확률모형을 이용한 정보보호 투자 포트폴리오 분석

양원석* · 김태성**† · 박현민***

Probabilistic Modeling for Evaluation of Information Security Investment Portfolios

Won-Seok Yang* · Tae-Sung Kim** · Hyun-Min Park***

■ Abstract ■

We develop a probability model to evaluate information security investment portfolios. We assume that organizations install portfolios of information security countermeasures to mitigate the damage such as loss of the transaction being processed, damage of hardware and data, etc. A queueing model and its expected value analysis are used to derive the lost cost of transactions being processed, the replacement cost of hardwares, and the recovery cost of data. The net present value for each portfolio is derived and organizations can select the optimal information security investment portfolio by comparing portfolios.

Keyword : Security Threats, Information Security, Investment Portfolio, Economic Analysis, Probability Model

1. 서 론

최근 급속도로 진행되고 있는 정보화에 비례하여, 해킹, 바이러스 등의 정보보호 침해(IT security breach)가 급격히 증가하고 있다. 정보보호 침해를 방지하고 그 피해를 최소화하기 위해서 기업이나 정부는 다양

논문접수일 : 2009년 02월 19일 논문게재확정일 : 2009년 08월 31일
논문수정일(1차 : 2009년 06월 18일)
* 한국전자통신연구원 기술전략본부 서비스정책연구부
** 충북대학교 경영정보학과/BK21사업팀
*** 부경대학교 시스템경영공학과
† 교신저자

한 형태의 수단을 준비하고 추진 중이다[2, 7].

많은 기업이나 정부에서 정보보호의 중요성을 인식하고 정보보호에 대한 투자에 관심을 두고 있지만, 최근 Computer Security Institute와 FBI가 공동으로 수행한 조사결과에 의하면 조사에 응답한 기관 중 56%가 정보보호 침해를 경험했고, 응답기관이 정보보호침해로 겪은 평균 손실이 20만 달러에 달한다는 것으로 밝혀졌다[7]. 이 조사결과에서 볼 수 있듯이, 정보보호에 대한 많은 관심에도 불구하고 정보보호에 대한 적절한 투자가 이루어지지 않고 있다. 정보보호에 대한 투자를 무조건적으로 증가시켜야 한다는 초기 접근방식은 오히려 정보보호에 대한 투자를 저해하는 요인으로 작용을 해왔으므로, 적정한 투자규모에 대한 탐색과 정보보호투자에 대한 경제적인 효과를 측정하여 합리적인 정보보호투자를 유도해야 할 필요가 있다.

정보보호 투자의 경제적인 측면에 대한 본격적인 연구는 최근에 들어서야 발표되기 시작했다(최근 연구동향에 대해서는 공희경과 김태성[1] 참조). 기존의 정보보호 투자 및 시스템의 경제성에 대한 대표적인 연구는 크게 회계 및 재무적인 접근 방법과 게임이론을 통한 접근 방법으로 구분된다.

Gordon and Loeb[8], Campbell et al.[4], Bodin et al.[3]은 회계학과 재무관리 기법을 이용하여 정보보호투자의 가치에 대한 다양한 연구를 수행하였다. Gordon and Loeb[8]은 중간정도의 취약성을 지닌 정보자산에 대한 투자가 가장 효과적인 것을 증명하였다. 하지만 정보보호 투자 총액의 다소 정도에만 관심을 두고, 구체적인 정보보호 투자대안에 대해서는 해결책을 제시하지 못하였다. Campbell et al.[4]은 대중에게 공개된 정보보호 침해가 기업에 미치는 경제적 손실을 주가 변동을 이용하여 측정하였다. 하지만, 공개되지 않은 정보보호 침해가 미치는 경제적 손실이나 정보보호 침해가 국가 전체에 미치는 영향에 대해서는 해결책을 제시하지 못하였다. Bodin et al.[3]은 다기준(multi-criteria) 의사결정방법론인 AHP (Analytic Hierarchy Process)를 이용하여 복수의 정보보호투자제안서를 비교하는 방법을 제시하였다. 복수개의 투자제안에 대한 비교에는 유용하게 쓰일 수 있지만, 투자대안의 비교방법이 전문가의 주관적 견해에 의존하였고 개별 정보보호 투자제안서에 대한 객관적인 성능측도를 개발하지 못한 한계가 있다.

