通信情報保護學會誌
第5卷 第2號, 1995. 6

보안관리를 위한 위협, 자산, 취약성의 분류체계
-BDSS 사례 -

김 기 윤*, 나 관 식**, 김 종 석***

요 약

본 논문는 정보시스템 보안관리에 대한 개념적 모형을 INFORSEC 및 한국전산원이 제시한 모형을 중심으로 기술했으며, 보안관리의 표준적인 분류체계를 근거로 BDSS의 위협, 자산, 취약성의 분류체계를 비교 함으로써 위협, 자산, 취약성의 관련성을 탐색 하고자 했다. 특히 위협의 원천과 가해자 측면에서 BDSS와 CRAMM의 경우를 비교함으로써, 분류체계의 장단점을 파악하고자 했다.

1. 서 론

정보를 보호해야 한다는 요구사항은 많은 정보시스템이 전산망으로 연결되어 있는 최근 정보시스템의 환경에서 특히 중요해지고 있다. 정보자산이 조직에서 차지하는 비중이 증대됨에 따라, 고의 혹은 실수로 인한 정보자산의 변경, 파괴, 불법적 공개 등으로 인한 손실로 부터 보호할 필요성이 대두되고 있다. 과거의 단순한 물리적 접근통제와 제도적인 안전장치 만으로는 효과적인 정보보호를 달성하는데는 한계가 있으므로, 종합적이고 체계적인 정보보호를 위한 보안관리체제를 구축해야만 한다.

정보보호(information security)란 정보를 입력, 처리, 저장, 출력, 정송 등 모든 단계에서 정보를 보호하기 위해서 정보의 비밀성(confidentiality), 무결성(integrity), 가용성(availability), 인증성(authenticity), 이용성(usability)을 확보하는 것이다. 본 논문에서 연구대상이 되는 위험은 정보시스템에서 정보보호에 대한 '보안위험(security risk)'이고, 위험관리 역시 구체적으로는 정보시스템에 대한 '보안위험관리(security risk management; 이하 '위험관리' 라고 칭함)'에 관한 것이다.

정보시스템 위험관리의 목적은 정보시스템이 제공하는 정보와 서비스에 대해 적절한 수준의 비밀성, 무결성, 가용성, 인증성, 이용성 등을 유지하는 것이다. 정보시스템 위험관리에는 정보시스템의 자산에 대한 위협을 식별하고, 위협의 크기와 빈도를 측정한 후에, 적절한 위험수준을 유지하기 위한 보안대책을 선택하는 활동을 포함하고 있다. 또한, 위험관리의 기능에는 조직내 정보기술에 대한 보안방침의 결정, 보안 위험분석 및 관리, 보안인식의 제고, 보안시스템에 대한 감사 등

* 광운대학교 경영학과 교수
** 경민전문대학 사무자동화과 전임강사
*** 광운대학교 경영학과 박사과정

이 포함된다.

선진국의 경우 대부분 정부조직 및 대기업에서는 정보시스템 위험관리가 매우 중요시되어 보안위험을 주기적으로 측정하도록 요구하고 있으나, 가장 큰 문제점은 이러한 보안위험을 측정하는 표준화된 방법이 아직 제시되지 않고 있다는 것이다. 미국 및 유럽의 선진국에서는 정보시스템 보안에 대한 인식이 높으므로 보안사건에 대한 과거 자료로써 계량적 위험분석 및 이를 위한 소프트웨어가 많이 사용되고 있다. 우리나라와 같이 정보시스템 보안에 관한 인식은 물론 교육이 미비한 상황에서, 우리나라 정보시스템 환경에 적합한 소프트웨어를 개발하기 위한 첫 단계는 우선 위험분석의 3요소인 위협, 자산 취약성의 분류체계를 파악하고, 그 다음에 이들 간의 관련성을 연구하는 일이다.

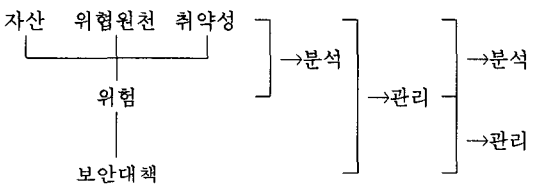
따라서 본 연구의 목적은 첫째, 정보시스템 위험관리에 대한 개념적 모형을 체계적으로 기술하고, 둘째, BDSS(Bayesian Decision Support System)의 위협, 자산, 취약성의 분류체계를 표준적인 분류체계와 비교 하고자 한다. 이를 위해서 본 논문의 2장에서는 정보시스템 보안관리에 대한 개념적 모형을 INFORSEC(Information Security) 및 한국전산원이 제시한 모형을 중심으로 기술했으며, 3장에서는 BDSS의 위협을 CRAMM(CCTA's Risk Analysis and Management Methodology)과 비교했고, 4장과 5장에서는 각각 BDSS의 자산과 취약성의 분류체계를 표준적인 분류체계와 비교해서 제시하였으며, 6장에서는 본 연구의 한계 및 향후 연구과제에 대해 언급했다.

2. 보안관리의 개념적 모형과 분류체계

2.1 보안관리의 개념적 모형

위험관리란 불확실한 사건의 피해를 식별, 통제, 최소화하는 전반적인 절차에 관계된 경영과학의 한 분야로서, 정보시스템 보안위험관리는 측정/평가된 위험에 대한 안전대책을 일정 수준까지 유지/관리하는 것이다. 그리고, 위험분석이란 정보시스템과 그 자산의 기밀성(confidentiality), 무결성(integrity), 가용성(availability), 기록성(accountability)에 영향을 미칠 수 있는 다양한 위협에 대해서 정보시스템이 취약함을 인식하고, 이로 인해서 예상되는 손실을 분석하는 것이다.

정보시스템 위험분석과 위험관리에 대한 개념에는 두가지 견해가 있다. 하나는 위험분석이 절차상 위험관리에 포함된다는 견해이고, 다른 하나는 다음과 같이 서로 독립된 영역으로 구분된다는 견해이다.



(그림 1) 정보시스템 위험관리 및 위험분석에 대한 두가지 견해

위험분석과 위험관리를 서로 독립된 영역으로 구분한 후자의 견해를 따르는 Moses (1992)에 의하면, 위험관리의 목적은 위험분석 결과에 의해서 현재의 보안수준을 허용된 수준까지 높이기 위해서 보안대책을 마련하는 것이다. 다시 말해서, 위험관리는 경영층이 받아들일 수 있는 수준까지 위협의 빈도와 영향을 감소시킬 수 있는 보안대책을 선택하는 것이다. 그러나, 일반적으로 위험관리 과정 내에 위험분석절차가 포함된 것으로 인식되고 있으며, 본 연구에서 다루는 위험이 '보안위험'이므로 보안위험관리는 보안관리내에 한 영역으로 간주하는 것이 합리적이다.

