중소기업 기술유출 대응매뉴얼

2007. 12

연구기관 : 한국산업기술진흥협회

본 보고서는 한국산업기술진흥협회가 중소기업기술정보진흥원의 연구용역 의뢰를 받아 수행한 연구의 결과입니다.

제 출 문

중소기업기술정보진흥원장 귀하

본 보고서를 2007년도 중소기업 기술유출방지사업으로 추진한 “중소기업 기술유출 대응매뉴얼”의 최종보고서로 제출합니다.

2007. 12. 18

연구기관명 : 한국산업기술진흥협회
연구책임자 : 허현회 상임이사
연 구 원 : 임자현 상무이사
한기인 부장
정해혁 차장
정선훈 차장
이동주 선임
오승룡 선임
김상길 과장
노민선 전임
이창주 대리
윤영근 대리
이혜정 연구원
박미진 연구원
김화정 연구원

< 목 차 >

< 표 목 차 >

< 그 림 목 차 >

제 1 장 서 론

제1절 매뉴얼의 목적

□ IT기술이 발전함에 따라 정보를 빼내는 방법이 점점 지능화되고 있는 요즈음 내부 기밀정보의 유출 문제는 기업의 생명을 좌우하는 중요한 이슈가 되고 있음

○ 전체 기업의 41.4%가 기밀유출에 대한 위협 정도가 심하다고 응답했으며, 특히 벤처기업의 경우 51.7%가 유출위협을 심각하게 느끼는 것으로 나타남 (산업기술진흥협회, 2006.8)

□ 최근 들어 중소기업의 기술력이 높아지면서 허술한 보안체제로 인한 첨단기술의 유출이 계속해서 증가하고 있으며, 해외진출 중소기업의 기술유출로 인한 피해도 심각한 수준으로 나타남

○ 기술유출 적발현황을 살펴보면 연도별로 계속해서 증가하고 있으며, 이 중 중소기업의 비율이 60%를 넘어섬(국가정보원, 2007.9)

○ 중소기업의 17.8%가 최근 3년간 산업기밀의 유출로 인해 피해를 입은 적이 있으며, 이 중 52.6%는 2회 이상 기밀유출을 경험한 것으로 나타남(중소기업청, 2007.6)

○ 중국과 동남아 지역에 진출한 중소기업 4곳 중 1개 업체는 기술유출 경험이 있는 것으로 조사됨(산업기술진흥협회, 2007.4)

□ 하지만 중소기업의 경우 기술유출에 대한 사전예방은 물론 사후대응이 상대적으로 소극적이며, 그 중요성에 비해 당장의 눈에 보이는 성과가 적기 때문에 기술유출 방지업무 수행을 위한 투자가 미흡한 상황임

○ 보안관리규정 마련(35.3%), 보안담당부서 설치(6.6%) 등 전반적인 보안인프라가 매우 취약(중소기업청, 2007.6)

○ 기술유출시 중소기업의 43.6%, 벤처기업의 41.2%가 특별한 조치를 취하지 않는 것으로 나타남(산업기술진흥협회, 2006.8)

○ 대부분의 중소기업(78.0%)이 보안비용으로 매출액의 1% 미만을 투자하고 있는 것으로 조사됨(중소기업청, 2007.6)

□ 본 매뉴얼은 위와 같은 중소기업의 실정을 바탕으로 실제 사례를 기반으로 하여 기술유출 방지 및 기술유출시 대응방안을 제시함으로써, 중소기업의 산업보안에 대한 인식을 제고하고, 기술경영 활동을 지원함을 그 목적으로 함

제2절 매뉴얼의 구성

□ 본 매뉴얼은 서론, 보안 자가진단, 기술유출 사전 대응방안, 기술유출 사후 대응방안, 기술유출 현황 및 사례 등 총 4개의 장과 1개의 부록으로 구성되어 있으며, 기술유출방지 관련 법제 및 서식자료집은 별책으로 구성하였음

<표1-1> 매뉴얼의 구성 및 주요 내용

구 분	제 목	주요 내용
제 1 장	서 론	매뉴얼의 목적·구성, 기술유출의 개념, 매뉴얼의 적용방법
제 2 장	보안 자가진단	6개 부문에 걸쳐 50개 문항으로 구성된 기업의 보안수준 측정을 위한 자가진단 서식
제 3 장	기술유출 사전 대응방안	보안정책, 자산관리, 인적자원관리, 시설관리, IT보안관리, 계약관리, 글로벌 보안관리
제 4 장	기술유출 사후 대응방안	퇴직자의 창업 또는 경쟁업체 취업, 영업비밀 침해, 지적재산권 침해, 해외진출 기업
부 록	기술유출 현황 및 사례	국내 중소기업, 해외진출 중소기업, 해외 기업의 기술유출 현황 및 사례
별 책	기술유출 방지 관련 법제 및 보안서식 자료집	국내·외 기술유출방지 관련 법제, 보안서식

○ 제1장 '서론'에서는 본 매뉴얼의 목적, 구성, 기술유출의 개념, 매뉴얼의 적용방법을 제시하였음

○ 제2장 '보안 자가진단'에서는 중소기업의 보안수준을 측정하는 자가진단서식을 6개 부문에 걸쳐 50개 문항으로 범주화하였으며, 각 문항을 통해 진단이 필요한 사항이 무엇인지 알 수 있도록 구성하였음

- 6개 부문 : 보안정책, 자산관리, 인적자원관리, 시설관리, IT보안관리, 유출사고의 대응

○ 제3장 '기술유출 사전 대응방안'에서는 보안정책, 자산관리, 인적자원관리, 시설관리, IT 보안관리, 계약관리 등 중소기업의 입장에서 기술유출을 사전에 예방할 수 있도록 다양한 대응방안을 제시하였으며, 기업이 해외 진출시 기술유출을 방지하기 위해 주의해야 할 사항을 함께 언급하였음

○ 제4장 '기술유출 사후 대응방안'에서는 중소기업의 기술유출 및 침해사건 발생시 대응방안을 제시하였으며, 최근 중국에서의 기술유출 피해가 잇따르고 있는 점에 착안하여 중국에서의 유출피해 경험시 대응방안을 함께 소개하였음

○ 부록 '기술유출 현황 및 사례'에서는 국내 중소기업과 해외 진출 중소기업에 대한 실태조사 분석결과 및 유출경험이 있는 기업에 대한 방문조사 등을 통해 실제 유출사례를 제시했으며, 해외기업의 경우 주요 기관의 홈페이지 및 언론기사 검색을 통해 사례를 발굴하였음

○ 별책에서는 국내·외 기술유출방지 관련 법제를 소개하였으며, 각종 보안서류 양식에 대한 예시문을 제시하였음

제3절 기술유출의 개념

1. 기술유출의 정의

□ 본 매뉴얼에서의 '기술유출'은 '기업의 입장에서 중요 자산으로 보호하고 있는 기술상의 정보와 노하우'(이하 '기술정보'라 함)에 대한 유출 및 침해행위를 말하며, 다음의 6가지 행위를 의미함

1) 절취·기망·협박 그 밖의 부정한 방법으로 기술정보를 취득하는 행위 또는 그 취득한 기술정보를 사용하거나 공개하는 행위

2) 규정 또는 계약에 따라 기술정보에 대한 비밀유지의무가 있는 자가 그 기술정보 등을 절취·기망·협박 그 밖의 부정한 방법으로 유출하는 행위 또는 그 유출한 기술정보를 사용하거나 공개하거나 제3자가 사용하게 하는 행위

3) 위의 1)과 2)의 규정에 해당하는 행위가 개입된 사실을 알고 그 기술정보를 취득·사용 및 공개하거나 그 기술정보를 취득한 후에 1)과 2)의 규정에 해당하는 행위가 개입된 사실을 알고 사용하거나 공개하는 행위

4) 위의 1)과 2)의 규정에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 기술정보를 취득·사용 및 공개하거나 기술정보 등을 취득한 후에 1)과 2)의 규정에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 기술정보를 사용하거나 공개하는 행위

5) 산업자원부 장관의 승인을 얻지 아니하거나 부정한 방법으로 승인을 얻어 국가핵심기술의 수출을 추진하는 행위

6) 국가핵심기술의 수출중지·수출금지·원상회복 등의 조치에 대한 산업자원부 장관의 명령*을 이행하지 아니하는 행위

* 다음에 해당할 때, 정보수사기관의 장에게 조사를 의뢰하고, 조사결과를 산업기술보호위원회에 보고한 후 위원회의 심의를 거쳐 이루어짐

- 신고대상인 국가핵심기술의 수출이 국가안보에 심각한 영향을 줄 수 있다고 판단하는 경우

- 위의 5)의 규정에 해당하는 경우 혹은 신고대상 국가핵심기술을 신고하지 아니하거나 허위로 신고하고 국가핵심기술을 수출한 경우

2. 기술유출의 요건

□ 기술유출은 국가, 기업, 기술개발자 등 각 이해관계자의 시각에 따라 기술거래, 기술협력 혹은 직업선택의 자유 등과 그 개념이 혼동되어 있으며, 기술유출의 개념을 명확히 정립하기 위해서는 다음과 같은 사항들을 우선적으로 확인할 필요가 있음

1) 불법성이 존재하는가?

- 모든 유출이 불법인 것은 아니며, 정당한 기술거래로 인한 기술이전 등은 적법한 것으로 기술유출이라고 할 수 없음

2) 반드시 보호할 가치가 있는가?

- 퇴직자가 전직 후 비밀유지의무가 명시되지 않은 기술정보를 사용했다고 해서 기술유출이라고 보기는 어려움

3) 유출에 대한 정당한 대가가 지급되었는가?

- 일반적으로 기술유출이 발생한 경우 당해 기술개발에 소요된 비용과 기술시장에서 거래될 경우에 받을 수 있는 대가에 비해 현저히 저렴한 금액으로 거래되기 마련임

4) 정당한 라이선스 허여(許與) 절차를 밟았는가?

- 정당한 절차를 밟지 아니하고 특허 등을 무단으로 도용하거나 타인의 제품을 모방하여 유사한 제품을 설계하는 것도 기술유출에 해당함

5) 국가의 정책적인 면이 고려되었는가?

- 최근 들어 세계 각국은 국가의 안보와 경제적 이익을 이유로 자국기술의 해외유출을 규제하려는 노력을 강화하고 있음
- 우리나라의 경우 '산업기술의 유출방지 및 보호에 관한 법률'에 의거하여 40개의 국가핵심기술을 지정하여 수출을 통제하고 있음(2007. 8)

제4절 매뉴얼의 적용방법

1. 매뉴얼 이용대상

○ 본 매뉴얼은 목적에서 상술한 바와 같이 중소기업을 상대로 제작되었으며, 중소기업의 CEO, 연구소장, 보안담당자, 인사총무나 연구기획 업무에 종사하는 직원을 주요 이용대상으로 함

2. 보안 자가진단

○ 본 매뉴얼의 이용자는 가장 먼저 자사의 보안수준을 측정하는 자가진단을 실시하여 자사가 보유한 자산의 보호수준을 파악해야 하며, 이를 통해 보안상 미흡한 분야를 찾아내려는 노력이 필요함

- 아직까지 대부분의 중소기업에서는 회사 보유 자산의 보호수준 파악은 고사하고 어떤 부분이 미흡한지에 대한 진단기준 조치 마련되어 있지 않은 것이 현실임

○ 자가진단 서식은 국제 정보보호 표준규격인 ISO/IEC 27001을 참고로 하여 3차례의 파일럿 테스트를 통해 중소기업의 형편에 맞도록 재구성하였음

- 자가진단 서식은 6개 부문*에 걸쳐 50개 문항으로 구성되어 있으며, 질문을 통해 진단이 필요한 사항이 무엇인지 알 수 있도록 설계되었음

* 6개 부문 : 보안정책, 자산관리, 인적자원관리, 시설관리, IT보안관리, 유출사고의 대응

○ 자가진단 결과는 기본적인 부분만 제대로 신경 쓰면 70점 이상(우수, 양호)의 점수를 취득할 수 있도록 설계되었으며, 만일 진단결과 점수가 70점 미만(보통, 취약, 위험)이라면 미흡한 부분을 보완하여 70점 이상의 수준을 지속적으로 유지할 수 있도록 노력해야 함

- 한국산업기술진흥협회가 주관하는 산업보안교육 참가자(86명)를 대상으로 기업의 보안수준을 측정한 결과 취약수준(44.7점)으로 나타나 기업들의 지속적인 개선활동이 요구됨

○ 본 매뉴얼에서는 자가진단 각 항목별로 해당 페이지를 안내함으로써 신속히 관련 대책을 찾아볼 수 있도록 배려함

3. 추진업무별 적용방법

○ 본 매뉴얼에서는 7개 부문의 72개 항목을 중소기업에서 기술유출 방지를 위해 우선적으로 추진해야 할 업무로 제시하였음

○ 추진업무별 보안대책 부분에 매뉴얼의 해당 페이지를 표시하여 업무별로 관련 사항을 쉽게 찾아볼 수 있도록 함

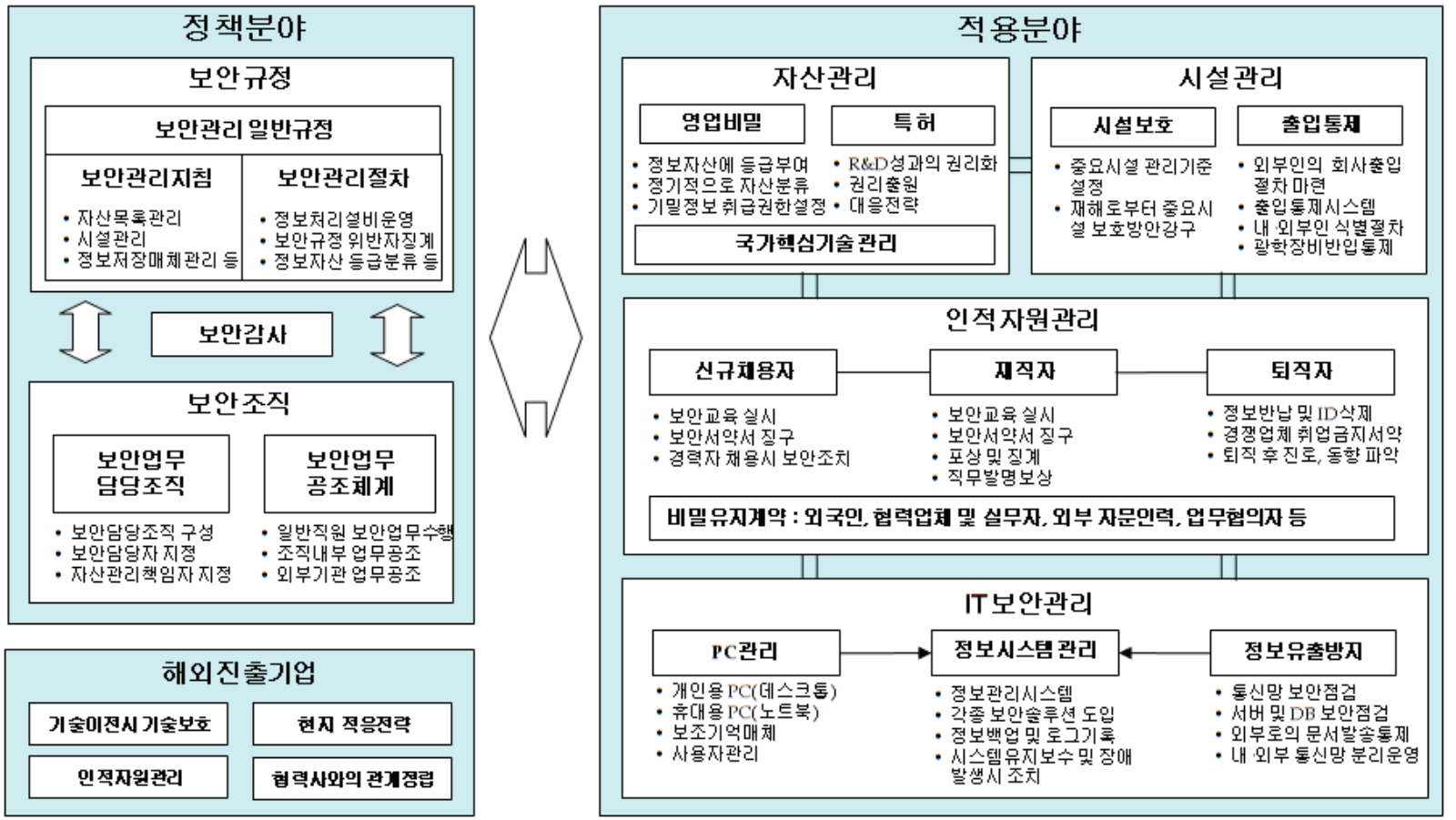
<표1-2> 추진업무별 적용방법

구 분	구성요소	추진업무	보안대책
1. 보안정책	보안규정	보안관리규정	p.39
		자산목록관리	p.42~45
		정보자산 등급분류	p.42~45
		시설관리	p.81~84
		보안규정 위반자 징계	p.40, p.70
		정보처리 설비 운영	p.89
		정보저장매체 관리	p.85~87
		보안규정, 지침, 절차 공지	p.39
	보안조직	보안담당조직 구성	p.39~40
		보안담당자 지정	p.39
		자산관리책임자 지정	p.44
		일반직원 보안업무 수행	p.40
		조직내부 업무공조	p.40
		외부전문기관 업무공조	p.41
	보안감사	정기 보안감사	p.40
2. 자산관리	영업비밀	영업비밀 보호	p.55~64
		정보자산에 등급 부여	p.42~44
		정기적으로 정보자산 분류	p.42~44
		기밀정보에 대한 권한 설정	p.44~45
		자산의 반출 통제	p.45
		기술보호에 대한 판단기준	p.60~61

구 분	구성요소	추진업무	보안대책
2. 자산관리	특 허	연구개발 성과의 권리화 권리출원 대응전략	p.46~47 p.49~54 p.46~54
	기 타	국가핵심기술 관리	p.65~67
3. 인적자원 관리	신규 채용자	보안교육 실시 보안서약서 징구 경력자 채용시 조치사항	p.68
	재직자	보안교육 실시 보안서약서 징구(재직자) 보안서약서 징구(프로젝트 참가자) 보안점검 실시 보안관련 포상 및 징계 직무발명보상	p.70 p.69 p.69 p.70 p.70 p.74~80
	외국인	신규채용시 기술협력, 기술자문, 투자협정시	p.71~72
	퇴직자	정보반납 및 개인정보 삭제 경쟁업체 취업금지서약 퇴직 후 진로 및 동향파악	p.73
	외부인력	협력업체 및 실무자 외부 자문인력 제품 구매자 등	p.74
4. 시설관리	보호기준	중요시설 관리기준 설정 재해로부터 중요시설 보호방안 강구	p.81~84 p.84
	출입통제	외부인의 회사 내 출입절차 출입통제시스템 설치 중요시설에 대한 광학장비 반입 통제 내・외부인 식별절차	p.81~84

구 분	구성요소	추진업무	보안대책
5. IT 보안관리	PC 관리	개인용 PC(데스크톱) 휴대용 PC(노트북) 보조기억매체 사용자 관리	p.85 p.86 p.86~87 p.85
	정보유출 방지	통신망에 대한 보안점검 서버 및 DB 현황에 대한 보안점검 외부로의 전자문서 발송 통제 내·외부 통신망 분리운영	p.89 p.89 p.87~88, p.85 p.88
	정보 시스템	정보관리시스템 내부생성 정보에 대한 백업 시스템 사용내역에 대한 로그기록 및 유지 시스템 유지보수 각종 보안솔루션 도입 및 사용 장애발생시 조치	p.87~88 p.89 p.89 p.90 p.87~88 p.90
6. 계약관리	기술계약 체결시 유의사항	공동연구계약 투자유치계약 라이선스계약 제조위탁계약 인수합병계약 합작투자계약	p.93~95 p.96 p.97~105 p.106 p.107 p.108
7. 글로벌 보안관리	해외진출	기술이전시 유의사항 현지적응전략 인적자원관리 협력사와의 관계정립	p.109 p.110 p.110~111 p.111

<그림1-1> 중소기업의 보안업무 추진을 위한 가이드라인



4. 단계별 적용방법

○ 본 매뉴얼에서는 기술유출 방지를 위해 중소기업이 추진해야 할 주요 보안 업무를 단계별로 구분하여 제시하였음

○ 1단계에는 중소기업이 추진해야 할 가장 기본적인 보안업무를 제시하였으며, 모든 중소기업이 반드시 시행할 것을 권장함

○ 단계가 높아질수록 보안업무의 추진효과가 높아지지만 추진업무의 양과 소요비용 또한 증가한다는 점을 고려하여 중소기업의 입장에서 2단계와 3단계 업무는 선택적으로 적용할 것을 권장함

□ 보안정책

1단계	2단계	3단계
보안담당자 지정 - 자산관리업무 병행	보안담당자, 자산관리담당자 별도 지정	보안전담조직 구성 - 보안담당자, 자산관리담당자 별도 지정
보안담당자에 의한 협의(俠義)의 보안업무 수행	대부분의 보안업무를 보안담당자가 추진하며, 조직 내·외부와 부분적인 공조업무 실시	보안업무 추진에 있어서 조직 내·외부의 업무공조체계 확립
보안관리규정 제정	필요시 보안관리규정을 개정하고, 보안관리 지침과 절차 시행	정기적으로 보안관리규정과 지침 및 절차를 제·개정
주요 항목에 대한 보안점검을 실시하고 위규자에 대해 보안지도 혹은 경고조치	필요시 보안감사를 실시하고, 위규자에 대해 경고 혹은 징계조치	정기적으로 보안감사를 실시하고 위규자에 대해 징계조치

□ 자산관리

1단계	2단계	3단계
회사 핵심정보에 대해 별도 관리	관리기준에 따라 정보자산의 등급을 분류하여 관리	관리기준에 따라 정기적으로 정보자산의 등급을 분류하여 관리
핵심 기밀문서에 대해 별도 관리	회사 주요 기밀문서에 대해 사용자별 권한설정 조치	모든 문서에 대해 사용자별 권한설정이 되어 있으며 정기적으로 권한설정을 변경·관리
회사의 주요 자산에 대한 반출을 통제	회사자산의 반출시 사전 혹은 사후인가 필요	회사자산의 반출시 반드시 사전인가가 있어야 하며, 물품의 반입·반출시에도 사전 허가 필요
영업비밀과 지적재산권 제도를 어느 정도 이해하며, 일부 활용이 가능함	영업비밀과 지적재산권의 보호 및 관리방안이 마련되어 있음	영업비밀과 지적재산권의 침해시 보호·관리방안 뿐만 아니라 유출시 대응전략도 마련되어 있음

□ 인적자원관리

1단계	2단계	3단계
신규채용자에 대해 보안서약서를 징구하고, 간단한 보안사항 설명	신규채용자에 대해 보안서약서를 징구하고, 필요시 보안교육 실시	신규채용자에 대해 보안서약서 징구 및 정기적인 보안교육을 실시하고, 경력자 채용시 별도의 보안조치 실시
재직자에 대해 필요시 간단한 보안교육 실시	재직자에 대해 외부전문가 초빙교육 실시	보안담당자에 대한 외부전문교육 실시
재직자에 대해 보안서약서 징구	재직자에 대해 연봉체결시마다 보안서약서를 징구하고 회사 내·외부 프로젝트에 참여하는 경우 보안서약서 별도 징구	

□ **인적자원관리(계속)**

1단계	2단계	3단계
재직자의 직무발명에 대해 승진 등의 비금전적 보상만 실시	재직자의 직무발명에 대해 비금전적 보상을 주로 하며, 일부 금전적 보상 실시	재직자의 직무발명에 대한 보상제도가 마련되어 있어 비금전적 보상과 함께 금전적 보상을 병행 실시
임직원들의 보안실천을 위해 필요시 보안점검 실시하고 위규자에 대해 경고 등의 조치	임직원들의 보안실천을 위해 정기적으로 보안점검 실시하고 위규자에 대한 징계·처벌 등의 조치	임직원들의 보안인식 제고를 위해 정기적으로 보안활동을 추진하고 유공자에 대한 포상과 위규자에 대한 징계조치
외국업체와 계약체결시 혹은 외국인 인력 고용시 보안서약서를 징구하고 간단한 보안사항을 설명	외국 협력업체 및 외국인에 대해 보안서약서를 징구하고, 필요시 보안교육 실시	
퇴직자에 대해 경쟁업체 취업금지 서약서를 징구하고 보안관련 주의사항 주지	퇴직자에 대해 퇴직인터뷰를 통해 퇴직 후 진로에 대해 확인	퇴직자에 대해 퇴직인터뷰를 통해 퇴직 후 진로에 대해 확인하고, 퇴직 후 일정기간 동안 진로 및 동향에 대해 인지
퇴직자에 대해 개인 PC 및 업무관련 자료를 반납하도록 조치하고 주요 계정의 ID 및 PW 삭제	퇴직자에 대해 개인 PC 및 업무관련 자료를 반납하도록 조치하고, 주요 반출물품에 대한 검색을 실시하며, 본인 계정의 ID 및 PW를 퇴사하자마자 즉시 삭제	
협력업체 등 외부인력에 대해 보안서약서 징구	협력업체 등 외부인력에 대해 보안서약서를 징구하고, 필요시 보안교육 실시	

□ **시설관리**

1단계	2단계	3단계
회사 내 시설을 중요도에 따라 구분하여 관리	회사 내 중요시설 보호를 위해 ID카드, CCTV 등 통제시스템 활용	회사 내 중요시설 보호를 위해 각종 통제시스템을 활용하고, 자연재해 및 기술유출 등 비상상황 발생시에 대한 보호대책 마련
외부인의 회사 내 출입절차를 마련하여 출입내역 관리	외부인의 회사 출입시 내부인력이 안내·관리하도록 하고, 물품의 사내반입을 통제	

□ **IT 보안관리**

1단계	2단계	3단계
개인용 PC에 ID 및 패스워드를 설정	개인용 PC에 설정된 ID 및 패스워드를 주기적으로 변경하고 화면보호기를 설정	
외부로부터 스팸성 이메일 수신하는 경우 삭제 조치하고, 열어보는 경우 사전에 바이러스 검사 실시	개인용 PC에 백신프로그램을 설치하여 정기적으로 바이러스 점검 실시	PC보안용 소프트웨어를 설치하고, 불법 소프트웨어 사용을 금지함
인가되지 않은 휴대용 PC(노트북)에 대한 사용을 금지하고, 휴대용 PC 사용자에 대한 보안서약서 징구	휴대용 PC의 반출시 저장내용 삭제 등 보안조치 실시	문서보안용 소프트웨어 설치
USB 등 보조기억매체 관리기준 마련	보조기억매체 반출시 저장내용 삭제 등 보안조치 실시	

□ **IT 보안관리(계속)**

1단계	2단계	3단계
개인용 PC에서 외부로 이메일 발송시 파일크기를 일정규모 이하로 제한하고, 이를 초과할 경우 부서장의 승인 후 발송	내부 인력 상호간의 자유로운 파일문서 송수신 금지	문서보안용 소프트웨어 설치
정보처리 설비의 운영절차 문서화 - 컴퓨터의 가동과 종료, 백업, 생성정보의 관리 및 폐기 등	장애발생시 유관기관 연락체계를 확립하고, 네트워크, 서버, DB현황 등에 대한 정기적인 보안점검 실시	네트워크 보안용 소프트웨어를 설치하고, 정보시스템에 대한 유지보수 실시

□ **계약관리**

1단계	2단계	3단계
기술계약 체결시 기술유출을 방지하기 위해 부당이용 금지, 서브 라이선스 금지 등 주요 사항을 계약서에 언급	기술계약 체결시 사전점검, 교섭 단계, 계약서 작성단계로 구분하여 기술유출 방지노력 추진	기술계약의 각 유형별로 계약단계별 기술유출 대응방안을 마련하여 추진

□ **글로벌 보안관리**

1단계	2단계	3단계
해외 진출시 또는 협력시 기술이전에 따른 기술유출 방지업무 중점 추진	해외 진출시 현지 적응을 위한 노력을 강화하고, 필요시 현지 고용인력에 대한 보안교육 실시	관련 대상국가의 기술유출 관련 법제를 잘 인지하고 있으며, 영업비밀과 지적재산권 침해시 신속히 대응할 수 있는 전략 마련

5. 기술유출사건 발생시 적용방법

○ 본 매뉴얼에서는 기술유출 및 침해사건 발생시 조치사항에 대해 국내와 해외로 구분하여 주요 구제방안을 중심으로 기술하였음

<국내 기업>

○ 영업비밀의 경우 퇴직자가 창업하거나 경쟁업체에 취업한 경우 조치사항(협조공문 발송)과 실제 침해행위 발생시 민사적·형사적 구제방안에 대해 기술하였음

○ 지적재산권의 경우 권리침해가 의심되는 경우(경고장 송부)와 분쟁발생시 행정적·민사적·형사적 구제방안에 대해 기술하였으며, 최근 들어 중요성이 증대되고 있는 대체적 분쟁해결(Alternative Dispute Resolution, ADR)에 대해 소개하였음

○ 아울러 지적재산권과 영업비밀을 침해하는 물품에 대한 수출입, 국내판매, 제조행위 등의 불공정무역행위에 대한 무역위원회의 구제제도를 안내하였음

<해외진출 기업>

○ 해외진출 기업의 사후 대응방안의 경우, 해외 기술유출의 대부분을 차지하는 중국에서의 유출 및 침해사건 발생을 중심으로 기술하였음

○ 영업비밀의 경우 성립요건과 침해행위 유형을 안내하였으며, 침해행위에 대한 행정적·민사적·형사적 구제방안을 기술하였음

○ 지적재산권의 경우 행정적·사법적 구제방안을 기술하였으며, 구제수단별 특이사항을 함께 소개하였음

- 행정적 구제시 전리권(특허, 실용신안, 디자인 등)의 경우 전리업무관리부서에서, 상표권의 경우 공상행정관리부서에서 담당
- 사법적 구제시 중국법원의 2심제 제도 설명 및 가처분 제도의 활용 등 효율적 구제방안 소개

○ 아울러 영업비밀 및 산업재산권 침해사건 발생시 조사, 심판, 소송비용에 대한 정부의 지원제도를 소개하였음

6. 보안양식의 활용

○ 본 매뉴얼의 별책에 수록된 각종 보안서류 양식은 다양한 분야에 종사하는 전문가의 의견이 수렴된 것이며, 기업에서 발생할 수 있는 대부분의 Case에 적용할 수 있도록 예시문 형태로 제시하였음

7. 유의사항

○ 본 매뉴얼은 중소기업의 기술유출 예방 및 유출시 대응에 관한 가이드라인을 제공하기 위한 목적으로 제작되었으며, 중소기업이 이를 실제 업무에 적용하면서 발생할 수 있는 문제에 대한 법적 책임을 지지는 않음

- 법적분쟁 발생시 원만한 대응을 위해서 해당 기업 자체적인 법적검토가 함께 요구됨

제 2 장 보안 자가진단

제1절 자가진단의 필요성

○ 기업이 기술 및 정보 등을 보호하기 위해서 가장 먼저 해야 하는 일은 자사가 보유하고 있는 자산의 보호수준을 파악하는 것이며, 이를 통해 보안상 미흡한 분야를 찾아내서 피해를 예방하는 것은 필수적임

○ 하지만 대부분의 중소기업에서는 회사 보유 자산의 보호수준의 파악은 고사하고 어떤 부분이 미흡한지에 대한 진단기준 조차 마련되어 있지 않은 형편임

○ 본 서식에서는 국제 정보보호 표준규격인 ISO/IEC 27001을 참고로 하여 3차례의 파일럿 테스트를 통해 중소기업의 형편에 맞도록 자가진단 기준을 설정하여 제시하였음

제2절 자가진단 방법

□ 자가진단 서식 구성

○ 기업의 보안수준을 측정하는 자가진단 서식은 6개 부문에 걸쳐 50개의 문항으로 구성되어 있으며, 질문을 통해 진단이 필요한 사항이 무엇인지 알 수 있도록 구성되어 있음

- 6개 부문 : 보안정책, 자산관리, 인적자원관리, 시설관리, IT 보안관리, 유출사고의 대응

□ 자가진단 방법

○ 각 부문 내 문항별로 0~3점까지 부여했으며, 문항별 점수를 합산하면 해당 부문의 현재 점수를 계산할 수 있음

○ 대상기업의 보안수준은 각 부문의 점수를 합하여 측정하며, 점수별로 우수, 양호, 보통, 취약, 위험 등 5가지 수준으로 구분함

<보안 수준>

점 수	보안 수준
85점 이상	**우수 수준** 보안에 대한 결점 및 취약성이 거의 없으며, 기술의 유출 및 침해사고 발생시 피해가 최소화되는 상태
70점 이상 ~85점 미만	**양호 수준** 보안에 대해 심각하지 않은 결점 및 취약성을 내포하며, 회사 차원의 보안업무가 나름대로 이루어지고 있는 상태
55점 이상 ~70점 미만	**보통 수준** 보안에 대해 일반적인 결점 및 취약성을 내포하며, 기술의 유출 및 침해정도에 따라 피해가 커질 수 있는 상태
40점 이상 ~55점 미만	**취약 수준** 보안에 대해 다소 심각한 결점 및 취약성을 내포하며, 기술의 유출 및 침해정도에 따라 치명적인 피해를 가져올 수 있는 상태
40점 미만	**위험 수준** 보안에 대해 심각한 결점 및 취약성이 상존하며, 기술의 유출 및 침해정도에 따라 치명적인 피해가 우려되는 상태

1. 보안정책(15점)

구 분	설 명	평 가	대 책
1.1	보안규정을 보유하고 있는가? ① 보유하고 있다 (2점) ② 보유하고 있지 않다 (0점)		p.39
1.2	회사의 보안정책, 지침, 절차 등의 내용에 대해 임직원들에게 공지하고 있는가? ① 공지하고 있다 (1점) ② 공지하고 있지 않다 (0점)		p.39
1.3	보안전담조직이 존재하는가? ① 보안전담조직과 보안담당자가 존재한다 (2점) ② 보안담당자만 존재한다 (1점) ③ 보안전담조직과 담당자 모두 존재하지 않는다 (0점)		p.39 ~ p.40
1.4	회사의 주요 정보(기술, 영업 등)는 어떻게 공유되는가? ① 업무담당자, 관계자 등 소수만이 볼 수 있다 (2점) ② 핵심정보를 제외하고는 직원들이 볼 수 있다 (1점) ③ 대부분의 정보에 대해서 직원들이 볼 수 있다 (0점)		p.39
1.5	임직원의 업무에 기밀사항의 보호 등 보안관련 내용이 포함되어 있는가? ① 포함되어 있다 (1점) ② 포함되어 있지 않다 (0점)		p.39 p.44
1.6	회사내 보안업무 수행을 위해 팀(혹은 그룹)간 업무 공조체계가 구성되어 있는? ① 구성되어 있다 (1점) ② 구성되어 있지 않다 (0점)		p.40

구 분	설 명	평 가	대 책
1.7	정기적으로 보안감사를 실시하고 있는가? ① 정기적으로 실시하고 있다 (2점) ② 필요할 때 수시로 실시하고 있다 (1점) ③ 실시하지 않고 있다 (0점)		p.40
1.8	회사가 보유한 주요 정보 및 자산을 보호하기 위해 투자하는 비용수준은 어떠한가? ① 기술적, 물리적, 관리적 보안을 위해 매년 일정비용 이상을 꾸준히 투자하고 있다 (3점) ② 특정 보안분야에 대해 필요시 비용투자가 이루어지고 있다 (1.5점) ③ 보안분야에 대한 투자가 이루어지고 있지 않다 (0점)		p.40 ~ p.41
1.9	보안업무 추진을 위해 외부 전문기관의 도움을 받고 있습니까? ① 도움을 받고 있다 (1점) ② 도움을 받고 있지 않다 (0점)		p.41

2. 자산관리(13점)

구 분	설 명	평 가	대 책
2.1	회사가 보유한 정보자산에 대해 목록 관리 등을 통한 관리기준을 수립하여 가지고 있는가? ① 그렇다 (2점) ② 그렇지 않다 (0점)		p.42 ~ p.45

구 분	설 명	평 가	대 책
2.2	회사의 정보자산을 그 중요성에 따라 '극비', '대외비', '일반' 등으로 등급을 구분하여 관리하고 있는가? ① 구분하여 관리하고 있다 (2점) ② 구분하지 않는다 (0점)		p.42 ~ p.44
2.3	회사의 정보자산에 대한 관리책임자를 지정하여 관리하고 있는가? ① 그렇다 (2점) ② 그렇지 않다 (0점)		p.44
2.4	회사의 정보자산 분류는 정기적으로 이루어지는가? ① 정기적으로 이루어진다 (2점) ② 필요시 이루어진다 (1점) ③ 이루어지지 않고 있다 (0점)		p.44
2.5	주요 기밀문서의 경우 어떻게 관리하고 있는가? ① 사용자별 권한 설정이 되어 있다 (2점) ② 사용자별 일부 권한 설정이 되어 있다 (1점) ③ 사용자별 권한 설정이 되어 있지 않다 (0점)		p.44 ~ p.45
2.6	특허, 실용신안, 디자인 등 지적재산권에 대한 관리방안이 마련되어 있는가? ① 권리출원 및 대응전략이 모두 마련되어 있다 (2점) ② 권리출원과 대응전략 중 하나만 마련되어 있다 (1점) ③ 마련되어 있지 않다 (0점)		p.46 ~ p.64
2.7	장비, 정보 또는 소프트웨어 등의 회사 자산의 반출은 어떤 식으로 이루어지는가? ① 사전 인가가 있어야만 반출이 가능하다 (1점) ② 사전 인가 없이도 반출이 가능하다 (0점)		p.45

3. 인적자원관리(20점)

구 분	설 명	평 가	대 책
3.1	신규 입사자에 대해 보안교육을 실시하고 있는가? ① 실시하고 있다 (1점) ② 실시하고 있지 않다 (0점)		p.68
3.2	기존 임직원을 대상으로 보안교육을 실시하고 있는가? ① 정기적으로 실시하고 있다 (2점) ② 필요시 실시하고 있다 (1점) ③ 실시하고 있지 않다 (0점)		p.70
3.3	임직원 보안의식을 제고하기 위해 퇴근시 혹은 자리 이탈시에 다음과 같은 활동을 수행하고 있는가? ① PC 전원 Off 여부 확인 ② 장시간 자리 이탈시 화면보호기 설정 여부 확인 ③ 노트북 방치 여부 확인 ④ 출입문, 캐비넷, 개인서랍 시건 여부 확인 ⑤ 문서 및 도면 방치 여부 확인 ※ 4개 이상 - 3점, 2~3개 - 2점, 1개 - 1점		p.40
3.4	신규 입사자에 대해 보안서약서를 징구하고 있는가? ① 보안서약서를 근로계약서와 별도로 징구하고 있다 (2점) ② 별도로 보안서약서를 징구하고 있지는 않지만, 고용계약서에 보안책임을 명시하고 있다 (1점) ③ 징구하고 있지 않다 (0점)		p.68
3.5	주요 R&D 프로젝트 참가자에 대해 보안서약서를 징구하고 있는가? ① 징구하고 있다 (2점) ② 징구하고 있지 않다 (0점)		p.69

구 분	설 명	평 가	대 책
3.6	종업원이 보안정책, 지침, 절차 등을 위반하는 직원에 대한 공식적인 징계 절차가 마련되어 있는가? ① 징계절차가 마련되어 있으며, 필요시 징계조치가 이루어진다 (2점) ② 징계절차는 마련되어 있으나, 징계조치는 거의 이루어지지 않는다 (1점) ③ 징계절차가 마련되어 있지 않다 (0점)		p.40 p.70
3.7	퇴직자에 대해 회사 정보자산의 유출방지를 위한 보안서약서를 징구하고 있는가? ① 징구하고 있다 (2점) ② 징구하고 있지 않다 (0점)		p.73
3.8	퇴직자의 향후 진로 및 동향을 파악하고 있는가 ? ① 모든 퇴직자의 동향을 파악하고 있다 (2점) ② 주요 임직원에 한하여 파악하고 있다 (1점) ③ 전혀 파악하고 있지 않다 (0점)		p.73
3.9	제3자(협력업체, 외국인 등)에 대한 관리를 하고 있는가? ① 별도의 관리방안이 마련되어 있으며, 대상자에 대한 보안서약을 하고 있다 (2점) ② 별도의 관리방안은 마련되어 있지 않으나, 대상자에 대한 보안서약은 하고 있다 (1점) ③ 별도의 관리방안이 마련되어 있지 않으며, 대상자에 대한 보안서약도 하고 있지 않다 (0점)		p.71 ~ p.72 p.74
3.10	회사의 정보자산에 대한 사용자(임직원, 계약자, 제3의 사용자 등)들의 접근권한은 퇴사, 계약종료, 역할 조정 등의 사유발생시 조정되어지고 있는가? ① 사유발생 즉시 조정되어진다 (2점) ② 사유발생 1주일 이내에 조정되어진다 (1점) ③ 조정이 지연되거나 이루어지지 않는다 (0점)		p.73

4. 시설관리(12점)

구 분	설 명	평 가	대 책
4.1	회사 내 중요시설에 대한 관리기준이 있는가? ① 관리기준이 존재한다 (2점) ② 관리기준이 존재하지 않는다 (0점)		p.81 ~ p.84
4.2	협력업체, 방문객 등 외부인의 회사 내 출입절차가 존재하는가? ① 출입절차가 존재하며, 출입관리대장을 기재한다 (2점) ② 출입절차가 존재하지만, 출입관리대장은 기재하지 않는다 (1점) ③ 별도의 출입절차가 존재하지 않는다 (0점)		p.81 ~ p.84
4.3	회사 내 중요시설에 대해 출입통제시스템을 설치하여 운영하고 있는가? ① 출입통제시스템을 운영하고 있으며, 내부의 한정된 인원만 출입이 가능하다 (2점) ② 출입통제시스템을 운영하고 있으며, 내부 인원은 자유로이 출입이 가능하다 (1점) ③ 출입통제시스템을 운영하고 있지 않으며, 내외부 인원의 자유로운 출입이 가능하다 (0점)		p.81 ~ p.84
4.4	외부인 식별을 위하여 임직원의 사원증 패용을 의무화하고 있는가? ① 의무화 하고 있다 (1점) ② 의무화 하고 있지 않다 (0점)		p.81 ~ p.84
4.5	건물 출입구나 중요시설에 대해 CCTV 등의 감시장치가 설치되어 있는가? ① 설치되어 있다 (2점) ② 설치되어 있지 않다 (0점)		p.81 ~ p.84

구 분	설 명	평 가	대 책
4.6	중요시설 및 통제구역에 대해 화재, 전원, 수해 등으로부터의 보호방안이 강구되어 있는가? ① 보호방안이 강구되어 있다 (2점) ② 보호방안이 강구되어 있지 않다 (0점)		p.84
4.7	회사 내 중요시설에 카메라, 비디오 카메라 등의 장비 반입이 규정에 의해 통제되고 있는가? ① 규정에 의해 통제되고 있다 (1점) ② 규정에 의해 통제되고 있지 않다 (0점)		p.81 ~ p.84

5. IT보안관리(30점)

구 분	설 명	평 가	대 책
5.1	다음과 같은 정보처리 설비의 운영절차가 문서화되어 규정되어 있는가? ① 컴퓨터의 가동과 종료절차 ② 백업절차 ③ 유지 보수절차 ④ 예상치 못한 운영상 또는 기술적인 어려움 발생시 지원연락처 ⑤ 비밀정보를 포함한 출력물의 관리 및 폐기절차 준수 ⑥ 시스템 오작동시 시스템의 재시작 및 복구절차 준수 ※ 해당되는 문항마다 0.5점		p.89 ~ p.90

구 분	설 명	평 가	대 책
5.2	통신망에 대한 보안점검을 실시하고 있는가? ① 보안상태에 대해 주기적으로 점검하고 있다 (2점) ② 필요가 있을 때만 실시하고 있다 (1점) ③ 보안점검을 실시하고 있지 않다 (0점)		p.89
5.3	서버 및 DB 현황에 대한 보안점검을 실시하고 있는가? ① 보안상태에 대해 주기적으로 점검하고 있다 (2점) ② 필요가 있을 때만 실시하고 있다 (1점) ③ 보안점검을 실시하고 있지 않다 (0점)		p.89
5.4	바이러스 침입, 해킹, 내부로부터의 정보유출을 방지하기 위한 대책을 강구하고 있는가? ① 각종 보안솔루션을 도입하여 사용하고 있다 (3점) ② 일부 보안솔루션을 도입하여 사용하고 있다 (1.5점) ③ 보안솔루션 도입은 아직 이루어지고 있지 않다 (0점)		p.87 ~ p.88
5.5	내부에서 생성된 주요 정보 및 소프트웨어는 백업되어 관리되고 있는가? ① 정기적으로 백업하여 관리하고 있다 (2점) ② 필요시 백업하여 관리하고 있다 (1점) ③ 백업하여 관리하고 있지 않다 (0점)		p.89
5.6	지식관리시스템(KMS), 전자결재시스템 등 회사 내 주요 정보에 대한 관리시스템이 존재하는가? ① 관리시스템이 존재하며, 권한에 따라 정보의 공유가 이루어진다 (2점) ② 관리시스템이 존재하며, 모든 임직원들에게 정보의 공유가 이루어진다 (1점) ③ 관리시스템이 존재하지 않는다 (0점)		p.87 ~ p.88

