제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

효율적인 위험분석 프레임워크에 관한 연구

조준식*, 엄정호*, 김인중**, 정태명*
*성균관대학교 정보통신공학부
**국가보안기술연구소
e-mail:jscho@rtlab.skku.ac.kr

A Study on Efficient Risk Analysis Framework

Joon-Sic Cho*, Jung-Ho Eom*, In-Joong Kim**, Tai M. Chung*
*Information & Communications Engineering, Sungkyunkwan University
**National Security Research Institute

요 약

네트워크와 인터넷의 발달로 국내 정보시스템의 환경이 복잡해지고, 그에 따른 위험도 증가함에 따라 정보시스템에 대한 위험관리의 중요성이 한층 더 부각되기 시작했다. 현재 국내 정보시스템에 대한 위험관리는 외국의 위험관리 방법론을 도입하여 수행하고 있으나, 국내 정보시스템 환경에 맞지 않아 체계적이고 정확한 위험관리가 이루어지지 않고 있는 실정이다. 물론 기업 및 연구소 등에서 국내 환경에 맞는 위험관리 방법론을 연구하고 있으나, 아직 그 결과가 미진한 상태이다. 본 논문에서는 체계적인 위험관리를 위해 효율적인 위험분석 방법론의 프레임워크를 설계하고, 위험분석 과정 중 자산분석, 취약성분석, 위협분석, 대응책분석을 국내외 표준을 기반으로 실제적이고 체계적인 방법과 절차를 제시하였다.

1. 서론

오늘날 정부기관 및 기업에서 정보시스템을 보호하기 위한 정책 및 투자가 증대되고 있는 가운데 효율적인 보안대책을 수립할 수 있도록 정보시스템에 대한 위험관리 분야의 관심이 높아지고 있다. 이러한 관심은 최근 OECD(Organization for Economic Cooperation and Development)의 9.11테러 1주기를 맞이해 사이버 테러와 침입에 대비해 정보시스템과 네트워크를 보호하기 위한 새로운 지침수립, 시행하는 것을 통해 단편적으로 알 수 있다. 정책에서 가장 중요한 9가지 기본원칙을 제시하고 있는데 주로 보안에 관련된 내용이며, 그 중에서도 위험평가와 보안관리에 대한 내용이 핵심이다. 구체적으로 위험평가에 대한 프레임워크를 제시하지는 않았지만 정보시스템에 대한 위협과 취약점을 구별하기 위한 분석을 수행해야 할 필요성과 이를 관리하는 포괄적인 내용을 제시하고 있다.

이렇게 정보통신의 발전과 함께 공공기관 및 민간기업들은 정보통신 시스템에 많이 의존하게 되고 정보시스템의 개방성이 증가함에 따라 정보시스템에 대한 다양한 위협 및 취약성에 따른 보안대책 수립에 주력하기 시작했다. 자국 및 자사의 정보시스템 보호를 위해 다각적인 위험관리 방법이 제시되고 있으며 정부, 공공기관 및 민간기업들이 연계를 통해 효과적인 위험관리를 할 수 있도록 대책을 마련하고 있다. 국내에서도 외국의 위험관리 및 위험분석 방법론을 분석하여 국내 정보시스템 환경에 적합한 방법론을 개발하기 위해 부단히 노력하고 있다.

본 논문에서는 국내외 위험관리 및 위험분석 표준과 기존에 개발된 외국의 위험분석 방법론의 분석자료를 바탕으로 국내 정보시스템 환경에 적합한 위험분석 프레임워크를 제시하려고 한다. 2장에서는 일반적인 위험분석 방법론에 대한 프레임워크를 알아보고 3장에서 본 논문에서 제시하는 위험분석 프레임워크를 기술할 것이다. 마지막으로 4장에서는 결론을 맺는다.

