정보통신망의 효율적 보안관리를 위한 비즈니스 프로세스 기반의 자산평가모델 및 방법론에 관한 연구

우 병 구[†] · 이 강 수[††] · 정 태 명[†††]

요 약

정보통신망의 보안관리나 위험분석시 정형화된 자산분석·평가는 필수적이지만, 기존의 위험분석 방법론 및 도구에는 자산의 분류체계만 다수 제시되어 있을 뿐 구체적인 자산파악 및 가치평가방법은 알려져 있지 않다. 또한, 기존의 자산분류체계는 주로 정보자산이 아닌 일반적인 위험평가를 위한 것이므로, 정보통신망의 정보자산에 대한 분류체계 및 자산가치 평가방법으로는 부적합하다. 특히, 자산평가시의 평가자의 주관성 문제를 해결하는 구체적인 방법이 제시되어있지 못하다. 본 논문에서는 이러한 문제점들을 해결하기 위해, 정형화된 자산평가모델의 정의, 새로운 자산분류스키마, 업무처리(BP)와 자산을 고려한 2차원적 자산업무분류스키마, 다양한 정량가치와 정성가치의 평가방법을 제시하고 특히 무형자산 평가시의 평가자의 주관성 문제의 단점을 보완할 수 있는 베타분포형 델파이 방법을 제안하고자 한다.

A Study on Business Process Based Asset Evaluation Model and Methodology for Efficient Security Management over Telecommunication Networks

Byoung-ku Woo[†] · Gang-soo Lee[††] · Tai-myoung Chung[†††]

ABSTRACT

It is essential security management and standardized asset analysis for telecommunication networks, however existing risk analysis methods and tools are not enough to give shape of the method to evaluate value and asset. they only support asset classification schemes. Moreover, since the existing asset classification schemes are to evaluate comprehensive general risk, they are not appropriate for being applied telecommunication networks and they can't offer any solutions to an evaluator's subjectivity problem. In this paper, to solve these problems, we introduce the standardized definition of asset evaluation model new asset classification scheme, two-dimensional asset process classification scheme to consider business process and asset, various evaluation standards for quantitative value and qualitative evaluation. To settle an evaluator's subjectivity problem, we proposed β - distribution Delphi method.

키워드 : 위험분석(Risk Analysis), 자산분류스키마(Asset Classification Schemes), 정형화 자산평가모델(Asset Evaluation Model), 보안관리(Security Management)

1. 서 론

국가·공공기관 및 기업체에서 정보기술에 대한 비중이 증대됨에 따라, 정보통신망의 효율적인 보안관리문제가 대두되고 있다[1-3]. 보안관리는 보안정책을 수립[4, 5], 실행 및 위험분석과정[6-8] 등을 통해 이루어지며 이를 위해서는 보안정책에 의해 보호 되야 하는 자산(asset)을 식별하고 그 가치를 평가해야한다. 또한, 국제공통평가기준(CC, Common Criteria)기반의 정보보호제품군별 공통 기능 및 보증요구사항이라 할 수 있는 CC의 보호프로파일(PP, Protection Profile)을 개발하기 위해서도 우선 자산평가가 이루어져야 한다[9, 10].

보안관리, 보안정책, 위험분석 및 정보보호 시스템 평가부문의 PP개발 등에서 각각의 방법론 또는 자산의 분류체계는 서로 상이하며 국제적인 표준 자산분류체계는 알려져 있지 않다. 또한, 보안관리나 위험관리를 위한 정보시스템 내의 자산의 가치평가 방법에 대한 연구는 매우 원론적인 수준에 머물고 있다. 따라서, 자산의 분류체계와 자산의 가치를 평가하는 정형적이고 이론적 근거를 갖는 자산평가방법론이 요구된다. 특히, 무형자산의 평가는 평가자의 주관성이 개입되므로, 이를 개선하기 위한 검증된 방법이 필요하다.

이와 같은 배경에서, 본 연구에서는 보안정책의 수립, 위

† 준 회 원 : 국가보안기술연구소 전문위원
†† 종신회원 : 한남대학교 컴퓨터공학과 교수
††† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2003년 5월 6일, 심사완료 : 2003년 5월 21일

험분석, 보안대책의 개발 및 정보보호 시스템 평가를 위한 PP의 개발 등에서 공통적으로 필요한 BP(Business Process) 기반의 자산파악 및 평가방법을 제시한다. 본 논문의 2장에서는 자산평가활동을 추상화하고 정형화한 모델인 "공통 평가모델"을 정의하고 이를 이용하여 새로운 "자산평가모델"을 정의한다. 3장에서는 BP 기반의 자산평가 방법론에서 사용되는 각종 기준과 방법들을 제시한다. 4장에서는 3장에서 제시한 내용을 이용한 BP 기반의 자산평가 방법론을 제시한다.

2. 자산 평가모델

2.1 공통 평가모델

ISO/IEC 9126과 14598[11, 12]에 근거하여 다음과 같이 "공통 평가모델"을 정의한다. 공통 평가모델이란 어떤 형태의 평가에도 적용할 수 있는 모델을 의미하며 공통 평가모델은 다음과 같이 정의한다.

$$M : x \rightarrow y \text{ 또는 } y = M(x)$$

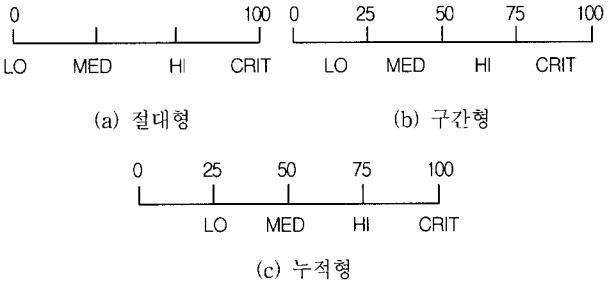
- M : 측정(measurement)행위이며 평가대상 실체의 속성을 서술하기 위해, 특정 단위 또는 카운팅 규칙을 사용하여 실체에 숫자 또는 범주를 할당하는 행위 또는 프로시저를 의미한다. 측정결과는 미리 정의된 측정스케일에 등급화 한다.
- x : 평가대상 속성이며 실체의 측정 가능한 물리적 또는 추상적 특성을 의미한다. x들로 구성되는 공간을 평가정의역(evaluation domain)이라 한다.
- y : '등급수준(rating level)'이며 서수(ordinal) 스케일상의 스케일 포인트이다. y들로 구성되는 공간을 평가 치역(evaluation range)이라 한다.

측정스케일은 다음과 같은 형태가 존재한다.

