다속성 위험평가: 위협지수

김기윤**, 나관식***

**광운대학교 경영학과, ***서원대학교 경영학부

Multi-Attribute Risk Assessment : Threat Index

Kim, Ki-Yoon, Na, Kwan-Sik

Kwangwoon University, Seowon University

E-mail : min1203@daisy.kwangwoon.ac.kr, ksna@seowon.ac.kr

요 약

다속성 위험평가는 위협과 보안요구사항의 집합을 순위화해서 계량적으로 위험을 평가하는 유용한 체계를 제공해 준다. 본 논문의 목적은 위험을 파악해서 순위화 하는 과정을 다속성 위험평가에 의해서 분석하는 이론과 사례를 제시하는 것이다.

1. 서론

보안관리에서 위험평가는 자산의 취약성을 식별하고 존재하는 위협을 분석하여, 이들의 발생가능성 및 위협이 미칠 수 있는 영향을 파악해서, 보안위험의 내용과 정도를 결정하는 과정이다. 위험이란 자산(또는 자산집합)의 취약성이 있는 부분에 위협요소가 발생하여 자산의 손실이 발생된 것이고, 위협이란 자산에 해를 줄 수 있는 위험의 원천이다. 여기서 취약성이란 조직이나 시스템에 피해를 끼칠 수 있는 원치 않는 사고의 잠재적 원인인 위협이 가해질 수 있는 자산의 약점이다. 이러한 취약성으로 인한 위험은 사건발생 확률 혹은 빈도와 예상되는 손실로 표현 할 수 있다. 그러나 위험의 발생가능성이나 발생 손실이 불확실한 경우, 혹은 위협에 대해서 여러 속성들을 평가해야할 경우에는 전통적인 위험평가방법으로는 해결이 불가능하다.

위협으로 인한 위험을 여러 가지 속성들로 분류해서 평가하는 다속성 위험평가의 장점은 보안관리자가 조직의 내 다양한 보안위험을 파악할 수 있고, 위협으로 발생 가능한 여러 잠재적 손실들을 추정할 수 있다는 것과, 위협에 대한 보안대책들의 상대적 중요성을 파악할 수 있는 통찰력을 제공해 준다는 것이다.

본 논문의 연구목적은 한국정보보호진흥원(KISA)의 침해사고통계를 근거로 불법행위에 대한 다속성 위험평가 모형인 위협지수를 도출하는 사례를 제시하는 것이다. 이를 위해서 2장에서는 다속성 위험평가와 가산형 모형의 이론적 배경을 기술했다. 3장에서는 가산형 모형에 의한 다속성 위험평가 절차로서 다속성에 대한 가산성 가정의 검토, 단일속성 함수의 평가, 가중치의 도출, 위협지수의 도출, 감도분석 등을 기술했다. 4장에서는 침해사고통계를 근거로 불법행위에 대한 다속성 위험평가 모형인 위협지수를 도출하는 사례를 제시했다. 5장에서는 연구의 요약 및 한계를 제시했다.

2. 다속성 위험평가와 가산형 모형

2.1 다속성 위험평가

다속성 위험평가는 위협과 보안요구사항의 집합을 순위화해서 계량적으로 위험을 평가하는 유용한 체계를 제공해 준다. 다속성 위험평가의 장점은 보안관리자가 조직 내의 위험을 파악해서 공격으로 인한 손실을 예상할 수 있게 해준다는 것이다.

위험평가팀의 구성원은 조직에 따라 다를 수 있지만, 위험분석자와 보안관리자(혹은 정보관리자)는 반드시 참여해야 한다. 위험분석자는 인터뷰를 하고, 보안관리자가 제공하는 정보를 기록해서 분석하고 감도분석을 수행해야하는 책임이 있다. 보안관리자는 위협에 대한 정보를 제공하기 위해서 조직 내의 정보관리자와 협의해야 한다.

