기업 5곳 중 1곳 기밀 유출 피해

글 | 노민선 _ 한국산업기술진흥협회 주임연구원 cool@koita.or.kr

'산업스파이 전쟁'이라는 용어가 거부감 없이 사용되는 현재의 기업 환경에서 어느 기업도 기밀정보의 유출에서 자유롭지 못하다. IMF 외환관리 이후 평생직장이라는 개념이 사라졌고, 이로 인해 최근에는 주요 기술이나 정보를 갖고 있는 핵심 임직원의 직장이탈이 가속 · 일상화되고 있다.

기업의 사활과 직결된 산업 기밀 보호

GDP 세계 11위, 수출 세계 12위, 외환보유고 세계 4위 등 우리 경제의 위상이 과거에 비해 높아진 것은 1980년대 이후 지속된 연구개발투자 및 인력의 증가 등 기업의 R&D 활동이 활발하게 추진되었기 때문에 가능했다고 할 수 있다. 1981년 이후 우리 나라의 연구개발투자는 약 60배가 증가하였으며, 산업체의 연구개발투자는 약 140배 증가하였다.

하지만 이처럼 국가역량이 강화되면서 세계적 기업들의 견제와 공세 또한 심해지고 있다. 견제와 공세는 특허소송, 불법기술유출, 전략적 제휴, 한국기업인수 등 다양한 형태로 나타나고 있는데, 이 중에서도 불법적인 기술유출은 국내의 기술기반을 잠식할 뿐만 아니라 연구원 및 기업의 기술개발 노력을 하루아침에 무산시키고, 그 피해액도 천문학적이라는 점에서 특히 우려할 만한 일로 간주되고 있다. 국가정보원에 따르면 참여정부 출범 이후 지난해말까지 기술유출 기도단계에서 적발된 사례는 총 61건으로 기술이 유출되었을 경우 예상되는 피해액은 82조 원이 넘을 것으로 나타났다.

이에 따라 최근 기업의 연구개발성과에 대한 효율적인 관리와 보호가 중대한 관심사가 되고 있으며, 신업기밀의 보호는 이미 기업에서 주요 경영전략으로 자리매김하고 있다. 특히 기업경쟁이 치열한 오늘날 기업 가치와 맞먹는 핵심기술을 포함한 산업기밀의 보호문제는 기업의 사활이 걸린 중대한 문제가 아닐 수 없다.

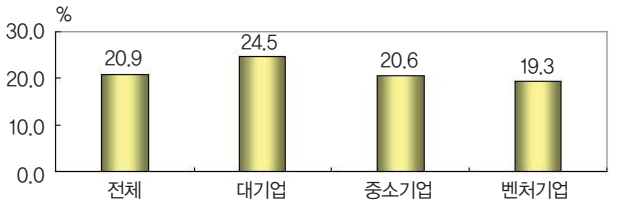
하지만 그 동안 기술개발의 산실이라고 할 수 있는 기업연구소의 산업기밀 관리현황에 대한 정확한 실태조사가 이루어진 적이 없으며, 일부 조사가 이루어지더라도 기업연구소 전체의 현황을 대표하기는 어려웠다. 이에 한국산업기술진흥협회는 기업연구소를 보유한 기업을 대상으로 조사방법론을 활용하여 표본기업을 선정하고, 이를 대상으로 실태조사를 하게 되었다. 2005년도 12월말 기준 기업연구소 연구개발전담부서를 보유한 1만1천325개사를 모집단으로 하여 업종별, 매출액별로 이원 층화추출한 459개사를 표본기업으로 조사하였으며, 95% 신뢰수준에 허용오차는 ±5.0% 수준이다. 이번 조사는 단순, 임의 형태가 대부분인 기존 조사의 한계를 극복하고, 통계적으로 의미 있는 결과를 산출해 냈다는데 가장 큰 의의가 있다.

