산업스파이 식별요령

- 첨단기술분야 종사자의 보안행동 수칙 -

목 차

1 당신은 세계 산업정보전쟁에 무방비 상태로 노출되어 있다.

최근 세계각국은 자국의 생존권 확보 전략 차원에서 첨단기술개발에 주력하는 한편, 다른 나라가 보유한 첨단기술을 입수하기 위해 수단과 방법을 가리지 않는 치열한 경제전쟁을 전개하고 있어 이제 외국으로부터 우리의 첨단기술을 보호하는 문제는 국가안보의 중요한 요소로 등장하였다.

최근 세계경제포럼(WEF)은 「2003~2004년 세계경쟁력보고서」에서 우리나라의 기술경쟁력이 세계 102개국 가운데 미국, 핀란드, 대만, 스웨덴, 일본에 이어 6위를 기록했다고 밝혀 우리나라가 세계 각국으로부터 첨단산업기술 유출의 표적지화 될 가능성이 점차 농후해 지고 있는 실정이다.

냉전종식에도 불구하고 외국의 정보수집 활동은 오히려 증가하고 있어 공무원뿐 아니라 비즈니스맨들도 이러한 위협에 직접 노출되어 있는 것이 현실이다.

매년 국내에서도 기업의 영업비밀이 절취되는 사례가 크게 증가하고 있는 가운데 전세계의 주요 언론들은 첨단기술을 보유한 국가들 간에 벌어지고 있는 국제 산업스파이 사건들을 심도있게 보도

하고 있다.

국경없이 진행되고 있는 산업스파이 전쟁 속에서 당신은 국내외 구별없이 언제 어디에서든 산업스파이들의 목표가 될 수 있으며, 특히 해외출장시에는 출장국가 또는 제3국의 정보활동 대상이 되어 정보를 탈취 당할 수 있다.

정보수집활동은 국가정보기관, 연구소, 정부투자기업, 사기업체, 테러조직에 의해서도 진행되고 있으며 최근에는 외국정보기관 요원이 단순히 과학자로 위장하여 수집하던 고전적 수법보다는 전문지식으로 무장하여 회의에 참석하는 등 직접 정보수집 활동에도 나서고 있다.

이렇게 전문지식을 바탕으로 할 때 정보수집 요원들은 각종 회의석상에서 다양한 질의를 통해 더 정확한 정보를 얻을 수 있기 때문이다.

각 국은 한국의 정치 · 경제 · 산업 · 군사 등 全 분야를 수집대상으로 하고 있다. 기술정보 뿐만 아니라 경쟁업체의 조직 · 운영상의 정보, 혹은 개인 신상정보도 수집대상이 되고 있다.

이 자료에 제시된 요령을 익히고 정보요원들의 기본수법을 이해함으로써 외국 경쟁업체 · 정보기관의 정보활동을 피할 수 있을 것이다.

또한 소개된 보안관리 요령을 통해 각국의 위협을 이해하고 이에 대처하는 방법과 행동요령을 습득할 것으로 기대된다.

2 정보수집에는 다양한 수법이 동원된다

각 국의 정보수집 활동은 그 나라의 문화수준, 장치체제, 商 관습, 자원(시간, 인력, 자본) 및 기술 경쟁력 등과 맞물려 매우 복잡한 방법으로 전개된다. 최소의 비용으로 노출되지 않고 목적을 달성하기 위해 먼저 수집계획을 작성하고, 컴퓨터, 소형 전자감시 장비 등 도구를 활용하기도하며 특수요원 투입, 포섭, 미인계, 협박 등 고전적 정보수집 수법도 여전히 사용하고 있다.

또 노출되지 않고 은밀히 정보를 획득하기 위해 남의 눈에 띄지 않는 평범한 차림으로 때로는 적극적으로 통제구역 관계자에게 질문을 하거나 호텔에서 소지품을 뒤지고 개인 노트북 컴퓨터를 훔치기도 한다.

다음은 당신이 경계해야 할 외국의 정보수집 방법을 소개한다.

