외국의 신종범죄 발생현황과 대책

- 한국 경찰의 지능범죄 수사대책에의 시사점을 중심으로 -

《 硏 究 陣 》

연구위원 : 민 수 홍(경기대학교 경찰행정학과 교수)
이 민 식(경기대학교 경찰행정학과 교수)

목 차

< 표 차 례 >

< 그 림 차 례 >

제1장 서 론

21세기를 맞은 현대 사회는 급속히 진행되는 세계화와 기술발전에 따라서 새로운 기회, 새로운 형태의 조직, 그리고 새로운 시장의 창출을 경험하게 되었다. 그러나 사회발전의 효과가 긍정적인 측면에만 국한되는 것은 아니어서 사회가 상업사회에서 지식정보화 사회로 진입하면서 새로운 양상의 범죄가 전개되고 있다. 사회변화와 범죄 사이에는 긴밀한 관계가 있어서 지식정보화 사회의 일반적인 특징이 신종범죄의 특징과 일치한다. 지식정보화 사회는 세계적(global)이고, 어느 곳에서든 쉽게 접근할 수 있으며(accessible), 자동화되고(automated), 부호화(encryption)를 통해서 자신의 신분을 숨길 수 있다. 신종범죄도 세계적인 특징이 있어서 범죄자들은 공간의 한계를 상당히 극복한 가운데 세계 도처에서 범죄를 저지를 수 있다. 과거에는 범죄에 접근하지 못하던 사람들이 이제는 범죄 대상이나 수단에 쉽게 접근할 수 있게 되었고, 생활의 편리를 위해 추진된 자동화로 인해 과거에는 수행하기 어려웠던 범죄들이 이제는 손쉬운 일이 되고 있다. 범죄자들은 또한 자신의 신분을 숨기기 용이해 졌다(Montano, 2001).

사회경제적 영역이 급격하게 변한다고 해서 범죄의 동기마저 변하지는 않겠지만[1], 과거부터 존재하던 범죄가 새로운 방식에 의해서 이루어지는 변종들이 생겨나고 있다. 예컨대, 신원도용범죄(identity crimes) 중에서 절대 다수를 차지하는 절도는 인류의 역사와 함께 있어온 범죄이지만 인터넷과 전자금융거래 등의 새로운 방법이 사용되면서 금세기 가장 빠르게 증가하는 범죄로 불리게 되었다. 고전적인 범죄유형인 화폐위조도 디지털 복사 및 인쇄기기의 발달에 따라 각국 정부를 위협하고 있으며, 세계 시장에서 치열하게 경쟁하는 기업들은 디지털 신무기로 무장한 산업스파이들로부터 자신들이 개발한 지식과 정보를 보호하기 위해 안간힘을 쓰고 있다. 인류의 편의를 위해서 개발된

1) 이러한 시각은 범죄학 이론의 한 축인 고전주의(Beccaria, 1963; Bentham, 1970)에 기초하고 있다. 이기적이고 쾌락추구적인 인간의 본성을 가정하고 범죄가 인간의 이러한 욕구를 즉각적이고 손쉬운 방법으로 충족시키는 경향이 있다고 했을 때, 특정한 일부 사람들만 범죄의 동기를 갖는 것이 아니라 모든 사람이 동기를 가지고 있다는 것이다. 이러한 시각에 동의하지 않는 학자들은 21세기의 범죄를 완전히 새로운 형태의 범죄로 보기도 한다(Etter, 2001).

기술과 정보가 범죄자들에 의해서 사용되면서 새로운 위험이 생겨나고 있는 것이다.

지식정보화 사회에서 범죄활동은 더 빠르게 일반화되지만 피해자는 피해사실과 피해정도를 모를 수 있고, 불법활동과 합법활동 사이의 경계가 불분명해 질 수도 있다. 그리하여 21세기에는 범죄수행이 용이해지는 반면 경찰이 범인을 검거하기는 더 어려워질 것으로 예상된다. 범죄통제를 책임지는 경찰은 변화하는 환경 속에서 다가오는 미래를 대비하기 위해서 다음과 같은 질문을 하게 된다.

1) 새로운 범죄기회를 만들어 내는 요인들은 무엇인가?
2) 범죄를 예방하고 발견해 내는 데는 어떤 어려움이 예상되는가?
3) 경찰로부터 시작되는 형사사법체계가 예상할 수 있는 어려움은 무엇이고 이에 어떻게 대비해야 하는가?

앞으로 일어날 범죄문제를 대처하기 위해서는 이상의 질문들에 대한 답변을 준비해야 한다. 그러나 장래에 일어날 일을 직접 예측하기 어렵기 때문에 우리사회보다 앞서서 새로운 유형의 범죄를 경험하고 있는 선진국들의 경험을 연구 분석함으로써 한국경찰이 미래의 범죄문제를 효과적으로 대비하는 것이 현실적으로 바람직하겠다. 이에 본 연구는 외국의 신종범죄 가운데 주요한 3가지(identity crime, 산업 스파이, 유가증권 및 화폐의 위조)를 선정하여 이들의 발생현황과 대책을 알아보았다. 특별히 한국 경찰이 신종범죄를 더 잘 통제할 수 있도록 선진외국의 경험 중에서도 우리나라 경찰대책에의 적용가능성과 시사점에 초점을 맞추어 연구하였다.

이하에서 다루어진 본 연구의 내용은 크게 세 부분으로 구성되어 있다.

제2장은 신원도용범죄(identity crime)의 개념, 유형, 외국의 실태와 추세를 개괄적으로 다루고, 외국의 연구에서 밝혀진 원인과 외국의 대응 및 입법을 소개하였다. 신원도용범죄를 담당하는 실무자를 위한 지침을 제시하면서 '피해자 점검표'를 <참고 1>에 첨부하여 실무에 적용할 수 있도록 하였다.

제3장에서는 산업스파이를 다룬다. 상업적 목적에서 수행되는 스파이 활동이 국가의 안보를 해칠 수 있기 때문에 경찰 등 형사사법기관의 수사역량을 강화해야 할 영역이다. 산업스파이의 개념과 유형을 살펴보고, 외국의 사례로 미국, 독일, 일본, 기타 외국의 경우를 정리하였다. 선진국에서 시행하고 있는 영업비밀의 보호와 산업스파이 대응체계를 미국, 독일, 일본, 유럽연합 등으로 나누어 살펴보고, 한국 상황에의 시사점을 제시하면서 '산업기밀 보호관련 법령'과 '산업기술보호대책'을 <참고 2>와 <참고 3>에

첨부하였다.

제4장은 최근에 국제적으로 큰 관심거리가 되고 있는 초정밀 위폐를 포함하는 화폐 및 유가증권의 위조를 다룬다. 화폐 및 유가증권 위조의 개념과 유형을 정리하고, 우리나라를 비롯하여 미국, 캐나다, 유럽연합의 위조 실태와 사례를 살펴보았다. 화폐와 유가증권의 위조에 대한 외국의 입법과 대응체계를 소개하면서 우리 상황에의 시사점을 정리하였다.

본 연구를 위해 외국의 관련 전문서적, 국내외의 학술지, 보고서, 신문 등을 참고하였고 외국 형사사법기관의 홈페이지에서 최신 정보를 수집하기도 하였다. 이해를 돕기 위해 필요한 부분에서는 <그림>과 <표>를 제시하였다.

하지만 신종범죄의 특성상 선진외국에서도 원인은 고사하고 정확한 실태마저 파악되어 있지 않은 경우가 많고, 외국 형사사법기관이 가지고 있는 중요 자료에는 접근할 수 없어 다루지 못한 점이 아쉽다. 본 연구에서 다루지 못한 부분은 이후의 계속적인 연구를 통해서 보완되기를 기대한다.

제2장 신원도용범죄(Identity Crimes)

타인의 신상정보를 이용한 범죄를 통칭 identity crime이라고 부르고, 이것은 21세기의 새로운 범죄 중 하나로 금세기에 가장 빨리 성장하는 범죄로 알려져 있다[2] (Newsweek, 2005.7.6). 미국의 연방거래위원회(Federal Trade Commission(FTC))의 조사 보고서(2003b)에 따르면, 미국에서 지난 1년 동안 1,000만 명 정도가 이 범죄의 피해자가 되었고, 그 비용도 대략 $50억[3]에 이른다고 한다. 이 범죄의 심각성은 누구든지 피해자가 될 수 있다는 점이다. 현대 사회를 살면서 우리는 모든 생활영역에서 신상정보의 흔적을 남기게 되었고 그만큼 피해의 가능성도 높아졌다(Graycar, 2001). 피해자는 금전적인 손실을 입을 수 있고, 손상된 신용등급을 바로잡기 위해 많은 시간과 노력을 투자해야 한다. FTC의 조사에 의하면, 피해자의 절반정도는 신용절도범이 자신의 개인정보를 어떻게 획득했는지 알지 못한다. 대략 25% 정도만이 자신의 신용카드, 신분증, 개인수표, 우편물을 도둑맞거나 분실했다고 밝히고 있다. 더욱이 신상정보의 오용으로 인해 전과를 갖게 된 피해자들도 있다. FTC 조사에 응답한 피해자가운데 4% 정도는 신용절도범이 경찰의 검문검색을 받거나 범죄사건으로 고발될 때 훔친 신상정보를 사용했다고 밝혔다. 범죄기록을 지우는 것은 매우 어려운 일이다. 그 결과 많은 피해자가 양산되면서 이들은 주변 사람들을 믿지 못하게 되고 더 나아가 의심하게 되면서 사회해체를 조장하게 된다.

최근에 역사상 최대의 개인정보 도난사건이 미국에서 발생했다. 카드 시스템스 솔루션이라는 미국의 한 회사가 신용카드 거래를 처리하는 과정에서 개인정보 보호를 소홀히 하여 신용카드 정보 4,000만 건이 해커들에게 노출되었고 이 정보들이 불법 거래되면서 피해자가 전 세계적으로 퍼져나가고 있다. 이 사건으로 한국인 14,000여 명의 신용정보가 유출된 것으로 알려져 있다. 즉 미국에서 신용카드로 물건을 샀거나 국내에서 온라인으로 미국회사의 상품을 구입한 신용카드 이용자 중 일부의 정보가 유출된 것이

2) 미국의 연방거래위원회(FTC)가 수행한 조사에서 identity crime은 가장 빠르게 증가하고 있는 범죄로 지목되었고, 이러한 조사결과는 2003년 9월 3일에 출판되었다.

3) 미국의 연방거래위원회(FTC) 위원장이 미국의회에서 증언한 바에 따르면 개인정보 절도 피해액이 1년에 530억$에 이른다고 한다. 이 가운데 소비자들의 직접적인 피해액이 50억$ 이며 나머지는 주로 소매업체와 사업자들이 부담하게 된다.

다. 유출된 정보는 신용카드 번호, 유효기간, 이용자 이름 등이다. 다행히 우리나라에서는 이 사건으로 인한 피해가 보고되고 있지 않지만 가까운 일본에서는 카드 고객의 손해가 발생한 것으로 알려져 있다(중앙일보 2005. 6. 23). 이 사건을 통해서 한 개인의 주의와 노력만으로는 신원도용범죄를 예방하기 어렵다는 사실을 알 수 있다.

Identity crime의 폐해를 인식하기 시작한 언론매체들은 identity crime 중에서도 identity(ID) theft를 현대사회에 대한 심각한 위협으로 보고 집중적인 보도를 하고 있다. CBSnews.com에서는 "매 79초마다 절도범이 누군가의 신상정보를 훔쳐서 피해자의 이름으로 계좌를 개설하고, 물건을 마구 사들인다"고 그 심각성을 지적하였다. 미국정부(United States General Accounting Office(USGAO), FTC, Office of the Inspector General, Federal Bureau of Investigation(FBI))나 사설 단체들도 점증하는 identity theft의 문제를 한 목소리로 경고하고 이 문제의 해결을 위해 노력하고 있다.

1. Identity Theft의 개념

미국 법무부는 identity theft와 개인정보관련 사기를 정의하면서 누군가가 다른 사람의 개인정보를 불법적으로 획득하고 사기와 기만의 방식으로 사용하여 주로 경제적 이익을 얻어내는 모든 종류의 범죄를 일컫는 폭 넓은 개념으로 보고 있다. 구체적인 형태로는 범죄자들이 다른 사람의 이름, 주소, 생년월일, 신원을 나타내는 번호(우리나라의 경우 주민등록번호 그리고 미국의 경우에는 사회보장번호), 여권번호, 운전면허증에 나타난 정보, 신용카드번호나 은행계좌번호, 전화카드 번호 등과 같은 남의 신상정보를 도용하는 것이다. 최근에는 개인의 생물측정학적 정보인 지문, 성문(voice print) 혹은 망막정보의 도용도 추가되고 있다. 이러한 방식으로 피해자의 은행계좌 등에서 돈을 인출해 가기도 하고, 피해자의 이름으로 휴대전화(소위 대포폰)를 만들거나, 피해자 명의의 자동차(소위 대포차)를 불법 거래하거나 이용하는 등 그 수법이 다양하다. ID theft는 그 자체가 일차적인 목표인 경우가 많지만 명의자와 사용자가 다른 대포폰이나 대포차의 경우처럼 종종 다른 범죄에 악용될 가능성도 존재한다.[4)]

4) 우리나라에서 다른 사람의 명의를 도용해서 개설한 휴대전화를 이용하여 여성 운전자만 골라 주차된 차를 옮겨 달라고 전화한 뒤 차를 빼러 나온 운전자를 협박해 금품을 빼앗은 사람이 구속되기도 했다(중앙일보 2005. 6. 23).

ID theft의 특징은 자기도 모르는 사이에 피해자가 될 수 있고, 피해를 회복하기까지 긴 시간과 노력, 비용이 소용된다는 점이다. 예컨대, 누군가가 당신의 개인정보를 훔쳐서 당신 이름으로 새로운 은행계좌를 만들거나, 당신 이름의 신용카드를 만들어 사용하되 고지서는 다른 곳으로 배달되게 하여 당신은 신용카드 사용내역을 알지 못하고, 당신이름으로 부정수표를 사용하거나, 당신의 은행계좌에서 돈을 빼내거나 다른 계좌로 이체하고, 파산을 신청하고, 당신 이름으로 취업을 하거나, 주택구입 융자금을 신청하거나 자동차나 휴대전화를 할부로 구입할 수 있다. 당신에게 이런 일이 발생해도 사실을 알기까지는 몇 달이 지나야 가능하다. 물론 미국의 연방법은 신용카드 사기사건의 경우에 소비자의 책임한도를 계좌당 $50로 정하고 있고, Visa나 Master 카드사는 소비자에게 부담을 지우지 않는다. 그러나 진정한 문제는 당신의 신용을 회복하는 일이다. California주의 한 공익조사기관이 수행한 설문조사에 의하면 identity theft 피해자가 신용을 회복하기 위해 사용한 금액은 변호사비를 제외하고 $30 ~ $2,000로 나타났다. 피해자는 사건발생 이후에 손상된 신용을 회복하기 위해 대개 2년 넘는 기간에 평균 175시간을 투입하고 평균 손실액은 $808로 나타났다.

2. Identity Theft의 유형

Identity theft는 신원도용범죄를 통해 직접적으로 금전적인 이익을 추구하는 것과 또 다른 범죄를 저지르기 위해 신원도용범죄를 저지르는 것의 2가지 유형으로 나눌 수 있다. 금전적인 이익을 추구하는 identity theft에는 신용카드사기, 부정수표 사용 등이 포함된다. 또 다른 범죄를 저지르기 위한 identity theft는 Newman(1999)이 제시한 유형으로, 절도범들이 identity theft를 이용하여 신분을 위장한 채 자신들이 의도한 불법 활동을 수행한다. 테러리스트들이 이 부류에 속하는 경우로 이들은 자신들에게 주어진 임무를 자유롭게 수행하기 위해서 ID 범죄를 사용한다. 미국에서 2001년에 발생한 9.11 사건의 테러리스트들은 자신들의 신원과 동기를 감추기 위해 identity theft를 이용하여 부정 운전면허증을 발급받은 바 있다. 이 연구에서는 신원도용범죄를 통해 직접적으로 금전적인 이익을 추구하는 유형에 초점을 맞추어 살펴보았다.

Identity 절도범들이 개인 신상정보를 얻는 방법은 다양하다. 신상정보 취득 방법을 3

가지로 분류하여 ①가짜 신상정보를 만드는 경우, ②실제 신상정보를 얻거나 훔치는 경우, 그리고 ③기존의 신상정보를 변조하는 경우로 나누기도 한다(Cornall, 2001).

또 다른 분류방법은 사용된 기술수준에 따라서 낮은 수준의 기술이 사용된 경우와 고도의 기술이 사용된 경우로 2분하는 것이다. 낮은 수준의 기술은 상대적으로 손쉽게 사용할 수 있기 때문에 가장 빈번하다. 낮은 수준의 기술이 사용된 구체적인 예로는 지갑이나 가방을 훔치는 방법과 Dumpster diving으로 불리는 쓰레기통을 뒤지는 방법이다. 후자는 개인의 쓰레기통을 뒤져 신상정보를 얻어 낸다. 반면에 고도의 기술이 사용된 경우는 숙련과 전문기술을 필요로 한다. 여기에는 인터넷의 사용, skimming, pretext calling 등이 포함된다. Skimming은 범법자가 ATM이나 신용카드의 자기테이프에 암호화되어 있는 정보를 컴퓨터를 이용하여 읽어내고 저장하는 것이다. 일단 저장된 정보는 다른 카드의 자기테이프에 재 암호화하여 입력함으로써 피해자의 것과 동일한 ATM 혹은 신용카드를 복제해 내게 된다(Federal Trade Commission, 2000). Pretext calling은 범법자가 피해자의 개인정보를 얻어낼 목적으로 자신의 신분을 속인 채 피해자에게 접촉을 하게 된다(Newman, 1999).

Identity 절도범들이 개인의 신상정보를 얻는 방법을 다음의 유형으로 분류하여 정리하였다.

- 우편: 배달되어 오는 편지와 (경우에 따라서는) 보내는 편지가 들어 있는 우편함은 손쉬운 절도의 대상이 된다. 절도범은 우편물 가운데 신용카드 대금청구서, 은행에서 보내 온 우편물을 찾아내어 정보를 훔치게 된다. 개인수표를 사용하는 미국의 경우에는 check washing이라는 방법도 사용된다. 우편물 속에 들어 있는 개인수표의 금액을 고치고 수령인을 절도범 자신으로 고쳐서 현금화하게 된다. 특별히 주의할 사항은 신용카드 회사에서 새 카드를 보내오는 메일을 조심해야 한다. 절도범이 새 카드를 손에 넣게 되면 손쉽게 신용카드 사기로 이어진다.
- 부정한 주소변경: 절도범이 우체국이나 피해자의 신용카드 회사에 주소변경 양식을 접수시켜서 우편이나 고지서가 절도범 자신의 주소나 다른 수취인의 주소로 배달되게 한다.
- 쓰레기 통: 절도범은 상점이나 큰 건물에 붙어 있는 대형 쓰레기 수납장에서 상점

이나 고객의 계정정보가 담겨진 채 버려진 편지를 찾는다. 다른 사람의 의심에서 벗어나기 위해 쓰레기를 뒤지는 걸인이나 청소원으로 가장하기도 한다.

- 주변의 구경꾼: 현금인출카드나 신용카드, 신분증 등을 공공장소에서 꺼내면 절도범이 관심을 갖고 볼 수 있다. 절도범들은 대게 유동인구가 많은 지역에 설치된 현금인출기 근처에서 피해자를 물색한다. 이들은 줌 기능이 있는 카메라나 캠코더 혹은 망원경의 도움을 받아 멀리 떨어진 곳에서 정보를 훔쳐보기도 한다.
- 분실된 혹은 훔친 지갑: 절도범이 누군가 분실한 지갑을 손에 넣거나 누군가의 지갑을 훔치게 되면 많은 신상정보를 얻게 된다. 이런 경우를 대비하여 지갑에서 주민등록번호 등 중요 신상정보가 들어 있는 신분증을 빼 놓는 것이 바람직하다.
- 사업장: 사업체의 피고용인이 합법적인 이유에서 수집해 놓은 정보를 불법적으로 검색할 수 있다. 금융기관에서 일하는 하위직 피고용인이 타인의 신상정보에 접근하여 불법으로 취득한 정보를 절도범들에게 팔 수 있다.
- 인터넷: 컴퓨터에 정통한 범죄자는 인터넷을 사용하여 손쉽게 피해자를 찾아 낼 수 있다. 절도범은 피해자의 개인 웹 페이지에서 신용카드나 은행계좌의 비밀번호로 자주 사용되는 생일, 전화번호 등의 가계정보를 찾아낸다.
- 자기테입 판독기(skimmer): 판독기를 이용하여 은행카드나 신용카드의 자기테이프에 입력된 계좌번호, 잔고, 확인 암호(verification code)를 알아낼 수 있다. Skimmer를 이용한 절도범들은 신용카드를 받는 매장에 근무하면서 정보를 빼내기 때문에 찾아내기가 어렵다. 결제를 위해 신용카드를 건네면 먼저 정상적인 카드 판독기에 넣은 다음에 카드주인 몰래 skimmer를 사용하여 불법적으로 정보를 빼내게 된다.
- Pretexting: 피해자가 거래하고 있는 믿을만한 회사의 직원으로 가장하여 피해자에게 전화를 걸어 개인신상정보를 캐내는 경우를 말한다.
- 중고 PC 하드 디스크: 미국에서 MIT 대학원생 두 명이 158개의 중고 하드 디스크 드라이브를 구입하여 그 안에 담겨진 자료를 조사한 적이 있다. 이들은 하드 디스크에서 지워진 파일이나 디렉터리를 복구하여 많은 정보를 얻을 수 있었다. 42개의 드라이브에는 신용카드 번호가 담겨져 있었고, 은행 현금자동인출기에 사

용되었던 것으로 추정되는 드라이브 한 개에는 거의 3000개의 현금자동인출 카드 번호, 계좌번호와 잔고 등이 담겨져 있었다.

컴퓨터에 입력된 자료를 지워도 이것이 쉽게 복구될 수 있다는 사실을 일반인들은 잘 알지 못하고 있다. 파일을 지워도 wiping이나 shredding으로 불리는 과정 즉 지워진 파일 위에 다른 파일을 여러 차례 덮어씌우지 않으면 옛 파일은 여전히 하드 드라이브에 남아 있게 된다(VideoPlus, 2003). 개인의 신상정보유출과 관련해서는 일반인들의 개인 PC 보안관리의식이 보다 근본적인 문제로 지적된다. 버려진 중고 PC의 하드 디스크에서 온라인 금융거래의 신분증으로 사용되는 공인인증서가 발견되는 경우도 많은 것으로 알려져 있다(중앙일보, 2005. 10. 31).

- Phishing: 인터넷 사기 중에서 가장 최근에 주목을 받고 있는 것이 Phishing이다. 개인정보(private data)와 낚시(fishing)의 합성어인 Phishing의 사기범들(phisher)은 불특정 다수(phish)에게 이-메일을 보내 고객의 계정에 오류가 있어 사기를 당할 가능성 혹은 다른 문제가 있으니 신용카드 정보나 개인 금융정보를 업데이트하도록 요구한다. 이 때 정보를 제공하지 않으면 소비자의 계정이 해지된다고 협박하기도 하고, 대출이나 사이트 무료이용 등 달콤한 제안을 하여 자신들이 만든 가짜 금융 사이트로 유인한다. 금융정보의 확인을 요청하는 공신력이 있어 보이는 거짓 이-메일은 아이러니하게도 사기를 두려워하는 소비자들의 두려움을 이용하여 사기를 친다. "Spoofing"이나 "Carding"으로도 불리는 이 사기기법이 너무도 많은 문제를 야기하고 있어서 FTC와 FBI 등은 최근에 Washington D.C.에서 기자 회견을 갖기도 했다.

  대표적인 사건으로는 2003년 말 세계최대 인터넷 경매업체인 eBay 사이트를 위장한 사건이다. 당시 사기범들은 “보안상의 위험으로 계정이 일시 차단되었으니 첨부된 링크를 클릭하여 eBay 홈 페이지에서 재등록하라”는 이-메일을 대량 발송하였다. 이 메일을 받은 이용자들 중 일부는 링크를 따라가서 가짜 eBay 홈 페이지에서 자신들의 신용카드번호, 비밀번호, 사회보장번호, 생년월일 등의 중요한 신상정보를 입력하였다. 우리나라에서도 최근에 가짜 금융 사이트를 이용한 사기가 발견되었다. 적발된 사건의 경우에 대형 포털 사이트의 인터넷 카페에 광고성 글을 남긴 뒤 이를 보고 클릭해 들어오는 이용자들을 유혹하여, 다수의 가짜 금융 사이

트 중에서 거래하는 은행을 고르게 하고, 대출알선을 미끼로 개인정보를 요구한 뒤 이를 이용해 피해자의 은행계좌에서 예금을 빼가는 방식이었다(중앙일보, 2005. 10. 17).

사기범들은 해외 전산망 등 여러 개의 컴퓨터 서버를 거치는 우회경로를 사용해서 가짜 금융 사이트를 만들고, 사기행각을 벌일 때만 사이트를 개설했다가 바로 폐쇄하기 때문에 수사기관도 이들을 검거하기 어려운 상황이다. FTC는 2003년 7월에 phisher로 의심되는 17세 소년을 상대로 그의 스팸메일 발송을 한평생 금지하고 $3,500의 벌금을 내용으로 하는 소송을 제기하였고, 이것은 phishing에 대한 최초의 소송으로 알려져 있다(VideoPlus, 2003).

- 악성코드(Malicious code): 해커들은 Trojan을 이용해 원격으로 입력 정보를 알아내고, Web hacking을 통해 인터넷 웹 페이지에서 ID와 비밀번호를 파악하며, Spyware를 이용하여 컴퓨터 사용자의 신상정보를 빼내기도 한다.

Identity 절도범들은 다른 사람의 신상정보를 훔쳐서 다양한 금융범죄를 저지른다. 구체적으로는 훔친 정보를 이용하여 대출을 받고, 현금 서비스를 받고, 신용카드를 만들거나 극단적인 경우에는 모든 금융계좌를 통제하기도 한다. 절도범들의 목적이 금전적 보상일 경우에 이들이 사용하는 사기기법에 따라서 유형을 분류할 수 있다.

- 절도범은 피해자의 이름, 생년월일, 주민등록번호 등을 이용하여 새로운 신용카드계좌를 개설한다. 그는 카드의 신용한계까지 사용하고는 대금지불을 하지 않음으로써 피해자를 신용불량자로 전락시킨다[5].

- 절도범이 피해자로 가장한 채 피해자의 신용카드 발급자에게 전화를 걸어 신용카드계좌의 주소를 변경한다. 범법자가 신용카드를 이용해도 청구서가 새로운 주소로 배달되기 때문에 피해자는 문제를 바로 알지 못한다[6].

---

5) 미국 오하이오 주의 한 학생이 고등학교 졸업후 처음으로 신용카드를 신청했다가 거절을 당하면서 누군가 자신의 이름으로 4개의 신용카드를 만들어 5만불의 빚을 진 사실을 발견한다. 조사결과 그 누군가는 바로 자신의 아버지임이 밝혀졌다(Silverlake, 2004).

6) 미국 필라델피아에 사는 나이지리아 출신 부부는 공항을 청소하면서 수백명의 신원을 도용하여 피해자 명의의 카드를 만들어 물품을 주문하여 50여개의 빈집으로 배달시켰다가 2002년에 기소되었다(Silverlake, 2004).

- 절도범이 피해자의 이름으로 휴대전화 서비스에 가입한다[7].
- 절도범이 피해자의 이름으로 은행계좌를 개설하고 부도수표를 남발한다[8].
- 절도범이 피해자의 인터넷 서비스 제공자(ISP)로 가장하여 계정정보를 새롭게 갱신해야 하며 등록을 위해 사용한 신용카드가 더 이상 유효하지 않거나 만기가 되었으니 계정을 유지하기 위해서 필요한 정보를 다시 입력하라고 이메일을 보낸다[9].

다른 사람의 개인정보를 훔쳐낸 절도범들은 사기꾼들에게 정보를 팔아넘긴다. 사기꾼들은 훔친 신분을 가지고 음란 사이트를 방문하거나, 자동차를 구입하고, 은행대출을 받고 나서 도주하여 무고한 피해자의 신용기록에 치명적인 손상을 입히게 된다. 피해자는 이 문제가 해결될 때까지 취직도 못하고, 신용카드로 물건을 구입하지도 못하며, 심한 경우에는 여권발급도 제한된다. 결국 피해자는 identity crime의 금전적, 법적, 심리적 피해를 고스란히 떠안게 되는 것이다.

3. 외국의 Identity Theft 실태와 추세

1) Identity theft의 실태

정부기관이나 연구기관 법집행기관들은 identity theft가 증가하고 있다고 주장한다. 이 범죄의 발생빈도에 대한 추정과 관련 피해액의 추정은 중요한 문제이지만 아직까지 경험적인 연구를 통해서 적절히 답변되지 못하고 있다. 이처럼 identity theft의 발생정도를 파악하기 어려운 이유로는 첫째, identity theft를 어떻게 정의할 것인가에 의견합의가 어렵다. 예컨대, 재미삼아 한번 누군가의 신용카드로 물건을 구입한 경우도 포함

7) 최근 한 탈북자는 대포통장과 대포폰을 만들기 위해 중국 브로커에게 140만원을 주고 인적사항을 구입한 혐의로 구속영장이 청구되었다(YTN, 2006. 2. 27). 소위 대포폰은 또 다른 범죄를 저지르기 위해 사용되기도 한다. 2006년 2월 26일에 치러진 토익시험에서 부정행위 알선자는 대포폰을 이용하여 의뢰자에게 답안을 전송한 것으로 알려졌다(YTN, 2006. 3. 1).

8) 국내에서는 500만원짜리 위조수표 뒤에 주민등록증을 분실한 61세 노인의 명의로 이서가 되어 있어 용의자 신원확보에 어려움을 겪기도 하였다(YTN, 2006, 2. 21).

9) 온라인 게임을 위한 적립금을 충전시켜 주겠다고 접근한 거짓 사이트 관리자에게 자신의 통장번호와 실증인증번호를 알려 주었던 한 게이머는 자신의 통장에서 50만원이 인출된 사실을 나중에 확인한 것으로 알려졌다(조선일보, 2006. 2. 16).

시켜야 하는지에 대해 이견이 있다. 둘째, 많은 사건이 신고 되지 않으며 일련의 사건들을 추적해서 계산하기 까지 몇 년이 걸릴 수도 있다. 셋째, identity theft를 전담해서 다룰 기관이 없다. 넷째, identity theft가 은행사기나 신용사기와 같은 다른 금융범죄와 함께 발생하는 경우가 많기 때문에 파악하는데 어려움이 있다. 이러한 이유에서 초기 정부통계는 발생빈도를 실제보다 낮게 파악하는 경향이 있다.

미국의 경우, 연방거래위원회(Federal Trade Commission)가 identity theft에 관한 정보를 수집하는 주요 기관이다. 1998년에 Identity Theft and Assumption Deterrence Act가 통과된 이후로 의회는 연방거래위원회로 하여금 신원증명서의 불법적인 사용에 대한 시민들의 모든 고충기록을 정확히 보관하도록 규정하였다. 연방거래위원회는 1999년 11월 1일부터 정보를 수집하여 온라인상의 데이터베이스를 운영하고 있고, identity theft에 대한 전국자료와 지역자료를 유일하게 제공한다.

<표 2-1> ID Theft 유형별 발생률

지난 1년 사이의 ID Theft 피해경험자	%
새 계좌개설 및 기타 사기	1.5
(신용카드 이외의) 기존카드나 계좌번호 오용	0.7
기존의 신용카드나 신용카드번호의 오용	2.4
총 피해경험자	**4.6**
지난 5년 사이의 ID Theft 피해경험자	%
새 계좌개설 및 기타 사기	4.7
(신용카드 이외의) 기존카드나 계좌번호 오용	2.0
기존의 신용카드나 신용카드번호의 오용	6.0
총 피해경험자	**12.7**

출처: Identity Theft Survey Report, FTC, 2003

미국의 연방거래위원회(FTC)는 identity theft 피해발생률을 추정하고, ID theft가 피해자에게 미친 영향, 피해자가 취한 행동 등을 파악하기 위해 설문조사를 실시하였다. 2003년 3월부터 4월까지 모두 4차례에 걸쳐서 매번 18세 이상 성인 1000여명을 대상으

로 전국적인 규모의 전화면접을 시행한 결과, 모두 4,057명의 성인의 자료가 수집되었다.

<표 2-1>를 보면, 조사 대상자 가운데 1.5%는 지난 1년 사이에 누군가 자신의 신상정보를 오용하여 새 신용계좌를 개설하거나, 대출을 받거나, 보험에 가입하거나, 아파트를 임대했다고 보고했다. 이 퍼센트를 미국 성인전체에 적용해 보면 지나 1년 사이에 323만 명에게 이러한 피해경험이 있었을 것으로 추정된다(<표 2-2> 참조).

<표 2-2> ID theft 유형별 발생률, 손실액, 문제해결에 투입된 시간과 모집단 추정치

	새 계좌개설 및 기타 사기	기존계좌의 오용 (신용카드와 기타카드 포함)	모든 ID Theft
지난 1년 사이의 피해자			
전체 중 %	1.5%	신용카드: 2.4% 기타 카드: 0.7%	4.6%
모집단 추정인원	323만명	668만명	991만명
사업체와 금융기관 손실			
가해자 1인당 평균	$10,200	$2,100	$4,800
추정 총피해액	$329억	$140억	$476억
피해자 손실			
피해자 1인당 평균	$1,180	$160	$500
추정 총피해액	$38억	$11억	$50억
피해자가 문제해결에 사용한 시간			
피해자 1인당 평균	60시간	15시간	30시간
추정 총 사용시간	1억 9400만 시간	1억 시간	2억 9700만 시간

출처: Identity Theft Survey Report, FTC, 2003

조사 대상자 중 2.4%는 지난 1년 사이에 누군가 자신이 갖고 있던 기존의 신용카드 혹은 카드번호를 오용하였으며, 대상자 중 0.7%는 지난 1년 사이에 자신이 갖고 있던

신용카드 이외의 다른 계정(예컨대, 예금계좌나 이동통신계정)의 오용을 경험하였다.

모든 유형의 ID theft를 포함했을 때 전체 조사 대상자 가운데 4.6%가 지난 1년 사이에 ID theft의 피해자가 되었다고 밝혔다. 이것을 미국의 전체 성인 모집단에 적용하면 1000만 명 가까운 미국의 성인들이 지난 1년 사이에 ID theft의 피해를 당했을 것으로 추산된다.

조사기간을 지난 5년간으로 확대하여 보면, 조사 대상자의 4.7%가 이 기간 중에 누군가 자신의 신용정보를 이용하여 새 계좌를 개설하거나 다른 종류의 사기를 쳐서 자신이 피해를 당했다고 밝혔다. 조사 대상자 중 6%는 동 기간 중에 기존의 신용카드나 신용카드번호의 오용 피해를 보고하였고, 2%는 (신용카드 이외의) 기존카드나 계좌의 오용을 보고하였다. 전체 모든 유형을 포함해 보면, 대상자의 12.7%가 지난 5년간 자신의 신상정보가 오용된 피해경험을 갖고 있는 것으로 나타났다.

"새 계좌개설 및 기타 사기"의 가해자는 평균적으로 $10,200 상당의 돈이나 물건, 서비스를 취득한 것으로 나타났다. 이것을 미국의 성인모집단에 적용해 보면, 기업체나 금융기관들은 지난 1년 사이에 이 유형의 ID theft로 인해서 $329억의 손실을 본 것으로 추정된다. 모든 유형의 ID theft를 포함하게 되면 가해자 1인당 평균 $4,800의 부정이익을 얻었고, 전체 피해 추산액은 지난 1년 사이에 $476억에 달한다.

피해자가 직접 당한 손실은 ID theft 의 전체 손실에서 작은 부분에 지나지 않지만, 피해자가 ID theft와 관련된 문제를 해결하는 데는 많은 비용(평균 $500)이 들어간 것으로 나타났다. 특히 "새 계좌개설 및 기타 사기"의 피해자들은 평균 $1,200를 사용하여 피해유형이 심각할수록 비용도 많이 드는 것을 알 수 있다.

ID theft의 피해자는 금전적인 손해 외에 자신의 신상정보 오용으로 생겨난 다양한 문제를 해결하느라 상당한 시간을 투자한 것으로 나타났다. 평균적으로 피해자는 문제해결에 30시간을 사용한 것으로 나타난다. 특히 피해유형이 심각할수록 시간도 많이 들어서 "새 계좌개설 및 기타 사기"의 피해자들은 평균 60시간을 투자했다.

피해자가운데 15%는 자신의 신상정보가 돈과 상관없는 방식으로 오용되었다고 밝혔는데 이 중 가장 일반적인 경우가 가해자가 경찰의 단속에 걸렸을 때 피해자의 신상정보를 사용한 것이다. 피해자의 4%가 이런 경험을 갖고 있었다.

피해자의 신상정보가 오용된 기간도 상당히 길어서 피해자의 13%는 오용된 기간이

6개월 이상이라고 밝혔다. 반면에 모든 종류의 ID theft 가운데 26%는 단 하루 동안 신상정보가 오용된 것으로 나타났다.

대부분의 피해자는 피해사실을 경찰 등에 신고하지 않은 것으로 나타났다. 피해자의 대략 25%정도만이 경찰에 범죄를 신고했다고 밝혔다. 심각한 유형인 "새 계좌개설 및 기타 사기"의 경우에도 43%만이 신고를 해서 과반이 신고를 하지 않은 것을 알 수 있다.

<표 2-3> 2002년에 미국 연방거래위원회에 접수된 Identity Theft 범죄유형

범죄자가 다른 사람의 신원을 도용하여 저지른 범죄유형	%
신용카드 사기	42%
전화 혹은 공공요금 사기	22%
은행 사기	17%
취업관련 사기	9%
정부 공문서 혹은 연금 사기	8%
대출 사기	6%
기타	16%
Identity theft 미수 사건	8%

자료: http://www.consumer.gov/idtheft/

개인의 신상정보가 새나간 이유 중 가장 빈번한 것이 절도에 의해서였다. 즉 지갑이나 우편물을 잃어버리거나 도둑을 맞은 경우 등이 빈번하여서 피해자의 25%정도가 이러한 방식으로 신상정보가 새 나갔다고 밝혔다. 피해자 가운데 대략 절반 정도는 어떻게 하여 자신의 신상정보가 도용되었는지 모르고 있었다.

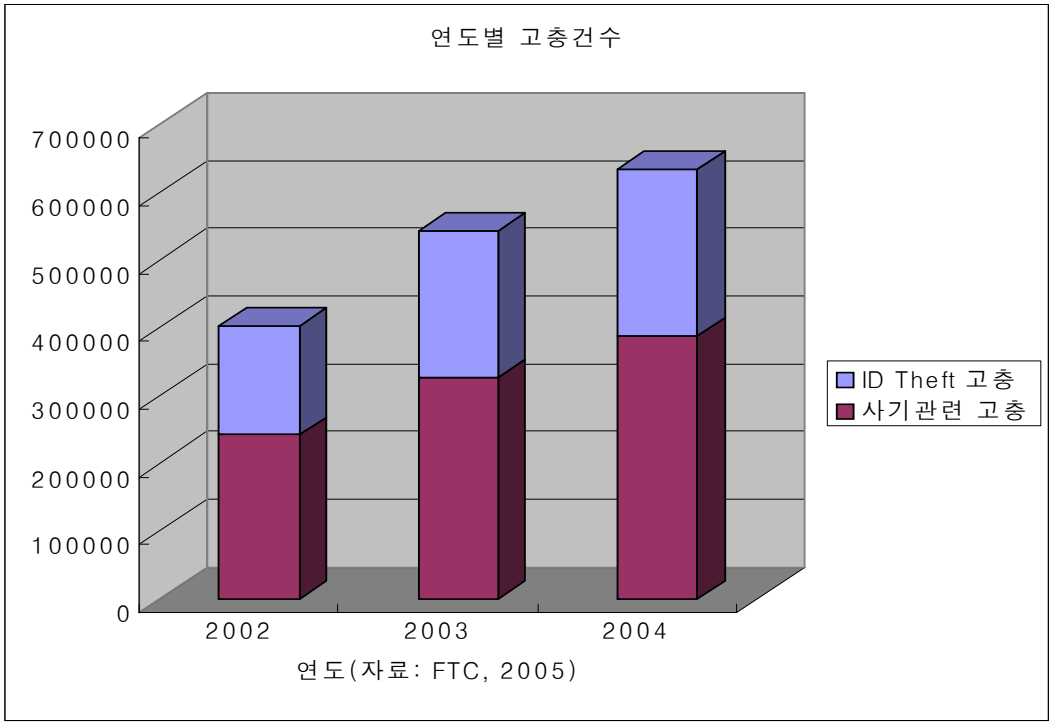
2) Identity theft의 추세

미국의 연방거래위원회에서 만들어 관리하는 소비자 고충 데이터베이스인 Consumer Sentinel에 소비자 사기 및 Identity theft와 관련하여 2004년 1년간 접수된 건수는 635,000건이 넘는다(FTC, 2005. 2. 1). Consumer Sentinel은 소비자 사기와 ID theft에 대한 자료를 FTC와 150개 다른 조직(예컨대, 미국 국방부, FBI, 미국 재무부 비밀 검찰부, 미국 체신검사소, 호주 경쟁 및 소비자 위원회, 캐나다 Phonebusters 등)으로부터

수집하여 미국과 전 세계의 수사담당 실무가들이 참고할 수 있도록 제공한다.

1997년에 시작된 이 데이터베이스에는 현재 200만 건 이상의 사기와 ID theft관련 고충이 포함되어 있다. 미국 각 주의 검찰총장들과 19개국 소비자 보호기관을 포함하는 1200개 이상의 법집행기관은 이들 자료를 이용할 수 있다.

<그림 2-1> 연도별 ID theft 고충 건수



2004년도에는 635,000건 이상의 고충이 접수되었는데 이 가운데 61%는 사기와 관련된 것이고 39%는 ID theft와 관련된 것이다. 접수된 ID theft를 유형별로 나누어 살펴보면, 신용카드 사기가 28%로 가장 많았고, 전화 혹은 공공요금 사기가 19%, 은행 사기가 18%, 취업사기는 13% 순으로 나타났다. 이밖에 다른 주요 유형에는 공문서/연금 사기와 대출사기가 포함된다.

ID theft 유형 가운데 가장 빠르게 증가하고 있는 것이 "전자금융거래"이다. "전자금융거래"와 관련된 ID theft 접수건수는 2002년에서 2004년 사이에 두 배 이상 증가하였다.

지역에 따라서 ID theft 신고건수에서 큰 차이가 발견된다. 인구 10만 명당 피해자 수로 보았을 때 Arizona주가 143건으로 가장 높았고, 그 뒤를 이어 Nevada주 126건, California 주 122건, Texas주 118건, Colorado주 96건, Florida주 92건, New York주 92건, Washington주 91건, Oregon주 88건 등 주로 서부와 남부에서 신고건수가 높게 나타났다.

연방거래위원회(2003)에 따르면 2000년에 identity theft로 보고된 사례는 31,117건이고 2001년에는 86,198건으로 177% 증가하였고, 2002년에는 161,819건으로 87% 증가하였다. 다른 사기관련 고충건수는 2000년에 107,890건에서 2001년에 133,891건으로 24% 증가하였고, 2002년에는 218,384건으로 63% 증가하여서 identity theft의 증가율이 다른 사기관련 사건보다 상대적으로 높게 나타난다. 과연 identity theft가 다른 절도범죄보다 더 빠르게 증가하고 있는 것인지에 대해서 Allison et al.(2005)이 통계분석을 한 바 있다. 분석결과 identity theft와 다른 종류의 절도관련 범죄(신용카드사기, 자동차절도, 강도, 부정수표 사용) 발생추세 사이에서 통계적으로 유의미한 차이가 발견되었다. 즉 identity theft 사례가 다른 종류의 절도범죄보다 더 증가하고 있는 추세가 발견되었다.

