네트워크 위험 분석 및 취약점 점검 방법에 관한 연구

A Study on the Methodologies to Assess Network Vulnerability

박원주, 서동일
한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀

Won-Joo Park(wjpark@etri.re.kr), Dong-Il Seo(bluesea@etri.re.kr)

요약

기업 네트워크 환경 및 인터넷상에서 발생할 수 있는 보안상의 취약점들은 악의를 가진 내외부의 공격자들에게 악용될 가능성이 있다. 이러한 상황은 기업으로 하여금 정보 자산의 유출 및 파괴 등의 물리적인 피해와 더불어 복구를 위한 인력 및 시간의 소요 등 금전적인 손해를 야기시킨다. 이에 정확한 네트워크 보안 위험을 분석하여 이러한 피해의 가능성을 사전에 파악하고, 예방할 수 있는 방안을 마련하여 최대한의 보안성을 확보하여야 한다. 본 고는 이를 해결하기 위한 네트워크의 보안 수준을 측정하고 분석할 수 있는 국내에서의 접근 방법론을 살펴보고, 적절한 평가 절차 및 평가 수행 방법, 점검 항목을 도출한다.

■ 중심어 : | 네트워크 보안 수준 | 취약성 평가 | 위험 수준 평가 |

Abstract

This paper proposes to analyze a security level about information property systems. This method uses objective and quantitative risk level assessment.

The method analyzes administrative, physical and technical aspects of information property system commonly. This method also uses administrative, physical and technical weights individually according to requirements security assessment purpose. And it shows risks weighting mean and importance of information property by graph. The most right and up systems in maps is prior to other systems. Also, Quantitative analysis presents more objective and efficient results for security level assessment of information system.

■ Keyword : | Network Security Level | Vulnerability Assessment | Risk Level Assessment |

I. 서 론

기업 네트워크 환경 및 인터넷상에서 발생할 수 있는 보안상의 취약점들은 악의를 가진 내외부의 공격자들에게 악용될 가능성이 있다. 이러한 상황은 기업으로 하여금 정보 자산의 유출 및 파괴 등의 물리적인 피해와 더불어 복구를 위한 인력 및 시간의 소요 등 금전적인 손해를 야기시킨다. 이에 정확한 네트워크 보안 위험을 분석하여 이러한 피해의 가능성을 사전에 파악하고, 예방할 수 있는 방안을 마련하여 최대한의 보안성을 확보하

접수번호 : #041110-003
접수일자 : 2004년 11월 10일
심사완료일 : 2004년 12월 08일
교신저자 : 박원주, e-mail : wjpark@etri.re.kr

여야 한다. 그러나 현재 실제 업무 환경에서는 보안조치(safeguard)를 적용할 때 네트워크의 보안 수준이 어느 정도 되며 (AS-IS), 또 어느 정도로 보안조치를 적용하여 보안 수준을 향상시켜야 할지 (TO-BE)에 대한 정확한 판단 기준이 없는 실태이다.

이를 해결하기 위하여 현재 네트워크의 보안 수준이 어느 정도 되는가에 대한 분석 평가를 할 수 있는 방법론을 구축하고 적절한 평가절차 및 평가수행방법, 점검항목이 필요한 실정이다.

II. 관련 연구

1. 정보시스템의 위험 분석

국내에서 정보 시스템의 위험 분석은 조직 자체에서 내부의 역량으로 수행되는 경우는 거의 없으며 다만 간단한 체크리스트나 취약점 분석 솔루션을 이용한 내부 시스템 점검이 대부분이다. 정보보호 기반 보호법의 법적 요구사항, 정보 보호 시스템의 구축, 보안 위협 등의 이유로 조직에서는 현재의 보안 수준을 측정하고 정책적 대안을 수립하고자 한다. 이를 위하여 정보보안 컨설팅을 발주하게 되고, 이때 컨설팅 업체에서 필수적인 모듈로 수행하게 되는 부분이 위험 분석이다.

