情報保護學會論文誌
第19卷 第6號, 2009. 12

정보보호를 위한 인적자산 관리지표 실증 연구

차 인 환,[1†] 김 정 덕[2‡]
[1]A3 시큐리티, [2]중앙대학교

An Empirical Research on Human Factor Management Indicators for Information Security

Inhwan Cha,[1†] Jungduk Kim[2‡]
[1]A3 Security Ltd., [2]Chung-Ang University

요 약

본 논문은 인적자산 보안관리에 관한 프레임워크를 개발하였고 이를 기반으로 관리지표와 보안수준 제고 요인을 도출하고 이를 실증적으로 분석한 연구이다. 인적자산 보안관리 프레임워크는 인원보증(Personnel Assurance), 개인역량(Personnel Competence), 보안 통제(Security Control) 분야로 구성되어 있으며, 관리지표는 9개 항목의 26개 지표로 도출되었다. 또한 보안수준 제고 요인은 보안인지, 규칙준수, 실수억제 항목으로 도출되었다. 연구결과, 보안관리 지표와 관리수준 제고 항목의 실증분석 결과는 대부분 부합성과 유의성을 가지고 있었으며 조직의 인적자산 보안관리 시 유용하게 적용될 것으로 기대된다.

ABSTRACT

This study is to develop a human resource (HR) security framework, and related HR security indicators in the context of information security. The HR security framework consists of three constructs, personnel assurance, personnel competence, and personnel security control. Based on the framework, HR security management indicators are derived as 26 indicators in 9 items out of 3 categories. An empirical research has been performed to verify the relevance and consistency between the indicators by conducting a questionnaire-based survey. Also, interrelationships between the proposed indicators and HR related security level were analyzed by the multiple regression analysis. As a result, the proposed hypothesis were mostly accepted, showing the significant relationships between the indicators and security level.

Keywords: Human Resource Security, Personnel Security, Management Indicators

I. 서 론

Solms(2006)은 정보보호 변천과정을 4가지 단계로 구분하였으며, 첫 번째 단계는 정보보호 기술 중심, 두 번째 단계는 정보보호 관리 중심, 세 번째 단계는 조직화/제도화 중심, 네 번째 단계는 정보보호 거버넌스 중심으로 분류하였다[20]. 따라서 현재 선진국에서는 최고경영층의 정보보호에 대한 역할과 책임을 강조하는 거버넌스 체계가 구축 중에 있다. 그러나 한국은 정부를 위시하여 정보보호 수준 제고를 위하여 많은 노력을 하였지만, 기술적 측면에서의 정보보호 노력에 치중하였고 비즈니스 차원에서의 정보보호 노력은 상대적으로 미흡하다고 할 수 있다[1].

정보보호 조직화/제도화 및 거버넌스 노력은 공히 조직 내의 인적자산 관리의 중요성을 강조하고 있다고 할 수 있다. 즉 정보보호 전담부서만이 아닌 조직 전체 구성원의 정보보호 노력을 강조하고 있으며 특히 정보보호를 기술적 이슈보다 인적 문제로 인식하

접수일(2009년 9월 25일), 수정일(2009년 11월 30일), 게재확정일(2009년 12월 16일)
† 주저자, captain757@hanmail.net
‡ 교신저자, jdkimsac@cau.ac.kr

고 있다. 또한 정보보호가 미치는 사회적 영향이 지대하게 됨에 따라 비즈니스 이슈로서 이를 해결하기 위한 전사적 활동이 강조되고 있는 실정이다. 정보보호에서 인적자산은 실질적으로 보안업무를 수행하는 주체일 뿐 만 아니라, 보안성패의 중요한 요인으로 볼 수 있다. 또한 ISO 27001과 같은 국제표준에서도 인적자산 보안관리를 별도 도메인으로 분류하고 중요한 과제로 관리하는 것은 보안사고의 모든 부분에서 인적자산이 의도적이거나 비의도적으로 연관되어 있기 때문이다.

최근의 인적자산에 의한 보안 사고는 지속적으로 증가하는 추세[7-9,13]이나, 보안연구는 기술적 부분에 치중되어 있으며 인적자산 보안에 대한 연구는 부진한 실정이다. Mikko와 Robert(2005)는 1994~2004년까지 20여개의 IS 저널에 기고된 1,280편의 보안분야 논문 중 비기술적인 부분이 24% 수준으로 기술적 중심의 연구가 진행되고 있다고 하였다[18]. 또한 Rita Goh(2003)는 인적자산 중심의 전사적 보안관리 연구가 필요하다고 강조하였다[12].

