韓國IT서비스學會誌
第7卷 第1號
2008年 3月

정보보호를 위한 다속성 위협지수 : 시뮬레이션과 AHP 접근방법

이강수* · 김기윤** · 나관식***

Multi-Attribute Threat Index for Information Security : Simulation and AHP Approach

Kang-Soo Lee* · Ki-Yoon Kim** · Kwan-Sik Na***

■ Abstract ■

Multi-attribute risk assessments provide a useful framework for systematic quantitative risk assessment that the security manager can use to prioritize security requirements and threats. In the first step, the security managers identify the four significant outcome attributes(lost revenue, lost productivity, lost customer, and recovery cost). Next, the security manager estimates the frequency and severity(three points estimates for outcome attribute values) for each threat and rank the outcome attributes according to AHP(Analytic Hierarchy Process). Finally, we generate the threat index by using multi-attribute function and make sensitivity analysis with simulation package(Crystal Ball). In this paper, we show how multi-attribute risk analysis techniques from the field of security risk management can be used by security managers to prioritize their organization's threats and their security requirements, eventually they can derive threat index. This threat index can help security managers to decide whether their security investment is consistent with the expected risks. In addition, sensitivity analysis allows the security manager to explore the estimates to understand how they affect the selection.

Keyword : Information Security, Multi-Attribute Threat Index, Simulation

* (주)드림와이즈 팀장
** 광운대학교 경영학과 교수, 본 연구는 2007년도 광운대학교 교내학술연구비 지원에 의해 이루어졌음.
*** 서원대학교 경영정보학과 교수, 교신저자

1. 서 론

컴퓨터와 통신의 결합체인 정보기술의 발달로 인해 오늘날 우리는 풍요로운 정보화 시대에서 생활하고 있다. 하지만 정보화가 진행될수록 정보의 남용 및 악용과 같은 역기능이나 컴퓨터 범죄 등으로부터 정보보호의 필요성이 증대되고 있으며, 정보시스템의 환경이 하드웨어 중심에서 사용자 및 응용프로그램 중심으로 이행함에 따라 정보시스템 보안 위험관리의 중요성도 더욱 커지고 있다.

정보시스템 보안 위험관리를 위해서는 무엇보다도 먼저 합리적인 도구에 의한 위험평가가 이루어져야 한다. 일반적으로 정보시스템은 위험의 발생 가능성이나 발생 손실이 매우 불확실하며 위협에 대해서 여러 속성들을 평가해야 하는 다속성 의사결정문제 이므로, 단일속성의 평가를 기반으로 하는 전통적인 위험평가방법들은 적용할 수가 없다. 이에 비해서 다수의 위협으로 인한 위험을 평가할 수 있는 다속성 위험평가는, 보안관리자가 조직 내의 다양한 보안위협을 파악할 수 있고, 위협으로부터 발생 가능한 잠재적 손실들을 추정할 수 있다는 것과, 위협에 대한 보안대책들의 상대적 중요성을 파악할 수 있는 통찰력을 제공해 준다는 등의 장점이 있다[1].

정보보안 위험분석에 관한 연구는 정보시스템과 정보시스템의 보안정책에 대한 폭넓은 접근을 필요로 하며, 이는 보안관리자의 보안정책에 대한 전문가적 의견 수렴을 통해서 이루어진다. 이에 따라 본 연구에서는 정보시스템의 위험을 효과적으로 평가하기위해서 다음과 같은 절차에 의해 연구문제에 접근하고자 한다. 첫째, 분석대상 기업의 인터넷 침해사고와 관련한 위협을 도출하고, 그 빈도를 측정한다. 둘째, 보안관리자와의 인터뷰를 통해 위협에 따른 위험속성을 파악하여 모형이 요구하는 가정을 검토하고, 손실의 크기 및 위험속성별 가중치를 측정한다. 셋째, 이들 측정값들에 다속성 위험평가 모형을 적용하여 위협지수를 도출하고, 감도분석을 통해 어떤 위협들이 위협지수에 큰 영향을 미치는지를 분석한다. 넷째, 시뮬레이션 기법을 이용하여 위협지수의 변화량에 대한 감도분석을 실시한다.

따라서 본 논문의 연구목적은 구체적으로 다음과 같이 요약될 수 있다. 첫째, 다속성 함수와 시뮬레이션을 이용한 다속성 위험평가모형에 의해 정보시스템의 위험을 평가하는 새로운 기법을 제안한다. 둘째, 사례기업의 위험분석결과를 토대로, 정보시스템의 위험분석을 위한 실무적 적용절차를 제공한다.

2. 기존 연구

다속성 위험평가는 위협과 보안요구사항의 집합을 순위화해서 계량적으로 위험을 평가하는 도구인데, 보안관리자가 조직 내의 위험을 파악해서 위협으로 인한 손실을 예상할 수 있게 해준다는 것이 장점으로 알려져 있다[7]. 이를 이용한 구체적인 위험평가절차는 일반적으로 다음과 같다[1, 8].

- 위협으로 인해 발생되는 위험결과 속성들을 식별한 후에, 속성에 대한 가산성을 검토한다.
- 각 위협에 대한 발생 빈도와 속성의 가치를 추정하고 단일속성함수를 평가한다.
- 관심의 대상이 되는 속성들에 대해서 우선순위를 확정하고 가중치를 평가한다.
- 위협 및 속성의 우선순위에 대한 자료에 기초해서 위협지수를 계산한다.

아래에서 논의되는 네 가지 가정들을 만족한다면 가산형 모형(additive value model)을 적용할 수 있는데, 이는 다음과 같은 가산형 함수를 기반으로 하여 다속성 대체안을 평가하는 모형이다[10, 6].

$$v(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{n} w_i v_i(x_i) \qquad (1)$$

여기서 $v_i(x_i)$는 x_i에 정의된 단순속성함수이고, w_i는 속성의 가치 x_i에 대한 함수의 가중치이다. 구체적으로 가산형 다속성 함수는 다음과 같은 다섯 단계에 의해 도출된다[1, 8].

- 가산형 모형의 적용 가능성을 확인하기 위해서, 가산형 가정들에 대한 타당성을 검토한다.
- 단일속성함수 $v_i, v_2, \cdots, v_n$을 측정한다.
- 가중치 $w_1, w_2, \cdots, w_n$을 도출한다.
- 각 대체안의 가치와 순위를 계산한다.
- 감도분석을 실시한다.

