ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

클라우드 서비스 도입을 위한 보안 중요도 인식에 대한 연구☆

The Important Factors in Security for Introducing the Cloud Services

윤 영 배[1] 오 준 석[2] 이 봉 규[1*]
Young Bae Yoon Junseok Oh Bong Gyou Lee

요 약

클라우드 서비스는 2008년 대기업의 기업용 서비스로 우리나라에 도입되었으나, 그 효과에 대한 인식이 높아짐에 따라 중소기업은 물론 공공기관까지 도입을 추진하는 등 중장기적으로 확산될 조짐이다. 그동안 많은 연구에서 클라우드 서비스 활성화의 저해요인으로 보안문제를 지적하였으나 예상되는 보안위협과 함께 대응 기술만을 제시하는 수준이었다. 이에 본 연구에서는 클라우드 서비스를 사용 해본 경험이 있는 기업 종사자들을 대상으로 이들이 인식하고 있는 보안위협의 중요도에 대하여 분석하였다. 이를 위해 클라우드 서비스 보안 영역을 관리적, 물리적, 기술적 보안으로 구분하고 각 영역별 세부요인들을 도출하였다. 순서화 로짓 모형을 통해 각 영역 및 세부 요인별 중요도를 분석한 결과 물리적 보안과 관리적 보안의 중요성을 높게 평가하는 것으로 나타났다. 또한 각 영역별로 보안정책, 서비스 시설에 대한 출입감시/통제 및 어플리케이션 보안을 중요하게 인식하는 것으로 확인되었다. 본 연구결과는 클라우드 서비스를 도입한 기업 종사자들의 실제 사용경험을 바탕으로 그들이 인식하는 보안위협 우선순위를 제시하여 향후 클라우드 서비스를 도입하려는 기업 및 기관들의 보안전략 수립에 도움이 될 것으로 기대된다.

☞ 주제어 : 클라우드 서비스, 보안 중요도, 순서화 로짓 모형

ABSTRACT

The cloud service has become the significant factor to save the IT operation cost and to improve the productivities in companies. It was introduced to Korea for enterprise services of major companies in 2008. As the increase of recognition for its effect, more small businesses and public institutions plan to introduce the cloud computing services. The cloud computing researches have only focused on the security threats and response technologies to them. Therefore, this research analyzed the importances of responses to security threats in specific domains. The domains were divided into managerial, physical, and technical security. The specific factors in three domains were used for the analysis in this research as well. The ordered logit model was used for the analysis and the analysis results showed that physical security and managerial security are considered to be significantly important in the cloud computing security. The results also presented that the security policy, the control and surveillance to service infrastructure, and application security are highly important in the respect of specific factors. This research will contribute to enterprises or institutions in Korea, which want to introduce the cloud computing services, by aiding the establishment of effective security strategies.

☞ keyword : Cloud Services, Security Importance, Ordered Logit Model

1. 서 론

클라우드 컴퓨팅은 IT 자원을 직접 보유하지 않고 사용자가 필요한 시점에 필요한 만큼 사용하고 그에 상응하는 비용을 지불하는 방식이다. 이러한 특징 때문에 최근 클라우드 컴퓨팅이 기존의 메모리, 컴퓨팅 파워, 저장 공간 등의 제약을 극복할 수 있는 방안으로 주목받고 있다.

클라우드 컴퓨팅은 IT 자원의 소유없이 일부 또는 전체를 아웃소싱하는 속성 때문에 보안문제로부터 자유롭지 못하다[1]. 클라우드 컴퓨팅 환경에서는 다양한 보안위협이 복합적으로 파생되어 정보 유출, 서비스 장애 등을 야기할 수 있는 만큼 보안위협을 제거하고 신뢰할 수 있는 서비스 환경을 구축하는 것이 중요하다. 하지만 과도한 보안수준의 적용은 비용 낭비는 물론 서비스 사용자에게 불편을 초래할 수 있는 만큼 사용자의 편의성과 서비스의 안정성을 조화롭게 반영할 수 있는 보안전략을 수립할 필요가 있다.