- 연속 형태 : 실수 또는 정수 축이 측정스케일이 될 수 있으며 정량 평가 시에 사용된다.
- 이산 형태 : 정성 평가시에 사용되며, 실수 축 상의 불연속적인 점 또는 구간이다. 스케일의 크기(유한하다고 가정)를 분할한 개수에 따라 여러 측정 스케일 체계들로 나눌 수 있다.
  - 2단계 : Low/High, Pass/Fail, True/False, 0/1
  - 3단계 : Low, Medium, High
  - 4단계 : Low, Medium, High, Critical

유한한 실수 또는 정수 축을 단계수로 나누어 등급수준을 대응시키는 방법은 (그림 1)과 같이 3가지 경우가 존재한다[15].

위험분석시 자산가치 평가, 자산중요성 평가, 위협수준 평가, 취약성수준 평가, 위험수준 평가가 실시되며, 각 평가들은 다음과 같이 일반 공통모델을 적용할 수 있다[6-8].



(그림 1) 측정스케일의 선택방법

2.2 자산평가모델 설계

자산평가모델은 평가대상 기관(TOE, Target of Evaluation)의 정확한 자산파악 및 자산분류를 위해 자산공간 내의 단위자산(elementary asset) a_i들과 업무공간내의 단위업무들을 자산분류공간과 업무분류공간의 결합공간인 자산업무분류공간에 사상하고 분류된 각 자산에 대해 정량가치 또는 정성가치를 평가하는 업무를 추상화 및 정형화한 것이다.

본 연구에서는 공통 평가모델을 이용하여 자산평가모델을 정의하였으며, 집합 또는, 공간, 사상 개념 및 프로시저(procedure) 개념을 이용하였다. 특히, 사상의 불확실성 및 주관성 문제 때문에 함수가 아닌 프로시저를 이용한다.

자산평가모델(AAM)의 정의는 다음과 같이 정의한다.

AAM = <A, AS, B, BS, ABS, AVS, ALS, *ident, vevl, levl*>

- A(자산공간) = $\{a_1, a_2, \cdots, a_i, \cdots, a_n\}$,
  여기서, a_i는 단위자산(elementary asset).
- AS(자산분류공간) = $\{AS_1, \cdots, AS_i, \cdots, AS_n\}$,
  $AS_i = \{AS_{i1}, \cdots, AS_{ii}, \cdots, ASin\}$,
  여기서, $AS_{ij} \in A$ 2수준 분류의 경우
- B(업무공간) = $\{b_1, b_2, \cdots, b_i, \cdots, b_n\}$,
  여기서, b_i 단위업무(elementary business).
- BS(업무분류공간) = $\{BS_1, \cdots, BS_i \cdots, BS_n\}$,
  $BS_i = \{BS_{i1}, \cdots, BS_{ii}, \cdots, BSin\}$,
  여기서, $BS_{ij} \in B$ … 2수준 분류의 경우
- ABS(자산업무분류공간) = AS × BS
- AVS(정량가치공간) = R(실수공간)
- ALS(정성가치공간) = {L1, L2, …, Ln}
- ident(자산파악 프로시저) : AS → ABS
- vevl(정량가치평가 프로시저) : ABS → AVS
- levl(정성가치평가 프로시저) : AVS → ALS

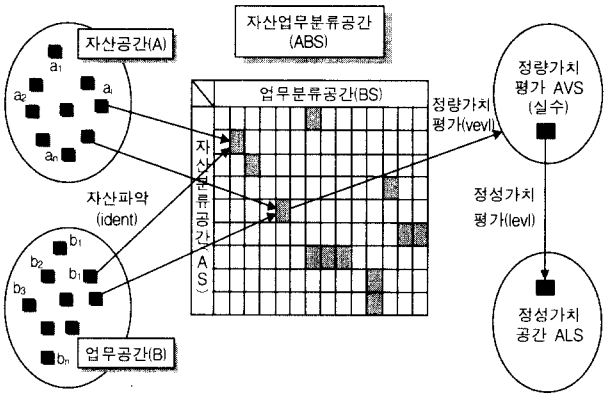
본 연구에서는 자산가치의 개념을 다음과 같이 두 가지로 분류하여 정의한다.

- 정량가치 : 평가 시점에서의 자산의 정량적 또는 절대

적, 고유 가치이며, 실수 형태의 금액 값이다.

- 정성가치 : 평가 시점에서의 자산의 정성적 또는 상대적 가치이며, 조직의 규모에 따라 결정되는 가치이다. 이는 자산을 보유하고 있는 조직의 규모에 따라, 정성가치를 1부터 n개의 수준에 대응하여 얻을 수 있다.

(그림 2)는 자산평가모델의 구조를 보인다.



(그림 2) 자산평가모델의 구조

자산분류공간(AS, Asset classification Space)은 자산분류스키마(ACS, Asset Classification Schema)라하며 구조적 공간이다. ACS는 n층으로 구성된 자산분류 계층구조이며 자산평가 대상기관의 특성과 무관하게 정의된다. 업무분류공간(BS, Business classification Space)은 업무분류스키마(BCS, Business Classification Schema)라하며 구조적 공간이다. BCS는 n층으로 구성된 업무분류 계층구조이며 자산평가 대상기관의 업무구조 또는 조직구조에 따라 결정된다. 즉, BCS는 자산평가대상기관에 따라 달라진다. 자산업무공간은 자산분류공간과 업무분류공간의 결합공간이며, 자산업무분류스키마(ABCS, Asset Business Classification Schema)라 한다. ABCS 처럼 자산과 업무의 결합으로 자산을 분류하는 방법을 2차원적 자산분류 스키마라 할 수 있다.

정량가치평가 프로시저(vevl)은 ABS 내의 분류된 단위자산을 정량가치공간(AVS)에 대응시키는 과정이다. 즉, 자산의 정량적 가치측정 과정에 해당한다. 정성가치평가 프로시저(levl)는 정량가치공간(AVS) 내의 자산 값을 정성가치공간(ALS)에 대응시키는 과정이다. 즉, 자산의 정성적 가치수준의 측정과정에 해당한다. 정량가치공간은 실수 즉, 아날로그(analog) 형태로 구성되며 정성가치공간은 n의 수준을 갖는 원소 즉, 디지털(digital)로 구성되므로, 이 프로시저는 AD(Analog-Digital) 변환이라 할 수 있다.

3. 자산분류스키마 및 평가알고리즘 구조

3.1 기존의 자산분류체계 문제점

PP/ST 가이드[10] 및 CC[9] 등과 같은 정보보호 시스템 평가기준 부문과 자산분류결과를 제시한 기존의 위험분석 방법 및 평가 도구 중 CMU의 OCTAVE[14], 정보보호진흥원(KISA)의 위험분석 방법[15], BS-7799[2,3], 한국전산원의 HWAK[16], 캐나다의 CSE[17], ETRI의 PRAM[18]에서의 자산분류 체계는 다음과 같은 문제점을 가진다.

