情報保護學會論文誌
第 22 卷 第 1 號, 2012. 2

클라우드 컴퓨팅 서비스에 관한 정보보호관리체계

신 경 아,† 이 상 진‡
고려대학교 정보보호대학원

Information Security Management System on Cloud Computing Service

Kyoung-a Shin† , Sang-jin Lee‡
Information Security Department, Graduate School Information management and security, Korea University

요 약

클라우드 컴퓨팅 서비스는 이용자 요구에 실시간으로 유연하게 컴퓨팅 자원을 제공하고 사용량만큼 과금하는 고효율의 차세대 IT 서비스 이다. 그러나 이용자는 데이터를 '위탁'하고, 인프라, 플랫폼, 어플리케이션 서비스를 '제공'받는 '위탁/제공'의 서비스 구조와 적용기술, 자원공유, 데이터센터 위치 등으로부터 비롯된 많은 위협에 직면해 있다. 클라우드 서비스 도입의 가장 큰 걸림돌로 작용하는 보안과 신뢰성을 담보하기 위해서는 객관적인 평가 기준이 필요하다. 지금까지 정보보호관리체계는 조직의 보안관리 및 IT 운영의 보안 지표로 활용되어 왔다. 그러나 클라우드 컴퓨팅 서비스는 기존의 조직 내 IT 환경과는 다른 관점의 보안관리와 평가기준이 필요하다. 본 논문에서는 클라우드 특성에 맞는 정보보호관리체계를 설계하기 위하여 클라우드 서비스의 핵심요소를 위협관리영역으로부터 도출하고 기본적인 보안관리가 누락되지 않도록 기존 정보보호관리체계의 모든 통제영역을 포함하고 있다. 또 온라인 셀프환경에 따른 서비스 이용을 지원하고 서비스 계약, 제공자 사업현황을 포함하는 서비스 보안관리를 추가하여 설계한다.

ABSTRACT

Cloud computing service is a next generation IT service which has pay-per-use billing model and supports elastically provisioning IT infra according to user demand. However it has many potential threats originating from outsourcing/supporting service structure that customers 'outsource' their own data and provider 'supports' infra, platform, application services, the complexity of applied technology, resoucrce sharing and compliance with a law, etc. In activation of Cloud service, we need objective assessment standard to ensure safety and reliability which is one of the biggest obstacles to adopt cloud service. So far information security management system has been used as a security standard for a security management and IT operation within an organization. As for Cloud computing service it needs new security management and assessment different from those of the existing in-house IT environment. In this paper, to make a Information Security Management System considering cloud characteristics key components from threat management system are drawn and all control domain of existing information security management system as a control components are included. Especially we designed service security management to support service usage in an on-line self service environment and service contract and business status.

Keywords: cloud security, cloud ISMS, cloud computing service

접수일(2012년 1월 2일), 수정일(2012년 2월 15일),
게재확정일(2012년 2월 24일)

† 주저자, fruitnara@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr

I. 서 론

클라우드 컴퓨팅 서비스(이하 클라우드 서비스)는 인프라와 개발환경, 어플리케이션 서비스를 제공하고 이용자 요구 기반 하에 실시간으로 유연하게 컴퓨팅 자원을 제공하고 사용한 만큼 과금하는 서비스이다. 클라우드 서비스는 IT 서비스의 집약으로 고효율, 저비용, 관리의 전문성, 실시간성, 편리성이라는 화려한 수식어와 함께 차세대 IT 서비스로 주목받고 있다[2,4].

클라우드 서비스는 이용자가 데이터를 '위탁'하고, 인프라와 개발환경, 응용서비스를 '제공'받는 '위탁/제공' 서비스이다. 데이터 소유주는 이용자이나 관리는 제공자라는 이분법적 서비스 구조, 분산기술과 가상화 기술을 접목시킨 유기적인 통합제어의 복잡성, 웹 인터페이스 방식에 의한 취약성, 다중 이용자 간의 자원 공유로 인한 침해 가능성 증가, 데이터센터의 국외 배치로 인한 국내법 규제의 이탈 등 여러 위협 요인을 가지고 있다. 특히 제공자의 서비스 보안을 위해 서비스 구조 비공개 및 이용자의 내부 감사 불가, 사고발생 시 책임소재 규명이 어렵다는 점에서 많은 분쟁의 가능성을 내포하고 있다[1,2,3,8,10,11,16,17,19,20].

한국 IDC가 발표한 '2011 국내 기업 IT 수요조사'에 의하면, 국내 기업의 클라우드 서비스 사용 비율은 13%로 미미한 수준으로 조사됐다. 이는 클라우드 서비스에 대한 기업이용자의 불안과 신뢰성 부족이라고 볼 수 있다[20]. 이용자의 불안을 해소하고 신뢰를 담보하기 위해서는 클라우드 서비스에 대한 객관적인 평가방안이 마련되어야 한다. 지금까지 정보보호관리체계는 조직의 보안관리 및 IT 운영의 보안 지표로 활용되어 왔다. 그러나 클라우드 서비스는 IT 환경의 새로운 패러다임으로서 기존의 조직 내 IT 환경과는 다른 관점의 보안관리와 평가기준이 필요하다.

본 논문에서는 클라우드 서비스를 제공함에 있어 반드시 보장해야 하는 핵심 요소를 식별하고 이를 정보보호관리체계에 반영하고자 한다. 클라우드 서비스의 핵심요소를 클라우드 위협관리영역으로부터 도출하고, 클라우드 핵심요소에 치우쳐 기본적인 보안관리가 누락되지 않도록 기존 정보보호관리체계의 모든 통제영역을 포함하되 클라우드 보안관리 영역에 맞게 재배치한다. 이는 기존 정보보호관리체계의 관리·물리·기술적 관점의 완전성을 유지할 수 있게 한다. 또 온라인 셀프환경에 따른 서비스 이용을 지원하고 계약의 공정성, 과금 체계, 제공자의 사업현황을 포함하는 서비스 제반환경 통제를 추가하여 이용자의 권익을 보호하는 서비스 보안관리를 정의한다. 이로써 클라우드 컴퓨팅 서비스 정보보호관리체계(이하 클라우드 정보보호관리체계)는 클라우드 서비스의 원활한 제공을 위한 보안관리와 서비스 제반환경을 통제하는 서비스 보안관리로 구성된다.

Ⅱ장에서는 클라우드 서비스의 핵심요소를 식별하기 위해 클라우드 위협을 조사하고, 이를 분류하여 위협관리영역을 정의한다. 위협관리영역은 클라우드 서비스의 핵심요소를 나타내며 관리체계 설계의 주축이 된다. Ⅲ장은 위협관리영역의 보안통제를 분석하여 클라우드 정보보호관리체계를 설계하고 타 정보보호관리체계와의 차이점을 분석한다. 1절에서는 클라우드 보안관리를 위협관리영역에 따라 ISO 27001의 보안통제를 분석하고 필요한 보안통제를 정의한다. 2절에서는 클라우드 서비스 보안관리의 보안통제를 정의한다. 3절에서는 통제영역과 통제요소로 구성된 클라우드 정보보호관리체계를 설계한다. 4절에서는 타 클라우드 정보보호관리체계와의 차이점을 분석한다. Ⅳ장은 결론을 맺는다.

