ISSN 2288-4866 (Print)
ISSN 2288-4882 (Online)
http://www.jiisonline.org
J Intell Inform Syst 2020 September: 26(3): 37~50 http://dx.doi.org/10.13088/jiis.2020.26.3.037

정보보호 대책의 성능을 고려한 투자 포트폴리오의 게임 이론적 최적화

이상훈
충북대학교 경영정보학과
(sanghoon@chungbuk.ac.kr)

김태성
충북대학교 경영정보학과
(kimts@chungbuk.ac.kr)

사물 인터넷, 빅데이터, 클라우드, 인공지능 등 다양한 정보통신기술이 발전하면서, 정보보호의 대상이 증가하고있다. 정보통신기술의 발전에 비례해서 정보보호의 필요성이 확대되고 있지만, 정보보호 투자에 대한 관심은 저조한 상황이다. 일반적으로 정보보호와 관련된 투자는 효과를 측정하기 어렵기 때문에 적절한 투자가 이루어지지 않고 있으며, 대부분의 조직은 투자 규모를 줄이고 있다. 또한 정보보호 대책의 종류와 특성이 다양하기 때문에 객관적인 비교와 평가가 힘들고, 객관적인 의사결정 방법이 부족한 실정이다. 하지만 조직의 발전을 위해서는 정보보호와 관련된 정책과 의사결정이 필수적이며 적정 수준의 투자와 이에 대한 투자 효과를 측정 할 필요가 있다. 이에 본 연구에서는 게임 이론을 이용하여 정보보호 대책 투자 포트폴리오를 구성하는 방법을 제안하고 선형계획법을 이용하여 최적 방어 확률을 도출한다. 2인 게임 모형을 이용하여 정보보호 담당자와 공격자를 게임의 경기자로 구성한 뒤, 정보보호 대책을 정보보호 담당자의 전략으로, 정보보호 위협을 공격자의 전략으로 각각 설정한다. 게임 모형은 경기자의 보수의 합이 0인 제로섬 게임을 가정하고, 여러개의 전략 사이에서 일정한 확률 분포에 따라 전략을 선택하는 혼합 전략 게임의 해를 도출한다. 여러 종류의 위협이 존재하는 현실에서는 한 개의 정보보호 대책만으로 일정 수준 이상의 방어가 힘들기 때문에, 다수의 정보보호 대책을 고려해야한다. 따라서 다수의 정보보호 위협에 따른 정보보호 대책이 배치된 환경에서 정보보호 대책의 방어 비율을 이용하여 정보보호 대책 투자 포트폴리오를 산출한다. 또한 최적화된 포트폴리오를 이용하여 방어 확률을 최대화하는 게임 값을 도출한다. 마지막으로 정보보호 대책의 실제 성능 데이터를 이용하여 수치 예제를 구성하고, 제안한 게임 모델을 적용하고 평가한다. 본 연구에서 제시한 최적화 모델을 이용하면 조직의 정보보호 담당자는 정보보호 대책의 방어 비율을 고려하여 정보보호 대책의 투자 가중치를 구할 수 있고, 효과적인 투자 포트폴리오를 구성하여 최적의 방어 확률을 도출 할 수 있을 것이다.

주제어 : 게임이론, 정보보호, 투자 포트폴리오

논문접수일 : 2020년 6월 3일 논문수정일 : 2020년 6월 25일 게재확정일 : 2020년 7월 19일
원고유형 : 일반논문(급행) 교신저자 : 김태성

1. 서론

사물 인터넷, 빅데이터, 인공지능 등 새로운 정보통신기술의 발전으로 인해 삶의 질이 향상되었지만, 정보통신기술의 의존도가 높아졌고 이에 따른 사이버공격, 정보 유출 등 정보화의 역기능이 발생하고있다(Ministry of Science and ICT et al., 2019a). 이처럼 정보보호의 중요성은 점점 증가하고 있으며, 정보보호를 강화하려는 노력 없이는 정보통신기술의 발전도 매우 어려울 것으로 보인다(Seo and Park, 2017). 2019년 정보보호 실태조사에 따르면 조직의 87%는 정보보호가 중요하다고 인식하고 있는 것으로 조사되었다(Ministry of Science and ICT et al.,

2019b). 하지만 조직의 정보보호 예산 편성은 2016년 48.15, 2017년 36.2%, 2018년 32.3%로, 매년 감소하고 있는 것으로 나타났다(Ministry of Science and ICT et al., 2019b). 이와 같이 정보보호에 대한 투자가 적절하게 이루어지지 않고 있는 상황이며, 이에 따른 정보보호 투자에 대한 관심이 필요하고 적정 수준의 투자 규모와 경제적인 효과를 측정 할 필요가 있다. 실제로 정보보호 투자에 소요되는 비용은 정보보호 침해로 인한 피해액에 비하여 상당히 낮을 것으로 예상되며, 이는 정보보호 피해 예상 금액의 37%를 초과하면 안된다고 연구되었다(Gordon and Loeb, 2002).