첫째, CC와 기존 PP 등 정보보호 시스템 평가 부문에서는 자료만을 기준으로 하고 있다. 이에 따라, 조직전체의 자산평가에는 부적합하다. OCTAVE에서는 장비를 기준으로 분류함으로서, 자산평가 대상기관 내의 데이터나 소프트웨어 및 응용들을 분류하기가 어렵다.

둘째, 모든 경우에, 자산평가대상기관의 응용을 고려하지 않고 있다. 따라서, 자산파악 및 평가시에 자산평가대상기관 내부자의 지식을 활용하기 어렵다. 사실 자산평가대상기관의 내부자만 자산평가대상기관의 응용에 대한 지식을 가지고 있다. 또한, 자료나 정보를 최상위 단계에서 분류하고 있다. 자산평가대상기관내의 자료와 정보는 매우 추상적이며 응용과 결부되어야만 가치가 있으므로 자료와 정보를 하위수준으로 분류하는 것이 좋다.

셋째, 정보보호진흥원의 자산분류는 하드웨어와 소프트웨어를 최상위 단계에서 분류함으로서 자산파악시의 결정성이 저하된다. 예컨대, 웹서버의 경우 H/W와 시스템 S/W를 하나의 플랫폼으로 간주하므로, 자산평가시에는 하나의 시스템으로 보는 것이 유리하다.

넷째, OCTAVE 등은, 인간을 고려하지 않고 있다. 따라서, 인간은 자산평가대상기관의 주체이며 위험의 근원이므로 반드시 분류 돼야 한다. 참고로, 자산평가대상기관의 위험은 주로 인간 때문에 발생하며 정보시스템은 인간의 도구에 지나지 않는다.

다섯째, KISA 및 HWAK의 경우, 네트워크와 환경을 최상위 단계에서 분류하고 있다. 최근의 자산평가대상기관의 정보시스템에서는 네트워크와 서버(H/W, OS 등)를 구분하기가 어렵다. 네트워크가 곧 컴퓨터이기 때문이다. 따라서, 네트워크를 하위수준으로 분류하는 것이 유리하다. 또한 BS7799와 CSE에서는 서비스 또는 프로세스를 최상위에서 분류하고 있다. 서비스나 프로세스개념은 자산평가대상기관의 '응용'으로 처리하는 것이 유리하다.

3.2 자산업무분류스키마(ABCS)

자산분류스키마는 자산 파악 및 분류업무에 직결되므로, 자산파악의 용이성과 결정성(determinism)을 제고하여 자산을 분류해야한다. 특히, 자산파악의 결정성이란 자산의 분류결과가 분류자에 무관하게 일정한가를 나타내는 성질이다. 하나의 자산에 대한 분류결과가 여러 가지로 나타날 때 자산파악의 결과는 비결정적(non-determinism)이다. 기존의 자산분류스키마는 비결정적이라는 문제점을 내포하고 있다.

본 연구에서 제시하는 ABCS는 이러한 문제점을 개선하

기 위한 기본 가정은 다음과 같다.

- 조직내의 자산은 자산평가 대상기관내의 업무(즉, 비즈니스 부서)에 따라 설치, 운영된다.
- 조직내의 자산은 BP에 따라 그 가치가 달라진다.
- 조직내의 업무구조는 조직마다 다르며 이미 체계화되어 있다.

이와 같은 가정에 따라, ABCS는 ACS와 BCS의 결합공간으로 구성되며, AS와 BS는 각각 계층구조를 갖는다. 예를 들어, 3수준의 분류 즉, 상위 수준, 중위 수준, 하위 수준으로 구성된 ABCS의 템플리트는 <표 1>과 같은 형태를 가진다. <표 1>에서 단위자산 a_i는 조직내의 업무 적으로는 BS_i 분류 BS_j 분류 내에 BS_k로 분류되며, 자산분류로는 AS_i 분류 AS_j 분류 내에 AS_k 분류에 해당된다.

〈표 1〉 3수준의 ABCS 템플리트

업무분류(BS) / 자산분류(AS)			응용 상위분류 BS_i								
						중위분류 BS_j					
							하위 BS_k				
자산 상위 분류 AS_i											
	중위 분류 AS_j										
		하위 AS_k					자산a_i				

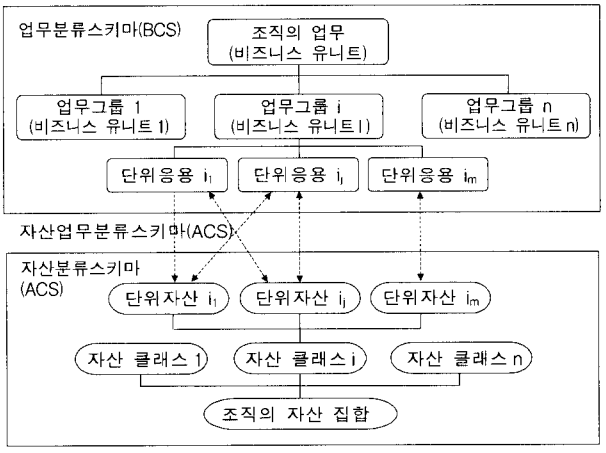
BCS는 평가대상기관의 응용을 위한 기능구조 또는 업무분류구조(WBS, Work Break-down Structure)자체를 사용하며 평가대상기관에 종속된 것이므로, 미리 정의할 필요가 없다.

ACS에서 최상위 수준을 '클래스', 중위 수준을 '컴포넌트', 하위 수준을 '엘리먼트'라 칭한다. 위험평가를 위한 자산평가의 경우, IT에 대한 위험만을 평가할 경우가 많으므로, IT 자산클래스와 인간클래스만을 고려할 수 있다. 이는 평가대상기관의 위험평가 정책 및 범위에 따라 나머지 자산 클래스를 고려한다.

본 연구에서 제시하는 ACS의 속성은 다음과 같다.

- 최상위 수준에서 IT 자산, 인간자산, 비 IT 자산 및 무형자산 클래스로 분류한다.
- 응용 S/W에는 자산평가 대상기관의 응용 분야(기능조직)별 S/W를 분류한다. 자산평가 대상기관대부분의 자산평가 대상기관조직은 응용을 위한 IT를 도입하고 응용별로 개발하므로 자산가치 평가가 용이하다.
- 시스템 S/W에는 별도의 솔루션으로 구매하는 COTS 패키지를 나타낸다.
- 서버 시스템은 PC를 포함해 서버의 H/W 및 OS를 포함한다.
- 컨텐츠에는 IT에서 사용하는 디지털자료(응용 데이터, DB, 보안데이터, 관리데이터, 문서)를 포함한다.
- 거래처 시스템의 B2B 시스템형태에서는 인간은 사람이 아니고 거래처 컴퓨터 자체가 될 수도 있다. 이 개념은 e-비즈니스 시스템에서 활용되고 있다.
- 무형자산에는 노하우, 지적자산 등을 포함한다.
- 비 IT 자산의 경우는 일반문서를 포함한다.

