정량적 방법을 이용한 위험분석 방법론 연구

박 중 길†

요 약

위험분석은 조직의 특성을 반영하여 자산분석, 위협분석, 취약성 분석을 통하여 조직의 주요 자산에 대한 위험도를 분석하고 적절한 대응책을 제시하는 것을 목적으로 한다. 하지만, 기존의 TTA 위험분석 방법론은 전체의 개략적인 흐름은 제시하고 있으나, 각 단계에서의 구체적인 행위를 제시하지 못하고 있다. 즉 위협분석 단계에서는 어떠한 기준으로 각 위협을 어떻게 분류하여야 하는가하는 문제와 분류된 위협을 어떤 방식으로 위험도 계산에 반영해야하는가에 대한 구체적인 제시가 미흡한 현실이다. 또한 취약성 분석 단계에서는 발견되는 취약성을 어떠한 항목을 기준으로 분류하여야 하며, 발견되는 각 자산별 취약성을 위험분석의 위험도 산정에 어떤 과정을 통하여 반영해야하는가에 대한 제시 역시 미흡하다. 따라서 본 논문에서는 기존 TTA의 방법론에서 제시하고 있지 않은 위협분석과 취약성 분석 단계에서의 정량적인 평가가 가능한 방법론을 제시한다. 이를 위하여 본 논문에서는 자산 가치 평가에 조직의 비즈니스 프로세스를 기준으로 업무 영역 분류를 통한 유형자산 가치분석과 무형자산 가치분석을 수행하고 이를 바탕으로 취약성을 분석하고 위험도를 계산하였다. 이러한 방법은 국내 정보시스템의 현실을 반영하고, 환경적 취약성과 기술적 취약성의 영향력을 반영하여, 조직의 자산별로 수치화된 위험도 산정을 가능하게 한다. 이는 위험분석 평가 대상 조직의 자산별 위험도 분석이 가능하게 한다.

키워드 : 위험분석, 취약성, 위협

Methodology of Analyze the Risk Using Method of Determinated Quantity

Joong-Gil Park†

ABSTRACT

The risk analysis's aim is analyze the risk for the asset of organization with asset assessment, vulnerability assessment, threat assessment. existing TTA risk analysis methodology model propose to overall flow, but can not propose to detail behavior of each level. That is, step of risk analysis is insufficient in classification of threat and detail proposal of considered the risk with classified threat. So this paper propose that analysis and evaluate the vulnerability and threat assessment with determinated quantity. this paper consider current national information system and threat of environment and technology. so can estimate the risk with determinated quantity. finally, analyze the asset risk of organization.

Key Words : Risk Analysis, Threat, Vulnerability

1. 서 론

현대의 정보통신시스템 주변에는 수많은 위협요소와 취약성이 존재함으로써 언제든지 정상적인 운영을 방해할 수 있으며 다양한 형태의 부정적인 영향이 발생될 수 있는 상황이다. 특히 네트워크의 발전으로 인해 다수의 컴퓨터가 신경망처럼 연결되고 한 시스템에서 발생한 문제가 실시간으로 다른 컴퓨터에도 영향을 미칠 수 있게 되는 현재의 상황에서는 관리가 전체 시스템에 이루어져야 하며, 이때에는 관리가 전체 시스템을 고려하여 제공되어야 한다. 이러한 일련의 과정을 위험분석이라 한다[1].

현재 많은 조직이나 기업내부에서 자신들의 정보보호 수준을 제고하기 위한 기술적 점검이나 정보보호 컨설팅에 대한 수요가 매우 빠른 속도로 확산되고 있다. 국내에서도 금융권, 대기업 등을 중심으로 제품 중심이 아닌 "조직의 보안 차원"에서 위험분석이 이루어지기 시작하여 급속한 성장을 이루고 있다. 특히, 고객의 자산을 운용·관리하는 금융권에서 이러한 움직임이 있는 것은 정보시스템에 대한 보호관리 미비는 곧 자산의 손해로 이어질 수 있다는 인식을 갖기 시작했다는 것으로 풀이될 수 있다.

조직의 차원에서 보안 관리를 수행한다는 것은 운영 장비에 존재하는 기술적 취약성을 찾아내어 제거하는 단순한 기술적 수행에서 벗어나 기술적인 내용과 함께 조직의 관리적 측면, 물리적 측면까지도 포함시켜야 한다. 이러한 과정을 통해 기술적인 문제점이 제도적으로 제거되어 조직의 보안

† 정 회 원 : 국가보안기술연구소 책임연구원
논문접수 : 2006년 10월 2일, 심사완료 : 2006년 10월 23일

강도를 높일 수 있게 되는 것이다. 또한, 위험분석은 다양한 위험요소에 의해 기관의 정보유출 및 보안 침해 사고가 발생할 수 있는 가능성을 확인하고 가능성을 낮추기 위해 투입해야 할 자원의 규모 그리고 투입 후에 위험도의 낮아지는 정도를 계산하는 과정을 포함하기도 한다.

