디지털산업정보학회 논문지 제6권 제2호-2010년 6월

정보시스템 감리에서의 정보보호 감리모형 설계

이 지 용* · 김 동 수** · 김 희 완***

A Design on the Information Security Auditing Framework of the Information System Audit

Lee, Ji Yong · Kim, Dong Soo · Kim, Hee Wan

〈Abstract〉

This paper proposes security architecture, security audit framework, and audit check item. These are based on the security requirement that has been researched in the information system audit. The proposed information security architecture is built in a way that it could defend a cyber attack. According to its life cycle, it considers a security service and security control that is required by the information system. It is mapped in a way that it can control the security technology and security environment. As a result, an audit framework of the information system is presented based on the security requirement and security architecture. The standard checkpoints of security audit are of the highest level. It was applied to the system introduction for the next generation of D stock and D life insurance company. Also, it was applied to the human resources information system of K institution and was verified. Before applying to institutions, system developers and administrators were educated about their awareness about security so that they can follow guidelines of a developer security. As a result, the systemic security problems were decreased by more than eighty percent.

Key Words : Security Architecture, Security Audit Framework, Information System Audit

Ⅰ. 서론

정보시스템감리를 수행함에 있어 기본이 되는 지침으로는 정보시스템감리기준[1]이 있다. 그러나 최신의 개발방법론과 새로운 유형의 사업에 대한 점검항목이 미비하여 실제로 감리현장에서 적용하기 어려움에 따라 감리시에 참고할 수 있는 새로운 감리지침의 개발 필요성이 제기되고 있다.

정보시스템은 매우 방대한 자산으로 이루어져 있으며 조직의 특성상 고유하면서도 중요한 역할을 담당한다. 기업에서는 정보화 사업의 수행에 있어서 정보시스템 개

* 서울지방경찰청 사이버수사관(제1저자)
** (주) 키삭 대표컨설턴트
*** 삼육대학교 컴퓨터학부 부교수(교신저자)

발의 목적 달성 및 운영의 효율성 향상을 위하여 개발단계에서부터 외부 감리업체 및 정보 보호 전문 업체를 통한 외부감리 혹은 내부감리를 실시해 오고 있다. 또한 정보화 사업은 정보시스템에 대한 도입, 개발, 운영 및 유지보수를 중심으로 이루어지기 때문에 이러한 정보화 사업 전 과정을 통해 정보보호 측면에서 충분한 고려가 되어야만 시스템의 성공적인 개발은 물론 시스템 인수 이후에도 조직의 정보보호 관리를 보장할 수 있으며, 유지보수로 인한 불필요한 예산소요를 방지하는 등 성공적인 정보화 사업을 기대할 수 있다.

한국정보사회진흥원에서 2004년 12월에 발간한 '정보시스템 보안 감리지침 연구'에는 시스템 개발공정과 시스템 운영공정에 대하여 감리영역별로 시스템 아키텍처 영역, 응용시스템 영역, 데이터베이스 영역으로 나누어 점검 항목을 기술하고 있다[2]. 이는 해당기관의 보안정책에 부합되는 정보보호감리항목을 도출하기 위한 해당기관이 보유하고 있는 정보자산 식별이 모호하고, 개별 공공기관에 따라 다루는 정보유형의 성격이 매우 상이하나, 획일적인 보안등급 기준을 설정하여 보안감리항목을 작성하였다는 제한사항이 있다.

현재까지 실시되어온 정보시스템 감리는 최소한의 정보보호 분야에 대한 점검과 평가를 수행함으로써 사업 개발단계나 운영단계에 있어서의 충분한 정보보호 요구를 충족시킬 수 없었다. 정보보호 문제에 대한 분석과 평가는 정보시스템의 개발단계에서부터 행해졌을 때 조직이나 시스템의 정보보호 관리의 효율성 향상을 기대할 수 있다. 따라서 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.

최근에는 한국정보사회진흥원을 중심으로 개발단계에 대한 정보보호감리지침을 연구하거나 시스템 개발 공정별로 정보보호 분야에 대한 감리지침 연구가 수행되기도 하였으나 정보보호감리에 대한 체계적인 감리지침은 아직까지 마련되지 않은 상태이며 평가항목 또한 충분치 못한 것이 현실이다. 따라서 정보화 사업에 있어서 체계적인 정보보호감리를 통한 정보시스템의 성공적인 구축과 운영은 반드시 필요한 사항이라 할 수 있다.

본 논문에서는 정보시스템 정보보호감리의 필요성과 현행 정보시스템 보안 감리지침에 대해서 살펴보고 정보화 사업 감리영역별 정보시스템 개발 정보보호감리 항목을 제안한다. 제안 항목으로는 정보화 사업에서의 정보보호 요구사항을 근거로 시스템생명주기(SDLC)에서의 주요 감리항목을 작성하였다. 또한, IT 관점에서 자산을 체계적으로 파악하고 관리하기에 용이하도록 감리영역을 하드웨어, 소프트웨어, 네트워크 영역으로 분류하였다. 분류된 항목에서 정보보호감리 항목을 추출하기 위하여 정보보호아키텍처의 보안[4-5], Cobit4.0[7], ISO/IEC12207[8], ISO27001[9], 정보보호관리체계(ISMS : Information Security Management System)[9]를 참조하여 감리항목들을 도출하였다.

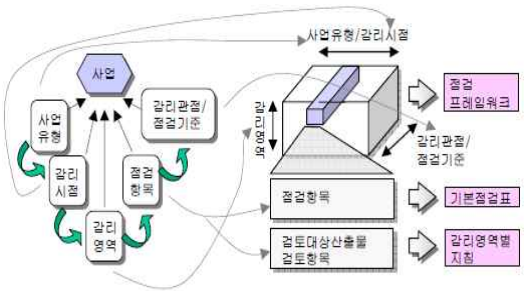
Ⅱ. 관련 연구

2.1 정보시스템 감리

「정보시스템의 효율적 도입 및 운영 등에 관한 법률」에서 감리기준은 감리의 계약, 감리계획 수립, 착수회의, 현장 감리, 감리보고서 작성, 감리결과 조치내역 확인 등 감리업무를 효율적으로 수행 할 수 있도록 감리의 절차 및 방법을 규정하고 있으며, 정보시스템의 구축·운영에 관한 사항을 종합적으로 점검·평가 할 수 있도록 정보시스템 감리 기본점검표를 제시하고 있다 이에 기본점검표를 중심으로 기본점검표의 구성 배경 및 기본점검표에서 정의된 점검항목을 점검하기 위한 점검항목별 검토항목을 사업유형/감리시점/감리영역별 지침으로 제시하고, 기본점검표와 감리영역별 지침에 대한 활용체계를 권고한다[3].

