https://doi.org/10.5392/JKCA.2018.18.04.010

PIMS 인증결함의 보완조치 우선순위에 관한 연구

A Study on the Priority of Complementary Measures about Deficiencies on the PIMS Certification

강다연*, 전진환**, 황종호***
동명대학교 국제물류학과*, 신한데이타시스템 정보보호본부 정보보안기획팀**, 동명대학교 경영정보학과***

Da-Yeon Kang(mswcrash@hanmail.net)*, Jin-Hwan Jeon(germanus74@gmail.com)**,
Jong-Ho Hwang(jongho@tu.ac.kr)***

요약

대다수의 국내 기업 개인정보보호 담당자는 방송통신위원회가 인정하는 개인정보보호 관리체계(PIMS) 인증 취득에 난이도가 존재한다고 판단한다. 이는 사업자마다 개인정보취급에 대한 고유한 특성과 업무절차가 반영되어 정형화된 업무를 규정하기 힘들고, 인증취득을 위해 거치는 여러 과정에서 인증컨설턴트, 인증심사원의 경험에 상당부분 의존할 수밖에 없기 때문이다. 결과적으로 인증취득 실무경험이 부족한 담당자는 PIMS 인증 초기에 무엇을 우선적으로 이행하고 준비해야 하는지에 많은 난관에 부딪히게 된다. 본 연구에서는 계층적 의사결정 기법(AHP)을 통해 인증취득 실무담당자의 PIMS 인증결함의 보완조치 우선순위를 살펴봄으로서 향후 PIMS 인증취득을 원하는 기업이나 인증결함에 따른 보완조치 시 담당자가 우선적으로 선행할 부분을 검토하고자 한다.

■ 중심어 : | 개인정보보호 관리체계 | 결함 | AHP | 우선순위 | 측정 |

Abstract

Most of the privacy officers of organizations are hard to think of the corrective action about deficiencies of the PIMS(Personal Information Management Systems) certification. Because, it is difficult to define the priority of the complementary measures due to the unique characteristics and procedures of personal information protection for each organization. The purpose of this study is to evaluate the priority of the complementary measures using the Analytic Hierarchy Process(AHP). According to the results, it is important to comply with the legal requirements in the first tier. The second tier, PIMS experts answered that dedicated organization, password management, and agreement of the subject are important. Above all, agreement of the subject was found the highest priority for complementary measures about PIMS's deficiencies.

■ keyword : | PIMS | Deficiency | AHP | Order of Priority | Measure |

I. 서 론

국내 개인정보보호 관리체계(PIMS; Personal Information Management System)는 2011년부터 시행되어 개인정보보호를 잘 관리하는 기업들을 식별하는 수단으로 활용되어 왔으며[1], 시행 이후 2016년 3월 현재 총 41개 기업에서 인증을 취득함으로서 개인정보 관련 인증의 구심점이 되고 있다[2].

접수일자 : 2018년 01월 31일
수정일자 : 2018년 04월 06일
심사완료일 : 2018년 04월 06일
교신저자 : 전진환, e-mail : germanus74@gmail.com

모범사례(Best practice)를 중요시하는 대부분의 국내·외 인증과 동일하게, PIMS 역시 신청기관의 개인정보 취급업무가 수립된 정책(지침, 가이드 등)에서 적시하고 있는 절차대로 관리적·기술적·물리적 보호조치를 타당하게 이행하고, 관리·감독되고 있는지 심사 시 확인하여 기준에 부합하는 기관에 인증을 부여하고 있다.

그러나 사업자는 PIMS 인증기준에 부합할 수 있도록 상당한 자원을 투입해야만 하고, 산출의 긍정적인 효과를 달성하기에 상당한 양의 자원과 집중이 필요하며 이를 지속적으로 관리해야만 한다. 인증체계를 구축하는 사전단계에서부터 심사가 진행되는 심사단계, 심사 후 보완조치 단계, 취득 후 지속적으로 관리감독하는 사후관리 등에 수반되는 인적·물적 자원의 투입과 업무량은 상당하다.