그러나 FTC 고충자료의 타당도에 대한 우려의 목소리가 들린다. 연방거래위원회는 신고를 요구하지 않고 이 기관에 고충을 제기한 개인들로부터 얻은 자료를 수집한 것이다. 따라서 연방거래위원회의 데이터베이스가 대표성 있는 identity theft 자료를 포함하고 있다고 보기는 어렵다. 특정한 유형의 identity theft는 과대-접수되기도 하고 일부는 과소-접수되기도 한다. 많은 피해자들은 피해사실을 FTC에 신고하지 않고, 법집행기관도 보고하지 않는 경우가 많아서 FTC의 통계는 실제보다 과소평가되었을 것으로 추정된다. 결국 연방거래위원회의 데이터베이스는 기껏해야 미국 내 identity theft 수준을 대략적으로 나타내는 것으로 판단된다.

Identity theft에 대한 또 다른 자료는 Office of the Inspector General(OIG)에서 얻을 수 있다. OIG는 피해자가 Social Security Administration(SSA)에 제기한 자신의 사회보장번호 오용혐의에 관해 경험적인 조사를 수행하는 곳이다. OIG가 연구를 하게 된 주요 이유 가운데 하나는 identity thief가 주로 노인들을 대상으로 하고 있다는 우려 때문이었다. OIG는 1997년 10월 1일부터 1999년 3월 31일까지 사이에 기관에 접수된 사건가운데 무작위 확률표집을 이용하여 400개의 사례를 선정하고 이로부터 자료를 수집하였다. 연구결과, 접수된 혐의 가운데 불법적인 신용카드사용과 일거리나 노동허가

를 얻기 위해 다른 사람의 신원증명을 사용하는 경우를 포함하는 identity theft가 81.5%로 가장 높게 나왔다(Office of the Inspector General, 1999).

마지막으로 미국회계국(U. S. General Accounting Office(USGAO))의 자료를 사용할 수 있다. USGAO는 identity theft 문제를 다루는 전문가들을 대상으로 면접을 수행하기도 한다. USGAO는 ID theft 분야에 대한 경험적 연구가 부족하고 이 범죄에 대한 일반적인 인식이 부족하다는 점을 강조한다. USGAO에서는 identity theft의 양을 전국적으로 측정하려고 시도하고 있다. USGAO는 identity theft의 발생률을 추정하기 위해 수많은 지표를 이용한다. 추정을 위해 사용되는 지표에는 연방기관에 의한 형사사건의 수사건수, 신용카드 회사가 제시한 금융손실, 시민들이 관련 정부기관이나 민간단체에 접수한 고충 및 문의건수 등이 포함된다. 자료에 따라서 추정이 달라지지만 공통적으로 나타나는 부분은 identity theft가 빠르게 증가하고 있다는 사실이다.

Identity theft가 절도와 관련된 다른 범죄보다 더 빠르게 증가하고 있지만 여전히 전체 절도관련 범죄 가운데 상대적으로 작은 퍼센트를 차지하고 있다는 사실에 주목해야 하겠다. Florida주의 한 경찰서 자료를 분석한 결과, 2002년도에 강도는 1505건, 자동차 절도는 6670건 신고된 것에 비해 identity theft는 320건이 신고 되었다. 결국, 대부분의 사람들은 identity theft의 피해자가 될 위험보다는 자동차 절도의 피해를 당할 위험이 훨씬 더 높다는 것이다.

3) 피해자와 가해자

Identity theft의 피해자와 가해자는 어떠한 특징을 가지고 있는 사람들인가? 하는 문제는 이 문제를 설명하는 데 중요한 실마리를 제공하게 된다. 아쉬운 점은 아직 여기에 대한 연구가 많지 않다는 것이다.

미국의 연방거래위원회(2000)와 OIG(Office of the Inspector General, 1999)는 피해자의 인구학적 특징으로 피해자의 연령분포, 피해자와 가해자의 관계유형, 피해 방법, 범죄를 경찰이나 신용기관에 신고했는지 여부, 사건발생에서 피해자가 피해사실을 발견하기까지 걸린 기간 등을 조사한 바 있다. 자료분석 결과, 전체적으로 identity theft 피해자의 평균연령은 41세 이고, 대부분의 피해자는 가해자와 모르는 사이였고, 범죄피해가 발생한 시점부터 피해사실을 인지하게 되기까지 12개월에서 14개월 정도의 시간이 걸

린 것으로 나타났다. 피해자들의 신고율은 매우 낮은 편이다. 2002년의 경우에 FTC에 identity theft를 보고한 피해자들 가운데 47%만이 경찰서에 신고를 했고 나머지 53%는 신고를 하지 않았다고 밝혔다.

신용절도범들은 피해자의 신상정보를 평균 3개월 정도 오용하는 것으로 나타났다. 그러나 신용절도범이 피해자의 정보를 이용하여 새로운 계좌를 개설한 경우에는 요용기간이 더 길어서 이런 피해사건의 25%정도는 6개월 정도 지속되었다.

Identity 절도범들의 인구학적 구성에 대해서는 알려진 연구결과가 많지 않다. National Incident Based Reporting System(NIBRS)에서 1997년부터 1999년까지 수집한 자료에서는 사기, 뇌물수수, 위조지폐, 횡령, 그리고 재산범죄 등으로 구성되는 경제범죄자를 조사한 바 있다. Identity theft에 관한 직접적인 자료를 찾기 어려우므로 이와 가까운 성격인 경제범죄자에 대한 NIBRS의 자료분석을 통해서 identity 절도범들을 추정해 볼 수 있을 것이다. 그러나 NIBRS 자료는 법 집행기관의 낮은 보고율 때문에 신뢰도와 대표성에 문제가 있을 수 있다. 2003년 9월의 경우에 법집행 기관들 가운데 27%만이 NIBRS에 범죄통계를 보고한 것으로 알려져 있다. ID theft의 피해자 중에는 노인과 청소년들이 포함된다. FTC의 최근자료에 의하면, 60세 이상을 대상으로 한 ID theft 사건이 218% 증가한 것으로 나타난다. 노인들은 젊은 사람들보다 신용한도가 높고, 더 많은 금융자원을 갖고 있어서 사기범들의 주요대상이 되고 있다. 그러나 65세 이상의 피해자들 중 66% 정도는 피해사실을 신고하지 않았다(참고로 18세에서 24세 사이의 피해자는 17%만 신고를 하지 않았다). 특별히 일부 노인층을 사기의 대상으로 삼기도 한다. 1928년 이전에 출생한 미국 남부의 흑인 노인들을 대상으로 과거 노예생활에 대한 보상금으로 $5,000을 받을 수 있다고 속여 사회보장번호 등을 빼내어 사기를 치기도 하였다. 발생 빈도가 드물기는 하지만 아동을 대상으로 한 ID theft는 교활한 형태의 범죄로 확산되고 있다. 현재 약 2%정도를 차지하는 아동대상의 범죄가 증가하는 것을 우려하여 미국 의회는 아동들을 ID theft로부터 보호하기 위한 국가 신용체계의 변경을 고려하고 있다. 일부 전문가들은 아동을 대상으로 한 ID theft는 피해아동이 성장하여 운전면허를 신청하거나 대학 학자금융자를 신청하기까지 장기간 발견되지 않는 경향이 있어서 실제보다 축소 보고되고 있다고 추정한다. 더욱이 범인이 가족원인 경우에는 피해사실을 알고 있어도 신고하기 어렵다. 신용기록이 나쁘거나 운전면허가

정지된 가족이나 친구가 깨끗한 신분으로 다시 시작해 보고자 할 때 청소년 대상의 ID theft가 발생한다. 어린이와 청소년들을 대상으로 한 신용교육이 이들을 보호하는 데 도움이 될 수 있다.

Allison과 그의 동료들(2005)이 Florida주의 한 대형 시 경찰서 자료를 분석한 결과에 따르면, identity theft의 범법자들은 놀랍게도 여자가 다수를 차지하는 한편 피해자는 대부분이 남자였다. 범법자의 63%가 여성인 반면, 남자는 37%에 그쳤다. 이와 대조적으로 피해자의 54%는 남자였고 여자는 46%였다. 인종적으로도 피해자와 가해자사이에 분명한 차이가 관찰되었다. 피해자는 압도적으로 백인(72%)이 많았고, 가해자는 압도적으로 흑인(69%)이 많았다. 조사 대상지역의 인종구성을 고려해 보아도 피해자 가운데 백인이 비율에 맞지 않게 많고, 가해자 가운데는 흑인이 많다. 남미계는 피해자나 가해자로서 모두 인구구성보다 낮게 나타났다. 연령을 살펴보면, 가해자보다는 피해자에게서 더 큰 범위가 관찰된다. 피해자의 연령범위는 5살에서 81살까지로 나타난 반면, 가해자는 21살에서 49살로 나타났다. 피해자의 평균연령은 41세로 가해자의 평균연령인 32세 보다 높았다[10]. 피해자의 대부분은 가해자를 알지 못했다. 약 41% 정도가 피해자와 가해자가 이전에 관계가 있었고 59%는 관계가 없었던 것으로 밝혀졌다.

가해자의 직업을 보면 53%가 실업상태로 나타났고, 41%가 직장이 있었으며, 3%는 은퇴한 경우였고, 3%는 장애를 가지고 있었다. 이러한 자료에 비추어 본다면, identity theft를 저지르는 범법자들은 주로 경제적인 이익이 주요한 동기인 것으로 추리해 볼 수 있다. 이러한 추리는 이전의 연구에서 되어 진 주장과도 맥을 같이 하는 것이다 (Federal Trade Commission, 2000; Newman, 1999). Identity theft를 저지른 범법자들 가운데 64%는 혼자서 범죄를 저지른 것으로 밝혀졌고, 33%는 범법자가 2명이었고, 3%는 세 명이 함께 저지른 것으로 나타났다. 이러한 결과는 일반적인 기대치와 다른 것으로 조금 놀라운 것이다. 일반적으로 identity theft는 여러 명의 범죄자가 협력하여 신용카드와 신분증을 훔치고 다른 금융범죄를 저지르는 사기집단이 개입한 것으로 알려져 왔었다. Newman(1999)은 조직범죄가 identity theft에 관여하고 있다고 주장한 바 있다. 그러나 Allison과 그의 동료들이 사용한 자료는 타당도와 신뢰도의 문제를 가지고 있어서 이 결과를 일반화하기에 어려움이 있다.

FTC연구에 의하면, 피해자 가운데 25%이상은 절도범이 누구인지 알고 있었다. 신상

10) FTC자료에 의하면, 피해자의 절반이상이 40대 미만이고, 피해자의 11% 정도는 60세 이상이었다.

정보 절도사건의 35%는 가족이나 친척이 절도범인 것으로 나타나서 신상정보의 불법적인 사용이 일상에서 접촉이 빈번한 가까운 사람들 사이에서 발생하기 쉽다는 사실을 알 수 있다.

4. Identity Theft가 증가하는 원인

현대를 정보의 시대, 디지털의 시대라고 부른다. 기술이 발달함에 따라 우리는 공간의 제한을 상당부분 극복하고 있다. 집에서도 외국기업의 제품을 인터넷으로 주문할 수 있는 편리함을 누리는 것이다. 그러나 우리가 편의성을 누리기 위해서는 그만큼 프라이버시를 희생하는 경향이 있다. 인터넷 주문을 하기위해 개인의 신용카드정보를 외국의 기업에 제공해야 하고 국내외적으로 퍼져나간 신상정보가 identity 절도범들의 손에 들어갈 확률도 전보다 훨씬 높아진 것이다.

Identity theft가 증가하고 있는 것으로 나타났지만 우리는 왜 증가하고 있고 얼마나 증가하고 있는지에 대해서는 명확히 알지 못한다. 현재는 이에 대한 가능한 이유를 몇 가지 제기해 보는 단계이다. 예컨대, 새로운 기술이 발전하면서 신상정보에의 접근가능성이 커진다는 점이다. 온라인으로 은행계좌 거래를 하고, 대금을 지불하며, 상품을 구입함으로써 인터넷상에서 구할 수 있는 개인정보의 양이 기하급수적으로 증가하게 되었다. 인터넷을 이용하여 공문서에 접근할 수 있는 경우도 늘고 있다. 출생증명서, 결혼증명서, 사망확인서 등을 인터넷으로 편히 볼 수 있도록 많은 공문서의 형태가 변형되고 있다[11].

새로운 기술혁명이 세상을 바꾸고 사람들의 삶을 편하게 만들고 있다. 그러나 이 기술혁명은 부정적인 측면도 가지고 있어서 개인정보에 대한 접근가능성이 커짐에 따라 identity theft를 저지를 수 있는 새로운 기회가 증가한 것이다. 이러한 시각은 일상활동이론의 관점에서 쉽고 명확하게 설명될 수 있다. 이 이론에 의하면 범법자, 피해자(물건), 능력 있는 보호자의 부재라는 3가지 요인이 시간과 공간상에서 충족되면 범죄가

11) 우리나라는 2002년 11월부터 '대한민국 전자정부'를 운영하여 각종 민원서류의 인터넷 열람 등이 가능해졌다. 그러나 대법원과 행정자치부의 인터넷 민원서류 내용이 파일형태로 개인 컴퓨터에 저장될 수 있어 위변조의 문제가 제기되고 있다(중앙일보, 2005. 9. 28).

발생하기 쉽다는 것이다(Cohen and Felson, 1979). 일상활동이론의 관점에서 보면, 기술 발전에 따라서 3가지 요인 가운데 2가지인 피해자와 보호자에 변화가 생기게 되었다. 즉 인터넷에 저장된 개인정보의 양이 급증하면서 범행하기에 적절한 대상의 양이 크게 늘어났다. 반면에 개인정보가 남용되는 것을 공식적으로 보호하는 규정이 충분하지 못하기 때문에 보호자의 기능이 감소하였다. 하루가 다르게 발전해 가는 기술을 규정이 쫓아가지 못하는 지체현상으로 인해 identity theft가 일어날 확률이 이전보다 커진 것으로 해석할 수 있다.

Identity theft의 증가에 대한 또 다른 설명으로 신고관행의 변화를 들 수 있다. 즉 identity theft의 증가는 시민의 신고증가와 경찰의 사건취급에서의 변화 때문에 생겨났다는 것이다. Identity theft를 규정하는 법은 비교적 최근에서야 만들어 졌고, 일반 대중이나 경찰 모두에게 이것은 최근에 생겨난 일이다. 이 범죄의 증가는 인간 행동에서의 변화보다는 신고와 보고에서의 변화 때문일 수 있다. 이러한 추론된 설명은 앞으로의 경험적인 연구에 의해서 밝혀져야 할 부분이다.

또 다른 가능한 설명은 오늘날의 후기 자본주의 사회에서 발견되는 즉석의 신용(instant credit)지급방법에서 찾을 수 있다. 연방거래위원회의 Beale은 “오늘날 소비자는 지갑에 아무것이 없어도 전자제품 체인점인 Circuit City에 들어가 15분이면 3,000불짜리 플레스마 텔레비전을 사서 나올 수 있다”고 한다(MSN NBC, 2005.05.25). 즉석의 신용지급방법은 경제적인 이익에 의해 동기화된 identity theft를 유발시키고 있다. 이러한 금융 시스템은 잠재적인 범법자들에게 동기를 제공하고, 위험부담은 낮고 상대적으로 보상은 높은 ID 범죄를 저지를 수단을 제공하는 셈이다.

이밖에 identity theft의 발생을 용이하게 만드는 요인들을 다음과 같이 생각해 볼 수 있다.

- 첫째, 주민등록번호가 우리의 신원을 확인해주는 암호로 폭넓게 사용되고 있어서 절도범이 주민등록번호를 알아내는 것은 쉬운 일이다. 주민등록번호는 은행, 신용카드 회사, 보험회사, 병원, 전화회사, 공공도서관, 학교 등에서 사용되고 있을 뿐만 아니라 체육관에 등록하거나, 백화점 회원으로 가입할 때도 요구하고, 인터넷 사이트에 가입할 때도 요구하고 있다. 따라서 다른 사람의 주민등록번호에 접근할 수 있는 곳이 많고, 일단 정보를 알게 되면 상당히 넓은 영역에서 사기를 저지를

수 있다.

- 둘째, 온라인이나 오프라인 모두의 영역에서 신용카드의 사용이 빠르게 증가하면서 신용카드번호를 훔치게 되면 손쉽게 identity 사기를 저지를 수 있다. 절도범들은 식당 식탁 위나, 주유소 주변, 그리고 쓰레기통이나 쇼핑 백 안에 버려진 신용결제 영수증을 쉽게 찾을 수 있다.
- 셋째, 20세기에는 제삼자에 의한 광대한 기록보관 체계가 증가하여 은행, 병원, 신용정보 관리기관, 보험회사와 정부기관 등이 개인정보를 모으고 관리하기 시작했다. 제삼자에 의해 수집된 신상정보들에 접근할 수 있는 수많은 사람들 중 일부의 실수나 나쁜 의도에 의해서 신상정보가 절도범들의 손에 들어가기 쉬워진 것이다. 미국 정부 대 Miller의 판례를 보면, 1976년에 미국 연방대법원은 제삼자가 가지고 있는 신상자료에 대해 미국인들은 프라이버시의 헌법적 권한을 갖지 못한다고 판결하였다. 예컨대, 개인이 은행에 계좌를 개설하여 거래를 하기 위해서는 개인자료를 은행 측에 양도하게 된다는 것이다. 따라서 정보는 개인에 관한 것이지만 이것을 수집하고 보관한 은행이 정보를 소유하게 된다는 입장이다. 미국 연방대법원은 이러한 논거를 전화통화기록에까지 확대 적용하였다.
- 넷째, 남의 신용카드번호를 전문적으로 훔치고 매매하는 해커(hacker)들이 증가하고 있다. 이들 가운데 일부는 러시아, 동유럽, 나이지리아 등의 조직범죄집단과 연결되어 있는 것으로 추정된다. 이들에 의해 피해를 본 은행도 많아서 Western Union, Egghead, CreditCards.com 등이 포함된다. 신용정보 절도범들은 훔친 신상정보를 이용하여 합법적인 정보 브로커로부터 추가적인 정보(예컨대, 이름, 주소, 주민등록번호 등)를 구입해서 identity theft를 저지른다.
- 다섯째, 은행 간의 합병도 identity theft의 급증에 공헌하고 있다. 작은 은행들이 큰 은행에 합병되면서 개인신상정보가 거대한 데이터베이스에 편입되어 개인정보의 보호가 강화될 수도 있지만 한번 새나가면 엄청난 파장이 생겨나고 있다.
- 여섯째, 금융기관들이 개인신상정보 보호를 위한 정부의 권고를 대체로 무시하고 있다. 정부는 또한 사기를 근절시키기 위해 개인 신상정보를 수집하고 사용하는 신용조사기관과 신용발행회사를 강하게 규제하고 있지 못하다.

Identity 절도범의 입장에서 보면, 이상에서 살펴 본 요인들로 인하여 ID 범죄를 손쉽고, 조용하게 저지를 수 있다. 이들은 자신의 거실 안락의자에 앉아 범죄를 저지를 수 있다. 게다가 identity theft는 수개월 혹은 수년간 발견되지 않을 수 있다. 그렇다면 가해자에게 identity theft는 위험부담은 낮고 수익은 높은 매력적인 일이다. 범죄자들은 대부분의 identity theft가 수사되지 않고 체포될 확률이 낮다는 것을 잘 알고 있다. 따라서 identity theft는 체포되고 기소될 위험이 낮으면서 돈을 벌 수 있는 기회를 제공한다. 잡힌다고 해도 처벌은 보호관찰이나 적은 벌금이 될 가능성이 높다. Identity 절도범들은 또한 경찰이 이 범죄를 수사하기 어렵고, 비용과 시간이 많이 소요된다는 점을 알고 있다. 범죄자들은 특히 국가와 국가 사이에서 발생한 범죄의 경우에 수사가 어렵다는 점을 알고 이것을 이용하고 있다.

5. Identity Theft에 대한 외국의 관련 입법

ID 절도를 범죄로 규정하고 개인의 신상정보가 범죄수행에 사용된 피해자들의 권리를 보호하는 법이 만들어 진 것은 불과 몇 년 전의 일이다. 미국 의회는 1998년 10월에 Identity Theft and Assumption Deterrence Act를 통과시켜서 identity theft를 새로운 범죄로 규정하고 있다. 이 법에 따라서 다른 사람의 신원증명서를 권한 없는 사람이 가지고 있으면 제18조에 의해 연방범죄를 구성한다. 보다 구체적으로 이 법은 다음과 같이 규정하고 있다. “연방법을 위반하거나 주 혹은 지역법에서 중범죄로 규정된 범죄나 불법행위를 저지르거나 이를 돕거나 교사하기 위해 적법한 허락 없이 다른 사람의 신원증명의 수단을 고의로 양도하거나 사용하게 되면 연방법을 위반하게 된다.” 이법이 만들어지기 전에는 신원서류의 부정한 제작, 사용, 양도만을 법으로 다루었고 개인정보의 절도, 범죄적 사용은 다루지 못했었다. 이 법을 위반하면 Secret Service나 FBI와 같은 연방기관이 수사를 하고, 법무부가 기소를 하게 된다(Hoar, 2001).

Identity Theft 법안이 만들어지면서 다음과 같은 4가지의 성과를 이룰 수 있었다. 첫째, 신용이 손상된 사람을 피해자로 확인할 수 있게 되었다. 은행사기나 신용카드 사기 등의 금융범죄를 다루는 법규에서는 통상 금전적인 손실을 입은 개인, 사업체, 금융기

관만이 피해자로 인정되었었고 신용이 파괴된 identity theft의 피해자는 인정받지 못했었다. 둘째, 사람들이 모든 종류의 identity theft를 신고할 수 있는 접점으로 연방거래위원회를 지정하여 모든 ID 절도사건에 관한 자료를 수집하게 됨으로써 문제점을 확인할 수 있게 되었고 법집행기관이 중앙의 한 곳에서 조사자료를 검색할 수 있게 되었다. 셋째, 이 법이 만들어지면서 처형(處刑) 가능성이 커졌고, 자산몰수 규정이 확대되어 경찰과 검사의 사건수사가 용이해졌다. 넷째, 이법으로 인하여 법을 위반할 의도를 가지고 다른 사람의 개인신상정보를 훔치는 것을 불법으로 규정함으로써 연방법의 허점을 막게 되었다. 과거에는 허위 신분증이나 문서의 제조와 소지만이 금지되었었다.

1999년 4월에 10개의 연방 법집행기관과, 5개의 은행규제기관, 미국 양형 위원회, 주 경찰총장 연합이 연방거래위원회와 만나 위원회 데이터베이스에 포함되어야 할 내용과 소비자교육용 소책자에 포함되어야 할 내용을 논의하였고, 1999년 11월에는 연방거래위원회가 소비자 hotline을 설치하고 ID theft 정보센터에서 고충을 접수하기 시작했다. 2000년 7월에는 전국의 법집행조직들이 연방거래위원회의 정보센터에 접근할 수 있게 되었다. 정보센터가 시작된 이후로 46개 연방기관과 300개의 주 기관, 6개 지방기관들이 이 데이터베이스에 참가하게 되었다.

연방거래위원회는 그러나 수사권이나 법집행권한을 가지고 있지 못하다. Identity Theft 법을 위반하면 미국 재무부 비밀감찰부(U.S. Secret Service), FBI, 미국 우편검사소(U.S. Postal Inspection Service) 등이 수사하고 법무부와 경찰이나 보안관 같은 지방 법집행기관들이 법을 집행하게 된다. 예컨대, 미국 재무부 비밀감찰부는 위조증권의 수사를 강조한다. 여기서 다루는 위조증권에는 화폐위조, 수표위조, 신용카드 위조, 증권과 채권위조 등 양도할 수 있는 거의 모든 유통증권의 위조를 다룬다. 재무부 비밀감찰부는 금융범죄를 저지르는 조직범죄도 다룬다. 도용한 금융 및 신상정보를 이용해 금융범죄를 저지르는 조직범죄집단은 특히 나이지리아와 아시아의 조직범죄에서 많이 발견된다.

연방법과 유사한 Identity theft에 관한 주법은 1996년에 Arizona주에서 처음 만들어졌고, 그 이듬해인 1997년에 California주에서 만들어 졌다. 주법의 일례를 들어보면, 2001년에 Florida주는 다음과 같은 Fraudulent Practice Statute(ch. 817.567)를 제정하였다. “다른 사람의 신상정보를 그 사람의 동의를 취득하지 않은 채 의도적으로 부정한 방식으로 사용하거나 그렇게 사용할 의도로 소지한 것은 개인 신상정보의 불법사용범

죄를 구성하고 이것은 3급 중범죄로 s. 777.082, s. 775.083, s. 775.084에 해당되면 처벌 가능하다." 이 입법이 만들어지기 전에는 Florida 주법에서 실제적인 금융손실을 입은 은행이나 보험회사 같은 곳만이 identity theft의 피해자로 여겨졌고 범죄자에 의해 신원정보가 도용된 사람들은 다양한 형태의 사기범죄의 매개물로만 여겨졌었다. 형사사법 체계는 신원을 도둑맞은 사람들을 피해자로 인정하지 않았고 따라서 신원의 불법적인 사용을 통제하거나 보호하지 못했다. 현재의 Florida 주법은 금융기관뿐만 아니라 개인의 신원증명서가 불법적으로 사용되어 해악을 입은 개인도 피해자로 인정한다. 신원증명서가 불법적으로 사용된 개인들은 수많은 후유증을 경험하는 데 구체적으로는 신용카드의 발급이 거부되고, 대출 또는 임대가 거부되거나 취업이 막히고 범죄전과를 얻게 되는 경우도 있다.

이밖에 미국의 California주에서는 주민들에게 영향을 미치는 기업의 과실을 공개하도록 규정한 공개법이 2003년에 만들어지면서 정보유출 사례에 대해 알 수 있게 되었다. 아마 이 법이 없었다면 2005년 6월에 발생한 카드 시스템스 솔루션에서 발생한 사상 최대의 정보유출 사고에 대해서도 들을 수 없었을 것이다. 그러나 법이 만들어지고 난 이후에도 신상정보를 이용한 범죄의 피해자들은 자신의 힘으로 신용을 회복하기 위해 고군분투해야 한다. 이 범죄가 상대적으로 새로운 범죄이면서도 폭넓게 퍼져 있어서 경찰이나 피해자 지원단체도 아직 적절한 대응을 마련하지 못하고 있다.

미국의 경우에 최근까지 identity theft의 공식적인 피해자는 사취를 당한 상인이나 신용서비스제공회사로 제한되었었다. 현재 미국의 주 가운데 절반정도는 별개의 identity theft죄를 만들어서 신상이 도용된 사람 역시 법적인 피해자로 여겨지도록 규정하고 있다. 그러나 이들 주에서 조차 경찰관들이 이 법을 따라가지 못하고 있다. 문제를 더 악화시키는 것은 경찰이 범죄발생 장소를 알기 전에는 피해자의 신고를 받아들일 수 없다는 입장을 취한다는 점이다. 그러나 identity theft는 사람이 직접 저지르기도 하고, 전화나 우편, 인터넷으로 지질러지기도 하여 실제 범죄발생의 위치를 정확히 아는 것이 불가능한 경우가 종종 있다. 이런 이유에서 미국의 많은 주가 피해자의 거주지를 범죄발생장소로 삼는 것을 허용하고 있지만 실무를 맡는 경찰관들은 이러한 규정을 모르는 경우가 자주 있다.

이 외에도 identity theft와 관련된 문제로 출소(出訴)기한법(statute of limitation)을 꼽을 수 있다. 이 법에서는 형사사건의 발견일자보다 발생일자에 기초한다. 그러나

identity theft가 드러나기까지는 시간이 많이 걸리고 수사하는 데도 많은 시간이 소요되어 발생시점과 발견시점 사이에서 범법자는 자신의 범죄 흔적을 지우고 수사기관에게 유용할 수 있는 정보를 파괴하게 된다.

투자사기나 증권사기의 복잡한 하부구조를 밝혀내는 데 필요한 자원이 부족할 뿐만 아니라 법집행기관이 이런 사건들을 효과적으로 수사할 기술과 훈련이 부족한 것도 문제점으로 지적된다. 미국 정부는 이 문제를 해결하기 위해서 2단계로 접근하고 있다. 먼저, identity theft 사건을 기소하기 위해 법 집행기관들 간의 협조 하에 전국규모의 소탕작전을 시행한다. 다음으로, identity theft에 대한 처벌을 강화하기 위해 새로운 입법을 추진한다.

2002년 5월에 미국 법무부장관은 전국적으로 identity theft의 소탕작전을 수행한 바 있다. 이 소탕으로 24개 사법지구에서 135명에 대해 73건을 형사 기소하였다. 이러한 노력은 연방 법집행기관이 identity theft와 싸우기 위한 두 가지 전략 가운데 하나였다. 다른 한 가지 전략은 identity theft에 대한 기존의 연방형법을 강화하는 것이다.

2002년에 California 주 상원의원인 Feinstein은 Identity Theft 처벌강화법안을 입안하여 identity theft가 심각한 범죄와 함께 발생할 경우 형을 무겁게 하도록 하였다. 즉 심각한 형태의 identity theft에 대해서는 처벌과 검사의 소송제기능력을 강화하였다. 특히 제안된 법률제정에서는 “중/특수(aggravated) identity theft”라는 새로운 범죄를 정의하여 심각한 identity theft는 더 무겁게 처벌하도록 하고 있다. 제안된 법에는 또한 증거요구의 간소화도 포함되어 있어서 identity theft를 저지를 의도를 다른 사람의 신상정보를 가지고 있는 것만으로도 범죄를 구성한다.

Feinstein의 강화법안보다 더 강력하고 논쟁의 대상이 되는 것이 2001년에 만들어진 미국의 애국법이다. 이 법으로 인하여 identity 절도범을 포함한 다양한 혐의자들을 수사하고 기소하는 방식에 상당한 변화가 초래되었다. 2002년 여름에 발표된 은행계좌개설과 관련된 새 규정은 테러에의 자금조달을 차단할 의도로 만들어진 것이나 identity theft와 사기범죄를 통제하는 데도 도움이 된다. 이 규정에 따르면 금융기관은 새 계좌를 개설하고자 하는 사람의 신원을 확인해야 하고, 신원확인에 사용된 정보기록을 유지해야 하고, 계좌개설자가 테러리스트 혐의자 목록에 포함되어 있는지 확인해야 한다.

은행계좌개설과 관련된 새 규정과 비슷한 시점에 California주는 개인의 사회보장번

호를 공시하거나 표시하는 것을 금지하는 새 법이 발효되었다. 이 법은 사회보장번호가 암호화되지 않는 한 누구도 인터넷으로 전송을 요구할 수 없도록 하고 있다. 또한 어느 기관도 개인의 사회보장번호를 우편물에 인쇄할 수 없도록 하였다. 이 법에서도 증명이나 행정적인 목적으로 사회보장번호를 수집, 사용, 유포하는 것은 금지하고 있지 않다. 그러나 California 주민이 은행이나 다른 기관에 자신의 사회보장번호를 사용하지 말라고 요청하면 그 기관은 접수후 30일 이내에 추가적인 비용청구 없이 그 요청을 수용해야 한다.

다른 주의 경우를 보면, New York 주는 2002년 10월에 개인의 신상정보를 훔치고 소지하는 것이 중범죄(felony)를 구성할 수 있는 법을 최초로 만들었다. 이 법에 따르면, identity theft를 이용하여 $500이상의 절도를 하면 최고 7년까지 수감될 수 있다. Virginia 주 의회는 2002년 11월에 Identity theft에 대한 처벌을 강화하면서 경찰이 좀 더 공격적으로 범죄사건을 소추하도록 권고하였다.

California주는 Phishing을 막기 위해 2005년 9월 31일 미국에서 처음으로 반피싱법을 제정하였다. 이 법은 금융기관을 가장해 개인정보를 수집하는 사기 수법에 대한 강력한 처벌규정을 담고 있다. 이 법에는 또한 California 주 정부가 온라인 금융사기 피해자에게 최고 50만 달러까지 보상하도록 하는 내용을 담고 있다(중앙일보, 2005. 10. 17).

6. Identity Theft에 대한 외국 정부의 대응

Identity theft의 해결율은 다음의 몇 가지 이유에서 매우 낮은 것으로 알려져 있다. 첫째, 이 범죄의 복잡성 때문에 대부분의 다른 절도관련 범죄보다 체포영장을 발부받는데 필요한 사항을 충족시키기 어렵다. 둘째, 사법권의 문제가 존재한다. 특히 인터넷을 통해서 발생한 범죄의 경우에는 범죄, 범법자, 피해자가 다 다른 도시, 주, 국가에 있을 수 있어서 어려움이 있다. 이 경우에 피해자가 identity theft를 법집행기관에 신고하는 것마저도 어려운 일이다. 셋째, 형사사법체계는 선정적인 범죄에 몰두하는 경향이 있어서 비폭력적인 범죄는 충분한 관심을 받지 못하고 있다. Identity theft는 사건이 복잡하고 성공적으로 기소를 한다고 해도 가벼운 형벌이 나오는 경향이 있기 때문에 제한된

인력을 가진 경찰로서는 폭력범죄나 마약범죄 사건수사에 더 몰두하는 경향이 있다. 넷째, 이 범죄와 관련이 있는 금융기관들의 협조를 얻기 어렵다. 신용카드 회사나 은행은 자사와 관련된 identity theft에 대해 감추고 싶어 하는 경향이 있다. 자사의 고객정보를 잘 관리하지 못했다는 것이 알려질 경우에 고객이탈 등의 부정적인 결과가 따라올 수 있기 때문이다. 이상의 여러 요인들이 작용하여 수사절차 상의 어려움을 증가시키고 혐의자 체포에 드는 비용을 증가시킨다(U. S. General Accounting Office, 2002).

과연 identity theft사건의 해결율은 절도관련 다른 범죄와 비교해서 더 낮은 것인가 아니면 비슷한 것인가? Allison et al. (2005)이 수행한 실증적 연구결과에 의하면, identity theft 해결율의 변화는 사기범죄, 신용카드범죄, 부정수표범죄, 자동차 절도와 비슷한 것으로 나타났다. 다만 강도와 비교해 보면 identity theft의 해결율이 감소하고 있는 것으로 드러난다[12]. 이 문제에 대한 보다 정확한 추세를 파악하기 위해서는 장기간에 걸친 연구가 필요하다.

경찰이 신고를 접수해도 극히 일부의 사건만이 해결된다. 예컨대, 1999년 San Diego 경찰서에 신고 된 identity theft는 783건이고 이 가운데 50건의 경우에만 범인이 체포되었다. Los Angeles 경찰서의 경우 1999년에 3000건 이상을 접수했지만 이 가운데 1% 정도만 해결되었다.

Identity theft의 범인이 검거되는 경우에도 피해자는 형사사법절차로부터 배제되고 있다. 이 범죄의 피해자들도 다른 피해자들과 마찬가지로 자신의 사건이 어떻게 처리되고 있는지를 알고 싶어 하고, 적당한 시점에서는 형사처리 과정에 참여하고 싶어 한다. 그러나 피해자권리는 폭력범죄 피해자에게만 제한되는 경우가 일반적이어서 identity theft 피해자는 형사사법절차에 대해 통보 받지 못하거나 참여하는 데 어려움이 있다. 경찰로서도 전통적인 범죄와 그 수법과 양상이 다른 identity crime에 대해 소극적인 대처를 하는 경향이 있음으로 해서 피해자들의 분노를 유발하는 경향이 있다.

국내외적으로 ID theft를 예방하기 위해 온라인 구매를 하거나, 웹사이트에 암호 등의 식별자료를 입력할 때 공인인증서 같은 과학기술을 사용하고 있다[13]. 가장 일반적으

12) Allison과 그의 동료들(2005)은 ID theft를 "불법적인(unlawful) 의도를 가지고 다른 사람의 개인정보를 불법적으로(illegal) 사용하거나 양도하는 것"으로 정의하고, 1998년에 만들어진 'Identity Theft and Assumption Deterrence Act'위반으로 분류된 범죄와 기타 절도관련 범죄를 비교하였다.

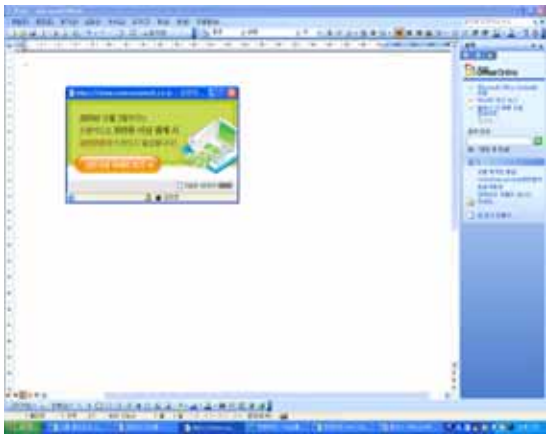
13) 우리나라는 전자공인인증제의 사용에서 다른 어느 나라보다도 활성화되어 있다. 선진국들은 전자공인인증체계를 서두르기보다 시스템을 갖춰나가겠다는 입장을 취하고 있다.

로 많이 사용되는 두 가지 방법이 암호화(encryption)와 인증(authentication)방법이다.

비밀유지를 위한 암호화란 인터넷 상에서 자료를 발송할 때 자료를 잠그고 열 수 있는 키(key)를 사용하는 것이다(<그림 2-2> 참조). 암호화를 이용하면 의도된 수신인 이외의 다른 사람이 그 자료를 보거나 변조하기 매우 어려워진다. 암호화를 사용하면 보내는 측에서 키로 자료를 뒤섞고 받는 측에서 키로 해독하게 된다. 좋은 암호화를 사용하면 외부인이 전송중인 자료를 엿보거나 변조하는 것이 거의 불가능하다. 인터넷 상에서 자료보안을 위한 표준적인 형태가 Secure Sockets Layer(SSL)이다. SSL은 자료를 암호화하는 키를 교환하기 전에 자료를 교류하는 양측을 확인하는 디지털 증명서를 사용한다.

<그림 2-2> Key를 이용한 암호화 인증

<그림 2-3> SSL



온라인에서 물품을 구입하기 위해 신용카드를 사용하기 전에 그 사이트가 자료보안을 위해 SSL을 사용하는지 확인할 필요가 있다. 확인하는 방법은 간단해서 웹 브라우저의 오른쪽 하단에서 자물쇠를 찾아보면 된다(<그림 2-3> 참조). 그러나 금융권이나 개인의 보안망과 시스템이 우수해도 해킹 기술이 빠르게 발전하기 때문에 전자공인인증제를 섣불리 활성화시키면 오히려 문제가 심각해 질수도 있다. 예컨대, 현재 사용중인 1024비트 공인인증서 암호체계가 2007년께는 해커들에 의해 뚫릴 것으로 예상되고 있어서 2048비트 급 공인인증서 암호체계로의 업그레이드를 준비해야 할 단계이다.

암호화는 이-메일의 메시지와 첨부파일을 보호하는 데도 사용될 수 있다. 암호화 프로그램인 Pretty Good Privacy(PGP)를 사용하면 되는데 무료로 배포되는 소프트웨어인 프리웨어를 다운로드 받아 가정용으로 사용할 수 있다.

(http://www.pgp.com/products/freeware.html)

인증은 사용자가 등록된 본인임을 확인하는 방법이다. 사용자는 자신을 인증하기 위해 사용자이름(user name)과 패스워드(password) 혹은 PIN을 입력하여 사용개시하게 된다. 인증을 통해 사용자의 신상을 보호하는 최선의 방법은 좋은 password를 사용하는 것이다. 남이 추측하기 어렵지만 본인은 써 놓지 않고 기억할 수 있는 것이 좋다. 사용자가 password를 잊어버렸을 때를 대비해 사용자의 기억을 돕는 비밀 질문을 작성할 때는 사용자만이 응답할 수 있는 좋은 질문을 고르도록 한다. 사이트에서 제공하는 질문이 너무 적어 적절한 질문을 찾을 수 없는 경우도 종종 있으므로 웹 사이트 관리

자들은 폭넓은 질문을 포함시키거나 기타 항을 만들어 응답자가 스스로 질문을 만들 수 있도록 배려해야 하겠다.

전자금융거래에 있어서 세계를 앞서고 있는 우리나라는 전자금융거래의 안전성을 제고하기 위해 비밀번호 입력방식의 변화를 예고하고 있다. 보안을 위해 사용되고 있는 보안카드의 사용이 2006년 3월부터 2개의 비밀번호를 지정받아 한 번호의 앞자리 숫자 두 개와 다른 번호의 뒷자리 숫자 두 개를 조합해서 입력해야 한다. 또한 전자금융거래로 큰 금액을 거래하기 위해서는 2006년 12월 이후부터 비밀번호를 무작위로 추출해 고객이 소지한 단말기에 표시하는 일회용 비밀번호 생성기를 사용할 계획이다(중앙일보, 2005. 9. 21).

7. 한국 상황에의 시사점

신종범죄인 ID theft를 효과적으로 대비하기 위해서는 일차적으로 실태조사를 실시할 필요가 있다. ID theft에 대해서는 우리가 아는 것보다 모르는 것이 더 많은 현실이다. 범죄현상을 모른 채 대책을 마련할 수는 없는 일이다. 따라서 ID theft가 얼마나 폭넓게 발생하고 있는지, 이 범죄로부터 피해자들은 어떠한 손해를 경험했는지, 피해자들은 문제해결을 위해 어떻게 대응했는지 등을 전국적인 표본조사를 통해 파악하는 것이 필요하다. 경찰자체로 조사를 계획하는 경우에는 치안연구소를 중심으로 실시하는 것이 바람직해 보인다. 외부의 전문기관과 공동조사를 실시한다면 정기적으로 전국규모의 피해자조사를 실시하고 있는 한국형사정책연구원의 설문문항에 ID theft피해경험을 추가할 수도 있을 것이다.

조사를 통해 파악한 실태에 기초하여 경찰과 관련 형사사법기관들은 대응책을 마련할 수 있을 것이다. Identity theft를 직접 담당하는 경찰관에게 도움을 주기 위해 미국의 실무가들이 개발하여 사용하고 있는 실무지침, 피해자 점검표, 담당 수사관을 위한 제언을 아래에 정리하여 제시하였다. 이밖에 ID theft를 예방하고 통제하기 위한 입법활동이 필요하다. ID theft를 범죄로 규정해야 경찰을 비롯한 실무기관이 보다 적극적인 대응을 할 수 있을 것이고, ID theft의 피해자를 위한 회복적 조치도 강구할 필요가 있다(Smith, 2001).

일상생활 중에 신용카드를 사용하거나, 신분확인을 위해 주민등록번호를 사용하거나, 인

터넷을 사용하는 사람이라면 ID theft의 피해자가 될 수 있다. 우리가 현대 사회에서 누리는 편리함을 포기하지 않는 한, 이제 현대인은 ID theft로부터 자유로울 수 없는 것이다. 그렇다면 ID theft에 대한 근본적인 최선의 대책은 현대인의 생활양식을 변화시켜 안전을 담보하기 위해 불편을 감수하도록 교육시키는 것이다. 고급기술에 의한 보안강화보다는 사용자의 보안의식을 강화시키는 것이 더 근본적이고 중요하다. 예컨대, 사용자가 온라인 금융거래를 안전하게 하기 위해 발급받은 공인인증서를 안전한 이동식 저장장치(USB)가 아닌 PC의 하드 디스크에 보관하고, 해킹에 대비해 컴퓨터 보안프로그램을 제대로 설치하지 않고, 주기적으로 업데이트 하지 않고, 실시간 감시기능이 작동하도록 설정해 놓지 않는다면, 공인인증서의 발급이 ID theft문제를 오히려 더 심각하게 만들 수 있다(중앙일보 2006. 1. 4). 또한 Phishing의 경우처럼 문제에 대한 해결책이 마련되지 않은 경우에도 사용자들의 주의가 가장 중요하다. 따라서 일반국민들을 상대로 안전한 전자상거래를 위해 불편을 감수해가며 자신의 신상정보를 지키도록 가르치고, ID theft의 피해자가 되었을 때 취할 조처를 가르치는 교육프로그램을 준비해야 하겠다. 미국에서는 ID theft의 해악을 알리고 그 예방책을 상세히 담고 있는 서적들이 많이 출판되고 있으며(VideoPlus, 2003; Abangnale, 2004; Arata, 2004; The Silver Lake Editors, 2004), FTC를 중심으로 한 국가기관도 피해예방을 위한 국민교육에 앞장서고 있다(<그림 2-4> 참조).