그동안 많은 연구들이 클라우드 서비스 활성화를 위

1 Graduate School of Information, Yonsei University, Seoul 120-749, Korea
2 Communications Policy Research Center, Yonsei University, 120-749, Korea
* Corresponding author (bglee@yonsei.ac.kr)
☆ 본 연구는 방송통신위원회의 융합방송통신전문인력양성사업의 연구결과로 수행되었음(KCA-2012-0902-1)
[Received 5 September 2012, Reviewed 24 September 2012, Accepted 15 November 2012]

한 선결과제로 보안 문제를 지적하였으나 예상되는 보안 위협과 기술적 대응방안을 나열하는 수준이었다. 하지만 기업용 클라우드 서비스를 도입하는 궁극적인 목적이 생산성과 효율성을 높여 조직 경쟁력을 강화하는 것인 만큼 보안에 대한 투자 또한 우선순위에 맞게 차별적으로 수행되어야 할 필요가 있다. 이에 본 연구에서는 현재 기업용 클라우드 서비스를 도입하여 업무에 활용 중인 기업의 종사자들이 중요하게 인식하는 보안 영역과 세부요소를 제시하고자 한다. 클라우드 서비스 보안 영역을 관리적, 물리적, 기술적 보안으로 구분하고 각 영역별 세부요소를 추가하여 분석하고자 한다. 본 연구는 기업용 클라우드 서비스 실사용자가 평가하는 보안위협의 경중을 제시함으로써 향후 기업용 클라우드 서비스를 도입하는 기업이 보안전략 수립시 활용할 수 있을 것으로 기대된다.

2. 관련 연구

2.1 클라우드 서비스

클라우드 서비스는 IT 자원을 사용자의 단말기에 직접 설치하지 않고 '원격으로 빌려쓰는' 새로운 형태의 컴퓨팅 패러다임이다[2]. 클라우드 환경에서 사용자는 단말기 성능과 무관하게 필요한 서비스만 선택하여 손쉽게 사용할 수 있다[1].

국내에서는 2008년부터 SK C&C, KT, 삼성 SDS 등 대기업 위주의 기업용 클라우드 서비스가 제공되었으며 2010년부터 개인용 클라우드 서비스가 도입되면서 다양한 IT 사업영역으로 확대되고 있다. 우리나라 정부 또한 클라우드 서비스를 국가 경쟁력을 좌우할 수 있는 중요한 수단으로 인식하여 2009년부터 5년간 공공부문의 클라우드 서비스 도입을 통해 IT 운영비용을 절감하고 세계 시장의 점유율도 향상시키겠다는 계획을 수립하여 시행 중에 있다[3].

2.2 클라우드 서비스 보안에 관한 연구

클라우드 서비스는 IT 자원의 일부 또는 전체를 아웃소싱하는 근본적인 속성 때문에 보안문제로부터 자유로울 수 없다. 시장 조사기관인 IDC에서 IT업체 임원 244명을 대상으로 클라우드 서비스 활성화를 위한 선결과제를 조사한 결과 보안문제가 선정된 바 있다[4]. CSA(2010)에서는 클라우드 컴퓨팅 보안 위협으로 컴퓨팅 남용 및 오용, 공유기술 취약점, 데이터 유실 및 유출 등 7가지를 제시하였고[5], Gartner(2008)에서는 클라우드 컴퓨팅 보안 위협을 방지하기 위한 기술적 요구사항으로 기밀성과 데이터 암호화, 사용자 인증 등 7가지를 명시하였다[6]. 또한, 김태형 등(2012)은 클라우드 컴퓨팅의 데이터 및 시스템 보안 기술을 논하였고[7], 류준상(2010), 은성경 등(2009)은 클라우드 컴퓨팅을 플랫폼, 스토리지, 네트워크 및 단말기로 구분하여 각각에 필요한 보안 기술을 제시하였다[8,9].

한편, 클라우드 서비스의 효과적인 보안을 위해 관리적, 물리적, 기술적 보안 대책의 조화를 강조한 연구도 있었다. 신경아 등(2012)은 클라우드 컴퓨팅 서비스 정보보호 관리체계를 관리・물리・기술적 관점으로 구분하였고[10], 김성준(2010)은 완벽한 클라우드 컴퓨팅 보안 기술은 없는 만큼 관리적, 물리적, 기술적 대책을 통한 대응을 강조하였다[11]. 또한 이경재(2010), 김동훈(2011)도 클라우드 컴퓨팅 환경에 특화된 관리적, 물리적, 기술적 보안대책의 수립 필요성을 제시하였다[12, 13]. 오준석 등(2012)은 클라우드 서비스 보안영역에 대해 민간기업과 공공기관 종사자들이 각각 인식하는 위협의 차이를 비교 분석한 바 있다[14].

