정보시스템 도입에 따른 보안기능 컴포넌트 대체 수준 의사결정
Decision on Replacing Security Components for Information Systems

*최명길, 김현우, 김은혜, 김세헌
*국가보안기술연구소, 한국과학기술원 산업공학과
Myeonggil Choi, Hyunwoo Kim, Eunhye Kim, Sehun Kim
National Security Research Institute
Department of Industrial Engineering, KAIST

Abstract

Enterprises and governments currently utilize COTS based information systems which are a kind of component based systems. Especially, COTS are widely utilized as information security systems and information systems including information security functions. This paper suggests an appropriate adaptation level of security functional components and a cost effective priority among them. 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.

Keywords: COTS, COTS based information systems, security component, AHP.

1. 서 론

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 [1, 2].

정보시스템의 보안 문제와 별개로 소프트웨어 생산성에 대한 위기가 심각해짐에 따라 소프트웨어 개발 생산성 향상을 위한 다양한 연구가 수행되었다. 소프트웨어 개발의 생산성 향상을 위해 가장 적합한 접근법으로 컴포넌트 기반 개발 방법론(component based development method)이 알려져 있다 [3, 4, 5]. 컴포넌트 기반 개발 방법론을 적용한 대표적인 정보시스템으로 COTS 기반 정보시스템(commercial off the shelf based information systems)을 들 수 있다 [5, 7, 8].

COTS 기반 정보시스템은 다양하게 정의할 수 있지만, 본 연구는 정부기관이 시스템을 개발할 때, 비용을 절감하기 위해서 민간 개발 정보시스템의 일부 또는 전부를 획득하여 정부 개발 정보시스템의 컴포넌트로 활용하여 개발된 시스템으로 한정한다 [9, 10].

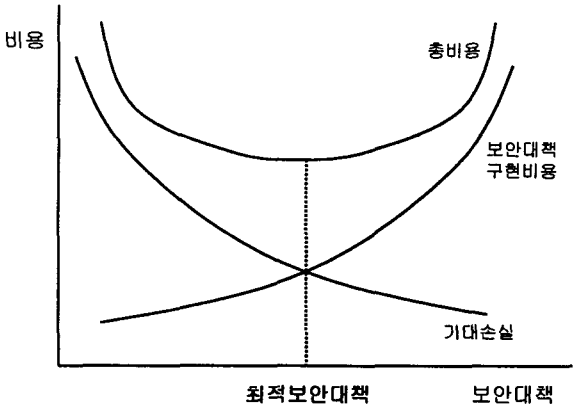
국가기관이 COTS 기반 정보시스템을 활용하는 목적은 다음과 같다. 첫째, 기존의 완성된 상용 정보시스템은 조직의 특성을 반영하기 어려우므로 국가기관은 조직의 특성을 반영한 정보시스템의 도입을 추구한다. 둘째, 국가기관은 도입 비용이 저렴하고, 도입효과가 높은 정보시스템 개발을 추구한다. 셋째, 국가기관은 정보시스템의 합리적인 비용으로 안전한 정보시스템의 도입을 원한다. 즉 정보시스템 중 높은

보안성과 신뢰성을 요구하는 컴포넌트는 많은 비용을 투자하여 개발하고, 신뢰성이 덜 중요한 컴포넌트는 시장에서 도입하여 최종적으로 조립하여 정보시스템의 신뢰성을 확보할 수 있다 [11, 12].

오늘날 컴포넌트 기반 정보시스템의 형태인 COTS기반 정보시스템은 정부기관이나 민간조직에 있어서 널리 활용되고 있으며, 특히 정보보호시스템과 정보보호기능이 결합된 정보시스템 도입에 있어서 폭넓게 채용되고 있는 실정이다 [1, 2]. 따라서 정부기관과 민간조직은 보안이 확보된 COTS 기반 정보시스템 도입을 추구하고 있으며, 보안 관련 컴포넌트 도입 방법을 결정해야 한다. 즉 외부에서 개발된 보안 관련 컴포넌트는 신뢰성은 낮은 반면 조달 비용이 저렴하고, 조직내의 보안 전문가가 개발한 보안 컴포넌트는 신뢰성이 높은 반면 개발 비용이 상승될 수 있다. 즉 보안 컴포넌트의 신뢰성 수준과 비용은 트레이드 오프(trade-off) 관계를 유발한다.

