디지털산업정보학회 논문지 제12권 제3호-2016년 9월
http://dx.doi.org/10.17662/ksdim.2016.12.3.133

개인정보관리체계계(PIMS)를 이용한 클라우드컴퓨팅 개인정보 보안 개선 방안 연구

정 혜 인* · 김 성 준**

Personal Information Management System (PIMS) improvement research using cloud computing security

Jeong Hyein · Kim Seongjun

〈Abstract〉

Recently, in the adoption of cloud computing are emerging as locations are key requirements of security and privacy, at home and abroad, several organizations recognize the importance of privacy in cloud computing environments and research-based transcription and systematic approach in progress have. The purpose of this study was to recognize the importance of privacy in the cloud computing environment based on personal information security methodology to the security of cloud computing, cloud computing, users must be verified, empirical research on the improvement plan. Therefore, for existing users of enhanced security in cloud computing security consisted framework of existing cloud computing environments. Personal information protection management system:

This is important to strengthen security for existing users of cloud computing security through a variety of personal information security methodology and lead to positive word-of-mouth to create and foster the cloud industry ubiquitous expression, working environments.

Key Words : Personal Information Protection Management System (PIMS), Cloud Computing , Privacy Improvements

Ⅰ. 서론

최근 들어 클라우드컴퓨팅의 도입에 있어 보안 및 개인정보보호가 핵심적인 요구사항으로 주목받고 있으며, 국내외 여러 조직에서는 클라우드컴퓨팅 환경에서의 개인정보보호의 중요성을 인식하여 전사적이고 체계적인 접근법에 기초한 연구가 진행되고 있다.

클라우드 컴퓨팅이 과거의 네트워크 컴퓨팅, 유틸리티 컴퓨팅, 서버 기반 컴퓨팅, 그리드 컴퓨팅 등에 대한 연구들을 기반으로 진화클라우드 컴퓨팅 환경에서의 정보보호해온 IT 서비스이다[1].

클라우드 컴퓨팅은 현재 IT분야에서는 분산된 서

* 남서울대학교 복지경영대학원 석사과정(주저자)
** 남서울대학교 산업보안학과 교수(교신저자)

버나 스토리지, 네트워크와 같은 인프라 자원과 PC나 모바일 기기들의 디바이스 자원들을 가상화나 그리드컴퓨팅 기술 등을 이용해 각 자원간의 구분을 없애고 언제 어디서나 효율적인 서비스를 이용할 수 있도록 하는 기술과 서비스가 특징이다[2].

클라우드 컴퓨팅 활성화 종합계획(2010)은 국내 클라우드 컴퓨팅 시장 활성화를 통해 2014년까지 국내 클라우드 컴퓨팅 시장을 2009년(6,739억원)의 4배인 2조5천억원 규모로 키우고, 세계시장 점유율을 10%까지 확대하는 등 세계 최고 수준의 클라우드 컴퓨팅 강국 도약을 정책목표로 설정하고 있다. 또한 주간기술동향(2013)은 국내 클라우드 컴퓨팅 시장 활성화를 통해 2014년까지 국내 클라우드 컴퓨팅 시장을 2009년(6,739억원)의 4배인 2조5천억원 규모로 키우고, 세계시장 점유율을 10%까지 확대하는 등 세계 최고 수준의 클라우드 컴퓨팅 강국 도약을 정책목표로 설정했다. 범정부 클라우드 컴퓨팅 활성화 종합계획(2009)는 국내 클라우드 컴퓨팅 시장 활성화를 통해 2014년까지 국내 클라우드컴퓨팅 시장을 2009년(6,739억원)의 4배인 2조5천억원 규모로 키우고, 세계시장 점유율을 10%까지 확대하는 등 세계 최고 수준의 클라우드 컴퓨팅 강국 도약을 정책목표로 설정했다.

최고 수준의 IT인프라를 활용하는 클라우드 컴퓨팅 서비스의 확산에 따라 스마트 폰을 활용하여 언제든지 원하는 서비스 요청이 가능하게 되었다. 그러나 이러한 최신 IT서비스의 이면에는 보안 위협이 존재한다. 클라우드 서비스를 통해 데이터 뿐 아니라 개인정보의 수집 및 활용 또한 용이해지면서, 개인정보 유출・노출 및 악용의 위험이 높아지고 있어, 이러한 사항을 고려한 클라우드 보안 방안이 필요하다. 클라우드 컴퓨팅 서비스 제공자가 개인정보보호에 대한 충분한 방안을 마련하고 시행할 수 있도록, 정부의 법제 마련 등 범국가적 지원이 필요한 상황이다. 따라서 클라우드컴퓨팅의 산업 활성화 방안과 실증연구가 거의 없는 실정이다.

최근까지 진행된 클라우드컴퓨팅 관련 연구들은 클라우드 도입사례와 클라우드 컴퓨팅 환경으로의 기존 시스템 이전에 관련한 방법론과 방안에 대해 연구하고 한계점이 있는 실정이다[3]. 또한 1994년부터 2012년까지 주요 해외 저널에 게재된 클라우드 컴퓨팅 관련 연구 논문들은 사회 네트워크 분석 척도를 활용하여 연구 논문간의 인용 관계와 동일 논문에 출현하는 키워드간의 관계로 중복되고 있는 실정이다[1].

또한 클라우드 컴퓨팅 서비스의 발전과 클라우드 환경에서의 개인정보보호 이슈와 클라우드컴퓨팅 서비스를 이용하는 서비스 이용자의 개인정보 안전성을 보장하고 서비스 제공자의 잠재적 개인정보 침해 위험을 줄일 수 있는 방향을 중심으로 이루어진 실정이다[4].

본 연구의 차별점은 이상의 논의를 바탕으로 크게 3가지로 구분된다. 첫째, 이용자 측면에서의 클라우드 컴퓨팅에 영향을 미치는 주요 요인들을 고찰하고, 클라우드컴퓨팅의 활성화 및 경쟁력 강화 방안에 대해 전략적인 제언하고자 한다. 둘째, 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률안을 통해 클라우드 산업활성화를 위한 지원 방안에 대해 제언하고자한다. 셋째, 클라우드컴퓨팅 서비스의 발전과 클라우드 환경에서의 개인정보보호 이슈를 정리해보고 클라우드컴퓨팅 서비스를 이용하는 서비스 이용자의 개인정보 안전성을 보장하고 서비스 제공자의 잠재적 개인정보 침해 위험을 줄일 수 있는 방향을 생각해 보고자 한다.

본 연구는 클라우드컴퓨팅 이용자들의 클라우드컴퓨팅 보안에서의 영향요인들에 대해 파악하고 이들 요인이 개인정보보호 행동에 영향을 미치는 요인들에 대한 인과관계를 실증 연구함으로써 클라우드컴퓨팅 보안에서의 효과적이고 효율적인 발전방안을

제시하고자 한다. 본 논문의 구성은 다음과 같다. 제Ⅱ장에서는 클라우드컴퓨팅의 정의와 특성 그리고 시장 현황을 정리하고, 기존 클라우드컴퓨팅 선행연구를 살펴본다. 제Ⅲ장에서는 클라우드컴퓨팅 산업 발전 동향에 대해 살펴본다. 제Ⅳ장에서는 개인정보보호 동향을 기술하였다. 제Ⅴ장에서는 클라우드컴퓨팅에서의 개인정보보호를 기술하였고, 마지막으로 제Ⅵ장에서는 연구결과 및 시사점, 향후 연구방향에 대해 논의하였다.

Ⅱ. 이론적 배경

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅이 과거의 네트워크 컴퓨팅, 유틸리티 컴퓨팅, 서버 기반 컴퓨팅, 그리드 컴퓨팅 등에 대한 연구들을 기반으로 진화클라우드 컴퓨팅 환경에서의 정보보호해온 IT 서비스이다[1]. 클라우드 컴퓨팅이 구성할 수 있게 만들어진 공유된 자원 풀에 편리하면서도 주문형으로 네트워크 접근을 할 수 있게 하는 모델이다.

클라우드 컴퓨팅은 공적 또는 사적 분야에서 사용사례, 기반 기술, 안건, 위험요소, 유용성 등에 대해 진화하고 있는 패러다임이다. 또한 클라우드 컴퓨팅은 산업에서 모델, 벤더, 시장적 요소가 결합된 거대한 생태학적 시스템이며 다양한 클라우드 방법들을 아무르는 형태를 띠며 필요한 관리는 용이해야 하며 서비스 제공자와 상호 대화가 최소화되어야 한다. 클라우드 컴퓨팅은 현재 IT분야에서는 분산된 서버나 스토리지, 네트워크와 같은 인프라 자원과 PC나 모바일 기기들의 디바이스 자원들을 가상화나 그리드컴퓨팅 기술 등을 이용해 각 자원간의 구분을 없애고 언제 어디서나 효율적인 서비스를 이용할 수 있도록 하는 기술과 서비스가 특징이다[2].

