情 報 保 護 學 會 誌
第 11 券 第 6 號, 2001. 12

시스템 보안공학 능력 성숙도 모델 (SSE-CMM) 고찰

김 종 기*, 이 철 원**, 이 동 호***, 박 춘 식**

요 약

정보보안 분야가 성숙해짐에 따라 다양한 평가방법론들이 개발되어 적용되고 있다. 그러한 방법론들 중에서 본고에서는 품질 보증의 수단으로써 정보보안 제품/시스템의 개발기관의 보안공학 수행 능력을 평가하기 위한 SSE-CMM에 대하여 살펴본다. SSE-CMM의 개념적 기초가 되는 보안공학에 대하여 먼저 살펴보고, 보안공학 수행 능력의 수준을 평가하기 위한 평가 기준의 체계와 구성과 함께, SSE-CMM을 이용하여 평가를 수행하기 위한 평가방법론을 구체적으로 제시하고 있는 SSAM에 대하여도 살펴본다.

SSE-CMM이 근거하고 있는 보안공학은 효과적인 정보보안을 도모하기 위한 개념적 틀이라는 점을 몇 가지 정보보안관리 지침들과의 비교를 통하여 논의하였다. SSE-CMM은 현재 ISO 표준으로 상정되어 표준화가 진행 중이다. 정보보안 분야의 여러 평가방법론들과 더불어 보다 다양한 관점에서 정보보안의 효과성을 보증해주는 도구로 활용될 것이다.

Ⅰ. 서 론

사회 전반의 정보화가 급진전됨에 따라 정보보안에 대한 관심과 필요성이 급격히 증대되고 있다. 정보보안을 효과적으로 유지하기 위해서는 신뢰성 있는 보안통제가 정보시스템에 구현되어 있어야 한다. 정보시스템의 보안성 평가는 크게 제품/시스템의 기능 및 보증성에 대한 평가와 보안관리체계의 적합성에 대한 평가로 구분되어 발전되어 왔다. 제품에 대한 평가방법론으로는 TCSEC, ITSEC, CC 등의 기준들이 널리 알려져 있으며, 보안관리체계의 평가방법론으로 ISO의 GMITS와 BS7799가 주목을 받고 있다.

SSE-CMM(System Security Engineering -Capability Maturity Model)은 보안성 평가에 있어서 위의 두 접근법과는 상이한 개념에 기초하고 있다. 품질 보증의 수단으로서 개발 과정의 최종 산출물인 제품에 대한 평가는 그 의도의 적절성과 합목적성에도 불구하고 평가 과정에서의 과도한 비용이 소요되고 상당한 기간이 필요하다는 점이 문제가 되고 있다. 제품의 생산 공정에 대한 적절한 품질 보증이 이루어짐으로써 최종 산출물의 평가에 소요되는 노력을 상당히 감소할 수 있다는 점에서 개발 공정에 대한 평가가 의의를 가진다. 따라서, 제품에 대한 평가와 개발 공정에 대한 평가는 상호보완적이라고 할 수 있다. SSE-CMM은 보안제품/시스템의 개발조직이 주요 적용대상이라는 점에서 정보시스템을 운영하는 조직의 보안관리의 적절성을 평가하는 보안관리체계 평가방법론과 차이가 있다.

제품의 생산 공정에 대한 평가로는 정보시스템 일반에 대한 평가 모델로서 ISO 9000-3 "소프트웨어 개발 공급과 유지보수를 위한 지침(Guidelines for the development supply and maintenance of software)", SPICE, CMM(Capability Maturity Model) 등이 대표적이다. 최종 산출물에 대한 품질의 통제에서 생산 공정의 품질의 통제로 초점을 옮긴다는 품질 관리의 기본적인 철학의 변화에 있어서는 CMM과 동일한 근거를 두고 있지만, ISO 9000은 합격/불합격이라는 이분법적인 단계를 전제로 하고 있는데 반하여 CMM은 다단계의 품질 수준을 구분하고 있다[1][2]. SSE-CMM도 CMM의 기본적인 품질 통제 개념을 그대로 수용하고 있다.

본고에서는 SSE-CMM에 대한 이해를 증진시키기 위하여 SSE-CMM이 기반하고 있는 보안공학과

* 부산대학교 경영학부 조교수 (jkkim1@hyowon.pusan.ac.kr)
** 국가보안기술연구소
*** 부산대학교 경영학부 박사과정

함께 SSE-CMM의 구성과 내용에 대하여 설명하고, SSE-CMM을 이용한 평가 방법인 SSAM을 살펴보며, 또한 보안관리 지침들과의 비교를 통하여 SSE-CMM의 유용성을 논의한다.

Ⅱ. 보안공학과 SSE-CMM

1. 보안공학의 개념과 목표

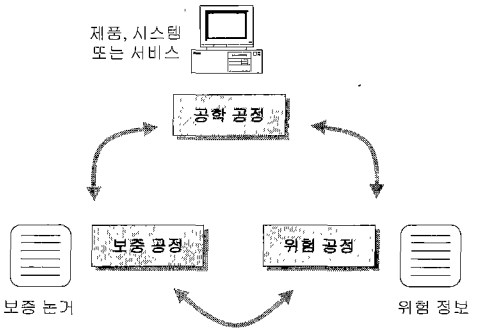
시스템 보안공학은 과학적이고 공학적인 기법을 적절히 적용하여 효과성과 보증의 필요성에 준거하여 보안 정책을 시스템 명세로 전환하고, 관련된 보안 매개변수를 통합하고, 전체적인 시스템 보안 설계를 최적화하도록 모든 환경적, 운영적 및 기술적 보안 원칙의 적합성을 보장하며, 시스템 보안공학 노력을 전체적인 시스템공학 노력에 통합하도록 하는 일련의 통합된 활동이다[3]. SSE-CMM은 보안공학 공정 모델(security engineering process model)의 하나로서 SE(Systems Engineering) CMM을 근간으로 설계되었으며, 시스템 보안공학의 특수한 원칙을 다루기 위하여 SE-CMM의 실무들을 정보보안의 영역에서 해석하고, 보안공학 고유의 새로운 공정 분야나 실무를 식별하였다. 공정 능력과 구체적인 영역을 분리하는 모델의 구조는 SE-CMM의 구분과 흡사하다.

