정보시스템 위험분석 평가도구

김 강*, 조경식*

*강원관광대학

Evaluation Tool for Analyzing Method of the Information System

Kang Kim*, kyoung-sik Cho*

*KangWon Tourism College

E-mail : kkang424@hanmail.net, kscho21@hanmail.net

요 약

네트워크를 기반으로 하는 시스템들의 발전으로 인하여 매우 다양한 침입이 확산되고 있다. 따라서, 침입자들로부터 위험을 줄이기 위해 평가도구에 관한 연구가 활발하다. 본 논문에서는 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 관리 측면에서 취약점을 쉽게 찾을 수 있도록 지원하며, 수행해야 할 권고를 제시한다.

Abstract

Very various intrusion by development of systems that is based on network is spread. Therefore, Evaluation Tool has been an active research area to reduce the risk from intrusion. On this thesis, 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.

키워드

위험분석(Threat analyzing), 정보보호(Information protection)

Ⅰ. 서 론

컴퓨터 및 네트워크 기술이 발전하고 이에 대한 의존도가 증대함에 따라 컴퓨터의 결함은 인적, 물적 손실뿐만 아니라 조직의 경쟁력을 약화시키는 결과를 초래하게 되어 정보사회의 역기능으로 컴퓨터 보안문제가 중요하게 대두되고 있다. 이러한 보안문제에 대처하기 위해서 정보보호를 요하는 시스템에 대한 불법적인 침입을 분석하고 대응에 관한 연구가 활발히 진행되고 있다.[1][2][3][4][5]

최적의 정보시스템 보안체계를 구축하기 위해서는 조직의 정보시스템 운영환경을 분석하고, 취약분야와 위험요소를 파악하여 비용 효과적인 측면에서 효율적인 대응책을 제시해주는 위험분석 과정이 반드시 필요하다. 이를 위해서는 위험분석의 방법론 및 절차가 확립되어야 하며, 이를 위한 위험분석 표준이 필요하다.

따라서 체계적이고 종합적인 정보보호관리체계가 요구되고 있으며, 이를 통한 정보자산 등에 대한 정보보호관리체계(Information Security Management Syatem : ISMS) 인증제도를 적용하여 IT환경의 안전·신뢰성을 확보할 필요성이 증대되고 있다. 대부분의 조직에서 정보시스템의 의존도가 높아짐에 따라 보안사고에 대한 대책마련이 요구되며,[6][7] 대책마련을 위해서는 전반적인 보안요소를 고려한 종합적인 정보시스템 위험분석 평가도구가 요구된다.

Ⅱ. 위험분석

1. 위험분석의 요소

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. 위험분석 모델은 (그림1)과 같다.

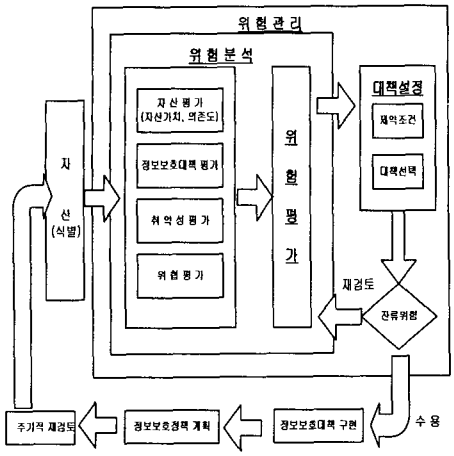


그림 1. 위험분석 모델

1.1 자산분석

자산분석은 자산식별을 통하여 조직의 자산을 파악하고 자산의 가치 및 중요도를 산출하며, 정보자산과 업무처리와의 관계도 알아낼 수 있다. 자산평가는 위험분석결과의 정확도를 결정하는 매우중요한 과정이다. 자산식별과정은 크게 자산조사와 자산가치정의 2가지로 나눌 수 있으며, 자산조사과정에서는 조사할 자산의 범위를 설정하고, 자산목록을 작성한다. 자산가치 산정과정에서는 자산을 정량적 또는 정성적으로 산출하는 기준과 절차를 정의 한다. [8]

1.2 위협분석

자산은 다양한 종류의 위협에 처해있다. 위협은 시스템, 조직, 조직의 자산에 피해를 주는 원치 않은 사고를 일으킬 잠재성으로 내재한다. 이러한 피해는 인가되지 않은 파괴, 공개, 변경, 훼손, 불가용성, 손실 등 IT시스템에 의해 처리되는 정보 또는 서비스에 대한 직간접의 공격으로부터 발생할 수 있다. 자산의 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.