Cavusoglu et al.[5], Cavusogulu et al.[6]는 게임이론을 주로 이용하여 정보보호 투자 의사결정에 사용할 수 있는 분석모형과 개별 정보보호기술(침입탐지 시스템)의 경제적 가치에 대한 연구를 수행하였다. Cavusoglu et al.[6]은 침입탐지 시스템의 경제적 가치를 게임이론을 이용하여 도출하였다. 하지만, 침입탐지 시스템을 제외한 여타 정보보호 기술대안의 경제적 가치를 산출하기 위해 적용할 수 있는 일반적인 모델이 아니라는 한계가 있고, 다양한 정보보호 기술대안을 복합적으로 사용하여 정보보호 시스템을 구현하는 현실을 고려해보면, 전체적인 정보보호 시스템 투자믹스(mix)인 정보보호 투자 포트폴리오를 어떻게 구성해야 하는지에 대해서도 해결책을 제시하지 못하였다. Cavusoglu et al.[5]는 경제적 효과가 가장 큰 정보보호 기술대안을 선택하기 위한 의사결정모형을 제시하였다. 하지만, 대부분 조직에서 단일 정보보호 기술대안에 의존하기 보다는 복수개의 정보보호 기술대안을 선택하는 현재 상황을 고려할 때, 다양한 기술대안이 복합적으로 어울려 최적의 효과를 내기 위한 포트폴리오 결정에는 활용되기 어렵기 때문에 실무적으로 적용하기에는 한계가 있는 연구이다.

결과적으로 기존 정보보호의 경제적인 측면에 대한 대표적인 연구들은 주로 기업대상으로 개별 정보보호 기술대안의 경제적 가치를 측정하거나, 정보보호 투자 의사결정 절차를 제시하거나, 정보보호침해의 경제적 손실을 측정하는 방법에 대해 이루어졌다. 반면, 객관적인 측도를 이용하여 기업의 정보보호 투자 포트폴리오를 평가하거나, 다양한 정보보호 대안들을 이용한 경제적으로 최적인 투자에 대한 연구는 부족한 현실이다.

본 논문에서는 대기행렬 모형을 이용하여, 위협에 의해 작업 유실이 발생하는 실시간 정보시스템

의 보안 포트폴리오의 경제성 분석모형을 제시하고, 도출된 특성값을 이용하여 대상 조직에 적합한 보안 포트폴리오를 선정하는 수치 예를 보인다. 본 논문에서 다루는 모형은 구체적으로 다음과 같다. 최근 정보통신 기술의 발달로 은행거래, 재고처리, 웹 쇼핑 등 대부분 거래와 온라인 작업이 실시간으로 처리된다. 이를 위해 거래의 세부 단위인 트랜잭션과 트랜잭션을 전송하는 패킷이 정보통신망에서 실시간으로 전송된다. 본 논문에서는 이와 같이 실시간으로 데이터를 처리하는 정보시스템을 다룬다. 정보시스템에서는 트랜잭션 작업의 발생, 대기, 처리가 발생하므로 입력과 출력이 존재하는 대기행렬모형과 같다. 정보시스템에서 트랜잭션과 같은 작업의 발생 및 처리는 대기행렬모형의 고객 및 서비스와 동일하다. 최근 대기행렬모형에서는 바이러스와 같은 위협(threat)에 의해 작업이 유실되는 상황을 Negative Customer(NC)와 Disaster(DST)로 모형화한다[10, 11, 13-15]. 일반적으로 시스템에 NC가 발생하면 대기 및 처리중인 작업 1개가 유실되고 DST의 경우에는 전체 작업이 유실된다. 한편, 바이러스나 해킹 등의 시스템에 대한 보안 위협들은 1개 이상의 작업을 파기시킬 수 있다. 따라서 본 논문에서는 기존 연구와 달리 시스템에 발생한 위협에 의해 유실되는 작업 수가 일정한 확률분포를 따르는 것으로 가정한다.

