# 객체지향 자산분류모델을 이용한 위험분석에 관한연구

# IT Systems Risk Analysis Using Object Oriented Asset Classification Model

이 혁 로* 안 성 진**
Hyeak-Ro Lee Seong-jin Ahn

## 요 약

정보통신환경의 빠른 변화에 따라서 정보자산의 효과적인 관리의 중요성이 강조되어지고 있다. 국내에서도 정보인프라에 대한 정보보호를 위해서 중요자산에 대한 위험분석 및 취약성 분석 강조되어지고 있다. 따라서 효과적인 자산분석을 위해 자산분류 체계화가 선행되어야 한다. 이에 따라, 본 논문에서는 기존의 연구내용들을 조사하여 자산분류를 체계화하고, 이를 토대로 객체지향 자산분류 모델을 제안한다.

## Abstract

In these days, many organizations try to manage their assets in safe way due to fast change in information-communication environment. In Korea, risk analysis and vulnerability analysis for security improvement of critical asset is booming by enforcement of Act on security of information and communication infrastructure. It is obligate that each critical information infrastructure needs to get vulnerability analysis.

In this paper, we proposed Object Oriented Asset Classification model for asset analysis and risk analysis.

☞ keywords : 정보보호, 위험관리, 자산분류

## 1. 서론

정보시스템을 보유하고 있는 기업이나 조직이 다양한 유형의 위협이나 취약성으로부터 발생하는 정보자산에 대한 정보보안 위험을 인식하면서 정보보호 관리의 중요성이 강조되고 있다. 정보시스템은 정보보호 관리 하에서 운용되어야 하며, 정보보호 관리는 위험관리를 포함하고 있다. 위험관리는 위험분석과 보안대책단계로 구성되며, 위험분석은 파악과 측정단계를 포함하고 있다.

최근의 위험분석 프로세스는 자산기반 모델이 주류를 이루고 있으며, 표준모델로 활용되고 있다[1]. 자산기반 위험분석에서는 자산분석의 질이 위험분석의 질과 비례한다. 따라서, 효과적인 위험분석을 위해서는 체계적인 자산분류모델이 필요하다. 자산은 정보시스템 내에서의 역할, 물리적/논리적인 특성 또는 다른 기준에 따라 클래스화 될 수 있다. 클래스에 따라 실제 인스턴스를 파악하고 척도에 따라 등급화 시키는 것이 자산분석의 과정이다. 정보시스템이라는 단어에서도 알 수 있듯이 자산들은 서로 유기적으로 영향을 미치면서 하나의 시스템을 이루고 있기 때문에 이들 간의 연관관계를 파악하는 것도 자산분석에 포함되어야 한다[2]. 자산분석단계에서 수행하는 일련의 공정은 객체지향모델[3]과 유사점을 가지고 있다.

(표 1) 자산모델과 객체지향모델

| 자산분류 모델 | 객체지향 모델 |
|---|---|
| 클래스화 할 수 있다. | 클래스(Class) |
| 하위 자산은 상위자산의 속성을 물려받는다. | 상속(Inheritance) |
| 자산간에는 물리적/논리적 연관성을 갖는다. | 상호작용(interaction) |

* 정 회 원 : 한국과학기술정보연구원 선임연구원
leehr@kisti.re.kr
** 정 회 원 : 성균관대학교 컴퓨터교육학과 교수
Sjahn@comedu.skku.ac.kr
[2008/01/15 투고 - 2008/01/19 심사 - 2008/04/16 심사완료]

이에 따라, 본 논문의 2장에서는 기존의 자산분류방법을 조사 및 분석하여, 이 결과를 통해 3장에서 정보시스템 위험분석프로세스 및 업무의 연관성을 고려한 객체지향 자산분류모델을 제시하며, 4장에서는 이를 이용한 사례연구 통해 자산을 분류하고, 평가과정을 기술하여 유용성을 입증하고, 끝으로 5장에서 결론을 맺는다.

## 2. 관련 연구

### 2.1 기존의 정보시스템 자산분류 조사

기존의 정보보호관리, 위험관리, 위험분석 표준, 지침 및 도구들 중에서 자산분류에 대한 정보가 나타나 있는 것들은 정보보호관리 국제기준인 ISO/IEC-13335(GMIT)[4], 카나다의 CSE[5], CMU의 OCTAVE[6], 국내의 국가보안기술연구소의 PRAM [7], 한국과학기술원의 팬타 및 한국전산원의 HAWK[8], 상용제품인 BDSS[9]를 조사하였다. 자산분류모델의 중요성에도 불구하고 기존의 위험분석 방법들에서는 이를 구체적으로 다루지 않고 있다. 표 2는 기존의 자산분류체계들을 분류수준을 기준으로 비교 분석하였다. 대부분의 기준에서는 자산을 유형, 무형으로 나누어 유사한 분류체계를 택하고 있지만 카나다 CSE의 경우 5수준으로 세분화하고 있으며 OCTAVE에서는 주로 IT자산만을 대상으로 하고 있다.