보안공학의 목표는 다음과 같다.

- 기업에 관련된 보안 위험에 대한 이해를 얻는다.
- 식별된 위험에 적절한 균형 있는 보안 필요성을 정립한다.
- 프로젝트에 활용되는 다른 분야의 활동과 시스템 형상 또는 운영 명세로 통합되도록 보안 필요성을 보안 지침으로 변환한다.
- 보안 메커니즘의 정확성과 효과성에 있어서 신뢰나 보증을 확립한다.
- 시스템이나 운영에 있어서 잔여 보안 취약성이 허용(즉, 수용 가능한 위험)됨에 따른 운영상의 영향을 결정한다.
- 모든 공학 분야와 전문 분야의 노력을 시스템의 신뢰성에 대한 이해로 통합한다.

2. 보안공학 공정

SSE-CMM은 보안공학을 아래의 그림 1과 같이 위험, 공학 및 보증의 세 가지 기본적인 분야로 나눈다. 이러한 분야들은 서로 독립적이라는 의미는 아니지만, 분리해서 고려할 수는 있다. 가장 단순한 수준에서 위험 공정은 개발된 제품이나 서비스에 내재한 위험을 식별하고 우선순위를 부여한다. 보안공학 공정은 위험에 의해서 제기된 문제에 대한 해결책을 결정하고 구현하기 위하여 다른 공학 분야와 함께 이루어진다. 마지막으로, 보증 공정은 보안 해결책에 대한 신뢰를 제시하고 이 신뢰를 고객에게 전달한다. 이러한 세 분야는 보안공학 공정이 위에서 설명한 목표를 달성하도록 함께 수행된다.



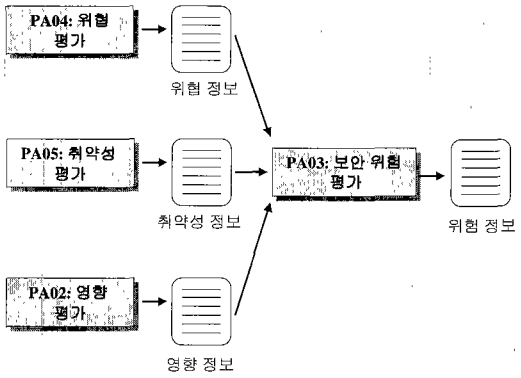
〔그림 1〕 보안공학 공정의 주요 분야

2.1 위험 공정

보안공학의 주요 목표는 위험을 감소시키는데 있다. 위험 평가는 아직 발생하지 않은 문제를 식별하는 공정이다. 위협과 취약성의 발생 가능성을 검토하고 바람직하지 않은 사건의 잠재적인 영향을 고려하여 위험을 평가한다. 그러한 발생 가능성과 관련된 것은 불확실성인데, 특정한 상황에 매우 의존적이다. 불확실성의 요소들에 관련된 예측의 정확성에 따라 그 요소들은 많은 불확실성을 가지기 때문에 보안의 계획 수립과 정당화는 매우 어려울 수 있다.

보안 사고는 위협, 취약성 및 영향의 세 가지 요소에 의해서 결정된다. 취약성은 위협에 의해서 이용될 수 있는 자산의 속성이며, 보안상의 약점을 의미한다. 취약성과 위협 모두 존재하지 않는다면 보안상 바람직하지 않은 사건은 발생하지 않을 것이며, 따라서 위험도 없다. 위험 관리는 위험을 평가하고 계량화하고, 조직에 대한 위험의 허용 가능한 수준을 결정하는 공정이다. 위험을 관리하는 것은 보안 관리에 중요한 부분이다.

위험은 보안대책을 구현하여 완화하는데, 위협, 취약성, 영향 또는 위험 그 자체를 대상으로 한다. 그러나, 모든 위험을 완화하거나 특정한 위험을 완전히 없애는 것은 불가능하다. 이것은 많은 부분에서 위험 완화 비용과 그에 관련된 불확실성 때문이다. 따라서, 약간의 잔여 위험을 항상 받아 들여야 한다. 불확실성이 많이 존재하는 경우에는 부정확한 특성으로 인하여 위험 수용이 매우 문제가 된다. SSE-CMM 공정 분야에는 그림 2와 같이 위협, 취약성, 영향 및 관련 위험을 분석하도록 보장하는 활동이 포함된다.



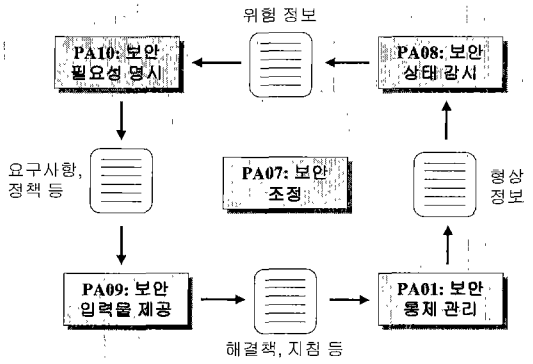
〔그림 2〕 보안 위험 공정

2.2 공학 공정

다른 공학 분야와 같이 보안공학은 개념, 설계, 구현, 시험, 배치, 운영, 유지보수, 및 폐기에 걸쳐서 이어지는 공정이다. 이러한 공정에 걸쳐서 보안 공학자는 시스템공학 팀의 다른 부분과 밀접하게 작업하여야 한다. SSE-CMM은 보안 공학자가 더 큰 팀의 일부이며 다른 분야의 기술자와 그들의 활동을 조정할 필요가 있다는 것을 강조한다. 이것은 보안이 더 큰 공정에 통합된 부분이며, 분리되고 동떨어진 활동이 아니라는 점을 확실히 한다.

위에서 설명한 위험 공정으로부터의 정보, 시스템 요구사항에 대한 다른 정보, 관련 법률, 정책을 이용하여 보안 필요성을 파악한다. 보안 필요성이 식별되면 구체적인 요구사항을 파악하고 추적한다.