따라서 본 논문은 기존 선행연구의 고찰, 인적 자산에 의한 사고의 동기와 위협 등을 포괄적으로 연구하고 정보보호에서의 인적자산 보안관리를 위한 프레임워크와 관리지표를 개발하는 목적으로 수행되었다. 연구방법은 선행연구와 전문가 의견수렴 과정을 거쳐 연구지표를 도출하고, 도출된 지표의 내적일관성과 타당성, 용이성, 신뢰성에 대한 부합성 분석을 실시하였다. 또한 도출된 관리지표들이 보안수준 제고에 유의한지에 관하여 SPSS 12를 이용한 다중회귀분석을 실시하였다.

II. 인적자산 보안에 관한 선행연구

인적자산 보안에 대한 개념은 조직의 구성원이나 협업관계에 있는 인원이 조직의 보안정책에 따라 보안업무를 안전하게 수행하기 위한 개인적 관점의 업무영역이다[10]. 본 논문에서는 인적자산 보안관리 대상을 조직의 내부의 구성원과 외부의 인가된 인원으로 설정하였다.

2.1 인적자산 보안위협과 대책

정보보호의 위협 양상은 기술과 환경에 따라 다양하게 변화하지만, 근본적인 속성은 인원을 통하여 이루어진다는 점이다. 이는 정보보호 업무와 연관된 일련의 행위와 원인 및 수단이 사람을 통하여 이루어지며 위협의 중심에는 항상 인간이 존재하기 때문[6,12]이다. 인적자산에 의한 최근의 보안사고 사례는 정보보호 위협의 심각성을 시사하며 주요 사례는 다음과 같다. IDC(2008)는 공격 경로의 59%가 내부에서 발생하고 Diloitte(2008)는 사고의 79%가 사람에 의하며 발생한다고 하였다. 또한 Human Firewall Council(2007)은 사고원인을 내부 사용자의 부적절한 네트워크 접속 및 사용 78%, 내부의 직접적인 공격이 33% 수준으로 평가하였다[7,8,9,13]. 이러한 인적자산에 의한 위협 원인은 악의적 공격, 보안의 무지, 부주의나 실수, 규칙의 미준수로 평가되었으며 위협 중 '인가된 사람이 인가된 절차를 통하여 인가된 정보에 접근하여 야기되는 보안위협이 가장치명적인 것'으로 판단된다.

위와 같은 인적자산 위협에 대한 정보보호 대책은 조직의 특성과 비즈니스 목표와 부합되는 정책아래 조직 구성원 모두의 자발적인 참여, 인적자산의 지속적인 역량 강화를 통하여 보완되고 발전되어야 한다[5,14.21]. 그러나 정보보호 업무를 기술적인 부분만 강조하여 인적요인에 대한 관리를 간과하거나, 보안을 바라보는 시각이 협소하여 보안관리에 대한 도전을 기술적 방어에만 치중하여 전사적 대처능력이 저하되는 사례는 없어야 한다. 또한 위협은 외부에서 발생하고 시스템적인 보안대책으로 보안환경이 구축되었다는 판단이나, 한 번의 보안조치 사항이 지속성을 가진다는 오해는 경계되어야 한다[3,11,14].

2.2. 인적자산 보안관리 기준 비교

인적자산 보안의 중요도에 대한 보편적 인식에도 불구하고 이에 대한 구체적인 기준은 미흡한 실정이다. 기존의 인적보안 관리 기준은 ISO 27001 등의 일부 국제기준에 부분적으로 포함되어 있다. 또한 미국, 영국, 호주 등 일부 국가에서는 인적자산에 대한 보안 기본원칙을 간략하게 제시하고, 이 원칙에 따라 정부 산하기관이나 주정부에는 조직의 특성을 고려한 별도의 간략한 보안 가이드라인을 유지하고 이를 실행하고 있는 실정이다. 인적자산 보안에 대한 국제적인 기준은 ISO 27001, NIST SP 800-53, 미 국방부 보안 프로그램, 영국 및 호주 정부의 보안 프로그램을 대표적으로 볼 수 있으며 아래와 같다.

