군사기밀 유출자에 대한 손해배상 제도 적용 방안

박준정*, 김광조*

*카이스트 정보보호대학원

A Compensation Method to the Deliberate Military Secret Leakers

Joon-Jeong Park*, Kwangjo Kim*

*Graduate School of Information Security, KAIST.

요 약

현존하는 적의 위협에 노출되어 있는 우리나라에서 국가안보는 그 어떤 분야보다 중요한 영역이다. 이를 위해 범정부 차원에서 다양한 정책과 노력을 경주하고 있는데, 정작 국가안보 최일선에 있는 군에서 군사기밀 유출 사고가 끊임없이 발생하여 국가안보에 막대한 위협요소로 대두되고 있다. 이러한 군사기밀 유출 사고를 살펴보면 금전적인 유혹과 개인의 이익을 위한 기밀 불법 거래가 대부분이며, 특히 최근 사회적으로 군피아 논란 중 큰 이슈가 된 '방위력개선 관련 군사기밀 대규모 해외유출사건' 등에서도 피의자는 금전적 이익을 보장받는 대가로 군사기밀을 유출해 왔다. 이에 본고에서는 실제 기밀유출 차단 효과를 높이기 위해 인간의 심리적인 특성을 활용하여 군사기밀보호법상 고의적으로 군사기밀을 유출한 자에 대해 손해배상 제도를 적용하는 방안을 제안하며, 장기적으로는 '징벌적 손해배상 제도' 도입 필요성을 고찰한다.

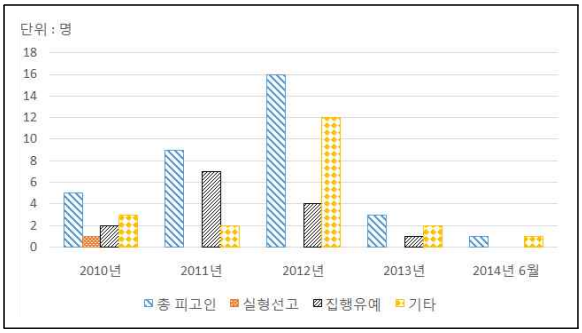
I. 서론

산업기밀보호센터[1]에 따르면, 우리나라 산업기술 해외유출 사건의 약 80%는 금전유혹과 개인이익을 위해 발생하고 있다. 2014년 7월 검찰[2]에서 발표한 '방위력개선 관련 군사기밀 대규모 해외유출사건' 피의자들도 금품과 향응을 제공받으며 군사기밀 수십 건을 유출하였다. 이와 같은 사건이 발생할 때마다 '군피아' 논란이 확산되며 우리 군에 대한 대국민 신뢰도는 추락하게 된다.

기밀이나 기술 유출 사고 상당수가 현금 제공, 향후 취업 약속 등 금전적인 문제와 직결되어 있다. 이는 기밀 유출로 인해 본인이 얻을 수 있는 이익이 적발되었을 때 감수해야 할 손해보다 훨씬 크기 때문이다.

'군사기밀'이란 일반인에게 알려지지 아니한 것으로서 그 내용이 누설되면 국가안전보장에 명백한 위험을 초래할 우려가 있는 군 관련 문서, 도화, 특수매체기록 또는 물건[3]으로, 군에서는 다양한 보안대책을 적용하여 이를 보호하는데 만전을 기하고 있으며, 유출시 군사기밀보호법에서 정한 바에 따라 처벌을 받도록 하고 있다.

그러나, 국방부[4]가 2014년 8월 국회 법제사법위원회 소속 홍일표 의원에게 제출한 자료에 의하면 [그림 1]과 같이 최근 5년 간 총 33명이 군사기밀을 유출하였지만 실형 선고를 받은 사람은 단 1명에 불과하고, 대부분 집행유예 이하의 처분을 받았다. 벌금형의 경우에도 유사 분야인 산업기밀 유출시 벌금보다 현저하게 낮다.



[그림 1] 최근 5년 간 군사기밀 유출자 사법처리 현황

특히 군사기밀 유출시 국가안보에 미치는 악영향이 환산할 수 없을 정도로 막대함에도 불구하고 손해배상 청구에 대한 근거가 미약하고, 손해배상을 청구한 사례도 전혀 없어 군사기밀 유출 차단 효과에 대한 실효성이 낮다.

