. 이 사건에서 피고인 B와 같은 개발자의 경우 평소 프로그램의 핵심 자료에 아무런 제한 없이 접근이 가능할 것이므로 퇴근, 외부 업무, 퇴직 시 등에 외부 반출을 못하도록 하는 규정과 물적 시설을 중분히 운영하더라도 의도하기에 따라서 얼마든지 회피가 가능하므로 (굴지의 대기업에서 끊임없이 침해와 경쟁사로의 유출 사건이 일어나고 있는 것이 현실이다) 이미 회사 내부적으로 업무상 접근 권한이 주어진 직원이 행위자인 경우 그에 대한 접근 제한 조치의 상당성을 따지는 것은 무의미할 뿐 아니라 개념적으로도 모순이다. 마찬가지로 비밀로서의 표시도 영업비밀의 나머지 요건 즉 외부에 알려져 있지 않고 경제적 가치를 가지며 유출될 경우 큰 손해를 가져오는 자산이라는 것을 충분히 알고 있는 직원과의 관계에서 표시를 하지 않았다고 하여서 인식의 흠결로 인정할 수는 없는 것이다.

다만, 사안에 따라서는 기업의 규모 등을 고려해서 비밀관리성을 인정하기 어렵다고 한 판례도 있으므로 주의를 요한다.

수원지방법원 안산지원 2018. 4. 6. 선고 2017고정710 판결

고소인 회사는 플라스틱 자동 성분 분석기계 제조업 등을 목적으로 2004. 11. 8. 설립된 회사로서 자본금이 32억원을 상회한다. 또한 연매출이 25억원 정도이고, 국내 폐기물 선별기 시장을 약 30%정도 점유하고 있는 바, 그 규모나 능력이 미미하지 아니한 것으로 보임에도 앞서 든 사정에 비추어 볼 때, 이 사건 프로그램 소스코드를 영업비밀로서 관리하기 위한 상당한 노력을 했다고 보기 부족하다.

서울중앙지방법원 2016. 11. 4. 선고 2015가합568041

원고가 일부 직원들로부터 보안서약서를 제출 받은 사실만으로는 원고가 소규모 회사라는 점을 고려하더라도, 이 사건 파일들이 상당한 노력에 의하여 비밀로 유지되었다고 보기 힘들다.

영업비밀 표준관리체계 구축을 위한 컨설팅은 다음과 같은 순서와 내용으로 진행 가능하다.

DAY 1	DAY 2	DAY 3	DAY 4	DAY 5
DAY 1	DAY 2		DAY 3	

현황 조사·분석 Analysis	계획 수립 Planning	관리 체계 구축 Implementation	구축 상황 점검 Monitoring	후속 보완 / 결과 보고 Modification
기업 특성을 고려한 보호관리 체계 수립을 위한 조사·분석	현황 분석 결과를 바탕으로 기업의 영업비밀 보호관리 체계 수립 계획 제시	제도적·인적·물적 분야에서의 보호관리 체계를 수립	영업비밀 관리 체계 분야별 이행 상황 점검	점검 결과를 토대로 미비 사항 보완 및 후속 조치
□ **기업 특성 조사** - 규모(종업원 수, 매출 등) - 업종, 시장점유율 등 - 현안 및 요구 사항	□ **현황 분석 결과 보고** - 영업비밀 유출 위험성 - 보호관리 수준 - 임직원 인식 수준	□ **제도적 관리** - 영업비밀 규정 제정 - 등급분류 - 표시 및 고지 등	□ **구축 상황 점검** - 분야별 이행 상황 확인 - 미비 사항 및 원인 조사 - 애로 사항 확인	□ **보완 조치 시행** - 분야별 보완 조치 이행 - 단계별 개선 방안 제시 - 후속 이행 사항
□ **보호관리 현황 조사** - 제도적·인적·물적 분야 - 영업비밀 유출 경험 - 설문·면접·현장 실사	□ **관리 체계 수립 (안) 제시** - 목표 수준 설정 - 단계별 추진 방안 - 부문별 이행 과제	□ **인적 관리** - 영업비밀 서약서 - 영업비밀 교육 - 징계/보상 절차 마련	□ **보고 및 면담** - 구축 상황 보고 - 대표자 및 임원 면담 - 담당자·직원 면담	□ **구축 결과 보고 및 평가** - 컨설팅 성과 및 한계 - 향후 일정 및 계획 수립
□ **현황 분석** - 정량/정성 평가 - 취약점 파악 - 갭(GAP) 분석	□ **세부 계획 수립** - 추진 일정 (Roadmap) - 수행 인력/조직 (TF) 구성	□ **물적 관리** - 분리 보관 - 출입 제한 - 이용·반출·접근 제한	□ **후속 보완 계획 수립** - 미비 사항의 보완 - 관리 체계 수정	□ **정기적 모니터링** - 영업비밀 관리 체계 정착 여부 확인 - 고도화 방안 수립

Ⅳ. 영업비밀 등급 분류 체계

1. 개요

1.1 등급 분류의 필요성

영업비밀로 보호할 정보에 대한 등급 분류는 그 자체로 영업비밀 보호를 위한 필수적인 요건은 아니라고 할 수 있다. 대법원의 일관된 입장에 따르면 영업비밀로 보호받기 위한 요건으로 비밀관리성의 핵심은 영업비밀 보유자가 주관적으로 해당 정보가 비밀이라고 인식하는 것으로는 부족하고, 해당 정보에 접근할 수 있거나 접근한 자로 하여금 객관적으로 그 정보가 비밀이라는 사실이 인식 가능한 상태에 이르는 것이기 때문이다. 그 대표적인 방법이 비밀임을 표시하거나 고지하는 것이다. 결국, 영업비밀에 해당하는 정보를 반드시 등급을 나눠 분류해야 하는 것은 아니다. 오히려 무엇이 영업비밀에 해당하는지를 특정하고 구분하는 것이 더 본질적인 요소라 할 수 있다.

대법원 2008. 7. 10. 선고 2008도3435 판결 외 다수

'상당한 노력에 의하여 비밀로 유지된다'는 것은 그 정보가 비밀이라고 인식될 수 있는 표시를 하거나 고지를 하고, 그 정보에 접근할 수 있는 대상자나 접근 방법을 제한하거나 그 정보에 접근한 자에게 비밀준수의무를 부과하는 등 객관적으로 그 정보가 비밀로 유지 · 관리되고 있다는 사실이 인식 가능한 상태인 것을 말한다.

한편, 영업비밀 침해가 문제된 사안에서 법원은 영업비밀 보유자가 일반적·추상적 보호 조치만을 취했을 뿐, 당해 사건에서 침해 여부가 쟁점이 된 정보를 구분하거나 분류를 하지도 않고, 따라서 상대방이 무엇이 영업비밀인지 여부를 알 수 없는, 다시 말해 '객관적 인식 가능 상태'에 이르지 못했기 때문에 비밀관리성을 인정할 수 없다고 판단하고 있다.

대법원 2008. 7. 10. 선고 2008도3435 판결

피고인들 중 일부가 입사할 때 '업무상 기밀사항 및 기타 중요한 사항은 재직 중은 물론, 퇴사 후에도 누설하지 않는다'는 내용의 일반적인 영업비밀준수 서약서를 작성한 사실은 있으나, 피해회사에서 업무와 관련하여 작성한 파일에 관하여 보관책임자가 지정되어있거나 별다른 보안장치 또는 보안관리규정이 없었고, **업무파일에 관하여 중요도에 따라 분류를 하거나 대외비 또는 기밀자료라는 특별한 표시를 하지도 않았으며,** 연구원뿐만 아니라 생산직 사원들도 자유롭게 접근하여 파일서버 내에 저장된 정보를 열람 · 복사할 수 있었고, 방화벽이 설치되지 않아 개개인의 컴퓨터에서도 내부 네트워크망을 통하여 접근할 수 있는 등 이 사건 파일들이 상당한 노력에 의하여 비밀로 유지되었다고 보기 어려운 점을 종합하여 보면, 이 사건 파일은 영업비밀에 해당하지 않는다.

서울중앙지방법원 2010.6. 16. 선고 2009가합41286 판결

원고는 보안관리 규정을 제정하여 직원들에게 보안 및 비밀유지를 위한 **교육을 주기적으로 실시**하였고, 원고는 원고 소속 직원들인 피고들에게 **'보안규정 서약서'에 서명**토록 하여 이를 제출 받은 사실, 원고는 연구개발 전담부서를 두고 여기에서 개발된 기술정보 등을 관리하기 위하여 USB사용제한 등의 외부저장장치 제한정책, 영업비밀의 분류관리를 위하여 개발이력 관리시스템, **문서보안 시스템**을 적용하고 있고, 보안인증서에 의하여 접속하는 사내 인트라넷 시스템을 확보하고 있는 사실, 원고는 **프린터출력물 제어시스템**을 적용하고 있고, 원고의 연구소에서는 연구원이 노트북을 반출할 경우 엄격하게 사전 승인이 요청되고 있으며, 원고의 영업기밀 문서는 별도의 **문서보관실 캐비닛에 보관 후 시정장치**를 통해 개폐하고 있는 사실, 원고는 주식회사 에스텍시스템에게 원고의 보안 인력경비를 맡긴 사실을 각각 인정할 수 있다. 그러나 원고가 위와 같이 보안관리를 하여 왔다고 하더라도, **구체적으로 이 사건 영업자료가 비밀로 분류되었다거나 이 사건 영업자료에 그와 같은 표시가 되었다고 볼만한 자료가 없는 점**, 원고는 문서를 자료, 문서, 도면, 사진으로 구분하여 대외비로 관리하였다고 주장하면서도 이 사건 영업자료에 관하여는 어떻게 분류 및 관리하였는지를 밝히지 못하고 있는 점, 이 사건 서약서상의 기밀유지조항은 원고가 그 직원들에게 일반적추상적인 기밀유지의무를 부과한 것에 불과한 것으로 보여지는 점 등에 비추어 보면, 위와 같은 인정사실만으로는 원고가 이 사건 영업자료를 상당한 노력에 의해 비밀로서 관리하였다고 보기 어렵고, 달리 이를 인정할 만한 증거가 없다.

서울서부지방법원 2015. 2. 5. 선고 2013가합31847

원고의 **취업 규칙에서 직원들의 비밀 준수 의무**를 규정하고 있고, 피고 C 등이 각 체결한 **연봉 계약서에 비밀 누설 금지의무**가 규정되어 있으며, 피고 F, G가 비밀 준 수 서약서를 작성한 사실, 2010.10.경 원고 직원 L이 위 각 소스 파일에 대한 보안 관리를 책임지게 된 사실, L은 2010. 11. 2 경 각 팀장에게 솔루션 관련 원천 소스 에 대한 보안을 철저히 하라는 취지의 지시를 한 사실, 솔루션 사업부에서는 소스 세 이프 2005라는 프로그램을 통하여 소스들을 관리해 왔는데, 솔루션 사업부 직원들은 각자에게 개별적으로 부여 된 아이디와 비밀 번호를 이용하여서만 소스 세이프 2005 에 접속할 수 있었던 사실은 인정할 수 있다.

그러나 앞서 든 증거들 빛 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사정 들, 즉 ① 공통 소스 및 각 업무 소스 파일에 대하여 피고 C 등이 원고에 재직 할 당시 **영업 비밀 표시 또는 비밀 등급 표시가 된 적이 없는 점,** ② 원고가 설립 된 2008. 12. 5. 이후 Lol 솔루션 사업부의 부장으로서 보안 관리 책임을 담당하게 된 2010. 10. 경까지 2 년에 가까운 기간 동안 위 각 소스 파일에 대한 보안 유지 업무가 특정 책임자의 관리 아래 수행되지 않은 점, ③ 피고 F가 소속되어 있던 ss 팀은 위 소스를 다른 자료들과 함께 ss 팀의 공용 서버에있는 공용 폴더에 저장해두고 팀 원들이 필요에 따라 업무에 사용 하였는데, 그 팀원들은 소스 세이프 2005에 접속하 는 방식과 달리 하나의 아이디와 비밀 번호를 공동으로 사용하여 위 공용 서버에 접 근 해 저장된 자료를 사용해 왔던 점, ④ 실제로 피고 F도 퇴사 무렵 소스 세이프 2005가 아닌 위 공용 폴더에 있던 공통 소스와 업무 소스를 다른 자료와 함께 자신 의 외장하드에 복사하여 나왔던 점 등에 비추어 보면, 위 공통소스 및 각 업무 소스 파일이 객관적으로 비밀로 유지, 관리되고 있다는 사실이 인식 가능한 상태에 있었다 고 인정하기에 부족하다.