유도 심문

- 자연스럽게 일상적인 대화를 하면서 개인신상, 직업, 주변인물 등에 대한 정보를 유출해 낸다.
- 유도심문은 매우 교묘하여 공무원 · 기업가들은 쉽게 그 진의를 간파할 수 없다.
- 상대방을 편안하게 만들어 경계심을 없앤다.
- 정보수집을 위해 기술적으로 접근한다는 것을 인식하기 어렵다.
- 상대방이 쉽게 거절할 수 없는 질문도 자연스럽게 한다.

도청

- 대화를 엿듣는다. 자연스럽게 곁에 다가가서 엿듣거나 녹음기, 비디오 등 장비를 활용하기도 하며 공공장소, 대중교통, 식당, 카페, 휴게실 뿐 아니라 자기 신상과 업무에 대해

대화하는 사교 모임을 이용하기도 한다.

- 경우에 따라 교통감시 · 보행자감시 카메라 등을 사용한다.

무단 침입

- 서류 · 시청각 자료를 절취 · 복사하거나 도청장치 설치 등을 목적으로 사무실, 제한구역, 전자장비실에 침입하기도 한다.
- 거주지, 투숙호텔 등에 대한 무단침입은 해외출장지 정부, 제3국 정보기관 또는 외국기업 등에 의해 이루어지며 종종 호텔 종업원들의 협조를 얻기도 한다.
- 또한 몇몇 외국기업은 정보수집 대상기업의 컴퓨터망에 침투할 수 있는 해킹장비를 보유하고 있다.

무단침입의 증거

- 누군가가 노트북 컴퓨터를 사용한 흔적이 있거나 손상된 경우
- 포장이 개봉되었거나 다시 봉한 흔적이 있는 경우
- 여행용 가방의 자물쇠가 없어졌거나 강제로 열려고 시도한 흔적이 있는 경우
- 물품을 아예 분실한 경우

통신 도 · 감청

- 이동통신, PDA와 같은 개인 통신장비에 대한 비합법적 · 합법적 도 · 감청 · 행위가 점차 증가하고 있다.
- 각국의 통신사는 대부분 해당 정부의 통제를 받고 있기 때문에 특히 통신감청에 취약하며 사무실, 호텔 등의 유무선 전화가 모두 타켓이 된다.

※ 대다수 국가들이 상업적으로 이용되는 암호체계를 해독하고 감청할 만한 능력을 보유하고 있어 팩스, e-mail 등도 감시 가능

어떻게 자신과 회사를 보호할 수 있을까?

가. 평상시 보안행동 수칙

지켜야 할 것

- 빈손으로 출근, 빈손으로 퇴근한다.
- 불요불급하지 않는 문서는 복사하지 않는다.
- 비밀이 포함된 문서나 자료 또는 폐지, 휴지는 반드시 폐기하며 당 한 장이라도 함부로 버리지 않는다.
- 입 조심하기를 마치 병마개 같이 하여 "말로만의 보안"을 강조하거나, "너만 알고 있어"라며 비밀을 흘리지 않는다.
- 작은 정보라도 경쟁사에 큰 도움이 될 수 있다는 것을 명심한다.
- 업무수행관련 지식이나 노하우는 문서화하여 지적자산으로 등록 후 활용한다.
- 통제구역은 알 필요도 없고 갈 필요도 없으며 무단출입하지 않는다.
- 3內(작업시 視內, 결재시 手內, 보관시 函內)의 원칙을 항상 지키며 비밀자료가 보관된 문서함은 반드시 잠근다.
- 비밀유출의 주된 경로는 항상 내부에 있음을 명심하자.

- 퇴근 때나 자리를 잠시 비울 때에는 방치되는 자료가 없도록 항상 정리 정돈한다.
- 전출 또는 퇴직시 보유하고 있는 모든 비밀문서는 반납한다.
- 사내 상주 외부인(외국기술고문 및 고용인, 컨설턴트, A/S업체)에 대한 내부정보 제공은 정보유출의 경로가 됨을 명심하자.
- 내 주변에 누군가가 기밀을 탐지하고자 기도하고 있을 가능성을 항상 명심하여 보안상의 허점은 없는지 살펴보고 점검한다.
- 보안의 취약부분은 항상 보안담당자에게 통보하고 조치하며, 보안사고 발생시 은폐하지 말고 보안관리자에게 즉시 보고하여 대처한다.
- 내방객의 사무실 출입을 최대한 억제한다.
- 문서류, 디스켓, CD를 승인없이 무단 반출하지 않는다.
- 모든 PC는 반드시 부팅 패스워드를 적용하여, 화면보호기 기능과 암호를 설정한다.
- 공유 폴더를 사용하는 경우에는 반드시 암호를 설정한다.
- 바이러스 검색 및 예방 소프트웨어를 설치하고 초기 동작 시에 작동토록 하며 항상 최신 버전을 유지하도록 자동 업데이트한다.
- 시스템을 사용하지 않을 때나 자리를 비울 때는 반드시 로그아웃한다.
- 인터넷 브라우저 보안레벨은 사용업무에 따라 적정한 레벨로 조정 사용한다.
- 외부로 메시지(e-mail, FTP 등)를 전송할 때는 반드시 회사에서 지급한 계정만을 사용한다.