클라우드 컴퓨팅 서비스의 발전과 클라우드 환경에서의 개인정보보호 이슈와 클라우드컴퓨팅 서비스를 이용하는 서비스 이용자의 개인정보 안전성을 보장하고 서비스 제공자의 잠재적 개인정보 침해 위험을 줄일 수 있는 방향을 연구했다[4]. 사회교환이론을 연구의 이론적 프레임워크로 하여, 지각된 가치와 전환의도와의 관계를 실증적으로 분석하였다[5]. Value-based adoption Model(VAM)를 기반으로 클라우드 컴퓨팅 서비스 도입의도에 관한 프레임워크를 제시했다[6]. 1994년부터 2012년까지 주요 해외 저널에 게재된 클라우드 컴퓨팅 관련 연구 논문들의 서지정보 및 인용정보를 수집하였으며, 사회 네트워크 분석 척도를 활용하여 연구 논문간의 인용 관계와 동일 논문에 출현하는 키워드간의 관계로부터 연구 주제들간 네트워크 변화를 분석하였다[1]. 이를 통해서 클라우드 컴퓨팅 관련 분야의 연구 주제들간의 관계를 파악할 수 있었고, 클라우드 컴퓨팅에 대한 연구 동향 맵(research trend map)을 작성하여, 클라우드 컴퓨팅과 관련된 연구 주제들의 동태적인 변화를 확인하였다. 클라우드 컴퓨팅은 큰 값을 저장할 수 있는 장치로 감지된 보안, 감지된 프라이버시, 감지된 향락과 감지된 상호 작용성을 통해 클라우드 컴퓨팅 환경에서의 보안위협으로부터 개체 사이의 정보를 교환하는 본질적인 통신이다[7]. 클라우드 도입사례와 클라우드 컴퓨팅 환경으로의 기존 시스템 이전에 관련한 방법론과 방안에 대해 연구하고 한계점을 도출하고 클라우드 컴퓨팅을 위한 기존 시스템의 현대화에 대해 방안을 제시했다[3]. 클라우드 컴퓨팅 서비스를 사용화함에 있어서 보안문제가 가장 중요한 전제가 되며 동시에 내부의 중요한 데이터가 외부의 네트워크와의 연결 위에서 유출되거나 노출될 위험을 안고 있는 것이라고 제시했다[8]. 클라우드서비스에 대한 보안 요구사항이 개인사용자와 기업 사용자에 따라 다르며,

개인 사용자는 익명성 보장에 중점을 두는 반면에 기업사용자는 컴플라이언스에 중점을 둔다[9]. 클라우드는 기존 IT 환경의 보안 위협을 그대로 상속하고, 클라우드 특성에 따른 가상화, 다중임차, 원격지에 정보위탁, 사업자 종속, 모바일 기기접속 등, 신규 공격 위협이 존재한다. 이에 따라 클라우드 컴퓨팅에서 발생할 수 있는 개인정보위협에 대하여 보안취약점 노출과 관련해 정보를 암호화하기 위해 주요 문제와 제기된 정보를 알아보도록 하고자 한다[10].

2.2 개인정보보호관리체계(PIMS)

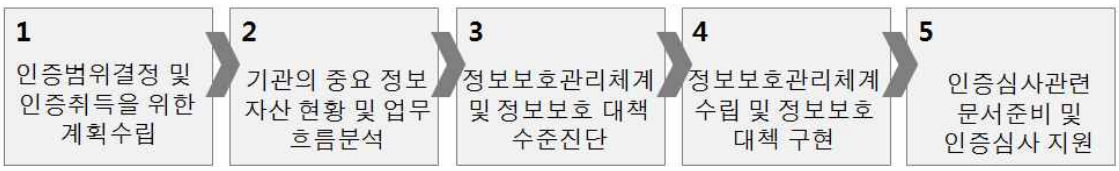
개인정보보호 관리체계(PIMS: Personal Information/privacy Management System)는 개인정보에 특화해 기업이 고객들의 개인정보를 보호 활동을 지속적이고 체계적으로 수행하기 위한 체계를 지칭한다[11]. 또한 PIMS는 방송통신위원회에서 민간사업자를 대상으로 사업자가 개인정보를 안전하게 보호할 수 있는 환경조성하고 이를 검증받을 수 있는 인증 제도이다[12].

<그림 1>과 같은 프레임 워크에 따라 다섯 단계로 나뉘어져 실행되고 있다. PIMS의 프레임워크를 살펴보자면 명확한 목표를 정하고 전략을 세우는 계획 수립단계, 수립된 계획을 실행하는 단계, 수립 결과를 계획에 대비하여 검토하는 단계, 검토 결과를 차기 계획에 반영하는 단계로 구성이 되고 이 단계를 지속적으로 반복하게 된다. 특히 개인정보보호를 목표로 할 경우에 이 과정은 정책을 수립하고 조직을 구성한 후, 침해위험 분석에 따른 보호 대책 적용 계획을 수립하는 침해위험관리 과정을 거쳐 개인정보 관리계획에 따른 대책구현 및 운영, 이후 검토와 모니터링을 포함하는 사후관리로 이루어지게 된다.

2011년부터 개인정보보호 관리체계(PIMS)를 시행하고, 심사를 통해 신청기업이 개인정보보호를 위해 일정수준 이상의 관리적·기술적·물리적 대책을 수립 및 운영하고 있을 경우 인증을 부여하고 있다[13]. 이에 따라 이용자 및 정보주체는 해당 기관의 인증취득 여부를 통해 개인정보의 누출가능성을 최소화하고 효과적으로 보호하고 있음을 갈음하는 수단이 되고 있다.

인증을 획득하는 기업은 개인정보 수집·이용·보유·제공·파기 등 전체 라이프사이클 전 과정에서 개인정보에 대한 안전성과 신뢰성 및 이용자 권리보호를 위한 전사적인 활동을 323개의 평가항목을 통해 공인 받게 된다[14]. 개인정보 보호 활동을 체계적이고 지속적으로 수행하기 위한 개인정보보호 유관 법적 요구사항을 기반으로 전사적인 기술적·관리적 요구사항을 제시하고 한다[15].

보안관제 운영감리는 정보보호 및 개인정보보호에 있어서 위험을 사전에 분석하여 보안 사고를 줄이고, 보안사고 발생 시 내부정보유출 위험관리와 기술적 보호를 확보하고자 하는 것으로 새로운 프레임워크를 만들었으며 또한 ISO 27001, ISMS, PIMS 등에서 추출한 운영감리 관련 항목과 기타 관련 선행연구를 토대



<그림 1> PIMS 프레임워크

로 “정보보호정책”, “정보보호 교육 및 훈련분야”, “인적보안”, “접근통제”, “운영관리”, “보안사고 관리”에 대한 보안관제 운영감리지침 과 점검항목에 대해 분류 및 도출하였다. 점검항목의 사업유형은 ITIL을 기준으로 “서비스 운영(Service Operation)”, “서비스 유지보수(Service Maintenance)”, “서비스 재개발(Service Redevelop)”으로 분류하여 효율적으로 이루어지도록 연구하였다. 정보보호관리체계와 개인정보보호 관리체계의 주요 특성을 살펴보고, 두 체계 간의 유사점과 차이점을 식별하며, 개인정보관리체계의 운영을 위한 국제 표준 구성 요소를 제시 했다[11]. 국내 PIMS 도입에 예상되는 기존 ISMS, ePrivacy, PIA제도와의 중복성을 연구하고, 중복성 해소방안을 제시하여 이를 위해 중복성 개념을 고찰하고, 제도적 중복과 방법론적 중복의 개념을 바탕으로 ISMS와 PIMS 인증제도간의 중복성을 평가하였다[16]. 정보시스템 감리 해설서를 기준으로 정보보호관리체계(ISMS) 및 개인정보보호관리체계(PIMS)를 비교하여 본 감리모델을 제안하며 ITIL(Information Technology Infrastructure Library) 및 Cobit(Control Objectives for Information and Related Technology)을 참고하여 연구하였다.

Ⅲ. PIMS기반의 클라우드 컴퓨팅 환경에서의 개인정보보호 조치 개선안

3.1 클라우드컴퓨팅 환경에서의 개인정보보호 개선의 필요성과 영역의 정의

3.1.1 클라우드컴퓨팅 환경에서의 개인정보보호 개선의 필요성

클라우드 컴퓨팅 서비스 이용자는 물리적 IT인프라를 보유하지 않고 서비스 제공자로부터 IT인프라를 임대하여 사용하고, 원격의 서버에 중앙 집중식으로 데이터를 저장하게 되어 분산된 컴퓨터 환경에 비하여 효율적으로 정보 접속에 대한 모니터링을 실시할 수 있다. 또한, 가상화 기술을 이용하여 데이터 복구 및 시스템 교체 작업을 쉽고 빠르게 수행할 수 있다. 보안 사고, 재해 발생시 유형과 피해의 규모에 따라 국가적·사회적 파급효과가 크기 때문에, 그 중요도 측면에서 적절히 관리되고 통제되어야 한다.

한국인터넷진흥원에서는 체계적이고 지속적인 관리체계를 구축할 수 있는 개인정보 관리체계 수립을 위한 인증심사 항목은 관리과정, 보호대책 및 생명주기의 총 3가지 통제분야와 16개의 통제 내용, 40개의 통제 목적, 124개의 통제항목, 310개의 점검항목으로 구성되어 있으며, 많은 기업들이 제공된 지침 기준에 맞춰 관리과정 요구사항, 보호대책 요구사항, 생명주기등 개인정보 보호를 지속적 체계적으로 수행하기 위해 개인정보와 관련된 위험을 평가하고 그 위험을 예방하기 위한 대책을 수립하여 클라우드 컴퓨팅의 구성 요소를 보호하고 있다[17].

개인정보보호 활동의 일환으로 PIMS 통제 항목을 참조하여 공공 및 민간분야에서의 클라우드 서비스가 적용되면서, 클라우드 서비스로 인한 시장 성장과 순기능적 측면만을 강조할 수는 없다. 실제도 클라우드 서비스가 확대되면서, 시스템의 장애 및 오류, 내부자의 정보유출 및 관리 소홀 등으로 인한 개인정보 침해사고에 따른 성능의 저하 및 요인이 될 수 있다.

클라우드 컴퓨팅은 개인정보를 클라우드 환경에서 수집, 저장, 처리 및 이용되는 모든 정보를 의미하며 개인정보 처리과정에서 새롭게 생성되는 모든 정보를 포함한다. 클라우드 컴퓨팅 환경에서는 서비스 제공자와 이용자 간 정보 주체 및 소유에 따라 개인정보보호의 범위를 합리적으로 규정하여 통제 절차를 수립하여 보안 정책 수립 시 참고가 될 수 있도록 개인정보보호 지침의 개선이 필요하다.

클라우드 컴퓨팅은 원격의 서버에 중앙 집중식으로 데이터를 저장하게 되어 분산된 컴퓨터 환경에 비하여 효율적으로 정보 접속에 대한 모니터링을 실시할 수 있다. 또한 가상화 기술을 이용하여 데이터 복구 및 시스템 교체작업을 쉽고 빠르게 수행할 수 있으며 새로운 보안 위협에 대하여 대응 방안을 쉽게 적용할 수 있는 등 많은 장점과 탄력성(elasticity), 빠른 적용과 릴리즈, 광대역 네트워크 접속, 다중 접속(multi-tenancy), 활용에 제한이 없는(ubiquity) 유연성 등 클라우드 컴퓨팅의 고유한 속성들은 클라우드를 선택한 기업과 기관에게 획기적인 효율성을 제공하지만 원천적으로 내재된 보안 위협을 제거해야 하는 대책수립이 필요하다. 클라우드 컴퓨팅을 이용하는 이용자들이 개인정보자기결정권을 보장하고 서비스 제공자의 잠재적 개인정보보호 업무 위험을 줄이기 위한 고려사항을 살펴보고 이에 대한 절차와 대응방안에 대한 내용을 지침화할 필요가 있다.

