韓國IT서비스學會誌
第18卷 第5號
2019年 12月, pp.155-164

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2019.18.5.155

정보보호 대책 수준을 고려한 정보보호 투자 최적화: 유전자 알고리즘 접근법*

임정현** · 김태성***

Optimization of Information Security Investment Considering the Level of Information Security Countermeasure: Genetic Algorithm Approach*

Jung-Hyun Lim** · Tae-Sung Kim***

■ Abstract ■

With the emergence of new ICT technologies, information security threats are becoming more advanced, intelligent, and diverse. Even though the awareness of the importance of information security increases, the information security budget is not enough because of the lack of effectiveness measurement of the information security investment. Therefore, it is necessary to optimize the information security investment in each business environment to minimize the cost of operating the information security countermeasures and mitigate the damages occurred from the information security breaches. In this paper, using genetic algorithms we propose an investment optimization model for information security countermeasures with the limited budget. The optimal information security countermeasures were derived based on the actual information security investment status of SMEs. The optimal solution supports the decision on the appropriate investment level for each information security countermeasures.

Keyword : Information Security Investment, Genetic Algorithm, Optimization of Investment

Submitted : November 4, 2019 Accepted : December 16, 2019

* 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018S1A5A2A01039356).

** 충북대학교 경영정보학과 석사과정

*** 충북대학교 경영정보학과 교수 및 보안경제연구소장, 교신저자

1. 서 론

새로운 기술의 끊임없는 등장으로 정보보호 위협이 고도화·지능화되고 있으며 위협의 유형 또한 다양해지고 있다. 이에 따라 각 기업에서 정보보호에 대한 투자가 증가하고 있으나, IT 예산 중 정보보호 관련 예산이 차지하는 비율은 높지 않다. 침해사고를 경험한 사업체는 2017년 2.2%, 2018년 2.3%로 침해사고는 정보보호 예산에도 불구하고 꾸준히 발생하는 것으로 나타났다(과학기술정보통신부, 2019). 기업의 정보보호 현황에 적합하고 기업 운영비용을 최소화할 수 있는 정보보호 대책의 선택은 적정투자 수준을 결정하기 위한 가이드라인 역할을 할 수 있다(공희경 등, 2008). 또한, 정보보호 투자에 있어 관리 유연성은 침해사고를 사전 예방을 통해 불확실한 피해를 완화할 수 있다(Benaroch, 2018). 따라서 기업 환경에 맞게 정보보호 대책 운영비용을 최소화하고 불확실한 피해를 완화할 수 있는 정보보호 투자 최적화가 필요하다.

정보보호 투자 효과를 예측하기 위한 연구는 꾸준하게 수행되어 왔으나, 다양한 기업 환경에서 '정보보호 투자를 어떻게 해야 하는지'에 대한 세부적인 연구는 상대적으로 부족하다. 본 연구에서는 '정보보호 투자를 어떻게 해야 하는지'에 대한 세부적인 사항을 고려하였다. 정보보호 대책 도입여부 뿐만 아니라 정보보호 대책 도입 수준을 고려하였고, 정보보호 대책이 침해사고를 완벽히 막지 못할 수 있다는 것을 고려하였다. 기존 연구에서는 정보보호 대책이 완벽하지는 못하다는 것을 고려하였으나(Gupta 등, 2006), 정보보호 대책 도입 수준에 대해서는 고려하지 않았다(Gupta 등, 2006; 김길환 등, 2018).

본 연구에서는 기업의 제한된 투자금액 안에서의 투자, 대책의 수준에 따라 침해사고로 인한 피해액에 차등을 두었다. 침해사고의 고도화·지능화 및 예측이 어려운 점을 고려하여 침해사고를 무작위로 생성하였고 기업이 기존에 보유하고 있는 정보보호 대책들의 수준을 설정하고 제한된 투자금액 내에서의 투자 최적화 모형을 만들고 유전자 알고리즘을 이용하여 최적화 모형의 해를 탐색하는 방법을 제안한다.

본 연구의 결과는 다양한 기업 환경에서 정보보호 대책에 대한 투자 최적화를 효과적으로 수행하고 의사결정에 도움이 될 것이라 기대한다.