본 논문에서 위협에 의해 정보보안 침해사고의 물리적 피해(하드웨어 고장 및 작업 유실)만이 발생한다고 가정한다. 따라서 보안 포트폴리오 구성에 따른 보안시스템 구축 투자비, 유실된 작업 복구비용인 유실비용, 하드웨어 고장에 따른 대체비용을 고려한다. 유실비용은 유실된 작업 수에 비례한다. 대체비용은 위협이 발생하면 확률적으로 발생한다고 가정한다. 보안 포트폴리오 구성이 우수할수록 보안시스템 구축비용이 증가하나 위협 발생률은 감소한다고 가정한다. 본 논문에서는 먼저 위협률에 따른 유실비용과 수리비용을 유도한다. 보안 포트폴리오 구성에 따른 보안시스템 구축, 유실, 대체 비용의 변화를 통해 경제성 분석 방법을 제안한다. 고정비인 보안시스템 구축투자비와 변동비인 유실비용과 대체비용을 현재가치로 환산하여 보안 포트폴리오의 손익을 제시한다.

이후 논문 구성은 다음과 같다. 제 2장에서는 시스템 성능치를 유도하고 포트폴리오의 경제성을 분석한다. 제 2.1절에서는 수리모형을 제시한다. 제 2.2절에서는 임의시점 시스템 상태(작업 수) 확률을 유도한다. 제 2.3절에서는 포트폴리오 구축에 따른 비용절감 효과를 이용하여 포트폴리오의 경제성을 평가한다. 제 3장에서는 수치 예제를 제시한다. 제 4장에서는 연구의 결론 및 추후 연구 주제에 대해 정리한다.

2. 모형 및 경제성 분석

2.1 모형

본 논문에서는 정보시스템을 M/M/1 모형으로 간주한다. 정보통신 네트워크상에서 불특정 다수의 정보서비스 이용자들의 작업요구 발생은 포아송과정을 따른다고 가정하는 것이 자연스럽다. 다양한 정보시스템의 특성을 반영하기 위해서는 작업 처리시간이 일반분포를 따른다고 가정하는 것이 가장 적합할 것이나, 분석의 용이성을 위해 지수분포를 가정하고 추후 연구에서 일반분포로 확장할 수 있을 것이다. 정보시스템에서 처리해야 할 작업은 발생률이 λ인 포아송 과정에 따라 발생하고 작업 처리시간은 서비스율이 μ인 지수분포를 따른다고 가정한다.

보안 대책의 조합에 따라 J개의 보안 포트폴리오가 가능하다. 포트폴리오 j에서 발생률이 η_j인 포아송 과정에 따라 위협이 발생하고, d_k의 확률로 k개의 작업이 유실된다. 시스템에 k개 이하의 작업이 있는 경우에는 시스템내의 모든 작업이 유실된다. 아울러, α의 확률로 시스템의 하드웨어에 손상을 입히고 하드웨어에 저장된 작업 자료의 β 비율만큼 손상된다. 유실 작업, 손상 자료 및 손상 하드웨어는 순간적으로 복구 및 대체된다고 가정한다.

시스템의 시작점에서는 하드웨어에 저장된 자료는 없다고 가정한다. 처리 및 대기 중인 작업의 유실비용은 건당 c_L, 하드웨어 대체비용은 대체 건당 c_W, 그리고 손상된 자료의 복구비용은 건당 c_D이다. 포트폴리오 j에서 포트폴리오 구축 투자비를 c_j라 표기한다.

포트폴리오 j가 클수록 보안체계가 우수하다고 가정한다. 따라서 j가 증가할수록 포트폴리오 구축 투자비는 증가하나 위협 발생률이 감소한다. 즉, $i>j$에 대해 $c_i>c_j$이고 $\eta_i<\eta_j$이다. 본 논문에서는 단위 회계기간을 τ, 단위 회계기간 동안의 이자율을 θ로 표기한다.