현재 국내외 정보보호 인증체계(BS7799 및 KISA의 정보보호 관리체계 인증[ISMS])를 획득하기 위해서는 정보보안 정책 및 지침을 수립하고 조직 내 위험관리 현황을 심사원들에게 제출하여야 한다. 이를 준수하기 위해서 반드시 수행하여야 하는 것이 위험분석 단계이다.

2. 국내 위험 분석 방법론

위험분석 방법론은 보안관리를 수행함에 있어 IT자산, 위협, 취약성, 대응책을 중심으로 대상 IT조직 환경의 위험을 세부적으로 측정하는 절차와 기술을 말한다. 전 세계적으로 수많은 위험분석 방법론이 존재하며 국내 보안컨설팅 업계에서도 각자의 방법론을 개발하여 업무에 적용하고 있다. 위험분석 방법론의 선택의 문제는 적용하고자 하는 조직의 정보시스템 환경과 조직특성, 속해진 산업군에 따라 다양한 방법론을 검토해 볼 수 있으며 적정한 방법론의 선택이 중요하다. 국내의 위험분석 방법론은 크게 다음과 같이 분류할 수 있다.

표 1. 국내 위험 분석 방법론의 분류

구분	내 용
분석수준	- 기본적 접근 방법(Baseline Approach) - 상세 접근 방법(Detailed Approach)
측정방법	- 정량적 방법(*Quantitative Approach*) - 정성적 방법(Qualitative Approach)
분석도구	- 인력 조사 방법(Manual Approach) - 도구 활용 방법(Tool Based Approach)

분석 수준에 의한 접근방법은 위험분석을 기본적 접근방법과 상세 접근방법으로 구분한다. 그 이유는 대부분의 조직은 많은 정보시스템이 존재하며, 조직 내의 모든 정보시스템을 대상으로 동등한 레벨의 위험분석을 수행하려면 너무 많은 시간이 소요되고 효율성도 떨어지기 때문이다. 따라서, 위험에 많이 노출된 정보시스템과 사업측면에서 매우 중요한 시스템을 파악하기 위해서 정보자산 분석을 먼저 수행하고 자산 중요성 평가 결과에 따라 상세 위험분석 또는 기본통제 방식을 선별적으로 수행할 수 있다. 초기의 보안컨설팅에서는 대부분의 회사들이 개별 정보 자산에 대한 취약점분석을 중요시하고 위험분석에 대한 개념이나 지식이 부족한 편이었다. 이 시점에서는 기본적 접근방법을 많이 사용하였으며 시간이 지나면서 회사마다의 방법론이 축적되는 동안 두 접근방법을 정보자산 중요도에 따라 병행하여 사용하기도 하였으며 상세 접근방법만을 사용하기도 한다. 현재 네트워크 보안에 있어 자산 중요성 평가 결과에서 하위레벨의 평가를 받은 자산이라 할지라도 이 자산의 취약점으로 인해 주요 핵심자산에 심각한 유해를 끼칠 수도 있는 만큼 보안컨설팅 업체에서 수행되는 정보보호 기반시설 등의 위험분석에 있어서는 대부분의 경우 상세 접근 방법을 적용하고 있다.

정보 자산 분석의 경우 프로젝트 시간과 비용 등을 고려하여 정성적 방법을 많이 사용한다. 보통 각 산업 별 조직 특성에 맞는 자산 중요성 평가기준에 따라 3점 혹은 5점 척도를 사용하여 정성적 평가를 하게 된다. 반면 국내 사이트의 특성상 위험 분석이나 취약점 분석의 경

우 정확한 결과 수치에 따른 보고 및 수준관리가 필수적인 경우가 많으므로 각 회사의 방법론 및 조직의 특성에 따른 계량화 기법을 적용하여 정량적 평가를 사용하는 경우가 보통이다.

분석도구에 따른 구분은 위험분석 과정을 수행할 때 이를 보다 효율적이고 정확성을 높이기 위하여 사용되는 자동화 소프트웨어를 일반적으로 자동화된 위험 분석도구라고 일컬으며 도구별 특성 및 세대에 따라 다음과 같이 구분할 수 있다.

