표준번호 TTAS.KO-12.0007

공공정보시스템 보안을 위한 위험분석 표준 - 위험분석 방법론 모델

김학범
TTA 정보보호기술위원회(TC10) 간사
한국정보보호센터 표준과제책임자

Ⅰ. 서론

국제적으로 보안관리 분야의 중요성이 부각되면서 관련산업이 많은 발전을 하고 있다. 최적의 정보시스템 보안체계를 구축하기 위해서는 조직의 정보시스템 운영환경을 분석하고, 취약분야와 위험요소를 파악하여 비용효과적인 측면에서 효율적인 대응책을 제시해주는 위험분석 과정이 반드시 필요하다. 이를 위해서는 위험분석의 방법론 및 절차가 확립되어야 하며, 이를 위한 위험분석 표준이 시급히 마련되어야 한다.

위험분석 관련 표준은 크게 3분야로 나누어져 있다.

- ㅇ 공공정보시스템 보안을 위한 위험분석 표준 : 개념과 모델
- ㅇ 공공정보시스템 보안을 위한 위험분석 표준 : 위험분석 방법론 모델
- ㅇ 공공정보시스템 보안을 위한 위험분석 표준 : 위험관리와 평가

본 고에서 소개하는 내용은 위의 3분야 중 두번째 단계인 "위험분석 방법론 모델"에 관한 것이다. 제정된 표준의 목적은 공공정보시스템을 운영하거나 구축하고자 하는 모든 보안담당자가 효과적인 위험관리를 수행할 수 있도록 위험분석의 세부절차와 위험분석 수행을 위한 구체적인 기술을 제시하는데 있다. 이 분야에 대한 국제표준이 제정되고 있으나 국내 정보시스템 환경이 외국과 많이 다르고 국제표준을 그대로 수용하기에는 어려운 점이 많다. 또한 구미 선진국에서도 국제표준을 수용하면서 자

국내 정보시스템 환경에 맞는 위험관리 및 위험분석 표준을 제정하여 활용하고 있다. 따라서 이 표준을 제정하여 공공기관의 보안업무 담당자들이 알맞은 보안대응책을 수립할 수 있도록 위험분석 방법론을 쉽게 적용하는데 도움을 주고 더 나아가 국내 공공기관들의 보안관리 체계수립에 도움을 주고자 한다. 또한 위험분석 수행시 활용하는 세부기술들도 제시한다.

"위험분석 방법론 모델"에 관한 표준인 이 표준은 TR 13335 국제표준의 Part 2와 Part 3의 위험분석 및 위험관리 부문과 관련이 있다. 일반적인 위험분석의 구조와 절차 및 위험분석을 수행하기 위한 구체적인 기술(Techniques)이 다루어진다. TR 13335-3에서 다루어진 위험분석 기술(Techniques) 부문보다 세부적이고 실용적인 관점에서 위험분석 방법론 모델을 정의한다.

본 고는 2장에서 위험분석 모델에 관한 개요를 소개하며, 3장에서는 위험분석 방법론 모델을 마지막으로 4장에서 결론을 맺는다.

Ⅱ. 위험분석 모델 개요

2.1 개요

위험분석은 보안관리(IT Security Management)를 수행하기 위한 필수적인 과정으로 시스템의 위험을 평가하고, 비용효과적인 대응책을 제시하여 시스템 보안정책과 보안대응책 구현 계획을 수립하는 위험관리의 핵심역할을 담당한다. 위험분석의 목적은 보호되어야할 대상 정보시스템과 조직의 위험을 측정하고, 이 측정된 위험이 허용가능한 수준인지 아닌지 판단할 수 있는 근거를 제공하는 것이다.

2.2 위험분석 모델

위험분석을 효과적으로 수행하기 위해서는 수행하기 전에 우선, 조직의 정보시스템의 중요도를 파악하여 위험분석 실시범위와 깊이를 결정해야 한다. 위험분석은 수준에 따라서 수행절차가 복잡하고, 시간과 인력소모가 크므로, 시스템 환경에 맞는 위험분석 수준을 선택하는 것이 중요하다. 본격적인 위험분석 수행에 앞서 사전 위험분석을 통하여 위험분석의 수준을 결정한다. 수준이 결정되면 위험분석을 기본통제 방식으로 할 것인지, 상세 위험분석으로 할 것인지를 알 수 있다. 전체적인 위험분석 모델의 구성도는 다음장 (그림 1)과 같다.

