전산감리의 항목별 연관관계가 계량화에 미치는 영향에 관한 연구

신승중*, 김현수**
*중부대학교 정보공학부
** 국민대학교 정보관리학과

A Study on the Effect of the Relation-by-Item of the Computer Audit to the Quantification

Shin-sungjung*, Kim-hyunsoo**
* School of Information Engineering, Joong Bu University
**School of Management Information Management, Kookmin University

요 약

현재까지 연구되고 있던 정보보호관련분야의 계량화방법을 좀 더 다른 방법으로 접근하여, 정보시스템 환경 하에서 보안 및 관리 운영 평가 지수에 계량화하여 1차 집단과 2차 집단간의 차이를 연구하였다. 정보화 관련항목에 대하여 빈도 분석을 적용함으로서 군별, 항목별 분류를 통한 항목 비례 가중치법을 산출하였다. 또한, 선지정 가중치법을 이용하여, 보호지수와 관리운용지수에 따른 상관관계를 조사하여 안전관리 지수를 계량화 하였다.

제 1 장 서 론

1. 개 요

정보시스템의 환경 하에서는 정보화의 역기능인 보안사고 및 그 피해가 증대되고 있다고 한다. 그러므로, 정보시스템 구축 및 유지보수에 있어서 정보의 안전을 도모해야 한다는 필요성이 강력히 대두되고 있으며, 특히 신뢰할 수 있는 대 국민 서비스를 제공해야 하는 공공기관의 정보시스템 구축사업에 있어서 시스템보안은 더 이상 선택의 문제가 아닌 필수 기능으로 인식되고 있으며, 기업도 이와 마찬가지이다. 그러므로 이러한 정보자산은 대내적으로 설계, 구축상에 내재되어 있는 보안취약성을 가지고 있으며, 대외적으로는 자산이 보유하고 있는 가치에 따라서 끊임없이 조직의 내·외부인에 의한 도전을 받고 있다. 이러한 요인들에 의해 정보자산은 다양한 위험에 직면해 있으며, 사고 발생시 커다란 손실을 기업, 공공기관등의 조직에게 입힐 수 있다. 따라서 이러한 위험을 봉쇄하거나 감소시키기 위해서는 정보시스템을 효과적으로 통제할 수 있는 기능과 역할이 필요하다. 이러한 측면에서 정보시스템의 보안/통제 감리지침 개발은 조직의 자산에 대한 정보보호활동을 객관적으로 점검할 수 있는 지침을 제시하게 될 것이다.

정보시스템 보안/통제 감리지침의 개발은 정보시스템 감리활동이 활성화되면서 감리수행시, 감리활동에 대한 객관성 및 공정성을 부여하고 감리인에 대한 자질향상을 위한 지침서로 제시하기 위한 것이다. 이는 향후 보안/통제 감리지침을 적용하게 될 공공부문의 정보시스템 보안/통제 감리지침의 표준으로 활용코자 함이며, 이를 통하여 공공부문 정보시스템 보안/통제에 대한 안전성 및 신뢰성을 보장하기 위한 목적으로 연수하려 한다.

정보시스템이 행정, 금융, 산업, 교통, 군사 분야 등 국가 사회전반에 보급되어 활용됨에 따라 그 정보시스템을 교란시키거나 파괴, 무력화시키는 것이 엄청난 손상과 피해를 입힐 수 있을 뿐 아니라 궁극적으로는 공격목표와 수단이 될 가능성이 증대되고 있기 때문이다.

정보범죄가 날이 갈수록 지능화되고 악성화 됨으로써 그 피해가 이제는 정보자체의 손상에 국한되는 것이 아니라, 시스템 전체의 기능을 마비시키거나 파괴함으로써 개인이나 기업은 물론 궁극적으로는 국가의 안위까지도 위협하는 상황에 이르렀기 때문이다.

오늘날 세계각국은 나라마다 각기 국가정보 기반구조(NII) 구축에 많은 투자와 심혈을 기울이고 있다. 그런데 그 국제정보화사회 (GIS:Global Information Society)의 기본철학이 개방화 민주화에 기조를 두고 있기 때문에 각 나라는 자국의 중요 정보를 철저히 보호해야할 심각한 국면에 봉착하고 있다. 바로 이러한 국면의 위협과 대응상황을 정보전 즉 사이버 전쟁(Cyber War)으로 표현하고 있는 것이다.

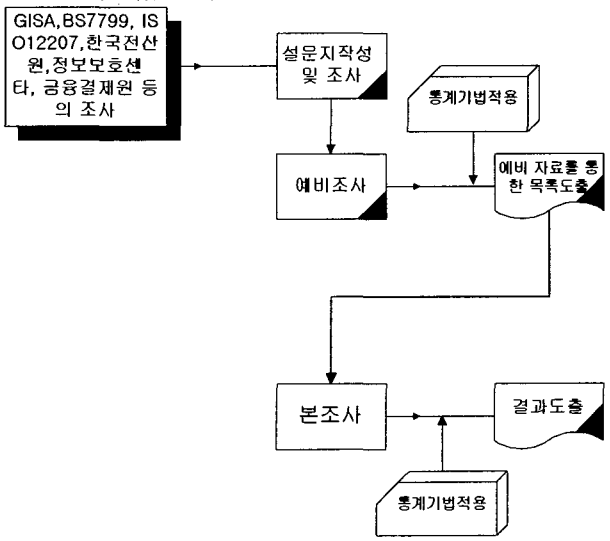
2. 연구의 내용

국내 기업에서의 정보보호에 대한 인식은 몇몇 대기업을 중심으로 이루어지고 있었으며 정보보호를 기반사업으로 하는 기업들이 최근에 와서 중소기업 형태에서 벤

처기업 형태로 다양한 제품개발과 신기술 확보로 국가적인 경쟁력을 갖추고 있다고 볼 수 있겠다. 이러한 기업의 환경에서 실제 보안상태와 운영상태, 그리고, 시스템 환경과 안정성 대책, 전산센터, 하부조직 및 지정의 4가지 군의 형태로 나누어 각각이 지니고 있는 보호지수(S), 관리운영 지수(O), 보호지수와 관리운영 지수를 산출하여 안전관리 지수를 항목에 속성별로 선형계획법을 적용하여 도출하는 군별 선별지정 가중치법과 각 군별 항목수 비례 가중치법을 적용 항목비례 가중치법을 산출하여 각각 비교함으로써 어떠한 방법이 보안감리 및 관리운영 평가에 용이한 방법이 도출될 것인가에 연구에 초점을 두고 있다. 그리고, 외국에서 적용되고 있는 정보 보호에 여러 가지 분야를 점검하며, 본 연구에서 1차집단 전문가과 2차 전문가집단을 대상으로 보안관리 상태 및 운영 실태를 연구하였다.

3. 연구방법

본 설문의 내용은 한국전산원의 감리표준안과 정보보호센타, BS7799, 금융결제원, 등의 자료와 본연구의 예비조사시 사용했던 예비자료를 근거로 작성하였다.



제 2 장 전산감리의 이론적 고찰

1. 용어의 정의

요구사항(Requirement) : 문제해결을 위해 사용자가 원하는 조건이나 능력, 계약서나 표준, 명세서, 기타 다른 공식적인 문서를 만족할 수 있는 시스템 구성요소에 해당하는 조건이나 능력

시스템 요구사항(System Requirement) : 시스템 요구사항에는 개발되어질 시스템의 특정 의도가 명시될 수 있어야 하는데 시스템의 기능, 능력, 안전, 보안, 인터페이스, 운영 및 유지보수, 설계 제약사항 등이 이에 해당됨.

