Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1277

클라우드 컴퓨팅 정보보호 프레임워크에 관한 연구

김 정 덕,[1†] 이 성 일[2‡]
[1]중앙대학교, [2]딜로이트 안진회계법인

A Research on the Cloud Computing Security Framework

Jung-duk kim[1†], Seong-il Lee[2‡]
[1]Chung-ang University, [2]Deloitte Anjin LLC

요 약

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. 이를 위해 본 논문에서는 전략적 연계 모델을 참조하여 클라우드 컴퓨팅 정보보호 프레임워크를 제시하였다. 클라우드 컴퓨팅 정보보호 프레임워크는 클라우드 위협, 보안통제 활동, 클라우드 이해관계자를 중심 축으로 합목적성, 책임성, 투명한 책임소재의 벽면으로 구성된다. 중심 축은 클라우드 환경에서 정보보호 활동을 수행하는 주요 목적인 위협 최소화목표와 이해관계자를 지정하고 그들이 해야 할 정보보호 활동을 정의하고 있다. 또한, 3개 벽면은 클라우드 환경에서 정보보호 활동을 수행하기 위한 원칙이며 중심 축 간의 접점에서 7개 서비스 패키지 도출을 위한 방향을 제공한다.

ABSTRACT

Cloud computing's unique attributes such as elasticity, rapid provisioning and releasing, resource pooling, multi-tenancy, broad-network accessibility, and ubiquity bring many benefits to cloud adopters(company and organization), but also entails specific security risks associated with the type of adopted cloud and deployment mode. To minimize those types of risk, this paper proposed cloud computing security framework refered to strategic alliance model. The cloud computing security framework has main triangles that are cloud threat, security controls, cloud stakeholders and compose of three sides that are purposefulness, accountability, transparent responsibility. Main triangles define purpose of risk minimization, appointment of stakeholders, security activity for them and three sides of framework are principles of security control in the cloud computing, provide direction of deduction for seven service packages.

Keywords: Cloud Computing, Information Security, Risk Management, Governance; Framework

I. 서 론

인터넷 기술의 급격한 발달은 IT 운영 패러다임의 변화와 혁신을 주도하고 있다. 이러한 패러다임 속에서 클라우드 컴퓨팅은 IT자원을 필요한 만큼 빌려서 사용하는 기본 개념을 내재하고 있으며 서로 다른 조직을 하나의 IT 인프라로 묶어주는 "Extended Enterprise"의 기반을 제공한다.

정보화 시대의 기업들은 IT를 전담하는 전문 인력을 고용 및 육성해야 하는 비용 부담을 갖게 되었으며 대규모 정보처리 설비(컴퓨터, 네트워크 장비, 소프트웨어, 응용프로그램 등)를 설치, 운영 및 유지보수 해야 하는 투자가 필요하기 때문에 다루기 어렵고 복잡한 IT를 자체적으로 운영하는 것보다 상대적으로 낮은 비용에 외부 전문가를 활용할 수 있는 아웃소싱을 선호하게 되었으며 클라우드 컴퓨팅은 IT 아웃소싱의 보다 발전된 형태라고 할 수 있다[1].

접수일(2013년 11월 25일), 게재확정일(2013년 12월 4일)
† 주저자, jdkimsac@cau.ac.kr
‡ 교신저자, seongilee@deloitte.com(Corresponding author)

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, 채택된 클라우드 환경에 내재된 고유한 정보보호 위험을 감수하여야 한다. 따라서, 클라우드 컴퓨팅 적용을 많은 수의 기업과 기관들에게 활성화 하고 적용 기술을 진화시키기 위해서는 클라우드 보안 위협을 제거할 수 있는 대책 마련이 필수적이다[2].

본 논문에서는 클라우드 컴퓨팅 도입 및 운영 시 클라우드 공급자와 소비자, 브로커, 감사자 등 이해관계자가 어떤 위협에 어떻게 대책을 수립하고 적용해야 하는지 방향을 제공하는 클라우드 컴퓨팅 정보보호 프레임워크를 제시한다. 본 논문의 클라우드 컴퓨팅 정보보호 프레임워크는 클라우드 보안대책을 서비스 패키지로서 정의하기 위한 기준이 되며 클라우드 컴퓨팅 위험관리 체계수립의 토대를 제공한다.

본 논문의 구성은 다음과 같다.

첫째, 클라우드 컴퓨팅 정보보호 프레임워크 개발을 위한 이론적 배경을 고찰하고, 국내외 동향과 클라우드 컴퓨팅 정보보호 프레임워크의 필요성에 대해 살펴본다. 둘째, 전략 연계 모델에 기반한 클라우드 컴퓨팅 정보보호 프레임워크의 개발 과정 및 방법을 서술하고, 본 연구에서 수립한 클라우드 컴퓨팅 정보보호 프레임워크에 대해 설명한다. 셋째, 정보보호 분야 전문가들과의 포커스 면담을 통해 본 연구에서 제시한 클라우드 컴퓨팅 정보보호 프레임워크의 필요성과 실현 가능성을 검증한다. 마지막으로 연구 결과를 종합하여 결론과 연구의 한계, 향후 연구 방향을 제시한다.

II. 이론적 배경

클라우드 컴퓨팅 정보보호에 대한 국제표준은 JTC 1과 ITU-T 등 양대 국제표준기구에서 2010년경부터 시작되어 현재 진행 중에 있다.

