석사 학위논문
Master's Thesis

# 국가기밀의 금전적 가치평가 방법론

A Scheme on Monetary Evaluation of State Secrets

박 준 정 (朴 准 廷 Park, Joon-Jeong)
정보보호대학원
Graduate School of Information Security

**KAIST**

2016

# 국가기밀의 금전적 가치평가 방법론

A Scheme on Monetary Evaluation of State Secrets

# A Scheme on Monetary Evaluation of State Secrets

Advisor : Professor Kim, Kwangjo

by

Park, Joon-Jeong
Graduate School of Information Security
KAIST

A thesis submitted to the faculty of KAIST in partial fulfillment of the requirements for the degree of Master of Science and Engineering in the Graduate School of Information Security. The study was conducted in accordance with Code of Research Ethics*.

2015. 12. 2.

Approved by

Professor Kim, Kwangjo _____

[Advisor]

---

* Declaration of Ethical Conduct in Research: I, as a graduate student of KAIST, hereby declare that I have not committed any acts that may damage the credibility of my research. These include, but are not limited to: falsification, thesis written by someone else, distortion of research findings or plagiarism. I affirm that my thesis contains honest conclusions based on my own careful research under the guidance of my thesis advisor.

# 국가기밀의 금전적 가치평가 방법론

박 준 정

위 논문은 한국과학기술원 석사학위논문으로
학위논문심사위원회에서 심사 통과하였음.

2015 년 12 월 2 일

심사위원장 김 광 조 (인)

심사위원 김 명 철 (인)

심사위원 임 채 호 (인)

MIS
20143825

박 준 정. Park, Joon-Jeong. A Scheme on Monetary Evaluation of State Secrets. 국가기밀의 금전적 가치평가 방법론 Graduate School of Information Security. 2016. 38 p. Advisor Prof. Kim, Kwangjo

**ABSTRACT**

The term "State Secrets" is limited to the facts, goods, or knowledge classified as state secrets, the access to which is permitted to a limited scope of persons in order to avoid any serious disadvantage to the national safety. Despite state secret leakages can have devastating effects for the country, they occur continuously and are perceived as social issues.

This paper suggested the factors of leaking state secrets by analyzing secret leakage cases and presented those factors as ‘The secret leakage triangle model’ derived from ‘The fraud triangle model’ used in the field of criminal psychology.

Based on this model, we propose a methodology to assess the monetary values of state secrets in order to reduce the possibility of secret leakage at the maximum. This scheme establishes different evaluation models depending on the monetary characteristics of secrets and provides 3 specific application scenarios to evaluate the pros and cons of our approach.

Keywords: The Secret Leakage Triangle, Monetary Evaluation, State Secrets

# 목 차

# 표 목 차

# 그 림 목 차

# 제 1 장 서 론

## 1.1 연구 배경

대한민국은 지구상 유일한 분단국가로서 '국가안보'는 모든 국민들의 관심사이자 생존을 위한 가장 기본적인 조건이다. 국민들이 행복한 삶을 영위할 수 있도록 국가 차원에서 안보 역량 향상을 위해 다양한 노력을 기울이고 있다. 하지만 역설적으로 국가안보 최일선에 있는 군에서 군사기밀 유출 사고가 지속적으로 발생하여 안보에 위협요소로 작용하고 있는 것도 사실이다.

산업기밀보호센터에 따르면, 우리나라 산업기술 해외유출 사건의 약 80%는 금전유혹과 개인이익을 위해 발생하고 있다[1]. 2014년 7월 검찰에서 발표한 '방위력개선 관련 군사기밀 대규모 해외유출사건' 피의자들도 금품과 향응을 제공받으며 군사기밀 수십 건을 유출하였다[2]. 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. 특히 국가(군사)기밀 유출시 국가안보에 미치는 악영향이 환산할 수 없을 정도로 막대함에도 불구하고 손해배상 청구에 대한 근거가 미약하고, 손해배상을 청구한 사례도 전혀 없어 국가(군사)기밀 유출 차단 효과에 대한 실효성이 낮다.

한편, 한국산업기술보호협회에서는 우리나라 기술유출 피해액을 연간 약 50조 원으로 추정하고 있는데 이는 우리나라 국내총생산의 3% 수준이며, 중소기업 4,700여 개의 연평균 매출액에 해당하는 금액이라고 발표[3]하는 등 일반 국민들이 체감할 수 있는 구체적인 수치를 제시하고 있는데 반해, 국가기밀의 경우 금전적 가치나 피해규모를 막연한 개념으로만 제시할 뿐 구체적인 데이터로 나타내지 못해 국민들의 관심에서 쉽게 잊혀진다.

국가기밀 유출 사고에 영향을 미치는 요인을 분석하고, 금전적 가치평가 방법론을 정립하여 기밀 유출사건 발생시 신뢰성 있는 피해금액을 제시한다면 국가기밀 유출 사고의 주요 원인에 대한 현실적인 대책을 마련할 수 있다. 또한 불법행위로 인해 발생할 이익을 회수할 수 있을 뿐 아니라 국민들의 관심과 경각심 고취도 가능할 것으로 판단되어, 궁극적으로 국가기밀 유출 사고를 줄이는데 기여할 수 있을 것이다.

## 1.2 연구 목적 및 범위

각종 정보나 기밀 등의 유출을 차단하기 위해 다양한 수단을 이용할 수 있는데, 첨단 정보보호 기술·장비를 활용할 수 없는 분야는 인간의 기본적인 심리 특성을 이용한 제도와 정책을

적용해야 한다. 금전적 이익을 취하려는 공격자는 무엇을 어떻게 공격할지 결정하고 실제 공격에 성공한 후 이익을 얻는데[4], 심리학적으로 사람들은 그들이 얻을 수 있는 이익보다 손실에 대해 영향을 더 많이 받는다[5]. 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[6]. 이런 심리학적 특성을 활용하여 기밀 유출 피의자가 얻을 수 이익을 차단하고, 손실을 더 크게 느낄 수 있는 정책을 개발하는데 본 연구의 목적이 있다. 국가기관에서 발생 가능성이 높은 보안사고자 행위 요인을 행동 심리학적 관점에서 모델링하는 한편, 그에 따른 보안정책 방향을 설정하고 보안대책을 수립하는 것을 궁극적인 목표로 한다.

국가기밀을 보호하기 위해 다양한 정책과 제도 등이 적용되고 있는데, 기밀의 가치를 금전적으로 환산하여 활용하려는 노력은 다소 부족한 실정이다. 따라서 본고에서는 상기 목적을 달성하기 위해 '국가기밀 가치평가 방법론'을 정립하여 기밀의 금전적 가치를 평가하고, 이를 바탕으로 기밀 유출자에 대한 손해배상 적용 방안 등 제재 수단을 도입할 수 있는 이론적 근거를 제시하고자 한다. 금전적 목적으로 발생하는 기밀 유출 사고를 감소시켜 국가기밀 보호 수단을 추가할 수 있는데 의미가 있으며, 큰 틀에서 국가안보를 강화하는데 일조할 수 있으리라 판단된다.

이를 위해 본고에서는 국가기밀의 일부인 군사기밀의 예를 들어 국가기밀의 금전적 가치평가 모델을 정립한다. 군사기밀의 가치를 평가하기 위해 이익 창출 여부에 따라 군사기밀을 크게 2가지 범주로 구분한다. 군사기밀 중 이익을 창출할 수 있는 방위산업 관련 기밀(이하 '방산기밀')과 방산기밀에 해당하지 않는 군사기밀(이하 '일반 군사기밀')로 구분하여 서로 상이한 가치평가 방법론을 적용한다.

기밀은 내용에 따라 Ⅰ급·Ⅱ급·Ⅲ급으로 나눌 수 있는데, 본고에서는 1) 기밀의 내용 자체의 정성적 가치에 대한 평가가 현실적으로 불가한 점, 2) Ⅰ급 기밀은 극히 소수로서 유출된 전례가 전혀 없는 점, 3) Ⅱ급 기밀과 Ⅲ급 기밀의 차이점이 불분명한 점 등을 종합적으로 고려하여 연구 범위를 Ⅱ급 기밀로 한정한다.

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

## 1.3 논문의 구성

제 2장에서는 부정행위에 영향을 미치는 요인, 무형자산의 가치평가이론 및 주요 용어 등 본고 전체의 내용을 이해하는데 필요한 배경 지식에 대해 살펴본다. 제 3장에서는 기밀 유출로 인해 문제가 발생한 사례와 동향을 제시하고, 다양한 분야에서 이미 진행된 연구에 대해 고찰한다. 제 4장에서는 기밀 유출에 영향을 미치는 요인과 각 요소의 관계 등 기밀 유출 판단 과정을 분석한다.

제 5장에서는 금전적 측면에서의 대책을 마련하기 위해 가장 핵심적인 기밀의 가치평가 모델을 제안한다. 제 6장에서는 3개의 시나리오에 대해 앞 장에서 제안한 가치평가 모델과 기존 유사 분야 연구에서 제안된 모델을 적용하여 가치평가를 시행한 후 결과를 비교 분석한다.

제 7장에서는 기밀의 가치평가 모델을 활용할 수 있는 방안과 그에 따른 기대 효과를 제시하며, 마지막 제 8장에서는 결론을 맺는다.

# 제 2 장 배경 지식

## 2.1 부정행위에 영향을 미치는 요인

기밀 유출 사고에 영향을 미치는 요인을 도출해 보기 위해 일반적인 사람들이 부정행위를 자행할 때 영향을 미치는 요인에 대한 이론을 참고해 볼 수 있다. 이에 관해 다양한 이론이 있지만, 본고에서는 대표적인 두 가지 이론에 대해서 고찰해 본다.

### 2.1.1. 부정 삼각형(The Fraud Triangle)

저명한 범죄학자 Donald R. Cressy는 1972년 본인의 저서에서 다년간의 경험과 사례연구를 통해 금전적 부정행위가 발생하는데 영향을 미치는 요인을 3가지로 정리하여 그림 2.1과 같이 제시[7]하였으며, 세부 내용은 다음과 같다.

- 동기(Motivation or Pressure) : 범죄자가 최초에 본인의 부정행위 실행 여부를 동기화할 때 영향을 미치는 것
  (예 : 금전적 문제, 개인적 습관, 미래에 대한 불안감 등)
- 기회(Opportunity) : 어떤 조직 및 시스템의 취약점으로, 범죄자가 부정행위를 저지르는데 이용할 수 있는 것
  (예 : 불충분한 내부통제, 부정행위에 대한 관대한 인식 등)
- 자기 합리화(Rationalization) : 범죄자가 본인의 부정행위를 정당화하는 것으로, 부정행위를 자행한 원인이 본인이 아닌 다른 부분에 있거나 부정행위를 저지를 수밖에 없는 상황이었다고 스스로 판단하는 것
  (예 : 불공정한 인사 관행, 실제 피해를 입은 사람이 없을 것이라는 착각 등)

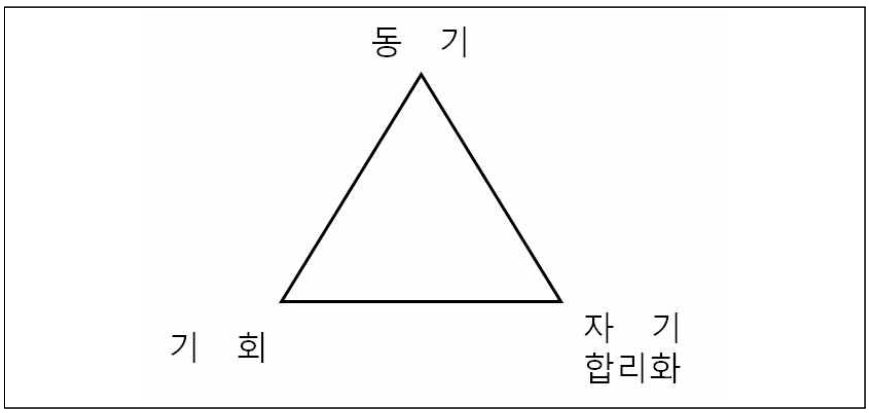

그림 2.1 부정 삼각형의 구성 요소

### 2.1.2. 부정 다이아몬드(The Fraud Diamond)

David T. Wolfe와 Dana R. Hermanson은 2004년 부정행위에 영향을 미치는 요인으로 그림 2.2와 같이 '부정 다이아몬드' 모형을 제시[8]하였는데, 상기 부정 삼각형에 '역량' 요인을 추가한 것으로 볼 수 있다.