(표 2) 기존의 자산분류 체계

| 기준 | 대분류 | 분류수준 |
|---|---|---|
| GMIT | 7종 (물리적 자산, 정보/데이터, 소프트웨어, 활동, 사람, 무형 자산, 환경) | 없음 |
| 카나다 CSE | 8종 (정보, 프로세스, 플랫폼, 인터페이스, 인사, 환경, 기타 유형자산, 무형 자산) | 5 |
| BDSS | 8종 (설비 및 지원장비, 컴퓨터장비, 매체 및 소모품, 문서, 인력요소, 시스템 소프트웨어, 응용 소프트웨어, 신용도) | 2 |
| HAWK | 7종 (H/W, 운영체제, 네트워크, 자료, 응용, 사용자, 환경) | 2 |
| KAIST 팬타 | 6종 (S/W 및 자료(업무 프로세스에 직접적으로 연관), OS, HW, 네트워크, 인원, 환경) | 없음 |
| ETRI PRAM | 5종 (데이터, SW, HW, 네트워크, 기타) | 없음 |
| OCTAVE | 9종 (서버, 네트워크 장비, 보안장비, 워크스테이션, PC, 랩탑, 저장장치, 무선장비, 기타) | 없음 |

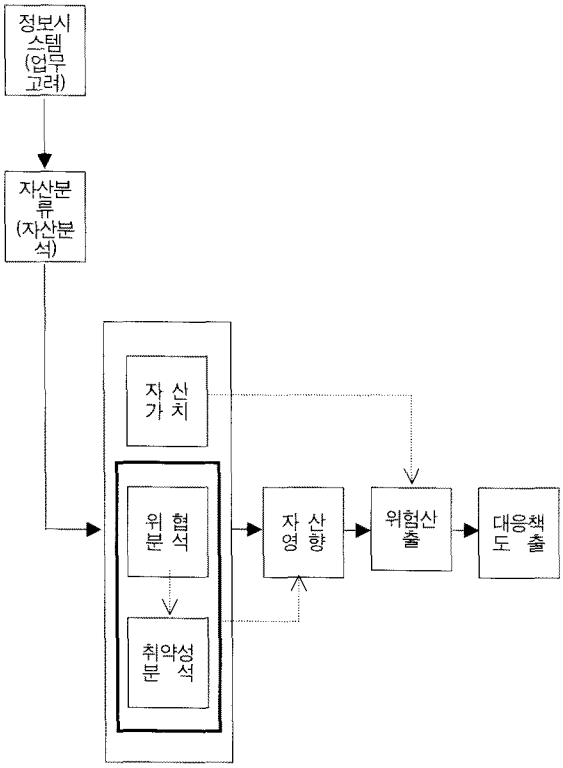
### 2.1 기존의 정보시스템 자산분류 문제점

기존의 방법들은 다음과 같은 문제점을 안고 있다. 첫째, 대부분의 방법들은 계층적으로 자산분류를 하지 않았다. 자산분류는 자산의 특성 또는 속성에 따라 상위 클래스, 중간 클래스 등 계층적 구조를 가져야 자산파악이 용이하며 중복을 피할 수 있다. 또한, 자산의 속성은 상위분류의 자산클래스로부터 물려받게 되어있다. 운영체제라는 자산클래스는 소프트웨어라는 상위 클래스로부터 자산의 속성들을 물려받게 되며, 이 속성은 차후에 위협, 취약성의 분석에 영향을 미치게 된다. 하지만 기존 방법들은 계층성을 가지는 자산을 평면적으로 분류하였다. 둘째, 자산간 의존성이 고려되지 않았다. 자산간 의존성은 자산가치, 위협 및 취약성 분석에 영향을 줄 수 있으므로 반드시 식별해야 한다. 예를 들어, 물리적으로 A라는 자산에 B라는 자산이 의존성을 가지고 있다고 가정하자. 자산 B의 위협 및 취약성 분석 시에는 자산 A의 영향을 받게되고, 자산 A의 가치평가 시에는 B의 영향을 받게 된다. GMIT에서 이를 제시하였지만 실제적으로 모델링은 되지 않은 상태이다. 셋째, 확장성이 고려되지 않았다. 평가대상조직내의 자산은 다양하므로 분류 모델은 확장성을 보장하면서 일관성을 유지하는 것이 필요하다. 기존의 방법론에서는 이를 고려하지 않았다.