본 연구의 구성은 다음과 같다. 제 2장에서는 관련 문헌을 고찰한다. 제 3장에서는 연구의 모형을 정의하고 제 4장에서는 모형의 해를 유전자 알고리즘을 통해 탐색하는 방법을 설명한다. 제 5장에서는 수치예제를 통해 연구 모형을 적용한다. 제 6장에서는 본 연구의 결론과 향후 발전 방향을 제시한다.

2. 문헌고찰

정보보호 최적 포트폴리오를 구성하고 가치를 평가하는 연구는 이전부터 활발히 진행되어 왔으며 현재에도 꾸준히 진행되고 있다. Bodin 등은 AHP 평가 방법을 사용하여 기업의 정보 시스템 보안 유지 및 강화를 위한 최적의 예산 배분 결정 모델을 제시하였고(Bodin 등, 2005), 양원석 등은 확률모형을 활용하여 보안 포트폴리오 구성 전후를 비교하고 경제적으로 분석하여 보안 포트폴리오의 가치를 평가하였다(양원석 등, 2009). Fielder 등은 게임이론 방법과 조합 최적화, 게임이론과 조합 최적화를 결합하여 중소기업 정보보호 대책 결정 방법을 제시했다(Fielder 등, 2016). Nespoli 등은 정보보호 대책 최적화 분야에서 기존 다양한 방법론을 비교하기 위한 기준을 제시하고 기존의 연구들을 분석하였다(Nespoli 등, 2018).

Gupta 등은 대책 비용과 취약점을 최소화하기 위해 유전자 알고리즘 접근법을 활용하여 최적의 보안 포트폴리오를 구성하였다. 취약점의 특성과 보안기술을 이진표현으로 나타내었으며 취약점의 특성과 보안기술을 비교하여 잔여 취약점과 운영비용을 최소화하는 최적해를 도출하였다(Gupta 등,

2006). 김길환 등에서는 주어진 침해사고의 발생빈도, 평균 피해액, 평균 투자비용, 방어비율의 점추정치를 이용하여 침해사고와 대책을 구성하였으며, 침해사고로 인한 피해액과 대책의 운영비용을 최소화하는 방법을 유전자 알고리즘을 활용하여 도출하였다(김길환 등, 2018). 그러나 이 연구에서는 정보보호 대책을 도입 또는 미도입으로만 구분하였다. 이는 침해사고와 대책의 취약성 관계에서 발생하는 피해, 즉, 대책의 수준을 고려하지 못해 실제 방법론을 적용하기 어려운 한계가 있다. 또한, 투자예산을 고려하지 않은 최적 대책 도입만을 고려하여 차선의 대안은 선택하지 못하게 되는 한계가 존재한다. 즉, 기존 연구에서는 정보보호 대책의 도입여부만을 고려하여 구체적으로 해당 대책에 얼마의 금액을 투자하여하는지에 대한 의사결정 지원에 한계가 있다(Gupta 등, 2006; 김길환 등, 2018).

본 연구에서는 기존 연구의 한계를 극복하여 실제 사례에 적용할 수 있도록 유전자 알고리즘 표현을 이진표현이 아닌 정수로 표현하여 세분화하여 제한된 투자금액 내에서의 최적해를 탐색한다. 침해사고가 발생하는 피해를 대책의 수준에 따라 차등함으로써 대책의 도입여부뿐만 아니라 기존에 보유하고 있던 대책에 대해서 추가적인 투자까지 고려하고, 정보보호 대책의 범주를 넓힘으로써 유전자 알고리즘이라는 메타 휴리스틱 방법의 장점을 극대화한다.

3. 연구 모형

n개의 보안 침해사고 유형과 기업이 보유하고 있는 m개의 정보보호 대책이 존재한다고 할 때, 본 연구에서는 n개의 보안 침해사고 유형을 무작위로 추출하고, 정보보호 대책의 속성을 객관화할 수 있다고 가정하였다. 각 변수에 대한 설명은 다음과 같다.

v_{id} : 보안 침해사고 i의 평균 피해액
v_{il} : 침해사고 i의 수준
v_{ip} : 침해사고 i의 공격 목표
c_{il} : 정보보호 대책 i의 수준
c_{iL} : 강화된 정보보호 대책 i의 수준
c_{ip} : 정보보호 대책 i의 방어 목표
c_{iu} : 정보보호 대책 i의 강화 비용
d_i : 침해사고 i로 인한 피해액
d : 총 피해액
i : 투자금액
d_g : 투자 최적화가 이루어진 후 총 피해액
λ : 평균 피해액 계수(0.2)

