DBpia

논문 18-43-02-30 The Journal of Korean Institute of Communications and Information Sciences '18-02 Vol.43 No.02
https://doi.org/10.7840/kics.2018.43.2.439

유전자 알고리즘을 이용한 정보보호 대책 투자 포트폴리오의 최적화

김 길 환◆, 양 원 석°, 김 태 성*

Optimization of Information Security Investment Portfolios Using a Genetic Algorithm

Kilhwan Kim◆, Won Seok Yang°, Tae-Sung Kim*

요 약

빅데이터, 인터넷, IoT, 소셜 미디어의 급증에 따라 보안 침해사고의 규모 및 유형도 증가하고 있다. 침해사고 유형의 다양화에 따라 이를 방어하기 위한 정보보호 대책도 세분화되고 다양해지고 있다. 따라서 정부 및 기업의 정보보호 대책의 포트폴리오 구성 방안은 매우 복잡한 의사결정 문제로 귀결된다. 본 연구에서는 투자비용 관점에서 정보보호 대책의 최적 포트폴리오 구성 방안을 제시하고 유전자 알고리즘을 이용하여 투자비용 최소화 방안을 도출한다. 보안 침해사고의 발생률, 피해액, 정보보호 대책의 투자비용, 그리고 보안 침해사고에 대한 각 정보보호 대책의 방어확률이 알려져 있다는 가정 하에 정보보호 대책의 포트폴리오 구성에 따른 투자비용을 최적화 모형으로 정식화하고 유전자 알고리즘을 이용하여 최적해를 도출한다. 마지막으로 다양한 정보보호 운영 시나리오를 고려하여 본 논문에서 제시한 최적화 방법론의 수치 예제를 다룬다.

Key Words : information security, risk management, countermeasure selection, genetic algorithm, multi-objective optimization

ABSTRACT

We propose an optimization method of the investment cost for countermeasure portfolios in information security using a genetic algorithm. With the rate of information security breaches, the expected damage cost by security breaches, and the rates of countermeasures filtering security breaches, we formulate the selection problem of an optimal countermeasure portfolio for information security as a mathematical optimization problem based on the investment cost and develop a solution procedure based on a genetic algorithm. In addition, we present numerical examples, considering various scenarios in information security.

Ⅰ. 서 론

빅데이터, 인터넷, IoT, 소셜 미디어가 증대됨에 따라 공공기관 및 기업에서는 다양한 종류의 보안 침해사고에 노출되고 있다[1]. 최근 정보보호 침해사고의 유형이 다양해졌을 뿐만 아니라, 침해사고의 발생 빈

※ 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"(과제번호 H2101-17-1001) 및 충북대학교 보안경제연구소의 지원을 받아 수행되었음.
◆ First Author : (ORCID:0000-0002-0577-7906)Department of Management Engineering, Sangmyung University, khkim@smu.ac.kr, 정회원
° Corresponding Author : Department of Business Administration, Hannam University, wonsyang@hnu.kr, 정회원
* Department of Management Information Systems, Chungbuk National University, kimts@cbnu.ac.kr, 종신회원
논문번호 : KICS2017-11-370, Received November 30, 2017; Revised January 11, 2018; Accepted January 11, 2018

www.dbpia.co.kr

도와 피해액의 규모도 점차 증가하고 있다. 증대되는 보안 침해 위협에 대처하기 위해 공공기관 및 기업에서는 다양한 정보보호 대책(countermeasures or controls)에 투자하고 있다[2]. 한두 가지 정보보호 대책만으로는 고도화되는 보안 침해사고에 효과적으로 대처할 수 없기 때문에 정보보호 대책에서는 특정 영역에 물리적인 접근 통제부터, 생체 인식을 통한 접근 권한 통제, 방화벽, 정보 보안 교육, 정보 보안 관리 체계의 점검 및 개선 등 매우 폭넓은 방식의 대책을 모두 포괄한다[3].

일반적으로 각각의 정보보호 대책이 방어하는 정보보호 위협이 서로 상이하다. 한 가지 보안 위협을 매우 많은 대책들이 서로 중복적으로 방어할 수도 있고, 어떤 위협에 대해서는 이를 방어해주는 대책이 거의 없을 수도 있다. 하나의 정보보호 대책이 여러 위협을 동시에 방어할 수도 있으며, 어느 하나의 침해 유형을 막기 위해서는 여러 대책이 서로 보완적으로 필요한 경우도 있다. 따라서 보안 침해사고 유형의 증대 및 다변화, 정보보호 대책의 다양화 및 세분화, 그리고 이들 간의 복잡한 상호 관계를 고려할 때, 기업 및 공공기관에서 최적의 정보보호 대책 투자 포트폴리오를 결정하는 것은 매우 복잡한 의사결정 문제로 귀결된다.

정보보호 대책에 대한 최적 투자 포트폴리오를 결정하는 의사결정 문제가 복잡해지는 이유는 크게 다음의 네 가지로 요약된다. 첫째, 정보보호 투자 의사결정 시, 정보보호 대책 투자비용과 보안 침해사고 전체 피해액의 사이에 적절한 균형이 중요하다. 정보보호 대책에 대한 투자가 증가하면 침해사고 피해액은 감소하지만 투자비용은 증가한다. 반면, 정보보호 대책에 대한 투자가 감소하면 투자비용은 감소하지만 침해사고 피해액은 증가한다. 둘째, 정보보호 대책의 포괄 범위(coverage)와 투자의 중복성 간에 적절한 균형이 고려되어야 한다. 정보보호 대책이 방어하는 침해사고의 범위를 최대한 확장하면 동일한 침해 위협에 대해 중복적이고 불필요한 투자가 발생하게 된다. 반면, 투자의 중복성을 최소화하면 정보보호 대책이 방어하는 포괄 범위가 너무 협소해지게 된다. 셋째, 개별 침해 위협의 발생률과 피해액이 침해사고 유형에 따라 다양하므로 발생 위험도에 따라 차별화된 방어 수준을 확보해야 한다. 즉, 전체적인 방어 체계를 적절히 유지하면서 중요한 침해사고는 더 집중하여 방어할 수 있도록 효과적으로 정보보호 대책을 구성해 나가야 한다. 넷째, 개별 침해사고 유형의 발생률과 정보보호 대책이 방어하는 침해 위험의 방어 비율이 시시각각 변화한다. 정보 환경의 급변에 따라 다양한 신종 및 변종 위협이 빠르게 나타나고 사라지고 있다. 따라서 개별 대책의 방어 범위와 비율을 끊임없이 재평가하고 정보보호 대책의 투자 포트폴리오를 신속히 재구성해야 한다.

지금까지 논의한 복잡성을 고려하면, 기존의 정성적인 보안 지침과 체크리스트만으로는 정보보호 대책의 투자 포트폴리오에 대한 의사결정 문제를 해결하기 어렵고 데이터와 계량적인 모형을 통해 최적의 의사결정을 수행하는 노력이 필요하다.

본 연구에서는 유전자 알고리즘을 이용하여 정보보호 대책에 대한 최적 투자 포트폴리오를 도출하는 방법을 제안한다. 보안 침해사고의 발생 빈도, 평균 피해액, 정보보호 대책의 평균 투자비용, 그리고 각 정보보호 대책이 각 보안 침해사고를 방어하는 비율을 알고 있다는 가정 하에 정보보호 대책의 투자 포트폴리오 의사결정 문제를 수학적 최적화 모형으로 정식화하고 유전자 알고리즘을 이용하여 최적화 모형의 해를 탐색하는 방법을 제시한다. (모형의 모수 추정은 [4]에 적용된 방법을 활용할 수 있다). 아울러, 본 논문에서 제시한 최적화 방법론의 적용가능성을 확인하기 위해 수치 예제를 다루고 제시된 방법론의 성능을 분석하기 위해 실험을 수행하였다.