표 2. 분석 도구 활용의 세대에 따른 분류

1세대	위험분석을 방법론 기반의 문서로 진행
2세대	위험분석을 문서 기반 자체의 분석과정을 단순히 Tool Base로 수행
3세대	네트워크 스캐닝을 수행하고, 주기적으로 업데이트되는 취약점 보고와, 대응책 라이브러리 등의 도구 사용
4세대	위험분석 결과 대응책의 효과를 비교분석하고, 다른 네트워크상의 위험을 비교하며 시뮬레이션기법으로 분석하는 도구들의 사용

현재 국내에서는 대부분 1~3 세대로 구분된 범위 내에서의 위험분석을 진행 중이나 4세대를 지향한 위험분석도구에 대한 접근도 이루어지고 있다[1].

3. 국내 취약점 점검 방법론

국내 취약점 점검 방법은 크게 정보보호전문업체의 정보보호컨설팅 수행방법론이 대표적이며, 그 외에 금융분야의 정보통신 기반 시설을 대상으로 금융감독원의 취약점 분석 평가 체계와 한국정보보호진흥원의 정보보호 관리체계 인증 방법론이 있다.

3.1 정보보호전문업체의 정보보호컨설팅 수행방법

국내의 정보보호전문업체의 정보보호컨설팅 수행방법론을 살펴보면 국외의 BS7799, ISO17799, ISO13335, GMITS, OCTAVE와 국내의 정보보호관리체계인증방법론(ISMS, 한국정보보호진흥원) 등을 참고하여 자체 환경에 맞게 수정하여 개발한 것이 대부분이다. 각 방법론은 환경/현황분석에서부터 자산분석, 위협/취약성분석, 위험분석/평가, 보호대책수립/정보보호모델링, 정보보호정책/지침 등 체계 구현 및 사후 관리의 모듈로 구성되어 있다.

3.1.1 정보보호현황분석

네트워크 위험분석을 위하여 사전에 현황 파악 필요하며, 이 단계에서는 해당 조직의 환경과 특성을 올바로 파악하여 효과적인 취약점 점검을 수행을 하기 위해 조직의 정보환경을 분석하고 평가하는 환경 분석과 정보자산에 대해서 목록을 작성하고 중요성을 분류하는 자산분석으로 구분되어 진행된다.

3.1.2 취약성 분석

취약점 분석은 자산분석 단계에서 파악된 자산에 대한 위협과 자산이 가진 취약점을 관리적, 물리적, 기술적 단계로 진단하며 기술적 보안 측면에서는 네트워크 구조 분석, 트래픽 분석, 네트워크 장비 점검, 보안시스템 점검, 시스템 점검, 응용프로그램 점검, PC 점검, 모의해킹 등의 작업을 통해 현존하고 있는 위험을 도출하게 된다.

과거에 수행되었던 네트워크 보안수준 측정의 경우 보통 네트워크 장비의 보안 설정사항 점검을 수행하는데 그쳤었다. 하지만 제대로 된 네트워크 보안 수준 측정 및 위험분석을 수행하기 위해서는 네트워크 보안과 밀접한 관련이 있는 보안시스템, 시스템, 응용프로그램, PC 등까지도 병행하여 점검하여야 하며 이외에 네트워크 시스템의 운용환경이나 물리적 환경의 특수성을 점검하는 관리 및 물리적 취약점 점검이 수행되어야 한다.

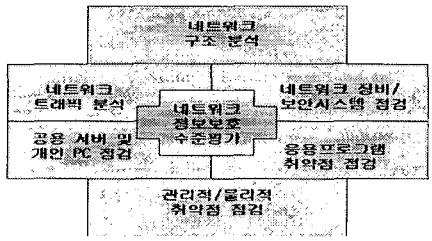

그림 1. 보안 수준 평가를 위한 취약점 분석 항목

취약점 분석 평가를 통해 현존하고 있는 위험을 도출한 후 진단결과를 분석하여 보안강화 방안 및 전체적인

보안대책을 수립, 제시함으로써 내/외부 위협에 대응할 수 있는 보안체계를 구현하게 된다.

