정보시스템의 체계적인 위험관리를 위한 실용적인 위험감소 방법론에 관한 연구

엄 정 호[†]·우 병 구[††]·김 인 중[†††]·정 태 명[††††]

요 약

본 논문에서는 정보시스템의 위험관리 과정에서 위험감소 단계를 구체적이고 체계적인 방법과 절차를 제시하여 최적의 대응책을 선택할 수 있도록 하였다. 본 논문에서 제시한 실용적인 위험감소 방법론은 기존의 위험감소 절차보다 좀 더 체계적으로 수행절차를 수립하였으며, 각 단계마다 수행해야 할 프로세스를 구체적으로 정의하여 어떤 위험관리 방법론에 적용하더라도 쉽게 사용할 수 있도록 하였다. 실용적인 위험감소 방법론은 기존의 대응책 평가, 대응책 방법 선택, 대응책 기술 선택, 위험수용 평가, 비용효과 분석 그리고 대응책 구현을 포함한 6단계로 수행된다. 실용적인 위험감소 방법론의 특징은 대응책 구현에 앞서 대응책 수립 방법과 그 방법에 따른 기술들을 식별된 위험의 특성에 맞게 대응책을 선택할 수 있다. 그리고 기존의 대응책 평가를 통해 기능이 우수한 것은 재사용함으로써 동일한 대응책을 구현하는 중복작업과 구현 비용의 낭비를 방지할 수 있다. 또한 최종 대응책을 결정할 때 최고경영자층의 의견을 반영하여 조직과 업무 특성에 맞게 조직이 요구하는 대응책을 선택할 수도 있게 하였다.

A Study on The Practical Risk Mitigation Methodology for Systematical Risk Management of Information System

Jung Ho Eom[†] · Byeong Koo Woo[††] · In Jung Kim[†††] · Tai M. Chung[††††]

ABSTRACT

In the paper, we can select the best safeguard as proposed the definite and systematical method and procedure on risk mitigation of risk management for information system. The practical risk mitigation methodology has a good fulfillment procedure and a definition to fulfill procedure on each phase. So, it is easy to fulfill and can apply to any risk management methodology. The practical risk mitigation is composed of 6 phases, which are the existing safeguard assessment, safeguard means selection, safeguard technique selection, risk admission assessment, cost-effective analysis and safeguard embodiment. The practical risk mitigation's advantages are as follow. Efficient selection of safeguards to apply to risk's features with safeguard's means and techniques before embodying safeguards. Prevention of redundant works and security budgets waste as re-using the existing excellent safeguards through the existing safeguard assessment. Reflection of organization's CEO opinions to require special safeguards for the most important information system.

키워드 : 위험관리(Risk management), 위험감소(Risk Mitigation), 위험분석(Risk Analysis), 비용효과 분석(Cost-effective Analysis)

1. 서 론

최근에 네트워크 및 인터넷의 발달로 조직의 업무형태가 정보시스템을 위주로 하는 정보화 업무 형태로 전환되고 있다. 특히, 대부분의 조직들이 중대한 업무와 중요정보를 정보시스템에서 수행하거나 저장해 두는 경우가 많아졌다. 이에 따라 의도적이거나 비의도적인 해킹, 정보 유출, 변조, 파괴, 사보티지 등 조직의 목표와 이익을 침해하거나 업무를 마비시키는 보안사고들이 증가하게 되었다. 따라서 조직들은 이러한 정보시스템에 대한 위협요소에 대처하기 위해 최우선적으로 조직에서 보유하고 있는 정보시스템에 대한 안전도를 평가하는데 관심을 갖게 되었다. 즉, 위험요소를 식별하고 분석하여 효과적이고 경제적인 보안대책을 수립하도록 하는 위험관리 방법론의 연구와 위험관리 도구 개발에 심혈을 기울이기 시작했다.

위험관리란 조직이 업무를 수행함에 있어서 관련 정보시스템들을 식별하고, 정보시스템들이 가지고 있는 고유의 약점인 취약점을 파악하고, 이런 취약점을 이용하여 위험을 발생시키는 위협요소들을 도출하며, 위험이 주는 잠재적 영향을 조사하여 효과적인 보안대책을 수립하는 활동이다. 위험관리 단계는 일반적으로 위험정도를 평가하는 위험평가, 위험정도를 수용위험 범위까지 줄이는 위험감소, 위험감소

† 준 회 원 : 대한민국 공군 장교 복무
†† 준 회 원 : 성균관대학교 대학원 전기전자 및 컴퓨터공학과
††† 정 회 원 : 성균관대학교 대학원 전기전자 및 컴퓨터공학과
†††† 종신회원 : 성균관대학교 정보통신부 교수
논문접수 : 2002년 11월 18일, 심사완료 : 2003년 3월 3일

까지의 절차를 재평가하여 대응책 수립이 적절한지를 평가하는 평가 단계로 구성되어 있다[1-3].

위험관리의 위험감소 단계는 위험수준이 높은 정보시스템에 대해서 적절한 대응책을 수립·적용하여 안전성을 확보하기 위한 단계이다. 본 논문에서는 체계적이면서 효율적으로 위험을 감소시킬 수 있도록 최적의 대응책을 선택할 수 있는 실용적인 위험감소 방법론을 제시할 것이다.