본 연구에서 제안된 방법을 이용하면 정보보호 담당자는 복잡한 정보보호 대책 포트폴리오 구성에 대한 의사결정을 효과적으로 수행할 수 있다. 아울러, 보안 침해 위협의 변화에 따라 현재의 포트폴리오를 재평가하고 보완해야 할 부분이 무엇인지를 신속하게 결정할 수 있다. 마지막으로, 새로운 정보보호 대책 도입에 따른 침해사고 유형별 방어율의 변화와 기대되는 침해 피해액을 수치적으로 계산할 수 있어 정보보호 담당 실무자들의 과학적인 의사결정에 도움이 되리라 기대한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 문헌을 고찰한다. 3장에서는 본 논문에서 해결하고자 하는 문제를 수학적 최적화 모형으로 정식화한다. 4장에서는 정식화된 최적화 모형을 해결하는 절차를 제시한다. 5장에서는 수치 예제를 통하여 제시된 방법이 어떻게 적용되는지를 보이고, 제안된 방법의 성능에 대한 실험을 수행한다. 마지막으로 6장에서는 본 논문의 결론과 향후 발전 방향을 제시한다.

Ⅱ. 문헌 고찰

제한된 예산 하에서 정보보호 대책에 대한 적절한 포트폴리오를 구성하는 문제에 관한 연구는 다수 존

www.dbpia.co.kr

재한다[4-11]. 이러한 연구는 크게 정성적인 접근 방법과 정량적인 접근 방법으로 나누어 볼 수 있다.

정성적인 연구 방법은 최적의 투자 포트폴리오 구성에 대한 정량적인 해법을 주기 보다는 정보보호 투자의 가이드가 될 수 있는 체크리스트로서의 역할을 해주는 것을 목표로 한다. 정성적인 접근 방법의 대표적 연구는 다음과 같다[5-7]. Alberts and Dorofee(2002)는 OCTAVE 시스템에서 정보보호의 위험 요소를 정성적으로 평가하는 방법을 제시하였다[5]. Bistarelli et al.(2007)은 정보 시스템을 사이버 공격으로부터 보호하기 위하여 사용해야 할 정보보호 대책을 선택하는 정성적인 접근 방법을 제시하였다[6]. Egan and Mather(2004)는 정보보호 대책이 포괄할 영역을 결정하는 전략적 의사결정을 위한 체크리스트를 제시하였다[7].

정량적인 연구 방법에서는 현재의 예산 제약과 정보보호 위협 하에 정보보호 대책의 최적 포트폴리오를 정량적으로 제시하는 것을 목표로 한다. 그러나 Baker et al.(2007)이 지적하였듯이 정보보호 대책의 효과를 정확하게 측정하는 신뢰도 높은 방법은 아직 존재하지 않으며 기업의 정보보호 담당자들도 이를 수치로 제시하는 데 어려움을 느끼는 편이다[8]. 그럼에도 불구하고, 정보보호 위협의 종류와 정보보호 대책의 다양성이 지속적으로 증가하는 상황에서 정성적인 가이드만으로는 복잡한 의사결정에 한계를 가지기 때문에 정보보호 대책의 최적 포트폴리오를 결정하는 문제에 대한 정량적 접근 방법에 관한 연구가 계속되어 왔다[4,9-11].

정량적 접근 방법 중에 본 연구와 관련 있는 연구는 다음과 같다. Gupta et al.(2006)은 발생 가능한 보안 위협과 해당 위협을 방어할 수 있는 대책들을 나열한 후, 보안 위협을 최대로 방어하면서 투자 비용을 최소화하는 정보보호 대책 포트폴리오를 선택하는 정량적 방법을 제시하였다[9]. 이 연구에서는 위협을 최대로 방어하는 목적과 정보보호 대책 투자비용을 최소화하는 목적을 동시에 만족하도록 다중 목적 최적화를 수행하는 유전자 알고리즘을 이용하여 최적 포트폴리오를 도출하였다. 그러나 이 연구는 다음과 같은 한계점을 가진다. 첫째, 보안 위협 별로 발생할 수 있는 발생률이나 침해 시 발생하는 피해액을 고려하지 않고 보안 위협을 방어하는 개수를 목적으로 하여 최적 포트폴리오를 도출하기 때문에, 피해액이나 발생률이 높은 위협이나 그렇지 않은 위협이나 동등하게 방어 수준이 결정된다. 둘째, 특정 정보보호 대책이 특정 보안 위협을 방어하는 비율을 1, 1/2, 0으로만 모형화하여 변종 공격이 다양화해지는 현실에서 보호대책이 보안 위협 별로 방어하는 방어 비율을 더 세분화하여 표현하기가 어렵다.

Rees et al.(2011)은 퍼지 로직과 유전자 알고리즘을 이용하여 정보보호 대책의 최적 포트폴리오를 계산하는 방법을 제시하였다[4]. 이 연구에서는 먼저 퍼지 로직을 이용하여 불확실성 하에서의 침해사고 위협의 발생 빈도, 정보보호 대책의 방어 비율, 그리고 침해사고 피해액을 표현한다. 그리고 침해사고에서 발생하는 총 기대 피해액을 퍼지 로직의 합을 이용하여 계산하고, 독립성 가정 하에 작동하는 정보보호 대책들의 결합 방어 비율을 퍼지 로직의 곱을 이용하여 계산한다. 이를 이용하여 불확실성 하에서의 정보보호 대책의 포트폴리오의 기대 피해액을 계산한다. 이렇게 퍼지 로직을 이용하여 계산된 피해 금액과 정보보호 대책의 투자 비용을 입력으로 하여 유전자 알고리즘으로 정보보호 대책의 최적 포트폴리오를 도출해 낸다.

본 연구는 [4]와 유사한 접근 방법을 택한다. 다만 퍼지 로직을 이용하여 침해사고의 발생 빈도, 피해액, 보안 대책의 방어 비율을 표현하여 최적화에 이용하기보다는 각 모수의 점추정치를 이용하여 침해사고의 피해비용과 정보보호 대책 투자 비용의 기대치를 각각 도출하고 유전자 알고리즘을 적용하여 최적의 포트폴리오를 탐색한다. [4]에서는 침해사고 피해액과 정보보호 대책 투자액을 단순 합산하여 최적화를 수행했으나 본 연구에서는 [9]와 유사하게 침해사고 피해액의 최소화와 정보보호 대책 투자 금액의 최소화를 동시에 고려하는 다중 목적 하의 유전자 알고리즘을 이용한다.

본 연구에서 이러한 접근방법을 택한 이유는 점추정치를 이용하는 방법과 다중 목적을 최적화하는 것이 다음과 같이 현실 문제를 해결하는데 더 적합하다고 판단하기 때문이다. 첫째, 퍼지 로직에 비해 단순한 점추정치를 이용하기 때문에 정보보호 분야의 실무자가 모형의 요소가 최종 결과에 미치는 영향을 이해하기가 쉽다. 퍼지 로직을 이용하는 방법은 이에 익숙하지 않은 실무자가 실제 문제에서 이를 추정하여 모형에 반영하기 쉽지 않다. 둘째, 침해사고의 발생 횟수와 피해액을 정확히 집계하기 어려운 현실을 감안하면, 추정의 불확실성이라는 문제를 모형의 각 요소에 내재시켜 그 결과를 도출하기보다는 침해사고 피해액과 정보보호 대책의 투자비 중 무엇이 더 중요한지에 대해 전략적으로 판단하고, 이에 따른 최적 포트폴리오의 변화를 추적해 보는 것이 의사결정에 도움이 되리라 여겨진다. 예를 들어 현재 침해사고 피해

www.dbpia.co.kr

액의 1/3 정도 밖에 통계에 반영되지 않고 있다면, 이를 각 침해사고의 발생 피해액의 추정치에 불확실성의 요소로 도입하기 보다는 침해사고 피해액에 3배의 가중치를 반영하여 최적화를 수행하고, 특별히 과소평가된 침해사고의 경우 피해액의 점 추정치를 변경해 가며 최적 포트폴리오의 변화를 살펴보는 것이 훨씬 단순하고 이해하기 쉽다.