이에 따라 본 연구에서는 PIMS 인증 취득 시 도출되는 주요한 결함항목에 대해 살펴보고, 계층적 분석기법(Analytic Hierarchy Process: AHP)을 통해 결함에 따른 보완조치 시 담당자가 우선적으로 선행할 부분을 검토하고자 하는 것이 목적이다. 향후 인증 신청기관 및 취득기관에서 원활한 인증의 운영을 위해 기업의 이해를 돕고, 실무적 제언을 도출하는데 그 목적이 있다.

본 연구의 구성은 다음과 같다. 먼저, 제1장은 서론으로 연구의 목적과 의의를 설명하고 있으며, 제2장은 PIMS 인증과 관련된 개요, AHP에 관한 이론적 선행연구를 포함하고 있다. 제3장에서는 연구모형과 연구도구의 개발을 위한 연구의 설계를 설명하였다. 제4장은 AHP 통한 개인정보의 우선순위에 대한 분석결과를 제시하고 있으며, 제5장에서는 분석결과로부터 도출된 결론 및 시사점을 포함하고 있다.

II. 선행연구

1. 개인정보보호 관리체계(PIMS)

개인정보보호 관리체계는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의3(개인정보보호 관리체계의 인증)과 「개인정보보호 관리체계 인증 등에 관한 고시」(방송통신위원회 고시 제2013-17호)(‘13년 9월)에서 규정하고 있는 3개 분야, 124개 통제항목으로 운영되어 왔다[3]. 이후 2015년 12월 행자부의 개인정보보호 인증제(PIPL; Personal Information Protection Level)과 통합하여 86개의 항목으로 유형별(공공기관, 대기업, 중소기업, 소상공인)로 인증대상을 구분하고 있다[4].

인증의 절차는 준비, 심사, 인증, 사후관리단계의 4단계로 구분된다. 먼저, 준비단계는 인증심사 이전에 인증체계를 구축하기 위해 2~3개월 정도 국내 법령에서 요구하는 수준의 기술적 보호조치를 이행 및 보완해 나가는 단계이다. 통상 전문 컨설턴트로부터 컨설팅이 수반되며, 이때 수립된 정책을 실무에 적용하여 운영 시 산출물로서 증적자료로 준비하게 된다.

심사단계에서는 인증심사원이 신청기관의 관리체계가 인증기준에 부합하는지 현장실사 및 서면심사로 확인하는 단계이며, 심사결과로 신청기관에서 누락되거나 미흡한 사항에 대한 결함항목이 도출된다.

인증단계에서는 심의위원회를 통해 신청기관에서 수행한 결함항목의 보완조치 이행절차가 적절하였는지, 신청기관의 관리체계 수준이 인증취득 요건에 부합하는지를 심의한다. 심의결과가 적합할 경우 신청기관은 인증을 취득하게 된다. 상기에서 설명한 3가지 단계는 최초인증심사에 해당한다. 사후관리단계는 인증을 취득한 신청기관이 지속적으로 관리체계 유지를 위해 노력을 경주하는지에 대한 여부를 매년 1회 이상 심사로 확인하는 단계에 해당한다.

이와 같이 인증취득 과정에 정형화된 절차를 가지고 있으나 실무 담당자의 입장에서는 상당한 업무량을 소화해야 하는 문제가 있다. 먼저, 초기 구축운영 시 인증심사를 위한 증적자료를 확보해야 하며, 무엇보다도 인증심사 후 도출된 결함항목에 대한 보완조치의 이행이 상당한 부담으로 작용한다. 모든 과정에서 처리해야 하는 일에 대한 우선순위 정하기 위한 컨설팅과 보호조치에 수반되는 비용도 신청기관에 부담으로 작용한다.

2. PIMS개인정보보호 관리체계(PIMS)관련 연구

조직이 목표로 하는 정보보호 수준을 유지할 수 있도록 개인정보보호 관리체계를 검토하며 보완하는 개인정보보호 관리체계 인증제도는 조직의 개인정보보호

관리 능력에 대한 보증의 역할을 수행한다. 개인정보보호 관리체계와 관련된 연구는 다음과 같다.

