ISSN 2234-4438
중소기업융합학회 논문지 제6권 제3호 pp. 13-19, 2016 DOI : http://dx.doi.org/10.22156/CS4SMB.2016.6.3.013

국내·외 정보보호 관리체계기반의 인적보안의 이론적 비교연구

나현대[1], 정현수[2*]
[1]숭실대학교 IT정책경영대학원, [2]숭실대학교 융합연구원

A Theoretical Comparative Study of Human Resource Security Based on Korean and Int'l Information Security Management Systems

Hyeon-Dae Rha[1], Hyun-soo Chung[2*]
[1]Department of ITPM, Soongsil University
[2]Soongsil Convergence Research Institute

요 약 ICBM(IoT, Cloud, Bigdata, Mobile)의 다양한 융합적 환경에서 IT기술의 발전이 진화되어 기존에 없던 다양한 새로운 정보보안의 위협이 생기고 있다. 또한 주요 금융권과 정부 공공기관을 대상으로 대형 정보유출 사고가 급증하면서 인적 보안의 중요성을 강조하고 있다. 이에 체계적인 정보보호 관리체계 구축은 해킹 및 보안 침해사고가 발생하는 경우 신속하게 대응하여, 피해 규모를 최소화 한다. 본 논문에서는 ISO27001, NIST 800-53, K-ISMS, COBIT, Cyber Security Framework등 주요 정보보호 관리체계에 나타난 인적보안 통제항목의 이론적 비교, 분석을 수행함으로써 보안사고의 주요 원인인 인적보안 문제에 관하여 효과적인 통제 방안과 시사점을 제시하였다.

키워드 : ISO27001, K-ISMS, Cyber Security Framework, 정보보호 관리체계, 인적보안

Abstract In various ICBM (IoT, Bigdata, Cloud, Mobile) IT convergence environments, IT technologies have been evolved, new information security threats have been occurred. As information security incidents in major public agencies, financial institutions and companies occurred, it was emphasized that the importance of human security was disclosed. Thus, implementing of information security management system could protect hacks and security breaches and respond quickly to accidents so it minimized the sized of loss. In this paper, comparison of human security controls shown in ISO27001, COBIT, NIST 800-53, K-ISMS, Cyber Security Framework such as the main information security management systems was analyzed, and proposed of the security implications about effective controls of human resources security issues.

Key Words : ISO27001, K-ISMS, Cyber Security Framework, ISMS, Human Resource Security

1. 서론

최근 정보보호 동향은 ICBM(IoT, Cloud, Bigdata, Mobile) 환경에서 융합적인 신규 서비스들이 출시되어 새로운 다양한 형태의 신규 보안 위협이 예상되고 있다. 인터넷 침해사고의 해킹기법은 기존 DDoS 공격의 수법에서 장기적이고 지속적인 사이버 공격(APT 공격)으로 진화하여 피해를 증가시키고 있다. 이에 비해 우리나라는 사이버 안전기술과 대응체계는 융복합적으로 발전된 ICT(Information and Communications Technologies) 수준에 비해 많이 뒤떨어진 실정이다[1]. 특히 사이버 범죄나 공격으로 인한 국가나 기업체, 개인의 유·무형의 경제적 피해는 계속 증가하고, 심지어 국가안보까지 위협함에 따라 사이버보안 체계를 갖추는 일이 시급하게 요

Received 2016-06-30 Revised 2016-08-17 Accepted 2016-09-02 Published 2016-09-30
*Corresponding author : Hyun-Soo Chung(hsj6553@ssu.ac.kr)

구되고 있다.

2014년 가트너 보고서에 의하면 환경변화에 따른 보안위협 및 보안기술 추이가 기술 중심 (Control-centric)의 대응에서 사람중심 (People-centric)으로 전망하고 있다[2].

2014년 1억400만 건의 정보유출사고가 발생한 카드3사 역시 사람에 대한 보안의 중요성을 알린 사건이었다. 이 같은 내부자 위협은 국내, 외적으로 광범위 하게 일어나고 있는 현상이며, 기술적 공격과 함께 많은 부분을 차지하는 내부 인적 보안의 위협에 대한 통제와 관리가 시급하다[3]. 인적보안은 기술적, 물리적 접근통제, 관리적 측면(채용, 징계, 퇴직 등)에서 의사결정을 의한 중요한 지표를 제시한다. 인적 보안의 범위는 내부 정보에 접근 권한을 소유한 내부 직원, 인가 자 직원 관리 및 외부인의 출입 관리, 퇴직자 및 외주인력 관리 등이 주를 이룬다.