<그림 2-4> ID theft에 대해 알리고 교육하는 미국 사이트

출처: www.consumer.gov/idtheft/

1) Identity crime 담당 실무자를 위한 지침

Identity theft의 피해자가 사건을 신고하면 경찰관이 가장 먼저 반응을 하게 된다. 경찰관은 사건을 접수하면서 피해자로부터 identity theft에 관한 정보를 수집할 뿐만 아니라 피해자가 감정적으로나 금전적으로 회복할 수 있도록 지침을 제공할 수 있다(Mazerolle, 2001). 경찰관은 접수단계에서부터 시작하여 피해자와의 협력관계를 발전시켜서 피해자로 하여금 무력감대신 도움을 받고 있다는 안도감을 갖도록 이끌어야 한다.

다른 범죄사건의 피해자들처럼 identity theft의 피해자들도 충격, 두려움, 분노, 좌절, 무력감과 인격적인 모독을 경험하게 된다. 이러한 것은 일반적이고 정상적인 반응이다. Identity theft의 피해자가 자신에게 주어진 사기범죄기록을 말소시키고 올바른 신용평가를 회복하기까지는 상당히 오랜 기간 폐해와 스트레스를 경험한다. 다른 범죄와 달리 이 과정이 몇 년까지 걸릴 수 있다. 사기범이 체포되지 않으면 피해자는 언제 다시 문제가 불거질지 모른다는 불확실성에 대한 두려움을 갖고 살아야 한다.

피해자를 다루는 경찰관은 피해자의 폐해가 일회적이지 않고 오랜 기간 동안 지속되어 상당한 스트레스를 경험한다는 사실을 인지해야 한다. 사건의 신고단계에서 피해자를 처음으로 만나는 경찰관은 아래에 제시된 피해자 점검표를 이용한 피해자 면접을 실시하여 수사를 위한 기본 정보를 얻게 된다. 경찰관은 피해자의 추가적인 폐해를 막기 위해 필요한 일련의 행동들에 대해 구두로 하나씩 교육시켜야 한다. 사건의 종결시점에서 다시 한 번 피해자를 교육하게 되면 identity theft의 예방법에 대한 지식을 강화시킬 수 있다.

2) 피해자 점검표의 사용

피해자가 집에 가지고 가서 작성해 오는 점검표로부터 수사관은 사건에 관한 정보를 수집하여 identity theft의 원인과 범인을 추적하는데 도움을 받을 수 있다.

피해자 점검표는 4개 부문으로 구성되어 있다. 첫 번째 부문에서는 피해자가 identity theft를 신고한 날자, 시간, 경찰서를 기록한다. 이런 정보는 피해자가 피해사실을 신용정보기관이나 금융기관 등에 신고할 때 필요한 것들이다. 두 번째 부문은 “피해자 정보”에 관한 것으로 피해자의 이름, 주소, 생년월일 등을 기록한다. 이 정보는 수사경찰관에게

필요한 것들이다. 세 번째 부문은 “가해자 정보”로 가해자가 피해자의 은행계좌나 신용카드를 사용하여 부정하게 거래한 내력을 피해자가 적는다. 네 번째 부문은 “Identity theft의 추정 가능한 원인”으로 피해자가 신용카드, 주민등록 번호, 혹은 기타 개인 신상정보를 사용했던 때와 장소 혹은 다른 원인을 회상해 내도록 한다. 다른 범죄사건에서처럼 identity crime에서도 피해자가 범죄와 관련한 정보를 가장 많이 알고 있다.

피해자는 점검표에 나와 있는 대로 identity theft와 관련된 구체적인 정보(예를 들면, 신용카드, 은행, 전화사용 명세서와 같은 서류)를 수집하여 경찰에 제출해야 한다. 피해자가 신용카드 회사, 은행, 통신회사 등으로부터 정기적으로 받는 서류가 수사관에게 필요한 정보가 된다. ‘피해자 점검표’는 2장 후미에 <참고 1>로 제시되어 있다.

3) Identity crime담당 수사관을 위한 제언

피해자가 점검표를 작성하고 담당 경찰관과 만나 사건에 대해 알고 있는 바를 진술하는 등 경찰관의 지시에 따르면서 범죄해결에 도움이 되는 서류 등을 준비하면 자신이 사건에 참여하고 있다는 느낌을 발전시키게 된다. 그렇다면 담당 경찰관은 어디에서부터 수사를 시작해야 하는가? 경찰관은 신용카드 신청서 혹은 신용 조사기관(credit bureau)의 보고서에 나타난 거짓 “현주소”부터 수사해야 한다. 일반 범죄는 범죄현장에서부터 수사가 시작되지만 identity crime은 신상정보의 절도가 발생한 곳이 아니라 ID 절도범이 피해자의 신용카드로 구입한 물품이 배달된 곳에서부터 수사해야 한다. 일반 범죄수사와 달리 끝에서부터 거슬러 올라가며 수사하면 identity crime을 저지르는 조직이 파악되는 등 사건이 해결되는 경우가 자주 있다.

피해자로부터 얻을 수 있는 정보가운데 가장 중요한 것이 신용 조사기관의 보고서이다. 신용조사기관이 발행한 보고서마다 피해자에 대해 다른 정보를 담고 있을 수 있다. 따라서 각 보고서에 나타난 “현주소”나 그 인근지역에서 범인의 소재에 대한 추가적인 단서를 얻을 수 있다. “현주소”는 대개 우편함이거나 빈 아파트 건물 혹은 ID 절도범의 친구나 친척의 주소인 경우가 종종 있다. 담당 경찰관은 신용조사기관의 보고서에서 단서를 찾아낼 수 있는 능력과 보고서에 포함된 정보를 해석할 수 있는 능력을 개발해야 한다.

두 번째로 중요한 정보는 범죄자가 남의 신분을 도용하여 신용카드나 금융서비스를

신청하면서 기관에 제출한 신청서 사본이다. 대부분의 신용카드 회사나 금융기관은 identity theft의 피해자에게 이 사본을 제공해 준다. 이 신청서에는 신용조사기관의 보고서에 포함되어 있지 않은 유용한 정보가 담겨 있다. 즉 직장주소, 집 주소, 집 전화번호, 우편번호, 보증인 등의 정보가 포함되어 있다. 물론 이런 정보가 가짜일 확률이 높지만 그렇다고 이들 정보의 잠재적인 가치를 과소평가해서는 안 된다. 수사관들이 여러 개의 신용카드 신청서에서 발견되는 거짓 이름과 주소, 전화번호로부터 유사한 유형을 확인하여 사기조직을 검거한 사례가 있다(Collins and Hoffman, 2003a). 담당 경찰관은 남의 신분을 도용하여 신청한 백화점이나 전화회사, 은행 등 다른 신청서들도 유심히 조사할 필요가 있다. 이들 신청서와 신용조사기관의 보고서를 함께 수사하다 보면 하나의 단편적인 증거가 다른 증거로 연결되면서 눈덩이 커지듯 identity theft의 원인이 파악되기도 한다.

Identity theft 수사를 돕는 도구로는 온라인상의 흔적을 추적하는 컴퓨터 소프트웨어를 들 수 있다. 한 예로 미시간 주립대학교에서 만든 온라인 범죄추적 수사시스템(Online Criminal Tracking Investigation System(OCTIS))을 들 수 있다. OCTIS는 World Wide Web 내부 은밀한 곳에 저장된 정보에 대해 심층 조사를 할 수 있다. 예를 들어 범죄자가 다른 사람의 신원을 도용해 은행에서 신용카드를 발급받았다면, 신용카드 신청서에 나와 있는 작은 정보가 웹 서치 사이트에 입력되면서 또 다른 정보가 단계마다 조금씩 확대되는 방식으로 만들어져서 범인의 흔적이 생기게 된다. 미시간 주립대학의 형사사법대학에서는 이 프로그램에 대한 교육과정을 개설하여 주 경찰관들과 FBI요원들을 교육하고 있다(Collins and Hoffman, 2003b).

<참고 1> 피해자 점검표

피해자께서 이 점검표를 작성하여 정보를 제공하시면 사건 수사가 용이해 집니다. 점검표에서 묻고 있는 각 문항에 성실히 응답해 주시기 바랍니다. 응답을 마치시면 이것을 복사하여 한 부는 보관하시고 다른 한 부는 관련문서들과 함께 담당 경찰관에게 제출해 주십시오.

제1부 경찰신고관련 정보

경찰신고와 관련된 자세한 정보를 작성하여 보관 하십시오.

경찰에 신고한 날자: _____년 _____월 _____일
신고한 경찰서: _____
신고를 접수한 경찰관 이름: _____
신고한 경찰서 전화번호: _____
신고접수번호: _____

제2부 피해자 정보

작성일자: _____년 _____월 _____일
성명: _____
집 전화번호: _____
직장 전화번호: _____
휴대전화 번호: _____
이-메일주소: _____@_____
주소: _____
_____

연락하기 좋은 시간과 장소:

_____

생년월일: _____년 _____월 _____일
성 별: 남자( ) 여자( )
결혼여부: 미혼( ) 기혼( )

직 업: _____
직장명과 주소: _____
_____

당신 이름을 사칭한 절도범이 당신의 주민등록번호를 사용했나요? 예( ) 아니오( )

지난 1년(12개월) 동안 다음의 열거된 기관에 당신의 신상정보를 제공한 적이 있습니까? 있다면, 신상정보를 제공한 회사나 은행의 이름과 주소를 적으십시오.

일반전화 회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

휴대전화 회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

국제전화 회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

인터넷 서비스 공급 회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

케이블 회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

주택대출 금융회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

자동차대출 금융회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

학자금대출 금융회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

신용카드 회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

은행: 있다( ) 없다( )
있다면, 회사명과 주소: _____

증권회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

보험회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

인터넷으로 물품을 구입한 회사: 있다( ) 없다( )
있다면, 회사명과 주소: _____

당신이 가입한 보험 회사:

_____

지난 1년 동안 의사를 만나 진찰을 받으신 적이 있습니까? 있다( ) 없다( )
있다면, 병원명과 주소:

_____
_____
_____
_____

지난 1년 동안 병원에 입원한 적이 있습니까? 있다( ) 없다( )
있다면, 병원명과 주소:

_____
_____

처방전으로 약을 구입한 약국이 있습니까? 있다( ) 없다( )
있다면, 약국명과 주소:

_____
_____
_____
_____

지난 1년 동안 취업을 위해 지원한 적이 있습니까? 있다( ) 없다( )
있다면, 회사명과 주소:

_____
_____
_____

제3부 당신 이름을 도용한 사기범에 관한 사항

신용카드 사기

1. 당신 이름을 도용한 사기범이 당신이름으로 신용카드를 새로 신청했거나 카드를 발급 받아 사용했다면 아래의 질문에 답하시오. (*여기에 해당되지 않으면 2로 가시오.)

신용카드를 신청한 날자: _____년 _____월 _____일
신용카드로 지불을 청구한 금액: _____원
신용카드 유형(Visa, MasterCard, BC 카드, 기타): _____
신용카드 발급은행(국민, 외환, 신한 등): _____
-또는-
신용카드 발급상점(롯데, 현대, LG, GS 등): _____

신용카드가 당신 명의외의 다른 사람(배우자 등)에게도 발급되었습니까?
예( ) 아니오( )
발급되었다면, 누구에게 발급되었습니까? _____

신용카드 신청은 다음 중 어떤 방법으로 하였나요?
___ 전화신청
___ 인터넷 신청
___ 우편이나 팩스신청(사전 승인된 신청 포함)
___ 상점에서 신청

신용카드 신청서에 기록된 집 주소: _____
_____
신용카드 신청서에 기록된 회사명과 주소: _____
_____
신용카드 신청서에 기록된 집 전화번호: _____

신용카드 신청서에 기록된 직장 전화번호: _____

신용카드 신청서에 기록된 신원보증인이나 가까운 친척이름:

_____

_____

_____

이밖에 당신의 사건과 관련하여 중요하다고 여겨지는 것은 무엇이든 아래에 쓰시오.

2. 당신 이름을 도용한 사기범이 당신이름으로 된 기존의 신용카드를 사용했다면 아래의 질문에 답하시오.

신용카드로 지불을 청구한 날자: _____년 _____월 _____일

신용카드로 지불을 청구한 금액: _____원

신용카드 회사에 주소변경을 요청하면서 접수된 새 주소:

_____

_____

사기범은 다음 중 어떤 방법으로 신용카드를 이용해 물품을 구입했나요?

___ 전화로 구매

___ 인터넷으로 구매

___ 우편이나 팩스로 구매

___ 상점/회사/은행에서 직접 구매

당신의 신용카드가 사용된 회사, 상점, 은행의 이름과 주소:

_____

_____

_____

신용카드 유형(Visa, MasterCard, BC카드 기타): _____
신용카드 발급은행(국민, 외환, 신한 등): _____

-또는-

신용카드 발급상점(롯데, 현대, LG, GS 등): _____

신용카드가 당신 이외의 다른 사람(배우자 등)에게도 발급되었습니까?

예( ) 아니오( )

발급되었다면, 누구에게 발급되었습니까? _____

구매된 물품이 배달된 주소:

_____

_____

이밖에 당신의 사건과 관련하여 중요하다고 여겨지는 것은 무엇이든 아래에 쓰시오.

현금인출카드(ATM)를 이용한 사기

사기범이 당신이름으로 된 현금인출 카드나 번호를 사용하여 현금을 인출했다면 아래의 질문에 답하시오.

은행명: _____
현금을 인출한 날자: _____년 _____월 _____일
현금을 인출한 금액: _____원
현금을 인출한 장소: _____

이밖에 당신의 사건과 관련하여 중요하다고 여겨지는 것은 무엇이든 아래에 쓰시오.

일반전화나 휴대전화 요금의 부정한 청구(대포폰)

사기범이 당신이름으로 일반전화나 휴대전화를 개통하여 사용했다면 부정한 요금 청구서를 첨부하여 제출하시오.

제4부 Identity theft의 추정 가능한 원인

1. 당신은 오늘, 어제 그리고 지난주에 신용카드를 사용한 적이 있습니까? 있다면, 어디에서 신용카드를 사용하였습니까? 당신의 수첩을 보면서 당신이 신용카드를 사용했을 것 같은 모든 장소의 목록을 작성하시오. 신용카드를 사용한 곳의 이름과 주소의 목록을 아래에 기록하시오. 사용한 장소가 많으면 뒷장의 빈 공간을 이용하시오.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

2. 당신은 오늘, 어제 그리고 지난주에 운전면허증을 신분증으로 사용한 적이 있습니까? 있다면, 어디에서 운전면허증을 신분증으로 사용하였습니까? 당신의 수첩을 보면서 당신이 운전면허증을 사용했을 것 같은 모든 장소의 목록을 작성하시오. 운전면허증을 사용한 곳의 이름과 주소의 목록을 아래에 기록하시오. 사용한 장소가 많으면 뒷장의 빈 공간을 이용하시오.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

3. 당신은 오늘, 어제 그리고 지난주에 주민등록증을 사용한 적이 있습니까? 있다면, 어디에서 주민등록증을 사용하였습니까? 당신의 수첩을 보면서 당신이 주민등록증을 사용했을 것 같은 모든 장소의 목록을 작성하시오. 주민등록증을 사용한 곳의 이름과 주소의 목록을 아래에 기록하시오. 사용한 장소가 많으면 뒷장의 빈 공간을 이용하시오.

1. _____
2. _____
3. _____
4. _____
5. _____

6. _____
7. _____
8. _____
9. _____
10. _____

4. 당신의 신상정보(예컨대, 운전면허증, 주민등록증, 의료보험카드 등)에 접근할 수 있었을 사람은 누구입니까? 그들의 이름과 관계를 기록하시오. 의심이 가는 사람이 많으면 뒷장의 빈 공간을 이용하시오.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

제3장 산업스파이

1. 산업스파이의 개념

스파이 또는 스파이활동(spy, espionage)이라 함은 보안조치를 무력화하고 상대의 허점을 공략함으로써 원하는 정보를 취득하는 일련의 과정을 가리킨다(Winkler, 1997). 과거 냉전시대에 이 개념은 특정 국가의 정보요원이 경쟁 국가의 정치, 국방, 외교 등에 관한 정보를 비밀리에 정탐, 수집하는 행위를 가리키는 것이었다.[14] 그러나 80년대 이후 냉전체제가 와해되어 더 이상 미국과 소련을 중심으로 한 이데올로기 경쟁이 무의미하게 되자, 이제는 국제적 경제패권주의에 의하여 정치, 외교, 경제적 정보와 함께 첨단기술을 개발한 산업체를 표적으로 산업기밀을 수집, 탐지하는 소위 산업스파이의 문제점이 더 중요하게 부각되었다(사법연수원, 1999).

산업스파이(industrial espionage)란 국내 또는 세계 시장의 치열한 경쟁에서 이점을 차지하기 위해 경쟁상대 회사들에 관한 정보와 자료를 수집하는 일련의 과정[15]을 말하는 것으로 간단히 정의할 수 있다. 그러면, 여기서 정보(information)는 무엇을 의미하는가? 고전적 의미에서 정보는 “조직화된 자료”(organized data)를 뜻하지만, 산업스파이 대상으로서의 정보는 “경쟁관계에 있는 상대 조직에 해를 끼칠 수 있는 지식, 또는 정보를 취득하는 쪽의 경쟁력을 강화할 수 있는 지식”을 말한다(Winkler, 1997:4). 따라서 그러한 정보는 작게는 전화번호나 영업계획일수도 있고, 컴퓨터 패스워드나 비즈니스 카드일수도 있고, 크게는 설계도나 하이테크 원천기술일수도 있다.

산업스파이는 정보수집과정에서 합법적인 수단뿐만 아니라 불법적인 수단도 사용한다. 예컨대, 가장 무해한 수준에서, 산업스파이는 특정 기업체의 활동을 파악하기 위해 출판물, 웹사이트, 특허관련서류 등(흔히 영업정보라고 불리는 것)을 합법적인 방법으로 검토하는 것에서부터 뇌물, 공갈협박, 기술적 감시, 도청 그리고 경우에 따라서는 폭력

14) 미국 CIA와 구소련 KGB 간의 스파이전이 대표적인 예가 될 것이다.

15) Denning, Dorothy E.(1999), Information Warfare and Security, Addison-Wesley. 또한 다음을 보라. http://www.newhaven.edu/california/CJ625/p6.html.

까지도 사용하는 다양한 형태로 나타난다.

큰 회사들은 대개 합법적 수단으로 산업스파이활동을 수행하는 부서가 있으며, 또한 많은 기업들이 갈수록 다양하고 교묘해지는 스파이활동에 대응하기 위해 상당한 양의 자원을 소비한다. 미국정부는 자국 기업과 경쟁관계에 있는 프랑스 회사가 항공관제레이더 계약을 따내기 위해 브라질 공무원에게 뇌물을 공여한 사실을 알아내기 위해 도청 등의 불법적 산업스파이 활동을 용인한 적이 있다.

산업스파이는 민간기업에 의해서 뿐만 아니라 정부에 의해서도 행해진다. 대부분의 정보기관들이 산업스파이 활동에 관여하고 있다는 것은 공공연한 사실이다. 유럽의회들은 미국의 NSA(National Security Agency)와 영국, 캐나다, 호주, 뉴질랜드 기관들에 의해서 작동되는 커뮤니케이션 스파이 체계인 에셜론이 유럽기업들과 경쟁관계에 있는 미국기업들을 돕기 위해 사용된다고 의심한다. 프랑스 정부는 미국의 항공역학 및 위성회사들에 대한 산업스파이 활동을 지속적으로 수행해 왔다. Tupolev Tu-144 초음속 항공기 개발과 콩코드기의 디자인 모방은 20세기 산업스파이의 가장 대표적인 예의 하나이다.[16]

요컨대, 산업스파이는 일차적으로는 국가안보의 목적보다는 상업적 목적에서 수행되는 스파이활동이다. 그러나 그것이 국가의 안보와 무관한 것은 아니다. 왜냐하면, 산업스파이로 인하여 중요한 산업기반이 타격을 입을 경우 국가의 성장 동력 또한 파괴될 수 있기 때문이다. 사실, 미국, 일본 등 주요 선진국들은 산업스파이 문제를 국가안보의 차원에서 다루고 있다. 따라서 최근에 날로 심각해지고 교묘해지고 있는 산업스파이 사건을 효과적으로 예방하고 적극적으로 대처하기 위해서는 일차적으로는 민간 기업들의 보안의식 및 보안능력의 향상이 전제되어야 하겠지만, 경찰 및 검찰 나아가 국가정보원 등 국가기관들의 수사역량의 강화도 늦출 수 없는 중요한 사안이라 할 것이다.

2. 정보의 유형

Ira Winkler는 산업스파이(corporate espionage)가 대상으로 하는 정보의 유형을 12가

16) http://en.wikipedia.org/wiki/Industrial_espionage

지로 분류하였다(Winkler, 1997:4-11).

(1) 컴퓨터 관련 정보(Computer-based Information)

현대의 디지털시대에서는 거의 대부분의 정보가 컴퓨터와 관련되어 있다고 해도 과언이 아닐 것이다. 정보는 형식화되기 위해 컴퓨터에 기록되거나 컴퓨터 환경 속에서 창출된다. 컴퓨터는 스프레드시트, 데이터베이스, 프로젝트디자인과 같은 전통적인 용도보다도 이메일 때문에 더 중요한 정보원이 될 수 있다. 이메일은 날로 발전하는 해킹기술로 인해 잠재적으로 가장 취약한 컴퓨터 정보의 한 가지이다. 현대 디지털시대에서 이메일 사용은 거의 모든 조직에서 보편화되어 있다. 대부분의 평범한 사내메모에서부터 가장 민감한 프로젝트 세부사항에 이르기까지 사실상 거의 모든 형태의 조직(회사) 정보를 교신하기 위해 이메일을 사용한다. 이메일 교신에는 회사의 현안 및 직원들의 문제, 프로젝트 추진상황 등 수 많은 정보들로 가득 차 있다. 이처럼 컴퓨터 관련 정보는 산업스파이에게는 극도로 유익한 정보원인 것이다.

(2) 공식문서(Formal Documents)

기업들은 전략계획, 계약관련 보고서, 제조공정, 생산보고서 등 다양한 유형의 공식문서들을 인쇄하고 복사하여 보관한다. 이러한 보고서들은 유출될 경우 회사를 파멸에 이르게 할 수 있을 정도로 중요한 정보를 포함하기도 한다.

(3) 초안문서(Draft Documents)

공식문서의 기초가 되는 초안은 흔히 쓸모없는 것으로 치부되기 쉬우나 그것이 담고 있는 정보는 그렇지 않다. 전형적으로 초안문서는 최종문서가 담고 있는 것과 같은 사실을 담고 있으며, 따라서 이러한 초안문서가 산업스파이의 표적이 되기 쉽다.

(4) 워킹페이퍼

공식문서나 초안문서에 포함되어 있는 정보의 상당 부분이 일상적인 업무의 한 부분인 워킹페이퍼에서도 발견될 수 있다. 프로젝트 수행팀들은 구체적인 행위목록, 상황보

고서, 연구개요, 업무서신, 상품내역 등을 작성한다. 이러한 문서들은 그 프로젝트나 조직에 관한 중대한 정보를 포함할 수 있어서 일반적으로 배부가 제한되지만, 대개의 경우 민감한 것으로 생각되지 않으며 공식문서처럼 엄격히 통제되지 않는다.

(5) 스크랩페이퍼

대부분의 사람들은 업무수행 과정에서 불가피하게 또는 무의식적으로 자신의 생각을 메모하거나 쪽지 등을 쓴다. 워킹페이퍼가 등한시될 정도라면 이러한 스크랩페이퍼는 당연히 무시될 것이다. 컴퓨터 접속코드를 적은 포스트잇이나 프로젝트 감독관의 이메일 주소가 적힌 메모지 등을 주의 깊게 다루지 않는 것과 마찬가지이다. 그러나 이처럼 사소해 보이는 정보매체 조차도 우리가 보호하려고 애쓰는 공식문서와 마찬가지로 민감한 자료를 내포할 수 있는 것이다.

(6) 내부통신(Internal Correspondence)

회사내부의 통(서)신은 믿기 어려울 정도로 많은 양의 정보를 포함한다. 예컨대 기업들은 프로젝트 자료, 신상정보, 회사동향, 기타 다양한 정보로 가득 찬 그들 자신의 뉴스레터, 정책문서, 의사록 등을 작성한다. 이러한 문서를 작성하는 사람들은 자신들이 민감한 정보원들을 생산하고 있다는 사실을 인식하지 못하는 경우가 많다.

(7) 정부 및 관공서 관련 문서(Legal and Regulatory Filings)

정부 및 규제기관들은 기업들로 하여금 다양한 정보를 출판하도록 요구한다. 기업은 연례보고서, 특허신청서 등 법이 요구하는 다양한 형태의 문서들을 작성한다. 이러한 문서의 내용은 대개 관련 정부기관들에 의해서 특정화되지만, 많은 기업들이 그러한 요건의 범주를 넘어 필요이상으로 많은 정도를 노출시킨다.

(8) 기타 기록(Other Records)

특별히 비즈니스 세계에서는 거의 모든 행위를 어딘가에 기록으로 남겨둔다. 여행을 할 때는 호텔이나 항공사, 자동차렌트사 등에 기록을 남긴다. 전화를 하거나 받을 때도

행위가 기록된다. 누군가를 호출하거나 컴퓨터에 로그온하여 인터넷을 검색할 때도 기록이 남는다. 이런 유형의 기록들은 어떤 사람을 범죄자로 기소하거나, 회사의 기밀에 접근하기 위해, 그리고 중요한 계획에 차질을 주기위해 사용될 수 있다. 물론, 이런 유형의 정보에 접근하는 것은 합법적인 경우가 많다.

(9) 신문 기타 공개된 정보(The Press and Other Open Source Information)

산업스파이가 표적으로 삼은 회사에 대한 정보를 취득하기 위해 항상 불법적인 활동을 해야 할 필요는 없다. 그들이 필요로 하는 기초자료는 신문이나 무역관련 잡지에서도 쉽게 발견할 수 있으며, 인터넷 접근을 통해 누구나 이용할 수 있는 데이터베이스들도 많이 있다. 이러한 정보원들은 누가 어떠한 계약을 땄고, 특정 프로젝트에는 어떤 임원이 관여한다는 등 산업스파이 공격의 초기단계에 상당히 유용한 정보들을 제공해 준다. 어떤 경우에는 표적 회사에 대한 공격적 행위를 하지 않고서도 공개된 정보원으로부터 필요한 모든 정보를 구할 수 있는 경우도 있다.

(10) 공식회의(Formal Meetings)

조직의 공식모임에서 직원들은 회사나 프로젝트에 관한 이슈에 대해서 토론하게 된다. 이러한 모임의 참가자들은 대개 회사의 중역이기 때문에 그러한 모임에서 논의되는 정보들은 흔히 매우 민감한 것이다. 참가자들은 대개 사전에 회의 의제와 회의 자료를 준비하고 회의 중에는 회의내용을 기록한다. 이 모든 자료들이 산업스파이에게는 매우 귀중한 정보이기 때문에 그러한 회의내용이 도청되기라도 한다면 그 피해는 상상하기 힘들 것이다.

(11) 비공식모임(Informal Meetings)

직원들은 어느 때고 전화상으로 또는 직접 모여서 일해 대해 서로 의논할 수 있다. 이러한 비공식모임에서 논의되는 정보의 민감성은 상황에 따라 크게 다르다. 특히 전화대화는 매우 민감한 정보를 포함할 수 있다.

(12) 우연한 대화(Casual Conversations)

사무실 안 밖에서 이루어지는 일상적인 대화들은 가장 간과되기 쉬운 정보원이다. 직원들은 자신의 업무에 관한 말을 하지 않을 수 없다. 휴식시간에 담배를 피우거나, 퇴근 후 동료들과 간단히 맥주를 한잔 할 때도 업무는 자연스럽게 대화의 주제가 된다. 때로 민감한 회사 문제에 대해 남들보다 많은 정보를 말함으로써 자신을 과시하려는 경우도 있다.

3. 산업스파이의 유형

산업스파이라 하면 종래에는 다른 나라 스파이 기관들에 의한 비밀정보 취득을 의미하는 경우가 많았다. 당시의 스파이들은 소위 "스파이활동"(cloak and dagger) 책략을 사용하여 유괴, 납치, 고문, 살해, 도청 등과 같은 불법적인 행위를 자행하였다. 이러한 전통적인 방법들이 지금도 일부 정보기관들에 의해 여전히 사용되고 있긴 하지만, 그와 같은 "물리적" 정보취득 방법을 사용할 필요성은 근래에는 정보통신기술의 발달로 현저히 감소하였다. 오늘날에는 대부분의 비밀 영업정보를 불법적 수단을 사용하지 않고서도 취득할 수 있다. 또한, 스파이활동의 주체도 크게 변화하여, 최근에는 외국 정부나 스파이기관들에 의한 스파이활동은 크게 감소하였고, 산업스파이의 절대 다수가 서로 경쟁관계에 있는 민간기업체들에 의해 자행되고 있는 추세이다.

B. Parad는 산업스파이 기법들을 무려 79종으로 정리하였으나, 서로 유사하거나 중첩되는 경우가 많아, 아래에서는 비교적 빈번히 발생하고 중대한 것으로 인식되는 몇 가지를 소개하기로 한다(Parad, 1997:9-59). 다만, 이러한 방법들은 불법인 경우도 있으나, 그렇지 않은 경우도 많다.

(1) 스카우트(Hiring Away)

경쟁회사의 기밀정보를 취득하는 가장 간단한 방법은 경쟁회사의 핵심직원이나 컨설턴트 등을 스카우트하는 방법이다. 경쟁사의 직원을 영구히 채용하거나 아니면 자문위원 등의 명목으로 일시적으로 스카우트하여 필요한 정보를 획득할 수 있다.

(2) 평가(Evaluation)

정교한 볼베어링 제조기술을 취득하고자 하는 한 회사(A)가 새 회사(B)를 만들어 표적으로 삼은 회사의 제조기술을 위장 구매케 하는 경우를 예로 들 수 있다. 이때 상품 샘플, 설계명세서, 원료공급자 및 고객 목록, 제조장비, 핵심 직원들의 이름, 영업 및 마케팅 계획, 광고주, 인쇄업자, 운송업자의 이름, 상품포장 및 기타 영업자료 등을 그 회사의 영업평가를 위해 일시적으로 취득할 수 있으며, 이것들을 복사한다. A회사는 "평가"에 공식적으로 참여한 것이 아니기 때문에 그 의도를 알아채지 못한 제조회사는 무심코 귀중한 정보를 경쟁회사에 넘겨주는 셈이 된다.[17]

(3) 입찰전쟁(Bidding War)

표적으로 하는 시스템이나 상품을 공급하는 복수의 제조업자들을 입찰에 참여시킨 후 모든 관련된 배경적 정보를 제출케 하여 "최상의" 것을 선택한다. 공개입찰과 비밀입찰 중 어느 것이든 사용할 수 있다. 또한 실제로 상품을 구매할 필요도 없다. 이 기법은 짧은 기간 안에 복수의 경쟁회사들로부터 상당한 양의 정보를 취득하게 해준다.

(4) 시사회 전시품의 유치(Trade Show Exhibit Retention)

이 기법은 특정 상품의 시사회나 전시회 개최를 빌미로 경쟁 국가나 기업들의 제조품 또는 부품들을 사전에 확보하여 분해 또는 조립해 봄으로써 그 제조상의 비밀 등을 취득하는 행위를 말한다.

(5) 유령회사("Dummy"/Shell Companies)

특정 상품의 구매사실이 외부에 알려지기를 원치 않는 기업의 경우 유령회사나 비밀딜러를 이용하여 상품의 수송 경로를 변경함으로써 익명으로 남을 수 있다. 이와 같은 암행방법은 대개 통상금지 조치가 부과된 국가의 회사들에 의해 사용된다.

17) 이와 유사한 경우로서, 구매희망자로 가장한 스파이가 상품의 평가를 위해 관련 기록 및 자료를 경쟁회사로부터 넘겨받아 그 기록과 자료를 넘겨주지 않고 악용하는 '기록유치'(Record Retention)라는 기법도 있다.

(6) 컴퓨터접속 또는 해킹(Computer Hook-up)

전화회선으로 컴퓨터의 단말기 등에 접속하는 기법 또는 해킹은 경쟁사의 귀중한 데이터베이스를 간단히 약탈하거나 파괴하는 것을 가능케 한다. 한 전직 사원이 개인용 컴퓨터를 이용하여 자신이 다니던 회사 직원들의 패스워드를 도용, 그 회사의 컴퓨터 시스템에 침입하여 생산품 관련 자료와 고객목록을 불법 취득하였으며, 그것을 동일한 상품을 대폭 할인된 가격에서 출하하기 위해 사용한 사례도 있다.

(7) 학술적 교환(Scientific Exchanges)

과거 소련을 비롯한 동구권 및 제3세계 국가와 미국을 비롯한 서방국가들 사이에서 종종 볼 수 있었던 일로서, 미국 및 서방국가의 학자들은 소련 및 동구권에서 인문학을 주로 연구하는데 반해, 소련 및 동구권의 학자들은 미국 및 서방국가에서 마이크로일렉트로닉스, 컴퓨터, 플로트 유리, 기화폭탄, 지질학, 의료 및 미용화학 등과 같은 주로 첨단 전략 과학기술분야의 연구를 하는 현상을 말한다.

(8) 방문(Visiting)

표적으로 삼은 기업을 탐방하는 과정에서 보고, 만지고, 샘플링 하는 등의 방법으로 정보를 취득하는 것을 말한다. 예컨대, 경쟁항공사의 항공기 제조시설을 탐방하는 과정에서 부품의 재질을 파악하기 위해 접착력이 있는 신발을 신고서 공장 바닥에 있는 먼지나 부스러기를 수집하는 경우가 이에 해당한다.

(9) 전송자료의 가로채기(Interception of Data Transmission)

암호화하지 않은 사업상, 기술상의 정보를 전화, 팩스, 컴퓨터, 위성중계 등을 통하여 전송할 경우 이러한 정보를 중간에서 가로채는 것을 말한다. 이러한 전송자료의 가로채기에는 인공위성과 해킹 등 고도의 컴퓨터기술이 동원된다. 즉, 감시컴퓨터가 경쟁사의 통화, 전송기록을 모니터링 하다가 특정한 단어나 문자가 감지되면 자동으로 전체 대화내용이나 전송내용을 녹음, 기록할 수 있다.

(10) 정보브로커(Information Broker)

정보브로커들은 일상적으로 컴퓨터 데이터베이스들을 검색하고, 정부기관이나 기업체 임직원들을 만나고, 도서관이나 기타 정보원들을 통해 현안 문제에 대한 정보를 수집한다. 특히 최근에는 화학, 전자공학, 마케팅 등 특정 분야로 전문화된 정보브로커도 활동하고 있다고 한다. 산업스파이는 이러한 정보브로커에게 비용을 지불함으로써 손쉽게 원하는 정보를 얻을 수 있다.

(11) 휴대전화 도·감청(Public Airways)

과거에는 일반 라디오 스캐너만으로도 휴대전화 도청이 가능했다. 최근에는 휴대전화 도청이 기술적으로 어려워졌다지만 여전히 가능하다는 사실이 밝혀졌다. 얼마 전 국정감사에서 한나라당 모 의원은 복제 휴대폰을 통한 도·감청이 가능하며, 이동통신 3개사 중 1개사만 도청이 안 된다고 주장했다. 이에 대해 정보통신부는 제조공정을 모르면 휴대폰의 복제는 거의 불가능하며 복제 휴대폰 활용이 사실상 어렵다고 주장하였다. 그러나 국가정보원조차 불가능하다고 못 박았던 부호분할다중접속(CDMA) 도청도 복제 휴대폰만으로 간단히 이루어지는 것으로 실험결과 밝혀졌다.

(12) 자료의 촬영, 녹음, 도청 등(Photo/Video/Audio Recording, Eavesdropping)

립스틱, 시계, 자동차안테나, 안경테, 담배 갑, 라이터, 펜, 책 등으로 위장한 소형카메라나 녹음기로 원하는 문서, 물건, 사람, 장치, 작업 등을 촬영하고 녹음하는 것은 전형적인 산업스파이 수법 중 하나이다. 또한 오디오나 비디오, 기타 전자 장비를 이용한 기술적 도청은 산업스파이의 한 가지 중요한 수단이다. 몰래카메라, 라디오송신기 등은 전화나 실내외의 전자단자에 설치할 수 있으며, 심지어 플라스틱 못으로 위장하여 가구나 벽에도 장착할 수 있고, 옷소매, 구두 축, 보석, 조화, 전등, 벽시계 등에도 설치할 수 있다.

(13) 전통적인 절도(Old-Fashioned Theft)

이것은 필요한 정보가 담긴 매체, 서류 등을 직접 절취하는 방법이다. 사무실에 침입

하여 필요한 물건을 훔치는 경우도 있고, 길거리에서 단순 소매치기로 위장하는 경우도 있다. 예컨대, 미국에서 한 컨설팅회사의 대표는 미세전자회로의 비공개디자인을 절취하였다는 죄목으로 기소되기도 하였다.[18]

(14) 항공촬영(Aerial Photography)

고성능 카메라를 갖춘 인공위성이나 내장 카메라를 갖춘 민간항공기가 표적으로 삼은 공장이나 시설을 촬영하는 방법이다. 예컨대, 비밀리에 고용된 한 사진작가가 DuPont사가 건립하고 있는 공장시설을 항공 촬영하였다. 이 공장은 메탄올을 생산하기 위한 시설이었다. 메탄올의 제작방법은 대단히 비밀스러운 것이나 공장의 기본구조를 알아냄으로써 전문가들은 그 제작방법을 알아낼 수 있을 것이다.[19]

(15) 위장침투(Infiltration)

전문적인 자격을 갖춘 산업스파이가 표적으로 삼은 회사에 임시 또는 정식 직원으로 위장 침투한다. 스파이는 자기 회사나 자신을 고용한 기업에 경쟁 회사의 중요 정보를 지속적으로 보내주거나 그 회사의 경쟁력을 크게 훼손할 수 있는 행위를 저지를 수도 있다.

(16) 위장취업면접(Job Interviews)

비밀리에 고용된 헤드헌터가 경쟁 기업의 과학자나 디자이너 혹은 핵심 임직원에게 접근, 더 크고 더 좋은 조건을 갖는 기업에 알선시켜 주겠다고 속여 가짜 취업면접을 갖고 이 면접을 통해 그 사람의 기술, 현재 하고 있는 프로젝트의 내용, 상대기업의 내적 구조 등을 알아내는 방법이다.

(17) 중고품시장(Used Equipment Market)

이는 정당한 절차를 거쳐 동맹국에 판매된 특정 국가의 장비를 통상금지 또는 수출

18) The Associated Press, 1981.10.6. Business News Section; (Parad, 1997:18 참조).
19) E.I. DuPont de Nemours & Co. v. Christopher, 431 F.2d 1012, 166 U.S.P.Q. 421 (1970), cert. denied, 400 U.S. 1024 참조.

제한 조치로 인해 정상적으로 구매할 수 없는 국가나 그 국가의 기업이 중고품으로 사들이는 것을 말한다. 처음에 장비를 판매한 국가는 그러한 재판매의 사례가 워낙 많기 때문에 일일이 통제하기가 사실상 어렵다. 또는 통제를 지나치게 엄격하게 하면 다른 국가가 그 틈새를 이용하여 이득을 취할 수도 있다.

(18) 용도변경(Misapplication of Field of Use)

이는 예컨대 민간용으로 제작된 물품이나 시스템을 군사용으로 전용하는 경우를 예로 들 수 있다. 이러한 전용 역시 전략물품으로 분류되어 구매하기 어려울 경우에 발생할 수 있다.

(19) 공갈(Blackmail)

마약, 여자, 돈 등은 표적으로 삼은 상대를 옭아매는 가장 전통적인 수법이다. 권위상실, 가정불화, 회사에 대한 불만, 궁핍 등의 문제에 노출된 사람들은 자기가 소속된 회사나 자신의 국가를 배반하기 쉽다. 따라서 이와 같은 약점을 가지고 있는 사람들은 공갈협박에 잘 넘어가고 매수되기도 쉽다.

(20) 여자정보원(Women: Intelligence Agents)

기자, 학생, 비서, 스튜어디스, 영사관직원 등으로 가장한 여자정보원이 특히 무역쇼나 회의에 출장 중인 비즈니스맨을 대상으로 미인계를 이용, 애정행각을 한 후 이를 몰래카메라나 비디오에 담아 협박하여 정보를 빼내는 등의 사례를 흔히 볼 수 있다.

(21) 장난감모델(Toy Models)

한때 미국에서는 록히드사의 극비에 부쳐진 스텔스 비행기의 장난감 모델이 대박을 터트렸는데, 그 이유는 장난감이 실물과 너무나 흡사했기 때문이었다. 장난감 제조업자는 무역잡지에서 그 비행기의 제원을 구하였고, 실물을 관찰한 민간 조종사로부터 스케치를 제공받았으며, 항공 산업에 종사하는 엔지니어들과 접촉하였던 것으로 드러났다.

(22) 종업원들(Employees)

자기 회사를 싫어하여 다른 일자리를 찾는 직원들은 자기 회사의 귀중한 정보를 경쟁회사에 넘겨주거나 돈이나 여자 또는 마약과 교환할 수 있다. 또한, 전 고용주와 경쟁하기 위해 스스로 사업체를 설립하거나 전 고용주와 경쟁관계에 있는 업체를 위해 일하는 전직 직원들은 전 고용주의 지적 정보를 의도적으로 폭로하거나 사용할 수 있다.

(23) 고객(Customers)

이는 믿을 만한 고객이 경쟁업체에 중요 정보를 유출하는 경우이다. 일례로, 특정 업체의 향후 가격할인계획, 새로운 슬로건, 트레이드마크 등은 그 업체의 주요 고객이라면 알 수 있는 경우가 많다. 이 고객을 경쟁업체가 직간접적으로 접촉하여 그가 알고 있는 정보를 빼내는 것이다.

(24) 부동산중개업체(Real Estate Agencies)

부동산중개업자들을 이용하여 표적으로 삼은 기업의 건물배치, 설계, 장비, 재정상태, 담보권 등과 같은 정보를 취득하는 경우이다. 중개업자들은 거래를 성사시키기 위해 부동산구매자 또는 임차를 원하는 사람의 정보 요구를 대부분 수용해 주어야 하기 때문에 스파이는 이러한 유리한 입지를 이용하는 것이다.

(25) 자발적인 아이디어 제공(Unsolicited Idea Submissions)

표적으로 삼은 기업이 특정 사업 아이디어나 프로젝트의 개발을 추진 중이라는 정보를 사전에 입수한 스파이가 자신이 창안한 것이라고 하면서 유사한 아이디어를 그 기업의 요구가 없었음에도 불구하고 제공한다. 그 회사가 제공받은 아이디어를 거부하고 나중에 자신들의 아이디어를 상품화하려할 때 스파이는 지적재산권 관련 소송을 제기한다. 그 회사 입장에서는 어쩔 수 없이 소송에 말려들게 되고 그 과정에서 관련 사업정보와 자료가 노출되게 된다.

(26) 광고 및 세일안내문(Advertising and Sales Literature)

회사의 상품 및 용역의 판매를 담당하는 마케팅 직원들의 열성적인 노력이 오히려 회사에 해가되는 경우이다. 선전을 위한 각종 광고 및 안내문들이 상품의 기술적 측면이나 특허 및 출원 등에 관한 민감한 정보를 담고 있을 때, 이를 경쟁 업체가 입수해서 더 향상된 제품을 제작하여 먼저 특허를 출원할 수도 있을 것이다.

(27) 정부(Government)

정부 관료가 고의로 언론에 정보를 흘리거나 아니면 부주의하게 정보를 누출시키는 경우이다. 후자의 한 예로, 과거 미국 정부의 한 부서가 동 베이루트에서 폭파된 미국 대사관의 수리를 위한 도면을 부주의하게 특정 인쇄회사에 주었는데, 이 회사는 그 도면을 아무런 보안허가도 갖는 않은 최소한 11개의 레바논 건설회사들에 팔아넘긴 사건이 있었다.

(28) 소송 및 법정기록(Lawsuits and Court Records)

기업들 간에 불공정경쟁, 특허 및 상표침해, 파산 및 재편 등을 이유로 소송이 벌어질 경우, 그러한 소송에 관한 법정기록은 대개 관련 기업들의 원료공급자, 고객, 가격, 마케팅전략, 설계자 등에 관한 풍부한 정보를 담고 있기 때문에 소송 및 법정기록들은 산업스파이의 주요한 표적이 된다.