ISO 27001(2005)은 국제 보안표준의 기본으로

활용되고 있으나[4] 인적자산 부분은 고용 전, 고용 중, 고용 후로 분류하고 인적자산 보안관리를 고용 시기 중심으로 구분되어 있다. 즉 업무 시점을 중심으로 간략한 보안조치 사항에 국한하여 부분적으로 인적자산을 관리토록 구성되어 인적자산 보안관리의 포괄적 기준으로 적용하기에는 한계를 가지고 있다[15].

NIST 800-53(2006)은 보안통제 항목 중심으로 구성되어 있으며 보안관리 프로세스의 통제 항목에 인적 자산 관리 요인을 중요한 변수로 보고 있다. 또한 인식 및 교육훈련, 보안의식, 인증 및 평가를 중점으로 관리토록 제시 하고 있다. 그러나 통제 중심의 인적자산의 관리로 제한되어 있으므로 인적자산에 대한 보증과 사고억제 등에 대한 관리 항목은 미흡한 실정이다[19].

미 국방부 보안 프로그램(2001)은 인원에 대한 신뢰와 교육이 가장 중요한 보안관리 요인으로 평가하고 있다. 즉 보안 의식, 개인 보안책임제, 통제 및 억제, 기본원칙의 철저한 준수, 교육훈련, 기술의 이해를 기반으로 구성되어 있다. 또한 보안신고와 빠른 대응, 다양한 교육 프로그램, IT 프로세스와 연계성을 강조하고 있는 특징이 있다. 그러나 인적자산의 평가와 보안의식 관리의 지표가 구체화되지 못하고 기술영역으로 분산되어 부분적인 지표로 활용이 가능한 실정이다[10].

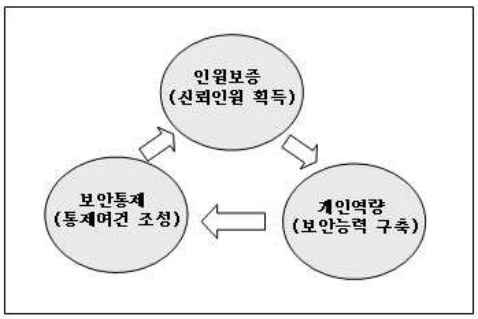
영국 정부의 인적자산 보안 프로그램(2007)은 별도의 프레임워크를 가지고 있으며 인원의 신뢰성과 기술적 이해를 중점으로 관리되도록 제도화되어 있다. 즉 고용이나 계약 시 충분한 보안 서약을 요구하고 정기적인 교육 프로그램 및 평가를 통하여 지속성 여부를 판단하고 있다. 또한 심리적 영향 평가를 통하여 개인의 보안 내적 요인을 평가하고 있는 특징이 있다. 그러나 사고조치에 대한 기준이 미흡하며 법규 준수에 대한 관리부분이 다른 기준과 비교하여 상대적으로 부족하고 지표의 구체성이 미흡한 실정이다[17].

호주 정부의 보안 프로그램(2006)은 8가지 항목으로 인적자산 보안관리를 수행하고 있다. 즉 자산의 분류, 법제화, 위험관리 등으로 관리 항목이 구성되어 있으며 위협분석과 평가를 지속적으로 수행하여 조직의 보안 취약점을 도출하고 있다. 그러나 사고통제와 인원에 대한 인식 및 교육훈련에 대한 부분은 미흡 하다[16].

III. 인적자산 관리지표를 위한 연구모형

3.1 관리지표 개발을 위한 프레임워크

본 논문에서 인적자산 보안관리 지표를 개발하기 위하여 기존 문헌을 참조하고 한미국방 정보보호 전문가의 의견을 수렴하여 인적자산 보안관리 프레임워크를 개발하였다. 인적자산 보안관리 프레임워크는 ① 신뢰할 수 있으며 개인적인 능력과 자질을 갖춘 인원을 획득하고[10,12], ② 개인 보안관리를 충분하게 지지할 수 있는 개인적인 보안역량을 구비하고[16,17], ③ 임무 수행 중 지속적인 관리와 개인의 보안통제를 유기적으로 실행[5,11]하고 순환하는 것이며 [그림 1]에서 보는 바와 같다.