3.1.3 국내 정보보호전문업체 컨설팅 방법론 비교

다음은 국내 대표적인 정보보안 컨설팅 업체의 방법에 대한 단계별 진행 흐름을 요약 비교한 것이다. 개별 모듈에 대한 분석 기법 등에는 차이가 있으나 위험 분석에 이르기까지의 큰 흐름은 대동소이하다[2].

표 3. 국내 정보보호 전문 업체 보안컨설팅 방법론 비교

A사	B사	C사
현황분석 -요구사항분석 -보안현황분석 -범위선정 위험관리 -자산분석 -위협분석 -취약성분석 -위험평가 -위험관리대상선정 정보보호모델링 -보안조직 -보안지침/절차 -정보보호체계수립 -마스터플랜수립 보안관리 -보안교육 -기술이전 -사후관리 -유지보수	환경분석 -업무현황분석 -자산파악 -진단 및 평가 기준 보완 정보보안관리 체계 수립 -관리체계 진단 계획 수립 -관리체계진단 -관리체계분석/평가 기술적취약점 진단 및 평가 -기술적 취약점 진단 계획 수립 -기술적취약점진단 -기술적취약점 진단 및 평가 마스터 플랜 수립 -이행과제 도출 -우선순위결정 -Roadmap 설정	환경분석 -환경분석 -자산분석 취약점분석 -통제평가 -모의 해킹 -기술적취약점점검 -로그분석 -물리적 보안점검 위험분석 -위험분석 및 선정 마스터플랜수립 -정보보호모델링 -마스터플랜수립 -보안정책/지침수립 -벤치마킹(BMT) 사후 관리 -침해사고대응 -인증지원 -보안감사 -보안교육

3.2 금융감독원의 취약점 분석 평가 체계

금융분야 정보통신기반시설 취약점분석 평가 작업은 정보통신기반보호법 시행령에 따라 취약점 분석/평가에 관한 기준을 정하였으며, 동 기준을 기초로 하여 금융감독위원회 소관 주요통신기반시설의 취약점 분석/평가에 필요한 세부기준을 제시하고 있다. 취약점 분석/평가라 함은 주요정보통신기반시설에 대한 요구 분석, 자산 분석, 취약성 분석, 위협 분석을 통해 해당 시설의 각종 전자적 침해행위 등 위협요인을 파악하고 위협요인에 대한 취약점 식별, 침해사고 발생시 영향 분석 및 기존 보호대책을 평가하여 적정 수준의 보호 대책을 수립하는 일련의 과정을 말한다.

취약점 분석/평가 절차는 전담반 구성, 취약점 분석/평가 계획 수립 단계, 요구분석단계, 범위선정단계, 자산 분석 단계, 위협분석단계, 취약성 분석 단계, 기존 보호대책 분석 단계, 위험 평가 단계, 보안대책 권고안 제시 단계 등 총 9단계에 걸쳐 진행되며 세부 모듈은 다음 [그림 2]와 같다.

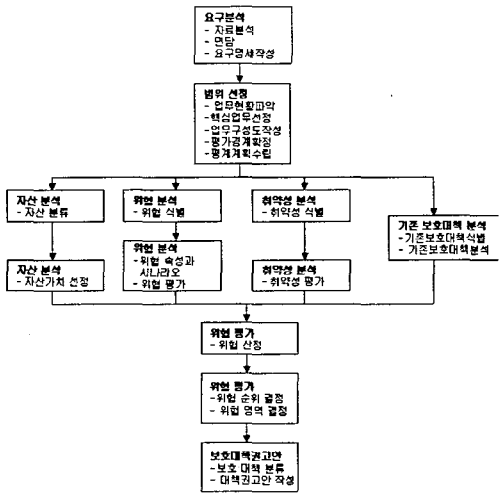

그림 2. 금융 분야의 취약점 분석 및 평가 절차

금융분야의 주요 주요정보통신기반시설의 취약점 분석 /평가 항목은 관리 및 운영적 항목과 기술적 항목으로 구분하여 제시하고 있다[3].

