TCO기반 Security ROI를 활용한 정보보호 투자성과 평가방법

이종선*, 이희조**
*고려대학교 컴퓨터정보통신대학원 소프트웨어공학과
**고려대학교 컴퓨터·통신공학부
{jslee0410, heejo}@korea.ac.kr

Evaluating Information Security Investment using TCO-based Security ROI

JongSun Lee*, HeeJo Lee**
*Graduate School of Computer and Information Technology, Korea University
**Dept of Computer Science & Engineering, Korea University

요 약

보안 취약성이 끊임없이 보고되고 있다. 이는 보안솔루션의 초기 효과수준을 유지하기 위해서는, 새로운 취약성이 보고되면 즉시 대처하는 지속적 관리활동이 필요함을 뜻한다. 한편 기업성과 개선을 위한 IT투자성과관리가 강조되는 가운데, 정보보호 솔루션 도입 시 재무적 타당성 증명이 요구되고 있다. 이를 위해 여러 형태의 ROSI(Security ROI)가 제시되었으나, 지속적 보호활동에 따른 관리비용이 중요하게 다루어져야 함에도 불구하고 비용에 대한 고려가 적고 효과산정에만 치우쳐, 경영자의 의사결정을 지원하는 실제적인 재무 성과지표로 활용될 수 없었다. 이에 본 논문은 조직수준의 비용효과 최적화를 추구하는 정보보호 관리체계에 기반을 두어 효과를 산정하고, 비용 산정은 지속적 관리활동이라는 특징을 반영하여 TCO에 기반을 둔 개선된 ROSI를 제안한다. 또한, 제안한 ROSI를 활용한 보안솔루션 평가사례를 제시한다. 증명이 어려운 정보보호 분야 투자타당성 증명은 물론 보안솔루션 선택 시 실제적인 의사결정 판단근거로서 활용될 수 있다.

1. 서론

보안 취약성이 끊임없이 보고되고 있다. 이는 정보보호 대책으로서 도입된 보안솔루션의 초기 효과수준을 유지하기 위해서는, 새로운 취약성이 보고되면 즉시 대처하는 지속적 관리활동이 필요함을 뜻한다[1]. 한편 기업성과 개선을 위한 IT투자성과관리가 강조되는 가운데, 정보보호 솔루션 도입 시 사전평가를 통한 재무적 타당성 증명이 요구되고 있다[2][3]. 이를 위해 지금까지 여러 형태의 ROSI(Security ROI)가 제시되었다[5][6][7]. 투자 의사결정의 근거가 되는 ROSI는 효과산정 및 비용산정 모두가 정확해야 한다. 그럼에도 지금까지의 ROSI는 효과의 증명만을 강조하고, 지속적 보호활동에 소요되는 관리비용을 비용산정에 고려하지 않아 정확성이 결여되었다. 부정확한 ROSI는 경영자의 합리적 의사결정을 지원하는 실제적 재무 성과지표로 활용될 수 없다. 이에 본 논문은 조직수준의 비용효과 최적화를 추구하는 정보보호 관리체계에 기반을 두어 효과를 산정하고, 비용 산정은 지속적 관리활동이라는 특징을 반영하여 TCO에 기반을 둔 개선된 ROSI를 제안한다. 증명이 어려운 정보보호 분야 투자타당성 증명은 물론 보안솔루션 선택 시 실제적인 의사결정 판단근거로서 제안된 ROSI를 활용할 수 있다.

2장에서는 논문의 배경을 설명하고, 3장에서는 효과요소 및 비용요소를 균형 있게 고려한 개선된 ROSI를 세부적으로 제안하며, 4장에서는 제안 ROSI를 활용한 보안솔루션 평가사례를 제시하고, 5장에서는 결론을 제시하였다.