저장 데이터에 대한 접근 통제 및 처리방침 클라우드 컴퓨팅 이용자의 개인정보 또는 기밀정보를 보호하기 위하여 데이터에 임의로 접근하여서는 안된다. 따라서 이용자 개인정보보호를 위하여 이용자 데이터 접근 범위와 접근 시 이력을 기록하도록 하는 내용을 계약에 명시하고 클라우드 컴퓨팅 이용자가 민감한 정보와 개인정보를 접근하는 통제 절차와 방법을 구체적으로 제시하는 것을 좀 더 중요하게 생각하였다. 또한 클라우드 컴퓨팅 형태에 따라 개별 데이터 보관 주기를 준수하기 위하여 구체적인 데이터 보존 절차를 명시하고 이에 대한 배상의 책임을 명시하는 것이 필요하게 되었다[18-20].

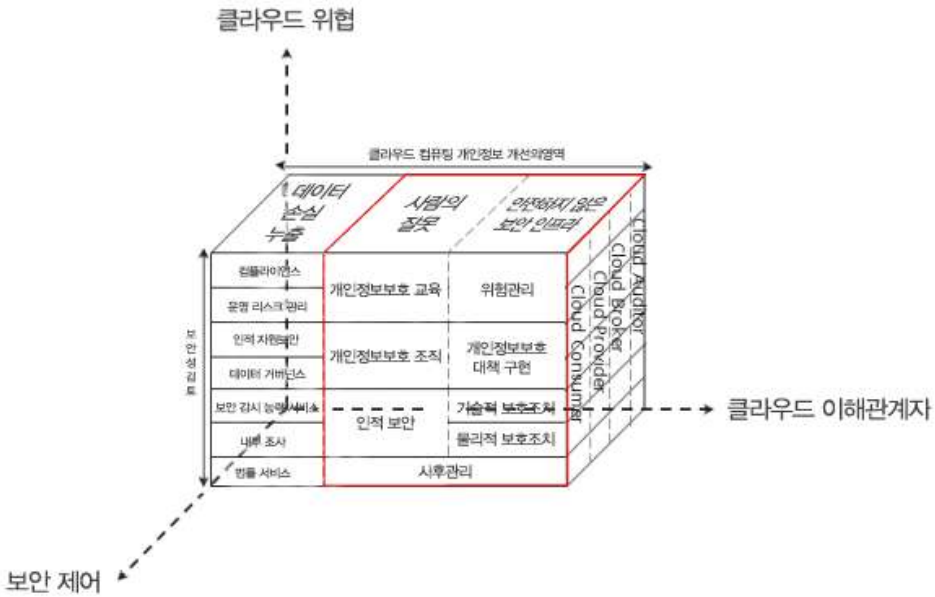
3.1.2. 클라우드컴퓨팅 환경에서의 개인정보보호 개선 영역

개인정보 프레임워크가 조직에서 효과적으로 작용하기 위해서는 비즈니스 및 보안과의 전략적 연계가 필수적인 요소다. 개인정보 수준만을 강조한 개인정보 프레임워크는 효율성을 강조하는 보안과 대립하게 되며 결과적으로 비즈니스 성과를 저하하게 된다.

그렇기 때문에 비즈니스 및 보안과의 조화로운 개인정보 프레임워크를 정의하기 위해 전략 연계 모형에 개인정보보호 요건을 투영하여 클라우드 컴퓨팅 개인정보 프레임워크를 정의하였다. Henderson, J. and N.Venkaraman은 전략연계 모형을 설명하기 위해 다음과 같은 3개 요소를 축으로 보안 활동을 투영하였다. 클라우드로써 전략 연계 모델을 활용하기 위해 클라우드 컴퓨팅을 주요 보안활동으로 간주하였으며 목적, 프로세스 및 주체는 전략 연계모형의 원론적인 의미를 반영하여 개인정보 관점에서 고려되는 부분으로 본 논문에서는 2장 선행연구를 통해 전략 연계 모델에 기반하여 “목적”은 클라우드 위협으로 “프로세스”는 보안통제 활동으로 “주체”는 클라우드 이해관계자로 구분하였다.

또한 클라우드 위협, 보안통제 활동 및 클라우드 이해관계자에는 개별 축을 정의하기 위한 세부 구성요소가 존재했으며 클라우드 컴퓨팅의 개인정보 보안 지침 갸선의 영역을 그린 클라우드 컴퓨팅 보안 구성 요소 중 사람의 잘못과 안전하지 않은 보안 인프라의 운영으로 범위를 정하였다. 그리고 PIMS의 개인정보 대책의 관리과정, 보호대책 및 생명주기의 총 3가지 통제분야와 16개의 통제 내용, 40개의 통제목적, 124개의 통제항목, 310개의 점검항목으로 검토하고, 클라우드 컴퓨팅의 지향성을 고려하여 새로운 항목을 추가 하였다.

클라우드 컴퓨팅의 경우 PIMS 통제항목 중 관리과정, 보호대책 항목에 운영에 대한 부분을 다루고 있기 때문에 관리 및 보호를 이용한 클라우드 컴퓨팅의 개인정보 개선 시 고려해 볼 수 있는 점검 항목에 대해 따로 정리하였다[21-23]. 특히, 이용자의 개인정보를 안전하게 보호할 수 있도록 기술적·관리적·물리적



<그림 2>클라우드 컴퓨팅 개인정보보호 조치 개선 점검 프레임워크

조직적인 다양한 보호 대책들을 구현하고 지속해서 관리 운영을중심으로 점검항목을 사용하였으며, 일정 수준 이상의 개인정보 관리과정, 보호대책, 생명주기를 제고하여 지속적으로 유지할 수 있도록 점검항목을 도출 하였다[24-25].

3.2 PIMS기반의 개인정보보호 보안지침 개선 항목

3.2.1 개인정보 보안지침 개선 항목

PIMS(개인정보보호 관리체계) 인증심사 기준은 개인정보 관리과정, 생명주기 및 권리보장, 보호대책 3개 분야로 이루어져 있다. PIMS의 구성요소로 첫째, 관리과정 요구사항은 개인정보보호를 체계적이면서 주기적으로 수행하고 있는지에 대한 여부를 점검하는 항목이라고 할 수 있다. 둘째, 보호대책 요구사항은 개인정보를 안전하게 보호하기 위한 관리적, 물리적, 기술적 보호조치를 점검하는 항목이다. 셋째, 생명주기 요구사항은 생명주기 관리와 정보주체의 권리보장의 법률 준수여부를 점검하는 항목을 말한다.

(1) 위험관리의 점검항목

위험관리는 신청사업자의 목표 및 정책, 법적 요구사항 등을 고려하여 조직, 역할, 책임, 주요과정을 포함한 클라우드 컴퓨팅 위험관리 계획을 수립하고, 신청기관에 적합한 위험관리 방법을 선택하여야 한다. 이 위험관리 방법은 클라우드 컴퓨팅의 조직과 개인정보보호 환경변화에 대응할 수 있도록 지속적으로 검토하여야 한다. 위험관리 계획은 신청사업자의 목표 및 정책, 법적요구사항 등을 고려하여 작성되어야 한다.

위험관리 계획은 신청사업자의 목표 및 정책, 법적 요구사항 등을 고려하여 작성되어야 한다. 첫째, 클라

우드 컴퓨팅 위험관리 방법론은 상세위험분석접근법, 베이스라인접근법(Baseline approach) 등 있다. 둘째, 클라우드 컴퓨팅 위험관리 방법론은 사업자(신청기관) 업종유형, 개인정보취급서비스 종류, 조직구조 등에 따라 사업자가 선택할 수 있다. 이와 관련하여 PIMS에서는 3개의 통제항목과 7개의 세부 점검 항목을 제시하고 있다. 제시된 항목은 큰 차이점 없이 클라우드 컴퓨팅 운영에도 적용 할 수 있기 때문에 따로 새로운 항목을 도출지 않았다.

(2) 개인정보보호 대책 구현의 점검항목

개인정보보호대책의 클라우드 컴퓨팅의 이행계획에 따라 보호대책을 구현하고, 대책의 효과성에 대하여 주기적인 검토를 수행하여야 한다. 또한 클라우드 컴퓨팅 환경에서 발생할 수 있는 보안 문제로 인해 개인정보보호대책의 이행계획에 따라 대책을 구현하여야 한다. 구현 후 검토 계획에 따라 일정 시간이 흐른 후 구현 성과를 검토 및 보고 하여야 한다. 따라서 기존 PIMS 통제분야에서 개인정보 보호 대책 구현 항목 중 보호대책의 효과적 구현 항목의 세부 점검 항목에 “클라우드 컴퓨팅 유형별 개인정보보호 대책”에 대한 1개의 항목을 추가 하였다. 개인정보보호대책의 이행계획에 따라 클라우드 컴퓨팅 보호대책이 일관성 있게 구현되어야 하며, 구현 여부 및 변경관리 내역이 문서화 되어 있어야 하기 때문이다.

