情報保護學會論文誌
第12券 第4號, 2002. 8

대학교를 대상으로 한 위협에 따른 손실의 수치화

이 현 숙*, 변 진 욱**, 기 주 희**, 이 동 훈***, 임 종 인***, 박 영 우****, 윤 재 석****

Measure of the loss resulting from the threat in the University

Hyun Sook Rhee*, Jin Wook Byun*, Ju Hee Ki*, Dong Hoon Lee**,
Jong In Lim***, Young woo Park****, Jae Suk Yun****

요 약

본 논문에서는 대학교를 대상으로 하여 발생 가능한 위협을 분류하여 그에 따른 손실의 크기를 수치화 하는 방법론을 제시하고자 한다. 이러한 손실의 수치화는 경제학적 예측모델을 수립함으로서, 향후 동일한 피해 사례에 대한 예측을 용이하게 하여 손실비용을 최소화하는데 있어서 하나의 방법론이 될 수가 있다. 손실을 수치화 시키는 방법은 다음과 같은 단계로 나눌 수가 있다. 첫째로는 자산을 평가한다. 둘째로는 자산에 영향을 미치는 위협요소를 분류한다. 셋째로는 자산이 가지고 있는 취약성을 분석한다. 넷째로는 어떠한 위협요소가 자산에 손실을 발생시켰을 경우에 손실의 크기를 수치화 시킨다. 그러면 이렇게 수치화 시키는 방법을 예제를 통해서 설명하려고 한다.

ABSTRACT

In this paper we classify the possible threat and introduce the method that measures the loss resulted from the threat in the university. This is the method that the amount of the loss minimized in the case of the same quality in damage as establish a economical prediction model. The method of measuring the loss is as follows. First, asset should be clearly identified and valued. Second, threats which may result in harm to asset should be classified. Third, vulnerabilities which is weaknesses associated with asset should be analyzed. Fourth, measure the value of the loss. we explain the valued method by the example.

Keyword : *가치분석지수, 취약성 분석, 손실*

Ⅰ. 서 론

손실을 수치화 시키기 방법은 다음과 같은 단계로 나눌 수가 있다. 첫째로는 자산을 파악하여 그 가치를 평가한다. 자산에 대한 손실을 측정하거나 예측하기 위해서는 우선 자산에 대한 정의와 평가가 정확히 이루어져야 할 것이다. 둘째로는 자산에 영향을 미치는 위협요소를 분류한다. 셋째로는 자산이 가지고 있는 취약성을 분석한다. 넷째로는 이렇게 분석된 자료를 해석하여 어떠한 위협요소가 자산에 손실을 발생시켰을 경우에 손실의 크기를 수치화 시킨다.

이렇게 평가된 결과는 평가자의 주관이 개입된다는 단점을 가지게 된다. 그러나 결과를 데이터베이스화 시켜서 다음의 분석에서 활용하게 된다면 평가된 결

* 고려대학교 정보보호대학원 정보보호학과 박사과정
** 고려대학교 정보보호대학원 정보보호학과 석사과정
*** 고려대학교 정보보호대학원 정교수(jilim@tiger.korea.ac.kr)
**** 한국정보보호진흥원 연구원

과의 신뢰성은 계속해서 증가하게 될 것이고 이러한 방법에 의해서 객관성의 수치를 높일 수 있다. 여기서는 우선 자료의 수치화 시키는 방법을 소개하겠다.

Ⅱ. 배경

2.1 측정척도

자료를 측정하는 방법에는 정성적 측정방법과 정량적 측정방법이 있다. 정성적 측정방법은 대상을 분류하거나 구분하고 범주에 속하는지 여부를 판가름하는 방법이고 정량적 측정방법은 수리적 조작이 가능한 측도가 된다.

2.2 평가의 어려움

2.2.1 정량분석의 문제점

정량분석(Quantitative Analysis)에 의해서 수량화된 분석 결과는 위험이 직·간접적으로 특정 자산에 영향을 미치는 정도를 금전적으로 나타내주기 때문에 위협 발생시 피해정도를 산술적으로 산출할 수 있는 장점이 있다. 그러나 유형자산의 정량화는 어느 정도 가능하나 무형자산의 정량화는 많은 통계 데이터와 경험이 요구된다. 특히 전산 데이터와 같은 자산의 경우 정확한 정량화 수치를 구하는 것이 무척 어렵다. 정량화가 어려운 자산의 경우 분석이 용이하지 않는 단점이 있다. 또한 연간기대손실치(ALE:Annual Loss Expectancy)의 산출과정이 대부분 미국 국립표준기술연구원(NIST)의 FIBS-65에 근간을 두고있기 때문에 산출결과가 국내환경에 맞지 않는 어려움이 있다.

