情 報 保 護 學 會 誌
第 13 券 第 6 號, 2003. 12

프로세스 보증을 통한 제품 평가 효율성 향상 방안

임 종 인*, 김 태 훈**, 이 태 승**

요 약

IT 산업이 급속히 발전하면서 정보보호와 관련된 문제가 중요한 고려 사항으로 대두되고 있다. 이러한 문제 해결의 일환으로 정보보호제품에 대한 수요가 증가하고 있으며, 또한 이들 정보보호제품의 안전·신뢰성이 중요한 이슈로 부각되고 있다. 정보보호제품에 대한 보안성 평가가 이미 시행되고 있지만, 보안성 평가에는 비교적 많은 시간이 소요되므로 개발자가 평가 과정을 거쳐 적시에 제품을 시장에 출시하는 데에는 어려움이 따른다. 본 고에서는 정보보호제품 개발 프로세스를 공통평가기준에서 요구하는 수준으로 개선하도록 함으로써, 제품 평가 준비 및 평가에 소요되는 비용과 시간을 경감시키고 평가의 효율성을 향상시킬 수 있는 방안을 모색하여 보고자 한다.

Ⅰ. 서 론

불과 몇 년 전만 하여도 정보보호는 정부기관의 비밀 데이터를 보호하는 것 등에만 한정되는 것처럼 여겨졌으나, 현재는 금융 거래, 계약, 개인 정보, 인터넷 등에 관련된 광범위한 분야에서 중요한 개념으로 확대되고 있다. 이에 따라 개인 또는 조직의 중요한 정보를 보호하고 유지하기 위하여 침입차단시스템, 침입탐지시스템 등 정보보호제품 및 정보보호컨설팅 등 정보보호서비스에 대한 수요가 급증하고 있으며, 이와 함께 정보보호제품의 안전·신뢰성에 대한 평가 요구가 증가하고 있다.

최근 정보보호제품이 시장에 출시되는 경향은 두 가지로 나누어 볼 수 있다. 일정 기간에 걸쳐 비용을 지불하면서 평가단계를 거쳐 인증을 획득한 후 출시되는 제품과, 특별한 목적 및 필요성에 의하여 평가 단계를 거치지 않고 개발과 동시에 시장에 출시되는 제품이 있다. 평가를 받지 않은 제품은 평가인증을 획득한 제품과 비교하여 신뢰성 및 안정성, 보안성에 대한 보증을 제공하기 어려우므로, 정보보호제품을 채택하여 사용하고자 하는 회사 혹은 기관의 경우 평가를 통하여 인증을 획득한 제품에 대한 수요가 증가하고 있다.

최신 해킹 및 바이러스 등의 공격방법으로 인한 위협에 대처하기 위하여 신속한 정보보호제품의 개발 및 업그레이드가 요구되고 있으나, 평가과정에 소요되는 기간으로 인하여 평가 과정을 거쳐 필요로 하는 기능을 가진 신뢰성 있는 제품이 적시에 출시되지 못하는 경우가 종종 있으므로 최근의 위협에 적절하게 대응하지 못하는 경우가 발생할 수 있다.

공통평가기준에 의한 평가는 '평가보증등급(EAL, Evaluation Assurance Level)' 수준에 따른 보증요구사항 만족 여부를 검토하는 과정을 거쳐야 하므로 일정 기간의 평가 시간이 소요되고 있다. 또한 이러한 평가의 상당 부분이 실제 정보보호제품 개발 프로세스와 연관되어 있으므로, 제품 개발 프로세스를 공통평가기준에서 요구하는 수준으로 향상시키지 않고는 신속한 평가와 높은 보증등급의 획득을 기대하기 어렵게 되었다.

본 고에서는, 정보보호제품의 개발 단계에서부터 보안 공학 개념을 적용하여 공통평가기준에서 요구하고 있는 수준으로 개발 프로세스를 개선함으로써, 개발된 정보보호제품 자체의 신뢰성 향상뿐만 아니라 평가를 받기 위한 준비에 필요한 노력과 평가에 소요되는 시간 등도 절감할 수 있음을 보이고자 한다.

Ⅱ. 공통평가기준의 보증요구사항

2003년 11월에 정보통신부는 정보화촉진기본법 제

* 고려대학교 정보보호대학원(jilim@korea.ac.kr)
** 한국정보보호진흥원({taihoon, tslee}@kisa.or.kr)

15조 제1항의 규정에 의거하여 '정보보호시스템 공통평가기준(이하 공통평가기준)'을 개정·고시하였으며(제2003-52호), 공통평가기준은 향후에 정보보호제품 평가에 적극 활용될 것이다.

