情報保護學會論文誌
第13券 第5號, 2003. 10

개선된 OCTAVE 접근방법을 이용한 정보시스템 취약성 평가 사례연구*

김 기 윤**, 양 동 구***

Case Study for Information System Vulnerability Assessment through Improved OCTAVE Approach

Ki-Yoon Kim**, Dong-Gu Yang***

요 약

업무연속성 관점에서 IDEF 접근방법에 의해서 주요 업무 프로세스를 파악하고, 관련 정보자산을 Skandia 모형으로 식별 한 후에, OCTAVE 접근방법에 의해서 위협을 단계적으로 분석하기 위해서, Nessus Version 1.4.2를 이용하여 도서관 정보시스템 중에서 가장 중요한 자산인 서버에 대해서 취약성을 평가했다. 기존 OCTAVE 접근방법에 IDEF 접근방법과 Skandia 모형을 동시에 이용하는 개선된 OCTAVE 접근방법을 이용한 취약성 평가 사례를 제시했다.

ABSTRACT

We analyze key business process by using IDEF method in the perspective of business continuity, identify key information assets by using Skandia model, and use Nessus Version 1.4.2 to assess vulnerability about the sever of library information system according to OCTAVE(The Operationally Critical Threat, Asset, and Vulnerability Evaluation) approach. We suggest the vulnerability assessment case for introducing improved OCTAVE method including IDEF method and Skandia model.

keyword : *업무 프로세스, 위협, 취약성, OCTAVE*

Ⅰ. 서 론

e-Business 확산을 위한 새로운 정보기술의 활용에 따라서 정보보호문제는 기업의 안전한 업무활동을 위협하는 중요한 문제로 대두되고 있다. 업무 프로세스 관점에서 정보기술의 영향력은 증가한 반면에 이에 대한 관리는 더욱 어려워짐에 따라서 기업들은 효과적인 통제 프로그램이 필요하고, 특히 기업의 경쟁도구로서 정보에 대한 효과적인 정보보호 프로그램을 필요로 하고 있다. 기업들은 90년대 후반부터 정보보호기술에 대한 투자를 확대하고 있으나, 최근 그 투자 경향이 네트워크 보호중심에서 정보자산보호중심으로 변화하고 있다.

미국 경우 최근 5년 사이에 정보보호에 대한 꾸준한 투자에 따라 정보보호 관련 사고율(사고율=사고경험자/총 응답자)은 다소 감소하는 추세를 보이고 있으나, 평균 손실금액(평균 손실액=총손실액/사고건수)은 오히려 증가하는 경향을 보이고 있다. 또한,

* 본 논문은 2003년도 광운대학교 교내학술연구비에 의해서 이루어졌음.
** 광운대학교 경영대학 경영학과(min1203@daisy.kw.ac.kr)
*** 현대정보기술 금융사업단(dgyang@hit.co.kr)

정보기술기반의 취약성에 대한 사고율은 2/3을 차지하지만, 손실액은 1/3을 차지하고 있다. 이러한 결과에 비추어 볼 때, 정보기술기반에 대한 기술적 위험보다는 전사적인 기업위험 관점에서 업무 프로세스 중심의 관리적 위험에 대한 내부통제가 보다 더 강화될 필요가 있다. 2001년에 제정된 정보통신기반보호법에 의해서 주요정보통신기반시설로 지정된 관리기관은 취약성 분석평가를 자체전담반 혹은 외부기관에 위탁해서 2년마다 의무적으로 시행토록하고 있다. 정부기관은 물론 기업도 정보보호가 기술 중심의 통제에서 업무위험 중심의 통제로 변화해야하며, 정보보호통제 구축 후에도 업무 프로세스의 성숙도를 향상시키기 위해서 관리적 위험 관점에서 지속적으로 관리되어야 한다.

위기관리는 비상계획, 긴급대응, 재해복구, 업무연속성(정상업무가동) 단계로 구분되며, 비상계획은 취약성 및 위험 평가, 업무영향분석, 위험관리 및 보안관리 등으로 세분할 수 있다. 위기관리 관점에서 취약성이란 시스템의 일부가 위기발생가능영역에서 반응하는 정도를 나타낸다. 이러한 업무 프로세스 관점에서의 취약성 평가는 비상사태로 업무연속성에 문제가 발생할 경우에 적정시간 안에 순차적으로 업무가 원상회복하는 체계를 수립하는 업무연속성계획(BCP; Business Continuity Planning)의 위험평가를 위해서 필수적인 절차이다.[2,4,10,12]

본 논문의 목적은 첫째, 업무연속성 관점에서 기업 시스템의 내부통제의 중요한 요소인 정보보호를 위해서 업무 프로세스 관점에서 IDEF 접근방법에 의해서 주요 업무 프로세스를 파악한 후에, 관련 정보자산을 Skandia 모형으로 평가하고, 둘째, OCTAVE(The Operationally Critical Threat, Asset, and Vulnerability Evaluation) 접근방법에 의해서 위협을 단계적으로 분석하고, 가장 중요한 자산인 서버에 대해서 취약성을 Nessus Version 1.4.2를 사용하여 평가함으로써, 셋째, 기존 OCTAVE 접근방법에 IDEF 접근방법과 Skandia 모형을 동시에 이용하는, 개선된 OCTAVE 접근방법에 의한 A 대학교 도서관 정보시스템에 대한 취약성 분석 사례를 제시하는 것이다.

II. 정보시스템 취약성 평가 접근방법

위험이란 자산(또는 자산집합)의 취약한 부분에 위협요소가 발생하여 자산의 손실이 발생된 것이다. 취약성으로 인한 위험은 사건발생 확률 또는 빈도와 예상되는 손실로 표현할 수 있다. 위험분석은 자산의 취약성을 식별하고 존재하는 위협을 분석하여, 이들의 발생가능성 및 위협이 미칠 수 있는 영향을 파악해서 보안위험의 내용과 정도를 결정하는 과정이다. 위험분석방법 1세대는 체크리스트, 즉 간단한 설문지로 기본적으로 확인할 수 있는 문항을 만들어 현재 보안수준을 진단하는 것이다. 2세대는 문서기반 방법이고, 3세대는 단순자동도구로서 문서기반을 소프트웨어를 이용하여 효율성을 높인 방법이다. 4세대는 복합자동도구로서 위험분석 단순도구에 스캐닝과 주기적인 갱신기능이 병합된 도구이고, 5세대는 취약성에 대한 대응책의 효과를 비교분석하고 시뮬레이션을 하는 기능이 있는 도구이다. 위험분석방법은 취약성 분석의 내용에 추가하여 조직의 사업의 목표와 임무를 수행하기 위한 자산 가치를 고려하는 점이다.[1,3] 위험분석방법에는 ISO 13335 GMITS(Guidelines for the management of IT security), BS7799(ISO 17799), CSE(Communication Security Establish) Risk Assessment, VAF(Vulnerability Assessment Framework), OCTAVE(The Operationally Critical Threat, Asset, and Vulnerability Evaluation), NIST Risk Management Guide for IT Systems 등이 있다.[6]

