韓國 컴퓨터情報學會 論文誌
第11卷 第6號, 2006. 12

2006-11-6-2-3

정보시스템 위험관리 프로세스 모델링에 관한 연구

김 태 달*

The research regarding an information system risk management process modeling

Tai-dal Kim *

요 약

정보기술 발전과 수요자의 정보 요구 증대에 따른 위험요소 증가에 대비하기 위해서 조직 내에서는 정보기술 자원의 무결성, 가용성, 기밀성에 대한 내. 외부의 정보 및 시스템과 데이터에 대한 통제가 요구되고 있다. 본 논문에서는 다양한 루트로 침입하는 위험을 종합적으로 관리할 수 있는 정보기술위험관리시스템 개발을 위해 필요로 하는 요구기능과 구조를 국내외 사례를 중심으로 조사하고 분석하였다. 그리고 궁극적으로 위험관리 통합프로세스 모델을 설계함으로서 위험 요소에 대해 사전에 대비 할 수 있도록 유도하는데 목적을 두었다.

Abstract

From the hazard which it prepares in the hazards increase which it follows in information demand augmentation of information technical development and the consumer from inside systematizing integrity and solubility of information technological resources, inside against a confidentiality. The control against information and a system and a data outside is demanded. From the dissertation which it sees demand function and the structure which do information technical risk management system development it will be able to manage the danger which it infiltrates with the root which is various overview in hazard necessity it investigated the inside and outside of the country instance in the center and it analyzed. And it plans the dangerous civil official integrated process model ultimately as against a hazards it will be able to prepare in the dictionary in order, it put the place objective which it induces.

▸ Keyword : 네트워크관리시스템(NMS), 서버관리시스템(SMS), 변경관리시스템(CMS), 정보기술위험관리시스템(ITRMS), 전사적자원기획(ERP), 전사적암호관리(ESM), 형상관리(CM), 사업프로세스관리(BPM), 무전망침입검출시스템(IDS), 무전망침입보안시스템(IPS)

• 제1저자 : 김태달
• 접수일 : 2006.11.06, 심사일 : 2006.11.18, 심사완료일 : 2006. 12.20
* 청운대학교 컴퓨터학과 교수
※ 본 논문은 청운대학교 학술연구과제비로 연구 수행되었음.

Ⅰ. 서론

위기는 예측하지 못한 상태에서 발생한 사건이다. unexpected 가 아닌 unpredictable 즉 위기 자체가 예상하지 못한 것이 아니고, 위기가 언제 닥칠지 예측할 수 없다는 뜻이다.[12]

위기로 인하여 조직의 일상적인 운영이 방해받고 있다. 부분적인 문제인 사고에 비해 위기는 전체 조직의 운영에 영향을 미칠 수 있는 잠재력이 있다. risk management가 조직 내 부분적 문제 해결한다면 Crisis management는 조직 내.외의 전체적 문제를 해결하는 특성을 갖는다.[3] 위기는 위협과 피해(재정적 손실, 스테이크 홀더들의 부상 또는 사망, 구조물이나 재산상의 손실, 명성의 훼손, 환경피해)를 가져온다.[6] 위기는 다양한 대상을 위협한다. 일개 회사나 조직의 위기로 인해 해당 산업계 전체가 영향 받을 수 있다.

Lerbinger(1997)는 위기의 속성을 급작성(suddenness), 불확실성(uncertainty), 시간제약성(time compression)을 갖는다고 했다.[10]

위기로 인한 부정적인 결과를 예방하거나 최소화함으로써 위기의 피해로부터 조직에 부정적인 영향을 주는 사건들의 위험성과 불안 요인을 감소시키고 조직이 능동적으로 대처할 수 있도록 하는 전략적인 계획을 수립해야 한다.

Littlejohn(1983)는 비상사태를 피하기 위해 노력하고, 위기 발생에 대비하여 계획하고, 필요할 때에는 그것을 실행에 옮기는 다각적인 조직 차원의 예방(prevention), 실행(performance), 학습(learning)하는 일련의 노력이라고 했다.[5]

국내 대형 정보시스템 개발 전문 기업체와 기관들 몇 군데는 현재 조직 내에 위험관리 모델을 자체적으로 개발하여 적용하고 있는 곳도 있으나 대부분은 프로젝트 관리자에게 일임하는 경향이 아직도 많다.

본 논문은 프로젝트 수행과정에서 발생 될 수 있는 각종 프로젝트 저해요인들에 대해 조사 분석하고 프로젝트가 지연되어 발생할 수 있는 예산과 인력 및 소요기간들에 대한 비효율성에 대해 적절하고 효율적으로 관리 할 수 있도록 하는 모델을 제안하는데 그 목적을 두고 있다.

