위협별 대응기술들의 상관관계를 고려한 보안 투자 모델링

김민식* · 임종인**

요 약

보안 투자에 대한 정당성을 확보하기 위해 보안 투자에 대한 투자대비효과 분석이 반드시 요구된다. 본 논문에서는 최적의 보안 투자 의사결정을 어렵게 하는 요소들을 고려함과 동시에 투자대비효과를 정량적인 수치로 표현하여 효과적인 의사 결정을 지원할 수 있는 모델링을 제안한다. 본 모델링은 최적의 정보보안 솔루션을 선정하기 위하여 잔여 위험 수치를 판단 기준으로 활용하고, 가용한 정보보안 솔루션 중에서 정보보안 솔루션들의 위협별 대응기술들의 상관관계를 고려하여 정확성을 높여준다.

The Best Model to Optimize Security Investments with Considering a Corelation of Response Techniques Against Each Threat

Min Sik Kim* · Jong In Lim**

ABSTRACT

To get legitimacy of a security investment, the analysis of ROI about the security investment is required. In this paper, we suggest a practical quantitative model with considering factors that do decision-making of optimized security investment difficult. This model makes use of the value of a residual risk to decide the best information security solution and considers a corelation of response techniques of the information security solution against each threat to do exact decision-making.

Key words : ROI(Return On Investment), Security Investment, Integer Programming

접수일 : 2008년 12월 12일; 채택일 : 2009년 3월 2일

* ETRI 부설연구소

** 고려대학교 정보경영공학전문대학원

1. 서 론

인터넷과 IT 환경의 급속한 발전으로 정보화 사회로의 빠른 변화가 진행됨에 따라 동시에 정보화 역기능이 큰 위협으로 등장하기 시작했다. 새로운 해킹 기법 및 바이러스의 출현, 내부자에 의한 보안 위험, 물리적인 보안 위험 등은 계속하여 증가하고 있다. 기업 및 조직의 정보 시스템에 대한 의존도 증가와 기존 고정자산의 가치를 넘어서는 무형의 정보 자산 가치의 증가로 인하여 기업의 정보 자산 보안에 대한 중요성이 강조되고 있다. 정보시스템에 대한 의존도 증가는 정보 시스템의 침해 사고 발생 시 사업상의 치명적인 손실을 가져올 수 있으며, 기업경영의 연속성을 보장할 수 없다. 정보 자산에 대한 다양한 위험에 대해 효과적인 후보 정보보안 솔루션을 제시하여 사용자가 정보보안 위험에 대처할 수 있는 방법론이 요구된다. 적절한 투자비용을 결정하는 문제는 언제나 불확실성 속에서 실시되기 때문에 이론적으로 보다 확고하게 분석된 의사결정 지원 과정이 필요하다[1~3].

정보 시스템을 운영하는 인력들은 주요 정보 자산들을 보호하기 위하여 어떠한 보안 투자를 하여야 하며 얼마나 많은 보안 투자를 해야 하는가와 같은 고민에 직면해 있다. 따라서 보안 투자에 대한 정당성을 확보하고 투자 예산의 의사결정권자들에게 투자의 결과를 가시적으로 입증하기 위해서는 보안 투자에 대한 투자대비효과 분석 과정이 요구된다.

오늘날 투자에 있어서 그것이 실제로 기업의 발전에 도움이 되는지에 대한 정당성과 정확성에 대한 가치 평가를 위해 투자 수익률(ROI : Return On Investment) 모델을 통해 그것의 경제적 가치를 분석하는 방법이 널리 사용되고 있다. 정보보안에 대한 투자는 IT 투자와는 달리 투자 자체가 부를 창출하기 위한 목적이 아니라 정보 자산을 보호하고 잠재적 손실의 가능성을 최소화하기 위한 목적을 갖는다. 정보 보안을 위한 정보보안 솔루션의 평가에 있어서 가장 중요한 요소는 보안 위협에 의해 노출될 수 있는 정보 자산의 잠재적 위험을 얼마나 감소시킬 수 있는지에 달려있다. 그러나 한정된 보안 투자 예산, 효과적인 정보보안 솔루션과 관련 위협들과의 복잡한 다대다 관계(Ex : 하나의 보안 솔루션은 하나의 위협 방어에만 효과적인 것이 아니라 경우에 따라 두 개 이상의 다양한 위협들에 효과적임), 구현상의 제약조건 등의 요소들은 최적의 보안 투자 의사결정에 있어서 어려움을 발생시킨다.