공통평가기준은 평가를 통하여 보증을 제공하는 방법을 취하고 있는데, 평가를 통한 보증의 제공은 보증을 얻는 전통적인 방법인 동시에 공통평가기준 및 이전의 ITSEC 등과 같은 다양한 기준이 취하는 보증방법론의 기초가 되는 것이기도 하다. 보증은 IT 제품 또는 시스템이 보안 목적을 만족시킨다는 신뢰의 기초가 되는 것이며, 공통평가기준은 정확한 입증 자료가 제시되지 못하는 주장, 이전의 관련 경험 및 이용 경험 등에 대한 참조가 아니라, 평가자의 능동적인 조사를 통하여 보증을 제공하게 된다(여기에서 말하는 능동적인 조사란, IT 제품 또는 시스템의 보안성을 판정하기 위하여 이를 평가하는 것을 의미한다). 공통평가기준의 3부에서는 '보증요구사항'을 정의하고 있으며, 보증 평가의 척도를 정의한 평가보증등급(EAL, Evaluation Assurance Level), 보증클래스, 패밀리, 그리고 패키지 형식의 평가보증등급을 구성하는 개별 보증 컴포넌트, 보호프로파일 및 보안목표명세서 평가를 위한 기준 등을 포함하고 있다.

공통평가기준에서는 다른 보증방법론의 상대적인 이점을 배제하거나 논평하지 않음으로써 다른 보증방법론에 대하여 유연한 태도를 유지하고 있으며, 현재 및 향후에도 계속 연구되고 또한 이를 수용하기 위한 검토에 관하여도 언급하고 있다. 공통평가기준은 제품 자체에 대한 평가를 위한 것이라고 인식되기도 하지만, 공통평가기준 3부에서는 다음과 같은 내용의 평가기술을 포함할 수 있음을 언급하고 있으며, 이것들에만 국한되는 것도 아니라고 명시하고 있다[1].

a) 프로세스와 절차의 분석 및 검사
b) 프로세스와 절차가 적용되고 있음을 검사
c) TOE 설계 표현간의 일치성 분석
d) 요구사항에 대한 TOE 설계 표현의 분석
e) 증거의 검증
f) 설명서 분석
g) 개발된 기능 시험 및 제공된 결과 분석
h) 독립적인 기능 시험
i) (결함 가정을 포함한) 취약성 분석
j) 침투 시험

위에서 언급하고 있는 항목들을 살펴볼 때, 공통평가기준이 정보보호제품에 대한 평가기준이라고 알려져 있음에도 불구하고 프로세스에 관련된 부분을 직접 언급하거나 간접적으로 의미함으로써 상당 부분 프로세스와 관련된 내용을 포함하고 있음을 알 수 있다. 이러한 내용으로 볼 때 공통평가기준을 단순히 정보보호제품 자체에 대한 평가기준이라고 판단하는 것보다는, 정보보호제품 기획 및 설계 단계에서부터 개발, 배치, 운영 및 유지 보수에 이르기까지의 모든 프로세스를 평가할 수 있는 포괄적인 기준으로 받아들이는 것이 합리적인 것으로 사료된다.

또한 이러한 내용을 다른 각도에서 고려하여 본다면, 정보보호제품 업체에서 적절한 프로세스를 수행하여 제작 혹은 작성한 정보보호제품은 공통평가기준 3부에서 요구하는 보증요구사항의 일부 혹은 전부를 만족할 수 있을 것이고, 더 나아가 이것은 평가에 상당한 영향을 미칠 수 있을 것이다.

Ⅲ. 프로세스 평가를 통한 보증

제품의 품질에 영향을 미칠 수 있는 요소에 대한 연구는 많이 진행되어 왔으며, 특히 기술, 인적 자원, 프로세스(공정) 등의 요소가 중요한 내용으로 간주되고 있다. 이 중에서 프로세스는 다른 요소들을 융합하여 표현할 수 있다는 점에서 중요한 의미를 가진다고 할 수 있다.

이러한 프로세스를 평가하기 위한 다양한 기준이 이미 많이 알려져 있으며, 또한 실제로 활용되고 있지만, 기존에 알려져 있던 대부분의 프로세스 평가기준은 일반적인 형태로 사용이 가능한 것들이어서 특별히 정보보호제품에 특화된 것이라고 보기에는 어렵다.