2.2.1 사전(상위수준) 위험분석

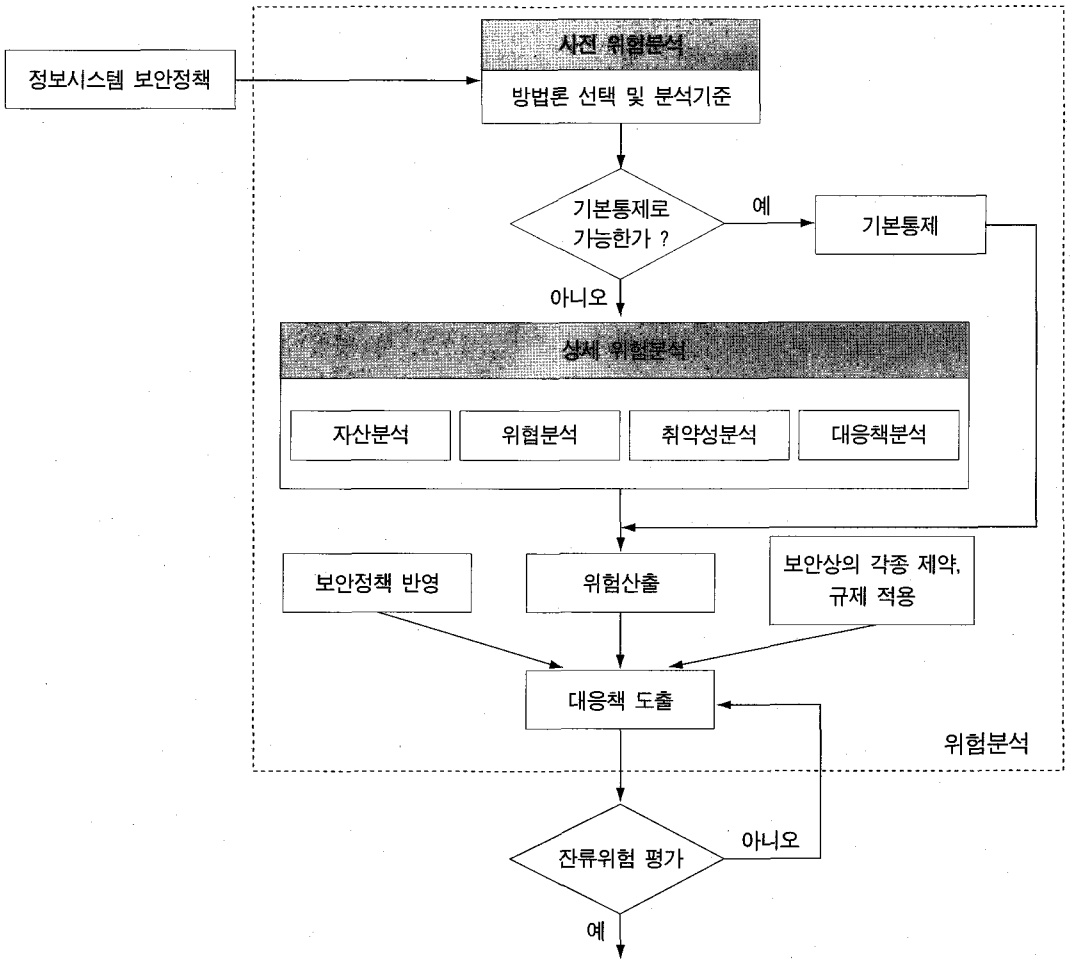
사전 위험분석의 목적은 효과적인 위험분석을 수행하기 위해 현재 조직의 정보시스템 환경에 적합한 위험분석 수준을 결정하기 위함이다. 사전 위험분석에서 고려할 사항은 다음과 같다.

① 정보시스템의 사용목적
② 정보시스템에 대한 업무의 의존도
③ 개발, 유지보수, 대체의 관점에서 시스템에 대한 투자 정도
④ 시스템의 자산가치

2.2.2 기본통제

기본통제 방식의 목적은 정보시스템에 대한 최소의 보안대책 수립이다. 이 방식은 적은 비용으로 전 조직의 기본적인 보안수준을 수립할 수 있다.

이 방식의 장점은 위험분석 실시에 드는 자원과 비용이 거의 없으며, 보안대책 실시에 드는 시간과 노력이 최소화된다는 것이다. 단점은 기본통제의 수준을 어느 정도로 하느냐에 따라 수준이 너무 높으면 지나치게 높은 수준의 보안요구로 인해 과다비용이 들 수 있고, 반대로 너무 낮으면 필요한 보안요구를 간과하여 취약



(그림 1) 위험분석 모델

성을 그대로 노출시킬 수 있다는 것이다. 그러므로, 기본통제 방식은 조직의 요구사항을 반영하여 적절한 수준으로 조정되어야 한다.

기본통제의 작성 방법은 다음과 같다.

① 조직의 보안정책을 참조하여 세부 통제사항을 작성한다.

② 공공기관의 경우 정부부처 및 공공기관에서 요구하는 보안요구 사항을 참조하여 반영한다.

③ ISO, KICS 등 국내/외 표준을 참조하여 반영한다.

④ 외국의 보안 컨설팅기관에서 작성한 기본통제를 참조한다.

⑤ 정보감리 등을 통하여 얻은 결과를 반영한다.

2.2.3 상세 위험분석

상세 위험분석 방식은 정보시스템이 조직의 업무상 중요도가 높거나 자산가치가 클 경우 적용한다. 일반적으로 위험분석을 수행한다고 하는 것은 상세 위험분석을 수행함을 말한다.

상세 위험분석시 소요되는 시간과 비용을 줄이고 분석과정에서의 오차를 줄이기 위해서 위험분석 자동화도구를 사용하는데 자동화도구를 가장 적절히 활용하기 위해서는 다음 사항을 고려하고 준수해야 한다.

① 입력데이터의 정확성
② 사용자에 대한 교육
③ 수작업의 병행
④ 분야별 전문적인 점검도구 활용(예 : 네트웍 취약성 분석도구 등)
⑤ 관리층의 폭 넓은 지원

Ⅲ. 위험분석 방법론 모델

3.1 개요

위험분석 방법론은 보안관리를 수행함에 있어 IT자산, 위협, 취약성, 대응책을 중심으로 대상조직 IT환경의 위험을 세부적으로 측정·분석하는 절차와 기술을 말한다.

