한국산학기술학회논문지
Vol. 10, No. 3, pp. 579-588, 2009

# AHP 기법을 이용한 보안환경을 고려한 COTS 기반 정보시스템의 보안기능 컴포넌트 대체 수준 의사결정

최명길[1], 황원주[2], 김명수[3*]
[1]중앙대학교 상경학부, [2]인제대학교 정보통신공학과·UHRC, [3]강원대학교 경영학과

# Decision on Replacing Components of Security Functions in COTS Based Information Systems in Security Environment Utilizing AHP

**Myeonggil Choi[1], Won-Joo Hwang[2] and Myoung-Soo Kim[3*]**
[1]**Department of Business Administration, Chung-Ang University**
[2]**Department of Information and Communications Engineering, UHRC, Inje University**
[3]**College of Business Administration, Kangwon National University**

**요 약** 기업과 정부기관은 COTS를 사용한 정보시스템을 개발하고 있다. 특히, COTS는 정보보호시스템과 정보시스템의 컴포넌트로 활용되고 있다. 본 연구는 보안기능 개발을 위해서 필요한 COTS의 선택 수준과 비용을 고려할 때 COTS 컴포넌트의 우선순위를 제시한다. 보안기능 컴포넌트 선택과 관련된 비용 효과적인 의사결정을 위하여, 본 연구는 정보보호기술을 계층화하고, 다기준의사결정 기법을 사용하여 COTS 컴포넌트의 우선순위를 제시한다.

**Abstract** Enterprises and governments currently utilize COTS (Commercial off-the-Shelf) based information systems which are a kind of component based systems. Especially, COTS are widely utilized as components of information security systems and information systems. This paper suggests an appropriate adaptation level and a cost effective priority to replace security functional components in security environment. To make a cost effective decision on adapting security functional components, this paper develops a hierarchical model of information security technologies and analyzes findings through multiple decision-making criteria.

**Key Words :** COTS, COTS based information systems, security component, AHP.

## 1. 서론

인터넷의 발달은 정보시스템의 보안 위험을 가중시키고 있으며, 조직은 정보시스템의 안전한 운영을 위해 많은 자원을 보안에 투자하고 있다. 상존하는 보안 위협에 대처하기 위해서 일반 정보시스템과 정보보호시스템과의 경계가 모호해지고 있다[13,14].

정보시스템의 보안 문제와 별개로 소프트웨어 생산성에 대한 위기가 심각해짐에 따라 소프트웨어 개발 생산성 향상을 위한 다양한 연구가 수행되었다. 소프트웨어 개발 생산성 향상을 위해 가장 적합한 접근법으로 컴포넌트 기반 개발 방법론(component based development method)이 알려져 있다[2,3,11]. 컴포넌트 기반 개발 방법론을 적용한 대표적인 정보시스템으로 COTS 기반 정보시스템(commercial off-the -shelf based information systems)을 들 수 있다[17,20,23].

COTS 기반 정보시스템은 다양하게 정의될 수 있지만, 본 연구는 COTS 기반 정보시스템을 정부 및 기업이 COTS를 정보시스템의 컴포넌트로 획득하여 정부 및 기업이 자체적으로 개발한 컴포넌트와 결합하여 개발한 시스템으로 한정한다[4,6].

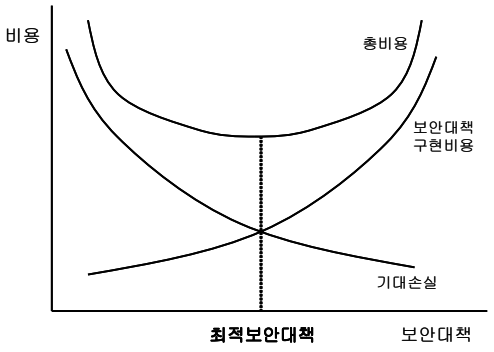
정부 및 기업이 COTS 기반 정보시스템을 활용하는

*교신저자: 김명수(mywoo@kangwon.ac.kr)
접수일 09년 01월 21일 수정일 09년 02월 19일 게재확정일 09년 03월 23일

목적은 다음과 같다. 첫째, 기존의 완성된 상용 정보시스템은 조직의 특성을 반영하기 어려우므로 정부 및 기업은 조직의 특성을 반영한 정보시스템을 도입하기를 원한다. 둘째, 정부 및 기업은 도입 비용이 저렴하고, 도입효과가 높은 정보시스템 개발을 추구한다. 셋째, 정부 및 기업은 정보시스템의 보안과 비용을 고려하여 정보시스템의 도입을 원한다. 즉 정보시스템 중 보안성과 신뢰성을 요구하는 컴포넌트는 자체적으로 비용을 투자하여 개발하고, 보안성과 신뢰성이 덜 중요한 컴포넌트는 시장에서 도입하여 최종적으로 조립함으로 보안성과 신뢰성이 확보된 정보시스템을 도입한다[10,24].

위에서 언급된 원인으로 정부와 기업은 컴포넌트 기반 정보시스템인 COTS 기반 정보시스템을 널리 활용하고 있으며, 특히 정보보호시스템과 정보보호기능이 결합된 정보시스템을 도입할 때 폭넓게 채용하고 있다[13,14]. 정부와 기업은 보안성이 확보된 COTS 기반 정보시스템 도입을 위하여 보안 관련 컴포넌트 도입 방법을 결정해야 하는 문제에 부딪치고 있다. 즉 외부에서 개발된 보안 관련 컴포넌트는 신뢰성이 낮은 반면 조달 비용이 저렴하고, 조직내의 보안 전문가가 개발한 보안 컴포넌트는 신뢰성이 높은 반면 개발비용이 상승될 수 있다. 따라서 보안 컴포넌트의 신뢰성 수준은 비용과 트레이드 오프(trade-off) 관계를 유발한다. 특히 사용자가 정부기관일 경우 COTS 기반 정보시스템의 보안은 중요하다. 정부기관은 정보시스템의 정보보호 요구수준에 따라 COTS 기반 정보시스템의 정보보호기능 중 많은 부분을 정부가 직접 개발한 기능으로 대체한다. 대체수준은 COTS 기반 정보시스템의 정보보호 요구수준에 따라 다르며, 정보보호 요구수준이 낮으면 COTS 기반 정보시스템의 대부분의 기능을 사용할 수 있고, 정보보호 요구수준이 높으면 COTS 기반 정보시스템의 보안기능 컴포넌트의 많은 부분을 대체해야 한다.