이러한 절차에 의해 위협을 평가하기 위해서 보안관리자는 어떤 위협이 조직의 자산에 잠재적인 위험이 되는지를 결정하고, 관심의 대상이 되는 위협들을 파악해야한다. 다음으로는 가산형 다속성모형의 적용 가능성을 검정하기 위해서, 이들 위협으로 인해 발생할 수 있는 위험의 속성들을 식별하고 4가지 가산성 가정(이전성, 선호독립성, 차별독립성, 절충독립성)에 부합하는지를 검토해야 한다. 비록 모든 속성에 대한 이들 가산성 가정들이 만족되는지를 검정하는 것은 불가능할지라도, 완벽하지는 않지만 강한 증거가 있다면 가산형 모형은 순수 가산형 모형에 매우 근접하는 값을 제공해 준다[5].

이러한 기존연구결과에 기초하여 정보시스템의 위험평가에 이 가산형 다속성모형을 적용하는 것이 적합한 것으로 알려져 있으므로[1, 7, 8], 본 연구에서는 이를 이용하여 정보시스템의 위협지수를 측정하고자 한다.

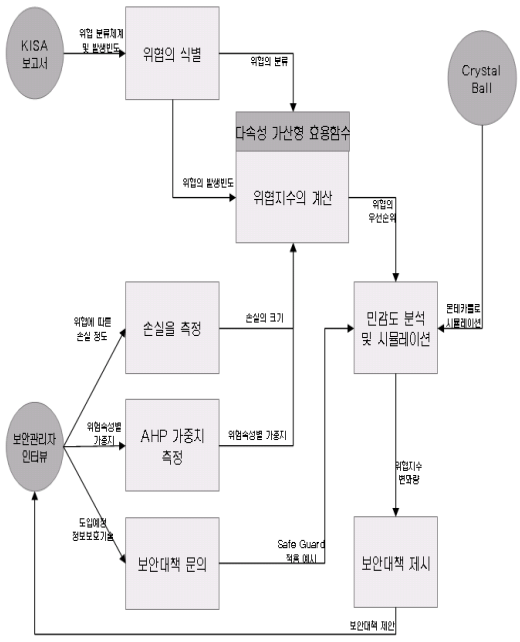
3. 연구모형

본 논문에서는 연구목적 달성을 위해 제 2장에서 검토된 다속성 함수의 수학적 모형을 이용하여 정보시스템의 위협지수를 측정하고자 한다. 이 위협지수의 활용을 통해 대상 사이트의 보안수준을 정확하게 파악하고, 효과적인 보안관리 계획을 수립할 수 있는 심도 깊은 분석이 가능하다. 사례연구에서는 본 논문에서 도출된 연구모형의 실무적 적용절차를 제시하고, 현업에서의 적용 가능성을 모색해 보고자 한다.

먼저, 위협지수 측정을 위해서는 분석대상 정보시스템의 보안에 영향을 미칠 수 있는 다양한 위협들과 구체적인 발생빈도 데이터가 요구된다. 또한 결과변수인 손실의 종류와 식별된 위협들이 발생했을 경우 나타나는 피해의 크기도 측정되어야 한다.

위험분석에 사용될 위협들의 발생빈도 정보로는 해당 사이트의 과거 사고발생기록 데이터를 활용하는 것이 바람직하다. 하지만 본 연구의 사례기업은 그러한 데이터를 관리하고 있지 않고 있으므로, 대안으로서 한국정보보호진흥원(KISA)의 인터넷 침해사고 동향 및 분석월보의 불법행위 통계자료[4]를 이용하고자 한다. 이 데이터는 국내 모든 사이트들을 대상으로 집계된 자료이므로, 충분히 대표성을 가지고 있다고 판단된다. 인터넷 포털 서비스를 제공하는 사례기업의 정보자산에 대한 공격 결과로 예상되는 위험속성들은 사이트의 정보시스템보안 담당자에 대한 심층 인터뷰를 통해서 식별되었으며, 구체적으로 수익감소, 고객상실, 생산성감소, 복구비용의 네 가지 이다. 이들 위험속성들에 대해서, 개별 위협이 발생했을 때 입게 되는 예상 손실의 크기도 함께 측정하였다. 각 위험속성들의 상대적 중요성은 AHP(Analytical Hierarchy Process)를 이용하여 측정하였다. 이렇게 해서 도출된 위협의 발생빈도, 손실의 상대적 중요성, 손실의 크기를 다속성 모형에 적용하여 불법행위별 위협지수를 산출하였다. 감도분석을 위해서는 크리스탈볼(Crystal Ball) 프로그램의 몬테카를로 시뮬레이션을 이용하였다.

이러한 연구체계를 기반으로, 본 논문에서는 [그림 1]과 같은 다속성 위험평가모형을 이용한 위협지수의 측정절차를 제안하고자 한다.



[그림 1] 다속성 위협지수에 의한 정보보호 분석모형

4. 분석절차

4.1 위협의 식별

대부분의 회사에서는 보안사고 관련 통계자료를 체계적으로 보유하고 있지 않음으로 대안으로서 우리나라의 전체 사고발생 빈도를 고려할 수 있는데, 구체적으로 본 연구에서는 한국정보보호진흥원(KISA)에서 발표한 통계자료를 이용하고자 한다. 한국정보보호진흥원(KISA)의 인터넷침해사고대응지원센터(Korea Internet Security Center, http://www.krcert.or.kr)에서 발행하는 인터넷 침해사고 동향 및 분석월보 2005년 12월호[4]에 의하면, 신고 된 2005년도의 침해유형에 따른 불법행위의 빈도는 <표 1>과 같다. 발생빈도 관점에서 보면 홈페이지변조, 불법자원사용, 침입시도, 불법침입, 서비스 거부의 순으로 발생 건수가 많았다.

〈표 1〉 침해유형에 따른 불법행위의 빈도

침해유형	2004년 총계	2005년 총계
침입시도	3,241	596
불법침입	1,647	9
불법자원 사용	3,048	6,308
홈페이지 변조	4,812	16,602
서비스 거부	0	3
총계	**12,748**	**23,608**

주) 자료 : 한국정보보호진흥원(KISA).

4.2 손실의 측정

연구자와의 인터뷰를 통해 보안관리자는 먼저 어떤 위협이 조직의 자산에 잠재적인 위험이 되는지를 결정하고, 관심의 대상이 되는 위협들에 대한 순위를 매겨야 한다. 다음으로는 각 위험 속성들이 가산성 가정(additivity assumption)을 만족하는지를 검토하게 된다. 즉, 가산형 모형의 적용을 위한 가정으로서 각 속성들에 대해 이전성(transitivity), 선호 독립성(preference independence), 차별 독립성(difference independence), 절충 독립성(tradeoff independence)이 성립되어야 한다. 본 연구에서는 회사 내의 정보자산에 대한 공격 결과로 예상되는 위험속성으로서 수익감소, 고객 상실, 생산성 감소, 복구비용의 네 가지 직접손실들을 고려했다. 이러한 네 가지 위험속성들 간에는 종속적인 관계가 없는 독립적인 속성들로 식별되었고, 가산성 가정들을 모두 충족한다고 판단된다[1].