다양한 정보통신기술이 발전함에 따라서, 기업의 전략과 의사결정은 직관이나 경험에 의존하는 과거와 달리, 데이터를 활용한 과학적인 분석이 많아지고 있다. 이에 많은 기업은 비즈니스 인텔리전스 시스템을 활용하고 있다(Kwon, 2014). 또한 조직의 발전을 위해서는 정보보호와 관련된 정책과 의사결정이 필수이며, 조직은 정보보호와 관련된 위협에 대응하기 위하여 제한된 예산에서 최선의 정보보호 대책에 투자하고 실행해야한다(Fielder et al., 2016). 하지만 수많은 정보보호 위협을 완전히 방어할 수 있는 대책은 존재하지 않기 때문에, 서로 다른 기능을 갖는 여러 종류의 정보보호 대책을 구성해야 한다(Jeong ang Jeong, 2011). 이에 조직의 중요한 과제는 발생 가능한 정보보호 위협을 이해하고 알맞는 정보보호 대책 포트폴리오를 구성하여 경제적인 효과를 측정하는 것이다(Kumar et al., 2008). 일반적인 금융분야에서의 투자와는 다르게 정보보호와 관련된 투자는 효과를 정확히 측정할 수 없기 때문에, 대부분의 조직은 투자 규모를 줄이지만, 정보보호 제품의 벤더는 규모가 크고 성능이 높은 고가의 제품에 집중하게 된다(Gordon and Loeb, 2002). 또한 정보보호 대책은 종류와 성능이 다양하기 때문에 의사결정 과정은 더욱 복잡하고, 따라서 정보보호 담당자는 정보보호 대책의 성능을 객관적으로 비교하고 평가할 수 있어야 한다. 하지만 정보보호 투자 효과 측정의 체계적인 방법이 부족하고, 정량적인 분석 및 객관적인 예측이 어려워 정보보호 투자 의사결정에는 한계가 발생한다(Kong et al., 2012).

본 연구에서는 이러한 논의를 바탕으로 복수의 정보보호 위협에 대한 정보보호 대책의 성능을 고려한 최적의 정보보호 대책 투자 포트폴리오와 그에 따른 투자 결과를 도출한다. 정보보호 대책의 성능을 이용하여 게임 행렬을 구성하고 선형계획법을 이용하여 정보보호 대책 투자 포트폴리오를 최적화한다. 게임 모형은 경기자가 두 명인 상황에서 경기자의 보수의 합이 0인 제로섬 게임(zero-sum game)을 가정한다. 게임의 경기자로 정보보호 담당자와 공격자를 설정하고, 정보보호 담당자의 전략으로 정보보호 대책을 선택하고, 공격자의 전략으로 정보보호 위협을 선택하여 게임을 진행한다. 다수의 위협이 존재하는 상황에서는 단일의 정보보호 대책으로는 일정 수준 이상의 방어가 힘들기 때문에, 다수의 정보보호 대책 사이에서 일정한 확률 분포를 주고 이 확률에 따라 정보보호 대책을 선택하는 혼합 전략(mixed strategy) 해를 도출한다. 본 연구에서 제시한 최적화 모델을 이용하면 정보보호 대책의 방어 비율을 이용하여 가중치를 구할 수 있고 정보보호 대책의 도입 여부만을 판단하는 단순한 의사결정이 아닌 구체적인 투자 비중을 판단할 수 있는 효과적인 의사결정을 지원한다. 본 연구의 시사점은 다음과 같다. 첫째, 정보보호 대책의 실제 데이터를 이용하여 분석을 진행

하였다. 조직의 정보보호 담당자는 정보보호 투자 대책 수립 시 실무적인 의사결정에 본 연구에서 제시한 방법론을 활용할 수 있을 것이다. 둘째, 정보보호 대책의 투자 가중치를 도출하였다. 정보보호 대책의 투자 여부만이 아닌, 정보보호 대책 각각의 투자 비중을 도출하였기 때문에 다수의 정보보호 대책을 고려하여 투자 의사결정을 진행해야하는 상황에서 투자 포트폴리오를 쉽게 구성할 수 있다. 셋째, 정보보호 대책의 투자 포트폴리오를 구성한 뒤 최적의 방어 확률을 구할 수 있다. 조직의 정보보호 투자 예산에 맞는 정보보호 대책을 도출하여 구체적인 투자 효과를 측정 할 수 있다는데 실무적인 의의가 있다.

본 연구의 구성은 다음과 같다. 2장에서는 관련 문헌을 분석한다. 3장에서는 연구 모형을 제시하고 최적화 모형을 도출한다. 4장에서는 수치예제를 이용하여 제안된 모형의 성능을 실험하고, 정보보호 대책 투자 포트폴리오를 도출한다. 5장에서는 본 연구의 결론과 한계점 및 향후 연구를 제시한다.

2. 문헌연구

다양한 정보보호 기술과 성능이 개발되고 있고, 이러한 기술 중 다수는 서로가 보완적인 기술이기 때문에 정보보호와 관련된 투자를 분석하기 위해서 합리적인 방법론이 필요하다 (Cavusoglu et al., 2004). 정보보호 투자와 관련된 연구는 정보보호 대책에 대한 투자의 이익 및 정보보호 위협에 대한 잠재적인 손실을 추정하는 게임이론을 이용한 연구 방법과 게임이론 이외에, 위험 분석, 의사결정 분석 등 다양한 분야의 분석 방법을 사용하는 연구로 나눌 수 있다.