보안시스템을 구축하면, 작업 유실, 하드웨어 대체, 저장 자료 복구 횟수 감소에 따른 비용 절감 효과가 발생한다. 즉, 보안 포트폴리오를 우수하게 구성할수록 시스템 구축 투자비는 증가하나, 비용 감소에 따른 경제적인 이득을 얻는다. 따라서 포트폴리오 투자 대비 비용절감 효과를 분석하여 포트폴리오의 경제적인 효과를 평가할 수 있다.

본 논문에서 쓰이는 기호를 정리하면 다음과 같다.

- λ : 작업 발생률
- μ : 작업 처리시간 비율(서비스율)
- J : 포트폴리오 개수
- η_j : 포트폴리오 j에서 위협 발생률
- d_k : 위협 발생 시, k개의 작업이 유실될 확률
- α : 위협 발생 시, 시스템의 하드웨어가 손상될 확률
- β : 위협 발생 시, 하드웨어에 저장된 작업 자료의 손상 비율
- c_L : 작업 유실 건당 작업 유실비용
- c_W : 하드웨어 손상 건당 하드웨어 대체비용
- c_D : 자료 손상 건당 자료 복구비용
- c_j : 포트폴리오 j구축 투자비
- τ : 단위 회계기간(예, 1년)
- θ : 단위 회계기간 동안의 이자율
- p_n : 임의 시점에서 시스템에서 처리 및 대기 중인 작업의 수가 n일 확률
- L_j : 단위 회계기간 τ동안 포트폴리오 0(보안 시스템이 없는 경우) 대비 포트폴리오 j의 작업 유실비용의 감소분
- W_j : 단위 회계기간 τ동안 포트폴리오 0대비 포트폴리오 j의 하드웨어 대체비용의 감소분
- $R_j(y)$: y회계연도말까지 포트폴리오 0대비 포트폴리오 j의 자료 복구비용의 감소분
- $C(y,\theta)$: 이자율이 θ인 경우, y 회계연도까지 손익의 현재가치

2.2 시스템 성능 분석

임의 시점에서 시스템에서 처리 및 대기 중인 작업 수의 확률을 p_n으로 표기한다. 위협발생률을 η라 하자. 작업 수에 따른 균형방정식(balance equation)은 아래와 같다.

$$\lambda p_0 = \mu p_1 + \eta[p_1(d_1+d_2+\cdots)+p_2(d_2+d_3+\cdots)+p_3(d_3+d_4+\cdots)+\cdots]$$

$$\lambda p_k + \mu p_k + \eta p_k = \lambda p_{k-1} + \mu p_{k+1} + \eta(p_{k+1}d_1 + p_{k+2}d_2 + p_{k+3}d_3\cdots),\ k=1,2,\cdots.$$

p_n을 아래와 같이 가정한다.

$$p_n = p_0\rho^n,\ n=0,\ 1,\ 2,\ \cdots. \tag{1}$$

$D(z)$를 아래와 같이 정의한다.

$$D(z)=\sum_{n=1}^{\infty} d_n z^n.$$

식 (1)을 균형방정식에 대입하면, 아래와 같이 ρ에 대한 방정식을 얻는다.

$$\lambda = \rho\left\{\mu + \frac{\eta[1-D(\rho)]}{1-\rho}\right\}. \tag{2}$$

식 (1)과 균일화(normalization) 조건을 이용하면, 임의시점의 작업 수 분포를 얻는다.

$$p_n = (1-\rho)\rho^n, \quad n = 0, 1, 2, \cdots. \tag{3}$$

- 비고 1 : 위협이 없는 경우 $\eta = 0$, $D(z) = 0$이다. 식 (2)에서 $\rho = \lambda/\mu$이므로 M/M/1 대기행렬 모형의 결과를 얻는다[14].

위협에 의해 1개 또는 M개의 작업이 유실된다고 하자. 각 위협의 발생률을 ϵ과 δ라 하면, $D(z)$는 아래와 같다.

$$D(z) = d_1 z + d_M z^M. \tag{4}$$

여기에서 $\eta = \epsilon + \delta$, $d_1 = \epsilon/(\epsilon+\delta)$, $d_M = \delta/(\epsilon+\delta)$이다. 식 (2)에 식 (4)를 대입하고, $M \to \infty$라 하면, 다음을 얻는다.

$$\lambda = \rho\left[\mu + \epsilon + \frac{\delta}{1-\rho}\right]. \tag{5}$$

- 비고 2 : 식 (5)는 NC와 DST의 도착률이 ϵ과 δ인 M/M/1 대기행렬모형의 결과와 같다[14].