[그림 1] 인적자산 보안관리 프레임워크

3.2 인적자산 보안관리 지표 도출

본 연구의 보안관리 지표는 인적보안에 관한 선행연구 자료의 참조문헌과 주한 유엔군 사령부 및 한미연합군사령부의 한미 정보보안 전문가들로 구성된 전문가들의 토의와 의견 수렴을 통하여 도출되었다, 또한 김정덕(2003), 김정덕과 김기윤(1998)의 기존 연구에서 제시된 정보보호 지표의 고려요소인 타당성, 객관성, 용이성, 기술과 환경 요소 등을 참조 하고 반영하였다.

본 연구에서 인적자산 관리지표는 3개 분야, 9개 항목, 26개 지표로 구성되어 있다. 보안수준 제고 분야는 인적자산 보안관리 프레임워크에서 제시된 인원보증, 개인역량, 보안통제로 구성되어 있으며 [표 1]과 같다.

첫째, 인원보증(Personnel Assurance)은 배경조사, 자력평가, 보안인증 항목으로 구성되어 인원의 신뢰성에 중점을 두고 관리하는 항목이다. 배경 조사 항목은 조사대상의 범위, 신원조사, 범위의 선정을 지표로 구성 되어 있으며, 자력평가 항목은 인터뷰, 추천 또는 보증, 보안자력이나 이력을 평가하는 지표로 구성되어 있다. 보안인증 항목은 서약이나 동의, 해지

[표 1] 인적자산 보안관리지표 구성

구 분	관리항목	관리지표	ISO 27001 (2005)	NIST 800-53 (2006)	DOD (2001)	MI5 (2007)	ISSPCS (2006)
인원 보증	배경조사	조사대상	-	○	○	○	-
		신원조사	○	○	○	○	○
		조사범위	-	-	○	○	-
	자력평가	인터뷰	-	-	○	○	○
		추천/보증	-	-	○	-	○
	보안인증	보안자력	-	-	-	○	○
		서약/동의	○	○	○	○	○
		해지/중지	○	○	○	○	○
개인 역량	보안의식	승인변경	○	○	○	○	○
		관리의식	○	○	○	○	○
		윤리의식	○	○	-	○	○
	보안교육	직업의식	-	-	○	○	○
		프로그램	-	○	○	○	○
		필수교육	○	○	○	○	○
	보안평가	IT 교육	-	○	○	○	-
		인센티브	-	-	-	○	○
		개인평가	-	-	-	○	○
보안 통제	업무통제	RED 팀	-	-	○	-	-
		임무구분	-	-	○	-	○
		업무교환	○	-	-	○	○
	사고통제	업무분장	-	-	○	-	○
		사고대응	○	○	○	-	-
		사후조치	○	○	○	-	○
	접근통제	신고의무	-	-	○	○	○
		체계통제	○	○	○	○	○
		시설통제	○	○	○	○	○

또는 중지, 승인 변경에 관한 지표로 구성되어 있다.

둘째, 개인 역량(Personnel Competence)은 보안 의식, 보안교육, 보안평가 항목으로 구성되어 있으며 개인의 보안업무 수행 능력에 관한 항목이다. 보안의식 항목은 보안관리 의식, 사회 규범적 윤리 의식, 직업의식으로 구성되어 있으며 보안교육 항목은 보안 프로그램의 시행, 개인별 필수 교육의 이수, IT 지식 및 이해를 위한 교육으로 구성되어 있다. 보안평가 항목은 인센티브 적용, 보안평가로 구성되어 있다.

셋째, 보안 통제(Security Control)는 업무통제, 사고통제, 접근통제 항목으로 되어 있으며 보안업무 간 보안사고 방지를 위한 개인관점의 통제 분야이다. 업무통제 항목은 임무구분, 업무교환, 업무 분장으로 구성되어 있으며 사고통제 항목은 사고대응, 사후조치, 신고 의무로 구성되어 있다. 접근통제 항목은 정보시스템과 정보보호 시설의 접근통제로 되어 있다.

3.3 인적자산 보안수준 제고 항목 도출

위와 같은 인적자산 관리지표가 인적자산의 보안관리 유지에 목적이 있다면, 이러한 지표들이 잘 유지되고 관리되기 위하여 지속적 보안수준 제고 노력이 요구된다. 보안수준 제고를 위한 항목은 선행연구와 한미 국방 정보보호 전문가의 의견을 수렴하여 도출되었으며 아래와 같다. 보안인지는 보안에 관련된 제반 지식과 규칙을 이해하고 숙지하는 수준을 말하며 '보안 제도나 지침, 기술적인 부분을 포함한 제반 사항에 대한 숙지 및 이해의 정도 그리고 윤리적인 가치아래 보안을 지키려는 개인의 의식과 실천의 정도'[12]이다. 규칙준수는 보안연속성 보장에 관한 사항으로 '조직의 보안지침에 따라 지속적으로 이를 준수하는 것'[10]이다. 실수 억제는 인간본연의 실수를 제어하고 이를 억제하기 위한 항목으로 기술적인 뒷받침과 보안인지 기반이 요구되는 항목이다[6]. 즉 인간의 인지 수준이

미치지 못하는 실수를 보완하는 수단 및 통제 요인이라 할 수 있다.