(3) 사후관리의 점검항목

<표 1> 요구사항과 액터 및 유스케이스와의 할당 테이블

통제분야	통제내용	통제 목적 수	통제 항목 수	사용 여부	통제항목 / 세부점검항목
관리과정	1. 개인정보보호 정책 수립 및 범위설정	1	3		7
	2. 경영진의 책임 및 조직 구성	1	2		4
	3. 위험관리	**1**	**3**	**사용**	**3/7**
	4. 개인정보보호 대책 구현	**1**	**1**	**사용**	**1/2**
	5. 사후 관리	**1**	**2**	**사용**	**2/4**
소계		5	13		28
보호대책	1. 정보보호정책	3	6		13
	2. 개인정보보호 조직	**2**	**4**	**사용**	**4/8**
	3. 개인정보보호 분류	2	2		6
	4. 개인정보보호 교육	**2**	**4**	**사용**	**4/7**
	5. 인적보안	**1**	**3**	**사용**	**3/9**
	6. 침해사고관리	3	7		13
	7. 기술적 보호조치	**8**	**9**	**사용**	**9/24**
	8. 물리적 보호조치	**3**	**9**	**사용**	**9/20**
소 계		26	79		
생명주기	1. 개인정보 수집에 따른 조치	3	10		20
	2. 이용 및 제공에 따른 조치	5	16		46
	3. 개인정보 관리 및 파기에 따른 조치	1	6		16
소계		9	32		84
합계		40	124		310

클라우드 컴퓨팅에 대한 지속적인 개선활동이 문서화되고, 정기적으로 재검토하여야 한다. 또한 클라우드 컴퓨팅의 지속적으로 모니터링되어 클라우드 컴퓨팅의 법적 요건 및 개인정보보호정책과 조직의 목적과의 일치성을 만족시켜야 한다. 교정 및 사전 대책이 구현되어야 하며 그 결과가 평가되어야 지속적인 개선활동이 이루어질 수 있다. 특히 개인정보보호 관련 클라우드 컴퓨팅의 대내외 환경변화가 조직에 미치는 영향을 분석하고, 이행점검 결과, 보안사고의 영향 등을 반영할 수 있는 클라우드 컴퓨팅에 관련하여 재검토 절차가 수립되어야 한다. 이와 관련하여 PIMS에서는 2개의 통제항목과 4개의 세부 점검

<표 2> 위험관리의 보안점검 항목

통제분야	통제항목	점검항목	비 고
위험관리	위험관리 계획 수립	신청사업자의 목표 및 정책, 법적 요구사항 등을 고려하여 위험관리 계획을 수립하는 절차가 있는가?	
		위험관리 방법은 환경변화에 대응할 수 있도록 지속적인 검토가 이루어지고 있는가?	
	위험평가	수립된 위험관리계획에 따라 위험평가를 수행하고 있는가?	
		개인정보침해사고의 방지가 가능한 합리적인 목표 위험수준을 설정하였는가?	
	위험관리를 위한 보호대책 및 이행계획 수립	위험관리 계획에 따른 보호대책이 선정되었는가?	
		책임, 예산, 일정, 운영 계획 등이 포함된 위험관리를 위한 보호대책의 이행계획이 적절하게 수립되었는가?	
		위험관리를 위한 보호대책의 이행계획에 대한 최고경영자 또는 CPO의 승인이 있는가?	

<표 3> 개인정보보호 대책 구현의 보안점검 항목

통제분야	통제항목	점검항목	비고
개인정보보호 대책 구현	보호대책의 효과적 구현	개인정보보호대책의 이행계획에 따라 보호대책이 구현 되었는가?	
		구현된 보호대책의 정확성 및 효과성을 검토하였는가?	
		클라우드 컴퓨팅 유형별 개인정보보호 정책 지침 관리계획을 구현 및 검토하고 있는가?	추가

<표 4> 사후관리의 보안점검 항목

통제분야	통제항목	점검항목	비고
사후관리	모니터링 및 개선	신청사업자의 개인정보보호정책과 목적을 충족시키기위해 개인정보보호와 관련한 법적 요건 및 환경변화에 대해 지속적인 모니터링 활동을 수행하고 있는가?	
		모니터링 결과에 따른 교정 및 사전 대책이 마련되어 구현되었으며, 그 결과가 평가되고 있는가?	
	개인정보보호관리체계의 재검토	공식적이고 정기적인 개인정보보호관리체계의 재검토를 위한 절차 또는 규정이 존재하는가?	
		개인정보보호관리체계의 재검토시 개인정보의 효율성, 범위의 적절성, 수준 등에 대하여 다음의 내용을 고려하고 있는가? - 개인정보의 내용 및 흐름 - 적용 기술상의 내 외부의 변화 - 내부이행점검 결과 - 모니터링 결과	

항목을 제시하고 있다. 제시된 항목은 큰 차이점 없이 클라우드 컴퓨팅 운영에도 적용 할 수 있기 때문에 따로 새로운 항목을 도출 하지 않았다.

(4) 개인정보보호 조직의 점검항목

개인정보보호 조직체계를 구성하여 클라우드 컴퓨팅환경에서의 보안문제가 발생했을 때 개인정보관리책임자 및 개인정보 취급부서별 책임자, 담당자를 지정하여야 한다. 개인정보보호활동에 대한 경영층의 명확한 지원 및 방향제시를 보증할 수 있는 조직을 구성하여야 한다. 또한 개인정보보호관리 활동을 수행하고 검증하는 인력들에 대한 책임, 권한 및 상호 연관관계를 정의하고 문서화하여야 한다. 상시 종업원 수가 5명 미만인 정보통신서비스 제공자등의 경우에는 지정하지 않을 수 있다. 이 경우에는 그 사업주 또는 대표

<표 5> 개인정보보호 조직의 보안점검 항목

통제분야	통제항목	점검항목	비고
개인정보보호조직	개인정보보호 조직체계 구성	조직 내 개인정보보호 업무를 수행하기 위한 내부조직체계가 구축되어 있는가?	
	개인정보관리책임자(CPO) 지정	이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보관리책임자가 지정되었는가?	
		개인정보 취급부서별 책임자 및 담당자를 지정하고 있는가?	
		클라우드 컴퓨팅 서비스 사용 조직의 보안책임자 지정하였는가?	추가
	역할 및 책임	개인정보관리책임자 지정 시 최고경영자가 승인하였는가?	
		개인정보관리책임자의 개인정보보호에 관한 역할 및 책임이 정의되었는가?	
		개인정보 취급부서의 책임이 명시되고 개인정보 취급부서별 책임자 및 관리 담당자의 역할 및 책임을 정의하였는가?	
		개인정보취급자의 개인정보보호에 관한 역할과 책임 및 권한이 정의되었는가?	
	보고 및 의사소통체계	개인정보관리책임자와 각 부서별 책임자 및 담당자와 의사소통할 수 있는 보고라인, 방법 및 역할과 책임이 정의되어 있는가?	

<표 6> 개인정보보호 교육의 보안점검 항목

통제분야	통제항목	점검항목	비고
교육 및 훈련	교육 및 훈련 대상	교육・훈련의 대상은 개인정보관리책임자(CPO), 개인정보 취급자 및 개인정보취급부서 책임자 및 관리 담당자 등을 포함하고 있는가?	
		조직이 보유한 개인정보를 공유, 제공 받거나 접근 권한을 부여받은 외부 직원에 대한 교육훈련을 제공 하는가?	
	교육 및 훈련내용	교육내용은 개인정보보호 관련 법률 및 제도, 사내 규정 ,관리적 기술적 조치사항 및 이를 수행하기 위한 방법 등 개인정보취급자가 필수적으로 알아야 하는 사항을 포함하는가?	
		개인정보보호 교육시 교육대상자의 직위 및 담당하는 업무의 특성에 따라 교육 내용을 차별화하여 적합한 교육을 실시하고 있는가?	
		클라우드 컴퓨팅에 대한 기술적/관리적 보호조치 교육을 실시하고 있는가?	추가
	교육 및 훈련 시행	교육 및 훈련이 계획에 따라 년2회 이상 시행되고, 이에 대한 기록을 유지 하는가?	
		교육 및 훈련은 개인정보보호정책의 절차 및 역할 변경이 있는 경우에 실시하고, 이에 대한 기록을 유지 하는가?	
	교육 및 훈련 평가	교육 훈련의 효과를 측정, 분석하여 다음의 교육계획에 반영되고 있는가?	

자가 개인정보관리책임자가 된다.

(인터넷으로 정보통신서비스를 제공하는 것을 주된 업으로 하는 정보통신서비스 제공자등의 경우에는 상시 종업원 수가 5명 미만으로서 전년도 말 기준으로 직전 3개월간의 일일평균이용자가 1천명 이하인 자를 말함) 개인정보관리 활동을 계획, 관리하는 개인정보관리책임자는 충분한 권한을 가진 임원급 또는 개인정보와 관련하여 클라우드 컴퓨팅 이용자의 고충처리를 처리할 수 있는 부서장이어야만 의사 결정에 따른 시행이 이루어질 수 있다. 따라서 기존 PIMS 통제분야에서 개인정보보호 조직 항목 중 개인정보관리책임자(CPO)지정 항목의 세부 점검 항목에 "클라우드 컴퓨팅 사용 조직의 보안 책임자" 에 대한 1개의 항목을 추가 하였다. 클라우드 컴퓨팅 이용자의 개인정보를 보호하고 클라우드 컴퓨팅과 관련한 이용자의 고충을 처리하기 위하여 클라우드 컴퓨팅책임자를 지정하여야 한다.

(5) 개인정보보호 교육의 점검항목

클라우드 컴퓨팅에서 발생할 수 있는 보안교육·훈련 계획을 수립하고, 관련자 모두에게 개인정보취급자가 필수적으로 알아야 하는 사항을 교육하여야 한다. 보안 지침 교육·훈련은 개인정보책임자(CPO), 개인정보관리자가 주체가 되며, 개인정보 취급자, 개인정보취급부서 책임자 및 관리 담당자 등을 대상으로 한다. 따라서, 개인정보책임자(CPO)와 개인정보관리자에 대한 차별화된 교육이 별도로 존재하는지 확

<표 7> 인적보안의 보안점검 항목

통제분야	통제항목	점검항목	비고
인적보안	개인정보취급자 감독	업무상 개인정보를 취급해야 하는 사람들을 최소한으로 제한하고 있는가?	
		클라우드 컴퓨팅 환경에 접근하는 개인정보취급자 최소한으로 제한하고 있는가?	추가
		개인정보 취급자 명단을 관리하고 있는가?	
		개인정보취급자의 업무 수행 시 적격심사를 진행하고 있는가?	
		클라우드 컴퓨팅 서비스 제공에 따른 외부자 보안대책 수립·시행하고 있는가?	추가
		클라우드 컴퓨팅 서비스 계약·서비스수준협약을 통한 외부자 보안을 실시하고 있는가 ?	추가
		개인정보취급자가 다수일 경우, 개인정보 취급자를 관리할 수 있는 부서별 책임자 및 담당자를 지정하고 적절한 관리·감독 방안을 마련하는가?	
	인사규정	인사규정 또는 채용계약서 등에 개인정보취급자가 직무상 취득한 개인정보를 훼손·침해 또는 누설하는 경우 관계법령상의 책임 및 처벌규정에 대해 명시하고 있는가?	
		개인정보취급자의 퇴직 및 직무변동 시, 인사부서와 개인정보 관련부서 간에 상호 공지가 이루어지는가?	
		클라우드 컴퓨팅 서비스 제공에 따른 내부 책임 및 역할 구분하고 있는가? 예)서비스의 적합성,비밀유지(서약서),징계처분절차 등	추가
	개인정보보호 서약	내부직원(정규직/계약직/임시직)의 개인정보 취급 업무 시작 시 개인정보보호에 관한 책임 및 의무를 고지한 개인정보보호서약서를 징구하는가?	
		제3자등 외부 인원에게 개인정보처리시스템 접근권한을 부여하는 경우 개인정보보호에 관련된 사항이 계약서에 포함되어 있으며, 개인정보를 취급하는 인원에 대해서는 개인정보보호 서약서를 받는가?	
		직원 고용조건 변경 및 퇴사 시에 개인정보보호서약서를 재작성하고 책임사항을 주지시키고 있는가?	

