경영정보학연구
제25권 제4호, 2023년 11월 http://dx.doi.org/10.14329/isr.2023.25.4.027

정보보호 대책의 효과성을 고려한 정보보호 투자 의사결정 지원 모형

A Model for Supporting Information Security Investment Decision-Making Considering the Efficacy of Countermeasures

박 병 조 (Byeongjo Park) 충북대학교 융합보안협동과정 박사과정
김 태 성 (Tae-Sung Kim) 충북대학교 경영정보학과 교수/보안경제연구소장, 교신저자

요 약

정보통신기술의 발달로 정보보호의 중요성이 커졌지만, 기업은 제한된 예산 내에서 적절한 대책을 선택하는 데 어려움을 겪고 있다. Sönmez and Kılıç(2021)는 정보 보안 침해를 완화하기 위한 최적의 투자 조합을 결정하기 위해 AHP 및 혼합 정수 계획을 사용하는 모델을 제안했다. 그러나 1) 보안 위협에 대한 보안 대책의 효과를 객관적으로 측정하지 못하고, 2) 투자로 인한 위험 감소가 투자 이전에 측정한 위험 수준을 초과하는 비현실적인 현상이 발생하고, 3) 여러 위협에 대해 단일 대응책을 사용할 때 중복된 투자가 이루어진다는 한계가 있었다. 본 연구에서는 베타 확률 분포를 사용하여 대책의 효과를 객관적으로 정량화하고, 위험 감소 수준이 투자 이전에 측정된 위험 수준을 초과하지 않고 보안 대책이 중복 투자되지 않도록 최적화 모델을 개선했다. 개선된 모델을 국내 중소기업을 대상으로 실증분석한 결과, Sönmez and Kılıç(2021)의 최적화 모델보다 더 나은 결과를 도출했다. 개선된 최적화 모델을 사용하면 정보보호 비용, 수량, 대책 효율성을 고려하여 고정된 예산 내에서 최적의 대책별 투자 포트폴리오를 도출할 수 있고, 정보 보안 예산을 확보하고 정보 보안 위협을 효과적으로 해결하는 데 도움이 될 것이다.

키워드 : 정보보호 투자, 정보보호 대책 효과성, AHP, MIP, 의사결정지원 시스템, 시각화

Ⅰ. 서 론

정보보호는 신중하고 시기적절한 방식으로 처리되어야 하는 매우 복잡한 문제로 정보보호 담당자는 악의적인 공격에 현명하게 대응해야 한다(Sönmez and Kılıç, 2021). 정보보호 담당자의 주요 과제 중 하나는 정보보호와 관련된 위협에 대응하기 위해 정해진 예산 범위에서 최적의 대책을 선택해서 조직의 위험을 낮추는 것이다(Fielder *et al.*, 2016). 정보보호 담당자는 기업의 정보자산을 지키기 위해 최고 경영진의 지원을 받아야 하고, 최고

† 본 과제(결과물)는 2023년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다(2021RIS-001).

경영진의 지원을 받기 위해 올바른 보안 지출 계획을 세우고 최적의 대책을 선택하기 위해선 기업의 취약성을 유발하는 위협적인 행동이나 상황을 분석해야 한다(Solms, 1996; Sönmez and Kılıç, 2021).

끊임없이 진화하는 정보보호 위협은 기업의 정보 자산에 지속적으로 위협을 가하여 기업의 신뢰성, 경쟁력, 고객 신뢰 및 재정적 이익에 영향을 미친다(Whitman and Mattord, 2016). 정보통신 기술의 지속적인 발전으로 사이버 공격, 범죄 및 보안 위반은 더욱 정교하고 빈번하게 일어나고 있으며, 여러 산업 분야에서 운영되는 기업들은 다양한 보안 사고로 인해 기업의 귀중한 자산에 심각한 피해가 발생하고 있다(Miaoui and Boudriga, 2019). 따라서, 보안은 더욱 강화되어야 하고, 보안사고의 위험을 줄이기 위해 우선적으로 적용되어야 할 주요 보안요인들을 도출할 필요가 있다(허진, 이애리, 2020). 사이버 공격과 같은 문제가 조직 내 IT 시스템 보안의 중요성을 부각시켰고 지금까지 실무와 이론에서 많은 관심을 받아왔다(Heidt *et al.*, 2019).

Gartner(2022)의 조사결과를 따르면 전세계적으로 정보 보안 및 리스크 관리 제품 및 서비스에 대해 2022년에는 1,691억 달러를 지출했고, 2023년에는 11.3% 증가해 1,883억 달러 이상 지출 할 것으로 예상한다. 그러나 투자 증가에도 불구하고 IBM 시큐리티(2022)의 '2022 데이터 유출 비용 연구 보고서'에 의하면 최근 2년간 보안 사고로 인한 관련 비용이 12.7% 늘어났고, Ponemon(2020)의 4,150명 이상의 IT보안 리더와 현직자 대상 조사 결과에 의하면 응답자의 72%는 보안 투자를 적절하게 활용하지 못한다고 조사되었다. 중소기업의 경우 Kaspersky(2021)의 조사에 의하면 50명 이상 중소기업의 보안 지출은 15만 달러로 상대적으로 적은 비용을 지출하고 있고, 중소기업의 관심사는 데이터 보안 문제와 정보보호를 위한 비용 확보의 어려움이 있다고 조사되었다. 중소기업은 정보보호 투자 비용이 부족하기 때문에 보안 관리를 위한 기술이나 장비 구축에 어려움을 겪고 있다(Armenia *et al.*, 2021). 정보보호 투자는 올바른 보안 지출 계획을 세우고 최적의 대책을 선택하기 위해선 기업의 취약성을 유발하는 위협적인 행동이나 상황을 분석해야 하며, 정보보호 대책의 성능을 객관적으로 비교하고 평가할 수 있어야 한다(이상훈, 김태성, 2020; Sönmez and Kılıç, 2021).

본 연구는 이러한 문제점들을 바탕으로 Sönmez and Kılıç(2021)의 모델을 개선하고 투자 결과를 도출한다. Sönmez and Kılıç(2021)는 위협별 위험의 상대적 크기를 구하기 위해 전문가 대상으로 AHP 방법을 적용한다. 최적화 모델은 정보보호 대책 비용, 수량을 고려해 제한된 예산 내에서 감소되는 위험 크기를 최대화하고, 목표 위험 감소율에 소요되는 예산을 최소화하기 위해 혼합정수계획법을 사용해 최적화 모델을 만들었다. 그러나 정보보호 위협을 대처하는 정보보호 대책의 효과성을 주관적으로 측정하여 객관적인 판단이 어려우며, 최적화 모델을 만들 때 전체 위험 크기를 감소시키는 것을 목표로 만들어 정보보호 대책을 통해 감소되는 위험 크기 각 위협의 위험 크기가 보다 커지는 현실적인 문제가 발생했고, 하나의 정보보호 대책이 여러 정보보호 위협에 사용될 때 중복 비용 지출을 고려하지 않은 문제가 발생했다. 본 연구에서는 Sönmez and Kılıç(2021) 모델의 세가지 문제점을 개선한 최적화 모델을 제시하고, 중소기업에 적용하기 위해 국내 정보보호 공시의 정보보호 예산과 조달청 나라장터에서 제공하고 있는 정보보호 대책 비용을 참고하여 Sönmez and Kılıç(2021) 모델의 결과와 비교하였다.

Ⅱ. 문헌고찰

정보보호 투자 의사결정 지원을 위한 연구는 크게 경제성, 보안 위험 평가, 투자 최적화 관점으로 연구되어 왔다. Gordon and Loeb(2002)은 보안 사고로 인한 손실을 관련 취약성을 줄이는 데 필요한 투자와 비교했고 정보 보호 투자비용은 정보보호 피해 예상 금액의 37%를 초과하면 안 된다는 정보보호 투자 경제성에 대한 연구 결과를 도출하

였다. 그러나 외부 효과와 같은 불확실성을 고려하지 않은 한계점을 가지고 있었지만, Gordon *et al.*(2014)은 Gordon and Loeb(2002)의 사이버 투자 모델을 확장하여 외부 효과를 통합함으로써 한계점을 해결했다.