구 분	설 명	평 가	대 책
5.7	FD, CD, USB 등 정보의 저장이 가능한 매체에 대한 관리절차가 마련되어 있는가? ① 관리절차가 마련되어 있다 (2점) ② 관리절차가 마련되어 있지 않다 (0점)		p.86 ~ p.87
5.8	외부로의 전자문서 발송에 대한 통제시스템이 마련되어 있는가? ① DRM, DMS 등 문서관리시스템이 마련되어 있다 (2점) ② 문서관리시스템은 마련되어 있지 않으나, 중요 문서에 한해 사전승인을 필요로 한다 (1점) ③ 전자문서 발송에 대한 통제가 존재하지 않는다 (0점)		p.87 ~ p.88
5.9	PC 및 주요 시스템 사용자에 대한 패스워드 관리를 하고 있는가? ① 정례적으로 패스워드를 변경하고 있으며, 이를 수시로 점검한다 (2점) ② 정례적으로 패스워드를 변경할 것을 권장하고 있으나, 이행여부를 점검하지는 않는다 (1.5점) ③ 각 시스템에 패스워드를 사용한다 (1점) ④ 각 시스템에 대한 패스워드 사용을 강제하지 않는다 (0점)		p.85
5.10	임직원이 장기간 자리를 이석하는 경우 어떠한 조치를 취하고 있는가? ① 화면보호기 작동 및 패스워드를 사용한다 (2점) ② 별다른 조치를 취하지 않는다 (0점)		p.82 p.85
5.11	내부 통신망과 외부 통신망(인터넷, 협력회사 등)을 분리하여 운영하고 있는가? ① 분리하여 운영하고 있다 (2점) ② 함께 사용하고 있다 (0점)		p.88

구 분	설 명	평 가	대 책
5.12	정보시스템의 사용 내용에 대한 로그를 기록하고 유지하는가? ① 로그를 기록하고 일정 기간 동안 보관한다 (2점) ② 로그를 기록하지만 용량의 문제로 단기간 동안만 보관한다 (1점) ③ 로그를 기록하지 않는다 (0점)		p.89
5.13	주요 장애 발생시 장애내용이 보고되어 신속하게 시정조치가 이루어지는가? ① 장애내용이 보고되어 신속한 시정조치가 이루어진다 (2점) ② 장애내용은 보고되지만 시정조치는 다소 지연되는 경향이 있다 (1점) ③ 장애내용은 보고되지 않지만, 시정조치는 신속하게 이루어진다 (1점) ④ 장애내용이 보고되지 않으며, 시정조치도 다소 지연되는 경향이 있다 (0점)		p.90
5.14	정보시스템에 대한 유지보수를 실시하고 있는가? ① 정보시스템 설치 업체와의 계약을 통해 정기적으로 유지보수를 실시하고 있다 (2점) ② 문제 발생시에만 관련 업체에 요청하여 유지보수하고 있다 (1점) ③ 유지보수를 하고 있지 않다 (0점)		p.90

6. 유출사고의 대응(10점)

구 분	설 명	평 가	대 책
6.1	정보시스템에 대한 재해발생시 다음과 같은 대응절차가 수립되어 있는가? ① 비상시 따라야 할 절차와 관련자의 책임규정 ② 유관기관과의 연락체계 구성여부 ③ 제한된 시간 내에 필수 업무 및 지원서비스를 대체장소로 이전하여 운영하기 위한 절차 ④ 정상적인 사업 활동으로 복귀하기 위한 원상복귀 절차 ⑤ 위기관리를 포함한 비상절차 및 프로세스에 대한 임직원 교육 ※ 해당되는 문항마다 1점		p.90
6.2	기술유출 및 침해사고 발생시 회사 차원의 대응방안이 마련되어 있는가? ① 구체적으로 마련되어 있다 (3점) ② 일부분이 마련되어 있다 (1점) ③ 마련되어 있지 않다 (0점)		p.115 ~ p.139
6.3	부정경쟁방지 및 영업비밀 보호에 관한 법률, 산업기술의 유출방지 및 보호에 관한 법률, 국가연구개발사업 공통보안지침 등 기술유출 방지와 관련된 주요 법규에 대해 인지하고 있는가? ① 법규의 내용 대부분에 대해 알고 있다 (2점) ② 법규의 내용 일부분에 대해 알고 있다 (1점) ③ 법규의 내용에 대해 거의 알지 못한다 (0점)		별책 제1장

제 3 장 기술유출 사전 대응방안

제1절 보안정책

□ 보안관리규정 제정 및 시행

○ 기업의 비밀정보를 효과적으로 관리하고 보호하기 위해서는 보안관리에 관한 명문화된 규정을 제정하여 시행하여야 함

○ 보안관리규정은 기업의 정보자산을 보호하기 위해 가장 기본이 되는 것이며, 규정 제정시 다음과 같은 사항을 고려해야 함

- 내용이 모호해서는 안되며, 표현이 정확해야 함
- 이해하기 쉬워야 함
- 선언적이기 보다는 구체적인 실행이 가능해야 함
- 내용이 자세하게 언급되어 있어야 함

○ 보안관리규정은 주기적으로 개정해야 하며, 개정이 되었을 경우 모든 임·직원에게 그 내용을 공지해야 함

- 보안규정을 적용함에 있어 만들어지는 지침과 절차의 경우에도 임직원들이 그 내용을 인지할 수 있도록 조치해야 함

○ 보안관리규정에는 보안 업무의 분류, 보안업무의 조직 및 기능, 자산의 분류와 관리, 인적자원관리, 시설관리 및 침입방지, IT보안관리, 보안규정 위반자 조치사항 등이 언급되어 있어야 함

○ 보안관리규정 내용은 <별책 p.77> 참조

□ 보안조직의 구성 및 운영

○ 규모가 큰 기업의 경우 보안전담조직을 구성하여 운영하는 것이 가장 바람직하나, 그렇지 못한 경우 보안담당자를 지정하여 담당자로 하여금 업무를 수행하도록 해야 함

○ 각 부서의 장을 보안책임자로 임명하여 보안업무를 수행하도록 하고, 직원 개개인의 업무에 보안관련 내용을 포함시켜야 함

- 업무상 생성되는 주요 정보에 대한 취급권한을 명확하게 하여 회사 임직원들이 업무와 무관한 정보에 접근하는 것을 차단해야 함

○ 인사, 총무, 관리, IT 등 경영지원 각 분야에서 종합적으로 보안업무를 지원하고, 각 부서의 장을 위원으로 하는 보안관리위원회를 구성하여 부서 상호간의 업무공조를 도모해야 함

- 보안관리위원회의 경우 회사 내 보안업무의 의사결정기관으로 보안규정의 제·개정, 주요 보안정책에 대한 결정, 보안위규자 징계 등의 업무를 수행할 수 있음

□ 보안감사

○ 보안업무의 실효성을 확보하기 위해 회사의 보안상황 전반에 대해 1년에 최소 1회 이상의 정기적인 감독활동이 이루어져야 함

- 문서(전자문서 포함), 인적자원, 시설, 전산 분야의 보안활동 전반에 대한 점검활동이 요구됨

○ 정기적인 감독활동 이외에 임직원의 보안마인드 제고를 위해 다음 사항에 대해 수시로 보안점검 활동이 이루어져야 함

- 대외비 정보(문서 및 도면) 방치 여부
- 개인서랍, 캐비넷, 출입문 시건 여부
- 개인휴대용 정보저장매체(카메라폰, PDA, PMP 등) 출입규정 준수여부
- PC DATA 공유설정 여부(화면보호기, Password 등)
- 사내 사용허가 전산저장매체(노트PC, 디지털촬영기기, CD/DVD RW, USB Memory 등) 관리현황

○ 정기 및 수시 보안감사 결과에 따른 유공자 포상과 위반자 징계 활동을 병행하여야 함

□ 보안투자

○ 보안업무의 경우 당장의 성과로 이어지지 않기 때문에 중소기업의 경우 보안업무 추진을 위한 투자에 인색하기 마련임

○ 하지만 기업의 형편에 맞게 우선순위를 정해 매년 일정비용을 지속적으로 투자하는 것이 중요함

○ 효율적인 투자를 위해서는 정부의 다양한 지원제도를 활용할 필요가 있음

- 기업의 기술유출방지설비에 대한 투자금액의 3% 세액공제(<별책 p.24> 참조)
- 정부의 보안설비 구축 지원사업(<표3-1> 참조)

□ 외부 전문기관 활용

○ 기술, 영업 등 회사의 주요 기밀정보를 보호하기 위해서는 기업 스스로의 노력이 가장 중요하지만, 유출 및 침해사건 발생시 즉각적인 대응 및 피해의 최소화를 위해 외부의 전문기관을 적절히 활용해야 함

<표3-1> 주요 기관별 산업보안 지원내용

기관명	지원 내용
정 부	· 산업기술 보호 설비 구축에 필요한 기술 및 경비 지원 · 산업보안기술의 개발지원 · 산업기술 보호교육 · 산업기술보호 유공자 포상 · 국제협력사업
국가정보원 산업기밀 보호센터	· 산업기술 유출방지 활동 및 보호조치 · 국가 연구개발사업 보안실태 점검 및 보안관리 · 산업스파이 신고상담소 운영 · 지적재산권 침해 대응 활동 · 산업보안 설명회 및 워크숍 개최 · 산업보안협의회 운영 · 산업보안 관련 정책자료 제작/지원
경 찰 청	· 산업기술유출 신고접수 · 산업기술유출 수사 · 산업보안협의회 운영 · '산업스파이신고 접수' 온라인 운영
특 허 청	· 특허법률 구조 지원 · 산업재산권 분쟁조정 지원 · 위조상품 신고포상금 제도 운영 · 해외 지식재산권 보호센터 운영

제2절 자산관리

1. 자산의 분류 및 관리

□ 자산목록(Asset Inventory) 관리

○ 자산을 분류하고 자산별 소유관계와 등급을 명확히 정의하여 이를 문서화해야 함

○ 자산관리의 효율성을 위하여 부서별 자산목록과 회사 전체의 자산목록으로 구분하여 관리해야 함

○ 연말기준 보유 자산목록을 보안관리위원회에 보고해야 함

□ 자산의 분류

○ 자산은 그 유형에 따라 다음과 같이 분류할 수 있으며, 그 중요성에 따라 등급을 구분하여 관리해야 함

<표3-2> 자산의 분류

구 분	세 부 내 용
정 보	· 기업이 보유/관리하고 있는 모든 종류의 정보 - R&D정보, 영업정보, 조직정보, 임직원정보 등
문 서	· 기업이 보유/관리하고 있는 모든 문서(전자, 출력) - 정책/지침, 업무관련 문서, 인사기록, 송장 등
인 력	· 기업과 관련있는 모든 인원 - 내부직원, 퇴직자, 협력업체, 고객 등
소프트웨어	· IT시스템에서 사용되는 프로그램 - 운영시스템, 어플리케이션 프로그램, 통신 프로그램 등
설 비	· 업무에 활용되는 하드웨어 - 업무용 서버, 책상, 의자, 캐비넷 등
기 타	· 외부기관으로부터 제공받는 서비스 - 정보서비스, 통신서비스 등

○ 자산은 그 중요성에 따라 일반적으로 3등급으로 구분하며, 비밀성·무결성·가용성을 고려하여야 함

1) 등급분류 원칙

- 비밀정보는 내용의 가치에 따라 분류하되 과대평가나 과소평가하여 분류하지 않아야 함. 과대분류는 필요이상의 제한으로 업무의 지장을 초래하고, 과소분류는 비밀에 대한 관리소홀로 비밀의 주요 내용이 유출될 수 있음
- 동일한 업무의 문서라도 각각의 비밀내용과 가치에 따라 독립적으로 분류해야 함
- 기업의 비밀등급 분류시 그 명칭이나 등급의 분류기준 모두 기업의 재량이나 일반적으로 업무의 성격, 보호 필요성, 회사에 대한 기여도 등을 종합적으로 고려하여 판단하여야 함
- 중소기업의 경우 위의 분류원칙에 따라 일반적으로 3등급으로 구분하는 것이 바람직하나, 규모가 크거나 보호해야 할 자산이 많은 기업의 경우 1등급의 기밀정보를 '극비'와 '비밀'로 다시 세분하기도 함

2) 등급 분류

- 1등급 : 기밀정보(In-Confidence)
  · 개발소프트웨어 소스코드, 개발설계서, 고객비밀정보 등 회사 내에서도 접근권한이 부여되는 민감한 정보
- 2등급 : 대외비 정보(Internal Use Only)
  · 회사 임직원에게는 공개되나 대외적으로는 비밀로 유지하는 정보
- 3등급 : 일반정보(Public)
  · 회사소개 자료, 제품 설명자료 등 외부에 공개 가능한 정보

3) 특성

- 비밀성(Confidentiality)
  · 정보의 소유자가 원하는 대로 정보의 비밀이 유지되어야 함

- 무결성(Integrity)

  · 비인가된 자에 의한 정보의 변경, 삭제, 생성 등으로부터 보호하여 정보의 정확성과 완전성이 보장되어야 함

- 가용성(Availability)

  · 정보시스템은 적절한 방법으로 작동되어야 하며, 정당한 방법으로 권한이 주어진 사용자에게 정보 서비스를 거부하여서는 안됨

○ 소유 중인 모든 자산은 소유자가 년 1회 주기적으로 자산의 가치를 검토하여 재분류하여야 함

□ 자산의 등록 및 관리

○ 각 부서별로 자산관리책임자를 지정하고, 회사 전체의 자산관리책임자가 총괄하여 관리함

- 형편상 자산관리책임자를 별도로 지정하기 곤란하면, 보안관리책임자가 업무를 병행하도록 조치해야 함

○ 신규 자산의 등록은 소유자가 필요시 부서장의 허가를 득하여 부서의 자산목록에 직접 등록하고, 각 부서의 담당자는 신규 등록된 자산에 대해 회사 전체의 자산관리책임자에게 보고한 후 자산코드를 부여하여 관리하여야 함

○ 자산의 최종소유자는 해당 자산에 대한 최종 승인권자(임원)이며, 자산에 대한 관리 및 배포권한을 가짐

○ 회사를 위해 협력업체 등 제3자가 생성한 정보자산의 지적소유권을 회사에 귀속시켜야 함

□ 자산의 접근권한

○ 회사 임직원과 협력업체 등 제3자의 경우 자산에 대한 접근권한은 최소범위 내에서 부여해야 하며, 알아야 할 필요가 있는 자에 국한하여야 함

- 업무와 무관한 어떠한 자산에도 접근하지 못하도록 통제해야 함

○ 자산에 대한 접근권한은 자산의 소유자 또는 권한을 위임받은 관리자(전산정보팀)에 의해 부여됨

○ 관리자는 사용자의 접근권한을 정기적으로 점검하고, 사용자의 입・퇴사, 계약종료, 역할조정 등 사유발생시 재설정 할 수 있음

□ 자산의 반출

○ 1등급(기밀) 정보의 경우 임원(예: 연구소장, 영업본부장 등), 2등급 정보의 경우 부서장의 사전승인 없이 외부로 유출 또는 공개해서는 안됨

- 외부공개 결정시 사전에 반드시 보안성 검토를 해야 하며, 공개내용 등 관련 기록을 보관, 유지하여야 함

○ 자산의 반출이 발생할 경우 목록관리대장에 기록

□ 자산의 폐기

○ 자산의 폐기는 폐기사유가 발생한 시점에 소유자가 최종 승인권자(임원)의 허가를 득한 후 폐기처리

○ 컴퓨터와 CD등 정보저장매체의 경우 폐기시 일반 장비와 동일하게 처리해서는 안되며, 해당 장비에 대한 폐기절차가 반드시 필요함

- 하드디스크의 경우 Low Format을 3~4회 하여도 일부 정보를 되살릴 수 있기 때문에, 본체와 하드디스크를 분리하여 재사용 금지를 위해 강한 자기장으로 자성을 완전히 삭제하고 그 후 물리적으로 파괴하여 폐기해야 함

○ CD의 경우 손으로 부러뜨렸을 경우 80% 이상, 잘게 부수었을 경우에도 30% 이상의 내용 복구가 가능하기 때문에 CD의 내용을 완전히 폐기하는 장비(예: DX-CD2 등)를 구비하여 사용할 필요가 있음

○ 자산의 반출과 폐기가 발생할 경우 목록관리대장에 기록

2. 지적재산권 권리화 및 보호

□ 연구개발 성과의 권리화

○ 산업재산권의 개념

- 산업활동과 관련된 사람의 정신적 창작물(연구결과)이나 창작방법에 대해 인정하는 독점적 권리인 무체재산권을 의미함
- 새로운 발명 등에 대하여 그 발명자 및 승계인 등에게 일정기간 동안 독점배타적인 권리를 부여하는 대신, 이를 일반에게 공개하여야 하며 일정 존속기간이 지나면 누구나 이용·실시하도록 함으로써 기술진보와 산업발전을 추구

○ 산업재산권 확보의 필요성

1) 시장에서 독점적 지위 확보

- 특허 등 산업재산권은 독점배타적인 무체재산권으로 신용창출, 소비자의 신뢰도 향상 및 기술판매를 통한 로열티 수입이 가능함

2) 특허분쟁의 사전 예방

- 자신의 발명 및 개발기술을 적시에 출원하여 권리화함으로써 타인과의 분쟁을 사전에 예방하고, 타인이 자신의 권리를 무단으로 사용할 경우 법적 보호가 가능함

3) R&D 투자비 회수 및 향후 추가 기술개발의 원천

- 막대한 기술개발 투자비를 회수할 수 있는 확실한 수단이 되며 확보된 권리를 바탕으로 타인과 분쟁 없이 추가 응용 기술개발 가능

4) 정부의 각종 정책자금 및 세제지원 혜택

- 특허, 실용신안 등 산업재산권을 보유하고 있는 경우 벤처기업으로 인정을 받아 각종 벤처기업 지원 혜택을 비롯, 정부자금 활용과 세제지원 혜택을 받을 수 있음

○ 산업재산권의 종류

- 산업재산권은 특허권, 실용신안권, 디자인권 및 상표권을 총칭하며, 이 중 특허권이 대표적임

<표3-3> 산업재산권의 종류

구 분	정 의	예 시	존속기간
특 허	아직까지 없었던 물건 또는 방법을 최초로 발명한 것(대발명)	벨이 전자를 응용하여 처음으로 전화기를 생각해 낸 것과 같은 발명	설정등록일로부터 출원일 후 20년까지
실 용 신 안	물건에 대한 간단한 고안(소발명)이나 이미 발명된 것을 개량해서 보다 편리하고 유용하게 쓸 수 있도록 한 물품에 대한 고안	분리된 송수화기를 하나로 하여 편리하게 한 것과 같은 형상이나 구조 등에 관한 고안	설정등록일로부터 출원일 후 10년까지
디자인	물품의 형상, 모양, 색채 또는 이들을 결합한 것으로서 시각을 통하여 미감을 느끼게 하는 것	탁상전화기를 반구형이나 네모꼴로 한 것과 같이 물품의 외관에 대한 형상, 모양, 색채에 관한 디자인	설정등록일로부터 15년까지
상 표	타인의 상품과 식별하도록 하기 위하여 사용되는 기호, 문자도형, 입체적 형상, 색채, 홀로그램, 동작 또는 이들을 결합한 것, 그 밖에 시각적으로 인식할 수 있는 것으로서 타인의 것과 명확히 구분되는 것	전화기 제조회사가 자사제품의 신용을 유지하기 위해 제품이나 포장 등에 표시하는 표장으로서의 상호, 마크 등	설정등록일로부터 10년(10년마다 갱신가능, 반영구적 권리)

□ 지적재산 권리의 보호

○ 담당부서 설치 및 전담자 지정

- 특허분쟁 발생시 경영진을 보좌하여 신속하고 적절한 조기대응을 하기 위해서는 사내에 특허담당부서가 설치되어 있어야 함

- 중소기업의 경영환경상 특허담당부서를 설치하기가 용이하지 않을 경우 자사의 특허기술 분석, 경쟁기업의 특허활동 감시, 미래의 분쟁 가능성 대비 등에 대한 업무수행을 위해 특허전담자를 우선적으로 지정

○ 제품출시보다 특허출원 우선

- 특허제도는 발명을 공개하는 대가로 특허권을 부여하는 제도이므로 이미 일반에 알려진 발명에 대해서는 특허권을 부여하지 않음

- 따라서 새로 개발한 기술에 대한 특허를 출원하기 전에 제품을 출시하거나 광고 등을 통해 이미 대중에 공개되어 있다면, 추후에는 특허를 받을 수 없으므로, 반드시 공개 이전에 특허 출원을 먼저 하는 것이 무엇보다 중요함

- 특허출원을 하기 전에 제품출시 또는 제품광고를 하게 되면 누구나 합법적으로 동일한 제품을 만들어 판매하는 것이 가능하게 되므로 경쟁업체에게 뜻밖의 이익을 안겨주는 결과가 됨

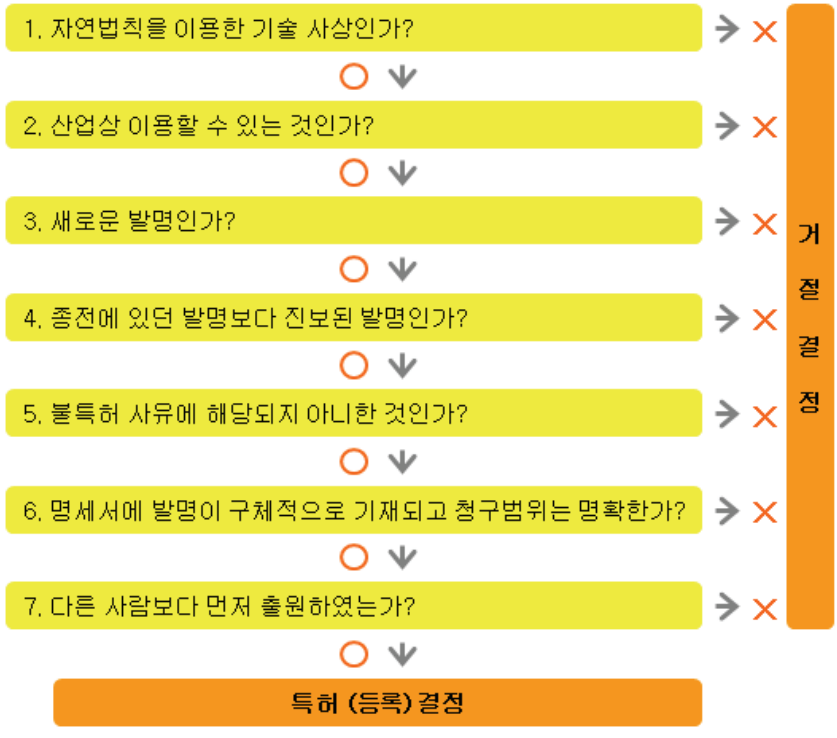
<사례> 일본의 마루나사 vs 나성준 사건

- 일본의 마루나사는 마루나 연사기에 관한 실용신안을 일본 및 한국에 출원하여 등록을 받음
- 그 후 한국의 나성준이 동제품을 생산하여 판매에 나서자 마루나사는 나성준을 상대로 특허침해 소송을 제기
- 그러나 마루나사가 특허를 출원하기 전 이미 제품의 카탈로그 및 팜플렛을 한국에 다량 배포하였고, 제품에 대해 누구나 쉽게 알 수 있는 상태가 되었다는 점이 인정되어 패소함

□ 특허 권리취득 절차[1)]

○ 등록요건

<그림3-1> 특허와 실용신안 등록요건



- 특허(등록) 결정을 받을 수 없는 발명

・공공질서 또는 선량한 풍속을 문란하게 하거나 공중의 위생을 해칠 염려가 있는 발명(예: 지폐위조기, 도박에 필요한 기구, 아편흡입기구 등에 관한 발명)

・국방상 필요한 경우(정부는 정당한 보상금 지급)

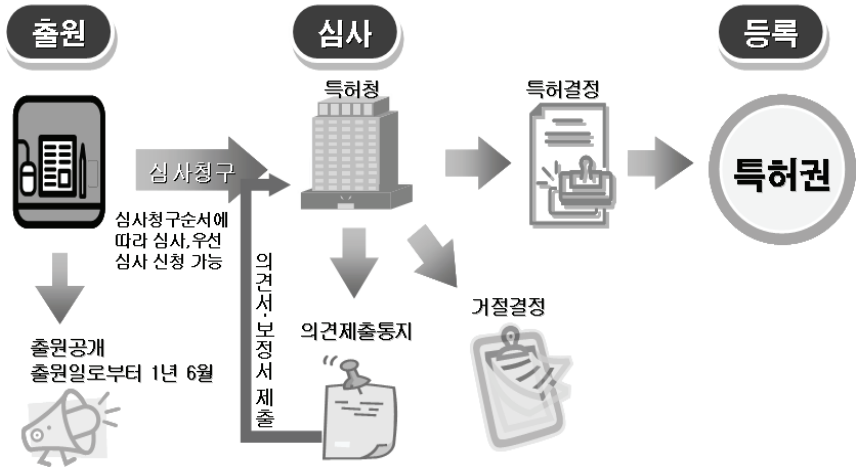
1) 지난 2006년 10월 1일부터 새롭게 개정된 특허법이 시행됨에 따라 본문의 내용은 2006년 10월 1일 이후 출원・등록하는 특허와 실용신안을 중심으로 기술하였으며, 「중소기업을 위한 지식재산 관리 매뉴얼(2006.3, 대한변리사회)」을 참고함

○ 특허 권리취득 절차

- 특허출원이란 새로운 발명을 한 사람이 그 발명을 공개하는 대가로 독점권을 갖기 위해 특허를 허락해 달라고 국가(특허청)에 일정한 양식 및 절차에 따라 신청하는 행위를 의미함

- 특허청은 이러한 신청을 받게 되면 절차와 양식이 맞게 되었는지를 보고 제대로 된 출원에 대하여 특허권을 허여하여야 할 일정한 요건을 갖추었는지를 심사하여 특허 여부를 결정하게 됨

<그림3-2> 특허 권리취득 절차



○ 특허출원 서류의 제출

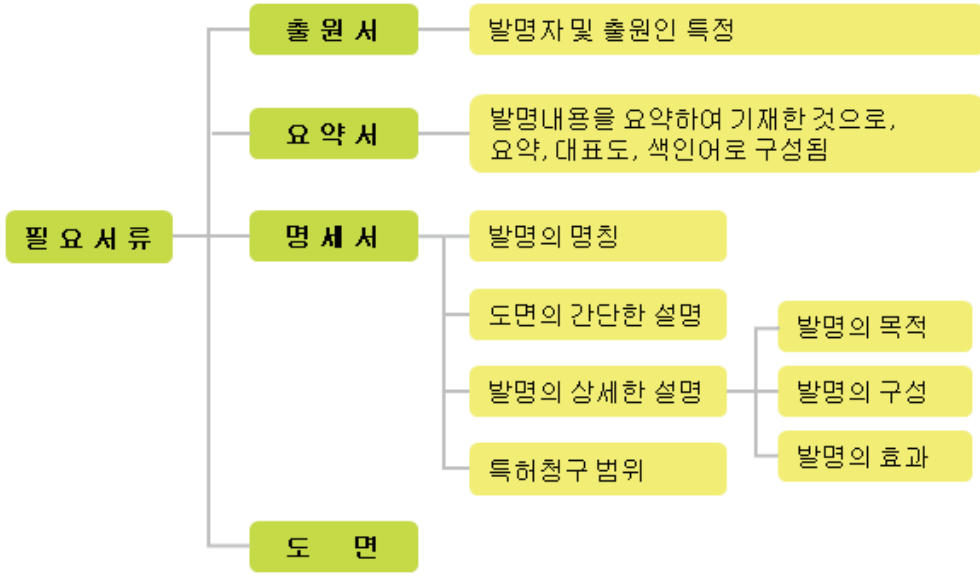
- 특허출원을 하려고 하는 경우, 소정사항을 기재한 「특허출원서」를 특허청에 제출하여야 함

  · 특허출원서에는 요약서, 명세서, 도면(필요한 경우)이 첨부되어야 함

- 특허출원서류를 작성할 때에는 특허출원서, 요약서, 명세서의 순으로 작성하고, 그 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 출원인이 제출한 출원서류에 기재된 내용을 보고 용이하게 실시할 수 있을 정도로 그 발명의 목적, 구성, 효과를 구체적으로 기재하여야 함[2)]

2) 특허출원서, 요약서, 명세서 등의 서식은 특허청 홈페이지(www.kipo.go.kr)에서 다운로드 받을 수 있음

<그림3-3> 특허출원시 필요한 서류



○ 특허의 심사절차

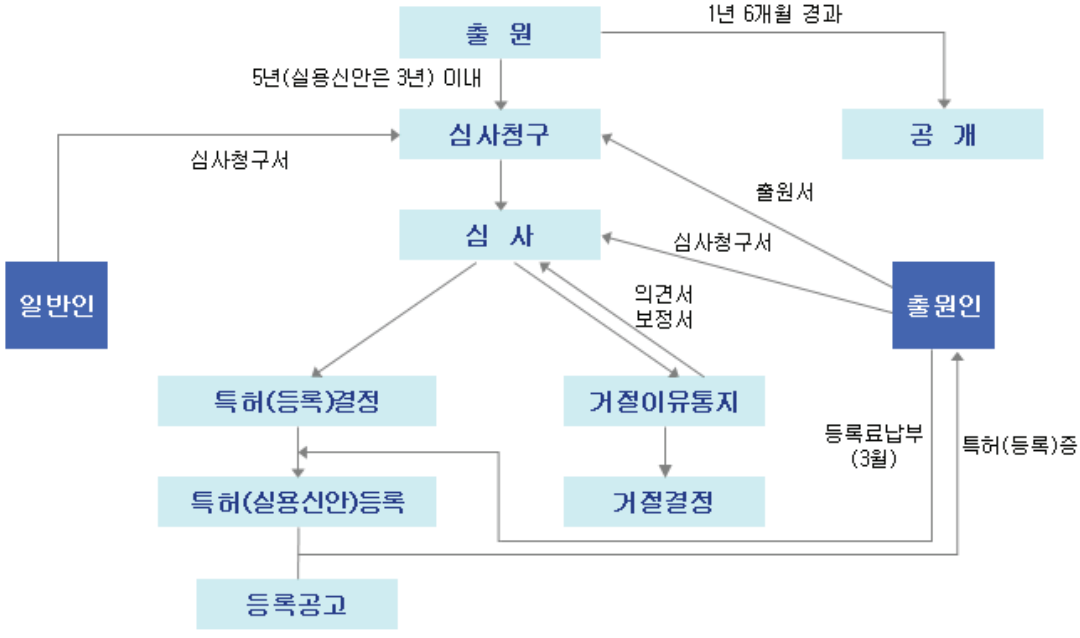
1) 방식심사

- 방식심사는 출원서나 명세서 등의 출원서류가 특허법에서 정하고 있는 절차적, 형식적 요건을 구비하고 있는지 여부를 심사하는 것을 말함

- 특허출원된 전부에 대하여 심사하는 것으로, 특허 허여 여부를 심사하는 「실체심사」와 구별됨

- 전자출원의 경우 자동적으로 체크가 되기 때문에 수수료 미납 등 일부 예외를 제외하고는 출원 전에 문제가 있는지 여부가 확인될 수 있음

<그림3-4> 특허(실용신안) 출원 및 심사절차



2) 출원공개

- 특허출원과 실용신안출원에 대하여 그 출원일(우선권 주장시 우선일)로부터 1년 6개월 후 또는 출원인의 조기공개 신청이 있을 때 특허청은 기술내용을 「공개특허공보」에 게재하여 일반인에게 공개

※ 정보제출 : 출원공개 전에도 출원계속 중이면 누구든지 당해 발명(고안)이 특허(등록결정)될 수 없다는 취지의 정보를 증거와 함께 특허청장에게 제출할 수 있음(2006. 10. 1 정보제공 건부터 적용)

- 출원공개 후부터 특허권의 설정등록까지의 기간 동안 출원공개된 발명을 업으로서 실시한 자에 대하여 미리 서면으로 경고함으로써, 특허권 설정등록 후 실시료 상당액의 지급을 청구할 수 있는 '보상금 청구권' 이라는 권리가 출원인에게 부여됨

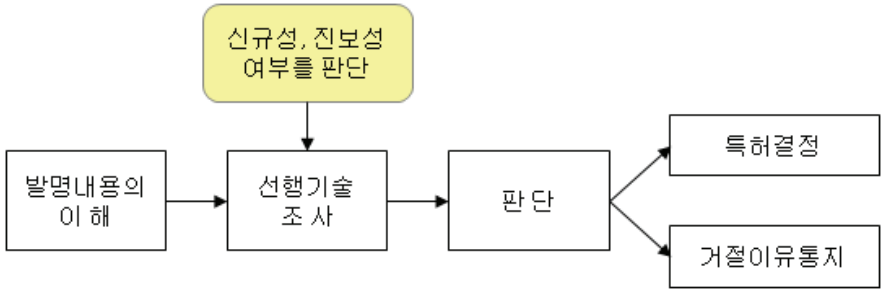
3) 심사청구

- 심사는 출원일로부터 5년(실용신안은 3년) 이내에 「출원심사청구서」를 제출하고, 심사청구료를 납부함으로써 개시되며, 심사청구기간 중에 심사청구를 하지 않는 경우에는 출원이 취하한 것으로 간주됨

4) 실체심사

- 심사청구된 출원은 심사관에 의해 특허 허여 여부에 관한 실질적인 심사가 진행됨

<그림3-5> 특허심사의 내용



① 거절이유의 통지

- 실체심사단계에서 심사관이 심사한 결과, 거절이유에 해당한다는 심증을 얻는 경우에는 바로 거절결정하지 않고, 그 취지를 출원인에게 통지하는 절차를 의미하며, 거절이유의 통제는 '의견제출통지서'라는 양식으로 출원인(또는 대리인)에게 발송됨

- 통지된 거절이유의 대부분은 선행기술이 기재되어 있는 문헌이 인용참증으로 제시된 후 발명으로서 신규하지 않다든지(신규성 결여), 용이하게 발명할 수 있다든지(진보성 결여), 또는 명세서의 표현이 명료하지 않다든지(기재불비) 하는 이유 등임

② 의견서, 보정서의 제출

- 특허심사관의 의견제출통제서에 대한 의견서나 보정서를 제출

③ 심사관 면담

- 의견제출통지서를 받은 경우 의견서나 보정서를 제출하기 전에 직접 심사관과의 면담을 통해 거절이유에 대한 의견을 청취하고 자기가 출원한 발명에 대한 기술적인 설명이나 인용된 문헌과 기술적 대비에 대하여 의견을 말하고 심사관에게 직접 이해를 구해 의견서나 보정서에 반영시킬 수 있음

5) 최종처분

- 실체심사는 심사관의 결정에 의해 종료되며, 심사관에 의한 최종 처분은 특허를 허여하는 「특허결정」과 특허권이 부여되지 않는 「거절결정」의 두 종류가 존재함

① 특허결정

- 심사관이 심사한 결과, 거절이유를 발견할 수 없었던 경우 또는 거절이유를 발견하였지만 의견제출 통지에 대한 출원인의 의견서 또는 보정서에 의하여 거절이유가 해소된 경우 심사관은 그 특허출원에 대하여 특허를 허여한다는 취지의 결정을 함

② 거절결정

- 심사관이 통지한 거절이유에 대하여 출원인이 의견서 또는 보정서를 제출하였지만 거절이유를 극복하지 못한 것으로 판단되는 경우 심사관은 그 특허출원에 대하여 거절결정을 함
- 출원인은 거절결정에 대하여 순차적으로 거절결정불복심판, 심결취소의 소 등을 제기할 수 있음

3. 영업비밀 보호

□ 영업비밀의 개념

○ 영업비밀(Trade Secret)이란 공연히 알려져 있지 아니하고 독립된 경제적 가치를 지니는 것으로서 상당한 노력에 의하여 비밀로 유지된 생산·판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 의미함

- 기술정보 : 생산 및 제조공정, 제조방법 등

<표3-4> 기술상의 영업비밀

대 상	설 명	비 고
시설 및 제품의 설계도	중요 공장의 설계도면, 기계장치의 배치도, 제품 생산 라인의 설계도, 공정 설계도	그 회사만의 독자적이며, 미공개된 정보나 자료
물건의 생산 및 제조방법	제품의 생산, 가공, 조립 또는 제조방법으로 비법이거나 미공개된 것	
물질의 배합방법	물질을 생성하는 반응순서, 원료의 배합순서, 배합비율, 시차 등으로서도 미공개 되고, Reverse Engineering으로 알아낼 수 없는 것	식품이나 음식의 제조비법, 의약품이나 화공약품의 제조생산 방법 등
연구개발 보고서 및 데이터	연구개발과정, 결과보고서 및 연구에 사용된 데이터	연구에 성공하지 못하고 실패한 자료도 영업비밀로 보호 가능
실험데이터	개발 중인 시제품 또는 시제품의 성능 실험, 의약품의 효능 시험, 기계장치의 시운전 데이터 등	
시설, 기계설비, 장비	기업이나 개인이 독자적으로 개발하여 보유하고 있는 시설, 특수장비와 설비 등	시설과 지역을 통제구역으로 지정하고 접근을 제한하여 비밀로 관리

- 경영정보 : 마케팅 전략, 고객 리스트, 기업의 기본계획 등

<표3-5> 경영상의 영업비밀

대 상	설 명	비 고
각종 주요계획	경영전략, 신규 투자계획, 신제품 개발/생산계획, 마케팅/판매계획, 인력수급계획 등	공개되면 경쟁업체의 대응이 있을 수 있는 계획은 영업비밀로 지정
고객명부	지역별 고객리스트, 연령별 또는 직업별 분류표 및 대리점/영업점의 제반 영업자료 등	고객정보의 유출은 개인 정보보호 차원에서 사회적 물의를 일으킬 수 있음
관리정보	원가분석, 마진율, 거래처 정보, 인사/재무관리 및 경영분석 정보 등	공개되면 자사의 피해가 우려되거나 경쟁회사에 유리한 정보
매뉴얼 등 중요자료	·그 기업의 기술과 경험을 바탕으로 한 방법 기술 서류 ·그 회사만의 독특한 방법이나 기법을 담고 있는 모든 매뉴얼 등	·원료 투입순서, 화합물의 반응방법, 합성방법 등 ·판매기법, 고객 접근 및 설득방법, 시장 조사방법, 원가 산정방법 등

□ 영업비밀의 요건

○ 「부정경쟁방지 및 영업비밀 보호에 관한 법률」 제2조 제2호에서 언급한 영업비밀의 정의규정에서는 영업비밀의 개념적 요소로서 다음과 같은 세 가지의 요건을 들고 있으며, 이는 영업비밀 침해시 법적보호를 받기 위한 필수조건임

1) 비공지성

- 영업비밀이 본법의 보호대상이 되기 위해서는 당해 기술 등이 '공연히 알려져 있지 아니한 것'이어야 함

- 여기에서 '공연히 알려져 있지 아니한'이란 불특정 다수인이 그 정보를 알고 있거나 알 수 있는 상태에 있지 아니한 것을 의미
- 다만 보유자 이외의 타인이 당해 정보를 알고 있다 하더라도 보유자와의 사이에 비밀 준수의 의무가 형성된 경우라면 비공지 상태라고 할 수 있음
- 또한 보유자와 무관한 제3자가 독자개발 등에 의해 동일한 정보를 보유하고 있더라도 그 제3자가 당해 정보를 비밀로서 유지하고 있는 경우 역시 비공지 상태의 정보라고 할 수 있음

2) 경제적 유용성

- 영업비밀로서 보호받기 위해서는 어떤 정보가 경제적 가치를 가지고 있어야 함을 전제로 하며, 이는 특정한 정보의 사용을 통해 경쟁업자에 대한 경제상의 이익을 얻을 수 있거나 정보의 취득 또는 개발을 위해 상당한 비용이나 노력이 필요한 경우 등을 의미
- 또한 현실적으로 사용되고 있지 않더라도 미래에 경제적 가치를 발휘할 가능성이 있는 정보(잠재적으로 유용한 정보)와 과거에 실패한 연구데이터와 같은 정보 또한 경제적 가치를 가지고 있는 것으로 인정
- 다만, 탈세방법·공해물질의 배출방법 등 반사회적인 정보 및 실현가능성이 없는 정보는 경제적 유용성을 지니고 있다고 볼 수 없음

3) 비밀관리성

- 경제적 유용성을 지닌 비공지 상태의 기술·경영정보라 하더라도 영업비밀로 보호받기 위해서는 당해 정보 소유자의 비밀성 유지를 위한 관리상태가 지속되고 있어야 함(영업비밀 소유자의 관리의사와 관리노력)
- 어느 경우에 비밀로서 관리되고 있다고 인정될 수 있는가는 구체적인 상황에 따라서 개별적으로 판단되어야 할 것이나, 대략 다음과 같음
  - ·당해 정보에 접근할 수 있는 사람의 수를 제한하거나, 접근자에게는 그 정보를 사용·공개할 수 없다는 취지의 비밀준수 의무를 부과하는 경우
  - ·당해 정보에 비밀표시를 하여 접근할 수 있는 자에게 그것이 영업비밀이라는 사실을 주지시키고 있는 경우
  - ·당해 정보에 대한 접근을 공간적·물리적으로 제한하는 경우 등

- 그러나, 영업비밀에 해당되는 정보는 물적인 매체(서류, 디스크, 필름 등)에 체화된 것 뿐만 아니라 개인의 기억에 의한 것도 있으므로 반드시 위 방안이 동시에 지켜져야 하는 것은 아님

  · 예컨대 영업비밀임을 표시하지 아니하였다고 해서 산업스파이 등 외부자의 침해행위가 면책되는 것은 아니며, 영업비밀에 비밀준수의무가 명시되어 있지 않다고 해서 종업원이 이를 타기업에 유출시키는 행위가 면책되는 것은 아님

4. 영업비밀과 특허의 비교

□ 영업비밀과 특허의 법적 차이

○ 영업비밀(노하우)은 비밀성과 유용성이 있는 기술정보로 상당한 노력에 의해 비밀로서 관리되고 있으므로 라이선스를 받지 않으면 접근할 수 없음

- 해당기술이 이미 알려진 제품을 보다 경쟁적이고 효율적으로 만드는 제조공법이나 소프트웨어 프로그램 코드 등은 생산설비나 제품을 분석하여도 해당 기술을 쉽게 알 수 없는 경우가 많으므로 영업비밀로서 보호하는 것이 유리함[3)]

- 다음은 영업비밀침해금지와 관련된 대법원 판례로 영업비밀로 인정되기 위해서 어느 정도까지 관리해야 하는지를 보여주는 좋은 사례임

> "(중략)…당해 업체의 직원들조차 자신이 연구하거나 관리한 것이 아니면 그 내용을 알기 곤란한 상태에 있어 비밀성이 있고, 당해 업체는 공장 내에 별도의 연구소를 설치하여 관계자 이외에는 그 곳에 출입할 수 없도록 하는 한편 모든 직원들에게는 그 비밀을 유지할 의무를 부과하고, 연구소장을 총책임자로 정하여 그 기술정보를 엄격하게 관리하는 등으로 비밀관리를 하여 왔다면, 그 기술정보는 부정경쟁방지법 소정의 영업비밀에 해당하고…(중략)" (大判 1996. 12. 23)

3) 日本 發明協會編, ライセンス契約實務ハンドブック, 56面.

