韓國 컴퓨터情報學會 論文誌
第12卷 第2號, 2007. 5.

2007-12-2-4-2

보안 위험분석을 위한 안정성 평가 시스템 설계 및 구현

조 경 식*

Design and implementation on Safety assesment system for security threat analyzing

Kyoung-sik Cho*

요 약

대부분의 조직에서 정보시스템의 의존도가 높아짐에 따라 정보시스템 보안 사고에 대한 위험이 증가하고 있다. 본 논문에서는 정보보호관리체계와 위험분석방법을 적용하여 보안 위험분석을 위한 안정성 평가시스템을 설계 및 구현하였다. 또한, 위험평가 시 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 관리 측면에서 취약점을 쉽게 찾을 수 있도록 지원하며, 안정성 확보를 위하여 수행해야 할 권고를 제시한다.

Abstract

Risk of damage on information system being grow according to increasing its dependence rate on most of organization. On this work, make planed for a safety assessment system in which information protection management system and threat analyzing method. Also, during threat assesment, we have planned possible an equal-weight applied assesment and considering the characteristics of the organization, an assesment which security factor's weight is variably applied to, and respective organizations to examine its security by itself in order to support the easy findings of the vulnerabilities on the management point of view, and to show the advices to practice.

▸ Keyword : 정보보호(information protection), 위험분석(threat analyzing)

• 제1저자 : 조경식
• 접수일 : 2007.4.18, 심사일 : 2007.4.25, 심사완료일 : 2007. 5.17.
* 강원관광대학 부사관과 교수

Ⅰ. 서 론

컴퓨터를 통한 정보의 처리, 관리, 저장, 유통 등이 보편화되고 각 조직에서는 컴퓨터로 관리되고 있는 정보에 대한 의존도가 높아지고 있다. 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 정보보호기술에 대한 관심이 고조되고 있다. 최근에 발생하는 보안사고는 예전의 호기심을 가진 개별적이고 산발적인 보안사고와는 달리 조직적이고, 전문적이며, 집중적인 양상으로 확산되고 있다.[1]

국제적으로 보안관리 분야의 중요성이 부각되면서 관련 산업이 많은 발전을 하고 있다. 국제 표준화 기구(ISO)에서는 수년 동안 보안관리 분야의 표준화 작업을 수행해 왔으며 일부 분야는 이미 표준화가 완료되었다. 특히 보안관리의 핵심 분야인 위험관리와 위험분석에 대한 표준화 작업은 상당히 진전을 보여 왔다.[2,3,4,5,6]

그리고 위험 관리의 핵심 부분인 위험 분석에 대한 도구들이 개발되고 있지만 정확성과 효율성을 높이고 안정성 확보를 위하여 수행해야할 권고 사항을 제시할 수 있는 시스템에 대한 요구가 증가하고 있다.

본 논문에서는 최적의 정보시스템 보안체계를 구축하기 위하여 조직의 정보시스템에 잠재되어있는 위험을 세부적으로 조사하고 분석하고 평가하여, 취약분야와 위험요소를 파악하고 비용 효과적인 측면에서 효율적인 대응책을 제시해 주는 종합적인 정보시스템 안전성 평가시스템을 제안한다.

Ⅱ. 정보보호 관리 체계

1. 정보보호관리

정보보호관리는 보안정책 수립, 위험 분석, 보안대책의 선택·구현, 정보보호시스템 구축, 보안대책 평가를 하나의 과정(process)으로 인식하여 체계적·종합적으로 관리하는 활동을 총칭하는 개념이다.