본 논문에서는 최적의 정보보안 투자 의사결정을 어렵게 하는 요소들을 고려함과 동시에 투자대비효과를 정량적인 수치로 표현하여 효과적인 의사 결정을 지원할 수 있는 모델링을 제안한다. 본 모델링은 가용한 정보보안 솔루션 중에서 정보보안 솔루션들의 위협별 대응기술들의 상관관계를 고려하여 투자대비효과의 정확성을 높여주며 동시에 여러 제약조건들을 만족시키면서 잔여 위험 수치를 최소화할 수 있는 최적의 정보보안 솔루션 조합을 신속하고 정확하게 도출한다. 본 논문의 구성은 정보보안 솔루션 선택을 위한 방법론 관련 연구 소개, 제안하고 있는 방법론 및 샘플 소개, 결론으로 구성된다.

2. 관련 연구

초기에 정보보안 솔루션 결정을 위한 대부분의 방법론들은 정량적인 위험분석 결과보다는 정성적인 위험분석 결과에 치중되어, 수치화된 위험분석 결과를 산출하지 못하였다[2]. 일반적으로 IT 시스템의 잠재적 성과를 정량적인 값으로 평가하기 위한 수단으로 투자 수익률(ROI=Net Benefit / Cost× 100%) 분석 기법이 사용된다. IT 시스템에 대한 예산 투자는 향후 어느 정도 수익을 증대시킬 수 있는가를 기준으로 투자 정당성을 논한다. 정

보보안 솔루션 구축에서도 같은 기준의 투자 수익률 산정 잣대를 적용하여 정보보안 솔루션들에 대한 선택의 기준을 제시한다면 일관성이 유지되기 때문에 정보보안 투자 전략 선별의 기준 제시를 위한 표준 지표로서의 의미를 갖는다. 단, 투자 수익률 값을 도출하는 과정을 어떻게 객관적이고 효과적으로 수행하는가가 의사 결정에 지배적인 영향을 미치게 된다.