소프트웨어 요구사항(Software Requirement) : 소프트웨어 요구사항에는 사용자 요구사항을 포함하여 구축하고자 하는 시스템의 기능적(function), 업무적(business) 측면으로 개발되는 응용시스템에 대한 요구사항을 의미.

보안 요구사항(Security Requirements) : 권한이 없는 사람/ 시스템이 정보를 읽거나 수정할 수 없도록하며, 권한이 없는 사람/ 시스템이 그것들에 대한 접근을 거부하지 않도록 하는 정보보호에 관한 요구사항.

품질 요구사항(Quality Requirements) : 수행하느냐를 나타내는 측정 가능한 속성과 원하는 목표수준, 품질요건은 신뢰도, 사용성, 적용성 요건들로 분류

기능 요구사항(Functional Requirement) : 시스템이나 소프트웨어에서 수행해야 할 사항을 명시하는 요구사항

감리기준(Audit Standard) : 각 활동에서 이루어지는 태스크, 산출물들이 방법론과 관련없이 반드시 수행되어야 하는 사항들.

감리방법(Audit Standard) : 각 활동에서 이루어지는 태스크, 산출물들이 방법론과 관련 없이 반드시 수행되어야 하는 사항들.

시스템 감사(System Audit) : 감사 대상으로부터 독립적이고 객관적인 입장의 시스템 감사인이 정보시스템을 종합적으로 점검 및 평가하고, 조직체의 장에게 조언 및 권고하는 동시에 Follow-up 하는 일련의 활동.

시스템 감사인(System Auditor) : 다음과 같은 지식 및 능력을 가지고 시스템 감사에 종사하는 사람.

(1) 정보시스템에 대한 기본지식
(2) 시스템감사에 대한 지식
(3) 시스템감사 실시 능력
(4) 시스템감사 실시에 관한 지식

비밀성(Confidentiality) : 정보가 비인가된 개인, 개체 또는 처리(processes)과정에서 누설되거나 공개되지 않는 특성

무결성(Integrity) : 자료가 의도적이거나 비의도적으로 변경, 파괴되지 않는 특성

가용성(Availability) : 인가된 개체(entity)가 요구할 때 정보기술 자원에의 접근과 사용을 가능케 하는 특성

감사(audit) : 시스템에 취해진 활동이나 기록을 독립적으로 검토하여 시스템 보안 방침이나 절차, 통제의 적절성이나 준수여부를 확인하고, 문제점들을 권고해주는 절차.

감사추적(audit trail) : 시스템 접근단계에서 종료단계까지의 일련의 과정에서 행한 모든 활동을 재생, 검토, 조사할 수 있는 시스템 활동의 시간별 기록

로그(log) : 시스템 사용에 관련된 전체의 기록, 즉 입출력내역, 프로그램 사용내역, 자료변경내역, 시작시간, 종료시간 등의 기록

보안대책(safeguard) : 시스템의 취약성, 위협 등을 줄이기 위한 보안기능이나 기법, 절차, 기술, 보안 통제와 유사함.

보안통제(security control) : 보안방침을 실현하기 위해 필요한 요구사항이나 준수사항을 언급한 일련의 규칙

보안성 평가(security evaluation) : 보안기능이 보안 요구사항이나 보안평가기준을 어느정도 만족시키는지 기술적으로 평가하는 과정

보증(assurance) : 보안기능이나 보안제품이 보안방침에 따라 적절히 수행되는 지에 대한 신뢰도

위험분석(risk analysis) : 시스템 자산, 위협, 취약성, 영향 등을 분석하여 효과적인 보안대책을 수립하는 과정.

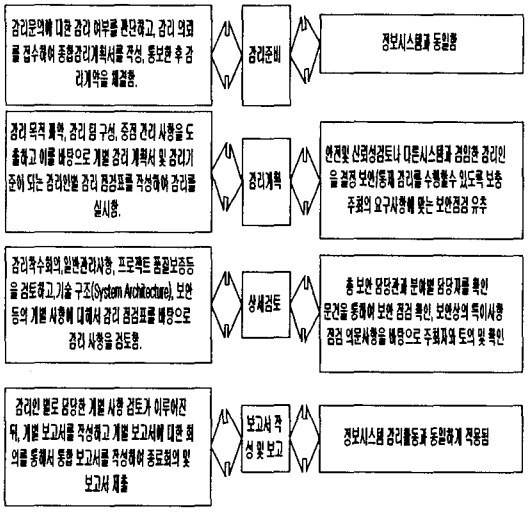
위협(threat) : 자산에 손상을 입힐 수 있는 위험의 원천

접근통제(access control) : (1)다른 주체와의 통신, 또는 컴퓨터 시스템이나 네트워크의 기능 및 서비스의 사용 등을 위한 주체의 권한이나 능력의 제한, (2)개체에 대한 주체의 접근을 제어하는 기능

취약성(vulnerability) : 위협에 의해 이용될 수 있는 자산내의 약점

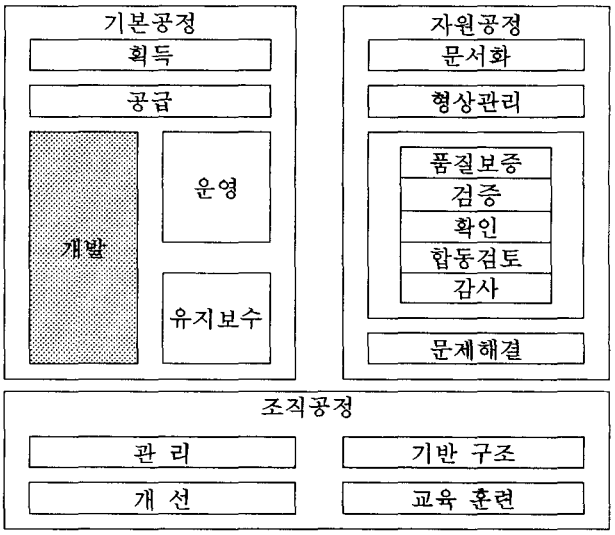
2. 감리의 절차

정보시스템 감리수행 절차는 주관기관의 감리의뢰를 바탕으로 한 감리 준비 단계부터 시작되어 기초자료분석, 감리팀 구성, 중점감리사항과 감리기준을 선정하는 감리계획 수립단계, 착수 회의, 프로젝트 표준, 품질을 검토하고 데이터베이스, 응용시스템, 기술아키텍처등에 대한 상세 검토 단계를 거쳐서 감리 종료 회의 및 보고와 최종보고서를 제출하는 보고서 작성 및 보고단계로 진행된다. 감리인의 관점에서 바라 본 감리절차는 그림과 같다.



3. ISO/IEC의 기본공정

보안관리측면에서 정기적, 주기적 수행 과 수행기관의 요청에 의하거나 의무적 수행이 타당하며, 현재운영하고 있는 감리에 따른 비용과 효과를 종합적으로 고려되고 있다.