주요 용어 정의는 국제표준으로 발간되었으며 관련 클라우드 보안아키텍처, 보안통제, 프라이버시 통제 등에 대한 표준화 작업이 현재 진행 중 이다.

NIST, ETSI 등 미국 및 유럽에서도 클라우드 보안에 대한 기준, 지침 등이 다수 개발되어 널리 사용되고 있으며, 이의 내용이 국제표준 작업에 반영되고 있다.

CSA(Cloud Security Alliance) 등 산업계에서도 보안가이드 3.0, 클라우드 보안통제 3.1 등이 개발되어 많은 기업/기관에서 참조 모델로서 사용되고 있으며, 이의 내용이 국제표준으로 반영되고 있다.

"클라우드 컴퓨팅 서비스의 정보보호 통제에 대한 최적실무(Code of practice for information security controls for cloud computing services based on ISO/IEC 27002)"라는 명칭의 국제표준으로 제정이 진행 중인 ISO/IEC 27017에서는 다음과 같이 16개 클라우드 환경의 위험 영역(domain)을 선정하였다[3](Table 1. 참조).

Table 1. Definition of Cloud Risk from ISO27017

Risk Type	Definition
Loss of governance	For public cloud deployments, customers necessarily cede control to the cloud provider over a number of issues that may affect security.
Responsibility ambiguity	Given that use of cloud computing services spans across the customer and the provider organizations, responsibility for aspects of security can be spread across both organizations, with the potential for vital parts of the defences to be left unguarded if there is a failure to allocate responsibility clearly.
Isolation failure	Shared resources and multi- tenancy are defining characteristics of public cloud computing.
Vendor lock in	Dependency on proprietary services of a particular cloud service provider could lead to the cloud service customer being tied to that provider.
Compliance and legal risks	Investment in achieving certification may be put at risk by migration to use cloud computing if the cloud service provider cannot provide evidence of their own compliance with the relevant requirements or if the cloud provider does not permit audit by the cloud service customer.
Handling of security incidents	The detection, reporting and subsequent management of security breaches is a concern for cloud service customers, who are relying on the provider to handle these matters.

Risk Type	Definition
Management interface vulnerability	Customer management interfaces of a public cloud provider are usually accessible through the Internet and mediate access to larger sets of resources than is typical with traditional hosting providers and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.
Data protection	Cloud computing poses several data protection risks for cloud customers and providers.
Business failure of the proider	Such failures could render data and applications essential to the consumer′sbusiness unavailable.
Malicious behaviour of insiders	Damage caused by the malicious actions of insiders working within an organization can be substantial, given the access and authorizations they may have.
Service unavailability	This could be caused by a host of factors, from equipment or software failures in the provider′s data centre, through failures of the communications between the customer systems and the provider services.
Migration and integration failures	Migrating to use cloud services may involve moving data and applications from the customer environment to the provider environment, with associated configuration changes.
Evolutionary risks	A cloud service that haspassed the security assessment of the customer during the acquisition phase might have new vulnerabilities introduced during its lifetime due to changes in software components introduced by the cloud service provider.
Cross border issues	One feature of cloud computing is that the cloud service provider′s systems may be located in a different jurisdiction to that of the customer - or the provider′s systems may be split across multiple jurisdictions.
Insecure or incomplete data deletion	Requests to delete cloud resources, for example, when a customer terminates the use of a cloud service with a provider, may not result in complete deletion of the customer′s data from the provider′s systems.

NIST SP 500-291에는 클라우드 컴퓨팅과의 상호운용성, 이식성, 정보보호, 접근성을 확보하기 위해 현존 표준분야의 조사 내용, 이를 통한 표준 모델, 사례, 유스 케이스, 연계성 평가 프로그램 등이 포함되어 있다. 해당 문서는 클라우드 컴퓨팅과 관련된 이해관계자에게 아래와 같이 5가지 권고사항을 전달하고 있다[2].

- 모든 이해관계자의 요구사항을 수용해야 함
- 표준 개발에 참여
- 검증되지 않은 기술을 운영 환경에 적용하기 위해 적극적인 테스트 실행
- 클라우드 컴퓨팅 표준의 구체화
- 국가 전체에 클라우드 컴퓨팅 표준 활용

NIST SP800-291에서 정보보호를 언급하는 관점은 “Cross-Function”이다. 정보보호를 하나의 독립적인 기능으로 인식하지 않고, 모든 클라우드 서비스의 안전성을 제공하기 위한 내재화된 기능으로 인지하는 관점이다. 또한 정보보호 기능을 구현하는 주체를 클라우드 공급자로 보고 있다.

클라우드 컴퓨팅 정보보호 분야를 표준화 하기 위해서는 정보보호 자체적인 기능과 성능을 고려하는 것도 중요하지만 다른 서비스에 정보보호 부분이 포함되어 서비스 성능의 저하를 최소화 하는 수준에서 최대한의 정보보호 목표를 달성하도록 프레임워크 및 서비스 패키지를 개발하여야 한다.

CSA의 OCF(Open Certification Framework)는 클라우드 제공자가 글로벌하게 인정된 신뢰할 수 있는 인증을 취득할 수 있도록 하려는 업계 주도의 계획이다.

CSA의 클라우드 정보보호 프레임워크와 통제 목적에 따라서 유연성 있고 점진적인 다중 계층 클라우드 제공자 인증을 위한 프로그램을 제공하며, 중복되는 노력과 비용을 회피하기 위해 공인회계 분야에서 개발한 제3자 평가 및 증명서를 통합하였다.