(그림 3)은 자산평가 대상기관의 BCS, ACS 및 ABCS의 관계를 보인다.



(그림 3) ACS, BCS 및 ABCS의 관계

자산평가 단계에서 각 자산의 정성, 정량적가치를 평가하여 해당 위치에 기입하면 자산 클래스별, 업무 클래스별 또는 전체 자산가치를 구할 수 있다.

3.3 정량가치 평가방법

기존의 정량가치 평가기준으로 하드웨어자산의 경우, HAWK[16] 및 CRAMM[19]에서 적용한 방법은 자산에 대한 성능 대비 가격변동에 따른 자산 교체비용을 적용하였으나, 시세차액을 고려한 교체비용을 산정 하는데 시간이 많이 걸리며, TTA-KO-12.0007[6] 및 BS-7799[3]에서 적용한 감가상각비는 운영시 시간경과에 의한 해당 자산의 평가절하를 고려하여 감가상각비용 속성에 해당하는 자산의 취득비용과 사용연수와 사용연한만을 입력한 결과를 H/W 자산가격으로 결정한다.

TTA-KO-12.0007과 BS-7799에서는 상용 S/W는 구매비용에 무료 보상이 가능한 보증 정보의 합으로 산정하고 있다. TTA-KO-12.0007와 BS-7799에서는 개발 S/W는 재개발비에 기회비용을 합산하고 있다. 자료와 무형자산의 경

우, HAWK에서는 자료와 무형자산에 대한 가치산정을 위해 복구비용과 손실비용을 이용한 간접적 산정을 적용하였고, TTA-KO-12.0007와 BS-7799는 자료에 대해선 복구비용을, 무형자산에 대해서는 중요도에 따른 정성적 평가로 자산가격을 산정 하였다.

〈표 2〉 자산 및 취득 방법별 계산유형(A~H)

자 산		취 득 방 법			
자산 분류	자 산 컴 포 넌 트	자체 개발	용역 개발	구 입	기 타
IT 자 산	1.1 응용	A	B	C	D
	1.2 시스템 S/W(OS제외)	A	B	C	D
	1.3 서버시스템(OS포함)	E	F	G	H
	1.4 보조장비 (드라이버 S/W 포함)	B	F	G	H
	1.5 네트워크시스템 (컨트롤러 H/W포함)	E	F	G	H
	1.6 컨텐츠	L	L	L	L
인 간	2.1 사용자	I	J		K(고객)
	2.2 응용담당자	I	J		
	2.3 IT 담당자	I	J		
비 IT 자 산	3.1 사무기	E	F	G	H
	3.2 설비	E	F	G	H
	3.3 문서자료	A	B	C	D
무 형 자 산	4.1 비즈니스 협력관계				L
	4.2 노하우				L
	4.3 지재권				L
	4.4 명 성				L

〈표 3〉 유형별 계산규칙(정량가치 평가)

유 형	계 산 방 법	근 거
A	개발비×CI + Ava	개발비 인정
B	{(용역비 + 내부자인건비 + 용역관리비)×CI} + Ava	조직내 용역관리비 등 고려
C	{(취득가액 + 업그레이드비용)×CI} + Ava	구입후 업그레이드 비용 포함
D	(일반 판매가격)×CI + Ava	판매가 적용
E	[개발비용 - {취득연한×(개발비용/사용연한)}]×CI + Ava	H/W 감가삼각비 적용
F	[용역 총비용 - {취득연한×(용역 총비용 / 사용연한)}] × CI + Ava	H/W 감가삼각비 적용
G	[취득비용 - {취득연한×(취득비용 / 사용연한)}]×CI + Ava	H/W 감가삼각비 적용
H	[판매가격 - {취득연한×(판매가격 / 사용연한)}]×CI + Ava	H/W 감가삼각비 적용
I	년봉×CI	경력년수를 고려
J	용역비×CI	경력년수를 고려
K	고객수×고객당비용	조직의 특성을 고려
L	"베타분포형 델파이 방법" 적용	평가의 객관성을 제고

(*) 자산이 다수의 업무에서 공용할 경우, 공유율과 BP 가중치를 적용한다.

본 연구는 평가대상 조직내의 기존 자산을 평가하는 것이므로, 개발할 소프트웨어 자산에 대한 개발비용을 예측하거나 용역대가를 산정 할 필요는 없다.

본 연구에서는 자산의 클래스와 취득 방법별로 평가기준을 달리하고 있으며 <표 2>와 <표 3>은 각 자산 클래스별 평가기준을 보인다.

BP의 가중치 산정은 TOE 내의 단위업무를 기준으로 기밀성, 무결성, 가용성에 관한 평가 요인들을 측정하여 베타분포형 델파이 방법을 적용하여 평가하며 기밀성(C)과 무결성(I)의 자산가치 산정값(CI)을 산출한다.

가용성(Availability)은 다음과 같이 3가지 요소를 고려하여 산출한다.

- 교체비용(RC, Replacement Cost) :

$$RC = RH \times \sum_{i=1}^{n} (RPi \times WHi)$$

(RH : Replacement Hour,
RP : Replacement Person,
WH : Wages per Hour)

- 데이터 손실비용(UA, Unrecovered Amount) :

$$UA = 1/2 \times BP \times \sum_{i=1}^{m} (SPi \times WHi)$$

(BP : Backup Period,
SP : Support Person,
WH : Wages per Hour)

- 업무 피해비용(DA, Damage Amount)

$$DA = AH \times \sum_{i=1}^{l} (DPi \times WHi) + AL$$

(DP : Damage Person,
WH : Wages per Hour,
AH : Alternation Hour)

AL(Acquired Lost)는 베타분포형 델파이 방법을 사용하여 정량화하며 가용성 측면의 자산비용(Ava)은 RC + UA + DA가 된다. 따라서 BP를 고려한 자산가치 평가는 업무단위의 기밀·무결성을 종합한 가치척도(CI)와 가용성 측면의 자산가치 평가비용을 합하여 계산한다.

BP 적용 자산가치 = (순수 자산가치 × CI) + Ava

3.4 베타분포형 델파이 방법

비즈니스 협력관계, 노하우, 지적재산권 등의 무형자산의 가치는 같이 평가자에 따라서 평가결과의 편차가 매우 크다. 이와 같은 평가의 불확실성 및 주관성문제는 확률적 방법, 퍼지(Fuzzy)이론 적용, 델파이(Delphi) 방법 등으로 극복을 하고 있다.

베타분포(Beta distribution)는 1950년대 이래 공정관리에

사용된 모델인 PERT/CPM의 기본 모델이며 인간에 의해 행해지는 현상을 매우 잘 반영하고 있다[20, 21].

