DOI: 10.3745/KIPSTD.2010.17D.3.223

정보보호 아키텍처 구성과 보안활동이 정보자산보호 및 조직성과에 미치는 영향

정 구 헌[†] · 이 동 욱[††] · 정 승 렬[†††]

요 약

본 연구는 정보보호 아키텍처 구성과 보안활동이 정보자산보호 및 조직성과에 미치는 영향력을 밝히는데 목적을 갖고 정부, 공공기관, 민간기업 종사자 300명을 대상으로 설문조사 하였다. 연구결과 분류식별과 위험분석 관리요인이 내부정보 유출방지를 위한 정보보호 아키텍처 구성 및 보안활동에 유용성을 갖는 것으로 나타났다. 그리고 정보기술 아키텍처와 구성원의 인식과 교육요인은 기각됨으로써 제한적인 정보보호 아키텍처 구성 및 보안활동이 요구됨을 시사해 주었다. 독립변인으로서의 아키텍처와 구성원에 대한 재인식을 위한 교육은 그 만큼 중요함을 인식시켜 주고, 일반화된 프로세스로 정보보호 통제나 관리 활동에 크게 기여하지 못하고 다만 위험분류 식별관리와 위험분석 관리의 일반화를 통한 엄격한 보안활동이 유의적인 조직성과에 미치는 영향이 큼을 시사해 준 것이라 할 수 있다.

키워드 : 아키텍처 구성, 보안활동, 정보자산보호, 조직성과

The Effect of Composition and Security Activities for Information Security Architecture on Information Asset Protection and Organizational Performance

Gu Heon Jeong[†] · Dong Wook Yi[††] · Seung Ryul Jeong[†††]

ABSTRACT

This study was carried out for the purpose of inquiring into the effect of composition and security activities for information security architecture on information asset protection and organizational performance in terms of general information security. This study made a survey on 300 workers in the government, public institutions and private companies, which it showed that management factors of risk identification and risk analysis, in general, have an usefulness to composition and security activities for information security architecture to prevent inside information leakage. And the understanding and training factors of IT architecture and its component were rejected, requiring the limited composition and security activities for information security architecture. In other words, from the reality, which most institutions and organizations are introducing and operating the information security architecture, and restrictively carrying out the training in this, the training for a new understanding of architecture and its component as an independent variable made so much importance, or it did not greatly contribute to the control or management activities for information security as the generalized process, but strict security activities through the generalization of risk identification and risk analysis management had a so much big effect on the significant organizational performance.

Keywords : Architecture Configuration, Security Activities, Information Asset Protection, Organizational Performance

1. 서 론

정보화 사회에서의 시스템 활용을 위한 활동은 정보 자체가 주요한 원천이 되나, 정보를 취급하는 과정에서 오는 취약성으로 인하여 내부정보에 대한 유출에 노출되고 있는 경우가 많다. 이 같은 피해는 인가 받지 않은 불법적인 사용자에 의한 정보시스템의 파괴, 개인 신상 비밀의 누설 및 유출, 불건전 정보의 유통 등과 같은 피해로 나타나고 있다[3]. 이렇듯 정보화 사회에서는 자신이 원하는 정보를 언제, 어디서든 손쉽게 얻을 수는 있지만 반면, 정보화의 부작용으로 인해 생기는 피해 또한 막대하다[2].

※ 본 연구는 2010년도 국민대학교 교내연구비 지원으로 수행됨
† 정 회 원 : 경찰청 정보통신관리관실
†† 정 회 원 : 넥스젠엔씨지(주)
††† 종신회원 : 국민대학교 비즈니스IT전문대학원 교수
논문접수 : 2010년 2월 4일
수 정 일 : 1차 2010년 3월 22일, 2차 2010년 4월 28일
심사완료 : 2010년 5월 2일

최근 국가기관 및 공공기관의 내부 업무 흐름에 있어 업무용 PC에서 생산되고 있는 전자적 형태의 데이터가 제대로 관리되지 못한 채 악의적인 내부자에 의해 무단으로 유출되거나 컴퓨터 바이러스 등 악성 코드에 의해 외부에 노출되는 등 정보보안 사고가 급증하고 있다. 이로 인해 정보보안 패러다임이 네트워크 보안에서 콘텐츠 보안으로 변화하고 정보유출 위협 또한 상승하고 있어 고객정보 또는 기업의 기밀정보가 전자우편, 인터넷 메신저 서비스, P2P 등을 통해 무차별적으로 유출되는 등 내부정보 유출 사고에 따른 경제적 손실 또한 급격히 증가하고 있다[3].

이 같은 내부정보의 유출은 특히 내부자의 컴퓨터 사용 환경을 통해 주로 발생하게 되는데 그 유형도 다양하여 고성능 업무용 PC의 보급과 USB 메모리 및 외장 하드디스크 등 휴대용 저장매체의 보편화, 초고속 유선 인터넷과 와이브로(WiBro: Wireless Broadband) 및 HSDPA(High Speed Downlink Packet Access) 등 광대역 무선 인터넷 등 정보통신망의 발전뿐만 아니라 공익 근무요원, 사무 보조원(계약직) 및 대체 근무자, 외국인 근로자 등 상시 근무자와 외부 위탁업체, 외부 컨설팅업체, 응용시스템 개발업체 등 많은 외부자에게 내부 정보가 불가피하게 노출되어 국가기관 및 공공기관은 물론 민간 기업까지도 내부정보 유출의 위협이 계속 증가하고 있다[7, 33].

「2008 CSI Computer Crime & Security Survey」 보고서에 따르면 정보보안 사고 중에서 컴퓨터 바이러스가 50%(1위), 내부자에 의한 것이 44%(2위)로 조사되어 그 심각성을 잘 나타내고 있다[2].