게임이론을 이용한 정보보호 투자 관련 연구에서는 여러가지 변수를 사용하여 분석을 진행하고 균형을 구했지만 대부분의 연구는 실증 분석이 아닌 임의의 변수를 설정하여 가설을 검증하였다. Cavusoglu et al.(2004)은 정보보호 투자의 가치를 정의하기가 어렵고, 정보보호 투자 분석은 높은 수준의 데이터 수집이 필요하기 때문에 이런 제한 사항을 극복하는 정보보호 ROI (Return on Investment) 평가의 한 방법으로 게임이론을 이용한 보안 투자 방법론을 제시하였다. 또한 정보보호를 예방, 탐지, 응답 3개의 단계로 나누고, 각 단계별로 방화벽, 침입 탐지 시스템, 모니터링의 확률변수를 사용하여 최적 투자 의사결정을 분석하였다. Cavusoglu et al(2005)은 침입 탐지 시스템의 가치를 게임 이론으로 분석하였고, 기업과 침입자의 전략에 따른 보수를 설정하여 혼합 전략 내쉬 균형을 찾은 뒤 각 변수들을 설명했다. 이런 분석은 정보보호 투자의 효과를 정량적으로 측정하지 않고, 대책을 도입하는 비용을 고려하기 때문에 다루기 쉽다. 그러나 보안에 투자할 금액을 결정하는 데에는 도움이 되지 않는다. 각 정보보호 대책의 비용만을 측정할 뿐, 정보보호 위협과 그에 따른 대책의 효과는 측정하지 않기 때문이다. Cavusoglu et al.(2008)은 투자 수준, 취약성 등을 게임 이론을 이용하여 분석하고 보안 투자 방법을 제시하였다. Fielder et al.(2016)은 게임 이론과 조합 최적화 방법론을 이용해 정보보호 담당자와 공격자의 관점에서 여러 수준의 보안 정책에 따른 내쉬 균형을 구하고, 정보보호 관련 예산의 최적화 분석을 진행하였다. 이 연구에서는 인터넷을 통한 해킹 만을 가정하였기 때문에 실제 환경에서 발생하는 여러 종류의 공격과 정보보호 대책 간의 분석은 이루어지지 않았다. 또한 게임이론 경기자

의 전략을 공격 및 방어의 여부로만 나누었고, 어느 정도의 공격과 방어가 이루어졌는지 다루지 않았다.

게임이론 이외의 방법을 이용한 정보보호 투자와 관련된 연구들은 주로 기업이나 투자자 입장에서 정보보호의 가치를 측정하거나 정보보호 의사결정의 절차를 도출하였다. Bodin et al.(2005)은 정보보호 투자와 관련된 제안서를 AHP 방법론으로 평가했으며, 정보보호 목표를 효율적으로 달성할 수 있도록 적합한 투자기준을 제시하였다. Gordon and Loeb(2002)에 의하면 정보보호에 대한 투자가 증가할수록 효용이 감소하는 한계 효용 체감의 법칙이 발생하고, 따라서 중간 수준의 투자를 하는 것이 효과적이라는 결과를 도출하였다. 하지만 이 연구에서는 외부 효과와 같은 불확실한 경제 상황은 고려하지 않았고, 실제 기업의 투자가 연구의 결과와 일치하는지에 대해서 추가 연구가 필요하다고 하였다. 이익과 손실에 대한 추정은 기업이 정보보호 대책을 배치하는데 유용하지만, 대책의 종류와 수량을 결정하는데 한계가 있다. Gupta et al.(2006)은 보안 위협과 위협에 따른 보안 대책을 선택한 후, 보안 위협의 투자 비용을 최소화하면서 방어를 가능한 높일 수 있는 정보보호 대책의 투자 포트폴리오를 제시하고, 유전자 알고리즘을 이용하여 최적화하였다. Kong et al.(2012)은 전사적 차원의 BSC 방법론을 이용해 정보보호 투자 전략 수립 및 타당성을 검증하였다. 이런 의사결정 방법론을 이용하여 잠재적인 정보보호 위협을 식별하고 예상 손실을 측정하여 정보보호 대책을 배치할 수 있지만, 정보보호 기술의 효과와 성능을 고려하지 않는다. 다양한 위협들이 정보보호 대책에 어떤 영향을 미치는지를 측정할 수 없다. 또한 각 정보보호 대책들의 상호 보완적인 관계와 손실을 판단할 수 없다. Kumar et al.(2008)은 정보시스템의 정보보호 대책을 평가하는 포트폴리오를 설계하기 위하여 시뮬레이션 모델을 개발하고 평가하였다. 정보보호 위협으로 인한 침입, 손실, 복구 등의 변수를 고려하였고 정보보호 투자 포트폴리오의 가치를 평가하였으나, 비선형 모델은 설명하지 못하였고 실제 데이터 수집 및 검증이 필요하다고 하였다. Sawik(2013)은 제한된 예산 하에서 침해 위협 발생률, 손실액, 정보보호 대책의 침해 위협 방어율을 가정하고 잠재적인 손실을 최소화하하는 모델을 제시하여 정보보호 대책의 최적 선택 문제를 혼합정수계획법을 이용하여 구했다. 혼합정수계획법을 이용하면 가정에 따른 정확한 해를 구할 수 있지만, 침해 위협과 정보보호 대책의 유형이 각각 20개 이상일 경우 최적 해를 구하기 위해 많은 시간이 필요하다.