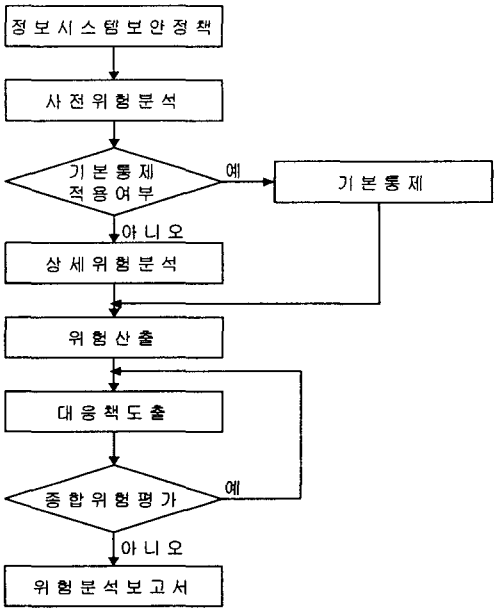
2. 일반적인 위험분석 방법론

위험분석은 보안관리를 수행하기 위한 필수적인 과정으로 시스템의 위험을 평가하고, 비용효과적인 대응책을 제시하여 시스템 보안정책과 보안대응책 구현계획을 수립하는 위험관리의 핵심적인 부분이다. 위험분석의 목적은 보호되어야할 대상 정보시스템과 조직의 위험을 측정하고, 이 측정된 위험이 허용 가능한 수준인지 아닌지 판단할 수 있는 근거를 제공하는 것이다. 위험분석이란 정보시스템과 그 자산의 비밀성, 무결성, 가용성, 기록추적성에 영향을 미칠 수 있는 다양한 위협에 대해서 정보시스템의 취약성을 식별하고, 이로 인해서 예상되는 손실을 분석하는 것으로서, 위험분석의 3대요소인 자산, 위협, 취약성의 관계분석을 통해 조직에 효과적인 보안 대책을 수립한다. 위험분석의 3대요소인 자산, 위협, 취약성은 다음과 같다.

- 자산(Asset) - 자산은 조직의 입장에서 가치를 갖는 모든 것을 통칭한다. 단, 정보시스템 환경에서 지칭하는 자산은 조직의 정보시스템 관련 자산들로 그 의미가 축소된다. 자산분석을 통하여 보호해야할 자산들을 식별하고 체계적으로 분류하여, 소유하고 있는 자산들의 가치를 평가하게 된다.
- 위협(Threat) - 위협은 시스템 또는 조직에 손실을 초래할 수 있는 원치 않는 사건을 일으키는 잠재적인 원인으로서, 자산에 해를 줄 수 있는 위험의 원천을 말한다. 위협분석은 이렇게 위협을 식별하고 분류하여, 발생 빈도와 손실 정도를 측정한다.
- 취약성(Vulnerability) - 위협에 의해 이용될 수 있는 자산이 내포하고 있는 약점을 말한다. 다시 말해 정보시스템에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어 등에 존재하는 약점을 뜻한다. 취약성 분석은 이렇게 약점을 확인하고 분류하여 위협을 감소시키는 과정을 말한다.

이러한 요소들을 분석하는데 있어서 가장 중요시하는 것은 얼마만큼 비용 효과를 거둘 수 있는지 그 목적을 두고 있다.

위험분석은 일반적으로 다음과 같은 8가지 과정을 통해 위험분석 보고서를 작성하며 정보시스템을 분류, 가치를 산정하여, 그에 따른 위협, 취약성, 영향 등을 분석, 평가하여 적절한 대응책을 수립하게 된다.



[그림 1] 위험분석 모델

① 정보시스템보안정책 - 조직에서 현재 적용하고 있는 보안 정책을 중심으로 위험분석을 시작한다.

② 사전위험분석 - 효과적인 위험분석을 수행하기 위해 현재 조직의 정보시스템 환경에 적합한 위험분석 수준을 결정하기 위함이다.

③ 기본통제 - 정보시스템에 대한 최소의 보안대책을 수립하는 과정이다. 기본통제 수준을 조절하는 것에 따라 비용이 많이 드는 높은 수준의 보안대책을 수립하던지 비용이 적게드는 낮은 수준의 보안대책을 수립할 수 있다. 이는 조직의 요구사항을 반영하여 적절한 수준으로 조정할 수 있다.

④ 상세분석 - 정보시스템이 조직의 업무상 중요도가 높거나 자산 가치가 클 경우 적용하게되는 분석 방식으로 위험분석에서의 자산 분석, 위협 분석, 취약성 분석, 대응책 분석의 일련의 과정을 지칭한다.

⑤ 위험산출 - 위에서 얻은 데이터와 분석 결과를 바탕으로 위험을 측정하고 산출한다.

⑥ 대응책도출 - 지금까지 분석된 결과를 바탕으로 조직이 원하는 수준의 대응책을 제시하는 과정이다.

⑦ 종합 위험평가 - 분석된 결과를 바탕으로 전반적인 위험을 기술하고 분석된 위험이 조직의 업무

처리에 미치는 영향을 나타낸다. 또한 참고로 허용위험수준과 비용효과분석을 통해 분석된 결과를 조직에서 가장 시급한 필요대응책으로 구성하고 타당한 위험분석을 수행하였는지 평가하게 된다. 이러한 과정을 거친 후 문제점이 없는지 판단하고 있을 경우 다시 대응책도출과정을 수행한다.

