내부 정보보호를 위한 인원보안 관리 방안 연구

차인환*

A study on the Development of Personnel Security Management for Protection against Insider threat

Cha-in hwan*

요 약

본 연구는 최근의 내부 보안위협 추세를 고려하여 인원보안 관리 수준을 효과적으로 측정할 수 있는 인원보안 관리 지표를 개발하는 목적으로 수행되었으며 이론적인 고찰과 기존의 보안관리 체계와 연구 자료를 분석하여 문제점을 도출하고 개선방향을 설정하였다. 연구할 관리항목 지표는 보안 전문가들의 예비 조사를 거쳐 연구 관리지표를 선정하고, 타당성 검증을 위하여 설문조사를 실시하였다. 도출된 관리항목 지표는 인원 보증(Personnel Assurance), 개인 역량(Personnel Competence), 보안 환경(Security Environment)으로 분류하였으며, 지표별 타당성, 중요성, 보안위험 수준에 대한 설문 조사결과를 분석하였다. 조사 결과, 대부분의 관리 지표들이 바람직한 것으로 나타났다. 향후 관련 항목 간의 요인분석 등을 통하여 보다 발전된 인원보안 관리의 계량화 연구가 필요하다.

ABSTRACT

Insider threat is becoming a very serious issue in most organizations and management is responsible for security implementation. This study is to develop a personnel security management indicators in the areas of Personnel Assurance, Personnel Competence, and Security Environment and protection against insider threats. In this study, the information security management system and related papers are examined by reviewing the existing researches and cases. Proposed indicators are verified by pilot test, empirically analyzed to expose experts' perception and the validity, importance, and risk level of each indicators through a questionnaire. Result were encouraging, but additional study focused on personnel security management using factor analysis is needed in the future.

키워드

Insider Threat, Personnel Security, Security Measurement, Measurement Indicator

Ⅰ. 서 론

오늘 날 첨단 과학기술과 정보통신의 비약적인 발전은 우리의 삶 자체를 근본적으로 변화시키고 네트워크를 통한 정보 수집 및 교류가 활발히 이루어짐에 따라 전통적으로 중시되었던 물리적인 가치보다는 정보 가치가 더욱 중요시 되고 있다[1].

특히 대부분의 사람들은 인터넷을 유용한 도구로 여길 뿐만 아니라 모든 조직 환경에 없어서는 안 될 중요한 도구로 인식되고 있다. 그러나 해킹, 바이러스

* 주한 유엔사/ 한미연합사, 광운대학교 경영대학원(MIS전공) 접수일자 : 2008. 10. 22
심사완료일자 : 2008. 12. 12

등 악성 코드의 범람, 사이버 테러 등과 같은 일반적 정보화 역기능과, 내부 위협으로부터 보호받아야 할 정보 자산의 유출이 심화되고 있는 실정이다[2][3][4].

그러나 내부위협의 심각성에 대비한 내부위협 추세 및 행태에 대한 평가와 인원보안 관리를 연계한 포괄적인 인원 보안관리에 대한기준이나 연구는 미흡한 실정이다. 이 연구는 내부위협의 추세와 양상을 고려하고 조직의 인원보안 관리 수준 향상을 위한 방안과 보안관리 항목별 지표를 작성하기 위하여 인원보안 관리지표의 개념을 정립하고 관리 지표를 도출하여 연구 조사 및 분석을 실시하였다.

II. 정보보안관리

2.1 정보보안 관리에 관한 연구

2.1.1 정보보안과 보안관리

정보보안의 정의는 기밀성, 무결성, 가용성이 강구되어 정보를 보호하는 일체의 행위(ISO 27001,2005)라고 정의하고 국정원(2008)에서는 정보시스템 및 통신망을 통해 수집, 가공, 저장, 검색하거나 송수신 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 물리적, 기술적 일체의 행위라고 정의하고 있으며, 정보보안의 보안목표는 기밀성, 무결성, 가용성으로 구성되어 있으며 관리 항목은 거버넌스, 인원, 정책, 위험관리, 법적 기준, 수행, 기술로 분류되어 있다[5][6][7].

Whitman and Mattord(2008)은 정보보안 관리의 목표가 조직 목표 달성을 위하여 조직의 프로세스와 협업관계를 유지한 제반 보안활동이라고 하였으며 계획, 정책, 프로그램, 프로젝터 관리를 관리 원칙으로 제시하였다. 정보보안 아키텍처는 Eloff(2002), Whitman (2003)에 의하여 주로 연구되었으며 Eloff 아키텍처는 전략적(거버넌스, 문화, 계획, 편성, 감사, 통합관리, 요구, 결정), 전술적(위험평가, 인식/교육, 실행, 표준, 가이드라인), 운영적(접근통제, 식별인가, 물리/네트워크/논리적 기술) 관점에서 분류하고 정보, 기술, 사람을 기반으로 구성하였으며, Whitman 아키텍처는 관리적(전략, 계획, 편성, 재해복구, 정책, 위험관리), 전술적(우발계획, 연속성, 인원보안, 사고대응, 논리적 보안), 운영적(접근통제, 식별인가)으로 분류하고 정보, 사람, 네트워크, 인터넷, 시스템, 하드웨어를 기반으로 제시하였다[8][9][10].

정보 보안관리 모형의 국제표준은 ISO 시리즈, CC ,Cobit, NIST 시리즈, SSE-CMM, ITIL, ISF, OCTAVE 등 다양하게 발전되어 왔으나 이 연구에서는 2개의 보안 관리체계(ISMS, ESM)를 중심으로 고찰되었다.

ISMS(Information System Management System)는 ISO에서 개발 되었으며 Broderick(2006)는 BS 7799(2002), ISO 17799/27001(2005), Cobit가 이 체계의 중요한 참조 기준으로 적용됨을 나타내었으며, 카네기 멜론대학 소프트웨어 공학 학회에서개발한 ESM (Enterprise Security Management)은 Caralli (2004)의 연구에서 BS 7799(2002), ISO 17799(2005), Cobit (2005), ITIL, ISF의 기준을 중요한 참조 기준으로 적용하였다[11][12][13].