Sawik(2013)은 침해사고 유형별 발생률, 발생 피해액, 정보보호 대책의 침해사고 방어 비율이 점추정치로 주어진다는 가정 하에 정보보호 대책의 효과가 독립적으로 작용하는 경우 최적 정보보호 대책 포트폴리오 문제가 혼합 정수계획법(mixed integer programming)으로 모형화될 수 있음을 보였다[10]. [10]의 방법은 혼합정수계획법을 이용하므로 유전자 알고리즘과 달리 정확한 전역 최적해를 구할 수 있으나, 침해사고 유형과 정보보호 대책이 20개를 넘어서면 적절한 시간 내에 해를 구하기 어렵다. 최근 침해사고 유형과 정보보호 대책이 증대 및 다변화하여 정보보호 위협에 역동적으로 대처해야 하는 상황을 감안하면 현실 문제에 적용하기 어려운 측면이 있다.

최근 Fielder et al.(2016)은 게임이론과 조합 최적화이론을 결합하여 최적 정보보호 대책을 결정하는 방법을 제시하였다[11]. 아울러 정보보호 대책 관련 기존 연구를 게임이론을 이용한 연구, 최적화이론을 이용한 연구, 실제 데이터를 이용한 연구, 정보보호 대책의 최적 포트폴리오 구성을 위한 연구 등으로 분류하여 제시하였다.

본 연구는 최적화를 위한 수학적 모형 측면에서는 [10]과 유사하게 침해사고 유형별 발생률, 발생 피해액, 정보보호 대책의 각 침해사고 방어 비율의 점추정치를 이용하여 목적 함수를 구성한다. 한편, [10]에서 침해사고 유형 및 정보보호 대책이 증가할수록 최적해를 구하기 어렵다는 단점을 극복하기 위해 최적 포트폴리오를 찾는 알고리즘으로 혼합정수계획법 대신 [4]와 유사한 유전자 알고리즘을 적용한다. 아울러, [10]에서는 정보보호 대책에 대한 예산제약 하에, 기대 피해액을 최소화하는 투자 포트폴리오를 구한 반면, 본 연구에서는 [9]와 같이 정보보호 대책에 대한 투자비와 보안 침해사고의 피해액을 가중치로 조합하는 다중 목적 하의 유전자 알고리즘을 적용한다. 그 이유는 보안 침해사고의 발생 빈도와 피해비용의 추정이 불확실한 상황을 고려할 때, 정보보호 대책에 대한 투자비 대비 피해비용의 가중치를 전략적으로 조정해 가며 최적 투자 포트폴리오의 변화를 의사결정자가 파악할 수 있게 하기 위해서다.

Ⅲ. 모 형

n개의 보안 침해사고 유형과 m개의 정보보호 대책이 시장에 존재한다고 할 때, 본 논문에서는 다음 수치의 점추정치를 산정할 수 있다고 가정한다.

- d_i: 보안 침해사고 i 발생 시 평균 피해금액
- p_i: 한 기간 동안 (예, 월별, 분기별) 보안 침해사고 i의 발생률
- c_j: 한 기간 동안 정보보호 대책 j의 운영비용 (정보보호 대책 j 투자비의 감가상각비 포함)
- q_{ij}: 정보보호 대책 j의 침해사고 i 방어 비율

이때 $i=1,\cdots,n$이고 $j=1,\cdots,m$이다. 아울러, 한 정보보호 대책의 침해사고 방어 비율은 다른 정보보호 대책의 도입 여부에 무관하게 독립적으로 작용된다고 가정한다.

정보보호 대책의 투자 의사결정 변수 x_j는 다음과 같이 정의된다.

$$x_j = \begin{cases} 1, \text{정보보호 대책 } j \text{ 도입} \\ 0, \text{정보보호 대책 } j \text{ 미도입} \end{cases}.$$

정보보호 대책의 투자 포트폴리오를 $\boldsymbol{x}=(x_1,\cdots,x_m)$라 표기한다.

정보보호 대책의 투자 포트폴리오 $\boldsymbol{x}$가 결정되면, 침해사고 i를 방어하지 못해 침해로 이어지는 비율 r_i는 다음과 같이 표현된다.

$$r_i = \prod_{j=1}^{m} (1-q_{ij})^{x_j}.$$

정보보호 대책 투자 포트폴리오 $\boldsymbol{x}$하에서 한 기간 동안 침해사고 i에 의해 발생하는 피해액의 기대치 y_i는 다음과 같다.

$$y_i(\boldsymbol{x}) = d_i p_i r_i = d_i p_i \prod_{j=1}^{m} (1-q_{ij})^{x_j}.$$

정보보호 대책 투자 포트폴리오 $\boldsymbol{x}$하에서 한 기간 동안 기대되는 보안침해사고의 총 피해 비용 $C_1(\boldsymbol{x})$와 정보보호 대책의 운영비용 $C_2(\boldsymbol{x})$는 다음과 같이 계산된다.

www.dbpia.co.kr

$$C_1(\boldsymbol{x}) = \sum_{i=1}^{n} d_i p_i \prod_{j=1}^{m} (1-q_{ij})^{x_j}.$$

$$C_2(\boldsymbol{x}) = \sum_{j=1}^{m} c_j x_j.$$

침해사고 피해비용의 가중치를 w_1 그리고 정보보호 대책 투자비용의 가중치를 w_2라고 하자. 최적 정보보호 대책 포트폴리오 구성 문제는 다음과 같이 가중치 벡터 $\boldsymbol{w}=(w_1,w_2)$가 주어져 있을 때 포트폴리오 $\boldsymbol{x}$의 가중 비용 $C(\boldsymbol{x};\boldsymbol{w})$를 최소화하는 문제가 된다.

$$\textit{minimize} \quad C(\boldsymbol{x};\boldsymbol{w}) = w_1 C_1(\boldsymbol{x}) + w_2 C_2(\boldsymbol{x}).$$
$$\textit{subject to} \quad x_j \in 0,1, \quad j=1,\cdots,m.$$

정보보호 담당자는 현재 추정치에 대한 과소 또는 과대 추정에 대한 판단, 미래의 침해 사고 발생률 및 피해액의 추이, 미래의 정보보호 대책 운영비용의 추이 등을 고려하여 두 비용에 대한 가중치를 변경해 가며 최적 정보보호 대책 포트폴리오를 구성한다.

Ⅳ. 최적해 탐색 방법

정보보호 대책의 최적 투자 포트폴리오를 찾기 위해서는 투자 포트폴리오의 가능해 공간인 $\{\ \boldsymbol{x}; x_j \in 0,1, j=1,\cdots,m\}$를 탐색해야 한다. x_j가 0 또는 1이므로 총 2^m개의 가능해가 존재한다. 정보보호 대책이 20개만 되어도 가능해의 개수가 1,048,576개나 된다. 정보보호 대책의 개수가 증가하면 모든 가능해를 탐색하기 어렵기 때문에 본 연구에서는 유전자 알고리즘이라는 메타휴리스틱 방법을 사용하여 최적해를 탐색한다[12].

유전자 알고리즘으로 최적해를 탐색하기 위해서는 해를 유전자로 표현하는 방식, 해의 적합도를 평가하는 함수, 초기 인구의 생성 방법 및 세대 진화의 반복 횟수, 세대 진화의 연산 방법인 적자선택(selection), 교차(crossover), 변이(mutation)에 대한 설계가 필요하다.