- 인센티브(Incentive) : 부정행위를 저지르기 원하거나 해야 할 필요가 있는 것
- 기회(Opportunity) : 보통 사람이 이용할 수 있는 시스템 상의 취약점으로 부정행위에 활용 가능한 것
- 자기 합리화(Rationalization): 부정행위가 위험을 감수할 가치가 있다고 본인 스스로 확신하는 것
- 역량(Capability) : 보통의 사람이 목표한 무엇인가를 이끌어 내는데 필요한 특성이나 능력으로, 부정행위에 대한 기회가 있는 상태에서 실제 그 행위를 현실화할 수 있는 것

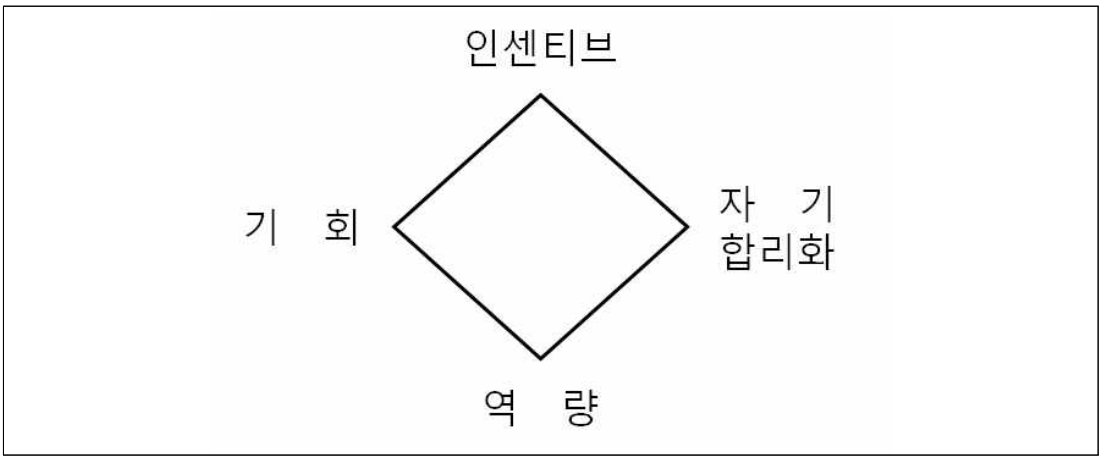


그림 2.2 부정 다이아몬드의 구성 요소

## 2.2 무형자산의 가치평가이론

본고에서는 '무형자산의 가치평가이론'을 적용하여 군사기밀의 가치평가 모델을 정립하였다. '무형자산'이란 물질적인 실체를 가지지 않고 보유자에게 권리와 특전을 부여하면서 경영과는 불가분의 관계에 있는 것으로 미래 어느 때에, 어느 정도의 가치를 가질 것인가를 정확히 파악한다는 것은 극히 어려운 일이라고 정의되어 있다. 금융자산과 유형자산 이외에 보유하고 있는 모든 자산이라고 정의할 수도 있다[9].

'무형자산의 가치평가이론'의 대표적인 3가지 분야인 원가접근법, 수익접근법, 시장접근법 적용 가능성을 검토하였으며, 군사기밀이 가지는 내재적 가치에 따라 분야를 달리하여 상이한 방법론을 활용하였다.

### 2.2.1. 원가접근법

원가접근법은 대상자산이 보유하는 미래의 서비스력과 동일한 서비스력을 얻기 위한 필요 금액을 산출함으로써 자산 보유자의 미래이익을 측정하는 방법이다[10].

평가대상 자산을 현재시점에서 재제조, 재획득하는데 소요되는 각종 제반 소요비용을 합하고 이에 감가수정을 가하여 평가대상 자산이 가치는 가치를 산정하여 평가하는 방법이다. 즉, 평가대상 자산의 가치는 새 자산을 구입, 개발하는 비용과 그 자산의 내용연수기간 중에 얻어지는 경제적 수익의 경제적 가치가 일치한다는 가정 하에서 평가대상이 실현하는 장래의 모든 경제적 수익의 재조달을 위하여 필요한 비용이다[9].

### 2.2.2. 수익접근법

수익접근법은 새로운 자산을 구축비용 또는 제조비용의 관점에서 벗어나, 자산의 수익력 분석에 초점을 맞추고 있는 계산방법이다. 수익접근법의 기본은 자산가치를 당해 자산의 내용기간 동안 거두는 순경제적 이익의 현재가치로 평가하는 것이다[10].

평가대상으로부터 발생되는 미래현금흐름의 현개자치의 합계로서 평가대상을 평가하는 방식이다. 즉, 평가대상을 소유 또는 운영함으로써 발생하는 추가적인 현금흐름을 추정하여 평가대상의 가치를 평가하는 방식으로, 미래지향적이며 이론적으로 가장 근본적인 가치산정 방식이다[9].

### 2.2.3. 시장접근법

시장접근법은 가장 직접적이고 이해가 쉬운 감정평가 방법으로, 시장에서 일어나고 있는 거래의 판단을 종합해서 미래이익에 대한 현재가치를 평가하는 것이다. 이러한 방법의 활용이 가능하게 되려면 다음 두 가지 요건이 만족되어야 한다. 1) 활발한 공개시장이 존재할 것, 2) 비교가능한 자산이 거래되고 있을 것 등이다[10].

가치평가에 있어 가장 먼저 시도될 수 있는 방법으로 거래하려는 대상과 유사한 거래사례를 찾아 이와 비교함으로써 시장가치를 추정하는 것이다. 하지만 유사한 사례가 존재하지 않으면 이 방식을 사용할 수 없기 때문에 본고에서는 적용하지 않았다.

## 2.3 국가기밀

### 2.3.1. 정의

‘비밀’이란 그 내용이 누설될 경우 국가안전보장에 해를 끼칠 우려가 있는 국가기밀로서 보안업무규정에 따라 비밀로 분류된 것을 말한다. 비밀은 그 중요성과 가치의 정도에 따라 표 2.1과 같이 Ⅰ급 비밀, Ⅱ급 비밀, Ⅲ급 비밀로 구분하며, 각급기관의 장의 책임 하에 비밀의 분

류・취급・유통 및 이관 등의 모든 과정에서 비밀이 누설되거나 유출되지 아니하도록 보안대책을 수립하여 시행하고 있다[11].

표 2.1 비밀의 구분

| 구 분 | 내 용 |
|---|---|
| Ⅰ급 | 누설될 경우 대한민국과 외교관계가 단절되고 전쟁을 일으키며, 국가의 방위계획・정보활동 및 국가방위에 반드시 필요한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 비밀 |
| Ⅱ급 | 누설될 경우 국가안전보장에 막대한 지장을 끼칠 우려가 있는 비밀 |
| Ⅲ급 | 누설될 경우 국가안전보장에 해를 끼칠 우려가 있는 비밀 |

‘국가기밀’이란 국가의 안전에 대한 중대한 불이익을 피하기 위하여 한정된 인원만이 알 수 있도록 허용되고 다른 국가 또는 집단에 대하여 비밀로 할 사실・물건 또는 지식으로서 국가기밀로 분류된 사항만을 말한다[12].

### 2.3.2. 생애주기(life cycle)

국가기밀은 기밀을 활용하는데 불편함을 최소화하면서도 해당 기밀을 가장 안전하게 보호할 수 있도록 최초 생산 단계에서부터 활용, 파기까지 어느 정도 정형화된 생애주기(life cycle)를 보이고 있으며, 이를 도식화해 보면 그림 2.3과 같다.

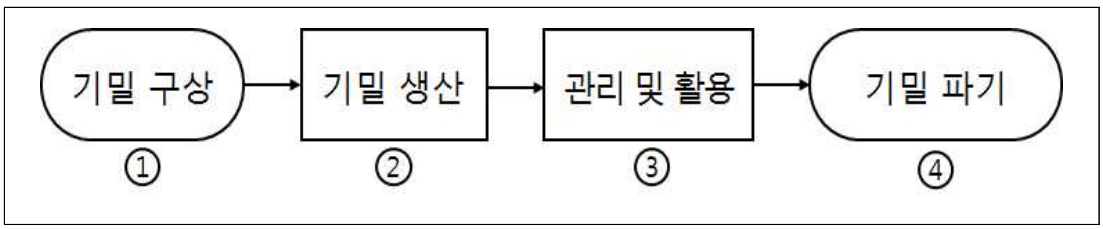


그림 2.3 기밀의 일반적인 생애주기

상기 각 단계별 정의는 아래와 같다.

- 단계 1 : 필요한 기밀을 생산하기 위해 최초 구상
- 단계 2 : 구상한 기밀을 실제 생산
- 단계 3 : 기밀을 업무에 활용하고, 안전하게 보관・관리
- 단계 4 : 활용기간이 만료된 비밀을 파기

### 2.3.3. 군사기밀

‘군사기밀’이란 일반인에게 알려지지 아니한 것으로서 그 내용이 누설되면 국가안전보장에 명백한 위험을 초래할 우려가 있는 군 관련 문서, 도화, 특수매체기록 또는 물건으로서 군사기

밀이라는 뜻이 표시 또는 고지되거나 보호에 필요한 조치가 이루어진 것과 그 내용을 말한다. 군사기밀은 그 내용이 누설되는 경우 국가안전보장에 미치는 영향의 정도에 따라 Ⅰ급 비밀, Ⅱ급 비밀, Ⅲ급 비밀로 등급을 구분한다. 군 및 관계 기관에서는 다양한 보안대책을 적용하여 이를 보호하는데 만전을 기하고 있으며, 유출시 군사기밀보호법에서 정한 바에 따라 처벌을 받도록 하고 있다[13].

군사기밀도 국가기밀의 일부로서 상기 그림 2.3과 같이 국가기밀의 생애주기와 동일한 양상을 지니고 있다. 본고에서는 기밀의 금전적 가치평가 모델을 수립하기 위해 일반적으로 수익을 창출할 수 있는지 여부에 따라 군사기밀을 크게 '방산기밀'과 방산기밀을 제외한 '일반 군사기밀'로 구분하였으며, 그림 2.4와 같이 표현할 수 있다.

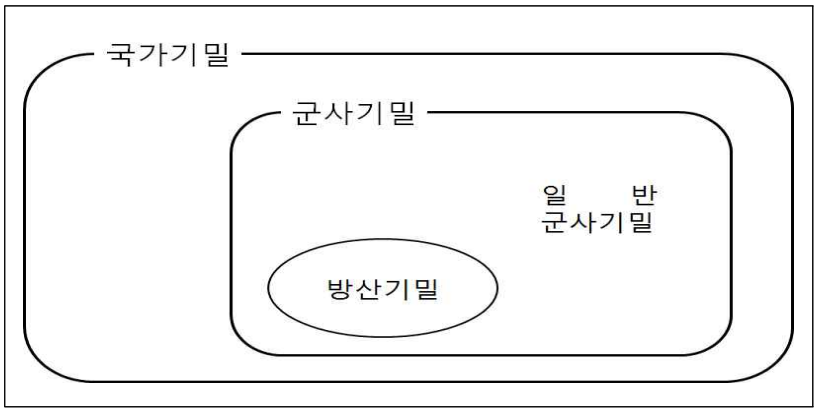

그림 2.4 국가기밀의 구분

#### 2.3.3.1 방산기밀

'방산기밀'이라는 용어는 법령 등에 명시되어 있지 않지만 군 및 방위산업 관련 기관 및 업체 등에서 통용되는 단어로, '방위산업물자를 연구·개발하거나 제조, 시험분석, 납품 또는 수출하는 과정에서 보호하여야 하는 군사기밀'로 해석해 볼 수 있다.

이러한 방산기밀은 군사기밀의 범주에 속하는 일부 기밀자료이지만, 관련 내용이 외부로 유출시 특정인들에게는 막대한 이익을 창출할 수 있는 독과점적인 데이터를 포함하는 특성이 있다. 따라서 방위산업 관계자들에 의해 다양한 수단을 통해 군 내부에 있는 방산기밀 자료가 불법적으로 유출되어 암암리에 활용될 가능성이 있다. 그림 2.5에서 보는 것처럼, 실제 국방부 검찰단에 정보공개를 청구하여 수령한 군사기밀 유출사건 총 8건 중 7건이 방산기밀을 유출[14]한 것이었다.