다속성 위험평가절차는 다속성의 식별과 가산성 가정의 검토, 단일속성함수의 평가, 가중치의 도출, 위협지수의 도출 등 연속적인 네 단계로 수행되는데, 구체적으로는 다음과 같다. 첫째, 보안관리자는 위협으로 발생되는 위험결과에 대한 속성들을 식별한 후에, 속성에 대한 가산성을 검토한다. 두 번째, 보안관리자는 각 위협에 대한 빈도와 속성의 가치를 도출하고, 단일속성함수를 평가한다. 세 번째, 보안관리자는 관심대상인 속성들에 대해서 우선순위를 확정하고, 가중치를 평가한다. 네 번째, 위협 및 속성의 우선순위에 대한 자료를 가지고 위협지수를 계산한다.

2.2 가산형 모형

다목표 의사결정문제의 위험평가에있어서, 다속성 대안들을 평가할 수 있는 가산형 모형을 적용할 수 있다(Edwards, 1977; Keeney et. al., 1999). 가산형 모형(additive value model)은 다음과 같은 가산형 함수를 근거로 다속성 대체안을 평가하는 모형이다.

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

여기서 $v_i\ (x_i)$는 x_i 수준에 정의된 단순속성함수이고, w_i 는 속성의 가치 x_i 에 대한 함수의 가중치이다. 구체적으로 가산형 다속성 함수는 다음과 같은 다섯 단계에 의해 도출된다.

- 가산형이 확실한지 알기 위해서 가산형 가정에 대한 타당성을 검토한다.
- 단일속성함수 $v_1,\ v_2\ ,\ ...,\ vn$ 을 평가한다.
- 가중치 $w_1,\ w_2,\ ...,\ w_n$ 을 평가한다.
- 각 대체안의 가치와 대체안의 순위를 계산한다.
- 가정을 모형화 하기 위해서 우선순위가 얼마나 중요한지 알기 위한 감도분석을 실시한다.

3. 가산형모형에 의한 다속성 위험평가 절차

3.1 가산성 가정의 검토

보안관리자는 어떤 위협이 조직의 자산에 잠재적인 위험이 되는지를 결정하고, 관심대상이 되는 위협들을 순서대로 나열한다. 위협별로 위험의 속성들을 식별한 후에, 각 속성들에 대해서 가산성 가정(additivity assumption)이 적합한지 검토한다. 가산형 모형의 가정으로서 각 속성들에 대해서 이전성(transitivity), 선호 독립성(preference independence), 차별 독립성(difference independence), 절충 독립성(tradeoff independence)이 성립되어야 한다. 비록 모든 속성에 대한 이들 가산성 가정들이 만족되는지를 검정하는 것이 불가능할지라도, 완벽하지는 않지만 강한 증거가 있다면 가산형 모형은 순수 가산형 모형에 매우 근사하는 값을 제공해 준다(Yoon, et. al., 1995).

3.1.1 이전성

만약 X_1 이 X_2 보다 선호되고, X_2 가 X_3 보다 선호된다면, X_1 이 X_3 보다 선호된다는 것을 만족해야 한다. 여기서 $X_1,\ X_2,\ X_3$ 는 결과 집합이다. 예를 들어서, 만약 어떤 조직이 단 하나의 결과속성인 수익감소만을 가지고 있고, 각 결과발생은 수익감소 폭의 확대를 초래한다고 가정한다. 이때 보안관리자는 모든 경우에 있어서 보다 많은 수익감소 보다는 보다 적은 수익감소를 선호할 것이라고 가정하는 것이 합리적일 것이다. 이전성은 모든 합리적인 의사결정자가 따라야 할 규범적인 가정(normative assumption)이다.

3.1.2 선호독립성

하나의 속성에 대한 의사결정자의 선호 서열이 다른 속성의 고정된 값에 의존하지 않는다면, 선호 독립성이 존재한다. $X_1,.....,\ X_n$ 이 의사결정 속성을 나타내고, $X_{2,....}\ X_n$ 이 상수로 고정되어 있을 때, X_1 의 각기 다른 수준에 대한 의사결정자의 선호 서열이, $X_{2,....}\ X_n$ 이 상수로 고정되어 있다는 사실에 의존하지 않는다는 것이다. 예를 들어, X_1 이 생산성 감소이고 X_2 가 수익 감소, X_3 가 고객 상실 이라면, 의사결정자는 나머지 두 속성의 어떤 결합에서도, 보다 많은 생산성 감소보다는 보다 적은 생산성 감소를 선호하게 된다. 비록 이것은 규범적인 가정은 아닐지라도, 컴퓨터 보안 문제에 적용되지 못할만한 이유는 발견할 수 없다.