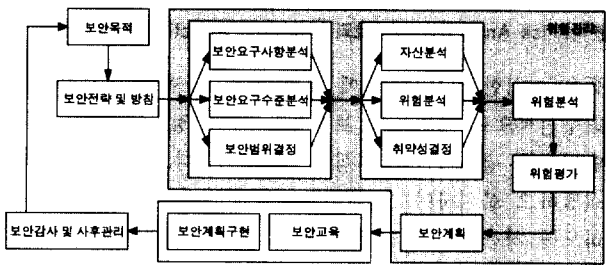
본 논문의 2장에서는 위험관리의 개념에 대해서 간략히 서술하며, 3장에서는 일반적인 위험감소 단계를 설명하고, 4장에서는 본 논문에서 제시하는 실용적인 위험감소 방법론을 제시한다. 마지막으로 결론을 맺는다.

2. 위험관리

2.1 위험관리의 개요

위험관리란 조직의 목표를 달성하기 위해 필요한 정보시스템 자원들에 대해 영향을 줄 수 있는 불확실한 사건들 즉, 위험요소를 식별, 평가, 그리고 최소화시키는 일련의 과정들을 말한다.

위험관리는 조직의 IT 관련 정보시스템 뿐만 아니라 환경적인 요소, 인적 요소 등 정보시스템을 운영하는데 필요한 모든 요소들에 대해서 위험으로부터 보호해야 한다. 또한, 어떠한 위험관리 방법이나 기술을 사용할지라도 보안대책을 선택하여 실행할 때 소비되는 시간과 자원들을 최소화하면서 동시에 모든 정보시스템과 관련된 요소들이 적절히 보호, 유지할 수 있도록 적절한 균형을 제공하는 것이 중요하다. 위험관리를 수행함으로써 조직과 정보자산에 해를 입힐 수 있는 위험을 측정할 수 있고 측정된 위험의 수준에 따라 효과적인 대응책 수립이 가능하며, 정보시스템 관리자들에게 정보시스템을 효율적으로 보호할 수 있는 자료들의 제공을 가능하게 한다[4, 7, 8, 10, 11].

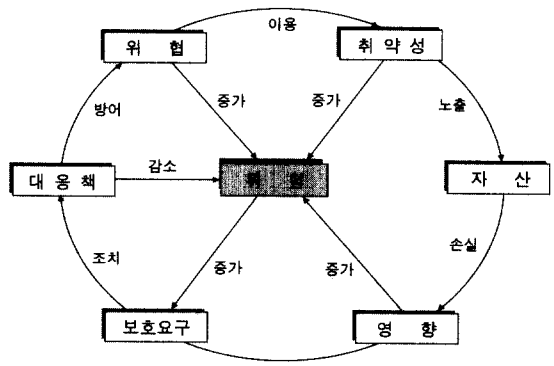


(그림 1) 위험관리의 일반모델

2.2 위험관리의 요소

위험관리 요소에는 자산, 위협, 취약성, 영향 및 위험이 있다[2-4, 8, 12].

- 자산 : 정보시스템을 비롯해서 정보시스템 운영과 관련된 모든 가치 있는 요소를 가르킨다. 본 논문에서는 IT 관련 자산 즉, 정보시스템 운영과 관련된 요소들에 한정하며, 하드웨어, 운영체제, 응용 소프트웨어, 네트워크, 데이터, 사용자, 환경적 요소 등이 있다.
- 취약성 : 조직, 하드웨어, 소프트웨어, 절차, 관리 등과 같은 자산이 잠재적으로 갖고 있는 약점이다, 취약성은 그 자체로서 손상을 초래하지는 않으며 단순히 위협이 자산에 영향을 줄 수 있는 조건만 제공한다.
- 위협 : 자산에 해를 줄 수 있는 위험의 원천이며, 위협을 통해서 정보시스템이나 서비스가 취급하는 정보의 분실 또는 접근 불가, 직/간접적으로 비인가된 파괴, 누설, 수정 등과 같은 결과를 초래한다.
- 영향 : 보안사고가 자산에 미치는 결과를 말하며, 결과는 특정 자산의 파괴, 기밀성/무결성/가용성의 상실, 또는 조직의 이미지 손상과 같은 간접적인 손실 등 모두 포함한다.
- 위험 : 특정 위협이 취약성을 이용하여 자산을 공격해서 손상을 초래할 수 있는 잠재력이다. 위험은 보통 위험발생 확률과 영향의 결합에 의해 결정지어질 수 있으며 자산의 가치와 위협수준에 의해 결정될 수도 있다.



(그림 2) 위험관리 요소간 상관관계

2.3 위험관리 절차

위험관리는 일반적으로 IT 관련 정보시스템의 위험을 평가하는 위험평가 단계, 위험평가에 따라 비용-효과적인 대응책을 제시하여 위험정도를 수용위험 범위까지 줄이는 위험감소 단계, 그리고 성공적인 위험관리 프로그램이 제대로 수행되고 있는지를 주기적으로 검사하고 평가 단계로 수행되어진다[5, 6, 9].