이 표준에서 제시하는 위험분석 방법론 모델은 사전 위험분석을 거친후 상세 위험분석을 수행하는 기본적이며 일반적인 과정을 방법론으로 도출해낸 것이다.

① 내용상 신뢰도 : 국외에서 널리 사용되고 있는 방법론(Rand, BDSS, BS7799, EDI, CRAMM, LAVA)을 참조하였으며, 국내외 표준을 반영하였다.
② 기술상 특징 : 위험을 분석하여 산출하는 방법엔 정량적인 수치(1~100점)로 나타내는 정량분석과 위험의 정도를 기술변수(상, 중, 하 또는 높음, 보통, 낮음 등)로 나타내는 정성분석이 있는데, 위 두가지 방법을 모두 활용할 수 있도록 하였으며, 신뢰성이 있는 정성분석에 좀 더 비중을 두었다.
③ 적용상 특성 : 국외 표준과 방법론을 참조로 하되, 학문적 이론에서 탈피하여, 국내 정보시스템 환경에 맞게 적용할 수 있도록 실용적인 방법론 모델을 제시하였다. 또한 정보시스템 환경이 업무(Business)의 관점에서 고려되고 있는 현실을 반영하여, 위험분석시 업무처리절차(Business Process)를 고려할 수 있도록 하였다. 또한 정보시스템 구축 및 운영단계에서 모두 적용할 수 있도록 고려되었다.

3.2 기법

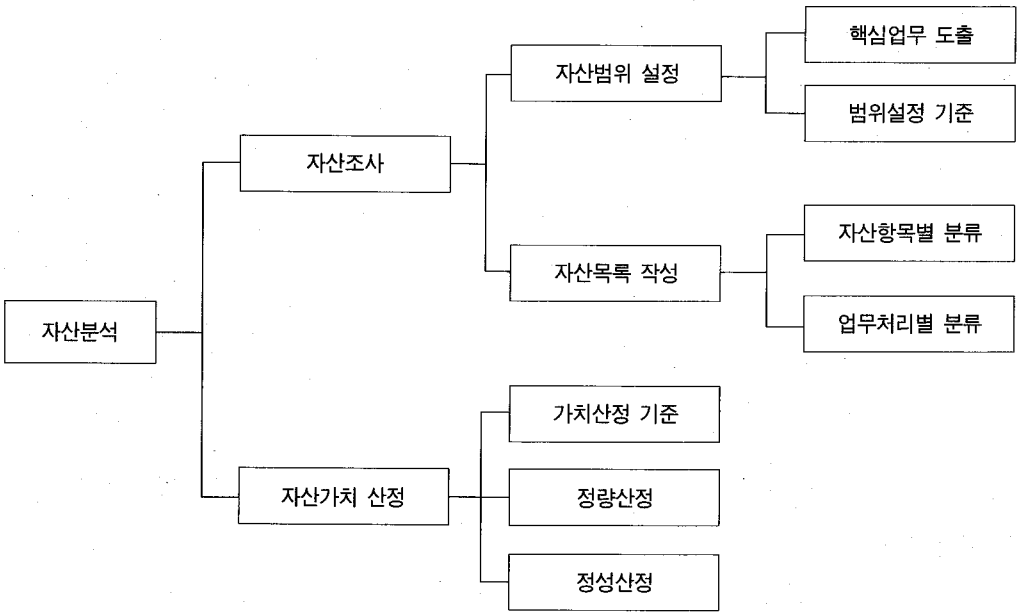
위험분석의 방법을 크게 두가지로 나누면 정량분석과 정성분석으로 나눌 수 있으며, 정량분석법에는 과거자료 접근법, 수학공식 접근법, 확률분포 추정법, 점수법, 확률지배, 몬테칼로 시뮬레이션 등이 있고, 정성분석법에는 질문서법(Questionnaire), 델파이법(Delphi), 순위행렬법(Ranking Matrix), 행렬법(Matrix), 퍼지(Fuzzy), 시나리오(Scenario), 결정법(Decision), 통계적 접근법(Statistical) 등이 있다.

3.3 자산분석(평가)

자산분석을 통하여 조직의 자산을 파악하고, 자산의 가치 및 중요도를 산출하며, IT자산과 업무처리와의 관계도 알아낼 수 있다. 자산 분석과정은 크게 자산조사와 자산가치 산정의 두가지로 나눌 수 있다.

3.3.1 자산조사

자산조사는 조직의 운영·경영에 중요한 영향을 미치는 다양한 IT자산을 식별하고, 분류하는 작업으로서, IT자산에 관한 적절한 관리는 조직의 자산을 적절하게 보호하는데 있어서 필수적인 과정이다.



(그림 2) 자산분석 과정

가) 자산범위 설정

자산범위 설정시에는 반드시 업무적인 측면을 고려해야 한다. 즉, (1) 조직의 운영·경영 측면의 검토 (2) 핵심 업무처리(Business Process) 도출 (3) 범위 설정기준 도출의 과정을 거쳐 범위설정을 해야한다.