정보보호 대책 투자 포트폴리오 $\boldsymbol{x}$는 각 자리의 가능한 값이 0과 1이므로 길이가 m인 이진표현으로 유전자를 나타낸다. 유전자의 적합성을 평가하는 평가함수는 해당 유전자에서의 침해사고의 피해비용과 정보보호 대책의 운영비용을 적절히 고려해야 한다. 정보보호 대책의 운영비용은 모든 가능한 정보보호 대책을 도입한 비용보다 커질 수 없고 침해사고의 피해비용은 어떠한 정보보호 대책도 도입하지 않을 때보다 커질 수 없다. 따라서 $C_1(\boldsymbol{x})$, $C_2(\boldsymbol{x})$, $C(\boldsymbol{x};\boldsymbol{w})$에 대해 다음이 성립한다.

$$C_1(\boldsymbol{x}) \le C_1(\boldsymbol{0}) = \sum_{i=1}^{n} d_i p_i.$$

$$C_2(\boldsymbol{x}) \le C_2(\boldsymbol{1}) = \sum_{j=1}^{m} c_j.$$

$$C(\boldsymbol{x};\boldsymbol{w}) \le w_1 C_1(\boldsymbol{0}) + w_2 C_2(\boldsymbol{1}) = C_{upper}(\bullet;\boldsymbol{w}).$$

이때 $\boldsymbol{0}$과 $\boldsymbol{1}$은 모든 요소가 0과 1인 벡터이다. $C_{upper}(\bullet;\boldsymbol{w})$는 가중치 벡터 $\boldsymbol{w}$하에서 가중합 비용 $C(\boldsymbol{x};\boldsymbol{w})$이 가질 수 있는 상한 값 중 하나이다.

정보보호 대책 포트폴리오 $\boldsymbol{x}$의 적합도 $f(\boldsymbol{x};\boldsymbol{w})$는 다음과 같이 해당 포트폴리오가 도입될 때 $C_{upper}(\bullet;\boldsymbol{w})$에 비해 감소되는 가중합 비용으로 정의한다.

$$\begin{aligned} f(\boldsymbol{x};\boldsymbol{w}) &= C_{upper}(\bullet;\boldsymbol{w}) - C(\boldsymbol{x};\boldsymbol{w}) \\ &= w_1[C_1(\boldsymbol{0}) - C_1(\boldsymbol{x})] + w_2[C_2(\boldsymbol{1}) - C_2(\boldsymbol{x})] \end{aligned}$$

어떠한 해에 대해서도 가중합 비용은 $C_{upper}(\bullet;\boldsymbol{w})$에 비해 작으므로 적합도 $f(\boldsymbol{x};\boldsymbol{w})$는 항상 비음의 값을 갖는다.

유전자 알고리즘에서 적합한 초기 인구 수 N은 문제에 따라 다르다. N이 너무 작으면 해 공간을 충분히 탐색하기 어렵고 N이 너무 크면 해의 적합도 개선은 미미하며 계산 시간만 증가한다. 본 연구에서는 초기 인구수 N을 m과 $2m$ 사이의 값으로 설정한다. 각 유전자가 0과 1이 될 확률을 1/2로 하여 무작위 추출을 통해 초기 세대를 생성한다.

정해진 반복 횟수에 도달하거나 최근 K 세대의 적합도 상승이 일정 수준을 계속 넘지 않으면 유전자 알고리즘의 세대 반복을 종료한다. 이 수준은 다음과 같이 유전자 알고리즘 첫 세대의 최우수 해인 $\boldsymbol{x}_0^*$의 가중합 비용의 ϵ배로 정한다.

$$\epsilon[w_1 C_1(\boldsymbol{x}_0^*;\boldsymbol{w}) + w_2 C_2(\boldsymbol{x}_0^*;\boldsymbol{w})].$$

초기해의 가중합 비용의 ϵ 정도만큼도 개선되지 않기를 $K=50$ 세대를 반복하면 유전자 알고리즘을 종료하고 그때까지의 세대 중 가장 우수한 해를 최적해

www.dbpia.co.kr

로 선택한다. ϵ은 0.001과 같이 매우 작은 값으로 정의된다.

다음 세대를 생성하기 위한 반복에서는 먼저 E명의 현 세대의 최우수 개체를 선택하여 다음 세대로 보존하는 엘리트주의(elitism)를 구현한다[13]. 다음으로 N개의 개체 중 적합도가 높은 개체를 중복 추출을 허용하여 부모가 될 $(N-E)$의 개체를 선택한다. 본 연구에서는 적합도 등수-기반 선택을 수행하였다. 적합도에 따라 등수를 정한 후, r번째 적합도를 가진 개체에 선택 가능성의 척도 $S(r)$을 다음과 같이 부여한다.

$$S(r)=\frac{1}{\frac{N}{3}\sqrt{2\pi}}e^{-\left(\frac{r}{N/3}\right)^2},\ r=1,\cdots,N.$$

그러면 r번째 적합도를 가진 개체가 부모로 선택될 확률 $P_S(r)$은 다음과 같이 주어진다.

$$P_S(r)=S(r)/\sum_{i=1}^{N}S(i),\ r=1,\cdots,N.$$

선택된 부모 객체는 쌍을 이루어 유전자가 교차된다. 본 연구에서는 한지점교차(one-point crossover)로 유전자를 교차시킨다[13]. 유전자 교차를 통해 생성된 자식들은 유전자 변이의 과정을 거친다. 자식 유전자의 각 유전자 자리는 확률 p_m으로 0 또는 1로 무작위 변이를 일으킨다.

V. 수치 예제

본 연구에서는 다양한 정보보호 운영 시나리오를 고려하여 다음과 같이 확률적으로 모형에 적용되는 수치를 생성한다.

- d_i: 각각 $\mu=8$, $\sigma=1.5$인 로그-정규분포를 따른다고 가정
- p_i: 각각 [0.01, 0.1]의 균등분포를 따른다고 가정
- c_j: 각각 $\mu=5$, $\sigma=1$인 로그-정규분포를 따른다고 가정
- q_{ij}: 정보보호 대책 j가 방어하는 침해사고 수 n_i를 먼저 생성. 정보보호 대책의 운영비용이 클수록 더 많은 침해사고에 대응할 수 있게 n_i 생성. 시행횟수가 $(n-1)$, 성공확률을 c_j의 CDF(cumulative distribution function) 값으로 하는 이항분포를 이용하여 n_i를 생성한 후 1을 더해 줌. 그리고 정보보호 대책 j가 방어할 n_i개의 침해사고를 임의 추출. 추출된 침해사고에 대해 방어 비율을 [0.1, 0.95]의 균등분포로 생성. 나머지 침해사고에는 0의 방어비율 부여.

이때 $i=1,\cdots,n$이고 $j=1,\cdots,m$이다.

먼저 침해사고의 유형과 정보보호 대책이 각각 10개인 경우를 다룬다. 즉, $n=10$, $m=10$이다.

Table 1은 침해사고 발생 시의 평균 피해금액과 한 기간 내 각 침해사고의 발생률을 나타낸다.

Table 2는 한 기간 동안 정보보호 대책의 평균 운영비용이다.

Table 3은 정보보호 대책 별로 침해 사고의 방어 비율이다. Fig. 1에서는 방어 비율을 음영으로 표시하였다. 검은 색에 가까울수록 방어 비율이 1에 가깝고 하얀색에 가까울수록 방어 비율이 0에 가깝다.