INFORSEC(Information Security) '92 Security Investigations Programme의 여러 과제 중 하나로, 위험분석에 관한 과제의 궁극적인 목표는 전 유럽에 기존 혹은 개발 중인 위험관

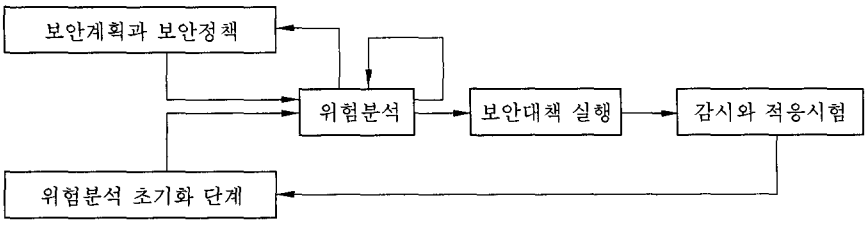


그림 2 NIFOSEC의 위험관리 모형

리방법들을 널리 쓰이게 하기 위한 전략을 수립하는 것이었다. 이를 위해서 위험관리를 구성하는 구성요소의 식별 및 이들 간의 상호관계 규명, 그리고 위험분석 과정의 모형화 등이 과제의 핵심이었다. 위험관리 모형의 구성요소에는 위험분석, 자산들 간 종속성 평가, 위협평가, 우연적인 위협의 식별 및 평가, 의도적인 위협의 식별 및 평가, 기존 보안대책의 식별과 검토, 그리고 취약성 평가, 제약조건 식별, 보안대책의 식별 및 선택, 감시와 적응시험 등이 있다.

(그림2)에서 위험관리는 위험분석의 상위개념이며, 위험분석 초기화 단계 및 보안계획과 보안정책이 수립된 후에, 위험분석은 (그림3)과 같이 실행되고, 선택된 보안대책을 설치해서 유지관리하기 위해서 최종적으로 감시(monitoring)와 적응시험을 하고, 다시 위험분석 초기화 단계로 휘드-백 된다. (그림3)은 위험분석 구성요소들간의 관계를 나타낸 것이다. 위험분석의 첫단계로 정보시스템의 자산을 식별해서 분류한 후에, 자산들간의 종속성을 평가해서, 위협이 독립적으로 자산에 영향을 주는지 평가하고, 기존의 보안대책을 식별해서 취약성을 평가한다. 이와 동시에 보안목적과 제약조건을 식별한 후에, 위험의 크기를 측정하고, 그 영향을 결정한 후에, 적절한 보안대책을 선택하게 된다.

1993년에는 EC(European Communities)에서 '위험분석'이라는 보고서를 발행했다. 여기서는 기존 66개 위험분석방법들을 분석하여 유럽 전체에서 공동으로 활용될 수 있는 분석방법을 개발하기 위해서 '요구구조(claim structure)'라는 도구를 개발하여 유럽표준 뿐만아니라 국제표준으로 발전시키려 하였다. 1994년에는 현재 국제표준화기구(ISO: International Organization for Standardization)의 ISO/IEC (International Electrotechnical Commission) JTC1/SC27에서 '정보기술보안관리지침

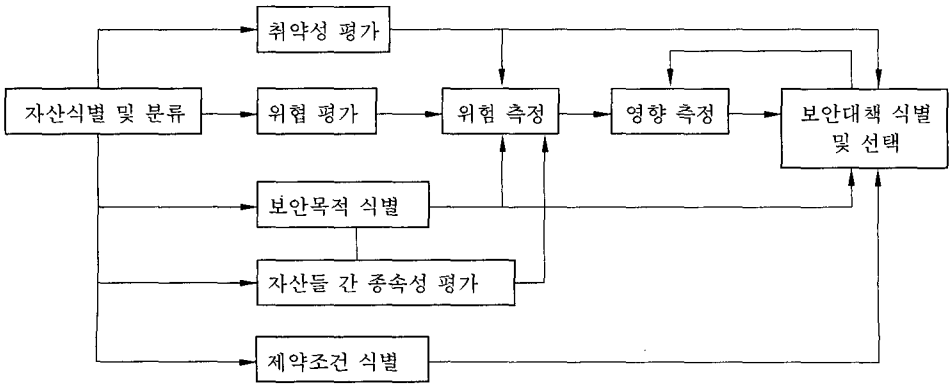


그림 3 NIFOSEC의 위험관리 모형

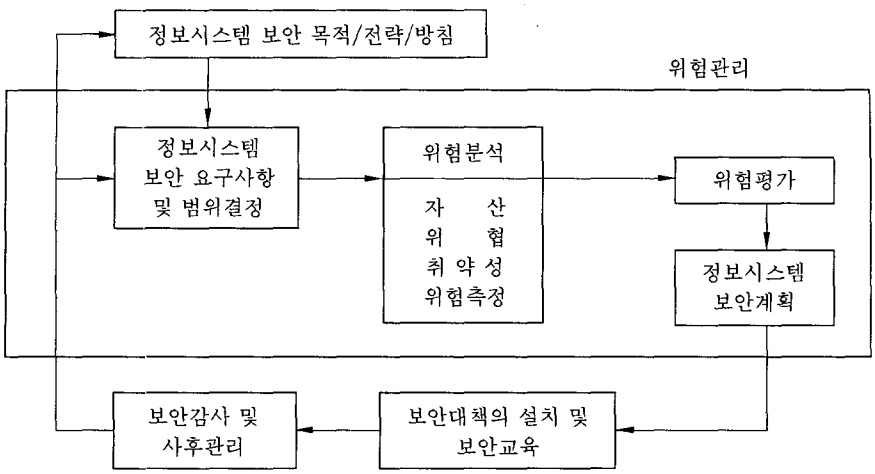


그림 4 정보시스템 보안관리의 개념적 모형

(GMITS: Guidelines for the Management of IT Security)'으로 위험분석에 관한 표준화를 진행시키고 있다.

김기윤외 12인(1994)이 제안한 정보시스템 보안관리의 개념적 모형은 (그림4)와 같다. 보안위험에 대한 관리, 즉 정보시스템에서 위험관리는 보안관리의 하위개념이다.