정보시스템 감리지침 범위

※지원공정과 조직공정의 일부분이 포함됨

IOS/IEC 12207의 기본구조

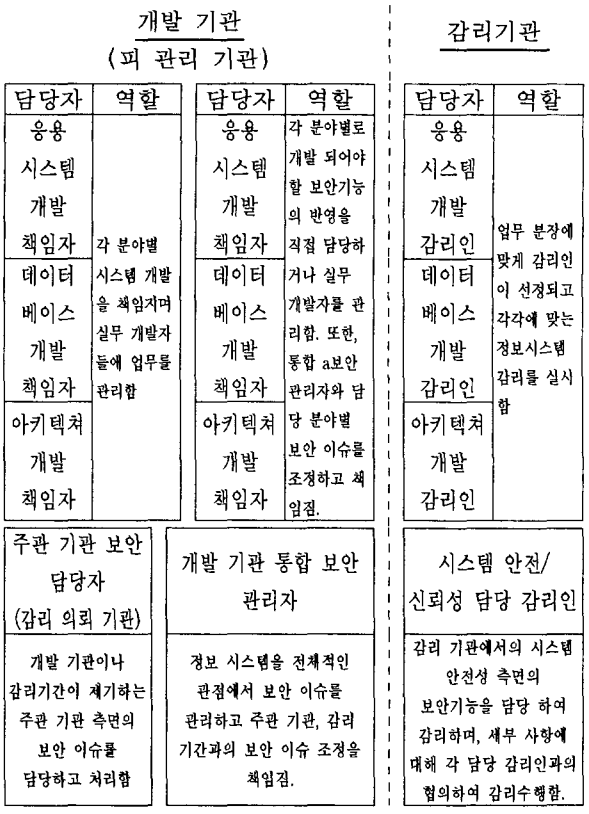
4.감리시기

1) 감리의 적시성

본 연구에서는 시스템 개발공정에 따른 보안감리사항을 연구하고자 하므로, 감리시기에 따른 보안점검사항의 변화를 고려하여야 한다. 다시 말하면, 시스템 분석단계 이후에서는 보안계획서의 수립(계획단계)의 여부와 보안분석과정에서 도출된 분석서를 점검하여야 하며, 설계단계 이후에서는 분석과정에서 도출되었던 보안쟁점들을 바탕으로 구성된 통합 정보보호체계(Security Architecture)에 대한 문건들을 확인하고, 구축단계에서는 설계된 보안기능들의 실제 적용여부를 검토하는 보안/통제 감리를 예상할 수 있다. 또한, 감리시기가 구축단계 한번만 이루어 질 경우에는 최종감리보고서만을 제출하므로 주관기관은 본 감리 보고서에서 지적된 사항들에 대한 검수작업을 직접 확인해야겠지만, 두 번 이상의 감리가 이루어 질 수 있다면, 감리인은 처음 감리시 지적된 사항들에 대한 이행여부를 확인하고, 그에 따른 보고서를 작성할 수 있다.

2) 감리의 조직성과

보안감리시에 고려되어야 할 또 다른 사항으로는 보안기능이 개발기관에서 선임한 담당자 한 사람에 의해서 개발되어 지는 것이 아니라는 사실이다. 따라서, 감리인이 데이터베이스 보안 및 응용시스템 보안에 대한 보안기능을 살펴보려고 한다면, 개발기관의 통합 보안관리자와 함께 각 분야별로 선임 또는 겸임으로 선정된 응용시스템 보안담당자와 함께 검토해야 한다는 것이다. 마찬가지로, 네트워크 보안사항과 서버 보안사항을 검토하고자 한다면, 시스템 아키텍처를 그림과 같이 나타 낼수 있다. 물론, 프로젝트의 규모와 특성에 따라서 개발기관이나 감리기관의 담당 조직이 다르겠지만, 일정규모 이상의 큰 프로젝트에서는 본 그림과 같이 담당자들이 별도로 선임되어 있을 수 있으며, 규모가 적은 프로젝트에서는 일반적으로 겸임으로 프로젝트 수행 조직이 구성될 수 있겠다.



<그림 정보시스템 개발기관과 감리기관의 관계>

외국의 정보보호 수준

미 국방부에 의해서 1981년에 설립된 CSC(Computer Security Center, 1985년에 NCSC로 바뀜)는 안전한 전산시스템의 이용을 촉진시키기 위해서, 1983년에 전산체계 평가기준 (TCSEC; Trusted Computer System Evaluation Criteria, 표지 색깔 때문에 "Orange Book"이라고도 함)을 제시했다. 이 기준은 전산시스템의 보안성을 효과적으로 평가하기 위한 기본적인 요구사항을 정하고, 그 요구사항에 따른 평가등급을 부여하고 있다. 또한, 이러한 기준이 사용되는 영역은 보안제품의 공급자, 이용자, 평가자 등이다. TCSEC은 접근제어방법에 근거

해서 보안시스템이 접근하는 주체와 그 대상인 객체를 관련 데이터베이스 시스템을 통해서 제어한다는 관점에서 다음과 같은 요구사항을 갖고 있다. 이에 대한 것으로 시스템 환경은 강제적 보안정책(인가받지 않은 사람은 비밀자료에 접근 할 수 없음)과 임의적 보안정책(선택된 사용자만이 자료에 접근 할 수 있음)이 있고, 안전성 대책은 접근 대상이 되는 자료에 대한 보안등급을 식별하는 표지(label)를 표시할 수 있어야 한다. 그리고 전산센타는 누가 자료에 접근하고 어떤 자료가 허가되는지, 접근하는 주체와 객체에 대한 신분확인과 허가자료는 명확하게 식별되어야 한다. 또한 하부조직 및 지점은 보안관련 사건들의 발생이 기록되어서 감사자료로서, 추적이 가능하도록 유지/보호되어야 한다. 보증 또한 위 4가지 요구사항을 실행 및 평가할 수 있는 하드웨어/소프트웨어 기법이 운영되어야 한다. 끝으로 지속적 보호는 이러한 기본적 요구사항들은 간섭 및 비인가 된 변조로부터 지속적으로 보호되어야 한다.

위 요구사항을 기반으로 해서 원격접근 전산체계에서 처리되는 비밀 정보에 대한 위협을 감소시키기 위해서 다음과 같은 안전관리평가기준을 제시했다. 안전관리평가기준의 분류기준을 크게는 6가지로 구분하고, 존재여부에 대한 6과 존재하지만 사용이 불가할 때 5, 불량 4, 보통 3, 우수 2, 최우수 1 로 세분하고 있으며, 각 분류기준 별로 시스템환경, 안전성대책, 전산센터, 하부조직 및 지점에 대한 내용을 기술하고 있다.

영국에서는 국내 표준인 정보보안관리 지침(BS7799, Code of Practice for Information Security Management)을 토대로 이를 국제 표준 (ISO/IEC JTC1 SC27 TR13335, Guidelines for Management of Information Technology Security)에 적극 반영시키고 있으며 유럽연합 국가에서의 유사한 작업(독일의 IT Baseline Protection Manual 등)에 공동 작업을 수행하고 있다. 또한 BS7799에 대한 인증제도(accreditation)를 마련하여 정보보호 수준을 평가하고 있으며 이러한 인증체계를 타국에도 적용시키려는 노력을 시도 중이다. 참고로 BS7799에서 제시하는 주요 내용을 살펴보면, 우선 보안정책에서 시작되어 보안 조직과 그 하부 구조로 정보보안 기반구조, 제 3자 접근 통제가 있으며, 자산의 분류와 통제에 있어서는 자산에 대한 책임 추적성과 정보의 분류가 있다. 또한, 인사 보안은 직무상의 보안, 사용자 훈련, 보안사건 대응이 있으며, 물리적, 환경적 보안에는 보안구역과 설비 보안이 있다. 컴퓨터 및 네트워크 관리에는 운영절차와 책임, 시스템 계획과 검수, 바이러스, 유지보수, 네트워크 관리, 저장매체 처리와 보안, 데이터와 소프트웨어 전송시 보안이 있으며, 시스템 접근제어서는 다양한 관계를 유지시키기 위하여 시스템 접근에 대한 비즈니스 요구사항, 사용자 접근관리, 사용자 책임, 네트워크 접근제어, 컴퓨터 접근제어, 응용시스템 접근제어, 시스템 접근 및 사용 감시가 있다. 이는 물리적 보안과 사용자간의 신뢰성과 타당성을 중시여기는 요인으로 볼 수 있으며, 특히, 시스템 개발 및 유지보수에서는 시스템 보안 요구사항, 응용시스템 보안, 응용시스템 파일 보안, 개발 및 지원환경이 있고, 업무지속성 계획과 준거성이 이 마련되어 있다. 이중에서 준거안에는 법/제도 준거, 정보기술시스템의 보안 검토, 시스템 감리 고려사항등이 들어 있다.