- 관리 및 운영적 항목

(1) 정보보호정책/지침
(2) 정보보호 조직편성 및 인사관리
(3) 정보보호 교육 및 훈련
(4) 외주운영/관리와 제 3자(Third party)통제
(5) 정보통신시스템 운영/관리 및 접근 통제
(6) 물리적 보안
(7) 정보보호시스템 운영/관리
(8) 비상 계획 및 복구 체계
(9) 침해사고 인지/판단/대응체계

• 기술적 항목

(1) 사용자 신원 확인 및 인증체계

(2) 네트워크 접근 메커니즘 및 이용 방식

(3) 저장매체의 자료 보호 및 접근 메커니즘

(4) S/W 불법 사용 가능성 및 존재

(5) 시스템 자원의 오용 가능성

(6) S/W 반입/반출 메커니즘

(7) 악성S/W 차단 메커니즘

(8) 전송데이터보호메커니즘 및 전자서명인증체계

(9) 전화 및 무선통신망 보호 메커니즘

(10) 전송 트래픽 통제 및 통신서비스 가용성 확보

(11) 전송 회선보호 및 메시지 전송 시 오류 제어 메커니즘

3.2.1 한국정보보호진흥원의 정보보호관리체계

정보 보호 관리 체계 (ISMS : Information Security Management System)는 정보보호의 목적인 기밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립하여 지속적으로 관리/운영하는 체계이며, 현재 정보통신부 정보 보호 관리 체계 의 요구사항을 기반으로 한국정보보호진흥원(KISA)에서 시행하고 있는 국내의 대표적인 인증제도이다.

ISMS는 PDCA(Plan-Do-Check-Act)를 반영한 체계로써, "정보보호 정책수립", "관리체계 범위설정", "위험관리", "구현", "사후관리"의 5단계로 구성된다.

먼저 기관의 정보보호 수준 평가 평가를 위해 정보자산 분류 및 식별과 각 자산의 중요도를 평가하고, 정보자산에 대한 위협과 취약성을 분석한다. 위험 평가 과정을 통하여 Unacceptable Risk와 Acceptable Risk 도출함으로써, 관리 대상의 위험에 대한 통제 사항을 선택하고 보안 대책을 구현한다. 마지막으로 정보 보호 관리체계 구축을 위한 계획 제시하고 지속적인 관리 및 검토를 수행함으로써 정보통신부 정보보호 관리체계 인증을 획득한다[4].