이에, 본고에서는 실제 기밀유출 차단 효과를 높이기 위해 인간의 심리적인 특성을 활용하여 군사기밀보호법상 고의적으로 군사기밀을 유출한 자에 대해 손해배상 제도를 적용하는 방안을 강구하고자 하며, 장기적으로는 '징벌적 손해배상 제도' 도입 필요성까지 고찰해 보고자 한다.

군사기밀 유출사건이라는 국가안보에 관련된 대단히 중요한 보안사항이나, 모든 자료는 인터넷 등에 이미 공개된 내용만을 이용하여 고찰하였다.

II. 관련 내용

2.1 관련 사례(1)

(사례 1) 2011년 8월 전직 공군참모총장은 수수료 25억 원을 받고 미국 방산업체에 군사기밀을 유출[5]하였는데, 그동안 국가안보에 기여한 공로 등이 인정되어 '징역 10개월 / 집행유예 2년'을 선고받았다.

(사례 2) 2012년 2월 '국방중기계획' 등 군사기밀 유출 사건 당시 피의자들 역시 금품을 수수한 대가로 다수 군사기밀을 거래[6]하였는데, '누설을 통해 위협이 현실화되지 않았다[7]'는 이유로 형사처벌 대상에서 제외되었다.

(사례 3) 2014년 7월 '방위력개선 관련 군사기밀 대규모 해외유출사건'에서도 현역 군인 등이 금품과 향응을 수수하면서 국내·외 25개 업체에 총 31건의 군사기밀을 유출하였는데, 과거 선례에 비추어 볼 때 이들 피의자에게 징역형이나 고강도의 벌금형이 선고될 가능성은 높지 않은 것으로 판단된다.

이처럼 고의로 군사기밀을 유출한 피의자에 대해서도 형사처벌 수위가 대단히 낮아 군사기밀보호법의 효력에 대한 의문이 지속 제기되고 있다.

2.2 유사 분야 법률과 비교

군사기밀보호법의 한계를 인식하고 발전방안을 도출하기 위해, 민간 분야에서 유사한 부문의 관련 법률 특성을 고찰한다.

2.2.1 개인정보보호법

이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다[8].

이 법 제39조(손해배상책임)에서는 개인정보처리자의 위법행위로 인해 정보주체가 손해를 입으면 손해배상을 청구할 수 있도록 명문화되어 있다.

2.2.2 부정경쟁방지 및 영업비밀 보호에 관한 법률

이 법은 타인의 영업비밀을 침해하는 행위 등을 방지[9]하기 위하여 제정되었다.

이 법 제11조(영업비밀 침해에 대한 손해배상책임)에서는 고의 뿐 아니라 과실에 의한 영업비밀 침해행위에 대해서까지 손해배상 책임이 명문화되어 있다.

또한, 이 법 제18조(벌칙)를 통해 징역과 벌금을 동시에 부과할 수도 있는 특징이 있다.

2.2.3 산업기술의 유출방지 및 보호에 관한 법률

이 법은 산업기술의 부정한 유출을 방지하고 산업기술을 보호[10]하기 위해 제정되었다.

이 법 제36조(벌칙)에는 위법 행위자에 대해 최대 10억 원의 벌금에 처할 수 있고, 부정경쟁방지 및 영업비밀 보호에 관한 법률과 마찬가지로 징역과 벌금형을 동시에 부과할 수도 있다.

2.3 관련 연구 및 한계

이경호[11]는 산업기술 유출에 따른 피해금액을 산정하기 위한 모델을 연구하였으며, 장월수[12]는 군사비밀 유출에 따른 피해금액 산정 모델을 연구하였다. 하지만 연구의 결과물들이 해당 분야에서 피해금액 산정에 대한 공식적인 기준으로 활용되는데 한계가 있었고, 심리학적 특성을 바탕으로 해외 및 국내 유사 법률과 비교 분석하여 거시적인 관점에서 법률상 발전방안까지 도출한 연구는 다소 미비하였다.

III. 발전 방안

3.1 군사기밀보호법상 손해배상 관련 조항 신설

각종 정보유출을 차단하기 위해 다양한 수단을 이용할 수 있는데, 첨단 정보보호 기술 / 장비를 활용할 수 없는 분야는 인간의 기본적인 심리 특성을 이용한 제도와 정책을 적용하는 것이 효율적이다.

