http://dx.doi.org/10.14400/JDC.2014.12.2.513

정보시스템의 정보보호를 위한 사전점검에 관한 연구

이근호
백석대학교 정보통신학부

A Study of Pre-inspection for Information Security in Information System

Keun-Ho Lee
Division of Information Communication, Baekseok University

요 약 IT기술의 발전에 따라 다양한 신규 IT서비스가 생겨나고 있다. 신규 IT 서비스는 이용자의 서비스 접근의 편의성을 제공하나 네트워크와 복합 단말기 사용 등 정보시스템의 복잡도가 증가하고 있어 다양한 보안에 대한 위협과 취약성이 증가하고 있다. 정보시스템에 대한 안전성을 확보하기 위하여 정보통신 서비스 구축단계에서부터 정보보호 취약점 분석 등을 통해 사전에 취약점을 제거하고 정보보호 대책을 수립하여 적용하였는지에 대한 점검 활동에 대한 제도를 마련하고 있다. 본 논문에서는 정보시스템에 사전점검 방법에 대한 각 나라별 소개와 추진현황에 대해서 살펴본다. 한국인터넷 진흥원에서 추진하고 있는 사전점검 방법에 대한 추진 방향과 안전성을 확보하기 위한 활성화 방향에 대해서 제안한다.

주제어 : 정보시스템, 사전점검, 시큐어코딩, 보안, 라이프사이클

Abstract According to the development of IT technology, various new technologies are being produced. As the complexity of the information system like using the network and convergence devices is increasing, threat and vulnerability against various security problems are increasing even though new IT services provide the convenience of users' accessibility to services. In order to secure the safety of information system, the weakness is being removed through the information protection vulnerability analysis starting from information and communication service construction stage and the system is being prepared for pre-inspection activities about whether the information protection measures were established and applied. In this paper, introduction and current status of each country about advanced check-up systems in the information system are to be identified. Progress direction about the advanced pre-inspection system which is driven by Korea Internet Security Agency and its activation plan to secure the safety are to be suggested.

Key Words : Information System, Pre-inspection, Secure Coding, Security, 라이프사이클

Received 15 January 2014, Revised 16 February 2014
Accepted 20 February 2014
Corresponding Author: Keun-Ho Lee(Baekseok University)
Email: root1004@bu.ac.kr

ISSN: 1738-1916

1. 서론

IT 기술을 통한 다양한 신규 IT서비스가 제공되어 지면서 정보시스템 관리에 대한 중요성이 대두되고 있다. 이러한 신규 IT 서비스를 위한 정보시스템에 대한 많은 취약점과 보안위협요소가 새롭게 도출되고 있으며, 사회적으로 큰 영향을 미치는 보안사고가 급증하고 있다. 특히 신규 IT 서비스는 이용자의 서비스 접근 편의성을 제공하나 무선 네트워크나 복합 단말기 사용 등 정보시스템의 복잡도의 증가로 인해 많은 보안 위협요소와 취약점이 증가하고 있다. 특히 다양한 유형의 침해사고의 발생 가능성이 매우 커지고 있는 상황이다. 하지만, 이에 상응하는 예방적인 차원에서의 선행 투자는 거의 미흡한 실정이며, 서비스 제공을 위한 정보시스템의 취약점 발견 및 수정에 소요되는 비용이 운영단계에서는 설계단계 대비 60~100배 증가하는 것을 알 수 있다[1,2,3,9].

비용의 낭비를 줄이기 위해서는 정보통신망의 구축 또는 정보통신서비스의 제공 이전에 계획 및 설계 등의 과정에서 정보보호를 고려하여 필요한 조치를 취하거나 계획을 마련하는 작업을 통해 비용을 절감할 수 있다. 정보보호 사전점검에 대한 제도도입 관련 법으로는 정통망법 제 45조 2의 정보통신 서비스 제공자는 새로이 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획 또는 설계에 정보보호 관한 사항을 고려하여야 하고, 정보통신서비스 또는 전기통신사업을 시행하고자 하는 자에게 대통령으로 정하는 정보보호 사전점검 기준에 따라 보호조치를 하도록 권고하고 있다.

사전점검은 국내의 정보시스템 감리, 개인정보영향평가, 전자금융 보안성 심의 등과 국외의 DHS Security in the Software 라이프사이클, ISO27036-part3, MS SDL, NIST National SCRM, ISA Security-SDLA의 제도가 있다.