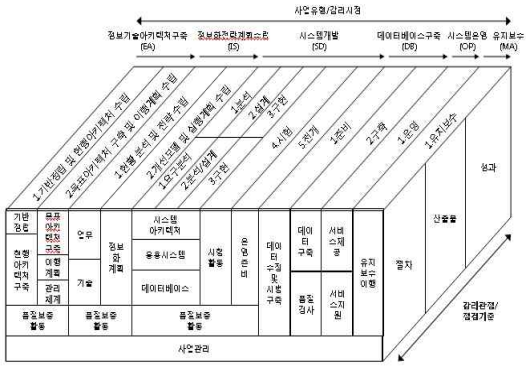
사업유형기반 점검체계는 감리 대상이 되는 정보화사업의 유형에 따라 감리를 시행하기 위한 점검체계이다. 이에 감리기준의 기본점검표에 대한 확장가능성과 체계적 안정성을 높이기 위한 개념적 모델을 정립하였다[6].

이러한 개념모델을 바탕으로, 사업유형기반 점검체계의 구성요소인 정보시스템 감리점검 프레임워크 와 기본점검표, 감리영역별 지침이 <그림 1>과 같이 도출되었다.



<그림 1> 개념모델과 정보시스템 감리점검 프레임워크

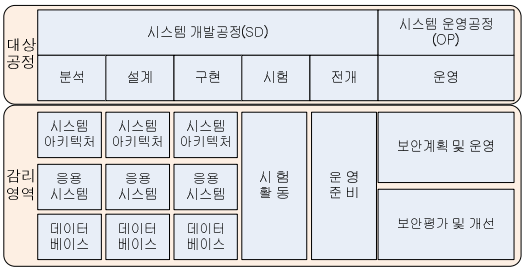
감리점검 프레임워크는 개념모델에 근거하여 사업유형·감리시점, 감리영역, 감리관점·점검기준을 통합하면 아래 <그림 2>와 같은 감리점검 프레임워크가 구성된다[3].



<그림 2> 정보시스템 감리점검 프레임워크

2.2 현행 보안감리 지침의 구성

한국정보사회진흥원에서 개발한 '정보시스템 보안 감리지침 연구'는 점검 프레임워크의 구조적/정보공학적 개발 모델을 기반으로 감리시점과 감리영역을 고려하여 작성되었다[6]. 감리시점으로는 크게 시스템 개발공정(SD)과 시스템 운영공정(OP)으로 구분하였고 세부적으로는 분석단계, 설계단계, 구현단계, 시험단계, 전개단계, 운영단계로 구분하여 각 단계별로 보안 감리 시에 감리인이 참고하여야 하는 점검항목을 도출하고 상세한 감리수행 방법을 기술하였다. 이는 구축하고자 하는 정보시스템의 특성을 고려하여 각 단계 종료 시에는 반드시 검토되어야 할 항목을 기준으로 감리를 수행할 수 있음을 의미한다. 한국 전산원의 보안 감리지침 대상공정과 감리영역은 <그림 3>와 같다[3].



<그림 3> 정보시스템 보안감리 공정 및 영역

감리영역별로는 시스템 아키텍처 영역, 응용시스템 영역, 데이터베이스 영역으로 분류하였다. 감리영역별로 보안점검항목을 도출함으로써, 각 분야의 감리인이 시스템의 보안상태를 함께 점검할 수 있도록 하여 시스템 아키텍처 영역에만 치중했던 보안영역을 각 분야에서 세심하게 검토할 수 있도록 지침을 작성하였다. 시스템 아키텍처는 플랫폼(하드웨어, 시스템 소프트웨어, 네트워크 구성요소)과 기술아키텍처(개발, 실행, 운영 아키텍처)를 집합적으로 의미한다. 응용시스템은 업무 시스템의 자동화된 부분으로 특정 업무를 수행하기 위해 필요한 프로그

램을 의미하며 플랫폼과 상호 응용 아키텍처는 포함하지 않는다. 데이터베이스는 데이터베이스를 관리하는 운영체제를 제외하고 업무를 지원할 수 있도록 데이터를 받아들이고 저장, 공급하기 위하여 일정한 구조를 가지는 데이터 집합에 대한 영역이다.

현행 정보시스템 감리기준의 기본 점검표는 각 공정별로 감리 영역을 구분하여 세부 점검사항을 제시하고 있으며, 정보시스템 개발공정에서 감리영역을 시스템 아키텍처로 한정하여 검토항목을 살펴보면 다음과 같이 분석단계에서 4개항, 설계단계에서 3개항, 구현단계에서 2개항으로 구분되어 있음을 알 수 있다.

이를 각 단계별, 감리영역별로 정리하면 다음 <표 1>과 같다

<표 1> 시스템 아키텍처의 주요검토 항목

단계	감리영역	주요검토항목
분석	시스템 요구사항	▪ 기존시스템 및 새로운 시스템의 운영환경 분석의 적성적 ▪ 시스템 요구사항의 명세화의 적정성 ▪ 하드웨어, 네트워크, 시스템 소프트웨어의 식별의 적정성
	개발 시스템 구조의 설계 및 설치	▪ 개발 시스템 구조의 설계 및 설치의 적정성
설계 및 구현	운영 시스템 구조 설계	▪ 요구사항의 운영 시스템구조 설계 반영의 적정성 ▪ 시스템 구조의 구성항목에 대한 용량산정의 적절성 ▪ 외부 시스템과의 인터페이스 설계의 적절성
	운영 시스템 구조 구현	▪ 운영 시스템구조 설계결과 반영구현의 적정성 ▪ 운영 시스템구조 시험계획의 적정성

2.3 현행 보안감리 지침의 문제점

현행 보안감리와 관련한 문제점을 보다 구체적으로 파악하면 다음과 같다.

첫째, 보안감리에 대한 인식 및 연구가 부족하다. 보안을 하나의 감리 분야로 인식하지 않고 시스템 아키텍처의 하나로 인식하고 있어, 보안 감리에 대한 체계적인 연구가 이루어지고 있지 못하고 시스템 아키텍처의 일부분으로 연구되거나 점검항목을 도출하였을 뿐이다. 그러나 보안은 시스템 아키텍처 뿐 아니라, 응용프로그램, 데이터베이스, 운영체제, 관리적인 부분, 물리적인 부분 등 정보시스템 전 부분의 요소로 포함되어 있기 때문에 기존의 연구와 감리 수행으로는 한계가 있다.