금전적 이익을 취하려는 공격자는 무엇을 어떻게 공격할지 결정하고 실제 공격에 성공한 후 이익을 얻는데[13], 심리학적으로 사람들은 그들이 얻을 수 있는 이익보다 손실에 대해 영향을 더 많이 받는다[14]. 또한, 손실과 이익을 불균형하게 인식하고, 의사결정 과정에서 이익보다 손실이 동기를 부여하는데 효과적이며, 이익이 더 클 경우에도 본인이 감수해야 할 손실을 더 나쁘게 (크게) 인식하는 경향이 있다[15].

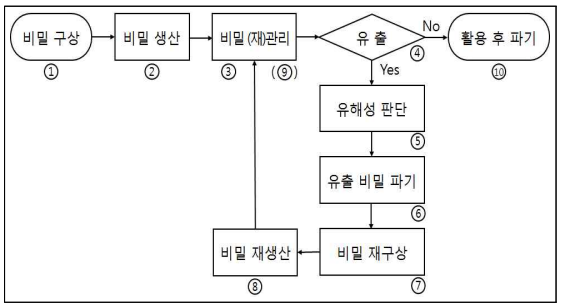
이런 심리학적 특성을 활용하여 고의적으로 군사기밀을 유출할 경우 공격자가 얻을 이익을 차단하고, 손실을 더 크게 느끼도록 해당 기밀 유출로 인해 국가가 입을 피해에 대해 손해배상 의무를 부과할 수 있도록 군사기밀보호법상 손해배상 관련 조항을 신설해야 한다.

3.2 군사기밀 유출시 피해규모 산정 방안 정립

현재 우리 국가에서는 군사기밀 유출시 피해규모 산정 방안을 정립하지 않았기 때문에 공신력 있는 피해규모를 확인할 수 없는 실정이다. 손해배상 소송을 제기하기 위해서는 최우선적으로 공신력 있는 피해규모를 산출할

(1) 검찰 발표일 기준

수 있어야 하며, 사회적 공감대가 형성될 수 있도록 민-관-군 합동으로 이에 대한 연구를 진행하는 것이 바람직하다.



[그림 2] 군사비밀의 life cycle

여기서 우리는 피해규모 산정에 대한 한 가지 방법론을 제시하기 위해 [그림 2]와 같이 군사비밀의 life cycle을 제시하였으며, 각 단계별 정의는 [표 1]과 같다.

[표 1] 단계별 정의

단계	정 의	비고
1	필요한 비밀을 생산하기 위해 최초 구상	
2	구상한 비밀을 실제 생산	
3	비밀을 업무에 활용 / 보관	
4	비밀 유출 여부 판단	○
5	유출된 비밀의 유해성 및 가치 정도 판단	○
6	유출된 비밀 파기	○
7	유출된 비밀을 대체할 수 있는 비밀을 다시 구상	○
8	재구상한 비밀을 생산	○
9	재생산한 비밀을 업무에 활용 / 보관	○
10	활용기간 만료 비밀 파기	

피해규모를 산정할 때는 평상시 비밀 생산 및 관리에 소요되는 고정비용을 제외하고, 실제 비밀이 유출되어 피해를 입은 단계(단계 4 ~ 단계 9)에서 소요되는 비용만을 합산하면 아래 수식 (1)과 같다.

$$C_t = C_4 + C_5 + \cdots + C_9 \quad (1)$$

C_t : 피해규모 총 비용
C_k : 단계 k에서 소요되는 (피해를 입은) 비용

각 단계에서는 최대한 객관성을 유지할 수 있도록 정량적으로 평가해야 한다. 그런데 유출된 비밀의 유해성 판단 단계(단계 5)에서 정량적 평가가 불가할 경우에 한해 정성적 평가를 고려해 볼 수 있다.

상기 모델을 적용하여 2014년 7월 '방위력개선 관련 군사기밀 대규모 해외유출 사건' 피해액을 계산해 보면, **총 피해규모(C_t)는 약 99.31억 원**이다. 세부 계산내역은 [표 2]와 같다. 이 피의자들은 1천만 원 상당의 금품과 액수불상 향응을 제공받고[2] 총 100억 원의 가치가 있는 군사기밀을 유출하였다.

