주요 정보통신기반시설의 평가컨설팅 방법론에 대한 연구

A Study on the Evaluation Consulting Methodology of Important Information Communication Base Facility

이영로[1], 조재완[2]
Young Ro Lee, Jae Wan Cho

:Abstract

It soaks but 2001 July information communication base step law enforcement and the Enforcement Ordinance are published to follow, in order to support the establishment of evaluation and protective measure in order the vulnerability analysis against the facility of the agency which manages an important information communication base hour opinion to designate information protection specialty enterprise. As information protection specialty enterprise being revealed evacuation laboratory back 12 enterprises from information communication department become designation as the consulting enterprise and they do an enterprise activity actively. It follows in diffusion of the IT and information reconciliation level the other side where our country belongs in the world-wide first group, the research against the disfunction plan of preparation comparison the fact that law it is come negligently all actuality. The network as it will give management coat fatal effect even at obstacle occurrence hour of instant for of case and IT facility of the cyber transactions which leads, in the future there to be to corporate management, there is a possibility the stable civil official of information Facilities for communications very seeing in the portion which is important. Present condition and important propulsion contents of information communication base step law enforcement after, against a vulnerability analysis of information protection relation field and evaluation consulting methodological application situation to sleep it researches from the dissertation which it sees consequently and it does.

Key Words : **Enforcement Ordinance, vulnerability analysis, information protection, evaluation consulting methodological**

목 차

1) 한국정보사회진흥원 U-인프라구축단장, (02)2131-0601, lyr@nia.or.kr 2) 경동대학교 사회복지경영학부 경영학과 교수, (033)639-0346, jwcho@kl.ac.kr

Ⅰ. 서 론

정보통신기술의 적용이 일상화됨에 따라, 정보통신시설을 이용한 정보의 교환, 활용, 전자적인 거래 등은 활성화 되어 있는 반면, 내외부의 공격으로부터 정보통신시설을 보호하는 장치는 아직까지 취약한 것이 우리나라의 실정이다.

최근의 중국해커 들에 의한 정부 및 국가주요시스템의 해킹사례는 우리나라의 정보보호수준을 단적으로 설명해 주고 있으며, 앞으로 많은 연구와 적용이 필요함을 설명해 주고 있다.

정보통신기반보호법의 제정에 따라, 정부의 노력으로, 그동안 취약했던 우리나라 정보보호 관련 산업이 활성화 되어 왔고, 정부에 의해 주요정보통신기반시설로 지정된 시설에 대해서는 취약점 분석 및 평가를 통하여 사이버 보안을 강화하는 결과를 가져온 것으로 알려져 있다[3].

정보보호 컨설팅 전문업체는 국가적으로 중요한 주요정보통신기반시설에 대하여 취약점 분석 · 평가 및 보호대책수립을 지원하는 민간업체로서, 별도의 심사기준을 거쳐 정부가 지정[4] 하도록 되어있다.

이들 업체는 주요기반시설에 대한 안정적 운영과 동 시설에 내장된 중요 정보의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 전자적 침해행위 등 다양한 위협요인을 파악하고 이들 위협요인에 대한 주요정보통신기반시설의 취약점 침해 시 파급효과 및 대책을 식별 분석 평가하는 것을 담당하고 있다.

정보보호 컨설팅 전문업체는 이러한 역할을 수행하면서, 정부가 지정한 주요기반시설에 대해서 컨설팅을 제공함으로서, 시장참여기회가 주어져 왔다. 최근 이슈가 되고 있는 정보통신시설의 침해에 대비한 보호체계 구축과 취약점에 대한 사전적인 대비책을 강화하기 위해서는 우리나라도 표준화된 방법론에 대한 연구가 필요하며, 보급을 위한 노력이 필요하다.

이번 실증조사에서는 12개의 정보보호 컨설팅 전문업체에서 전문업체 지정 이후의 공공기관의 정보보호능력 향상을 위하여 적용하는 도구인 평가컨설팅 방법론에 대해 자세히 조사를 하고, 공통적으로 적용하는 절차와 모형에 대해서 연구하고자 한다.

Ⅱ. 정보통신기반시설 취약점 분석 및 평가 기준 현황

2.1 취약점 분석 및 평가 개요

정보통신기반보호법 제8조에 의하여 지정된 주요정보통신기반시설 관리기관의 장은 동법 제9조와 동법 시행령 제17조 내지 제19조에 따라 소관 시설에 대한 취약점을 분석 및 평가를 하도록 되어있다.

또한 주요정보통신기반시설의 안정적 운영과 동 시설에 내장된 중요 정보의 기밀성. 무결성에 영향을 미칠 수 있는 전자적 침해행위 등 다양한 위협요인을 파악하고 이들 위협요인에 대한 주요정보통신기반시설의 취약점, 침해 시 영향(피해규모 및 정도) 및 대책을 식별, 분석, 평가 하도록 하고 있다.

취약점 분석 및 평가를 통하여 주요정보통신기반시설에 대한 경제적(효과/비용)이고 실효성 있는 보호대책을 수립[5]하는데 필요한 정보의 제공이 가능하며, 결과적으로 효과적인 분야별 보호계획 수립 근거를 제공하고 있다. 주요정보통신기반시설을 관리하는 기관은 취약점 분석 및 평가를 위해서 별도의 전담반을 구성하여 소관 시설에 대한 취약점 분석 및 평가를 시행하게 하고 있으며, 분야별 일정 수준이상의 전문가를 확보하거나, 자체 전담반의 전문성을 보강하기 위해 필요한 경우 외부 전문기관 또는 기업에게 소관시설의 취약점 분석 및 평가를 의뢰하거나 그 지원을 요청하도록 하고 있다. 실제 대부분의 경우, 12개 전문업체[6]에 위탁하여 분석 및 평가를 하고 있다.

3) 정보보호방법론 현황, KISA, 2002. 12. 4) 정보통신기반보호법, 2001 5) 정보통신기반보호법 제5조 제1항 www.kisa.or.kr 2004년 6월 현재 6) 한국전산원, 2004년 7월 김성훈, 2003.12.

2.1.1 취약점 분석 및 평가 시기

관리기관은 2년마다 1번씩 정기적으로 소관시설에 대하여 정밀한 방식 에 의한 취약점 분석 및 평가를 시행하고, 이에 따라 적절한 보호대책을 수립하고 시행한다.

취약점 분석 및 평가를 수행하지 않는 연도에는 소관시설에 대하여 자체점검(간이 취약점 분석 및 평가)을 실시하고, 주요정보통신기반시설의 추가 및 변동 등 중요한 변화가 발생하거나, 중대한 사고가 발생한 경우에는 관리기관의 장의 판단 하에 수시로 자체점검을 시행하도록 하고 있다. 또한 일반적으로 주요정보통신기반시설로 새로이 지정된 경우에는 6개월 이내에 취약점 분석 및 평가를 하여야 한다.

