Journal of The Korea Society of Computer and Information
Vol. 21 No. 11, pp. 79-83, November 2016

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2016.21.11.079

Information Security Activity of Analysis Phase in Information Security Model in Accordance with SDLC

Seong-Yoon Shin*, Tae-Wuk Lee**

Abstract

In this paper, we define four levels of analysis, design, implementation, and testing of the configuration of the development phase by S/W development life cycle. In particular, it dealt with the stage of the analysis phase to prepare an information system developed intensively. Details of the derivation of the information security requirements, it can be seen that comes from the perspective of confidentiality, integrity, availability and accountability, etc. It dealt with from the first manifestations of the projects planning to final planning to establish information security in activities of the Information Security requirements. As an example exhibited by assessing the information security analysis phase activities of S corporations, it can be seen that the improved sales rise in information security activities.

▸ Keyword : S/W Development Life Cycle, Analysis Phase, Confidentiality, Integrity, Accountability

I. Introduction

정보시스템을 개발 할 때에 정보보호의 반영과 구현에 대한 요구사항들이 매우 많아지고 높아지고 있으며, 정보시스템을 구축한 후 정보보호를 염두 해두고 이를 고려하는 추가적인 방식보다는 정보시스템의 분석, 설계, 그리고 구현하는 과정 중에 정보보호를 반영하는 임베디드 방식이 비용 면에서 매우 효과적이고 안전하다. 그리고 2002년 7월에 개정된 OECD 정보보호 가이드라인을 보면 정보시스템 및 네트워크 설계·구현 단계부터 정보보호를 고려하도록 권고 하고 있다.

정보보화 활동과 관련된 연구로는 인터넷 사용자를 대상으로 안전한 정보보호 활동을 이끌 수 있는 선행 요소들을 실증적으로 탐색하기 위하여 수행된 연구[1]와 한국의 정보보호 위원회의 활동이 정보보호를 위한 거버넌스 구현과 정보통신 보안효과에 끼치는 영향을 확인하는 연구[2]가 있다. 또한 기업 내부의 정보보호 담당자들을 대상으로 조직 내부의 정보보호 담당자의 보안전담 업무수행 비중과 조직의 정보보호 수준 등 현상을 이해하고 이들 간의 상관관계의 분석과 영향도를 분석한 연구[3], 중소기업체의 정보화 수준을 분석함에 있어서 개개의 개인정보보호와 관련한 활동들을 어떻게 평가할 수 있는가에 대하여 중점을 둔 연구[4], 일반적 관리활동의 하나로써 개인의 정보보호를 수행하기 위한 관리를 거버넌스 측면에서 더 좋게 만들고자 개인 정보보호관리 모델을 제시하고 이것과 연관된 개념 및 수행방안에 대해서 제시한 연구[5], 국내의 정보보안솔루션의 보안성을 지속시키기 위한 서비스 현황을 분석하고, 정보보안솔루션의 특징 및 특성을 생각하여 보안성을 지속시키는 서비스 대가가 반영될 수 있는 정책적 방안을 제안한 논문[6], 그리고 전략적인 관점, 관리적/운영적인 관점, 기술적인 관점 등 다차원적인 관점에서 믿을만한 보안 거버넌스 관리를 할 수 있도록 사람의 인적측면이 고려된 보안 거버넌스 프레임워크 개발에 관한 연구[7] 등이 있었다.

또한 개발 단계별 정보보호에 관한 연구로는 도서관 개인정

• First Author: Seong-Yoon Shin. Corresponding Author: Tae-Wuk Lee
*Seong-Yoon Shin(s3397220@kunsan.ac.kr), School of Computer Information & Communication Engineering, Kunsan National University.
**Tae-Wuk Lee(twlee@knue.ac.kr), Dept. of Computer Education, Korea National University of Education.
• Received: 2016. 10. 14, Revised: 2016. 10. 23, Accepted: 2016. 11. 22.