결국 영업비밀 보유자의 입장에서 기술정보 또는 경영정보의 등급을 분류하는 것은 그 자체가 목적이 되는 것이 아니라, 이를 통해 해당 정보에 접근하는 자가 객관적으로 그것이 영업비밀로 관리되고 있음을 인식할 수 있게 만들기 위한 조치이기 때문에 의미가 있는 것이며, 앞서 본 판례에서와 같이 일반적·추상적 보호 조치만으로는 비밀관리성을 인정받지 못할 수 있기 때문에 중요하다고 할 수 있다.

나아가 영업비밀에 해당하는 기술정보나 경영정보를 누구에게도 알려주지 않아도 된다면 등급 분류는 더더욱 필요성이 적을 것이나, 기업 내에서 공유하고 활용해야 할 정보를 모두 영업비밀로 정하는 경우에는 업무 효율성이 심각하게 저해될 것이라는 점에서도 적정한 등급 분류가 필요한 이유라 할 수 있다.

특히, 영업비밀 침해 사건에 있어서 영업비밀 보유자는 영업비밀을 구체적으로 특정해야 한다는 점에서도 영어비밀에 해당하는 정보의 등급 분류는 매우 중요한 의미를 가진다.

대법원 2013. 8. 22. 자 2011마1624 결정

'영업비밀 침해행위의 금지를 구함에 있어서는 법원의 심리와 상대방의 방어권 행사에 지장이 없도록 그 비밀성을 잃지 않는 한도에서 가능한 한 영업비밀을 구체적으로 특정하여야 하고, 어느 정도로 영업비밀을 특정하여야 하는지는 영업비밀로 주장된 개별 정보의 내용과 성질, 관련 분야에서 공지된 정보의 내용, 영업비밀 침해행위의 구체적 태양과 금지청구의 내용, 영업비밀 보유자와 상대방 사이의 관계 등 여러 사정을 고려하여 판단하여야 한다.

1.2 영업비밀 등급 분류 기준

영업비밀은 기술상 또는 경영상 정보로서 문서나 도면, 장치 등의 유형물로 존재하는 경우도 있으나 대부분의 경우는 디지털 파일 등 무형적인 형태로 존재하고, 정보의 특성상 그 가치가 고정되어 있기 보다는 상황에 따라, 누가, 언제 그 정보를 활용하는가에 따라 가치가 상대적인 경우가 많기 때문에, 어떤 기준에 의해서든 정확한 등급을 분류한다는 것은 매우 어려운 일일 수밖에 없다.

1.2.1 영업비밀 지정 기준(특허청, 2012)

[표 33] 영업비밀 지정 기준(2012)

<table>
<tr><th colspan="2">등급분류(금액)</th><th colspan="2">비밀 여부(등급)</th><th>분류 기준</th></tr>
<tr><td rowspan="10">비용 및 노력의 투입정도 / 유출시 피해정도</td><td>10</td><td rowspan="7">영업비밀</td><td>1급</td><td rowspan="2">- 유출 시 회사의 존망이 우려되는 정보
- 새로운 경쟁자를 발생시키는 정보
- 회사에 직접적으로 상당한 매출을 발생시키는 핵심 정보</td></tr>
<tr><td>9</td></tr>
<tr><td>8</td><td rowspan="3">2급</td><td rowspan="3">- 유출 시 매출 및 고객과의 관계, 기술개발 지연 등의 피해가 예상되는 정보
* 영업부 (예시: 고객비밀정보, 컨설팅 산출물)
* 솔루션 사업부 (예시: 고객비밀 정보, 프로젝트 산출물)
* 연구소 (예시: 개발소프트웨어 소스코드, 개발설계서)
* 경영기획팀 (예시 : 회사경영정보, 회사정보, 인사정보)</td></tr>
<tr><td>7</td></tr>
<tr><td>6</td></tr>
<tr><td>5</td><td rowspan="2">3급</td><td rowspan="2">- 일시적으로 회사 업무 추진에 장애를 주거나 경쟁자에게 유리한 정보
- 회사 임직원에게만 한정적으로 공개되는 정보</td></tr>
<tr><td>4</td></tr>
<tr><td>3</td><td colspan="2" rowspan="3">일반문서</td><td rowspan="3">- 정보의 취득이나 개발을 위해 특별한 비용이나 노력이 투입되지 않은 정보
- 유출 시 손실 비용을 무시할 정도로 사소한 정보
- 공지되어 널리 알려져 비밀이 아닌 것
- 간행물 등 매체에 실린 정보, 판매 제품을 분해하여 쉽게 획득할 수 있는 정보</td></tr>
<tr><td>2</td></tr>
<tr><td>1</td></tr>
</table>

1.2.2 영업비밀 등급 분류 가이드(특허청, 2016)

[표 34] 영업비밀 등급 분류 가이드(2016)

평가 항목		평가 내용	배점	점수	총점	등급
창출 및 유지 비용		해당 정보를 개발하고 유지하기 위해 투입한 인력, 시간, 자금 등을 전체적으로 산정하여 평가 (예) 전체 매출액 대비 해당 연구개발 투자비 비중	10	상(10), 중(6), 하(1) 중 택 1(A)	자체 분류	특급 (Confidential)
산출 정보 수준		산출된 정보의 품질과 수준(정확성, 신규정, 사용용이성 등)을 평가 (예) 해당 분야 경쟁업체와의 상대적 기술수준 격차	15	상(15), 중(9), 하(3) 중 택 1(B)	75점 이상	1등급 비밀 (Restricted)
정보 활용도 (공유 정도)		해당 정보에 대한 활용빈도와 범위를 평가 (예) 해당 기술이 적용된 제품 수	10	상(10), 중(6), 하(1) 중 택 1(C)	50점 이상	2등급 비밀 (Internal Use)
정보 활용 파급 효과	내부 활용 효과	해당 정보가 기업의 가치(수익) 창출에 기여한 정도 (예) 기업 전체 매출액 대비 해당 정보의 기여도	35	상(35), 중(21), 하(7) 중 택 1(D)	50점 미만	3등급 공개 (Public)
	외부 유출 위험	정보 유출로 인해 예상되는 영업 손실 가능성을 평가 (예) 정보 유출로 기업에 발생하는 매출 감소액	30	상(3), 중(18), 하(6) 중 택 1(E)		

1.3 기타 등급 분류 기준

1.3.1 정보자산 관리 기준

한국정보통신기술협회에서 제시한 '조직의 정보보호를 위한 자산 관리 지침'(2010, 이하 '지침'이라 함)을 참고하여 정보(지침에서는 서버 및 PC와 같은 물리적 자산을 포함한 각종 디지털 정보 및 데이터 등을 포함한다고 하고 있다.)보호 관점에서 보호해야 할 자산에 대하여 어떻게 정의하고, 어떠한 기준으로 보호조치 방안을 제시하고 있는지 참고해볼 수 있다.

해당 지침에서는 '자산'이란 정보(데이터), 소프트웨어(컴퓨터 소프트웨어 등), 물리적 자산(서버 등), 서비스, 인력 등 조직에서 보유하고 있는 가치가 이는 모든 것을 말한다고 정의하고 있다. 이러한 자산을 관리할 때는, 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 등 정보보호 요구사항을 충분히 고려해야 한다고 하고 있는데, 각각의 개념은 다음과 같이 정리해볼 수 있다.

용어	개념
기밀성	자산이 유출 또는 외부에 공개 되었을 경우 업무에 미치는 영향
무결성	자산이 변조되었을 경우 업무에 미치는 영향
가용성	자산을 사용/이용할 수 없을 경우 업무에 미치는 영향

자산의 중요도는 각 평가요소(C, I, A) 별로 1~3점을 부여하며, 해당 자산의 최종 중요도 값의 범위는 3~9점에 해당하게 된다.

구분	무결성(I)	L(1)			M(2)			H(3)		
	가용성(A)	L(1)	M(2)	H(3)	L(1)	M(2)	H(3)	L(1)	M(2)	H(3)
기밀성(C)	L(1)	3	4	5	4	5	6	5	6	7
	M(2)	4	5	6	5	6	7	6	7	8
	H(3)	5	6	7	6	7	8	7	8	9

다만, 유형자산과 무형자산을 모두 포함하는 '정보 자산'의 분류 방식 기준을 영업비밀 등급 분류에 그대로 적용하기에는 한계가 있을 수 있다.

1.3.2 기술(가치)평가 기준

이 외에, 기술(가치)평가 방법에서의 등급(혹은 중요도) 산정 방법(혹은 기준)을 참고해볼 수 있을 것이다.

특허 등급 평가의 경우, 권리성, 기술성, 활용성을 평가지표로 삼고 있으며(한국발명진흥회, 특허분석평가시스템) 각각의 개념과 배점 비율은 다음과 같다.

용어	개념
권리성(35점)	제 3자와의 특허분쟁에서 독점배타적 지위를 유지할 수 있는 정도
기술성(35점)	기술동향과 부합하거나 선도하는 정도
활용성(30점)	비즈니스에 활용되는 정도 및 활용 가능성

'기술가치 평가 기준'(한국기업·기술가치평가협회, 2012)은 다음과 같은 기준을 제시하고 있다.

대항목	중항목	중항목 설명
Ⅰ.기술요인(기술성)	기술의 혁신성	기술 자체의 속성
	기술의 환경성	다른 기술/인프라와의 관계
	기술의 사회성	기술 관련 법사회문화적 문제
Ⅱ.시장요인(시장성)	시장환경요인	정치 경제 사회 등 시장외적 문제
	상품/산업 특성	상품 산업 등 공급자 특성
	시장특성	수요측 요인
	경쟁특성	산업과 시장에서의 경쟁특성
Ⅲ.기업요인(사업성)	전략요인	다른 기술, 상품, 산업 보완 여부
	기술개발력	기술인력, 조직과 능력
	생산력	공정기술, 투입요소, 시설 등
	재무구조	자본구조, 일반재무구조
	유통 및 마케팅능력	유통 물류, 마케팅 역량과 노력
	기타	기타 기업 내 요인
Ⅳ.수익성	수익 및 비용 구조	수익구조, 비용구조
	수익의 속성	수익의 성장성, 안정성
Ⅴ.경영(역량)요인	경영자	경영자의 기업가정신, 능력 등
	핵심전문인력	기술 영업 관리 등의 핵심인력

다만, 이러한 방법론 역시 기업이 보유한 방대한 정보 또는 영업비밀의 등급 분류에 그대로 적용하는데는 현실적 한계가 있다는 점은 유의할 필요가 있다.

2. 중소기업을 위한 영업비밀 등급 분류 체계

2.1 유형별 영업비밀 등급 분류 체계

기업이 보유하고 있는 영업비밀 정보를 유형/종류별로 등급을 미리 특정하여 임직원에게 제시하는 방법으로, 등급분류에 따른 업무 부담이 경감되는 장점이 있으며, 영업비밀 보호관리 체계 구축 시작 단계의 소규모 기업에 적합하다.

아래 정보별 등급은 영업비밀보호센터 제공 '영업비밀 등급 자가 확인 서비스'에서 제시된 내용과 영업비밀 판례 분석 결과, 영업비밀 실태 진단 및 보호관리 체계 구축 컨설팅 경험을 종합하여 일반화한 것으로, 일부 정보는 기업 실정에 맞게 조정하는 것이 바람직할 것이다(예를 들어, 서비스 업종의 경우 '고객정보'의 중요성이 높으므로, 이를 1등급으로 변경).

[표 35] 영업비밀 정보 유형별 등급 분류

구분		해당 정보	등급*
영업비밀	기술정보	**(연구개발)** 신제품/기술 개발 계획, 연구개발 보고서, 연구결과물 활용 계획서, 실험데이터, 연구노트, 노하우, 출원 전 특허정보, 프로토타입/시제품	1등급
		(생산/품질 관리) 제품/설비/장치의 도면, 제조 방법(성분비율, 배합방법/비율 등), 소스코드, 회로도, 공정설계도, 신규 투자 계획, 작업지시/표준서/시방서	1등급
	경영정보	**(고객 정보)** 고객/거래처 정보(성명, 연락처, 거래 이력, 특성, 단가 등)	2등급
		(영업 정보) 시장조사서, 마케팅 기획서, 실적 보고서, 제품/공사 단가, 원가 정보	2등급
		(관리 정보) 구매규격서/양식, 수주 및 납품 현황, 설비 보유/가동 현황, 생산/재고 현황 정보, 인사 정보(근태, 입사, 휴직, 퇴사 등), 회의록, 사규, 업무매뉴얼, 발주 정보, 시스템 정보, 대리점 현황	3등급
일반 정보		**(공개 정보)** 홍보 자료, 기업/제품 소개 자료, 교육 계획, 복리 후생 정보, 경영 공시 정보, 홈페이지 게시 정보, 입찰 정보, 발표 자료, 입찰 제안서(공개), 소비자 매뉴얼, 채용 정보, 특허 등록 정보	없음

2.2 약식 영업비밀 등급 분류 체계

기존 영업비밀 등급 분류 가이드(특허청, 2016)에서 제시하는 기준 중 가장 핵심적인 요소라고 할 수 있는 '정보 활용 파급 효과' 중심으로 해당 정보의 생성자 또는 보유자가 점수를 부여하거나 3점 또는 5점 척도에 따라 결정하는 방법이다.