인하여야 한다. 수탁자나 제3자 등 개인정보를 공유, 제공, 접근할 수 있는 모든 인력이 클라우드 컴퓨팅에 대한 의무사항을 인식할 수 있도록 보장하여야 한다. 교육내용은 관련 법률, 규제, 사내규정, 보호조치 방법 등을 포함해야 하며, 특히 개인정보취급자가 클라우드 컴퓨팅 이용자의 개인정보를 유출할 경우에는 중벌에 처해진다는 사실을 주지시키는 것은 개인정보보호책임자의 의무이므로 이러한 사항을 교육 내용에 포함해야 한다. 따라서 기존 PIMS 통제분야에서 개인정보보호 교육 항목 중 교육 및 훈련내용 항목의 세부 점검 항목에 “클라우드 컴퓨팅 기술적/관리적 교육” 에 대한 1개의 항목을 추가 하였다. 클라우드 컴퓨팅의 전반적인 기술적/ 관리적 요구사항 및 중요성, 관련 법규 및 개인의 보안책임에 관한 교육을 받아야 하기 때문이다.

(6) 인적보안의 점검항목

개인정보취급자는 최소한으로 제한하고 개인정보취급자 명단 관리 및 책임명시, 처벌규정을 마련하여야 한다. 클라우드 컴퓨팅시스템에 대한 접근권한은 개인정보관리책임자, 개인정보취급자를 대상으로 최소한으로 부여하여야 한다. 계약직 및 임시직원은 물론 정식직원이 개인정보 취급 관련 클라우드 컴퓨팅을 사용 시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어져야 한다. 따라서 기존 PIMS 통제분야에서 인적보안 항목 중 개인정보취급자 감독 항목의 세부 점검 항목에 “클라우드 컴퓨팅 접근의 최소화”, “외부자 보안 대책”, “계약/서비스수준협약 보안” 에 대한 3개의 항목을 추가 하였다. 개인정보취급자가 다수일 경우 부서별 책임자 및 담당자접근을 최소화하도록 해야하며 작업장 내 업무 감독, 일일 작업 기록 검토, 월간 작업 기록 검토, 작업 사전 승인 등의 적절한 관리・감독 방안을 마련하여야 하기 때문이다. 또한 인사규정 항목의 세부 점검 항목에 “클라우드 컴퓨팅 책임 및 역할 구분” 대한 1개의 항목을 추가 하였다. 인사규정 또는 채용계약서 등에는 클라우드 컴퓨팅을 이용한 개인정보취급자가 개인정보를 유출한 경우에 대한 법적책임 등 개인정보에 대한 임직원 및 개인정보취급자에 대한 책임 및 처벌 규정을 확실하게 포함되어야 한다.

(7) 기술적 보호조치의 점검항목

클라우드 컴퓨팅 접근통제 정책을 수립하고, 개인정보취급자의 접근통제 및 모니터링을 이행하여야 한다. 클라우드 컴퓨팅 업무 요구사항에 기초하여 논리적, 물리적, 네트워크 접근을 관리하기 위한 통합적인 접근통제 정책이 문서화되어야 하며 이와 관련하여 PIMS에서는 9개의 통제항목과 25개의 세부 점검 항목을 제시하고 있다. 제시된 항목은 큰 차이점 없이 클라우드 컴퓨팅 운영에도 적용 할 수 있기 때문에 따로 새로운 항목을 도출하지 않았다.

(8) 물리적 보호조치의 점검항목

개인정보를 취급하는 공간에 대해 클라우드 컴퓨팅 출입통제 등 물리적 보호조치를 취하고 접근가능한 인원은 허가받은 인력에 한해 최소화하여야 하며 클라우드 컴퓨팅을 통한 개인정보처리 및 저장시설, 장비, 사무실, 보관소 등을 보호하기 위한 보호 구역을 정의하고 보호구역에 대한 물리적 접근을 통제하기 위한 대책을 마련해야 한다. 장비 유지보수를 위한 반출입 시에도 개인정보를 삭제하거나 암호화하여 이를 통한 개인정보유출이 발생하지 않도록 하여야 한다. 이와 관련하여 PIMS에서는 9개의 통제항목과 21개의 세부 점검 항목을 제시하고 있다. 제시된 항목은 큰 차이점 없이 클라우드 컴퓨팅 운영에도 적용 할 수 있기 때문

<표 8> 기술적 보호조치의 보안점검 항목

통제분야	통제항목	점검항목	비고
기술적 보호조치	개인정보취급자 권한관리	개인정보 취급자 등록 및 해지를 위한 문서화된 계정관리 절차를 마련하고 수행하고 있는가?	
		개인정보취급자 계정은 유일한 식별자를 가지고 식별자는 적절한 명명규칙을 따르고 있는가?	
		개인정보 취급자 계정 생성 및 권한부여 절차가 적절히 직무분장 되어 있으며 사용자 권한 변경의 기록을 별도로 검토하고 있는가?	
	접근통제 정책 수립	개인정보보호 요구사항에 기초하여 개인정보처리시스템에 대한 접근통제 정책이 존재하는가?	
	네트워크 접근	다음을 포함하는 네트워크 접근정책이 수립되어 있고, 이에 따라 운영되고 있는가? - 접근통제 정책에 따라 인가된 사용자만이 네트워크에 연결할 수 있도록 함 - 사용자 터미날과 컴퓨터 서비스간에 물리적 및 논리적 경로의 통제 - 접근통제 정책에 따른 네트워크 라우팅 통제 - 원격 사용자의 적절한 인증 - 중요한 정보 서비스, 사용자 그룹, 시스템 그룹의 별도 분리 및 비인가자의 접근통제 대책 마련 등	
		외부업체에 의한 유지보수 작업 시 불법적인 네트워크 접근을 통해 개인정보가 노출되지 않도록 보안조치를 취하는가?	
	운영체제 접근	다음을 포함하는 개인정보처리시스템 운영체제 접근통제가 존재하며, 이에 따라 이행되고 있는가? - 개인정보처리시스템 대한 안전한 로그온 절차 - 식별 및 인증관리	
		개인정보처리시스템의 운영체제 접근통제가 다음의 사항을 포함하며 이에 따라 운영되고 있는가? - 터미널 자동확인 및 주요 터미널 통제 - 시스템 유틸리티 프로그램의 사용제한 - 중요 서비스의 연결시간을 업무시간 내로 제한 등	
	응용프로그램 접근	정보 및 응용 프로그램 기능의 접근이 개인정보 응용 프로그램 접근통제 정책에 따라 제한되는가?	
		개인정보를 처리하는 응용프로그램에서 권한에 따른 기능 및 메뉴만 제공하고 불필요한 기능을 통제하고 있는가	
		중요 정보 및 응용 프로그램 출력이 등급 및 전달자를 포함하여 출력되는가?	
	데이터베이스 접근	다음의 사항을 포함하는 데이터베이스 내의 개인정보보호를 위한 운영 절차가 있는가? - 데이터베이스 관리자 및 사용자의 식별 - 데이터 테이블 수준에서 사용자의 접근 권한을 명시 - 데이터사전 및 유틸리티에 대한 접근통제 명시	
	암호정책	문서화된 암호정책이 있는가?	
		암호정책은 암호화 대상 및 암호화 방법은 명확하게 정의하고 있는가?	
		암호정책은 법적 요건을 만족하고 있는가?	
	개발과 운영환경의 분리	개발 및 테스트 시스템이 운영시스템과 분리되어 있는가?	
		운영 및 테스트/개발 시스템에 대해 서로 다른 로그온 절차가 존재하는가?	
	네트워크 운영대책	다음과 같은 내용을 포함한 네트워크 운영절차 및 보안 정책이 수립되고 이행되는가? - 네트워크 분리 - 접근권한 통제 - 책임 및 직무분리 - 원격접속설비 관리	
		네트워크를 구성하는 주요 자산에 대한 목록 및 구성도를 유지하고 있는가?	
		개인정보 침해위험 관리를 통해 접근통제가 이루어지도록 네트워크가 물리적 또는 논리적인 영역으로 분리되어 있는가?	
		외부 사용자에게 서비스를 제공하는 네트워크는 내부 업무용 네트워크와 분리되는가?	
		외주개발업무에 사용되는 네트워크는 내부 운영 네트워크와 분리되는가?	
		내부망에서 사용하는 주소는 사설 IP주소를 사용하며 내부 IP주소체계는 외부로 유출되지 않도록 하고 있는가?	
		합법적인 승인 없이 네트워크 모니터링을 수행할 수 없도록 되어 있는가?	

에 따로 새로운 항목을 도출 하지 않았다.

Ⅳ. 개인정보관리체계 기반의 클라우드컴퓨팅 개인정보보호 보안 개선안 검증

개인정보관리체계를 기반으로 한 클라우드컴퓨팅 환경에서의 개인정보보호 보안 개선을 위해 본 논문에서는 개인정보관리체계의 점검 항목과 추가로 도출한 항목들의 적합성을 검증 하고자 한다. 이를 위해 클라우드컴퓨팅 사용 경험이 있는 조직구성원들을 대상으로 설문을 실시하였다.