보안 문제에 대하여 해결책을 만들어내는 공정에는 일반적으로 가능한 대안을 도출하고 가장 유망한 것을 결정하기 위한 평가가 관련된다.



〔그림 3〕 전체 공학 공정

이 활동과 나머지 공학 공정을 통합하는 것이 어려운 이유는 해결책이 보안 고려사항 단독으로만 선택될 수 없다는 점이다. 비용, 성과, 기술적 위험, 사용 편의성 등을 포함하여 광범위한 다른 고려사항들이 반드시 다루어져야 한다. 보편적으로는 이슈들을 재검토할 필요성을 최소화하도록 이러한 의사결정이 다루어져야 한다. 도출된 분석은 또한 보증 노력에 대한 중요한 기반을 형성한다.

수명 주기 후기에서 새로운 위험이 시스템을 운영이 불안전하지 않도록 하기 위하여, 인지된 위험에 관련되어 제품과 시스템이 적절히 구성되도록 보장하기 위하여 보안 공학자에게 요청한다.

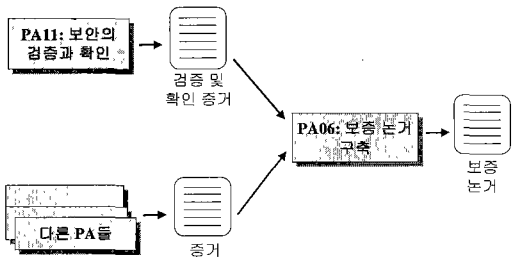
2.3 보증 공정

보증은 보안 필요성이 충족되었다는 확신의 정도로 정의된다[4]. 이것은 보안공학의 아주 중요한 결과물이다. 보증에는 많은 형태가 있다. SSE-CMM은 보안공학 공정으로부터의 결과물의 반복성에 대한 신뢰라는 한 가지 측면에 공헌한다. 성숙한 조직일수록 덜 성숙한 조직보다 동일한 결과를 반복할 가능성이 더 많다는 것이 이런 신뢰의 기반이다. 상이한 보증의 형태간의 상세한 관계는 지속적으로 연구되어야 한다.

보증이 보안과 관련된 위험에 대응하기 위하여 추가적인 통제를 부가하는 것은 아니지만, 구현된 통제가 예상되는 위험을 감소할 것이라는 확신을 제공한다.

보증은 보안대책이 의도된 데로 기능하리라는 확신으로 볼 수 있다. 이런 확신은 정확성과 효과성이라는 속성에서 유도된다. 정확성은 설계에 따라 보

안대책이 요구사항을 구현한다는 속성이다. 효과성은 보안대책이 고객의 보안 필요성을 적절히 충족하도록 보안을 제공하는 속성이다. 메커니즘의 강도도 역할을 하지만, 추구하는 보안과 보증의 수준에 의해서 조정된다.



[그림 4] 보증 공정

보증은 일반적으로 논거(argument)의 형태를 띤다. 논거에는 시스템의 속성에 대한 주장이 담겨 있으며, 주장은 증거에 의해서 뒷받침된다. 증거는 정상적인 보안공학 활동의 과정에서 개발되는 문서화의 형태를 자주 가진다.

SSE-CMM 활동 자체는 보증과 관련된 증거의 생산에 관련된다. 예를 들어, 공정 문서화는 지속적인 향상의 대상이 되는 잘 정의되고 성숙한 공학 공정에 따라서 개발되었다는 것을 나타낸다. 보안 검증 및 확인은 제품이나 시스템의 신뢰성을 구축하는데 많은 역할을 한다.

공정 분야 내에 포함된 많은 산출물 예는 증거에 도움이 되거나 증거의 일부분을 구성한다. 현대의 통계적 공정 통제는 제품을 생산하는데 사용된 공정에 초점을 맞춤으로써 더 높은 품질과 더 높은 보증 제품을 더 비용 효과적이고 반복적으로 생산할 수 있다는 것을 제시한다. 조직 실무의 성숙도는 공정에 영향을 미치고 공정에 기여한다.

Ⅲ. SSE-CMM의 개발 배경과 목적

1. SSE-CMM의 개발 배경

보안공학을 잘 정의되고 성숙한 분야로 발전시켜 정보보안 제품과 서비스의 품질과 비용, 가용성을 보다 향상시키고자 하는 목적으로 카네기 멜론 대학의 소프트웨어 공학연구소(SEI) 주관으로 40개 이상의 정부기관과 업체가 참여하는 SSE-CMM 프로젝트 그룹이 1995년 1월에 결성되었다. 1996년 10월에 모델 설명(Model Description) 문서 version 1.0이 제시되었고, 1997년 4월에 평가 방법(Appraisal Method) version 1.0이 발표되었으며, 1999년 4월에 모델과 평가 방법 version 2.0이 제안되었다.

고객과 공급자 모두는 보안 제품, 시스템 및 서비스를 향상시키는데 관심을 당연히 가지고 있다. 보안공학 분야에는 몇 가지 널리 수용되는 원칙들이 있기는 하지만 보안공학 실무들을 평가하기 위한 프레임워크로는 SSE-CMM이 최초로 개발되었다[5]. 현대의 통계적 공정 통제 방법론에서는 높은 품질의 제품은 그것을 생산하는 공정의 품질을 강조함으로써 보다 비용 효과적으로 생산할 수 있으며, 조직의 실무의 성숙도는 그러한 공정에 내재된다고 본다. 안전한 제품과 시스템의 개발에 필요한 시간과 비용이 증가하고 있음을 상기할 때 보다 효율적인 공정이 필요하다.

2. SSE-CMM의 범위와 대상

SSE-CMM은 보안공학 실무에 대한 표준적인 척도를 제공하기 위하여 개발되었으며, 다음의 사항들을 다룬다.

- 개발, 운영, 유지보수 그리고 폐기를 포함한 수명주기 전반
- 관리, 조직 및 공학 활동을 포함하는 조직 전체
- 시스템, 소프트웨어, 하드웨어, 인적 요소, 시험 공학, 시스템 관리, 운영 및 유지보수와 같은 다른 분야와의 동시적인 상호작용
- 획득, 시스템 관리, 인증, 인정 및 평가 기관을 포함한 다른 조직과의 상호작용

SSE-CMM과 평가 방법은 다음과 같이 사용되도록 개발되었다.