3.1.3 차별독립성

가산형 모형은 의사결정자가 속성 값의 차이를 서열화 시킬 수 있다는 것을 가정한다. 차별 독립성은 선호 독립성에서 한걸음 더 나아간 것으로, 속성 값의 차이에 대한 서열이, 주어진 다른 속성들의 고정된 결과 값 하에서 변경되지 않을 것을 요구한다. 예를 들어 고객 상실과 복구비용의 위험평가 수준이 7점 리커트 척도라면, 이 척도의 간격은 다른 속성들의 측정 수준에 따라 변하지 않아야 한다는 것이다.

3.1.4 절충독립성

절충 독립성은 모든 다른 속성들이 고정되어 있을 때, 두 속성 사이의 절충(tradeoff)이 다른 속성들의 고정된 수준에 영향을 받지 않는다는 것이다. 만약 $X_1,\ldots,X_n$ 이 3개 이상의 속성집합일 때, X_1, X_2 의 모든 속성 쌍에 대한 절충이 X_3 의 고정된 수준의 유지에 영향을 받지 않는다는 것을 의미한다. 절충 독립성 또한 규범적인 가정은 아니지만, 정보시스템에 대한 위협의 공격이 성공해서 발생한 두 가지 위험 결과 사이의 절충이, 다른 위험 결과에 의해서 영향을 받는다고 할만한 이유는 발견할 수 없다.

3.2 단일속성함수의 평가

가산형 다속성함수를 도출하기 위해서는 각 속성에 대한 단일속성함수를 평가해야하는데, 각 속성의 관련 범위에 대한 결과의 선호를 반영하고자 하는 것이 목적이다. 여기서 각 속성별로 측정 척도가 상이함에 따른 계산상의 문제를 해결하기 위해서 이 함수의 결과 값을 0에서 1사이의 값으로 표준화 시킨 함수의 형태는 다음과 같다.

$$V_i(X_{ij}) = X_{ij} / X_j^*$$

한여기서 X_{ij} 는 j번째 속성의 i번째 속성의 값이고, X_j^* 는 그 속성들 중에서 최대 값이다. 따라서 이 식은 $0 \le V_i(X_{ij}) \le 1$을 만족하고, 1에 가까울수록 보다 위험이 심각하다는 것을 의미한다. 보안관리자의 위험선호에 따라서, 이러한 단순한 선형함수 대신에 볼록 혹은 오목함수를 이용할 수도 있다.

보안관리자는 정보시스템에 대해서 연간 공격빈도가 많은 위협들을 파악하고, 이들 위협 때문에 발생가능한 위험속성들을 식별해서 손실수준을 여러 가지 척도(시간단위, 화폐단위, Likert 척도 등)로 측정한다. 예로써, 손실수준을 위험속성 관점에서 3점 척도(최소, 평균. 최대)로 측정하는 경우에는, 일반적으로 보안관리자는 위험결과에 대한 속성가치, 즉 손실수준의 상한과 하한을 먼저 추정한 후에, 평균을 추정한다.

3.3 가중치의 도출

가산형 다속성함수를 도출하기 위한 세 번째 단계는 각 속성에 대한 가중치를 평가하는 것이다. 속성의 상대적 가중치를 결정하기 위해서 SWM(Swing Weight Method)를 이용한다. SWM은 사용하기 간편하며, 보안관리자가 쉽게 이해할 수 있는 장점이 있으며(Butler and Fischbeck, 2001), 다음과 같은 3단계의 과정을 거쳐서 가중치를 도출하게 된다.