우선, 박대회 등(2015)는 공공기관의 정보시스템 운영 단계에서 필요한 개인정보보호 관점의 운영관리 점검 항목을 개발하였다. PIMS 및 PIMS의 심사항목을 비교/분석하고 개인정보처리시스템에 대한 관리를 외부에 위탁하는 공공기관의 특성을 고려하여 개인정보보호법의 위탁자 관련 조항을 근거로 점검항목을 도출하였다[5].

박태경 & 김세현(2014)는 PIMS와 PIPL의 속성을 가지고 컨조인트 분석을 통해 중소기업과 소상공인을 대상으로 선호하는 유형의 제도를 분석하였다. 연구 결과 속성 중에서는 인증 후 혜택을 가장 중요시 하는 것으로 나타났다[6].

박대하 & 한근희(2013)은 국내 개인정보보호법의 위탁 시 준수사항을 토대로 클라우드 및 개인정보 관련 국제 표준과 국내 인증 제도를 분석하여 클라우드 개인정보 위탁이 가능한 시나리오를 제시하고 클라우드 환경에서 개인정보 위탁자에 해당하는 클라우드 소비자와 개인정보 수탁자에 해당하는 클라우드 제공자 간의 위탁 관리를 위한 개인정보보호 관리체계 통제를 제안하였다[7].

차건상 등(2013)은 공공기관 및 민간기업의 개인정보보호담당자와 개인정보관리체계 인증제 관련 전문가를 대상으로 개인정보보호법상의 자율규제 확보를 위한 인증제 마련시 고려사항을 도출하여 개인정보보호법상의 적용대상을 고려한 개인정보관리체계 인증제 도입 방안을 제시하였다[8]. 또한 정보보안 표준의 비교/분석을 통해 연구한 연구들이 많았다[9][10].

이외에 개인정보관리적인 측면의 연구로는 개인정보 통합콘텐츠관리시스템 개발을 통해 콘텐츠의 활용을 극대화 하는 방안을 제시한 연구가 있으며[11], 김희완 외(2011)는 개인정보영향을 평가하고 그에 따른 개인정보보호 감리 절차 및 방법을 제시하였다[12].

3. 계층분석의사결정(AHP)

Saaty(1977)에 의해 고안된 AHP는 계층분석적 의사결정 방법으로 복잡한 의사결정 문제를 계층적으로 분석하여 최적의 대안을 선정하는 기법이다[13]. 분석에 있어 주관적인 평가요인을 포함함으로써 기업, 병원, 국방 등에서 계획수립 및 의사결정, 한정된 자원의 배분과 관련된 다양한 문제를 해결하는데 탁월하다. 주요 의사결정 문제로 특정 대안의 선택서 부터 계획, 할당, 평가, 비용편익 분석, 우선순위 평가 등에서 활용가능하다[14].

AHP 기법은 객관적 평가요인뿐만 아니라 주관적 평가요인을 포함하여 평가할 수 있는 유연성을 가진 기법으로 수리적 이론보다 참여자의 직관을 바탕으로 하여 그 논리적 접근이 쉽다는 장점을 가진다. 특히 집단내 의사결정문제 등에 유용하기 때문에 1980년대 이후 경영과학 분야에서 주요 의사결정 기법으로 인정받고 있다.

대부분의 의사결정문제가 그러하듯 불완전한 정보와 한정된 자원하에서 목적과 기준에 일치되는 최적의 대안을 선택해야 하는 문제를 가지고 있다. 이러한 관점에서 AHP는 최종적인 목적 아래 하위기준들을 수립한 뒤 상위 목표의 관점에서 하위 기준을 평가하여 가중치를 부여하여 평가하는 방식을 취한다[15].

Ⅲ. 연구설계

1. 연구모형

본 연구모형은 한국인터넷진흥원(KISA ; Korea Internet & Security Agency)의 개인정보보호관리체계(PIMS)의 주요결함 항목을 근간으로 하였으며, 연구자와 전문가들의 협의를 통해 평가항목을 구성하였다[16].