2.2.2 정성분석의 문제점

정성분석(Qualitative Analysis)은 상기와 같은 정량분석의 문제점을 해결하고자 하는 움직임에서 발전되었다. 금융기관(은행, 증권회사, 투자회사)과 같은 곳에서 금융자산을 대상으로 위험분석을 적용하였을 경우 대상자산은 이미 정량화 되어 있기 때문에 정량분석이 적절하나 정보시스템의 경우 네트워크, 전자정보(Electrical Data)등은 이의 적용이 적절치 못하다. 따라서 정성분석은 위험을 정량화 되지 않은 기술변수(예를 들면 상/중/하)로 나타냄으로써 정량화가 가져오는 오차를 줄이고 분석 과정에서 전문가의 의견을 최대로 반영할 수 있는 장점이 있다. 그러나 전문가의 주관적 판단이 지나치게 작용할 우려가 높고 위험관리에 있어서 중요한 기능인' 보안계획의 수립과 대응책 구현을 위한 비용효과 분석이 용이하지 않는 단점이 있을 수 있다.

Ⅲ. 본론

전체적인 평가의 단계를 살펴보면 크게 3단계로 나눌 수 있다.

3.1 자산의 평가

자산은 재산과 같은 뜻으로 쓰이며, 유형·무형의 물품·재화나 권리와 같은 가치의 구체적인 실체(實體)를 의미한다.

〔표 1〕 자산 분류

자산의대분류	자산의 소분류
유형자산	경제적 자산
	물리적 자산
	문서·자료 자산
	소프트웨어 자산
	인적 자산
무형자산	

또 자산의 분류는 크게 위에 있는 〔표 1〕을 따른다.

평가하려는 대상의 자산요소를 파악하여 대상 조직 내에서 각각의 자산요소들이 차지하는 비중을 파악한다. 자산요소들의 비중을 파악하기 위해서는 다음에 예로 보이는 질문 평가지를 이용한 절대평가방식을 이용한다. 질문 평가지의 형식은 Y/N, 단답형 대답이고 각각의 자산요소가 가지고 있는 가치를 실제적인 데이터에 근거하여 분석한다. 이렇게 분석한 자산요소의 수치를 "가치분석지수"라고 하겠다. 그리고 이 "가치분석지수"는 평가대상의 자산의 특성을 평가에 반영시킨다.

〔표 2〕

학교 내의 부수적인 수익금	응답
• 매점의 연평균 순수익은 얼마인가?	2억
• 복사실의 연평균 순수익은 얼마인가?	1억5천
• 문구점의 연평균 순수익은 얼마인가?	3억

총 항목수 : 3개, 총 금액 : 6억 5천, 가치분석지수 : 0.015

자산평가방법은 다음과 같다.

첫째는 조직에 따른 자산요소를 파악하여 구분한다. 둘째는 자산요소의 가치를 파악한다. 셋째는 각 요소에 가중치를 부여한다. 여기서 가중치의 의미는 자산에 있어서의 중요도라 할 수 있는데 자산이 위협요소에 위해서 손실이 발생했을 경우에 그 손실 정도를 계량화하기 위해서 필요한 단계가 된다. 또 가중치는 조직의 특성을 표현하게 된다.

여기서 자산의 요소별 가치를 유형별로 분류하여 수치화 시킨 값을 가치분석지수라고 부를 것이다. 이 값은 위협에 의한 손실을 계량화 할 때에 손실의 양을 실제적으로 비교 가능하도록 하기 위해서 필요하다.

3.2 위협요소 분류

자산에 영향을 끼칠 수 있는 위협요소를 파악한다. 위험요소는 〔표 3〕과 같이 분류할 수 있다.

〔표 3〕 위협의 분류

인위적		자연적	시스템 결함적
고의적	우발적		
도청 정보변조 시스템해킹 테러 컴퓨터바이러스 방화, 도난	자료입력실수 전원변동 파일삭제 접근통제의실수	지진 벼락 홍수 태풍 화재	운영체제의 결함 프로그램 결함 과부하 하드웨어 고장

3.3 취약성 분류

첫째는 대상이 가지고 있는 취약점을 파악하여 분류한다. 〔표 4〕와 같이 분류할 수 있다.

이 단계는 어떠한 위협에 의해서 손실이 발생한다면 그 손실은 자산의 약점인 취약점에서 발생한다는 관점에서 분석하려는 의도이다.

둘째는 대상이 가지고 있는 취약성의 정도를 파악한다. 즉, 취약성 요소와 자산의 요소에 따라서 각기 다르게 손실을 발생시킬 것이기 때문에 각각의 가중치의 의미를 부여하게 된다. 이러한 취약성의 정도를 파악하기 위해서는 평가 대상 전체의 통제 수준을 평가해야 한다. 즉, 취약성의 분류별로 필요한 전체 기본 통제 중에서 현재 구현되어져 있는 통제의 백분율 값을 통제평가지수라고 부를 것이다.