보안과 관련된 내용을 보완한 것으로는, 기존의 성숙도 모델을 연구하고 보안공학을 다루기 위하여 만들어진 SSE-CMM(ISO/IEC 21827 Information Technology-Systems Security Engineering - Capability Maturity Model)이 있으며, 유사한 많은 프로세스 평가 기준 중에서 공통평가기준과 비교적 많은 공통 부분을 가지고 있는 것으로 판단된다[2]. SSE-CMM은 적절한 보안공학을 보장하기 위하여 존재하여야 하는 조직의 보안공학 프로세스의 핵심적인 내용을 정의하고 있다. SSE-CMM은 평가를 받지 않은 제품을 사용하는 구매자와 사용자가 제품이나 시스템의 개발자 혹은 운영자의 주장에 전적으로 의존하여야 하는 상황에서 조직이 보다 성숙된 방법으로 보안공학을 수행하도록 요구하는 것이다(SSE-CMM은

정보보호제품에 국한되어 사용되지는 않지만, 본 고에서는 정보보호제품만을 대상으로 고려할 것이다).

SSE-CMM의 모델 설명 문서 본문에는 시스템 인증자, 시스템 인정자, 제품 평가자 및 제품 분석자 등을 포함하는 평가 기관(Evaluation organisation)이 SSE-CMM을 사용하여 얻을 수 있는 효과를 다음과 같이 기술하고 있다.

a) 제품 혹은 시스템 변경에 독립적인, 재사용 가능한 프로세스 평가 결과
b) 보안공학 및 타 분야와의 통합에 대한 신뢰
c) 보안 평가 작업량을 감소시키는 증거에 대한 능력 기반의 신뢰

또한, 시스템 통합자, 애플리케이션 개발자, 제품 판매자 및 서비스 제공자를 포함하는 엔지니어링 기관(Engineering organisation)이 SSE-CMM을 사용하여 얻을 수 있는 효과를 다음과 같이 기술하고 있다.

a) 반복적이고 예측 가능한 프로세스 및 실무(practice)를 이용하여 재작업 경감
b) 계약자 선정시 진정한 작업 수행 능력에 대한 신뢰 제공
c) 계량된 조직의 능력(성숙도) 및 개선에 대한 집중

이와 같은 내용을 기반으로 하여 볼 때, 높은 수준의 보안공학을 적용한 프로세스를 사용하여 제품을 개발하는 경우, 개발자와 평가자가 모두 비용과 시간 등에서 효율성을 얻을 수 있으리라 사료된다.

Ⅳ. 기존 연구 동향 비교

국제공통평가기준 프로젝트에서는 1996년 초에 보증 접근법을 다루는 작업 그룹 AAWG(Alternative Assurance Working Group)를 결성하여 다양한 보증방법론 간의 상호 관련성에 관한 연구를 진행하였고, 현재는 ISO/IEC JTC 1/SC 27에서 표준화 작업을 진행하고 있다[3]. 이것은 정보기술전문가들이 요구하는 보안요구사항에 적합한 보증방법을 선택적으로 사용하게 함으로써 효율적이고 경제적인 보증을 얻기 위한 공통적인 보증 프레임워크를 개발하는 것을 목적으로 하고 있으며, 선택적 보증방법의 사용은 보증방법간의 호환성(compatibility)과 순응성(compliance)을 이용하여 특정 보증방법을 근거로 평가받았던 증거물을 재사용함으로써 비용과 시간을 절약하고 결과적으로 적시에 제품 출시가 가능하도록 하기 위한 것이다.

FRITSA(ISO/IEC 15443)라고 알려진 이 연구의 본래 목적은 다양한 프로세스 평가기준을 사용한 평가결과를 공통평가기준을 이용한 제품 평가와 직접적으로 연결시키려는 것은 아닌 것으로 보이지만, 이와 유사한 의미를 갖는다고 볼 수 있을 것이다. 하지만 이러한 연구의 결과를 그대로 국내 환경에 도입하는 데에는 약간의 문제가 있을 것으로 사료된다.