본 연구에서는 Sawik(2013)을 참조하여 정보보호 대책과 정보보호 위협의 모형을 구성하였고, 이를 게임 행렬로 표현한 뒤, 선형계획법을 이용하여 최적 해를 도출하였다. 기존의 게임이론을 이용한 정보보호 투자 모델에서는 공격자와 방어자를 경기자로 하는 2인 게임을 진행하고, 경기자의 전략을 공격과 방어의 여부 두 가지만을 전략으로 가정하였지만(Cavusoglu et al., 2005; Cavusoglu et al., 2008; Fielder et al., 2016), 본 연구에서는 실제 기업 환경에서 발생하는 다수의 정보보호 위협과 그에 따른 정보보호 대책의 선택을 전제로 최적 방어 확률을 도출한다. Fielder et al.(2016)에서는 공격자와 방어자의 전략으로 다수의 정보보호 위협과 정보보호 대책을 가정하고 게임이론의 내쉬 균형을 구했지만 공격자와 방어자의 각 전략을 하나의 집합으로 계산하였기 때문에 개별 정보보호 대책의 선택

〈Table 1〉 Comparative Analysis of Related Work

Methodology / Subject	Game theory	Optimization	AHP	Genetic algorithm
Investment amount	Cavusoglu et al.(2004), Cavusoglu et al.(2008)	Fielder et al.(2016), Gordon and Loeb(2002)		
Investment portfolio		Kumar et al.(2008), Sawik(2013)	Bodin et al.(2005), Kong et al.(2012)	Gupta et al.(2006)

비중을 도출하지 못하였다. 이를 해결하기 위하여, 본 연구에서는 경기자의 이익(방어 확률)은 최대화하면서 다수의 전략 선택 비중을 최적화하는 게임 모델을 설정하고, 선형계획 모형으로 정식화 한다. 게임이론의 내쉬 균형을 이용하면 경기자 전략의 비중을 도출하고 평균 기대 이익을 구할 수 있지만, 경기자의 보수를 최대화하는 게임 값은 구하기 어렵기 때문에, 목적식을 최대화하는 선형계획법을 이용한다. 한편, 정보보호 투자 포트폴리오와 관련된 기존 연구에서는 다수의 정보보호 대책 도입을 가정하고 제한된 예산에서 정보보호 대책의 유형에 따라 무작위로 투자했고 정보보호 대책의 도입 여부와 수준을 고려했다(Gupta et al., 2006; Sawik, 2013). 하지만 어떤 정보보호 대책이 중요하고 예산의 비중이 높게 투자되어야 하는지는 고려하지 않았고, 이에 본 연구에서는 정보보호 대책의 유형별 중요도(비중)를 고려하는 정보보호 대책 투자 포트폴리오를 분석한다. 또한, Sawik(2013)에서는 정보보호 위협을 서로 독립이라고 가정하였고 여러 위협들이 서로 영향을 미치는 관계를 반영하지 못했다. 실제 환경에서는 정보보호 위협이 서로 밀접한 관계가 있기 때문에, 본 연구에서는 정보보호 위협의 전체 집합 안에서 일정한 확률분포를 주고 각 위협들이 어느 정도의 비중으로 발생하는지를 고려하였다.

3. 연구 모형

게임 이론은 상호 의존적인 상황에서 경쟁자들이 상대방의 행동에 대한 기대나 예측을 근거로 전략적 의사결정을 하는 이론체계이다(Neumann and Morgenstern, 1974). 게임 이론에서는 불확실한 상황에서 합리적인 전략을 어떻게 결정할 것인지 수학적으로 분석하고 자신과 상대방의 선택이 서로에게 어떤 영향을 미치는지에 대해 이론적으로 설명하며, 경쟁과 협력에 대한 최선의 방법론을 제시한다(Neumann and Morgenstern, 1974). 게임 상황을 분석하기 위한 구성요소로 게임 상황에 놓여있는 경기자, 경기자가 사용하는 전략, 경기자의 효용의 크기를 나타내는 보수가 있으며, 경기자의 전략에 따른 보수를 이용해서 문제 상황을 분석할 수 있다(Nash, 1951). 본 연구에서는 정보보호 담당자와 공격자를 경기자로 하는 2인 게임 모델을 이용하고, 정보보호 담당자의 전략을 정보보호 대책으로, 공격자의 전략을 정보보호 위협으로 구성한다. n 개의 서로 다른 정보보호 위협이 발생하고 있는 상황에서 m 개의 서로 다른 정보보호 대책을 정보시스템에 배치한다고 가정한다. 이때, 정보보호 담당자는 다수의 정보보호 대책을 확률에 따라 선택하는 혼합 전략을 사용한다.

- i: 정보보호 담당자의 전략(정보보호 대책, $i=1, \cdots;m$)
- j: 공격자의 전략(정보보호 위협, $j=1, \cdots;n$)
- p_i: 정보보호 대책 i 의 선택 확률($\sum_{i=1}^{m} p_i = 1$)
- d_{ij}: 정보보호 대책 i 의 정보보호 위협 j 에 대한 방어 비율
- C: 정보보호 대책 투자 포트폴리오를 반영한 최적 방어 확률

정보보호 대책의 투자 포트폴리오는 $P=(p_1, p_2, \cdots, p_m)$이고, 정보보호 위협 j의 집합을 $T=(t_1, t_2, \cdots, t_n)$이라 한다. 정보보호 위협에 대한 정보보호 대책 i 의 방어 비율은 d_{ij} 이다. n 개의 정보보호 위협에 대한 m 개의 정보보호 대책을 배치한 상태에서, 최적화된 정보보호 대책 투자 포트폴리오를 반영한 최적 방어 확률은 다음과 같다.