OCF는 3 단계의 신뢰(trust)를 기반으로 Fig.1.과 같이 구축하였고, 각 단계는 클라우드 서비스 제공자의 운영에 대한 점진적인 가시성과 투명성 목표 수준을 제시한다[4].

Fig.1.에서 1 단계인 STAR 자체 평가를 통해 클라우드 제공자는 CSA 클라우드 정보보호 프레임워크에 따른 컴플라이언스 상태를 보여주는 CAIQ(The Consensus Assessments Initiative Questionnaire)와 CCM(Cloud Controls Matrix) 분

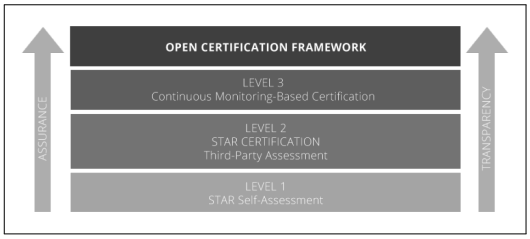

Fig.1. Structure of CSA OCF

석에 따른 2개 보고서를 제출하여야 한다.

2 단계인 STAR 인증(제3자 평가)의 개념은 CSA CCM을 통합한 ISO/IEC 27001:2005 관리체계 표준의 요구사항과 조직의 내부 요구사항 또는 명세를 사용하여 관리체계의 성숙도를 평가하는 것이다. 성숙도는 점수로 주어지며, 모든 점수는 관리체계의 각 영역에 점수를 부여하고 전체 관리체계에 대한 총점을 산정하는데 사용된다. 클라이언트는 평가자가 살펴보고 점수를 부여하는 프로세스에 자신의 내부 수행능력 기준을 추가할 수 있다.

3 단계는 인증 기반의 지속적인 모니터링으로써 현재 개발이 진행 중이며, 지속적인 감사 증적의 수집을 기반으로 소비자 요구사항을 충족하는지 여부를 실시간 모니터링 할 수 있는 기반을 구축하여야만 획득할 수 있다.

III. 프레임워크 정의

정보보호 프레임워크가 조직에서 효과적으로 작용하기 위해서는 비즈니스 및 IT와의 전략적 연계가 필수적인 요소이다. 정보보호 수준만을 강조한 정보보호 프레임워크는 효율성을 강조하는 IT와 대립하게 되며 결과적으로 비즈니스 성과를 저하하게 된다. 본 논문에서는 비즈니스 및 IT와 조화로운 정보보호 프레임워크 정의하기 위해 전략 연계 모형(strategic alignment model)에 정보보호 요건을 투영하여 클라우드 컴퓨팅 정보보호 프레임워크를 정의하였다.

3.1 전략 연계 모형의 세 축

Henderson, J. and N. Venkaraman은 전략 연계 모형을 설명하기 위해 다음과 같은 3개 요소를 축으로 IT 활동을 투영하였다[5].

- 목적(Aspiration): 비즈니스와 IT를 연계한 목적을 설명하는 축이다. 특정 비즈니스에 IT

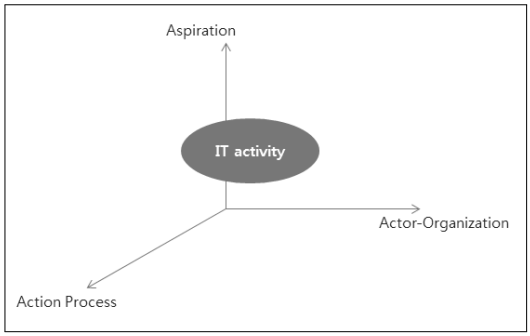

Fig.2. Strategic alliance between business and IT

를 도입한 목적을 설명하는 축으로서 클라우드 컴퓨팅은 IT활동의 일환으로 볼 수 있다.

- 프로세스(Action Process): IT활동에 대한 기준을 제시하는 메타 활동을 설명하는 축이다.
- 주체(Actor-Organization): IT활동의 주체를 설명하는 축이며 해당 활동의 이해관계자를 포함한다.

클라우드 컴퓨팅 정보보호 프레임워크의 기본 구조로써 Fig.2.의 전략 연계 모델을 활용하기 위해 클라우드 컴퓨팅을 주요 IT활동으로 간주하였으며 목적, 프로세스 및 주체는 전략 연계 모형의 원론적인 의미를 반영하여 정보보호 관점에서 재정의 하였다(Fig.3. 참조).

Fig.3.에 나타난 바와 같이 중심 축인 목적, 프로세스 및 주체를 정보보호 관점에서 재정의하기 위한 고려사항은 다음과 같다.

- 목적: 클라우드 컴퓨팅을 IT활동으로 본다면 정보보호 측면에서는 제거해야 하는 대상인 위협

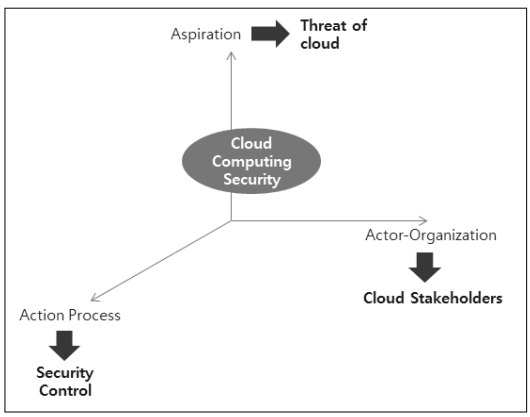

Fig.3. Redefinition of main triangles

요소를 의미한다.