[표 2] 단계별 소요되는 (피해를 입은) 비용[(2)]

단계	비 용	상세 내역	비고
4	800만원	조사인건비 400만원, 경비 300만원, 간접비 100만원	
5	90억원 (정성적 추정값)	비밀 등급/내용별 실제 가치 50억원, 국가신뢰도 하락 20억원, 전력화 차질 등 국가안보에 미치는 영향 20억원	
6	100만원	파기 과정 인건비 100만원	
7	2억 500만원	자료 수집 1,500만원, 자체 연구 9,000만원, 외부 연구용역 1억원	
8	6억 7,500만원	인건비 6.75억원, 재료비 42만원	
9	4,200만원	물리적 장비/공간 구비 및 유지 100만원, 인건비 1,400만원, 비밀보호훈련 1,100만원, 보안점검 1,600만원	

3.3 기밀 유출 사고 발생시 민사소송 제기

군사기밀 유출 사고가 발생되면 현재는 국가에서 형사소송만을 진행하고 있다. 하지만 군사기밀보호법상 손해보상 관련 조항을 신설하고 적절한 피해규모 산정 방안이 정립되면 우리 국가가 입은 피해나 앞으로 입게 될 피해를 정확히 산출하고 이를 토대로 피의자에게 민사소송을 제기하여 국가 차원에서 피해보상을 받도록 해야 한다.

3.4 군사기밀보호법상 벌금 상향 등 처벌 강화

일본은 2013년 12월 '특정비밀보호법'을 제정하여 국가 안전보장과 관련된 기밀 유출자에게 최고 10년 이하의 징역형을 부과[16]하는 등 국가기밀 유출을 방지하기 위해 관련 법률을 강화하고 있다.

우리나라에서 최근 잇따라 발생한 정보유출 사고에 대해 최성준 방송통신위원장은 '개인정보보호법상 과징금 최대한도가 1억 원이라는데 한계가 있으며, 과징금을 강화해야 한다는 의견에 동의한다[17]'고 밝혔다.

산업기술 유출시 최고 10년 이하의 징역 또는 10억 원의 벌금을 부과할 수 있고, 징역과 벌금을 병과할 수 있는 등 선진국 사례 및 우리나라 유사 법률을 참고하여 군사기밀을 유출한 자에 대한 형사처벌 수위를 현행 최고 징역형 7년 / 벌금형 5천만 원보다 높게 조정해야 한다.

3.5 징벌적 손해배상 제도 도입 검토

징벌적 손해배상 제도는 민사상 범죄에 대해 실제 손해액 이상의 손해배상 책임을 부과하여 경각심을 일깨워주는 제도로, 우리나라에서는 대기업의 불공정거래 근절 및 안전사고 재발 방지 관련 분야에서 본 제도 도입을 검토해야 한다는 주장 등으로 인해 널리 알려지게 되었다.

선진국에서는 다양한 분야에서 징벌적 손해배상 제도를 적용하고 있으며, 미국에서는 처벌을

(2) 2급 비밀 1건에 대한 계산값으로, 유출된 비밀이 여러 건일 경우 산정방법은 추가로 검토해야 한다.

통한 억지 기능을 가진 효과적인 구제수단으로 인식[18]되고 있다.

우리나라에서는 현재까지 징벌적 손해배상이 입법화되지 않았으나, '도입을 검토해 볼 수 있는 시기가 되었다[19]'고 보는 이들도 상당수 존재하는 등 여론이 성숙되어 가는 단계이다.

장기적으로 고의적 군사기밀 유출자에 대해 징벌적 손해배상 제도 적용 여부를 판단할 때, 피의자가 형사처벌을 받은 정도를 감안하여 손해배상액을 산정해야 한다.

IV. 기대 효과

- 군사기밀 유출사고 감소 / 사회적 비용 절감

  고의적 군사기밀 유출자에 대해 제도적으로 (징벌적) 손해배상을 청구할 수 있고, 실제 청구하게 된다면 배상액 규모가 크지 않더라도 다양한 원인에 의해 발생하는 기밀 유출 사고를 상당 부분 감소시킬 수 있고, 이에 따른 사회적 비용 역시 절감할 수 있다.

- 국가안보 기여 및 대국민 신뢰도 향상

  심리적 예방 효과 및 실질적 손해배상 청구를 통해 군사기밀 유출을 예방할 경우 국가안보에 기여하고 국방보안 수준 향상에 크게 공헌할 수 있다.

  또한, 군사기밀이 유출될 때마다 국민들이 불안해하고 군에 대해 부정적 인식이 팽배해지는 경향도 국방보안 수준이 향상됨에 따라 자연스럽게 해결될 수 있다.

- 손해배상 이익은 보안 관련 분야에 재투자

  (징벌적) 손해배상으로 얻는 이익은 해당 기밀을 재생산하고 관리하는데 사용하거나, 기타 군 관련 보안 분야 발전에 활용한다면 우리 군의 보안업무 수행 체계 및 보안수준을 더욱 향상시킬 수 있을 것이다.