취약성이란 조직이나 시스템에 피해를 끼칠 수 있는 원치 않는 사고의 잠재적 원인인 위협이 가해질 수 있는 자산(또는 자산 집합)의 약점이다. 이러한 취약성 평가방법은 일반적으로 네트워크 또는 서버 기반의 스캐닝 툴을 활용하여 네트워크나 서버 등이 노출된 정보시스템의 취약성을 찾아내는 방법과 모의 해킹을 통해서 현재 보안상태를 점검하는 방법이다. 이러한 기존 취약성 평가방법은 네트워크나 시스템의 결점, 즉 취약점을 기술적 위험에 대한 대응만을 고려하지만, 기술적 위험보다는 관리적 위험이 급격히 증가하고 있으므로, 기술적 위험보다는 관리적 위험 관점에서 취약성을 평가해야만 한다.

OCTAVE는 Carnegie Mellon University에 SEI(Software Engineering Institute)에서 1999년에 개발한 정보보안 위험평가방법이다. OCTAVE 접근방법의 3단계 8절차로 구성되어있다. 1단계에는 조직의 자산에 대한 위협을 파악한다. 이를 위해서 경영층의 지식을 파악하고(절차 1), 운영층의 지식을 파악하고(절차 3), 스탭층의 지식을 파악하고(절차 3), 그리고 위협상황을 파악한다(절차 4). 2단계에는 취약성을 식별하고(절차 5), 위협에 따른 영향을 분석한다(절차 6). 3단계에는 보안 전략 및 계획을 수립한다. 위험분석

을 실행하고(절차 7), 보안전략을 개발한다(절차 8). OCTAVE 접근방법에서는 조직 내에 일반관리직 및 정보기술직 구성원 3-5명으로 분석 팀을 구성해서, 조직 내에 다양한 계층의 조직구성원들과 면담과 workshop 에 의해서 정보시스템의 취약성 평가를 실행하게 된다.[7]

본 연구에서는 기존 OCTAVE 접근방법의 1단계를 개선시키기 위해서 IDEF 방법에 의한 업무 프로세스 분석과 Skandia 모형에 의한 정보자산 평가를 추가로 분석하고, 2단계 위협경로분석은 Nessus Version 1.4.2 으로 취약성을 평가하고, 3단계 위험영향(절차 8)을 측정해서, 사례적용 하고자 한다. 연구 내용은 취약성에 초점을 맞추어서, 업무 프로세스 분석, 자산분석, 위협분석, 취약성평가 등 네 단계로 구분해서 기술하고자 한다.

Ⅲ. 정보시스템 취약성 평가절차

3.1 업무 프로세스 분석

업무 프로세스 관점에서 취약성 평가을 위해서 IDEF(Integration DEFinition)를 이용해서 조직의 업무 프로세스를 분석한다. IDEF 방법은 기업이나 조직의 실체를 추상화하여 모델화하고(AS-IS), 작성된 모델의 체계적인 분석을 통하여 문제점을 추출하여 개선된 기업의 모델(TO-BE)을 설계할 수 있도록 개발된 시스템 분석 및 설계 방법이다. 1976년에 미 국방부에서는 진보된 정보시스템의 구축을 전제로 한 항공, 우주 관련 가상의 기업모델(Virtual Enterprise Model)을 표현하기 위한 방법의 연구가 시작되었고 이 연구의 결과로 개발된 것이 IDEF(Integration DEFinition) 방법이다. 1990년대 미 공군의 지원을 받아 Knowledge Based Systems사(KBSI)가 수행한 IICE(Information Integration for Concurrent Engineering) 프로그램에서 IDEF3(Process Description Capture Method), IDEF4 (Object-Oriented Design Method), IDEF5 (Ontology Description Capture Method)가 개발 발표되었다.[9] IDEF는 미상무성과 NIST에 의해서 FIPS(Federal Information Processing Standard)로서 채택된 업무프로세스 분석을 위한 표준적인 방법론이다.

업무연속성관리에서는 파악된 업무프로세스들에 대한 우선 업무대상을 도출하기 위해서 업무복구목표시간(RTO: Recovery Time Objective)과 필요자료에 대한 업무복구목표시점(RPO: Recovery Point Objective)을 설정해야 한다. 그러나 본 연구는 취약성 평가가 주된 목적이므로, OCTAVE 접근방법을 적용하기 전에, 중요한 정보자산을 파악하기 위해서 분석팀이 다양한 계층의 조직구성원들과 면담을 통해서 IDEF 방법을 이용해서 조직의 핵심 업무 프로세스를 분석하는 것이다.

3.2 자산분석

자산이란 조직 내에 가치를 가지고 있는 모든 것이다. 기업의 자산가치 평가방법은 수익가치법(income approach), 자산가치법(asset based approach), 상대가치법으로 구분할 수 있다. 자산가치법은 재무상태에 기초한 방법으로 회사의 자산, 부채 및 자본항목을 평가하여 수정대차대조표를 작성한 후 자산총계에서 부채총계를 공제한 기업의 순자산가치를 기준으로 평가하는 기법으로, 유형에는 장부가치법(book value), 청산가치법(liquidation), 대체가치법(replacement)이 있다.[5]

정보 관련자산에는 하드웨어 같은 유형자산이외에, 소프트웨어나 데이터베이스 같은 비재무적, 비물질적인 자료처리 관련 무형자산이 있다. 즉 재무제표에는 보이지 않는 숨어있는 자산이지만, 기업의 목표달성에 경쟁우위를 가져다주는 지식자산(knowledge assets)이 포함되어 있다. 이러한 무형자산에 대한 현행 회계기준은 역사적 원가주의에 근거하고 있으나, 그 가치가 취득원가와 상이한 경우가 많기 때문에, 무형자산의 가치는 개별요소별 지표를 측정하는 방법과 개별 무형자산의 가치를 측정하는 방법을 이용하고 있다. 개별요소별 지표측정법은 무형자산을 창출하는 각 요소에 대한 지표를 직접측정 하므로 직접측정법이라고도 하며, 스웨덴의 Skandia 모형, 미국의 균형점수표(Balanced Scorecard), 영국의 Annie Brooking 모형 등이 있다.[10] 개별 무형자산 가치측정법은 개별 무형자산에 대한 화폐적 가치측정으로서, 원가접근법, 시장접근법, 이익접근법 등이 있다. 개별요소별 지표측정법은 무형자산의 원천을 구별하고 관리할 수 있다는 장점은 있으나, 타 기업 혹은 전기의 무형자산 가치와 비교가 어렵다는 단점이 있다. 개별 무형자산 가치측정법은 무형자산 원천별 구분과 비교가능성을 동시에 만족시키는 우수한 방법이나, 측정을 위해서 많은 정보와 비용이 소요된다는 문제점이 있다.[5]