그러므로, 위험관리의 영역은 (그림4)에서 큰 네모 안의 영역이며, 외부 영역을 포함한 전체그림이 보안관리의 영역이다. 이와 같이 (보안)위험관리는 보안관리에서 가장 중요한 영역이다. 관리란 일반적으로 계획, 실행, 평가의 주기를 가지므로, 보안관리 역시 계획단계에서 보안목적의 수립 및 위험관리에 의해서 보안계획이 작성되고, 실행단계에서 보안대책을 설치하고, 평가단계에서 보안감사 및 사후관리를 하고, 다시 계획단계로 피드 백 된다. 정보시스템 보안관리의 구체적인 과정은 다음과 같이 요약할 수 있다.

(1) 정보시스템 보안 목적/전략/방침

조직의 전체 수준에서 운영수준 까지 계층구조별로 달성해야 할 보안 목적, 목적을 달성하기 위한 방법으로서 전략, 그리고 이를 위해 실행하는 세부적인 방침을 정해야 한다.

(2) 정보시스템 보안 요구사항 및 범위 결정

정보시스템 보안 목적/전략/방침을 기초로 해서 위험관리를 수행하기 위해서 최소한의 보안 요구사항 및 위험관리의 범위를 결정하게 된다.

(3) 자산 분석

보호해야 할 전산자원들을 식별하고, 체계적으로 분류하여, 소유하고 있는 자산들의 가치를 평가하는 기본적인 단계이다. 여기서 자산이란 하드웨어, 소프트웨어, 데이타/데이타베이스, 사용자/전산요원, 시스템 관련문서, 전산자료 저장매체, 통신망 및 관련장비, 등을 말한다.

(4) 위협 분석

위협(threat)은 자산(asset)에 해를 줄 수 있는 위험의 원천이다. 이와 같은 위협을 식별하고 분류해서, 발생빈도와 손실크기(혹은 강도(severity))를 측정하는 것을 말한다. 위협에는 위협원천에 따라, 자연재해로 인한 위협들(화재, 수재, 정전, 등), 사람에 의한 의도적 위협들(단말기, 디스켓, 등의 파괴 및 절취와 같은 물리적 공격, 그리고 시스템 자원의 불법사용, 허가되지 않은 자원의 불법접근, 타인으로 위장하여 허가되지 않은 권한사용, 바이러스, 벌레 등 유해 프로그램 삽입

과 같은 기술적 공격), 사람에 의한 비의도적 위협들(명령어 혹은 프로그램의 조작미숙 및 조작실수), 정보시스템의 결함(운용체제 결함, 응용프로그램의 결함, 통신 프로토콜의 결함, 통신 소프트웨어의 결함)이 있다.

(5) 취약성 분석

취약성(vulnerability)이란 정보시스템에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어의 약점을 뜻한다. 이와 같은 약점을 확인하고 분류하여 위협을 감소시키는 것이 취약성을 분석하는 목적이다. 취약성에는 경영적 혹은 관리적 취약성(보안관리, 인원관리, 절차상관리, 사고대책관리, 등에 대한 취약성), 논리적 혹은 기술적 취약성(하드웨어, 응용소프트웨어, 운영체계, 데이타베이스, 네트워크, 등에 대한 취약성), 물리적 취약성(출입통제, 환경관리, 등에 대한 취약성)이 있다.

(6) 위험 측정

자산에 대한 손실을 분석하는 과정으로서, 위협의 발생확률과 손실크기를 곱해서 기대손실을 가능하면 계량적으로 계산한다. 손실크기를 화폐가치로 계산할 수 없으면, 정성적인 위험분석법을 이용한다.

(7) 위험평가

위험관리 방법에 따라서 위험통제(위험회피, 손실방지, 손실감소)혹은 위험재무(위험인수와 위험이전)를 하게 된다. 보안관리자는 위험통제비용과 위험재무비용을 고려해서 적절한 조합을 구해야 한다. 위험재무는 경영학적 측면으로서 위험통제로도 통제가 불가능할 때 선택하는 방법이며, 비용이 너무 많이드는 방법이다. 위험통제는 손실을 사전에 통제하는 개념이고, 전산전문가와 경영자 간의 긴밀한 협의에 의해서 세부적인 보안대책이 이루어져야 한다. 여기에는 위험평가과정에서 의사결정자의 위험인식태도에 따라서 비용효과적으로 여러가지 보안대책 중에서 최적 보안대책(safeguard)을 선택하는 단계이며, 여기서 선택해서 추진하는 비용까지 계산해야 한다.

(8) 정보시스템 보안계획

정보시스템의 구성을 보여주는 구성계획, 보안대책의 설치를 위한 설치계획, 시스템의 변경시 필요한 변경계획, 비상시를 대비한 비상계획 등을 작성한다. 여기서 구성계획에서는 시스템의 구성요소와 구성요소들 간의 관계, 그리고 기존 보안대책의 설치현황 등이 작성되고, 설치계획에서는 새로운 보안대책의 설치에 필요한 자원, 일정 등이 작성된다. 또한, 변경계획에서는 시스템에 대한 확장, 새로운 시스템의 추가 등의 변경에 대한 계획이 작성되고, 비상계획에서는 비상사태를 대비한 계획이 작성된다.

(9) 보안대책의 설치 및 보안교육

보안대책은 안전대책, 혹은 통제, 혹은 대응책(safeguard, or control, or countermeasure)이라고도 불리고 있다. 보안대책은 위험을 감소시키기 위한 보호조치를 의미하며, 여기에는 장치, 절차, 기법, 행위 등이 포함된다. 새로운 보안대책을 기존 시스템에 설치하고, 효과적으로 운영하기 위해서 사용자와 관리자에 대한 보안교육을 실행하여 보안인식을 제고시킨다.

(10) 보안감사 및 사후관리

보안감사는 구축된 시스템이 효과적으로 운영되고 있는지 점검하는 활동이다. 기존 시스템의 운영상태를 파악하여 문제점을 조사해서 감사지침서를 작성하며, 이를 보안방침의 수립이나 위험관리에 반영되도록 한다.

