품질과 비용을 고려한 프로세스 기반의 보안공학방법론에 관한 연구

최 명 길*

A Study on a Security Engineering Methodology for Information Security Systems Considering Quality and Cost

Myeonggil Choi*

Abstract

For reliability and confidentiality of information security systems, the security engineering methodologies are accepted in many organizations. To improve the effectiveness of security engineering, this paper suggests a security methodology ISEM, which considers both product assurance and production processes, takes advantages in terms of quality and cost. To verify the effectiveness of ISEM, this paper introduces the concepts of quality loss, and compares the development costs and quality losses between ISEM and CC through the development of VPN system.

Keywords : Security Engineering, Product Assurance, Production Assurance, ISEM

논문접수일 : 2009년 03월 27일 논문게재확정일 : 2009년 06월 15일

* 중앙대학교 상경학부 경영학 전공, 조교수, e-mail : mgchoi@cau.ac.kr

1. 서 론

인터넷의 발전은 전자상거래, 전자정부 등 다양한 형태의 전자 서비스 등을 가능하게 하였지만, 반면에 해킹, 컴퓨터 바이러스 유포 등 사이버 위협을 동시에 급증시키고 있다. 이러한 사이버 위협은 금융기관, 전자상거래 사이트 등의 개인정보 유출을 발생시키고 있을 뿐만 아니라 국가 전산망까지 위협하고 있는 실정이다. 정부, 기업, 연구소 등은 사이버 위협에 대처하고, 안전한 정보통신시스템 운영을 위해서 정보보호시스템 개발, 운영에 많은 인력과 비용을 투자하고 있다[ISO/IEC(a), 1996; J. Leach, 2003; S. Y. Lee 외 2인, 2006].

정부기관, 연구소, 기업 등은 안전하고 신뢰성이 높은 정보보호시스템을 개발하기 위하여 다양한 정보보호시스템 개발방법론을 채택하고 있으며, 특히 고품질의 정보보호시스템을 확보하기 위하여 국제공통기준(Common Criteria : CC), ITSEC(Information Technology Security Evaluation Criteria), SSE-CMM(Systems Security Engineering-Capability Mature Model) 등과 같은 보안공학기법을 채용하고 있다[SSE-CMM, 1999; M. D. Konard 외 2인, 1996].

보안공학방법론은 보증 대상에 따라 정보보호제품 자체를 보증하는 제품보증접근법과 개발 프로세스를 보증하는 개발프로세스보증접근법으로 구분할 수 있다[R. Baskerville, 1992; L. Godrdon 외 1인, 1992; T. P. Horman 외 2인, 2006]. 제품 자체를 보증하는 방법은 정보보호시스템의 기능 및 보증 평가를 통해서 제품의 품질을 보증한다. 제품보증접근법은 CC, ITSEC 및 TCSEC(Trusted Computer Security Evaluation Criteria) 등이 있다. 제품보증접근법은 높은 수준의 품질 보증을 제공하는 장점이 있지만, 단점은 제품 보증에 소요되는 비용이 높고, 보증 기간이 많이 소요된다.

개발프로세스 보증 접근법은 개발 프로세스를 보증함으로서 제품의 품질을 보증하는 방법으로 보증 초점을 제품 자체에서 개발 프로세스로 변경한 방식이다. 개발 프로세스 보증 접근법을 사용하는 보안 공학 방법론으로는 SSE-CMM, SPICE(Software Process Improvement and Capability dEtermination), ISO 9000-3(Guidelines for the Development Supply and Maintenance of Software) 등이 있다. 개발 프로세스보증접근법은 제품보증접근법과 비교할 때 비용이 저렴하고, 보증에 소요되는 기간이 짧지만, 보증 수준은 낮다. 따라서 높은 수준의 신뢰도를 요구하는 정보보호시스템을 보증하기 위해서는 제품 보증방법을 많이 사용하는 반면, 중간 수준 이하의 정보보호시스템의 보증을 위해서는 개발 프로세스보증방법을 많이 사용한다[DoD, 1985; ISO/IEC(b), 1999; Y. Lee 외 2인, 2006].

높은 수준의 신뢰도를 요구하는 정보보호시스템을 개발하고 운영하는 조직도 정보보호시스템을 보증하는 데 소요되는 자원 및 기간이 충분하지 못한 경우가 대부분이다[BSI, 2003; M. D. Higginbothan 외 3인, 1998]. 따라서 높은 수준의 보증 수준을 제공할 수 있으면서, 상대적으로 보증 비용이 저렴하고, 보증 기간이 짧은 보안공학 방법론이 필요하다. 제품보증 방법과 개발 프로세스 보증방법은 상호 배타적일 수 있지만, 두 방법을 조화시키면 상대적으로 저렴한 비용으로 높은 수준의 보증이 가능한 보안공학방법론을 개발할 수 있다[COBIT, 1998; http, 1999].

본 논문에서는 이러한 두 가지 방법론의 장단점을 조화시켜 비용과 품질을 고려한 보안공학 프로세스 기반의 효과적인 정보보호시스템 개발 방법론을 제시하고자 한다. 제품 보증 접근법의 장점인 높은 보증 수준과 개발 프로세스 보증 접근법의 장점인 저비용으로 보증 문제를 해결할

수 있는 보안공학방법론인 ISEM(High Secure Engineering Methodology)을 제시한다. ISEM 방법론은 CC, ITSEC, TCSEC 등과 같은 제품 보증 접근법의 장점인 보증의 정확성을 반영하고, SSE-CMM, SPICE 등과 같은 개발 프로세스 보증 접근법의 장점인 저비용 보증을 결합한 보안공학 방법론이다.

본 논문이 제시하는 보안공학 방법론은 다음과 같은 특징을 가지고 있다. 첫째, 기존의 보안공학방법론은 품질에 초점을 둔 나머지 정보보호시스템 개발 및 평가비용을 고려하고 있지 않다. 따라서 본 논문이 제시하는 ISEM 방법론은 개발 및 평가 비용을 고려하여 정보보호시스템의 품질을 관리할 수 있는 특징을 가지고 있다. 둘째, 기존의 보안공학 방법론은 정보보호시스템의 등급이나 프로세스 등급에 의해서 개발과 평가가 진행됨으로 개발 프로세스와 평가에 있어서 경직성을 가지고 있다. 그러나 본 논문이 제시하는 ISEM 방법론은 정보보호시스템의 특성에 따라 개발 프로세스를 단계별로 탄력적으로 운영할 수 있다. 셋째, ISEM 방법론은 정보보호시스템의 개발비용을 최소화하고, 정보보호시스템의 개발 상황에 따라 개발 프로세스를 신축적으로 운영할 수 있는 특징이 있다.

본 논문의 구성은 다음과 같다. 제 1장은 서론으로 연구의 필요성 및 관련 연구를 서술한다. 제 2장에서는 제품 보증 중심의 보안공학방법론인 CC, ITSEC, TCSEC 등을 고찰한다. 제 3장에서는 프로세스 중심의 보안공학방법론인 SSE-CMM, SPICE 등을 살펴본다. 제 4장에서는 본 논문이 제시하는 보안공학방법론인 ISEM을 설명하며, 제품 보증 접근법에서 소요되는 비용과 ISEM 방법론에서 소요되는 비용을 비교할 수 있는 비용 함수를 이용하여 ISEM 방법론의 비용 효과성을 입증한다. 제 6장은 본 논문의 결론이다.

1.1 관련 연구

본 연구와 관련되는 연구는 기존의 보안공학방법론과 기준 표준과의 관련성 연구, 효과적인 정보보호시스템 개발을 위한 보안공학방법론 연구, 보안공학방법론의 활용 연구 등 3가지 등이 있다. 정보시스템 개발 방법론은 비용과 품질을 고려한 정보시스템 개발 문제를 주로 다루고 있지만, 보안공학방법론에서는 정보보호시스템의 품질 문제에만 초점을 두고 있는 실정이다.

보안공학방법론과 기준 표준과의 관련성 연구로는 Wood 등의 "ISO 9000 and Information Security", Pijl 등의 "ISO 9000 versus CMM : Standardization and Certification of IS Development" 등의 연구가 대표적이다[ISO/IEC(a), 1999; J. Leach, 2004]. Wood 등의 연구에서는 정보보호를 강화하려는 노력을 무위로 만드는 이유가 적절한 정보기반(Infrastructure)의 부재라고 지적하고 있다. 이 연구는 ISO 9000이 내포하는 정보보호관리에 초점을 둔 보안공학방법론과 기존의 정보보호대책을 결합하면 조직의 전반적인 정보보호를 강화할 수 있다고 주장한다.

