웹기반 보안 관리 수준 분석 도구★

김점구* · 최경호** · 노시춘* · 이도현***

요 약

기존의 보안 관리 수준을 측정하기 위한 방법들이 다양하지만 IT 자산을 중심으로 한 평가만이 이루어지고 있는 관계로 조직 전반에 걸친 분석이 이루어지지 못했다. 따라서 본 논문에서는 보안 관리 수준 점검을 손쉽게 할 수 있도록 웹 기반 보안 관리 수준 분석 도구에 대해 제시한다. 본 도구의 경우는 전사적 정보 보호 관리 방법론인 ISO 27001의 보안통제 항목들을 기반으로 설문 내용을 구성하였다.

Tools for Web-Based Security Management Level Analysis

Jeom Goo Kim* · Kyong Ho Choi** · Si Choon Noh* · Do Hyeon Lee***

ABSTRACT

Today, the typical web hacking attacks are cross-site scripting(XSS) attacks, injection vulnerabilities, malicious file execution and insecure direct object reference included. Web hacking security systems, access control solutions, access only to the web service and flow inside but do not control the packet. So you have been illegally modified to pass the packet even if the packet is considered as a unnormal packet. The defense system is to fail to appropriate controls. Therefore, in order to ensure a successful web services diagnostic system development is necessary. Web application diagnostic system is real and urgent need and alternative. The diagnostic system development process must be carried out step of established diagnostic systems, diagnostic scoping web system vulnerabilities, web application, analysis, security vulnerability assessment and selecting items. And diagnostic system as required by the web system environment using tools, programming languages, interfaces, parameters must be set.

keywords : Web-based, Security management, ISO 27001

접수일(2012년 5월 31일), 수정일(1차: 2012년 6월 10일), 게재확정일(2012년 6월 11일)

★ 본 연구는 2012년도 지식경제부 지역혁신센터사업인 산업기술보호특화센터 지원으로 수행되었음.

* 남서울대학교 컴퓨터학과

** 경기대학교 산업기술보호특화센터

*** 남서울대학교 IT융합기술사업단

1. 서 론

오늘날 많은 조직들이 조직의 목적 달성을 위하여 정보 시스템 구축에 힘쓰고 있다. 정보 시스템은 조직의 목적 달성을 위해 반드시 필요한 것으로 조직의 모든 Business Process에 영향을 미치게 되는 불가분의 관계이다. 대부분의 조직에서 IT 자원들은 이러한 조직의 Business Process에 따라서 이용 가능한 자원들이 정해지거나 달라진다. 왜냐하면 조직에서 거의 대부분의 작업들이 정보 시스템을 통하여 이루어지고 있으며, 데이터의 이동 또한 컴퓨터를 통해 이루어지고 있기 때문이다. 하지만 조직들이 시스템 구축에 급급한 나머지 시스템 관리부분에서 많은 부분 허점이 노출되고 있고 실제로 위험이 발생하고 있다. 아무리 정보 시스템이 잘 구축되어 있다 하더라도 시스템을 보호하고 있는 환경이나 운용하고 있는 인력 수준에 따라서 위험의 정도가 달라진다. 즉, 위험이란 것이 단순히 IT 자원만의 문제로 인한 것이 아니라 물리적, 환경적인 부분에서도 많이 발생된다는 것이다. 일례로 정보화의 역기능 발생 사례를 살펴보면 70% 이상이 기술적인 부분이 아닌 물리적, 환경적인 부분에서 발생된다고 한다. 따라서 정보를 보호하기 위한 방편으로 기술적인 부분도 중요하지만 그 외의 인적, 물리적, 환경적 관점에서 접근하는 것도 매우 중요하다[1].

본 논문에서는 조직에서 위험이 노출되는 부분을 사전에 미리 감지하여 자신 조직의 보안 수준이 어느 정도 인지를 웹을 통하여 확인하고 점검할 수 있는 도구를 제시하고 자 한다. 본 논문의 2장에서는 국내・외 정보 보호 관리 기준들에 대해서 비교하고 3장에서는 보안 관리를 위한 수준 평가 방법에 대해 제시한다. 4장에서는 제시된 보안 관리를 위한 수준 평가 방법에 대하여 사례 연구를 통해 실제 활용 방안을 살펴보고 5장에서는 본 논문을 통해 얻을 수 있는 점과 보완할 점을 제시하는 것으로 결론을 맺는다.

