정보시스템 안전성 평가 도구 설계 및 구현

홍승구*, 김 강** 박진섭*
*대전대학교 컴퓨터정보통신공학부
**강원관광대학 컴퓨터정보계열

Design and Implementation on Evaluation Tool for Security of the Information System

Seung-Goo Hong*, Kang Kim** Jin-sub Park*
*Dept. of Computer and Communications Engineering, Daejeon Univ.
**Dept. of Computer Information KangWon Tourism College
E-mail : sghong@zeus.dju.ac.kr

요 약

본 논문에서는 정보보호관리체계와 위험분석방법을 적용한 안전성 평가 도구를 설계하였다. 또한, 위험평가시 동일한 가중치를 적용한 평가와 조직의 특성에 따라 보안요소의 가중치를 가변적으로 적용한 평가를 할 수 있도록 하였으며, 각 조직이 자체적으로 보안 점검을 할 수 있도록 설계함으로서 관리적 측면에서 취약점을 쉽게 찾을 수 있도록 지원하며, 수행해야 할 권고를 제시한다.

1. 서 론

컴퓨터를 통한 정보의 처리, 관리, 저장, 유통 등이 보편화되고 각 조직에서는 컴퓨터와 관리되고 있는 정보의 의존도가 높아지고 있다.(정보화 순기능)

이와 같은 정보는 초고속통신망의 집약적인 발전과 인터넷의 확산으로 막대한 양의 정보를 공유하게 되었고, 누구나 손쉽게 원하는 정보를 얻을 수 있게 되었다.

그러나, 최근에는 정보화의 역기능 현상으로 해킹, 바이러스, 개인정보의 불법적 유출, 스팸메일 등의 피해 및 위협이 심각한 사회문제로 대두됨으로써 정보보호의 중요성이 증대되고 사회 각 분야에서 정보보호기술에 대한 관심이 고조되고 있다.

최근에 발생하는 보안사고는 예전의 호기심을 가진 일부에 의한 개별적이고 산발적인 보안사고와는 달리 조직적이고, 전문적이며, 집중적인 양상으로 확산되고 있다.

따라서 체계적이고 종합적인 정보보호관리체계가 요구되고 있으며, 이를 통한 정보자산 등에 대한 정보보호관리체계 인증제도를 적용하여 정보통신환경의 안전·신뢰성을 확보할 필요성이 증대되고 있다.

대부분의 조직에서 정보시스템의 의존도가 높아짐에 따라 보안사고에 대한 대책마련이 요구되며, 대책마련을 위해서는 전반적인 보안요소를 고려한 종합적인 정보시스템 안전성 평가도구가 요구된다.

본 논문에서는 정보보호관리체계를 기반으로 한 안전성 평가 도구를 설계하고 구현함을 보여준다.

2. 정보보호관리체계

2.1 정보보호관리기준

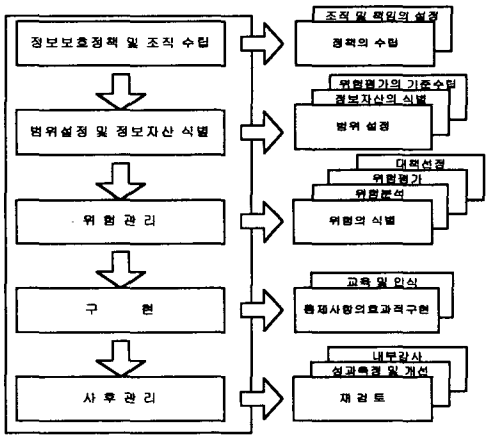
정보보호관리기준이란 조직 일반에 공통적으로 적용될 수 있는 정보보호관리활동에 관한 표준적인 가이드라인을 말하며, 정보보호관리는 정보보호의 분류방식중 하나인 관리적, 기술적, 물리적 대책 분류에서의 관리적 대책만을 다루는 것이 아니라, 보안정책 수립, 위험 분석, 보안대책의 선택·구현, 정보보호시스

템 구축, 보안대책 평가를 하나의 과정(process)으로 인식하여 체계적·종합적으로 관리하는 활동을 총칭하는 개념이다.

