論文
3-9-19

다중 가중치를 적용한 웹 기반 정보보호수준 측정 도구 설계 및 구현

(Design and Implementation of a Web-Based Tool for Information Security Levelling with Multiple Weights)

성 경* 최 상 용** 소 우 영*** 김 성 옥****
(Kyung Sung) (Sang-Yong Choi) (Woo-Young Soh) (Song-Ok Kim)

요 약

최근 보안 사고가 증가됨에 따라 조직의 효율적인 정보보호 관리를 위한 보안수준 측정 방법 및 도구의 개발에 대한 요구가 높아 가고 있다. 그러나 대부분 외국의 연구로서 수준 측정을 위한 항목 구성이 우리 조직의 실정에 맞지 않고 또한 도구 역시 사용의 편이성이나 경제성을 제공하지 못하고 있으며, 국내의 연구 또한 조직의 특성을 적절히 감안하지 못하고 있다. 따라서 본 논문에서는 최근 개발된 국내의 표준을 기초로 조직이 정보보호 관리체계를 구축하기 이전에 조직의 정보보호수준을 보다 정확하게 측정하기 위한 도구를 설계 구현하였다. 수준 측정 시 4가지의 다중 가중치를 조직의 특성에 따라 가변적으로 적용하여 측정결과의 정확성을 높였다.

ABSTRACT

Recently there has been increasing demand on developing methodologies and tools for measuring the information security level of organizations for the efficient security management, as the growth of security incidents. However, most methodologies from foreign countries are not realistic in constructing the checklists, moreover their tools provide neither the ease of use nor the inexpensiveness, and most domestic works are not properly considering the characteristics of the organizations. In this study, based on the recently developed standard for information security management, an information security levelling tool is designed and implemented which can be used before building an information security management system while considering the characteristics of organizations more efficiently. The efficiency comes from applying multiple variable weights for security levelling according to the characteristics of organizations.

제 1 장 서론

정보화 사회에서는 정보처리와 유통이 대개 실시간으로 이루어지며 많은 중요 정보가 네트워크를 통하여 전송되어 원격 사용자도 용이하게 접근할 수 있다. 이는 정보의 오남용이나 파괴 행위도 실시간

* 정회원 : 동해대학교 컴퓨터공학과 조교수
* 정회원 : 한남대학교 컴퓨터공학과 석사과정
* 정회원 : 한남대학교 컴퓨터공학과 교수
* 정회원 : 한남대학교 컴퓨터공학과 교수

논문접수 : 2002. 9. 25.
심사완료 : 2002. 12. 12.

으로 대량으로 일어날 수 있음을 의미한다.

즉 정보화는 순기능과 함께 역기능을 동반하고 순기능이 클수록 역기능도 그에 비례해서 커질 수 있으며 때로는 역기능 때문에 순기능 자체가 크게 제약을 받을 소지가 있다. 따라서, 이러한 위험으로 인한 손실로부터 정보자산을 보호할 수 있는 관리체계구축의 필요성이 높아지고 있다. 보안의 개념도 정보화가 진전됨에 따라 1970년대의 데이터보안(data security)중심의 개념에서, 1980년대의 컴퓨터보안, 1990년대의 정보보안(information security) 및 최근의 네트워크 보안으로 변천되고 있다[1]. 이러한 변천 과정에 따라 과거의 단순한 물리적 접근통제와 제도적 안전장치만으로는 효과적인 정보보호 수준 달성에 한계가 있어 네트워크 상에서 종합적이고 체계적인 보안관리체계의 구축이 높이 요구되고있다.

정보보호 관리체계 구축을 원하는 조직은 적절한 정보보호 수준측정 과정을 통하여 현재의 정보보호 상태를 파악하고 보안상 취약한 부분과 보강해야 할 부분 등을 식별하여 체계적이고 비용 효과적인 정보보호 관리체계를 구축할 수 있는 방안이 요구된다. 그러나 최근 대부분의 연구는 정보보호수준 측정 프로세스를 위험관리모델, 위험분석 모델 등에 포함하여 인식하여 왔다. 이로 인해 다음과 같은 문제점이 발생한다. 첫째, 정보보호 수준측정이 조직의 현재의 종합적인 보안수준을 측정하는 것이 아니라 단순히 대응책 구현상황을 점검하는데 그치고 있다. 둘째, 정보보호 관리체계구축을 위한 비용 문제이다. 정보보호 수준측정을 위해서는 정보보호 수준측정 단계가 포함된 고가의 위험관리 또는 위험분석을 위한 도구를 도입해야하기 때문에 소수의 대규모 조직을 제외한 대다수의 투자비용이 부족한 중소규모 조직에서는 도입에 어려움이 따르게 된다. 또한 도입하였더라도 대부분의 도구들이 전문적인 지식 없이는 수행할 수 없는 것이 현 실정이다.

정보보호 수준측정 프로세스에서 수준측정 방법론은 수준측정의 정확성과 성공여부를 좌우하는 중요한 문제이다. 선진국의 정보보호 수준측정을 위한 접근법으로는 SAFE체크리스트, 컴퓨터 보안 핸드북 체크리스트, AFIPS체크리스트, LLNL체크리스트 등이 있다. SAFE체크리스트는 844개 항목, AFIPS체크리스트는 954개 항목, 컴퓨터 보안 핸드북 체크리스트는 790개 항목, LLNL체크리스트는 854개 항목으로 구성되어 있다[2]. 이 중 대표적인 접근법은 LLNL체크리스트이며 '예', '아니오', '해당안됨' 으로만 표시하게 되어있다[1]. 위에서 언급한 체크리스트는 대부분 기존 시스템을 감사하기 위해 만들어진 것이므로 문항수가 많을 뿐 아니라 복잡하여 전문 분석가의 도움을 필요로 한다.

BS7799[3]에서는 물리적 보안, 기술적 보안, 관리적 보안차원의 지표를 비교적 포괄적으로 제시하고 있어 정보보호 관리체계 구축뿐만 아니라 정보보호수준을 측정하기 위한 지표로서도 좋은 참고가 된다. 정보보안수준 계량화를 위한 도구로는 BDSS(Bayesian Decision Support System)[4]와, CRAMM(CCTA Risk Analysis and Management Methodology)[5] 등의 소프트웨어가 있다. 그러나 선진국에서 개발된 이러한 도구들은 사용이 어렵고 분석항목이 우리 실정과 다르기 때문에 널리 이용되지 못하고 있다[2]. 이러한 실정을 감안해 볼 때, 전술한 외국의 방법 및 도구를 그대로 도입하여 사용하는 것은 현실적이지 못하다. 국내의 정보보호 수준측정 관련 연구로는 정보시스템 안전성 평가도구 개발[6] 및 정보보안수준 계량화[1] 등이 있으나 부족한 실정이다. 예를 들면, 위험평가 시 동일한 가중치를 적용한 평가와 조직의 특성에 따라 보안요소의 가중치를 가변적으로 적용 평가하여, 각 조직이 자체적으로 보안 수준을 점검을 할 수 있는 방안[5]이 제시되었다. 그러나, 이 도구에서 사용된 가중치 부여방법은 항목별 보안요소에 대해 가용성, 무결성, 기밀성에 대한 가중치를 상, 중, 하 각각 10점, 7점, 4점으로 적용한 단순한 가중치 적용방법을 선택하였고, 또한 자산에 대한 가중치는 설정하였으나, 업무프로세스에 대한 가중치는 설정되어 있지 않다. 그러나 조직에 따라, 같은 업무프로세스라 하더라도 조직에서 차지하는 비중이 다를 수 있기 때문에, 업무프로세스별 가중치를 별도로 주어야 할 필요가 있고, 또한 복잡한 조직에 적용가능하고 측정결과의 정확도를 높이기 위해서는 가중치를 단순 적용하기보다는 각 항목에 대하여 세부적으로 가중치를 적용할 필요가 있다.