ISMS는 11개 항목과 39개 통제목표, 133개 통제요인으로 구성되어 있으며 조직의 목표에 부합되고 조직의 구조, 정책, 계획, 실행, 책무, 절차 등을 포함한 정보보안 관리체계로서 조직의 보안위험을 감소하기 위하여 체계의 구축, 실행, 평가, 정비 유지 및 연속성 관리 등의 프로세스를 포함하고 있으며 PDCA(Plan, DO, Check, Act) 사이클을 제시하고 있고 ESM은 2004년 보안 환경과 보안 관리의 복잡성과 어려움에 대한 새로운 보안관리 모형으로 카네기 멜론 대학에서 제안되었으며 조직의 목표에 부합되고 관리적 관점에 비중을 강화하여 보안관리를 조직 전체가 전사적으로 수행되어야 하는 체계로서 8개의 관리 항목과 38개 통제목표로 구성되어 있으며 전략적 목표와 일치, 조직 요구에 부합, 자산관리와 프로세스 관리의 관계, 보안 방향성의 일치, 내부통제의 지속성, IT 서비스와 운영 능력 향상, 자산 라이프 사이클 관리, 측정으로 항목을 분류하였다[6][7].

2.1.2 도전

정보 활용과 유용성에 대비한 정보의 유출, 도난, 오용, 악의적 공격, 개인정보의 침해, 사용자의 실수 등 다양한 형태의 위협은 심화되고 있는 추세이며 이러한 위협에 대응하기 위하여 Kahan(2002)는 정보보

안은 변화의 중심의 위치하고 있으며 기존의 기술적 보안관리는 보안의 넓은 영역에 대한 도전을 해결하기 제한된다고 하였으며 Koh(2003)은 좋은 정보보안 관리는 조직 전반의 적절한 프로세스, 조직 구성원 모두의 참여, 조직 간의 소통, 인원의 성숙도 등이 중요한 요인으로 분류하고 보안을 바라보는 시각이 협소하여 보안관리에 대한 도전에 대처하는 수준이 미흡하므로 보안대책이 기술 중심에서 사람 중심으로 변화되어야 한다고 강조하였다[3][14][15].

최근의 위협 추세는 신속성, 지능화, 무차별 공격의 특성을 가지고 있으며 이에 대응하기 위한 적극적이고 전사적인 보안관리가 절실하게 요구되고 있다. Beritino(2007)는 기술적 보안 관리와 보안부서의 노력만으로 다양하고 예고없는 빠른 보안위협 대응이 제한됨을 지적하였으며 위협 양상변화에 부합되고 효율성 제고를 위하여 조직 구성원 총원이 참여하는 보안 프로세스 기반 하에 전사적인 보안 관리와 특히 내부 위협에 대한 새로운 도전에 직면해 있다.

2.2 내부 보안위협에 관한 연구

Contons와 Kleiman(2008)은 공격의 동기를 탐욕, 권력, 복수, 정치적 이해, 두려움, 일반적인 악에서 비롯된다고 하였으며 Pleeger(2005)는 이러한 동기가 공격을 수행하기 위하여 기술과 지식과 도구를 포함한 방법, 공격 달성을 위하여 소요되는 시간과 접근성이 용이한 기회, 공격을 수행하려는 이유인 동기가 필요하고 하였다[3].

공격 동기와 구성 요건이 충족되면 실질적인 공격이 이루어지며 공격은 시설의 무단 출입, 정보자산의 무단 절취 등 물리적인 경로와 시스템의 악의적 접근, 자료의 변조, 훼손을 위한네트워크 공격, 자료의 무단 복제 및 복사 등 논리적인 경로를 통하여 정보 자산에 접근하는 행태의 양상을 가지고 있으며 정보보안 관리의 취약점을 통하여 공격이 실행되며 관리의 취약점으로는 물리적, 자연적, 환경적, 정책적, 인적, 하드웨어, 소프트웨어, 인적 요인, 매체, 전자파, 네트워크 등이 있다[9][16].

2.2.1 위협 유형과 내부위협

위협은 발생되는 특성에 따라 의도적 위협과 비의도적 위협으로 구분되며 의도적 위협은 외부인과 내부인에 의하여 기술적 위협와 물리적 위협 환경에서 도출된 취약점을 이용하여 표적이 되는 정보 자산을 공격하는 형태이며, 비의도적 위협은 사람, 재해, 시스템의 결함에 의하여 발생되는 위협으로 사람의 실수나 조작 미숙, 자연재해나 설비 장애로 나타나는 위협과 OS 결함이나시스템의 결함으로 나타는 시스템적인 결함에서 비롯되며 위협의 근원지에 따라 내부위협과 외부 위협으로 구분된다[3][4][9][15].

본 연구에서 다루어지는 내부 위협에 관하여 RAND 연구소(2002)는 조직으로부터 정보자산에 접근권한이 부여된 사람으로부터 야기되는 위협이라고 정의하였으며 미국방부는 내부 위협 대상을 인가된 고용원, 인가된 방문자로 구분하고 내부 위협을 유발하는 사람들의 특징을 조직에 불만이 있는 사람, 불법 유출에 관련된 사람, 무관심이나 실수로 유출을 발생한 사람으로 분류하고 있다. Human Firewall Council (2007)은 내부 유출의 피해와 비즈니스의 관계에 관하여 공격은 조직의 기밀이나 지적 재산의 유출, 데이터의 무결점에 대한 손상, 개인 또는 사적 정보의 무단 유출, 중요 정보자산의 손상이나 파괴, 통신의 방해, 공격 피해의 확장성의 형태로 문제가 야기되며 피해가 발생한 조직은 고객 이탈, 경쟁력 약화, 신뢰 감소, 협조의 제한, 금융적 손실, 나쁜 평판이나 이미지의 추락 등의 심각한 손해로 이어진다고 하였으며 미 국방부는 2008 정보보증(IA : Information Assurance) 기조 연설에서 인가된 사람이 인가된 절차를 통하여 인가된 정보에 접근하여 유출하는 내부 보안위협이 가장 치명적이고 위협적이며 통제가 어려운 상태라고 평가하였다[17][18][19].

