http://dx.doi.org/10.14400/JDC.2014.12.7.133

병원정보시스템에서의 정보보호를 위한 감리모형

유완희*, 한기준**, 김동수***, 김희완****
Tobetech* ,건국대학교 컴퓨터공학부**, 건국대학교 정보통신대학원***, 삼육대학교 컴퓨터학부****

An Audit Model for Information Security of Hospital Information System

Wan Hee Yu*, Ki Joon Han, Dong Soo Kim***, Hee Wan Kim****
Dept. of Support Center, Tobetech***
Dept. of Computer Engineering, Konkuk University**
Graduate School of Information and Telecomunications, Konkuk University***
Dept. of Computer Engineering, Shamyook University****

요 약 최근 병원정보시스템은 병원 경영을 위한 다양한 서비스, 진료 활성화와 진료의 질 향상을 위하여 대용량의 데이터베이스를 보유하게 되었다. 하지만, 병원정보시스템에 대한 정보보호대책은 미흡한 편이다. 따라서, 병원정보시스템 구축할 때, 정보보호에 대한 대책을 적절하게 마련하여 정보보호 감리를 수행하여야 하며, 위험관리를 통한 정보보호 수준을 유지할 수 있도록 정보보호 관리체계(ISMS)를 수립하고 관리해야 한다.
본 논문에서는 병원정보시스템, 정보보호관리체계, 병원정보 보호 요구사항 및 위협요소를 근거로 병원정보시스템에 적합한 정보보호 감리모형을 제안하였다. 감리모형에서는 의료기관의 특성이 잘 반영되어 있는 ISO27799와 비교하여 점검항목들을 도출하였다. 보안영역은 물리적, 기술적, 관리적 영역으로 분류하고 각각에 세부적으로 정보보호 항목들을 도출하였다. 또한 ISO27799의 위험관리 절차에 따라 점검항목을 매핑함으로써 보안성과 효율성을 동시에 향상시킬 수 있도록 설계하였다. 제안한 감리모형은 IT 전문가들의 5점 척도 설문 조사 결과 평균 4.91점으로 나타나 적합하다는 결론이 도출되었다.

주제어 : 병원정보시스템, 정보보호관리체계, 감리모형, 점검항목

Abstract Recently, Hospital information systems have the large databases by wide range offices for hospital management, health care to improve the quality of care. However, hospital information systems for information security measures are insufficient. Therefore, when we construct the hospital information system, we have to audit the information security measures for them, and we have to manage the ISMS(Information Security Management System) to maintain the information protection level through the risk managements.
In this paper, we suggested the hospital information security audit model for the protection of health information privacy by the current hospital information systems, information security management system(ISMS), and hospital information security requirements and threats. We derived the check items compared with ISO27799 reflected the characteristics of the hospital. We classified the security domains as the physical, technical, administrative domain, and derived the check items for information security. We also designed the check lists by mapping the ISO27799 risk management process to improve the security and efficiency simultaneously. Our model by the five-point scale survey of IT experts was verified the suitability with the average of 4.91 points.

Key Words : Hospital Information System, ISMS, Audit Model, Check Lists

* 본 논문은 2013년 삼육대학교 학술지원비(RI자율2013086)에 의하여 지원되었음.
Received 2 May 2014, Revised 7 June 2014
Accepted 20 July 2014
Corresponding Author: Hee Wan Kim(Shamyook University)
Email: hwkim@syu.ac.kr

ISSN: 1738-1916

1. 서론

정보시스템 감리를 통해서 얻을 수 있는 기대효과는 프로젝트관리의 수준과 프로젝트 품질관리체계가 향상되고, 프로젝트 표준의 준수 및 표준설정의 완성도가 향상되며, 사용자 요구사항이 충실하게 구현되어 데이터베이스의 일관성, 독립성, 통합성, 유연성과 응용시스템의 유지보수성이 향상된다고 말할 수 있다[1].

병원 정보시스템은 영상 데이터를 저장, 관리, 전송하여 관리하는 의료영상저장 전송시스템인 PACS(Picture Archiving and Communication System), 환자의 처방 전달 및 진료내역을 관리하는 처방전달시스템인 OCS (Order Communication System), 환자의 전자의무기록을 수기에서 전자문서로 기록하고 보존하는 전자의무기록시스템인 EMR(Electronic Medical Record)로 주로 구성되어 있다. PACS, EMR, OCS가 효율적으로 연동되기 위한 병원정보시스템 구축을 위한 감리모형[2]에 대한 연구는 되어 있으나, 병원정보시스템에서의 정보보호를 위한 감리 모형에 대한 연구가 필요한 시점이다.

이에 본 연구에서는 ISMS 기준을 만족하고 의료기관의 특성을 반영하는 병원정보시스템의 정보보호 감리모형을 제시하고자 한다. 병원정보시스템 정보보호에 적합한 정보보호 감리모형을 도출하기 위하여 병원정보시스템, KISA-ISMS[3], ISO27799[4], 병원정보 보호 요구사항 및 위협요소를 조사·분석하고, 이를 근거로 병원정보시스템의 효율적인 정보보호를 위한 감리모형을 제시하고자 한다. 병원정보시스템의 정보보호와 관련하여 조사하고, 병원정보시스템의 정보보호감리 프레임워크를 도출하고 감리모형을 물리적, 기술적, 관리적 영역으로 분류하여 세부적인 정보보호 항목들을 도출하였다. 또한 ISO27799의 위험관리 절차에 따라 점검항목을 매핑하여 보안성과 효율성을 동시에 향상시킬 수 있도록 설계하였다. 제안한 정보보호 감리 모형은 전문가의 설문 조사를 통해 적합성을 검증하였다.

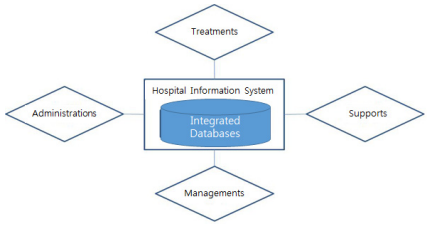
2. 관련 연구

2.1 병원정보시스템

병원에서 발생하는 정보는 의료인이 환자를 다루는 의료과정과 병원의 경영관리활동의 환경을 중심으로 발생하고 있다. 병원정보시스템은 타 조직체와는 다르게 전문 직종 간에 생성 교환되는 정보의 양이 방대하고 정보의 신속, 정확성과 장기적 보관을 필요로 한다는 점에서 정보의 흐름은 매우 중요한 의미를 지니고 있다. 병원정보시스템을 알아보기 위해 관련 자료를 살펴보면 의료정보시스템의 개념과 혼용되어 사용되거나, 협의의 의료정보시스템으로서 인식된 것을 알 수 있다[2].