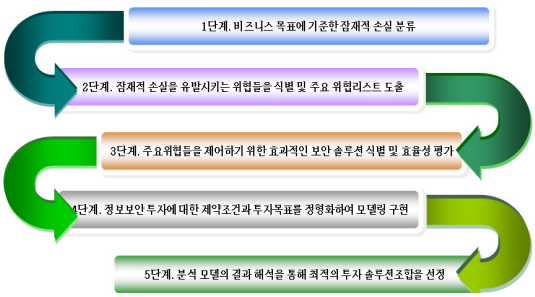
최근 정보보안 솔루션 선택을 위한 의사 결정 문제를 해결하기 위해 정량적인 값을 기반으로 한 모델링 기법들이 제안되고 있다. 예를 들면, [5]와 [7]에서는 어느 정도 잠재적 피해를 줄일 수 있는가를 기준으로 보안 투자에서의 투자 수익률 기반 모델링 기법을 제안하고 있다. 모든 정보보안 솔루션들의 도입 목표는 현재 기관이 처한 잠재적 손실을 사전에 인지하고 최소화하기 위한 것이므로 비즈니스의 영속성 측면에서 어떤 정보보안 솔루션이 얼마만큼의 손실을 예방할 수 있는가를 간접적으로 측정하는 위험 측정 지표를 활용하는 것은 충분히 타당하다. [5]와 [7]에서는 기존 ROI 모델을 바탕으로 한 ROSI(Return On Security Investment)={(기저위험-잔여위험-비용)/비용}t× 100% 모델이 제안되었다. 투자에 대한 효과를 감소한 위험으로 간접적으로 측정하였다. 기저위험은 현재 기관이 내재하고 있는 잠재적인 경제적 손실 추정치를 나타내고, 잔여위험은 정보보안 솔루션을 구현하고 남게 되는 위험 잔여량을 나타내며, 비용은 투자비용을 나타낸다. 추가적으로 [7]에서는 잔여위험=기저위험 × 공격우회율(bypass rate) 개념이 추가되어 좀 더 구체적인 개념을 제시하고 있다. 공격우회율이란 특정 정보보안 솔루션이 대응 가능한 위협들에 대해 얼마만큼의 방어 성능을 보여주는가를 측정하는 지표이다. 공격우회율의 값은 0~1사이의 값을 갖는다. 공격우회율 값이 0이라면 해당 정보보안 솔루션은 관련 공격을 100% 방어해 낼 수 있다는 것을 의미하고 1이라면 방어효과가 전혀 없다는 것을 의미한다. [9]에서는 [5]와 [7]에서의 개념을 도입함과 동시에 정수계획법(IP : Integer Programming)을 기반으로 정보보안 솔루션 조합의 투자대비효과 분석을 위한 정보보안 솔루션 분석 모델을 생성하고, 정보보안 솔루션 결정에 중요한 영향을 미치는 다양한 제약 조건들을 정형화하여 상기 정보보안 솔루션 분석 모델에 적용함으로써, 제약 조건들을 만족하는 범위 내에서 최소의 잔여 위험을 갖는 정보보안 솔루션 조합을 최적의 정보보안 솔루션 조합으로 결정하는 것을 특징으로 하는 모델링을 소개하고 있다.

3. 최적의 정보보안 솔루션 선정을 위한 모델

수치화되고 정량적인 위험분석의 결과는 최고경영층의 보안관련 의사결정에 도움을 준다는 것은 누구나 공감할 것이다. 일반적으로 정보보안 투자에 있어서 기존에 제안되었던 ROSI 값을 판단 기준으로 활용할 수도 있지만 본 논문에서는 잔여 위험 값을 판단 기준으로 활용하고자 한다. 잔여위험 값을 판단 기준으로 활용한 것은 정보자산의 가치가 갈수록 커지고 있으며 침해사고 발생이 기업의 이미지에 큰 손실을 발생시키며 사업의 지속성에 치명적인 피해를 유발할 수 있으므로 제약조건들을 만족하는 범위 내에서 잔여위험이 가장 낮은 조건이 최적의 투자 조건으로서 의미가 있기 때문이다.

본 논문에서는 [9]에서 제안되었던 모델링 기법을 도입함과 동시에 해당 모델링의 문제점을 개선시켜 잔여 위험 수치의 정확성을 높여 정보보안 투자를 최적화하고자 한다. 본 논문에서 제안하고자 하는 정보보안 솔루션 조합 선정을 위한 단계별 흐름도는 (그림 1)에서 보여준다. 정보보안 솔루션 조합을 결정하는 방법은, 비즈니스 목표에 기준한 잠재적 손실 분류와 가중치 설정 단계; 잠재적 손실을 유발시키는 위협들을 식별 및 주요 위협리스트 도출 단계; 주요 위협들을 제어하기 위

한 효과적인 정보보안 솔루션 식별 및 효율성 평가하는 단계; 정수계획법을 이용하여 투자에 대한 제약조건과 투자목표를 정형화하여 분석 모델 작성 단계; 분석 모델의 결과 해석을 통해 최적의 정보보안 투자 솔루션 조합(잔여 위험을 최소화시키는 조합)을 결정하는 단계를 포함하는 것을 특징으로 한다. 복잡한 제약조건하에서 가장 최적화된 정보보안 솔루션 투자 방식을 빠르고 정확하게 결정하기 위해 수학적 모델링 기법 중에 하나인 정수 계획법(Integer Programming) 방식을 활용되고 있다[6, 8]. 수학적 모델을 활용하면 여러 가지 조건들을 고려해야 하는 복잡한 문제라도 논리적이고 간편하게 표현할 수 있어 빠르고 정확하게 해집합을 찾을 수 있다. 위험에 대한 정보보안 솔루션 적용 효과를 모델링을 통해 시뮬레이션하여 위험의 감소 및 변경된 결과를 미리 파악할 수 있다.