최근 전 세계적으로 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.[7,8]

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

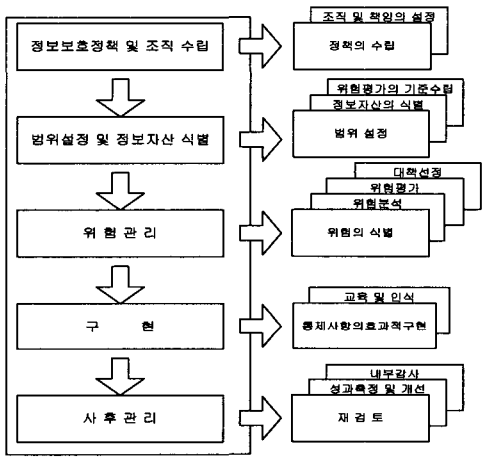


그림 1. 정보보호관리 과정
Fig. 1 Information protection management process

2. 위험분석

위험분석은 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. [6]

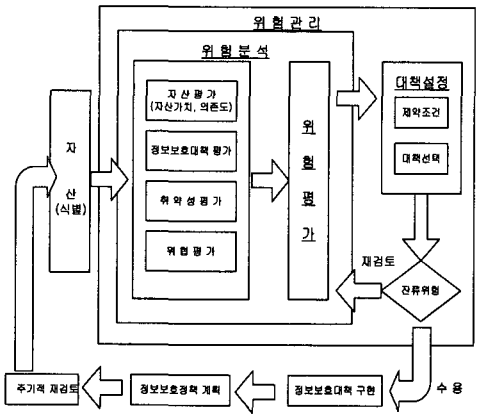


그림 2. 위험분석 모델
Fig. 2 Risk analyzing model

2.1 위험분석의 요소

2.1.1 자 산

자산은 위험관리와 위험분석의 기초가 되는 요소이다. 정확한 자산파악에 실패하면 보안조치에 허점을 제공하고, 올바른 위험관리와 위험분석을 할 수 없다.

자산의 정확한 식별은 상당한 시간과 많은 비용이 요구되므로 보안수준에 맞지 않는 불필요한 자산까지 파악할 필요는 없다. 따라서 자산의 분석범위는 시간과 비용 등의 제약조건을 고려하여 구체적인 분석수준에 맞게 결정해야 한다. 자산은 조직의 환경과 문화에 따라 정확한 평가가 수행되어야 하고, 각 자산간의 상호의존성을 정확하게 파악해야 한다.

2.1.2 위 협

위협은 자산에 해를 줄 수 있는 위험의 원천이고, 잠재적인 공격을 말하는 것으로 자산가치에 대한 평가 다음으로 수행해야 할 위험분석의 요소이다. 이에 따른 위협의 예는 (표 1)과 같다.

표 1. 위협의 분류
Table. 1 Kind of threat

분 류	내 용
자연적 위협	자연재해, 정전 등
사람에 의한 의도적 위협	하드웨어 파괴/절도, 시스템의 불법사용/방해, 정보의 위조, 변조, 삭제, 유해프로그램의 삽입 등
사람에 의한 비의도적 위협	조작 미숙, 조작 실수, 데이터 누출
정보시스템의 결함	운영체계의 결함, 응용프로그램의 결함, 과부하, 하드웨어 고장, 전원고장, 통신망장애 등

2.1.3 취약성

취약성은 자산을 손상시켜 위험을 일으키는 시스템의 약점으로 자산, 위협, 보안대책간의 함수 관계를 갖는 실체이다. 또한 보안 대책 시스템의 약점이다. 취약점이 있다고 해서 곧바로 자산의 손실을 입지는 않지만 위험요소들이 침입할 수 있는 근거를 제공하게 된다. 즉 자산의 경제적인 손해를 끼치는 잠재적인 원인이 된다.

2.1.4 위험평가

위험은 위협이 자산의 취약성을 이용하여 직접적이거나 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 비밀성, 무결성, 인증성, 가용성, 책임추적성, 신뢰성 등에 손실을 주게 된다. 영향을 표현하는 방법은 여러 가지 있지만 크게 정량적인 방법과 정성적인 방법으로 구분될 수 있다.