COTS 기반 정보시스템의 보안 컴포넌트의 신뢰성 수준과 비용을 고려한 의사결정은 Solms가 제안한 조직의 최적 보안 대책 결정 모형을 통해서 이해할 수 있다. Solms는 <그림 1>과 같이 보안 대책의 구현 및 운용 비용과 구현된 보안 대책에 의해서도 보호되지 않는 위험이 발생시키는 기대 손실의 합계인 총비용이 최저가 되는 수준에서 보안 대책을 강구한다. 즉 최적보안대책 결정모형은 가장 비용 효과적인 보안 대책이 먼저 고려된다는 가정하에서, 한계 효용과 한계 비용이 일치하는 점에서 최적화된다[25].




**[그림 1]** 최적보안대책 결정 모형

본 연구는 COTS 기반 정보시스템의 보안 컴포넌트의 대체 수준에 초점을 둔다. COTS 기반 정보시스템의 소유자는 선별된 정보보호기능의 신뢰 수준을 객관적인 기준이나 방법 없이 임의대로 결정했다. 따라서 COTS 기반 정보시스템 도입 시 보안기능 컴포넌트를 객관적인 기준에 따라 대체하지 않음으로 보안기능 컴포넌트의 도입은 보안성과 비용 측면에서 효과적이지 못하다. 정부 및 기업은 중요한 보안기능 컴포넌트를 보안 환경을 고려한 객관적인 기준에 따라 자체 개발한 보안기능 컴포넌트로 대체하면 COTS 기반 정보시스템의 보안성 확보와 비용 효과적인 개발이 가능하다. 정부기관 및 민간기업이 비용 효과적이며, 최적의 보안을 확보할 수 있는 보안기능 컴포넌트의 대체 수준 결정에 사용될 수 있는 보안기능 컴포넌트 대체 수준 결정 방법론이 필요하다.

본 연구는 COTS 기반 정보시스템의 도입에 따른 최적의 보안기능 컴포넌트 대체 수준을 결정하는 방법과 보안기능 컴포넌트간의 우선 순위를 제시한다. 이를 위해 본 논문은 보안기능 컴포넌트의 대체 우선 순위 결정을 위해 정보보호기술 분류에 따른 보안기능 컴포넌트 모형을 개발하고, 보안기능 컴포넌트의 상대적 중요도를 정보보호 연구기관의 연구원, 정부기관의 정보보호관리자, 정보보호 시스템 개발자를 대상으로 전문가 설문조사를 수행하였다. 설문조사결과는 AHP(analytic hierarchy process)방법론을 사용하여 분석하고, 각 보안기능 컴포넌트의 중요도를 결정한다.

본 논문의 구성은 다음과 같다. 2장은 컴포넌트 기반 개발방법론을 활용한 COTS 기반 정보시스템의 관련 연구를 설명하고, 3장은 COTS 기반 정보시스템의 개발절차를 서술한다. 4장은 연구방법론을 제시하고 있으며, 5장은 AHP를 활용한 보안기능 컴포넌트의 우선 순위를 결정하고 보안기능 컴포넌트의 대체 수준을 분석한다. 6장은 결론이다.

## 2. 관련 연구

COTS 기반 정보시스템의 보안기능 컴포넌트 대체 문제는 COTS 컴포넌트 선정 연구와 관련이 있다. COTS 기반 정보시스템의 보안기능 컴포넌트 대체와 관련된 연구로는 COTS 기반 정보시스템 도입시 보안기능 컴포넌트 도입을 통한 보안성 확보와 관련된 연구[5,15,16], COTS 기반 정보시스템의 컴포넌트 선정을 위한 방법 연구[18,22,23,26], 비용을 기준으로 한 보안기능 컴포넌트 선정 연구[8,9,24] 등이 있다. 다음은 COTS 기반 정보시스템의 보안 컴포넌트 선정과 관련된 최근의 연구이다.

Dean and et al.는 보안성이 없는 COTS 컴포넌트를 이용하여 COTS 기반 정보시스템 개발시 보안성 확보 방법을 탐색하고 있으며, COTS 기반 정보시스템의 보안성 확보 방법으로 Security Wrapper Technology를 제시하고 있다[15]. 이 연구는 Security Wrapper 기술을 사용하여 COTS 기반 정보시스템의 보안성 확보의 가능성을 입증했다. 그러나 이 연구는 Security Wrapper가 신뢰성 있는 컴포넌트임을 전제하고 있으며, COTS의 컴포넌트 도입 관점에서 Security Wrapper의 효과적인 도입 방법에 대해서는 고려하고 있지 않다.

Reifer and et al.는 COTS 기반 정보시스템의 도입에 따라 보안 문제가 심각해지고 있는 상황에서, 보안기능 컴포넌트를 도입할 때 발생하는 비용을 예측할 수 있는 비용예측모델을 제시하고 있다[24]. 이 연구는 비용관점에서 COTS 기반 정보시스템의 사용자가 보안 컴포넌트 도입 여부를 결정할 수 있게 하지만, 보안 컴포넌트가 주는 장점과 보안기능 컴포넌트간의 중요성을 고려하고 있지 않다.

Oh and et al.는 다기준의사결정(multiple criteria decision making) 방법을 사용하여 COTS 컴포넌트를 선택할 수 있음을 보여주고 있다[23]. 이 연구는 소프트웨어 품질 메트릭을 기준으로 COTS 컴포넌트를 선정하는 의사결정기법을 도입했다. 그러나 이 연구는 의사결정기법의 적용 가능성은 제시하였지만, 다차원의 기준을 소프트웨어 품질 결정에 적용할 때 발생하는 복잡성을 고려하지 않고 있다.