- 공학 조직에서 자신의 보안공학 실무를 평가하고 개선을 정의하는 도구
- 시스템 또는 제품의 보안 보증의 한 요소로서 조직 능력 기반의 신뢰를 확인하는 보안공학 평가 기관을 위한 기반 제공
- 고객이 공급자의 보안공학 능력을 평가하기 위한 표준적인 메커니즘

안전한 시스템과 신뢰성 있는 제품의 생산과 운영을 위해서는 이전의 작업에서 획득한 지식이 향후에도 적용되는 지속성, 프로젝트를 성공적으로 수행하도록 보장하는 방법이 반복적으로 사용되도록 하는

반복성, 개발자와 평가자 모두가 보다 효율적으로 작업할 수 있도록 지원하는 효율성, 보안 필요성이 다루어지고 있다는 확신을 가지는 보증과 같은 속성들이 요구된다. 이러한 목적들을 달성하기 위해서는 보안공학 실무를 이해하고 향상시키도록 조직들을 이끌어 가는 메커니즘이 필요하다. 이러한 요구를 충족시키기 위하여 안전한 시스템, 신뢰성 있는 제품, 그리고 보안공학 서비스의 품질과 가용성을 향상시키고 인도 비용을 줄이기 위한 목적으로 SSE-CMM이 개발되었다. SSE-CMM의 사용과 관련된 이해 당사자들에게 다음과 같은 효과들이 예상된다.

- 공학기관: 시스템 통합자, 응용 개발자, 제품 판매자 및 서비스 제공자가 포함되며, 반복적이고 예측 가능한 공정과 실무에 대하여 재작업을 줄임으로써 얻는 비용 절감, 계약자 선정에서 진정한 작업 수행 능력에 대한 신뢰, 그리고 조직의 자격(성숙도)과 능력 향상에 대한 집중화된 노력이 가능하다.
- 획득기관: 내외부의 원천에서 시스템, 제품 및 서비스를 획득하는 기관과 최종 사용자가 포함되며, 재사용 가능한 표준적인 제안요청서 용어와 평가 수단, 비자격 응찰자를 선택하는 위험(능력, 비용, 일정) 감소, 산업 표준에 근거한 일관된 평가로 인한 항의의 감소, 그리고 예측 가능하고 반복적인 제품이나 서비스의 신뢰 수준을 얻을 수 있다.
- 평가기관: 시스템 인증자, 제품 평가자 및 제품 분석자들이 포함되며, 시스템이나 제품의 변경과는 독립적으로 재사용 가능한 공정 평가 결과, 보안공학과 보안공학에 관련된 다른 분야와의 통합에 있어서의 신뢰를 얻을 수 있다.

3. 공정의 의미

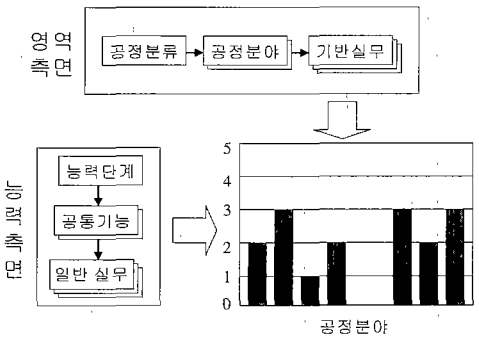
공정이란 주어진 목적을 달성하기 위하여 수행되는 단계의 순서이다. 공정은 어떤 최종 결과(즉, 제품, 시스템 또는 서비스)의 생산과 도출에 관련되는 작업, 지원 도구, 그리고 인력의 총체적인 시스템으로, SSE- CMM은 공정이 생산비용, 일정 및 품질을 결정하는 요소로 인식하여 공정을 향상시키기 위한 방법에 주목함으로써 품질관리의 새로운 흐름과 맥락을 같이 한다.

공정 능력은 조직의 잠재력을 지칭하며, 한 조직이 수행하리라고 기대되는 범위이며, 공정성과는 특정한 프로젝트의 실제 수행 결과를 측정한 것이다. 공정 성숙도라는 개념은 특정한 공정이 어느 정도로 명시적으로 정의되고, 관리되고, 측정되며, 통제되고, 효과적인지를 나타낸다. 공정 성숙도는 능력의 발전 가능성을 의미하며, 한 조직의 공정의 풍부성과 조직 전반에 걸쳐 얼마나 일관되게 적용되었는지를 나타낸다. CMM은 공학 기관을 임기응변적인 덜 조직화되고 덜 효과적인 상태에서 고도로 구조화되고 고도로 효과적인 상태로 발전시키기 위한 프레임워크이다. 모델을 사용함으로써 조직의 공정 능력을 향상시켜 통계적 공정 통제하의 공정으로 이끌 수 있다. CMM을 적용한 결과, 많은 소프트웨어 개발 기관들이 비용, 생산성, 일정, 그리고 품질에 대하여 바람직한 결과를 나타내고 있다고 연구되었다[6].

Ⅳ. SSE-CMM의 구성

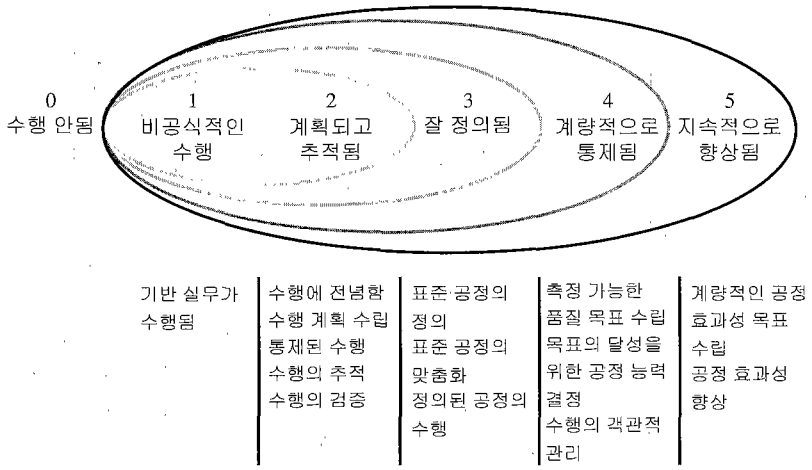
SSE-CMM은 영역(domain)과 능력(capability)이라는 두 측면으로 나누어진 일련의 실무(practice)들로 구성된다. 이러한 구조는 SE-CMM으로부터 채용하였는데, 영역 측면인 보안공학의 공정의 기본적인 특징으로부터 능력 측면인 보안공학 공정의 공정관리와 조직화 특징을 확연히 구분하기 때문에 SSE-CMM에 특히 적절한 것으로 생각된다.