2.2.2 내부위협 사례 및 평가

내부 위협의 위협 수준은 심각성은 최근 국내외 위협 사례 평가 자료에서 그 추세를 판단할 수 있다. CSI의 Global Security Survey(2007)에서 공격 경로의 59%가 내부에서 발생하고 매체의 도난이나 분실로 인한 사고가 50%, 사용자의 실수에 의한 사고가 50% 수준으로 평가되었으며, Diloitte의 보고서(2007)는 사고의 79%가 사람에 의하며 발생하고 있으며, IDC

(2007)는 사고원인 분석을 통하여 사고원인 발생 순서로 고용원의 문제, 기술적 위협관리에 대한 사용자와 관리자의 기술 부족, 정보자산의 도난, 장비의 오류, 내부 스파이, 무선에 의한 사고 순으로 나타났으며 조직규모가 클수록 내부 보안위협 수준이 높고 내부 보안위협 수준은 대조직의 기준으로 2005년과 대비 약 20% 증가한 55% 수준이고 외부 위협은 20% 수준으로 평가하였다. Human Firewall Council 연례 보고서(2007)는 사고 원인을 내부 사용자의 부적절한 네트워크 접속 및 사용 78%, 내부의 직접적인 공격이 33% 수준으로 평가하였으며 Fawaz(2008)의 위협 유발자 유형 및 동기에 관한 연구에서 사람의 실수에 의한 사고 52%, 정직하지 못한 사람에 의한 사고가 10%로 전체의 과반수가 사람에 의하여 야기된 사고로 분류하였고, 현직에 근무하는 고용원에 의한 사고가 전체의 81%, 돈과 관련된 동기가 44%로 나타났다.

CIO Magazine(2007)에서 실시된 CEO, CIO, 보안관계자(CISO/CSO/INFOSEC DIR)의 설문조사에서 전 설문 조사 종합 결과 해커에 의한 공격은 41%, 내부자에 의한 공격은 69%로 나타났으며 보안관계자들의 설문은 내부자의 보안사고가 84% 수준으로 분석되었다[16][20][21][22][23].

국내의 내부보안 사고는 국가정보원 연례 보고서(2007)에서 산업 기술 유출은 점진적으로 증가됨을 나타내고 있으며 사고 유발자 124명중 퇴직 직원 73명, 현직 직원 31명으로 전체의 83%를 차지하고 사고의 90%가 실수에서 유발됨을 나타내고 있다. 국내 일간지의 최신 자료에는 내부자의 유출이 70% 이상 수준(전자신문, 2008.9.11)으로 평가하고 P 계열회사의 두 건의 내부 직원에 의한 핵심기술 유출에 따른 예상 손실액을 5년간 2조 5천억원, 15조원으로 추산되었다. 또한 2008년 내부 구성원의 도덕적 해이와 관리 부실로 야기된 G기업의 고객 개인정보 유출, 보안정책 부재와 정보 자산 관리 기반 부실의 원인에서 비롯된 국가 기록물 무단 유출 등은 대표적인 우리나라의 내부보안의 문제점을 보여주는 사례이며 내부 사고의 진실에 대하여 침묵하는 불편한 진실(an inconvenient truth)을 부상시키어 내부 위협 에 대한 관심의 계기가 되었다[24][25].

한편으로 보안 관리에 대한 오해를 보안관리의 취약점으로 평가한 Contos와 Kleiman(2007)는 주요 오해들은 위협은 네트워크 외부에서 발생하고, 위협요인은 언제나 식별이 가능하며, 계획만 수립되고 시스템이 구축되면 보안의 안전한 수준이 쥬지될 것이며, 전문 기관에 의뢰하여 보안을 관리하면 문제점을 해결한다는 오해를 일부 가지고 있다고 하였으며, 서승우(2008)는 웜이나 바이러스만 잘 대응하면 보안이 잘 관리되고, IT 개발 투자이후 보안을 후차적으로 조치하여도 보안 수준은 정상적으로 유지될 것이며, 한번 취약점을 조치하면 잠재된 반복적 위험은 없을 것이라는 오해가 있음을 나타내고 있으며 이러한 오해들이 보안관리 발전을 저해하는 요인으로 평가하였다.

오늘날 정보보안 환경은 다양하고 복잡한 위협의 현상과 여러 가지 복합적인 환경 속에서 변화가 진행중이다. 이재우(2008)의 위협 추세 변화에 관한 연구에서 신종 범죄의 라이프 사이클 단축, 악성 소프트웨어 전파의 빠른 속도와 팽창, 공격 수단의 복잡함을 가지고 있는 기술적 특징의 변화와 단순한 공격의 동기에서 금전, 매수, 사기, 조직범죄, 해킹, 사이버 테러, 이성, 권력 등 다양한 동기로 변화되고 합법적인 기회를 조성하고 지능적인 형태로 발전되고 있으며 시스템 공격에서 웹공격으로 경로가 변경되고 외부위협에서 내부 위협으로 위협의 패턴이 변화되고 있다고 하였다[3][26][27].

위에서 살펴본 바와 같이 정보보안의 내부 위협은 인가된 내부 인원의 실수나 악의적 의도에서 비롯되고 식별과 대응이 어려우며 치명적인 위험의 결과를 주므로 내부위협 요인 최소화를 위하여 구성원에 대한 보다 철저하고 효과적인 인원보안 관리가 요구되는 실정이다.

2.3 인원보안 관리 지표 개발

2.3.1 이론적 고찰

Whitman(2006)는 인원보안 관리에 정의를 보안관리에 관련된 인원에 대한 고용, 교육, 인식 등 프로세스에 사람이 연관된 제반 관리라고 하였다. 인원보안 관리에 관련된 국제표준은 관리체계 모형 상의 한 부분으로 관리되어 실질적인 실용성이 제한되는 한계가 있는 이유로 다수의 조직에서 별도의 인원보안 프로그램을 가지고 있으며 관리지표 개발을 위하여 참조

된 몇가지 내용을 살펴보면 아래와 같다[28].

Grobler(2003)은 ISO 17799에서 인원보안과 관련된 항목을 인원이 관련된 직무와 자원에 대한 보안관리, 훈련, 위험 대처능력, 사용자의 책무, 권한의 관리로 분류하였고 ISMS는 별도의 인원관리 항목에 고용 전, 고용 중, 고용 후로 구분하여 지표를 관리하고 있으며 ESM은 보안의식, 보안교육, 인적 자원, 경쟁력, 연속성을 인원보안 관리의 지표로 설정하고 있다[8][12][18].

