2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

정보보호시스템 평가와 소프트웨어 프로세스 심사 방법 비교

이지연, 유희준, 최진영
고려대학교 컴퓨터학과 정형기법 연구실*
e-mail : jylee@formal.korea.ac.kr

Comparison between Information Secure System Evaluation and Process Assessment

Ji – Yeon Lee, Hee-Jun Yoo, Jin-Young Choi
Dept. of Computer Science and Engineering , Korea University

요 약

현대 사회는 정보통신 기술의 발달로 정보 시스템의 사용이 급격히 증가 되고 있다. 정보화의 가속화에 따라 다양한 역기능들 또한 도출되고 있다. 여러 가지 역 기능들로부터 정보를 보호하고 안정한 정보 유통을 위한 양질의 정보보호 시스템을 위해 정보보호 제품에 대한 평가가 요구 되고 있다. 이런 이유로 전세계적으로 많은 평가 기준들이 만들어지고 있으며, 국내에서도 침입차단 시스템에 대한 평가기준을 만들고 이를 사용해 평가를 하고 있다. 본 논문에서는 국내 침입차단 시스템 평가 기준과 소프트웨어 프로세스 심사방법 중 하나인 SPICE 사이의 연관성을 찾아보고자 한다.

1. 서론

현대 사회는 정보통신 기술의 발달로 정보 시스템의 사용이 급격히 증가 되고 있다. 정보화의 가속화에 따라 다양한 역기능들 또한 도출되고 있다. 인터넷 등 정보 통신망에 대한 취약성 및 위험이 가중되고 있고 정보 유출, 파괴, 정보 위,변조 등의 컴퓨터 범죄와 해킹 급증, 바이러스 감염, 서비스 방해 , 불건전 정보 유통 등 정보화 역기능이 확산 되고 있는 추세로 체계적이고 총체적 정보보호 대책이 필수로 요구되고 있다. 컴퓨터 범죄로부터 정보를 보호하고 안전한 정보 유통에 의한 정보화를 촉진하고, 보안성, 신뢰성이 검증된 양질의 정보보호 시스템을 보급함으로써 효율적인 정보보호 체계를 구축하고, 다양한 정보보호 시스템 수요 및 시장을 창출해서 정보보호 산업을 육성하기 위해 정보보호 제품에 대한 평가가 요구되고 있다. 현재 우리나라에서 사용하는 침입차단 시스템에 대한 평가제도는 제품의 기능과 품질에 따라 이들을 7 개의 등급으로 나누어 인증하는 방법을 사용하고 있다.

평가하고자 하는 보안 소프트웨어들은 일반적인 소프트웨어에 보안기능이 추가된 특성화된 소프트웨어이다. 따라서, 일반적인 소프트웨어를 개발하는 프로세스를 관리, 심사하는 SPICE 와 연관성을 찾을 수 있을 것이라 생각된다. 소프트웨어 프로세스 심사란, 소프트웨어가 가지고 있는 일정 지연, 비용증대, 고객의 불만족 등의 문제를 줄이기 위한 다른 방안으로 소프트웨어를 개발하는 프로세스를 관리하는 것이다. 여기서 프로세스 관리란 제조업에서 사용해 왔던 기술을 소프트웨어 개발에 적용하는 것과 유사하며, 이 방법을 통해 소프트웨어의 개발, 유지보수, 지원에서 프로세스를 개선하는 것이다. 이 후자의 방법이 제대로 되고

있는가를 점검하여 문제점을 파악하여 개선하는 토대를 마련하는 것을 소프트웨어 프로세스 심사라고 한다.

본 논문에서는 앞서 설명한 소프트웨어 프로세스 심사 방법인 SPICE 와 침입차단 시스템 평가 기준을 비교함으로써 둘 사이의 연관성을 살펴보고자 한다.

본 논문의 구성은 2 장에서 프로세스 심사 기준 중 하나인 SPICE 에 대해 소개하고, 3 장에서는 현재 국내에서 사용되고 있는 침입차단 시스템 평가 기준에 대한 설명, 그리고 4 장에서는 둘 사이의 연관성을 기술하고 있다. 5 장에서 결론으로 끝을 맺겠다.

2. SPICE (Software Process Improvement and Capability dEtermination)

일반 사용자에게 보다 편리한 사용자 인터페이스 환경을 제공하기 위해서는 현재의 윈도우 기반 사용자 인터페이스의 차원을 넘어서 사용자의 작업을 대행해 줄 수 있는 에이전트 시스템이 제공되어야 한다. 또한 에이전트 시스템 서비스 확장과 사용보급을 위하여 응용 되고 있다.