2.2 보안관리의 분류체계

보안관리의 분류체계, 특히 위협, 자산, 취약성

에 대한 분류체계가 학자들의 관점에 따라 서로 다르므로, 본 연구에서는 Solms & Eloff & Solms(1990)의 분류체계를 표준적인 분류체계로 설정해 놓고, BDSS의 사례를 비교분석하고자 한다. 본 연구에서는 보안에 대한 표준적인 분류체계를 물리적 보안, 논리적 보안, 경영 보안으로 분류하고, 이에 대한 하위요소를 다음과 같이 구분하였다.

(1) 분류 P : 물리적 보안(physical security)

P1 : 환경 보안(environment security) - 정보시스템의 자산이 설치되어 있는 건물과 관련된 모든 위험에 대한 보호.

P2 : 물리적접근 보안(physical access security) - 권한있는 사람의 물적접근 통제와 관련된 모든 위험에 대한 보호.

P3 : 물적가용 보안(physical availability security) - 하드웨어를 항상 사용하지 못하는 위험에 대한 보호.

(2) 분류 L : 논리적 보안(logical security)

L1 : 소프트웨어 보안(software security) - 모든 응용 및 운영 시스템의 정확하고 연속적인 운영장애에 대한 보호.

L2 : 데이타 보안(data security) - 모든 데이타 항목에 대한 권한없는자의 접근 및 변경에 대한 보호.

L3 : 통신 보안(communication security) - 통신시스템의 보안과 관련된 위험에 대한 보호.

(3) 분류 M : 경영 보안(management security)

M1 : 관리적 보안(administrative security) - 최고경영층 측면에서 보안정책과 관련된 모든 위험에 대한 보호.

M2 : 조직적 보안(organizational security) - 조직적 측면 특히 중간관리층의 보안관리의 실행과 관련된 모든 위험에 대한 보호.

M3 : 인적 보안(personnel security) - 조직구성원 개개인의 보안과 관련된 모든 위험에 대한 보호.

물리적 보안은 전산실이나 통신실 등의 시설물과 정전압/무정전 설비, 공기정화설비, 집진장치 등 물리적 시설과 장비에 대한 물리적 침입과 파괴, 자연재해 등의 위협요인으로 부터 자산을 보호하기 위한 정보통신시설, 설비의 위치설정, 기계적 기준 등을 말한다. 논리적 보안은 소프트웨어와 데이타를 대상으로 불법적이고 의도적인 접근 또는 비의도적인 실수나 오용으로 부터 보호하기 위해서 인증, 암호화 등 접근통제나 통신보안을 하는 것을 말한다. 경영 보안은 물리적 및 논리적 자산을 다루는 사람과 조직 그리고 행정에 관한 것으로 인간에 의한 의도적 및 비의도적 위협으로 부터 보호하는 것을 말한다.

여기서 P, L, M 간의 관계는 M 〉 P 〉 L이다. 즉 물리적 보안에 논리적 보안이 포함되어 있고, 경영보안에는 물적 보안은 물론 논리적 보안도 포함되어 있다. 예로써, 논리적 보안이 물리적 보안에 의존되어 있기 때문에, 하드웨어 보안이 파괴되면 소프트웨어 보안도 파괴된다. 또한 물리적 보안과 논리적 보안이 경영 보안에 의존되어 있기 때문에, 보안정책 자체가 잘못되어 있으면 하드웨어 및 소프트웨어 보안에 모두 영향을 주게 된다. 위협, 자산, 취약성의 관계를 단순화시키기 위해서 모두 표준분류체계에 의해서 동일하게 분류할 수도 있지만, 이런 경우 위험분석의 유연성 및 구체성이 결여될 수 밖에 없다. 그러므로, 위협, 자산, 취약성의 분류체계는 서로 다를 수 밖에 없다.

3. 위협의 분류체계

Loch와 Carr 그리고 Warkentin(1992)은 위협을 원천(source)의 위치에 따라서 내부 및 외부(internal & external) 위협으로, 가해자(perpetrator)가 누구인가에 따라 인간 및 비인간(human & non-human) 위협으로, 또한 의도(intent)의 유무에 따라서 우연적 및 의도적(accidental & intentional) 위협으로 구분했다. 그리고 이와 같은 위협의 결과를 폭로, 수정, 파괴, 사용거부 등 네가지로 분류했다.

BDSS(Bayesian Decision Support System)는 미국의 OPA(Ozier, Perry & Associates Inc.)에서 개발되었다. 베이스 정리(Bayes's theorem)를 근거로한 통계적 방법을 이용했고, 통합적인 위험관리구조(IRMA; Integrated Risk Management Architecture)를 갖는 소프트웨어이다. 자산의 분류는 유형 및 무형으로 구분되고, 61개의 위협과 94개의 취약성 집단으로 구성되어 있다. 위협과 취약성 간의 mapping은 계층적/다수준/다기능 나무구조로 되어있고, 총 2400여개 항목으로 구성되어 있다. 각 위협에 대한 위험곡선과 평균 연간손실(ALE; Annualized Loss Exposure)을 출력시키며, 1900개의 보안대책을 제시할 수 있는 소프트웨어이다.

영국의 CCTA(Central Computer and Telecommunications Agency)는 CRAMM(CCTA's Risk Analysis and Management Methodology)을 보안관리를 위한 표준적인 접근방법으로 공인하고 있다. CRAMM은 17개의 본원적 위협(generic threats)을 이용해서 각 자산집단에 대해서 위협 및 취약성 질문을 32개까지 선택적으로 발생시킬 수 있고, 또한, 자산집단, 위험수준, 기존 통제방법을 근거로 900개의 보안대책을 제시할 수 있는 소프트웨어이다. Moses(1992)는 CRAMM에서의 위협들을 편의상 31개의 형태로 분류했다.

이와 같이 CRAMM의 31개 위협들과 BDSS의 61개의 위협들을 본 연구에서는 위협의 원천이 내부인지 혹은 외부인지, 그리고 위협의 가해자가 인간인지 혹은 비인간인지에 따라 (표 1)과 같이 분류했다. 이들을 비교분석한 결과를 요약하면 다음과 같다.

첫째, 인간에 의한 내부위협에서 인간의 오류를 CRAMM에서는 7가지로 분류했지만, BDSS에서는 4가지로만 분류했다.

둘째, 비인간에 의한 내부위협에서 CRAMM은 통신 네트워크 위협을 2가지(WAN, LAN)로 세분화 했지만, BDSS는 화재위협을 3가지(대, 중, 소)로 세분화 했다. 내부위협 측면에서는 CRAMM은 통신 네트워크와 관련된 위협이 세분화되어 있지만, BDSS에는 이와 관련된 위협이 없다.