둘째, 보안감리를 수행하기 위한 감리원의 정보보안 수준이 미흡하다. 보안에 대한 중요성을 인식하기 시작한 시기는 불과 몇 년 되지 않았으며, 보안 기술의 급속히 발전하고 있으나 보안 분야에 대한 연구와 관련된 지침이 부족하여 감리원의 보안 분야에 대한 수준이 미흡한 상황이다.

셋째, 보안감리를 위한 여건이 아직 성숙되어 있지 않다. 시스템 아키텍처와 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.

이러한 문제점이 해결되지 않은 상황에서도 정보보호 기술은 비약적으로 발전하여 정보보호 아키텍처를 구축하는 수준에까지 도달했다. 따라서 현재의 보안 감리 수행 방법으로는 정보보호아키텍처에 대한 감리를 수행하기 어렵다고 판단되며, 인식부족, 인력부족, 예산부족 등의 상황에서도 급증하는 보안 요구를 수용하여 정보보호 아키텍처에 대한 감리를 수행하기 위해서는 새로운 정보보호감리 접근 방법이 필요한 설정이다.

2.4 현행 보안감리 지침의 개선의 필요성

정보시스템 감리는 감리기준에 정의된 절차와 방법에 따라 시행되고 있으며, 감리결과로 제시되는 감리 보고서에서는 감리 분야별로 현장 감리를 통하여 발견된 사업의 주요한 문제점과 개성방향을 제시하는 세부 지적사

항과 이를 토대로 사업의 성패에 큰 영향을 미칠 수 있는 사항을 종합적으로 판단하여 제시하는 감리 분야별 검토의견이 있다.

실제 시스템에 대한 개선 작업은 세부 지적사항을 토대로 개선되기 때문에 세부 지적사항이 매우 중요하다고 할 수 있으며, 현장 감리에 참여한 감리인은 감리 분야별로 사업의 진행상태 또는 결과를 감리 입장에서 함축, 평가하여 감리 검토의견(적정, 보통, 부적정의 판정(평가))을 감리 보고서에 제시한다.

이와 같은 검토의견은 감리 업무의 특성상 참여한 감리인의 주관적이고 전문적인 판단에 근거하여 영역별 검토의견이 제시된다. 그러나 감리 검토의견은 감리 영역별로 일종의 평가 개념이 도입되어 정보화 사업추진의 적정성 여부를 판정하는 역할을 수행하고 있기 때문에 객관적인 판단에 근거하지 않는 경우, 분쟁의 소지가 있다.

그러나 정보시스템 감리 기준은 그 동안 정보시스템 개발 보안을 위해 변화된 사항을 반영하지 못하여 판단은 오직 투입된 감리인의 경험에 의존하거나, 정보보호 전문업체의 전문 컨설턴트의 의견을 반영하고, 감리인마다 다른 해결책을 제시하는 수준에 머물러 있어 사업의 특성에 맞는 감리지침 개선이 필요하다.

2.5 개발 단계별 주요 정보보호 요구사항

새로운 정보시스템을 개발할 때, 개발 단계별로 정보보호에 관한 제반 문제를 분석, 평가하고 개선사항을 도출하여 개발시스템에 반영함으로써, 정보시스템의 개발 이후 발생할 수 있는 문제점들을 사전에 식별하여 예방할 수 있으며, 시스템의 안전성과 신뢰성을 보장할 수 있게 된다. 개발 단계의 구성은 방법론에 따라 약간의 차이를 보이나 ISO표준[8, 9], 국내표준[2], NIST[10]등에 의거하여 분석, 설계, 구현, 시험의 4단계로 구분하고 이에 대한 단계별 정보보호 활동을 도출한다. 개발 보안감리는 4단계로 구분된 각 개발 단계별 정보보호 활동이 이루어지고 있는지 점검하게 된다.

2.5.1 분석 단계

분석단계는 정보시스템 개발을 준비하는 단계로 정보시스템 개발 과정에서 가장 중요하고 어려운 작업이면서 간과되기 쉬운 작업이라고 할 수 있다. 분석 단계에서는 프로젝트 대상이 되는 정보시스템이 무엇인지를 정의하고, 이 정보시스템이 처리하는 기본적인 정보가 무엇인지 파악해야 한다. 또한 이 단계에서 정보시스템 개발을 위한 전체적인 프로젝트 수행 계획에 정보보호를 위한 일정계획 및 자원계획이 반영되어야 한다. 정보시스템의 규모가 크거나 또는 중요할 경우 별도로 ISP사업을 거쳐 정보시스템의 아키텍처 개발 및 마스터플랜을 수립하기도 한다[2].

일반적으로 정보보호 요구사항은 기밀성, 무결성, 가용성, 책임추적성 등의 관점에서 도출된다. 기밀성 요구사항은 정보시스템 내 비밀정보 분류, 정보시스템 기능의 제한 등을 포함한다. 무결성 요구사항은 정보시스템 내 정보를 변경할 수 있는 개인/업무 식별, 정보시스템 자체의 무결성, 정보시스템의 변경 기능에서의 무결성 보장 등을 포함한다. 가용성 요구사항은 모든 구성요서의 가용성 요구사항을 식별할 필요가 있으며, 정보시스템 구성요소간의 의존성 및 상호작용을 파악하고 네트워크 등 인프라의 가용성 요구사항을 식별해야 한다. 책임추적성 요구사항은 사용자 식별 및 인증 과 정보보호 사고 조사시 필요한 정보를 제공하기 위해 감사에 대한 요구사항을 포함한다[2].

2.5.2 설계 단계

설계단계는 분석 단계에서의 요구사항이 정보시스템으로 구현되기 위해 해석되고 구체화 되는 과정으로, 정보시스템의 요구사항을 반영하기 위해 정보시스템 설계팀이 기본설계와 상세설계를 한 후, 정보보호 요구사항의 만족 여부를 판단하기 위해 정보보호 전문가에게 설계 결과를 보여주고 의견을 구하기도 한다. 일반적으로

정보시스템 설계팀은 정보보호 요구사항에 대한 전문성이 부족하기 때문에, 정보시스템 설계 내에 정보보호 요구사항이 충분히 반영되지 않을 가능성이 높다. 따라서 정보시스템 설계 결과에 대해 정보보호전문가는 많은 검토의견 및 제안을 제시할 수밖에 없으며, 정보시스템 설계팀은 이를 다시 설계에 반영하기 위해 재작업에 들어가게 되는 것이 관행적으로 반복되어 온 것이 사실이다.