Table 1. Average amount and rate of information security breach during a period

breach	amount	rate
breach1	1286	0.09
breach2	2111	0.072
breach3	30886	0.068
breach4	3314	0.099
breach5	3619	0.069
breach6	39050	0.074
breach7	5951	0.059
breach8	447	0.063
breach9	1064	0.036
breach10	1528	0.023

Table 2. Average operating cost for each countermeasure during a period

control	amount
ctrl1	886
ctrl2	244
ctrl3	21
ctrl4	299
ctrl5	92
ctrl6	51
ctrl7	119
ctrl8	53
ctrl9	72
ctrl10	79

www.dbpia.co.kr

Table 3. Filtering rate of a countermeasure for each security breach

breach	ctrl1	ctrl2	ctrl3	ctrl4	ctrl5	ctrl6	ctrl7	ctrl8	ctrl9	ctrl10
breach1	0.635	0.655	0	0	0	0.626	0	0.165	0	0
breach2	0.101	0	0.497	0.221	0	0.687	0	0	0.285	0
breach3	0.287	0.859	0	0.225	0.414	0	0	0.296	0.194	0.288
breach4	0.704	0.249	0.18	0.895	0.937	0	0	0.816	0.284	0.554
breach5	0.504	0	0	0.906	0.287	0	0.768	0	0	0
breach6	0.621	0.211	0	0.449	0.372	0	0	0	0	0.402
breach7	0.741	0.853	0.535	0.356	0	0	0.661	0	0.431	0
breach8	0.423	0.658	0	0.713	0	0	0	0.303	0	0
breach9	0.194	0	0	0.152	0.362	0	0	0	0.586	0
breach10	0.399	0.392	0	0	0	0.858	0.799	0.256	0.478	0.729

침해사고 비용의 가중치 w_1과 정보보호 대책 운영 비용의 가중치 w_2의 비율을 Table 4와 같이 변경하며 정보보호 대책의 최적 포트폴리오를 탐색한다.

인구수를 20으로 하고 최대 300번 세대를 반복하도록 설정했다. 단, 초기 세대의 최우수 해의 가중합 비용의 0.001 이상의 개선이 50 세대 동안 일어나지 않으면 반복을 중지하였다.

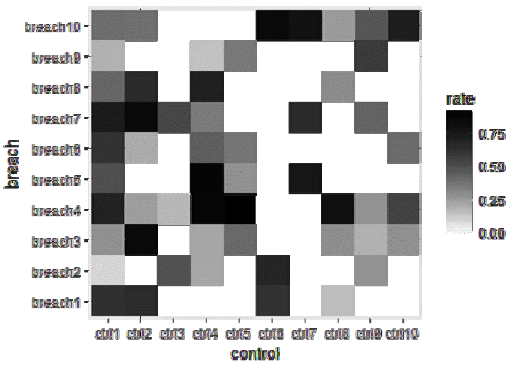


Fig. 1. Filtering rate of a countermeasure for each security breach

Table 4. Weights of the damage cost caused by a security breach and the operating cost

w_1	w_2	w_1/w_2
5	1	5
4	1	4
3	1	3
2	1	2
1	1	1
1	2	1/2
1	3	1/3
1	4	1/4
1	5	1/5

가중치 조합 w_1과 w_2에 따라 유전자 알고리즘으로 탐색한 최적 정보보호 대책의 포트폴리오, 침해사고 비용, 그리고 정보보호 대책의 운영비용은 Table 5와 같다. (Table 5에서 침해사고 비용은 obj1 그리고 정보보호 대책의 운영비용은 obj2로 표기). Fig. 2는 가중치 변화에 따른 최적 비용의 변화 궤적을 보여준다. Table 5에서 w_1이 증가할수록 총 비용에서 침해사고 비용의 비중이 증가한다. 따라서 w_1이 증가할수록 가능한 침해사고를 방어하기 위해 보다 많은 정보보호 대책을 운영하는 방향으로 최적 포트폴리오가 구성된다. 반면, w_2가 증가할수록 운영비용을 최소화하기 위해 정보보호 대책의 개수가 감소하는 방향으로 최적 포트폴리오가 구성된다.

유전자 알고리즘이 최적해를 어떻게 찾았는지를 살펴보기 위해, $w_1 = w_2 = 1$인 경우 각 세대에서의 가중합 비용의 최우수, 평균, 최열등 값의 변화를 추적한 결과는 Fig. 3과 같다. 20세대 전에 최종적인 최우수해로 빠르게 수렴했고, 평균값에서 세대를 거듭할수록 우수한 개체가 적자생존 했고, 최열등 해의 값에서 최종 최우수 해에 적합된 후에도 개체가 교차와 변이

Table 5. Optimal portfolios and costs over weights

w1	w2	x1	x2	x3	x4	x5	x6	x7	x8	x9	x10	obj1	obj2
5	1	1	1	1	1	1	1	0	1	1	1	252	1797
4	1	1	1	1	1	1	1	0	1	1	1	252	1797
3	1	1	1	1	1	1	1	0	1	1	1	252	1797
2	1	0	1	1	1	1	1	0	1	1	1	587	911
1	1	0	1	1	1	1	1	0	0	0	1	656	786
1	2	0	1	1	1	1	0	0	0	0	1	727	735
1	3	0	1	1	0	1	0	0	0	0	1	1341	436
1	4	0	1	1	0	1	0	0	0	0	1	1341	436
1	5	0	0	1	0	1	0	0	1	0	1	2263	245

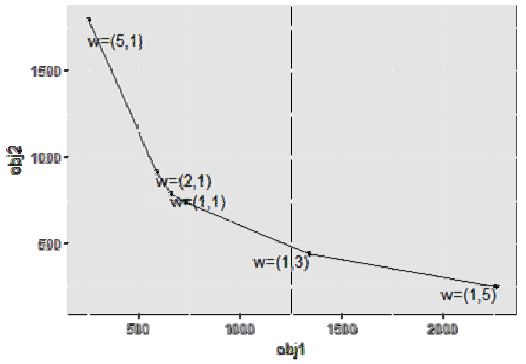


Fig. 2. Damage cost and operating cost over weights

www.dbpia.co.kr

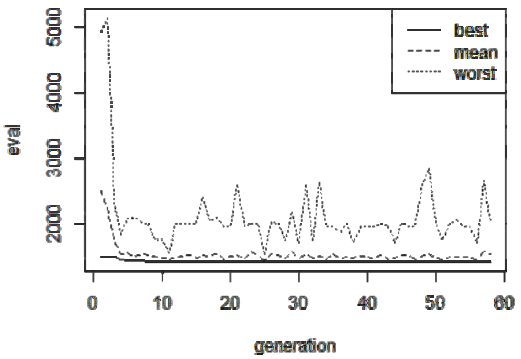


Fig. 3. The cost of best, mean, worst over generations ($w_1 = w_2 = 1$)

등으로 적절히 변동하여 다른 최적해가 있는지 탐색이 계속되어 진행되었음을 확인할 수 있다.

Fig. 4는 $w_1 = w_2 = 1$일 때 유전자 알고리즘으로 탐색한 최적 포트폴리오 구성 시 침해사고의 방어 비율을 나타낸다. Fig. 4의 왼쪽 그림은 포트폴리오에 포함된 정보보호 대책의 침해사고 별 방어 비율이다. 오른쪽 그림은 포트폴리오에 포함된 정보보호 대책이 모두 적용되었을 때 각 침해사고 별 방어 비율이다.

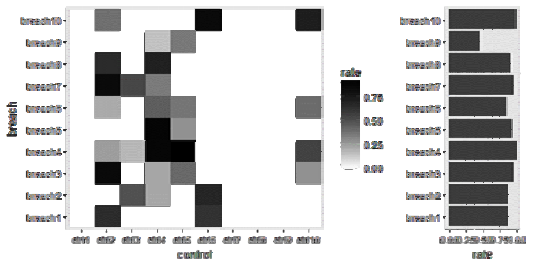


Fig. 4. Filtering rates under the optimal portfolios ($w_1 = w_2 = 1$)

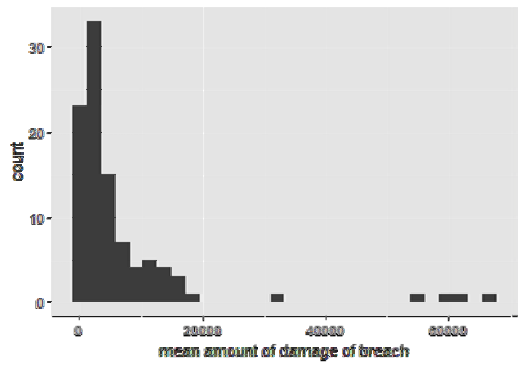


Fig. 5. Distribution of the damage cost

다음으로 침해사고의 유형이 100개 그리고 정보보호 대책이 100개인 경우의 수치예제를 다룬다. 즉, $n = 100$ 이고 $m = 100$ 이다.