- 프로세스: 클라우드 컴퓨팅 정보보호 측면에서는 목적(위협요소 제거)를 달성하기 위한 활동인 보안통제 활동으로 설명될 수 있다.
- 주체: 클라우드 컴퓨팅 활동을 수행하는 주체와 클라우드 컴퓨팅의 위협요소를 제거하는 주체는 동일하기 때문에 정보보호 프레임워크 정의 시 이해관계자가 달라지지 않는다.

3.2 클라우드 컴퓨팅 정보보호 프레임워크의 세 축

클라우드 컴퓨팅 정보보호 프레임워크는 전략 연계 모델에 기반하여 "목적"은 클라우드 위협으로, "프로세스"는 보안통제 활동으로, "주체"는 클라우드 이해관계자로 세 축을 구성한다(Fig.3. 참조). 또한, 클라우드 위협, 보안통제 활동 및 클라우드 이해관계자에는 개별 축을 정의하기 위한 세부 구성요소가 존재한다(Fig.4. 참조).

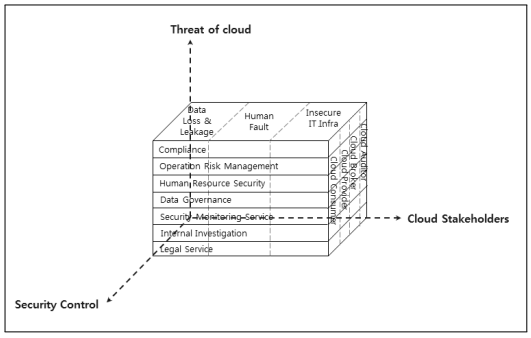

Fig.4. Main triangle of framework

목적 축은 클라우드 컴퓨팅의 제거대상 위협을 나타내며 CSA에서 Survey한 클라우드 환경의 9개 위협 요소를 기준으로 한다[6]. 본 논문에서는 9개 위협요소를 실제 리스크가 발생하는 대상(Data, IT)과 발생시키는 주체(Human)로 구분하여 다음의 3가지 유형으로 그룹핑 하였다.

- 데이터 손실과 유출(Data Loss & Leakage)
  - 불법 데이터(Data Breach)
  - 데이터 손실(Data Loss)
- 사람의 고의나 실수(Human Fault)
  - 계정이나 서비스 트래픽 탈취 (Account or Service Traffic hijacking)
  - 악의적인 내부자 (Malicious Insiders)
  - 클라우드 서비스의 오남용 (Abuse of Cloud Service)
  - 불충분한 책임의식(Insufficient Due Diligence)
- 안전하지 않은 IT 인프라 (Insecure IT Infra)
  - 안전하지 않은 인터페이스와 응용프로그램 기반 구조 (Insecure Interfaces and API's)
  - 서비스 거부 (Denial of Service)
  - 기술 공유 취약점 (Shared Technology Vulnerability)

보안통제 활동 축은 위협제거를 목적으로 수행하는 활동을 나타내며, NIST SP500-299에 언급된CSA TCI-RA 2.0의 비즈니스 운영 지원 서비스(BOSS: Business Operation Support Service)를 참고하였다[7].

비즈니스 운영 지원 서비스는 비즈니스 운영의 기밀성, 무결성, 가용성을 지원할 수 있는 7개 유형의 정보보호 활동을 정의하고 있다.

- 운영 리스크 관리: 비즈니스 운영에 부정적인 영향을 주는 각종 리스크를 관리하는 활동
- 인적자원 보안: 인력의 고의나 실수에 의한 보안사고를 관리하기 위해 교육 제공, 보안서약서 징구 등 인력을 관리하는 활동
- 데이터 거버넌스: 데이터 공유에 대한 보안 정책, 접근 원칙 등을 정의하는 활동
- 정보보호 모니터링 서비스: 정보보호시스템이나 IT 인프라에서 제공하는 보안 경고(Alert)나 로그를 지속적으로 모니터링하고 문제 발생 시 대응체계를 가동하는 활동
- 내부 사고조사: 정보보호시스템이나 IT 인프라에 저장된 보안로그를 조사하여 침해 여부 판단이나 보안사고를 조사하는 활동
- 준거성: 클라우드 컴퓨팅 활용 시 준수해야 하는 조직 간의 정보보호 정책 및 관련 법률 준수를 지원·모니터링 하는 활동
- 법률 지원 서비스: 개인정보보호 등 클라우드 환경에서 발생 가능한 법률 분쟁이나 조정 건을 해결하는 서비스

클라우드 이해관계자 축은 NIST SP500-291에서 제시하는 4개 이해관계자 그룹을 참조하였다[2]

- 클라우드 사용자Cloud Consumer): 클라우드 공급자와 사업적인 관계를 유지하면서, 클라

우드 서비스를 활용하는 개인이나 조직
- 클라우드 감사인(Cloud Auditor): 클라우드 서비스와 정보시스템 운영 및 성능, 정보보호 수준에 독립적인 평가를 수행하는 관계자
- 클라우드 공급자(Cloud Provider): 클라우드 소비자에게 가용한 서비스를 제공하여야 하는 개인이나 조직
- 클라우드 브로커(Cloud Broker): 클라우드 서비스의 활용 및 성능관리, 서비스 전달을 담당하며, 클라우드 공급자와 소비자 간의 협상 및 관계 유지를 조율하는 개체

NIST에서는 클라우드 환경에서 정보보호 및 개인정보보호를 주관하는 이해관계자를 클라우드 공급자로 보고 있으며, 클라우드 공급자는 다른 이해관계자가 정보보호 활동을 수행할 수 있는 기반을 마련해야 한다고 언급하고 있다.

