산업기술 보안에 대한 조사 및 분석과 개선 방안★

김성종*

요 약

최근 들어 산업기술 유출 문제의 심각성이 대두됨에 따라 보안에 대한 중요성도 나날이 증대되고 있다. 본 논문에서는 산업기술 보안에 대한 연구 동향과 산업기술 유출 실태에 대해 조사하여 여러 가지 측면에서 분석하였으며, 산업기술 유출 문제의 심각성과 그에 따른 보안의 시급성을 보였다. 마지막으로 산업기술 보안에 필요한 개선 방안을 법률적, 경영 방식, 기술적 측면으로 나누어 제시하였다.

Survey and Analysis of Industrial Technology Security, Propose the Improvement Plan

Kim Seong Jong*

ABSTRACT

According to the advent of the seriousness of industrial technology outflow, concerns are mounting about the importance of security, recently. In this paper, I studied a research trend about industrial technology security and real condition of the outflow, analyzed it in various ways, and showed a seriousness of the issue and urgency of the security. Finally, I suggested methods of improving needed in the industrial technology security in legal, business and technical ways.

Key words : Industrial technology, Security, Research trend, Legal ways, Business ways, Technical ways

접수일(2015년 5월 11일), 수정일(1차: 2015년 5월 22일, 2차: 2015년 5월 30일), 게재확정일(2015년 6월 01일)

★ 본 논문은 극동대학교 교비학술연구 지원 사업에 의하여 연구되었음.

* 극동대학교 유비쿼터스IT학과

1. 연구의 필요성 및 동향

1.1 연구의 필요성

현대 사회는 급격한 기술의 발전과 더불어 산업기술의 불법적인 유출 역시 증가하여 심각한 사회 문제로 대두되고 있다. 불법적인 산업기술의 유출은 기업의 성장과 발전을 저해함과 동시에 나아가 국가 전반의 이익에 해를 끼치는 사회의 중요한 문제들 중 하나이다. 따라서 날로 심각해지는 불법적인 산업기술의 유출을 방지할 수 있는 구체적인 해결 방안을 마련하는 것은 중요하며 시급하다 할 수 있다.

1.2 연구 동향

현재 우리나라는 불법적인 산업기술 유출을 막기 위하여 법률적, 경영방식, 사회인식, 기술적인 면 등 다방면에 걸쳐 개선과 재정비를 진행 중이다.

먼저 법률적으로는 법률의 정비, 법조문의 구체화 등을 통하여 진행 중이며, 그 예로 2015년 1월 법률 제13083호 '산업기술 유출방지 및 보호에 관한 법률'이 지속적으로 개정되어 공포되었다.[1-2] 정부에서는 기술유출의 심각성을 인식하여, 법조문의 정비를 통한 처벌수위를 높이는 식의 개정 역시 계속 추진하고 있다.

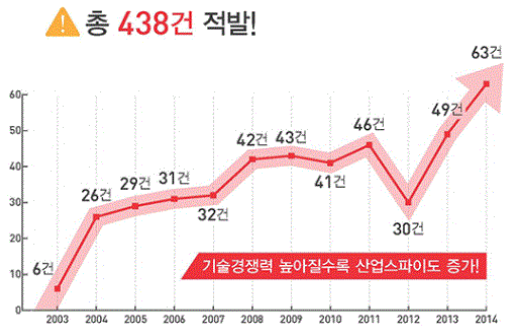
경영방식에 있어서도 영업비밀 관리 매뉴얼의 도입, 임직원을 대상으로 한 정기적인 보안 교육 등의 노력을 보이고 있으며,[3] 사회적 인식 부분 역시 기존의 관련 업종 전문가들로 한정적으로 이루어졌던 인식 개선이 최근에는 공공 캠페인, 세계 보안 엑스포 등을 통하여 다양한 계층을 대상으로 널리 진행되고 있다.

또한 기술적 측면에서는 불법적인 산업기술 유출 시도가 빈번해지고 그 방식이 진화하면서 반대급부로 다양한 형태의 보안 솔루션들도 시장에 등장했다. 그러나 기존의 보안 솔루션들은 대부분 고가에 다기능 제품이어서 중소기업에 적용하기 어려운 면이 있으며, 기업 맞춤형 보안 솔루션의 필요성에 대두됨에 따라 정부에서도 2007년부터 매년 중소기업 산업기술개발 사업을 통하여 30억원을 지원하고 있다.[4-5]

2. 연구 내용

2.1 산업기술 유출 실태 및 분석

현재 우리나라는 눈부신 기술 발전과 한류의 확산 등에 힘입어 다방면의 산업이 호황기를 맞이하고 있다. 하지만 동시에 산업의 핵심인 산업기술이 불법적으로 유출되는 사례 또한 증가하고 있으며, 산업 자체의 기강을 흔들고 있는 상황이다.