COTS 기반 정보시스템의 보안 컴포넌트의 신뢰성 확보 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 위험에 의한 기대손실의 합계인 총비용이 최저가 되는 수준에서 보안 대책을 강구한다. 즉 최적보안대책 결정모형은 가장 비용 효과적인 보안 대책이 먼저 고려된다는 가정을 전제로 하고, 한계 효용과 한계 비용이 일치하는 점에서 최적화된다 [13].

본 연구는 COTS 기반 정보시스템의 보안 컴포넌트에 초점을 둔다. 조직은 비용효과적이며, 최적의 보안성을 확보할 수 있는 보안기능 컴포넌트 대체 수준을 결정해야 하는 문제에 직면한다. COTS 기반 정보시스템은 국가기관이 정보시스템을 획득하는 중요한 방법이며, 특히 국가기관이 도입하는 시스템의 보안성 확보를 위해서 중요 보안 컴포넌트를 자체 개발을 통해 개발한다면 비용 효과적이고, 안전성이 확보된 정보시스템을 확보할 수 있다.



<그림 1> 최적보안대책 결정 모형

본 연구는 COTS 기반 정보시스템의 도입에 따른 최적의 보안기능 컴포넌트 대체 수준을 결정하는 방법과 비용 효과적인 보안기능 컴포넌트간의 우선순위를 제시한다. 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. 설문조사 결과는 AHP(Analytic Hierarchy Process) 방법론을 사용하여 분석하여 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 활용하여 보안기능 컴포넌트의 우선 순위를 결정하고 보안기능 컴포넌트의 대체 수준을 분석

한다. 6장은 결론이다.

2. 관련 연구

COTS 기반 정보시스템의 보안 컴포넌트 대체 문제는 COTS 컴포넌트 선정 연구와 관련성을 가지고 있다. COTS 기반 정보시스템의 보안 컴포넌트 대체와 관련된 연구로는 COTS 기반 정보시스템 도입 시 보안 컴포넌트 도입을 통한 보안성 확보와 관련된 연구 [14, 15, 16], COTS 기반 정보시스템의 컴포넌트 선정을 위한 방법 연구 [8, 17, 18, 19], 비용을 기준으로 한 보안 컴포넌트 선정 연구 [20, 21, 22] 등이 있다. 다음 연구는 COTS 기반 정보시스템의 보안 컴포넌트 선정과 관련된 최근의 연구이다.

John C. Dean and et al.는 보안성이 없는 COTS 컴포넌트를 이용하여 COTS 기반 정보시스템을 개발 시 보안성을 확보하는 방법을 탐색하고 있으며, COTS 기반 정보시스템의 보안성 확보 방법으로 Security Wrapper Technology를 제시하고 있다 [14]. 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.

Donald J. Reifer and et al.는 COTS 기반 정보시스템의 도입에 따라 보안 문제가 심각해지고 있는 상황에서, 보안 컴포넌트를 도입할 때 발생하는 비용을 예측할 수 있는 비용예측모델을 제시하고 있다 [20]. 이 연구는 비용관점에서 COTS 기반 정보시스템의 사용자가 보안 컴포넌트 도입 여부를 결정할 수 있게 하고 있지만, 보안 컴포넌트가 가져올 수 있는 수익과 보안 컴포넌트간의 중요성을 고려하고 있지 않다.