[표 36] 약식 영업비밀 등급 분류

구분		내부 활용 효과	외부 유출 위험
기준		해당 정보가 기업의 가치(수익) 창출에 기여한 정도 (예) 기업 전체 매출액 대비 해당 정보의 기여도	정보 유출로 인해 예상되는 영업 손실 가능성을 평가 (예) 정보 유출로 기업에 발생하는 매출 감소액
배점방식	배점	50점	50점
	등급	1등급 (80~100점) / 2등급 (50~80점) / 3등급 (50점 미만)	
척도방식	3점	(기업 수익 창출 기여도) 크다 - 보통이다 - 적다	(유출 시 손실 규모) 크다 - 보통이다 - 적다
	5점	매우 크다 - 크다 - 보통이다 - 적다 - 매우 적다	매우 크다 - 크다 - 보통이다 - 적다 - 매우 적다

이러한 방법은 기준이 간단하고, 척도 방식에 의할 경우 직관적이고 신속한 판단이 가능한 장점이 있으며, 기업의 사정이나 해당 정보의 내용을 잘 아는 대표자나 임원, 관리자가 직접 등급분류를 하는 경우에 적합하다. 다만, 평가자에 따라 편차가 클 수 있으므로 주의를 요한다.

2.3 영업비밀 정의 기반 등급 분류 체계

영업비밀의 법적 정의에 따라 3가지 보호 요건별로 각 0~2점 사이의 값을 부여한 후, 이를 곱한 결과값을 기준으로 영업비밀의 등급을 분류하는 방식으로, 한 가지 요소라도 값이 0이면 영업비밀이 될 수 없다.

기존의 등급 분류 기준이나 방법이 주로 위험성이나 가치 등 정성적인 기준을 통해 평가한 값을 합산하는 방식이었기 때문에, 이미 공연히 알려진 정보라고 하더라도 그 정보를 취득하는데 비용이 많이 들었다거나 가치가 크다면 높은 등급이 유지될 수 있는데 반해, 이 방식에 의하면 '비공지성'의 값이 0이기 때문에 다른 요소는 고려할 필요도 없이 영업비밀에서 제외된다는 점에서 효율적일 수 있다.

[표 37] 영업비밀 정의 기반 등급 분류

공식	구분	배점	설명	예시
S × V × M 결과값 0 = 일반정보 1, 2 = 2급 4, 8 = 1급 --- 0= 일반정보 1, 2= 대외비 4= 비밀 8= 극비	비공지성 Secrecy	0	불특정 다수에게 공개된 정보	인터넷 검색 결과, 신문기사, 출판/간행물 학위논문, 특허 공보 등
		1	통상적인 방법으로 입수하기 어려운 정보	조사 보고서, 계약서, 제안서, 계획서 등
		2	보유자를 통하지 않으면 알 수 없는 정보	연구개발 결과, 제품/공정 정보, 투자계획 등
	경제적 유용성 Value	0	경제적 가치가 없는 정보	사내 회식/경조사 공지, 소모품 내역
		1	취득/개발에 비용 또는 노력이 투입된 정보	시장조사 보고서, 계약서, 사내 보고 문서
		2	상당한 비용 또는 노력이 투입된 정보	연구개발 성과, 소스코드, 도면, 고객정보
	비밀유지성 Manageability	0	비밀로 관리할 수 없거나 구성원이라면 모두 알아야 하는 정보	영업/홍보 자료, 특허 등록 정보, 신고/공개 의무 정보, 조직도, 업무분장, 연락처 등
		1	업무상 필요한 자에게만 공개하는 정보	실험 데이터, 특정 공정 노하우 등
		2	승인된 자에 한해 공개하는 정보	연구개발결과, 제품/공정 정보, 경영계획 등

예컨대, 전자 계측기를 제조하는 기업에서 기존 제품의 성능을 개선하기 위한 연구개발을 진행했다고 가정하면, 연구개발 목표와 범위를 설정하기 위해 이루어지는 선행 기술 조사를 통해 입수한 경쟁사의 특허 정보는 이미 공지된 것이기 때문에, 비공지성(S) 값이 0이 되므로 그 자체만으로도 영업비밀로 보호관리할 실익이 없다. 다음으로 선행기술조사 결과를 바탕으로 작성한 선행기술조사 보고서의 경우에는 대부분의 정보가 공지된 것이지만 특정한 기술 정보를 취합하여 정리한 것으로 비공지성 측면에서 '통상적인 방법으로 입수하기 어려운 정보'에 해당하며 값이 1이 되고, 연구개발 계획서의 경우에는 해당 문서를 작성한 담당자나 기업을 통하지 않고서는 알 수 없는 정보로서 비공지성(S) 값이 "2"가 된다.

비공지성(S) 값이 1 또는 2가 되는 정보의 경우, 다음 단계로 경제적 유용성(V)을 판단하게 되는데 정보의 경제적 가치는 여러 가지 기준에서 가치를 산정할 수 있으나 (대표적으로 기술가치평가에서 활용하는 수익접근법, 비용접근법, 시장접근법, 로열티 공제법 등이 있다), 이 기준은 그러한 전문성을 가지지 못한 임직원들에 의한 평가이므로 해당 정보를 작성하거나 취득하는데 소요된 비용을 기준으로 가치를 산정하게 된다. 따라서, 특허 데이터베이스 검색을 통해 비교적 용이하게 취득한 선행기술조사 보고서의 경우에는 V 값이 "1"이 되고, 상당 기간의 연구개발을 통해 완성한 연구개발결과 보고서는 V 값이 "2"가 된다.

다음으로, 비공지성과 경제적 유용성에서 모두 0이 아닌 값이 부여된 정보의 경우에는 비밀유지성(M) 값을 판단하게 된다. 영업비밀의 정의 또는 보호 요건에서 비밀관리성은 논리적으로 이미 영업비밀을 전제로 하는 것이기 때문에, 그 의미대로라면 어떤 정보가 영업비밀인지 여부를 판단하거나 등급을 분류하기 위한 기준으로 사용하기에 부적절하다. 따라서, 영업비밀 정의 기반 등급 분류 기준으로서 '비밀유지성(M)'은 어떤 정보를 비밀로 유지할 수 있는가 또는 해당 정보를 공유해야 할 범위가 어느 정도인가라는 의미로 사용한다. 앞서 예를 든 사례에서, 전자 계측기의 제조·판매를 위해 인증이나 허가를 받기 위해 또는 받는 과정에서 불가피하게 기술정보를 공개해야만 할 경우에는 M값이 "0"이 될 수 있다.

이 기준은 기업의 여건에 따라서 다양한 방식으로 변형할 수 있다. 예를 들어, 어떤 정보가 영업비밀에 해당하는지를 전혀 구분한 적이 없는 기업의 경우, 1단계 분류 작업으로서 비공지성(S) 값만을 기준으로 등급 분류를 할 수도 있다. 기업이 보유하고 있는 정보가 경제적 가치가 없는 경우는 드물고, 만약 경제적 가치가 전혀 없는

정보의 경우 해당 임직원이 직관적으로 알 수 있기 때문에, 경제적 유용성은 당연하다고 전제하고 '비공지성'만을 기준으로 등급 분류를 한 사례도 있다. 비슷한 경우로 경제적 유용성(V) 값만을 기준으로 등급 분류를 행할 수도 있음은 마찬가지이다.

이 기준은 법률상 영업비밀의 정의에 가장 부합하고, 비공지성을 기준으로 1차 등급 분류를 할 경우 상당한 정도의 정보를 등급분류 대상에서 제외할 수 있다는 점에서 효율적이며, 기존의 정성적인 판단 기준에 비해 상대적으로 간편하고 일관성 있는 판단이 가능하다는 장점이 있다.

2.4 영업비밀 등급 분류의 실무

적지 않은 경우 기업이 보유한 정보에 대해 영업비밀 등급을 분류하는 데는 많은 어려움이 존재하는데, 가장 큰 이유는 기업이 보유하고 있는 정보가 매우 방대하기 때문이고, 아주 예외적인 경우를 제외하고는 기업의 임직원 전체가 영업비밀 등급 분류 작업을 수행해야 하는데도 불구하고 그 의미나 필요성에 대한 인식 수준이 낮기 때문이다. 또한 기술적 한계로 인하여 아직까지는 보안 솔루션 등을 통해 정보를 자동 분류하는 것도 불완전하고, 비용 부담 문제가 있다.

따라서 실무적으로 영업비밀 등급 분류를 시행하기에 앞서 기업의 현황을 정확히 파악하고, 그 결과를 바탕으로 치밀한 준비가 필요하다. 아래 표는 일반적인 영업비밀 등급 분류 절차인데, 몇 가지 단계를 당연히 전제하고 있거나 생략되어 있기 때문에 실무적으로는 다소 변형이 불가피하다.

[표 38] 영업비밀 등급 분류의 절차[21)]

단계	구분	내용
1	**대상 식별**	• 기술정보 (연구개발 정보, 생산 제조 정보 등) • 경영정보 (인사/총무 정보, 회계/재무 정보, 구매/판매 정보)
2	**등급 산정**	• 평가 지수별 점수 합계 • 5개 평가 지수 : 정보 창출 및 유지 비용, 산출 정보 수준, 정보활용도, 내부 활용효과, 외부 유출 위험
3	**분류/표시**	• 특급 기밀 정보 (Confidential) • 1등급 비밀 정보 (Restricted)

21) 우리 기업의 영업비밀 등급분류 가이드, 특허청, 2016

		• 2등급 대외비 정보 (Internal Use) • 3등급 공개 정보 (Public)
4	**보호대책 수립/운영**	• 제도적 관리 : 영업비밀 구분, 관리 전담 인력 지정, 관련 규정 • 인적 관리 : 영업비밀 보호 의무 부과 및 고지, 관련 교육 실시 • 물리적 관리 : 영업비밀 개발, 보관 장소 지정, 접근/사용 권한 제한, 분쟁 대비 증거 확보

[표 39] 영업비밀 등급 분류의 실무상 절차(예)

단계	구분	내용
1	**현황 파악**	• 기업의 영업비밀 보호 관리 체계 및 인프라 • 최고 경영자의 의지 및 투입 가능한 자원(예산 및 인력) • 임직원의 영업비밀 보호에 대한 인식 수준
2	**대상 식별**	• 기술정보 (연구개발 정보, 생산 제조 정보 등) • 경영정보 (인사/총무 정보, 회계/재무 정보, 구매/판매 정보)
3	**TF 조직**	• 영업비밀 등급 분류 책임자 및 담당자 지정 • 영업비밀 등급 분류 기준 및 범위 협의 • 영업비밀 등급 분류 단계별 일정 수립 • 등급별 보호 관리 방안 수립
4	**관련 교육 또는 설명**	• 임직원 대상 영업비밀 등급 분류의 필요성 교육 • 영업비밀 등급 분류 기준 및 판단 방법 설명
5	**등급 산정**	• 등급 분류 실행 • 등급 분류 결과 취합 • GAP 분석 (등급분류 기준에 부합하는지, 특정 등급에 편중되어 있지 않은지 등을 확인)
6	**보호 관리**	• 등급별 표시 • 등급별 보호 관리 조치 시행
7	**모니터링 및 개선/보완**	• 업무 효율성 저해 사례 수집 • 등급 분류 조정 요청 사례 수집 및 분석 • 관련 규정 및 방침 위반 여부 감사 • 기존 등급 분류 체계 개선 사항 도출

Ⅴ. 주요 국가의 영업비밀 보호 체계 (비밀관리성을 중심으로)

1. 개요

미국, 유럽, 일본 등 주요 국가들 역시 영업비밀의 보호 요건으로 '비밀관리성'을 규정하고 있으며, 관련 법률 및 상세 규정은 다음과 같다.