다음의 [그림 1]과 같이 계층 1의 평가요인으로 관리과정, 보호대책, 생명주기의 요구사항으로 설정하였다. 또한, 계층 2에서는 각 요구사항의 하부요인으로 선정하여 연구모형을 설정하였다. 관리과정의 하부요인으로는 개인정보보호 조직 및 구성 및 지원할당, 보호대책의 효과적 구현으로 선정하였으며, 보호대책 요구사항 하부요인으로는 개인정보취급자 지정 및 감독, 인터넷 접속통제 개인정보 취급자 권한관리, 개인정보 취급자 접근권한 검토, 개인정보 취급자 및 사용자 패스워드 관리, 암호정책 수립 및 이행, 분석 및 설계보안관리,

개인정보 처리활동 모니터링 및 점검, 개인정보 마스킹, 물리적 접근통제 총 10개의 요인으로 구성하였다. 생명주기 요구사항의 하부요인으로는 정보주체의 동의, 개인정보 취급방침 마련 및 게시, 외부위탁 관리감독으로 구성하였다.

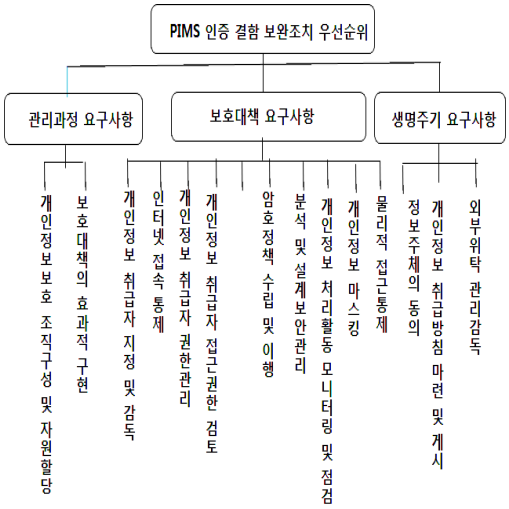

그림 1. PIMS 인증 결함 보완조치 우선순위

2. AHP 평가기준 및 평가항목

본 연구를 위한 평가기준 및 평가항목에 따른 구체적인 설명은 다음의 [표 1]과 같다.

표 1. AHP 평가기준 및 평가항목

평가기준		평가항목	설명
계층 1	개인정보보호 관리체계 요구사항	관리과정 요구사항	개인정보보호 관리체계를 수립하고 운영하기 위해 인증을 위한 최소한의 요구사항을 필수적으로 구현해야 함
		보호대책 요구사항	위험관리를 통해 선정된 통제사항을 개인정보보호 관리체계를 수립하고 운영하기 위해 효과적으로 보호대책을 수립해야 함
		생명주기 요구사항	개인정보 생명주기(수집, 이용제공, 파기)에 따른 정보통신망법 등 법적 요건을 충족시킬 수 있어야 함
계층 2	관리과정 요구사항	개인정보보호조직 구성 및 자원할당	개인정보관리책임자(CPO) 직급 임원급으로 상향 조정 및 실무전담 조직 강화 필요
		보호대책의 효과적 구현	위험감소를 위해 선정한 세부 수행과제의 이행여부 적절성 및 효과성에 대한 검토 필요
	보호대책 요구사항	개인정보 취급자 지정 및 감독	부정확한 개인정보취급자 지정 (선정기준 및 절차 부재)
		인터넷접속 통제	개인정보취급자(다운로드, 파기, 접근권한 설정 권한 보유) PC 외부 인터넷 차단(망분리) 미적용
		개인정보 취급자 권한 관리	업무목적과 무관하게 개인정보취급 권한을 과도하게 부여하고 있음
		개인정보 취급자 접근권한 검토	개인정보처리 권한 부여·변경의 적정성 여부 검토 미수행
		개인정보 취급자 및 사용자 패스워드	기업 스스로 정한 사용자 패스워드 정책 미준수 및 법적 요구사항(복잡도 등) 미반영
		암호정책 수립 및 이행	주요 개인정보(비밀번호, 금융정보, 주민번호 등) 저장, 전송 시 암호화 미적용
		분석 및 설계 보안관리	개인정보처리시스템 개발 시 개인정보영향평가 수행이 미흡함
		개인정보 처리활동 모니터링 및 점검	개인정보 오남용 여부 확인을 위한 개인정보 접속기록 모니터링 미이행
		개인정보 마스킹	개인정보취급시스템에서 일관된 마스킹 처리가 미흡함
		물리적 접근통제	보호구역에 비인가자의 출입통제와 접근이력의 주기적 검토가 미흡함
	생명주기 요구사항	정보주체의 동의	필수 및 선택적으로 수집하는 개인정보 항목에 대한 이용자의 동의가 누락됨
		개인정보 취급방침 마련 및 게시	신청기관의 개인정보취급방침에 법적 요구사항이 일부 누락됨
		외부위탁 관리감독	개인정보 수탁사에 대한 관리감독 미흡