그럼에도 불구하고 조직 내부에서 증가하는 보안 위협을 관리하고 통제하기 위해서 주로 사용하는 바이러스 예방 프로그램이나 침입통제 같은 보호 시스템이 기술적 측면에서만 의존해 여전히 정보유출의 가능성을 남겨두고 있다. 따라서 이를 보완하기 위해 보안 위협에 대한 개인 행동이나 보안 기술을 사용하는 조직 구성원에 대한 관리통제가 부족한 것이 현실이다[8-10]. 또한 안전하게 내부 조직의 정보와 시스템을 보호하기 위해서는 기술적인 측면보다 관리적 측면 즉 효과적인 보안 정책을 세우고 이를 조직 구성원들이 실행할 수 있는 속성을 규명하여 자사에 맞게 동기 부여를 하는 것이 중요하다[32]. 이는 2008년 8월 한국산업기술보호협회가 지식경제부와 공동으로 1176개 기업·기관을 상대로 조사를 벌인 결과, 하드웨어 측면에 해당하는 물리적·기술적 보안은 상대적으로 효과가 높은 반면, 소프트웨어 측면에 해당하는 관리적·인적 보안관리 및 통제 속성은 상대적으로 낮은 수준으로 나타난 데서 그 중요성을 알 수 있으며, 그 중에서도 특히 인적 보안은 만족도와 효과가 가장 낮은 점에서 이를 규명하려는 본 연구의 중요성을 알 수 있다[21]. 이러한 중요성에도 불구하고 현재까지 진행된 정보보호 아키텍처 구성과 보안활동 관련 연구는 보안통제의 Michael Pastore(2003), 서보밀(2006)과 정보보호정책과 성과에 선한길(2005), 정보시스템 기술유출 피해산정의 한국산업기술보호협회(2008) 등과 아키텍처 보안의 손상우 외(2006) 아키텍처 활용 내부 통제시스템 개선을 연구한 이희중·황종선(2006)의 연구를 들 수 있다. 그러나 이들 연구와 본 연구와 연계성이 적고 정보보호 아키텍처의 고도화에 따른 보안활동의 접목과 이러한 정보자산보호 측면과 조직성과 관점에서 하나의 경로로 연계시킨 본 연구와 뚜렷한 차이와 한계를 보인다[8-10, 18, 31].

따라서 본 연구에서는 정보보호에 대한 종합적인 관점에서 내부정보 유출이 급증하고 있는 최근 상황에서 이를 효과적으로 관리, 통제하려는 고유 속성에 대한 정보보호에 관한 연구를 한 단계 발전시킨 연구가 되기 위해 정보보호 아키텍처 구성 및 보안활동에 대한 정부, 공공기관, 민간기업의 사용자와 관리자간 카테고리별 활용 수준에 따른 정보자산 보호에 미치는 영향력을 밝히는데 본 연구의 목적을 갖는다.

2. 연구방법

2.1 연구모형

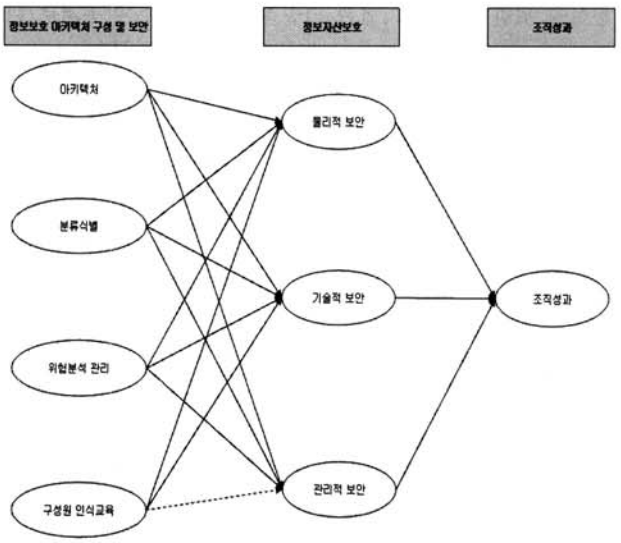
본 연구의 기본 연구 모형은 정보보호 아키텍처 구성과 보안활동이 정보자산보호 및 조직성과에 미치는 영향을 검증하는 데 있다.

기본 연구모형에서 정보보호 아키텍처 구성과 보안활동은 Michael Pastore(2003)의 척도와 정보자산보호의 Kevin Soo Hoo(2000)와 Ariss(2001)의 물리, 기술, 관리적 통제요인과 Gerber et al.(2001)의 조직성과에 미치는 영향 요인을 도출하기 위해 조직 내 수행하는 직접적인 기능보다는 효율적인 정보보호를 위한 관리적 체계로 정의하고, 관련 변수로 정보보호 아키텍처 구성, 정보자산분류식별, 위험분석관리, 구성원 인식교육을 변수로 구성하였다[30-31, 34].

그리고 정보자산보호 요인은 정보보호 수준에 따른 직접적인 활동으로 관리적, 기술적, 물리적 보안 요인으로 정의하고, 정보에 대한 인가된 사람에게 접근을 허용하되 인가되지 않은 사람에게는 접근을 통제하는 물리적 보안활동, 네트워크, 응용시스템에 대한 기술적 접근통제활동과 외부인의 불법적인 접근시도와 내부 관련자들의 부주의나 고의적인 행동에 의해 불법접근이 이루어질 가능성이 항상 존재한다는 점에서 이러한 불법적 접근에 의한 마지막 보호 수단인 암호화와 정보보호 정책에 의거하여 적절하게 운영되고 있는지를 확인하는 관리 운영적 통제활동을 반영하여 물리적 보안, 기술적 보안, 관리적 보안 요인을 변수로 구성하였다[12, 26, 32].

그밖에, 정보자산보호에 미치는 조직성과로서의 종속 변수에서는 정보자산보호를 통한 조직 목표로 보안사고 감소, 고객의 인식제고와 만족도 향상, 협력사와의 정보보호 신뢰도 향상, 개인정보보호에 대한 리스크 평가를 조직성과의 종속변수로 반영하였다.

이상의 상호개념과 모형을 도식화하면 다음과 같다.



(그림 1) 연구모형

2.2 가설설정

기본 연구모형에서 제시된 정보보호 아키텍처 구성 및 보안활동이 정보자산보호 및 조직성과에 미치는 영향을 검정하기 위한 가설을 다음과 같이 구성하였다.

정보보호관리 활동을 구성하는 변수는 이론적 고찰을 통해 정보보호 아키텍처 구성과 정보자산 분류 및 식별, 위험분석 및 관리, 구성원의 정보보호 인식 및 교육활동으로 구성하였다.

