KIPS Tr. Software and Data Eng.
Vol.3, No.11 pp.465~470 pISSN: 2287-5905

http://dx.doi.org/10.3745/KTSDE.2014.3.11.465

Software Security Supplementation Guide Line Based on ISO 27001 for the SP Certified Organization

Eun-Ji Yoon† · Young B. Park††

ABSTRACT

The SP quality assessments from national IT industry promotion agency of Korea(NIPA) assesses ability of software development process. And the SP quality assessments is getting popular over the nation. But, in the SP quality assessments, there is no concern about security attribute. In this paper new secure process base on ISO 27001 is proposed for the organization that is already passed SP quality assessments. This process can detect security threatening factors and gives chance to protect those factors. Furthermore, since detected security weaknesses can be used as a measurement, the system can be managed in aspect to security attribute.

Keywords : Software Security, ISO 27001, SP Quality Assessments, Security Measurement, Security Threatening Factors

SP 인증 조직의 소프트웨어 보안 향상을 위한 ISO 27001 적용방안 연구

윤 은 지† · 박 용 범††

요 약

한국의 정보통신산업진흥원(NIPA)에서 제공하는 SP 품질 인증은 소프트웨어 개발 프로세스의 역량을 평가 및 인증하는 제도이다. SP 품질 인증은 국내에서 개발된 인증모델로서 전국적으로 확산되고 있다. 최근 보안성이 문제되고 있으나, SP 품질 인증에서는 별도의 보안 속성에 대한 프로세스를 정의하고 있지 않다. 본 논문에서는 SP 품질 인증을 획득한 기업 및 조직들의 보안성 향상을 위해 ISO 27001을 기반으로 하는 새로운 보안 프로세스를 제시한다. 제안 프로세스를 통해 보안 위협요소들을 검출해낼 수 있고, 이러한 요소들에 대처할 수 있는 기회를 제공한다. 또한 검출된 보안 취약점은 보안 척도로 이용될 수 있으므로 시스템의 보안 측면 관리가 가능하다.

키워드 : 소프트웨어 보안, ISO 27001, SP 품질 인증, 보안 척도, 보안 위협요소

1. 서 론

소프트웨어 제품이 현대인의 생활 전반에 걸쳐 사용되면서 소프트웨어는 갈수록 복잡하게 되었다. 복합적인 다양한 기능을 요구하게 됨에 따라 소프트웨어의 품질에 대한 시험 측정의 중요성이 높아지고 있다[1, 2]. 또한 시장 경쟁에서 살아남기 위해서는 높은 품질의 소프트웨어를 적은 비용으로 더 빠르게 개발하는 것이 중요하다[3, 4].

국내의 소프트웨어 개발 업체는 90%가량이 중소기업으로, 그 규모가 영세하여 우수한 제품을 개발하여도 업체의 낮은 지명도와 마케팅 능력 부재 등으로 인하여 시장개척에 어려움을 겪고 있다. 또한, 세계적인 추세로 볼 때, 사회 및 경제 발전과 더불어 소비자의 인식이 제품의 가격보다는 품질 및 안정성 등으로 그 관심이 변해가고 있다[5, 6].

소프트웨어 업체들과 소비자들의 소프트웨어 품질에 대한 중요성이 높아짐에 따라 이를 뒷받침할 소프트웨어 품질 인증 방법에 대한 다양한 연구가 진행되었다[7]. 그리고 품질 인증을 위한 기관들도 점차 생겨났고, 소비자는 전문기관에 의한 품질 인증 결과를 통해 신뢰성 있는 제품을 선택할 수 있다[8]. 국외의 경우 1980년대 이후 CMMI 및 SPICE 등과 같은 소프트웨어 프로세스 능력평가 및 개선모델을 연구하여 발전시키고 있다. 국내에서도 소프트웨어 산업의 특징과 현황을 분석하여 한국정보통신기술협회(TTA)에서는

※ 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "2014년도 고용계약형 정보보호 석사과정 사업"의 연구결과로 수행되었음(과제번호 H2101-14-1001).
† 준 회 원 : 단국대학교 컴퓨터학과 석사과정
†† 종신회원 : 단국대학교 컴퓨터과학과 교수
Manuscript Received : September 29, 2014
Accepted : October 15, 2014
* Corresponding Author : Young B. Park(ybpark@dankook.ac.kr)

GS(Good Software) 인증을, 정보통신 산업진흥원(NIPA)에서는 국내 실정에 적합한 소프트웨어 프로세스 인증 모델인 SP(Software Process) 인증을 발표하였다.