2. 관련 연구

2.1 업무 연속성 측면에서의 보안 수준 관리

정보화의 역기능으로 인하여 조직의 업무의 연속성에 영향을 미치게 되면 재정적인 면은 물론이거니와 조직의 이미지 실추 등으로 나타나게 된다. 업무의 연속성이라는 것은 조직이 어떠한 문제로 인하여 운영상 어려움이 발생하였다 하더라도 업무를 멈추지 않고 적절하게 지속하는 것을 뜻한다. 이러한 영향 때문에 대부분의 정보 보호 관리 기준들에서도 업무 연속성 측면을 상당 부분 고려하고 있다. 예를 들어 BS 7799 : 1999(Information Security Management)의 세션 11[2], ISO/IEC 13335(GMITS)[3] 와 NIST의 SP 800 시리즈[4] 등에서도 업무 연속성 계획에 대한 절차에 대해서 언급하고 있다[5].

2.2 국내・외 정보 보호 관리 기준

<표 1> 관리 기준 비교

구분	관리기준(국내)	ISO/IEC 13335	연구 개발은	SSE-CMM
작성기관	KISA	ISO/IEC JTC1	영국 BSI	미국 ISSEA
특징	- 연구 개발은을 국내 실정에 맞도록 문서화 - 연구 개발은보다 교육 훈련 부분을 구체화하고 일부분을 축소시킴	- 여러 표준 문서에서 자료를 수집하여 이를 체계적으로 정리한 보고서로 지침 성격을 가짐 - 조직이 보유한 정보자산이 주요 대상	- 정보보호 관리체계를 효율적으로 수립, 수행, 감시하기 위한 방법론 제시 - 조직 상호간의 신뢰성 있는 거래를 위한 기준	- ISO/IEC 12207에 기초한 IT 정보보호프로세스 성숙도 측정 - 정보보호관리 지침에 보조적으로 사용가능
작성 년도	2001	1996	1999	1999.4
작성 목적	정보보호관리 체계 수립/인증	IT 보호관리	정보보호관리 체계 수립/인증	IT 시스템 보호관리
적용 범위	전사적	IT	전사적	IT 시스템
통제사항분류	13개 분야	조직적&물리적 7개 분야 IT 시스템분야 5개 분야	10개 분야	기본/프로젝트 및 조직 22개 분야
통제사항 수	131개	63개	127개	123개

<표 2> 인터넷 설문조사의 장·단점[10]

장점	단점
· 표본수가 많아져도 추가비용이 들지 않음 · 고수입, 고도기술전문가들의 특정집단에 쉽게 접근가능 · 인터뷰 비용없이 사용자와 상호작용 · 신제품, 신기술의 잠재적 성패를 측정할 수 있는 의견 수집 가능 · 설문응답의 빠른 회수가 가능 · Java, VBScript, ActiveX기술 등의 활용 · 설문 응답이 편리 · 24시간 수행 가능	· 인터넷 사용인구에 국한 · 주된 리서치 방법론이 아니므로, 다른 조사 방법론과 의 비교와 경험을 통해 여타 방법론과 동일선상에 도달할 필요성이 있음. · 인터넷 표본은 전체 인구를 비 대표함 · 자기 기입 표본의 문제 · 설문 응답자에게 지불하는 인센티브 문제 · 설문 조사 시스템 설치의 고정 비용 · 응답자의 프라이버시에 관한 문제

정보 보호 관리는 위험 관리의 상위 개념이며 위험 관리는 위험 분석의 상위 개념으로 하위 개념들을 모두 포함한다. 정보 보호 관리는 조직의 정보 시스템에 대한 전반적인 사항을 다루며 정보보호에 관련된 업무를 몇 개의 통제 분야(클래스)로 나누고 각 통제 분야별로 다수의 통제 대책(컴포넌트)으로 구성된다. 이러한 정보 보호 관리 기준들의 예로 영국 BSI의 연구 개발은(ISO/IEC 17799 : 2000은 Part 1이 국제 표준으로 인정된 것임)와 카네기 멜론 대학의 SSE-CMM [6], ISO/IEC 13335(Guidelines for the Management of IT Security : GMITS)과 국내의 정보보호 관리 기준 등이 있다[7].