3. 연구 모형 및 방법

3.1 연구 모형

본 연구는 변수들을 리커트 5점 척도로 측정하였으며 이는 순서형 데이터를 포함한다. 이처럼 종속변수가 순서형인 경우 선형회귀분석 모형을 사용할 수 없고 순서화 로짓 모형(Ordered Logirt Model)을 사용해야 한다[15]. 식(1)은 순서화 로짓 모형을 일반 회귀식처럼 취급하기 위해 순서화된 종속변수와 독립변수 간의 관계를 가정하고 있다.

$$y^{*} = \sum_{k=1}^{k} \beta_k x_k + \epsilon \qquad [\epsilon N(0,1)] \tag{1}$$

여기서 ε는 표준정규분포를 따르며 y*는 관찰 불가능한 응답변수로 응답자가 관찰 가능한 응답 y를 선택하는 기준을 제공한다. 응답자가 선택 가능한 응답(y)이 J개 존재한다면 y*는 1부터 J까지의 선택하는 내재적 기준이 된다.

식(2)는 범주화된 기준 y*와 관찰 가능한 응답 y의 관계를 나타낸 것이다. μ1에서 μj-1은 y*의 경계 값으로 총 J개의 관찰 가능한 응답들에 대해 특정한 j를 선택하는 기준이 된다. 일반적으로 μJ는 다양한 값으로 추정될 수 있으나 회귀분석을 위해 μ1=0으로 정규화 시켜준다.

$$\begin{aligned} y &= 1, \text{ if } \quad y^* \le \mu_1(=0) \\ &= 2, \text{ if } \quad \mu_1 < y^* \le \mu_2 \\ &\quad \vdots \\ &= J, \text{ if } \quad \mu_{j-1} < y^* \end{aligned} \tag{2}$$

순서화 로짓모형은 이산한 종속변수를 확률의 개념으로 연속성을 확보하므로 y=j를 선택할 확률 Prob(y=j)는 식 (3)과 같이 구할 수 있다.

$$\begin{aligned} \Pr ob(y=j) &= \Pr ob(\mu_{j-1} < y^* = \sum_{k=1}^{k} \beta_k x_k + \epsilon \le \mu_j) \\ &= F(\mu_j - \sum_{k=1}^{k} \beta_k X_k) - F(\mu_{j-1} - \sum_{k=1}^{k} \beta_k X_k) \end{aligned} \tag{3}$$

분석결과에 나타난 계수만으로 종속변수에 대한 독립변수의 강도를 예측할 수 없으므로 한계효과를 분석해야 한다. 특정 설명변수에 대한 확률의 한계효과는 식 (4)와 같이 정의된다.

$$\frac{\delta \Pr ob(y=j)}{\delta x_k} = [\frac{e^{\mu_{j-1} - \sum_{k=1}^{k} \beta_k X_k}}{(1+e^{\mu_{j-1} - \sum_{k=1}^{k} \beta_k X_k})^2} - \frac{e^{\mu_j - \sum_{k=1}^{k} \beta_k X_k}}{(1+e^{\mu_j - \sum_{k=1}^{k} \beta_k X_k})^2}]\beta_k \tag{4}$$

3.2 기술 통계

본 연구 수행을 위해 기업용 클라우드 서비스를 도입한 KT, SKT, 웅진 홀딩스 직원 등에게 설문조사를 실시하였다. 총 211개의 설문지를 회수하여 결측치 6부를 제외한 205부를 분석에 활용하였다.

연구 분석에 활용된 설문응답자의 인구통계학적 특성을 살펴보면, 남성이 77.6%(159명), 여성이 22.4%(46명)이었고, 20대가 33.7%(69명), 30대가 45.9%(94명), 40대가 20.4%(42명)이었다. 근무기간은 3년 미만이 52.1%(107명), 3년 이상~5년 미만 18.5%(38명), 5년 이상~10년 미만 13.7%(28명), 10년 이상이 15.6%(32명)이었다. 직장규모가 300명 미만인 중소기업 종사자는 32.2%(66명)이었고 300명이상인 대기업 종사자는 67.8%(139명)이었다.

또한, 독립변수들 사이의 독립성을 검증하기 위하여 상관분석을 실시하였다. (표 1)은 클라우드 서비스 보안 중요도 인식을 분석하기 위해 사용된 독립변수간의 상관관계를 분석한 결과이다. 상관계수(r^2)의 값이 전반적으로 0.5이하로 독립변수사이의 독립성이 검증되었다.

