情報保護學會論文誌
第20卷 第2號, 2010. 4

작업처리율을 고려한 정보보호 투자 포트폴리오 평가

양 원 석,[1†] 김 태 성,[2‡] 박 현 민[3]
[1]한남대학교 경영학과, [2]충북대학교 경영정보학과/BK21사업팀, [3]부경대학교 시스템경영공학과

Considering System Throughput to Evaluate Information Security Investment Portfolios

Won-Seok Yang,[1†] Tae-Sung Kim,[2‡] Hyun-Min Park[3]
[1]Department of Business Administration, Hannam University,
[2]Department of Management Information Systems, Chungbuk National University,
[3]Department of Systems Management and Engineering, Pukyong National University

요 약

본 논문에서는 정보보호 침해에 의해 조직에서 운영하는 정보시스템의 작업처리율이 저하되는 경우를 가정하고, 이러한 정보보호 침해에 대비하기 위해 조직에서 설치하는 다양한 보안 대안들로 구성되는 포트폴리오의 경제성을 평가한다. 확률모형을 이용하여 보안 위협 발생률에 따른 포트폴리오 별 작업처리율 및 평균 수리횟수를 분석하여 투자기간 동안 발생한 매출액과 수리비용을 제시한다. 아울러 작업처리율에 따른 매출액, 포트폴리오 별 보안시스템 구축 투자비, 수리 비용에 이자율을 적용하여 투자기간 동안 손익의 현재가치를 산출한다. 연구결과는 각 조직 별로 예산 제약과 투자대안 선정기준에 맞춰 최적 투자 포트폴리오를 선택하는데 활용될 수 있다.

ABSTRACT

We consider an information system where its throughput deteriorates due to security threats and evaluate information security investment portfolios. We assume that organizations adopt information security countermeasures (or portfolios consisted of countermeasures) to lessen the damage resulted from the productivity (or throughput) deterioration. A probability model is used to derive the system throughput and the average number of repairs according to the occurrence rate of security threats. Considering the revenue from throughput, the repair cost, and the investment for the security system, the net present value for each portfolio is derived. Organizations can compare information security investment portfolios and select the optimal portfolio.

Keywords: Information Security Breach, Security Threat, Investment Portfolio, Throughput, Economic Analysis, Probability Model

I. 서 론

정보서비스의 이용이 민간 및 공공 부문 등 사회 전반에 널리 확산되고, 무선 네트워크의 이용과 인터넷 프로토콜에 기반한 서비스가 보편화되면서, 해킹, 바이러스등의 전통적인 정보보호 침해(information security breach) 뿐만 아니라 피싱 등의 다양한 신종 정보보호 침해가 발생하고 있다[1]. 정보보호의 중요성에 대한 인식 수준은 높아지고 있지만 정보보호 침해를 방지하기 위한 투자는 정보보호 인식 수준만큼 증가하고 있지 못하다. 정보보호에 대한 투자가 증가하지 않는 데에는 다양한 이유가 있겠지만, 정보보호 침해로 인한 피해 규모를 화폐가치로 측정하기가 어렵다는 것이 주요 이유일 것이다.

접수일(2009년 9월 13일), 수정일(2009년 12월 25일), 게재확정일(2010년 1월 27일)
† 주저자, wonsyang@hnu.kr
‡ 교신저자, kimts@chungbuk.ac.kr

정보보호 침해로 인해 발생하는 피해에 대해서는 2000년대 중반부터 다양한 연구가 수행되어 왔다. Gordon과 Loeb[2]은 정보보호의 목표인 기밀성, 무결성, 가용성의 상실로 발생하는 피해를 직접비용과 간접비용, 명시적비용과 잠재적비용으로 구분하여 파악하는 개념적 틀을 제시하였다. 유진호 외[3]는 Gordon 과 Loeb[2]의 개념적 틀을 사용하여 2003년 1월 25일 에 발생한 슬래머웜에 의한 인터넷침해사고의 피해 규모를 산출하였다. 양원석 외[4]는 정보보호 침해로 인해 발생한 정보시스템의 하드웨어 대체비용, 저장자료 복구비용, 트랜잭션 유실비용을 고려하여 최적 정보보호 투자 포트폴리오를 분석하였다.

일반적으로 바이러스나 해킹 등의 정보보호 위협은 정보통신시스템의 정상적인 기능을 방해하고 시스템의 성능을 악화시킨다. 분산서비스거부공격 (Distributed Denial of Service Attack)에 의해 특정 라우터에 트래픽이 집중되면, 해당 라우터는 정상적인 트래픽을 처리하지 못하므로 시스템의 성능이 저하되는 결과를 초래한다.