전 세계적으로 정보기술(IT: Information Technology) 위험관리에 대한 솔루션이나, 추천 할 수 있는 특별한 솔루션이 없는 상태로 조직에서는 주로 외부보안(바이러스 백신, 방화벽, 침입방지시스템, 암호화 등)과 내부보안(접근제어, 문서유출 방지 등)에만 관심이 집중되고 있는 상황이다. IT 기술과 수요자의 정보 욕구가 증가함으로서 이제 조직체 내에서 IT자원에 대한 무결성(Integrity), 가용성(Availability), 기밀성(Confidentiality)에 대한 내. 외부의 정보 및 시스템과 데이터 통제는 물론이고 위험에 대해 종합적으로 관리할 수 있는 시스템 솔루션 개발이 시급히 요구되고 있다.[1]

현재 기업의 전체 IT 전산자원에 대한 내. 외부의 위협(Threat)중, 외부 보안 보다 더욱 중요하고 비중이 큰 내부통제 및 보안관리 분야는 위험이 그대로 노출되고 있는 실정이다. 이에 기업 IT 위험관리(위험식별, 위험분석, 통제설계, 통제구현, 위험모니터링, 위험대응, 발생한 위험 평가, 통제재설계 및 개선)의 일련의 기업 위험관리 프로세스 모델에 대해, 국내 (주) 메타리스크의 정보기술위험관리시스템(ITRMS)의 연구 및 개발 결과를 기반으로 모델에 적용 제안하였다.

Ⅱ. 정보기술 위험관리시스템

정보기술위험관리시스템(ITRMS[1]: Information Technology Risk Management System)이란 기업의 정보기술자원의 기획, 개발 및 운영과 관련된 프로세스(Process), 프로젝트(Project) 및 IT자원 전반에 대한 위험을 통합적으로 관리할 수 있도록 지원하여 주는 시스템이다. 그리고 ITRMS 개념도는 그림 1.과 같으며, 선진국의 정보시스템위험관리시스템 및 권고안은 다음과 같다.

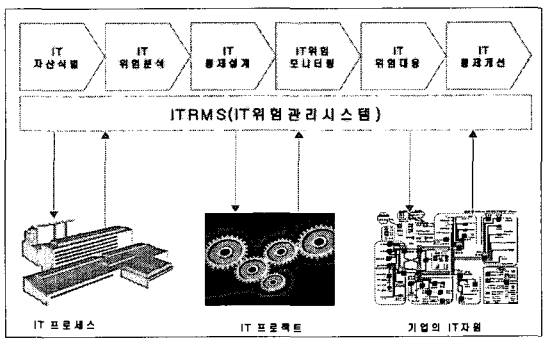

그림 1. ITRMS 개념도
Fig. 1 the ITRMS concept diagram

정보시스템 내부통제 및 감사에 관한 대표적인 국제조직인 ISACA(Information System Audit and Control Association)는 1980년 후반부터 CoBIT(Control OBjectiv

es for IT)[15]이라는 가이드라인을 제시하였으며, COSO (Committee of Sponsoring Organizations of the Treadway Commission)[11]는 ERM(Enterprise Risk Management)[6]에 대한 이해를 촉진하고, 국제적인 실행 기준을 만들기 위해 ERM의 본질적 의미, 구성요소 등으로 이루어진 ERM 프레임워크를 2004년 발표했다.[10]

미국 Carnegie Melon University의 Software Engineering Institute는 위험관리에 대하여 지속적인 위험관리가 중요한 것으로 강조하고 있으며, 캐나다 연방정부는 1999년 자국의 정부기관 및 공공기관의 정보시스템 보호를 위하여 Threat and Risk Assessment Working Guide를 제정 공표하였다.[12]

세계적으로 대표적인 Accounting 펌이자 정보기술 컨설팅 회사인 PWC사 중 스위스 브랜치에서 GRMS(Global Risk Management Solutions) [13]서비스를 특화하여 제공하고 있다.

미국의 표준기구인 NIST[7]는 미 연방정부 및 기관들을 위해 정보기술에 대한 위험관리 지침을 제정하여 이를 사용하도록 권고하고 있다.

반면에 현재 국내 기업에서 사용하고 있는 IT 관리시스템은 주로 NMS(Network Management System), SMS(Server Management System), CMS(Change Management System) 및 정보보호시스템(방화벽, IDS, IPS, 바이러스 백신, 암호화 도구 등) 등 인데, 이들을 통합 계측 및 제어할 수 있는 통합 위험관리시스템 구축이 시급히 요구되는 현시점에 놓여있다.