나) 자산목록 작성

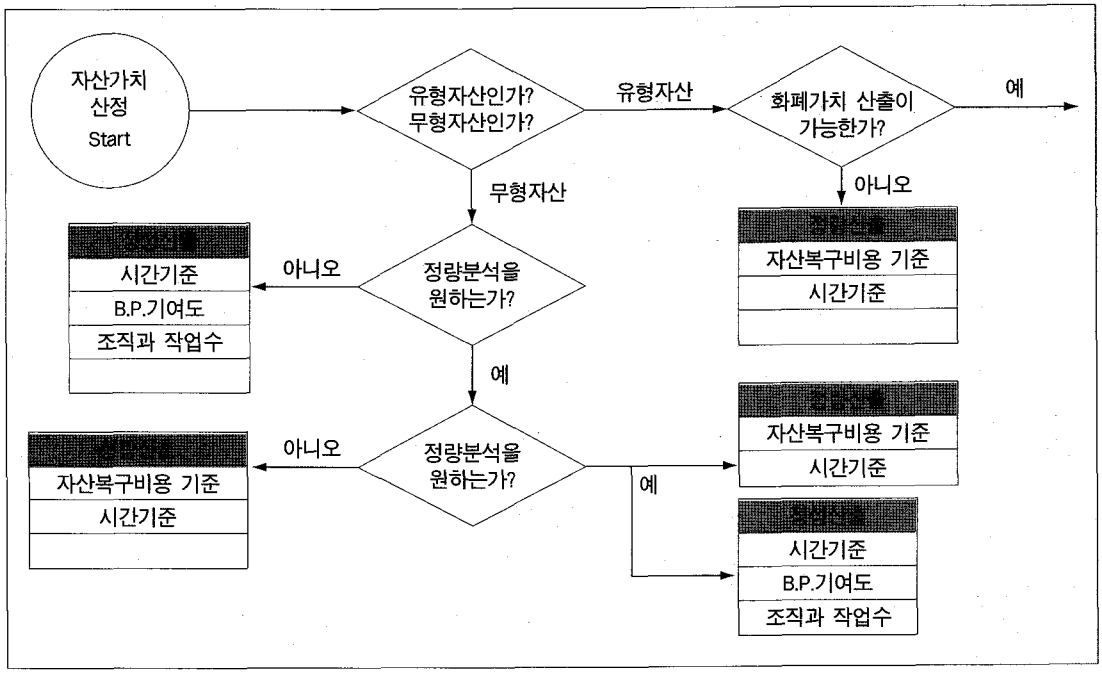
자산목록 작성은 자산범위 설정을 통하여 파악된 조직의 규모와 운영목적 및 환경을 바탕으로 위험분석 대상자산의 실질적인 파악작업이다. 자산목록 작성은 자산범위(Boundary of Asset)에서 정의된 기준에 따라 가능한 모든 IT자산을 나열할 수 있어야 한다. 자산목록 작성시 고려해야 될 사항은 아래와 같다.

① 자산항목별 분류 및 자산범위에 따른 선별
② 업무처리를 고려한 자산조사
③ 조직을 고려한 자산조사
④ 업무처리와 자산간의 관계정립
⑤ 자산항목별 분류 및 조사

3.3.2 자산가치 산정

자산가치 산정은 자산의 중요도를 파악하고 위협(Threat)이 발생할 경우 있을 수 있는 피해(영향 : Impact)를 측정하기 위한 정보를 얻기 위해 위험분석 대상자산의 가치(Value)를 정량 또는 정성적인 방법으로 평가하는 과정이다. 자산의 특성에 따라 정량적인 수치로 산정이 가능한 것도 있으나, 그렇지 못한 경우도 많으므로 정확한 자산가치를 산정하기 위해서는 위 두 가지 방법 모두를 혼용하여 사용한다. 전체적으로 정량/정성 분석의 가치기준을 적용하는 flow를 예로서 다음장 (그림 3)과 같이 나타낼 수 있다.

자산가치 산정시 정량적, 정성적 방법을 적용할 때 기준을 살펴보면 다음과 같다.



(그림 3) 자산가치 적용 Flow 예

정량적 기준	정성적 기준
• 자산도입비용 • 자산복구비용 기준 • 자산교체비용 기준	• 업무처리에 대한 자산의 기여도 • 자산이 영향을 미치는 조직과 작업의 수 • 시간(복구시간) • 기타(조직의 특성에 맞는 기타 요소들)

가) 정량적 기준

① 자산도입비용 기준 : 자산도입비용은 위험분석을 시스템 구축시 적용할 경우 그대로 사용할 수 있다. 그러나 운영중인 시스템과 조직을 대상으로 한 위험분석에는 그대로 사용되기 어렵다.

② 자산복구비용 기준 : 자산복구비용은 "자산도입비용" 기준을 적용할 수 없는 무형적(Intangible) 자산의 가치산정에 사용되는 기준으로, 무형자산(시스템관리자나 데이터)의 경우 정성분석 기준을 중심으로 자산가치를 산정하는 것이 타당하다.

③ 자산교체비용 기준 : 자산교체비용은 자산의 가치를 측정하는데 있어 도입당시의 비용을 기준으로 평가하는 것보다 자산을 교체할 경우의 비용을 기준으로 산정하는 것이 정확한 위험분석을 하는데 타당하다고 판단될 경우 적용한다. 특히 하드웨어 관련 자산들은 가격이 급속히 떨어지고 성능은 급속히 향상되기 때문에 자산의 가치를 당시 기준으로 평가하는 것은 적절치 못하다.

나) 정성적인 기준

정성적인 기준은 데이터, 정책 등과 같이 분석대상 자산의 화폐가치 산정이 어려운 경우에 적용되면 이때 우선적으로 고려할 사항은 다음과 같다.