합계(total)	1군	2군	3군	4군
s	844	2050	978	545
o	1851	1711	4869	1790
cso	2,695	3,761	5,847	2,335

합계*평균(total)	1군	2군	3군	4군
s	2476.00	6157.75	2469.56	1373.80
o	5001.31	4953.21	12553.88	4586.50
cso	7,477.31	11,110.96	15,023.44	5,960.3

합계(기업)	1군	2군	3군	4군
s	514	1321	601	336
o	1198	1131	2992	1085
cso	1,712	2,452	3,593	1,421

합계*평균(기업)	1군	2군	3군	4군
s	1417.71	4118.56	1478.78	829.20
o	3344.88	3472.07	7618.23	2683.19
cso	4,762.59	7,590.63	9,097.01	3,512.39

합계(은행)	1군	2군	3군	4군
s	241	554	289	161
o	493	442	1472	546
cso	734	996	1,761	707

합계*평균(은행)	1군	2군	3군	4군
s	669.286	1393.00	694.778	383.40
o	1118.06	1022.14	3655.02	1358.25
cso	1,787.346	2,415.14	4,349.798	1,741.65

합계(정부)	1군	2군	3군	4군
s	89	175	88	48
o	160	138	405	159
cso	249	313	493	207

합계*평균(정부)	1군	2군	3군	4군
s	389.000	646.188	296.000	161.20
c	538.375	459.000	1280.63	545.063
cso	927.375	1,105.188	1,576.63	706.263

제 3 장 정량적방법의 접근

정보시스템의 보안 및 관리운영 평가지수의 계량화를 위한 검사항목을 일반적인 방법에 따라 4개의 군(시스템 환경, 안전성 대책, 전산센터, 하부조직 및 지점)과 세부항목으로 분류하였으나 각 항목별 상태를 6개의 등급으로 분류, 측정치를 세분함으로써 무형 및 유형자산의 감가상각에 따른 복제구비용 산출의 적정화를 도모하였다. 그리고 각 군의 항목별 속성을 정보보호 관련항목, 관리운영 관련항목 또는 공통의 항목으로 분류하여 군별, 속성별 및 종합평가지수를 산출함으로써,

i 군별 상대적 위험요소의 복구 (localization)

ii 정보시스템 운영 주체의 운영 성격을 반영한 계량화 (characterization) 을 모색하였다.

평가지수 산출을 위하여 본 연구에 적용한 방법으로서, 방법 I (군별 항목비례 가중치법)에서는 군별 항목수 비례 단순 가중치를 적용하였다. 방법II(군별 선지정 가중치법)에서는, 가중치의 산출을 위하여 군별과 항목의 속

성별로 선형계획법을 적용하였다.
방법Ⅰ에서 적용한 가중치는 군별 체크리스트의 도수에 따른 상대적 비중을 반영한 것으로 방법Ⅱ에 의하여 얻어진 결과와의 상호 연관성을 기대할 수 있다.

방법Ⅰ. 군(Group)별 항목 비례 가중치 법

1. 군별 비례상수 : $\mu_i = \dfrac{N_i}{N}$, N : 총 문항 수
   , N_i : i 군의 문항 수
   (a) 군별 보호지수 비례상수 : $\mu_i^s = \dfrac{N_i^s}{N^s}$,
   N_i^s : i군의 정보보호관련 문항 수
   (b) 군별 관리운영지수 비례상수 : $\mu_i^o = \dfrac{N_i^o}{N^o}$,
   N_i^o : i군의 관리운영 관련 문항 수
   $N_i = N_i^s + N_i^o$, $N^s = \sum_i N_i^s$, $N^o = \sum_i N_i^o$
2. 각 항목의 측정값 :
   $v(i,j,k,l) = \alpha\, v_s(i,j,k,l) + (1-\alpha)\, v_o(i,j,k,l)$
   $(0<\alpha<1$ 는 상수)
   i : 군분류, j : 대분류
   k : 중분류, l : 소분류
   (a) $v_s(i,j,k,l)$: 정보보호 측정값
   (b) $v_o(i,j,k,l)$: 관리운영 측정값.

3. 군별, 속성별 평가지수

	1군 시스템 환경	2군 안전성 대책	3군 전산 센터	4군 하부조직 및 지점
보호지수 (S)	S_1	S_2	S_3	S_4
관리운영 지수 (O)	O_1	O_2	O_3	O_4
안전관리지수(CSO)	SO_1	SO_2	SO_3	SO_4

(a) 군별 보호지수 : $S_i = \sum_{j,k,l} \mu_i^s v_s(i,j,k,l)$
(b) 군별 관리운영지수 : $O_i = \sum_{j,k,l} \mu_i^o v_o(i,j,k,l)$
(c) 군별 안전관리 지수 : $SO_i = \lambda S_i + (1-\lambda) O_i$
   , $0<\lambda<1$ (비례상수)
(d) 안전관리지수 : $CSO = \sum_i x_i SO_i$,
   x_i : 비례상수

방법Ⅱ. 군(Group)별 선지정 가중치 법

1. 군별 비례상수 : $\delta_1 = p_1$, $\delta_2 = p_2$, $\delta_3 = p_3$, $\delta_4 = p_4$
   (a) 군별 보호지수(S_i) 비례상수 : δ_i^s
   (b) 군별 관리운영지수(O_i) 비례상수 : δ_i^o

2. 각 항목의 측정값 :
   $v(i,j,k,l) = \alpha\, v_s(i,j,k,l) + (1-\alpha)\, v_o(i,j,k,l)$
   $(0<\alpha<1$ 는 상수)
   (a) $v_s(i,j,k,l)$: 정보보호 측정값
   (b) $v_o(i,j,k,l)$: 관리운영 측정값.

3. 군별, 속성별 평가지수

	1군 시스템 환경	2군 안전성 대책	3군 전산 센터	4군 하부조직 및 지점
보호지수 (S)	S_1	S_2	S_3	S_4
관리운영 지수 (O)	O_1	O_2	O_3	O_4
안전관리지수(CSO)	SO_1	SO_2	SO_3	SO_4

(a) 군별 보호지수 : $S_i = \sum_{j,k,l} \delta_i^s\, v_s(i,j,k,l)$
(b) 군별 운영지수 : $O_i = \sum_{j,k,l} \delta_i^o\, v_o(i,j,k,l)$
(c) 군별 안전관리 지수 : $SO_i = \lambda S_i + (1-\lambda) O_i$
   $(0<\lambda<1$ 는 비례상수)
(d) 안전관리지수 : $CSO = \sum_i x_i SO_i$,
   x_i : 비례상수.