정보보호 대책의 강화비용은 현재 보유하고 있는 대책을 구입하는데 현재까지 투입된 총 누적비용을 의미한다. 이때 i = 1, …, n이고, j = 1, …, m이다. 침해사고 수준(v_{il})은 취약점의 주요 특징을 파악하고 심각도를 반영하는 수치를 산출하는 CVSS(Common Vulnerability Scoring System)를 참고하여 정의하였다(Houmb과 Franqueira, 2009). CVSS 점수는 0.1부터 10까지 정의되어 있으나 본 연구에서는 계산의 편의를 위해 1부터 10까지의 정수 10단계로 정의하였다. 정보보호 대책의 수준은 0(도입예정)부터 10까지의 정수로 대책의 수준을 객관화 할 수 있다고 가정하고 설정하였다. 따라서 침해사고의 수준과 정보보호 대책의 수준은 식 (1), 식 (2)와 같이 정의하였다.

$$v_{il} = \begin{cases} 1 & \text{수준} \\ \vdots & \\ 10 & \text{수준} \end{cases} \quad (1)$$

$$c_{il} = \begin{cases} 0 & \text{도입예정} \\ \vdots & \\ 10 & \text{도입 수준} \end{cases} \quad (2)$$

기업이 보유한 정보보호 대책이 결정되면 침해사고 i에 의한 피해액과 전체 침해사고에 대한 총 피해액은 식 (3), 식 (4)와 같이 정의하였다. 여기서 j는 침해사고 i의 공격목표와 매칭되는 대책을 말한다. 또한 평균 피해액 계수 λ(0.2)는 침해사고 v_i 발생 시 최대 피해액과 최소 피해액의 중간값이 침해사고 i의 평균 피해액 v_{id}과 같아지도록 하는 계수

이다. v_i 발생 시 최대 피해액은 침해사고 수준 v_{il}이 9이고 정보보호 대책 c_{jl}이 0인 경우이며, 최소 피해액은 $v_{il}-c_{jl}$=1인 경우이다.

$$d_i = \begin{cases} (v_{il}-c_{jl})v_{id}\lambda, \text{if } v_{il} > c_{jl} \\ 0 \quad\quad , \text{if } v_{il} \leqq c_{jl} \end{cases} \tag{3}$$

$$d = \sum_{i=0}^{n} (v_{il}-c_{jl})v_{di}\lambda \tag{4}$$

정보보호 투자를 통해 대책이 강화된 이후의 총 피해액과 주어진 투자금액과 강화비용에 관한 제약식은 식 (5), 식 (6)과 같이 정의하였다.

$$d_i = \begin{cases} (v_{il}-c_{jl})v_{id}, \text{ if } v_{il} > c_{jL} \\ 0 \quad\quad , \text{ if } v_{il} \leqq c_{jL} \end{cases} \tag{5}$$

$$\text{제약식} : \sum_{i=0}^{m} (c_{iL}-c_{il})c_{iu} < i \tag{6}$$

본 연구는 정보보호 투자 최적화 문제는 주어진 투자금액 내에서 기업이 보유하고 있는 정보보호 대책들을 강화하고 침해사고로 인해 발생할 수 있는 총 피해액을 최소화 하는 것이 목표이다.

4. 최적해 탐색 방법

본 연구에서 유전자 알고리즘을 최적해 탐색 방법으로 선정한 이유는 대책의 수준이 0부터 10까지로서, 최적해 탐색 범위가 최대 11m개이며 대책의 범위 또한 소프트웨어, 하드웨어, 교육 및 훈련, 서비스로 모든 대책을 포함하기 때문에 탐색 범위를 모두 탐색하기에 어려움이 있다. 본 한계점 해결을 위해 메타휴리스틱 방법 중 유전자 알고리즘을 선택했다. 유전자 알고리즘은 1975년에 개발된 생물의 진화 과정을 기반으로 한 최적화 탐색 방법으로 풀고자 하는 문제에 대한 가능한 해들을 정해진 형태의 자료구조로 표현한 다음 이를 점차적으로 변형함으로써 최적해를 도출한다. 해들을 나타내는 자료구조는 유전자, 이를 변형함으로써 세대 반복을 통해 최적 해를 탐색하는 과정은 진화로 표현한다(김동욱과 이원영, 2018).