- 위험 평가 단계 : IT 관련 정보시스템을 운영하는데 필요한 모든 요소들에 관련된 잠재적인 위협을 식별하고, 위협을 통해 발생할 수 있는 위험을 분석하여 위험수준을 측정하는 활동을 말한다. 위험평가는 자산 식별, 위협 평가, 취약성 평가, 영향 평가 및 대응책 결정 등의 과정을 거친다. 그리고 위험수준 산출은 취약성수준, 위협수준, 위협발생 확률, 영향 및 자산의 가치를 고려하여 산출한다.

- 위험감소 단계 : 위험평가 단계에서 나온 결과를 토대로 적절한 대응책을 구현하고, 평가하고, 우선순위를 결정하여 위험을 수용범위 수준까지 감소시키는 활동을 말한다. 평가된 위험 모두를 감소시키거나 위험을 100% 감소시키는 것은 현실적으로 불가능하기 때문에 조직의 목표, 보안정책, 보안예산 등을 반영하여 수용범위 수준으로 위험을 감소시키도록 한다.
- 평가 단계 : 조직의 IT 관련 정보시스템 운영에 있어서 정보시스템의 확장, 변경, 갱신, 인력의 교체, 조직의 보안정책의 변경 등으로 나타날 수 있는 위험관리 프로세스 변경에 대해서 지속적으로 평가하고 수정해 나가는 일련의 활동을 말한다. 평가는 주기적으로 수행해야 하며, 평가를 통해서 식별된 변경사항에 대해서는 반드시 위험분석을 통해서 조직의 보안 목표와 정책에 맞게 위험관리 프로세스를 수정해야 한다.

〈표 1〉 위험관리 절차

위험평가 단계	위험감소 단계	평가 단계
• 자산 식별 • 위협 평가 • 취약성 평가 • 영향 평가 * 위험정도 결정	• 위험정도 우선 순위에 따른 대응책 목록 작성 • 비용효과 분석 • 적절한 대응책 설정 • 대응책 구현 계획 수립 및 실행 * 위험정도 우선 순위에 따른 최적의 대응책 실행	• 정보시스템들의 변경사항 식별 • 인력 변경 식별 • 보안정책 변경 확인 • 위험관리 프로세스의 수정 • 주기적인 평가 활동 수행 * 실용적이고 효율적인 위험관리 프로세스 유지

3. 일반적인 위험감소 방법

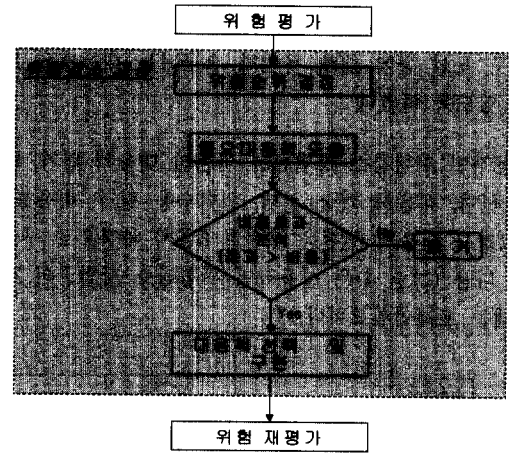
위험감소는 위험관리의 두 번째 단계로, 식별된 위험의 우선 순위에 따라 대응책을 수립하여 위험수준을 수용범위 수준까지 낮추는 활동을 말한다. 일반적인 위험감소 방법은 다음과 같은 절차를 따른다[9].

① 위험순위 결정 : 위험평가에 따른 결과를 바탕으로 자산의 위험수준이 높은 순으로 우선 순위를 결정한다. 위험수준의 우선 순위는 자산 또는 기타 항목별로 일정한 기준에 따라 우선 순위를 나타낸다.

② 필요 대응책 도출 : 위험평가를 통해서 식별된 대응책들이 위험요소에 대해서 모두 적절하거나 실행가능 한 것은 아니다. 그래서 이 단계에서는 식별된 대응책들을 우선순위의 위험요소에 대해서 위험수준을 최소화시킬 수 있는 가장 적절한 대응책들을 도출하는 것이다.

③ 비용효과 분석 : 위험을 감소시키기 위하여 필요한 대응책들의 수행여부를 비용적인 측면에서 고려하여 판단하는 분석과정을 말한다.

④ 대응책 선택 및 구현 : 비용효과 분석을 통해서 선택된 대응책들 중에서 위험수준을 수용가능한 수준까지 낮출 수 있는 대응책을 선택하여 구현하는 단계이다.



(그림 3) 일반적인 위험감소 절차

4. 실용적인 위험감소 방법론

4.1 실용적인 위험감소 방법론 개념

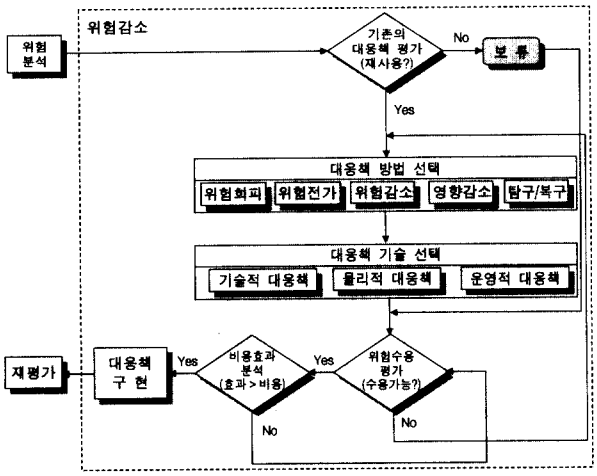
본 논문에서 제시하는 위험감소 방법론은 기존의 위험관리에서 사용하고 있는 위험감소 방법보다 좀 더 체계적인 프레임워크로 설계되었고, 위험감소 방법론의 전 과정에 구체적인 절차를 제시하였다. 또한 각 과정별로 업무를 수월하게 수행할 수 있도록 판단 기준과 평가 공식을 수립하였다. 실용적인 위험감소 방법론이 다른 위험감소 방법과 비교하면 다음과 같은 특징을 갖는다.

