Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.4, Aug. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.4.933

정보보호 사전점검 활성화를 위한 점검항목 개선 연구*

최 주 영,[1†] 김 진 형,[2] 박 정 섭,[2] 박 춘 식[1‡]
[1]서울여자대학교, [2]한국인터넷진흥원

A Study on Improvement of Inspection Items for Activation of the Information Security Pre-inspection*

Ju Young Choi,[1†] JinHyung Kim,[2] Jung-Sub Park,[2] Choon Sik Park[1‡]
[1]Seoul Women's University, [2]Korea Internet & Security Agency

요 약

IT환경은 사물인터넷, SNS, 빅데이터, 클라우드 컴퓨팅 등으로 급변하고 있다. 이 기술들은 기존 기술에 새로운 기술이 추가되어 정보시스템 간의 복잡도를 증가시킨다. 그러므로 신규 정보통신서비스의 보안 기능 강화가 필요하다. 정보보호 사전점검은 신규 정보통신서비스 설계 단계부터 보안을 고려한 개발 단계를 제시하여 신규 정보통신서비스 제공자와 이용자에게 안정성 및 신뢰성 보장을 목표로 한다. 기존 '정보보호 사전점검(점검영역 22개, 통제항목 74개/세부항목 129개)'은 6단계(요구사항, 설계, 교육, 구현, 시험/테스트, 대응/사후)로 구성되어 있으며 실효성 검토를 위해 실제 정보시스템 개발 업체에서 파일럿 테스트를 수행하였다. 그 결과로 점검항목에 대한 개선 요구사항과 일부 점검항목의 재구성이 필요한 것으로 나타났다. 본 논문은 정보시스템의 사전예방이 목적인 '정보보호 사전점검'의 활성화를 위한 연구를 하였다. 그 결과로 요구사항과 보완사항이 반영된 '정보보호 사전점검(점검영역 16개, 점검항목 54개/세부항목 76개)'을 도출하였다.

ABSTRACT

IT environments such as IoT, SNS, BigData, Cloud computing are changing rapidly. These technologies add new technologies to some of existing technologies and increase the complexity of Information System. Accordingly, they require enhancing the security function for new IT services. Information Security Pre-inspection aims to assure stability and reliability for user and supplier of new IT services by proposing development stage which considers security from design phase. Existing 'Information Security Pre-inspection' (22 domains, 74 control items, 129 detail items) consist of 6 stage (Requirements Definition, Design, Training, Implementation, Test, Sustain). Pilot tests were executed for one of IT development companies to verify its effectiveness. Consequently, for some inspection items, some improvement requirements and reconstitution needs appeared. This paper conducts a study on activation of 'Information Security Pre-inspection' which aims to construct prevention system for new information system. As a result, an improved 'Information Security Pre-inspection' is suggested. This has 16 domains, 54 inspection items, 76 detail items which include some improvement requirements and reconstitution needs.

Keywords: Information Security Pre-Inspection, Security Development Lifecycle

접수일(2015년 6월 17일), 수정일(1차: 2015년 7월 29일, 2차: 2015년 8월 17일), 게재확정일(2015년 8월 17일)
* 이 논문은 2015학년도 서울여자대학교 컴퓨터과학연구소 교내학술연구비의 지원을 받았음.
† 주저자, jychoi@swu.ac.kr
‡ 교신저자,csp@swu.ac.kr(Corresponding author)

I. 서 론

2015 국가정보보호백서에서 2013년 국내 민간 사업체 응답자 중 3.7%는 신규 정보통신서비스 보안에 투자한 것으로 조사되었다. 투자 순서는 'SNS 보안', '모바일 보안', '클라우드 보안', '빅데이터 보안', '사물인터넷 보안' 순이다. 또한 향후 신규 정보통신서비스 보안에 투자 계획을 갖고 있는 사업체는 응답자 가운데 7.1%로 '모바일 보안', 'SNS 보안', '빅데이터 보안', '클라우드 보안', '사물인터넷 보안' 순으로 투자 계획이 있음을 보였다[1].

이는 신규 정보통신서비스(SNS, 빅데이터, 클라우드 컴퓨팅, 사물인터넷 등)가 출현하는 IT 환경은 이를 대응하는 보안 기능이 요구됨을 보여준다.