사전점검은 국내외 7개의 사전점검 라이프사이클 분석을 통해서 6단계의 라이프 사이클로 안을 도출하고 있다[9].

본 논문에서는 사전점검에 대한 국내외 현황을 살펴보고, 국내외의 라이프사이클과 특징을 비교 분석하고, 한국인터넷진흥원(KISA)에서 고려하고 있는 사전점검에 대한 진행 상황을 소개한다. 사전점검이 활성화되기 위한 개선 방안에 대하여 제안한다.

2. 사전점검 현황

2.1 국내 사전점검

– 정보시스템 감리 기준(2012)

정보시스템감리의 경우 정보 시스템의 감리의 업무 범위, 절차 및 준수 사항 등 감리를 하기 위한 사항을 정하는 목적으로 진행이 되고 있다. 정보시스템 구축 및 운영에 관한 사항을 종합적으로 점검하고 문제점을 개선하는 제도이다. 제도에 대한 라이프사이클은 요구분석, 분석/설계, 구현, 시험으로 구성되어 있다.

요구분석의 경우 운영환경 분석, 사용자 요구사항, 시스템 보안 요건, 구성요소 검증, 아키텍처 수립, 현행 업무 분석, 운영시스템 업무 분석, 사용자 요구사항, 응용시스템 모델링, 사용자 접근통제 보안, 데이터 식별, 데이터 현황분석, 데이터의 흐름, 데이터베이스설계, 데이터 모델링, 엔티티/프로세스간의 관계, 접근권한 통제의 내용을 포함한다.

분석/설계의 경우 상세 보안설계, 설치 검증 계획, 업무기능 상세 설계, 사용자 인터페이스 설계, 내외부 시스템에 대한 인터페이스 설계, 사용자 접근 통제 보안에 대한 설계, 응용 시스템 테이블 설계, 테이블과 업무규칙 정의, 공통 코드 설계, 데이터베이스 성능 설계, 데이터 접근 권한 통제 설계, 데이터베이스백업 복구 계획, 초기 데이터 구축 계획, 기존 데이터 전환 계획을 포함한다.

구현의 경우 시스템 도입 설치, 시스템 구성 요소 검증, 시스템 시험 계획, 인터페이스 편의성, 내외부 시스템 인터페이스, 사용자 접근 통제 보안, 단위 시험 수행, 통합 시험 계화 테이블간의 업무 관계, 성능 고려한 데이터베이스 구현, 설계에 따른 접근 권한 통제, 데이터베이스 접합성을 포함한다.

시험은 운영환경 준비 반영, 통합 시험 계획 실시, 시스템 완전성 무결성, 시험 계획 실시, 성능 가용성, 보안성 검증, 관리 개선, 시스템 최적화, 사용자 운영 지침서 작성, 사용자 인수 시험, 운영에 필요한 설치 배포, 초기 데이터 구축 전환, 업무 시스템 전환, 최종 사용자 승인을 포함한다[9].

– 개인정보 영향 평가

개인정보 영향평가(PIA:Privacy Impact Assement)는 개인정보를 활용하는 새로운 정보시스템의 도입이나 개

인정보 취급이 수반되는 기존 정보시스템의 중대한 변경 시 동 시스템의 구축, 운영, 변경 등이 프라이버시에 미치는 영향에 대하여 사전에 조사 예측 검토하여 개선 방안을 도출하는 체계적인 절차 방법을 말한다. 시스템 구축 변경 등을 완료하기 이전에 사전적 평가 수행을 통해 동 사업의 시행이 국민의 프라이버시에 미치는 중대한 영향을 사전에 파악하고 그 영향을 줄이거나 없앨 수 있는 방안을 모색하는 방법이다. 개인정보 영향 평가 수행 시기는 시스템 개발 단계에서 시스템 분석, 시스템 설계에서 사전분석, 위험분석 및 평가, 개선계획 도출 및 보고서 작성 부분이다. 사전 분석 단계에서는 영향평가 필요성 검토, 영향평가 수행 주체의 선정, 평가계획 수립의 내용이 포함된다. 개인정보 관리현황 분석에서는 평가자료 수집, 개인정보 흐름분석, 개인정보 침해요인 분석 및 개선방안 도출 및 위험도 산정이 포함된다. 영향평가 결과 정리 단계에서는 개선계획 수립, 보고서 작성을 포함한다[9].