논 논문에서는 성능저하를 고려한 시스템 분석 모형을 이용하여 위협이 존재하는 정보시스템을 확률적으로 모형화하고 투자의 경제성을 분석한다. 시스템 성능저하에 대한 확률적인 분석은 지난 20여년간 다양한 연구가 진행되어 왔다[5-9]. 본 논문에서는 Yeh[7]와 같이 시스템이 복수개의 상태로 구성되어 있다고 가정한다. 시스템의 상태는 시스템 성능을 의미한다. 위협에 따라 정보시스템에 미치는 피해가 상이하므로 복수 개의 상태를 가정하는 것이 현실적이다. Yeh[7]에서는 시간 간격을 두고 시스템을 관찰할 수 있다고 하였다. 그러나 정보시스템에서는 시스템 통계를 전산적으로 처리하여 실시간으로 추출할 수 있으므로 본 논문에서는 실시간으로 시스템의 상태를 관리한다고 가정한다. 시스템의 고장을 방지하고 안정적으로 운영하기 위해 예방정비를 도입하였다. 시스템 관리자는 시스템의 성능이 일정 상태 이하로 저하되는 경우 시스템을 수리한다. 정보시스템은 사용자들에게 일정 수준 이상의 성능을 제공해야 한다. 따라서 대부분의 경우 시스템 고장 전에 시스템을 수리하는 것이 바람직하다.

본 논문에서는 보안 위협 발생률에 따른 포트폴리오 별 작업처리율 및 평균 수리횟수를 확률적으로 분석하고 투자기간 동안 발생한 매출액과 수리비용을 제시한다. 작업처리율에 따른 매출액, 포트폴리오별 보안시스템 구축 투자비, 수리 비용에 이자율을 적용하여 투자기간 동안 손익의 현재가치를 산출한다. 마지막으로 모수 추정방안 및 다양한 수치 예를 제시한다.

II. 모형

시스템은 가동 능력에 따라 $0,1,\cdots,\beta$의 상태로 구분된다. 상태 k에서 서비스 시간은 비율이 μ_k인 지수분포를 따른다. 시스템 상태 k가 증가할수록 시스템의 성능이 악화된다. β는 시스템 고장을 의미한다. 정의에 따라 $i>j$ 이면, $\mu_i>\mu_j$ 이고 $\mu_\beta=0$ 이다.

보안 대책의 조합에 따라 M개의 보안 포트폴리오가 가능하다. m번째 포트폴리오를 PF_m이라 표기한다. PF_o는 보안 대책이 없는 경우를 의미한다. PF_m에서는 비율이 ω_m인 포아송 과정에 따라 위협이 발생한다. $m=0,1,\cdots,M$ 에 대해 m이 클수록 PF_m의 보안체계가 우수하다고 가정한다. 즉, $i>j$에 대해, $\omega_i<\omega_j$ 이다. 위협은 g_k의 확률로 시스템 상태를 k만큼 증가시킨다($k=1,\cdots$). 위협에 의해 시스템 상태가 β 이상이 되는 경우에는 시스템 상태를 β로 간주한다. 시스템 관리자는 시스템의 고장을 막고 성능을 일정 수준 이상으로 유지하기 위해 시스템의 상태가 α 이상인 경우 시스템을 수리한다. 본 논문에서는 α를 수리수준이라 부른다. 수리시간은 비율이 δ인 지수분포를 따른다. 시스템은 수리 중에도 작동한다고 가정한다. 수리 중에는 위협이 발생하지 않는다고 가정한다.

본 논문에서는 다음의 매출 및 비용을 가정한다. 첫째, 매출은 정보시스템에 의해서만 발생하고, 서비스 건당 p만큼의 매출이 발생한다. 둘째, PF_m의 보안시스템 구축 투자비 c_m이 발생한다. m이 클수록 PF_m의 보안체계가 우수하므로 $i>j$에 대해 $c_i>c_j$ 라 가정한다. 투자비는 보안시스템 구축 초기에 1회 발생한다. 셋째, 시스템 수리 건당 c_R 로 수리비용이 발생한다. 단위 회계기간을 τ로 표기한다. 단위 회계기간 동안 이자율을 θ로 표기한다.

본 논문에서 이용하는 기호를 정리하면 다음과 같다.