Fig. 5는 100개 침해사고의 평균 피해금액 분포이다. Fig. 6은 100개 정보보호 대책의 한 기간 동안 평균 운영비용 분포이다.

Fig. 7은 정보보호 대책 별 침해 사고의 방어 비율을 나타낸다. 검은 색에 가까울수록 방어 비율이 1에 가깝고 하얀색에 가까울수록 방어 비율이 0에 가깝다.

앞선 수치 예와 동일하게 Table 4의 가중치 w_1과 w_2를 적용하여 유전자 알고리즘을 통해 최적 포트폴리오를 탐색하였다. 인구수를 100개로 하고 최대 300번 세대를 반복하여 가중치 w_1과 w_2의 조합별로 최적 정보보호 대책 포트폴리오, 해당 포트폴리오 적용 시의 침해사고 비용 C_1, 정보보호 대책의 운영비용 C_2를 구하였다. 총 반복횟수는 300으로 설정하였고 초기 세대 최우수 해의 가중합 비용의 0.001 이상의 개선이 50세대 동안 일어나지 않으면 반복을 중지하

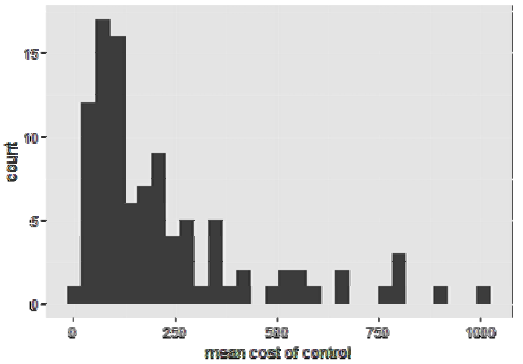


Fig. 6. Distribution of the operating cost

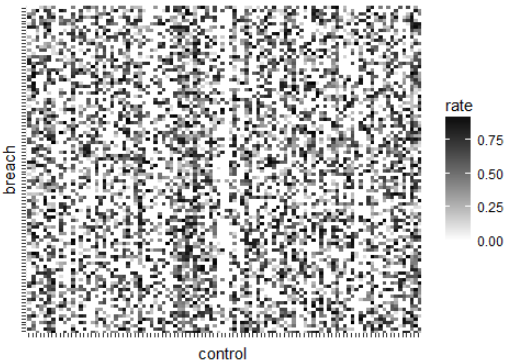


Fig. 7. Filtering rate according to a countermeasure and a security breach ($n = 100$, $m = 100$)

www.dbpia.co.kr

도록 하였다.

$n=100$ 이고 $m=100$인 경우, 가중치 w_1과 w_2의 조합에 따라 유전자 알고리즘으로 탐색한 최적 정보보호 대책의 포트폴리오, 침해사고 비용, 그리고 정보보호 대책의 운영비용은 Table 6과 같다. (Table 6에서 침해사고 비용은 obj1 그리고 정보보호 대책의 운영비용은 obj2로 표기). Fig. 8은 가중치 변화에 따른 최적 비용의 변화이다.

Fig. 9는 유전자 알고리즘이 최적해를 어떻게 찾았는지를 살펴보기 위해 $w_1=w_2=1$인 경우 각 세대에서의 가중합 비용의 최우수, 평균, 최열등 값의 변화를 추적한 결과이다. $n=10$ 이고 $m=10$인 Fig. 3과 비교해보면 $n=100$ 이고 $m=100$인 Fig. 9에서 더 많은 세대가 진행된 후 수렴이 일어나 반복이 중단되었음을 볼 수 있다. 40세대 전에 최종적인 최우수해로 빠르게 수렴하였고, 평균값에서 세대를 거듭할수록 우수한 개체가 적자 생존하였고, 최열등 해의 값에서 최종 최우수 해에 적합된 뒤에도 개체가 교차와 변이 등으로 적절히 변동하여 다른 최적해가 있는지 탐색이 계속되어 진행되었음을 확인할 수 있다.

Table 6. Optimal portfolios and cost over weights ($n=100,\ m=100$)

w1	w2	x1	x2	x3	x4	...	x96	x97	x98	x99	x100	obj1	obj2
5	1	0	0	0	0	...	0	1	0	0	0	48	1475
4	1	0	0	0	0	...	0	0	0	0	0	70	1402
3	1	0	0	0	0	...	0	1	0	0	0	95	1263
2	1	0	0	0	0	...	0	1	0	0	0	125	1176
1	1	0	0	0	0	...	0	0	0	0	0	236	1029
1	2	0	0	0	0	...	0	0	0	0	0	450	915
1	3	0	0	0	0	...	0	1	0	0	0	671	783
1	4	0	0	0	0	...	0	0	0	0	0	1057	689
1	5	0	0	0	0	...	0	0	0	0	0	909	732

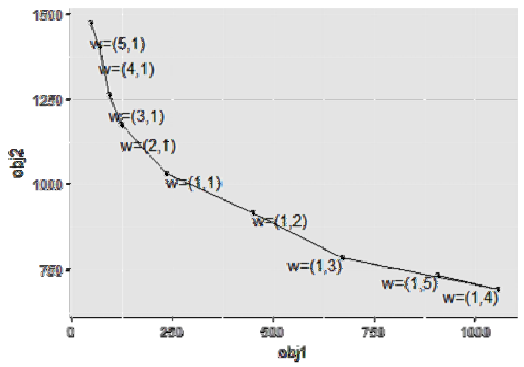


Fig. 8. Damage cost and operating cost over weights ($n=100,\ m=100$)

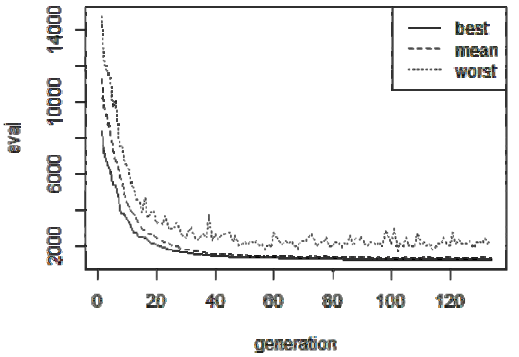


Fig. 9. The cost of best, mean, worst over generations ($w_1=w_2=1,\ n=100,\ m=100$)

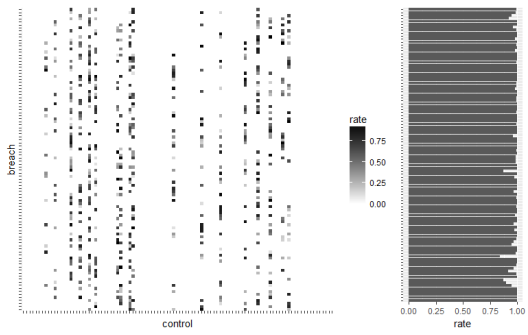


Fig. 10. Filtering rates under the optimal portfolios ($w_1=w_2=1,\ n=100,\ m=100$)

Fig. 10은 $w_1=w_2=1,\ n=100,\ m=100$일 때, 유전자 알고리즘으로 탐색한 최적 포트폴리오 구성 시 침해사고의 방어 비율을 나타낸다. 18개의 정보보호 대책이 선택되었고 최적 포트폴리오가 실행될 경우 대부분의 침해사고에 대해 95% 이상의 방어 비율을 구현하는 것으로 산출되었다.