실제적으로 취약성 요소별 통제평가지수를 계산하는 방법은 다음과 같은 다음과 같은 평가지를 이용하여 Yes항목수를 전체 항목수로 나눈 백분율 값으로 다음과 같이 표현하게 된다. 앞에서 분류한 취약성 요소 중에서 직무분리에 해당하는 경우의 예가 된다.

〔표 4〕 학교조직의 취약성 분류

취약성 분류		취약성 세부 분류
관리적 취약성	조직 및 요원	직무분리
		관리자 및 요원 승계
		자질 및 교육훈련
		운영 요원
	지침 및 절차	지침 및 절차의 제정 개폐
		운영조직 및 운영요원
		시설 및 장비
		운영 통제
		보안
		백업 및 비상 대책
		통신망
		지침 및 절차에 대한 준수현황
	백업 및 비상 대책	백업 매체수록 및 순환사용 절차
		백업매체 외부 소산주기
		전산센터 재해복구 대책
		비상조치 요령, 교육훈련
물리적 취약성	시설 및 장비	전산 장비
		인명 및 장비에 대한 위해 요소
		부정전 시설, 중요증서 현물관리
		정기점검 실시, 유지보수계약
		경영층의 장애사항 인지도 및 개선노력
논리적 취약성	보안	보안관리 일반, 보안관리 적정성
		Data 보안대책, 서버보안, 침입탐지 시스템 보안
		컴퓨터실 출입통제, 보안시스템 운영
		프로그램 및 유틸리티등에 대한 통제
		인사이동, 신규채용 및 퇴직시의 보안대책
		컴퓨터 바이러스 방지대책
		비밀번호 및 암호화키 통제 절차
	운영 통제	데이터 입력권한 통제, 데이터 내역기록
	통신망	통신망 운영시스템 및 사용자 관리
		주요관리자의 직무분리 및 업무수행 능력
		온라인 관련 보안대책
		데이터 보안대책
		시스템 운영 통제
		사용자 및 운영자에 대한 연수

〔표 5〕

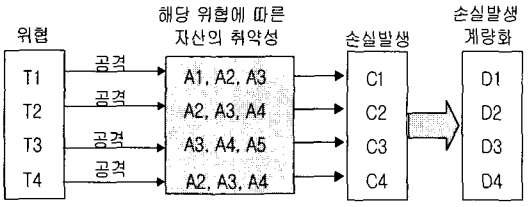
직무 분리	YES/NO
• 내부규정이나 지침에 운영요원에 대한 직무권한과 책임이 명확히 규정되어 있는지 여부	YES
• 주전산기에 대한 접근이 오퍼레이터 이외의 요원에게는 금지되어 있는지의 여부	NO
• 기타 운영요원과 오퍼레이터와의 직무가 상호 중복되는 것이 없는지의 여부	NO
• 오퍼레이터가 프로그램 소스를 직접 확인할 수 없도록 되어 있는지 여부	YES

총 항목수 : 4, YES 항목수 : 2, 통제평가지수 :0.5

또, 어떠한 평가대상에서 위협요소의 발생 가능성은 통제평가지수의 값이 적으면 적을수록 손실의 가능성이 커지게 된다. 따라서 위협요소의 발생가능성은 1-(통제평가지수)의 값으로 표현되며 이를 취약성 요소수치라고 부를 것이다. 〔표 5〕의 경우에는 취약성 요소수치가 0.5가 될 것이다.

3.4 위협요소 별 손실의 수치화 방법

어떠한 위협요소를 선택하여 그러한 위협이 발생했을 때에 실제로 손실의 양을 수치화 시키는 방법을 소개하려고 한다. 대학교를 대상으로 평가하는 방법을 설명하고 있다.



〔그림 1〕 위협의 자산에 대한 취약성 공격 모델링

3.4.1 손실 수치화의 방법 I

[단계1] 위협요소가 영향을 주는 취약성 요소 구분 단계

어떠한 위협요소T1이 자산에 손실을 발생시킬 때에는 자산의 모든 요소에 골고루 발생시킨다고 보기는 어렵다. 예를 든다면 컴퓨터 바이러스의 경우에 관리적 취약성인 조직요원부분이나 지침이나 절차와 같은 취약성 요소에서는 발생하지 않았음을 알 수 있다. 이렇게 위협은 자산의 요소 중에서 특히 취약성을 가지고 있는 요소에 손실을 발생시키며 그 정도에도 차이가 있을 것이다. 그렇다면 위협요소T1이 주로 위협을 가하게 되는 취약성 요소를 구분하고 그 정도를 파악할 필요가 있다. 이것은 위협요소가 각 취약점 요소에 영향을 준 빈도를 측정하여 계속 데이터 베이스화 시켜서 평가에 활용하는 기준으로 삼으면 될 것이다.

[단계2] 위협의 상대지수 파악 단계

취약성 요소에 따라서 위협에 의한 손실의 발생 정도는 모두 다르기 때문에 취약성에 대한 발생 빈도를 다른 취약성과의 상대적인 값으로 표현할 필요가 있다. 이와 같은 위협의 취약성 요소별 상대적 발생 가능성을 나타내는 수치를 위협의 상대지수라고 부를 것이다.