SPICE 는 소프트웨어 프로세스 (조달, 공급, 개발, 운영, 유지 보수, 지원) 에 대한 계획, 관리, 감시, 통제, 개선을 위한 능력 심사와 개선을 목적으로 하고 있다. SPICE 는 소프트웨어 제품의 개발 혹은 공급을 담당하는 공급자, 혹은 요청에 따라 현재의 프로세스 능력이나 혹은 잠재적인 개발 능력을 파악하려는 자, 프로세스 심사를 직접 훈련시키거나 프로세스 개선을 모니터링 하려는 심사원이나 요청자 모두에게 사용될 수 있으며, 개발 능력 수준은 0 부터 5 까지 6 개 수준으로 결정된다. SPICE 의 심사에서는 기존의 심사모형을 적용할 수도 있지만 모형과 심사 방법의 기초를 제공하는 참조 모형과 호환성을 요구한다. 참조모형에서는 소프트웨어의 획득, 공급, 개발, 운영 및 지원 들을 수행하는 조직의 프로세스와 각 프로세스 능력을 특징짓는 프로세스 속성(Process Attribute: PA) 에 관한 내용을 설명하고 있다. 참조 모형은 프로세스 차원과 프로세스 능력의 2 개 차원으로 구성된다.

2.1 프로세스 차원

프로세스 차원은 소프트웨어의 개발, 유지, 획득, 공급 및 운영 관련 조직의 프로세스들을 구분하기 위해 3 개 주요 생명주기 프로세스 (기본(Primary), 지원(Supporting), 조직(Organizational)) 그룹과 5 개 (고객-공급자(Customer-Supplier), 공학적(Engineering), 지원 (Supporting), 관리(Management), 조직 (Organization)) 범주 총 40 개 프로세스들로 구성되어 있다. 참조모형의 각 프로세스는 목적 기술문(purpose statements) 을 통해 그 내용을 알 수 있는데, 여기에는 프로세스의 독특한 기능적 목표를 포함하여 프로세스의 산출물 식별에 필요한 추가적인 자료를 포함한다. 그러나 참조모형 자체에서는 프로세스 목적 기술문 구성요소의 성취 방법이나 그 순서를 정의하지는 않고 있다.

2.2 프로세스 능력 차원

프로세스의 능력 차원은 6 개의 프로세스 능력 수준과 9 개의 PA(Process Attribute)로 구성되어 있다. PA 는 프로세스 목적과 경영목표의 효과성을 관리 및 개선하는 전반적인 능력의 한 측면을 설명하는 것으로서 프로세스 수행능력 개선에 따른 능력수준의 향상은 해당 속성들의 결합으로 나타나게 된다.

기본적인 프로세스 목적의 만족은 프로세스 능력구축의 첫 단계이며, 이후는 해당 관리활동 (Management Practice: MP) 의 수행증거를 통해 PA 를 수준별로 파악할 수 있다. 즉, MP 는 해당특성과 연결해 프로세스 능력 정도를 나타내는 지표로 사용되며, 활동 구현에 관한 지침으로는 활동 수행 특성과 프로세스 관리 지원을 위한 메커니즘을 제공하는 자원 및 기반구조 특성, 그리고 프로세스 차원에서 해당 MP(management practice)를 지원하는 관련 프로세스등이 활용된다.

세부 능력 수준은 Level 0 부터 Level 5 까지의 6 개 수준으로 구분되며, 각 수준별 9 개 관련 PA 들은 다음과 같다. Level 0 (불완전 수준)은 프로세스 목적 달성이 전반적으로 실패하여, WP(work product) 혹은 프로세스 결과물이 거의 없거나 식별이 거의 불가능한 경우에 해당한다. Level 1 (수행 수준) 은 프로세스 목적이 전반적으로는 달성되었으나 적극적인 계획 및 성취가 없는 수준이며, PA1.1 (프로세스 수행속성)이 해당된다. Level 2(관리 수준)에서는 명세 된 절차에 따라 WP 가 산출되고 프로세스의 계획 및 추적 수행이 가능하여 명세된 표준과 요구사항에 적합한 WP 가 산출되며, 관련

속성은 PA2.1 (수행 관리 속성) 과 PA2.2 (작업 산출물 관리 속성) 이다.