미 국방부(DOD)는 ISO 시리즈, CC, COBIT 등 국제 표준을 참조하여 GAO의 지침과 NIST의 표준화된 보안지침을 근간으로 인원보안관리 업무를 수행하고 있으며 GAO의 인원보안 인원검증 프로그램을 활용하고 있으며 검증 프로그램은 개인 검증 정보의 공유, 요구 타당성, 전자적 요구 및 승인, 인터뷰 활성화, 지속적인 평가, 조사방법으로 구성되어 있다. 미국방부의 인원보안 관리 규정(2003)은 인원보안 관리 항목이 세부적으로 구성되어 있으며 자국민 중요정보 취급, 선교육 후보직, 충성심, 애국심, 정신 및 신체의 건강, 사회규범 및 도덕성을 기본 원칙으로 설정하고 보안 신고 의무, 보안교육 및 평가, 신원조사 구체화 등을 포함하고 있다[29][30][31].

랜드연구소(2000)는 내부위협을 일으키는 사람을 인가된 구성원으로 분류하고 그들이 야기하는 보안 문제로 범위를 설정하였으며 내부 보안의 위협 항목을 사람(동기, 지식, 행위), 도구(하드웨어, 소프트웨어, 컴퓨팅환경, 비용, 네트워크), 환경으로 분류하고 내부 위협을 대응하기 위한 방법으로 사용자와 공급자간의 보안패치 구축, 이벤트 로그의 지속적 관리 및 분석, 접근통제 강화, 고용 인원의 관리, 악성코드 및 악성 인원의 시스템적인 관리로 구분하고 보조적으로 Red Team(보안 상태를 평가하기 위한 내부에 편성된 인원들이 실제 시스템을 공격하거나, 사람에게 접근하여 자료를 비인가적으로 달라고 요청하는 유인식의 평가 기법), Sandboxes(기술적으로 주요 자산에 직접 접근을 방지하기 위한 메카니즘의 일부로써 완충적 기능을 수행시키는 방법), Banner, Wrapping 등을 활용하고 있다[19].

연합사(CFC)는 한국군과 미군의 보안규칙을 준용한다는 원칙아래 별도의 보안규칙과 인원 보안 프로그램을 유지하고 있으며, 인원의 교육과 인식 및 사용자의 실수 방지를 위한 보완절차와 인가 및 인증에 대한 접근 통제를 중점적으로 관리하고 있으며 정보자산의 분류와 공개 원칙을 세분화하여 개인별로 정보자산이나 정보보호 시설 또는 구역, 정보시스템에 접근이 허용되어 있으며 개인의 보안은 개인 책임제로 수행될 수 있도록 가이드라인을 유지하고 있다. 이정우, 박준기, 이준기((2005)는 중소기업 정보보호 관리 모델의 개발 연구를 통하여 보안조직 및 환경 프로세스를 CEO와 구성원의 의지 및 의식으로 분류하고 인원 보안관리 지표를 인식, 교육, 훈련으로 제시하였다[31][32].

2.3.2 인원보안 관리 지표 연구 수준 및 방법

내부 보안위협의 원인은 인가된 인원의 충성심 결핍, 도덕적 해이, 교육 부재에 의한 사용자의 실수, 인식의 부족, 관리 기반 및 환경의 취약에서 비롯되나 대부분의 보안관리 체계는 인원보안관리 부분을 하나의 기능으로 분류하여 구체적인 인원보안 관리 표준을 제공치 못하므로 실질적인 인원보안 업무 수행이 제한되는 실정이다. 또한 인원보안을 포함한 관리적 관점의 연구 부진도 하나의 요인으로 볼 수 있으며 이에 관하여 Mikko와 Robert(2005)는 1990년부터 2004년간 20개의 세계 주요 IS 저널에 게재된 1,280편의 논문을 조사하였고 그 중 전체의 79%를 차지하는 14개 주요 주제에 비기술적 보안관리 부분의 연구는 23%에 거치고 있으며 보안사고의 빈도가 1998년 37%에서 2003년 90%가 증가한 추세에 대비하여 현저하게 부진한 것으로 평가하였고 인원보안 관리 주제를 직접적으로 연구 노력은 국내외 모두 아주 부족한 편이다[33].

위에서 기술한 바와 같이 내부위협은 심화되나, 기존의 연구와 기준은 보안관리가 사용자(사람)와 도구(정보화)를 동일한 기반 수준으로 평가하고 있으며 또한 기술적 보안 중심의 보안관리 체계 자체 완전성을 목적으로 보안지표가 구성되어 있으며, 사람의 행위, 의식, 욕구, 인식 등 무형적이나 중요한 요인에 대한 지표 항목이 미흡하고, 보안위협의 양상과 패턴의 변화에 부합되지 못하여 시스템적인 보안 관리에 주력하여 내부 위협 요인의 변화나 내부 구성원의 환경 및 행태 변화에 대한 연구는 미흡한 편이다[33][34].

본 연구에서는 이와 같은 기존 정보보안 관리의 문제점을 인식하여 보안위협과 인원보안의 상관관계를 목적 지향적으로 문제를 분석하고 관련 참조 이론을 이용하여 탐색적 연구를 수행하였으며 보안 이론과 아키텍처, 모형과 선행 연구자료를 참조하고 정보화 수준 측정하기 위하여 활용되는 정보화 지표 접근 방법(거시경제적 접근, 사회경제 지표적 접근, 정보 유통량 측정 방법 등)과 정보화 수준을 측정하는 정보 인프라 지수의 평가 방법(미시적 차원과 거시적 차원, 기술적 차원과 비즈니스 차원, 내부적 차원과 외부적 차원 등), BSC 방법(혁신 및 학습 관점, 재무관점, 내부사업 관점, 고객관점)을 포괄적으로 참조하고, 부합성 평가를 고려하여 Hatry(1980)와 Rosen(1993)의 시의 적절성, 신뢰성, 이해성, 통제성, 정확성, 통제성 등의 요소와 정보보안 지표 선정과 관련된 김정덕(2003)의 정확성, 객관성, 미래 예측성, 현실 적용성 등의 요소를 고려하고 김현수(1999)의 타당성, 상대적 중요성, 보안사고의 심각성, 사고 발생 확률에 관한 고려사항을 포괄적으로 참조하여 지표를 개발하였으며 포괄적인 지표 후보를 비교하면 표 1에서 보는 바와 같다[5].