효과적인 정보보호시스템 개발을 위한 보안공학방법론 연구로는 John Leach의 "Security Engineering and Security RoI" 및 Lee 등의 "Integrating Software Lifecycle Process Standards with Security Engineering" 등의 연구가 대표적이다[A. R. W. Fung 외 2인, 2003; B. Hankcock, 2000]. Leach의 연구는 정보보호시스템 개발 이전에 취약성 및 위협을 분석하고, 정보보호시스템이 운영되는 환경을 고려하여, 분석된 취약성 및 위협을 대처할 수 있는 정보보호시스템을 개발해야 한다고 주장하고 있다. Leach의 연구는 정보보호시스템 설계에 필요한 원칙을 다음과 같이 4가지로 제시하고 있다. 첫째는 정보보호시스템 개발자는 설계를 위하여

객관적인 사실에 근거하여 보안 위협을 분석해야 하고, 둘째, 위협과 해결, 대책을 정량화해야 하고, 셋째, 위험과 경영관리체계가 보안 환경에서의 적합성 여부를 측정할 수 있는 정량적인 메커니즘을 제시해야 하고, 넷째, 첫 번째에서 세 번째 원칙을 준수하여 보안 대책을 조정해야 한다. 동 연구의 기여점은 보안공학방법론을 정성적인 방법론에서 데이터를 근거로 하는 정량적인 보안공학방법론의 필요성을 제안하고 있다.

Lee 등의 연구는 보안공학 개념을 결합한 소프트웨어 개발 수명주기 방법론에 보안공학 개념을 도입하고 있다. 본 연구는 소프트웨어 개발 수명주기와 보안공학방법론을 결합한 개발방법론 없이 정보보호시스템을 개발할 경우에는 혼란이 야기된다. 결과적으로 개발 기간의 지연과 안전성을 확보하지 못한 정보보호시스템이 개발될 수 있다고 주장한다. 따라서 이 연구는 소프트웨어 개발 수명주기상의 모든 프로세스와 결과물을 보안공학방법론과 통합해야 한다고 제안하고 있다. Lee 등의 연구는 소프트웨어 개발 수명주기와 보안공학방법론의 결합의 필요성을 제시하고 있다[B. Hankcock, 2000].

조직의 보안대책 강화를 위한 대표적인 보안공학방법론의 활용 연구로는 Eloff 등의 Information Security Management : An Approach to Combine Process Certification and Product Evaluation[L. Barnard 외 1인, 2000]과 동일 저자의 Information Security Management : A Hierarchical Framework for Various Approach[T. P. Horman, 2006] 등이 대표적이다. Eloff 등의 Information Security Management : An Approach to Combine Process Certification and Product Evaluation 연구는 조직의 보안 관리를 위해서 프로세스 평가와 평가 받은 제품을 적절히 혼용하여 사용할 것을 주장하고 있다. 이 연구는 어떤 조직은 BS7799와 같은 보안지침을 중심으로 사용하는 반면, 어떤 조직은 TCSEC, ITSEC, CC 등의 평가 받은 제품을 이용하여 보안을 강화하고 있다고 밝히고 있다. 그러나 두 가지 접근법 중 어느 하나만을 사용할 때는 보안이 강화될 수 없으며, BS7799와 같은 프로세스 평가와 평가받은 제품을 적절히 혼용할 때 조직의 보안을 강화할 수 있다고 주장한다. 이 연구의 의의는 보안공학방법론을 경영 관리 프로세스에 적용함과 동시에 제품의 활용방법을 제시했다는 점이다. 동일한 저자의 Information Security Management : A Hierarchical Framework for Various Approach는 보안 관리와 관련된 인증(certification), 평가(evaluation), 지침(guideline), 표준(standard) 등의 여러 가지 개념을 보안공학의 관점에서 정리하고, 보안 관리를 강화하기 위해 활용하는 방법을 제시하고 있다[http, 1999].

2. 보안공학방법론 고찰

2.1 제품보증중심의 보안공학방법론

제품보증중심의 보안공학방법론으로는 CC, TCSEC, ITSEC 등이 있다. 1985년에 미국은 TCSEC을 제정하였으며 영국, 독일, 프랑스, 네덜란드 등은 공동으로 ITSEC을, 1991년에 캐나다가 CTCPEC (Canadian Trusted Computer Product Evaluation Criteria)을 제정하였다. 이와 같이 선진각국은 자국의 실정에 맞는 평가기준을 제정하여 발전시켜 왔으며, 최근에는 이러한 기준들이 CC로 통합되어 국제표준으로 자리 잡고 있다[SEI, 1999; ISO/IEC(b), 1999].

미국은 1960년대 후반 컴퓨터시스템의 비밀정보를 보호하기 위한 연구를 시작하여 1972년에 미 국방부 지침 5200.28(DoD Directive 5200.8)과 5200.28-M(ADP Security Manual-Techniques

and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems)을 제정하였다. 이 문서는 국방부의 비밀정보를 보호하기 위한 보안정책, 보안요구사항, 기술적 대책 등을 담고 있다. 1983년 미국은 기존의 자료를 바탕으로 하여 일반적으로 오렌지 북(Orange Book)으로 알려진 안전한 컴퓨터시스템 평가 기준인 TCSEC의 초안을 작성한 후, 1985년에 미 국방부 표준(DoD 5200-28-STD)으로 채택하였다.

미 국방부는 안정성이 입증된 컴퓨터 시스템을 국방부 및 정부 기관에 보급하기 위하여 TCSEC을 C1, C2, B1, B2, B3, A1 등 6개의 등급으로 분류하여, 각 기관의 특성에 맞는 컴퓨터 시스템을 도입하도록 권고하였다. 이후 TCSEC은 네트워크용 정보보호시스템 평가를 위한 TNI(Trusted Network Interpretation of the TCSEC), 데이터베이스용 정보보호시스템 평가를 위한 TDI(Trusted Database Interpretation of the TCSEC), 서브시스템 평가를 위한 CSSI(Computer Security Subsystem Interpretation of the TCSEC) 등으로 확장되었다. 1992년 미국의 국가안전국(NSA : National Security Agency)과 국립표준기술원(NIST)은 공동으로 TCSEC, TNI, TDI, CSSI 등 4개 평가기준을 단일화하기 위해 FC(Federate Criteria)를 제정하였으나, CC의 제정으로 인해 시행하지 않고 있다.

ITSEC은 영국, 독일, 프랑스 및 네덜란드 등 4개국이 자국의 정보보호시스템 평가기준을 제정하여 시행해 오다 평가기준이 상이함에 따라 정보보호 제품의 중복 평가로 인해 소요되는 시간, 인력 및 비용을 절감하기 위해서 개발된 공통적인 평가기준이다. 4개 국가들은 1989년에 기존의 기준을 최대한 수용한 평가기준을 개발하기로 합의하고, 공동 기준을 제정하기 위해 노력한 결과, 1991년에 ITSEC V.1.2를 제정하였다[D. Brink, 2001]. ITSEC은 TCSEC과 달리 단일 기준으로 모든 정보보호제품을 평가하려고 하였다. 따라서 보안기능은 개발자가 제품이 사용될 환경을 고려하여 설정하거나 TCSEC 혹은 독일의 ZSIEC(Criteria for the Evaluation of Trustworthiness of Information Technology Systems)에서 미리 정의한 보안기능을 사용하고, 제품에 대한 평가는 보증만으로 수행하고 있다[R. Anderson, 2001].

국제공통기준(CC)은 기존의 평가기준이 자국마다 상이함으로써 발생하는 평가에 소요되는 비용을 줄이기 위하여 단일한 평가기준 제정을 위한 노력의 결과로 탄생했으며, 현재 ISO/IEC 국제표준으로 제정되어 있다. 기존의 평가기준을 운영하던 미국, 캐나다, 프랑스, 독일, 네덜란드 및 영국 등 6개국이 1993년 국제공통기준을 개발하기로 합의하고, 1993년 6월에 구성된 CCEB (Common Criteria Editorial Board)가 1996년 1월 V.1.0을 발표한 후, CCEB를 해체하고, CCIB (Common Criteria Implementation Board)를 구성하였다. CCIB는 국제공통기준 V.1.0에 대해서 각국이 보내온 약 800개의 논평을 처리하여 V.2.0을 1997년 10월에 발표하였고, ISO는 1999년에 국제공통기준을 ISO 15408로 확정하였다.

2.2. 프로세스 중심의 보안공학방법론 고찰

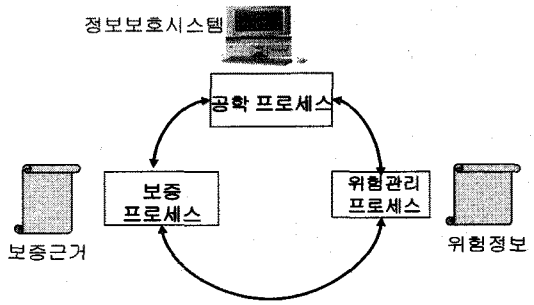
SSE-CMM은 정보보호시스템의 개발 프로세스에 대한 품질 보증을 평가함으로써 최종 산출물의 품질을 평가한다는 보안공학방법론이다. 정보보호시스템의 제품 중심의 보안공학방법론과는 달리, 정보보호시스템 개발 프로세스에 대한 품질을 평가함으로써 정보보호시스템의 품질을 평가할 수 있다는 개념에 착안하고 있다. SSE-CMM은 정보보호시스템의 개발조직의 프로세스를 평가한다는 점에서 정보시스템의 운

영 조직의 보안관리 적절성을 평가하는 보안관리 체계 평가방법론과 차이가 존재한다[E. C., 1992; M. Eloff 외 1인, 2000; J. Herbsleb 외 4인, 1994]. SSE-CMM 외에도 제품의 개발 프로세스를 평가하는 보안공학방법론으로는 ISO 9000-3 "소프트웨어 개발 공급과 유지보수를 위한 지침(Guideline for the development supply and maintenance of software)", SPICE, 등이 있다.