$$C = \sum_{i=1}^{m} \sum_{j=1}^{n} p_i d_{ij}$$

게임 이론의 모형으로 제로섬 게임(zero-sum game)을 가정하였고, 정보보호 담당자의 손실은 공격자의 이익으로 이어지기 때문에 상대방의 전략인 정보보호 위협에 대한 정보보호 대책의 방어 비율을 고려하여야 한다. 따라서 본 연구의 최적화 문제에서 정보보호 담당자는 상대방인 공격자의 전략에 따른 정보보호 대책의 성능을 고려하여 모든 정보보호 위협에 대해 일정 수준 이상의 방어 확률을 유지하는 정보보호 대책 투자 포트폴리오를 구성해야한다. 정보보호 대책의 방어 비율을 고려하여 최적 방어 확률인 C 를 최대화하는 정보보호 대책 투자 포트폴리오 P 를 산출한다. 본 연구에서 제안한 게임 모형을 다음의 선형계획법으로 표현할 수 있다.

$$\begin{aligned} &\text{Max} && C \\ &\text{s.t} && p_1, p_2, p_3, \cdots p_m \geq 0 \\ &\sum_{i=1}^{m} p_i d_{ij} \geq C && \textit{for } j=1, 2, 3, \cdots, n, \\ &&& \text{and } \sum_{i=1}^{m} p_{i=1} \end{aligned}$$

정보보호 담당자는 정보보호 대책의 방어 비율을 고려하여 정보보호 대책을 확률적으로 선택하게 되고, 제한된 예산안에서 여러 정보보호 대책들의 투자 비중을 최적화하여 예상 방어 확률을 도출한다.

4. 수치예제

이 장에서는 본 연구에서 제안한 모델의 수치예제를 제시하고 실험한다. 다양한 정보보호대책의 성능을 기반으로 정보보호 대책 포트폴리오를 구성하기 위하여 정보보호 대책과 관련된 자료를 수집하였다. Kumar et al.(2008)에 의하면 정보시스템의 위협을 방어할 수 있는 정보보호 대책은 Firewall, Antivirus, IDS(Intrusion Detection Systems), encryption 등 이 있다고 하였고, 조직은 여러 종류의 정보보호 대책을 배치하여 위협을 줄일 수 있다고 하였다. 또한 Survey on Information Security(2019)에 의하면 정보보호 관련 제품을 이용하는 국내 기업은 93.5%이며, 정보보안 제품 중 시스템 보안의 이용률은 78.9%로 가장 높았고, 네트워크 보안은 75.7%로 두 번째로 높았다. 따라서 정보보호 대책은 Kumar et al.(2008)의 모형을 참고하여 시스템 및 네트워크 보안 제

품인 Firewall, IPS(Intrusion Prevention Systems), Antivirus 3개로 선정하였다. Firewall, IPS는 NSS labs의 Next generation firewall comparative report (2019), Next generation intrusion prevention system comparative report(2017)을 각각 참고하였다. Next generation firewall comparative report(2019)은 12개 벤더의 Firewall 제품을 실험하였고 방어 성능을 여러가지 환경에 따라 평가하여 종합적인 제품의 효과를 도출하였다. 실험 결과 제품의 성능은 최고 97.7%, 최저 77.7%로 나타났다. Next generation intrusion prevention system comparative report(2017)은 9개 벤더의 IPS 제품을 실험하였고, 실험 결과 제품의 성능은 최고 99.9%, 최저 25%로 나타났다. Antivirus의 성능을 분석하기 위하여 AV- Comparatives의 Malware Protection Test(2018)을 참고하였다. Malware Protection Test(2018)는 18개 벤더의 제품을 대상으로 실험하였으며 20,046의 멀웨어 샘플을 이용하여 여러가지 환경의 실험을 진행하였다. 실험 결과, 최고 성능은 100%, 최저 성능은 40.5%로 나타났다.

정보보호 대책의 성능(방어 비율)은 소수점 첫째자리에서 반올림하여 나타냈으며 Rakes et al.(2012)을 참고하여 균등 분포(Uniform distribution)로 생성하였고, 각 정보보호 대책의 보고서를 기반으로 성능의 범위를 도출하였다<Table 2>. 조직에서 정보보호 대책의 투자를 진행할 때 고려해야 할 실제 환경은 매우 복잡하고 다양하지만, 본 연구의 수치 예제를 구성하기 위하여 각 정보보호 대책의 보고서를 기반으로 도출한 성능의 실험 환경은 모두 동일하다고 가정한다. 또한 정보보호 위협은 임의의 n개가 발생한다고 가정한다.

〈Table 2〉 Performance of Countermeasures

Performance / Countermeasure	High	Low	Uniform distribution
Firewall	98%	78%	[0.78,0.98]
IPS	100%	25%	[0.25, 1]
Antivirus	100%	41%	[0.41, 1]

정보보호 대책의 성능을 기반으로 정보보호 대책과 위협이 각각 3개(m=3, n=3)인 균등 분포로 생성한다. 먼저 동일한 정보보호 대책으로 구성한 포트폴리오를 분석하고, 3개의 다른 종류의 정보보호 대책으로 구성한 포트폴리오를 분석한다. Firewall, IPS, Antivirus의 게임 행렬은 <Table 3>, <Table 4>, <Table 5>와 같다. <Table 3>은 조직의 정보보호 대책으로 서로 다른 성능을 가진 Firewall 3개를 선택하고 조직에 발생하는 위협이 3개인 상황에서 [0.78, 0.98]인 균등 분포로 방어 비율을 생성하였다. 게임의 최적화 결과 Firewall 1, 2, 3의 포트폴리오 가중치는 각각 49.11%, 0%, 50.98%로 최적화 되었고, Firewall 1, 3이 선택되었다. 최적화된 포트폴리오가 실행될 경우 전체 위협에 대해 최적 방어 비율은 85.94%로 도출되었다. <Table 4>는 정보보호 대책으로 IPS 3개를 선택하고, 조직에 발생하는 위협이 3개인 상황에서 [0.25, 1]인 균등 분포로 방어 비율을 생성하였다. 게임의 최적화 결과 IPS 1, 2, 3의 포트폴리오 가중치는 각각 71.58%, 28.42%, 0%로 산출되었고, IPS 1, 2가 선택되었다. 이에 따른 최적 포트폴리오가 실행될 경우 전체 위협에 대한 최적 방어 비율은 73.95%로 도출되었다. <Table 5>는 Antivirus를 3개 선택하고 조직에 발생하는 위협이 3개인 상황에서 [0.41, 1]인 균등 분포로 방어 비율을 생성하였다. 게임의 최적화 결과 Antivirus 1, 2, 3의 포트폴리오 가중치는 각각 68.58%, 31.42%, 0%로 산출되었고, 최적화된 포트폴리오가 실행될 경우 전체 위협에 대해 최적 방어 비율은 74.25%이다.