Kie Sung Oh and et al.는 multiple criteria decision making 방법을 사용하여 COTS 컴포넌트를 선택할 수 있음을 보여주고 있다 [8]. 이 연구는 소프트웨어 품질 메트릭을 기준으로 삼아 COTS 컴포넌트를 선정하는 의사결정기법을 도입했다. 그러나 의사결정기법의 적용 가능성은 제시하였지만, 소프트웨어 품질을 결정하는 다차원의 기준을 의사결정기법에 적용할 때 발생하는 복잡성에 대해서는 고려하지 않고 있다.

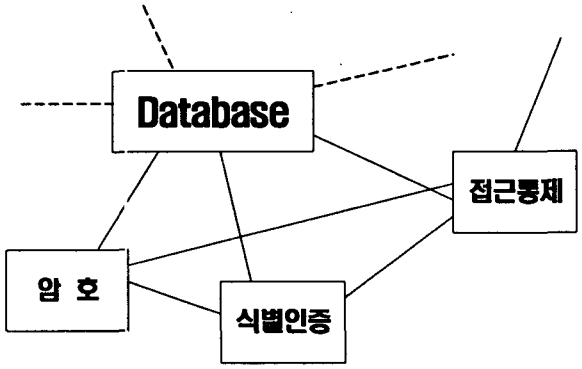
COTS 기반 정보시스템에 맞은 COTS 제품을 선택하는 방법이 제대로 정형화되어 있지 않아서 전체 COTS 기반 정보시스템의 안정성을 보증하지 못한다. Fan Ye와 Tim Kelly는 적절한 COTS 제품을 선택하는 것이 안전한 시스템을 완성하는데 있어서 중요한 요소라고 생각하고, 안전 지향적인 시스템에 맞는 COTS 선택 방법을 제시하였다 [17]. 이들이 제안한 CBCPS (Contract-Based COTS Product Selection)에서는 COTS 제품의 선택에 앞서 먼저 시스템의 위험 분석을 통해 현재 시스템이 가지고 있는 위험 요소를 파악하고, 새로운 COTS가 도입되고 난 후에 나타날 수 있는 잠재적인 위험요소까지도 분석을 마쳐야 한다. 그런 다음 시스템 위험분석을 통해 얻은 자료를 새롭게 선택하고자 하는 COTS 기능이 갖추고 있어야 하는 정보보호 요구사항으로 삼게 된다. 이렇게 얻은 정보보호 요구사항은 COTS를 선택하는데 있어 평가와 선택의 기준으로 사용되는데, COTS의 선택 단계에 앞서 시스템이 갖고 있는 위험요소를 파악하므로 새로운 COTS가 적용된 후의 시스템 안정성을 더욱 보장할 수 있는 방법이다.

D. Kunda는 안정된 COTS 기반 정보시스템의 관건은 시스템의 요구사항에 잘 부합되는 COTS를 선택하는 데 있다고 보았다 [23]. 하지만, 정형화된 COTS 선택방법의 부재로 많은 시간과 비용이 필요하며, 시간과 비용을 투자한 COTS의 선택 후에도 여전히 존재하는 불확실성으로 인해 시스템의 안전이 위협 받을 수

있다. Kunda는 COTS를 평가하고 선택하는 데 있어서 다각도의 접근방법이 필요하다고 보고, COTS를 평가하고 선택할 때 고려해야 되는 COTS의 기능적 특성, 품질적 특성, 비용적인 면, 사회적 인지도의 4가지 요소를 제안하였다. 4가지 요소들의 상대적 중요도를 AHP를 이용하여 분석하여, COTS의 평가와 선택과정에 이 요소들을 어떻게 참조해야 되는지에 관한 정성적인 기준을 제시하였다.

3. COTS 기반 정보시스템의 개발 절차

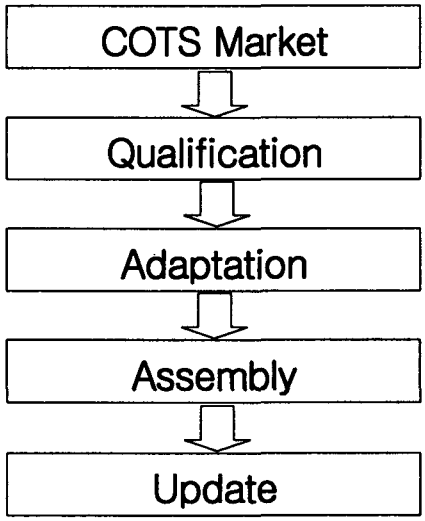
<그림 2>는 보안기능 컴포넌트로 구성된 COTS 기반 정보시스템의 한 예를 보여준다.