Table 7은 $w_1=w_2=1,\ n=100,\ m=100$일 때, 최적 보안대책 포트폴리오 하에서의 침해사고 방어 비율의 분포이다. 100개 중 96개의 침해사고에 대해 방어 비율 90% 이상을 보이고 있으며, 나머지에 대해서도 80% 이상의 방어 비율을 보여주고 있다.

$n=100$이고 $m=100$인 경우의 수치 예제를 실행하는데 총 81.11 초가 소요되었다. 제안된 최적화 방법은 R로 구현하였으며, Windows 7를 구동하는 컴퓨터에서 수행되었다. CPU는 Intel(R) Xeon E5-1650 3.50GHz이고 메모리는 32GB였다. 따라서 유전자 알고리즘을 활용하면 침해사고와 정보보호 대책의 개수가 백 여 개로 상당히 큰 경우에도 몇 분의 실행 시간 안에 최적 포트폴리오를 찾을 수 있다.

www.dbpia.co.kr

Table 7. Distribution of the filtering rate under the optimal portfolios ($w_1 = w_2 = 1,\ n = 100,\ m = 100$)

filtering rate	frequency
[0,0.8)	0
[0.8,0.85)	1
[0.85,0.9)	3
[0.9,0.95)	5
[0.95,1]	91

마지막으로 본 논문에서 제안한 유전자 알고리즘을 활용한 최적화 방법의 성능 테스트를 다룬다. 침해사고 유형과 정보보호 대책의 개수를 같게 한 후 ($n = m$), n을 10에서 25까지 변화시키며 임의로 최적화 문제를 생성한 후, 완전탐색(full search)을 통해 얻은 정확한 전역 최적해와 유전자 알고리즘으로 탐색한 최적해를 비교해보았다. 가중치는 $w_1 = w_2 = 1$로 설정하였다. 유전자 알고리즘의 인구수는 m과 동일하게 그리고 반복횟수는 300으로 설정하였다. 초기 세대의 최우수 해에 비해 0.001이상 개선되지 않고 50세대 이상 지속되면 반복을 중지하였다.

정보보호 대책 수에 따른 완전탐색(FS)과 유전자 알고리즘(GA)의 최적 정보보호 대책 포트폴리오 산출 결과는 Table 8과 같다. Table 8에는 두 방법의 성능 비교를 위해 가중합 비용과 실행시간을 제시하였다. 실행 시간은 프로세서를 사용한 시간을 초 단위로 측정한 결과이다. Table 8에서 유전자 알고리즘과 완전탐색의 해의 가중합 비용이 거의 같다. 즉, 유전자 알고리즘이 전역 최적해를 제대로 탐색함을 알 수 있다. 한편, 정보보호 대책 수가 늘어남에 따라 유전자 알고리즘의 실행시간은 선형에 가깝게 증가하나 완전탐색은 기하급수적으로 증가한다. 완전탐색의 경우 정보보호 대책의 수가 하나 늘어날 때마다 탐색해야 할 해의 수가 2배씩 증가하여 실행시간이 기하급수적으로 증가한다. 반면, 유전자 알고리즘은 인구수 증가에 따른 해 탐색 횟수가 세대별로 선형으로 증가하며, 다만 반복횟수의 종료 지점이 인구수에 따라 증가하므로 선형에 비해 조금 더 크게 실행 시간이 증가한다.

완전탐색으로 탐색한 정확한 최적해의 가중합 비용 대비 유전자 알고리즘 방법으로 탐색한 최적해의 가중합 비용의 비를 이용하여 본 논문에서 제안한 최적화 방법의 정확도를 측정하였다. 가중합 비용의 비가 1이면 두 해가 같고 1보다 크면 제안된 방법의 해의 가중합 비용이 더 큼을 의미한다. 정보보호 대책 수에 따른 최적화 방법의 정확도 분석 결과는 Fig. 11과 같다. Fig. 11에서 본 논문에서 제시한 최적화 방법의 해와 완전탐색의 정확한 최적해의 가중합 비용이 8% 이내임을 확인할 수 있다. Fig. 11의 직선은 정보보호 대책의 수에 따른 정확도를 선형회귀분석으로 적합한 결과이다. 회귀선의 증가율이 아주 낮게 나타난다. 아울러, 회색의 음영부분은 95% 신뢰구간을 나타낸다. 정보보호 대책 수가 증가함에 따른 완전탐색 실행시간의 급증으로 인해 정보보호 대책 수가 25일 때까지만 분석하였으나 Fig. 11의 정확도 분석 결과를 보면, 정보보호 대책의 개수가 더욱 크게 증가하더라도 정확도의 감소가 이루어지지는 않으리라 예상된다.

Table 8. Cost and run time of the proposed optimization and full search according to the number of controls

number of control	cost-FS	cost-GA	time-FS	time-GA
10	566.31	566.31	0.07	0.09
11	790.35	790.35	0.14	0.08
12	882.27	882.27	0.27	0.11
13	1005.59	1005.59	0.61	0.09
14	1279.57	1279.57	1.42	0.13
15	1383.88	1494.41	2.64	0.13
16	1711.2	1711.2	5.65	0.11
17	1829.48	1829.48	12.46	0.12
18	1213	1213	26.51	0.15
19	880.91	880.91	56.57	0.2
20	897.15	897.15	121.89	0.17
21	1146.45	1146.45	263.7	0.16
22	1707.63	1787.56	588.62	0.19
23	1042.42	1079	1343.51	0.20
24	1120.3	1120.3	2896.83	0.34
25	1067.13	1067.13	6025.1	0.39

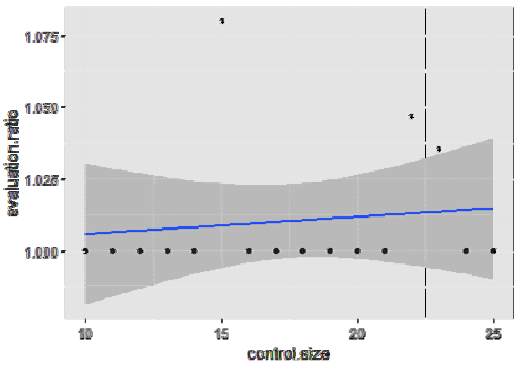


Fig. 11. Accuracy of the proposed optimization according the number of controls

www.dbpia.co.kr

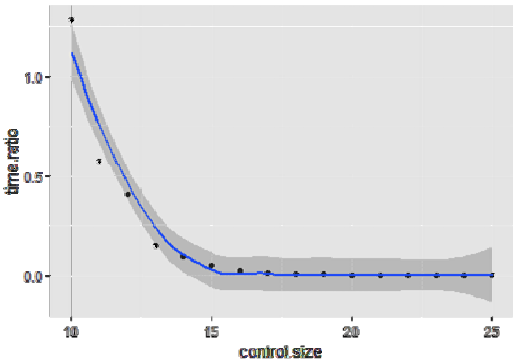


Fig. 12. Ratio of the time between the proposed optimization and full search according to the number of controls

Fig. 12은 정보보호 대책 수에 따른 본 논문에서 제안한 최적화 방법과 완전탐색의 실행시간 비이다. 실행시간 비가 1이면 두 방법의 실행시간이 같고 1보다 작으면 제안한 방법의 실행시간이 완전탐색보다 빠르다. Fig. 12에서는 국소회귀분석을 통해 적합한 평균선과 신뢰구간을 함께 나타냈다. 정보보호 대책의 수가 15개 이상이 되면 본 논문에서 제안한 최적화 방법이 완전탐색에 비해 현저히 빠르게 실행됨을 알 수 있다.