<Table 6>은 각 정보보호 대책의 최적화된 가중치와 포트폴리오가 실행될 경우 전체 위협에 대한 방어 비율을 나타낸다.

〈Table 3〉 Game Matrix of Firewall

Countermeasure \ Threat	Threat 1	Threat 2	Threat 3
Firewall 1	93.42%	78.41%	90.67%
Firewall 2	92.97%	87.97%	82.49%
Firewall 3	81.96%	93.21%	81.38%

〈Table 4〉 Game Matrix of IPS

Countermeasure \ Threat	Threat 1	Threat 2	Threat 3
IPS 1	69.1%	92.32%	91.86%
IPS 2	86.18%	27.69%	76.88%
IPS 3	53.4%	63.88%	74.34%

〈Table 5〉 Game Matrix of Antivirus

Countermeasure \ Threat	Threat 1	Threat 2	Threat 3
Antivirus 1	79%	63.46%	80.11%
Antivirus 2	50.65%	97.79%	61.45%
Antivirus 3	99.51%	54.86%	75.55%

〈Table 6〉 Optimized Weight and Defence Probability of Countermeasures

Weight \ Countermeasure	Firewall	IPS	Antivirus
Alternative 1	49.11%	71.58%	68.58%
Alternative 2	0%	28.42%	31.42%
Alternative 3	50.89%	0%	0%
Optimized defence probability	85.94%	73.95%	74.25%

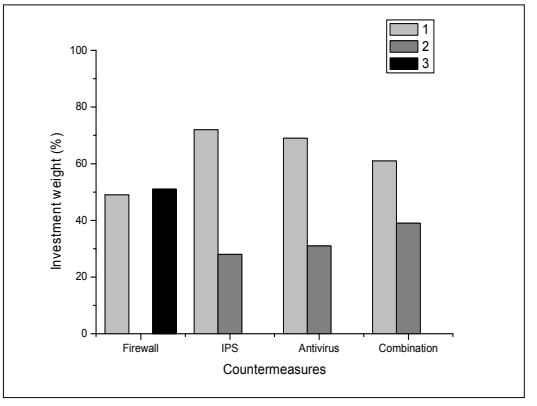
지금까지 단일의 정보보호 대책을 각 3개씩 정보시스템에 배치하는 상황을 고려하여 최적화를 진행하였다. 마지막으로 Firewall, IPS, Antivirus 세 종류의 정보보호 대책을 각각 한 개씩 배치하는 포트폴리오 최적화를 진행한다. 실제로 하나의 정보보호 위협을 방어하기 위해 여러 대책이 서로 보완적으로 필요하기 때문에, 조직은 단일 품목의 정보보호 대책을 여러 개 배치하기 보다는 다수의 정보보호 대책을 상황에 맞게 조합하여 배치한다. <Table 7>은 Firewall, IPS, Antivirus 제품 중 각각 첫번째 제품을 배치하는 게임 행렬을 구성하였다. 실제 정보보호 대책 각각의 성능 평가 환경은 다르지만, 본 연구에서는 각 대책에 대한 실험 환경과 위협의 특성이 동일하다고 가정한다.

〈Table 7〉 Game Matrix of Countermeasures

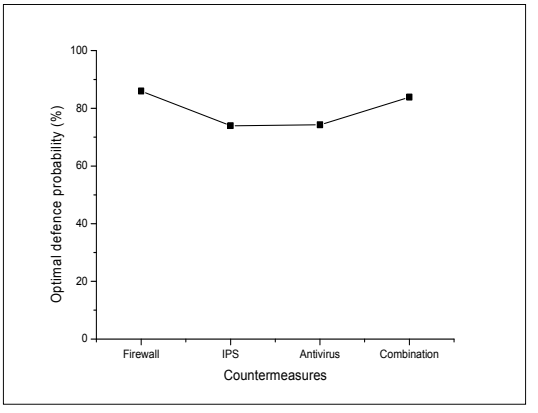
Countermeasure \ Threat	Threat 1	Threat 2	Threat 3
Firewall 1	93.42%	78.41%	90.67%
IPS 1	69.1%	92.32%	91.86%
Antivirus 1	79%	63.46%	80.11%

<Table 7>의 최적화 결과 Firewall 1, IPS 1, Antivirus 1의 포트폴리오 가중치는 각각 60.74%, 39.26%, 0%로 산출되었고 Firewall 1, IPS 1이 선택되었다. 최적화된 포트폴리오가 실행될 경우 전체 위협에 대해 최적 방어 비율은 83.87%로 도출되었다.