유전자 알고리즘을 활용하기 위해서는 해를 유전자로 표현하는 방식, 해의 적합도를 평가하는 적합도 함수, 초기 인구 생성, 선택, 교차 방법, 변이에 대한 설계가 필요하다.

정보보호 대책은 도입예정인 대책을 포함하여 수준을 0부터 9까지 정의하였다. 따라서 해를 표현하는 유전자는 각 자리가 0부터 9사이의 값인 길이가 m인 정수표현(integer representation)이다. <표 1>은 대책 조합을 해로 표현한 예시이다. SW1, SW2 등은 기존에 기업에서 보유하고 있는 대책을 의미하며 각각의 대책 수준을 대책 조합 해로 표현하였다.

〈표 1〉 해를 표현하는 방식

	SW1	SW2	SW3	HW1	HW2
수준	4	5	2	6	8

초기해 생성은 기업의 객관화된 대책 수준을 기준으로 제한된 투자금액 안에서의 무작위 투자가 이루어진 경우의 수를 모집단 개수만큼 생성하는 방식을 사용한다. 초기해는 다음세대 생성을 위한 해집단으로 초기해 생성 이후 유전자 연산에 따라 다음세대를 생성한다.

선택은 엘리트 유전자(적합도가 높은 유전자)를 선별하는 과정으로서 이전세대에서 개체를 선택하여 다음세대를 구성한다. 본 연구에서는 순위 선택(rank selection) 방법을 사용하여 적합도가 높은 유전자를 선택한다. 적합도는 피해액이 가장 적은 유전자를 구별하기 위해 설정하였다.

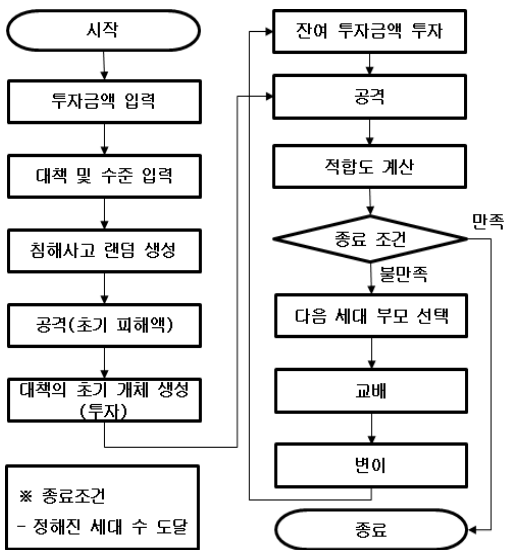
교배는 이전 세대에서 선택된 엘리트 유전자들이 부모가 되고 부모의 유전자를 사용하여 하나 이상의 자손을 생성하는 연산으로 여러 가지 교배 방식 중 일반적인 교배방식인 한 지점 교차(one point crossover)방식을 사용하여 진행하였다. 한 지점 교차 방식은 한 개의 교차 포인트가 선택되면 교차 포인트를 기준으로 교배를 진행하는 방식이다.

돌연변이는 유전자 세대 반복을 통해 얻어지는 해가 해공간의 제한성을 극복하고 새로운 탐색 해

들을 얻는 연산이다. 돌연변이 연산 방식 중 스왑 변이(swap mutation)방식과 무작위 리셋(random resetting)을 사용하며 스왑 변이 방법은 무작위로 염색체의 두 위치를 선택하고 값을 교환하는 방식이고 무작위 리셋 방법은 허용된 집합의 값을 무작위로 선택된 유전자에 할당하는 방식이다.

본 연구에서는 제한된 투자금액이라는 제약으로 인해 엘리트 유전자를 교배한 모든 다음세대 해를 활용할 수 없다. 예를 들면 엘리트 유전자 교배 후 생성된 정보보호 대책 유전자 중, 제한된 투자금액을 초과하는 유전자가 발생할 가능성이 있다. 이런 유전자는 다음세대 유전자로 적합하지 않기 때문에 본 연구에서는 교배 후 생성된 유전자 중 적합한 유전자를 선별하고 모집단 개수에서 모자란 개수만큼 무작위 리셋 변이 방식을 활용하여 돌연변이를 생성한다. 또한 스왑 변이 확률을 정의하여 확률만큼 변이를 추가 생성한다. 돌연변이 생성 또한 제한된 투자금액을 초과하지 않는 유전자를 선별한다.

본 연구의 유전자 알고리즘 흐름도는 [그림 1]과 같다. 유전자 알고리즘을 통한 해 탐색 종료는 종료조건에 의해 이루어진다.