- $0,1,\cdots,\beta$: 시스템 상태,
- μ_k : 상태 k에서 서비스 율, $k=0,1,\cdots,\beta$,
- M : 포트폴리오 개수,
- PF_m : m번째 포트폴리오, $m=0,1,\cdots,M$,
- ω_m : PF_m에서 위협 도착률, $m=0,1,\cdots,M$,
- g_k : 위협 도착 시 시스템 상태 악화 확률, $k=1,\cdots$,

- α : 수리수준,
- δ : 수리 율,
- p : 서비스 건당 매출,
- c_m : PF_m 보안시스템 구축 투자비, $m=0,1,\cdots,M$,
- c_R : 건당 수리비용,
- τ : 단위 회계기간,
- θ : 단위 회계기간 동안 이자율,
- ρ : 시스템 작동을 위한 최저 서비스 율,
- π_k : 시스템 상태가 k일 확률, $k=0,1,\cdots,\beta$,
- Ψ_m: PF_m에서 작업처리율,
- $P(m,\alpha,y)$: PF_m, 수리수준 α, y년 경과된 시점에서의 손익의 누적 현재가치.

III. 경제성분석

PF_m에서 시스템 상태에 대한 전이율(transition rate) 행렬 Q는 다음과 같이 표현된다.

$$Q=\begin{bmatrix} -\omega_m & \omega_m g_1 & \cdots & \omega_m g_{\alpha-1} & \omega_m g_\alpha & \cdots & \cdots & \omega_m \bar{g}_\beta \\ 0 & -\omega_m & \ddots & \ddots & \omega_m g_{\alpha-1} & \cdots & \cdots & \omega_m \bar{g}_{\beta-1} \\ \vdots & 0 & \ddots & \ddots & \ddots & \cdots & \cdots & \vdots \\ 0 & \vdots & 0 & \ddots & \omega_m g_1 & \cdots & \cdots & \omega_m \bar{g}_{\beta-\alpha-1} \\ \delta & \vdots & \ddots & 0 & -\delta & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \delta & 0 & \cdots & \cdots & \cdots & \cdots & 0 & -\delta \end{bmatrix} \quad (1)$$

여기서 $\bar{g}_k=\sum_{m=k}^{\infty} g_m$ 이다. 시스템 상태가 k일 확률을 π_k라 하자. 그리고 π_k의 확률벡터를 $\pi=(\pi_0,\cdots,\pi_\beta)$라 정의한다. 식 (1)을 전이율 행렬로 갖는 마코프체인에 대해 다음 관계가 성립한다 [10].

$$\pi Q=0. \quad (2)$$

$$\pi e=1. \quad (3)$$

여기서 e는 크기가 $\beta+1$이고 모든 원소가 1인 열벡터이다. 식 (3)은 확률 분포의 합이 1이라는 정규화(normalization) 조건이다. 식 (2)에서 다음의 상태방정식을 얻는다.

$$\begin{aligned} &\omega_m\pi_0=\delta(\pi_\alpha+\cdots+\pi_\beta),\\ &\omega_m\pi_k=\omega_m(g_k\pi_0+\cdots+g_1\pi_{k-1}),\\ &\qquad k=1,\cdots,\alpha-1,\\ &\delta\pi_k=\omega_m(g_k\pi_0+\cdots+g_{k-\alpha+1}\pi_{\alpha-1}),\\ &\qquad k=\alpha,\cdots,\beta-1,\\ &\delta\pi_\beta=\omega_m(\bar{g}_\beta\pi_0+\cdots+g_{\beta-\alpha-1}\pi_{\alpha-1}),\ k=\beta. \end{aligned}$$

먼저, η_k를 아래와 같이 정의하자.

$$\begin{aligned} &\eta_k=\sum_{i=0}^{k-1}\eta_i g_{k-i},\ k=1,\cdots,\alpha-1,\\ &\tilde{\eta}_k=\frac{\omega_m}{\delta}\sum_{i=0}^{\alpha-1}\eta_i g_{k-i},\ k=\alpha,\cdots,\beta-1,\\ &\tilde{\eta}_\beta=\frac{\omega_m}{\delta}\sum_{i=0}^{\alpha-1}\eta_i g_{k-i},\ k=\beta. \end{aligned}$$

여기에서 $\eta_0=1$이다. 상태방정식을 순차적으로 풀면 다음을 얻는다.

$$\pi_k=\eta_k\pi_0,\ k=1,\cdots,\alpha-1, \quad (4)$$

$$\pi_k=\tilde{\eta}_k\pi_0,\ k=\alpha,\cdots,\beta. \quad (5)$$

식 (3)-(5)를 이용하면 다음을 얻는다.