인적보안의 통제를 포함하는 조직의 보안은 각 분야의 유기적인 협조와 노력에 의해 지켜질 수 있으며, 한 분야의 취약점은 조직 전체의 보안수준을 저하시킨다. 그러므로 조직에서 비즈니스의 연속성 확보하고 각종 위협으로부터 정보자산을 보호하기 위해 체계적인 위험 관리가 필요하게 되었다. 국내에서도 “정보통신망 이용 촉진 및 정보 보호 등에 관한 법률”에 근거하여 정보보호 관리체계 인증 제도를 실시하고 있다. 정보보호 관리체계는 단순히 일회성의 단편적인 정보보호대책이라기 보다 좀 더 체계적이고 통합적인 정보 보호 대책을 실현함으로써 정보보호관리체제 수준을 향상 시킨다. 국외의 주요 정보 보호관리체계로는 IS0/IEC 27001, 27002, COBIT, NIST800-53, 미국 Cyber Security Framework 등이 있으며, 이들은 국제적인 표준으로 인적보안에 대한 통제요소를 기술하고 있다.

본 논문에서는 이와 관련한 이론적 배경으로 국내, 외 정보보호 관리체계에 나타난 인적보안 요소를 살펴보고, 각 표준에 나타난 인적보안 지침을 비교, 분석함으로써 효율적인 인적 보안 통제에 관한 제언을 제시 하고자 한다.

2. 관련 연구

인적자산에 의한 보안 사고는 지속적으로 증가하는 추세이나, 보안연구는 기술적 부분에 치중되어 있어 인적자산 보안에 대한 연구는 비교적 적으며 산업 보안에서 기밀 유출의 문제로 인적 보안 연구를 실시한 것이 주를 이루었다. 본 논문에서는 인적보안의 관리 대상을 조직의 내부의 인원으로 제한하였다.

2.1 인적 보안의 개념

인적보안이란 조직의 구성원이 조직의 보안정책에 따라 충실히 보안업무를 수행하고 있는가의 개인적 관점으로, 최소한의 공개 원칙, 보안인증의 지침과 절차를 준수하여 인원으로부터 보안 문제가 발생하는 것을 미연에 방지하기 위한 활동을 통칭한다[4]. 물리적, 기술적 관리 수단과는 다르게 인적보안 관리는 정보를 소지하고 취급하는 직원이 보호 활동의 주체이자 객체이며 보호수단이기도 한다[5].

2.2 정보보호 관리체계와 인적보안

2.2.1 ISO/IEC 27001

ISO/IEC 27001은 정보보호 관리체계에 관한 국제표준이며, PDCA(Plan-Do-Check-Act) 모델에 근거해 ISMS를 수립하고 구현 및 운영하며 모니터링과 검토 그리고 관리 개선의 4단계로 나눌 수 있다[6]. ISMS수립 단계에서는 보안 정책을 확립하고, 이와 관련한 정보보호 관리체계의 구현 범위를 설정한 후, 해당하는 정보 자산을 구별한다. 다음단계로는 위험의 판별 및 분석과 평가를 통해, 식별된 위험에 대응하기 위한 통제 목록 중 통제 목적과 통제사항을 선택한 후 구현계획서를 만든다. ISMS구현과 운영 단계에서는 수립 단계의 구현 계획에 근거해, 관련 보안 대책을 효과적으로 구현하여 운영한다. 필요한 경우 해당 교육과 훈련을 진행할 수 있다. ISMS 모니터링 과 검토단계애서는 정보보호 관리체계의 운영 현황을 정규적이고 지속적으로 관찰하고 점검한다. ISMS 관리와 개선 단계는 정보보호 관리체계 개선을 위해 발견된 문제점과 개선 사항에 관련하여 이를 수정하고 예방 활동을 수행 한다[7].

ISO/IEC 27002는 정보보호정책 및 물리적 보안과 접근통제 등 정보보호와 관련한 11개 영역의 133개 통제 항목이 존재하며, 이중 인적보안과 관련한 통제항목 수는 6개이다. ISMS 수립을 위한 세부 실무적인 지침과 일반적인 실천 원칙을 담고 있다.