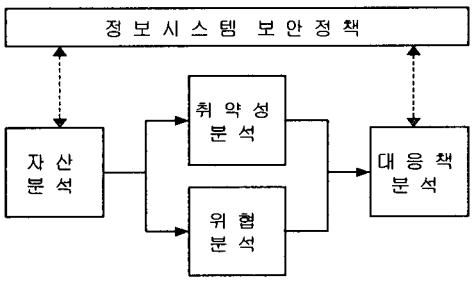
⑧ 마지막으로 위험분석 보고서를 작성하여 경영진에게 최종 보고서를 제출한다.

이처럼 위험분석 최종 보고서가 완성된 후에 이 결과를 바탕으로 시스템별 보안정책을 작성하고 부문별 보안 계획을 수립한다. 이 계획이 수립되면 대응책을 구현하고, 관련 교육을 실시한 후, 다시 재평가하여 조직에서 허용 가능한 위험수준을 만족하는지 검토하고, 재분석 실시 여부도 판단한다.

3. 효율적인 위험분석을 위한 프레임워크

대부분의 방법론들 역시 정확한 위험분석을 하기 위해 상세분석을 수행한다. 그렇지만 대부분 외국의 위험분석 방법론을 국내에 도입하고 있고 이렇게 도입된 방법론은 국내 실정에 맞지 않아 본 연구에서 몇 가지 과정들을 수정한 방법론을 제시하려 한다.

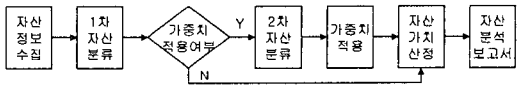
상세분석 과정의 자산, 위협, 취약성, 대응책의 분석을 충실히 수행해야 올바른 위험평가를 내릴 수 있다. 다음과 같은 순서의 세부분석을 통해 효율적인 상세분석을 할 수 있다.



[그림 2] 상세분석 과정

(1) 자산분석

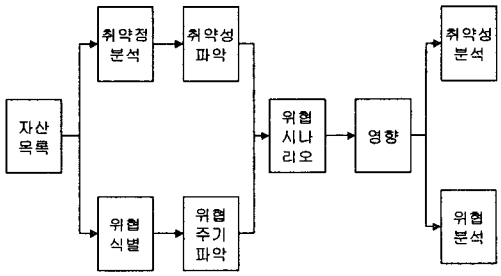
자산분석 방법은 인적요소, 환경적요소, 하드웨어, 응용소프트웨어, 네트워크, 데이터, 응용체제를 중심으로 분석한다. 일반적인 자산분석에 국한되지 않고 자산의 분류를 부서별, 업무별, 사용자별, 보안기능별(기밀성, 무결성, 가용성), 보안대책 등의 자산에 중요도 가중치를 부여함으로써 중요도를 달리 할 수 있다.



[그림 3] 자산 분석 과정

(2) 취약성분석 및 위협분석

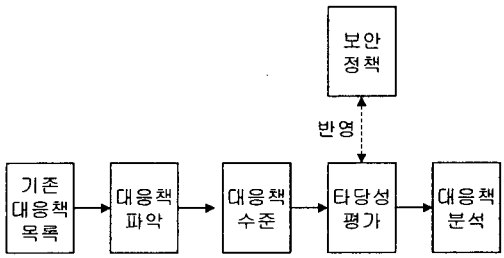
자산분석 후 자산이 내재하고 잇는 취약성과 위협을 분석하는 과정이다. 여기서 어떠한 취약성이 있는지 조사하는 과정뿐만 아니라 취약성의 노출 정도와 그에 따른 결과를 정확하게 판단하여 위험정도를 분석한다. 또한 위협분석 방법에 있어서 취약성에 대한 위협이 어느 정도 이루어지고 있는지, 어느 정도의 발생 주기로 위협이 이루어지는지, 또한 그 결과는 어느 정도로 예측되는지 위협시나리오를 통해 취약성과 함께 분석한다.



[그림 4] 취약성분석 및 위협분석 과정

(3) 대응책분석

자산에 대한 보호가 어느 정도로 효율적으로 이루어지고 있는지 대응책에 대한 분석을 수행한다. 취약성과 위협의 관계를 앞 과정에서는 위협 시나리오를 통해서 분석하였지만, 이 단계에서는 좀 더 세분화시켜 총체적인 관계를 정립하게 된다. 또한 부적절하게 높은 수준의 대응책을 적용하는지, 대응책이 필요한 자산에 적용되고 있지 않는지를 분석하여 최종적인 위험평가를 내릴 수 있게 한다

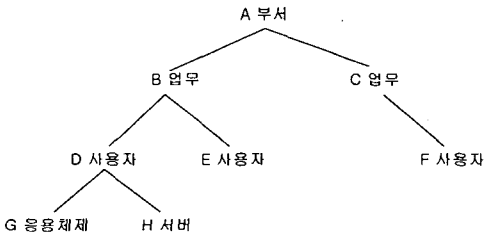


[그림 5] 대응책 분석 과정

기존에 있는 대응책 목록을 중심으로 현재 적용하고 있는 대응책과 적용 가능한 대응책을 모두 파악한다. 단순히 파악하는 것이 목적이 아닌 취약성과 위협과의 관계를 파악하여 대응책의 수준을 결정하고 이를 통해 어느 정도의 효과를 거두고 있는지 분석한다.