- 폭넓은 적용성 : 위험감소 단계의 절차를 체계적으로 제시하여 어떠한 위험관리 방법론에도 적용하여 사용할 수 있다.
- 사용 용이성 : 위험감소 단계의 모든 과정의 수행방법이 구체적이고 세부적으로 설명되어 있어서 위험관리 관리자가 사용하기가 용이하다.
- 위험요소에 적합한 최적의 대응책 도출 가능 : 위험평가를 통해 얻은 위험요소의 특성에 따라 대응책의 방법을 선택하고, 그 방법에 맞는 기술을 구현하여 최적의 대응책을 도출할 수 있도록 하였다. 또한, 위험수용 분석 및 비용효과 분석을 통해서 수용위험 범위를 만족시키면서 대응책 실행 비용이 적은 대응책을 선택할 수 있다.
- 중복 작업 및 예산 낭비의 방지 : 기존의 수행하던 대응책을 평가하여 대응책 기능이 우수한 것은 대응책 수립 과정에서 새로운 위험요소에 대한 대응책 선택시 재사용할 수 있도록 한다. 하나의 대응책이 여러 위험요소에 대한 보호대책으로 사용이 가능하기 때문에 새로운 위험요소일지라도 기존의 대응책으로 대체 가능할 수 있으므

로 동일한 대응책을 다시 구현하는 중복 작업과 구현 비용을 낭비하는 것을 방지할 수 있다.

- 조직이 요구하는 대응책 선택 가능 : 최종 대응책 결정시 최고경영자층의 의견을 반영하여 조직의 특성, 조직의 기밀정보 및 대외 비밀업무 등을 다루는 정보시스템의 업무 특성 등에 대해 특별히 요구되는 대응책을 결정할 수 있도록 하였다.

실용적인 위험감소 방법론은 기존의 대응책 평가, 대응책 방법 선택, 대응책 기술 선택, 위험수용 평가, 비용효과 분석, 그리고 대응책 구현을 포함한 6단계 과정으로 구성되어 있다. 다음 (그림 4)은 실용적인 위험감소 방법론의 절차를 나타내는 프레임워크이다.



(그림 4) 실용적인 위험분석 방법론의 프레임워크

4.2 실용적인 위험감소 방법론 절차

4.2.1 기존의 대응책 평가

기존의 대응책 평가는 IT 관련 정보시스템에 대한 위험관리를 시작한 시점 이전에 수립해서 실행되고 있는 대응책들이 식별된 위험에 대해서 효과적이면서 타당하게 적용되고 있는지를 평가하는 과정이다. 또한 위험요소에 대해 효율적으로 적용되고 있는 대응책에 대해서 대응책 수립과정에서 선택, 구현, 실행 등의 불필요한 작업을 예방하기 위한 활동이기도 하다.

기존의 대응책 평가는 대응책 평가 방법과 위험 감소율을 이용하여 평가한다.

- 대응책 평가 : 적합성, 타당성 및 대응책 기능을 기준으로 수행한다.
  - 적합성 평가 : 식별된 모든 대응책들이 자산의 취약성 및 위협 요소에 상응하게 제대로 적용하여 실행되고 있는지를 평가한다.
  - 타당성 평가 : 취약성 및 위협 요소에 적합하게 적용되었을지라도 대응책이 중복되어 적용되어 있지 않은지, 낮은 취약성 및 위협요소에 고가의 대응책 또는 높은 취약성 및 위협요소에 낮은 수준의 대응책이 적용되고 있지 않은지 등을 평가한다.
  - 대응책 기능 평가 : 대응책들이 취약성 및 위협 요소에 적합하게 적용되고 타당할지라도 대응책 자체 능력에 미치지 못하도록 구현되었는지, 또는 그 기능 및 운영이 제대로 실행하여 대응책 자체의 기능이 충분히 유지하는지 판단한다. 다시 말해서 대응책 수준 평가는 대응책 자체의 기능을 평가하는 것이다.

다음 <표 2>는 대응책 평가 방법 기준을 나타낸다.