그리고 정보보호 아키텍처 구성 및 보안활동은 ISO17799 (2003)의 기준과 Kevin Soo Hoo(2000) 및 이재유 외(2008)의 정보자산보호에 미치는 영향이 조직이 구현한 장치로서 직접적으로 정보보호의 기능을 담당하는 관리, 기술, 물리적 활동이 주 범주의 대상이다[17, 34].

즉 개인들이 보안과 관련하여 반사회적인 행동을 하지 못하도록 하는데 가장 핵심적인 부분을 설명하기 위한 억제이론으로 잠재적으로 정보유출을 시도하고자 하는 사람들에 대한 통제가 필요하며, 이러한 가정은 정책으로 대변되는 활동과 위반 행위에 대한 처벌을 동반한다[35].

여기에서 정책은 조직이 적절하고 안전한 시스템 사용을 위하여 제시하는 지침이라고 볼 수 있으며 조직의 정보보호를 위한 보안 관리자들이 제시하는 가이드라인이다. Wiant (2005)는 억제 이론을 활용하여 정보보호에 관련된 요소 중에서 정책(Policy)에 대한 부분에 초점을 맞추었으며 정책과 개인의 인식과 관계의 인과성을 주장하였다[35].

정보보호 아키텍처 구성 및 보안활동이 정보자산보호에 영향을 미치고, 이와 같은 영향은 조직의 본질적인 고객만족과 유연한 사고대응에 기여함을 여러 연구에 제시하고 있어[26, 28, 36], 본 연구에서도 이를 반영하여 검증하고자 한다. 이에 따라 설정된 연구의 가설은 다음과 같다.

H1 : 정보보호 아키텍처 구성 및 보안활동은 물리적보안에 유의미한 정(+)의 영향을 미칠 것이다.

H1-1 : 아키텍처는 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H1-2 : 분류식별은 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H1-3 : 위험분석 관리는 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H1-4 : 구성원 인식교육은 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H2 : 정보보호 아키텍처 구성 및 보안활동은 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H2-1 : 아키텍처는 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H2-2 : 분류식별은 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H2-3 : 위험분석 관리는 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H2-4 : 구성원 인식교육은 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H3 : 정보보호 아키텍처 구성 및 보안활동은 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H3-1 : 아키텍처는 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H3-2 : 분류식별은 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H3-3 : 위험분석 관리는 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H3-4 : 구성원 인식교육은 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H4 : 정보자산보호는 조직성과에 유의미한 정(+)의 영향을 미칠 것이다.

H4-1 : 물리적 보안은 조직성과에 유의미한 정(+)의 영향을 미칠 것이다.

H4-2 : 기술적 보안은 조직성과에 유의미한 정(+)의 영향을 미칠 것이다.

H4-3 : 관리적 보안은 조직성과에 유의미한 정(+)의 영향을 미칠 것이다.

2.3 표본 추출 및 방법

본 연구논문의 목적을 수행하기 위해 조사대상은 정부, 공공기관, 민간기업 종사자를 대상으로 내부 정보시스템에 대한 사용자 및 관리자 300명을 선정하여 설문조사를 실시하였다.

먼저, 설문 내용의 구성 타당성과 조사의 현실성을 판단하기 위한 예비조사 및 본 조사에 있어서 자료수집의 방법은 문헌 조사 분석을 통해, 관련 논문 및 문헌, 간행물 등을 참고하여 조사하며, 실증조사 분석도를 각 기관별로 균등분할하여 조사하였다.

표본추출방법은 비확률 표본추출방법의 하나인 편의적 표본추출방법을 실시하였으며, 조사대상을 선정 후 2009년 8월 1일부터 8월 30일까지 약 한 달간 총 300부의 설문지를 배포하였으며 이중 총 272부를 회수하여 결측치와 불성실기재누락자를 제외한 유효설문지 총 210매를 분석에 사용하였다.

이상의 표본의 개요를 요약하면 <표 1>과 같다.

〈표 1〉 표본의 개요

조사대상	정부, 공공기관, 민간기업 종사자
조사범위	300명
조사기간	2009년 8월 1일 ~ 8월 30일
자료수집	유효표본 수: 210명 분석에 사용

2.4 설문지의 구성

설문지의 각 항목들은 선행연구에서 사용된 설문과 이론을 근거로 응답자의 일반적 특성, 시스템 이용자의 보호활동, 통제활동, 성과요인으로 분류된 세부적인 요인들에 대한 각 변수의 정의를 기초로 작성하였다.

설문지 항목은 Likert가 개발한 5점 등간척도를 사용하였으며, 인구 통계적 요인인 개인적인 특성은 명목척도로 구성하였다.

본 연구에서 사용된 조사항목 및 설문지 구성은 정보보호관리 및 통제활동에 미치는 영향에 대해 Michael Pastore (2003)와 Kevin Soo Hoo(2000)를 중심으로 자사 내 정보시스템 이용 관련 종사자를 대상으로 시스템 운영 관리시 느끼는 인식 차이를 비교 조사하기 위하여 3개 측정변수를 66문항과 인구 통계적 요인 6개 항목으로 총 72개 항목으로 구성하였다.

2.5 분석방법

본 연구에서 설정된 가설들을 검증하기 위하여 수집된 자료의 실증분석은 통계 패키지 프로그램인 SPSS 12.0과 공변량구조모형의 프로그램인 AMOS 4.01을 이용하였다. 자료분석을 위한 통계적 기법은 기술적 통계 및 추론 통계로 대별할 수 있다. 이 중에서 기술통계, 신뢰성은 SPSS 12.0에 의해서, 그리고 적합성 검증, 가설의 검증을 위한 구조방정식 모델의 추정은 AMOS 4.01에 의해서 수행하였다. 모델의 적합도는 모델과 실제 공분산 자료 사이의 일치성의 정도를 평가하는 것이며 모델의 적합성 평가를 통하여 초기 모델이 부적합한 경우 적합 모델을 찾기 위하여 수정지수(Modification Indices)를 이용토록 하였다.