(29) 무역박람회(Trade Shows)

무역박람회는 대개 특정 분야에서 최고의 그리고 가장 최근의 상품들을 전시한다. 여기서 판매원들은 서로 교류를 갖고 자기 회사나 타사의 상품과 영업 및 마케팅 전략에 관한 지식을 교환한다. 따라서 무역박람회는 요원들을 보충하고 경쟁 기업에 관한 정보를 비공식적으로 수집할 수 있는 최고의 기회를 제공해준다.

(30) 여론조사와 마케팅조사(Polls and Market Surveys)

산업스파이는 여론조사 기관을 고용하여 경쟁 업체들의 원료공급업자, 고객, 회사중역 및 관리자 등을 대상으로 서베이나 여론조사 및 시장조사를 수행하는 형식으로 경

쟁 기업들의 규모, 능력, 의도 등을 파악하기도 한다.

(31) 영향력 있는 면허권자(Prospective Licensees)

특정 기업이 만든 상품의 취급허가를 받은 사람이나 바이어들은 허가 받은 기술이나 상품에 관한 세부사항을 질문할 권리를 갖는다. 따라서 이러한 사람들이 그 기업의 시설, 능력, 상품개발 및 제조방법 등에 관하여 취득한 정보를 비밀 준수 약정을 위반하여 사용, 수정하거나 퍼뜨릴 경우 이는 그 기업에 큰 재앙이 될 것이다.

(32) 인터넷(Internet)

인터넷은 비용이 거의 들지 않고, 속도가 빠르며, 대개 합법적이란 측면에서 오늘날 가장 각광받는 정보수집 도구 중의 하나이다. 산업스파이는 인터넷으로 경쟁업체의 홈페이지에 접속하여 새로운 상품의 특성과 출시일, 인수합병 소식 등 필요한 정보를 구할 수 있다. 그러나 보다 비밀스런 정보를 입수하기 위해서는 해킹 등 불법행위가 필요할지 모른다.

4. 외국 산업스파이 사건의 최근 사례

1) 미 국

아래에서는 미국 법무부(U. S. Department of Justice)가 인터넷 홈페이지를 통해서 공개한 경제스파이처벌법 적용 사례들 중 2000 이후의 사례들을 중심으로 소개하기로 한다(국가정보원 2005:90-95).[20]

(1) 미카엘 장, 다니엘 박(Mikahel Chang, Daniel Park) 사건(2000년)

이 사건은 '장'과 제3의 인물이 고객리스트·데이터베이스와 관련하여 경제스파이법

20) http://www.fbi.gov/hq/ci/cases.htm에서 다른 사례들도 볼 수 있음.

위반 혐의로 기소된 사건이다. 캘리포니아 산호세 지역에 거주하는 '장'(32세)과 '박'(33세)은 2000년 6월 14일 연방 대법원에 의해 경제스파이법상의 영업비밀 절취혐의로 기소되었다. '장'은 자신이 전에 근무하던 캘리포니아 리버모어에 위치한 세미 서플라이사에서 절취한 자료가 영업비밀 자료임을 알면서도 법적 허가를 받지 않고 수령·사용했다는 사실을 인정하였다. 또한 그 자료가 세미 서플라이사의 고객·주문관련 데이타 베이스 자료임을 인지하고 있었다고 자백했다. '박'은 상업적 목적과 개인적 이익을 위해 저작권을 고의적으로 침해한 사실을 인정하였다. 또한 자신이 절취한 세미 서플라이사의 영업비밀 자료를 열람하기 위해 동 회사의 프로그램을 무단복제 하는 등 저작권 침해사실을 인정하였다. 동 건의 조사는 FBI의 하이테크범죄 전담팀과 법원의 컴퓨터 해킹·지적재산권 전담팀의 감독하에 이루어졌다.

(2) 피터 모크(Peter Morch) 사건(2000년)

피터 모크는 켈리포니아주 파탈루마에 있는 시스코(Cisco)사의 소프트웨어 관련부서에서 근무하다가 사직했다. 시스코사 근무 당시 모크는 음성·광 네트워크 소프트웨어 개발팀에서 팀장을 맡고 있었다. 퇴사 전날 모크는 CD에 자신의 연구 프로젝트와 관련된 자료뿐만 아니라 음성·광 네트워크 소프트웨어 제품과 관련 각종 자료를 모두 담아서 회사를 나왔다. 그로부터 오래지 않아 모크는 시스코사의 경쟁회사인 칼릭스 네트워크사(Calix Network)에서 근무를 시작했다. 미연방수사국 특수요원과 검찰 컴퓨터 해킹·지적재산팀의 공조 수사로 모크는 기소되었다.

(3) 파우스토 에스트라다(Fausto Estrada) 사건(2001년)

파우스토 에스트라다는 뉴욕에 위치한 식음료 용역업체 플릭인터내셔날사 직원으로서 마스터카드사 본부에 파견되어 식음료 서비스를 담당하고 있었다. 파우스토는 카글리오스트로라는 가명을 사용하여 비자카드사에 마스터카드사의 영업비밀을 판매하겠다는 편지를 발송하였다. 편지 내용은 마스터카드사의 1999년, 2000년도 영업비밀을 10만 달러에 판매하겠으며 10만 달러를 더 주면 금년도의 매우 귀중한 자료들을 함께 넘겨주겠다는 것이었다. 파우스토는 마스터카드사와 거대 연예매니지먼트 회사와의 계약 내용을 판매하려 했던 것이다. FBI의 컴퓨터침해·지적재산 담당팀이 함정수사에 착수했

다. FBI 특수요원이 비자카드사 임원으로 위장해 파우스트와 만나 마스터카드사 영업비밀을 구매하기 위한 협상을 시작했다. FBI 특수 요원은 호텔 방에서 파우스토와 은밀히 만나 마스터카드사 기밀 문건을 현금과 교환했다. 이때 파우스토는 FBI 요원에게 신뢰를 심어주기 위해 "나는 마스터카드사 임원들이 어디에서 식사하는지 까지도 알고 있다"는 말을 전했다고 한다. 파우스토는 2001년 3월 21일 경제스파이법 위반, 전신사기, 장물의 주간(interstate) 이동 등 5가지 혐의로 기소되었다.

(4) 니콜라스 다도나(Nicholas Daddona) 사건(2001년)

니콜라스 다도나(44세)는 FMP사(Fabricated Metal Products)에 재직하면서 남몰래 경쟁사인 아이릿 툴메이커사(Eyelet Toolmakers)에도 이중 근무했다. FMP사는 탄환의 부품, 스프링클러 부속품, 연료 필터 캔 등을 설계·생산하는 회사이다. 다노나는 이 두 회사에 동시에 근무하면서 FMP사의 기계부품 제작·생산 계획을 아이릿 툴메이커사와 그 협력회사에 넘겼다. 2002년 3월 11일 니콜라스 다도나는 5개월간에 걸친 전자감시 장비를 통한 감시, 가택연금 그리고 36개월간의 보호관찰 처분을 받았다. 다도나는 또한 4,000달러의 벌금과 100달러의 특별 추징금을 납부토록 명령받았다. 그 후 다도나는 본건에 대하여 FMP사측에 1만 달러의 손해 배상금을 별도 지불키로 합의했다. 본건은 FBI 특수 요원이 수사했다.

(5) 모리스(Morris) 사건(2002년)

모리스는 2002년 7~8월에 걸쳐 브룩우드사의 신기술을 경쟁사인 W. L 고어사에 판매하려고 하였다. 이 기술은 미 국방성의 군사 직물제품 관련 신기술로서 수백만 달러의 가치가 있는 것이었다. 모리스는 2002년 7월 26일부터 8월 5일까지 고어사의 직원이라고 확신하는 한 사람에게 수차례 전화를 해서 브룩우드사의 영업비밀을 10만 달러에 넘기겠다고 제안하였다. 그러나 모리스가 고어사의 직원이라고 믿었던 사람은 국방성의 비밀 공작원이었다. 둘 사이의 전화통화는 모리스가 2002년 8월 5일 뉴저지 턴파이크 도로상에서 체포될 때까지 계속되었다. 고어사는 모리스가 전화를 해서 불법적인 정보를 판매하겠다고 제안했을 때부터 연방수사기관과 접촉하기 시작하였다. 고어사의 신속한 제보로 비밀 공작원이 모리스와 지속적으로 접촉할 수 있었다. 모리스는 경제스파이

법 위반으로 기소되었으며 징역 10년과 벌금 25만 달러를 선고받았다.

(6) 이고르 세레브리야니(Igor Serebryany) 사건(2003년)

이고르 세리브리야니(Igor Serebryany)는 시카고대 학생으로서 디렉TV사(DirecTV)의 법률자문회사인 존스데이사에 근무하고 있던 중 디렉TV사의 위성방송 수신용 최첨단 기술인 4세대 조건부 접근제어 카드(Conditional Access Card)와 관련된 영업비밀을 절취하였다. 디렉TV사는 협력사인 엔디에스 아메리카사와의 민사소송 때문에 이 자료를 존스데이사에 제출해 두고 있던 상태였다. 디렉TV사는 디지털 위성을 통해 디지털 TV 프로그램을 미국 각지로 송출하고 있는 회사로 이 방송을 수신하기 위해서는 시청자들이 상기 카드를 필수적으로 구비해야 한다. 디렉TV사는 협력사들과 카드 개발을 위해 2,500만 달러를 투입하였다. 세리브리야니는 6개월간의 가택연금 기간을 포함한 5년 구금형과 함께 14만 6천 달러를 디렉TV사와 동 회사의 법률자문회사에 지불하라는 판결을 받았다.

2) 독 일

(1) 독일정부, 감청 통해 군수산업스파이 검거[21]

독일 방첩기관은 주독 중국대사관 본(Bonn) 분관에 대한 감청을 통해 무기기술 유출 기도를 저지하였다. 연방헌보청 방첩요원들은 감청을 통해, 군수회사 다이나마이트 노벨사의 전직 직원 한스(60세)가 중국 정보요원에게 새로운 형태의 탄약개발에 관한 연구정보 판매를 제의하는 동향을 포착하였다고 한다. 이후 한스는 자신이 접촉한 중국 정보요원에게 관련 서류들을 넘겨준 바, 연방헌보청은 동 사실을 연방검찰에 통보, 연방검찰이 한스를 체포하였으며 그는 범행사실을 자백하였다.

(2) 독일정부, 미사일기술 유출관련 스파이사건 조사 중[22]

독일 검찰은 외국에 미사일 부품을 공급해준 것으로 의심되는 기업의 수출책임자를

21) 05.4.18日字, 獨 Focus誌.
22) “Germany probes new spy case on missile technology” (01.4.30字 Reuter통신).

체포했다고 밝혔다. 이 사건은 수출통제 위반과 스파이 혐의에 관한 것으로서, 민감한 기술이 제3의 국가로 유출되는 상황에 대한 일련의 사건 중 가장 새로운 것이다. 검찰 측 관계자는 “현재 확보된 정보에 의하면 최소한 2001-2년부터 외국으로의 기술유출이 시작되었고 스파이 조직이 개입되어 있으며 미사일을 개발하는데 필요한 진동측정 장비부문이 주로 유출된 것으로 보인다”라고 밝혔다. 구동독 투린지아 주에 위치한 이 기업의 수출책임자는 사무실과 주거에 대한 수색이 행해진 후 하루 만에 체포되었다.

3) 일 본

(1) 알츠하이머병 연구자료 유출 사건

일본인 오카모토 다카시(43세)는 1999년 미 오하이오 주 클리블랜드 병원재단 연구소에서 알츠하이머병을 연구하던 중 일본 이화학연구소로 전직하면서 DNA 샘플을 빼돌린 혐의로 2001년 5월 미 연방대배심에 의해 기소되었으나 일본은 그의 신병인도를 거부하였다. 일본 정부는 미국 측의 신병인도 요구에 대해 '99년 당시에는 일본에 미국의 경제스파이법에 해당하는 법률이 없다는 이유로 인도를 거부하였다. 그러나 2004년 1월에 동경 고검은 오카모토의 행위는 절도·기물손괴죄에 해당하므로 미일상호 범인인도 조약에 의거, 미국에 신병을 인도키로 결정하고 그를 구속·수사하는 한편 신병인도 심리를 개최하였다. 그러나 동경 고등법원은 그의 미경제스파이법 저촉여부는 그 행위가 이화학연구소의 이익을 도모했는가가 중요한데 연구소의 이익에 보탬이 없었다며 신병인도를 거부하고 오카모토를 석방하였다. 한편, 일본정부는 동 사건을 계기로 부정경쟁방지법에 형사처벌 조항을 신설, 영업비밀 누설시에는 3년 이하 징역 또는 벌금형을 부가토록 규정하는 한편, 문부과학성도 연구시료의 권리 귀속, 반출·취급절차 등을 명시한 연구시료 취급에 관한 규정을 제정하였다.

(2) 일본방위청 정보통신 시스템 자료 유출 사건

후지쓰에 근무하는 기시가와((34세, 전 육상자위대 간부)는 회사가 보유한 방위청 자료를 절취하여 회사측에 금품을 요구하다 체포되었다. 후지쓰에서 통신시스템 엔지니어로 일하던 기시가와는 2002년 8월초, 동 회사가 관리·보수 중이던 방위청 정보통신

시스템 관련 자료를 은밀히 복사, 외부로 유출하여 평소 알고 지내던 고마츠(59세) 등으로 하여금 후지쓰에 접근, 동 데이타를 보여주면서 사건무마 명목으로 금전을 요구토록 사주하였다. 협박을 받은 후지쓰는 기시가와를 공갈미수 혐의로 경찰에 고소하는 한편 범인들의 금전요구 장면을 촬영, 증거물로 제출하였다. 가나가와현 경찰은 11월 범인 4명을 검거, 공갈미수 혐의로 요코하마 지방재판소에 기소하였다

4) 기타 외국의 산업스파이 사건사례

(1) 프랑스 경찰, 산업스파이 혐의로 중국인 여성 조사 중[23)]

프랑스 경찰은 산업스파이 혐의로 조사 중인 발레오사(차량부품 업체) 직원인 중국인 여성(22세)의 컴퓨터 파일을 분석 중인 것으로 알려졌다. 리 리 황(Li Li Whang)이라는 이 여성은 지난주 발레오사가 신용계약 위반과 불법적 전산망 침투혐의로 고소한 지난 금요일 예비 구류상태에서 조사를 받기 시작했다. 혐의를 부인하고 있는 이 여성은 지난 2월부터 파리 남서쪽 외곽에 위치한 발레오사의 연구개발부서에서 인턴으로 근무중이었다. 지난 금요일 실시된 가택 수색에서 경찰은 6대의 컴퓨터와 2개의 하드드라이브를 찾아냈는데 발레오사에 의해 비밀로 관리되던 자료를 포함, 엄청난 용량을 보관하고 있었다. 그녀는 여러 회사에 의해 개발 중인 수십 가지의 차량 디자인 자료도 무단 복제한 것으로 보인다. 경찰 소식통은 범죄연루사실을 증명할 예비증거물들이 컴퓨터로부터 확보되었다고 하였다.

(2) 페라리사, 산업스파이 혐의로 도요타사 고소

이탈리아 스포츠카 생산업체인 페라리는 자사의 핵심 자동차 설계기술을 유출한 혐의로 도요타 자동차를 2003년 11월 이탈리아 경찰에 고소하였다. 페라리는 자사 공기역학 전문연구원이 독일 퀼른소재 도요타 모터스포츠(TMG)로 전직하면서 최신 F1 대회 경주용차 'F2002' 제조 기밀서류를 절취하였으며, 도요타자동차가 동 자료를 이용하여 자사 모델과 유사한 경주용차 'TF103'을 생산하였다며 고소장을 제출하였다. 이탈리아

23) "French police investigate Chinese woman accused of industrial espionage"(05.5.4 AFP).

경찰은 독일 경찰에 사건 수사를 의뢰, 쾰른 소재 TMG사무실·컴퓨터 등에 대한 압수수색과 함께 연구원을 체포하여 혐의내용을 조사하였다. 이와 관련, TMG는 페라리 전 연구원이 자사에 이직해 온 것은 사실이나 부정한 일은 결코 없었다고 부인하였으며 도요타 자동차 일본 본사도 구체적인 사항은 아직 파악되지 않았다고 발표하였다.

(3) 스웨덴, 산업스파이 혐의로 러 외교관 2名추방

스웨덴 정부는 자국기업 에릭슨의 핵심 기술자료 유출혐의로 스웨덴 주재 러 대사관 외교관 2명을 추방 조치하였다. 스웨덴 외교부는 2003년 11월 주 스웨덴 러시아 대사를 소환하여 러시아 외교관 2명을 외교상 기피인물(PNG)로 통보, 추방하였으며 동 조치는 자국 에릭슨 산업스파이 사건과 관련이 있다고 발표하였다. 스웨덴 국가안보경찰은 러시아 외교관 추방발표 전 주에 에릭슨의 중요 기밀자료를 외국 정보기관에 넘기려는 혐의로 동 회사 전·현직 직원 3명을 체포하였는데 그 중 1명은 스웨덴 국가안보에 심각한 위해 행동을 한 혐의로 검거되었다고 발표하였다. 이와 관련, 러시아 외교부는 스웨덴의 조치에 대하여 유감을 표하며 적절한 대응 조치를 취할 용의가 있다고 반응하였다. 한편, 에릭슨은 이동통신 장비뿐만 아니라 스웨덴·英 공동개발 JAS-39 그리펜 전투기 탑재 레이다 등 군용 레이다 시스템을 생산하고 있는 회사로 동 사건과 관련, 체포된 산업스파이들은 고위직 임원이 아니어서 유출 자료에 의해 큰 손해를 입지 않았다고 발표하였으나 유출 자료가 어떤 분야 자료인지에 대해서는 언급을 회피하였다.

(4) 이스라엘, 대규모 산업스파이 적발[24)]

이스라엘 경찰은 지난 일요일, 스파이웨어 등을 통해 기업 전산시스템에 침입, 기밀자료를 유출시킨 혐의로 11명의 사립탐정을 체포했다고 밝혔다. 이스라엘 언론은 체포된 사람 중엔 이들 외에도 자료유출을 의뢰한 것으로 추정되는 유수기업의 경영진들이 포함돼 있다고 보도했다. 이러한 산업스파이 행위로 부당이득을 취한 것으로 보이는 기업에는 위성TV 방송사 예스사, 이동통신 업체 펠레폰사와 쎌콤사, 자동차·광천수 수입업체 등이 망라되어 있다. 암호명 "경마작전(horserace)"으로 명명된 이번 수사는 지난해 11월 이스라엘의 유명한 소설가가 자신의 신작소설이 출판되지 않았는데도 인터

24) "Israel rocked by industrial espionage scandal"(5.29字 DPA통신)

넷상에 나돌고 있다고 경찰에 신고함으로써 시작되었다. 그의 컴퓨터를 조사한 경찰은 범행에 트로이목마 바이러스가 이용된 것을 확인하였고 영국에 거주하는 그의 전 사위이자 컴퓨터 전문가인 이스라엘인을 용의자로 지목하였다. 그는 지난주 현지에서 체포되어 송환절차를 논의 중에 있다. 경찰은 용의자가 유수한 기업들로부터 기밀을 빼내려는 사설탐정들을 위해 이러한 바이러스를 개발해준 것으로 추정하고 있다. 이들 바이러스는 판촉용 CD에 숨겨져 수많은 기업들에 배달되어 아무도 눈치 채지 못하게 주 전산망을 감염시켰다. 사설탐정들은 또한 같은 목적으로 바이러스를 은닉한 이메일을 업체 관련자들에게 발송해온 것으로 보인다.

(5) 대만, VIA 테크놀로지사 CEO 기소

대만 지방검찰청은 2003년 12월 VIA 테크놀로지 회장과 사장 첸웬치 및 직원 창 치하오 등 3명을 경쟁사인 D-Link의 시뮬레이션 테스트 프로그램 절취 및 저작권 침해혐의로 기소하였다. VIA 테크놀로지는 경쟁사의 영업비밀을 절취하기 위해 2000년 자사에 근무하던 창 치하오를 퇴직 후 D-Link에 입사케 하여 D-Link가 개발한 시뮬레이션 테스트 프로그램 관련 자료를 절취 후 퇴직케 한 후 '02년 네트워크 디자인 매니저로 재고용하였다. 대만 지방검찰청은 동 사건과 관련, VIA 테크놀로지의 회장과 사장 첸웬치 및 창 치하오를 저작권 침해 및 기술절취 혐의로 기소하였다. VIA 테크놀로지는 '02년 자본금이 7억 2천만 불에 이르는 대만의 대표적인 반도체 칩 디자인 회사이며 특히 사장 첸웬치(46세)는 반도체 선두주자로 인정받아 왔다.[25]

5. 영업비밀에 대한 국제적 보호와 외국의 산업스파이 대응체계

1) 영업비밀의 국제적 보호

선진국에서는 이미 19세기 초반 영국에서 영업비밀을 판례로 보호하기 시작한 이래 영업비밀 보호의 필요성을 절감하여 각국 실정에 맞게 어떤 형태로든 보호하여 왔고, 20세기 중반에 이르러서는 지적재산 및 영업비밀 보호에 관한 제도의 국제적 통일화

25) 이상, 외국의 산업스파이 사건사례는 국가정보원의 「첨단 산업기술 보호동향」(2004-5)을 참조하였음.

작업도 시작하였다.[26]

현재, 영업비밀 또는 비공개정보는 1994년의 국제법상 WTO/TRIPs 협정 즉, 무역관련 지적재산권에 관한 협정(Agreement on Trade-Related Aspects of Intellectual Property Rights)에 의하여 보호되고 있다. 이 협정의 제7절은 「비공개정보의 보호」(protection of undisclosed information)라는 표제 하에 제39조에서 영업비밀의 보호에 관하여 규정하고 있다.[27]

동 협정 제39조 2항은 "자연인 및 법인은 합법적으로 자신의 통제 하에 있는 정보가 자신의 동의 없이 건전한 상업적 관행에 반하는 방법으로 타인에게 공개되거나, 타인에 의해 획득 또는 사용되는 것을 금지할 수 있는 가능성을 갖는다. 단, 그와 같은 정보는 다음과 같은 것이어야 한다. (가) 전체로서 또는 그 구성요소의 정밀한 배려 및 조합의 형태로서 당해 정보의 종류를 통상적으로 다루고 있는 업계의 사람들에게 일반적으로 알려져 있지 않거나, 쉽게 접근될 수 없다는 의미에서 비밀인 것, (나) 비밀이기 때문에 상업적 가치를 갖는 것, (다) 적법하게 동 정보를 통제하고 있는 자에 의해서 비밀로 유지되기 위한, 그 상황 하에서 합리적인 조치의 대상이 되는 것"이라고 규정하고 있다.[28]

나아가, 제39조 3항은 정부에 제출된 특정한 정보를 보호할 회원국의 의무를 규정하고 있다. 즉, "회원국은 신규 화학물질을 이용한 의약품 또는 농약품의 판매를 허가하는 조건으로 작성에 상당한 노력이 소요된 미공개 실험결과 또는 기타 자료의 제출을 요구하는 경우, 이러한 자료를 불공정한 상업적 사용으로부터 보호한다. 또한 회원국은 대중을 보호하기 위해 필요한 경우 이외에, 또는 불공정한 상업적 사용으로부터 동 자료의 보호를 보장하기 위한 조치가 취하여지지 않을 경우에는 이러한 자료가 공개되는 것으로부터 보호한다"고 규정하고 있다.[29]

2) 외국의 산업스파이 대응체계

(1) 미 국

---

26) 김용선, 특허정보, 1996.1, 46면.
27) 정병두, 미공개정보의 보호, 법무부(편), UR협정의 법적 고찰(하), 법무부, 1994, 590면 이하 참조.
28) 이상 법원도서관, 조약집, 제3권(다자조약 3) 상, 재판자료 제69집, 1995, 455면 참조.
29) 이상 법원도서관, 조약집, 제3권(다자조약 3) 상, 재판자료 제69집, 1995, 455면 참조; 한상훈(2000) 참조.

A. 첨단기술 유출방지 노력[30]

가. 정부차원의 활동

FBI는 1994년부터 미국 내 외국 산업스파이를 추적하고 그 표적이 되는 기업에게 위험을 경고하는 전담부서를 설치·운영하고 있다. 또한 2001년 5월 CIA, NSA 등 정부부처 합동으로 설립한 국가방첩센터(NCIX: National Counterintelligence Executive)는[31] 미 첨단기술·핵심인력에 대한 외국정부·기업의 탐지실태에 관한 자료를 수집하여 유관기관 및 업계에 전파하고, 해외·국내·통신·군사 등 기관별로 분산되어 있는 국가 방첩업무의 통합조정 및 상호협력을 증진하며, 매년「외국의 대미 산업첩보 수집활동 실태에 관한 연례 보고서」를 작성, 의회에 보고하는 등의 업무를 수행하고 있다. 그리고 국무부 산하 외교안보자문위원회(OSAC: Overseas Security Advisory Council)가 1980년대 중반 민간부문과 정부부문 합동으로 설립되었으며, 회원으로 가입되어 있는 1,800여개 기업체에 산업스파이 관련 정보 등 다양한 정보자료를 제공하고 있다.

나. 민간단체의 활동

1955년 민간 보안산업 활성화와 전문성 제고를 위해 설립된 미 산업보안협회(ASIS: American Society for Industrial Security)는[32] 세계 최대 민간 보안협회로 FBI·법무부 등과 공조하여 산업보안 관련 교육, 인력양성, 정보제공, 정책건의 등의 기능을 수행하고 있으며, 기업 정보자산관리과정, 시설보안관리과정 등 교육 프로그램을 운영하면서 각종 보안 관련 이슈에 대한 해결책을 제시하고, 보안 관련 잡지(시큐리티 매니지먼트 등 3종)를 발간, 회원사에 배포하는 한편 전시회·세미나 등 국제교류활동을 수행하며, 보안전문 자격증(CPP, PSP, PCI 등 3종)을[33] 발급하고 인터넷 정보자료센터를 운

30) 국가정보원, 첨단산업기술보호동향 제3호: 2-6.
31) '94년 5월 국가 방첩 역량을 강화하기 위해 창설된 NACIC(The National Counterintelligence Center)가 '01년 5월 NCIX로 개칭됨.
32) 본부는 버지니아주 알렉산드리아 소재, 22개국 204개 지부에 총 33,000여명의 회원(기업 보안책임자·임원, 컨설턴트 등)을 두고 있으며 국내에는 현재 회원 10명이 활동 중(지부는 미결성).
33) CPP(공인보안전문가, Certified Protection Professional), PSP(물리보안전문가, Physical Security Professional), PCI(공인조사전문가, Professional Certified Investigator).

영하고 있다.

다. 법령・제도 정비 등을 통한 보안시스템 구축

[수출 통제]

수출관리규정(Export Administration Regulations)[34]에 따라, 상무부 주관으로 복합용도(군・민수 겸용)의 기술을 수출할 때에는 대상기술의 특징, 성능 및 수출 대상국에 따라 수출 가능여부를 결정한다. 또한, 국제무기거래규정(International Traffic in Arms Regulations)에 따라, 국무부 주관으로 방산물품・서비스 및 기술적 데이터 등에 대한 수출을 통제한다.

[외국인 투자제한]

1988년 제정된 종합무역법(통칭 Exon Florio법) 5021조에 의거, 미 대통령은 국가 안보에 위협이 된다고 판단되는 경우 외국인의 미국 기업 인수・합병을 정지시키거나 금지할 수 있다.

[경제스파이처벌법 제정]

클린턴 전 대통령은 1995년 7월, 의회 연례보고서를 통해 외국의 경제스파이 행위를 미 국익에 대한 실질적 위협으로 간주한다고 발표하였고, FBI는 1996년 2월, 연간 800여건의 기업비밀이 해외로 유출되고 있다면서 법무부를 통해 경제스파이처벌 법안을 의회에 제출하였다. 이후 1996년 9월, 하원에서 399대 3의 압도적 표차로 통과된 데 이어 상원 의결을 거쳐 96.10.13 정식 발효되었다.

동 법은 영업비밀을 '비밀유지를 위한 합리적 조치가 취해지고 독립된 가치가 있는 유무형의 모든 정보'로 규정하면서, 1831조에서는 '외국 정부・기관・요원에 이익을 줄 의도를 가지고 있거나 이익을 준다는 것을 알면서도 고의로 영업비밀을 침해한 경우' 개인은 50만불 이하의 벌금이나 15년 이하의 징역 또는 병과, 조직・단체에 대해서는

34) 통제대상 기술 선정기준을 대테러, 생화학무기, 범죄통제, 국가안보, 화기협정, 지역안정, 중요품목(주로 국가핵심 기술) 등으로 명시하고 있다.

1,000만불 이하 벌금형을 부과한다고 규정하였다. 또한 1832조에서는 '해당 영업비밀 소유권자 이외의 제3자가 경제적 이익을 위하여 미국 내 주간 또는 국제무역을 위해 생산된 재화와 관련된 영업비밀을 침해한 경우' 개인은 50만불 이하의 벌금이나 10년 이하의 징역 또는 병과, 조직·단체에 대해서는 500만불 이하의 벌금형을 부과한다고 규정하였다.

B. 국가방첩전략

미 국가방첩관실(The Office of National Counterintelligence Executive)은 2001년 5월, 국가방첩역량 강화를 위해 CIA, NSA 등 정부부처 합동으로 버지니아주 랭글리 소재 CIA본부 내에 설립되었다.[35] 그 주요 임무는 ① CIA·FBI·법무·국방·에너지부 등의 간부로 구성된 「국가방첩정책위원회」의 의장역할 수행, ② 해외·국내·통신·군사 등 미정부내 모든 국가방첩기관의 활동 통합 지휘 및 「국가방첩전략」 작성·집행, ③ 미 첨단기술·핵심인력에 대한 외국정부·기업의 탐지실태에 관한 자료를 수집, 유관기관 및 업계에 전파, ④ 매년 「외국의 대미 산업첩보 수집활동 실태에 관한 연례보고서」를 작성, 의회에 보고하는 등의 업무 수행이다.

다음은 국가방첩관실이 2005년 3월에 작성한 국가방첩전략 중 산업스파이에 관련되는 부분만을 발췌한 것이다.[36]

가. 서 문

본 국가방첩전략은 2002년 11월 개정된 국가방첩활동강화법에 따라 국가방첩관실이 최초로 작성 발표한 "연례방첩활동계획"으로서 05.3.1 부시 대통령의 재가를 받았다. 1947년 제정된 국가안보법은 「방첩」의 개념을 "스파이, 여타 정보활동·파업으로부터 또는 외국정부·요원과 그 대리자 및 외국조직·외국인·국제테러분자들의 암살 활동으로부터 보호하기 위한 정보수집 및 대응활동"이라고 규정하고 있다. 방첩활동이란 본 전략에 명시되고 있는 재래적 위협이나 21세기의 새로운 외국의 첩보활동 위협에 대응하기 위해 국내·외에서 수행되는 방어활동 및 공격활동을 모두 포함하는 것이다.

35) 94년 5월에 설립된 NACIC(The Nat'l Counterintelligence Center)를 근간으로 재창설됨.
36) 국가정보원, 첨단산업기술보호동향 제4호: 96-112에서 발췌.

나. 개 요

미국의 국가방첩전략은 '평화수호'를 위해 테러 및 폭정국가와의 전쟁을 수행해 나가고, '평화유지'를 위해 열강국가들과의 우호적 관계를 발전시켜 나가며, 또 '평화확장'을 위해 전 세계적으로 자유롭고 개방된 사회를 조성해 나가는 데 있다.

이러한 기본목표들은 쉽게 성취될 수 있는 것이 아니다. 테러분자, 폭정권력, 평화와 자유의 적들은 외부에서 가만히 바라보고만 있는 것이 아니라 미국과 우방들을 와해시키려고 적극 활동하면서 차원 높은 첩보활동도 전개하고 있다.

각국 적들이 특별히 추진하고 있는 사항들을 보면, ① 미국의 민감정보·의도·기술·활동·공작 등 국가안보 관련 기밀에 침투, 수집·손상시킴으로써 자국의 이익을 증진시키고 미국이 추구하는 목표를 좌절시킴, ② 미국의 수집대상 첩보를 조작하고 비밀 영향공작을 전개함으로써 정책 입안자들이 보고 받는 사실·실체를 조작, 왜곡시킴, ③ 미국의 흑색수집활동, 특수활동, 특수공작, 민감첩보 및 군사·외교적 활동 등의 국가안보활동 시행을 추적, 방해, 반격함, ④ 중요 기술 및 여타 민감정보를 획득, 자국 군사역량의 제고 또는 경제적 우위 확보를 도모함이 있다.

외국의 이러한 정보활동은 미국의 안보와 번영에 대해 총체적 위협이 되고 있다. 미국은 이러한 위협을 극복하기 위한 국가적·체계적인 세부 정책이 필요하며, 그 열쇠는 국가안보전략을 지원하는 전략적 대응방첩 활동을 수행하는 데 있다.

미국의 국가방첩전략에는 다음과 같은 네 가지의 핵심 목표가 있다: ① 외국세력·테러그룹·국제범죄조직 및 여타 미국에 위해를 끼치려는 자들의 정보활동 파악 및 정세를 분석, 무력화시키는 것, ② 적의 부인·침투·영향공작·조작 등으로부터 정보수집 및 분석능력을 보호하는 것, ③ 민감한 국가안보작전을 성공적으로 수행할 수 있도록 돕는 것, ④ 우리의 생존에 직결된 국가안보 관련 기밀·극히 중요한 자산·기술 등에 대한 절취·외국으로의 밀 유출·악용 등을 방지하는 것.

우리는 이러한 목표를 성취하기 위하여 적대적 정보활동에 대응한 대간첩활동·대기만활동·공세적 공작활동 등을 포함한 전방위적인 방첩활동 역량 강화계획을 수립한다. 이러한 각급 국가안보기구들은 전략적으로 운용되어야 하며 외국의 위협으로부터 미국을 보호하고 미국의 이익을 증진시키는데 활용되어야 한다.

이 문서는 미국의 광범한 국가안보목표 및 미국이 직면한 외국의 대미첩보활동위협

상황과 관련하여 국가방첩전략을 새롭게 제정한 것이다.

다. 방첩과 국가안보

미국은 현재 국가의 안보, 자유, 번영에 대한 중대한 도전과 직면해 있다. 전 세계적인 테러 및 대량살상무기에 대한 대응, 국가안보의 확립, 국방능력의 강화, 다른 동맹국과의 관계 발전, 경제성장 등을 동시에 이루어 나가야 한다. 이 시점에 적국의 다양한 정보활동은 크나큰 위협이 되고 있다. 외국 정보기관, 적국 테러리스트, 국제 범죄조직, 해커 등이 美국가 안보에 위해를 가하고자 은밀하게 활동하고 있으며 방첩은 바로 이러한 행위를 차단하고 국가 안보를 수호하기 위한 핵심적인 활동이다. (중략)

[미국 안보의 초석이 되는 첨단기술 보호]

미국 국방전략은 우리의 첨단기술을 적극 활용하고 민감한 기술에 많이 의존하는 방향으로 지속적으로 변화하고 있다. 핵심 기밀이 유출되어 적국의 무기설계에 사용된다면 적국보다 전략적 우위를 점하기 위한 우리의 계획이 수포로 돌아갈 수 있다.

우리는 핵심기술과 불가분의 관계에 있는 무기개발에 수십억 달러의 예산을 지출하고 있다. 외국 정보기관이 첨단 기술정보를 절취할 경우 우리가 투자한 자원의 손실은 물론 국가안보상 우위 상실까지 초래하게 된다.

오늘날 90개 이상의 국가들이 우리의 첨단 기술정보를 노리고 있다. 이들은 은밀히 활동하는 단순한 범주를 넘어 미국을 방문하는 사업가, 유치과학자, 유학생, 무역 전시회 등을 활용하고 디브리핑을 통한 정보 수집 등 다양한 방법을 활용하고 있다.

방첩활동은 국가방첩전략에 기반하여 기획·시행되어야 하며 연구소, 전략 시설, 산업시설 등에서도 방첩을 업무의 일부로 생각하여야 한다. 사건이 터진 다음에 과학자·기술자 등 연구개발 인력에 방첩·보안 관련 의무사항을 부과해서는 안 될 것이다. 통합 정리된 방첩 관련 정보가 정부고위관리들에게 제공될 것이며 적절한 때에는 민간기업 보안담당관에게도 제공될 것이다.

광범위한 위기관리 방법, 실질적인 보안 기법 및 전략적인 세계관을 도입하는 것은 외국 정보기관의 위협에 대응할 수 있는 최상의 방법이다. 우리는 민간영역(특히 과학기술 분야)을 대상으로 한 위해정보 제공 및 적들의 다양한 정보 절취·획득 방법에 대

한 교육을 확대, 경각심을 제고할 것이다.

국가 수호의 임무를 수행하는 정부기관들은 중앙·지방 기관, 민간 산업체는 물론 외국과도 정보를 공유하기 위한 새로운 채널을 구축하고 있다. 우리는 적들이 이러한 새로운 체계를 악용할 수 없도록 해야만 한다. 만일 그런 일이 발생한다면 정보공유의 궁극적인 목적은 의미를 잃게 되는 것이다. 테러와의 전쟁 중에 우리는 외국 정부 및 국제기관과 유대관계를 맺어왔으나 그들의 관점과 관심사항은 우리와는 달랐다. 우리는 잠재적인 위험에 대응할 수 있도록 정보를 공유해야하며 동시에 민감한 정보출처, 방법, 작전들은 보호해야 한다.

[방첩활동을 통해 기업간의 공정한 경쟁을 유도, 외국 기관의 정보활동으로 우리기업들이 피해를 입지 않도록 보장]

미국은 시장경제를 도입한 나라이며 우리는 개인의 자유와 국부의 토대인 자유무역의 가치를 높게 평가한다. 하지만 적국이 우리기업의 지적재산권을 침해하고 부당한 이익을 취하려 하는 경우, 해당 무역거래는 불공정한 것으로 판단할 수 있다. 대부분의 외국 경쟁사들이 개방되어 있고 합법적으로 운영되고 있긴 하지만 전부다 그렇다고는 볼 수 없는 상황이다. 심지어 외국정보 기관의 지원을 받는 일부 경쟁사의 경우 미국기업의 첨단기술을 획득하기 위해 전통적인 정보활동 기법을 사용하고 있다. 민감한 영업비밀·지적재산의 유출은 막대한 경제적 피해를 가져올 뿐만 아니라 국가안보의 토대를 허물고 있다. 비합법적으로 미국의 기술을 획득한 외국 기업은 우리기업과 불공정 경쟁을 할 수 있으며 이에 따라 우리 기업은 기술혁신을 위해 또 막대한 연구개발비를 투입해야 한다.

우리 경제가 정보기술과 네트워크가 주는 편리함에 많이 의존하고 있는 지금, 국가의 경제와 안보는 외국정보기관의 전산망 침범과 해킹에 더욱 취약해졌다. 우리는 이러한 위협의 실체를 명확히 밝혀 적절한 대응이 가능토록 해야만 한다.

우리는 미국 산업계 전반에 걸쳐 자행되고 있는 적국의 정보활동을 적발해야 하며 각 기업에 그들의 주도면밀한 활동에 관한 위해정보를 제공, 기업들이 위기에 처하지 않도록 할 것이다. (중략)

라. 결 론

21세기 초, 자유・평화・번영에 대한 전망은 그다지 밝지 않았다. 우리는 아직도 전쟁 중인 국가이며 우리의 조국은 테러에 의해 큰 타격을 입었다. 우리를 향하고 있는 위협은 심대하고 다양하며 이와 함께 외국 정보기관의 위협 또한 복잡성을 띄고 있다. 이러한 위협에 대응하기 위해 미국의 국가방첩전략은 우리의 모든 방첩역량을 동원, 적극성을 띄어야한다.

이러한 전략적 대응은 다음을 포함한다: ① 외국정보기관의 위협(인간, 기술, 사이버)에 대응하기 위한 우리의 방첩역량 개선, ② 방첩 분석・전략적 계획 등 모든 요소를 총 동원, 외국 정보활동의 위협이 미국에 해를 가하기 전 이들을 인지, 평가, 와해하고 이용, ③ 정부의 방첩 요소들을 조정, 통합하고 전략적인 조화를 이루도록 할 것, ④ 국가안보 관련 정부 정책수립에 방첩분야를 활용할 것.

C. 기업의 사이버보안 전략[37]

정보시스템을 보다 안전하게 보호하고 나아가 국가안보를 강화하기 위해 민간부문은 정보보안을 기업경영의 일부분으로 생각하여야 한다. 정보보안은 단순히 기술적인 문제만이 아님에도 불구하고 종종 그렇게 취급되고 있다. 하지만 어떤 조직을 막론하고 정보자산을 보호하기 위해 가장 중요시해야 할 것은 정보보안을 단순히 기술적인 문제가 아닌 조직 경영상 핵심 업무의 하나로 취급해야 하는 것이다.

정보보안경영 특별T/F는 정보보안경영체제를 정부가 주도하기보다는 기업이 자발적으로 시행할 경우 성공할 가능성이 높을 것으로 판단하고 있다. 우리가 적절한 지침과 가이드라인을 제공한다면 국가 사이버공간 방어전략에 대응하는 민간부문에서의 대책마련이 가능하다. 다음의 권고사항들은 일반기업, 비영리단체 및 교육기관 등 전 분야에 걸쳐 폭넓게 적용될 수 있다.

[권고사항] ① 모든 기업들은 경영절차에 사이버보안을 포함시킬 수 있도록 정보보안 경영체제를 도입해야 한다. 특별T/F는 기업들이 효과적으로 정보보안 프로그램을

37) 본 자료는 최근 미국이 첨단기술 유출로 인한 국가경쟁력 저하를 예방하기 위해 관계, 업계, 학계 대표 40여명으로 '정보보안경영 특별 태스크포스팀'을 구성하여 작성한 「미국기업의 사이버보안 전략 보고서」(국가정보원 번역)의 일부분을 발췌한 것임.

시행할 수 있도록 여러 형태의 관리체계를 개발하였다. 정보보안경영체제 도입에 필요한 국제정보보안표준(ISO 17799)과 연방정보보안관리법(FISMA: Federal Information Security Management Act)에 이은 정보보안경영체제(ISG: Information Security Governance)표준이 바로 그것이다.

[권고사항] ② 모든 기업은 정보보안경영체제를 도입하여 이에 따라 시스템을 가동한다는 것을 인터넷 홈페이지를 통해 공지해야 한다. 정보보안경영체제의 도입을 홈페이지를 통해 공지함으로써, 전 미국의 사이버보안 강화를 위한 민간부문의 자발적인 노력을 유도하는데 많은 도움을 줄 수 있을 것이다. 또한 주요 산업협회들은 인터넷 홈페이지 게재에 필요한 정보보안경영체제의 공통 문안과 로고도 필요하게 될 것이다.

[권고사항] ③ 특별T/F팀에 참가한 기업 등이 솔선하여 정보보안경영체제를 도입하고 소프트웨어협회・정보기술협회 등 유관 단체들은 회원사에 이 체제의 적용을 독려・확산해야 할 것이다. 자발적인 참여를 유도하기 위해서는 정보보안경영 특별T/F에 참여한 기업부터 빨리 이 권고사항을 받아들이고 실천해야 한다. 주요 산업 관련 협회・기관 등도 회원사들이 정보보안경영체제를 도입하고 권고사항을 이행할 수 있도록 독려해야 한다. 또한 국가 사이버보안위원회의 참가기관들은 정보보안경영체제를 받아들여 홈페이지에 이를 게시하는 등 구성원 단체가 따라 할 수 있도록 하고, 대기업은 중소기업에까지 정보보안경영체제를 전파할 수 있도록 협력사, 공급사, 고객들과 함께 확산을 추진해야 한다.

[권고사항] ④ 국토안보부는 정보보안경영체제와 이 보고서 핵심내용을 민간부문에 적극 추천하고, 사이버보안이 기업경영의 일부로서 운영될 수 있도록 적극 독려해야 한다. 국토안보부는 모든 기업들이 조기에 정보보안경영체제를 수용할 수 있도록 사회적인 캠페인 등을 전개해야 한다.