세째, 인간에 의한 외부위협에서는 CRAMM은 외부인에 의한 4가지 위협만 있지만, BDSS는 도난, 폭탄, 전쟁의 위협을 각기 2가지로 세분화 했다.

네째, 비인간에 의한 외부위협에서 자연재해의 종류를 CRAMM에 비해서 BDSS에서는 다소 지나칠 정도로 세분화시켰다.

다섯째, 인간에 의한 내부위협에서는 상대적으로 CRAMM에 비해서 BDSS가 위협들이 세분화되어 있지 못한 반면에, 비인간에 의한 외부위협에서는 CRAMM에 비해서 BDSS가 다소 지나치게 세분화되어 있다.

위협과 자산과 취약성과의 관련성을 파악하기 위해서 BDSS의 61개 위협항목에 대해서 3가지로 분류된 본 연구의 표준적인 분류체계인 P, L, M을 ( ) 안에 표시한 것이 (표1)이다.

표 1 BDSS와 CRAMM의 위협

원천 \ 가해자	인 간	비 인 간
내부 위협	BDSS 위협 (10개) (P, L, M) 자원의 오용 (P, L) 유지보수자 오류. (L) 운영자 오류, 프로그래머 오류, 사용자 오류. (M) 직원부족, 사기행위, 파업, 태업(내부 ; 데이타/소프트웨어), 태업(내부 ; 물적). CRAMM 위협 (12개) 직원부족, 직원에 의한 도난, 직원에 의한 의도적 손해, 직원에 의한 시스템 침투, 자원의 오용, 시스템 운영자 오류, 광역통신망(WAN) 운영자 오류, 근거리통신망(LAN) 운영자 오류, 응용프로그래머 오류, 시스템 프로그래머 오류, (내부) 사용자 오류, 유지보수자 오류.	BDSS 위협 (15개) (P, L, M) 큰 규모/중간 규모/작은 규모의 내부화재(화재규모별로 3가지로 구분), 내부에서 우연적인 폭발. (P, L) 중앙컴퓨터장치 고장, 배관 누수. (P) 보조장치 고장, 음성통신장치 고장, 공기정화장치(HVAC) 고장 (L) 내부정전, 전력의 불안정, 통신 고장(데이타), 구입된 소프트웨어 고장. (M) 의학적 응급사태 CRAMM 위협 (12개) 사무실내 화재, 사무실내 수재, CPU 고장, 저장장치 고장, 입출력 장치 고장, 주변장치 고장, 광역통신망(WAN) 장치 고장, 근거리통신망(LAN) 고장, 전원장치 고장, 시스템 및 소프트웨어 고장, 광역통신망 반송자(WAN carrier) 서비스 고장, 독립적인(standalone) 마이크로 컴퓨터 고장
외부 위협	BDSS 위협 (12개) (P, L, M) 파괴행위, 소란(폭동)행위, 폭탄위협, 폭발, 방화, 인질행위, 재래 전쟁행위, 핵 전쟁행위. (L, M) 데이타 도난, 태업(외부 ; 데이타/소프트웨어) (P, M) 물적자산 도난(250불 이상), 태업(외부 ; 물적) CRAMM 위협 (4개) 외부인에 의한 도난, 외부인에 의한 의도적 손해, 외부인에 의한 시스템 침투, (외부) 사용자 오류. (4개)	BDSS 위협 (24개) (P, L, M) 건물화재, 외부에서 우연적인 폭발, 지진(리히터 5.0 이상), 화산활동, 산사태, 단층함몰, 댐 파손, 계절적 홍수, 조수에 의한 홍수, 해일, 큰 회오리바람, 태풍, 별똥(운석)충돌, 전염병, 방사능 오염, 비행기 충돌, 유독성 오염 (P, L) 열대성 비바람, 천둥/번개 비바람, 눈보라, 진눈깨비, 큰바람(70mph 이상), 모래폭풍. (L) 외부정전 CRAMM 위협 (3개) 건물화재, 건물수재, 기타 자연재해(지진, 폭풍, 번개 등).

4. 자산의 분류체계

정보시스템의 자산분류는 속성, 위험지대(혹은 위치), 형태 등의 측면에서 다양하게 분류될 수 있다. 자산은 속성에 따라 유형자산과 무형자산으로, 그리고 위치에 따라 물리적 위험지대와 논리적 위험지대로, 그리고 형태에 따라 하드웨어, 소프트웨어, 데이타/데이타베이스, 사용자/전산요원,

시스템 관련문서, 전산자료 저장매체, 통신망 및 관련장비, 기타 부대설비 등으로 구분할 수 있다.

예로서, BDSS에서는 자산의 분류를 크게 유형자산(tangible asset)과 무형자산(intangible asset)으로 구분하고, 유형자산은 (1) 설비/지원 장비, (2) 컴퓨터 장비, (3) 매체 및 소모품, (4) 문서, (5) 인력요소 등 5가지로 분류하고, 무형자산은 (6) 시스템 소프트웨어, (7) 응용 소프트웨어, (8) 신용도 등 4가지로 분류하고 있다. 위협과 자산과 취약성과의 관련성을 파악하기 위해서 아래 53개의 자산항목에 대해서 9가지로 분류된 본 연구의 표준적인 분류체계인 Pi, Li, Mi, i=1,2,3를 ( ) 안에 표시하였다.

(1) 설비 및 지원 장비

P1 : 건물, 전기, 기계, 화재진압기, 화재감지기, 음성통신장비, 비품, 기타.

P2 : 물리적 접근/보안

(2) 컴퓨터 장비

P3 : 중앙처리장치(CPU), 입출력장치, 저장장치, 통신장치, 제어장치, 지원장치, 기타.

(3) 매체 및 소모품

P4 : 자기테잎, 하드디스크, 대량 저장매체, 출력용지의 재고, 지정출력용지의 형식, 기타 매체 및 소모품.

(4) 문서

M1 : 보안, 정책/표준 절차, 기타 문서.

M2 : 응용시스템, 시스템 소프트웨어, 하드웨어, 데이타 화일.

M3 : 사용자 매뉴얼

(5) 인력요소

M1 : 경영, 운영, 관리.

M2 : 프로그래밍 및 분석, 보안.

M3 : 기타 인력요소

(6) 시스템 소프트웨어

L1 : 운영시스템/실행 소프트웨어, 시간 할당시스템, 거래처리시스템, 사용자시간 계산시스템, 뱃치 입력처리시스템, 시스템 유티리티, 기타 시스템 소프트웨어.