3. 연구결과

3.1 조사 대상자의 인구 통계학적 특성

다음 <표 3>은 조사 대상자의 인구통계학적 특성에 대해 분석한 결과이다. 분석결과 성별은 남자 188명(89.5%), 여자 22명(10.5%)으로 나타났고, 연령은 29세 이하 52명(24.8%), 30-39세 84명(40.0%), 40-49세 54명(25.7%), 50세 이상 20명(9.5%)으로 나타났다. 최종학력은 고졸 8명(3.8%), 전문대졸 24명(11.4%), 대졸 134명(63.8%), 대학원 이상 44명(21.0%)으로 나타났고, 조직 유형은 민간기업 94명(44.8%), 정부기관 54명(25.7%), 공공기관 52명(24.8%), 자치단체 10명(4.8%)으로 나타났다. 직위는 사원 46명(21.9%), 대리 52명(24.8%), 과장 58명(27.6%), 부장/차장/이사 38명(18.1%)으로 나타났고, 실무경험은 5년 이하 44명(20.9%), 6-10년 52명(24.8%), 11-15년 56명(26.7%), 16년 이상 58명(27.6%)으로 나타났다.

3.2 모형의 적합성 평가

모형의 적합성 평가는 공분산 구조모형이 연구가설에 적합한 정도를 알아보는 과정으로 절대적합지수(absolute fit measures : x^2, GFI, AGFI, RMSR), 증분적합지수(incremental fit measures : NNFI, NFI, Delta 2), 간명적합지수(parsimonious fit measures : PGFI, PNFI, AIC) 등이 이용되고 있다. 본 연구의 가설에 의한 전체적인 구조모형에 대한 분석을 실시한 결과 적합도지수중 x^2(카이자승 통계량)=

〈표 2〉 설문지 구성 내역

		번호	문항수	척도	출 처
정보보호 아키텍처 구성 및 보안활동	아키텍처 구성 분류식별(정보자산) 위험분석 관리 구성원 인식 교육	1-4 5-8 9-12 13-16	16	Likert 5점 척도	Karin Hone et al.(2002) Basie von Solms(2001) Michael Pastore(2003)
보호요인	물리적 통제 기술적 통제 관리적 통제	1-10 1-10 1-10	30	〃	Sonny S. Ariss(2001) ISO17799(2003) Kevin Soo Hoo(2000)
성 과	정보보호활용 고객만족 정보자산 보호 리스크 평가 사고대응	1-5 1-5 1-5 1-5	20	〃	Gerber et al.(2001) Dhillon & Gholamreza(2001) Sonny S. Ariss(2001)
인구통계적 요인	· 성별 · 연령 · 직책 · 경력	1-6	6	명목척도	
계			72		

〈표 3〉 조사 대상자의 인구 통계학적 특성

구분		빈도	퍼센트
성별	남자	188	89.5
	여자	22	10.5
연 령	29세 이하	52	24.8
	30-39세	84	40.0
	40-49세	54	25.7
	50세 이상	20	9.5
최종학력	고졸	8	3.8
	전문대 졸	24	11.4
	대졸	134	63.8
	대학원 이상	44	21.0
조직유형	민간기업	94	44.8
	공공기관	52	24.8
	정부기관	54	25.7
	자치단체	10	4.8
직 위	사원	46	21.9
	대리	52	24.8
	과장	58	27.6
	부장/차장/이사	38	18.1
	기타	16	7.6
실무경험	5년 이하	44	20.9
	6-10년	52	24.8
	11-15년	56	26.7
	16년 이상	58	27.6
합계		210	100.0

(4.681), p-value=(0.197), RMR(원소간 평균제곱 잔차)=(0.006), GFI(기초적합지수)=(0.994), AGFI(조정적합지수)=(0.934), NFI(준적합지수)=(0.996), CFI(비교적합지수)=(0.998)로 분석되었다. 일반적으로 구조방정식 모형분석에는 다른 여러 기준의 적합지수가 이용되기 때문에 다른 통계치를 비교하여 평가하는 것이 합리적이며(Browne & Cudeck, 1993), 그에 따른 다른 적합지수의 판단 기준은 다음과 같다. 먼저 tucker-lewis Index(TLI) : 구조모형의 분산이 전체적인 분산에서 차지하는 비율과 유사한 지표로써 0.9 이상이면 적합하다. 또한 Delta 2 : 표본 수에 따라 값이 달라질 수 있는 NFI 값을 조정한 값으로 0.9 이상이면 적합하다. Delta 2의 값은 기초모형과 표본에 따라 값이 크게 달라지지 않아 안정적이므로 최근의 연구에서 많이 사용되어지는 지수이다. 위와 같은 지표 기준에 의한 분석 결과는 다음과 같다. TLI=(0.985), Delta 2 IFI(incremental fit index)=(0.998)로 기본적인 요건을 충족하고 있으므로, 본 연구에서 설정한 연구가설에 대한 이론적 모형에의 전반적인 적합도는 양호하다는 것이 증명되었다. 다음의 <표 4>는 연구의 전체적인 구조모형의 측정개념들의 확인 요인 분석 결과를 나타낸 것이다.

3.3 상관분석

기준 타당성(criterion-related validity)은 하나의 속성이나 개념의 상태에 대한 측정이 미래 시점에 있어서의 다른 속성이나 개념의 상태 변화를 예측하는 능력을 의미한다. 본 연구의 경우에 기준 타당성은 정보보호관리 통제활동에 대한 독립변수와 정보자산보호에 대한 매개변수, 조직성과에 대한 종속변수 간의 연관성을 검증하기 위하여 신뢰성 분석과 확인요인분석을 했고 단일 차원성이 증명된 각 요인들에 관한 상관관계를 알아보기 위하여 다중상관분석을 실시하였다. 분석결과가 유의하게 나타나는 경우 기준타당성을 만족시킨다고 할 수 있는 것이다.

본 연구에서는 측정오차를 줄이고 단일차원으로 구성된 개념의 대표성을 높이기 위하여 총합척도(summated scale)를 사용하였고, 평균점수가 높을수록 구성개념 내용에 더욱 동의한다고 볼 수 있다. 이상의 요인분석결과를 바탕으로 상관분석을 시행한 결과는 다음 <표 5>과 같다.