1.3 취약성

자산과 관련된 취약성은 물질적배치, 조직, 절차, 인력, 관리, 행정, 하드웨어, 소프트웨어 또는 정보상의 약점을 포함한다. 취약성은 IT시스템이나 사업목표에 유해한 위협이 침투하는 경로가 되지만 취약성 자체는 피해를 일으키지 않는다. 취약성은 단지 하나의 조건 즉 위협에 의해 자산의 피해를 끼치게 되는 일련의 조건이고 다양한 근원의 취약성을 고려해야 한다.

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.

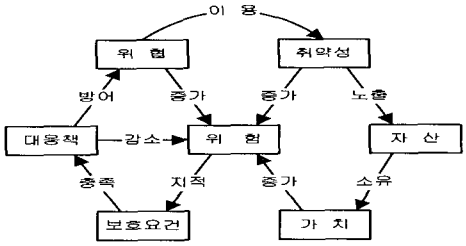


그림 2. 위험 요소들과의 관계

2. 평가방법 및 고려사항

평가는 자산과 정보보호정책으로 구분하여 평가를 하였다. 평가를 위해서는 평가목록을 작성하는데 목록에는 범위설정을 통하여 파악된 조직의 규모와 운영목적 및 환경을 바탕으로 요소들을 분류하고 평가요소는 파악된 핵심 업무처리와 기타기준의 범위 내에서 작성하였다. 작성 시 고려사항은 아래와 같다.

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

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 7개의 대분류로 나누고, 이를 다시 세분화해서 분류한 뒤 목록을 작성하였다.

하드웨어 : CPU, 디스크, 보드, 프린터 등
운영체제 : UNIX, Windows, LINUX 등
응용소프트웨어 : 소스프로그램,
문서편집프로그램, 진단프로그램 등
네트워크 : 허브, 라우터, 게이트웨이 등
데이터 : 실행자료, 문서자료, 백업자료 등
사용자 : 관리자, 일반사용자, 개발자 등
환경 : 전산실 등

2.2 업무처리별 분류 및 조사

일반적으로 IT업무처리시 대상조직들이 잠재하고 있는 위험요소의 실체를 파악하는 데 부족하다. 궁극적으로 IT자산이 조합되어 수행되어지는 업무처리에 대해 가해지는 것이다. 업무처리와 자산간의 관계를 정립함으로 각 자산의 가치와 중요도를 더욱 정확하게 파악할 수 있다.

3. 자산 평가

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

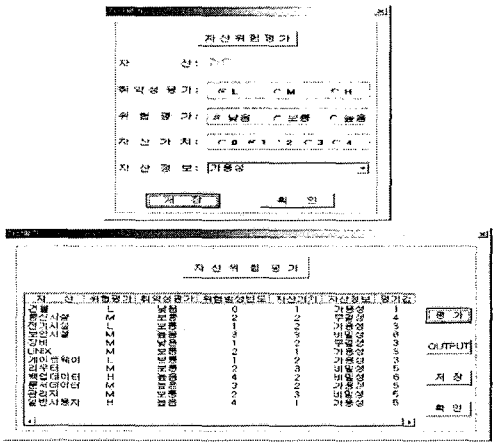


그림 3. 자산위험 평가

4. 정보보호 평가

정보보호평가 및 취약성평가는 조직 및 자산이 잠재적으로 갖고 있는 약점으로 근본적으로는 위험의 근원을 명확히 파악하고 그에 다른 보안대책을 수립하는데 목적이 있다. 기존에 제시된 평가방법 중 ISMS요구사항 평가 및 세부통제사항과 취약성평가방법을 이용하여 평가하였다.