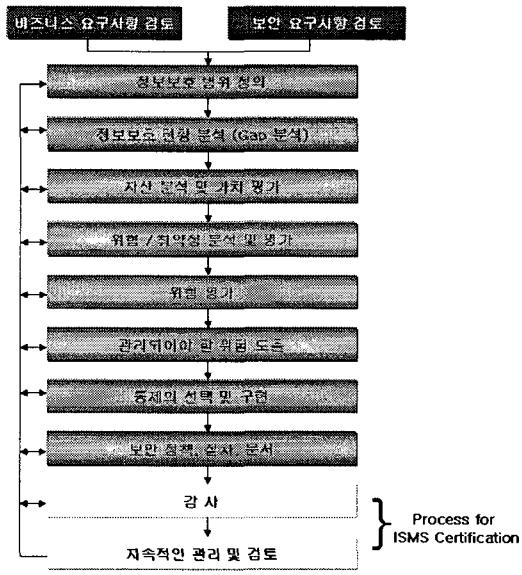

그림 3. ISMS 방법론

III. 네트워크 보안 수준 접근 방법

1. 효과적인 위험 관리를 위한 절차

기존의 위험 분석 및 취약점 분석 방법론들은 기술적인 영역과 관리적, 물리적인 영역을 총괄하여 위험을 집계하는 데에 한계성을 보이고 있다. 자산의 수가 많은 경우 수많은 정보 자산들에 대한 실사를 하는데 많은 시간을 소비하게 될 수 있으며, 조직에서 원하는 부분만을 따로 관리하기가 용이하지 않은 단점이 있다. 즉 A 기업은 주로 기술적인 취약점을 집중 관리 하고 싶은데, 물리적, 관리적 위험까지 모두 집계하여 산정하려면 매번 집계 및 위험 분석의 평가 시간이 오래 걸려 즉시성이 반영되지 않을 수 있는 단점이 있다. 특히 정보보호에 대한 보안조치를 처음 적용할 경우에는 관리적, 물리적, 기술적인 모든 영역의 보안을 골고루 향상시켜나가기에 어려운 점이 많다. 대부분 비인가 외부자로부터 해킹을 차단하는 것을 1차 목표로 둔 후, 추후 인가내부자, 인가외부자로부터의 위협을 막아나가는 것으로 보안조치의 적용 범위를 넓혀 나가는 것이 일반적이다. 이런 경우에 적합하도록 관리적, 물리적, 기술적인 영역을 유연하게 관리할 수 있는 방법론이 필요하다. 또한 보안조

치를 적용시켜나가는 단계별로 중요시하는 보안 영역을 지정할 수 있도록 하는 것이 보다 국내 현업 환경에 적합하다.

이에 조직의 정보 자산에 대한 위험 분석을 수행하는데 보다 객관적이고 정량적인 방법을 사용하여 효과적이고 효율적인 위험 관리를 할 수 있는 방법을 제시하고자 한다. 본 제언을 위해 수행되어야 하는 절차를 요약하면 [그림 4]와 같다.

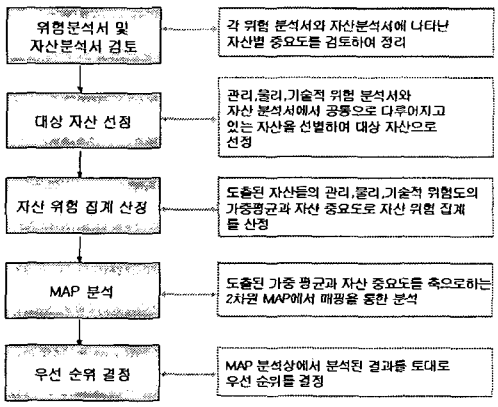

그림 4. 효과적인 위험 관리를 위한 절차

1.1 위험 분석 결과 및 자산 분석 결과의 Review

관리적/물리적/기술적 위험 분석 결과와 도출된 각 자산별 관련 위험도, 자산 분석 결과에서 나타난 각 자산별 중요도를 검토하여 "자산들의 목록"과 "각 자산별 위험 평가"와 "중요도 평가 내용"을 포함하여 정리한다.

1.2 대상 자산 선정

'가' 단계에서 파악된 자산들 중에 관리, 물리, 기술적 위험도 분석과 자산 중요도 평가가 공통적으로 모두 수행된 자산들을 도출하여 대상 자산으로 선정한다. 이러한 대상 자산의 선정과 분석을 위해 관리, 물리, 기술적 위험 분석시에 각 자산별로 상세하게 관리 부서, 물리적인 위치, 기술적 점검 내용 및 취약점이 도출되어 있어야 하고 이에 따른 위험 분석 이 사전에 이루어져 있어야 한다.

1.3 자산 위험 집계 산정

도출된 대상 자산들의 관리, 물리, 기술적 위험의 가중 평균과 자산 중요도를 자산 위험 집계 산출 공식에 따라 계산한다. 관리, 물리, 기술적 위험의 가중 평균을 구하기 위한 공식은 각 보고서에서 산정한 자산별 위험도(H, M, L)를 3점, 2점, 1점으로 환산하여 합산한 후에 가중치의 합으로 나누어 단순 가중 평균을 구한다. 식(1) 또한, 각 자산별 위험의 가중평균에 자산 중요도를 고려하여 평가하기 위해 자산 위험 집계를 식 2를 사용하여 산정한다.