L2 : 데이타베이스 관리시스템

L3 : 통신시스템

(7) 응용 소프트웨어

L1 : 소프트웨어, 오용과 남용.

L2 : 데이타, 가용성.

(8) 신용도 ;

M1 : 공공신뢰, 시장점유율, 공급자 지원, 기타.

여기서 (1) 설비 및 지원 장비, (2) 컴퓨터 장비, (3) 매체 및 소모품은 물리적 보안에, (6) 시스템 소프트웨어, (7) 응용 소프트웨어는 논리적 보안에, (4) 문서, (5) 인력요소, (8) 신용도는 경영 보안에 포함된다. 이와 같은 자산의 분류항목들은 서로 각각 독립적이어야 한다. 자산의 독립성은 특정 위협 및 취약성과의 관계를 정의하는데 뿐만 아니라, 자산의 가치를 산정하는데도 필요하다.

5. 취약성의 분류체계

취약성이 있다고 해서 곧 바로 손실를 입지는 않지만, 위협요소들이 침입할 수 있는 근거를 제공하게된다. 한가지 위협에 대해서 여러가지 보안대책을 강구할 필요도 있고, 반대로 한가지 보안대책이 여러가지 위협에 대한 보호조치로 선택될 수도 있다. 그러므로, 위협의 관점보다는 취약성

의 관점에서 보안대책의 분류체계를 고려하는 것이 합리적이다. 취약성 개념은 정보시스템에 대한 위험을 모형화하는데 중요한 역할을 한다. 취약성 개념에는 일반적으로 다음과 같이 세가지가 있다.

첫째 취약성을 '자산의 속성(attribute of assets)'으로 정의 하고 있다. Otwell과 Aldridge(1989)는 취약성을 "자산을 손상시켜서 위험을 일으키는 시스템의 성질"이라고 했다. 보다 구체적으로 "시스템 내에서 불법적 상태로 변화되는데 소요되는 노력의 양(the amount of effort)에 대한 부적인 정도(inverse measure)" 라고 정의했다. Moses(1992)는 취약성을 "기존 시스템의 약점"이라고 했다.

둘째 취약성을 '보안대책의 결핍(absence of safeguards)'으로 정의하고 있다. Guarro(1988)는 취약성을 "위협공격에 대한 통제 실패확률"이라고 했다. 시스템보안 연구위원회(1991)에서는 취약성을 "위협공격에 노출되어 있는 시스템의 상태"라고 했다. Gilbert(1991)는 취약성을 "보안대책시스템 내에 약점, 혹은 보안대책의 결핍"이라고 했다. 체크리스트 접근방법에 의해서 위험관리를 하는 경우에는, 취약성을 보안대책의 결핍상태로 정의하고 취약성 평가를 위해서 보안대책의 유무를 식별하여, 보안대책이 결핍상태에 있는 경우 위협발생을 감소시킬 수 있는 보안대책을 제시한다.

세째 취약성을 '자산과 위협의 관계(relationship between assets and threats)'로 파악하고 있다. Katzke(1988)는 취약성을 "자산, 위협, 보안대책, 보안대책 효과 간의 함수관계를 갖는 실체(entity)"라고 정의했다. Schmidt(1988)는 취약성을 "위협영향과 자산의 대응관계"로 파악하고, 취약성을 도출하기 위해서 다음과 같은 3가지 고려사항을 제시했다. 첫째는 자산이 위협받을 가능성, 둘째는 자산이 위협에 의해 손상되는 정도, 세째는 보안대책효과이다.

취약성의 분류는 일반적으로 물리적 취약성(출입통제, 환경관리 등), 기술적 취약성(하드웨어, 운영체제, 응용소프트웨어, 네트워크, 데이타베이스 등), 관리적 취약성(보안관리, 전산요원/이용자 관리, 보안정책의 문서화, 사고대책 관리 등)으로 구분할 수 있다. 그러나, 자산의 경우와 마찬가지로 취약성에 대한 분류체계 역시 관점에 따라 서로 다르므로, 본 연구에서 설정한 표준적인 분류체계를 근거로, BDSS의 사례를 비교분석하고자 한다.

예로써, BDSS의 취약성 계층구조는 우선 취약성을 크게 5개 집단으로 분류하고, 그 하위요소들을 20개 집단으로 세분하였으며, 그 아래에 모두 94개의 취약성 항목들을, 다음과 같이 제시하고 있다.

(1) 물리적 시설

P1 : 화재감지기 및 진압기 - 화재감지기, 화재진압기.

P1 : 입지 - 지질, 기후, 군사시설의 근접도, 산업시설의 근접도, 외부화재로 인한 재난, 수송시설, 공공시설, 사회적 환경, 인적자원, 공급자 지원.

P1 : 건축 - 설계, 빌딩자재, 비품.

P1 : 전력시스템 - 전력원, 전력용량, 보조전원, 긴급통제.

P1 : 기계시스템 - 상하수도관, 공기정화장치(HVAC).

(2) 접근

L1 & L2 : 소프트웨어/데이타 접근 - 접근통제 소프트웨어, 응용 소프트웨어 및

데이타 접근, 시스템 소프트웨어.

P2 : 물리적 접근 - 데이타 처리지역, 지원설비, 터미날지역, 사용자지역, 관리지역, 편의시설, 주변지역, 컴퓨터지역, 통제품목, 창고

L3 : 통신 접근 - 외부 접근보안, 논리적 접근보안, 전송보안.

(3) 시스템 소프트웨어(공급자 제공) :

L1 : 일반사항 - 공급자지원 보안, 정전감지 및 오류교정, 변경통제 및 시험.

L1 : 운영시스템 - 주기억장치의 보호, 실행영역, 보안 및 통제 사양, 시스템 로그, 주기억장치의 잔류기억 초기화.

L1 : 시스템 유티리티 - 일반 유티리티, 데이타베이스 관리시스템, 온라인 시스템.

(4) 하드웨어(공급자 제공)

P3 : 메인프레임, 콘트롤러, 통신장치, 직접접근 저장기기, 테입 드라이브, 터미날, 프린터, 출력장치 마이크로 휘치 필름.

(5) 관리

M3 : 인사 - 고용, 훈련 프로그램, 행동관찰, 인사이동 및 직책변동, 퇴직.

M1 : 보안관리 - 정책 및 표준, 훈련 및 주의, 패스워드 및 사용자 ID관리, 물적 접근관리, 적용한계성의 분류, 데이타 관리.