가산형 다속성함수를 적용하기 위해서는 먼저 각 속성들에 대한 단일속성함수를 도출해야 한다. 여기서 각 속성별로 측정 척도가 상이함에 따른 계산상의 문제가 발생할 수 있는데, 이를 해결하기 위해서 함수의 결과 값을 0에서 1사이의 값으로 표준화 시키는 작업이 필요하다. 따라서 이 함수는 다음과 같은 형태가 된다.

$$v_i(x_{ij}) = x_{ij}/x_j^* \qquad (2)$$

여기서 x_{ij}는 위협 i에 대한 위험속성 j의 손실 값이고, x_j^*는 그 속성들 중 최대값이다. 따라서 이 식은 $0 \le v_i(x_{ij}) \le 1$을 만족하고, 1에 가까울수록 보다 위험이 심각하다는 것을 의미한다. 보안관리자의 위험선호 성향에 따라서, 이러한 단순 선형함수 대신에 볼록 혹은 오목함수를 이용할 수도 있다. 보안관리자는 정보시스템에 대해서 연간 공격빈도가 많은 위협들을 파악하고, 이들 위협으로 인해 발생 가능한 위험속성들을 식별해서 손실수준을 여러 가지 척도(시간단위, 화폐단위, 리커트 척도 등)로 측정하게 된다. 예를 들어 손실수준을 위험속성 관점에서 3점 척도(최소, 평균, 최대)로 측정하는 경우, 일반적으로 보안관리자는 손실수준의 상한과 하한을 먼저 결정한 후에 평균을 추정하게 된다.

4.3 가중치의 도출

다음으로는 각 속성에 대한 가중치를 도출하여야 하는데, 본 논문에서는 AHP를 이용하고자 한다. AHP는 1970년대에 Satty[9]에 의해 개발되었으며, 30여년이 지난 현재까지도 많은 이론 및 응용연구가 진행되어오고 있다. 다속성 의사결정 문제는 기본적으로 상충되는 다수의 기준 하에서 최적의 대안을 선택하는 문제로서, AHP는 이와 같은 의사결정 문제를 해결하기 위한 합리적인 분석적 틀을 제공해준다.

AHP에서 사용되는 평가척도는 비율척도이기 때문에, AHP는 대안의 우선순위 결정 문제뿐만 아니라 자원배분에 관한 문제에도 적용될 수 있다. 또한, AHP에서 사용되는 척도는 이산형과 연속형의 값을 모두 취할 수 있으며, 쌍별 비교 값은 실제 측정에 의해 얻을 수도 있고 평가자의 상대적 선호도를 반영하는 척도 값에 의해서도 얻을 수 있다.

AHP의 적용은 집단적 합의(group consensus)에 의한 계층구성(design of a hierarchy)과 개별 의사결정자로 부터의 평가(evaluation)로 크게 구분 지을 수 있다. 주어진 의사결정문제를 계층화한 후, 상위계층에 있는 한 요소(또는 기준)의 관점에서 직계 하위계층에 있는 요소들의 상대적 중요도(relative importance) 또는 가중치(weight)를 쌍별 비교(pairwise comparison)에 의해 측정하는 방식을 통해, 궁극적으로는 최하위 계층에 있는 대안들의 가중치 또는 우선순위(priority)를 구할 수 있도록 해준다. 또한 AHP는 의사결정자의 오랜 경험이나 직관 등을 평가의 바탕으로 하고 있기 때문에, 수치로 표현할 수 있는 양적(quantitative) 평가기준은 물론이고 흔히 의사결정문제에서 다루기 곤란하면서도 반드시 고려하지 않으면 안 될 질적(qualitative) 평가기준들도 비교적 쉽게 처리할 수 있다. 뿐만 아니라 분석과정도 직관적이고 비교적 단순하다는 장점을 지니고 있다[9].

4.4 위협지수 계산

다음으로는 앞에서 도출된 가중치를 가산형 다속성함수에 적용하여 위협지수(TI : Threat Index)를 계산하게 되는데, 이 위협지수는 개별 위협에 대한 상대적인 중요성을 반영하는 값이다. 위협 i에 대한 위협지수 TI_i는 보안관리자의 각 위험속성에 대한 주관적인 추정치와 빈도추정치를 근거로 다음과 같이 계산한다[7, 8].

먼저 앞에서 제시된 식 (2)를 이용해서 각 위험속성의 가치를 합할 수 있도록 정규화 작업을 해야 한다. 식 (2)에 각 위험속성의 상대적 가중치 ω_i를 곱해서 모두 더하면 위협 i에 대한 손실의 총합이 된다.

$$v(i) = \sum_{i=1}^{n} w_i v_i(x_{ij}) \qquad (3)$$

최종적으로, 위협 i에 대한 위협지수 TI_i는 위협 i의 발생 빈도인 $Freq_i$와 발생 손실인 식 (3)의 곱으로 계산된다.

$$TI_i = Freq_i \sum_{j=1}^{n} w_j v_i(x_{ij}) \quad (4)$$

여기서 만약 위협 i에 의해 발생되는 손실이 P_{low}, $P_{expected}$, P_{high}의 확률로 손실크기의 변화가 있다고 하면 식 (5)와 같게 된다.

$$\begin{aligned} TI_i = {} & P_{low} Freq_i \sum_{j=1}^{n} w_j v_i(x_{ij})_{low} \\ & + P_{expected} Freq_i \sum_{j=1}^{n} w_j v_i(x_{ij})_{expected} \\ & + P_{high} Freq_i \sum_{j=1}^{n} w_j v_i(x_{ij})_{high} \end{aligned} \quad (5)$$

다속성 의사결정기법의 장점은 속성의 이질적인 단위들(시간단위, 화폐단위, 리커트 척도 등)을 정규화해서 가중치를 부여하여 함께 합할 수 있다는 것이다. 보안관리자는 위험에 대해서 중립적이라는 가정을 하고 있으나, 만약 보안관리자의 위험에 대한 태도가 위험회피 혹은 위험추구형 이라면 이에 적합한 효용함수를 도출하여 적용해야 한다.