이러한 전통적인 정보시스템 설계과정은 정보보호 전문가의 적극적인 개입이 배재된 상태에서 정보보호 방법이 정보시스템 설계에 반영되어 온 방식으로서 매우 비효과적이며 비효율적이라고 볼 수 있다. 보다 효율적이고 효과적이며 안전한 설계를 위해서는 정보보호 전문가가 정보시스템 설계팀에 포함되어 설계과정 초기부터 정보보호 요구사항이 반영될 수 있도록 해야 하며, 또한 정보보호 기능과 정보시스템 기능간의 다양한 상쇄효과를 고려해서 설계될 수 있도록 통합된 설계 접근방식을 사용해야 한다[2].

또한, 정보시스템 설계시 정보보호를 반영할 때, 비용대 위험가능성 상쇄효과를 고려해야 한다. 즉, 위험을 감소시키기 위해서는 정보보호 구현비용이 초래되고, 반면 위험을 방치하면 조직에 손실을 미칠 수 있는 가능성이 있으며 이는 곧 조직의 비용으로 간주되기 때문이다. 따라서 조직에 100% 완전한 정보보호는 있을 수도 없으며, 또한 그러한 방식의 정보보호는 비용 효과적이지 못하므로, 적절한 수준에서 위험을 감소시킬 필요가 있다. 즉, 조직은 수용가능 한 위험수준을 결정해야 한다.

2.5.3 구현 단계

구현 단계에서는 하드웨어 획득, 소프트웨어 도입 또는 개발 작업과 단위 시험 등의 작업을 위해 정보보호 구현 및 검토, 운영관리계획 및 지침 개발 활동이 수행된다. 정보보호의 관점에서는, 설계단계에서의 수립한 정보보호 아키텍처가 구현단계에 명확하게 이행되는지를 파악하는 것이 필요하다.

이러한 구현은 네트워크, 서버, 어플리케이션 영역이 중요하다. 어플리케이션 영역은 실제 정보보호 설계 요건들이 코딩에 반영되어야 하기 때문에 코딩 시에는 정보보호 설계요건을 만족하기 위해 사용자 데이터 입력시 무결성을 체크하기 위한 입력 체크 프로그램, 기밀성을 보장하기 위한 암호화 프로그램 등 다양한 정보보호 관련 모듈들을 개발해야 한다. 뿐만 아니라 개발 언어에 대한 구체적인 정보보호 취약성을 해결하기 위한 노력이 필요하다. 즉, JAVA, ASP, C, PHP 등 각 개발 언어에 따라 공통적이거나 각 언어의 특성에 따른 정보보호 취약성이 존재하므로 이러한 문제를 해결하기 위해 각 개발 언어에 해당되는 표준적인 정보보호 코딩 지침을 적용하여 오류 없는 소프트웨어 개발을 유도해야 한다[2].

사용 제품을 도입할 경우, 상용 제품이 정보보호 요구사항을 만족시키지 못할 수도 있으므로 정보보호 요구사항 만족여부를 판단해야 하며 필요한 경우, 상용 제품에 대해 수정을 요구하거나 이를 보완할 수 있는 관리적, 기술적 및 물리적 대책을 고려해서 추가로 구현해야 한다. 또한 이 단계에서는 향후 이 정보시스템이 이관되고 운영될 경우의 정보보호 계획을 수립해야 한다[2].

2.5.4 시험 단계

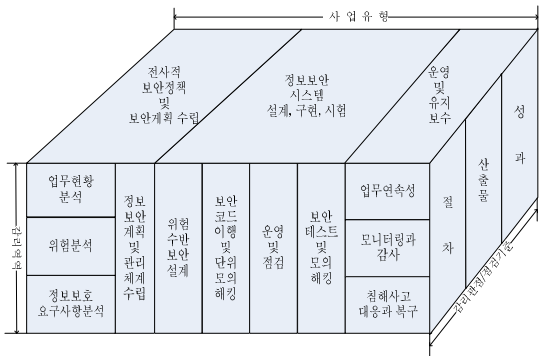
시험 단계에서는 개발이 완료된 정보시스템이 정보보호 요구사항을 만족 하는지 정보보호 시험, 이관을 위한 정보보호 설정, 이관 후 정보보호 시험 활동이 수행된다. 시험 과정에서도 정보보호 요구사항이 만족되는지에 대한 시험절차가 준비되어야 한다. 시험 단계는 기능시험, 통합시험, 인수시험 등 기능 및 사용자의 요구사항 만족여부에 대한 검증 작업이 수행된다.

시험은 정보보호 요구사항과 설계요건이 구현단계에서 명확히 반영되었는지를 파악하는 것이기 때문에 정보보호 아키텍처의 각 계층에 따라 이루어져야 한다. 그러나 모든 실패 가능성을 시험할 수는 없으므로 인수시험은 일반적으로 긍정적인 문구로 문서화된 요구사항 위주

로 실시된다.

시험이 이루어진 후에 이관을 하면, 개발된 정보시스템이 기존의 운영환경에 연결되게 된다. 이 경우 또 다른 시험이 필요하게 된다. 즉, 기존의 운영환경과 연계 사에서 정보보호 문제가 없는지 시험이 필요하다. 기존 네트워크망에 신규 개발 정보시스템이 설치될 경우 기존 네트워크망의 정보보호 요건이 신규 개발 정보시스템의 정보보호 요건에 적합한지 시험해야 한다. 또한 기존의 정보보호환경이 신규 정보 시스템과 연동에 문제가 없는지 시험해야 한다. 또 다른 중요한 시험은 침투테스트이다. 정보보호 여건들이 모두 반영되었을 경우 실제 침투에 얼마나 안전하게 반응하는지를 시험해야 한다. 이 시험을 통해 기존 정보시스템의 안전성을 확인할 수 있다[2].

감리 사업의 유형과 감리영역 그리고 감리 관점/감리 기준을 하나로 구성하여 정보보호 감리 프레임워크를 도식하면 <그림 4>와 같다.



<그림 4> 정보보호 감리 프레임워크

Ⅲ. 정보보호 감리 모형 제안

3.1 정보보호 감리 모형

정보시스템 정보보안 구축사업은 기존 시스템이나 신규 시스템을 구축 운영하고 있는 조직에서 정보시스템의 보안을 구현하기 위한 방법으로 조직의 정보시스템에 대한 위험 및 취약점 분석을 하여 이를 기초로 위험과 취약점을 줄이기 위한 방법으로 보안 도구를 선정하고 그 설치는 보안 제품을 판매한 보안업체가 주도하여 온 것이 일반적이다. 그러나 이런 방법은 보안 시스템 구성은 일관된 보안정책의 부재와 위험수준의 수용 범위 등에 대한 원칙이 없고 조직의 비즈니스 정책과 목표의 달성에 대한 보안요구에도 부합하지 못하여 정보시스템 보안에 크게 기여하지 못하고 있는 실정이다. 따라서 정보시스템 보안에 관련된 사업을 전사적 보안 정책 및 보안 계획 수립을 별도의 사업으로 시행하고 계획에 근거하여 정보시스템 보안대책을 구현하는 사업을 수행하여 구현된 보안 시스템을 운영/관리하는 것을 구분하여 사업으로 추진하는 것이 적정할 것으로 판단한다.