V. 결론 및 향후 연구

군사기밀 유출의 주요 원인은 금전적 대가, 대인관계, 스파이 활동 등 다양하다. 우리는 본 연구에서 금전적 대가를 통한 기밀 유출 사례를 주로 살펴보았는데, 고의적 군사기밀 유출자에 대해 (징벌적) 손해배상을 청구하게 되면 다양한 원인에 의해 발생하는 기밀 유출을 차단하는데 효과가 클 것으로 판단된다.

또한, 군사기밀을 취급하는 다수 인원들에게 경각심이 고취되어 실수에 의한 기밀 유출도 줄어들 것이라고 예측해 볼 수 있다. 이를 통해 군피아 논란 등으로 인해 추락한 대군 신뢰도 역시 자연스럽게 향상되고, 국방보안 관련 분야의 지속적인 발전이 가능할 것이다.

본고에서 기술한 방법론은 여러 접근 방법 중 한 가지 예를 제시한 것이며, 피해금액 산정에 신뢰성을 기하기 위해서는 전문 연구기관에 의한 심층 연구가 수행되어야 하고, 사회 각계각층의 의견을 수렴하는 등의 절차를 반드시 거쳐야 한다.

앞으로 국가(군사)기밀을 보호하기 위한 다양한 법률 및 정책들 간 문제점과 발전방안에 대해 연구를 진행할 것이며, security economics 차원에서 해외 사례를 참고하여 군사기밀 유출 관련 사회적 비용을 정확히 판단하는 연구가 필요하다.

또한, '방어자가 모든 공격을 방어해야 한다는 것은 가능하지도 않고 필요하지도 않다[13]'는 관점에서 비용 대비 효과적인 보안업무 수행 시스템에 대한 연구도 추진되어야 할 것이다.

[참고문헌]

[1] 산업기밀보호센터, "http://service12.nis.go.kr/servlet/page?cmd=preservation&cd_code=outflow_1&menu=AAA00#.VD47J01xlZQ"

[2] 대검찰청, "http://www.spo.go.kr/seoul/notice/notice/notice01.jsp?mode=view&board_no=116&article_no=579011," July 2014.

[3] 군사기밀보호법, 법률 제12556호, 2014.5.9.

[4] 뉴시스, "http://www.newsis.com/ar_detail/view.html?ar_id=NISX20140820_0013119720&cID=10301&pID=10300," Oct. 2014.

[5] MBC, "http://imnews.imbc.com/replay/2011/nw1200/article/2899994_13044.html," Oct. 2011.

[6] 문화일보, "http://www.munhwa.com/news/view.html?no=2012020301070927182004," Mar. 2014.

[7] 내일신문, "http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=086&aid=0002139442," Dec. 2012.

[8] 개인정보보호법, 법률 제11990호, 2013.8.6.

[9] 부정경쟁방지 및 영업비밀 보호에 관한 법률, 법률 제11963호, 2013.7.30.

[10] 산업기술의 유출방지 및 보호에 관한 법률, 법률 제11690호, 2013.3.23.

[11] 이경호, "기술유출 사고로 인한 피해금액 산정을 위한 모델 연구," 고려대학교 박사학위논문, 2009.

[12] 장월수, "군사비밀 유출에 따른 피해금액 산정을 위한 모델 연구," 고려대학교 박사학위논문, 2012.

[13] C. Herley, "Security, cybercrime, and scale," *Communications of the ACM*, 57(9), pp. 64-71, Sep. 2014.

[14] M.E. Zurko and R.T. Simon, "User-centered security," *Proceedings of the 1996 workshop on New security paradigms. ACM*, New York, pp. 27 - 33, Sep. 1996.

[15] R. West, "The psychology of security : why do good users make bad decisions?," *Communications of the ACM*, 51(4), pp. 34-40, Apr. 2008.

[16] 국회도서관 법률정보실, "입법현안 법률정보," 20호, pp. 1-68, Mar. 2014.

[17] 디지털타임즈, "http://www.dt.co.kr/contents.html?article_no=2014101402109960800006," Oct. 2014.

[18] 김현수, "미국법상 징벌적 손해배상," 재산법연구, 29(2), pp. 325-355, 2012.

[19] 법제처 세계법제정보센터, "징벌적 손해배상 연구," Dec. 2012.