따라서, 본 연구에서는 각 조직의 정보보호 수준측정을 위한 가중치를 조직의 특성을 감안한 조직별 가중치, 업무프로세스별 가중치, 프로세스 소속자산에 대한 가중치 및 점검항목별 가중치의 4가지 다중

가중치를 부여함으로써 정확성을 높일 수 있는 정보보호 수준측정 방법을 제안하여 구현 하고자 한다.

본 연구를 통한 기대성과는 다음과 같이 크게 3가지로 제시할 수 있다.

첫 번째는 다중 가중치 방식을 적용하여 세부적인 항목과 프로세스에 각각의 가중치를 부여하고 조직의 특성을 고려함으로서 좀 더 정확한 값을 도출해 낼 수 있다. 두 번째는 측정결과를 조직전체의 정보보호수준, 업무프로세스별 정보보호수준 및 업무프로세스 내의 자산별 정보보호수준의 3가지로 도식화하여 보여줌으로써 조직의 관리자가 직관적으로 현재 조직이 처한 상황과 취약한 부분을 판단할 수 있어 정보보호 관리체계 구축을 위한 효율적이고 비용 효과적인 의사결정의 기초를 제공하고, 추가적인 대책구현을 요하는 취약 부분의 우선순위 결정에 도움을 줄 수 있다. 마지막으로 정보보호 수준측정을 위한 도구를 웹기반으로 구현함으로 고가의 위험관리 및 위험분석 소프트웨어를 구입하거나, 외부 업체에 위탁할 필요 없이 실시간으로 간단하게 조직의 정보보호 수준을 측정하여 비용을 절감할 수 있다.

본 연구의 범위는 전체적인 위험분석 도구를 구현하는 것이 아니고, 위험분석과정 가운데 정보보호 수준 측정에 해당되는 과정, 즉, 자산분류, 자산가치 산정, 대응책 구현상황분석 등의 과정을 구현하는 것이다. 따라서 본 연구에서는 위협/취약성 분석, 대응책 분석, 비용 효과적인 대응책 제시, 잔류위험평가 등 위험관리/위험부분 프로세스 내에서 정보보호 수준 측정에 해당되지 않는 부분은 제외한다.

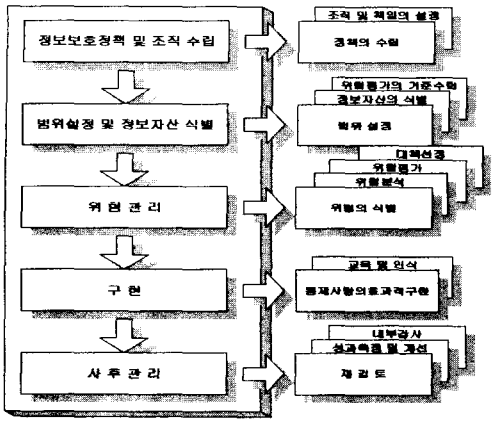
본 논문의 구성은 2장에서 전체적인 정보보호 관리체계 모델과, 정보보호 수준측정을 위한 국내의 2가지 방법론, BS7799, 그리고 정성적 분석 소프트웨어인 CRAMM을 분석하여 본 연구에서 제시한 방법론과 비교해 보고, 3장에서는 본 연구의 정보보호 수준 측정도구의 설계 및 구현에 대하여 기술하며, 4장에서는 가중치를 부여하였을 경우와 부여하지 않았을 경우 프로세스별 정보보호 수준과 자산별 정보보호 수준의 결과를 비교분석하고, 마지막으로 5장에서 결론 및 향후과제를 제시한다.

제 2 장 관련연구

정보란 정보시스템에 의해 가공, 처리, 저장되는 데이터뿐만 아니라 이들 데이터로부터 유추해 낸 자료로 정의할 수 있으며, 정보보호는 이러한 유형, 무형의 정보들을 내부 또는 외부의 위협으로부터 보호하는 것[7]으로서 정보시스템의 자료와 이에 관련된 모든 자산에 대해 이들 정보와 자산의 무결성, 기밀성, 가용성을 관리하기 위하여 수립되는 통제구조라고 볼 수 있다. 이러한 정보시스템 및 이에 관련된 모든 정보와 자산에 대한 통제구조를 체계적으로 구축하기 위한 수단으로 정보보호 관리체계의 구축이 필요하며, 이를 위해 국외에서는 여러 가지 다양한 국제표준과 방법론들이 제안되어 왔다. 그러나 이러한 국제표준들을 국내에 그대로 적용하기에는 국내의 환경이 많이 다르므로 국제적인 표준을 수용하면서 국내의 상황을 반영할만한 표준 제정이 요구되어 국내의 실정에 맞는 기준을 한국정보통신기술협회에서 제안하였고[8], 이 표준에 따른 해설서를 한국정보보호 진흥원에서 제작하였다[7]. 따라서 본 논문은 이 표준에 기초하여 수준측정 항목을 구성하였으며 본 절에서는 이 해설서에 따른 전반적인 정보보호 관리과정을 2.1절에서 살펴보고자 한다. 2.2절에서는 정보보호 수준측정에 관련된 연구와 관련 표준 및 도구들을 살펴보고, 2.3절에서 기존 방법들의 문제점과 본 연구에서의 제안 사항을 논한다.

2.1 정보보호 관리과정

한국 정보보호 진흥원에서 발표한 정보보호 관리기준 해설서[7]에 따르면 정보보호 관리과정은 다음 [그림 1]과 같이 5과정 14개 항목으로 이루어지며, 각 과정에서 세부지침을 작성하여 정보보호관리의 목표를 달성할 수 있도록 계획한다.

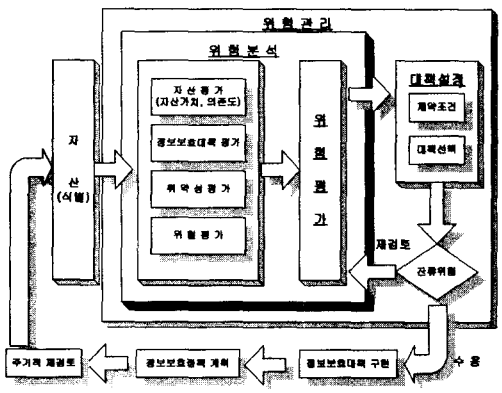


[그림 1] 정보보호 관리과정
[Fig. 1] Information Security Management Process

정보보호정책은 어떤 조직의 기술과 정보자산에 접근하려는 사람이 따라야 하는 규칙의 형식적인 진술이다. 효율적인 정보보호정책을 위해서 각각의 조직 수준과 사업 단위별로 다양한 목표, 전략, 정책을 수립하여야 한다.