본 연구에서는 SSE-CMM이 기반을 두고 있는 보안공학방법론, SSE-CMM, SPICE 등을 고찰한다.

보안공학방법론(security engineering)은 과학적이고 공학적인 기법을 활용하여 정보보증에 근거를 두고, 정보보안 정책을 시스템 규격으로 개발하고, 정보보호시스템의 보안 설계를 최적화하고, 효과적으로 정보보호시스템을 개발하기 위한 일련의 통합된 활동이다[김종기 외 3인, 2001; GISA, 1995; DoD, 1985; M. Eloff, 2000]. 보안공학은 다음과 같은 목표를 가진다. 첫째, 조직과 관련된 보안 위험을 식별한다. 둘째, 식별한 위험을 대처할 수 있는 적절한 보안 대책을 수립한다. 셋째, 보안 대책의 정확성과 효과성에 대해서 보증 근거를 확립한다. 넷째, 시스템이나 운영에 있어서 수용 가능한 위험을 허용함에 따라 위험의 수용 여부를 결정한다.

보안공학은 <그림 1>과 같이 전체 시스템의 개발 프로세스를 위험관리 프로세스, 공학 프로세스 및 보증 프로세스 등 3개 분야의 기본 프로세스로 구분할 수 있다. 이러한 기본 프로세스는 서로 독립적일 수 없지만, 분리하여 고려할 수 있다[김종기 외 3인, 2001; M. Eloff, 2000]. 위험관리 프로세스는 개발된 제품이나 서비스에 내재한 위험을 식별하고 우선순위를 부여한다[GISA, 1995]. 공학 프로세스는 식별된 위험을 대처하기 위해서 보안대책을 수립한다. 마지막으로 보증 프로세스는 보안대책에 대한 근거를 제시하고, 이 근거를 보안공학 관련자에게 전달한다. 보안공학의 목표는 세 가지 프로세스를 걸쳐서 성취된다[E. C., 1992].



〈그림 1〉 보안공학 프로세스

SSE-CMM은 정보보호시스템의 개발조직의 프로세스를 평가한다는 점에서 정보시스템의 운영 조직의 보안관리 적절성을 평가하는 보안관리체계 평가방법론과 차이가 존재한다[R. Hefner 외 1인, 1997; J. Herbsleb 외 4인, 1994]. SSE-CMM은 최종적인 정보보호시스템의 품질 관리에서 개발 프로세스를 품질 관리 대상으로 삼는다는 점에서 CMM과 동일한 근거를 두고 있다. ISO 9000은 품질에 대해서 합격/불합격의 판단을 내리고 있다. 그러나 CMM은 다단계의 품질 등급으로 구분하고 있으며, SSE-CMM도 CMM의 기본적인 품질 등급을 수용하고 있다.

SSE-CMM은 정보보호시스템과 서비스의 품질, 가용성을 제고하기 위하여 카네기멜론 대학의 소프트웨어 공학연구소 주관으로 보안공학 실무를 평가하기 위해 개발되었고, 다음 사항을 다룬다. 첫째, 개발, 운영, 유지보수 그리고 폐기를 포함한 정보보호시스템 생명주기 전반, 둘째, 관리, 조직 및 공학 활동을 포함하는 조직 전체, 셋째, 시스템, 소프트웨어, 하드웨어, 인적 요소, 시험 공학, 시스템 관리, 운영 및 유지보수와 같은 다른 분야와의 동시적인 상호작용, 넷째, 획득, 시스템 관리, 인증, 인정 및 평가 기

관을 포함한 다른 조직과의 상호작용 등이다.

SSE-CMM은 첫째, 공학 조직에서 보안공학 실무를 평가하고 개선을 정의하는 도구로서, 둘째, 정보보호시스템 보증의 한 요소로서 조직의 능력 수준을 확인하는 평가 도구로서, 셋째, 고객이 공급자의 보안공학 능력을 평가하기 위한 표준의 역할을 수행할 목적으로 사용되도록 개발되었다.

안전하고 신뢰성 있는 정보보호시스템을 생산하고 운영하기 위해서는 이전의 작업에서 획득한 프로세스가 향후에도 적용될 수 있도록 특정 활동과 절차가 정교하고 반복적으로 수행되어야 한다. 지속적으로 적용하기 위해서는 보안공학 실무의 이해와 향상에 필요한 메커니즘이 필요하다. 보안 공학의 지속적인 적용, 보안공학의 서비스의 품질과 가용성 제고, 정보보호시스템의 설치비용을 감소하기 위해 SSE-CMM이 개발되었다.

SPICE는 소프트웨어 개발 프로세스를 평가하는데 사용되는 프레임워크를 일련의 문서들로 기술하였다. 조직은 소프트웨어 생산에 필요한 각 단계에 문서를 적용할 수 있으며 계획(Planning), 관리(Managing), 모니터링(Monitoring)등의 각 단계를 평가할 수 있는 기준을 제공한다[T. Finne, 2000].

SPICE의 기본 목표는 개발 프로세스 개선 및 능력 수준의 판정이다. 21개의 개발 프로세스들이 시스템 이론을 바탕으로 설정된 평가범위에 똑같이 적용되는 것이 아니므로 평가범위에 따라 프로세스를 개별적으로 적용하고 평가한다. SPICE는 프로세스 차원과 능력차원의 2차원 구조를 가지고 있다. 프로세스 차원은 개발 프로세스들로 이루어졌으며, 능력차원은 각 프로세스 능력을 결정짓는 프로세스 속성에 관한 내용으로 구성되어 있다. 그러나, 프로세스와 프로세스 속성만으로는 능력수준의 세부 설명이 불충분하기 때문에 신뢰성 있고 일관성 있게 프로세스 능력을 평가할 수 없다. 따라서 이런 문제를 해결하기 위한 프로세스 목적 및 프로세스 속성은 이해 가능한 프로세스 수행 및 능력의 지표(indicators)들로 구성된다. 만약 한 프로세스에 해당되는 지표를 객관적이고 가시적으로 제시할 수 있다면 그 프로세스는 목적을 달성한 것으로 평가될 수 있다.

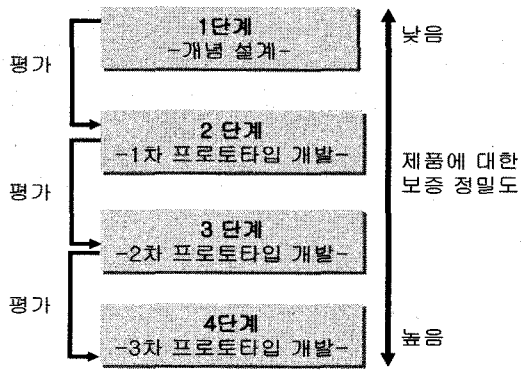
SPICE와 CMM과의 가장 큰 차이는 SPICE는 CMM의 성숙도 수준과 같은 특정 개선 방법론을 피하면서 프로세스 능력을 측정하는 방법을 개발하는 것이다. 이러한 목적에서 SPICE에서 선정된 방법은 개별 프로세스의 구현과 제도화를 측정하는 것이다. 반면에 CMM의 성숙도 수준은 개별 프로세스가 아니라 조직 전체의 성숙도를 측정하는 것이다.

3. 프로세스기반의 ISEM 방법론

정보보호시스템의 평가는 제품의 기능 및 보증을 평가하는 제품평가와 개발과정에 대한 적절한 품질을 확인하는 프로세스 평가로 나눌 수 있다. 정보보호시스템의 품질 보증수단으로 사용되는 제품에 대한 평가는 방법론은 개발 프로세스 평가방법론에 비해 고품질의 보증성을 얻을 수 있는 대신에 평가과정에서 고비용이 소요되고 상당한 기간이 필요하다는 점이 문제가 될 수 있다[2, 4]. 개발 프로세스에 대한 평가방법론은 프로세스에 대한 적절한 품질보증이 이루어짐으로써 제품 평가방법론보다 저비용과 짧은 기간이 소요된다는 장점이 있다.

본 장은 보안제품 평가방법론과 개발 프로세스 평가방법론이 갖고 있는 단점을 상호 보완하여 적정 수준의 비용과 품질을 고려하는 보안공학적 개념의 정보보호시스템 개발 평가에 관한 방법론(ISEM : High Secure Engineering Me-

thodology)을 제시한다. ISEM 방법론은 높은 신뢰성을 요구하는 정보보호시스템의 개발에 필요한 프로세스 보증 접근법 및 제품 보증 접근법의 장점을 채택하고 있다. ISEM 방법론은 정보보호시스템 개발 및 평가비용의 절감과 품질 향상을 위하여 제품 평가방법론과 개발 프로세스 평가방법론을 상호 보완한 개념을 적용하고 있다. ISEM은 <그림 2>에서와 같이 개념 설계 및 프로토타입 개발 단계 등 4단계로 구성된다.