첫째, 보안관리자는 위험속성에 대해서 상대적 중요성 나타내는 순위를 결정한다. 둘째, 보안관리자에게 가장 중요한 관심대상이 되는 1순위 속성에 대해서 100점을 부여하고, 나머지 속성들에 대한 순위의 상대적인 값을 1점에서 100점까지의 값을 부여한다. 셋째, 순위의 전체 합이 1이 되도록 정규화해서 가중치를 도출한다. 즉 모든 속성들을 평가한 점수의 합계로 개별 속성의 점수를 나누어서 전체 가중치의 합이 1이 되도록 정규화 한다.

3.4 위협지수의 도출

가산형 다속성함수를 도출하기 위한 위협에 대한 우선순위를 이용해서 위협지수(TI: Threat Index)를 계산하는 것인데, 이 위협지수는 개별 위협에 대한 상대적인 중요성을 반영한다. 위협 a에 대한 위협지수 TIa는 보안관리자의 주관적인 속성가치의 추정치와 빈도 추정치를 근거로 다음과 같이 계산한다 (Butler and Fischbeck, 2001; Butler, 2002).

$$TI_a = Freq_a * [P_{low} * (\Sigma_{j=attributes} W_j * V_j(X_{j\ low})) + P_{expected} * (\Sigma_{j=attributes} W_j * V_j(X_{j\ expected})) + P_{high} * (\Sigma_{j=attributes} W_j * V_j(X_{j\ high}))]$$

여기서 함수 $Vj(Xj)$ 는 속성 j 에 대한 각 속성가치 Xj 를 함께 합할 수 있도록 정규화한 것이다. 다속성 의사결정기법의 장점은 속성의 이질적인 단위들(시간단위, 화폐단위, Likert 척도 등)을 정규화해서 속성가중치에 따라서 가중치 Wj 를 부여하여 함께 합할 수 있다는 것이다. 보안관리자는 위험에 대해서 중립적이라는 가정을 하고 있으나, 만약 보안관리자의 위험에 대한 태도가 위험회피 혹은 위험추구라면 이에 따른 효용함수를 도출하여 적용해야 한다.

3.5 감도분석

가산형 다속성함수를 도출하는 마지막 단계는 감

도분석을 실행하는 것이다. 감도분석의 목적은 기존 분석이 주요 변수들에 대한 보안관리자들의 불확실성 범위에 얼마나 민감한지를 결정하는 것이다. 본 연구에서는 다음과 같은 3가지의 감도분석인 위험속성의 손실추정치, 위험속성의 가중치, 위협의 발생확률추정치를 재검토해 볼 수 있다. 보안 관리자는 가장 발생확률이 높은 값뿐만 아니라 상한과 하한 값도 함께 추정하게 되는데, 이를 통해서 확률밀도함수(probability density function)를 도출하여 감도를 분석할 수 있다. 이러한 감도분석의 이점은 보안관리자의 불확실성이 각 위협의 우선순위에 얼마나 영향을 주는지 알 수 있다는 것이다.

4. 사례연구

본 사례연구 대상인 A기업은 일반 소비자 대상의 인터넷 쇼핑몰을 운영하고 있는 업체로서, 전자제품과 일반 생활용품등을 판매하고 있다. 2001년 기준으로 종업원은 25명이며, 연간 매출액은 약 15억원 이였다. 이 회사는 보안관리자를 따로 두지는 않고 있으며, 시스템관리자가 DBA(데이터베이스 관리자)와 보안관리자의 업무를 겸하고 있다. 시스템의 보안을 위해서는 OS와 DBMS, 라우터 등에서 기본적으로 제공하고 있는 기능 이외에는 방화벽(fire wall)을 설치하고 있어서, 소규모 업체이지만 나름대로 보안관리를 위해 노력하고 있는 회사이다.