클라우드 컴퓨팅 정보보호 체계수립의 기준으로서 클라우드 컴퓨팅 정보보호 프레임워크를 활용하기 위해서는 3개 중심 축의 정의 뿐만 아니라 축의 상호 작용을 통해 파생되는 구현 시 요구사항과 요구사항의 실무적용을 위한 서비스 패키지를 정의하여 프레임워크의 완전성을 제고하여야 한다.

3.3 클라우드 컴퓨팅 정보보호 프레임워크 구현방안

클라우드 컴퓨팅 정보보호 프레임워크의 3개 중심 축을 통해 형성되는 벽면은 클라우드 컴퓨팅 환경에서 목적, 주체, 프로세스가 상호 작용하여 정보보호 활동을 수행하기 위한 원칙과 방향을 제시한다(Fig.5. 참조).

Fig.5.에 나타난 3개 벽면을 정의하면 다음과 같다.

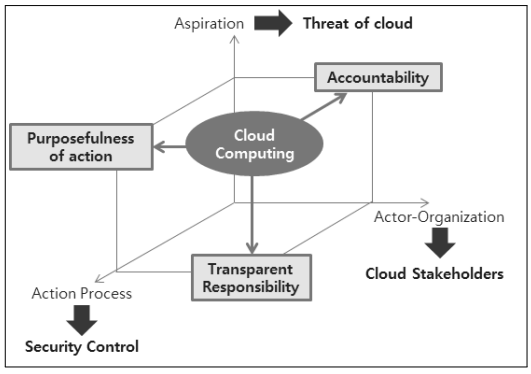

Fig.5. Deploy concept of cloud and security tp strategic alliance model

첫째, 책임성은 목적 달성을 위한 이해관계자의 역할 및 책임을 명확히 정의하는 벽면이다.

둘째, 활동의 합목적성은 무조건적인 보안이 아닌 목적 기반으로 활동(정보보호 대책)을 선택하는 방법을 정의하는 벽면이다.

셋째, 소속이 다른 클라우드 컴퓨팅 이해관계자들은 위험을 제거하는 정보보호 활동을 수행함에 있어 책임소재에 대한 대립이 있을 수 있다. 효과적인 정보보호 활동을 위해서는 이러한 책임소재를 구분할 수 있는 투명성이 필요하다.

3개 벽면은 클라우드 컴퓨팅 환경에서 정보보호 활동을 수행하기 위한 기준이며 이를 토대로 필요한 서비스 패키지를 도출할 수 있다.

3.4 서비스 패키지 도출

본 논문에서 제시하는 클라우드 컴퓨팅 정보보호 프레임워크는 전략 연계 모델에 클라우드 컴퓨팅과 정보보호를 투영한 3개 중심 축 및 벽면을 명확히 정의하고 필요한 서비스 패키지를 도출하는 것이다. 서비스 패키지 도출을 위해 클라우드 위협 축과 보안통제 활동 축의 접점인 활동의 합목적성을 분석하여 필요한 활동을 목록화 하였다(Fig.6. 참조).

Fig.6.에 나타난 바와 같이 "합목적성" 충족을 위해서 7개 정보보호 활동이 도출되었다.
- 정보보호 거버넌스: 모든 클라우드 위협을 대응하기 위한 기반으로서 선정되었음
- 데이터 보안: On/Off-line 데이터에 존재하는 위협에 대응 및 데이터 거버넌스 실행 기반
- 클라우드 컴퓨팅 통합 계정관리: IT서비스 운영 및 사용자 관리의 핵심이며 데이터 측면 보다는 사람과 IT에 존재하는 위협에 주로 초점을 둠

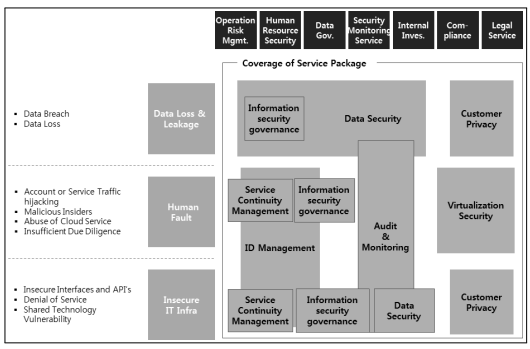

Fig.6. Security control for "purposefulness"

- 서비스 연속성 관리: 운영 리스크 관리를 위한 핵심 활동이며 사람 및 IT에 존재하는 위협을 포괄함
- 감사 및 모니터링: 정보보호 모니터링 및 내부 사고조사를 구현하기 위해 클라우드 위협 전반적으로 활용됨
- 고객 개인정보보호: 고객 개인정보 자체에 초점을 두고 있으며 법률 및 규제에 대한 준거성 구현을 위해 활용됨
- 가상화 보안: 개인정보보호법 및 정보통신망법에서 요구하는 망분리와 밀접한 관련이 있으며 주로 사람의 고의나 실수로 인한 손실에 대응하기 위해 활용됨

도출된 7개 정보보호 활동은 서비스 패키지의 핵심 구성요소이며 투명성과 투명한 책임 소재의 구현을 위한 서비스 패키지로서도 활용된다.