퍼지이론도 불확실의 표현 모델로서 1964년 스텐포드대학의 Zadde 교수가 제시한 이래 제어 및 계측 등 불확실성 및 애매성이 포함된 각종 현상들을 모델링하고 있다[22].

델파이 방법은 불확실성이 있는 미래를 예측하기 위한 그룹 의견조정 방법이며, 위험평가나 소프트웨어 개발비 산정부문 등에서 다수의 전문가에 의한 예측 방법으로 활용되고 있다[23].

본 연구에서는 다음사항을 가정하고 컨텐츠·무형자산 등의 가치평가를 위해 '베타분포형 델파이 방법'을 제안한다.

- 가정 1 : 자산의 가치에 대한 개인적 평가 값들은 베타분포를 갖는다.
- 가정 2 : 다수의 전문가들의 평가 값은 다수의 익명적 의견조정과정을 통해 일정한 평가 값에 수렴한다.

베타분포는 구간 [0, 1]에서 정의되는 2-모수 분포이며, 다음과 같은 확률밀도 함수를 가진다[20].

$$f(x)=\begin{cases}\dfrac{\Gamma(\alpha+\beta)x^{\alpha-1}(1-x)^{\beta-1}}{\Gamma(\alpha)\Gamma(\beta)} & (0\le x\le 1)\\ 0 & (x\le 0 \text{ or } x\ge 1)\end{cases}$$

여기서, 평균과 분산은 다음과 같다.

$$\text{평균 : } E(x)=\alpha/(\alpha+\beta)$$

$$\text{분산 : } Var(x)=\frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}$$

베타분포는 α와 β의 값을 변화시킴으로써 여러 형태의 모양을 얻을 수 있다. 일반적으로 많이 사용되는 형태는 구간[a, b] 상에서 최소의 값(a), 최우(maximum likelihood)의 값(m) 및 최대의 값(b)을 통해 다음 추정공식으로 평균과 분산을 구한다.

$$\text{평균 : } \mu=(a+4m+b)/6 \quad \text{분산 : } \nu=[(b-a)/6]^2$$

베타분포형 델파이 방법에서 자산 평가자는 자산에 대한 경영적 및 실무지식을 가진 사람과 개별면담 또는 설문으로 통해, 각 무형자산 항목에 대해 각각 평가한다. 이때 베타분포의 3가지 모수, 최소값(a), 최대값(b), 최우값(m)을 정하고 이를 이용해 평균(μ)과 분산(ν)을 구한다. 자산 평가자들 간의 평가결과(즉, μ와 ν)가 다르므로, 이를 조정하기 위해서 익명으로 3라운드에 걸쳐 재평가하여 최종평가결과를 도출한다.

- 조정자 : 우선 평가대상자료(instrumentation) 배포하고 3라운드에 걸친 평가표 배포 및 비동기적으로 평가결과를 정리한다(서로 다른 내용을 해당자에 배포). 최종 평가결과를 도출하여 평가자에게 통보한다.
- 평가자 : 3~5명으로 구성되며 평가대상자료를 통한 무형자산의 자산가치평가(베타분포의 3가지 모수(a, b, m)을 정한다. 평가대상자료와 이전라운드의 평가결과를 참고로 하여 재평가를 실시하고 평가결과를 조정자에게 송부한다.

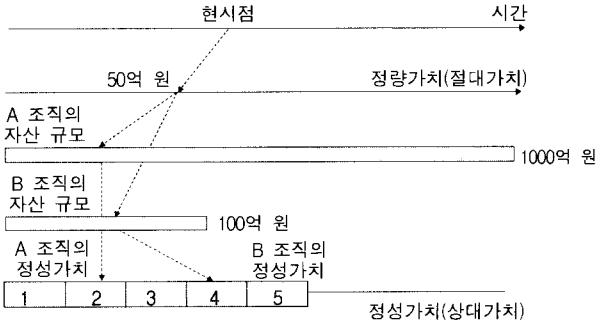
3.5 정성가치 평가방법

<표 4>는 기존의 위험분석 방법론 및 도구 등에서 사용하는 정성가치 기준을 요약한 것이다.

〈표 4〉 기존 위험분석 정성가치의 기준

구 분	정성가치 평가대상 속성	수준 수
BS-7799	자산가치	5
카나다 CSE	자산민감도	5
NIST-65, HAWK	손실액	8
	연간기대손실치(ALE)	7
한국 TTAS	자산	5
CRAMM	자산가치	10
ETRI-PRAM	자산가용성, 금전손실, 법적 책임	5
ISO-13335-5	자산가치	5

정량가치는 자산의 현재가격을 의미하며 구입가격에 감가상각비 등을 고려한 가치이며, 자산을 보유한 조직의 규모에 무관한 값으로 정량가치는 시간에 따라서 변동된다. 정성가치는 자산의 정량가치를 조직의 규모를 고려해 5가지 수준으로 구분한 것으로 (그림 4)는 정량가치와 정성가치간의 관계를 보인다.



〈그림 4〉 정량가치와 정성가치간의 관계

본 연구에서는 해킹 등으로부터 발생한 조직내 자산의 피해액을 기준으로 정성가치를 평가한다. <표 5>의 자산별 정성가치 계산유형에 대해 <표 6>~<표 8>과 같이 각 자산유형별 정성가치 평가기준을 정의하였다. 본 정성가치 평가기준은 정성가치 평가기준 조정단계에서 평가대상기관의 보안정책, 평가정책 및 조직의 매출규모에 따라, 기본 변수(비용)를 조정한다.

〈표 5〉 자산별 정성가치 계산유형 (A~H)

자 산		계산유형	계산규칙
자산클래스	자산컴포넌트		
IT 자산	1.1 응 용	A	<표 6>
	1.2 시스템 S/W	A	<표 6>
	1.3 서버 시스템	A	<표 6>
	1.4 보조장비	A	<표 6>
	1.5 네트워크 시스템	A	<표 6>
	1.6 컨텐츠	B	<표 7>
인 간	2.1 사용자	C	<표 8>
	2.2 응용 담당자	C	<표 8>
	2.3 IT 담당자	C	<표 8>
비 IT 자산	3.1 사무기	A	<표 6>
	3.2 설 비	A	<표 6>
	3.3 문서 자료	B	<표 7>
무형자산	4.1 비즈니스 협력관계	A	<표 7>
	4.2 노하우	A	<표 7>
	4.3 지재권	A	<표 7>
	4.4 명 성	A	<표 7>

〈표 6〉 H/W, S/W 및 IT 자산가치 수준 (계산유형 A)