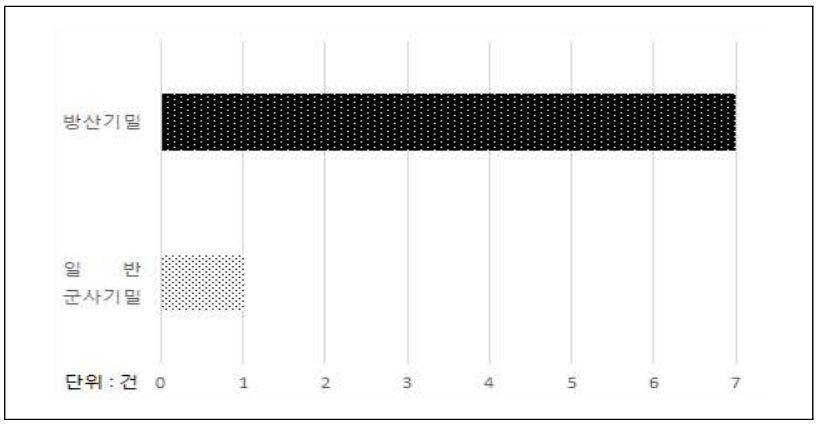

그림 2.5 기밀 유출사건 현황

#### 2.3.3.2 일반 군사기밀

‘일반 군사기밀’은 방산기밀을 제외한 군사기밀의 대부분에 해당하는 기밀로, 유출될 경우 국가안전보장 및 군사작전 등에 부정적인 영향을 미칠 수 있다. 특정 인원이나 단체에 이익을 창출할 수는 없으며, 내용 그 자체로서 보호되어야 할 가치를 지닌다. 군사기밀 보유현황 등은 외부로 공개되어 있지 않아 정확한 내용을 확인하기 곤란하다.

# 제 3 장 문제 사례 및 선행 연구

## 3.1 공개된 군사기밀 유출사건 동향

2011년 8월 전직 공군참모총장은 수수료 25억 원을 받고 미국 방산업체에 군사기밀을 유출하였는데, 그동안 국가안보에 기여한 공로 등이 인정되어 '징역 10개월 / 집행유예 2년'을 선고받았다[15].

2012년 2월 '국방중기계획' 등 군사기밀 유출 사건 당시 피의자들 역시 금품을 수수한 대가로 다수 군사기밀을 거래[16]하였는데, '누설을 통해 위협이 현실화되지 않았다[17]'는 이유로 형사처벌 대상에서 제외되었다.

2014년 7월 '방위력개선 관련 군사기밀 대규모 해외유출사건'에서도 현역 군인 등이 금품과 향응을 수수하면서 국내·외 25개 업체에 총 31건의 군사기밀을 유출하였는데[2], 과거 선례에 비추어 볼 때 이들 피의자에게 징역형이나 고강도의 벌금형이 선고될 가능성은 높지 않은 것으로 판단된다.

2015년 9월 북한의 포격도발 상황 관련 군사기밀을 인터넷 사이트에 게시한 인원은 형사처벌 대상에조차 포함되지 않고 감봉 1개월의 징계에 그쳤다[18].

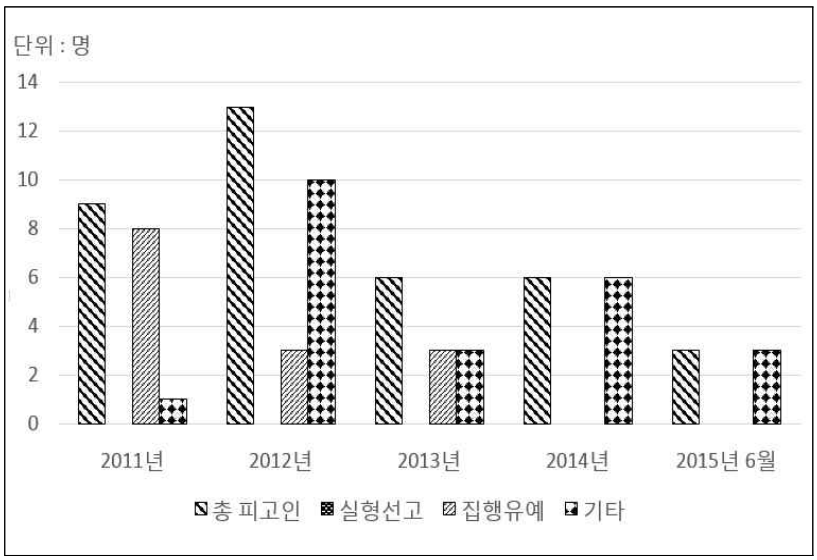


그림 3.1 최근 5년 간 군사기밀 유출사범 판결 결과

국방부가 2015년 9월 국회 법제사법위원회 소속 임내현 의원에게 제출한 자료[19]에 의하면 그림 3.1과 같이 최근 5년 간 총 37명이 군사기밀을 유출하였지만 실형 선고를 받은 사람은 단 한 명도 없고, 모두 집행유예 이하의 처분을 받았다. 벌금형의 경우에도 유사 분야인 산업기밀 유출시 벌금보다 현저하게 낮다.

2015년 3월 2일 정보공개 청구를 통해 국방부 검찰단으로부터 제공받은 최근 5년 간 군사기밀보호법 위반 사건 판결결과[14] 총 8건을 분석한 결과 역시 8건 모두 피고인에게 집행유예 혹은 선고유예가 선고되었다.

표 3.1 군사기밀보호법 위반 사건 판결 결과(정보공개 청구 자료)

| 사건번호 | 판결선고일 | 피고인 양형 결과 |
|---|---|---|
| 2010고20 | 2011. 3.16. | · 피고인 : 징역 2년 / 집행유예 4년 |
| 2011고15 | 2011.12. 2. | · 피고인 1 : 징역 2년 / 집행유예 3년<br>· 피고인 2 : 징역 1년 6월 / 집행유예 2년 |
| 2011고7 | 2011.12. 2. | · 피고인 : 선고유예 |
| 2011고17 | 2012.10.10. | · 피고인 : 징역 3년 / 집행유예 5년 |
| 2012고18 | 2012.10.19. | · 피고인 : 징역 10월 / 집행유예 2년 |
| 2012고29 | 2012.12.28. | · 피고인 1 : 징역 1년 / 집행유예 2년<br>· 피고인 2 : 징역 10월 / 집행유예 2년 |
| 2012고30-2 | 2013. 1.22. | · 피고인 : 선고유예 |
| 2012고34,26 | 2013. 3.25. | · 피고인 : 징역 3년 / 집행유예 5년 |
| 2014노111 | 2014.11.26. | · 피고인 1 : 징역 1년 6월 / 집행유예 3년<br>· 피고인 2 : 징역 3년 / 집행유예 5년 |

이처럼 악의적으로 군사기밀을 유출한 피의자에 대해서도 형사처벌 수위가 대단히 낮아 군사기밀보호법의 효력에 대한 의문이 지속 제기되고 있어 기밀 유출을 예방하기 위한 현실적인 대안을 마련해야 할 필요가 있다.

## 3.2 개인정보의 가치 분석

해외에서는 특정 경제학자와 보안 전문가들을 중심으로 정보보호에 대한 포괄적인 학제간 연구가 진행되고 있으며 이러한 연구로는 WEIS(Workshop on the Economics of Information Security)가 대표적[20]이다. 상기 학회에서 개인정보 관련 경제성 연구는 최근 개인정보 소유자가 본인의 개인정보에 대해 가지는 역설적 가치(Privacy Paradox)[21]에 대한 측면에 대한 연구가 비교적 활발히 진행되고 있는 것으로 판단된다.

웹 페이지 검색 과정에서 실험 참가자들의 태도를 바탕으로 그들이 개인정보를 얼마의 가치로 생각하느냐를 분석한 연구에서 개인정보 보호와 관련된 옵션을 선택한 사람은 79%였는데 그에 대한 금액을 지불하겠다는 사람은 15%에 불과한 역설적인 자세를 실험으로 증명하였다[22]. 또한, 인터넷 사용자들이 개인정보 보호에 높은 가치를 두고 있지만, 정작 본인의 개인정보를 보호하기 위해 지불하려는 가치가 상대적으로 낮은 이유를 경제학적 관점에서 실제 위험이 발생한 가능성이 지극히 낮기 때문이며, 이것이 Privacy Paradox가 발생하는 주요 원인임을 증명한 연구도 있다[23].

한편, 스마트폰 사용자들을 대상으로 비슷한 종류와 성능을 지닌 어플리케이션을 설치할 때 어느 어플리케이션에 더 많은 프리미엄을 제공하는지에 대한 실험도 진행되었다. 사용자들은 다른 조건이 비슷한 경우 개인정보에 접근하는 승인을 최소화하는 어플리케이션에 1.5달러의 프리미엄을 제공할 의사가 있다고 답변했다. 이를 통해 사용자들은 개인정보 보호에 상당한 관심이 있으며 개인정보를 비교적 안전하게 보호할 수 있을 것으로 판단되는 어플리케이션에 금전적 가치를 지불하는 경향이 확인되기도 했다[24].

사용자가 어떤 웹 사이트에 가입하려고 할 때는 해당 사이트에서 제공하는 웹 서식을 작성해야만 하며, 이는 개인정보를 수집하는 주요 수단이 된다. 웹 서식에서 의무적으로 작성해야 하는 필드를 정해 놓으면 통상 나머지 선택적 작성 필드는 공개하지 않는 경향이 있다. 하지만 의무적 작성 필드의 수가 클수록 금전적 보상을 크게 할 경우, 사용자들은 선택적 작성 필드 역시 더 많이 작성하는 경향이 있다는 사실도 확인되었으며, 이를 통해 개인정보를 더 많이 수집하기 위해 어떤 전략을 구사해야 하는지를 암시한 연구도 있다[25].

우리나라에서는 상기 분야에 대한 연구는 아직 진행되지 못하고 있는 실정이며, 개인정보가 유출될 경우 피해비용 산정에 관한 연구가 비교적 활발히 진행되고 있다.

### 3.2.1. 정량적 분석

정보보호 침해사고에 있어 투자 대비 효과의 관계에 대한 초기 연구[26]에서 최초로 피해액의 구조를 직접비용, 간접비용, 명시적 비용, 잠재적 비용 등으로 구분하여 제시되었다. 표 3.2는 Gordon-Loeb의 프레임워크의 해당 내용을 구체화[27]한 것으로, 본 분류 기준과 유사한 방법을 적용하여 개인정보 유출 관련 피해비용 연구가 다수 진행되었다.

표 3.2 Gordon-Loeb 프레임워크에 기초한 정보보호 침해사고 피해액 구조

<table>
<tr><th colspan="2">구 분</th><th colspan="2">명시적 비용</th><th>잠재적 비용</th></tr>
<tr><td rowspan="2">직접비용</td><td>기대이익<br>감소</td><td>매출이익<br>감소액</td><td>생산효율<br>저하손실</td><td rowspan="2">잠재적<br>책임비용</td></tr>
<tr><td>추가비용<br>발생</td><td>복구비용</td><td>복구불능<br>정보자산가치</td></tr>
<tr><td colspan="2">간접비용</td><td colspan="2">예방 투자액</td><td>이미지 손상<br>주가 하락</td></tr>
</table>

Gordon-Loeb의 프레임워크를 적용하여 개인정보가 유출되었을 경우 표 3.3과 같이 간접비용(4개 항목), 직접비용(6개 행목), 명시적 비용(6개 항목), 잠재적 비용(4개 항목)을 종합적으로 고려하여 유출된 개인정보의 가치를 계산하는 방법[28]이 연구가 되었다.

표 3.3 Gordon-Loeb 프레임워크를 적용한 개인정보의 가치 판단 고려요소

| | | | |
|---|---|---|---|
| 간접비용 | - 고객 신뢰도 측정비용<br>- 시스템 보완 및 교체비용<br>- 산업파급효과 | - 기업 이미지 손실 | |
| 직접비용 | - 브랜드 이미지 대응비용<br>- 사고 대응 인건비<br>- 고객 감소로 인한 매출 감소 | - 법적 비용<br>- 벌금 | - 보상받지 못한 개인의 정보가치 |
| 구 분 | 명시적 비용 | 잠재적 비용 | |

또한, 개인정보 유출사건이 발생했을 때의 피해를 직접피해(4개 항목)와 간접피해(7개 항목)로 구분하여 피해비용을 산출하는 방법[29]도 제안되었으며, 세부내용은 표 3.4와 같다.

표 3.4 개인정보 유출에 따른 직·간접 피해비용 산출시 고려요소

| 피해 구분 | 대상 | 항 목 | |
|---|---|---|---|
| 직접피해 | 개인 | - 보이스피싱, 파밍 피해액<br>- 보상받지 못한 개인정보 가치비용<br>- 유출방지를 위한 개인정보 예방비용<br>- 유출방지를 위한 보험금액 | |
| 간접피해 | 개인 | - 개인소송비용 | |
| | 기업 | 1차 | - 매출감소 |
| | | 2차 | - 법적 비용<br>- 개인정보유출로 인한 순영업비용<br>- 징벌적 과징금 |
| | | 3차 | - 보안예방 및 복구비용<br>- 산업 파급효과 |

### 3.2.2. 가상가치측정방법

가상가치측정방법(Contingent Valuation Methods, CVM)은 직접적으로 측정하기 어려운 공공재의 이용과 관련된 의사결정을 하여야 할 가상적인 상황을 설정하고 각 개인이 어떤 선택을 할 것인지를 설문조사를 통해 조사하여 그 가치를 평가하는 방법[30]이다. 어떤 공공재의 가치를 직접적으로 질문하여 답을 구하는 방법으로 해당 공공재를 수용하는데 있어서 지불할 수 있는 금액을 분석하는 지불의사가치(Willingness to Pay, WTP), 해당 공공재를 포기하는데 있어서 얼마의 보상이 적절한지 분석하는 수용의사가치(Willingness to Accept, WTA) 방법을 주로 활용한다.