4.1 설문조사 방법과 표본응답자 구성

4.1.1 설문조사 방법

설문기간은 2016년 6월 5일 ~ 2016년 8월 20일까지 설문을 위한 부가적인 설명과 함께 온라인으로 진행되었으며 총 32명이 응답하였다.

4.1.2 표본응답자 구성

설문조사 대상으로는 <표 9>과 같이 선정하였으며, 담당 업무는 보안(40.62%), 교육/정책(15.62%), 운영/개발(15.62%), 기타(15.62%), 경영/관리(9.38%), 영업(3.12%)으로 구성되었다.

<표 9> 표본 응답자의 구성

구분	보안	보안	영업	경영/관리	교육/정책	영업
비율	12명 (28.57%)	10명 (23.81)	6명 (14.29%)	6명 (14.29%)	5명 (11.9%)	1명 (3.12%)

4.2 설문결과

4.2.1 표본집단의 특성에 관한 설문 결과

(1) 응답자의 현 직무 경력에 대한 설문결과

설문 응답자의 직무경력에 대한 질문은 3년 이하, 3년 이상~7년 이하, 7년 이상~10년 이하, 10년 이상~15년 이하, 15년 이상으로 구분하였고 다음 <표 10>와 같이 응답 하였다. 또한 설문 응답자의 개인(정보)보호 경력에 대한 질문은 없음, 3년 미만, 3~5년 미만, 5~10년 미만, 10년 이상으로 구분하였으며 다음 <표 11>와 같이 응답 하였다.

<표 10> 설문 응답자의 직무 경력

구분	3년 이하	3년 이상 ~ 7년 이하	7년 이상 ~ 10년 이하	10년 이상 ~ 15년 이하	15년 이상
비율	15명 (46.88%)	5명 (15.62%)	2명 (6.25%)	2명 (6.25%)	8명 (25.00%)

<표 11> 설문 응답자의 개인(정보)보호 경력

구분	없음	3년 미만	3~5년 미만	5~10년 미만	10년 이상
비율	6명 (18.75 %)	11명 (34.38%)	4명 (12.50%)	2명 (6.25 %)	9명 (28.12%)

(2) 개인정보관리체계 및 운영 및 평가 수행경험, 보호조치 필요성에 대한 설문결과

클라우드컴퓨팅 개인정보보호 보안 개선 방안을 위해 본 논문에서 도출한 항목의 적합성 여부 판정에 앞서, 설문 응답자들의 개인정보관리체계의 수행 여부와 보호조치 필요성 인식에 대해 알아보기 위하여 첫째, 개인정보관리체계의 운영 및 평가 수행 경험 여부에 대한 질문, 둘째, 개인(정보)보호 개선의 필요 여부에 대한 질문으로 총 2개의 질문을 구성하였다.

설문 응답자 중 정보보호관리체계의 운영 및 평가

수행 경험 여부에 대해서는 14명이 “아니오”라고 답하였으며, 클라우드컴퓨팅 환경에서의 개선을 고려한 보호조치의 필요 여부에 대한 질문은 30명이 “필요하다”고 응답하였다.

<표 12> 물리적 보호조치의 보안점검 항목

통제분야	통제항목	점검항목	비고
물리적 보호조치	물리적 보호구역	개인정보 취급 공간과 개인정보처리, 저장시설 및 장비를 보호하기 위한 보호구역을 정의하였는가?	
		보호구역 내의 개인정보 문서, 장비, 매체를 반출입하기 위한 적절한 절차가 있는가?	
		유지보수를 위한 반출입 시 개인정보를 안전하게 관리하기 위한 통제방안을 운영하는가?	
		보호구역에 대하여 정책에서 명시한 물리적 접근 통제가 수행되고 출입기록이 남겨지고 있는가?	
	물리적 접근통제	보호구역의 출입 내역을 주기적으로 검토하고 있는가?	
		출입허가의 타당성을 주기적으로 검토하고 있는가?	
	사무실 보호	책상위에 개인정보 자료를 방치한 채로 오랜 시간 자리를 비우지 않도록 하는 정책이 있으며 준수되고 있는가?	
		컴퓨터에 중요한 화면을 띄워놓고 이석하지 않도록 하는 정책이 있으며 준수되고 있는가?	
		팩스, 복사기, 공개 단말기, 하드디스크가 있는 프린터 등 사용자가 지정되어 있지 않은 사무 장비에 대한 보호대책이 있는가?	
	개인정보처리 활동 모니터링	개인정보처리시스템 사용 및 접근에 대한 모니터링 절차와 책임이 정의되어 있고 이에 따라 이행되고 있는가?	
		모니터링 결과를 점검하는 주기가 정의되어 있으며, 이에 따라 모니터링 결과가 검토되며 보고되는가?	
	개인정보 열람기록 검토 및 오남용방지	개인정보취급자의 오남용을 방지하기 위하여 개인정보 열람 및 권한 없는 열람 시도에 대한 기록을 남기는가?	
		개인정보 열람 기록을 주기적으로 검토하여 권한없는 열람 및 과도한 접근시도 등의 사용내역을 분석하여, 개인정보 오남용, 이상징후를 추적하여 보고하고 필요한 조치를 취하는가?	
	시각동기화	개인정보처리시스템의 접근 및 처리내역과 관련한 정보의 정확성을 보장하고 해당 자료가 법적인 증거나 징계 자료로서 효력을 갖기 위해서 시스템 시각을 정확히 설정하는가?	
	기술적 점검	개인정보처리시스템이 절차에 따라 운영되고 있는지를 점검하기 위한 점검이 정기적으로 수행되는가?	
		기술적인 점검은 자격이 있고 숙련된 인력에 의해 점검하며, 허가된 인력의 감독 하에 수행되는가?	
		기술적 점검시 점검도구의 오용을 방지하기 위한 대책이 수립되어 있는가?	
		기술적 점검결과 발견된 취약성에 대한 대응방안 및 조치가 이행되며, 적절한 관리층에 보고되고 있는가?	
	케이블 보호	통신 회선이 도청이나 손상으로부터 보호되고 있는가?	
	장비의 안전한 폐기 및 재사용	개인정보 장비의 재사용시에는 저장 매체에 기록된 내용을 완전히 삭제하여 복구가 불가능한지 확인하고 사용하는가?	
		개인정보 장비의 폐기 시에는 저장 매체를 물리적으로 파기하거나, 저장된 정보가 완전히 삭제되어 복구가 불가능한지 확인하고 있는가?	

4.2.2 상세 지침항목의 적합성 검증 설문결과

<표 13> 개인정보보호관리체계의 운영 및 평가 수행 경험

구분	예	아니오
비율	18명 (56.25 %)	14명 (43.75 %)

<표 14> 개인정보보호관리체계의 운영 및 평가 수행 경험

구분	필요하다	필요하지 않다
비율	30명 (93.75 %)	2명 (6.25 %)

본 논문에서는 클라우드컴퓨팅 환경에서의 개인정보보호 개선과 관련하여 개인보호관리체계 수립 시 보안성을 보장하기 위해 8개의 통제항목을 도출하였다. 도출된 통제항목의 세부 점검 항목 적합성을 검증한 설문 결과는 다음과 같다.

개인정보보호관리체계 기반의 클라우드컴퓨팅 환경에서의 개인정보보호 개선 수행과 관련하여 도출한 '개인정보 위험관리' 점경항목으로 7개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 이를 정리하면 다음 <표 15>와 같다.

개인정보보호관리체계 기반의 클라우드컴퓨팅 환경에서의 개인정보보호 개선 수행과 관련하여 도출한 '개인정보 대책 구현'점경항목으로 2개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확

<표 15> 클라우드컴퓨팅 개인정보보호 보안 개선 시 '개인정보 위험관리'의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	0 명 (0%)	0 명 (0%)	8 명 (25%)	10 명 (31.25%)	14 명 (43.75%)
2	0 명 (0%)	1 명 (3.12%)	5 명 (15.62%)	13 명 (40.62%)	13 명 (40.62%)
3	0 명 (0%)	0 명 (0%)	6 명 (18.75%)	11 명 (34.38%)	15 명 (46.88%)
4	0 명 (0%)	1 명 (3.12%)	6 명 (18.75%)	9 명 (28.12%)	16 명 (50%)
5	0 명 (0%)	0 명 (0%)	3 명 (9.38%)	15 명 (46.88%)	14 명 (43.75%)
6	0 명 (0%)	1 명 (3.12%)	6 명 (18.75%)	11 명 (34.38%)	14 명 (43.75%)
7	0 명 (0%)	0 명 (0%)	11 명 (34.38%)	8 명 (25%)	13 명 (40.62%)

<표 16> 클라우드컴퓨팅 개인정보보호 보안 개선 시 '개인정보 대책 구현'의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	0 명 (0%)	0 명 (0%)	9 명 (28.12%)	9 명 (28.12%)	14 명 (43.75%)
2	0 명 (0%)	1 명 (3.12%)	10 명 (31.25%)	10 명 (31.25%)	12 명 (37.5%)

인해보면 이를 정리하면 다음 <표 16>와 같다.

개인정보보호관리체계 기반의 클라우드컴퓨팅 환경에서의 개인정보보호 개선 수행과 관련하여 도출한 '개인정보 사후관리'점검항목으로 4개 세부 점검항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 이를 정리하면 다음 <표 17>와 같다.

개인정보보호관리체계 기반의 클라우드컴퓨팅 환경에서의 개인정보보호 개선 수행과 관련하여 도출한 '개인정보 조직'점검항목으로 8개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 이를 정리하면 다음 <표 18>와 같다.

개인정보보호관리체계 기반의 클라우드컴퓨팅 환경에서의 개인정보보호 개선 수행과 관련하여 도출한 '개인정보 인적보안'점검항목으로 9개 세부 점검항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 이를 정리하면 다음 <표 20>와 같다.