(표 1) 보안 중요도 인식 독립변수 상관관계 분석 결과
(Table 1) Correlations of Independent Variables

	관리적 보안	물리적 보안	기술적 보안	성별	연령	근무 기간	직장 인원수
관리적 보안							
물리적 보안	0.207						
기술적 보안	-0.108	0.166					
성별	-0.009	-0.004	0.026				
연령	-0.114	-0.001	0.031	0.313			
근무 기간	0.022	-0.000	0.167	0.162	0.565		
직장 인원수	0.026	0.126	0.018	0.093	-0.016	-0.010	

이와 함께 관리적 보안 중요도 인식을 분석하기 위한 독립변수의 r^2는 최소 0.001에서 최대 0.565로 나타났으며, 물리적 보안의 중요도 인식 분석에 활용된 독립변수간 r^2도 최소 0.005에서 최대 0.565로 확인되었다. 마지막으로 기술적 보안 중요도 인식을 분석하기 위한 독립변수의 r^2도 최소 0.002에서 최대 0.565로 나타나는 등 보안 영역별 세부 독립변수 사이의 독립성도 확보되었다.

3.3 연구 변수

앞에서 살펴본 클라우드 서비스 보안 관련 기존 연구를 토대로 본 연구의 변수를 도출하였다. 클라우드 서비스 보안영역을 관리적, 물리적, 기술적 보안으로 구분하고 (표 2)와 같이 정의하였다.

(표 2) 본 연구의 변수
(Table 2) Research Variables

연구 변수	내 용
관리적 보안	정책적・제도적・인사적 관리방법 등을 효과적으로 활용 및 보완함으로써 수행
물리적 보안	서비스 관련 시설 및 장비 보호를 위해 물리적인 요소를 통제함으로써 수행
기술적 보안	전문기술이 필요한 보안요소 활용을 통해 보안위협을 식별・제거함으로써 수행

또한 각 보안영역의 중요도 인식에 영향을 주는 세부요인을 분석하고자 선행 연구를 토대로 보안영역별 구성요소를 (표 3)과 같이 정의하였다.

(표 3) 본 연구의 변수
(Table 3) Research Variables

보안 영역	연구변수	내 용
관리적 보안	보안정책	CEO(CIO)의 지휘방침 등이 반영된 정책·절차 마련 및 정기적 리뷰
	보안조직 편성	보안 업무 수행을 위한 적정 규모의 조직 구성 및 책임·권한 부여
	보호자산 분류·통제	선별적인 보안 적용을 위한 조직내 자산 중요도 평가, 분류 및 목록화
	인적보안	전·현직 직원 및 외부인 등에 대한 보안 교육 및 각종 권한부여 관리 등
	보안사고 관리	사고 확산 방지 및 피해 최소화를 위한 보고·처리 등 일련의 대응 관리
	보안 감사	보안 지침·절차 등의 적절한 시행 여부에 대한 정기적 점검 및 보고
물리적 보안	장비/시설 위치 선정	천재지변(지진, 홍수 등)으로부터 안전한 위치 선정 및 시설 배치
	시설내 환경 통제	온도, 습도, 공기 등 환경요인에 의한 장비/시설 훼손 및 고장 방지
	출입 감시/통제	서비스 관련 시설에 대한 불법적 접근 감시 및 출입 통제(CCTV 등)
	지원 유틸리티	정전, 통신 중단 등에 대비한 자원 백업, 예비설비 보유 및 주기적 점검
	자산 반·출입 통제	주요 시설내 USB, 스마트폰, 노트북 등의 반·출입 통제
기술적 보안	단말기 보안	악성코드 감염, 개인정보 유출, 단말기 분실 등 단말기에 잠재된 보안위협
	네트워크 보안	전송 데이터 절취, DDoS 공격 등 네트워크에 잠재된 보안위협
	플랫폼 보안	운영체제 및 Hypervisor 보안 등 플랫폼에 잠재된 보안위협
	스토리지 보안	접근제어 및 자료 암호화 등을 통한 스토리지에 잠재된 보안위협
	어플리케이션 보안	프로그램·사용자 인증, 결재 보안 등 어플리케이션에 잠재된 보안위협

4. 분석 결과

4.1 클라우드 서비스 보안 영역 중요도 인식

클라우드 서비스를 사용 중인 기업의 직원들은 물리적 보안을 가장 중요하게 인식하는 것으로 나타났다. (표 4)를 보면 물리적 보안과 관리적 보안이 5% 유의수준에서 통계적으로 유의하고 물리적 보안은 $\hat{\beta}$계수가 0.7868로 클라우드 컴퓨팅 보안 중요도 인식에 가장 영향을 주는 변수로 나타난다. 여기서 $\hat{\beta}$계수는 각 변수에 대한 추정계수(coefficient)를 의미한다.