위 프레임워크를 개발보안주기에 도입을 하면 아래 <표 2>와 같이 개발보안주기(Secure SDLC)[11]에 적용할 수 있다.

<표 2> 개발보안주기별 주요 감리사항

개발보안 프로세스	단계 주요감리사항
분석	▪ 정보보호 요구사항 ▪ 개발보안 정책(언어, 프레임워크 등) ▪ 정보보호 관리체계(규정 및 절차)
설계	▪ 보안 아키텍처 및 코드 설계 ▪ 보안 패턴 및 위험 모델링 ▪ 정보보호 테스트 계획 ▪ SDLC 단계별 보안성 검토 프로세스 개선
구현	▪ 소스코드 취약점 리뷰 및 분석 ▪ 취약점 감사 및 개선
시험	▪ 어플리케이션 취약점 분석 ▪ 취약점 감사 및 개선
운영	▪ 어플리케이션 변화관리 보안성 감리 ▪ 신규보안 취약점 감리 ▪ 주기적인 보안 취약점 감리 ▪ 어플리케이션 방어

3.2 단계별 감리 점검항목 제안

정보보호 감리와 관련된 보안 지침에 관한 연구나 정보시스템 감리점검해설서에 따른 기본 점검항목과 감리지침이 사업별 감리영역에 따른 기본점검항목과 검토항목을 제시하고 있다. 미국의 연방정보시스템에 대한 보안통제 권고, ISO27001, 정보보호아키텍처(EISA) 등을 참조하여 기본점검항목을 도출하였다[9, 10].

3.2.1 전사적 정보보안 정책 및 보안계획 수립

전사적 정보보안 정책 및 보안계획 수립은 AS-IS 분석단계라고 할 수 있는 업무 현황 분석, 위험 분석, 정보보호 요구 사항 분석의 3부분을 가지고 TO-BE인 정보보안 계획 및 관리체계수립을 목적으로 하고 있다. 특히 정보보안 계획 및 관리체계수립은 정보보호관리 국제 규격인 ISO27001을 기준으로 정보보호 관리체계, 자산관리, 인적자원관리 등 크게 10가지의 보안영역으로 정의하여 보안관리체계에 대한 표준화된 평가 및 관리척도를 감리하도록 하였다.

3.2.1.1 업무현황 분석

∨ 보안위험에 노출시 시스템의 안전성에 영향을 유발하게 되는 정보보호 대상 자산을 파악하여 목록을 작성하는 등 문서화 작업이 이루어져 있는지 확인해야 한다.
∨ 정보시스템에 선정된 정보보호 대상 자산에 대한 자산 분류도가 작성되었는지 확인해야 한다.
∨ 정보보호 대상 업무를 선정하여 우선순위를 부여되어 있는지 확인해야 한다.
∨ 장단기 비즈니스 목표와 주진 전략이 수립되었는지 확인해야 한다.
∨ 보안 목표 설정과 자산식별이 이루어졌는지 확인해야 한다.
∨ 보안 대상(정보시스템/자동화 시스템)과 영역식별이 이루어 졌는지 확인해야 한다.

3.2.1.2 위험분석

∨ 전산실 및 정보자산이 있는 모든 장소 및 시설에 대해 예상되는 위협을 식별하여 목록을 작성하는 등 문서와 작업이 이루어져 있는지 확인해야 한다.
∨ 시스템 운용을 위해 사용할 장비 및 설비에 대한 위협요인을 식별하여 목록을 작성하는 등 문서화 작업이 이루어져 있는지 확인해야 한다.
∨ 시스템을 포함한 운용기관의 현 정보보호 수준을 진단하여 취약성을 식별 및 분류하는 등 문서화 작업이 이루어져 있는지 확인해야 한다.
∨ 영역별 취약점 및 위협 분석이 이루어졌는지 확인해야 한다.
∨ 내외부 물리적/환경적 위협 분석이 이루어 졌는지 확인해야 한다.
∨ 정보시스템 및 자동화 시스템에 대한 취약점 분석이 이루어 졌는지 확인해야 한다.

3.2.1.3 정보보호 요구사항 분석

∨ 사용자 데이터 보호, 객체 재사용, 식별 및 인증, 비밀성, 보안기능 보호, 자체시험, 보안관리, 자원활용, 세션설정 및 통제, 감사, 안전한 경로 등의 보안기능 요구사항들이 정의 되었는지 확인해야 한다.
∨ 형상관리, 배포 및 운영, 개발과정, 설명서, 생명주기 지원, 시험과정 취약성 분석 등의 정보시스템 보증요구사항들이 적용되었는지 확인해야 한다.
∨ 시스템을 포함한 운용기관의 정보보호 요구사항이 충분히 이해하고 명확하게 정의하여 문서화하였는지 확인해야 한다.
∨ 정보보호 요구사항을 분석하기 위한 표준의 설정여부와 요구사항에 대한 변경관리가 이루어지는지 확인해야 한다.
∨ 정보보호 요구사항을 분석하기 위한 표준의 설정여부와 요구사항에 대한 변경관리가 이루어지는지 확인해야 한다.
∨ 사업내역과 관련된 정보보호를 달성하기 위해서 프로젝트 요약서가 작성되어 있는지 확인해야 한다.
∨ 사업내역과 관련된 정보보호를 달성하기 위해서 정보

보호 프로젝트 설계서가 작성되었는지 확인해야 한다.
∨ 보안관련 제도와 규정 및 표준 분석이 이루어 졌는지 확인해야 한다.
∨ 상호 접속 및 통합 사양과 보안요구 사항이 분석 되었고 이루어 졌는지 확인해야 한다.