– 보안성 심의

전자금융감독 규정 제 36조에 보안성 심의의 제도는 사업 계획 단계에서 금융감독원장에게 보안성 심의를 요청하도록 되어 있다. 사업 계획 단계는 전산실을 신규로 설치 이전하거나 재해복구 센터를 구축할 때, 외국 금융기관의 전산시설에 대한 해외 설치 이전 및 공동 이용을 하는 경우, 전자금융거래 안전성 확보를 위하여 금융감독원장이 필요하다고 인정하는 경우가 해당된다[9].

– 정보기술부문 실태평가

전자금융감독규정 제 58조, 세칙 제 3장에 의하면 금융감독원장은 금융기관의 정보기술부문의 건전성 여부를 감독하고, 성격 및 규모 정보기술 부분에 대한 의존도 등을 감안하여 규정된 금융기관에 대하여 검사를 통해 정보기술 부분 운영 실태플 평가하고 그 결과를 경영실태 평가 등 감독 및 검사업무에 반영하여야 한다. 정보기술부분 실태평가는 검사기준일 현재 평가대상기관의 정보기술 부문 실태를 IT감사, IT경영, 시스템 개발 도입 유지보수 IT서비스 제공 및 지원의 부문별로 구분 평가하고 부문별 평가 결과를 감안하여 종합평가해야 한다[9].

2.2 국외 사전점검

– DHS Security in the Software Lifecycle

국토안보국(DHS)은 생명주기 프로세스 관련 방법론, 모델, 모범사례를 기술하고 있다. 그 결과 소프트웨어 악용 결함을 방지하는 지원 기술에 대해 설명하고 있다. 또한 소프트웨어 개발 라이프 사이클의 개념화 단계의 산출물이 보안향상에 도움이 되는 요소로서의 통합에 대해 설명하고 있다. 개념, 구현 및 소프트웨어의 생산에 관련된 보안 문제에 대한 인식과 이해를 증진, 소프트웨어 개발 프로세스의 인식 및 지원방법에 기여 또는 소프트웨어 보안 손실 방지에 도움을 주고, 조직의 보안 결함 및 현재 수명주기 프로세스 및 절차를 인식하고 이해하기 시작할 수 있는 정보 콘텍스트를 제공, 일발적인이 기존 절차의 보안강화 사례 및 보안 지향 접근 방식에 대한 충분한 정보를 제공하고 해당 조직의 현재 비보안 적용 사례를 제공한다. 라이프사이클은 정보보안 위협분석, 요구기반 공학 및 소프트웨어보안, 개선모델 및 라이프사이클 방법론 적용, 보안 인식제고, 교육, 훈련, 최소 수준의 보안 소프트웨어 실행 요구사항으로 구성되어 있다[4,9].

– ISO/IEC 27036: Information security for supplier relationships

ISO/IEC 27036은 4개의 part로 구성되어 있다. Part 1은 Information security for supplier relationships-Overview and Concepts, Part 2는 Common Requirements, Part 3은 Guidelines for ICT Supply Chain, Part 4는 Guidelines for security of cloud services로 구성되어진다. 라이프사이클에서 ICT 공급망 보안은 계약 프로세스, 조직의 프로젝트 활성화, 프로젝트 프로세스, 기술적 프로세스의 단계를 구성하고 있다[5,9].

– Microsoft SDL

SDL(Software Development Lifecycle)은 소프트웨어 개발에 중점을 둔 보안 보증 프로세스이다. 기존 개발 주기에 소프트웨어 보안 및 개인정보보호 기능을 통합하고, Training과 Response를 제외하면 소프트웨어 개발 생명주기와 유사하다. <Table 1>에서 라이프사이클은 교육, 요구사항, 설계, 구현, 검증, 배포, 응답을 구성되어 있다. 개발 단계에 수행하는 보안 구현이 일부 개선 또는 임시

방식보다 보안 향상이 된다[9].

- ISA Security Compliance Institute

SDLA(Security Development Lifecycle Assurance)는 “보안 개발 라이프사이클”에 부합하는지 판단하기 위해 공급자의 제품 개발 프로세스를 평가하는 보증 프레임워크이다. 라이프사이클은 Security Management Process, Security Requirements Specification, Security Architecture Design, Security Risk Assessment, Detailed Software Design, Document Security Design, Document Security Guidelines, Module Implementation & Verification, Security Integration Testing, Security Process Verification, Security Response Planning, Security Validation Testing, Security Response Execution의 단계로 구성되어 있다[6,9].