주요 업무 프로세스별로 파악된 정보자산에 대한

무형자산 측정법 중 Skandia 모형이 부분적으로 식별되는 정보자산에 대해서 개별적으로 측정 가능한 가장 효율적인 방법을 제시하고 있다. 식별된 자산의 분류 및 측정은 개별요소별 지표측정인 Skandia 모형에서와 같이 재무, 고객, 과정, 개선 및 개발, 인간 등 5가지 가치항목으로 측정한다.[11] 하드웨어는 유형자산으로 자산가치법 중에서 장부가치법 혹은 대체가치법으로 측정가능하다. 소프트웨어 중에서 자체 개발한 소프트웨어는 무형자산의 특수한 형태인 창조적인 지적재산권이므로 개발비로 측정하지만, 구입한 소프트웨어는 자산가치법인 장부가치법 혹은 대체가치법으로 측정하는 것이 타당하다. 하드웨어 및 소프트웨어 이외에 데이터베이스, 문서, 자료, 직원 등은 Skandia 모형의 지표들을 이용해서 측정한다.

3.3 위협분석

OCTAVE에서는 자산, 행위자, 동기, 접근, 결과(asset, actor, motive, access, outcome)와 같은 5가지 속성 측면에서 위협의 유형을 분석한다. 첫째, 자산은 조직에 가치가 있는 것으로서 전자적 혹은 물적 형태의 정보, 정보시스템, 전문지식을 소유한 집단 등이다. 둘째, 행위자는 자산에 대한 보안요구(비밀성, 무결성, 가용성)를 침해하는 사람으로서 조직의 내부자와 외부자로 구분된다. 셋째, 동기는 행위자의 의도가 의도적인지 우연적(비의도적)인지를 의미한다. 넷째, 접근은 행위자가 자산을 어떻게 접근하느냐에 따라서, 네트워크 접근과 물적 접근으로 구분한다. 다섯째, 결과는 자산의 보안요구를 침해한 것으로서, 중요한 정보의 폭로(disclosure) 및 수정(modification), 중요한 정보, 하드웨어, 혹은 소프트웨어의 파괴(destruction), 그리고 중요한 정보, 소프트웨어, 혹은 서비스의 장애(interruption) 등 4가지 범주(폭로, 수정, 파괴, 장애)가 있다.

OCTAVE 에서는 위협에 대한 표준적인 네 가지 범주는 개인 관점에서 네트워크 접근을 이용한 인간 행위자와 물적 접근을 이용한 인간 행위자로 구분하고, 조직 관점에서 통제 가능한 시스템 문제와 통제 불가능한 기타 문제로 구분한다.

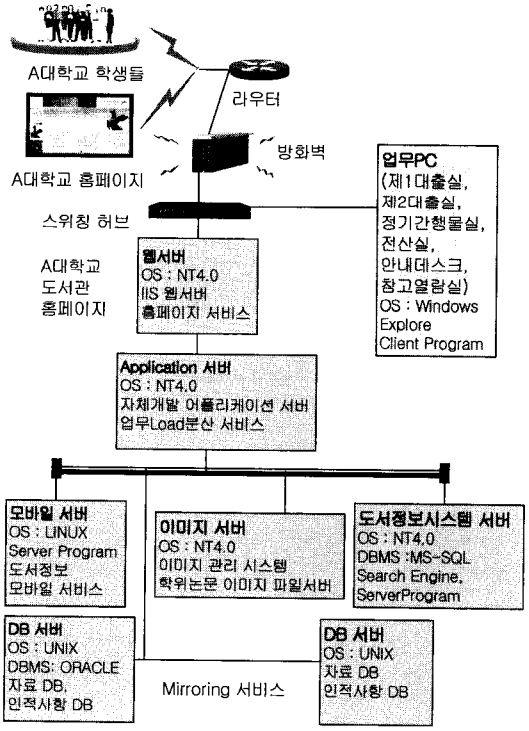
첫째, 네트워크 접근을 이용한 인간 행위자 영역에 속하는 위협들은 조직의 중요 자산에 네트워크를 기반으로 공격하는 위협들로서, 사람의 직접적인 의도적 혹은 우연적 행위이다. 네트워크를 이용한 인간의 위협 행위자는 조직의 내부 행위자와 외부 행위자로 구분할 수 있다. 내부 행위자들로는 비악의적인 조직구성원(컴퓨터 시스템과 정보를 우연히 남용하거나 오용하는 조직 내에 사람), 불만스런 조직구성원(컴퓨터 시스템과 정보를 의도적으로 남용하거나 오용하는 사람) 등이 있고, 외부 행위자들로는 공격자(도전 혹은 재미를 위해서 컴퓨터 시스템을 공격하는 사람), 스파이(정치적인 이득을 위해서 컴퓨터를 공격하는 사람), 테러리스트(정치적 이득을 위해서 공포를 조성시키기 위해서 컴퓨터를 공격하는 사람), 경쟁자(경제적 이득을 위해서 컴퓨터 시스템을 공격하는 사람), 범죄자(개인적으로 재무적인 이득을 위해서 컴퓨터를 공격하는 사람), 파괴자(손해를 끼치려고 컴퓨터 시스템을 공격하는 사람) 등이 있다. 둘째, 물적 접근을 이용한 인간 행위자 영역에 속하는 위협들은 조직의 중요 자산에 물적 접근에 의해서 공격하는 위협들로서, 사람의 직접적인 의도적 혹은 우연적 행위이다. 셋째, 시스템 문제 영역에 속하는 위협들은 조직 정보시스템 문제로서, 하드웨어 결함, 소프트웨어 결함, 기업관련 시스템의 비가용성, 바이러스, 악의적인 코드(malicious code), 다른 시스템과 관련된 문제 등이다. 넷째, 기타 문제 영역에 속하는 위협들은 조직 통제 밖에 놓인 문제들로서, 조직의 정보시스템에 영향을 줄 수 있는 홍수, 지진, 폭풍 같은 자연재해는 물론 통신, 전기 같은 중요한 시설의 비가용성으로 인한 상호의존적 위험이 포함된다. 위협분석을 위해서 자산, 행위자, 동기, 접근, 결과와 같은 5가지 속성 측면에서 위협의 유형을 분류한 후에, 식별된 위협의 원천과 결과를 근거로 위협을 분석한다.