〈그림 2〉 ISEM 4단계 구성도

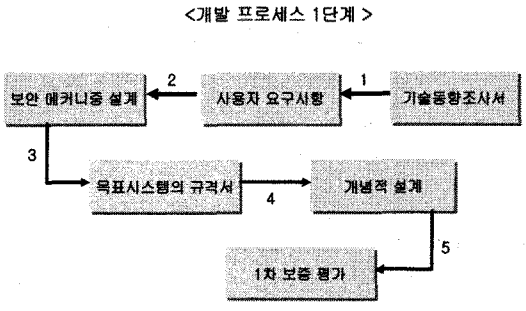
ISEM과 개발 프로세스 중심의 보안공학방법론과의 차이점은 제품 보증 수준의 정밀도(granularity level)이다. 기존의 개발 프로세스 중심의 보안공학방법론은 한 조직 안에서는 제품 보증에 있어서 동일한 수준의 정밀도를 가지고 있다. 반면에 CC, ITSEC 등과 같은 제품 평가 방법론은 등급에 따라 보증 정밀도가 달라진다. ISEM 방법론은 다단계의 프로세스를 거치는 동안 정밀도의 수준이 높아진다. 즉, 1단계에서 4단계로 프로세스를 진행하면서 정밀도의 수준이 높아진다. CC, TCSEC, ITSEC 등에 포함되어 있는 등급이라는 개념은 ISEM에서는 단계라는 개념에 포함되어 있다. 제품 중심의 보안공학방법론은 높은 등급일수록 높은 보증수준을 요구하는 것과 같이, ISEM 방법론에서는 1단계에서 4단계로 올라갈수록 보증 수준에 있어 높은 정밀도를 요구한다. CC 접근법과 ISEM의 근본적인 차이는 CC 접근법은 정형화된 보안공학방법론으로 개발대상의 특성을 고려하지 않는 측면이 있고, ISEM은 개발 대상의 특성에 따라 유연하게 보안공학방법론을 적용할 수 있다.

정보보호시스템의 신뢰성은 문서의 형태로 보증될 수 있으며, ISEM 방법론은 CC, TCSEC 등 제품 중심의 보안공학 방법론에 비해 보증 수준이 낮다. ISEM 방법론에서는 개발자와 평가자가 제품 개발 및 평가에 필요한 최소한의 문서를 작성토록 설계되어 있다.

ISEM 방법론에서는 개발자가 모든 정보보호시스템을 개발하는데 4단계의 전 과정을 거치는 것이 아니며, 시스템이 요구하는 신뢰성의 수준에 따라 개발 프로세스 단계가 결정된다. 개발자는 높은 신뢰성이 요구되는 정보보호시스템을 개발하는 경우에는 4단계 프로세스를 거쳐야 하지만, 낮은 신뢰성이 요구되면 2단계 또는 3단계의 프로세스만을 수행한다.

3.1 개발 프로세스 1단계

1단계에서 개발자는 개념적인 수준에서 정보보호시스템을 설계하며 설계의 신뢰성을 보증해야 한다. ISEM 방법론의 1단계는 <그림 3>과 같이 개발프로세스, 보증 평가로 구성된다.



〈그림 3〉 개발 프로세스 1단계

개발 프로세스 1단계에서 개발자가 수행해야 할 활동은 다음과 같다

1) 정보보호시스템의 최신 기술동향을 조사한다. 2) 사용자 요구사항, 보안환경 등을 분석한다. 3) 보안 메커니즘을 설계한다. 4) 목표 시스템을 규격화한다. 5) 정보보호시스템을 개념적으로 설계한다.

개발자는 목표 시스템(개발하고자 하는 정보보호시스템)의 최신 기술동향을 파악하여 반영해야 하며, 사용자의 요구사항과 보안환경을 분석해야 한다. 이와 같은 조사와 분석을 바탕으로 암호 알고리즘, 보안 프로토콜 등 보안 메카니즘을 설계하고, 목표 시스템의 기술 규격서를 정의해야 한다. 목표 시스템의 기술 규격서에는 위험 분석, 사용자 요구사항, 기능요구사항, 보증요구사항 등을 포함해야 한다.

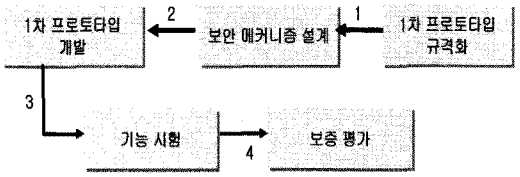
개발자는 형상 관리를 위해 시스템을 하위 시스템(sub-system) 단위로 서술해야 한다. 제품의 보증을 위해 개발자는 개발 프로세스 1단계의 활동을 문서화해야 한다. 개발자가 작성해야 할 문서는 1) 기술 동향 조사서, 2) 사용자요구사항분석서, 3) 보안 메커니즘 설계서, 4) 목표 시스템의 규격서, 5) 정보보호시스템의 개념 설계서, 6) 형상관리서 등이 있다.

1단계에서 정보보호시스템의 보증 정밀도는 낮다. 1단계에서는 개발자가 사용자요구사항 분석서, 규격서, 개념설계서 등을 자세히 서술할 필요가 없기 때문이다. 그러나, 개발자는 보안 메커니즘 설계, 형상 관리에 대한 사항을 자세하게 서술해야 한다. 개발 활동이 종료된 후 평가자는 개발 프로세스의 준수 여부, 개념적 설계의 신뢰성, 형상 관리의 완전성 등을 평가해야 한다. 평가자는 평가기간과 비용을 줄이기 위하여 체크리스트 및 인터뷰 방법을 사용하여 개발 프로세스 준수 여부를 평가해야 한다. 개발 프로세스 1단계에서 평가자는 보안 메커니즘과 형상 관리를 중심으로 정보보호시스템을 평가해야 한다. 보안 메커니즘은 높은 신뢰성을 요구하는 정보보호시스템 개발시 가장 중요한 기능이다.

3.2 개발 프로세스 2단계

ISEM 방법론의 2단계 개발 프로세스에서는 개발자는 1차 프로토타입을 개발하고, 평가자는 개발된 1차 프로토타입을 평가한다. <그림 4>에서 보는 것과 같이 개발자는 개념적 설계를 1차 프로토타입에 반영해야 한다. 1차 프로토타입이 개발된 후, 평가자는 보안 메커니즘과 1차 프로토타입의 구현 정확성을 검증해야 한다.

<개발 프로세스 2단계>



〈그림 4〉 개발 프로세스 2단계

ISEM의 개발 프로세스 2단계는 다음과 같다. 1) 1차 프로토타입의 규격을 서술한다. 2) 1차 프로토타입에 반영할 보안 메커니즘을 설계한다. 3) 1차 프로토타입을 개발한다. 4) 정보보호시스템의 기능을 시험한다.

개발 프로세스 2단계에서 중요한 활동은 1차 프로토타입에 반영할 정보보호 메커니즘을 구현하는 것이다. 2차 프로토타입의 개발을 위하여 개발자는 정형화 방법(formal method)을 사용하여 보안 메커니즘을 설계해야 하고 수학적인 방법으로 완전성을 검증할 수 있어야 한다. 이 활동을 통해 보안 메커니즘의 취약성과 관련된 기능의 검증이 이루어진다.

1차 프로토타입의 보증을 위해서 개발자는 1) 1차 프로토타입의 규격서, 2) 보안 메커니즘 설계서, 3) 기능 시험 결과서, 4) 정보보호시스템의 개념 설계서, 5) 형상관리서 등을 개발해야 한다.

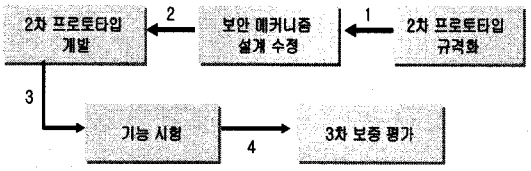
개발자가 프로세스 3단계에서 개발하는 2차 프로토타입의 보증 정밀도는 2단계에서 개발한 1차 프로토타입의 정밀도보다 높다. 개발자는 정형화된 방법(formal method)을 사용하여 1차 프로토타입의 규격서, 보안 메커니즘 설계서 등을 서술해야 한다. 특히, 보안 메커니즘 설계서는 정보보호 프로토콜의 동작 관점에서 1단계에서 이루어진 보증 평가 결과를 반영해야 한다. 2단계가 요구하는 보증 정밀도 수준은 1단계보다 높지만, 개발자가 서술해야 하는 문서는 CC에서 요구하는 문서에 비해 간단하다.

2단계에서 평가자는 1차 프로토타입과 보증 간의 일치 여부를 중점적으로 검증해야 한다. 평가자는 신뢰성과 무결성을 검증하기 위해서는 개발자가 제출한 문서를 평가해야 하고, 아울러 독립성 시험을 실시하여 보안 메커니즘과 기능 시험 결과를 검증해야 한다. 기존의 보안 공학방법론과 달리 ISEM 방법론에서는 평가자가 보안 메커니즘과 기능 시험에 중점을 두고 평가할 것을 요구하고 있다.