(표 4) 보안 중요도 인식에 관한 분석 결과
(Table 4) Analysis results for the awareness of the security importance

변수	$\hat{\beta}$	exp($\hat{\beta}$)	t	P
관리적 보안	0.6863	1.9863	3.1	0.002**
물리적 보안	0.7868	2.1963	3.42	0.001**
기술적 보안	0.2063	1.2292	0.88	0.378
성별	0.3063	1.3583	0.9	0.371
연령	0.0354	1.0361	1.26	0.207
근무기간	-0.0282	0.9722	-0.75	0.453
직장인원수	-0.1052	0.9001	-0.95	0.343
cut 1	6.8632	cut 2		9.4288
LR chi2-square	29.46	Log Likelihood		-195.6195

* cut 1, cut 2 : 순서화 선택에 대한 한계치

물리적 보안의 exp($\hat{\beta}$)는 2.1963인데 이것은 '클라우드 서비스 보안이 중요하지 않다' 보다 '중요하다'고 인식하는 오즈(odds)가 물리적 보안을 중요하다고 평가할 때 약 2.2배가 되는 것을 의미한다. 여기서 오즈란 선택모형에서 중요도에 대한 확률값을 의미하는 것으로 선택할 확률을 선택하지 않을 확률로 나눈 값에 해당한다. 동일한 방법으로 관리적, 기술적 보안은 각각 약 2.0배, 1.2배의 높은 오즈를 갖는다고 볼 수 있다.

(표 5) 보안 중요도 인식 한계효과 변화
(Table 5) Marginal effect changes on the awareness of security importance

변수	Prob(y=3) 보통이다	Prob(y=4) 중요하다	Prob(y=5) 매우 중요하다
관리적 보안	-0.1240	0.0147	0.1093
물리적 보안	-0.1421	0.0168	0.1253
기술적 보안	-0.0373	0.0044	0.0329
성별	-0.0577	0.0114	0.0463
연령	-0.0064	0.0008	0.0056
근무기간	0.0051	-0.0006	-0.0045
직장인원수	0.0190	-0.0022	-0.0168

(표 5)는 클라우드 서비스 보안 중요도 인식에 대한 한계효과 변화를 분석한 것이다. 클라우드 서비스를 매

우 중요하다고 인식하는 비율은 남성보다 여성이 4.6% 높았다. 또한, 물리적 보안의 중요성을 한 단계 높게 평가하면 클라우드 서비스 보안을 매우 중요하다고 인식하는 비율이 12.5% 증가하였다. 동일한 방법으로 관리적 보안 중요도의 확률변화량은 약 10.9%였다.

4.2 클라우드 서비스 관리적 보안 중요도 인식

클라우드 서비스 관리적 보안 영역 중 보안정책, 인적보안, 보안사고 관리, 보안조직 편성 등의 순으로 중요하게 인식하는 것으로 나타났다. (표 6)을 보면 보안정책 $\hat{\beta}$ 계수가 0.8324로 클라우드 서비스 관리적 보안 중요도 인식에 가장 영향을 주는 변수로 나타난다. 또한, '클라우드 서비스 관리적 보안이 중요하지 않다' 보다 '중요하다'고 인식하는 오즈가 보안정책을 중요하다고 평가할 때 약 2.3배가 되는 것으로 나타났으며, 인적보안은 약 1.9배, 보안사고 관리가 1.8배의 높은 오즈를 갖는 것으로 나타났다.

(표 7)은 클라우드 서비스 관리적 보안 중요도 인식에 대한 한계효과 변화를 분석한 것이다. 보안정책의 중요성을 한 단계 높게 평가하면 클라우드 서비스 관리적 보안을 매우 중요하다고 인식하는 비율이 19.7% 증가하였다. 동일한 방법으로 인적보안는 14.5%, 보안사고 관리는 14.2%의 확률변화량을 나타냈다.

(표 6) 관리적 보안 중요도 인식에 관한 분석 결과
(Table 6) Analysis results for the awareness of the managerial security importance

변수	$\hat{\beta}$	exp($\hat{\beta}$)	t	P
보안정책	0.8324	2.2989	3.68	0**
보안조직 편성	0.1635	1.1777	0.69	0.49
보호자산 분류·통제	0.0883	1.0923	0.44	0.661
인적보안	0.6162	1.8519	3.11	0.002**
보안사고 관리	0.5989	1.8201	2.57	0.01**
보안 감사	0.1503	1.1622	0.64	0.522
성별	0.3098	1.3631	0.87	0.382
연령	-0.0609	0.9409	-2.11	0.035**
근무기간	0.0420	1.0429	1.06	0.29
직장인원수	0.0088	1.0088	0.08	0.939
cut 1	6.2577	cut 2		9.1457
LR chi2-square	58.64	Log Likelihood		-171.1821