인적 자원 보안에 관한 내용은 고용이전과 고용 도중 그리고 고용의 종료 3단계로 나누어 지침을 정리하고 있다. 고용 전에는 채용을 위한 사전 심사나 고용조건에 명

시하는 보안 역할에 책임에 관한 내용을 다룬다. 고용 동안에는 준수해야 하는 공식적인 규율을 명시하며, 퇴사 후는 종사기업 정보 및 장비 반환, 기밀 서약의 통제사항을 언급하고 있다.

2.2.2 COBIT 5

1996년 ITGI(IT Governance Institute)는 전문가들의 합의과정을 거쳐 개발된 IT 거버넌스, 통제 및 보증을 위한 실무 추천서인 COBIT(Control Objectives for Information and related Technology)을 개발하였다. IT 거버넌스를 프레임워크의 형태로 하여 실제 활용되는 Best Practice를 담고 있어, 구조와 개발 방법론에 실무규범으로 사용한다. 즉, 보안은 품질(Quality), 신용(Fiduciary)과 함께 IT 거버넌스의 세 가지 요구 사항의 하나로 취급된다. COBIT 5는 5개의 도메인과 37개 프로세스, 그리고 프로세스별 세부행동 등으로 구성된다. COBIT 5는 5개의 원칙이 존재한다[8].

① 이해관계자의 요구 충족: IT 거버넌스는 효과, 위험, 자원 평가와 관련된 의사 결정 시 관련된 모든 의사결정자들을 고려해야 한다.

② 조직의 모든 부문 포괄: IT 거버넌스는 IT 조직/기능에만 한정되는 것이 아니라, 조직 내 모든 거버넌스와 연계 및 통합되어야 한다.

③ 하나의 통합적인 프레임워크 적용: COBIT 5는 기업 내 IT와 관련된 모든 것(업무, 조직, 지침, IT 시스템 등)을 통합하는 모델로서 활용되어야 한다.

④ 총체적인 접근방법의 활용: 조직의 IT를 효과적으로 관리하기 위해서는 모든 구성요소에 대한 총체적인 고려가 필요하다.

⑤ 거버넌스와 관리의 분리: COBIT 5.0에서는 COBIT 4.0/4.1과는 달리 거버넌스와 관리영역을 분리하여 정의하고 있다. 관리 영역에는 실제 IT 업무 담당자들의 기획, 시스템 구축, 운영, 모니터링 활동이 포함되며, 거버넌스 영역에는 고위 경영진들을 위한 의사결정, 평가 및 모니터링 활동들이 포함된다[9].

2.2.3 NIST 800-53 Rev.4

NIST 정보보안 표준안은 미국 'E-Government Act'의 일부(Title Ⅲ)인, 연방 정보보안 관리법(FISMA)에 근거해 표준안 (FIPS; Federal Information Process Standard))과 특별 고시 (SP; Special Publication) 형태로 제공된다[10]. NIST800-53은 정보시스템에 대한 정보보안 계획수립, 문서화 이행에 관한 내용을 다룬다. 이 프레임워크에서는 ①정보시스템 분류, ②정보보안 통제(대책) 선택, ③정보보안 통제 실행, ④정보보안 통제 평가, ⑤정보시스템 보안 인정, ⑥정보보안 통제의 모니터링의 단계를 순환 반복하여 개선할 것과 정보보안 통제 항목으로 18개 분야 256개 항목을 자세하게 정의해 제시했다[11].

접근통제, 보안의식 교육, 감사 가능성, 보안평가, 구성관리, 침해사고 대응, 유지보수, 매체보호, 보안계획, 위험평가 등 모든 통제사항을 포함한다. 인사보안 통제 내용은 IS027001과 유사하다.

2.2.4 Cyber Security Framework

오바마는 2013년 2월 주요 기반시설의 사이버보안 강화를 위한 행정명령(Executive Order 13636)과 정책지침(PDD 21)을 발표하였다[12].