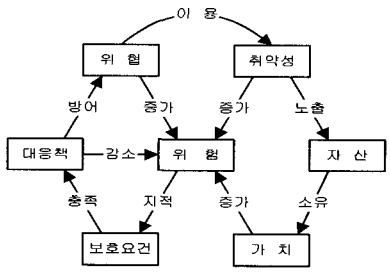


그림 3. 위협 요소들과의 관계
Fig. 3 Relation of risk elements

III. 평가 시스템 설계 및 구현

1. 평가시스템 구성

평가시스템의 설계를 위해 본 논문에서 설정한 프로세스는 (그림 4)에서 제시한 바와 같이 위험분석 모델을 중심으로 구성하였다. 제시된 프로세스는 평가시스템을 형식화하는데 도움을 주고 그러한 프로세스를 따르는데 필요한 절차 또는 단계에 대한 지침을 제공한다. 프로세스는 4단계로 이루어지며 2단계의 위험분석단계에서는 다시 2가지 평가를 실시한다.

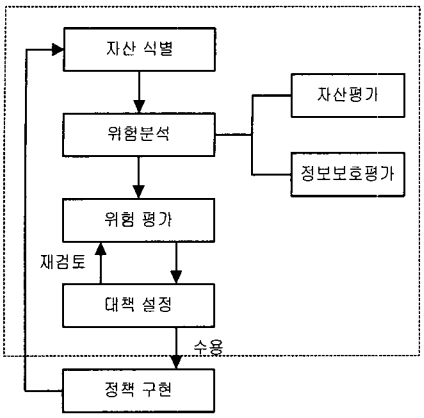


그림 4. 평가시스템 프로세스
Fig. 4 process of asessment syatem

2. 평가시스템의 구현

2.1 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 하드웨어, 운영체제, 응용소프트웨어, 네트워크, 데이터, 사용자, 환경의 7개의 대분류로 나누고, 이를 다시 세분화해서 분류한 뒤 목록을 작성하였다.

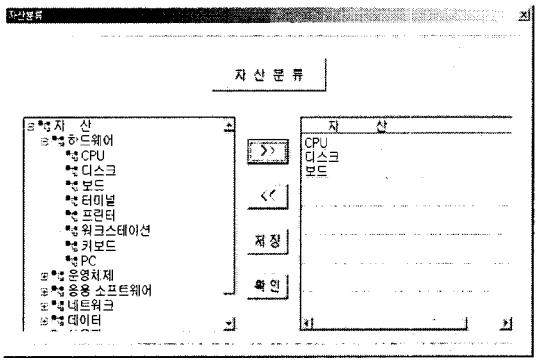


그림 5. 항목별 분류
Fig. 5 kind of item

2.2 자산 위험 평가

각 자산에 대한 위험평가는 자산위험빈도와 자산가치로 그 값을 결정하는데, 먼저 빈도가치는 (표 2)와 같이 각 자산의 가치를 결정하는 위협과 취약성의 두 가지를 평가하며, 이 값에 모든 시스템의 자산가치가 더해졌을 때, 그 정보시스템의 위험정도를 결정한다.

표 2. 위험의 빈도
Table. 2 frequency of risk

위협의 정도	취약성의 정도	위험 빈도 가치
높음	High	4
	Medium	3
	Low	2
중간	High	3
	Medium	2
	Low	1
낮음	High	2
	Medium	1
	Low	0

자산 위험 평가는 (표 3)에서와 같이 자산 가치와 자산 위험 빈도의 교차점을 찾음으로서 그 값이 결정되며, 이 수치는 시스템을 구성하는 자산 사이를 구분하기 위해 사용된다.

표 3. 자산 위험 평가
Table. 3 Assessment of property risk

빈도가치 \ 자산가치	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

끝으로 자산에 대한 자산정보를 결정한다. 자산정보는 자산이 가지는 보안요소로서 가용성, 무결성, 비밀성으로 구분하며, 산술식은 다음과 같다.

$$A_z = A_v + A_{f_{(0 \le A_v \le 4.0 \le A_f \le 4)}} \quad \text{(식 1)}$$

$$A_f = T + V_{(0 \le T \le 2,0 \le V \le 2)} \quad \text{(식 2)}$$

(식 1)에서 자산 위험 평가 값을 Az, 자산의 가치를 Av, 자산 위험 빈도를 Af로 설정하였으며, 그 범위는 각각 0~4까지의 범위를 가진다. (식 2)에서 자산의 빈도위협의 정도를 T로, 취약성의 정도를 V로 설정하였으며 그 범위는 각각 0~2까지의 범위를 가진다.