이러한 위험 분석에 대한 요구는 2001년 7월에 "정보통신기반 보호법"을 시행함으로써 가속화되고 있으며, 국내 주요 정보통신기반 인프라를 보유한 조직에서 운영 중인 정보시스템을 안전하면서도 안정적으로 운용하기 위해 증가하고 있다. 이러한 국내외의 추세에 맞추어 국내의 현실에 맞는 위험분석 평가 프로세스 및 관련도구의 개발이 시급하다. 위험분석을 실제로 수행하기 위한 방법론은 이미 여러 가지가 개발되어 발표되었다. 각 방법론들은 나름대로의 장·단점과 특징을 가지고 있으나 기본적으로 객관적이지 못 한 결과를 생성한다는 문제점을 가지고 있다. 본 논문에서는 기존의 방법론에서 제시하고 있는 프로세스의 문제점을 분석하고 이러한 문제점을 해결하면서 보다 객관적이고 정량적인 위험분석 결과를 생성할 수 있는 개선된 프로세스를 제시하고 이의 우월성을 증명하고자 한다.

본 논문의 2장에서는 위험 분석과 관련된 국내와 연구내용을 소개하고, 3장에서는 그 중 한국 현실에 적합하게 되어있는 TTA의 위험분석 방법론의 문제점에 대하여 알아본 뒤, 4장에서 새로운 위험분석 방법론을 제시한다. 5장에서는 새로운 위험분석 방법론과 TTA의 위험분석 방법론을 비교하고 6장에서는 그에 대한 결론을 내린다.

2. 관련연구

II장에서는 GMITS, BS7799,IAM과 같은 외국에서 연구되는 위험분석 방법론과 국내에서 연구된 TTA의 위험분석에 대하여 소개한다.

2.1 GMITS

국제표준 ISO/IEC TR 13335(Guidelines for the Management of IT Security)이며, 5개의 파트로 구성된다. 상위수준의 위험분석을 먼저 실시하고 4가지의 위험분석 방법 중에서 하나를 선택하도록 되어 있다. 4개의 위험분석 방법은 Baseline approach, Informal approach, Detailed risk analysis, Combined approach이다. 그리고 5개의 파트 구성은 다음과 같다[2].

- Part 1 : Concepts and model for IT Security
- Part 2 : Managing and planning IT Security
- Part 3 : Techniques for the management of IT Security
- Part 4 : Selection of safeguards
- Part 5 : Safeguards for external connections

GMITS에서 제시하는 가치 척도는 무시해도 무방함, 낮음, 중간, 높음, 매우 높음으로 구분하고 있다. 평가에 고려해야 할 사항으로는 법률, 규정위반, 조직의 이미지 손상, 부정적 영향 등이 있다. 평가방법은 정량적 평가뿐 아니라, 정량적 평가가 곤란한 것은 정성적 평가가 가능해야 하며, 자산과 자산의 종속관계가 올바르게 식별되어야 올바른 평가결과를 기대할 수 있는 특징을 가지고 있다.

이 방법론을 구매하기 위해서는 ISO 표준 대표기관인 기술표준원에서 유료로 구매해야 한다.

2.2 BS7799

이 방법론은 영국 표준협회(BS)에서 1993년부터 제정한 BS7799이며 후에 ISO 17799가 되었다. 정보 시스템의 보안관리(SMS)에 대한 지침이며, 평가 기준이기도 하다. 영국에서는 ISO 17799를 기반으로 한 평가 스키마가 구축되어 있으며, 국내에도 이 제도를 컨설팅하는 많은 업체가 존재한다. 이 방법론에서 정보 자산의 가치는 조직 및 비즈니스에 미치는 영향력을 기반으로 산정하여 자산의 속성에 맞도록 정성적/정략적인 방법으로 가치를 평가할 수 있다. 즉 자산 도입비용, 복구비용, 교체 비용을 기준으로 하는 정량적 방법과 업무처리의 기여도, 자산의 피해가 영향을 미치는 조직(조직의 인원 수, 보안 속성 등)에 대한 영향을 기준으로 평가하는 정성적 방법을 이용한 위험분석 방법론이다. ISO 17799의 평가 방법론은 다음과 같은 과정으로 구성되어 있다[3].

- 정보보호 정책 정의
- ISMS의 범위 정의
- RA 실시
- 위험 관리
- 구현할 목적과 통제를 선택
- Statement of Applicability(SoA) 준비

ISO 17799에서 진행되는 전체 위험분석 단계는 다음의 (그림 1)과 같은 위험분석 단계를 가진다.