Ⅳ. 실증분석

1. 연구도구의 개발

본 연구의 분석을 위해 개발된 설문지는 계층적 분석과정을 고려하여 Saaty(1990)가 제안한 9점 척도를 사용하였으며, 응답자의 편의를 돕기 위해 각 평가항목에 대한 설명을 함께 제시하였다. 전문가를 대상으로 하는 계층분석과정은 설문의 수량보다 설문의 목적에 부합하는 전문가들의 의견을 반영하는 것이 매우 중요하다[17].

2. 자료의 수집

본 연구를 위한 AHP설문은 2016년 1월부터 2월까지 PIMS 인증 전문심사원, 신청기관 실무담당자, PIMS 인증 컨설턴트 각 10명씩 30명을 대상으로 설문을 실시하였다. 하지만, 설문의 방대함으로 인해 12부(40%)만 모든 질의에 응답하였고, 이를 회수하여 분석에 사용하였다. 분석을 위해 AHP 응답에 대한 조사결과는 Expert Choice 2000을 적용하였으며, 인구통계적 특성은 SPSS 2.0을 적용하였다.

먼저, AHP 설문은 응답자가 일관성을 가지고 평가항목에 응답했는지 검증하기 위해 일관성 비율(CR ; Consistency Ratio) 값을 계산하여 응답의 신뢰성을 검토한다. 일반적으로 CR 값이 0.1 이하이면 응답자의 설문결과는 합리적 일관성을 가진다고 볼 수 있으며, 0.2 미만이면 용납할 수 있는 수준이라고 판단한다. 하지만 0.2 이상일 경우 일관성이 부족한 것으로 판단하여 재검토하게 된다[14]. 본 연구에서는 CR이 0.2를 초과한 7명의 의견은 최종분석에서 제외하고 하였다.

최종분석에 사용된 응답자의 인구통계학적 특성을 살펴보면, 40대 남성 5명으로 신청기관 실무담당자 3명, PIMS 전문심사원, 인증컨설턴트 각 1명으로 나타났다. 개인정보보호 업무경력은 5년 미만 1명, 10년 미만 2명, 15년 미만 2명이었으며, PIMS 인증과 관련된 전담경력도 동일한 것으로 나타났다.

응답자에게 신청기관에 PIMS 구축 시 가장 어려운 점이 무엇인지 물어본 결과, 다음과 같이 조직내 공감대 형성부족을 가장 많이 어려워하는 것으로 나타났다. 이는 정보주체의 권리 강화 및 개인정보보호에 대한 관심을 갖도록 조직에 대한 정부의 정책적 관리와 제도적인 지원이 시급함을 나타낸다.

표 2. PIMS 구축 시 가장 어려운 점

구분	비율
전사차원의 개인정보보호에 관한 공감대 부족 (필요성 인지 부족)	60%
경영층의 비적극적인 PIMS 구축 지원	20%
국내 컴플라이언스의 높은 수준의 기술적 관리적 보호조치의 요구	20%

다음으로 신청기관이 인증을 취득한 후 PIMS 인증을 유지하는데 가장 크게 영향을 미칠 수 있는 정책이 무엇인지 질의한 결과, 자발적으로 이행한 기업에 인센티브 등이 지원되기를 원하는 것으로 나타났다.