II. 클라우드 위협관리영역

본 장에서는 클라우드 서비스의 핵심요소를 식별하기 위하여, 클라우드 위협을 분석하고 클라우드 위협관리영역을 정의한다. 클라우드 위협을 근원적 위협과 파생 위협으로 구조화하여 이를 각각 위협 대분류와 위협 소분류로 구분한 위협관리영역은, 클라우드 보안관리의 핵심으로 클라우드 정보보호관리체계의 골격이 된다.

2.1 클라우드 위협관리영역

본 절에서는 클라우드 서비스의 핵심요소를 식별하기 위하여 클라우드 위협을 조사하여 이를 위협관리영역으로 분류하였다. 클라우드 서비스에서 발생하는 위협은 클라우드 서비스의 특성을 반영하며 클라우드 보안관리의 핵심을 나타낸다. 따라서 클라우드 위협을 식별하고 이를 통제함으로써, 안전한 서비스 제공을 보장할 수 있으며 클라우드 특성에 맞는 정보보호관리체계를 설계할 수 있다.

위협은 가트너, RSA, CSA, JAPAN, ENISA, UC 버클리에서 발표한 위협[8,16,17]중 클라우드 서비스에서 새롭게 부상한 위협 또는 클라우드 서비스

에서 위험도가 가중되는 위협 중에서 위협관리가 가능한 위협을 발췌하였다. 클라우드 서비스 위협을 관리·물리·기술 관점으로 바라보면, 관리적 관점으로는 '위탁/제공'의 서비스 구조와 데이터센터의 위치 문제가 해당되며, 기술적 관점으로는 적용기술과 자원공유 문제가 클라우드 서비스의 근원적 위협이라고 할 수 있다. 물리적 관점에 해당하는 신규 위협은 없다. 기존과 동일한 물리·환경적 위협으로 존재하기 때문에 클라우드 위협관리영역에서 별도로 식별하지 않고 기존의 보안관리와 동일하게 적용하려고 한다. 데이터센터의 위치를 관리적 관점으로 분류한 것은 위치에 따라 재판관할권이 달라지고 법 적용이 달라진다는 점에서 준거성을 포괄하는 관리적 관점으로 분류하였다.

클라우드 위협은 '위탁/제공'의 서비스 구조와 적용기술, 자원공유, 데이터센터의 위치에서 근원적인 위협이 시작된다. 클라우드 서비스는 이용자가 데이터를 '위탁'하고, 인프라와 개발환경, 응용서비스를 '제공'받는 '위탁/제공' 서비스이다. 클라우드 서비스의 첫 번째 위협은 서비스 제공자와 데이터 소유주가 각기 다른 위탁/제공 서비스 구조에서 출발한다. 조직의 업무환경과 IT 서비스 환경 및 데이터가 제3자에 의해 관리된다는 것은 데이터의 유출, 관리의 불투명성, SLA/계약의 불공정성과 불이행, 사고에 대한 책임소재 규명 어려움 등 많은 위험을 내포하고 있다. 클라우드 서비스의 두 번재 위협은 클라우드 서비스의 적용기술이다. 클라우드 서비스는 분산 기술과 가상화 기술을 근간으로 이기종 서버와 스토리지, 네트워크를 통합·관리하는 유기체적 특성을 가지고 있다. 통합·관리의 유기체적 특성은 제어 오류 및 인프라 운영 관리의 복잡성을 가중시킨다. 또한 웹 인터페이스 방식을 이용하는 클라우드 접속은 웹 취약점을 이용한 공격에 노출되어 있다. 세 번재 위협은 자원 공유이다. 가상화에 의한 멀티테넌트 환경과 분산기술에 의한 이용자 간의 자원공유는 내부 침해를 통한 이용자 데이터에 대한 불법 접근 위험을 내포하고 있다. 네 번재 위협은 국외의 데이터센터 위치이다. 저비용, 에너지 절감을 위한 데이터센터의 국외 배치는 국내 법규의 통제를 벗어나 법적, 관리적 문제를 양산하게 된다.

클라우드의 4가지 근원적 위협은 다시 관련 파생위협으로 분류할 수 있다. '위탁/제공' 서비스 구조 위협의 파생위협에는 데이터 보안 위협, 관리적 보안 위협, SLA/계약 분쟁 위협이 있다. 적용기술 위협의 파생위협에는 가용성 침해 위협, 분산기술 위협, 가상화 위협, 웹 인터페이스 위협이 있다. 자원공유 위협의 파생위협에는 접근통제 우회 위협이, 데이터센터의 위치 위협의 파생위협에는 법 규제 이탈 위협이 있다. 클라우드의 4가지 근원적 위협과 각 파생위협을 위협 대분류와 위협소분류로 명명하고 위협 설명과 관련 위협을 분류하면 〔표 1〕과 같다. 〔표 1〕은 클라우드 서비스의 핵심요소를 나타내는 위협관리영역이 된다.

III. 클라우드 정보보호관리체계 분석 및 설계

본 장에서는 클라우드 정보보호관리체계의 보안관리와 서비스보안관리를 설계하고자 한다. 클라우드 서비스의 원활한 서비스 제공을 위한 관리·물리·기술적 관점의 보안관리를 정의하기 위해서, 클라우드 위협관리영역을 기준으로 기존 정보보호관리체계의 클라우드 통제를 분석하고 필요한 통제를 정의한다. 클라우드 서비스 보안관리에서는 이용자의 서비스 이용을 지원하고 계약의 공정성, 과금 체계, 제공자의 사업현황을 포함하는 통제영역을 정의한다. 클라우드 보안관리와 클라우드 서비스 보안관리로 구성된 클라우드 정보보호관리체계를 설계한다. 마지막으로 설계한 클라우드 정보보호관리체계가 타 정보보호관리체계와 어떤 차이점이 있는지를 설계 방법과 구성면에서 분석한다.

3.1 클라우드 보안관리

정보보호관리체계는 법적·제도적 정보보호요구사항에 따라 업무 프로세스 전반에 관리, 물리, 기술적 보안 조건을 충족하고 문서화함으로써 조직내 정보보호활동에 일관성과 효과성을 증대시키고자 도입되었다. 정보보호관리체계에는 국제 인증인 ISO 27001〔5〕이 있으며, 국내 인증으로는 K-ISMS, G-ISMS가 있다. ISO 27001과 K-ISMS, G-ISMS는 통제영역의 분류 차이만 있을 뿐 통제항목이나 통제내용에 있어서는 두드러진 차이가 없는 것으로 분석된다. 여러 정보보호관리체계 중 ISO 27001이 오랜 기간 변화를 거치면서 보다 체계적이고 세부적인 통제를 담고 있기 때문에 ISO 27001 통제영역과 비교하여 클라우드 위협 통제를 분석하고자 한다.