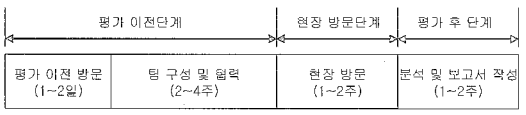
이러한 ISO 17799를 위한 위험분석 평가도구로서 영국에서 제작한 COBRA 도구가 있다. 이 도구에서는, 모든 위협과 취약성 평가를 통하여 해결책과 권장사항을 제시해준다. 이 도구에서는 가능한 위험과 위협의 연관관계를 설정하고 하고, 잠재적인 영향을 분석한다. 자산의 중요도를 파악하고, 조직의 특정 자산에 대한 위협이 발생할 경우, 자산 손실의

(그림 1) BS7799의 위험분석 프로세스

영향도를 평가하기 위한 정보를 얻기 위해서, 위험분석 대상 자산의 가치를 평가하는 프로세스를 포함하고 있으나, 기준이 추상적이고 주관적이기 때문에 널리 활용되지는 않는다.

2.3 IAM(INFOSEC Assessment Methodology)

NSA의 15년간의 경험으로 개발되었으며 국방부의 교육용 자료로 사용하기 위해 개발되었다. 미정부의 정보시스템에 관련된 자에게만 교육이 이루어지고 있는 방법론이다. 한 기관의 잠재적인 취약성을 분석하는 방법론이며, 취약성 발견시에 그에 대한 적절한 대응책을 제시할 수 있도록 하였다. 다음의 (그림 2)와 같이 총 3개의 단계로 구성되며, 각 단계에 대한 설명은 <표 2>과 같다.



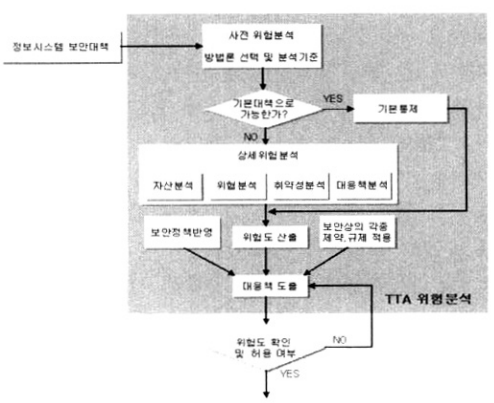
(그림 2) IAM의 3단계

〈표 1〉 IAM의 단계별 목적과 일정

단 계	목 적	진행일정
평가 이전 단계	· 고객의 요구분석 · 고객정보 중요도 파악 · 평가계획 설계 · 중요정보를 보유하고 있는 시스템 확인 · 현장방문에 대한 사전준비	· 정보의 중요성 파악 · 시스템 구성 확인 · 평가범위 결정 · 시스템 문서 요구 및 검토 · 전문가 인원 확충 · 문서 재검토 · 사전분석 · 현장방문에 대한 논의
현장 방문 단계	· 사전평가단계에서 작성된 정보 분석 · 데이터 수집 및 평가 · 분석결과 도출	· 기조모임 · 시스템 정보의 수집 및 평가 · 평가정보 분석 · 초기 권고안 작성 · 브리핑
평가 후 단계	· 평가분석 종결 · 결과보고에 대한 준비 및 조정	· 문서에 대한 추가적인 검토 · 전문가 의견 고려 · 최종보고서 작성

2.4 TTA의 위험 분석 방법론

TTA의 위험분석 방법론은 공공정보시스템 보안을 위한 위험분석 표준 방법론으로서 활용되고 있다[ref].



(그림 3) TTA에서 제시하는 위험분석 프로세스

TTA에서의 위험분석은 시스템의 위험을 평가하고 비용대비 대응책을 제시하여 시스템의 보안 정책과 보안 대응책 구현 계획을 수립하는 위험관리의 핵심 역할을 담당하는 것을 주요 목적으로 한다. TTA에서 제시하는 위험분석 프로세스는 (그림 3)과 같다[1].

3. TTA의 위험분석 방법론의 문제점

구미 선진국에서는 국제 표준을 수용하면서 자국내 정보시스템의 환경에 맞는 표준을 정의하여 활용하고 있으나, 방법론의 대부분에서 자국의 현실을 반영하여 그 절차와 세부 방법론을 정의하고 있다. 이러한 현실은 국내의 현실을 반영하여 적용하기에는 무리가 있다. 따라서 TTA의 표준 위험분석 방법론은 국내의 현실을 반영하여 적용된 위험분석 방법론이다. 그러나 TTA의 표준 위험분석 방법론에서는 몇가지 문제점을 가지고 있다.

첫째, 현재 TTA에서 제시하는 취약성 분석방법에서는 취약성의 유형을 제시하지 않고 평가자의 주관에 따라 정의하고 있다. 이러한 방법은 기관에 따라, 혹은 기관의 시스템에 따라 그 유형의 기준이 달라지게 되어, 비즈니스 프로세스를 고려한 시스템 사이에서도, 상대적인 취약성 분석 및 위험분석이 어렵게 되는 문제를 야기하게 된다.