[권고사항] ⑤ 미국 공인회계사 협회 등은 회계감사 시 기업의 정보보안경영체제 수립 상태도 감사할 수 있도록 자체 회계감사규정 등을 수정해야 한다. 재무보고 시 IT 기술의 역할에 대해 보다 관심을 더 기울여야 할 필요가 있다. 내부 통제가 적절히 되고 있음을 보여주기 위해서는 IT분야의 통제가 반드시 포함되어야 하며, 최근 회계감사관들도 정보보안이 기업경영관리의 일부분임을 강조하고 있다. 회계와 감사에 관한 참조내용들이 COSO[38]의 내부통제 프레임워크에 이미 포함되어 있지만 정보보안경영체제를 위한 로드맵을 제공하고 있지는 않다. 이에 COSO 가이드라인을 개정하여 정보보

안경영체제를 위한 지침을 제공하게 된 것이며, 우리는 민간기업에서 자체적으로 평가가 가능하고 감사관들도 지속적으로 이 방침을 적용할 수 있도록 할 것이다. 또한 특정 가이드가 없을 때에는 ISO 17799와 함께 COBIT[39]의 내용을 참조할 수도 있다.

정보보안경영체제를 단숨에 도입하여 제대로 이행하기는 어려울 것이며 끊임없는 개선노력이 필요할 것이다. 정보보안경영체제 특별T/F는 민간기업에서 정보보안경영체제를 발전시켜 나갈 수 있도록 지원하고자 권고사항 및 툴을 개발하였다. 하지만 이것만으로는 불충분할 것이다. 이것은 기업정보시스템을 보호하고 나아가 국가안보를 강화하는 시작점이 된다는데 의미가 있다. 특별 T/F에서 제공하는 권고사항과 툴이 기업의 정보보안경영체제를 도입하고 이행하는데 참고사항이 되길 바란다. 무엇보다 가장 중요한 것은 일단 시행하는 것이니 바로 도입하여 점차적으로 발전시켜 나가길 바란다.

D. 미국의『경제스파이처벌법』

미국은 1996년 10월에 경제스파이처벌법(Economic Espionage Act)을 제정하여 시행하고 있다. 아래에서는 그 중에서 영업비밀의 보호에 관한 규정들(제90장: 제1831 - 1839조)을 소개하기로 한다.

제 1831조 경제스파이

(A) 총론 - 외국정부·조직·기관·단체에 이익을 줄 의도를 가지고 있거나 이익을 준다는 것을 알고 있으면서 고의로 ① 영업비밀을 절취하거나, 정당한 권한없이 획득·반출 또는 사취한 자 ② 정당한 권한없이 영업비밀을 복사·복제·스케치·사진촬영하거나 컴퓨터를 통한 자료 송수신·수정·파괴·사진의 복사·전송·발송·제공·우편발송·통화 및 전달하는 자 ③ 정당한 권한없이 입수되었다는 사실을 알면서도 영업비밀을 입수·구매·절취·소유하는 자 ④ 제①항~제③항의 범죄행위를 하려다가 미수에 그친 자 ⑤ 제①항~제③항의 범죄를 음모하거나 또는 둘 이상의 타인과 그 목적

38) COSO(Committee of Sponsoring Organizations of The Treadway Commission): 경영윤리·내부통제·기업지배구조 등의 측면에서 기업경영의 질을 개선하려는 목적으로 1985년 설립된 미국비정부 자율조직임.

39) COBIT(Control Objectives for Information and Related Technology): 미국의 정보시스템 감사 및 통제 협회(ISACA: Information Systems Audit and Control Association)에서 1996년 개발한 정보시스템 통제에 대한 표준 모델임.

달성을 위한 행위를 착수한 자에 대해서는 (B)에 규정한 경우를 제외하고 50만 달러 이하의 벌금, 15년 이하 징역 또는 이 둘을 병과할 수 있다.

(B) 조직 - (A)항에 기술된 불법행위를 범한 조직·단체에 대해서는 1000만 달러 이하의 벌금을 부과할 수 있다.

제 1832조 영업비밀의 절취

(A) 제3자의 경제적 이익을 위하여 주간 또는 국제무역을 위하여 생산된 재화와 관련된 영업비밀을 부정사용할 의사를 갖고 있을 뿐 아니라 영업비밀소유자의 이익을 침해한다는 사실을 인지하거나 의도하면서 고의로 ① 영업비밀을 절취하거나, 정당한 권한없이 획득·반출 또는 사취한 자 ② 정당한 권한없이 영업비밀을 복사, 복제, 스케치, 사진촬영하거나 컴퓨터를 통한 자료송수신·수정·파괴, 사진의 복사·전송·발송·제공, 우편발송, 통화 및 전달하는 자 ③ 정당한 권한없이 입수되었다는 사실을 알면서도 영업비밀을 입수, 구매, 절취, 소유하는 자 ④ 제①항~제③항의 범죄행위를 하려다가 미수에 그친 자 ⑤ 제①항~제③항의 범죄를 음모하거나 또는 둘 이상의 타인과 그 목적 달성을 위한 행위를 착수한 자에 대해서는 (B)에 규정한 경우를 제외하고 벌금, 10년 이하의 징역에 처하거나 또는 이 두 가지를 병과할 수 있다.

(B) 조직 - (A)항에 기술된 불법행위를 범한 조직·단체는 500만 달러 이하의 벌금을 부과할 수 있다.

제 1833조 예외 조항

본 장의 규정은 ① 미합중국 정부기관, 주 정부의 기관 또는 주 소속의 정치단체 등에 의하여 수행되는 합법적 활동과 ② 해당 범죄와 관련 법적 권한이 있는 미합중국 정부기관 및 주 정부의 기관과 주 소속의 정치단체 등에 대한 범죄혐의 조사 보고활동은 금지하지 아니한다.

제 1834조 몰 수

(A) 법원이 본장에서 규정한 범죄행위자를 판결할 때는 다른 형벌 선고에 부가하여 다음에 열거하는 재산의 미합중국 정부 몰수를 병과해야 한다. ① 본 장에서 규정한 범죄행위로 인하여 직·간접적으로 획득한 재산이나 파생된 재산 ② 법원이 그 성격, 범위, 중요도 등을 고려하여 판단해서 범죄의 수행 또는 범죄수행의 촉진을 위해 어떠한 형태로든 사용되었거나 사용이 의도되었다고 결정한 개인이나 조직의 재산

(B) 본 조 규정에 대하여 몰수될 재산, 재산의 압류처분 그리고 이와 관련된 행정 · 사법상의 절차는「1970년 포괄적인 약물남용금지 및 통제법」제413조(몰수가 적용되지 않는 (d)와 (j)항은 제외)가 적용된다.

제1835조 비밀유지 명령

법원은 본 장에 근거하여 기소 또는 다른 절차를 수행함에 있어 연방 형사·민사소송법, 연방증거법 및 적용 가능한 법의 요건과 일치하는 범위 내에서 영업비밀을 유지하기 위한 명령이나 기타 필요하고도 적절한 조치를 취해야 한다. 미국정부에 의한 중간 항소는 영업비밀 공개를 허가하거나 지시하는 법원의 명령 또는 결정에 근거하여야 한다.

제 1836조 위법행위 금지를 위한 민사절차

(A) 법무장관은 민사소송을 통해 본조 위반행위에 대한 적절한 법적 구제를 받을 수 있다.

(B) 美 연방법원은 본 조항에 의하여 민사소송에 대해 배타적 재판 관할권을 갖는다.

제 1837조 국외행위에 대한 적용

본 장의 규정은 다음에 열거한 경우에는 미국 밖에서 발생한 행위에 대해서도 적용된다. ① 위반자가 미국시민이거나 영주권자 또는 미국법에 의하여 설립된 기관이거나 정치단체인 경우 ② 위반을 조장하는 행위가 미국내에서 이루어진 경우

제 1838조 타 법률과의 관계

본 장 규정은 영업비밀의 불법사용을 규제하는 다른 미 연방법, 주법, 공공기업법, 소유권법, 토지법 등에서 규정한 민·형사상의 구제조치에 우선하거나 대신하는 것으로 해석할 수 없으며 (정보자유법으로 알려진) 제5편 552조에 규정된 정부관리의 적법한 정보공개행위에 대해서는 영향을 미치지 아니한다.

제 1839조 용어의 정의

본 장에서 사용된 ①「외국기관」이라 함은 외국 정부에 의해 실질적으로 소유, 통제, 지원되거나 경영되는 모든 기관, 부서, 재단, 협회, 사업조직, 주식회사 및 상사 등을 의미한다. ②「외국 에이전트」라 함은 외국정부의 모든 관리, 피고용인, 대리인, 대표단 또는 대표를 의미한다. ③「영업비밀」이라 함은 유형·무형을 불문하고 문자적, 물리적, 전기적 형식에 의한 저장·축적여부와 관계없이 공정, 계획, 공구, 프로그램 고안, 공식, 디자인, 사진, 진행 및 절차, 프로그램, 코드를 포함한 모든 형태의 재정적, 사업적, 과학적, 기술적, 경제적 정보로서 다음의 경우를 의미한다. a) 영업비밀의 소유자가 그러한 정보를 비밀로 유지할 수 있도록 하는 합리적 조치를 취하고 b) 그 정보가 실질적 또는 잠재적 가치가 있는 것으로서 일반적으로 알려지지 않았고, 일반인들이 정당한 수단을 통해 쉽게 확인할 수 없는 경우 ④「소유자」라 함은 영업비밀에 대한 정당한 법적 소유권이나 면허를 소지하고 있는 사람 또는 기관을 의미한다.

(2) 독일의 첨단기술 유출방지 노력[40]

A. 독일의 민관산업보안활동 개관

독일정부는 1990년 부정경쟁방지법을 제정하는 등 산업기술 보호를 위해 지속적으로 관련 법령 및 제도를 정비해 오고 있으며 기업들은 산업기밀 보호의 주체로서 자체 보안부서 및 전담직원을 두고, 기술보호·안전 등 기업 보안활동을 수행하면서, 주 산업보안협회를 매개로 정부기관과 정보교류 등 긴밀한 민관협력 관계를 유지하고 있다. 또

40) 국가정보원, 첨단산업기술보호동향 제4호: 31-39.

한 1993년 독일산업연맹(BDI) 등 중앙 경제단체들과 9개의 주 산업보안협회를 회원으로 하는 연방산업보안협회(ASW)를 구성하여 산업보안 관련 경제계의 입장을 연방 정부에 전달하고 관련 정보를 활발히 교류하고 있다. 최근 들어서는 각 부처가 수집한 산업보안 관련 정보를 연방총리실이 종합하여 연방산업보안협회 등을 통해 기업에 지원하는 한편 기업체와 정부간 간담회를 통해 기업체의 산업보안 관련의견을 수시로 수렴하는 등 협조체제를 더욱 강화하고 있다.

B. 독일정부의 산업보안활동 실태

가. 민간기업에 대한 정보지원 체계

독일 정부차원의 산업보안활동에는 총리실 등 10여개 부처가 참여하고 있으며 총리 등 최고위층의 관심도 상당히 높다. 관계기관은 수집한 산업보안 정보를 연방총리실에 지원하고, 연방총리실이 이를 토대로 보고서를 작성, 연방산업보안협회에 정기지원(서면)하며 연방산업보안협회는 이 자료를 E-mail을 통해 회원사에 발송한다. 그러나 보안 및 출처보호 문제로 발송되는 정보의 내용은 제한적이며 민감한 정보는 구두로 별도 제공하고 있다. 활동을 주도하는 부처는 연방 총리실 및 연방 내무부로서, 연방 총리실 직원이 연방산업보안협회 주관으로 개최되는 주요 기업체간 정기 간담회에 참석하여 기업의 산업보안 관련 요구사항을 수렴하는 한편 정부기관이 수집한 정보를 브리핑하기도 한다.

나. 산업스파이 행위에 대한 대응

산업스파이 행위는 주 경찰이 처리하는 것이 원칙이나, 기업이 협조를 요청하거나 위험한 사태라고 판단될 경우, 예를 들면 핵, 잠수함 등 민감한 기술 유출이 의심될 경우에는 연방정보부(BND)나 연방헌보청(BfV)이 개입한다. 또한 각 주 헌보청 등은 산업보안 관련 세미나 등에서 주제발표를 하거나「보안포럼」에 참여, 최근 산업보안 동향에 대한 브리핑을 실시하고, 기술유출에 대한 경각심 제고 및 실무지식 전파를 위해 교육을 실시하거나 '노하우 보안'등 책자를 발간, 배포하며, '산업스파이 예방을 위한 10가지

황금률', '기업 보안관리 수준 확인을 위한 자가 테스트' 등을 작성, 기업에 지원하고, 1999년부터 스파이방어 전용 '은밀한 전화'를 개설, 24시간 신고상담 체제를 구축하고 있다.

C. 독일의 산업보안관련 법령 및 제도

가. 독일의 산업보안 관련법령

독일의 영업비밀 보호관련 기본법규는 '부정경쟁방지법'(Gesetz gegen den unlauteren Wettbewerb)이며 그 외 '노동법', '민법', '형법' 등을 근거로 민·형사상 대응을 할 수 있다. 독일의 부정경쟁방지법은 우리나라의 영업비밀보호법과 유사하나, 친고죄를 원칙으로 하고 공공의 이익을 위해 필요하다고 인정되는 경우에만 피해자의 고소 없이 기소할 수 있으며, 미수범은 인정되나 예비, 음모는 처벌할 수 없으며 3년 이하의 징역 또는 벌금에 처할 수 있다(외국 유출시에는 5년 이하). 또한 '부정경쟁방지법' 이외에도, 근로계약을 맺은 자에 대해서는 노동법·민법·형법에 의해, 제3자에 대해서는 민법·형법에 의해 영업비밀 침해에 대한 민·형사 소송 제기가 가능하다. 기술유출 방지를 위한 '동종업계전직금지' 계약과 관련, 퇴직예정 직원과 전직금지 계약을 맺는 것이 가능하며 일부 기업에서는 실제 체결하는 경우도 있으나, 전직금지기간은 최고 1년에 그치며 그 기간 동안은 회사에 근무하는 것과 동일한 수준의 급여 지급이 필요하다.

나. 독일의 산업보안 전문가 육성실태

독일의 산업보안 인력은 연방 및 주 산업보안협회, 기업체 보안부서, 민간 보안업체 등에서 주로 근무하고 있는데, 고졸자를 대상으로 한 3년 과정의 직업교육과정을 수료한 인력도 일부 있으나 군, 경찰 등 정보수사기관 퇴직자들이 주축을 이루고 있으며, 최근 민간부문에 보안전문가 수요가 증가하면서 정보수사기관의 인력들이 많이 전직하고 있는 상황이다. 산업보안 전문가는 "상의인증 보안전문가" 제도에 의해 자격을 인정받는데, 기업에서 보안업무에 종사하는 인력 등이 주 산업보안협회가 주관하는 교육을 받고 주 상의가 주관하는 시험에 합격함으로써 자격을 취득하게 되며, 주 산업보안협회의 교육은 총 200시간으로 법률 및 상황대처, 보호기법 등의 내용으로 구성되어 있고,

주 상의가 주관하는 시험의 응시자격은 ① 직업교육과정 수료 후 기업 보안관련 부서 2년 이상 근무자, ② 6년간 기업 근무경험 있고 보안부서 2년 이상 근무자, ③ 기타 특별한 경우 보안관련 능력이나 경험을 제시할 수 있는 자로 한정된다.

D. 독일의 『부정경쟁방지법』

독일은 1990년 10월에 부정경쟁방지법을 제정하였으며, 2002년 8월에 21차 개정하여 오늘에 이르고 있다. 아래에서는 영업비밀 관련조항만 발췌하였다.

제1조(일반조항) 업무상의 거래에서 경업의 목적으로 선량한 풍속에 반하는 행위를 하는 자에 대해서는 그 행위의 유지 및 손해배상을 청구할 수 있다.

제17조(영업비밀의 누설) ① 기업의 종업원, 근로자 또는 견습공으로서 근로관계에 의해 위탁받거나 접근 가능한 영업비밀을 고용기간 동안에 경업목적, 자신의 이익, 제3자의 이익을 위하여 또는 사업체의 보유자에게 손해를 가할 목적으로, 권한 없이 누군가에게 전달한 자는 3년 이하의 징역 또는 벌금에 처한다.

② 경업의 목적 또는 자신의 이익을 위해, 제3자의 이익을 위하여 또는 사업체의 보유자에게 손해를 가할 목적으로 1. 영업상 또는 경업상의 비밀을 a. 기술적 수단의 사용 또는 b. 기밀의 복제 또는 c. 기밀이 복제된 물건의 탈취에 의해 권한없이 취득 또는 확보하거나 2. 제1항에 정해진 통지 또는 제1호에 의한 자기 또는 타인의 행위에 의해 취득한 영업상 또는 경영상의 비밀, 혹은 기타의 권한없이 입수하거나 확보한 영업상 또는 경영상의 비밀을 권한없이 이용하거나 또는 어떤 자에게 통지한 자는 전항과 같은 형을 처한다.

③ 미수범은 처벌한다.

④ 특히 중한 사태에서는 형벌은 5년 이하의 자유형 또는 벌금으로 한다. 행위자가 통지를 함에 있어, 비밀이 외국에서 이용되는 것임을 알고 있는 경우, 또는 행위자 스스로 외국에서 이용하는 경우에는 원칙적으로 중한 사태에 해당한 것이 된다.

제18조(영업비밀의 누설) 업무상의 거래에서 자기에게 위탁된 도면, 모형, 형, 형지 또는 처방을 경업의 목적 또는 자기의 이익을 위해 권한없이 이용하거나 제3자에게 전

달 통지한 자는 2년 이하의 자유형 또는 벌금에 처한다. 전조 제4항은 본조의 경우에 준용한다.

제19조 제17조 및 제18조의 규정에 위반한 자는 동시에 발생한 손해를 배상할 의무를 진다. 의무자가 수인 있는 때에는 연대채무자로 된다.

제20조 ① 경업의 목적 또는 자기의 이익을 위해 제3자를 유혹해서 제17조 또는 제18조에 위반한 행위를 시키려고 시도한 자 또는 이와 같은 위반행위를 시키려고 하는 타인의 제의를 받아들인 자는 2년 이하의 자유형 또는 벌금에 처한다.
② 경업의 목적 또는 자기의 이익을 위해 제3자를 유혹해서 제17조 및 제18조에 위반한 행위를 하려고 제의한 자, 또는 타인의 요구에 대해서 그 같은 행위를 할 용의가 있는 뜻을 표시한 자는 전항과 같은 형에 처한다.
③ 형법전 제 31조(범죄행위 협력·참가 시도 처벌 규정)를 적용한다.

제20조의A 제17조, 제18조 및 전조에 위반한 행위에 대해서는 형법전 제5조 제7호(국외범 처벌규정)의 규정을 적용한다.

제21조 ① 본법에 제기된 중지 또는 손해배상 청구권은 청구권자가 당해 행위 및 의무자를 안 때로부터 6개월간 행사하지 아니한 때에는 시효에 의해 소멸한다. 청구권자의 인식의 유무를 불문하고 행위시로부터 3년을 경과한 때에도 동일한 것으로 한다.
② 손해배상청구권에 대하여는 손해의 발생 전에는 시효의 진행을 개시하지 않는다.

(3) 일본의 기술 유출방지 노력

최근 일본 정부는 자국핵심연구원의 해외취업이나 외국기업의 적대적 인수·합병에 따른 기술정보 유출방지를 위해 관련 법제를 정비하고 있으며 각 기업들에서도 자사보안관리 대책을 강화하고 있다.[41]

41) 국가정보원, 첨단산업기술보호동향 제2호: 2-6, 9-11.

A. 정 부

일본에서는 최근 증가하고 있는 외국기업의 고급인력 스카우트와 적대적 인수·합병으로 핵심기술 및 기업정보가 해외로 유출, 기업경쟁력이 약화되고 있다는 인식이 확산되고 있다. 이에, 경제산업성은「기업가치연구회」를 설치, 2005년 중으로 기업비밀 보호 및 기술유출 대응책을 구체화할 예정으로, 장기근속·기술개발 성과 등에 연동한 스톡옵션제 도입, 정규직 확대, 비밀유지·동일업종으로의 전직 금지계약 체결 등을 통해 장기적인 고용환경을 개선함으로써 우수 핵심연구원의 해외유출을 방지하고, 적대적 인수·합병으로 부터 일본기업을 보호하는 방안으로 종업원 주주제도 확대, 신주발행에 의한 주주 증원·'독약계획'[42] 허용 등 적극적 경영권 방어수단을 위한 연구도 진행할 계획이다.

또한 경제산업성은 첨단 IT기술 해외유출 방지를 위한 관련 법제 정비를 추진 중으로 연료전지·디지털가전·LCD 등 신산업 육성전략을 마련한 데 이어 유관기업에 대해 관련기술 국외유출 방지에 전력토록 권고하고, 특허기술의 해외이전과 해외 공장내 사용을 엄격하게 통제하는 방향으로 부정경쟁방지법 개정을 추진하는 한편, 상공회의소와 공동으로 04.10월부터 05.2월간 전국 16개 지역에서 기업 정보보안 담당자 대상 "정보보안 세미나"를 개최, 최신 보안정보·관련 대책 등을 발표할 예정이다.

그러나 일본 내 일부에서는 프랑스 르노의 닛산자동차 인수 등 M&A를 통해 선진 경영기법을 도입하여 기업재생을 도모한 케이스를 언급하면서, '독약계획'은 미국에서도 적용 사례가 감소 추세에 있고 일본 상법상으로도 주주평등의 원칙에 위반된다고 지적하며, 일본정부가 국제적인 M&A 흐름에 역행하는 정책을 채택, 외국으로부터 통상마찰을 초래하는 딜레마에 봉착할 수 있다고 지적하였다.

B. 기 업

일본 기업들에서도 중요기술 보호를 위한 각종 보안제도를 도입하고 있는 바, 제조업체들의 경우도 중국 등 해외 현지공장에서의 핵심기술 유출사고 증가 등을 이유로 자국 내 생산공장 설립을 확대하고 있다.

---

42) 독약계획(Poison pill right plan)이란 적대적 기업인수 시도에 대한 방어수단으로 피인수 기업 주주에게 합병시 주식을 극히 낮은 가격에 인수할 수 있는 권리등을 부여하는 것을 말한다.

LCD 패널을 생산하는 샤프는 첨단 LCD 가공기술의 열람범위를 극소수 임원으로 한정하고, 특허등록도 피하는 블랙박스 전략을 사용 중으로, 올해 초 1,000억 엔을 투입, 액정 패널·TV 등 일괄 생산을 위해 설립한 미에·가메야마 공장의 경우 공장 전체를 파악할 수 있는 임원은 마치다 가츠히코 사장이하 극소수 임원뿐이며, 공장 종업원에 대해서도 소속 외 다른 부서의 출입을 엄격히 금지하고 카메라폰의 공장 내 반입을 전면 금지하였으며, 완제품 공장을 해외에 설립할 경우에는 기술유출의 우려가 있다고 판단, 향후 2년간 확장 및 신설하는 5개 공장 모두를 일본 내에 설립하는 방안을 검토하였다.

캐논의 경우 제조용 기계와 공구를 회사 외부에서 구입하지 않고 회사 내에서 직접 제작·사용함으로써 기술관련 정보의 외부유출을 원천차단하고 있으며, 마츠시다는 가전 디자이너(270명)중 최상급 연구원이 퇴직할 경우 과제위탁 계약을 체결, 경쟁국 업체로 취업하는 것을 차단하는 퇴직자 관리 제도를 시행중이다.

한편, 니혼게이자이 신문은 주요 제조업체 115개사를 대상으로 자국 내 생산공장 건설 계획을 조사한 결과, 향후 3년간 국내생산을 확대할 기업이 대상 업체의 절반에 달하고 있다고 보도하였다. 조사에 참여한 기업들은 중국 등 해외 현지공장에서 경쟁력의 원천인 기술유출 사례가 지속 증가함에 따라 기술유출을 사전 차단하는 동시에, 첨단제품 주개발거점이 일본 내에 있으므로 개발·생산·출하과정의 순환이 용이한 일본에서 공장을 운영하는 것이 유리하다면서, 해외 공장에서는 범용제품을 지속 생산하되, 고부가가치 제품의 경우는 다시 자국에서 생산하는 방안을 검토 중이라고 답변하였다. 또한, 동 신문은 이러한 국내생산 확대의 원인을 일본이 구조조정 등 힘겨운 과정을 거치면서 “Made in Japan”으로 글로벌 경쟁에서 승리할 수 있다는 자신감을 되찾은 것이라고 설명하였다.

C. 지적재산권보호활동

일본은 지난해 국내특허 39만 건, 해외특허 22만 건을 출원하고 해외 로얄티 수입을 35억불이나 거둔 지적재산권 강국이나, 지적재산권에 대한 침해사례도 지속 증가, 지난해 일본세관의 위조 상품 수입적발 건수는 7,412건으로 6.2% 증가하였으며 외국기업의 지재권 침해에 대한 일본기업의 제소건수도 206건을 기록하였다.

일본 재무성은 주요국과 위조품 단속협력을 강화하기 위해 EU와는 세관업무 상호지

원협정, 중국 및 아시아 국가와는 위조품 수출업자에 대한 정보공유협정 체결을 각각 추진하고, 외무성은 일본 위조품 범람에 적극 대응하기 위해 189개 해외공관에 “지적재산권 보호 대응 매뉴얼” 을 배포하는 한편 지적재산권 보호 담당관을 금년 안에 임명할 방침이라고 발표하였다. 경제산업성은 위조 상품 수출입 업자를 형사처벌 대상에 포함하고, 해외 불법기술 지도에 대해서도 처벌할 수 있도록 법 개정을 추진 중이며, 무역보험 적용대상을 지재권 사용료 등으로 확대한 후 최초로 태국에 수출되는 애니메이션 비디오 판권을 보험대상으로 지정했고, 향후 게임・영화・음반 등으로 대상을 확대할 계획이다. 농림수산성도 일본에서 육성된 우량품종의 무단사용을 방지하기 위해 “품종조사수사관”을 신설하고 무단사용 입증 필요성에 대비, DNA 분석대상 품목을 확대하는 등 대책 마련에 착수하였다.

한편, 지재권 침해에 적극 대응하고 유기적 협력체제 구축을 위해 총무・법무・문부・농림수산・경제산업성, 경찰청 등이 참가하는 “모방품・해적판 관계성・청 회의”를 설치하였는데, 동 회의에서는 각 성・청들이 모방품・해적판에 대한 정보를 공유할 수 있는 데이터베이스를 구축, 해외에서의 피해사항을 파악하여 국내유입 방지 등에 활용하고, 실효성 있는 정책입안 및 관련 법률・제도개정 등을 조속 추진할 것을 합의하였다.

D. 일본의 『부정경쟁방지법』

일본은 1993년 5월에 『부정경쟁방지법』(법률 제47호)을 제정하였으며, 2003년 5월에 개정하여 시행하고 있다.

제1조(목적) 이 법률은 사업자간 공정한 경쟁 및 이와 관련된 국제 협약의 정확한 이행을 위하여 부정경쟁의 방지 및 부정경쟁에 관계된 손해배상에 관한 조치 등을 강구함으로써 국민 경제의 건전한 발전에 기여하는데 목적이 있다.

제3조(금지청구권) ① 부정경쟁에 의하여 영업상의 이익을 침해받거나 침해받을 우려가 있는 자는 그 영업상의 이익을 침해한자 또는 침해할 우려가 있는 자에 대하여 그 침해의 정지 또는 예방을 청구할 수 있다.

② 부정경쟁에 의하여 영업상의 이익을 침해받거나 침해받을 우려가 있는 자는 전항의 규정에 의한 청구를 할 때에는 침해행위를 조성한 물건(침해행위에 의하여 생긴 물

건을 포함한다)의 폐기, 침해행위에 제공된 설비의 제거, 그 밖의 침해의 정지 또는 예방에 필요한 행위를 청구할 수 있다.

제4조(손해배상) 고의 또는 과실에 의한 부정경쟁 행위로 타인의 영업상의 이익을 침해한 자는 침해에 의하여 생긴 손해를 배상할 책임을 진다.

제7조(신용회복의 조치) 법원은 고의 또는 과실에 의하여 부정경쟁 행위로 타인의 영업상의 신용을 해쳤던 자에 대하여는 그 영업상의 신용이 침해된 자의 청구에 의하여 손해배상에 갈음하거나 손해배상과 함께 그 자의 영업상의 신용을 회복하는데 필요한 조치를 명할 수 있다.

제9조(외국의 국기 등의 상업상의 사용 금지) ① 누구라도 외국의 국기 또는 국가의 문장, 그 밖의 기장으로 경제산업성 령으로 정한 것(이하「외국 국기 등」이라고 한다)과 동일 또는 유사한 것(이하「외국 국기 등 유사 기장」이라고 한다)을 상표로 사용하거나 외국 국기 등 유사 기장을 상표로 사용한 상품을 양도, 인도, 양도 또는 인도를 위해 전시, 수출, 수입하거나 외국 국기 등 유사 기장을 상표로 사용하고 역무를 제공할 수 없다. 단, 그 외국 국기 등의 사용허가(허가에 유사한 행정처분을 포함한다. 이하 동일)를 행한 권한이 있는 외국 관청의 허가를 받았을 때는 그러하지 아니하다. (중략)

제10조(국제기관의 표장의 상업상의 사용 금지) 누구라도, 그 국제기관(정부간의 국제기관 및 이것에 준한 것으로 경제산업성 령으로 정한 국제기관을 말한다. 이하 이 조에 있어 동일)과 관계가 있다고 오인시키는 방법으로 국제기관을 표시한 표장으로 경제산업성슈으로 정한 것과 동일 또는 유사한 것(이하「국제기관 유사 표장」이라고 한다)을 상표로 사용하거나 국제기관 유사 표장을 상표로 사용한 상품을 양도, 인도, 양도 또는 인도를 위해 전시, 수출, 수입하거나 국제기관 유사 표장을 상표로서 사용하고 역무를 제공할 수 없다. 단, 이 국제기관의 허가를 받았을 때는 그러하지 아니하다.

제11조(외국 공무원 등에 대한 부정 이익의 공여등의 금지) ① 누구라도 외국 공무원 등에 대하여 국제적 상거래 관련 영업상의 부정 이익을 얻기 위해 그 외국 공무원

등에 그 직무에 관한 행위를 시키거나 시키지 않거나 그 지위를 이용하여 다른 외국 공무원 등에게 그 직무에 관한 행위를 시키거나 시키지 않도록 알선할 목적으로 하여 금전 그 밖의 이익을 공여하거나 그 청약 또는 약속을 해서는 아니된다. (중략)

제14조(벌칙) 다음 각 호에 해당한 자는 3년 이하의 징역 또는 3백만엔 이하의 벌금에 처한다. 1. 부정의 목적으로 제2조 제1항 제1호 또는 제13호에 언급한 부정경쟁을 행한 자 2. 상품 또는 역무 또는 그 광고 또는 거래에 이용한 서류 또는 통신에 그 상품의 원산지, 품질, 내용, 제조방법, 용도, 수량 또는 그 역무의 질, 내용, 용도 또는 수량에 관하여 오인시킬 수 있도록 허위 표시를 한 자(전호에 언급한 자를 제외한다) 3. 제9조, 제10조 또는 제11조 제1항의 규정에 위반한 자

제15조 법인의 대표자 또는 법인 또는 사람의 대리인, 사용인 그 밖의 종업원이 그 법인 또는 사람의 업무에 관하여 제14조의 위반 행위를 한 때에는 행위자를 처벌하는 한편 그 법인에 대하여 1억 엔 이하의 벌금형을 그 사람에 대하여 제14조에서 정한 형을 부과한다.

(4) 중국의 지적재산권 보호활동

A. 개 요

중국 정부는 미국・일본 등의 지속적인 요청에 따라 자국내 지적재산권 침해사범 형사처벌을 강화하고 전국적인 단속활동을 전개하는 등 지적재산권 침해에 대해 적극 대응키로 결정하였다.

최근 중국내 지재권 침해와 관련하여 알도나스 미 상무부 차관은 04.9.15 중국 방문시 중국 지방당국은 미국기업들에게 타격을 주고 있는 지적재산권 침해행위를 엄중 단속하여야 한다고 요구하였으며, 래시 상무부 차관보도 8월 중국내 지적재산권 침해행위에 지방 관리들이 가담하고 있음이 분명하며 이는 조직범죄라고 주장하였다. 또한, 일본 경단련 오쿠타 회장도 9.14 보시라이 중국 상무부장과의 접촉시 중국내 모방품과 해적판 제작 등 지적재산권 침해사범에 대한 강력한 형사처벌 도입을 요청하였다.

이에 보시라이 상무부장은 지난 5년간 지적재산권 단속요원을 대폭 증원하는 등 단

속에 전력을 다하고 있으며 향후 법률개정 등을 통해 강력한 형사처벌을 도입할 예정이라고 설명하였다. 또한 장즈강 상무부 부부장도 2005년 8월까지 1년간 주요 도시와 전국 15개성을 대상으로 해적판 생산·상표권 침해에 대한 일제 단속을 실시할 계획이며, 공안부, 신식산업부, 상무부 등 12개 정부기관이 참여하는「국가지적재산권보호공작조」를 설립하였다고 발표하였다.

한편 영국 파이낸셜 타임스는 9.20 중국정부의 강력한 지적재산권 침해 단속발표 이후 스위스 "신젠타"가 자사농약 특허침해를 이유로 중국 법원에 제소한 소송에서 승소판결을 받았다고 보도하였다. 그러나 외국정부와 기업들은 중국정부의 지재권 침해행위 단속강화에도 불구하고 아직도 중국이 지재권 보호에는 관심이 없는 것 같다고 중국정부의 의지에 의구심을 표명하였다.[43]

B. 중국의 『부정경쟁방지법』

중국은 1993년 9월 2일 제8회 전국인민대표대회 제3차 회의에서 『부정경쟁방지법』을 통과시켰으며, 1993년 9월 2일 중화인민공화국 주석령 제10호로 이를 공포하였다. 이 법은 모두 5개의 장으로 구성되어 있으나 제2장의 내용만 소개하기로 한다.

제2장 부정경쟁행위

제5조 경영자는 다음에 열거된 부정한 수단을 사용하여 시장교역 행위를 하거나 경쟁 상대에게 손해를 입혀서는 안된다. 1. 타인의 등록상표를 사칭하는 행위 2. 유명상품 고유의 명칭·포장·장식 또는 유명상표와 유사한 명칭·포장·장식을 임의로 사용함으로써 타인의 상품과 혼동을 일으켜 구매자로 하여금 그 유명상품으로 오인하도록 하는 행위 3. 타인의 기업명칭 또는 성명을 임의로 사용함으로써 타인의 상품으로 오인하게 하는 행위 4. 상품에 인증표시·우량표시 등 품질표시를 위조 또는 도용하거나, 원산지를 위조하여 상품품질에 대하여 오인을 일으키게 하는 행위

제6조 공기업 또는 기타 법에 의하여 독점적 지위를 누리고 있는 기업의 경영자는

43) 국가정보원, 2004, 첨단산업기술보호동향 제2호: 12-13.

다른 경영자의 공정한 경쟁을 배제할 목적으로 타인이 그 지정된 경영자의 상품을 구매하도록 한정하여서는 안된다.

제7조 정부 및 소속기관은 행정권력을 남용하여 타인이 그 지정된 경영자의 상품을 구매하도록 한정하거나 다른 경영자의 정당한 경영활동을 제한하여서는 안된다. 정부 및 소속기관은 행정권력을 남용하여 외지상품의 본지시장 진입을 제한하거나 본지상품의 외부시장 유출을 제한하여서는 안된다.

제8조 경영자는 재물이나 기타 수단을 사용하여 상품을 판매 또는 구매할 목적으로 뇌물을 제공하여서는 안된다. 장부기재를 하지 않고 뒷거래로 상대 회사 또는 개인에게 리베이트를 주는 경우 뇌물을 제공한 것으로 처리한다. 상대 회사 또는 개인이 뒷거래로 리베이트를 받은 경우에도 뇌물 수수로 처리한다. 경영자는 상품 판매 또는 구매시 명시적 방법으로 상대방에게 리베이트를 주거나 중개자에게 커미션을 줄 수 있다. 경영자가 상대방에게 리베이트를 주거나 중개자에게 커미션을 주는 경우에는 반드시 사실대로 장부에 기재하여야 하며, 리베이트나 커미션을 받은 경영자도 반드시 사실대로 장부에 기재하여야 한다.

제9조 경영자는 광고나 기타 수단을 이용하여 상품의 질량・성분・성능・용도・생산자・유효기간・생산지 등에 대해 허위선전을 하여 오인을 일으키게 하여서는 안된다. 광고 사업자는 명확히 인지하고 있거나 인지할 수 있는 상황에서 허위광고를 대리・설계・제작・유포하여서는 안된다.

제10조 경영자는 다음에 열거한 수단을 사용하여 영업비밀을 침해하여서는 안된다. 1. 절취・기망・협박 기타 부정한 수단으로 권리자의 영업비밀을 취득하는 행위 2. 위 항목의 수단으로 권리인의 영업비밀을 공개・사용하거나 제3자가 사용하도록 허가하는 행위 3. 약정 또는 권리인의 영업비밀보호 관련 요구를 위반하거나 취득한 영업비밀을 공개・사용 또는 제3자가 사용하도록 허가하는 행위 (중략)

제11조 경영자는 경쟁상대를 배제할 목적으로 원가보다 낮은 가격으로 상품을 판매

하여서는 안된다. 다음에 열거한 사항에 해당하는 경우는 부정경쟁행위에 속하지 않는다. 1. 신선한 상품을 판매하는 행위 2. 유효기간이 곧 도래하는 상품 또는 재고 상품을 처리하는 경우 3. 계절성 가격인하 4. 채무상환·제품전환·휴업 등으로 인해 제품가격을 인하하여 판매하는 경우

제12조 경영자는 구매자의 의지에 반하여 상품을 끼워서 팔거나 기타 불합리한 조건을 부가하여서는 안된다.

제13조 경영자는 다음에 열거한 경품판매에 종사하여서는 안된다. 1. 경품을 제공한다고 속이거나 고의로 경품 대상자를 내정하는 방식으로 경품 판매를 하여서는 안된다. 2. 경영자는 경품판매 방식을 사용하여 저질 상품을 고가에 판매하여서는 안된다. 3. 추첨식 경품판매는 최고 당첨금액이 5천元(약 70만원)을 초과하여서는 안된다.

제14조 경영자는 허위사실을 날조하거나 유포하여 경쟁 상대방의 상업신용·상품명성을 저해하여서는 안된다.

제15조 입찰자는 입찰과정에 관여하여 가격을 높이거나 내려서는 안된다. 입찰자와 입찰공고자는 경쟁상대방의 공정한 경쟁을 배제할 목적으로 상호 결탁하여서는 안된다.

(5) EU의 지적재산권 보호활동

EU 집행위는 외국의 불법복제·기술도용으로 부터 역내 업계를 보호하기 위해 “대외 지적재산권 보호강화 전략”을 수립하였는바 그 주요내용은 다음과 같다: (1) 외국의 지적재산권 침해실태 조사를 정기적으로 실시하고, 동 결과를 바탕으로 “우선감시대상국”(Priority Country)을 지정, 중점 관리한다. (2) WTO/TRIPs 협정의 미비점을 개선하는 한편 주요 교역국과의 무역협정상 지적재산권 관련규정을 정비한다. (3) 세계지적재산권기구(WIPO) 등과의 공조 하에 법령, 인프라 미비로 지적재산권 침해행위 근절에 어려움을 겪고 있는 개도국에 대해 기술적 지원을 확대한다. (4) “무역장벽규정”(TBR) 등 분쟁해결제도 활용을 장려하고, 민간업계와 회원국 정부·EU 집행위 전문가 간 협력체제를 구축한다. (5) 이와 동시에 유럽기업들은 지적재산권 보호를 위해 각종 대책

을 철저히 수립한 후 생산라인의 동구국가 이전 및 연구·사무업무를 중국·인도 등으로 외주를 주는 방안을 검토 중이다.[44]

6. 한국 상황에의 시사점

1) 국내 산업스파이 사건의 특징 및 유형

1998년부터 2005년 6월까지 국내에서 적발된 산업스파이 사건은 총 82건이며, 업계추산 약 76조 9,529억원의 피해를 예방한 것으로 집계되었다. 최근 국내에서 발생한 산업스파이 사건의 특징과 실태를 유형별로 분석해보면 아래와 같다.[45]

(1) 산업스파이 사건의 특징

최근에 국내에서 발생한 산업스파이 사건의 특징을 살펴보면 첫째, 피해가 해당 기업에만 그치지 않고 국가경제에까지 악영향을 미쳤고, 둘째, 대부분 기술개발 참여자가 죄의식 없이 자행한 것이었으며, 셋째, 단발성 범죄로서 범행증거의 확보 및 추적이 곤란하였고, E-Mail, 복사 등의 방법으로 유출하여 피해사실의 인지가 곤란하였다는 특징을 갖는다.

(2) 분야별 산업스파이 사례분석

분야별로 산업스파이 사건사례를 살펴보면 휴대폰·모니터 등 IT분야 유출기도 현상이 심화되고 있는 실정인 것으로 나타났다. 휴대폰과 LCD·PDP모니터 등 차세대 선도기술 분야에 대한 기술유출기도가 전체 82건 중 59건(72%)을 차지하는 등 편중현상이 심화되고 있다.[46]

---

44) 국가정보원, 2004, 첨단산업기술보호동향 제2호: 11.
45) 국가정보원(http://www.nis.go.kr/docs/terror/indus/type.html).
46) 2003년 10월, 국내 A社 간부가 대만 Z社와 공모, PDP제조기술 유출을 기도하다 적발됨.

<표 3-1> 분야별 산업스파이 사례

유출분야	정보통신	전기전자	정밀기계	생명공학	정밀화학	기타
82건	27건	32건	10건	5건	4건	4건

(3) 신분별 산업스파이 사례분석

신분별로 산업스파이 사건사례를 살펴보면 전·현직 직원의 보안관리가 부실한 실정인 것으로 나타났다. 전·현직 직원에 의한 기술유출이 82건 중 73건(89%)을 차지할 정도로, 내부 인적 위해요소에 의한 기술유출사건 발생이 빈번하였다.[47] 연구원들의 경우, 본인이 개발한 기술은 본인 소유라는 인식이 강하여 죄의식 없이 개발기술을 유출·사업화하는 경우가 많고, 사업화 이후에는 내부인과 연계하여 지속적인 기술유출 루트로 활용하였다.[48]

<표 3-2> 신분별 산업스파이 사례

신분별	유치과학자	기술고문	현직직원	전직직원
82건	6건	3건	25건	48건

(4) 유출수법별 산업스파이 사례분석

유출수법별로 산업스파이 사건사례를 살펴보면 연구원 매수 및 위장 합작법인 설립에 의한 유출수법이 많은 추세인 것으로 나타났다. IMF 구조조정을 겪은 연구원들은 신분에 대한 불안감 때문에 고액연봉, 중국 등 해외근무 조건이 제시되면 거부하기가 어려운 등 금전적 유혹에 취약하다.[49] 해외업체들은 국내핵심연구원에게 접근, 합작법인 설립시 경영권을 주겠다고 유혹하거나 경영컨설팅이라는 명분으로 관련기술 절취

47) 2003년 9월, S社 연구소장 등 5명이 일본 K社에 휴대폰 제조기술을 유출하다 적발됨.
48) 2001년 2월, L社 前연구원 2명이 '디지털TV'핵심기술을 CD에 복사 유출, 사업화하면서 지속적으로 현직 연구원의 유인을 기도하다 적발됨.
49) 2003년 4월, T연구소 연구원 4명이 고액연봉과 해외취업 알선 등 유혹에 넘어가 국책연구 과제인 IMT-2000기술을 해외로 불법 유출하려다가 적발됨.

후 영업목적으로 절취기술을 재활용하는 사례가 빈발하였다.[50]

<표 3-3> 유출수법별 산업스파이 사례

유출수법	매수	공동연구	기술자문	위장합작	불법수출
82건	66건	7건	3건	5건	1건

2) 산업스파이 단속시 애로사항

(1) 단속 관련 법규의 미비

앞에서 본 바와 같이, 우리나라는 1986년부터 시작된 WTO/TRIPs 협정을 계기로 1991년 12월 부정경쟁방지법을 개정하여 영업비밀 보호제도를 도입하게 되었다. 그 후, 1998년 삼성전자 반도체 해외유출사건을 계기로 법 명칭을 '부정경쟁방지및영업비밀보호에관한법률'로 변경하고, 손해배상청구시 침해자가 얻은 이익액을 청구인의 손해액으로 추정할 수 있도록 하였으며, 영업비밀을 해외로 유출한 자를 가중 처벌토록 하였고, 전직 임직원이 제3자에게 영업비밀을 누설한 경우도 처벌하는 등 영업비밀 침해행위에 대한 형법법규를 대폭 강화하는 방향으로 법률개정을 하였다. 그러나 이 개정법은 범행주체를 기업의 전·현직 임직원으로 제한하고, 범행대상을 기술상 영업비밀로 한정하며, 미수나 예비 음모에 대한 처벌규정이 없고, 산업스파이의 형태에 불문하고 친고죄로 규정하고 있어 단속에 애로가 있어왔다. 2004년 말에 이와 같은 실무상 애로점과 산업계의 요구를 반영해, 범행주체 및 대상을 확대하고 미수·예비·음모도 처벌하며 친고죄 규정을 폐지하는 법 개정이 이루어짐으로써 법령의 미비로 인한 단속상 애로점은 상당부분 해소되었으나, 스파이 관련 기술적 진보속도와 급변하는 대내외 상황을 감안하면 제도의 개선은 지속적으로, 재빨리 이루어져야 할 것이다.