개인의 지불의사가치(WTP) 수준을 조사하여 성별, 결혼 유무, 취업 여부, 나이, 교육 및 수입 등 다양한 요인에 따라 개인정보 보호를 위한 지불의사가치 결정에 영향을 미칠 수 있다는

연구[31]가 있었으며, 이름, 전화번호, 메일주소, 주민번호, 아이디 등 다양한 개인정보들을 그룹화 하여 각개 그룹이 유출될 경우 수용의사가치(WTA)를 추정하여 위자료 산정 모델을 수립해야 한다는 연구[32]도 진행됐다.

### 3.2.3. 기타

개인정보 유출에 따른 손해배상액 산정기준을 연구하면서 개인정보의 중요도(2개 항목), 개인정보 피해정보(3개 항목), 개인정보처리자의 과실(3개 항목)을 종합적으로 검토하여 가감 과정을 거쳐 손해배상액을 산정하는 모형이 표 3.5와 같이 제시[33]되기도 했다.

표 3.5 개인정보 유출시 손해배상(위자료) 판단을 위한 항목

| 구분 | 세부 항목 |
|---|---|
| 개인정보 중요도 | - 민감정보 포함 여부<br>- 개인식별성 여부 |
| 개인정보 피해정도 | - 피해기간<br>- 피해범위<br>- 정보노출 여부 |
| 개인정보처리자의 과실 | - 고의 여부<br>- 피해방지 활동 |

또한, 개인정보를 처리하는 기업에서 개인정보가 유출되었을 경우 표 3.6과 같이 피해자 및 가해자측 참작요소(반영정도)를 고려한 손해배상 책임의 필요성이 제안[34]되기도 했다.

표 3.6 개인정보 유출로 인한 손해배상시 피해자측 참작요소

| 항 목 | 내 용 | 반영정도 |
|---|---|---|
| 사회생활상 불이익 | 스팸문자, 스팸메일 등 사회생활상 불이익 발생 | +++ |
| | 사회생활상 불이익 미발생 | + |
| 후속손해 | 재산적 손해 발생<br>(손해액 입증 곤란) | +++ |
| | 재산적 손해 발생<br>(손해액 입증) | ++ |
| | 재산적 손해 미발생 | + |
| 피해자의 과실 | 피해자의 무과실 | 0 |
| | 피해자의 과실 | - |

### 3.3 산업기술 및 영업비밀 유출 피해비용 분석

일반 기업에서 기술유출 사고가 발생할 경우 기술의 경제적 수명 추정, 매출액 추정, 여유현금흐름 산출, 할인율, 기술기여도 추정 등의 과정을 통해 종합적으로 고려하여 해당 기술유출로 인한 피해금액을 산정할 수 있는 모델이 연구[35]됐다.

한편, 영업비밀 침해가 발생할 경우 이익액과 손해액을 산정함에 있어 해당 기밀 유출로 인한 실제손해를 기준으로 하면서, 불법행위를 한 자가 불공정하게 얻은 이익을 고려하는 방법을 취하는 미국 연방법원 양형기준 가이드라인[36]을 참고해야 한다는 주장도 있었다. 어떤 경우에는 산업기술을 재개발하는데 소요되는 비용을 손해배상액으로 판단하기도 하며, 이조차 불가할 경우는 연구개발비를 손해배상으로 볼 필요가 있다는 연구[37]도 진행됐다.

우리나라에서도 영업비밀이 유출되었을 경우 기본적으로 피해자가 얻은 이익을 손해로 추정하고, 손해액 입증이 곤란한 경우 법원 직권에 의해 손해배상액을 인정하는 것이 바람직하다는 의견도 제기[38]됐다.

### 3.4 군사기밀 유출 피해비용 분석

군사기밀 유출시 피해비용 관련 분야는 국내·외 연구자료가 거의 없으며, 선행연구 1건만 확인할 수 있었다. '국가안보에 미치는 악영향'을 군사기밀 유출시 입게 되는 피해 중 가장 큰 부분으로 설정하고, 군인들을 대상으로 설문조사를 시행하여 가상가치측정방법(CVM) 중 지불의사가치(WTP) 수준을 도출하였다. 이 값에 기밀 생산 비용 등을 포함하여 피해비용을 분석하는 모델이 제시됐다[39].

### 3.5 선행 연구의 한계

개인정보 유출, 사이버보안 침해사고, 산업기술 유출 피해비용 분석 등의 분야는 오랫동안 다양한 연구가 진행되었다. 하지만 군사기밀 관련 피해비용 산출 방법론은 단 1건이 제안되었으며, 더 큰 범주에서 국가기밀과 관련된 가치평가 방법론은 연구되지 않았기 때문에 사실상 국가기밀의 금전적 가치평가 방법론은 부재한 실정이다.

군사기밀 관련 연구 역시 기본적으로 각 개인이 실제로 행한 행위를 분석하여 가치를 평가하지 않고, 가상적인 상황을 만들어 개인이 행할 행위를 질문하는 방식을 취하기 때문에 매우 큰 오류를 범할 가능성이 있는 가상가치측정방법[30]을 적용하여 신뢰성에 한계가 있다.

정량적으로 평가할 수 없는 '군사기밀 내용의 가치'라는 정성적인 부분을 설문조사 결과만을 바탕으로 정책·정보 분야 기밀은 기본적으로 100억 원 이상, 방산기밀은 80억 원 이상, 작전기밀은 75억 원 이상 이상으로 일괄적으로 책정한 결과, 가치평가 비용이 지나치게 높아지게 되어 현실성이 부족하다. 실제로 설문조사 결과 역시 가장 많은 인원(36%)이 '군사비밀 내용의 가치를 금액으로 환산할 수 없다'고 답변하였음에도 불구하고, 해당 답변을 제외한 설문조사 결과를 그대로 활용하여 결과를 도출하였다.

또한, ‘개인정보의 잠재적 제공자에게 개인정보보호를 위한 지불의사를 직접적으로 설문하여 측정하는 것은 바람직하지 않다’는 관점[40]에서, 이 연구는 해당 기밀을 직접 취급하면서 잠재적 제공자가 될 수 있는 인원들을 대상으로 설문조사를 실시하여 객관성 확보 자체가 곤란하다는 단점이 있다.

# 제 4 장  기밀 유출 판단 과정

## 4.1 국방 보안 환경 및 기밀 유출 사고의 특성

군 부대 및 시설은 승인된 인원에 한해 출입이 가능하고 국방망은 외부 인터넷과 물리적으로 완전히 분리되어 있어[41] 외부인이 군 내부에 접근하기 극히 제한되는 고유한 특성을 보유하고 있다. 대단히 통제된 환경 하에서 발생한 기밀 유출 사고를 분석해 본 결과 '사람'이 가장 큰 보안 취약점이라는 사실을 확인할 수 있었다.

이 장에서는 이미 공개되어 있는 기밀 유출 사고 사례를 토대로 '기밀 유출 여부 판단 과정'을 전형적인 모델로 재정의 한다. 각 단계별 판단에 미치는 요소를 식별하고, 이 요인들이 보안사고와 연결되는 판단 및 행동에 어떤 영향을 미치는지에 대해 고찰한다.

## 4.2. 기밀 유출 사고 재구성을 통한 모델링

제 3장에서 살펴본 군사기밀 유출 사고 사례 중 가장 일반적이며 보편적 사례를 통해 모델링을 한다. '방위력 개선사업 관련 기밀 유출 사건'의 상황[2]을 정리해 보면 다음과 같다.

< 상 황 >

1. 방산업체 임원 A
   - 사업상 필요에 의해 기밀 수집 시도
2. 브로커 B
   - A로부터 기밀 불법 수집 제의 수락
   - 기밀을 취급하는 C에게 의도적으로 접근
3. 군 관계관 C
   - B로부터 기밀 유출 청탁 접수
   - 유출 여부에 대해 고민·판단

상기 상황에서 C가 기밀 유출 여부를 판단하는 과정을 단계로 구분하고, 각 단계별 진행 과정을 도식화 하면 그림 4.1과 같다.

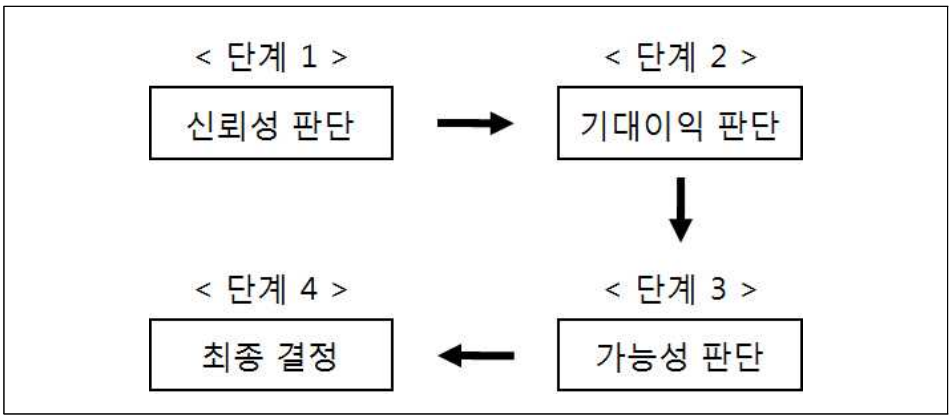

그림 4.1 기밀 유출 판단 과정

각 단계별로 C의 판단에 미치는 강화요인 및 처벌요인은 표 4.1과 같으며, 상황에 따라 기타 요인이 추가되거나 제외될 수 있다.

표 4.1 기밀 유출 판단 단계별 영향을 미치는 요인

| 단 계 | 강화요인 | 처벌요인 | 비고 |
|---|---|---|---|
| 1 | 브로커 신뢰성 | · | |
| 2 | 금전, 승급, 대인관계 | 타인의 의심, 처벌 강도, 조직 문화 | |
| 3 | 기밀 획득 용이성, 기밀 유출 용이성 | 예상되는 보안대책, 적발 가능성 | |
| 4 | · | · | 단계 1~3 종합판단 |

## 4.3. '기밀 유출 삼각형'과 각 요소의 관계

제 2장에서 고찰한 부정 삼각형과 같은 방식으로 기밀 유출 판단 과정을 도식화 하면 '기밀 유출 삼각형'을 도출할 수 있고, 이는 그림 4.2와 같다. 단계 1 ~ 3이 '기밀 유출 삼각형'의 세 가지 요소이며, 단계 4는 세 가지 요소를 종합적으로 판단하는 과정이다.

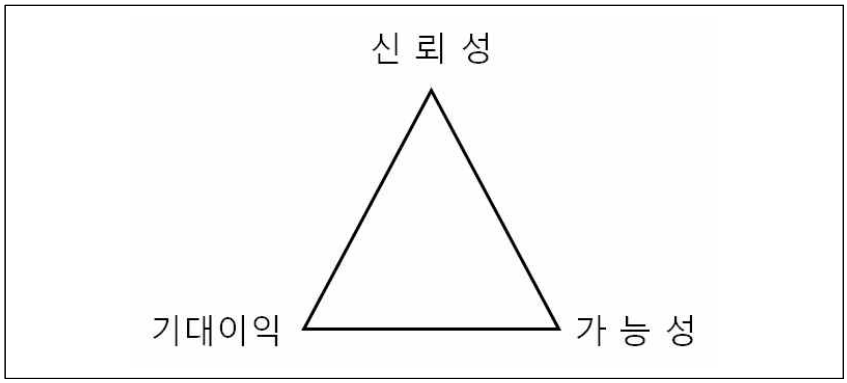

그림 4.2 기밀 유출 삼각형

일반적으로 군사학에서 ‘적의 위협도’를 판단할 때, 3가지 변수를 고려한다. 적이 아군을 공격하려는 생각 정도인 ‘적 의도’, 적이 아군을 공격할 수 있는 능력인 ‘적 역량’, 그리고 적의 공격에 대응할 수 있는 ‘아군 역량’이다. 이들의 관계를 간단히 다음 수식 (1)과 같이 표현할 수 있다.

$$\text{적의 위협도} \propto \frac{\text{적 의도} \times \text{적 역량}}{\text{아군 역량}} \tag{1}$$

적의 위협 수준을 판단하는 과정에서 착안하여 기밀 유출 판단 삼각형의 각 요소인 ‘신뢰성(Reliability, $r$)’, ‘기대이익(Expected profit, $e$)’, ‘가능성(Possibility, $p$)’과 ‘최종 판단(Final decision, $F$)’ 간의 관계를 수식 (2)와 같이 직관적으로 판단해 볼 수 있다.

$$F = \phi(r, e, p) \tag{2}$$

여기서 세 가지 변수 $r, e, p$는 $F$와 양의 상관관계를 갖는다. $F$값이 특정 임계값을 초과할 경우 기밀을 유출하기로 결정하게 되고, 반대의 경우는 기밀을 유출하지 않도록 결정한다. 신뢰성($r$), 기대이익($e$), 그리고 가능성($p$) 중에서 신뢰성은 개인적인 감정과 관련된 부분으로 어떤 대책을 도입한다고 해도 영향을 미칠 수 없다. 가능성은 조직에서 다양한 보안대책을 도입하는 것으로 낮출 수 있지만, 보안대책의 종류가 너무 많고 기밀 유출 사고에 있어 그 효과를 측정하는 것은 현실적으로 불가능하다.