둘째, 유형별 취약성과 자산별 취약성의 식별과 관찰을 동일한 관점에서 시작하지 않음으로 인하여, 식별된 각 취약성을 조직의 자산이 가지는 위험도에 반영하는함에 있어, 평가자의 주관이 많은 부분을 차지하게 된다. 즉 자산별 취약성 수준과 유형별 취약성 수준을 평가하고 수치화 시킬 수 있는 객관적인 기준을 제시하지 않아, 평가자의 주관에 따라 특정 취약성이 부각이 될 수 있으며, 특정 취약성은 무시될 수 있다.

셋째, 취약성의 등급 기준 및 수준 평가에 있어, 동일한 5등급의 취약성 수준 평가 기준을 제시하고 있다. 즉 TTA에서는 개별 취약성의 추상적인 등급을 제시할 뿐, 각 취약성이 가지는 보안요소(기밀성, 무결성, 가용성)의 측면에서 개별 취약성이 가지는 요소를 단단하여 평가할 수 있는 점이 부족하다. 또한 개별 취약성과 위협의 관계를 추상적으로 정의할 뿐, 하나의 자산에 대하여 각 위협과 취약성이 미칠 수 있는 위험도를 구체적으로 비교할 수 있는 방법을 제시하지 않고 있다.

넷째, 특히 취약성 수준 평가에서 중요한 A.L.E의 산출에서 중요한 E.F(Exposure Factor)의 산출 방식은 매우 정성적으로 표현하고 있다. TTA의 방법론에서는 사용되는 E.F.는 취약성 수준 산출과 연계하여 위험시나리오에서 자산-위협을 기준으로 대응책과 연관하여 산출하고 있다. 또한 E.F.산출시 사용되는 값은 중요도라는 평가자의 주관적 의견을 절대적으로 반영하고 있기 때문에 평가자의 의견에 따라 매우 편차가 커질 수 있는 문제가 있다. 현재 TTA에서 사용하는 E.F. 산출식은 아래와 같은 추상적인 형태로 표현되고 있다.

의의 수이다.

가정 2.

○취약점의 수준이 모두 n이면 VULNERABILITY_FACTOR는 0에 수렴한다.

가정 3.

○취약점의 개수를 정의할 수 없는 임의의 수이고, 취약점의 평가 수준이 모두(m+n-1)이면 VULNERABILITY_FACTOR는 1에 수렴한다.

이러한 가정하에서 각 취약성의 평가 수준은 아래와 같은 형태로 표현된다. $Effect(A)B$를 요소 B가 요소 A에 미치는 영향도라고 할 때, 환경적 취약성과 기술적 취약성의 수준을 취약점 평가값의 크기대로 내림차순으로 정리하여 나타낸 평가값의 집합을 $R(Vuln)$이라 하면

○취약점의 수 : $\{Vuln | Vuln \in \{0,1,2,3...\infty\}\}$

○취약점의 최저 평가 수준: $IR \in \{\{n\},\{n,n\},\{n,n,n\},...\infty\}$ 이고, $R(Vuln) \in IR$ 이면 위의 VULNERABILITY_FACTOR의 값은 0에 수렴하거나, 0으로 귀결된다.

○취약점의 최대 평가 수준: $IR \in \{\{(m+n-1)\},\{(m+n-1),(m+n-1)\},...\infty\}$이고, $R(Vuln) \in IR$ 이면 위의 VULNERABILITY_FACTOR의 값은 1에 수렴하거나, 1로 귀결된다.

따라서 각 위협에 해당하는 VULNERABILITY_FACTOR를 평가하는 값은 아래와 같이 표현될 수 있다.

〈표 7〉 VULNERABILITY 평가식

VULNERABILITY_FACTOR per One Threat

$$= \sum_{i=1}^{v} \frac{R(i)-n}{m^i} \quad \text{.... (A)}$$

<증 명>

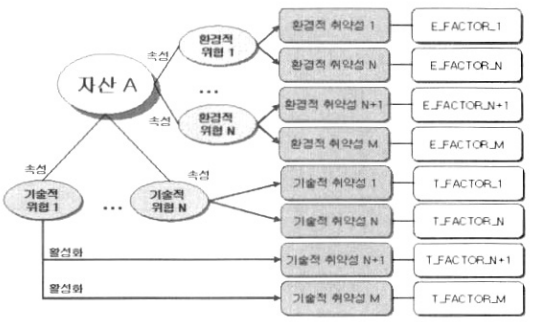
○현재 본 방법론에서 제시하는 위협의 분류등급을 고려하여, m은 $m \geq 9$의 범위에 있는 정수를 가지고 변화한다고 가정하며, n은 $m \geq n \geq 1$의 범위에 있는 정수값을 가진다고 가정한다.

○평가식 A에서 $V \to \infty$ 일 경우, 위 평가식(A)에 대한 가정 (1)을 만족한다.

○취약점의 수준 평가식에서 최저 및 최대 평가수준을 증명하면.