임의 시점에서 시스템에서 처리 및 대기 중인 작업 수를 N으로 표기한다. 식 (3)에서 다음의 평균 작업수를 얻는다.

$$E[N] = \rho/(1-\rho). \tag{6}$$

이제 포트폴리오 j에서 ρ와 N을 ρ_j와 N_j로 표기한다. 여기서 $j = 0, 1, \cdots, J$ 이다. $j = 0$은 보안 대책이 없는 경우를 의미한다. 식 (2)와 식 (6)에서, 다음을 얻는다.

$$\lambda = \rho_j\left\{\mu + \frac{\eta_j[1-D(\rho_j)]}{1-\rho_j}\right\}, \quad E[N_j] = \frac{\rho_j}{1-\rho_j}. \tag{7}$$

2.3 경제성 분석

단위 회계기간 τ동안 포트폴리오 0대비 포트폴리오 j의 작업 유실비용의 감소분을 L_j라 하자. 포트폴리오 j에서는 포트폴리오 0대비 평균 $E[N_j] - E[N_0]$개 작업 유실을 방지할 수 있으므로, L_j는 다음과 같다.

$$L_j = c_L(E[N_j] - E[N_0])\tau = c_L\left(\frac{\rho_j}{1-\rho_j} - \frac{\rho_0}{1-\rho_0}\right)\tau. \tag{8}$$

단위 회계기간 τ동안 포트폴리오 0대비 포트폴리오 j의 하드웨어 대체 비용의 감소분을 W_j라 하자. τ동안 하드웨어 대체횟수는 $\alpha\eta_j\tau$이므로 W_j는 다음과 같다.

$$W_j = c_W\alpha(\eta_0 - \eta_j)\tau. \tag{9}$$

은행거래, 재고처리, 웹 쇼핑 등의 서비스를 제공하는 정보시스템에서는 하루에도 수천 만건의 작업을 실시간으로 처리한다. 반면, 보안 위협은 한 달에 수십 건 정도가 발생한다. 따라서 위협 발생률은 작업 발생률에 비해 현저하게 낮다. 즉, 시스템의 작업 처리시간은 위협 발생 시간 간격 대비 현저하게 짧다. 아울러, 정보시스템에서는 실시간으로 작업을 처리하므로 현재 시스템에서 처리 및 대기 중인 작업 대비 저장 자료 수가 현저하게 크다. 따라서 근사적으로 k번째 위협 발생 시점까지 시스템에 발생한 작업이 모두 처리되었다고 간주할 수 있다. 첫 번째 위협 발생 시점에는 시스템에 λ/η_j개의 작업 자료가 저장되어 있다. 위협이 발생하면, 저장 자료의 $\alpha\beta$만큼 손상되므로 평균 $\alpha\beta(\lambda/\eta_j)$개의 자료를 복구해야한다. 한편, 자료 복구가 순간적으로 이루어지므로 시스템에는 기존 λ/η_j개 자료가 저장되게 된다. 두 번째 위협이 발생하면, 기 저장 자료 λ/η_j개와 첫 번째 위협에서 두 번째 위협 발생까지 신규로 저장된 λ/η_j개를 합한 $2\lambda/\eta_j$개의 자료가 저장되어 있다. 따라서 두 번째 위협 발생 시점에는 $\alpha\beta(2\lambda/\eta_j)$개의 손상자료를 복구해야한다. 결과적으로 k번째 위협이 발생한 시점까지 총 자료 복구 횟수의 기대 값은 다음과 같다.

$$\alpha\beta\left(\frac{\lambda}{\eta_j}\right)+\alpha\beta\left(\frac{2\lambda}{\eta_j}\right)+\cdots+\alpha\beta\left(\frac{k\lambda}{\eta_j}\right)=\alpha\beta\left(\frac{\lambda}{\eta_j}\right)\frac{k(k+1)}{2}.$$