표 3. PIMS 인증 유지에 영향을 미치는 요인

구분	비율
자율적 이행에 따른 우수기업의 인센티브 지원	80%
법령에 의한 유출사고에 대한 강력한 기준	20%

3. AHP 분석결과

본 연구를 위한 AHP 분석결과는 다음과 같다. 먼저, PIMS 인증 결함 발생 시 1계층의 개인정보보호관리체계 요구사항 중 보완조치 우선순위를 분석한 결과, [표 4]와 같이 개인정보 생명주기(수집, 이용·제공, 목적달성 후 파기)요구사항의 보완조치를 우선적으로 판단하고 있었다.

표 4. 개인정보보호관리체계 요구사항에 대한 중요도

계층1	중요도	우선순위
관리과정 요구사항	0.157	1
보호대책 요구사항	0.276	3
생명주기 요구사항	0.567	2
CI	0.00	

표 5. 요구사항별 세부통제항목에 대한 중요도

계층1	계층2	CI	중요도	순위
관리과정	개인정보 조직구성 및 자원할당	0.00	0.571	1
	보호대책의 효과적 구현		0.429	2
보호대책	개인정보취급자 지정 및 감독	0.02	0.046	1
	인터넷 접속통제		0.108	7
	개인정보 취급자 권한관리		0.168	5
	개인정보 취급자 접근권한 검토		0.170	4
	개인정보취급자 및 사용자 패스워드 관리		0.046	1
	암호정책 수립 및 이행		0.062	8
	분석 및 설계보안관리		0.124	6
	개인정보 처리활동 모니터링 및 점검		0.193	3
	개인정보 마스킹		0.043	9
	물리적 접근통제		0.038	10
생명주기	정보주체의 동의	0.00	0.646	1
	개인정보 취급방침 마련 및 게시		0.093	3
	외부위탁 관리감독		0.261	2

두 번째로, 2계층의 요구사항별 세부통제항목에 대한

보완조치의 우선순위를 살펴본 결과, [표 5]와 같이 관리과정 요구사항에서는 개인정보보호 업무를 전담조직의 구성을 우선시 하고 있었고, 보호대책 요구사항에서는 취급자 및 사용자의 패스워드 관리를 중요하게 판단하고 있었다. 마지막으로 생명주기 요구사항에서는 개인정보 수집 시 정보주체로부터의 동의부분의 조치가 우선시 되어야 한다고 판단하고 있었다.

마지막으로 도출된 세부통제항목의 보완조치 우선순위를 평가한 결과 다음과 같이 무엇보다도 생명주기 요구사항의 정보주체로부터 동의받는 것을 가장 먼저 조치해야 할 결함으로 판단하고 있었다.

표 6. 요구사항별 세부통제항목에 대한 중요도

계층1	계층2	최종우선순위
생명주기	정보주체의 동의	0.366
생명주기	외부위탁 관리감독	0.148
관리과정	개인정보 조직구성 및 자원할당	0.090
관리과정	보호대책의 효과적 구현	0.067
보호대책	개인정보 처리활동 모니터링 및 점검	0.053
생명주기	개인정보 취급방침 마련 및 게시	0.053
보호대책	개인정보 취급자 접근권한 검토	0.047
보호대책	개인정보 취급자 권한관리	0.046
보호대책	분석 및 설계보안관리	0.034
보호대책	인터넷 접속통제	0.030
보호대책	암호정책 수립 및 이행	0.017
보호대책	개인정보취급자 지정 및 감독	0.013
보호대책	개인정보취급자 및 사용자 패스워드 관리	0.013
보호대책	개인정보 마스킹	0.012
보호대책	물리적 접근통제	0.010

V. 결론

AHP 분석결과를 요약하면, PIMS 전문가들은 인증심사에서 결함이 도출될 경우 국내 법령에 따른 컴플라이언스 이행, 전담조직의 활동, 취급자의 관리, 기술적 통제 등의 순으로 미이행시 법적 위험이 높은 순으로 보완조치의 우선순위를 정하고 있음을 알 수 있다.