* cut 1, cut 2 : 순서화 선택에 대한 한계치

(표 7) 관리적 보안 중요도 인식 한계효과 변화
(Table 7) Marginal effect changes on the awareness of managerial security importance

변수	Prob(y=3) 보통이다	Prob(y=4) 중요하다	Prob(y=5) 매우 중요하다
보안정책	-0.0628	-0.1339	0.1968
보안조직 편성	-0.0123	-0.0263	0.0387
보호자산 분류·통제	-0.0067	-0.0142	0.0209
인적보안	-0.0465	-0.0991	0.1457
보안사고 관리	-0.0452	-0.0963	0.1415
보안 감사	-0.0114	-0.0242	0.0355
성별	-0.0252	-0.0464	0.0715
연령	0.0046	0.0098	-0.0144
근무기간	-0.0032	-0.0068	0.0099
직장인원수	-0.0007	-0.0014	0.0021

4.3 클라우드 서비스 물리적 보안 중요도 인식

클라우드 서비스 물리적 보안 영역 중 출입 감시/통제 ($\hat{\beta}$계수 0.3981)를 물리적 보안 중요도 인식에 가장 영향을 주는 변수로 인식하고 있었다.

(표 8) 물리적 보안 중요도 인식에 관한 분석 결과
(Table 8) Analysis results for the awareness of the physical security importance

변수	$\hat{\beta}$	exp($\hat{\beta}$)	t	P
장비/시설 위치 선정	0.2842	1.3286	1.57	0.117
시설내 환경 통제	0.3465	1.4142	1.64	0.102
출입 감시/통제	0.3981	1.4890	2.01	0.044**
지원 유틸리티	0.3969	1.4872	1.93	0.054
자산 반·출입 통제	0.2627	1.3004	1.31	0.192
성별	-0.1057	0.8997	-0.29	0.771
연령	0.0156	1.0157	0.53	0.594
근무기간	-0.0319	0.9686	-0.83	0.407
직장인원수	0.2049	1.2274	1.83	0.067
cut 1	6.1385	cut 2		9.0858
LR chi2-square	32.21	Log Likelihood		-184.5656

* cut 1, cut 2 : 순서화 선택에 대한 한계치

이와 함께, '클라우드 서비스 물리적 보안이 중요하지 않다' 보다 '클라우드 서비스의 물리적 보안이 중요하다'고 인식하는 오즈가 출입 감시/통제가 중요하다고 생각할 때 약 1.5배 높은 것으로 나타났다. 이와 마찬가지로, 지원 유틸리티는 약 1.48배, 시설내 환경 통제가 약 1.41배의 높은 오즈를 갖는 것으로 나타났다.

(표 9)는 클라우드 서비스 물리적 보안 중요도 인식에 대한 한계효과 변화를 분석한 것이다. 출입 감시/통제와 지원 유틸리티의 중요성을 한 단계 높게 평가하면 물리적 보안을 매우 중요하다고 인식하는 비율이 약 6.5% 증가하였다.

(표 9) 물리적 보안 중요도 인식 한계효과 변화
(Table 9) Marginal effect changes on the awareness of physical security importance

변수	Prob(y=3) 보통이다	Prob(y=4) 중요하다	Prob(y=5) 매우 중요하다
장비/시설 위치 선정	-0.0396	-0.0070	0.0466
시설내 환경 통제	-0.0483	-0.0085	0.0569
출입 감시/통제	-0.0555	-0.0098	0.0653
지원 유틸리티	-0.0553	-0.0098	0.0651
자산 반·출입 통제	-0.0366	-0.0065	0.0431
성별	0.0144	0.0032	-0.0176
연령	-0.0022	-0.0004	0.0026
근무기간	0.0045	0.0008	-0.0052
직장인원수	-0.0286	-0.0051	0.0336

4.4 클라우드 서비스 기술적 보안 중요도 인식

클라우드 서비스 기술적 보안 영역 중 어플리케이션 보안($\hat{\beta}$계수 0.6614)을 가장 중요하게 인식하는 것으로 나타났다.

어플리케이션 보안을 중요하다고 평가할 때 '클라우드 서비스 기술적 보안이 중요하지 않다' 보다 '중요하다'고 인식하는 오즈가 약 1.9배가 되는 것으로 나타났다. 동일하게 스토리지 보안은 약 1.6배의 높은 오즈를 갖는 것으로 나타났다.