범위의 설정은 해당 조직에서 중요하다고 판단되는 요소를 포함해야 하며, 자산평가 과정은 크게 자산 조사와 자산가치 산정의 2가지로 나눌 수 있으며, 자산조사과정에서는 조사할 자산의 범위를 설정하고 자산목록을 작성한다. 자산가치산정 과정에서는 자산을 정량적 또는 정성적으로 산출하는 기준과 절차를 정의한다.

위험관리 절차는 다음 [그림 2]와 같다.



[그림 2] 위험관리 절차
[Fig. 2] Risk Management Process

정보보호에 대한 위험으로부터 정보자산을 보호하기 위해 선택된 통제사항은 적절한 관리 조치와 우선 순위에 따라 구현되어야 한다. 정보보호 계획이 일단 완료되면 대책 실행 및 시험을 실시하고 보안 준수를 점검한다.

사후관리 과정에는 다음의 사항이 포함된다.

- 정보보호관리체계의 재검토
- 정보보호관리체계의 모니터링 및 개선
- 내부감사

2.2 정보보호 수준측정 관련연구

이 절에서는 정보보호 수준측정에 관한 기존의 국내외 관련연구를 분석하여 문제점을 제시하고 이에 대한 본 연구의 제안사항을 논한다.

2.2.1 정보시스템 안전성 평가도구

정보시스템 안전성 평가도구[6]는 정보보호관리체계와 위험분석 방법을 적용한 안전성 평가도구로서 위험평가 시 가중치를 동일하게 또는 상이하게 줌으로써 각 조직의 특성에 따라 조직이 자체적으로 보안 점검을 할 수 있도록 설계된 도구로 관리적 측면에서의 취약점을 쉽게 분석할 수 있다. 이 도구는 평가를 위한 항목을 작성하는 범위설정, 자산의 가치평가, 취약성평가, 위협평가, 발생 빈도에 따른 가치평가, 자산정보 등을 포함하는 자산평가, 5개 항목의 ISMS 요구사항평가 및 11개 항목의 세부통제사항과 취약성평가방법을 이용한 정보보호 평가, 자산의 근본적인 약점을 파악하고 취약성과의 관계를 분석하는 취약성 분석, 그리고 기관별로 가중치를 차등 적용(즉, 가용성, 기밀성, 무결성 중 가장 비중이 높은 항목을 10점으로 하고 각각 7점, 4점으로 적용)하여 ISMS 요구사항 평가 및 세부통제사항에 대한 평가를 각각의 질문에 대해 "예", "아니오", "보통"으로 답하고 그 결과를 항목단위 평균값으로 나타내는 가중치부여 등의 단계로 구성되어 있다.

이 평가도구는 몇 가지의 개선될 점이 있다. 첫째, 단순한 가중치 적용의 문제다. 자산분석에서의 가중치 적용과, 기관별 특성을 반영한 가중치 적용의 의도는 좋으나, 실제적으로 가중치를 부여함에 있어서 항목별 가중치를 단순하게 부여하여 효율성

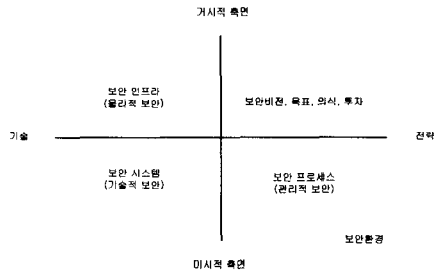
이 떨어진다.

둘째, 업무프로세스에 대해 가중치를 적용하지 않는다는 것이다. 조직이 복잡해지고 대형화됨에 따라 업무프로세스가 조직에서 차지하는 비중이 다를 수 있으나 이를 고려하지 않는다면 정보보호수준 측정 결과의 정확성이 낮아질 수 있으며, 항목별 가중치를 세부적으로 부여할 경우 측정 결과의 정확성이 더 높아질 것이다.

본 연구에서는 이러한 문제를 보완하기 위해 다중 가중치 적용방안을 제안하였으며, 업무프로세스별로 가중치를 적용하고, 각 기준 항목별 세부항목에 대하여 그 중요도별로 가중치를 차등 적용하였다.

2.2.2 정보보안수준 계량화

정보보안수준 계량화[1]는 정보보안 수준을 효과적이고 효율적으로 측정할 수 있는 간편한 지표를 개발하여 계량화하였다. 이 연구에서는 다음 [그림 3]과 같이 보안수준 차원을 거시적 수준과 미시적 수준으로 구분하고, 보안 구현방법 차원을 기술과 전략으로 구분하였다.



[그림 3] 보안환경 차원
[Fig. 3] Aspect of Security Environment

대분류 항목으로서 전통적인 보안요소인 물리적 보안, 기술적 보안, 관리적 보안과 정보보안 의식/투자/환경 등 4가지 범주를 설정하였다. 그리고, 파일럿테스트를 거쳐 완성된 보안수준 측정지표 후보에 대해 우선 항목요소로서의 일반적인 타당성을 조사하고, 항목의 상대적인 중요성을 조사하였다. 보안지수 계량화를 위해 대항목 및 중항목을 기준으로, 바람직한 가중치 비율에 대해 전문가 견해를 조사하였다. 또한 전문가의 소속집단과 경력연수에 의한 의견차이를 분석하여 가중치의 타당성을 검증하였다. 그 결과 도출된 항목별 가중치는 다음 <표 1>과 같다.

이 연구는 우선 정보보안 수준의 개념을 정립하고, 정보보안 수준 측정을 위한 지표항목을 도출하였으며, 정보보안 수준을 계량화할 때 총량화 방법과 가중치 수준에 대한 결과를 도출하였다.

그러나 여기에서도 업종별 또는 조직의 특성별로 정보보안 수준의 차이가 있는지 분석하고, 보안의 각 부문별로 취약점이 무엇인가를 분석할만한 기준을 제시하지 못했다.

본 연구에서는 다중 가중치 적용방안을 제안하였으며, 각 기준 항목별로 기밀성, 무결성, 가용성에 해당되는 중분류 항목에 속한 세부항목에 대하여 그 중요도별로 가중치를 적용하였다.

<표 1> 정보보호 점검 항목별 가중치
<Table 1> Weight of check list Information Security

대 분 류		가중치
물리적 보안		22.5510
	물리적 접근통제	10.2245
	환경위험에 대한 대책	5.4694
	업무연속성 확보계획	6.8980
기술적 보안		31.3265
	시스템 접근통제	6.2916
	감사추적	3.6080
	응용프로그램 보안	3.6794
	데이터베이스 보안	4.4651
	하드웨어 보안	3.0722
	네트워크 보안	6.7508
	PC 및 바이러스 보안	3.4600
관리적 보안		23.0612
	보안 조직	3.5867
	보안 정책	4.2041
	보안 계획	3.4286
	자산파악	2.6480
	위험분석	4.1020
	인사 보안	2.6735
	유지보수 점검	2.7551
정보보안의식투자환경		23.0612
	CEO의 의지 및 마인드	6.0510
	임원/부서장의 의지 및 마인드	3.7245
	직원의 의지 및 마인드	4.3367
	정보보안 관련투자	3.9082
	정보보안 법/제도/표준	2.3163
	보안상태 점검 목록 및 수행	2.7245

2.2.3 BS7799 세부점검항목

BS7799는 영국에서 상무성을 주관으로 "정보보안 관리 실무규범"이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용하도록 1995년 처음 제정되고, 1999년 10월에 ISO표준으로 제안되어 IOS/IEC DIS 17799-1이 정보보호 관리체계 구축을 위한 지침서로 제정하였다. BS7799는 두 부분으로 구성된다.