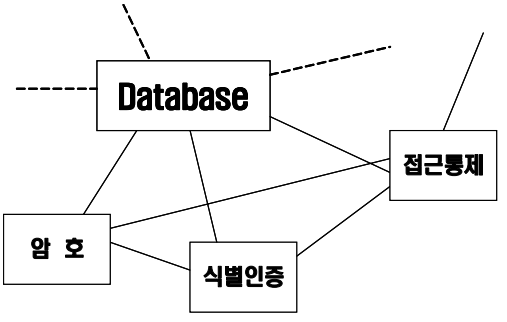
Ye와 Kelly는 적절한 COTS 제품을 선택하는 것이 안전한 시스템을 완성하는데 있어서 중요한 요소라고 생각하고, 안전 지향적인 시스템에 맞는 COTS 선택방법을 제시하였다[26]. 이들이 제안한 CBCPS (contract-based COTS product selection)에서는 COTS 제품의 선택에 앞서 먼저 시스템의 위험분석을 통해 현재 시스템이 가지고 있는 위험요소를 파악하고, 새로운 COTS 컴포넌트를 도입한 후에 발생할 수 있는 잠재적인 위험요소까지도 분석을 마쳐야 한다. 시스템 위험분석을 통해 얻은 결과를 사용하여 새롭게 선택하려는 COTS 컴포넌트의 정보보호 요구사항으로 도출한다. 도출된 정보보호 요구사항은 COTS 컴포넌트를 선택하는데 있어 평가와 선택의 기준으로 사용한다. COTS컴포넌트를 선택하기에 앞서 현재 시스템의 위험요소를 분석함으로 COTS 컴포넌트을 통해 시스템의 보안성을 확보할 수 있다. 그러나, 잠재적인 위험요소의 파악은 매우 복잡한 일이며, 전체 시스템의 위험요소를 매번 검사하는 것은 비용측면에서 효과적이지 못하다.

Kunda는 안정된 COTS 기반 정보시스템도입의 관건은 시스템 요구사항에 부합하는 COTS 컴포넌트 선택에 있다고 제안한다[19]. 정형화된 COTS 컴포넌트 선택 방법의 부재는 COTS 컴포넌트 선택시 많은 비용을 발생시키고 있으며, COTS 컴포넌트를 선택한 후에도 여전히 존재하는 불확실성으로 인해 COTS 기반 시스템의 보안성이 위협받을 수 있다. 따라서 Kunda는 COTS 컴포넌트를 평가 및 선택시 COTS 컴포넌트의 기능적 특성, 품질적 특성, 비용 측면, 사회적 인지도 등의 4가지 요소를 제시한다. 이 연구는 제시된 4가지 요소들의 상대적 중요도를 AHP를 사용하여 분석하고, 제안된 요소들을 얼마만큼 참고해야 될 지를 결정하는 정성적인 기준을 제시하였다.

## 3. COTS 기반 정보시스템의 개발 절차

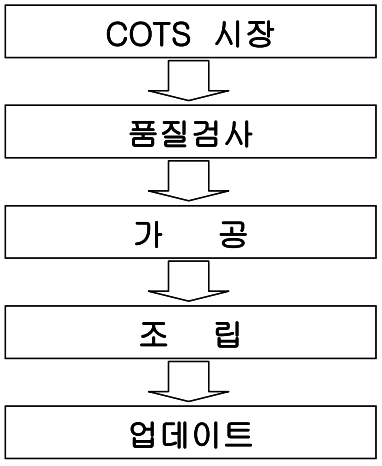
[그림 2]는 보안기능 컴포넌트로 구성된 COTS 기반 정보시스템의 한 예를 보여준다.

COTS 컴포넌트를 도입하여 시스템을 설계하는 주된 원인은 비용의 절감과 신기술의 빠른 도입 및 업데이트에 있다. 시스템의 보안과 COTS 기반 정보시스템의 장점을 반영하기 위해서는 COTS 컴포넌트의 특성을 고려한 보안 기능 설계가 이루어져야 한다.




**[그림 2]** COTS 기반 정보시스템 구성

COTS 기반 정보시스템의 개발은 <그림 3>과 같은 절차로 이루어진다[12]. COTS 기반 정보시스템 개발은 우선 COTS 컴포넌트를 시장에서 적절하게 선택하여 조립이 가능하도록 가공한다. 가공된 COTS 컴포넌트는 안정적인 아키텍처를 기반으로 조립하게 되며, 이 과정을 통해 개발된 COTS 기반 정보시스템은 사용자의 요구사항에 따라 COTS 컴포넌트를 교체함으로써 손쉽게 변경할 수 있다. COTS 기반정보시스템의 각 개발단계에서 정보보호 관련 사항들을 살펴보면 다음과 같다.




[그림 3] COTS 기반 시스템 개발 절차

### 가. COTS 시장(COTS market)

COTS 시장에는 다양한 제품들이 출시되어 있지만, 제품의 규격화는 이루어져 있지 않은 실정이다. 규격화가 되지 않은 제품 중에서 조직의 특성에 적합한 제품을 선정해야 한다.

### 나. 품질검사(qualification)

COTS 기반 정보시스템 개발 절차 중 정보보호에 관련하여 가장 중요한 단계는 품질검사(qualification)이다. 사용자는 조직이 도입하는 COTS 기반 정보시스템에 적절한 컴포넌트를 구입해야 하는데, COTS 시장에 있는 모든 컴포넌트가 우수한 것은 아니다.

COTS 기반 컴포넌트의 경우 동일한 기능을 제공하고 같은 개발표준을 준수하더라도 품질과 성능의 차이가 존재한다. 따라서 COTS 컴포넌트 선정 기준이 필요하며, 기준에 의한컴포넌트 품질검사 절차가 필요하다. COTS 컴포넌트 품질검사를 위해서는 품질검사 비용이 수발된다.