IT위험관리시스템(ITRMS)의 구조 및 기능구성체계는 궁극적으로 IT위험관리 프로세스 전반의 기능을 자동화하여 위험관리 관련자들이 효과적으로 위험관리를 할 수 있도록 지원해 주는 시스템이다.

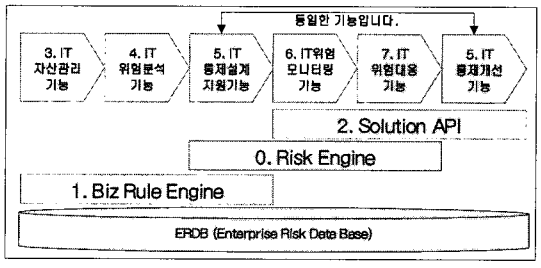

그림 2. ITRMS 기본구조
Fig. 2 the ITRMS Basic structure

ITRMS의 기본구조와 기능에 대해 조사한 결과는 그림 2.와 같다.

2.1 전사적 위험데이터베이스(ERDB) 구축 지원

ERDB 는 전사적인 관점에서 위험관련 데이터인 정보자산, 자산에 대한 위협, 현행 통제대책, 현행 위험취약점, 위험상태에 대한 정보를 기업이 일관성 있고 효율적인 위험관리데이터베이스를 구축할 수 있도록 지원하는 기능을 갖는다.

2.2 IT 자산관리 기능

기업 관점에서 관리하고 보호해야 할 정보자산의 도입, 변경, 유지보수, 사고이력 등의 정보를 저장, 가공, 사용하도록 지원하는 기능이다.

2.3 IT 위험분석기능

자산연동기법, 정보자산 중요도산정기법, 위협시나리오분석기 및 Noun-Verb FDL을 통하여 구축된 위험관련 정보자산, 위협, 현행통제대책, 취약점의 상호연관관계분석을 통해, 기업의 핵심적인 위험에 집중하여 위험을 효율적으로 분석해 주는 기능이다.

2.4 IT 통제설계지원기능

IT 위험분석기능을 통하여 도출된 자산, 위협, 취약점, 현행통제대책, 취약점간 상호연관관계분석을 기반으로 개선하거나 신규로 도입하여야 할 통제대책을 자동 추출하는 기능이다.

2.5 IT 위험모니터링 기능

IT위험모니터링 기능은 두 가지 경로를 통하여 위험상태 정보를 사용자에게 제공하게 된다. 첫 번째는 각각의 process owner에 의한 자체 평가 리포트와 이슈 및 문제발생 보고이며, 두 번째는 각종 솔루션(NMS, SMS, ESM, IPS, ERP, DBMS, Help Desk, CMS, 자동패치지원, 바이러스 백신 등)으로부터 주요 위험관련 정보를 제공 받아 자체 필터링 기능을 통하여 위험을 분류, 적합한 사용자에게 즉시 통보해 주는 기능이다.

2.6 IT 위험대응 기능

IT 위험대응 기능은 IT 위험모니터링 기능을 통하여 사용자에게 통보된 위험을 인지하고 이에 적합한 대응책(위험완화, 비상계획, 백업시스템 가동 등)을 사용자에게 자동으로 연계하여 제공하는 기능이다.

III. ITRMS의 논리적, 물리적 구성

ITRMS(IT위험관리시스템)의 논리적 구성체계는 그림 3.과 같으며, ITRMS의 시스템 주요 기능 구성도는 그림 4.와 같다.[2]

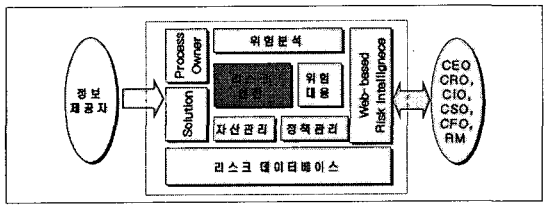

그림 3. ITRMS 논리 구성도
Fig. 3 the ITRMS Logical block diagram

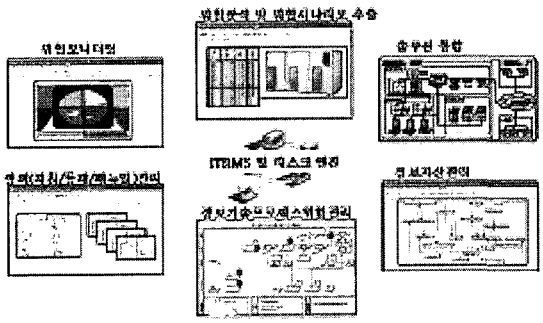

그림 4. ITRMS 기능 구성도
Fig. 4 the ITRMS Function block diagram

VI. ITRMS의 모델링 제안

4.1 시스템 개발 및 운영상 위험관리 서비스의 제공

위험요소를 내포한 개발프로젝트 수행 시 적용되는 개발 생명주기 모델로는 나선형(spiral)모델과 시제품화모델(prototype) 모델이 있다.