3.1.1 데이터 보안

데이터 보안은 서비스를 이용하는 이용자의 데이터를 보호하는 영역이다. 유무형 자산에 대해 소유자, 중요도 식별, 책임, 분류, 취급방법, 라벨링 등을 다루

〔표 1〕 클라우드 서비스 위협관리영역 정의

위협 대분류	위협소분류	위협소분류 설명	관련 위협
위탁/제공	데이터 보안 위협	서비스 제공자에 의한 데이터 유출 위협	- 제공자의 인수, 합병, 폐업에 의한 데이터 유출 위협 - 내부직원의 권한 남용에 의한 자료 유출 위협 - 개인과 기업의 사적정보가 정부 및 법 집행기관에 노출될 위협 - 서버의 잔존데이터 유출 위협
	관리적 보안 위협	서비스 제공자의 관리의 소극성, 미숙함, 증거 은닉에 의한 위협	- 클라우드 환경 및 협업 클라우드 환경에서 사고발생시 서비스 제공자와 협력사 간에 책임소재를 규명하기 어려움 - 서비스 제공자의 보안사고에 대한 소극적 대응 가능성 - 책임소재를 판별하기 위한 제공자의 보안통제 관련증거의 은닉 또는 미제공, 사고추적을 위한 정보의 접근이 제한적임 - 클라우드 환경 및 협업 클라우드 환경에서의 일관된 보안정책 적용 어려움 - 온라인 자동화 셀프환경에서 이용자 신분 도용에 의한 위협 증대 - 관리자에 의한 시스템 오용, 정책적 설정 오류 등의 위협 - 내부직원의 권한 남용에 의한 자료 유출 위협 - 개인과 기업의 사적정보가 정부 및 법 집행기관에 노출될 위협
	SLA/계약 분쟁 위협	불명확한 계약 조건, 불공정한 계약, 계약 불이행으로 인한 분쟁 위협	- 보안수준 규정이 부적절한 위협 - 규제 및 법률 등 관련 규제의 미비 - 소프트웨어 라이센싱 위배 위협 - 지적재산권 분쟁 위협 - 서비스 제공자 의존도가 높은 위협 - 제공자의 인수, 합병, 폐업 등에 의한 서비스 중단 위협
적용 기술	가용성 침해 위협	컴퓨팅 자원관리의 오류와 비표준화에 의한 서비스 중단 위협	- 집중화된 서비스로 분산서비스공격인 DDoS 등의 공격 위협 증대 - 이기종간의 제어 오류로 인한 서비스 중단 위협 - 하이퍼바이저와 Guest OS간의 오류로 인한 시스템 중단 - 멀티테넌트 환경에서 자원격리 부적절로 타 이용자의 처리부하로 인한 속도 저하 위협 - 사고 발생시 이용자의 가상머신들이 상호 연결되어 이용자 서비스 연쇄 중단 및 대규모 피해 야기 - 서비스 구조의 복잡성으로 인한 사고대응 부적절 위협 - 데이터, 응용프로그램, 서비스에 대한 이동성, 호환성을 제공할 표준화된 절차나 데이터 표준 포맷이 존재하지 않아 이전데이터의 사용불가 위협 - 확장가능한 스토리지 미비 위협 - 불확실한 성능 예측에 의한 위협 - 신속한 스케일링의 미비 위협
	자원 공유	분산된 이기종 시스템의 제어오류 위협	- 이기종간의 데이터 제어 오류로 인한 데이터 유출/손상, 서비스 중단 위협 - 데이터를 저장하는 서버의 지속적인 위치 변동으로 물리적 서버 및 네트워크 손상 시 저장 데이터의 식별이 어려워 복구 지연에 따른 서비스 중단 위협 - 시스템 간 협업처리과정에서 비암호화된 데이터의 통신 중 도청 위협
	데이터 센터의 위치	하이퍼바이저, 가상머신 등 가상화 기술로 인한 위협	- 하이퍼바이저와 Guest OS간의 오류로 인한 시스템 중단 - 멀티테넌트 환경에서 해킹 및 관리자 실수 등에 의해 이용자 정보유출 - VDI 통신 프로토콜 사용으로 인한 통신 도청 위협 - 플랫폼 API, 가상화 SW 취약점으로 인한 위협
	웹 인터페이스 위협	웹 인터페이스에 의한 위협	- 웹 인터페이스 방식에 의한 웹 취약점 공격 위협
자원 공유	접근 통제 우회 위협	자원격리 실패 및 인증을 우회한 비인가 접근 위협	- 클라우드 환경 및 협업 클라우드 환경에서의 일관된 계정관리 정책 적용 어려움 - 계정도용에 의한 대량연산능력을 패스워드 크랙에 악용하거나 봇넷 등 공격 에이전트로 악용할 위협 - 데이터 격리 미흡으로 인한 타 이용자 소유 데이터 접근 위협 - 클라우드 컴퓨팅 웹 인터페이스 취약점으로 인한 접근통제 우회 위협 - 클라우드 관리 소프트웨어 또는 웹 브라우저의 취약점으로 인한 접근통제 우회 위협 - 관리소프트웨어 내부의 가상머신 프로파일 정보 유출
데이터 센터의 배치	법 규제의 이탈 위협	국외에 위치한 데이터센터의 국내법 적용 불가 위협	- 데이터센터가 국외에 위치하는 경우 보안규정과 보안사고에 대해 각 나라마다 상이한 법규로 인한 국내법 적용 불가능 위협

는 ISO 27001의 자산관리 영역과 유사한 점은 있으나 ISO 27001의 자산은 조직 내 자산과 유형 자산을 포함한다는 점이 다르다. 클라우드 서비스에서 서비스 제공과 더불어 중요한 부분은 이용자 데이터의 보안이다. 이용자 개인정보와 회사의 영업비밀이 제공자의 관리 하에 타 사용자와 공유된다는 점에서 클라우드의 서비스 구조적 측면과 기술적 환경 하의 데이터 보안은 더욱 강조되는 영역으로 그 중요도와 통제범위를 고려할 때 새로운 통제 영역으로 구성되어야 한다. 클라우드 서비스 이용자 데이터 보안은 암호화 뿐만 아니라 정보보호 관점으로 기술적 보호조치와 생명주기에 따른 보호조치, 이용자의 권리가 보장되어야 한다.

데이터 암호화에서는 암호화와 키관리 주체가 제공자가 아닌 이용자로 변경된다. 제공자는 데이터의 보호서비스를 구성하고 실행하는 주체이며 이용자는 데이터의 중요도를 산정하여 적절한 보호서비스를 결정하여 선택해야 한다. 기술적 보호조치는 생명주기에 따른 보호조치와 병행해야 한다. 이용자의 데이터는 VM 이미지로 통합된다. 따라서 VM 이미지의 주요 정보를 필터링하여 변환시킴으로써 주요 정보를 노출시키지 않고 보호하는 방법을 강구해야 한다[13]. 그 외 데이터 보안등급에 따른 접근통제, 익명 접근 가능, 모니터링을 통한 데이터 접근 통제 및 접근기록 유지, 정기적인 비인가 접근 감사, 메모리와 스토리지의 데이터 완전삭제 등의 보안통제가 필요하다[9].

3.1.2 관리적 보안

관리적 보안은 조직의 정보보호 및 운영에 대한 기본 정책을 수립하고 업무활동에 체계적인 정보보호활동을 수행하는 것이다. ISO 27001의 인적보안, 정보보호정책, 정보보호조직, 준거성, '물리적, 환경적 보안' 영역이 관리적 보안에 해당된다. 전반적인 보안 관리를 포함하는 관리적 보안은 클라우드 관리보안이라 하여 기존의 관리보안과 별다른 차이점은 없다. 다만 클라우드 서비스 제공과 관련하여 다루는 범위는 좁아지고 전문성이 증가하였다. 인적보안에서는 내부 인력의 신원조회 강화 및 내부자로부터의 위협이 대두되며, 정보보호조직에서는 정보보호 및 개인정보를 책임지는 구성원의 책임과 역할, 정보보호위원회의 구성을 정의하고, 정보보호정책에서는 클라우드의 법적 준거성과 기술보안의 준거성을 포함하는 내부 규정을 수립하고 준거성 준수를 점거하는 감사가 포함된다. 물리/환경 보안은 데이터센타, 사무실, 건물입구 등의 출입통제와 방재 등의 통제가 있다.