2.1.2 취약점 분석 및 평가 절차

취약점 분석 및 평가 절차는 〈그림 1〉과 같다.

1단계: 전담반 구성, 취약점 분석 및 평가 계획 수립

2단계: 취약점 분석 및 평가 대상 선별

3단계: 위협 및 취약요인 분석

4단계: 기존의 보호대책 분석 및 취약점 평가

5단계: 보호대책 수립

〈그림 1〉 취약점 분석 및 평가 절차

가) 1단계: 전담반 구성, 취약점 분석 및 평가계획 수립

취약점 분석 및 평가를 수행할 전담반을 구성한다. 전담반은 정보보호책임자를 중심으로 주요정보통신기반시설 관리자 및 운영자와 정보보호에 전문성을 가진 자로 구성된다. 전담반은 취약점 분석 및 평가기준에 따라 소관 주요정보 통신기반시설의 취약점 분석 및 평가 수행방법, 점검항목, 절차, 기간, 소요예산 등을 포함한 취약점 분석 및 평가계획을 수립한다.

나) 2단계: 취약점 분석 및 평가대상 선별

2단계에서는 취약점 분석 및 평가대상 주요정보통신기반시설의 구성 및 업무내용을 확인하여 평가범위를 확인한다. 취약점 분석 및 평가와 이에 따른 보호대책 수립이 필요한 주요정보통신기반시설의 세부자산을 선별하여 그 목록 및 구성도를 작성하고, 각 자산별 중요도를 부여한다. 분류 항목으로는 물리적 자산, 소프트웨어, 정보/데이터, 인적자산, 무형자산 등으로 나눌 수 있다.

다) 3단계: 위협 및 취약요인 분석

주요정보통신기반시설에 실제 문제가 발생하였거나 또는 발생될 수 있는 위협요인을 식별하고, 각 위협요인별 발생원인, 빈도와 침해 시 영향 등을 분석한다.

정보통신기반시설에 발생할 수 있는 취약점을 식별하고, 소관시설의 특수성을 고려하여 취약점 점검항목을 마련한다. 식별된 취약점별로 그 존재 여부 및 취약성 정도를 확인한다. 자체적으로 운영중인 전담팀을 이용하거나, 정보보호컨설팅전문업체가 개발한 취약점 탐지도구 등을 이용하여 점검항목에 대한 취약점을 탐지하고, 탐지도구를 이용한 방법 외에 관리기관의 인적, 물리적, 관리적 체계 등의 취약점에 대한 구조적인 분석도 수행한다.

라) 4단계: 기존의 보호대책 분석 및 취약점 평가

위협요인, 취약점에 대한 기존 보호대책의 적정성, 효율성 및 문제점 등을 파악하고 분석하여 위협요인과 취약점과의 상관관계, 침해사고 발생가능성, 침해사고 발생시 조직에 미치는 영향, 새로이 필요하거나 보완되어야 할 보호대책(정보보호시스템 구축 포함)의 도출, 기존대책과의 연계성 등을 평가 한다.

마) 5단계: 보호대책 수립

취약점 분석 및 평가 또는 자체점검에 따른 보호대책 안 중에서 가장 효율적인 대책과 동 대책의 집행방법을 채택한다. 2년마다 실시하는 취약점 분석 및 평가 또는 자체점검을 토대로 주요 정보통신기반시설 보호대책을 매년 수립하고 시행한다.

2.2 취약점 분석 및 평가범위와 평가항목

2.2.1 취약점 분석 및 평가범위

가) 전자적 제어 및 운영시스템

사회기반시설을 직접적으로 제어 및 운영하는데 관계되는 시스템으로서 마비될 경우 사회기반시설이 제공하는 서비스가 중단되는 시스템을 의미한다. 그 예로서는 전력부문의 발전 및 송 · 배전시스템, 항공부문의 관제통신시스템, 항만부문의 항만운영정보시스템, 금융부문의 입 · 출금 · 이체관련 시스템, 통신부문의 망관리시스템 등이 여기에 해당한다.

나) 정보시스템

사회기반시설을 직접 제어 및 운영하는 시스템은 아니나, 마비 시 행정업무나 국민경제 등에 중대한 혼란을 초래하는 시스템으로서, 경영정보시스템, 철도 · 항공 · 통신 등의 예약 및 과금관련 시스템, 주민등록 또는 국세관련 시스템 등이 여기에 해당된다.

다) 통신시스템 (네트워크 장비)

교환기, 라우터 등 교환설비, 전송단국장치, 중계장치, 다중화장치, 분배장치 등 전송설비의 주요정보통신기반시설 보호와 관련된 관리 및 운영사항 으로는 첫째, 주요정보통신기반시설을 관리 및 운영하는 인력에 관한 사항, 둘째, 관련된 물리적 시설 및 환경에 관한 사항, 셋째, 시설 보호대책(정보보호시스템 포함)의 운용 및 시행과 관련된 사항이 있다.

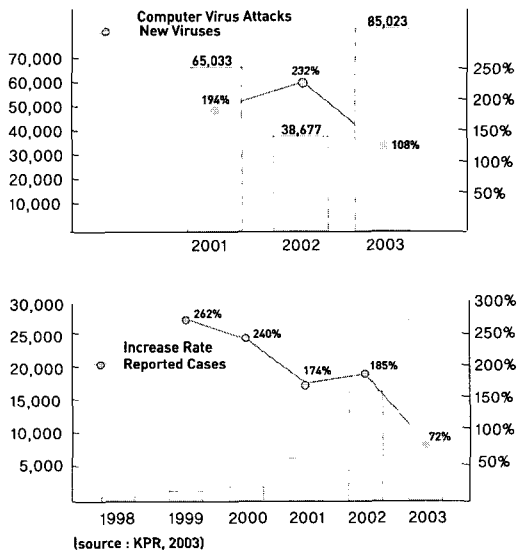
2.2.2 취약점 분석 및 평가항목

취약점 분석 및 평가 항목은 크게 기술적 사항 과 관리 운영적 사항으로 나눌 수 있다. 주요정보통신기반시설의 기술적 사항으로는 주요 정보의 기밀성을 보장하기 위한 메커니즘(암호화), 비인가자에 의한 네트워크 접근을 통제하기 위한 침입차단 및 침입탐지시스템 등 정보보호시스템의 설치에 관한 사항이 있으며, 서비스 제공자와 서비스 이용자간의 정보유통 시 송 · 수신자의 신원확인 및 송 · 수신 정보의 무결성 확보를 위한 공인 전자서명 인증체계 구축 등을 포함하고 있다. 우리나라의 주요정보통신기반시설의 관리 및 운영사항 은 주로 영국의 BS7799 등의 국내외 정보보호 관리표준을 참조하였으며, 시설 보호를 위한 전문인력 및 조직편성, 기반시설 보호에 관한 교육 · 훈련 등의 적정성, 시설 출입자의 통제, 침해사고 발생시 인지 및 판단 · 대응체계 등의 적정성 등을 다루고 있다.