- 요구사항평가 : 관리프레임워크 구축, 구현실시, 문서화, 문서통제, 기록
- 세부통제항목 : 정보보호정책, 정보보호조직, 제3자의 접근, 자산의 분류와 통제, 인적보안, 물리적/환경적보안, 컴퓨터와 네트워크의 관리, 시스템 접근통제, 시스템개발과 유지, 업무 연속성, 요구사항준수

5. 취약성분석

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

- Very High : 매우높음
- High : 비교적 높음
- Medium : 보통
- Low : 낮음
- Negligible : 취약성이 거의 없음

특히 취약성분석을 통하여 도출된 분석 자료를 바탕으로 위험을 나타내는 취약성 수준을 산출하는 2가지 유형을 적용하였다.

III. 구현 및 분석

1. 평가 방법

ISMS 요구사항 평가 및 세부통제사항에 대한 평가를 (그림 4)와 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. 가중치는 각 조직별로 상이하게 적용하며, 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).

기관에 따라 정보보호 우선순위가 다르며, 동일한 보안 사고라도 기관에 따라 피해의 정도는 상이하게 나타난다. 따라서 가중치의 비중과 그 비율을 차등적으로 적용하는데 가장 비중이 높은 항목을 10점으로 하고 각각 7점, 4점으로 적용한다.

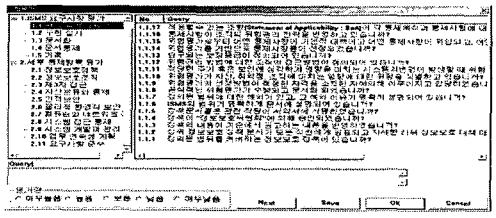


그림 4. 요구사항 평가

2. 가중치 변경에 따른 분석

2.1 동일한 가중치 적용

(그림5)는 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. 평가 결과 전체 평균은 6.7이고 보안요소의 항목별 평균은 가용성항목이 34.2, 무결성 항목이 34.6, 비밀성항목이 31.1이다.