3.1.3 SLA/계약 분쟁[16,18]

SLA(Service Level Agreement)는 계약서 외에 서비스 수준을 정량화하여 명확히 함으로써 분쟁의 요소를 줄이고 서비스의 품질을 보장하기 위한 약정이다. 모든 IT 서비스를 '위탁/제공'하는 클라우드 서비스에서는 공정한 계약과 서비스 품질의 보장이 선행되어야 한다. SLA와 계약서는 보안관리의 준거성 영역으로 서비스 제공에 있어 우선적으로 준수할 내용이 될 것이다. ISO 27001의 준거성 영역에서는 대외적인 법 요구사항과 내부 규정 요구사항을 파악하여 정책적 준수와 기술적 준수, 그리고 정보시스템 감사를 다룬다. 서비스 계약과 SLA에 대해서는 10. 통신 및 운영관리 영역의 제3자 서비스 관리에서 SLA 계약 여부를 다루고 있으나 이는 제3자 위탁관리 측면에서 위탁관리 요구사항을 다루고 있다. 그러나 클라우드 서비스에서는 제공자와 이용자 간의 서비스와 서비스 품질을 다뤄야 한다는 점에서 SLA와 계약에 관한 통제영역이 새롭게 정의되어야 한다.

클라우드 서비스 계약에는 제공자와 이용자의 권리, 의무, 책임사항을 명시해야 한다. 제공자의 의무부분에서는 서비스 가용성, 인프라에 대한 실시간 확장성, 과금규칙, 이용자 데이터의 보호 의무를 명시해야 한다. 이용자 책임부분에서는 비인가 행위를 금지하고 이에 대한 책임을 명시하며, 악의적인 사용에 대한 모니터링 허용 등이 포함되어야 한다. 특히 클라우드 서비스에서는 이용자의 저작권 침해가 클라우드 서비스 제공자에게도 저작권 침해책임을 부담할 수 있다는 점을 고려하여 이용자의 지적재산권 침해 책임을 명시해야 한다. 그 외 면책조항과 피해보상 절차, 분쟁의 해결 등에 대해 명시해야 한다.

클라우드 서비스 계약에서 준수해야 할 관계법령으로는 "약관규제법", "디지털콘텐츠 이용표준이용약관", "전자거래기본법", "전자상거래소비자보호법", "정보통신망법", "전기통신사업법", "콘텐츠산업진흥법" 등이 있다. 지난 10월 5일 방송통신위원회에서 "클라우드 SLA 가이드 및 개인정보보호수칙 자료(10.5)"를 통해 SLA의 평가지표를 제시하였다. 평가지표에는 가용성, '백업, 복구, 보안', 고객지원, 위약금, 계약조건, 보안, 확장성, 서비스 수준 보고 등을 구체적인 수치와 함께 나타내고 있다. 클라우드는 새로운 IT 서비

스 유형으로 아직 표준적인 규율내용이 마련되어 있지 않다는 점에서 이용자의 권익이 침해당할 수 있으므로 약관규제법에 따라 공정성 여부를 판단해야 한다. 클라우드 서비스 정보보호관리체계에서는 계약(약관)과 SLA가 공정하고 이들 관계법령을 준수하도록 통제해야 한다.

3.1.4 서비스 가용성

서비스 가용성은 서비스 제공자의 기본 의무로서 클라우드 서비스의 가장 중요한 특성으로 중단없는 서비스 제공을 의미한다. 성능 및 확장성은 가용성과 함께 클라우드 서비스의 주요 특성으로 유연한 성능과 확장성을 보장해야 한다. ISO 27001의 정보보안 사고관리, 사업연속성 관리, 통신 및 운영관리 영역이 해당된다. 가용성에서 다루는 성능 관리나 백업, 복구, 사고대응은 기존의 보안관리와 마찬가지로 IT 서비스의 필수 통제이나 통제방식이 달라진다. 가상화와 분산구조에 따른 백업과 복구 대책, 성능, 확장성 면에서 세부 통제내용이 추가되어야 한다. 추가할 세부 통제로서 가상화이미지 백업 대책, 컴퓨팅 자원의 자동화된 복구 및 성능 관리[7], 성능 관리와 연계한 DDoS 대책 마련, 네트워크 이중화, 다양한 단말 접속 지원, API 표준화[6], 성능 및 안정성 테스트 등이 있다[11].

3.1.5 분산기술과 가상화기술[19]

분산기술과 가상화기술[4]은 기존 ISO27001에서는 다뤄지지 않은 클라우드 서비스의 근간이 되는 기술이다. 분산기술은 저비용의 대규모 컴퓨팅 자원을 연동하여 활용성 및 가용성을 향상시킴으로써 비용을 절감하고, 가상화기술은 실시간 자원의 변경, 가상 머신의 라이브 마이그레이션 등 매우 유용한 기능을 제공하여 시스템의 활용성 및 유연성 향상에 크게 기여하고 있는데 반해 대량연산능력의 악용이나 가상화를 제어하는 하이퍼바이저의 취약점은 큰 위협으로 동작하고 있다. ISO 27001 통신 및 운영관리와 정보시스템 도입, 개발 및 유지보수 영역과 공통점을 찾을 수는 있으나 분산기술과 가상화기술은 보안관리의 구조를 변경한다. 이전에는 각 컴퓨팅 자원(서버, 네트워크, 스토리지)별 관리 중심이었다면 분산기술과 가상화기술에서는 자원에 대한 통합 관리가 매우 중요하다. 클라우드 환경 내의 모든 자원에 대한 개별 자원 가상화 뿐만 아니라 자원에 대한 통합 관리가 이루어져야 한다. 클라우드 서비스 보안통제로는 분산환경과 가상화의 구조관리, 분산환경 하의 데이터를 저장하는 서버의 위치 변동에 따른 데이터관리방안, 하이퍼바이저 관리 방안, 자동화된 통합관리시스템 등이 필요하다.

분산환경에서는 데이터를 저장하는 서버의 위치가 지속적으로 변동되기 때문에, 개별 컴퓨팅 자원(서버, 스토리지 등)이 손상될 위험은 상대적으로 높다. 이러한 컴퓨팅 자원의 손상 시 저장 데이터의 위치 식별이나 특정 위치의 데이터 정보에 대한 식별이 어려워 복구를 어렵게 할 수 있다. 이러한 문제를 해결하기 위해 데이터의 중복 저장이나 데이터에 대한 정보인 메타 데이터의 관리가 체계적으로 이행되어야 한다.

가상화에서 하이퍼바이저는 가상머신을 제어하고 자원을 배분하는 역할을 수행한다[14]. 하이퍼바이저의 감염 및 오류는 전체 서비스에 영향을 줄 수 있으므로 클라우드관리시스템의 하이퍼바이저에 대한 관리가 중요하다[6]. 하이퍼바이저 관리방안으로는 가상머신별 자원 사용량을 제한, 디스크를 분할하여 호스트와 가상영역간의 경계 구분, 하이퍼바이저의 무결성 및 모니터링, 이력 관리, 가상화 OS의 내·외부 데이터 이용에 대한 로그 정보 관리, VDI(Virtual Desktop Infrastructure) 통신 암호화 등이다[10,11].