2014년 4월 16일 소프트웨어 공학센터는 2009년부터 2012년까지 SP 인증을 획득한 기업과 인증을 획득하지 않은 기업을 비교하여 발표하였다. SP 인증을 획득한 기업은 인증을 획득하지 못한 기업보다 매출이 급격하게 증가하였고, 제품 결함률과 결함 제거율은 낮아지는 등의 효과를 거두었다.

그러나 이는 소프트웨어 프로세스의 역량에 대한 심사와 인증을 할 뿐, 보안성까지 보증해주지 않는다. 따라서 본 논문은 SP 인증을 취득한 기업 및 조직의 보안성을 향상시키기 위해 ISO 27001을 결합시킨 보안 프로세스를 제안한다.

2. SP(Software Process) 인증

2.1 SP 인증

SP 인증이란 정보통신산업진흥원에서 조직 또는 기업의 소프트웨어 개발 단계별 작업절차 및 산출물 관리 역량 등을 분석하여 소프트웨어 개발 프로세스 역량기준을 평가 및 인증하는 제도이다. 2008년 9월부터 시행하여 2009년 상반기부터 인증 심사를 시작했다[9].

2.2 SP 인증 영역

SP 인증은 5개의 영역, 17개의 평가항목을 가지며 76개의 세부평가항목이 존재한다.

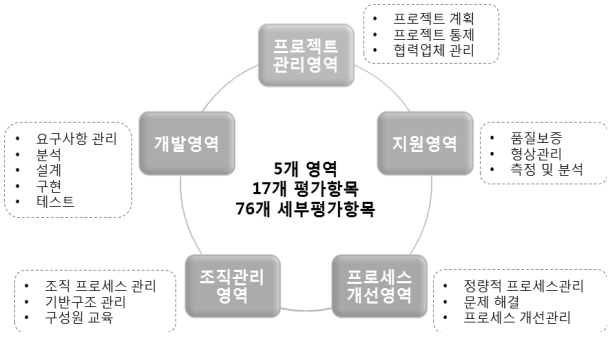

Fig. 1. Quality Certification of SW Process

프로젝트 관리 영역은 프로젝트의 목표와 범위를 정의하고 목표 달성을 위한 계획을 수집하며 전반적인 프로젝트의 활동을 검토하고 통제하여, 프로젝트의 목표를 달성할 수 있도록 프로젝트를 관리한다. 이 영역은 프로젝트 계획, 프로젝트 통제, 프로젝트 협력업체 관리의 평가항목을 가진다.

개발 영역은 사전에 계획된 프로젝트 수행 계획에 따라 요구사항을 추출하고, 분석, 설계, 구현, 통합 및 테스트 등 소프트웨어를 개발한다. 이 영역은 요구사항 관리, 분석, 설계, 구현, 테스트를 평가항목으로 삼는다.

지원 영역은 프로젝트 수명주기 동안 프로젝트 개발 및 관리 활동을 통제하여, 프로젝트의 성공률을 높이기 위해 프로젝트 활동 전반을 지원한다. 이 해당 영역에는 3가지의 평가항목이 존재하며 품질보증, 형상관리, 측정 및 분석이 존재한다.

조직관리 영역은 조직 기반구조 및 구성원 교육체계를 구축하여 조직에 필요한 표준 프로세스를 개발, 적용하여 조직 내 프로젝트의 체계적인 이행을 하도록 한다. 이 영역의 평가항목으로는 조직 프로세스 관리, 기반구조 관리, 구성원 교육이 있다.