3.4 취약성평가

취약성은 정보자산이 지닌 잠재적인 약점을 말하며, 이 약점 자체가 직접적인 위험을 초래하지는 않지만, 위협에 의해 이용되어 위험을 발생시킬 환경을 제공한다. 본 연구에서 취약성 평가(assessment)는 취약성분석으로 식별된 취약성을 측정한 것으로 위험분석절차를 포함하고 있다. 취약성분석의 대표적인 방법으로는 한국정보보호진흥원(CERTCC)에서 제공하는 방법들이 있다. 대표적인 방법으로는 라우터의 보안설정을 점검하는 RAT, 네트워크의 보안설정을 점검하는 Nmap, 컴퓨터의 취약점을 점검하는 Nessus, NT의 IIS 웹 서버 취약성을 점검하는 CIS 외에 SATAN, ISS, COPS, TIGER 등이 있다.

Ⅳ. 정보시스템 취약성 평가 사례

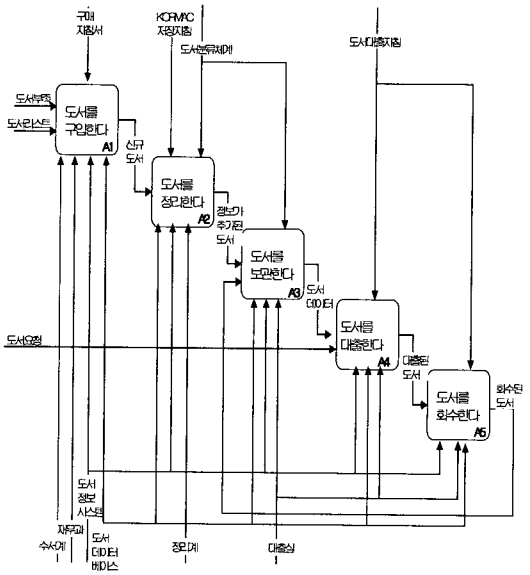
A 대학교 도서관 정보시스템은 대학본부 학사정보시스템과는 독립적으로 운영되고 있다. 도서관 정보시스템은 내부 직원들의 업무지원을 위한 부분과 교수 및 학생을 위한 서비스 부분으로 나누어진다. 본 시스템의 업무지원분야는 C/S(Client/Server) 기반 방식으로 구축이 되어 있고 서비스 분야는 Web기반 방식으로 되어 있어서, 내부적으로는 업무의 효율성을 올리고자 하였으며, 외부적으로는 One-Stop 서비스 방식을 채택하여 운영하고 있으며 향후 비젼은 전자도서관(Digital Library)을 구축하는 것이다.



〔그림 1〕 A 도서관의 정보시스템

4.1 업무 프로세스 분석

IDEF 방법으로 분석한 A도서관의 업무 프로세스는 그림과 같이 도서구입, 도서정리, 도서보관, 도서대출, 도서회수의 주요 행동(Activity)으로 구성이 되어 있다. 모든 행동(Activity)은 투입과 산출, 통제 메카니즘으로 구성이 되어 있는데 선행 행동은 다음 행동에 영향을 미친다. 도서구입단계에서는 도서 데이터베이스를 기준으로 도서의 존재유무를 확인하며,



〔그림 2〕 A 도서관의 업무 프로세스

도서정리단계에서는 DDC 및 KDC 분류 체계에 따라 KORMARC 형태로 신규 도서정보를 데이터베이스에 정리하며, 도서 보관 및 대출, 회수 에서는 도서 데이터베이스 및 도서관리시스템이 주요 업무의 핵심에 위치한다.

모든 행동은 그림에서 보듯이 도서정보시스템과 도서데이터베이스와 매우 관련이 깊은 것을 알 수 있으며, 도서정보시스템과 도서데이터베이스는 모든 행동에 메카니즘으로 작용하고 있다. 이는 모든 행동을 수행하기 위해서는 도서정보시스템과 도서 데이터베이스를 이용해야 하는 것을 의미 한다. 이와 같이 IDEF 방법으로 분석한 A도서관의 업무 프로세스의 연속성 관점에서 가장 중요한 자산은 서버, PC, 데이터베이스, 서적 등으로 파악되었다.

4.2 자산분석

Skandia 모형에서 지식자산의 가치기반은 고객 가치, 조직적 가치, 인적 가치 등 세요소가 독립적으로 존재하지 않고 서로 연계되어 있으며, 세 요소들로부터 재무적 가치가 창출되고 있다. 조직가치는 과정과 개선 및 개발로 두 가지로 다시 세분되어서, 재무, 고객, 과정, 개선 및 개발, 인간 등 5가지 요소에 따라서 지식자산을 분류해서 다음과 같은 지표로 그 가치를 측정한다.

재무적 가치에는 통상적인 대차대조표의 내용을

〔표 1〕 A 도서관 자산의 분류와 측정

가치	자산		지표	측정치
재무	H/W	서버	대체비용	1억5천만(원)
		PC	대체비용	5천5백만(원)
	S/W		대체비용	6천5백만(원)
	DB		대체비용	3천만(원)
	서적		구입비용	9억2천만(원/년)
	직원		평균월급x직원수	5억2천5백만(원)
고객	학생 및 교수		이용자 수 대출 건 수 1인당 대출권수	2,640(명/일) 615(건/일) 21.9(권/명/년)
조직	과정	도서관 조직	관리운영비 통신비 IT직원/총 직원수	4천만(원/년) 1백만(원/년) 14(%)
	개선	도서관 조직	직원훈련비용 40세미만 직원비율	0(원) 27(%)
인적	직원		직원 수 직원 평균연령	15(명) 43(년)

포함하는 것으로 과거 측정치로 대부분 알려져 있는 지표들이 있다. 고객가치에는 고객종류, 고객기간, 고객역할, 고객지원, 고객성공 등에 관한 현재 활동에 관한 지표들이 있다. 과정가치에는 가치창출을 지원하는 기술의 역할에 관해 현재 활동에 관한 지표들이 있다. 개선 및 개발 가치에는 미래 기회를 포착하기 위한 노력을 나타내는 조직의 미래가치에 관한 지표들이 있다. 인적 가치에는 직원들의 능력과 역량에 관한 지표들이 있다.