X_k를 위협의 도착시간 간격을 나타내는 확률변수라 하자. 기간 x동안의 위협 발생 횟수의 확률변수를 M이라 하면 다음을 얻는다.

$$X_1+\cdots X_M<x. \tag{10}$$

식 (10)의 양변에 기대값을 취하면, $E[M]/\eta_j<x$이다. M은 식 (10)을 만족시키는 최대 정수이므로 다음을 얻는다.

$$E[M]=\lfloor x\eta_j\rfloor. \tag{11}$$

여기서 $\lfloor\ \rfloor$는 y를 넘지 않는 최대정수이다. 결국, 근사적으로 기간 x동안 복구비용의 기대 값은 다음과 같다.

$$c_D\alpha\beta\left(\frac{\lambda}{\eta_j}\right)\frac{(1+\lfloor x\eta_j\rfloor)\lfloor x\eta_j\rfloor}{2}. \tag{12}$$

y회계연도말까지 포트폴리오 0대비 포트폴리오 j의 자료 복구비용의 감소분을 $R_j(y)$로 표기한다. y회계연도말까지 기간은 $y\tau$이다. 식 (11)의 x를 $y\tau$로 치환하여 식 (12)에 대입하면, 다음과 같이 $R_j(y)$를 얻는다.

$$R_j(y)=c_D\alpha\beta\lambda \left\{\frac{(1+\lfloor y\tau\eta_0\rfloor)\lfloor y\tau\eta_0\rfloor)}{2\eta_0}-\frac{(1+\lfloor y\tau\eta_j\rfloor)\lfloor y\tau\eta_j\rfloor}{2\eta_j}\right\}. \tag{13}$$

포트폴리오 투자비 c_j는 시스템 구축 초기에만 발생하는 고정비용이다. 반면, 유실, 대체 및 복구비용은 매 회계연도마다 발생하는 변동비용이므로 현재가치로 환산시, 이자율을 고려해야한다. 한편, 식 (8), 식 (9), 식 (13)의 유실, 대체, 복구비용의 감소치는 보안시스템 구축에 따라 포트폴리오 0대비 포트폴리오 j가 얻는 이득이라 할 수 있다. 이자율이 θ인 경우, y회계연도까지 손익의 현재가치를 $C(y,\theta)$라 하자. 식 (8), 식 (9), 식 (13)에서 다음을 얻는다.

$$C(y,\theta)=-c_j+(L_j+W_j)\sum_{k=1}^{y}\frac{1}{(1+\theta)^k}+\sum_{k=1}^{y}\frac{R_j(k)}{(1+\theta)^k}. \tag{14}$$

각 기업은 투자비의 제한, 손익 분기점 등의 투자 기준에 맞춰 식 (14)를 최대화하는 경제적인 보안 포트폴리오를 선정할 수 있다.

3. 수치 예

단위 회계기간 τ는 1년, 이자율 θ는 10%라 가정한다. 작업 및 위협 발생률의 기준 단위를 시간으로 한다. 따라서 $\tau=365\times24=8{,}760$이다. 보안 포트폴리오는 5개를 구성할 수 있다고 가정한다.

기업에서 <표 1>과 같은 정보보안 관련 통계를 얻을 수 있다고 하자.

<표 1>에서 다음과 같이 시스템 파라미터를 추정할 수 있다.

$$\lambda=\text{가},\ \mu=\text{나},\ \eta_0=\text{다}/\tau,\ \alpha=\text{바}/\text{다},\ \beta=\text{마}/(\text{가}\times\tau).$$

위협 발생 시, Ω개의 작업이 유실된다고 하자. 시스템에는 다양한 종류의 위협이 발생하기 때문에 Ω의 분포를 정확히 알기 어렵다. 이러한 불확실성을 고려하여 Ω가 기하분포를 따른다고 가정한다. 이 경우 d_k와 $D(z)$는 다음과 같다.