〈Table 1〉 Lifecycle of the Microsoft SDL

Phase	Contents
Security Training	Establish Security Requirements Create Quality Gates/Bug Bars Security & Privacy Risk Assessment
Requirements	Establish Design Requirements Analyze Attack Surface Threat Modeling
Implementations	Use Approved Tools Deprecate Unsafe Functions Static Analysis
Verifications	Dynamic Analysis Fuzz Testing Attack Surface Review
Release	Incident Response Plan Final Security Review Release Archive
Response	Execute Incident Response Plan

3. 정보보호 사전점검 비교 분석

국내유사제도인 정보시스템관리, 개인정보 영향평가, 전자금융 보안성 심의 등과 국외 유사제도인 DHS Security in the Software Lifecycle, ISO27036-part3, MS SDL, NIST National SCRM, ISA Security-SDLA에서의 공통적인 특징은 정보보호 시스템에 대한 사전점검이 정보보호에 상당히 중요한 역할을 하고 있음을 시사하고 있다. 사전점검 제도의 국내외 유사제도의 라이프사이클 프로세스, 통제영역과 특징에 대해서 비교 분석한다.

3.1 라이프사이클 프로세스

라이프사이클 프로세스의 경우 공통된 영역의 내용이 많으며, 각 통제영역에 대한 요구사항에서도 공통점이 많이 있음을 확인할 수 있다. 국내 유사제도의 경우 관련 법규에 기반한 사전 점검 형태의 통제로 구성이 되고 있으며, 라이프사이클 단계별 보안요구사항이 비구체적이며, 단계에서 주로 결과에 대한 구현 중심의 보안 요구사항 및 통제항목에 대한 언급을 하고 있다. 점검 결과에 대한 등급화에 대한 내용도 포함하고 있다. 반면 국외 유사제도의 경우 명확한 방법론을 제시하고 있으며, 교육과 사후대응 단계가 추가된다. 시스템 개발 단계뿐만 아니라 공급체인 관점으로 확장된 개념으로 이용되고 있다. 기존 소프트웨어 보증 개념에 보안 위협이 추가되어 발전된 형태를 이루고 있다[9].

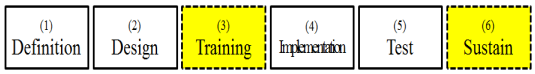
3.2 통제영역과 특징

국내유사제도에서의 통제영역은 요구사항 중심에 대한 통제와 통제중심 실행 실습을 제공한다. 정보시스템 감리 외 별도 세부 가이드라인은 없는 상황이다. 타 표준/제도와의 연계성은 상당히 높은 편이다. 결과인 구현단계 중심의 보안 요구사항이 필요하다. 세부 가이드 라인이 부족하고, 외부 표준/제도와 관련성 있는 연계가 높다. 국외 유사제도의 경우 절차 중심 실행 실습 중심을 제공한다. 세부 가이드라인이 별도로 존재하고, 교육/훈련/단계의 상세화를 통해서 자격증, 전공과정 연계 등의 내용을 포함하고 있다. 타 표준/제도와의 연계성도 국내 유사제도와 함께 높다. 라이프사이클에 교육/사후대응 단계의 별도 적용이 가능하고, 시스템 개발에서 공급 체인 전체로 확대된 개념을 가지고 있다. 보증에 대한 개념을 포함하고 있다[9].

4. 사전점검 적용 방안

한국인터넷진흥원(KISA)에서는 정보보호 시스템의 안전성을 위하여 사전점검 제도를 6단계에 대한 모델링으로 제안하고 있다. KISA에서 사전점검을 위해서 제안하고 있는 사전점검 모델링은 6단계의 라이프사이클로

구성되어 있으며 [Fig. 1]과 같다[9].



[Fig. 1] Modeling in Pre-inspection

KISA에서는 정보보호 사전점검의 절차와 방법에 대한 내용을 [Fig.1]의 프로세스를 구축하였다. 각 단계별로 요구사항정의, 설계, 구현, 시험/테스트, 대응/사후의 각 단계에서 필요로 하는 요구사항과 통제항목을 구성중이다. 일반적인 소프트웨어 구축 단계를 기준으로 각 단계별로 정보보호를 위한 점검 항목으로 6단계 22영역 73개 점검항목으로 세부 127개의 안을 구성하고 있다.