[단계3] 위협 요소별 손실정도 파악 단계

위협 요소별 손실정도는 위협요소가 영향을 미치게 되는 취약성 요소를 파악하여 그 취약성 요소가 가지고 있는 취약성의 정도를 평가한 값인 취약성 요소수치와 발생위협에 대한 그 취약성 요소의 상대적 발생 가능성인위협의 상대지수로 다음과 같이 표현할 수 있다.

$$\sum_{\lambda} \text{취약성요소수치} \times \text{위협의상대지수}$$

(λ : 위협의 영향을 받는 취약성 요소)

이 수치는 위협요소에 의한 손실의 정도를 어떠한 위협이 발생한다면 자산의 취약성요소에 발생할 것이라는 관점에서 최대정도를 측정하려는 것이다.

〔표 6〕에서는 위협요소 중에서 도청의 경우에 있어서 손실 정도를 계산하는 예이다.

(위협요소별 손실정도)

$= \sum$(취약성요소 수치)×(위협의 상대지수)

$=(0.75\times0.03)+(0.00\times0.02)+\cdots$

$+(0.70\times0.06)=0.4584$

도청의 경우에 위협요소별 손실정도는 0.4584로 나타나게 된다.

〔표 7〕에 제시한 표는 대학교를 대상으로 위협요소별 손실정도를 실제로 구한 것이다.

이렇게 평가한 위협 요소별 손실정도는 사실상 손실의 가능성을 표현한 값으로 자산의 가치를 수치에 적용하지는 않았다. 따라서 측정된 위협 요소별 손실정도의 수치를 가지고 실제 손실의 크기를 비교하는 것은 옳지가 않다.

〔표 6〕

취약성 대분류	취약성 세부 분류	통제 평가 지수	발생 유무	상대 지수
관리적 취약성	직무분리	0.50		
	관리자 및 요원 승계	0.60		
	자질 및 교육훈련	0.25	O	0.03
	운영 요원	0.33		
	지침 및 절차의 재정 개폐	0.50		
	운영조직 및 운영요원	1.00	O	0.02
	시설 및 장비	1.00		
	운영 통제	0.60	O	0.12
	보안	0.71	O	0.10
	백업 및 비상 대책	0.00		
	통신망	0.50	O	0.04
	지침 및 절차에 대한 준수현황	0.50		
	백업 매체수록 및 순환사용 절차	0.25		
	백업매체 외부 소산주기	0.20		
	전산센터 재해복구 대책	0.50		
	비상조치 요령, 교육훈련	0.33	O	0.02
물리적 취약성	전산 장비	0.00		
	인명 및 장비에 대한 위해 요소	0.66		
	부정전 시설, 중요증서 현물관리	0.40		
	정기점검 실시, 유지보수계약	0.83		
	경영층의 장애사항 인지도 및 개선 노력	0.66		
논리적 취약성	보안관리 일반, 보안관리 적정성	0.60	O	0.15
	Data 보안대책, 서버보안, 침입탐지 시스템 보안	0.49	O	0.11
	컴퓨터실 출입통제, 보안시스템 운영	0.75	O	0.10
	프로그램 및 유틸리티등에 대한 통제	0.25		
	인사이동, 신규채용 및 퇴직시의 보안대책	0.50		
	컴퓨터 바이러스 방지대책	0.50		
	비밀번호 및 암호화키 통제 절차	0.40	O	0.09
	데이터 입력권한 통제, 데이터 내역기록	0.50	O	0.10
	통신망 운영시스템 및 사용자 관리	0.50		
	주요관리자의 직무분리 및 업무수행 능력	0.50		
	온라인 관련 보안대책	0.36	O	0.06
	데이터 보안대책	0.30	O	0.06
	시스템 운영 통제	0.30		
	사용자 및 운영자에 대한 연수	0.50		

〔표 7〕 위협 요소별 손실정도

위협		위협요소	위협요소별 손실정도
인위적	고의적	도청	0.4584
		정보변조	0.5257
		시스템 해킹	0.581
		테러	0
		컴퓨터바이러스	0.6255
		방화	0.067
		도난	0.561
	우발적	자료입력 실수	0.496
		전원변동	0.40
		접근통제의 실수	0.4725
자연적		지진	0.6245
		벼락	0.5995
		홍수	0.6115
		태풍	0.6085
		화재	0.6465

[단계4] 자산 요소별 취약성 분류단계

자산요소 별로 관련을 가지는 취약성을 분류해 놓는다. 뒤에서 손실을 평가할 때에 이용할 것이다.

[단계5] 자산요소별 관련 취약성요소의 최대 연관도 파악단계

위에서 파악한 자산요소별 관련 취약성요소는 그 관련된 정도가 동일하지 않다. 이러한 자산 요소별로 관련을 가지는 취약성 요소의 관련 정도를 수치화 시킨 값을 **취약성관련 최대연관도**라 부를 것이다.