[그림 1] 유전자 알고리즘 흐름도

5. 수치 예제

실제 중소기업의 정보보호 투자 현황을 이용하여 본 연구의 모델을 적용하였다. 사례가 된 중소기업의 정보보호 투자 현황은 기존에 보유하고 있는 7개의 정보보호 대책과 신규 도입예정인 1개의 정보보호 대책으로 구성되어 있다.

〈표 2〉 중소기업의 정보보호 투자 현황

대책1 (P/L)	대책2 (P/L)	대책3 (P/L)	대책4 (P/L)	대책5 (P/L)	대책6 (P/L)	대책7 (P/L)
Anti virus (3/7)	취약점 분석 (15/7)	방화벽 (10/8)	IPS (15/8)	WAF (15/8)	교육 (10/5)	관제 (50/8)

P/L : Price/Level(가격 단위 : 백만원).
WAF : Web Application Firewall.

<표 2>는 중소기업의 정보보호 투자 현황을 나타낸다. P/L은 가격(price)과 수준(level)을 뜻한다. 가격은 각 정보보호 대책을 구입하는데 현재까지 투입된 총 누적비용을 뜻하며 수준은 완벽한 보안 수준 대비 보유하고 있는 대책의 상대적인 수준을 뜻한다. 가격의 단위는 백만원이다.

본 연구의 강화비용은 각 정보보호 대책을 구입하는데 현재까지 투입된 총 누적비용을 수준으로 나눈 값으로 가정한다. <표 2>를 이용하여 본 논문에 적용 가능한 속성 값들을 구성하면 <표 3>과 같다. <표 3>의 보호대상 정보자산(asset)은 각 정보보호 대책이 방어하는 대상을 의미하며 강화비용 또한 단위는 백만원이다. <표 3>에서 대책 8은 신규 도입예정인 대책으로 수준을 0으로 설정하였다.

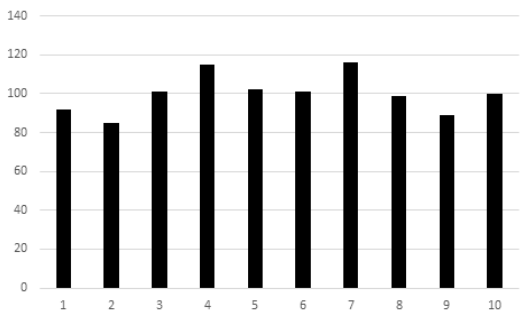
그 이외의 변수들은 침해사고 개수 1,000개(n = 1,000), 대책 수 10개(m = 10), 초기 인구 집단 40명, 엘리트 유전자 개수 6개로 설정하였다. 투자금액은 해당 기업의 금년 정보보호 예산인 2,000만원으로 설정하였다. 초기 인구 집단은 초기 투자가 이루어진 대책들의 조합을 의미한다.

침해사고 1,000개에 대한 수준분포는 [그림 2]와 같다. 생성된 침해사고는 각각 위험 수준 및 공격

목표가 설정되며 공격목표와 대책의 보호목표를 매핑하여 피해액을 산정한다. 실제 사례에서는 하나의 침해사고가 여러 자산을 공격할 수 있지만 본 연구에서는 1,000개의 침해사고를 랜덤하게 생성하였기 때문에 하나의 침해사고가 하나의 자산을 공격한다고(피해를 줄 수 있다고) 가정하였다.

〈표 3〉 투자 시나리오

	대책 1	대책 2	대책 3	대책 4	대책 5	대책 6	대책 7	대책 8
구분	SW 1	SW 2	HW 1	HW 2	SW 3	Edu 1	SO	Edu 2
보호자산	1	2	3	4	5	6	7	6
수준	7	7	8	8	8	5	8	0
강화비용	0.4	2.1	1.3	1.9	1.9	2	6.3	2



[그림 2] 침해사고 수준 분포

본 연구에서는 높은 대책의 수준은 낮은 수준의 침해사고를 완벽히 예방한다고 가정한다. 각 침해사고의 공격목표와 각 대책의 방어목표를 매핑하여 침해사고의 수준이 대책의 수준보다 높을 시 수준 차에 따라 초기 피해액을 산정한다. 초기 피해액 산정 이후 유전자 알고리즘을 통해 대책의 수준을 강화시키며 총 피해액이 적은 대책 조합을 토대로 대책 수준 강화를 반복하여 최적 대책 조합 수준을 도출한다.