4.5 감도 분석

이렇게 해서 산출된 위협지수의 안정성을 검정하기 위해서는 감도 분석을 해야 한다. 감도 분석의 목적은 기존의 분석 결과가 주요 변수들에 대한 보안관리자들의 불확실성 범위에 얼마나 민감한지를 평가하는 것이다. 본 연구에서는 크리스탈 볼의 몬테카를로 시뮬레이션 기법을 이용하여 위험속성의 손실추정치와 위협의 발생확률추정치를 재검토 하고자 한다. 보안관리자는 가장 발생확률이 높은 값뿐만 아니라 상한과 하한 값도 함께 추정하게 되는데, 이를 시뮬레이션의 분포 값으로 입력하여 보안관리자의 불확실성이 각 위협지수에 얼마나 영향을 미치는지를 분석할 수 있다.

4.6 보안대책의 평가

정보보호 기술은 정보보호 기반기술(암호기술, 인증기술, 정보보호 평가기술), 시스템 및 네트워크 보호기술(시스템 보호기술, 네트워크 보호기술), 응용체계 보호기술(정보보호 응용기술, 해킹 바이러스 대응기술)로 구분 할 수 있다[2]. 또한, 정보보호 기술의 영역은 깊이에 따라서 예방(prevention), 탐지(detection), 복구(recovery) 등 세 가지의 영역으로 구분할 수 있다. 어떤 보안기술은 두 가지 영역에 속할 수 있으며, 또한 예상되는 위협에 대해서 한 가지 이상의 보안기술을 선택할 수도 있다. 예방기술은 위협이 손실로 진행되는 것을 억제시킴으로써 위협의 발생빈도를 줄여준다. 탐지기술은 공격이 진행 중인지 혹은 발생했는지를 식별하여 대응할 수 있도록 해준다. 복구기술은 기 발생된 손실을 탐지해서, 시스템관리자가 시스템 무결성을 복구할 수 있도록 해준다.

〈표 2〉 정보보호 기술의 영역

예방	Secure OS, 패킷 필터 방화벽(PF FW), 응용 방화벽(AP FW), 회로 방화벽(CIR FW), 스마트 카드, 가상 사설 네트워크(VPN), 취약성 평가 스캐너, 바이러스 방지 소프트웨어, Line Encryption, Authentication Policy Servers, 전자우편 필터
탐지	호스트 기반 침입탐지 시스템(IDS), 네트워크 기반 침입탐지 시스템, 네트워크 모니터링, Auditing, Key Stroke, Replicator
복구	백업 및 재난복구 도구들, 로그 분석, Load Balancing, 포렌식스(Forensics), 감리(Auditing), Key Stroke, Replicator

일반적으로 보안관리자는 기업의 필요에 따라서 예방, 탐지, 복구의 각 영역을 담당하는 정보보호기술을 도입하여 보안대책으로 사용한다. 인터넷 침해사고 발생 및 그에 대한 손실이 발생되는 것을 사전에 차단하기 위한 탐지 및 예방 기술과, 발생된 손실의 최소화를 위한 복구 기술은 모두 꼭 필요한 보안대책이다. 그러나 보안관리자는 회사의 영역별 중요도, 도입 및 유지비용 등의 제반 여건을 고려하여 보안전략을 세우고, 필요한 정보보호기술을 도입하게 된다.

5. 사례연구

5.1 사례연구 대상시스템

본 연구에서 개발된 모형의 현실적인 적용 가능성을 모색하기 위해서, 인터넷 포탈 서비스를 제공하는 한 기업을 선정하여 사례연구를 실시하였다. 대상 기업은 인터넷 포털 서비스를 기반으로 하는 수익모델을 가지고 있어서 인터넷 침해사고의 위협에 노출되어 있지만, 체계적인 보안팀이 구성되어 있어서 외부 침해에 대한 즉각적인 대응과 조치가 가능한 선두권 업체이다.

구체적으로 사례연구대상인 B기업은 게임 개발 및 퍼블리싱을 주요 수익모델로 삼고 있는 연간 매출액 약 3,000억원, 종업원수 약 1,700명인 상장기업이다. 이 회사는 보안관련 담당 업무자가 총 11명이며, 그 중에서 보안업무경력 7년인 보안팀장과의 면담을 통해 연구에 필요한 데이터를 수집하였다. 이 업체가 운영하고 있는 수많은 서버들 중 핵심 서비스를 제공하는 게임 퍼블리싱 서버군을 사례연구의 직접 조사대상이 되는 시스템으로 선정하였으며, 이 시스템은 약 3천대의 서버(WEB 서버, WAS서버, DB서버, 보안서버 등)로 구성되어 있다.

5.2 위협의 식별

사례연구 대상기업의 보안관리자는 '다년간의 보안팀 운영을 통해서 각종 보안대책이 마련되어 있어서 외부 인터넷에 의한 침해사고는 거의 발생하지 않고 있으며, 사고가 발생하더라도 즉각적인 대응으로 인하여 피해 정도는 미미하다'라고 응답하였다. 보안관리자는 <표 3>과 같은 한국정보보호진흥원 침해사고 통계분석보고서를 근거로, 해당 기업이 침해당한 경우를 가정하여 연간 공격빈도수 및 손실규모가 큰 불법행위에 대한 보안위험을 계량적으로 추정해야 한다.

〈표 3〉 침해유형에 따른 불법행위의 빈도

불법행위	빈도	%
침입시도	596	2.52
불법침입	9	0.04
불법자원사용	6,308	26.72
홈페이지 변조	16,692	70.70
서비스거부	3	0.01
합계	23,608	100.00

주) 자료 : 한국정보보호진흥원(KISA).

5.3 손실의 측정

사례연구 대상기업의 보안관리자는 주요 위험속성으로 수익감소, 고객상실, 생산성감소, 복구비용의 네 가지를 고려하였다. 한국정보보호진흥원에서 파악한 불법행위들로 인한 위험속성은 다양한 손실단위로 측정될 수 있는데, 보안관리자는 기업정보의 유출을 우려하여 모든 위험속성들에 대해서 7점(1점~7점) Likert 척도로 측정하였다. 구체적으로 주된 관심대상인 다섯 가지의 위협으로 인한 불법행위들의 손실크기는, 네 가지 위험속성 관점에서 최소, 평균. 최대 값으로 측정하였다.

〈표 4〉 기업의 불법행위에 따른 손실수준

불법행위		수익감소 (7점척도)	고객상실 (7점척도)	생산성감소 (7점척도)	복구비용 (7점척도)
침입시도	최소	1	1	3	1
	평균	1	1	5	1
	최대	1	1	7	1
불법침입	최소	3	1	3	2
	평균	3	2	5	4
	최대	3	3	7	5
불법자원사용	최소	3	1	4	3
	평균	3	2	6	4
	최대	3	3	7	5
홈페이지변조	최소	4	3	4	1
	평균	4	5	6	2
	최대	4	6	7	3
서비스거부	최소	6	2	4	1
	평균	6	4	6	2
	최대	6	5	7	3

B기업의 보안관리자는 각 위협별로 위험속성의 손실 크기가 달라질 것으로 예상했다. 일례로 고객상실의 손실을 크게 하는 위협은 홈페이지변조와 서비스거부이지만, 복구비용은 반대로 불법침입과 불법자원사용이 더 크게 될 것으로 응답했다. 왜냐하면 복구솔루션이 별도로 도입되어 있어서, 홈페이지변조나 서비스거부로 인한 피해에 대해서는 즉각적인 복구가 가능하기 때문이다.