의료정보시스템은 크게 병원정보시스템, 지역의료정보시스템, 의료정보서비스로 구분되며, 이중 병원정보시스템은 병원의 여러 업무를 수행하는데 필요한 정보를 적시에 적절하게 제공하는 시스템으로 여러 형태의 기능을 수행하는 단위 시스템들의 복합체이다. 병원정보시스템은 의료기관을 운영·분석하고 의료의 질을 향상시키는데 중추적인 역할을 한다[5].

또한 한편으로는 고객서비스 중심 의료정보시스템의 구성을 위해 내부 프로세스 중심의 가장 핵심 시스템으로서 크게 원무행정 부문을 지원하는 시스템과 진료정보를 지원하는 시스템으로 구성되어 있다. [Fig.1]에 병원정보시스템의 일반적 구조를 나타내었다[5]. 병원정보시스템은 의사가 행하는 진찰 및 치료를 지원하는 진료업무, 진료를 지원하는 진료지원, 환자예약, 접수, 수납 등을 지원하는 원무행정과 인사, 급여, 회계, 자산, 원가 등을 관리하는 의료경영관리 업무로 나눌 수 있다.



[Fig.1] Hospital Information System Architecture[5]

병원정보시스템의 대상 업무 성격에 따른 분류는 <Table 1>과 같다[6]. 병원관리시스템을 분류하면 4가지 시스템으로 대별할 수 있으며, 의사가 행하는 진찰 및 치료를 보조하는 진단업무, 병력관리, 처방관리, 검사, 치료결과관리 등을 지원하는 진료업무시스템, 검사업무, 약제업무, 간호업무, 급식업무, 환자지원 등을 지원하는 진료지원시스템, 환자 예약업무, 접수업무, 수납업무, 의무기록 업무 등을 지원하는 원무행정시스템과 인사, 급여업

무, 회계업무, 자산업무, 재고관리, 원가관리 등을 지원하는 일반관리시스템으로 나눌 수 있다.

〈Table 1〉 Classification of Hospital Information System[6]

	Target Tasks
Medical Services	- diagnosis and treatment - disease history management, education, inspection, treatment management, literature search, and research management
Medical Supports	- services to support the treatment - inspection services, pharmaceutical services, nursing services, Central Supply business, catering services, patient support services
Adminst rations	- claims for medical services - patient scheduling tasks, receptionist duties, storage services, medical records work
Manage ments	- human resources, payroll services, accounting services, property services, inventory management, cost management

2.1.1 진료업무 시스템

(1) 처방전달시스템(OCS: Order Communication System)

처방의 원활한 전달을 위해 구성된 시스템으로 진료의사에 의하여 발생된 처방은 신속, 정확하게 필요한 부서로 전달되어 처리된다. 즉, 원무부서로 이동된 처방은 정확한 수납계산과 건강보험 청구를 시행하게 해주고, 약국/검사부서 등 지원부서로 이동된 처방은 투약과 검사를 시행하도록 해준다. 검사결과, 투약력 등의 자료는 다시 Feedback되어 진료에 도움을 줄 수 있다[7].

(2) 전자의무기록(EMR : Electronic Medical Record)

환자의 진료 과정에서 발생된 모든 자료나 기록을 전산에 입력, 보관하는 시스템을 말한다. 환자 대기, 시간 감소 및 정보저장의 편의성, 접근의 용이성, 보험청구 업무의 자동화, 자동통계처리, 인건비 절감 등의 장점이 있다[7].

(3) 의료영상저장전송시스템(PACS : Picture Archiving and Communication System)

의료 환경에서 발생되는 각종 의학영상(X-Ray), 컴퓨터단층촬영(CT : Computed Tomography), 자기공명영상(MRI : Magnetic Resonance Imaging), 양전자단층촬영(PET : Positron Emission Tomography), 단일광자단층촬영(SPECT : Single Photon Emission Computed Tomography) 등을 디지털 데이터로 획득하고 컴퓨터 저장 장치에 저장하며, 이를 네트워크에 연결된 다수의 컴퓨터에 전송하여 조회 활용할 수 있게 하는 시스템이다[7].

2.1.2 진료지원 시스템

(1) 임상병리정보시스템(LIS : Laboratory Information System)

병원의 각 검사실과 각 진료과별로 구축된 네트워크로 검사실에서 자동으로 실험실 검사 결과들이 환자 등록 시스템에 검사 항목으로 입력되고, 그 결과에 대하여 담당 의사가 단말기에서 볼 수 있다. 이들 각 검사실에서 단말기를 통해서 환자의 기록을 열람하고, 진단에 필요한 자료를 검토한다[7].

(2) 간호정보시스템(NIS : Nursing Information System)

간호기록의 전산화 작업은 의료기관의 비용을 절감하고 생산성을 제고하는데 필수적이다. 의료 관계자들이 환자의 정보를 쉽고 빠르게 접할 수 있고 중복적인 서류들을 유지하는데 소요되는 행정적인 비용을 감소시킬 수 있으며, 연구를 수행하기 위해 필요한 자료수집 및 분석이 용이해 진다[8].

2.1.3 원무관리 시스템

(1) 원무관리시스템(PM/PA : Patient Management /Patient Account)

환자관리와 진료비 관리 시스템으로 수가관리, 진료비 계산, 병실관리, 보험수혜관리, EDI청구, 미수관리, 마감시재 관리, 수익일보 등의 자료를 관리 할 수 있다.

(2) 전자청구시스템(EDI : Electronic Data Interchange)

환자가 진료를 본 후 진료비 총액 중 환자 본인부담금을 뺀 나머지 진료비를 건강보험심사평가원에 청구하는 전자청구시스템이다.

2.1.4 일반관리 시스템

(1) 일반관리시스템(MIS : Management Information System)

인적자원의 효율적인 관리를 위한 인사급여 부문과 약품과 위생물품을 관리하는 재고부문, 소유한 자산에

대해 관리해주는 회계부문 등으로 구성된 시스템이다[9].

(2) 경영자정보시스템(EIS : Executive Information System)

OCS, PM/PA, MIS 등의 각종 정보를 통하여 언제든지 병원운영과 관계된 통계 자료를 수치, 그래프 형식으로 경영자의 의사결정을 지원하는 시스템이다[9].