### 다. 가공(adaptation)

가공(adaptation) 단계는 선정된 COTS 컴포넌트를 설계하거나, 이미 개발되어 운용 중인 COTS 기반 정보시스템에 조립이 가능하도록 COTS 컴포넌트를 적절히 가공하는 단계이다. COTS 컴포넌트의 가공을 위해서는 COTS 기반 정보시스템의 개발 절차의 전체적인 과정과 구조를 고려해야 한다. 즉 COTS 기반 정보시스템은 정보보호 요구사항에 맞도록 개발되어야 한다. COTS 컴포넌트는 개별적으로 동작하는 것이 아니라, 다른 COTS 컴포넌트와 연결되어 상호작용을 한다. COTS 기반 시스템이 비밀성, 무결성, 가용성 등의 보안기능을 고려하여 운영되기 위해서는 각 COTS 컴포넌트 간의 상호관계를 고려하여 가공해야 한다. 특히 컴포넌트간의 보안 수준 문제, 접근통제수준 문제, 암호 프로토콜 설정 문제 등은 COTS 기반 정보시스템의 보안에 영향을 미치는 중요한 문제이다. 따라서 이 문제는 COTS 기반 정보시스템이 지향하는 보안 수준이나 정책에 관련된 문제이며 위험평가 및 객관적인 의사결정을 통해 결정되어야 한다. 선정된 COTS 컴포넌트는 사전에 정의된 정보보호 요구수준에 따라 가공한다. COTS 기반 정보시스템 도입시 COTS 컴포넌트 대체 수준을 사전에 결정하면 COTS 컴포넌트 가공비용을 최소화시킬 수 있다.

### 라. 조립(assembly)

가공된 COTS 컴포넌트를 안정된 아키텍처를 기반으로 만드는 과정이 조립(assembly) 단계이다. 기본적으로 에러가 많이 발생하는 시스템은 정보보호에 취약할 수밖에 없으므로 시스템의 용량과 구조를 고려하여 COTS 컴포넌트를 조립하여야 한다.

### 마. 업데이트(update)

추가적으로 시스템에 새로운 데이터와 기능이 요구될 때는 COTS 기반 정보시스템을 업데이트한다. 이 단계에서 COTS 컴포넌트의 추가, 교체, 삭제 등이 발생한다.

## 4. 연구방법론

본 연구는 COTS 기반 정보시스템 도입에 따른 보안기능 컴포넌트의 대체 우선 순위를 결정하기 위해 AHP 방법론을 활용하였다. AHP는 복잡한 문제를 단순화시켜 합리적인 의사결정이 가능하도록 지원해주는 계층적 분석 방법론으로 복수의 기준에 대한 가중치를 동시에 고려하기 보다는 두 개씩 짝을 지어 이원비교를 하여 조사

대상 기준들 간의 상대적 중요도를 명확하게 판단하게 한다[7]. AHP는 대상 기준들간의 상대적 중요도를 판단할 때 일관성 정도(consistency ratio)를 나타낼 수 있어 일관성이 결여된 경우 수정작업이 가능하다.

본 연구는 3단계의 연구방법을 채용하였다.

**[단계 1]**

먼저 AHP의 적용을 위해서 해결하려는 문제를 하위의 구성 요소로 분해하여 계층적으로 나타낸다. COTS 기반 정보시스템의 보안 기능 컴포넌트의 대체 수준을 결정하기 위해서 보안기능 컴포넌트를 하부 구성 요소로 분류하였다. 보안 기능 컴포넌트를 하부 구성 요소로 분류하기 위해 본 연구는 정보보호기술을 분류하고, 분류된 정보보호기술을 보안기능 컴포넌트 계층 모델로 작성한다.

**[단계 2]**

COTS 기반 정보시스템 도입 시 보안 기능컴포넌트의 대체 수준의 결정을 위해서는 보안기능 컴포넌트의 우선순위를 결정해야 한다.

보안 기능 컴포넌트의 대체 수준 결정을 위해 설문조사는 2 part로 나누어 진행하였다. 설문 Part A는 COTS 기반 정보시스템의 보안기능 컴포넌트의 우선 순위를 이원비교를 통해 도출하고, AHP 방법론을 사용하여 검증하였다. 즉 설문은 AHP 방법론에 사용되는 이원비교를 수행하는 것으로 보안기능 계층에 속하는 컴포넌트의 상대적 중요도를 비교한다.

설문 Part B는 Part A 설문 결과의 유효성을 검증하기 위해서 COTS 기반 정보시스템이 요구하는 정보보호 요구수준의 순위를 비교하여 Part A의 연구결과를 검증하였다. 즉 보안환경의 위협 정도를 5점 척도로 구분하고, 보안환경에 따라 COTS 기반 정보시스템이 대체해야 하는 보안기능 컴포넌트의 순위를 측정하였다.

보안기능 컴포넌트의 대체 수준의 순위와 보안환경의 위협 정도에 따른 COTS 기반 정보시스템이 요구하는 보안기능 컴포넌트의 순위를 비교하면, AHP를 사용한 연구 결과의 유효성을 검증할 수 있다.

설문은 전문가 조사(delphi approach)를 통해 이루어졌고, 설문조사 대상으로 <표 1>이 나타내듯이 정보보호전문 연구기관 연구원, 정보보호관리자, 정보보호시스템 개발자, 정보보호분야 교수 등으로 구성되어 있다.

**[표 1]** 조직 유형별 설문조사 대상 분포

| 설문 응답자 | 응답자 | 분포 (%) |
|---|---|---|
| 연구기관 연구원 | 17 | 33 |
| 정부기관 정보보호관리자 | 9 | 18 |
| 정보보호시스템 개발자 | 21 | 41 |
| 정보보호 분야 교수 | 4 | 8 |
| 합 계 | 51 | 100 |

**[단계 3]**

전문가 설문조사에서 획득한 데이터의 결과를 AHP 방법론을 적용하여 분석하고, 보안기능 컴포넌트간의 우선 순위를 결정하였다.

AHP 방법론을 적용한 대체 수준 순위의 유효성을 검증하기 위해서 보안환경의 위협 정도에 따라 COTS 기반 정보시스템이 요구하는 보안기능 컴포넌트의 대체 여부를 결정하는 설문 결과를 분석하고, AHP 방법론의 결과와 비교한다.