2.4 인원보안 관리 지표의 개발

2.4.1 관리 지표 개발 절차

본 연구에서 인원보안 관리 지표는 6단계를 걸쳐 개발되었으며, 1단계에서 기존의 연구와 참고자료 등을 분석하여 포괄적인 지표 후보를 도출하였으며 2단계에서는 1단계에서 도출된 후보요소들에 대한 개념을 정의하고, 3단계에서는 한미 국방 전문가로 구성된 전문가 그룹 토의를 통하여 후보지표에 대한 파일럿 테스트를 실시하였다. 4단계에서는 한미연합사 장병 중 보안 경험이 있거나 업무를 수행하거나 IT 보안과 연관이 있는 대상자 50명을 엄선하여 지표의 타당성 등 연구와 관련된 의견을 수집하고 5단계에서 지표 항목의 타당성과 가중치, 중요성, 사고의 충격 등에 대한 통계 분석을 실시하였으며 마지막 6단계에서는 바람직한 인원보안 관리지표를 제시하였다.

2.4.2 관리 지표 개발

1단계에서 제시된 지표 항목을 토대로 최종 지표 항목을 도출하기 위하여 인원보안의 계층적 구조를 발전시켜 활용할 필요가 있고 정보보안 요소, 서비스, 역량의 보안지표 고려사항을 참조하여 상호 연계성과 구현 가능성을 예상하여 계층적 수준을 대분류, 중분류, 소분류로 구분하고 미시적 차원의 개념을 적용하여 조직의 프로세스 차원에서 인원보안 관리 지표를 도출하였으며 지표의 분류는 인원보증(인가된 사람이), 개인역량(인가된 활동을), 보안환경(인가된 환경 내에서)으로 분류한 후 중분류와 소분류로 구분하였다.

인원보증(Personnel Assurance)은 신원조사, 인터뷰, 보안 인증으로 구성되어 있다. 신원조사는 인원의 배경조사에 해당하는 항목이며 신원조사대상에 따른 범위를 선정하고 신원조사 결과를 평가하는 지표로 구성되어 있으며 대부분의 조직에서 목표 달성을 위하여 우수한 자원을 구성원으로 활용하고자 하는 본질적인 인적 자원관리의 목적이기도 하다. 지식과 인성과 바른 가치관 등 제반 요소를 잘 갖춘 사람을 선별하는 것의 첫 번째 단계이며 정책으로 부여된 개인의 권한과 책임을 고려하여 구분하여 수행되어야 한다. 미국방부의 경우 최근 5년 또는 18세 이후의 기간을 대상으로 초기 신원조사를 실시하며 이후 매 5년마다 정기적인 신원조사를 실시하고 있으며 보안인증 등급(극비인원, 중요인원, 일반인원)을 분류하여 부적격 요건 중 하나 이상의 문제가 발생하여도 고용 불가 요인으로 적용토록 조치되고 있으며 핵심인원은 가족, 친구관계, 과거 동료관계, 이혼 등 개인 사생활 등에 대한 현지 탐문 조사를 병행하고 있다. 신원조사를 통하여 기본적인 검증이 이루어진 사람에 대하여 인터뷰가 실시되고 인터뷰시 정확성, 자발적 참여, 추천서 또는 평가서, 운전 경력 및 교육 경력 등을 포함한 개인이력 및 병력, 행위에 대한 포괄적인 관찰이 이루어지면 개인의 보안인증을 실시한다. 보안 인증은 보안 등급(정보자산 취급 등급)의 적절성을 평가하여 조직과 계약이나 서약을 통한 동의가 이루어지면 최초 보안교육 확인에 따라 출입증, 시스템 접근 인가, 정보자산의 취급이 가능하게 된다. 또한 고용이 일시 정지되거나 해지되면 즉시 개인의 해당 보안 등급이 정지되어 시설이나 구역의 출입이나 정보시스템 접근이 불가하도록 관리된다. 미 국방부는 별도로 고용 계

약서와 별도로 보안서약서에 보안 신고의 의무와 시스템 내의 개인 컴퓨팅에 관한 모니터링에 관한 서약을 포함하여 프라이버시 보호와 관련된 법적 타당성을 확보하고 설치 용도에 부합되게 시스템을 사용토록 통제하고 있고 보안신고는 보안 위반 행위를 인지하거나 발견한 사람이 즉시 신고토록 강제 의무화 되어 있다[17][30][36].

개인 역량(Personnel Competence)은 보안교육, 보안의식, IT 이해 및 보안평가 항목으로 구성되어 있으며 미 국방부는 보안교육을 개인의 보안 수준과 비례되는 항목으로 관리자 책임의 영역으로 보고 있으며

표 1. 인원보안 관리 후보 항목 지표 비교
Table. 1 Comparison personnel security management suggested indicators

대분류	중분류	소분류(항목)	ISMS (2002)	ESM (2005)	DOD (2003)	RAND (2000)	CFC (2004)	이정우외 (2005)
인원보증	신원조사	신원조사 범위의 설정	○	-	○	○	○	-
		신원조사 평가 기준의 정립	-	-	○	○	○	-
	인터뷰	기록과 조사의 정확성	○	○	○	○	○	-
		자발적 참여	-	○	○	-	○	-
		추천서 또는 평가서	-	-	○	-	-	-
		개인 이력 및 병력	-	-	○	○	○	-
		행위의 관찰	-	-	○	-	-	-
	보안인증	인가 등급의 적절성	○	○	-	○	○	○
		서약 또는 계약의 동의	○	-	○	○	○	-
		인증의 해지 및 중지	-	○	○	-	-	-
개인역량	보안교육	지속적인 교육	○	○	○	○	○	○
		개인 교육이력 관리	-	-	○	-	○	○
	보안의식	개인 보안 인식 수준	-	○	○	○	-	○
		보안 윤리 이해 정도	○	○	-	-	-	-
		법적 구속력과 적용 적절성(탈락)	○	○	-	○	-	○
	IT이해	사용자 운용 능력 정도	-	○	○	-	-	-
		IT 위협 대응 수준	○	-	○	-	-	-
		조직 프로세스의 이해(탈락)	-	○	-	-	○	-
	보안평가	개인 보안평가 수준	○	○	○	○	○	-
		모니터링 운용 분석(보안통제 항목 이동)	○	○	○	○	○	○
보안환경	가	보안감사 실시 및 평가	○	-	○	-	○	○
		보안 훈련 실시 및 평가	-	-	○	-	-	-
		개인 보안수준의 인센티브 적용(탈락)	-	-	○	-	○	○
		보안위반 조치 및 관리	○	○	-	○	○	○
	보안조직	조직 및 편성의 문서화	○	○	○	○	○	-
		임무와 역할의 분장	○	○	○	-	○	-
		보안 전문 기구 운영(탈락)	-	-	-	○	-	○
	보안통제	물리적 통제	○	○	○	○	○	○
		논리적 통제	○	○	○	○	○	○
	보안시설	시설/ 구역의 보호 등급 및 기준 설정	-	-	○	-	○	-
		출입 인원의 통제 및 등급 부여	-	-	○	○	○	○
		비상 대비 계획 수립 적절성	○	○	○	○	○	○
		출입 인원의 인가 수준 확인(탈락)	○	○	○	-	○	○

