Journal of the Korean Data & Information Science Society
2011, **22**(2), 207–215

한국데이터정보과학회지

정보 보안 위험: 컨조인트분석 활용 사례 연구[†]

박노진[1] · 이동훈[2]

[1]단국대학교 정보통계학과 · [2]고려대학교 정보경영공학전문대학원

접수 2011년 1월 2일, 수정 2011년 2월 11일, 게재확정 2011년 3월 2일

요 약

정보 자산에 대한 위험 분석은 주로 한국정보통신기술협회나 국제표준화기구의 표준에 따라 이루어지고 있다. 그 과정은 자산분석, 위협분석, 취약성분석, 대응책분석의 순서로 이루어져있다. 이 과정은 분석 대상, 즉 자산을 명확히 파악하는 것부터 시작된다. 기존의 방법은 그 대상을 물리적 자산에 따라 분류하는 것이 일반적이다. 한편, 국제결제은행 규약이 제시하는 방법에 따르면 위험 분석의 대상을 운영에 따른 분류를 통해 규명하게 된다. 본 논문에서는 물리적 자산 중심의 기존 방법과 더불어 업무 중심의 분석 방법이 유용할 수도 있음을 보이고자 하였다. 컨조인트 분석 기법을 활용하여 상황에 따라 물리적 자산 중심의 방법과 업무 중심의 방법의 유용성의 차이를 예를 들어 분석하였다.

주요용어: 국제결제은행, 운영 위험, 위험 분석, 정보 보안, 컨조인트 분석.

1. 서론

정보시스템에 어떤 위협이 발생하여 손실이 발생하는 과정을 그림 1.1에 그려 보았다. 위험분석은 자산, 위협, 취약성, 영향을 고려하여 위험을 측정하는 과정을 의미하며, 측정된 위험의 수준을 원하는 수준으로 낮추기 위해 보호대책 프로파일을 제공하는 것을 위험평가라고 한다. 한편, 위험분석과 위험평가를 통칭하여 위험관리라고 한다 (한국정보보호진흥원, 2002). 위험분석은 적용하고자 하는 조직과 환경에 따라 다양한 방법론에 의해 수행될 수 있으며 적절한 방법론을 선택하는 것이 중요하다. 위험분석 방법론은 결과의 성격에 따른 분류와 요구사항에 따른 분류로 나눠진다. 기존 방법의 개념과 유형, 장단점을 표 1.1에 정리하였다. 두 방법의 근본적인 차이는 손실을 정량적으로 계산할 것인가와 그렇지 않으면 정성적으로 계산할 것인가 하는 점에 있다. 정량적으로 손실이 얼마라고 할 수 만 있다면 좋겠으나 자산의 가치를 측정하는 것이 반드시 정량적으로 이루어질 수 없는 측면이 있다. 자산에 대한 평가 혹은 감정도 역시 주관적인 면이 있고 자산을 정성적으로 혹은 상대적으로 측정해야 하는 경우가 있다. 상황에 따라서 두 가지 방법을 적절히 혼합하여 사용하는 것이 적절해 보인다.

그런데, 어느 방법을 사용하던지 공통적으로 자산을 확인하는 과정이 우선되어야 하는데 그 과정에 몇 가지 어려운 점이 있다. 무엇 보다 모든 자산을 분석한다는 것이 물리적으로 불가능할 수 있다는 것이고 자산의 가치에 대한 평가가 시점과 장소에 따라 달라질 수도 있다는 것이다 (Ahn과 Jo, 2003). 한편, 정보시스템의 궁극적 목적은 원활한 정보 서비스의 수행에 있다고 할 때, 정보시스템에서 자산을 파악하는 것도 중요하지만 업무의 흐름을 파악하고 그에 따른 시스템의 위험을 파악하는 것도 중요하다고 보인

[†] 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다.
[1] 교신저자: (448-709) 경기도 용인시 수지구 죽전동, 단국대학교 정보통계학과, 교수.
E-mail: rjpak@dankook.ac.kr
[2] (101-712) 서울특별시 성북구 안암동, 고려대학교 정보경영공학전문대학원, 교수.