50) 2001년 10월, 미국계 설계용 프로그램회사인 C社 한국지사는 기술적 컨설팅을 명분으로 국내전자·기계회사에 접근, 기술자료를 절취한 후 자사 인터넷 망에 게재·공개함.

(2) 기술상 영업비밀성 입증 곤란

현행법상 영업비밀은 비공지성, 경제성, 비밀유지성을 갖추어야 하는데, 수사대상이 된 영업비밀은 대부분 첨단기술 분야이기에, 피의자는 유출한 자료가 업계에 공지되었거나 별거 아니라는 식으로 항변하는 경우가 많은데, 이에 대해 중립적으로 진술해 줄 참고인이 없는 경우가 대부분이다. 결국 그러한 참고인은 피의자의 회사 동료일 수밖에 없어, 적극적인 진술을 회피하는 경우가 대부분이고, 이런 태도는 공판단계에서 피의자에 대한 온정적 판결을 이끌어내는데 한몫하고 있다.

(3) 외국인 등과 공모시 유출기술 회수 및 처벌의 곤란

해외 기술유출 사범은 대개 외국인이나 해외 거주 교민 등과 공모하여 범행하는 경우인 바, 이미 해외로 기술이 유출된 경우에는 그 회수가 어려워 피해기업에 돌이킬 수 없는 손해를 입힐 우려가 있고, 해외에 거주하는 공모자에 대해 범죄인인도협약이 맺어져 있는 국가라 하더라도 검거 및 수사가 지연되거나 어렵고, 이런 협약이 없는 국가에 대하여는 아예 검거를 할 수 없어, 죄질이 무거운 해외공범은 방치되고 있는 실정이다.[51]

3) 산업스파이에 대한 경찰의 대응

여기서는 미국 연방수사국 첩보부서(FBI Intelligence)의 산업스파이 대응전략을 소개하기로 한다.[52] 이러한 전략에 대한 검토는 우리 경찰의 산업스파이 대응력 및 지능수사 능력 향상을 위해서도 필요할 것이다.

(1) 외국의 테러단체 등이 미국을 직접적으로 위협할 수 있는 대량살상무기(WMD: Weapons of Mass Destruction)의 제조 기술 혹은 장비를 취득하지 못하게 막아라. 이러한 무기가 미국에 성공적으로 사용될 경우에 초래할 파괴적 결과는 참으로 끔찍하다. 따라서 어떤 적대적 국가나 집단이 WMD를 생산 또는 사용할 능력을 갖지 못하도록 하는 것이 우리의 일차적 관심사이다. 우리는 WMD관련 기술이 미국 정부나 민간으로부터

51) 이상 남상봉, "산업스파이 수사사례 분석 및 대응방안" 참고.
52) http://www.fbi.gov/publications/strategicplan/stategicplantext.htm

외국의 테러단체 등에 공개적으로나 비밀리에 유출되는 것을 막기 위해 애쓸 것이다.

이를 위해, 우선적으로 ① 미국에서 활동하는 외국 스파이들이 관심을 갖는 WMD관련 표적이 무엇인지 파악하라. ② 다른 (국내의 또는 외국의) 정보기관들, 그리고 표적이 되고 있는 산업시설들과 전략적 파트너십을 형성하라. ③ WMD를 표적으로 하는 외국 스파이들의 야욕을 분쇄하기 위해 세련된 작전을 펼쳐라.

(2) 외국 스파이들의 국내 정보기관에의 잠입을 막아라. 국내 정보기관들은 국가의 가장 민감하고 중요한 비밀들을 보유하고 있다. 따라서 국가의 안전을 확보하기 위해서는 외국의 스파이가 이러한 정보기관들에 잠입하는 것을 막기 위해 노력해야 한다. FBI는 다른 정보기관들이 보유 정보를 보호하는 능력을 향상시킬 수 있도록 하기 위해 긴밀히 협력할 것이며, 스파이의 침투를 즉각적으로 확인하고 분쇄하기 위한 사전 조치들을 다할 것이다.

이를 위해, 우선적으로 ① 미국에서 활동하는 외국 스파이들이 관심을 갖는 국내 정보기관이 어느 것이며 또한 그 표적이 무엇인지 파악하라. ② 다른 (국내의 또는 외국의) 정보기관들과 전략적 파트너십을 형성하라. ③ 미국을 표적으로 하는 외국 스파이에 대한 대응 인력을 증가시켜라. ④ 미국에서 활동하는 외국 스파이들로부터의 위협을 이해하라. ⑤ 국내 정보기관들을 표적으로 하는 외국 스파이들의 야욕을 분쇄하기 위해 세련된 작전을 수행하라.

(3) 미국 정부와 계약 관계에 있는 법인 및 기업에 대한 외국 스파이의 침투를 막아라. 미국 정부는 많은 기관들과 정책 및 주요 현안에 관한 연구용역계약을 맺고 있기 때문에 이들 단체 및 기업들이 보호되어야 한다. 만일 이들이 적대적인 스파이에 의해 위험한 상황에 처할 경우 미국은 치유할 수 없는 해를 입을 것이다. FBI는 그러한 프로젝트에 대한 위협을 평가하고 그 위협에 대응하기 위해 다른 정보기관들과의 협력을 통해 맡은바 책임을 효과적으로 수행해야 한다.

이를 위해서 ① 외국 스파이가 관심을 갖는 법인 및 기업들을 알아야 한다. ② 위협을 제대로 알기 위해서 표적이 되고 있는 기관, 기업, 및 시설과 전략적 파트너십을 형성해야 한다. ③ 미국의 이익을 위협하고 있는 외국 스파이를 분쇄하기 위한 작전을 수행해야 한다.

(4) 국가의 중요 자산을 스파이들의 위해로부터 보호하라. 국가의 주요 자산이란 그것이 적에 의해서 유출되거나 수정되거나 조작될 경우 미국과 미국 경제의 안전성을 심각하게 해칠 수 있는 정보나 정책, 계획, 기술, 산업 등을 말한다. FBI는 특히 경제스파이, 학술연구, 민간 기업의 R&D 등의 영역에서 국가의 주요한 자산에 대한 위협을 확인하고 그 취약성을 평가함에 있어서 주요한 역할을 수행한다.

이를 위해서 ① 외국의 스파이가 관심을 갖는 주요 국가자산을 알아야 한다. ② 국가주요자산을 확인하기 위해 공공 및 민간영역과 전략적 파트너십을 형성하라. ③ 국가주요자산을 표적으로 하는 외국 스파이를 확인하라. ④ 국가 주요자산을 보호하기 위해 세련된 작전을 수행하라.

(5) 미국의 전략적 목적에 가장 중대한 위협이 되고 있는 국가에 초점을 맞춘 방첩작전을 수행하라. 유일한 초강대국으로서 미국은 지구촌의 거의 모든 국가들로부터 표적이 되고 있다. FBI는 미국의 이익에 대한 위협을 파악하는 일과, 미국의 이익에 가장 심각한 위협이 되고 있는 국가나 개인들에게 그 방첩자원을 집중시킬 것이다. 특히 FBI는 스파이, 테러리즘, 대량살상무기의 확산, 국가의 기간산업, 미국 정부의 점유취득관리, 외국에서의 첩보활동 등과 관련된 위협을 검토할 것이다.

이를 위해서 ① 미국에서 활동하는 외국 스파이들로부터의 잠재적 위협을 이해하라. ② 외국 정보기관들로부터의 위협을 분쇄하기 위해 그들의 직원, 작전, 의도 등을 파악하는 등 세련된 작전을 수행하라. ③ 미국에 있는 외국 스파이들에 의한 위협과 그들의 첩보활동에 대하여 정책입안자들에게 통보하라.

(6) 외국의 (방첩) 정보를 수집하고 생산, 보급하라. FBI는 행정명령 12333호에 의거하여 외국의 (방첩) 정보를 수집, 생산, 보급하는 권한을 갖는다. 행정명령과 국가안보법(National Security Act) 모두 “외국정보”를 외국의 정부, 조직, 사람 등에 관한 정보라고 정의하고 있다. 역사적으로 FBI의 관심은 방첩정보 수집에 있었으며, 지금도 국가의 수많은 정보수요를 충족시킬 수 있는 엄청난 정보수집능력을 보유하고 있다.

이를 위해서 ① 국내외 정보의 수집을 위해 FBI가 보유하고 있는 인력자원 네트워크를 최대한 활용하라. ② FBI의 국내외 정보수집능력을 확장하라. ③ 수집한 모든 국내외 정보가 국내 정보기관들에 공유될 수 있도록 하라.

<참고 2> 산업기밀 보호관련 법령

1. 「부정경쟁방지및영업비밀보호에관한법률」 (2004.1.20 개정)

구분	내 용
민사적 구제	금지 또는 예방의 청구 (10조 1항) 영업비밀의 보유자는 영업비밀 침해행위를 하거나, 하고자 하는 자에 대하여 그 행위에 의하여 영업상의 이익이 침해 되거나 침해될 우려가 있는 때에는 법원에 그 행위의 금지 또는 예방청구 가능
	폐기·제거 등의 청구 (10조 2항) 영업비밀 보유자는 영업비밀 침해행위 금지·예방청구시 침해행위를 조성한 물건의 폐기, 침해행위에 제공된 설비의 제거 등 필요조치 병행청구 가능
	손해배상의 청구 (11조) 고의 또는 과실에 의한 영업비밀 침해행위로, 영업비밀 보유자의 영업상 이익을 침해하여 손해를 가한 자는 그 손해를 배상할 책임이 있음
형사적 구제	누구든지 부정한 이익을 얻거나 기업에 손해를 가할 목적으로 그 기업에 유용한 영업비밀을 외국에서 사용하거나 외국에서 사용될 것임을 알고 제3자에게 누설시 7년 이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하 상당의 벌금(18조 1항) 누구든지 부정한 이익을 얻거나 기업에 손해를 가할 목적으로 그 기업에 유용한 영업비밀을 취득·사용하거나 제3자에게 누설시 5년 이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하 상당의 벌금(18조 2항) 위 조항의 미수범 처벌(18조의 2) 18조 1항의 죄를 범할 목적으로 예비 또는 음모한 자는 3년 이하의 징역 또는 2천만원 이하의 벌금(18조의 3, 1항) 18조 2항의 죄를 범할 목적으로 예비 또는 음모한 자는 2년 이하의 징역 또는 1천만원 이하의 벌금(18조의 3, 2항) 위 18조 각 항의 경우 위반행위자 뿐만 아니라 법인까지도 처벌(19조)

2. 형법 및 특허법

구 분		내 용
형법	영업비밀에 접근할 권한이 있는 내부자에 의한 비밀누설시	업무상 비밀누설죄 (317 조) 특정한 직업을 가진 사람이 그 업무처리 중 알게 된 타인의 비밀을 누설시 3년 이하의 징역이나 금고, 10년 이하의 자격정지 또는 700만원 이하의 벌금
		횡령·배임죄 (355 조) 타인의 재물을 보관하는 자가 그 재물을 횡령 하거나 반환을 거부하는 경우 또는 타인의 사무를 처리하는 자가 그 임무에 위배하는 행위로써 재산상의 이익을 취득하거나 제3자로 하여금 이를 취득하게 하여 본인에게 손해를 가하는 경우 5년 이하 징역 또는 1,500만원 이하 벌금
		업무상 횡령·배임죄(356 조) 업무상의 임무에 위배하여 횡령·배임죄를 범하는 경우 10년 이하의 징역 또는 3천만원 이하의 벌금
	비밀에 접근할 수 없는 제3자에 의한 비밀침해시	비밀 침해죄 (316 조) 봉함 기타 비밀장치한 사람의 편지,문서 또는 도화를 개봉한 자나 전자기록 등 특수매체 기록을 기술적 수단을 이용하여 그 내용을 알아낸 자는 3년 이하 징역이나 금고 또는 500만원 이하의 벌금
		절도죄(329 조) 타인의 재물을 절취한 자는 6년 이하 징역 또는 1,000만원 이하 벌금
특허법		특허권 또는 전용실시권을 침해한 자는 7년 이하 징역 또는 1억원 이하 벌금, 단 피해자의 고소가 있어야 함 (225 조) 특허청·특허심판원·특허문서 전자화기관 등 특허업무와 관련된 기관의 前·現職 직원이 직무상 지득한 비밀 누설시 2년 이하 징역 또는 300만원 이하 벌금 (229 조)

3. 기타 관련법률

구 분	내 용
통신망 이용 촉진 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 (49조, 62조)
통신비밀 보호법	전기통신·우편·대화 등을 통하여 송수신되는 영업비밀을 감청· 녹음하거나 또는 그 취득한 내용을 공개·누설하는 경우 7년 이하의 징역 (3조, 11조)
컴퓨터 프로그램 보호법	타인의 프로그램을 무단으로 복제·개작·번역·배포·발행·전송한 자는 3년 이하의 징역 또는 5천만원 이하의 벌금 (29조, 46조)

<참고 3> 산업기술보호대책[53]

1. 인원보안관리

산업스파이 사건의 80% 이상이 전·현직 임직원에 의해 발생하고 있으며, 앞으로도 정보통신(IT)·생명공학(BT) 등 첨단기술분야 핵심인력에 대한 스카우트 경쟁이 치열하게 전개될 것으로 예상된다. 따라서 핵심인력에 대한 보안관리는 다른 무엇보다도 중요하다고 할 것이다. 핵심인력 관리는 무엇보다도 직원들이 회사에 대한 애사심을 가지고 스스로 기업의 이익실현을 위해 영업비밀 등을 보호하는 능동적인 자세를 가질 수 있도록 직무발명보상제도 실시 및 각종 인센티브 부여 등 사기진작 책의 시행이 더욱 중요하다.

가. 채용시 보안관리

재직 중 지득한 회사기밀을 누설하는 경우 손해배상은 물론 민·형사상 책임을 지겠다는 내용과, 재직 중 작성·개발한 논문·특허 등 지적재산권의 소유권이 회사 소유임을 명기하여 영업비밀의 무단사용으로 인한 법적 분쟁여지를 사전에 차단하기 위해 보안서약서를 징구하여야 한다.[54]

보안업무 규정 또는 지침, 사내·외에서 발생한 보안사고·사례 등을 중점 교육하여 보안에 대한 경각심을 제고하여야 한다. 보안교육 종료 후에는 확인란에 본인서명을 받거나 수료증을 발급하면 재직 또는 퇴직 후, 회사기밀 누설로 인한 법적 분쟁시 회사기밀을 보호하기 위한 회사의 노력을 입증하는 증거로 사용할 수 있다.

경력직원을 채용할 때는 전 회사의 업종·근무부서 및 영업비밀 취급사실, 퇴직 시 경업금지 계약서 작성여부 등을 확인하여야 한다. 전 직장에서 영업비밀을 취급한 경우 서약서에 전 직장에서 지득한 영업비밀을 재직 중 사용하지 않겠다는 내용을 명기하도록 한다. 최근 핵심인력 불법 스카우트를 둘러싼 소송이 급증하고 있는데, 상기 내용을 계약서에 명기함으로써 소송에 휘말릴 경우에도 상대방 회사의 영업비밀을 침해할 의

53) 국정원 홈페이지: http://www.nis.go.kr/docs/terror/indus/protect/man/01.html.

54) 1997년 국내 모 업체에서는 기술개발을 위해 유치한 러시아 과학자가 동 업체에서 개발한 기술을 무단으로 인터넷에 게재, 판매를 시도하였으나 입사시 작성한 계약서에 개발기술에 대한 소유권을 명기하지 않아 사법 처리하지 못하고 강제출국 시키는 선에서 마무리하였다.

사가 없었음을 입증하는 증거자료로 활용 가능하다.

나. 재직중 보안관리

정기면담을 실시하여 금전적 문제·근무여건 등 애로사항을 파악, 경쟁업체로의 전직을 사전에 차단한다. 프로젝트 참여, 성과급 지급 기회 등을 이용하여 보안서약서를 징구한다. 핵심사업·기술개발 참여 직원에 대해서는 인사카드에 동 내용을 기록하여, 퇴직 시 경업금지계약서 작성할 때 참고한다.

보안교육은 자체 보안부서에서 실시하는 것이 좋으나, 직원들의 관심을 끌고 교육효과를 높이기 위해 외부강사를 초빙하는 것도 필요하다. 사내·외 보안사고 및 자체 보안 점검시 적발된 보안위규 사례를 지속적으로 수집·정리하여 보안교육시 활용할 필요가 있다.

보안교육과 함께 임직원의 보안의식을 제고하고 경각심을 일깨우는 방법으로 정기·불시 보안점검을 실시하는 것이 좋다. 이때 중점 점검사항으로는 사무실 출입문·서류함 시건 여부, 책상 위 중요서류 방치 여부, 쓰레기통에 중요서류 무단투기 여부 등을 들 수 있다. 보안점검 결과 우수자에 대해서는 포상 등을 통해 격려하고, 규정 미준수 등 위규자에 대해서는 적절한 불이익을 부과함으로써 경각심 제고를 유도해야 한다.

다. 퇴직시 보안관리

직원이 퇴직할 경우 개인 PC 패스워드 및 ID를 삭제하고, 중요자료 외부유출 방지를 위해 출입증, 디스켓, 연구노트 등 지급물품 환수 및 반출물품 검색을 하며, 영업비밀 보유자 등 핵심인력이 경업금지 기간 중 경쟁업체로 전직할 경우, 관련법규에 의해 처벌받는다는 사실을 고지하고 퇴직서약서에 동 내용을 명기한다.[55]

라. 유치과학자 보안관리

계약서상에 보안준수 의무 및 위반시 처벌조항을 명기함은 물론 연구성과물의 소유

55) 퇴직자가 보유한 영업비밀을 고려, 경업금지 업종·분야를 구체적으로 한정해야 향후 영업비밀 누설로 인한 법적 대응시 유리하다. 경업금지기간은 업종, 제품의 라이프 사이클, 특허출원 상황 등을 통계적으로 정리, 합리적으로 결정한다.

권이 회사에 있음을 명확히 규정해야 한다. 관리담당자를 임명하여 연구활동 과정에서의 특이한 언동・동향 등을 상세히 파악하고, 필요시 관계기관에 통보한다. 연구목적과 무관한 타 분야 연구실, 실험실, 자료보관실 등 중요시설의 무단출입과 사진촬영 등을 제한한다. 중요 연구자료, 노트북 등의 외부 무단반출을 금지한다. 계역만료시는 연구노트, 성과물 등 각종 연구자료를 회수하고 개인컴퓨터 패스워드 및 ID를 삭제하고, 반출희망 자료에 대해서는 보안성 검토 후 제공하거나 별도 우송한다.

마. 협력업체등 외부인보안관리

협력업체등 외부인의 보안관리를 위해서는 해당업체의 장 및 출입인원에 대한 보안서약서를 징구한다. 고정출입 인원을 최소한으로 제한하고, 출입지역도 일정 한계를 두어 엄격하게 통제한다. 연 1회 이상 협력업체를 방문하여 보안점검 및 임직원 대상 보안교육을 실시한다. 제품소개・구매상담・공장견학 등 필요시 견학코스 지정, 기술자료 및 홍보 팜플렛 등에 대한 보안성 검토 등 영업비밀 누설 방지대책을 강구한다. 계약체결시 비밀유지 의무와 함께 위반시 손해배상 책임 및 관련법규에 의한 민・형사상 처벌규정을 명확히 기재한다. 제공한 자료는 가급적 회수하거나 관리를 철저히 하도록 지속적으로 교육한다. 과기・산자부, 국세청 및 지자체 등 관계기관에 연구비 또는 연구프로젝트 획득을 위해 관련자료 제공시 표지에 적정 등급으로 표시하고 관련기관에도 “대외비”에 준하여 취급하여 줄 것을 요구한다.

바. 해외사업장근무 현지인보안관리

현지인 기술인력에 의한 첨단기술 유출에 대비하여 현지 국가의 지적재산권 보호제도를 면밀히 파악한 후 실정에 맞도록 비밀준수 의무 및 손해배상 책임을 명확히 규정한다. 지역에 따라 현지인이 보안업무를 총괄하는 해외사업장이 있으나 가급적이면 본사직원이 분임보안 책임자가 되고 현지인을 보안담당자로 임명하는 것이 좋다. 지속적인 보안점검 및 교육을 실시하되, 일반적인 사항은 현지인 분임보안 담당자가 책임 실시토록 위임한다. 현지인 분임보안 책임자에 대해 인센티브 제공 등을 통해 퇴사시 재직 중 지득한 기밀누설을 금지하는 등 보안 조치한다. 비서・기사 등 내국인과 접촉이 많은 자, 경비・청소원 등 소외분야 종사자 등 현지인 보안취약 대상자는 중점관리하

고, 현지인 중요보직자는 특이동향 발견시 기록관리를 유지하고 임직원 인수인계시 관련 동향의 통보를 철저히 한다.

2. 문서보안관리

제품의 제조비법・연구데이터・시제품・설계도 등 기업의 독자적이고 미공개된 비밀자료는 외부로 유출될 경우 경쟁업체의 견제, 사업중단 등 기업경영에 막대한 손실이 발생한다. 기업의 비밀자료에 대해 수록상태 및 보관상황, 보관책임자의 운영상황, 비밀사항의 표시유무, 누설방지 장치의 설치유무 등을 점검하여 수시 확인하는 등 체계적인 관리가 필요하다.

가. 기술자료 보안관리 대책

제품의 설계도・소스코드 등 제품제조와 관련된 핵심 기술자료는 영업비밀로 분류・관리하여 법적 보호를 받을 수 있도록 하고 암호화하여 저장 또는 입출력 내용을 자동기록하는 등 보안대책을 강구하여야 한다. 중요자료의 외부 제공 및 열람을 엄격히 제한하되 사업추진상 필요에 의해서 영업비밀 자료를 대외에 제공해야 할 경우, 반드시 보안성 여부에 대한 면밀한 검토가 필요하다. 전시회・박람회 및 제품설명회 개최 시 외부인의 사진촬영을 금지하고 행사종료 후 반드시 관련 자료를 전량 회수하여야 한다. 기술이전, 하청계약 체결 시 자료를 제공하는 경우 반드시 비밀유지 의무조항을 포함시키고 이를 위반하였을 경우의 책임소재를 명시한다.

나. 비밀관리방법

비밀생산 시에는 제한된 장소에 최소인원만 참여하여 작성하고 초안지・파지 등을 철저히 처리하는 한편 기업실정에 맞게 적정 비밀등급으로 분류하여 필요한 최소량만 생산한다. 비밀의 보관은 원칙적으로 일반문서와 분리하여 이중 시건장치가 된 견고한 별도의 캐비닛에 보관하여야 하나 기업의 규모, 비밀의 양, 업무의 특성 등을 종합적으로 고려하여 결정한다. 비밀열람 시에는 보안담당관 승인 하에 업무관련자로 제한하여 열람하도록 하고 대출시에도 비밀관리 상태를 확인할 필요가 있다. 비밀의 파기 시에는

원형이 재생되지 않도록 완전히 소멸토록 파기하고 일반문서와 분리하여 재활용업체에 매각되거나 휴지통에 방치 또는 이면지를 활용하는 경우가 없도록 파기 조치한다. 비밀의 복사 시에는 원본에 복사 일시·부수·배포처를 명시하고 복사한 비밀의 등급과 예고문을 원본과 동일하게 분류한다.

다. 중요 연구프로젝트 수행시 보안관리 요령

연구프로젝트 계획수립시 참여인원을 최소화하여 연구활동에 대한 불필요한 인원의 접근을 차단한다. 연구프로젝트 참여자에 대해 보안서약서를 징구하고, 보안관리요령을 교육하는 한편 참여자의 퇴직 및 전보시에 중요사항 누설방지를 위해 보안조치를 실시한다. 회의 개최시에는 회의자료를 비밀로 생산하여 등재·관리하고 무단 복사하지 못하도록 하여야 하며 회의종료 직후 회수한다. 연구프로젝트에 대한 시제품 제작시에는 외부 용역업체에 설계도면·실험데이터 등 제공 후 회수 조치하고 연구성과물 등 핵심 기술자료는 일반문서와 분리 보관한다.

3. 시설보안관리

시설보안관리를 위해서는 생산공장·사무실·연구실 등 시설의 위치, 특성 등을 면밀히 검토하여 적절한 보안대책을 수립한다. 시설 자체보다는 그 시설이 가지고 있는 기능을 보호하기 위해 시설의 보안상 중요도에 따라 보안대책의 강도를 조정한다.

가. 보호구역의 설정 및 등급구분

일반적으로 제한지역은 기업의 비밀 또는 재산의 보호를 위하여 울타리 또는 경비원에 의해 일반인의 감시가 요구되는 지역(사무실, 공장 등 건물내부 전 지역)이다. 제한구역은 비밀 또는 주요시설·자재에 대한 비인가자의 접근을 방지하기 위해 출입 시 안내가 요구되는 지역(중역실, 전산실, 교환실, 제조기술 부서, 조립라인, 자재창고 등)이다. 통제구역은 비인가자의 출입이 금지되는 보안상 극히 중요한 지역(전산실, 비밀보관소, 통신실, 연구실, 위험물 창고 등)이다.

나. 출입자통제

임직원의 경우, 연구실, 공장, 사무실 등 사내지역 출입시 직원임을 표시하는 명찰을 패용하거나 유니폼을 착용하여 외부인과 구별한다. 시설별 중요도에 따라 출입인원을 제한할 필요가 있을 경우 출입증에 전자칩내장, 색상구분 등을 통해 출입자격을 제한한다. 외부인의 경우, 협력업체 직원, 전산실 보수 등 목적으로 정기 출입하는 자는 신원확인에 필요한 서류 및 보안유지 서약서를 징구한다. 정기출입증 색상은 임직원과 구분되도록 하여 정문에서 교부·회수하고, 명부를 비치하여 출입시간 기록을 유지한다. 임시출입자는 대장에 인적사항, 목적, 방문대상 직원 등을 기재하고 면회실 이용을 원칙으로 하되, 회사내부 출입이 필요한 경우 임시출입증 패용 후 직원안내를 받아 출입하도록 조치한다.

다. 출입차량통제

임직원, 협력업체 직원 등 사전 인가된 차량 외에는 사업장내 출입을 엄격 제한하고, 주차구역을 지정한다. 임시출입 차량에 대해서는 임시출입증을 교부하고 필요시 차량 내부 및 적재물에 대한 보안검색을 실시하고 탑승자의 신원을 확인한다.

라. 중요시설보호

CEO실, 회의실 등 중요시설에 대해서는 정기적인 도청확인점검을 한다. 외부인 의 방문에 대비하여 견학·시찰코스를 사전 지정하되 핵심 생산라인 등 중요시설은 대상에서 제외하고 사진촬영을 통제한다. 중요시설에는 CCTV, 적외선감지기, 카드키, 지문인식 시스템 등 과학장비를 설치하여 비인가자 등의 무단출입을 통제한다. 외부투시, 도청, 방화, 파괴물질 투척 등 긴급상황 발생시 즉각적인 상황전파 및 상황지원이 가능하도록 적절한 경보시스템을 설치한다. 핵심시설에 대한 비상키(마스터키)는 원칙적으로 용역경비·청소업체 직원에게 위탁관리를 금지하되 부득이한 경우 봉함관리하고 개봉시 반드시 보안담당자에게 사유를 소명케 한다.

마. 신분증관리

신분증은 직원과 외부인을 구별할 수 있도록 구분하고, 외부인의 경우도 방문자, 시

찰·견학자 등으로 구분한다. 신분증에는 전자칩을 내장하여 중요시설 출입시간 등을 자동 체크할 수 있도록 하고, 근무시 패용을 의무화한다. 신분증 갱신은 사용기간 장기화, 분실건수 증가 등 필요시 일괄 갱신하되 분실자에 대해서는 사유서 징구 및 징계하여 재발방지를 유도한다.

4. 전산통신보안관리

전산실은 통제구역으로 설정 관리하고, 유지보수 등의 목적으로 상시 출입하는 외부직원에 대해서는 보안서약서를 징구한다. 화재·폭발 등 사고발생 등에 의한 전산자료 소실에 대비하여 정기적으로 백업하도록 하고 백업자료는 별도의 안전한 건물에 보관한다.

가. 개인컴퓨터 보안관리

개인별 컴퓨터에는 ID 및 패스워드를 설정하고 주기적으로 변경토록 하되 쉽게 유추할 수 있는 패스워드 사용은 지양한다. 개인 PC별 화면보호기 및 전용 패스워드를 사용하고 화면보호기 작동시간을 20분 등으로 적절하게 지정한다. 방화벽·침입탐지 시스템을 설치하고 사내망과 외부망을 분리하여 해킹 피해 등으로부터 보호한다. 수리 등 목적으로 업무용 PC를 외부 반출시 저장내용 삭제 등 보안조치 후 보안부서의 확인·허가를 받아 반출한다. 디스켓·CD 등은 부서별 또는 회사에서 일괄구입 후, 관리번호를 부여, 지급하고 비밀 등 중요내용은 별도 디스켓·CD에 보관하여 특별관리한다.

나. 노트북 보안관리

인가되지 않은 개인용 노트북 사용을 금하고, 초기 동작시 사용자 식별 및 인증절차를 거치도록 조치한다. 노트북의 하드 디스크 내에는 중요정보 저장을 금지하고 업무상 목적으로 저장할 경우 file별로 패스워드 등 보안조치 후 허가한다. 노트북의 외부 반출시 해당 부서장의 승인을 받도록 하고 퇴근·출장 등으로 노트북을 사용하지 않을 경우 견고한 캐비닛 등에 보관한다.

다. 사용자ID 및 패스워드 보안관리

동일 ID로 동시에 동일 서버에 접속하지 못하도록 설계하고, 패스워드는 최소 6자리 이상이 되도록 설정한다. 패스워드는 동일 문자열이 연속 사용되지 않도록 설계하고(4자리 이상), 사용자 ID와 일치하는 패스워드 사용을 금지한다. 3회 이상 접속 실패 시 잠김 기능을 적용한다. 기 사용된 패스워드는 12개월 내 재사용 금지하고, 평문 조회가 불가능하도록 암호화하여 데이터베이스에 저장한다. 패스워드 분실시 사용자 확인절차를 거쳐 해당 관리자에 의해 삭제되어야 하며, 인터넷 망 사용시 ID 및 패스워드가 타인에게 노출되지 않도록 암호화하여 보관하거나 전송한다.

라. 이메일 보안관리

외부발송 E-Mail 크기를 일정규모 이하로 제한하고, 이를 초과할 경우에는 해 부서장의 승인을 받도록 조치한다. E-Mail을 이용한 내부자료 불법유출 시 관련규정에 의한 처벌내용을 수시 교육하고, 경각심을 확산시킨다.

제4장 화폐 및 유가증권 위조

위조화폐 및 위조유가증권은 지불수단으로서의 화폐와 유가증권에 대한 국민들의 신뢰에 손상을 가한다. 위조는 일반 대중이 화폐나 유가증권에 대해서 갖는 신념이나 신뢰를 기만하여 대중의 신뢰에 치명적인 영향을 미치게 된다. 또한 위조화폐의 경우에는 국가가 갖는 화폐의 발행과 사용에 대한 독점권을 침해하는 행위이다.

위폐가 피해 기업이나 개인에게 초래하는 비용에는 직접적인 것과 간접적인 것으로 나누어 볼 수 있다. 물건이나 서비스를 제공하고 받은 위폐만큼 피해자는 수입이 줄어들어 직접적인 비용을 경험한다. 일례로 미국에서 한 비영리 단체가 해외선교사들을 후원하기 위해 운영하던 소규모 상점인 Amen Gift Shop은 위조지폐로 $3,900의 피해를 경험하고 가게 문을 닫았다. 불행히도 소규모 영세 자영업이 위조범들의 피해대상이 되고 있다. 기업은 위폐의 피해를 줄이기 위해 직원들에게 위폐 감식법과 대처법 등을 교육하고 위폐를 가려낼 수 있는 안전 장비를 구입하는 데 추가적인 비용을 지불하게 된다(Chidley, 2004). 국가의 입장에서는 위폐문제가 심각해짐에 따라서 위폐방지 기능을 강화한 새로운 디자인의 화폐와 유가증권을 만들고 새 기능을 도입할수록 비용은 더 들게 된다. 세계 각국마다 위폐문제는 나날이 심각해지고 있어서 캐나다는 2004년에 $20 지폐와 $100 지폐를 새롭게 내놓았고, 러시아도 새 루블권을 내 놓을 계획이다(New York Times, 2004). 이 외에도 위폐는 일반 대중의 신뢰를 약화시켜서 국가경제 전체에 악영향을 미치게 된다(Altig, 2002).

우리는 초정밀 위폐 등 위조외화 유통이 증가될 경우 국내 금융질서 문란은 물론 국가 안보마저 위협받을 수 있다는 점을 인식하고 항상 화폐와 유가증권을 확인해 보는 습관을 생활화하는 한편, 환전업무 종사자의 식별능력 배양과 최신 위폐감별기 보급 등 대책을 지속적으로 강구해야겠다.

1. 화폐 및 유가증권 위조의 개념과 유형

화폐의 위조란 화폐발행권자가 아닌 자가 일반인이 진짜 화폐라고 오인할 수 있을 정도로 정밀한 가짜 화폐를 제조하는 것을 말하며, 변조는 진짜 화폐를 변형(예, 액면금액의 변경 등)하여 그 가치를 변경하는 것을 말한다. 우리나라의 경우 화폐 위·변조행위는 형법(제207조) 및 특정범죄가중처벌등에관한법률(제10조)의 규정에 따라 사형, 무기 또는 5년 이상의 징역에 해당하는 처벌을 받는다.

화폐위조의 유형

- 위조동전: 진짜 동전은 압단기로 찍어 만들지만 위조 동전은 대부분 주형이나 형판을 이용하여 주조된다. 이 경우에 위조 동전에 돌기처럼 생긴 형판 표시가 남는 경우가 종종 있다. 오늘날 위조 동전은 수집가들이 찾는 희귀한 동전을 모방하여 위조한다. 화폐의 가치를 높이기 위해 진짜 동전을 변형시키기도 한다. 가장 일반적으로 많이 사용되는 방법은 동전의 주조일자나 표식을 제거하거나, 추가하거나, 변형시키는 것이다.
- 위조지폐: 위조지폐는 그 제조방식에 따라서 전통적인 오프세트 인쇄방법을 사용한 경우와 최근 컴퓨터, 스캐너 및 프린터 기술의 발전에 따라 디지털 기술로 제조된 경우, 그리고 국가를 상대로 판매되는 정밀 화폐인쇄기를 이용해 만든 수퍼노트로 구분할 수 있다.
- 수퍼노트[56]: 달러 위폐에서 관심의 대상이 되고 있는 것은 너무나 정교해 위폐 감별기로도 식별이 어려운 '수퍼노트'이다. 특히 2005년 9월 15일에 미국 재무부가 마카오 소재 중국계 방코 델타 아시아 은행을 통한 북한의 위조 달러 지폐 유통 혐의를 공식발표하면서 큰 파문이 일고 있다(중앙일보, 2005. 11. 11). 미국은 2005년 8월에 국제 밀매조직을 적발하고 모두 4,600만 달러 상당의 위조지폐와 가짜 담배, 무기 등을 압수하면서 북한과 관련된 증거를 입수한 것으로 알려져 있다.

56) 미국 재무부 비밀 검찰부의 위폐전문가인 Pagano는 $100짜리 위조지폐를 수백만 달러어치 유통시킨 위조의 달인 Art Williams의 위폐에 10점 만점에 8-9점을 부여하면서 10점 만점은 북한 정부가 1000만 달러짜리 음각인쇄기를 이용하여 만든 '수퍼노트'에 주어진 다고 하였다(Kersten, 2005).

미국 재무부는 2005년 12월 16일에 한국, 중국, 일본, 동남아 국가, 유럽연합 회원국 등 40개국 대표를 초청하여 북한의 위폐제조 의혹에 대해 비공개 브리핑을 하였다. 브리핑에서 드러난 북한 위폐 현황을 보면, 1989년부터 북한의 위조지폐가 적발되기 시작한 것으로 알려졌다. 적발된 규모가 매년 270만 달러에 이르던 것이 2005년에는 1,000만 달러를 넘어섰고, 지난 16년 동안 적발된 위폐 총액은 5,000만 달러에 이르는 것으로 전해진다[57]. 무엇보다도 북한이 제조한 위폐는 너무 정교해 진짜와 구별이 어렵다는 '수퍼노트'로 불린다. 북한산 수퍼노트는 감식펜으로 판별할 수 없고, 은행의 전문 위폐 판별기에서나 구별이 가능한 것으로 알려져 있다. 한 소식통에 의하면, 이 위폐는 진품에서 결함으로 지적돼온 부분까지 바꿨으며 이 때문에 미국 당국이 위폐로 확인할 수 있었다고 한다(중앙일보, 2006. 2. 9). 수퍼노트는 개인차원에서 만들 수 없는 것으로 국제적인 규모의 범죄조직이나 국가차원에서만 만들 수 있는 것으로 알려져 있다. 다른 나라의 화폐를 정권차원에서 위조한 것은 독일의 히틀러 이후 처음이라는 버시바우 주한 미국대사의 말이 사실이라면 이 문제는 국제적으로 매우 심각한 성질의 문제임을 알 수 있다(중앙일보, 2005. 12. 8).

미국이 제시하고 있는 북한 위폐에 대한 증거는 크게 2가지로 나누어 볼 수 있다. 첫째, 북한 외교관이 위폐를 가지고 있다가 검거된 사건들이 있다. 북한 외교관들이 외교 행랑으로 위폐를 유통시키고 이것으로 물품을 구입하다 여러 번 적발된 사실이 있다. 예컨대, 2005년 5월 3일에 일본에서 조사된 북한 화물선에서 위폐가 발견되었고, 1996년 12월에는 루마니아 주재 북한 대사관 무역참사 김철호가 위폐 5만 달러를 유통시키다가 체포된 바 있다. 이 밖에 북한이 입금한 은행 계좌에서 위폐가 섞여 나온 사실도 있는 것으로 알려져 있다. 둘째, 북한은 1975년에 스위스에서 위폐 제조용 초정밀 인쇄기를 구입한 이래, 최근에는 스위스산 색변환 잉크와 일본과 프랑스에서 만든 정밀 화폐 인쇄기를 대량 구입했다고 한다(중앙일보, 2005. 12. 22). 특수잉크와 화폐인쇄기는 모두 국가를 상대로만 판매를 하고 있다. 미국측에서는 북한산 위조지폐가 제3국의 위폐 감식기를 통과할 수 있는지를 검사하는 최고급 '위폐검색기계'도 북한이 갖고 있다고 주장한다. 북한 위폐에 대

57) 미국의 정보당국은 북한이 제조한 것으로 추정되는 5000만 - 6000만 달러의 위조지폐를 확인한 것으로 알려졌다(중앙일보, 2006. 2. 9).

한 이러한 증거는 구체적인 물증이라기보다는 정황증거의 수준에 머물고 있으나 위폐와 같은 초국가적 범죄에 대해서는 국제사회가 공동으로 대처해야 하는 사항인 만큼 법집행기관들은 북한 위폐문제에 대해 자료를 수집하고 대책을 수립해야 할 단계이다.

국내에서 북한의 위폐문제에 대해 다룬 경우는 국가정보원이 국회에서 1999년까지 밝힌 바가 있다. 1998년 11월에 국정원은 국회 정보위에서 북한이 해외에 유통시키려다가 발각된 위폐가 1994년 이후로 13회에 달하며 총액은 460만 달러 이상이라고 밝혔다. 국정원은 1999년 10월 국회 정보위에서 북한이 최신 위폐 감별기로 식별이 어려운 수퍼노트를 제조했고, 외교관과 고위간부를 통해 해외에 유통시켰다고 밝힌 바 있다. 국정원은 정부의 대북화해 노력을 감안하여 북한 위폐에 대해 정보를 공개하지 않고 있으나 북한 위조 달러화가 국내에도 유입된 것으로 알려져 있다. 외환위기를 겪던 1997년 12월부터 1998년 8월 사이에 국내에서 발견된 22만 달러의 위조달러 가운데 $37,000 정도가 북한산으로 추정된다(중앙일보. 2005. 11. 11).

- 액면가를 변조한 지폐: 진짜 지폐를 변조하여 액면가를 높이는 방법이다. 많이 사용되는 방법으로는 액면가가 높은 지폐에서 숫자를 오려와 낮은 액면 금액권에 붙여 사용하는 경우이다. 지폐를 변조한 경우도 위폐에 해당되며 위폐와 동일한 처벌을 받게 된다.

<그림 4-1> 액면가를 변조한 달러화

<표 4-1> 위조미화의 종류와 특징

종 류	특 징
슈퍼노트	진폐와 같은 용지와 잉크, 요판인쇄로 제작, 정밀감식이나 최신 위폐 감별기로만 식별가능(특정 국가가 제작)
중급위폐	위조방지요소가 미흡하고 옵셋인쇄로 제작, 육안식별가능 (위폐조직이 제작)
저급위폐	위조방지요소가 없고 칼라복사기, 컴퓨터스캐너로 제작, 육안식별가능 (일반인 제작)
변조미화	1, 5불권 네모서리 액면숫자를 오리거나 탈색시켜 100, 50불권으로 변조
모조지폐	통용되지 않는 고액권(100, 10만불 등)을 모조한 지폐(장남감 등으로 사용)

출처: 국가정보원

유가증권(securities; Wertpapier)이란 증권상에 표시된 재산상의 권리의 행사와 처분에 그 증권의 점유를 필요로 하는 것, 즉 사법상 재산권을 표시한 증권을 말한다. 유가증권에는 법률상의 유가증권과 사실상의 유가증권이 포함된다. 법률상의 유가증권이란 어음, 수표, 화물상환권, 선하증권, 창고증권과 같이 법률상 일정한 형식을 필요로 하는 증권을 말하며, 사실상의 유가증권은 승차권, 상품권과 같이 법률상의 형식이 규정되어 있지 않는 유가증권을 말한다(이재상, 2000).

흔히 유가증권에 관한 죄란 '행사할 목적으로 유가증권을 위조·변조 또는 허위작성하거나 위조·변조·허위작성한 유가증권을 행사·수입 또는 수출함으로써 성립되는 범죄'를 말한다. 우리나라 형법에는 행사할 목적으로 공채증서[58] 기타 유가증권을 위조 또는 변조한 자(제214조1항)나 유가증권의 권리의무에 관한 기재를 위조 또는 변조한 자(제214조2항)는 10년 이하의 징역에 처하도록 하고 있다. 또한 동법은 자격모용에 의한 유가증권의 작성(215조), 허위유가증권의 작성등(제216조), 위조유가증권등의 행사등(제217조)에 대해서도 처벌규정을 두고 있다.

유가증권 위조란 작성권한 없는 자가 타인 명의의 유가증권을 작성하는 것을 말한다. 위조는 외형상 일반인에게 진정하게 작성된 유가증권이라고 오신케 할 정도로 정밀하

58) 공채증서란 국가 또는 지방자치단체에서 발행하는 유가증권(국채·공채 등)을 말한다.

게 작성될 것을 요한다. 위조의 방법(또는 유형)에는 제한이 없다. 약속어음의 액면란에 보충권의 범위를 초월한 금액을 기입하거나 폐지로 된 약속어음을 조합한 경우는 물론 타인이 위조한 백지의 약속어음을 완성하는 경우도 위조에 해당한다. 간접정범의 방법에 의한 위조도 가능하다. 따라서 기망수단에 의하여 타인으로 하여금 약속어음 용지에 발행인으로 서명·날인케 한 후 마음대로 어음요건을 기재하여 어음을 발행한 때에도 위조에 해당한다.