Fig.1.은 국내 사업체의 정보보호 제품 및 서비스 사용현황을 보여주고 있는데 대체적으로 사후대응에 대한 솔루션들이다[1]. 만약 사업체가 신규 정보통신서비스 보안에 투자한다면 사후대응 범주에 있는 정보보호 제품 및 서비스로 보안을 강화할 것으로 예상된다. 본 논문은 사후대응이 아닌 사전예방 측면에서 신규 정보통신서비스의 보안 강화를 연구한다.

신규 정보통신서비스는 일반적으로 조직의 운영 정보시스템과 연동하여 서비스를 제공한다. 신규 정보통신서비스 이용자는 안전성 및 신뢰성을 요구하고, 서비스 제공자는 조직 내 운영 중에 있는 정보시스템에 이관되었을 때 조직 전체의 정보시스템의 안전성 및 신뢰성이 보장되길 원한다.

이를 위해 한국인터넷진흥원은 신규 정보시스템의 설계 및 계획 단계에서 보안 취약점 정보를 분석하고 이를 고려한 소프트웨어 개발단계를 적용하도록 「정보보호 사전점검」권고제도를 시행하고 있다.

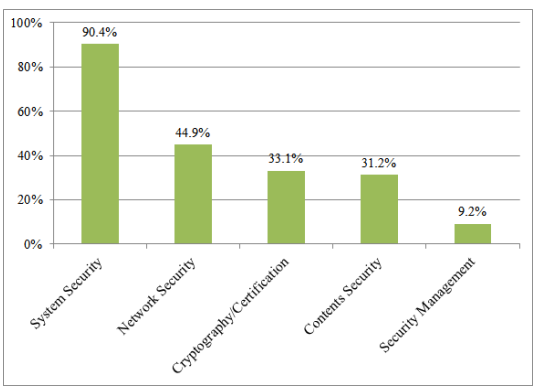

Fig. 1. Products and Service of Information Security (in 2013)

정부에서는 사이버 안심국가 실현을 목표로 예방 인프라 구축을 위하여 기존 인증(평가) 제도와 신규 인증(평가) 제도를 포함한 '사이버 검진'을 추진하고 있다. '사이버 검진'은 인증(평가) 대상에 따라 「정보보호관리체계(ISMS)[2]」,「정보보호 준비도 평가(SECU-STAR)[3]」, 「정보보호 사전점검」 등으로 구성한다.

본 논문은 2013년 발표된 「정보보호 사전점검」의 활성화를 위한 개선방안에 대하여 연구한다. 점검수행기관에서 파일럿 테스트 과정에서 얻어진 현업 실무자들의 요구사항과 사전점검의 실효성을 위한 보완사항을 반영한 개선된 新「정보보호 사전점검」을 제안한다.

Ⅱ장에서는 소프트웨어 개발단계에 보안요소를 추가할 경우 사후대응보다 사전예방이 효과적임을 제시한 관련 연구와 2013년 발표된 「정보보호 사전점검」을 간단하게 살펴본다. Ⅲ장에서는 활성화를 위한 요구사항 및 보완사항에 대한 개선방안을 정리하고, Ⅳ장에서는 개선방안을 반영한 新 「정보보호 사전점검」을 도출한다.

본 논문은 독자의 이해를 위해 기존 「정보보호 사전점검」에서 사용한 '통제항목/세부항목'의 명칭을 新 「정보보호 사전점검」에서 바뀐 '점검항목/세부항목'으로 통일하여 작성하였다.

II. 관련 연구

2.1 소프트웨어 개발단계 보안 방법론

NIST 소프트웨어 개발단계 보고서[4]는 소프트웨어 개발 5단계(요구분석-코딩-통합-베타테스트-제품출시)에서 동일 결함을 제거하는 비용 연구를 하였다. 동일한 단순결함이 발견된 제품을 각 개발 5단계에서 결함을 제거할 경우 비용의 차이가 있음을 보여준다. NIST 보고서는 동일한 결함에 대하여 '코딩'단계에서 결함을 제거하는 비용이 5배라면, '제품출시'단계에서 결함을 제거하는 비용은 30배임을 보여준다.