(1) V = 1의 경우

VULNERABILITY_FACTOR $= \frac{R(v)-n}{m} \leqq \frac{R(v)-n}{m} + \frac{R(i)-n}{m}$의 값이 되고 이때, $(n) \leqq R(i) \leqq (m+n-1)$ 이 되므로 이식은 성립한다. ($\because$ $m \geq 9$의 범위에 있는 정수, $m \geq n \geq 1$의 범위에 있는 정수)



(그림 4) 자산과 위협, 취약성의 관계구성

(2) V = k의 경우 위 식이 성립한다고 가정하면, 위의 평가식 (A)는V=K+1의 경우에도 성립해야 한다.

즉 $\sum_{i=1}^{k} \frac{R(k)-n}{m^i} \leqq \sum_{i=1}^{k} \frac{R(k)-n}{m^i} + \frac{R(i)-n}{m}$ 에서 양변에 $\frac{R(k+1)-n}{m^{k+1}}$를 더하면, 위 식은

$\sum_{i=1}^{k+1} \frac{R(k+1)-n}{m^i} \leqq \sum_{i=1}^{k+1} \frac{R(k+1)-n}{m^i} + \frac{R(i)-n}{m}$이

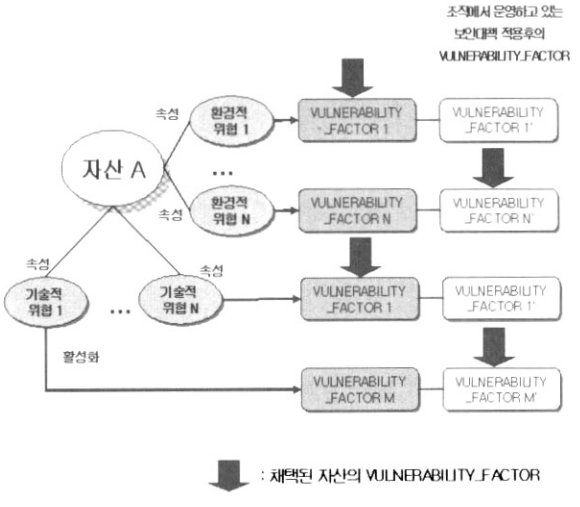
되고 $(n) \leqq R(i) \leqq (m+n-1)$이다.

따라서 V=K+1의 경우에도 성립하고, R(v) = {n, n, n, …}의 경우 가정 2가 성립한다.

(3) $R(\infty)$ = { (m+n-1), (m+n-1), (m+n-1), …}의 경우 VULNERABILITY_FACTOR = $\lim_{k \to \infty} \sum_{i=1}^{k} \frac{R(i)-n}{m^i}$ = 1이 되어 가정 3이 성립한다.

이러한 과정을 거쳐 생성된 VULNERABILITY_FACTOR는 각 자산의 환경적 위협과 기술적 위협이 자산에 미치는 영향력을 결정하는 하나의 요소로 적용된다.

각 결정요소는 조직에서 운영하고 있는 보안대책의 효과를 적용할 경우, 그 값이 변경되는데, 이는 아래의 그림에서 확인 할 수 있다.



(그림 5) 보안대책 적용후의 취약성 영향도 산정

$$E.F. = (\sum_{i=1}^{m} C_i W - \sum_{i=1}^{n} C_i W) \div \sum_{i=1}^{m} C_i W$$

$C_i W$: 자산-위협별 전체 대응책의 중요도 합

$C_i W$: 자산-위협별 실시 대응책의 중요도 합

4. 정량화를 위한 위험분석 방법 제안

4.1 위협의 식별 및 평가

제시하는 위험분석에서는 반드시 자산 가치 평가에 조직의 비즈니스 프로세스를 기준으로 업무 영역 분류를 통한 유형자산 가치 분석과 무형자산 가치 분석을 수행하도록 한다.

특히 자산의 가치 평가시 유의해야 할 부분은 조직의 비즈니스 프로세스와의 연관 관계를 통하여 분석하여야 한다는 점이다. 해당 자산이 조직의 주요 비즈니스 프로세스와 연관될 경우, 조직에서 자산이 차지하는 실질적인 가치를 평가할 수 있다. 이러한 관점에서 조직의 비즈니스 프로세스를 아래와 같은 형태로 분류하여 자산 가치 산정에 반영하도록 한다. 본 논문에서는 비즈니스의 프로세스를 3단계 레벨로 평가하기로 한다. 그러나 이 레벨은 평가자에 따라 그 값의 범위를 정하여 사용할 수 있다.