<Figure 1>은 각 실험에서 산출된 최적 정보보호 대책 포트폴리오의 가중치이다. 다수의 정보보호 대책을 선택해서 투자했을 경우라도 모두 성능이 다르고, 여러 종류의 정보보호 위협이 발



〈Figure 1〉 Investment Weight of Countermeasures



〈Figure 2〉 Optimal Defence Probability of Countermeasures

생하기 때문에 제한된 예산 하에서 적정 가중치로 정보보호 대책에 투자하는 것이 효과적이다. 각 실험 결과 산출된 최적화된 가중치로 포트폴리오를 구성했을 경우 최적 방어 확률은 <Figure 2>와 같다. 단일 정보보호 대책인 Firewall로 구성된 포트폴리오의 경우 방어 확률은 85.94%로 도출되었고, IPS로 구성된 포트폴리오의 경우 73.95%, Antivirus로 구성된 포트폴리오의 경우 74.25% 도출되었다. Firewall, IPS, Antivirus 제품 중 각각 첫번째 제품을 배치하여 실험하는 경우 최적 방어 확률은 83.87%로 도출되었다.

5. 결론

본 연구에서는 정보보호 대책 포트폴리오의 최적화 문제를 제시하고, 정보보호 담당자와 공격자의 관점에서 정보보호 대책과 정보보호 위협을 전략으로 하는 게임 이론을 모형화 하였다. 또한 실제 환경과 유사한 수치 예제를 이용해 제안한 게임 모형을 분석하고, 제안한 최적화 방법을 Python 3.7을 이용하여 구현하고 선형계획법으로 풀이하여 최적 해를 도출하였다. 기존 정보보호 투자 관련 연구에서는 단순한 모형만을 다루었기 때문에 현실에 적용할 수 없었고, 게임 이론을 이용한 연구에서는 정보보호 대책의 투자 여부만을 고려하고 가상의 데이터와 확률을 이용하여 결론을 도출하였지만, 본 연구에서는 투자의 여부만이 아니라, 정보보호 대책의 가중치를 산출하여 최적 포트폴리오를 구성하였다. 또한 기존의 게임 이론과 관련된 논문에서 도출한 내쉬 균형은 모든 경기자의 이익을 고려하여 최선의 전략을 도출하지만, 본 연구에서는 정보보호는 공격자의 공격을 최소화하는 방어 대책을 구해야 하기 때문에 공격자의 손실이 정보보호를 실행하는 조직의 이익이 되는 상황을 고려하여 제로섬 게임을 가정하였다. Firewall, IPS, Antivirus를 각각 한 개씩 고려하는 수치 예제에 따르면, Firewall, IPS, Antivirus가 각각 60.74%, 39.26%, 0%로 최적화 되었다. 즉, 조직의 정보보호 투자 예산을 Firewall, IPS, Antivirus에 각각 60.74%, 39.26%, 0% 비중으로 투자할 때, 조직의 총 방어 확률이 83.87%로 최대화 된다. 본 연구의 방법론과 예제를 실무에 활용하면 조직에서

는 여러 종류의 정보보호 대책을 고려할 수 있고, 각 대책의 적정 투자 수준을 조직의 예산에 반영할 수 있다. 정보보호 대책 각각의 비용을 고려하지 않고 성능을 기준으로 최적화 하였기 때문에, 본 연구에서 제안한 최적화 방법을 이용하면 조직의 정보보호 담당자는 정보보호 대책의 전략 수립 시 정보보호 대책의 특성을 고려하여 보다 효과적인 투자 의사결정을 진행 할 수 있을 것이다.

본 연구의 한계는 다음과 같다. 첫째, Firewall, IPS, Antivirus 등 기업이 고려할 수 있는 정보보호 대책의 성능을 고려하였지만, 정보보호 대책의 종류를 세 개로 제한했고, 가격을 고려하지 않았다. 향후 연구에서는 추가적인 정보를 고려할 필요가 있다. 둘째, 정보보호 대책의 성능은 실제 데이터를 사용하였지만, 데이터의 실험 환경과 위협의 특성을 모두 동일하다고 가정하였다. 향후 연구에서는 동일한 실험 환경의 데이터와 위협의 특성을 적용한다면 더 현실성 있는 분석과 결과를 제시할 수 있을 것이다. 셋째, 실무적인 관점의 검증이 이루어지지 않았다. 실무적인 관점에서 실제 정보보호 담당자의 의견을 반영하여 검증한다면 실무적인 의사결정에 도움이 될 것이다.

참고문헌(References)

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

Cavusoglu, H., B. Mishra, S. Raghunathan, "A model for evaluating IT security investments," *Communications of the ACM*, Vol.47, No.7 (2004), 87~92.

Cavusoglu, H., B. Mishra, S. Raghunathan, "The value of intrusion detection systems in information technology security architecture," *Information Systems Research*, Vol.16, No.1(2005), 28~46.

Cavusoglu, H., S. Raghunathan, W. T. Yue, "Decision-theoretic and game-theoretic approaches to IT security investment," *Journal of Management Information Systems*, Vol.25, No.2(2008), 281~304.

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

Gordon, L. A., M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security*, Vol.5, No.4(2002), 438~457.

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

Jeong, G. H., S. R. Jeong, "The effect of information protection control activities on organizational effectiveness: Mediating effects of information application," *Journal of Intelligence and Information Systems,* Vol.17, No.1(2011), 71~90.

Kong, H. K., T. S. Kim, J. Kim, "An analysis on effects of information security investments: a BSC perspective," *Journal of Intelligent Manufacturing*, Vol. 23, No.4(2012), 941~953.