위험의 가중평균
= (관리적 위험도 x W1 + 물리적 위험도 x W2
+기술적 위험도 x W3) / W1+W2+W3 … (1)

자산 위험 집계
= 자산별 위험의 가중평균 x 자산별 중요도… (2)

자산별 중요도는 1등급, 2등급, 3등급으로 평가되어 있는 것을 각각 3점, 2점, 1점으로 환산하여 자산 위험 집계를 구하는 공식에 적용하도록 한다.

1.4 MAP 분석

자산 중요도와 관리, 물리, 기술적 위험의 가중 평균을 축으로 하여 2차원 평면상에서 중요도 지수와 가중 평균 위험 지수의 mapping을 통해 분석한다. 위의 단계에서 구해진 위험의 가중평균을 X축으로, 자산의 중요도를 Y축으로 하여 자산별 MAP 분석을 실시한다. 예를 들어 A, B, C라는 시스템의 위험의 가중평균과 자산 중요도가 다음 표와 같다고 가정하고 MAP 분석을 하면 그림과 같다.

표 4. 시스템별 위험 가중평균과 자산 중요도(예)

구 분	시스템A	시스템B	시스템C
위험의 가중평균	M	L	H
자산 중요도	M	M	H

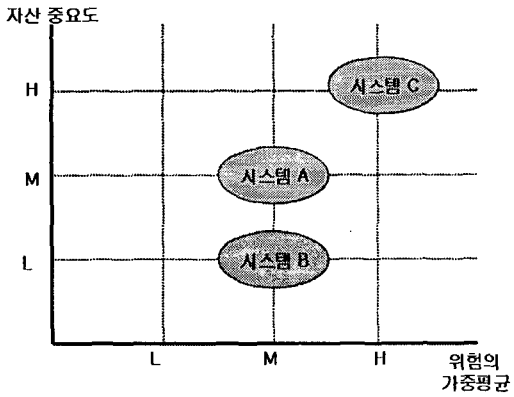

그림 5. MAP 분석(예)

1.5. 우선 순위 결정

MAP 분석을 통해 나타난 MAP 상의 위치를 토대로 자산 중요도와 위험의 가중평균을 고려하여 우측 상단으로 위치할수록 우선 순위를 높게 설정하게 된다. 위의 그림에서 보면 시스템 C가 가장 우선 순위가 높고, 그 다음으로 시스템 A, 시스템 B의 순으로 우선 순위가 결정된다. 위의 절차를 수행함으로써 각 자산에 대한 관리, 물리, 기술적 위험과 자산의 중요도를 종합적으로 반영할 수 있게 되고, 그 결과 선정된 자산별 보안 우선순위에 따라 조직 전반에 걸친 보안대책 구현의 방향성을 타진할 수 있다.

2. 위험 분석 결과의 활용 방안

본 고에서 제안된 자산 분석의 결과에 따라 중요 자산 등급별로 우선순위를 두어 보안조치를 적용시키면 보안에 대한 투자시 불필요한 투자를 막을 수 있다. 즉 중요한 정보가 담겨있지 않은 개인용 컴퓨터와 같이 상대적으로 중요등급이 떨어지는 자산에는 보안조치의 적용의 우선순위를 낮추고, 공용 서버와 같이 보안 우선 순위가 높은 시스템은 먼저 보안 서비스를 제공해 줌으로써 보안의 효율성과 효과성을 달성할 수 있다.

또한 주요 서비스 장비의 경우 운영자는 운영 정책을 performance를 최우선으로 할 것인지, 보안성을 최우선으로 할 것인지 고려해야 한다. 이 때, 자산 분석과 위험분석을 토대로, 중요도가 높은 자산들이 있는 위치의 경우 보안성을 우선적으로 고려한 운영정책을 가져가며, 중요성 등급이 낮은 자산은 performance를 우선적으로 고려하여 performance와 보안성의 균형을 잡을 수 있다.