〈표 3〉 비즈니스 프로세스 중요도를 고려한 등급 산정

비즈니스 프로세스 중요도	레벨	비즈니스 프로세스의 중요도 산정 기준
핵심적 비즈니스 프로세스	LEVEL 3 LEVEL 2 LEVEL 1	조직에서 동일한 성능 및 기능으로 제공될 수 있는 다른 비즈니스 프로세스가 작동하지 않을 경우, 조직의 업무에 심각한 영향을 미치는 정도로서 프로세스의 복구비용이 높은 프로세스
중요한 비즈니스 프로세스	LEVEL 3 LEVEL 2 LEVEL 1	조직에서 짧은 시간 동안 다른 시스템의 기능으로 대체될 수 있으나, 반드시 복구되어야 하는 프로세스
일반 비즈니스 프로세스	LEVEL 3 LEVEL 2 LEVEL 1	조직에서 장기간 동안 다른 시스템의 기능으로 대체될 수 있으나, 추가적인 프로세스 처리비용이 소모되는 비즈니스 프로세스

위에 근거하여 위협과 취약성의 평가는 아래와 같이 이루어진다.

㉮ 환경적 위협의 수준

〈표 4〉 환경적 위협의 수준 평가식

FEnv(조직의 통계자료, 비즈니스 프로세스에 미치는 영향)
= [ENV_VALUE(LEVEL1,PRORITY),
ENV_VALUE(LEVEL2,PRORITY),
ENV_VALUE(LEVEL3,PRORITY)]

- ENV_VALUE : 피 평가 조직의 환경 가치
- PRORITY : 비즈니스 프로세스 중요도

㉯ 기술적 위협 수준

〈표 5〉 기술적 위협의 수준 평가식

FTech(조직의 발생 빈도 통계자료, 비즈니스 프로세스에 미치는 영향)
= [TECH_VALUE(LEVEL1,PRORITY),
TECH_VALUE(LEVEL2,PRORITY),
TECH_VALUE(LEVEL3,PRORITY)]

- TECH_VALUE : 피 평가 조직의 기술 가치

㉰ 위험분석 대상이 되는 조직의 각 자산에 미치는 위협과 취약성 영향

〈표 6〉 취약성 영향 평가식

EFFECTAsset =
FUNC(ASSET_VALUE, FEnv(조직의 통계자료, 비즈니스 프로세스에 미치는 영향),
FTech(조직의 발생 빈도 통계자료, 비즈니스 프로세스에 미치는 영향),
VULNERABILITY_FACTOR)

- EFFECT : 특정 자산에 미치는 위험도의 영향
- 함수 FUNC : 특정 인자를 입력받아 산출되는 자산의 위험도 산정함수
- ASSET_VALUE : 피 평가 조직의 자산 가치
- VULNERABILITY_FACTOR : 식별된 위협의 평가 수준

4.2 취약성 분석과 위험도 계산

위의 평가식 중 EFFECTAsset 의 VULNERABILITY_FACTOR는 취약성의 식별과 분석을 통하여 산출된다.

(그림 4)를 살펴보면 위의 취약성 평가 기준으로 산출된 각 취약성에 대하여, 그 영향을 산정할 수 있는 VULNERABILITY_FACTOR를 산정할 경우, 그 값은 하나의 위협에 대한 취약성의 전체 VULNERABILITY_FACTOR 값의 총 합으로 표현될 수 있다.

이는 아래와 같은 가정을 가진 식으로 표현할 수 있다. 아래에서 표현되는 변수 중 전체 취약성의 등급 총 개수를 m등급이라고 하고, 각 등급은 양의 정수 평가값을 가진다고 가정한다. 또한 등급의 최저값을 n이라고 한다. 이 경우 분류된 취약성 등급의 최대값은 (m+n-1)로 표현될 수 있다. 또한 본 방법론에서는 위협과 취약성의 일관성을 위하여, 동일하게 비즈니스 프로세스를 고려하여 분류를 수행하고 있다. 따라서 현재 본 방법론에서 제시하는 위협의 분류 단계인 3등급을 적용할 때, $m \geq 9$의 범위에 있는 정수를 가지고 $m \geq n \geq 1$의 범위에 있는 정수값을 가지고 변화값을 적용한다.

가정 1.

○조직의 자산에 존재하는 위협에 대한 취약성의 개수는 임

위의 그림과 같이 특정 조직의 시스템 위험분석 평가자가 선정한 VULNERABILITY_FACTOR를 선별한 후, 이를 이용하여 각 자산의 위험도를 산정하고, 평가 결과에 반영하도록 한다.

위에서 채택된 VULNERABILITY_FACTOR가 위험분석 평가 대상조직의 관리자가 수용할 수 있을 때까지 반복하여, 이에 대한 결과를 산출하도록 한다.

이러한 값을 모두 산정하여 산출된 조직의 각 자산별 특정 위험도 값은 아래의 식과 같이 표시될 수 있을 것이다.