NIST 보고서에서 사용된 단순 결함요소가 정보보호 위협요소라 가정할 때, 위협요소 제거 비용은 정보시스템 개발 초기 단계에 투자할 경우 효과가 있음을 예상할 수 있다.

마이크로소프트사의 소프트웨어 개발 생명주기

(MS-SDL, Security Development Lifecycle)[5]는 소프트웨어 개발단계에서 취약점을 점검하는 도구이다. 마이크로소프트사는 SDL 적용 전(pre-SDL)과 적용 후(post-SDL)의 차이를 비교연구 하였다. 윈도우 XP(Vista)는 MS-SDL 적용 전/후 대비 소프트웨어 취약점이 119건에서 66건으로 45% 감소하고, MS-SQL Server는 SDL 적용 전/후 대비 소프트웨어 취약점이 34건에서 3건으로 91%감소하였음을 보여준다.

MS-SDL는 MS 관련 소프트웨어에 한정된 평가결과이지만 본 논문의 목표인 개발주기단계에 보안요소를 검증하는 절차는 비검증된 정보시스템보다 안정된 정보시스템을 만들 수 있는 가능성을 보여준다.

NIST SP 800-160[6]은 시스템 생명주기 표준문서(ISO/IEC 15288)를 참고한 '시스템 보안 엔지니어링 프로세스'를 제안한다. 11개의 프로세스는 보안요소를 강화한 내용으로 프로세스 단계별 시스템 보안 엔지니어링의 목적(Purpose)과 예상 결과(Outcome)를 정의한다. 또한 각 프로세스 단계에 보안 관련 작업(Activities)과 태스크(Tasks) 요소를 제시하므로 결과물을 예측할 수 있다.

NIST SP 800-160에서 제시한 작업과 태스크, 그에 따른 예측결과는 그 단계를 시행할 때 참고할 수 있는 가이드라인을 제공하므로 발주자 및 개발자는 점검 자료로 활용할 수 있을 것이다.

본 논문은 NIST SP 800-160 문서에서 두 가지를 접목하였다. 첫 번째, 11개의 시스템 보안 엔지니어링 프로세스와 6단계로 구성된 「정보보호 사전점검」을 비교하여 누락된 점검항목을 확인하는 과정을 진행했다[Fig. 2]. 두 번째, 「정보보호 사전점검」 6단계마다 자가 점검 할 수 있는 산출물 및 체크리스트가 필요함을 확인하고 이를 新「정보보호 사전점검」에 포함하였다.

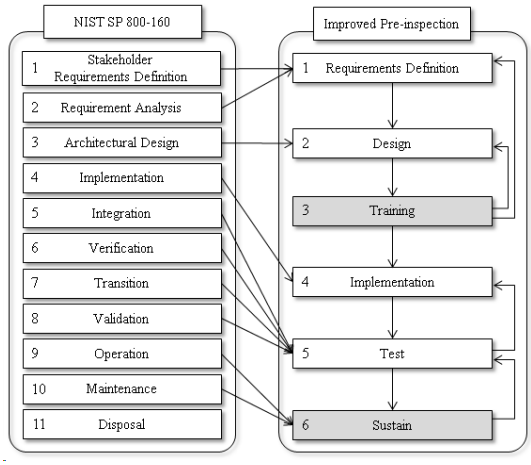

Fig. 2. Mapping table between NIST SP 800-160 and Improved Pre-inspection

新「정보보호 사전점검」은 각 단계별 독립적인 점검 수행이 가능하나 Fig. 2.에 음영 처리된 '3. 교육/훈련'과 '6.대응/사후' 단계에서 일부 결과물이 이전 단계에 영향을 줄 수 있다.

2.2 기존 「정보보호 사전점검」

「정보보호 사전점검」은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의2(정보보호 사전점검)를 권고제도로 신설(2012년 2월)하여 2013년 2월 18일부터 실행하게 되었다. 「정보보호 사전점검」 적용 대상은 일정규모(5억원이상)의 정보시스템 구축 등 정보통신서비스를 개발하고자 하는 정보통신서비스제공자 또는 전기통신사업자이다.

2014 국가정보보호백서[7]는 정보시스템 점검항목을 사전예방과 사후대응 두 분류로 나누고 사전예방은 「정보보호 사전점검」, 사후대응은 「정보보호관리체계(ISMS)」를 소개하고 있다.