Ⅲ. 기반보호시설 지정 현황

3.1 전자적 침해행위 사례의 증가

전자적 침해 행위로서는 해킹이 대표적인 사례이다. 우리나라의 해킹사례는 〈그림 2〉와 같이 해마다 큰 폭으로 증가하고 있으며, 2003년 한해에 약 25,000 건의 사례가 신고 접수되었고, 컴퓨터 바이러스는 85,023 건으로서 해를 거듭할수록 증가 하고 있다[7].



〈그림 2〉 우리나라의 해킹사례

7) 한국인터넷백서, 2004.

3.2 지정시설

현재 우리나라의 보호시설로 지정된 시설은 주요공공기관이 보유하고 있는 시설 이외에 정통신사업자 보유의 주요통신시설, 인터넷접속망, 무선인터넷망, 정보인증시스템, 금융 및 물류 시스템 등이 있는데, 이 시설들이 해킹을 당하여 시스템이 다운 될 경우 국가경영상 막대한 영향을 줄 뿐 아니라 경제적인 피해도 매우 크다 하겠다.

또한 관리기관이 필요하다고 인정하여 기술적 지원을 요청하는 경우 국가보안업무를 수행하는 기관의 장에게 우선적으로 요청하도록 하고 있다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가보안업무를 수행하는 기관의 장이 관계중앙행정기관의 장과 협의하여 기술적 지원을 할 수 있도록 규정하고 있다.

외교통상부(1개), 행정자치부의 정부고속망, 지방행정정보망(2개), 정보통신부의 자체통신망, 인터넷, 우정사업분야 등(17개)이 있으며, 통신망 분야에는 인터넷접속망(KT, 데이콤, 하나로통신), 무선인터넷망(SK텔레콤, SK신세기통신, KT프리텔, LG텔레콤), 초고속국가망(KT, 데이콤)등이 있고, 인터넷 분야에는 인터넷교환시스템(한국통신), 정보인증시스템(한국전산원, 한국정보인증), 인터넷주소자원관리시스템(한국인터넷정보센터), 전자서명인증관리시스템(한국정보보호진흥원), 보건복지부에는 국민건강보험공단, 국민연금관리공단, 건강보험심사평가원의 정보시스템 등(3개)이 있다.

그 외에 국가안전보장에 중대한 영향을 미치는 시설로서는 도로 · 지하철 · 공항 시설, 전력 · 가스 · 석유 등 에너지 · 수자원 시설, 방송중계 시설, 원자력 · 국방과학 · 첨단방위산업관련 정부출연연구기관의 연구시설 등이 있다.

Ⅳ. 방법론들에 대한 논의

4.1 취약점 분석 및 평가의 개념

취약점 분석 평가는 대체적으로 자산(Asset), 위협(Threat), 취약성(Vulnerability) 및 위험(Risk)의 관계를 나타낸다. 여기서 위험은 자산 · 위협 · 취약성의 관계가 있다고 한다.

여기서 자산(asset)은 조직 내의 가치를 갖고 있는 모든 것을 지칭하고, 위협은 시스템이나 조직에 피해를 끼칠 수 있는 원치 않는 사고의 잠재적 원인으로 정의되고, 취약성은 위협이 가해 질 수 있는 자산의 약점으로 정의되고, 위험은 이러한 여러 가지 위협요소가 발생하여 자산의 손실, 손상을 유발할 잠재성으로 정의 할 수 있다. 따라서 위험 분석과 취약성 분석은 차이가 있다고 할 수 있다. 즉, 위험 분석은 자산의 위약성을 식별하고 존재하는 위협을 분석하여 이들의 발생가능성 및 위협이 미칠 수 있는 영향을 파악해서 보안위험의 내용과 정도를 결정하는 과정이다. 반면, 취약성 분석은 네트워크 또는 서버기반의 스캐닝 툴을 활용하여 네트워크나 서버 등이 노출된 정보시스템의 취약성을 찾아내는 방법과 모의 해킹을 통해서 현재의 보안 상태를 점검하는 방법이다[8].

취약점 분석은 네트워크나 시스템의 결점을 기술적, 위험에 대한 대응만을 고려하지만, 위험분석은 취약점 분석 내용에 추가하여 조직의 사업의 목표와 임무를 수행하기 위한 자산의 가치를 고려하는 점에서 차이가 있다. 취약점 분석도구는 정보시스템 보안의 중요성이 대두되면서 계속 발전 보완되어 오고 있다. 초기에는 체크리스트를 이용하여, 간단한 설문을 함으로서 현재의 보안수준을 확인하였으나, 방법론의 개발, 자동체크 도구의 개발에 따라 최근에는 종합시뮬레이션까지 가능한 상태이다.

4.2 국외의 분석 및 평가 참조 모델

취약점은 자산이 지닌 잠재적인 약점을 말하며, 이 약

8) 조태희, 2002

점 자체가 직접적인 위험을 초래하지는 않지만, 위협에 의해 이용되어 위험을 발생시킬 환경을 제공한다. 취약점은 실시하는 대응책이 늘어날수록 감소하지만, 대응책 자체도 완벽할 수 없으므로 잠재적인 취약점을 지니고 있다고 보아야 한다.

일반적으로 국제적으로 통용되는 평가 방법론은 ISO의 13335 GMITS, BS7799(ISO17799), OCTAVE (Operationally critical threat, Asset, and Vulnerability Evaluation), NIST-Risk Management Guide for IT Systems 등이 있고, 취약점 분석과 관련된 항목을 보면 다음과 같다.

4.2.1 ISO 13335 GMITS

(Guidelines for the management of IT security)

가) 환경 및 기반시설

건물, 출입문, 창문의 물리적보안, 불안정한 전력, 홍수가능지역 위치 등을 뜻한다.

나) 하드웨어

주기적 교환계획 부재, 전압 및 온도 변화 민감성, 습기. 먼지 민감성, 자기장 영향 등 주로 하드웨어 장치에 미치는 환경적인 영향 등을 뜻한다.

다) 소프트웨어

개발자를 위한 불완전한 명세서, 소프트웨어 테스트, 복잡한 사용자 인터페이스, 인증 메커니즘, 감사(audit-trail), 소프트웨어 내의 오류, 보호되지 않은 password table, 잘못된 접근권한 할당, 악의적인 소프트웨어 다운로드, 로그아웃 관리, 백업부족, 저장매체의 삭제 없는 재사용 또는 폐기 등을 뜻한다.

라) 통신

도청가능성, 송수신자 식별부족, 암호화되지 않은 패스워드, 부적절한 네트워크 관리 등을 뜻한다.