(3) 의사결정지원시스템(DSS : Decision Support System)

의사결정에 필요한 계량적 기법이나 통계적 기법을 컴퓨터에 저장하여 각종 대안들을 비교 분석하거나 의사결정에 필요한 중요 정보를 제공하는 정보시스템이다[9].

(4) 전사적 자원관리시스템(ERP : Enterprise Resource Planning)

병원의 모든 자원을 효율적으로 통합운영하기 위한 전사적 자원 관리 시스템이다[9].

(5) 고객관리시스템(CRM : Customer Relationship Management)

의료의질 평가나 서비스 및 병원 마케팅 차원의 고객관리를 위한 시스템이다[7].

(6) 지식관리시스템(KMS : Knowledge Management System)

병원조직 내에 분산되어 있는 지식을 효과적으로 저장·관리·활용하여 관리자의 의사결정을 지원하는 지식경영시스템이다[7].

2.2 정보보호 감리

2.2.1 정보시스템 정보보호 감리 개념 및 필요성

정보시스템 감리가 정보시스템의 전 분야를 대상으로 한다면 정보보호감리는 정보시스템의 정보보호 분야를 중심으로 실시하는 감리라 할 수 있다. 현재까지 실시되어온 정보시스템에 대한 감리의 형태는 최소한의 정보보호 분야에 대한 점검과 평가를 수행함으로써 사업 개발단계나 운영단계에 있어서의 충분한 정보보호 요구를 충족시킬 수 없었다[10].

정보보호 문제에 대한 분석과 평가는 정보시스템의 개발단계에서부터 행해졌을 때 조직이나 시스템의 정보보호 관리의 효율성 향상을 기대할 수 있다.

이러한 점을 고려하여 정보보호감리의 개념을 다시 정의하면, 정보보호감리란 '정보시스템의 안정성과 신뢰성을 보장하기 위하여 정보시스템의 구축과 운영을 포함한 전 과정에 걸쳐 정보보호 문제점을 식별하고 개선사항을 도출하여 시정토록 하는 것'이라 할 수 있다.

2.2.2 정보보호감리 현황 및 문제점

정보보호 사업은 정보보호 체계 및 제품 인증, 정보통신보호법 기반의 주요 정보통신망 시설의 취약점 진단, SI프로젝트에서의 보안 솔루션 제공, 운영환경에서의 정기적인 취약점 진단, BSP나 ISP 또는 IT 품질 컨설팅 등과 연계된 정보보호 컨설팅, 정보보호체계 구축을 위한 보안 컨설팅 등 다양하게 수행되고 있다. 그러나 현재 정보보호 감리의 수준은 많은 부분에서 미흡한 실정이다[10].

정보보호 감리의 문제점은 첫째, 정보보호 감리에 대한 인식 및 연구가 부족하다. 정보보호를 하나의 감리 분야로 인식하지 않고 시스템 아키텍처의 하나로 인식하고 있어, 정보보호 감리에 대한 체계적인 연구가 이루어지지고 있지 못하고 시스템 아키텍처의 일부분으로 연구되거나 점검항목을 도출하였을 뿐이다. 그러나 정보보호는 시스템 아키텍처뿐만 아니라 응용프로그램, 데이터베이스, 운영체제, 관리적인 부분, 물리적인 부분 등 정보시스템 전 부분의요소로 포함되어 있기 때문에 기존의 감리 수행으로는 한계가 있다.

둘째, 정보보호 감리를 수행하기 위한 감리원의 수준이 미흡하다. 정보보호에 대한 중요성을 인식하기 시작한 시기는 불과 몇 년 되지 않았으며, 정보보호 기술이 급속히 발전하고 있으나, 정보보호 분야에 대한 연구가 부족하고 관련된 지침이 정비되지 않아 감리원의 보안분야에 대한 수준이 미흡한 상황이다.

셋째, 정보보호 감리를 위한 여건이 아직 성숙되어 있지 않다. 시스템아키텍처와 보안을 분리하여 보안 부분에 별도의 정보보안 전문 감리원을 투입하려고 해도 관련 감리를 위한 예산 배정에 한계가 있어, 현실적으로 개선이 곤란한 것이 사실이며 예산 책정의 특성상 대응책 마련이 용이하지 않은 실정이다[10].

2.3 병원정보시스템 정보보호 감리

병원정보시스템이 갖추어진 병원의 업무환경은 기술

적 측면의 외부자에 의한 위협뿐만 아니라 내부 사용자에 의한 위협으로 병원정보의 비밀성, 무결성, 가용성을 훼손할 위험이 높은 곳이다. 일부 대형 병원을 제외하고는 일반 중소 병원이나 의원 등에서의 정보보호 인식수준은 낮은 수준이며, 정보보호 예산에 대한 투자 또한 미비 하다. EMR, OCS 등의 정보시스템에 대한 사용자 인증과 접근제어 및 권한관리, 의료정보에 대한 전자서명 및 암호화, 감사 및 추적체계 등 시스템 차원의 보안 대책과 보안정책 및 관리적 차원의 보안관리 체계가 정비되지 못한 의료기관이 많은 실정이다[5].

의료분야에서 기술적 보호 방안 수립 시 고려해야 할 사항으로 의료서비스의 시스템 구조 측면과 병원정보 저장, 관리 단계에 대한 보호 대책이 있다.

의료서비스 시스템 구조측면에서의 보호대책은 기밀성 위협, 가용성 위협, 접근제어 위협이 있다. 기밀성 위협은 환자관리의 편의성 때문에 빈번히 사용되는 무선통신의 보안 취약점으로 인하여 원격의료나 인터넷병원은 내・외부의 침입으로부터 취약하므로 무선통신서비스에 대한 식별 및 인증 서비스를 강화해야 한다. 가용성 위협은 각 네트워크 접점에 침입차단 및 탐지시스템을 구축하고 서비스의 안전성 확보를 위한 정책을 적용하여야 하며, 접근제어로는 병원 내 PC에 대한 침해차단 및 탐지를 위해 기본적인 Ant-Virus및 보안정책에 PC 방화벽, 패치관리 등의 설치를 규정하여 설치하고, 병원 보안정책에 따르지 않는 PC의 네트워크 접근을 통제하기 위하여 NAC 솔루션 구축하여야 한다[5].