이근호[8]는 국내외 사전점검 생명주기를 분석하여 사전점검의 6단계(정의, 설계, 교육, 구현, 테스트, 대응/사후)을 제시하였다. [8]의 연구에서는「정보보호 사전점검」의 추진 배경 중심으로만 서술하여 점검항목에 대한 자세한 설명이 부족하다. 이에 본 논문은 점검수행기관의 자료(점검영역 22개, 점검항목 74개/세부점검항목 129개)를 참고하였다.

기존 「정보보호 사전점검」의 문제점은 첫째, 점검항목이 중복되어 있다. 기존 3.교육(점검영역 3개, 점검항목 6개/세부점검항목 10개)의 점검영역은 '3.1 개발자 교육/훈련 관리, 3.2 개발자 교육/훈련 프로그램, 3.3 개발자 자격평가'로 구분되어 있다. 교육 단계 세부점검항목(10개) 요소를 분해하였을 때, 3.1 영역은 '교육/훈련 계획'에 대한 내용으로 3.3 영역은 '교육/훈련 프로그램 후 평가' 내용으로 재구성할 수 있다. 분해 및 재구성 과정은 교육단계 세부점검항목을 10개에서 4개로 중복된 점검항목 6개를 제거할 수 있다. 교육단계 뿐만 아니라, 각 점검단계의 요소는 분해 및 재구성을 통한 점검항목의 중복제거가 필요하다.

둘째, IT 서비스가 새롭게 등장할 때마다 설계와

구현 단계의 점검항목이 재구성 되어야한다. 신규 IT 서비스는 지속적으로 나타나는데 이를 반영할 때마다 기존「정보보호 사전점검」의 설계와 구현 단계가 전반적으로 재구성되는 어려움이 있다. 이를 해결하기 위해 설계와 구현 단계의 관계성을 재구성하고 탄력적으로 대응하기 위한 모듈화가 필요하다.

셋째, 점검 이행 여부를 판단할 수 있는 산출물에 대한 제시가 부족하다. 기존「정보보호 사전점검」은 점검 항목만 제시되어 점검대상업체에서 산출물 기준의 불분명으로 점검 준비에 애로사항이 발생하고, 점검수행기관에서 점검 지표의 부재로 점검수행평가 후 결과 집계의 어려움이 나타났다.

넷째, 이관 절차의 점검항목 누락되었다. 신규 IT 서비스가 조직 운영시스템에 이관할 때 이관절차 및 통제 등에 대한 점검항목이 필요하다.

III. 기존「정보보호 사전점검」의 개선 방안

기존「정보보호 사전점검」점검항목의 실효성 확보를 위해 점검수행기관은 공기업 및 사업체를 대상으로 파일럿 테스트를 수행하여 현업부서의 요구사항을 수렴하였다. 또한 점검수행기관 내부 구성원은「정보보호 사전점검」활성화 방안으로 점검항목을 재구성하는 보완사항이 나타났다. 다음은 도출된 요구

Table 1. Implementation of Improved Information Security Pre-inspection

		Domain	Inspection items(detail items)	
Implementation	(1) Required items	4.1 Information system implementation environment security management	4.1.1	Implementation environment security administrator (2)
			4.1.2	Implementation environment security management guideline
			4.1.3	Development tool security
			4.1.4	Development security verifying tool management
			4.1.5	Implementation environment periodic inspection
	(2) Selection of the implementation type	4.2 Network security implementation(Ref. 2.2.2)	4.2.1	Vulnerability management of network devices and network security devices
			4.2.2	Network security inspection conduct (2)
			4.2.3	Wireless communication range inspection (2)
			4.2.4	Blocking non-authorized wireless AP access
			4.2.5	VPN
			4.2.6	Traffic monitoring (2)
		4.3 Database security implementation(Ref. 2.2.3)	4.3.1	Database performance insurance (2)
			4.3.2	Data integrity
			4.3.3	Database security management
		4.4 Source code security implementation(Ref. 2.2.4)	4.4.1	Source code development security (2)
			4.4.2	Application user test
			4.4.3	Security verification via Execution code analysis
			4.4.4	Code signature verification
		4.5 Encryption and certification implementation(Ref. 2.2.5)	4.5.1	Encryption
			4.5.2	Certification
		4.6 User security implementation	4.6.1	User storage media security
			4.6.2	User system security
			4.6.3	Terminal registration, certification procedure and management methods
			4.6.4	Protection measure for responding terminal-malicious codes
			4.6.5	Mobile terminal management system

사항과 보완사항이다.