제 4 장 항목별 비교

1.분류항목별 비교표

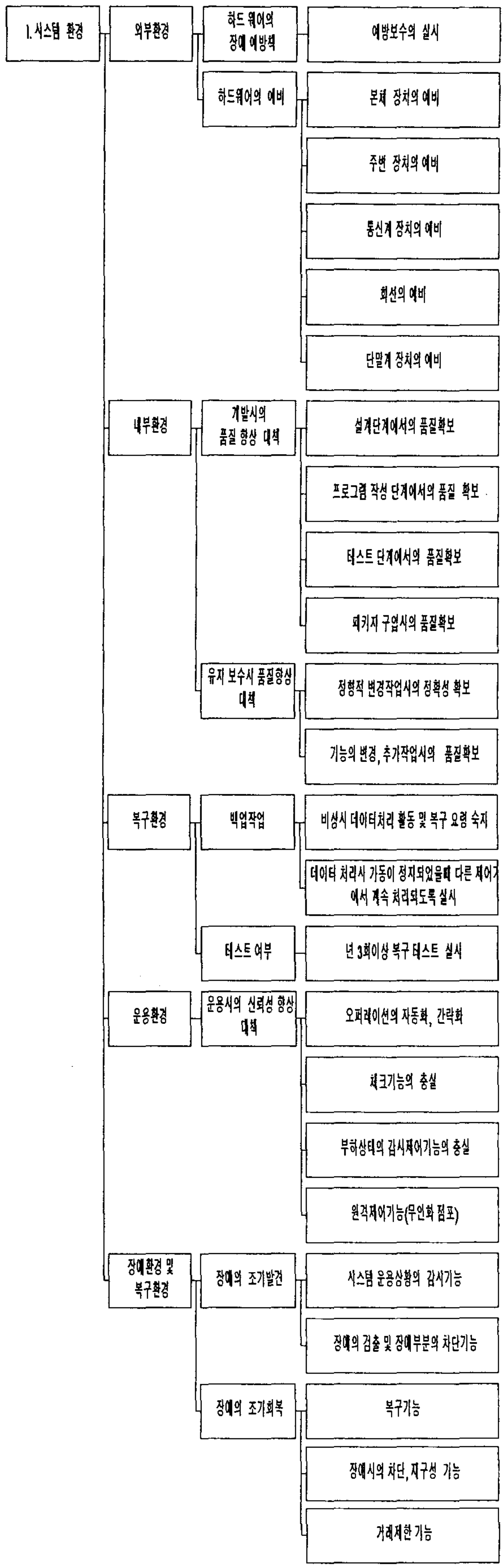
항목	대분류	중분류	소분류	[illegible] (94.12)	[illegible] (98.12)	BS7799	금융결제원	[illegible] (98.10)	[illegible]
시스템 환경	외부환경	하드웨어의 장애 예방책	예방보수의 실시			○	○		○
		하드웨어의 예비	본체 장치의 예비		○		○		○
			주변 장치의 예비				○		○
			통신계 장치의 예비				○		○
			회선의 예비				○		○
			단말기 장치의 예비		○		○		○
	내부환경	개발시의 품질 향상 대책	설계 단계에서의 품질 확보				○	○	○
			프로그램 작성 단계에서의 품질 확보				○	○	○
			테스트 단계에서의 품질확보				○	○	○
			패키지 구입시의 품질확보			○	○	○	○
		유지 보수시 품질향상 대책	정형적 변경작업시의 정확성 확보	○		○	○		○
			기능의 변경, 추가작업시의 품질 확보	○		○	○		○
	복구환경	백업작업	비상시 데이터 처리	○	○	○			○
			데이터 처리시 가동이 정지되었을 때 다른 제어기에서 계속 처리되도록 실시	○	○				
		테스트 여부	년 3회이상 복구 테스트 실시		○	○			○
	운용환경	운용시의 신뢰성 향상 대책	오퍼레이션의 자동화, 간략화				○		○
			체크기능의 충실				○		○
			부하상태의 감시제어기능의 충실설			○	○		○
			원격제어기능(무인화 점포)			○	○	○	○
	장애환경 및 복구환경	장애의 조기발견	시스템 운용상황의 감시기능			○	○		○
			장애의 검출 및 장애부분의 차단기능				○		○
		장애의 조기회복	거래제한기능				○		○
			복구기능		○		○		○
			장애시의 차단 · 재구성 기능	○	○				

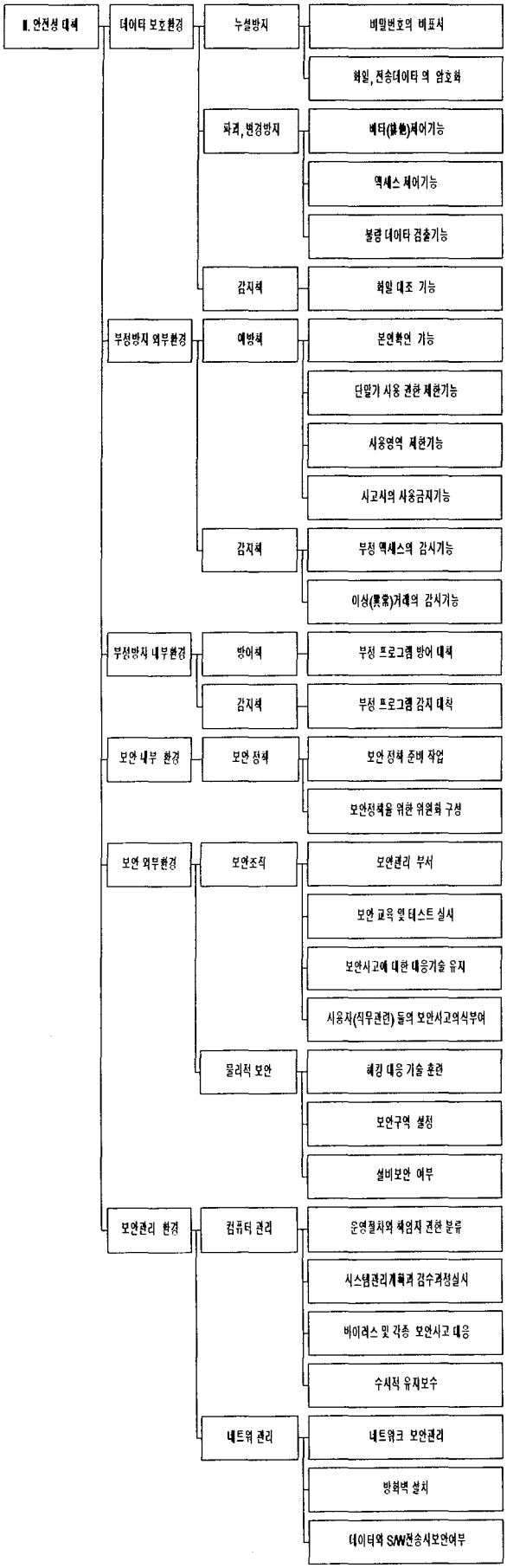
항목	대분류	중분류	소분류	표준화 (94.12)	정보보호 (96.12)	BS7799	금융 결제원	보안협회 (98.10)	해외조사
안전성 대책	데이터 보호환경	누설 방지	비밀번호의 비표시	○	○		○		○
			파일, 전송데이타의 암호화		○		○		○
		파괴, 변경방지	배타(排他)제어기능				○		○
			액세스 제어기능				○		○
			불량 데이터 검출기능				○		○
		감지책	파일 대조 기능				○		○
	부정행위 외부환경	예방책	본인확인 가능	○	○	○	○	○	○
			단말기 사용 권한 제한기능		○		○	○	○
			사용영역 제한기능	○	○	○	○	○	○
			사고시의 사용금지기능				○		○
		감지책	부정 액세스의 감시기능	○			○		○
			이상(異常)거래의 감시기능	○			○		○
	부정행위 내부환경	방어책	부정 프로그램 방어대책		○	○	○	○	○
		감지책	부정 프로그램 감지 대책		○	○	○	○	○
	보안내부 환경	보안 정책	보안정책 준비작업			○		○	○
			보안정책을 위한 위원회 구성			○		○	○
	보안외부 환경	보안조직	보안관리 부서			○		○	○
			보안교육 및 테스트 실시						○
			보안사고에 대한 대응기술 유지			○		○	○
			사용자(직무관련)들의 보안사고의식 부여						○
		물리적 보안	해킹 대응 기술 훈련						○
			보안구역 설정		○	○	○	○	○
			설비보안 여부			○	○		○
	보안관리 환경	컴퓨터 관리	운영절차와 책임자 권한 분류		○	○		○	○
			시스템 관리계획과 점수과정 실시		○	○		○	○
			바이러스 및 각종 보안사고 대응	○	○	○	○	○	○
			수시적 유지보수		○				○
		네트웍 관리	네트워크 보안관리	○	○	○		○	○
			방화벽 설치		○			○	○
			데이터와 S/W전송시 보안여부		○			○	○