입력된 정보보호 대책과 침해사고에 대한 초기 총 피해액은 9,652,963원이며, 제한된 투자금액 내에서의 최초투자를 무작위로 진행하여 초기 인구를 생성하고, 초기 인구 생성 후 적합도가 가장 높은 6개의 엘리트 유전자를 선택하였다. <표 4>는 초기 인구와 적합도가 가장 높은 엘리트 유전자를 나타낸다. 적합도가 가장 높은 엘리트 유전자는 <표 4>에서 굵은 글씨와 밑줄로 표시하였다.

〈표 4〉 초기세대와 엘리트 유전자

번호	대책 1	대책 2	대책 3	대책 4	대책 5	대책 6	대책 7	대책 8
1	7	7	8	8	8	5	8	3
2	10	10	8	8	8	5	8	0
3	10	8	8	9	10	9	8	0
4	7	7	8	8	8	5	8	2
5	7	7	10	8	10	5	8	2
6	7	7	10	10	8	5	8	0
7	**10**	**10**	**9**	**9**	**8**	**5**	**8**	**4**
8	**7**	**7**	**8**	**8**	**9**	**5**	**8**	**6**
9	7	7	8	8	10	5	10	1
10	7	9	9	8	8	5	8	1
11	7	7	8	8	8	7	8	3
12	8	7	8	8	8	5	8	2
13	7	7	10	10	8	5	8	1
14	7	7	8	8	8	5	8	4
15	7	7	8	8	8	6	8	2
16	7	7	8	8	8	5	8	5
17	7	7	10	8	8	5	8	4
18	**8**	**7**	**8**	**8**	**9**	**5**	**8**	**8**
19	7	7	8	8	8	10	8	0
20	7	10	8	10	8	5	8	1
21	7	10	8	8	8	7	8	0
22	7	7	8	8	8	5	9	0
23	7	7	8	10	8	5	10	0
24	**7**	**7**	**8**	**9**	**8**	**8**	**8**	**6**
25	7	9	8	9	8	7	8	0
26	7	10	10	8	8	10	8	0
27	7	8	8	8	9	7	8	0
28	7	10	8	8	8	9	8	0
29	7	7	9	8	9	5	8	2
30	**7**	**7**	**9**	**8**	**8**	**5**	**8**	**9**
31	7	7	8	8	8	5	9	0
32	9	10	10	9	8	5	8	0
33	7	8	8	8	8	8	8	2
34	7	7	9	8	8	5	8	6
35	7	7	9	9	8	5	9	3
36	7	7	8	8	8	7	8	4
37	7	10	8	10	8	5	9	0
38	7	10	8	8	8	8	8	0
39	7	7	8	8	9	5	8	5
40	**7**	**7**	**8**	**8**	**8**	**5**	**8**	**7**

교배는 한 지점 교차를 활용하였으며, 교차 시 제한된 투자금액을 초과하는 유전자는 제외시켰다. 따라서 본 연구에서는 교배 후 해집단 개수에서 모자란 유전자 수만큼 무작위 리셋 방식으로 돌연변이를 발생시켰다. 그 후 20%의 확률로 스왑변이 방식으로 무작위 두 개의 유전자를 교환하는 방법을 사용하였으며, 변이 또한 제한된 투자금액을 넘지 않는 범위에서만 생성할 수 있도록 설계하였다. 초기 인구에 대한 다음 세대 유전자 및 엘리트 유전자는 <표 5>와 같다.