프로세스 개선 영역은 조직과 프로젝트의 사업목표 달성을 위해 조직 및 프로젝트의 프로세스를 정량적으로 운영하고 개선하며 관리한다. 이 영역은 정량적 프로세스 관리, 문제 해결, 프로세스 개선 관리를 평가항목으로 한다.

2.3 SP 인증 등급 체계

소프트웨어 프로세스 품질 인증 등급이란 소프트웨어 개발 프로젝트 수행과 관련한 활동 역량수준을 평가요소 기준으로 심사한 결과이다. 프로젝트 차원에서부터 조직 차원으로 프로젝트 수행 역량을 강화할 수 있도록 초기 수준(1등급), 우수 수준(2등급, 프로젝트 차원), 최우수 수준(3등급, 조직 차원)의 3단계 구조로 구성된다. 이 중 우수 수준과 최우수 수준만이 유효한 인증등급으로 부여된다[9].

Fig. 2. Assesment object of SP certification

1등급은 프로젝트의 성공 여부와 관계없이 특정 프로젝트를 수행할 수 있는 수준이나, 프로젝트 수행을 위한 기본적인 활동들이 안정적으로 수행되지 못해 품질, 비용 납기 측면에서 기대되는 목표를 충족시키지 못할 확률이 높은 상태로 프로젝트 수행을 위한 프로세스 역량 개선이 필요한 수준이다.

2등급은 개별 프로젝트를 수행하기 위해 필요한 프로젝트 차원의 프로세스가 수립되고 이를 기반으로 프로젝트를 통제하여 성공적으로 프로젝트를 수행할 수 있는 역량수준이다. 해당 등급은 프로젝트 관리, 개발, 지원 영역을 평가요소로 삼는다.

3등급은 조직의 프로세스 체계를 정의하고 정량적인 데이터 관리를 통해 조직 차원의 프로세스를 개선하고 발생되는 문제의 근본 원인을 해결함으로써 일관된 품질 수준의 프로젝트 수행이 가능하며, 지속적으로 프로세스를 개선할 수 있는 역량수준이다. 해당 등급은 프로젝트 관리, 개발, 지원, 조직관리, 프로세스 개선을 평가영역으로 한다.

본 연구에서는 SP 인증의 유효등급인 2등급을 획득한 조직 및 기업의 보안성을 향상시키기 위하여, 5가지 평가영역 중 프로젝트 관리 영역, 개발 영역, 지원 영역에 대하여 다룬다.

3. SP 인증의 보안성 고려

SP 인증은 소프트웨어 프로세스에 대한 품질을 인증할 뿐, 소프트웨어의 보안성까지 인증하지는 않는다. SP 인증의 부족한 부분을 보완하기 위하여, 본 연구에서는 보안성에 대하여 고려하였다.

주로 소프트웨어 제품에 요구되는 품질을 정량적으로 기술하기 위하여 ISO/IEC 9126을 채택한다[10]. ISO/IEC 9126은 기능성, 신뢰성, 사용성, 효율성, 이식성, 유지보수성의 외부 품질특성 6개와 27개의 내부 품질특성으로 구성된다[11]. 그러나 이는 소프트웨어 프로세스 전반을 아우르지 못하며, 소프트웨어 품질속성이 6개의 품질속성에 국한되는 단점을 지니고 있다. 소프트웨어 품질은 어떠한 시각으로 보는가에 따라 여러 가지 품질 모델이 있을 수 있으며 품질 모델이 달라짐에 따라 품질 요소도 달라진다[7]. ISO/IEC 9126의 세부 매트릭스 중 기능성의 부 특성으로 보안성을 평가하고 있지만, 평가기준의 범위가 좁고 보안기능의 일부분에 대한 평가기준이다. 따라서 보안성을 평가하는 기준으로 사용되기에 부적절하다[10]. 이와 같은 이유로 인하여 본 연구는 소프트웨어 프로세스 전반에 걸쳐 보안성을 고려할 수 있는 ISO/IEC 27001을 채택한다. 이는 물리적인 시스템뿐만 아니라 체계, 관리 등을 포함하여 보다 포괄적이다. 또한 ISO/IEC 27001은 체계적으로 위험을 관리하며, 낮은 수준의 기술적 보안 한계를 극복하는 장점을 지닌다.