<그림 2> COTS 기반 정보시스템

COTS 컴포넌트를 도입하여 시스템을 설계하는 가장 큰 이유는 비용의 절감과 신기술의 빠른 도입 및 업데이트이다. 시스템의 보안을 유지하면서 COTS의 이러한 장점을 최대한 고려하기 위해서는 COTS의 특성을 고려한 보안 설계가 이루어져야 한다.

COTS 기반 정보시스템의 개발은 <그림 3>과 같은 절차에 의해 이루어진다 [24]. COTS 기반 정보시스템 개발은 우선 COTS 컴포넌트를 제공하는 시장에서 적절한 제품을 선택한 후, 이것을 조립이 가능하도록 적절히 가공한다. 가공된 COTS 컴포넌트는 안정적인 아키텍처를 기반으로 조립하게 되며, 이렇게 만들어진 시스템은 요청에 따라 COTS 컴포넌트를 교체함으로써 손쉽게 변경이 가능하게 된다. 각 단계에서의 정보보호 관련 사항들을 간단히 살펴보면 다음과 같다.



<그림 3> COTS 기반 시스템 개발 절차

가. COTS Market

COTS 소프트웨어 시장에는 다양한 제품들이 출시되어 있지만, 제품의 규격화가 이루어지지 않은 실정이다.

나. Qualification

COTS 기반 정보시스템 개발 절차 중 정보보호에 관련하여 가장 중요한 단계는 Qualification이다. 사용자는 자신의 시스템에 적절한 컴포넌트를 구입해야 하는데, COTS 시장에 있는 모든 컴포넌트가 우수한 것은 아니다. 컴포넌트간의 품질의 차이는 매우 극심하며, 심지어 동일한 기능을 제공하고 같은 개발표준을 준수하는 컴포넌트라 할 지라도 품질과 성능의 차이가 나타날 수 있다. 그러므로, COTS 컴포넌트에 대한 선정 기준이 필요하며, 기준에 맞는 컴포넌트 평가 절차가 이 단계에서 이루어져야 한다. 하지만, COTS 컴포넌트 평가를 위해서는 많은 비용이 발생하게 되므로, 보안기능 컴포넌트의 대체 수준이 적절하다고 제시되어 있는 경우에는 평가뿐만 아니라 다음 과

정인 가공단계에 필요한 비용까지도 최소로 할 수 있다.

다. Adaptation

Adaptation 단계는 선정된 COTS 컴포넌트를 설계하고자 하거나, 이미 개발되어 운용되고 있는 COTS 기반 정보시스템에 조립이 가능하도록 적절히 가공하는 단계이다. COTS 컴포넌트를 가공해야 한다는 점에서 COTS 기반 정보시스템의 개발 절차의 전체적인 과정과 구조를 고려해야만 한다. 즉 COTS 기반 정보시스템의 정보보호 요구사항에 맞게 이루어져야 한다. COTS 컴포넌트는 개별적으로 동작하는 것이 아니라, 다른 COTS 컴포넌트와 연결되어 상호작용을 한다. COTS 컴포넌트간에 기본적인 보안 요소인 비밀성, 무결성, 가용성이 유지되면서 시스템이 운용되기 위해서는 각 COTS 컴포넌트들 사이의 상호관계를 고려해서 가공해야 한다. 특히 컴포넌트간의 보안 수준 문제, 정보접근 허용수준 문제, 암호 프로토콜의 설정 등의 사항들은 정보보호에 큰 영향을 미치는 요소들이므로 매우 중요하다. 이 문제는 COTS 기반 정보시스템이 지향하는 보안 수준이나 정책에 관련된 문제이며 위험 평가 등을 바탕으로 신중히 결정해야 한다. 선정된 COTS 컴포넌트는 정의된 수준 또는 형태로 인터페이스를 가공해야 한다.