마) 문서

보호되지 않은 보관, 폐기부주의, 통제 안 된 상태의 복사 등을 뜻한다.

바) 인력

보안인력 부재, 보안인식 부재, 정보시스템의 부정확한 사용, 감시체제 부재, 통신매체 사용부주의, 부적절한 고용절차 등을 뜻한다.

4.2.2 BS7799 (ISO 17799)

가) 직원 보안

직원 부재, 외부인 청소원 관리부재, 보안훈련, 문서화, 감시체제 등등 주로 인적보안에 대한 사항 등을 뜻한다.

나) 물리환경 보안

건물, 공간의 물리적인 접근. 통제에 대한 부적절하고 부주의 한 사용, 홍수 등 천재지변 가능지역, 저장소, 저장매체의 잘못된 관리, 주기적 교체, 외부 오물, 습기, 먼지, 온도, 전압의 변화에 부적절한 대응 등을 뜻한다.

다) 컴퓨터 및 네트워크 관리

보호되지 않은 통신 라인, 신분확인. 인증 메커니즘 부재, 메시지 전송, 수신의 증거 부족, 보호되지 않은 공개 네트워크 연결 등 주로 정보통신기기 사용에 있어서의 문제점 등을 뜻한다.

라) 시스템 접근제어 및 개발 유지

복잡한 사용자 인터페이스, 저장매체의 삭제 없는 폐기 및 재사용, 감사부재, 문서 부재, 신원확인 인증 부재, 불충분한 소프트웨어 테스트, 미비한 Password 관리, 개발자를 위한 불완전한 명세서, 접근권한의 잘못된 할당, 잘 알려진 소프트웨어의 결함등 주로 시스템 운용상의 문제 등을 뜻한다.

4.2.3 권고안 간의 관계

각각의 권고안별 주요내용은 차이가 거의 없으나, 다루는 내용의 강조점에 있어서 〈표 1〉과 같이 서로 상이한 부분이 다소 있다.

〈표 1〉 권고안별 주요내용

GIMITS	BS7799
1. 환경 및 기반시설	
2. 하드웨어	1. 직원 보안
3. 소프트웨어	2. 물리환경 보안
4. 통신	3. 컴퓨터 및 네트워크 관리
5. 문서	4. 시스템 접근제어 및 개발 유지
6. 인력	
7. 일반적으로 적용되는 취약성	

4.3 국내 전문업체의 방법론

정부의 정보통신기반시설지정에 따라, 우리나라도 국제적인 표준에 따른 취약점 분석 및 평가가 가능하게 되었고, 관련된 국제표준(권고안)에 근거한 민간기업의 자체 방법론의 개발이 활발하였다. 현재 우리나라에서 전문업체로 지정된 기업은 12개[9]로서, 〈표 2〉에서 보는 바와 같다.

〈표 2〉 우리나라에서 전문업체로 지정된 기업

구분	전문업체 명	비고
1차	마크로테크놀러지(주), 시큐아이닷컴(주), (주)시큐어소프트 등 8개 기업	1개 업체는 지정 취소(2002. 4월)
2차	(주)인포섹, 퓨처시스템 등 4개 기업	

대표적인 기업의 방법론은 개별회사별 홈페이지나 대외 발표 자료를 토대로 분석을 해 보면, 〈표 3〉에 나타나듯이 대부분이 유사함을 알 수 있으나, 세부 활동내역, 체크리스트 등에서 차이가 다소 난다. 또한 실제 적용 시에는 산업별 특성차이, 발주기관의 요청에 의한 수정 등이 일어나므로 상당부분의 커스터마이징을 통하여 적용되고 있다[10]

〈표 3〉 대표적인 기업의 방법론 차이

구분	방법론명	주요 특징 및 내용	비고
A 사	SSCM	· 3개 분야: 관리적보안, 기술적보안, 물리적보안 · 4단계 프레임워크 : 현황분석, 위험관리, 보안체계수립, 보안관리	
B 사	Cubic	· 4단계 프레임워크 : 현황분석, 보안설계, 보안구현, 보안관리 · 9개 모듈 : 위험분석, 취약점분석, 모의해킹, 체계설계, 보안감사 및 규정 적합성 검사, 보안정책개발 및 수정보완, 보안솔루션 벤치마킹 테스트, 보안교육, 보안관제시스템 설계 및 구축 (24개 프로세스를 조합하여 9개 모듈구성)	
C 사	I3P	· 5단계 프레임워크 : 착수단계, 업무분석단계, 위험분석단계, 대책수립단계, 종료단계	
D 사	TASCOM	· 6단계 프레임워크 : 환경분석, 위협/취약점분석, 위험분석, 마스터플랜수립, 구현, 사후관리	
E사	ISCM	· 5단계 프레임워크 : 현황파악, 위험평가, 체계설계, 구현, 이행지원	

V. 방법론의 적용

5.1 정보통신시스템에서의 추진방법론 설계

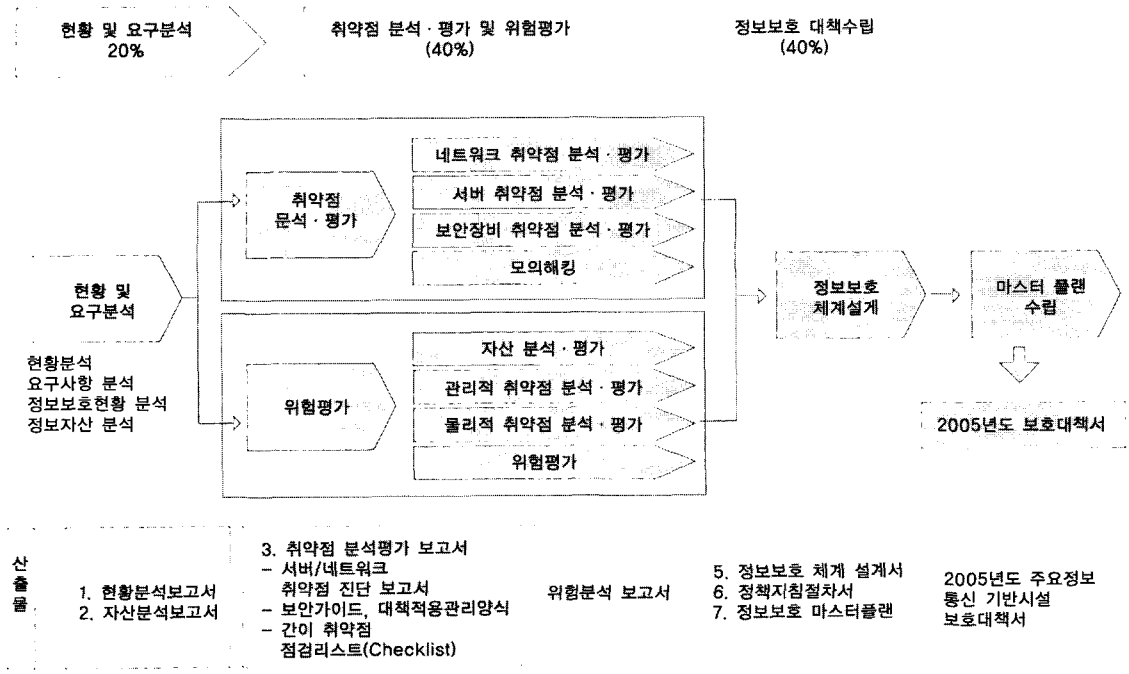
현재 적용되고 있는 방법론의 대부분은 정보보호컨설팅의 전체과정을 모듈화 하여 제공하고 있다. 따라서 정보통신분야 시설의 취약점 분석 및 평가에 한정하여 적용이 가능한 모델설계는 필수적인 부분만을 뽑아서 정리를 할 필요가 있고, 〈그림 3〉에서 보는 바와 같다. 여기서는 전체과정을 현황 및 요구분석, 취약점분석 · 평가 및 위험평가, 정보보호대책 수립의 3단계로 축약하여 표현하여 보았다. 그런 다음 각 단계별로 가중치를 정하여 전체 과정에서의 Work Load를 배분한다.