또 어떠한 자산요소가 여러 가지 취약성을 가지게 된다면 자산이 위협을 받았을 때에 일반적으로 그 위협에 의해서 자산 전체가 파괴되지는 않을 것이다. 그러므로 여기서 파악된 취약성요소의 최대연관도의 합은 1보다 많지는 않다.

〔표 8〕의 예는 대학교를 대상으로 자산요소 별 취약성 관련 최대연관도를 구한 것이다.

[단계6] 손실의 수치화 단계

위에서 평가한 취약성관련 최대 연관도와 취약성 요소별 손실정도 수치 그리고 자산의 가치를 결합하여 손실을 다음과 같이 수치화 한다.

$$(\text{손실}) = \sum_{\text{취약성요소별}} \{(\text{취약성관련 최대 연관도}) \times (\text{취약요소별 손실정도수치}) \times (\text{자산의 가치})\}$$

〔표 8〕 취약성과 관련을 가지는 자산목록

자산 분류		자산의 세부 분류	통계 평가 지수	연관된 취약성 및 최대연관도	
유형 자산	경제적 자산	학교 내의 부수적인 수익금	0.015	A.1.4	0.05
				A.2.2	0.02
				B.1.3	0.05
				B.1.5	0.02
				C.3.6	0.03
		외부의 지원금 및 기부금	0.09	C.3.3	0.03
		학생들의 등록금	0.8	C.1.2	0.04
				C.3.3	0.02
				C.3.4	0.04
	물리적 자산	학습 공간	0.75	A.2.3	0.43
		학습 도구	0.57	B.1.1	0.03
		학습 환경	0.83	A.2.6	0.01
				A.2.7	0.01
				A.3.3	0.03
				B.1.2	0.04
				B.1.3	0.03
				C.1.2	0.04
				C.1.6	0.02
				C.3.4	0.03
				C.3.5	0.03
	문서·자료 자산	도서관·연구실에 비치된 서적	0.75	A.1.3	0.05
				B.1.4	0.05
				C.2.1	0.05
				C.3.6	0.05
		연구 분야 별 논문	0.50	A.1.3	0.05
				B.1.4	0.05
				C.2.1	0.05
				C.3.6	0.1

다음에서는 컴퓨터 바이러스의 경우에 손실을 계산해 보려고 한다.

컴퓨터 바이러스가 주로 발생하는 경우의 취약성 요소는 〔표 9〕와 같다는 것을 앞 절에서 알 수 있었다.

〔표 9〕에 나타나 있는 세부항목과 연관된 자산의 요소를 찾아서 자산의 유형별로 그에 대한 손실을 평가하면 된다.

다음에는 〔표 10〕에서 설명한 방식에 의해서 자산의 유형별로 그에 대한 손실을 구한 것이다. 표를 통해서도 알 수 있듯이 어떠한 손실이 발생했을 때 경제적 손실, 물리적 손실, 문서·자료 손실 등 여러 가지 면에서 살펴볼 수 있다.

그러나 그 크기의 비교는 자산 요소의 특성상 용이하지가 않고 객관화시키기가 어렵다. 또, 평가하는 대상이나 상황에 따라서 다르게 될 것이다.
즉, 바이러스의 경우에 경제적 손실은 0.00417%이고 물리적 손실의 경우에는 0.645%이지만 물리적 손실이 경제적 손실보다 크다고는 말할 수 없다.

단지, 바이러스로 인한 손실이 "경제적 손실은 182,247,500원"이고 "물리적으로는 0.645%가 손실되었다"라고 표현할 수 있을 뿐이다.

Ⅳ. 관련용어 정리

경제적 손실을 수치화 시키기 위해서 관련된 용어를 정리하면 다음과 같다.

⊙ 가치분석지수

자산의 요소별 가치를 실제적인 데이터에 근거하여 평가한 수치로 유형별로 앞에서 분류한 유형별로 그 가치의 크기를 수치화 시킨 값을 의미한다.

⊙ 통제평가지수

취약성의 분류별로 필요한 전체 기본 통제 중에서 현재 구현되어져 있는 통제의 백분율 값을 의미한다.