〈표 2〉 대응책 평가 방법 기준

평가 수준	등급	기 준
Very low	1	자산의 취약성, 위협요소에 대한 대응책이 전혀 제 기능을 수행하지 못함
Low	2	자산의 취약성, 위협요소에 대한 대응책이 어느 정도 관련은 있으나, 다른 위협요소에 대한 대응책으로도 수용위험 범위까지 위험 감소가 가능하고 대응책 자체 기능을 완전하게 수행하지 못함
Medium	3	자산의 취약성, 위협요소에 대한 대응책이 적합하게 적용되었으나, 위험감소 효과가 떨어지고 구현된 대응책 기능과 운영이 미흡함
High	4	자산의 취약성, 위협요소에 대한 대응책이 적합하게 적용되었고, 그 위협요소에 대한 위험 감소율은 만족하며, 대응책 자체 기능 및 운영도 정상적으로 수행함
Very high	5	자산의 취약성, 위협요소에 대한 대응책이 최적으로 선택되었고, 이외의 위협요소까지도 위험을 감소시킬 수 있으며, 대응책 구현도 완벽하고 오류없이 그 기능을 수행함

- 위험감소율 : 기존의 대응책에 대한 위험감소율은 이전의 위험관리 수행 자료를 바탕으로 하여 5등급으로 평가한다. 대응책이 적용되어 위험이 감소되는 비율은 대응책을 구현할 때 모두 기록해 둔다.

다음 <표 3>은 기존의 대응책 분석 방법을 나타낸다.

〈표 3〉 기존의 대응책 평가 방법

위험 \ 대응책	대응책 종류	대응책 평가		대응책 순위
		대응책 기능	위험 감소율	
위험 1	대응책 1			
	⋮			
	대응책 N			
⋮	대응책 1			
	⋮			
	대응책 N			
위험 N	대응책 1			
	⋮			
	대응책 N			

만약 기존의 대응책이 적절치 못할 경우에는 바로 폐기하는 것이 아니라 일단 보류해 둔다. 그것은 위험평가 단계에서 새롭게 식별된 위험요소에 적용될 가능성이 있기 때문에 재사용이 가능하다.

4.2.2 대응책 방법 선택

위험평가를 통해 식별된 위험요소에 대해서 효과적으로 위험수준을 줄일 수 있는 보호대책 방법을 선택하기 위한 활동이다. 위험요소에 대한 대응책 방법에는 위험 회피, 위험 전가, 위협 감소, 영향 감소, 위험요소 탐지/복구 등이 있으며, 대응책 방법을 복합적으로 사용할 수도 있다. 최적의 대응책 방법은 위험 회피, 위협 감소, 영향 감소 방법이며, 위험발생 이후에 사후조치로는 탐지/복구 방법이 유용하다. 자산의 위험요소에 대한 최적의 대응책 방법을 선택하기 위해서는 조직 및 정보시스템의 특성과 비용을 반드시 고려해야 한다. 조직의 특성에는 조직의 목표, 업무특성, 예산 및 보안정책 등이 있으며, 정보시스템의 특성에는 업무 의존도, 사용용도, 사용자 등을 고려해야 한다. 비용에 대해서는 비용효과 분석에서 자세히 설명할 것이다.

4.2.3 대응책 기술 선택

위험요소의 위험수준을 줄이면서 효과성을 극대화하기 위한 대응책을 구현하는 기술을 선택하는 과정이다. 대응책들이 적절하게 구현되어야만 식별된 위험요소를 회피, 감소, 탐지, 차단, 제한 등 할 수 있다. 대응책 기술에는 기술적, 물리적, 운영적 대응 기술이 있으며, 복합적으로 사용하여 그 효과를 높일 수도 있다. 대응책 기술을 선택해서 사용할 때는 대응책 사용의 용이성, 사용자에 대한 투명성, 대응책 기능의 수행 능력, 대응책 방법의 종류, 대응책의 내구성 등을 고려해야 한다. 다음은 대응책 기술의 종류이다.

- 기술적 대응책 : 위협요소에 의해서 손상을 입을 수 있는 통신, 소프트웨어, 하드웨어 등 IT 관련 정보시스템 기능 등을 보호하기 위해 구현하는 대응책이다. 세부적인 방법으로는 인증, 접근제어, 침입탐지 기술 등이 있다.
- 물리적 대응책 : 기술적, 운영적 대응책과 같이 혼합하여 이용되는 기술로써, 외적(물리적) 요인에 의한 위험의 손실을 줄이고 조직의 임무를 보호하고 관리하는 대응책이다. 세부적인 방법으로는 잠금장치 설치, 화재경보 시스템, 차폐벽 등이 있다.
- 운영적 대응책 : 조직의 목적과 임무에 맞게 보안 절차, 가이드라인 등을 수립하여 운영측면의 대응책이다. 세부적인 방법으로는 사고대응 처리절차, 보안규칙 수립, 보안 절차 수립 등이 있다.

다음 <표 4>는 대응책 방법과 대응책 기술에 따른 대응책 종류를 나타낸다.