의료서비스 정보의 저장, 관리 단계에 대한 보호대책은 의료정보서비스에 접근하는 사용자는 사용권한에 따라 식별되고 허가되어야 하므로 사용자 별로 업무에 따른 접근권한을 정의하고 SSO/EAM과 같은 권한에 따른 관리체계 구축이 필요하며, 전자의무기록시스템, 처방전달시스템, 의료영상전송시스템 등의 정보가 암호화 되지 않아 정보시스템 관리・접근하는 사용자에게 환자의 의료기록이 쉽게 노출됨에 따라, 어플리케이션의 정보생성 시점부터 DB암호화, 백업미디어에 대한 보호조치를 강구하여야 한다.

2.4 병원정보시스템의 정보보호 감리의 필요성

병원정보의 많은 위협들로부터 보호하기 위해 병원정보보호는 그 필요성이 더욱 높아진다. 병원정보는 진료를 받는 환자를 통해서 의료인이나 의료기관이 취득·보유하는 개인정보이다. 전자 문서 등의 형태로 전산화된 병원정보는 환자의 의미기록에 관련된 정보로써, 신상정보, 생체정보, 환자의 건강력, 진단명, 질병 상태, 치료 경과 등을 포함하고 있다. 환자에게 있어 이러한 병원정보의 노출은 정신적, 사회적, 경제적인 피해를 초래할 가능성 있어 사적 비밀보장의 측면에서 볼 때 본인의 허가 없이 정보가 유출 되지 않도록 보호하고 보안을 유지할 필요성이 있다. 또한 정보에 대한 무결성에 대해 침해당했을 경우는 부정확한 정보가 생성되어 추가적인 문제를 발생 시킬 수 있다.

이에 따라 체계적인 위험관리를 통해 위험을 분석 및 평가하여 적절한 정보보호 대책을 마련했는지 점검할 수 있는 정보보호 감리제도가 필요하다.

2.5 선행 병원정보시스템 프레임워크 연구

문병철이 제시한 “효율적인 병원정보시스템 구축을 위한 감리 모형“에서는 응용시스템 영역을 OCS, PACS, EMR 3가지로 세분화하여 도출시켰다[2].

〈Table 3〉 Security considerations of hospital information system[2]

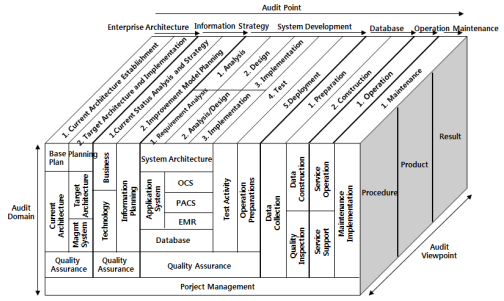
System	Considerations
OCS	Server duplication, network duplication, equipment interface
EMR	Server speed, OCS, EMR system interface, EMR server capacity
PACS	High Speed of the Network configuration, the storage system, the image quality

병원정보시스템은 2.1 에서처럼 OCS, EMR, PACS 외에도 많은 시스템들로 구성되어 있다. 그러나, 선행연구에서는 응용시스템을 3가지로만 구분하였다. 주로 보안부분에서 고려한 사항이 가용성이나 성능 관점에서만 제시했기 때문에 정보보호 관점에서 미흡한 면이 있다.

3. 병원정보시스템 정보보호 감리모형

본 논문에서는 ISO27799기반의 병원정보시스템 정보보호 감리 모형을 현행 정보시스템 감리 프레임워크 모델[3]을 참고 하였다. ISO27799과 ISMS의 위험관리 절

차 및 통제분야와 정보보호 감리 시점 및 점검항목을 비교 매핑함으로써 병원정보시스템 정보 보호 감리 모형을 제시하였다.



[Fig. 2] Hospital Information System Audit Framework[2]

3.1 사업유형 및 감리시점

3.1.1 사업유형 및 감리시점 분류

현행 정보시스템 감리프레임워크의 사업유형 및 감리시점과 병원정보시스템 정보보호 감리시점을 매핑하고 KISA-ISMS[3]의 위험관리과정을 참고하여 병원정보시스템 정보보호 감리시점을 구성하였다.

〈Table 4〉 Comparison of Current Information System Audit Framework

Current Information System Audit1)	Hospital Information Systems Audit	Description
Requirement Analysis	PLAN	Hospital Data Protection planning
Analysis/Design		Setting of hospital data protection Range
		Risk management and evaluation Plan
Implementation	DO	Selection and implementation of data security controls
Test		Test
Deployment	CHECK	Operating and maintenance
	ACT	

1) : [3]

(1) 병원정보시스템 정보보호 계획 수립

프로젝트 대상이 되는 정보시스템이 무엇인지를 정의하고 정보시스템이 처리하는 기본적인 병원정보가 무엇인지 파악해야 한다. 정보시스템 개발을 위한 전체적인 프로젝트 수행 계획에 병원정보 보호를 위한 일정계획 및 자원계획이 반영되어야 한다.

(2) 병원정보 보호 범위 설정

업무 프로세스별 정보 보호 요구사항을 토대로 범위를 설정한다. 정보보호 요구사항의 만족 여부를 판단하기 위해 병원정보보호 전문가에게 설계 결과를 보여주고 의견을 구하기도 한다.

(3) 위험 관리 및 평가 계획

병원정보의 위험요소들을 분석하여 평가하고 위험관리에 대한 대책을 세운다.

(4) 보안 통제사항 선택 및 구현

하드웨어 획득, 소프트웨어 도입 또는 개발 작업과 단위 시험 등의 작업을 위해 병원정보보호 구현 및 검토, 운영관리계획 및 지침 개발 활동이 수행된다.

(5) 시험

개발이 완료된 정보시스템이 병원정보보호 요구사항을 만족하는지 정보보호시험, 이관을 위한 정보보호 설정, 이관 후 정보보호 시험 활동이 수행된다. 시험단계는 기능시험, 통합시험, 인수시험 등 기능 및 사용자의 요구사항 만족여부에 대한 검증 작업이 수행된다.

(6) 운영 및 유지보수

보안 사고에 대응하며 운영하고 유지 보수하는 사업이다. 일반 정보시스템 운영사업과 달리 악성코드나 침입탐지 및 예방을 항시 감시 할 수 있는 체제를 갖추어야 한다. 침해사고 경보를 참조하여 대응체제를 갖추고 바이러스나 해킹에 대한 대응과 사고에 대한 신속한 조치 및 복구가 필수적인 사업이다.