[표 40] 주요 국가의 영업비밀 비밀관리성 관련 규정

미국	**Defend Trade Secrets Act § 1839 Definitions** the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if— (A) the owner thereof has taken **reasonable measures** to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information;
유럽 (EU)	**EU Trade Secrets Directive Article 2(1)** 'trade secret' means information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to **reasonable steps under the circumstances**, by the person lawfully in control of the information, to keep it secret;
일본	**〈不正競争防止法〉第二条** この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう
중국	**《反不正当竞争法》第九条** 本法所称的商业秘密，是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。
베트남	**Law on Intellectual Property Article 84.** Being kept secret by its owner with **necessary measures** so that it shall neither be disclosed nor easily accessible.

2. 국가별 규정 및 판례

2.1 일본

2.1.1 개요

일본은 〈부정경쟁방지법〉을 통하여 영업비밀을 보호하고 있으며, 목적이나 정의, 규율대상 등에 있어 우리나라와 대체로 유사하다.

기술정보 유출 사례가 증가하고 피해 규모도 점차 확대되면서, 일본에서는 기술 유출 위험이 심각하게 대두되었고, 영업비밀 보호강화를 정부의 지식재산 전략이자 나아가 국가 성장 전략의 중요한 요소라고 인식하게 되었다. 이에 따라 영업비밀 보호에 관한 제도의 검토, 종합적인 강화 시책 등이 제시되었고, 2015년에 이러한 내용이 반영된 부정경쟁방지법 개정안이 공포되었다.

우리나라와 일본의 영업비밀 보호제도 주요 내용을 비교해보면 다음과 같다[22].

항 목	**부정경쟁방지 및 영업비밀보호에 관한 법률** 법률 제13081호, 2015. 1. 28. 개정	**일본 부정경쟁방지법** 법률 제54호, 2015. 7. 1. 개정
영업비밀 침해죄 벌금형 상한	국내유출: - 5,000만원/재산상의 이득의 10배가 5,000만원 초과 시 이득액의 2배 이상 10배 이하 국외유출: - 1억 원/재산상의 이득의 10배가 1억원 초과 시 이득액의 2배 이상 10배 이하	국내유출: - 개인 2,000만 엔 - 법인 5억 엔 국외유출: - 개인 3,000만 엔 - 법인 10억 엔
영업비밀 전득자에 대한 처벌	영업비밀 침해 행위를 한 자 누구나 처벌 대상으로 함	부정하게 공개된 영업비밀임을 알고 그 영업비밀을 취득한 전득자의 부정한 공개·사용에 대해서도 처벌 대상으로 하고, 또한 전득자의 처벌을 양벌 규정의 대상으로도 함
영업비밀 침해품의 유통규제	별도의 규정 없음	기술상의 비밀을 사용하는 행위에 의해 발생한 물건(영업비밀 침해품)의 유통 규제를 도입

22) 일본 영업비밀보호법의 주요 개정내용 및 시사점, 한국지식재산연구원, 2015

친고죄 여부	2004년 법개정을 통해 침해죄를 비친고죄로 규정	2015년 법개정을 통해 침해죄를 비친고죄로 규정
미수범 처벌여부	2004년 법개정을 통해 미수범을 처벌토록 함	2015년 법개정을 통해 미수범을 처벌토록 함
몰수 규정	별도의 규정 없음	영업비밀 침해에 의해서 얻은 부정 수익을 임의적으로 몰수하는 규정을 신설
추정규정[23]	별도의 추정 규정 없음	합리적 경험 법칙의 범위 및 원고와 피고가 입증하는 부담의 공평성 등의 관점에서 일정한 조건(영업비밀의 범위, 피고의 주관, 추정이 미치는 대상 행위)하에 한정하고, 추정 규정 적용
제척기간	제척기간 10년 소멸시효 3년	제척기간 20년 소멸시효 3년

2.1.2 영업비밀의 정의

일본의 부정경쟁방지법 제 2조 6항은 “영업비밀이란 비밀로 관리되고 있는 생산방법, 판매방법 기타 사업 활동에 유용한 기술상 또는 영업상의 정보로 공연히 알려지지 아니한 것을 말한다.”고 규정하고 있는데, 우리나라와 대동소이하다.

2.1.3 비밀관리성 판단

일본 경제산업성은 기업이 영업비밀을 적절하게 관리할 수 있도록 2003년 1월 『영업비밀 관리지침(営業秘密管理指針)』을 책정·공표하였고, 동 지침에서는 사업자의 실태를 감안한 합리성이 있는 비밀관리방법으로 ① 영업비밀로 인정되기 위한 관리방법 및 ② 누설위험을 최소화하기 위한 고도의 관리방법을 제시하고 있으며, 2015년 전부개정을 통해 그 요건을 완화한 바 있다.

영업비밀 관리지침에서 제시하는 필요한 비밀관리조치의 정도는 다음과 같다.

23) 민사소송 절차에서 원고(피해자)가 피고(침해자)에 의해 영업비밀의 부정사용 입증 책임에 대한 부담을 경감하기 위해 원고가, (1) 피고가 생산 방법 또는 정령에 규정된 영업비밀(기술상의 비밀)을 부정 취득하고 있는 것과 (2) 피고가 해당 기술상의 비밀을 사용하는 행위에 의해서 발생하는 물건을 생산하고 있는지 또는 정령에 규정된 해당 기술상의 비밀을 사용한 것이 분명한 행위를 하는 것을 입증하면, 피고가 해당 영업비밀을 부정사용한 것으로 추정하는 규정

> 비밀관리성 요건이 충족되기 위해서는 영업비밀 보유기업의 비밀관리 의사가 비밀관리조치에 의해 직원 등에게 명확하게 제시되어 당해 의사에 대한 직원의 인식 가능성이 확보될 필요가 있다. 구체적으로 필요한 비밀관리조치의 내용·정도는 기업의 규모, 업태, 직원의 직무, 정보의 성질과 기타 사정의 여하에 따라 다르며 기업에서의 영업비밀 관리 단위(본 지침 13항 참조)는 직원이 이를 일반적이고 용이하게 인식할 수 있는 정도의 것으로 할 필요가 있다.

즉, 비밀관리성 요건을 충족하려면 영업비밀 보유 기업이 특정 정보를 비밀로서 관리하고자 하는 의사가 구체적 상황에 따라 경제적이고 합리적인 비밀관리조치에 의해 직원에게 명확하게 제시되어 결과적으로 직원이 당해 비밀관리 의사를 용이하게 인식할 수 있어야 한다는 것이다.

가. 대상자

비밀관리조치의 대상자는 직무 범위와 관계없이 당해 정보에 합법적이고 현실적으로 정보를 접할 수 있는 직원(예를 들어, 시건장치가 없는 서고를 열람할 수 있는 타 부서의 직원도 포함)이다.

나. 합리적 구분

비밀관리조치는 영업비밀 여부에 대한 합리적 구분과, 영업비밀 정보임을 밝히는 조치로 구분된다. 여기서 합리적 구분이란 정보의 성격, 기밀성의 중요도 등에 따라 영업비밀이 일반정보와 합리적으로 구분되는 것을 말하며, 정보가 구체화된 매체(예를 들어 출력물, 전자 파일)마다 영업비밀 여부를 표시할 것을 요구하는 것이 아니라, 기업에서 규모, 업태 등에 입각한 관리 방법에 맞게 영업비밀 정보 포함 여부를 직원이 판별할 수 있으면 된다.

다. 기타 비밀관리조치

합리적 구분 이외에 필요한 비밀관리조치로는 표시, 접근 제한, 영업비밀 정보의 종류·유형의 목록화 등을 꼽을 수 있다. 여기서는 비밀관리조치 대상자인 직원이 해당 정보가 비밀정보에 속하며 일반 정보와는 취급이 달라야 한다는 규범 의식이 생길 정도의 노력이여야 한다는 것이 중요하다.

비밀관리조치의 구체적인 내용이나 정도는 당해 영업비밀에 접근하는 직원 수, 업태, 직원의 직무, 정보의 성격, 사무실의 상황이나 기타 사정에 따라 당연히 달라지게 된다. 예를 들어 영업비밀에 합법적이고 현실적으로 접근하고 있는 직원이 소수인 경우, 상황에 따라서는 해당 직원들 간 구두에 의해 '비밀정보'로 확인하는 정도의 조치만으로 충분한 경우도 있을 것이다.

2.1.4 판례

일본 법원은 비밀관리성과 관련하여 다음과 같이 판시하고 있다.

기업 규모를 고려	비밀번호 등에 의한 접근 제한, 비밀이라는 표시 등이 없었음에도 불구하고 전체 직원수가 10명 정도인 특성상 정보에 대한 일상적인 접근을 제한할 수 없다는 점을 이유로 비밀관리성을 인정 (오사카 지방법원 판례 2013년 2월 27일 2001년 (ワ) 10308 호)
영업상의 필요성 고려	고객정보의 복사본을 상사 등에게 배포하거나 자택으로 반입하거나 수첩 등으로 관리하여 계약 후에도 파기하지 않았다고 하더라도 이들은 영업상의 필요성에 기초한 것으로서 직원은 본 건의 고객정보를 비밀이라고 용이하게 인식할 수 있도록 했다고 판단해 비밀관리성을 인정(지적재산 고등법원 판례 2012년 7월 4일 2011년 (ネ) 10084 호)
정보의 특성 고려	ＰＣ수지의 제조기술에 관한 정보는 세계적으로 드문 정보로서 제조에 관계한 직원은 당해 제조기술이 비밀이라고 인식하고 있었다고 판단해 비밀관리성을 인정 (지적재산 고등법원 판례 2011년 9월 27일 2010년 (ネ) 10039 호)
물리적 관리체제가 결여된 경우에도 비밀관리성 인정	염가로 판매해 지속적인 거래를 하고 있는 등의 지극히 효과적인 영업활동이 가능하다는 정보의 중요성과 정보가 공개되었던 것이 11명의 직원에 불과했다는 점과 더불어 피고가 퇴직하기 직전에 비밀유지서약서를 제출했다는 점 등의 사정을 감안해 비밀관리성을 인정 (오사카고등법원 판례 2008년 7월 18일 2008년 (ネ) 245 호)

이 외, 구체적 비밀관리조치와 관련한 일본 법원의 판시사항은 다음과 같다.

종이매체에 대한 비밀관리조치 및 관리성 인정	인재파견업을 하는 회사의 사원이 파견노동자의 고용계약에 관한 정보 등을 반출한 사례에 있어 당해 정보는 시건을 한 책장에의 보관이나 복사의 제한·회수, 비밀표시가 되어 있지 않았으나 사원과는 비밀유지계약 체결, 당해 정보의 관리에 관한 일반적인 주의환기 등의 사정을 감안해 비밀관리성을 인정 (도쿄지방법원 판례 200년 12월 26일 2000년 (ワ) 22457호)

전자매체에 대한 비밀관리조치 및 관리성 인정	정보가 들어있는 컴퓨터의 ID와 패스워드를 복수의 사원들이 공유하고 있으며 더욱이 ID와 패스워드를 포스트잇에 써서 붙여 놓아 퇴직자가 있어도 ID와 패스워드가 변경되지 않았다는 사안에 있어 ID나 패스워드의 취지가 유명무실화된 사정이 있다면 특히 그와 같은 사정이 인정되지 않는 한 비밀관리성을 인정하는데 지장을 주지 않는다고 판단해 비밀관리성을 인정 (오사카지방법원 판례 2008년 6월 12일 2006년 (ワ) 5172호)
	패스워드가 변경되지 않고 컴퓨터에 패스워드를 기재한 포스트잇을 붙인 자가 있었고 가격표 리스트를 인쇄한 것에 「대외비」 등의 날인을 하는 규정도 없었다는 사안에 있어 가격표 리스트에 기계 제조업자에게 있어 일반적으로 중요하다는 사실이 명백한 매입 원가 등의 정보가 기재되어 있었다는 점 등을 참작해 가격표 리스트의 외부 제시나 반출이 허용되었다는 사정은 인정하기 어렵다고 판단해 비밀관리성을 인정 (나고야지방법원 판례 2008년 3월 13일 2005년 (ワ) 3846호)
고객정보 관련 비밀관리성을 부정	이 사건의 고객정보는 고객 카드와 고객정보시스템이라는 2개의 방법에 의하여 관리되고 있던 바, 고객카드에는 그 표지등에 영업비밀인 취지의 표시가 없고, 이 사건 점포의 종업원이라면 누구든지 볼 수 있는 상태로 보관되고 있었고, 고객관리시스템은 이 사건 점포의 종업원이면 비밀번호 등을 이용하지 않고도 누구든지 고객정보를 열람할 수 있었음. 이러한 가운데, 피고가 원고에 재직할 당시에, 비밀유지의무를 부과하는 정보관리규정도 존재하지 않았다는 점에서, 이 사건 점포의 고객정보가 정보의 이용자인 종업원에게 비밀이라고 인식할 수 있을 정도로 관리되고 있었다고 인정하기 어려운 점에서, 영업비밀 해당성과 이에 따른 부정취득행위를 인정하지 않고 관련 청구를 기각함 (도쿄지방법원 판례 2016년 2월 15일 선고 2015년 (ワ) 17362호)

2.2 중국

2.2.1 개요

중국의 영업비밀은 우리나라의 부정경쟁방지법과 유사한 『반부정당경쟁법』에서 '상업비밀(商业秘密)'이라는 명칭으로 보호하고 있으며(이하 '영업비밀'이라 함), 보호 요건 등에 있어 기본적으로 한국의 제도와 크게 다르지 않다.