보안 위험 평가는 정성적, 정량적 비교가 동시에 평가되어야 하는 복잡한 의사 결정으로 AHP 기법을 이용한 평가 연구가 일반적으로 사용되어 왔다. Bodin *et al.*(2005)은 AHP 기법을 활용하여 기밀성, 가용성 및 무결성과 같은 보안 속성 기준으로 보안 투자 비교했고, 정보보호 목표를 효율적으로 달성할 수 있도록 적합한 투자기준을 제시하였다. Kong *et al.*(2008)은 정보보호 제품을 선정하는 과정을 AHP 기법으로 모델링 하고, 실증자료를 통해 수치 예제를 제공하여, 실무적으로 사용할 수 있는 평가모델을 제시하였다.

정보보호 투자 최적화는 유전자 알고리즘, 게임이론, 정수계획법 등과 같은 최적화 방법론 통해 연구되어 왔다. Gupta *et al.*(2006)은 정보보호 대책의 운영비용과 취약점을 최소화하는 보안 포트폴리오를 유전자 알고리즘을 통해 구성했다. 임정현과 김태성(2020)은 정해진 정보보호 예산 범위내에 적절한 정보보호 투자 포트폴리오를 구성하기 위해 유전자 알고리즘을 사용해 산업군별 침해사고 데이터와 정보보호 대책의 수준을 고려한 최적화 모델을 제시했다.

Cavusoglu *et al.*(2008)은 투자 수준, 취약성 및 투자 보상을 게임 이론을 통해 전략적인 투자 방법을 제시했다. Sawik(2013)은 사이버 위협을 방지하거나 완화하기 위해 최적의 대응책 선택을 다루기 위해 혼합정수계획법 접근 방식을 제안했으며, 제한된 예산 내에 잠재적인 손실을 최소화했다. Fielder *et al.*(2016)은 한정된 예산 내에 최적의 투자 전략을 도출하기 위해 게임 이론과 배낭 알고리즘을 결합하여 정보보호 투자 포트폴리오를 구성했다. Sönmez and Kılıç(2021)는 최적의 정보보안 위험 관리 및 투자 결정을 위해 AHP 기법을 통해 위협의 위험 크기를 측정하고, 정보보호 대책의 개수와 금액을 고려하여 제한된 예산 내에 위험 크기를 최대화하는 것과 목표 전체 위험 감소율에 대해 예산을 최소화하기 위해 혼합정수계획법을 통한 두가지 최적화 모델을 제시하였다.

위 연구들은 다양한 방법을 통해 정보보호 투자 의사결정 지원에 도움을 주었다. 하지만, Sönmez and Kılıç(2021)의 연구를 제외하고는 보안 위험 평가, 제한된 예산, 정보보호 대책 비용, 수량, 효과성 중 일부만 고려하여 실제 기업에 적용하기에 어려움이 있다. Sönmez and Kılıç(2021)는 실제 기업에 적용할 수 있게 보안 위험 평가, 제한된 예산, 정보보호 대책 비용, 개수, 효과성을 모두 고려했지만 전체 위험 크기에 중점을 두고 최적화 모델 연구를 진행해서 일부 위험 크기가 정보보호 대책을 통해 감소되는 위험 크기보다 작아지는 문제가 발생했다. 모든 정보보호 대책은 모든 위협에 대해 완벽하게 막을 수가 없는 현실의 상황에 맞지 않는 결과를 만들었다(Bodin *et al.*, 2008). 그리고, 하나의 정보보호 대책이 둘 이상의 위협에 대해 방어할 때 정보보호 대책의 비용을 방어하는 위협의 개수만큼 지출하여 지출금액이 예상보다 높게 나오는 문제가 발생했다. 또한 정보보호 대책의 효과성 측정을 연구자가 직접 측정해 실제 기업에 적용하기 어려운 문제가 있다.

본 연구는 Sönmez and Kılıç(2021)의 연구 모델의 문제점 및 한계점을 개선하는 모델을 만들었다. 실제 환경에 적용하기 위해 국내 정보보호 공시 정보보호 예산 정보와 조달청 나라장터에서 제공하고 있는 정보보호 대책 비용을 참고하였고, 위협에 대한 정보보호 대책의 효과성은 정보보호 대책 효과성 분석 보고서를 참고해 선행 연구와 비교 분석해 결과를 도출했다.

Ⅲ. 연구 모형

3.1 보안 위험 평가

위험 크기 측정을 위한 보안 위험 평가는 Sönmez

and Kılıç(2021)의 AHP 기법을 통한 위험 크기 측정 모델을 사용했다.

보안 위험 평가는 자산, 취약점, 위협을 고려하여 평가를 진행해야 된다. 위협은 자산의 손실 및 취약점을 발생시키는 원인으로 위협에 대한 평가가 우선 진행되어야 된다. n개의 정보보호 위협의 유형이 있으면 기업의 특성에 따라 물리적 위치, 보안 대상, 부서 또는 업무 부서 및 비즈니스 프로세스 등을 기준으로 그룹화 할 수 있다. 위협 그룹과 위협이 정의되면 위협 발생 가능성과 심각도에 대해 보안 전문가 대상으로 AHP 보안 위험 평가를 수행하고 일관성 지수 상한을 초과하게 되면 재평가를 진행한다. 보안 전문가가 둘 이상일 경우 개별적으로 평가를 진행하고, 일관성 지수가 0.2 이상의 결과는 제외하고 0.2 미만의 평가 결과를 가지고 기하평균을 통해 단일 평가 값을 도출한다.

i: 정보보호 위협(i = 1, ⋯, n)
$U(i)$: 정보보호 위협 i가 속한 그룹
$ESG_{U(i)}$: 위협 i가 속한 그룹의 심각도
ESW_i: 위협 i의 심각도
ST_i: 위협 i의 전체 심각도
$ELG_{U(i)}$: 위협 i가 속한 그룹의 발생 가능성
ELW_i: 위협 i의 발생 가능성
LT_i: 위협 i의 전체 발생 가능성
MT_i: 위협의 위험 크기

위협의 위험 크기(The magnitude of risks of the threat, MT)를 구하는 식은 다음과 같다.

$$ST_i : ESG_{U(i)} \times ESW_i, \ \forall i = \{1, 2, ..., n\} \quad (1)$$
$$LT_i : ESG_{U(i)} \times ELW_i, \ \forall i = \{1, 2, ..., n\} \quad (2)$$
$$MT_i : ST_i \times LT_i, \ \forall i = \{1, 2, ..., n\} \quad (3)$$

위협에 대한 전체 심각도(The severity levels for the threat, ST)와 전체 발생 가능성(The likelihood levels for the threat, LT)에 대한 크기를 구한다. ST는 (1)과 같이 위협이 속한 그룹의 심각도(The eigenvectors for the severity for groups, ESG)와 그룹 내 위협의 심각도(The eigenvectors for the severity for threats within groups, ESW) 가중치를 곱한 값이고, LT는 (2)와 같이 위협이 속한 그룹의 발생 가능성(The eigenvectors for the likelihood for groups, ELG)과 그룹 내 위협의 발생 가능성(The eigenvectors for the likelihood for threats within groups, ELW) 가중치를 곱한 값이다. MT는 (3)과 같이 ST와 LT의 곱이다.

3.2 정보보호 대책의 효과성 측정

n개의 정보보호 위협을 예방 및 대응하기 위해선 m개의 대책이 필요하며, 기업의 규모별로 정보보호 대책의 비용(Cost of countermeasure, CC)과 최대 수량(Maximum number of countermeasure, MC)이 달라진다.

r: 정보보호 대책(r = 1, ⋯, m)
CC_r: 정보보호 대책 r의 비용
MC_r: 정보보호 대책 r의 최대 수량

정보보호 대책은 여러 위협에 사용할 수 있으며, 정보보호 대책의 효과성은 위협 별로 다르다. Sönmez and Kılıç(2021)는 경험에 기반한 효과성 측정방식을 사용했다. 경험 기반 효과성은 상황에 따라 달라지기 때문에 객관적으로 사용하기 어려운 점이 있고, 정보보호 전문가가 아니면 측정하기 어려운 문제점이 있다. 따라서 본 논문에서는 Kumar *et al.*(2008)의 효과성 측정방식인 베타 확률 분포 식을 사용해 위협에 대한 정보보호 대책의 효과성(Efficacy of Countermeasure, EC)을 구했으며, 변수에 대한 정의와 식은 다음과 같다.