〔표 9〕 바이러스에 관한 취약성 요소 분석

취약성 분류		취약성 세부분류	세부항목 기호	통제 평가 지수	취약성 요소 수치	상대 지수	취약요소별 손실정도 수치
논리적 취약성	보안	컴퓨터실 출입통제, 보안시스템 운영	C.1.3	0.75	0.25	0.05	0.0125
		프로그램 및 유틸리티등에 대한 통제	C.1.4	0.25	0.75	0.20	0.0125
		컴퓨터 바이러스 방지대책	C.1.5	0.50	0.50	0.05	0.0125
		비밀번호 및 암호화키 통제 절차	C.1.6	0.40	0.60	0.10	0.0125
	통신망	통신망 운영시스템 및 사용자 관리	C.3.1	0.50	0.50	0.05	0.0125
		주요관리자의 직무분리 및 업무수행 능력	C.3.2	0.50	0.50	0.05	0.0125
		온라인 관련 보안대책	C.3.3	0.36	0.64	0.20	0.0125
		데이터 보안대책	C.3.4	0.30	0.70	0.15	0.0125
		시스템 운영 통제	C.3.5	0.30	0.70	0.10	0.0125
		사용자 및 운영자에 대한 연수	C.3.6	0.50	0.50	0.05	0.0125

〔표 10〕

자산	자산의 세부 분류	통계평가 지수	연관된 취약성 및 최대연관도		손실가치	
경제적 자산	학교 내의 부수적인 수익금 (6억 5천)	0.015	A.1.4	0.05	650,000,000×0.03×0.025 =487,500	182,247,500 의 손실 0.417%
			A.2.2	0.02		
			B.1.3	0.05		
			B.1.5	0.02		
			C.3.6	0.03		
	외부의 지원금 및 기부금(50억)	0.09	C.3.3	0.03	5,000,000,000×0.03×0.128 =4,680,000	
	학생들의 등록금 (380억)	0.8	C.1.2	0.04	38,000,000,000×0.02×0.128 +38,000,000,000×0.02×0.105 =177,080,000	
			C.3.3	0.02		
			C.3.4	0.04		
물리적 자산	학습 공간	0.75	A.2.3	0.43		0.645%
	학습 도구	0.57	B.1.1	0.03		
	학습 환경	0.83	A.2.6	0.01	0.06×0.02+0.105×0.03 +0.07×0.03=0.00645	
			A.2.7	0.01		
			A.3.3	0.03		
			B.1.2	0.04		
			B.1.3	0.03		
			C.1.2	0.04		
			C.1.6	0.02		
			C.3.4	0.03		
			C.3.5	0.03		
문서/ 자료자산	도서관·연구실에 비치된 서적	0.75	A.1.3	0.05	0.05×0.025=0.00125	0.150%
			B.1.4	0.05		
			C.2.1	0.05		
			C.3.6	0.05		
	연구분야 별 논문	0.50	A.1.3	0.05	0.01×0.025=0.00025	
			B.1.4	0.05		
			C.2.1	0.05		
			C.3.6	0.1		
		0.80	B.1.1	0.05	0.05×0.0125+0.05×0.15 +0.05×0.025+0.05×0.06 +0.05×0.025+0.05×0.025 +0.05×0.128+0.05×0.105 +0.05×0.07+0.05×0.025 =0.031275	6.2550%
			B.1.3	0.05		
			B.1.4	0.05		
			C.1.1	0.05		
			C.1.2	0.05		
			C.1.3	0.05		
			C.1.4	0.05		
			C.1.5	0.05		
			C.1.6	0.05		
			C.1.7	0.05		
			C.2.1	0.05		
			C.3.1	0.05		

〔표 10〕 계속

자산	자산의 세부 분류	통계평가 지수	연관된 취약성 및 최대연관도		손실가치	
소프트웨어 자산			C.3.2	0.05		6.2550%
			C.3.3	0.05		
			C.3.4	0.05		
			C.3.5	0.05		
			C.3.6	0.05		
	응용 소프트웨어	1.00	C.1.1	0.05	0.05×0.0125+0.05×0.15 +0.05×0.025+0.05×0.06 +0.05×0.025+0.05×0.025 +0.05×0.128+0.05×0.105 +0.05×0.07+0.05×0.025 =0.031275	
			C.1.2	0.05		
			C.1.3	0.05		
			C.1.4	0.05		
			C.1.5	0.05		
			C.1.6	0.05		
			C.1.7	0.05		
			C.2.1	0.05		
			C.3.1	0.05		
			C.3.2	0.05		
			C.3.3	0.05		
			C.3.4	0.05		
			C.3.5	0.05		
			C.3.6	0.05		
인적 자산	교수·박사·석사	0.33	A.1.3	0.05	0.05×0.025=0.00125	0.125%
			A.2.6	0.1		
			A.2.4	0.05		
			C.3.6	0.05		
학생의 학업에 대한 호감도		0.50	A.2.8	0.1		
선·후배 사이의 유대감		0.50				
유능한 교수진		0.75	A.1.4	0.05		
교수·연구원의 프로젝트를 비롯한 업무 수행 능력		0.6	A.1.3	0.05		
학교의 명예, 학교에 대한 외부인의 인지도		1.00				

⊙ 취약성 요소수치

1-(통제평가지수)의 값으로 위협요소의 발생 가능성을 도출하기 위한 값이다. 어떠한 위협요소의 발생 가능성은 통제평가지수의 값이 적으면 적을수록 손실의 가능성이 커지게 된다는 특성을 평가에 반영한 값이다.