제1부는 10개의 주요 분야로 나뉘어진 127개의 통제 항목으로 구성되어 있으며, 현재 사용되고 있는 최선의 정보보안 실무들로 구성된 종합적인 보안 통제 목록을 제공한다.

제2부에서는 ISMS 구축방안을 제시하며, 정보보안 정책의 정의, ISMS범위 정의, 위험평가 수행, 위험관리, 통제목적과 구현되는 통제 선택, 정보보안 정책의 문서화 등 여섯 단계로 구성된다. BS7799에서는 위험관리의 중요성을 강조하고 있다. 이 프로세스에서는 먼저 모든 정보 자산과 조직에 있어서 그들의 가치를 분석하고, 어떤 정보가 왜 중요한지를 식별하는 정책을 고안하도록 한다. 2단계에서는 낮은 가치를 가진 정보를 제외하여 관리 대상의 범위를 정의한다. 다음으로, 가치를 상실하는데 따른 위험을 분석하며, 그 위험을 어떻게 관리할지를 결정한다. 그 다음 단계는 위험을 관리하기 위한 보안대책을 선정한다. BS7799에는 이러한 보안대책이 열거되어 있다. 또한 BS7799의 목록은 완전한 것이 아니며, 원하는 경우에는 추가적인 보안대책이 포함될 수 있다는 것을 명시하고 있다.

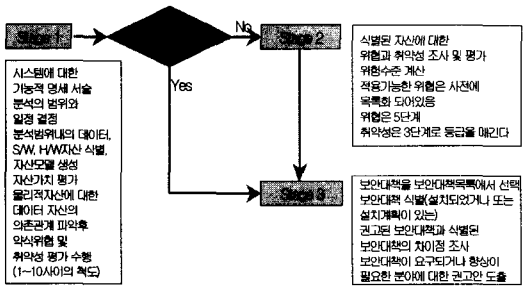
BS7799는 10개 분야의 127개의 세부통제항목으로 구성하고 있어 분야별 점검항목을 선정하는데 지침이 될 수 있으나, 이러한 외국의 세부통제항목들을 그대로 적용하기에는 국내의 실정에 맞지 않는다[9]. 이러한 이유로 BS7799등 최근 외국의 정보보호에 관한 여러 표준들을 참고하고 한국의 실정에 맞게 보완하여 2002. 5. 한국정보통신기술협회에서 '정보보호 관리표준'을 제정하였다. 이 표준은 BS7799를 기반으로 하고 있으나, BS7799와는 달리 국내 실정에 맞게 12개의 분야에 119개의 세부통제항목으로 구성되어 있다.

이 표준의 세부통제항목은 전반적인 정보보호에 관해 점검할 수 있도록 구성되어있다. 그러나, 'CEO의 의지 및 마인드', '임원/부서장의 의지 및 마인드', '직원의 의지 및 마인드', '정보보안 관련투자' 등의 항목에 대해서는 세부적으로 다루지 않고 있으며 위의 네 가지 항목은 중요한 지표로 측정되었다[1]. 이에 본 연구에서는 이 표준의 119개 항목에 위의 네 가지 항목에 대한 세부점검사항 8개 항목을 종합하여 총 127항목으로 설정하였다.

2.2.4 CRAMM

CRAMM(CCTA Risk Analysis and Management Model)은 영국의 표준화 기관인 CCTA(Central Computer and Telecommunications Agency)에서 정부기관의 정보시스템 위험관리를 위하여 전통적인 위험관리 모형을 기초로 개발된 소프트웨어이다.

CRAMM은 다음 [그림 4]와 같이 3단계로 구성된다. 1단계는 기본통제목록 수준의 보안만을 요구하는 시스템을 식별하여 상세한 분석을 수행하며, 시간과 자원을 낭비하지 않도록 중대한 위험의 가능성이 있는 자산에 대하여 더욱 상세한 검토를 수행하는데 목적을 두고 있다.



[그림 4] CRAMM의 프로세스 구성

[Fig. 4] Construction Process of CRAMM

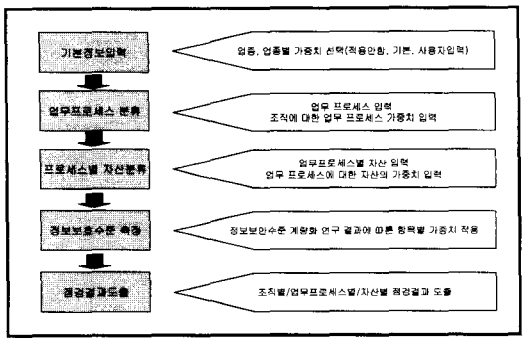
2단계는 시스템의 위협과 취약성을 조사하며, 식별된 자산에 대한 위협 파악, 위협 및 취약성 평가 수행, 위험 수준 계산, 위험 분석 결과 검토회의 개최 등으로 구성되어 있고, 3단계는 보안대책의 선택을 중심으로 위험관리 과정을 구성하고 있으며, 수차례의 수정을 거쳐 2001년에 Version 4.0을 발표하였다.

CRAMM은 정보보호 수준측정, 위험분석, 위험관리 등의 기능을 포함하고 있어, 거대조직의 전체적인 정보보호의 목적을 달성하기 위한 위험관리체계 구축에는 효과적인 도구로 잘 알려져 있다. 그러나 이 도구는 우선 외국의 실정에 맞게 작성된 세부통제항목들을 적용하고 있어서 국내의 실정에 맞지 않으며[9], 정보보호에 관한 전문적인 지식이 없이는 사용이 어렵고, 수행 시간이 오래 걸리며, 고가의 도구로서 중소규모의 조직에서 사용하기에는 적합하지 못하다.

본 연구에서는 이러한 문제를 해결하기 위해, 대규모 조직뿐만 아니라 중 소규모 조직에서도 전문적인 지식이 없이도 간단히 정보보호수준 측정 도구로 활용할 수 있도록 웹기반으로 설계함으로서 가용성을 높였다.

제 3 장 정보보호수준 측정도구 설계 및 구현

본 연구에서는 정보보호수준 측정도구를 위에서 설명한 바와 같이 기본적으로 정보보호 관리기준에서 제시된 프레임워크를 따르면서 4가지의 서로 다른 다중 가중치를 부여하여 좀더 세밀하고 정확한 정보보호 수준을 측정할 수 있는 도구를 설계하였다. 그 4가지의 가중치는 조직의 특성별 가중치, 업무프로세스별 가중치, 자산별 가중치, 그리고 전술된 항목별 가중치이다. 본 연구의 프로세스 구성을 보면 다음 [그림 5]와 같다.

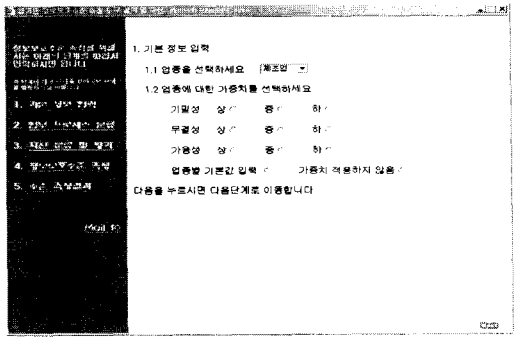


[그림 5] 정보보호수준 측정 프로세스

[Fig. 5] Process of Information Security Level Measurement

3.1 기본정보 입력

기본정보 입력 단계에서는 조직이 속한 업종을 입력하고, 조직의 가용성, 무결성, 기밀성에 대한 가중치를 선택할 수 있게 하였다. 이 단계에서는 사용자의 판단에 따라 가중치를 입력하거나 생략할 수도 있게 설계하였다[그림 6].