보안교육은 최초 교육, 보충교육, 해외 여행 등의 수시교육, 종료교육으로 시기에 따라 분류하고 학교에서 실시되는 학교 보안교육, 자체적으로 실시되는 부대교육으로 구분하여 실시되도록 의무화하고 교육은 한미 국방 보안 전문가 토의에서 가장 우선되어야 하는 보안관리 요인으로 식별되었다. 보안의식은 정신 보안의 영역이며 초기 인터뷰나 신원 조사시 일부 검증되기도 하기만 조직의 구성원이 조직에 대한 충성도와 친밀도와 서로 협조관계를 평가하는 사항이며 공격의 원인에서 언급한 바와 같이 조직의 불만, 악의적인 외부인과의 공모, 해고 등의 불만으로 보안의식이 희박해지면 보안관리 차원에 아주 취약한 요인으로 대두되므로 일반적으로 정신, 문화적 수준, 도덕적 규범, 사회적 신뢰 등의 요인으로 무형적인 보안의 가치로 평가되고 문제가 발생하지 않도록 지속적인 관심과 행위에 대한 관찰이 요구되는 항목으로 볼 수 있다. IT의 이해와 학습은 정보화 기반하에 보안업무 수행간 필수적으로 요구되는 항목이며 IT의 편리성에 대비되는 항목으로 주기적인 교육이나 홍보 등을 통하여 개인의 운영 능력을 유지할 필요가 있으며 보안사고 사례 및 추세 분석에서 언급한 바와 같이 사용자

의 사용 실수와 오류에 의한 사고 사례에서 나타나고 있다. 보안평가는 보안수준을 객관적으로 평가하는 도구이며 보안관심 제고와 동기 부여를 위한 인센티브와 제재를 적절하게 유지할 필요가 있으며 미국방부의 경우 보안평가 결과를 일상 개인근무 평정과 교육 전과정의 성적에 반영하고 있으며, 가상의 공격팀에 의한 공격(Red Team) 등 다양한 방법으로 평가를 실시하고 조직의 특성에 따라 보안감사와 지도방문을 계획에 반영하고 추진하고 있다[37][38][39][40].

보안 환경(Security Environment)은 보안조직, 보안통제, 보안시설로 구성되며 보안조직은 실질적으로 보안 업무의 실무를 관장하는 조직이므로 조직의 특성과 규모에 맞게 편성되어야 하고 임무와 역할이 구체적으로 부여되어야 한다.

Briney과 Prince(2002)는 보안조직의 규모를 조직내의 컴퓨터 수를 기준으로 설정하였으며 소형 조직은 컴퓨터 수가 10~100대, 중형 조직은 컴퓨터 수가 100~1,000대, 대형 조직은 컴퓨터 수가 1,000~10,000대, 초대형 조직은 컴퓨터 수가 10,000 이상으로 분류하였으며 Whitman과 Mattord(2007)는 위 조직의 규모에 적합한 보안 조직을 제시하였고 표준 보안 조직은 그림 1에서 보는 바와 같다.

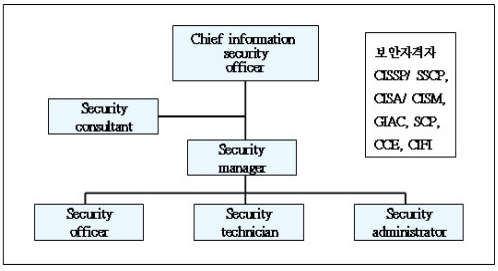

그림 1. 인원보안 관리 표준 조직
Fig. 1 Personnel security standard organization

보안통제는 물리적 통제와 논리적 통제로 구분되며 물리적 통제는 설비나 시설을 기반으로 시설의 출입을 통제하는 것을 말하며 지문, 홍체, RFID, 뱃지 등 출입인증 식별이 가능한 매체로 인가된 시설에 출입하는 형태로 자동화 시스템으로 관리되고 하드웨어, 소프트웨어의 무단 반출입을 통제하거나, 저장매체가 포함된 장비와 물품을 임의로 시설 외부로 반출할 수 없도록 하는 것이다. 논리적 통제는 정보시스템의 인가 및 인증이나, 정보시스템 내에서 비인가된 소프트웨어의 사용 차단, 보안관제 시스템의 운용, 인가된 인원의 인가된 범위의 자료 접근 및 생성, 정보공유 권한 및 지식관리 권한의 통제 등 보호해야 할 자산에 해당 보안 인증을 가지고 있는 사람이 접근할 수 있도록 통제하는 것이다. 보안시설은 정보자산의 안전한 시설 내 보관을 의미하며 보호 시설의 가치와 중요도에 따라 출입이 자유로운 시설, 통제되는 시설로 구분되어 관리되어야 하며, 보호 등급이 설정된 시설이나 구역은 인가된 사람에 한하여 가능토록 통제하는 것이다. 보안통제는 조직의 자료나 정보 자산이 등급에 맞는 시설이나 체계에 보호되고, 인가된 사람만 접근하기 위한 통제 항목이다[2][8][41][42][43].