버려야 할 것

- 업무 편의를 이유로 의도적으로 비밀등급을 하향 조정한다.
- 직위 등을 내세워 절차나 규정을 무시한다.
- 우리 부서에는 비밀이 될 만한 문서가 없다고 생각한다.
- 비밀자료를 사유화 또는 死藏化한다.
- 문서를 필요이상으로 복사, 이면지로 사용하거나 함부로 휴지통에 버린다.
- 기업비밀 · 연구자료 등이 포함된 중요문서를 충분한 보안성 검토없이 무단 폐기, 폐지 등으로 외부 반출되도록 한다.
- 퇴근시 자료 및 서류를 책상 위에 그대로 방치한다.
- 여행시 · 술집 등에서 접촉하는 상대방에게 신원 확인없이 자신이 알고 있는 회사비밀을 과시하고 자랑하거나 업무내용을 알려준다.
- 퇴직한 옛 동료나 혈연, 지연, 학연 등으로부터 요청을 받고 대외보안이 요구되는 회사 비밀자료를 제공한다.
- 내방객을 불필요하게 사무실로 안내한다.
- "규정은 규정이고 현실은 현실이다.", "보안수칙은 업무를 저해하는 번거로운 것이다" 라고 생각, 보안수칙 및 절차를 무시한다.
- 동료의 보안위반 사실을 공공연히 눈감아 준다.
- 네트워크 공유 사유가 소멸되었는데도 공유해제를 소홀히 한다.
- 사내 정보를 허가되지 않은 개인용 컴퓨터 또는 Web Hard 등 저장매체에 저장, 사용한다.
- 인가된 전문가 아닌 아무에게나 장비를 점검 보수한다.
- 불법 소프트웨어, 비인가 소프트웨어 등을 업무용으로 사용한다.
- e-mail을 통해 허가되지 않은 자료 및 중요

데이터를 유출한다.

- 전산 출력물을 규정에 따라 처리하지 않는다.
- 공통 ID나 부서 관리자 ID를 개인용도로 사용하며, 사용자 ID를 타인에게 대여하거나 패스워드를 알려준다.

나. 해외 출장시 보안행동 수칙

위험도를 낮추자

외국 체류시 당신의 행동에 따라 기밀 정보를 절취 당할 가능성을 높일 수도 낮출 수도 있다.

하지만 당신의 방문목적을 숨기기가 힘든 경우도 있다.

해외기술세미나에 참석한다면 당신은 정부 프로그램 또는 기업 프로젝트와의 연관 관계를 드러낼 수밖에 없다.

당신이 입고있는 옷도 주변 사람들의 주목을 끌게 하는 요인이 될 수 있다.

꼭 필요한 경우가 아니면 기업의 로고가 들어간 옷을 입지 않도록 한다. 이런 신중한 행동은 범죄, 대중 소요 사태, 테러 등으로부터 당신을 보호할 수 있다.