〈표 4〉 대응책 방법과 기술의 관계

대응책 방법	대응책 기술	세부 기술
위험 회피	기술적	패스워드, IC 카드 등
	물리적	차폐벽, 접근 통제 등
	운영적	보안교육 등
위험 전가	운영적	보험 등
위협 감소	기술적	특권 통제, 침입 탐지 등
	물리적	자료 매체 접근 통제 등
	운영적	사고처리 절차 훈련 등
영향 감소	기술적	바이러스 복구, 백업 등
	물리적	소화기 등
	운영적	사고처리 절차 숙달 등
탐지 / 복구	기술적	침입탐지, 바이러스 제거 등
	물리적	화재경보 등
	운영적	주기적인 위험평가 수행 등

4.2.4 위험수용 평가

조직이 각 항목별 자산에 손실을 입히는 위험에 대해서 조직의 보안목표, 보안정책, 보안전략을 기반으로 조직의 목표, 업무 프로세스에 손실을 입히지 않는 범위내로 위험수준을 감소시킬 수 있는 대응책을 선택하는 과정이다. 수용위험 수준은 위험분석 초기에 구성된 위험분석팀이 조직의 특성, 보안정책 및 업무목표를 고려하여 자산의 가치, 위협 및 취약성 수준을 바탕으로 각 정보시스템 구성요소에 맞게 결정한다. 어떠한 대응책을 수립하여 적용할지라도 위험이 100% 감소되지 않기 때문에 조직의 목표와 업무 프로세스에 지장을 초래하지 않는 범위내에서 위험수용 범위를 설정해야 한다. <표 5>는 수용위험 범위를 결정할 때 기준의 예를 나타낸다.

〈표 5〉 수용위험 범위 결정 기준의 예

수용위험 범위 기준
자산 가치가 상당히 높거나 위협이 발생할 경우 조직의 업무수행에 큰 손실을 발생시키는 위협요소를 지닌 정보시스템에 대한 수용위험 범위
자산 가치가 높은 편이며, 조직의 업무수행을 정지시키는 위협요소를 지닌 정보시스템에 대한 수용위험 범위
자산 가치는 그다지 높지 않으나, 위협 발생 확률이 높고, 위협이 발생할 경우 업무수행을 중지시켜야 하는 정보시스템에 대한 수용위험 범위

위험수용 범위가 결정되면, 위험수용 범위내로 만족시키는 대응책들을 선택한다. 이 과정에서 대응책을 선택할 때에는 위험수용 범위를 만족시키는 모든 대응책들을 도출하여야 한다. 그것은 위험수용 범위를 만족시킬지라도 비용효과 분석에서 비용측면을 만족시키지 못하는 대응책이 있을 수 있기 때문이다.

4.2.5 비용효과 분석

비용효과 분석은 위험평가, 대응책 수립 과정 및 위험수용 평가를 수행한 후 위험을 감소시키기 위하여 대응책을 결정

하는 과정에서 비용측면에서 효율성을 분석하는 과정이다. 즉, 조직의 보안 예산과 위험수용 범위를 고려하여 제안된 대응책이 위험을 감소시키는 데 소비되는 비용과 위험을 방치했을 경우 손해를 보는 비용을 비교하여 수용 위험범위를 만족시키면서 최소의 비용이 드는 대응책을 선택하기 위한 분석 과정이다. 본 논문에서는 비용효과 분석을 수행할 때 초기 투자비용, 오류감소에 따른 절약비용, 운영비용 등을 가지고 이익 및 투자수익률을 계산하여 평가한다[1, 13].

위험요소에 대해 수립되고 위험수용 범위를 만족시키는 대응책들을 확인하고 대응책 설치비용, 즉 투자비용을 산출한다. 그리고 대응책을 설치, 운영함으로써 발생하는 이익을 산출한다. 마지막으로 투자수익률을 계산하여 효율성을 평가하여 조직의 목표 이익에 부합되는 최적의 대응책을 선택하도록 한다.

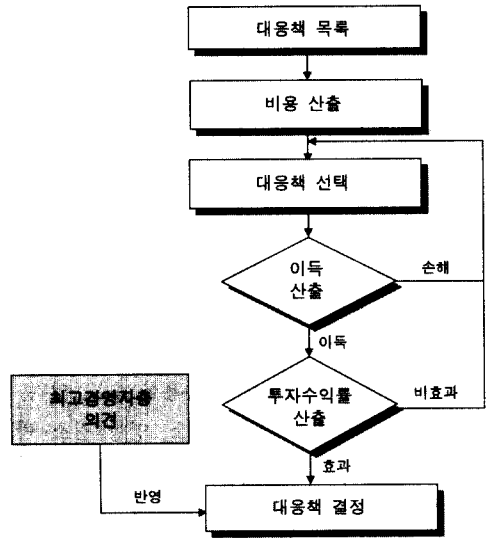
다음은 비용효과 분석을 수행할 때 고려해야 할 사항이다.

- 대응책간 상호보완성 : 어떤 한 대응책이 여러 가지의 위험요소에 적용될 수 있는데, 이런 위험요소를 개별적으로 분리하여 대응책을 수립하지 않는다. 또한 몇몇 대응책이 조합하여 어떤 위험요소에 적용될 때 뜻하지 않은 또 다른 효과를 볼 수 있다. 즉, 또 다른 위험요소에 적용될 대응책 비용을 줄일 수 있다는 것이다.
- 한가지 위험요소에 여러 가지 대응책 적용 : 한가지의 위험요소의 위험을 감소시키기 위하여 여러 가지의 대응책이 조합되어 적용되는데, 그 조합되는 여러 가지 대응책들 중 최적의 대응책을 선택해야 한다.
- 전체적인 정보시스템의 성능 저하 : 여러 가지의 대응책 설치로 인해 정보시스템 자체의 성능을 저하시킬 수 있으므로 기존의 대응책과 새로운 대응책의 보완성을 고려하고 새로운 대응책의 복잡성, 상호보완성, 사용 용이성 등을 고려하여 최상의 효과를 볼 수 있는 대응책을 선택하도록 한다.
- 대응책간 배타성 : 어떤 위험요소에 몇 가지 대응책에 대해 상호간 기능을 수행하는 수준의 정도를 구별할 수 있는 실제의 이익을 산출할 수는 없다. 즉, 기능면에서 우선순위를 정할 수 없을 때는 비용효과를 반영하여 선택하도록 한다.