5.2 각 단계별 수행 내용

5.2.1 현황 및 요구분석

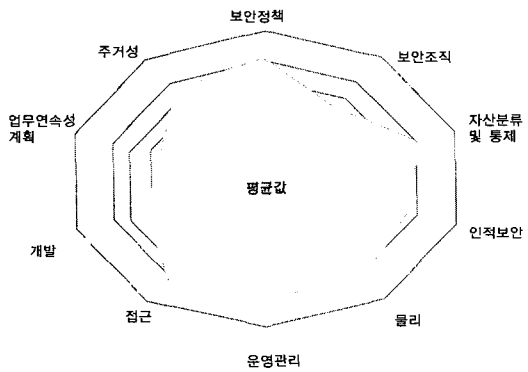
정보보호 관리체계에 대한 국제적 Best Practice인

9) www.kisa.or.kr, 2004년 7월 10) 김성훈, 2003.12.



〈그림 3〉 취약점 분석 및 평가 과정

BS7799의 10개 Domain을 기준으로 〈그림 4〉와 같이 정보보호 수준을 평가한다.



〈그림 4〉 정보보호 수준평가 모형(BS7799)

그 내용은 보안정책, 보안조직, 자산분류 및 통제, 인적보안, 물리적보안, 운영관리, 접근, 개발, 업무연속성 계획, 준거성 등으로 분류 하며, 각 항목별로 그래프를 그리고, 전체적인 관점에서 부족한 분야에 대해 쉽게 볼 수 있도록 하였다.

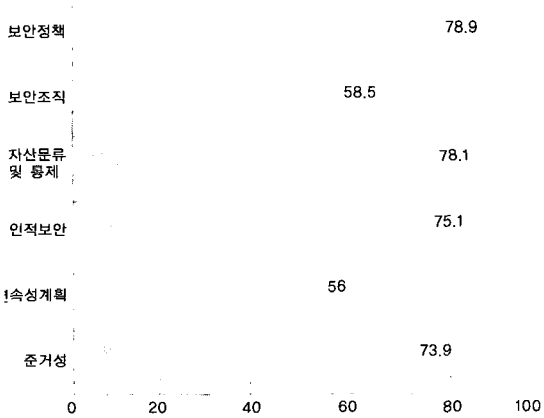
또한 그래프의 중심에는 전체평균점수를 기록하여 전체적인 보안수준을 알기 쉽도록 그린다. 각 항목별로 평균대비 낮은 분야에 대해서 집중적인 개선을 통하여 정보보호 수준을 향상시킬 수 있도록 한다. 일반적으로 평균 80점 이상의 수준을 목표로 추가적인 개선 노력을 하게한다.

점수대별 등급은 5단계로 하며, 등급1 (10~30): 전혀 보안위험에 대응하지 않는 수준, 등급2 (30~49): 일부 보안위험에 대응하나 명확한 기준 없이 임의로 대응하는 수준, 등급3 (50~69): 기본적인 기준 보유, 핵심 보안위험에 대응하는 수준, 등급4 (70~89): 보안위험을 측정, 관리하며, 대책의 계획 및 이행을 지속할 수 있는 수준, 등급5 (90~100): 지속적인 측정, 관리를 통해 새로운 위험도 대응할 수 있는 Best practice 수준으로 구분한다.

가) 관리적보안 영역

관리적보안 영역은 〈그림 5〉에서 보는바와 같이 보안정책, 보안조직, 자산분류 및 통제, 인적보안, 사업연속성계획, 준거성을 포함하고 있으며, 각각에 대해 수준평가를 한다. 보안정책 및 보안조직은 조직 내 내규 및 지침서가 어느 정도 구비되어 있는지를 나타내며, 보안조직이 구성을 통한 보안정책의 구성체계가 필요하고, 전사적인 보안조직 과의 연계 및 책임과 역할이 어느 정도 구체화되어 있는지를 보게 된다. 자산분류 및 인적보안은 자산의 중요도와 민감도에 따른 분류 및 통제가 잘 되어있는지를 나타내며, 기반시설 운영 및 담당자에 대한 보안기밀 준수여부, 정보보호에 대한 전문교육 시행 및 교육체계 등을 나타낸다.

업무 연속성 및 준거성은 기반시설에 대한 인프라 측면의 가용성 보장상태 , 업무연속성 계획에 대한 체계수립, 관련 규정 및 외부감사(을지훈련 등)를 준수 등을 나타낸다.



〈그림 5〉 관리적보안 영역 정보보호 수준평가 내용(예)

나) 기술적보안 영역

기술적보안 영역은 통신 및 운영 관리, 접근 통제, 개발의 3가지로 구분할 수 있는데, 시스템운영의 관리 및 모니터링, 기반시설의 가용성 보장을 위한 회선 및 장비의 이중화, 운영과 보안관리의 분리 등을 필요로 한다. 접근 통제는 시스템과 관리영역의 네트워크 분리 및 통제, 무결성 점검시스템(Tripwire) 구축 및 적용, 접근통제시스템 구축 및 적용 등이 되어 있는지를 나타낸다. 시스템 개발 및 유지보수는 신규시스템의 도입 및 업그레이드 시의 운영 측면에서 보안요구 및 검토 정도를 점검하고, 보안패치의 적용 등을 위한 테스트 환경이 잘 갖추어져 있는지에 대한 평가를 한다.

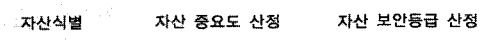
다) 물리적보안 영역

물리적보안 영역은 일반적 통제, 정보시스템기기보안, 보안구역 이 물리적 보안항목에 해당된다.