(1) ISO/IEC 15443는 3개 부분으로 구성되어 있으며, 1부에서는 개념 및 개략적인 소개를 하고 2부에서는 수십여 종에 이르는 다양한 보증방법론에 대한 개요를 설명하고 있다. 가장 중요한 3부는 2부에서 소개된 보증방법론과 공통평가기준의 순응성 등에 관한 비교 연구로 이루어져 있다. 이 연구의 결과를 수용하여 적용하기 위해서는 사전에 몇 가지 가정이 필요하게 되는데, 가장 중요한 것은 공통평가기준을 포함하여 ISO/IEC 15443의 2부에서 소개하는 다양한 보증방법론이 이미 상당부분 실제로 활용되어 있어야 한다는 점이다. 우리나라의 경우 2002년 8월에 공통평가기준이 고시되어 평가를 시행할 수 있게 되었으므로 아직 보편화된 상태는 아니라고 할 수 있고, 또한 다양한 보증방법론이 이론적으로는 연구되고 있으나 실제 활용도는 낮은 수준이라고 사료되므로 ISO/IEC 15443에서 소개하고 있는 보증방법론을 활용하고 있는 상태에서 공통평가기준을 도입하는 경우에 얻을 수 있는 장점에 대한 고려가 상대적으로 크지 않게 된다. 다시 말해서, ISO/IEC 15443의 연구 결과는 정보보호제품 업체가 이미 하나 이상의 보증방법론을 채택하여 사용하고 있을 경우에 의미를 갖는 것이고, 다양한 보증방법론을 채택하여 사용하고 있을수록 ISO/IEC 15443의 연구 결과를 도입하여 얻는 효과가 클 것이다.

(2) ISO/IEC 15443의 2부에는 상당히 많은 보증방법론이 소개되고 있지만, 대부분의 경우에는 표준으로 제정되어 사용되고 있지 못한 것들이다. 따라서 국제 표준 등으로 제정되어 있지 않은 경우를 제외하고는 어떠한 보증방법론을 채택하여 사용하고 있음을 인정받을 수 있는 방법에 한계가 있다. 또한 자체적으로 임의의 보증방법론, 예를 들어 SSE-CMM을 채택하여 사용하고 있다고

하더라도, 이를 인정받기 위해서는 높은 비용 및 시간이 요구되는 프로세스 평가를 받아야 하는 경우가 있다.

(3) ISO/IEC 15443의 핵심 내용이라고 할 수 있는 3부는 1997년에 발표된 AAWG의 보고서(Task 1 Report)를 그대로 수용한 것이며, 그 이후에 특별히 진전된 내용의 보고서를 발표하지 못하고 있다.

AAWG 보고서(Task 1 Report)의 핵심 내용은 SSE-CMM과 공통평가기준을 엘리먼트 단위로 비교하여 순응성 여부를 검토하고, 호환이 되는 부분에 대한 재평가를 생략하는 방법을 제시하고 있다. 따라서 만일 기존에 SSE-CMM을 도입하여 프로세스 평가를 시행하여 그 결과를 인정받은 경우라면 향후 생산된 제품의 평가 효율성을 제고하는 방안을 고려해 볼 수 있는 가능성이 생기는 것이다.

하지만 현재 국내 정보보호제품 업체의 환경을 고려하여 볼 때, 공통평가기준에 의한 정보보호제품의 평가와 별도로 SSE-CMM을 이용한 프로세스 평가를 받기 위한 추가 비용의 지출은 바람직하지 않은 것으로 보인다. 또한 SSE-CMM이 특정한 프로세스나 순서를 제시하지 않기 때문에 이에 대한 신뢰 수준을 보장하는 것도 문제가 될 수 있다.

V. 프로세스 보증을 통한 정보보호제품 평가의 효율성 향상 방안

프로세스 평가와 제품 평가가 근본적으로 다른 것으로 생각됨에도 불구하고 이를 통합하려는 시도가 가능한 것은, 보안공학이 적용된 프로세스(예를 들어 SSE-CMM의 PA)를 수행하면서 나오는 산출물(예를 들어 SSE-CMM의 BP에 제시된 Work Products)이 정보보호제품 평가에서 요구되는 제출물과 유사한 특성을 가지고 있으면서 또한 평가에 활용될 수 있기 때문이다.

적절한 프로세스에 의하여 생산된 정보보호제품은 제품 개발 공정에서 평가에 필요한 산출물을 자연스럽게 출력하게 될 것이고, 이 산출물은 평가에 필요한 요소를 상당부분 포함하게 되어 손쉽게 평가를 준비할 수 있게 될 뿐만 아니라 평가의 효율성 제고에도 영향을 미치게 될 것이다. SSE-CMM과 공통평가기준을 비교 검토하는 경우, SSE-CMM의 PA09 Provide Security Input에 속하는 BP.09.03 Identify Security Alternatives를 수행함으로써 공통평가기준의 EAL 3 및 EAL 4에서 요구하는 ADV_HLD.2의 내용을 상당부분 만족시킬 수 있음을 알 수 있다. 하지만 이러한 비교는 추상적인 내용을 많이 포함하고 있는 것이며, 공통평가기준에서 요구하는 수준으로까지 세부적으로 기술하기 위해서 몇 가지 보완이 필요하다.