한국정보보호진흥원(KISA)에서 집계하고 있는 불법행위의 속성들은 서로 종속적이다. 즉 침입시도를 통해서 불법침입이 이루어지고, 그 후에 불법자원사용이나 자료변조삭제 또는 서비스 거부가 발생되므로, 하나의 침입사고에 의해 다수의 불법행위가 발생할 수 있다. 일련의 연속적인 시간흐름을 따라서 불법행위들이 순차적으로 손실을 발생시킬 수 있으므로 침입시도 자체로는 거의 손실이 발생되지 않지만, 침입 후에 불법자원사용이나 자료변조 또는 서비스 거부 등의 후속 행위에 따라서 손실크기가 증가되는 경향이 있다.

5.4 가중치의 도출

다음으로는 AHP기법을 이용하여 각 손실변수들에 대한 가중치를 도출하고자 한다. 이를 위해서는 정보시스템 보안분야의 전문지식과 보안사고가 발생했을 때 회사에 미치는 영향을 추정할 수 있을 정도의 능력을 함께 갖춘 사람을 대상으로 심도 깊은 인터뷰가 이루어져야한다. 사례기업의 경우 정보시스템보안 부서 직원들은 회사의 전반적인 경영 현황에 대한 식견이 부족하고, CEO나 임원급 고위간부들의 경우는 정보시스템 보안분야에 대한 지식이 부족하여서 이들은 모두 적합한 대상자로 보기 어려웠다. 따라서 정보시스템 보안부서의 책임을 맡고 있는 보안관리자가 가장 적합한 대상자로 결정되었다.

일반적으로 AHP는 전문가의 견해를 계량화하는 기법이기 때문에 한명을 대상으로 분석을 진행한다면 결과의 안정성에 문제가 있을 수 있다. 본 연구에서는 보안관리자만이 유일한 적합자로 파악되어서 결과의 안정성에 문제가 있을 수 있으므로, 이를 보완하기위하여 보안관리자가 회사 내의 해당업무 담당자들로부터 자문을 구한 뒤에 응답하도록 요구하였다. 즉, 보안 기술에 대해서는 해당업무의 실무자들에게 보다 구체적인 현황을 파악하도록 요구하였고, 손실의 추정에 있어서도 회계와 관리부서의 책임자들과 구체적인 경영성과지표들에 대해서 논의한 후에 응답하도록 유도하였다.

가중치 도출에 사용된 설문양식과 응답결과는 다음 표와 같다.

〈표 5〉 설문양식과 응답결과

A	A가 더 중요				=	B가 더 중요				B
	9	7	5	3	1	3	5	7	9	
수익감소					○					고객상실
수익감소		○								생산성감소
수익감소		○								복구비용
고객상실		○								생산성감소
고객상실		○								복구비용
생산성감소							○			복구비용

B기업의 보안관리자는 수익감소와 고객상실이 동등하게 가장 중요하고, 이어서 복구비용과 생산성감소 순으로 중요하다고 평가하였다. B기업 보안관리자의 설문응답에 대한 쌍별 비교행렬로 부터 가중치를 계산하고 일관성을 측정하는 절차는 다음과 같다.

〈표 6〉 쌍별 비교행렬

구 분	수익감소	고객상실	생산성감소	복구비용
수익감소	1	1	7	7
고객상실	1	1	7	7
생산성감소	1/7	1/7	1	1/5
복구비용	1/7	1/7	5	1

<표 5>의 응답결과를 기초로 만들어진 이 쌍별 비교행렬을 이용하여, 각 손실변수들의 가중치를 도출하고 응답의 일관성을 검정하기 위한 일관성비율 계산 결과는 다음 <표 7>과 같다.

〈표 7〉 가중치 및 일관성비율

구 분	수익감소	고객상실	생산성감소	복구비용	계/값
가중치	0.43	0.43	0.04	0.09	0.99
최대고유치(λmax)					4.33
일관성지수(CI : Consistency Index)					0.11
일관성비율(CR : Consistency Ratio)					0.12

응답자의 주관을 반영한 결과인 쌍별 비교행렬 도출 시, 다수의 속성들을 서로 짝을 지어 비교하게 되므로 응답의 일관성이 결여될 가능성이 있다. AHP에서는 이를 검정하기 위한 지표로서 CR을 이용하는데, 0.1보다 작은 경우 일관성이 아주 잘 지켜진 것으로 보고 있으며, 0.2까지는 받아들여 질만한 값으로 간주하고 있다. 하지만 0.2를 초과하게 되면 일관성에 심각한 문제가 있는 것으로 판단하여 다시 측정할 것을 권고하고 있다[3].

<표 7>의 일관성지수 CR의 계산 결과를 보면, 본 사례에서 도출된 보안관리자의 응답은 0.12인 것으로 나타났다. 가중치의 응답을 도출하기위한 방법이 생소하고, 판단에는 고도의 지적 노동이 요구된다는 다는 것 등을 감안한다면 이는 충분히 받아들여질 만한 수치라고 볼 수 있다.

5.5 위협지수의 계산

다음으로는 보안관리자와의 인터뷰에 근거하여 불법행위들이 회사 내에서 얼마나 자주 발생하는지를 평균, 최대, 최소의 세 가지 확률 값으로 추정하였다. 위협지수는 각 위협별로 상대적인 중요도를 가중 평균하여 구한 것으로서, 측정단위가 존재하지 않는다. 이 위협지수에 의해서 상대적으로 어떤 위협의 잠재손실이 얼마나 큰지 식별할 수 있다. 또한 위협지수들의 합계를 구해서 다른 정보시스템의 위협과도 비교할 수 있다.