〈표 8〉 자산별 특정 위험도 계산

$$RISK\_VALUE = \sum_{i=1}^{NmOfAst} \sum_{i=0}^{NmOfTht} FUNC(ASSET\_VALUE,$$

FEnv(조직의 통계자료, 비즈니스 프로세스에 미치는 영향),
FTech(조직의 발생 빈도 통계자료, 비즈니스 프로세스에 미치는 영향),
VULNERABILITY_FACTOR)

- NmOfAst : 위험분석 대상 조직의 위험분석 대상 자산의 개수
- NmOfTht : 위험분석 대상 자산에 대한 환경적, 기술적 위협의 개수
- EFFECT : 특정 자산에 미치는 취약성의 수준 및 영향
- 함수 FUNC : 특정 인자(취약성과 관련된 정보)를 입력받아 산정하는 자산에 대한 취약성의 영향도 함수
- ASSET_VALUE : 피 평가 조직의 자산 가치
- VULNERABILITY_FACTOR : 식별되고 선택된 취약성의 평가 수준

5. TTA 위험분석과 비교분석

5.1 위협 분석 비교분석

기존 TTA의 방법론을 따를 경우, 위협의 영향도가 가지는 함수는 아래와 같이 표현될 수 있다.

〈표 9〉 TTA의 위협의 영향도

$F_{tta}(Threat) = m \times x$

m : TTA방법론에서가지는
위협분석평가계수$(0 \leq m \leq 120)$

x : TTA방법론에서식별된위협

새롭게 제시되는 위협의 영향도는 개별 자산 가치에 영향을 받기 때문에, 그 영향도의 변위는 아래와 같이 표현될 수 있다.

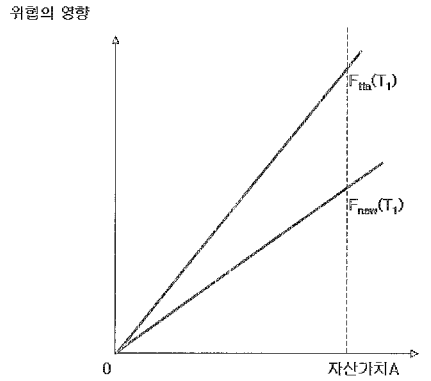
〈표 10〉 제시된 위협의 영향도

$F_{\neq w}(Threat) = m \times x$

m : 기존TTA방법론의
위협분석평가계수$(0 \leq m \leq 1)$

x : 제시된위협분석(TTA방법론)
에서식별된위협

위의 두 가지 위협분석 방법론에 따라, 개별 위협에 대한 위협의 영향도에서 발생할 수 있는 편차는 아래의 그래프에서 확인할 수 있다.



(그림 6) 방법론에 따른 위협의 영향도 비교

제시한 위협의 영향도 산출법은 위협의 손실가치와 관련되는 취약성의 관계쌍으로 정의되어, 기존의 TTA에서 제시하는 위협 영향도 산출법보다 상대적으로 매우 작은 편차를 보이게 되어, 위험분석 평가자의 주관에 따르는 영향을 최소화시킴을 확인할 수 있다.

5.2 취약성 분석과 위협별 위험도 산정 비교분석

TTA의 경우 위협의 1회 손실 가치를 계산하면 아래와 같다.

〈표 11〉 TTA 경우, 위협의 1회 손실 가치

$SingleEffect\ Value_{byThreat} = m \times n \times Asset\ Value$

m : 위협의심각도$(0 \leq m \leq 20)$
n : 관련취약성의등급$((0 \leq \lfloor x \rfloor \leq 5)$: n은정수)
$Asset\ Value$: 위협에 의하여영향을 받는자산의가치

본 논문은 각 프로세스의 레벨을 3단계로 평가하였기 때문에 1점~9점가지 적용하여 구성할수 있다. 또한 평가된 등급을 이용하여 각 위협별 취약성의 영향도를 아래의 평가식으로 산출할 수 있다.

$I(A)B$를 요소 B가 A에 적용시키는 위험 영향값이라고 하고, 각 위협에 해당하는 취약점의 수준을 내림차순으로

적용한 값을 $\{R(V)\}$라고 할 때, 각 위협에 해당하는 취약성의 영향도를 평가하는 값은 아래와 같이 표현될 수 있다.

〈표 12〉 취약성의 영향도

$$\text{VULNERABILITY\_FACTOR per One Threat} = \sum_{i=1}^{v} \frac{R(i)-1}{9^i}$$

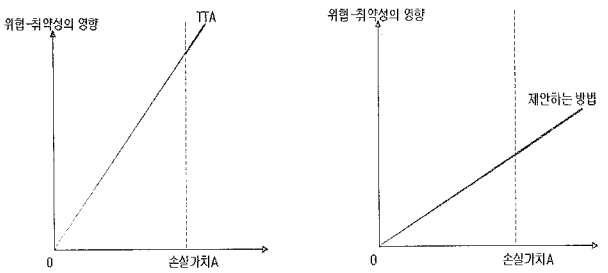
새롭게 제시되는 위협별 1회 손실 가치는 아래와 같이 표현할 수 있다.