4. ISO 27001

ISO/IEC 27001은 국제표준화기구(ISO: International Organization for Standardization) 및 국제전기기술위원회(IEC: International Electrotechnical Commission)에서 제정한 정보보호 관리체계에 대한 국제 표준이자 정보보호 분야에서 가장 권위 있는 국제 인증이다[12].

ISO 27001은 크게 관리적 보안, 기술적 보안, 물리적 보안의 3가지 통제 분야로 나뉘며, 관련 11개 영역, 133개의 항목이 존재한다[13].

ISO 27001을 사용할 경우 다음과 같은 효과를 기대할 수 있다. 우선, 조직의 필수적인 정보 자산을 보호할 수 있으며, 대외 경쟁력 유지 및 법규를 준수하게 된다. 뿐만 아니라 정보에 대한 위험을 체계적으로 관리할 수 있고, 낮은 수준의 기술적 보안 한계를 극복할 수 있다.

Table 1. Control object of ISO/IEC 27001

통제 분야	통제내용	통제 항목 수	세부 통제항목 수
관리적 보안	1. 보안정책	1	2
	2. 정보보호 조직	2	11
	3. 자산관리	2	5
	4. 인적자원 보안	3	9
	5. 정보보안 사고관리	2	5
	6. 업무 연속성 관리	1	5
	7. 준거성	3	10
기술적 보안	1. 통신 및 운영 관리	10	32
	2. 접근 통제	7	25
	3. 정보시스템 획득, 개발 및 유지보수	6	16
물리적 보안	1. 물리적 보안 및 환경적 보안	2	13

5. ISO 27001을 적용한 SP 인증의 보안성 향상 프로세스

SP 인증은 보안 측면을 보증해주지 않는다. 이 밖에도 다음과 같은 약점이 존재한다. 단계별 검토 수행이 제대로 이루어지지 않으며, 식별된 문제에 대한 분석이 이행되지 않는다. 또한 요구사항과 산출물에 대한 추적관리가 다소 부족하고, 설계 시 테스트 계획이 제대로 수립되지 않는다. 구현에 대한 구체적인 방법에 대한 표현문서도 부족하다.

본 절에서는 ISO 27001을 토대로 하여 SP 인증의 2등급을 획득한 개발 조직 및 기업의 프로세스 보안성 향상과 앞서 언급한 약점들을 보완할 수 있는 수행 활동 및 산출물을 제안한다.

5.1 제안 프로세스

Table 2. Process for security improvement based on ISO 27001

	계획	현황 분석	위험 분석	설계	구현	테스트
프로젝트 관리	계획단계 준비	ISO 27001 Gap Analysis	위험분석 / 평가	ISO 27001 통제항목 구현 계획 수립	구현단계 검토	ISO 27001 SOA 작성 (Statement of Applicability)
	프로젝트 계획	현황분석 단계 검토	위험분석 단계 검토	설계단계 검토		테스트단계 검토
	계획단계 검토					
개발		현황점검 / 분석		구조 설계	시스템 개발	통합 테스트
		요구사항 분석		상세 설계	시스템 통합	시스템 테스트
				테스트 설계		
지원	품질보증 계획수립	현황분석 단계 품질보증 검토	위험분석 단계 품질보증 검토	설계단계 품질보증 검토	구현단계 품질보증 검토	테스트단계 품질보증 검토
	계획단계 품질보증 검토					

5.2 제안 프로세스 단계별 활동 및 산출물

1) 계획단계

a) 계획단계 준비

- 이 활동은 프로젝트를 산정하여 프로젝트 계획서, WBS (Work Breakdown Structure), 프로젝트 비용 계획서를 작성하고, 방법론을 채택하여 방법론 계획서를 산출물로 한다.

b) 프로젝트 계획

- 프로젝트 계획을 수립하여 프로젝트 계획서와 정보보호 범위를 정의하여 인증 범위서를 산출물로 정의한다.

c) 품질보증 계획 수립

- 본 활동을 통해 품질보증 계획서를 작성한다.

d) 계획단계 품질보증 검토

- 계획단계 품질보증을 검토하여 계획단계 검토 보고서와 QA 보고서 작성 및 보고활동을 통해 QA 활동 보고서를 작성한다.