행정명령 13636호는 주요 기반시설의 보호체계 구축을 위한 사이버보안 프레임워크의 개발 과 보급을 핵심 목적으로 하여, 이에 따라 사이버보안 프레임워크(Framework for Improving Critical Infrastructure Cyber Security)를 개발했다. 프레임워크는 크게 주요기능을 5가지로 첫째, 인식(Identify) 둘째, 보호(Protect) 셋째, 탐지(Detect) 넷째, 대응 (Respond) 마지막으로 복구(Recover)로 분류한다. 각 기능에 포함된 사이버 보안 결과물들을 프로그램 수요 및 특정 활동에 따라 그룹화한 범주를 나누었다. 하위분류(subcategories) 는 범주를 보다 더 구체적으로, 전문화된 활동을 명시하였다. 참조내용(reference)을 통해 주요 기반시설 부문에서 일반적으로 사용되는 구체적인 표준, 가이드라인, 시행방식 등을 제시했다. Cyber Security Framework는 인적보안 통제로 내부직원 및 외부 협력사, 파트너의 정보보안 역할과 의무, 보안교육 인적보안 세부실천사항을 포함한다.

2.2.5 K-ISMS

한국정보화진흥원의 ISMS는 ISO/IEC 27001의 국제적 표준을 접목하면서, 국내의 상황을 고려하여 제작된 정보보호 관리 표준모델이다. '정보통신망 이용 촉진 및 정보 보호 등에 관한 법률' 제47조에 근거해 규정이 제정되어, 적절한 정보보호 관리체계 구축을 통한 국내 정보

보호 수준을 향상시키고 정보보호 산업의 활성화에 기여하고 있다. K-ISMS는 13개 분야의 92개 통제사항에 기반 하여, 정보보호 관리체계를 수립하고 운영하려는 조직이 이를 활용 할 수 있다.

국내 ISMS의 인적 보안 통제내용은 내부 사용자, 조직구성원 및 정보시스템을 취급하는 제3자, 외주인원의 실수, 사기, 도난, 오용의 위험을 제거하거나 최소화하는 내용을 포함한다. 또한 정보보호의 위협과 취약점에 대해 관련자들이 해당 내용을 반영하고, 업무 이행 시 조직의 정보보호 정책을 준수하도록 한다.

3. 정보보호 관리체계의 인적보안 분석

3.1 정보보호 관리체계의 인적보안 항목의 비교

각각의 특징과 고유 철학을 담고 있지만 인적보안의 구체적 내용 분석을 위하여 국내, 외 주요한 정보보호 관리체계의 인적보안 조항을 비교하였다. Table 1은 5가지의 정보보호 관리체계에 포함된 인적보안 통제항목을 K-ISMS를 기준으로 서로 비교하여 정리한 내용을 나타내고 있다.

Table 1. Comparison Analysis for Control Lists of Human Resource Security

K- ISMS	ISO/IEC 27001, 2013	COBIT 5	Cyber security Framework	NIST 800-53 Rev.4
6.1.1. Main Duty Staff Assignment and Supervision	A.6.1.1, A.7.2.1 Verification of New Employees before Hiring or Contracting	APO13.12	ID.GV-2; Information Security Roles & Responsibilities of Internal, External and Partners	PM-1, PS-7
Described on Awareness, Training and Education Chapter Separately	A.7.2.2	APO07.03, BAI05.07	PR.AT-1; Training for All Users	PM-13, AT-2
6.1.2 Separation of Duties	A.6.1.1, A.7.2.2	APO07.02 DSS06.03	PR.AT-2; Roles & Responsibilities of Permitted Users	PM-13, AT-3
Mention Separately on the Chapter for Third Party Personnel Management	A.6.1.1, A.7.2.2	APO07.03, APO10.04, APO10.05	PR.AT-3; Roles & Responsibilities of Third-party Stake holders (Suppliers, Customers, Partners included)	PS-7, SA-9
6.1.2 Separation of Duties	A.6.1.1, A.7.2.2 All employees of the organization are required to follow policies and procedures established by executives.	APO07.03	PR.AT-4; Roles & Responsibilities of Senior Executives	PM-13, AT-3
6.1.2 Separation of Duties	A.6.1.1, A.7.2.2	APO07.03	PR.AT-5; Roles & Responsibilities of Physical Security Personnels	PM-13, AT-3
6.1.3 Non Disclosure Agreement 6.2.1 Employment Termination and Management of Duty Change	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, Secure Organization according to Termination and Change of Employment	APO01.06	PR.DS-5; Protection Control for Data Leaks	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC31, SI-4
6.2.1 Employment Termination and Management of Duty Change 6.2.2 Regulations of Rewards and Punishment	A.7.1.1, A.7.3.1, A.8.1.4 Official Process for Security Violation Personnel	APO07.01, APO07.02, APO07.03, APO07.04, APO07.05,	PR.IP-11; Detailed Practices of Human Resources Security (Deprovisioning, Personnel Screening Included)	PS family