각 단계에서 수행한 연구 내용을 자세히 서술하면 다음과 같다.

[단계 1]은 AHP 방법론 적용을 위해 보안기능 컴포넌트를 3계층으로 구분하여 개발한다. 보안기능 컴포넌트를 계층으로 분류하는 방법은 정보보호기술 분류 연구결과를 수용했다 [1]. 다양한 정보보호기술 분류가 있지만, 정보보호 기술 분류의 근본적인 골격은 유사하므로 본 논문은 정보보호기술을 포괄적으로 포함할 수 있는 분류방법을 개발하였다.

본 연구가 개발한 분류의 최상위 계층은 정보보호 기반기술, 네트워크 및 시스템 보호기술, 보안관리기술 등 3가지이다. 정보보호 기반기술은 암호관련 기반기술, 키관리기술로 구성되며, 네트워크 및 시스템 보호기술은 네트워크 보호와 시스템 보호로 구성된다. 보안관리기술의 2번째 계층은 네트워크 보안관리와 시스템 감시 및 운영관리로 구성된다. 각 계층의 마지막 단계는 <그림 4>와 같이 구성된다.

[단계 2]는 전 단계에서 개발한 계층모델을 바탕으로 전문가를 대상으로 2가지 형태의 설문을 실시하여 연구결과의 유효성을 검증하였다.

설문지 Part A는 COTS 기반 정보시스템의 보안기능 컴포넌트의 대체 의사결정을 위해 필요한 데이터를 수집하기 위해 배포되었다. 설문조사는 각 계층에 속하는 컴포넌트 간의 상대적 중요도를 측정하는 내용으로 구성되었다. 설문척도는 의사결정 요인의 이원비교를 위해 1점

에서 9점까지의 수치로 표현하였는데, 1은 비교하는 두 컴포넌트의 동등한 중요도를 나타내고, 9는 한 컴포넌트가 절대적으로 중요함을 나타낸다. 이 척도는 각 단계의 컴포넌트간의 상대적 중요도(relative weight)에 관한 주관적인 판단을 수치로 나타낸 것이다.

설문지 Part B는 보안환경의 위협수준을 5점 척도로 분류하였다. 이것은 COTS 기반 정보시스템을 둘러싸고 있는 보안환경의 위협 수준을 반영하는 것으로 1은 보안환경의 위협수준이 가장 낮은 보안환경을 가정하고 5는 보안환경의 위협수준이 가장 높다고 분류하였다. [1단계]에서 분류된 각 보안기능 컴포넌트를 보안 환경에 따라서 대체 필요성을 지적해 줄 것을 요청하였다. 즉 위협수준이 낮은 보안환경에서 보안 기능 컴포넌트의 대체가 필요함을 지적한다면 보안기능 컴포넌트의 중요성이 높다는 의미이다. 그러므로 위협 수준이 낮은 보안환경에서도 COTS 기반 정보시스템의 보안기능 컴포넌트의 대체 필요성이 높은 경우라면 COTS 기반 정보시스템의 보안성을 위해 정부 및 기업이 직접 개발한 보안기능 컴포넌트를 우선 순위에 따라 대체해야 한다는 의미이다. 즉 대체 수준의 순위와 보안환경의 위협수준에 따른 보안기능 컴포넌트의 대체 순위를 비교하면 연구 결과의 유효성을 증가시킬 수 있다.

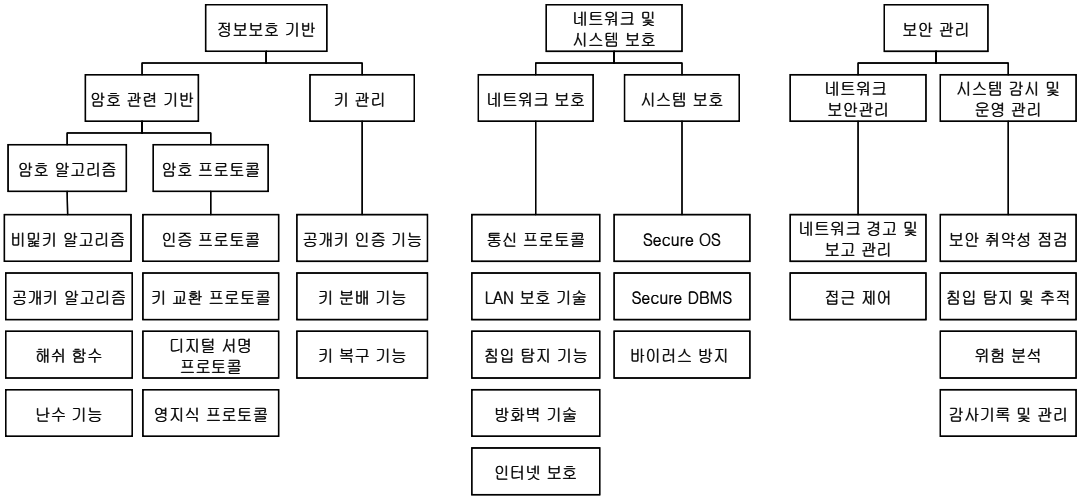
설문지는 온라인과 오프라인을 통하여 총 150부의 설문을 송부하여 57부를 회송 받았다. 설문지 회송률은 38%였으며, 이로부터 총 51부의 유효한 설문을 획득하였다.

[단계 3]에서 사용한 AHP 방법론을 간단히 설명하면 다음과 같다. 설문조사를 통해 우선 순위를 체계적으로 구하기 위해서는 중요도 척도에 따른 이원비교행렬(pairwise comparison matrices)을 다음과 같이 구성해야 한다.

$$A=\begin{bmatrix} w_1/w_1 & w_1/w_2 & \cdots & w_1/w_n \\ w_2/w_1 & w_2/w_2 & \cdots & w_2/w_n \\ \vdots & & & \vdots \\ w_n/w_1 & w_n/w_2 & \cdots & w_n/w_n \end{bmatrix}$$

여기서 $w_i$ 와 $w_j$ 는 i번째 속성과 j번째 속성의 가중치를 나타내는데, $w_i/w_j$ 는 i 가 j 에 미치는 상대적인 우월성을 나타내게 되므로, 주 대각선의 원소들이 모두 1이 되는 역수행렬이 된다.