3.1.2 정보보호 감리시점과 ISMS 관리과정 비교

기업이나 기관은 정보자산의 무결성, 비밀성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하고 지속적으로 관리, 운영하기 위하여 정보보호관리체계(ISMS)를 수립하여 관리한다. 병원정보시스템 정보보호 관리체계를 위하여 KISA-ISMS[3]과 ISO27799[4]

의 정보관리체계의 관리과정을 비교하였다.

〈Table 5〉 Comparison of ISO 27799, KISA-ISMS, and HIS Audit

Steps	ISO 277991)	KISA-ISMS2)	Hospital Information Systems Audit
PLAN	ISMS Plan	Information Protection Policy Plan	Hospital Data Protection Planning
		Management System Range Setting	Setting of hospital data protection Range
		Risk Management	Risk management and evaluation Plan
DO	ISMS Implementation and Operation	Implementation	Selection and implementation of data security controls
CHECK	ISMS Monitoring	Post Management	Operating and maintenance
ACT	ISMS Maintenance		

1) : [4] 2) : [3]

ISO 27799:2008, KISA-ISMS 등 정보보호관리체계의 관리과정은 순환주기를 갖고 있다. 병원 환경의 위험관리 절차에 따라 정보보호 감리시점을 도출하였다.

〈Table 6〉 Comparison of ISO 27799 Risk Management Process and HIS Audit

ISO 277991)		Hospital Information Systems Audit
PLAN	Gap analysis	Hospital Data Protection Planning
	Security Improvement Plan	
	Selection of compliance scope	Setting of hospital data protection Range
	Medical Information Security Forum Establishment	Risk management and evaluation Plan
	Risk assessment of medical information	
	Risk Management	
	Apply History	
	ISMS Documentation	
	Risk action planning	
	Assigment	
DO	Selection and implementation of security controls	Selection and implementation of data security controls
	Education and training	Operating and maintenance
	Operations Management	
	Resource Management	
	Security Incident Management	
CHECK	The need for ongoing assurance	
	Compliance assessment	
ACT (ISMS Maintenance)		

1) : [4]

ISO27799은 ISMS를 위험기반을 기반으로 수립하고 PDCA 사이클에 따라 관리한다. 의료정보의 위험관리/평가 및 위험 조치 계획 수립은 ISMS 수립단계인 PLAN단계에서 이루어지고 보안통제 선택 및 구현은 ISMS 구현 및 운영단계인 DO단계에서 이루어진다. 또한 운영 및 유지보수는 ISMS 모니터링 및 검토단계인 CHECK단계와 ISMS 유지 및 개선 단계인 ACT단계에서 이루어진다. ISO 27799의 PDCA 사이클과 병원정보관리시스템의 정보보호 단계를 비교하여 제시하였다.

〈Table 7〉 Comparison of KISA-ISMS Risk Management Process and HIS Audit

KISA-ISMS1)		Hospital Information Systems Audit
Information Protection Policy Plan		Hospital Data Protection Planning
Management System	Management System Range Setting	Setting of hospital data protection Range
	Identification of information assets	
Risk Management	Risk management strategy and planning	Risk management and evaluation Plan
	Risk analysis	
	Risk evaluation	
	Selection of Information Security	Selection and implementation of data security controls
	Information Security Plan	
Implementation		
Post Management		Operating and maintenance

1) : [3]

KISA-ISMS은 ISO2779와 달리 위험관리가 관리과정으로 명시되어 있다. 위험관리 안에는 위험관리전략 및 계획수립, 위험분석, 위험평가, 정보보호대책 선택, 정보보호 계획수립의 단계가 포함되어 병원관리시스템의 위험관리 및 평가계획과 보안 통제사항 선택 및 계획 단계로 도출하였다.

3.2 감리영역

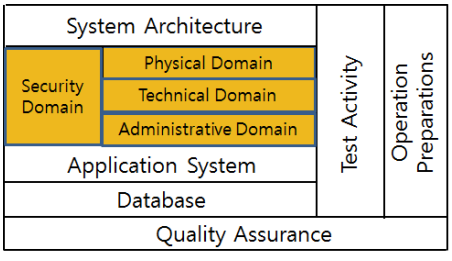
감리영역은 위에서 제시한 의료분야 정보보호 요구사항을 토대로 영역을 구분하였다. 기존 연구의 정보보호 영역과 비교 제시하였다.

〈Table 8〉 Comparisons of Information Protection Domain

Current IS Framework	Hwang Hae Su1)	Lee Hyeong Chan2)	This paper
System Architecture	Device Player	Physical Domain	Physical Domain
	Network	Netwok	
	Server	Mobile Center	
	Information	Software Domain	Technical Domain
	N/A	N/A	Administrative Domain

1) : [11] 2) : [12]

기존연구[11][12]에서는 주로 단말 등과 같은 물리적 영역과 응용프로그램 및 플랫폼등과 같은 소프트웨어 영역, 네트워크 및 서버영역의 3가지로 나누었다. 본 연구에서는 의료정보 보호 요구사항을 토대로 현행 감리프레임워크에서 보안영역을 별도로 추가하였으며, 보안영역에는 물리적 영역, 기술적 영역, 행정적 영역으로 나누어 제안하고자 한다.



[Fig. 3] Suggested Hospital Information Systems Information Security Domain

3.3 감리관점 및 점검기준

감리관점 및 점검기준은 기존 정보시스템 감리와의 호환성을 위하여 기본적으로 현행 프레임워크의 관점과 기준을 적용했다.

〈Table 9〉 Check Standard by Audit View[13]

Audit View	Check Standard	Related characteristics
Process	Plan Reasonability	Business management planning construction/management, evaluation of suitability of establishing and following procedures
	Process Reasonability	Establishing development / management / maintenance procedure and reasonable establishment of risk/schedule/quality/form/human resources/change managements
	Compliance	Following plans and risk / schedule / quality / form / human resources / change management procedures fairly
Product	Functionality	Sufficiency, completeness, accuracy, interoperability, and connectivity of the Functionality function
	Integrity	Data integrity and accuracy
	Usability	User convenience, management convenience, and learning
	Stability	System stability, service continuity, quick restoration
	Security	System confidentialness and safety
	Efficiency	Efficiency of using information resources (human resources, server, etc), work efficiency, quick answers, system extendability, technology development compatibility
	Compliance	Following criteria / procedure / standard / methodology of the product
	Consistency	Analysis, alteration, existing, traceability, maintainability
Performance	Sufficiency	Satisfaction of work/technical requirements, achieving performance goals, sufficient task scope
	Realizability	Concreteness, feasibility, efficiency of investment, achieving the performance goals, system availability
	Productivity	Speed and receptiveness of Agile, frequency of release and repetition, test productivity, business accomplishment and productivity