국내·외 정보 보호와 관련한 기준들이 많이 있지만 앞서 설명한 것과 같이 물리적, 환경적인 부분까지 고려하여 평가가 이루어지는 즉, 전사적으로 보안 수준을 점검 할 수 있도록 제시하고 있는 기준들은 연구 개발은나 국내의 정보보호 관리 기준 정도이다.

ISO/IEC 13335(GMITS)의 경우는 기본적으로 IT 보호 관리를 목적으로 작성되었고, 조직이 보유하고 있는 정보 자산이 주요 대상이라고 볼 수 있다. 또한 카네기 멜론 대학의 SSE-CMM의 경우는 IT 정보 보호 프로세스에 매핑 시켜 성숙도를 측정하는 수단으로 이용하기 때문에 기존의 프로세스들이 오래 동안 적용되면서 프로세스들의 성숙도를 측정하고 분석하는 것이다. 따라서 기본적으로 정보 시스템 구축 정도가 오래 되지 않은 우리나라 실정에서는 맞지 않다.

ISO27001의 경우는 '인증'과 연결되어 활용되기는 하지만 인증만을 목적으로 하는 것이 아니라 광범위하고 총체적인 'Best Practice'를 제시하여 정보보호 관리를 실행함에 있어서 평가 지표나 적절한 대책 선택을 위한 방법으로 활용 될 수 있다. 또 국내의 정보보호 관리 기준 역시 이러한 연구 개발은의 수준을 프로세스별로 내용을 더하거나 삭제하여 우리나라의 수준에 맞도록 수정한 것이다. 따라서 본 논문에서는 연구 개발은을 보안 수준 평가에 이용하도록 한다. <표 1>은 국내·외 관리 기준들에 대하여 비교한 것이다.

2.3 인터넷을 이용한 설문 방법

본 논문에서는 보안 수준 평가의 방법으로 인터넷을 통한 설문을 통하여 얻어진 결과를 토대로 보안 수준을 측정한다. 설문은 통계 조사의 한 방법으로 전체 대상에 대한 문제의 답이나 그 특성(일반적인 경향)을 찾기 위해 대상의 일부, 혹은 집단을 표본 추출하여 자료를 수집하고 정리, 분석함으로써 그 경향을 알아보는 것이다[8]. 이런 설문을 웹을 통하여 실시하게 되는 데 기존의 설문 방법과 방법론 측면에서는 상당히 유사하지만 인터넷이란 매체 환경의 특성을 이용하여 "즉각적인 상호작용"이 가능하다는 점[solomon, 1995]과 멀티미디어 적인 디자인 요소가 사용된다는 데 가장 큰 차이가 있다[9]. 인터넷을 통한 설문조사의 장·단점을 정리하면 <표 2>와 같다.

3. 보안 관리 수준 평가

3.1 보안 관리 수준 평가 설문 항목

본 논문에서는 앞서 2.2절에서 설명한 것과 같이 설문으로 얻어진 결과가 최대한 조직의 전반에 걸친 보안 관리 수준을 이끌어 낼 수 있도록 하기 위하여 많은 정보 보호 관리 기준들 중에서 ISO27001을 이용하도록 한다. ISO27001에서는 인증을 받기 전에 미리

자신들의 조직의 보안 관리 수준을 측정할 수 있도록 지침으로 제시하고 있는데 그 지침은 연구 개발은의 서브셋인 PD시리즈이다. 연구 개발은의 PD시리즈의 문서들은 기존의 조직이 가지고 있는 보안 정책과 위험 관리에 대한 사항과 항목들이 BS7799의 기준에 적절한 지에 대해 자체적으로 평가하고 그에 따른 보안 통제 항목을 제시하는 문서들이다. 보안 통제 항목을 선정하여 지침으로서 제공하고 있는 것이 PD 시리즈 중에서 PD 3002로 내용에 바로 연구 개발은 Part 1. "Code of Practices for Information Security Management"[2]가 포함되어 있다. 본 논문에서는 이러한 연구 개발은의 내용을 토대로 설문항목을 구성하였다.