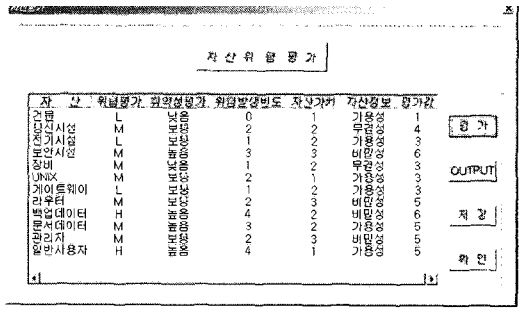


그림 6. 자산위험 평가
Fig. 6 Assessment of property risk

(그림 6)은 자산을 평가하는 프로그램으로 식별된 자산을 바탕으로 취약성 평가, 위협 평가를 통해 자산 위험 빈도를 평가한다. 취약성 평가는 "Low", "Medium", "High"로 3단계 평가를 하며, 위협평가는 "낮음", "보통", "높음"의 3단계 평가를 실시하였다. 또한 자산의 가치 평가는 0~4까지 5단계로 평가하였으며, 자산정보는 가용성, 무결성, 비밀성으로 표현하였다.

2.3 정보보호 평가

2.3.1 가중치 적용

정보시스템 사용 기관에 따라 정보보호 우선 순위가 다르며, 동일한 보안사고라도 기관에 따라 피해의 정도는 상이하게 나타난다. 그러므로 가중치는 각 조직별로 상이하게 적용하여야 한다. 먼저 의료기관의 경우, 환자의 개인기록, 진료기록, 영상자료 등 의료정보가 불법적으로 공개되지 않도록 방지해야 하며(비밀성), 제조업의 경우, 정보의 불법적인 파괴나 지체로부터 보호되어야 하고(가용성), 마지막으로 금융기관은 개인의 금융정보가 해커이나 금융관계자로부터 불법적으로 변조되는 것을 방지해야 한다(무결성).

따라서 조직의 업무 특성에 따라 보안요소 중 중요시되는 요소에 가중치를 차등적으로 적용한 후, 가중치의 비율을 4:3:3, 5:3:2, 6:3:1 중 하나를 선택하여 적용한다.

2.3.2 평가 값 결정

평가에 대한 항목의 평가요소별 평점은 10점을 기준으로 하며, 보안요소에 대한 평가는 상대적 평가를 실시한다.

항목별 평가는 항목 내 평가요소의 평균으로 나타내며, 보안요소에 대한 상대평가는 10을 기준으로 4:3:3, 5:3:2, 그리고 6:3:1의 가중치 비율을 선택하여 평가 값을 결정하였다.

산술식은 다음과 같다.

$$W_z = \frac{1}{\omega}\sum_{i=1}^{\omega} T_a \quad \cdots\cdots \text{(식 3)}$$

$$W_A = \frac{1}{l}\times\frac{1}{\alpha}\sum_{i=1}^{\alpha} X_i \quad \cdots\cdots \text{(식 4)}$$

$$W_I = \frac{1}{m}\times\frac{1}{\beta}\sum_{j=1}^{\beta} Y_j \quad \cdots\cdots \text{(식 5)}$$

$$W_C = \frac{1}{n}\times\frac{1}{\gamma}\sum_{k=1}^{\gamma} Z_k \quad \cdots\cdots \text{(식 6)}$$