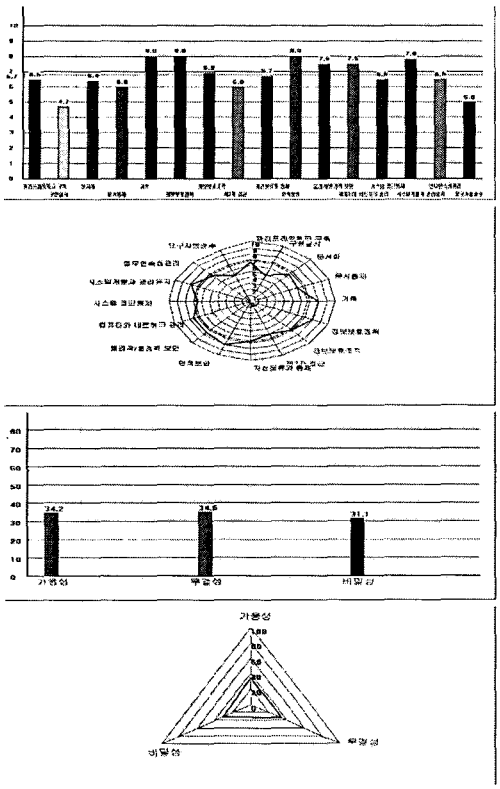


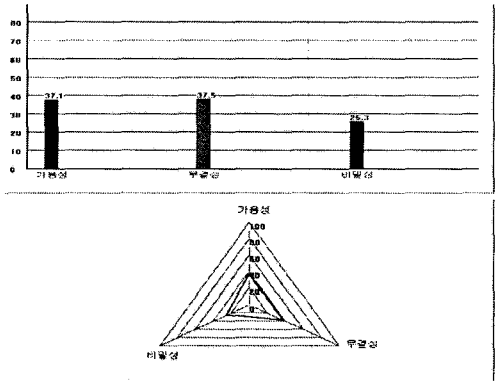
그림 5. 동일한 가중치 적용

2.2 상이한 가중치 적용

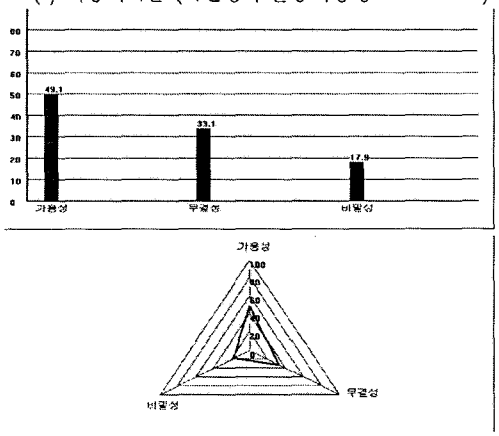
의료업의 경우 평가결과 (그림6)에서와 같이 비밀성에 대한 비중이 가중치 비율에 따라 타 업무에 비해 강조되고 있다.

따라서 동일한 가중치 평가를 마친 후 그 결과 값에 업무특성에 맞는 가중치를 부여하면 (그림6)과 같이 가중치비율에 따라 상이하게 평가 값을 얻을 수 있다. 그림에서와 같이 (1), (2), (3)의 가중치 비율은 각각 4:3:3, 5:3:2, 6:3:1이며 이 비율은 조직의 업무특성에 따라 적용 가능하다.

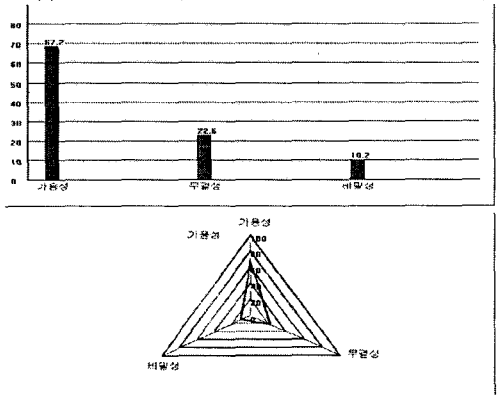
(그림6)에서 비밀성 항목이 타 항목에 비해 상대적으로 작은 값을 가지며, 이는 비중이 큰 항목의 값을 상대적으로 작게 평가함으로써 그 항목에 상대적으로 많은 투자를 요구하게 된다. 따라서 각 조직은 조직의 업무를 기준으로 가중치 비율을 조직에 맞게 선택할 수 있다.



(1) 가중치비율 (비밀성:무결성:가용성 = 4 : 3 : 3)



(2) 가중치비율 (비밀성:무결성:가용성 = 5 : 3 : 2)



(3) 가중치비율 (비밀성:무결성:가용성 = 6 : 3 : 1)

그림 6. 의료기관의 평가

3. 평가 결과 분석

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 권고안은 우선순위를 적용하도록 되어있으며, 복구 우선순위는 조직의 특성에 따른 가중치가 높고, 취약점 권고안에 단계가 높은 항목을 우선으로 하여 복구 우선순위를 결정하도록 구현하였다.

IV. 결 론

본 논문에서는 ISMS에서 제시하고 있는 통제항목과 각 자산별 체크리스트를 종합적으로 점검 하고 위험분석 및 평가를 일관성 있게 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, 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 보안 투자예산의 편성에 우선순위를 결정 할 수 있게 되었다.

향후, 보다 다양한 자산과 세부 통제 항목의 다양성을 고려하고 GUI 환경 보강및 업무별 통제항목의 가중치 설정에 대한 수식화와 일반화에 대한 연구가 필요하다. 또한 점검후의 권고안을 구체적으로 제시할 수 있는 조건의 다양화에 대한 추가 연구가 있어야 할 것이다.

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", British Standard Institution.
[4] "ISO/IEC TR 13335-4" : Information technology - GMITS - Part 4 : Selection of safeguards, 2000.
[5] ISACA."COBIT : Audit Guideline, 3rd Ed.", July 2000.
[6] Donald L. Pipkin, "Information Security Protecting the Global Enterprise", HP, 2000.
[7] Harold F. Tipton Micki Krause, "Information Security Management HAND BOOK", Auerbach, 4th, 2000.
[8] "공공정보시스템 보안을 위한 위험분석 표준-위험분석방법론 모델", 한국정보통신기술협회, 정보통신단체표준(TTAS.KO- 12.0007), 2000.