하지만 이 회사는 아직 자체적으로 시스템 공격에 대한 자료는 축적하고 있지 않으므로, 본 사례연구를 위해서는 우리나라의 평균적인 값을 적용하고자 하며, 이를 위해서 구체적으로 한국정보보호진흥원(KISA)에서 발표한 자료를 이용한다. 한국정보보호진흥원(KISA) 내에 침해사고대응팀(CERTCC-KR; KOREA Computer Emergency Response Team Coordination Center, http://cert.certcc.or.kr/)의 침해사고 통계분석보고서에 의하면, 2002년에 위협에 의해서 신고 된 침해유형에 따른 불법행위의 빈도는 [표 1]과 같다. 발생빈도 관점에서 보면 침입시도, 불법침입, 불법자원사용, 자료변조삭제, 서비스 거부 순으로 발생건수가 많다. 악성 프로그램을 이용한 침입시도 및 불법침입이 많다. 특히 트로이 목마를 이용한 침입시도 및 불법침입 증가와 함께 네트워크 공유설정에 있어 패스워드를 설정하지 않거나 쓰기권한까지 부여한 시스템을 대상으로 한 불법침입이 증가했다.

참고로 2002년도 피해신고 접수된 해킹사고가 15,192건, 바이러스가 38,677건, 해킹시도탐지 22,036건이고, OS 관점에서는 6,444건 중에서 Windows가 4,377건이다.

표 1. 침해유형에 따른 불법행위의 빈도

불법행위	빈도	%
침입시도	4,044	37.5
불법침입	3,364	31.2
자료유출	1	0.0
자료변조삭제	61	0.6
불법자원사용	3,296	30.6
홈페이지 변조	5	0.0
시스템 파괴	0	0.0
시스템 오류	2	0.0
서비스 거부	11	0.1
합계	10,784	100

자료: 한국정보보호진흥원(KISA)

A 회사의 보안관리자는 위와 같은 한국정보보호진흥원 침해사고 통계분석보고서를 근거로, 연간 공격빈도수 및 손실크기가 큰 불법행위(침입시도, 불법침입, 불법자원사용, 자료변조삭제, 서비스 거부)에 관심을 갖고, 이를 근거로 회사 조직 내에 보안위험을 계량적으로 평가해서 위협지수를 도출하여, 침해로 인한 손실에 대한 대응책을 수립하려고 한다. 이를 위해 위험분석자로서 보안관리자에게 위협의 집합으로서 불법행위의 빈도자료를 제시하였으며, 보안관리자가 제공하는 위협관련 정보를 기록하고, 인터뷰하고, 위협지수를 계산하고, 감도분석을 실행하였다.

4.1 다속성에 대한 가산성 가정의 검토

위협으로 발생되는 직접손실에는 수익감소, 고객상실, 생산성감소, 복구비용 등이 있고, 간접손실에는 자금흐름의 정지, 고객대기시간의 손실, 대외 신인도 하락 등이 있다. A 회사의 보안관리자는 회사 내의 정보자산에 대한 공격의 결과로 예상되는 위험속성들로서, 수익감소, 고객 상실, 생산성 감소, 복구비용 등 네 가지 직접손실을 고려했다. 이러한 네 가지 손실속성들 간에는 종속적인 관계가 없는 독립적인 속성들로 식별되고, 가산성 가정을 충족한다고 판단된

다. 나머지 3가지 가정들도 앞에서 검토한 대로 본 연구에 적용 가능할 만큼 만족되었으므로, 다음 단계의 분석을 계속 진행할 수 있다.

4.2 단일속성함수의 평가

한국정보보호진흥원에서 파악한 9개 불법행위 중에서 침입시도, 불법침입, 불법자원사용은 빈도수가 매우 높으므로, 그리고 자료변조 삭제 및 서비스 거부는 빈도수는 낮지만 손실 강도(severity)가 매우 높으므로 분석대상에 포함시켰다. 주된 관심대상이 되는 5개 불법행위들로 인한 위험속성은 다양한 손실단위로 측정될 수 있다. 고객상실과 복구비용은 7점(0점 - 6점) Likert 척도로 측정했고, 수익감소는 화폐가치(원)으로, 생산성 감소는 시간(시)으로 측정했다. 보안관리자는 위험결과에 대한 속성가치, 즉 손실수준의 상한과 하한을 먼저 추정한 후에, 평균을 추정했다. 주된 관심대상인 5개의 위협으로 인한 불법행위들의 손실크기를 4가지 위험속성 관점에서 3점 척도(최소, 평균. 최대)로 측정했다.