Level 3 (확립수준) 소프트웨어 공학의 기본 원칙에 근거해 올바르게 정의된 프로세스를 사용하여 프로세스를 수행하고 관리하는 단계로 PA3.1 (프로세스 정의속성)과 PA3.2(프로세스 자원속성) 가 관련된다. Level 4(예측가능 수준) 는 목표달성을 위해 정의된 프로세스가 일정한 통제하에 일관되게 수행되고, 결과 측정값의 수집과 분석 및 프로세스 능력의 정량적 이해, 그리고 개선된 수행 예측과 관리 능력들을 보유하여 WP 품질에 관한 정량적 파악이 가능한 단계이며, PA4.1 (프로세스 측정 속성)과 PA4.2(프로세스 통제속성)가 관련된다. 그리고 level 5 (최적 수준)는 현재와 미래 경영목표에 부합하는 프로세스 수행의 반복 가능성이 높은, 즉 프로세스의 최적화가 가능한 수준이다. 해당 속성으로는 PA5.1 (프로세스 변경속성) 과 PA5.2 (지속적 개선 속성) 가 있다.

서수적(ordinal)으로 정의되는 프로세스 능력수준은 최하위 불완전 수준부터 최상위 수준까지 각 능력수준별 PA 의 % 척도로서 성취정도를 표시한다.

N	Not Achieved	0% ~15%	정의된 속성을 달성했다는 증거가 없음
P	Partially Achieved	16% ~50%	정의된 속성을 약간 달성하였음
L	Largely Achieved	51% ~85%	정의된 속성을 상당히 달성하였음
F	Fully Achieved	86% ~	정의된 속성을 완전히 달성하였음

3. 국내 침입차단시스템 평가 방법

국내에서 최초로 시도되는 평가 방법으로서 기능 요구사항에 대한 평가 방법과 보증 요구사항에 대한 평가 방법으로 나뉘어 진다.

우선 기능 요구사항에 대한 평가 방법은 침입차단시스템의 기능 요구 사항인 신분확인, 접근통제, 무결성, 비밀성, 감사기록 및 추적, 보안관리에 대한 각 요구사항에 대한 만족도 정도를 확인하고, 보증 요구사항에 대한 평가 방법은 침입차단시스템의 보증 요구 사항인 개발과정, 형상관리, 운영환경, 설명서, 취약성에 대한 평가 방법은 다음과 같다.

개발과정은 기능명세, 기본설계, 상세설계, 구현 단계로 이루어지며, 각 개발과정에서 산출되는 문서들을 작성하는 방법에 대해 설명한다. 시험은 시스템을 구성하는 요소들이 제대로 동작하고 성능 요구에 적합하다는 것을 보증하는 일이다. 침입차단시스템 시험의 종류와 방법에 대해 알아보며, 시험계획과 시험 결과로 구성되는 시험서의 작성방법에 대해 설명한다. 형상관리는 침입차단시스템의 개발과정에서 시스템의 변화과정을 통제하기 위한 관리 방법이다. 형상관리는 크게, 형상항목의 식별, 형상관리체계로 구분되고, 형상관리 체계는 형상변경통제, 형상 항목의 감사, 형상관리 도구의 지원이 있으며, 이들 항목에 대해 설명한다. 운영환경은 침입차단 시스템의 설치와 침입차단 시스템의 시동 및 운용환경으로 구성되며, 침입차단시스템의 설치지침서와 운용지침서에 대해 설명한다. 설명서는 침입차단시스템의 올바른 사용과 안전한 운영을 위해 필요한 기본 문서로, 사용자 설명서와 관리자 설명서 작성법에 대해 설명한다.

취약성은 시스템을 개발 및 운영시에 발생하는 다양한 취약성을 분석하는 과정으로 취약성 분석과 오용 분석 과정으로 나누어 진다.

4. 프로세스 심사와 침입차단 시스템 평가등급 비교

4.1 유사점

국내에서 현재 사용하고 있는 침입차단시스템의 평가 방법은 소프트웨어의 기능부분을 중점적으로 평가하고 있고, 프로세스 심사의 경우는 기능부분을 포함한 조직, 인력, 관리 등 소프트웨어를 개발하기 위한 다양한 부분들을 심사한다.