의료분야의 특수한 요구사항은 개인 의료정보의 기밀성, 무결성, 감사가능성, 가용성을 보장해야 한다. 이러한

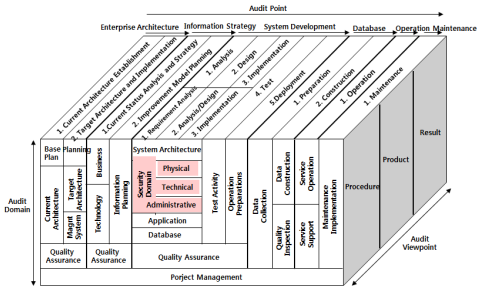
의료정보 보호의 4대 요소를 보장하는 것은 의료분야 특화된 전문성을 요구한다. 의료정보 보호의 4대 요소를 반영 하였다.

3.4 병원정보시스템 정보보호감리 프레임워크

3.4.1 병원정보시스템 정보보호감리 프레임워크 정립

위에서 제시한 사업유형/감리시점, 감리영역, 감리관점/점검기준을 적용하면 아래와 같은 점검 프레임워크가 구성된다.

[Fig. 4]는 현행 정보시스템감리 프레임워크를 참고하여 사업유형/감리시점, 감리영역, 감리관점/점검기준을 적용하였으며, 3.2 감리영역에서 제안한 모델을 현행 정보시스템 감리 프레임워크에 적용하였다.



[Fig. 4] Suggested Hospital Information System Information Security Audit Framework

3.4.2 병원정보시스템 정보보호 감리점검항목

병원정보시스템의 정보보호 구현을 위한 감리 점검항목을 도출하는데 있어서 ISO27799을 참고하여 위험관리 절차에 따라 보안 통제사항 선택 및 구현 단계의 점검항목을 도출하였다. 위험을 수용 가능한 수준으로 통제하기 위한 항목들을 선택하여 구현한다. ISO27799에서 제시한 통제사항을 토대로 점검항목을 도출하고 ISO27799의 통제분야와 매핑하였다.

(1) 물리적 영역

물리적 영역은 환자 데이터의 암호화 정책과 OCS, EMR, PACS등의 정보의 암호화 대책, 원격의료나 인터넷병원의 무선통신 서비스에 대한 식별 및 인증 대책, OCS, EMR, PACS 등의 접근에 대한 대책, 의사, 간호사, 방사선사 등의 사용자 인증 대책이 적정하게 선택되고 구현되었는가와 진료정보의 원격접속에 대한 이력관리 대책이 적정하게 선택 및 구현되었는가를 점검항목으로 도출하였다.

〈Table 10〉 Check Lists of Physical Domain

Check Lists	ISO 277991)
Did you select and implement all patient's data encryption policies ?	7.4 Physical Environmental security
Did you select and implement the data encryption measures like OCS, EMR, PACS ?	
Did you select and implement the identification and authentication measures for remote medicine and wireless services of internet hospital ?	
Did you select and implement the access control measures like OCS, EMR, PACS ?	7.7 Communications and Operations Management
Did you select and implement the user authentication measures for doctors, nurses, radiation technologists ?	7.5 Personnel Security 7.8 Access Control

1) : [4]

(2) 기술적 영역

기술적 영역에서는 권한이 없는 환자 접근시 사유 관리, 특정 환자 기록의 정보보호, 병원 프로그램에 대한 악성코드 대책과 의료접근통제를 위한 요구사항이 적정하게 선택되고 구현되었는가를 점검항목으로 도출하였다. 또한, 의료접근통제를 위한 대책과 모든 환자 데이터를 암호화하여 관리하는지, EMR, OCS, PACS 백업에 대한 대책, 병원정보시스템 감사 고려사항, 의료 정보 교환의 대책이 적정하게 선택 되고 구현되었는가를 도출하였다.

〈Table 11〉 Check Lists of Technical Domain

Check Lists	ISO 277991)
Are there any managements for unauthorized patient access ?	7.7 Communications and Operations Management
Are there any information protections for specific patient's records ?	
Did you select and implement the malicious code measures for hospital programs ?	
Did you select and implement the requirements for medical access control ?	7.8 Access Control

Did you encrypt all patient's data?	7.9 Information System Introduction, development, maintenance,
Did you select and implement the backup measures like OCS, EMR, PACS ?	
Did you select and implement the audit considerations for hospital information system ?	7.12 Compliance
Did you select and implement the medical information exchange measures ?	7.7 Communications and Operations Management

1) : [4]

(3) 관리적 영역

관리적 영역은 상시 근무인원이 5인 이상인 의료기관에서 내부관리 계획, 진료정보의 열람이나 제공에 관한 내용 확인과 진료, 영상, 간호 기록업무를 총괄하는 책임자를 지정했는지를 점검항목으로 도출하였다. 또한, 진료정보를 진료목적 외의 다른 용도로 이용할 경우 별도의 동의 여부와 진료정보를 의료법에서 정한 보존기간 동안 보유 여부를 관리적 영역으로 도출하였다.

〈Table 12〉 Check Lists of Administrative Domain

Check Lists	ISO 277991)
Do you have the internal management plan for the medical institutes working more than five people ?	7.3 Information Protection Organization 7.4 Resource Management
Can you check the contents for medical information except medical laws ?	
Do you have a supervisor for managing the medical care, video, nursing record ?	
Do you have any consents if you use another purpose except medical purpose ?	7.7 Communications and Operations Management 7.10 Security Incident Management
Do you have the medical information which has the retention period ?	

1) : [4]

4. 정보보호 감리모형 검증

본 논문에서는 병원정보시스템의 정보보호 감리를 위한 감리영역, 감리시점, 감리 점검항목 등에 대하여 그 필요성 및 실효성을 검증하기 위하여 감리원 및 의료IT 담당자, 의료IT 종사자를 대상으로 설문하는 방법을 사용하였다. 설문조사의 대상은 <Table 13 >과 같이 선정하였으며, 감리원(40%), 의료IT종사자(33.3%), 의료IT담당자(26.7%)로 구성되어 있다.