정보통신 분야 기업 24.7% 기밀유출 피해

최근 3년간 산업기밀 유출 경험을 조사한 결과 응답기업의 20.9%가 내부 기밀정보가 외부로 유출되어 피해를 본 것으로 나타났다. 기업규모별로 살펴보면 보안역량이 미흡한 중소규모 기업들의 피해경험이 높을 것이라는 일반 생각과는 다르게 대기업의 피해가 24.5%로 가장 높았으며, 그 뒤로 중소기업의 20.6%, 벤처기업의 19.3%가 유출피해를 본 것으로 나타나, 기업규모가 클수록 기밀유출 비율이 높은 것으로 보인다. 특히 연구개발투자 상위 20대기업 중 11개사(55.0%)가 기밀유출로 인해 피해를 본 경험이 있다고 응답했다.

이는 대기업의 경우 자체적으로 보유하고 있는 기술수준이 우수할 뿐만 아니라 경쟁기업에서 기술을 빼내가기 위한 주요 타깃으로 삼고 있는 경우가 많기 때문으로 보인다. 뿐만 아니라 산업기밀 관리에 대해 대내외적으로 느끼는 위협에 대해서도 대기업이 중소 · 벤처기업에 비해 상대적으로 크게 느끼는 것으로 나타났다. 대기업의 경우 47.9%가 위협이 심하다고 응답한 데 반해 중소 · 벤처기업의 경우 39.7%에 불과했으며, 위협이 별로 없다고 응답한 기업의 비중은 대기업이 5.3%에 불과했으나, 중소 · 벤처기업의 경우

〈기업규모별 산업기밀 유출현황(최근 3년간)〉



10.7%에 달했다.

산업기밀 유출 경험을 업종별로 살펴보면 정보통신이 24.7%로 가장 높았으며, 기계소재 22.0%, 전기전자 21.3%, 서비스업 20.5%, 화학섬유 17.9%, 건설업 17.6% 등의 순으로 나타났다. 이는 기술수준이 타 업종에 비해 상대적으로 높고 기술변화가 심한 첨단산업 중심으로 기밀 유출이 이루어지고 있음을 의미한다.

평생직장 개념이 무너지는 등 고용환경의 변화로 인해 인력이동에 의한 유출이 갈수록 증가하고 있다. 기밀유출 관련자를 조사한 결과 퇴직사원이 63.5%로 가장 많았으며, 현직사원 17.7%, 고용외국인 4.2% 등으로 대부분 내부자에 의해 유출이 이루어지는 것으로 보인다. 기밀유출 방법은 핵심인력스카우트가 28.1%로 가장 높게 나타났다. 뿐만 아니라 조사기업 중 회사 연구원 중 최근 2년간 퇴사 후 경쟁업체로 전직한 경우가 있다고 응답한 기업이 30.7%에 달했다. 업종별로는 정보통신 41.6%, 전기전자 31.5%, 기계소재 29.0%, 화학섬유 28.6% 등의 순으로 나타났다.

퇴직사원에 의한 기밀 유출 63.5%로 가장 높아

이와 같은 조사결과는 내부 임직원에 대한 기밀유출 시도로부터 기밀을 보호하기 위한 예방적 조치를 취하는 것이 무엇보다 중요하다는 사실을 시사한다. 현행 법률에 의하면 종업원은 근무하는 회사에 대해 비밀유지의무를 부담하며, 이를 위반할 경우 회사측에 민사상 구제를 인정하고 위반자에 대해 형사상으로 처벌하고 있다.

'부정경쟁방지 및 영업비밀보호에 관한 법률'에 종업원의 영업비밀유지의무(제2조 제3호 라목)를 인정하고 있으며, 상법에 이사의 비밀유지의무(제382조의 4)를 인정하고 있다. 퇴직 후에도 비밀유지의무가 적용되는 것에 대해서는 법에 명백한 규정은 없지만 판례는 고용계약이나 영업비밀유지의무의 성질상 종업원은 퇴직 후에도 영업비밀을 침해하지 않을 신의칙상 의무를 부담한다고 보았다(대법원 1996.12.23).

포괄적인 법률내용에 비해 비밀유지의무 위반에 대한 법률요건의 입증이 쉽지 않기 때문에 법적 조치를 확실히 하기 위해 비밀유지계약의 중요성이 갈수록 커지고 있다. 하지만 조사결과에 따르면 대기업의 경우 입 · 퇴사시 비밀유지서약을 하는 비율이 높은 편이나, 중소 · 벤처기업의 경우 그 비율이 크게 낮다.