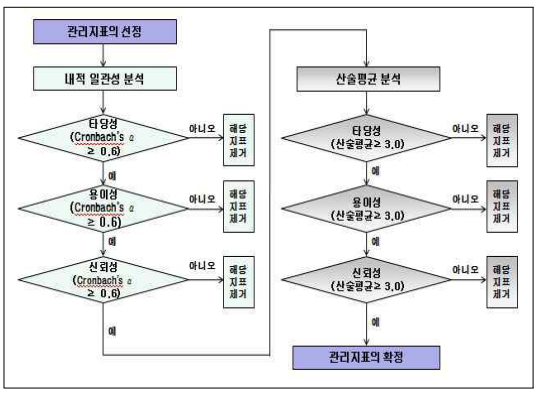
IV. 인적자산 보안관리 지표 실증분석

위에서 도출된 관리지표의 실증 분석을 위하여 ① 관리지표 검증을 위한 부합성 분석, ② 도출된 관리지표와 보안수준 제고 간 유의성 검증을 위한 다중회귀분석을 실시하였다. 부합성 분석에서 내적일관성(Cronbach's α) 계수 값이 0.6이상일 경우, 산술평균 분석에서 3.0 이상의 경우에 한하여 관리지표로 채택하였다. 또한 다중 회귀분석에서 Pearson 상관 계수가 유의수준 0.01, 0.05, 0.001에서 통계적으로 유의한지를 검증하였으며 이를 위한 분석도구로서 SPSS 12를 사용하였다.

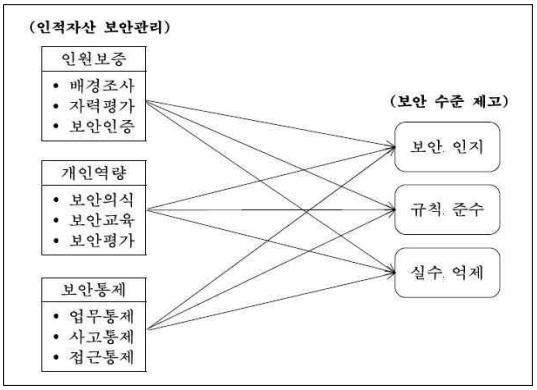
4.1 실증분석 설계

인적자산 보안관리 지표 도출을 위한 부합성 분석은 도출된 지표의 내적일관성을 검증하고 개별 지표들에 대한 지표의 타당성, 유의성, 신뢰성을 평가하였다. 분석 절차는 개별 지표의 타당성, 용이성, 신뢰성을 순차적으로 평가하고 모든 항목에 부합되는 지표에 한하여 최종 지표로 채택하였으며 [그림 2]에서 보는 바와 같다.

본 연구모형은 도출된 지표들이 보안수준 제고에 얼마나 유의한지에 관한 연구 질문을 실증적으로 분석하기 위하여 설계되었다. 즉 지표의 항목들이 보안수준에 영향을 미치는지에 관한 연구이며 유의한 영향을 미칠 경우, 지표들은 실질적인 보안수준 제고에 유용할 것으로 평가될 수 있을 것이다. 본 연구에 적용되



[그림 2] 인적보안관리지표 부합성 분석 연구모형



[그림 3] 인적보안관리지표와 보안수준 간의 연구모형

는 두 변수 간의 다중회귀분석을 위한 연구 모형은 [그림 3]과 같다.

연구 가설은 인적자산 보안관리와 보안수준 제고 간의 관계 검증을 위하여 구성하였다. 가설 1.1~1.9는 인원보증을 철저하게 할수록 보안 수준 항목이 높아진다. 가설 2.1~2.9는 개인역량 관리를 철저하게 할수록 보안 수준 항목이 높아진다. 가설 3.1~3.9는 보안통제를 철저하게 할수록 보안 수준 항목이 높아진다고 설정하였으며 가설 중 인원보증과 보안수준 제고의 항목 간 가설은 [표 2]와 같다.