$$\pi_0=\frac{1}{1+\sum_{k=1}^{\alpha-1}\eta_k+\sum_{k=\alpha}^{\beta}\tilde{\eta}_k}.$$

PF_m에서 작업처리율을 Ψ_m이라 표기하자. 작업처리율은 서비스를 완료하고 시스템을 떠나는 단위 시간당 작업 수이므로 다음을 얻는다.

$$\Psi_m=\sum_{k=0}^{\beta}\pi_k\mu_k. \quad (6)$$

식 (6)을 이용하면, PF_m에서 기간 τ동안 발생하는 매출액은 아래와 같다.

$$p\Psi_m\tau. \quad (7)$$

이제 시스템 상태가 α 이상인 경우에는 다른 상태로 전이하지 않는다고 가정한다. 그리고 α 이상의 상태를 F 라 표기하자. 이 경우 PF_m에서 상태 $0,1,\cdots,\alpha-1,F$ 에 대한 전이율 행렬 $\tilde{Q}$ 는 다음과 같다.

$$\tilde{Q}=\begin{bmatrix} -\omega_m & \omega_m g_1 & \omega_m g_2 & \cdots & \omega_m g_{\alpha-1} & \omega_m \bar{g}_\alpha \\ 0 & -\omega_m & \omega_m g_1 & \cdots & \omega_m g_{\alpha-2} & \omega_m \bar{g}_{\alpha-1} \\ \vdots & 0 & \ddots & \cdots & \cdots & \vdots \\ & \vdots & 0 & \ddots & & \omega_m \bar{g}_2 \\ & & & \ddots & -\omega_m & \omega_m \\ & & & & \ddots & 0 \end{bmatrix} =\begin{bmatrix} G & \mathbf{q} \\ \mathbf{0} & 0 \end{bmatrix} \quad (8)$$

PF_m에서 시스템 상태 0에서 α 이상이 되어 수리를 시작할 때까지 기간을 Γ_m이라 하자. Γ_m은 식 (8)의 $\tilde{Q}$를 전이율 행렬로 갖는 흡수 마코프체인의 흡수시간과 동일하다. 흡수 마코프체인의 결과를 이용하면 다음을

얻는다.

$$E[\Gamma_m] = -x_0 G^{-1} \mathbf{e}. \quad (9)$$

여기서 $\mathbf{e}$는 크기가 α이고 모든 원소가 1인 열벡터이다. $\boldsymbol{x}_0$는 마코프체인의 초기조건을 의미하며 $\boldsymbol{x}_0$의 원소는 다음과 같다.

$$\boldsymbol{x}_0 = (1,0,\cdots,0).$$

평균 수리시간이 $1/\delta$ 이므로 평균적으로 $E[\Gamma_m]+1/\delta$ 기간에 한 번씩 시스템을 수리한다. 따라서 PF_{m}에서 τ 동안 평균 수리비용은 다음과 같다.

$$\frac{c_R \tau}{E[\Gamma_m]+1/\delta}. \quad (10)$$

PF_{m}과 수리수준 α에서 y 년 경과된 시점에서의 손익의 현가를 $P(m,\alpha,y)$라 하자. 포트폴리오 구축 투자비는 시간 0에서 발생한다. 반면, 매출과 수리비용은 시간에 따라 발생하는 변동비이다. 투자기간 τ동안의 이자율이 θ이므로, 식 (7), (10)을 이용하면 $P(m,\alpha,y)$은 다음과 같다.

$$P(m,\alpha,y) = -c_m + \tau \sum_{k=1}^{y} \left[p\Psi_m - \left(\frac{c_R}{E[\Gamma_m]+1/\delta} \right) \right] \frac{1}{(1+\theta)^k} \quad (11)$$

IV. 모수추정방안 및 수치 예

시스템이 상태 k에서 운영된 총 시간을 t_k, t_k 동안 완료된 서비스 개수를 s_k, PF_{m}에서 시간 t 까지 발생한 위협 개수를 v_m, 그리고 i 번째 시스템 수리시간을 r_i 라 표기한다. 여기에서 $k=0,1,\cdots,\beta, m=0,1,\cdots,M$, $i=1,2,\cdots$. 서비스 시간, 위협 발생 간격, 수리시간이 지수 분포를 따르므로 시스템 모수를 다음과 같이 추정할 수 있다[11,12].