M2 : 품질보증 - 의무의 분리, SDLC 표준, 시스템 개발검토, 시험, 변화통제.

M2 : 비상계획 - 비상준비, 비상계획 메뉴얼, 위기대처능력, 훈련시험, 계획유지관리

M2 : 운영 - 의무의 분리, 공급자지원, 생산통제, 작동 로그, 백업, 테입 관리시스템.

M2 : 응용 및 시스템 소프트웨어 - 의무의 분리, 시스템 개발절차, 백업 및 회복절차

M2 : 유지관리 및 시험 ; 컴퓨터 장비, 시설, 사무실관리, 접근보안 시스템, 전기 시스템.

M1 : 경영계획 - 예산, 장기계획, 조직계획.

여기서 (1) 물리적 시설, (4) 하드웨어는 물리적 보안에, (3) 시스템 소프트웨어는 논리적 보안에, (5) 관리는 경영보안에 포함된다. (2) 접근만은 물리적 및 논리적 보안이 중복되어 있다.

이와 같이 취약성을 분류한 후에, 취약성을 평가하는 목적은 자산에 손실이 발생될 수 있는 약점을 식별하고 분류하여 위협을 감소시키는데 있다. Moses(1992)에 의하면, 취약성 평가(vulnerability assessment)란 "식별된 위협원천에 의해서 손상될 수 있는 기존 시스템의 약점에 대한 심각성 수준을 식별하고 평가하는 것"이라고 했다. 취약성 평가는 취약성에 대한 정의에 따라 그 방법이 달라질 수 있다. 단순히 '자산의 속성'으로만 정의하면, 취약성을 정성적으로나 정량적으로 평가하기가 어렵다.

'자산과 위협의 관계'로 정의하면, 관계에 대한 구체적 모형이 제시되어야 한다. 계량적인 평가모형을 도출해도 실증적으로 적용하는데는 위협발생 혹은 손실발생에 대한 확률추정을 해야하는데, 이에 대한 과거자료를 확보한다는 것은 사실상 어려운 문제이다.

6. 결 론

본 논문은 정보시스템 보안관리에 대한 개념적 모형을 한국전산원이 제시한 모형을 중심으로 기술했으며, BDSS의 사례를 비교분석하기 위해서 표준적인 분류체계를 설정해 놓고, BDSS의 위협, 자산, 취약성의 분류체계를 비교 함으로써, 위협, 자산, 취약성의 관련성을 탐색 하고자 했다.

첫째, 보안관리는 과정적 측면에서 정보기술 보안의 목적/전략/방침 설정 → 정보기술 보안 요구사항 및 범위결정 → 자산 분석→ 위협 분석→ 취약성 분석 → 위험 측정 → 위험평가에 의한 보안대책의 선택 → 정보기술보안계획에 의한 비용효과 분석 → 보안대책 구현 및 보안교육 → 보안감사 및 사후관리로 구성되어 있다.

둘째, 보안관리에 대한 표준적인 분류체계를 물리적 보안(환경 보안(P1), 물적접근 보안(P2), 물적가용 보안(P3)), 논리적 보안(소프트웨어 보안(L1), 데이타 보안(L2), 통신 보안(L3)), 경영 보안(관리적 보안(M1), 조직적 보안(M2), 인적 보안(M3))으로 분류하였다.

세째, 위협의 원천에 따라 내부위협과 외부위협, 그리고 위협의 가해자에 따라 인간위협과 비인간위협으로 분류했을때, BDSS의 위협은 인간위협보다는 비인간위협에, CRAMM의 위협은 외부위협보다는 내부위협에 편중되어 있다. 표준분류체계에 의한 P, L, M과의 관련성은 (표1)과 같다.

네째, BDSS에서는 자산의 분류를 크게 유형자산 (tangible asset)과 무형자산 (intangible asset)으로 구분하고, 유형자산은 (1)설비 및 지원 장비(P1, P2), (2)컴퓨터 장비(P3), (3)매체 및 공급(P3), (4)문서(M1, M2, M3), (5)인원(M1, M2, M3) 등 5가지로 분류하고, 무형자산은 (6) 시스템 소프트웨어(L1, L2, L3), (7) 응용 소프트웨어(L1, L2), (8) 신용도(M1) 등 4가지로 분류하고, 53개의 자산항목으로 세분화되어 있다.

다섯째, BDSS에서는 취약성의 분류를 크게 5개 집단, 즉 (1)물리적 시설(P1), (2) 접근(P2, L1, L2, L3), (3) 시스템 소프트웨어(L1), (4) 하드웨어(P3), (5) 관리(M1, M2, M3)로 분류하고, 그 하위집단으로 20개 집단으로 분류하고, 그 아래에 모두 94개의 취약성 항목으로 세분화되어 있다.

표준분류체계에 의한 P, L, M에 의해서 위협과 취약성의 관계, 혹은 자산과 취약성의 관계, 혹은 위협과 자산의 관계를 설정해야 한다. 일반적으로 자산의 분류체계는 발생된 손실에 대한 대체비용을 계산하기 위해서 독립적으로 이용되지만, 특히 위협과 취약성의 분류체계 간에는 서로 종속적인 관계를 설정하게 된다. 여기서 P, L, M간의 관계는 M 〉 P 〉 L 이다. 즉 물리적 보안에 논리적 보안이 포함되어 있고, 경영보안에는 물리적 보안은 물론 논리적 보안도 포함되어 있다. 그러므로, 보안설계에서 가장 중요한 문제는 위협과 취약성 간의 M 〉 P 〉 L의 종속관계를 설정하는 일이다.

BDSS에서는 61개의 위협과 94개의 취약성 간에 mapping이 정해져 있다. 즉 위협 P, L, M의 요소와 취약성 P, L, M의 요소를 대응시키는 규칙을 다수준, 다기능으로 정해서 2400 여개나 되는 질문들을 만들어 놓았다. 하나의 질문으로서 하나의 특정 위협에만 대응되는 한가지 취약성을 파악할 수도 있다. 예로써, 화재와 화재진압기와의 관계이다. 어떤 경우에는 여러개의 위협에 대응되는 한가지 취약성을 파악 할 수도 있다. 예로써, 여러개의 위협에 대응되는 한가지 비상계획과의 관계이다. 이와 같이 위협과 취약성의 각 요소들 간의 관계를 어떻게 mapping시켜서 설계하느냐에 따라 보안관리의 효율성이 결정된다.