3.1.6 웹 인터페이스

웹 인터페이스는 클라우드 서비스 이용이 웹 인터페이스 방식을 사용하기 때문에 그동안의 웹 취약점에 의한 위협이 클라우드 서비스에서는 더욱 가중되고 있다. 특히 웹 인터페이스와 피싱 등 사회공학적 기법이 결합될 때 보안인식이 부족한 일반인의 경우 피해가 더욱 커질 수 있다. 기존 ISO 27001에서는 정보시스템 도입, 개발 및 유지보수 영역에서 어플리케이션의 보안요구사항, 정확한 처리, 개발 및 지원 보안, 기술 취약점 관리 등으로 웹 인터페이스를 포함한 통제를 구성하고 있어 클라우드 서비스에서도 기존 통제를 유지하면 된다. 다만 웹 취약점은 이용자에게 쉽게 노출되고 더욱 지능화되고 있어 고객서비스 측면에서 이용자의 안전한 사용을 위한 공지 및 교육 등의 지원이 필요하다.

웹 인터페이스 통제로는 웹 필터링, 피싱사이트 차단, 대역폭 관리, 웹 접근제어, SSL 등의 웹 서비스 통제와 이메일 보안통제 등이 있다.

3.1.7 접근통제

접근통제는 논리적 접근통제로 정보시스템, 서비스, 데이터, 네트워크 등의 이용을 인가된 이용자로 제한하는 통제이다. ISO 27001의 접근통제는 접근통제 정책, 계정과 패스워드 관리, 네트워크, 운영체제, 어플리케이션, 이동컴퓨팅 측면의 모든 접근에 대해 개별 통제하고 있다. 그러나 클라우드에서의 접근통제는 개별통제가 아닌, 통합인증이어야 하며 그에 따른 권한관리, 자원격리, VM이미지 접근통제, 다양한 단말의 접근통제, 세션보호, 모니터링 및 로그 검토 등을 주요 통제로 다루어야 한다.

클라우드 서비스의 통합인증은 운영체제, 어플리케이션, 유무선 네트워크 등의 인증을 가상머신 상에서 통합 관리해야 한다. 또한 다수의 이용자와 응용서비스 관리, 복잡한 유기적 자원의 할당을 위해서 단일의 인증을 통한 권한할당과 인증 토큰관리가 필요하다. 단일 계정을 통한 권한관리 방식의 IAM(Identity and Access Management, IAM)은 다음과 같은 주요 기능을 지원한다[6,15].

- 이용자 계정에 의한 자원할당과 회수
- 디렉터리 서비스 및 디렉터리 동기화
- 통합 SSO
- 인증 토큰관리와 자원할당
- 사용자 프로파일과 자격관리
- 특권사용자 관리
- RBAC와 정책관리

클라우드 서비스의 자원격리는 서로 다른 이용자 간의 충돌을 최소화하기 위하여 접근을 허용하는 영역을 설정하고 권한을 차등화 해야 한다. 세 번째는 VM 이미지 접근통제이다. 가상화 시스템으로부터 생성된 VM이미지를 안전하게 관리하기 위한 가상화 관리 시스템을 두어 접근통제와 증적을 확보해야 한다. 접근통제는 VM이미지의 소유주(owner)가 허용한 이용자에게 이미지 접근권한을 부여하는 것이며, 증적확보는 VM이미지의 생명주기에 따른 로그기록의 저장이다. 그 외 다양한 단말의 접근통제와 세션보호, 모니터링 및 로그 검토 등이 있다. 모바일 단말의 인증, 무선접속 인증과 통신 세션 암호기술을 적용해야 한다. 또한 서비스 상의 최대 세션 수, 계정 접속지역, 유형 등을 고려하여 세션을 정의하여 관리해야 하며, 접근을 모니터링하고 로그기록을 정기적으로 검토해야 한다.

3.1.8 법 규제 이탈

클라우드 서비스에서 데이터센터를 국외에 위치시키는 것은 법적 준거성의 문제를 유발한다. 클라우드 서비스에서 데이터는 전 세계의 데이터센터에 분산·저장될 수 있고, 여러 곳에 데이터 복사본이 존재할 수 있다. 데이터센터의 위치가 법체계가 미비하거나 국제협정을 존중하지 않는 국가 등에 위치할 경우, 시스템이나 데이터가 압수될 수 있고 법 집행을 위해 과도한 고객정보 노출이 발생할 수 있다는 문제점이 있다. 또한 영토고권이 미치지 못하는 지역에 데이터가 위치하는 경우 법적 증거자료 수집이 불가능하게 된다[16].

데이터센터의 위치에 따른 국내법 규제의 이탈 위협은 클라우드 서비스에서 등장한 새로운 위협으로 ISO 27001에서는 다루지 않고 있다. ISO 27001의 준거성 영역에 데이터센터의 위치에 대한 내용을 세부통제로 추가해야 할 것이다. 데이터센터의 위치 통제에 대해서는 서비스 가입시 데이터센터의 위치를 공지하고 국외로 데이터센터의 이전시 이용자의 사전동의와 승인을 받도록 규정해야 한다. 그 외 클라우드 서비스가 준수해야 할 관련 법은 "전자거래기본법", "전자상거래소비자보호법", "정보통신망법", "전기통신사업법", "콘텐츠산업진흥법", "개인정보보호법" 등이 있으며 이들 관련 법을 준수하여 정책 수립과 기술적 준수, 감사 등의 통제가 있다.

3.2 클라우드 서비스 보안관리[20]

본 절에서는 IT 환경 전체를 서비스로 제공받는 과정에서 이용자의 권익을 보호하기 위한 서비스 보안관리를 설계한다. 서비스 보안관리에서는 위협관리영역의 SLA/계약 분쟁 위협을 관리하며, 위협관리영역에 위협으로 식별하지는 않았으나 이용자에 대한 서비스 지원과 사업자의 사업 현황 파악이 포함된다.

기존의 정보보호관리체계는 조직 내에 물리적인 IT 환경을 구축하고 위탁운영을 병행하였으나 클라우드 서비스에서는 인프라에서부터 데이터까지 IT 서비스 전체를 위탁운영하는 방식이기 때문에 더욱 제공자의 안정된 서비스를 담보할 수 있어야 한다. 서비스 보안관리는 기존의 정보보호관리체계에서는 다루지 않은 부분이다. 온라인으로 클라우드 서비스를 이용함에 불편이 없도록 지원하고, 이용자의 서비스 계약이 공정하고 서비스 품질이 보장수준대로 이행되는지, 사업자의 기술력과 경영상태가 안정한지 등 서비스 제반환경

을 통제하는 영역이다.