⊙ 위협의 상대지수

위협요소에 의한 손실 가능성을 내포하는 값으로 하나의 위협요소가 여러 가지 취약성의 요소 중에서 어떠한 취약성에 영향을 주며 그 취약성에대한 영향의 정도를 다른 취약성과의 상대적인 값으로 표현한 것이다.

⊙ 위협 요소별 손실정도

위협요소에 의한 손실의 정도를 평가하는 수치로써 다음과 같이 표현할 수 있다.

$\sum_{\lambda}$ 취약성 요소수치×위협의 상대지수

(λ: 위협의 영향을 받는 취약성 요소)

〔표 11〕 바이러스에 의한 손실

자산의 분류		자산의 세부 분류	바이러스에 의한 손실
유형자산	경제적 자산	• 학교 내의 부수적인 수익금	182,247,500의 손실 0.417%
		• 외부의 지원금 및 기부금	
		• 학생들의 등록금	
	물리적 자산	• 학습 공간	0.645%
		• 학습 도구	
		• 학습 환경	
	문서·자료 자산	• 도서관·연구실에 비치된 서적	0.150%
		• 연구 분야 별 논문	
	소프트웨어 자산	• 시스템 소프트웨어	6.2550%
		• 응용 소프트웨어	
	인적 자산	• 교수, 박사, 석사	0.125%
무형자산	• 학생의 학업에 대한 호감도		0%
	• 선·후배 사이의 유대감		
	• 유능한 교수진		
	• 교수·연구원의 프로젝트를 비롯한 업무 수행 능력		
	• 학교의 전통과 역사		
	• 학교의 명예, 학교에 대한 외부인의 인지도		

⊙ 취약 요소별 손실정도

위협 요소별 손실정도 중에서 관련 취약성 요소수치에 대한 손실정도를 표현한 값으로 다음과 같다.

취약성 요소수치×위협의 상대지수

⊙ 취약성 관련 최대 연관도

위에서 파악한 자산요소별 관련 취약성요소는 그 관련된 정도가 동일하지 않다. 이러한 자산 요소별로 관련을 가지는 취약성 요소의 관련 정도를 수치화 시킨 값이다.

⊙ 손실

손실의 발생은 어떠한 위협요소가 발생하였을 때 그 위협요소가 자산의 약점인 취약점을 공격하여 발생시킨다는 관점에서 수치화를 시도하였고 그 공격에 의한 손실의 정도 또한 자산요소의 특성에 따라서 다르다는 관점에서 손실의 수치화를 시도하였다. 손실은 위에서 평가한 취약성관련 최대 연관도와 취약성 요소별 손실정도 수치 그리고 자산의 가치를 결합하여 다음과 같이 수치화 한다.

$$(\text{손실}) = \sum_{\text{취약성요소별}} \{(\text{취약성관련 최대 연관도}) \times (\text{취약요소별 손실정도수치}) \times (\text{자산의 가치})\}$$

V. 결 론

대학교를 대상으로 하여 자산을 평가하고 그러한 자산에 나타날 수 있는 위협에 대하여 손실에 발행할 경우에 그 크기를 계량화하는 방법에 대해서 소개하였다.

여기서 소개한 방법은 어떠한 자산에 대한 손실이 하나의 값으로 표현한 것이 아니고 여러 가지 기준으로 표현하였다. 즉, 경제적 손실, 물리적 손실 등의 유형별 손실을 측정하는 방법을 소개하였다.

그러나 이렇게 측정한 유형별 손실들은 비교가 용이하지가 않다. 즉, 자산의 평가방법이 자산요소의 특성에 따라서 정성적 방법과 정량적 방법이 있었기 때문에 그에 따라서 손실의 크기를 측정하는 방법도 정성적 방법과 정량적 방법이 있게 되고 이러한 이유로 인하여 크기의 비교가 어렵다. 예를 든다면 대학교 자산에 있어서 한 요소인 등록금 같은 경우는 그 요소 자체가 수치화 되어져 있어서 정량화 시키는 것이 가능하지만 자산의 다른 예인 논문의 경우는 그 가치를 정량화 한다는 것이 사실상 어렵다. 만약 어떠한 자산요소간의 측정의 비교기준이 만들어진다면 이러한 수치들의 비교가 가능해질 것이다.