이원비교의 결과를 나타내는 행렬의 고유벡터(eigenvector)를 이용하면 어느 한 계층 내의 요소들 사이의 가중치를 구할 수 있는데, 이 가중치는 각 요소들 간의 상대적 중요도를 나타낸다. 일반적으로 $n\times n$ 의 행렬 $A$ 에 대하여 $[AW=\lambda W]$ 를 만족하는 스칼라 $\lambda$ 와 $n\times 1$ 의 고유벡터 $W(=(W_1,W_2,\cdots,W_n)^T)$ 가 존재하는데, 이러한 경우 $\lambda_{\max}$ 에 대응하는 고유벡터 $W$ 가운데에서 $\Sigma W_j=1$ 을 만족하는 고유벡터가 그 계층 내의 요소들 간의 가중치가 된다.




**[그림 4]** 보안기능 컴포넌트의 계층 모델

행렬 $A$ 의 일관성의 정도가 클수록 $\lambda_{max}$ 는 $n$ 에 가까워지며, 이러한 특성을 이용하여 일관성 지수(consistency index: CI)를 다음의 식을 통해 구할 수 있다.

$$CI = (\lambda_{max} - n)/(n-1)$$

CI와 경험적 자료로 얻어진 평균 무작위 지수(random index: RI)의 비율을 일관성 비율이라 하는데, 일관성 비율이 10% 이내인 경우에 우선순위에 무리가 없는 신뢰할 수 있는 결과라 할 수 있다.

## 5. 보안기능 컴포넌트 대체 수준 결정

[단계 3]은 설문을 통해서 획득된 데이터를 AHP를 사용하여 분석하였다. AHP를 사용하여 얻은 보안기능 컴포넌트의 우선 순위는 <표 2>와 같다. 1 계층에서 보안기능 컴포넌트의 순위는 정보보호 기반기술, 네트워크 및 시스템 보호기술, 보안관리 순으로 나타났다. 정보보호 기반기술은 암호관련 기반기술, 키 관리 기술 순으로 나타났다. 암호관련 기반기술에서는 암호 알고리즘의 우선순위가 암호 프로토콜의 우선 순위보다 높은 것으로 나타났다.

네트워크 및 시스템 보호기술의 2번째 계층은 네트워크 보호, 시스템 보호 순으로 나타났고, 보안관리의 2번째 계층은 네트워크 보안관리, 시스템감시 및 운영 관리의 우선 순위가 동일하게 나타났다.

모든 보안기능 컴포넌트의 우선 순위는 보안 기능 컴포넌트의 대체 수준을 결정하는 정보를 제공해 준다. <표 3>은 보안기능 컴포넌트의 전체 우선 순위로 보안기능 컴포넌트의 대체 수준을 나타낸다.

<표 3>에서 알 수 있듯이 해쉬함수와 난수 기능을 제외한 암호관련 기반기술에 속해 있는 보안기능 컴포넌트는 모두 10위 안에 속한다. 이를 통해 보안기능 컴포넌트 중 암호관련 기반기술이 COTS 기반 정보시스템의 도입 시 대체해야 할 중요 컴포넌트임을 알 수 있다. 이 결과는 암호모듈 검증프로그램(cryptography module validation program)[21]을 통해서 암호기능 컴포넌트를 검증하여 안전성을 확보하려는 노력이나 자체적으로 암호개발을 통해서 안전성을 확보하려는 정책과 일치한다. 암호로 대표되는 정보보호기반 기술의 안전성을 확보하기 위해서 각국 정부는 많은 노력과 자원을 투입하고 있는 실정이다. 따라서 COTS 기반 정보시스템의 도입 시

**[표 2]** 보안기능 컴포넌트 우선 순위

| 구분 | | | 정보보호기능 | 중요도 | 우선순위 |
|---|---|---|---|---|---|
| 정보보호기반(0.7306) | 암호관련 기반 (0.8300) | 암호알고리즘 (0.5458) | 비밀키 암호 알고리즘 | 0.6769 | 1 |
| | | | 공개키 암호 알고리즘 | 0.1986 | 2 |
| | | | 해쉬함수 | 0.0583 | 4 |
| | | | 난수기능 | 0.0662 | 3 |
| | | 암호프로토콜 (0.4542) | 인증 프로토콜 | 0.2296 | 2 |
| | | | 키교환 프로토콜 | 0.6074 | 1 |
| | | | 디지털 서명 프로토콜 | 0.0815 | 3 |
| | | | 영지식 프로토콜 | 0.0815 | 3 |
| | 키 관리 (0.1700) | | 공개키 인증 기능 | 0.3300 | 2 |
| | | | 키 분배 기능 | 0.3400 | 1 |
| | | | 키 복구 기능 | 0.3400 | 2 |
| 네트워크 및 시스템 보호(0.1884) | 네트워크 보호 (0.7500) | | 통신 프로토콜 기능 | 0.0944 | 4 |
| | | | LAN 보호기술 기능 | 0.2020 | 2 |
| | | | 인터넷 보호 | 0.0944 | 4 |
| | | | 방화벽 기술 | 0.1302 | 3 |
| | | | 침입 탐지 기능 | 0.4791 | 1 |
| | 시스템 보호 (0.2500) | | Secure OS | 0.3400 | 1 |
| | | | Secure DBMS | 0.3300 | 2 |
| | | | 바이러스 방지 기술 | 0.3300 | 2 |
| 보안 관리(0.0810) | 네트워크 보안관리 (0.5000) | | 네트워크 경고 및 보고 관리 | 0.5000 | 1 |
| | | | 접근제어 | 0.5000 | 1 |
| | 시스템 감시 및 운영 관리 (0.5000) | | 보안 취약성 점검 | 0.2453 | 2 |
| | | | 침입 탐지 및 추적 | 0.2453 | 2 |
| | | | 위험 분석 | 0.1864 | 4 |
| | | | 감사기록 및 관리 | 0.3230 | 1 |

조직의 특성에 따라 암호 알고리즘, 암호 프로토콜, 키 관리 등의 컴포넌트의 대체가 필요하다.