2. 배경

2.1 IT 투자성과 관리

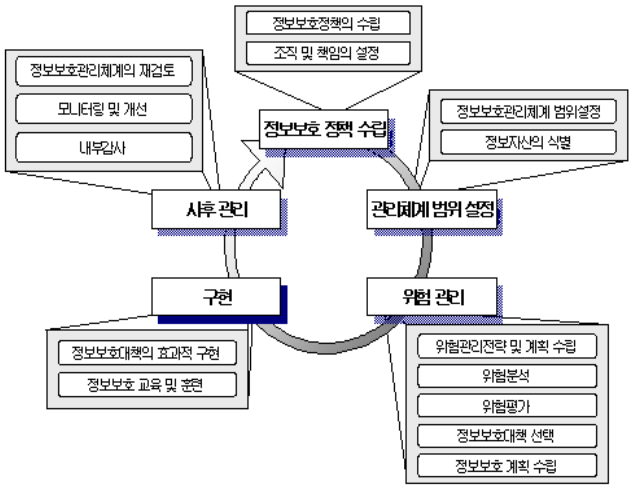
비즈니스 활동에서 IT의 중요성이 증가함에 따라, IT투자를 기업성과 개선에 직결시키려는 노력이 증대되고 있다. 기업성과는 비용절감 및 효과향상이 병행되어야 극대화될 수 있다.

$$\text{기업성과}(Performance) = \frac{\text{효과}(Benefits)}{\text{비용}(Costs)}$$

한정된 IT예산의 공정하고 투명한 최적화 분배를 목표로, 사전 성과평가를 실시하고 그 결과를 토대로 최대효과가 예상되는 부분에 정보화투자를 실시한다. 또한, 사후에도 지속적으로 성과를 평가하여 그 결과에 대한 책임을 규명한다[3].

2.2 정보보호 관리체계

조직 전체 차원에서 체계적으로 정보보호를 계획하고 대처한다면 관리비용을 크게 줄일 수 있다[4].



(그림 1) 정보보호 관리과정

정보보호 관리체계란 (그림 1)의 관리과정을 통해 조직의 자산을 효율적으로 보호할 수 있도록 기술적, 물리적, 관리적, 조직적인 다양한 보호 대책들을 구현하고 지속적으로 관리, 운영하는 종합적인 체계이다. 정보보호 관리체계 수립의 이점은

- 정보보호 목표수준의 지속적 유지 : 도입순간에만 효과가 있는 일회적 정보보호가 아닌 지속적 관리를 가능하게 한다.
- 정보보호 투자성과의 최적화 : 위험분석 및 위험평가를 기초로 효과와 비용간의 최적화 균형을 유지할 수 있다.
- 정보보호 관리지식의 축적과 프로세스 개선으로 장기적으로 피해를 줄일 수 있다[1].

2.3 ROSI (Security ROI)

정보보호 투자의 재무적 정당성을 증명하기 위한 성과지표로서, 정보보호 프로젝트 또는 보안 솔루션 후보들 간의 비용효과 분석을 위해 사용된다[2].

$$ROSI = \frac{Risk\ \ Exposure \times Risk\ \ Mitigated(\%)}{Cost} - 1$$

지금까지 다양한 Security ROI지표들이 제시되었다[5][6][7]. 그러나 정보보호 투자의 직접적인 효과증명이 어려운 특성 때문에 효과증명에 치우친 경향이 있다.

한편 끊임없는 취약점의 등장은 완벽한 보안대책은 존재하지 않으며, 지속적인 정보보호 관리활동이 필요함을 의미한다. 이를 ROI측면에서 바라보면 초기 효과수준 유지를 위해 관리활동이 필요하고, 그에 따른 비용이 지속적으로 소요됨을 의미하므로, 비용요소 산정에 노력하여 정확한 결과를 도출할 수 있다면 궁극적으로 실질적인 기업성과 개선에 도움이 된다. 이에 지속적인 정보보호 관리활동의 비용측면을 강화한 실질적인 ROSI를 제안한다.

3. 개선된 ROSI (Security ROI)

$$ROSI = \frac{\sum R(i) + \sum P(j)}{TCO} - 1$$

R : 위험감소 효과,
P : 관리생산성 효과,
TCO : 총소유비용

제안 하고자 하는 ROSI는 세 요소로 구성된다.

- 위험감소 효과 : 자산보호에서 얻을 수 있는 효과를 의미한다.
- 관리생산성 효과 : 정보보호 관리활동을 수행함에 있어, 솔루션이 가져다주는 생산성 향상 효과를 의미한다.
- TCO : Total Cost of Ownership. 도입 및 운용비용을 모두 고려한 총소유비용을 의미한다.