반부정당경쟁법 제9조는 "영업비밀이란 공중에 알려지지 아니하고, 상업적 가치가 있으며, 그 권리자가 비밀보호조치를 취한 기술정보와 경영정보 등 상업 정보[24]를 말한다."고 규정하고 있다.

중국과 한국의 영업비밀 정의 및 성립 요건을 비교해보면 다음과 같다

24) 개정 전 법 제9조 제3항은 "기술정보 및 경영정보"만을 규정하고 있었으나, 2019년 개정을 통해 "기술정보, 경영정보 등 상업정보"로 수정되었다.

중국 〈반부정당경쟁법〉 제9조	한국 〈부정경쟁방지법〉 제2조 제2호
비공지성(不为公众所知悉)	비공지성
상업적 가치(商业价值)	경제적 유용성
비밀보호조치(权利人采取保密措施)	비밀관리성
기술정보(技术信息), 경영정보(经营信息) 등 상업정보(商业信息)	생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보

중국의 반부정당경쟁법은 1993년 제정된 이래 2017년 1차 전면적 개정(修订)에 이어 2019년 영업비밀 제도 위주의 개정(修正)이 이루어진 바 있다. 17년 개정에서는 1) 영업비밀 개념의 명확화, 2) 영업비밀 침해유형 확대 및 책임 범위 조정 등이 이루어 졌고, 19년의 개정은 1) 손해로 인정된 금액의 5배까지 배상액을 정할 수 있도록 하는 징벌적 손해배상제도 도입, 2) 영업비밀 침해행위에 대한 피해자의 입증책임 완화, 3) 영업비밀 침해유형 및 침해주체 확대를 주요 개정 내용으로 한다.

2.2.2 비밀관리성 판단

최고인민법원의 사법해석[25] 제 11조 제1항 내지 제3항에서는 '비밀보호조치'란 권리자가 정보의 누출을 방지하기 위해 채택한 합리적인 보호 조치를 의미한다고 하고 있으며, 비밀보호조치를 취했는지 여부는 정보 저장 장치의 특성, 권리자가 비밀보호를 원하는 의사, 비밀보호조치의 식별 가능 정도, 타인이 정당한 방식으로 비밀보호의 난이도를 알아낸 행위 등의 요소에 근거하여 판단하고, 아래와 같은 조치를 취하여 일반적인 상황에서 정보의 누출을 방지할 수 있다면 비밀보호조치가 취해진 것으로 본다.

25) <최고인민법원의 부정경쟁행위 민사안건 심리에 대한 법률적용에 관한 몇 가지 문제의 해석>(《最高人民法院关于审理不正当竞争民事案件应用法律若干问题的解释》, 法释〔2007〕2号 2007년 1월 12일)

① 비밀정보를 지득하는 범위를 제한하고, 필수적으로 알아야 할 관련인에게만 내용을 공지하는 경우
② 비밀정보 저장매체에 대해 잠금장치 등의 조치를 하는 경우
③ 비밀정보의 매체상에 비밀표지를 표시하는 경우
④ 비밀정보에 비밀번호 또는 코드 등을 적용한 경우
⑤ 비밀보호약정을 체결한 경우
⑥ 비밀기구, 공방, 차량 등 장소에 내방자를 제한하거나 비밀 보호 요구를 하는 경우
⑦ 비밀정보를 보호하기 위하여 기타 합리적 조치를 취한 경우

이 외, 중국 공상국 영업비밀 규정[26] 제2조 제4항에서는 "권리자가 비밀보호조치를 취한다 함은, 비밀보호협의를 체결하거나, 비밀보호 제도 및 기타 합리적인 비밀보호 조치를 마련하는 것을 포함한다."고 규정하고 있다.

2.2.3 판례

법원은 일반적으로 영업비밀 권리자가 영업비밀이 존재한다는 것을 알거나 또는 당연히 알고 있는 그 종업원 또는 업무 관련 제3자에게 서면으로 비밀보호 의무를 부과하였는지를 중심으로 합리적 비밀보호 조치를 하였는지를 판단하고 있다.[27]

'비밀보호조치'로 인정되는 요건에 대하여, 최고인민법원은 판례[28]를 통해 1) 권리자의 비밀 보호에 대한 주관적 의도가 드러나야 하고, 2) 권리자가 실시한 보호조치가 객관적인 식별성[29]을 가져야 하며, 3) 정상적인 상황에서 관련 정보가 유출되는 것을 충분히 방지해야 한다고 설시하고 있다.

결국, 비밀보호조치가 취해졌는지 여부는 권리자와 침해자의 관계 및 구체적인 정황을 바탕으로 판단하게 된다고 할 것이다.

---

26) 정식 명칭은 <영업비밀 침해행위 금지에 관한 약간의 규정>(《关于禁止侵犯商业秘密行为的若干规定》) 으로, 공상행정관리국의 행정명령이다. (工商行政管理局令第41号, 1995년 11월 23일)
27) 광동성 고급인민법원 (1997)奥知终字第53号, 최고인민법원 (2012)民监字第253号, 최고인민법원 (2000) 知终字 第3号, 중국 광동성 선전시 중급인민법원 (2014) 深中法知民终字 第30号 등 다수
28) 最高人民法院 (2011) 民申字第122号民事判决书
29) 보호조치의 식별성이란, 영업비밀을 주장하는 권리자가 영업비밀의 내용범위를 명확히 확정하고 그 범위를 객관적인 매개체를 통하여 나타나게 하여, 보호의무를 가지는 사람이 보호의 대상이 되는 정보가 무엇이고, 권리자가 그 정보를 영업비밀로 분류하여 보호하고 있다는 점을 식별하게 하기에 충분한 것을 의미한다. (孔祥俊 主编 , 商业秘密司法保护实务 , 中国法律出版社 , 2012)

비밀관리성을 인정한 판례	피고가 원고 회사 내 어떠한 정보가 영업비밀에 속하는지 알았을 것이고 회사의 이익을 보호하기 위하여 반드시 적당한 비밀보호조치를 취해야 하는 필요성 또한 알고 있었을 것이라는 등의 이유로, 원고 회사의 비밀보호조치를 엄격하게 판단할 것은 아니고, 영업비밀 관리자였던 피고가 원고 회사가 비밀보호조치를 취하지 않았다고 항변하는 것은 신의성실의 원칙에 반한다고 판시(江苏省高级人民法院(2006)苏民三终字第00789号 民事判决书)
비밀관리성을 부정한 판례	원고가 영업비밀임을 주장하는 교습 방식 및 자료에 대하여 합리적이고 유효한 비밀보호조치를 취하지 않았고, 그 내용은 공중의 영역에 속하는 것이거나, 서적, 무료 청강, 온라인 등의 경로를 통해 이미 공개되었으므로 영업비밀로 보호될 수 없고, 고객명단의 경우에도 장기적이고 안정적인 거래관계를 형성하였다는 점을 증명할 수 없어 역시 영업비밀로써 보호될 수 없다고 판시((2014) 浦民三 (知) 初字第1045号(1심), (2015) 沪知民终字第643号(2심))

2.3 미국

2.3.1 개요

미국은 2016년 오바마 대통령이 서명한 〈영업비밀보호법(Defend Trade Secret Act, 이하 DTSA))〉가 법률로 확정되어 시행(Law No. 114-153)됨에 따라, 종래 개별 주(州)에서 다루어지던[30] 영업비밀 관련 사건을 연방 법원에서도 다루게 되었다.

DTSA는 미연방 형사법(US Code Title 18 : Crimes and Criminal Procedure)에 영업비밀 침해에 대한 형사적 제재 규정을 추가한 것으로, 이 법이 기존의 주(州)법에 우선하는 것은 아니므로, 영업비밀 보유자는 선택에 따라 여전히 개별 주(州)의 법률에 따라 영업비밀을 보호할 수도 있다(단, 내부고발자에 대한 면책 조항은 주법에 우선함).

30) 종래 미국에서 영업비밀 보호는 주로 "통일영업비밀법Uniform Trade Secret Act)에 기초하여 각 주(州)별로 별도의 영업비밀 관련 법령이 적용되었는데, 캘리포니아, 텍사스 등 일부 주(州)를 제외하고는 영업비밀 보호를 민사적 구제 수단으로 한정하고 있었다. 연방 차원에서는 "경제스파이법(Exonomic Espionage Act)가 있었고, 여기에서 영업비밀 침해에 대한 형사상 처벌 규정을 마련하고 있었다.

DTSA의 시행으로 인해 '영업비밀 절도(Theft of trade secret)' 행위에 대한 처벌이 강화되었으며(500만 달러 또는 침해로 취득한 이익의 3배 중 더 큰 금액을 초과하지 않는 금액을 벌금으로 부과), 내부 고발자에 대한 면책, 소송절차에서의 영업비밀 유지를 위한 조치가 강화되었고, 연방법원에서의 압류명령·금지명령·손해배상 등 민사 구제 수단을 신설하였다.

2.3.2 영업비밀(Trade Secret)의 정의

미국의 영업비밀 보호 관련 법체계는 '통일영업비밀법(Uniform Trade Secrets Act, 이하 UTSA)'과 '경제스파이법(Economic Espionage Act, 이하 EEA)', 그리고 2016년 시행된 '영업비밀보호법(Defend Trade Secrets Act)' 등으로 구성된다. UTSA와 DTSA에서 규정하고 있는 영업비밀 정의를 살펴보면 다음과 같다.

UTSA[31]	DTSA
제1조 정의 동법에 사용되는 용어는 문맥상 달리 요구되지 않는 한 다음을 뜻한다. (4) 영업비밀은 공식, 패턴, 편집물, 프로그램, 도안, 방법, 기술 또는 과정을 포함한 정보로서 다음의 요건을 갖춘 것을 의미한다. (i) 현실적 또는 잠재적으로 독립된 경제적 가치를 가지고 있으며, 일반적으로 알려져 있지 않고, 그 공개 또는 이용으로부터 경제적 가치를 얻을 수 있는 타인이 정당한 수단에 의해 쉽게 알아볼 수 없고, (ii) 비밀유지를 위하여 상황에 따른 합리적인 노력을 하여야 한다.	**§ 1839. 정의** 동법에 사용되는 용어는 다음을 뜻한다. (3) 영업비밀은 패턴, 계획, 편집물, 프로그램 장치, 공식, 디자인, 도안, 방법, 원형, 방법, 기술, 과정, 절차, 프로그램, 또는 코드를 포함한 모든 형태와 유형의 재정적, 상업적, 과학적, 기술적, 경제적 또는 공학적 정보로서 그 정보가 유형물이든 무체물이든, 어떠한 물리적, 전자적, 그래픽적, 사진적, 서면적 방식으로 저장, 편집, 기억되었는지는 불문한다. (A) 영업비밀의 보유자는 비밀 정보를 유지하기 위하여 적절한 조치를 취하여야 하고, (B) 그 정보가 현실적 또는 잠재적으로 독립된 경제적 가치를 가지고 있고, 일반적으로 알려져 있지 않으며, 공중이 적절한 수단에 의하여 쉽게 알아볼 수 없어야 한다.

31) SECTION 1. DEFINITIONS. As used in this [Act], unless the context requires otherwise:
(4) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
(i) derives independent economic value, actual or potential, from not being generally known to,

미국 연방법이나 주(州)법에 따라 어떠한 정보가 “영업비밀”로서의 요건을 충족하는지 여부는 배심원이 결정하는 사실관계의 문제로서, 다음 6가지의 요소를 고려하여 판단하는 것이 일반적이다.