IV. 결 론

최근까지 정보시스템 보안관리의 주요 활동으로 개별 정보시스템에 대한 취약점 분석 및 대책 수립이 주를 이루었으나 앞으로는 개별 취약점 분석활동을 통합한 위험분석 및 관리가 필수적인 보안관리 활동이 될 것이다. 아직까지 국내에서 위험 분석은 초기의 단계이다. 지금까지 많은 보안컨설팅 회사들이 외국의 모델을 토대로 각자의 방법론을 만들어 고객 사이트에 적용해왔다. 이런 위험 분석은 많은 비용, 인력, 시간 등을 투자해야 하는 프로젝트이므로 처음에 접근방법의 선택이 매우 중요하다.

앞으로, 위험 분석은 자동화된 도구를 활용하는 방법이 주축을 이룰 것이다. 아직은 최고의 수준이라고 할만한 자동화 도구가 개발되지 않았지만 많은 업체들에서 개발계획을 세우거나 활발히 개발 중에 있으므로 머지않아 위험분석 방법은 도구를 기초로 한 방법이 주를 이루게 될 것이다. 이러한 위험 분석 도구의 개발을 위하여 계속적인 취약점 분석활동을 통한 취약점 정보 DB의 축적과 이를 통제하는 활동이 선행되어야 한다. 또한 해외 방법론의 장점을 습득하여 국내 환경에 적합하게 개발된 위험분석 방법론을 개발하여 위험 분석 도구에 적용해야할 것이다.

본 고는 국내 외의 다양한 위험 및 취약점분석 방법론들을 살펴보고 효과적인 위험 관리 절차를 제시하고 이 때 수반되어야 하는 자산 위험도 산정 방법을 제안하였다. 또한 시스템별 가중 평균과 자산 중요도를 고려하여 MAP분석을 실시하여 우선순위에 따라서 보안 대책 방향을 타진해 볼 수 있는 방법을 제안하였다.

모든 보안은 "single point of failure"가 성립한다. 즉 관리자가 발견한 A 에 대한 보안조치를 적용했다 하더라도, 관리자가 미처 인지하지 못한 위험 B에 의해 침해사고가 발생하여 보안의 실패가 일어날 수 있다. 위

험 분석은 조직이 소유하고 있는 자산을 식별하고 이에 대한 보안 위협을 파악 평가하며 취약점을 분석한 결과로 도출된 위험에 대하여 이를 적절히 통제할 수 있는 대책을 세울 수 있는 근거를 제공한다는 점에서 네트워크, 시스템, 어플리케이션 등의 다양한 정보자산의 위험 및 취약점을 관리할 수 있게 하고 결과적으로는 보안의 효과성과 효율성을 달성할 수 있게 해준다는 점에서 유용하다 할 수 있겠다.

참 고 문 헌

[1] 박원주, 서동일, 김대영, "네트워크 보안수준 평가를 위한 위험 분석 방법에 관한 연구", 한국사이버테러정보전학회 춘계학술대회, pp.161~165, 2004.

[2] 박원주, 서동일, "국내의 네트워크 취약점 점검 방법론에 관한 연구", pp.127~131, COMSW 2004.

[3] http://www.fss.or.kr

[4] http://www.kisa.or.kr/isms/

저 자 소 개

박 원 주(Won-joo Park) 정회원

- 1998년 2월 : 충남대학교 정보통신공학과 졸업(공학사)
- 2000년 2월 : 충남대학교 정보통신공학과졸업(공학석사)
- 2000년 2월~현재 : ETRI 정보보호연구단 연구원

<관심분야> : 네트워크 보안, 컴퓨터 통신, 네트워크

서 동 일(Dong-Il Seo) 정회원

- 1989년 2월 : 경북대학교 전자공학과 졸업(공학사)
- 1994년 2월 : 포항공과대학교 정보통신공학과졸업(공학석사)
- 2004년 8월 : 충북대학교 전자계산학과졸업(이학박사)
- 1994년~현재 : ETRI 정보보호연구단 선임연구원

<관심분야> : 인터넷 정보보호, 컴퓨터 통신, 네트워크관리