○ 특허는 특허권자나 정당한 권원이 있는 자만 사용할 수 있는 독점적인 배타권이므로 라이선스를 받지 않고 실시하면 권리침해가 됨

- 의약품이나 제조품처럼 해당기술의 내용이 신제품과 일치하고 제품을 분석하면 기술내용을 알 수 있는 기술을 보호하기 위해서는 특허를 이용하는 것이 유리함

<표3-6> 영업비밀과 특허의 법적 차이

구 분	영업비밀(노하우)	특 허
법적성격	· 비밀로 유지, 관리되고 있는 사실상태 보호	· 공개대가로 부여되는 독점권
보호대상	· 생산방법, 판매방법 기타 영업활동에 유용한 기술상 또는 경영상 정보	· 자연법칙을 이용한 고도한 기술적 사상(신기술)
절차/기간	· 등록 불필요 · 비밀이 알려질 때까지	· 등록 필요 · 출원일로부터 20년
독점성	· 동일 영업비밀 병존 가능 · 권리행사에 제한 없음	· 동일특허권 병존 불가 · 권리행사에 제한 있음 (강제, 법정실시권 등)
침해행위	· 절취, 기망 등 부정취득행위 · 부정취득한 영업비밀의 사용, 공개행위 · 비밀유지의무가 있는 자가 영업비밀보유자에게 손해를 줄 목적으로 사용, 공개행위	· 정당한 권원 없이 특허권을 영업으로서 실시하는 행위
관련법	· 부정경쟁방지 및 영업비밀 보호에 관한 법률	· 특허법

□ 영업비밀과 특허의 장·단점

○ 일반적인 기술보호 수단으로 특허권 취득을 들 수 있는데, 이는 법적 보호가 강력하다는 장점이 있는 반면, 공개에 의하여 기술내용이 해외에도 알려지게 되고 특허권의 효력이 출원한 국가에만 미친다는 단점이 존재함

○ 한편, 영업비밀의 경우 비밀로 유지되는 한 영구적으로 유효하고, 특허출원이나 권리화가 필요하지 않다는 장점이 있으나, 독점성이 없고 기업의 관리능력에 효력이 좌우된다는 단점이 존재함

<표3-7> 영업비밀과 특허의 장·단점

구 분	영업비밀(노하우)	특 허
장 점	· 비밀로 유지되는 한 영구적으로 유효 · 특허출원 절차의 번거로움 및 권리화에 추가비용 없음 · 기술내용 미공개로 인해 기술경쟁우위의 유지가 가능	· 법에 의한 배타적 독점권 보장 · 기술가치 상승
단 점	· 기업의 비밀유지노력 등 관리능력에 효력 좌우 · 독점성이 없음	· 권리화에 추가비용 발생 · 기술이 공개됨 · 등록국가에서만 유효 · 유효기간이 제한됨

□ 기술보호에 대한 판단기준

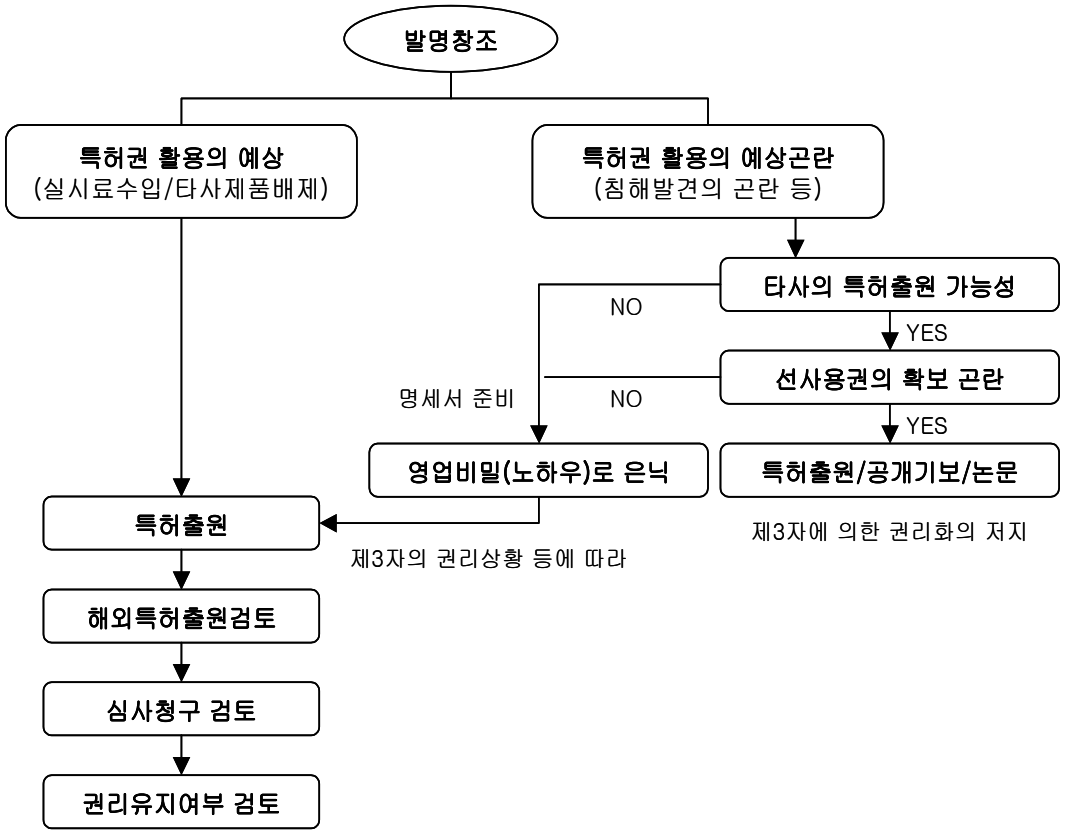
○ 특허로 보호

- 대상기술이 장래 표준으로 될 가능성이 있는 기술이나, 대상기술과 제품의 관계를 고려하여 제품에 가까운 기술일수록 특허로 보호할 필요
- 자사의 기술수준이 경쟁회사에 비해 많은 차이가 나지 않아서 대상기술에 쉽게 도달할 수 있는 경우 또는 대상기술의 예상수명이 특허권 취득에 필요한 기간보다 길다고 판단되는 경우 특허 취득을 통한 보호가 바람직함

○ 영업비밀로 보호

- '타사의 독자개발이 곤란한 기술'이나 '특허권의 침해발견이 곤란한 기술'에 대해서는 영업비밀로 보호하는 것이 바람직함
  - 다만, 타사에 제조현장을 보여줄 필요가 있는 기업, 인재의 유동성이 높은 기업 등 영업비밀로서 계속 관리하는 것이 곤란한 경우 또는 해외 추진사업의 경우에는 비밀관리의 곤란성이나 해당 국가의 법, 제도 등을 충분히 고려하여 신중한 선택이 요구됨
- 영업비밀로 보호하기로 한 경우에는 사업의 자유도를 확보하기 위하여 특허법상 인정되는 선사용권의 증거확보 필요
- 역설계(Reverse Engineering)로 발견할 수 없는 기술, 예를 들어 계측방법, 계측장치, 제어알고리즘 등과 같이 역설계를 해도 타사의 침해를 발견할 수 없는 기술은 영업비밀로 보호

<그림3-6> 기술의 보호관리 방법



□ 선사용권

○ 선사용권 활용의 필요성

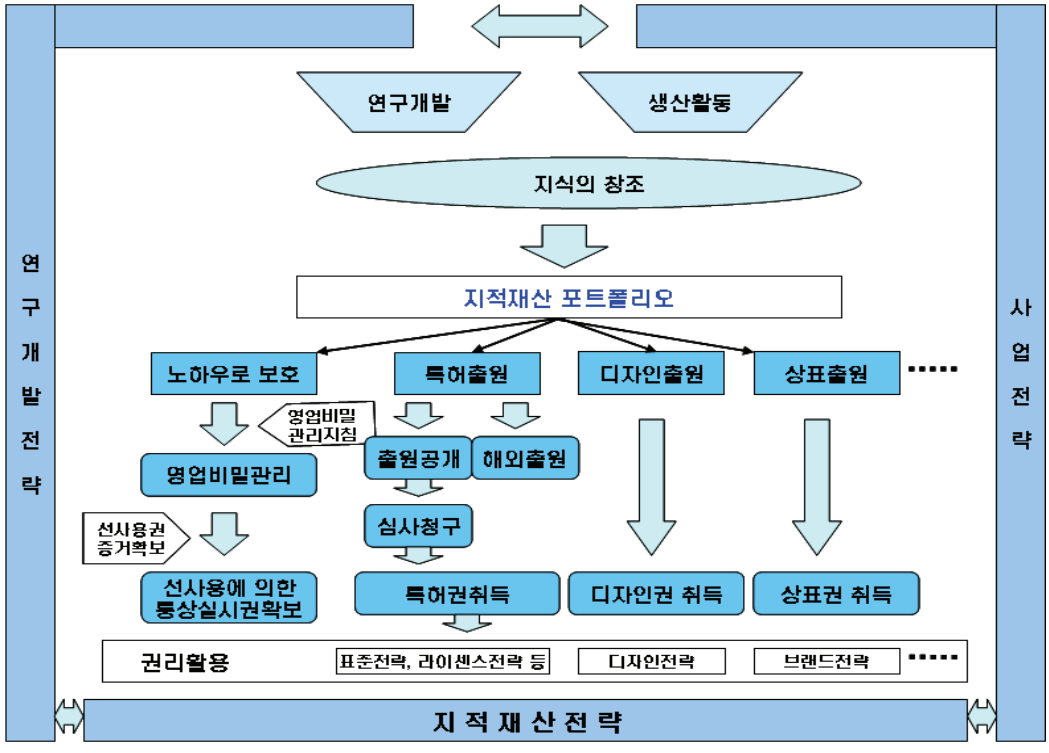
- 특허권이 침해되면 특허권을 행사하여 침해자를 배제할 수 있지만, 대부분의 중소기업들은 자사가 보유한 특허권의 침해여부를 모니터링 할 수 있는 체제를 구축하기가 매우 어렵고, 침해사실을 확인했다 하더라도 침해자가 외국기업이나 협력업체인 경우 조사·교섭비용이나 영업상의 이유 때문에 특허권을 행사하기가 현실적으로 어려움

  · 이러한 경우 기업은 특허권을 취득해서 얻는 이익보다 특허권을 취득하기 위해 발명내용을 공개함으로서 발생하는 손실이 더 크게 됨

- 이를 해소할 수 있는 방안으로서 발명내용을 공개하지 않고 영업비밀로 보유하면서 동일한 발명에 관한 특허권을 취득한 자에게 발명을 실시할 권리를 주장할 수 있는 것이 선사용권 제도임

- 발명의 성질에 따른 효용성에 대한 작업이 선행되어야 하겠지만 중소기업의 지식재산전략의 하나로서 선사용권제도의 활용을 적극적으로 검토할 필요가 있음

<그림3-7> 지식재산의 전략적 관리를 위한 순서도



○ 선사용권의 요건

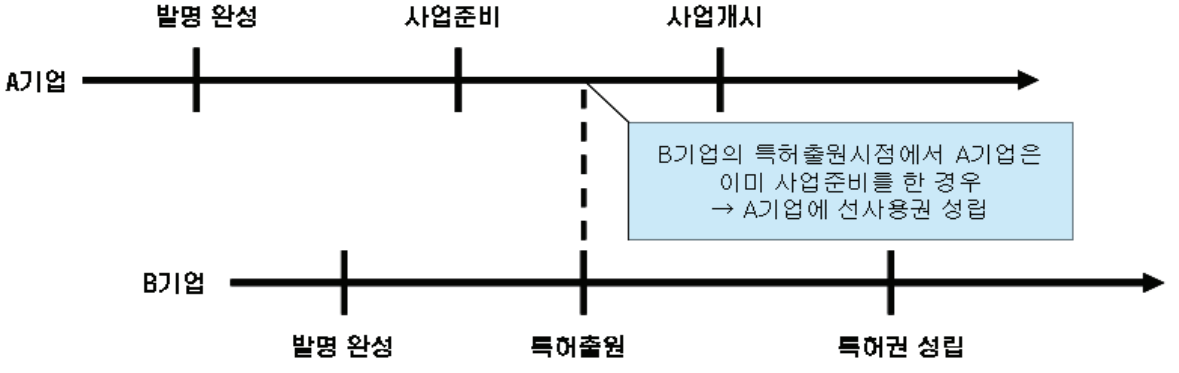
① 특허출원과 관련되는 발명의 내용을 모르고 스스로 그 발명을 하거나 또는 특허출원과 관련된 발명을 모르고 그 발명을 한 사람으로부터 지득하여,

② 특허출원시에 실제로,

③ 국내에서,

④ 그 발명의 실시를 하거나 실시준비를 하고 있는 자

<그림3-8> 선사용권의 개념도



○ 선사용권의 효과

- 그 실시 또는 준비를 하고 있는 발명 및 사업의 목적범위 안에서 그 특허출원과 관련된 특허권에 대하여 무상으로 통상실시권을 가지며, 제3자에게 이전할 수도 있음
- 선사용권의 발생은 국내실시에 한정되며 실시시기는 출원시까지로 보지만 일시적 실시에 대하여는 선사용권을 인정하지 않으며, 선의로 실시하여야 권리가 발생함
- 사업의 목적을 변경하는 경우에는 인정하지 않으며 생산규모를 확대하는 것은 인정됨

○ 선사용권제도의 활용방법[4)]

- 일상 업무 속에서 증거가 되는 자료를 확실하게 작성·보존하고, 특히 해당 자료가 언제 작성되었는지를 증명할 수 있도록 조치를 해 두는 것이 매우 중요함

4) 일본 특허청, 「선사용권제도의 원활한 활용을 향하여」, 2006.6

· 선사용권을 입증하기 위한 증거가 되는 자료로는 발명자의 연구노트, 기술성과보고서, 설계도, 제품사양서 등의 기술관련 서류와 사업계획서, 사업개시결정서, 견적서, 납품서 등의 사업관련 서류가 있음

· 증거자료의 증거능력을 제고하기 위해 공증인에게 공증을 통하여 확정일자를 확보하거나 공공기관의 시험증명서를 받아 두도록 함

○ 선사용권제도의 적용에 적합한 발명

- 일반적으로 다음과 같은 발명은 발명내용을 공개하는데 따른 손실이 크고 특허권을 취득해도 그다지 이득이 되지 않으므로 선사용권제도를 활용하는 것이 적합함

① 타인이 독자적으로 동일한 발명을 하는 것이 용이하지 않다고 판단되는 발명

② 발명을 이용한 제품을 분해·분석해도 발명내용을 쉽게 알 수 없는 발명

③ 특허권을 취득해도 특허권침해를 발견하는 것이 매우 곤란하여 특허권이 유명무실해질 가능성이 높은 발명

④ 처음부터 특허권의 취득 가능성이 낮은 발명

5. 국가핵심기술의 수출승인 및 사전신고

□ 「산업기술」과 「국가핵심기술」(산업기술보호법[5] 제2조)

○ 산업기술

- '산업기술'은 제품 또는 용역의 개발·생산·보급 및 사용에 필요한 제반 방법 내지 기술상의 정보 중에서 관계 중앙행정기관의 장이 지정 또는 공고하는 기술을 말함

○ 국가핵심기술

- 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 산업기술로서 산업기술보호위원회의 심의를 거쳐 지정된 산업기술을 말함

□ 국가핵심기술의 지정 및 운영

○ 국가핵심기술의 지정 및 운영절차

- 관계 중앙행정기관의 장은 소관 산업기술을 대상으로 필요 최소한의 지정대상기술을 선정하면, 산업기술보호위원회[6]에서 심의를 거쳐 국가핵심기술 지정

  · 선정기준 : 국가안보 및 국민경제에 미치는 파급효과, 관련 제품의 국내외 시장점유율, 해당분야의 연구동향 및 기술 확산과의 조화 등을 종합적으로 고려하여 선정

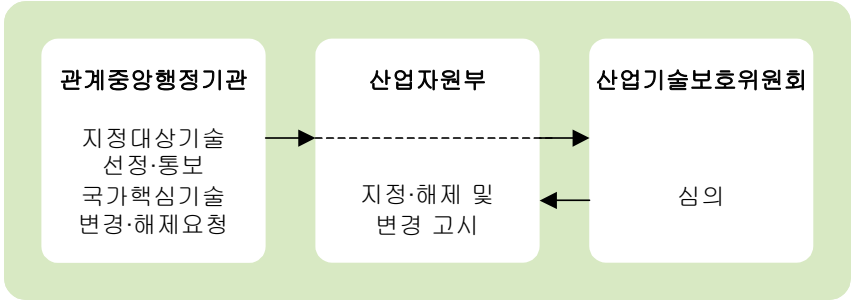
- 산업기술보호위원회는 국가핵심기술 지정·변경 및 해제에 관하여 이해관계인의 요청이 있는 경우 의견진술 기회 제공

---

5) '산업기술의 유출방지 및 보호에 관한 법률'(2006.10.27 공포, 2007.4.28 시행)

6) 산업기술의 유출방지 및 보호에 관한 주요정책을 심의하기 위해 국무총리 소속하에 설치하며, 위원회는 위원장(국무총리), 부위원장(과학기술부총리)을 포함한 25인 이내의 위원으로 구성하고, 간사위원은 산업자원부 장관이 맡도록 하고 있음(산업기술보호법 제7조)

<그림3-9> 국가핵심기술의 지정 및 운영절차



□ 국가핵심기술의 수출승인 및 사전신고

○ 정부에서는 국가핵심기술의 해외수출에 대한 사전승인 또는 사전신고제도를 운영함으로써 국가핵심기술을 관리함

- 국가가 지원하여 개발한 핵심기술을 외국기업 등에 매각이나 이전 등의 방법으로 해외로 수출하고자 할 경우에는 산업기술보호위원회의 심의를 거쳐 산업자원부 장관의 승인을 받도록 함
- 민간 자체개발한 핵심기술을 해외로 수출하고자 할 경우에는 산업자원부 장관에게 사전 신고하도록 함

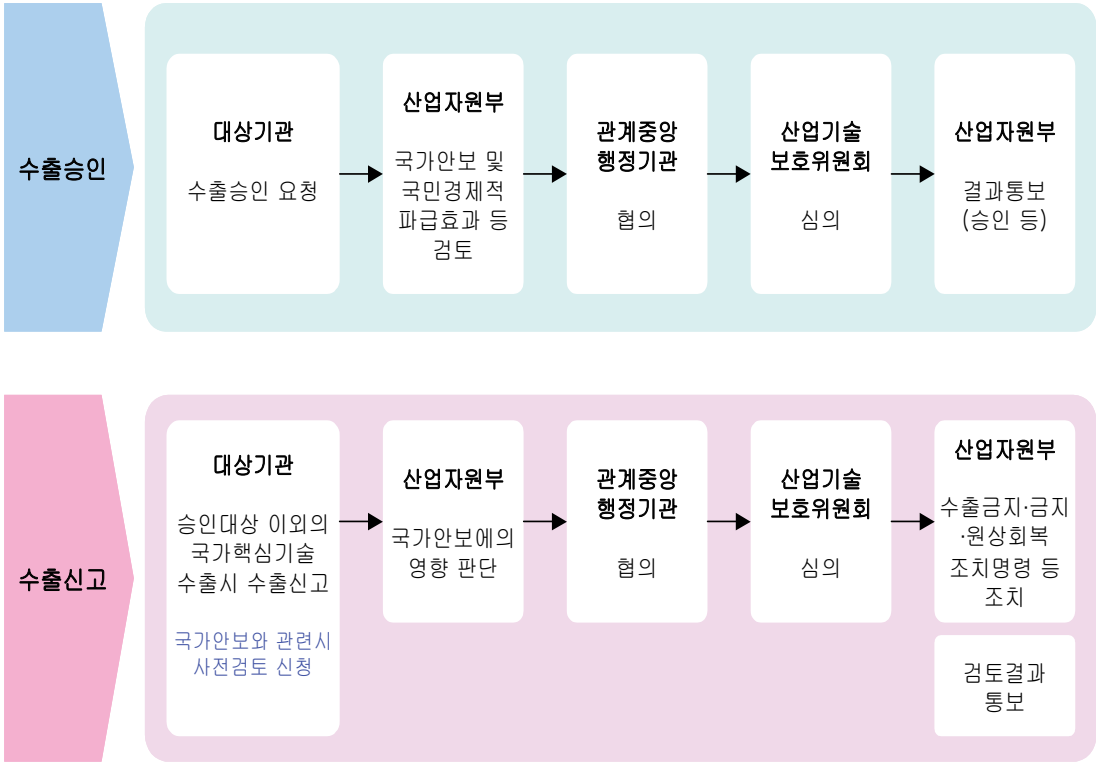
○ 신고대상 국가핵심기술의 수출이 국가안보와 관련되어 있는 지 여부에 대한 사전검토 제도 실시

- 국가안보와 관련 있다고 판단하는 경우 산업기술보호위원회의 심의를 거쳐 수출중지, 수출금지, 원상회복 등의 조치를 명함

○ 위반시 벌칙

- 산업기술을 외국에서 사용하거나 사용되게 할 목적으로 유출 및 침해행위를 한 경우 '7년 이하의 징역' 또는 '7억원 이하의 벌금'
- 산업기술을 외국으로 유출할 목적으로 예비·음모한 자는 '3년 이하의 징역'또는 '3천만원 이하의 벌금'

<그림3-10> 국가핵심기술의 수출승인 및 신고절차



□ 국가핵심기술 지정 현황

○ 정부는 하이브리드 및 연료전지 자동차 관련 설계기술과 미세공정 80나노급 이하 D램 반도체의 설계·공정·조립기술 등 40개 기술에 대해 국가핵심기술로 지정함(2007. 8. 21)

- 전기전자 4개, 자동차 8개, 철강 6개, 조선 7개, 원자력 4개, 정보통신 6개, 우주 5개

제3절 인적자원관리

1. 신규채용자

□ 보안 서약서 징구

○ 재직 중에 지득한 회사의 기밀을 누설하는 경우 손해배상은 물론 민·형사상 책임을 지겠다는 내용 명기

○ 재직 중에 작성·개발한 특허나 논문 등 지적재산권의 소유권이 회사에 있음을 명기하고, 영업비밀의 무단사용으로 인한 법적 분쟁여지를 사전에 차단

○ 입사시 근로계약서에 보안서약 내용을 포함해도 무방하나, 회사와 근로자간의 책임한계를 서약서에서 명확히 해야 함

○ 보안 서약서의 내용은 <별책 p.82> 참조

□ 보안교육 실시

○ 보안업무 규정 또는 지침, 사내·외 발생 보안사고 사례, 보안의무 위반시 벌칙 등에 대한 보안교육을 실시하여, 보안에 대한 경각심을 제고

○ 필요시 외부의 전문기관에 의한 보안 무료교육 수강도 적극적으로 활용할 필요가 있음[7)]

□ 경력자 채용시 조치사항

○ 동종업계의 우수한 경력자를 채용하는 것은 별도의 비용을 투자하지 않고 중요한 정보를 획득하는 가장 손쉬운 방법임

○ 하지만 연구개발직의 경우 이전 직장에서 비밀유지서약이나 경쟁업체 취업금지서약을 했을 가능성이 높으며, 이를 무시할 경우 경력자 본인은 물론 채용한 업체도 영업비밀 침해행위(부정경쟁방지 및 영업비밀보호에 관한 법률 제2조 제2호의 라목의 중과실에 의한 침해)가 될 수 있기 때문에 특히 주의를 요함

---

7) 중소기업기술정보진흥원(www.tipa.or.kr), 한국산업기술진흥협회(www.koita.or.kr), 중소기업진흥공단(www.sbc.or.kr) 등에서 중소기업을 위한 보안교육이 실시되고 있으며, 향후 교육기관 및 교육횟수 또한 늘어날 것으로 예상됨

○ 가능하면 경력자를 전직회사와 동일한 업무에 종사하지 않게 하는 것이 바람직하며, 업무수행 중에 전직회사 비밀의 사용을 금지하는 서약을 입사시에 받으면 전직회사의 영업비밀을 적극적으로 보호해 줌으로써 분쟁 예방에 노력한 근거가 될 수 있음

○ 경력자는 전직회사의 임직원들과 사적인 친분관계가 있으므로 고의가 아니더라도 정보를 제공할 개연성이 많으며, 위장취업 했을 가능성도 배제할 수 없으므로 일정 기간 동안 근무 태도를 예의 주시할 필요가 있음

2. 재직자

□ 보안 서약서 징구

○ 연봉계약서를 작성할 경우 보안서약서를 함께 징구하여 지속적으로 보안의 중요성을 각인시킬 필요가 있음

○ 회사에서 수행하는 중요 프로젝트에 참여하는 경우 비밀유지 서약서를 별도로 징구해야 함

○ 보안 서약서의 내용은 <별책 p.82> 참조

□ 제품개발 단계에 따른 차별화된 보상시스템 설계

○ 기업의 입장에서 핵심 연구인력에 대한 처우개선은 외부로부터의 기술유출을 막기 위해 가장 중요한 과제임

○ 한정된 재원을 가지고 우수 인력의 보상욕구를 충족시키기에는 현실적으로 불가능하며, 이의 해결을 위해서는 무엇보다 보상재원을 효율적으로 배분하는 것이 필요함

○ 이를 위해서는 기술개발, 특허신청, 시제품 출시단계, 양산 등 기술개발의 제 단계별로 보상을 확대 실시하고, 양산 시점에는 파격적인 보상을 해주는 것이 필요함

- 경쟁사에서 탐내는 기술 역시 양산이 가능하여 당장 어느 정도의 매출을 올릴 수 있고, 고객에게 인정받는 기술이며, 이 시기에 인력유출 시도 또한 가장 많이 나타남

○ 최근 정부에서는 「직무발명제도」를 개선하였으며, 그 내용은 별도로 살펴보기로 함(p.74 참고)

□ 보안교육 실시

○ 보안교육은 자체적으로 실시하는 것도 좋으나, 직원들의 관심을 끌고 교육효과를 높이기 위해 외부 전문가를 초빙하는 것도 필요함

○ 사내 보안담당자의 업무역량 강화를 위해 외부 전문교육에 참여하는 것도 검토할 필요가 있음

○ 사내외 보안교육 종료시 참석자 서명 및 수료증 발급 등을 통해 향후 법적 분쟁 발생시 회사기밀을 보호하기 위한 회사 차원의 노력을 입증하는 자료로 활용할 수 있음

□ 보안점검 실시

○ 보안교육도 중요하지만, 교육 후 임직원들의 보안실천이 보다 중요함

○ 정기, 불시 보안점검을 실시한 후 보안우수자 및 위반자에 대해 적절한 포상 및 불이익을 부과함으로써, 임직원들의 보안의식 제고 및 주의 환기를 유도할 필요가 있음

□ 포상 및 징계

○ 회사내 다양한 보안이벤트를 실시하여 임직원들의 보안마인드를 함양하고, 보안업무 유공자의 경우 고과에 반영하거나 상금을 지급하는 등의 포상을 실시하여 임직원의 참여도를 제고해야 함

○ 보안규정을 위반하는 자의 경우 징계 이상의 강력한 조치를 취하여 보안업무를 일상화된 기업문화로 정착시켜 나가야 함

○ 포상과 징계에 대한 의사결정은 보안관리위원회를 통하여 이루어져야 하며, 초기단계에는 지도에 중점을 두는 것이 바람직함

3. 외국인

□ 신규채용시

○ 외국인 고급인력은 기업의 기술 및 경영정보에 접근할 수 있는 경우가 많아 기밀유출 위험성이 상대적으로 높기 때문에 다음 사항을 참고하여 비밀유지계약을 체결해야 함

○ 주요 내용

- 계약기간 중에 작성·개발한 모든 정보의 소유권은 회사에 귀속된다는 사실 명시
- 계약기간 중에는 물론 계약종료 후에도 일정기간 비밀유지 의무 부여
- 계약만료 후 비밀유출의 위험성이 있는 경쟁업체 취업금지 서약서를 징구하고 취업시 회사와 협의할 의무 명시
- 계약기간 중에 수행한 업무에 대해서 계약 후에도 특허출원, 상품화 등의 협조에 관한 내용 명시
- 기타 업무의 접근한계, 자료 반출 등에 관련된 사항

○ 보안 서약서의 내용은 <별책 p.90> 참조

□ 기술협력, 기술자문, 투자협정시

○ 상대방의 의도를 정확히 파악

- 상대회사의 협력과 관련된 업무수행 능력, 신뢰도 및 지금까지의 실적, 국제적인 활동 현황 등을 사전에 조사하여 그 의도를 파악하여야 함

○ 구체적인 협상 전에 상호 비밀유지계약 체결

- 협상내용에 대한 비밀유지계약의 체결로 협상결렬시 자료의 반환 및 사용금지 등 정보유출을 사전에 막고 사후책임을 명시할 수 있음

○ 기술자문 및 컨설팅 수행 전에 상호 비밀유지계약 체결

- 컨설팅, M&A, ISO인증 등을 실시할 때도 정보유출에 각별히 유의해야 하며, 구체적인 비밀유지계약을 체결한 후 수행

○ 실사에 참가하는 개인별 비밀유지계약 체결

- 업체와 비밀유지계약을 체결하였으나, 참가자가 개인적으로 비밀을 누설, 유출하는 것을 방지하기 위해 개인적으로도 비밀유지계약 체결 필요

○ 계약종료 후에도 일정기간 비밀유지의무 부과

- 기업의 핵심정보에 대한 지득 또는 인지한 사실을 누설시 책임관계 명시

○ 결과물에 대한 귀속문제를 명확히 하여야 함

- 특히 기술협력 또는 공동연구 시에 결과물에 대한 귀속문제를 명확히 하여야 함

○ 상호 의견대립과 분쟁시 해결절차를 명확히 하여야 함

<표3-8> 기술협력 실패사례

<사실관계>

- 하이닉스 반도체의 전신인 현대전자와 후지쯔사가 공동연구개발 추진함
- 이후 후지쯔사는 단독 명의로 한국, 일본, 미국에서 특허등록을 허여 받은 후, 하이닉스 반도체를 상대로 특허침해금지의 경고장을 보냄

<시사점>

- 이 경우 문제되는 것은 고의침해
- 조치사항 : 하이닉스 반도체는 몇 개월간 고생하여 회피설계
  - 회피설계시 중요한 것은 반드시 구성요소를 줄여야 하며, 현재 생산중에 있는 제품이 회피설계의 대상이 아니라 다음 제품(Next Version)을 대상으로 해야 한다는 점임
- 교훈 : 연구성과에 대한 권리확보의 중요성

4. 퇴직자

□ 정보반납 및 개인정보 삭제

○ 개인 PC 및 업무관련 자료를 퇴사시 반납하도록 하고, 주요 반출물품에 대한 검색을 실시

○ 개인 PC와 회사 메일계정의 ID 및 패스워드 삭제

○ 정보반납 및 개인정보 삭제는 임직원이 퇴사하자마자 곧바로 이루어져야 함

○ 개인이 업무수행 중 취득한 정보는 아무리 관리하더라도 각종 방법으로 유출되기 쉽지만 기본적으로 정보반납 서약 및 규정을 설정해 두면 문제 발생시 유리함

□ 경쟁업체 취업금지서약

○ 영업비밀 보유자 등 핵심 인력이 일정 기간 이내에 경쟁업체로 전직할 경우 관련법규에 의해 처벌받는다는 사실을 고지하고 퇴직시 동 내용을 명기해야 함

○ 퇴직자가 보유한 영업비밀을 고려하여 경업금지 업종, 분야, 기간을 구체적으로 한정해야 향후 영업비밀 누설로 인한 법적 대응시 유리함을 명심해야 함

○ 하지만 이는 헌법상 보장된 근로자의 직업선택의 자유를 침해하지 않는 범위 내에서 합리적으로 결정되어야 함

○ 보안 서약서의 내용은 <별책 p.98> 참조

□ 퇴직 후 진로 및 동향 파악

○ 모든 퇴직자에 대해 퇴직시 인터뷰(Termination Interview)를 통해 퇴직 후 진로에 대해 조사하여야 하며, 일부 퇴직자에 대해서는 퇴직 후 일정기간 동안 진로 및 동향에 대해 인지하고 있어야 함

5. 외부인력

□ 협력업체 및 실무자

○ 협력업체와 공동으로 업무 수행시 업체간에는 물론 실무자와도 반드시 비밀유지계약을 체결해야 함

○ 비밀유지계약을 체결함에 있어서 비밀유지기간, 생산된 비밀의 귀속문제, 비밀침해의 책임, 비밀의 취급 및 관리 등이 고려되어야 함

○ 보안 서약서의 내용은 <별책 p.106>, <별책 p.114> 참조

□ 제품 구매자 등

○ 제품소개, 구매상담, 공장견학 등에 있어서 장소를 사전에 지정하고, 기술자료 및 홍보 팜플렛 등에 대한 보안성 검토를 실시

□ 외부 자문인력

○ 컨설턴트, 고문변호사, 회계사 등 외부 자문인력의 경우 경쟁업체에도 유사업무를 수행할 가능성이 높으므로 이들과도 반드시 비밀유지계약을 체결해야 함

○ 일부 업종은 법으로 비밀유지업무가 명시되어 있으나 별도로 하는 것이 보다 완벽하며, 계약체결시 비밀유지 의무와 함께 위반시 손해배상 책임 및 관련 법규에 의한 민·형사상 처벌규정을 명확히 기재

○ 업무상 제공한 자료는 가급적 회수하거나 관리를 철저히 하도록 지속적으로 전문가에게 교육

6. 직무발명제도

□ 배경

○ 기술유출을 방지하기 위한 가장 근본적인 대책은 핵심인력에 대한 관리와 처우에 보다 관심을 쏟는 것임

- 2003년부터 2007년 7월까지 적발된 기술유출 사건(107건) 중 개인영리 및 금전유혹에 의한 유출이 약 72%(77건), 처우 및 인사 불만에 의한 유출이 약 20%(21건)를 차지함(국가정보원)

○ 직무발명보상제도는 직무발명에 대한 정당한 보상으로 종업원의 연구의욕을 고취하여 더 많은 우수발명 창출을 촉진함으로써 사용자(회사)의 이익을 증대시키고 이를 재원으로 R&D투자 및 종업원에 대한 보상을 확대해 나가는 'R&D 선순환시스템' 구축에 효과적인 방안이며, 기술유출 예방에 효과적인 대안이 될 수 있음

○ 직무발명제도는 2006년 3월 법 개정으로 인해 '발명진흥법'으로 일원화 되었으며, 본 절에서는 동 제도의 주요 내용 및 보상규정 작성시 유의사항에 대해서 살펴보기로 함

□ 직무발명의 의의 및 요건

○ 의의

- 직무발명이란 종업원 등에 의한 발명이 사용자 등의 업무범위에 속하고, 그 발명을 하게 된 행위가 종업원 등의 현재 또는 과거의 직무에 속하는 발명을 의미함(발명진흥법 제2조)

○ 요건

- 종업원이어야 함
- 그 발명이 회사의 업무범위 이내일 것
- 직무수행과정에 의해서 완성하였을 것

○ 직무발명 이외의 발명

- 종업원 발명 중 위 직무발명 외에는 모두 자유발명(직무발명의 반대)에 해당하고, 자유발명에 대해서는 종업원 발명자가 발명으로 인한 모든 권리를 취득하는 데에 제한이 없고 자유로움

□ 직무발명제도의 주요 내용

(1) 종업원 등의 직무발명 완성사실 통지의무(발명진흥법 제12조)

○ 종업원이 직무발명을 완성한 경우에는 지체 없이 그 사실을 사용자에게 문서로 통지하도록 함

- 2인 이상의 종업원이 공동으로 직무발명을 완성한 경우에는 공동으로 통지하여야 함

○ 통지시점은 통지서가 사용자에 도달한 때(도달주의) 효력이 발생하며, 서면·전자문서에 의한 통지 모두 인정됨

- 최근 대다수 기업 및 연구기관이 온라인 결재시스템을 활용하여 문서를 유통하고 있는 사실 반영

(2) 직무발명에 대한 사용자의 승계여부 통지의무(발명진흥법 제13조)

○ 종업원의 직무발명 완성사실 통지를 받은 사용자는 대통령령이 정하는 기간[8] 이내에 그 승계 여부를 문서로 통지하도록 하며, 동 기간 이내에 사용자가 직무발명에 대한 권리의 승계의사를 통지한 때는 그 권리는 사용자에게 승계된 것으로 간주함

○ 다만, 직무발명에 대한 사전예약승계규정[9]이 없는 경우에는 종업원의 의사에 반하여 사용자가 그 발명에 대한 권리의 승계를 주장할 수 없도록 함

<표3-9> 승계여부 통지에 따른 사용자와 종업원간 권리관계

구 분	사 용 자	종 업 원
승계의사 통 지	직무발명에 대한 권리 귀속 (발명진흥법 §13②)	정당한 보상청구권 취득 (발명진흥법 §15①)
불승계의사 통 지	무상의 통상실시권 취득 (발명진흥법 §10①)	직무발명에 대한 권리 귀속 (발명진흥법 §10①)

○ 사용자가 대통령령이 정하는 기간 이내에 승계여부 통지를 하지 않는 경우 그 발명에 대한 권리의 승계를 포기한 것으로 간주함

- 또한 이 경우 사용자는 종업원의 동의 없이는 통상실시권을 가질 수 없도록 하여 종전법 제11조 규정의 자유발명 간주규정의 효과를 유지

8) 법 12조에 따른 통지를 받은 날로부터 4개월 이내를 의미함(발명진흥법 시행령 제7조)
9) 종업원의 직무발명에 대하여 미리 사용자로 하여금 특허를 받을 수 있는 권리 또는 특허권을 승계시키기로 한 계약이나 근무규정으로써, 통상 기업체 내부의 고용계약, 근무규정, 직무발명(보상)규정 등의 형태로 운용

(3) 직무발명에 대한 합리적인 보상기준 마련(발명진흥법 제15조)

○ 계약 또는 근무규정에서 직무발명보상에 대해 정하고 있는 경우 그 정한 바에 따라 사용자와 종업원이 협의하여 결정한 보상이 합리적 절차에 의한 것으로 인정되면 이를 정당한 보상으로 간주

- 합리적 절차 여부의 판단요소로써

① 보상형태 및 보상액을 결정하기 위한 기준의 책정시 종업원과의 협의상황

② 종업원에 대한 보상기준의 공표 등에 대한 제시상황

③ 보상형태 및 보상액의 결정시 종업원으로부터의 의견청취의 상황 등을 제시하고 있음

- 상기 합리적 절차를 참고하여 종업원과 사용자간의 분쟁이 발생하지 않도록 운영하는 것이 무엇보다 중요하며, 분쟁이 발생했을 경우 그것을 신속하고 합리적으로, 원만하게 해결하기 위해 노력해야 함

- 직무발명규정 내용은 <별책 p.176>, <별책 p.192> 참조

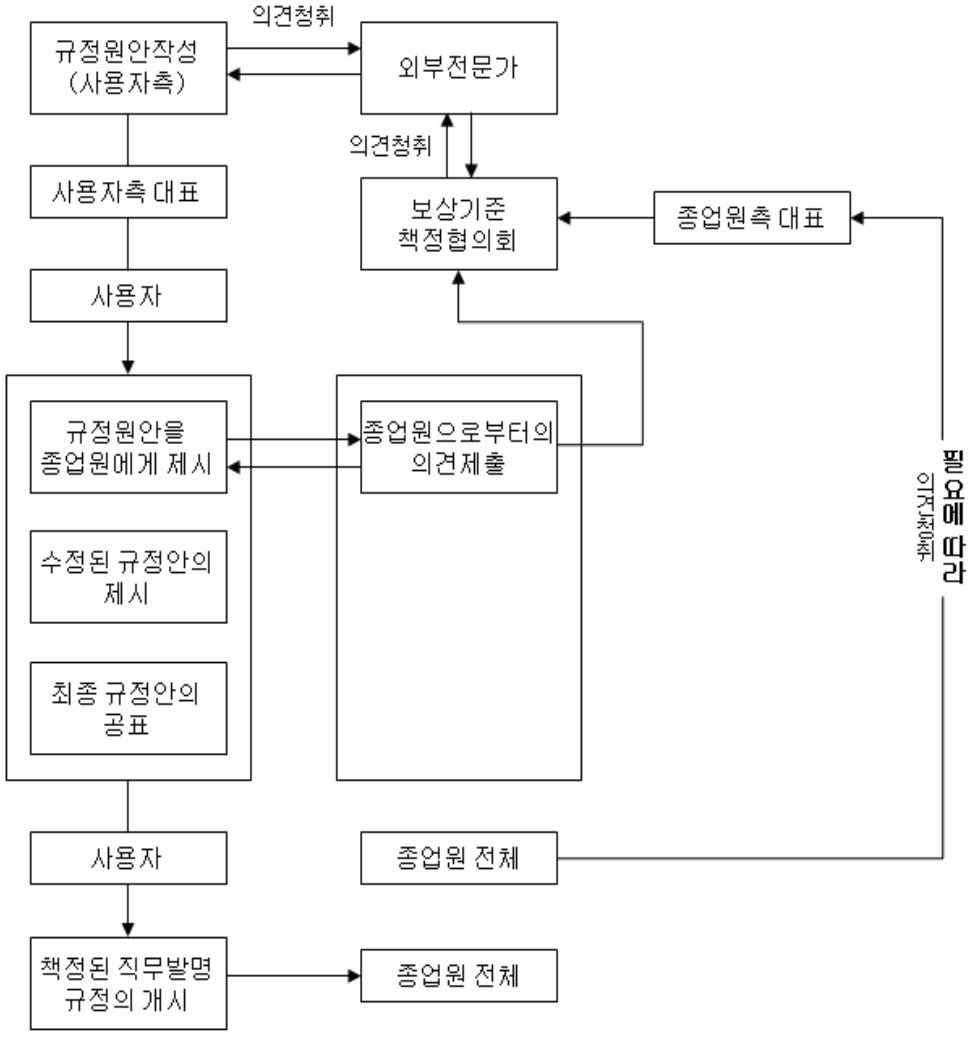
※ 소 제기시 법원의 우선 보상규정 및 보상절차의 합리성 여부를 먼저 판단하고, 합리적인 것으로 인정되면 사용자가 지급한 보상을 인정

○ 계약 또는 근무규정에서 직무발명보상에 대해 정하고 있지 않거나, 위에서 규정한 정당한 보상으로 볼 수 없는 경우에 보상액을 결정함에 있어서는 종전과 같은 기준을 적용

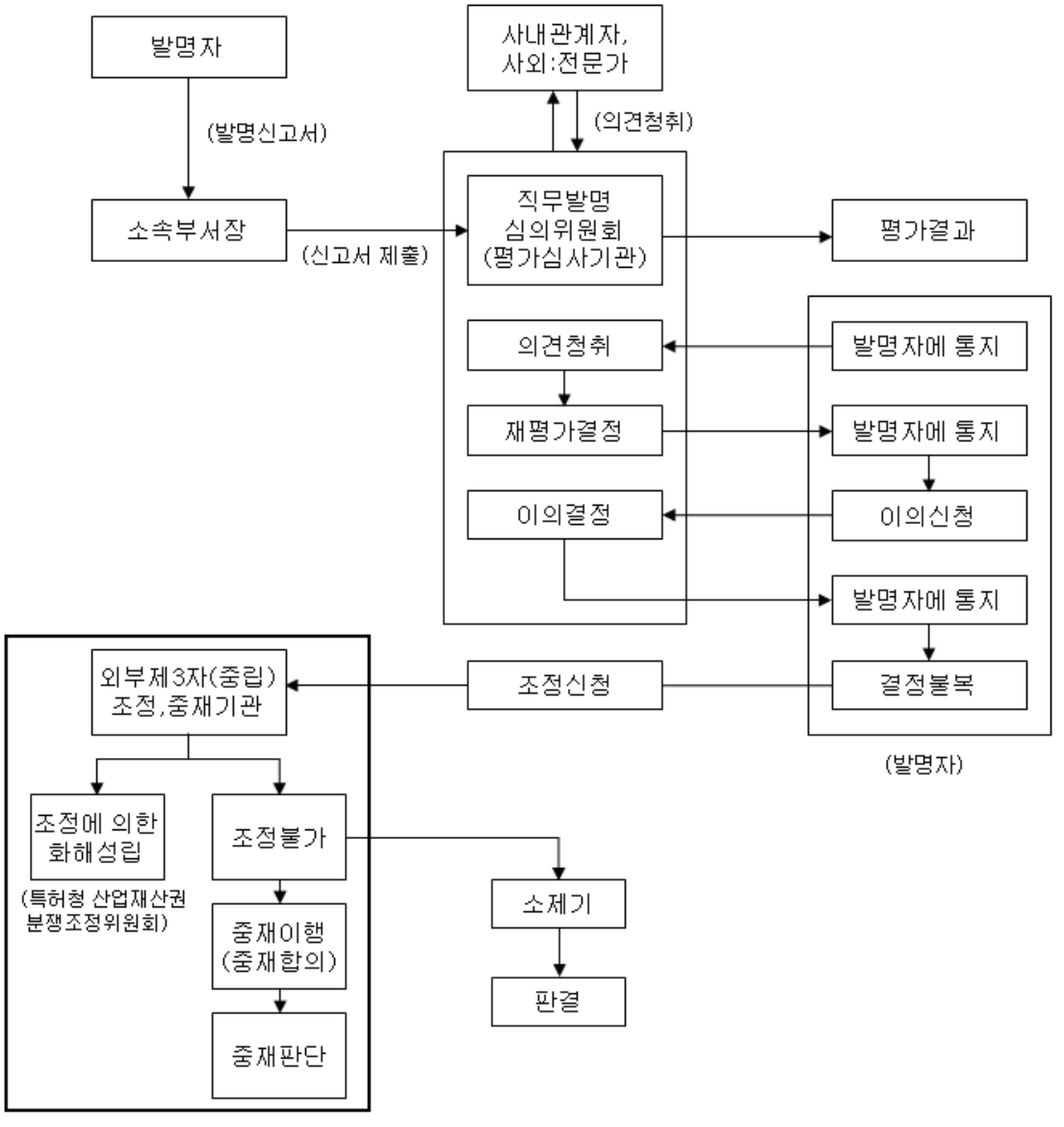
- 그 발명에 의하여 사용자가 얻을 이익의 액과 그 발명의 완성에 사용자 및 종업원이 공헌한 정도를 고려하도록 함

※ 법원이 정당한 보상액을 결정

<그림3-11> 직무발명보상기준 책정절차



<그림3-12> 직무발명보상기준에 따른 보상액 결정과 분쟁처리절차



(4) 직무발명의 출원유보요건 및 보상의무(발명진흥법 제16조)

○ 사용자가 종업원으로부터 직무발명에 대한 권리를 승계한 후, 출원하지 않는 경우 등에도 보상을 하여야 함

○ 출원유보시 사용자는 보상액을 결정함에 있어서 당해 발명이 산업재산권으로 보호되었더라면 그 발명을 한 종업원이 받을 수 있었던 경제적 이익을 고려하여야 함

(5) 직무발명관련 분쟁(발명진흥법 18조)

○ 현실적으로 직무발명에 대한 권리 귀속관계, 권리승계에 따른 보상관련 문제 등 직무발명과 관련한 다양한 분쟁요인이 존재하며, 이에 대한 신속한 해결을 지원하기 위해 사용자와 종업원간에 분쟁이 발생하는 경우 동법 제41조의 규정에 의한 산업재산권분쟁조정위원회에 조정을 신청할 수 있음

○ 조정의 효력은 '재판상 화해'와 동일하며, 조정신청은 재판상 시효의 중단의 효력이 존재함

- 조정이 성립되지 아니한 경우 1개월 이내에 소를 제기하여야 함

(6) 비밀유지의 의무(발명진흥법 19조)

○ 종업원은 사용자가 직무발명을 출원할 때까지 그 발명의 내용에 관한 비밀을 유지하여야 함

- 비밀유지의 의무를 위반하여 부정한 이익을 얻거나 사용자에게 손해를 가할 목적으로 직무발명의 내용을 공개한 자에 대해서는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처함, 단 이 부분은 사용자의 고소가 있어야 공소제기가 가능함

○ 사용자가 직무발명에 의한 권리를 승계하지 않음에 따라 종업원에게 권리가 귀속되는 경우 종업원은 비밀유지의 의무를 부담하지 않음

제4절 시설관리

□ 시설의 구분

○ 기업의 중요 자산의 침해와 유출을 방지하기 위하여 주요 사무실, 연구소, 중요 장지 설치장소와 시설지역 등을 통제하여 외부인의 접근과 출입을 제한할 필요가 있음