〈표 4〉 전체 모형의 적합도 검증

구 분	x^2	p	RMR	GFI	AGFI	NFI	CFI	TLI	Delta 2
전체 모형의 확인 요인분석	4.681	0.197	0.006	0.994	0.934	0.996	0.998	0.985	0.998

〈표 5〉 각 변수간 상관관계 검증

구분	아키텍처	분류식별	위험분석관리	구성원 인식교육	물리적보안	기술적보안	관리적보안	조직성과
아키텍처	1							
분류식별	.537**	1						
위험분석 관리	.571**	.677**	1					
구성원 인식교육	.477**	.645**	.650**	1				
물리적 보안	.448**	.636	.604**	.544**	1			
기술적 보안	.483**	.627**	.578**	.530**	.711**	1		
관리적 보안	.508**	.646**	.521**	.494**	.691**	.721**	1	
조직성과	.491**	.552**	.414**	.417**	.417**	.631**	.680**	1

**p<.01

3.4 가설의 검증

본 연구에서는 연구 가설의 확인을 위해 구조방정식 모형을 활용하여 이를 검증 하였다. 구조방정식은 회귀분석과 달리 공변량 분석을 통해 변수들 간의 직접효과와 이외에도 간접효과를 확인할 수 있기 때문에 복잡한 인과관계를 체계적으로 이해하는데 큰 도움을 준다. 또한 구조방정식 모형은 모형에 내재된 오차를 알 수 있고, 나아가 측정 모형과 이론 모형간의 관계를 전체적인 관점에서 검증할 수 있다는 점에서 큰 의의가 있다(김계수, 2004). 이에 본 연구에서는 구조방정식 모형을 활용하여 구성 개념들 간의 인과관계를 검정하였다.

1) 정보보호 아키텍처 구성 및 보안활동과 정보자산보호에 대한 가설

가설 1~3을 검정하기 위해 경로분석을 실시한 결과는 다음과 같다.

H1 : 정보보호 아키텍처 구성 및 보안활동은 물리적보안에 유의미한 정(+)의 영향을 미칠 것이다.

H1-1 : 아키텍처는 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H1-2 : 분류식별은 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H1-3 : 위험분석 관리는 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H1-4 : 구성원 인식교육은 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

"가설 1-1. 아키텍처는 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 아키텍처 요인의 경로계수는 0.047, t값이 0.846으로, 물리적 보안에 유의미한 영향을 주지 않는 것으로 나타나 가설 1-1은 기각되었다.

"가설 1-2. 분류식별은 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 분류식별 요인의 경로계수는 0.355, t값이 4.758로, 물리적 보안에 정(+)의 영향을 주는 것으로 나타나 가설 1-2는 지지되었다.

"가설 1-3. 위험분석 관리는 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 위험분석 관리 요인의 경로계수는 0.226, t값이 3.220으로, 물리적 보안에 정(+)의 영향을 주는 것으로 나타나 가설 1-3은 지지되었다.

〈표 6〉 정보보호 아키텍처 구성 및 보안활동이 물리적 보안에 미치는 영향

가설	독립변수		종속변수	Estimate	S.E.	C.R.	P
H1-1	아키텍처	→	물리적 보안	0.047	0.056	0.846	0.397
H1-2	분류식별	→	물리적 보안	0.355	0.075	4.758**	0.000
H1-3	위험분석 관리	→	물리적 보안	0.226	0.070	3.220**	0.001
H1-4	구성원 인식교육	→	물리적 보안	0.114	0.064	1.772	0.076

**p<.01

〈표 7〉 정보보호 아키텍처 구성 및 보안활동이 기술적 보안에 미치는 영향

가설	독립변수		종속변수	Estimate	S.E.	C.R.	P
H2-1	아키텍처	→	기술적 보안	0.115	0.057	2.011*	0.044
H2-2	분류식별	→	기술적 보안	0.357	0.076	4.682**	0.000
H2-3	위험분석 관리	→	기술적 보안	0.171	0.072	2.380*	0.017
H2-4	구성원 인식교육	→	기술적 보안	0.106	0.066	1.617	0.106

*p<.05, **p<.01

"가설 1-4. 구성원 인식교육은 물리적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 구성원 인식교육 요인의 경로계수는 0.114 t값이 1.772로, 물리적 보안에 유의미한 영향을 주지 않는 것으로 나타나 가설 1-4는 기각되었다.

H2 : 정보보호 아키텍처 구성 및 보안활동은 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H2-1 : 아키텍처는 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H2-2 : 분류식별은 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H2-3 : 위험분석 관리는 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H2-4 : 구성원 인식교육은 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

"가설 2-1. 아키텍처는 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 아키텍처 요인의 경로계수는 0.115, t값이 2.011로, 기술적 보안에 정(+)의 영향을 주는 것으로 나타나 가설 2-1은 지지되었다.

"가설 2-2. 분류식별은 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 분류식별 요인의 경로계수는 0.357, t값이 4.682로, 기술적 보안에 정(+)의 영향을 주는 것으로 나타나 가설 2-2는 지지되었다.

"가설 2-3. 위험분석 관리는 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 위험분석 관리 요인의 경로계수는 0.171, t값이 2.380으로, 기술적 보안에 정(+)의 영향을 주는 것으로 나타나 가설 2-3은 지지되었다.

"가설 2-4. 구성원 인식교육은 기술적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 구성원 인식교육 요인의 경로계수는 0.106 t값이 1.617로, 기술적 보안에 유의미한 영향을 주지 않는 것으로 나타나 가설 2-4는 기각되었다.

H3 : 정보보호 아키텍처 구성 및 보안활동은 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H3-1 : 아키텍처는 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H3-2 : 분류식별은 관리적 보안에 유의미한 정(+)의 영향

〈표 8〉 정보보호 아키텍처 구성 및 보안활동이 관리적 보안에 미치는 영향

가설	독립변수		종속변수	Estimate	S.E.	C.R.	P
H3-1	아키텍처	→	관리적 보안	0.195	0.063	3.092**	0.002
H3-2	분류식별	→	관리적 보안	0.513	0.084	6.076**	0.000
H3-3	위험분석 관리	→	관리적 보안	0.053	0.080	0.664	0.507
H3-4	구성원 인식교육	→	관리적 보안	0.070	0.073	0.960	0.337

**p<.01

을 미칠 것이다.

H3-3 : 위험분석 관리는 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

H3-4 : 구성원 인식교육은 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다.

"가설 3-1. 아키텍처는 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 아키텍처 요인의 경로계수는 0.195, t값이 3.092로, 관리적 보안에 정(+)의 영향을 주는 것으로 나타나 가설 3-1은 지지되었다.