일반적으로 IT개발과 관련된 대표적인 위험으로는 신기술적용에 따른 위험, 관련 법규 준수 및 적용에 따른 위험, 비용위험, 일정관리위험, 개발 대상 업무 프로세스의 표준화에 대한 위험, 적정 인력의 관리 및 이탈 방지에 대한 위험, 이슈 및 쟁점관리상의 위험 등이 있다.

4.2 통합 IT자산관리데이터베이스 제공

현재 대부분의 정보이용자는 필요에 따라 응용분야 별로 DB를 별도로 제한된 범위 내에서 구축하고 있어 위험에 적절하게 대처하기 어렵다.

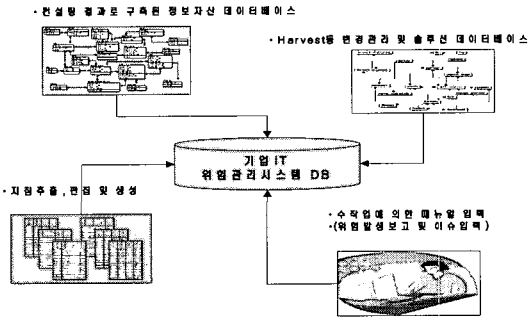

그림 5. 기업 ITRMS 통합 DB
Fig. 5 Enterprise ITRMS integrated DB

ITRMS는 별도의 DB구축 이외에 그림 5.와 같이 다른 솔루션으로부터 IT자산과 위험관련 데이터를 취합하는 IT자산관리데이터베이스 구축을 필요로 한다. 또한, 진단결과의 데이터베이스화 및 IT위험관리시스템 데이터베이스 구축을 위해서 템플릿 진화방식을 사용할 수 있어야 할 것이다.

4.3 응용중요도 분석 및 위험분석 지원

ITRMS는 응용중요도 분석을 통하여 위험분석을 그림 6.과 같이 보다 용이하고 정확하게 할 수 있도록 지원 할수 있어야 한다.

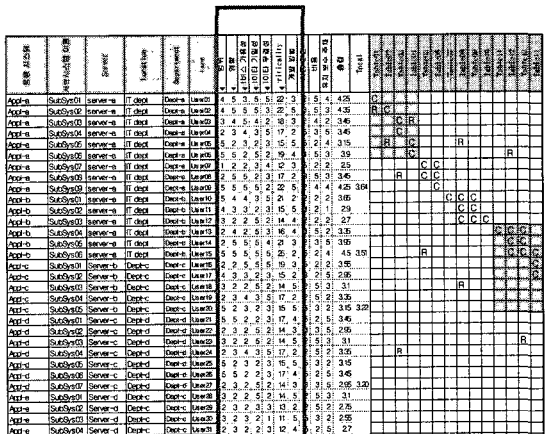

그림 6. ITRMS 응용서비스 중요도 연산 결과
Fig. 6 ITRMS application service important operation result

응용중요도 분석은 기본적으로 기존의 자산가치 분석방법인 임의가중치 방식(매우 중요, 중요, 보통, 낮음, 매우 낮음)에서 탈피하여, 응용의 속성을 국제적으로 인정된 속성(무결성, 기밀성, 가용성)과 사용범위 및 영향도에 따라 구체적인 수치로 전환하는 방식을 의미한다. 이를 통하여 응용자산에 대한 정확한 통제정책이 수립될 수 있어야 한다. 이러한 응용속성별 중요도 책정은 그림 7.과 같이 기업의 정보자산에 대한 다양한 시뮬레이션을 가능하게 해줄 수 있어야 한다.

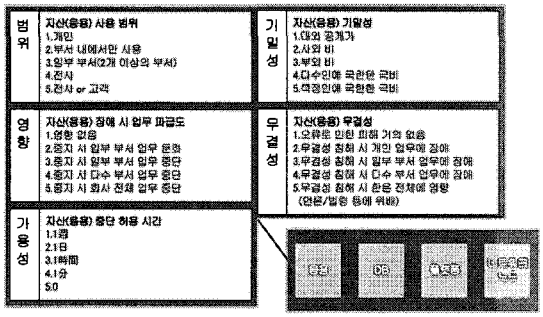

그림 7. 응용서비스 중요도 기준과 자산연동
Fig. 7 Application service importance standard and linked assets

서비스 중요도(Criticality)에 근거하여 조직의 중요자산에 대한 무결성, 기밀성, 가용성을 자동적으로 연산한 결과는 그림 8.과 같다.