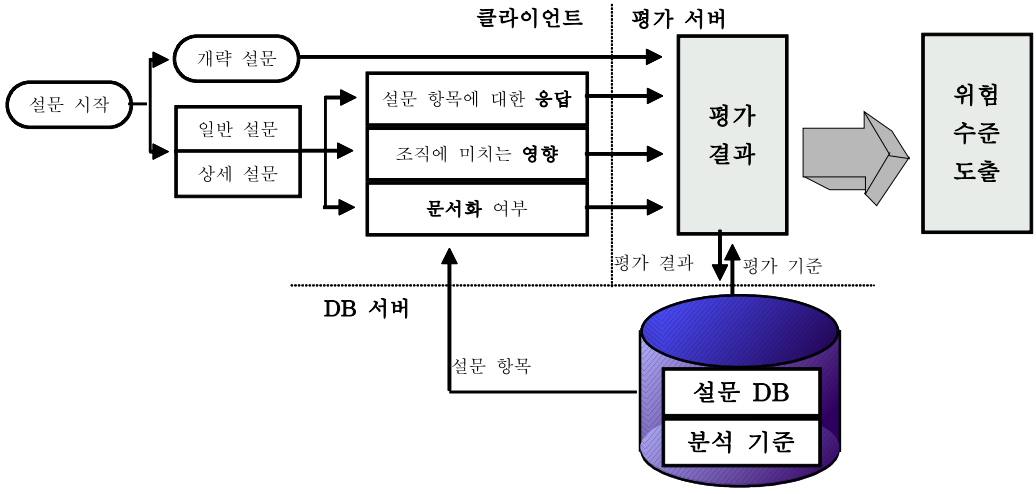
3.2 보안 관리 수준 평가 기준과 평가 방법

설문으로 얻어진 결과에 따라 보안 관리 수준을 도출하기 위한 기준이 필요하다. 기준으로는 CSI의 IPAK[11] 평가 방법에 따른다. IPAK은 세부 체크리스트에는 핵심적이고 실제적인 내용들이 포함되어 있어서 짧은 시간 내에 주요 실행 항목들의 내용들을 파악할 수 있다는 이점이 존재하지만 대영역 내에 세부 영역들이 세분화되어 있지 않는 문제점과 흔히 사용되지 않는 영역의 보안 관리 내용까지도 포함하고 있어서 전반적인 정보보호 관리 기준으로 활용하기에는 무리가 있다[12]. 하지만 IPAK의 평가 방법의 경우, 각 항목들에 대한 영향 평가와 함께 문서화 여부까지도 파악하여 평가에 반영하게 되어 있어서 좀 더 효과적이고 직접적인 평가가 가능하다. 또한 연구 개발은에서도 문서화의 중요성을 강조하고 있으므로 평가 방법으로 이용하기에 적합하다. 따라서 본 논문에서는 이러한 IPAK의 방법을 이용하기로 한다. 전체적인 평가는 (그림 1)과 같다. IPAK의 방법[13]을 이용하여 만든 평가 매트릭스는 <표 3>과 같다.

또한 평가 매트릭스에 따라 도출된 수준과 그에 따른 해석은 <표 4>와 같이 이루어진다. 위험 수준에 따른 해석은 NIST의 SP800-30 "Risk Management Guide for Information Technology Systems"[14]를 이용하였다.

각 설문 항목에 대한 영향 분석과 문서화 여부를 판단하여 위험 수준을 판별하게 되므로 모든 부분에서 보안 대책을 강구할 필요 없이 해당 설문의 수준에서만 보안 대책을 강구할 수 있으므로 조직에서 보안 대책으로 인한 비용을 감소할 수 있다.

보안 관리 수준의 도출을 앞서 설명한 것과 같이 해당 설문 항목이 조직에 미치는 영향과 함께 준수여부, 문서화 여부를 함께 판단하도록 하였다. 문서화 여부의 중요성은 연구 개발은에서도 강조하고 있는 부분으로써 본 논문에서도 상당히 중요한 부분으로 여기고 있다. 따라서 IPAK에서 문서화 여부에 가중치를 부여하여 위험 수준을 측정하는 방법은 본 논문의 목적과도 일치한다.