그림 5에 나타난 바와 같이 SSE-CMM의 아키텍처는 각 공정분야별로 조직의 능력 수준을 표시하는 프로파일을 생성할 수 있는 메트릭스 구조로 되어있다.



〔그림 5〕 SSE-CMM의 아키텍처

SSE-CMM에서 설명하는 모든 공정이 조직 내의 특정한 그룹이나 역할에 의해서 반드시 수행되어야 하는 것을 의미하지 않는다. 또한, 최신의 최고



〔그림 6〕 SSE-CMM의 능력 단계

수준의 보안공학 기법이나 방법론이 사용되어야 하는 것도 아니다. 그러나 모델에서 설명하는 기본적인 보안 실무를 포함한 공정을 가져야만 한다. 조직은 어떠한 방식으로든 자신의 기업 목적을 충족할 수 있는 자체적인 공정과 조직 구조를 자유롭게 창출할 수 있다.

능력 측면은 전반적인 공정관리와 조직화 능력에 관련된 보편적인 실무들로 구성된다. SSE-CMM에서는 공정 능력을 능력 수준, 공통 특징, 그리고 일반 실무의 세 가지로 세분화한다. 능력 단계는 공정의 성숙도를 나타내며, 하나 이상의 공통 특징으로 구성되는데, 그림 6과 같이 여섯 단계로 나눈다. 각각의 공통 특징은 다수의 보편적인 실무들로 상세화된다.

- "비공식적으로 수행되는 (Performed Informally)" 수준 1은 기반 실무가 포함된 공정을 조직이나 프로젝트에서 수행하는지의 여부에 초점을 둔다. 이 수준은 "관리하기 전에 행하여야 한다"라는 문구로 특징 지워진다.
- "계획되고 추적되는 (Planned & Tracked)" 수준 2는 프로젝트 수준의 정의, 계획 수립, 그리고 수행 이슈에 초점을 둔다. 이 수준은 "조직 전반의 공정을 정의하기 전에 프로젝트에서 무슨 일이 일어나고 있는지 이해한다"라는 문구로 특징 지워진다.
- "잘 정의되는 (Well Defined)" 수준 3은 조직 수준에서 정의된 공정들로부터 엄격히 맞추어진 것에 초점을 둔다. 이 수준은 "조직 전반의 공정을 창출하기 위하여 프로젝트에서 학습한 최선의 것을 이용한다"라는 문구로 특징 지워진다.
- "계량적으로 통제되는 (Quantitatively Controlled)" 수준 4는 조직의 기업 목표에 연관된 측정에 초점을 둔다. 기본적인 프로젝트 척도를 빨리 수집하고 사용하기 시작하는 것이 중요하기는 하지만 더 높은 수준을 달성할 때까지는 조직 전체에 걸쳐서 측정과 데이터의 사용이 기대되지는 않는다. 수준은 "그것이 무엇인지 모르면 측정할 수 없다"와 "올바른 것을 측정할 때만 측정에 의한 관리가 의미가 있다"라는 문구로 특징 지워진다.
- "지속적으로 향상되는 (Continuously Improving)" 수준 5는 앞의 수준에서 보여진 모든 관리 실무의 향상으로부터 효력을 얻은 다음에 획득된 이득을 지속하는 문화적 변화를 강조한다. 이 수준은 "지속적인 향상을 위한 문화는 건전한 관리 실무의 기초, 정의된 공정, 그리고 측정 가능한 목표를 요구한다"라는 문구로 특징 지워진다.

영역 측면은 보안공학 고유의 기본적인 실무들로 구성되는데, 공정 분야(process area; PA)들로 그룹화된다. 평가에 있어서 이 측면은 조직이 어떤 보안공학 실무를 수행할지를 결정하는데 활용된다. 공정 분야는 보안공학, 프로젝트, 그리고 조직의 세 부문으로 나누어지는데, 모두 22개가 있다. 각 공정 분야는 다수의 기반 실무(base practice)로 구성된다. 공정 분야가 수명 주기 단계나 분야 순서로 나열되었다는 것을 나타내지 않기 위해서 알파벳 순서로 나열되어 있다.

보안공학 분야에는 모든 주요 분야를 포괄하는 11개의 공정 분야로 그룹화된 61개의 보안 기반 실

〔표 2〕 SSE-CMM의 프로젝트 및 조직 공정 분야

공정 분야	목 표
PA12-품질을 보장한다	· 공정 품질이 정의되고 측정됨 · 산출물의 기대 품질 수준이 달성됨
PA13-형상을 관리한다	· 산출물의 형상에 대한 통제가 이루어짐
PA14-프로젝트 위험을 관리한다	· 프로젝트의 위험이 식별되고 통제됨
PA15-기술적 노력을 감시하고 통제한다	· 기술적 노력이 감시되고 통제됨
PA16-기술적 노력을 계획한다	· 기술적 노력의 모든 측면이 계획됨
PA17-시스템공학 공정을 정의한다	· 시스템공학 공정의 표준이 정의됨
PA18-시스템공학 공정을 향상시킨다	· 시스템공학 공정의 표준의 향상을 위한 계획을 수립하고 구현함
PA19-제품 라인 발전을 관리한다	· 생산 라인이 궁극적인 목적을 향하여 발전함
PA20-시스템공학 지원 환경을 관리한다	· 시스템공학 지원환경이 공정의 효과성을 극대화함
PA21-기술과 지식을 지속적으로 제공한다	· 프로젝트와 조직 목적을 달성하는데 필요한 기술을 확보함
PA22-공급자와 조정한다	· 효과적인 공급자를 선정하고 활용함

무가 포함되어 있다. 기반 실무는 현존하는 광범위한 자료, 실무, 및 전문지식에서 수집되었다. 선택된 실무는 보안공학 커뮤니티에서 시험된 실무들로서 현존하는 최선의 실무들을 대표한다. 표 1은 보안공학에 관련된 공정 분야를 보여준다.