최근 전세계적으로 해킹 및 바이러스 침해사고가 빈발하고 인터넷을 활용한 서비스 제공이 본격화되면서 정보보호라는 것이 기술적 이슈가 아닌 관리상의 문제라는 인식이 빠르게 확산되고 정보보호를 조직전체 차원에서 체계적으로 관리하는 정보보호관리(Information Security Management)에 대한 국제적 관심이 고조되고 있으며 국내에서도 이에 대한 연구가 진행되고 있다.

2.2 정보보호관리과정

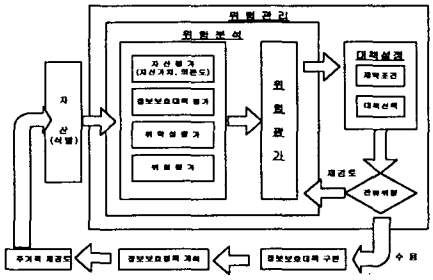
정보보호관리과정은 (그림 1)에서와 같이 5과정 14개 항목으로 이루어져 있으며, 각 과정에서 세부지침을 작성하여 조직이 정보보호관리의 목표에 도달할 수 있도록 계획하고 있다.



(그림 1) 정보보호관리 과정

3. 위험분석

3.1.1 위험분석 모델



(그림 2) 위험분석 모델

위험분석은 (그림 2)에서와 같이 위험관리 과정의 한 분야로서 정보시스템 보안정책(IT Security Policy)이 수립된 후 위험관리를 수행할 때 필요한 첫 번째 과정이다. 위험분석의 목적은 보호되어야할 대상 정보시스템과 조직의 위험을 측정하는 것이다. 또한 위험분석은 측정된 위험이 통제되어야 할 위험인지 아니면 받아들여질 수 있는 위험인지를 판단할 수 있도록 근거를 제공한다.

3.1.2 자산분석

자산분석은 자산식별을 통하여 조직의 자산을 파악하고, 자산의 가치 및 중요도를 산출하며, 정보자산과 업무처리와의 관계도 알아낼 수 있다. 자산평가는 위험분석 결과의 정확도를 결정하는 매우 중요한 과정이다.

자산식별 과정은 크게 자산 조사와 자산가치산정의 2가지로 나눌 수 있으며, 자산조사과정에서는 조사할 자산의 범위를 설정하고, 자산목록을 작성한다. 자산가치산정 과정에서는 자산을 정량적 또는 정성적으로 산출하는 기준과 절차를 정의한다.

3.1.3 위협 분석

자산은 다양한 종류의 위협에 처해 있다. 위협은 시스템, 조직, 조직의 자산에 피해를 주는 원치 않는 사고를 일으킬 잠재성을 갖는다. 이러한 피해는 비인가된 파괴, 공개, 변경, 훼손, 불가용성, 손실 등 IT 시스템에 의해 처리되는 정보 또는 서비스에 대한 직·간접의 공격으로부터 발생할 수 있다. 자산에 피해를 입히기 위하여 위협은 자산의 취약점을 파고든다. 위협은 자연적이거나 사람의 의도에 의한 것일 수 있으며 우연히 또는 계획적으로 발생한다. 두 경우 모두 위협을 식별하고 그 수준과 가능성을 평가해야 한다.

3.1.4 취약성

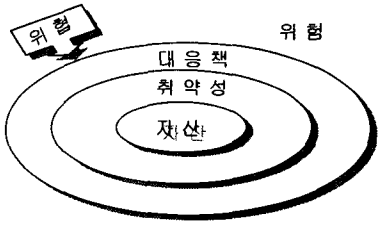
자산과 관련된 취약성은 물리적 배치, 조직, 절차, 인력, 관리, 행정, 하드웨어, 소프트웨어 또는 정보상의 약점을 포함한다. 취약성은 IT 시스템이나 사업목표에 유해한 위협이 침투하는 경로가 되지만 취약성 자체는 피해를 일으키지 않는다. 취약성은 단지 하나의 조건 즉, 위협에 의해 자산이 피해를 입게 되는 일련의 조건이다. 다양한 근원의 취약성을 고려한다.