$$\text{단}, l+m+n=10, W_A+W_I+W_C=100 \cdots \text{(식 7)}$$

(식 3)에서 WZ는 항목 내 평가 값에 대한 평균이고, w는 항목내 평가요소의 총 수이며, Ta는 항목 내 a번째 평가요소이다. (식 4)에서 WA은 가용성 평가 값의 평균이고, l은 가중치이며, α는 가용성항목의 총수이고, Xi는 가용성 항목의 i번째 평가 값을 뜻한다. (식 5)에서 WI는 무결성 평가 값의 평균이고, m은 무결성 항목의 가중치이며, β는 무결성 항목의 총수이고, Yj는 무결성 항목의 j번째 평가 값을 의미한다. (식 6)에서 WC는 비밀성 평가 값의 평균이고, n은 비밀성 항목의 가중치이며, γ는 무결성 항목의 총수이고, Zk는 비밀성 항목의 k번째 평가 값을 의미한다. 그리고, 가중치를 분모에 값을 곱함으로써 상대적으로 값이 작아지도록 하여 타 항목에 비해 더 많은 투자와 관심을 가지도록 하였으며, 가중치 비율의 합과 보안요소의 합은 (식 7)과 같이 각각 10과 100이 되도록 하였다.

IV. 실험 및 결과

1. 평가 방법

ISMS(Information Security management Syatem) 요구사항 평가 및 세부 통제사항에 대한 평가를 (그림 7)과 같은 도구를 이용하여 평가를 실시한다. 평가는 각각의 질문에 "매우 높음","높음","보통","낮음","매우 낮음"으로 답하며, 그 결과를 항목단위로 평균값으로 나타낸다.

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

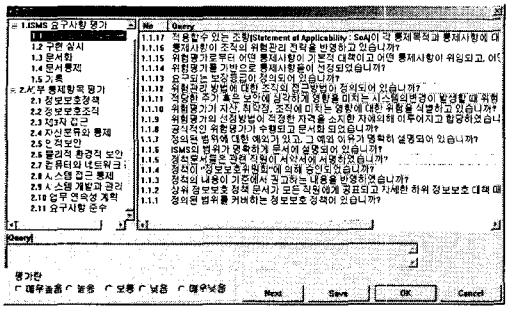


그림 7. 요구사항 평가
Fig. 7 Assessment of requirement

2. 가중치 변경에 따른 분석

2.1 동일한 가중치 적용

(그림 8)은 각 항목들에 동일한 가중치를 적용하여 평가한 결과이다.

각 항목에서 평균보다 작은 부분은 위험이 예상되는 부분으로 안전대책이 강구하여 피해 손실을 최소화하여야 한다.

각각의 항목은 10점을 기준으로 평가하며, 각 항목은 항목 내 평가 값을 평균한 값으로 표시한다.

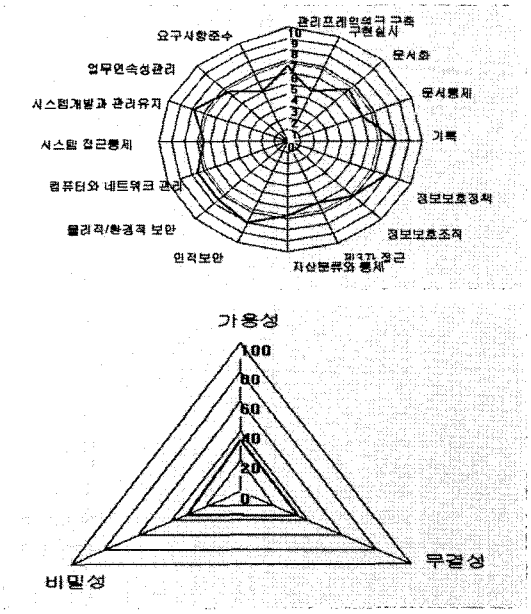
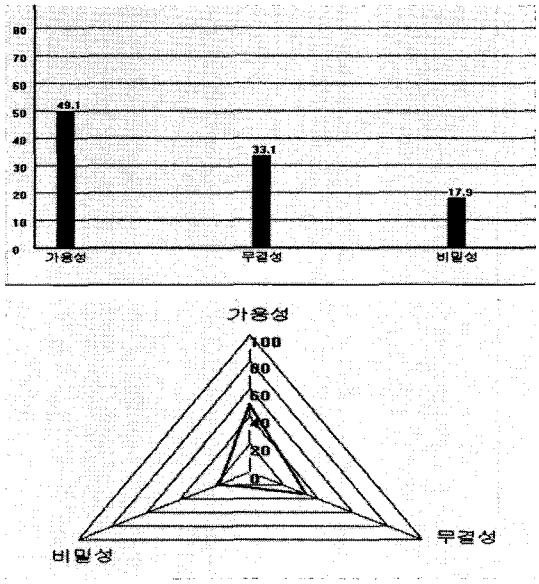