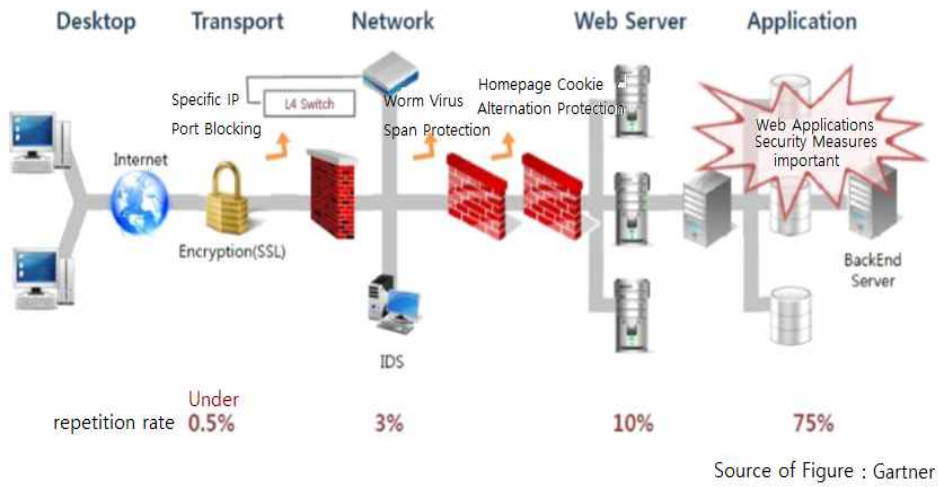

Fig. 1. Web Hacking Invasion Report of Gartner

보 가이드라인(안)을 제안하여 도서관 종류를 구분하지 않고 어느 도서관에서나 적용 가능하도록 하였으며 개개 도서관은 이 가이드라인(안)을 기반으로 도서관의 현실에 맞게 교정하여 사용할 수 있도록 한 연구[8], 원자력발전소와 연관된 규제요건과 기술표준문서를 바탕으로 원자력발전소의 S/W 구축 생명주기(SDLC) 단계별로 사이버보안 활동과 평가 항목들을 도출하여 S/W 구축 생명주기 단계별로 사이버보안 평가가 가능한 방법을 제시한 논문[9], 그리고 공공기관들의 정보시스템 운영 단계에서 필요한 개인정보보호 관점의 운영감리 점검 항목을 개발한 논문[10]이 있다.

그림 1은 가트너의 웹 해킹 침해 보고서(2012년도)로서 Application에서는 거의 75%대의 침해 비율을 보였다. 이것은 다시 한 번 S/W 개발 보안의 필요성은 웹사이트 공격의 약 75%가 응용프로그램(SW)의 취약점을 악용하여 해킹을 수행했다는 것을 증명하는 것이 되었다.

논문의 1장에서는 본 연구의 서론 및 관련연구를 살펴보고, 2장에서는 개발 단계의 정보보호 모델에 대하여 살펴보며, 3장에서는 분석단계의 정보보호 활동들을 정리하며, 4장에서는 회사에서 이를 구현한 예를 들어 평가 결과와 매출에 미친 영향 등을 살펴보고, 그리고 5장에서는 본 논문의 결론을 맺도록 한다.

II. Information Security Model of Development Phases

S/W 구축 생명주기별 개발 단계의 구성은 개발 방법론에 따라서 조금의 차이가 있으나 기본적인 요소들은 유사하다. ISO 표준, 국내 표준, NIST, 그리고 KISA의 자료 등에 따라서 개발의 기본 단계를 분석, 설계, 구현, 시험의 4단계로 정의하였다. 그리고 각 단계에 따른 13개의 파생되어 도출된 정보보호 활동을 기본으로 하였다. 그림 2과 같이 한국정보보호 진흥원의 『정보시스템 구축단계별 정보보호 가이드라인』에서 제시한 방법론 모델을 기본으로 하고 있다.

먼저 분석 단계는 정보시스템의 개발을 사전에 준비하는 단계로서 다음과 같은 순서대로 수행된다.

(1) 프로젝트의 수행 계획
(2) 시스템 개요와 특성 정의
(3) 정보보호의 현황 분석
(4) 정보보호의 요구 분석
(5) 위험평가 수행
(6) 정보보호의 계획 수립

다음은 설계 단계로서 분석단계에서의 요구사항이 정보시스템으로 구현되기 위해 분석 및 해석되고 조금 더 구체화되는 과정으로 다음과 같은 순서대로 수행된다.

(1) 정보보호의 설계
(2) 정보보호의 테스트 계획 수립

다음은 구현 단계로서 설계 단계에서 세운 정보보호 아키텍처가 구현 단계에서 확실히 이행되는지를 파악하는 것이 필요하다, 이 같은 구현은 네트워크, 서버, 어플리케이션, 데이터베이스, 그리고 클라이언트 각 영역에서 이루어지게 되며 다음과 같은 순서대로 수행된다.