## 3. 위험분석 프로세스 및 자산분류 모델

### 3.1 위험분석 프로세스

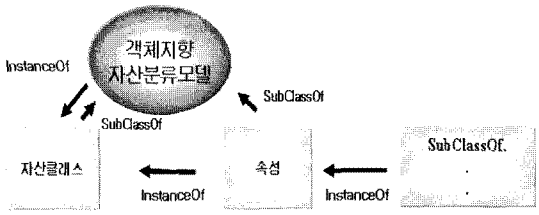
위험분석을 위해서는 분석을 위한 체계적인 절차가 요구 된다. 본 논문에서는 기존의 위험분석을 위한 프로세스의 문제점인 단위자산에 대한 분류를 시스템 단위로 구분하였으며, 자산 분류 또한 자산을 객체로 구분하여 자산을 분류하였다. 정보시스템 위험분석 프로세스는 그림 1과 같다. 자산의 가치(수준) 산정, 위협분석, 취약성 분석, 자산 영향, 위험 산출 및 대응책 도출의 과정을 갖는다.




(그림 1) 정보시스템위험분석 프로세스

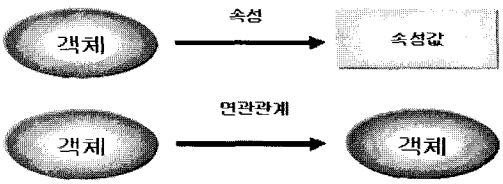
### 3.2 모델 정의(OOAC, Object Oriented Asset Classification)

객체지향 자산분류모델은 상위계층인 객체지향 자산분류 스키마 계층이며, 클래스와 속성들을 정의하기 위해 규정된 스키마 계층이다. 그림 2은 스키마의 구조를 보여주고 있다.




(그림 2) 객체지향 자산분류 스키마

다음 계층인 응용 클래스 계층은 규정된 스키마에 따라 클래스와 속성들을 정의하는 계층이다. 이 계층에서 정보시스템 도메인별 특정 자산분류가 만들어지게 된다. 마지막으로 응용 인스턴스 계층은 분석대상 정보시스템의 자산들을 정의된 스키마에 따라 인스턴스화 하는 계층이다. 정보시스템의 자산들은 정의된 클래스에 의해 객체화되고 속성들을 가지게 된다. 그림 3는 응용 인스턴스 계층에서 자산객체와 특성과의 관계를 node-and-link" 모델로 보여주고 있다.




(그림 3) 자산객체의 "node-and-link" 모델

### 3.3 모델의 특성

본 논문에서 제시하는 객체지향 자산분류 모델은 다음과 같은 특성을 가진다.

(1) 자산간 의존관계 표현이 용이하다.

정보시스템의 자산은 물리적/논리적으로 서로 의존관계를 가지고 있으며, 이는 자산파악 시 고

려되어야 한다. 본 OOAC모델은 자산간의 의존관계를 속성으로 정의하고 이를 쉽게 표현할 수 있다.

(2) 자산분류의 확장이 용이하다.

자산분류는 분석대상 정보시스템에 따라 유연하게 변경되고 확장될 수 있어야 한다. 본 OOAC 모델은 클래스의 상속개념을 도입하여 이를 용이하게 하였다.

(3) 다른 위험요소(위협, 취약성 등)와의 연관이 용이하다.

자산분석단계는 독립된 단계가 아니라 위협분석 및 취약성분석 단계와 유기적으로 연계가 되어야 한다. 자산의 속성으로써 위협 및 취약성을 표현하기 위해 본 OOAC모델은 얼마든지 확장이 가능하다.

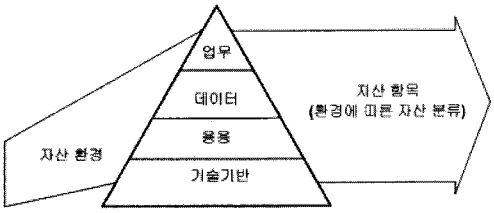
제시한 객체지향 자산분류(OOAC) 모델을 이용하여, 특정 도메인의 자산분류를 예로 하여, 자산을 클래스화하고 자산객체의 속성을 표현할 수 있다.

## 4. 사례연구

본 장에서는 제시한 객체지향 자산분류모델을 이용한 사례를 보인다. 자산분류를 위해 자산이 적용된 환경을 고려하여 업무, 데이터, 응용, 기반기술 측면에서의 환경에 따른 자산 분류를 하였다. 또한 각각의 환경에서 분류된 자산의 연관성을 고려하여 평가하였다.