○ 기업 내 주요시설에 대한 관리를 위한 구분은 다음과 같음

<표3-10> 시설의 구분

구 분	정의 및 구역의 예
공용구역	· 기관 내·외부의 모든 인력에게 공개된 구역 (예: 출입문, 로비, 대기실, 엘리베이터, 주차장 등)
일반구역	· 기관 내 인력이나 출입이 허가된 인원에 한하여 공개된 구역 (예: 일반 사무실, 회의실 등)
제한구역	· 기업의 업무를 지원하는 중요 설비가 위치하고 있는 구역 (예: 장비실, 전기실, 기계실 등)
통제구역	· 기술 및 경영정보의 상당수를 보유하여, 침해 및 유출시 기업의 운영에 치명적인 영향을 주는 구역 (예: 연구소, 중요제품 생산라인, 전산실 등)

□ 구역별 보호대책

(1) 공용구역

○ 공용구역에서는 기밀정보의 유출 및 침해가 발생하는 경우가 극히 드물지만 실질적으로 외부인의 출입통제가 이루어지는 구역

○ 외부인의 출입시 이름, 주소, 주민등록번호, 연락처 등 출입자의 주요 정보를 출입관리대장에 기재하고, 내부인력이 직접 공용구역으로 나와 안내하도록 해야 함

○ 외부인의 출입시 카메라, 비디오 카메라 등의 장비 반입을 원칙적으로 통제하여야 함

○ 하지만 출입통제는 임직원이나 외래인에게 과도한 불편을 주어 보호행위 자체에 거부감을 주지 않도록 각별히 유의할 필요가 있음

<표3-11> 공용구역에서의 보호대책

구 분	내 용	사용 가능한 장비
출입통제 시스템	· 시설로 출입하는 인원 및 차량을 통제하는 시스템	· RFID Tag gate · ID 카드 · Interlocking Portal Door
반출입관리 시스템	· 장비, 특히 전산장비의 반출입을 통제하는 시스템	· 정보유출 방지 X-ray · 문형 금속탐지기
화상감시 시스템	· 인원 및 차량 등의 출입여부의 확인을 위한 시스템	· CCTV 등
차량 출입통제 시스템	· 차량의 출입을 통제하기 위한 시스템	· 차량 번호판 인식 시스템 · 역방향 진입금지 시스템
방범 시스템	· 불법적 침입 및 시설의 피해를 경고하거나 방지하는 시스템	· 방탄유리 · 유리파손 알람 시스템

(2) 일반구역

○ 일반구역은 사무실이나 회의실 등 일반인들도 출입승인을 받으면 쉽게 들어갈 수 있기 때문에 주요 정보에 대한 보호수준이 약해지기 쉽기 때문에 의외로 유출 및 침해가능성이 높음

○ 일반구역에서는 외부인과 내부인의 구별이 중요하며, 원활한 식별을 위해 임직원의 사원증 패용이 필수적임

○ 사무실에서 자리 이석시에는 화면보호기를 설정하고 책상을 정리해야 하며, 주요 문서의 경우 캐비넷 보관후 반드시 시건장치를 하며, 복사기·팩스기 등은 사무실 안쪽에 비치해야 함

○ 공용 회의실에서는 회의 종료 후 현장에 관련자료를 남겨 두어서는 안되며, 보드칠판 등에 적힌 내용은 반드시 지워야 함

<표3-12> 일반구역에서의 보호대책

구 분	내 용	사용 가능한 장비
출입통제 시스템	· 구역 내로 출입하는 인원을 통제하는 시스템	· ID 카드
화상감시 시스템	· 인원의 출입여부를 위한 시스템	· CCTV

(3) 제한구역

○ 제한구역에서 직접적인 정보의 유출 및 침해가 발생하지는 않으나 설비들의 훼손, 파괴, 오작동 등으로 유출 및 침해가 발생할 수 있음

○ 제한구역의 경우 근무자 및 관련자는 자유롭게 출입할 수 있지만, 일반직원은 필요시 승인을 받고 출입하며, 외부인의 출입은 통제되어야 함

<표3-13> 제한구역에서의 보호대책

구 분	내 용	사용 가능한 장비
출입통제 시스템	· 구역 내로 출입하는 인원을 통제하는 시스템	· ID 카드 · 인터컴(제한구역)
화상감시 시스템	· 인원의 출입여부를 위한 시스템	· CCTV

(4) 통제구역

○ 통제구역은 기술에 대한 연구가 이루어지고, 중요 정보를 직접 보관하고 있기 때문에 최상위의 보호대책을 강구해야 함

○ 통제구역의 경우 근무자 이외는 출입을 금지하고, 관련자와 일반직원은 반드시 승인을 받은 후 출입하며, 외부인의 출입은 절대 금지되어야 함

<표3-14> 통제구역에서의 보호대책

구 분	내 용	사용 가능한 장비
출입통제 시스템	· 구역 내로 출입하는 인원을 통제하는 시스템	· ID 카드 · 강철 Door · 정맥인식 시스템
도감청 방지 및 전자파 차폐 시스템	· 유리창으로 전해지는 소리의 진동을 증폭하여 도청하거나 전화감청을 탐지 및 방지하는 시스템	· 전자파탐지장치
화상감시 시스템	· 인원의 출입여부를 위한 시스템	· CCTV

□ 재해로부터의 보호

○ 제한구역과 통제구역 등 회사 내 중요시설에 재해가 발생했을 때 그 피해규모는 기업경영에 치명적일 수 있음

○ 따라서 재해발생에 대비한 보호장치를 갖추는 것이 바람직하며, 그 장치로는 전기공급장치, 예비전략 공급장치, 항온항습장치, 누수탐지 및 차단장치, 화재경보 및 자동 진화장치, 침입경보장치 등이 있음

○ 필요시 즉각적인 대응을 위하여 외부 전문기관과의 연계방안이 마련되어 있어야 함

제5절 IT 보안관리

□ 사용자 PC

(1) 개인용 PC

○ 개인용 PC에 ID 및 패스워드를 설정하고 주기적으로 변경하도록 하되 '1234' 등 쉽게 유추할 수 있는 패스워드 사용 지양

- 패스워드 설정시 8자리 이상의 영문/숫자 혼용

- 3회 이상 접속 실패시 잠금 기능 적용

- 한 번 사용된 패스워드는 일정 기간(예: 1년) 동안 재사용 금지

○ 개인용 PC에 화면보호기 및 전용 패스워드를 사용하고 화면보호기 작동시간을 적절하게 지정(예: 10분)

○ PC 보안용 소프트웨어 설치

- 라이선스 없는 불법 소프트웨어 사용 금지

○ 컴퓨터 바이러스에 취약한 개인용 PC에 백신 프로그램을 이용하여 일정한 시간을 정하여 점검을 실시하고, 대부분 컴퓨터 바이러스 백신 프로그램이 보유한 자동 업그레이드와 예약점검 기능을 적극 활용

○ PC에서 작업한 중요문서는 평문 조회가 불가능하도록 암호화 하여 데이터베이스에 저장

○ 외부로의 e-mail 발송시 파일크기를 일정규모 이하로 제한하고, 이를 초과할 경우 부서장의 승인을 얻도록 조치

○ 외부로부터 e-mail을 받았을 때 전송처를 알지 못하거나 스팸 메일로 판단되는 경우에는 삭제하는 것이 좋고, 꼭 열어보고자 하는 경우에는 바이러스 검사를 먼저 실행하여 안전 여부를 확인한 후 열어봐야 함

○ 개인용 PC의 외부 반출시 저장내용 삭제 등 보안조치 후 보안담당부서(혹은 전산정보팀)의 확인·허가를 받은 후 반출

○ CD, 디스켓 등은 일괄 구입한 후 관리번호를 부여하여 관리하고, 중요 내용에 대해서는 별도의 CD 및 디스켓에 보관하여 특별관리

○ 공유폴더를 제거하여 내부 인력 상호간의 자유로운 파일문서 송수신 금지

(2) 휴대용 PC(노트북)

○ 인가되지 않은 휴대용 PC의 사용을 금하고, 초기 동작시 사용자 식별 및 인증절차를 거치도록 조치

○ 휴대용 PC의 하드디스크 내에는 중요정보의 저장을 금지하고, 이동식 저장장치의 사용을 통제

○ 휴대용 PC의 외부 반출시 부서장의 승인을 득한 후 반출

○ 휴대용 PC를 사용하지 않는 경우 캐비넷 등 밀폐된 공간에 시건장치를 하여 보관

○ 노트북 사용자에 대한 보안서약서 징구

- 보안 서약서의 내용은 <별책 p.130>, <별책 p.138> 참조

□ 보조기억매체

○ 보조기억매체의 개념

- 주기억장치에 기억된 데이터는 전원공급이 끊기면 기억된 내용이 소멸되기 때문에 현재 사용되지 않는 데이터에 기억된 내용을 그대로 보존하는 기억장치가 필요한데, 이 때 사용되는 매체를 보조기억매체라고 함

○ 보조기억매체의 관리

- 정부에서 권장하는 보조기억매체의 관리는 국가정보원에서 2007년 4월 제정한 'USB 등 보조기억매체 보안관리지침'(<별책 p.59> 참조)이 있으며, 주요 내용을 요약하면 다음과 같음

<표3-15> 보조기억매체 관리요령

구 분	세 부 내 용
보조기억매체	디스켓, 이동형 하드디스크(HDD), USB 메모리, CD, DVD등
도입시 보안적합성 검사	1. 사용자 식별 및 인증 2. 지정데이터 암호 및 복호화 기능 3. 지정된 자료의 임의 복제 방지 기능 4. 분실시 저장데이터의 보호를 위한 삭제 기능

보조기억매체의 사용	1. 보조기억매체 관리대장에 등재하여 부서장의 승인을 득한 후 사용 2. 등록된 보조기억매체만 사용하며, 업무목적 외의 사적인 용도로 사용될 수 없음 3. 보조기억매체는 일반용, 비밀용, 공인인증서용으로 구분하여 등록 및 사용
보조기억매체의 불용처리 및 재사용	1. 불용처리시에는 물리적 파기를 원칙으로 함 2. 타부서 이전 및 용도전환시에는 자료의 완전 삭제 및 포맷 후 사용 3. 비밀용은 데이터의 완전삭제, 포맷 및 자성소거 후 재사용
비밀용 보조기억매체의 사용 및 관리	비밀용 보조기억매체는 일반용과 마찬가지로 관리번호를 부여하고 이중 시건장치가 있는 캐비넷 등에 보관하며, 사용시에는 보조기억매체 사용대장에 사용목적 등을 작성한 후 사용

□ 정보관리시스템

(1) DRM 시스템 활용

○ DRM(Digital Rights Management, 디지털저작권관리) 시스템은 전자문서 유출을 사전에 방지하고 조직원에 의한 불법 사용내역을 자동 리포트 해 주는 제반 컴퓨터 솔루션을 의미함

○ DRM 시스템은 회사내 구성원끼리 노하우 공유를 위해 현재처럼 검색과 열람은 자유롭게 허용해 주면서도 허가 없는 자료의 무단 복제, 전송, 프린트나 스크린 캡처 등 자료의 무단 유출이 일어날 수 있는 가능성을 사전에 차단해 준다는 데 큰 의의가 있음

○ 만약 권한이 없는 사람이 중요 자료의 복제나 전송, 프린트 등을 시도하면 그 행위는 자동으로 차단되고, 중앙 컴퓨터에 자동으로 보고되어 관리자나 보안담당자가 그 내용을 알 수 있도록 구성되어 있음

○ DRM 시스템은 다음 6가지의 주요 기술과 기능을 결합해 구성해야 함

① 인증처리 시스템

② 암호화 처리 기술

③ 다양한 사용 권한 관리 기술

④ 크래킹 방지 기술

⑤ 사용자의 다양한 환경 및 응용소프트웨어를 지원할 수 있는 모듈 기술

⑥ 출력자 및 유출자 추적 기술

(2) 통합인증권한관리(EAM) 시스템

○ 기업들은 비즈니스의 성공을 위하여 외부로부터의 필요한 접근은 최대한 허용하면서 내부와 외부의 허가받지 않은 불법접근(침입)으로부터 시스템을 보호해야 하는 보안의 요구를 동시에 만족시켜야 함

○ 기업들은 외부로부터의 유해한 접근을 차단하기 위한 목적으로 방화벽(Firewall), 침입탐지시스템(IDS, IPS 등) 등 다양한 보안솔루션을 도입해야 함. 하지만 이러한 시스템은 네트워크의 외부와 내부를 구분하여 외부에서의 접근을 차단하는 데 초점을 맞추고 있으며, 통상적으로 내부에서의 접속은 아무런 제약 없이 허용

○ EAM(Extranet Access Management) 시스템은 말 그대로 엑스트라넷[10]에 사용자가 접근하는 것을 판단해 인증해 주는 솔루션임

- 다시 말해 인터넷을 통해 외부에서 협력업체 및 고객들이 한 번의 로그인으로 다양한 시스템에 접속할 수 있는 환경을 제공하면서도 컴퓨터 시스템에 인증된 사용자에 따라 차등을 부여하는 통합인증 및 권한관리 솔루션이라고 할 수 있음

(3) 지식관리시스템(KMS)

○ 지식관리시스템(Knowledge Management System)은 조직내의 인적자원들이 축적하고 개별적인 지식을 체계화하여 공유함으로써 기업경쟁력을 향상시키기 위한 기업정보시스템을 의미함

○ 이러한 지식관리시스템을 활용하여 기업내 인적자원이 소유하고 있는 지적자산을 기업내에 축적·활용할 수 있어야 하며, 무엇보다 적절한 권한부여를 통해 정보의 무분별한 공유를 막아야 함

---

10) 인트라넷의 확장개념으로 고객 및 협력업체와의 관계 증진을 위해 기업의 내부 통신시스템인 인트라넷에 이들을 포함시킨 새로운 통신구조

□ 백업시스템

○ 내부에서 생성되는 중요 정보에 대해서는 백업하여 관리하는 것이 바람직함

○ 천재지변, 화재 등에 대비하여 데이터센터(IDC)를 활용하거나 적어도 중요 기밀과 문서는 반드시 USB, CD, 디스켓 등에 주기적으로 백업하여 별도 장소에 보관할 필요가 있음

□ 보안점검

○ 다음과 같은 정보처리 설비의 운영절차가 문서화 되어 있어야 하며, 문서화된 내용은 전 임직원에게 공유되어야 함

- 컴퓨터의 가동과 종료절차
- 백업절차
- 유지보수 절차
- 예상치 못한 운영상 또는 기술적 어려움이 발생했을 때 지원연락처
- 비밀정보를 포함한 출력물의 관리 및 폐기절차
- 시스템 오작동시 시스템의 재시작 및 복구절차

○ 네트워크와 서버 및 DB현황에 대한 보안점검은 정기적으로 이루어져야 하며, 보안점검시 아래와 같은 사항을 주로 확인하여야 함

1) 네트워크 보안점검

- 방화벽에 관리자 이외의 계정이 있는지 확인
- 침입탐지시스템(IDS, IPS 등)에 관리자 이외의 계정이 있는지 확인
- 운용기록(log)에 대한 관리 및 유지여부
- 소프트웨어, 하드웨어의 변경사항 관리여부 등

2) 서버 및 DB 현황

- 시스템 로그 분석
- 최근 3개월 전까지의 시스템 로그가 보관되어 있는지 확인
- 로그파일의 백업여부 확인
- 시스템 취약성에 대한 점검이 주기적으로 이루어졌는지 여부 확인
- 패스워드 변경 및 접근권한 확인 등

□ 장애발생시 대응

○ 기업 내부에서 보안시스템에 장애가 발생하는 경우 장애내용이 보고되어 아래와 같은 대응절차를 바탕으로 즉각적인 조치가 이루어져야 하며, 규모가 작은 기업의 경우 전문업체를 활용하여 유지, 보수 및 점검하는 것이 효율적임

- 비상시 따라야 할 절차와 관련자의 책임규정
- 유관기관과의 연락체계 구성여부
- 제한된 시간 내에 필수업무 및 지원서비스를 대체장소로 이전하여 운영하기 위한 절차
- 정상적인 사업활동으로 복귀하기 위한 원상복귀 절차
- 위기관리를 포함한 비상절차 및 프로세스에 대한 임직원 교육

○ 외부로부터의 불법적인 침입이 의심되거나 탐지되는 경우 아래와 같은 기관에 지원을 요청해야 함

<표3-16> 정보시스템 불법침입시 지원기관

기관명	세 부 내 용	
정보통신부 사이버패트롤	전 화	1377 또는 02)3415-0112
	전자우편	singo@kiscom.or.kr
	홈페이지	http://www.cypatrol.or.kr/
국가정보원 산업기밀 보호센터	전 화	111 또는 02)3412-3800
	전자우편	홈페이지에서 신고
	홈페이지	www.nisc.go.kr
경찰청 사이버테러대응센터	전 화	주·야간 : 02)3939-112
	전자우편	cyber112@npa.go.kr
	홈페이지	www.ctrc.go.kr
한국정보보호진흥원 인터넷침해사고 대응지원센터	전 화	주·야간 : 118 (지방은 02-118)
	전자우편	cert@krcert.or.kr
	홈페이지	www.krcert.or.kr

제6절 계약관리

1. 기술계약의 유형

○ 기술계약은 계약의 성격에 따라 공동연구계약, 투자유치계약, 라이선스계약, 제조위탁계약, 인수합병계약, 합작투자계약 등으로 구분할 수 있음

<표3-17> 기술계약의 유형

구 분	설 명
공동연구 계 약	둘 이상의 파트너가 상호의 보완적인 자산 및 정보를 제공하여 합의된 공통의 기술개발 목표달성을 위하여 추진하는 계약
투자유치 계 약	R&D활동을 마친 후 당해 기술홍보를 통한 사업화를 도모하기 위해 외부로부터의 투자를 유치하는 계약
라이선스 계 약	기술제공자가 상대방인 기술도입자에게 특정기술에 대하여 실시권을 허락하는 계약
제조위탁 계 약	하청위탁자가 하청자에게 특정기술을 제공하고 상대방에게 자기의 기관으로서 당해기술을 실시하게 하는 계약(하청 라이선스 계약이라고도 함)
인수합병계약 (M&A)	당사자 일방이 기술의 소유권을 이전하는 계약과 둘 이상의 회사를 하나의 회사로 합병하는 것을 목적으로 하는 계약
합작투자계약 (JV)	2인 이상의 업자 간에 단일특정의 일을 행하게 하는 출자계약 또는 공동계약

2. 기술계약 체결시 유의사항

□ 계약 전 점검

○ 기본적으로 제휴 상대방은 계약 당시까지의 거래실적을 참고하여 신뢰관계가 있는 기업 중에서 선정하는 것이 가장 무난함

- 상대방의 사업내용 및 평판, 계약 이행능력 및 기술수준 등을 면밀히 검토해야 함

○ 기술계약과 관련한 사항(기술제공, 지적재산권, 라이선스 등)에 대한 법제도의 조사를 실시하여야 하며, 기술계약의 이전단계에서는 기술제공자는 비밀의 보호를 위하여 비밀유지 및 보호에 관련된 계약을 체결해야 함

□ 교섭 단계

○ 일반적인 기술계약단계 중에서 교섭단계가 기술유출이 가장 일어나기 쉬우며, 계약이 결렬될 경우를 미리 가정하여 개발 노하우 등 중요 정보를 제공하는 것을 조심해야 함

○ 합의까지 장기간 소요되거나 합의불성립으로 교섭이 결렬될 가능성이 높다고 하더라도 안이한 타협을 하지 않아야 함

○ 교섭상 유연한 대응은 필요하지만 타협 불가능한 부분을 사전에 명확히 규정해 주고, CEO와 계약교섭 담당자간 상호 인식을 공유하는 것도 바람직함

□ 계약서 작성 단계

○ 만약에 발생할 지도 모르는 기술유출에 대비하여 법적수단을 강구할 수 있도록 목적 외 부당이용 금지, 서브 라이선스 금지, 철저한 영업비밀 관리 등의 주요 사항들을 계약서에 명기해 두어야 함

○ 기술의 목적 외 남용을 금지하기 위해서는 핵심기술과 주변기술을 같이 패키지로 이전할 경우 계약서에 용도 외 사용금지 규정을 두어야 하며, 기술유출을 방지하기 위하여 비공개로 전문가의 판단을 얻을 수 있는 중재조항을 계약서에 삽입해야 함

3. 기술계약 유형별 대응방안

□ 공동연구계약

○ 공동연구계약은 둘 이상의 파트너가 상호 보완적인 자산 및 정보를 제공하여 합의된 공통의 기술개발 목표달성을 위하여 추진하는 계약을 의미하며, 기술의 전문화, 융합화 등이 촉진되면서 공동연구의 의존도가 갈수록 증가하고 있음

○ 공동연구개발성과인 기술을 이용한 다른 연구개발제한이나 제품생산제한은 공정거래법을 위반하는 불공정행위가 될 수 있으므로 공동연구계약 전 다음과 같은 사항들을 반드시 사전에 조사 및 검토해야 함

- 공동연구 범위(공동연구의 목적)의 명확화
- 상대방의 기술력, 신뢰성(경제력을 포함), 자사와의 관계, 성과의 실시에 대한 적합성(판매력, 생산력 등)
- 자사의 현재 보유기술과 그 권리화의 필요성
- 상대방에게 개시할 기술자료와 그 비밀유지의 필요성
- 자사의 분담능력(연구인력 및 연구비 분담)
- 연구분야에서 자사의 경업자와 그의 역량
- 제3자 소유의 특허발명 등과의 권리저촉관계
- 연구성과의 사업화 구상
  - 실시의 시기 및 실시형태, 실시의 분담, 실시에 의한 수익과 분배
- 다른 계약과의 저촉관계
  - 새로 공동연구계약을 체결하는 경우 이미 자사의 타부문이 체결하고 있는 계약과 중복 또는 저촉하는 경우가 있을 수 있으므로, 이러한 상황을 피하기 위해 계약을 전사적으로 체크할 필요가 있음
  - 특히 연구주제와 동일하거나 밀접한 연구주제에 대하여 제3자와 공동연구를 하거나 수탁을 하지 못하도록 하는 규정이 있을 때 계약위반이 될 수 있으므로 유의하도록 함
- 「독점규제 및 공정거래에 관한 법률」과의 관계
  - 아래의 공동연구계약상의 불공정거래행위 유형을 참고하여 가급적 위반되지 않도록 함

<표3-18> 공동연구계약상의 불공정거래행위 유형

공 정	불공정 우려
· 공동연구개발에 필요한 기술정보 공개 · 공개된 기술정보에 대한 비밀유지 의무 · 연구개발을 위한 부담 · 공동연구개발주제와 동일주제의 연구개발 제한 · 성과의 정의, 귀속, 비밀유지조항 · 노하우의 비밀유지를 위해 단기간에 한해 제3자와 공동연구개발 제한 · 성과의 개량발명 등 상대방에 공개·비독점 실시허락의무 부과 · 성과와 관련된 실시료의 분배	· 기존 기술의 사용제한 및 제3자 실시허여 제한 · 공동연구 개발성과를 사용한 제품 이외의 제품에 대한 생산·판매활동 제한 · 공동연구개발 주제 이외의 연구개발 제한 · 성과를 이용한 연구개발활동에 대한 필요 이상의 제한 · 성과의 개량발명 등의 상대방에 양도 또는 독점적 실시의무에 대한 제한 · 제품의 생산·판매·지역제한, 생산·판매수량제한, 판매처·판매방법제한, 원재료·부품구입처제한, 품질·규격제한 등(상대방의 사업활동을 부당하게 구속하고 제품시장에서의 경쟁 감퇴여부 판단에 의함)

<표3-19> 공동연구계약시 기술유출 대응방안

계약단계	기술 유출 및 침해 대응방안
공동연구과제 계획서 검토단계	· 공동연구의 후보기업 및 후보자가 자사의 기술유출 방지전략을 철저히 이행할 수 있는지를 확인 · 계획서 검토를 위한 실무협의과정에서 자사의 사업, 기술전략이 유출되지 않도록 사전 교육 · 연구과제를 세분화하여 각 연구자에게 전체상을 보이지 않도록 함으로써 자사의 중요 기술의 개시를 제한
공동연구 계약단계	· 사후 분쟁을 피하기 위하여 상대방과 공동연구 범위의 명확화, 지적재산권이나 노하우 등 권리의 귀속, 위반시 벌칙 등을 규정 · 공동연구개발에 성공하여 상용화 할 경우에 대비한 명백한 규정을 마련 - 제조, 판매는 어느 당사자가 하는가? - 제동연구개발 성과인 기술을 이용한 다른 연구개발 제한 - 공동연구개발 성과를 이용한 제품생산 제한
공동연구 결과물 사후관리 단계	· 공동연구 결과물에 대해 계약에 기재된 범위를 넘어선 성과의 활용이 양 당사자간의 합의 없이 발생했는지 감시 · 공동기술계약에 포함되지 않은 기업의 기술정보가 장비 등에 내재되어 공동기술개발업체에 유출되지 않도록 주의해야 함

○ 계약서의 내용은 <별책 p.146> 참조

□ 투자유치계약

○ 투자유치계약은 일반적으로 R&D활동을 마친 중소·벤처기업이 당해 기술의 사업화를 도모하기 위해 외부로부터의 투자를 유치하는 계약을 말하며, 이 경우 당해 기술에 대한 설명을 자세히 하게 되므로 기술유출 가능성이 상당히 높게 나타남

<표3-20> 투자유치계약시 기술유출 대응방안

계약단계	기술 유출 및 침해 대응방안
투자상담 단계	· 기업의 기술·사업 전략 정보를 제공하는 과정에서 자사의 신기술 혹은 신제품 아이디어가 유출되지 않도록 주의해야 함
예비심사 단계	· 투자 전문가들이 회사개요를 파악하고, 시장 및 기술에 대한 1차 검증을 하는 단계로, 자사의 사업계획서가 투자기관에 제출되므로 기술정보 유출의 위험성이 크게 나타남 · 하지만 자사기술의 우수성을 입증하기 위해 기술의 핵심적인 부분까지 공개하는 것은 피해야 함
공개 프레젠테이션 단계	· 프레젠테이션 단계에서 공개된 기술정보가 경쟁기업에 유출되지 않도록 주의해야 함 · 투자유치에 불리한 상황에 처하더라도 질의 및 응답과정에서 필요이상의 기술정보를 언급하지 않아야 함
본심사 단계	· 본심사에서 자사의 기술에 대해 투자심사역들이 명확히 이해하지 못하는 경우가 많기 때문에 외부 전문가의 자문을 구하는 것이 일반적인데, 이 경우 외부 전문가에 의한 기술정보 유출에 주의해야 함
사후관리 단계	· 투자가 결정되면 투자기관이 주요 경영사항에 대해 지원하게 되는데, 이 경우 기업의 비밀정보를 공유하게 되므로 외부로의 유출을 차단하기 위한 수단을 강구해야 함

○ 계약서의 내용은 <별책 p.152> 참조

□ 라이선스계약

○ 라이선스계약은 일명 실시권 설정계약이라고 하며, 제품이나 기술을 독자적으로 개발하는데 필요한 시간과 자원을 별도로 투입하지 않고 그 제품이나 기술을 획득하는 방법을 말함

○ 라이선스 계약시에는 핵심이 되는 중요 사항들을 미리 확인하고 핵심 조건들이 수용되지 않을 경우를 대비하여 대안을 마련하여 계약서에 포함시키도록 함

○ 조금이라도 유리하게 계약을 체결하고자 한다면 상대방에게 계약서 작성을 양보할 것이 아니라, 다른 라이선스계약서를 참조하거나 아래 점검사항들을 따라 스스로 계약서를 작성하는 것이 효과적

○ 계약의 전반에 걸쳐 기술 자체가 이전되어 버리는 결과를 가져올 수 있으므로 계약 체결 전 다음과 같은 사항들을 반드시 확인하도록 함

<표3-21> 라이선스계약시 점검사항

조 항	점검사항	비 고
1. 전 문	a. 계약 당사자의 명칭 등의 표시 (회사명, 본점 소재지, 창립 준거법) b. 계약 목적의 개요의 표시	b. 국내 계약인 경우에만 기재
2. 정 의	a. 특히 대상 기술은 상세하게 정의함. 본문과 함께 첨부, 부속서 등을 이용하여 오해가 없도록 정의를 내리고 Patent Lists를 첨부 b. 주요 정의 대상 항목: 본 기술, 본 제품, 본 특허, 노하우, 판매 가격, 고객, 화폐, 상표권, 관련회사, 허락지역, 선적, 개량 기술, 비밀정보 등	a. 특허 계쟁 회피를 목적으로 한 라이선스 계약에서는 대상 특허의 정의는 국가명과 특허번호만 기재하면 됨 b. 생략형(Abbreviation)도 자주 사용

조 항	점검사항	비 고
3. 라이선스 대 상	a. 라이선스의 형태: 독점 또는 비독점인가, 독점인 경우 라이센서는 자기 실시 가능한가, 재실시권 첨부인가 b. 실시 허락의 제한, 범위 - 제조, 판매제한(지역, 수출처, 생산량, 목적, 용도 등) - 허락 지역 이외의 취급(수출 금지 또는 라이센서의 승인 사항여부) - 국내 라이선스 허락인 경우 타국의 라이센시가 제조한 제품의 국내수입이 제한되어 있는가 c. 특허 라이선스 허락특허 표시, 특허 리스트의 제시 d. 노하우, 라이선스 라이선스 범위의 특정, 기술이전·기술 정보 제공 범위의 특정 e. 상표 라이선스가 부수되어 있는 경우 - 상표의 제시는 의무 또는 권리 - 사용 형태 - 품질 관리 규정	비독점인 경우 다른 라이센시의 유무, 가능하면 다른 라이센시의 명칭을 확인 c. 국내 특허 라이선스계약인 경우에는 전용실시권인지 통상실시권인지를 명시
4. 제한조항	a. 경합 또는 유사 제품 기술의 사용·판매제한은 있는가, 그 예외 규정은 마련되어 있는가(예: 고객으로부터의 요청이 있는 경우에는 경합품의 사용이 가능 등) b. 계약 종료 후에도 당해 제한 조항이 계속되는가(특히 노하우, 라이선스의 경우) c. 라이센시의 판매와 관련된 최선 노력 의무(Best Efforts)가 있는가	a. Non-Exclusive 라이센싱의 경우 독점금지법과의 관계를 체크 b. 합리적 기간을 초과하는 경우 독점금지법 저촉의 우려가 있음

조 항	점검사항	비 고
5. 기술료와 지 불	a. 계약 일시금(선급금, 개시비, 기술 이전비)은 있는가 b. 로열티의 계산방법은 무엇인가 - 정액법: 일괄 지불(Paid up Royalty) - 요율법: 판매 가격에 대한 요율(%), 요율의 대상이 되는 가격(순판매액) - 종량법: 제품 단위당 금액 및 그 산출 기준 및 슬라이드제 c. 최저 실시료(Minimum Royalty)는 있는가(적용 기준, 연단위로 부과하는가, 연기 규정이 있는가, 달성하지 않은 경우에 라이센서의 해제권과의 연동, Non-Exclusive Right로의 변경 등) d. 증설, 확장, 신제품 적용의 경우의 추가 요금의 필요성 여부 e. 실시료의 지불 방법 - 기간: 제1회, 마지막, 회수(연1회, 반년마다, 매분기마다 등), 미완성품의 처치 - 지불 조건: 은행 송금(수수료 부담) - 통화: 상대국 통화 또는 자국 통화, 외환 환전 방법 - 계약서에 지불처에 대한 명기여부 f. 회계감사, 기타 - 보고서(양식, 내용, 제출시기) - 라이센서의 회계감사(Audit)권, 외부 감사역의 기용 및 권한 - 실시료 산정 기록의 작성 및 보관(라이센시)	b. 실시료의 대상이 되는 가격(예: 순판매가격)의 정의는 의문이 생기지 않게 신중하게 정하도록 함 c. 최저 실시료는 독점적 실시권에 수반하는 경우가 많음 d. 특히 프로세스·라이선스의 경우 f. 회계감사권은 라이센시에 대한 견제 역할을 하므로 라이센서에게는 필요한 조항

조 항	점검사항	비 고
6. 세 금	a. 원천 소득 과세를 라이센시가 로열티로부터 징수하여 당국에 지불하고, 그 Tax Receipt를 라이센서에게 송부하는 규정의 유무 b. 라이센서가 세금을 부과하지 않는 경우의 조치(예: 로열티의 증액 등)	a. 원천 소득세의 감액은 라이센시에 의한 조세 협정에 기초한 신고가 필요
7. 기술이전 및 기술정보 제 공	a. 기술이전과 기술 정보 - 기술이전에 수반되는 제출 정보의 특정(기술 정보의 내용 체크) - Basic Eng'g Package 의 제출과 라이센시가 작성한 Detailed Eng'g Package의 체크(프로세스·라이선스의 경우) - 교육훈련의 일정, 장소, 인원수, 경비 부담 - 프로세스·라이선스에 대해서는 설비 설치 장소의 특정, 조건 - 건설, 제작, 운전의 지원, 라이센서의 기술자의 파견 - 시운전 입회, 성능 시험 참가 b. 설비 견학 등 - 라이센서의 설비의 견학 - 라이센시의 설비에 대한 라이센서의 고객의 방문	a. 특허 라이선스의 경우에는 적용하지 않음. 모든 기술 정보를 특정하고 계약 부속서에 기재(예: 기본 설계서, 상세 설계도서, 제조, 제작에 관한 기술 정보(원재료, 부품, 제조공정, 원료원단위, 사양서, 도면), 운전 매뉴얼(설비의 유지, 보전, 보수, 안전 대책 등), 시험 방법, 원료 및 제품의 규격) b. 제공 정보의 비밀 유지 의무, 목적 외의 사용제한은 비밀 유지조항에서 취급
8. 비밀유지	- 비밀정보의 정의 - 비밀정보의 특정(날인) - 비밀 유지 의무, 목적 외 사용 금지 - 제외 규정(공지 공용, 개시의 시점에서 소유, 정당한 권리자로부터 개시 제한 없이 입수)	a. 노하우와 라이선스의 경우에만 적용

조 항	점검사항	비 고
8. 비밀유지	- 비밀 유지 기간(영구는 피함), 라이선스계약 기간 종료와의 관계 - 비밀 서류의 복사·복제의 금지 또는 제한, 종업원 등의 비밀 유지 - 비밀 서류의 요구에 의한 반환 의무 - 하청업자의 비밀 유지(동일한 비밀 유지 의무를 부과한 후 개시)	b. 이하의 사항을 반드시 검토하도록 함 - 노하우의 라이센서에 의한 비밀 유지 필요. - 개량정보의 교환도 있고 상호 비밀 유지의무가 바람직함 - 구두로 전해진 비밀정보는 추후 문서로 제출
9. 특허침해	a. 제3자 특허 침해 책임 - 라이센서가 책임을 지고 라이센시를 면책하게 할 침해하고 있거나 침해의 우려가 있는 제3자 특허의 특정 - 라이센시가 침해 경고를 받은 경우 라이센서에 대한 통지 의무 - 대응책의 검토(설계 변경, 특허 무효 청구, 라이선스 취득, 사업 중지) - 라이센서의 특허권자와의 절충과 분쟁 해결 의무 - 라이센서의 책임의 한도 b. 특허권 침해의 배제와 구제 - 제3자가 허락 특허권을 침해한 경우 라이센서에 의한 대응과 라이센시에게 대응 권한의 위임. 비용의 결정 - 침해자로부터의 손해 배상금의 분배	a. 라이선스계약 체결일 이후의 특허 - 라이선스계약 체결일 이후의 특허 등 라이센서가 라이센시를 특허 침해로부터 면책한다는 표현이 많음 - 라이센서로서는 책임 없는 것으로 하는 경우가 많음(라이센서의 책임 한도는 실시료의 ○○%라는 규정도 많음) b. 제3자가 지역 내에서의 허락특허를 침해하는 경우 라이센서의 소송사항이기는 하나 라이센서의 의뢰에 의해 라이센시가 소송하는 경우가 있으며 수령한 배상금은 분배함

조 항	점검사항	비 고
9. 특허침해	c. 기타 - 라이센서의 허락 특허권의 유지 의무 - 특허의 유효성과 관련된 보증	c. 라이센서의 의무로서 특허의 유지, 노하우의 비밀 유지, 특허가 유효한 것의 보증이 있는데, 이들을 계약에 기재하는 것은 매우 어려운 교섭이 됨. 공정거래위원회의 가이드 라인을 체크
10. 금반언 (不爭의무)	a. 라이센시는 허락 특허의 유효성에 대해 다투지 않음. 만일 다툰 경우에는 라이센서에게 계약 해제권이 있음	
11. 개량기술의 취 급	a. 허락 특허 및/또는 노하우의 개량 - 특허, 노하우(기술 정보)에 대한 개량의 정의, 기술의 종류, 범위, 용도, 목적 등 - 상호 의무의 확인 - 개시의 시기, 방법, 조건(무상 또는 유상, 본 계약 조건과의 상이 여부) - 소유권, 특허권은 발명자에 속하고, 상대방에게 재실시권부 통상실시권을 허락(실시조건을 상세히 기재)	a. 공정 거래 위원회의 가이드라인 체크가 필요하며, 신중히 대응할 필요가 있음 b. 특히 개량 발명의 양도, 독점・실시권의 허락에 대해서는(대가가 수반되는 경우는 별도로 함)독점금지법상 문제가 많음
12. 성능보증	a. 생산 능력, 원료 수율, 품질, 용역 사용에 관한 보증	a. 노하우·라이선스계약상에서 성능보증은 일반적임. 왼쪽의 내용은 프로세스·라이선스를 상정하여 작성하였음

조 항	점검사항	비 고
12. 성능보증	b. 보증 조건 - 라이센서 제공 정보와 동일하게 설비 건설, 운전, 원재료의 조달 - 시운전(예: 48시간 운전)으로 보증 수치 달성 시 보증 완료 - Deemed Acceptance 조항의 기재 - 성능 미달의 경우의 결정(수정, Liquidated Damages의 지불 등) - 최고 책임 한도액의 설정(예: 로열티의 50% 등) - 제공 기술정보의 보증(일종의 하자 담보)	b. 'Deemed Acceptance 조항의 기재'는 어느 일정 기간 내에 라이센시의 사정으로 성능 보증 운전을 실시할 수 없는 경우 당해 기간 경과시에 검수로 간주하는 규정임
13. 라이선스 계약의 발 효	a. 계약 발효일(계약 발행일의 조건) - 모두(冒頭)의 일자(First Above Written) - 정부 인가가 필요한 계약의 경우에는 인가를 받은 날 - 제1회의 대가 지불일 등 b. 정부 인가를 취득할 수 없는 경우의 조치	a. 국제 라이선스계약의 경우 상대방 나라의 외환 관리 규정에 주의하여 입금 전에 기술 정보의 개시가 없도록 주의를 함 b. 계약 해지권, 중단 등의 조치를 규정
14. 계약기간 /계약해제	a. 계약 기간(시기(始期) 및 종기(終期), 연장 규정(1년마다 자동 연장) b. 라이센시의 의무 위반, 실시 태만에 대한 계약 해제 규정 c. 상대방의 도산에 관한 해지권 d. 양당사자 중 어느 일방에 의한 영업의 폐지, M&A에 의한 계약의 해지, 변경 등 e. 10년 이상의 라이선스계약은 계약 기간 중 변경조항의 마련	c. 라이센서의 도산, 파산의 경우, 라이센서의 기득권을 확보하는 처치가 필요. d. M&A 에 의한 기업 통합은 라이센서, 라이센시 쌍방에 큰 영향이 있으므로 상대방의 기업 자본 구성의 대폭 변경도 포함하여 해지조건으로 할 필요가 있음

조 항	점검사항	비 고
15. 면 책	a. 허락 기술의 실시, 제품의 사용에 대하여, 라이센시는 라이센서를 면책하고, 배상 의무를 면제 b. 간접 배상 무담보	a. 가능한 한 쌍무로 함 b. 가능한 한 쌍무로 함
16. 기 타	a. 양도: 계약의 양도 금지, 또는 사전 승인에 의한 양도 가능의 기재 b. 불가항력(Force Majeure): 불가항력 사유의 예시, 라이센시, 라이센서 쌍방에의 적용 c. 계약 준거법: 라이센서가 속하는 나라의 법률이 준거법이 되는 경우가 많음 d. 분쟁의 해결(Arbitration) - 재판관할의 기재 또는 중재판정의 기재(예: International Chamber of Commerce) - 중재지의 규정(제3국이 바람직함) - ADR 등의 검토 - 신의성실에 의해 협의로 해결(국내계약) e. 계약 해석·변경 - 완전한 합의: 계약 서류가 유일한 합의 서류이고 계약 발효일 이전의 합의, 메모, 결정 등은 효력을 상실 - 계약언어(국제 계약의 경우 영어가 바람직) - 계약의 어느 조항이 법률에 저촉된 경우 그 조항만이 무효가 되고 나머지는 유효함	a. 가능한 한 쌍무로 함. M&A에의 대항으로서도 사용 가능 b. 예견 가능성은 불가항력 요건이 아님 c. 제3국법을 제안하는 경우도 많음

조 항	점검사항	비 고
16. 기 타	- Non-Disclaimer(권리비포기): 어느 권리를 행사하지 않는다고 해서 당해 권리를 포기한 것은 아님 - 경제변동시 로열티의 변경 f. 최혜국 대우(Non-Exclusive Licensing의 라이센시에게 적용) g. 통지: 쌍방의 연락처 명기, 통신수단	- 일반적이지는 않지만 정액 지불의 경우 설정하는 경우가 있음 g. e-mail의 취급방법
17. 서명란	계약 당사자의 서명 권한자의 직위 및 성명의 기재(서명일, 장소의 기재가 있는 경우도 있음)	체결지법과의 관계주의

○ 계약서의 내용은 <별책 p.155> 참조

□ 제조위탁계약

○ 흔히 OEM계약이라고 하며, 기술면에서 우위에 있는 기업이 자체 내에서 생산공정을 수행하지 아니하고, 외부에 생산을 위탁하는 계약형식을 규율하는 것이 일반적임

○ 수탁자가 위탁자에 비해 기술수준이 낮은 경우가 대부분이기 때문에 위탁자에 의한 기술지도가 필수적이며, 이와 관련하여 생산공정, 제조설비, 기술지도 등 전범위에 걸쳐 기술유출이 일어날 가능성이 높음

<표3-22> 제조위탁계약시 대응방안

구 분	기술 유출 및 침해 대응방안
전략의 수립	· 노동집약적 공정은 해외에서, 기술집약적공정은 국내 혹은 지적재산권 보호가 가능한 국가에 두는 것을 원칙으로 하고 생산에 필요한 것만 현지에 이전해야 함
기술지도	· 제품 생산에 필요한 범위 만큼에 대해서만 지도해야 함
생산공정 관련 유의사항	· 중요한 제조공정 등은 특정 본사로부터 파견된 직원만 관여하도록 조치해야 함 · 외부판매제한, 자사의 중요한 노하우의 보호의무, 위반행위에 대한 처벌 관련 조항 등을 계약서에 삽입해야 함 · 본사에서 핵심부품을 모듈화하여 수출하고 해외에서 조립 · 순정품에 대한 위조방지 대책을 강구해야 함
제조설비에 대한 산업기술 보호유지	· 핵심 제조공정이 포함된 도면이나 서류의 블랙박스화를 추진할 필요가 있음 · 해외에 도면을 제공하는 경우 제조도면상에 게재된 시험방법, 소재정보 등 개발 노하우를 삭제하고 제공해야 함 · CAD/CAM 데이터는 현지 컴퓨터로 읽을 수 없도록 암호화해야 함
설비의 유지, 보수 관련	· 유지보수를 직접 수행하고 부득이하게 현지인을 고용할 경우 출입지역을 한정해야 함 · 설비의 판매계약에 제조설비의 정기적인 유지보수 조항을 삽입해야 함

○ 계약서의 내용은 <별책 p.161> 참조

□ 인수합병계약

○ 합병계약(Merger)이란 둘 이상의 회사가 청산절차를 거치지 않고 하나의 회사로 합쳐지는 것을 말하며, 인수계약(Acquisition)이란 인수기업이 주식매매와 자산매매를 통해 실질적으로 대상기업의 기업지배권을 넘겨받는 것으로 법률적으로 인수기업과 피인수기업은 개별적인 법인체로서 독립성을 유지함

○ 인수합병계약 역시 투자유치계약과 마찬가지로 추진과정에서 기업의 기술정보 대부분이 공개될 수 있으므로 기술유출의 위험성이 높게 존재함

<표3-23> 인수합병계약시 대응방안

계약단계	기술 유출 및 침해 대응방안
경영전략 수립 및 M&A 전략팀 구성	· 중요 산업기술은 원칙적으로 이전을 금지해야 함 · 중요 기술의 이전 필요시 M&A 전략팀에 의해 기술이전에 따른 피해 최소화 및 비밀유지 전략을 수립해야 함
인수의향서 및 비밀유지계약 체결	· 실제 계약서가 작성되어 법적으로 보호받을 수 있기 전까지 산업기술에 대한 세부자료가 제공되지 않도록 주의해야 함
정밀실사, 기업가치 평가 및 가격결정	· M&A 중개기관을 통하여 업무를 추진하는 경우 중개기관에 의해 산업기술이 무단 사용되지 않도록 비밀유지계약을 체결해야 함 · 중개기관을 통하지 않을 경우 비밀유지계약을 체결하고 재확인한 후 정밀실사(Due Diligence)를 진행해야 함
협상 및 계약서 작성	· 합병계약서에는 자료보존 방법과 유출의 금지, 제한에 관한 조항을 삽입해야 함 · 계약단계에서 근로자와의 보안서약서를 징구해야 함 · 개인이 비밀을 유출한 경우 합병상대기업의 연대책임을 명시해야 함

○ 계약서의 내용은 <별책 p.164> 참조

□ 합작투자계약

○ 합작투자(Joint Venture, JV)란 공동의 목적을 가진 둘 이상의 회사가 공동의 자본출자로 신규기업을 설립, 경영의 위험과 역할을 분담하여 공동의 목표를 추진하는 경영전략을 말함