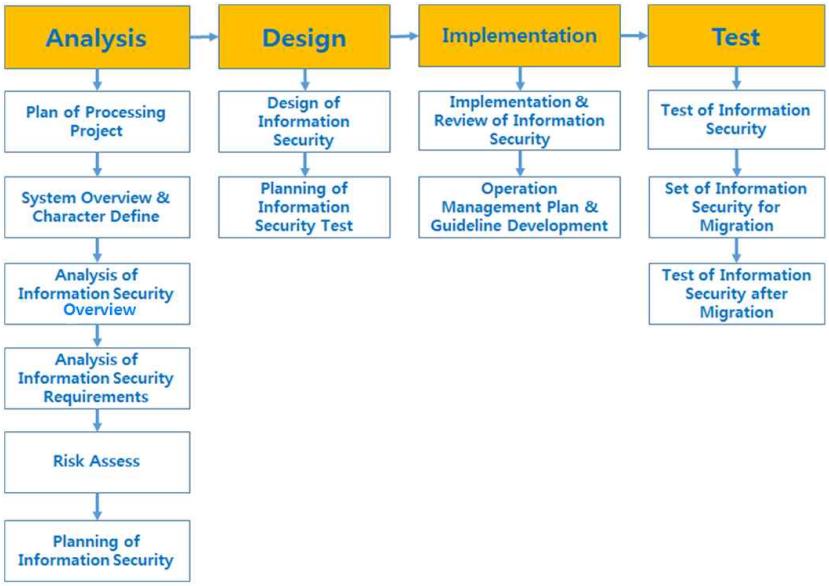

Fig. 2. Guideline of Information Security(SDLC)

(1) 정보보호의 구현과 검토
(2) 운영관리계획과 지침 개발

다음은 시험 단계로서 현재 개발이 완료되어 있는 정보시스템이 정보보호의 요구사항을 충족하는지 정보보호의 시험 및 이관에 대한 정보보호의 설정과 이관 이후의 정보보호의 시험 활동이 수행되며 다음과 같은 순서대로 수행 된다.

(1) 정보보호의 시험
(2) 이관을 위한 정보보호 설정
(3) 이관을 한 이후 정보보호 시험

III. Information Security Activity of Analysis Phase

SDLC 중에서 분석단계는 정보시스템의 개발을 준비하는 단계로서 정보보호 활동도 시작과 함께 수행되어야 한다. 분석단계에서는 정보기술 체계의 분석과 사용자의 요구 사항 도출 및 예측되는 위험 요소에 대한 평가도 함께 수행되어야 한다.

정보시스템을 개발할 때 일반적으로 정보보호의 요구사항은 기밀성, 무결성, 가용성, 그리고 책임 추적성 등의 관점에서 나온다. 자세한 정보보호 요구사항의 내용은 아래와 같다.

기밀성은 정보시스템 내부의 비밀정보를 분류, 정보시스템 내부의 기능에 대한 제한 등을 포함한다.

무결성은 정보시스템 내부의 정보를 변경할 수 있는 개인이나 업무의 식별, 정보시스템 자체의 무결성, 정보시스템의 변경 기능에서의 무결성 보장 등을 포함한다.

가용성은 정보시스템의 모든 구성요소의 가용성 요구사항을 식별할 필요가 있고, 정보시스템 구성요소간의 의존성과 상호작용을 파악하고 네트워크 등의 인프라의 가용성 요구사항을 식별해야 한다.

책임 추적성은 사용자 식별 및 인증과 정보보호의 사고를 조사할 때 필요한 정보를 제공하기 위해 감사에 대한 요구사항을 포함한다. 위험평가의 경우에서, 개발과정 중의 위험평가는 아직 대상 정보시스템이 구현되기 이전 상태이므로 취약성 평가에 의미가 없으므로 위험평가는 예상되는 위협을 바탕으로 이루어진다.

분석단계에서 정보보호에 대한 모든 대책이 요구사항에 반영되고 모두 다 설계되고 구현될 수는 없으므로 개발 전 과정에 걸쳐 추적이 가능하도록 해야 하며, 그 다음 운영단계에까지 대응 전략을 수립할 필요가 있다.

분석단계의 정보보호 활동 중 첫 번째는 프로젝트 수행 계획의 명시이다. 여기에선 단계별 정보보호 관련 수행 작업 내역을 명시하고, 일정 계획을 명시하며, 정보보호 작업을 수행할 담당자들 및 책임과 역할을 명시해야 한다.