(그림 1) 설문의 처리과정

<표 3> 평가 매트릭스

		질문항목(보안통제사항)					
		1		2		3	
문서화		0 (잘됨)	1 (안됨)	0 (잘됨)	1 (안됨)	0 (잘됨)	1 (안됨)
영향	1(낮음)	1	2	2	3	3	4
	2(보통)	2	3	4	5	6	7
	3(높음)	3	4	6	7	9	10

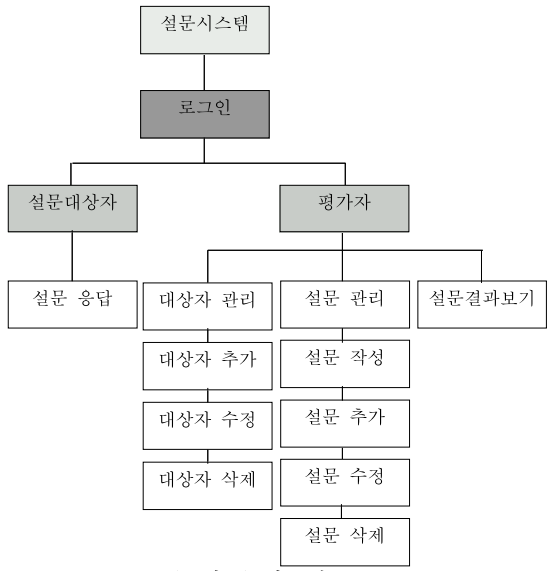
<표 4> 위험 수준과 해석

위험 수준	평가 매트릭스의 결과	해석
1(낮음)	1, 2, 3	조직의 관리자는 해당 분야에 대한 수정된 행동이 필요한지 또는 그 위험을 수용해야 할 지를 결정해야 함.
2(중간)	4, 5, 6	해당 분야에 대한 수정대책이 필요하고, 계획하여 바람직한 기간 내에 이들 행동을 수행하도록 하여야 함.
3(높음)	7. 8. 9. 10	해당 분야에 대한 수정대책이 강력히 필요하고, 기존의 행동들로 계속적인 운영이 가능하나 수정계획을 최대한 빨리 세워서 개발하여야 함.

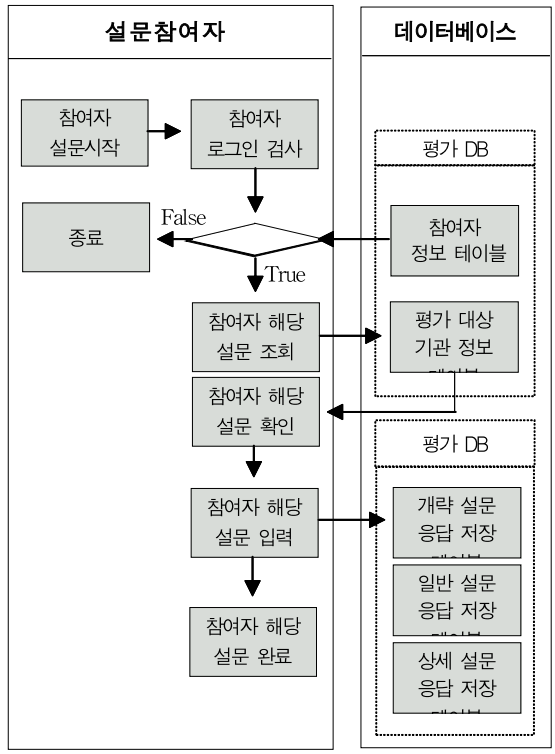
4. 사례 연구

4.1 웹 기반 보안 관리 수준 평가 시스템 설계

본 논문에서 데이터 베이스는 MySQL을 사용하였고 전체적인 시스템 구조는 (그림 2)와 같고 간략한 설문의 순서와 데이터베이스에 저장되어 있는 테이블과의 관계는 (그림 3)에서 보여주고 있다.