○ 합작투자에 의한 법인은 별도 법인으로서 유한책임 회사이기 때문에 합자기업의 위험부담 및 이윤분배는 합작 당사자의 출자지분에 따름

<표3-24> 합작투자계약시 대응방안

<table>
<tr><th>계약단계</th><th>기술 유출 및 침해 대응방안</th></tr>
<tr><td>대상기업 발굴</td><td>· 대상기업이 비밀유지 의무에 대한 이행능력이 있는지 여부를 확인해야 함</td></tr>
<tr><td>의향서(MOU)
체결</td><td>· 합작투자 할 상대방을 발굴하는 단계에서 상대방 기업에 핵심적인 기술정보에 대한 자세한 사항을 제공하지 않도록 주의해야 함
· 세부 계약 조건에 대해 신의성실의 원칙에 따른 의무를 부과하고 주요 기술에 대하여 제3자에게 공개하거나 이를 임의로 이용하지 않을 의무를 부담하도록 해야 함</td></tr>
<tr><td>합작투자기업
설립절차 진행</td><td rowspan="3">· 합작투자기업을 설립하는 팀의 담당자로부터 비밀유지서약서를 징구해야 함</td></tr>
<tr><td>최종계약
체결</td></tr>
<tr><td>합작투자기업
설립 완료</td></tr>
</table>

○ 계약서의 내용은 <별책 p.167> 참조

제7절 글로벌 보안관리

□ 해외 진출시 기술이전

○ 진출형태

- 핵심기술 및 첨단기술의 해외이전은 독립법인 형태로 진출하여 자체 보호함으로써 유출의 위험성을 줄여야 함
- 합작법인 형태를 통한 진출시 합작기업 역시 기술이전을 전제로 하는 경우가 대부분이므로 이전할 기술과 보호할 기술을 명확히 하고 보호대책을 공동으로 강구하여야 함

○ 진출목적

- 첨단제품과 기술은 지적재산권 보호가 우수한 국가에 진출하는 것이 바람직함
- 노동집약적이거나 비핵심 사업의 경우 해외 생산을 목적으로 인건비가 저렴한 국가로 이전하므로 보편화된 기술을 이전하는 것이 일반적이지만 중요 기술을 이전해야 하는 경우에는 이들 국가가 기술에 대한 권리보호에 취약하므로 별도의 대응책 마련이 필요함

□ 해외 기술이전시 기술보호

○ 기술을 영업비밀로 보호하고자 할 때에는 철저한 보호대책이 먼저 마련되어야 함

- 국내에서 영업비밀로 보호하고 있는 기술이라도 지적재산권 제도가 미흡한 국가에 진출할 때에는 사전에 특허를 출원하여 권리화를 완료한 후에 진출하는 방안도 검토할 필요가 있음

○ 특허 등을 통한 권리화도 중요하지만 생산공정, 상세기술, 운영기술 등 영업비밀로 보호할 기술이 있음에 유의해야 함

○ 이전할 기술의 가치평가와 기술이전시 예상수익, 현지 국가의 법률과 제도로 이전할 기술의 보호가 가능한지를 먼저 분석한 후 이전

□ 해외 진출시 현지 적응전략

○ 현지 채용인력들과의 우호적인 관계

- 성공적인 해외 진출 및 기술보호를 위해서는 글로벌 인적자원관리가 필수적이며, 무엇보다 현지 채용인력들과의 우호적인 관계 유지가 중요함

○ 현지 파트너와의 우호적인 관계

- 현지 파트너와의 우호적인 협력관계를 유지하고, 민감한 사항에 대해서는 반드시 문서화를 통해 구체적으로 명시해야 함

○ 현지 당국과의 우호적인 관계

- 현지 당국과의 우호적인 관계를 유지하여, 비밀 유출 및 침해시 적극적으로 활용할 수 있어야 함

□ 해외 진출시 인적자원관리

○ 내국인과 현지인의 업무구분

- 해외에 진출한 국내 기업의 경우 근로자의 대부분이 현지인이므로 기술유출 및 침해의 위험성이 높음

- 생산현장 근로자의 대부분이 현지인이더라도 핵심기술 및 시설의 보호담당은 내국인이 맡아야 함

○ 입사, 재직, 퇴사 등 단계별 보안관리

- 현지 채용인력의 경우 가능한 회사의 비밀정보에 대한 접근을 제한하고, 불가피하게 접근해야 하는 인력 채용시에는 당사자의 신뢰성을 우선적으로 고려해야 함

- 국내외를 막론하고 재직자를 통한 기밀유출이 많으므로 특별한 관리가 필요함

  · 서약을 하는 사람의 인적사항, 재직 중에는 물론 퇴직 후에도 일정기간 비밀유지를 할 의무 존재, 재직 중에 개발하였거나 생산한 모든 기술과 영업정보는 회사에 귀속된다는 내용이 포함된 보안 서약서 징구

  (보안서약서는 진출 국가의 제도나 관습 등을 고려하여 징구하여야 함)

  · 영업비밀 보호를 위한 보안교육 실시

- 퇴직자는 그 나라의 특별한 법령이 없는 한 모든 국가의 보편적 계약에 의해 영업비밀유지의무를 부과할 수 있음

  · 이를 위해서는 재직 중에 영업비밀을 취급하였거나 관리한 적이 있어야 하며, 영업비밀을 유지할 의무와 책임이 퇴직 후에도 있다는 선행 서약이 있어야 함

  · 중국 노동계약법(2008. 1. 1. 시행예정) 제23조와 제24조에는 중국 최초로 경쟁업체 취업 제한과 관련하여 회사(고용주)와 직원간의 비밀유지 범위, 경제적 보상, 기한 등 계약조항을 명시하여 영업비밀보호 강도가 높아짐

- 입사자(재직자 포함), 퇴사자 및 외국인에 대한 보안 서약서의 내용은 <별책 p.84>, <별책 p.92>, <별책 p.100> 참조

□ 해외 진출시 협력사와의 관계정립

○ 기존업체 인수합병시 기술투자 관계 명확화

- 기존업체를 인수 또는 합작하고 예정된 기술을 이전하는 경우에는 그 기술을 철저히 보호할 수 있도록 계약에 구체적으로 명시해야 함

- 만일 해당업체가 보유한 기술을 기반으로 인수합병하는 경우에는 대상기업이 특허권을 소유하고 있는지를 확인하고 만약 사용자인 경우에는 계약내용, 영업비밀의 보유현황 등을 엄밀하게 조사하여 인수 후 특허권 등으로 인한 지적재산권 분쟁을 예방해야 함

○ 이전할 기술의 명확한 범위설정

- 기술투자 시에 이전할 기술의 대상과 범위를 명확히 하여 원하지 않는 기술과 보호해야 할 핵심기술까지 이전해야 하는 사태를 방지해야 함

○ 협력업체 직원에 대한 접근 제한

- 회사의 업무를 아웃소싱하는 등의 이유로 외부업체 직원이 회사에 출입하는 경우 출입자의 지정, 출입가능 지역을 엄격하게 제한하여, 이들이 주요 비밀정보에 접근하는 것을 통제해야 함

제 4 장 기술유출 사후 대응방안

제1절 퇴직자의 창업 또는 경쟁업체 취업

□ 퇴직자에 대한 협조공문

○ 비밀유지 서약을 한 퇴직자가 창업을 한 경우에는 의무를 지킬 것을 요구하고, 경쟁업체에 취업한 경우에는 퇴직자와 취업한 회사에 비밀을 침해할 수 있으므로 비밀유지 서약을 이행할 것을 촉구

<표4-1> 퇴직자에 대한 협조공문 요지

○○○님 귀하

귀하는 우리 회사 재직 시는 물론 퇴직 후에도 비밀을 유지 및 보호하기 위해 1년간 경쟁업체에 취업하거나 창업하지 않겠다는 서약을 하였습니다.

그럼에도 귀하가 경쟁업체인 ○○○사에 취업을 함으로써 우리 회사의 영업비밀이 침해될 우려가 있으므로 비밀유지서약을 이행하여 주시기 바랍니다. 만약 이를 이행하지 않으면 법적인 조치를 취하게 되므로 불미스러운 일이 없도록 협조하여 주시기 바랍니다.

이에 대한 회신을 20○○년 ○○월 ○○일 까지 부탁드립니다.

□ 영업비밀보호 관련 협조공문

○ 퇴직자와 함께 퇴직자를 채용한 경쟁업체에도 경고 또는 협조 공문을 발송하는 것이 필요함

○ 퇴직자와 채용업체에 공문을 발송할 때에는 내용증명과 배달증명 우편으로 발송하는 것이 분쟁 발생시에 유리한 증거가 됨

<표4-2> 영업비밀보호 관련 협조공문 요지

○○○○주식회사(퇴직자를 채용한 업체)
대표이사 귀하

귀사에 취업한 ○○○는 우리 회사에 근무하면서 중요한 영업비밀을 알고 있으므로 영업비밀유지를 위하여 1년간 경쟁업체에 취업하지 않기로 서약한 자입니다.

그러나 귀사가 ○○○를 채용함으로써 우리 회사의 영업비밀이 유출될 심각한 우려가 있습니다. 따라서 우리 회사 퇴직자 ○○○를 취업제한기간인 20○○년 ○○월 ○○일까지는 귀사에 취업시키지 않는 것이 영업비밀 침해를 예방하는 최선의 방법이므로 적극 협조하여 주시기 바랍니다.

만약 이에 협조하지 않을 때에는 불가피하게 부정경쟁방지 및 영업비밀보호에 관한 법률 제10조 등에 의하여 법적인 조치를 취할 수밖에 없음을 양지하시고 귀사의 의사를 20○○년 ○○월 ○○일 까지 회신하여 주시기 바랍니다.

제2절 영업비밀 침해

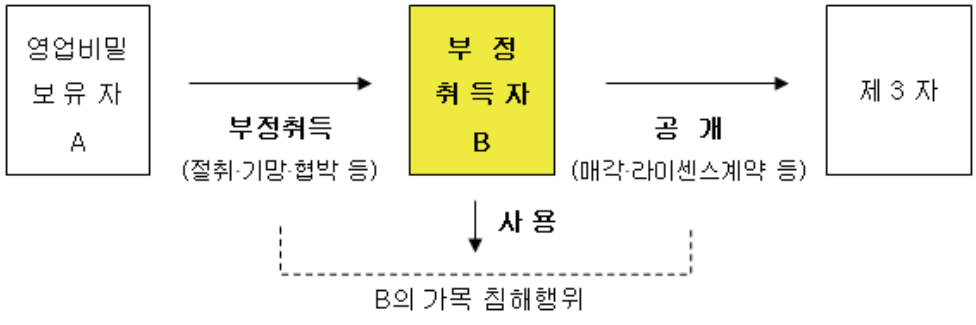
□ 영업비밀 침해행위 유형

○ '부정경쟁방지 및 영업비밀 보호에 관한 법률(제2조 제3호)'에서는 영업비밀 침해행위를 다음의 6가지 유형으로 나누어 한정적으로 열거하고 있으며, 이 6가지 유형을 '부정취득과 관련된 영업비밀 침해행위'와 '비밀유지 의무자의 부정공개 관련 영업비밀 침해행위'의 두 가지 유형으로 구분할 수 있음

(1) 부정취득행위와 관련된 침해행위

1) 영업비밀을 부정취득·사용·공개하는 행위

> 절취, 기망, 협박 기타 부정한 수단으로 영업비밀을 취득하는 행위(이하 "부정취득행위"라 함) 또는 그 취득한 영업비밀을 사용하거나 공개(비밀을 유지하면서 특정인에게 알리는 것을 포함)하는 행위(법 제2조 제3호 가목)



① 부정취득행위

- 제3자에 의한 산업스파이 행위의 전형으로서, 여기에서 규정한 '절취, 기망, 협박'은 부정취득행위의 전형적인 수단을 예시로 한 것이고 반드시 이에 한하지는 않음

- '기타 부정한 수단'이란 형벌법규 위반의 행위 및 그와 동등한 위법성을 가졌다고 판단되는 일체의 반사회적 수단을 포함하는 개념

  · 여기에는 금전에 의한 피용자 매수, 지위제공에 의한 고용계약 파기유인, 고객을 가장한 방법에 의한 생산시설 침입, 영업비밀 보유매체(문서, 디스켓, USB 등)의 취득, 영업비밀 보유매체의 복사·전송, 영업비밀의 내용을 기억하여 취득하는 행위, 도청이나 전파탐지 등 신의성실에 반하는 방법에 의한 영업비밀 침해행위가 모두 포함됨

② 부정취득한 영업비밀의 사용행위

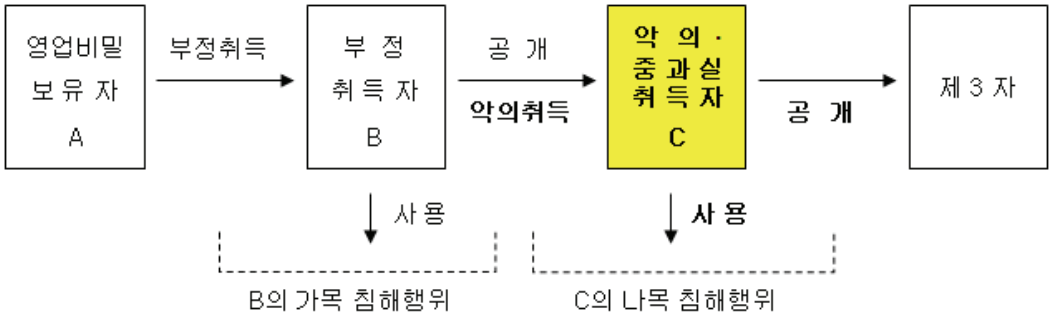
- 사용행위란 영업비밀을 그 고유의 용도 내지 사용목적에 따라 활용하는 행위를 의미함
- 여기에는 부정취득한 영업비밀을 제품의 제조 또는 영업활동 등에 직접 사용하는 행위는 물론 연구개발이나 영업활동 등을 함에 있어서 취득한 영업비밀을 참고로 하는 행위를 포함함

③ 부정취득한 영업비밀의 공개행위

- 부정한 수단으로 취득한 자의 행위로 영업비밀을 불특정인에게 공개하는 행위 및 비밀로 유지하면서 특정인에게 알리는 행위를 포함하며, 구체적으로 부정취득한 영업비밀을 제3자에게 매각 또는 라이선스 계약 등의 방법으로 공개하는 경우 등이 해당됨
- 부정공개행위는 구두·서면뿐만 아니라 도면·모형의 전시에 의해서도 가능하며, 제3자가 영업비밀을 알려고 하는 것을 방해하지 않는 부작위(不作爲) 형식에 의한 공개행위도 인정되고, 공개행위의 유상성(有償性)을 요건으로 하지 않음

2) 부정취득된 영업비밀을 악의[11]·중과실[12]로 취득·사용·공개하는 행위

> 영업비밀에 대하여 부정취득행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고, 그 영업비밀을 취득하는 행위 또는 그 취득한 영업비밀을 사용하거나 공개하는 행위(법 제2조 제3호 나목)



- 나목의 규정은 가목에서 규정된 부정취득행위를 전제로 당해 영업비밀의 유통과정에서부터 부정취득이 개입된 사실에 관하여 악의 또는 중과실인 채 이를 전득(轉得)하는 경우를 금지하려는 규정임
- 부정취득자로부터 직접 취득한 자 뿐만 아니라 전득자로부터 취득한 자도 본 규정의 적용을 받으며, 단순히 영업비밀 부정취득 행위가 개입된 사실을 인정하면서 또는 인식하지 못한 채 중대한 과실이 있으면서 영업비밀을 취득하거나 그것을 사용·공개하는 행위가 이에 해당됨
- 주관적 요건으로서 영업비밀의 취득당시에 악의 이외에 중과실에 의하여 취득한 것을 요건으로 한 것은 소송 중에 있어서 주관적 요건인 악의의 증명이 곤란하므로 행위자로서 조금만 주의를 기울였더라면 당연히 알 수 있었을 객관적 상황을 증명하면 중과실로 보아 악의와 동일시하려는 것임

---

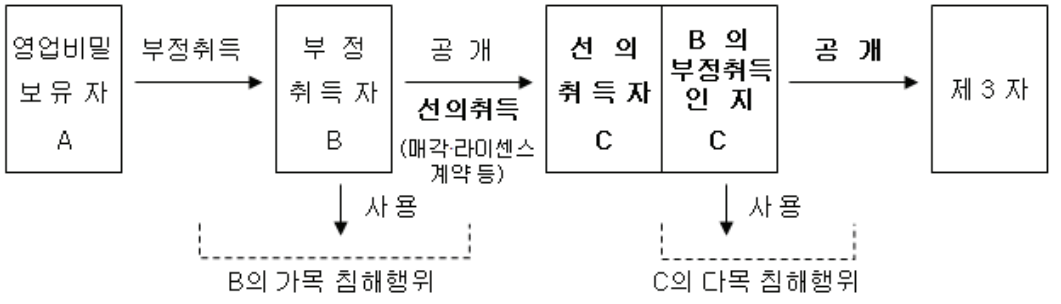
11) '악의'라 함은 매수자 C가 부정취득자 B로부터 영업비밀을 매수함에 있어서 당해 영업비밀은 B가 절취한 것이라는 사실, 즉 부정취득행위가 개입된 사실을 알고 있는 경우를 의미함

12) '중과실'에 의한 취득이란 매수자 C가 부정취득자 B로부터 영업비밀을 취득함에 있어서 사회적 지위, 종사하는 직업 등에 따라 평균적으로 요구되는 주의를 현저하게 게을리 하였기 때문에 부정취득행위가 개입된 사실을 알지 못한 것을 의미함

- 나목의 주관적 요건 판단의 기준이 되는 시점은 영업비밀 취득 당시임. 이 점에서 다목의 사후적 악의자에 대한 영업비밀 침해 행위가 침해 당시에는 선의·無중과실이었다가 취득한 이후 사용·공개할 당시에는 악의 또는 중과실로 전환되는 것을 의미하는 것과 구별됨

3) 선의취득 후 악의·중과실에 의한 사용·공개 행위[13)]

> 영업비밀을 취득한 후에 그 영업비밀에 대해 부정취득행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 사용하거나 공개하는 행위(법 제2조 제3호 다목)



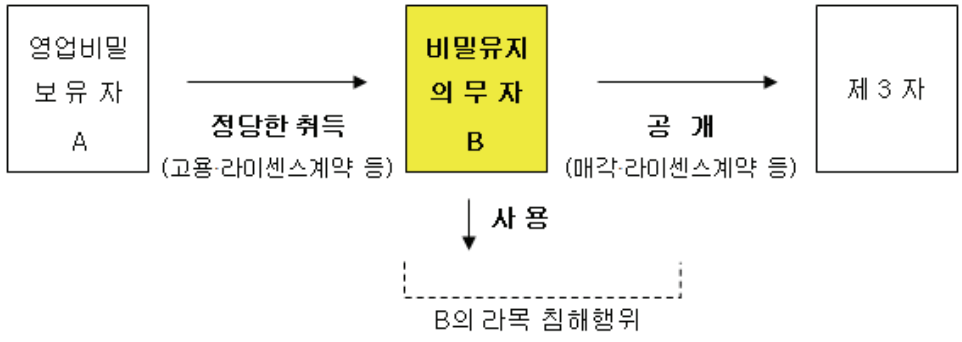
- 다목은 영업비밀의 취득시에는 선의·無중과실이었으나 취득 후 악의 또는 중과실이 인정되는 사후적 악의자에 대하여 당해 영업비밀의 사용 등을 침해행위로 보아 제한하려는 규정임
- 선의[14)]이며 중대한 과실 없이 영업비밀을 취득한 자가 그 후 영업비밀 보유자로부터 경고를 받거나 부정한 취득사실을 언론을 통해 알게 되는 등으로 자기가 취득한 영업비밀에 부정취득행위가 개입된 것을 알거나 중대한 과실로 알지 못하고 이를 사용하거나 공개하는 등의 행위도 규제하기 위한 것임. 영업비밀은 비록 유출되더라도 그것이 비밀로 유지되고 있는 한 보호할 가치가 있기 때문임

13) 본 규정에 대해서는 일정한 요건 하에 '선의자에 대한 특례'가 적용됨
14) '선의'라 함은 영업비밀 취득자가 부정취득자 또는 전득자로부터 영업비밀을 취득함에 있어서 당해 영업비밀에 부정취득행위가 개입된 사실을 알지 못한 것을 의미함

(2) 부정공개행위와 관련된 침해행위

1) 영업비밀을 부정 공개·사용하는 행위

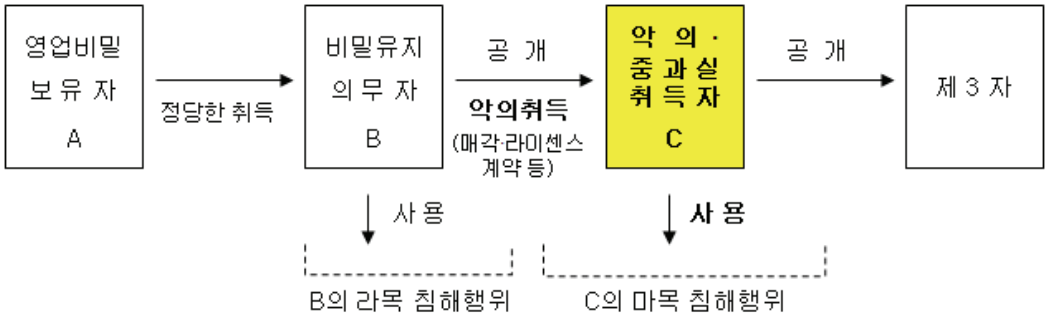
> 계약관계 등에 의하여 영업비밀을 비밀로서 유지하여야 할 의무가 있는 자가 부정한 이익을 얻거나, 그 영업비밀을 보유자에게 손해를 가할 목적으로 그 영업비밀을 사용하거나 공개하는 행위(법 제2조 제3호 라목)



- 본 규정은 정당하게 영업비밀을 취득한 자가 비밀유지의무를 부담하고 있음에도 불구하고 부정한 목적을 가지고 위 의무에 위반하여 당해 정보를 사용 또는 공개하는 행위를 규제하기 위한 것임
- 행위의 주체는 비밀유지의무가 있는 자로서, 예컨대 기업체의 임·직원 또는 영업비밀의 실시계약(License)에 의한 실시권자 등이 해당됨
- 비밀유지의무는 법률에서 그 의무를 명시한 경우는 물론, 개별적인 계약관계가 있는 경우 또는 이러한 계약관계가 없더라도 이에 준하는 신뢰관계가 있는 경우에는 신의칙상 비밀유지의무가 발생하며, 재직중이거나 퇴직 후 또는 계약중이거나 계약만료 후를 묻지 않음
- 침해행위에 있어서 침해자가 부정한 이익을 얻거나 본래의 영업비밀 보유자에게 손해를 가할 목적으로 영업비밀을 사용하거나 공개하는 행위이어야 함

2) 부정공개된 영업비밀을 악의·중과실로 취득·사용·공개하는 행위

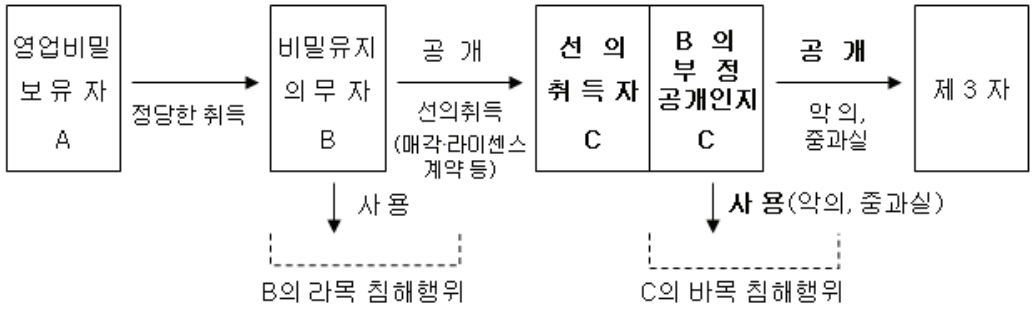
> 영업비밀이 라목의 규정에 의하여 공개된 사실 또는 그러한 공개행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 취득하는 행위 또는 그 취득한 영업비밀을 사용하거나 공개하는 행위(법 제2조 제3호 마목)



- '제2조 제3호 라목'의 부정한 행위에 의해 공개된 영업비밀에 대해 사후적으로 관여하는 것을 금지하려는 규정이며, 구체적 내용은 '제2조 제3호 나목'과 동일함

3) 선의취득 후 악의·중과실에 의한 사용·공개 행위[15]

> 영업비밀을 취득한 후에 그 영업비밀이 라목의 규정에 의하여 공개된 사실 또는 그러한 공개행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 사용하거나 공개하는 행위(법 제2조 제3호 바목)



15) 구체적 내용은 제2조 제3호 다목과 동일하며, 본 규정에 대해서는 일정한 요건하에 '선의자에 대한 특례'가 적용됨

□ 영업비밀 침해행위에 대한 구제수단

(1) 부정경쟁방지 및 영업비밀 보호에 관한 법률

1) 민사적 구제수단

「부정경쟁방지 및 영업비밀 보호에 관한 법률」에서는 영업비밀 침해행위를 민법상의 불법행위의 특수한 형태인 부정경쟁행위의 한 유형으로 분류하여 명문으로 규정하고, 이에 대해 침해행위의 금지 또는 예방청구권, 침해행위로 만들어진 물건 등의 폐기·제거청구권, 침해행위에 대한 손해배상청구권, 영업비밀 보유자의 신용회복청구권 등을 인정하고 있음

가. 금지 및 예방청구권

> 영업비밀의 보유자는 영업비밀 침해행위를 하거나, 하고자 하는 자에 대하여 그 행위에 의하여 영업상의 이익이 침해되거나 침해될 우려가 있는 때에는 법원에 그 행위의 금지 및 예방을 청구할 수 있음(법 제10조 제1항)

① 청구권자

- 금지청구권자는 영업비밀 보유자이며, 당해 영업비밀을 개발하여 보유하고 있는 자 외에 그 양수인, 라이센시(Licensee) 등과 같이 정당한 권원(權原)에 기해서 일정한 지배를 하고 있는 자를 포함함

② 금지·예방청구의 내용

- 영업비밀 침해행위에 해당하는 당해 영업비밀의 부정취득, 사용, 공개행위 등을 금지하는 것이 그 내용임. 구체적으로는 일정한 제품의 생산을 일정 기간 중지시키거나 완성제품의 배포·판매를 못하게 하는 것 등임

③ 금지·예방의 기간

- 영업비밀 침해가 없었더라면 보유자가 침해자에 대하여 경쟁상의 우위를 지킬 수 있는 기간(Leading Period) 또는 침해자의 독자적인 기술개발에 소요되는 기간 등이 될 수 있음

④ 청구권의 행사기간(소멸시효)

- 영업비밀 침해행위가 계속되는 경우에 영업비밀 보유자가 그 침해행위에 의하여 영업상의 이익이 침해되거나 침해될 우려가 있는 사실 및 침해행위자를 안 날로부터 3년간 이를 행사하지 않거나, 그 침해행위가 시작된 날로부터 10년이 경과한 때에는 시효로 인하여 소멸됨(동법 제14조)

나. 폐기·제거 등 청구권

> 영업비밀의 보유자가 제10조 제1항의 규정에 의한 청구를 할 때에는 침해행위를 조성한 물건의 폐기, 침해행위에 제공된 설비의 제거 기타 침해행위의 금지 또는 예방을 위하여 필요한 조치를 함께 청구할 수 있음(법 제10조 제2항)

① 의의

- 본 청구권은 영업비밀의 침해행위로부터 야기된 물적 상태의 제거를 통해 장래의 침해 재발을 막아 금지청구의 실효를 거두기 위해 인정되는 것임
- 단독으로 독립하여 행사할 수 없고, 반드시 금지 또는 예방청구에 수반되어야 하는 부대청구권임

② 청구대상

- 도면, 설계도, 고객리스트 등 침해행위를 조성한 물건의 폐기와 영업비밀을 사용하기 위한 기계 및 생산설비의 제거 등이 청구의 대상
- 예를 들어 A기업이 생명공학에 막대한 투자를 하여 특수한 효과를 가지는 미생물을 배양해 냈는데, 경쟁사인 B기업이 산업스파이를 동원하여 그 미생물의 시험종자를 절취했을 경우 위 미생물은 쉽게 배양·증식되는 것이므로, A기업은 법원에 B기업을 상대로 시험종자의 반환청구 및 그 배양설비 등의 폐기를 청구할 수 있음

다. 손해배상청구권

> 고의 또는 과실에 의한 영업비밀 침해행위로 영업비밀 보유자의 영업상 이익을 침해하여 손해를 가한 자는 그 손해를 배상할 책임이 있음 (법 제11조)

① 청구요건

- 침해자의 고의 또는 과실
- 영업비밀 침해행위의 존재
- 영업비밀 보유자의 영업상 이익 침해에 따른 손해의 발생
- 영업비밀 침해행위와 손해발생과의 인과관계

② 청구내용

- 영업비밀 침해행위에 의해 생긴 손해의 보전으로, 배상의 범위에 대해서는 영업비밀 침해행위와 상당한 인과관계가 있는 일체의 손해로서 적극적 손해와 소극적 손해를 모두 포함함

③ 청구권의 행사기간(소멸시효)

- 본 법에는 규정되어 있지 않으나 민법상의 규정이 그대로 준용되는데, 영업비밀 침해행위가 있은 사실 및 행위자를 안 날로부터 3년간 또는 그 행위가 시작된 날로부터 10년간 이를 행사하지 않으면 시효로 인하여 소멸됨(민법 제766조)

④ 손해액의 추정

- 영업비밀 침해행위에 기초한 물품을 침해자가 판매한 경우 그 판매수량에 해당 물품의 단위수량당 이익액을 곱한 금액을 영업비밀 보유자가 받은 손해액으로 추정함

라. 신용회복청구권

> 법원은 고의 또는 과실에 의한 영업비밀 침해행위로 영업비밀 보유자의 영업상의 신용을 실추하게 한 자에 대하여는 영업비밀 보유자의 청구에 의하여 제11조의 규정에 의한 손해배상에 갈음하거나 손해배상과 함께 영업상의 신용회복을 위하여 필요한 조치를 명할 수 있음(법 제12조)

- 영업비밀을 보유한 자는 고의 또는 과실에 의한 침해행위로 영업상의 이익을 실추하게 한 자에 대하여 법원에 금전배상을 갈음하거나 금전배상과 함께 영업상의 신용회복을 위하여 필요한 조치를 청구할 수 있으며, 구체적 조치의 예로는 침해사실의 공개, 합의각서 공개, 해명서신의 발송 등이 있음

2) 형사적 구제수단

가. 처벌규정

○ 영업비밀 침해행위에 대한 형사적 제재수단으로 징역과 벌금(제18조 제1항, 제2항, 제4항, 제18조의 2, 제18조의 3, 제19조)이 규정되어 있음

① 영업비밀을 침해한 자는 '누구든지' 형사처벌 가능

② 국내유출의 경우 '5년 이하의 징역' 또는 '재산상 이득액의 2배 이상 10배 이하에 상당하는 벌금'

- 예비·음모의 경우 '2년 이하의 징역' 또는 '1천만원 이하의 벌금'

③ 국외유출의 경우 '7년 이하의 징역' 또는 '재산상 이득액의 2배 이상 10배 이하에 상당하는 벌금'

- 예비·음모의 경우 '3년 이하의 징역' 또는 '2천만원 이하의 벌금'

④ '기술상의 영업비밀'에 '경영상의 영업비밀' 침해도 형사처벌범위에 포함

⑤ '양벌규정'을 통해 침해사범 개인뿐만 아니라 침해에 관여한 조직, 기업 등도 처벌할 수 있도록 함

나. 처벌요건

① 행위주체

- 과거에는 전·현직 임직원을 처벌대상으로 하였으나, 현행법에서는 '모든 위반자(관련자 전원)로 대상을 확대함
- '양벌규정'을 통해 침해사범 개인 뿐만 아니라 침해에 관여한 조직, 기업 등도 처벌할 수 있도록 함

② 보호객체

- '기술상의 영업비밀'에 '경영상의 영업비밀' 침해도 형사처벌 범위에 포함

③ 소추요건

- 피해기업의 고소·고발이 없어도 처벌이 가능하도록 하고 있으며, 미수범과 예비·음모자도 처벌

3) 선의자에 대한 특례

> 거래에 의하여 영업비밀을 정당하게 취득한 자가 그 거래에 의하여 허용된 범위 안에서 그 영업비밀을 사용하거나 공개하는 행위에 대해서는 금지 또는 예방청구권, 손해배상청구권 및 신용회복청구권 등의 규정 적용 배제(법 제13조)

가. 규정취지

○ 취득시점에는 고의 또는 중과실이 없었지만 나중에 피해자인 영업비밀 보유자로부터 경고장 등을 받음으로써 그 후부터 영업비밀 침해행위의 존재에 대하여 알게 된 자를 구제하기 위하여 마련된 특칙임

나. 특례적용 요건

① 거래에 의하여

- '거래'라 함은 매매 기타의 양도계약, 라이선스계약, 증여계약 등을 모두 포함하며 법률상의 전형적인 거래 뿐만 아니라 비전형적인 사실상의 거래 행위를 포함

② 영업비밀을 정당하게 취득한 자

- '영업비밀을 정당하게 취득한 자'라 함은 법 제2조 제3조 다목 및 바목의 규정에서 영업비밀을 취득할 당시에 그 영업비밀이 부정하게 공개된 사실 또는 영업비밀의 부정취득행위나 부정공개행위가 개입된 사실을 중대한 과실 없이 알지 못하고 그 영업비밀을 취득한 자를 말함(법 제13조 제2항)
- 즉, 영업비밀의 취득자가 영업비밀을 취득할 당시에 선의이며, 중대한 과실이 없어야 함을 의미

③ 거래에 의하여 허용된 범위 내

- '허용된 범위 내에서'란 거래의 내용에 따라 정당하게 취득한 권리의 범위 내를 뜻함
- 허용된 범위를 넘어서 부당하게 이익을 꾀하거나 영업비밀 보유자에게 손해를 끼칠 의도를 가지고 사용 또는 공개하는 행위는 침해행위로 되어 침해금지청구 등의 대상이 됨

(2) 형법

1) 영업비밀에 접근할 권한이 있는 내부자에 의한 누설

① 업무상 비밀*누설죄(제317조)

- 특정한 직업을 가진 사람이 그 업무처리 중 알게 된 타인의 비밀을 누설시 '3년 이하의 징역이나 금고', '10년 이하의 자격정지' 또는 '700만원 이하의 벌금'

  * '비밀'이라 함은 특정인 또는 일정한 범위의 사람에게만 알려져 있는 사실로서 타인에게 알려지지 아니하는데 본인에게 이익이 있는 사실이므로 영업비밀은 본조의 비밀에 포함된다고 할 수 있음

- 친고죄로서 고소가 있어야 공소를 제기할 수 있으며(형법 제318조), 범인을 알게 된 날로부터 6월을 경과하면 고소하지 못함(형사소송법 제230조 제1항)

② 횡령죄(제355조 제1항), 업무상 횡령죄(제356조), 특정경제범죄가중처벌법상 가중처벌(특경법 제3조)

- 타인의 재물을 보관하는 자가 그 재물을 횡령하거나 반환을 거부하는 경우 '5년 이하의 징역' 또는 '1,500만원 이하의 벌금'에 처하며, 업무상 임무에 위배하여 횡령죄를 범하는 경우 '10년 이하의 징역' 또는 '3천만원 이하의 벌금'에 처함. 미수범도 처벌함

- 특정경제범죄가중처벌법 제3조 제1항에 의하여 횡령 혹은 업무상 횡령을 통하여 얻은 재산상 이득액이 50억원 이상일 때는 무기 또는 5년 이상의 징역에 처하고, 5억원 이상 50억원 이하일 경우에는 3년 이상의 유기징역에 처하며, 이 경우 이득액에 상당한 벌금을 병과할 수 있음(동법 제3조 제2항)

- 회사가 비밀서류를 직원에게 회사 외부의 별도의 장소나 분소 같은 곳에 위탁하여 놓은 경우 또는 회사의 비밀서류를 다른 보안회사 등에 위탁하여 놓은 경우 이러한 비밀서류를 위탁받아 보관하고 있는 회사의 임직원은 비밀서류에 대하여 횡령죄를 범할 수 있음

- 하지만 통상 회사 내에 보관하던 자신의 업무관련 비밀서류를 무단으로 반출한 경우에는 횡령죄가 아니라 일반적으로 절도죄가 성립하게 됨. 왜냐하면 횡령죄의 객체는 자기가 점유하는 재물인데, 회사에 보관하고 있는 비밀서류의 경우 당해 비밀서류에 대한 소유권이 회사에 있고 또한 점유도 유출자의 단독점유가 아니라 회사와의 공동점유상태에 있기 때문임

③ 배임죄(제355조 제2항), 업무상 배임죄(제356조), 상법상 특별배임죄(상법 제622조 제1항), 특정경제범죄가중처벌법상 가중처벌(특경법 제3조 제1항)

- 타인의 사무*를 처리하는 자가 그 임무에 위배하는 행위**로써 재산상의 이익을 취득하거나 제3자로 하여금 이를 취득하게 하여 본인에게 손해를 가하는 경우 '5년 이하의 징역' 또는 '1,500만원 이하의 벌금'에 처하며, 업무상 배임죄의 경우 횡령죄와 마찬가지로 '10년 이하의 징역' 또는 '3천만원 이하의 벌금'으로 가중 처벌함. 미수범도 처벌함

  * 타인의 사무는 타인의 재산을 보호 내지 관리할 의무를 의미

  ** 임무에 위배하는 행위는 처리하는 사무의 내용, 성질 등 구체적 상황에 비추어 법률의 규정, 계약의 내용 혹은 신의칙상 당연히 할 것으로 기대되는 행위를 하지 않거나 당연히 하지 않아야 할 것으로 기대하는 행위를 함으로써 상호간의 신임관계를 저버리는 일체의 행위를 포함

(예를 들어 기업의 영업비밀을 사외로 유출하지 않을 것을 서약한 회사의 직원이 경제적인 대가를 얻기 위해 경쟁업체에 영업비밀을 유출하는 행위는 영업비밀을 사외로 유출하지 않는다는 점에 대한 회사와 직원간의 신임관계를 저버리는 배신행위로서 업무상 배임죄를 구성하는 임무에 위반하는 행위에 해당한다고 할 수 있음)

- 상법 제622조는 특별배임죄로서 회사의 발기인, 업무집행사원, 이사, 감사, 지배인 기타 회사영업에 관한 어느 종류 또는 특정한 사항의 위임을 받은 사용인이 그 임무에 위배한 행위로서 재산상의 이익을 취득하거나 제3자로 하여금 이를 취득하게 하여 회사에 손해를 가한 때에는 10년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 규정
- 특정경제범죄가중처벌법 제3조 제1항에 의하여 배임 혹은 업무상 배임을 통하여 얻은 재산상 이득액이 50억원 이상일 때는 무기 또는 5년 이상의 징역에 처하고, 5억원 이상 50억원 이하일 경우에는 3년 이상의 유기징역에 처하며, 이 경우 이득액에 상당한 벌금을 병과할 수 있음(동법 제3조 제2항)

2) 영업비밀에 접근할 수 없는 제3자에 의한 비밀침해

① 비밀침해죄(제316조)

- 봉함 기타 비밀장치한 사람의 편지, 문서 또는 도화를 개봉한 자나 전자기록 등 특수매체 기록을 기술적 수단을 이용하여 그 내용을 알아낸 자는 '3년 이하의 징역이나 금고' 또는 '500만원 이하의 벌금'

② 절도죄(제329조)

- 타인의 재물을 절취하는 경우 '6년 이하의 징역' 또는 '1,000만원 이하의 벌금'에 처하며, 미수범도 처벌함
- 산업스파이가 기업체의 영업비밀을 절취하였다고 볼 수 있을 만한 사례는 다음과 같음
  - · 영업비밀이 화체된 문서, 디스켓 등을 절취한 경우
  - · 영업비밀이 화체된 문서를 현장에서 복사, 촬영하여 그 내용을 파악해 간 경우
  - · 영업비밀이 화체된 문서 등을 가지고 나가 복사, 촬영 등을 하고 제자리에 갖다 놓은 경우

(3) 정보통신망 이용촉진 및 정보보호 등에 관한 법률

○ 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자는 '5년 이하의 징역' 또는 '5천만원 이하의 벌금'(제49조, 제62조)

- 해킹을 통한 영업비밀 침해시 형법상의 비밀침해죄가 적용될 수 있으나 특별법인 본 법을 적용하는 것이 바람직함

(4) 통신비밀보호법

○ 전기통신·우편·대화 등을 통하여 송·수신되는 영업비밀을 감청·녹음하거나 또는 그 취득한 내용을 공개·누설하는 경우 '10년 이하의 징역'과 '5년 이하의 자격정지'(제3조, 제16조)

(5) 컴퓨터 프로그램 보호법

○ 타인의 프로그램을 무단으로 복제, 개작, 번역, 배포, 발행 또는 전송한 자는 '3년 이하의 징역' 또는 '5천만원 이하의 벌금'(제29조, 제46조)

제3절 지적재산권 침해

□ 권리침해가 의심되는 경우 - 경고장 송부

○ 경쟁업체나 제3자가 자사의 지식재산권을 침해한다고 의심되는 경우 가장 먼저 침해행위를 뒷받침할 수 있는 증거자료(예: 물품, 카탈로그, 팜플렛 등)를 수집하고, 그 다음으로 침해품의 생산·판매 현황 및 침해자에 대한 기본정보를 조사해야 함

○ 증거조사 결과 수집한 대상물이 자사의 특허발명을 침해하고 있는지 여부를 검토하여, 자사의 특허를 침해하였다고 판단될 경우에는 신중하게 침해의 입증 방법을 모색해야 함

- 침해의 입증에 성공하지 못할 경우, 상대방으로부터 무고죄로 공격받을 수 있음

○ 자사 권리침해에 대해 입증이 가능하다고 판단되면 즉시 상대방에게 침해사실을 경고해야 함

- 경고는 통상 서면으로 행하고, 경고장에 특허번호, 공고번호, 발명의 명칭, 침해품 및 회답기한 등을 명시하여 통상 내용증명 우편으로 상대방에게 발송함

○ 경고장 송부는 특허권 등의 권리를 이용해서 경쟁업체가 제품을 판매하는 것을 막거나 적어도 일정기간 동안 방지하여 자사 제품의 시장점유율 관리 혹은 시장 선점에 유리하다는 이점이 존재함

- 하지만 침해피의자가 제조업자인 경우, 그 거래처인 유통·판매업자에게 경고하는 경우나 신문·업계소식지 등에 광고하여 경고하는 경우, 나중에 특허침해가 아닌 것으로 밝혀지면, 허위 사실의 고지 및 유포에 해당되어 손해배상청구를 받을 수 있으므로 주의가 필요

○ 경고장의 내용은 <별책 p.198> 참조

□ 분쟁발생시 구제수단

○ 특허관련사건(발생, 변경, 소멸 및 권리범위 등)의 분쟁은 전문적인 고도의 기술적 판단이 요구되므로 심판의 전문성과 공정성을 확보하기 위하여 1심은 특허청의 특허심판원에서 담당하고, 불복시 고등법원급인 특허법원을 거쳐, 대법원으로 상고하게 되는 심급구조를 취함

(1) 소송 및 심판

1) 행정적 구제수단 - 권리범위확인심판

- 권리범위확인심판이란 등록된 특허권을 중심으로 어느 특정기술이 당해 특허권의 권리범위에 속하는지 여부를 공적으로 확인하는 특허심판원의 심판제도를 의미함
- 권리범위확인심판은 특정권리의 내용범위의 확인이라는 권리의 내재적, 포괄적 확정이 아니라 특정권리와 분쟁관계에 있는 상대방의 사용 특허권과의 사이에서 구체적으로 권리의 충돌 또는 마찰이 존재하는지의 여부를 사안별로 가리는 제도로써, 심결을 빠른 시기에 얻을 수 있다면 실질적으로 이용가치가 매우 큼
- 변리사의 감정서, 권리범위확인심판이나 무효심판의 결과는 침해소송의 판단에 있어서 법원의 판단에 중요한 참고자료가 되고 있으므로, 침해소송의 제기에 앞서 변리사의 감정서, 권리범위확인심판이나 무효심판을 청구하여 결과를 확인한 후 침해소송 제기 여부를 결정하는 것도 중요한 소송전략 중 하나라고 할 수 있음

2) 민사적 구제수단

- 특허침해 등의 분쟁해결을 위해 침해금지 및 예방청구, 손해배상청구, 신용회복청구, 부당이득반환청구, 가처분 등의 민사적 구제수단이 존재함

① 금지 및 예방청구권(특허법 제126조)

- 특허권자 또는 전용실시권자는 자기의 권리를 침해한 자 또는 침해할 우려가 있는 자에 대하여 고의·과실을 불문하고 침해의 금지 또는 예방을 청구할 수 있음

- 침해금지 및 예방청구권의 내용 : 침해행위를 조성한 물건(물건을 생산하는 방법 발명인 경우에는 침해행위로 생긴 물건을 포함)의 폐기, 침해행위에 제공된 설비의 제거, 기타 침해예방에 필요한 행위를 청구할 수 있음

② 손해배상 청구권(특허법 제128조)

- 특허권자 또는 전용실시권자는 고의 또는 과실로 권리를 침해한 자에 대하여 손해배상을 청구할 수 있음

③ 신용회복 청구권(특허법 제131조)