"가설 3-2. 분류식별은 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 분류식별 요인의 경로계수는 0.513, t값이 6.076으로, 관리적 보안에 정(+)의 영향을 주는 것으로 나타나 가설 3-2는 지지되었다.

"가설 3-3. 위험분석 관리는 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 위험분석 관리 요인의 경로계수는 0.053, t값이 0.664로, 관리적 보안에 유의미한 영향을 주지 않는 것으로 나타나 가설 3-3은 기각되었다.

"가설 3-4. 구성원 인식교육은 관리적 보안에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 구성원 인식교육 요인의 경로계수는 0.070 t값이 0.960으로, 관리적 보안에 유의미한 영향을 주지 않는 것으로 나타나 가설 3-4는 기각되었다.

2) 정보자산보호와 조직성과에 대한 가설

가설 4를 검정하기 위해 경로분석을 실시한 결과는 다음과 같다.

H4 : 정보자산보호는 조직성과에 유의미한 정(+)의 영향을 미칠 것이다.

〈표 9〉 정보자산보호가 조직성과에 미치는 영향

가설	독립변수		종속변수	Estimate	S.E.	C.R.	P
H4-1	물리적 보안	→	조직성과	0.297	0.077	3.879**	0.000
H4-2	기술적 보안	→	조직성과	0.186	0.079	2.360*	0.018
H4-3	관리적 보안	→	조직성과	0.325	0.070	4.660**	0.000

*p<.05, **p<.01

H4-1 : 물리적 보안은 조직성과에 유의미한 정(+)의 영향을 미칠 것이다.

H4-2 : 기술적 보안은 조직성과에 유의미한 정(+)의 영향을 미칠 것이다.

H4-3 : 관리적 보안은 조직성과에 유의미한 정(+)의 영향을 미칠 것이다.

"가설 4-1. 물리적 보안은 조직성과에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 물리적 보안 요인의 경로계수는 0.297, t값이 3.879로, 조직성과에 정(+)의 영향을 주는 것으로 나타나 가설 4-1은 지지되었다.

"가설 4-2. 기술적 보안은 조직성과에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 기술적 보안 요인의 경로계수는 0.186, t값이 2.360으로, 조직성과에 정(+)의 영향을 주는 것으로 나타나 가설 4-2는 지지되었다.

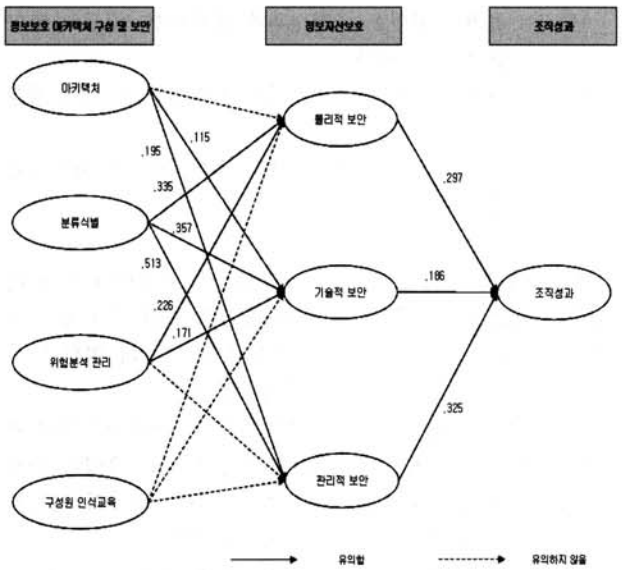
"가설 4-3. 관리적 보안은 조직성과에 유의미한 정(+)의 영향을 미칠 것이다."를 살펴보면 관리적 보안 요인의 경로계수는 0.325, t값이 4.660으로, 조직성과에 정(+)의 영향을 주는 것으로 나타나 가설 4-3은 지지되었다.

이상의 가설검증 결과를 요약하면 다음 <표 10>과 같다.

〈표 10〉 가설검증 결과요약

가설	독립변수		종속변수	Estimate	S.E.	C.R.	P	채택 여부
H1-1	아키텍처	→	물리적 보안	0.047	0.056	0.846	0.397	기각
H1-2	분류식별	→	물리적 보안	0.355	0.075	4.758**	0.000	채택
H1-3	위험분석 관리	→	물리적 보안	0.226	0.070	3.220**	0.001	채택
H1-4	구성원 인식교육	→	물리적 보안	0.114	0.064	1.772	0.076	기각
H2-1	아키텍처	→	기술적 보안	0.115	0.057	2.011*	0.044	채택
H2-2	분류식별	→	기술적 보안	0.357	0.076	4.682**	0.000	채택
H2-3	위험분석 관리	→	기술적 보안	0.171	0.072	2.380*	0.017	채택
H2-4	구성원 인식교육	→	기술적 보안	0.106	0.066	1.617	0.106	기각
H3-1	아키텍처	→	관리적 보안	0.195	0.063	3.092**	0.002	채택
H3-2	분류식별	→	관리적 보안	0.513	0.084	6.076**	0.000	채택
H3-3	위험분석 관리	→	관리적 보안	0.053	0.080	0.664	0.507	기각
H3-4	구성원 인식교육	→	관리적 보안	0.070	0.073	0.960	0.337	기각
H4-1	물리적 보안	→	조직성과	0.297	0.077	3.879**	0.000	채택
H4-2	기술적 보안	→	조직성과	0.186	0.079	2.360*	0.018	채택
H4-3	관리적 보안	→	조직성과	0.325	0.070	4.660**	0.000	채택

*p<.05, **p<.01



(그림 2) 연구모형의 경로추정치

4. 결 론

본 연구는 정보보호에 대한 종합적인 관점에서 내부정보 유출이 급증하고 있는 최근 상황에서 이를 효과적으로 관리, 통제하려는 고유 속성에 대한 정보보호에 관한 연구를 한 단계 발전시킨 연구가 되기 위해 정보보호 아키텍처 구성 및 보안활동이 정보자산 보호 및 조직성과에 미치는 영향력을 밝히는데 목적을 갖고 연구하였는데 그 결과를 요약하면 다음과 같다.