$$d_k=P(\Omega=k)=d(1-d)^{k-1},\ k=1,2,\cdots,$$
$$D(z)=(dz)/[1-(1-d)z].$$

기하분포의 경우 $E[\Omega]=1/d$이다. 한편 <표 1>에서 $E[\Omega]=\text{라}/\text{다}$이다. 모멘트방법(Method of Mo-

〈표 1〉 정보보안 관련 통계 예

구 분	항 목	값	단 위
가	작업 발생 건수	100	건/시간
나	작업 처리 능력	105	건/시간
다	위협 발생 건수	300	건/년
라	작업 처리 중 유실 건수	400	건/년
마	저장 자료 손상 건수	1000	건/년
바	하드웨어 교체 건수	50	건/년

〈표 2〉 포트폴리오별 위협 도착률 목표치 및 투자비

포트폴리오	위협 도착률		보안시스템 투자비	
	목표치	파라미터	금액(억 원)	파라미터
P1	0.0171	η_1	140	c_1
P2	0.0114	η_2	180	c_2
P3	0.0086	η_3	220	c_3
P4	0.0068	η_4	260	c_4
P5	0.0057	η_5	300	c_5

ments)을 이용하면[12], d를 다음과 같이 추정할 수 있다.

$$d = 1/(\text{라}/\text{다}).$$

포트폴리오별 위협 도착률 목표치와 보안시스템 투자비를 <표 2>와 같이 가정한다.

아울러, $c_L = 50$, $c_D = 10$, $c_W = 1000$이라 가정한다. 단위는 건당 만원이다.

보안시스템의 교체 수명주기를 7년으로 가정하여, 식 (14)에서 각 포트폴리오의 가치(또는 투자이익)을 산출하면 <표 3>과 같다.

P1, P2, P3은 손익분기점이 3년이고, P4, P5는 4년이다. 한편, 투자기간이 2년 이하인 경우에는 포트폴리오 1의 이익이 최대이나, 3년인 경우에는 포트폴리오 2, 그리고 4년인 경우에는 포트폴리오 3, 5년인 경우에는 포트폴리오 4의 이익이 최대이다. 6년 이후인 경우에는 포트폴리오 5의 이익이 최대임을 알 수 있다.

4. 결 론

본 연구에서는 정보시스템에 피해를 입힐 수 있는 보안위협이 도착하는 상황을 가정하여, 피해를 줄이기 위해 설치되는 보안 포트폴리오의 가치를 확률모형을 이용하여 평가하였다. 도출된 모형에 대해 복수개의 포트폴리오를 평가하여 해당 정보시스템에 적합한 투자 의사결정을 내리는데 참고할 수 있도록 수치 예제도 함께 제시하였다.

정보보안 투자의 성과에 대한 객관적인 측정의 어려움 때문에 정보보안에 대한 투자가(정보보안의 중요성에 대한 인식 수준에 비해) 증가하지 않았다는 점에서 본 연구 결과는 적정 수준의 정보보안 투자의 가이드라인의 역할을 할 수 있을 것이다.

〈표 3〉 포트폴리오별 투자이익

(단위 : 억원)

구 분	1년	2년	3년	4년	5년	6년	7년
P1	-123	-77	12	153	350	608	925
P2	-158	-96	23	210	474	817	1,240
P3	-195	-125	8	220	516	902	1,379
P4	-233	-159	-16	209	525	937	1,445
P5	-272	-195	-46	188	518	947	1,476

본 논문에서는 하드웨어 대체, 데이터복구 등의 물리적 피해와 작업 유실의 일부 업무상 피해만을 고려하였는데, 이 외에 매출손상, 업무 효율의 저하, 개인정보 유출에 따른 보상비용, 기업기밀 유출에 따른 경쟁력 손실 등의 비용에 대해서는 고려하지 못하였다. 상대적으로 직접적이고 명시적인 비용에 대해서만 모형에서 고려하였고, 간접적이고 잠재적인 비용에 대해서는 고려하지 못한 것이다. 기존의 여러 연구에서도 개념적이고 추상적인 수준에서의 논의만 되고 있고, 실제 응용할 수 있는 정도의 결과는 제시하지 못하고 있다[1]. 정보보호의 경제성에 대해 적합한 모형에 대한 연구도 필요하지만, 모형에서 사용할 수 있는 데이터를 확보하는 노력도 매우 중요하다. 실제로 정보보호 관련 데이터는 조직의 기밀에 해당되는 내용이 많아서 공개가 되지 않는 경우가 많다. 정보보호 관련 데이터를 확보할 수 있는 조사 방법과 지속적인 조사의 수행이 매우 필요할 것이다.