3.1 위험감소 효과산정

위험감소 효과산정은 3단계를 거친다.

▪ 1단계 : 위험분석 (Risk Analysis)

조직차원에서 체계적인 정보보호 활동을 유지하며, 목표수준에 적합한 투자비용 계획을 위해서는 위험분석이 선행되어야 한다. 보호대상으로서의 자산, 위협, 취약성에 대한 분석과정이며, 이 분석 결과를 바탕으로 위험규모의 평가가 실시된다.

<표 1> 위험분석과정

절차	내용
자산분석	자산(Asset) 식별
	자산 가치(Value) 산정
위협분석	자산 별 위협(Threat) 식별
	위협 별 발생가능성(likelihood) 파악
취약성 분석	자산 별 취약성(Vulnerability) 분석

▪ 2단계 : 위험평가(Risk Assesment)

위험분석 결과를 토대로 위험규모를 평가한다.

$$\text{위험} = A(i) \times T(j) \times V$$
A: 자산가치, T: 발생빈도, V: 취약성(%)

▪ 3단계 : 위험감소(Risk Mitigation) 효과산정

$$\text{위험감소효과} = \sum\{Min[\sum(R(i) \times M(j)), AV(i)]\}$$
R : 자산(i)의 위험
M : 위험의 감소율(%)
AV : 자산 $A(i)$의 가치

아래 <표 2>의 예에서, 보안대책 구현을 통하여 a1자산에 대하여 t1위협을 70%를 감소시켰으며, a2자산에 대하여 t1위협을 60%, t3위협을 50% 감소시켰다. 효과의 합은 자산 가치보다 클 수 없다. a2효과의 경우 효과의 합이 220이지만 자산 가치가 200이므로 200으로 산정한다.

<표 2> 위험감소 효과산정 예

자산	가치	위협	감소율	효과
a1	300	t1	0.7	210
		t2	-	-
a2	200	t1	0.6	120
		t2	-	
		t3	0.5	100
a3	400	t1	-	-
효과 합계				410

3.2 관리생산성 효과 산정

관리생산성 효과는 2단계를 거쳐 산정된다.

▪ 1단계 : 통제사항 활동검토

정보보호를 위해서는 관리적, 물리적, 기술적 통제활동이 필요하며, 이러한 종합적 활동을 통해 장기적인 관리비용을 절감할 수 있다. 다음은 정보보호 관리체계가 제시한 통제 분야이다[1].

<표 3> 정보보호 대책 분야

	통제 분야	통제사항 수
1	정보보호 정책	5
2	정보보호 조직	4
3	외부자 보안	4
4	정보자산 분류	4
5	정보보호 교육 및 훈련	4
6	인적 보안	5
7	물리적 보안	12
8	시스템개발 보안	13
9	암호 통제	3
10	접근 통제	14
11	운영 관리	23
12	전자거래 보안	5
13	보안사고 관리	7
14	검토, 모니터링 및 감사	11
15	업무연속성 관리	7
합계		120

통제사항을 선택하여 대책을 수립한다. 이 대책의 구현에는 구축비용과 운영비용이 소요되며, 정보보호 솔루션 도입 시 이러한 활동 수행의 비용절감 효과가 있다면 고려해야 한다.

▪ 2단계 : 관리생산성 효과산정

$$\text{관리생산성 효과} = \sum\{C\,before(i) - C\,after(i)\}$$
$C\,before$: 도입이전 활동비용,
$C\,after$: 도입이후 활동비용

보안 솔루션 도입이 관리활동의 생산성 개선을 주는 요인을 고려한다.

<표 4> 관리생산성 효과 산정 예

관리 활동	개선 내용	시간당 인건비	빈도 (년)	절감비용
장애분석	평균 60분에서 30분으로 개선	18만	12	108만
로그분석	평균 20분에서 10분으로 개선	18만	365	1,095만
효과 합계				1,203만

<표 4>에서 장애 상세분석 시 평균 60분이 소요되었으나, 도입이후 30분으로 단축되었다면, 연간 108

만원의 생산성 개선효과가 있는 것으로 산정한다.