첫째, 정보보호 아키텍처 구성 및 보안활동이 물리적 보안에 미치는 영향을 검증한 결과 독립변수별로 분류식별, 위험분석 관리가 물리적 보안에 통계적으로 유의미한 정(+)의 영향을 미치는 것으로 나타났다($p<.05$). 즉, 분류식별을 강조할 때 물리적 보안은 .355 높아지는 것으로 나타났고, 위험분석 관리를 강조할 때 물리적 보안은 .226 높아지는 것으로 나타났다. 따라서 정보의 물리적 보안의 향상을 위해서는 분류식별, 위험분석 관리가 중요한 요인임을 알 수 있다.

둘째, 정보보호 아키텍처 구성 및 보안활동이 기술적 보안에 미치는 영향을 검증한 결과 독립변수별로 아키텍처, 분류식별, 위험분석 관리가 기술적 보안에 통계적으로 유의미한 정(+)의 영향을 미치는 것으로 나타났다($p<.05$). 즉, 분류식별을 강조할 때 기술적 보안은 .357 높아지는 것으로 나타났고, 위험분석 관리를 강조할 때 기술적 보안은 .171, 아키텍처를 강조할 때 기술적 보안은 .115 높아지는 것으로 나타났다. 따라서 정보의 기술적 보안의 향상을 위해서는 아키텍처, 분류식별, 위험분석 관리가 중요한 요인임을 알 수 있다.

셋째, 정보보호 아키텍처 구성 및 보안활동이 관리적 보안에 미치는 영향을 검증한 결과 독립변수별로 아키텍처, 분류식별이 관리적 보안에 통계적으로 유의미한 정(+)의 영향을 미치는 것으로 나타났다($p<.05$). 즉, 분류식별을 강조할 때 관리적 보안은 .513 높아지는 것으로 나타났고, 아키텍처를 강조할 때 관리적 보안은 .195 높아지는 것으로 나타났다. 따라서 정보의 기술적 보안의 향상을 위해서는 아키텍처, 분류식별이 중요한 요인임을 알 수 있다.

넷째, 정보자산보호가 조직성과에 미치는 영향을 검증한 결과 독립변수별로 물리적 보안, 기술적 보안, 관리적 보안이 조직성과에 통계적으로 유의미한 정(+)의 영향을 미치는 것으로 나타났다($p<.05$). 즉, 관리적 보안을 강조할 때 조직성과는 .325높아지는 것으로 나타났고, 물리적 보안을 강조할 때 조직성과는 .297, 기술적 보안을 강조할 때 조직성과는 .186 높아지는 것으로 나타났다. 따라서 조직성과의 향상을 위해서는 물리적, 기술적, 관리적 정보자산보호가 중요한 요인임을 알 수 있다.

전체적으로 분류식별과 위험분석 관리요인이 내부정보 유출 방지를 위한 정보보호 통제활동에 유용성을 갖는 것으로 나타나고 정보기술 아키텍처와 구성원의 인식 교육 요인은 기각됨으로써 제한적인 보안 통제활동이 요구됨을 시사해 주었다. 이는 대다수 기관과 조직에서 정보기술 아키텍처를 도입 운영하고 이에 대한 교육이 이루어지고 있는 현실에서 독립변인으로서의 아키텍처와 구성원에 대한 재인식을 위한 교육은 그 만큼 일반화된 프로세스로 정보보호 통제나 관리 활동에 크게 기여하지 못하고 다만 위험분류 식별관리와 위험분석 관리의 일반화를 통한 엄격한 통제활동이 유의적인 조직성과에 미치는 영향이 큼을 나타내 준 것이라 할 수 있다. 따라서 조직 내부정보 유출과 보안사고가 급증하고 있는 현실에서 특정 기술 아키텍처에 의한 시스템 의존과 종사원의 인식교육에 기댄 기존의 보안 활동에서 벗어나 매우 철저한 분류기준에 의한 엄격한 분리시행과 주기적인 위험분석 활동과 이의 공지를 통한 조직 내 분위기 조성과 조직 전반에의 위기의식 공유가 중요하고 이의 확산과 동시 모두에 공유될 때 성과 또한 높아짐을 의미한다. 이는 기존 조직의 보안활동이 물리적, 기술적, 관리적 보안활동 요인 모두 조직성과에 유의한 영향을 미침을 주장한 손상수 외(2006), 이재유(2008), 행정안전부(2008)의 선행연구 결과와 일치된 결과로서 본 연구의 유용성을 뒷받침해 준 것이라 볼 수 있다.

따라서 조직 내 내부 정보유출 방지를 위한 정보보호관리 통제활동이 조직성과에 미치는 영향을 극대화시키기 위해서는 조직구성원에 대한 내부보안 분류 기준의 엄격한 통제 적용과 동시 정보보호 마인드의 중요성에 대한 경각심과 함께 역기능에 대한 피해를 예방하기 위한 철저한 식별분류 관리와 주기적인 위험분석 활동 및 물리적, 기술적, 관리적 보안 통제활동의 상설운영으로 조직 내 정보자원의 효율적인 운영과 성과를 높이려는 노력이 병행되어져야 할 것이다.

참 고 문 헌

[1] 강성원, "아키텍처 기반의 결정적 소프트웨어 진화계획의 가치 평가, 한국정보처리학회논문지," 제16권 제5호, pp.755-766. 2009.

[2] 강홍렬 · 이원태 · 최선희 · 신동익, 지식정보화를 위한 아키텍처 정책연구 : 정부통합전산센터와 아키텍처, 연구보고, 제16호, pp.1-126, 2006.

[3] 국가정보원, 2008년 국정감사 법제사법위원회 제출자료, 2008.

[4] 국가정보원 · 방송통신위원회, 2008 국가정보보호백서, 2008.

[5] 김정덕 · 이용덕, EA 기반의 전사적 정보보호 아키텍처(EISA) 참조 모델에 관한 연구, 학술대회, 제1호, pp.341-346, 2009.

[6] 김종서, EA 기반의 보안아키텍처 감리기법에 관한 연구, 건국대학교 정보통신대학원 석사학위논문, 2010.

[7] 방송통신위원회, 인터넷 정보보호 종합대책, 2008.

[8] 서보밀, 인지된 보안통제가 고객의 인터넷뱅킹 수용에 미치는 영향, 한국전자거래학회지, 11(1), pp. 25-52. 2006.