다 (한국정보보호진흥원, 2002). 자산에 대한 위협이 가해지고 취약한 부분에서 문제가 발생하여 업무의 중단 혹은 지연이 발생하면 바로 그것이 손실을 발생하게 되는 것이다. 따라서, 정보 시스템에 대한 위험 분석을 자산 중심에서 업무 중심으로 파악하는 것도 한 가지 방법이라고 생각된다. 금융기관에서는 약간 다른 의미의 위험분석이 업무 중심으로 이루어지고 있다 (김종호, 2001).

위에서 언급하였듯이 위험분석의 대상을 자산 중심으로 하는 것과 업무 중심으로 하는 것에 대한 의견이 존재하고 있다. 본 연구는 먼저 금융기관에서 수행하고 있는 업무 중심의 위험분석을 간단히 소개하고 기존의 자산 중심의 분석과 업무 중심의 분석을 비교하기 위해 컨조인트 분석에 의한 간단한 실험을 통해 그 차이를 실증하였다. 분석의 결과를 간단히 서술하면, 본 연구의 예에서는 시스템에 대한 위협 (혹은 침해)에 관심이 있는 경우 자산의 물리적 분류에 중요성이 있었고 시스템에 대한 보안에 관심이 있는 경우에는 운영상의 분류가 더 의미가 있음을 파악할 수 있었다. 그렇다면 예로 주어진 시스템의 경우, 물리적 자산에 주어지는 위협에 대한 대비와 그로인한 운영상의 손실을 줄이기 위한 보안 방법을 적절히 설정하는 것이 요구된다고 하겠다.

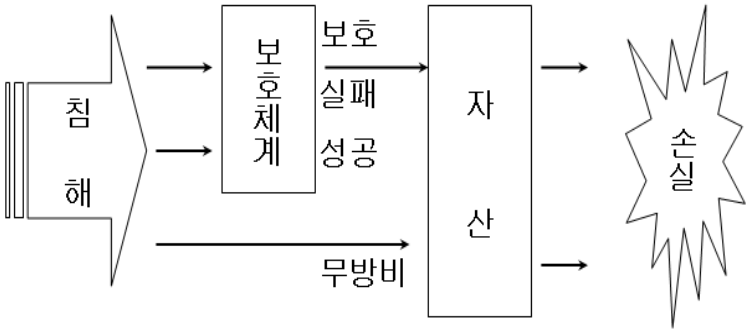

그림 1.1 자산에 대한 침해, 보호 그리고 손실의 관계

표 1.1 정량적/정성적 방법의 비교

구분	정량적방법(Quantitative Approach)	정성적방법(Qualitative Approach)
개념	-기대위험가치 분석을 위험발생확률과 손실크기를 통해 계량적으로 산출한다.	-손실크기를 화폐가치로 표현하기 어렵다 -위험크기는 기술변수로 표현한다.
유형	-수학공식 접근법 -확률분포 -퍼지 행렬법 -몬테카를로 시뮬레이션 -과거자료 분석법	-델파이법 -시나리오법 -순위결정법 -퍼지 행렬법 -질문서법
척도	연간기대손실(ALE)	점수 (5점척도, 10점척도)
장점	-비용, 가치 분석, 예산기회, 자료 분석이 쉽다.	-금액화하기 어려운 정보의 평가가 가능하다. -분석시간이 짧고 이해가 쉽다.
단점	분석의 시간, 노력, 비용이 크다	평가 결과가 주관적이어서 사용자에 따라 달라질 수 있다.
도구	-BDSS -RISKCALK -RISKWATCH -AnalyZ -RANK-KE -LRAM	-CRAMN -LAVA -RISKPAC -MARION -NetRISK