3.2.1.4 정보보안 계획 및 관리체계 수립
∨ 정보보호를 위한 관리방향과 지원사항 및 조직의 구성과 역할 및 책임을 규정하고 있는지 확인해야 한다.
∨ 정보자산 보호를 위한 분류체계 정의 및 보안등급에 따른 통제를 명시하고 있는지 확인해야 한다.
∨ 조직 구성원의 고용, 업무수행 및 퇴직 시 따라야 할 보안 관리체계를 정의하고 있는지 확인해야 한다.
∨ 정보자산에 대한 물리적, 환경적 보안요소를 정의하고 통제하도록 규정하고 있는지 확인해야 한다.
∨ 시스템 및 네트워크 운영 시 준수하여야 할 절차와 관리활동을 규정하고 있는지 확인해야 한다.
∨ 정보자산 및 서비스 이용 시 적용하여야 할 통제 항목과 활동을 규정하고 있는지 확인해야 한다.
∨ 정보시스템 개발 및 유지보수 시 보안 교구사항 및 통제 항목과 활동을 규정하고 있는지 확인해야 한다.
∨ 보안사고 관리를 통한 보안사고 피해 감소 및 재발 방지를 위한 활동을 규정하고 있는지 확인해야 한다.
∨ 장애, 재해 등 비상시 업무의 연속성을 확보하기 위한 활동을 규정하고 있는지 확인해야 한다.
∨ 수립된 보안정책 및 보안기술 표준의 준수 여부를 확인하기 위한 활동을 규정하고 있는지 확인해야 한다.
∨ 보안 정책에 따른 장비 보안 전략이 식별되고 설정 되었는지 확인해야 한다.

3.2.2 정보시스템 설계, 구현, 시험

3.2.2.1 위험 수반 보안 설계
∨ 현행 시스템의 네트워크 구성과 영역별 구성 및 기술적 특성이 분석되었는지 확인해야 한다.
∨ 영역별 시스템과 정보에 대한 무결성, 접근통제, 미디어 보호, 물리적, 환경적 보호 등의 대책수립, 등 보안 특수조건이 요구되는 시스템에 대한 보안 대책이 수립 되고 디자인 되었는지 확인한다.
∨ 조직의 정보요건에서 도출된 개념 테이터 모형과 데이터 사전, 데이터 규칙과 관련 표준을 바탕으로 전체 데이터 모델, 시스템 데이터 모델, 프로젝트 데이터모델로 상세히 설계되어 있는지 확인 한다.
∨ 응용시스템의 요건과 응용서비스 유형을 파악하여, 각 응용 시스템 별 네트워크 트래픽 특성 및 성능 요건이 설계 되었는지 확인한다.
∨ 정보시스템 서비스의 계속성을 보장하기 위한 주요 정보시스템 아키텍처 구성요소 별 이중화 요건 및 백업요건을 설계 하였는지 확인한다.
∨ 안전한 로그온 절차, 식별 및 인증관리에 의해 인가된 사용자만이 체계에 접근 가능하도록 하는 접근 통제 방안이 설계서에 반영되어 있는지 확인해야 한다.
∨ 네트워크를 통해 체계에 접근하는 사용자에 대한 통제 방안이 설계서에 반영되어 있는지 확인해야 한다.
∨ 사용자 별 접근권한 관리를 포함한 체계 접근통제에 대한 통합관리방안이 설계되어 있는지 확인해야 한다.
∨ 민감한 정보가 네트워크를 통해 전송될 때 이를 보호할 수 있는 방안이 설계되어 마련되어 있는지 확인해야 한다.
∨ 바이러스 및 악성코드와 해커의 위험에 대한 신속한 인지 및 식별지원으로 조기 대응토록 하는 방안이 설계서에 반영되어 있는지 확인해야 한다.
∨ 물리적 측면에서의 정보보호방안이 설계서에 반영되어 있는지 확인해야 한다.
∨ 제거된 위험 요소에 대한 대응방안이 정보보호 설계서에 반영 되어 있는지 확인해야 한다.
∨ 언어별 보안코드가 시스템 환경에 맞게 설계되어 있는지 확인해야 한다.
∨ 하드웨어 영역의 설계가 관리자/사용자 클라이언트, 서버, 침입차단시스템, 침입탐지시스템, 침입방지시스템, 백업장치 등 6개의 영역으로 세분화 되어 설계 되

었는지 확인 하여야 한다.
∨ 소프트웨어 영역은 운영체제, DBMS, 응용소프트에어의 3개 영역으로 세분화 되어 설계 되었는지 확인하여야 한다.

3.2.2.2 보안 코드 이행 및 단위 모의 해킹
∨ 개발 담당자 및 보안 담당자의 코드 검토가 이루어 졌는지 확인해야 한다.
∨ 자동화된 정적 및 동적 코드 검사가 이루어 졌는지 확인해야 한다.
∨ 시스템, 프로그램, 소프트웨어, 데이터베이스, 네트워크 별로 단위 모의 해킹이 이루어 졌는지 확인해야 한다.
∨ 단위 테스트가 이루어 졌는지 확인해야 한다.

3.2.2.3 운영 및 점검
∨ 구현된 시스템에 대한 일관성, 가용성, 효율성, 편의성에 대한 시험이 이루어졌는지 확인해야 한다.
∨ 구현된 시스템의 보안기능과 효율성 저하여부에 대한 성능시험이 이루어 졌는지 확인해야 한다.
∨ 구현된 통신망의 안정성에 대한 시험이 이루어 졌는지 확인해야 한다.

3.2.2.4 보안테스트 및 모의 해킹
∨ 기능테스트가 이루어졌는지 확인해야 한다.
∨ 위험 수반 테스트 가 이루어 졌는지 확인해야 한다.
∨ 시스템 테스트가 이루어 졌는지 확인해야 한다.
∨ 블랙/화이트 박스 테스트가 이루어 졌는지 확인해야 한다.

3.2.3 운영 및 유지 보수

3.2.3.1 업무연속성
∨ 사업연속성관리 체계를 구성하기 위한 프레임워크가 수립되어 있는가 확인한다.
∨ 사업연속성 계획을 수립하여 세부계획/절차의 문서화가 이루어 졌는지 확인한다.
∨ 사업연속성 테스트, 테스트 결과에 업무연속성계획이 변경 되었는지 확인한다.

3.2.3.2 모니터링과 감사
∨ 서버 시스템 사용 및 운영에 대한 감사 추적성(audit trail)을 확보할 수 있는 기능이 설계에 반영되어 있는지 확인해야 한다.
∨ 정보자원 사용에 대한 모니터링 및 불법행위에 대한 문서화 및 활동이 이루어 지는지 확인한다.
∨ 모든 로그 및 침입탐지 등에 대한 실시간 감시가 이루어지고 있는지 확인해야 한다.
∨ 모든 감사기록에 대한 주기적인 백업과 전송으로 자료손실 방지체계가 확립되어 있는지 확인해야 한다.