따라서 본고에서는 ‘최종 판단($F$)’ 값을 낮추기 위해 ‘기대이익($e$)’을 낮추는 방향의 접근을 시도한다. 금전 이익, 승급 가능성, 대인관계 등 다양한 요인이 기대이익에 포함될 수 있다. 하지만 대부분의 기밀 유출 사고가 금전적 문제와 연관되어 있고, 현 시점에서 실제 계량화할 수 있는 항목은 ‘금전 이익’ 분야 밖에 없기 때문에 기밀 유출시 기대되는 금전적 이익을 최소화하는 정책이 필요하다.

이를 위해 평소에는 기밀취급자에게 국가기밀의 중요성을 실감할 수 있도록 하고, 기밀이 유출될 경우에는 손해배상 소송 등에 활용할 수 있도록 국가기밀의 금전적 가치평가 모델을 제안한다.

# 제 5 장 군사기밀 가치평가 모델

## 5.1 핵심 개념

기밀 유출자가 얻을 수 있는 금전적 이익을 최소화하기 위해 기밀의 금전적 가치 평가가 선행되어야 한다. 현재 국가(군사)기밀의 가치를 평가함에 있어서 가장 근본적인 문제는 가치평가를 위한 객관적이고 구체적인 자료를 제시할 수 있는지 여부이다. '국가안보에 미치는 악영향'과 같이 정량적으로 판단하기 현실적으로 불가한 항목까지 수치화하여 결과를 얻으려고 할 경우, 전체적인 연구의 신뢰성까지 보장할 수 없는 상황에 직면할 수 있다.

실제 군사기밀 유출 사건 판례에서도 '군사기밀 유출로 인해 실제 국익에 해를 끼치지 않았다'는 이유로 감형이 되고 있다[42]. 여기서 시사하는 바는, 기밀이 유출됐다는 이유만으로 금전적 피해가 발생한 것 자체만으로 피해(손해)액을 판단하는 것은 너무 과다하다고 느낄 수 있다. 따라서 실제 발생한 손해만으로 비용을 산정해야 할 필요가 있다. 그런데 이게 어려울 때는 기밀 유출자의 이익을 계산하여 피해로 판단하는 방법 밖에 없다.

따라서 본고에서는 정량적으로 판단할 수 있는 분야에 대해서는 정량적으로 판단하여 결과를 도출한다. 정성적인 가치로 평가할 수밖에 없는 분야에 대해서는 정성적 가치를 배제한 채 정량적인 결과만을 제시한다.

방산기밀의 가장 큰 특성이 '수익을 창출할 수 있다'는 측면에 착안하여 본고에서는 방산기밀 가치평가 간 '수익접근법'을 적용하여 방산기밀 유출자가 얻을 수 있는 이익을 해당 방산기밀에 내재된 가치로 평가한다. 특허, 기술, 상표, 브랜드, 저작권 등은 수익접근법에 의한 가치평가가 가장 적합하다[10]고 인식되는 것과 같은 논리이다.

일반 군사기밀은 방산기밀과 달리 '기본적으로는 수익을 창출하지 않는다'는 속성이 있어 본고에서는 일반 군사기밀 가치평가 간 '원가접근법'을 적용하였다. 경영정보, 업무관행 관련 자료 등은 원가(비용)접근법이 가장 적합하다[10]고 인식되는 것과 같은 맥락이다.

## 5.2. 방산기밀 평가 모델

방산기밀은 유출되어 특정 업체의 이익을 창출했다는 전제 하에 수익접근법을 적용하여 모델을 수립한다. 어느 업체의 수익 여부를 판단하기 위해서는 손익계산서를 필요로 한다. 표 5.1은 재무제표 중 손익계산서의 일반적인 샘플이다.

표 5.1 손익계산서 샘플 단위 : 원

| 과 목 | 당기 | | 전기 | |
|---|---|---|---|---|
| | 지출액 | 수입액 | 지출액 | 수입액 |
| Ⅰ. 매출액 | - | - | - | - |
| Ⅱ. 매출원가 | - | - | - | - |
| Ⅲ. 매출총이익 | - | - | - | - |
| Ⅳ. 판매비와 관리비 | - | - | - | - |
| Ⅴ. 영업이익(손실) | - | - | - | - |
| Ⅵ. 영업외수익 | - | - | - | - |
| Ⅶ. 영업외 비용 | - | - | - | - |
| Ⅷ. 법인세 차감전순이익 | - | - | - | - |
| Ⅸ. 법인세 등 | - | - | - | - |
| Ⅹ. 당기순이익 | - | - | - | - |

특정 기업의 이익 현황을 판단함에 있어 기업구조 및 사업특성 등 고려해야 할 요소가 대단히 많다. 고려해야 할 상황 등이 너무 복잡할 경우 기밀의 가치를 평가하는 모델 프레임워크 수립 자체가 불가하기 때문에, 본고에서는 통상의 무기중개업체에서 자주 발생하는 상황을 바탕으로 2가지 방법을 우선 제안한다. 이를 토대로 향후 다양한 경우에 대해서도 가치를 측정할 수 있는 모델을 발전시킬 수 있을 것으로 기대한다.

### 5.2.1. '당기' 손익계산서 활용 방법

무기중개업체 특성상 다양한 사업을 추진하기보다는 한 가지 사업에 집중하는 경향이 많다. 이러한 업체에서 특정 방산기밀을 통해 이익을 창출한 경우 당기 손익계산서를 활용하여 불법적으로 유통한 방산기밀의 가치를 간접적으로 평가해 볼 수 있다.

상기 손익계산서 각 항목의 계산 과정을 그림 5.1에서 살펴보자.

그림 5.1 손익계산서를 이용한 당기순이익 계산 과정

(Ⅲ. 매출총이익) = (Ⅰ. 매출액) - (Ⅱ. 매출원가)
(Ⅴ. 영업이익) = (Ⅲ. 매출총이익) - (Ⅳ. 판매비와 관리비)
(Ⅷ. 법인세 차감 전 순이익) = (Ⅴ. 영업이익) + (Ⅵ. 영업외 수익) - (Ⅶ. 영업외 비용)
(Ⅹ. 당기순이익) = (Ⅷ. 법인세 차감 전 순이익) - (Ⅸ. 법인세 등)

해당 업체의 1년 총 이윤은 당기순이익($I$) 항목이고 이 값에 방산기밀이 사업에 미치는 영향 추정값($\alpha$)과 해당 사업이 업체에서 차지하는 비중($\beta$)을 곱한 결과가 방산기밀의 금전적 가치이며, 이는 수식 (3)과 같다.

$$\text{기밀의 가치} = I \times \alpha \times \beta \quad (3)$$
$$(0 < \alpha \leq 1,\ 0 < \beta \leq 1)$$

수식 (3)에서 기밀의 금전적 가치에 영향을 미치는 변수는 '당기순이익', '방산기밀이 사업에 미치는 영향 추정값($a$)', 그리고 '해당 사업이 업체에서 차지하는 비중($\beta$)' 총 3가지이다. 손익계산서의 신뢰도가 높다는 가정 하에, 당기순이익과 $\beta$는 객관적이고 정확한 값을 산출하여 적용할 수 있다. 반면, $a$는 그 자체가 추정값이기 때문에 비교적 모호한 성격을 지니는데, 실제 적용할 때는 수사기관 등에서 전반적인 사업의 진행 경과를 분석하여 $a$값을 결정해야 한다. 본고에서는 $a$값을 판단하는 한 가지 예를 표 5.2에 제시한다.

표 5.2 $a$값 판단의 예

| 방산기밀이 사업에 미치는 영향 | $a$값의 범위 |
|---|---|
| 무조건 사업 수주 | $\alpha = 1$ |
| 절대적으로 유리 | $0.8 < \alpha < 1$ |
| 현저하게(뚜렷하게) 유리 | $0.5 < \alpha \leq 0.8$ |
| 상대적으로 유리 | $0.2 < \alpha \leq 0.5$ |
| 단순 참고 | $0 < \alpha \leq 0.2$ |

당기 손익계산서를 활용하여 방산기밀의 가치를 계산하는 방법의 장점은 손익계산서의 신뢰도가 높을 경우 대단히 정확한 결과를 확보할 수 있다. 반면, 불법적으로 획득한 이익을 손익계산서에 포함하지 않을 가능성이 높아 손익계산서의 신뢰도 확보 자체가 곤란할 수 있는 단점도 존재한다.

### 5.2.1. '전기 및 당기' 손익계산서 활용 방법

무기중개업체 특성상 다양한 사업을 추진하기보다는 한 가지 사업에 집중하는 경향이 많다. 이러한 업체에서 특정 방산기밀을 통해 이익을 창출한 경우 당기 손익계산서를 활용하여 불법적으로 유통한 방산기밀의 가치를 간접적으로 평가해 볼 수 있다.

전년도와 당해년도 매출을 비교할 수 있는 경우는 더욱 정확한 계산값을 추출할 수 있다. 당해년도 당기순이익에서 전년도 당기순이익을 뺀 값이 순이익 증가액($\Delta I$)이며, 이 값에 방산기밀이 사업에 미치는 영향 추정값($a$)과 해당 사업이 업체에서 차지하는 비중($\beta$)을 곱한 결과가 방산기밀의 금전적 가치이며, 이는 수식 (4)와 같다.

$$기밀가치 = \Delta I \times \alpha \times \beta \quad (4)$$

($\Delta I$ = 전년도 당기순이익 – 당해년도 당기순이익)

상기 계산 방법은 1년 이내로 추진되는 단기사업의 경우에 효과적인 반면, 전년도 사업에서 추가·변경된 사업의 수가 많지 않아야 적용할 수 있다는 단점도 있다.

## 5.3. 일반 군사기밀 평가 모델

일반 군사기밀의 가치를 평가할 때 '국가안보에 미치는 악영향'이 가장 큰 요인임을 부정할 수는 없지만, 이 부분이 정량적으로 측정할 수 없는 가치라는 사실도 부정할 수 없다. 따라서 '국가안보에 미치는 악영향'은 형사법적 조치로 상쇄시킬 수 있다는 전제 하에 일반 군사기밀의 가치는 원가접근법을 적용해서 계산하는 것이 바람직하다.

### 5.3.1. 원가접근법 적용 방법

원가접근법은 가치 평가 대상물을 현재 시점에서 재생산하는데 필요한 비용을 계산하는 방법이다. 이를 군사기밀 유출 사고에 적용한다면, 유출된 군사기밀을 다시 생산하는데 필요한 비용으로 볼 수 있다. 기밀이 유출된다면 그림 5.2와 같이 일반적인 생애주기와는 다른 양상을 보이게 된다.