〈표 13〉 제안된 위협별 1회 손실가치

$$Single Effect\ Value_{by\ Threat} = \sum_{i=1}^{v} \frac{R(i)-1}{9^i} \times Asset\ Value$$

n : 위협과관련되어식별된취약성의전체갯수

$Asset\ Value$: 위협에의하여영향을받는자산의가치



(그림 7) 위협-취약성에 따른 손실가치 비교

기존 TTA의 방법과 새로운 취약성 식별 및 영향도 분석 방법을 적용할 경우의 차이는 위의 그래프와 같이 나타난다. 기존 TTA의 방법론에 의하여 변화할 수 있는 영역이, 제안하는 논문의 방법보다 큼을 직관적으로 확인할 수 있다.

6. 결 론

기존 방법론은 위험분석 수행과정에서 취약성 분석과 위협 분석을 수행할 때에 평가자의 주관이 강하게 개입될 수 있다. 즉, 동일한 취약성과 위협을 보고 평가자마다 그 가중치를 다르게 줄 수 있는 범위가 크다는 의미이다. 이렇게 평가자의 주관이 강하게 개입되면서 위험도 또한 여러 종류로 계산될 수 있으며, 결과적으로 생성되는 보호대책의 정확도가 감소될 수 밖에 없다. 필수적인 사항이 보호 대책에서 제외되어 심각한 취약점이 위협에 악용 될 수 있으며, 중요도가 떨어지는 위협 및 취약성에 대한 보호 대책이 강조 될 수 있는 것이다.

따라서 본 논문은 취약성 분석 및 위협 분석 수행 시에 평가자의 주관 개입을 최소화함으로써 어떤 평가자가 수행하더라도 그 결과의 내용이 객관적이고 정량화되어 있다. 평가자의 주관이 최대한 배제되었기 때문에 생성되는 보호대책 또한 큰 영향을 발생시킬 수 있는 취약점을 중심으로 수립될 수 있는 장점이 있다.

본 논문은 정규화 된 식과 그래프의 형태를 가지고 TTA 방법론과의 비교 분석을 하였다. 향후, 각 방법론에 대하여 실제 위험분석의 경우에 대하여, 구체적인 평가 값과 그 영향을 비교하여 정규화 된 식을 증명하는 연구가 진행되어져야 할 것으로 보인다.

정보보호의 중요성이 커지면서 위험분석에 대한 사람들의 관심 또한 증가하고 있다. 특히 우리나라는 정보통신기반보호법의 시행과 함께 국가적으로 주요 인프라 보호에 관심이 커지면서 위험분석 방법론이 각광을 받고 있다. 그러나 지금까지 개발된 위험분석 방법론들은 개발된 지 이미 많은 시간이 흘러 현재의 정보통신시스템에 부적합한 경우도 있으며, 이론적인 요소에 치우쳐 실제 환경에 적용하는 데에 어려움이 많은 것이 사실이다. 따라서 본 논문에서 제안한 위험분석 방법론은 이러한 시기에 현실 적용에 유리한 방법이며, 이를 기반으로 여러 특수성을 감안하여 새로운 방법을 연구하는 데에도 기초자료로 이용될 수 있을 것이다.

참 고 문 헌

[1] TTA, 공공정보시스템 보안을 위한 위험분석 표준 - 개념과 모델, TTAS.KO-12.007, 1998. 11.

[2] ISO/IEC TR 13335, 2000.

[3] British Standards Institution(BSI), BS7799, 1999.

[3] ISO17799-What is ISO17799(the ISO Security Standard)?, http://www.iso17799software.com, 2002. 8.

[4] Implementing BS7799 - A Blueprint.

[5] Where to find Consultants & Experties for ISO 17799 Worldwide, 2002. 8.

[6] How ISO17799 Work, http://www.gammassl.co.uk/bs7799/works.html, 2002. 8.

[7] David Brewer, Risk Assessment Models and Evolving Approaches,http://www.gammassl.co.uk/topics/IAAC.htm, 2000. 7.

[8] David Brewer, Easy Ways to Manage your Risk, http://www.gammassl.co.uk, 1999. 6.

[9] Gamma's Service, http://www.gammassl.co.uk, 2002. 8.

[10] GAO, Information Security Risk Assessment - Practices of Leading Organizations, GAO/AIMD-00-33, 1999. 11.

[11] GAO, Computer Security : Improvements Needed to Reduce Risk to Critical Federal Operations and Assets, GAO-02-

231T, 2001. 11.

[12] GAO, Homeland Security : A Risk Management Approach Can Guide Preparedness Efforts, GAO-02-208T, 2001. 10.

[13] GAO/AIMD, Information Security : Computer Attacks at Department of Defense Pose Infreasing Risks, GAO/AIMD-96-84, 1996. 5.

[14] i-SEC, http://www.i-sectesting.com, 2002. 8.

박 중 길

e-mail : jgpark@etri.re.kr

1986년 동국대학교 전자계산학과(학사)

1988년 서강대학교 전자계산학과(석사)

2002년 충남대학교 컴퓨터과학과(박사)

1988년~2000년 국방과학연구소 선임연구원

2000년~현재 국가보안기술연구소 책임연구원/팀장

관심분야 : 정보보호(컴퓨터보안, 네트워크보안)