- 특허권자 또는 전용실시권자는 타인이 고의 또는 과실로 특허발명을 침해하여 업무상의 신용을 실추하게 한 때에는 법원에 신용회복조치를 청구할 수 있으며, 법원은 손해배상에 갈음하거나 손해배상과 함께 업무상의 신용회복을 위해 필요한 조치를 명할 수 있음
- 신용회복조치 방법 : 신문, 잡지 등에의 권리자의 승소사실 게재 등

④ 부당이득반환 청구권(민법 제741조)

- 법률상 원인 없이 타인의 특허권 또는 전용실시권으로 인하여 이익을 얻고, 이로 인하여 권리자에게 손해를 가한 자에게 그 이익을 반환하도록 청구할 수 있음

⑤ 가처분(민사집행법 제300조)

- 법원은 특허권자의 신청에 의해 제소 전후를 불문하고 본안에 관한 최종심리 이전의 단계에서 침해피의자에게 잠정적으로 침해금지명령을 내릴 수 있음
- 가처분 신청이 법원에 의해 받아들여질지 여부가 결정되는데 걸리는 기간은 보통 3개월에서 6개월 정도이며, 특허권의 침해여부가 판단되어 가처분이 인정되면 침해피의자의 생산 및 판매가 중단되므로, 특허권자에게는 매우 실효적이고, 강력한 공격수단이 될 수 있음

3) 형사적 구제수단

- 특허침해 등에 대한 분쟁해결을 위해 징역, 벌금, 몰수 등의 형사적 구제수단이 존재함

① 특허권 침해죄(특허법 제225조)

- 특허권 또는 전용실시권을 고의로 침해한 자는 7년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 규정
- 친고죄로서 특허권자 또는 전용실시권자의 고소가 있어야 하며, 고의범인 경우에만 형사처벌이 가능함

② 몰수(특허법 제231조)

- 법원은 특허권 또는 전용실시권을 고의로 침해한 경우 침해행위를 조성한 물건 또는 그 행위로부터 생긴 물건은 이를 몰수하거나, 피해자의 청구에 의해 그 물건을 피해자에게 교부할 것을 선고해야 함
- 피해자는 물건의 교부를 받은 경우 그 물건의 가액을 초과하는 손해의 액에 한하여 손해배상을 청구할 수 있음

③ 양벌죄(특허법 제230조)

- 법인의 대표자, 법인 또는 개인의 대리인, 사용자, 기타 종업원이 임무와 관련하여 침해죄, 허위표시의 죄, 사위행위(詐僞行爲)의 죄를 범하였을 때에는 행위자를 벌하는 외에 그 법인과 개인에 대해 벌금형을 부과
- 법인의 경우 침해죄의 경우 3억원 이하의 벌금, 허위표시와 사위행위의 죄의 경우 6천만원 이하의 벌금

(2) 소송 이외의 해결제도(ADR)

○ 소송제기에 의한 해결 이외에, 재판 이외의 방법을 통한 분쟁해결수단(ADR, Alternative Dispute Resolution)을 시도해 볼 수 있으며, 다음과 같은 장점을 가짐

- 신속하고 비용측면에서 경제적임
- 소송보다 저렴한 비용을 들여 손해배상 청구가 가능
- 소송 절차에 의하여 공개될 수 있는 회사의 영업비밀 보호 가능
- 해당 분야 전문가들의 도움으로 분쟁의 조기해결 가능

○ 소송의 경우 국가의 권력을 배경으로 강제적인 분쟁해결 방법이나, ADR의 경우 당사자의 합의가 있어야 해결이 가능함

○ ADR에는 중재, 조정, 알선, 화해 등의 형태가 존재하며, 국내에서의 활용비율은 아직까지 그다지 높지 않음

1) 중재(Arbitration)

- 중재는 분쟁 당사자의 합의에 따라 분쟁에 관한 판단을 법원이 아닌 제3자(중재인 또는 중재기관)에게 맡겨 분쟁을 해결하는 방법으로, 대한상사중재원이 대표적임
- 중재판정은 당사자간에 있어서 법원의 확정판결과 동일한 효력이 있으며, 이 판정에 대한 불복절차가 존재하지 않음

2) 조정(Mediation)

- 조정은 중재와 마찬가지로 재판에 의하지 않고 당사자간의 분쟁을 해결하는 방법으로 성립한 화해의 효력은 민법상의 화해(민법 제731조)와 동일함
- 중재의 경우 제3자의 판단이 법적인 구속력을 가지고 당사자가 이에 반드시 따라야 하지만, 조정의 경우 법적인 구속력이 없어 당사자가 이에 반드시 따를 의무는 없음

3) 알선(Conciliation)

- 알선은 제3자가 당사자들의 분쟁해결에 협력하고 당사자 상호간의 자주적 해결을 통해 합의를 형성하도록 지원하고 조력하는 절차를 의미함
- 알선 결과 성립한 화해의 효력은 조정과 동일하며, 일반적으로 분쟁처리의 초기적 단계에서 주로 활용됨

4) 화해(Compromise)

- 당사자 쌍방의 상호 양보를 전제로 분쟁 해결과 관련한 합의가 이루어진 경우, 이러한 합의를 화해라고 함
- 화해는 민법상의 계약의 일종으로 정하고 있으며(민법 제731조), 당사자간에 화해를 하는 것만 아니라 법원에서 화해를 하고 그 조서에 기재를 하면 확정판결과 같은 효력을 가짐(민사소송법 제231조)
- 재판상의 화해는 소송절차 중에 하는 소송상의 화해와 소송을 제기하기 전에 하는 제소전의 화해를 포함함

<표4-3> 주요 중재·조정 기관

◈ 산업기술분쟁조정위원회

- 산업기술의 유출방지 및 보호에 관한 법률 제23조에 근거하여 산업기술의 유출과 관련된 분쟁의 신속한 조정을 위해 산업자원부장관 소속하에 본위원회가 설치될 예정임

◈ 대한상사중재원

- 민법 제32조 및 산업자원부 설립허가 제142호에 의해 설립되어 국내외 상거래상에서 발생하는 분쟁을 해결
- 경제자유구역 내에 지부를 설치하여 경제자유구역 내에 분쟁해결기반을 조성하고 외국인 투자유치와 경제자유구역의 운영을 지원
- 계약서 자동작성시스템을 개발하여 각종 상거래 계약서를 쉽게 작성할 수 있도록 하였고, 각 조문마다 해설을 달아 초보자들도 쉽게 이해할 수 있도록 함
- 주요업무 : 무료상담, 분쟁의 합리적 해결방안 모색, 상거래 실무 및 상관습 안내, 각종 교육·세미나 개최, 계약서 작성을 위한 가이드라인 제시, 관련 법류와 판례 및 클레임 자료 등 무료 제공

◈ 특허청 산업재산권분쟁조정위원회

- 첨단기술분야의 급속한 발전으로 분쟁내용이 고도화, 복잡화되어감에 따라 산업재산권 분야의 전문가에 의한 간이 중재·조정제도의 필요성이 커지면서 특허청이 발명진흥법에 근거하여 1995년 1월부터 설치·운영 중에 있음
- 조정대상은 조정신청일 현재 특허청에 등록되어 있는 산업재산권 또는 그 등록이 소멸되었다 하더라도 손해배상청구권의 소멸시효 이전인 산업재산권으로, 산업재산권의 무효 및 취소 여부, 권리범위확인 등에 관한 판단만을 요청하는 사항은 조정신청의 대상이 될 수 없음

◈ 컴퓨터프로그램보호위원회

- 컴퓨터프로그램 보호법을 기반으로 하여 소프트웨어 지적재산권에 관한 분쟁조정 및 알선업무를 수행
- 주요업무 : 소프트웨어 분쟁 및 법률상담, 심의 및 조정, 중재, 알선, 감정, 등록, 임치, 위탁관리, 침해대응 등

제4절 불공정무역행위에 대한 무역위원회의 구제제도

○ 불공정무역행위의 조사 및 산업피해구제에 관한 법률은 대한민국의 법령 또는 대한민국이 당사자인 조약에 의하여 보호되는 특허권·실용신안권·디자인권·상표권·저작권·저작인접권·프로그램저작권·반도체집적회로배치설계권 또는 영업비밀을 침해하는 물품(이하 '지적재산권침해물품 등'이라고 함)의 수출입, 국내판매, 제조행위 등을 불공정무역행위로서 금지하고 그 구제를 도모

○ 무역위원회를 활용하는 경우에는 소송과는 달리 신고서류 및 절차 등이 간편하고 신속한 조사가 행해진다는 장점이 있음

- 그러나 무역위원회의 행정조치에 대해 불복하는 경우 행정법원, 상고하는 경우 대법원의 판단까지 받아야 하기 때문에 시간 및 대리인 비용이 소요되는 단점도 존재

□ 신고절차

○ 누구라도 불공정무역행위의 사실이 있다고 인정되는 경우에는 조사하도록 무역위원회에 서면으로 신청할 수 있음

○ 불공정무역행위에 대한 조사신청은 위반행위가 있은 날로부터 1년 이내에 행해져야 함

○ 무역위원회는 조사신청이 있는 경우, 30일 이내에 조사개시의 여부에 대하여 결정

□ 제재수단

○ 시정조치명령

- 지적재산권침해물품 등의 수출입, 국내판매, 제조행위가 있다고 판정한 경우, 해당 행위자에 대하여 해당 물품 등의 수출·수입·판매·제조행위의 중지, 반입배제 및 폐기처분, 정정광고, 법위반에 의한 시정명령을 받은 사실의 공표, 기타 시정에 필요한 조치를 명할 수 있음

- 시정조치명령을 위반한 자에게는 3년 이하의 징역 또는 3천만원 이하의 벌금이 부과됨

○ 과징금

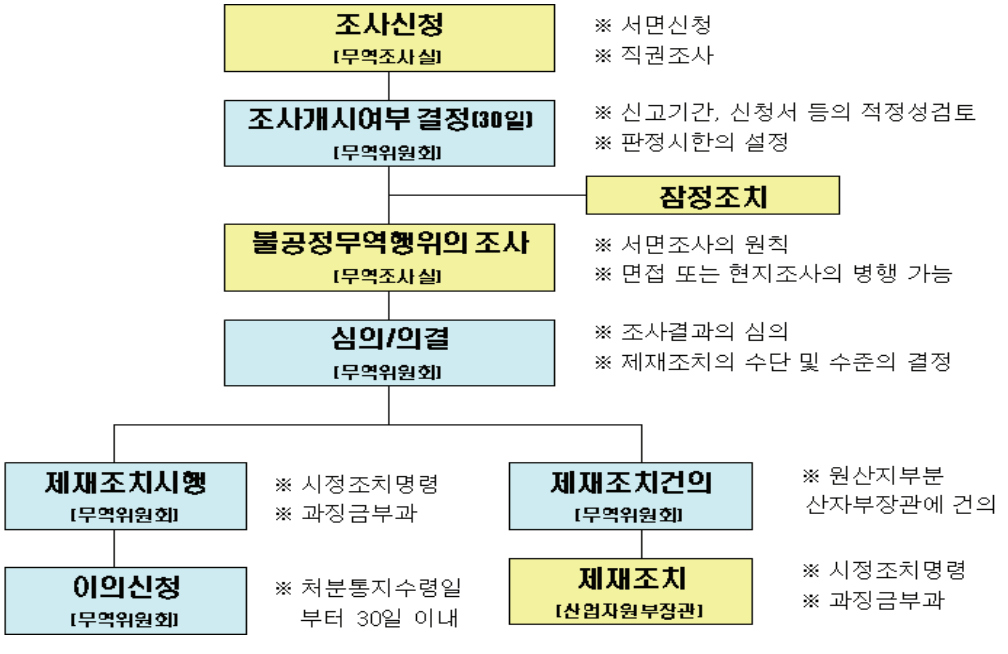
- 무역위원회는 불공정무역행위가 있다고 판정한 경우, 해당 행위자에 대하여 거래금액의 100분의 30을 곱한 금액의 범위 내에서 과징금을 부과할 수 있음
- 거래금액이 없거나 산정이 곤란한 경우에는 5억원을 초과하지 않는 범위 내에서 과징금을 부과

□ 이의신청

○ 무역위원회가 내린 시정조치명령 또는 과징금부과처분에 대해 불복할 경우에는 처분통지를 받은 날로부터 30일 이내에 이의신청을 할 수 있음

○ 무역위원회는 이의신청에 대하여 60일 이내에 결정하여야 하며, 30일 내에 기간을 연장할 수 있음

<그림4-1> 불공정무역행위 조사절차



제5절 해외진출 기업

○ 중국은 2004년부터 우리나라의 최대 무역국이며, 4만개 이상의 국내 기업이 진출하여 총 200억 달러 정도를 투자하고 있음

○ 대 중국 투자는 고임금으로 경쟁력을 잃어가던 국내기업들에게 새로운 생존 기반을 제공했다는 것이 대체적인 평가이지만 매출이익률 및 영업이익률은 갈수록 감소하고 있는 것이 현실임

○ 최근 들어 중국의 기술경쟁력 강화로 인해 한중간의 기술격차가 갈수록 줄어들고 있으며, 중국에 진출한 국내기업의 기술이전 압박도 커지고 있음

○ 이에 본 절에서는 중국진출 국내기업의 영업비밀과 지식재산권 침해시 대응 방안에 대해 살펴보기로 함

1. 영업비밀 침해

□ 영업비밀의 개념

○ 중국 반부정당경쟁법 제10조 제4항은 영업비밀에 대해

① 공중이 알지 못하고(비공지성),

② 권리자에게 경제적 이익을 가져다 줄 수 있고, 실용성을 구비한 동시에(경제적 유용성),

③ 권리자가 비밀조치(비밀관리성)를 취한 기술정보와 경영정보라고 규정

□ 영업비밀의 요건

○ 1995년 개정된 '영업비밀 침해금지에 관한 규정' 제2조는 영업비밀의 구성요건을 아래와 같이 4가지로 세분하여 규정

1) 공중이 알지 못하는 것

- 그 정보가 공개된 경로를 통해 직접 획득할 수 있는 것이 아닌 것, 즉 같은 업종에 종사하는 사람이 모르는 것을 의미

- 법원의 비공지성 판단시 고려사항(최고인민법원 해석 제17조)

  · 당해 정보가 국내외 공개된 출판물에 기재되었는지 여부

  · 당해 정보가 국내에서 사용을 통하여 공개되었는지 여부

  · 공개 보고회, 담화, 전람회 등을 통하여 공개되었는지 여부

  · 당해 정보가 관련된 범위의 사람들의 일반 상식 또는 관례인지 여부

  · 당해 정보의 보유자가 당해 정보를 취득 또는 생산하는데 지불한 노력과 대가 및 타인이 당해 정보를 취득하는데 지불한 노력과 대가를 포함하는 당해 정보를 취득하는데 곤란한 정도

2) 권리자에게 경제적 이익을 가져다 줄 것

- 권리자에게 현실적 혹은 잠재적 경제이익 또는 경쟁상 우위를 가져다주는 것을 의미

  · 동 규정 제2조 제5항에서는 설계, 절차, 제품의 배합, 제조방법 및 기술, 관리비결, 고객명단, 원재료 등의 출처정보, 판매전략, 원가계산서, 입찰서의 최저가격과 그 내용 등을 예시

- 시장에서 경쟁과 무관한 단지 비밀로 관리하고 있는 정보나 개인의 신상정보 등은 영업비밀에 해당하지 않음

3) 실용성을 구비한 것

- 정보가 객관적 유용성을 구비한 것으로 구체적으로 이용 가능하고, 그 정보를 이용하면 경제적 이익이 실현되는 것을 의미

  · 실용성은 경제적 가치의 기초로서 실용성이 없으면 경제적 가치도 없음

4) 비밀조치를 취할 것

- 사용자와 종업원 또는 거래처와의 비밀유지계약, 회사 내의 비밀유지제도, 기타 합리적인 비밀 유지조치[16] 등을 포함

16) '기타 합리적인 비밀유지 조치'에는 구두 또는 서면에 의한 비밀유지를 위한 협의, 영업비밀을 인지하고 있는 종업원 또는 업무관련 제3자에 대한 비밀유지 요구 등이 해당(중국 국가공상행정관리국 工商工字 제109호)

- 법원의 비밀관리성 판단시 고려사항(최고인민법원 해석 제20조)

· 반드시 알아야 할 직원들에게만 정보를 공개하여 알 수 있는 범위를 한정한 경우

· 정보가 수록된 매체에 대하여 밀봉하거나 기타 물리적 예방조치를 취하여, 당해 정보가 정상적인 상황 하에서 타인이 용이하게 취득하거나 접촉하지 못하는 경우

· 당해 정보에 비밀유지 표시를 하는 경우

· 제품의 배합량 및 제조공정에 비밀유지를 위한 기호를 사용하는 경우

· 당해 정보에 비밀번호를 부여한 경우

· 비밀유지협약을 체결한 경우

· 비밀정보가 있는 기계, 공장, 차량 등의 장소에 대하여 방문객들을 제한하고 그들에게 비밀유지 요구를 한 경우

· 기타 비밀 확보를 위한 노력을 한 경우

□ 영업비밀 침해행위 유형

○ 영업비밀의 침해행위 유형은 반부정당경쟁법 제10조 제1항과 제2항에 규정되어 있음

1) 부정한 수단에 의한 영업비밀의 취득(제10조 제1항 제1호)

- 절도·유혹·협박 또는 그 외의 부정한 수단에 의해 권리자의 영업비밀 취득

2) 부정한 수단에 의해 영업비밀을 취득한 후 사용·공개(제10조 제1항 제2호)

- 부정한 수단에 의해 취득한 권리자의 영업비밀을 공개·사용하고 타인에게 그 사용을 허락

3) 비밀유지 요구 또는 계약을 위반하여 영업비밀 사용 공개(제10조 제1항 제3호)

- 계약을 위반하거나 권리자의 영업비밀의 유지에 관한 요구를 위반하여 지득한 영업비밀을 공개·사용

4) 악의의 제3자에 의한 침해(제10조 제2항)

- 전항에 규정하는 위법행위를 명확하게 알고 있거나 지득한 제3자가 타인의 영업비밀을 취득·사용 또는 공개

5) 선의의 제3자의 문제

- 불법으로 영업비밀을 취득하거나 계약을 위반해서 영업비밀을 누설하는 등 불법행위를 한 자의 행위사실을 모르는 상태에서 영업비밀을 취득 사용하는 것은 선의로 보나,
- 권리자가 선의의 취득자에게 영업비밀임을 통지한 후 제3자에게 공개 사용한 경우에는 선의에서 악의로 전환

□ 영업비밀 침해행위에 대한 구제수단

(1) 행정적 구제수단

○ 영업비밀 침해행위에 대해 행정구제 절차를 활용할 수 있으며, 국가공상행정관리국에 신청하면 됨

- 영업비밀권리자가 공상행정관리국에 행정구제를 신청할 경우 신청인은 ① 피신청인(침해자)이 사용한 정보가 자신의 영업비밀과 일치한다는 것과 ② 피신청인이 당해 영업비밀을 취득한 상황(퇴직종업원, 업무관련자라는 사실)을 증명하면 됨
- 피신청인은 자기가 사용한 정보에 대해 합법적으로 취득 또는 사용하였다는 증거를 공상행정관리국에 제출하여야 하는데, 증거를 제출하지 못하거나 제출을 거부할 경우, 피신청인의 침해행위가 인정됨

(2) 민사적 구제수단

○ 반부정당경쟁법 제20조

- 상대방의 영업비밀을 침해한 침해자에 대해 손해배상 및 부정 경쟁행위 조사를 위해 지출한 합리적 비용의 배상책임을 부여
- 영업비밀권자에게는 그 영업상 이익이 침해되거나 침해 우려가 있는 사실 및 침해자를 안 날로부터 2년 이내에 침해중지 청구, 원상회복 청구, 사죄 청구, 손해배상 청구 등의 권리 인정

(3) 형사적 구제수단

○ 반부정당경쟁법 제25조

- 영업비밀 침해행위에 대해서 감독기관이 침해중지 명령을 해야 하고, 사건 정황에 따라 1만 위안 이상 20만 위안 이하의 벌금을 부과할 수 있도록 규정

○ 형법 제219조

- 반부정당경쟁법 제10조에 열거된 침해행위를 행하여 권리자에게 중대한 손해를 초래한 경우 3년 이하의 유기징역 또는 구류에 처함
- 특별히 엄중한 결과를 초래한 경우 3년 이상 7년 이하의 유기징역과 벌금을 병과할 수 있도록 규정

2. 지적재산권 침해

□ 지적재산권 침해 감시 및 단속

(1) 일반 행정기관에 의뢰

○ 공상행정관리국(工商行政管理局)은 상표권 침해 및 위조품에 대한 조사 및 증거를 수집할 권한을 갖고 있기 때문에 침해자 및 침해제품의 발견을 의뢰할 수 있음

○ 반면 특허권의 침해자 및 침해제품의 발견은 지식산권국(知識産權局)에서 담당함

○ 제품품질법에 위반되는 혐의가 있으면 국가질량감독검사검역총국(國家質量監督檢查檢疫總局)이 조사 및 증거수집 과정에서 상표권 및 특허권 침해사실을 적발할 수 있음

(2) 공안국, 인민검찰원에 고소

○ 특허권과 상표권의 침해가 범죄를 구성한다고 판단되는 경우 공안국, 인민검찰원에 고소하여 침해자 및 침해제품의 적발을 의뢰할 수 있음

○ 하지만 법적으로 형사입건이 가능함에도 불구하고, 실제로는 지식재산권 침해 단속에 적극적으로 나서지 못하고 있는 상황

(3) 민간기관의 활용

○ 컨설팅회사나 법률사무소에 자문을 구하도록 하며, 특허권, 상표권 등의 침해자 및 침해제품의 적발을 의뢰받아 처리하는 민간기관을 통해 증거를 수집할 수도 있음

□ 지적재산권 침해 구제방법

(1) 쌍궤제(雙軌制) 활용

○ 중국에서 전리권(특허권 등) 또는 상표권을 침해당했을 경우 구제받을 수 있는 방법은 지방정부의 전리관리기관(전리권의 경우), 공상행정관리기관(상표권의 경우)에 신고하거나 인민법원에 제소할 수 있는데, 이를 두 개의 수레바퀴를 이용한다고 하여 '쌍궤제(雙軌制)'라고 함

○ 이 경우 권리자는 행정적 구제와 사법적 구제 중 하나를 선택하거나 모두 이용할 수 있음

- 일반적으로 전리권 침해는 사법기관을 이용하고, 상표권 침해는 행정기관을 이용하는 것이 효율적임

(2) 전리권(특허, 실용신안, 디자인 등) 침해

○ 전리권자의 허가 없이 전리권을 침해하여 분쟁을 일으킨 경우 당사자가 협상하여 해결하며, 협상을 원하지 않거나 협상이 성립되지 않은 경우 인민법원에 소를 제기하거나, 전리업무관리부서에 처리를 청구할 수 있음

○ 전리업무관리부서가 처리할 때 권리침해행위 성립이 인정되면, 침해행위의 중지를 명하고, 불응하는 경우 인민법원에 강제집행 신청 가능

- 전리업무관리부서의 결정에 당사자가 불복하는 경우 처리통지를 받은 날로부터 15일 이내에 중국 행정소송법에 따라 인민법원에 소를 제기할 수 있음

○ 전리업무관리부서는 당사자의 청구에 따라 전리권 침해에 따른 배상액수를 조정할 수 있음

- 조정이 성립되지 않은 경우 당사자는 중국 민사소송법에 근거하여 인민법원에 소를 제기할 수 있음

○ 타인의 전리를 모방하는 경우, 법에 따라 민사책임을 지는 이외에, 전리업무관리부서가 시정을 명하고 이를 공고하며, 위법소득을 몰수하고 위법소득의 3배 이하의 벌금을 병과할 수 있음

- 위법소득이 없는 경우 5만 위안 이하의 벌금에 처할 수 있으며, 범죄를 구성하는 경우 법에 따라 형사책임을 부과함

○ 비전리물건을 전리물건으로 사칭하거나 비전리방법을 전리방법으로 사칭하는 경우, 전리업무관리부서는 시정을 명하고 이를 공고하며, 5만 위안 이하의 벌금에 처할 수 있음

○ 전리권침해의 배상액은 권리자가 침해에 의해 받은 손실 또는 침해자가 권리침해로 얻은 이익에 따라 확정하며, 침해소송의 시효는 2년으로 함

(3) 상표권 침해

○ 상표 등록자의 허가 없이 등록상표 전용권을 침해한 경우 당사자가 협상하여 해결하며, 협상을 원하지 않거나 협상이 성립되지 않은 경우 인민법원에 소를 제기하거나, 공상행정관리부서에 처리를 청구할 수 있음

○ 공상행정관리부서가 처리할 때 권리침해행위 성립이 인정되면, 침해행위의 중지를 명하고, 권리 침해상품과 사용도구를 몰수, 소각하는 동시에 벌금을 병과할 수 있음

- 공상행정관리부서의 결정에 당사자가 불복하는 경우 처리통지를 받은 날로부터 15일 이내에 중국 행정소송법에 따라 인민법원에 소를 제기할 수 있음
- 권리 침해자가 소를 제기하지도 않고, 이행하지도 않은 경우 인민법원에 강제집행 신청 가능

○ 공상행정관리부서는 당사자의 청구에 따라 상표전용권 침해에 따른 배상액수를 조정할 수 있음

- 조정이 성립되지 않은 경우 당사자는 중국 민사소송법에 근거하여 인민법원에 소를 제기할 수 있음

○ 상표전용권 침해행위에 대해서 공상행정관리부서는 법에 따라 조사, 처리할 수 있으며, 범죄를 구성한다고 판단될 경우 사법기관에 이송

○ 상표전용권 침해의 배상액수는 권리 침해자가 얻은 이익 또는 피침해자가 입은 손실을 기준으로 결정하며, 확정하기 어려울 경우 권리침해 행위 정상에 근거하여 50만 위안 이하의 배상

(4) 인민법원에 제소

○ 중국의 법원은 4단계로 구분되어 있으며, 2심제를 채택하고 있음

- 1단계 : 기층인민법원(지법 지원에 해당)

- 2단계 : 중급인민법원(지방법원에 해당), 북경 제1중급인민법원(국가지식산권국 소재지)
- 3단계 : 고급인민법원(고등법원에 해당)
- 4단계 : 최고인민법원(대법원에 해당)

○ 사법기관을 이용함으로써 침해행위 중지, 강제집행, 손해배상, 사죄광고를 통한 명예회복 등의 민사적 구제 가능

○ 사법기관 이용시 제1심 법원의 선택이 매우 중요함

- 중국의 지방에서 지식재산권 침해행위 발생시 지방보호주의로 인해 침해사실이 분명하고 증거가 명백함에도 불구하고 소송이 지연되는 일이 발생하는 경우가 많음
- 지방보호주의는 상급심과 대도시로 갈수록 약해지며, 따라서 지방의 인민법원보다는 대도시의 인민법원과 상급법원에 제소하는 것이 효과적임

○ 가처분 제도의 적극적 활용

- 중국은 전리법 개정(2001년)을 통해 '제소전 금지제도'를 도입하였는데, 전리권이나 상표권은 침해행위를 즉시 금지시키는 것이 효율적이므로 이를 위해서는 가처분제도를 적극적으로 활용할 필요가 있음

3. 심판 및 소송비용 지원

□ 지원대상

1) 등록된 산업재산권 침해에 대한 조사, 심판 및 소송비용

2) 반부정당경쟁법에 의하여 보호되는 권리의 침해에 대한 조사, 심판 및 소송비용

3) 국내·외 등록권리에 기하여 중국에 등록된 타인의 권리를 무효 또는 취소하기 위한 심판, 소송비용

□ 지원금액

○ 지원대상 1)과 2)의 경우

- 조사, 심판 및 소송에 있어서 실 소요비용의 70% 범위 내에서 1건당 조사비용 500만원, 심판 및 소송비용 5,000만원

○ 지원대상 3)의 경우

- 실 소용비용의 70% 범위 내에서 1건당 1,000만원

□ 지원신청

○ 지원신청은 KOTRA에 하며, 2개월 이내에 관련 조치를 취하여야 지원이 가능함

참 고 문 헌

참 고 문 헌

국가정보원, 산업보안 연구논총, 2007

_____, 산업보안 Focus, 2004

_____, 산업스파이 사건 재조명, 2004

_____, 산업스파이 식별요령, 2004

_____, 주요국의 산업기밀 보호관련 법령, 2004

_____, 첨단 산업기술 보호동향 2호~8호, 2004~2007

국제지식재산연수원, 특허분쟁대응전략과정, 2007

김윤배, 기업체 연구원들의 기술유출 예방지침서, 2007

대한변리사회, 중소기업을 위한 지식재산 관리 매뉴얼, 2006

산업자원부, 국가핵심기술지정, 2007

_____, 산업기술보호지침, 2007

삼성경제연구소, 한국의 특허경쟁력과 대응전쟁, 2005

_____, 핵심기술 해외유출의 실태와 대책, 2004

이동훈 외, 지식재산권법, 2007

일본 경제산업성, 영업비밀관리지침, 2003

_____, 기술유출방지지침, 2003

정보통신부・한국정보보호진흥원, 중소기업 정보보호 가이드라인, 2006

중소기업청・중소기업기술정보진흥원, 보안전략수립 전문가과정, 2007

_____, 중소기업 기술유출 사례 및 대응전략, 2007

_____, 중소기업 산업기밀관리 실태조사 보고서, 2007

중소기업청・중소기업진흥공단, 성공적인 중국 비즈니스를 위한 산업기술보호 세미나, 2007

최문기 외, 과학기술과 지식재산권법, 2007

특허청, 문답식으로 알아보는 개정 직무발명제도, 2006

_____, 보안업무실무, 2006

_____, 부정경쟁방지 업무해설서, 2004

_____, 영업비밀보호 가이드북, 2004

_____, 제13회 직무발명세미나, 2007

_____, 직무발명 보상절차 가이드라인, 2006

_____, 직무발명제도 이렇게 바뀌었습니다, 2006

_____, 해외 지식재산권 보호가이드북, 2006

프로그램심의조정위원회, IT관련 지적재산권 관리매뉴얼, 2006

한국기술거래소, 기술거래・평가 전문인력 양성을 위한 기본과정, 2006

_____, 기술유출 대응방안 매뉴얼, 2005

한국산업기술진흥협회, 기술정책 Hot-Issue 2호, 2003

_____, 기업연구소 산업기밀 관리실태 및 개선방안, 2006

_____, 전략기술/물자 수출통제제도 설명자료, 2007

_____, 중소기업 대상 기술유출 방지를 위한 산업보안 세미나, 2007

한국전자산업진흥회, 국제특허분쟁대응 표준 매뉴얼, 2007

_____, 국제특허세미나, 2007

한국정보보호진흥원, 정보보호관리체계 관리과정 가이드, 2004

_____, 정보보호관리체계 통제사항 가이드, 2004

한국정보통신수출진흥센터, 산업보안과 기술유출, 2004

_____, IT기술 해외유출 방지를 위한 매뉴얼, 2004

한국형사정책연구원, 산업스파이에 대한 형사법적 대응방안, 2000

황의창 외, 부정경쟁방지 및 영업비밀보호법, 2006

British Standard Institute(BSI), ISO/IEC 17799, 2005

_____, ISO/IEC 27701, 2005

KOTRA, 중국에서의 지식재산권 보호전략세미나, 2006

LG경제연구원, 핵심기술유출을 막는 4가지 전략, 2004

< 참고사이트 >

교도통신, www.kyodo.co.jp

니혼게이자이, www.nikkei.co.jp

대한상사중재원 www.kcab.or.kr

로이터통신, www.reuters.com

마이니치 신문, www.mainichi.co.jp

미국산업보안협회(ASIS, America Society for Industrial Security), www.asisonline.org

미 법무부(USDOJ, United States Department of Justice), www.usdoj.gov

요미우리 신문, www.yomiuri.co.jp

컴퓨터프로그램보호위원회 www.socop.or.kr

프랑스 국영방송 TF1, www.tf1.fr

All-China Women's Federation, www.women.org.cn

www.theresister.co.uk

www.therstandard.com

부 록 기술유출 현황 및 사례

제1절 국내 중소기업

1. 기술유출 현황

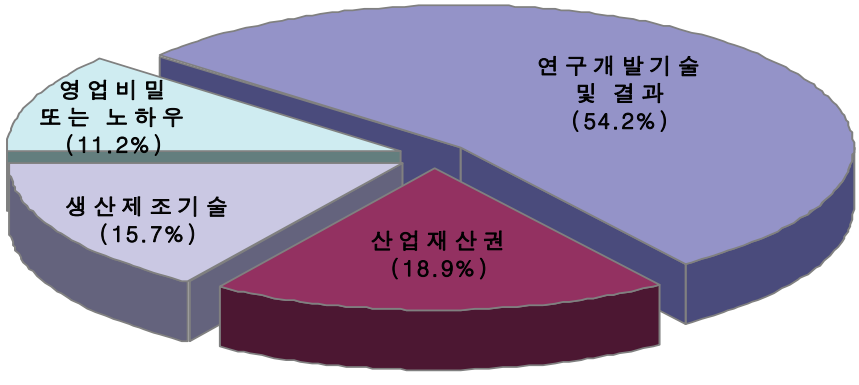
○ 다음은 중소기업청과 한국산업기술진흥협회에서 지난 2007년 3월 28일부터 5월 9일까지 1,200개 기업을 대상으로 실시한 「중소기업 산업기밀관리 실태조사」결과를 분석, 정리한 것임

가. 산업보안 인식수준

□ 핵심 산업기밀 내용

○ 중소기업이 보유하고 있는 핵심 산업기밀은 연구개발기술 및 결과가 54.2%로 가장 많았으며, 산업재산권 18.9%, 생산제조기술 15.7%, 영업비밀 또는 노하우 11.2% 등의 순으로 나타남

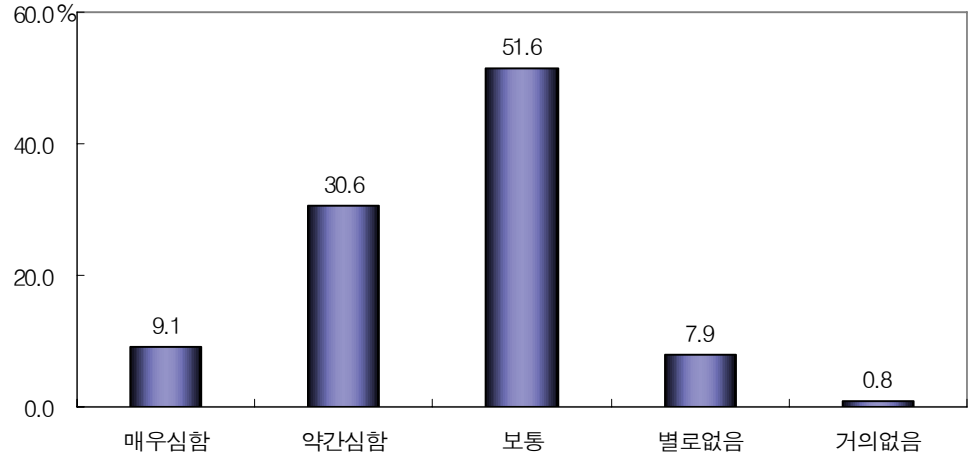
<그림-부1> 핵심 산업기밀 내용



□ 산업기밀 유출에 대한 위협정도

○ 중소기업들이 산업기밀 유출에 대해 대내외적으로 느끼는 위협의 정도는 응답기업의 39.7%가 심하다고 응답했으며, 51.6%는 보통수준이라고 응답함. 반면 위협이 없다는 응답은 8.7%에 불과했음

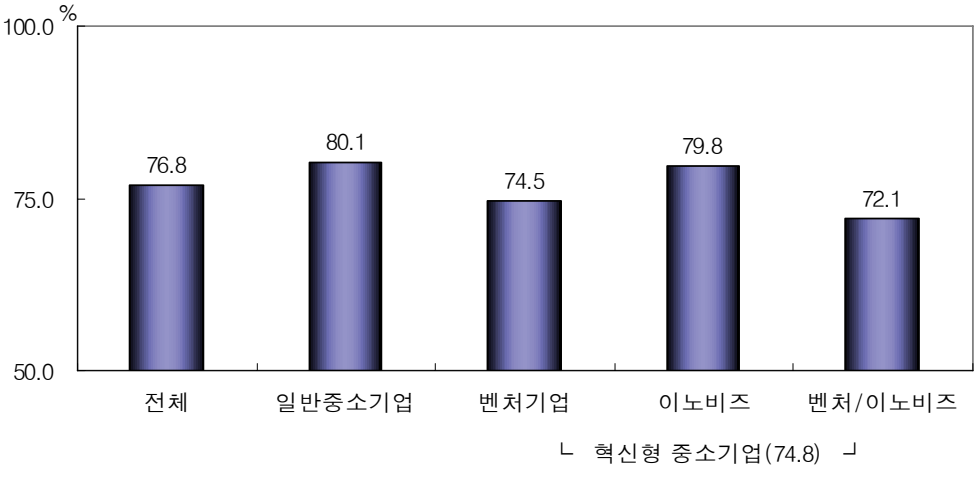
<그림-부2> 산업기밀 유출에 대한 위협정도



□ 중요 정보에 대한 비밀분류 여부

○ 응답 중소기업의 76.8%가 기술개발 과정에서 생성되는 중요한 정보들에 대해 비밀로 분류하여 관리하고 있는 것으로 나타남

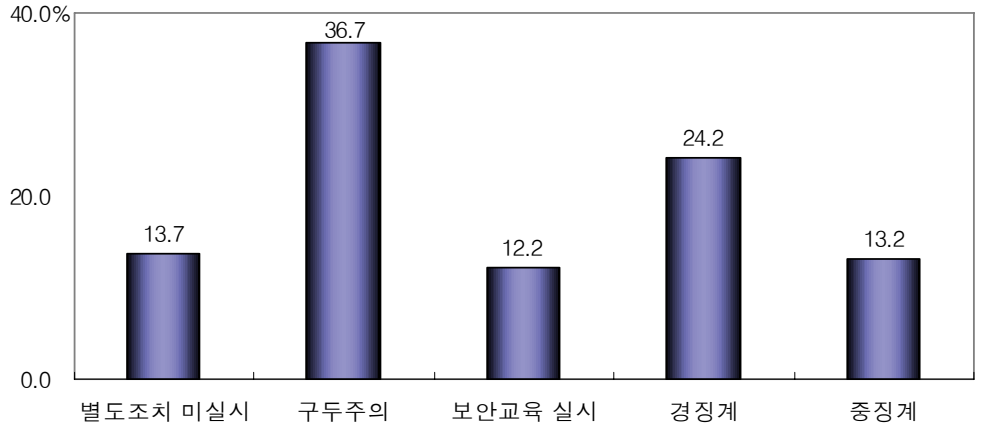
<그림-부3> 중요 정보에 대한 비밀분류 여부



□ 사내 보안규정 위반자 조치사항

○ 사내 보안규정 위반자에 대해 응답기업의 37.4%만이 징계 이상의 강한 처벌을 하는 반면, 대부분의 기업들이 별도조치를 실시하지 않거나 구두주의에 그치는 등 징계 이외의 형식적인 조치를 선호하는 것으로 나타남

<그림-부4> 사내 보안규정 위반자 조치사항



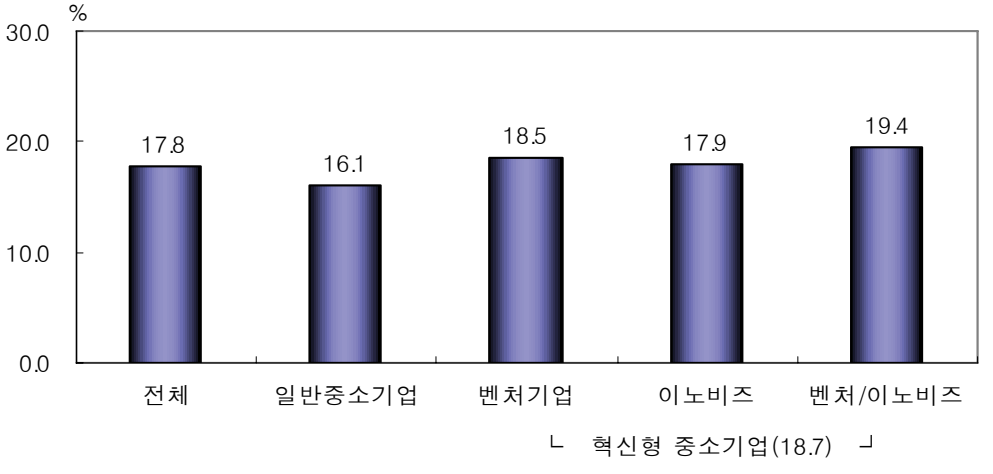
나. 산업기밀 유출현황

□ 산업기밀 유출현황

○ 응답 중소기업의 17.8%가 최근 3년간 산업기밀의 외부 유출로 인해 피해를 입은 것으로 나타남

○ 기업유형별로는 혁신형 중소기업의 기밀유출 비율이 18.7%로 일반 중소기업의 16.1%에 비해 높게 나타남

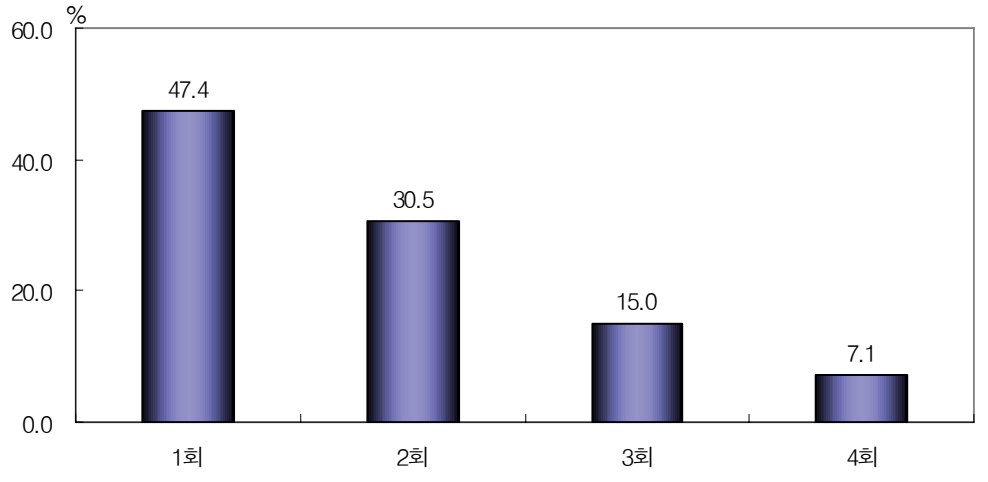
<그림-부5> 산업기밀 유출현황



□ 산업기밀 유출횟수

○ 최근 3년간 내부 기밀정보가 외부로 유출되어 피해를 입은 적이 있다고 응답한 기업 중 52.6%가 2회 이상의 기밀유출 경험이 있는 것으로 나타남

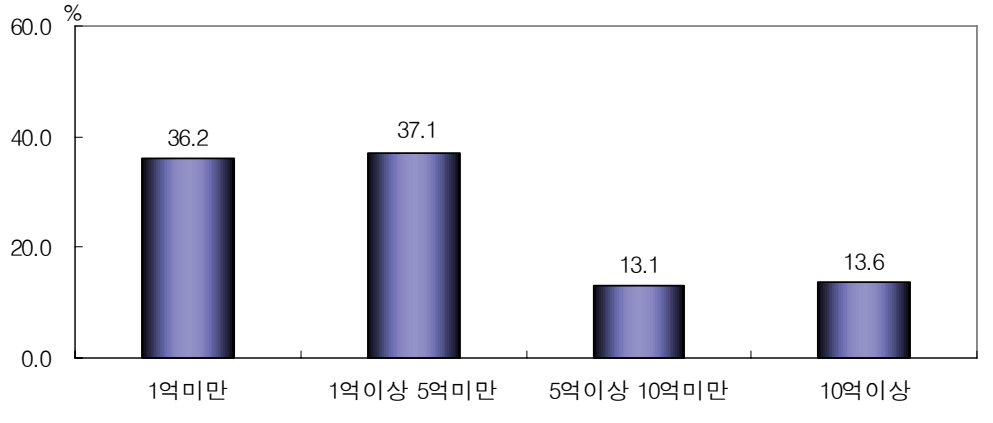
<그림-부6> 산업기밀 유출횟수



□ 1건당 산업기밀 유출 피해금액

○ 최근 3년간 산업기밀 유출경험이 있는 기업의 건당 피해금액은 '1억 이상 5억 미만'이 37.1%로 가장 높게 나타남

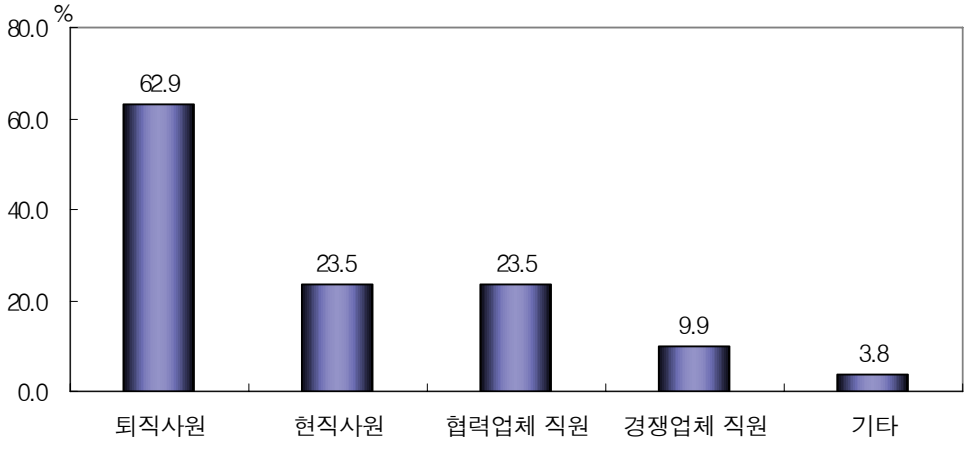
<그림-부7> 1건당 산업기밀 유출 피해금액



□ 산업기밀 유출관계자

○ 산업기밀 유출관계자는 퇴직사원이 62.9%로 가장 많았으며, 현직사원(23.5%), 협력업체 직원(23.5%)과 경쟁업체 직원(9.9%)이 주요 기밀유출 관계자로 조사됨

<그림-부8> 산업기밀 유출관계자(복수응답)



□ 산업기밀 유출시 조치사항

○ 산업기밀 유출시 특별한 조치를 취하지 않는 기업이 52.6%로 높게 나타나 중소기업의 경우 기밀유출에 대한 사후대응이 매우 소극적인 것으로 분석됨

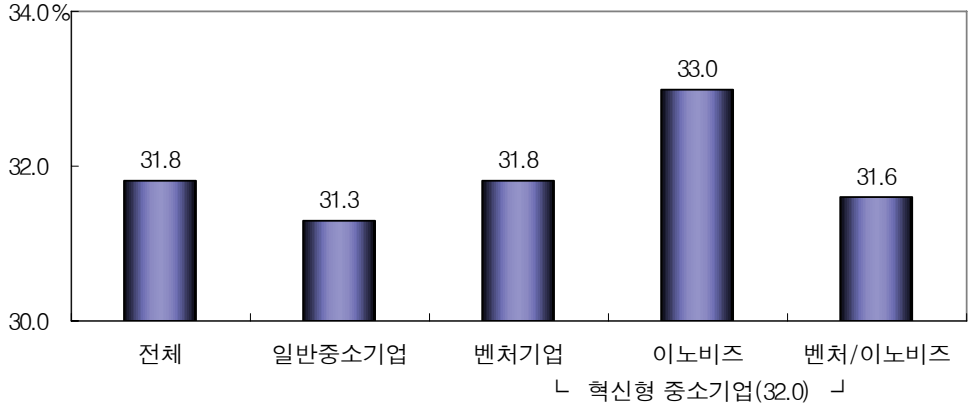
<표-부1> 산업기밀 유출시 조치사항(복수응답)

구 분	일반 중소기업	혁신형 중소기업	전 체
수사기관에 수사의뢰	2.8%	8.5%	6.6%
관계자(사) 고소, 고발	9.7%	18.4%	15.5%
관계자(사)에 손해배상 청구	4.2%	7.8%	6.6%
연구소 보안관리시스템 강화	38.9%	21.3%	27.2%
특별한 조치 미실시	47.2%	55.3%	52.6%
기 타	15.3%	9.9%	11.7%

□ 연구원 경쟁업체 전직현황

○ 응답 중소기업의 31.8%가 최근 2년간 소속 연구원이 퇴사 후 경쟁업체로 전직한 경험이 있는 것으로 나타남

<그림-부9> 연구원 경쟁업체 전직현황(기업유형별)



다. 산업기밀 관리현황

□ 조직 및 제도

○ 조직 및 제도의 경우 일반 중소기업과 혁신형 중소기업을 막론하고 전체적으로 50% 미만으로 낮게 나타남

○ 특히 보안담당부서 설치(6.6%), 정례 보안점검·감사(9.8%), 정례 보안관리 교육(14.9%) 등의 경우 20% 미만으로 낮게 나타나 이에 대한 관심과 대책이 요구됨

<표-부2> 산업기밀 관리현황(조직 및 제도)

구 분	일반 중소기업	혁신형 중소기업	전 체
보안관리규정 마련	37.4%	34.1%	35.3%
보안담당부서 설치	6.3%	6.8%	6.6%
보안담당자 지정	26.8%	25.4%	25.9%
정례 보안점검·감사	8.7%	10.4%	9.8%
정례 보안관리 교육	17.2%	13.5%	14.9%

□ 보안감독체계

○ 보안감독체계의 경우 방문자 출입통제와 입사시 비밀엄수서약을 제외한 모든 항목에서 50% 미만으로 나타남

○ 기업유형별로 살펴보면 혁신형 중소기업이 일반 중소기업에 비해 전반적으로 높게 나타남

<표-부3> 산업기밀 관리현황(보안감독체계)

구 분	일반 중소기업	혁신형 중소기업	전 체
연구노트·일지 작성	35.3%	36.1%	35.8%
입사시 비밀엄수서약	53.2%	60.6%	57.8%
퇴사시 비밀유지 및 경쟁업체 취업금지 서약	43.2%	50.9%	48.0%
방문자 출입통제	64.9%	68.3%	67.0%
거래업체에 대한 비밀유지 계약	41.2%	46.2%	44.3%

□ 기업연구소 출입 및 접근통제 수단

○ 연구소 출입 및 접근통제 수단으로 카드키 시스템을 활용하는 기업이 51.2%로 가장 많았으며, 그 다음으로 시건장치 32.2%, 지문인식 시스템 10.2% 등의 순으로 높게 나타남

<표-부4> 기업연구소 출입 및 접근통제 수단

구 분	시건장치	지문인식 시스템	카드키 시스템	기 타	합 계
일 반 중소기업	36.9%	10.7%	47.2%	5.2%	100%
혁신형 중소기업	29.4%	9.8%	53.6%	7.2%	100%
전 체	32.2%	10.2%	51.2%	6.4%	100%

2. 기술유출 사례

○ 다음은 중소기업청과 한국산업기술진흥협회에서 2007년 7월 5일부터 7월 27일까지 산업기밀유출 피해경험이 있는 65개 기업을 대상으로 실시한 방문조사 결과를 분석, 정리한 것임

가. 유출관계자

□ 전·현직 종업원

사례 1.