(그림 1) 연도별 해외 산업 스파이 적발 실적[6]

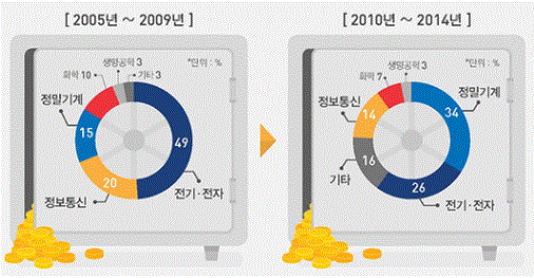
산업기밀 보호 센터의 발표 자료에 의하면 2003년부터 2014년 사이 해외 산업스파이 적발 건수는 총 438건에 달한다. 산업스파이 적발 건수는 꾸준히 증가하다가 2012년에 잠시 줄어들기도 하였지만 지구촌에 본격적인 한류 문화가 확산되면서 다시 급등하여 2014년에는 통계를 내기 시작한 2003년 대비 10.5배, 2012년 대비 2.1배나 증가하였다.

한편 한국 산업기술 보호 협회에 의하면, 기술유출 피해업체의 예상 피해액은 연평균 50조원에 달할 것으로 추정되며, 이는 2014년 GDP(국내총생산)의 5%에 해당하며 국내 중소기업 약 7,800여 개의 연매출과 맞먹는 금액이다.[7]

기술 유출에 따른 피해 기업의 규모별 현황을 살펴보면, 2010부터 2014년 사이 최근 5년간 대기업 16%, 중소기업 64%,, 대학 및 공공 연구기관 20%로 대기업에 비해 중소기업의 피해가 훨씬 심각한 것으로 나타났다. 중소기업이 대기업보다 4배나 심각한 이러한 결과는 대기업에 비해 자금력이나 보안에 관한 인식 및 기술력이 떨어짐 등에 그 이유를 찾을 수 있겠다.

2.2 산업분야별 기술 유출 현황 및 분석

최근 지난 10년간 산업분야별 기술 유출 현황을 5년 단위로 나누어 살펴보면 다음과 같다.

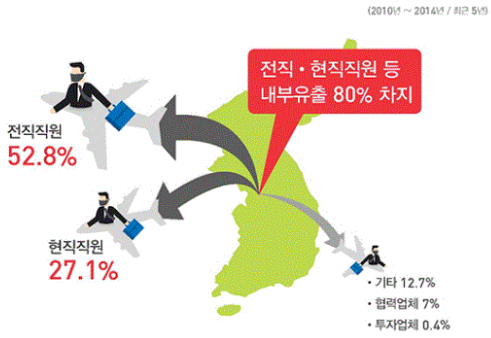


(그림 2) 산업분야별 기술 유출 현황[6]

그림 2에 보였듯이, 최근 들어 기술 유출의 분야 또한 점차 산업 전반으로 확대되는 추세이다. 지난 2005년부터 2009년 사이에는 전기·전자, 정보통신, 정밀기계, 화학 분야의 기술 유출이 대부분 이었으나, 최근 5년 동안은 정밀기계, 전기·전자, 기타, 정보통신 분야의 기술 유출이 많은 것으로 나타났다. 특히 2005년부터 2009년 사이에는 전기·전자 분야의 기술 유출이 절반에 가까웠으나 최근 5년 동안은 정밀기계 분야의 기술 유출이 가장 심한 점과 기타 산업분야의 기술 유출도 날로 정도를 더해 감을 알 수 있는데, 이는 이제 산업기술 유출이 대기업의 IT 기술 분야는 물론이요 중소기업의 정밀기계 분야 등 특정한 산업분야에서 만이 아니라 산업 전반에서 빈번하게 발생하고 있음을 나타내어 준다고 할 수 있겠다. 또한 산업기술진흥협회가 2010년도에 조사한 내용에 의하면, 기업의 산업보안 역량 수준은 대기업은 양호한 수준(75.7점)이나 중소기업은 취약 수준(45.7점)으로 나타났다.[8]