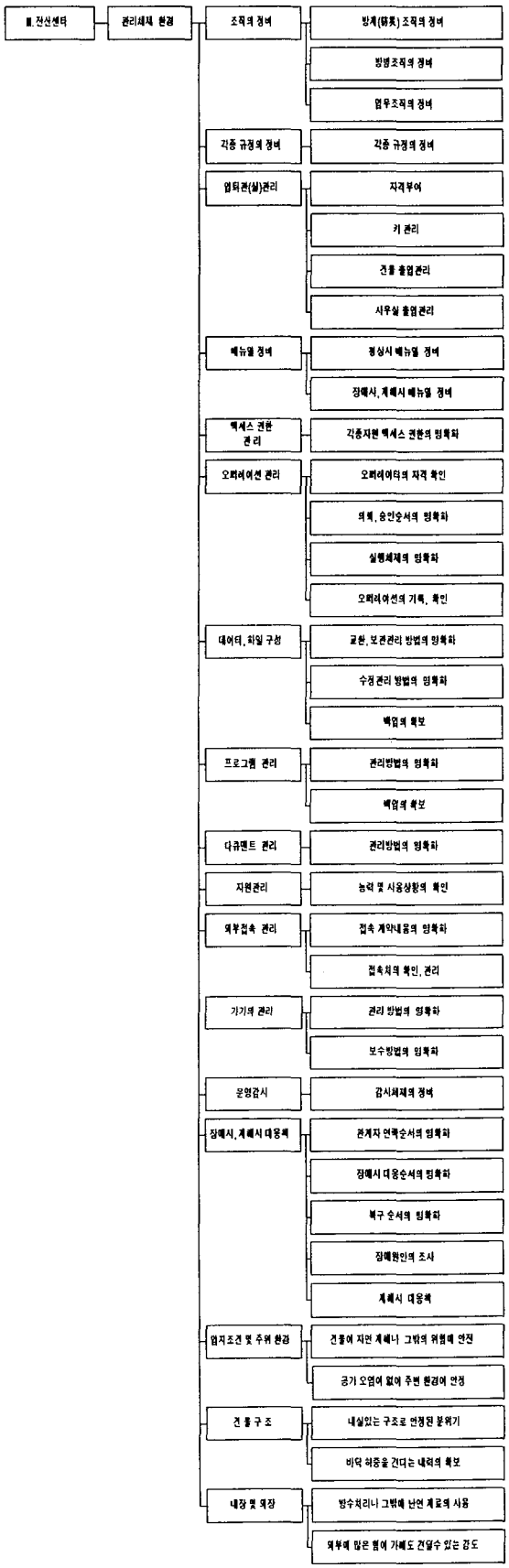
항목	대분류	중분류	소분류	표준화 (94.12)	정보보호 (96.12)	BS7799	금융 결제원	보안협회 (98.10)	해외조사
전산센터	관리체계 환경	조직의 정비	방재(防災)조직의 정비	○		○	○	○	○
			방범조직의 정비	○		○	○	○	○
			업무조직의 정비			○	○	○	○
		각종 규정의 정비	각종 규정의 정비				○		○
		입퇴관(실)관리	자격부여	○			○		○
			키 관리				○		○
			건물 출입관리	○		○	○		○
			사무실 출입관리	○		○	○	○	○
		매뉴얼 정비	평상시 매뉴얼 정비	○	○		○	○	○
			장애시, 재해시 매뉴얼 정비	○	○		○	○	○
		액세스 권한	각종 자원 액세스 권한의 명확화	○			○		○
		오퍼레이션 관리	오퍼레이터의 자격 확인	○		○	○	○	○
			의뢰, 승인 순서의 명확화	○		○	○		○
			실행체제의 명확화	○		○	○		○
			오퍼레이션의 기록, 확인	○	○	○	○		○
		데이터, 파일 구성	교환, 보관관리 방법의 명확화	○		○	○		○
			수정관리 방법의 명확화	○	○	○	○		○
			백업의 확보	○	○	○	○		○
		프로그램 관리	관리 방법의 명확화	○			○		○
			백업의 확보	○		○	○		○
		다큐멘트 관리	관리방법의 명확화				○		○
		자원관리	능력 및 사용상황의 확인	○			○		○
		외부접속 관리	접속 계약내용의 명확화			○	○	○	○
			접속처의 확인, 관리				○		○
		기기의 관리	관리 방법의 명확화		○	○	○		○
			보수방법의 명확화		○	○	○		○
		운영감시	감시체제의 정비				○		○
		장애시, 재해시 대응책	관계자 연락순서의 명확화		○		○		○
			장애시 대응순서의 명확화		○		○		○
			복구 순서의 명확화				○		○
			장애원인의 조사				○		○
			재해시 대응책		○		○		○