(그림 1) 정보보안 솔루션 조합 선정을 위한 단계별 흐름도

[9]의 경우에는 각각의 정보보안 솔루션들의 위협별 세부 대응기술들 상관관계를 고려하지 않으므로 위협별 정보보안 솔루션들의 세부 대응기술이 같거나 상호간에 종속관계에 있는 경우에도 불구하고 중복되게 수식에 적용되므로 투자대비효과가 과장되는 경우가 발생하여 정확성이 떨어지는 문제점을 갖고 있다. 본 논문은 [9]의 모델링에서 공격우회율의 산정 방식을 개선하여 잔여 위험 수치의 정확성을 높이는 것으로 (그림 1)의 정보보안 솔루션 조합 선정을 위한 단계별 흐름도에서 3단계부터 중점적으로 다루기로 한다.

투자대비효과를 분석하기 위해서는 필요한 입력 데이터의 값들을 분석을 통해 확보해야 한다. 본 정보보안 솔루션 결정을 위한 모델링에서는 정보보안 솔루션 도입 효과의 정의를 좀 더 구체적으로 설명하기 위하여 기존에 연구에서 정의된 공격우회율(Bypass Rate), 총 공격우회율(Net Bypass Rate), 기저위험, 잔여위험과 같은 부가적인 개념 정의들을 동일하게 따른다[7]. 총 공격우회율은 일반적으로 기관에서는 정보 시스템 보호를 위해 하나의 정보보안 솔루션만을 구현하는 것이 아니라 다양한 정보보안 솔루션들을 중첩하여 구현하기 때문에 총 공격우회율의 계산이 필요하다.

$$\text{총 공격우회율}(j) = \prod_{i \in \text{보안솔류션 집합}} \text{공격우회율}(j,\ i)$$

(그림 2) 총 공격우회율

본 모델링에서는, 대상 기관이 취한 위험상황과 관련된 위협들, 위협들의 효과적인 제어를 위한 정보보안 솔루션들의 선별과정이 끝났다면 정수 계획법을 통한 정보보안 솔루션 조합에 대한 총 잔여 위험을 계산하여 출력하는 함수를 목표함수(F)로 정의하고, 정보보안 솔루션 결정에 중요한 영향을 미치는 다양한 제약 조건들을 정형화하여 상기 목표 함수에 적용함으로써, 제약 조건들을 만족하는 범위 내에서 최소의 목표함수 값을 갖는 정보보안 솔루션 조합을 최적의 정보보안 솔루션 조합으로 결정한다. (그림 3)은 목표함수를 나타내는 모델링 수식을 나타낸다. M은 보안 위협의 개수, N은 정보보안 솔루션 후보의 개수, Xi는 정보보안 솔루션 후보 i의 선택 여부를 나타내는 Binary 변수(If Xi = 1, selected, If Xi = 0, not selected), Dj는 보안 위협 j에 의해 유발될 수 있는 잠재적 예상 손실액, rij는 정보보안 솔루션 후보 i가 보안

위협 j에 대해 보이는 공격우회율 행렬을 나타낸다. 상기 공격우회율(rij)은 0에서 1사이의 값으로 평가되는 정보보안 솔루션 후보의 방어율을 나타내는 것으로, 0이면 정보보안 위협 j를 완벽하게 방어할 수 있는 것을 의미하며, 1이면 완전히 무력한 것을 의미한다. 각 Cluster는 동일 위협에 대한 대응 기술이 같거나 종속관계에 있는 정보보안 솔루션 그룹을 의미한다.