(1) 호환이 가능한 것으로 판단되는 경우라도 평가보증등급(EAL)과 SSE-CMM 평가등급의 상호 관계에 관한 분명한 관계가 밝혀져야 할 것이다. 현재까지의 비교는 EAL 3 혹은 EAL 4를 대상으로 하고 있지만 SSE-CMM의 성숙도 레벨은 1을 가정하고 있는 것이다. 따라서 단순히 요구사항 및 문구의 내용이 유사하다고 해서 순응성이 보장된다고 보기에는 무리가 있다. EAL과 SSE-CMM 등의 성숙도 레벨에 관한 비교는 관련 논문을 참조하면 도움이 될 것이다[4].

(2) 공통평가기준과의 비교 대상 예로서 SSE-CMM을 언급하고 있지만, 호환성이 결여된 것으로 판명된 항목에 대하여 다른 프로세스 평가 모델에서 대안을 제시할 수도 있다. 이것은 연구 범위와 관련된 문제로서, 이러한 문제를 해결하기 위하여 ISO/IEC 15443 2부에서 다양한 보증방법론의 존재를 언급하고 있는 것으로 사료된다. 따라서 가능하면 다양한 보증방법론을 공통평가기준과 비교 검토할 필요가 있으며, 또한 공통평가기준의 다른 보증컴포넌트에 대하여서도 유사한 연구가 폭넓게 진행되어야 할 것이다.

V. 결론 및 향후 연구방향

공통평가기준에 의한 평가의 시행에 따라 국내 정보보호제품 제조 업체들은 향후의 국제 시장 환경 노출 상황에 대비하여야 하며, 또한 국제적인 경쟁력을 갖춤과 동시에 시장에서 필요한 제품을 적시에 공급할 수 있는 능력을 배양하여야 할 것으로 사료된다.

제품 개발을 완료한 후 평가를 수행하여 제품 인증을 받는 수준으로는 변화하는 시장의 요구에 점점 대응하기 어려워질 것으로 사료되므로, 이를 극복하기 위해서는 개발 프로세스의 개선을 통하여 공통평가기준의 보증요구사항의 요구사항을 만족시킬 수 있는 개

발 공정을 정립할 필요가 있다. 프로세스의 개선은 평가준비 및 평가에 소요되는 비용 및 시간을 단축함으로써 평가의 효율성을 제고하여 줄 수 있으며, 우수한 품질의 정보보호제품의 개발을 가능하도록 할 것이다.

향후에는 정보보호제품 개발 프로세스 개선과 공통평가기준 기반 평가의 상호 관련성 및 영향에 관한 연구가 지속적으로 이루어져야 할 것으로 사료된다.

참고문헌

[1] 정보통신부고시 제2003-52호, 정보보호시스템 공통평가기준, 2003. 11. 27

[2] ISO/IEC 21827 Information Technology - Systems Security Engineering - Capability Maturity Model Version 2.0, 1999. 4. 1

[3] ISO/IEC 15443-3 - Information technology - Security techniques - A framework for IT security assurance - Part 3: Analysis of assurance methods, 2001. 2. 26

[4] 김태훈, 이태승, 조규민, 이경구, "프로세스 평가 모델 등급과 정보보호시스템 공통평가기준 평가보증등급 비교", 한국사이버테러정보전학회 정보보증 논문지 제2권 제2호, pp.137~142, 2002. 12.

〈著 者 紹 介〉

임 종 인 (Jong In Lim)

1986년~현재 고려대학교(정보보호대학원) 교수
1991년~현재 한국정보보호학회 종신회원
1999년~현재 고려대 정보보호기술연구센터 센터장
1999년~현재 한국정보보호진흥원 사외이사
2000년~현재 고려대 정보보호대학원 원장
〈관심분야〉 정보보호 및 정책, 개인정보보호, 사이버법률

김 태 훈 (Tai-Hoon Kim)

1995년 성균관대학교 전기공학과(공학사)
1997년 성균관대학교 전기공학과(공학석사)
2002년 성균관대학교 전기전자및컴퓨터공학부(공학박사)
2002년~현재 한국정보보호진흥원 선임연구원
〈관심분야〉 보안공학, 공통평가방법론

이 태 승 (Tae-Seung Lee)

1994년 광운대학교 전자계산학과(이학사)
1996년 포항공과대학교 전자계산학과(공학석사)
1996년 ~ 2001년 삼성전자 소프트웨어센터 책임연구원
2002년~현재 한국정보보호진흥원 선임연구원
〈관심분야〉 네트워크 보안, 공통평가방법론, 프로세스 기반 보증성 평가