표 2는 프로젝트와 조직의 공정 분야를 보여주는

〔표 3〕 SSE-CMM의 보안공학 공정 분야

공정 분야	목 표
PA01-보안 통제를 관리한다	· 보안 통제가 적절히 구성되고 활용됨
PA02-영향을 평가한다	· 시스템에 미치는 영향을 식별하고 발생 가능성을 평가함
PA03-보안 위험을 평가한다	· 시스템이 운영되는 환경에 관련된 보안 위험을 이해함 · 정의된 방법론에 의거하여 위험의 우선순위를 부여함
PA04-위협을 평가한다	· 시스템의 보안에 위협을 초래하는 위협을 식별함
PA05-취약성을 평가한다	· 시스템의 보안 취약성을 이해함
PA06-보증 논거를 구축한다	· 산출물과 공정이 사용자의 보안 필요성이 충족됨을 보여주는 증거를 명확하게 제공함
PA07-보안을 조정한다	· 프로젝트 팀의 모든 구성원들이 업무를 수행하는데 필요한 보안공학 활동들을 인식하고 수행함 · 보안과 관련된 의사결정과 권고안들이 의사소통되고 조정됨
PA08-보안 상태를 감시한다	· 보안과 관련된 내외부 사건들이 탐지되고 추적됨 · 보안사고가 정책에 따라 처리됨 · 보안운영 상황에 대한 변화가 파악되고, 보안 목적에 따라 처리됨
PA09-보안 입력물을 제공한다	· 보안에 영향을 미치는 모든 시스템 문제가 검토되고, 보안 목표에 따라 해결됨 · 프로젝트 팀의 모든 구성원이 업무를 수행할 수 있도록 보안에 대하여 이해함 · 솔류션은 제공되는 보안 입력물을 반영함
PA10-보안 필요성을 명시한다	· 고객을 포함한 모든 이해관계자들 사이에 보안 필요성에 대한 공통된 이해를 가짐
PA11-보안을 검증하고 확인한다	· 솔류션이 보안 요구사항을 충족함 · 솔류션이 고객의 운영적 보안 필요성을 충족함

데, 이들은 SE-CMM으로부터 수용한 것이다.

Ⅳ. SSE-CMM 평가 방법

1. 평가 단계

SSE-CMM을 이용하여 평가를 수행하기 위한 방법론으로 SSAM (SSE-CMM Appraisal Method)[3]이 개발되었다. SSAM을 이용한 평가에는 그림 7과 같이 네 단계를 거친다.

1.1 계획 단계

계획 단계의 목적은 평가가 수행될 프레임워크를 수립할 뿐만 아니라 현장실사 단계를 위한 자원을 준비하는 것이다. 평가 후원자에 의하여 수립된 평가에 대한 목표를 충족하도록 평가의 한계와 목적을 정의하고 합의한다. 또한, 평가의 변수와 세부 사항을 문서화한 최종 평가 계획이 만들어지고 승인된다.

1.2 준비 단계

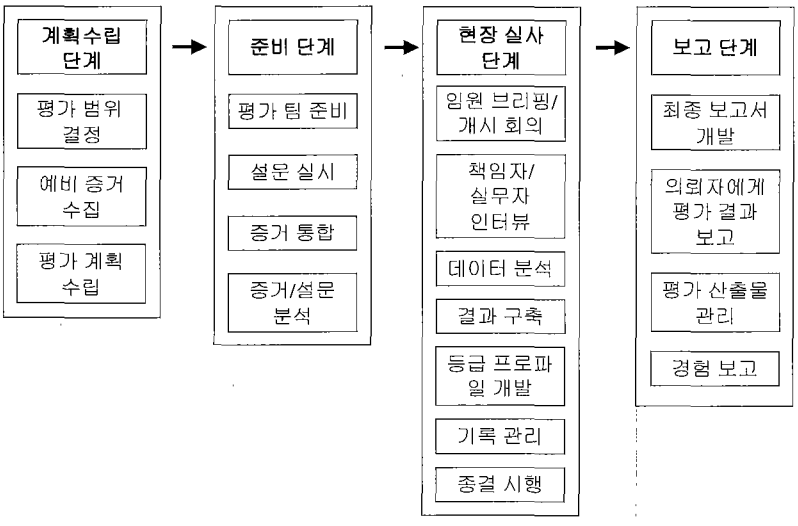
준비 단계의 목적은 현장실사 단계를 위한 평가팀을 준비하고, 설문지를 통하여 사전에 데이터를 수집하고 분석하는 것이다. 평가 팀에게 평가의 세부 사항을 숙지하게 한다. 또한, 설문을 수행하고 데이터를 수집하여 평가 개체에 대한 정보를 수집한다. 설문지에서 수집된 데이터를 분석하고, 뒷받침되는 증거를 수집한다. 이러한 분석으로부터 프로젝트 책임자와 실무자와의 인터뷰에서 사용될 질문들이 만들어진다.