그림 8. 동일한 가중치로 평가
Fig. 8 Assessment with the same weight

평가결과 전체 평균은 6.7이고 보안요소의 항목별 평균은 가용성항목이 34.2, 무결성 항목이 34.6, 비밀성항목이 31.1이다.

2.2 상이한 가중치 적용

의료업의 경우 비밀성에 대한 비중이 타 기관에 비해 강조되고 있다.



(비밀성:무결성:가용성 = 5 : 3 : 2)
그림 9. 의료기관의 평가
Fig. 9 Assessment of hospitals

따라서 동일한 가중치 평가를 마친 후 그 결과 값에 업무특성에 맞는 가중치를 부여하면 (그림 9)와 같은 평가 값을 얻을 수 있다. (그림 9)에서의 가중치 비율은 5:3:2이며 이 비율은 조직의 업무특성에 따라 적용 가능하다.

안은 우선 순위를 적용하도록 되어있으며, 복구 우선 순위는 조직의 특성에 따른 가중치가 높고, 취약점 권고안에 단계가 높은 항목을 우선으로 하여 복구 우선 순위를 결정하도록 구현하였다. (그림 9)에서 비밀성 항목이 타 항목에 비해 상대적으로 작은 값을 가지며, 이는 비중이 큰 항목의 값을 상대적으로 작게 평가함으로써 그 항목에 상대적으로 많은 투자를 요구하게 된다. 따라서 각 조직은 조직의 업무를 기준으로 가중치 비율을 조직에 맞게 선택할 수 있다.

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

위험을 분석하여 산출하는 방법으로 정량적 수치로 나타내는 정량적 분석과 위험의 정도를 기술변수(상, 중, 하 또는 높음, 보통, 낮음 등)로 나타내는 정성적 분석이 있으며, 본 논문에서는 두 가지 방법을 모두 활용할 수 있도록 구현하였다.

특히, 위험분석의 신뢰성이 있는 정량분석에 비중을 두고 실행한 결과 조직과 환경에 따라 다양한 방법으로 위험 수준이 각기 다르게 나타났음을 알 수 있다

따라서 위험분석 결과 조직에 위협적인 요소라 판단되는 평균이하의 항목에 대한 취약점에 대한 권고

V. 결론 및 과제

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 수립할 수 있는 권고사항을 직관적으로 알아 볼 수 있다.

또한, 각 조직의 업무특성, 즉 기밀성, 가용성, 무결성, 책임추적성 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 보안투자 예산의 편성에 우선순위를 결정 할 수 있다.

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

향후 연구로는 보다 다양한 자산과 세부 통제 항목의 다양성의 보강이 요구되며, 업무별 통제항목의 가중치 설정에 대한 수식화와 일반화가 요구되고 있다. 또한 점검후의 권고안을 구체적으로 제시 할 수 있는 조건의 다양화가 추가되어야 할 것이다.

참고문헌

[1] 한국정보보호진흥원, "정보보호관리체계(안) 모델", KISA, 2001.

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

[3] Baseline software, "Information Security Policies Made Easy", Baseline Software. Inc USA.

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

[5] 염흥렬, "정보보호 일반 표준화 로드맵", TTA, 2006.

[6] 진병문, "국내외 네트워크 보안 표준화 현황", 제4회 인터넷 서비스 및 네트워크 보안기술 컨퍼런스, 2006. 5

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

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

저 자 소 개

조 경 식

1986 단국대학교 계산통계학과 학사

1993 단국대학교 전산통계학과 석사

2001 단국대학교 전산통계학과 박사 수료

1999년 ~ 현재 강원관광대학 부사관과 조교수

〈관심분야〉 컴퓨터비전, 영상처리, 정보보안