라. Assembly

가공된 COTS 컴포넌트를 안정된 아키텍처를 기반으로 조립하는 과정이 Assembly 단계이다. 기본적으로 에러가 많이 발생하는 시스템은 정보보호에 취약할 수 밖에 없으므로 시스템의 용량과 구조를 고려하여 COTS 컴포넌트를 조립하여야 한다.

마. Update

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

4. 연구방법론

본 연구에서는 정보시스템 도입에 따른 보안기능 컴포넌트의 대체 우선 순위를 결정하기 위해 과학적 타당성을 인정받고 있는 AHP 방법론을 이용하였다. AHP는 복잡한 문제를 단순화시켜 합리적인 의사결정이 가능하도록 지원해주는 계층적 분석 방법론으로 복수의 요소들에 대한 가중치를 동시에 고려하기 보다는 두 개씩 짝을 지어 이원비교를 하게함으로써 조사하려는 요소들 사이의 상대적 중요도 판단을 명확하고 용이하게 할 수 있게 해 준다 [25]. 요소들 사이의 상대적 중요도를 판단할 때 판단의 일관성 정도(consistency ratio)를 알려주어 일관성이 결여되었을 때에는 수정작업을 가능하게 해 준다. 연구방법은 다음의 3가지 단계로 나눌 수 있다.

[단계 1]

AHP를 사용하기 위해서는 먼저 해결하고자 하는 문제를 하위의 구성 요소들로 분해하여 계층적으로 나타내어야 하는데, 이를 위해 본 연구에서는 정보보호기술을 분류하여 보안기능 컴포넌트의 계층 모델을 작성하였다.

[단계 2]

보안기능 컴포넌트간의 우선 순위를 도출을 위해 상대적 기여도를 전문가조사(Delphi approach)를 통해서 측정하였다. 설문대상은 정보보호전문가를 대상으로 실시하였으며, 정보보호전문가는 정보보호전문 연구기관 연구원, 정부기관 정보보호관리자, 정보보호시스템 개발자 등이다. 설문의 내용은 각 보안기능 계층에 속하는 컴포넌트간의 상대적 중요도를 측정하는 질문으로 구성되었다.

[단계 3]

전문가 설문조사를 통해 획득한 결과를 AHP 방법론을 적용하여 분석하고, 각 보안기능 컴포넌트간의 우선 순위를 결정한다.

각 단계에서 수행한 연구 내용은 다음과 같다. [단계 1]은 AHP 방법론을 적용하기 위해서 보안기능 컴포넌트를 3계층으로 구분하여 개발한다. 보안기능 컴포넌트를 계층으로 분류하는 방법은 정보보호기술 분류 연구 결과를 수용했다 [26]. 다양한 정보보호기술 분류가 이루어지고 있지만, 대체로 정보보호 기술 분류의 근본적인 골격이 유사하므로, 본 논문은 정보보호기술을 포괄적으로 포함할 수 있는 분류 방법을 개발하였다.