1.3 현장실사 단계

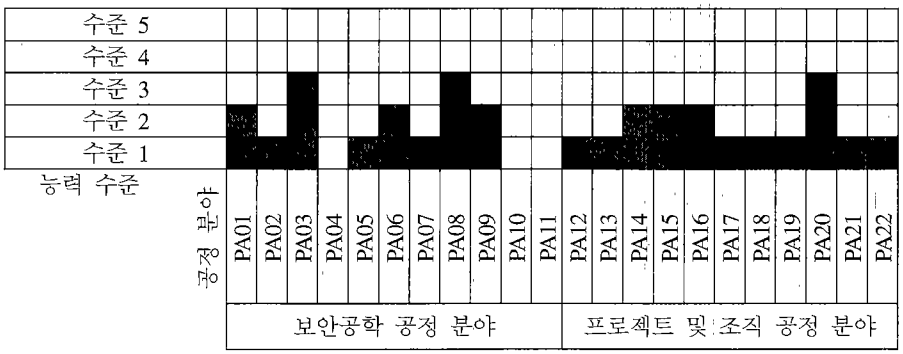
이 단계의 목적은 사전 데이터 분석의 결과를 조사하고, 평가 개체의 실무자에게 데이터 수집과 확인 절차에 참여할 기회를 제공하기 위한 것이다. 상위 경영층에게 평가 절차와 일정에 대하여 브리핑하며, 경영자는 평가 활동에 대한 배경을 설명한다. 평가 절차와 일정이 모든 평가 참여자에게 제시된다. 프로젝트 책임자와 실무자들을 인터뷰하고, 평가 결과를 대조한다. 예비 결과가 제안되며, 후속 질문이 제시된다. 평가 결과를 반영하기 위한 등급이 개발된다. 이 등급과 최종 조사 결과는 종료 회의에서 제시된다.

1.4 보고 단계

보고 단계의 목적은 현장 단계의 막바지에 시작된 데이터 분석을 매듭 짓고, 팀 조사 결과를 평가 후원자에게 제시하는데 있다. 추가적으로, 실무자들에게 향후의 향상을 위하여 평가 절차에 대한 의견을 제시하는 기회를 제공한다. 결과 보고서가 만들어지고 후원자에게 제시된다. 팀은 평가 현장에서 수집



〔그림 7〕 SSAM의 수행 절차



〔그림 8〕 공정 능력의 결정

한 모든 자료를 적절히 폐기하고 평가 절차에서 습득한 교훈에 대한 내부 보고서를 작성한다.

조직의 능력에 대한 평가는 해당 조직이 수행하였거나 수행하고 있는 프로젝트의 참여자에 대한 인터뷰와 인터뷰 결과에 대한 증거 자료의 수집을 기초로 이루어진다. SSAM 설명 문서에는 각 공정 분야별로 조직의 능력 수준을 평가하기 위하여, 인터뷰 대상자에 대한 상세한 설문지와 증거의 확보와 관리를 위한 데이터 추적지(Data Tracking Sheet; DTS)의 양식이 제시되어 있다.

2. 평가 결과의 표현

그림 8은 평가의 기본적인 결과를 보여준다. 0에서 5까지의 능력 수준은 각 공정 분야별로 결정되며, 단순한 막대 그림으로 표시된다. 평가의 실제 결과에는 이 요약 및 세부적인 조사 결과에서 각 분야에 대한 중요한 세부사항이 포함된다.

SSAM에서는 기반 실무의 100% 수행을 수준 1의 달성을 위한 요구사항으로 정의한다. 다른 모든 능력 수준은 이전 수준이 100% 달성되고 현 수준이 최소한 80% 달성되었을 때 부여된다. SSE-CMM 평가 방법은 능력 수준을 달성하기 위한 기준을 정의하고 있지만, 특정한 수준을 달성하는데 있어서 의뢰자가 부여한 중요성에 기초를 두고 기준을 재정의하기도 한다.

Ⅴ. SSE-CMM과 보안관리 지침의 연관성

정보보안 프로그램의 수립과 운영을 돕기 위하여 미국의 NIST 지침[7], 캐나다의 CSE 지침[8], 영국의 BS7799[9], ISO/IEC의 GMITS[10] 등과 같은 다수의 지침서들이 개발되었다. 보안 지침들 모두는 본질적으로는 동일한 주제를 다루고 있지만 각각의 문서는 개발된 국가의 적용 대상 조직과 환경에 맞추어 문화적, 법적, 제도적 특수성을 반영하여 다소 상이한 내용과 구성을 취하고 있다.

표 3에서 볼 수 있듯이 SSE-CMM에서 다루고 있는 공정 분야들이 다른 보안관리 지침에도 포함되어 있다. SSE-CMM과 보안관리 지침들과의 가장 큰 차이점은 활용 목적에 있다. 보안 지침 문서들과는 달리 SSE-CMM은 사용자가 보안 프로그램을 수립하는데 도움을 주거나 적절한 측면들이 고려되도록 확인하는데 있지 않다. 그러한 점들은 오히려 부수적인 측면이며, SSE-CMM의 주요 목적은 조직에 의해서 구현된 공정의 성숙도 수준을 평가하는데 있다. 따라서, 정보기술 보안 지침 문서들과 SSE-CMM은 상호보완적이다. SSE-CMM의 사용에 수반하여 보안 지침 문서를 활용함으로써 상당한 효과를 거둘 수 있을 것이다.

Ⅵ. 결 론

SSE-CMM은 현재 국제표준안으로 상정되어 ISO/IEC JTC1 SC27에서 표준화 작업을 진행하고 있으며, ISO 12207과 더불어 ISO 15504, ISO 13335와 같은 기존의 ISO 표준들과의 호환성과 연계성에 대한 수정이 반영된다면 국제표준으로 제정되는데 무리가 없을 것이다[11]. 정보시스템 보안 보증에 대한 다양한 접근법과 방법론들 가운데서 SSE-CMM은 정보보안시스템 개발기관의 공정에 대한 유일한 평가방법론으로서, CC와 같은 제품 중심의 접근법과