〈표 8〉 기업의 위협지수 계산

위협종류	최소	평균	최대	위협지수
침입시도	10.8	102.1	1.2	114.0
불법침입	0.3	3.7	0.1	4.1
불법자원사용	232.0	2,640.6	35.8	2,908.4
홈페이지변조	913.7	10,726.8	136.7	11,777.1
서비스거부	0.2	2.1	0.0	2.3
계	1,157.0	13.475.3	173.7	14,806.0

이 기업의 위협지수 크기는 홈페이지변조, 불법자원사용, 침입시도, 불법침입, 서비스거부의 순인 것으로 나타났으며, 위협지수의 총 합계는 14,806으로 측정되었다. 이 위협지수의 결과치만으로 봤을 때 사례연구 대상기업은 홈페이지변조에 의한 위협(11,777)이 가장 크고, 서비스거부(2.3)와 불법침입(4.1)이 아주 작은 것으로 나타나서 매우 큰 차이를 보였다. 이는 분석에 사용된 한국정보보호진흥원 침해사고 통계 보고서에서 홈페이지 변조가 가장 많은 빈도수(16,606)를 기록한 반면에, 서비스거부(3)와 불법침입(9)은 아주 적었기 때문인 것으로 분석된다.

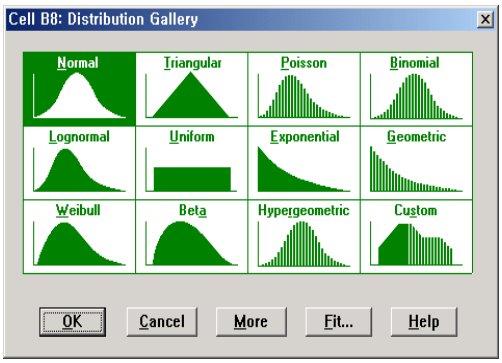
위협지수의 절대적 크기는 위협에 의해 발생되는 손실의 정도에 대한 보안관리자의 주관적 판단에 근거한 것으로서, 다른 기업의 위협지수를 서로 비교하는 것은 큰 의미가 없다. 다만 해당 기업의 보안관리자들이 인식하고 있는 침해위협의 상대적인 손실크기를 반영한 지수로서는 해석할 수 있을 것이다.

5.6 감도분석

감도분석의 목적은 주요 변수들에 대한 보안관리자의 불확실성 범위가 얼마나 결과에 영향을 미치

는지를 분석하는 것으로, 본 연구에서는 위험속성의 손실추정치, 위험속성의 가중치, 불법행위 발생확률추정치 등의 세 가지 이다. 이들 중 가중치는 AHP의 CR 값에 의해서 일관성 검정이 이루어 졌으므로, 시뮬레이션을 이용하여 위험속성의 손실추정치와 불법행위의 발생확률 추정치에 대해서 감도분석 하고자 한다. 시뮬레이션에는 Decisioneering 사에서 개발한 크리스탈볼(Crystal Ball) 프로그램을 사용하였다. 크리스탈볼은 Microsoft 사의 스프레드시트 프로그램인 엑셀(Excel)에 Add-on되어 동작하는 리스크 분석 소프트웨어로서, 엑셀의 스프레드시트 모델링에 몬테카를로 시뮬레이션 기능을 추가하여 확률론적 분석을 도와주는 역할을 한다. 본 연구에서는 위험속성 손실추정치와 불법행위의 발생확률추정치를 불확실한 값들의 분포로 정의하고, 그에 따른 위협지수의 변화량을 시뮬레이션을 통해 측정하였다.

첫 번째 단계에서는 데이터가 있는 셀에 확률분포를 선택하여 설정한다. 구체적으로는 다음 그림과 같이 정규, 삼각형, 포아송, 베타 등의 다양한 분포들 중에서, 해당 데이터에 가장 적합한 것을 선택해야 한다.

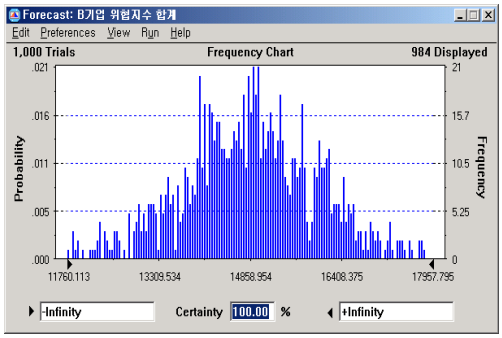


[그림 2] 적용가능 확률분포

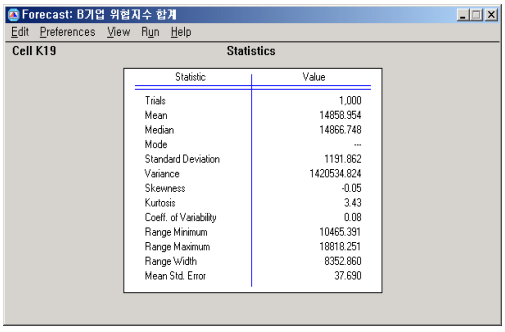
본 연구에서는 보안관리자의 응답에 의해 위험속성의 추정치에 대한 평균값과 상한 및 하한 값을 얻었기 때문에, 이에 적합한 삼각형분포를 적용하였다. 그리고 불법행위의 발생확률 추정치는 불확실한 어떤 행위의 발생확률을 추정하는 것이므로 정규분포를 적용하였다.

두 번째 단계에서는 예측 셀을 정의해야 한다. 예측 셀은 모델의 결과 값인 위협지수 셀이 된다. 이 모델에 위험속성의 추정치와 불법행위의 발생확률 추정치를 입력하여, 최종적으로 위협지수의 총합을 예측하는 시뮬레이션을 실행하였다. 각각의 불법행위별 위협지수를 예측 셀로 정의해도 되지만, 본 연구에서의 감도분석 목적은 전체적인 위협지수의 변화량을 측정하는 것이기 때문이다.

이러한 절차를 거쳐서 시뮬레이션을 실행시키면 모델에 의해 계산된 예측 값의 분포 그래프를 얻을 수 있다. [그림 3]은 B기업의 위협지수 합계에 대한 예측결과 그래프이고, [그림 4]는 [그림 3]에 대한 통계량 결과치이다.

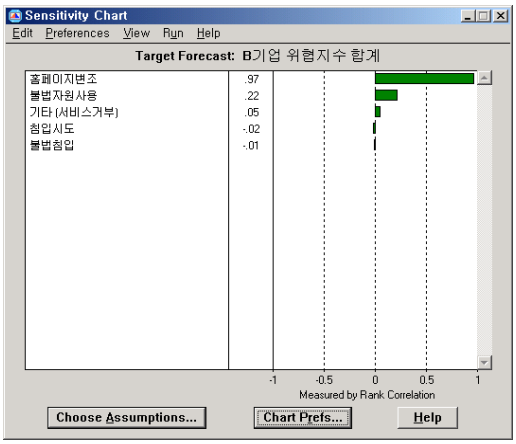


[그림 3] 위협지수 합계 변화량 시뮬레이션



[그림 4] 시뮬레이션 통계량 결과치

[그림 3]과 [그림 4]의 결과로 보면 사례기업의 총 위협지수는 10,465에서 18,818사이에 분포하며, 평균값은 14,858이고, 중앙값은 14,866이다. 시뮬레이션 결과 그래프와 통계량 수치는 <표 6>에서 계산된 사례기업의 위협지수 불확실성에 대한 예측치로서 의미가 있다. 위협지수의 변화량에 어떤 변수가 가장 많은 영향을 미치는지 분석해 본 민감도 그래프는 [그림 5]와 같다.