측정 스케일	등 급 화 기 준 (평가대상기관의 자산규모, 매출규모에 따라 금액을 따로 정함)
매우 낮음	금전적 손실이 적거나 없는 수준의 금액 (예 : 조직의 자산규모의 5%)
낮 음	최소한의 금전적 손실을 야기하는 수준의 금액 (예 : 조직의 자산규모의 10%)
중 간	보통의 금전적 손실을 야기하고 비즈니스 프로세스에 부정적인 영향을 미치는 수준의 금액 (예 : 조직의 자산규모의 20%)
높 음	심각한 손실을 야기하고 비즈니스 프로세스가 실패가 되는 수준의 금액(예 : 조직의 자산규모의 30%)
매우 높음	개별 또는 조직에 막대한 손실을 입히는 수준의 금액 (예 : 조직의 자산규모의 50%)

〈표 7〉 데이터 및 무형 자산가치 수준 (계산유형 B)

측정스케일	등 급 화 기 준
매우 낮음	기밀성/무결성/가용성이 중요하지 않은 데이터로 금전적 손실이 적거나 없음(예 : 조직의 자산규모의 5%)
낮 음	기밀성/무결성/가용성이 그다지 중요하지 않은 데이터로 최소한의 금전적 손실을 야기함 (예 : 조직의 자산규모의10%)
중 간	기밀성/무결성/가용성의 중요도가 보통인 데이터로 심각한 금전적 손실을 야기하고 비즈니스 프로세스에 부정적인 영향을 미침(예 : 조직의 자산규모의 20%)
높 음	기밀성/무결성/가용성의 중요도가 비교적 높은 데이터로 매우 심각한 손실을 야기하고 비즈니스 프로세스가 실패함 (예 : 조직의 자산규모의 30%)
매우 높음	기밀성/무결성/가용성의 중요도가 매우 높은 데이터로 개별 또는 조직에 막대한 손실을 입힘 (예 : 조직의 자산규모의 50%)

〈표 8〉 인간클래스(계산유형 C)

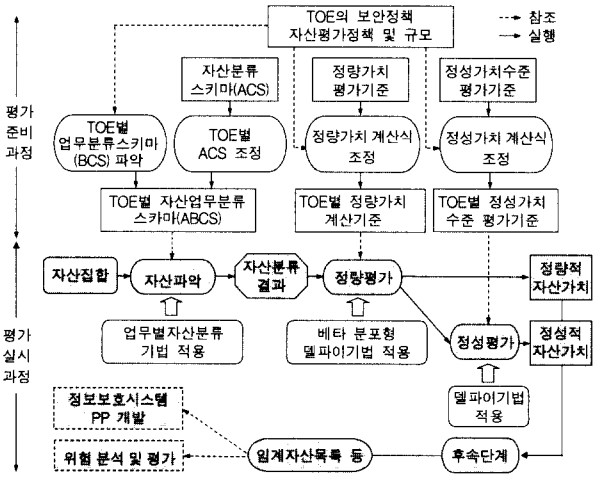
측정 스케일	등 급 화 기 준 (평가대상기관의 자산규모, 매출규모에 따라 금액을 따로 정함)
매우 낮음	금전적 손실이 적거나 없는 수준(예 : 업무 차질 없음)
낮 음	최소한의 금전적 손실을 야기하는 수준 (예 : 업무 75% 가동)
중 간	보통의 금전적 손실을 야기하고 비즈니스 프로세스에 부정적인 영향을 미치는 수준(예 : 업무 50% 가동)
높 음	심각한 손실을 야기하고 비즈니스 프로세스가 실패가 되는 수준 (예 : 업무 25% 가동)
매우 높음	개별 또는 조직에 막대한 손실을 입히는 수준 (예 : 업무 중단)

무형자산의 정량평가는 실수값을 산정하는 것이지만 정성평가는 5등급으로된 자산가치 수준을 평가하는 것이므로, 베타분포와 델파이를 동시에 적용하기는 무리가 있다. 본 연구에서는 자산의 정성가치 평가시에는 베타분포를 사용하지 않는 델파이 방법을 사용한다.

델파이 방법은 3~4절에서 제시한 베타분포형 델파이 방법과 유사하며 3개의 모수(a, b, m)대신 한 개의 수준값(1부터 5 사이의 값)만을 정한다.

4. BP 기반 자산평가 방법론 설계

BP 기반의 자산평가 방법론은 자산평가모델의 각 요소를 구체화한 것이며 (그림 5)는 본 연구에서 제시하는 BP 기반 자산평가 방법론의 구조를 보인다.



(그림 5) BP 기반 자산평가 방법론 구조도

4.1 평가준비과정

평가준비과정은 4단계로 구성되며 세부적인 내용은 다음과 같다.

① BCS 파악단계 : 평가대상기관의 업무구조로부터 BCS를 정의한다. 평가대상기관에는 업무구조가 이미 정해져 있고 조직이 구성되어 있으므로, 조직도 및 업무분

류구조도 등을 이용하면 쉽게 BCS를 파악할 수 있다. 자산평가의 입자성(granularity)에 따라 업무의 계층수를 정한다.

② ACS 조정단계 : 3장에서 정의된 ACS는 일반적인 분류체계이다. 따라서, 평가대상기관의 특성, IT자산만 평가, 모든 자산평가 등 범위와 평가목적을 고려하여 ACS를 자산평가 대상기관별 ACS를 정의한다.

③ 정량가치 평가기준 조정단계 : 평가대상기관의 각 자산의 현재 가치, 감가상각비, 사용연수 등 특성에 따라, 3장에서 정의된 정량가치 평가기준을 평가대상기관 환경에 맞도록 계수 등을 조정한다.

④ 정성가치 평가기준 조정단계 : 평가대상기관의 매출규모 등 특성 및 평가정책 등에 따라 3장에서 정의된 정성가치 평가기준을 자산평가 대상기관의 환경에 맞도록 조정한다.

4.2 평가실시과정

평가실시과정의 세부적인 내용은 다음과 같다.

① 자산파악 단계 : 자산집합(A)내의 각 단위 자산을 파악하여 자산평가 대상기관별 ABCS에 따라 분류한다. 자산평가 대상기관별 BCS를 이용하면 자산을 쉽게 파악할 수 있다. 파악된 자산의 신원을 ABCS의 해당 부분에 기입한다. 참조 기준을 참조하여 입력물인 평가대상 조직의 임무, 활동 및 비즈니스구조를 나타내는 조직구조도, WBS, 업무흐름도(WFD), 정보시스템도면, 네트워크도면 등으로부터 평가대상조직의 자산목록을 도출한다. 자산목록에는 자산의 식별자, 설치위치(BCS 내의 위치), 구입 년도, 상태(상, 중, 하), 획득비용, 획득방법(자체개발/용역개발/구입/기타) 등에 대한정보를 포함한다. 본 단계의 특성은 2차원적인(즉, 업무차원과 자산차원) 응용 자산식별 접근방법을 사용한다는 점이다.