$$\hat{\mu}_k = \frac{s_k}{t_k},\ \hat{\omega}_m = \frac{v_m}{t},\ \frac{1}{\hat{\delta}} = \frac{\sum_{i=1}^{K} r_i}{K}. \quad (12)$$

이때 t_k 및 t는 충분히 크다고 가정한다. PF_0가 현재 보안수준인 경우에는 식 (12)를 이용하여 시스템에서 $\hat{\omega}_0$를 산출한다. 반면, $m \geq 1$인 경우에는 PF_{m}을 적용한 기업 및 공공기관의 위협 발생률을 벤치마킹하여 $\hat{\omega}_m$를 산정한다.

〔표 1〕 시스템 서비스 율

(단위 : 시간당 건수)

서비스 율	값
상태 0 ($\hat{\mu}_0$)	20
상태 1 ($\hat{\mu}_1$)	10
상태 2 ($\hat{\mu}_2$)	5
상태 3 ($\hat{\mu}_3$)	3
상태 4 ($\hat{\mu}_4$)	1
상태 5 ($\hat{\mu}_5$)	0

〔표 2〕 포트폴리오 별 위협 발생률 및 투자비

(단위: 년발생횟수, 억원)

포트폴리오	위협 발생률		투자비	
	모수	값	모수	값
PF0	$\hat{\omega}_0$	100	c_0	-
PF1	$\hat{\omega}_1$	50	c_1	20
PF2	$\hat{\omega}_2$	25	c_2	25
PF3	$\hat{\omega}_3$	10	c_3	30

마지막으로 시스템의 모수가 식 (12)를 통해 추정되었다는 가정 하에 경제성 분석 예제를 제시한다. 어떤 기업의 정보시스템 서비스 율이 〔표 1〕과 같다고 가정한다.

정보보호 포트폴리오 구성에 따른 위협 발생률 추정치 및 투자비를 〔표 2〕와 같이 가정한다.

다양한 종류의 위협이 발생하므로 이에 따른 불확실성을 고려하여 위협의 크기 확률 g_m이 식 (13)과 같은 기하분포를 따르고 $g=0.5$이라 가정한다.

$$g_m = g(1-g)^{k-1},\ k=1,2,\cdots. \quad (13)$$

매출 및 비용은 다음과 같다. 서비스 당 매출 p는 월 1천 만원, 평균 수리기간 $1/\delta$는 12시간, 건당 수리비용 c_R은 2천만원이라 가정한다. 모수는 시간 단위로 환산하여 분석한다. 단위 회계기간 τ는 1년, 이자율 θ는 10%이다. 투자분석은 최대 7년으로 하였다.

식 (6)을 이용하여 포트폴리오 및 수리수준 α에 따른 작업처리율 Ψ_m를 계산하면 〔표 3〕을 얻는다.

작업처리율 기준이 $\rho > 16$라 하자. 〔표 3〕에서 모든 포트폴리오에 대해 수리수준이 4와 5인 경우는 작업처리율 기준을 만족하지 않으므로 현재가치 분석 대상에서 제외한다.

식 (11)을 이용하여 포트폴리오 0, 1, 2, 3의 손익

〔표 3〕 작업처리율

(단위: 시간당 건수)

수리수준 (α)	포트폴리오			
	PF0	PF1	PF2	PF3
1	19.58	19.78	19.89	19.96
2	18.29	18.48	18.57	18.63
3	16.67	16.83	16.92	16.97
4	14.91	15.05	15.10	15.17
5	13.08	13.21	13.30	13.31

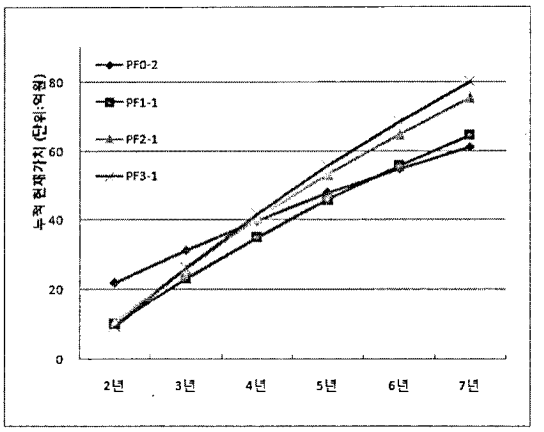
의 누적 현재가치를 산출하면 〔표 4〕를 얻는다. 예를 들어, 포트폴리오 0에서 수리수준이 1인 경우, 2년 동안 발생한 손익을 현재가치로 환산하면 19.6억원이 된다.