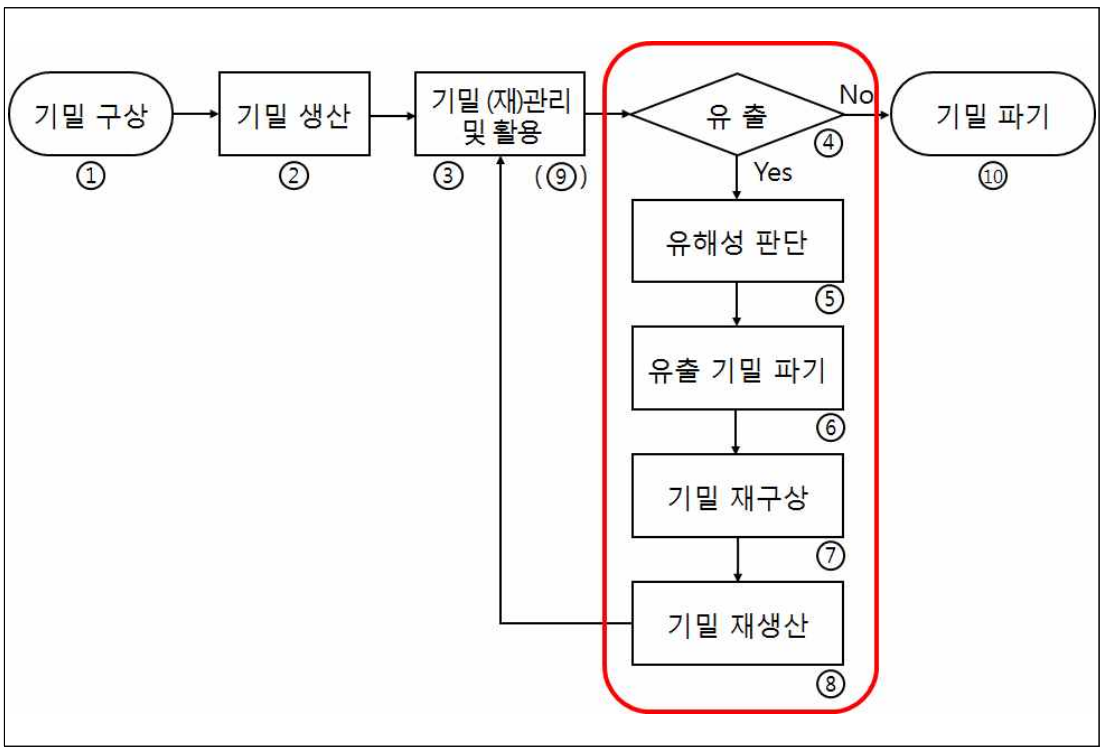


그림 5.2 유출된 기밀의 생애주기 및 유출로 인해 피해가 발생한 단계

상기 각 단계별 정의는 아래와 같다.

- 단계 1 : 필요한 기밀을 생산하기 위해 최초 구상
- 단계 2 : 구상한 기밀을 실제 생산
- 단계 3 : 기밀을 업무에 활용하고, 안전하게 보관·관리
- **단계 4 : 비밀 유출 여부 판단**
- **단계 5 : 유출된 비밀의 유해성 및 가치 정도 판단**
- **단계 6 : 유출된 비밀 파기**
- **단계 7 : 유출된 비밀을 대체할 수 있는 비밀을 다시 구상**
- **단계 8 : 재구상한 비밀을 생산**
- 단계 9 : 재생산한 비밀을 업무에 활용 / 보관 (단계 3과 동일)
- 단계 10 : 활용기간 만료 비밀 파기

기밀의 전 생애주기(단계 1 ~ 단계 10)에서 소요되는 비용을 계산하는 것이 아니라, 기밀 유출이 인지된 단계부터 해당 비밀을 다시 생산하는 단계(단계 4 ~ 8)에서 소요되는 비용만을 환산한다. 기밀이 유출된 상황에서만 단계 4 ~ 8에서 예산이 추가로 소요되며, 기밀이 유출되지 않았다면 본 단계 자체가 존재하지 않는다. 따라서 일반 군사기밀의 금전적 가치는 수식 (5)와 같이 계산된다.

$$\text{기밀의 가치} = C_4 + C_5 + \cdots + C_8 \qquad (5)$$

$$(C_k = \text{단계}\, k\text{에서 소요되는 비용})$$

단계별 피해비용 계산에 포함되어야 할 항목은 아래 표 5.3과 같다. 한 가지 유의할 사항은, 단계 5(유해성 판단)에서 해당 기밀이 국가안보에 미치는 악영향을 판단하게 되는데 이 부분은 정량적으로 환산할 수 없기 때문에 정성적인 가치로만 판단해야 하며, 유해성을 판단하기 위한 회의나 자문활동 등에 소요되는 비용만을 환산한다.

표 5.3 각 단계별 비용 산출 간 포함사항

| 단 계 | 단 계 명 | 비용 산출 간 포함사항 | 비 고 |
|---|---|---|---|
| 4 | 유출 | - 보안조사 인건비 - 보안조사 경비<br>- 보안조사 간접비 | |
| 5 | 유해성 판단 | - 회의비(자문) | |
| 6 | 유출 비밀 파기 | - 파기 과정 소요 인건비 | |
| 7 | 비밀 재구상 | - 자료 수집비 - 자체 연구비<br>- 외부 연구용역비 | |
| 8 | 비밀 재생산 | - 인건비 - 재료비 | |

## 5.4 추가 고려사항

### 5.4.1 방산기밀의 가격이 재생산원가보다 낮을 경우

해당 방위사업의 규모가 작거나 방산기밀이 사업에 미치는 영향 추정값($a$)이 작은 경우 등은 방산기밀의 가격이 재생산원가보다 더 적게 환산되는 문제가 발생할 수 있다. 이 경우 방산기밀이 창출한 가치와 재생산원가를 비교하여 더 큰 값을 취할 필요가 있다. 이는 수식 (6)과 같다.

$$\text{기밀의 가치} = \max((I \times \alpha \times \beta), (C_4 + C_5 + \cdots + C_8)) \quad (6)$$

### 5.4.2 여러 건의 기밀이 유출된 경우

원가접근법의 특성상 유출된 기밀이 1건일 경우와 여러 건일 경우에는 계산 방법이 동일하면 신뢰성이 낮아진다. 일반 군사기밀은 통상 여러 건이 동시에 유출되는 경우가 많기 때문에 이러한 사례에 대한 계산 방안도 정립될 필요가 있다. 유출된 기밀 건수에 따라 반복적으로 계산해야 하는 분야도 있고, 그렇지 않은 분야도 있다. 또한 기밀 내용의 관련성에 따라 상황에 따라 달리 적용해야 하는 경우도 존재하며, 자세한 내용은 표 5.4와 같다.

표 5.4 여러 건의 기밀 유출시 반복적으로 계산해야 하는 분야

| 단 계 | 단 계 명 | 기본 비용 산출 간 포함사항 | 반복 계산 |
|---|---|---|---|
| 4 | 유출 | - 보안조사 인건비<br>- 보안조사 경비<br>- 보안조사 간접비 | × |
| 5 | 유해성 판단 | - 회의비(자문) | × |
| 6 | 유출 비밀 파기 | - 파기 과정 소요 인건비 | ○ |
| 7 | 비밀 재구상 | - 자료 수집비<br>- 자체 연구비<br>- 외부 연구용역비 | 기밀의 관련도에 따라 상이 |
| 8 | 비밀 재생산 | - 인건비<br>- 직접 재료비<br>- 간접 재료비 | ○ |

상기 표 5.4은 기본적인 상황에서의 반복 계산 여부를 제시한 내용이며, 실제 상황에서는 더 복잡한 경우가 발생할 수 있어 계산과정의 세부내용은 상황 및 사례의 특성을 심도 있게 고려해야 한다.

# 제 6 장  기밀 가치평가 결과 및 비교 분석

이 장에서는 제 5장에서 제시한 가치평가 모델을 적용해서 기밀의 금전적 가치를 평가해 본다. 일부는 실제 사례이며, 일부는 다양한 경우에 대한 평가값을 확인해 보기 위해 실제 사례를 바탕으로 특정 부분을 재구성한 사례이다. 또한, 본고 모델의 장·단점을 확인할 수 있도록 군사기밀 피해평가를 위해 기존에 제시되었던 모델[39]을 적용하여 도출한 값과 상호 비교 및 분석하였다†.

## 6.1 방산기밀 가치 평가

### 6.1.1. 방산기밀 유출사건 1 (사례 1)

D사는 무기중개업체로 00년 방산기밀을 활용하여 1,300억 원 규모의 사업을 중개하였다. 00년 D사의 공식적인 손익계산서는 표 6.1이며, 매출액은 19.3억 원, 매출총이익 14.0억 원, 영업이익 2.0억 원, 법인세 차감 전 순이익 3.1억 원, 당기순이익 2.6억 원이다[43].

#### 6.1.1.1 본고 모델 적용

본고에서 제안한 모델을 활용하기 위해서는 업체의 정확한 손익계산서가 필요한데, D사의 손익계산서에는 상기 사업에서 발생한 이익이 누락되어 있다.

관련 업계에서 통용되는 수수료 평균값(7.5%)을 적용하여 누락된 이익을 계산하면 약 97.5억 원이다. 이를 매출액에 포함시켜 당기순이익을 다시 계산해야 하며 그 값은 100.1억 원이다.

상기 기밀은 사업 수주에 절대적으로 유리한 독점적 정보를 포함하고 있어, α값은 앞서 제시한 표 0.0에서 '절대적으로 유리' 항목의 평균값인 0.9를 적용하였다. β값은 누락된 이익을 포함하여 총 매출액 대비 해당 사업의 비중을 산정하였다. 앞 장에서 제시한 수식 (3)에 대입하여 계산해 보면,

$$100.1\text{억 원} \times 0.9 \times (97.5/116.8) = 75.2\text{억 원}$$

상기 방산 기밀은 D사에 75.4억 원의 이익을 창출하였으므로, 수익접근법 개념에서 75.4억 원의 가치가 있다.

---

† 금전적 가치 평가 간 기본 단위는 '억 원'이며, 소수점 이하 둘째 자리에서 반올림하였다.

표 6.1 D사의 손익계산서 단위 : 원

| 과 목 | 금 액 | |
|---|---|---|
| Ⅰ. 매출액 | | 1,934,341,959 |
| 상품매출 | 645,692,470 | |
| 임대료수입 | 166,829,294 | |
| 서비스용역수입 | 34,085,438 | |
| 오파수수료수입 | 1,087,734,757 | |
| Ⅱ. 매출원가 | | 532,013,833 |
| (1) 상품매출원가 | 532,013,833 | |
| 기초상품재고액 | 136,790,706 | |
| 당기상품매입액 | 395,223,127 | |
| Ⅲ. 매출총이익 | | 1,402,328,126 |
| Ⅳ. 판매비와 관리비 | | 1,205,080,755 |
| 급여 | 196,670,477 | |
| 상여금 | 15,701,151 | |
| 퇴직급여 | 64,224,718 | |
| 복리후생비 | 64,485,286 | |
| 건물관리비 | 20,050,084 | |
| 접대비 | 29,000,000 | |
| 감가상각비 | 78,631,833 | |
| 세금과 공과금 | 11,062,281 | |
| 차량유지비 | 34,174,595 | |
| 운반비 | 5,570,099 | |
| 여비교통비 | 39,420,597 | |
| 보험료 | 11,540,347 | |
| 통신비 | 8,727,260 | |
| 지급수수료 | 322,842,326 | |
| 수도광열비 | 8,341,287 | |
| 소모품비 | 5,754,241 | |
| 도서인쇄비 | 3,494,032 | |
| 회의비 | 18,191,069 | |
| 사무용품비 | 645,450 | |
| 지급리스료 | 264,883,622 | |
| 수선유지비 | 1,642,000 | |
| 잡비 | 29,000 | |
| Ⅴ. 영업이익(손실) | | 197,247,371 |
| Ⅵ. 영업외수익 | | 297,500,897 |
| 이자수익 | 96,875,908 | |
| 배당금수익 | 113,245,281 | |
| 자산수증이익 | 86,510,000 | |
| 잡이익 | 869,708 | |
| Ⅶ. 영업외 비용 | | 186,699,045 |
| 이자비용 | 58,978,133 | |
| 외환차손 | 95,797,875 | |
| 기부금 | 31,200,000 | |
| 잡손실 | 723,037 | |
| Ⅷ. 법인세 차감전순이익 | | 308,049,223 |
| Ⅸ. 법인세 등 | | 46,199,059 |
| Ⅹ. 당기순이익 | | 261,850,164 |

#### 6.1.1.2 기존 모델 적용

전술한 바와 같은 동일한 상황에서 기존 모델‡을 통해 유출된 기밀의 가치를 환산해 보면 표 6.2와 같다.

표 6.2 기존 모델을 활용한 기밀 가치평가 결과 (사례 1)

| 구 분 | 금 액 | 비 고 |
|---|---|---|
| 비밀 내용별 비용 | 80.0억 원 | 방산기밀은 80억 원에 해당 |
| 생산 비용 | 1.5억 원 | 인건비, 재료비, 행정비용 등 |
| 검증 비용 | 1.2억 원 | 용역사업 평균값 |
| 조사 비용 | 0.1억 원 | 조사관 인건비 |
| 총 계 | 82.8억 원 | · |

유출된 비밀이 방위산업과 관련되어 있는 방산기밀이기 때문에 기본적으로 비밀 내용이 80억 원의 가치가 있으며, 이에 생산·검증·조사 비용을 추가하여 82.8억 원의 가치가 있는 것으로 계산되었다.