- a_{ir}: i위협에 대한 r대책의 낙관적 효과성
- b_{ir}: i위협에 대한 r대책의 비관적 효과성
- m_{ir}: i위협에 대한 r대책의 근사적 효과성

- EC_{ir}: i위협에 대한 r대책의 효과성 기대치

$$EC_{ir} = \frac{a_{ir} + 4m_{ir} + b_{ir}}{6} \quad (4)$$
$$\forall i = \{1, 2, ..., n, \ \forall r = \{1, 2, ..., l\}$$

위협에 대한 대책의 효과성이 가장 좋을 때를 낙관적 효과성(Optimistic efficacy) a, 가장 효과가 안 좋을 때를 비관적 효과성(Pessimistic efficacy) b, 일반적인 효과를 가질 때를 근사적 효과성(Most likely efficacy) m이라 한다. 이때, 위협에 대한 대책의 기대효과 추정치는 베타 분포를 따른다는 것을 가정하고 이러한 확률분포를 이용하여 효과성에 대한 기대값은 (4)와 같다.

3.3 정보보호 투자 최적화 모델

Sönmez and Kılıç(2021)의 최적화 모델은 정보보호 위협에 대한 위험 크기를 고려해 정보보호 투자 최적화 모델을 만들었지만 두 가지 문제점이 있다. 첫 번째는 위협 별 위험의 크기가 정보보호 대책을 통해 감소되는 위험의 크기보다 작아지는 문제가 발생했고, 두 번째는 단일 정보보호 대책이 여러 정보보호 위협에 사용될 때, 각 위협 별로 해당 정보보호 대책의 비용을 중복 산정하는 문제가 발생했다. 본 연구에서는 이러한 문제점들을 해결하기 위해 다음과 같은 두 가지 조건을 추가해 모델을 개선했다.

추가 조건 1: 정보보호 대책으로 감소되는 각 위협의 위험 크기는 각 위협의 위험 크기보다 작거나 같아야 한다.

추가 조건 2: 정보보호 대책의 비용은 정보보호 위협의 수와 관계없다.

최적화 목표 1: 가용 예산(B)에 대한 감소된 전체 위험 크기 최대화

$$maximize \sum_{i=1}^{n} \sum_{r=1}^{l} MT_i \times EC_{ir} \times x_r \quad (5)$$

$$subject\ to \sum_{r=1}^{l} CC_r \times x_r \le B \quad (6)$$

$$and \sum i = 1^{n} \sum_{r=1}^{l} MT_i \times EC_{ir} \times x_r < MT_i \quad (7)$$

$$for\ 0 \le x_r \le MC_r, \quad (8)$$
$$\forall i = \{1, 2, ..., n, \ \forall r = \{1, 2, ..., l\}$$

최적화 목표 1에 대한 모델에서 제약 조건은 (6)과 같이 사용되는 모든 정보보호 대책이 예산보다 적거나 같아야 하며, (7)과 같이 각 위협의 위험 크기를 넘지 않도록 대책을 선택해야한다. 목표하는 전체 위험 감소량에 대해 예산을 최소화하는 최적의 정보보호 대책 선택은 (9)와 같이 결정된다. 이때 x_r는 정보보호 대책 r의 최대 개수인 MC_r를 초과할 수 없다.

최적화 목표 2: 목표 전체 위험 감소량(V)에 대한 예산 최소화

$$minimize \sum_{r=1}^{l} CC_r \times x_r \quad (9)$$

$$subject\ to \sum_{i=1}^{n} \sum_{r=1}^{l} MT_i \times EC_{ir} \times x_r \ge V \quad (10)$$

$$and \sum_{i=1}^{n} \sum_{r=1}^{l} MT_i \times EC_{ir} \times x_r < MT_i \quad (11)$$

$$for\ 0 \le x_r \le MC_r, \quad (12)$$
$$\forall i = \{1, 2, ..., n\}, \ \forall r = \{1, 2, ..., l\}$$

최적화 목표 2에 대한 모델에서 제약 조건으로 (10)과 같이 모든 정보보호 대책으로 인해 감소되는 전체 위협의 위험 크기가 목표 전체 위험 감소량 보다 크거나 같아야 하며, (11)과 같이 각 위협의 위험 크기를 넘지 않도록 대책을 선택해야 한다. 이때 x_r는 정보보호 대책 r의 최대 개수인 MC_r를 초과할 수 없다.

〈표 1〉 정보보호 투자 최적화 실험 시나리오

	시나리오 1	시나리오 2
최적화 목표 1. 가용 예산	5,000만 원	1억 원
최적화 목표 2. 목표 위험 감소량	60%	90%

Ⅳ. 실험결과

본 연구의 실험은 직원 수 100명인 중소기업이 정보보호에 대한 최초 투자를 한다고 가정했고, <표 1>과 같이 두 가지 목표에 대해 Sönmez and Kılıç(2021)의 최적화 모델과 본 논문에서 제시한 모델을 비교 분석하는 실험을 진행하였다.

4.1 실험 데이터

보안 위험 평가를 하기 위해 이경률 등(2018)의 기반시설 위협 분류를 참고하여 위협 목록을 <표 2>와 같이 작성하였다.

기반시설 위협은 대항목으로 오프라인 위협, 온라인 내부 위협, 온라인 외부 위협으로 분류된다. 각 세부항목에 대해선 오프라인 위협에는 자연재해, 정전, 물리적 위협, 조작 미숙, 조작 실수가 있고, 오프라인 내부 위협은 내부 직원, 협력업체가 있으며, 온라인 외부 위협은 사회공학 공격, 내부정보수집, 위장, 권한 획득, 비인가 접근, 데이터 유출, 과부화 유발, 시스템 결함, 위·변조, 악성코드로 분류된다.

보안 위험 평가는 2021년 11월 정보보안 컨설턴트 대상으로 기업 정보보호 위협의 발생 가능성과 기업 정보보호 위협의 심각도에 대한 설문조사를 실시하였고 8부 회수하였다. 8명의 응답자 중 결손치가 있는 응답지 및 일관성 비율이 0.2 이상인 응답지를 제외하고 총 4부를 유효 데이터로 판단했다. 4명의 전문가 의견을 기하평균을 사용하여 집단의견의 중요도를 산출하였고 소수점 네 번째에서 반올림하였다.

〈표 2〉 기반시설 위협 목록

대항목	세부항목	설명
오프라인 위협	자연재해	자연재해로 인해 시스템이 고장 나거나 파괴되어 기반시설 운영 중지
	정전	자연재해 또는 악의적인 전원공급 차단으로 기반시설의 전력공급 중단
	물리적 위협	기반시설 및 장비에서의 물리적인 문제 발생 전자 장비의 오염으로 인한 사용 불능, 전자기파로 인한 사용 불능, 시스템에서 활용하는 하드웨어에 고장 및 파괴, 시스템과 관련된 하드웨어 절도
	조작 미숙	기반시설을 담당하는 사람의 잘못된 조작으로 인한 입력 오류
	조작 실수	기반시설을 담당하는 사람의 실수로 잘못된 정보를 입력 또는 잘못된 절차의 운영
온라인 내부 위협	내부 직원	내부 직원이 의도적으로 기밀정보를 유출하거나 시스템의 운영 중지 및 파괴
	협력 업체	협력업체 직원이 의도적으로 기밀정보를 유출하거나 시스템의 운영 중지 및 파괴
온라인 외부 위협	사회공학 공격	악성코드가 포함된 스팸 메일 및 스피어 피싱 메일을 통한 시스템 내부 침투
	내부정보수집	미디어 탐색, 트래픽 분석, 도·감청 및 스니핑을 통해 인증정보 및 기밀정보와 같은 침입에 필요한 정보 수집
	위장	공격자가 정상적인 기기 및 시스템으로 위장해 전달되는 정보 및 침투에 필요한 정보를 수집하여 접근을 우회하거나 인증을 우회
	권한 획득	리소스 및 시스템에 권한이 없는 공격자가 권한을 획득하기 위해 우회 제어 및 권한을 위조하여 악의적인 행위 수행
	비인가 접근	인가되지 않은 공격자가 시스템으로부터 인가받기 위해 시스템에 대한 비인가 조작 시도
	데이터 유출	외부자에 의한 시스템의 접근 및 권한, 기밀정보와 관련된 비밀번호, 하드웨어 및 소프트웨어 정보, 공정 처리 정보, 자산정보 유출
	과부하 유발	시스템 구동 방해를 위해 시스템의 처리능력을 넘어서는 운영을 시도하는 공격(DoS 및 DDoS 공격)
	시스템 결함	시스템 구동을 위해 설치된 운영체제 및 프로그램에 존재하는 취약점에 의해 발생하는 위협
	위·변조	비인가된 공격자가 인증 관련 정보를 위·변조하여 시스템에 접근을 시도하거나 악의적인 의도로 데이터 변조
	악성코드	랜섬웨어, 트로이 목마, 중간자 공격 등을 통한 시스템 침투