2.3 산업기술 유출의 주체

최근 5년간 산업기술 유출의 주체를 살펴보면 다음과 같다. 산업기술 유출의 주체는 해당 기술의 가치를 잘 알고 있으며, 그 기술에 대한 접근권한이 있는 사람이 대부분인 것으로 나타났는데 이는 2008년 통계에서도 비슷한 결과를 보였다. 그림 3의 자료를 분석해 보면, 불법적인 기술 유출 대부분이 주로 전직, 현직 기업 내 구성원에 이루어지고 있으며, 협력업체에서의 유출 역시 무시 할 수 없다고 할 수 있다. 따라서 전직, 현직 직원을 대상으로 한 기술 유출 방지 방안 및 시스템 구축을 시급히 추진하여야 하며, 외부 협력업체와의 공동 작업 시 기술 유출 방지를 위한 표준 매뉴얼 제작의 필요성 또한 크다고 할 수 있겠다.



(그림 3) 산업기술 유출의 주체[6]

3. 개선 방안

3.1 법률적 측면

현재 우리나라는 불법적인 산업기술 유출방지를 위해 법률 제13083호 '산업기술 유출방지 및 보호에 관한 법률'이 2015년 1월 28일에 공포되어 시행되고 있다. 이 법률에 의거하여 산업기술을 불법적으로 외국에서 사용하거나 외국으로 유출한 자는 10년 이하의 징역 또는 10억원 이하의 벌금에 처하며, 이러한 범죄에 대한 예비 음모도 3년 이하의 징역이나 3천만원 이하의 벌금에 처하도록 되어있다. 그러나 이 법률의 벌칙 내용에서 벌금의 상한액이 10억원 이하로 규정되어 있어, 점점 피해 규모가 커지고 있는 실태를 반영하지 못할 가능성이 있으므로, 예상되는 피해액의 규모를 정확하게 조사 분석하는 위원회를 별도로 설립하여 운영함으로써 피해액 별 벌금 규모를 정하는 융통성도 필요하다 하겠다.

또한 경찰청에 따르면 2010년 40건(국내유출 31건, 해외유출 9건)에 불과했던 산업기술 유출사범 검거건수는 2011년 84건(국내 60건, 해외 24건)으로 늘었고,

2012년엔 140건(국내 113건, 해외 27건)으로 크게 증가했다. 하지만 기술유출 사건에 대한 검찰의 기소율은 12.8%(2012년)에 불과하며, 유죄가 입증되더라도 대부분 집행유예가 선고된다.[9] 이러한 결과는 기술유출 증거 확보의 어려움과 기술 유출에 대한 처벌 기준이 까다로운데다 처벌 수위도 터무니없이 낮아 일어난 현상이라 할 수 있다. 한편 산업기술 유출 시 법적 대응을 하지 않는 주요한 이유를 분석해보면 다음과 같다. 먼저, 산업기술 유출 사실을 입증하기 어려운 면이 있으며, 소송비용이 많이 들고, 거래 관계로 인하여 다투기 어려운 면이 있다. 특히 중소기업의 경우 이러한 여러 문제들을 처리해 줄 전담부서가 전무하여도 과언이 아니어서 문제의 심각성이 더하다 하겠다.[10] 또한 2011년에 개정된 '하도급 거래 공정화에 관한 법률'에서 처음 도입된 징벌적 손해배상제도의 경우 하도급 업체에 기술 자료를 요구한 사업자에게 그 피해액의 3배를 배상하도록 하였으나 제도의 도입 목적인 불법 행위 예방 효과는 미미하다는 평가가 있으며, '제52회 법의 날'을 맞아 서울지방변호사회와 법률신문사가 공동개최한 '징벌적 손해배상제도 도입에 관한 심포지엄'에서 하도급 분야에서 3배 배상제도는 불이익을 감수하기에는 실효성이 매우 낮기 때문에 징벌적 손해배상금을 수정해야 한다는 법률가의 의견이 제시되기도 하였다.[11] 그리고 최근 전국경제인연합회가 72개 대기업의 1차 협력사 334개를 대상으로 실시한 설문조사에 따르면, 징벌적 손해배상제도를 확대 시행하거나 신중히 추진하자는 업체가 73.9%에 달하는 것으로 조사되어 법률적 제도보완이 시급히 필요한 것으로 나타났다.[12]