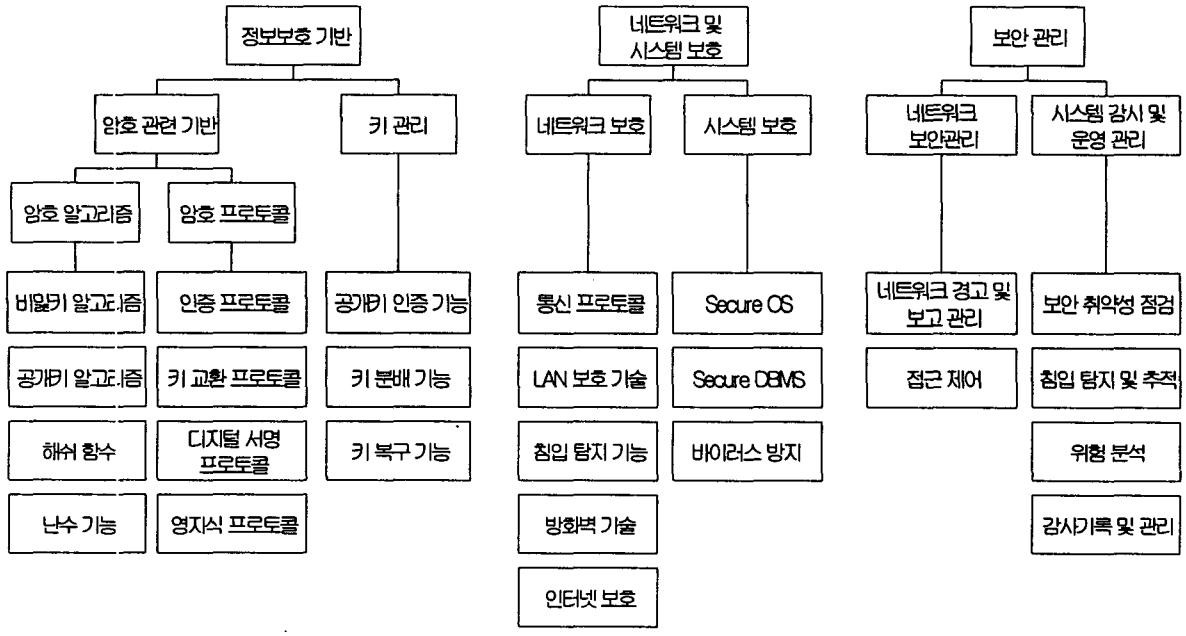
본 연구가 개발한 분류의 최상위 계층은 정보보호 기반기술, 네트워크 및 시스템 보호기술, 보안관리기술 등 3가지로 이루어진다. 정보보호 기반기술은 암호관련 기반기술, 키 관리기술로 구성되며, 네트워크 및 시스템 보호기술은 네트워크 보호와 시스템 보호로 구성된다. 보안관리기술의 2번째 계층은 네트워크 보안관리와 시스템 감시 및 운영관리로 구성된다. 각 계층의 마지막 단계는 <그림 4>와 같이 구성된다.

[단계 2]는 전 단계에서 개발한 계층모델을 바탕으로 전문가조사를 실시하였다.

설문지는 온라인과 오프라인을 통하여 총 150부의 설문을 송부하여 57부를 회송 받았고, 총 51부의 유효한 설문을 획득하였다. 설문지 회송률은 38%였고, 설문조사는 2003년 11월15일에서 2003년 12월 15일까지 한 달간 이루어졌다. 설문지의 일부를 부록 A에서 소개한다.

설문조사는 각 계층에 속하는 컴포넌트 간의 상대적 중요도를 측정하는 내용으로 구성되었다. 설문척도는 의사결정 요인의 이원비교를 위해 1점에서 9점까지의 수치로 표현하였는데, 1은 비교하는 두 컴포넌트의 동등한 중요도를 나타내고, 9는 한 컴포넌트가 절대적으로 중요함을 나타낸다. 이 척도는 각 단계의 컴포넌트 간의 상대적 중요도(relative weight)에 관한 주관적인 판단을 수치로 나타낸 것이다.

[단계 3]에서 사용한 AHP 방법론을 간단히 설명하면 다음과 같다.



<그림 4> 보안기능 컴포넌트의 계층 모델

설문조사를 통해 우선 순위를 체계적으로 구하기 위해서는 중요도 척도에 따른 이원비교 행렬(pairwise comparison matrices)을 다음과 같이 구성해야 한다.

$$A=\begin{bmatrix} w_1/w_1 & w_1/w_2 & \mathrm{L} & w_1/w_n \\ w_2/w_1 & w_2/w_2 & \mathrm{L} & w_2/w_n \\ \mathrm{M} & & & \mathrm{M} \\ w_n/w_1 & w_n/w_2 & \mathrm{L} & w_n/w_n \end{bmatrix}$$

여기서 w_i와 w_j는 i번째 속성과 j번째 속성의 가중치를 나타내는데, w_i/w_j는 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 A에 대하여 $[AW=\lambda W]$를 만족하는 스칼라 λ와 $n\times 1$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.