정보보호 위협의 심각도는 <표 3>과 같이 자연재해, 내부 직원, 물리적 위협, 조작 미숙, 조작 실수 순으로 높았고, 정보보호 위협의 발생 가능성은 <표 4>와 같이 협력업체, 사회공학 공격, 악성코드,

〈표 3〉 정보보호 위협의 심각도 AHP 평가 결과

대항목	대항목 간 상대적 가중치	세부항목	대항목 대비 세부항목 간 상대적 가중치	전체 세부항목 간 상대적 가중치	순위
오프라인 위협	0.493	자연재해	0.5571	0.3792	1
		정전	0.0522	0.0355	7
		물리적 위협	0.1302	0.0887	4
		조작 미숙	0.1302	0.0887	4
		조작 실수	0.1302	0.0887	4
온라인 내부 위협	0.311	내부 직원	0.8333	0.0983	2
		협력업체	0.1667	0.0197	11
온라인 외부 위협	0.196	사회공학 공격	0.213	0.0429	6
		내부정보수집	0.0215	0.0043	17
		위장	0.0524	0.0106	16
		권한 획득	0.1017	0.0205	9
		비인가 접근	0.1009	0.0203	10
		데이터 유출	0.1599	0.0322	8
		과부하 유발	0.0903	0.0182	14
		시스템 결함	0.0945	0.019	13
		위·변조	0.0685	0.0138	15
		악성코드	0.0972	0.0196	12
합계	1		3	1	

〈표 4〉 위협의 발생 가능성 AHP 평가 결과

대항목	대항목 간 상대적 가중치	세부항목	대항목 대비 세부항목 간 상대적 가중치	전체 세부항목 간 상대적 가중치	순위
오프라인 위협	0.493	자연재해	0.0354	0.0038	17
		정전	0.1072	0.0114	15
		물리적 위협	0.0634	0.0067	16
		조작 미숙	0.3142	0.0334	12
		조작 실수	0.4798	0.0509	7
온라인 내부 위협	0.311	내부 직원	0.1667	0.0434	9
		협력업체	0.8333	0.2171	1
온라인 외부 위협	0.196	사회공학 공격	0.2482	0.1572	2
		내부정보수집	0.1116	0.0707	4
		위장	0.044	0.0279	13
		권한 획득	0.0915	0.058	6
		비인가 접근	0.0933	0.0591	5
		데이터 유출	0.0552	0.0349	11
		과부하 유발	0.071	0.0449	8
		시스템 결함	0.0684	0.0433	10
		위·변조	0.0351	0.0222	14
		악성코드	0.1818	0.1151	3
합계	1		3	1	

〈표 5〉 정보보호 위협의 위험 크기

	세부항목	심각도 가중치	발생 가능성 가중치	위험 크기	순위
오프라인 위협	자연재해	0.3792	0.0038	0.0014	7
	정전	0.0355	0.0114	0.0004	14
	물리적 위협	0.0887	0.0067	0.0006	13
	조작 미숙	0.0887	0.0334	0.003	5
	조작 실수	0.0887	0.0509	0.0045	2
온라인 내부 위협	내부 직원	0.0983	0.0434	0.0043	3
	협력업체	0.0197	0.2171	0.0043	3
온라인 외부 위협	사회공학 공격	0.0429	0.1572	0.0067	1
	내부정보수집	0.0043	0.0707	0.0003	16
	위장	0.0104	0.0279	0.0003	17
	권한 획득	0.0205	0.058	0.0012	9
	비인가 접근	0.0203	0.0591	0.0012	8
	데이터 유출	0.0322	0.0349	0.0011	10
	과부하 유발	0.0182	0.0449	0.0008	12
	시스템 결함	0.019	0.0433	0.0008	11
	위·변조	0.0138	0.0222	0.0003	15
	악성코드	0.0196	0.1151	0.0023	6
합계		1	1	0.0335	

사회공학 공격, 내부정보수집, 비인가 접근 순으로 나왔다. 정보보호 위협의 위험 크기는 <표 5>와 같이 사회공학 공격, 조작 실수, 조작 미숙, 내부 직원, 협력업체, 조작 미숙 순으로 높다고 평가되었다.

4.2 정보보호 위협을 대처하는 정보보호 대책 선택 및 효과성 측정

본 연구에서 정보보호 각 위협에 할당할 수 있는 정보보호 대책의 개수는 최적화 계산시간을 고려하여 최대 3개로 가정하였고, 정보보호 대책의 개수가 아닌 사용 여부에 따라 계산할 수 있게 비용을 작성했다. 정보보호 대책은 Sönmez and Kılıç(2021)의 정보보호 대책을 참고했고, 정보보호 대책별 비용은 2022년 1월 국내 조달청 나라장터 종합쇼핑몰과 한국인터넷진흥원의 정보보호 공시를 참고하였다(한국인터넷진흥원, 2020; 국가종합전자조달청, 2023).

정보보호 대책의 효과성 중 firewall, IPS, anti-virus와 같은 일부 소프트웨어는 다양한 환경에서 실험을 통해 효과성을 측정하여 예측 결과를 확인할 수 있지만, 정책수립, 정보보호 교육 등과 같은 보안 제품 및 서비스는 효과성을 측정하기 어려운 한계점이 있다.

본 연구에서는 이러한 한계점을 고려하여 NSS labs의 Next Generation Firewall Comparative Analysis Report(2021), Next Generation Intrusion Prevention System Comparative Report(2019)를 기반으로 효과성의 범위를 도출하였다(NSS Labs, 2019; Skybakmoen, 2021). Next Generation Firewall Comparative Analysis Report (2021)은 12개 벤더의 Firewall 제품을 실험하였고 방어 성능을 여러 가지 환경에 따라 평가하여 종합적인 효과를 도출하였다. 실험 결과 최고 97.9%, 최저 77.7%로 나타났다. Next Generation Intrusion Prevention System Comparative Report (2019)는 9개 벤더의 IPS 제품을 실험하였고, 실험 결과 제품의 성능은 최고 99.9%, 최저 60.1%로 나타났다. 정보보호 대책 효과는 소수점 첫째자리에서 반올림하였고, 베타분포를 이용한 정보보호 대책

의 효과성 기대치를 구하기 위해 낙관적 효과성 a와 비관적 효과성 b의 범위를 정보보호 대책 보고서를 기반으로 도출하고 m의 범위는 a와 b의 사이 값을 갖을 수 있게 범위를 <표 6>과 같이 도출하였다.

정보보호 위협에 대해 정보보호 대책의 낙관적, 비관적, 근사적 효과성은 <표 6>의 범위 내에서 랜덤하게 추출하고, 효과성의 기대치를 구했다. 이때, 위협에 대한 정보보호 대책이 1개 일 때 효과성을 그대로 사용하지만, 정보보호 대책이 2개 이상 일 때는 대책 간의 상호작용을 고려해 비율을 조절했다. 최적화를 위해 필요한 각 위협의 위험 크기, 정보보호 대책의 금액, 효과성 정보는 <표 7>과 같이 정리하였다.