### 4.1 업무의 연관성을 고려한 자산분류

기존의 자산 분류체계는 (표 2) 기존의 자산분류 체계에서 와같이 5~9종으로 비슷한 분류체계를 갖기 때문에 자산의 식별이 용이하다. 하지만 자산이 사용되는 업무환경 및 정보시스템에 영향을 미치는 중복성을 고려하기 힘들다. 이에 그림 4와 같이 자산이 사용되는 환경(인적 환경, 시스템/컴퓨터 환경, 네트워크 환경, 네트워크 지원환경, 통합 환경, 무형 환경)에 따른 분류와 업무에 따른 자산 분석이 이루어져야 한다.




(그림 4) 업무에 따른 자산 분류

따라서, 서로 배타적이지 않고 서로 연관되어 있다. 예를 들면, 메일 서버관리자는 시스템/컴퓨터환경인 운영체제, 네트워크 환경인 메일 서버 및 네트워크 지원환경인 스위치와 연관되어 있다. 자산이 사용되는 환경과 업무에 따른 자산분류는 표 3과 같다.

(표 3) 자산 분류 체계 예시

| 환 경 | 자 산 | 비 고 |
|---|---|---|
| 시스템/컴퓨터환경(A) | ▪ 공개키 기술<br>▪ 스마트 카드<br>▪ 운영체제<br>▪ PC보안<br>▪ DB<br>▪ 미디어<br>▪ 지문인식<br>▪ 보안취약점 분석도구<br>▪ 기타 | |
| 네트워크 환경(B) | ▪ 방화벽<br>▪ 신뢰된 네트워크 분리<br>▪ 메시지 관리 시스템<br>▪ 네트워크 암호제품<br>▪ 기타 | |
| 네트워크 지원환경(C) | ▪ 스위치/라우터<br>▪ 라우터<br>▪ 유·무선랜<br>▪ 가상사설망<br>▪ 이동코드<br>▪ 다중 영역 솔루션<br>▪ 가드(guard)<br>▪ 키복구<br>▪ 기타 | |
| 통합 환경(D) | ▪ A+B+C<br>▪ B+C<br>▪ A+B<br>▪ A+C | 환경 A,B,C 상속받은 통합 자산 |
| 인적 환경(E) | | |
| 무형 환경(F) | ▪ 서비스<br>▪ 지적재산(저작권, 특허 등)<br>▪ 신용도(이미지, 사기 등) | |

### 4.2 자산평가방법

자산 평가는 자산의 중요도를 파악하고 위협이 발행할 경우 있을 수 있는 피해를 측정하기 위한 과정으로 위험 평가에 있어 필수적 단계이다. 자산평가는 1수준 ~ 5수준 등으로 나누어 평가할 수 있으며 평가구분은 조직의 성격에 따라 자산평가를 세부화 할 수 있다. 자산은 사용되는 환경 및 업무에 중복되어 있어 객체간의 연관관계를 고려하듯이 관계성을 고려해야한다. 예를 들어 표 4와 같이 시스템/컴퓨터 환경에서 $n$개의 업무가 존재하며 각 업무에는 여러 개의 자산이 존재한다. 각 자산은 여러 업무에 중복되어 사용되며, 또한 업무에 사용되는 빈도(중요도)도 다르다. 예컨대, 자산2는 80%의 사용빈도를 갖고 있고 자산3은 230%의 사용빈도를 갖고 있다. 즉, 자산3이 자산2보다 150%가 사용빈도가 많다.

(표 4) 환경·업무를 고려한 자산분류와 이용률 예시

(사용률 %)

| 환경별 \ 업무별 \ 자산별 | | 자산1 | 자산2 | 자산3 | 자산4 |
|---|---|---|---|---|---|
| 시스템/컴퓨터 환경 | 업무1 | 30% | 60% | - | 10% |
| 시스템/컴퓨터 환경 | 업무2 | 80% | - | 20% | - |
| 시스템/컴퓨터 환경 | … | - | 20% | 40% | 40% |
| 시스템/컴퓨터 환경 | 업무n | 10% | - | 90% | - |
| 네트워크 환경 | 업무n+1 | - | - | 80% | 20% |

본 논문에서는 환경·업무별 중복되는 자산에 대한 평가는 [자산수준 평가식]을 이용하여 평가하였다.