행렬 A의 일관성의 정도가 클수록 $\lambda_{\max}$는 n에 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 우선순위는 <표 1>과 같다. 1계층에서 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 우선 순위가 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 2>는 보안기능 컴포넌트의 대체 수준을 나타낸다. <표 2>에서 알 수 있듯이 해쉬함수와 난수기능을 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 검증 프로그램(Cryptography Module Validation Program) [27]을 통해서 암호기능 컴포넌트를 검증하여 안전성을 확보하려는 노력이나 자체 암호개발을 통해서 안전성을 확보하는 것이 시스템의 보안성을 견고히 할 수 있는 방법임을 나타낸다. 암호로 대표되는 정보보호기반 기술의 안전성을 확보하기 위해서 각국 정부는 많

<표 1> 보안기능 컴포넌트 우선 순위

구분			정보보호기능	중요도	우선 순위	전체 순위
정보 보호 기반 (0.7306)	암호 관련 기반 (0.8300)	암호 알고리즘 (0.5458)	비밀키 암호알고리즘	0.6769	1	1
			공개키 암호 알고리즘	0.1986	2	4
			해쉬함수	0.0583	4	15
			난수기능	0.0662	3	12
		암호 프로토콜 (0.4542)	인증 프로토콜	0.2296	2	5
			키교환 프로토콜	0.6074	1	2
			디지털 서명 프로토콜	0.0815	3	10
			영지식 프로토콜	0.0815	3	10
	키 관리 (0.1700)		공개키 인증 기능	0.3300	2	7
			키 분배 기능	0.3400	1	6
			키 복구 기능	0.3300	2	7
네트워크 및 시스템 보호 (0.1884)	네트워크 보호 (0.7500)		통신 프로토콜 기능	0.0944	4	20
			LAN 보호기술 기능	0.2020	2	9
			인터넷 보호	0.0944	4	20
			방화벽 기술	0.1302	3	16
			침입 탐지 기능	0.4791	1	3
	시스템 보호 (0.2500)		Secure OS	0.3400	1	17
			Secure DBMS	0.3300	2	18
			바이러스 방지 기술	0.3300	2	18
보안 관리 (0.0810)	네트워크 보안관리 (0.5000)		네트워크 경고 및 보고 관리	0.5000	1	13
			접근제어	0.5000	1	13
	시스템 감시 및 운영 관리 (0.5000)		보안 취약성 점검	0.2453	2	23
			침입 탐지 및 추적	0.2453	2	23
			위험 분석	0.1864	4	25
			감사기록 및 관리	0.3230	1	22

은 노력과 자원을 투입하고 있는 실정이다. 따라서 COTS 기반 정보시스템의 도입 시 조직의 특성에 따라 암호 알고리즘, 암호 프로토콜, 키 관리 등의 컴포넌트의 대체가 필요하다.

전체 컴포넌트의 우선 순위는 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 우선 순위를 참조하여 대체해야 한다.

<표 2> 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 방지 기술	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

동일하게 보안관리기술에 속하는 보안기능 컴포넌트를 COTS 기반 정보시스템을 도입할 때에도 관련 보안기능 컴포넌트의 우선 순위를 고려하여 대체하는 것이 비용 효과적으로 보안 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 배분하여 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 연구의 결과는 현재 각국에서 진행되고 있는 CMVP를 감안하면 활용도가 높을 것으로 고려된다.

본 논문의 결과는 COTS기반 정보시스템 도입 시 비용 효과적인 보안기능 컴포넌트 대체를 위해 효과적인 의사결정에 활용할 수 있다.