두 번째로 해야 할 것은 시스템 개요 및 특성 정의이다. 여기에선 정보시스템의 정확한 명칭과 기본기능을 정의하고 정보시스템에 책임이 있는 조직의 이름, 역할 등을 정의해야 한다. 그리고 정보시스템 목적 및 사용자 권한을 정의하고 시스템 전체

의 아키텍처, 인터페이스 및 운영환경을 정의하며 시스템 간 연계 및 연결 방식의 정의해야 한다.

세 번째로 해야 할 일은 정보보호 현황 분석이다. 이 단계에서는 기존 정보보호 환경을 분석하고 개발할 정보시스템에 영향을 미칠 수 있는 관리적, 물리적, 기술적 정보보호 현황을 조사 및 분석해야 한다.

네 번째로 해야 할 일은 정보보호 요구 분석이다. 여기에선 제안 요청서에 제시된 정보보호 요구들을 조사하고 법적, 내부 정책적 정보보호 요구들을 조사해야 한다. 또한 업무, 정보보호 담당자 및 IT 관련 담당자 등으로부터 정보보호 요구들을 조사해야 하고 정보보호 요구사항들을 영역별로 분류하여 정리한다.

다섯 번째로 해야 할 일은 위험평가이다 위험 평가에서는 위험평가 대상 정보시스템의 범위를 정의하고, 예상되는 위협들을 정의하며, 위협발생 빈도를 정의해야 한다. 그리고 위협발생 시 예상 피해 및 영향도 정의하고, 정보보호 위험도를 예측산정하며, 목표주준에 따른 수용 가능한 위험 수준을 정의해야 한다. 또한 위험 및 그에 따른 잔여 위험에 대응하기 위한 대책을 선정하고, 정보보호 요구사항에 대한 최종적인 정의 및 명세화를 수행하며, 요구사항의 문서화 및 이의 추적 가능한 문서화를 수행하는 일이다.

여섯 번째로 해야 할 일은 정보보호 계획 수립이다. 이 계획은 앞의 첫 번째부터 다섯 번째까지의 활동에 대한 이행계획을 포함하는 정보보호 계획을 수립하는 것이다.

IV. Examples of Implementation

본 논문에서는 S사를 대상으로 분석단계의 정보보호를 구현하였다. 일반적으로 정보시스템을 개발할 때 나오는 기밀성, 무결성, 가용성, 그리고 책임 추적성 등의 관점에 대한 요구사항들을 정밀 분석하였다. 분석단계의 정보보호 활동인 프로젝트 수행 계획의 명시부터, 시스템 개요 및 특성 정의, 정보보호 현황 분석, 정보보호 요구 분석, 위험평가, 그리고 마지막으로 정보보호 계획 수립까지의 활동을 최종적으로 평가한 결과는 그림 3와 같은 결과가 나타났다. 그림 3의 결과는 기밀성, 무결성, 가용성, 그리고 책임 추적성 등의 관점에서 정보보호 활동을 추가하여 나타나는 보안성이 더 증가하는 것을 알 수 있다.

정보시스템을 개발 할 때 분석단계의 정보보호 활동을 추가하여 수행한 결과 기밀성, 무결성, 가용성, 그리고 책임 추적성 등이 50% 정도 상승한 것으로 나타났다.

그리고 그림 4는 분석단계의 정보보호 활동을 추가하여 평가한 매출의 실적이다. 이 매출 실적 또한 소폭으로 상승한 것으로 나타났다.