개인정보보호관리체계 기반의 클라우드컴퓨팅 환

<표 17> 클라우드컴퓨팅 개인정보보호 보안 개선 시 '개인정보 사후관리'의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	0 명 (0%)	0 명 (0%)	12 명 (37.5%)	6 명 (18.75%)	14 명 (43.75%)
2	0 명 (0%)	2 명 (6.25%)	7 명 (21.88%)	9 명 (28.12%)	14 명 (43.75%)
3	0 명 (0%)	0 명 (0%)	6 명 (18.75%)	10 명 (31.25%)	16 명 (50%)
4	0 명 (0%)	0 명 (0%)	6 명 (18.75%	10 명 (31.25%)	16 명 (50%)

<표 18> 클라우드컴퓨팅 개인정보보호 보안 개선 시 개인정보 교육'의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	0 명 (0%)	0 명 (0%)	6 명 (18.75%)	12 명 (37.5%)	14 명 (43.75%
2	0 명 (0%)	0 명 (0%)	6 명 (18.75%)	12 명 (37.5%)	14 명 (43.75%
3	0 명 (0%)	1 명 (3.12%)	7 명 (21.88%)	9 명 (28.12%)	15 명 (46.88%)
4	0 명 (0%)	1 명 (3.12%)	5 명 (15.62%)	12 명 (37.5%)	14 명 (43.75%
5	0 명 (0%)	0 명 (0%)	11 명 (34.38%)	6 명 (18.75%)	15 명 (46.88%)
6	0 명 (0%)	1 명 (3.12%)	8 명 (25%)	11 명 (34.38%)	12 명 (37.5%)
7	0 명 (0%)	2 명 (6.25%)	7 명 (21.88%)	9 명 (28.12%)	14 명 (43.75%

경에서의 개인정보보호 개선 수행과 관련하여 도출한 '개인정보 기술적 보호조치'점경항목으로 12개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 이를 정리하면 다음 <표 21>와 같다.

<표 19> 클라우드컴퓨팅 개인정보보호 보안 개선 시 '개인정보 기술적 보호조치'의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	0 명 (0%)	0 명 (0%)	8 명 (25%)	11 명 (34.38%)	13 명 (40.62%)
2	0 명 (0%)	1 명 (3.12%)	5 명 (15.62%)	16 명 (50%)	10 명 (31.25%)
3	0 명 (0%)	1 명 (3.12%)	5 명 (15.62%)	15 명 (46.88%	11 명 (34.38%
4	0 명 (0%)	0 명 (0%)	6 명 (18.75%)	12 명 (37.5%)	14 명 (43.75%
5	0 명 (0%)	1 명 (3.12%)	6 명 (18.75%)	8 명 (25%)	17 명 (53.12%)
6	0 명 (0%)	0 명 (0%)	8 명 (25%)	8 명 (25%)	16 명 (50%)
7	0 명 (0%)	1 명 (3.12%)	7 명 (21.88%	10 명 (31.25%)	14 명 (43.75%)
8	0 명 (0%)	2 명 (6.25%)	4 명 (12.5%)	11 명 (34.38%)	15 명 (46.88%)
9	0 명 (0%)	0 명 (0%)	6 명 (18.75%)	12 명 (37.5%)	14 명 (43.75%)
10	0 명 (0%)	1 명 (3.12%)	6 명 (18.75%)	9 명 (28.12%)	16 명 (50%)
11	0 명 (0%)	1 명 (3.12%)	5 명 (15.62%	11 명 (34.38%)	15 명 (46.88%)
12	0 명 (0%)	2 명 (6.25%	6 명 (18.75%)	7 명 (21.88%)	17 명 (53.12%)
13	0 명 (0%)	1 명 (3.12%)	5 명 (15.62%	11 명 (34.38%)	15 명 (46.88%
14	0 명 (0%)	0 명 (0%)	3 명 (9.38%)	12 명 (37.5%)	17 명 (53.12%)
15	0 명 (0%)	0 명 (0%)	5 명 (15.62%)	11 명 (34.38%)	16 명 (50%)
16	0 명 (0%)	3 명 (9.38%)	4 명 (12.5%)	9 명 (28.12%)	16 명 (50%)
17	0 명 (0%)	0 명 (0%)	7 명 (21.88%)	10 명 (31.25%)	15 명 (46.88%)
18	0 명 (0%)	0 명 (0%)	6 명 (18.75%)	10 명 (31.25%)	16 명 (50%)
20	0 명 (0%)	0 명 (0%)	3 명 (9.38%)	15 명 (46.88%)	14 명 (43.75%)
21	0 명 (0%)	0 명 (0%)	5 명 (15.62%)	10 명 (31.25%)	17 명 (53.12%

<표 20> 클라우드컴퓨팅 개인정보보호 보안 개선 시 '개인정보 인적보안'의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	0 명 (0%)	0 명 (0%)	8 명 (25%)	7 명 (21.88%)	17 명 (53.12%)
2	0 명 (0%)	0 명 (0%)	6 명 (18.75%)	8 명 (25%)	18 명 (56.25%)
3	0 명 (0%)	0 명 (0%)	7 명 (21.88%)	9 명 (28.12%)	16 명 (50%)
4	0 명 (0%)	1 명 (3.12%)	5 명 (15.62%)	10 명 (31.25%	16 명 (50%)
5	0 명 (0%)	1 명 (3.12%)	4 명 (12.5%)	9 명 (28.12%)	18 명 (56.25%)
6	0 명 (0%)	0 명 (0%)	6 명 (18.75%)	13 명 (40.62%)	13 명 (40.62%)
7	0 명 (0%)	0 명 (0%)	7 명 (21.88%)	9 명 (28.12%)	16 명 (50%)
8	0 명 (0%)	2 명 (6.25%)	5 명 (15.62%)	7 명 (21.88%)	18 명 (56.25%)
9	0 명 (0%)	1 명 (3.12%)	6 명 (18.75%)	5 명 (15.62%)	20 명 (62.5%)

<표 21> 클라우드컴퓨팅 개인정보보호 보안 개선 시 '개인정보 기술적 보호조치'의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	0 명 (0%)	1 명 (3.12%)	8 명 (25%)	8 명 (25%)	15 명 (46.88%)
2	0 명 (0%)	1 명 (3.12%)	6 명 (18.75%)	8 명 (25%)	17 명 (53.12%)
3	0 명 (0%)	0 명 (0%)	7 명 (21.88%)	8 명 (25%)	17 명 (53.12%)
4	0 명 (0%)	1 명 (3.12%)	5 명 (15.62%)	10 명 (31.25%)	16 명 (50%)
5	0 명 (0%)	1 명 (3.12%)	7 명 (21.88%)	10 명 (31.25%)	14 명 (43.75%)
6	0 명 (0%)	0 명 (0%)	6 명 (18.75%)	10 명 (31.25%)	16 명 (50%)
7	0 명 (0%)	1 명 (3.12%)	9 명 (28.12%)	8 명 (25%)	14 명 (43.75%)
8	0 명 (0%)	2 명 (6.25%)	9 명 (28.12%)	10 명 (31.25%)	11 명 (34.38%)
9	0 명 (0%)	0 명 (0%)	10 명 (31.25%)	9 명 (28.12%)	13 명 (40.62%)
10	0 명 (0%)	0 명 (0%)	8 명 (25%)	11 명 (34.38%)	13 명 (40.62%)
11	0 명 (0%)	1 명 (3.12%)	5 명 (15.62%)	7 명 (21.88%)	0 명 (0%)

개인정보보호관리체계 기반의 클라우드컴퓨팅 환경에서의 개인정보보호 개선 수행과 관련하여 도출한 '개인정보 기술적 보호조치'점검항목으로 21개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 이를 정리하면 다음 <표 19>와 같다.

Ⅴ. 결론 및 향후 연구과제

5.1 결론

본 연구는 개인정보관리체계의 구성 항목들을 이용하여 클라우드컴퓨팅 환경에서의 개인정보보호 보안 개선 방안을 연구하고자 하였다. 그리고 이를 통해 클라우드컴퓨팅 환경에서의 개인정보보호를 효과적이고 효율적인 보안 개선방안을 논의하고자 하였다.

즉 클라우드컴퓨팅 환경에 대한 명확한 분석을 통해 개인정보보호 방안에 대해 논의하고, 이를 통해 클라우드컴퓨팅환경의 주요 특성들을 살핀 후 개인정보 관리체계를 적용시켜 지속적인 기존 이용자에게 보안성을 강화하고 유비쿼터스식, 업무 환경을 조성하고 클라우드 산업을 육성하는 긍정적인 구전을 유도할 수 있는 개선 방안을 제시하고자 하였다. 이를 위해 개인정보관리체계를 기반으로 각 단계에서 필요한 클라유드컴퓨팅 환경에서의 개인정보보호 점검 항목을 설계하였으며 본 논문을 실증 검증하기 위한 설문조사는 클라우드컴퓨팅을 사용한 조직원 및 일반인들을 대상으로 실시하였다.

연구결과 클라우드컴퓨팅 환경에서의 개인정보관리체계 개인정보 대책의 관리과정, 보호대책 및 생명주기의 총 3가지 통제분야와 16개의 통제 내용 통제항목 70개의 세부점검항목이 대부분 "매우접합" 라고 나타났다. 이는 클라우드컴퓨팅을 이용했던 경험자들이 생각하기에 개선방안이 필요하다고 본다 할 수 있다. 클라우드 컴퓨팅 기술적 보호에 대한 사례를 살펴보자면 A기업의 조직구성원이 다양한 편의성을 제공해주는 클라우드 컴퓨팅이 스토리지에 한계를 겪었으며 장치를 잃어버리거나 절취될 때 기존 클라우드 컴퓨팅이 정보 누설의 가능성으로부터 보안 위협의 가능성이 생겼다. 그러므로 사용자 인가, 접근 토큰, 키 생성에 의한 허용을 지속함으로써 안전한 클라우드 컴퓨팅 환경을 유지하면서 사용자 관리와 키 관리 할당을 제공해야 한다[25]. 둘째, 자원의 공유 및 집중화로 인한 유출 사례가 있다. 2008년 여름 B기업의 클라우드 서버가 인증요청 쇄도로 인하여 7~8시간 동안서비스 장애가 발생해 일시적으로 서비스가 중단되었다[26]. 셋째, 데이터 접근제어의 어려움으로 인한 사례가 있다. 2010년 12월, MS의 서비스 환경설정 오류로 클라우드상의 기업정보가 타인에게 열람된 사건이다. 이를 통해 대용량 데이터가 분산 파일 시스템을 통해 많은 서버들에 분산 저장/관리 됨에 따라 데이터 암호화, 이용자 인증, 접근제어 등 관리의 어려움이 증가되고 있다. 이와 같은 클라우드컴퓨팅 환경에서는 기존의 보안 기술들은 클라우드 환경의 보안 위협에 대응하기에는 가상화 기술의 구조적 특성을 인식하지 못하는 한계가 있으므로 클라우드 컴퓨팅 환경에 적합한 새로운 보안 기술을 개발할 필요가 있다[26].