부 록 A

1. 설문척도

척도	정의	설명
1	동등하게 중요	두 개의 요소가 똑같이 중요함
3	약간 더 중요	한 요소가 다른 요소보다 약간 더 중요함
5	더욱 더 중요	한 요소가 다른 요소보다 더욱 더 중요함
7	대단히 더 중요	한 요소가 다른 요소보다 대단히 더 중요함
9	절대적으로 중요	다른 요소에 비해서 비교할 수 없을 정도로 절대적으로 중요함

2. 최상위 계층에서의 이원비교

항목	← 왼쪽 항목이 더				동등하게 중요	오른쪽 항목이 더 →				항목
	매우 중요	상당히 중요	중요	약간 중요		약간 중요	중요	상당히 중요	매우 중요	
정보보호 기반기술										네트워크 및 시스템 보호
정보보호 기반기술										보안관리
네트워크 및 시스템 보호										보안관리

3. 2번째 계층에서의 이원비교

항목	←왼쪽 항목이 더				동등하게 중요	오른쪽 항목이 더→				항목
	매우 중요	상당히 중요	중요	약간 중요		약간 중요	중요	상당히 중요	매우 중요	
암호관련 기반기술										키 관리
네트워크 보호										시스템 보호
네트워크 보안관리										시스템 감시 및 운영관리

참 고 문 헌

[1] Committee on National Security Systems, No. 4009, National Information systems Security Glossary, 2003, 5.

[2] Committee on National Security Systems, No.11, Revised Fact Sheet, National Information Acquisition Policy, 2003, 7.

[3] 최성, 윤태권, "CBD 현황과 전망", 정보처리학회지, 제10권, 제3호, 2003.5.

[4] 김수동, "객체와 컴포넌트, 그리고 프레임웍", 정보처리학회지, 제10권, 제3호, 2003.5.

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

[6] Maurizio Morisio and Marco Torchiano, "Definition and Classification of COTS: A Proposal", LNCS, 1st International Conference, ICCBSS2002, Orlando, FL.USA, 2002, Feb.

[7] Anthony Earl, "Five Hurdles to the Successful Adoption of Component-Based COTS in a Corporate

Setting", ICCBSS 2002, LNCS, 2002, pp.97-107.

[8] 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, LNCS 2713, 2003, pp.626-631.

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

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

[11] Thomas G.Baker, "Lessons Learned Integrating COTS into Systems", ICCBSS 2002, LNCS, 2002, pp.21-30.

[12] Donald J.Reifer and et al., "Estimating the Cost of Security for COTS Software", ICCBSS2003, LNCS 2580, 2003, pp.178-186.

[13] 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, 1990, Oct., pp.217-222.

[14] John C. Dean, CD, and Li Li, "Issues in Developing Security Wrapper Technology for COTSs Software Products", ICCBSS 2002, LNCS 2255, 2002, pp.76-85.

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

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

[17] Fan Ye and Tim Kelly, "COTS Products Selection for Safety-Critical Systems", ICCBSS 2004, LNCS 2959, 2004, pp.53-62.

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

[19] M.Ochs, D.Pfahl, G..Chrobok-Diening and B. Nothhelfer-Kolb B., "A COTS Acquisition Process: Definition and Application Experience", 11th ESCOM Conference, Shaker, Maastricht, 2000.

[20] Donald J. Reifer, Barry W.Boehm and Murali Gangadharan, "Estimating the Cost of Security for COTS Software", ICCBSS 2003, LNCS 2580, 2003, pp.178-186.

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

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

[23] Douglas Kunda, "STACE: Social Technical Approach to COTS Software Evaluation", Component-Bases Software Quality, LNCS 2693, 2003, pp.64-84.

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

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

[26] 김기현, 은유진, 이인수, 이흥섭, "정보보호 기술 분류", 통신정보보호학회지, 제8권, 제1호, 1998

[27] NIST, "Security Requirement for Cryptographic Module", FIPS 140-2, 1994.