### 6.1.2. 방산기밀 유출사건 2 (사례 2)

방산기밀이 유출되는 다양한 경우를 비교하기 위해 앞서 제시한 사례 1에서 해당 사업의 규모만을 1/10로 축소한 가상의 시나리오를 제시한다.

E사는 00년 130억 원 규모 사업을 중개하면서 방산기밀을 불법 활용하여 (손익계산서에는 포함되지 않은) 9.8억 원의 이득을 챙겼다. E사의 손익계산서상 매출액은 19.3억 원, 당기 순이익은 2.6억 원이다.

#### 6.1.2.1 본고 모델 적용

손익계산서에 포함되지 않은 매출액 9.8억 원을 추가하면 E사의 매출액은 29.1억 원, 당기순이익은 12.4억 원이다. α값은 이전과 동일하게 0.9를 적용하여 수식 (3)에 대입하면 해당 기밀의 가치는 6.7억 원이다.

$$12.4억원 \times 0.9 \times (9.8/29.1) = 3.8억원$$

---

‡ 비밀유출 피해비용 = (비밀 내용별 비용 + 생산 비용 + 검증 비용 + 복구 비용 + 조사 비용 + 업무중단 비용) × 누설 건수

#### 6.1.2.2 기존 모델 적용

해당 사업 규모를 1/10로 축소한 시나리오를 적용하였기 때문에 E사의 사례를 기존 모델로 가치평가를 할 경우, 생산 비용과 검증 비용 역시 1/10 수준으로 축소하였다. 기존 모델을 적용한 가치평가 결과는 표 6.3과 같이 비밀 내용별 비용 80.0억 원에 기타 비용 0.4억 원을 합하여 총 80.4억 원 수준으로 평가되었다.

표 6.3 기존 모델을 활용한 기밀 가치평가 결과 (사례 2)

| 구 분 | 금 액 | 비 고 |
|---|---|---|
| 비밀 내용별 비용 | 80.0억 원 | 방산기밀은 80억 원에 해당 |
| 생산 비용 | 0.2억 원 | 인건비, 재료비, 행정비용 등의 1/10 |
| 검증 비용 | 0.1억 원 | 용역사업 평균값의 1/10 |
| 조사 비용 | 0.1억 원 | 이전 사례와 동일 |
| 총 계 | 80.4억 원 | · |

### 6.2 일반 군사기밀 가치 평가

#### 6.2.1. 일반 군사기밀 유출사건 (사례 3)

G씨는 00년 인터넷에 작전계획 기밀을 유출하였으며, 이로 인해 군에서는 이와 관계되어 있는 기밀을 재생산해야 하는 상황에 처했다. 해당 작전계획은 30개 부대에 배부되었으며, 이와 관련되어 있는 기밀을 보유하고 있는 부대는 1,000개이다.

#### 6.2.1.1 본고 모델 적용

이익을 창출하지 않는 일반 군사기밀은 '원가접근법'을 적용하여 재생산원가를 계산한다. 전술한 바와 같이, 정성적인 분야는 제외하고 오직 정량적으로 환산할 수 있는 분야만 계산한다. 수식 (5)를 적용하여 가치평가를 시행하며, 인건비를 상정할 때는 국방부에서 발행한 국방통계연보[45]에 명시된 중령 이하 장교의 평균 보수를 적용하였다. 세부 사항은 표 6.4와 같으며, 상기 기밀의 가치는 14.9억 원 수준으로 환산됐다.

표 6.4 본고 모델을 활용한 기밀 가치평가 결과 (사례 3)

| 단계 | 단 계 명 | 세부 내역 | 환산 비용 |
|---|---|---|---|
| 4 | 유출 | - 보안조사 인건비 (5명×5일×20만원=500만원)<br>- 보안조사 경비 (5명×5일×7만원=175만원)<br>- 보안조사 간접비 (100만원) | 800만원 |
| 5 | 유해성 판단 | - 회의비 (10명×1일×20만원=200만원) | 200만원 |
| 6 | 유출 비밀 파기 | - 파기 과정 인건비<br>(1,000명×1시간×2.5만원=2,500만원) | 2,500만원 |
| 7 | 비밀 재구상 | - 자료 수집비 (5명×20일×20만원=2,000만원)<br>- 자체 연구비 (20명×30일×20만원=1억 2,000만원)<br>- 외부 연구용역비(1.2억원) | 2억<br>6,000만원 |
| 8 | 비밀 재생산 | - 직접 인건비 (30명×30일×20만원=1억 8,000만원)<br>- 간접 인건비 (1,000명×3일×20만원=6억 원)<br>- 직접 재료비 (1,000부×5천원=500만원)<br>- 간접 재료비 (1,000부×5천원=500만원) | 7억<br>9,000만원 |
| 합계 | | · | 10억<br>8,500만원 |

### 6.2.1.2 기존 모델 적용

G씨가 유출한 기밀의 가치를 기존 모델에 적용하여 평가한 결과는 표 6.5와 같다. 작전계획 분야 기밀이므로 기본적으로 비밀 내용 75억 원에 기타 비용을 포함하여 총 78.1억 원이다.

표 0.0 기존 모델을 활용한 기밀 가치평가 결과 (사례 3)

| 구 분 | 금 액 | 비 고 |
|---|---|---|
| 비밀 내용별 비용 | 75.0억 원 | 작전계획 기밀은 75억 원에 해당 |
| 생산 비용 | 1.8억 원 | 인건비 1억 8천만원,<br>재료비 500만원 |
| 검증 비용 | 1.2억 원 | 용역사업 평균값 적용 |
| 조사 비용 | 0.1억 원 | 조사관 인건비 등 |
| 총 계 | 78.1억 원 | · |

## 6.3 결과 비교 및 분석

상기 사례 1 ~ 3에서 제시된 방산기밀 및 일반 군사기밀의 금전적 가치를 평가한 결과를 종합해 보면 표 6.6과 같다.

표 6.6 기밀 가치평가 결과 비교

| 구 분 | 총 사업비 | 금전적 가치 | |
|---|---|---|---|
| | | 본고 모델 | 기존 모델 |
| 사례 1 | 1,300억 원 | 75.2억 원 | 82.8억 원 |
| 사례 2 | 130억 원 | 3.8억 원 | 80.4억 원 |
| 사례 3 | - | 10.9억 원 | 78.1억 원 |

본고에서 제안한 모델은 방산기밀의 원래 사업규모에 따라 이익을 창출하는 수준이 다르므로 방산기밀 평가값이 이에 상응하여 변화한다. 따라서 기밀의 내용 및 활용도를 고려한 가치평가가 가능하다. 일반 군사기밀은 정성적인 분야가 제외되기 때문에 재생산원가 측면에서 기밀 가치가 11억 원 수준임을 확인할 수 있으며, 이는 해당 기밀이 배부되어 있는 범위 등에 따라 달라질 수 있다.

한편, 기존 모델은 기밀 내용의 정성적 가격이 고정되어 있기 때문에 기밀의 가치가 항상 80억 원 정도로 계산될 수밖에 없는 한계가 있다.

# 제 7 장 활용 방안 및 기대 효과

## 7.1 활용 방안

### 7.1.1. 국가기밀의 금전적 가치 평가 방법론 정립

산업기술이나 영업비밀과는 달리, 국가기밀 유출시 피해규모 산정을 위한 방법론이 부재한 상황이기 때문에 본고에서 제안한 모델을 바탕으로 공신력 있는 기관에서 국가기밀의 금전적 가치 평가 방법론을 정립할 필요가 있다. 사회적 공감대를 형성할 수 있도록 민·관·군 공동으로 이에 대한 연구를 진행하는 것이 바람직하다. 이를 통해 기밀 유출 사고 발생시 피해규모를 구체적인 데이터로 표현할 수 있고, 장기적으로 이 방법론이 신뢰성이 있다고 인정받게 되면 다양한 정책과 제도를 개선하는데 유용하게 활용될 수 있다.

### 7.1.2. 국가기밀 유출시 손해배상 관련 조항 신설

현재 우리는 국가기밀 유출 사고가 발생할 경우, 국가에서 형사소송만을 진행하고 있다. 하지만 관련 법률(군사기밀보호법 등)에 손해보상 조항을 신설하고 전술한 바와 같이 적절한 가치 평가 방안이 정립되면 국가가 입은 피해(또는, 앞으로 입게 될 피해) 규모를 기준으로 피의자에게 민사소송을 제기하여 보상을 받아야 한다.

### 7.1.3. '징벌적 손해배상' 제도 도입

징벌적 손해배상 제도는 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 통한 억지 기능을 가진 효과적인 구제수단으로 인식[45]되고 있다.

우리나라에서도 다양한 분야에서 '징벌적 손해배상 도입을 검토해 볼 수 있는 시기가 되었다[46]'고 보는 이들도 상당수 존재하는 등 여론이 성숙되어 가는 단계이다. 실제 금융위원회에서는 2015.3.11.부로 '신용정보의 이용 및 보호에 관한 법률'을 일부 개정하여 손해액의 3배 이하에서 손해배상 책임을 부여하는 징벌적 손해배상을 법제화 하였다[47].

장기적으로 고의적 국가기밀 유출자에 대해 징벌적 손해배상 제도 적용 여부를 판단할 때 유의할 점은, 피의자가 형사처벌을 받은 정도를 감안하여 손해배상액을 산정해야 하는 것이다.

## 7.2 기대 효과

### 7.2.1. 국가기밀 유출에 따른 사회적 비용 절감

국가기밀 유출자에 대해 제도적으로 (징벌적) 손해배상을 청구할 수 있고, 실제 청구하게 된다면 배상액 규모가 크지 않더라도 금전적 이익을 목적으로 발생하는 기밀 유출 사고 뿐 아니라 전반적인 기밀 유출 사고를 상당 부분 감소시킬 수 있으며, 이에 따른 불필요한 사회적 비용 역시 절감할 수 있다.

### 7.2.2. 국가안보 기여 및 대국민 신뢰도 향상

심리적 예방 효과 및 실질적 손해배상 청구를 통해 군사기밀 유출을 예방할 경우 국가안보에 기여하고 국가 차원의 보안 수준 향상에 크게 공헌할 수 있다. 또한, 기밀이 유출될 때마다 국민들이 불안해하고 정부에 대해 부정적 인식이 팽배해지는 경향도 보안 수준이 향상됨에 따라 자연스럽게 해결될 수 있다.

### 7.2.3. 보안 분야 예산 투자 증가

법제화를 통해 (징벌적) 손해배상으로 얻는 이익은 해당 기밀을 재생산하고 관리하는데 사용하거나, 정부 차원에서 보안 업무와 관련 있는 분야의 발전에 활용한다면 보안 예산은 자연스럽게 증액될 것이며, 우리나라의 보안업무 수행 체계 및 보안수준을 더욱 향상시킬 수 있을 것이다.

# 제 8 장 결론 및 향후 과제

## 8.1 결론

기밀 유출의 원인은 대인관계, 스파이 활동 등 다양한데, 그 중에서 가장 주목해야 할 부분은 '금전적 대가'이다. 기밀을 유출하여 적발되었을 때 감수해야 할 피해보다도 그것이 창출하는 금전적인 이익이 더 크기 때문에 기밀 유출 사고는 끊이지 않고 발생하고 있다.

우리는 "안전한 시스템 설계의 주목적은 보호되어야 할 자산의 가치보다 더 많은 비용을 들여 시스템을 파괴하도록 만드는 것이며, 이 때 '비용'은 노력이나 평판과 같은 추상적인 단어보다는 금전적 가치로 측정되어야만 한다[48]"는 관점에서 국가기밀 유출사고에 접근해 볼 필요가 있다.

본고에서는 기밀에 대해서 정성적인 부분을 제외하고 오직 정량적으로 환산할 수 있는 부분에 한해 금전적 가치 평가 모델을 제안하였으며,

**{안전한 시스템 설계의 주목적}은 {시스템을 파괴}하여 얻을 수 있는 {가치}보다**
**{국가기밀 보호하기 위해} {기밀을 유출} {금전적 이익}**

**{더 많은 비용}을 들여서 {시스템을 파괴}하도록 만드는 것이며,**
**{막대한 손해배상 감수} {기밀을 유출}**

**이 때 '비용'은 {추상적인 단어}보다는 {금전적 가치}로 측정** 하였다.
**{정성적인 부분} {정량적인 값}**

금전적 대가를 통한 기밀 유출에서 착안하여 국가기밀의 금전적 가치 평가 방법론을 제안했지만, 본 연구결과를 발전시킨다면 다양한 원인에 의해 발생하는 기밀 유출 사고를 전반적으로 감소시킬 수 있을 것이다.