각 포트폴리오에 대해 PF0에서는 수리수준 2, PF1에서 PF3까지는 수리수준 1의 누적 현재가치가 가장 크다. 손익을 최대화하는 최적 수리수준은 포트폴리오에 따라 변화함을 알 수 있다.

포트폴리오가 x이고 수리수준이 y인 경우를 PFx-y로 표기한다. 〔표 4〕에서 포트폴리오 별 최적 수리수준에 대한 누적 현재가치를 도시하면 〔그림 1〕과 같다.〔그림 1〕에서 3년차까지는 PF0, 4년차부터는 PF3의 누적 현재가치가 가장 크다.

보안 포트폴리오에 대한 투자의사결정은 기업의 경영여건 및 투자성향에 영향을 받는다. 아울러, 보안투자에 대한 의사결정 권한이 CFO(Chief Financial Officer)에게 있는 경우, 정보보호 투자에 따른 현금흐름 분석이 중요하다. 정보보호 투자가 기업 경영에 미치는 영향을 화폐가치로 환산하지 않으면 CFO는 여러가지 투자대안 중에서 최적의 대안을 선택하기 어렵다. 특히, 투자기간이 변동될 수 있는 경우를 고려한 의사결정시에는 이러한 어려움이 가중된다.

〔그림 1〕에서 보안투자가 없는 PF0와 보안투자가 있는 PF3과 비교해보자. 2년까지는 누적 현재가치를 비교하면 PF0가 PF3보다 10억 정도 이득이다. 기업이 단기적인 투자의사결정을 한다면 〔그림 1〕을 보면 PF0-2가 가장 최적이다. 시장 및 경영여건상 현재 시스템을 한시적으로 운영한다면 보안투자 없이 유지보수를 자주하지 않는 것이 단기적으로 이득이다. 한편, 7년차까지 누적 현재가치를 비교하면 PF3가 PF0 보다 20억원 정도 이익이다. 중장기적인 관점에서 투자의사결정을 내린다면 PF3-1이 최적이다. 보안투자를 하고 유지보수도 필요하다. 한편, 기업에서 보안투자



〔그림 1〕 포트폴리오 별 누적 현재가치

〔표 4〕 손익의 누적 현재가치

(단위: 억원)

포트폴리오	수리 수준	1년	2년	3년	4년	5년	6년	7년
PF0	1	10.3	19.6	28.0	35.7	42.7	49.1	54.9
	2	11.4	21.9	31.3	39.9	47.7	54.8	61.3
	3	11.3	21.5	30.9	39.3	47.1	54.1	60.4
PF1	1	-4.2	10.1	23.2	35.0	45.8	55.6	64.5
	2	-4.2	10.1	23.1	35.0	45.7	55.5	64.4
	3	-5.2	8.3	20.5	31.7	41.8	51.0	59.4
PF2	1	-6.3	10.8	26.3	40.3	53.1	64.8	75.4
	2	-7.0	9.4	24.3	37.9	50.2	61.4	71.5
	3	-8.3	6.8	20.6	33.1	44.5	54.8	64.2
PF3	1	-9.4	9.3	26.3	41.7	55.8	68.6	80.2
	2	-10.6	7.1	23.1	37.7	51.0	63.0	74.0
	3	-12.2	4.0	18.7	32.0	44.2	55.2	65.2

의 필요성을 인식하여 장기적인 관점에서 보안 투자를 계획하고 있으나 단기적인 자금 압박 때문에 투자비를 낮추려고 한다고 가정해보자. 이 경우에는 PF3보다 누적 현재가치가 조금 작은 PF2 투자를 대안으로 제시할 수 있다. 따라서 본 논문에서 제시한 방법을 이용하면, 기업이 경영여건을 고려하여 장단기적인 관점에서 보안투자 의사결정을 내릴 수 있다.