2. 연구 배경 및 방법

2.1. 운영위험

NBA (New Basel Accord)는 1988년에 체결된 기존의 BIS (국제결제은행)협약을 보완한 것으로 은행을 비롯한 금융기관에 많은 변화를 요구하고 있다. NBA와 기존의 BIS협약 사이의 차이점은 운영위험 (operational risk)이 추가된 점이다. 운영위험은 '부적적하거나 잘못된 내부의 절차, 인력, 시스템 및 외부 사건으로 발생한 손실의 위험으로 법률위험은 포함하나 전략위험과 평판위험은 배제한다.' 라고 정의된다 (BCSB, 2004). BIS는 금융 기관의 사업 분야를 ① 투자금융, ② 트레이딩과 매매, ③ 소매금융, ④ 기업금융, ⑤ 지급과 결제, ⑥ 대행서비스, ⑦ 자산관리, ⑧ 소매중개의 여덟 가지 사업 분야로 나누고 운영위험을 발생시키는 사건을 (1) 내부사취, (2) 외부사취, (3) 고용관행과 작업장 안전, (4) 고객, 상품과 사업관행, (5) 유형자산의 손실, (6) 사업방해와 시스템손실 그리고 (7) 체결, 인도 및 과정관리와 같은 일곱 가지로 분류한다.

따라서 금융기관에서는 7×8가지의 사업 영역과 사건간의 조합이 정의되고 각각의 조합에 대한 손실을 파악하는 과정을 통해 위험을 관리하는 방법을 사용하고 있다 (조하현 등, 2004). 7×8가지 조합에 더불어 네 가지 원인 (과정, 사람, 시스템, 외부요인)을 추가한 그림 2.1과 같은 3차원 구조 속에서 위험을 관리하는 방법이 요구되기도 한다 (장욱, 2004).

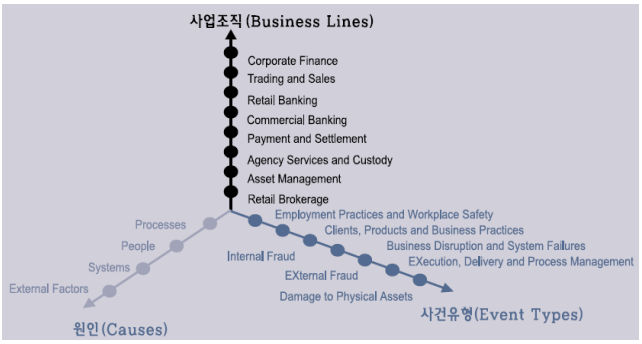

그림 2.1 운영위험 3차원 구조(출처: 장욱, 2004, p72)

몇 가지 정보 시스템의 업무 영역을 분류하면 예를 들어 표 2.1과 같다 (Kim과 Kim, 2008; Park 등, 2008; 신종민과 최덕원, 2000; 오상렬 등, 2002, 주철민 등, 1999). 한편, 정보시스템과 관련된 사고는 그림 2.2와 같이 웜·바이러스, 해킹신고처리 등 여덟 가지로 분류할 수 있겠다 (한국인터넷진흥원, 2010).

예를 들어, 국방관련 시스템의 경우 네 가지 업무분야와 여덟 가지의 사건을 고려할 수 있고 총 32 가지 조합의 손실이 가능하다고 하겠다. 각 32개 조합 그림 2.3에 해당하는 손실을 계산하여 합하면 전체 시스템의 손실을 구할 수 있겠다.