취업규칙 등에 임직원이 준수해야 할 영업비밀에 관한 사항을 규정하고, 서약서를 받아 보관하는 것은 기업측에는 매우 손쉬우면서도 분쟁 발생시에 강력한 효과를 발휘한다는 점에서 기업들의 인식전환이 요구된다. 물론 헌법상 보장되는 직업선택의 자유에 저촉되지 않는 범위내에서 제반 조치가 이루어져야 한다.

현행 법률이 종업원의 비밀유지의무 위반에 대한 민 · 형사상 구제수단을 보장하는데 반해 기업의 조치사항은 매우 미흡하다. 대기업의 경우 수사기관에 수사를 의뢰(52.2%)하거나 관계자(사)를 고소, 고발(34.8%)하는 등 강력한 조치를 주로 취하는 데 반해 중소기업과 벤처기업의 경우 특별한 조치를 취하지 않는 기업이 각각 43.6%, 41.2%로 높게 나타나 기밀유출에 대한 사후대응이 상대적으로 소극적인 것으로 나타났다.

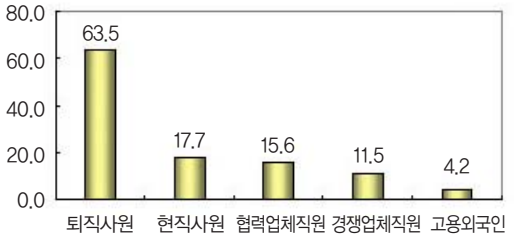
기술유출의 대부분은 인력의 이동에 있고, 인력의 이동은 더 좋은 근무조건에 있기 때문에 핵심기술 인력에 대한 처우개선을 통하여 기술유출의 원인이 되는 인력의 이동 자체를 최대한 억제하는 것이 필요하다. 기업의 보안관리 시스템을 강화하는 것도 중요하지만 무엇보다 중요한 것은 핵심기술 인력이 충분한 상을 받고 있다고 느끼도록 하는 것이다.

연구개발 성과에 대한 금전보상시스템을 보유한 기업의 비율이 47.5%로 나타났는데, 이는 연구원의 의욕을 돋우기 위한 기업차원의 노력이 꾸준히 이루어지고 있는 것으로 보인다. 한편 퇴직시 별도의 수당을 지급(5.7%)하거나, 퇴직 후 계약직(혹은 촉탁직)으로 재임용(4.6%), 퇴직 후 일정기간 생활보조비를 지급(1.5%)하는 등 퇴직시 공로보상이나 퇴직 후 관리는 아직까지 다소 미흡한 편이며, 기술의 변화주기가 빠른 첨단산업일수록 기밀유출방지를 위해 이를 확대, 운영할 필요가 있다.

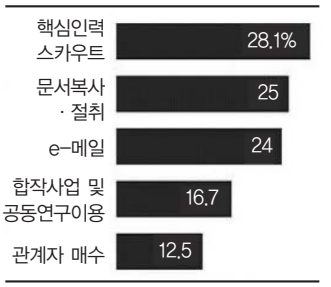
정보의 접근권한 통제 · 통합인증관리 선행돼야

내부자에 의한 기밀유출의 원인은 회사 기밀정보에 대한 무원칙하고, 무제한적인 접근권한 부여와 기밀정보 유출 방지를 위한 인증체계 미흡을 들 수 있다. 기업에서 발생하는 대부분의 보안사고는 내부자에 의해 이루어지기 때문에 아무리 강력한 방화벽이나 침

〈기밀유출 관련자(복수응답)〉



〈기술유출방법(복수응답 허용)〉



입탐지시스템이 구축되어 있어도 내부자의 기밀유출에는 속수무책일 수밖에 없다.