〔표 12〕 취약성 세부분류의 기호표

취약성 세부 분류	세부항목 기호
직무분리	A.1.1
관리자 및 요원 승계	A.1.2
자질 및 교육훈련	A.1.3
운영 요원	A.1.4
지침 및 절차의 제정 개폐	A.2.1
운영조직 및 운영요원	A.2.2
시설 및 장비	A.2.3
운영 통제	A.2.4
보안	A.2.5
백업 및 비상 대책	A.2.6
통신망	A.2.7
지침 및 절차에 대한 준수현황	A.2.8
백업 매체수록 및 순환사용 절차	A.3.1
백업매체 외부 소산주기	A.3.2
전산센터 재해복구 대책	A.3.3
비상조치 요령, 교육훈련	A.3.4
전산 장비	B.1.1
인명 및 장비에 대한 위해 요소	B.1.2
부정전 시설, 중요증서 현물관리	B.1.3
정기점검 실시, 유지보수계약	B.1.4
경영층의 장애사항 인지도 및 개선노력	B.1.5
보안관리 일반, 보안관리 적정성	C.1.1
Data 보안대책, 서버보안, 침입탐지 시스템 보안	C.1.2
컴퓨터실 출입통제, 보안시스템 운영	C.1.3
프로그램 및 유틸리티등에 대한 통제	C.1.4
인사이동, 신규채용 및 퇴직시의 보안대책	C.1.5
컴퓨터 바이러스 방지대책	C.1.6
비밀번호 및 암호화키 통제 절차	C.1.7
데이터 입력권한 통제, 데이터 내역기록	C.2.1
통신망 운영시스템 및 사용자 관리	C.3.1
주요관리자의 직무분리 및 업무수행 능력	C.3.2
온라인 관련 보안대책	C.3.3
데이터 보안대책	C.3.4
시스템 운영 통제	C.3.5
사용자 및 운영자에 대한 연수	C.3.6

참 고 문 헌

〔1〕 금융감독원, 검사업무편람(VI)-정보기술(IT)부분 검사업무, 2000.

〔2〕 김기윤, 나관식, "취약성 평가에 의한 정보보호 지표의 계량화 : 정보자산가치가중치법", *정보보호학회지*, pp. 51~62, March 2000.

〔3〕 김정덕, 이성일, "정보기술 위험관리 과정과 기법", *정보보호학회지*, pp. 16~23, June 2001.

〔4〕 김정덕, "정보보호를 위한 위험분석 방법 : 분류와 선택기준", *한국정보보호학회학술대회*, 19951.

〔5〕 Bernstein. T., Bhmani.A., Schultz.E. and C.A.Seigel, Internet Security for Business, 1997.

〔6〕 Haimens, Y.Y.Haimens, Assessment, pp. 584~644, 1998.

〔7〕 Ozier, Will., "Issues in Qunatitative Versus Qualitative Risk analysis," *Datapro Reorts on Information Security*, March 1992, pp. 101~107.

〔8〕 Ozier, Will., "Issues in Qunatitative Versus Qualitative Risk analysis," *Datapro Reorts on Information Security*, March 1992, pp. 101~107.

〔9〕 ISO/IEC JTCI/SC27 N720, *Guidelines for the Management of IT System Security (GMITS) : Part1-Concepts and Mode;s for IT Security*, ISO, Oct 1993.

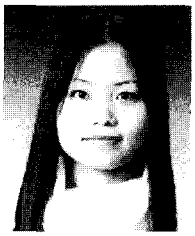
〔10〕 ISO/IEC JTCI/SC27 TR 13335-3, *Guidelines for the Management of IT System Security : Part3-Techniques for the Management of IT Security*, 1999.

〔11〕 *Incident Cost Analysis and Modeling Report I, II, Committee on Institutional Cooperation*, 2000.

〈著者紹介〉

이 현 숙 (Hyun sook Rhee) 비회원
1998년 2월 : 단국대학교 수학과 졸업
2000년 2월 : 단국대학교 대학원수학과 석사
2001년 3월~현재 : 고려대학교 정보보호대학원 정보보호학과 박사과정

변 진 욱 (Jin wook Byun) 비회원
2001년 2월 : 고려대학교 전산학과 졸업
2001년 3월~현재 : 고려대학교 정보보호대학원 정보보호학과 석사과정



기 주 희 (Ju Hee Ki) 비회원
2001년 2월 : 서울시립대학교 수학과 졸업
2001년 3월~현재 : 고려대학교 정보보호대학원 정보보호학과 석사과정

이 동 훈 (Lee dong hoon) 정회원
1983년 2월 : 고려학교 경제학과 졸업
1987년 12월 : Oklahoma University 전산학 석사
1992년 5월 : Oklahoma University 전산학 박사
1992년 8월 : 단국대학교 전자계산학과 전임강사
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
2001년 3월~현재 : 고려대학교 정보보호대학원 정교수, 한국 정보보호학회 편집위원장

임 종 인 (Jong in Lim) 정회원
1980년 2월 : 고려대학교 이과대학 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1986년 2월~현재 : 고려대학교 자연과학대학 정교수, 한국 정보보호학회 총무이사, 고려대학교 정보보호기술 연구소장

박 영 우 (Young woo Park)
2002년 현재 : 한국정보보호진흥원 팀장

윤 재 석 (Jae Suk Yun) 정회원
1998년 2월 : 동국대학교 영어영문학과 졸업
2000년 2월 : 서강대학교 신문방송학과 석사
2000년 3월~현재 : 한국정보보호진흥원 연구원