3.3 개발 프로세스 3단계

개발 프로세스 3단계에서 개발자는 2차 프로토타입을 개발하고, 평가자는 2차 프로토타입을 평가한다. <그림 5>와 같이, 3단계는 2단계의 개발 프로세스와 유사하다. 2차 프로토타입이 목표 시스템에 좀 더 근접하게 만들기 위하여, 개발자는 보안 메커니즘을 수정하고, 1차 프로토타입의 전체 기능을 개선해야 한다.

< 개발 프로세스 3단계>



〈그림 5〉 개발 프로세스 3단계

ISEM의 개발 프로세스 3단계는 다음과 같다. 1) 2차 프로토타입의 규격을 상세하게 서술한다. 2) 2차 프로토타입에 적용할 보안 메커니즘을 수정한다. 3) 2차 프로토타입을 개발한다. 4) 정보보호시스템의 전체 기능을 시험한다. 3단계에서 개발자는 정보보호시스템의 보안 메커니즘과 전체 기능을 확정해야 한다. 경우에 따라서 2차 프로토타입이 목표 시스템으로 확정될 수 있으며, 개발자는 2차 프로토타입을 목표 시스템으로 완료할 수 있다.

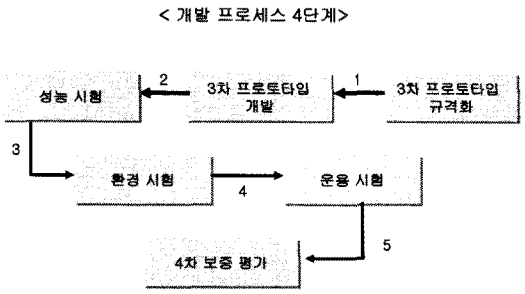
2차 프로토타입 보증을 위하여 개발자는 1) 2차 프로토타입 규격서, 2) 보안 메커니즘 설계서, 3) 기능 시험 결과서, 4) 정보보호시스템 상세 설계서, 5) 형상관리서 등을 작성해야 한다.

개발 프로세스의 2단계와 3단계 차이는 제품의 보증 정밀도 수준만이 다르다. 3단계에서 개발자는 목표 시스템에 대한 상세 규격서와 상세 설계서를 작성해야 한다. 2차 프로토타입의 보증 수준을 높이기 위해서 개발자는 보안 메커니즘과 기능의 정확성을 평가하기 위한 정량적 기준을 제시해야 한다. 평가자는 2차 프로토타입의 보안 메커니즘과 전체 기능에 대한 완전성을 검증해야 한다. 3단계에서 목표 시스템의 규격화 수준은 증가되지만, 개발 프로세스에 소요되는 비용과 기간은 2단계에서 소요되는 것과 유사하다.

3.4 개발 프로세스 4단계

개발 프로세스 4단계에서 개발자는 3차 프로

토타입을 개발하고, 평가자는 3차 프로토타입을 평가한다. 3차 프로토타입은 개발자가 의도한 최종적인 목표 시스템이며, 4단계에서 수행될 개발 프로세스는 <그림 6>과 같다. 4단계는 다음과 같은 활동을 포함한다. 1) 3차 프로토타입에 대한 규격을 기술한다. 2) 3차 프로토타입을 개발한다. 3) 성능 시험을 실시한다. 4) 환경 시험을 실시한다. 5) 운용 시험을 실시한다. 4단계에서는 정보보호시스템이 사용될 환경에서 3차 프로토타입의 운용 시험에 초점을 둔다. 운용 시험의 결과를 바탕으로 3차 프로토타입의 확정 여부가 결정된다.



〈그림 6〉 개발 프로세스 4단계

3차 프로토타입의 보증을 위해 개발자는 1) 3차 프로토타입 규격서, 2) 성능시험 결과서, 3) 환경시험 결과서, 4) 운용시험 결과서, 5) 형상관리서 문서 등을 작성해야 한다.

3차 프로토타입의 완전성을 보증하기 위해서, 개발자는 3차 프로토타입의 규격서에 만족하는지 여부를 확인해야 하며 이에 필요한 성능 시험, 환경시험, 운용 시험 등을 수행해야 한다. 성능시험, 환경시험, 운용시험시 필요한 정량적인 기준도 함께 제시해야 한다. 개발자는 3차 프로토타입의 시험 결과를 문서에 상세히 서술해야 하며, 4단계에서는 시험 결과서를 중점적으로 기술해야 한다. 평가자는 전반적인 시험 결과와 보증 사이의 일관성을 검증해야 한다. 4단계 종료 후 정보보호시스템의보증 수준이 결정되고, 모든 보증 문서가 완료되어야 한다. 정보보호시스템에 대한 모든 보증은 각 단계에서 문서 형태로 완료된다.

4. ISEM 방법론과 CC 적용 비교 분석

ISEM 방법론은 개발 프로세스 접근법의 장점과 보증 중심의 접근법의 장점을 결합한 개발 방법론이다. 따라서 ISEM 방법론의 효과성의 입증을 위해서는 실증 데이터를 사용하여 품질 및 비용의 관점에서 보증중심의 개발 방법론과 ISEM 방법론을 비교 분석할 필요가 있다. 본 논문은 대표적인 보증 중심의 개발방법론인 CC와 ISEM 방법론을 가상사설망(VPN : Virtual Private Network)시스템의 개발에 적용하고, 품질 및 비용의 관점에서 ISEM 방법론의 유효성을 검증하고자 한다.

ISEM 방법론의 유효성 검증을 위해서 본 논문은 개발비용과 품질 향상이라는 상반되는 목적 사이에는 트레이드오프(tradeoff)가 존재함을 인식하고, 트레이드오프를 해결하는 방식의 접근법을 채용한다. 품질과 비용간의 트레이드오프의 문제 해결을 위해 다양한 방식이 제안되고 있다[29].

본 논문은 품질 손실(quality loss)을 비용으로 환산시켜, 개발비용과 품질 손실의 합을 총 비용으로 산출한다. 품질 손실은 시스템의 성능이 최종 목표 범위에서 벗어날수록 증가하고, 높은 품질을 확보하기 위해서는 초기 설계 단계의 개선이 매우 중요하다. 그러나, 품질 손실을 낮추기 위해서는 많은 시간과 노력이 소요되어 개발비용이 더 높아 진다. 최근 제품 품질의 중요성이 강조됨에 따라 품질 손실이 증가하면 시스템의 성능이 떨어지고 사용자 만족도를 감소시켜 이윤이 낮아지는 결과를 가져온다. 따라서

최근의 연구는 품질 손실을 비용 개념으로 환산하고 있다[29].

본 논문은 정보보호시스템 개발에 따른 총 비용을 품질 손실 비용과 개발비용의 합으로 가정하고, ISEM 방법론과 CC 기준 적용시 발생되는 총비용을 비교하는 방식을 채택한다. 정보보호시스템의 개발에 소요되는 모든 시간, 비용 및 난이도는 보증요구사항에 전적으로 반영되며, 보증요구사항 개발에 소요되는 시간, 비용 및 난이도는 인력투입량(man/day)으로 측정할 수 있다고 가정하고, 인력투입량을 관찰하였다. 모든 개발과정에 소요되는 노력이 보증요구사항으로 반영될 수 있다는 가정은 다음과 같다. 정보보호시스템의 개발에 소요되는 비용은 크게 프로세스 설계 및 개발 등의 비용으로 구성된다. CC 기준은 특정한 개발 프로세스를 요구하지 않고, 프로세스 설계 및 개발 과정의 모든 사항을 보증요구사항으로 표현할 것을 요구한다. 따라서 모든 개발 과정에 소요되는 비용이 보증요구사항으로 반영된다고 하여도 무리가 없을 것으로 판단된다. ISEM 방법론의 경우에 있어서도 프로세스 설계 및 개발 등의 비용이 보증요구사항에 반영된다. 본 논문은 ISEM 방법론 및 CC를 이용하여 가상사설망 시스템을 개발하고, 개발과정의 실제 관찰 값을 개발비용 산정에 필요한 입력 값으로 사용하였다.

4.1 ISEM 방법론과 CC 기준의 품질 및 비용 분석법

본 논문이 제안한 ISEM 방법론과 CC의 접근법을 사용한 가상사설망 개발에 소요되는 개발비용은 다음과 같이 산출할 수 있다.

$$Cost_{ISEM} = \sum_{\forall i} D_i M_{ISEM_i} UC \quad (1)$$

식 (1)에서 D_i는 개별 보증요구사항 개발 난이도를 나타내고, M_{ISEM_i}는 개별 보증요구사항의 개발에 투입된 노력량, 즉 투입된 인력을 의미하며, UC는 투입된 인력된 단위당 비용을 나타낸다. D_i 산출하기 위하여 전문가 그룹을 구성하여 <표 1>과 같이 5점 척도의 난이도를 측정하였다.

ISEM 방법론을 이용하여 개발한 가상사설망 시스템의 품질 손실 비용은 다음과 같이 환산할 수 있다.

$$QL_{ISEM} = \sum_{\forall i} D_i W_{ISEM_i} M_{ISEM_i} UC \quad (2)$$

W_{ISME_i}는 ISEM 방법론의 개별 보증요구사항을 비교하여 품질의 손실이 발생할 경우, 품질 손실의 정도를 가중치(weight)로 나타낸 값이다.