(표 11)은 클라우드 서비스 기술적 보안 중요도 인식에 대한 한계효과 변화를 분석한 것이다. 어플리케이션 보안의 중요성을 한 단계 높게 평가하면 물리적 보안을 매우 중요하다고 인식하는 비율이 약 15.5% 증가하였다. 동일한 방법으로 스토리지 보안은 10.9%, 네트워크 및 플랫폼 보안이 약 6.5의 확률변화량을 나타냈다.

(표 10) 기술적 보안 중요도 인식에 관한 분석 결과
(Table 10) Analysis results for the awareness of the technical security importance

변수	$\hat{\beta}$	exp($\hat{\beta}$)	t	P
단말기 보안	0.1760	1.1924	0.71	0.481
네트워크 보안	0.2773	1.3195	1.13	0.257
플랫폼 보안	0.2759	1.3177	1.06	0.287
스토리지 보안	0.4650	1.5920	1.81	0.07**
어플리케이션 보안	0.6614	1.9376	2.46	0.014**
성별	0.1746	1.1908	0.47	0.636
연령	-0.0214	0.9788	-0.73	0.466
근무기간	0.0798	1.0830	1.81	0.07**
직장인원수	0.0280	1.0284	0.23	0.821
cut 1	4.6449	cut 2		7.1028
LR chi2-square	30.41	Log Likelihood		-156.7777

(표 11) 기술적 보안 중요도 인식 한계효과 변화
(Table 11) Marginal effect changes on the awareness of technical security importance

변수	Prob(y=3) 보통이다	Prob(y=4) 중요하다	Prob(y=5) 매우 중요하다
단말기 보안	-0.0082	-0.0331	0.0413
네트워크 보안	-0.0129	-0.0521	0.0650
플랫폼 보안	-0.0129	-0.0519	0.0647
스토리지 보안	-0.0217	-0.0874	0.1091
어플리케이션 보안	-0.0308	-0.1243	0.1552
성별	-0.0085	-0.0329	0.0414
연령	0.0010	0.0040	-0.0050
근무기간	-0.0037	-0.0150	0.0187
직장인원수	-0.0013	-0.0053	0.0066

5. 결론 및 시사점

본 연구는 클라우드 서비스 활성화의 가장 큰 장애요인으로 평가받는 보안위협을 실사용자들의 경험을 바탕으로 분석하였다. 클라우드 서비스에 내재된 다양한 보안위협을 기존 문헌에서 고찰하고 이를 체계화하여 변수들을 도출하였다. 이후 기업용 클라우드 서비스 실사용자에게 설문조사를 실시하고 순서화 로짓 모형으로 분석함으로써 보안 위협별 인식수준을 계량화하여 제시하였다.

기업용 클라우드 서비스 실사용자들은 물리적, 관리적 보안을 중요하게 평가하였다. 기존 연구가 기술적 위협과 그에 대한 대책을 중시한 반면, 실사용자들은 물리

적 보안과 관리적 보안의 중요성을 상대적으로 높게 인식하였다. 이는 향후 클라우드 서비스 도입 시 기술적 대책 뿐만 아니라 조직 환경 및 문화에 부합된 물리적, 관리적 보안대책 마련에도 힘써야 함을 보여준다.

관리적 보안 영역에서는 보안정책, 인적보안 및 보안사고 관리의 중요성이 높게 평가되었다. CEO(또는 CIO 등)의 확고한 의지와 방침이 반영된 보안정책이 수립되어 일사불란하게 시행되고, 전·현직 직원 및 상시출입자로부터 내부 불만자 등 취약인원에 대한 보안에 높은 관심이 요구되는 것으로 나타났다. 또한, 보안사고 발생시 효과적인 대응을 위해 구체화된 사고관리 매뉴얼을 수립하고 관련 절차를 숙달할 필요가 있을 것으로 보인다.

물리적 보안 영역에서는 출입감시/통제와 지원 유틸리티가 중요하게 인식되었다. 관리적 보안의 인원보안 중요성과 연계하여 클라우드 서비스 관련 시설에 대한 출입권한 설정을 강화하고 상시적인 감시/통제체계를 구축하여 불법적 침입 차단 및 사후 추적이 가능토록 해야 할 것이다. 또한, 통신중단이나 정전에 대비하여 자체 발전시스템 구비 또는 주요 자원 백업 등 무중단 서비스 지원의 중요성도 간과해서는 안 될 것이다.

기술적 보안 영역에서는 어플리케이션과 스토리지 보안을 중요하게 평가하였다. 어플리케이션 보안은 사용자의 관심과 의지로 상당부분 충족될 수 있는 만큼 교육을 강화하되 과도한 보안 수준적용은 사용 기피요인으로 작용할 수 있는 바 편의성과 보안성을 고려한 보안기술 적용이 필요할 것이다. 또한 중앙 집중화된 데이터의 분산이나 암호화, 차별적 접근 허용 등 스토리지 관리에도 주력해야 할 것이다.