V. 결 론

본 논문에서는 정보보호 침해에 의해 정보시스템의 작업처리율이 저하되는 경우, 정보보호 침해에 대비하기 위한 다양한 보안대안들로 구성되는 포트폴리오의 경제성을 평가할 수 있는 수리적인 모형을 제시하였다. 양원석 외[4]에서는 정보시스템의 하드웨어 대체비용, 저장자료 복구비용, 트랜잭션 유실비용 등 정보보호 침해로 인해 발생한 물리적 피해를 고려한 최적 정보보호투자 포트폴리오 선정을 위해 확률적 모델을 제시하였다. 정보보호 침해로 인한 피해를 물리적인 손실, 영업적인 손실, 법적 보상으로 인한 손실로 구분한다면, 양원석 외[4]에서는 물리적이고 가시적인 손실 부분만을 고려한 경우의 최적 투자포트폴리오를 선정하기 위한 연구이다. 영업적인 손실 중에서 시스템 비정상 작동으로 인한 시스템 가동률 저하, 업무지장 등은 쉽게 피해규모를 파악하기가 어렵기 때문에 투자의사결정에 고려되지 못하던 부분이다. 본 연구에서는 정보보호 침해로 인해 정보시스템의 작업처리율이 저하되는 등의 업무상 피해를 입을 수 있는 상황을 고려하여 최적 투자 포트폴리오를 선정하는 모형을 제시하였다는 점에서, 양원석 외[4]의 연구에서 고려하지 못한 피해형태를 다룬 연구이다.

공희경 외[13]에서는 다기준의사결정방법인 AHP를 이용하여 복수개의 정보보호투자대안 중에서 최적대안을 선정하는 의사결정모형을 제시하였다. 고려된 투자대안이 단일 기술들이고, 전문가의 주관적 의견을 취합 및 분석하여 최종결과를 도출하였다. 본 연구에서는 침해사고가 발생하고 시스템에 성능저하라는 영향을 미치는 상황을 세분화하여 모델링 하였다는 점에서 공희경 외[13]의 연구와는 차별화된 장점을 갖는다고 할 수 있다.

적정한 수준의 정보보호 투자가 이루어지기 위해서는 정보보호 투자의 효과, 정보보호 침해사고 발생으로 인한 손실 등에 대한 객관적인 분석, 궁극적으로는 재무적인 데이터로의 환산이 필요하다. 본 연구에서는 조직에서 고려하고 있는 정보보호 투자 포트폴리오에 대한 현가를 분석하고, 복수 포트폴리오간의 비교를 가능하게 할 수 있는 모형을 제시하고, 실제 적용가능성을 수치 예를 이용하여 제시함으로써, 조직에서 정보보호 투자 의사결정시 참고자료로 활용할 수 있을 것이다. 기업에서는 정보보호뿐만 아니라 서비스, 시스템 등의 다양한 분야에 대해 투자 여부, 규모, 시기, 우선순위 등에 대한 종합적인 투자 전략이 필요하다. 이러한 투자 전략은 기업의 손익과 같은 경영여건에 크게 영향을 받는다. 따라서 최적 투자 의사결정을 도출하기 위해서는 재무적인 측면에서 정보보호 투자에 대한 경제성 분석이 요구된다. 특히, 투자기간의 변동성을고려하는 경우에는 투자기간에 따른 손익분석이 필요하다. 따라서 장단기의 다양한 투자에 대한 의사결정이 필요한 경우 본 연구결과가 유용하리라 기대한다.

본 연구에서는 정보보호 침해로 인해 생산성(작업처리율)이 저하되는 경우를 고려하여 보안 투자 포트폴리오의 평가 모형을 개발하고 수치 예를 보였다. 하지만, 보안 투자로 인한 생산성 저하 감소분, 정보시스템 수리비용 등 투자로 인해 발생하는 현실적인 현금 흐름을 반영하지 못해 보안 포트폴리오 투자 효과의 현가가 시간 경과에 따라 점증하는 등의 다소 비현실적인 점이 한계이다. 하지만, 본 모형의 주된 목적은 복수개의 포트폴리오 간 비교를 하는 것이므로 연구결과의 활용에 큰 장애가 되지는 않는다.

정보보호 투자를 준비하고 있는 조직들은 순현가의 최대화를 투자기준으로 삼을 수도 있고, 회수기간이 짧은 투자 대안을 선호할 수도 있고, 내부수익률 기준으로 투자대안을 선정할 수도 있고, 비용 대비 효과의 정도를 중요한 투자기준으로 사용할 수도 있다. 추후에는 정보보호 투자를 수행하는 조직의 다양한 여건을 반영할 수 있도록, 현실적인 현금 흐름 데이터와 다양한 투자기법을 적용하여 현실적인 투자의사결정에 도움을 줄 수 있는 모형에 대한 연구가 필요할 것이다.

또한, 물리적 손실, 생산성 손실 등의 직접적인 손실 이외에 법적 보상 등의침해사고 발생으로 인한 파생적인 피해를 고려하는 것도 향후에 유망한 연구주제가 될 수 있을 것이다.