일반적 통제는 보안구역 설정과 연계한 물리적/환경적 통제 적용, 기반시설 관련 설비 및 자료에 대한 반 · 출입 관리의 적용 및 통제의 준수여부를 나타내며, 정보시스템 기기보안은 RF카드, 지문인식, 정맥인식, 무게인식 등 물리적 출입통제 설비의 적용 및 환경적 보안설비의 적용여부를 나타낸다. 보안영역은 보안 및 통제구역으로 구분되며, 대중화된 출입통제 적용, 보안 및 통제구역에 대한 출입통제의 관리 적용, 주요 정보통신기반시설 시스템의 내 · 외부 분리 관리정도 등을 나타낸다.

5.2.2. 자산분석

주요 정보통신기반시설의 정보자산에 대한 분석평가는 〈그림 6〉과 같이 자산식별, 자산 중요도 산정, 자산 보안등급 산정의 절차로 수행하여 보안등급별 보호 및 관리를 위한 근거자료로 활용한다.



〈그림 6〉 관리적보안 영역 정보보호 수준평가 내용(예)

첫 번째인 자산식별 단계에서는 정보통신기반시설의 자산을 용도별로 분류를 하는데, 보통 서비스 자산, 네트워크자산, 서버자산으로 나눈다. 서비스 자산으로는 각종응용 프로그램, 데이터, 응용서비스를 위한 정보자산을 포함하며, 네트워크자산은 주로 통신에 사용되는 라우터, 스위치, 방화벽, IDS/IPS 등이 포함되고, 서버

자산은 컴퓨터, 운영체계, 데이터베이스 등 서비스의 기반 환경을 이루는 서버장비를 포함한다.

두 번째 단계에서는 각각의 정보통신자산의 중요도를 산정하는데, 정보보호 3대 요소인 기밀성(confidentiality), 무결성(integrity), 가용성(availability)의 관점에서 분석을 수행한다. 또한 보조속성인MAO(Maximum available outage), 사용자수, 통신량(traffic), 복구시간(recovery time), 비용(cost), 영향(impact) 등으로 구분하여 중요도를 평가한다. 이러한 과정을 거쳐 최종적으로 1등급, 2등급, 3등급으로 자산을 분류하게 된다.

5.3 취약점 분석 및 위험평가

5.3.1 취약점 분석 및 평가의 절차

서버 취약점 진단대상 서버선정 기준은 정보통신기반보호법에 따라 주요정보통신기반시설로 지정된 서버와 지정예정 서버에 대해 취약점 진단을 수행한다.

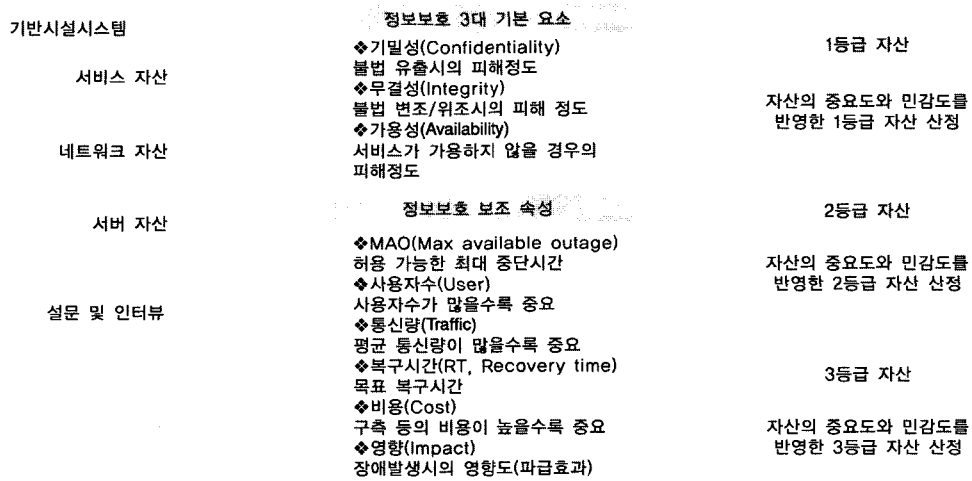
가) 모의해킹

기반시설에 대한 모의해킹을 위해서 먼저 해킹대상 서버를 선정한다. 선정된 서버에 대해 취약한 수준을 평가하며, 〈표 4〉와 같이 5단계의 평가기준에 따라 평가를 수행한다.

〈표 4〉 모의해킹 평가기준

등급	모의해킹 평가기준
안전(A)	보안에 취약한 문제점 발견되지 않음
양호(B)	내부망에서 일반사용자 권한으로 접근가능 일부 정보유출 가능
취약(C)	내부망에서 시스템권한(root)획득가능 외부망에서 웹 관리자 권한 획득가능
매우취약	원격에서 시스템권한(root) 획득가능
위험(E)	이미 해킹 당한 흔적 있음

안전(A)은 보안에 취약한 문제가 발견되지 않은 경우, 양호(B)는 내부망에서 일반사용자 권한으로 접근가능 수준의 경우, 취약(C)은 내부망에서 시스템권한(Root) 획득이 가능한 경우와 외부망에서 웹관리자권한 획득이 가능한 경우, 매우취약(D)은 원격에서 시스템 권한 획득이 가능한 경우, 위험(E)은 이미 해킹을 당한 흔적이 발견되는 경우를 나타낸다.



〈그림 7〉 주요 정보통신기반시설의 정보자산에 대한 분석평가

나) 서버의 취약성 진단

서버의 취약성 진단에는 보안 패치, 무결성. 가용성 진단, 인터넷웜 감염진단, 시스템 보안설정, 주요응용설정, 로그관리, 네트워크서비스, 파일시스템, 계정관리 등 9가지 사항에 대해 진단을 수행한다. 각각 항목에 대해서는 100점 기준으로 점수를 기록하고, 전체 평균값을 구한 후 아래와 같이 5단계의 등급기준으로 나누어 평가를 한다.

- 취약 (50이하) : 결점 및 취약성이 현재 매우 심각한 수준
- 미흡 (50~69) : 잠재적으로 높은 결점 및 취약성을 내포
- 보통 (60~79) : 보통의 결점 및 취약성을 내포
- 양호 (80~89) : 다소의 결점 및 취약성을 내포
- 우수 (90~100) : 취약점이 거의 없는 안전한 수준

서버(Unix, Windows)의 주요 보안 이슈로는 계정/패스워드 정책 강화, 시스템 디폴트 설정 수정, 로그관리/감사기능 설정 강화, 최신 서비스 팩/핫 픽스 등 보안 업데이트를 뜻한다.