① 회사 외부에 그 정보가 알려져 있는 정도
② 회사 내부의 고용인 등이 그 정보를 알고 있는 정도
③ 그 정보의 비밀을 지키기 위해 그 회사가 택한 수단의 정도
④ 그 회사와 경쟁업체에 있어 그 정보의 가치
⑤ 그 정보를 발전시키는 데 있어 그 회사가 투자한 노력이나 비용의 양
⑥ 타인이 그 정보를 제대로 획득하거나 복제하는 것의 난이도

2.3.3 비밀관리성 판단

비밀관리조치가 ‘합리적인’ 수준인지 여부에 대해 법원은 다음과 같은 요소를 포함하여 다양한 사정을 종합적으로 고려한다.

- (접근 제한) Restricting access to the information (e.g., locking it away in a secure place such as a vault or via computer or network security);
- (인원 제한) Limiting the number of people who know the information;
- (서약/계약) Having the people who know, or who come into contact with the trade secret, directly or indirectly, agree in writing not to disclose the information (e.g.,sign non-disclosure agreements (in the case of third parties) or confidentiality or employment agreements (in the case of employees and consultants/contractors)); and/or
- (비밀 표시) Marking any written material pertaining to the trade secret as confidential and proprietary and following up (as practical) in writing if verbal disclosure.

---

and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

2.3.4 판례

합리적인 노력을 부정한 판례	원고의 공장 입구에는 일부 보안 요원이 배치되어 있었으나 다른 출입문에는 접근 제한 표시도 없었고 잠겨 있지 않았으며, 폐기된 모터 도면과 설계도는 파괴되지 않은 채 그대로 버려졌으며, 몇 개의 설계노트는 금고에 보관되었으나 모터 설계도는 금고에 보관되지 않았고, 원고의 종업원들에게 특정 정보가 영업비밀에 해당한다는 사실을 고지하지도 않았으며, 비밀표시도 없었고, 고객이나 판매상들에게 도면, 부속품들이 제한 없이 제공되었으며, 일반 대중에게 공장의 생산 공정을 공개하기도 하는 등, 원고는 비밀정보 문서에 대한 접근을 제한하기는 하였으나 모터 설계 기술의 비밀성을 유지하기 위한 합리적인 노력을 충분히 했다는 입증을 하지 못하였다는 이유로 원고의 정보가 영업비밀에 해당하지 않는다고 판시(미네소타 대법원 C7-81-894, C0-81-1188)
	종업원 교육 교본은 종업원들이 계속 소지하여 집으로 가지고 갈 수 있었고, 교본이 영업비밀에 해당한다고 종업원들에게 교육시키지 않았으며, 타인의 접근 예방을 위한 보안절차들을 종업원들에게 교육시키지 않았으므로, 교본들이 비밀성 유지를 위해 합리적 노력이 투여된 대상이 아니었다고 판시(미연방 제9순회 항소법원 94-36222)
합리적인 노력을 인정한 판례	원고들이 보호하고자 하는 설계의 특성들은 상당한 시간과 노력, 비용을 투자하여 얻은 것으로 독립적인 경제적 가치를 지니고, 비밀성을 유지하기 위하여 영업비밀임을 고지한 점, 선택적으로 정보접근을 가능케 한 점, 비밀유지약정 체결, 비밀의 금고 보관 등은 원고의 비밀성 유지를 위한 합리적인 노력으로 보이며, 마지막으로 해당 정보가 동종 업계의 종사자들이 쉽게 획득하거나 알려질 수 있는 것으로 보이지 않으므로, 이상을 종합하면 해당 정보는 영업비밀로 볼 수 있다고 판시(미연방 캘리포니아 남부지방법원 No. 09-CV-1301)
	피고는 원고의 직원으로서 원고의 이익만을 위해 행동할 의무가 있다는 점에 동의하고, 따라서 영업비밀 자료를 보호하기 위한 피고의 노력도 원고의 노력으로 간주되어야 하는데, 피고는 영업비밀 자료를 사물함에 자물쇠를 채워 보관하였고, 근무 시간 이후에는 집으로 들고 갔으며, 다른 종업원들에게 전체 데이터 복제를 허용하지 않았던 바, 법은 완전한 비밀성을 요하는 것이 아니라 법상 보호를 받기 위한 합리적인 보안 노력만 있으면 충분하며, 원고는 소규모 가족 소유의 사업체로써 작은 규모와 장기적인 고용관계 때문에 종업원들이 해당 영업비밀을 비밀로 유지할 것이라고 믿었다는 추론은 합리적이고, 피고 스스로 도입한 보안 수단들도 비밀 유지에 기여하였으므로, 원고가 데이터를 합리적으로 보호하지 못했다고 판단한 원심은 법적 오류를 범하였다고 판시(인디애나 항소법원 71A05-0402-CV-99)

2.4 베트남

2.4.1 개요

베트남에서는 지식재산권법(Law on Intellectual Property, 2005), 노동법(Labour Code, 2012), 공정경쟁법(Law on Competition, 2004) 등에서 영업비밀 관련 정의 규정 및 처벌규정 등을 두고 있으며, 2005년 제정된 지식재산권법 제4조 제23호[32]에 따르면 영업비밀이란 재정적 또는 지적 투자를 통하여 취득한 정보로 아직 공개되지 않고 사업에 이용 가능한 정보를 가리킨다.

2.4.2 비밀관리성

지식재산권법 제 84조에서는 1) 일반적 상식이거나 쉽게 얻을 수 없는 정보 2) 해당 정보를 사용하지 않거나 갖고 있지 않은 사람보다 (갖고 있는 사람이) 사업에 사용되었을 때 유리한 경우 3) 영업비밀 보유자가 해당 영업비밀이 공개되거나 쉽게 접근할 수 없도록 필요한 조치를 취하여 비밀을 유지한 경우[33]에 영업비밀로써 보호받을 수 있다고 규정하고 있다.

2.4.3 판례

베트남에서는 영업비밀 유출과 관련된 판례[34]와 경업금지 관련 판례[35]가 있기는 하나, 구체적으로 비밀관리성이 쟁점이 된 판례는 아직 없는 것으로 보인다.

---

32) Article 4.-Interpretation of terms
23. A trade secret means information obtained from activities of financial and/or intellectual investment, which has not yet been disclosed and can be used in business.

33) Article 84.-General conditions for business secrets eligible for protection A business secret shall be protected when it satisfies the following conditions:
1. Being neither common knowledge nor easily obtained;
2. Being capable, when being used in business activities, of rendering advantages to its holder over those who do not hold or use it;
3. Being kept secret by its owner with necessary measures so that it shall neither be disclosed nor easily accessible.

34) 회사 제품 정보를 여동생에게 이메일로 보낸 직원을 비밀유지의무 관련 내부 노동 규정을 위반하였다는 이유로 해고한 것이 타당한지 여부가 쟁점이 된 사안(Case No 20/LD-ST dated March 17 2005)

35) 경업금지 대상인 '경쟁업체'가 주기적으로 갱신되고, 피고용자가 약정 준수에 대한 아무런 대가도 받지 못함에도 불구하고 약정이 유효한지 여부가 문제된 사안(Case No 09/2010/LDST dated December 10 2010)

참고로 유럽연합(EU)에서 운영하고 있는 “South-East Asia IPR SME Helpdesk”에서 배포한 2016년 “Protecting Your Trade secrets in South-East Asia”에 따르면, 동남아시아 국가의 경우 상대적으로 영업비밀 보호 관련 법제가 미비한 상황이라고 하면서, 베트남의 경우 영업비밀은 별도의 등록 절차 없이 생성 시점부터 보호되는데, 단 해당 정보를 비밀로 유지하기 위한 합리적 조치(reasonable measures)를 취해야 한다고 설명하고 있다.

합리적 조치의 내용에 대해서는 일반적인 인적·물적·제도적 조치 등이 있고, 내용상 중복되므로 생략한다.

3. 정리

이상에서 살펴본 바와 같이, 미국, 일본, 중국 등 해외 주요국의 영업비밀 관련 규정은 구체적인 내용에 다소 차이가 있기는 하나, 영업비밀로 보호받기 위해서는 ‘비밀관리성’ 요건을 만족해야 한다는 점에서는 동일하다.

표현상 미국은 ‘합리적 조치(reasonable measures)’, 일본은 ‘비밀관리조치’, 중국은 ‘비밀유지조치’, 베트남은 ‘필요한 조치(necessary measures)’를 취할 것을 요구하고 있는 등의 차이가 있으나, 관련한 법령이나 지침, 사법해석, 판례 등을 종합해 볼 때, 해당 국가에서 영업비밀로 보호받기 위해 반드시 취해야 할 특별한 조치가 요구되지는 않는 것으로 보이며, 비밀관리(혹은 유지) 조치가 ‘합리적’인지 여부와 그 정도를 판단함에 있어 어떤 절대적인 기준이 존재하는 것은 아니고, 사안별로 기업 규모 등을 고려하여 종합적으로 판단하고 있다는 점에서도 동일하다.

요컨대, 비밀관리성을 인정(또는 부정)한 사례를 종합해 볼 때, 어떤 정보가 영업비밀인지 여부를 표시하고 비밀유지의무를 부과하는 방식으로 고지(인지)하거나 서약서를 징구하는 등을 종합적으로 고려한다는 점에서 우리나라와 크게 다르지 않다고 보여진다.

이는 영업비밀을 보호하는 법의 취지나 영업비밀을 보호함에 있어 '비밀관리성'이 요구되는 이유에 비추어 볼 때 당연한 결과라고 할 수 있다. 즉, 국가마다 영업비밀의 법적 정의나 보호 요건이 표현상 다소 차이가 있어도 실질적인 의미에서는 큰 차이를 보이지 않는 이유는, 근본적으로 입법 목적 자체에 큰 차이가 없는데다 영업비밀에 해당하는 정보를 법적으로 보호하기 위해서는 불가피하게 '비밀관리성'이 요구될 수 밖에 없기 때문인 것으로 생각된다.

영업비밀을 보호하는 목적은 "건전한 거래질서를 유지"하기 위한 것이라고 법률상 명문화되어 있고, 대법원도 "영업비밀 침해행위를 금지시키는 목적은 침해행위자가 그러한 침해행위에 의하여 공정한 경쟁자보다 우월한 위치에서 부당하게 이익을 취하지 못하도록 하고 영업비밀 보유자로 하여금 그러한 침해가 없었더라면 원래 있었을 위치로 되돌아갈 수 있게 하는 데에 있다."고 하여 같은 취지로 판시하고 있다. 나아가 '비밀관리성'이 요구되는 이유에 관해서도 법원은 정보의 자유로운 유통·거래와 종업원 등 정보를 취득한 제3자를 보호하기 위한 것이라는 점을 밝히고 있다[36].

의정부지방법원 2018. 1. 30. 선고 2017노2162 판결

영업비밀의 정의에 비밀관리성 요건을 두는 이유는, 어떤 정보가 영업비밀인지 아닌지를 객관적으로 인식시켜 영업비밀이 아닌 정보가 자유롭게 유통·거래 될 수 있도록 하고, 나아가 관리되지 않는 대부분의 정보를 영업비밀로 인정하게 되면 종업원들이 회사에서 근무하면서 다루거나 취득한 대부분의 정보를 영업비밀로 보게 되어 그 종업원들이 동종업체에 취업하거나 동종업체에서 직원들을 고용하는 행위가 대부분 회사의 영업비밀을 침해하는 것으로 취급될 우려가 있기 때문이다. 또한, 이 사건과 같이 영업비밀은 범죄의 구성요건이 되므로, 대상 정보가 영업비밀임을 종업원이 객관적으로 인식할 수 있는 정도로 영업비밀의 개념을 명확하게 할 필요성이 있다.

결국, 미국 등 주요 국가들의 법제에서도 알 수 있는 바와 같이 영업비밀 보호 요건으로서 '비밀관리성'은 관련 규정의 자구(字句)나 표현 차이에도 불구하고, 실제 적용에 있어서 매우 유사한 이유는 정보의 자유로운 유통이나 거래, 제3자의 이익 보호, 거래질서 유지 등과 같은 본질적인 목적이나 철학을 달리 하지 않는 이상 큰 차이를 보이기 어렵기 때문일 것이다.

36) 서울고등법원 2018. 10. 11. 선고 2018라20665 결정도 같은 취지임

Ⅵ. 결론

영업비밀의 중요성이 증대됨에 따라, 미국이나 EU, 중국, 일본 등 주요 국가들에서 영업비밀 보호 제도를 강화하고 있고, 정부도 부정경쟁방지 및 영업비밀 보호에 관한 법률의 개정을 통해 영업비밀의 보호 요건을 완화하고 침해행위에 대한 처벌 규정을 강화하는 등으로 영업비밀 보호 제도를 개선하기 위해 노력하고 있다.