3.2.3.3 침해사고 대응과 복구
∨ 보안침해사고를 위한 대응/보고/협력 체계가 구축되어 있는지 확인한다.
∨ 보안침해사고 발생시 처리/복구/보고 관리활동이 이루어 지는지 확인한다.
∨ 보안침해사고 처리/복구 후 재발방지를 위한 정보공유 및 교육활동이 이루어지는지 확인 한다.

Ⅳ. 제안의 검증

본 논문에 정의된 정보보안감리 프레임워크를 검증하기 위하여 D생명보험과 P생명보험의 차세대 시스템 구축, D생명보험과 D증권의 차세대 시스템 구축 및 K기관의 인사정보시스템에 적용하였다.

먼저, 정보보안감리가 적용된 D생명보험과 정보보안감리가 적용이 되지 않은 P생명보험의 차세대시스템에 대한 감리결과는 <표 3>과 같았다.

<표 3> D생명보험과 P생명보험의 감리결과 비교

단계	문서명	D생명보험	P생명보험
전사적 보안정책 및 보안계획 수립	IT보안 환경 분석 보고서	내, 외부 보안 위협 및 분석 완료	보안이 배제된 전산환경 보고서
	위험분석 보고서	정보보안 중심 위험 보고서 작성	정보보안이 없는 일반 위험 보고서
	보안요구사항 정의서	보안 중심 보안 요구서 정의	없음
	정보보호 정책/지침/절차	ISO27001에 맞는 정보보호 정책 제정	기존 정책 지침 적용
정보보안 시스템 설계 구현 시험	보안아키텍쳐 보고서	ISO27001, 정보보호아키텍쳐가 적용된 보안 아키텍쳐 보고서	없음
	정보보호 설계 보고서	보안이 적용된 정보보호 설계서	없음
	개발보안 가이드라인	언어별 보안이슈가 적용된 개발보안 가이드라인	보안이슈가 적용되지 않은 개발보안 가이드라인
	정보보호 진단결과 보고서	개발단계별 완료에 따른 보안 점검	개발 이후 정보보호 전문업체를 통한 보안 점검
	보안 소스코드 리뷰 보고서		
	서버취약점 진단결과 보고서		
	어플리케이션 소스코드 진단보고서		
	모의해킹 진단결과 보고서		
운영 및 유지 보수	보안 모니터링	보안 모니터링 계획에 따른 지침 적용	개발 이후 적용
	침해사고 대응	초기 침해사고대응에 따른 지침 적용	개발 이후 적용
	복구계획	개발과 동시에 복구 계획이 적용됨	개발 이후 적용
기타	ISO27001	차세대 시스템 전개(Open)과 동시에 취득	새로운 프로젝트로 발주
	보안적용 기간	개발, SDLC별 보안적용으로 추가 보안 적용기간 없음	개발이후 보안성 문제로 전체적 보안 점검으로 전개(Open) 지연
	보안 인식	개발초기에 담당자 및 개발자에게 보안 교육으로 보안인식 상승	개발기간에 보안 제외로 개발이후 보안 적용으로 개발자 적응 늦음
	개발 기간	1년	1.5년
	추가 개발기간	없음	보안 적용으로 인한 1.5년의 보안 재적용 및 검증으로 전개(Open) 지연

정보보안 감리가 적용되지 않은 P생명보험의 차세대 시스템은 보안이 배제된 상태에서 개발됨으로 인하여 개발기간의 지연, 시스템 전개(open) 지연, 보안을 위한 새로운 프로젝트 발주 등이 발생한 반면에, 정보보안 감리가 적용된 D생명보험은 시스템 전개(open)와 동시에 ISO27001 취득, 개발기간 단축, 개발 참여자들의 보안 인식 제고 등의 효과를 가져왔다.

다음으로, D생명보험과 D증권의 차세대시스템은 시스템 전개(open)와 동시에 금융결제원에서 요구하는 정보보안요구사항을 만족을 하여 보안성 심의를 통과하고, 국제정보 보호인증인 ISO27001을 동시에 취득을 하는 것이었다. 그러나 프로젝트초기 감리에서 이러한 사항들이 배제가 되어 있었고, 정보보호전문업체가 선정이 되어 프로젝트에 참여를 하면서 차세대시스템 정보보호감리가 재정의 되었다.

'전사적 보안정책 및 보안계획 수립'에서 요구하는 '업무현황분석, 위험분석, 정보보호 요구사항 분석' 단계의 분석은 이루어 졌지만, 이는 정보보안이 아닌 일반적인 분석이 이루어 졌고, 최근의 보안 위협들이 반영이 되지 않았다. 이는 개발 이후에도 정보보안 위협이 그대로 존재함을 말해 주고 있었다. 더불어 '정보보안계획 및 관리체계 수립'은 기존에 보유하고 있던 것으로 진행을 하는 것으로 되어 있어 많은 문제점이 발생하고 있었다. '정보보안 시스템 설계, 구현, 시험' 단계에서는 보안의 기본이라고 할 수 있는 OWSP Top10, SANS20 등 국제적인 보안 취약점들이 제외된 상태에서 설계 되었고, 운

영 및 점검부분에서도 보안에 대한 부분은 제외가 된 것을 확인 할 수 있었다.

정보보안감리가 차세대시스템 프로젝트에 적용되지 않을 경우, 개발 이후 정보보안컨설팅 전문업체를 찾아 정보보호에서 요구하는 정보보안 적정성에 맞게 모든 프로젝트 산출물 및 결과물을 수정하여야 하며, 시스템의 유저인터페이스(UI) 및 데이터의 흐름들도 수정을 해야 한다. 결과적으로 시스템 전개(open)에 막대한 지장을 초래 하였고, 이는 예산 초과 및 기업의 이미지에도 많은 영향을 미치게 되었다. 정보보안감리 프레임워크가 적용된 D생명보험과 D증권의 경우는 프로젝트 착수 단계에서는 정보보안감리가 적용이 되지 않았지만, 착수 이후 바로 적용이 되어 모든 산출물 및 결과물은 정보보호감리 프레임워크를 기반으로 개발이 되었다. 이는 프로젝트 종료 이후 금융결제원의 보안성 심의를 통과하고, ISO27001을 바로 획득하는 결과를 가져왔다.