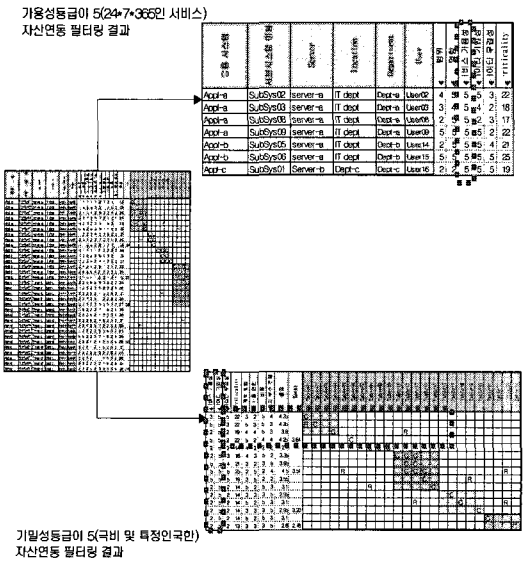

그림 8. 응용서비스 중요도 필터링 연산결과
Fig. 8 Application service important filter ring operation result

4.4 자산연동설계

자산연동설계에 따라 응용중요도 분석으로 전체자산에 대하여 자산 중요도를 계산할 수 있도록 지원해야 한다. 모든 응용은 데이터와 관련을 가갖고, 모든 응용은 하드웨어 플랫폼을 기반으로 하여 모든 응용은 사용자와 관리자가 존재하며, 또한 네트워크 트래픽 유형에 따라 경유해야 하는 네트워크노드(예 : 라우터, 스위치, 방화벽, 허브 등)와 링크(내부망, 무선망, 백본망, VPN 등)가 결정되어야 한다. 그림 9.는 이러한 정보자산간 관계 연동을 실제 시뮬레이션 하기 위해 만든 정보자산 연동설계 예시이다.

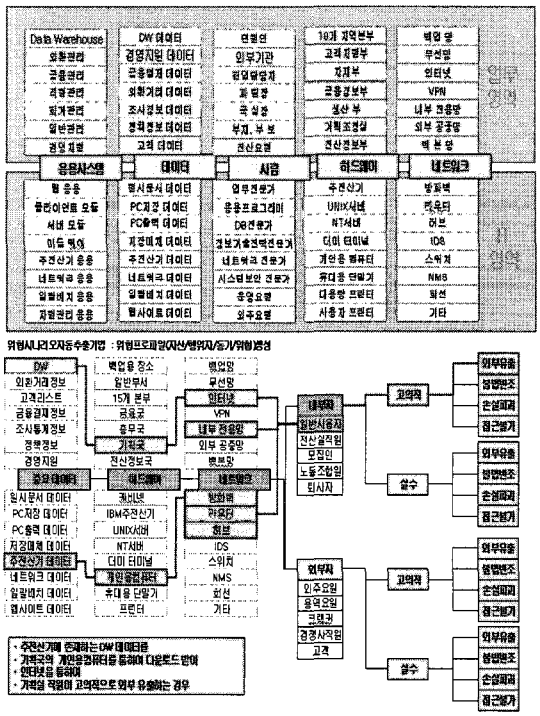

그림 9. 자산연동기법의 작동방법
Fig. 9 Operational method of the linked assets technique

4.5 프로세스 식별 및 위험관련 지표의 추출

ITRMS는 프로세스 지향적 이여야 하며, 다른 위험분석 및 취약점분석 툴들은 자산 중심의 위험분석을 실시하는데, ITRMS는 자산과 프로세스를 연계하여 위험을 분석해야 한다. 따라서 기업의 핵심프로세스를 식별하고, 각 프로세스별로 중요한 목적과 처리규칙(rules, control, risk range 등)을 정의 및 확인하여, 프로세스가 작동 중에 목적과 처

리규칙에 위배되는 트랜잭션이나 이벤트의 발생을 사용자에게 알려주고, 그림 10.과 같은 시나리오를 갖고 사전에 사용자가 능동적으로 내외부의 위협에 대처할 수 있도록 지원해야 한다.