$$F(X_1, X_2, \cdots\cdots, X_N) =$$

선정된 보안 솔류션들 중에서,

j 위협에 대한 대응 기술이 같거나 상호간에 종속관계에 있는 원소들을 Cluster 구성

If r_{aj}=최소값 in Cluster{r_{kj}}, r_{aj}는 초기값 사용, 나머지 $r_{kj} \rightarrow 1$ except r_{aj}

$$\text{잔여 위험의 합} = \sum_{j=1}^{M} (D_j \cdot \prod_{i=1}^{N} (r_{ij} - 1) \cdot X_i + 1))$$

(그림 3) 잔여 위험의 합

(그림 3)의 식에서 공격우회율은 함께 도입되는 정보보안 솔루션들의 위협별 대응기술들 간의 상호관계를 고려하여 값을 결정한다. 각 Cluster 그룹에서 정보보안 솔루션의 공격우회율 값이 최소값인 경우는 그 값(초기값)을 그대로 유지하며 나머지 정보보안 솔루션의 공격우회율 값은 1로 변경시켜 잔여 위험 감소에 영향력을 미치지 못하게 한다. 이것은 같은 위협에 대한 대응기술 원리가 같거나 상호간에 종속관계에 있는 경우에 중복 적용을 피하게 하므로 잔여 위험 수치의 정확도를 높일 수 있다.

다음은 15개의 정보보안 솔루션 중에서 10개의 정보보안 솔루션이 선정 (X1, X2, X3, X4, X5, X6, X7, X8, X9, X10, X11, X12, X13, X14, X15)= (1, 0 , 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)되었을 때의 예를 나타낸다. (그림 4)의 (a)는 다른 정보보안 솔루션과의 위협별 대응기술의 상관관계를 고려하지 않은(즉, 각 정보보안 솔루션이 단독으로 적용되는 경우) j 위협에 대한 각각의 정보보안 솔루션의 공격우회율 값을 나타낸다. (그림 4)의 (b)는 선택된 10개의 정보보안 솔루션들의 위협별 대응기술의 상관관계를 고려한 것으로, 2개 이상의 원소를 갖는 Cluster가 2개 존재하는 예로서, j 위협에 대한 각각의 정보보안 솔루션의 공격우회율 최종값을 나타낸다.

r_{1j}	r_{2j}	r_{3j}	r_{4j}	r_{5j}	r_{6j}	r_{7j}	r_{8j}	r_{9j}	r_{10j}	r_{11j}	r_{12j}	r_{13j}	r_{14j}	r_{15j}
0.1	0.4	0.3	0.5	0.3	0.6	0.2	0.2	0.6	0.3	0.3	0.4	0.5	0.6	0.2

(a). j 위협의 각각의 보안 솔루션에 대한 공격우회율: 초기값

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}
1	0	1	1	1	0	1	0	1	0	1	0	1	1	1
r_{1j}		r_{3j}	r_{4j}	r_{5j}		r_{7j}		r_{9j}		r_{11j}		r_{13j}	r_{14j}	r_{15j}
0.1		0.3	0.5	0.3		0.2		0.6		0.3		0.5	0.6	0.2
j 위협에 대한 대응기술이 같거나 상호간에 종속 관계에 있는 2개 이상의 원소들 갖는 Cluster 존재: Cluster A(r_{3j}, r_{7j}), Cluster B(r_{13j}, r_{14j}, r_{15j})														
0.1		1	0.5	0.3		0.2		0.6		0.3		1	1	0.2