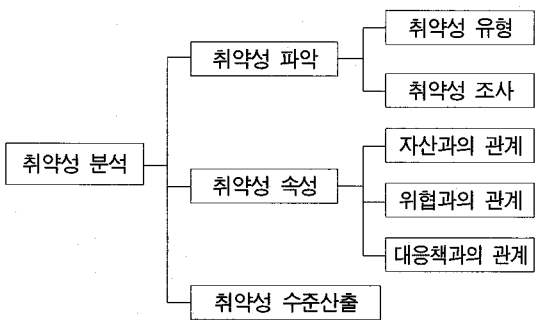
① 분석대상 자산의 업무처리에 대한 기여도
② 자산이 영향을 미치는 조직과 작업의 수
③ 시간(복구시간 등)
④ 기타(조직의 특성에 맞는 기타 요소들)

위의 사항을 고려하여 자산을 정성적인 방법으로 아래와 같이 크게 5등급으로 나누어 평가할 수 있다.

등급	설명
Very Hight (Scale : 5)	중요도가 가장 높은 경우
High (Scale : 4)	중요도가 비교적 높은 경우
Medium (Scale : 3)	중요도가 보통인 경우
Low (Scale : 2)	그다지 중요하지 않은 경우
Negligible (Scale : 1)	중요하지 않은 경우

3.4 취약성 분석(평가)

취약성 분석은 자산분석을 통하여 도출된 자산의 속성과 중요도를 바탕으로 자산이 근본적으로 가지고 있는 약점인 취약성을 발굴하고 취약성이 전체적인 위험에 미칠 수 있는 영향을 분석하는 과정이다.



(그림 4) 취약성 분석과정

취약성 분석과정은 크게 취약성 파악, 취약성 속성, 취약성 수준산출의 3과정으로 나눌 수 있으며, 취약성 파악에서는 유형별로 취약성을 파악하고 조사한다. 취약성 속성에서는 취약성과 자산, 위협, 대응책과의 상호관계를 파악한다. 마지막으로 취약성 수준산출에서는 파악된 취약성의 수준을 산출하여 우선적으로 고려해야 할 취약분야를 알 수 있도록 하고, 취약성을 여러 유형으로 나누어 각 유형별로 취약성 수준을 산출하는 경우와 단일개체(entity)로 보고 각 자산별로 취약성의 수준을 산출하는 경우로 나눈다.

3.5 위협 분석(평가)

위협분석은 자산에 피해(Impact)를 가할 수 있는 잠재적인 요소인 위협을 파악하고 발생가능성 등을 분석하는 과정으로서 위험을 산출하는데 있어 중요한 단계이다. 특히 자산과 취약성간의 관계를 정의함으로서 향후 위협이 미칠 대상을 고려하게 된다. 위협분석은 크게 위협파악, 위협속성, 위협순위의 3개 과정으로 나뉜다.

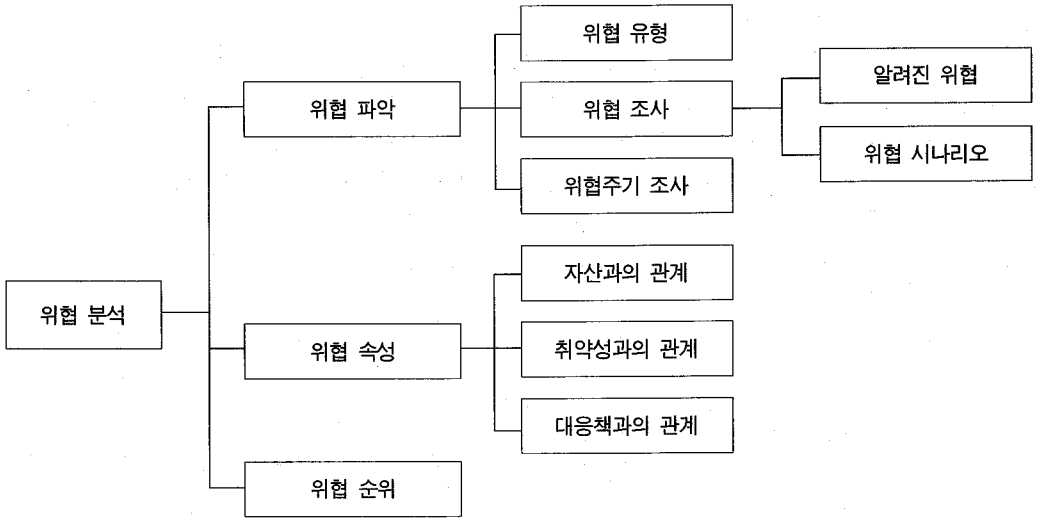
3.5.1 위협 파악

가) 위협 유형

위협이 영향을 미칠 수 있는 IT분야에 기초해 자산과 취약성과의 관계를 고려해 하드웨어(H/W), 운영체제(O/S), 응용소프트웨어(Application), 네트워크(Network), 데이터(Data), 사용자(Users), 환경(Environment)으로 분류한다.

나) 위협 조사

이 단계에서는 앞에 언급한 위협유형에 따라 현존하거나 알려지지 않은 위협들을 조사하는



(그림 5) 위협 분석과정

것이 목적이다.

① 알려진 위협(Confirmed Threats) : 알려진 위협은 조직에서 발생되었거나 파악된 위협들이다. 주로 전산실의 장애관리 일지나 IT 보안조직에서 대응했던 사고 대응일지 등을 바탕으로 조사할 수 있다.