3.2 인적보안 통제항목

위에서 언급한 국내·외 주요한 정보보안 프레임워크 5가지, ISO/IEC27001, 27002, COBIT, NIST800-53, 미국 Cyber Security Framework, K-ISMS와 김성용의 '정보보호 관리체계를 활용한 인적보안 통제 모델 연구'[13]의 논문을 참조하여, 여기서 제외된 NIST 800-53과 Cyber Security Framework내용을 추가적으로 더한 후 공통된 주요항목을 도출하였다. Table 2는 최종적으로 수집된 정보보호 관리체계의 인적 보안 통제 항목을 제시하고

있으며 통제항목과 관리체계가 잘 준행되고 있음을 보여주는 증빙문서를 제시하였다.

Table 2. Control List of Human Resource Security

Control List of Human Resource Security	Supporting Document
• Defining Roles and Responsibilities for All Users • Screening • Employment Contracts • Information Security Performance Management • Awareness, Training and Education of Information Security • Disciplinary Regulations • Responsibility prior to Termination • Return of Assets • Removal of Access Rights • Authorization Procedure of Provisioning • Job Performance Evaluation of Staffs • Physical Access Controls • Separation of Duties • Disposal of Media • User Registration • User Password management • Review of User Access Rights • Special Rights Management	• Job Descriptions • Employment Procedures / Employment Contracts • Training Plan / Training Reports/ Training Materials • Violated Details Documents for Information Security Disciplinary Personnels • Personnel Regulations / Duty Turnover Form • Non Disclosure Agreement

주요 인적 보안 통제 항목으로는 모든 조직원의 역할과 책임에 따른 접근 통제의 적용과 직무 분리, 고용 계약 에 따른 정보 보호 교육 및 훈련, 퇴직 시 자산의 반납과 매체 폐기 등 물리적인 인적보안 항목이 존재한다.

인적보안과 관련한 주요 문서로는 직무기술서, 고용절차/고용계약서, 교육계획서/결과서/교육교재, 보안관련 위반자 처벌사항 자료와 비밀유지 서약서등이 있다.

3.3 정보보호 관리체계의 인적보안 분석

ISO27001 인적보안은 고용 중에 정보보호 교육의 수립 및 교육훈련의 시행, 평가를 실시하고 있으나 K-ISMS에서는 인적보안 통제 항목에서는 교육과 훈련 부분을 별도의 장으로 분리하여 교육계획, 대상, 내용, 방법, 시행 및 평가에 관한 내용을 기술하고 있다.

ISO27001과 K-ISMS에서는 모두 상벌에 대한 규정을 두어, 임직원이 정보보호 관련 조직 내부 규정(예 : 정책, 지침, 절차 및 비밀유지서약서에 명시된 정보보호 책임을 충실히 이행하지 않고 조직 내 중요정보를 훼손, 누출한 경우, 관계법령상의 책임 및 처벌규정을 인사규정에 포함하고 아울러 정보보호 책임을 충실히 이행한 경우에 대한 보상방안도 함께 두고 있다

K-ISMS의 경우 인적보안 통제 지침에 정보보안 책임 임원에 대한 구체적인 내용이 없다. 현재 일정 규모이상의 기관의 경우 CSO를 두어야 하며 이를 총괄하므로 이에 대한 구체적인 책임 명시도 필요하다고 본다.

ISO27001은 업무 시점을 중심으로 보안조치 사항에 국한하여 인적자산을 통제하도록 되어 있어 좀 더 포괄적인 세부기준이 첨가 되어야 할 것이다.

NIST800-53은 상세하게 보안통제 항목 중심으로 구성되어 있어 보안관리 프로세스에 유용하며 효율적인 교육 훈련과 보안의식의 증대, 인증 및 평가를 중점으로 다루어 인적보안의 관리적 방안을 세부적으로 제시 한다.