2.2. 컨조인트 분석

그럼 과연 업무별 분석이 정보시스템을 분석하는데도 도움이 되는가를 알아보기 위해 간단한 실험을 하고자 한다. 전문가들에게 자산별 분류에 의한 손실 예측과 업무별 분류에 의한 손실 예측을 의뢰하고 그 결과를 분석하여 어느 방법이 손실을 예측하는데 더 효과적인가를 규명하고자 한다. 통계학에서 이

표 2.1 업무 분류표 예시

	교육	군사	금융	병원	중소기업
업무영역	교무 학사 인사 회계 물품 시설	기획 획득 인사 기타 (정훈, 군사시설, 동원 등)	수신 여신 외환 카드 자금운용 공통 고객정보 대행업무 기타	환자진료 환자간호 약품조제 /제제 진료비 수납 /청구	인사 회계 영업 무역 생산 구매 자재 품질 원가

구분	2009년 총계	2010												2010년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
웜 · 바이러스	10,395	932	1,302	1,085										3,319
해킹신고처리	21,230	898	1,076	1,053										3,027
-스팸릴레이	10,148	154	317	222										693
-피싱 경유지	988	78	106	116										300
-단순침입시도	2,743	232	230	345										807
-기타해킹	3,031	223	233	267										723
-홈페이지 변조	4,320	211	190	103										504
악성 봇(Bot)	1.0%	0.6%	0.6%	0.7%										0.6%

그림 2.2 월간 침해 사고 통계-예시

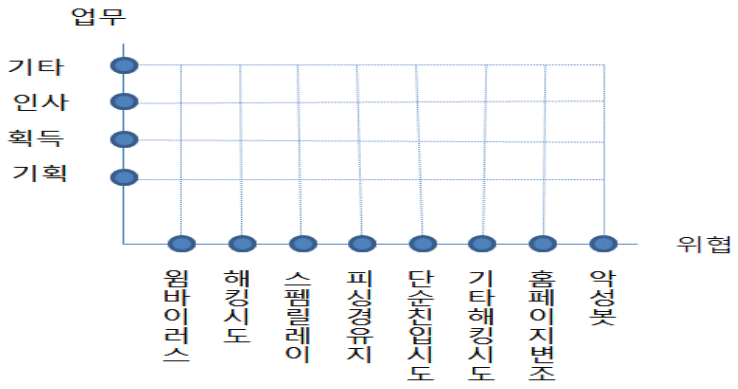

그림 2.3 국방 분야 업무/위협 이차원 그림 예시

런 종류의 실험을 수행하는 방법으로 컨조인트 분석이 사용되는데 간단히 그에 대해 설명하고 사례를 들어 분석을 수행하도록 하겠다.

컨조인트분석은 본래 마케팅조사에서 특정상품에 대하여 소비자들이 가장 중요하게 생각하는 특성을 찾아내는 방법 (이훈영, 2005)으로서 생산 (지혜영과 조완현, 2009), 소비자 (민완기 등, 2000)와 교육 (Hur와 Pak, 2007)과 관련된 여러 분야에서 활용되고 있다.

컨조인트분석의 분석 절차는 ① 특정상품에 대해 소비자들이 원하는 몇 가지 특성들을 서로 다양하게 결합하여 여러 가지 가상 상품을 만든다. ② 응답자들이 구매를 희망하는 순위를 정하게 한다. ③ 순위를 이용하여 특성들의 효용도와 중요도를 계산한다 (이훈영, 2005). 각 속성의 상대적 중요도는 속성들의 총효용을 특정 속성의 효용값으로 나누어 계산된다 (Levy, 1995). 본 연구에서는 손실 크기에 대한 순위를 조사하여 컨조인트 분석을 응용하고자 한다.

컨조인트 분석은 일종의 실험계획법으로서 식 (2.1)과 같은 모형을 기본으로 한다.

$$U_i = \beta_0 + \sum_{t=1}^{h_1} \beta_{1t} X_{1t} + \ldots + \sum_{t=1}^{h_k} \beta_{kt} X_{kt} + \epsilon_i, \tag{2.1}$$
$$h_j = m_j - 1,\ i = 1, 2, \ldots, n;\ j = 1, 2, \ldots, k$$