3.2 경영방식

앞의 연구 내용에도 기술하였듯이, 산업기술 유출의 주체는 현직 및 전직 직원들에 의하여 발생하는 내부유출이 80%에 이르는 것으로 조사되었다. 이러한 조사 결과는 내부 유출방지가 다른 어떤 조치보다 시급함을 보여주며 특히 산업기술 유출의 주체 중 52.8%를 차지하고 있는 전직 직원들에 의한 기술 유출의 심각성은 경영방식 면에서도 여러 변화가 필요함을 암시하고 있다. 산업기술 불법 유출에 대한 동기를 분석해 보니 개인의 영리를 목적으로 행해진 사례가 가장 많았다. 결국 산업기술의 불법 유출을 방지하기 위해서는 기업 임직원들에 대한 보안 교육과 처우 개선이 핵심이다. 이러한 문제들을 해결하기 위한 방안으로 법령 개정 등을 통하여 산업기술 유출 방지를 위한 교육 및 지원 기구의 운영을 제안한다. 제안된 기구의 주요 역할은 다음과 같다.

첫째, 산업기술 유출 방지가 반드시 필요한 기업들은 물론 기업 운영을 위한 원천 기술을 가지고 있다고 인정할 수 있는 기업 그리고 기술 보호를 요청하는 신생 기업이나 벤처 기업 등을 조사하여 산업기술 유출 방지를 위한 기업 풀을 구성하기 위한 기준을 마련한다.

둘째, 구성된 기업 풀에서 기업들의 산업 종류별 세부 분류를 통하여 효과적인 산업기술 유출 방지를 위한 맞춤형 교육 프로그램을 운영하도록 한다. 교육 프로그램의 운영에 예를 들면, 현직 임직원들에 대하여서는 정기적인 보안 교육을 의무적으로 실시하도록 강제하며, 퇴직 희망자들을 대상으로는 퇴사 전 산업기술 유출 문제에 대한 사전 교육 실시하도록 하여 불법적인 산업기술 유출이 원천적으로 차단될 수 있도록 하여야 할 것이다.

셋째, 세그먼트화 된 보안 매뉴얼을 개발한다. 현재 널리 운용되고 있는 보안 매뉴얼들은 대부분 중소기업들에 그대로 적용하기엔 무리가 있으며, 그 효과에도 의문이 있다. 이에 따라 아래 기술적인 측면에서 제안한 세그먼트 및 독립형 보안 솔루션의 표준 작업을 통하여 중소기업을 위한 맞춤형 보안 매뉴얼을 개발하고 보급하도록 한다. 이러한 시도들은 산업기술 유출 방지 시스템을 구축하여 운영하려 계획하고 있는 경영자 입장에서는 산업기술 유출 방지 시스템의 구축 시, 필요 인력과 시스템 관리를 위한 표준 매뉴얼도 미리 받아 볼 수 있어 정책 결정에 필요한 시간과 노력을 줄일 수 있을 것이다.

3.3 기술적인 측면

대기업의 경우 자체의 기술력이나 자금력을 통하여 불법적인 산업기술 유출에 적극 대응하고 있으나, 중소기업의 경우 전체 피해액의 약 64%로 대기업에 비해 4배나 많은 피해를 보고 있다. 대기업에 비해 상대적으로 기술력이나 인력과 자금력이 충분하지 못하므

로 중소기업의 경우 이를 만회할 만 한 기업 맞춤형 보안 솔루션의 개발이 시급하다 하겠다. 이러한 문제를 해결하기 위한 방안으로 다음과 같은 조건을 갖춘 보안 솔루션의 개발을 제안한다.