(그림 2) 시스템 구조



(그림 3) 절차와 DB테이블 관계

4.2 설문의 표본 추출

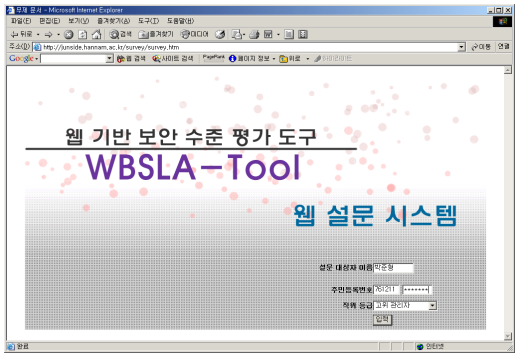
본 논문에서 적용할 표본 추출 방법은 확률 추출방법을 사용하였으며 확률 표본 추출 방법은 모집단의 구성요소들에게 표본을 추출할 수 있는 기회를 균등하게 부여한 상태 하에서 표본을 추출하는 방법이다. 확률 표본 추출 방법에 속하는 방법에는 단순 무작위 표출(simple random sampling), 층화 표출(stratified sampling), 집락 표출(cluster sampling), 체계적 표출(systematic sampling) 등이 있고 본 논문에서는 층화 표출 방법을 사용한다.

층화 표출 방법은 모집단을 일정한 기준에 따라 계층화된 각 계층으로부터 필요한 숫자만큼 표본을 추출하는 방법이다. 즉 모집단을 하나의 목록으로 묶는 단순 무작위 표본 추출방법과는 달리, 층화 표출 방법은 모집단을 여러 개의 소집단 목록으로 분할한 후에 각 목록으로부터 표본을 추출하여 통합하는 방법이다 [15].

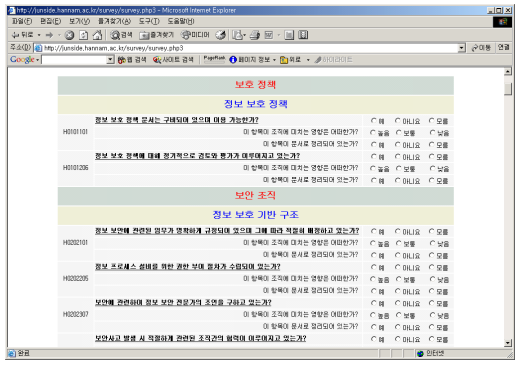
즉, 평가를 받는 조직에서 설문을 위한 설문 대상자를 선정할 때 부서와 직위에 따라서 대상자를 선정하게 되면 직위와 부서에 따른 보안 수준 점검 결과를 얻을 수 있게 된다. 따라서 좀더 믿을 만한 보안 수준을 도출해 낼 수 있다.

4.3 설문 시스템 설계 화면

아래 (그림 4)는 본 논문을 통해 설계한 설문 시스템의 초기화면이다. 본 시스템의 경우 보안 수준 점검 프로젝트를 실시할 경우에 프로젝트 ID와 직위를 선택하고 설문에 응하게 된다.



(그림 4) 시스템 초기화면



(그림 5) 설문 화면

설문 대상자의 경우는 단순한 설문만 화면에 출력되며 관리자의 경우에는 시스템 관리를 위한 부분이 출력된다. (그림 5)은 설문 대상자의 설문 화면이다. 설문은 조직에서 점검 수준의 깊이에 따라 개략, 일반, 상세 설문의 3가지를 선택할 수 있다. 설문은 각 문항 당 하나의 답을 반드시 선택해야 하고 모든 문항에 대한 응답이 끝나야만 설문이 종료된다.

본 논문에서 보안 수준 점검 도구는 기존의 종이로 하는 설문으로 인한 단점인 비용의 문제와 설문회수의 문제를 웹을 통한 설문으로 해결하였고, 조직의 보안 수준을 손쉬운 설문을 통해 파악할 수 있다는 장점이 있다.

5. 결 론

본 논문에서는 ISO 27001의 보안 통제 항목을 토대로 내용을 구성하여 웹을 기반으로 한 보안 수준 점검 도구를 설계하였다.

기존의 보안 수준 점검 도구의 경우는 IT자산에 너무 치우친 나머지 조직의 관리적, 환경적인 부분을 간과하였고 종이를 통한 설문을 하였던 관계로 설문이 갖는 기본적인 문제를 극복하지는 못했다. 하지만 본 논문을 통해 구현한 웹 기반 보안 수준 점검 도구의 경우는 기존 설문이 갖는 문제점을 극복했을 뿐 아니라 보안 수준의 점검을 웹을 통해 하게 됨으로써 경비 절감과 동시에 조직 자체 내에서 간단하게 점검할 수 있게 되었다는 점이 장점이라고 할 수 있다.