분석이 끝난 후에는 2차적으로 위험분석 대상 조직의 특성을 고려하여 대응책분석을 수행한다. 다른 대응책 분석과 달리 조직의 요구사항을 적극 반영하고, 자산의 규모, 부서의 특수성, 업무 종류, 사용자의 능력과 같은 요인에 따라 대응책을 분석한다.

앞의 과정에서 조사한 대응책을 가지고 어떻게 적용되고 있는지 한눈에 알아볼 수 있는 구조로 다음 [그림 6]과 같은 형식으로 대응책의 목록을 도식화한다.



[그림 6] Tree형식의 대응책 타당성 평가 구조

도식화한 목록은 조직이 가지고있는 특성에 맞추어 따로 적용시킬 수 있다. A부서의 B업무를 하는 D사용자의 G응용체제에 대한 대응책을 적용하는 과정에서 D사용자에 대한 보안교육, 정보보호 지침과 같은 대응책과 B업무를 수행하는 조직이 수행해야 할 보안상의 각종 제약, 규제 등의 대응책들을 적용할 수 있다.

이렇게 작성된 대응책 목록을 도식화하여 어느 부서의 어떤 자산이 존재하고 그에 따른 위협과 취약성이 어느 정도 존재하고 있는지 알아볼 수 있는 장점을 지니고 있다. 대응책 분석을 통해 알아본 관계는 다음 위험산출 과정과 종합평가 과정에서 비용효과 분석과 새로운 대응책을 수립하는 과정에서 사용할 수 있는 귀중한 자료로 활용이 된다.

4. 결론

국내 정보시스템 환경에 적합한 효율적인 위험분석 방법론을 개발하기 위해서는 우선 국내 위험관리 정책 현황을 정확하게 파악하고, 선진국들의 위험관리 정책을 살펴보고 실태를 파악한 뒤, 선진화 되어 있는 위험분석 분야의 장점을 적극 수용해야 한다. 또한 수용만이 아닌 외국의 위험분석 방법론 및 도구들을 정확하게 분석한 후 장단점을 축출하여 국내 정보시스템환경에 맞는 위험분석방법론 및 도구들을 연구해야한다.

본 논문에서는 효율적인 위험분석을 수행할 수 있도록 위험분석에 관한 방법론을 제시하였다. 이 방법론은 현재 연구되고 있는 방법론과 연구 방향이 같지만, 본 논문을 통해 자산분석 및 취약성분석, 위협분석, 대응책분석을 효과적으로 수행할 수 있고 정확한 자산분석을 통해 취약성 분석과 위협분석을 할 수 있게 한다. 또한 이에 해당하는 대응책들이 어떻게 적용되고 있는지 분석함에 있어서 자산과 위협, 취약성의 관계를 통해 가장 효율적인 대응책을 도출할 수 있다. 이렇게 분석된 결과는 조직의 특징에 맞도록 적용할 수 있으며 위험 수준에 따라서 대응책을 수립, 관련 교육들을 실시할 수 있다. 이러한 방법론은 앞으로 급격히 변화하는 시대적 상황에 발맞춘 위험분석에 대한 방법론과 분석모델의 기준을 제시하고 위험분석에 대한 기술력 향상과 위험분석 여건을 조성하는데 큰 도움이 될 수 있을 것으로 보인다.

참고문헌

[1] 한국정보통신기술협회, 공공기관 전산보안정책 수립을 위한 지침서, 1998.

[2] 정보보호진흥원, 취약점 분석·평가를 위함 위험산정 지침 Sep. 2001.

[3] 정태명외 2명, 인터넷 정보 보호, 영진닷컴, 2002.

[4] NIST, Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, 2001.

[5] ISO/IEC JTC 1/SC27, Guidelines for the Management of IT System Security(GMITS) 1996~1997.

[6] BSI, BS7799 Part 1 - Specification for information security management systems, 1999.

[7] CSE, Threat and Risk Assessment Working Guide, ITSG-04, Oct. 1999.

[8] OECD, OECD Guidelines for the Security of Information Systems and Networks Towards a culture of security, Aug. 2002.