정보보호 사전점검 단계별 점검항목은 다음과 같다. 6단계의 경우 3단계인 교육의 단계에 대한 프로세스에 대한 적용에 대한 차이가 존재하고 있다. 요구사항에 대한 정의 전부터 교육이 필요한 경우와 개발전에 교육이 필요한 경우를 위해서 점선으로 표기하였다. 1단계 요구사항 정의에서는 사점검검 계획, 정보보호 요구사항 정의를 구성하고 있다. 2단계 설계에서는 설계시 보안 관리 및 평가, 보안 아키텍처 설계, 애플리케이션 보안 설계, 개발환경 보안 설계로 구성하고 있다. 3단계 교육/훈련에서는 개발자 교육/훈련관리와 개발자 교육/훈련 프로그램, 개발자 자격 평가로 구성한다. 교육과 훈련의 단계는 현재 3단계에 적합한지에 대한 여부는 개발 환경에 따라서 변경될 수 있다. 타 프로세스에서는 교육의 경우 가장 선행단계에서 진행하여 사전점검에서도 3단계에서의 진행에 대한 방법적 내용을 좀더 고려하고 있는 상황이다. 4단계 구현은 개발환경 보안관리, 데이터베이스 보안 구현, 정보시스템 보안 구현, 네트워크 보안 구현, 어플리케이션 보안 구현, 앤드유저 보안 구현, 암호화 및 인증 구현으로 구성된다. 5단계 시험/테스트 단계에서는 점검 계획, 보안점검, 취약점 점검으로 구성된다. 마지막 6단계 대응/사후 단계에서는 대응계획, 대응절차 및 체계구축, 대응/사후 절차화로 구성된다.

정보보호 사전점검 단계별 절차는 사전점검 준비, 설계검토, 보호대책 적용, 보호대책 구현현황 점검, 사전검검 결과 정리로 구성된다. 추진단계는 계획, 설계, 구현, 시험, 운영으로 구성한다.

사전검검 대상자는 주관기관과 구축 사업자로 구분이 되며, 주관기관에서는 사전점검 준비시 사전점검 필요성 검토/계약, 점검팀 구성, 사업수행 계획서 작성/수정이 이뤄지고, 구축사업자는 세부 수행 계획서를 작성하고 세부 수행계획서를 보완하며, 보호대책을 구현하고 현장 검검 지원과 보호대책 적용현황을 확인하고 미적용 보호대책 구현계획을 수립한다.

점검팀에서는 정보보호 사전점검 수행 계획서 작성, 서비스 정의, 서비스 구조 분석, 보호자산 식별, 위협 분석, 취약점 분석, 위험 분석, 위협 시나리오 도출, 보호대책 도출, 보호 대책 컨설팅, 보호 대책 구현 현황 분석, 위협 시나리오 현장 점검, 사전점검 결과 보고서 작성 단계를 통해 정보보호 사전점검을 완료한다.

5. 사전점검 활성화 개선 방안

정보시스템에 대한 안전성을 확보하기 위한 다양한 법적 고지와 제도 활성화를 위하여 국내외 많은 제도가 만들어지고 있으며 새롭게 도입이 되고 있다. 하지만 각 제도별로 정보시스템에 대한 제도적인 적용과 내용의 중복성 등으로 인한 인력과 비용 등의 낭비가 예상이 된다. 앞서 살펴본 국내외 사전점검에 대한 내용을 기반으로 KISA에서는 사전점검을 6단계의 점검항목으로 구성하여 제안하고 있으며, 2014년 상반기 가이드라인을 제시할 계획이다. 사전점검의 기반은 08년 정보보호 사전검검에 대한 제도화의 필요성이 제기되어 11년 정보통신망법 제 45조의 2(정보보호 사전점검) 신설에 대한 의원 발의(2011년 3월 8일)와 국회통과(2011년 12월 29일) 이루어 졌다. 정보통신망법 개정 및 시행령 개정과 고시 제정이 2012년에 이뤄졌으며, 2013년 정보보호 사전점검 권고 제도 시행이 2013년 2월 18일 시작되었다. 제도적으로 사전점검에 대한 법적 고지를 통한 시행이 되고 있는데, 관련 제도에서는 정보시스템에 대한 안전성을 위하여 소프트웨어 개발보안에 대한 시큐어코딩과 같은 개발과정의 소프트웨어에 대한 보안성을 향상할 목적으로 적용되는 프로그래밍 언어에 대한 코딩 가이드라인들이 제공이 되고 있다. 하지만 이러한 소프트웨어 기반의 보안 약점과 취약점을 최소화 하도록 행정안전부에서 정보시스템 구축 운영 지침이 고시를 통해서 소프트웨어 개발보안에