먼저, PIMS 전문가들은 인증심사에서 도출된 결함 가운데 사내 개인정보보호를 위해 기술적·물리적 차원의 통제보다는 관리적 차원의 보완조치가 우선시 고려되어야 한다고 판단하고 있다는 점이다. 이는 [표 5]에서 정보주체의 동의, 외부위탁 관리감독 등 생명주기 요구사항의 항목이 1순위와 2순위를 차지하고 있다는 점에서 확인 가능하다.

실무담당자는 PIMS 결함 중 컴플라이언스와 관련된 항목이 있다면 가장 우선적으로 보완조치가 이루어져야 하며, 회사에 적용되어야 하는 법령이 무엇인지 당연히 잘 알고, 전사에 걸쳐 적용될 수 있도록 조치를 고려해야 한다고 볼 수 있다.

또한, 개인정보 처리를 위해 콜센터, 배송업체 등에 위탁함에 있어서 법령에서 요구하는 이용목적 달성 후 파기, 개인정보 유출방지, 개인정보 파일 및 DB의 암호화 등이 미흡할 경우 발생할 위험을 관리감독해야 한다고 판단하고 있는 점이다.

그런 다음의 우선순서로 조직의 개인정보보호 관련 보호대책을 효과적으로 적용하기 위한 전담조직의 마련과 인적·물적 자원의 적절한 할당으로 기수립된 보호대책들이 구현되어야 한다고 전문가들은 판단하다는 것이다. 이는 도출된 결함을 보완하기 위한 일시적인 보호대책의 수립을 넘어 적정 수준이상 전담 실무조직을 구성하고, 그들의 역할과 책임을 강화한다면 장기적인 계획 수립과 더불어 지속적인 관리·감독을 가능케한다는 측면에서 우선순위를 도출한 것으로 보인다.

마지막으로 전문가들은 개인정보보호를 위한 기술적 보호대책 항목들을 보완조치해야 한다고 고려하고 있는데, 보호대책 항목들의 순서를 볼 때 현업담당자의 측면에서는 실무적으로 중요한 의미를 가진다. 통상의 현업담당자들은 업무 특성상 기술적 전문지식을 보유한 실무자가 다수이기 때문에 보완조치 시 개인정보처리시스템의 기술적 취약점을 부분을 먼저 조치하고자 하는 경향이 많았다.

하지만, 보호대책의 우선순위에서 개인정보처리시스템에서 사용자의 처리활동을 대상으로 접속기록의 모니터링 절차보유와 모니터링 이행, 과도하게 부여된 취급자의 권한검토와 권한관리 항목 등이 패스워드관리, 개인정보 마스킹, 물리적 접근통제 보다 우위에 있다는

점은 개인정보취급자 대상 인적차원의 오남용 방지가 더욱 중요하게 조치되어야 한다고 판단된다.

본 연구의 한계점 및 향후 연구방향은 다음과 같다.

첫째, PIMS 전문가라고 할 수 있는 설문응답자들 대상의 업무적 성격이 상이하였다. 향후 연구에서는 응답자가 속한 집단별 평가 결과에 대한 비교・분석하는 연구가 진행되어야 할 것이다. 둘째, AHP기법은 요인 간의 상대적인 중요도만을 측정하기 때문에 다양한 변수에 의한 차이를 알 수 없었다. 추후 연구에서는 다른 연구 방법을 적용하여 분석할 필요성이 있다.

참 고 문 헌

[1] J. H. Jeon and K. R. Cho, "Major changes in the PIMS certification in accordance with the amended public notification," Review of KIISC, Vol.23, No.5, pp.20-23, 2013.

[2] http://isms.kisa.or.kr

[3] Ministry of Government Legistration, Act on Promotion of Information and Communications Network Utilization and Information Protection, 2015.

[4] Korea Communications Commission, Enacted Public Notification for Certification of Personal Information Management System(PIMS), 2013.