표 2. 불법행위의 빈도와 손실수준

불법행위 (건/년)		수익감소 (1000원)	고객상실 (7점척도)	생산성 감소 (시간)	복구비용 (7점척도)
침입시도 (4,044/년)	최소	0	0	0	0
	평균	0	0	0	0
	최대	0	0	0	0
불법침입 (3,364/년)	최소	0	0	0	0
	평균	0	0	0	1
	최대	0	0	0	2
불법자원사용 (3,296/년)	최소	0	0	0	1
	평균	1,000	2	2	2
	최대	10,000	5	40	3
자료변조삭제 (61/년)	최소	0	1	8	2
	편균	20,000	4	100	4
	최대	100,000	6	250	6
서비스 거부 (11/년)	최소	0	2	10	3
	평균	20,000	4	150	4
	최대	60,000	6	200	6

한국정보보호진흥원(KISA)에서 통계분석하고 있는 불법행위들의 속성들은 서로 종속적이다. 즉 침입시도를 통해서 불법침입이 있고, 그 후에 불법자원사용 혹은 자료변조삭제 혹은 서비스 거부가 발생되므로, 하나의 침입사고 내에 다수의 불법행위가 발생하게 된다. 연속적인 시간에 따라서 불법행위들이 순차적으로 손실을 발생시키므로, 침입시도 자체로는 거의 손실이 발생되지 않지만, 침입 후에, 불법자원사용 혹은 자료변조 혹은 서비스 거부에 따라서 손실크기가 증가되는 경향이 있다.

4.3 가중치의 도출

보안관리자는 네 가지 위험속성에 대한 상대적 중요성을 나타내는 순위를 고객상실, 수익감소, 생산성 감소, 복구비용, 순으로 결정했다. 보안관리자에게 가장 중요한 관심대상이 되는 1순위 속성인 고객상실에 대해서 100점을 부여하고, 나머지 속성들에 대한 순위의 상대적인 값을 1점에서 100점까지의 값으로 [표 3]와 같이 부여했다. 여기서 가중치의 합이 1이 되도록 표준화해서 가중치를 도출 한다.

표 3. 속성의 우선순위와 가중치

속성	순위	가중치
고객상실	100	0.42
수익감소	80	0.33
생산성 감소	40	0.17
복구비용	20	0.08
합계	240	1.0

4.4 위협지수의 도출

표 4. 위협지수

불법행위	최소 P_{low}=0.1	평균 P_{lexp}=0.89	최대 P_{high}=0.01	위협지수
침입시도	0	0	0	0
불법침입	0	79.8	1.8	81.6
불법자원사용	8.8	858.1	30.1	897.0
자료변조삭제	1.0	63.1	2.3	66.4
서비스거부	0.3	11.8	0.3	12.4
합계	10.1	1012.8	34.5	1057.4

위험분석자는 보안관리자와의 인터뷰를 근거로 불법행위들이 회사 내에서 얼마나 자주 발생하는지를 평균, 최대, 최소(P_{exp}, P_{high}, P_{low}) 등 세 가지 확률 값

으로 추정했다. 위협지수 TIa 는 각 위협별로 상대적인 중요도를 가중평균해서 구한 것으로서 측정단위가 존재하지 않는다. 위협지수에 의해서 상대적으로 어떤 위협의 잠재손실이 얼마나 큰지 식별할 수 있다. 또한 위협지수들의 합계를 구해서 다른 정보시스템의 위협과도 비교할 수 있다.