2) 현황분석단계

a) ISO 27001 Gap Analysis

- ISO 27001 Gap 분석 체크리스트를 작성한다.

b) 요구사항 분석

- 본 활동은 기능 요구사항 정의, 기술 요구사항 정의, 연동시스템 인터페이스 요구사항 정의, 보안 요구사항 정의, 운영 요구사항 정의의 활동으로 이루어지며, 각 활동별 요구사항 명세서와 요구사항 관리표, 요구사항 추적표를 산출물로 지정한다.

c) 현황분석단계 품질보증 검토

- 현황분석단계 품질보증을 검토하여 현황분석단계 검토 보고서와 QA 보고서 작성 및 보고 활동을 통해 QA 활동 보고서를 작성한다.

3) 위험분석단계

a) 위험분석/평가

- 위험/취약성 분석 및 평가를 통해 위험/취약성 리스트를 작성하고, 위험평가활동을 통해 위험분석 보고서를 만든다. 그리고 관리되어야 할 위험을 도출하여 위험분석 상세 결과 보고서를 작성한다.

b) 위험분석단계 품질보증 검토

- 위험분석단계 품질보증을 검토하여 위험분석단계 검토 보고서와 QA 보고서 작성 및 보고 활동을 통해 QA 활동 보고서를 작성한다.

4) 설계단계

a) ISO 27001 통제항목 구현 계획수립

- 통제항목에 따른 구현방안 계획을 수립하여 ISO 27001 통제항목 구현 계획서를 작성한다.

b) 구조 설계

- 본 활동에서는 ER Diagram을 작성한다.

c) 상세 설계

- 인터페이스, 코드, 화면, 데이터베이스, 프로그램을 설계하여 각각의 설계서를 작성한다.

d) 테스트 설계

- 테스트 계획을 수립하여 테스트 계획서를 작성한다.

e) 설계단계 품질보증 검토

- 설계단계 품질보증을 검토하여 설계단계 검토 보고서와 QA 보고서 작성 및 보고 활동을 통해 QA 활동 보고서를 작성한다.

5) 구현단계

a) 시스템 개발

- 데이터베이스를 구현하는 설계서를 작성하고, 그래픽을 구현하는 화면 설계서, 프로그램 구현의 산출

물로는 소스코드, 단위 테스트를 통해 단위 테스트 계획서와 단위 테스트 결과 보고서를 작성한다.

b) 시스템 통합
- 소프트웨어 통합을 수행하기 위하여 SVN을 산출물로 지정한다.

c) 구현단계 품질보증 검토
- 구현단계 품질보증을 검토하여 구현단계 검토 보고서와 QA 보고서 작성 및 보고 활동을 통해 QA 활동 보고서를 작성한다.

6) 테스트단계

a) ISO 27001 SOA 작성 : ISO 27001 SOA 보고서인 Statement of Applicability를 작성한다.

b) 통합 테스트 : 이 활동의 수행을 통해 통합 테스트 계획서와 통합 테스트 결과 보고서를 산출물로 작성한다.

c) 시스템 테스트 : 시스템 테스트 시나리오와 시스템 테스트 결과 보고서를 본 활동의 수행으로 작성되는 산출물로 지정한다.

d) 테스트단계 품질보증 검토 : 테스트단계 품질보증을 검토하여 테스트단계 검토 보고서와 QA 보고서 작성 및 보고 활동을 통해 QA 활동 보고서를 작성한다.