본 연구의 학문적, 실무적 시사점은 다음과 같다.

본 연구에서는 클라우드컴퓨팅 환경에서의 개인정보관리체계에 대한 연구를 수행했다는 점에서 학문적 기여도가 크다고 할 수 있다. 그리고 실무적 시사점으로 는 클라우드컴퓨팅을 이용했던 경험자들의 특성을 고려한 점검항목으로 개인정보관리체계 참여율을 크게 높여 클라우드컴퓨팅환경에서의 개인정보

보호 보안에 대해 개선할 수 있을 것이다.

<표 22> 클라우드컴퓨팅기술적보호에 대한 사례

A기업	B기업	C기업
· 키관리 할당 · 사용자 인가 · 접근 토큰 · 키 생성 · 사용자관리	· 자원의 공유 · 자원의 집중화 · 인증요청 · 클라우드서버 · 서비스 장애	· 데이터 접근제어 · 대용량 데이터 · 분산파일시스템 · 이용자 인증 · 접근제어

5.2 향후 연구 과제

본 연구의 의의와 한계점, 추후 연구방향은 다음과 같다. 본 연구는 첫째, 표본 응답자의 수가 많이 부족하였다. 향후 연구에서는 응답자의 수를 높여 폭넓은 연구를 진행할 필요가 있다. 또한 심층면접, 인터뷰 등을 활용하여 연구결과의 타당성 및 신뢰성을 향상시켜야 할 것이다. 둘째, 클라우드컴퓨팅을 이용한 경험자들의 특성을 고려한 세심한 연구가 필요하다. 클라우드컴퓨팅을 이용한 경험자들의 구체적이게 어떤 부분을 이용하고 경험하였는지에 대한 것을 확인해여 한다. 향후 연구에서는 이러한 개요 내용을 기반으로 하여 첫째, 개인정보보호를 위해 일정수준 이상의 관리적·기술적·물리적 대책을 수립 및 운영해야 하며 이용자 및 정보주체는 개인정보의 누출가능성을 최소화하고 효과적으로 보호하고 개인정보보호를 예방하는 데 도움이 되기를 기대한다. 둘째, 클라우드컴퓨팅 환경에서의 개인정보보호 보안 개선 방향을 연구하여 효율적인 클라우드컴퓨팅 개인정보 개선방안 연구가 이루어져야 할 것이다.

참고문헌

[1] 김동성·김종우, “클라우드 컴퓨팅 관련 논문의 서지정보 및 인용정보를 활용한 연구 동향 분석 : 사회 네트워크 분석의 활용,” 지능정보연구 제20권, 제1호, 2014. 3, pp. 195-211.

[2] 김성준, “클라우드 컴퓨팅환경에서의 기업정보보안 방안 : 정보보호관리체계(ISMS)를 중심으로,” 경영 컨설팅 리뷰 제1권, 제2호, 2010, pp. 194-20.

[3] 박성희·양해술, “클라우드 컴퓨팅 환경을 위한 기존 시스템의이전 방안 연구,“ 한국디지털정책학회, 디지털융복합연구, 제12권, 제10호, 2014, pp. 271-282.

[4] 김진형, “클라우드 컴퓨팅 환경에서의 개인정보보호 이슈,” 2014.

[5] 신선진·유일, “개인 클라우드 컴퓨팅 서비스로의 전환의도에 관한 연구: 사회교환이론을 중심으로,” 기술혁신학회지, 제18권, 제1호, 2015, pp. 176-203.

[6] 김동호·이정훈, “기업의 Cloud Computing 서비스 도입의도에 영향을 미치는 Cloud Computing 특성 요인에 관한 연구,” 한국전자거래학회지, 제17권, 제1호, 2012, pp. 111-136.

[7] 이지은·황찬규·권두순, “업무용도로 이용되는 모바일 인스턴트 메신저에서 인지된 보안성, 인지된 프라이버시, 인지된 즐거움, 인지된 상호작용성이 지속이용의도에 미치는 영향에 관한 연구,” 디지털산업정보학회논문지, 저널 지식맵, vol. 11, no. 3, 2015, pp. 159-177.

[8] 윤영배·오준석·이봉규, “클라우드 서비스 도입을 위한 보안 중요도 인식에 대한 연구,” 인터넷정보학회논문지, 제13권, 제6호, 2012, pp. 33-40.

[9] 배유미, “클라우드 컴퓨팅의 영향에 따른 운영체제 변화 및 보안에 관한 연구,” 한남대학교 대학원 : 컴퓨터공학과 박사학위논문, pp. 144-149.

[10] 조인제·김선규·양성병, “개인용 클라우드 컴퓨팅 서비스 수용저항에 영향을 미치는 요인에 관한 연구,” 지식경영연구, 제16권, 제1호, 2015.

[11] 염흥열・윤미연, “클라우드 컴퓨팅 보안 국제 표준화 동향,” 정보보호학회지, 제23권, 제3호, 2013, 6, pp. 14-18.

[12] 채정우・정진홍, “산업보안 관리체계를 위한 보안통제 프레임워크 구성에 대한 연구,” 한국공안행정학회보, 제22권, 1호, 2013, pp. 300~341.

[13] 전진환・조강래, “개정 고시에 따른 개인정보보호 관리체계(PIMS)인증의 주요변화,” 정보보호학회지, 제23권, 제5호, 2013, pp. 20-23.

[14] 박대하・백태석, “클라우드 컴퓨팅 개인정보보호 연구동향과 과제,” 정보보호학회지, 제21권, 제5호, 2011, pp. 37-44.

[15] 박경태・김세현, “개인정보보호 인증제도 선호도 분석에 관한 연구- 중소기업 및 소상공인을 중심으로,” 정보보호학회논문지, 제24권, 제5호, 2014. 10, pp. 911-918.

[16] 심미나, “효율적인 개인정보관리체계(PIMS) 인증제도 도입방안 연구 : 정보보호관리체계(ISMS) 인증제도와의 중복성 해소방안을 중심으로,” 고려대학교 박사학위논문, 2010.

[17] 한국인터넷진흥원 보고서, “개인정보보호 관리체계 국제 표준화 필요성,” 2013.

[18] 이주영, “클라우드 컴퓨팅의 특징 및 사업자별 제공 서비스 현황,” 방송통신정책, 제22권, 제6호, 2010, p. 6.

[19] M. Armbrust, et al., “Above the Clouds: A Berkeley View of Cloud Computing, University of California, Department of EECS,” Technical Report No. UCB/EECS, 2009, p. 28.

[20] NIST, “Guidelines on Security and Privacy in Public Cloud Computing,” NIST SP 2011, pp. 800-144.

[21] 이승훈・이우현, “클라우드 서비스 환경 내 개인정보보호측면에서의 국내외 동향분석,” 2014.

[22] 유우영・임종인, “클라우드 컴퓨팅 서비스 제공자의 개인정보보호 조치방안에 대한 연구,” 정보보호학회논문지, 제22권, 제2호, 2012, pp. 337-346.

[23] 김일태, “클라우드 컴퓨팅을 활용한 비즈니스 연구:모바일 클라우드 사례를 중심으로,” 석사학위논문, 포항공과대학교, 2012.

[24] 김용빈, “빅 데이터 활용에 있어서 개인정보보호 문제점 및 개선방안(PIMS 활용),” 강원대학교 산업대학원 컴퓨터정보통신공학과 석사학위논문.

[25] 진병욱, “퍼스널 클라우드 환경에서 사용자 관리를 위한 보안 프레임워크의 설계 및 평가,” 디지털산업정보학회논문지, Journal of the Korea Society of Digital Industry and Information Management, 저널 지식맵, vol. 12, no. 1, 2016, pp. 81-87.

[26] 박진호・이재휘, “클라우드 컴퓨팅 서비스 침해사례 분석 및 정보보안 기술동향,” 경북대학교 컴퓨터 학부, 2013.

[27] 정병호, “기밀정보 유출 경험을 가진 기업들의 정보사고 대응역량 강화에 관한 연구,” 디지털산업정보학회논문지, Journal of the Korea Society of Digital Industry and Information Management, 저널 지식맵, vol. 12, no. 2, 2016, pp. 73-86.

[28] 양환석, “신뢰도와 키를 이용한 보안 라우팅 기법에 관한 연구,” 디지털산업정보학회논문지, Journal of the Korea Society of Digital Industry and Information Management, 저널 지식맵, vol. 11, no. 3, 2015, pp. 69-77.

[29] 류준상, “그린 IT로서의 클라우드 컴퓨팅과 보안 이슈,” 고려대학교 석사 학위논문, 2010.

■ 저자소개 ■

정 혜 인
Jeong Hyein

2014년 6월~2016년 8월
남서울대학교 복지경영대학원
산업보안학과 석사과정 졸업
2014년 6월 나사렛대학교 디지털콘텐츠(학사)

관심분야 : 산업보안, 개인정보보호,
사물인터넷
E-mail : hyeinee15@naver.com

김 성 준
Kim Seongjun

2014년 2월~현재
남서울대학교 산업보안학과
조교수
2014년 2월 연세대학교 정보대학원(박사수료)
2009년 2월 동국대학교 법학과(박사)
2006년 8월 동국대학교 법학과(석사)
2003년 2월 동국대학교 법학과(학사)

관심분야 : 개인정보, 개인정보보호법,
정보보호, 사물인터넷, 빅데이터
E-mail : mvstar@hanmail.net

논문접수일: 2016년 8월 20일
수 정 일: 2016년 9월 8일
게재확정일: 2016년 9월 13일