[그림 5] 위협지수 민감도 분석

민감도 그래프는 홈페이지변조, 불법자원사용, 서비스거부, 침입시도, 불법침입의 5가지 위협들이 사례기업의 위협지수에 영향을 미치는 정도를 측정하여 그림으로 나타낸 것이다. 이 그래프에 의하면 사례기업의 위협지수는 홈페이지변조와 불법자원사용의 두 가지 위협에 의해 가장 많은 영향을 받는 것으로 나타났다. 따라서 본 사례기업의 경우는 홈페이지 변조와 불법자원사용 위협에 대한 관리에 보다 많은 자원을 투입하여야 할 것으로 판단된다. 또한 차후의 보안진단을 위한 위협지수 측정 시에는, 이들 두 가지 위협의 가중치가 보다 안정적으로 도출될 수 있도록 최선의 노력을 기울여야 할 것이다.

5.7 보안대책의 평가

사례연구 대상 기업은 정보시스템 침해사고를 방지하기 위해서 필요한 대부분의 정보보호기술을 보유하고 있어서, 실제로 침해사고에 의한 손실은 발생하지 않고 있다. 본 연구자들은 보안대책을 평가하기위한 방법으로서, 정보보호기술의 도입에 따른 위협의 발생빈도 감소 시뮬레이션에 의해 위협지수의 변화량을 측정하고자 한다. 위협의 발생빈도 감소 예측은 보안관리자와의 인터뷰를 통해 이루어졌으며, 1,000회의 시뮬레이션에 의해 그 변화량을 측정하였다.

사례기업의 보안관리자가 현재 시행중인 보안대책으로 제시한 정보보호기술은 다음과 같다. 첫 번째는 응용소프트웨어 방화벽(application firewall)으로 웹 방화벽으로도 불리며, 기존의 하드웨어 기반이 아닌 웹 어플리케이션 단에서 구동하는 방화벽 소프트웨어이다. 두 번째는 Anti-DDOS로서, 분산된 서비스 거부공격(Distributed Denial of Service)을 효과적으로 차단하기 위한 대응 솔루션이다. 세 번째는 OS패치 자동설치로서, Windows 서버시스템에서 Microsoft에서 제공하는 OS 패치를 자동으로 설치하도록 지원하는 시스템이다. 네 번째는 취약성평가 스캐너로서, 시스템에서 보안상 취약한 부분을 찾아내기 위한 솔루션이다.

사례기업의 보안관리자가 현 시점에서는 정보보안 기술의 추가적인 도입은 고려하고 있지 않고 있다고 응답하였기 때문에, 도입 예정 기술에 대한 평가는 진행할 수 없었다. 따라서 최근에 도입한 정보보안기술이 인터넷 침해사고에 대해서 실제로 어느 정도의 효과가 있는지를 분석하였다. 이를 위해서 보안관리자에게 각 정보보호기술의 도입에 따른 위협의 발생빈도 감소 정도를 추정하게 하였다.

〈표 9〉 정보보호기술 도입 시 위협의 발생빈도 감소 추정치(단위 : %)

정보보호 기술	손실 구분	침입 시도	불법 침입	불법 자원 사용	홈페이지 변조	서비스 거부
응용 방화벽	최소	70	70	40	80	0
	평균	80	90	90	90	0
	최대	100	100	100	100	0
Anti-DDOS	최소	0	0	0	0	90
	평균	0	0	0	0	100
	최대	0	0	0	0	100
OS 패치 자동설치	최소	30	30	20	30	20
	평균	60	50	50	40	50
	최대	80	80	80	80	60
취약성 평가 스캐너	최소	30	30	30	30	0
	평균	50	50	50	50	10
	최대	70	70	70	70	20

보안관리자의 예측을 근거로 감소된 발생빈도를 모델에 등록하여 위협지수에 대한 시뮬레이션을 실행시키면, <표 9>와 같은 통계량을 얻을 수 있다.

〈표 10〉 위협지수 감소 시뮬레이션 결과

통계치	도입전	응용 방화벽	Anti-DDOS	OS패치 자동설치	취약성 평가 스캐너
평균값	14859	1691	14746	8657	7614
표준편차	1192	132	1233	725	615
최소값	10465	1204	10400	6255	5355
최대값	18818	2064	19403	10794	9484

<표 9>의 결과를 보면, 응용방화벽이 도입전의 14,859에서 1,691로 가장 많은 감소를 보였으며, OS 패치 자동설치 솔루션, 취약성평가 스캐너가 8,657과 7,614로 절반 정도의 감소를 보였다. 하지만 Anti-DDOS는 14,746으로 거의 변화가 없는 것으로 나타났다.

따라서 사례기업은 응용방화벽 도입에 의해 위협지수의 평균값이 도입전의 약 11% 수준으로 감소되었으므로, 응용방화벽이 가장 효과적인 보호대책인 것으로 나타났다. 또한 취약성평가 스캐너와 OS패치 자동설치도 51%와 58% 수준으로 감소되는 것으로 나타나서, 이 기업의 보안 강화에 상당부분 기여한 것으로 나타났다. 하지만 Anti-DDOS의 경우는 위협지수의 감소가 거의 없는 보안대책인 것으로 분석되었으므로, 향후의 재 구매나 최신 버전으로의 업그레이드 시점에서 추가적인 예산배정을 하지 않고 점진적으로 폐기하는 것이 바람직할 것으로 판단된다.

본 논문의 사례기업은 추가적인 보안대책을 고려하고 있지 않아서, 현재 채택하고 있는 보안기술들만을 대상으로 감도분석을 실시하고 그 효과성을 평가 하였다. 하지만 추가적인 보안대책들을 고려하고 있는 기업을 대상으로 분석하고자 하는 경우에 있어서, 대안들 중 어떤 보안기술을 채택하는 것이 더 효과적일 것인가에 대한 의사결정문제에도 본 연구에서 제안한 방법론을 동일하게 적용할 수 있다.