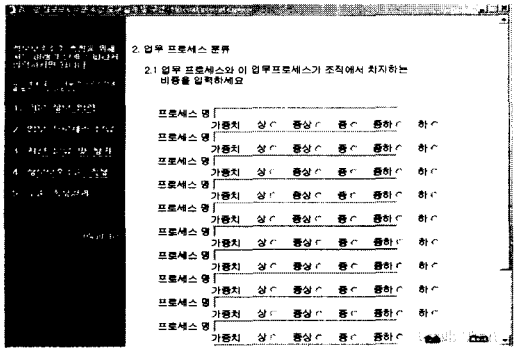


[그림 6] 기본정보 입력화면

[Fig. 6] Input Screen of Basic Information

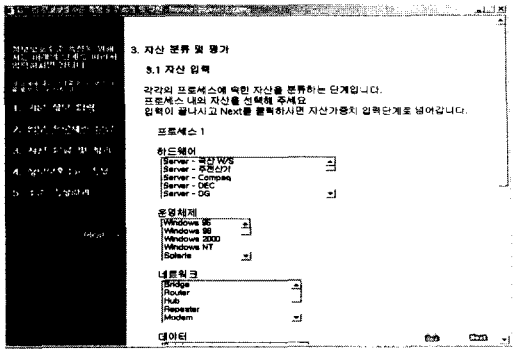
3.2 업무프로세스 분류

자산분류에 앞서 업무프로세스를 분류하는 이유는 일반적으로 IT 위험분석 수행 시 자산을 중심으로 분석해 왔으나 이는 대상조직에 잠재하고 있는 위험의 실체를 파악하는데 부족하다[10]. 위험의 피해는 IT 자산 각각에 가해지기도 하지만 궁극적으로는 IT 자산이 조합되어 수행되는 업무처리에 대해 가해진다[7]. 이러한 이유로 자산분석에 앞서 업무프로세스를 분류하고, 업무프로세스별 가중치를 입력한다. 프로세스가 조직에 차지하는 비중을 상, 중상, 중, 중하, 하와 같이 5개의 등급으로 입력하고, 이러한 등급에 대해 각각 1, 0.7, 0.5, 0.3, 0.1의 가중치가 적용되어 중요한 프로세스에 구현된 대응책은 더 높은 가치를 가지게 된다[그림 7].



[그림 7] 업무 프로세스 입력

[Fig. 7] Input Screen of Work Process



[그림 8] 자산 분류

[Fig. 8] Assets Classfication

3.3 자산분류 및 평가

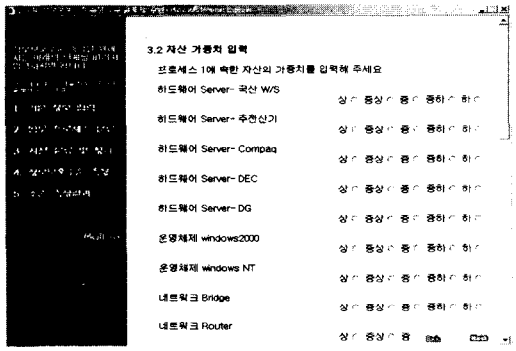
정확한 자산조사 만으로도 기본적인 위험관리가 가능할 만큼 자산조사는 매우 중요하다. 자산조사 수행에는 많은 시간, 노력, 인력, 정보가 필요하고, 따라서 조직에서 요구하는 보안수준과 업무처리에 맞는 조사가 필요하다[7].

자산의 분류는 다음 [그림 8]과 같이 자산의 유형과 성질을 바탕으로 크게 7개의 대분류로 나누고, 이를 다시 세분화해서 분류한 뒤 목록을 작성한다[7][10].

- 하드웨어(H/W)
- 운영체제(O/S)
- 응용소프트웨어(Application)
- 네트워크(Network)
- 데이타(Data)
- 사용자(Users)
- 환경(Environment)

프로세스별 자산을 입력하고 각 자산의 프로세스에 대한 가중치를 상, 중상, 중, 중하, 하 5개 등급으로 입력하게 된다.

입력된 값에 대해 각 자산은 1~0.1까지의 가중치를 가지게 됨으로 같은 조직의 같은 자산이라 하더라도 소속된 프로세스에 따라 중요도가 다른 경우, 정보보호 수준 측정에 좀더 정확한 결과를 도출할 수 있다[그림 9].



[그림 9] 자산 가중치 입력

[Fig. 9] Input of Assets Weight

3.4 정보보호 수준측정

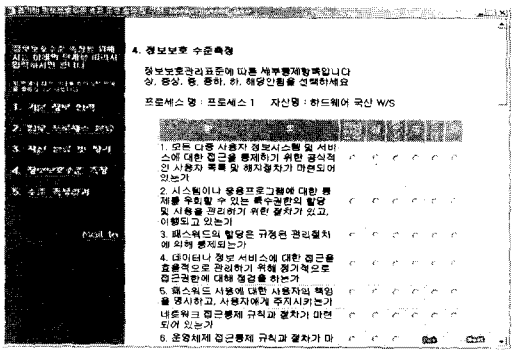
이 단계에서는 전술된 127개 항목으로 구성된 체크리스트를 이용하여 평가한다.

각 항목마다 정보보호를 위한 대책 구현을 상, 중상, 중, 중하, 하, 해당안됨의 6단계로 구분하였다.

- 상 : 문항의 조건을 90%이상 만족함
- 중상 : 문항의 조건을 70~90% 만족함
- 중 : 문항의 조건을 50~70% 만족함
- 중하 : 문항의 조건을 30~50% 만족함
- 하 : 문항의 조건을 30%이하 만족함
- 해당안됨 : 현 조직에서 이 항목은 해당되지 않음

이와 같이 구분된 각 단계에 대해서 1~0.1까지의 가중치를 실제 계산에서 적용하게 된다[그림 10]. 여

기서 '해당안됨'에 체크된 항목은 정보보호수준 측정 값을 종합할 때, 제외시킨다.



[그림 10] 정보보호 수준측정

[Fig. 10] Measurement of Information Security Level

각 항목에 관련된 가중치에 대해서는 기업이나 국가에서 정보보안 수준을 계량적으로 측정하여 수준을 파악하고, 조직간 비교분석 수행 시 활용될 수 있게 작성된 가중치표[1]에 따른 가중치를 적용하여 입력자에 의한 상대적 가중치와 항목별 절대가중치를 모두 고려하여 측정한다.

여기에서 조직의 특성에 따른 가중치가 추가로 적용된다. 조직의 특성에 따른 가중치를 부여하기 위해 세부통제사항 12가지 항목을 무결성, 기밀성, 가용성에 대해 분류하면 다음과 같다[6].