② 위협 시나리오(Threat Scenario) : 위협 시나리오는 파악되지 않은 위협을 발견하기 위해 사용하는 방법이다. 위협 시나리오는 가상적인 위협환경을 설정하고 발생가능한 위협을 유추하여 위협을 찾아내는 방법이다.

다) 위협주기 산출

위협에 대한 자극의 횟수가 주기이다. 주기는 위협의 잠재적인 파괴력을 증가시키는 또 다른 변수이다. 위협주기는 이미 발생한 위협을 기록한 통계자료를 이용하여 입력하는 경우가 있고, 통계자료가 없기 때문에 유추하는 경우가 있다.

3.5.2 위협 속성

실제로 관찰할 수 없는 잠재적인 위협의 속성을 파악하여 자산에 주는 영향을 알아내기는 쉽지 않은 일이다. 위협과 자산, 취약성, 대응책의 관계를 바탕으로 위협의 속성을 정의하면

① 위협은 자산이 잠재적으로 지닌 취약성을 이용하여 자산에 직접적인 위험을 초래한다. (자산, 취약성과의 관계)

② 대응책이 늘어나면 위협이 이용할 취약성이 감소하므로, 위협이 초래할 위험도 줄어든다. (취약성, 대응책의 관계)

3.5.3 위협 순위

위협순위는 위험분석 대상조직에 대해 가장 많은 영향(Impact)을 줄 수 있는 위협의 중요도를 정하여 나열하는 과정이다. 위협의 중요도를 전문가 의견을 취합하여 정하는 방식으로 정확도는 다소 떨어질 수 있으나 위협에 관한 과거자료가 매우 부족한 조직에서는 정성적인 방식에 의해 위협의 중요도를 정하는 것이 현실적인 방법이다. 산출방식은 의견을 취합하여 Matrix Scaling 하는 것이 보편적이다.

위협의 영향(Impact)을 결정짓는 가장 중요한 요소는 위협 발생주기이다. 화재나 건물붕괴같이 파괴력이 크나 발생주기가 미미한 위협보다는 해킹, 바이러스, 정전 등과 같이 파괴력은 적으나 발생주기가 지속적인 위협의 피해가 훨씬 심각하다. 위협주기를 기준으로 한 위협순위를 산출하는 과정을 예를 들면, '화재'라는 위협의 위협주기를 고려한 정성적 중요도가 5점이고, 이 위협과 관련된 자산들(주전산기(4점), 건물(3점), 라우터(5점) 등)의 정성적 가치의 합이 28점 이라고 가정했을 때 '화재'라는 위협의 정성적 점수는 5 + 28 = 33점이 되고, 이와같이 산출된 위협점수를 상호 비교하여 순위를 결정한다.

3.6 대응책 분석(평가)

3.6.1 대응책 파악

대응책 파악은 위험분석 대상조직에서 현재 수행하고 있는 각종 대응책(countermeasure)과 각 자산에 필요한 대응책을 모두 파악하는 단계로 각 대응책을 유형별로 분류하고 조사하여 목록을 작성한다.

3.6.2 대응책 속성

대응책 속성은 자산, 취약성, 위협과의 상호관계를 파악하기 위해 대응책의 속성을 분석한다.

① 대응책은 자산을 현존하는 위협으로부터 보호한다.(자산과 위협과의 관계)
② 대응책이 증가할수록 취약성은 감소하지만, 대응책 자체도 취약성을 가지고 있으므로, 취약성은 결코 0이 될 수 없다.(취약성과의 관계)
③ 대응책은 위협의 발생으로 인한 피해를 감소시키고, 유형에 따라 위협의 주기도 감소시킨다.(위협과의 관계)

3.6.3 대응책 순위

위험분석의 가장 큰 목적은 위험을 측정하는 것이지만 이에 못지 않게 비용효과적인 대응책을 제시하는 것도 위험분석에서 큰 비중을 차지한다. 비용효과적인 대응책을 제시하기 위해서는 제한된 비용을 조직에 가장 필요하고, 시급한 대응책에 우선적으로 투자를 해야한다.

3.7 위험 시나리오(자산-취약성-위협-대응책 매핑)

위험 시나리오란 어떤 한 자산(A)에 취약성(V)이 존재한다고 가정하면, 특정위협(T)의 공격으로 위험이 발생할 수 있고, 이에 대한 대응책(C)을 마련하여야 한다는 일련의 과정을 정의하는 것이다. 위험 시나리오가 자산-취약성-위협-대응책의 상호관계를 정의하는 것이므로 이들 요소간의 관계를 정의할 수 있는 공통적인 속성을 파악하는 것이 무엇보다 중요하다.

3.8 위험산출 및 평가

위험산출 및 평가 단계에서는 자산분석, 취약성분석, 위협분석, 대응책분석을 통하여 얻은 데이터와 분석결과를 바탕으로 위험을 측정하고 산출하여, 평가(Evaluation)한 후 대응책을 제시해 주는 위험분석의 최종 단계이다.

3.8.1 취약성 수준 산출

본 방법론에서 산출하는 취약성 수준은 위험 시나리오를 기준으로 연관되어 있는 대응책들 중 시행하고 있는 대응책들과 미 시행 대응책들 간의 비율을 말한다. 미 시행 대응책들이 많으면 많을수록 취약성 수준은 100에 근접하고

미 시행 대응책들이 적을수록 0에 근접한다.