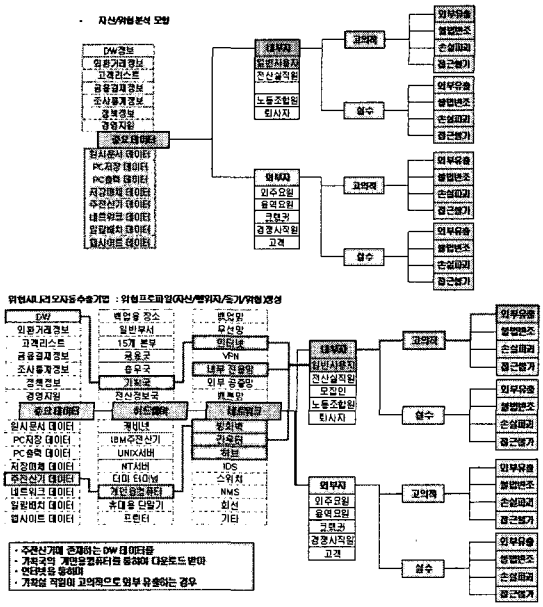

그림 10. 위협시나리오 자동추출기법
Fig. 10 Threat scenario automatic extraction technique

특히 그림 11.과 같이 위험지표를 통해 위험발생을 예보하는 Predictive Risk Indicator, 위험을 발생을 알려주는 Risk Sensor, 발생한 위험을 확인하고 추적하여 주는 Det ective Risk Indicator, 위험과 관련된 통계처리를 위해 필요한 Cumulative Risk Indicator로 구분하여 위험관련 정보를 수집, 처리, 제공해야 한다.

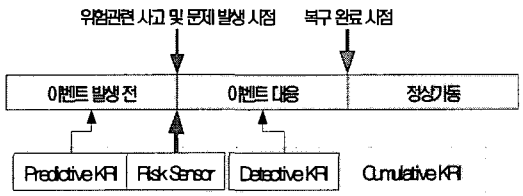

그림 11. 각종 이벤트와 KRI 유형
Fig. 11 Various event with KRI type

4.6 위협시나리오의 자동 생성

ITRMS는 위협시나리오작성엔진을 통하여 각 자산 간의 연동과 행위자와의 연계에 기초하여 주요 위협시나리오를 자동으로 생성하여 사용자에게 제공해야한다. 위협시나리오는 우선 각 자산연동(관계형테이블의 관계연산을 통하여 실시)에 의거 정보자산 노드링크를 트리구조로 생성해야 한다. 즉, 주요 행위자에 따라 접근된 주요자산별로 순차적으로 노드링크트리를 생성해야한다.

4.7 위험분석결과에 대한 통제설계 자동 지원

중요자산을 중심으로 하여 파악된 위협, 기존 통제대책과 취약점에 대한 시뮬레이션을 바탕으로 최적의 통제설계를 사용자가 선택 할 수 있도록 지원해야한다. 여기서 주로 사용되는 기법은 Noun-Verb type에 근거한 자산, 위협, 취약점, 위험 및 통제대책의 정의와 각 서술구조에 대한 상호참조기술이다.

ITRMS에서는 자동으로 추출한 위협시나리오에 대하여 현재의 통제대책을 사용자가 선택(마우스 클릭)하면 현재의 취약점이 확정된다. 이어서 사용자는 확정된 현재의 취약점에 대응하는 통제대책권고안을 컴퓨터 화면을 통하여 선택함으로써 그림 12.와 같이 필요로 하는 시스템 통제 대책과 지침과 메뉴얼이 만들어진다.

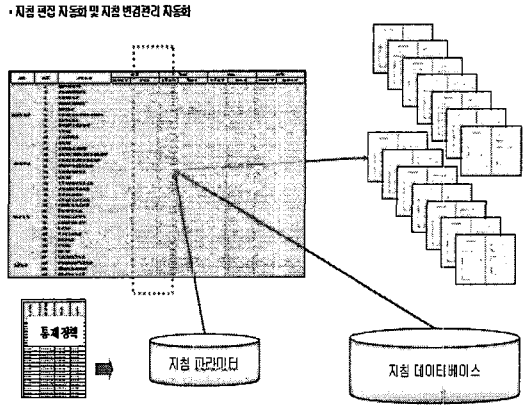

그림 12. ITRMS 의 지침 자동편집 기능
Fig. 12 Guide automatic editing function of ITRMS

4.8 ITSM 솔루션 통합 Risk 서비스 제공

ITSM(IT Service Management)의 국제표준인 ITIL(IT Infrastructure Library)[14]에 기반 하여 주요 ITSM 솔루션 업체의 도구를 통합하여 사용자에게 위험관련 정보를 통합적으로 제공해야한다. 이러한 ITSM 솔루션 통합을 통하여 ITSM 전체의 프로세스에 대한 위험관리 자동화를 용이하게 구현할 수 있을 것으로 판단한다.