행동 수칙

- 출발 전 당신이 방문할 국가에 대해 숙지하라.
  ※ 외국 정보기관의 정보수집 위협, 범죄문제, 교통수단 문제 등
- 여행사, 호텔 관계자에게는 당신의 출장목적 등 출장과 관련된 정보 노출을 최소화하라.
- 출장 중에는 업무와 관계없는 사람에게 기업의 현안사항, 그리고 회사내 직책 · 경력 · 담당업무 등 관련 정보를 언급하지 마라.
- 당신에게 접근, 의도가 불명확한 질문 또는 추궁하는 듯한 질문을 하는 사람은 무시하고 명확하지 않은 대답으로 일관하라.
- 컴퓨터, PDA 등 장비를 휴대하지 못하게 될 경우에는 이동식 저장 장치(플로피 디스크, 외장형 하드디스크, USB 메모리, CD-ROM 등)에 담아 항시 휴대한다.
- 대중 교통 등 공공장소에서는 업무상 비밀, 영업비밀 또는 민감한 정보에 대해 얘기하지 않는다.
- 기업의 민감한 정보 또는 영업비밀에 관해 발설해야 할 경우에는 기업의 자체 보안 가이드라인에 따른다.
- 비밀 또는 민감한 정보를 전송할 때는 타국의 컴퓨터, 팩스 또는 전화를 사용하지 않는다.
- 의심이 드는 특이한 상황이 발생한 때는 현지 주재 한국공관 또는 기업의 자사 등에 문의한다.

4 이런 사람은 산업스파이로 의심해야 한다

- 본인의 업무와 관련없는 다른 직원들의 업무에 대해 수시로 질문하는 사람
- 사진장비를 지나치게 많이 사용하는 사람
- 본인의 업무와 관련이 없는 다른 부서 사무실을 빈번히 출입하는 사람
- 연구실 · 실험실 등 회사기밀이 보관되어 있는 장소에 주어진 임무와 관계없이 접근을 시도하는 사람
- 평상시와 다르게 동료와의 접촉을 회피하거

나 최근 정서변화가 심한 사람

- 주요 부서에서 근무하다가 이유없이 갑자기 사직을 원하는 사람
- 업무를 빙자 주요기밀 자료를 복사, 개인적으로 보관하는 사람
- 주어진 임무와 관련 없는 D/B에 자주 접근하는 사람
- 사람이 없을 때 동료 컴퓨터에 무단 접근하여 조작하는 사람
- 특별한 사유없이 일과 후나 공휴일에 빈사무실에 혼자 남아 있는 사람
- 기술 습득보다 고위 관리자나 핵심 기술자 등과의 친교에 관심이 높은 연수생
- 연구활동보다 연구성과물 확보에 지나치게 집착하는 연구원
- 시찰, 견학을 하면서 지정된 방문코스 외에 다른 시설에 관심을 갖고 있는 방문객

5 여러분의 신고가 국익 손실을 방지한다.

외국 경쟁업체 · 정보기관의 정보수집 활동을 차단하는 대응활동은 여러분의 작은 관심과 경계의식에서부터 시작된다. 여러분의 작은 신고가 국익을 위해 큰 역할을 한다는 사실을 명심할 필요가 있다.

작은 내용이라도 신고하는데 주저하지 말아야 한다. 외국 경쟁업체 · 정보기관은 정보수집을 위하여 다양한 활동을 펼치고 있다. 단편적인 내용도 커다란 첨단기술 해외유출 기도사건의 일부분일 수 있다.

의심스러운 사건이 해외 체류시 발생한 경우

- 당신이 외국에 체류한다면 의심스러운 사건을 가까운 한국공관 또는 국가정보원(www.nis.go.kr 또는 ☎ 111)에 신고한다.
- 외국에서 기술유출 관련정보 등 민감한 사항을 기업보안 담당자에게 보고해야 할 경우에는 보고 받는 사람은 신분이 확실한 한국인으로 제한한다.
- 당신이 한국으로 복귀한 후 조직의 보안담당부서에 사건을 보고한다.

의심스러운 사건이 한국 내에서 발생한 경우

- 해당 조직 내규에 따라 사건을 보고한다.

산업기밀보호 상담센터

★ 막대한 예산 · 인력 · 시간을 투자하여 어렵게 개발한 국내첨단기술을 보호하기 위해 국가정보원은 산업기밀보호상담센터를 설치, 신고상담 전화 111을 24시간 운영하고 있습니다.

★ 산업기밀보호 상담센터는 첨단 산업기술유출혐의 산업스파이 색출 및 첨단산업체 보안지도 · 교육 지원 등 국내 첨단 기술보호를 위한 모든 내용에 대해 성실히 상담하고 있습니다.

★ 여러분의 정성어린 신고상담을 기대합니다.

신고 상담전화(국번 없이 111)
www.nis.go.kr

kangg9@naver.com

발특2004/7