첫째, 세그먼트 및 독립형 보안 솔루션의 개발을 제안한다. 기존의 UTM(Unified Threat Management)의 경우 안티바이러스, 방화벽, 가설사설망, 침입방지 시스템, 트래픽 쉐이핑, 콘텐츠 필터링, 웹 필터링, 메일 필터링 등 여러 가지 기능들을 통합적으로 제공해 준다. 이에 비해 본 논문에서 제안한 세그먼트 및 독립형 보안 솔루션이란, 현재 고가의 다기능화 되어 있는 보안 솔루션들을 가격 및 기능별 그리고 기업의 규모 등으로 분화하여 각각을 캡슐형으로 구현하고 기업의 입장에서는 필요한 캡슐들만을 선택하며, 선택된 캡슐들의 조립을 통하여 기업 맞춤형 보안 솔루션이 구축되어 진다. 또한 이러한 보안 솔루션의 설치 시 별도의 서버나 기타 부대장비가 필요 없도록 독립형 보안장비의 개발이 필요하다 하겠다. 이러한 시스템은 솔루션 구축 시 기업의 부담을 크게 덜어 줄 것이며, 관리 운영에도 도움을 줄 것으로 예측된다. 또한 보안 캡슐들 및 독립형 보안장비의 표준화 작업을 통하여 기업을 위한 맞춤형 표준 보안 매뉴얼의 개발이 가능해 질 것으로 사료된다. 이러한 시도들은 경영적인 측면에서도 도움이 될 것이다. 산업기술 유출 방지 시스템을 구축하여 운영하려 계획하고 있는 경영자 입장에서는 구축될 시스템의 표준화 된 성능 및 가격을 확정적으로 쉽게 예측할 수 있으며, 시스템 운영 시 필요 인력과 시스템 관리를 위한 표준 매뉴얼도 미리 받아 볼 수 있어 정책 결정에 필요한 시간과 노력을 줄일 수 있을 것이다.

둘째, 바이오기술(BT)과 정보기술(IT) 등을 융합한 차세대 지능형 생체인식 기술의 개발을 제안한다. 현재도 다양한 생체인식 기술이 개발되어 활용되고 있으나 기존의 기술들은 대부분 인식 기능에만 치우쳐 있어 내부인을 통한 기술 유출에는 대책이 없는 상태이다. 본 논문에서 제안한 차세대 지능형 생체인식 기술은 기존의 생체인식 기능에 보안 기능을 부가하기 위하여 다음과 같은 작업을 수행하도록 한다. 먼저 생체인식 시스템을 통하여 인증된 내부 인이 산업기술 유출이 우려되는 보안구역 내의 시스템에 접근할 시, 사용자의 보안 등급에 따라 접근할 수 있는 시스템 하드웨어 자원 및 소프트웨어 솔루션의 사용을 제한하도록 하여, 불법적인 산업기술 유출에 선제적으로 대처할 수 있도록 한다. 또한 로그인 시점부터 로그아웃 시점까지 주요 작업 내역을 자동으로 남기도록 하여 불법적인 파일 유출 등의 보안 사고를 사전에 방지하도록 할 수 있을 것이다. 마지막으로 인증된 내부인이 보안구역을 벗어날 경우 제안한 시스템이 그 내부인의 보안구역 내에서의 활동 시간 및 작업 내용을 보안 관리자들에게 자동으로 전송하며, 보안 관리자들은 그 내용의 적법성을 의무적으로 체크하도록 한다면 2차적인 기술 유출 방어벽을 구현할 수 있을 것으로 사료된다.

그러나 제안한 시스템에서는 개인정보의 취급 및 처리가 문제 시 될 수 있으므로, 내부인의 활동 시간 및 작업 내용을 암호화하여 처리하여, 적법성이 의심될 경우에만 복호화를 통한 확인 작업을 거치도록 하며, 시스템을 통해 수집된 개인정보는 유출 방지를 위해 보안 등급에 따라 차별화하여 일정 기간이 지나면 자동 삭제하도록 하여 개인의 프라이버시가 침해될 소지를 최소화 하도록 한다.

4. 결 론

불법적인 산업기술 유출이 발생하지 않도록 하기 위한 결론은 다음과 같다.

먼저 법률적인 측면에서는, 현재 한정적으로 시행하고 있는 징벌적 손해배상제도의 전면적 시행과 피해액의 10배를 보상하도록 하는 안을 제안한다. 중소기업의 경우 연평균 기술유출 피해액은 전체의 64%, 약 32조원에 차지하므로 본 논문에서 제안한 방안이 기술유출 예방 차원에서 제도적으로 자리 잡는다면 최소 10%의 기술유출 방지만으로도 3조원, 20%라면 6조원 이상의 피해를 줄일 수 있을 것으로 예상된다. 또한 현재 시행 중인 법률은 벌칙 내용에서 벌금의 상한액이 10억원 이하로 규정되어 있어, 점점 피해 규모가 커지고 있는 실태를 반영하지 못할 가능성이 있으므로, 예상되는 피해액의 규모를 정확하게 조사 분석하는 위원회를 별도로 설립하여 운영할 것을 제안한다.