여기서 k는 속성의 수, n은 주 프로파일의 수, m_j는 j번째 속성의 수준 수이며, $X_{1t}, \ldots, X_{kt}$는 각 속성의 수준을 정의하는 지시변수이다. 식 (2.1)에서 추정치 $\widehat{\beta}_{1t}, \ldots, \widehat{\beta}_{kt}$를 구하면 j번째 속성의 t번째 수준의 부분가치는

$$a_{jt} = \begin{cases} \widehat{\beta_{jt}} & t = 1, \ldots, h_j \\ -\sum_{t=1}^{h_j} \widehat{\beta_{jt}} & t = m_j \end{cases}$$

가 된다. 한편, 각 속성의 중요도 r_j는 수준별 부분가치 범위의 상대적 비중인

$$r_j = \frac{w_j}{\sum_{j=1}^{k} w_j}, \quad w_j = \max_t(a_{jt}) - \min_t(a_{jt})$$

의 정의된다.

3. 분석 사례

D대학교의 전산센터 관계자들을 인터뷰하여 중요한 자산 (서버) 세 가지 (SUN Fire V880; SUN E25K; HP9000/L2000), 중요한 업무 세 가지 (학사/행정; 홈페이지; 사이버강의), 중대한 위협 세 가지 (DDOS; 악성프로그램; 사용자도용) 그리고 보안 방법 세 가지 (방어벽; 인증시스템; 암호화)를 결정하였다. 주어진 속성을 바탕으로 자산분류/업무분류에 대한 아홉 가지 조합 (프로파일)을 정하였다 (표 3.1 - 표 3.2). 이렇게 구성된 각각의 프로파일에 대하여 예상 손실 크기에 따른 순위를 1등부터 9등까지 기입하도록 하였다. 조사는 2010년 9월 13일부터 16일까지 연구자가 해당 전산센터를 방문, 배포 및 수거하였다. 모두 16명의 관계자들이 설문에 응답하였다. 기종에 따른 분석과 업무에 따른 분석에 다소 간의 차이가 있음을 알 수 있다 (표 3.3 - 표 3.4).

• 자산 분류에 따른 분석 (표 3.3)

. 위협이 손실을 예측함에 가장 중요한 요인으로 나타남-기종별 분류가 손실과 관련하여 응답자들에게 가장 중요한 요인이 아님

. 위협이 보안 보다 중요하다고 나타남-기종이라는 명확한 물리적 대상이 존재함으로 위협의 대상이 명확하기 때문이라고 사려됨

. DDOS가 가장 위협적이고 인증시스템이 손실을 발생시키기에 영향력 (즉, 손실을 효과적으로 막지 못하는)이 있음-DDOS에 대한 효용이 가장 큰 양수임으로 DDOS가 손실을 크게 만드는데 가장 영

향을 미치는 위협임

- 업무 분류에 따른 분석 (표 3.4)

▪ 업무의 구분이 손실을 예측함에 가장 중요함-손실을 판단함에 있어 업무별 분류가 효과가 있음
▪ 보안이 위협 보다 중요하다고 나타남-업무라는 무형적 대상에 대하여는 위협의 방향이 모호하여 방어적 자세를 취함
▪ 업무 중 학사/행정지원이 손실이 가장 클 것으로 예상됨. 악성프로그램이 가장 손실을 크게 유발하고 방어벽이 손실에 대처하는 가장 효과적인 수단으로 보임

실제로 업무의 구분을 통한 분석이 자산 (기종)별 분석 보다 손실을 예측함에 있어서 중요함을 알 수 있다. 실시된 조사에 국한하여 볼 때, 전제 시스템을 업무별로 나누어 고려하는 것이 손실을 분석함에 있어 자산을 구분하여 분석하는 경우 보다 현실적으로 효과적이라고 할 수 있겠다. 자산에 관하여는 위협이, 업무와 관하여는 보안이 손실과 관련하여 우선하는 중요한 요인으로 보인다. 위협의 분명한 목적지가 구분 가능한 자산 분류에 의한 손실 분석에서는 위협의 존재가 중요하고 업무라는 무형적 개념에 관하여는 보안이 보다 현실적으로 중요하다는 의미로 받아드릴 수 있겠다. 가능하다면 자산 (기종)과 해당 자산이 수행하는 업무를 파악하여 위험분석을 (자산, 업무)로 짝을 지어 위협과 그에 대한 보안을 동시에 고려하는 것이 바람직해 보인다.