기업용 클라우드 서비스 도입의 주요 목적이 비용절감인 만큼 보안에 필요한 투자도 위협 우선순위에 따라 선별적으로 수행될 필요가 있다. 이에 따라 클라우드 서비스에 내재된 보안위협을 실제 사용자들의 인식을 토대로 평가한 본 연구결과는 향후 클라우드 서비스 도입 기업의 보안전략 수립 시 유용하게 활용될 것으로 기대된다. 또한, 향후 기업용 클라우드 서비스 비사용자들과의 인식차이나 기업규모에 따른 인식차이를 비교하는 연구가 수행될 경우 보다 유의미한 시사점이 도출될 것으로 기대된다.

참 고 문 헌(Reference)

[1] Korea Communications Commission and Korea Internet Security Agency, “Information Security guide for Cloud Services”, 2011.

[2] S.K.Eun, “Cloud Computing Security Technology Trends”, Review of Korea Institute of Information Security and Cryptology, Vol.20, No.2, pp.27-31, 2010.

[3] Korea Communications Commission and Korea Internet Security Agency, “Information Security guide for Cloud Services”, 2011.

[4] “Asia Pacific End-User Cloud Computing Survey”, International Data Corporation, 2009

[5] Cloud Security Alliance, “Top Threats to Cloud Computing V1.0”, 2010.

[6] Gartner, “Assessing the Security Risks of Cloud Computing”, 2008.

[7] T.H.Kim, I.H.Kim, C.W.Min and Y.I,Eom, “Security Technology Trend in Cloud Computing”, Korea Information Science Society review, Vol.30, No.1, pp.30-38, 2012.

[8] J.S.Ryu, “Cloud Computing as Green IT and Security Issues”, The Graduate School of Computer Information Communications, Korea University, 2010.

[9] S.K.Eun, N.S.Cho, Y.H.Kim and D.S.Choi, “Cloud Computing Security Technology”, Electronics and Telecommunications Trends, ETRI, Vol.24, No.4, pp.79-88, 2009.

[10] K.A.Shin and S.J.Lee, “Information Security Management System on Cloud Computing Service”, Journal of the Korea Institute of Information Security and Cryptology, Vol.22, No.1, 2012.

[11] S.J.Kim, “Information Security Plan on Cloud Computing: Information Security Management System”, Management Consulting Review, Vol.2, No.2, pp.194-208, 2010.

[12] K.J.Lee, “The Study on the Issue of Cloud Computing Security and the Plans for the Personal Information Protection”, Department of Information Security, The Graduate School of Information and Communications, Sungkyunkwan University, 2010.

[13] D.H.Kim, “A Study on the improvement and application of Information Security Management System for Cloud Computing Security”, Department

of Information Security, The Graduate School of Information and Communications, Sungkyunkwan University, 2011.
[14] J.S.Oh, Y.B.Yoon, J.R.Suh and B.G.Lee, “The Difference of Awareness between Public Institutions and Private Enterprises for Cloud Computing Security”, International Journal of Security and Its Applications, Vol.6, No.3, pp.1-10, 2012.
[15] S.W.Lee, S.H.Min, J.Y.Park and S.D.Yoon, “Application of Logit and Probit Model”, Pakyoungsa, 2005.

◐ 저 자 소 개 ◑

윤 영 배
2002년 한국항공대학교 항공교통학 (학사)
2011년~현재 연세대학교 정보대학원 석사과정
관심분야 : 정보통신 정책, 정보보호, 클라우드 서비스
E-mail : charismaox@yonsei.ac.kr

오 준 석
2002년 한성대학교 정보전산학부 (학사)
2004년 충북대학교 컴퓨터과학 (석사)
2006년 The Pennsylvania State University (석사)
2010년 The Pennsylvania State University (박사)
2011년~현재 연세대학교 연구원, 연구교수
관심분야 : 정보기술 융합, 클라우드 컴퓨팅, 빅데이터 마이닝
E-mail : jseok@yonsei.ac.kr

이 봉 규
1988년 연세대학교 상경대학 (학사)
1992년 Cornell University (석사)
1994년 Cornell University (박사)
1997년~2004년 한성대학교 정보전산학부 교수
2005년~현재 연세대학교 정보대학원 교수
관심분야 : IT 정책·산업, 방송통신융합정책, 모바일인터넷
E-mail : bglee@yonsei.ac.kr