그런데, 우리 기업의 실정을 보면 여전히 상당수의 중소기업이 영업비밀 보호 관리 역량의 미흡, 관련 정보의 부족 등으로 인해 영업비밀 보호·관리에 어려움을 겪고 있다. 특히, 기업의 규모나 업종에 따라 구체적으로 영업비밀에 해당하는 정보를 어떻게 보호·관리하는 것이 효과적인지에 관해 뚜렷한 기준이 마련되어 있지 않은 상황이다.

이 연구에서는 영업비밀 관련 판례의 분석을 통해 기업의 규모나 업종을 반영한 영업비밀 보호·관리 방법을 표준화하는 것과 영업비밀 보호 컨설팅 체계를 구축하는 것을 목표로 하였다. 영업비밀 관련 판례의 경우 2015년부터 2019년 상반기까지 선고된 영업비밀 관련 판결 총 1,596건 중 비밀관리성에 대한 구체적인 언급이 있는 사건 368건을 선별하여, 기술 분야별, 사건 유형별, 정보의 유형별로 법원이 어떤 사정을 고려하여 비밀관리성을 인정 또는 부정하는지를 조사하였으며, 기업의 규모나 업종 등의 특성을 고려할 경우 어떤 사정을 감안하는지를 살펴보았다.

기술 분야별로는 장비 설계도 등이 문제된 기계소재 분야 대비 소스코드 등이 문제된 전기전자, 정보통신 분야의 영업비밀 사건에서 접근 제한 등 물적 관리 조치를 취했는지 여부의 빈도가 조금 더 높게 나타났으며, 정보의 유형별로 볼 때 경영정보 보다 기술정보가 문제된 사건에서 법원이 접근 제한 등 물적 관리 조치를 더 자주 언급한 점이 특징으로 보인다. 또, 민사 사건 보다는 형사 사건에서 비밀관리성이 인정되는 비율이 더 높은 것으로 나타났다.

다음으로 이 연구에서는 판례 분석 결과와 컨설팅, 선행 연구자료 등을 종합적으로 고려하여 소기업, 중기업, 중견기업으로 기업을 분류하여, 제도적 관리·인적 관리·물적 관리 분야별로 기업이 취해야 할 조치를 제시하였다. 다만, 기업의 규모나 업종에 따라 영업비밀 보호·관리를 위해 필요한 조치가 명확히 구분되지 않는데다,

규모나 업종 또한 다양한 기준에 따를 수 있는 등 '표준화'가 가지는 본질적인 한계가 있음은 분명하다. 향후 추가적인 판례 분석과 기업 컨설팅 등을 통해 보완될 수 있을 것으로 기대된다.

기업이 보유한 정보를 영업비밀인 것과 그렇지 않은 것으로 구분하고, 나아가 정보의 가치 등에 따라 등급을 나누는 것은 영업비밀 보호·관리를 위해 매우 중요한 의미를 가진다. 그럼에도 불구하고 실제 기업이 보유한 방대한 정보에 대해 등급을 분류하는 것은 매우 어려운 일이다. 이번 연구에서는 영업비밀의 정의에 기반한 등급 분류 체계를 제시하였다. 어떤 정보가 '영업비밀'에 해당하려면 비공지성, 경제성, 비밀관리성 3가지 요건을 모두 충족해야 하고, 이 중에 하나라도 결여되면 '영업비밀'로 보호받지 못한다. 따라서 기업이 보유한 정보를 분류할 때도 동일한 기준과 방법을 적용한 것이다.

마지막으로, 이번 연구에서는 미국, 일본, 중국과 베트남의 영업비밀 보호, 특히 국가별 비밀관리성 판단에 어떤 특징이 있는지에 관해 살펴보았다. 표현에 있어서 미국은 '합리적 조치(reasonable measures)', 일본은 '비밀관리조치', 중국은 '비밀유지조치', 베트남은 '필요한 조치(necessary measures)'라는 차이가 있지만, 실질적인 측면에서 국가에 따라 명확히 구분되는 차이를 보이지는 않는다.

이번 연구는 영업비밀 관련 판례 분석 결과를 토대로 기업의 규모·업종별 영업비밀 표준 관리 체계를 제시하고자 시도했다는 점에서 의미를 가지는 동시에, 판례 분석이나 표준화가 가지는 본질적인 한계와 연구 내용이나 방법 등에서 한계가 있는 것도 분명하다. 향후 후속 연구와 기업 컨설팅 사례 등을 통해 지속적인 보완과 개선이 이루어지길 기대한다.

[붙임 1] 영업비밀 관리 규정

영업비밀 관리규정(일반형)

제1장 총칙

제1조 (목적) 이 규정은 주식회사 ABC(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 특허권, 실용신안권, 상표권, 디자인권, 저작권 등 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.

제3조 (보안업무의 분류) ① 회사의 모든 "정보"관련 업무를 "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. 영업비밀과 관련된 일체의 시설·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 총괄담당하는 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 수립.조정
7. 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 넣거나 통제구역을 설정하여 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 징구 해야 한다.

제9조 (관리대장) 각 영업비밀의 관리책임자는 제7조 제2항에 의하여 관리하고 있는 영업비밀에 대하여 등급별로 별지 서식의 영업비밀 관리/사용대장(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 정보에 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 외부로부터 취득하였을 경우 관련부서의 부서장에게 신고하고, 관련부서의 부서장은 이를 관리대장에 기재하여 임직원이 창출한 영업비밀과 같은 방법으로 관리한다.

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 서식의 영업비밀 관리대장에 신청내역을 기재한 이후 해당 영업비밀을 반출하거나 사용토록 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 등 해당 영업비밀의 기밀을 유지할 수 있는 적절한 수단을 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 별첨 등급별 취급규정에 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 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 비밀유지서약서를 징구할 수 있으며, 프로젝트 참여 등 필요시에는 별도로 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 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 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 비밀유지서약서를 제출 받고, 외부 기관과 사이에는 비밀유지계약을 체결한 이후에 영업비밀을 공개하여야 한다.

② 회사는 외부 기관과의 협의에 따라 비밀유지서약서 또는 비밀유지계약서의 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 영업비밀 침해구제

제32조 (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.

제33조 (영업비밀누설자에 대한 징계) 영업비밀 누설자에 대해서는 제29조의 규정에 의한 조치를 취함과 동시에 별도로 사규에 따라 징계할 수 있다.

제34조 (관련자에 대한 징계) 영업비밀 누설을 부주의나 과실로 알지 못하였거나 막지 못한 관계자에 대해서도 사규에 의해 징계할 수 있다.

제9장 보칙

제35조 (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.

[별첨]

등급별 취급 규정

1. '1급 비밀'을 기록한 문서, 도면, 사진, 서적, 자기 테이프, FD, CD, 컴퓨터 서버 등 (이하 '기록매체')의 취급은 다음과 같다.

(1) 보관

- 기록매체는 영업비밀 관리대장에 기록매체의 요지를 기입한 후 다른 문서와 구별하여 시건 장치가 있는 보관함에 엄중히 보관해야 한다. 이 때 열쇠 등은 관리책임자가 보관한다.
- 전자화된 정보를 정보시스템 기기에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 정보시스템 기기를 통제 구역 내에 설치한다. 만일 해당 정보시스템 기기를 통제 구역 내에 설치할 수 없는 경우에는 관리책임자는 타인의 접근을 방지하기 위한 최선의 보안조치를 취하여야 한다.
- 전자화된 정보를 외부기록매체에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 외부 기록매체를 시건 장치가 있는 보관함 등에 엄중히 보관해야 한다. 이 때 열쇠 등은 관리책임자가 보관한다.

(2) 열람

- 관리책임자의 허가 없이 기록매체를 열람할 수 없다.
- 해당 정보에 접근이 허락되지 않은 자는 기록매체를 열람할 수 없다.
- 전자화된 정보의 화면 표시는 입실이 제한되고 해당 정보의 보유자가 실재하는 장소에서 타인에게 보이지 않도록 각별한 주의를 기울이며 실시되어야 한다.
- 관리책임자는 영업비밀 사용대장에 열람자명, 일시 등을 기록한다.

(3) 복제

- 관리책임자의 허가 없이 기록매체를 복제할 수 없다. 이때 복제물은 원본과 동등하게 '1급 비밀'로 취급해야 한다.
- 전자화된 정보의 복제는 관리책임자만이 실시할 수 있다.
- 관리책임자는 영업비밀 사용대장에 복제자명, 일시, 목적 등을 기록한다.

(4) 반출

- 관리책임자의 허가 없이 기록매체를 반출할 수 없다.
- 관리책임자의 허가가 있을 경우에도 허가를 받은 본인만이 기록매체를 소지하도록 하며 유출 및 분실에 책임을 지도록 한다.
- 관리책임자는 영업비밀 사용대장에 반출자명, 일시, 목적, 반환시기 등을 기록한다.

(5) 폐기

- 기록매체는 사용 후 기록매체를 배부 받은 자의 책임 하에 적절한 방법에 의해 폐기하도록 한다.
- 전자화된 정보는 관리책임자의 승인을 얻어 제3자가 잔류정보를 해독할 수 없도록 필요한 조치를 취한 후에 폐기하도록 한다.
- 관리책임자는 영업비밀 관리대장에 폐기 일시 등을 기록한다.

2. '2급 비밀' 기록매체의 취급은 다음과 같다.

(1) 보관

- 기록매체는 영업비밀 관리대장에 기록매체의 요지를 기입한 후 다른 문서와 구별하여 시건 장치가 있는 보관함에 엄중히 보관해야 한다. 이 때 열쇠 등은 관리책임자가 보관한다.
- 전자화된 정보를 정보시스템 기기에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당정보시스템 기기를 통제 구역 내에 설치한다. 만일 해당 정보시스템 기기를 통제 구역 내에 설치할 수 없는 경우에는 관리책임자는 타인의 접근을 방지하기 위한 최선의 보안조치를 취하여야 한다.
- 전자화된 정보를 외부기록매체에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 외부기록매체를 시건 장치가 있는 보관함 등에 엄중히 보관해야 한다. 이 때 열쇠 등은 관리책임자가 보관한다.

(2) 열람

- 기록매체는 중대한 필요성이 인정되는 경우 기록매체 소지자의 책임 하에서 관계자에게 열람시킬 수 있다.
- 전자화된 정보의 화면 표시는 타인에게 보이지 않도록 주의를 기울이며 실시되어야 한다.
- 관리책임자는 영업비밀 사용대장에 열람자명, 일시 등을 기록한다.

(3) 복제

- 기록매체는 중대한 필요성이 인정되는 경우 기록매체 소지자의 책임 하에 복제하는 것이 가능하다. 단, 복제물은 원본과 동등하게 '2급 비밀'로 취급해야 한다.
- 전자화된 정보의 복제는 관리책임자의 승인을 얻어 기록매체를 배부 받은 자의 책임 하에 실시할 수 있다.
- 관리책임자는 영업비밀 사용대장에 복제자명, 일시, 목적 등을 기록한다.

(4) 반출

- 업무상 필요성이 인정되는 경우에만 기록매체를 반출할 수 있다.
- 이 경우 기록매체를 반출한 본인만이 기록매체를 소지하도록 하며 유출 및 분실에 책임을 지도록 한다.
- 관리책임자는 영업비밀 사용대장에 반출자명, 일시, 목적, 반환시기 등을 기록한다.

(5) 폐기

- 기록매체는 사용 후 기록매체를 배부 받은 자의 책임 하에 적절한 방법에 의해 폐기하도록 한다.
- 전자화된 정보는 제3자가 잔류정보를 해독할 수 없도록 필요한 조치를 취한 후에 폐기하도록 한다.
- 관리책임자는 영업비밀 관리대장에 폐기 일시 등을 기록한다.

3. '3급 비밀' 기록매체의 취급은 다음과 같다.

(1) 보관

- 기록매체는 영업비밀 관리대장에 기록매체의 요지를 기입한 후 다른 문서와 구별하여 보관해야 한다.
- 전자화된 정보를 정보시스템 기기에 보관하는 경우 암호화 등의 적절한 조치를 취한다.
- 전자화된 정보를 외부기록매체에 보관하는 경우 암호화 등의 적절한 조치를 취하고 해당 외부기록매체를 시건 장치가 있는 보관함 등에 엄중히 보관해야 한다. 이 때 열쇠 등은 관리책임자가 보관한다.