클라우드 정보보호 프레임워크의 벽면 중 책임성은 클라우드 이해관계자가 위협을 최소화 하기 위한 역할 및 책임을 의미한다(Fig.7. 참조). 이를 클라우드 환경에서 구현하기 위해서는 위협을 통제하기 위한 수단으로서의 활동과 활동에 대한 개별 이해관계자의 관점을 이해하여야 한다.

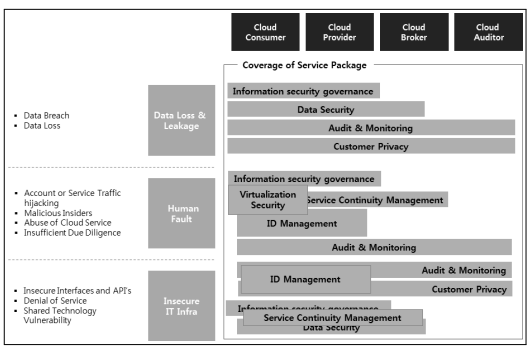

Fig. 7. Security control for "accountability"

예를 들어 "클라우드 컴퓨팅 환경에서 통합계정관리"를 구현하기 위해 클라우드 공급자와 사용자, 감사자의 입장은 서로 다르다. 클라우드 공급자는 계정관리를 위한 프로세스와 시스템을 구현하여야 하는 입장이고 클라우드 사용자는 사용자의 인증정보와 계정관리 정책을 제시하여야 한다. 클라우드 감사자는 클라우드 공급자가 클라우드 사용자의 정보를 안전하게 관리하는지, 법과 정책을 준수하는지 모니터링 하는 것이 역할이기 때문에 서비스 패키지를 정리하기 위해서는 이러한 관점들이 모두 반영되어야 한다.

마지막으로 투명한 책임소재 벽면은 클라우드 이해관계자에게 할당된 보안통제에 대한 책임의 한계를 표현하고 있다. 개별 서비스 패키지(정보보호 활동)는 클라우드 이해관계자의 책임 영역을 표시하고 있다(Fig.8. 참조).

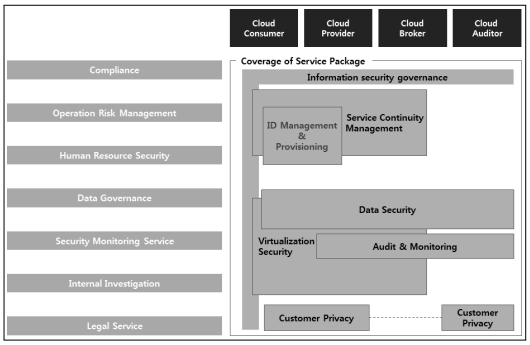

Fig.8. Security control for "transparent responsibility"

Fig.8.에 나타난 바와 같이 "정보보호 거버넌스" 서비스 패키지는 모든 이해관계자와 보안통제 활동에 넓게 분포하고 있으며 다른 서비스 패키지는 개별 이해관계자의 목적에 따라 할당되어 있다. 또한, 클라우드 공급자와 사용자가 클라우드 브로커나 감시자에 비해 상당적으로 많은 정보보호 책임을 소유하고 있음을 표현하고 있다.

IV. 전문가 의견

이 장에서는 본 논문에서 제안한 클라우드 컴퓨팅 정보보호 프레임워크에 대한 GRC(Governance, Risk, Compliance)연구회(포커스 그룹) 7명의 전문가 의견을 정리하였다.

현재 클라우드 컴퓨팅 정보보호 프레임워크에 대한 학술적 연구와 프레임워크에 대한 검증 방법을 제시한 선행연구가 미흡한 상태이므로 유사 선행 연구를 참조하여 정보보호 분야의 전문가들로 구성된 포커스 그룹 인터뷰를 수행하였다. 인터뷰 기준 및 방법을 정의하기 위해 참조한 선행 연구는 다음과 같다.

Cabrera et. al.(2008)은 조직적 해결과제의 우선순위를 결정하기 위한 중요도와 실현 가능성을 5점 척도를 이용해 결정하였다. 한편, 도출된 문제의 중요도가 높지만 실현 가능성이 낮은 경우 또는 중요도는

낮지만 실현 가능성이 높은 경우에는 전문가의 의견을 수렴해 우선순위를 부여하였다[8].

Sork(1982)은 우선순위 결정을 위해 5가지의 중요도 평가 기준과 3가지의 실행 가능성 평가기준에 따른 개별 선호도를 평가하고, 각각의 평가 점수들을 합산하는 집합적 의사결정(Aggregated Decision) 방법을 제시하였다[8].

본 연구에서는 Cabrera et. al.(2008)의 중요성과 실현 가능성을 검증 항목으로 사용하여 Fig.9.와 같이 프레임워크의 적정성을 판단하였다.