회사의 기밀이 되는 정보자산의 유출을 방지하기 위해서는 정보의 접근권한의 적절한 부여와 통합인증관리가 선행되어야 하며, 이를 위해서는 문서보안시스템과 DRM(디지털저작권관리)시스템 구축이 필수적이다. 기밀관리 시스템에 대한 조사결과 문서보안시스템 구축과 DRM 시스템 도입기업의 비중이 각각 27.7%와 6.1%로 낮게 나타났는데 일반문서 및 전자문서에 대한 외부로의 무단유출 가능성을 최소화하기 위해서는 양시스템 도입이 보다 확대될 필요가 있다.

하지만 기업이 산업기밀을 관리하는 데 있어 회사의 보안인프라 구축을 위한 투자를 결정하는 것은 보안업무의 특성이 당장 성과로 나타나지 않기 때문에 현실적으로 쉽지 않다. 조사결과 기업들은 산업기밀을 관리하는데 가장 큰 애로사항으로 핵심인력 유출 위험성과 보안인프라 투자 곤란을 꼽았다. 핵심인력 유출 위험성이 회사의 근무조건 등과 관련이 있어서 기업차원의 노력이 주로 요구되는 데 반해, 기업의 보안인프라 투자는 국익차원에서 정부의 지원이 검토되어야 한다. 예를 들어 최근 전자문서의 비중이 커지고 있다는 점을 감안하여 중소 · 벤처기업의 DRM 솔루션 도입비용을 정부에서 지원하는 것을 고려할 필요가 있다. 시스템 도입비용에 비해 그 효과가 훨씬 클 뿐만 아니라 매칭펀드 형식을 가미한다면

〈비밀유지계약 체결기업 현황〉

구 분	대기업	중소기업	벤처기업
입사시 비밀엄수서약 작성	78.7%	59.1%	48.7%
퇴사시 비밀유지 및 겸업금지 서약	73.4%	44.9%	38.6%

기업의 도덕적 해이도 방지할 수 있을 것이다.

정부차원의 기술보안 전문기관 육성 기대

'보안'은 당장은 이익이 되지 않지만 미래의 불확실성을 어느 정도 해소할 수 있다는 점에서 '보험'과도 같다. 기업의 내부 기밀정보가 외부로 유출되는 것을 방지하려면 먼저 산업기밀 보호를 위한 기업 스스로의 노력이 선행되어야 하며, 관련 제도나 정책이 뒷받침하는 형태로 이루어지는 것이 효율적이다. 특히 중소기업의 경우 산업기밀 관리의 중요성을 제대로 인식하지 못하는 경우가 많다.

기업차원의 보안관리의 핵심은 임직원 인사 및 보상관리다. 앞에서 언급한 바와 같이 기밀정보 유출 대부분이 전 · 현직 임직원에 의해서 이루어지고 있다. 평생 고용의 개념이 사라지고 고용이 유연해짐에 따라 성과에 대한 합리적인 보상의 중요성이 갈수록 증가하고 있다.

핵심역량을 보유한 대기업의 경우 자체적으로 강력한 보안시스템을 보유하고 있는 경우가 많다. 하지만 규모가 작고 투자여력이 부족한 중소기업의 경우 보안관리규정 마련, 임직원 입 · 퇴사시 보안서약, 정기적인 보안점검 등 비용이 들지 않는 기본적인 관리활동부터 시작하는 것이 바람직하다. 기본관리를 통해 보안수요를 파악한 후 보안관리시스템을 구축하는 것이 효과적이다.

정부는 기업의 산업기밀 관리노력을 지원하는 기술보안 전문기관의 육성을 적극 추진할 필요가 있다. 조사결과 기업들은 산업기밀 보호를 위해 정부차원에서 가장 우선적으로 추진해야 할 사항으로 기술보안 전문기관의 육성(27.8%)을 꼽았으며, 그 다음으로 보안교육, 지도, 자문활동 지원(25.0%)이 필요하다고 응답했다. 중소 · 벤처기업의 경우 개발한 기술을 보호할 수 있는 전문인력이나 재정적인 여력이 별로 없다. 산업현장에서의 보안실천을 위해 지도, 자문, 교육을 담당할 수 있는 기관의 설립이 필수적이다. ST

글쓴이는 서강대학교 경영학과를 졸업했다.