② 정량평가 단계 : 본 단계는 2장의 자산평가모델에서 levl 프로시저에 해당한다. 각 자산의 자산취득가격 정보와 제품수명 정보 등을 바탕으로 하여, 조정된 정량가치 평가기준상의 설계한 계산유형을 적용하여 정량적 자산가치를 평가한다.

무형자산의 경우, 자산취득가격 정보만으로는 평가하기 어려우므로 다수의 자산관련 전문가들로부터 베타분포형 델파이 방법을 이용하여 평가자별 주관성을 줄인다. 베타분포형 델파이 방법은 3장에서 상세하게 설명하였으며 수작업으로 실시하거나 또는 전산시스템을 이용해 구현할 수 있다.

개별 및 클래스별 자산에 대한 정량가격은 <표 9>와 같이 상위수준에서 2차원(즉, 자산-응용 차원)적으로 나타내거나 <표 10>과 같이 하위 수준에서 단위자산별로 정렬할 수도 있다.

③ 정성평가 단계 : 자산평가 모델에서 vevl 프로시저에 해당한다. 각 자산의 정량평가결과와 평가대상 조직의 매출규모, 자본금 규모, 직원수 등의 자료를 이용하고 "조정된 정성가치 평가기준"을 참조하여 자산의 정량평가결과로부터 정성가치(5단계 스케일)를 평가한다.

〈표 9〉 정량평가결과

(단위 : 억원)

ACS(ACS) \ BCS(BCS)		인사관리	자재관리	판매관리	회계관리	품질관리	소 계
IT	응용 S/W	2	2	3	1	0.5	8.5
	시스템 S/W	2	1.5	2	1	4	10.5
	서버 시스템	1	0.3	0.1	0.2	0.4	2
	보조장비	2	1	0.5	0.4	1	4.9
	네트워크시스템	1	1	1	1	1	5
	컨텐츠	2	3	10	1	0.5	16.5
인간	사용자	0.2	0.2	15	0.4	0.3	16.1
	응용담당	1	1	2	1	1	6
	IT 담당	0.5	0.5	0.7	0.5	0.3	2.5
비IT	사무기	2	1.5	2	0.9	0.3	6.7
	설 비	5	2	10	1	2	20
	문서자료	1	1	2.5	1	0.5	6
무형	비즈니스	10	15	50	12	15	102
	노하우	2	2	14	2	4	24
	지재권	0	0	2	0	2	4
	명 성	0	0	100	0	0	100
소 계		31.7	32	214.8	23.4	32.8	334.7

예를 들어, 웹 서버의 정량가치가 1억이라면 매출 규모가 10억원인 A사와 매출규모가 100억원인 B사는 정성가치가 각각 다르다. 즉, A사는 4등급(높음)이며 B사는 2등급(낮음)이 될 수 있다. 특히, 등급의 평가는 평가기준이 있다하더라도 평가자별 주관성이 있으므로, 이를 줄이기 위해 다수의 자산관련 전문가들로부터 "델파이 방법"을 이용하여 평가자별 주관성을 줄인다. "델파이 방법"은 3장에서 설명하였으며 수작업으로 실시하거나 또는 전산 시스템을 이용해 구현할 수 있다. 앞의 정량평가단계에서는 무형자산에 대해서만 "베타분포형 델파이 방법"을 사용하지만 전성평가 단계에서는 모든 자산에 대해 "델파이 방법"을 사용한다. <표 11>과 같이 개별 및 클래스별 자산에 대한 정성평가 수준(1~5등급)을 도출한다.

〈표 10〉 정량평가 결과(하위수준의 1차원적 표현)

자산 id	자 산 명	정량가치(억 원)	기 타
1	응용 S/W	8.5	
2	웹 서 버	5	
3	그 룹 웨 어	2.3	
4	WP	0.2	

④ 후속단계 : 개별 및 클래스별 자산에 대한 정성가액(1~5등급)을 자산유형별 및 업무별 정량가치 및 정성가치수준을 정렬하여 "임계자산목록"을 구한다. 위험분석 및 평가, 정보보호 시스템 평가관련 PP개발 등 자산

평가결과를 활용하는 업무에서 필요한 형태로 가공한다. 예를 들어 <표 12>와 같은 임계자산목록들을 생성해 낼 수 있다.

〈표 11〉 정성평가 결과의 예

ACS(ACS) \ BCS(BCS)		인사 관리	자재 관리	판매 관리	회계 관리	품질 관리	평 균
IT	응용 S/W	2	2	3	1	1	1.80
	시스템 S/W	2	1	2	1	1	1.40
	서버 시스템	2	1	1	2	3	1.80
	보조장비	3	2	1	2	3	2.20
	네트워크시스템	3	3	5	2	3	3.20
	컨텐츠	1	2	4	2	1	2.00
인간	사용자	2	2	4	2	1	2.20
	응용 담당	3	3	4	3	2	3.00
	IT 담당	2	2	3	2	1	2.00
비IT	사무기	3	2	1	1	1	1.60
	설 비	3	2	4	1	2	2.40
	문서자료	1	2	3	1	2	1.80
무형	비즈니스	3	4	5	3	2	3.40
	노하우	1	1	4	2	1	1.80
	지재권	1	1	3	1	2	1.60
	명 성	1	3	5	2	1	2.40
평 균		2.06	2.06	3.25	1.75	1.68	2.16

〈표 12〉 임계자산목록의 예

임계 순위	업무별 임계자산			자산별 임계자산		
	업 무	정 량 가 치	정 성 수 준	자 산	정 량 가 치	정 성 수 준
1	판매관리	214억원	3.25	비즈니스	102억원	3.4
2	인사관리	31억원	2.06	네트워크 시스템	5억원	3.2
3	자재관리	30억원	2.06	응용담당자	6억원	3.0

5. 분석 및 결론

정보통신망의 효율적인 보안관리나 위험분석시에 자산분석 및 평가는 필수적인 업무이나, 기존의 자산분석은 분류체계만 다수 제시되어 있을 뿐 구체적인 자산파악 및 가치평가 방법은 알려져 있지 않다. 또한, 기존의 자산분류 체계는 주로 정보시스템이 아닌 일반적인 위험평가를 위한 것이므로, 현재의 정보시스템에 대한 자산을 분류하기에는 부족한 점이 많다. 특히, 자산평가시의 평가자의 주관성문제를 해결하는 구체적인 방법이 제시되어있지 않다.

본 연구에서는 기존의 보안관리 및 위험분석의 이러한 문제점들을 분석하고 각각에 대한 해결책을 제시하였다.

자산평가에 대한 정형적인 모델의 부재의 문제점에 대해서 ISO/IEC 9127, 14598에 근거한 일반평가모델을 기반으로 집합과 함수개념을 이용하여 정형화된 자산평가모델을 새롭게 정의하였다.