〈표 1〉 보증요구사항의 개발 난이도 척도

보증요구사항 개발 난이도 기준	매우 쉬움	다소 쉬움	평이함	다소 어려움	매우 어려움
척도	1	2	3	4	5

〈표 2〉 보증요구사항의 품질 손실 척도

산출기준	품질손실 없음	품질손실 약간있음	품질손실 있음	품질손실 다소있음	품질손실 매우있음
척도	0	1	2	3	4

W_i를 산정하는 방식은 <표 2>과 같이 [0, 4]로 적용하였다.

식 (1)과 식 (2)를 이용하여 ISEM 방법론을 사용한 가상사설망 시스템의 총 개발비용을 산출하면 다음과 같다.

$$TC_{ISEM} = QL_{ISEM} + Cost_{ISEM} \quad (3)$$

CC를 사용한 가상사설망 시스템의 개발에 필요한 비용을 산출하면 다음과 같다.

$$Cost_{CC} = \sum_{\forall i} D_i M_{CC_i} UC \quad (4)$$

M_{cc_i}는 CC를 이용하여 가상사설망 시스템 개발시에 요구되는 개별 보증요구사항의 개발에 투입되는 인력을 의미한다. CC를 이용하여 개발한 가상사설망의 품질 손실을 비용으로 환산하면 다음과 같다.

$$QL_{CC} = \sum_{\forall i} D_i W_{CC_i} M_{CC_i} UC \quad (5)$$

W_{cc_i}는 ISEM 방법론의 보증요구사항과 비교할 때 발생할 수 있는 품질 손실을 의미하며, 품질 손실 정도를 가중치로 환산하는 방법은 <표 3>과 같이 [0, 4]로 적용하였다. 식 (4)과 식 (5)를 이용하여 CC를 이용한 가상사설망의 개발에 소요된 총비용을 산출하면 다음과 같다.

$$TC_{CC} = QL_{CC} + Cost_{CC} \quad (6)$$

4.2 ISEM 방법론과 CC 기준의 품질 및 비용 비교

위에서 제시된 품질 및 비용 접근법을 사용하여 A社의 가상사설망 시스템의 품질 및 비용을 비교하였다. <표 3>는 가상사설망 시스템 개발에 사용된 ISEM 방법론 및 CC 접근법간의 보증요구사항을 비교한 것이다. 보증요구사항의 난이도의 평가는 CC 보증요구사항과 ISEM 개발방법론을 동시에 경험한 보안엔지니어 10명이 참여하였다.

<표 4>는 가상사설망의 보증요구사항 개발과정에서 산출된 인력투입량을 나타내고 있으며, 난이도는 개발 및 평가 전문가 그룹에 의뢰하여 산출한 결과이며, ISEM 방법론과 CC 기준의 보증요구사항의 난이도는 동일하다.

〈표 3〉 ISEM 방법론과 CC의 보증요구사항 비교

ISEM 방법론 보증요구사항	CC 보증요구사항
기술동향 조사서	
사용자요구조건 분석서	보안목표명세서
목표시스템 규격서 1차 프로토타입 규격서 2차 프로토타입 규격서 3차 프로토타입 규격서	기능명세서
개념설계서(1단계) 개념설계서(2단계)	기본설계서
보안메커니즘 설계서(1단계) 보안메커니즘 설계서(2단계) 보안메커니즘 설계서(3단계) 정보보호시스템 상세설계서	상세설계서
기능시험 결과서(2단계) 기능시험 결과서(3단계) 성능시험 결과서(4단계) 환경시험 결과서(4단계) 운용시험 결과서(4단계)	시험서
	모듈시험서
형상관리서(2, 3, 4단계)	형상관리문서
	생명주기지원
	취약성 및 오용분석서

ISEM 방법론 보증요구사항과 CC 접근법의 보증요구사항의 man/day가 차이가 나는 근본

〈표 4〉 ISEM 방법론과 CC의 보증요구사항 난이도 및 인력 비교

ISEM 방법론 보증요구사항	난이도	인 력 (man/day)	인 력 (man/day)	난이도	CC 보증요구사항
기술동향조사서	3	8			
사용자요구조건 분석서	4	7	108	4	보안목표명세서
목표시스템 규격서 1차 프로토타입 규격서 2차 프로토타입 규격서 3차 프로토타입 규격서	3 3 3 3	12 11 92 24	103	3	기능명세서
개념설계서(1단계) 개념설계서(2단계)	4 4	8 26	218	4	기본설계서
보안메커니즘 설계서(1단계) 보안메커니즘 설계서(2단계) 보안메커니즘 설계서(3단계)	5 5 5	5 50 72	121	5	상세설계서 (보안메카니즘)
정보보호시스템 상세설계서	4	304	745	4	상세설계서
기능시험결과서(2단계) 기능시험결과서(3단계) 성능시험결과서(4단계) 환경시험결과서(4단계) 운용시험결과서(4단계)	3 3 4 4 4	2 282 51 136 25	506	3	시험서
			1048	3	모듈시험서
형상관리서(2, 3, 4단계)	4	23	26	4	형상관리문서
			42	1	생명주기지원
			50	2	취약성 및 오용분석서

적인 이유는 엔지니어링의 주안점에서 발생한다. ISEM은 규격서를 정형화에 주안점을 두는 반면에 CC 접근법은 개념적 설계와 시험에 주안점을 두는 엔지니어링 방식이다.

〈표 5〉 CC 접근법의 개발비용

(단위 : 천원)

CC 보증요구사항	개발 난이도	인 력	비 용
보안목표명세서	4	108	37,152
기능명세서	3	103	26,574
기본설계서	4	218	74,992
상세설계서(보안메카니즘)	5	121	52,030
상세설계서	4	745	256,280
시험서	3	506	130,548
모듈시험서	3	1048	270,384
형상관리문서	4	26	8,944
생명주기지원	1	42	3,612
취약성 및 오용분석서	2	50	8,600
총 비용			869,116

〈표 6〉 ISEM 방법론의 품질 손실 비용

(단위 : 천원)

ISEM 방법론 보증요구사항	난이도	인 력	품질손실	비 용
기술동향조사서	3	8	0	0
사용자요구조건분석서	4	7	1	2,408
목표시스템 규격서	3	12	0	0
1차 프로토타입 규격서	3	11	0	
2차 프로토타입 규격서	3	92	0	
3차 프로토타입 규격서	3	24	0	
개념설계서(1단계)	4	8	2	5,504
개념설계서(2단계)	4	46	1	15,824
보안메커니즘 설계서(1단계)	5	5	0	0
보안메커니즘 설계서(2단계)	5	50	0	
보안메커니즘 설계서(3단계)	5	72	0	
정보보호시스템 상세설계서	4	304	3	313,728
기능시험결과서(2단계)	3	2	0	0
기능시험결과서(3단계)	3	282	0	
성능시험결과서(4단계)	4	51	0	
환경시험결과서(4단계)	4	136	0	
운용시험결과서(4단계)	4	25	0	
형상관리서(2, 3, 4단계)	4	23	0	0
모듈시험서	1	1048	4	90,128
생명주기지원	1	42	4	8,944
취약성 및 오용분석서	2	50	4	3,569
총 비용				620,020

ISEM 방법론 및 CC 접근법의 개발비용은 식 (1)과 식 (4)에 의해서 각각 산출될 수 있다. 여기서 단위당 개발비용은 소프트웨어 대가 산정 기준의 중급기술자 하루 비용인 86,000원으로 가정하였다. <표 5>은 ISEM 방법론을 적용한 가상사설망 시스템의 개발비용을 나타내고 있다. <표 6>은 CC 접근법을 적용한 가상사설망 시스템 개발비용을 나타내고 있다. 개발비용은 개발단계에서 투입된 비용을 각 단계별로 추적하여 산출하였다.

<표 6>은 식 (2)를 이용하여 ISEM 방법론이 CC 접근법과 비교할 때 발생하는 품질 손실비용을 산출한 결과이다. 품질 손실은 ISEM 방법론의 보증요구사항과 CC 기준의 보증요구사항을 비교하여 5점 0등간척도를 이용하여 손실 정도를 판단하였다. ISEM 방법론이 제공하지 않은 CC 기준의 보증요구사항에 대해서는 '품질 손실이 매우 있다'고 판단하고, CC 기준의 보증요구사항 개발에 소요되는 비용을 기회비용으로 간주하였다. <표 7>는 식 (5)에 따라 CC 접근법이 ISEM 방법론과 비교할 때 발생하는 품질 손실 비용이다.

식 (3)과 식 (6)에 따라 ISEM 방법론과 CC 접근법의 개발비용과 손실 비용을 합한 총비용을 구하면 <표 8>과 같다.