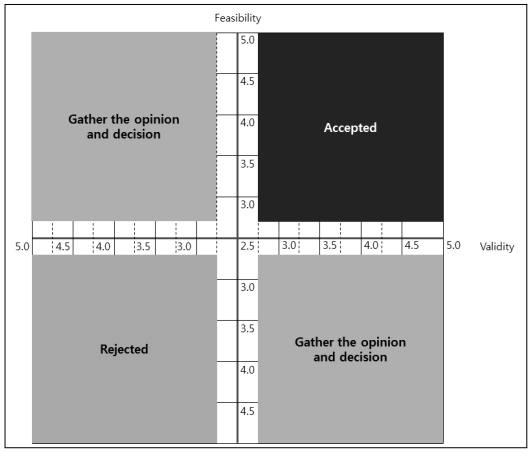

Fig.9. Verification matrix

Cabrera et. al.(2008)의 중요도와 실현가능성을 검증항목으로 적용하는 과정에서 도입 과도기에 있는 클라우드 컴퓨팅의 특성을 고려하여 중요도를 적용의 타당성으로 변경하였고 다음의 [표 2]와 같이 조작적 정의를 수행하였다.

또한, 검증 과정에서 타당성은 높지만 실현 가능성이 낮은 경우와 타당성은 낮지만 실현 가능성이 높은 경우에는 포커스 그룹의 의견을 수렴하여, 채택 및 기각 여부를 판단하였고, 타당성 및 실현 가능성이 2.5 이하인 구성 요소는 부적합한 것으로 기각하였다.

Table 2. Operational definition of verification items

Item	Operational Definition
Validity	The validity as component of cloud computing security framework
Feasibility	The feasibility as component of cloud computing security framework

포커스 그룹 인터뷰를 수행하기 위해 연구소 및 정보보호 분야의 전문가 7명이 참여한 포커스 그룹을 구성하여 설문과 심층 면접을 수행하였다. 설문은 도출된 클라우드 컴퓨팅 정보보호 프레임워크 구성 요소의 타당성과 실현 가능성을 측정하기 위해 리커드 5점 척도를 사용하였고, 설문 종류 후 30분에 걸쳐 참여자들 간에 의견을 교환하고, 도출된 정보보호 프레임워크 구성 요소가 중요한 이유를 연구자의 주도하에 대화형식으로 토론하였다.

포커스 그룹 인터뷰 결과, 본 연구에서 제시하고 있는 클라우드 컴퓨팅 정보보호 프레임워크의 중심 축, 파생벽면, 서비스 패키지의 구성 요소들은 "Fig.9. Verification Report"의 채택 영역에 모두 포함되었다(Fig.10. 참조).

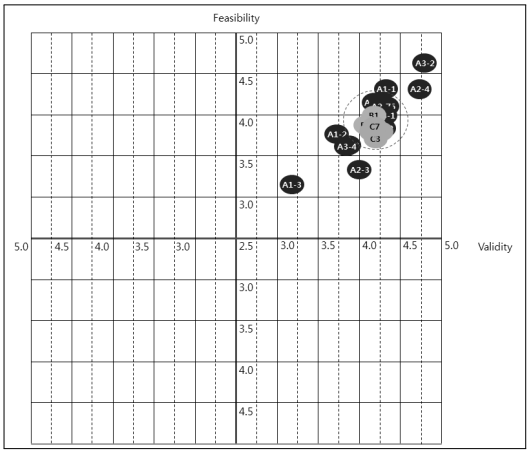

Fig.10. Result of focus group interview

포커스 그룹에 포함된 전문가들은 클라우드 컴퓨팅 정보보호 프레임워크의 타당성 및 실현 가능성을 다소 높은 수준으로 평가하였다. 이러한 평가 결과는 전문가들이 클라우드 컴퓨팅의 시장 활성화를 인정하고 있으며 이에 따른 정보보호 프레임워크의 필요성을 공감하고 있음을 시사한다. 다음의 Table 3.에는 포커스 그룹 인터뷰를 통해 파악된 클라우드 컴퓨팅 정보보호 프레임워크 구성요소의 타당성 및 실현 가능성 점수가 자세하게 정리되어 있다.

Table 3. Detailed result of focus group interview

Components of cloud computing security framework		Validity	Feasibility
A1-1	Data loss & leakage	4.4	4.4
A1-2	Human fault	3.7	3.6
A1-3	Insecure IT infra	3.1	3.2
A2-1	Operation risk management	4.3	4.3
A2-2	Human resource management	4.3	3.9
A2-3	Data governance	4.0	3.4
A2-4	Security Monitoring	4.7	4.4
A2-5	Internal Investigation	4.3	4.1
A2-6	Compliance	4.4	4.1
A2-7	Legal service	3.6	3.7
A3-1	Cloud customer	4.4	4.0
A3-2	Cloud provider	4.9	4.6
A3-3	Cloud auditor	3.9	3.6
A3-4	Cloud broker	3.9	3.6
B1	Accountability	4.2	4.0
B2	Purposefulness	4.2	3.9
B3	Transparent responsibility	4.1	3.9
C1	Security governance	4.2	3.9
C2	Data security	4.2	3.9
C3	ID management	4.1	3.8
C4	Service continuity management	4.1	3.9
C5	Audit and monitoring	4.2	3.9
C6	Client privacy	4.2	3.9
C7	Virtualization	4.1	3.9

Fig.10.과 Table 3.에 나타난 바와 같이 포커스 그룹은 “A1-3, 안전하지 않은 IT인프라”에 대해서 타당성과 실현 가능성에 상대적으로 낮은 점수를 부여하였다. 포커스 그룹 전문가와의 토의 결과, “안전하지 않은 IT인프라”는 클라우드 컴퓨팅에 고유한 이슈가 아니며 IT에 내재된 고유 위험이므로 클라우드의 주요 목적이 되기는 어렵고, 클라우드 컴퓨팅 IT 인프라에만 한정적인 보안대책을 구현하는 것도 현실적이지 않다는 의견이었다. 이러한 연구 결과는 향후 연구에서 보다 클라우드 컴퓨팅 정보보호에 고유한 서비스 패키지를 생성하고 국내외 기업들이 어떻게 이들을 활용하는가에 대한 추가적인 연구가 필요함을 시사한다.