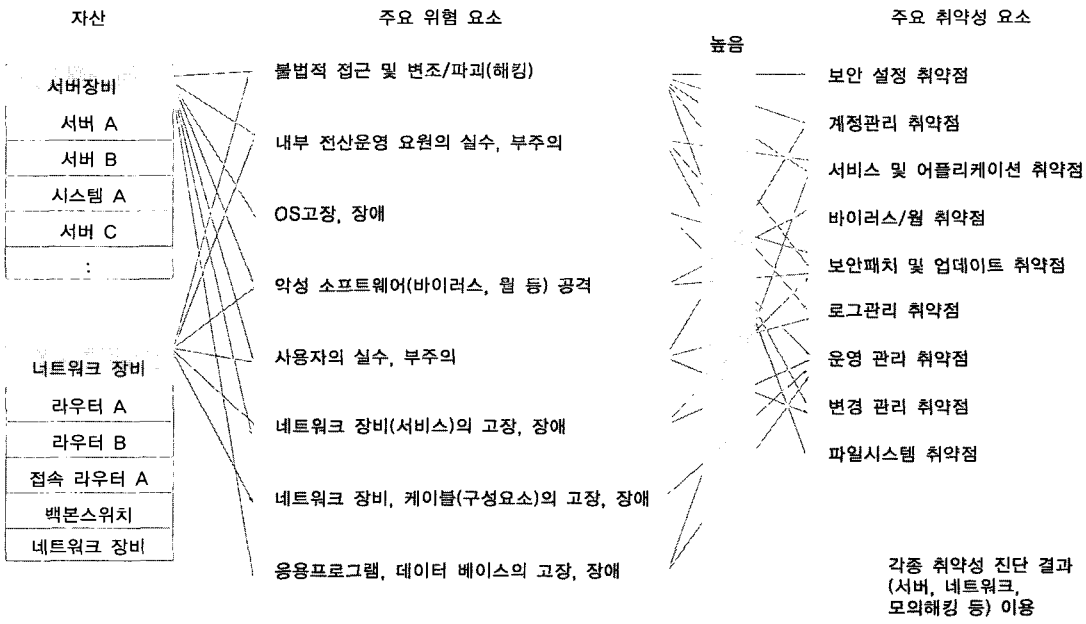
다) 네트워크의 취약성 진단

네트워크 취약점 진단항목은 보안관리, 로그관리, 원격관리, 계정관리 등 4개 항목으로 구분할 수 있다 .

각각의 항목 중에서 평균에 비하여 미흡한 항목에 대해서 집중적인 개선이 필요하게 된다.

네트워크 역시 상기 5단계의 평가 단계에 따라, 평가를 수행한다. 네트워크에서의 주요 이슈사항으로는 Enable Secret 사용, Username Login 사용, Encrypt Password 사용, IP Source Routing 제한, NTP Server 사용 시 추가적인 보안 설정 등이 있다.

또한 침입탐지 및 방화벽을 활용한 보안 이슈로는, 보안 정책에 대한 주기적인 유효성 검증 및 불필요한 Network Object 삭제, 변경관리(보안정책의 변경 시 보안성 검토 및 승인 등에 대한 관리강화 필요), 로그관리(별도의 백업 미디어를 통한 로그 보관 및 로그 점검에 대한 이행증적 유지, 침입 탐지 및 로그 분석에 대한 이행증적 유지, 원격 관리를 위한 IP Address 접근제어 설정, NetBIOS 서비스 제거, 관리자 IP 주소에 대한 접근제어 적용)등이 있다.



〈그림 8〉 위험분석 방법론(예)

5.3.2 위험분석

위험분석을 실질적이고 효율적으로 수행하기 위해서는 〈그림 8〉과 같이 위험 시나리오를 개발해야 한다. 위험 시나리오는 각 요소들(자산-위협-취약성)이 결합하여 실제로 일어날 수 있는 가상의 상황을 의미하는 것으로, 각 요소들에 대한 평가 값을 사용하여 위험 시나리오별로 위험 수준을 평가하며, 향후 침해사고 대응 시나리오에 대한 참고자료로도 사용한다.

5.3.3 위험분석 결과 및 대응책 선정

KIX의 주요 자산에 대해 위험 수준이 높은 시나리오들을 개발하고, 각 시나리오들에 대한 대응책들을 〈그림 9〉와 같이 선정한다.

5.4 대책수립

〈그림 10〉과 같이 각 항목별 위험 분석 결과를 종합하여 관리적, 기술적, 물리적인 대책을 수립하고, 공통적인 사항은 별도로 분리하여 대책을 수립한다.

우선 주요과제에 대한 개략적인 카테고리 작업을 수행한 후 각 카테고리별로 세부적인 사항에 대한 대책을 수립한다.

각 세부항목에 대해서는 별지를 이용해서 구체적인 추진방법, 자원투자계획, 일정계획 등 실행계획을 수립하여 최종 실행 가능한 형태로 작성을 한다.

Ⅵ. 결론 및 시사점

우리나라의 주요기반시설에 대한 보안대책은 기반보호법 제정이후 보호시설로 지정된 주요시설을 중심으로 자체 혹은 외부의 컨설팅을 받아서 추진되고 있으며, 정보통신시설의 기본적인 보호대책은 갖추어진 것으로

자산유형	위험(위협-취약성)시나리오	위험	대응책 선정
	위험 시나리오	위험	ICMP Redirects 기능의 제한 설정
네트워크 장비	악의적인 목적으로 라우팅 경로를 수정, 이용할 가능성 있음	7	IP Source Routing 기능의 제한 설정
라우터 A	IP Source Routing을 통해 내부 네트워킹 경로를 파악하여 Routing 되지 않는 중요 Server로의 비인가된 접근 가능성 있음	7	Username Login 사용에 따른 ID/PW 입력 방식의 한층 강화된 로그인 절차로 접근제어
라우터 B	User Mode로의 접근시 Login Password만을 사용한 인증 방식은 Password크랙을 통한 침입 가능성이 있음	7	잘못된 로그온 시도(5회)에 대한 계정 잠금 설정 및 잠금 유지 기간(60분) 설정
시접속 라우터	취약성이 알려진 Setuid, Setgid 설정 파일이 존재하여 이를 이용한 침입이 가능함	8	최신의 보안 패치를 유지 할 수 있도록 해야함.
백본스위치	로그온 실패 횟수에 따른 계정 잠금 정책이 Default로 미흡하게 설정되어 있어 지속적인 공격이 가능함	7	사용하지 않은 취약성이 알려진 Setuid, Setgid 파일에 대해 Setuid, setgid 설정 제거
:	최신 보안 패치가 적용되어 있지 않아 최신 공격에 대한 대비가 미흡함	7	사용자 교육 및 (비)정기적 점검
서버 장비	비인가된 사용자가 Null Session을 통해 사용자 인증을 거치지 않고 서버에 접근 가능함	8	레지스트리 값 수정 및 포트 차단을 통한 외부로부터의 접근 차단
서버 A	일부 계정의 패스워드가 쉽게 추측가능한 것으로 설정되어 있어 지속적 공격이 가능함	8	계정과 동일하거나 유사하지 않은 6자 이상의 영문, 숫자, 특수문자의 조합으로 암호 설정
서버 B			
시스템 A			
:			