클라우드 서비스 보안관리는 서비스 지원, 계약(SLA) 및 과금, 제공자 사업현황으로 구성된다. 서비스 지원은 온라인 셀프방식에 의해 서비스 구축이 가능하도록 쉽고 간단하며 편리한 서비스 사용환경을 구축하는 것이다. 이해하기 쉽고 조작이 간단한 자동화 구축시스템, 도움말 등의 기술지원 프로세스와 실시간 고객 응대, 고객지원 정책, 고객지원 조직, 고객만족도 평가 등의 고객지원 프로세스가 있다[20]. 계약 및 과금에는 계약서 또는 이용약관의 공정성과 법적 준거성, SLA에는 서비스 품질에 대한 명확한 지표 제시 및 품질 측정 방법 명시, 서비스 품질(SLA) 준수를 알려주는 월간 보고서 등, 과금체계에는 공정하고 세부적인 요금정책 및 사용기록 등의 과금내역 고지 등

〔표 2〕 클라우드 정보보호관리체계 통제영역과 통제요소

번호	통제영역	통제영역 정의	통제 요소		위협관리영역
1	서비스 운영보안	서비스의 가용성과 성능, 확장성을 보장할 수 있도록 자동화된 관리 및 모니터링, 변경관리를 준수하고 사고대응과 복구체제를 구축하여 안정적인 서비스 운영 관리를 보장해야 함.	- 성능 관리 - 확장성 관리 - 분산시스템과 가상화 관리 - 보안사고 관리 - 백업/복구 관리 - 모니터링 - 변경관리		- 가용성 (성능 및 확장성 관리)
2	서비스 데이터 보안	서비스 이용자의 데이터를 보호하기 위한 데이터 암호화를 지원하고 데이터 보안등급과 분류, 생명주기별 보호조치를 마련해야 함	- 데이터 암호화 - 데이터 분류 및 관리(보호등급, 권한관리, 백업/복구) - 데이터의 준거성		- 데이터보안
3	서비스 접근통제	서비스를 제공함에 있어 허가된 접근과 비인가된 접근을 효율적으로 통제할 수 있는 인증체계와 권한관리로 서비스의 신뢰성과 안전성을 보장해야 함.	- IAM(통합계정권한관리) - 자원격리 - 세션통제		- 접근통제
4	보안 아키텍처	서비스 처리의 정확성과 실시간성, 안정성을 보장하기 위한 정보시스템의 요소기술과 구성관리, 구성요소별 보안 특성을 관리해야 함.	- 분산시스템 구조 - 가상화시스템 구조 - 성능 및 확장성 기술 - 웹 보안 - 가상화 보안 - 스토리지 보안 - 서버 보안 - 네트워크 보안 - 단말 보안 - 어플리케이션 보안		- 분산기술 - 가상화기술 - 웹 인터페이스
5	관리적 보안	서비스 관리를 위한 방침과 지원을 수립하고, 내외부 직원의 관리 및 정보보호조직을 구성하여 정보보호 및 개인정보의 책임을 부여해야 함. 위험관리계획을 수립하고 테스트 및 개선활동으로 사업의 연속성을 확보해야 함.	- 정보보호정책 - 정보보호조직 - 정보보호감사 - 자산관리 - 인적보안 - 시설보안 - 사업연속성계획(위험평가)		- 관리보안
6	고객서비스 보안	이용자가 서비스를 이용함에 있어 불편함이 없도록 기술적 인적 지원체제를 마련하고, 서비스 계약은 관련 법에 따라 공정하게 체결되고 적정한 과금체계를 갖추어야 함. 제공업체의 안정된 사업현황을 파악할 수 있도록 경영상태를 공개하고, 보험가입 등을 통한 배상책임을 보장해야 함.	고객지원	- 기술지원 프로세스 - 고객지원 프로세스	- SLA/계약서 - 법 규제 이탈
			계약 및 과금	- 계약서(이용약관) - SLA - 과금체계 - 계약 관련 법 준거성	
			제공자 사업현황	- 기술인력 현황 - 서비스 장비 현황 - 사업 연혁 - 경영 상태 - 보험가입 등 배상책임 보장	

〔표 3〕 타 정보보호관리체계의 설계방법 및 특징 비교

번호	ISO 27001	CCM	클라우드 인증 프레임워크
개발주체	-ISO 위원회 -IEC 위원회	- CSA의 Control matrix Working Group	- 산/학/관/연 클라우드 서비스 자문위원회와 클라우드서비스 인증제도 TFT
설계방법	-	-전문가 그룹 외 ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum, NERC CIP 등 기존 관리체계 통제준수를 통한 검증〔12〕	- 클라우드 서비스 특징, IT 아웃소싱 방법론, 정부 정책과 지침, ASP 인증제도 및 관련 인증제도 참조〔20〕 - 사업자의 구현가능성과 타당성 검토, 이용자와 공청회 등 검증〔20〕
특징	국제표준 ISO community Forum 웹사이트와 논문지를 통한 ISO 관리체계 연구, 의견수렴 등을 통해 지속적으로 개선〔5〕	데이터통제와 운영관리의 클라우드 서비스 부분 반영 정보보호통제의 보편적 성향이 강함	클라우드 특성을 반영하고 서비스 유형별 평가, 사업자 평가 등의 평가항목으로 구성
클라우드 서비스 관리의 한계점	클라우드의 전반적인 관리 특성이 반영되지 않아 서비스 특성과 기술 특성, 서비스 지원에 대한 보안관리가 불가능	데이터통제와 운영관리 외에 현재까지 발표된 통제로는 기존 정보보호 관리체계와의 차별성이 없어 클라우드 서비스 특성, 기술 특성, 서비스 지원에 대한 보안관리가 불가능	논문에 나타난 평가항목은 클라우드 서비스를 평가하기 위한 목적으로 수립되었기 때문에 평가중심으로 구성되어 기술 특성과 클라우드 서비스에 필요한 보안관리가 부족함

이 있다. 제공자 사업현황에는 서비스의 원활한 제공을 보장할 수 있는 제공자의 기술인력과 서비스 장비 현황, 사업 연혁, 매출규모와 부채 등의 경영 상태, 보험가입을 통한 배상책임 보장 등이 있다〔20〕.

3.3 클라우드 정보보호관리체계 설계

클라우드 서비스 정보보호관리체계는 관리·물리·기술 관점의 보안관리와 서비스 보안관리로 구성된다. 클라우드 보안관리는 클라우드 서비스의 핵심요소를 반영하고 있는 위협관리영역을 기준으로 통제영역을 정의하고 각 통제영역의 보안요구사항을 반영하여 통제요소를 분류하였다. 클라우드 서비스 보안관리는 이용자의 권익을 보호하고 안정된 서비스 제반환경에 대한 통제로 구성하였다.

클라우드 보안관리에는 5개의 통제영역으로 설계하였다. 클라우드 서비스의 핵심은 가용성과 '성능 및 확장성', 데이터 보안 이다. 가용성과 성능 및 확장성은 서비스 운영보안 영역으로 분류하였다. 가용성과 성능, 확장성은 클라우드 서비스의 기본 서비스 특성으로 모두 운영상의 보안관리로 볼 수 있다. 데이터 보안은 이용자의 데이터를 보호한다는 측면에서 서비스 데이터 보안 영역으로 분류하였다. 데이터 암호화를 비롯한 보안등급, 백업/복구 등의 데이터 관리, 생명주기별 보호조치와 이용자 권한 등 데이터 준거성 등을 포함하며 통제범위와 중요도를 고려하여 개별 통제영역으로 구성하였다. 분산기술과 가상화기술, 웹 인터페이스는 기술적 동작과 논리 구조를 다루는 보안 아키텍처 영역으로 구성하였고 접근통제는 서비스 접근통제 영역으로 구성하였다. 마지막으로 정보보호정책, 정보보호조직, 정보보호감사, 인적보안, 시설관리, 사업연속성계획(위험평가 포함) 등의 제공자 조직 내 보안관리는 관리적 보안 영역으로 구성하였다.