국가기밀의 일부인 군사기밀의 예를 들어 무형자산 가치평가 방법론을 적용하여 기밀자료 가치평가 모델을 정립하였으며, 향후 다양한 목적으로 활용할 수 있는 첫걸음을 제시하였다. 정량적 접근을 통해 기밀의 특성에 따라 상이한 가치평가 방법론을 적용하여 신뢰성 및 활용 가능성을 동시에 제고시킨 최초의 연구로 판단된다.

본고에서 제안한 방법론은 다양한 접근 방법 중 일부의 예를 제시한 것이며, 기밀의 금전적 가치 평가에 신뢰성을 기하기 위해서는 전문 연구기관에 의한 심층 연구가 수행되어야 하고, 사회 각계각층의 의견을 수렴하는 등의 절차를 반드시 거쳐야 한다.

## 8.2 향후 과제

앞으로 국가(군사)기밀을 보호하기 위한 다양한 법률 및 정책들 간 문제점과 발전 방안에 대한 연구를 진행할 것이며, 보안 경제학 차원에서 해외 사례를 참고하여 기밀 유출 관련 사회적 비용을 정확히 판단하는 연구도 검토할 예정이다.

한편, 연구 진행 간 인터넷 등에 공개된 자료만을 활용하였기 때문에 일부 현황은 실제와 다를 수 있으며, 향후 상세한 현황 등을 확보할 수 있다면 연구의 신뢰도를 더욱 향상시킬 수 있을 것으로 기대한다.

# 참 고 문 헌


[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,” 2014년 7월.

[3] Sang-No Lee, “War without gunfire, Industrial espionage,” The 5th International Intellectual Property & Industrial Security conference, May 2015.

[4] Cormac Herley, “Security, cybercrime, and scale,” Communications of the ACM, 57(9), pp. 64-71, Sep. 2014.

[5] Mary E. Zurko, Richard T. Simon, “User-centered security,” Proceedings of the 1996 workshop on New security paradigms. ACM, New York, pp. 27-33, Sep. 1996.

[6] Ryan West, “The psychology of security : why do good users make bad decisions?,” Communications of the ACM, 51(4), pp. 34-40, Apr. 2008.

[7] Donald Ray Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement*, Montclair, p. 30, Apr. 1972.

[8] David T. Wolfe and Dana R. Hermanson, *The Fraud Diamond: Considering the Four Elements of Fraud*, CPA Journal 74.12, pp.38-42, Dec. 2004.

[9] 김흥수, *무형자산 가치평가론*, 북메이트, pp. 189-216, 2005년 9월.

[10] Gordon V. Smith and Russell L. Parr, *지적재산과 무형자산의 가치평가*, 세창출판사, pp. 199-212, 2000년 5월.

[11] 보안업무규정, 대통령령 제26140호, 2015.3.11.

[12] 국가정보원법, 법률 제12948호, 2014.12.30.

[13] 군사기밀보호법, 법률 제13503호, 2015.9.1.

[14] 국방부(정보공개 청구 자료), “군사기밀보호법 위반사건 판결문,” 2015년 3월.

[15] MBC, “http://imnews.imbc.com/replay/2011/nw1200/article/2899994_13044.html,” 2011년 8월.

[16] 문화일보, “http://www.munhwa.com/news/view.html?no=2012020301070927182004,” 2014년 5월.

[17] 내일신문, “http://news.naver.com/main/read.nhn? mode=LSD&mid=sec&sid1=102&oid=086&aid= 0002139442,” 2012년 12월.

[18] 브릿지경제, “http://www.viva100.com/main/view.php?key=20150921010005250,” 2015년 9월.

[19] 임내현 의원 공식홈페이지, “http://www.nhlim.com/”, 2015년 10월.

[20] 민경식, 송혜인, “정보보호의 경제적 분석 연구 동향,” 한국정보보호진흥원, 2008년 10월.

[21] Paul Syverson, “The Paradoxical Value of Privacy,” In 2nd Annual Workshop on Economics and Information Security (WEIS ’03), Mar. 2003.

[22] Sören Preibusch, “The value of privacy in Web search,” In 12nd Annual Workshop on Economics and Information Security (WEIS ’13), June 2013.

[23] Ignacio N. Cofone, “The Value of Privace: Keeping the Money Where the Mouth is,” In 14nd Annual Workshop on Economics and Information Security (WEIS ’15), June 2015.

[24] Serge Egelman, Adrienne Porter Felt, and David Wagner, “Choice Architecture and Smartphone Privacy: There’s A Price for That,” In 11nd Annual Workshop on Economics and Information Security (WEIS ’12), June 2012.

[25] Sören Preibusch, Kat Krol, and Alastair R. Beresford, “The privacy economics of voluntary over-disclosure in Web forms,” In 11nd Annual Workshop on Economics and Information Security (WEIS ’12), June 2012.

[26] Lawrence A. Gordon and Martin P. Loeb, “The Economics of Information Security Investment,” Information and System Security, 5(4), pp. 438-457, Nov. 2002.

[27] 신영웅, 전상훈, 임채호, 김명철, *국가 사이버보안 피해금액 분석과 대안: 3·20 사이버 침해사건을 중심으로*, 국가정보연구, 제6권 제1호, pp.129-173, 2013년 6월.

[28] 박채희, “개인정보 침해사고로 인한 경제적 피해규모 산출방법의 연구,” 한양대학교 석사학위 논문, 2012년 2월.

[29] 김상봉, 김정렬, 노맹석, 지인엽, 조경준, “개인정보유출과 조류독감의 간접피해비용 추정기법 연구,” 국민안전처 국립재난안전연구원, 2014년 12월

[30] 권오상, *환경경제학*, 박영사, 2007년 8월.

[31] 유승동, 유진호, *개인정보 보호를 위한 지불의사비용 결정요인*, 한국정보보호학회 논문지, 제24권 제4호, pp. 695-703, 2014년 8월.

[32] 권홍, “CVM을 이용한 개인정보 침해사고의 위자료 산정,” 충북대학교 석사학위 논문, 2011년 2월.

[33] 차건상, “개인정보 유출에 따른 손해배상액 산정기준에 관한 연구,” 숭실대학교 박사학위 논문, 2011년 12월.

[34] 신재형, “개인정보 유출로 인한 기업의 책임: 손해배상책임을 중심으로,” 서울대학교 석사학위 논문, 2015년 2월.

[35] 이경호, “기술유출 사고로 인한 피해금액 산정을 위한 모델 연구,” 고려대학교 박사학위 논문, 2009년 8월.

[36] U.S.S.G.(United States Sentencing Guidelines) §2 B1.1 Commentary 3 (b).

[37] 안성수, *형사상 영업비밀 침해에 있어서 이익과 손해액 산정*, 정보법학, 제11권 제1호, pp.21-59, 2007년 7월.

[38] 김국현, “영업비밀 침해로 인한 재산적 이득 및 손해에 관한 검토,” 대검찰청 기술유출사건연구회, 2013년 12월.

[39] 장월수, “군사비밀 유출에 따른 피해금액 산정을 위한 모델 연구,” 고려대학교 박사학위 논문, 2012년 8월.

[40] 김철완, 정준현, 이상원, 오영석, “개인정보보호제도 시행의 경제·사회적 파급효과 분석연구,” 정보통신정책연구원, 2001년 12월.

[41] 투코리아, “http://defence21.hani.co.kr/34228”

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

[43] 명진공인회계사 감사반, A사 재무제표

[44] 국방부, *2014 국방통계연보*, p. 55, 2014년 12월.

[45] 김현수, *미국법상 징벌적 손해배상*, 재산법연구, 29(2), pp. 325-355, 2012년 8월.

[46] 법제처 세계법제정보센터, “징벌적 손해배상 연구,” 2012년 12월.

[47] 신용정보의 이용 및 보호에 관한 법률, 법률 제13216호, 2015.3.11.

[48] Christof Paar, Jan Pelzl, *Understanding Cryptography*, Springer, Aug. 2009.

# 감 사 의 글

우선, 대한민국 최고 공과대학인 한국과학기술원에서 석사 학위 과정을 수학할 수 있도록 기회를 제공한 기무사령부 및 육군에 감사의 말씀을 드립니다.

전산 분야 지식이 부족하여 졸업 여부조차도 낙담할 수 없는 상황에서 큰 부담을 감수하신 채 저를 지도학생으로 받아주시고 졸업할 때까지 관심과 정성으로 지도해 주신 김광조 교수님께 진심으로 존경과 감사의 말씀을 올립니다.

전공 지식과 경험 등에서 한없이 부족한 제가 '정보보호대학원'에 입학할 수 있도록 도움을 주신 주대준 전 부총장님, 김명철 전 학과장님께도 감사드립니다.

다양한 관점에서 정보보호 분야를 바라볼 수 있도록 도와주시고, 석사학위 논문 심사위원으로 도움을 주신 임채호 교수님께도 감사드립니다.

암호와 정보보안 연구실에서 학업 및 연구 간 도움도 많이 받았고, 다양한 활동을 통해 정도 많이 들었던 이동수, 칼리드, 김학주, 최락용, 정제성, 김경민, 홍진아, 아미난또 역시 감사합니다.

전공 과목을 수강하면서 혼자 힘으로 해결할 수 없는 상황에 부딪칠 때마다 도움을 주었던 정보보호대학원 석사과정 7기 동기생들에게도 고마움을 표시하고 싶습니다.

지근거리에서 학업 뿐 아니라 개인적인 사항들까지도 기꺼이 도와주며 저에게 힘을 북돋아 주었던 안수현, 배찬우 학우에게도 감사합니다.

마지막으로 석사학위 2년 간 항상 곁에서 사랑과 신뢰를 바탕으로 칭찬과 응원을 통해 전폭적인 지지를 보내준 제 아내 강가영, 아들 박선우, 딸 박선아 및 모든 가족들에게 감사드립니다.

# 이 력 서

성 명 : 박준정
생년월일 : 1981. 5.27.
연 락 처 : sunsun64@kaist.ac.kr

## 학 력

1997. 3. - 2000. 2. 목포고등학교
2000. 3. - 2004. 2. 육군사관학교 지휘행동학과 (학사)
2014. 3. - 2016. 2. 한국과학기술원 전산학부 정보보호대학원 (석사)

## 경 력

2014. 7. - 2014. 9. Workshop on Cryptographic Hardware and Embedded Systems 2014 (CHES 2014), 부산, 파라다이스 호텔, 9.23.-26. 운영 지원

## 연 구 과 제

2014. 7. - 2015. 6. Intrusion Detection System for Critical Infrastructures Using Big Data Analytics (KAIST-KUSTAR Institute)
2015. 4. - 2015. 8. 국가재난안전통신망의 장기간 보안성을 보장하는 산업 발전 전략 (KAIST 미래전략연구센터)

## 학 회 활 동

1. 박준정, 김광조, “군사기밀 유출자에 대한 손해배상 제도 적용 방안,” 한국정보보호학회 동계 학술대회(CISC-W ’14), 한양대학교, 서울, 2014.12.6.

2. 정제성, 김경민, 김학주, 박준정, 안수현, 이동수, 최락용, 김광조, 김대영, “경량 암호를 이용한 IoT Secure SNAIL 플랫폼 구성(I),” 한국정보보학회 동계학술대회(CISC-W ’14), 한양대학교, 서울, 2014.12.6.
3. 박준정, 김광조, “국방 보안사고에 대한 행동 심리학적 분석 방법,” 2015 한국정보보호학회 영남지부 학술대회, 2015.2.13. 부산대학교, 부산.
4. 박준정, 김소라, 안수현, 임채호, 김광조, “조직의 실시간 보안관리 체계 확립을 위한 ‘인터페이스 보안’ 강화에 대한 연구,” *정보처리학회 논문지*, 제4권 제5호, pp.171-177, 2015. 5.31.
5. 박준정, 김광조, “국가 사이버 안보 역량 강화를 위한 ‘사이버 방위산업’ 육성 방안,” 한국정보보호학회 하계학술대회(CISC-S ’15), 한국과학기술원, 대전, 2015. 6.25.-26.
6. 박준정, 김광조, “국가기밀의 금전적 가치평가 방법론,” 한국정보보호학회 충청지부 학술대회, 서원대학교, 청주, 2015.10.16.
7. 배찬우, 안수현, 박준정, 신승원, 김광조, “웹 스캐닝을 이용한 캠퍼스 내 웹사이트 보안 취약점 발굴 및 웹 보안 연구,” 한국정보보호학회 충청지부 학술대회, 서원대학교, 청주, 2015.10.16.
8. 박준정, 김광조, “국가기밀의 유출 요인과 금전적인 대책,” 한국정보보호학회 동계학술대회 (CISC-W ’15), 서울여자대학교, 서울. 2015.12.5.