표 3.1 자산분류에 의한 프로파일

서버	위협	보안
SUN Fire V880	DDOS	방어벽
SUN Fire V880	사용자도용	인증시스템
SUN Fire V880	악성프로그램	암호화
HP9000/L2000	DDOS	인증시스템
HP9000/L2000	사용자도용	암호화
HP9000/L2000	악성프로그램	방어벽
SUN E25K	DDOS	암호화
SUN E25K	사용자도용	방어벽
SUN E25K	악성프로그램	인증시스템

표 3.2 업무 분류에 의한 프로파일

업무	위협	보안
사이버강의	악성프로그램	방어벽
SUN Fire V880	사용자도용	암호화
사이버강의	DDOS	암호화
HP9000/L2000	악성프로그램	인증시스템
HP9000/L2000	악성프로그램	암호화
사이버강의	사용자도용	인증시스템
SUN E25K	사용자도용	방어벽
SUN E25K	DDOS	인증시스템
SUN E25K	DDOS	방어벽

4. 결론

전산 관련 위험을 측정 및 관리함에 있어서 대부분의 방법이 자산의 분류에 따른 분석을 사용하고 있

표 3.3 자산분류에 따른 컨조인트 분석 결과

요인	속성	효용	중요도
기종	SUN Fire V880	-.062	36.170
	HP9000/L2000	.563	
	SUN E25K	-.500	
위협	DDOS	1.021	57.447
	사용자도용	-.667	
	악성프로그램	-.354	
보안	방어벽	-.062	6.383
	인증시스템	.125	
	암호화	-.063	

표 3.4 업무분류에 따른 컨조인트 분석 결과

요인	속성	효용	중요도
업무	학사/행정지원	1.111	58.015
	홈페이지 관리	-.5783	
	사이버 강의	-.533	
위협	DDOS	-.089	7.634
	사용자도용	-.044	
	악성프로그램	.133	
보안	방어벽	-.533	34.351
	인증시스템	.067	
	암호화	.467	

다. 본 연구는 금융기관에서 사용하는 운영위험과 같이 업무에 따른 손실을 측정하여 위험을 관리할 것을 제안하였다. 실제로 자산 혹은 업무에 따른 위험을 고려하는 것이 어떤 차이가 있는가를 보기 위해 컨조인트 분석을 활용하여 보았다. 사례 연구 결과 위험 분석의 대상이 자산인지 업무인지에 따라 위협과 보안을 고려하는 수준이 다름을 볼 수 있었다. 자산을 중심으로 하는 위험관리는 그 목적이 위협으로부터의 시스템 안정성이라면 업무 중심의 위험관리는 위협 상황에서의 적절한 보안을 통한 시스템의 지속성이 그 관심사라고 할 수도 있겠다. 따라서, 시스템에 대한 위협 (혹은 침해)에 관심이 있는 경우 자산의 물리적 분류에 중요성이 있었고 시스템에 대한 보안에 관심이 있는 경우에는 운영상의 분류가 더 의미가 있음을 파악할 수 있었다. 그렇다면 예로 주어진 시스템의 경우, 물리적 자산에 주어지는 위협에 대한 대비와 그로인한 운영상의 손실을 줄이기 위한 보안 방법을 적절히 설정하는 것이 요구된다고 하겠다. 즉, 두 가지 분석 방법의 적절한 결합을 통해 바람직한 위험관리가 가능할 것이라고 하겠다.

참고문헌

김종호 (2001). 운영위험의 중요성과 측정방법. <대은경제리뷰>, 2001년 3월호.