클라우드 서비스 보안관리는 고객서비스 보안으로 명명하였고, 온라인 셀프 환경의 기술지원 프로세스와 고객 요청을 지원하는 인적 지원서비스, SLA/계약서, 과금체계, 제공업체의 기술력, 경영 안정성 등 서비스 계약 및 서비스 사용 과정에서 발생하는 제반 문제를 해결하고 지원하는 부분으로 구성된다. 고객 지원에는 기술지원 프로세스와 고객지원 프로세스가 있으며, 계약 및 과금에는 계약서 또는 이용약관, SLA, 과금체계와 계약 관련 법 준거성이 있고, 제공자 사업현황에는 기술력, 인력, 조직, 경영 상태, 보험가입 등 배상책임 보장 등이 있다.

〔표 2〕는 클라우드 정보보호관리체계의 통제영역과 통제요소, 관련 위협관리영역을 나타낸다.

3.4 타 정보보호관리체계의 분석

본 절에서는 3.3절에서 설계한 클라우드 정보보호

관리체계와 타 정보보호관리체계의 설계방법과 구성에 대해 분석한다. 분석대상은 정보보호관리체계 국제표준인 ISO 27001과 클라우드 서비스 관련하여 클라우드의 보안을 연구하는 클라우드보안연합(CSA)의 CCM(Cloud Control Matrix)[12], 방송통신위원회에서 시행하는 클라우드 서비스 인증제 관련하여 서광규의 클라우드 서비스 인증 수립을 위한 프레임워크(이하 클라우드 인증 프레임워크)를 대상으로 한다.

일반적인 표준이나 관리체계의 수립은 요구사항을 식별하여 이를 만족하도록 설계하고 이에 대한 구현가능성과 타당성 검증을 통해 완성된다. [표 3]과 같이 CSA CCM과 클라우드 인증 프레임워크에서는 관련 분야 전문가 그룹에 의한 개발 및 검증, 기존 관리체계 통제영역에 대한 준거성을 통한 타당성 검증을 택했다. ISO 27001에서는 관리체계 수립 이후 온라인 커뮤니티를 통해 관리체계의 연구와 의견제시의 통로를 마련하고 논문지를 통해 연구를 장려함으로써 지속적인 정보보호관리체계의 개선을 이루고 있다.

본 논문에서 설계한 클라우드 정보보호관리체계에서는 클라우드 서비스 정보보호요구사항을 식별하기 위하여 신뢰기관에서 발표한 위협을 분석하였고, 식별된 요구사항을 클라우드 보안통제에 반영하였다. 관리체계로서 기본적인 보안관리가 누락되지 않도록

ISO 27001 정보보호관리체계의 모든 통제영역을 포함함으로써 국제표준 보안관리의 완전성을 유지하였다.

그 외 각 관리체계의 특징과 클라우드 서비스 관리의 한계점은 [표 3]과 같다. 타 정보보호관리체계의 클라우드 서비스 관리의 각 통제영역을 살펴보면 그 한계를 잘 알 수 있다. 설계한 클라우드 정보보호관리체계의 통제영역과 통제요소를 타 정보보호관리체계의 통제영역과 비교하면 [표 4][1]와 같다. 클라우드 위협 중 SLA/계약 분쟁, 분산기술과 가상화기술, 법규제 이탈은 ISO 27001과 CCM 모두 별도 통제하지 않고 있다. 그 외 영역에 대해서도 3.1절에서 언급한 것처럼 ISO와 CCM 모두 통제가 미흡하여 클라우드 서비스 특성, 기술 특성, 서비스 지원에 대한 보안관리가 모호한 특성을 가진다. 클라우드 인증 프레임워크 논문에서는 인증 평가 기준을 간략히 나타내고 있어 정확한 클라우드 통제여부를 논할 수 없으나 평가 중심의 설계로 인해 보안관리 내용이 부족하다고 판단된다.

설계한 클라우드 정보보호관리체계는 클라우드 인증 프레임워크와 서비스 특성을 고려해야 한다는 점에서 방향성이 일치하였으며, 서비스 지원과 사업자 현황의 통제에서는 클라우드 인증 프레임워크를 참조하였다. 그러나 위협분석으로부터 도출된 위협관리영역을 정의한 점과 위협관리영역을 기준으로 ISO 27001의 클라우드 보안통제의 한계점을 분석하고 관리체계의 통제영역을 설계한 점에서 타 클라우드 정보보호관리체계 설계와 다른 점이다. 지난 2월 1일 클라우드 인증 프레임워크를 모태로 한 클라우드 서비스(인증) 심사기준[21]이 발표되었으며 전반적인 구조에서 그 차이를 확인할 수 있다.

그러나 본 클라우드 정보보호관리체계가 실용화되기 위해서는 현재 2단계 통제영역의 설계를 3단계로 구체화해야 한다.

IV. 결 론

본 논문은 새로운 IT 서비스 패러다임으로서 클라우드 컴퓨팅 서비스의 정보보호관리체계를 설계하였다. 기존의 조직 내 IT 서비스 환경과는 다른 관점으로 IT 서비스의 위탁/제공 방식에 따른 수익형 비즈니스라는 점을 고려하여 안정적인 서비스 운영의 클라우드 보안관리 측면과 서비스 제반환경 측면으로 통제영역을 구성하였다. 또 클라우드 서비스의 핵심요소를 정보보호관리체계에 반영하고자 하였다. 클라우드 서비스의 핵심요소를 주요 위협으로부터 도출한 위협관리영역을 클라우드 관리체계의 주축으로 하고, 위협으로부터 누락될 수 있는 기본 보안관리를 위해 기존 정보보호관리체계의 모든 통제영역을 포함시켜 보안관리의 완전성을 유지하도록 클라우드 정보보호관리체계를 설계하였다. 서비스 측면에서는 온라인 셀프환경에 따른 서비스 이용을 실시간 지원하고 계약의 공정성, 과금 체계, 제공자의 사업현황을 포함하도록 설계하였다. ISO 27001의 보안관리와 클라우드의 위협관리, 비즈니스 측면의 서비스관리를 종합하여 클라우드 서비스의 보안관리와 평가를 위한 통제영역으로 서비스 운영보안, 서비스 데이터 보안, 서비스 접근통제, 보안 아키텍처, 관리적 보안, 고객서비스 보안의 6개 통제영역과 41개 통제요소를 구성하였다. 설계한 클라우드 정보보호관리체계를 타 정보보호관리체계와

1) [표 4]는 클라우드 정보보호관리체계의 통제영역과 유사한 타 관리체계의 통제영역을 나타낸 것으로 유사정도를 표시하지 않아 미미한 유사성을 보임에도 유사 통제영역으로 분류한 한계점을 가지고 있다.