분석 대상인 피해 비용의 범위를 확대하는 것 이외에도, 향후에 수행될 수 있는 연구주제를 정리하면 다음과 같다.

본 연구에서는 도착한 위협은 일정한 확률로 피해를 발생시킨다고 가정을 했는데, 실제로는 도착한 위협과 정보시스템의 취약성의 관계 사이에서 피해가 발생한다. 위협이 발생하더라도 취약성이 없거나 적은 정보시스템과 취약성이 많은 정보시스템은 피해의 범위와 규모가 매우 다르게 된다. 물론 이 부분을 확률로 처리할 수도 있지만, 위협의 특성(원천, 종류, 발생률)과 시스템의 특성(취약점, 보유자산의 종류 및 가치)에 따라 매우 다양한 형태의 피해가 발생하는 상황을 모형화하는 것이 필요하다.

또한 본 연구에서 하드웨어 대체비용, 데이터 복구비용, 작업 유실비용을 모두 상수로 처리했는데, 좀더 실제 복구비용을 반영한 함수 형태로 모형에 반영하는 것이 필요하다. 하드웨어 대체비용은 하드웨어의 종류(PC, 서버 등)에 따라 이산확률분포의 형태가 적합할 것이고, 데이터복구 비용은 데이터복구 소요시간에 비례하는 선형함수(또는 계단형 선형함수) 형태가 적합할 것이다. 작업 유실비용은 처리대상 작업의 가치에 따라 다양한 비용이 발생할 수 있으므로, 일반함수의 형태를 가정하는 것이 바람직할 것이다.

참 고 문 헌

[1] 공희경, 김태성, "정보보호 투자효과에 대한 연구 동향", 「정보보호학회지」, 제17권, 제4호(2007), pp.12-19.

[2] 행정안전부, 한국정보사회진흥원, 2008 정보화 통계집, 한국정보사회진흥원, 2008.

[3] 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.79-83.

[4] Campbell, K., L.A. Gordon, M.P. Loeb, and L. Zhou, "The economic cost of publicly announced information security breaches : Empirical evidence from the stock market," *Journal of Computer Security*, Vol.11, No.3 (2003), pp.431-448.

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

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

[7] Computer Security Institute, *CSI/FBI Computer Crime and Security Survey*, 2006.

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

[9] Gordon, L.A., M.P. Loeb, and W. Lucyshyn, "Information security expenditures and real options : A wait and see approach," *Computer Security Journal*, Vol.19, No.2(2003), pp.1-7.

[10] Harrison, P.G. and E. Pitel, "Sojourn times in single-server queues with negative customers," *Journal of Applied Probability*, Vol.30, No.4(1993), pp.943-963.

[11] Harrison, P.G. and E. Pitel, "The M/G/1 queue with negative customers," *Advances in Applied Probability*, Vol.28, No.2(1996). pp.540-566.

[12] Mendenhall, W., R. Scheaffer, and D.D. Wackerly, *Mathematical Statistics with Applications*, 3rd edition, Duxbury Press, Boston, 1986.

[13] Towsley, D. and S.K. Tripathi, "A single server priority queue with server failures and queue flushing," *Operations Research Letters*, Vol.10, No.6(1991). pp.353-362.

[14] Yang, W.S. and K.C. Chae, "A note on the GI/M/1 queue with Poisson negative arrivals," *Journal of Applied Probability*, Vol.38, No.4(2001). pp.1081-1085.

[15] Yang, W.S., J.D. Kim, and K.C. Chae, "Analysis of M/G/1 stochastic clearing systems", *Stochastic Analysis and Applications*, Vol. 20, No.5(2002), pp.1083-1100.