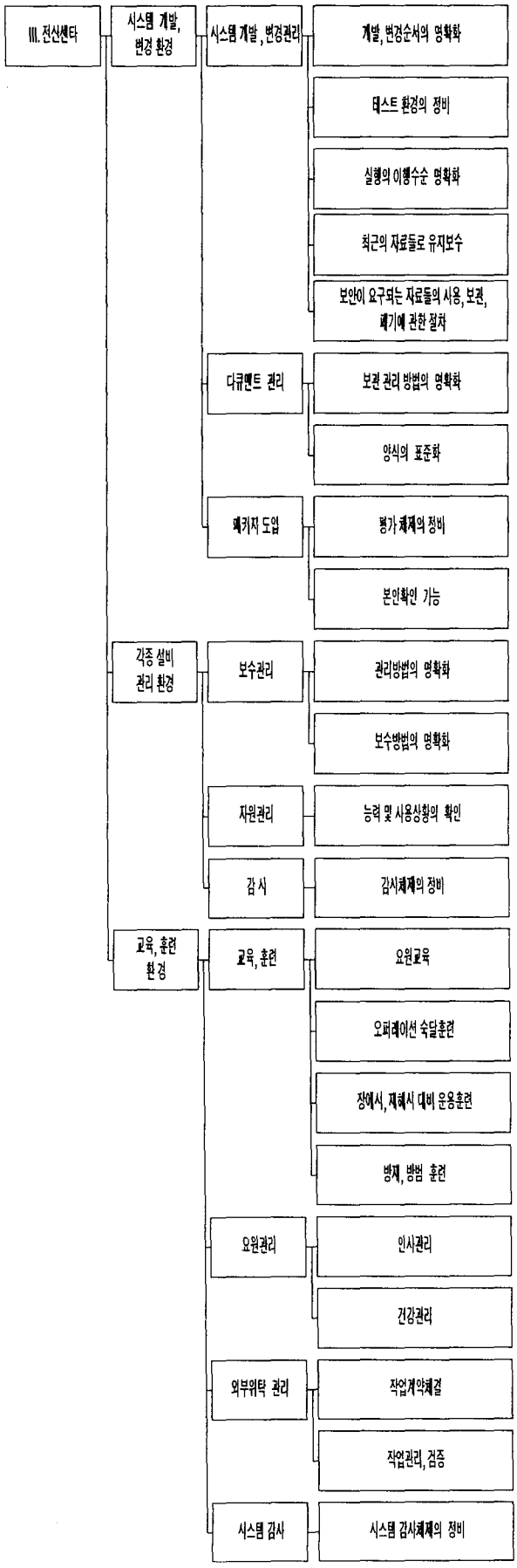
항목	대분류	중분류	소분류	[illegible] (94.12)	[illegible] (96.12)	BS7799	금융 결제원	[illegible] (96.10)	실태조사
전산센터	시스템 개발, 변경관리	시스템 개발, 변경관리	개발, 변경순서의 명확화				○		○
			태스트 환경의 정비			○	○		○
			실행의 이행 수순 명확화			○	○		○
			최근의 자료들로 유지보수	○	○				
			보안이 요구되는 자료들의 사용, 보관, 폐기에 관한 절차	○	○			○	
		다큐멘트 관리	보관 관리 방법의 명확화				○		○
			양식의 표준화				○		○
		패키지 도입	평가 체계의 정비	○			○		○
			본인확인 가능	○	○	○	○		○
	각종 설비 관리 환경	보수관리	관리방법의 명확화			○	○		○
			보수방법의 명확화			○	○		○
		자원관리	능력 및 사용상황의 확인				○		○
		감시	감시체계의 정비				○		○
	교육, 훈련 환경	교육, 훈련	요원교육	○	○		○		○
			오퍼레이션 숙달훈련	○	○	○	○		○
			장애시, 재해시 대비 운용 훈련	○	○		○		○
			방재, 방범 훈련			○	○		○
		요원관리	인사관리		○	○	○		○
			건강관리				○		○
		외부위탁 관리	작업계약 체결				○		○
			작업관리, 검증				○		○
		시스템 감사	시스템 감사체제의 정비			○	○		○
하부조직 및 지점	관리체계 확립	조직의 정비	방재조직의 정비			○	○		○
			방범조직의 정비			○	○		○
			업무조직의 정비			○	○		○
		각종 규정의 정비	각종 규정의 정비	○	○		○		○
	운용관리	매뉴얼의 정비	평상시 매뉴얼 정비	○	○		○		○
			장애시, 재해시 매뉴얼 정비	○	○		○		○
		거래의 관리	사용시 조작권한 명확화	○		○	○		○
			오퍼레이터 키 관리	○	○	○	○		○
			사용시 조작내용 기록, 검증	○	○	○	○		○
			사고계좌의 관리				○		○
		데이터, 파일관리	각종 데이터, 파일의 관리	○		○			○
		프로그램관리	관리방법의 명확화			○	○		○
			백업의 확보	○	○	○	○		○
			컴퓨터 바이러스의 대책	○	○	○	○		○
		기기관리	관리방법의 명확화		○	○	○		○
			보수방법의 명확화		○	○	○		○
		OA기기의 관리	OA기기 관리 방법의 명확화			○	○		○
			기록매체 관리방법의 명확화				○		○
		섭외단말의 관리	운용관리 방법의 명확화				○		○
		장애시, 재해시 대응책	관계자 연락 순서의 명확화						○
			장애시 처리방법의 명확화		○				○
	감리	감리 체계	감리는 독립적이고 객관적으로 구성	○					
			전문가 또는 유자격자를 양성하여 감리업무를 수행할수 있도록 적절한 임무 부여	○				○	
		감리 실시	전산망의 안전, 신뢰성 제고를 목적으로하여 예방차원에서 실시함	○				○	
			실시 결과에 따라 사후 조치	○					

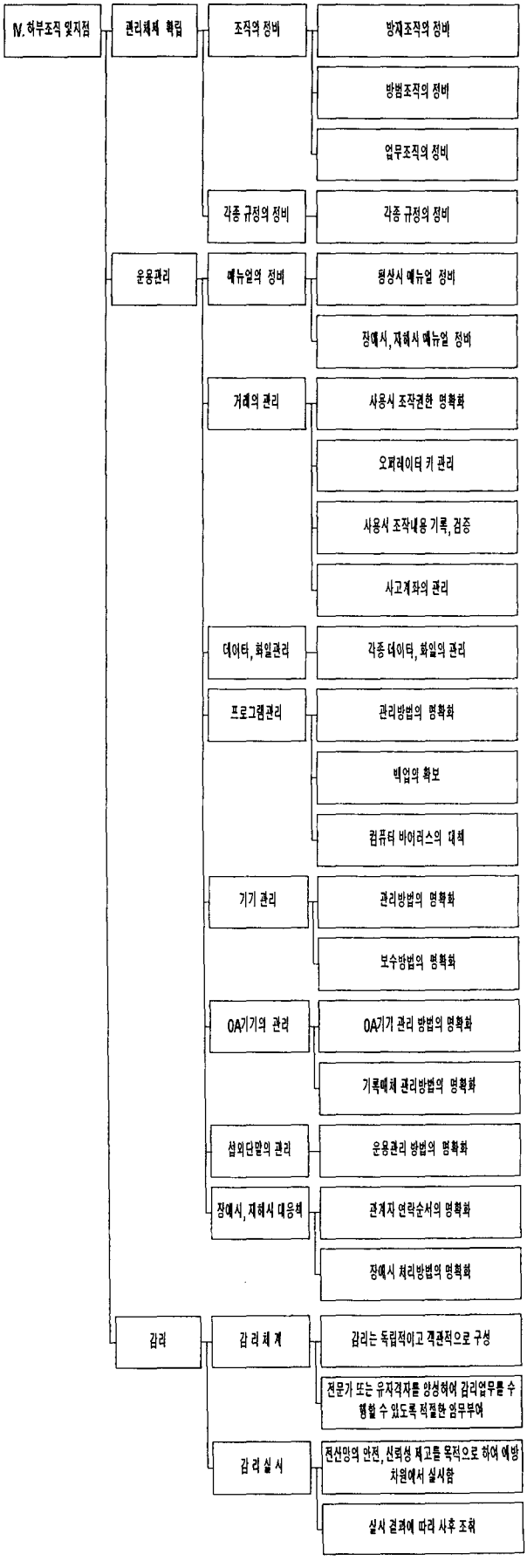
2. 분류별 체계도




Ⅱ. 안전성 대책
데이타 보호환경
누설방지
비밀번호의 배포서
화일, 전송데이타 의 암호화
파괴, 변경방지
배타(排他)제어기능
액세스 제어기능
불량 데이타 검출기능
감지책
화일 대조 기능
부정방지 외부환경
예방책
본인확인 기능
단말기 사용 권한 제한기능
사용영역 제한기능
시고시의 사용금지기능
감지책
부정 액세스의 감시기능
이상(異常)거래의 감시기능
부정방지 내부환경
방어책
부정 프로그램 방어 대책
감지책
부정 프로그램 감지 대책
보안 내부 환경
보안 정책
보안 정책 준비 작업
보안정책을 위한 위원회 구성
보안 외부환경
보안조직
보안관리 부서
보안 교육 및 테스트 실시
보안사고에 대한 대응기술 유지
시용자(직무관련) 들의 보안사고의식부여
물리적 보안
해킹 대응 기술 훈련
보안구역 설정
설비보안 여부
보안관리 환경
컴퓨터 관리
운영절차와 책임자 권한 분류
시스템관리계획과 검수과정실시
바이러스 및 각종 보안사고 대응
수시적 유지보수
네트워 관리
네트워크 보안관리
방화벽 설치
데이터와 S/W전송시보안여부