6. 결 론

본 논문의 주요 연구목적은 다속성 함수와 시뮬레이션을 이용한 다속성 위험평가모형으로 정보시스템의 위협을 평가하는 기법을 제안하고, 사례연구를 통해 정보시스템 위험분석의 이론적, 실무적 틀을 제공하려는 것이다.

이를 위해 첫째, 인터넷 침해사고에 노출된 정보시스템의 위협 정도를 정성·정량적으로 계산하고, 객관적이고 적절한 보안대책을 평가하는 방법을 제안하였다. 보안관리자와의 인터뷰를 통해서 위험을 계량화하는 방법을 제시하였으며, 전문가의 주관적 판단에 객관성을 부여하기 위해 다속성 위험평가모형을 도출하여 적용하였다. 이 모형에 의해서 측정된 위협지수는 모든 정보시스템에 반복하여 적용할 수 있는 체계적인 보안관리도구로

서, 위협의 크기를 측정하는데 큰 도움을 줄 수 있다.

둘째, 국내에서 인터넷 포털 서비스를 제공하는 상장회사를 선정하여, 해당 기업 보안관리자와의 인터뷰를 통해 연구방법론을 설명하고 보안대책에 관한 응답을 받았다. 이 기업은 위험속성으로 수익감소, 고객 상실, 생산성 감소, 복구비용 등을 들었으며, 가산형 다속성함수를 이용하여 위협지수를 도출할 수 있었다. 이들 각 위험속성들의 측정단위가 화폐 및 시간 단위, Likert 척도 등으로 서로 다르게 측정되어도 표준화하여 개별 위협의 상대적 중요성을 파악할 수 있었다. 그리고, 몬테카를로 시뮬레이션에 의해 정보보호기술 도입 이후의 위협지수 변화량을 분석함으로서 도입 보안기술의 효과성을 측정하였으며, 궁극적으로 이를 향후의 보안대책 선정에 관한 합리적인 의사결정 지표로도 활용할 수 있다.

본 연구에서 사용된 한국정보보호진흥원(KISA)의 침해사고통계에서는 불법행위들을 침입시도, 불법침입, 불법자원사용, 자료변조삭제, 서비스 거부 등으로 분류하고 있는데, 이들은 시스템침투과정 중에 발생되는 불법행위의 침해정도를 나타내고 있다. 이러한 불법행위의 분류체계가 이론적인 위협의 분류체계와 다소 상이하고, 서로 종속적이라는 것이 본 연구의 한계점이다. 따라서 앞으로의 연구에서는 이러한 한계점을 극복하고 분석대상 조직의 특성을 합리적으로 반영하기 위해서, 개별 조직들이 체계적으로 유지관리 하는 데이터를 활용하는 것이 바람직할 것이다.

끝으로, 본 연구에서는 위협지수를 사례대상 조직의 정보보호기술 효과성 평가를 위해서만 사용하였지만, 정보시스템 간 또는 조직들 간의 정보시스템 위협크기를 상대적으로 비교하는 목적으로도 활용할 수 있을 것이다. 또한, 이 분석기법을 정보시스템이 아닌 일반 재해분야에 적용하여 재난복구대책을 수립하는 목적으로 이용함으로서, 그 활용범위를 다양화할 수도 있을 것이다.

참 고 문 헌

[1] 김기윤, 나관식, “다속성 위험평가기법을 이용한 정보시스템의 위협지수 측정”, 「리스크관리연구」, 한국리스크관리학회, 제15권, 제2호(2004), pp.103-126.

[2] 김배현, 나원식, 유인태, 권문택, “국방 정보보호 기술 발전 동향”, 「정보보호학회지」, 한국정보보호학회, 제12권, 제6호(2002), pp.58-66.

[3] 장양철, 안병석, “AHP를 이용한 정보시스템 개발업체 선정에 관한 연구”, 「한국IT서비스학회지」, 제5권, 제3호(2006), pp.187-201.

[4] 한국정보보호진흥원(KISA) 인터넷침해사고대응지원센터, “인터넷 침해사고 동향 및 분석월보”, 2005, http://www.krcert.or.kr.

[5] K. Paul Yoon and Ching-Lai Hwang, *Multiple Attribute Decision Making : An Introduction*, Sage Publications, 1995.

[6] Ralph L., Keeney and H. Raiffa, *Decision with Multiple Objectives : Preference and alue Trade Offs*, John Wiley and Sons, 1976.

[7] Shawn A., Butler, “Security Attribute Evaluation Method : A Cost Benefit Approach”, *24th International Conference on Software Engineering Proceedings*, (2000), pp.220-240.

[8] Shawn A., Butler and Paul Fischbeck, “Multi-Attribute Risk Assessment”, *Technical Report CMU-CS-01-169*, 2001.

[9] Thomas L., Saaty, *The Analytic Hierarchy Process*, McGraw-Hill, New York, 1980.

[10] W., Edward, “How to Use Multi-attribute Utility Measurement for Social Decision-Making”, *IEEE Transactions on Systems, Man and Cybernetics*, (1977), pp. 326-340.

◈ 저 자 소 개 ◈

이 강 수 (kslee@dreamwise.co.kr)

(주)드림와이즈 기술연구소 연구팀장으로 재직 중이며, 숭실대학교에서 공학사, 광운대학교에서 경영학 석사 학위를 취득했다. IT Project 로서 LG전자 KMS 통합검색시스템 구축, 한국청소년상담원 통합관리시스템 구축, 국립중앙도서관 통합인증시스템 구축 등을 수행한 바 있다. 주요 관심분야는 정보기술 위험관리(Security and Incident Risk, BCP 등)이다.

김 기 윤 (min1203@kw.ac.kr)

광운대학교 경영학과 교수로 재직 중이며, 고려대학교에서 공학사, 경영학 석사, 경영학 박사 학위를 취득했다. Journal of Systems and Software, Journal of Information System Education 등의 국제학술지 및 경영과학, 경영정보학연구, 리스크관리연구, 정보보호학회논문지, 정보화정책 등에 논문을 게재한 바 있다. 주요 관심분야는 정보기술 위험관리(S/W Risk, Security & Incident Risk, BCP 등) 이다.

나 관 식 (ksna@seowon.ac.kr)

서원대학교 경영정보학과 교수 겸 미국 앨라배마 주립대학교(UAH) 대학원 Affiliate Professor로 재직 중이며, 광운대학교에서 경영학사, 경영학 석사, 경영학 박사 학위를 취득했다. Journal of Systems and Software 등의 국제학술지 및 경영과학, 경영정보학연구, 리스크관리연구, JITAM, 정보화정책, 정보보호학회지 등에 논문을 게재한 바 있다. 주요 관심분야는 SCM, 정보기술 위험관리, 소프트웨어 프로젝트관리, DSS 등이다.