Cyber Security Framework의 특징은 5단계의 시차적인 절차로 설계되어 침해 사고가 발생할 경우 신속한 대응과, 다양한 컨텐츠의 교육 프로그램, IT 프로세스와 밀접한 연계성을 강조하는 특징이 있다.

모든 정보보호 관리체계에서 현재 기업의 근무환경이 클라우드 네트워크를 이용하거나 모바일 형태로 업무가 진행되는 부분이 많아, 개인 모바일장비의 사용과 이와 관련한 보안 지침을 마련하는 것이 필요하다고 본다.

3.4 효율적인 인적보안의 위한 제언

사람으로 인한 보안의 사고위협을 최소화하고 기업의 생산성 증대를 위한 인적보안을 유지위한 주요한 5가지 방안을 기술하고자 한다.

첫째, 보안 침해사고는 정보통신망법과 전자금융거래법에서 요구하는 요건에 따라 임원급으로 정보보호최고책임자를 선임하고, 내, 외부 자 에 대한 접근통제 및 모니터링 방안을 수립, 운영한다. 둘째, 정보통신망 법 및 개인정보보호법에서 요구하는 주기적인 교육 활동을 연 2회 이상 전사적실시 한다. 셋째, 보안서약서의 중요성을 환기시키고 퇴사 시 기밀을 준수할 것과 이에 대한 불이행시 조치가 있음을 주지시킨다. 넷째, 보안사항에 대한 일일 점검, 주간 점검, 월별 점검 및 연 1회의 주기적인 감사를 통해 현황 파악 및 개선 사항 그리고 문제점이 조치되었는지를 파악한다. 다섯째, 출입 통제를 다루는 물리적 보안과 이동식 저장매체 관리 등 중요 정보자산에 접근 제어 및 물리 봉인을 실시한다.

4. 결론

ICBM의 다양한 융합적인 기술의 IT환경에서 예상치 못하는 위협이 항상 내재하지만, 많은 침해사고의 주범은 인적 자원, 내부 인가 자를 통해 발생한다. 정보보호 관련 전문시장조사기관인 포네몬 연구소(Ponemon Institute)에서 발표한 '위험에 처한 기업들: 내부 임직원들에 의한 중요 정보의 유출 위험(Risky Business: How Company Insiders Put High Value Information at Risk)' 조사 결과에 따르면 데이터 유출의 대부분이 내부자의 악의적인 행위 또는 실수 등에 의해 발생하였다. 이에 반해 설문에 참여한 72%의 기업들이 "중요 데이터에 대한 내부 직원들의 접근 통제와 관리에 대한 확신이 없다"라고 답해, 대다수의 기업 및 기관들이 잠재적인 정보유출 사고의 피해자가 될 수 있음을 암시했다[14].

그러므로 인적자산의 위협에 대한 정보보호 대책은 조직의 특성을 고려하여 비즈니스 목표에 부응하는 보안 정책의 수립이 우선적으로 이루어져야 한다. 공통적인 부분은 경영진의 정보보안에 대한 적극적인 참여와 인식으로 중요 정보자산의 접근통제나 직원들을 위한 꾸준한 교육이 시행되어야 한다. 본 논문에서는 날로 중요해지는 기업의 인적보안 통제 지침이나 관리 방안을 연구하기 위해 국내, 외 정보보호 관리체계, ISO27001, COBIT5, NIST 800-53, Cyber Security Framework, K-ISMS 속에 기술된 인적 보안 통제 관리지침을 비교, 분석해 보았다. 기존 연구가 ISO27001 중심으로 이루어졌으나 본 논문에서는 K-ISMS를 기준으로 세계 주요 5가지의 정보보호 관리체계를 모두 다루어 이에 나타난 인적보안 통제항목을 비교 분석하였다.