Ⅱ.전산센터
관리체제 환경
조직의 정비
방재(防災) 조직의 정비
방범조직의 정비
업무조직의 정비
각종 규정의 정비
각종 규정의 정비
입퇴관(실)관리
자격부여
키 관리
건물 출입관리
사무실 출입관리
메뉴얼 정비
정상시 메뉴얼 정비
장해시, 재해시 메뉴얼 정비
액세스 권한 관리
각종자원 액세스 권한의 명확화
오퍼레이션 관리
오퍼레이터의 자격 확인
의뢰, 승인순서의 명확화
실행체제의 명확화
오퍼레이션의 기록, 확인
데이터, 화일 구성
교환, 보관관리 방법의 명확화
수정관리 방법의 명확화
백업의 확보
프로그램 관리
관리방법의 명확화
백업의 확보
다큐멘트 관리
관리방법의 명확화
자원관리
능력 및 사용상황의 확인
외부접속 관리
접속 계약내용의 명확화
접속처의 확인, 관리
가기의 관리
관리 방법의 명확화
보수방법의 명확화
운영감시
감시체제의 정비
장해시, 재해시 대응책
관계자 연락순서의 명확화
장해시 대응순서의 명확화
복구 순서의 명확화
장해원인의 조사
재해시 대응책
입지조건 및 주위 환경
건물에 자연 재해나 그밖의 위험에 안전
공기 오염이 없이 주변 환경이 안정
건 물 구 조
내실있는 구조로 안정된 분위기
비닥 하중을 견디는 내력의 확보
내장 및 외장
방수처리나 그밖에 난연 재료의 사용
외부에 많은 틈이 가해도 견딜수 있는 강도


III. 전산센타
시스템 개발, 변경 환경
시스템 개발, 변경관리
개발, 변경순서의 명확화
테스트 환경의 정비
실행의 이행수순 명확화
최근의 자료들로 유지보수
보안이 요구되는 자료들의 사용, 보관, 폐기에 관한 절차
다큐멘트 관리
보관 관리 방법의 명확화
양식의 표준화
메키저 도입
봉가 체제의 정비
본인확인 가능
각종 설비 관리 환경
보수관리
관리방법의 명확화
보수방법의 명확화
자원관리
능력 및 사용상황의 확인
감 시
감시체제의 정비
교육, 훈련 환경
교육, 훈련
요원교육
오퍼레이션 숙달훈련
장애시, 재해시 대비 운용훈련
방재, 방범 훈련
요원관리
인사관리
건강관리
외부위탁 관리
작업계약체결
작업관리, 검증
시스템 감사
시스템 감사체제의 정비


IV. 하부조직 및 지점
관리체제 확립
조직의 정비
방재조직의 정비
방범조직의 정비
업무조직의 정비
각종 규정의 정비
각종 규정의 정비
운용관리
메뉴얼의 정비
평상시 메뉴얼 정비
장애시, 재해시 메뉴얼 정비
거래의 관리
사용시 조작권한 명확화
오퍼레이터 키 관리
사용시 조작내용 기록, 검증
사고계좌의 관리
데이타, 화일관리
각종 데이타, 화일의 관리
프로그램관리
관리방법의 명확화
백업의 확보
컴퓨터 바이러스의 대책
기기 관리
관리방법의 명확화
보수방법의 명확화
OA기기의 관리
OA기기 관리 방법의 명확화
기록매체 관리방법의 명확화
섭외단말의 관리
운용관리 방법의 명확화
장애시, 재해시 대응책
관계자 연락순서의 명확화
장애시 처리방법의 명확화
감리
감리체계
감리는 독립적이고 객관적으로 구성
전문가 또는 유자격자를 양성하여 감리업무를 수행할 수 있도록 적절한 업무부여
감리실시
전산망의 안전, 신뢰성 제고를 목적으로 하여 제3자 입장에서 실시함
실시 결과에 따라 사후 조치

제 4 장 토의 및 결론

정보보호지표 항목개발 및 계량화 연구에서 단순가중치법과 상대가중치법을 통하여 0,1로만 계량화하는데에는 어는 정도의 차이가 발생하는 것으로 결론을 도출할 수 있었다. 본 연구에서는 항목비례가중치법과 선가중치법을 통하여 측정범위를 1-6까지 범위를 만들었고, 이를 통하여 0,1에서 발생되는 오류를 최소화 하는데 본 연구에 의미를 두고 있다.

2차집단의 설문 결과는 감리 시기나 항목별 상관관계에 유의적인 값이 설정되지 못하였지만 1차 감리 전문가 집단에서는 그들의 경력별, 항목별 연관 관계가 유의함을 볼 수 있었다. 그러므로 전산, 감리의 효과나 효율성을 높이기 위해서는 감리 집단을 이용하는 것이 긍정적으로 사료되며, 항목별 연관관계는 항목에 대한 중요성이 경력과 다소 비례함을 알 수 있었다.

참 고 문 헌

[1] 정보시스템 보안/통제 감리지침 연구, 한국전산원, 1998, pp.8-22.

[2] 김명룡외 3인 "정보보호현황", 한국정보보호센터. 1996, pp. 357-384.

[3] 이재우, "중요정보 기반 구조 보호", '98 한국정보통신망침해사고대응팀협의회 해킹방지 워크샵 자료집, 한국정보보호센터, 1998, pp. 122-123.

[4] 신승중, 김현수, "보안감리를 위한 계량화에 관한 연구", 한국정보처리학회 춘계 학술발표논문집 제6권 제1호, 1999, pp.860-863.

[5] 정보보호지표 항목개발 및 계량화 연구, 한국정보보호센터, 1998, pp. 1-3.

[6] 정보보호지표 항목개발 및 계량화 연구, 선진 외국의 정보보호 수준 평가 활동, 한국정보보호센터, 1998, pp. 4-7

[7] 한인구, 윤종호, "정보시스템 통제 및 감사가 컴퓨터 범죄의 인지된 위험에 미치는 영향: 금융기관을 중심으로," 경영정보학연구, 제5권 1호, 195. 6, pp.112-128.

[8] IOS/IEC JTC1/SC27N689, Guidelines for the Management of IT System Security: Part3-Techniques for the Management of IT Security, IOS, Mar. 1993.

[9] IOS/IEC JTC1/SC27 N720, Guidelines for the Management of IT Security(GMITS): Part2-Managing and Planning IT Security(GMITS): Part2-Managing and Planning IT Security, IOS, May.1993.

[10] ISO/IEC JTC1/SC27 N777, Guidelines for the Management of IT System Security (GMITS):Part1-Concepts and Models for IT Security, ISO, Oct. 1993.

[11] ISO/IEC JTC1/SC27 N442, Key Management Part1: Framework, ISO, Mar. 1994.

[12] Katzke, S., "A Government Perspective on Risk Management of Automated Information Systems," Proceedings of the 1988 Computer Security Risk Management Model Builders Workshop, 1988, pp.3-20.