- 가용성 : 인적보안, 물리 및 환경적 보안, 통신 및 운영관리, 시스템 개발보안, 업무연속성 관리, 침해사고 대응 및 복구
- 무결성 : 정보자산 분류와 통제, 접근통제
- 기밀성 : 아웃소싱 및 제3자 접근, 인적보안, 물리 및 환경 보호, 접근통제, 요구사항 준수

해당되지 않은 2가지의 항목, 즉, 정보보호 정책과 정보보호 조직은 조직의 특성에 관계없이 구성되어 있어야 하기 때문에 가용성, 무결성, 기밀성에 관계없이 동일한 가중치를 부여한다.

전술된 가중치표[1]를 가용성, 무결성, 기밀성에 따라 분류하면 다음과 같다.

- 가용성 : 물리적 접근통제, 환경위험에 대한 대책, 업무연속성 계획, 감사추적, 응용프로그램보안, 하드웨어 보안, 네트워크 보안, 위험분석, 인사보안, 유지보수 점검
- 무결성 : 물리적 접근통제, 시스템 접근통제, 데이터베이스 보안, PC 및 바이러스 보안, 자산파악
- 기밀성 : 물리적 접근통제, 환경위험에 대한 대책, 시스템접근통제, 데이터베이스 보안, 인사보안, 정보보안 법/제도/표준

해당되지 않은 항목, 즉, 보안조직, 보안정책, 보안계획, CEO의 의지 및 마인드, 임원/부서장의 의지 및 마인드, 직원의 의지 및 마인드, 정보보안 관련투자, 보안상태 점검 목록 및 수행 등은 가용성, 기밀성, 무결성과는 상관없는 기본적인 요구사항으로 간주한다.

3.5 점검항목 측정치 종합

먼저, 자산 항목별 취득할 수 있는 가용성, 무결성, 기밀성에 대한 최대점수(MVAL: Maximum Value of Asset List)를 구해보면 다음의 식으로 표현할 수 있다.

$$MVAL_{(i)}a = \frac{(TVA_{(i)}a \times (TVL \times (Adda/100))}{TVa}$$

$TVA_{(i)}a$ i번째자산의가용성에해당하는항목의머리정의된값(가중치표)의합

(TVA_i:무결성, TVA_c 기밀성)

TVL: 체크리스트에서기본항목을제외한가중치적용항목(가중치표)의점수의합

$Adda$ 가용성의가중치($Addi$:무결성, $Addc$ 기밀성)

→상:50, 중:30, 하:10적용안함: 각각33.3

TVa 체크리스트전체에대한가용성에해당하는항목(가중치표)의점수의합

(TVi:무결성, TVc 기밀성)

같은 방법으로

$$MVAL_{(i)}i = \frac{(TVA_{(i)}i \times (TVL \times (Addi/100))}{TVi}$$

$$MVAL_{(i)}c = \frac{(TVA_{(i)}c \times (TVL \times (Addc/100))}{TVc}$$

를 도출할 수 있다

또한 자산에 공통적으로 해당하는 점검항목의 기밀성, 무결성, 가용성에 대한 최대값 또한 이러한 공식으로 도출해 낼 수 있다.

$$MVBLa = \frac{(TVBa \times (TVL \times (Adda/100))}{TVa}$$

$$MVBLi = \frac{(TVBi \times (TVL \times (Addi/100))}{TVi}$$

$$MVBLc = \frac{(TVBc \times (TVL \times (Addc/100))}{TVc}$$

가중치가 적용된 각 항목별 점수(VL: Value of Check List apply weight)는 다음의 공식에 의해 구해질 수 있다.

$$VL_{(j)}a_{(i)} = \frac{DVL_{(j)}a_{(i)} \times MVALa}{TVA_{(j)}a}$$

$DVL_{(j)}a_{(i)}$: i번째자산의가용성에해당하는j번째항목의정의된(가중치표)점수

같은 방법으로 $VLc_{(i)}, VLi_{(i)}, VBa_{(i)}, VBc_{(i)}, VBi_{(i)}$ 또한 도출해 낼 수 있다.

가중치가 적용된, 각 자산리스트에 대한 측정점수(CTVAL: Checked Total Value for each Asset List)는 다음의 공식에 의해 구해질 수 있다.

$$CTVALa = \sum (CVL_{(j)}a_{(i)} \times VL_{(j)}a_{(i)})$$

$CVL_{(j)}a_{(i)}$: j번째자산에대한점검항목중가용성에속하는 i번째항목의점검점수
(상:1, 중상:0.7, 중:0.5, 중하:0.3, 하:0.1)

같은 방법으로
$CTVALi, CTVALc, CTVBLi, CTVBLc, CTVBLa$
를 계산해 낼 수 있다.

각 자산에 대한 정보보호 수준(SLA : Security Level for each Asset)을 측정해 보면,

$$SLA_{(i)} = (\frac{CTVAL_{(i)}a + CTVAL_{(i)}i + CTVAL_{(i)}c}{MVAL_{(i)}a + MVAL_{(i)}i + MVAL_{(i)}c}) \times 100$$

이 되고, 프로세스 각각에 대한 정보보호 수준(SLBP : Security Level for Business Process)을 측정하기 위해 먼저, 공통항목에 대한 정보보호 수준(SLB : Security Level for Base List)을 측정해 보면,

$$SLB = (\frac{CTVBLa + CTVBLi + CTVBLc}{MVBLa + MVBLi + MVBLc}) \times 100$$

이 되고,

$$SLBP_{(i)} = \frac{\sum_{i=1}^{n}(SLA_{(i)} \times ADDA_{(i)}) + (SLB \times ADDB) + (\frac{CBLV}{BLV} \times 100)}{n+2}$$

$AddA$: 자산에대한가중치(상:1, 중상:0.7, 중:0.5, 중하:0.3, 하:0.1)

$AddB$: 공통항목에대한가중치(상:1, 중상:0.7, 중:0.5, 중하:0.3, 하:0.1)

$CBLV$: 기본점검사항의점검값 BLV: 기본점검사항의값의총합

이 된다.

조직 전체에 대한 정보보호 수준(SLO : Security Level of Organization)은 다음의 식으로 얻을 수 있다.

$$SLO = \frac{\sum_{i=1}^{n}(SLBP_{(i)} * Add_{BP(i)})}{n}$$

$Add_{BP(i)}$: i번째업무프로세스의가중치

이렇게 도출된 값을 이용하여 본 정보보호 수준 측정 도구는 전체조직의 정보보호 수준, 업무프로세스별 정보보호 수준, 자산별 정보보호 수준 등 3가지의 결과를 보여준다.

제 4 장 실험 결과 분석

4.1 측정 결과

가중치를 적용하지 않고 전체 항목의 측정값을 '상'으로 가정했을 때와, '중', '하'로 가정했을 때의 결과를 보면 모든 값이 '상'일 때는 100%정보보호 수준을 만족하고, 모든 값이 '하' 일 때는 10%의 정보보호 수준을 만족하는 결과가 도출되었다. 그리고 모든 값이 '중'일 때에는 정보보호 수준이 50%로 측정되었다<표 2>. 이러한 결과로 볼 때, 프로세스와, 자산, 조직의 가중치를 부여하지 않고 측정했을 때의 결과는 구현된 대책의 상황에 따라 도출된다고 볼 수 있다.