Ⅵ. 결 론

본 논문에서는 정보보호 침해사고의 유형 및 이에 대처하기 위한 정보보호 대책이 다양한 경우 유전자 알고리즘을 이용하여 비용을 최소화하는 최적의 정보보호 대책 포트폴리오 구성 방법을 제시하였다. 기존에도 유전자 알고리즘을 이용하여 최적의 정보보호 대책 포트폴리오를 구성하는 연구가 있었으나, 비용을 고려하지 않고 단지 침해사고 방어 유형 건수만을 고려하는 등으로 단순화된 모형만을 다루어 현실에 적용하기 어렵거나, 퍼지이론을 이용하여 최적 포트폴리오를 도출하여 정보보호 담당자가 모형을 구성하기 어려운 단점이 있었다. 본 연구에서는 보안침해사고 유형별로 발생 빈도와 피해액, 정보보호 대책의 운영비용을 점추정할 수 있다는 가정 하에 유전자 알고리즘을 이용하여 침해사고 피해액과 정보보호 대책 운영비용을 적절히 조화시키는 최적의 정보보호 대책 포트폴리오 방안을 도출하는 방법을 제시하였다. 또한 점추정치의 불확실성을 고려하여, 침해사고 피해액과 정보보호 대책의 운영비용에 대해 중요도를 가중치로 조정해가며 최적 투자 포트폴리오가 어떻게 변하는지를 의사결정자에게 제시할 수 있도록 가중치 기반의 다중-목적 최적화를 수행하였다.

본 논문에서 제시한 최적화 방법을 적용하면 100개의 침해사고 유형과 100개의 정보보호 대책을 다루는 문제에서도 빠른 시간 내에 해를 구할 수 있다. 아울러, 25개 이하의 정보보호 대책을 다루는 문제에서 정보보호 대책의 수가 증가하더라도 해의 정확도가 크게 훼손되지 않으며 실행시간도 선형에 가깝게 증가함을 확인하였다. 혼합 정수계획법에 기반을 둔 기존 연구에서 20개 이상의 정보보호 대책을 다루는 경우 문제해결에 어려움을 겪었다는 점을 고려하면 본 논문에서 제안한 최적화 방법이 실용성 측면에서 효과적임을 보여준다고 할 수 있다.

마지막으로 본 연구의 한계와 향후 발전 방향을 제시하며 결론을 마무리한다. 첫째, 본 연구에서는 실제 데이터를 사용하기 보다는 가상의 데이터를 이용하여 제안된 방법을 적용해 보았다. 향후 실제 데이터를 이용하여 제안된 방법을 적용해 본다면 제안된 방법의 현실 적용 가능성을 한층 높일 수 있을 것이다. 둘째, 본 연구에서는 정보보호 대책의 도입 여부만을 고려하여 최적의 정보보호 대책 포트폴리오를 구성하였다. 현실에서는 한 정보보호 대책의 도입 수준이 여러 수준으로 나누어져 있으므로 향후 연구에서는 정보보호 대책을 여러 수준 중 어떤 수준으로 도입할 것인지에 대한 문제로 확장하여 최적화 방법을 제시할 수 있으리라 여겨진다. 셋째, 본 연구에서는 제안한 방법을 테스트하기 위하여 완전탐색의 결과와 제안된 방법을 비교하였다. 향후 혼합 정수계획법을 이용하는 방법에 대해서도 실행시간을 분석하면, 정보보호 대책의 수에 따라 적절한 최적화 방법을 제시할 수 있으리라 여겨진다.

References

[1] A. Bendovschi, “Cyber-attacks-trends, patterns and security countermeasures,” *Procedia Econ. and Finance*, vol. 28, pp. 24-31, 2015.

[2] W. S. Yang and T. S. Kim, “Analysis on operation of anti-virus systems with real-time scan and batch scan,” *J. KICS*, vol. 38B, no. 11, pp. 861-869, 2013.

[3] National Intelligence Service, Ministry of Science, ICT and Future Planning, Korea Communications Commission, Ministry of the Interior, Financial Services Commission, *2017 National Information Security Whitepaper*,

www.dbpia.co.kr

2017.

[4] L. P. Rees, J. K. Deane, T. R. Rakes, and W. H. Baker, "Decision support for cybersecurity risk planning," *Decision Support Systems*, vol. 51, no. 3, pp. 493-505, 2011.

[5] C. J. Alberts and A. Dorofee, *Managing information security risks: The octave approach,* Addison-Wesley Longman Publishing Co., Inc., 2002.

[6] S. Bistarelli, F. Fioravanti, and P. Peretti, "Using cp-nets as a guide for countermeasure selection," in *Proc. 2007 ACM Symp. Applied Comput.*, pp. 300-304, 2007.

[7] M. Egan and T. Mather, *The executive guide to information security: Threats, challenges, and solutions,* Addison-Wesley Professional, 2004.

[8] W. H. Baker, L. P. Rees, and P. S. Tippett, "Necessary measures: Metric-driven information security risk assessment and decision making," *Commun. ACM*, vol. 50, no. 10, pp. 101-106, 2007.

[9] M. Gupta, 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, pp. 592-603, 2006.

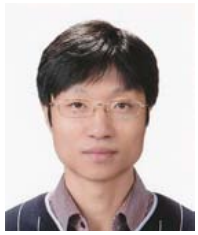
[10] T. Sawik, "Selection of optimal countermeasure portfolio in IT security planning," *Decision Support Systems*, vol. 55, no. 1, pp. 156-164, 2013.

[11] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Systems*, vol. 86, no. C, pp. 13-23, 2016.

[12] J. H. Holland, *Adaptation in natural and artificial systems: An introductory analysis with application to biology, control, and artificial intelligence*, Ann Arbor, MI: University of Michigan Press, 1975.

[13] E.-G. Talbi, *Metaheuristics: From design to implementation*, vol. 74. John Wiley & Sons, 2009.

김 길 환 (Kilhwan Kim)



1994년 2월 : KAIST 경영과학과 졸업
1996년 2월 : KAIST 산업경영학과 석사
2009년 2월 : KAIST 산업및시스템공학과 박사
1998년 11월~2003년 3월 : LG CNS 선임컨설턴트
2003년 4월~2005년 3월 : 기업정보화지원센터 선임연구원
2009년 1월~2012년 8월 : ETRI 선임연구원
2012년 8월~현재 : 상명대학교 경영공학과 조교수
<관심분야> 확률모형, 대기행렬 이론, 최적화 이론, 서비스 플랫폼, 데이터 마이닝

양 원 석 (Won Seok Yang)

1993년 2월 : KAIST 경영과학과 학사
1995년 2월 : KAIST 경영과학과 석사
2000년 2월 : KAIST 산업공학과 박사
2000년 2월~2007년 1월 : LG U+ 차장
2007년 2월~2010년 2월 : 한국전자통신연구원 기술전략연구본부 선임연구원
2010년 3월~현재 : 한남대학교 경영학과 교수
<관심분야> 확률모형, 대기행렬시스템, 데이터마이닝, 생산운영관리, 통신정책, 보안경제성

www.dbpia.co.kr

김 태 성 (Tae-Sung Kim)

1997년 2월 : KAIST 산업경영 박사

1997년 2월~2000년 8월 : 한국전자통신연구원 선임연구원

2005년 1월~2006년 2월 : University of North California at Charlotte 방문교수

2010년 7월~2012년 8월 : Arizona State University 방문연구원

2000년 9월~현재 : 충북대학교 경영정보학과 교수, 보안경제연구소장, 보안컨설팅연계전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 행정안전부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, KISA ISMS/PIMS 인증위원회 위원, 한국전력 정보보안자문위원, 보안GRC리더스포럼 공동의장

<관심분야> 통신 및 보안 분야의 경영 및 정책 분석

www.dbpia.co.kr