3.1.5 위험평가

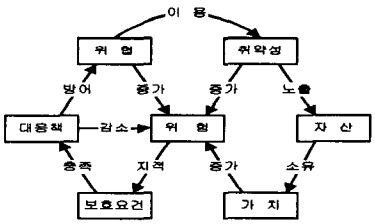
위험은 위협이 자산의 취약성을 이용하여 직접적이

거나 간접적인 피해를 유발할 수 있는 잠재적인 가능성이다. 따라서 위험이 높다는 의미는 이러한 가능성이 높다는 의미이다.

영향은 위협의 발생으로 인하여 자산에 실질적으로 가해진 사건의 결과이다. 그로 인하여 자산은 위협이 가지고 있는 4가지(파괴, 변조, 폭로, 거부) 피해를 입게 되며 이는 자산에 대한 기밀성, 무결성, 인증성, 가용성, 책임추적성, 신뢰성 등에 손실을 주게 된다. 영향을 표현하는 방법은 여러 가지 있지만 크게 정량적인 방법과 정성적인 방법으로 구분될 수 있다.



(그림 3) 위험 요소들과의 관계(1)



(그림 4) 위험 요소들과의 관계(2)

4. 평가도구의 설계 및 구현

4.1 평가 요소

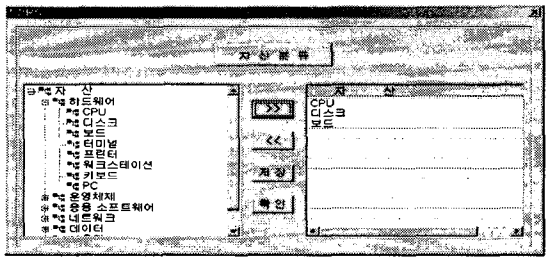
평가는 자산과 정보보호정책으로 구분하여 평가를 하였다. 평가를 위해서는 먼저, 평가목록을 작성하는데 목록에는 범위 설정을 통하여 파악된 조직의 규모와 운영목적 및 환경을 바탕으로 요소들을 분류하고, 또한, 평가요소는 파악된 핵심업무처리(Business Process)와 기타기준의 범위내에서 작성하였다. 작성시 고려사항은 다음과 같다.

- 목록별 분류 및 범위에 따른 분류
- 업무처리를 고려한 조사
- 조직을 고려한 조사
- 업무처리와 요소와의 관계정립
- 항목별 분류 및 조사

4.1.1 항목별 분류 및 조사

항목별 분류 및 조사방법은 IT 관점에서 체계적으로 파악하고 관리하기에 용이하다. 그러나 업무처리를 파악하는 데는 어려움이 많다. 항목별 분류 및 조사는 유형과 성질을 바탕으로 7개의 대분류로 나누고, 이를 다시 세분화해서 분류 뒤 목록을 작성하였다.

- 하드웨어(H/W) : CPU, 디스크, 보드, 터미널, 프린터, 워크스테이션, 키보드 등
- 운영체제(O/S) : UNIX, Windows98, LINUX, NT 서버, Solaris 등
- 응용소프트웨어(Application) : 소스프로그램, 문서편집 프로그램, 진단프로그램, 개발프로그램, 정보처리프로그램, 각종 유틸리티 등
- 네트워크(Network) : 허브, 라우터, 게이트웨이, 방화벽 등
- 데이터(Data) : 실행중인 자료, 문서데이터, 백업데이터 등
- 사용자(Users) : 관리자, 일반사용자, 개발자, 경영자
- 환경(Environment) : 전산실 등



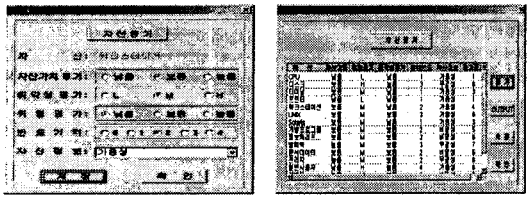
(그림 5) 항목별 자산분류

4.1.2 업무처리별 분류 및 조사

일반적으로 IT업무처리시 대상조직들이 잠재하고 있는 위험(Risk)요소의 실체를 파악하는데 부족하다. 궁극적으로 IT 자산이 조합되어 수행되어지는 업무처리에 대해 가해지는 것이다. 업무처리와 자산간의 관계를 정립함으로서 각 자산의 가치와 중요도를 더욱 정확하게 파악할 수 있다.