〈표 5〉 2세대 유전자와 엘리트 유전자

번호	대책 1	대책 2	대책 3	대책 4	대책 5	대책 6	대책 7	대책 8
1	**7**	**7**	**8**	**9**	**8**	**8**	**8**	**6**
2	7	7	8	9	9	5	8	8
3	7	7	8	9	8	5	8	9
4	7	7	8	9	8	5	8	4
5	7	7	8	9	8	5	8	7
6	7	7	8	9	9	5	8	6
7	**8**	**7**	**8**	**8**	**8**	**8**	**8**	**6**
8	**8**	**7**	**8**	**8**	**9**	**5**	**8**	**8**
9	8	7	8	8	8	5	8	9
10	8	7	8	8	8	5	8	4
11	8	7	8	8	8	5	8	7
12	8	7	8	8	9	5	8	6
13	**7**	**7**	**9**	**8**	**8**	**8**	**8**	**6**
14	7	7	9	8	9	5	8	8
15	7	7	9	8	8	5	8	9
16	7	7	9	8	8	5	8	4
17	7	7	9	8	8	5	8	7
18	7	7	9	8	9	5	8	6
19	10	10	9	9	8	5	8	4
20	7	7	8	8	8	8	8	6
21	7	7	8	8	9	5	8	8
22	7	7	8	8	8	5	8	9
23	7	7	8	8	8	5	8	4
24	7	7	8	8	8	5	8	7
25	7	7	8	8	9	5	8	6
26	**7**	**7**	**8**	**8**	**8**	**8**	**8**	**6**
27	7	7	8	8	9	5	8	8
28	7	7	8	8	8	5	8	9
29	7	7	8	8	8	5	8	4
30	7	7	8	8	8	5	8	7
31	7	7	8	8	9	5	8	6
32	9	10	8	8	8	8	8	3
33	10	7	8	9	8	5	9	5
34	7	7	9	9	8	5	9	5
35	10	9	8	8	8	5	8	4
36	7	7	8	8	10	5	8	8
37	7	7	8	8	8	5	9	3
38	7	7	8	8	8	9	8	5
39	7	7	8	8	8	5	8	6
40	**7**	**7**	**8**	**8**	**9**	**7**	**8**	**6**

[그림 3] 세대별 피해액

[그림 3]은 각 세대별 최소 피해액을 통해 최적해 탐색까지의 과정을 그래프로 나타내었다.

여러 예제로 시험해본 결과 30세대 이내에서 모두 최적해가 도출되었기 때문에, 본 연구의 유전자 알고리즘은 30세대에 도달하면 세대 반복을 종료한다. <표 6>에서는 시나리오에서의 정보보호 대책 투자 최적해를 나타낸다. 최적 정보보호 대책 구성은 초기 총 피해액 9,652,963원에서 2,930,600원으로 6,722,363원만큼 피해를 최소화 하였으며, 제한된 투자금액 중 300,000원을 제외한 19,700,000원을 사용하였다.

〈표 6〉 최적 대책 구성

	대책 1	대책 2	대책 3	대책 4	대책 5	대책 6	대책 7	대책 8
수준	8	7	9	8	8	7	8	7

수치예제는 시나리오를 통해 본 연구의 투자 최적화 모델을 적용하였다. 시나리오에서 유전자 알고리즘 최적해 세대는 모두 20세대 이하에서 탐색되었다. 이는 본 연구의 제약조건인 제한된 투자

금액 범위 안에서의 탐색과 기존 정보보호 대책의 수준 이하의 해 탐색은 제외하였기 때문으로 보인다. 도출된 정보보호 대책 최적 조합은 피해액을 최소화하고 각 기존 정보보호 대책에 대한 강화 방안 및 신규 정보보호 대책의 도입 수준을 제시한다.

6. 결 론

본 연구의 유전자 알고리즘은 JAVA를 사용하여 프로그램을 구현하였으며 기존 유전자 알고리즘의 연산을 논문의 특성에 맞게 응용하여 정보보호 투자 최적화 시스템을 개발하였다. 기존의 유전자 알고리즘을 활용한 정보보호 대책 포트폴리오 최적화 연구에서는 대책의 수준을 고려하지 않고 침해사고에 대한 피해액을 산정하였으나 이는 현실을 반영하는데 한계가 있다. 따라서 본 연구에서는 정보보호 대책의 도입여부뿐만 아니라 정보보호 대책의 도입수준(대책별 투자액)과 기존에 보유하고 있는 정보보호 대책에 대해서도 수준을 강화할 수 있는 방법을 제시하였다.

본 연구에서 제시한 최적화 방법을 적용하면 기업의 정보보호 투자 예산, 기존 대책 수준을 고려할 수 있기 때문에 기존 정보보호 대책 투자 최적화 연구에서 제시되었던 도입여부 의사결정보다 자세한 의사결정 지원을 할 수 있을 것이라 기대한다. 또한 이진표현이 아닌 정수표현을 활용하여 유전자 알고리즘 방법론의 장점을 극대화하였다. 기존 연구에서 이진표현을 사용하여 정보보호 대책 도입여부만 고려하여 최적 정보보호 대책 조합을 도출한 것보다 구체적으로 해당 대책에 얼마의 금액을 투자하여야 하는지에 대한 의사결정을 지원한다. 일반적인 정보보호 투자 현황에서 정보보호 대책의 개수가 10개를 넘지 않는 점을 고려할 때, 정보보호 대책의 도입여부를 고려하는 이진표현보다 각 대책에 대한 적정 투자수준 의사결정을 지원하는 정수표현의 유전자 알고리즘의 효율이 우수하다고 할 수 있다.