유가증권 변조란 진정하게 성립된 유가증권의 내용에 권한 없는 자가 그 유가증권의 동일성을 해하지 않는 범위에서 변경을 가하는 것을 말한다. 예컨대 어음의 발행일자·액면 또는 지급인의 주소를 변경하는 것이 여기에 해당한다(이재상, 2000).

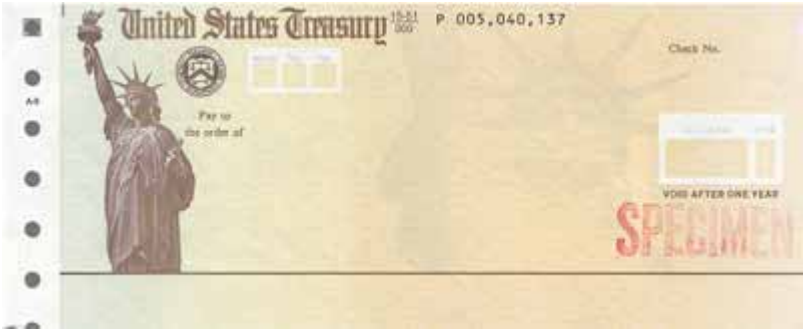
미국에서 많이 발견되는 유가증권변조에는 정부수표의 액수를 변조하는 경우와 수신인을 변조하는 경우를 포함한다.

액수를 변조한 수표: 정부수표의 위조는 금액을 변조하는 경우가 많다. 이러한 변조를 막기 위해 잉크 제거제나 용매에 화학적으로 반응하는 용지를 사용한다. 또한 위조방지 장치로 “U.S. Treasury"라는 요판잠상을 사용하여 사무용 복사기로 복사가 되지 않도록 하였다. 수표는 건식인쇄과정을 거치는데 이때 사용하는 잉크도 표백에 반응하도록 특별히 제작된다. 물로 지운다거나 알코올이나 표백제를 사용하면 용해하여 눈에 띄게 만들어져 있다.

<그림 4-2> 수표의 숫자를 변조한 경우

수신인을 변조한 수표: 정부수표의 수신인을 변조하여 타인에게 발행된 수표를 가로채는 방법이다.

<그림 4-3> 위조방지 장치가 추가된 미국 정부수표



2. 화폐 및 유가증권 위조범죄의 실태와 최근의 사례

1) 우리나라

위폐문제로부터 우리나라도 자유로울 수 없다. 한국은행의 발표에 따르면, 국내에서 발견된 위폐의 매수와 액수 모두 증가하고 있다. 국내에서 발견되는 위폐문제는 국내화폐의 위조와 외국화폐의 위조로 나누어 볼 수 있다. 먼저, 한국은행이 발표한 '2005년 중 위조지폐 발견현황'에 비추어 국내화폐의 위조실태를 보면, 2005년도에 신고, 접수된 위조지폐는 총 12,889장으로 2004년도의 4,353장에 비해 3배 가까이 증가했다. 이 중에서도 5000원권 위조지폐가 급증하여 2004년도에 987장이던 위폐가 2005년도에 7,337장으로 7배 이상 증가한 것으로 나타났다. 5000원권 위폐 중에서도 1983년에 나와 위조방지용 은선이 들어 있지 않은 5000원권이 79%를 차지하였다. 그러나 위폐의 증가가 5000원권에만 국한된 것이 아니다. 10000원권 위폐는 2004년에 3,237장에서 2005년도에 5,404장으로 67% 증가했고, 1000원권 위폐도 2004년의 129장에서 2005년에 148장으로 15% 증가하였다(chosun.com, 2006. 2. 1).

국내에서 발견되는 외화 위조지폐도 그 매수와 액수가 크게 증가하고 있다. 외화 위폐의 매수를 보면, 2001년도에 189장이던 것이 2002년에 286장, 2003년에 544장, 2004년에 667장, 2005년 상반기에만 1,623장에 달하고 있다. 외화 위폐 중에서도 통화가치가

높고 기축(基軸)통화인 달러화만을 골라 국내에서 발견된 액수를 보면, 2005년 11월말까지 $83,790로 집계되어 2004년도 한 해 동안 발견된 $26,150의 3배가 넘는 액수를 기록하였다. 발견매수로 보더라도 2005년 11월까지 842장의 달러 위폐가 발견되어 2004년도의 420장에 비해 2배가 넘는 규모이다. 달러화 위폐를 종류별로 나누어 보면, 소위 '슈퍼노트'로 불리는 초정밀 $100 위폐가 835장으로 압도적으로 많았으며, $50 위폐 5장과 $10 위폐 2장이 2005년 11월까지 국내에서 발견되어 슈퍼노트가 국내에서도 큰 위협이 되고 있음을 알 수 있다(한국아이닷컴, 2005. 12. 25).

국내에서 발견되는 외국의 위조지폐와 수표는 모조미화, 염색미화, 변조미화, 위조수표로 나눌 수 있다. 모조미화의 경우에는 위조범이 10만 달러권이나 100만 달러권 등 통용되지 않는 고액권을 모조하여 미국정부의 위조 보증서를 보여주며 액면가의 30-40%로 판매하는 사기 행각을 벌인다. 염색미화는 사기범이 검은 색종이나 영문글자가 새겨진 염색종이 뭉치를 보여주며 이것을 화학약품으로 처리하면 $100짜리 진폐로 원상회복할 수 있다고 속여 약품구입비 명목으로 금품을 사취한다. 최근에는 백색미화를 이용하는 경우도 보고되고 있다. 변조미화의 예로는 1928년에 발행된 $1와 $2짜리 지폐가 희소하여 고가로 거래된다는 점을 악용하여 1995년에 발행된 $1짜리 지폐를 1928년에 발행된 것으로 변조하고 도장을 인쇄하여 사기를 치는 경우이다. 이 경우는 진폐를 변조하였기 때문에 위폐감별기에 적발이 되지 않는다. 위조수표는 외국의 수표를 국내에서 확인하기 어렵다는 점을 이용하여 사기를 친다. 국내에서는 주로 미국이나 일본의 은행수표와 여행자 수표 등이 사기에 이용되고 있다.

국제 사기조직들은 우리나라의 외환거래 자유화조치를 이용하여 위조 미국채권으로 국내에서 사기를 자행하고 있다. 특히 사기에 사용되는 미국채권은 500만 달러와 1000만 달러짜리로 중국, 대만, 싱가포르, 러시아 등지에서 유통되다 국내에 반입되고 있다. 위조단은 1930년대와 40년대에 미국 CIA가 장개석 총통에게 군자금을 지원하기 위해 미국채권을 발행하였으나 중국 국민당 정부가 대만으로 쫓겨나면서 중국본토 내 사당 등에 숨겨두었던 채권이 최근에 발견되었다며 액면가의 절반 값으로 판매하겠다고 하여 피해자들을 속이는 것으로 알려졌다. 위조단은 국내에서 위조 미국채권의 진위여부를 식별하기 어렵고 미국측에 감정을 의뢰하더라도 시간이 많이 걸린다는 점을 이용하고 있다(국가정보원, 2003).

2) 미 국

미국의 위조 현황

기축통화인 미국 달러는 전세계적으로 7,000억 달러가 유통되고 있다. 미 재무부 비밀 검찰부에 따르면, 이 가운데 434만 달러의 위폐가 미국 내에서 유통된 것으로 추정된다. 2004년에 미국 국내에서 만들어진 위폐는 537만 달러로 추산되는데 이 가운데 법집행기관에 의해 압수된 금액은 103만 달러에 이르고 나머지 434만 달러는 유통되고 있다(Locy, 2005). 미국에서 위폐는 지난 100여년 이상 낮은 수준으로 유지되고 있다. 예를 들면, $10짜리 지폐 만장 가운데 1장 정도가 위조지폐인 것으로 추정되고 있다. 미국 정부는 이를 위해 화폐에 위조방지 장치를 도입하고 있고, 적극적으로 법을 집행하고 있으며, 대중을 상대로 위폐방지를 위한 교육을 실시해오고 있다.

디지털 복사기술의 발달에 힘입어 현재 발견되는 $5, $10, $20짜리 위폐의 약 97%가 컴퓨터 및 칼라 복사기로 만들어진 것이다. $50짜리 지폐의 경우에는 약 80%가 가정에서 컴퓨터를 이용해 만들어 진다. 가정용 컴퓨터를 이용한 위폐제조가 급증하고 있다. 1995년에 미국에서 발견된 모든 종류의 위폐가운데 디지털로 만들어진 위폐가 1% 미만이었던 것이 2004년에는 54%까지 증가하였다(www.moneyfactory.gov/newmoney). 빠르게 발전하는 컴퓨터 및 디지털 인쇄기술의 발달을 이용하여 개인들이 보다 진폐에 가까운 위조지폐를 쉽게 만들면서 미국 정부는 달러 지폐의 도안을 새롭게 바꾸고 있다(Locy, 2005).

달러의 새 도안과 위조방지 장치

미국은 1996년 3월 25일에 $100 지폐에 위조방지 장치를 보강하여 새로 디자인했다. 그 이후로 $50 짜리 지폐는 2004년 9월 28일에 새로이 발행하였으며, $20 지폐는 2003년 10월 9일에 새롭게 선보였다. 새 $10짜리 지폐는 2006년 3월 2일부터 유통될 것으로 알려져 있다. 새로운 $100짜리 지폐는 새 $10지폐가 발행된 이후에 발행될 예정이다. 비교적 소액지폐인 $1, $2, $5짜리 지폐의 경우에는 조만간 새로운 도안으로 바뀔 계획이 없다. 미국정부는 위조범들보다 앞서기 위해서 매 7년에서 10년마다 지폐의 도안을 새롭게 할 계획이다.

새 지폐에 사용되는 위조방지 장치에는 미세인쇄, 명기된 안전사, 숨은 그림(은화),

요판잠상, 색변환 잉크 등이 포함된다. 새 $100짜리 지폐에 사용된 안전장치를 살펴보면 아래와 같다(World Almanac & Book of Facts, 2005).

1 .미세인쇄(microprinting): 초상화 주변에 “미합중국(THE UNITED STATES OF AMERICA)”이 반복적으로 미세 인쇄되어 있다. 육안으로 보면 잘 보이지 않고 확대하면 볼 수 있다. 사무 복사기나 프린터로는 이 미세글자가 정확히 출력되지 못한다.

2. 명기된 안전사/은선(inscribed security thread): 자외선에 노출되면 붉은 빛을 내는 안전사로 투명한 폴리에스테르 실이 화폐종이에 섞여 있다. 이 실 위에는 액면금액이 인쇄되어 있다. 예컨대 $100지폐의 안전사에는 “USA 100”이 반복적으로 인쇄되어 있다.

<그림 4-4> 미세인쇄(좌)와 안전사(우)

3. 숨은 그림(은화: watermark): 1996년부터 모든 액면금액의 지폐에 비치는 무늬나 그림을 담고 있다.

4. 요판잠상: 화폐의 금액을 나타내는 숫자나 글자를 요철방식으로 삽입하여 눈으로는 잘 보이지 않지만 감각으로 느낄 수 있어서 오프세트 인쇄와 같은 평판인쇄로는 모방하기 어렵다.

5. 색변환/시변색 잉크(color shifting ink): 보는 각도에 따라서 녹색에서 검은색으로

색이 변하는 잉크가 사용되고 있다.

새롭게 소개되는 위폐방지 기술

미국의 연방준비위원회(Federal Reserve Board)는 위조억제시스템(Counterfeit Deterrence System)을 가동하고 있다. 이것은 화폐를 복사하거나 인쇄하려는 사람에게 짖어대는 감시견과 같은 역할을 한다. Adobe Photoshop제조사 같이 세계적인 규모의 컴퓨터 복사기나 소프트웨어 회사들은 화폐의 스캔이나 인쇄를 막기 위해 이 시스템을 사용하고 있다. 누군가 화폐를 스캐너나 복사기에 넣고 복사를 시도했을 때 기계가 $20과 $50짜리 지폐에 들어 있는 칼라코드를 탐지하게 되면 작동이 중단되고 경고등이 켜지는 시스템이다.

영국의 Cowburn과 그의 동료들은 2005년 7월 28일자 Nature지에 새로운 인증방법을 소개하였다. 신용카드나 종이를 현미경으로 보게 되면 융기된 곳이 있고 패인 곳 등 불규칙적인 요철을 볼 수 있다. 영국의 과학자들은 이 불규칙적 요철을 독특한 신원감정 코드로 만드는 방법을 개발하였고, 런던의 한 회사는 벌써 이 방법을 이용하여 레이저에 기반한 코딩 시스템을 만들었다. 레이저 광선을 종이나 플라스틱의 표면에 비추어 빛의 산란정도를 측정하여 0과 1을 부여함으로써 물질의 표면을 확인할 수 있는 2진법 코드를 만든다. 연구자들은 종이가 구겨지거나 물에 젖거나 표면이 문질러져도 코드를 읽을 수 있다고 밝혔다. 이 코드를 활용하면 위폐를 막을 수 있는 혁신적인 방법이 될 수 있다(Science News, 2005).

미국의 위조지폐 역사

위조지폐는 미국 역사상 가장 오래된 범죄 가운데 하나이다. 미국 역사상 초기에는 위폐범을 국사범으로 다루어 사형에 처했었다. 미국에서 은행마다 독자적으로 화폐를 발행했던 19세기에 위폐는 매우 심각한 문제였다. 남북전쟁 당시에 통용되던 모든 화폐의 1/3정도가 위조지폐였던 것으로 추정된다. 당시에는 대략 1,600여개의 주 은행들이 독자적인 지폐를 디자인하고 인쇄하였다. 지폐마다 디자인이 달라서 7,000여 종의 화폐가 유통되었고 그 결과로 4,000여 종에 달하는 위폐를 구분해 내기 어려웠다.

1863년에 국가에서 화폐를 발행하면서 위폐문제를 해결할 수 있을 것으로 예상했으

나 단기간에 위폐문제가 다시 심각해져서 미국 정부는 1865년 7월 5일에 위조화폐적발을 담당하는 재무부 비밀검찰부(United States Secret Service)를 설립하였다. 비밀검찰부가 만들어진 이후로 위폐문제가 상당히 감소하였지만 이 범죄는 지속되어 국가경제와 시민들에게 잠재적인 위험을 제기하였다. 위폐제조에 사용된 방법은 시간이 흐르면서 진화하여 전통적인 오프세트 인쇄방법으로부터 칼라 복사기, 최근에는 스캐너, 컴퓨터, 잉크젯 인쇄기를 사용하는 방법으로 변모해 왔다. 오늘날 위조지폐범들은 기초적인 컴퓨터 지식과 훈련만으로 컴퓨터를 이용하여 위폐를 만들 수 있다. 미국의 워싱턴주 시에틀에서는 초등학교 6학년 학생이 $1짜리 위조지폐를 만들어 카페테리아에서 사용하다 체포된 바 있다(New York Times, 2005. 4. 9).

위폐가 늘어나는 데는 몇 가지 이유가 있다. 위폐를 제조할 수 있는 도구를 구하기 쉬워졌고, 이들 기계의 성능이 지속적으로 향상되고 있어서 많은 사람들이 필요한 기술을 가질 수 있다. 사무 복사기와 프린터 기술의 발달로 기술 없이도 쉽게 고해상도의 칼라 복제를 할 수 있게 되었다.

미국의 비밀검찰부는 모든 위폐사건에 대해 무관용정책을 취하고 있다. 모든 위폐사건은 그 규모와 상관없이 구금이나 벌금의 무거운 처벌을 받게 된다. 인접국인 캐나다의 경우에 위폐범에 대해 주어지는 처벌이 미국보다 상대적으로 가벼워 억제효과에 문제가 있는 것으로 지적되고 있다.

3) 캐나다

캐나다의 경우 유통되고 있는 캐나다 달러는 대략 400억 달러에 이르는 것으로 추정되고 있다. Bank of Canada에 따르면, 2003년에 1,270만 달러어치의 위조지폐가 유통되었고, 이것은 2002년도의 추정치인 490만 달러보다 2배 이상 증가한 것이다. 대부분의 위조지폐는 $10과 $20짜리인 것으로 알려졌다. 캐나다에서 위조지폐 사건은 전체 형사범죄의 5%정도를 차지하여 6번째로 빈번하게 발생하는 범죄유형이 되고 있다(McClearn, 2004). 캐나다에서는 최근에 위폐사건으로 전국적인 홍역을 치른바 있다. 2000년에서 2001년 사이에 Ontario주 남서부지역인 Windsor에서 $100짜리 위조지폐가 대량으로 유통되어 전국적으로 은행, 경찰, 상인들을 당황하게 만든 바 있다. 2001년에 일부 상인들은 위폐의 두려움으로 $100짜리 지폐를 받지 않기도 했었다. 4명의 위조범들이 만든 위폐(일명, Windsor 지폐)는 너무 정교하여 550만 달러에 이르는 위폐가 유

통되었다. 범인들은 체포되어 교도소에 보내졌지만 이들이 만든 위폐는 여전히 유통되고 있어 주의가 요구된다. 이 사건으로 인해 캐나다는 2004년 3월 중반에 새 $100짜리 지폐를 발행해야 했다.

4) 유럽연합

유럽연합이 새 유로화를 2002년 1월에 공식 출범시키면서 유럽에서 위폐문제가 잠시 근절되는 듯 했다. 2001년에 12개 유로지역 국가에서 모두 65만장의 위폐가 발견되던 것이 새 유로화의 등장으로 167,000건으로 급감하였던 것이다. 이것은 새 유로화에 도입된 위폐방지장치인 홀로그램과 색변환 잉크 덕분에 이전보다 위조가 어려워졌기 때문이다. 그러나 위조범들이 새 기술을 터득하기 시작한 것으로 보인다. 유럽중앙은행에 따르면, 2003년 중반까지 발견된 위폐만 23만 건을 넘은 것으로 나타났다. 위조범들이 통화가치가 높아진 유로화를 위조의 대상으로 삼기 시작했고, 위조방지 장치에 대한 대응책을 마련하면서 유로화 위조가 급격히 증가하고 있는 것으로 전문가들은 판단하고 있다. 이 경우에 유로화가 도입되기 이전에 유럽 각 국가들에서 발생한 위조건수의 총합보다도 더 많은 위조가 생겨날 것으로 예상된다.

유로화의 도입이 갖는 특별한 위험성

새로운 화폐가 도입되거나 기존의 화폐 도안이 변경되면 일반 대중들이 새 지폐에 대해서 친밀하지 않기 때문에 위조화폐의 유통이 성공할 확률이 높아진다. 이런 맥락에서 새로운 도안의 화폐로 교체할 때는 미리 새 도안에 대해 일반대중을 상대로 알릴 필요가 있다. 특히 새 화폐에 사용된 위조방지 장치에 대해 자세히 홍보하여 일반인들이 이 장치를 사용하도록 유도하는 것이 필요하다.

단일 유로화의 도입으로 유통되는 지역이 넓어짐에 따라 유럽연합의 회원국뿐만 아니라 비회원국에서도 사용되는 경우가 증가하여 위조화폐를 발견해 내거나 유죄판결을 내리기가 전보다 어려워진다.

유럽연합 회원국가들 사이에 위조에 대한 법 구조와 조항들이 동일하지 않아 위조를 조장할 가능성이 존재한다. 즉 위조에 대해 엄한 처벌을 하지 않는 국가나 위조에 대한 법집행이 소극적인 국가에서는 위조가 활발히 일어날 수 있고, 그 영향은 유럽연합 전

체와 비회원 국가에까지 미칠 수 있다.

마지막으로, 화폐위조는 새로운 형태의 테러로 사용될 수 있다. 이 경우에 대상이 되는 국가의 경제피해는 전통적인 형태의 테러보다 그 해악이 더 클 것으로 예상된다.

3. 외국의 화폐 및 유가증권위조 범죄에 대한 입법

1) 미 국

미국화폐의 위조지폐를 제조하거나 진폐를 변조하여 액면가를 높이는 행위는 United States Code 제18장 471항 위반으로 벌금이나 최고 15년형에 처하거나 두 가지 처벌을 다 받을 수 있다. 또한 사기를 칠 의도로 미국 위폐를 소지한 행위는 United States Code 제18장 472항을 위반한 경우로 벌금이나 최고 15년형에 처하거나 두 가지 처벌을 모두 받을 수 있다. 미국 동전가운데 액면가 5센트 이상의 위조 동전을 제조하는 사람은 다른 위폐범과 동일한 처벌을 받는다. 진짜 동전의 화폐가치를 높이기 위해 변조한 경우는 United States Code 제 18장 331항을 위반하게 되어 벌금이나 최고 5년형 혹은 두 가지 처벌을 모두 받을 수 있다.

미국 정부의 수표, 채권 등을 위조, 변조하는 행위는 United States Code 제18장 510항을 위반한 것으로 벌금이나 최고 10년형 혹은 두 가지 처벌을 모두 받을 수 있다.

미국이나 외국의 지폐, 수표, 채권, 우표 수입증지, 증권 등을 복사하는 행위는 (지정된 방식을 따르지 않을 경우[59]) United States Code 제18장 474항을 위반한 것으로 벌금이나 최고 15년형 혹은 두 가지 처벌을 모두 받을 수 있다.

2) 독 일

독일의 경우에 위조화폐는 형법 8장(Geld-und Wertzeichenfälschung)에 따라서 처벌된다. StGB 제146조에는 위조화폐를 유통시키거나 사용할 의도를 가지고 위조, 변조,

59) 미국과 외국의 우표를 부정한 목적 없이 복사하는 것은 다음의 조건을 충족시키는 범위에서 허락된다. 흑백으로 복사하는 경우에는 어떠한 크기이든 가능하다. 칼라로 복사하는 경우에는 실제 크기의 3/4미만이거나 1.5배 이상의 크기여야 한다. 소인이 찍힌 우표는 어떠한 크기도 복사가 가능하다. 미국이나 외국의 수입증지의 경우에는 흑백복사만 허용된다.

구입하는 행위를 처벌할 수 있다. 또한 StGB 제149조에서는 위조화폐의 예비적인 행위들로 위조에 필요한 도판, 프레임, 숨은 그림(watermarks) 등을 제조, 판매, 보유를 처벌할 수 있다고 규정한다.

3) 국제법

위조화폐 문제의 독특한 특징이라면 이 범죄가 해외에서 자행되었을 경우를 대비하여 영토 내에서만 형법을 적용할 수 없다는 점이다. 국내외적으로 적용되는 위조화폐에 대한 처벌은 위조화폐의 제조, 수입, 수출, 수송, 판매, 사용을 다 포함한다. 위조화폐를 제재한다는 것은 모든 거래의 기초가 되는 화폐교환의 안전과 신속성의 일반이익을 보호하는 행위이다. 위조화폐로 인해 침해를 받는 이익의 중대성으로 인하여 무거운 처벌이 정당화된다.

1925년에 프랑스 루블화가 헝가리에서 대량으로 위조되면서 프랑스는 큰 피해를 당했다. 이 사건에 대한 수사의 결과로 위조범들이 네덜란드에서 체포되어 헝가리에서 기소되었으나 이들은 결국 관대한 처벌만을 받은 바 있다. 이 사건의 규모가 전례가 없을 정도로 켰고, 헝가리 당국의 비합리적인 처리, 피해국의 정치적인 무게로 인하여 국제적인 수준에서 위조문제를 다루어야 할 필요성이 대두되었다. 사실 한 국가 안에서만 위조화폐 문제를 다룬다는 것은 불충분하다. 이런 이유에서 프랑스의 발의로 많은 국가들이 1929년에 제네바에서 통화위조 억제를 위한 국제협약에 참가하였다. 이 협약에서는 화폐위조에 대항하여 초국가적으로 이행할 규정을 입안하였다.

국제법상 통화위조는 국제사회의 공통이익을 침해하는 범죄로 규정되어 있다. 국제법은 해적, 인신 및 마약의 부정거래 등과 함께 화폐위조를 범죄로 규정하고, 그 구성요건과 형량 등은 각 국가에 위임한다. 통화위조를 다루는 국제법으로는 1929년 4월 20일에 제네바에서 채택된 '통화위조의 방지에 관한 협약'이 있다. 이 협약의 제3조에서는 통화의 위조 및 변조, 위조 또는 변조된 통화의 사용, 취득, 타국으로의 반입 행위뿐만 아니라 이와 같은 행위의 미수 및 공범을 범죄로 규정하여 중죄로 처벌해야 한다고 규정하고 있다. 제5조에 의하면, 이상의 통화위조 범죄의 양형에 있어서 내외국 통화를 구별해서는 안 되며, 처벌을 상호주의적 조건 아래 두어서도 안 된다고 규정한다. 국제법은 통화위조 범죄자에게 인도 아니면 소추를 하도록 요구하는 원칙을 관철하여 자국에서 처벌하지 않으면 반드시 인도해야 한다고 밝히고 있다. 이러한 원칙은 제네바 협

약이 채택된 이후 80여년이 흐르면서 관습법으로 굳어져 가고 있다. 더욱이 국제관계에서는 정황증거만으로 족하며 '확고한 증거'가 필요하지 않은 것으로 해석되고 있다. 영역주권상 제3국이 타국 영역 안에 들어갈 수 없기 때문에 국제관계에서는 정황증거로 족하다는 것이다(중앙일보, 2006. 1. 3).

이 협약이 체결된 지 70여년 이상이 지난 오늘날 단일 유로화가 현실화되면서 국제적인 차원에서 달러화에만 집중되던 위조범들의 관심이 유로화로 확산됨에 따라서 유로화의 위조 가능성이 커졌다. 그리하여 새 유로화의 도입에 따른 새로운 화폐보호의 필요성에 입각하여 2000년 5월 29일에는 가장 근본적인 문제에 대해 Council Framework Decision이 채택되었다.

4. 위폐 및 유가증권 범죄에 대한 외국의 대응체계와 정보관리

1) 미 국

1986년에 설립된 미국 재무부의 비밀검찰부는 미국 통화의 위조 수사를 처음부터 위임 받았다. 동 部의 위조부서는 United States Code 제18장 3056항으로부터 위폐조사 권한을 부여 받고 있다. 비밀검찰부는 주와 지역의 법집행 기관, 외국의 법집행 기관들과 긴밀히 협조하고 있으며, 위조범들보다 한 발 앞서가기 위해 최신의 복사기술을 끊임없이 조사하고 있다.

미국정부는 위폐에 대해 매우 적극적으로 법집행을 하고 있다. 2004년도의 경우에 사법당국은 달러 위폐가 유통되기 전에 그 절반정도인 4,400만 달러를 압류하였다. 같은 기간 중에 전세계적으로 유통되던 대략 4,470만 달러를 세계각지에서 찾아낸 바 있다. 비밀검찰부는 2004년에 미국 내에서 위폐와 관련하여 모두 2,879명을 체포하였다. 위폐로 기소된 이들에 대한 유죄판결율은 99.3%로 매우 높다. 미국 정부는 외국에서 만들어진 위조 달러화에 대해 특별히 적극적인 대응을 하고 있어서 최근 미국 내에서 유통되다 발견된 위폐가운데 외국에서 만들어진 위폐의 비율이 계속 낮아지는 추세이다. 2002년도에 미국에서 발견된 위폐가운데 50%정도가 외국에서 만들어진 것이었던 것에 비하여 2003년도에는 42%, 2004년도에는 36%로 매년 그 비율이 낮아지고 있다.

비밀검찰부는 2004년에 위폐와 관련하여 개인 컴퓨터와 같은 디지털 장비 453개를 압류하였다. 디지털 위조보다 고전적인 형태인 오프세트 인쇄는 해외에서 더 많이 사용되고, 미국 내에서는 디지털 위조가 많이 사용되고 있다.

2) 유 럽

단일 유로화를 위조로부터 보호하기 위한 노력은 최근에 와서야 관심의 대상이 되고 있다. 이에 대한 최초의 규정은 Council Regulation 974/1998로 유럽연합에 참여하는 국가들로 하여금 유로화 지폐와 동전의 위조에 대해서 적절한 제재를 담보하도록 요구하고 있다. 이 일반적인 규정의 토대 위에서 유익한 논의를 한 결과 Framework Decision이 2000년에 채택되어 유로화의 위조에 대한 형사처벌과 제재를 강화시켰고, Reg. 1338/2001에서 유로화의 위조를 방지하기 위해 필요한 조치들이 마련되었다.

5. 한국 상황에의 시사점

오늘날의 위조범들이 컴퓨터와 프린터 등으로 손쉽게 잘 무장하기는 하였으나 미세한 부분에 신경을 쓰지 않아 질 낮은 위폐를 만들어 내곤 한다. 이들은 색변환 잉크, 숨은 그림, 요판잠상, 안전사 등에는 관심이 없다. 그저 $20 지폐와 비슷해 보이는 위폐를 만들어서 영세가게의 점원을 속일 수 있을 정도면 족하다. 따라서 영세사업자등 일반인을 상대로 위폐판별법을 교육하여 일상적인 소규모 거래에서 위폐여부를 확인하게 되면 위폐문제를 상당히 줄일 수 있을 것으로 기대된다.

지폐에 안전장치를 마련하는 것 못지않게 일반 대중에게 지폐에 설치된 안전장치를 알리는 것이 중요하다. 일반인들에게 위폐문제를 인식시키기 위해 미국 정부는 대중 교육프로그램을 시행해 오고 있다. 예컨대, 새 $10짜리 지폐가 나올 예정인 상황에서 미국인들이 새 지폐에서 사용된 안전장치를 이해하고 사용하도록 교육시키고 있다. 특별히 $10짜리 지폐를 사용하고 다루는 사람들, 특별히 도소매업에서 현찰을 다루는 사람들을 대상으로 찾아 나서거나 대중매체를 이용하여 교육하고 있다.

<그림 4-5> 위폐 구별법을 알리고 교육하는 미국의 사이트

위조된 화폐나 유가증권을 수사하게 되는 법집행 실무자들은 아래의 감정방법과 수사절차를 참고할 필요가 있다.

유가증권의 위·변조 감정방법

현미경 검사: 유가증권을 확대하여 지표면이 훼손되었는지 검사한다.

적외선 검사: 빛의 파장을 이용하여 사용된 잉크의 성분, 투과여부 등을 검사한다.

자외선 검사: 암실에서 자외선의 장·단파를 지표면에 조사하여 이상유무를 검사한다. 특히 형광반응의 유무를 살펴본다.

필흔재생기 검사: 유가증권에 처음 기재되었던 것을 지우고 다시 기재했는지를 알아보기 위해 필흔유무를 조사한다(양후열, 2002).

위조통화 수사 절차

1. 은행에서 확인을 거친 위폐를 제외하고 일반인이 신고한 경우에는 현미경 검사를 통해 위폐를 확인한다.
2. 신고된 위폐로부터 지문을 채취한다.
3. 경찰청장에게 보고한다.
4. 과학수사연구소나 한국조폐공사에 감정을 의뢰한다.
5. 위폐제조 방법, 지폐의 일련번호 등에 대해 관련기관과 정보를 교환한다.
6. 위조된 달러인 경우에는 미국 재무부의 비밀검찰부(Secret Service)를 통해 기존에 발견된 위폐와 동일한 일련번호를 인지를 확인한다.

지구촌이라 불리는 세계화가 빠르게 진행되고 있고, 컴퓨터와 인쇄기술이 하루가 다르게 발전하면서 위조의 문제는 전세계적인 현상으로 급증하고 있으며, 우리나라도 예외일 수 없다. 특히 최근에는 진폐와 동일 기법으로 제조되어 육안으로 식별할 수 없는 초정밀 위조 달러가 국내에서 발견되고 있고, 국제행사와 외국인의 출입이 빈번해 지면서 위조 유로화, 엔화, 위안화 등 다양한 위조 외화가 반입되고 유통되고 있어서 각별한 관심과 주의가 요망된다. '슈퍼노트'로 불리는 초정밀 위폐가 국내에 대량으로 반입된다면 국내의 금융질서 문란은 물론 국가 안보마저 위협받을 수 있는 상황이다. 정부는 일반국민과 환전업무 종사자를 대상으로 한 식별능력 제고를 위한 교육과 최신 위폐감별기 보급 등 정부차원의 준비를 해야 하겠다. 또한 위조를 어렵게 만드는 장치를 주기적으로 강화시켜야 한다. 기존의 지폐나 유가증권을 새로운 도안으로 변경할 때는 새 도안에 대해 일반인들에게 미리 알릴 필요가 있다. 특히 새 도안에 사용된 위조방지 장치에 대해 자세히 홍보하여 일반인들이 이 장치를 사용하여 위폐를 줄여나가도록 인도해야 하겠다.

위조를 담당하는 경찰관은 위조통화를 방법에 따라 분류하고, 데이터베이스화하여 수사를 돕고, 새로운 방법의 위조통화를 발견하게 되면 관계기관에 신속히 알리는 경보체계를 구축하는 것이 필요하다(이종화, 2002). 오늘날의 위조는 더 이상 한 기관, 국가만의 힘으로 근절될 수 있는 성격이 아니기 때문이다.

6. 외국 위조지폐의 식별요령

아래에서는 국가정보원이 제공한 외국 위조지폐의 식별요령을 소개하고자 한다.

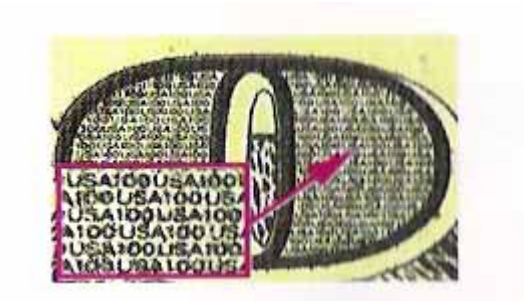
1) 위조미화 식별요령

(1) 중・저급 위조미화

위의 그림은 신권을 보여주고 있다. 진폐는 위조방지를 위해 90년부터 은선・미세문자를, 96년부터 은화・시변색잉크를 보강하였으며 이러한 보안요소가 위조여부를 확인할 수 있는 점검포인트이다. 미화는 요판인쇄 기법을 사용하여 인쇄부분의 촉감이 오돌오돌하며 확대 관찰하면 번짐현상이 있고 문자・무늬가 선명하다. 또한 미화의 지질은 면과 마를 혼합하여 내구성이 강하며 적・청색 특수 실이 내재되어 있어 핀 등으로 분리할 수 있다.

① 은선: 빛에 비춰보면 "USA100"이 세겨진 은선이 선명하게 나타난다.

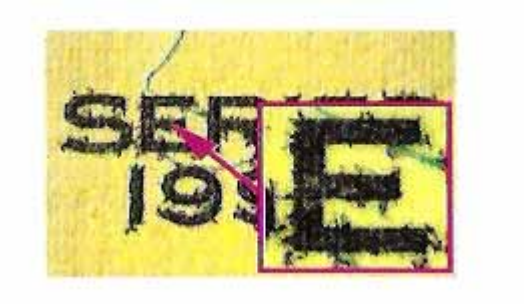
② 미세문자: “100”자를 확대경으로 보면 “USA100″이 선명하게 나타난다.



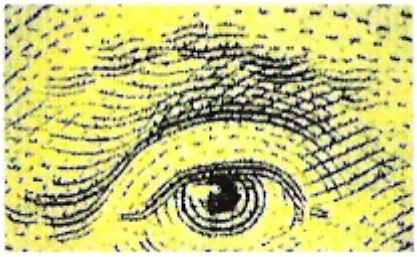
③ 은화: 빛에 비춰보면 프랭클린 초상화가 선명하게 나타난다.

④ 시변색잉크: “100”자가 보는 각도에 따라 색이 녹색에서 흑색으로 변한다.

⑤ 번짐현상: 문자・무늬 주위에 잉크 번짐 현상이 나타난다.



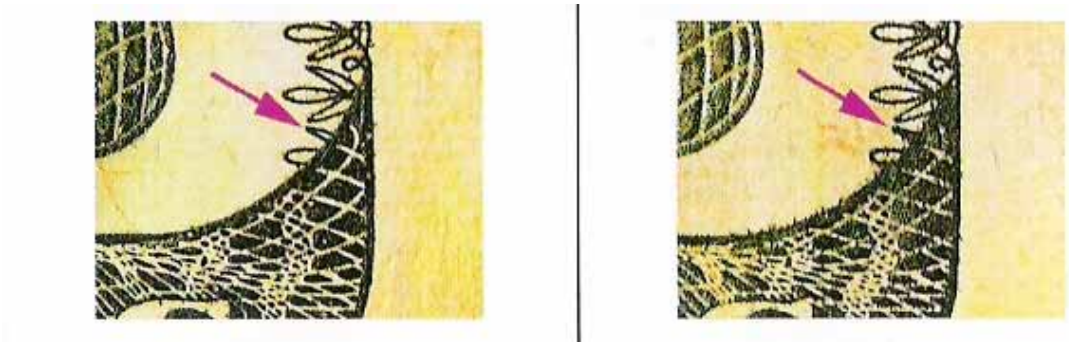
⑥ 선명도: 눈동자가 선명하고 생동감이 있다.



(2) 슈퍼노트

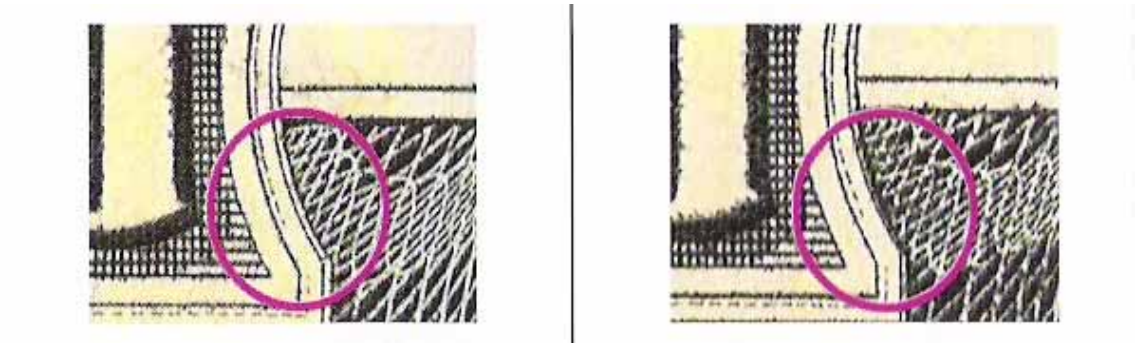
슈퍼노트는 진폐와 같은 위조방지요소를 가지고 있고 요판인쇄로 제작되어 육안식별이 매우 어렵다. 그러나 미화의 문자・무늬는 전문가에 의해 수조각으로 만든 동판으로 제작되기 때문에 슈퍼노트라도 인쇄부분의 모양・간격이 진폐와 100% 일치하기는 불가능하다.

① 고리내부가 진폐(왼쪽)는 비워있으나 위폐(오른쪽)는 검게 채워져 있다.

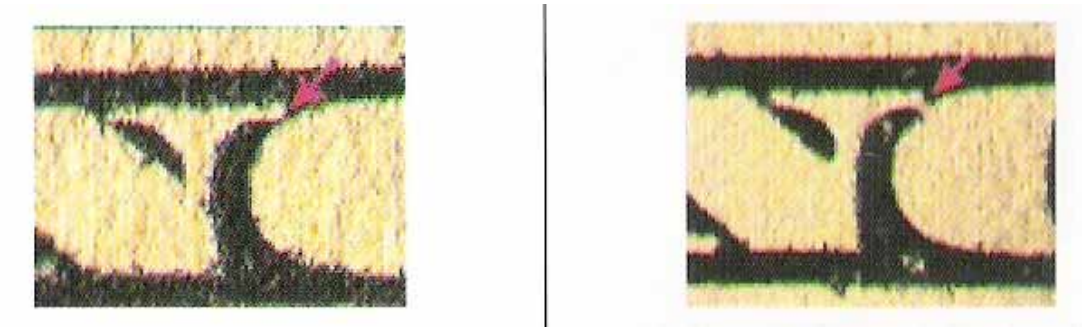


② STATES 문자의 “A″와 “T″자의 연결부분이 진폐(왼쪽)는 떨어져 있으나 위폐(오른쪽)는 붙어 있다.

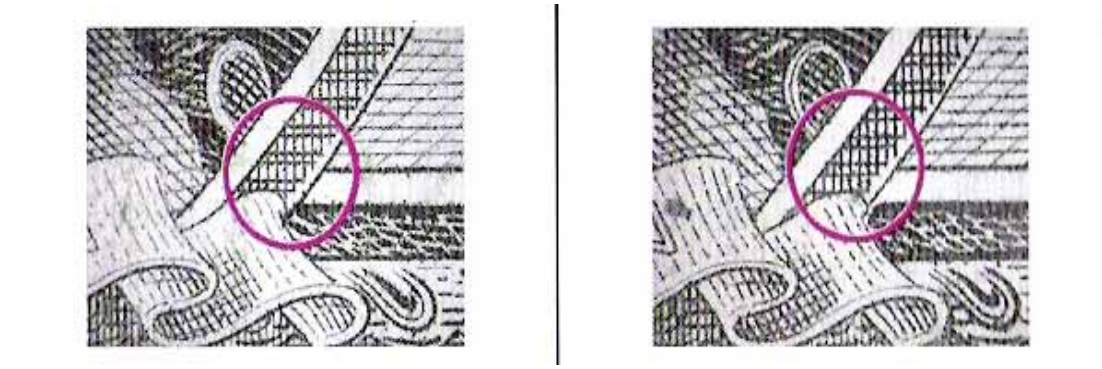
③ 100을 둘러싼 외곽표시선이 진폐(왼쪽)는 2개의 선이 평행을 이루나 위폐(오른쪽)는 내려올수록 좁아진다.



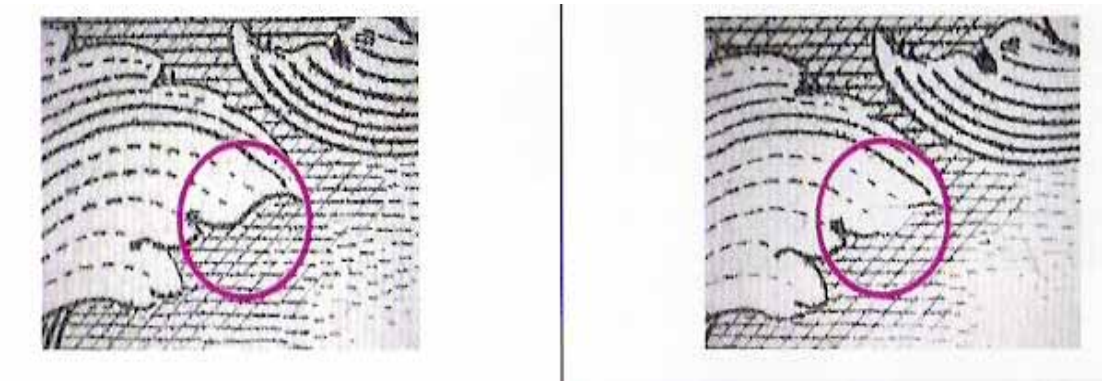
④ NOTE 문자의 “N”과 “O”자 연결부분이 진폐(왼쪽)는 떨어져 있으나 위폐(오른쪽은)는 붙어있다.



⑤ 초상화 외곽 타원형과 초상화 하단 프랭클린 리본 끝부분이 교차하며 맞닿은 가로선을 보면 진폐(왼쪽)는 좁은 칸부터 위폐(오른쪽)는 넓은 칸부터 시작한다.



⑥ 숫자(100) 아래 레이스 부분을 보면 진폐(왼쪽)는 레이스가 선명하게 연결되어 있으나 위폐(오른쪽)는 레이스가 연결되어 있지 않다.



2) 위조엔화 식별요령

① 요판인쇄: 액면문자 및 은행명이 요판인쇄되어 진폐는 손으로 만져 오돌오돌한 촉감을 느낄 수 있으나 위폐는 미끌미끌하다.