마지막으로 보안감리 프레임워크가 전체적으로 적용이 되지 않은 K기관의 사례이다. K기관의 경우는 운영 및 유지보수의 경우 자체적으로 적용이 되고 규정이 잘 되어 있기 때문에 '전사적 보안정책 및 보안계획 수립, 정보보안 시스템 설계, 구현, 시험' 중 인사시스템에 적용하였다. 인사시스템은 K기관에서 상당히 중요하고 권한에 관한 문제가 발생을 하고 있었다. 이 기관에서 중심적으로 점검한 감리 항목은, 자료의 흐름, 해당 화면의 보안성, 권한에 따른 접근 권한 등의 특징을 미리 고객사에서 제시를 하였기 때문에 이것을 위주로 하여 감리를 수행 할 수 있었다. 다음 <표 4>는 정보보호감리의 적용 전, 후의 비교이다.

<표 4>와 같이 정보보호감리 프레임워크를 적용할 경우 개발 전 단계에 걸쳐 내·외부에서 발생하고 있는 보안 이슈를 미리 적용할 수 있고, 정보보호 보안 이슈에 따른 개발 지연, 전개(open) 지연 등을 사전에 예방하며, 시스템 운영자 및 개발자들에게 보안에 대한 인식을 사전에 주입하여 개발자 스스로 개발 보안가이드라인을 지키도록 할 수 있었다.

<표 4> K기관의 정보보호감리 적용 전, 후 비교

단계	문서명	적용 전	적용 후
전사적 보안정책 및 보안계획 수립	IT보안 환경 분석 보고서	일반적인 IT환경 분석 보고서	보안이 적용된 환경 보고서로 수정
	보안요구사항 정의서	고객의 보안 요구사항 미정의	고객의 보안 요구사항이 정의되고 명시되었음
	정보보호 정책/지침/절차	일반적인 정보보호정책/지침/절차서	해당 인사시스템을 위한 정보보호정책/지침/절차서 개발
정보보안 시스템 설계 구현 시험	보안아키텍쳐 보고서	없음	인사시스템을 위한 정보보호 아키텍쳐 개발
	정보보호 설계 보고서	없음	해당기관 사정에 맞는 정보보호 설계서 작성
	개발보안 가이드라인	없음	해당 개발 언어에 따른 개발보안 가이드라인 제공

V. 결론 및 향후 과제

본 논문은 정보 시스템의 보안범위와 그 동안 연구된 보안요구를 기반으로 보안 아키텍처와 보안감리 프레임워크 및 감리 점검 항목을 제안하였다. 제시된 보안감리 기본점검항목들은 사업의 단계에 따라 요구되는 통제나 서비스의 최상위 수준을 제시하였고 정보 시스템이 적용되는 분야별 보안요구에 따라서 더욱 세분화되고 구체화되어야 한다. 세분화된 감리 점검항목은 각 항목별로 감리프레임워크에서 제시한 감리점검기준을 설정하여야 한다. 이는 정보 시스템의 응용분야별 보안요구와 함께 추후 더 연구 발전 되어야 할 분야이다. 뿐 아니라 본 논문에서는 정보보안 시스템의 구현에 대한 감리 점검항목만 제시하였지만 정보보안 시스템의 유형이나 기술이 지속적으로 발전하고 있고 정보시스템 영역이 점차 개방형 시스템으로 전환되고 있으며 비즈니스 시스템과의 연동이 보편화될 것으로 판단되어 정보 시스템 보안감리 사업의 유형은 계속 확장이 예상된다. 따라서 보안영역도 더욱 다양화되고 세분화되어야 할 것이며 관련 연구가 지속적으로 이루어져야 한다.

본 연구의 결과가 반영되어 정보 시스템 보안 감리에

대한 후속 연구가 촉진되고 정보 시스템 및 관련 보안에 대한 국내기술 확보기회와 기술개발의 전환점이 되기를 기대한다.

참고문헌

[1] 행정안전부, 정보시스템 감리기준, 행정안전부고시 제2008-18호, 2008. 6. 19.

[2] 한국정보보호진흥원, 정보시스템 구축단계별 정보보호 가이드라인, 2004. 12.

[3] 한국정보사회진흥원, 정보시스템감리점검해설서 V3.0, 2008.

[4] 한국정보사회진흥원, 공공부문 정보보호 아키텍처 구성 방안 연구, 2004.

[5] 한국정보사회진흥원, 정보시스템 보안/통제 감리 지침 연구, 1998.

[6] 한국정보사회진흥원, 정보시스템 보안 감리지침 연구, 2004.

[7] ISACA Korea chapter, CoBIT 4.0 한글판, 2006.

[8] ISO/IEC 12207, Information Technology : Software Life Cycle Processes, Aug, 1995.

[9] ISO/IEC 27001, International standard-Information technology - Security techniques-Information security management systems – Requirements, 2005.

[10] NIST, Special Publication 800-53, Revision 1 Recommended Security Controls for Federal Information Systems, 2006, pp. 31-105.

[11] Siponen, “Secure-System Design Methods: Evolution and Future Directions,” IT Professional, vol. 8, no. 3, 2006, pp. 40-44.

■ 저자소개 ■

이 지 용
Lee, Ji Yong

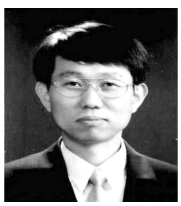
현 재 서울지방경찰청 광진경찰서 사이버수사관
2010년 건국대학교 정보통신대학원 정보시스템감리전공(공학석사)
2007년 한국방송통신대학교 컴퓨터공학과 이학사
CISA, CISSP, PMP, CEH, CHFI, ECSA, 정보처리기사

관심분야 : 정보시스템감리, 정보보안, 디지털증거분석
E-mail : jiyong0825@paran.com

김 동 수
Kim, Dong Soo

현 재 (주)키삭 대표컨설턴트, 건국대학교 정보통신대학원 겸임교수
2005년 국민대학교 경영정보학과 경영학박사
2001년 서울산업대학교 전자계산학과 공학석사
1981년 광운대학교 전자계산학과 이학사
전자계산기조직응용기술사, 정보통신기술사, 정보시스템 수석감리원

관심분야 : 정보시스템 감리, u_city 감리, 프로젝트 관리, 소프트웨어공학
E-mail : dskim@kisac.co.kr



김 희 완
Kim, Hee Wan

2001년 3월~현재 삼육대학교 컴퓨터학부 부교수
2002년 2월 성균관대학교 전기전자 및 컴퓨터공학부(공학박사)
1995년 8월 성균관대학교 정보공학과(공학석사)
1987년 2월 광운대학교 전자계산학과(이학사)
1988년 한국전력공사 정보처리처
정보관리 기술사, 정보시스템 수석감리원

관심분야 : 분산 DB, 보안 데이터베이스, 정보시스템 감리
E-mail : hwkim@syu.ac.kr

논문접수일 : 2010년 5월 7일
수 정 일 : 2010년 5월 20일
게재확정일 : 2010년 6월 5일