A 도서관의 재무적 가치 중에서 하드웨어, 소프트웨어(원문정보 프로그램, 방화벽 프로그램 등 9종), 데이타베이스는 유형자산으로 자산가치법 중에서 대체가치법으로 측정했고, 그 외에 서적, 직원 등에 대한 재무적 가치와 고객가치, 조직가치, 인적가치는 Skandia 모형의 지표들을 이용해서 [표 1]과 같이 측정했다. 서적과 직원의 재무적/인적 가치가 매우 높지만, 업무연속성 관점에서는 서버, PC, 데이터베이스가 보다 더 중요한 자산으로 판단되었기 때문에 위협 및 취약성 분석은 이들 정보자산에 대해서 실행한다.

4.3 위협분석

주요 자산인 서버, PC, 데이터베이스, 서적에 대한 관리자들의 보안 관심영역을 폭로, 수정, 파괴, 장애 등 4가지 측면에서 도출하고, 이에 대한 보안 요구사항을 분석했다. 폭로는 내부의 중요정보를 외부에 노출시키는 것이며, 수정은 내부정보의 변경을 의미하며, 파괴는 시스템 및 데이터베이스의 손상 및 삭제를 의미한다. 장애는 시스템의 서비스가 불능인 상태를 의미한다. 각 주요 자산에 대한 보안 관심영역과 보안 요구사항은 [표 2]와 같다.

업무 연속성 관점에서 가장 중요한 자산인 도서관 리시스템 서버는 도서관의 전산실 담당자가 서버를

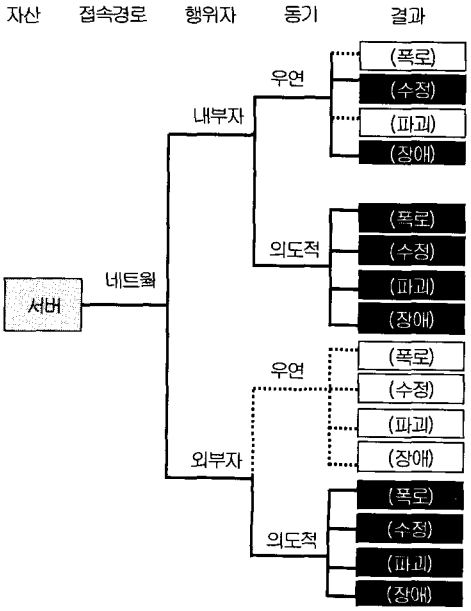
〔표 2〕 주요 자산에 대한 보안 관심영역과 요구사항

자산	자산의 특성	보안 관심영역	보안 요구사항
서버	서버는 크게 UNIX서버와 NT 서버로 구성이 되어 있으며, UNIX서버는 데이터베이스를 저장하고 있으며, NT 서버는 도서관리시스템 및 홈페이지서비스를 하고 있음.	<폭로> ID/PW 폭로, <수정> ID/PW 수정, Sub 디렉토리 수정. <파괴> 서비스 시스템 파괴, <장애> 서버의 정지로 인한 운영 중단.	<가용성> 서버는 1일 24시간 중단 없이 운영되어야 함. <기밀성> 오직 관리자만이 서버를 관리해야 함.
PC	PC는 전반적으로 도서관 직원들이 업무를 진행할 경우 반드시 사용해야 하는 도구 임. PC를 이용하여 정보를 입력, 서버에서 정보 검색, 업무 처리를 함.	<폭로> 개인 ID/PW 폭로, <수정> Client 프로그램을 이용한 잘못된 정보 기입, <파괴> PC의 파일 및 자료 파괴, <장애> PC의 정지.	<가용성> PC는 업무시간에 중단 없이 사용이 가능해야 함.
데이터베이스	데이터베이스는 크게 도서 데이터베이스와 인적사항 데이터베이스로 구성되어 있음.	<폭로> 보호대상 데이터베이스의 폭로(인적데이터베이스), <수정> 도서 데이터베이스 및 인적 데이터베이스 수정. <파괴> 데이터베이스의 삭제, <장애> 데이터베이스의 접근 불능.	<가용성> 모든 데이터베이스에 1일 24시간 접속이 가능해야 한다. <무결성> 데이터베이스의 내용이 입력상태와 일치해야 함.
서적	A도서관의 서적은 총 365,240권을 보유하고 있으며, 교수 및 학생을 대상으로 대출 서비스를 하고 있음.	<파괴> 도서자료의 도난, 분실, 훼손으로 인하여 대출서비스의 불가.	<가용성> 도서관 개관시간에 맞추어 도서대출 서비스를 해야 한다.

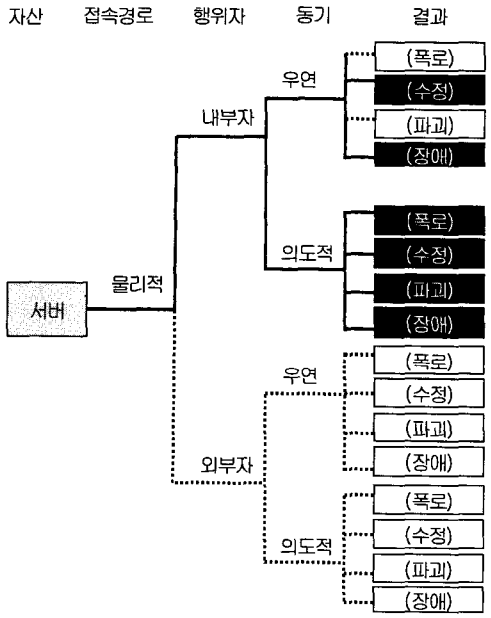
관리하고 있으며, T회사와 유지보수계약을 맺어 정기적으로 유지보수를 하고 있다. 본 시스템에 접속할 수 있는 사람으로는 내부 담당직원과 유지보수자가 있다. 이들에 의한 시스템의 위협정도는 크게 우려되지 않지만, 외부자에 의한 네트워크를 통한 시스템 접근이 우려된다. 기존 보안시스템이 구축 되어 있으나, 도서관 서버로의 해킹 및 의도적인 접근으로 인하여 서버 내의 자료 삭제 및 변경, 관리자 모드 변경 등이 잠재적 위험으로 예상된다. 이 외에 시스템적 위협과 기타 위협이 존재하는데, 시스템적 위협은 도서관리 소프트웨어의 결함, 바이러스, 타 시스템과의 충돌, 통신문제가 예상되며, 기타 위협으로는 전원공급 문제, 요구사항 반영의 미비, 자연재해, 장비의 잘못된 수정, H/W 및 S/W의 통제능력 부족이 있을 수 있다. 업무 연속성 관점에서 가장 중요한 자산인 서버에 대한 위협들은 네 가지로 분류할 수 있다. 즉 네트워크 접근을 이용한 인간 행위자 영역에 속하는 위협들, 물리적 접근을 이용한 인간 행위자 영역에 속하는 위협들, 시스템 문제 영역에 속하는 위협들, 기타 영역에 속하는 위협들 등이 있다.