〈표 6〉 대책 효과성 범위

	Lower Bound	Upper Bound	Distribution
optimistic a	98%	100%	Uniform[0.98, 1]
pessimistic b	0%	60%	Uniform[0, 0.6]
most likely m	b%	a%	Uniform[b, a]

〈표 7〉 정보보호 위협 별 정보보호 대책과 효과성

정보보호 위협	정보보호 대책 1			정보보호 대책 2			정보보호 대책 3		
	예방 대책	효과성	금액 (만원)	예방 대책	효과성	금액 (만원)	예방 대책	효과성	금액 (만원)
자연재해	CDR	0.75	50,000						
정전	UPS	0.41	364,000	CDR	0.59	50,000			
물리적 위협	서버 복제	0.37	2,000	물리적 보안 강화	0.49	1,500	물리적 백업	0.15	1,000
조작 미숙	보안교육 및 평가	0.59	150	감사	0.41	500			
조작 실수	데이터 배포 및 거버넌스 정책 개선	0.59	1,500	휴가	0.41	0			
내부 직원	운영 분리	0.41	0	필수 휴가	0.17	0	채용 전 면접	0.42	0
협력 업체	보안교육 및 평가	0.46	150	감사	0.54	500			
사회공학 공격	이메일 보안 기술	0.51	720	자동실행 비활성화	0.49	0			
내부정보 수집	트래픽 관리	0.42	2,100	암호화 솔루션	0.29	700	Load and Unload Drivers	0.29	0
위장	Load and Unload Drivers	0.44	0	IPS	0.56	3,400			
권한 획득	디지털 서명	0.53	1,600	IAM 시스템	0.47	800			
비인가 접근	감사	0.14	500	IPS	0.44	3,400	신뢰 가능한 채널	0.42	320
데이터 유출	암호화 솔루션	0.76	700	강력한 암호	0.24	550			
과부하 유발	대역폭 확장	0.3	1,000	트래픽 관리	0.7	2,100			
시스템 결함	정기적인 소프트웨어 패치	0.4	0	SLA, PaaS	0.6	900			
위・변조	암호화 솔루션	0.66	700						
악성 코드	안티바이러스	0.37	500	방화벽	0.28	2,500	IPS	0.35	3,400

4.3 실험 결과

4.3.1 가용 예산 내에 감소된 전체 위험 크기 최대화

가용예산 5천만 원에 대한 최적화 결과는 <표 8>과 같다.

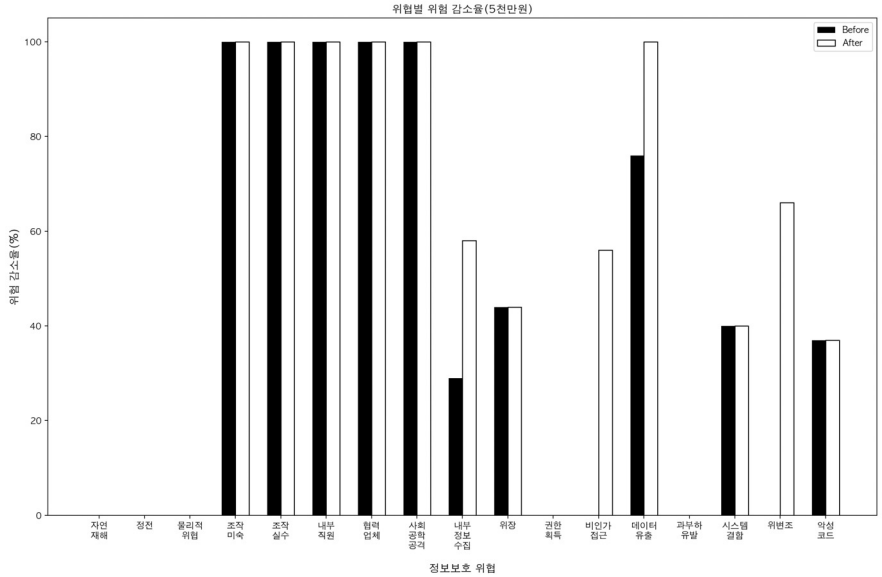
개선 모델이 Sönmez and Kılıç(2021)의 최적화 모델보다 예산은 240만 원, 대책은 2개 더 많이 사용했지만, 정보보호 위협을 2개 더 대처했고, 위험 크기를 3.69% 더 감소시켰다. 각 정보보호 위협에 대한 위험 크기 감소량은 <그림 1>과 같다.

Sönmez and Kılıç(2021)의 최적화 모델은 조작 미숙, 조작 실수, 내부 직원, 협력업체, 사회공학 공격, 내부정보수집, 위장, 데이터 유출, 시스템 결함, 악성코드를 대처했으며, 개선 모델은 비인가 접근, 위·변조를 추가로 더 대처했고, 내부정보 수집수집과 데이터 유출은 개선 모델이 위험 크기를 더 감소시켰다. 가용 예산 1억 원 수준에서의 실험 결과는 <표 9>와 같다.

개선 모델이 Sönmez and Kılıç(2021)의 최적화 모델보다 예산은 400만 원, 대책은 2개 더 적게 사용했지만, 같은 정보보호 위협의 수에 대해 2.38% 더 위험 크기를 감소시켰다. 각 정보보호 위협에 대한 위험 크기 감소량은 <그림 2>와 같다.

〈표 8〉 가용 예산 5천만으로 감소된 전체 위험 크기 최대화

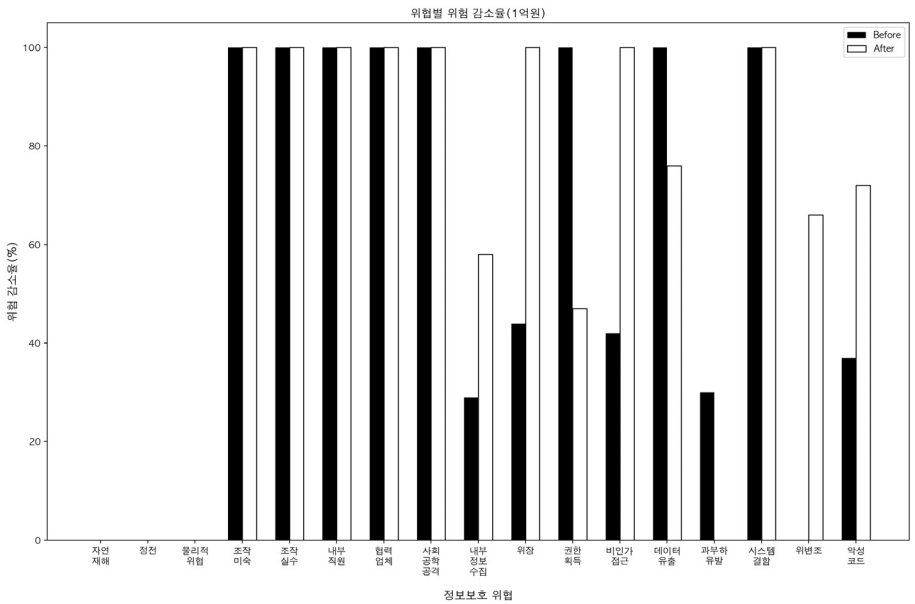
	Sönmez and Kılıç(2021)의 최적화 모델	본 연구에서 제안한 최적화 모델
사용 예산	4,720만 원	4,940만 원
대처한 위협 수	10개	12개
총 위험 크기 대비 제거된 위험 비율	74.6%	78.29%
사용된 대책의 수	13개	15개



〈그림 1〉 위협 별 감소된 위험 크기(가용예산 5천만 원)

〈표 9〉 가용 예산 1억 원으로 감소된 전체 위험 크기 최대화

	Sönmez and Kılıç(2021)의 최적화 모델	본 연구에서 제안한 최적화 모델
사용 예산	9,890만 원	9,490만 원
대처한 위협 수	13개	13개
총 위험 크기 대비 제거된 위험 비율	82.67%	85.05%
사용된 대책의 수	19개	17개



〈그림 2〉 위협 별 감소된 위험 크기(가용예산 1억 원)

두 가지 모델은 같은 개수의 위협에 대해 대처했지만, 내부정보수집, 위장, 비인가 접근, 악성코드에 대해서 개선 모델이 더 좋은 효과를 보여줬고, 과부하 유발에 대해선 개선모델이 대처하지 못했지만 위・변조에서 더 많은 위험 크기를 감소시켰다.