3.1 현업 「정보보호 사전점검」의 요구사항

기존 「정보보호 사전점검」은 국내[9,10], 국외[11-14]의 시스템개발 생명주기(SDLC)를 참조하여 영역과 점검항목을 최대한 반영하여 제안하였다. 이로부터 점검과정에서 중복되거나 불필요한 점검항목에 대한 수정이 요구되었다.

현 구현환경에서 발주자 및 개발자는 점검항목에 대한 부담을 가짐으로 개발 시 이를 적용할 가능성이 낮다. 그러므로 자발적으로 적용할 수 있는 점검항목 제공을 위한 간소화 작업이 요구되었다.

3.2 「정보보호 사전점검」 활성화를 위한 보완사항

「정보보호 사전점검」은 권고사항으로 개발단계 항목에 대한 명칭을 '통제(Control)'보다는 '점검(Inspection)'의 의미로 사용되어 '통제항목/세부항목'에서 '점검항목/세부항목'으로 명칭을 변경하였다. 다음은 新「정보보호 사전점검」의 보완사항을 기술한다.

3.2.1 구현단계 모듈화

'구현'단계는 '설계'단계에서 선택한 구현유형에 따라 점검항목이 달라진다. 예를 들어 '구현'단계는 새로운 정보통신서비스를 추가하거나 더 이상 사용하지 않는 정보통신서비스의 구현유형을 삭제할 수 있도록 탄력적으로 재구성이 필요했다. Table 1.의 '구현' 단계는 기본항목(Required items)과 선택항목(Selection of the Implementation type)으로 모듈화 하였다.

모듈화 기준은 '2.2 보안아키텍처 설계' 점검항목이며 (1)기본항목은 정보시스템 전체 구성 및 구현환경의 일반적인 보안요소를 설계한 '2.2.1 정보시스템 보안 아키텍처 설계'와 (2)선택항목은 정보시스템 구현유형에 따른 '2.2.2 네트워크 아키텍처 설계'에서 '2.2.6 암호화 및 인증 설계'까지로 분리하였다.

'4.1 정보시스템 구현환경 보안관리'는 '4.1.1 구현환경의 보안관리자'에서 '4.1.5 구현환경 주기적 점검'까지 일반적인 구현환경 보안요소를 점검한다.

신규 정보시스템은 요구사항 및 설계 단계에서 서비스를 위한 구현유형이 결정된다. 따라서 '구현' 단계에서는 결정된 구현유형만 점검하고 관련 없는 구현유형은 생략할 수 있도록 '정보시스템 구현유형에 따른 선택항목(4.2~4.6)'을 구성하였다.

3.2.2 산출물 및 체크리스트 제시

「정보보호 사전점검」은 발주자 및 개발자의 자율적인 점검과정 진행을 목적으로 한다. 그러나 기존 「정보보호 사전점검」은 평가지표의 부재로 점검수행에 어려움이 있었다.

이를 위해 신규 정보통신서비스를 기획하는 발주자 또는 개발자가 스스로 평가할 수 있는 도구를 제시하였다. 점검항목/세부항목에 준하는 산출물 및 체크리스트에 유도된 결과는 안전한 정보시스템 구축을 할 수 있도록 자가진단 도구로 활용할 수 있다. 도출된 산출물 및 체크리스트는 점검 대상 업체에게 점검 준비과정을 일목요연하게 정리한 가이드라인을 제시한다.

3.2.3 신규 정보시스템 이관 점검항목 추가

신규 개발된 정보시스템을 운영시스템에 이관하는 과정의 점검항목이 누락되어 '5.2 정보시스템 이관' 점검항목을 추가하였다. 이관 점검항목은 운영환경으로의 이관이 통제된 절차에 따라 이루어지는 것을 목적으로 한다.