Kumar, R. L., S. Park, C. Subramaniam, "Understanding the value of countermeasure portfolios in information systems security,"

Journal of Management Information Systems, Vol.25, No.2(2008), 241~280.

Kwon, Y. O., "A study on the use of a business intelligence system: the role of explanations," *Journal of Intelligence and Information Systems,* Vol.20, No.4(2014), 155~169.

National Intelligence Service, Ministry of Science and ICT, Ministry of the Interior and Safety, Korea Communications Commission, Financial Services Commission, *2019 Nation Information Security White Paper*, 2019a.

Ministry of Science and ICT, Korea Information Security Industry Association, *2019 Survey on Information Security*, 2019b.

Nash, J., "Non-cooperative games," *Annals of Mathematics*, Vol.54, No.2(1951), 286~295.

Rakes, T. R., J. K. Deane, L. P. Rees, "IT security planning under uncertainty for high-impact events," *Omega*, Vol.40, No.1(2012), 79~88.

Richardson, R., *2010/2011 CSI Computer Crime and Security Survey*, 2011.

Sawik, T., "Selection of optimal countermeasure portfolio in IT security planning," *Decision Support Systems*, Vol.55, No.1(2013), 156~164.

Seo, B. G., D. H. Park, "The theory of games and the evolution of animal conflicts," *Journal of Intelligence and Information Systems,* Vol.23, No.1(2017), 143~159.

Smith, J. M., "The theory of games and the evolution of animal conflicts," *Journal of Theoretical Biology*, Vol.47, No.1(1974), 209~221.

Von Neumann, J., O. Morgenstern, *Game Theory and Economic Behavior*, John Wiley and Sons, New York, 1944.

Von Solms, R., J. Van Niekerk, "From information security to cyber security," *Computers & Security*, Vol.38(2013), 97~102.

Abstract

Game Theoretic Optimization of Investment Portfolio Considering the Performance of Information Security Countermeasure

Sang-Hoon Lee* · Tae-Sung Kim**

Information security has become an important issue in the world. Various information and communication technologies, such as the Internet of Things, big data, cloud, and artificial intelligence, are developing, and the need for information security is increasing. Although the necessity of information security is expanding according to the development of information and communication technology, interest in information security investment is insufficient. In general, measuring the effect of information security investment is difficult, so appropriate investment is not being practice, and organizations are decreasing their information security investment. In addition, since the types and specification of information security measures are diverse, it is difficult to compare and evaluate the information security countermeasures objectively, and there is a lack of decision-making methods about information security investment. To develop the organization, policies and decisions related to information security are essential, and measuring the effect of information security investment is necessary. Therefore, this study proposes a method of constructing an investment portfolio for information security measures using game theory and derives an optimal defence probability. Using the two-person game model, the information security manager and the attacker are assumed to be the game players, and the information security countermeasures and information security threats are assumed as the strategy of the players, respectively. A zero-sum game that the sum of the players' payoffs is zero is assumed, and we derive a solution of a mixed strategy game in which a strategy is selected according to probability distribution among strategies. In the real world, there are various types of information security threats exist, so multiple information security measures should be considered to maintain the appropriate information security level of information systems. We assume that the defence ratio of the information security countermeasures is known, and we derive the optimal solution

* Department of MIS, Chungbuk National University
** Corresponding author: Tae-Sung Kim
Department of MIS, Chungbuk National University
1 Chungdae-ro, Seowon-gu, Cheongju-si, Chungbuk 28644, South Korea
E-mail : kimts@chungbuk.ac.kr

of the mixed strategy game using linear programming. The contributions of this study are as follows. First, we conduct analysis using real performance data of information security measures. Information security managers of organizations can use the methodology suggested in this study to make practical decisions when establishing investment portfolio for information security countermeasures. Second, the investment weight of information security countermeasures is derived. Since we derive the weight of each information security measure, not just whether or not information security measures have been invested, it is easy to construct an information security investment portfolio in a situation where investment decisions need to be made in consideration of a number of information security countermeasures. Finally, it is possible to find the optimal defence probability after constructing an investment portfolio of information security countermeasures. The information security managers of organizations can measure the specific investment effect by drawing out information security countermeasures that fit the organization's information security investment budget. Also, numerical examples are presented and computational results are analyzed. Based on the performance of various information security countermeasures: Firewall, IPS, and Antivirus, data related to information security measures are collected to construct a portfolio of information security countermeasures. The defence ratio of the information security countermeasures is created using a uniform distribution, and a coverage of performance is derived based on the report of each information security countermeasure. According to numerical examples that considered Firewall, IPS, and Antivirus as information security countermeasures, the investment weights of Firewall, IPS, and Antivirus are optimized to 60.74%, 39.26%, and 0%, respectively. The result shows that the defence probability of the organization is maximized to 83.87%. When the methodology and examples of this study are used in practice, information security managers can consider various types of information security measures, and the appropriate investment level of each measure can be reflected in the organization's budget.

Key Words : Game theory, Information security, Investment portfolio

Received : June 3, 2020 Revised : June 25, 2020 Accepted : July 19, 2020
Corresponding Author : Tae-Sung Kim

저 자 소 개

이 상 훈

충북대학교 경영정보학과에서 석사 학위를 취득하였고, 현재 경영정보학과 박사과정에 재학 중이다. 주요 관심 분야는 정보통신과 정보보호 분야의 경영 의사결정 및 최적화이다.

김 태 성

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.