보안 약점 진단 도구의 사용에 대한 강조되고 있다. 이러한 보안 약점 진단 도구의 사용시 문제점은 소프트웨어의 특징은 코드에 대한 결함과 위험이 코드의 오류중 미탐과 오탐에 대한 최소화를 위한 방법론과 관련 점검 도구의 개발이 필요하다. 관련 유사제도와의 차별화를 위한 방법으로 필수 항목에 대한 부분을 좀더 완화하고, 점검 대상에 대한 폭넓은 적용 보다는 단기/중장기 전략의 수립을 통한 제도 적용이 필요해 보인다. 아울러 현재 ISMS(정보보호관리체계)와 차별화를 위한 방법으로 시스템 개발 이전에 사업계획부터 보안 점검을 할 수 있는 방법을 적용하여 안전성을 확보하는 것이 필요하다. 국내 유사제도와의 통합으로 인한 인력 및 비용에 대한 절감을 위한 정책적 방법도 함께 진행되어야 한다. 사전점검이 제대로 안착이 될 경우 신규 IT 정보 서비스의 경우 많은 보안의 취약점을 개선할 수 있을 것이고, IT 인프라의 활성화에 기여가 크게 예상된다.

6. 결론

IT기술의 급격한 발전에 따라 다양한 신규 IT서비스 모델이 도출되고 많은 기업이 융합의 모델을 통한 발전을 이뤄가고 있다. 융합 신규 IT 정보 서비스는 이용자의 서비스 접근의 편의성을 제공하는 네트워크를 이용한 정보시스템의 복잡도가 증가하고 있어 다양한 보안에 대한 위협은 계속 크게 증가하고 있다. 정보시스템에 대한 안전성을 확보하기 위하여 정보통신 서비스 구축단계에서부터 정보보호 취약점 분석 등을 통해 사전에 취약점을 제거하고 정보보호 대책을 수립하여 적용하였는지에 대한 점검 활동에 대한 제도를 마련하고 있다. 본 논문에서는 정보시스템에 사전점검에 대한 각 나라별 소개와 추진현황에 대해서 살펴보았다. 한국인터넷 진흥원에서 추진하고 있는 사전점검에 대한 추진 방향과 안전성을 확보하기 위한 제도의 활성화 방향에 대해서 제안한다.

REFERENCES

[1] Pilyong Kang, "Security Risk Evaluation Scheme for Effective Threat Management", Journal of KIISE:Information Networking", Vo.36, No.5, pp.380~386, 2009

[2] S. Drew, "Reducing Enterprise Risk with Effective Threat Management," Information Systems Security, vol.13, Jan. 2005, pp.37-42.

[3] G. Stonebumer, A. Goguen, and A. Feringa, "RiskManagement Guide for Information Technology Systems," NIST SP 800-30, NIST, 2002

[4] DHS Security in the Software 라이프사이클, 2006

[5] ISO/IEC 27036:Information Security for supplier relationships

[6] ISA Security Compliance Institute(ISCI), Security Development 라이프사이클 assurance, 2013

[7] Keun-Ho Lee, "Analysis of Threats Factor in IT Convergence Security", Journal of the Korea Convergence Society, Vol.1, No.1, pp. 49~55, 2010

[8] Keun-Ho Lee, "A Security Threats in Wireless Charger Systems in M2M", Journal of the Korea Convergence Society, Vol.4, No.1, pp. 1~5, 2013

[9] Education Course of Information Security Pre-inspection, KISA, 2013.10.21~2013.10.23

이 근 호(Lee, Keun Ho)

- 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수
- 관심분야 : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호, ISMS(정보보호관리체계), 정보보호사전점검
- E-Mail : root1004@bu.ac.kr