서버에 대한 접속경로가 네트워크를 이용한 방법에서는 행위자가 내부자와 외부자로 구분된다. 내부자가 실수 및 우연으로 시스템에 영향을 줄 수 있는 부분은 정보를 수정 하거나 실수로 인하여 시스템이 정지되는 서비스 장애가 있을 수 있다. 또한, 내부자 혹은 외부자가 의도적으로 혹은 악의적으로 시스템(서버)에 대한 정보를 폭로, 수정, 파괴 및 장애를 초래 할 수 있다.

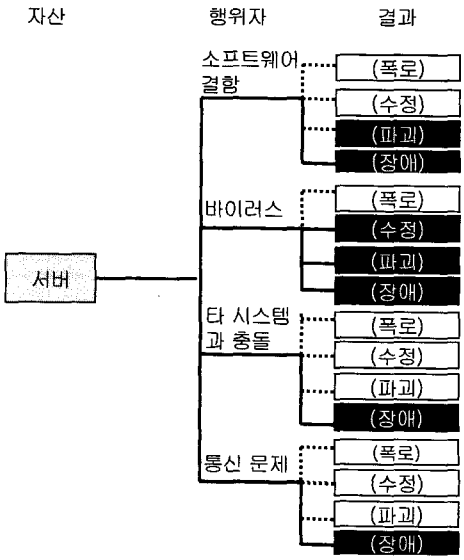
서버에 대한 물리적 접근은 원천적으로 외부인 접근이 차단되며, 내부인 만이 접근 가능하다. 내부인이 서버에 접근하는 경우는 서버 관리자와 유



〔그림 3〕 네트워크 접근에 의한 인간 행위자 위협



〔그림 4〕 물리적 접근에 의한 인간 행위자 위협

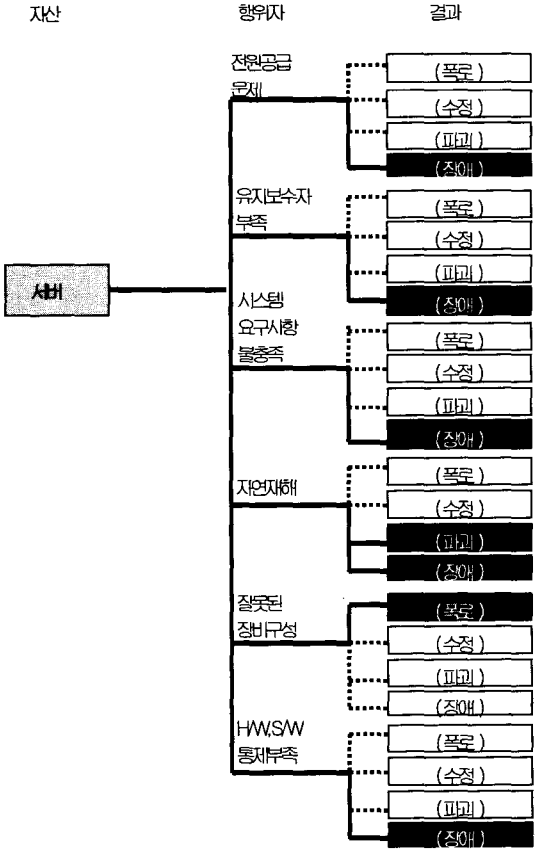


〔그림 5〕 시스템 문제 영역에 속하는 위협

지보수자만이 접근 가능하며, 관리자와 유지보수자가 우연적으로 정보를 수정 하거나 실수로 인하여 시스템이 정지되어서 서비스 장애가 발생할 수 있다.

시스템 문제 영역에 속하는 위협으로 도서관리시스템 및 상용소프트웨어의 자체적 결함 때문에 발생 가능한 위협, 바이러스 혹은 악성 프로그램 때문에 발생 가능한 위협, 타 시스템과의 충돌 때문에 발생 가능한 위협, 통신문제 때문에 서버에 영향을 줄 수 있는 위협 등을 고려해 볼 수 있고, 이로 인한 결과들은 [그림 5]와 같이 정보의 수정, 파괴, 장애가 발생할 수 있다.

서버에 대해서 기타 발생 가능한 위협들로는 전원공급 문제, 유지보수자의 부족, 시스템 요구사항 불충족, 자연재해, 잘못된 장비구성, 하드웨어 및 소프트웨어에 대한 통제능력 부족 등이 있고, 이로 인한 결과들은 [그림 6]과 같이 대부분이 서비스 장애를 발생 시킨다.



〔그림 6〕 기타 영역에 속하는 위협들

4.4 취약성평가

A 대학교 도서관 정보시스템에서 가장 중요한 NT 웹 서버에 대한 취약성 분석을 Nessus Version 1.4.2를 사용하여 실시하였다. NT 웹 서버에 대해서 취약성분석을 실시한 이유는 도서정보시스템 이용 및 웹을 이용한 서비스 접속이용도가 가장 높고, 업무연속성 관점에서 가장 중요한 자산이기 때문이다. 다시 말해서, A 대학교 도서관 정보시스템의 NT 웹 서버는 교수, 학생 및 일반인을 상대로 공개되어 있고, 해킹 및 악성 프로그램에 가장 많이 노출되어 있어서 업무 연속성에 장애가 될 수 있는 가능성이 가장 높기 때문이다.

Nessus 에 의한 취약성 평가는 잠재적 손실가능성에 대한 강도(severity)를 3점 척도(고, 중, 저)로 측정되는데, 서버에 대한 Port 서비스 분석결과는 고 강도 9개, 저 강도 55개, Open Port 17개로 총 81개가 발견 되었고, 서버와 연결된 PC 에서는 고 강도 17개, 저 강도 73개, Open Port 39개로 총 129개가 발견되었다. 서버의 경우 고 강도는 당장 조치를 취하여 하며, Open Port의 경우는 시스템 서비스 정책에 따라서 사용하지 않는 Port는 폐쇄를 시키고, 사용하는 Port의 경우 지속적인 모니터링이 필요하다. 서버에 대한 취약성이 고 강도가 나온 9개의 경우만을 보다 세부적으로 분석한 결과가 [부록 1]이다.