민완기, 권세혁, 장송자 (2000). 컨조인트 분석을 이용한 전자상거래에서의 소비자 구매 결정에 관한 연구. <한국데이터정보과학회지>, **11**, 347-357.

신종민, 최덕원 (2000). 군사 운영 체계에서의 XML 도입 및 활용을 위한 정보 시스템 계획. <대한산업공학회/한국경영과학회 2000 춘계공동학술대회 논문집>, 449-452.

오상렬, 김현준, 김영철 (2002). 중소기업 ERP시스템 구축 사례 연구- I 기업을 중심으로. <한국산업정보학회 2002년도 추계공동학술대회 논문집>, 279-295.

이훈영 (2005). <이훈영교수의 마케팅조사론>, 도서출판 청람, 서울.

장욱 (2004). 운영리스크관리 실패사례 연구. <금융리스크리뷰>, 2004년 겨울호.

조하현, 이승국, 김종호 (2004). <운영리스크-측정과 관리>, 서울, 세경사.

주철민, 조증성, 남호수 (1999). 섬유산업의 재고관리를 위한 정보시스템 구축에 관한 사례연구. <한국데이터정보과학회지>, **10**, 271-277.

지혜영, 조완현 (2009). 컨조인트 분석을 이용한 휴대폰 속성 분석. <한국데이터정보과학회지>, **20**, 695-703.
한국정보보호진흥원 (2002). <위험분석도구 선정지침 연구보고서>, 한국정보보호진흥원, 서울.
한국인터넷진흥원 (2010). <인터넷 침해사고 동향 및 분석 월보>, 2010년 3월호.
An, C. S. and Jo, S. G. (2003). A case study of business process centered risk analysis for information technology security. *IE Interfaces*, **16**, 421-431.
Basel Committee on Banking Supervision (BCBS)(2004). *Basel II: International convergence of capital measurement and capital standards: A revised framework*, Bank for international Settlements.
Hur, J. S. and Pak, R. J. (2007). Conjoint analysis for the preferred subjects of elementary school computer education. *Journal of the Korean Data & Information Science Society*, **18**, 357-364.
Kim, J. S. and Kim, W. S. (2008). The effects of the next-generation system in the banking industry on the simplification of business processes and the development of new products. *Information Systems Reviews*, **10**, 159-177.
Levy, D. S. (1995). Modern marketing research techniques and the property professional. *Property Management*, **13**, pp 33-40.
Park, C. S., Lee, H. U. and Koh, S. H. (2008). A study on the hospital information systems usability evaluation. *Information Systems Reviews*, **10**, 289-311.

Journal of the Korean Data & Information Science Society
2011, **22**(2), 207–215

한국데이터정보과학회지

Information security risk: Application of the conjoint analysis [†]

Ro Jin Pak[1] · Dong Hoon Lee[2]

[1]Department of Information Statistics, Dankook University
[2]Graduate school of Information Management Security

Received 2 January 2011, revised 11 February 2011, accepted 2 March 2011

Abstract

This Risk analysis on information related assets is conducted primarily according to the standards the Korea Information and Telecommunications Technology Association (TTA) or the International Organization for Standardization (ISO). The process is made of asset analysis, threat analysis, vulnerability analysis, and response plan analysis. The risk for information related assets belongs to the operational risks suggested by BIS (Bank for International Settlements) and the information related losses can be estimated in terms of BIS' suggestion. In this paper it is proposed that how to apply the method proposed by BIS to estimate the loss of information assets.

Keywords: BIS, conjoint analysis, information security, operational risk, risk analysis

[†] This work was partially supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract.
[1] Corresponding author: Professor, Dept. of Information Statistics, Dankook University, Yongin 448-701, Korea. E-mail: rjpak@dankook.ac.kr
[2] Professor, Graduate School of Information Management Security, Korea University, Seoul 136-701, Korea.