> 용접기기 관련 기술을 개발하는 A사는 얼마 전 신입 연구원 B를 채용하고 신기술 개발에 참여시킴. 그러나 몇 달이 지나도록 B는 기대했던 것만큼의 성과를 내지 못하였고, 결국 CEO는 B의 역량이 부족하다고 판단하여 그를 해고함
>
> 이에 불만을 품은 B는 A사의 핵심기술 중의 하나인 전원공급장치 도면 등 관련 정보를 개인 노트북에 다운로드받는 방식으로 몰래 가지고 나가, 연구직을 보장받는 대가로 이를 경쟁업체로 넘김

○ 기업유형 : 기계소재

○ 유출대상 : 전원공급장치 관련 기술정보

○ 피해규모 : 약 1억원

○ 유출인지 : B가 퇴사한 지 6개월 후 B와 친분이 있는 내부 직원에 의해 알게 됨

○ 조치사항

- B에게 전화로 구두 경고하는 수준에서 그침
- 새로 개발된 기술은 가능하면 특허출원을 하고, 같은 연구소 직원이라도 본인이 담당하고 있는 소스를 타인에게 공개하지 말 것을 교육

사례 2.

○○ 소프트웨어 부분 국내 최고 기술을 보유하고 있는 B사에서 개발 업무를 담당하던 팀원 5명이 단체로 회사를 퇴직하고 직접 후발업체를 설립함

B사에서는 퇴직사원이 후발업체로 이직하는 경우가 종종 있어 이를 알고도 묵인하였는데, 얼마 후 퇴직자들이 B사의 기술 노하우를 이용하여 유사한 제품을 생산, 판매하고 있다는 사실을 확인하고 소송을 제기함

○ 기업유형 : 정보통신

○ 유출대상 : 소프트웨어 솔루션

○ 유출배경 : B사는 ○○ 소프트웨어 관련 분야에서 국내점유율 70%를 차지하는 국내 선두기업으로 항상 국내·외 후발주자들로부터 기술유출에 대한 위협을 받고 있음

○ 피해규모 : 사업비(약 20억원) + α

○ 유출인지 : 시장규모가 작을 뿐만 아니라 국내 선두기업으로서 유통경로를 훤히 꿰뚫고 있기 때문에 자연스럽게 인지 가능

○ 조치사항 : 현재 소송 진행중이며, 앞으로 비슷한 사건이 다시 발생하지 않도록 확실히 사건을 매듭짓고자 함

사례 3.

게임개발업체인 C사에서 캐릭터 개발 담당자로 근무하던 A는 C사의 신제품 출시를 몇 달 앞둔 시점에서, 사내의 친분 있는 프로그램 소스 개발 담당자와 함께 경쟁업체로 이직함

이들은 그동안 C사에서 중점적으로 개발해 왔던 게임 프로그램 소스와 캐릭터를 도용하여 유사한 게임을 만든 뒤 시장에 먼저 출시함

○ 기업유형 : 정보통신

○ 유출대상 : 연구개발 중인 게임 프로그램 소스와 캐릭터

○ 유출배경 : 게임 상품은 생명주기가 매우 짧은 편이고, 일단 흥행 조짐이 보이는 게임이 하나 출시되면, 얼마 후 시장에서는 이를 모방한 게임과 캐릭터가 우후죽순처럼 생겨남

○ 피해규모 : 약 10억원

- 경쟁업체가 먼저 제품을 출시함에 따라 게임개발을 원래 계획하고 추진했던 C사가 오히려 경쟁업체의 저작권을 침해하게 되는 아이러니한 상황이 발생함

○ 유출인지 : 신제품 출시 마무리 단계에 있을 때 경쟁업체에서 C사의 것과 유사한 게임을 출시하였다는 소식을 접함

○ 조치사항 : 법적 대응을 위해 변호사를 고용하고 소송 준비 중

사례 4.

B는 D사에서 근무하는 외국인 기술훈련생 중 한 명으로, D사의 대표는 B가 어느 정도 기술력을 갖추고 있고 매사에 성실한 태도로 작업에 임한다는 판단 아래 그를 부설연구소에서 프로젝트 연구개발에 참여할 수 있도록 조치함

연구소에서도 능력을 인정받던 B는 몇 달 뒤 갑자기 어머니가 위독하시다는 핑계로 휴가를 내고 모국으로 돌아갔으며, D사에서는 나중이 되어서야 B가 자국 업체에 D사의 핵심기술 노하우를 넘긴 사실을 알게 됨

○ 기업유형 : 전기전자

○ 유출대상 : 새로 개발 중인 회사 핵심기술

○ 유출배경 : 외국인 근로자에 대한 국내 중소기업의 수요가 늘어나면서, 외국인 고용자가 한국 기업에서 익힌 기술과 노하우를 모국 기업에 유출시키는 사건이 증가하고 있음

○ 피해규모 : 약 20억원

○ 유출인지 : CEO가 작업장을 돌던 중 우연히 다른 외국인 기술훈련생이 B에 대해 이야기하는 것을 듣게 됨

○ 조치사항

- 유출 사실을 확인한 후 곧바로 B의 행방을 쫓았으나, B는 이미 모국에서 잠적한 후였음
- 외국인을 포함한 모든 직원들을 대상으로 퇴직시 D사에서 습득한 기술 및 노하우를 타사에서 이용하지 않는다는 내용의 서약서를 작성하도록 함

사례 5.

Z사는 90년대 중반 공동창업을 통해 ○○ 제조장비 사업을 시작하였으며, 창업 당시 두 창업자는 서로 간에 동종분야에서의 창업을 금지하는 서약서를 작성함

하지만 공동창업주 한 명이 회사를 그만두고 동종 사업분야에서 재창업을 시도하는 사건이 발생함

○ 기업유형 : 전기전자

○ 유출대상 : 회사 창업의 근간이 되었던 핵심기술 및 영업노하우

○ 피해규모 : 기술적 노하우가 유출되고 영업망이 감소되는 등의 피해를 입음

○ 유출인지 : 공동 창업자가 퇴사하고 새로운 사업을 시작하는 것에 대해 의심을 품고 미리 대응방안 강구

○ 조치사항 : 창업시 계약조건을 근거로 법적 조치를 취해 법원에 의해 상대방의 영업금지 가처분 신청이 받아들여졌음

사례 6.

E사에서는 일본 시장 진출을 목표로 주식거래 관리 프로그램을 개발 중이었으나, 개발 책임자와 연구원 전원이 약 한 달간의 간격을 두고 모두 퇴사함. 이들은 그동안 개발했던 기술자료 등을 가지고 국내 경쟁업체로 이직하여 독립된 사업팀을 조직함

전직한 업체에서 유사한 프로그램을 개발하여 일본 내 투자회사 등과 함께 일본에 합작회사를 설립하려 시도하였으나 국내 정보기관에 의해 발각되면서 계획이 무산됨

○ 기업유형 : 정보통신

○ 유출대상 : 온라인 주식거래 프로그램

○ 유출배경 : 회사 내에서 자신들의 미래가 불투명하다고 판단하고 있던 기술유출자들이 경쟁업체로부터 금전적인 유혹에 넘어가 유출행위를 저지름

○ 피해규모 : 정확한 피해규모를 추정하기 어려움

- 기술유출자들이 E사가 망해야 자신들이 살아남을 수 있다는 논리로 회사를 음해함
- 전체적으로 회사 조직이 와해되고 있는 듯한 조짐이 있으며, CEO와 직원들 간의 상호 불신이 심화됨

○ 유출인지 : 정보기관의 수사 결과

○ 조치사항

- 검찰에 사건 가담자 전원을 고소하였으며, 1심 재판결과 유죄가 인정되어 현재 항소심이 진행중임
- 보안관리 프로그램을 설치하고, 연구기획팀장을 통해 연구원의 개발성과에 대한 관리를 보다 철저히 함
- 관리자들이 보안교육을 받고 사내에 전파교육 실시

□ 협력업체 종사자

사례 1.

기존의 거래업체로부터 제품개발을 의뢰받은 F사는 시제품 제작을 마치고 샘플과 도면을 넘긴 뒤 양산발주를 기다렸으나, 오랫동안 연락이 오지 않음

한참 후에야 F사는 거래업체가 자사의 개발 제품을 토대로 중국 공장에서 이미 양산을 시작했다는 사실을 확인하게 됨

○ 기업유형 : 기계소재

○ 유출대상 : 제품 샘플 및 도면

○ 피해규모 : 전년대비 매출이 30% 이상 감소하였고, 양산을 하지 못하게 됨에 따라 근로자 20여명을 해고함

○ 유출인지 : 평소 친분이 있던 동종업계 사람이 중국 출장을 갔다가 소식을 듣고 사장에게 알려줌

○ 조치사항 : 협력업체와 거래를 끊고, 향후 계약체결건에 대해서는 제품 도면을 100% 공개하지 않는다는 방침을 정함

사례 2.

건설현장 내 리프트를 제조하는 G사의 후발업체인 H사는 본래 타워크레인 제작만을 전담하던 중견기업으로, 얼마 전부터 타워크레인 개발 사업을 중단하고 리프트 제조 시장에 뛰어듦

G사는 H사의 기술수준이 자사보다 최소 2~3년 이상 뒤쳐진 것으로 생각했으나, G사의 부품제조를 맡고 있는 협력업체의 도움으로 예상 밖으로 빠른 시일 내에 G사의 기술력을 따라잡게 됨

○ 기업유형 : 전기전자

○ 유출대상 : 리프트 제조에 이용되는 각종 부품 제조기술

○ 유출배경 : 업무의 특성상 특정한 기업이 동종업계 대부분의 외주 업무를 담당하여 협력업체를 통한 기술유출 가능성 상존

○ 피해규모 : H사가 G사의 시장을 잠식하면서 약 20~30억원 규모의 매출액 감소

○ 유출인지 : 회사 자체적인 시장동향 분석결과를 통해 인지

○ 조치사항

- 정확한 물증이 없어 특별한 조치를 취하지 못함
- 부품업체에 도면을 넘겨줄 경우 반드시 유인물 형태를 띠도록 하며, CAD 자료도 철저히 관리하도록 함
- 내부 직원들을 대상으로 협력업체관리 교육 실시

사례 3.

자동차 부품을 개발하는 H사는 제품 제조를 맡긴 외부 하청업체를 통해 일본과 제휴해서 개발한 신기술 정보가 경쟁업체로 유출되는 사건을 겪음
여기에 기술제휴 과정에 참여했었던 H사의 현직사원까지 경쟁업체로 이직하여 H사의 신기술을 무단으로 이용하는 데 도움을 줌

○ 기업유형 : 기계소재

○ 유출대상 : 자동차 부품관련 핵심기술

○ 유출배경 : H사가 거래한 외부 협력업체는 H사 뿐만 아니라 동종 업계의 여러 회사를 상대하기 때문에 협력업체를 통해 경쟁업체의 기술들이 서로 노출될 우려가 있었음

○ 피해규모 : 일본과 기술제휴를 위해 투자한 금액만 해도 3억원이 넘으며, 향후 피해금액까지 고려하면 이보다 훨씬 더 커질 것으로 예상됨

○ 유출인지 : 시장이 좁고, 기술제휴가 종료된 지 얼마 되지 않은 시점이어서 금방 인지 가능

○ 조치사항 : 업계의 특성상 협력업체를 바꾸기 어려운 상황이어서 협력업체를 상대로 소송을 제기하지는 못하고 경고문을 발송함

사례 4.

자연친화적인 웰빙 조리기구를 개발하는 J사의 대리점 업주 50여명은 서로 담합하여 J사의 제품을 무단으로 카피한 뒤 유사제품 생산을 시도함
아울러 인터넷 포털 사이트에 안티카페를 개설하여 J사를 비방함

○ 기업유형 : 기계소재

○ 유출대상 : 유해성분을 정제하고 산화를 최소한으로 억제시키는 튀김기 제조기술

○ 유출배경 : 관련 기술을 개발하는 업체가 거의 없기 때문에 후발업체의 견제가 심하고, 직원들이 퇴사하여 직접 창업하는 경우가 종종 발생함

○ 피해규모 : 실제로 핵심기술이 유출되지는 않았으나, 약 5억원 정도의 피해를 입음

○ 유출인지 : 여러 대리점에서 J사와의 거래를 파기하자 이를 이상하게 여기고 진상조사를 실시하여 알게 됨

○ 조치사항

- 협력업체 간담회를 통해 기술유출에 대한 주의 경고
- 핵심기술의 경우 가능하면 특허를 출원하고, 협력업체와의 계약시 계약조건을 보다 구체적으로 작성하도록 함

사례 5.

네트워크 및 IT인프라 관리 소프트웨어를 개발하는 K사는 대기업 계열사인 한 정보통신 업체와 공동 연구개발을 진행하던 도중, 협력업체에서 내부 사정을 이유로 갑자기 연구개발 협력을 중단

얼마 후 해당 협력업체는 그동안 K사와 함께 개발해온 솔루션 소스를 이용하여 먼저 신제품을 출시하고, 이로 인해 막대한 이익을 챙김

○ 기업유형 : 정보통신

○ 유출대상 : 공동연구 중이었던 네트워크 관리 솔루션

○ 유출배경 : 대기업(甲)과 중소기업(乙)이 지속적으로 원·하청 관계를 유지하거나, 기술개발 관련 협력을 하고 있는 경우, 중소기업 측의 입장에서는 대기업 담당자의 무리한 요구사항을 거절하기 어려움

○ 피해규모 : 협력업체가 독점적으로 제품을 출시해 얻은 이익이 약 50억원에 이름

○ 유출인지 : 협력업체에서 출시한 신제품을 보고 인지

○ 조치사항 : 공동 연구개발 당시 계약서를 작성하지 않았기 때문에 특별한 조치를 취하지 못함

□ 경쟁업체 종사자

사례 1.

(1) 귀금속 디자인 업체인 L사의 신제품이 출시되었다는 소식을 접한 경쟁업체에서 백화점 매장에 진열되어 있던 L사의 제품을 구매하여 디자인을 카피한 뒤 생산·유통시킴
(2) 경쟁업체에서 입사를 희망하는 L사의 퇴직 디자이너에게 디자인 포트폴리오를 요구하여 신제품 디자인 도안이 경쟁업체에게 공개됨

○ 기업유형 : 디자인

○ 유출대상 : 신제품 디자인

○ 유출배경

- 회사간 디자인 카피가 일상화 되어 있으며, 제품을 구매하면 바로 카피가 가능하다는 업계 특성 때문에 이를 관리하는데 한계가 존재
- 디자인 생명주기가 짧아 모든 디자인에 대해 특허를 취득하여 관리하는 것이 현실적으로 어려움

○ 피해규모 : 약 15억원

○ 유출인지 : 매장과 국내외 전시회 등을 통해 인지

○ 조치사항

- 회사 내에 지문인식시스템, CCTV 등을 설치·활용하도록 하고 개인적인 복사를 금지
- 디자인의 경우 '회사 소유'라기 보다는 '디자이너 소유'라는 인식이 강해, 직원들에게 퇴직시 경쟁업체로 이직하여 L사에서 개발한 디자인을 활용하지 않도록 교육

사례 2.

M사 관계자가 제품 전시회에 참석했다가 자사의 것과 거의 흡사한 기계를 발견하고 이를 수상히 여겨 확인한 결과, 지난 전시회 때 M사 제품을 눈여겨보았던 경쟁업체에서 M사 핵심연구원인 A를 스카우트하여 유사한 제품을 생산·유통시켰다는 정황을 포착

A는 M사에서 오랫동안 가족처럼 함께 지내던 직원으로, 전시회 개최를 4개월 정도 앞둔 당시 갑자기 개인 사정이 생겼다면서 회사를 사직함

○ 기업유형 : 기계소재

○ 유출대상 : 회사의 핵심기술인 ○○ Machine

○ 유출배경

- M사는 평소에 독자적인 기술개발에 많은 투자를 하고, 국내외 주요 전시회에 활발히 참가하면서 많은 경쟁업체의 타겟이 되었음
- 직원에 대한 믿음이 커서 입·퇴사시 서약서 징구 등 어떤 조치도 취하지 않음

○ 피해규모 : 약 10억원 + α

○ 유출인지 : 전시회에 참가한 회사관계자가 우연히 발견

○ 조치사항

- 변호사를 고용하여 소송을 진행하였으며, 증거 입증문제와 시간·비용상의 이유로 경쟁업체와 1억 5천만원에 합의하면서 사건 종료
- 유출사건 이후 직원들 입·퇴사시 서약서를 징구하고, 모든 기술개발 건에 대해 특허 출원 추진

사례 3.

영상처리기술을 기반으로 자동차, 반도체, 전자산업 등 다양한 분야에 적합한 ○○ 시스템을 개발·공급하는 S사는 국내 한 전시회에 출품한 샘플이 에이전시를 통해 유출되는 사건이 발생함

샘플을 획득한 산업스파이는 제품을 분해하여 사진을 찍고 도면을 그린 뒤 경쟁업체로 정보를 넘김

○ 기업유형 : 전기전자

○ 유출대상 : S사의 기술적 노하우가 담긴 ○○ 시스템 샘플(완제품)

○ 피해규모 : 약 5억원

○ 유출인지 : 전시회가 끝난 뒤 얼마 후 경쟁업체에서 자사와 거의 유사한 제품을 출시

○ 조치사항 : 에이전시 회사와 담당자를 상대로 소송 진행 중

사례 4.

주차장 내 자동승강기 로봇을 개발하는 N사의 생산 공장에 정체를 알 수 없는 사람들이 무단으로 침입하여 로봇 사진을 찍고 달아남

이 사실을 알게 된 N사는 수소문 끝에 유출된 승강기 로봇 사진을 회수하였으나, 이미 설계도면이 경쟁업체로 넘어간 후였음

경쟁업체는 세부 설비구조만 조금씩 변형시키는 방법으로 관련 처벌규정을 피해가면서 유사제품을 제작·판매함

○ 기업유형 : 건설엔지니어링

○ 유출대상 : 자체 브랜드까지 가지고 있었던 주차장 자동승강기 로봇 모델로, 특허취득 준비 중이었던 핵심기술

○ 유출배경

- 새로운 기술개발 소식이 들리면 동종 기업들이 서로 카피하는 행태가 만연되어 있음
- 공장에 시건장치를 설치하였으나 무용지물이었음

○ 피해규모 : 약 5억원

○ 유출인지 : 관련 전문업체가 국내에 많지 않아서 자연스럽게 인지 가능

○ 조치사항

- 유출된 기술에 대한 특허 취득 포기
- 이후 개발한 신모델에 대한 관리를 더욱 엄격히 함

□ 기타

사례 1.

> 도로, 항만, 철도, 교량 등 사회간접자본(SOC) 관련 토목업무를 담당하고 있는 T사는 어느 날 갑자기 대표가 회사를 넘기고 사라지면서 혼란에 빠졌으며, 신임 경영진과 노조 간의 갈등으로 오랜 기간 동안 쟁의행위가 발생함
>
> 이러한 경영혼란을 틈타 연구개발인력 다수가 경쟁업체로 이직하고, 회사의 주요 기밀들이 유출됨

○ 기업유형 : 건설엔지니어링

○ 유출대상 : 핵심연구인력, 영업망, 핵심기술 등을 망라한 회사의 주요 기밀정보 일체

○ 유출배경 : 회사의 인수합병에 대한 직원들의 거부감과 신임 경영진과 직원들 간의 대화부족으로 장기간 노사분규가 발생하여, 핵심인력과 기밀정보에 대한 관리가 제대로 이루어지지 않음

○ 피해규모 : 약 50억원

- 영업정보 유출로 인해 매출액이 지속적으로 감소함
- 현재 회사는 기존에 진행하고 있었던 프로젝트로 운영되고 있으며, 신규계약체결은 거의 이루어지지 못하고 있는 상황
- 책임급의 핵심 연구인력 다수가 경쟁업체로 이직하면서 기술경쟁력이 약화됨

○ 유출인지 : 인력의 전직 등을 통해 자연스럽게 인지

○ 조치사항

- 최근 노사분규가 종료되었으나, 쟁의행위 기간 중에는 인력이나 정보관리에 전혀 신경을 쓰지 못함
- 분규 해결 이후 연구개발 인력을 보강하고, 퇴사한 직원들에 대한 복귀를 설득하고 있으며, 일부는 재입사함

사례 2.

소방자동화기기 생산업체인 K사의 ○○ 제품 시연회에 참관한 산업스파이가 시연 과정을 캠코더로 찍어 동영상을 인터넷에 유포시킴

이 때문에 K사의 기술이 경쟁업체에 고스란히 노출되었고, 경쟁업체에서는 제품의 단점과 실험 과정상의 문제점 등을 공개적으로 지적하고 나섬

또한 기존 고객사들과 앞으로 계약체결을 앞둔 신규 거래업체들로부터 문의전화와 항의전화가 쇄도함

○ 기업유형 : 기계소재

○ 유출대상 : 개발 완료 단계에 있었던 ○○ 시스템

○ 유출배경 : 제품 시연회에는 자문 등을 목적으로 외부인들이 참관하게 되는 경우가 많은데, 이들에 대한 보안검색이 전혀 이루어지지 않음

○ 피해규모

- 제품에 대한 신뢰도가 떨어지고 기업 이미지가 크게 실추되어 제품 수주에 어려움을 겪음
- 이미 계약이 성사된 경우에도 확인 차원에서 시연회 실시를 다시 요구하는 경우가 발생함

○ 유출인지 : 관련업계 종사자가 인터넷에서 동영상을 보고 알려줌

○ 조치사항 : 외부사람이 회사를 방문할 경우 방명록을 작성하도록 하고, 각종 전자제품 사용을 제한함

나. 유출 산업기밀

□ 연구개발기술 및 결과

사례 1.

> 반도체나 각종 첨단 디지털 기기에 활용되는 레이저 장비를 생산하는 A사의 창업 멤버 중 한 사람이었던 B는 임원진과의 불화가 심해지자 퇴사를 결심하고 동일업종의 회사를 창업함
>
> 이후 B는 A사의 각 파트별 핵심 연구원을 한두명씩 스카우트해가는 방법으로 7명의 연구원을 자신의 회사로 데려가, E사의 핵심기술이자 원천기술인 레이저 마킹 기술을 활용하여 제품을 생산함

○ 기업유형 : 기계소재

○ 유출대상 : 회사 창업 당시의 원천기술

○ 유출배경 : 회사 대표이사와 연구소장 간의 불협화음이 오랫동안 계속되었고, 이에 불만을 품은 연구소장이 퇴사하면서 동료 연구원들을 스카우트함

○ 피해규모 : 회사 창업의 근간이었던 기술이 유출되어 초기 회사가 안정화되는데 큰 타격이 되었음

○ 유출인지 : 회사 관계자가 고객사에 제품을 납품하러 갔다가 우연히 타회사의 제품견적서를 발견하면서 핵심기술 유출사실을 인지

○ 조치사항

- 유출사실 확인 후 뒤늦게 특허출원을 추진했으나, 상대방 업체에서 이미 공개된 기술이라고 주장하면서 반박함. 이러한 과정이 반복되면서 출원된 특허 중 반려된 건수가 절반이 넘음
- 사건 후 모든 개발기술에 대한 특허출원을 추진함
- 경쟁업체 취업금지, 보안유지각서, 비밀유지각서 등 보안관련 서약서를 징구함
- 회사 내부에 DRM(Digital Rights Management), CCTV, 카드키 등 보안시스템 구축

사례 2.

구조물 안전진단 관련 기술을 개발하는 B사의 부설연구소에서는 얼마전 ○○ 계측시스템 개발에 성공함

그러나 기술개발 후 실용화에 이르기까지 준비기간이 점점 길어지자 인사와 영업을 담당하고 있던 A와 B가 연구개발 관련 정보를 가지고 경쟁업체로 이직하는 사건이 발생함

경쟁업체에서는 그동안 B사가 공들여 개발한 계측시스템 정보를 손쉽게 획득할 수 있었으며, B사보다 먼저 특허 출원 및 등록을 시도함

○ 기업유형 : 건설엔지니어링

○ 유출대상 : ○○ 계측관리 시스템

○ 유출배경 : CEO와 연구개발자 사이에 연구개발 종료시점과 상용화시점에 대한 심각한 갈등이 있었으며, 그 사이 인사담당 임원과 영업담당 임원이 연구개발 관련 정보를 취득함

○ 피해규모 : 향후 5년간 약 50억원 정도의 손실 예상

○ 유출인지 : 좁은 경쟁시장으로 쉽게 인지

○ 조치사항

- 별도의 조치를 취하지 못함
- 연구소 인원이 아닌 관리직 종사자가 경쟁업체로 이직한 경우, 실질적인 기술보유자가 아니기 때문에 절취 사실을 입증하지 못하는 한 소송제기가 불가능

사례 3.

C사의 부설연구소에서 유전자 진단 기기 및 치료제를 개발하던 연구원 5명이 집단으로 회사를 그만둔 뒤, 회사를 창업함

이들은 각 분야별 전문연구원들로 구성되어 있었고, C사에서 지난 2년간에 걸쳐 개발한 유전자 분석 장비 기술을 이용하여 유사제품을 생산, C사보다 먼저 제품 판매에 나섬

○ 기업유형 : 화학섬유

○ 유출대상 : 유전자 분석장비 관련 기술

○ 유출배경 : 사내 볼링동호회 회원이었던 5명의 연구원이 의기투합하여 새로운 회사를 창업함

○ 피해규모 : 약 8억원

○ 유출인지 : 시장 조사를 하다가 인지

○ 조치사항

- 법원에 소송을 제기했으며, 1심에서 승소하고 현재 2심 계류중
- 경쟁업체 취업금지 서약 구체화 등 퇴직자에 대한 관리감독 강화 및 사내 동호회에 대한 지원 폐지

사례 4.

S사에서 주요 연구과제를 담당하던 연구원 A는 토목방수 관련 기술과 노하우를 가지고 동종업계로 이직함

A가 가지고 나간 기술은 S사의 핵심 기술은 아니었으나 2년여에 걸친 연구개발 끝에 제품생산 준비 중에 있는 것이었음

동종업계 회사인 B사로 이직한 A는 가지고 나간 기술의 내용을 일부 변경하여 신기술 인증까지 받고 상품화하였으며, 지금까지도 계속 활용 중에 있음

○ 기업유형 : 기계소재

○ 유출대상 : 토목방수기술

○ 유출배경 : 유출기술의 연구담당자였던 A는 본인의 연구가 회사 핵심기술로 인정받지 못하고, 제품생산 일정이 계속해서 미루어지는 것에 대해 오랫동안 불만을 품고 있었음

○ 피해규모 : 피해규모의 정확한 산정은 불가능하나, 유출자의 소속 회사인 B사가 먼저 신기술 인증을 받음으로써 S사가 제품을 생산하는데 차질을 빚음

○ 유출인지 : 제품생산을 앞둔 시점에서 경쟁회사에서 먼저 신기술 인증을 받고 제품을 상용화했다는 소식을 듣고 인지

○ 조치사항 : '한솥밥 먹던 식구'라는 인식 때문에 법적 대응을 하지 않음

□ 산업재산권

사례 1.

제조업의 방수(Water-Proof)제지 기술을 건축자재에 적용시킨 ○○ 기술을 새롭게 개발하여 특허출원에 성공한 D사는 협력업체였던 하청제조사에 제품 생산을 맡기고 기다리고 있던 중 시장에 D사의 것과 유사한 제품이 유통되고 있다는 사실을 알게 됨

이를 수상히 여긴 D사는 상황파악에 나섰고, 하청업체 사장이 D사의 경쟁업체와 모의하여 신제품 관련 기술을 경쟁업체에 넘기고 유사한 제품을 만들어 유통시킨 사실을 확인함

○ 기업유형 : 건설엔지니어링

○ 유출대상 : 회사 핵심기술

○ 유출배경 : D사의 제품을 생산하던 협력하청업체에서는 평소 D사 이외에도 여러 경쟁회사들의 제품을 함께 취급했기 때문에 각 회사별로 기술정보를 파악하는 것이 용이했음

○ 피해규모 : 약 10억원

○ 유출인지 : 시장에 유사제품이 유통되고 있는 사실을 확인함으로써 인지

○ 조치사항

- 변호사를 선임하여 소송을 준비했으나 구체적인 증거가 부족하여 상대방을 처벌하지는 못하고, 공문을 보내 경고하는 차원에서 사건을 마무리함
- 상대방보다 한 발 앞서 계약을 체결하고, 가격경쟁에서 우위를 점하는 방식 등을 이용하여 자체적으로 피해를 줄이려 노력함

사례 2.

고객사를 통해 우연히 회사 제품과 유사한 제품이 시장에서 판매되고 있다는 소식을 접한 E사는 얼마 전까지 E사에서 기술개발 담당자로 근무했던 A가 회사의 특허 기술을 이용하여 경쟁업체에서 유사한 제품을 개발하여 판매하고 있다는 사실을 알게 됨

A는 과거 E사의 주요 기술을 모두 꿰뚫고 있었던 핵심인력이었으며, 이미 특허 등록되어 있는 E사의 기술 일부를 교묘하게 수정하여 이용하고 있었음

○ 기업유형 : 정보통신

○ 유출대상 : 회사의 독점적인 특허기술인 네트워크 트래픽 관리 솔루션

○ 피해규모 : 기술유출에 의한 직접적인 피해는 그다지 크지 않았지만 시장이 작기 때문에 거래처를 뺏기면서 발생한 영업활동에서의 애로가 더 큰 문제로 작용함

○ 유출인지 : 영업사원이 고객사로부터 타사에서 유사한 제품을 판매하고 있다는 정보를 입수함

○ 조치사항

- 사실을 확인하자마자 바로 소송절차에 돌입했으며, 현재 소송 진행 중
- 퇴직사원을 대상으로 한 소송이 이제는 기업간 소송으로 확대됨

사례 3.

로그분석 솔루션 전문 개발업체인 F사가 보유한 특허기술을 외국계 경쟁업체가 무단으로 사용하면서 F사와 외국계 경쟁업체 간의 특허분쟁사건이 발생함

○ 기업유형 : 정보통신

○ 유출대상 : 로그분석 솔루션 관련 특허기술

○ 유출배경 : 2007년부터 시행된 전자금융거래법의 영향으로 금융권과 공공기관들이 보안강화에 나섰으며, 이로 인해 보안로그분석 솔루션에 대한 수요가 크게 늘어남

○ 피해규모 : 약 10억원

○ 유출인지 : 거래업체를 통해 인지

○ 조치사항

- 소송을 제기하고 판결이 나기까지 약 1년이 소요됨
- 재판 결과 특허의 소유권이 F사에 있음이 입증되었고, 경쟁기업과 유상사용허가 계약을 체결하면서 사건이 마무리됨

□ 생산제조기술

사례 1.

금속재료 제조업체인 G사에 원재료를 납품하는 협력업체 직원이 회사의 현장을 보고 제조기술의 노하우를 파악하여, 경쟁업체에 정보를 제공함

○ 기업유형 : 기계소재

○ 유출대상 : 구리 및 구리합금재료 제조기술

○ 유출배경

- 생산제조 현장에 회사 외부 사람이 출입하는 것에 대해 아무런 제한이 없었음
- 동종 업계에서는 20여개의 업체가 경쟁 중에 있으며, 선두업체 1~2개사를 제외한 나머지 업체들 사이에서는 경쟁이 매우 심한 상황이었음

○ 피해규모 : 매출액 20% 감소

○ 유출인지 : 6개월 후 동종업계 사람을 통해 알게 됨

○ 조치사항

- 회사 외부로 노하우가 유출되었다는 사실을 바로 알아차리지 못해서 즉각적인 대응을 할 수 없었음
- 사건발생 이후 자재납품 창고를 별도로 마련하여 납품업체 직원이 현장에 출입하지 못하도록 조치함

사례 2.

금속재료 표면처리제 약품 제조업체인 H사의 기술책임자 A가 퇴사하면서 그가 개발했던 제조기술 전체를 가지고 경쟁업체로 이직함. 뒤이어 개발에 참여했던 다른 연구원 3명도 퇴사한 뒤 기술책임자를 따라 경쟁업체로 이직

○ 기업유형 : 화학섬유

○ 유출대상 : 약품 제조기술

○ 유출배경 : 퇴직 직원들은 회사 기숙사에서 함께 거주하는 친분관계가 두터운 사이였음

○ 피해규모 : 약 15억원

○ 유출인지 : 평소 친분이 있던 내부 직원을 통해 인지

○ 조치사항

- 경쟁업체와 이직당사자를 대상으로 소송을 제기
- 재판진행 과정에서 경쟁업체가 제품의 국내 판매를 중단하고 손해배상을 약속하여 고소를 취하함
- 경쟁업체에서는 이직 당사자들에 대해서 퇴사 조치함

사례 3.

전기부품 제조업체인 I사에서 개발자로 근무하던 직원이 퇴직하면서 지그(Jig) 관련 기술을 경쟁업체로 빼돌려 실제 생산라인에 적용시킴

※ 지그(Jig) : 기계의 부품을 가공할 때에 그 부품을 일정한 자리에 고정하여 칼날이 닿을 위치에 쉽고 정확하게 정하는 데에 쓰는 보조용 기구

○ 기업유형 : 전기전자

○ 유출대상 : 온도센서용 반도체소자 제조기술

○ 유출배경 : 국내 소자업체들은 일본으로부터 핵심기술을 도입하여 사용하다가 최근 들어 독자기술을 확보하기에 이르렀으며, 동종업체간 경쟁이 심함

○ 피해규모 : 약 3억원

○ 유출인지 : 유출자와 함께 근무하던 연구원이 그의 행동을 수상히 여기고 동향을 파악하면서 인지

○ 조치사항

- 혐의사실을 입증할 증거가 부족하여 회사 차원에서 별도의 조치를 취하지 못함
- 향후 모든 연구성과에 대해서는 법적보호를 위해 권리화 추진

□ 영업비밀 또는 노하우

사례 1.

> A사의 연구소에서 국책과제를 준비 중이었던 연구원 B, C가 한 달 간격으로 회사를 그만두고, 얼마 후 팀장 D까지도 개인 신상문제를 이유로 퇴사함
>
> 몇 개월 뒤 국책과제 입찰을 위해 사업제안서를 발표하는 장소에서 퇴사한 B, C, D가 경쟁업체 대표로 나와 A사의 콘텐츠를 가지고 프레젠테이션을 하고 있는 것을 목격함

○ 기업유형 : 정보통신

○ 유출대상 : A사가 준비 중이던 온라인 교육콘텐츠 사업 기술제안서, 노하우, 관련 DB 등 영업비밀 일체

○ 유출배경 : 업계 전반적으로 새로운 아이디어와 노하우가 거의 고갈된 상태여서 새로운 콘텐츠 개발이 절실한 상황임

○ 피해규모 : 약 10억원 규모의 국책과제 입찰에서 탈락하고 사업권은 경쟁업체로 넘어감

- 경쟁업체는 유출기업의 콘텐츠뿐만 아니라 기술제안서, 인적네트워크 등을 이용하여 다수의 유사계약을 체결함

○ 유출인지 : 사업제안서 발표 장소에서 마주침

○ 조치사항

- 과제관리 기관에 항의해 보았으나 별 소득이 없었음
- 혐의에 대한 입증사유가 부족하여 특별한 대응을 하지 못함

사례 2.

B사에 근무하던 연구원 A는 본인이 관심 있는 연구를 더 해보고 싶다면서 회사를 퇴직하고 개인회사를 설립. 그러나 얼마 후 A는 동료 연구원이었던 C를 스카우트해가고, B사에서 함께 연구하던 내용을 바탕으로 제품을 개발·출시, B사의 일부 거래업체들과 계약을 맺음

○ 기업유형 : 화학섬유

○ 유출대상 : 기능성 화장품 원료 제조법

○ 피해규모 : 약 5,000만원

○ 유출인지 : A가 퇴사한 후 6개월쯤 지났을 때 B사 관계자가 거래처를 방문하여 우연히 소식을 접함

○ 조치사항

- A에게 경고차원에서 내용증명 우편을 보내 위법사항을 인식시킴
- 내용증명을 받은 상대방 측에서 서로간의 영업범위를 잘 조정하여 이후 큰 마찰이 빚어지는 것을 방지
- A가 설립한 회사는 급속히 성장하여 현재 B사의 경쟁업체로 발전함

사례 3.

안테나 모듈 제조업체인 J사에서 영업사원으로 근무하던 A는 기술개발을 담당하는 4명의 동료직원들을 포섭하여 핵심기술과 함께 본인이 가지고 있던 고객정보를 CD로 미리 구워 놓은 후 경쟁업체로 이직함
경쟁업체는 현재 J사와 거의 유사한 제품을 제작하여 판매하고 있음

○ 기업유형 : 전기전자

○ 유출대상 : 안테나 모듈 설계·생산기술 및 관리고객 명단

○ 피해규모 : 약 10억원 정도로 피해규모를 추정하고 있으나, 경쟁업체가 대규모 생산체제를 갖추고 영업에서 우위를 점하면서 앞으로 피해금액이 더 늘어날 것으로 예상됨

○ 유출인지 : J사와 경쟁업체에 동시에 부품을 납품하고 있는 협력업체 직원으로부터 퇴직사원들이 경쟁업체에서 근무하고 있다는 사실을 듣고 인지

○ 조치사항

- 법적대응을 검토하였으나 증거불충분으로 포기함
- 기존 거래업체에 상기 사실을 통보
- 지식관리시스템(Knowledge Management System)을 구축, 기존의 암묵지를 형식지로 전환하도록 하고, 이에 대해 인센티브 부여

제2절 해외진출 중소기업

1. 기술유출 현황

○ 다음은 한국산업기술진흥협회에서 2007년 4월 24일부터 4월 27일까지 중국, 베트남에 진출한 국내 중소기업 20개사를 대상으로 실시한 「해외진출 기업의 산업기밀관리 실태조사」결과를 분석, 정리한 것임

가. 산업기밀 유출현황

○ 해외에 진출한 국내 중소기업을 대상으로 조사한 결과 20개 응답기업 중 5개사(25.0%)가 최근 3년간 보유기술 및 정보가 외부로 유출되어 어려움을 겪은 적이 있다고 응답함

○ 유출시 처리방법은 대처가 곤란하여 포기한다는 응답이 3개사(60.0%)로 가장 높았으며, 민·형사상 법적대응 1개사(20.0%), 특별한 조치를 취하지 않았다는 응답이 1개사(20.0%) 등의 순으로 나타남

나. 산업기밀 관리현황

○ 현지 국가에서의 보유기술 및 정보의 유출정도는 과거에 비해 매우 증가했다는 응답과 다소 증가했다는 응답이 각각 8개사(40.0%)로 나타났으나, 과거와 비슷하다는 응답은 4개사(20.0%)에 불과하고 감소했다는 응답은 없는 것으로 나타남

○ 보유기술 및 정보관리에 대해 대내외적으로 느끼는 위협의 정도는 매우 심하다는 응답과 다소 심하다는 응답이 각각 6개사(30.0%)로 높게 나타났으며, 보통이라는 응답은 5개사(25.0%), 위협이 없다는 응답은 3개사(15.0%)에 불과했음

○ 한편, 현지 당국의 기술보호 노력에 대해서는 불만스럽다는 응답이 9개사(45.0%)로 나타났으며, 보유기술 및 정보 관리에 대해 대내외적으로 느끼는 위협에 대해 12개사(60.0%)가 심하다고 응답함

2. 기술유출 사례

○ 다음은 중소기업청과 한국산업기술진흥협회에서 2007년 7월 5일부터 7월 27일까지 해외 진출 중소기업 중 산업기밀유출 피해경험이 있는 기업을 대상으로 실시한 방문조사 결과를 분석, 정리한 것임

가. 유출관계자

□ 현지채용 인력

사례 1.