3.3 비용(TCO) 산정

$$TCO = \sum\{\text{해당 계정항목}(i) \times \text{소요비용}(i)\}$$

<표 5> TCO 비용항목

비용구분		비용항목
직접 비용	H/W 비용	구입・폐기 비용
	S/W 비용	OS, 응용S/W, 유틸리티
	인건비	개발, N/W관리, 문제해결 및 수리, 트래픽관리 및 계획, 성능튜닝, 사용자 운영, OS지원, 유지보수비, 시스템관리, 평가 및 구매, S/W라이센싱 및 분배, 자산관리, 응용 관리, 보안 및 바이러스 예방, 하드웨어 설치, 구성/재구성, 저장장치 관리, 디스크 파일관리, 저장장치 용량계획, 백업 및 복구, 아웃소싱비, 교육과정개발, 정보시스템 교육, End-user
	운영비	유지보수 계약, 지원계약, 교육과정 및 인증비, 여행・출장비
	기타 비	임대자산비, 기타 월비용, 커뮤니케이션 비
간접 비용	최종사용자 정보시스템 비용	동료 및 최종사용자 지원, 자기학습, Futz Factor, End-user개발
	다운타임	계획된 다운타임, 돌발적인 다운타임, 헬프데스크 해결시간 동안의 다운타임

<표 5>는 솔루션 도입 및 운영 시 발생되는 비용을 회계 상의 비용계정항목 별로 구분한 것이다[3]. 해당 계정항목 별 비용이 발생할 것인지 여부를 조사하여 TCO를 산정한다.

4. 제안 ROSI를 활용한 평가 사례

4.1 벤더 간 IDS 솔루션 평가

제안한 ROSI 산정방법에 따라, 두 벤더의 IDS 솔루션을 비교 평가하였다. <표 6>은 평가결과표이며, 기간은 1년으로 한정하였다. 기존 ROSI 산정방법을 사용하여 초기 도입비용만을 고려한 결과 A제품의 성과가 우수한 것으로 나타났다. 그러나 제안한 ROSI 산정방법에 따라 생산성 개선효과 및 지속적 관리활동에 소요되는 인건비 및 기타 비용을 고려하여 재 산정한 결과, B제품의 ROSI가 높은 것으로 평가되었다. 결국 B제품을 도입해야 기업성과 개선에 도움이 된다는 결론을 얻을 수 있었다.

<표 6> 제안 ROSI를 이용한 평가결과

	A 제품	B 제품
위험경감 효과	15억	15억
초기 도입비용	3억	3.5억
기존 ROSI	400%	329%
관리생산성 효과	3천만	5천만
TCO	4.8억	4.5억
개선 ROSI	219%	244%

5. 결론

지속적 보호활동에 소요되는 관리비용을 비용에 반영함과 동시에 관리생산성 효과를 반영하여 실제적 투자 의사결정 지표로서 활용될 수 있도록 개선하였다. 본 논문이 제시한 ROSI를 활용하면 다음의 효과를 기대할 수 있다. 첫째, 일정수준의 정보보호 투자가 필요함에도 그 타당성을 증명하지 못하여 정보자산이 위험에 노출됨을 예방할 수 있다. 둘째, 보다 비용효율적인 보안솔루션을 선택할 수 있어 기업성과 개선에 실질적인 도움을 줄 수 있다.

참고문헌

[1] 한국정보보호진흥원, “정보보호관리체계 위험관리 가이드”, 2004

[2] Lawrence A. Gordon, Martin P. Loeb, "2006 CSI/FBI Computer Crime and Security Survey", p.8, 2006

[3] 구본재, 권민영, 김중식, "경영혁신을 위한 IT 거버넌스" 네모북스, pp.25-28, 2006

[4] Roberta Witty, William Malik, “Security TCO Model Helps With More Than Cost Savings”, Gartner Information Security Strategies, 2001

[5] Huaqiang Wei, Deb Frinke, Olivia Carter, Chris Ritter, “Cost-Benefit Analysis for Network Intrusion Detection Systems”, CSI 28th Annual Computer Security Conference, 2001

[6] Marco Cremonini, Patrizia Martini, “Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA)”, 4th Workshop on the Economics on Information Security, 2005

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