〈그림 9〉 위험분석 및 대응책 선정과정(예)

영역	주요과제	세부과제	단기적 발전
관리	1 정보보호 정책 · 지침절차 제 · 개정	1-1 전산원 보안 내규 반영 및 기반시설 정책의 규정화 1-2 정보보호 정책 · 지침절차/매뉴얼의 체계화 1-3 정보보호 정책지침의 관리 및 유지계획 수립	주기적인 갱신 및 검토
	2 정보보호 조직강화	2-1 보안조직 재구성(CERT) 2-2 보안조직 역량강화 계획수립(역할/책임, 활동강화) 2-3 보안 전문인력 충원	지속적 강화
	3 기반시설 정보자산 관리체계 수립	3-1 정보자산 관리체계 수립(가치평가 및 보안등급 선정) 3-2 정보자산 관리방안 마련	지속적 강화 (전문화)
	4 인적 보안 강화	4-1 기반시설 관련 비밀준수 강화 4-2 보안교육 수행계획(정보보호 전문교육	
	5 업무연속성 계획	5-1 침해사고 대응체계(비상계획) 강화 5-2 업무연속성계획의 개요 및 사례소개	단계적 확대적용
	6 준거성 강화	6-1 간이/자체 취약점 진단 방안 마련 6-2 취약점 진단도구(Scanner) 구축 6-3 내부 강사 계획 마련	

영역	주요과제		세부과제	단기적 발전
물리	7 물리적 출입통제 강화	A시설	7-1 기반시설 접근의 출입통제강화(시건, 별도영역구성) 7-2 물리적 출입통제의 보안관리 강화	지속적 강화 (개선사업)
		B시설	7-3 물리적 출입통제 보안관리의 지속적 강화	
기술	8 기반시설 보안 운영관리 강화		8-1 보안 운영관리 강화(기업의 역할과 임무) 8-2 보안 운영과리 강화(위탁운영시의 역할과 임무)	안정적 서비스 보장을 위한 지속적인 성능향상
	9 접근통제 강화		9-1 시스템 접근통제 강화계획(보안설정 강화 및 고도화) 9-2 네트워크 접근통제 강화계획(보안설정 강화)	
	10 신규시스템 보안 및 유지 보수를 위한 Testbed구축		10-1 신규시스템 도입시의 보안수준 유지방안 10-2 Testbed의 단계적 확장방안	
	11 침해사고 예방계획	A시설	11-1 통합보안관제시스템 고도화	발전 모델에 따른 단계적 확대 적용
		B시설	11-2 통합보안관제시스템의 집중화	
	12 침해사고 대응계획	A시설 B시설	12-1 침해사고 유형별 대응 및 복구계획 수립	
공통	13 취약점 분석평가 계획		13-1 취약점 분석 · 평가 용역사업의 연도별과제	지속적 강화
	14 보안시스템의 고도화		14-1 기반시설 시스템의 안정성과 신뢰성 보장을 위한 보안 솔루션 검토	

〈그림 10〉 대책수립을 위한 세부과제(예)

보인다. 이는 초기 정보보호시장의 형성 및 각 기업별로 자체적인 방법론의 적용이라는 결과를 가져왔다. 그중에서 취약점 분석 및 평가에 업체별 방법론의 구성이 유사하고, 기업별 경쟁력을 고려하여 개별적으로 적용하고는 있으나, 표준화된 방법론의 정립은 미비한 상태이다. 본 연구에서는 국내에 적용되고 있는 방법론의 공통

점을 뽑아서, 적용 가능한 모델을 제시하여 보았고, 정보통신분야의 1개 시설을 대상으로 한 사례조사를 통하여, 각 단계별 주요내용 및 결과물에 대해 조사를 하여 보았다.

본 연구조사의 한계는 초기 현황 조사에서부터 취약점 분석까지에 대해서는 비교적 공통으로 적용 가능한 모델을 제시하였다고 생각되나, 보호대책 수립 및 그 이후에 대해서는 미진한 점이 많이 있다.

따라서 보다 광범위한 사례조사를 통하여, 보편타당성이 있는 표준모델에 대해 정립을 할 필요가 있고, Best Practice 사례조사를 통하여 산업현장에 적용이 가능한 보다 실질적인 결과 도출이 필요하며, 적용범위도 기반시설 뿐만 아니라 일반기업에서도 적용이 가능한 모델의 연구가 더욱더 필요하다. 또한 기반시설 운영자(기관, 기업)와 컨설팅전문업체의 경영상의 효과에 대한 연구도 절실히 필요하다고 본다.

참고 문헌

1. John Leach, TBSE. (2003). "an engineering approach to the design of accurate and reliable security systems," Computers & Security, Vol. 23 No.1, Elsvier
2. Albin Zuccato, (2004). "Holistic security requirement engineering for electronic commerce," Computers & Security Vol. 23.
3. ISO/IEC 17799:2000, (2000b). "Information technology – code of practice for information security management," International Standard Organization
4. ISO/IEC TR 13335-1,(1996). "Information Technology – guidelines for the management of IT security – part1: concepts and models for IT security," International Standard Organization
5. ISO/IEC TR 13335-2, (1997). "Information Technology – guidelines for the management of IT security – part2 : managing and planning IT security," International Standard Organization; 1997.
6. ISO/IEC TR 13335-3, (1998). "Information Technology – guidelines for the management of IT security – part3 : technique for the management of IT security," International Standard Organization
7. Shon Harris, McGraw Hill, CISSP Certification Exam Guide
8. Rolf Moulton and Robert S. Coles, (2004). "Applying information security governance," Computers & Security Vol. 22 No.7
9. 한국정보보호진흥원 홈페이지(www.kisa.or.kr)
10. 한국정보보호진흥원 기반보호팀, (2001). "취약점 분석?평가를 위한 취약점분석, 자산분석 및 위험분석 지침(안)"
11. 한국정보보호진흥원, (2002). "취약점 분석?평가 모델"
12. 한국정보보호진흥원 기반보호팀, (2001). "취약점 분석?평가 방법론 소개"
13. 정보통신기반보호법 제8조, 제9조, 동법 시행령 제17조 내지 제19조, (2001).
14. 한국전산원, (2004). "한국인터넷백서"
15. 김성훈, 한국정보보호진흥원, (2003). "취약점 분석?평가 품질관리 연구 및 활용방안"
16. 안성일, 정보통신부, "우리나라의 주요정보통신기반 보호정책"
17. 한국전산원, 인포섹, (2004). "주요정보통신기반시설 취약점 분석 및 평가 보고서"