기존의 자산분류체계를 분석하고 현재의 정보시스템의 획득방법을 고려하여 새로운 자산분류공간 체계를 제시하였다. 또한, 자산과 업무를 함께 고려한 2차원적인 자산업무분류공간을 제시하여 조직의 업무와 업무별 자산의 관계를 명확히 파악할 수 있도록 하였다.

자산의 정량가치와 정성가치간의 정의의 모호성 문제의 해결을 위해 정량가치는 자산에 대한 절대적 가치로 평가하며, 정성가치는 조직의 자산규모를 고려한 상대적인 자산가치(5등급)로 평가한다. 따라서, 본 연구에서는 모든 자산에 대해 정량가치를 평가한 후 정성가치로 전환하여 평가한다.

평가의 주관성 및 불확실성 문제의 해결을 위해서 무형자산의 정량평가시 베타분포형 델파이방법을 적용하며, 정성평가시 델파이방법을 적용하여 평가의 신뢰도를 높였다.

정성가치 평가기준의 일반성 문제의 극복을 위해 본 연구에서는 조직의 규모를 반영하여 평가하고 자산의 유형별로 평가기준을 조정하는 절차를 마련하여 정성가치 평가의 정확성 등을 고려하였다.

제시한 BP 기반 자산평가 방법론을 실제의 다수의 기관에 적용하여 문제점을 발견하고 정량평가 계산식 및 정성평가 방법을 조정·보완하는 분야와 본 연구결과를 기반으로 한 실시간 위험분석의 위협·취약성 분석설계 등은 향후 연구과제로 남긴다.

참 고 문 헌

[1] NIST, "A Introduction to Computer Security : The NIST Handbook," pub., 800-12, 1991.

[2] ISO/IEC TR 13335-1, 2, 3, IT 보안 개념 및 모델, 1996, IT 보안 관리 및 계획, 1997, IT 보안 관리 기법, 1998.

[3] British Standards Institution(BSI), BS-7799, 1999.

[4] R. Macmillan, Site Security Policy Development, http://www.auscert.org.au/Information/Auscert_info/Papers/Site_Security_Policy_Development.txt.

[5] Alan Robiette, Developing an Information Security Policy, JISC Committee on Authentication and Security, February, 2001.

[6] TTAS, "공공정보시스템 보안을 위한 위험분석 표준-개념과 모델", TTAS.KO-12.0007, 1998.

[7] NIST, "Risk Management Guide for Information Technology Systems," NIST-SP-800-30, October, 2001.

[8] Will Ozier, "Risk Analysis and Assessment," Information Security Management Handbook(4'th Ed.), CRC Press, 2000.

[9] CC, Common Criteria for Information Technology Security Evaluation, Version 2.1, CCIMB-99-031, August, 1999.

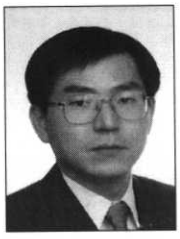
[10] ISO/IEC PDTR 15446, "Information technology-Security techniques-Guide for the production of protection profiles and security targets," Draft, April, 2000.

[11] ISO/IEC-9126 "IT-Software product evaluation-Quality characteristics and guidelines for their use, December, 1991.

[12] ISO/IEC 14598, "IT-Software product evaluation, Part 1, 1997, Part 5, 1997., Part 6, 1997.

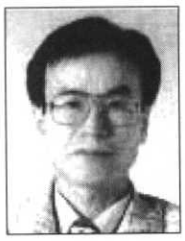
[13] D. Peeples, "The Foundations of Risk Management," 20'th NISSC, pp.577-602, May, 1997.

[14] OCTAVE, "OCATVE Criteria, Version 2.0," Carnegie Mellon Software Engineering Institute, OCATVE Method Implementation Guide Version 2.0, OCTAVE, June, 2001.
[15] 박순태, 보호프로파일 개발을 위한 위험분석, 정보보호뉴스, 2000. 8 외 다수의 정보보호뉴스 수록자료.
[16] 송관호(외), "정보시스템 보안을 위한 위험분석 소프트웨어 개발", 한국전산원 연구보고서, 1997.
[17] CSE, "A Guide to Security Risk Management for IT Systems," Government of Canada, Communications Security Establishment(CSE)," 1996.
[18] 김정덕(외), "위험 분석 도구 기초기술 개발에 관한 연구", ETRI 연구보고서, 2001.
[19] CRAMM, "A Practitioner's View of CRAMM."
[20] A. Pagnoni, Project Engineering Computer oriented Planning and Operational Decision Making, Springer-Verlag, 1990.
[21] W. Royce, "Software Project Management-Unified Framework," Addison Wesley, 1998.
[22] 이광형, 오길록, Fuzzy이론 및 응용, 홍릉과학출판사, 1991.
[23] B. Boehm, "Software Engineering Economics," Prentice-Hall, 1981.



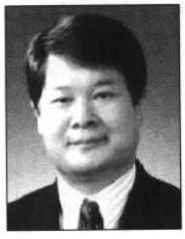
우 병 구

e-mail : bkwoo@ece.skku.ac.kr
1983년 영남대학교 수학과(이학사)
1992년 경북대학교 전산공학과(공학석사)
1986년~1996년 삼성전자 통신연구소 팀장
2002년 성균관대학교 전기전자 및 컴퓨터 공학부, 박사과정 수료
1996년~현재 국가보안기술연구소 전문위원
관심분야 : 정보보안 정책, 네트워크 보안, 위험분석, 정보보호 시스템 평가・인증



이 강 수

e-mail : gslee@eve.hannam.ac.kr
1981년 홍익대학교 컴퓨터공학과(학사)
1983년 서울대학교 대학원 전산학과 (이학 석사)
1989년 서울대학교 대학원 전산학과 (이학 박사)
1985년~1987년 국립 대전산업대학교 전자계산학과 전임강사
1992년~1993년 미국 일리노이대학교 객원교수
1995년 한국전자통신연구원 초빙연구원
1998년~1999년 한남대학교 멀티미디어학부장
1987년~현재 한남대학교 컴퓨터공학과 정교수
관심분야 : 소프트웨어공학, 병행시스템 모형화 및 분석, 정보보호시스템 평가, 멀티미디어교육 커리큘럼



정 태 명

e-mail : tmchung@ece.skku.ac.kr
1981년 연세대학교 전기공학과(학사)
1984년 University of Illinois Chicago, 전자계산학과 학사(학사)
1987년 University of Illinois Chicago, 컴퓨터공학과 석사(석사)
1995년 Purdue University, 컴퓨터공학(박사)
1985년~1987년 Waldner and Co., System Engineer
1987년~1990년 Bolt Bernek and Newman Labs., Staff Scientist
1995년~현재 성균관대학교 정보통신공학부 부교수
관심분야 : 네트워크 관리, 네트워크 보안, 시스템 보안, 전자상거래, 실시간 시스템