자산별 취약성 수준을 통하여 각각의 IT자산이 가지고 있는 위험을 간접적으로 알 수 있으며, 무엇보다도 각 자산과 관련된 업무처리에 대한 위험을 파악할 수 있다. 항목별 취약성 수준을 통하여 보안관리의 어느부문에 문제점이 있는지 파악할 수 있다. 예를 들어 '패스워드 유출 취약성'의 산출결과가 높게 나왔다면 이는 세부적으로 접근통제에 문제가 있는 것이며 크게는 대상조직의 인증보안에 문제가 있는 것으로 진단할 수 있다.

3.8.2 A.L.E 산출

A.L.E(Annual Loss Expectancy Value : 연간 기대 손실치)란 IT자산에 가해질지도 모르는 피해(Impact)를 화폐단위로 측정한 값이다. A.L.E는 미국 NIST(National Institute of Standard and Technology : 미국국립표준기술원)에서 FIPS(연방표준)-65라는 문서를 통해 1979년 산출방법을 공개한 이래 정량분석에서 사용되는 A.L.E는 이 방식을 근간으로 하고있다. 위협주기에 따라 A.L.E의 변동폭이 매우 크고, 산출값이 비현실적인데 이는 단순히 자산가치와 위협주기만 고려하기 때문이다. 본 방법론에서 제시하는 A.L.E산출 방법은 다음과 같다.

A.L.E = Value(자산가치) X Exposure Factor(위협에 노출 정도) X Tf(위협주기)

자산가치와 위협주기는 자산분석과 위협분석에서 언급한 절차에 따라 산출하여 적용하고, 자산이 위협에 어느 정도 노출되어 있는지를 나타내는 E.F는 위험 시나리오의 자산-취약성-위협-대응책의 관계에서 자산-위협을 기준으로 관련 있는 대응책과 시행하고 있는 대응책 및 미 시행 대응책의 비율로부터 산출할 수 있다.

$$E.F = V = \left(\sum_{i=1}^{i=n} CiW - \sum_{i=1}^{i=n} C'iW\right) \div \sum_{i=1}^{i=n} CiW$$

- CiW : 자산-위협별 전체 대응책의 중요도 합
- C'iW: 자산-위협별 실시 대응책의 중요도 합

3.8.3 위험 순위

위험순위란 자산 또는 기타 항목별로 위험의 정도가 높은 순으로 나열하여 위험을 감소시켜야 할 항목들의 우선순위를 나타내기 위한 것이다. 위험순위는 체크리스트를 사용하여 간단한 위험분석(예를 들면 기본통제 : Baseline Control)을 수행할 때 결과도출에 자주 사용되는 방식이다. 위험순위를 산출하는 기준은 여러 가지가 있으나 본 방법론에서는 취약성, 자산가치, ALE를 기준으로 위험순위를 도출하였다.

① ALE 기준 : ALE 기준의 위험순위 산출은 정량적으로 ALE를 산출할 수 있는 자산에 대해서만 순위를 매긴다. 따라서, 정량적 가치산정이 어렵거나 해당 자산의 위협주기가 제대로 파악되지 않은 자산의 경우는 ALE 기준의 위험순위에 반영되지 않는다는 것을 고려해야 한다.

② 취약성 수준 기준 : 취약성 수준 기준의 위험순위 산출은 전 자산을 대상으로 한다. 취약성 수준은 자산별로 대응책의 시행 및 미 시행의 비율로 산출되므로 모든 자산의 위험순위를 산정할 수 있다.

③ 업무처리 중요도 기준 : 자산 분석시 작성되었던 핵심 비즈니스 프로세스(Core Business Process)에 대한 위험정도를 취약성 수준을 기준으로 평가한다. 그래프를 작성하여 나타낼 수 있고, 보안정책이나 위험분석시 정해진 위험기준(취약성 등급기준)

의 기준선에 따라 위험도를 표시한다.

3.8.4 필요대응책 도출

과거의 기록과 현재상태에 근거한 위험분석은 그 분석결과가 아무리 정확하다고 하더라도 미래에 일어날 수 있는 각종 보안사고 및 재해 등을 예측하고 대비하기에는 부족하다. 따라서 현재 분석된 결과를 바탕으로 가상의 시나리오를 적용하여 그 결과를 관찰하고 알맞은 대응책을 강구하기 위하여 적용하는 과정이 What-if Scenario이다.

What if ? ---특정 위협이 발생한다면 ?
---특정 대응책을 구현한다면 ?
---특정 자산을 도입한다면 ?

위협, 위협주기, 대응책 등이 What if 시나리오에서는 변수(Parameter)로 이용될 수 있다. 발생가능성이 있는 다양한 조건과 환경들을 가상으로 위험분석 대상조직이나 시스템에 가상 적용하여 그 결과를 바탕으로 새로운 대응책을 제안할 수 있다.

3.8.5 비용효과 분석

비용효과 분석이란 위험을 감소시키기 위하여 필요한 대응책들의 수행여부를 비용적인 측면에서 고려하여 판단하는 분석과정을 말한다. 이 과정을 통하여 위험분석 결과를 가장 효과적으로 활용할 수 있으며, 예산의 제약 등을 고려하여 제한된 비용으로 최적의 효과를 얻을 수 있도록 최고 경영진의 의사결정을 지원한다.