4.3.2 목표하는 전체 위험 감소량에 소요되는 예산 최소화

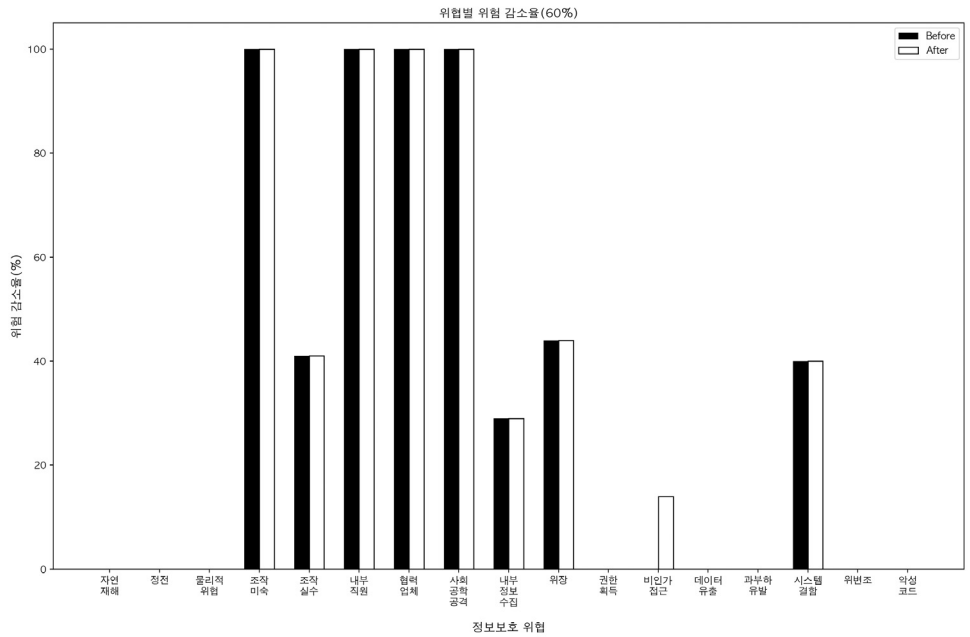
측정된 위협의 전체 위험 크기 중 60% 감소시키기 위해 소요되는 예산 최소화 결과는 <표 10>과 같다. 개선 모델이 650만 원 더 적은 금액으로 같은 정보보호 대책의 수를 사용해, 위협을 1개 더 대처했고, 위험 크기를 0.5% 더 감소시켰다. 각 정보보호 위협에 대한 위험 크기 감소량은 <그림 3>과 같다.

두 최적화 모델 모두 조작 미숙, 조작 실수, 내부 직원, 협력 업체, 사회공학 공격, 내부정보수집, 위장, 시스템 결함을 같은 위험 크기에 대해 감소시켰으나, 개선 모델은 비인가 접근에 대해 추가로 더 위험 크기를 감소시켰다. 90% 위험 감소에 소요되는 예산 최소화 결과는 <표 11>과 같다. 개선 모델이 위협 수를 1개 덜 대처했지만, 5,350만 원 더 적은 비용으로 같은 정보보호 대책을 사용했고, 위험 크기를 0.46% 더 감소시켰다. 각 위협에 대한 위험 크기는 <그림 4>와 같다. 개선모델이

물리적 위협을 대처하지 못했고, 악성코드의 위험 크기를 더 적게 감소시켰지만, 내부정보수집, 위장, 비인가 접근에 대해 더 많은 위험 크기를 감소시켰다.

〈표 10〉 전체 위험 크기 60% 감소에 소요되는 예산 최소화

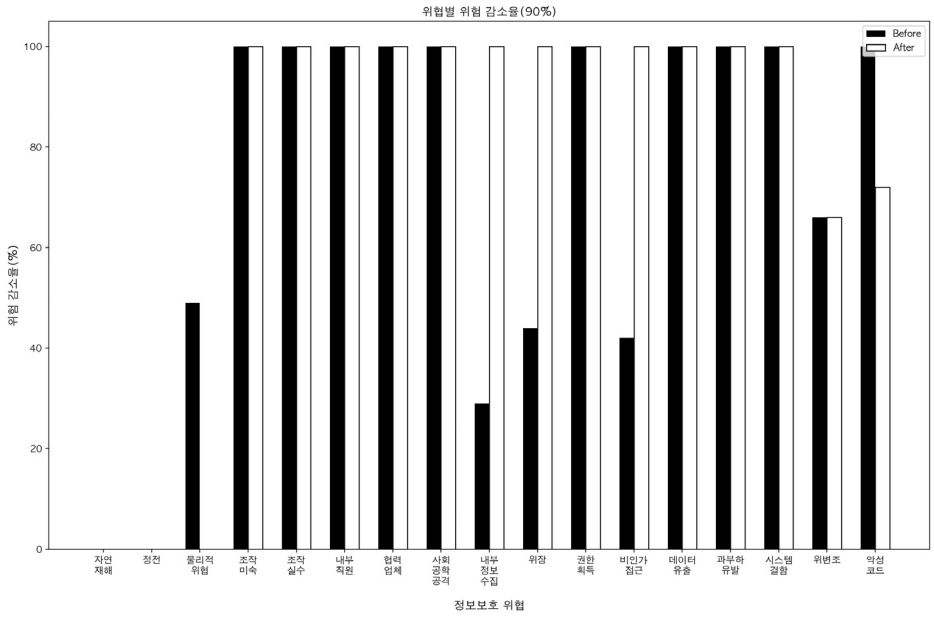
	Sönmez and Kılıç(2021)의 최적화 모델	본 연구에서 제안한 최적화 모델
사용 예산	2,020만 원	1,370만 원
대처한 위협 수	8개	9개
총 위험 크기 대비 제거된 위험 비율	61.61%	62.11%
사용된 대책의 수	10개	10개



〈그림 3〉 위협 별 감소된 위험 크기(목표 전체 위험 감소량 60%)

〈표 11〉 전체 위험 크기 90% 감소에 소요되는 예산 최소화

	Sönmez and Kılıç(2021)의 최적화 모델	본 연구에서 제안한 최적화 모델
사용 예산	20,090만 원	14,740만 원
대처한 위협 수	15개	14개
총 위험 크기 대비 제거된 위험 비율	90.1%	90.56%
사용된 대책의 수	10개	10개

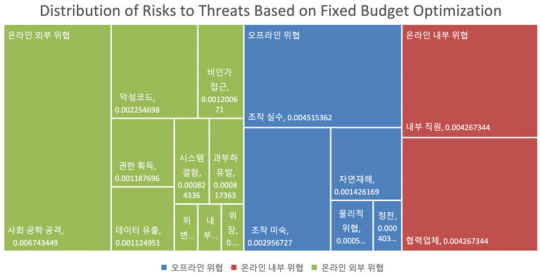


〈그림 4〉 위협 별 감소된 위험 크기(목표 전체 위험 감소량 90%)

4.4 시각화

각 목적에 맞게 최적화 결과를 도출하면 결과를 바탕으로 트리맵을 이용한 시각화를 한다. 트리맵 시각화는 전체 시각화 공간을 빈 공간 없이 사용하여 상대적으로 작은 공간에 많은 수의 계층적 노드를 표시할 수 있는 시각화 기법으로 직사각형 모양으로 구성되고 테두리 색상과 레이블은 내포된 요소를 보다 이해하기 쉬운 시각적 보기에 사용된다. 본 연구에서는 위협에 대한 위험 크기와 최적화 목표 결과를 위협 별 감소된 위험 크기, 위협 별 비용 분배, 대책 별 감소된 위험 크기, 대책 별, 비용 분배에 대해 시각화할 수 있고, 본 연구에서는 위협의 위험 크기와 가용 예산 1억 원에 대한 개선 모델의 결과를 <그림 5>, <그림 6>, <그림 7>, <그림 8>, <그림 9>와 같이 시각화했다.