[표 2]인원보증과 보안 수준제고 항목 간 연구가설

구 분	연구가설
가설1.1	배경조사를 철저하게 수행할수록 보안 인지 수준이 높아진다.
가설1.2	배경조사를 철저하게 수행할수록 규칙 준수 수준이 높아진다.
가설1.3	배경조사를 철저하게 수행할수록 실수 억제 수준이 높아진다.
가설1.4	개인자력 평가를 철저하게 수행할수록 보안 인지 수준이 높아진다.
가설1.5	개인자력 평가를 철저하게 수행할수록 규칙 준수 수준이 높아진다.
가설1.6	개인자력 평가를 철저하게 수행할수록 실수 억제 수준이 높아진다.
가설1.7	보안인증을 철저하게 수행할수록 보안 인지 수준이 높아진다.
가설1.8	보안인증을 철저하게 수행할수록 규칙 준수 수준이 높아진다.
가설1.9	보안인증을 철저하게 수행할수록 실수 억제 수준이 높아진다.

4.2 설문조사와 자료수집

본 연구의 설문조사는 리커드 척도 5를 적용하였고 국방분야 보안관계자를 대상으로 실시되었다. 배포한 설문은 총 85부이며 이중 65부가 회수되어 약 76%의 회수율을 보였다. 자료수집의 인구통계학적 특성은 다음과 같다. 응답자 현황 중 가장 많은 분포를 차지하고 있는 것은 과장급 29명(45%), 30대 25명(39%), 관리적 보안업무자 41명(64%), 보안 경력 11년~15년이 25명(39%)으로 나타났다.

4.3 실증분석 결과

4.3.1 부합성 분석 결과

인원보안관리 지표의 부합성 분석 결과, 모든 지표들은 내적 일관성(Cronbach's α) 계수 값이 0.6 이상으로 나타나 일관성을 유지하고 있으며, 부합성 분석 평가기준인 타당성, 용이성, 신뢰성에 대한 지표들의 산술 평균값은[표 3]과 같다.

[표 3] 부합성 분석을 위한 산술 평균 결과

구분	항목	지표	평균값		
			타당성	용이성	신뢰성
인원보증	배경조사	PA11	4.121	4.020	4.165
		PA12	4.272	3.216	4.254
		PA13	3.983	3.985	4.103
	자력평가	PA21	4.494	4.136	4.354
		PA22	3.805	3.737	4.185
		PA23	2.124	3.845	3.907
	보안인증	PA24	3.266	3.973	3.826
		PA31	4.320	4.272	4.225
		PA32	4.126	3.704	3.823
개인역량	보안의식	PA33	3.987	3.865	3.927
		PC11	4.754	3.526	3.946
		PC12	4.453	3.247	3.827
	보안교육	PC13	3.982	3.498	3.906
		PC21	4.271	4.151	4.220
		PC22	4.242	3.970	4.154
	보안평가	PC23	4.315	4.049	4.182
		PC31	4.050	4.220	4.252
		PC32	3.487	4,599	4.734
보안통제	업 무통제	PC33	3.728	3.568	4.241
		PS11	4.119	3.944	4.213
		PS12	3.858	3.164	3.901
	사고통제	PS13	3.927	3.383	4.110
		PS21	4.175	3.926	3.938
		PS22	4.304	3.545	3.887
	접근통제	PS23	3.593	3.472	4.486
		PS31	4.362	4.133	4.215
		PS32	4.211	4.571	4.584

지표별 평균값이 대부분 판정의 기준이 되는 값인 3.00이상으로 나타나고 있으나, 인원보증 분야의 법규준수 지표(PA23)는 타당성의 기준에 미치지 못하여 지표로서 탈락 조치하였다. 법규준수 지표(PA23)의 탈락은 지표의 내용이 보안인증 항목과 중복되어 있으므로 타당성에서 유효하지 못한 것으로 평가되었다. 그러나 이를 제외한 모든 지표들은 본 연구에서 도출한 지표들이 일관성과 부합성을 충분히 확보하고 있음을 뒷받침하는 것으로 판단된다. 그러므로 산술평균 분석에서 3.0 이상에 부합되지 않는 법규준수 지표(PA23)를 제외한 총 3개 분야, 9개 항목, 26개 지표를 인적자산 보안관리 지표로 채택하였다.