3.8.6 종합평가

종합평가는 지금까지 분석된 결과를 바탕으로 전반적인 위험을 기술하고 분석된 위험이 조직의 업무처리에 미치는 영향을 나타내는 과정이다. 뿐만 아니라 비용효과 분석 등을 통하여 얻어지는 결과는 조직에서 가장 시급한 필요 대응책들을 간략하게 기술하고 예산을 확보하기 위하여 최고경영진을 설득할 수 있는 충분한 자료를 수록하여야 한다. 필요하다면 IT 보안정책(IT Security Policy)을 수정하여야 하며 위험분석시 포함된 각 시스템들에 대한 시스템 보안정책(System Security Policy)도 새로 작성하거나 보완하여야 한다.

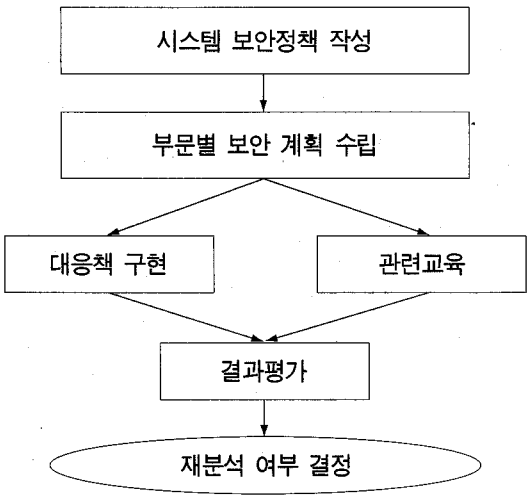
종합평가는 다음과 같은 내용으로 구성한다.

① 종합평가의 구성비용
② 대상조직/시스템 종합
③ 취약성 수준의 평가(자산별, 분야별, 업무처리측면)
④ ALE 결과의 평가
⑤ 비용효과 분석의 결과 및 주요 이슈, 문제점
⑥ 위협에 대한 평가
⑦ 기타 예산, 정책, 조직의 개선점, 문제점

취약성 수준의 평가는 취약성 분석결과가 조직에 미치는 영향을 종합적이고 간단명료하게 해석하고 정리함으로서 최고경영자의 결정을 도와준다. ALE 결과의 평가는 위험분석의 결과가 미치는 영향을 종합적으로 정리한다. 비용효과 분석의 평가는 비용효과 분석을 통하여 도출된 필요대응책들의 구현 필요성, 보안예산의 증감유무, 투자 대 효율 등을 종합적으로 정리하여 최고경영자로 하여금 투자에 대한 결정을 돕는다.

종합평가가 마무리되면서 사실상의 위험분석은 마무리된다. 위험분석 결과를 바탕으로한 다음단계는 위험분석의 결과를 바탕으로 시스템별 보안정책을 작성하고 부문별 보안계획을 수립한다. 계획이 수립되면 대응책을 구현하고, 관련교육을 실시한 후, 다시 재평가하여 조직에서 허용가능한 위험수준을 만족하는지 검토하고,

재분석을 실시해야하는지도 결정한다.



(그림 6) 위험분석 이후 과정

Ⅳ. 결론

본 고는 정보통신단체표준으로 금년 3월 제정된 '공공정보시스템 보안을 위한 위험분석 표준 - 위험분석 방법론 모델'에 대해서 소개한 내용으로 표준내용을 간략하게 소개하였으므로 보다 상세한 내용을 참조하실 분들은 원안을 참조하시기 바란다. 제정된 표준은 다양한 위험분석 방법론의 기준이 될 수 있는 기본적인 방법론 모델을 도출한 것으로서 보안관리 실무, 보안관리 컨설팅, 관련 소프트웨어 개발 등 다양한 분야에서 활용될 수 있을 것으로 기대된다.

산학협동을 위한 S/W전문가 인력 DB구축

충남대학교 소프트웨어연구센터는 SW전문가 인력 DB 및 벤처창업 정보가 담긴 포털사이트(http://sw.cnu.ac.kr)를 개설했다고 3월 26일 밝혔다. 이번에 구축된 SW전문가 인력 DB에는 CALS, EC, 디지털 라이브러리 등 3개 분야에 각각 21명, 19명, 23명 등 63명의 전문가가 등재돼 있다. 포털사이트에 등재된 전문가는 충남대 김종우, 류재철 교수와 한국전자통신연구원 책임급 연구원 6명이 인력DB관리위원회를 구성, 선정했으며 산업체 요구에 적합한 분류체계를 도입하기 위해 연구분야별 분류보다는 응용분야별 분류체계를 적용했다. 또 인터넷 검색시스템을 통한 전문가 검색을 위해 단순, 상세, 분야별 검색기능이 부여돼 있는 것도 특징이다. 벤처업체를 위한 포털사이트는 중소기업청 창업지원제도에 대한 창업정보와 국내외 기술동향정보, 특허관련 벤처창업지원제도에 대한 기술정보, 국내 인터넷 관련기관 소식지 가운데 소프트웨어 관련 뉴스, 추천사이트, 공개 소프트웨어 자료실 등의 메뉴로 구성돼 있다. 소프트웨어연구센터 김찬권 전임연구원은 「지역 SW분야 산업체의 기술 경쟁력을 높이는 데 주안점을 둬 DB제작과 포털사이트 구축을 하게 됐다」며 「업체가 SW 개발시 시간을 단축할 수 있고 품질을 향상시켜 지역 산, 학, 연 연계활동 활성화에 기여할 것으로 기대한다」고 말했다.