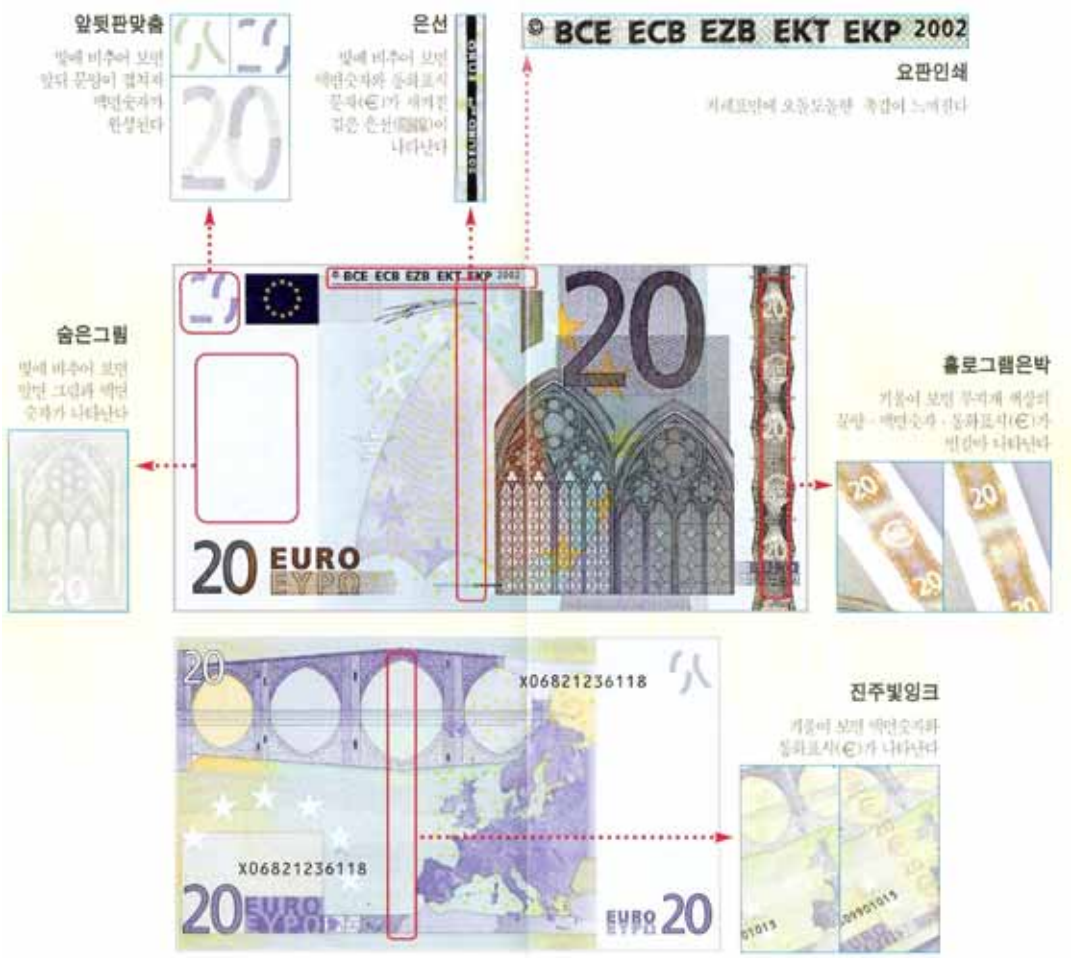
② 은화: 진폐는 중앙여백을 불빛에 비추면 초상화(후꾸자와 유기치)가 나타나는데 위폐는 초상화가 나타나지 않거나 뚜렷하지 않다.

③ 미세문자: 진폐는 앞면 액면숫자 아래 부분에 NIPPON GINKO(일본은행)가 미세하게 인쇄되어 있는 반면 위폐는 조잡하게 인쇄되어 있다.

④ 점자은화: 점자가 사용되어 진폐는 두 개의 고리모양(◎)의 맹인용 점자가 은화형태로 표시되는 반면 위폐는 없다.

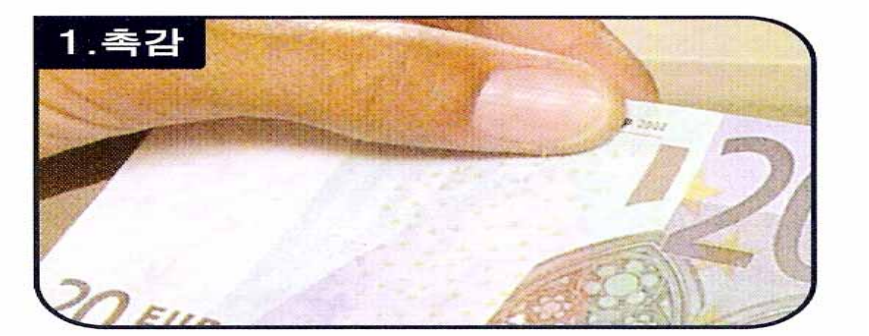
3) 위조유로화 식별요령

(1) 소액권(5, 10, 20유로)의 경우



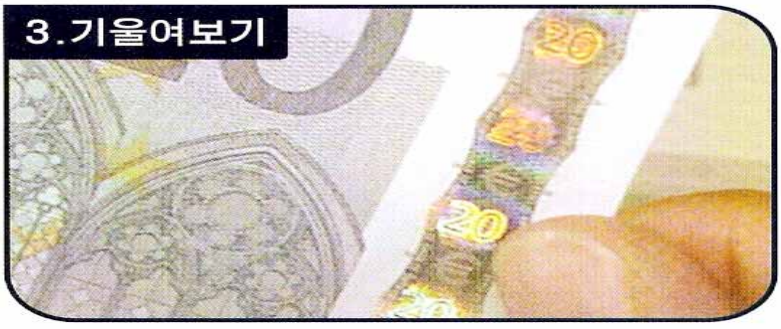
<기초식별방법>

① 유럽중앙은행(ECB) 문자·액면숫자 등을 만지면 지폐표면에 오돌오돌한 촉감이 느껴진다.



② 빛에 비추어보면 숨은 그림·은선이 나타난다.

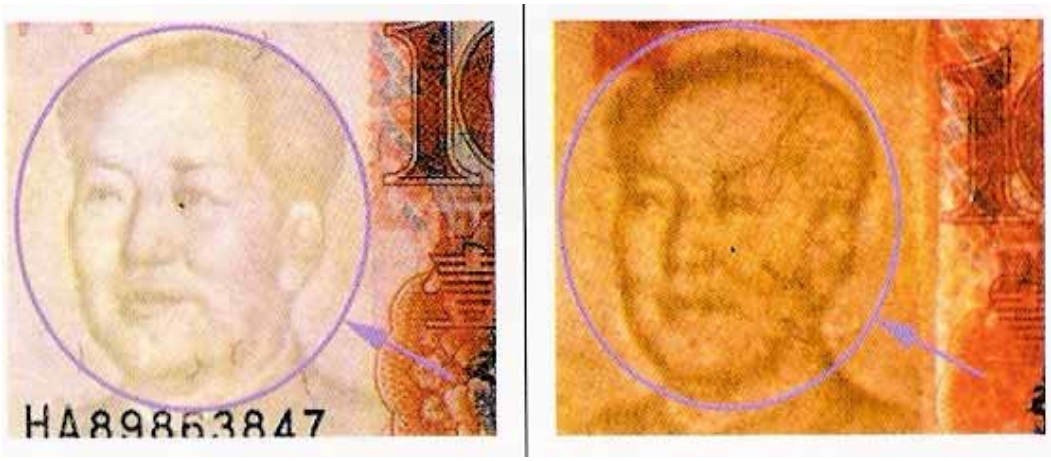
③ 홀로그램 은박을 기울여 보면 무지개 색상의 문양·액면숫자·통화표시 등이 번갈아 나타난다.



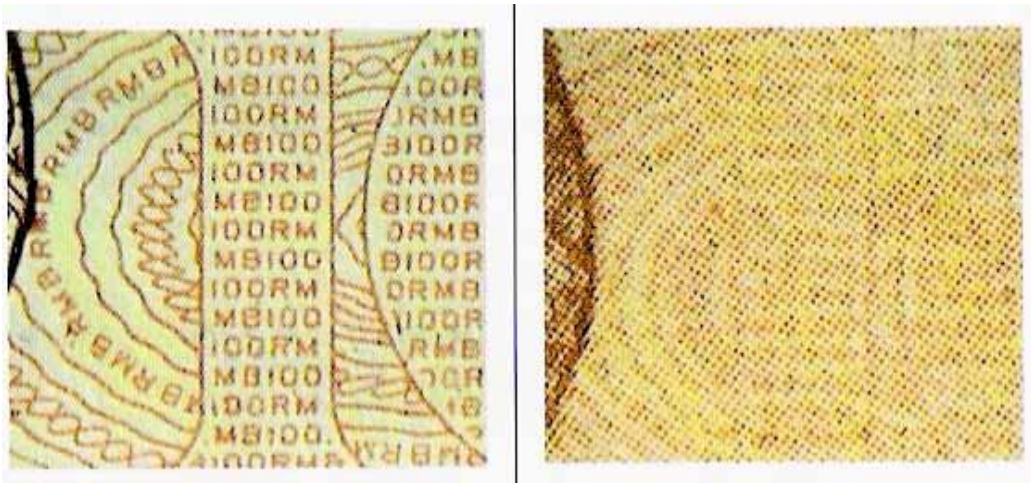
(2) 고액권(50, 100, 200, 500유로)의 경우

4) 위조위안화 식별요령

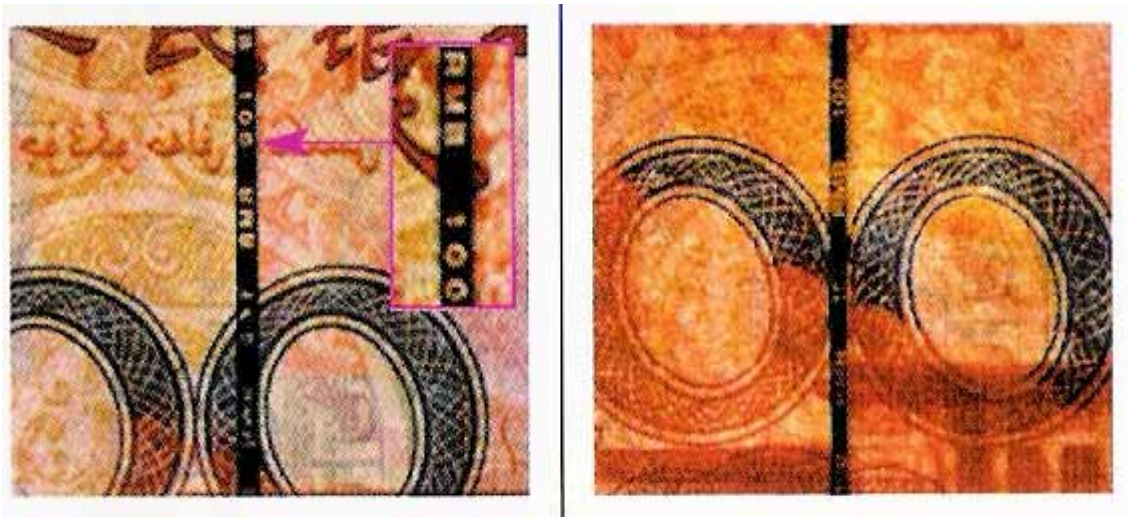
① 은화: 진폐(왼쪽)는 불빛에 비추면 모택동 초상화 그림이 선명하게 나타나고 위폐(오른쪽)는 은화가 없거나 있어도 입체감, 선명도가 떨어진다.



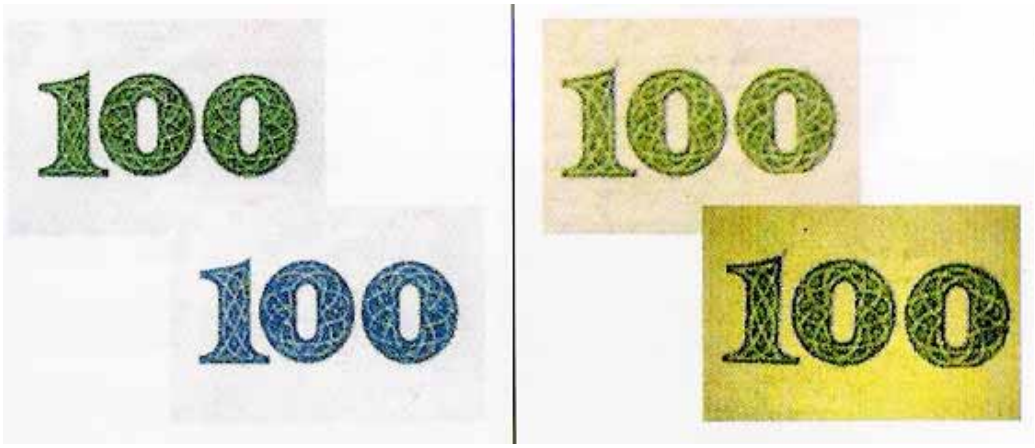
② 미세문자: 진폐(왼쪽)는 RMB 100이 선명하게 인쇄되어 있으나 위폐(오른쪽)는 조잡하게 인쇄되어 있거나 없다.



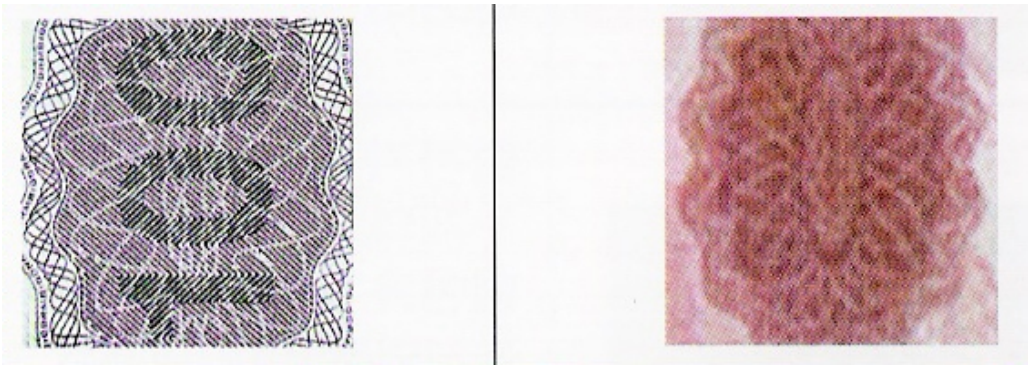
③ 은선: 진폐(왼쪽)는 RMB 100이 선명한데 반해 위폐(오른쪽)는 없거나 문자간격, 크기가 진본과 다르다.



④ 시변색잉크: 진폐(왼쪽)의 경우 보는 각도에 따라서 녹색에서 남색으로 변하는데 반해 위폐(오른쪽)는 색깔변화가 없거나 희미하다.



⑤ 잠상: 진폐(왼쪽)는 각도를 달리하여 보면 “100”이라는 숫자가 세로로 보이는 반면 위폐(오른쪽)는 안 나타난다.



⑥ 점자: 진폐는 손으로 만졌을 때 오돌오돌한 촉감이 느껴지는 반면 위폐는 미끌미끌하다.

제5장 요약 및 결론

21세기를 맞은 현대사회는 빠른 속도로 진행되는 세계화와 기술발전에 따라서 상업사회에서 지식정보화 사회로 진입하고 있고, 동시에 새로운 양상의 범죄를 경험하고 있다. 지식정보화 사회에서는 범죄수행이 용이해지는 반면 경찰이 범인을 검거하기는 더 어려워질 것으로 예상된다. 앞으로 일어날 신종범죄문제를 효과적으로 대처하기 위해서 새로운 유형의 범죄를 경험하고 있는 선진국들의 경험 가운데 신원도용범죄(identity crime), 산업 스파이, 유가증권 및 화폐의 위조문제를 선정하여 연구하였다. 선정된 3가지 신종범죄에 대한 연구결과는 요약하여 아래에 제시하였다.

1. 요 약

1) 신원도용범죄(Identity Crimes)

타인의 신상정보를 이용한 범죄를 identity crime이라고 부른다. 이 범죄는 금세기에 가장 빠르게 증가하고 있는 범죄로 알려져 있다. identity crimes 중에서 가장 대표적인 범죄인 identity theft와 개인신원정보관련 사기에 대해서 미국 법무부는 누군가가 다른 사람의 개인정보를 불법적으로 획득하고 사기와 기만의 방식으로 사용하여 주로 경제적 이익을 얻어내는 모든 종류의 범죄를 일컫는 것으로 정의하고 있다.

ID theft의 특징은 자기도 모르는 사이에 피해자가 될 수 있고, 피해를 회복하기까지 긴 시간과 노력, 비용이 소요된다는 점이다. 절도범이 개인의 신상정보를 훔치는 방법은 다양해서 일상생활의 다양한 영역에서 발생한다. 구체적으로 보면, 남의 우편물을 훔쳐서 신상정보나 신용카드 등을 얻기도 하고, 개인이나 기관이 사용하고 버린 쓰레기에서 정보를 구하기도 하며, 줍거나 훔친 남의 지갑에서 정보를 얻기도 하고, 인터넷을 이용하거나, 신용카드의 자기테입을 불법으로 복제하기도 한다. 특히 가장 최근에 주목을 받는 Phishing은 불특정 다수에게 이-메일을 보내 고객의 계정에 문제가 있으니 신

용카드 정보나 개인의 금융정보를 업데이트 하도록 요구하거나, 대출이나 사이트 무료 이용 등 달콤한 제안을 하여 타인의 신상정보를 알아낸다.

타인의 개인정보를 훔쳐낸 절도범들은 사기꾼들에게 정보를 팔아넘긴다. 사기꾼들은 훔치거나 구입한 타인의 신분을 가지고 음란 사이트를 방문하거나, 자동차를 구입하고, 은행계좌나 신용카드를 만들어 한계까지 사용하고 나서 도주하여 무고한 피해자의 신용기록에 치명적인 손상을 입히게 된다. 피해자는 이 문제가 해결될 때까지 취직도 못하고, 신용카드를 사용하지도 못하게 된다. 더욱 심각한 문제는 피해자가 신용을 회복하기까지 경제적인 비용부담이 크고, 상당한 시간을 투자해야 한다는 점이다. California 주의 한 공익조사기관이 수행한 설문조사에 의하면 identity theft 피해자가 신용을 회복하기 위해 사용한 금액은 변호사비를 제외하고 $30~$2,000로 나타났으며, 피해자가 사건발생 이후에 손상된 신용을 회복하기까지 대개 2년 넘는 기간에 평균 175시간을 투입하고 평균 손실액은 $808로 나타났다.

미국의 경우, 연방거래위원회가 2003년에 4000여명의 성인을 대상으로 수집한 자료를 분석한 결과 조사 대상자가운데 4.6%가 지난 1년 사이에 identity theft의 피해경험을 가지고 있는 것으로 나타났다. 또한 연방거래위원회에 접수된 identity theft관련 고충건수는 매년 증가하고 있다. 특히 “전자금융거래”와 관련된 identity theft가 급증하고 있는 것으로 나타난다. 피해자 가운데는 사리판단이 정확하지 않은 노인이나 아동이 포함된다.

Identity theft가 빠르게 증가하는 원인을 범죄자의 관점에서 찾아 볼 수 있다. 첫째, 타인의 신상정보를 손쉽게 구할 수 있다. 둘째, 범죄사실이 수개월 혹은 수년간 발견되지 않을 수 있다. 셋째, 신고 되지 않거나 신고 되도 체포될 확률이 낮다. 결국, identity theft는 손쉽고 조용하게 범죄를 저지를 수 있고, 체포되거나 기소될 위험이 낮으면서 돈을 벌 수 있는 매력적인 범죄인 셈이다.

미국이 identity theft문제를 인식하여 공식적인 대책을 수립한 것은 비교적 최근의 일이다. 미국은 1998년에 Identity Theft and Assumption Deterrence Act를 통과시켜 identity theft를 새로운 범죄로 규정하였다. 새로운 법안이 만들어지면서 연방거래위원회를 지정하여 identity theft에 관한 신고를 접수하고 자료를 수집하게 하였다. 그러나 이 범죄가 상대적으로 새로운 범죄이면서 폭넓게 퍼져 있어서 경찰이나 피해자 지원단체도 아직 적절히 대응하지 못하고 있는 것으로 지적된다. 미국은 2가지 전략을 취하고

있는 바, 전국적인 규모의 소탕작전을 수행하고 있고 identity theft에 대한 기존의 연방 형법을 강화해 가고 있다. California주는 2005년 9월에 반phishing법을 제정하여 강력한 처벌규정을 마련하였다.

신종범죄인 identity theft를 효과적으로 대비하기 위해서 경찰은 먼저 실태조사를 할 필요가 있다. 조사를 통해 실효성 있는 대책을 마련할 수 있을 것이다. 또한 입법활동을 통해 identity theft를 범죄로 규정해야 경찰을 포함한 실무기관이 보다 적극적으로 대응할 수 있을 것이다. 그러나 근본적으로 identity theft가 현대인의 생활양식과 긴밀히 관련되어 있는 현상이므로 국민들로 하여금 일상에서 신상정보를 지키기 위해서 주의를 기울이고, 안전을 위해서 불편을 감수하도록 계몽시킬 필요가 있다. 또한 identity theft의 피해자가 되었을 때 취할 조치를 가르치는 교육 프로그램을 마련해야 하겠다.

2) 산업스파이

산업스파이는 주로 상업적 목적에서 수행되는 스파이활동이다. 그러나 산업스파이로 인하여 국가의 중요한 산업기반이 타격을 입을 경우에는 그 국가의 성장 동력 또한 파괴될 수 있기 때문에 오늘날 각국은 산업스파이 문제를 국가안보의 차원에서 중요하게 다루고 있다.

종래의 산업스파이는 유괴, 납치, 고문, 살해, 도청 등과 같은 불법적 행위를 자행하는 경우가 많았으나, 근래에는 정보통신기술의 발달로 그와 같은 '물리적' 정보취득 방법을 사용할 필요성이 현저히 감소하였으며, 대부분의 비밀 영업정보를 불법적 수단을 사용하지 않고서도 취득할 수 있게 되었다. 또한 스파이활동의 주체도 크게 변화하여 최근에는 외국 정부나 스파이기관들에 의해서보다는 서로 경쟁관계에 있는 민간기업체들에 의해 자행되고 있는 것이 대부분의 추세이다.

산업스파이에 있어서 이와 같은 패러다임의 변화는 각국의 산업스파이에 대한 대응체계도 과거와는 다른 양상을 띠게 하였다. 과거 정부일변도의 대응체계가 최근에는 해당 기업체와 민간단체들이 산업스파이에 대한 대응에 주체적으로 참여하게 됨으로써 소위 정부와 민간이 공동전선을 형성하는 형태로 발전하고 있다. 각국은 산업보안관련 법령과 제도의 정비 등을 통한 보안시스템 구축에 노력하고 있으며, 기업 및 민간은 자체 보안역량을 강화하고 산업보안관련 교육, 전문 인력양성, 정보제공, 정책건의 등을 통해 정부기관과의 공조를 확대하고 있다.

우리나라의 경우 아직 산업스파이 문제의 심각성에 대한 인식이 부족하고, 단속을 위한 관련 법규도 미비하며, 대응 인력 및 기술이 충분치 못하여 산업스파이 문제에 대해 효율적인 대응을 하기에 어려움이 있다. 따라서 최근에 날로 심각해지고 교묘해지고 있는 산업스파이 사건을 효과적으로 예방하고 적극적으로 대처하기 위해서는 일차적으로는 민간 기업들의 보안의식 및 보안능력의 향상이 전제되어야 하겠지만, 경찰 및 검찰 나아가 국가정보원 등 국가기관들의 공조 및 수사역량의 강화도 늦출 수 없는 중요한 사안이라 할 것이다.

3) 화폐 및 유가증권 위조

위조화폐와 위조유가증권은 일반대중이 화폐나 유가증권에 대해서 갖는 신념이나 신뢰를 기만하여 대중의 신뢰에 치명적인 영향을 미친다. 특별히 위조화폐는 국가의 화폐 발행과 사용에 대한 독점권을 침해하는 심각한 행위이다.

위조된 화폐나 유가증권이 초래하는 비용을 기업이나 개인 차원과 국가 차원으로 나누어 볼 수 있다. 기업이나 개인이 위조 화폐나 유가증권을 받게 되면 그만큼 수입이 줄어들어 직접적인 비용을 경험한다. 또한 기업은 위폐의 피해를 줄이기 위해 직원들에게 위폐 감식법과 대처법 등을 교육하고 감식 장비를 구입하는 데 추가적인 비용을 지불하게 된다. 국가 차원에서는 위폐문제가 심각해짐에 따라 위폐방지 기능을 강화한 새 도안의 화폐와 유가증권을 도입함에 따라 비용부담이 커진다. 더욱이 초정밀 위폐의 유통이 증가할수록 금융질서 문란은 물론 국가 안보마저 위협을 받게 된다.

화폐의 위조 가운데서도 가장 일반적인 지폐위조에는 전통적인 오프세트 인쇄방법이 사용된 경우와 최근 컴퓨터 및 프린터 기술의 발전에 힘입은 디지털 기술로 제조된 경우, 국가를 상대로만 판매되는 초정밀 화폐 인쇄기를 이용해 만든 수퍼노트로 구분할 수 있다. 최근에는 미국이 북한의 수퍼노트 제작과 유통 혐의를 제기하면서 국제문제화 되고 있다. 미국의 발표에 따르면, 1989년부터 적발되기 시작하여 지난 16년간 모두 5000만 달러에 이르는 북한산 위폐가 적발된 것으로 알려져 있다. 미국이 제시하는 북한 위폐의 증거는 2가지이다. 첫째, 북한 외교관이 위폐를 가지고 있다가 검거된 사건들이 있다. 둘째, 북한은 1975년에 스위스에서 화폐제조용 초정밀 인쇄기를 구입한 이래, 최근에는 스위스산 색변환 잉크와 일본과 프랑스에서 만든 정밀 화폐인쇄기를 대량 구입했다고 한다. 북한 위폐에 대한 증거가 정황증거의 수준에 머물고 있으나 국제간

금융질서를 깨뜨리고 국가 안보를 위협하는 사안인 만큼 경찰을 포함한 법집행기관들은 북한 위폐에 대해 자료를 수집하고 대책을 수립해야 할 단계이다.

국내에서 발견된 위조 화폐와 위조 유가증권은 매수와 액수 모두 증가하고 있다. 국내 화폐와 외국 화폐의 위조로 나누어 보아도 모두 크게 증가 하고 있어서 정부차원의 대책이 필요한 시점이다.

미국의 경우를 보면, 지난 100여년 이상 위폐를 낮은 수준으로 유지하고 있다. 이것은 미국 정부가 지속적으로 위조방지장치를 도입하고, 적극적으로 법을 집행하며, 대중을 상대로 위폐방지를 위한 교육을 실시해 온 결과이다. 미국 정부는 위폐에 대해 매우 적극적으로 법집행을 하고 있어서 2004년의 경우에 사법당국이 달러 위폐가 유통되기 전에 그 절반정도를 압류하였다. 미국 정부는 또한 위조범들보다 앞서기 위해 매 7년에서 10년마다 지폐의 도안을 새롭게 해 오고 있고, 위조방지 장치로 미세인쇄, 안전사(은선), 은화, 요판잠상, 색변환(시변색) 잉크 등을 사용하고 있다.

미국의 인접국인 캐나다에서는 위폐범에게 주어지는 처벌이 미국보다 상대적으로 가벼워 억제효과에 문제가 있는 것으로 지적되고 있다. 캐나다에서 위조지폐 사건은 전체 형사범죄의 5% 정도를 차지하여 6번째로 빈번하게 발생하는 범죄유형이 되고 있다.

수퍼노트를 제외한 대부분의 위조된 지폐와 유가증권은 컴퓨터 및 칼라 복사기로 만들어 진 것이다. 따라서 영세사업자 등 일반인을 상대로 위폐판별법을 교육하여 일상적인 소규모 거래에서 위폐여부를 확인하게 되면 이 문제를 상당히 줄일 수 있을 것으로 기대된다. 지폐에 안전장치를 마련하는 것 못지않게 일반 대중에게 지폐에 설치한 안전장치를 알리는 것이 중요하다.

세계화의 빠른 진행과 컴퓨터와 인쇄기술의 발전과 더불어 위조의 문제는 전세계적인 현상으로 급증하고 있다. 특히 최근에는 진폐와 동일한 기법으로 제조되어 육안으로 식별할 수 없는 초정밀 위조 달러가 국내에서 발견되고 있고, 국제행사와 외국인의 출입이 빈번해지면서 위조 유로화, 엔화, 위안화 등 다양한 위조 외화가 반입되고 유통되고 있어서 각별한 관심과 주의가 요망된다. 수퍼노트가 대량으로 국내에 반입된다면 새로운 형태의 테러로 국가의 안보마저 위협할 수 있다. 정부는 일반국민과 금융기관 종사자를 대상으로 교육을 강화시켜야 할 것이고, 최신 위폐감별기를 보급시키고, 주기적으로 위조방지 장치를 강화시켜야 할 것이다. 위조를 담당하는 경찰관은 각 외화별로 위조지폐 식별요령을 익히고, 위조통화를 방법에 따라 분류하고, 데이터베이스화 하여

수사에 돕고, 발견한 위조통화를 관계기관에 신속히 알려 공동으로 대처하는 체계를 구축할 필요가 있다.

2. 결 론

세계는 빠르게 변하고 있고, 범죄자들도 이러한 변화를 이용하여 새로운 방식에 의한 범죄를 수행하고 있다. 21세기 지식정보화 사회는 세계적(global)이고, 접근이 용이하며(accessible), 자동화되고(automated), 부호화(encryption)된 특징을 갖는다. 신종범죄도 지식정보화 사회의 특징을 반영하여 범죄자들은 공간의 한계를 상당히 극복한 가운데 세계 도처에서 범죄를 저지를 수 있고, 범죄 대상이나 수단에 쉽게 접근할 수 있으며, 과거에는 수행하기 어려웠던 범죄들이 자동화로 손쉬운 일이 되고, 부호화를 통해 자신의 신분을 손쉽게 숨길 수 있게 되었다.

지식정보화 사회에서 범죄활동이 빠르게 일반화되고 있지만 피해자는 피해사실과 피해정도를 모를 수 있고, 불법 활동과 합법 활동 사이의 경계가 불분명해 질 수도 있다. 그리하여 21세기에는 범죄수행이 용이해지는 반면 경찰이 범인을 검거하기는 더 어려워질 것으로 예상된다.

경찰을 비롯한 오늘날의 형사사법기관들은 빠른 변화와 새로운 기회 창출에 따라 새로운 형태의 범죄가 생겨나면서 새로운 도전에 직면해 있다. 새로운 범죄라고 해서 과거에는 없었던 완전한 별종범죄라기보다는 기존의 범죄가 새로운 기회를 이용하여 생겨나는 변종인 경우가 대부분이지만 과거에 사용해오던 대응만으로 신종범죄를 통제하기는 어렵다. 새로운 도전과 이에 대한 대응 여하에 따라서 새 시대가 질서를 유지하며 발전을 하느냐 아니면 혼란과 해체의 나락으로 떨어지느냐의 경로가 결정될 것이다. 아래에서는 새로운 범죄에 대한 대응책을 몇 가지 정리하여 제시하였다.

첫째, 새로운 유형의 범죄에 대한 연구를 통해 그 실태와 원인을 파악해야 하겠다. 소위 신종범죄에 대한 연구는 선진국에서도 찾아보기 어려워 그 실태파악 마저 어려운 것이 현실이다. 그러나 실태를 알고 더 나아가 원인을 알아야 효과적인 해결책을 제시할 수 있음은 두말할 나위가 없다. 경험적인 연구를 통해서 탐색하고 설명해가는 수고

없이 해결책을 구한다면 연목구어(緣木求魚)의 우를 범하게 된다.

둘째, 필요하다면 새로운 유형의 범죄를 규제할 수 있는 입법화 작업이 필요하다. 기존의 법규로 새로운 범죄를 통제하기 어려워 피해의 위험이 커지게 된다면 입법화를 거쳐 범죄로 규정하는 것이 필요하다. 이 경우에도 실태조사에 기초하여 입법을 요구한다면 설득력을 얻게 된다.

셋째, 신종범죄는 변화된 일상생활과 밀접한 관련을 맺고 있어서 일반국민들의 일상생활에서의 주의가 요구되고 범죄로부터 스스로를 지키기 위해 생활양식의 변화가 필요하다. 정부는 범죄피해를 줄일 수 있도록 대국민 교육 프로그램을 운영할 필요가 있다. 신종범죄로부터 국민들을 보호하기 위해서는 경찰 등 공기관 뿐만 아니라 민간단체들이 나서서 범죄피해를 막는 방법과 대처법 등 관련 정보를 제공하는 것이 필요하다. 이를 위해서 인터넷 웹 사이트의 운영도 효과적이다. 범죄문제의 해결을 위해 형사사법기관 이외의 시민과 시민단체의 협조와 참여가 중요하다. 이를 위해서 시민들이 형사사법기관에 대해 신뢰하고 확신을 가지도록 경찰 등 형사사법기관들이 대민 관계를 형성하고 유지하는 일이 중요하다고 하겠다. 지역 주민들로 하여금 자신들이 살고 있는 지역사회에 대해 상징적으로나 실질적으로 이해관계를 강화시키도록 돕고 이것을 범죄예방과 연결시키는 전략이 필요하겠다.

넷째, 기술의 발달이 새로운 범죄의 발생에 기여했다면, 범죄에 대한 대응도 기술발전의 도움을 받아야 한다. 발달된 기술을 응용하여 대상 견고화(target hardening)와 감시와 보호의 수준을 높일 수 있을 것이다. 다만, 범죄예방을 위해서 사용하는 기술의 수준은 범죄자들이 사용하는 기술보다 앞서 있어야 하고 이를 위해서 지속적으로 개량된 기술을 채택해야 한다. 범죄예방을 위해 사용한 기술이 범죄자들이 사용하는 기술수준보다 뒤지게 되면 오히려 범죄수행에 악용될 우려가 존재한다.

다섯째, 새로운 범죄를 통제하기 위해서는 새로운 동반자 관계가 필요하다. 세계화와 대상에의 접근성의 향상으로 시간과 공간의 한계를 상당히 극복하고 있는 신종범죄에 대응하기 위해서는 형사사법기관들 사이의 공조, 공기관과 사기관 사이의 협력, 국가와 국가간의 협력을 통해서 범죄를 예방하고 범죄사건을 해결할 수 있게 된다. 예컨대, 컴퓨터를 이용하여 사이버 상에서 발생하는 신종범죄들을 통제하기 위해서는 국경을 초월한 많은 기관들의 노력이 필요하다.

참고문헌

1. 신원도용범죄(Identity Theft)

<국내 문헌>

"대한민국 전자정부 이단 스톱" 중앙일보 2005. 9. 28.
"'미 카드사 해킹' 국내 불똥 튀나" 중앙일보 2005. 6. 23.
"신종 '짝퉁 사이트' 금융사기 등장" 중앙일보 2005. 10. 17.
"'온라인 신분증' 공인인증서 보안 비상" 중앙일보 2005. 10. 31.
"올해는 속지 말고 뚫리지도 말자" 중앙일보 2006. 1. 4.
"인터넷, 텔레뱅킹 비밀번호 입력 방식 변경" 중앙일보 2005. 9. 21.
"차 좀 빼주세요 강도" 중앙일보 2005. 6. 23.

<영미 문헌>

Abagnale, Frank. 2004. The Real U Guide to Identity Theft. Real U Guides.

Arata, Michael J. 2004. Preventing Identity Theft for Dummies. Wiley Publishing, Inc.

Beccaria, Cesare. 1963. On Crimes and Punishments. Indianapolis: Bobbs-Merrill.

Bentham, Jeremy. 1970. An Introduction to the Principles of Morals and Legislation. London: The Athlone Press.

Cohen, L. E. & Felson, M. 1979. Social change and crime rates: A routine activities approach. American Sociological Review, 44:588-608.

Collins, Judith M. and Sandra K. Hoffman. 2003a. Identity Theft: A Case Study. Michigan State University. Lansing, MI.

Collins, Judith M. and Sandra K. Hoffman. 2003b. Identity Theft First Responder

Manual for Criminal Justice Professionals. Flushing, NY: Looseleaf Law Publications, Inc.

Cornall, Robert. 2001. "Criminal Futures." Paper presented at the 4th National Outlook Symposium on Crime in Australia, New Crimes or New Responses convened by the Australian Institute of Criminology and held in Canberra 21-22 June 2001.

Etter, Barbara. 2001. "Computer Crime." Paper presented at the 4th National Outlook Symposium on Crime in Australia, New Crimes or New Responses convened by the Australian Institute of Criminology and held in Canberra 21-22 June 2001.

Federal Trade Commission. 2000. Identity Theft victim complaint data: Figures and trends on identity theft. Retrieved November 20, 2002, from http://www.ftc.gov/bcp/workshops/idtheft/charts-update.pdf

Federal Trade Commission. 2003a. Fraud complaint and identity theft victims by state. Retrieved March 31, 2003, from

http://www.consumer.gov/sentinel/trends.htm

Federal Trade Commission. 2003b. Identity Theft Survey Report.

Federal Trade Commission. 2005. National and State Trends in Fraud and Identity Theft: January - December 2004 Retrieved February 1, 2005, from http://www.consumer.gov/sentinel/trends.htm

Graycar Adam. 2001. "New Crimes or New Responses." Paper presented at the 4th National Outlook Symposium on Crime in Australia, New Crimes or New Responses convened by the Australian Institute of Criminology and held in Canberra 21-22 June 2001.

Hoar, Sean B. 2001. "Identity Theft: The Crime of the New Millennium." United States Attorney's USA Bulletin. Executive Office for United States

Attorneys, U.S. Department of Justice.

Lininger, Rachael and Russell Dean Vines. 2005. Phishing: Cutting the Identity Theft Line. Wiley Publishing, Inc.

Lininger, Rachael and Russell D. Vines. 2005. Cutting the Identity Theft Line. Wiley, John & Sons, Incorporated.

Mazerolle, Lorraine. 2001. "Policing in the 21st Century: What works and what doesn't." Paper presented at the 4th National Outlook Symposium on Crime in Australia, New Crimes or New Responses convened by the Australian Institute of Criminology and held in Canberra 21-22 June 2001.

Newman, Q. J. 1999. Identity theft: The cybercrime of the millennium. Port Townsend, WA:Loompanics Unlimited.

Office of the Inspector General. 1999. Analysis of social security number misuse allegations made to the Social Security Administration's fraud hotline (Management Advisory Report, A-15-99-92019). Washington, DC: Author.

Smith, Russell G. 2001. "Controlling Cross-border Economic Crime." Paper presented at the 4th National Outlook Symposium on Crime in Australia, New Crimes or New Responses convened by the Australian Institute of Criminology and held in Canberra 21-22 June 2001.

Stuart F. H. Allison, Amie M. Schuck, Kim Michelle Lersch. 2005. "Exploring the Crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics". Journal of Criminal Justice 33:19-29.

Sullivan, Bob. 2004. Your Evil Twin: Behind the Identity Theft Epidemic. Wiley, John & Sons, Incorporated.

Synovate. 2003. Federal Trade Commission - Identity Theft Survey Report Retrieved September, 2003, from

http://www.consumer.gov/sentinel/

The Silver Lake Editors. 2004. Identity Theft: How to Protect Your Name, Your Credit and Your Vital Information ... and What to Do When Someone Hijacks Any of These. CA: Silver Lake Publishing.

U. S. General Accounting Office. 2002, June. Identity fraud: Greater awareness and use of existing data needed (Publication No. USGAO-02-766). Washington, DC: Author.

VideoPlus. 2003. Identity Theft Someone is Watching You. Lake Dallas, TX: Momentum Media.

Welsh, Amanda. 2004. Identity Theft Protection Guide: Safeguard Your Family, Protect Your Privacy, Recover a Stolen Identity. St. Martin's Press.

"Instant credit means instant identity theft: Retailers, banks in a rush make things easy for imposters". MSN NBC May 25, 2005.

"Grand Identity Thief" Newsweek July 6, 2005.

2. 산업스파이

<국내 문헌>

국가정보원. 2004. 미국 기업의 사이버보안 전략.
국가정보원. 2005. 日本의 知的財産保護戰略.
국가정보원. 2004. 산업보안연구논총.
국가정보원. 2004. 첨단산업기술보호동향 제1호.
국가정보원. 2004. 첨단산업기술보호동향 제2호.
국가정보원. 2005. 첨단산업기술보호동향 제3호.
국가정보원. 2005. 첨단산업기술보호동향 제4호.
김용선. 1996. 특허정보.
남상봉. 2004. "산업스파이 수사사례 분석 및 대응방안."

법원도서관. 1995. 조약집, 제3권(다자조약 3) 상, 재판자료 제69집.
사법연수원. 1999. 新種犯罪: 형사실무.
정병두. 1994. 미공개정보의 보호. 법무부(편),
한상훈. 2000. 산업스파이에 대한 형사법적 대응방안. 한국형사정책연구원.
법무부. 1994. UR협정의 법적 고찰(하),

<외국 자료>

Dorothy E., 1999. "Information Warfare and Security" Addison-Wesley 3rd printing. July

E.I. DuPont de Nemours & Co. v. Christopher, 431 F.2d 1012, 166 U.S.P.Q. 421 (1970), cert. denied, 400 U.S. 1024.

Fialka, John J. 1999. War by Other Means: Economic Espionage in America. W. W. Norton & Company.

Parad, Boris. 1997. Commercial Espionage: 79 Ways Competitors Can Get Any Business Secrets in Any Country. Global Connection, Inc.

The Associated Press, 1981.10.6. Business News Section.

U.S. Department of Justice. 1997. Federal Prosecution of Violation of Intellectual Property Rights. U.S. Department of Justice.

Winkler, Ira. 1997. Corporate Espionage. Prima Publishing.

http://en.wikipedia.org/wiki/Industrial_espionage
http://www.fbi.gov/hq/ci/cases.htm
http://www.fbi.gov/hq/ci/economic.htm
http://www.fbi.gov/intelligence/intell.htm
http://www.fbi.gov/publications/strategicplan/stategicplantext.htm
http://www.irational.org/APD/CCIPS/ip.html#FPVIPR

http://www.nacic.gov/
http://www.newhaven.edu/california/CJ625/p6.html.
http://www.nis.go.kr/docs/terror/indus/type.html .
http://www.pimall.com/nais/econesp.html
http://www.sfalx.com/h_intell_manual.htm#CHAPTER%207
http://www.usdoj.gov/criminal/cybercrime/home.html#FPVIPR
http://www.usdoj.gov/criminal/cybercrime/intell_prop_rts/toc.htm#V
http://www.usdoj.gov/criminal/cybercrime/ipmanual/06ipma.htm

3. 화폐 및 유가증권 위조

<국내 문헌>

국가정보원. 2003. 국제금융범죄 이렇게 막자.
양후열. 2002. “위·변조 유가증권 및 위·변조 화폐.” 수사연구, No. 227, p10-17.
이재상. 2000. 형법각론. 박영사.
이종화. 2002. “위조 통화범죄 수사.” 수사연구, No. 227, p24-30.
중앙일보. 2005. 11. 11. “북한 ‘마카오 은행 대북 거래금지’ 반발.”
중앙일보. 2005. 12. 8. “버시바우 미국 대사 관훈클럽 토론.”
중앙일보. 2005. 12. 22. “‘북한 위조 달러’ 한·미 이견 심각.”
중앙일보. 2006. 1. 3. 김찬규 “북한 달러 위조 명백한 국제범죄.”
중앙일보. 2006. 2. 9. “북한 의지에 따라 해결 가능한 문제.”
한국아이닷컴. 2005. 12. 25. “외화 위조지폐 극성.. 대부분 초정밀 ‘수퍼노트.’”
Chosun.com. 2006. 2. 1. “‘다’ 5000원권 위폐 기승.”

<영미 문헌>

Altig, David E. 2002. 5. 1. "Why is stable money such a big deal?" Economic Commentary: Federal Reserve Bank of Cleveland.

Chidley, Joe. 2004. 8. 30. "Money: the do-it-yourself approach." Canadian Business, Vol. 77, Issue 17, p6-6.

Grandi, Ciro. 2004. "The Protection of the Euro against Counterfeiting." European Journal of Crime, Criminal Law and Criminal Justice, Vol. 12/2, p89-131.

Kersten, Jason. 2005. 7. 28. "The Art of Making MONEY." Rolling Stone, Issue 979, p58-96.

Locy, Toni. 2005. 8. 18. "Digital imaging changed face of counterfeit bills." USA Today.

McClearn, Matthew. 2004. 8. 30. "Making Money." Canadian Business, Issue 17, p47-59.

New York Times. 2004. 1. 7. "Russia: New Ruble Bank Notes Planned." Vol. 153, Issue 52721, pW1-W1.

New York Times. 2005. 4. 9. "Official Say Sixth Graders Counterfeited." Vol. 154. Issue 53179, pA15-A15.

Science News. 2005. 8. 20. "Roughing up counterfeiters." Vol. 168. Issue 8. p126-126.

World Almanac & Book of Facts. 2005. New U. S. Currency Designs. p118-119.