4.2 자산 평가

자산평가는 자산의 가치평가, 취약성평가, 위협평가, 발생빈도에 따른 가치평가, 자산 정보 등 5단계로 구분하여 평가를 하였다. 각각의 평가는 정성적 평가를 실시하였고, 평가에 따라 자산의 등급을 결정하였다. 그리고, 자산의 정보 평가를 바탕으로 조직의 가중치를 결정하는데 자산정보에는 가용성, 무결성, 기밀성 등으로 구분하여 비중이 많은 순으로 가중치를 정보보호 평가에 적용하였다.



(그림 6) 자산평가

4.3 정보보호 평가

정보보호평가 및 취약점 평가는 조직 및 자산이 잠재적으로 갖고 있는 약점으로 근본적인 위험의 원천을 명확히 파악하고 그에 따른 적절한 보안 대책을 수립하는데 목적이 있다.

기존에 제시된 평가방법 중 ISMS요구사항평가 및 세부통제사항과 취약성평가방법을 이용하여 평가하였다.

<표 1> 정보보호 평가 항목

대 분 류	세 부 항 목
요구사항 평가	1. 관리 프레임워크 구축
	2. 구현 실시
	3. 문서화
	4. 문서통제
	5. 기록
세 부 통 제 항 목	1. 정보보호 정책
	2. 정보보호 조직
	3. 제3자의 접근
	4. 자산의 분류와 통제
	5. 인적보안
	6. 물리적 환경적 보안
	7. 컴퓨터와 네트워크 관리
	8. 시스템 접근 통제
	9. 시스템 개발과 유지
	10. 업무 연속성 계획
	11. 요구사항 준수
합 계	

4.4 취약성 분석

취약성분석은 자산을 통하여 도출된 자산의 속성과 중요도를 바탕으로 자산이 근본적으로 가지고 있는 약점인 취약성을 발굴하고 취약성이 전체적인 위험에 미칠 수 있는 영향을 분석하는 과정이다. 따라서 자산의 잠재적인 위험을 산출하고 평가하기 위해 사전 작업으로 자산의 근본적인 약점을 파악하고, 자산의 취약성과의 관계를 파악하여 자산에 미치는 취약성의 영향을 도출하였고, 또한 취약성 등급기준은 위험평가 과정에서 산출되는 취약성 수준을 평가하기 위해 자산가치 산정기준에서 도출된 5단계 등급으로 기준을 정하였다.

<표 2> 취약성 등급

취약성 등급	취약성 수준
Very High	매우 높음
High	비교적 높음
Medium	보 통
Low	낮 음
Negligible	취약성이 거의 없음

특히 취약성분석을 통하여 도출된 분석자료를 바탕으로 위험을 나타내는 취약성 수준을 산출하는 2가지 유형(여러 유형을 나누어 유형별로 수준 산출, 단일객체로 보고 자산별로 수준 산출)을 적용하였다.

4.5 가중치 적용

가중치는 각 기관별로 상이하게 적용하는데 우선 의료기관의 경우, 환자의 개인기록, 진료기록, 영상자료 등 의료정보가 불법적으로 공개되지 않도록 방지해야 하며(기밀성), 제조업의 경우, 정보의 불법적인 파괴나 지체로부터 보호되어야 하고,(가용성) 마지막으로 금융기관은 개인의 금융정보가 해커이나 금융관계자로부터 불법적으로 변조되는 것을 방지해야 한다.(무결성)

이와 같이 기관별 따라 정보보호 우선 순위가 다르며, 동일한 보안사고라도 기관에 따라 피해의 정도는 상이하게 나타난다. 따라서 기관별로 가중치를 차등적으로 적용하는데 가장 비중이 높은 항목을 10점으로 하고 각각 7점, 4점으로 적용한다.