6. 결 론

소프트웨어 개발 기업 및 조직들의 소프트웨어의 품질 보증 및 향상을 위한 SP 인증이 전국적으로 확산되어 사용되고 있으나, SP 인증에서는 별도의 보안 속성에 대한 프로세스를 정의하고 있지 않다.

본 논문은 SP 품질 인증을 획득한 기업 및 조직들의 보안성을 향상시키기 위해 ISO 27001을 기반으로 SP 인증 프로세스의 보안성 향상 방향을 제시하였다. 보안 위협요소 검출이 가능하며, ISO 27001의 통제항목에 입각한 구현 계획을 수립하게 된다. 뿐만 아니라 SOA 적용성 보고서를 통해 보안 취약점에 대한 지속적인 관리가 가능하다. 따라서 SP 인증을 획득한 기업 및 조직들의 본 프로세스 적용으로 보안성 향상이 기대된다.

그러나 제시한 보안 프로세스에서 분석 단계 및 단계별 검토가 차지하는 비중이 크고, 이는 일일이 사람의 작업을 요하므로 프로젝트 수행 기간에 영향을 미친다. 그러므로 자동화 시스템이 적용된다면 SP 인증을 획득한 기업 및 조직들의 보안성 향상에 보다 많은 기여를 할 것이라 예측하며, 향후에는 분석단계 및 단계별 검토단계에서의 시스템 자동화에 대한 연구가 필요하다.

References

[1] H. S. Yang, D. H. Bae, “Standardization of Software Quality and Trend of Test Certification Technologies,” *KIISE*, Vol.23, No.3, pp.45-55, 2005.

[2] K. S. Lee, J. W. Kim and Y. E. Jung, “Software Quality Evaluation using Software Development Guideline,” *KIISE*, Vol.29, No.2, pp.121-123, 2002.

[3] El Emam, K., Jung, H.-W, “An empirical evaluation of the ISO/IEC 15504 assessment model,” *Quality control and applied statistics*, Vol.47, No.5, pp.583-586, 2002.

[4] Fusaro, P., El Emam, K., and Smith, B, “Evaluating the Interrater Agreement of Process Capability Ratings,” *Proceedings of the International Software Metrics Symposium*, Vol.4, pp.2-11, 1997.

[5] I. O. Song, “An Empirical Research on Software Process Model of Small Business for SP-Certirication,” *Master’s Thesis of SoongSil Graduate School*, 2010.

[6] TTA, “GS Certification,” 2013.

[7] W. S. Kim, J. W. Oh, K. H. Yoon, C. W. Lee, C. S. Wu, W. H. Jang and S. H. Lee, “A Reference Model for Software Quality Certification,” *KIISE*, Vol.28, No.2, pp.526-528, 2001.

[8] Jeffrey M. Voas, “Certification: Reducing the hidden costs of poor quality,” *IEEE Software*, Vol.16, No.4, pp.22-25, 1999.

[9] NIPA, “Quality Certification of SW Process,” 2011.

[10] J. M. Lee, “Investigation in Evaluation Matrix for Security Software Product,” *KIISE*, Vol.33, No.2, pp.427-432, 2006.

[11] C. D. Cho, “Effectiveness Proof through Case Studies of Software Process Quality Certification Standards,” *Master’s Thesis of ChungAng Graduate School*, 2011.

[12] http://ko.wikipedia.org/wiki/ISO/IEC_27001, 2013.

[13] ISO/ICE 27001, “Information technology Security techniques Information security management systems Requirements,” 2005.

윤 은 지

e-mail : yooneunji@dankook.ac.kr
2013년 단국대학교 컴퓨터과학과(학사)
2013년~현 재 단국대학교 컴퓨터학과 석사과정
관심분야 : Software Engineering, Software Process Certification

박 용 범

e-mail : ybpark@dankook.ac.kr
1991년 N.Y. Polytechnic University
Science & Engineering(Ph.D.)
1993년~현 재 단국대학교 컴퓨터과학과
교수
관심분야 : Intelligent Software Engineering,
Security Software