5가지 정보보호 관리체계의 인적보안 통제사항 중 3가지 이상에서 기술된 공통통제항목을 도출하였으며, 각각의 인적보안 체계에 대한 분석을 실시하고 효율적인 인적보안 통제를 위한 제언을 하였다. 특히 빅데이터의 도입과 활용등 데이터의 거버넌스에 많은 관심을 기울이는 트렌드에 비추어 각 기관별 민감 데이터의 구별, 등급과 보관 등 정보 관리 책임자의 지정과 역할 분담도중요한 이슈로 남는다. 인적 보안의 점검항목이 정보 보안 프레임워크 내 관리적, 물리적, 기술적으로 구현되어 유출사고를 방지하여야 한다. 또한 보안은 끊임없는 인식의 과정이므로 입사 전후 보안 서약의 의무, 정규적인 사내 보안교육 활동과 보안 점검을 통한 상벌 내역으로 발전적인 조직의 보안 문화를 형성하여야 한다. 통제항목 간의 비교분석을 통해 도출된 항목들은 국내외 관련 표준 관리방안의 내용을 개선하고, 조직의 정보보호 관리체계의 수준을 높이는데 도움이 될 수 있다. 이 논문은 이론적 연구이므로 이에 대한 설문과 증명을 위한 실증적 후행연구가 한계점으로 남는다.

REFERENCES

[1] Y. Y. Shin, S. H. Jeon, C. H. Lim and M. C. Kim, "Economic Damages Assessment for National Cyber Security Measures - Analysis of the March 20 Cyber Attack", *Journal of National Intelligence Studies, KANIS*, Vol. 6, No. 1, pp. 129-173, Summer. 2013.

[2] Ministry of Science, *ICT and Future Planning*, K-ICT Security SPARK, pp. 10, 2015.

[3] E. S. Kang, "Galaxy Note 7 : stating the lowest prices," http://www.dt.co.kr/contents.html?article_no=2014092202100960800002, 2014. 9.

[4] I. H. Cha, *An Empirical Research on Developing Personnel Security Management Indicators in Information Security, Master Thesis*, Kwangwoon University, pp. 19, 2009.

[5] T. K. Lee, *Prevention of Industrial Information leakage & Methods for Personnel Security, Master Thesis*, Sungkyunkwan University, p. 13, 2011.

[6] T. Humphreys, *How to implement an ISO/IEC 27001 information security management*, ISO Management Systems, pp. 40, 2006.

[7] H. S. Kang, "An Analysis of Information Security Management System and Certification Standard for Information Security," Journal of Security Engineering, Vol. 11, No. 6, pp. 455-468, Dec. 2014.

[8] ISACA, *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT*, ISACA, pp. 14, 2012.

[9] LG CNS, "Review on IT Governance based on COBIT Model," http://blog.lgcns.com/473, 2014. 12.

[10] K. Dempsey, G. Witte and D. Rike, "Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," *NIST*, 2014.

[11] Y. H. Back, "A Study on Vulnerability Check Lists of Information Systems Security Control in Public Sector," *Audit and Inspection Research Institute, Korea*, pp. 28, 2015.

[12] B. H, Bae and E. J. Song, “Comparative Analysis and Implications of Cyber Security Strategies - the US, EU, and UK,” *Information Communication and Broadcasting policy; KISDI*, Vol. 26, No. 21, pp. 5, 2014.
[13] S. Y. Kim, “A Study of Human Security Control Model Utilizing the Information Security Management System,” *Master Thesis, Kangwon University*, pp. 78-89, 2013.
[14] H. K. Yoon, “Data Leakage in North America; Major Cause is on Human Resources in the inside of Organization,” http://www.itdaily.kr/news/articleView.html?idxno =79159, 2016. 6.

저 자 소 개

나 현 대(Hyeon Dea, Rha) [학생회원]

- 1998년 8월 : 숭실대학교 정보과학대학원 석사
- 2014년 2월 : 숭실대학교 SW특성화대학원 석사
- 2016년 3월~ 현재 : 숭실대 IT정책 경영학과 박사과정 재학 중

<관심분야> : 정보보안, 네트워크

정 현 수(Hyun-soo Chung) [정회원]

- 1982년 2월 : 숭실대학교 전자계산학과 학사
- 1991년 2월 : 숭실대학교 컴퓨터학과 석사
- 1995년 2월 : 숭실대학교 컴퓨터학과 박사
- 1982년 2월 ~ 2005년 11월 : ETRI 책임연구원
- 2006년 2월 ~ 2011년 3월 : TANC CTO
- 2009년 2월 ~ 2012년 2월 : 한남대학교 경영정보학과 겸임교수
- 2012년 4월 ~ 현재 : 숭실대학교 숭실융합연구원 교수

<관심분야> : 정보보호, ICBM , IT 감리 & 컨설팅