<표 7>에서 보는 것과 같이 가상사설망 시스

〈표 7〉 CC 접근법의 품질 손실 비용

(단위 : 천원)

CC 보증요구사항	난이도	인 력	품질손실	비 용
기술동향분석서	3	16	4	8,256
보안목표명세서	4	215	0	
기능명세서	3	205	2	53,148
기본설계서	4	435	0	0
상세설계서(보안메커니즘)	5	242	1	52,030
상세설계서	4	1489	0	0
시험서	3	1011	1	130,548
모듈시험서	3	2096	0	0
형상관리문서	4	52	0	0
생명주기지원	1	83	0	0
취약성 및 오용분석서	2	100	0	0
총 비용				243,982

템 개발시 ISEM 방법론과 CC 접근법과 비교할 때, ISEM 방법론에 소요되는 총 비용이 약 15% 정도 저렴하다. 따라서, ISEM 방법론은 CC 접근법보다 품질과 비용 면에서 효과적이라고 할 수 있다. 다만, ISEM 방법론은 CC 접근법과 달리, 프로세스를

설계하고, 운영하는 데 추가 비용이 소요되므로 이러한 비용을 고려하면 실제 15% 보다 많은 비용 절감이 나타날 수 있다. 그러나, ISEM 방법론에서 품질 손실이 집중적으로 발생하는 상세설계서에 대한 품질 손실을 줄이면 전체 품질 손실의 비용은 상당히 개선될 수 있을 것으로 판단된다.

위의 논의에서 다소 문제가 발생할 수 있는 점은 품질 손실의 측정 부분이다. 품질 손실이 보증요구사항이 보증요구사항 단위로 발생한다고 가정하고 있다는 점이다. 정보보호시스템의 기능성, 보안성, 유지 보수성 등의 기준을 수립한 후, 최초 목표로 하는 시스템의 품질과 실제로 개발하여 달성된 시스템 품질간의 차이에 대해 측정하여 품질손실 비용을 계산할 수 있다. 그러나, 이 방법은 시스템의 기능성, 유지 보수성 등과 관련된 모든 품질기준을 도출해야 하기 때문에 목표로 하는 품질과 실제 달성된 품질간의 차이를 측정하기가 쉽지 않다. 따라서 본 논문은 품질 손실의 측정을 보증요구사항에 한정하여 측정하였다.

〈표 8〉 ISEM 방법론과 CC 접근법의 총비용 비교

(단위 : 천원)

개발 비용	품질손실 비용	총 비용
ISEM	346,408	620,020
CC	869,116	243,982

ISEM 방법론과 CC 접근법의 비교에서는 품질 손실이 보증요구사항의 개발 투입량만큼 발생한다고 가정하여 품질 손실을 측정하였다. 보증요구사항의 중심으로 품질 손실이 발생한다고 가정하고 측정하였다. 보증요구사항의 중심으로 품질 손실이 발생한다고 가정하고 인력투입량을 측정하였기 때문에 보증요구사항 개발에 투입되는 인력만큼 품질 손실이 발생하는 것은 합리적인 가정이라 할 수 있다.

ISEM 방법론은 프로세스 중심 보안공학방법론을 근간으로 프로세스 중심 보안공학방법론의 단점을 보완하기 위해서 제품보증중심의 보안공학방법론인 CC 방법론의 장점을 결합한 형태의 방법론이다. 따라서 본 연구에서는 ISEM 방법론과 프로세스 중심 보안공학방법론과의 비교를 통해서 ISEM 방법론의 우수성을 입증하는 검증을 시도하지 않았다. 그러나 연구의 엄밀성의 위해서는 프로세스 중심의 보안공학방법론과의 비교가 필요하지만, 관련 데이터를 획득할 수 없어서 비교를 할 수 없었다. ISEM 방법론과 프로세스 중심의 보안공학방법론과의 중요한 차이점은 다음과 같다.

첫째, ISEM 방법론은 개발 프로세스와 보증요구사항을 적절하게 결합함으로서 비용 효과적으로 정보보호시스템의 품질을 관리할 수 있는 반면에 프로세스 중심의 보안공학방법론은 비용을 고려하지 않고 프로세스 관리를 통해서 품질을 통제할 수 있다는 점이다. 둘째, ISEM 방법론에서는 제품 중심의 보안공학방법론과 같은 사용자 요구사항 및 보안기능 요구사항 등 보증요구사항을 반영하여 조직의 프로세스를 설계할 수 있다. 그러나 프로세스 중심의 보안공학방법론은 프로세스 최적화에 초점을 두고 조직의 특성에 맞는 프로세스 설계가 가능하지만 보증요구사항을 반영하지 못하고 있다. 셋째, ISEM 방법론은 정보보호시스템 개발상황이나 특성에 따라 개발 프로세스를 단계별로 운영할 수 있으나 프로세스 중심의 보안공학방법론은 정보보호시스템의 특성에 따라 프로세스 개발을 신축으로 운영할 수 없다는 점이다.

5. 결 론

본 논문에서는 높은 신뢰성을 요구하는 정보보호시스템을 개발하는 데 필요한 효과적인 보안공학방법론인 ISEM을 제안하였다. ISEM 방법론은 제품 보증 접근법과 개발 프로세스 보증 접근법의 장점을 수용한 개발방법론이다.

제품 보증 접근법은 높은 품질의 정보보호시스템을 개발할 수 있지만, 개발에 따른 많은 비용을 수반한다. 이에 반해, 개발 프로세스 보증 접근법은 제품 보증 접근법에 비해서 비용이 덜 소요되지만 품질이 다소 저하될 수 있다. 본 논문은 이와 같은 개발비용과 품질 향상이라는 상반되는 목적 사이에 발생하는 트레이드오프 문제를 해결하는 개발방법론을 제안하고 있다. 제시한 ISEM 방법론은 정보보호시스템 개발시 4단계의 프로세스 과정과 단계별 보증 요구사항을 준수하도록 설계되어 있다. 특히, ISEM 방법론은 정보보호시스템의 특성에 따라서 개발 프로세스를 단계별로 신축적으로 운영할 수 있다. ISEM 방법론은 높은 보증 수준과 비용 효과적인 개발 방식을 제시하고 있어 높은 신뢰성을 요구하는 정보보호시스템 개발에 적합하다. 즉, 높은 보증 수준을 유지하면서 비용면에서 효과적인 개발 프로세스를 제공하고 있다는 장점을 보여주고 있다.

ISEM 방법론의 유효성을 검증하기 위해서 개발 비용과 품질 손실비용의 개념을 적용하여 품질과 비용의 관점에서 대표적인 제품 보증 접근법인 CC와 비교하였다. 정보보호시스템 개발에 소요되는 시간, 비용이 보증요구사항에 반영된다고 가정하여 가상사설망 시스템 개발에 소요되는 총비용을 산출, ISEM 방법론의 유효성을 정량적으로 검증하였다.

본 논문이 제시하는 ISEM 방법론은 개발 프로세스 중심의 접근법과 제품 중심의 접근법의 장점을 결합한 정보보호시스템 개발방법론으로서 높은 신뢰성을 요구하는 정보보호시스템을 비용 효과적으로 개발하는 방법론으로 적합하며, 향후 ISEM 방법론을 정보보호시스템은 물

론 정보시스템 개발에도 적용할 수 있도록 연구 발전시킬 필요가 있다.

국내에서는 정보보호시스템 개발시에 기존의 소프트웨어 개발 방법론을 사용하고 있는 실정이다. 이러한 이유는 정보보호시스템 개발의 특수성을 인식하지 못하고 있으며, 관련 프로젝트의 규모도 커지 않기 때문이다. 국내에는 많은 숫자의 정보보호업체가 존재하고 있지만 체계적인 정보보호방법론을 적용한 프로젝트 사례가 거의 발표되지 않고 있으며, 정보보호시스템 개발의 난맥이 더욱 깊어지고 있다. 따라서 본 논문이 제시하는 방법론은 국내의 정보보호업체가 활용할 수 있는 중요한 참조모델로 활용될 수 있다.

참 고 문 헌

[1] 김종기, 이철원, 이동호, 박춘식, "시스템 보안공학 능력 성숙도 모델 고찰", *정보보호학회지*, 제11권 제6호, 2001.

[2] 한국정보보호진흥원, "정보보호시스템 평가 인증 가이드", 2004.

[3] Anderson, R., "Why information Security Is Hard(An Economic Perspective)", Proceeding of 17th Annual Computer Security Applications Conference, 2001.

[4] Avusoglu, H., Mishra, B. and Raghunathan, S., "A Model for Evaluating IT Security Investments", *Communication of ACM*, Vol. 24, No. 7, 2004.

[5] Barnard, L. and Soms, R., "A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls", *Computer and Security*, Vol. 19, No. 2, 2000, pp. 185-194.

[6] Baskerville, R., "The Developmental Duality of Information Systems Security", *Journal of Management Informations*, Vol. 4, No. 1, 1992, pp. 1-12.

[7] British Standard Institute, BS 7799 : Code of Practice for Information Security Management(CoP), PD0003.

[8] Brink, D., A Guide to Determining Return on Investment for e-Security, RSA Security Inc., 2001.

[9] COBIT, Framework, Information Systems Audit and Control Association(ISACA), 1998, 2nd Edition.

[10] CSE, Canadian Handbook on Information Technology Security, Communications Security Establishment, Government of Canada, 1998.