4.3.2 다중회귀 분석 결과

위에서 도출된 관리항목은 다중회귀분석을 통하여, 독립변수(인원보증, 개인역량, 보안통제)와 종속변수(보안인지, 규칙준수, 실수억제) 간 상관관계를 분석하였다. 분석 결과를 종합하면 인원보증과 개인역량 항목이 보안통제 항목보다 보안수준 제고에 보다 유의한 것으로 나타났으며 세부결과는 [표 4]와 같다.

인원보증 분야의 배경조사는 보안수준 제고의 모든 항목에 유의하였다. 자력평가는 규칙준수와 실수억제에 유의하였으나, 보안인지에서 기각되었다. 이는 개인의 자력평가 수준이 높다고 보안인지 수준이 높아지는 것이 아님을 시사한다. 보안인증은 보안인지와 규칙준수에 유의하나, 실수억제에는 유의하지 않는 것으로 평가된다. 이는 보안인증이 개인의 접근통제와 취급 정보의 분류를 중심으로 구분되므로 실수 억제에는 유의성이 미흡한 것으로 판단된다. 개인역량 분야의

[표 4]다중회귀분석 결과

인적자산 보안관리		보안수준 제고		
분야	항목	보안인지	규칙준수	실수억제
인원보증	배경조사	채택	채택	채택
	자력평가	기각	채택	채택
	보안인증	채택	채택	기각
개인역량	보안의식	채택	채택	채택
	보안교육	채택	채택	채택
	보안평가	채택	채택	기각
보안통제	업무통제	기각	기각	채택
	사고통제	채택	채택	기각
	접근통제	채택	기각	채택

보안의식과 보안교육은 중요한 보안수준 제고의 항목으로 모두 유의성을 가지고 있으나, 개인의 보안평가가 실수를 억제하는 것에 대한 유의성은 미흡한 것으로 나타났다. 이는 보안평가의 이론적 내용보다 실질적인 운영 능력이 실수억제에 보다 유의한 것으로 판단된다.

보안통제 분야의 업무통제는 보안수준 제고의 실수억제 항목에는 유의하나, 보안인지와 규칙준수에는 유의성이 미흡한 것으로 나타났다. 이는 업무통제의 영역이 업무분장과 개인의 역할 및 의무를 강조하는 사항이므로 보안인지과 규칙 준수와 유의성이 상대적으로 미흡한 것으로 판단된다. 사고 통제는 보안인지와 규칙준수에는 유의하나 실수억제에는 유의성이 미흡한 것으로 나타났다. 이는 사고통제가 실수를 억제하는 어느 정도의 순기능은 있으나, 사후 통제의 개념이 강하므로 유의성이 미흡한 것으로 판단된다. 접근통제는 보안인지와 실수억제에 유의하나, 규칙준수에는 유의성이 미흡한 것으로 나타났다. 이는 접근통제의 항목이 기술적인 방법을 강구하여 시스템적인 조치로서 통제는 가능하나 개인적 관점의 통제로는 유의성이 미흡한 것으로 판단된다.

위의 검증결과를 종합적으로 해석하면, 도출된 보안관리 지표와 보안수준 제고의 항목은 대체로 유의한 것으로 나타났다. 또한 기각된 항목일지라도 보안관리 시 모든 항목이 중요하므로 실증분석의 통계적 유의성과 이론적 타당성을 고려하여 조직의 특성과 보안환경에 부합되도록 이를 고려하여 적용하는 것이 바람직할 것이다.

V. 결 론

본 논문은 증가되는 인적자산의 보안위협에 효과적이고 체계적으로 대응하기 위한 인적자산 보안관리 지표 개발의 실증 연구로서 결과는 아래와 같다.

첫째, 본 논문은 정보보호를 위한 인적자산 보안관리 지표에 대한 최초의 학술연구이다. 또한 인적자산 보안관리 분야와 현존하는 보안위협 요인 및 대책을 포괄적으로 연구하여 시의성과 실용성을 갖추고 있다.

둘째, 인적자산 보안관리에 관한 실증적인 연구를 통하여 인적자산 보안관리 프레임워크와 인적자산 보안 관리지표(3개 분야. 9개 항목, 26개 지표)를 도출하였다. 이는 정보보호에서 인적자산 보안관리에 대한 이론적 배경이 될 뿐만 아니라, 국가 차원이나 기업 차원의 인적자산 보안관리의 참고가 되는 지표로 유용할 것이다.