(b). j 위협의 각각의 보안 솔루션에 대한 공격우회율 : 최종값

(그림 4) 공격우회율 최종값 결정 방식

(그림 4)에서 공격우회율 최종값들이 결정되면 잔여 위험의 수치를 도출하는 모델링 식 (그림 3)에 적용하여 선택된 정보보안 솔루션 조합별 잔여 위험의 수치가 도출된다. 선택된 정보보안 솔루션 조합들에서 정형화된 여러 제한 요소들(한정된 투자 예산, 감내 가능한 총 잔여 위험, 정보보안 솔루션 후보들 간의 배타성, 정보보안 솔루션 후보의 구현의 절대적 필요성 등)을 만족시키는 조합들을 선별한 후 잔여 위험의 수치가 최소인 경우의 정보보안 솔루션 조합을 최적의 정보보안 솔루션 조합으로 최종 투자 의사결정을 내리게 되는 것이다. 제안 모델링 기법을 통해 산출된 최적해는 어떤 정보보안 솔루션을 구현할 것인가에 대한 정보와 총 구현비용, 정보보안 솔루션들의 가치를 총체적으로 설명해준다. 즉, 의사 결정에 필요한 각 정보보안 솔루션 조합에 관한 모든 정보들이 자동적으로 의사 결정자에게 제공되므로, 의사 결정자는 많은 전문 지식이 없어도 최적의 정보보안 솔루션을

용이하게 결정 할 수 있다.

4. 결 론

본 논문에서 제안한 정보보안 솔루션 결정 방법론은 추천된 정보보안 솔루션 후보들을 위험완화 효과 측면에서 정량적으로 평가하여 가장 효과적인 정보보안 솔루션 조합을 선별한다. 구체적으로 최적의 정보보안 투자 의사결정을 어렵게 하는 요소들을 고려함과 동시에 최적의 정보보안 솔루션을 선정하기 위하여 잔여 위험 수치를 판단 기준으로 활용하며, 특징적으로 정보보안 솔루션들의 같은 위협에 대한 대응기술 원리가 같거나 상호간에 종속관계에 있는 경우에 중복 적용을 피하게 하므로 잔여 위험 값의 정확도를 높인다. 향후 다량의 사례연구가 필요하며 추가적으로 적용 기관의 정보 시스템 네트워크 환경을 고려한 공격우회율 등의 값들의 객관성 확보를 위한 개선 연구가 요구되며, 시간에 따른 자산 가치 등의 변화를 반영한 모델링 연구가 요구된다.

참 고 문 헌

[1] 특허 10-2002-004531, 정보보안 위험 지수 시스템 및 그 방법, 이경호.

[2] 특허 10-2002-0045118, 실시간 정보보안 위험분석 시스템 및 그 방법, 이경호.

[3] 특허 10-2002-0045126, 실시간 정보보안 위험관리 시스템 및 그 방법, 이경호.

[4] Xiaomeng Su, “An Overview of Economic Approaches to Information Security Management”, Technical Report TR-CTIT-06-30 Centre for Telematics and Information Technology, University of Twente, Enschede, ISSN 1381-3625, August 2006.

[5] Wes Sonnenreich, Jason Albanese and Bruce Stout, “Return On Security Investment(ROSI)-A Practical Quantitative Model”, Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006.

[6] Wayne L. Winston, “Introduction To Mathematical Programming”, Operations Research : Volume One, Fourth Edition, TOMSON, 2003.

[7] Ashish Arora, Dennis Hall, C. Ariel Pinto, Dwayne Ramsey and Rahul Telang, “Measuring the Risk-Based Value of IT Security Solutions”, Published by the IEEE computer Society, November, December 2004.

[8] Ian Barland, Phokion G. Kolaitis, Madhukar N. Thakur, “Integer Programming as a Frame work for Optimization and Approximability”, IEEE, 1996.

[9] 특허 2008-0036667, 보안 대응책 결정 방법 및 장치, 김민식 외 4인.

김 민 식

2000년 한양대학교 전기공학과 (학사)
2003년 한양대학교 전자통신전파 공학과(석사)
2007년~현재 고려대학교 정보경영공학전문대학원 (박사과정)
2003년~현재 ETRI 부설연구소 근무

임 종 인

1980년 고려대학교 수학과
1982년 고려대학교 수학과 (석사)
1986년 고려대학교 수학과 (박사)
2000년 고려대학교 자연과학대학 정교수
현재 고려대학교 정보경영공학전문대학원
고려대학교 정보보호기술연구센터 센터장