참 고 문 헌

〈국내문헌〉

김기윤, "정보기술에 대한 위험분석방법", 기업경

영연구, 광운대학교 , 기업경영연구소, Vol.3, 1994. 11, pp.1-18.

_____ 과 김정덕, "정보시스템 위험분석과 관리", '94년도 추계학술대회논문집, 한국경영정보학회, 1994. 11., pp. 277-297.

_____ 과 김정덕,"정보보호를 위한 위험분석방법: 분류와 선택기준을 중심으로", '94년도 학술대회논문집, 한국통신정보보호학회, 1994. 11, pp. 303-315.

_____ 외 12인, "전산망 보안을 위한 위험관리 지침서", 연구보고서, 한국전산원, 1994. 12.

_____ 과 신동익, 김정덕, 박태완, "전산망 보안관리를 위한 기술지원서: 소프트웨어 보안", 연구보고서, 한국전산원, 1994. 12.

〈외국문헌〉

[1] Baskerville, Richard, "Information System Security Design Method: Implications for Information Systems Development," ACM Computing Surveys, Vol.25, No.4, Dec. 1993, pp375-414.

[2] Commission of the European Communities Security Investigations Projects, Risk Analysis Methods Database, Project S2014 - Risk Analysis, Report Number 19744 (S2014/WP08), Version 1.0, Jan. 1993.

[3] Commission of the European Communities Security Investigations Projects, Final and Strategy Report, Project S2014 - Risk Analysis, Report Number 9744 (S2014/WP08), Version 1.0, Feb. 1993.

[4] FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974, U.S. Department of Commerce/National Bureau of Standards, May. 1975.

[5] FIPS PUB 65, Guidelines for Automatic Data Processing Risk Analysis, U.S. Department of Commerce/National Bureau of Standards, Aug. 1979.

[6] FIPS PUB 73, Guidelines for Security of Computer Applications, U.S. Department of Commerce/National Bureau of Standards, Jun. 1980.

[7] Hysert, R., The Life-Cycle Model in the Risk Management Framework, Proceedings of the 5th International Computer Security Risk Management Workshop, Ottawa, Canada, Mar. to Apr. 1993 pp.10-20.

[8] ISO/IEC JTC1/SC27 N689, Guidelines for the Management of IT System Security: Part3-Techniques for the Management of IT Security, ISO, Mar. 1993.

[9] ISO/IEC JTC1/SC27 N720, Guidelines for the Management of IT Security(GMITS): Part2-Managing and Planning IT Security, ISO, 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. Katzke, Stuart W., A Government Perspective on Risk Management of Automated Information System, Proceedings of Computer Security Risk Management Model Buildings Workshop, Denver, Colorado, May. 1988, pp.3-11.

[12] Loch, Karen D. & Carr, Houston H. & Warkentin, Merrill E., "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly, Jun. 1992, pp.173-186.

[13] Moeller, Robert R., Computer Audit, Control, and Security, John Wiley & Sons, Inc., 1989.

[14] Moses, Robin, "Risk Analysis and Management," Computer Security Reference Book edited by Jackson, K. M. & Hruska, J. & Parker, Donn B., CRC Press, Inc., 1992, pp.227-263.

[15] "CCTA Risk Analysis and Management Methodology(CRAMM)," Datapro Reports on Information Security, December 1992, pp.101-110.

[16] "A European Standard for Risk Analysis," Proceedings of the 10th World Conference on Computer Security, Audit and Control, Lodon, UK, 1993, pp.527-541.

[17] NIST, U.S. Department of Justice Simplified Risk Analysis Guidelines, NISTIR 4387, Aug. 1990.

[18] Ozier, Perry & Associates and Pickard, Lowe and Garrick, Inc., BDSSTM(the Bayesian Decision Support System), BDSS Product Support Group, OPA, 1988.

[19] Ozier, Will, "Issues in Quantitative Versus Qualitative Risk Analysis," Datapro Reports on Information Security, March 1992, pp101-107.

[20] Paker, Donn B., "The Baseline Challenge to Risk Assessment," Proceedings of the 10th World Conference on Computer Security, Audit and Control, Lodon, UK, 1993, pp490-526.

[21] Perry, William E. & Kuong, Javier F., EDP Risk Analysis and Control Justification, Management Advisory Publications 1981.

[22] Rainer, Rex K., Jr. & Snyder, Charles A. & Carr, Houston H., Risk Analysis for Information Technology, Journal of Management Information Systems, 1991, Vol.8, No.1, pp.129-147.

[23] Robak, Edward & Security and Emergency Planning Staff, U.S. Department of Justice Simplified Risk Analysis Guidelines(SRAG), National Institute of Standards and Technology, Aug. 1990.

[24] Solms, R von & Eloff, J. H. P. & Solms, S. H. von., "Computer security management: a framework for effective management involvement," Information Age, Vol.12, No.4, Oct. 1990, pp. 217-222.

[25] Stang, David J. & Moon, S.,

Network Security Secrets, IDG Books Worldwide, Inc., 1993.

[26] System Security Study Committee & Computer Science and Telecommunication Board & Commission on Physical Science, Mathematics, and Applications, National Research Council, Computers at Risk, National Academy Press, 1991.

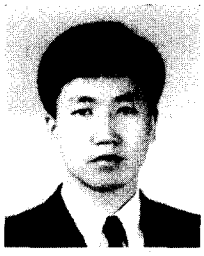
[27] Wood, Charles C. & Banks, William W. & Guarro, Sergio B. & Garcia, Abel A. & Hampel, Victor E. & Sartorio, Henry P., Computer Security: A Comprehensive Control Checklist, John Wiley & Sons, 1987.

□ 著者紹介

김 기 윤

1976년 고려대학교 공과대학 토목/환경공학과 학사
1979년 고려대학교 경영대학원 석사
1985년 고려대학교 대학원 경영학과 박사
1980년 - 현재 광운대학교 경영학과 교수

※ 주관심분야 : 정보시스템 보안/위험관리



나 관 식

1986년 광운대학교 경영학과 학사
1988년 광운대학교 경영학과 석사
1992년 광운대학교 경영학과 박사
1993년 - 현재 경민전문대학 사무자동화학과 전임강사

※ 주관심분야 : 정보시스템 보안/위험관리

김 종 석

1993년 광운대학교 경영학과 학사
1995년 광운대학교 경영학과 석사
1995년 - 현재 광운대학교 경영학과 박사과정

※ 주관심분야 : 정보시스템 보안/위험관리