현재 본 보안 수준 점검 도구의 경우는 앞서 설명

한 것과 같이 조직의 높은 관점에서 보안 수준 점검이 이루어지고 있다. 이런 점검 결과가 세부적인 위험분석을 행하는데 있어 반영될 수 있는 서로간의 상관관계를 고려하는 즉, 보안 수준 점검 결과를 세부적인 위험분석에서 반영하여 이용할 수 있는 방법을 향후 과제로 남긴다.

참고문헌

[1] 이강신 외, “국내·외 정보보호 관리 모델에 관한 고찰”, 정보보호학회지 제 11 권 제 3호, 2001. 6, pp 24-37.

[2] BSI, "Information security management - Part 1 : Code of Practices for Information Security Management", 연구 개발은-1:1999, 1999.

[3] ISO/IEC, "Guidelines for the Management of IT Security(GMITS)," TR 13335, 2000. 3.

[4] NIST, SP300-3, 4, 12, 14, 16, 18, http://www.nist.gov.

[5] 박정현, “업무 연속성 유지를 위한 5단계와 프로젝트 시작 및 관리," 정보보호 21C, 2002. 3, pp78-80.

[6] SSE-CMM, "Project, Systems Security Engineering Capability Maturity Model(SSE-CMM) - *Model Description Document*," V.2, http://www.sse-cmm.org, 1999. 4.

[7] 박현우 외, “정보 시스템을 위한 범용 웹기반 위험분석 프로세스," 2002 한국 디지털 컨텐츠 학회 학술 대회(DCS 2002) 논문집, Vol.3, 2002. 12, pp 205-209.

[8] 정효숙 외, "표본 조사 학습을 위한 웹 설문 분석 시스템의 설계 및 구현," 한국 정보 교육 학회, 정보 교육 학회 논문지, 2000, pp375-384.

[9] 김광용 외 “웹 설문 조사의 기술적 방법론 문제에 관한 연구," 한국 경영 학회, 1999년도 하계 경영학 관련 통합 학술 대회 발표 논문집, 1999, pp237-242.

[10] 김광용 외, “인터넷 설문 조사를 활용한 사이버 쇼핑몰 디자인에 관한 연구," 경영 정보학 연구 제 9 권 제 2 호, 1999. 6, pp133-150.

[11] CSI, "IPAK(Information Protection Assessment Kit)," http://www.gocsi.com.

[12] 신수정, “주요 정보보호 실행 기준들의 구조 및 특징," 정보보호 21C, 2002. 4, pp76-81.

[13] 조태희, "주요 정보통신 기반시설 취약점 분석·평가 모델," KISA KTnet-2002 발표자료, 2002.

[14] NIST, "Risk Management Guide for Information Technology Systems," SP800-30, Oct. 2001.

[15] 이경서, “조사 방법론," 학문사, 2001.

[저 자 소 개]

김 점 구 (Jeom Goo Kim)

1990년 2월 광운대학교
전자계산학과 이학사
1997년 8월 광운대학교
전자계산학과 석사
2000년 8월 한남대학교
컴퓨터공학 박사
1999년 3월~ 현재 남서울대학교
컴퓨터학과 교수
IT융합연구소장

email : jgoo@nsu.ac.kr

노 시 춘 (Si Choon Noh)

1987년2월 : 고려대학교
경영정보학 석사
2005년2월 : 경기대학교
정보보호기술 박사
2002년11월 : KT 시스템보안부장
2004년 12월 : KT 충청전산국장
2005년3월 ~ 현재 :남서울대학교
컴퓨터학과 교수
IT융합연구소연구위원

email : nsc321@nsu.ac.kr

최 경 호 (KyongHo Choi)

2002년 경기대학교 경제학사
2005년 경기대학교 경제학석사
2008년 경기대학교 정보보호학박사
2012년 경기대학교 연구교수
(산업기술보호특화센터)

email : cyberckh@gmail.com

이 도 현 (Do Hyeon Lee)

2001년2월 한양대학교
전자전기공학부
공학사
2003년8월 한양대학교
전자통신전파공학과
공학석사
2011년2월 한양대학교
전자컴퓨터통신공학과
공학박사
2011년4월 ~ 현재 남서울대학교
IT융합기술사업단
연구교수

email : itt@nsu.ac.kr