> 보안 카메라 전문 생산업체인 A사는 중국 심천에 현지 법인을 설립한 뒤 제조업체를 선정하여 제품생산에 착수함
> 하지만 제품이 생산·판매되고 있던 도중 현지에서 고용한 현지 생산직 직원이 A사의 제품 회로도를 몰래 절취하여 도주하는 사건이 발생함
> 유출자는 제품 도면을 가지고 다른 도시로 이동, 그곳에서 유사한 물건을 제조·판매하여 막대한 이익을 챙김

○ 기업유형 : 전기전자

○ 유출대상 : 제품 회로도

○ 유출배경

- A사는 관련 분야에서 국내 최고의 기술력을 보유한 중소기업으로 최근 중국에 현지 법인을 설립함
- 중국 현지에서 제조업체를 선정하여 제품생산을 준비하고 있었으며, 이를 위해 필요한 완제품 샘플 및 주요 기술도면 등이 중국 현지에 넘어가 있는 상황이었음

○ 피해규모 : 유출자가 제품가격을 지나치게 낮게 책정하여 유통시킴으로써 전체 제품가격이 하락하였으며, 불법복제 제품의 불량률이 높아 기업과 제품의 이미지가 손상됨

○ 유출인지

- 유출자가 제품을 상용화하기 전까지는 유출사건이 있었는지 전혀 파악하지 못함
- 고객사에서 A사 제품과 매우 유사한 제품이 시장에 새롭게 출시되었다고 먼저 제보해 주어서 인지

○ 조치사항

- 유출사건에 대한 사전확인 작업과 동시에 중국 공안에 신고하여 협조를 요청한 뒤 유출자를 추적함
- 유출자 체포 후 사건 종료

사례 2.

세계적인 가발 제조업체인 B사는 노동집약적인 가발산업의 특성상 10여년 전부터 중국과 인도네시아에 생산기지를 마련하여 제품을 생산하고 있었는데, 갑자기 중국 공장의 매출과 시장점유율이 감소하면서 경영위기에 처하는 상황이 발생함

원인을 조사한 결과 중국 공장에서 일하던 핵심 기술자가 중국경쟁업체로 이직하여 유사 제품을 만들어 해외 바이어들에게 낮은 가격으로 판매, 시장을 차츰차츰 잠식해 가고 있었던 것으로 확인됨

○ 기업유형 : 화학섬유

○ 유출대상 : 세계적 수준의 가발제조 기술

○ 피해규모 : 정확한 피해규모를 확인할 수는 없으나, 대응이 늦었을 경우 도산 위기에 처했을 수도 있었음

○ 유출인지 : 매출액과 시장점유율이 급감하여 자체 조사에 나선 끝에 인지

○ 조치사항

- 긴급자금 3억원을 투입해 본사 파견인력이 주요 기술을 통제하고, 핵심제품 일부를 본사에서 직접 생산·조달하는 방식으로 생산라인을 개편
- 현지근로자와 기밀유지계약서를 작성하고, 근로자뿐만 아니라 외부 방문객에게도 개별 ID를 부여하여 출입구역을 지날 때마다 기록이 남도록 함

사례 3.

> 전자제품 부속품 생산업체인 M사의 중국 현지 공장 책임자로 지내던 A는 자신이 승진하지 못할 것을 대비하여 휴대전화 진동모터 관련 설계도면 수십장을 자신의 아파트로 빼돌려 놓았으나, 이 같은 사실이 곧 회사 임원진에 의해 적발되어 회사로부터 강제 퇴직조치 당함
>
> 이에 앙심을 품은 A는 자신과 함께 일했던 중국인 기술자 B를 통해 새로 개발 중인 스테핑 모터 설계도면을 넘겨받고 M사의 경쟁업체인 중국의 N사에 접근, 모터 설계도를 제공하는 대가로 이익의 20%를 받기로 함
>
> 뿐만 아니라 A는 M사의 것과 유사한 스테핑 모터를 자체 제작하여, N사의 한국 책임자인 C를 통해 국내 전자업체에 판매를 시도함

○ 기업유형 : 전기전자

○ 유출대상 : 스테핑 모터 제작기술

○ 피해규모 : 직접적인 피해금액은 크지 않지만, 유출되었을 경우 향후 5년간 400억원 가량의 피해가 있었을 것으로 예상됨

○ 유출인지 : 정보기관이 관련 정보를 입수하여 M사에 알려줌

○ 조치사항

- 관련자 고소고발
- 부정경쟁방지 및 영업비밀보호에 관한 법률위반으로 A를 구속기소하고, C를 불구속기소함

□ 협력업체 종사자

사례 1.

> ○○ 검사 측정기를 개발하는 H사는 얼마 전 중국 청도에 진출하였으나 파트너가 관련 기술을 몰래 빼내 같은 업종의 회사를 설립, 거래선을 모두 빼앗겨 결국 공장 문을 닫고 한국으로 철수함

○ 기업유형 : 전기전자

○ 유출대상 : ○○ 검사 측정기 관련 응용 프로그램

○ 유출배경

- 중국 기업이나 관리들은 투자만 하면 모든 것을 해 줄 것처럼 호의를 보이다가도 일단 투자를 시작하고 나면 본색을 드러내는 경우가 많음
- 파트너에 대한 다각적이고도 장기적인 신용조사가 부족했고 치밀한 계약 체결이 이루어지지 못했음

○ 피해규모 : 파트너사는 H사보다 비교우위에 있는 현지 인맥과 정보력을 바탕으로 영업망을 장악하였고, H사는 매출이 급감하여 회사 존립 위기에 처함

○ 유출인지 : 기존 거래처의 담당자를 통해 인지

○ 조치사항 : H사의 협력업체는 탄탄한 자본력을 바탕으로 청도 인근 지역을 이끌어 가는 중견기업으로 지역사회에 미치는 영향력이 강해, H사는 이러한 기업을 대상으로 아무런 법적 대응을 취하지 못한 채 결국 공장을 폐쇄하고 한국으로 철수함

사례 2.

상하이 인근 창저우에 투자한 기계관련 업체인 S사는 S사가 지분 75%를, 중국의 파트너사가 나머지 25%를 현물(토지)로 투자하는 방식으로 합작계약을 맺음

그런데 중국 업체는 계약서의 '이후 토지를 평가해 자본금 이상 나오면 현금으로 보상한다'라는 조항을 빌미로 토지 자산평가를 다시 받아 자본금보다 1억 위안(약 1백 50억원) 이상 많이 나왔다며 보상을 요구함

○ 기업유형 : 기계소재

○ 유출대상 : 중국 업체가 S사의 핵심기술이나 노하우를 노렸다기 보다는 중국현지 실정을 잘 모르는 S사를 사기 대상으로 삼고 의도적으로 접근함

○ 피해규모 : 합작회사를 설립하기 전에 사건이 발생하여 중국 진출이 완전 무산됨

○ 조치사항 : S사의 대표가 중국업체의 땅값을 미리 알고 문제의 소지가 될 만한 조항을 일부러 계약서에 포함한 것이라고 생각했지만, 특별한 조치를 취할 길이 없었음

□ 경쟁업체 종사자

사례 1.

각종 장갑을 생산, 판매, 수출하고 있는 M사의 상해 생산 공장에 경쟁업체 사람으로 추정되는 중국인이 불량품을 모아 놓는 창고에 몰래 잠입함. 창고에는 품질심사에서 탈락한 폐기 직전의 제품들이 쌓여 있었고, 침입자는 이를 뒤지고 있다가 M사의 건물 관리인에게 목격되어 붙잡힘

○ 기업유형 : 화학섬유

○ 유출대상 : 환경친화성 산업용 보호장갑 제조기술

○ 피해규모 : 품질검사 단계에서 탈락한 제품이라 하더라도 기능상의 문제라기보다는 규격이 맞지 않거나 바느질 불량에 따른 것이 대부분이기 때문에 제품이 외부로 유출되었을 경우 M사가 입었을 타격이 매우 컸을 것으로 예상됨

○ 유출인지 : 건물관리인이 침입자를 발견

○ 조치사항

- 침입자에게 사실을 추궁하였으나 끝까지 부인하여 별도로 신고는 하지 않고 구두로 강하게 주의를 주는 선에서 그침
- 불량품 저장창고 및 폐기장 근처에 CCTV를 설치하여 관리감독을 강화하고, 외부인이 함부로 사내에 출입할 수 없도록 철저히 통제함

사례 2.

포토프린터 엔진과 전용 카트리지를 개발·판매하고 있는 P사는 자사가 발명특허권을 가지고 있는 제품과 유사한 모델이 중국 절강성(浙江省)의 한

공장에서 제조되어 동남아 지역으로 대량 수출되고 있는 사실을 알게 됨
P사가 증거확보를 위해 제품을 구입하여 살펴본 결과 경쟁사의 제품이 P사의 특허기술을 침해하고 있는 것으로 판명되었고, 이를 증거로 하여 유사품이 수출·판매되고 있던 동남아 각 국에 중국 경쟁회사를 제소함

○ 기업유형 : 전기전자

○ 유출대상 : 포토프린터 전용 카트리지 개발 관련 특허

○ 피해규모 : 약 50억원

○ 유출인지 : 유사제품 직접 구입 후 확인

○ 조치사항

- 경쟁업체 제품을 구입하여 특허권 침해 여부를 확인한 뒤 곧바로 경쟁사를 제소하였으며, 재판에서 승소하여 경쟁업체의 제품의 동남아 판매가 금지됨
- 사건발생 이후 P사는 한국과 중국에서 뿐만 아니라 제3국에서의 특허 출원에 대해서도 관심을 갖기 시작하고, 기 취득한 지적재산권에 대한 관리, 감독체계도 강화함

사례 3.

전자제품 등에 사용되는 발포제를 제조하는 K사는 2년간의 노력 끝에 신제품 개발에 성공하고, 중국 저장성에 위치한 공장에서 본격적인 생산에 돌입함
비슷한 시기, 중국 J사는 K사의 중국 지사장인 A에게 접근, J사의 회사 지분과 부사장직을 보장하는 조건으로 K사의 신제품 제조기술과 유통관리 등에 대한 영업비밀을 가지고 나올 것을 제안하였으며, A는 K사의 해외영업담당인 B와 C까지 매수하여 관련 정보를 J사에 넘김

○ 기업유형 : 화학섬유

○ 유출대상 : 전자제품 등에 사용되는 발포제 제조기술 및 유통관리 프로그램 등 K사가 2년여에 걸쳐 수십억원을 투자하여 개발한 기술

○ 유출배경 : 최근 중국으로 진출하는 국내 기업들이 늘어나면서 현지에서 지사나 공장을 관리·감독하는 한국인 책임자가 중국기업들로부터 기술유출의 대가로 금전적 유혹을 받는 경우가 많아짐

○ 피해규모 : 유출되었을 경우 해외 거래처와 판매 단가 등이 공개되면서 연간 약 100억원의 피해를 입었을 것으로 추정됨

○ 유출인지 : 국내 정보기관의 수사 결과

○ 조치사항 : 관련 기술이 J사에 넘어가기 전 경찰이 지사장 A 등 관련자 3명을 불구속 입건하고, 이들로부터 기술을 매입한 중국 J사 대표에 대해서는 중국 공안의 협조를 얻어 수배령을 내림

나. 상표도용 및 무단복제

사례 1.

콘덴서 생산업체인 T사는 중국 현지에서 생산한 제품에 대해 바이어가 물량을 뚜렷한 이유 없이 계속해서 줄이자, 이를 이상히 여기고 자체 조사를 실시함

조사 결과, 바이어가 T사 몰래 중국 내에서 직접 모조품을 제조해 중국 내수시장에 정품과 섞어 유통시키고 있는 사실을 포착함

○ 기업유형 : 전기전자

○ 유출대상 : 콘덴서 제조기술

○ 유출배경

- 일명 '짝퉁'으로 불리는 중국산 모조품은 한국산 제품 전반에 대한 이미지를 실추시키는 주범이지만, 중국정부가 단속에 소극적이며 처벌 강도도 약해 한국의 많은 중국진출 기업들이 고전하고 있음
- 모조품의 경우 최종품을 완전 조립한 후에도 상표나 라벨을 부착하기 전까지는 처벌이 사실상 불가능하며, 중국 업체에서는 이를 악용하여 마지막 작업단계인 상표 및 라벨 부착은 비밀리에 재빨리 진행하는 방식을 이용하고 있음

○ 피해규모 : 저질의 모조품에 대한 반품 및 교환 신청이 급증하고 소비자들로부터 항의가 쇄도하여 이를 해결하는 과정에서 약 20억원의 피해를 입었으며, 무엇보다도 기업 이미지가 많이 손상됨

○ 유출인지 : 거래물량이 점점 줄어들어 이를 수상히 여기고 자체 조사에 나선 끝에 인지

○ 조치사항 : 중국 바이어에 대한 소송을 제기했으며, 현재 소송 진행 중

사례 2.

K사는 핸드폰용 부품을 제조·납품하는 회사로 중국 심천에 새로 생산공장을 건립하고 제품을 생산하던 중, 중국의 한 단속업체로부터 중국의 전자제품회사인 H사가 인근지역에서 K사 부품의 모조품을 대량생산하여 유통시키려 하고 있다는 정보를 입수함

그러나 부품 견본품을 단속업체에 보내고 사실 확인 절차를 걸치는 사이 모조품은 모두 판매되었고, K사와 단속업체는 H사가 모조품 생산을 다시 시도할 것이라 예상하고 이를 예의주시함

○ 기업유형 : 전기전자

○ 유출대상 : 핸드폰에 내장되는 각종 부품

○ 피해규모 : 약 50억원

○ 유출인지 : 중국의 한 단속업체가 K사 부품의 모조품이 중국에서 다량으로 생산되고 있음을 알려줌

○ 조치사항

- 불법으로 모조품이 생산되고 있다는 사실을 인지하자마자 중국 단속팀과 함께 감시를 시작함
- 광동성에 H사의 또 다른 판매점과 제품창고가 있다는 사실을 알게 된 K사가 감독당국에 기습단속을 요청하여 중국 단속팀이 3,600여개의 모조품을 몰수, 폐기 처분함

제3절 해외 기업

1. 기술유출 현황

<국가별 주요 현황>

○ **미국산업보안협회(American Society for Industrial Security, ASIS)**

- 미국 내 산업스파이로 인한 피해액이 연간 약 2,500억 달러(2001년)로 미국 전체 연구비를 능가하는 것으로 추정
- 이는 피해업체당 평균 30~50만 달러에 해당

○ **미국 대통령 직속 과학기술위원회**

- 외국의 산업스파이에 의한 미국 내 피해규모가 1,000억 달러에 육박하는 것으로 나타남(2004년)

○ **미국 국무부**

- 브라질, 중국, 파키스탄, 말레이시아, 파나마와 아프리카 국가들을 미국의 주요 지적재산권 침해 국가들로 발표(2004년)
  - 남반구를 통틀어 브라질에서의 미국 지적재산권 침해 피해액이 약 800만 달러로 추정(2003년)
- 중국의 경우 세계 최대 지적재산권 침해상품 유통국가로 미국이 2002년 한해 중국으로부터 입은 피해액만 20억 달러로 나타남

○ **독일 연방정보부(Bundes Nachrichten Dienst, BND)**

- 독일은 산업스파이로 인해 연간 5만명의 실업자가 발생하는 것으로 추정

○ **캐나다 보안정보부(Canadian Security Intelligence Service, CSIS)**

- 최근 국회에 제출한 연례보고서에서 "외국 스파이들이 캐나다의 첨단 과학기술과 경제, 군사정보를 빼내는데 주력하고 있어 국가안보가 위협받고 있다"고 경고하면서, 한 고위 정보관리의 말을 인용해 중국이 가장 적대적으로 캐나다의 기술정보를 불법 취득 활동을 벌이고 있다고 발표

○ **일본 특허청**

- 일본 특허청은 일본 무역진흥회(JETRO)와 공동으로 중국과 대만에 진출한 일본계 기업을 대상으로 모방피해 실태조사를 실시(2003)
- 중국에 진출한 54.3%의 일본기업이 위조품으로 인한 피해를 경험했으며, 29.0%는 이로 인한 피해금액이 1억엔 이상으로 나타남

<산업스파이로 인한 피해 현황>

○ **미국산업보안협회(ASIS, 1999년)**

- 조사대상 : <Fortune>지 선정 1,000대 기업
- 보안체계 : 63%만이 산업스파이 대비 보안시스템 구비
- 피해경험 : 약 50%
- 피해횟수 : 평균 2.45건
- 기밀유출
  - 현직직원 30%, 전직직원 28%, 외부자로서 내부자처럼 일하는 사람 22%, 전문 산업스파이 및 정보요원 20%
- 피해금액 : 총 피해금액 450억 달러(건당 약 50만 달러)

○ **미국 연방수사국(FBI)**

- 가장 빈번하게 외국스파이의 표적이 되는 기업은 하이테크 기업이며, 이어서 제조업과 서비스업의 순으로 나타남
- 스파이들은 주로 연구개발 전략, 제조 및 마케팅 계획, 고객 리스트 등에 관심을 보이는 것으로 나타남

○ **미국 국가방첩관실(ONCIX, 2005년)**

- '외국 경제정보 수집활동 및 산업스파이 실태'에 대한 조사결과, 외국기업(36%), 외국정부(21%)가 미국의 핵심기술을 노리고 있는 것으로 조사됨
- 자료에 의하면 FBI는 2005년 말 현재 122개의 사건을 수사 중이며, 미 상무부에서는 1,300개의 사건 조사에 착수하여 그 중 31건에 대해 형사상 유죄판결을 이끌어낸 것으로 나타남

○ **캐나다 보안정보부(CSIS)**

- 산업스파이 행위로 입는 피해액이 월 평균 10억 달러로 추산
- 이와 같은 피해규모는 미국의 경제규모가 캐나다에 비해 10배 이상 크다는 점을 감안할 때 상당한 수준임

○ **스위스 경찰청**

- 1992년부터 2001년까지 외국 정보기관들이 개입된 산업스파이 사건을 총 31건 적발하였다고 발표

<기타 기술유출 피해 현황>

○ **미국 전자산업협회(The Electronic Industries Alliance, EIA)**

- 첨단산업의 경우 외국으로의 기술유출로 인해 매출액의 0.1%의 직접손실과 0.3%의 간접비용을 합하여 매출액의 0.4%의 손해를 보는 것으로 추정

○ **미국 Secret Service, 카네기 멜론 대학**

- '사이버 범죄 실태조사'결과 조사대상의 63%가 사이버범죄로 인해 관리적 손실을 입었다고 응답하였으며, 경제적 손실과 기업의 명성에 손상을 입었다는 대답은 각각 40%와 23%로 조사됨

○ **McAfee사**

- 조사대상 : 미국, 영국, 프랑스, 독일, 호주에 소재한 종업원 수 250명 이상 기업의 IT관련 의사결정권자
- 조사결과 : 최근 2년 동안 정보유출 경험이 한 번도 없었던 기업은 6%에 불과할 뿐 지난해 60%의 기업이 정보유출을 경험하였으며, 정보유출사건으로 인한 평균 피해금액이 1억 8천 2백만 달러에 이르는 것으로 나타남

○ **SanFrancisco Chronicle誌**

- 7천개가 넘는 기술기반 업체들이 입주해 있는 실리콘 밸리는 미국 어느 지역보다도 기밀 절취 관련 기소가 많이 발생하는 곳으로 산업기밀 유출이 연중 빈번하게 발생하고 있으며, 정보절취의 75~85%가 내부 직원에 의해 행해지는 것으로 나타남

2. 기술유출 사례

□ 미국[17)]

(1) Connecticut Man Pleads Guilty in U.S. Court to Selling Stolen Microsoft Windows Source Code
(U.S. v. Genovese, Southern District of New York, August 29, 2005)

○ Microsoft사의 Source Code를 불법으로 판매한 혐의로 Genovese가 기소된 사건

○ William P. Genovese. Jr.는 본인 홈페이지 'illmob.org'에 자신이 훔친 Microsoft Windows NT 4.0과 Windows 2000의 소스 코드를 올리고 이를 판매한다는 메시지를 게시하는 한편, 소스 코드 를 복제하거나 취약성을 발견하길 원하는 사람들에게 접근을 허용함

○ Microsoft사가 고용한 온라인 보안 회사의 검사관과 FBI는 피의자의 웹 사이트에서 소스 코드를 다운로드 받은 후 피의자에게 돈을 지불하는 과정을 거치면서 이 같은 사실을 확인함

○ 또한 피의자는 다른 컴퓨터에 그가 원격 조정할 수 있는 바이러스를 유포하고, Keylogging Software를 사용하여 피해자들의 컴퓨터를 장악하였으며, 자신이 무슨 일을 하는지 인스턴트 메시지를 통해 피해자들에게 알림

○ Genovese는 법원으로부터 최대 10년을 복역할 것과 이익금의 두 배에 상당하는 금액 또는 25만 달러의 벌금형이 선고됨

(2) Silicon Valley Engineer Indicted for Stealing Trade Secrets and Computer Fraud
(U.S. v. Zhang, Northern District of California, December 22, 2005)

17) 미국 연방법무부(USDOJ, United States Department of Justice)에서 공개한 경제 스파이법 관련 사례

○ Netgear, Inc.는 컴퓨터 네트워킹 제품을 생산하는 회사로 Marvell Semiconductor, Inc.와 Broadcom Corporation사의 주요 고객임

○ Netgear사의 전직 직원이었던 피의자는 Marvell사의 제품에 대한 영업비밀 및 비공개 정보와 제한된 정보에 대한 접근권한을 가지고 있었고, Broadcom사로부터 스카우트를 제의받은 피의자는 Marvell사의 Extranet을 통해 이 회사의 스위치와 트랜스세이버 제품에 관한 기밀 수십 건을 세 차례에 걸쳐 다운로드 받아 Broadcom사 직원들에게 이메일을 통해 전달함

(3) Chip Design Engineer Pleads Guilty to Transporting Stolen Property of Silicon Valley Company to Taiwan
(U.S. v. Tsai, Northern District of California, September 6, 2005)

○ Silicon Valley에 소재한 반도체 회사에서 디자인 엔지니어로 근무하던 Shin-Guo Tsai가 Volterra's VT1103 제품과 관련된 데이터 시트를 훔쳐 타이완에 있는 경쟁업체로 전송한 혐의로 체포됨

○ 데이터 시트에는 회사 소유의 대외교섭과 관련된 각종 정보가 담겨 있었으며, 이는 미화 12만 달러 이상의 가치를 지닌 것으로 추정됨

(4) Software Executive Admits to Conspiring to Misappropriate Chief Competitor's Trade Secrets - Second Guilty Plea in Case Involving Trade Secret Theft by Corporate Executives of Business Engine Software Corporation(BES)
(U.S. v. McMenamin, Northern District of California, September 29, 2005)

○ Business Engine Software Corporation(BES)사의 부사장인 William F. McMenamin은 경쟁회사들에 대해 경쟁적 우위를 점하기 위해 회사의 다른 임원들과 공모하여 10개월 동안 수차례에 걸쳐 경쟁사인 Niku사의 컴퓨터 네트워크와 애플리케이션에 불법으로 접속하여 영업 비밀을 빼냄

(5) Two San Jose Men Indicted for Stealing Trade Secrets Worth Over $1 Million
(U.S. v. Lam(Tran), Northern District of California, November 4, 2004)

○ C&D Semiconductor Services Inc.(C&D)의 전 직원이었던 Mr. Lam은 More Technology Services Inc.(MTS)을 설립하고, C&D로부터 핵심기술을 도용하여 이를 재가공한 뒤 제품을 생산·판매하는 한편, C&D의 고객들을 유치함

○ Mr. Lam이 훔친 기술은 'Track Systems'이라고 불리는 것으로, 고감도 사진 필름을 실리콘웨이퍼[18]에 적용하는 반도체 장비 관련 기술이며, 그는 이를 위해 C&D의 직원 몇 명을 스카우트하여 도안과 조립도, 유사 장비 등 관련 자료와 공구세공술을 획득함

○ 추정되는 손실액은 약 119만 달러임

(6) Former IT Director of Silicon Valley Company Pleads Guilty to Theft of Trade Secrets - Scheme to Steal and Offer Back-Up Tapes to Competitor Foiled When Competitor Contacted FBI
(U.S. v. Woodward, Northern District of California, August, 1, 2005)

○ IT 회사인 Lightwave Microsystems, Inc.의 전직 디렉터였던 Brent Alan Woodward가 회사의 기밀이 포함된 백업 테이프를 훔쳐 이것을 경쟁업체인 JDS-Uniphase사에 넘김

○ Brent Alan Woodward는 2002년 말 Lightwave사가 영업중단을 발표하자, 영업비밀이 담긴 백업 테이프를 훔쳐 'Joe Data'라는 이름으로 관련 정보 판매를 시도하고, 'lightwavedata@yahoo.com'이란 이메일 계정을 개설하여 관련 정보를 JDS사의 기술 담당관에게 제공함

18) 실리콘웨이퍼는 집적 회로가 조립되어 있는 얇은 실리콘 원판을 말하며, 조립 후에 검사가 끝나면 웨이퍼는 개별 칩으로 잘려서 완성된 집적 회로로 사용됨

(7) Los Angeles Man Sentenced for Stealing Trade Secrets Pertaining to 'Smart Card' Technology
(U.S. v. Serebryany, Central District of California, September 8, 2003)

○ Igor Serebryany는 DirecTV사의 법률 고문인 Jones Day Reavis & Pogue의 복사서비스 담당직원으로, 고용기간 중 DirecTV사의 '4세대 접속카드'와 관련된 핵심 기밀을 훔침

○ 그동안 DirecTV사는 그동안 법률 고문인 Jones Day에게 DirecTV사의 벤더 중 하나인 NDS Americas, Inc.와의 소송과 관련해 '4세대 접속카드' 기술을 포함한 회사의 기밀자료들을 제공해 왔음

○ DirecTV사는 미국 전역의 가정과 기업에 디지털 엔터테인먼트와 텔레비전 프로그래밍을 제공하는 업체로, 수신을 원하는 가입자가 DirecTV사의 위성신호를 받기 위해서는 제한수신시스템[19] 접속카드 등 하드웨어 아이템이 필요함. 접속카드는 위성 프로그램의 보안유지를 위해 필요한 핵심 컴포넌트로, DirecTV사는 '4세대 접속카드' 개발을 위해 2,500만 달러 이상을 투자함

○ Igor Serebryany는 캘리포니아 중앙법원으로부터 6개월간의 가택연금을 포함한 집행유예 5년을 선고받았으며, 손해배상금으로 DirecTV사와 Jones Day에게 $146,085를 지급할 것을 명령받음

(8) Guilty Plea to Economic Espionage
(U.S. v. Morris, District of Delaware, October 17, 2002)

○ John Berenson Morris는 섬유회사인 Brookwood Companies, Inc.의 가격정보자료를 훔쳐 이를 경쟁사인 Newark-based W. L. Gore & Associates, Inc. 측에 넘기려다 체포됨

19) 제한수신시스템(Conditional Access System) : 특정 방송 프로그램에 대한 수신 가능 여부를 사용자의 디지털 수신기가 결정하도록 하는 장치로, 정당한 수신료를 지불하는 사람만이 프로그램을 시청할 수 있도록 하기 위한 디지털 방송 상업화의 기본 필수기능임. 최근에는 과금과 편리성, 안정성 등을 고려하여 가입자의 고유개인정보를 가진 스마트 카드로 사용자에게 비밀키를 전달하는 것이 일반화 되어 있음

○ 유출된 가격정보는 군용 직물제품 생산을 위한 수백만 달러 상당의 국방부 입찰 건과 관련된 것으로, Morris는 W. L. Gore사에 전화를 걸어 이를 넘겨주는 대가로 10만 달러를 요구함. 그러나 W. L. Gore사는 이 같은 사실을 곧바로 연방법원에 연락하였고, Morris는 W. L. Gore사의 직원으로 위장한 국방부 비밀수사관과 접선을 시도하다 체포됨

○ John Berenson Morris에게는 10년형의 징역형과 25만 달러의 벌금형이 선고됨

(9) Former Engineer of White Plains Software Company Receives Two Years in Prison for Theft of Trade Secret
(U.S. v. Kissane, Southern District of New York, October 15, 2002)

○ 소프트웨어 개발회사인 System Management Arts Incorporated (SMARTS)사에서 엔지니어로 일하던 전직 직원 Timothy Kissane는 자신이 개발하고 있던 'InCharge'라는 이름의 소프트웨어 패키지 소스코드를 이메일을 통해 경쟁업체로 넘긴 혐의로 기소됨

○ 소스코드는 소프트웨어 패키지 개발에 있어 가장 근본적이고도 핵심이 되는 프로그램으로, 만약 경쟁회사가 이를 획득할 경우 기존에 가지고 있던 소프트웨어를 완벽하게 새로운 것으로 손쉽게 변형시킬 수 있음. 이 때문에 SMARTS사는 Incharge의 소스코드를 핵심기밀로 분류·관리하고 있었으며, 보안을 위해 소스코드 접근권자인 Kissane과도 고용계약당시 관련 정보에 대한 '평생' 비밀유지서약을 했던 것으로 밝혀짐

○ 그러나 Kissane는 갑자기 회사를 그만둔 뒤 SMARTS사의 경쟁회사 두 곳에 InCharge의 소스코드를 판매하고자 한다는 이메일을 보냈으며, 경쟁회사들은 이 사실을 곧바로 SMARTS사에 알림

(10) New Indictment Expands Charges Against Former Lucent Scientists Accused of Passing Trade Secrets to Chinese Company
(U.S. v. Comtriad, District of New Jersey, April 11, 2002)

○ Lucent Technologies사에서 'PathStar Access Server'의 개발담당자로 일하던 전직직원 Hai Lin과 Kai Xu, 그리고 PathStar 프로젝트 컨설턴트였던 Yong-Qing Cheng 등 세 명은 이메일, 패스워드로 보호되는 웹사이트, 중국 방문 등의 방법을 통해 베이징 소재의 벤처기업인 Datang Telecom Technology Co.에 'PathStar Access Server' 의 하드웨어와 소프트웨어를 훔쳐 넘겨줌

○ PathStar Access Server는 아날로그 음성 신호를 인터넷이 인식 가능한 전송 단위로 전환시켜 다양한 전화통화법을 가능하게 하는 시스템으로, Lucent사의 핵심기술이었음

○ 본래 이들 세 명은 ComTriad Technologies, Inc.라는 회사를 설립하고, 훔친 기술을 도용한 'CLX-1000'이라는 수정판 제품을 자체적으로 제조·판매하기 위해 벤처 캐피탈 컨설턴트를 통해 융자신청을 시도함. 그러나 컨설턴트가 'CLX-1000' 시제품에 대한 검증과 확인을 위해 관련 자료를 요구하자 Lucent사의 기술을 도용한 사실이 탄로날까봐 그와의 접촉을 중단함

○ 대신 이들은 베이징에 소재한 Datang사에게 함께 합작회사를 설립할 것을 제안하여, Datang사로부터 50만달러를 투자받고 'CLX-1000'의 시제품을 제공하기로 함

○ 이후 이들은 자신들의 범죄가 들통날까봐 ComTriad사의 모든 공식문서에서 자신들의 이름을 삭제하고, 회사 전자메일 이용시에도 본인의 이름을 사용하지 않았으며, 아내들의 명의로 휴대폰을 개설한 것으로 드러남

□ 일본

(1-1) 덴소 기밀 도난 : 중국인 용의자, 데이터 이미 암호화
(마이니치 신문, 2007년 3월 17일)

○ 대형 자동차 부품 회사인 덴소사(아이치현 카리야시)에서 기밀 데이터를 기록한 컴퓨터가 외부에 유출되는 사건이 발생하였으며 용의자로 중국인 엔지니어 양루촨이 체포됨

○ 그러나 용의자가 데이터를 옮긴 일부 기억매체는 발견이 되지 않았고, 입수한 매체의 경우에도 암호화 되어진 것으로 판명됨. 소재 불명의 매체에 기록된 데이터는 암호화되어 이미 일본 밖으로 반출되었을 가능성이 있어 경찰이 제공처와 이용 목적 등을 추적 중에 있음

○ 조사에 따르면, 용의자는 2006년 10월부터 12월까지 회사 대여 노트북에 사내 데이터베이스를 통하여 엔진 설계 등과 관련된 대량의 데이터를 다운로드한 뒤, 노트북을 집으로 가지고 가 자신의 컴퓨터와 외장 하드 디스크에 데이터를 복사한 것으로 밝혀짐

○ 경찰에서 회사 대여 컴퓨터를 압수하여 분석한 결과, 여러 기억매체에 접속한 흔적이 발견되었으며, 데이터가 저장되어 있는 파일에는 데이터 전송으로 인해 생긴 단절적 엑세스 기록이 남아있었음. 자택과 직장의 가택수사에서 찾아낸 여러 개의 기록매체와 조합해 본 결과, 아직 찾아내지 못한 기억매체가 존재하는 것으로 판명됨

○ 압수한 기록매체를 분석 하려고 하자 암호화와 패스워드 설정이 되어있어 데이터의 내용을 확인 할 수 없었으며, 해독하려고 하면 기록이 지워지는 것도 있었음. 자택에서 압수한 용의자의 컴퓨터는 하드 디스크가 부분적으로 파괴되어 있는 것으로 보아 증거인멸을 꾀한 것으로 판단됨

○ 2006년 10월부터 3회에 걸쳐 중국에 다녀온 것으로 밝혀진 용의자는 발각시 피해를 최소한으로 줄이기 위해 자체적으로 조치를 강구했으며, 자동차 산업 등 민생적 목적으로 중국으로 반출을 계속했을 가능성이 있다고 경찰은 판단하고 있음

(1-2) 덴소 사건 중국인 사원의 입건 단념
(요미우리 신문, 2007년 4월 7일)

○ 대형 자동차 부품 회사인 덴소사에서 약 13만 건에 달하는 제품 데이터를 반출한 용의자로 체포된 양루촨 사원을 나고야 지검에서 지난 6일 처분을 보류한 채 석방시킴

○ 횡령한 업무용 노트북의 가격이 약 6만엔으로 저가이고, 이미 반환이 완료되었기 때문에 지검에서는 기소유예 처분을 내릴 것으로 보여짐

○ 아이치현 경찰은 기업기밀의 유출의 가능성이 있다고 보고 부정경쟁방지법 위반(영업기밀 침해)의 적용도 검토하였지만, 사건 동기나 실제 데이터의 거래가 이루어졌는지에 대한 확인이 불가능하여 포기함

○ 용의자는 사내 규정을 위반하고 컴퓨터를 반출한 일이나 휴대용 하드 디스크 등 기억매체에 데이터를 복사한 것은 인정하지만, 데이터를 유출한 동기에 대해서 '연구를 위한 것'이라고 주장하고 있음

○ 덴소사 홍보부는 '아직 처분이 확정된 것이 아니기 때문에 특별히 할 말은 없으며 용의자에 대해서는 이후 사내 방침에 따라 처분하겠다'고 밝힘. 한편 용의자는 지난 3월 17일자로 덴소사로부터 해고됨

(2) 일본 경시청, 러시아 연계 반도체 산업스파이 사건 조사
(교도통신, 2005년 10월 20일)

○ 일본 경찰은 2005년 10월 러시아 무역대표부 소속 요원이 주도한 군용으로 전용가능한 반도체 기술에 대한 스파이 사건을 조사 중이라고 밝힘. 도쿄 경시청은 도시바 자회사의 전직 직원이 러시아 정보요원에게 백만엔을 받고 관련 정보를 유출한 것으로 추정된다며 업무상 배임혐의로 관련 서류 일체를 검찰에 송부함

○ 조사 결과, 유출자는 도시바 자회사에 근무한 경력이 있는 일본인으로 2004년 봄 도쿄 인근의 전자 전시회에서 러시아 요원을 처음 알게 되었으며, 러시아 요원과 접촉할 때마다 서류나 메모리 카드를 이용하여 반도체 기술관련 정보를 건넨 것으로 추정함

○ 유출된 정보는 '지속적인 게이트 신호에 의한 제어, 단극, 단방향성의 고속 스위칭 소자(IGBT)' 기술 등의 반도체 관련 기술로, 일반적으로 상용제품에 쓰이고 있으나 잠수함이나 전투기의 레이더와 미사일 유도시스템에도 적용되고 있음

○ 일본인은 돈이 필요했었다면서 금품수수 및 정보제공 혐의를 순순히 인정하였고, 회사는 그의 배신으로 큰 타격을 입었음

○ 러시아 요원은 2004년 6월 이미 일본을 떠난 후였으며, 스파이 사건을 담당하는 경시청의 공공안보실은 그가 다시는 입국하지 못하도록 외무성을 통해 조치를 취할 예정이라고 밝힘

(3) 러시아에 기밀 정보 제공한 니콘 전직사원 서류 송검
(Techno Nikkei web, 2002년 11월 14일)

○ 전 재일 러시아 통상대표부원이 대형 정밀기기 회사인 니콘사의 전직사원과 접촉하여 광통신에 이용되는 광학소재 기밀을 입수한 사건으로, 경시청 공안부는 11월 10일 절도혐의로 관련자들을 서류를 송검할 예정임

○ 공안부는 이미 러시아로 귀국한 전 통상대표부원이 첩보기관인 GRU의 일원으로 일본에서 스파이 활동을 하고 있었던 것으로 보고 있으며, '군사용으로 사용이 가능'한 광학소재 기밀을 수집할 목적으로 접촉을 꾀했다고 보고 있음. 이를 위해 전 통상대표부원은 도내에서 자주 니콘사의 전직직원과 접촉하였으며 전직 직원은 올 봄에 퇴직함

○ 러시아 스파이들은 일반적으로 스쳐 지나가는 순간 자료를 건네받는 'Flash Contact'이란 수법을 많이 쓰는 것으로 알려져 있지만, 최근에는 음식점 등에서 접촉하면서 정보를 입수하는 케이스가 많아짐

○ 러시아 통상대표부원에 의한 정보 수집활동은 작년 10월에도 경시청 공안부에 의해 적발된 바가 있으며, 이는 러시아 통상대표부원이 대형 전기 회사의 자회사 사원과 도내의 이자카야 등지에서 접촉을 반복하면서 군사용으로 사용 가능한 기밀 정보를 입수하고 그 대가로 현금을 건넨 경우임

(4) 나카무라씨, 미국에서 니치아 화학공업에 승소, 기업 기밀 유출을 둘러싼 재판 종결
(Techno Nikkei web, 2002년 11월 14일)

○ 전 니치아 화학공업의 기술자이자 미국 University of California, Santa Barbara(UCSB) 대학 교수인 나카무라 슈지가 니치아 화학공업에 재직할 당시 취득한 특허(특허 제2628404호)를 회사에 양도하면서 '상당한 대가'에 대한 금액과 산정하는 방식에 대한 심리가 2002년 11월 19일 도쿄지방재판소에서 시작됨

○ 한편, 같은 내용의 미국에서의 재판은 2002년 11월 6일 니치아 화학공업과 미국 Cree, Inc.가 화해에 합의함으로서 종결됨

○ 이미 2002년 10월 10일 나카무라씨가 승소한 것으로 밝혀진 미국재판은, 니치아 화학공업이 Cree사와 Cree사 자회사인 Cree Lighting Co., 미국 North Carolina State University(NCSU), 나카무라씨 등을 North Carolina 주 동부 연방 지방 재판소에 제소한 사건이며, 니치아 화학공업은 나카무라씨가 기업기밀을 Cree사측에 누설하였고 Cree사는 그 기밀 정보를 부정사용 하였다고 주장함

○ 당시 미재판소는 니치아 화학공업 측에 나카무라가 누설한 기업기밀을 구체적으로 특정지을 것을 요구하였고, 니치아 화학공업은 증거서면을 제출했지만 재판소는 그 증거서면으로부터 나카무라씨가 누설한 기업기밀이나 부정사용의 사실을 확인하지 못함. 이에 미국 재판소는 소송의 쟁점이 없다고 판단하여 니치아 화학공업의 청구를 기각하였고 나카무라씨가 승소함

□ 프랑스

(1) Michelin사 산업스파이 충격
(프랑스 국영방송 TF1, 2005년 10월 18일)

○ 세계적인 타이어 제조업체인 프랑스 Michelin사는 지난 월요일, Z BTO 타이어를 일본랠리 기간인 토요일 밤과 일요일 사이에 오비히로 보조 주차장에서 도난당했다고 밝힘

○ 4월에 있었던 뉴질랜드 랠리에서 첫 선을 보인 이후, 6번이나 되는 테스트를 통과한 Michelin사의 "매직타이어 Z BTO"는 세바스티앙 뢰브(Sébastien Loeb)가 세계 타이틀을 획득하는데 중요한 역할을 담당했었음

○ Michelin사의 랠리 프로그램 책임자인 에이메(Aimé)는 수상한 사건이 일어나기 몇 시간 전 유사한 제품의 타이어가 배달되었음이 분명하다고 설명하면서, 다음 달 열리는 세계 랠리 챔피언십에서는 BTO 타이어의 복제품에 대한 철저한 관리감독에 들어갈 것이라고 밝힘

○ Michelin사는 이번 도난이 처음이 아니며, 아일랜드 몽델로 공원 경주에서 수퍼바이크 자동차 타이어에 대해 이미 같은 공격을 당한 적이 있다고 주장함

(2) Chinese Girl Summoned for Questioning over Espionage Case in France
(All-China Women's Federation, August 01, 2007)

○ 24세의 중국 여학생 Li Li가 VALEO사의 영업기밀을 훔친 혐의로 프랑스로부터 소환요구를 받고 있는 사건임

○ 피의자는 교환학생 프로그램을 통해 프랑스에 입국했으며, 2005년 프랑스의 자동차 부품 회사인 VALEO사에서 인턴으로 근무하기 시작함

○ 그녀는 신의성실의 원칙위배와 회사 정보시스템에 침입한 혐의로 선배 동료 직원에 의해 기소되었는데, 그녀가 중국 자동차 산업의 중심지인 Hubei 출신이었기 때문에 더욱 강한 의심을 받게 됨

○ Li는 회사 컴퓨터에서 그녀의 이동식 하드디스크로 몇몇 문서들을 다운로드 받았다는 것은 인정했으나, 회사 기밀을 훔친 것에 대해서는 강하게 부인하고 있으며, 단지 인턴십 리포트를 작성하기 위해 참고 자료로 문서를 다운로드 받은 것이라고 주장하고 있음

○ 그러나 Li가 다운로드 받은 문서들은 BMW 모델 및 부품 디자인을 포함하여 2005년부터 2006년까지 중국에서의 VALEO의 개발 계획과 관련된 것이었기 때문에 현재 프랑스 내에서는 이 사건을 아주 조심스럽게 다루고 있으며, 여론도 좋지 않은 형편임

□ 영국

(1) Forensic Computing Uncloasks Industrial Espionage
(www.theresister.co.uk, 2004년 7월 15일)

○ British Midland Tools사는 이 회사의 전직 사원들이 회사의 핵심기술 도안이 담긴 전자 카피본을 훔쳐 Midland International Tooling Ltd(MIT)사에 입사한 사실을 입증해 줄 것을 컴퓨터 과학수사 회사인 Vogon International에 의뢰함

○ British Midland Tools사는 경쟁사인 MIT사가 자신들의 전직 직원들이 회사를 퇴사한지 얼마 되지 않아 근거리 내에 자신들과 같은 서비스를 제공하는 회사를 새롭게 차린 것을 보고 의심하기 시작함

○ 용의자들이 전자 도면을 훔쳐 MIT사로 이직한 뒤, 약 3백만 파운드의 가치가 있는 것으로 평가되는 British Midland Tools사의 고객 유치에 British Midland Tools사는 MIT사를 상대로 법적 조치를 취하게 됨

○ Vogon사의 수사관들은 MIT사에 대한 수색 명령과 더불어 수색 체포 과정에서 British Midland Tools사의 복제품임을 입증하는 제품임을 입증하는 MIT사의 AutoCAD 시스템을 확보함

○ MIT사 측에서는 자신들의 제품 도안이 이미 2000년에 만들어진 것이라고 주장했지만, 재판 결과 도안은 2002년 이후 British Midland Tools사의 컴퓨터로부터 MIT사의 컴퓨터로 정교하게 복제된 것으로 밝혀짐

(2) U.K Police Arrest Two Linked to Computer Espionage Case
(www.thestandard.com, 2005년 5월 31일)

○ 런던 경찰은 기업의 비밀자료를 훔치기 위해 악성 소프트웨어를 사용한 이스라엘 산업 스파이로 추정되는 컴퓨터 컨설턴트 Michael Haephrati와 그의 아내 Ruth Haephrati를 체포함

○ 이들은 이스라엘 경찰에 의해 산업 스파이 혐의로 조사받고 있는 소프트웨어 프로그래머들과 기업 중역들 중 일부일 것으로 추정됨

○ Michael은 스파이 활동에 사용하기 위해 트로이 목마(Trojan Horse)로 알려진 악성 소프트웨어 프로그램을 개발하여, 이를 이메일로 첨부하여 기업들의 컴퓨터로 발송함

○ 영국에서 이들이 체포되기 전 이미 이스라엘에서는 같은 수법의 일당 18명을 체포한 바 있음

□ 벨기에

(1) 벨기에 법정이 산업스파이 행위 수에즈사를 고소
(로이터통신, 2006년 8월 17일)

○ 벨기에 법정은 2004년도에 벌어진 사건과 관련하여 협력업체인 엘렉트라벨사에 손해를 끼친 것으로 추정되는 수에즈사와 5명의 프랑스 산업스파이를 기소함

○ 이들은 스파이 활동과 해킹을 선동하고, 사적인 커뮤니케이션 내용을 가로채려는 것에 대해 기소되었으며, 검사는 이들이 개인에 따라 6개월에서 5년까지의 징역형과 각각 20만유로에 이르는 벌금형을 선고받을 것이라고 밝힘

○ 수에즈사는 지난 일 년 동안 100% 프랑스 혈통으로 구성된 엘렉트라벨사의 소규모 주식들을 사들였고, 벨기에 전자관련 정보시스템의 안전성을 테스트하기 위해서 모의 테스트를 진행한 것뿐이라고 설명함

○ 검사는 다섯 명 중 세 사람은 두 회사에 결코 고용된 적인 없었던 반면, 한 명은 수에즈사에서 일했었고, 또 다른 한 명은 엘렉트라벨사에서 일했었다고 밝힘

중소기업 기술유출방지 대응매뉴얼

발 행 일 2007년 12월 18일 발행

편집 및 발행 중소기업청(☎042-481-4403, 4508),
중소기업기술정보진흥원(☎02-3787-0505, 0502)

연 구 기 관 한국산업기술진흥협회(☎02-3460-9072)