- 항목별 보안요소 구분(포괄적 분류)
- 가용성 : 관리프레임 구축, 인적보안, 물리적 환경적 보안, 컴퓨터/네트워크관리, 시스템개발과 관리유지, 업무연속성관리
- 무결성 : 구현실시, 문서통제, 기록, 문서화, 정보자산의 분류와 통제,
- 기밀성 : 구현실시, 문서통제, 기록, 제3자 접근, 인적보안, 물리적 환경보호, 시스템 접근 통제, 요구사항 준수

항목별 보안요소 구분은 위와 같이 포괄적으로 구분하여 적용하였으나 항목내 세부평가요소는 보안요소별(가용성 무결성, 기밀성)로 적용하였다.

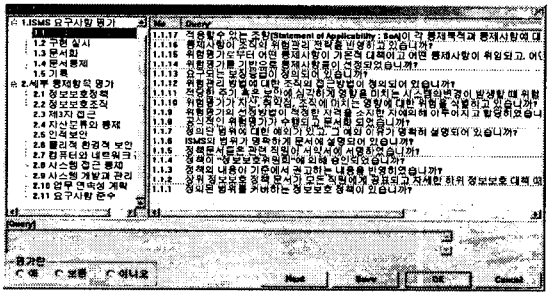
5. 도구 구현결과 및 분석

5.1 평가방법

ISMS 요구사항 평가 및 세부통제사항에 대한 평가를 (그림 7)과 같은 도구를 이용하여 평가를 실시한다. 평가는 각각의 질문에 "예", "아니오", "보통"으로

답하며, 그 결과를 항목단위로 평균값으로 나타낸다.

각 항목에 대한 평가는 1단계에서는 동일한 기준을 적용하여 평가를 실시하며, 2단계에서는 조직의 특성에 따른 가중치에 적용한 후 동일한 평가를 실시한다.

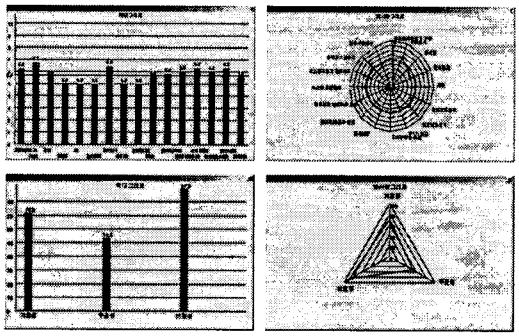


(그림 7) 요구사항 평가(ISMS)

5.2 가중치 변경에 따른 분석

5.2.1 동일한 가중치 적용

(그림 8)는 각 항목들에 동일한 가중치(항목당 10점을 기준)를 적용하여 평가한 결과이다. 각 항목에서 평균보다 작은 부분은 위험이 예상되는 부분으로 안전대책이 강구하여 피해 손실을 최소화하여야 한다.

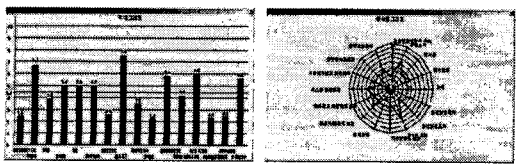


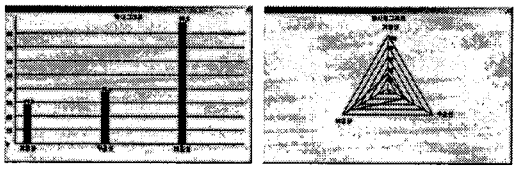
(그림 8) 동일한 가중치를 적용한 경우

5.2.2 기업별 가중치 적용 사례

5.2.2.1 의료기관

의료기관의 경우 기밀성에 대한 비중이 타 기관에 비해 강조되고 있으며 기밀성과 관련된 항목에 가중치의 비중을 두고 평가한 결과이다. (기밀성>무결성>가용성)