셋째, 인적자산 보안관리 수준 제고를 위한 항목을 개발하고 이를 실증적인 방법으로 검증하였다. 도출된 보안관리 제고 항목을 인적자산 보안관리 시 참조 기준으로 적용하면 유용할 것으로 기대된다.

또한 본 논문은 주한 유엔군사령부 및 연합군사령부에 근무하는 한미 국방보안 실무전문가들의 숙련된 경험 요인들이 포함되어 있으므로 본 연구에서 제시된 미 국방부와 일부 외국군에게 적용되고 있는 '신고의무', 'RED팀 평가' 등의 지표들은 유효할 것으로 기대된다.

그러나 본 연구에서 도출된 지표를 이용한 조직에서의 실제적인 적용 평가는 제한되었다. 향후, 본 논문을 통하여 제시된 연구결과를 실제 조직에서 적용하고 이를 분석하거나 성과를 측정하는 등의 후속적인 연구가 필요하다.

참 고 문 헌

[1] 김정덕, "개인정보보호를 위한 관리체계와 거버넌스," 정보보호학회지, 18(6), pp. 1-5, 2008년 12월.

[2] 한국정보보호진흥원, "국가 정보보호수준 평가지수 모델개발 및 활용에 관한 연구," 정보전략 05-01, 2005년 12월.

[3] F.L. Greitzer, L.J. Kanggas, T.W. Edgar, A.J. Brothers, and P.R. Paulson, "Predictive Adaptive Classification Model for Analysis and Notification: Internal Threat," technology report PNNL-16713, May 2007.

[4] J.S. Broderick, "ISMS, Security Standard and Regulation," Information Security Technical Report, vol. 11, issue. 1, pp. 26-31, Mar. 2006.

[5] R.A. Caralli, "Managing for Enterprise Security," CMU/SEI-2004-046, Dec. 2004.

[6] J. Caylor, M.E. Withman, P. Fendler, and D. Baker, "Rebuilding Human Firewall," Information security development, ACM, pp. 104-106, Oct. 2005.

[7] CIO Megazine, "The Global State of Information Security," July 2008.

[8] CISCO, "Annual Security Report," Nov. 2008.

[9] Deloitte, "Global Security Survey," Nov. 2008.

[10] DOD, "Personnel Security Program," May 2001.

[11] J.H.P. Eloff and M.M. Eloff, "Information Security

Architecture," Computer Fraud & Security, 2005(11), pp. 10-16, Nov. 2005.
[12] R. Goh, "The Importance of the Human Element," Doctorial Dissertation, June 2003.
[13] IDC, "2007 Global Security Survey," Apr. 2008.
[14] V. Leveque, "Computer Society, Information Security, a strategic approach," IEEE, May 2006.
[15] ISO/IEC, "ISO 27001," Oct. 2005.
[16] ISSPCS, Reference No. 6 : "Personnel Security Functional Discipline," July 2005.
[17] MI5, "Personnel Security," NSAC, July 2007.
[18] S. Mikko and W. Robert, "A Critical Assessment of IS Security between 1990~2004," ECIS 2007, pp. 1551-1559, Dec. 2005.
[19] NIST, "SP 800-53," Apr. 2006.
[20] B.V. Solms, "Information Security the Fourth Wave," Computers & Security 25, pp. 165-168, Elsevier, Mar. 2006.
[21] M.E. Whitman and H.J. Mattord, "Management of Information Security," Dec. 2007.

<著者紹介>

차 인 환 (Inhwan Cha) 정회원
1993년 2월: 한국 해군대학 수료
1998년 2월: 한남대학교 경영학과 석사
2001년 5월: 네덜란드국방대학교 국제관계 수료
2009년 8월: 광운대학교 경영정보학과 박사
2009년 10월: A3 시큐리티 R&D 이사
<관심분야> 정보보호관리/거버넌스, Human Factors 보안, 보안정책, 국제보안

김 정 덕 (Jungduk Kim) 종신회원
1979년 2월: 연세대학교 정치외교학과 학사
1981년 8월: 연세대학교 경제학과 석사
1986년 5월: University of South Carolina, MBA
1990년 12월: Texas A&M University, Ph.D. in MIS
1995년 3월: 중앙대학교 정보시스템학과 교수
<관심분야> 정보보호관리/거버넌스, 시스템감리, IT 전략/관리