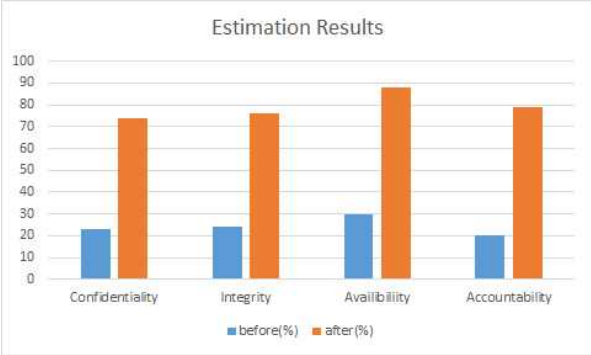

Fig. 3. Estimation Results

Fig. 4. Sales Results

V. Result

본 논문에서는 S/W 구축생명주기별 개발 단계의 구성을 개발 방법론에 따라서 분석, 설계, 구현, 그리고 시험의 4단계로 정의하였고 13개의 파생되어 도출된 정보보호 활동을 기본으로 하였다. SDLC 중에서 분석단계는 정보시스템의 개발을 준비하는 단계로서 정보기술 체계의 분석과 사용자의 요구 사항 도출 및 예측되는 위험 요소에 대한 평가도 함께 수행하였다. 정보보호의 요구사항은 도출은 기밀성, 무결성, 가용성, 그리고 책임 추적성 등의 관점에서 하였다. 분석단계의 정보보호 활동 중 첫 번째인 프로젝트 수행 계획의 명시부터 마지막 정보보호 계획 수립까지를 다루었다. 그리고 S사의 분석단계의 보안 요구사항을 구현하여 전체적인 시스템의 분석과 매출의 향상도를 평가하였다.

본 논문은 SDLC 중에서 분석단계의 개발을 철저히 준비하고 기밀성부터 추적성까지 정보보호 활동을 추가하면 정보보호 시스템을 개발 할 때 보다 더 효율적이며 매출 실적 또한 상승

한다는 것을 나타내는 매우 중요한 연구임을 알 수 있다.

REFERENCES

[1] Myoung-Yong Um, Moon-Ki Rhee, Tae-Ung Kim, “Empirical Study on Internet Users'Information Privacy Concerns and Information Protection Behavior,” J. of The Korean Association of Computer Education, Vol. 18, No. 1, pp. 69-79, Jan. 2016

[2] Kunwoo Kim, Jongduk Kim, “A study on effects of implementing information security governance by information security committee activities, ” J. of The Korean Institute of Information Security & Cryptology, Vol. 25, No. 4, pp. 915-920, Aug. 2015

[3] Dong-Keun Choi, Mi-Sun Song, Jong In Im, Kyung-Ho Lee, “Study the role of information security personnel have on an organization's information security level, ” J. of The Korean Institute of Information Security & Cryptology, Vol. 25, No. 1, pp. 197-209, Feb. 2015

[4] Byung-chul Kim, “The SME Informatization Level Analysis and Design for Privacy,” J. of The Digital Convergence, Vol. 13, No. 2, pp. 121-126, Feb. 2016

[5] Chang-Soo Moon, Sun-Hyung Kim, “A Study on Advanced Model for Personal Information Security Management,” J. of KIIT, Vol. 13, No. 1, pp. 93-99, Jan. 2015

[6] Yeon-ho Jo, Yong-pil Lee, Jong-in Lim, Kyoung-ho Lee, “A Study on Policy for cost estimate of Security Sustainable Service in Information Security Solutions,” J. of The Korean Institute of Information Security & Cryptology, Vol. 25, No. 4, pp. 905-914, Aug. 2015

[7] Hyojik Lee, Onechul Na, Soyong Sung, Hangbae Chang,“ A Design on Security Governance Framework for Industry Convergence Environment,” Journal of the Korea Convergence Society, Vol. 6, No. 4, pp. 33-40, Aug. 2015

[8] Yonghee Noh, Tae-Kyung Kim, “A Study on Developing Guidelines for Personal Information Protection in Library,” J. of Korea Society for Information Management, Vol. 32, No. 2, pp. 21-61, Jun. 2015

[9] Dal-mi Seo, Ki-Jong Cha, Yo-Soon Shin, Choong-Heui Jeong, Young-Mi Kim, “Assessment Method of Step-by-Step Cyber Security in the Software Development Life Cycle,“ Journal of The Korea Institute of Information Security & Cryptology, Vol. 25, No. 2, pp. 363-374, Apr. 2015

[10] Dae-Ha Park, Sang-Nyeong Yoo, Heung-Youl Youm, “Development of Information System Operational Audit Checklist for Personal Information Protection in Public Organizations,” Journal of Security Engineering, Vol. 12, No. 1, pp. 47-64, Feb. 2015

Authors

Seong-Yoon Shin received his M.S. and Ph.D degrees from the Dept. of Computer Information Engineering of Kunsan National University, Kunsan, Korea, in 1997 and 2003, respectively. From 2006 to the present, he has been a professor in the same department. His research interests include image processing, computer vision, and virtual reality.

Tae Wuk Lee received the B.S. degree in Science Education from Seoul National University in 1978 and M.S. and Ph.D. degrees in Computer Science and Computer Education from Florida Institute of Technology, U.S.A. in 1982 and 1985, respectively. Dr. Lee is currently the Professor of the Department of Computer Education at Korea National University of Education, Korea since 1985. He is interseted in Computer Science Education and Knowledge Engineerings.