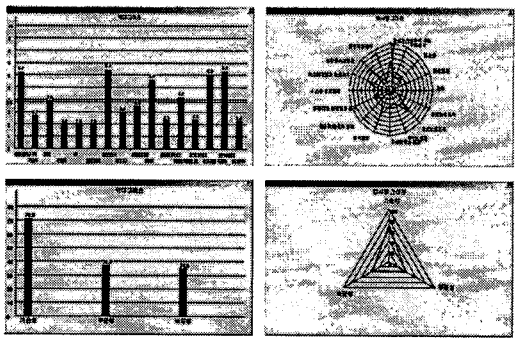




(그림 9) 의료기관의 평가결과

5.2.2.2 제조업

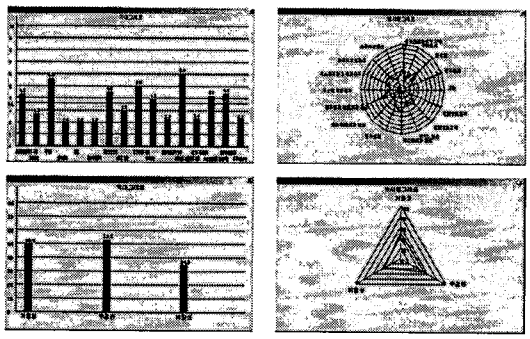
제조업의 경우 가용성항목에 가중치의 비중을 두고 평가를 실시한 결과이다. (가용성>무결성>기밀성)



(그림 10) 제조업의 평가결과

5.2.2.3 금융산업

금융산업의 경우 무결성 요건이 타 기관에 비해 주요시되며 무결성에 비중을 두고 평가한 결과이다. (무결성>가용성>기밀성)



(그림11) 금융기관의 평가결과

해당 조직의 특성을 반영하지 않고 동일한 가중치를 적용하는 경우, 각 조직간의 상대적 평가를 할 수 있어 어느 조직이 정보보호가 잘되어 있는지 그리고 어느 항목이 상대적으로 취약한지를 판가름 할 수 있으나, 보안사고 발생시 어느 항목에 우선을 두고 복구작업을 할 것인지, 또한, 동일한 보안사고가 발생하더라도 조직간의 피해규모는 상이하다는 것을 인정해야

한다.

그러나, 조직의 특성에 따라 차등적으로 가중치를 적용한 경우, 조직에서 우선적으로 보호해야할 정보보호 우선 순위에 따라 보안사고 발생시 피해복구 계획과 피해비용산정 등을 합리적으로 산출할 수 있다.

5.3 평가결과 분석

위험분석을 위해 자동화 도구를 이용하여 소요되는 시간과 비용을 절감하고 분석과정에서의 오차를 줄일 수 있도록 구현하였다.

위험을 분석하여 산출하는 방법으로 정량적 수치(10~4점)로 나타내는 정량적 분석과 위험의 정도를 기술변수(상, 중, 하 또는 높음, 보통, 낮음 등)로 나타내는 정성적 분석이 있는데 위 두 가지 방법을 모두 활용할 수 있도록 구현하였으며, 신뢰성이 있는 정량분석에 비중을 두고 실행한 결과 조직과 환경에 따라 다양한 방법으로 위험 수준이 각기 다르게 나타났음을 알 수 있다.

특히 위험분석 결과 조직에 위협적인 요소라 판단되는 평균이하의 항목에 대한 취약점에 대한 권고안은 우선 순위를 적용하도록 되어있으며, 복구 우선 순위는 조직의 특성에 따른 가중치가 높고, 취약점 권고안에 단계가 높은 항목을 우선으로 하여 복구 우선 순위를 결정하도록 한다.