정보시스템 이관에 대한 점검항목은 '5 시험/테스트' 단계에서 추가하였다. '5.2 정보시스템 이관' 점검항목은 다음 항목을 참고하였다.

- ISMS(11.2.1)-정보시스템 인수
- NIST800-160(TR-1)-시스템 안전한 전환 계획
- NIST800-160(TR-2)-시스템의 안전한 전환 수행

'5.2.1 정보시스템 이관' 점검항목을 통해 '정보시스템 이관 계획서'와 '정보시스템 이관 시 문제 대응

Table 2. Comparison table for Pre-inspection and Improved Pre-inspection

	Existing Pre-inspection			Improved Pre-inspection		
	Domain	Inspection #	Detail #	Domain	Inspection #	Detail #
Requirements Definition	2	9	17	2	6	9
Design	4	14	30	2	9	17
Training	3	6	10	1	2	4
Implementation	7	30	46	6	25	31
Test	3	5	9	2	5	5
Sustain	3	10	17	3	7	10
Total	22	74	129	16	54	76

방안'을 산출물로 명시하였다.

IV. 개선된「정보보호 사전점검」

본 Ⅲ장에서 제시된 개선 방안을 토대로 기존「정보보호 사전점검」 점검항목을 개선하고 점검항목에 대한 산출물 및 체크리스트를 도출하였다.

Table 2.은 기존「정보보호 사전점검」과 新「정보보호 사전점검」의 점검영역 수 , 점검항목 수, 세부항목 수를 비교하였다.

Table 3. Improvement of Information Security Pre-inspection

	Domain	Inspection items(detail items)	
Requirements Definition	1.1 Information Security requirements definition	1.1.1	Information System Information Security requirements definition
		1.1.2	Information Security compliance definition
		1.1.3	Information Security threats definition (2)
		1.1.4	Risk management measure establishment (3)
	1.2 Preliminary inspection plan	1.2.1	Implementing company evaluation
		1.2.2	Information Security inspection plan establishment for each development step of Information system
Design	2.1 Security management and evaluation when designing	2.1.1	Design security requirements (2)
		2.1.2	Security management for designing
		2.1.3	Development environment security design
	2.2 Security architecture design	2.2.1	Information system security architecture design (4)
		2.2.2	Network architecture design (2)
		2.2.3	Database architecture design (2)
		2.2.4	Source code security design
		2.2.5	Data security design (2)
		2.2.6	Encryption and authorization design (2)
Training	3.1 Developers education/training	3.1.1	Education/training Plan (2)
		3.1.2	Education/training Program (2)
Implementation	Ref. Table 1. (4.1~4.6)		
Test	5.1 Security inspection execution	5.1.1	Security setting inspection
		5.1.2	Vulnerability inspection
		5.1.3	Security inspection execution
		5.1.4	Measures establishment
	5.2 Information system transfer	5.2.1	Information system transfer
Sustain	6.1 Response procedure	6.1.1	Response procedure on security incidents
	6.2 Response system construction	6.2.1	Working consistency plan
		6.2.2	Change management
		6.2.3	Data Safety (2)
		6.2.4	Periodic Security Patch (2)
	6.3 Response/Post procedure	6.3.1	Incidents analysis and sharing
		6.3.2	Recurrence prevention (2)

이에 대한 검토 작업을 위해 「정보보호 사전점검」과 관련 있는 업계, 학계, 공공기관 전문가자문을 실시하였다.

Table 3.은 개선된 『정보보호 사전점검』(점검영역 16개, 점검항목 54개/세부항목 76개)이다. '4. 구현(4.1~4.6)'에 대한 점검항목은 3.2.2 구현단계 모듈화를 설명한 Table 1. 내용과 동일하므로 자세한 항목 정보는 Table 1.로 대체한다.

'3. 교육/훈련'은 '1.2 사전점검계획' 점검항목에서 교육/훈련에 대하여 사전 정의를 포함하고 '2.1 설계 시 보안관리 및 평가' 점검항목에서 교육/훈련을 계획하는 내용을 사전 설계하므로 연관성을 갖는다. '6.2 대응체계구축'은 침해사고 이후 '5. 구현'에 직접 또는 간접적으로 연관성을 갖는다.