위에서 도출된 후보 항목에 대하여 한미 국방분야 보안전문가(한미연합사, 주한 유엔사, 한국 국방부의 보안업무 담당관급 이상)들을 대상으로 항목의 타당성과 중요성에 대하여 1차 검증을 실시하였으며 대부분의 항목에 대하여 대체로 긍정적으로 평가되었으나 중복성이 있는 5개 항목은 탈락하고 1개의 항목은 분류를 변경하였으며, 최종적으로 도출된 항목은 조작적 정의에 해당되는 소분류를 포함한 계층별 지표는 표 2와 같다.

표 2. 계층별 관리 지표
Table. 2 Layer of management indicators

대분류	중분류	소항목수
인원보증	신원조사	2
	인터뷰	4
	보안인증	3
개인역량	보안교육	2
	보안의식	2
	IT 이해	2
	보안평가	4
보안환경	보안조직	2
	보안통제	3
	보안시설	3

파일럿 테스트를 거쳐서 완성된 연구 항목지표는 항목 요소로서 타당성과 상대적 중요성을 조사하고

항목별로 보안위협에 대한 위험 수준의 정도를 조사하였으며 이는 관리 항목의 지표들이 제대로 수행되지 않으면 어느 정도의 보안위험이 유발되는지를 조사하는 목표로 이루어졌다.

III. 인원보안 관리 지표의 검증

인원보안 관리 지표의 타당성을 검증하고 인원관리에 효과적이고 위협 대응에 적합한 보안관리 지표를 개발하기 위한 통계분석의 결과는 다음과 같다.

3.1 자료 수집 및 표본의 특성

본 연구의 조사대상은 한미연합사 근무 장병 중 보안직책을 수행한 경험이 있거나 보안업무를 수행하거나 보안과 관련된 IT 업무를 수행하는 장병을 50명을 엄선하여 국방 행정정보시스템을 이용하여 이메일 설문조사를 실시하였으며, 총 배포된 설문지의 수는 50부이었으며 회수된 설문지는 총 47부로 94%이었다.응답자 분포는 부장급 5명, 과장급 18명, 대리급 24명, 연령대는 50대 7명, 40대 19명. 30대 21명, 보안경력으로 실무자 10명, 보안업무 유경험자 28명, IT 보안종사자 8명, 기타 1명, 보안경력으로 1~5년 24명, 6~10년 16명, 10년이상 7명이었다.

표 3. 인원보안 관리 지표 분석 결과
Table. 3 The result analysis of management indicators

대분류	중분류	소분류(항목)	타당성	중요성	위험수준
인원보증	신원조사	신원조사 범위의 설정	3.35	3.58	3.52
		신원조사 평가 기준의 정립	3.81	3.94	3.14
	인터뷰	기록과 조사의 정확성	3.15	3.75	3.11
		자발적 참여	4.21	4.10	3.68
		추천서 또는 평가서	3.55	3.54	2.14
		개인 이력 및 병력	3.21	3.61	3.14
		행위의 관찰	3.76	3.56	3.02
	보안인증	인가 등급의 적절성	3.45	3.44	3.87
		서약 또는 계약의 동의	4.21	4.26	4.58
		인증의 해지 및 중지	3.21	4.12	4.64
개인역량	보안교육	지속적인 교육	4.21	4.57	3.55
		개인 교육이력 관리	3.51	3.21	2.07
	보안의식	개인 보안 인식 수준	4.27	4.68	3.77
		보안 윤리 이해 정도	3.94	3.54	3.45
	IT 이해	사용자 운용 능력 정도	4.10	3.86	3.84
		IT 위협 대응 수준	3.16	3.54	3.61
	보안평가	개인 보안평가 수준	3.56	3.21	3.11
		보안감사 실시 및 평가	3.74	3.74	3.84
		보안 훈련 실시 및 평가	3.52	3.22	3.20
		보안위반 조치 및 관리	3.47	4.21	3.99
보안환경	보안조직	조직 및 편성의 문서화	3.87	3.77	3.58
		임무와 역할의 분장	3.55	3.60	3.26
	보안통제	물리적 통제	3.97	4.12	4.51
		논리적 통제	4.21	4.64	4.66
		모니터링	4.54	4.17	3.19
	보안시설	시설/ 구역의 보호 등급 및 기준 설정	3.58	4.36	3.76
		출입 인원의 통제 및 등급 부여	3.26	4.10	3.54
		비상 대비 계획 수립 적절성	3.15	3.31	3.10

3.2 인원보안 지표의 분석

본 연구에서 인원보안 관리 항목 지표로 도출된 인원 인증, 개인 역량, 보안 환경 관리 항목에 대한 지표로서의 타당성과 상대적 중요성 그리고 위협에 관련된 위험의 수준을 조사하였고 척도는 5점 척도를 사용하였으며, 5점이 가장 높거나 가장 바람직한 수준이고, 1점이 가장 낮거나 가장 바람직하지 않은 수준으로 나타내고 있으며 지표에 대한 통계 분석은 표 3과 같다.

표에서 보는 바와 같이 후보로 선정된 대부분의인원보안 관리 지표는 평균치가 3.0이상으로 나타났고 위험 수준의 2개 지표는 3.0 이하로 통계치를 보이고 있으나, 대부분의 항목에서 높은 타당성과 중요성 그리고 항목의 보안관리가 미흡하면 발생되는 보안위험의 심각성을 가지고 있는 것으로 나타났다.

통계에서 보는 바와 같이 타당성과 중요성은 서로 유사한 통계치를 나타내고 있으며 타당성 조사에서는 자발적 참여, 서약이나 계약의 동의, 지속적인 교육, 개인의 보안인식, 사용자의 IT 운용 능력, 논리적 통제, 모니터링이 대체로 높은 타당성을 보이고 있고,

중요성 조사에서는 자발적 참여, 서약이나 계약의 동의, 인증의 해지 또는 중지, 지속적인 교육, 개인 보안 인식, 보안위반의 조치, 물리적 통제와 논리적 통제, 모니터링, 시설 및 구역의 통제와 출입인원의 관리 지표는 4.0 이상으로 높은 중요성 요인으로 나타났다.