4.5 감도분석

감도분석의 목적은 주요 변수에 대한 보안관리자의 불확실성의 범위가 얼마나 민감한지를 분석하는 것으로, 다속성 위험평가의 세 가지 추정치인 위험속성의 손실추정치, 위험속성의 가중치, 불법행위 발생확률추정치를 재검토한다. 추정된 공격빈도 측면에서 연구대상이 된 불법행위의 빈도 순위는 침입시도, 불법침입, 불법자원사용, 자료변조삭제, 서비스 거부 순으로 많았지만, 다속성 위험평가 결과로 계산된 위협지수는 불법자원사용, 불법침입, 자료변조삭제, 서비스 거부, 침입시도 순으로 높았다. 이와 같은 순위차이는 보안관리자의 주관적인 추정치인 불법행위들에 대한 위험속성의 손실추정치, 위험속성 간 상대적 중요도인 가중치 추정치, 불법행위에 대한 3가지 발생확률 추정치 때문에 발생된 것이기 때문에, 이와 같은 순위차이를 이해하기 위해서 보안관리자와 입력자료 및 추정치에 대한 일관성을 재검토했다. 위험관리자의 추정치에 대한 불확실성이 위협지수의 순위에 얼마나 영향을 주는지 검토하기 위해서, 일관성이 결여된다고 주관적으로 판단되는 추정치에 대해서만 부분적으로 what if 분석을 시행했다. 즉 세 가지 추정치 중에서 두 가저 추정치를 고정시키고, 나머지 한 가지 추정치들 중에서 보안관리자의 재 추정치를 반복적으로 입력시켜서 위협지수의 순위변화를 관찰했다.

먼저 손실 추정치에 있어서, 가장 높은 위협지수를 보이고 있는 불법자원사용의 경우, 평균적인 고객상실을 2로 평가 하였는데, 재검토 하였을 때 이를 1로 평가하였다. 이 경우 불법자원사용에 대한 위협지수를 다시 계산해 보면 589.0이 되어서 308.0만큼 감소하였다. 이는 매우 큰 감소이기는 하지만 2순위인 불법침입의 81.6보다는 월등히 높은 값 이여서, 1순위와 2순위의 상대적인 서열은 그대로 유지되는 것으로 나타났다. 하지만 세번째 순위를 보이고 있는 자료변조삭제는, 평균 수익감소가 첫번째 추정에서는 2천만원이였으나 재검토시에는 3천만원으로 변경되었는데, 이 경우는 위협지수가 81.3으로 15.7이나 높아져서 2순위인 불법침입보다 불과 .3만큼 적은 값이 된다. 물론 이 경우도 순위가 바뀐것은 아니지만, 그 차이가 아주 미미해서 순위가 바뀔 가능성이 커지게 된다. 따라서 보안관리자는 보안대책 수립을 위한 의사결정시에 이러한 2위와 3위의 순위가 변경될 수 있다는 가능성을 충분히 고려하여야 한다.

다음으로 속성 우선순위 가중치의 경우 재검토에서 수익감소를 80에서 70으로 변경하였다. 이 경우 속성의 가중치는 다음 표5와 같이 변경된다. 따라서 새로운 가중치를 적용하여 위협지수를 다시 계산하면 불법자원사용 940.0, 불법침입 91.8, 자료변조삭제 79.0, 서비스거부 12.3, 침입시도 0으로, 거의 모든 위협지수가 다소 높아졌지만 순위에 영향을 줄 만한 변화는 찾아볼 수 없었다. 따라서 이 가중치의 경우는 추정치가 어느 정도 변화하더라도 결과에는 거의 영향을 미치지 않으므로, 감도분석에 비교적 안정적인 결과를 보이고 있다.

불법행위의 발생확률 추정치는 시례회사에서 축적된 통계치를 적용하는 것이 바람직하지만, 현실적으로 그러한 자료를 유지관리하고 있지 않아서 한국정보보호진흥원에서 발표한 우리나라 전체 통계치를 적용하였으므로, 이 값은 추정의 오차는 없다고 보아야 한다. 하지만, 우리나라 전체의 통계치와 사례회사의 실제 불법행위 발생분포는 차이를 보일 수 있으므로, 결과 해석 시에 이에 대한 고려가 요구된다.