[자산수준 평가식]

$N$= 자산평가 수준
$Ai$= 자산 $i$
$BIZn$= 업무 수
$ABi$= 자산$i$에 대한 업무 사용률(%)
$AVi$= 자산평가 수준에 따른 자산가치 $i$
$ALVi$= $i$의 자산수준 가치값
$ALi$= $i$의 자산수준

$$ALVi = \frac{1}{N} \circ \frac{\sum_{Ai}^{BIZn} ABi}{BIZn} \circ AVi$$

$$ALi = \frac{1}{1+(\frac{1}{ALVi-1})^2}$$

$AL_i$는 [0,1]사이의 값이며, 1에 가까울수록 자산가치 수준이 높다. 위 식의 자산평가의 장점은 환경·업무별 중복된 자산을 고려할 수 있고, 조직의 성격에 따른 평가구분 및 자산 평가스케일(수준)을 적용할 수 있다.

## 5. 결론

정보보호를 위해서 중요자산에 대한 위험분석 및 취약성 분석 강조되어지고 있다. 따라서 효과적인 자산분석을 위해 자산분류 체계화가 선행되어야 한다. 자산은 정보시스템 내에서의 역할, 물리적/논리적인 특성 또는 다른 기준에 따라 클래스화 될 수 있다. 클래스에 따라 실제 인스턴스를 파악하고 척도에 따라 등급화 시키는 것이 자산분석의 과정이다. 이에 따라, 본 논문에서는 기존의 연구내용들을 조사하여 자산분류를 체계화하고, 이를 토대로 객체지향 자산분류 모델을 제안하였다.

자산기반 위험분석에서 분석 결과의 질은 체계적인 자산분류모델의 영향을 받는다. 이에, 본 연구에서 제시한 객체지향 자산분류 모델은 기존 방법들의 자산분류를 종합하고 문제점을 개선한 것이다.

자산분류 모델은 자산분류를 클래스 화하고, 객체지향 기법을 이용하여 모델링함으로써 자산간 연관관계 표현이 용이하며, 자산분류의 확장과 다양한 환경에 따른 업무 및 다른 위험요소와의 연관이 용이하다.

본 결과는 자산분류를 기반으로 하는 위험분석 방법 및 도구개발에 이용됨으로써 체계적인 위험분석 방법을 위한 기반연구로 활용될 것이라 기대된다.

## 참 고 문 헌

[1] Young-hwan Bang, Yoon-jung Jung, In-jung

Kim,"The Design and Development for Risk Anlysis Automaitc Tool", LNCS 3043, Part 1, pp.491-499, May. 2004.

[2] ISO/IEC TR 13335, 3부, "IT 보안관리 지침", 1998.

[3] S. Khoshafian, et al., "Object Orientation", 2'rd Computer Application Conference, 1997.

[4] ISO/IEC TR 13335, 1부, "IT보안 개념 및 모델"(1996), 2부 "보안관리 및 계획"(1997).

[5] CSE, "A Guide to Security Risk Management for IT Systems", Government of Canada, Communications Security Establishment(CSE)", 1996.

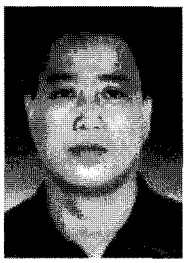
[6] OCTAVE, "OCATVE Criteria, Version 2.0", Carnegie Mellon Software Engineering Institute(2001. 12), OCATVE Method Implementation Guide Version 2.0, OCTAVE, 2001. 6, http://www.sei.cmu.edu/publications/pubweb.html.

[7] 김정덕 (외), "위험 분석 도구 기초기술 개발에 관한 연구", ETRI 연구보고서, 2001.

[8] 송관호(외), "정보시스템 보안을 위한 위험분석 소프트웨어 개발" 한국전산원 연구보고서, 1997.12.

[9] 김기윤, 나관식, 김종석, "보안관리를 위한 위협, 자산, 취약성의 분류 체계", 정보보호학회지, 6권 1호, 1995. 6.

## ◐ 저 자 소 개 ◑



**이 혁 로**

1996년 대전산업대학교 정보통신공학과 졸업(학사)
2004년 공주대학교 교육정보대학원 영상매체학과 졸업(석사)
2007년 성균관대학교 일반대학원 교과교육학과(박사 수료)
1990~현재 한국과학기술정보연구원 선임연구원
관심분야 : Optical Network, IPv6 Technology, Network Security,
E-mail : leehr@kisti.re.kr

**안 성 진**

1988년 성균관대학교 정보공학과(학사)
1990년 성균관대학교 정보공학과(석사)
1998년 성균관대학교 정보공학과(박사)
2000년~현재 성균관대학교 컴퓨터교육학과 교수
관심분야 : Network Measurement, Network Security, IPv6
E-mail : Sjahn@comedu.skku.ac.kr