본 논문은 점검항목 제시에만 초점을 둔 기존 『정보보호 사전점검』을 점검수행기관에서 본격적으로 시행하기에 앞서 요구사항과 보완사항을 도출하고 이를 개선하였다. 산출물의 부재로 통계적인 접근의 어려움은 본 논문에서 보완한 산출물 및 체크리스트가 적절한 집계 정보를 제공할 것이며 이어지는 점검항목 개선에 밑거름이 될 것으로 사려된다.

V. 결 론

개선된 『정보보호 사전점검』은 신규 정보통신서비스 발주자 및 개발자에게 소프트웨어 개발단계에서 고려해야 할 정보보호 요소를 제시하여 안전한 정보시스템 구축을 기대할 수 있다.

본 논문에서 도출된 자료는 발주자에게 신규 정보통신서비스 운영을 위한 업체 선정 과정에서 안전성 정보시스템 개발 평가지표로 활용되고, 개발자에게 안전한 구현환경을 자가 진단 할 수 있는 참고 자료가 될 것이다. 『정보보호 사전점검』의 N/A 평가방법에서 정량적 평가방법을 위한 추후 연구가 필요하다.

References

[1] 2015 National Information Security White Book, pp. 300, May 2015.

[2] Information Security Management System(ISMS), http://isms.kisa.or.kr/

[3] SECUrity Assessment for Readiness (SECU-STAR), The Korea Federation of ICT Organizations, Nov. 2014.

[4] NIST, "The Economic Impacts of Inadequate Infrastructure for Software Testing", May 2002.

[5] Security Development Lifecycle, http://www.microsoft.com/security/sdl/about/benefits.aspx

[6] NIST Special Publication 800-160, "Systems Security Engineering-An Integrated Approach to Building Trustworthy Resilient Systems", May 2014.

[7] 2014 National Information Security White Book, pp. 300, May 2015.

[8] Keun-Ho Lee, "A Study of Pre-inspection for Information Security in Information System", Journal of Digital Convergence, 12(2), pp.513-518, 2014.

[9] NIA-PAG(NIA's IT Project Auditing Guideline)v2.0-2013.08, NIA, 2013.

[10] PIA(Privacy Impact Assessment), KISA, 2011.

[11] DHS(Department of Homeland Security),Security in the Software Lifecycle Making Software Development Processes - and Software Produced by Them-More Secure, 2006.

[12] ISO/IEC DIS 27036-3, Guidelines for ICT supply chain security, 2013.

[13] NIST, Notional Supply Chain Risk Management Practices for Federal Information Systems, October 2012.

[14] ISA Security, NIST Cybersecurity Framework ISCI Response to Request for Information, ISASecure, 2013.

〈저 자 소 개〉

최 주 영 (Ju Young Choi) 정회원
1999년 2월: 서울여자대학교 컴퓨터학과 이학사
2003년 2월: 서울여자대학교 대학원 컴퓨터학과 이학석사
2012년 2월: 서울여자대학교 대학원 컴퓨터학과 이학박사
2011년 3월~현재: 서울여자대학교 정보보호학과 초빙강의교수
〈관심분야〉 정보보호관리체계, 정보보호 사전점검, 클라우드컴퓨팅 보안

사 진

김 진 형 (JinHyung Kim) 정회원
2006년 2월: 서울여자대학교 정보보호학과 공학사
2008년 2월: 서울여자대학교 대학원 컴퓨터학과 이학석사
2013년 2월: 서울여자대학교 대학원 컴퓨터학과 이학박사
〈관심분야〉 개인정보보호, 클라우드컴퓨팅 보안, 정보보호 사전점검

박 정 섭 (Jung-Sup Park) 정회원
1999년 2월: 한국외국어대학교 정치외교학과 학사
2001년 2월: 한국외국어대학교 경영정보학과 석사
2008년 3월~현재: 서울과학기술대학교 IT정책대학원 박사과정
〈관심분야〉 정보보호

박 춘 식 (Choon Sik Park) 종신회원
1995년: 일본동경공업대 공학박사
1982년~1999년: 한국전자통신 연구원 책임연구원
2000년~2008년: 국가보안기술연구소 책임연구원
2009년~현재: 서울여자대학교 정보보호학과 교수
〈관심분야〉 개인정보보호기술, 클라우드컴퓨팅 보안