**[표 3]** 보안기능 컴포넌트 대체 수준

| 보안기능 컴포넌트 | 대체 수준 |
|---|---|
| 비밀키 암호 알고리즘 | 1 |
| 키교환 프로토콜 | 2 |
| 침입 탐지 기능 | 3 |
| 공개키 암호 알고리즘 | 4 |
| 인증 프로토콜 | 5 |
| 키 분배 기능 | 6 |
| 키 복구 기능 | 7 |
| 공개키 인증 기능 | 7 |
| LAN 보호기술 기능 | 9 |
| 영지식 프로토콜 | 10 |
| 디지털 서명 프로토콜 | 10 |
| 난수기능 | 12 |
| 네트워크 경고 및 보고 관리 | 13 |
| 접근제어 | 13 |
| 해쉬함수 | 15 |
| 방화벽 기술 | 16 |
| Secure OS | 17 |
| Secure DBMS | 18 |
| 바이러스 방지기술 | 18 |
| 통신 프로토콜 기능 | 20 |
| 인터넷 보호 접근제어 | 20 |
| 감사기록 및 관리 | 22 |
| 침입 탐지 및 추적 | 23 |
| 보안 취약성 점검 | 23 |
| 위험 분석 | 25 |

<표 4>는 COTS 기반 정보시스템에서 요구하는 보안기능 컴포넌트의 정보보호 요구수준에 대한 설문 결과를 백분율로 환산하여 정보보호 요구수준이 높은 것부터 순위를 매겨 정리한 것이다. 보안환경의 위협 정도에 따라 보안기능 컴포넌트의 대체 여부를 결정하는 설문을 분석하면, 낮은 수준의 보안환경에서도 대체 필요성이 있는 보안기능 컴포넌트는 정보보호 요구수준이 높다는 것을 의미하게 되며 설문 결과 나타나는 점수는 정보보호 요구수준이 높을수록 낮게 나타난다. 따라서 설문 결과를 백분율로 환산한 점수가 낮을수록 정보보호 요구수준의 순위는 높게 책정되었으며, 백분율의 평균은 58.6%, 표준편차는 0.187이다. <표 4>를 보면 정보보호 요구수준이 높은 보안기능 컴포넌트들은 대체로 <표 3>에서의 보안기능 컴포넌트 대체 수준의 우선 순위도 높은 것을 알 수 있다.

전체 컴포넌트의 대체 수준은 비록 낮지만, 네트워크 및 시스템 보호 기반 기술에 속하는 보안 기능 컴포넌트는 네트워크 및 시스템과 관련된 COTS 기반 정보보호시스템을 도입할 때 네트워크 및 시스템 보호에 속하는 보안기능 컴포넌트의 대체 수준을 참조하여 대체해야 한다.

**[표 4]** 보안환경에 따른 보안기능 컴포넌트 대체 순위

| 보안기능 컴포넌트 | 정보보호요구 수준 |
|---|---|
| 비밀키 암호 알고리즘 | 1 |
| 키교환 프로토콜 | 2 |
| 공개키 암호 알고리즘 | 3 |
| Secure OS | 4 |
| 인증 프로토콜 | 5 |
| 난수기능 | 6 |
| 키 분배 기능 | 7 |
| 디지털 서명 프로토콜 | 8 |
| 키 복구 기능 | 9 |
| 영지식 프로토콜 | 10 |
| 인터넷 보호 | 11 |
| 해쉬함수 | 12 |
| LAN 보호기술 기능 | 13 |
| 공개키 인증 기능 | 14 |
| Secure DBMS | 15 |
| 침입 탐지 기능 | 16 |
| 감사기록 및 관리 | 17 |
| 바이러스 방지 기술 | 18 |
| 침입 탐지 및 추적 | 19 |
| 접근제어 | 20 |
| 방화벽 기술 | 21 |
| 네트워크 경고 및 보고 관리 | 22 |
| 통신 프로토콜 기능 | 23 |
| 보안 취약성 점검 | 24 |
| 위험분석 | 25 |

동일하게 보안관리기술에 속하는 보안기능 컴포넌트를 COTS 기반 정보시스템을 도입할 때에도 관련 보안기능 컴포넌트의 대체 수준을 고려하여 대체하면 비용 효과적으로 보안기능 컴포넌트를 채택할 수 있다.

AHP 분석 결과는 COTS 기반 정보시스템 도입 시 보안기능 컴포넌트 대체 결정에 지침을 제공해 줄 것이며, 비용의 관점에서 보면 한정된 자원을 효과적으로 배분하

여 비용 효과적인 COTS 기반 정보시스템을 도입할 수 있도록 한다.

## 6. 결 론

정보시스템과 정보보호시스템의 경계가 모호해지는 상황에서 COTS기반 정보시스템은 보안기능 컴포넌트를 포함하고 있으며, 보안기능 컴포넌트를 대체하는 과정에서 비용, 보안, 신뢰도 등을 함께 고려해야 하므로 보안기능 컴포넌트 대체 대상과 범위를 결정하기가 어렵다. 본 연구는 COTS 기반 정보시스템의 효과적인 보안기능 컴포넌트 대체를 위해 보안기술을 분류하고, 분류한 보안기술을 바탕으로 보안 전문가를 대상으로 설문을 실시하였다. 설문을 통해 획득된 정보와 AHP 방법론을 통해 보안기능 컴포넌트의 대체 수준을 결정하는 데 필요한 보안기능 컴포넌트의 우선 순위를 제공한다.

본 논문의 결과는 COTS 기반 정보시스템 도입에 따른 보안가능 컴포넌트 대체시 한정된 자원을 효율적으로 배분하는 의사 결정에 효과적으로 활용할 수 있다.

## 참고문헌


[1] 김기현 외, "정보보호 기술 분류", *통신정보보호학회지*, 제8권, 제1호, 1998.

[2] 김수동, "객체와 컴포넌트, 그리고 프레임웍", *정보처리학회지*, 제10권, 제3호, 2003.