〔표 4〕 클라우드 정보보호관리체계의 구성 비교

번호	클라우드 정보보호관리체계		ISO 27001	CCM	클라우드 인증 프레임워크
	통제영역	통제 요소			
1	서비스 운영보안	- 성능 관리 - 확장성 관리 - 분산시스템과 가상화 관리 - 보안사고 관리 - 백업/복구 관리 - 모니터링 - 변경관리	10.통신및운영관리. 13.정보보안사고 관리	7.운영관리 10.복구	- 가용성 - 성능 및 적합성 - IaaS 서비스 - (클라우드서비스 사업자) 네트워크 및 데이터센터의 서비스 제공 기반, 보안 - (클라우드서비스 사업자) 서비스 지속성
2	서비스 데이터 보안	- 데이터 암호화 - 데이터 분류 및 관리(보호등급, 권한관리, 백업/복구) - 데이터의 준거성	해당없음	2.데이터통제	- 보안 및 신뢰성
3	서비스 접근통제	- IAM(통합계정권한관리) - 자원격리 - 세션통제	11.접근통제	5. 정보보안 (계정, 권한, 검토 등)	- 보안 및 신뢰성
4	보안 아키텍처	- 분산시스템 구조 - 가상화시스템 구조 - 성능 및 확장성 기술 - 웹 보안 - 가상화 보안 - 스토리지 보안 - 서버 보안 - 네트워크 보안 - 단말 보안 - 어플리케이션 보안	12.시스템도입, 개발, 유지보수	9.배포관리 11.보안아키텍처	- 구조 및 적합성 - SaaS 서비스
5	관리적 보안	- 정보보호정책 - 정보보호조직 - 정보보호감사 - 자산관리 - 인적보안 - 시설보안 - 사업연속성계획(위험평가)	5.정보보호정책 6.정보보호조직 7.자산관리 8.인적보안 9.물리적,환경적 보안 14.사업연속성관리	1. 준거성 3.시설보안 4.인적보안 5.정보보안 6.법 8.위험관리	- 보안 및 신뢰성 - (클라우드서비스 사업자) 서비스 지속성
6	고객서비스 보안	고객 지원: - 기술지원 프로세스 - 고객지원 프로세스 계약 및 과금: - 계약서(이용약관) - SLA - 과금체계 - 계약 관련법 준거성 제공자 사업 현황: - 기술인력 현황 - 서비스 장비 현황 - 사업 연혁 - 경영 상태 - 보험가입 등 배상책임 보장	15. 준거성	해당없음	- (클라우드서비스, 클라우드 사업자)고객지원 - (클라우드서비스 사업자) 일반 현황
구성개요	2단계 6개 통제영역 41개 통제요소		3단계 구성 11개 통제영역, 39개 통제목표, 133개 통제항목	2단계 11개 통제영역, 98개 통제항목	2단계 - 클라우드 서비스 평가 7개 통제영역, 30개 통제항목 - 클라우드 서비스 사업자 5개 통제영역, 23개 통제항목

설계방법과 구성에서의 차이를 비교, 분석하였다.

본 논문은 클라우드 컴퓨팅 서비스의 정보보호관리체계를 제안하여 객관적인 서비스 측정을 가능하게 하고 안전한 클라우드 서비스를 정착시키는데 기여할 것이다.

참고문헌

〔1〕 Brend Grobauer, Tobias Walloschek, Elmar Stocker, "Towards a cloud-specific Risk Analysis Framework", Siemens IT Solutions and Services, pp. 6-22, April 2010

〔2〕 민영기, 장연욱, "범국가 차원의 ICT신기술 패러다임 : 클라우드 컴퓨팅 활성화 전략" CIO \Report vol 17, pp, 1-12, 2009년 11월

〔3〕 박춘식, "클라우드 컴퓨팅에서의 보안 고려사항에 관한 연구", 한국산학기술학회논문지 vol. 12 No. 3, pp.1408-1416, 2011년 9월

〔4〕 김재열, 차규일, 김영호, 강동재, 임은지, 정성인, "그린 운영체제 동향", 전자통신동향분석 제24권 제4호, pp. 99-111, 2009년 8월

〔5〕 ISO/IEC, "ISO/IEC 27001:2005 - Information security management systems-Requirements", http://www.17799.com/, October 2005.

〔6〕 이강찬, 이승윤, "클라우드 컴퓨팅 표준화 동향 및 전략", 전자통신동향분석 제25권 제1호, pp.90-99, 2010년 2월

〔7〕 김창수, 김학영, 남궁한, "클라우드 서비스를 위한 대규모 클러스터 관리기술 개발", 전자통신동향분석 제24권 제4호, p. 89-98, 2009년 8월

〔8〕 금융보안연구원, "금융부문 클라우드컴퓨팅 보안 가이드", 10(2), pp. 15-22, 2010년 11월.

〔9〕 은성경, 조남수, 김영호, 최대선, "클라우드 컴퓨팅 보안 기술", 전자통신동향분석 제24권 제4호, pp. 79-88, 2009년 8월

〔10〕 이경호 외, "클라우드 컴퓨팅 서비스 보안관리 가이드라인 수립 프로젝트 최종 보고서", 한국인터넷진흥원, 2010년 11월

〔11〕 20111011_클라우드_서비스_정보보호_안내서_원본(최종).pdf, 한국인터넷진흥원, 2011년 10월.

〔12〕 "CSA CCM", https://cloudsecurityalliance.org /research/initiatives/ccm/, CSA, 2010.

〔13〕 Shilpashree Srinivasamurthy, Davic Q. Liu, "survey on cloud computing security", 2nd IEEE International Conference on Cloud Computing Technology and Science, pp. 1-8, November 2010.

〔14〕 김지연, 김형종, 박춘식, 김명주, "클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석연구", 정보보호학회지 제 19권 제4호, pp. 72-77, 2009년 8월

〔15〕 SecaaS working Group, "defined categories of service 2011", https://cloudsecurityalliance.org /wp-content/uploads/2011/09/SecaaS_V1_0.pdf, 2011

〔16〕 이대희, 이창범 외 5인, 클라우드컴퓨팅 활성화를 위한 법제도 개선방안 연구, 한국인터넷진흥원, pp. 1-307, 2010년 12월

〔17〕 CSA, "Security Guidance for critical areas of focus in cloud computing v2.1", Cloud Security Alliance, pp. 1-76, 2009년 12월

〔18〕 클라우드 SLA 가이드 도입방안, 방송통신위원회, 2011년 10월

〔19〕 클라우드 컴퓨팅 확산의 10가지 장애요인과 기회요인, 한국소프트웨어진흥원, "SW Insight", pp 94, 2009년 5월

〔20〕 서광규, "클라우드 서비스 인증 수립을 위한 프레임워크", 정보화정책저널 제18권 제1호, pp. 24~44, 2011년 봄호

〔21〕 한국클라우드서비스협회, "클라우드 서비스(인증)심사기준", http://www.excellent-cloud.or.kr /common/download.asp?downfile=클라우드 서비스 심사기준.pdf&path=board, 한국클라우드서비스협회, 2012년 2월

〈著者紹介〉

신 경 아 (KyoungA Shin) 종신회원
1993년 2월: 광운대학교 전자계산학과 졸업
2001년 2월: 한국교원대학교 교육대학원 컴퓨터교육학과 교육학석사
2008년 3월~2010년 7월: 고려대학교 정보경영공학전문대학원 정보보호학과 석사 수료
2010년 9월~현재: 에이쓰리시큐리티 수석 컨설턴트
〈관심분야〉 정보보호, 클라우드보안, 정보보호관리체계, 정보보호교육

이 상 진 (SangJin Lee) 종신회원
1987년 2월: 고려대학교 학사 졸업
1989년 2월: 고려대학교 석사 졸업
1994년 8월: 고려대학교 박사 졸업과정 수료
1989년 10월~1999년 2월: ETRI 연구원 역임
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 디지털 포렌식, 모바일 포렌식, 심층 암호, 해쉬 함수