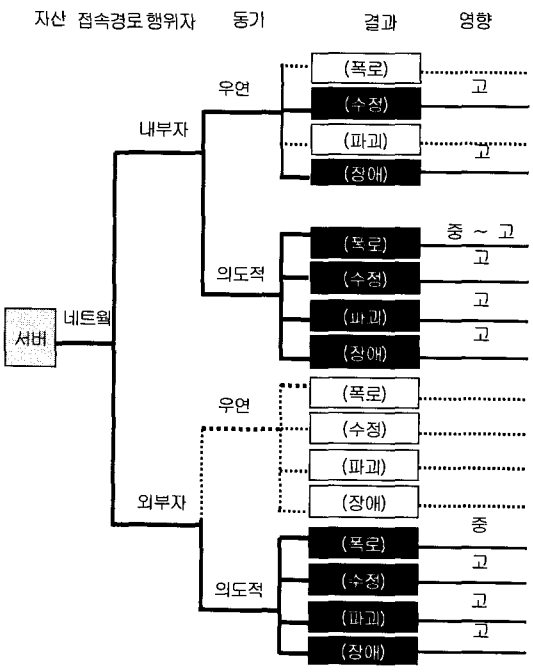
서버에 대한 취약성 분석 결과를 근거로, 서버 및 이와 연결된 PC 에서 취약성 때문에 발생 가능한 폭로, 수정, 파괴, 장애에 대한 위험 영향(risk impact)을 기술하고, 이에 대한 잠재적 손실 크기를 3점 척도(고, 중, 저)로 평가한 것이 [표 4]이다.

이러한 위험 영향을 평가한 후에, 도서관 정보시스템 이용자의 신뢰, 직원들의 업무 생산성, 운영비용, 시설 등을 고려해서 서버에 대한 네 가지 위협경로분석(네트워크 접근을 이용한 인간 행위자 영역에 속하는 위협들, 물리적 접근을 이용한 인간 행위자 영역에 속하는 위협들, 시스템 문제 영역에 속하는 위협들, 기타 영역에 속하는 위협들) 관점에서 위험 영향 평가를 한다. 네 가지 위협경로분석 중에서, 서버에 대한 네트워크 접근을 이용한 인간 행위자 영역에 속하는 위협들의 영향을 평가한 것이 [그림 7]이다.

이와 같은 위협경로 별로 위협결과인 폭로, 수정, 파괴, 장애의 위험영향을 근거로 정보보안전략을 수

〔표 4〕 서버 및 PC 에 대한 위험 영향 평가

자산	결과	위험 영향	평가
서버	폭로	도서 정보 및 회원 정보 보호의 실패는 도서관 조직 및 장비의 신용의 손실을 가지고 온다.	중
	수정	부정확한 도서정보 및 회원정보 수정은 도서관 업무의 생산성과 고객신뢰도에 영향을 미친다.	고
		홈페이지 정보의 수정은 교수, 학생, 직원들의 업무수행에 영향을 미친다.	고
	파괴	만일 도서데이터 베이스가 파괴된다면, 빠른 시일 내에 도서정보의 재구축이 거의 불가능하고, 도서정보의 조회 및 검색서비스를 제공하지 못한다.	고
	장애	웹 서버의 장애는 도서정보 서비스에 직접적으로 영향을 미친다.	고
PC	폭로	개인용 컴퓨터들은 개인적 업무를 행하는데 있어서 잠재적이며 광범위한 위협들에 노출되어 있다. 고의적이든 우연이든 개인용 컴퓨터들에 대한 접속은 매우 간단하다. 도서관에 출입을 하는 학생들 혹은 외부인이 물리적인 방법을 통한 도서관의 개인용 컴퓨터 접속은 어려우나 컴퓨터 화면을 훔쳐보기는 아주 쉬우며, 네트워크를 통한 방법으로는 파일공유, 바이러스, 해킹 등에 노출되어 있다. 도서정보 및 도서이용자 정보의 폭로가 예상이 된다.	중
	수정	Client용 도서관리 프로그램의 수정은 직원들의 시간 손실, 정보손실, 도서정보 변경, 사용자 정보의 변경 등의 결과를 초래 할 수 있다.	고
	파괴	개인용 컴퓨터의 파괴는 도서관의 모든 업무를 중단시킨다.	고
	장애	개인용 컴퓨터에 대한 오랜 접속장애는 도서관 업무를 불가능하게 한다.	고



〔그림 7〕 서버에 대한 네트워크 접근에 의한 인간 행위자 위협의 영향 평가

립하게 된다. 이를 위해서 경영층 관점에서는 정보보호 인식 및 훈련, 보안정책 및 규정, 비상계획 및 재난복구계획 등이 파악되어야 한다. 운영층 관점에서는 물적 보안계획 및 절차, 물적 접근통제, 보안감사, 시스템 및 네트워크 관리, 시스템 관리 도구, 암호, 취약성 및 보안사고에 대한 관리책임 등이 파악되어야 한다. 이와 같이 업무 프로세스 분석, 자산분석, 위협분석 후에 실행되는 취약성 평가의 결과로 파악된 주요 자산에 대한 위험영향을 극소화시킬 수 있는 보안대책의 구축이 정보보안전략의 핵심이 된다.

V. 결 론

기존 OCTAVE 접근방법의 단점은 업무 프로세스 분석 없이 조직계층(경영층/운영층/스탭층) 별로 분석하고 있고, 자산분석도 비재무적 무형자산이 대부분인 정보자산에 대해서 자산가치분석을 하지 않는다는 점이다. 개선된 OCTAVE 접근방법은 이러한 단점을 보완하기 위해서, 기존 OCTAVE 접근방법에 IDEF 접근방법과 Skandia 모형을 동시에 이용하는 개선된 방법이다. 이를 이용해서 도서관 정보시스템 중에서 가장 중요한 정보자산인 서버에 대한 취약성 평가 사례 적용결과는 다음과 같다.

첫째, 업무 프로세스 분석은 IDEF 방법으로 분석한 A도서관의 업무 프로세스는 도서구입, 도서정리, 도서보관, 도서대출, 도서회수 등 행동으로 구성이 되어 있고, 가장 중요한 자산은 서버, PC, 데이터베이스, 서적 등으로 파악되었다. 둘째, 자산분석은 재무적 가치 중에서 하드웨어, 소프트웨어, 데이터베이스는 유형자산으로 자산가치법 중에서 대체가치법으로 측정했고, 그 외에 서적, 직원 등에 대한 재무적 가치와 고객가치, 조직가치, 인적가치는 Skandia 모형의 지표들을 이용해서 측정 결과, 업무 연속성 관점

에서는 서버, PC, 데이터베이스가 중요한 자산으로 판단되었다. 셋째, 위협분석은 관리자들의 보안 관심 영역을 폭로, 수정, 파괴, 장애 등 4가지 측면에서 도출하고, 이에 대한 보안 요구사항을 분석했고, 가장 중요한 자산인 서버에 대한 네 가지 위협경로분석(네트워크 접근을 이용한 인간 행위자 영역에 속하는 위협들, 물적 접근을 이용한 인간 행위자 영역에 속하는 위협들, 시스템 문제 영역에 속하는 위협들, 기타 문제 영역에 속하는 위협들)을 했다. 넷째, 취약성 분석은 NT 웹 서버에 대해서 Nessus Version 1.4.2 를 사용하여 실시하였다. 서비스 접속이용도가 가장 높고, 업무연속성에 장애가 될 수 있는 가능성이 가장 높은 자산인 NT 웹 서버에 대해서 취약성 분석을 실시했다.