[3] 최성, 윤태권, "CBD 현황과 전망", *정보처리학회지*, 제10권, 제3호, 2003.

[4] D.Carney, Assembling Large Systems from COTS Components: Opportunities, Cautions, and Complexities. SEI Monogra
-phs on Use of Commercial Software in Government Systems, Software Engineering Institute, Pittsburgh, USA, June, 1996.

[5] Meeson, Reginald, Analysis of Secure Wrapping Technologies, Institute for Defense Analyses Alexandria, Va, 1997.

[6] K.Wallnau, Carney and B. Pollabk, How COTS Software Affects the Design of COTS-Intensive Systems, SEI Interactive, June, 1998.

[7] T. L. Saaty, Decision Making for Leaders: The Analytical Hierarchy Process for Decisions in a Complex World, RWS Publications, 1995.

[8] C.Abts, B. Boehms, E.B.Clark, "COCOTS: A COTS Software Integration and Cost Model-Model Overview and Preliminary Data Findings", ESCOM, 2000.

[9] C.Abts, B.Boehms, and E.B.Clark, "COCOTS:A Software COTS-Based Systems Cost Model-Evolving Towards Maintenance Phase Modeling", ESCOM, 2001.

[10] Thomas G.Baker, "Lessons Learned Integrating COTS into Systems", ICCBSS 2002, *Lecture Notes in Computer Science*, pp.21-30, 2002.

[11] Nicky Boertien, Maarten W.A.Steen, Henk Honkers, "Evaluation of Component-Base
-d Development Methods", *Proceedings of Sixth CAiSE/IFIP8.1 International Workshop on Evaluation of Modeling Methods in Systems Analysis and Design*, 4-5 June, 2001.

[12] Christine L. Braun, "A lifecycle process for the effective reuse of commercial off-the-shelf (COTS) software", *Proceedings of the Symposium on Software reusability*, pp.29-36, 1999.

[13] Committee on National Security Systems, National Information systems Security Glossary, No. 4009, 2003.

[14] Committee on National Security Systems, Revised Fact Sheet, National Information Acquisition Policy, No.11, 2003.

[15] John C. Dean, CD, and Li Li, "Issues in Developing Security Wrapper Technology for COTSs Software Products", ICCBSS 2002, *Lecture Notes in Computer Science*, Vol. 2255, pp.76-85. 2002.

[16] J.C. Dean, "Security Wrapper Technology for COTS Software Products", *Proceedings of 13th Annual Software Technology Conference, Utah, 2001*.

[17] Anthony Earl, "Five Hurdles to the Successful Adoption of Component-Based COTS in a Corporate Setting", ICCBSS 2002, *Lecture Notes in Computer Science*, Vol.2255, pp.97-107, 2002.

[18] D.Kunda and L.Brooks, "Identifying and Classifying Processes that Support COTS Component Selection: A Case Study", *European Journal of Information Systems*, Vol.9, No.4, pp.226-234, 2000.

[19] Douglas Kunda, "STACE: Social Technical Approach to COTS Software Evaluation", Component-Bases Software Quality, *Lecture Notes in Computer Science,* Vol.2693, pp.64-84, 2003.

[20] Maurizio Morisio and Marco Torchiano, "Definition and Classification of COTS: A Proposal", 1st International Conference, ICCBSS2002, *Lecture Notes in Computer Science*, Vol.2255, pp.21-35. 2002.

[21] NIST, "Security Requirement for Cryptographic

Module", FIPS 140-2, 1994.
[22] M.Ochs, D.Pfahl, G..Chrobok-Diening and B. Nothhelfer-Kolb B., "A COTS Acquisition Process: Definition and Application Experience", *Proceedings of 11th ESCOM Conference*, 2000.
[23] Kie Sung Oh and et al., "A Selection Process of COTS Components Based on the Quality of Software in a Special Attention to Internet", HIS, *Lecture Notes in Computer Science*, Vol.2713, pp.626-631. 2003.
[24] Donald J.Reifer and et al., "Estimating the Cost of Security for COTS Software", ICCBSS2003, *Lecture Notes in Computer Science*, Vol. 2580, pp.178-186. 2003.
[25] R.Solms, J.H.P.Eloff and S.H.Soms, "Computer Security Management: A Framework for Effective Management Involvement", *Information Age*, Vol.24, No.4, Oct., pp.217-222. 1990.
[26] Fan Ye and Tim Kelly, "COTS Products Selection for Safety-Critical Systems", ICCBSS 2004, *Lecture Notes in Computer Science Vol.* 2959, pp.53-62. 2004.

**최 명 길**(Myeonggil Choi) **[정회원]**

- 1993년 : 부산대학교 학사
- 1995년 : 부산대학교 석사
- 2004년 : 한국과학기술원 박사
- 1995년 ~ 2000년 : 국방과학연구소 연구원
- 2000년 ~ 2005년 : 한국전자통신연구원 국가보안기술연구소 선임연구원
- 2005년 ~ 2007년 : 인제대학교 조교수
- 2008년 ~ 현재 : 중앙대학교 조교수

<관심분야>
보안성평가, 홈네트워크 보안, 정보보호정책 및 관리

**황 원 주**(Won-Joo Hwang) **[정회원]**

- 1998년 : 부산대학교 컴퓨터공학과 학사
- 2000년 : 부산대학교 컴퓨터공학과 석사
- 2002년 : 오사카대학 정보시스템공학과 박사
- 2002년 ~ 현재 : 인제대학교 정보통신공학과 조교수

<관심분야>
홈네트워크, 정보보호

**김 명 수**(Myoung-Soo Kim) **[정회원]**

- 1999년 : 부산대학교 경영학사
- 2001년 : 한국과학기술원 경영공학 석사
- 2006년 : 한국과학기술원 경영공학 박사
- 2006년 ~ 2008년 : SK 경영경제연구소 연구원
- 2008년 ~ 현재 : 강원대학교 경영학과 전임강사

<관심분야>
정보통신경영, e-Business 전략 수립, 정보보안, 통신시스템 분석