[9] 선한길, 국내기업의 정보보호정책 및 조직요인이 정보보호성과에 미치는 영향, 국민대학교 대학원 박사학위논문, 2005.

[10] 손상우 · 김문기 · 이병호, FMIPv6 적용을 위한 보안 아키텍처 연구, 한국정보처리학회:학술대회논문집, 한국정보처리학회 2006년도 제25회 춘계학술발표대회, pp.1183-1186. 2006.

[11] 신수정 · 최영진 · 정석춘, 서용원공동활용자원식별을 위한 전자정부 시스템 아키텍처 서술 방안, 한국정보처리학회논문지, 16(4), pp.631-642. 2009.

[12] 양재영, 정보보안아키텍처 구축에 관한 연구, 전자상거래학회지, 제9권 제1호, pp.3-26, 2008.

[13] 연수권, EA기반의 정보보호 아키텍처 감리기법에 관한 연구, 건국대학교 대학원 석사학위논문, 2006.

[14] 윤종희 · 신세철 · 백윤흥 · 조정훈, 임베디드 프로세서의 성능 향상을 위한 DIAM의 진보한 아키텍처, 한국정보처리학회논문지, 16(6), pp.443-452, 2009.

[15] 이관우, 다중 관점 제품계열아키텍처의 가변성 관리 및 일관성 검사를 위한 특성 지향 접근방법, 한국정보처리학회논문지, 15(6), pp.803-814. 2008.

[16] 이용덕, 전사적 통합 정보보호 아키텍처 프레임워크에 관한 연구, 중앙대학교 대학원 석사학위논문, 2010.

[17] 이재유 · 김수동, 서비스 지향 아키텍처의 클라이언트를 위한 실용적 프로세스 모델, 한국정보처리학회논문지, 15(4), pp. 513-522. 2008.

[18] 이희중 · 황종선, J2EE 아키텍처를 활용한 재무보고 내부통제 시스템 개선 연구, 한국정보처리학회:학술대회논문집, 한국정보처리학회 2006년도 제26회 추계학술발표대회, pp.637-640. 2006.

[19] 장현미 · 김경진 · 김혜리 · 정지희 · 홍승필 · 강성민, 인터넷 환경 내 개인정보보호 아키텍처 설계 방안, Entrue Journal of Information Technology, 제8권 제1호, pp.117-131, 2009.

[20] 최동진 · 김민규 · 윤희병 · 이일로, 개방형 아키텍처 컴퓨팅 환경의 기술 아키텍처 및 구성요소 분석에 관한 연구, 한국IT서비스학회 학술대회 논문집, 제1호, pp.472-475, 2009.

[21] 한국산업기술보호협회, 기술유출에 따른 피해규모 산정을 위한 모델 연구, 한국산업기술재단 주관, 2008.

[22] 한국정보사회진흥원, 2008 국가정보화백서, 2008.

[23] 행정안전부, 정보보호 중기 종합계획, 2008.

[24] 황상규 · 권혁진, 국방정보화 합동능력통합개발을 위한 아키텍처 활용방안연구, 한국정보처리학회지, 15(6), pp.114-119. 2008.

[25] Ariss, S. S., Computer Monitoring: Benefits and Pitfalls Facing Management. Information and Management, 39(7), 2002, pp.553-558.

[26] Cavusoglu, H., Mishra, B. & Raghunathan, S., "The Value of Intrusion Detection Systems in Information Technology Security Architecture," Information systems research, Vol.16 No.1, pp.28-46. 2005.

[27] CSI, 2008 CSI Computer Crime & Security Survey, 2008.

[28] Dalton, M., Kannan, H. & Kozyrakis, C. "Raksha: A Flexible Information Flow Architecture for Software Security," In: International Symposium on Computer Architecture new, Vol.35 No.2, pp.350-363, 2007.

[29] Eloff, J. H. P. & Eloff, M., "Integrated Information Security Architecture," Computer Fraud and Security, No.11, pp.10-16, 2005.

[30] Gerber, M., Solms, R. & Paul, O., Formalizing information security requirements. Information Management & Computer Security, 9(1), 2001, pp.32-37.

[31] Pastore, M., New Enterprise Focus : Building Security Teams. Esecurity Planet, 2003.

[32] Pulkkinen, M., Naumenko, A. & Luostarinen, K., "Managing information security in a business network of machinery maintenance services business - Enterprise architecture as a coordination tool," The Journal of systems and software, Vol.80 No.10, pp.1607-1620, 2007.

[33] Ross, S. J., "Enforcing information security: architecture and responsibilities," NETWORK SECURITY, No.2, pp.7-10, 2008.

[34] Soo Hoo, Kevin, How Much is Enough? A Risk-Management Approach to Computer. Security. working paper, CRISP, 2000.

[35] Wiant, T. L., Information security policy's impact on reporting security incidents, Computers & Security, 24, 2005, pp.448-459.

[36] Yan, H., Xiaorong, X. & Yingduo, H., "A Survey to Design Method of Security Architecture for Power Information Systems," POWER SYSTEM TECHNOLOGY(BEIJING), Vol.29 No.1, pp.35-39, 2005.

정 구 헌

e-mail : jghsky@police.go.kr
1992년 광주대학교(학사)
2005년 아주대학교(석사)
2008년~현 재 국민대학교 BIT전문대학원 박사과정
1992년~현 재 경찰청 정보통신관리관실
관심분야 : 경찰정보통신보안, 개인정보보호, 엔터프라이즈 아키텍처 등

이 동 욱

e-mail : ydw0003@nate.com
1993년 안동대학교(학사)
2002년 동국대학교(석사)
2008년~현 재 국민대학교 BIT전문대학원 박사과정
1993년~2001년 강원정보기술(주)
2005년~현 재 넥스젠엔씨지(주)
관심분야 : 엔터프라이즈 아키텍처, 데이터 웨어하우스, 정보보안 등

정 승 렬

e-mail : srjeong@kookmin.ac.kr
1985년 서강대학교(학사)
1989년 Univ. of Wisconsin(석사)
1995년 Univ. of South Carolina(박사)
1995년~1997년 삼성SDS 컨설팅사업부 컨설턴트
1997년~현 재 국민대학교 BIT전문대학원 교수
관심분야 : 프로세스 설계, 시스템 구현, 프로젝트 관리 등