본 연구의 한계점은 다음과 같다. 첫째, 모든 침해사고와 대책들의 수준을 객관화할 수 있고, 높은 수준의 대책은 낮은 수준의 침해사고를 완벽히 예방한다고 가정하였다. 하지만 실제 사례를 살펴보면 낮은 수준의 침해사고가 높은 수준의 대책에 대해서 피해를 발생시킬 가능성도 존재한다. 둘째, 침해사고의 속성들을 랜덤하게 생성하기 때문에 침해사고의 속성에 따라 매번 결과가 달라질 수 있다. 향후 실제 침해사고 데이터를 수치화하고 적용하면 좀 더 현실적인 방법론이 될 수 있을 것이다. 셋째, 실무적인 관점에서의 검증이 필요하다. 실무전문가의 의견을 수렴하는 정성적인 기법과 본 연구의 결과를 비교하여 보편적인 적용에 대해 검증할 필요가 있다.

참고문헌

공희경, 전효정, 김태성, “AHP를 이용한 정보보호투자 의사결정에 대한 연구”, *Journal of Information Technology Applications and Management*, 제15권, 제1호, 2008, 139-152.

과학기술정보통신부, 2018 정보보호실태조사, 2019.

김길환, 양원석, 김태성, “유전자 알고리즘을 이용한 정보보호 대책 투자 포트폴리오의 최적화”, *한국통신학회논문지*, 제43권, 제2호, 2018, 439-451.

김동욱, 이원영, “유전자 알고리즘을 이용한 프로젝트 포트폴리오 투입인력 최적화 모델에 관한 연구”, *한국IT서비스학회지*, 제17권, 제4호, 101-117.

양원석, 김태성, 박현민, “확률모형을 이용한 정보보호 투자 포트폴리오 분석”, *한국경영과학회지*, 제34권, 제3호, 2009, 155-163.

Benaroch, M., “Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making”, *Information Systems Research*, Vol.29, No.2, 2018, 315-340.

Bodin, L.D., L.A. Gordon, and M.P. Loeb, "Evaluating information security investments using the analytic hierarchy process", *Communications of the ACM*, Vol.48, No.2, 2005, 78-83.

Fielder, A., E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment", *Decision Support Systems*, Vol.86, 2016, 13-23.

Gupta, M., J. Rees, A. Chaturvedi, and J. Chi, "Matching information security vulnerabilities to organizational security profiles : a genetic algorithm approach", *Decision Support Systems*, Vol.41, No.3, 2006, 592-603.

Houmb, S.H. and V.N. Franqueira, "Estimating ToE risk level using CVSS", *2009 International Conference on Availability, Reliability and Security*, 2009, 718-725.

Nespoli, P., D. Papamartzivanos, F.G. Mármol, and G. Kambourakis, "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks", *IEEE Communications Surveys & Tutorials*, Vol.20, No.2, 2018, 1361-1396.

About the Authors

임 정 현 (lowly13@naver.com)

충북대학교 컴퓨터공학과에서 학사 학위를 취득하였다. 현재 충북대학교 경영정보학과 석사과정에 재학 중이다. 주요 관심 분야는 정보통신과 정보보호 분야의 정책 및 투자, 경영과학, 개인정보보호이다.

김 태 성 (kimts@cbnu.ac.kr)

한국과학기술원 산업경영학과에서 박사를 취득하고, 한국전자통신연구원 정보통신기술경영연구소에서 근무한 후, 현재 충북대학교 경영정보학과에서 교수로 재직하고 있으며 보안경제연구소 소장을 맡고 있다. University of North Carolina at Charlotte과 Arizona State University에서 Visiting Professor와 Visiting Scholar로 각각 근무하였다. 국내외 경영과학, 정보통신, 정보보호 관련 학술지 및 학술대회에서 논문을 발표하였으며, 주요 관심 분야는 정보통신과 정보보호 분야의 경영 및 정책 의사결정이다.