〈Table 13〉 Results of the Surveyors

	IT Auditor	Medical IT Manager	Medical IT Employee	Total
number	18	12	15	45
percent	40	26.7	33.3	100

감리점검항목에 대한 설문은 제안한 보안 통제사항 선택 및 구현 단계의 점검항목 중에서 병원정보에 관한 중요한 항목을 선정하여 나열하고 각 항목마다 매우필요(5점), 필요(4점), 보통(3점), 필요없다(2점), 전혀 필요없다(1점)으로 표기하는 5점 척도를 적용하여 검증하였다.

4.1 물리적 영역에서의 점검항목 설문 결과

물리적 영역에서 점검항목에 대한 설문 결과는 진료정보의 원격접속에 대한 이력관리 대책이 적정하게 선택되고 구현되었는가는 평균 5.0으로 나타났으며, OCS, EMR, PACS등의 정보의 암호화 정책에서는 4.8 나타났으며, 모든 점검항목의 평균이 4.8 에서 5.0 으로 설문 의견을 나타내었다.

〈Table 14〉 Results of Check Lists in Physical Domain

Check Lists	5~4	3	2~1	Avg	SD
Did you select and implement all patient's data encryption policies ?	45	0	0	4.89	0.29
Did you select and implement the data encryption measures like OCS, EMR, PACS ?	43	2	0	4.80	0.43
Did you select and implement the identification and authentication measures for remote medicine and wireless services of internet hospital ?	45	0	0	4.93	0.23
Did you select and implement the access control measures like OCS, EMR, PACS ?	43	2	0	4.84	0.39
Did you select and implement the user authentication measures for doctors, nurses, radiation technologists ?	45	0	0	5.00	0.00
Total Average	96%	4%	0%	4.89	0.27

4.2 기술적 영역에서의 점검항목 설문 결과

기술적 영역에서 점검항목에 대한 설문 결과는 도출된 8개 점검항목 중에서 권한이 없는 환자 접근시 사유관리 정책, 특정 환자 기록의 정보보호 대책, 모든 환자 데이터 암호화 정책과 OCS, EMR, PACS 백업에 대한 대책에서 4개 점검항목이 공히 평균 5.0으로 매우 필요한 것으로 나타났으며, 모든 영역에서 매우필요 항목의 응답률이 97%로 점검항목의 도출이 적정함을 보여주고 있다.

〈Table 15〉 Results of Check Lists in Technical Domain

Check Lists	5~4	3	2~1	Avg	SD
Are there any managements for unauthorized patient access ?	45	0	0	5.00	0.00
Are there any information protections for specific patient's records ?	45	0	0	5.00	0.00
Did you select and implement the malicious code measures for hospital programs ?	44	1	0	4.89	0.32
Did you select and implement the requirements for medical access control ?	45	0	0	4.93	0.23
Did you encrypt all patient's data?	45	0	0	5.00	0.00
Did you select and implement the backup measures like OCS, EMR, PACS ?	45	0	0	5.00	0.00
Did you select and implement the audit considerations for hospital information system ?	43	2	0	4.84	0.39
Did you select and implement the medical information exchange measures ?	45	0	0	4.96	0.19
Total Average	97%	3%	0%	4.93	0.18

4.3 관리적 영역에서의 점검항목 설문 결과

관리적 영역에서 점검항목에 대한 설문 결과는 진료, 영상, 간호 기록업무를 총괄하는 책임자 지정과 진료정보를 진료목적 외의 다른 용도로 이용할 경우 별도의 동의 여부에서 평균 5.0으로 나타났으며, 모든 점검항목의 평균이 4.76 에서 5.0 으로 설문 의견을 나타내어 모든 영역에서 매우필요 항목의 응답률이 95%로 점검항목의 도출이 적정함을 보였다.

〈Table 16〉 Results of Check Lists in Administrative Domain

Check Lists	5~4	3	2~1	Avg	SD
Do you have the internal management plan for the medical institutes working more than five people ?	43	2	0	4.84	0.39
Can you check the contents for medical information except medical laws ?	42	3	0	4.76	0.48
Do you have a supervisor for managing the medical care, video, nursing record ?	45	0	0	5.00	0.00
Do you have any consents if you use another purpose except medical purpose ?	45	0	0	5.00	0.00
Do you have the medical information which has the retention period ?	45	0	0	4.91	0.26
Total Average	95%	5%	0%	4.91	0.22

병원정보시스템 정보보호 감리 점검항목의 3가지 영역에서의 18개 점검항목에 대한 5점 척도 설문 결과 평균 4.76점 이상으로 점검항목이 매우 필요하다고 응답하였으며 기술적 영역이 전체 평균점에서 가장 높은 점수를 보였다. 3가지 영역의 전체 평균은 4.91로 제안한 정보보호 감리 프레임워크의 점검항목들의 도출이 적적함을 보였다.

〈Table 17〉 Total Results of HIS Audit Model

Audit Domain	Number of Checklist	Total Average	Average	
			Lowest	Highest
Physical	5	4.89	4.80	5.00
Technical	8	4.93	4.78	5.00
Administrative	5	4.91	4.76	5.00
Total	18	4.91	4.76	5.00

5. 결론 및 향후 연구과제

2000년대 들어서면서 의료분야의 정보화 속도가 급속하게 발전하면서 예전의 종이 의무기록 시절과는 달리 대용량의 데이터베이스를 보유하고 있고, 병원 경영을 위한 다양한 서비스, 진료 활성화와 진료의 질 향상을 위한 첨단 의료 IT의 발달로 의료정보가 방대해짐에 따라

의료정보 보호가 중요해졌다[7]. 따라서, 병원정보시스템 구축 시 의료 분야에 맞는 국내외 위험관리 표준절차에 따라 위험을 분석 및 평가하여 정보보호 대책을 적절하게 마련하도록 점검 및 문제점을 개선토록 정보보호 감리를 수행하며 지속적인 위험관리를 통해 정보보호 수준을 유지할 수 있도록 정보보호관리체계(ISMS)를 수립 및 관리해야 한다.

본 논문에서는 정보보호관리체계(ISMS)를 기준으로 병원관련 인증과 정보보호관리 인증들을 조사 비교 분석하고 의료정보 보호에 제일 적합한 ISO27799 인증을 제시하고 설명하였다. 또한 병원분야 정보 보호 요구사항을 ISO27799기반의 병원정보시스템 정보보호를 물리적, 기술적, 관리적 영역으로 분류하고 각각에 세부적으로 정보보호 점검항목을 도출하였다. 또한 ISO27799의 위험관리 절차에 맞추어 정보보호 감리시점을 수립하고 점검항목과 ISO27799 통제분야를 매핑함으로써 보안성과 효율성을 동시에 향상시킬 수 있도록 설계하였으며, 전문가의 설문을 통하여 적합성을 검증하였다.