서버 및 이와 연결된 PC 에서 위협에 의한 취약성 때문에 발생 가능한 폭로, 수정, 파괴, 장애에 대한 위험 영향을 파악했고, 이에 대한 잠재적 손실 크기를 3점 척도(고, 중, 저)로 평가한 후에, 서버에 대한 네 가지 위협경로분석 관점에서 위험 영향을 평가했다.

본 연구는 OCTAVE 접근방법 절차 7까지만 적용한 사례이며, 절차 8의 적용을 위해서는 위험평가 기준을 설정해서 보안대책을 구현하는 보안전략이 수립되어져야 한다. 앞으로의 보다 체계적인 방법론 제시를 위해서는 IDEF 방법에서 업무흐름과 정보자산과의 연계성, Skandia 모형의 가치분류체계의 종속성 등 문제점들이 연구되어져야 한다.

참 고 문 헌

[1] 김기윤, "위험관리와 위기관리: 정보시스템의 재난복구", 리스크관리연구, 한국리스크관리학회, 제8집, 1997 가을호, 1997. 12, pp.291~315.

[2] 김기윤, 김종기, 김정덕, 이경석, "행정전산망의 재해복구를 위한 비상계획 현황과 개선방안", 통신정보보호학회지, 한국통신정보보호학회, 제9권, 제1호, 1999. 3, pp.87~100.

[3] 김기윤, 나관식, "취약성 평가에 의한 정보보호 지표의 계량화: 정보자산가치가중치법", 통신정보보호학회지, 한국통신정보보호학회, 제10권, 제1호, 2000. 3, pp.52~62.

[4] 김종기, 김기윤, 이경석, 김정덕 "정보시스템재해에 대비한 업무지속성관리", 통신정보보호학회지, 한국정보보호학회, 제11권, 제1호, 2001. 2, pp.9~19.

[5] 조성표, "지식자본시대 회계의 과제: 무형자산의 측정과 보고", 회계저널, 제9권, 제2호, 2000년, pp.135~163.

[6] 조태희, 취약점 분석 평가 방법론 소개, 한국정보보호진흥원 기반보호팀, http://www.kisa.or.kr/cip/data/ trend2/trend_in_001_4.pdf에서 재인용.

[7] Christopher J. Alberts and Audrey J. Dorofee, OCTAVE-SM Method Implementation Guide Version 2.0, Vol.1-18, Carnegie Mellon Software Engineering Institute, June 2001.

[8] CSI/FBI, Computer Crime and Security Survey, 2002.

[9] Knowledge Based Systems, Inc. (KBSI), A structured approach to enterprise modeling and analysis, http://www.idef.com/default.html

[10] Kristen Noakes-Fry and Trude Diamond, "Business Continuity and Disaster Recovery Planning and Management: Perspective", Gartner Research, DPRO-100862, 8 October 2001, pp.1~15.

[11] Lief Edvinsson and Michael S. Malone, Intellectual Capital, Sejong Books Inc., Printed in Korea, 1998.

[12] Martin Nemzow, Business Continuity Planning, International Journal of Network Management, Vol.7, 1997, pp.127~136.

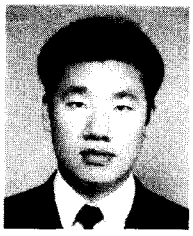
부 록

〔부록1〕 서버에 대한 취약성이 고강도인 경우 분석

서비스 명	강도	분석 결과
Snmp (161/udp)	고	Simple Network Management Protocol - SNMP Agent를 이용하여 외부에서 원격 조정 및 Back Door 침투의 가능성이 있다.
Netbios-ssn (139/tcp)	고	Netbios Session Service - 원격으로 Host에 접속할 경우 접속 ID/Password가 기본값으로 설정 되어 있어서 관리가 요망된다.
Smtp (25/tcp)	고	Simple Mail Transfer Protocol - 현재 Smtp 설정이 Mail From Testing 으로 되어 있다. 메일을 보낼 경우 프로그램에서 반영 되며, 이러한 부분은 외부인이 메일을 이용하여 시스템을 멈추게 할 수 있다. 또한 공격자들은 Smtp와 관련하여 Root권한을 습득 할 수 있다.
Http (80/tcp)	고	www-Http (World Wide Web) - "iiscrack.dll" 파일이 발견됨.(트로이 목마의 유형) 외부인이 웹서버상의 모든 서비스 기능을 이용당 할 수 있음. 파일 삭제 바람.
Http (80/tcp)	고	www-Http (World Wide Web) - Shtkl.ISAPI에서 취약점이 발견 되었다. 긴 URL을 인식하지 못하여 URL서비스에 문제가 발생 될 수 있다. Upgrade를 요함.
Http (80/tcp)	고	www-Http (World Wide Web) - IIS서버에 .THR ISAPI 필터 보유. Internet Information Service 에 문제 발생 여지가 있다. Upgrade 및 Patch 요함.
Http (80/tcp)	고	www-Http (World Wide Web) - ISAPI 필터로 인해 IIS 웹 서버 상에서 오버버퍼가 발생하고 있다. 공격자들로 인해 서비스 거부의 원인이 될 수 있다. Upgrade를 요함.
FTP (21/tcp)	고	FTP Control - FTP 서버가 "STAT *? AAA...AAA"라는 명령어에 취약점을 보이고 있다. 공격자들이 이를 악용할 소지가 있다. Upgrade를 요함.

〈著者紹介〉

김 기 윤 (Ki-Yoon Kim) 정회원
1976년 2월 : 고려대학교 공과대학 토목환경공학과(공학사)
1979년 9월 : 고려대학교 경영대학원(경영학석사)
1985년 2월 : 고려대학교 대학원(경영학박사)
1980년 3월~현재 : 광운대학교 경영대학 경영학과 교수
<관심분야> 보안관리, 위험분석, 업무연속성관리



양 동 구 (Dong-Gu Yang) 정회원
1999년 2월 : 광운대학교 경영학과(경영학사)
2001년 2월 : 광운대학교 대학원 경영학과(경영학석사)
2002년 9월~현재 : 광운대학교 대학원 경영학과 박사과정 중
2003년 3월~현재 : 현대정보기술 금융사업단 BCP 컨설턴트
<관심분야> 보안관리, 위험분석, 업무연속성관리