산업기술 유출 시 중소기업의 경우 문제를 해결할

전담부서가 전무한 상태이므로 정부적인 차원에서 대책위원회 등을 상시 가동할 수 있도록 지원책을 강구할 필요가 있겠다. 또한 본 논문에서 제안한 산업기술 유출 방지를 위한 교육 및 지원 기구의 운영을 통하여, 경영자 입장에서는 산업기술 유출 방지 시스템의 구축 시, 필요 인력과 시스템 관리를 위한 표준 매뉴얼도 미리 받아 볼 수 있도록 도와주며, 정책 결정에 필요한 시간과 노력을 줄일 수 있도록 하여야 할 것이다. 본 논문에서 제안한 이러한 노력들이 종합적으로 이루어진다고 가정하면, 현재 약 80%, 2014년 기준 약 50건에 달하는 내부자에 의한 기술유출 건수를 매년 약 10%씩만 줄여 나가도 5년 후에는 약 20건(2014년 기준 40%)의 기술유출을 줄이는 효과가 있을 것으로 사료된다.

기술적인 측면으로, 본 논문에서는 기술력이나 인력과 자금력이 충분하지 못한 중소기업을 위한 맞춤형 보안 솔루션의 개발과 차세대 지능형 생체 인식 시스템을 제안하였다. 제안된 세그먼트 및 독립형 보안 솔루션을 통하여 기업들은, 각 기업의 규모와 특성에 맞게 필요한 기술들만을 선별하여 솔루션을 구축한다면 부담을 최소화할 수 있을 것이다. 예를 들어, 기존 UTM에서 주로 구현되는 8가지 정도의 솔루션 중 기업의 특성에 따라 몇 가지 솔루션과 서버의 개수를 줄 일 수 있다면, 그 만큼의 비용이 절약됨은 물론이요 시스템의 관리 비용 또한 줄일 수 있을 것이다. 또한 본 논문에서 제안한 개인정보 보호가 고려된 바이오기술(BT)과 정보기술(IT)을 융합한 차세대 지능형 생체인식 시스템이 성공적으로 활용된다면 경영적인 측면에서 제시한 방안과 시너지 효과를 일으켜 불법적인 산업기술 유출 방지에 많은 도움을 줄 것으로 사료된다.

참고문헌

[1] 국가법령정보센터, http://www.law.go.kr/ lsSc.do?menuId=0&subMenu=1&query=%EC%A0%9C13083%ED%98%B8

[2] ‘산업기술 유출 방지를 위한 법적고찰’, 박성배, 법학연구 제13집 제1호, pp. 137-170, 2010

[3] ‘기업의 산업기술 유출방지 연구’, 정병일, 산업보안연구학회 논문지, 제1권 제1호, pp. 1-19

[4] 중소기업청 제품성능기술과 보도자료, 2009. 07.06.

[5] 중소기업청 산학협력과 보도자료, 2009.10.19

[6] 산업기밀보호센터, http://service12.nis.go.kr/ servlet/page?cmd=preservation&cd_code=outflow_1&menu=AAA00

[7] 한국산업기술보호협회, http://www.kaits.or.kr/front/bmt/bbs/list.act?bbs_config_nid=2

[8] ‘산업기술 보안의식과 정보보안 투자가 ISMS인증에 미치는 영향 분석’, 김인관, 건국대학교 기술경영학과 석사논문, 2011.08

[9] 뉴데일리 경제, http://biz.newdaily.co.kr/news/article.html?no=10045921, 2014.08.26.,

[10] ‘첨단기술의 유출방지를 위한 관련법규의 형사법적 문제점과 개선방안에 관한 연구’ 홍민지, 지식재산연구 제3권 제1호, pp. 137-171

[11] 법률신문 뉴스, https://www.lawtimes.co.kr/ Legal-News/Legal-News-View?serial=92588, 2015. 04. 23.

[12] Chosun Biz, http://biz.chosun.com/ site/data/html_dir/2013/02/18/2013021800968.html, 2015. 05. 30.

[저 자 소 개]

김 성 종 (Seong-jong Kim)

1987년 2월 공학사(전자공학)
1989년 2월 공학석사(응용컴퓨터)
1998년 8월 공학박사(응용컴퓨터)

email : ksj@kdu.ac.kr