SPICE 에서는 소프트웨어 개발주기에서 각 단계들을 심사해서 정해진 완성도를 이룰 경우 LEVEL을 받기 위한 요구사항을 만족할 수 있지만 보안등급 평가 기준요구사항에서는 개발된 소프트웨어들의 기능이 어느 정도 인지를 판단하고 그 기능에 따라 등급을 평가한다. 여기서 설명하는 프로세스 심사에서 지금의 평가 방법에서 요구하는 보증부분을 심사할 수 있는 프로세스를 찾을 수 있다.

우선 기능부분은 프로세스의 능력 심사 시 기본적으로 완수 되어야 하는 부분이고, 보증 부분에 있어서 개발부분의 기능명세서, 기본명세서, 상세설계서는 문서로서의 가치가 아니라 시스템의 전반적인 요구사항을 확인하는 단계라는 점에서 Customer-Supplier process 에서 CUS.3 , Requirements

Elicitation 과 구체적인 설계에 대한 문서화는 Engineeing process 인 ENG 부분에서 심사할 수 있고, 개발의 각 단계별 보안기능 시험 및 결과를 재시하고 시험서에 기술된 시험의 일부를 직접 수행하는 방법은 Support process 의 SUP.4 Verification 과 SUP.5 Validation 에서 확인 할 수 있다. 그리고 형상관리는 SUP.2 의 형상관리 프로세스에서, 안전한 시동, 백업, 유지보수 및 운용에 대한 절차에 대한 운영환경은 CUS.4 Operation 부분에서, 설명서는 SUP.1 Documentation 에서, 취약성은 Management process 의 MAN.4 Risk Management 에서 심사 할 수 있다. 이런 방법으로 지금 현재 침입차단 시스템에서 요구하는 사항들을 심사할 수 있는 프로세스들이 있고 이것들의 성취도에 따라 등급이 부여될 수 있다. 그리고 보안등급 평가기준에서는 기능적인 측면을 강조해서 등급을 평가하는 만큼 일반 소프트웨어의 개발단계에서 요구되는 사항들보다 더욱 복잡하고 정형화된 요구사항을 갖고 있다.

4.2 차이점

이 두 가지의 기준은 소프트웨어를 심사하는 면에서 같지만 차이점이 있다. 침입차단 시스템 평가기준은 완성된 소프트웨어가 갖고 있다고 말하는 기능이 잘 수행되는지의 여부를 판단해서 등급을 부여하고 그 기능들을 좀더 정형화된 방법으로 증명할 수 있다면 고등급을 받을 수 있다. 프로세스 심사의 경우는 물론 소프트웨어의 기능도 중요하지만 그 소프트웨어의 개발단계에서 갖는 조직이나 인력 관리 등의 부분에 대한 평가가 이루어져야만 고등급을 받을 수 있고, 이 경우는 소프트웨어 프로세스 심사를 거쳐 LEVEL 을 알고자 하는 다른 조직이나 사람에 의해서도 심사의 대상이 될 수도 있다. 그리고 보안 평가는 어떤 승인된 조직에 의해서 평가가 이루어 지지만 SPICE 의 경우 일정한 자격 요건을 갖춘 심사원이라면 소속된 조직에 상관없이 심사에 참여 할 수 있다.

5. 결론

앞에서 비교해 본 두 가지 평가 방법은 보안 소프트웨어와 일반 소프트웨어라는 점에서 심사하는 기준에 유사점과 차이점을 갖는다. 소프트웨어를 심사하는 방법이기 때문에 유사점을 갖고 있지만, 평가하는데 있어서 중점적으로 보는 부분이 다르기 때문에 소프트웨어를 평가하는 기준도 약간의 차이를 가지고 있다.

본문에서 살펴본 결과에 의하면, 소프트웨어의 능력을 평가하는 두 방법이 유사한 프로세스를 가지고 평가를 진행 한다는 것을 찾을 수 있었다. 하지만, 앞서 언급한 대로, 기능을 중요시한다는 점과 기능보다는 관리를 중요시한다는 점에서 차이점들을 나타내고 있다. 이런 차이점을 서로 고려한다면 서로를 연계될 수 있는 부분이 생기리라 생각된다.

참고문헌

[1] SPICE Information Technology -Software Process Assessment- 1998.12.

[2] 국내외 정보보호시스템 평가 가이드 한국정보보호센터 1998.11

[3] 소프트웨어 프로세스 심사의 이해: SPICE 중심으로, 정호원 황선명, 정보과학회지 제 17권 제 1호, 1999.1.