4.9 위기 유형과 문제점

위기로부터 안전한 조직은 하나도 없다. 위기는 예측하지 못한 상태에서 발생한 사건이며, 잘못 대처할 경우 조직, 산업 또는 스테이크 홀더들에게 부정적인 영향을 미칠 수 있는 중대한 위협이다. 또한 위기의 유형에는 자연재해, 악의, 기술적 문제, 인적 문제, 도전, 대규모 피해, 조직의 범죄, 작업장 폭력, 루머가 있는데 이중 기술적문제와 인적문제, 대규모피해, 조직의 범죄 등이 있다.

4.10 위험관리 수행절차를 감안한 센서구성

본 논문에서는 이들을 감안한 ITRMS 체계구축을 위한 모델링의 제한된 범위라고 생각하고, 이들 시스템을 개발하기 위해 그림 13.과 같은 수행 절차를 감안하여 센서를 구성하도록 제안한다.

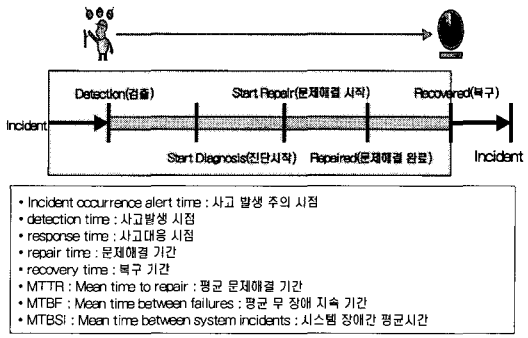

그림 13. 위험관리 수행절차
Fig.13 Risk Management official accomplishment process

4.10.1 응용센서

KRI와 관련된 통제 컴포넌트를 응용에 삽입하여 KRI관련 이벤트나 트랜잭션을 검출할 수 있어야 한다.

4.10.2 DBMS센서

DB내 주요 테이블의 핵심 컬럼에 대한 무결성 로직(Domain Integrity)을 삽입하고, 트랜잭션 시 KRI에 해당하는 DB트랜잭션을 검출할 수 있어야 한다.

4.10.3 System 관리 도구 Agent 센서

NMS(Network Management System), SMS (Server Management System), CMS (Configuration Management System) 등 시스템관리도구가 설치된 서버에 로드 되어 KRI 관련 트랜잭션 및 이벤트를 검출할 수 있어야 한다.

4.10.4 보안관련 포인트 솔루션 센서

외부보안과 관련된 방화벽, IPS, 백신프로그램 및 외부의 주의 및 긴급메일 등에서 KRI 관련 이벤트나 트랜잭션을 검출할 수 있어야 한다.

4.10.5 기타 종합적인 구성체계 및 개념설계

필요시 출입통제장치관리시스템, 원격모니터링시스템, 경비관리시스템 등과 연동하여 KRI 관련 이벤트나 트랜잭션을 검출할 수 있어야 한다.

그리고 IT위험관리시스템 기술 사양에 있어 IT위험관리시스템 데이터베이스 기본 구조는 기본적으로 전사적(Enterprise)차원에서의 정보자산 통합관리가 가능해야 할 것이다. 또한 각 정보자산 간의 연동을 고려하여 설계되어야 할 것이다.

이러한 연동은 저장된 자산 스펙, 자산 히스토리, 자산관련 위협, 위협에 대한 현재의 통제대책, 존재하는 취약점 그리고 개선하거나 신규로 도입해야 하는 통제대책을 FDD(Formal Descriptive Definition)에 의해 분류하여 저장함으로써 각 위험관리 요소들 간의 정확한 상호협력과 추적가능성을 확보하도록 설계되어야 할 것이다.

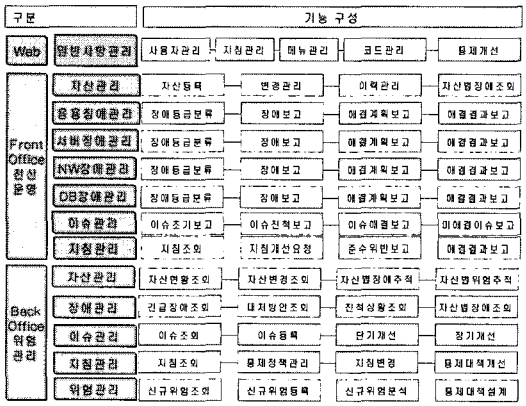

그림 14. ITRMS 기능 및 메뉴체계도
Fig.14 the ITRMS function and menu system

그리고 IT위험관리시스템 기능구성도는 그림 14.와 같이 크게 관리대상인 전산자원의 운영을 담당하는 Front Office와 이에 대한 위험관리를 담당하는 Back Office의 두 서브시스템으로 구성되어 이들 상황을 Web 상에서 볼 수 있도록 한다. 그리고 각각의 핵심은 보호하고 관리해야 정보자산에 대한 각종 위험의 발생예보, 발생경보, 발생상황추적, 대응프로세스 전개, 사후보고 및 위험평가, 개선대책의 이행 등을 지원할 수 있도록 설계되어야 하는데 그림 15.와 같이 데이터베이스를 개념설계 했다.