(2) 열람

- 전자화된 정보의 화면 표시는 타인에게 보이지 않도록 주의를 기울이며 실시되어야 한다.

(3) 복제

- 기록매체는 중대한 필요성이 인정되는 경우 기록매체 소지자의 책임 하에 복제하는 것이 가능하다.
- 전자화된 정보의 복제는 중대한 필요성이 인정되는 경우에만 기록매체를 배부받은 자의 책임 하에 실시할 수 있다.
- 관리책임자는 영업비밀 사용대장에 복제자명, 일시, 목적 등을 기록한다.

(4) 반출

- 기록매체를 반출한 본인만이 기록매체를 소지하도록 하며 유출 및 분실에 책임을 지도록 한다.
- 관리책임자는 영업비밀 사용대장에 반출자명, 일시, 목적, 반환시기 등을 기록한다.

(5) 폐기

- 기록매체는 사용 후 기록매체를 배부 받은 자의 책임 하에 적절한 방법에 의해 폐기하도록 한다.
- 전자화된 정보는 제3자가 잔류정보를 해독할 수 없도록 필요한 조치를 취한 후에 폐기하도록 한다.
- 관리책임자는 영업비밀 관리대장에 폐기 일시 등을 기록한다.

영업비밀 관리규정(소규모기업용)

제1장 총칙

제1조 (목적) 이 규정은 주식회사 ABC(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 특허권, 실용신안권, 상표권, 디자인권, 저작권 등 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.

제3조 (보안업무의 분류) 회사의 모든 "정보"관련 업무를 "일반업무"와 "보안업무"로 구분한다.

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. 영업비밀과 관련된 일체의 시설·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 총괄담당하는 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 서약서 등의 집행
6. 보안관련 규정 및 지침 수립·조정
7. 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 정보자산을 그 중요성과 가치의 정도에 따라 "일반정보"와 "영업비밀"로 분류하고, 필요시 그 분류를 변경할 수 있다.

② "영업비밀"이란 경쟁사 또는 대외로 유출될 경우 회사가 손해를 입을 수 있는 실험·분석정보/데이터, 실험결과서, 연구재료, 연구결과보고서, 회의록, 신제품사양·설계도·규격서, 시작품, 신제품개발계획, 제조공법(방법), 금형·물건, 품질관리정보, 시장정보, 고객정보, 제품서비스가격정보, 신제품판매정보 등을 말하며, 이에 제한되지 아니한다.

③ 영업비밀은 5년 이상 보존한다. 다만, 회사의 보안관리책임자 또는 각 부서장은 각 영업비밀의 특성을 고려하여 10년 이상의 기간을 보존기간으로 지정할 수 있다.

제7조 (영업비밀 표시 및 보관) ① 영업비밀은 그 표지에 "대외비" 표시를 와 함께 각 등급에 따라 아래와 같이 구분하여 표시하여야 한다. 다만, 전자문서인 경우에는 파일명 및 문서의 내용 중에, 물건에 대해서는 표찰이나 포장 등에 하여야 한다.

② 영업비밀이 화체된 서류, 물건 등은 일반 문서, 물건 등과 분리하여 별도의 보관함, 금고 등 보안장치를 구비하고 있는 용기에 넣거나 통제구역을 설정하여 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 징구 해야 한다.

제9조 (관리대장) 각 영업비밀의 관리책임자는 제7조 제2항에 의하여 관리하고 있는 영업비밀에 대하여 등급별로 별지 서식의 영업비밀 관리/사용대장(이하 '관리대장'이라 함)을 비치하고 변동사항 등에 대한 기록을 유지·관리하여야 한다.

제10조 (취급자격) 제6조에 의하여 분류된 영업비밀의 취급자격은 대표이사, 보안관리책임자, 해당 영업비밀이 속한 담당부서의 부서장·실무 담당자 기타 대표이사가 지정한 임직원으로 한다.

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 담당부서장에게 이를 통보하고, 회사의 업무를 위해서만 사용하여야 한다.

③ 보안관리책임자는 컴퓨터 또는 전자기록매체의 사용, 반입·반출 등에 관한 기준을 정하여 임직원에게 고지하고, 임직원은 이를 준수하여야 한다.

④ 보안관리책임자는 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 정보에 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 외부로부터 취득하였을 경우 관련부서의 부서장에게 신고하고, 관련부서의 부서장은 이를 관리대장에 기재하여 임직원이 창출한 영업비밀과 같은 방법으로 관리한다.

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 보안관리책임자 또는 영업비밀 관리책임자에게 신청하여야 하고, 위 관리책임자는 신청인의 영업비밀 취급 자격을 확인한 이후 그 자격이 인정되는 경우에 한하여 별지 서식의 영업비밀 관리대장에 신청내역을 기재한 이후 해당 영업비밀을 반출하거나 사용토록 하여야 한다. 이때 대표이사 또는 보안관리책임자가 지정한 영업비밀의 사용 또는 반출에 대해서는 사전에 대표이사 또는 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 보안관리책임자 또는 영업비밀 관리책임자의 사전 승인을 얻어야 하고, 영업비밀을 이송 받은 부서의 책임자는 해당 영업비밀의 사용이 종료되는 때에는 즉시 해당 영업비밀을 원래 보관하고 있던 부서에 반환하여야 한다.

제22조 (이송방법) ① 영업비밀을 사내에서 대여·사용·유통을 위하여 이송할 때에는 밀폐포장이나 용기 등 해당 영업비밀의 기밀을 유지할 수 있는 적절한 수단을 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 보안관리책임자가 최종 관리한다. 보안관리책임자는 영업비밀의 보관, 열람, 복제, 반출, 폐기 등에 관한 별도의 기준을 정할 수 있다.

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 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 비밀유지서약서를 징구할 수 있으며, 프로젝트 참여 등 필요시에는 별도로 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 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 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 비밀유지서약서를 제출 받고, 외부 기관과 사이에는 비밀유지계약을 체결한 이후에 영업비밀을 공개하여야 한다.

② 회사는 외부 기관과의 협의에 따라 비밀유지서약서 또는 비밀유지계약서의 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 영업비밀 침해구제

제32조 (구제조치) ① 보안관리책임자 및 각 부서장은 회사의 영업비밀을 침해당했을 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.

제33조 (영업비밀누설자에 대한 징계) 영업비밀 누설자에 대해서는 제29조의 규정에 의한 조치를 취함과 동시에 별도로 사규에 따라 징계할 수 있다.

제34조 (관련자에 대한 징계) 영업비밀 누설을 부주의나 과실로 알지 못하였거나 막지 못한 관계자에 대해서도 사규에 의해 징계할 수 있다.

제9장 보칙

제35조 (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.

[별지]

영업비밀 관리/사용대장

■ 영업비밀 관리대장

관리 번호	비밀 등급	관리 대장 등록일	영업 비밀 명칭	대상 (매체)	보관 장소	관리 책임자	보존 기간	폐기일	비고

■ 영업비밀 사용대장

관리 번호	비밀 등급	영업 비밀 명칭	사용 반출 일자	사용 /반출자	사용 목적	반환 예정 일자	서명	반환 일자

[붙임 2] 비밀유지 서약서

비밀유지서약서

성명		입사일자	
생년월일		소속/직급	
담당업무			

위 본인은 주식회사 ABC(이하 '회사'라 함)로부터 영업비밀 및 영업자산의 중요성과 영업비밀 등의 보호와 관련한 법령 및 회사의 취업규칙, 영업비밀 관리규정 기타 사규, 방침, 정책 등에 관하여 충분한 설명을 듣고 그 내용을 이해하였기에, 다음 사항을 준수할 것을 서약합니다.

1. 본인은, 아래와 같은 정보가 회사의 영업비밀에 해당함을 확인하며, 회사의 취업규칙, 영업비밀 관리규정 기타 사규, 방침, 정책 등을 준수할 것을 서약합니다.

① 영업비밀 관리규정 기타 회사의 내부규정에 기재된 영업비밀 보호대상

② 영업비밀임이 표시된 기술자료, 공장배치도, 제품 설계도면, 금형, 시제품, 제조 및 판매 매뉴얼, 제조원가, 판매 및 가격결정, 거래선 자료, 인력정보 등에 관한 정보 등

③ 통제구역, 시건장치, 패스워드 등으로 접근이 제한된 컴퓨터시스템, 보관함, 통제구역에 보관된 기록매체, 문서, 물건, 정보 등

④ 아래 각 호의 영업비밀 및 영업자산

구분	명칭	설명
1		
2		
3		

⑤ 그 밖에 회사가 영업비밀로 지정하고 표시하였거나, 회사가 영업비밀로 관리하고 있는 비밀정보

[추가 사항 기재]

2. 본인은, 회사에 재직 중 취득하였거나 취득하게 되는 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산을 재직 시는 물론 퇴사 후에도 이를 비밀로 유지하고, 회사의 사전 서면 동의 없이는 경쟁업체나 제3자에게 제공하거나 누설하지 않으며, 부정한 목적으로 공개하거나 사용하지 않을 것을 서약합니다.

3. 본인은, 회사에 재직 중 취득하였거나 취득하게 되는 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산에 대한 모든 권리가 회사의 소유임을 인정하고, 이를 회사에 귀속시킬 것을 서약합니다.

4. 본인은, 회사에 재직 중 회사의 승인을 받지 아니하고는 통제구역, 허가 받지 않은 정보, 시설 등에 접근하지 아니하며, 회사의 영업비밀을 복제하거나 사본 등의 형태로 보관하지 아니할 것을 서약합니다.

5. 본인은, 입사 전 또는 재직 중에 취득한 타인의 영업비밀 등에 해당하는 정보를 회사에 제공하거나 개시하지 않을 것이며, 업무상 그 정보의 개시가 불가피하다고 판단되는 경우에는 사전에 회사와 상의하여 타인의 영업비밀 등을 침해하지 않도록 할 것을 서약합니다. 6. 본인은, 회사에 재직 중에 회사의 사전 승인을 받지 아니하고는 회사와 동종, 유사업체의 임직원으로 겸직하거나 자문을 제공하지 아니할 것을 서약합니다. 7. 본인은, 회사의 컴퓨터 등 정보처리장치와 정보통신망을 업무용으로만 사용할 것이며, 회사가 불법 행위 방지 및 영업비밀 등의 보호를 위하여 필요한 경우 본인의 컴퓨터 등 정보처리장치나 전자우편 또는 인터넷 등 정보통신망의 사용 내역, 기타 필요한 정보를 모니터링 할 수 있으며, 불법행위 또는 영업비밀 등의 누설이나 침해의 우려가 있을 경우 관련 내용을 열람 또는 조사할 수 있음을 *(이해하고, 이에 동의합니다.)*	8. 본인은, 퇴사 시 재직 중에 보유하였던 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산과 관련된 자료 모두를 회사에 반납하고, 이에 관한 어떠한 형태의 사본도 개인적으로 보유하지 않으며, 반납할 수 없는 것은 폐기할 것을 서약합니다. 9. 본인은, 회사에서 퇴사한 날로부터 [ ] 년의 기간 동안 위 제2항의 영업비밀 및 영업자산이 누설되거나 이용될 가능성이 있는 기업 또는 단체에 취업하거나, 그와 같은 기업 또는 단체를 창업 또는 설립하여 회사와 경쟁하지 않을 것을 서약합니다. 만약 본인이 취업 혹은 창업하고자 하는 기업 또는 단체가 본 서약서에 따른 경업금지의 대상이 되거나 대상인지 여부가 불분명할 경우, 사전에 회사에 통보하여 회사의 확인 및 동의를 받을 것을 서약합니다.

위 서약한 사항을 위반할 경우 관련 법규에 의한 민·형사상 책임을 감수할 것임을 서약합니다.

(위 내용을 확인하고 이해하였으며, 이에 서명함)

20__. __. __.

서약자: (서명)

주식회사 ABC 귀하

기업 규모·업종별 영업비밀 표준관리체계 마련 연구

발행일 | 2020년 1월

발행인 | 특허청장 박원주

발행처 | 특허청 산업재산보호정책과(www.kipo.go.kr)
대전시 서구 청사로 189(둔산동) 정부대전청사 4동
TEL (042) 481-5425
FAX (042) 472-1360

기업 규모·업종별 영업비밀 표준관리체계 마련 연구

특허청
대전광역시 서구 청사로 189 정부대전청사 4동
TEL. 042-481-5425 http://www.kipo.go.kr

ISBN : 979-11-89854-62-1 13500
DOI : 10.8080/P9791189854621