그러나, 본 논문에서 제시한 모형에 대해 다음과 같은 한계점이 있으며 이에 대한 향후 연구가 필요하다.

첫째, 향후 연구에서는 의료정보의 요구사항 및 위협요소 대책에 대해 ISO27799가 얼마나 잘 반영되어 있는지 정확한 검증이 필요하다.

둘째, ISO27799가 국제 표준이다 보니 국내 의료기관과 다른 부분이 존재할 수 있고, 모든 의료기관의 의료정보화 수준이 동일하지 않다는 부분도 감안되어야 할 것이다.

셋째, 현재 대형병원에서 적용하고 있는 정보보호체계는 주로 ISO27001을 도입하고 있다. 국내 의료기관에서 ISO27799 도입을 통한 효과성을 검증해야 할 것이다.

끝으로 본 연구는 실제 병원정보시스템 구축 및 운영사업에 적용하여 효과성을 검증하지 못한 한계를 가지고 있다. 그러나, 실제적인 병원정보시스템 정보보호 감리에 적용해 나가면서 수정, 보완하면 실무적으로 병원정보시스템의 정보보호 감리모형으로 기여할 것으로 판단되며, 제안한 감리모형으로 자리 잡을 수 있도록 향후 추가적인 연구가 필요하다.

ACKNOWLEDGMENTS

This paper was supported by the Shamyook University Rearch Fund in 2013.

REFERENCES

[1] Dae-Won Moon, Si-Young Jang, Information System Managements-Business Managements, System Development and Audit Practices, Seoul: Myungkungsa, 1998.

[2] B. C. Mun, D. S. Kim, H. W. Kim, The Audit Model for efficient Hospital Information System Construction, Korea Society of IT Services, Vol. 11, No. 2, pp.197-211, 2012.

[3] Korea National Information Society Agency, Information System Audit Guideline Manual V3.0, Korea National Information Society Agency, 2008.

[4] ISO/IEC 27799, Health informatics - Information security management in health using ISO/IEC 27002, ISO, 2008.

[5] Sung-Hyun Park, The Suggestion of the Medical ISMS for the Small and Medium Hospitals and the Study on the Consulting Method Regarding to the Technical Protection, Master of Engineering dissertation, Graduate School of International Information of Dongguk University, 2013.

[6] Hye-Jung Kim, A Study on Indicator Development to Evaluate Hospital Information System : based on Balanced Scorecard Method, Master of Public Health dissertation, Graduate School of Public Health of Yonsei University, 2006.

[7] Hyung-Goo Kang, A Study on the Personal Health Information Security in Hospitals, Master of Engineering dissertation,, Graduate School of Information Communication of Konkuk University, 2012.

[8] Hyung-Ae Kim, Nursing Information System Development for Improving Nursing Work, Master of Nursing dissertation, Graduate School of

Chungang University, 2004.
[9] Ki-Ho Yeo, A study of ISMS application in health organization using ISO 27799, Master of Engineering dissertation,, Graduate School of Information Communication of Konkuk University, 2012.
[10] J. Y. Lee, D. S. Kim, H. W. Kim, A Design on the Inforamtion Security Auditing Framework of the Information System Audit, Korea Society of Digital Industry and Information Management, Vol. 6, No. 2, pp.233-245, 2010.
[11] H. S. Hwang, G. H. Lee, A Study on the Mobile Security for Secure Smartwork Improvements, Korea Institute of Information Security and Cryptology, Vol. 21, No. 3, pp.22-34, 2011.
[12] H. C. Lee, J. H. Yi, K. W. Sohn, Smartwork Security Threats and Measures, Review of Korea Institute of Information Security and Cryptology, Vol. 21, No. 3, pp.12-21, 2011.
[13] Hojun Jegal, Juhyung Lee and Taekgu Kim., *Scaling software agility : best practices for large enterprises*., Euiwang.: Euiwang Publishing Inc, 2008.

유 완 희(Yu, Wan Hee)

・2013년 8월 : 건국대학교 정보통신대학원 (공학석사)
・2013년 1월 ~ 2014년 3월 : 인투데이터시스템 대리
・2014년 4월 ~ 현재 : ㈜투비텍 과장
・관심분야 : 정보시스템 감리, 프로젝트 관리, 데이터베이스, 소프트웨어 공학
・E-Mail : top215@naver.com

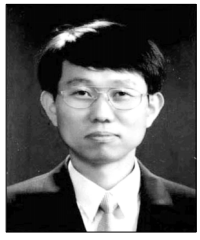
김 동 수(Kim, Dong Soo)

・1981년 2월 : 광운대학교 전자계산학과(이학사)
・2001년 2월 : 서울산업대학교 전자계산학과(공학석사)
・2005년 2월 : 국민대학교 경영정보학과(경영학박사)
・1991년 12월 : 전자계산조직응용기술사 취득
・1995년 8월 정보통신기술사 취득
・1998년 2월 ~ 현재 : (주)키삭 대표컨설턴트
・2008년 3월 ~ 현재 : 건국대학교 정보통신대학원 겸임교수
・관심분야 : u_city 감리, 프로젝트 관리, 정보시스템 감리, 소프트웨어 공학
・E-Mail : dskim@kisac.co.kr

한 기 준(Han, Ki Joon)

・1979년 2월 : 서울대학교 수학교육학과(이학사)
・1981년 2월 : KAIST 전산학과(공학석사)
・1985년 2월 : KAIST 전산학과(공학박사)
・1990년 1월 ~ 1991년 1월 : Stanford 대학 전산학과 Visiting Scholor
・1985년 3월 ~ 현재 : 건국대학교 컴퓨터공학부 교수
・관심분야 : 데이터베이스, GIS, LBS, 텔레매틱스, 정보시스템 감리 등
・E-Mail : kjhan@db.konkuk.ac.kr

김 희 완(Kim, Hee Wan)



・1995년 8월 : 성균관대학교 정보공학과(공학석사)
・2002년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
・1996년 5월 : 정보관리기술사 취득
・2007년 1월 : 정보시스템 수석감리원 자격 취득
・2001년 3월 ~ 현재 : 삼육대학교 컴퓨터학부 교수
・관심분야 : 정보시스템 감리, 프로젝트 관리, 데이터베이스, 정보시스템 보안, 데이터 보안
・E-Mail : hwkim@syu.ac.kr