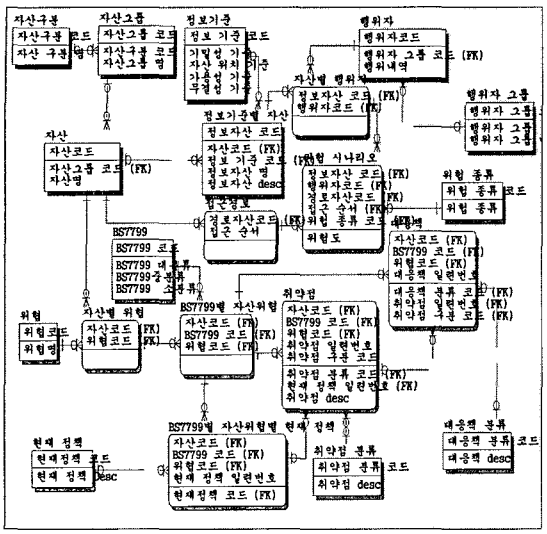

그림 15. ITRMS DB 개념설계
Fig.15 the ITRMS DB conceptual design

V. 결론

본 논문에서는 국내. 외 위험분석 프로세스를 조사, 분석하여 기본모델을 설정하였으며, ITRMS 연구 및 개발 결과와 관련 툴을 사용하여 시뮬레이션 하였다. 그 결과 향후 국내에서정보시스템 위험관리 시스템에 대한 확대 적용을 통한 실험적 데이터가 축적될 경우, 각종위험 요소들에 대한 종합적인 관리가 예상 되었다. 그리고 안정적 관리를 위해 다양한 분야에 적용, 실제적인 실험데이터를 얻어서 패키지화하는데 계속적인 연구가 필요하다고 판단하였다.

참고문헌

[1] 이형원, 정보통신부, "IT창업경진대회 ITRMS 출품 명세서", 2004

[2] (주)메타리스크, "IT위험관리시스템 제품 사양서", 2006

[3] e-TQM, "위험관리", 삼성SDS, 2003

[4] ARM standard, AIRMIC,ALARM,IRM, 2002

[5] Annual defense report, www.dod.mil/ ex-ecsec/adr2003/index.html, 2003

[6] "Enterprise Risk Management", Jerry, Micccolis, Samir Shah, 2000

[7] NIST, "Computer Security Resource Clearinghouse",http://csrc.nist.gov/

[8] Gary Stonebumer, Alice Goguen, and Alexis Feringa,"Risk Management Guide for Information Technology systems", NIST, 2001

[9] ISO/IEC Guide 73,"RM Terminology Guidelines for use in standard", 2000

[10] ITGI, "IT Control Objectives for Sarbanes-Oxley", 2004

[11] COSO, "Enterprise Risk Management", http://www.aon.com/us/busi/risk_management/risk_consulting/ent_risk_mgmt/default.jsp

[12] CSE, "Threat and Risk Assessment Working Guide", 2006 http://www.cse-cst.gc.ca /publications/gov-pubs/itsg/itsg04-e.html

[13] PricewaterhouseCoopers, "Channel Islands: GRMS Services, http://www.pwc.com

[14] Office of Government Commerce. ITIL Refresh Statement. Retrieved February 13, 2006.

[15] ISACA, "serving IT governance professionals-COBIT online", 2006

저 자 소 개

김 태 달

1979.2. 숭실대학교 전자계산학과(學士),
1992.2. 숭실대학교 정보과학대학원 (碩士)
1997.2. 숭실대학교 대학원 컴퓨터학과 (工學博士)
1986.08.04 정보처리기술사
2004. 6.3 국무총리상 수상(제17회 정보문화의달 국가정보화유공자로 선정)
1997.03.01~2006(현재). 청운대학교 컴퓨터학과 교수
2003.12.05~2005.12.31. (사)한국정보통신기술사협회 감사
2006.03.01~2006(현재).한국정보처리학회 UTS연구회위원장

〈관심분야〉 정보시스템 감리, u-CITY, ITS, GIS 등 컴퓨터 응용분야