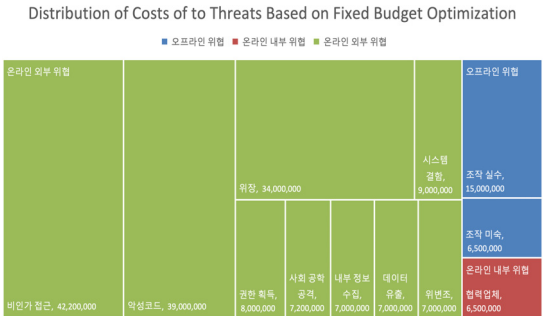
<그림 5>는 위협의 위험 크기를 시각화한 것으로 온라인 외부 위협, 오프라인 위협, 온라인 내부 위협 순으로 위협 그룹이 크다는 것을 볼 수 있고, 각 그룹 내 위협 중 사회공학 공격, 조작 실수, 내부 직원이 위험 크기가 가장 큰 것을 볼 수 있다.



〈그림 5〉 위협의 위험 크기

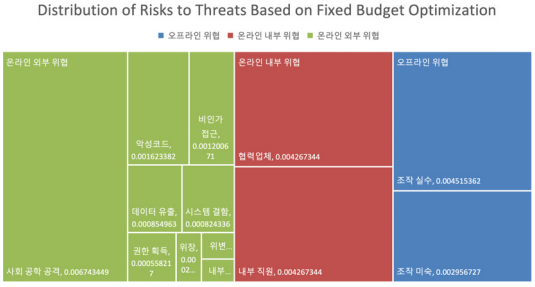
<그림 6>은 가용예산 1억 원에 대한 최적화 결과 중 위협 별 비용 분배를 시각화한 것으로 온라인 외부 위협, 오프라인 위협, 온라인 내부 위협 순으로 예산을 많이 사용한 것을 볼 수 있다. 온라인 외부 위협 내에서 비인가 접근, 악성코드, 위장 순으로 비용을 지출했고, 오프라인 위협은 조작

실수, 조작 미숙 순으로, 온라인 내부 위협은 협력업체, 내부 직원 순으로 비용을 지출한 것을 볼 수 있다.



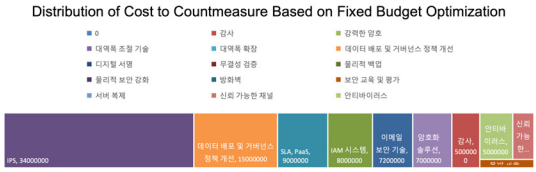
〈그림 6〉 위협 별 비용 분배(1억 원)

<그림 7>은 가용예산 1억 원에 대한 최적화 결과 중 위협 별 감소된 위험 크기를 시각화한 것으로 온라인 외부 위협, 온라인 내부 위협, 오프라인 위협 순으로 위험 감소량이 큰 것을 볼 수 있다. 온라인 외부 위협은 사회공학 공격, 악성 코드, 데이터 유출, 시스템 결함 순으로 위험 감소량이 많았고, 온라인 내부 위협은 협력업체, 내부 직원 순으로 위험 감소량이 많았으며, 오프라인 위협은 조작 실수, 조작 미숙 순으로 위험 감소량이 많은 것을 보여준다.



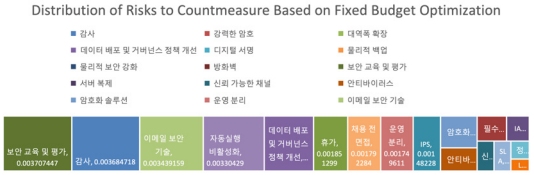
〈그림 7〉 위협 별 감소된 위험 크기(1억 원)

<그림 8>은 가용예산 1억 원에 대한 최적화 결과 중 대책 별 비용 분배에 대한 시각화로 IPS, 데이터 배포 및 거버넌스 정책 개선, IAM 시스템, 이메일 보안 기술 순으로 비용을 많이 사용한 것으로 보여준다.



〈그림 8〉 대책 별 비용 분배(1억 원)

<그림 9>는 가용예산 1억 원에 대한 최적화 결과 중 대책 별 감소된 위험 크기에 대해 시각화한 것으로 보안 교육 및 평가, 감사, 이메일 보안 기술, 자동실행 비활성화 순으로 위험 크기를 많이 감소시킨 것을 보여준다.



〈그림 9〉 대책 별 감소된 위험 크기(1억 원)

Ⅴ. 결 론

본 논문은 정보보호 투자관리 의사결정을 위해 Sönmez and Kılıç(2021)의 최적화 모델의 한계점을 개선하여, 기업에서 발생할 수 있는 위협을 전문가 대상 보안 위험 평가를 진행했고, 실제 정보보호 대책 데이터를 일부 가지고 실험하였고, 두 가지 최적화 목표에 대해 Sönmez and Kılıç(2021)의 최적화 모델보다 좋은 성능의 결과를 보여주었다. 대부분의 정보보호 위협에 대해 Sönmez and Kılıç (2021)의 최적화 모델과 개선 모델이 같은 효과를 보여줬지만 일부 위협에 대해서는 개선 모델이 감소시킨 위험 크기가 많았다는 것을 볼 수 있다. 또한 정보보호 대책의 중복 사용에 대해 고려하여 목표 위험 감소량에 대해 좀 더 적은 비용으로 정보보호 대책을 선택한 것을 보여준다.

본 연구는 베타 확률 분포를 사용하여 정보보호 대책의 객관적 측정을 하였고, 다양한 정보보호 대책의 효과성을 정량적으로 측정할 수 있게 도움을 주었다. 기존 연구에서는 정보보호 효과성 측정을 위해 연구자가 정보보호 전문가이거나, 정보보호 전문가 자문을 통한 주관적인 측정을 하는 방식 위주였고, 이는 정보보호 지식이 부족하거나, 정보보호 전문가 자문이 어려운 경우에는 측정하기 어렵고, 주관적인 측정방식은 상황에 따라 달라지기 때문에 객관적으로 사용하기 어렵다. 본 연구에서 제시하는 정보보호 효과성 측정 방법을 사용하면 정보보호 효과성 측정을 할 수 없거나, 객관적인 측정이 필요한 경우 사용하는데 도움을 줄 수 있다. 본 연구에서 개선한 최적화 모델은 Sönmez and Kılıç(2021)의 최적화 모델에서 투자로 감소된 위험이 투자 이전에 측정한 위험 수준을 초과하는 비현실적인 문제를 개선해 위험 감소가 측정한 위험 수준을 초과하지 않는 현실적인 환경으로 개선했고, 단일 정보보호 대책의 중복 투자 문제점을 고려하여 가용 예산내에 다양한 정보보호 대책을 사용해 효율적인 정보보호 투자가 될 수 있게 하였다.

본 연구는 정보보호 투자관리 지원을 위한 다양한 도움을 줄 수 있다. 보안 위험 평가를 통해 기업에서 발생할 수 있는 정보보호 위협 중 가장 위험한 정보보호 위협이 무엇이고 다른 정보보호 위협에 비해 상대적으로 얼마나 큰지 확인하고 대처할 수 있게 도움을 줄 수 있다. 정보보호 대책 효과성에 대한 기대치를 통해 거버넌스 수립, 정보보안 교육과 같은 효과성 측정이 어려운 정보보안 제품 및 서비스가 얼마나 효과가 있는지 예측하는데 도움을 줄 수 있다. 정해진 예산에 대한 최적화 계산을 통해 예산내에 어떤 제품을 구매하는 것이 좋은 지 확인할 수 있으며, 위험 감소량에 대한 최적화 계산을 통해 우선적으로 구매해야 하는 대책이 무엇인지 확인할 수 있게 도움을 줄 수 있다. 또한 트리맵 시각화를 통해 직관적으로 어떤 정보보호 위협이 위험하고, 어떤 정보보호 대책이 효과가 좋으며, 어떤 정보보호 대책을 우선 구매하는 것이 좋은지 도움을 줄 수 있다. 정보보호 담당자는 경영진에게 정보보호 예산 확대를 위한 요구 시 트리맵을 통한 시각화 결과를 사용하여 타당성 확보를 위한 도구로 활용할 수 있고, CEO/CFO는 정보보호 예산 편성 및 정보보호 부서의 예산요구 검토 시 지원해주는 도구로 사용가능 할 것이다. 또한 단독으로 소프트웨어를 만들어 사용할 수 있으나 기존 GRC(Governance, Risk and Compliance) 솔루션의 일부로 사용하여 도움을 줄 수 있다고 본다.