위의 인원보안 관리 지표를 제대로 이행하지 않는다면 보안위협에 대한 보안 위험성이 어느 정도인지 조사한 위험 수준 조사에서 서약 또는 계약의 동의, 인증의 해지 및 중지, 물리적 통제와 논리적 통제가 보안위험을 심각하게 손상할 수 있는 지표로 나타났으며 추천서 또는 평가서에 의한 인원 인증과 개인 교육 이력관리는 3.0 이하로 위험 수준에 크게 영향을 미치지 않는 것으로 나타났으며 연구 결과를 통하여 나타난 내용을 참조하여 조직에서 포괄적 인원보안 관리 및 내부위협 대응을 위한 자료로 사용할 수 있으며 조직의 특성을 고려하여 필요한 항목만 선택적으로 활용할 수 있을 것이다.

Ⅳ. 결 론

본 연구는 최근의 내부 위협의 양상을 고려하고 효율적으로 내부 위협에 대응하기 위하여 인적 자원 요인을 대상으로 인원보안 관리 지표를 개발하는 목적으로 연구되었다. 연구를 위하여 이론적인 고찰과 기존의 연구 자료와 지표를 분석하였으며 최근의 내부 위협 보안사례와 양상을 분석하여 내부위협과 인원보안 관리를 연계하여 연구하고 개선 방향을 설정하였다. 연구지표의 도출을 위하여 한미 국방보안 전문가들에게 예비조사를 실시하여 개선 방향의 타당성을 검증하고 토의 결과를 반영하여 인원보안 관리지표 항목을 선정하였다.

선정된 항목의 지표에 대한 실증적 분석을 위하여 보안 경력이 있거나 보안 업무에 종사하는 인원을 대상으로 관리항목 지표의 타당성, 상대적 중요성, 항목이 수행되지 않을시 예상되는 보안 위험 수준에 대한 설문조사 형식으로 분석하고 지표에 대한 타당성을 도출하였다.

연구 결과에서 도출된 결과의 대부분은 관리 항목 지표로서 타당하고 바람직한 항목으로 나타났으며, 인원인증의 계약과 서약의 동의, 인증 업무,개인 역량의 인식과 교육, 보안환경의 보안통제가 특히 중요하고 중점적으로 관리되어 할 요소로 나타났으며 본 연구에서 제시된 인원보안 관리 지표를 활용은 인원보안 관리 수준에 향상과 내부 보안위협을 대응에 효율적으로 활용될 것으로 기대된다.

그러나 본 연구는 관리 항목 지표별 타당성, 중요성, 위험 수준을 분석하여 타당한 결과를 도출하였으나, 보안위협 세부적인 요인과 인원보안 관리 요인 간의 상관관계 분석 및 항목 간 관계를 조사하여 보완할 필요가 있으며, 또한 보안수준 평가를 위하여 가중치를 도출하고 수치화하여 기존의 보안관리 체계 및 인원관리 기준과 연계한 연구와 발전이 필요하다.

참고 문헌

[1] 한영묵, “정보보호 개론”, 2005.
[2] 김세하, “정보보호 관리 및 정책”, 2002.
[3] Contos 외, “Enemy at the Water Cooler”, 2008.
[4] Lenaghan 외, Managing Security Threats and Vulnerabilities for Small to Medium Enterprises, 2007.
[5] 이철원 외, “정보보호 평가방법론 고찰”, “BS 7799를 중심으로 한 운영적 접근법”, 2001.
[6] Carson, Understanding ISO 17799, 2000.
[7] Sam, ISMS ISO 27001, 2007.
[8] Whitman 외, “Management of Information Security”, 2008.
[9] Pfleeger 외, “Security in Computing”, 2002.
[10] Hentea, Information Security Management Architecture and Design Issues, 2007.
[11] Caralli, Managing for Enterprise Security, 2004.
[12] Caralli, A Process Improvement Approach to Security Management, 2006.
[13] Broderick, ISMS Security Standard and Regulation, 2006.
[14] Rojas, The Information Security management Process Model, 2006.
[15] Haar 외, A Model for deriving information security control attribute profiles, 2003.
[16] US CERT, Insider Threat Study, 2008.
[17] Caylor, Rebuilding the Human Firewall, 2006.
[18] Grobler, A Model to Information Security status of an organization, 2003.
[19] Bozek 외, Research on Mitigating the Insider Threat, 2000.
[20] CIO Megazine, “The Global State of Infor-

mation Security", 2007.
[21] IDC, Security Survey Chart, 2007.
[22] CISCO, 2007 Annual Security Report, 2007.
[23] Tittel 외, CISSP Study Guide, 2004.
[24] 한국정보사회진흥원, "2007 정보화 통계집", 2007. 10.
[25] 국정원, "2008 국가정보보호 백서", 2008.
[26] 서승우, "보안경제학", 2008.
[27] IEEE Computer Society, Information Security, a strategic approach, 2006.
[28] Whiteman, Leveraging People to Safeguard Information Resources, 2005.
[29] Dep. Homeland Security, Personnel Security Guidelines, 2004.
[30] DOD 5800.2 Personnel Security Program, 1995.
[31] DOD Directive and US Army Security Regulation Series
[32] 이정우 외, "중소기업 정보보호 관리모델 개발 : 실증연구", 2005.
[33] Mikko 외, A Critical Assessment of IS Security between 1990~2004, 2005.
[34] Goh, The Importance of the Human Element, 2003.
[35] US GAO, DOD Personnel Security Investigations and Cleaeances, 2008.
[36] Lacey, Nation Security Personnel System Evaluation Plan, 2007.
[37] 홍승필, "유비쿼터스 컴퓨팅 보안", 2007.
[38] 대통령령 149, "보안업무시행규칙", 2005.
[39] NORTEL, Unified Security Architecture for enterprise network security, 2003.
[40] VITA, Information Technology Personnel Security Guideline, 2008.
[41] 김종필 외, "정보보호 핵심지식", 2002.
[42] 임종인 외, "Cyber Space의 법과 기술", 2002.
[43] Campbell, An Introduction to Information Control Models, 2005.

저자 소개

차인환(Cha-in Hwan)

2007 광운대학교 경영정보학과 (박사수료)
2005 ~ 현재 주한 유엔사/연합사 보안 과장
※ 관심분야 : 정보보안 관리, 보안감사, 정보화 전략 계획수립, 프로세스 혁신 등