〔표 4〕 SSE-CMM과 정보보안 관리지침의 비교

SSE-CMM	GMITS	NIST 편람	BS7799
PA01-보안통제를 관리한다	17절, 후속 조치	10장, 직원/사용자 이슈 14장, 컴퓨터 지원 운영에서의 보안 고려사항	5절, 인적 보안 6절, 통신 및 운영 관리 8절, 시스템 개발 및 유지보수
PA02-영향을 평가한다	10절, 위험분석 전략 대안; GMITS 3부	7장, 컴퓨터 보안위협 관리	개요
PA03-보안위험을 평가한다	10절, 위험분석 전략 대안; GMITS 3부	7장, 컴퓨터 보안위협 관리	개요
PA04-위협을 평가한다	10절, 위험분석 전략 대안; GMITS 3부	7장, 컴퓨터 보안위협 관리 4장, 보편적인 위협	개요
PA05-취약성을 평가한다	10절, 위험분석 전략 대안; GMITS 3부	7장, 컴퓨터 보안위협 관리	개요
PA06-보증논거를 구축한다	14절, 보안대책 구현	9장, 보증	10절, 준거성
PA07-보안을 조정한다	13절, IT 보안 계획	6장, 컴퓨터 보안 프로그램 관리	2절, 보안 조직 6절, 통신 및 운영 관리
PA08-보안상태를 감시한다	17절, 후속 조치	18장, 감사 증적 12장, 컴퓨터 보안 사고 처리	10절, 준거성
PA09-보안 입력물을 제공한다	8절, IT 보안 정책 11절, IT 보안 권고안 12절, IT 시스템 보안 정책 13절, IT 보안 계획 15절, 보안 인식	5장, 컴퓨터 보안 정책 13장, 인식, 교육 및 훈련 15장, 물리적 및 환경적 보안	1절, 보안 정책 3절, 자산 분류 및 통제 5절, 물리적 및 환경적 보안
PA10-보안 필요성을 명시한다	8절, IT 보안 정책 11절, IT 보안 권고안 12절, IT 시스템 보안 정책 13절, IT 보안 계획	8장, 컴퓨터 시스템 수명주기에서의 보안 및 계획수립 11장, 비상사태 및 재해에 대한 준비 16장, 식별 및 인증 17장, 논리적 접근통제 19장, 암호	1절, 보안 정책 7절, 접근통제 8절, 시스템 개발 및 유지보수 9절, 업무 지속성 계획 수립
PA11-보안을 검증하고 확인한다	17절, 후속 조치 14절, 보안대책 구현	8장, 컴퓨터 시스템 수명주기에서의 보안 및 계획수립 18장, 감사 증적	10절, 준거성

BS7799 (ISO 17799-1)와 같은 보안관리 중심의 접근법과 더불어 정보보안의 평가에 있어서 중요한 평가접근법의 하나로 자리매김할 전망이다. 이상의 세 가지 방법론은 상호 보완적이며, 정보보안의 효과성을 극대화시키기 위한 고유의 역할을 할 것이다[12].

참 고 문 헌

〔1〕 G. Pijl, G. Swinkels and J. Verrijdt, "ISO 9000 versus CMM: Standardization and certification of IS development," *Information & Management*, Vol. 32, 1997, pp.267-274.

〔2〕 Wood, C. and K. Snow, "ISO 9000 and Information Security," *Computers & Security*, June 1995 (Vol. 14, No. 4) pp. 287-288.

〔3〕 CMU, *SSE-CMM Appraisal Method*, Version 2.0, Software Engineering Institute, Carnegie Melon Univ., April 1999.

〔4〕 J. William and G. Jelen, *A Framework for Reasoning about Assurance*, Arca Systems, 1998.

〔5〕 R. Hefner and W. Monroe, "System Security Engineering Capability Maturity Model," *Conference on Software Process Improvement*, 1997.

〔6〕 CMU, *System Security Engineering*

Capability Maturity Model, Model Description, Version 2.0, Software Engineering Institute, Carnegie Melon Univ., April 1999.

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

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

[9] BSI, *BS7799 - Code of Practice for Information Security Management*, British Standards Institute, 1999.

[10] ISO/IEC TR 13335, *Guidelines for the Management of IT Security*, ISO/IEC JTC 1/SC 27/WG 1, 1996.

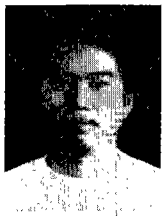
[11] ISO/IEC JTC1 SC27, DIS 21827, *Information Technology-System Security Engineering-Capability Maturity Model* (SSE-CMM), 2000. 10.

[12] M. Eloff and S. H. Solms, "Information Security Management: A Hierarchical Framework for Various Approaches," *Computers & Security*, Vol. 19, 2000, pp.243-256.

〈著者紹介〉

김 종 기(Jongki Kim)
정회원

1987년 : 부산대학교 경영학과 학사
1988년 : Arkansas State University, MBA
1992년 : Mississippi State University, Ph.D. in MIS
1993년 3월 ~ 1998년 12월 : 국방정보체계연구소 선임연구원
1999년 3월 ~ 현재 : 부산대학교 경영학부 조교수
관심분야 : 정보시스템 보안관리, 전자상거래, 프로젝트 관리

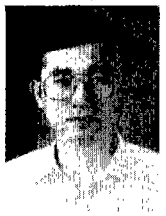


이 철 원(Cheol Won Lee)

1987년 : 충남대학교 수학과 (이학사)
1989년 : 중앙대학교 전자계산학과 (이학석사)
1989년 ~ 1996년 : 한국전자통신연구원 선임연구원
1996년 ~ 2000년 : 한국정보보호센터 선임연구원
2000년 ~ 현재 : ETRI 부설 국가보안기술연구소 팀장
관심분야 : 컴퓨터 및 네트워크 보안, 정보통신 기반보호, 정보보호시스템 평가기준

이 동 호(Dongho Lee)

1996년 : 부산대학교 경영학과 학사
1998년 : 부산대학교 경영학과 석사
1999년 5월 ~ 2000년 5월 : 부산대학교 경영경제 연구소 전임연구원
2001년 ~ 현재 : 부산대학교 경영학과 박사과정 재학중
관심분야 : 정보시스템 보안관리, GDSS, E-Biz와 전자상거래, 웹 데이터베이스 어플리케이션 개발/모델링



박 춘 식(Choon Sik Park)
종신회원

광운대학교 전자통신공학과 졸업 (학사)
한양대학교 대학원 전자통신공학과 (석사)
일본 동경공업대학 전기전자공학과 졸업(암호학 전공, 공학박사)
1989년 10월 ~ 1990년 9월 일본 동경공업대학 객원연구원
1989년 ~ 현재 ETRI 부설 국가보안기술연구소 책임연구원, 정보보증연구부장
1999년 ~ 현재 한국통신정보보호학회 편집(논문지)이사, 논문지 편집위원장
관심분야 : 암호이론, 이동통신보안, 정보전