다음 (그림 5)은 비용효과 분석 절차를 나타낸다.

① 대응책 목록 확인
대응책 수립 과정인 기술 및 방법 선택과정에서 제안된 대응책 목록을 확인한다.

② 비용 산출
제안된 각 대응책에 대한 비용을 산출한다. 비용을 산출할 때는 초기 투자비용과 운영비용을 모두 포함한다. 초기 투자비용은 대응책을 처음으로 설치할 때 드는 비용으로 프로그램 개발비용, 장비 구입비용 등이 있으며, 운영비용은 대응책 설치후 지속적으로 유지하기 위한 비용으로 인건비, 소모품비, 성능향상 비용 등이 있다.



(그림 5) 비용효과 분석 절차

③ 대응책 선택
최저의 비용이 드는 대응책을 선택한다. 만약, 동일한 비용이 드는 대응책일 경우에는 위험감소율이 높은 것을 선택하도록 한다. 위험감소율까지 동일하다면, 대응책의 설치 용이성, 사용 편리성, 대책의 유형 등을 고려하여 선택하도록 한다.

④ 이익 산출
대응책을 선택하여 설치하였을 경우, 그 대응책으로 인해 발생할 이익을 계산하는 것이다. 즉, 대응책을 수행하지 않아 발생한 손해와 대응책을 설치하여 운영하였을 때 드는 비용을 비교하여 분석하는 것이다. 동일한 대응책이라고 할지라도 이익이 높은 것을 선택하도록 한다. 예를 들어, 어떤 정보시스템의 대응책 미설치로 연간 손실액이 5,000,000원이고, 수용위험까지 위험수준을 낮추는데 두 가지의 A, B 대응책중 A는 연간 운영비용이 4,000,000원이고 B는 3,000,000원이라면, B의 대응책을 선택하는 것이다.

⑤ 투자수익률 산출
제안된 대응책에 대한 비용효율을 분석하고 위험을 감소시키기 위한 비용이 이익을 가져다 줄 것인가를 평가하는 것이다. 본 논문에서는 투자수익률을 가지고 분석한다. 투자수익률(Investment Return Rate)은 초기 투자비용, 연간 운영비용, 오류감소에 따른 절약비용을 가지고 산출한다.

- 투자 수익률 계산 방법

$$\text{투자 수익률(IR)} = (\text{오류감소 비용} - \text{연간운영 비용}) / \text{초기투자 비용} * 100$$

즉, 투자수익률은 연간 순수이익을 초기 투자비용으로 나눠서 백분율로 환산한 것이다.

투자 수익률(IR) = 연간순 수익 / 초기투자 비용 * 100

⑥ 대응책 결정

위험수용 범위를 만족시키고 이익, 투자수익률이 높은 대응책을 결정할 수 있도록 한다. 대응책을 결정할 때 간과하지 말아야할 요소중에 하나가 조직의 최고 경영자층의 결정이다. 위험관리를 수행하는 관리자들이 위험감소 방법에 의해 선택된 대응책일지라도 최고 경영자층은 조직의 보안정책, 기밀정보 및 대외 비밀 업무 등을 다루는 정보시스템에 대해 비용에 상관없이 최저의 수용위험 범위를 갖고 최대의 기능을 갖은 대응책을 선택할 수도 있기 때문이다. 그래서 실용적인 위험감소 방법론에서 대응책을 결정할 때는 최고 경영자층의 의견을 반영하도록 하였다.

4.2.6 대응책 구현

결정된 대응책들이 대응책의 방법과 기술에 따라 실제 형태로 변환시키는 과정으로 이 과정을 통해 대응책의 기능이 수행 가능하게 된다.

5. 결 론

본 논문에서는 위험감소 단계를 좀 더 체계적이고 구체적으로 절차와 방법을 수립하여 실용적으로 활용할 수 있는 위험감소 방법론을 제시하였다. 기존의 대응책 분석을 통하여 재사용이 가능한 대응책을 식별하여 위험요소에 대한 똑같은 대응책을 구현하지 않도록 중복작업 및 보안 예산의 낭비를 방지할 수 있다. 그리고 식별된 위험요소에 대해서 적절히 대응할 수 있는 대응책의 선택 방법과 그에 따른 기술을 제시하여 위험요소에 가장 적합한 대응책을 선택하도록 하였다. 위험수용 평가는 대응책 수립과정에서 선택된 대응책들의 위험감소률을 분석하여 수용가능한 위험범위를 만족시키는 대응책들만 선택하도록 하였다. 이 과정에서는 한 위험요소에 대한 수용위험 범위를 만족시키는 대응책들을 모두 선택하도록 한다. 그것은 위험수용 범위를 가장 낮게 만족시킨 대응책이 비용측면에서도 가장 낮을 수 있는 것은 아니기 때문이다. 그리고 이익산출, 투자수익률 공식을 적용한 비용효과 분석을 통해서 조직의 보안예산 안에서 최적의 대응책을 수립, 구현할 수 있게 하였다. 또한, 최고경영자층의 의견을 반영하여 조직의 보안정책에 따라 보안예산 내에서 조직의 정보시스템 특성에 맞는 보안대책을 선택할 수 있도록 하였다.