<표 3> 취약점 권고안

구 분	내 용
1단계	• 평균보다 0.5~1.0 사이의 항목들 • 취약점 요소들에 대한 사전교육
2단계	• 평균보다 1.0~1.5사이의 항목들 • 취약점에 대한 자산의 재분류 및 보안 대책 강구
3단계	• 평균보다 1.5이하의 항목들 • 적극적인 대응책 강구

6. 결 론

본 논문에서는 정보보호관리 기준체계에서 제시하고 있는 통제항목과 각 자산별 체크리스트를 종합적으로 점검 할 수 있는 도구의 설계와 구현을 보여준다. 설계된 도구를 통하여 각 조직이 자체적으로 보안 취약점을 관리적 차원에서 점검하고 대책을 수립 할 수 있는 권고사항을 직관적으로 알아 볼 수 있다.

또한, 각 조직의 업무특성, 즉 기밀성, 가용성, 무결성 등의 보안 핵심요소에 자체적으로 가중치를 고려하여 종합적인 보안 취약점을 점검 할 수 있도록 설계함으로서 각 조직의 보안 담당자가 자가 진단이 가능하도록 설계하였다. 한편 주어진 조건을 변경함으로서 향후 보안 투자 예산의 편성에 우선순위를 결정할 수 있다.

일반적으로 보안사고가 발생된 후 복구 우선순위는 긴급 자산의 가용성측면에서 고려된다고 볼 때 이 도구를 이용함으로서 복구 우선순위 결정 및 업무 연속성 관리에도 활용 될 수 있을 것으로 사료된다.

향후 연구로는 보다 다양한 자산과 세부 통제 항목의 다양성을 고려하고 GUI 환경 보강이 요구되며, 업무별 통제항목의 가중치 설정에 대한 수식화와 일반화가 요구되고 있다. 또한 점검후의 권고안을 구체적으로 제시 할 수 있는 조건의 다양화가 추가 될 수 있다.

참 고 문 헌

[1] "정보보호관리체계(안) 모델", KISA, 2001.

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

[3] "BS7799 Part 2 : The Management Standard".

[4] "BS7799 PD3001 : Preparing for BS7799 Certification".

[5] "BS7799 PD3002 : Guide to BS7799 Risk Assessment and Risk Management".

[6] "BS7799 PD3003 : Are you ready for a BS7799 Audit?".

[7] "BS7799 PD3004 : Guide to BS7799 Auditing".

[8] "BS7799 PD3005 : Selecting BS7799 Controls".

[9] ISO/IEC TR 13335-1: Information technology-Guidelines for the management of IT Security (GMITS) Part 1: Concepts and models for IT Security. 1996.

[10] "ISO/IEC TR 13335-2" : Information technology-GMITS Part 2 : Managing and planning IT Security,1997.

[11] "ISO/IEC TR13335-3" : Information technology - Security techniques - GMITS Part 3: Techniques for the management of IT Security, 1998.

[12] "ISO/IEC TR 13335-4" : Information technology - GMITS - Part 4 : Selection of safeguards, 2000.

[13] "IT Baseline Protection Manual", GISA, 2000.

[16] Donald L. Pipkin, "Information Security Protecting the Global Enterprise", HP, 2000.

[19] "정보통신망 안전·신뢰성에 관한 기준 해설서 개발", 한국정보보호센터, 1999.

[20] "인터넷 정보보호 운영규범 개발", 한국정보보호센터, 1998.

[22] "공공기관 정보시스템을 위한 비상계획 및 재해복구에 관한 지침서", 한국정보통신기술협회, 정보통신단체표준(TTAS.KO-12.0009), 2000.

[23] "공공기관 정보시스템 구축 준비단계의 보안지침서", 한국정보통신기술협회, 정보통신단체표준(TTAS.KO-12.0008), 2000.

[24] "공공정보시스템 보안을 위한 위험분석 표준-위험분석방법론 모델", 한국정보통신기술협회, 정보통신단체표준(TTAS.KO-12.0007), 2000.

[25] "정보보호 관리기준 해설서", 한국정보보호진흥원, 2001.11

[27] http://www.kisa.or.kr/technology/sub3/AC_9901.html

[28] http://www.kisa.or.kr/sysevaluation/menu1/sub3/control.html