[11] GISA, IT Baseline Protection Manual (ITBPM), BSI, Germany, 1995.

[12] Godrdon, L. and Loeb, M., "The Economics of Information Security Investment", *ACM Transactions on Information and System Security*, Vol. 5, No. 4, 2002, pp. 438-457.

[13] Software Engineering Institute, Carnegie Mellon Univ. : SSE-CMM Appraisal Method, V.2.0, 1999.

[14] Department of Defense, Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1985.

[15] European Commission, Information Technology Security Evaluation Criteria(ITSEC), 1992.

[16] Eloff, M. and Solms, S. H., "Information Security Management, An Hierachical Framework for Various Approaches", *Computers and Security*, Vol. 19, No. 3, 2000, pp. 243-256.

[17] Eloff, M. and Solms, S. H., "Information Security Management, An Approach to Combine Process Certification And Product Evaluation", *Computers and Security*, Vol. 19, No. 8, 2000, pp. 698-709.

[18] Finne, T., "Information Systems Risk Management : Key Concepts and Business Process", *Computer and Security*, Vol. 19, No. 3, 2000, pp. 234-240.

[19] Fung, A. R. W., Farn, K. J., and Lin, A. C., "A Study on the Certification of the Information Security Management Systems", *Computer Standards and Interfaces*, Vol. 25, No. 5, 2003, pp. 447-461.

[20] Gentile, F., Giuri, L., Guida, F., Montolivo, E., and Volpe, M., "Security Evaluation in Information Technology Standards", *Computers and Security*, Vol. 13, No. 8, 1994, pp. 647-650.

[21] Hankcock, B., "From the Editior", Computer and Security, Vol. 19, No. 1, 2000, pp. 2-5.

[22] Hefner, R. and Monroe, W., "System Security Engineering Capability Mutulrity Model", Proceedings of Conference on Software Process Improvement, 1997.

[23] Herbsleb, J., Carton, A., Rozum, J., Siegel, J., and Zubrow, D., "Benefits of CMM-Based Software Process Improvement : Initial Results", CMU/SEI-94-TR-013, Pittsburgh, Pa., Software Engineering Institute, Carnegie Mellon University, 1994.

[24] Higginbothan, M. D., Maley, J., Milheizler, A. J., and Suskie, B. J., "Integrating Information SE with Systems Engineering with System Engineering Tools", *Proceedings of 7th IEEE International Workshops on Enabling Technologies : Infrastructure for Collaborative Enterprises*, 1998, pp. 320-326.

[25] http://www.sse-cmm.org/Papers/SSECMM/v2Final.pdf, SSE-CMM Project, Systems SE Capability Maturity Model Version 2.0 April, 1999.

[26] Horman, T. P., Wrona, K., and Holtmann, S., "Evaluation of Certification Validation Mechanisms", *Computer Communications*, Vol. 29, No. 3, 2006.

[27] ISO/IEC(a), Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and General Model, Version 2.1, 1999.

[28] ISO/IEC(b), Common Criteria for Information Technology Security Evaluation Part 2 : Security Functional Requirements Version 2.1, 1999.

[29] ISO/IEC(c), Common Criteria for Information Technology Security Evaluation Part 3 : Security Assurance Requirements Version 2.1, 1999.

[30] ISO/IEC, Common Methodology for Information Technology Security Evaluation Part 2 : Evaluation Methodology Version 1.0, 1999.

[31] ISO/IEC TR13335, Guideline for the Management of IT Security, ISO/IEC JTC1 SC27/WG1, 1996.

[32] Konard, M. D., Paulk, M. C., Graydon, A. W., "An Overview of SPICE's Model for Process Management", Proceedings of the fifth International Conference on Software Quality, 1995, pp. 291-301.

[33] John Leach, "TBSE-an Engineering Approach to the Design of Accurate and Reliable Security Systems", *Computers and Security*, Vol. 23, No. 2004, pp. 63-76.

[34] John Leach, "Security Engineering and Security RoI", *Computers and Security*, Vol. 22, No. 6, 2003, pp. 482-486.

[35] Lee, S. Y., Jung, T. M., and Choi, M., "An Empirical Study of Quality and Cost Based Security Engineering", *Lecture Notes in Computer Science,* Vol. 3903, 2006.

[36] Lee, Y., Lee, J., and Lee, Z., "Integrating Software Lifecycle Process Standards with Security Engineering", *Computers and Security*, Vol. 21, No. 4, 2002, pp. 345-355.

[37] Mark, P., Curtis, B., Chrissis, M., and Weber, C., "Capability Maturity Model for Software version 1.1", CMU/SEI-93-TR-24, Pittsburgh, Pa, Software Engineering Institute, Carnegie Mellon University, 1993.

[38] Massacci, F., Prest, M., and Zannone, N., "Using a Security Requriements Engineering Methodology in Practice : The Compliance with the Italian Data Protection Legislation", *Computer Standard and Interfaces* Vol. 27, No. 5, 2005, pp. 445-455.

[39] Mecuri, RT., "Analyzing Security Costs", *Communication of ACM*, Vol. 46, No. 6, 2003.

[40] Mouratidis, H., Gorgini, P., and Manson, G., "When Security Meets Software Engineering : a Case of Modelling Secure Information Systems", *Information Systems*, Vol. 30, No. 8, 2005, pp. 609-629.

[41] NIST, An Introduction to Computer Security : The NIST Handbook, National Institute of Standards and Technology, U.S., Department of Commerce, 1995.

[42] Pfleeger, S. L., "A Framework for Security Requirements", *Computers and Security*, Vol. 10, No. 6, 1991, pp. 515-523.

[43] Piazzal, C., Pivato, E., and Rossi, S., "CoPS-Checker of Persistent Security", *Lecture Notes in Computer Science*, Vol. 2988, 2004, pp. 93-107.

[44] Pijl, G., Swinkels, G., and Verijdt, J., "ISO 9000 versus CMM : Standardization and Certification of IS Development", *Information and Management*, Vol. 32, 1997, pp. 267-274.

[45] A.Purse, S., "Improving the ROI of the Security Management Process", *Computers and Security*, Vol. 23, No. 7, 2004, pp. 542-546.

[46] Purse, S. A., "Balancing Opportunity and Risk", *Information Security Bulletin*, Vol. 9, No. 4, 2004.

[47] Purse, S. A., A Practical Guide to Managing Information Security, Artech House, 2004.

[48] Qadeer, S. and Rehof, J., "Context-Bounded Model Checking of Concurrent Software", *Lecture Notes in Computer Science*, Vol. 3440, 2005, pp. 93-107.

[49] Robinson, J., "Computer Security Evaluation : Developments in the European ITSEC Programme", *Computers and Security*, Vol. 11, No. 6, 1992, pp. 518-524.

[50] Shin, S. M., Cho, B. R., "Trade-off Studies on Process Parameters : A Robust Design Perspective", *Proceedings of the 11th Industrial Engineering Research Confer-*

ence, Orlando, FL, 2000.

[51] Stallings, W., Cryptography and Network Security : Principles and Practice, Second Ed., Prentice-Hall, Englewood Cliffs, NJ., 1999.

[52] Steve, M. and Carol, B., "CMM Appraisal Framework, Version 1.0, "CMU/SEI-95-TR-001, Pittsburgh, Pa., Software Engineering Institute, Carnegie Mellon University, 1995.

[53] Strous, L., "Security Evaluation Criteria", *Computers and Security*, Vol. 13, No. 5, 1994, pp. 379-384.

[54] Schneier, B., Applied Cryptography, John Wiley and Sons INC., New York, 1993.

[55] Watt, S., "Computer Security Manager", Elsevier Science Publishers Ltd., England, 1989.

[56] Wood, C. C. and Snow, K., "ISO 9000 and information, Security", *Computer and Security*, Vol. 14, No. 4, 1995, pp. 287-288.

[57] Wood, C. C. and Snow, K., "ISO 9000 and Information Security", *Computers and Security*, Vol. 14, 1995, pp. 287-288.

[58] Wood, C. C., "Shifting IS Security Responsibility from User Organization to Vendor/Publisher Organizations", *Computer and Security*, Vol. 14, No. 4, 1995, pp. 283-284.

[59] Wood, C. C., How to Achieve a Clear Definition of Responsibilities for Information Security, DATAPRO, Information Security, 1993.

[60] Zuccato, A., "Holistic Security Requirement Engineering for Electronic Commerce", *Computers and Security*, Vol. 23, No. 1, 2004, pp. 63-76.

저자소개

최 명 길

중앙대학교 상경학부 경영학전공 조교수로 재직 중이다. 부산대학교 경영학사(1993), 경영학석사(1995), 한국과학기술원 공학박사(2004)를 취득하였다. 국방과학연구소 연구원(1995~2000) 및 한국전자통신연구원(ETRI) 국가보안기술연구소 선임연구원(2000~2005)을 거쳐, 인제대학교 조교수(2005~2007)로 재직했다. 관심분야는 정보시스템 보안성평가, 홈네트워크 보안, 정보보호정책 및 관리 등이다.

◈ 이 논문은 2009년 03월 27일 접수하여 1차 수정을 거쳐 2009년 06월 15일 게재확정되었습니다.