본 논문이 제시한 실용적인 위험감소 방법론은 기존의 체계성 및 효율성을 높이고 최적의 대응책을 선택하도록 유도하였다. 또한 실용적인 위험감소 방법론이 다른 위험관리 방법에서 사용한 위험감소 분야보다 구체적인 절차와 방법을 제시하여 어떤 위험관리 방법론에 적용하더라도 쉽게 사용할 수 있고 전체적인 프로세스의 성능을 향상시킬 수 있도록 하였다.

그러나 정확성과 체계성을 강조함에 따라 절차상의 복잡성을 노출하였다. 이로 인해 대규모의 정보시스템 환경에서 위험관리를 수행하는 과정중에 위험감소 단계의 수행기간이 늘어날 수 있는 단점이 있다. 이 분야에 대해서는 앞으로 지속적인 연구가 요구된다.

참 고 문 헌

[1] "국가기간 전산망 표준화 연구중 전산망 보안을 위한 위험관리 지침서", 한국전산원, 1994.

[2] "Risk Analysis and Management Standards for Public Information Systems Security- Concepts and Models," 한국정보통신기술협회(TTA), 1998.

[3] "Risk Analysis and Management Standards for Public Information Systems Security-Risk Analysis Methodology Model," 한국정보통신기술협회(TTA), 2000.

[4] 엄정호 외 다수, "정보시스템의 위험관리 과정 중에서 체계적이고 효율적인 위험감소 방법론 제기", WISC 2002, pp.805-813, Sept., 2002.

[5] "A Guide to Security Risk Management for Information Technology Systems," MG-2, CSE Manual, 1996.

[6] "A guide to Risk Assessment and Safeguard Selection for Information Technology," MG-2, CSE Manual, 1996.

[7] B. D. Jenkins, "Security Risk Analysis and management," Countermeasures, Inc., 1998.

[8] "Information Technology-Security techniques-Guidelines for the management of IT security," ISO/IEC JTC 1/SC 27, 1997.

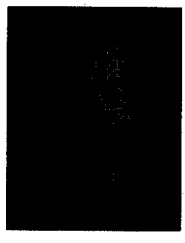
[9] Gary Stonebumer, Alice Goguen, and Alexis Feringa "Risk Management Guide For Information Technology Systems," NIST, Oct., 2001.

[10] Ginzberg, M. J. and Moulton, R. T., "Information technology risk management," 'Next Decade in Information Technology,' Proceedings of the 5th Jerusalem Conference, pp.602-608, 1990.

[11] Harold F. Tipton and Micki Krause, "Information Security Management Volume 3," 4th Edition, Auerbach Publications, pp.417-430, 2002.

[12] "BS 7799-Guide to Risk Assessment and Risk management," BSI, 1998.

[13] Jung Ho Eom, Sang Hoon Lee and Tai M. Chung, "A study on the Simplified Cost-Benefit Analysis to Select Safeguards against Risks in the Risk Management," SAM 2002, pp.292-297, June, 2002.



엄 정 호

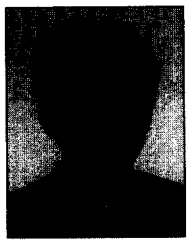
e-mail : jheom@rtlab.skku.ac.kr

1994년 공군사관학교 항공공학과(학사)

2003년 성균관대학교 정보공학과(공학석사)

1994년~현재 대한민국 공군 장교 복무

관심분야 : 인터넷 정보보호, 정보시스템의 위험관리 등



우 병 구

e-mail : bkwoo@rtlab.skku.ac.kr
2000년~현재 성균관대학교 전기전자 및 컴퓨터공학과 박사과정
관심분야 : 위험관리, 취약성분석

김 인 중

e-mail : cipher@etri.re.kr
1990년 충남대학교 전자공학과 학사
1992년 충남대학교 전자공학과(석사)
1992년 국방과학연구소 선임연구원
2000년 국가보안기술연구소 전임연구원 (교육기관 침해사고대응팀 운영 과제책임자)
2001년 성균관대학교 전기전자 및 컴퓨터공학과 박사과정
관심분야 : 위험분석, 취약성분석, 정보보호

정 태 명

e-mail : tmchung@ece.skku.ac.kr
1981년 연세대학교 전기공학과 학사
1984년 University of Illinois Chicago IL, U.S.A 전자계산학과 학사
1987년 University of Illinois Chicago IL, U.S.A 전자계산학과 석사
1995년 Purdue University W. Lafayette, IN, U.S.A 컴퓨터공학과 박사
1985년~1987년 Waldner and Co. System Engineer
1987년~1990년 Bolt Bernek and Newman Labs. Staff Scientis
1995년~현재 성균관대학교 정보통신부 부교수
관심분야 : 위험 관리, 액티브 네트워크, 침입 탐지 시스템, VPN, 네트워크 관리, 통합 보안관리 등