본 연구 모델은 하나의 정보보호 위협에 대해 다양한 정보보호 대책을 사용하게 될 때 정보보호 대책 간의 상호작용을 고려하지 않는다는 한계점이 있다. 추후에 개선된 연구 모델로 다양한 산업군에서 사용할 수 있게 소프트웨어를 만들게 되면 정보보안 투자에 어려움을 겪는 많은 기업들에게 도움을 줄 수 있을 것으로 기대한다.

참 고 문 헌

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

[2] 국가종합 전자조달청, “나라장터 종합 쇼핑몰, 2023, 1, 20, Available at https:www.g2b.go.kr:8092/sm/ma/mn/SMMAMnF.do.

[3] 이경율, 이선영, 임강빈, “기반시설 보안위협 분류 및 분석”, *한국통신학회논문지*, 제43권, 제3호, 2018, pp. 572-579.

[4] 이상훈, 김태성, “정보보호 대책의 성능을 고려한 투자 포트폴리오의 게임 이론적 최적화”, *지능정보연구*, 제26권, 제3호, 2020, pp. 37-50.

[5] 임정현, 김태성, “침해사고 통계 기반 정보보호 투자 포트폴리오 최적화 : 유전자 알고리즘 접근법”, *Information Systems Review*, 제22권, 제2호, 2020, pp. 201-217.

[6] 한국인터넷진흥원, “정보보호 공시 현황”, 2022, 12, 1, Available at https://isds.kisa.or.kr/kr/publish/list.do?menuNo=204942.

[7] 허진, 이애리, “스마트팩토리의 주요 보안요인 연구: AHP를 활용한 우선순위 분석을 중심으로”, *Information Systems Review*, 제22권, 제4호, 2020, pp. 185-203.

[8] Armenia, S., M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer, “A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs”, *Decision Support Systems*, Vol.147, 2021, p. 113580.

[9] 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, pp. 78-83.

[10] Bodin, L. D., L. A. Gordon, and M. P. Loeb, “Information security and risk management”, *Communications of the ACM*, Vol.51, No.4, 2008, pp. 64-68.

[11] Cavusoglu, H., S. Raghunathan, and W. T. Yue, “Decision-theoretic and game-theoretic approaches to IT security investment”, *Journal of Management Information Systems*, Vol.25, No.2, 2008, pp. 281-304.

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

[13] Gartner, “Gartner Identifies Three Factors Influencing Growth in Security Spending”, 2022, 10, 13, Available at https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i.

[14] Gordon, L. A. and M. P. Loeb, “The economics of information security investment”, *ACM Transactions on Information and System Security*, Vol.5, No.4, pp. 438-457, 2002.

[15] Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou, “Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model”, *Journal of Information Security*, Vol.6, No.1, 2014, pp. 24-30.

[16] 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, pp. 592-603.

[17] Heidt, M., J. P. Gerlach, and P. Buxmann, “Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments”, *Information Systems Frontiers*, Vol. 21, 2019, pp. 1285-1305.

[18] IBM Security, “Cost of a Data Breach Report 2022”, 2022. 11. 7., Available at https://www.ibm.com/security/data-breach.

[19] Kaspersky, “SMBs and Enterprise plan to increase IT security budgets equally up to 14% in the next three years”, 2023. 2. 8., Available at https://www.kaspersky.com/about/press-releases/2023_smbs-and-enterprise-plan-to-increase-it-security-budgets-equally-up-to-14-in-the-next-three-years.

[20] Kumar, R. L., S. Park, and C. Subramaniam, “Understanding the value of countermeasure portfolios in information systems security”, *Journal of Management Information Systems*, Vol.25, No.2, 2008, pp. 241-280.

[21] Miaoui, Y. and N. Boudriga, “Enterprise security investment through time when facing different types of vulnerabilities”, *Information Systems Frontiers*, Vol.21, 2019, pp. 261-300.

[22] NSS Labs., “NSS Labs Announces 2019 Next Generation Intrusion Prevention Systems (NGIPS)

Group Test Results", PR Newswire, 2019.

[23] Ponemon Institute, "Closing the IT Security Gaps 2020 Global Study by the Ponemon Institute", HPE Inc., 2020.

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

[25] Skybakmoen, T., "Next Generation Firewall Comparative Analysis", Media Zones, 2022.

[26] Sönmez, F. Ö. and B. G. Kılıç, "A decision support system for optimal selection of enterprise information security preventative actions", *IEEE Transactions on Network and Service Management*, Vol.18, No.3, 2020, pp. 3260-3279.

[27] Von Solms, R., "Information security management: The second generation", *Computers and Security*, Vol.15, No.4, 1996, pp. 281-288.

[28] Whitman, M. E. and H. J. Mattord, "Threats to information protection-industry and academic perspectives: An annotated bibliography", *Journal of Cybersecurity Education, Research and Practice*, Vol.2016, No.2, Article 4.

Information Systems Review
Volume 25 Number 4
November 2023

A Model for Supporting Information Security Investment Decision-Making Considering the Efficacy of Countermeasures

Byeongjo Park* · Tae-Sung Kim**

Abstract

The importance of information security has grown alongside the development of information and communication technology. However, companies struggle to select suitable countermeasures within their limited budgets. Sönmez and Kılıç (2021) proposed a model using AHP and mixed integer programming to determine the optimal investment combination for mitigating information security breaches. However, their model had limitations: 1) a lack of objective measurement for countermeasure efficacy against security threats, 2) unrealistic scenarios where risk reduction surpassed pre-investment levels, and 3) cost duplication when using a single countermeasure for multiple threats. This paper enhances the model by objectively quantifying countermeasure efficacy using the beta probability distribution. It also resolves unrealistic scenarios and the issue of duplicating investments for a single countermeasure. An empirical analysis was conducted on domestic SMEs to determine investment budgets and risk levels. The improved model outperformed Sönmez and Kılıç's (2021) optimization model. By employing the proposed effectiveness measurement approach, difficulty to evaluate countermeasures can be quantified. Utilizing the improved optimization model allows for deriving an optimal investment portfolio for each countermeasure within a fixed budget, considering information security costs, quantities, and effectiveness. This aids in securing the information security budget and effectively addressing information security threats.

Keywords: ***Information Security Investment, Countermeasure Efficacy, AHP, MIP, Decision Support System, Visualization***

* Ph.D. Student, Department of Convergence Security, Chungbuk National University
** Corresponding Author, Professor, Department of MIS; Director, Cybersecurity Economics Research Institute, Chungbuk National University

◐ 저 자 소 개 ◑

박 병 조 (byeongjo06@cbnu.ac.kr)

충북대학교 융합보안학과에서 석사학위를 취득하고, 현재 동대학원 박사과정에 재학 중이다. 주요 관심 분야는 정보통신과 정보보호 분야의 의사결정 및 투자 최적화이다.

김 태 성 (kimts@cbnu.ac.kr)

KAIST 산업경영학과에서 박사를 취득하고, 한국전자통신연구원에서 선임연구원으로 근무한 후, 현재 충북대학교 경영정보학과에서 정교수, 보안경제연구소장, 보안컨설팅연계전공 및 대학원 융합보안전공 주임교수로 재직하고 있다. 국가정보원 보안관리실태평가 자문 및 평가위원, 행정안전부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, 병무청 정책자문위원, 한국전력 정보보안 자문위원, 한국지역정보개발원 선임이사, ISMS-P 인증위원회 위원, 정보보호산업 분쟁조정위원회 위원, 금융감독원 데이터분야 외부평가위원으로 활동하고 있으며, 주요 관심분야는 정보통신과 정보보호 분야의 경영 및 정책 의사결정이다.

논문접수일 : 2023년 06월 01일 **게재확정일 : 2023년 07월 25일**
1차 수정일 : 2023년 07월 12일