참 고 문 헌

[1] 국가정보원, 방송통신위원회, 행정안전부, 지식경

제부, "2009 국가정보보호백서," pp. 17-26, 2009년 4월.

[2] L.A. Gordon and M.P. Loeb, Managing Cyber-Security Resources: A Cost-Benefit Analysis, McGraw-Hill, New York, pp. 53-60, Jan. 2006.

[3] 유진호, 지상호, 송혜인, 정경호, 임종인, "인터넷 침해사고에 의한 피해손실 측정," 정보화정책, 15(1), pp. 3-18, 2008년 3월.

[4] 양원석, 김태성, 박현민, "확률모형을 이용한 정보보호 투자 포트폴리오 분석," 한국경영과학회지, 34(3), pp. 155-163, 2009년 9월.

[5] M. Ohnishi, H. Kawai, and H. Mine, "An optimal inspection and replacement policy for a deteriorating system," Journal of Applied Probability, vol. 23, no. 4, pp. 973 - 988, Dec. 1986.

[6] C.T. Lam and R.H. Yeh, "Optimal maintenance policies for deteriorating systems under various maintenance strategies," IEEE Transactions on Reliability, vol. 43, no. 3, pp. 423 - 430, Sep. 1994.

[7] R.H. Yeh, "Optimal inspection and replacement policies for multi-state deteriorating systems," European Journal of Operational Research, vol. 96, no. 2, pp. 248-259, Jan. 1997.

[8] C.C. Hsieh and K.C. Chiu, "Optimal maintenance policy in a multistate deteriorating standby system," European Journal of Operational Research, vol. 141, no. 3, pp. 689 - 698, Sep. 2002.

[9] C.C. Hsieh, "Replacement and standby redundancy policies in a deteriorating system with aging and random shocks," Computers and Operations Research, vol. 32, no. 9, pp. 2297 - 2308, Sep. 2005.

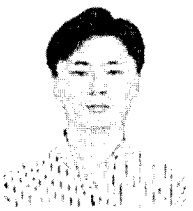
[10] S.M. Ross, Stochastic Process, John Wiley & Sons, New York, pp. 251-253, 1996.

[11] H.W. Lilliefors, "Some confidence intervals for queues," Operations Research, vol. 14, no. 4, pp. 723-727, Aug. 1966.

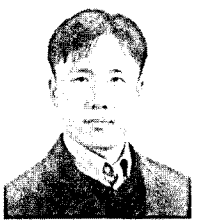
[12] W. Mendenhall, R. Scheaffer, and D.D. Wackerly, Mathematical Statistics with Applications, 3th Ed., Duxbury Press, Boston, pp. 367-370, 1986.

[13] 공희경, 전효정, 김태성, "AHP를 이용한 정보보호 투자 의사결정에 대한 연구," Journal of Information Technology Applications & Management, 15(1), pp. 137-150, 2008년 3월.

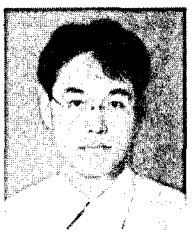
〈著者紹介〉



양 원 석 (Won-Seok Yang) 정회원
1993년 2월: KAIST 경영과학과 학사
1995년 2월: KAIST 경영과학과 석사
2000년 2월: KAIST 산업공학과 박사
2000년 2월~2007년 1월: LG텔레콤 차장
2007년 2월~2010년 2월: 한국전자통신연구원 기술전략연구본부 선임연구원
2010년 3월~현재: 한남대학교 경영학과 조교수
〈관심분야〉 확률모형, 대기행렬 이론, 생산관리, 통신정책, 통신망 성능분석, 기술경제성, 안 경제성



김 태 성 (Tae-Sung Kim) 종신회원
1991년 2월: KAIST 경영과학과 학사
1993년 2월: KAIST 경영과학과 석사
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2000년 9월~현재: 충북대학교 경영정보학과 교수, 학과장
〈관심분야〉 정보보호 및 정보통신 분야의 경영 및 정책 의사결정



박 현 민 (Hyun-Min Park) 정회원
1996년 2월: 연세대학교 경영학과 학사
1998년 8월: KAIST 산업공학과 석사
2009년 8월: KAIST 산업및시스템공학과 박사
2009년 9월~현재: 부경대학교 시스템경영공학과 기금교수
〈관심분야〉 확률모형, 대기행렬 이론, 품질관리, 정보보호 경제성 분석