<표 2> 가중치의 변화에 따른 수준측정결과
<Table 2> Result of Level Measurement According to the Weight Changing

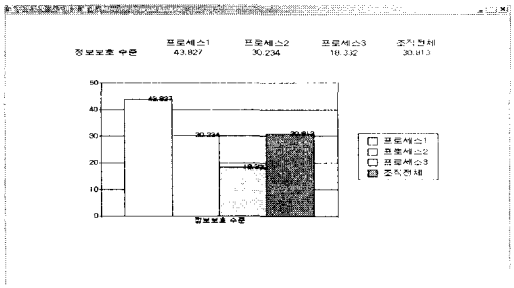
비고		상	중	하
가중치 부여	자산	100	50	10
	프로세스	100	50	10
	업종별	100	50	10
가중치 부여하지 않음		100	50	10

이제 각 항목에 대해서는 같은 값을 넣고, 업종별 가중치를 부여했을 때와 부여하지 않았을 때, 그리고, 그 각각에 대해 프로세스별 가중치를 부여했을 때와 부여하지 않았을 때, 자산별 가중치를 부여했을 때와 부여하지 않았을 때의 결과를 비교분석 함으로서 본 연구의 접근방법의 타당성과 적절성을 보인다.

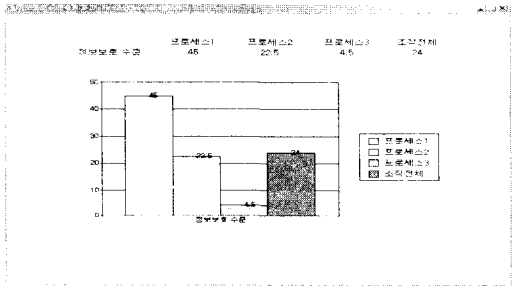
이 비교분석에서의 입력 값은 다음과 같다

- 프로세스 수 : 3개
- 프로세스 당 자산 수 : 17개
- 자산의 가중치 : 1,0.5,0.1 3가지의 경우
- 프로세스의 가중치 : 1,0.5,0.1 3 가지의 경우
- 업종별 가중치 : 기밀성 > 무결성 > 가용성의 순서
- 점검상황 : 업종별 가중치를 주지 않을 경우
  -> 자산가중치만 주었을 때
  -> 프로세스 가중치만 주었을 때
  -> 자산과 프로세스의 가중치를 주었을 때
  : 업종별 가중치를 주는 경우
  -> 자산가중치만 주었을 때
  -> 프로세스 가중치만 주었을 때
  -> 자산과 프로세스의 가중치를 주었을 때
- 항목별 대책 구현 사항 : 같은 자산에 대하여는 가중치를 주었을 때와 주지 않았을 때 모두 같은 값

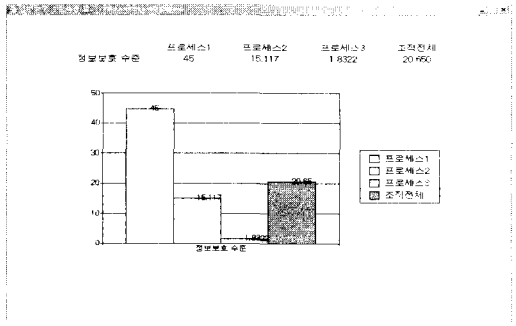
위의 각 경우에서 도구를 테스트한 결과는 다음 [그림 11]부터 [그림 16]과 같다.



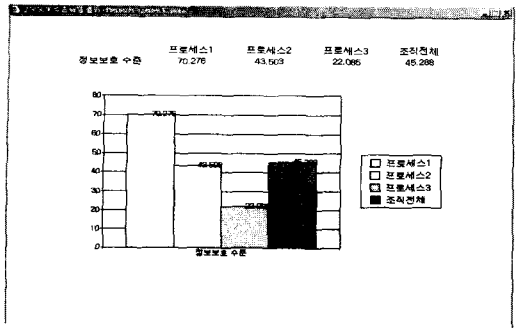
[그림 11] 업종, 자산별 가중치만 부여하였을 때
[Fig. 11] Applying the type of Industry and Assets Weight



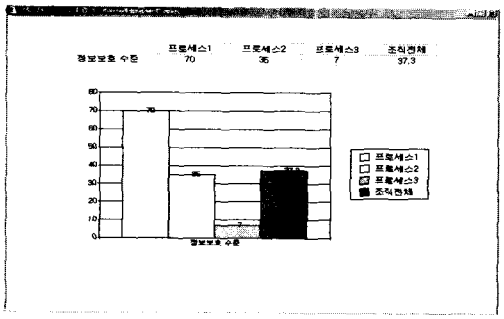
[그림 12] 업종별, 프로세스별 가중치만 부여하였을 때
[Fig. 12] Applying the type of Industry and Process Weight



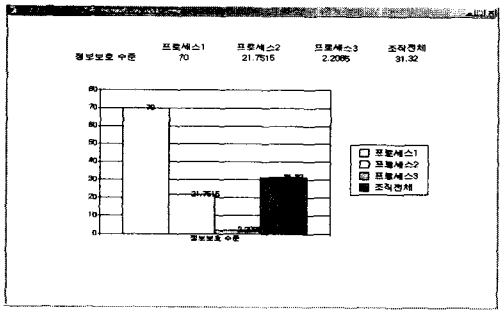
[그림 13] 업종별, 자산별, 프로세스별 가중치를 부여하였을 때
[Fig. 13] Applying the type of Industry, Assets and Process Weight



[그림 14] 자산별 가중치만 부여하였을 때
[Fig. 14] Applying the Assets Weight



[그림 15] 프로세스별 가중치만 부여하였을 때
[Fig. 15] Applying the Process Weight



[그림 16] 자산별, 프로세스별 가중치만 부여하였을 때
[Fig. 16] Applying the Asseys and Process Weight

4.2 측정 결과 분석

제 4장에서는 실질적인 정보보호수준 측정 도구의 실행결과를 여러 가지 입력 값을 달리하면서 측정해 보았다. 그 결과 가중치를 주지 않은 경우 모든 항목에 대해 '상' 수준의 구현이 이루어진 조직에서는 정보보호의 수준 또한 높게 나오고, 반대의 경우에는 낮게 나왔다. 그러나, 가중치의 개념을 도입함으로써 조직에서의 프로세스 및 자산 등이 차지하는 비중을 정보보호수준 측정에 반영할 수 있게 되었다.

종합적인 측정 결과를 표로 나타내면 다음과 같다<표 3>.

<표 3> 가중치에 따른 결과
<Table 3> Result According to Weight

		프로세스 1	프로세스 2	프로세스 3	조직 전체
업종별 가중치 부여하지 않음	자산가중치	70.276	43.503	22.085	45.288
	프로세스가중치	70	35	7	37.3
	자산, 프로세스 가중치	70	21.7515	2.2085	31.32
업종별 가중치 부여	자산가중치	43.827	30.234	18.332	20.813
	프로세스가중치	45	22.5	4.5	24
	자산, 프로세스 가중치	45	15.117	1.8322	20.650

이러한 여러 가지 상황에서 실험을 해 본 결과, 조직 전체의 정보보호 수준은 자산별 가중치, 프로세스 가중치, 업종별 가중치 모두에 따라 영향을 받음을 알 수 있다.

또한, 구현대책에 가중치를 주지 않았을 경우 상당히 높게 측정되었다 하더라도 가중치를 주게되면 기밀성, 무결성, 가용성에 다른 항목에서 획득된 점수에 따라 조직의 정보보호 수준이 크게 차이가 남을 볼 수 있다.