표 5. 속성의 우선순위와 가중치(두번째 추정결과)

속성	순위	가중치
고객상실	100	0.44
수익감소	70	0.30
생산성 감소	40	0.17
복구비용	20	0.09
합계	230	1.0

결론적으로 이러한 3가지 추정치의 감도분석결과, 1, 2 순위간에는 변동 가능성이 거의 없으나, 2, 3 순위 간에는 변동 가능성이 어느정도 있는 것으로 나타났다. 따라서 보안시스템 강화를 위한 의사결정시에, 이를 고려하는 것이 바람직 할 것으로 판단된다.

3. 결론

보안관리자들에게 다속성 위험평가 모형인 위협지수는 반복 사용할 수 있는 체계적인 보안관리도구로서, 위협의 크기를 식별하는데 큰 도움을 줄수 있다. 이 절차를 실제 사례를 통해 적용한, 본 연구의 요약 및 연구의 한계와 미래 연구방향은 다음과 같다.

첫째, 한국정보보호진흥원(KISA)의 침해사고통계에서 불법행위들 중에서 침입시도, 불법침입, 불법자원사용, 자료변조삭제, 서비스 거부 순으로 발생빈도가 많으나, 위협지수 계산 결과로는 불법자원사용, 불법침입, 자료변조삭제, 서비스 거부 순으로 위험이 많은 것을 알 수 있다.

둘째, 사례에서 네 가지 위험속성인 수익감소, 고객상실, 생산성 감소, 복구비용이 파악되었으며, 각 독립적인 속성들에 대한 이전성, 선호 독립성, 차별 독립성, 절충 독립성 등 가산성 가정이 성립되는 경우에는 가산형 다속성함수를 이용해서 위협지수를 도출할 수 있다.

셋째, 각 속성들의 측정단위가 화폐 및 시간 단위, Likert 척도 등 서로 다르게 측정되어도 표준화하고 가중평균해서 구한 위협지수들을 통해서 개별 위협의 상대적 중요성을 파악 할 수 있다.

네째, 위협지수의 상대적 크기 순으로 보안대책을 구축하는 효율적인 보안전략을 수립 할 수 있다.

현재 한국정보보호진흥원(KISA)의 침해사고통계에서 불법행위들의 분류속성인 침입시도, 불법침입, 불법자원사용, 자료변조삭제, 서비스 거부 등은 위협의 공격으로 시스템을 침투하는 과정 중에 발생되는 불법행위의 침해정도를 나타내고 있다. 이러한 불법행위의 분류체계가 이론적인 위협의 분류체계와 다소 상이하고, 서로 종속적인 것이 본 연구의 제약이다. 앞으로 이와 같은 다속성 위험평가모형에 대한 연구는 위협지수의 상대적인 크기를 서로 비교해서, 보안대책들 혹은 조직(기관)들의 상대적 보안위험의 중요도를 분석하는데 활용할 가치가 있다. 또한, 재해통계자료에 적용해서 재해별 재해지수를 계산하여 상대적 중요도에 따라 재난복구대책을 수립하는데 이용할 수 있으므로 그 활용범위가 매우 넓다.

[참고문헌]

[1] 한국정보보호진흥원(KISA), 통계 분석보고서, 2002년 12월. http://cert.certcc.or.kr

[2] Edward, W., "How to Use Multiattribute Utility Measurement for Social Decision-Making," IEEE Transactions on Systems, Man and Cybernetics, 7(5) pp.326-340, 1977.

[3] Keeney, R. L. and Raiffa, H., Decision with Multiple Objectives, Wiley, 1999.

[4] Robert T. and Terence Reilly, *Making Hard Decisions*, Duxbury, Clemons, 2001.

[5] Shawn A. Butler, "Security Attribute Evaluation Method: A Cost Benefit Approach," *24th International Conference on Software Engineering Proceedings,* pp. 22-240, May 2000.

[6] Shawn A. Butler and Paul Fischbeck, "Multi-Attribute Risk Assessment," *Technical Report CMU-CS-01-169,* December 2001.

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