[5] D. H. Park, S. N. Yoo, and H. Y. Youm, "Development of Information System Operational Audit Checklist for Personal Information Protection in Public Organizations," Journal of Security Engineering, Vol.12, No.1, pp.47-64, 2015.

[6] K. T. Park and S. H. Kim, "A Study on the Preference Analysis of Personal Information Security Certification Systems: Focused on SMEs and SBs," Korea Institute of Information Security and Cryptology, Vol.24, No.5, pp.911-918, 2014.

[7] D. H. Park and K. H. Han, "A Study on PIMS Controls for PII Outsourcing Management under the Cloud Service Environment," Korea Institute of Information Security and Cryptology, Vol.23, No.6, pp.1267-1276, 2013.

[8] G. S. Cha, H. H. Han, and Y. T. Shin, "An Effective Personal Information Management System to Ensure Self-imposed Control on Personal Information Protection Act," Journal of KISS: Information networkings, Vol.39, No.3, pp.276-281, 2012.

[9] K. Hone and J. H. P. Eloff, "Information security policy-what dointernational information security standards say?," Computers & Security, Vol.21, No.5, pp.402-409, 2002.

[10] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," Information & Management, Vol.46, No.5, pp.267-270, 2009.

[11] 신동석, "분산 콘텐츠 기반의 머천트: 개인정보 통합콘텐츠관리 시스템 개발," 한국콘텐츠학회논문지, 제6권, 제5호, pp.113-121, 2006.

[12] 김희완, 유재성, 김동수, "정보시스템 감리에서 개인정보 영향평가를 통한 개인 정보보 보호," 한국콘텐츠학회논문지, 제11권, 제3호, pp.84-99, 2011.

[13] T. L. Saaty, "How to make a decision: The analytic hierarchy process," European Journal of Operation Research, Vol.48, No.1, pp.9-26, 1990.

[14] O. S. Vaidya and S. S. Kumar, "Analytic hierarchy process: An overview of applications," European Journal of Operational Research, Vol.169, pp.1-29, 2004.

[15] G. T. Cho, Y. G. Cho, and H. S. Kang, *Leading the lader's hierarchy decision making,* Dong-Hyun Publish, Seoul, 2003.

[16] KISA, *개인정보보호 관리체계(PIMS) 인증의 주요 결함 사례*, Privacy Global Edge 2014-CPO

포럼, 2014.

[17] J. G. Yoon, “A Comparison of 3 Statistical Technique for Evaluation MIS Sucess Factor = Application Efeects and Limitations of AHP as a Research Methodology,” Journal of the Korean Operations Research and Management Science Society, Vol.21, No.3, pp.109-124, 1996.

저 자 소 개

강 다 연(Da-Yeon Kang) 정회원

- 2006년 2월 : 한국해양대학교 해운경영학과(경영학사)
- 2008년 2월 : 부산대학교 경영학과(경영학석사)
- 2014년 8월 : 한국해양대학교 해운경영학과(경영학박사)
- 현재 : 동명대학교 국제물류학과 겸임교수

<관심분야> : 정보시스템 보안관리, 보안정책관리, 항만물류보안, 데이터베이스

전 진 환(Jin-Hwan Jeon) 정회원

- 1998년 2월 : 인제대학교 경영학과(경영학사)
- 2001년 2월 : 인제대학교 경영학과(경영학석사)
- 2006년 2월 : 부산대학교 경영학과(경영학박사)
- 현재 : 신한데이타시스템 정보보호본주 정보보안기획팀 부부장

<관심분야> : 정보시스템 보안관리, 전자상거래, 지식경영시스템

황 종 호(Jong-Ho Hwang) 정회원

- 1994년 2월 : 일본 TAKUSHOKU 대학교 상학과(경영학사)
- 1996년 2월 : 일본 TAKUSHOKU 대학교 상학연구(경영학석사)
- 1999년 10월 : 일본 TAKUSHOKU 대학교 상학연구(경영학박사)
- 2000년 2월 ~ 현재 : 동명대학교 경영정보학과 교수

<관심분야> : 정보시스템 보안관리, 데이터베이스, 경영자료분석, 데이터마이닝, 비즈니스특허모델