V. 결론 및 향후 연구

본 논문은 전략적 연계 모델을 참조하여 클라우드 컴퓨팅 정보보호 프레임워크를 정의한 개념적 연구이다. 클라우드 컴퓨팅 정보보호 프레임워크는 클라우드 위협, 보안통제 활동, 클라우드 이해관계자를 중심 축으로 합목적성, 책임성, 투명한 책임소재의 벽면으로 구성된다. 중심 축은 클라우드 환경에서 정보보호 활동을 수행하는 주요 목적인 위협 최소화와 이해관계자를 지정하고 그들이 해야 할 정보보호 활동을 정의하고 있다. 또한, 3개 벽면은 클라우드 환경에서 정보보호 활동을 수행하기 위한 원칙이며 중심 축 간의 접점에서 7개 서비스 패키지 도출을 위한 방향을 제시하였다. 클라우드 컴퓨팅 정보보호 프레임워크는 최근 IT의 주요 이슈로 자리 잡은 클라우드 컴퓨팅의 정착을 위한 핵심 요구사항인 정보보호 이슈 해결의 기준이 될 것으로 기대된다. 예를 들어, 클라우드 컴퓨팅을 제공하는 기업의 보안담당자와 클라우드 컴퓨팅을 활용하는 기업의 보안담당자가 쟁점 사항에서 협의할 수 있는 기준과 원칙으로서도 활용 가능할 것으로 판단된다.

클라우드 컴퓨팅 환경에서 정보보호 활동을 수행하기 위한 개념적 틀을 제시하는 본 논문의 정보보호 프레임워크는 다음과 같은 한계점을 내재하고 있다.

첫째, 개념을 정리하여 논리를 전개하는 연구의 특성 상 실증연구에서 활용하는 통계적 검증 방법 적용이 어렵다. 이러한 한계를 극복하기 위해 향후 연구를 통해 구체적인 활용 사례를 개발하고 사례 연구 기법을 활용한 연구를 전개할 계획이다.

둘째, 클라우드 컴퓨팅 환경에서 정보보호 분야는 이전부터 논의되었던 이슈이지만 이론적 기반이 현재 미흡하며 국내의 경우 명확한 클라우드 환경을 구축한 기업들이 극히 드물게 존재하기 때문에 연구를 전개하는 과정에서 학술적 참고문헌 및 Best Practice 취합에 제약사항이 존재하였다. 이러한 제약사항을 극복하기 위해 본 논문에서는 ISO, NIST, CSA 등 국제 표준 및 해외 연구 기관의 자료를 주로 참조하였으나 향후에는 국내외 기업들의 적용 사례를 심층 연구하여 실무 공헌에 연구의 초점을 두고자 한다.

References

[1] National Standard Coordinator Office, “Standard framework of cloud computing,” Working Deliverables, Korea Agency

for Technology & Standards, MINISTRY OF TRADE, INDUSTRY & ENERGY, Dec. 2012.
〔2〕 NIST Cloud Computing Standards Roadmap Working Group, "NIST Cloud Computing Standards Roadmap", NIST SP500-291 Version 2, July 2011.
〔3〕 ISO/IEC JTC1 SC27, "Information technology -- Security techniques -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002", ISO/IEC WD 27017, October 2013.
〔4〕 CSA, "Open Certification Framework," Working Deliverables, Cloud security alliance, August 2012.
〔5〕 Henderson, J. and N. Venkaraman, "Strategic Alignment: Leveraging IT for transforming organizations," IBM Systems Journal, V32 N1, 1993.
〔6〕 CSA, "The Notorious Nine Cloud Computing Top Threat in 2013," Working Deliverables, February 2013
〔7〕 NIST Cloud Computing Security Working Group, "NIST Cloud Computing Security Reference Architecture", NIST SP500-299, pp. 245-267, May 2013.
〔8〕 Cabrera, D., J. T. Mandel, J. P. Andras, & M. L. Nydam, "What is the crisis? Defining and prioritizing the world's most pressing problems," Front Ecol Environ, pp.469 - 475. 2008.

〈저자소개〉

김 정 덕 (Jungduk Kim) 종신회원
1979년 2월: 연세대학교 정치외교학과 졸업
1981년 2월: 연세대학교 경제학과대학원 석사
1986년 2월: Univ. of S. Carolina, MBA
1990년12월: Texas A&M University, Ph.D. in MIS
1991~1993: 한국전산원, 선임연구원
1995~현재: 중앙대학교, 교수
〈관심분야〉 정보보호 GRC, People-Centric Security

이 성 일 (Seongil, Lee) 종신회원
1998년 2월: 중앙대학교 정보시스템학과 졸업
2002년 2월: 중앙대학교 정보시스템학과 석사
2011년 8월: 동국대학교 경영정보학과 박사
2011년 12월~현재: 딜로이트 안진회계법인 기업 리스크 자문본부
관심분야: 정보보호 거버넌스, 정보보호관리체계, IT 위험관리