제 5 장 결론 및 향후과제

본 연구는 조직의 정보보안 수준을 효과적으로 측정할 수 있는 방법론을 제안하였다. 최근 개발된 정보보호 관리표준의 119가지 항목에 정보보안수준 계량화에서 정보보호수준 측정지표로 도출된 8가지의 항목을 추가하여 128가지 항목을 자산 및 업종별 가중치 순으로 분류하여 점검항목을 작성하였다. 이들 항목에 대해 프로세스에 종속된 자산별 정보보호 수준을 업종별 가중치를 부여하여 먼저 도출한 다음,

이를 토대로 프로세스별 정보보호 수준을 도출하였다. 또한 프로세스별 정보보호 수준과 자산에 포함되지 않는, 자산에 독립적으로 점검을 요 하는 항목에 대한 점검값을 종합하여 전체 조직의 정보보호 수준을 도출하였다.

정보보호 수준을 도출한 결과 자산에 대한 정보보호수준이 독립적으로는 완벽하다고 도출되었을 지라도 그 자산이 프로세스에서 차지하는 비중과 그 자산이 소속된 프로세스가 조직에서 차지하는 비중과, 또한 업종의 성격(기밀성, 무결성, 가용성)에 따라 종합적인 결과에서는 낮은 비중을 차지할 수 있다는 것을 볼 수 있었다.

이와 같이 업종별 가중치, 프로세스에 대한 가중치, 프로세스에 속한 자산에 대한 가중치, 체크항목에 대한 가중치 등 4가지의 다중가중치를 적용함으로써 정보보호 수준측정의 정확성 및 신뢰성을 높일 수 있었다.

또한, 웹을 기반으로 구현함으로써 사용자가 더 쉽고 간단하게 조직의 정보보호 수준을 측정할 수 있으며 그 결과가 가시적인 도표로 나타남으로서 현재의 정보보호 수준을 쉽게 볼 수 있었다. 또한 구현된 도구는 정보보호 전문가가 아닌 기업의 경영자나 운영자 또는 조직에 책임이 있는 관리자 등이 자산의 목록을 입력하고 비교적 간단한 체크리스트에 표시함으로써 쉽게 사용할 수 있다.

본 연구에서 도출된 점수는 절대적인 정보보호 수준으로서의 역할보다는 수준을 점수화 함으로써 유사 업종의 평균적인 정보보호 수준과 상대적인 비교 대상으로 활용될 수 있으며, 현재 보안상 취약한 자산 및 프로세스를 쉽게 분석할 수 있다.

본 연구의 활용방안을 몇 가지로 요약해보면 첫째, 정보보호 관리체계를 구축하기에 앞서 현재의 정보보호수준을 점검하고자 하는 조직이 활용할 수 있으며, 둘째, 정보보호 관리체계 구축을 원하는 조직에서는 본 도구의 측정결과를 바탕으로 위험분석 또는 위험관리 방법론을 선택하는데 활용될 수 있다. 셋째, 현재 정보보호 관리체계가 구축되어 있는 조직에서도 추후 정보보호 관련투자를 위한 우선순위 결정에 활용할 수 있으며, 마지막으로, 기존의 위험관리/위험분석 도구들과는 달리 정보보호에 대한 기본적인 지식만으로도 조직의 소유자나 경영자 또는 관리자 등이 쉽게 사용할 수 있다.

향후 연구과제로는 첫째, 점검항목을 전문적인 지식을 가진 정보보호 전문가가 아닌 기업의 경영자, 또는 운영자 등이 수행함으로 인한 주관성의 문제를 최소화 할 수 있는 방법이 개발되어야 할 것이며, 둘째, 웹 상에서 운영되기 때문에 조직의 보안 취약성 등에 대한 중요 정보의 보안문제 등이 앞으로 해결되어야 할 것이다.

또한 본 연구의 결과를 기초로 하여 업종별 또는 조직의 특성별로 정보보호 수준의 차이를 분석하기 위한 지표항목 개발과 적용방법이 개발될 경우 종합적인 정보보호 관리 체계 연구에 유용할 것이다.

※ 참고 문헌

[1] 김현수, "정보보호수준 계량화 연구", 경영정보학 연구 제9권 제4호, p182-201, 1999. 12.

[2] 박진섭, 김봉희 "베이스라인 보안정책을 위한 위험분석 체크리스트", Journal of the Institute of Industrial Technology(Taejon Univ.) Vol. 8. No. 2 : 23-40, 1997.

[3] "BS7799 Part 1 : The Code of Practice", British Standard Institution. Part 2 : The Management Standard".

[4] "위험분석 도구 기초기술 개발에 관한 연구", 한국 전자통신 연구원 부설 국가보안기술연구소, 2001,

[5] "CRAMM User Guide", Issue 2.0., U.K. Security Service and CESG, 2001.2.

[6] 홍승구, 김 강, 박진섭, "정보시스템 안전성 평가 도구 설계 및 구현" '2002년한국멀티미디어학회 춘계학술발표논문집' 2002. 05. pp.959-964

[7] "정보보호 관리기준 해설서", 한국 정보보호 진흥원, 2001. 11.

[8] "정보보호 관리표준" , 한국정보통신기술협회, 2002. 5.

[9] 김기윤, 김용겸 '정보시스템의 위험관리 - 외국의 위험관리방법과 한국전산원의 위험관리 방법의 비교', 한국 리스크 관리연구 Vol.5, No.0, pp.27-63., 1995,

[10] "취약점 분석, 평가를 위한 자산분석 지침(안) - 위험산정 및 분석 방법 이론 소개", 한국 정보보호 진흥원, 2001. 9.

인터넷 사이트

http://www.tta.or.kr/Stdinfo/jnal/janl69/8-2.htm
http://www.kisa.or.kr/K_trend/KisaNews/200011/Standardization_06.html
http://www.kisa.or.kr/K_trend/KisaNews/200011/Trend6.html
http://www.kisa.or.kr/K_trend/KisaNews/200011/Trend7.html
http://www.kisa.or.kr/isms/intro_01.html

성 경

1988년 목원대학교 전자정보학과
1993년 경희대학교 전자계산학과 석사
2000년 한남대학교 컴퓨터공학과 박사수료
1994~ 현재 동해대학교 컴퓨터공학과 조교수
관심분야 : 정보보호, 신경회로망

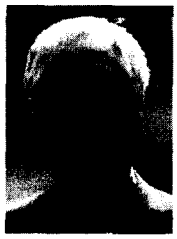
소 우 영

1979년 중앙대학교 전산학과 (공학사)
1981년 서울대학교 계산통계학과(이학 석사)
1991년 메릴랜드대학교 전산학과(이학박사)
1991년 ~ 현재 한남대학교 컴퓨터공학과 교수
관심분야 : 정보보호, 신경회로망, 인공지능

최 상 용

2000년 한남대학교 수학과
2001년~ 현재 한남대학교 컴퓨터공학과 석사과정
관심분야 : 정보보호, 시뮬레이션

김 성 옥



1966년 연세대학교 수학과
1976년 Univ. of Minn. 전산학과 이학석사
1989년 연세대학교 수학과(전산전공)이학박사
1983년 ~ 현재 한남대학교 컴퓨터공학과 교수
관심분야 : 수치해석, 시뮬레이션