FOCUS 4

클라우드 컴퓨팅 보안 위협요소 소개와 창조경제 실현을 위한 방향성 제안

양희동*, 황세운**

클라우드 컴퓨팅은 지난 2008년,'제 2의 디지털 혁명'이라는 말까지 생길 정도로 엄청난 기대와 함께 등장하였다.5년이 지난 지금, 클라우드 컴퓨팅 기반의 서비스는 기하급수적으로 늘어나고 있고 수요도 증가하고 있다. 가트너는 전 세계 클라우드 시장이 2015년까지 957억 달러까지 늘어날 것으로 보인다고 전망하였다.그러나 클라우드 컴퓨팅은 기존 IT 환경의 보안 위협을 그대로 안고 있을 뿐 아니라 가상화의 문제, 모바일 기기를 통한 접속 시의 문제, 데이터 이전에 관한 불안감 등으로 인하여 신규 공격의 위협이 증가하고 있다. 또한 사용자가 점차 늘어감에 따라 서비스의 규모가 커짐으로 해서 침해사고도 대형화 되고 피해액도 증가되고 있으며 이것으로 인해 사용자들의 클라우드 컴퓨팅 서비스에 대한 불안감이 증가되고 있다.전 세계적으로 클라우드 컴퓨팅의 보안에 관한 연구가 계속되고 있지만 아직 국내에서는 그 대응책이 미흡한 실정이다. 따라서 본 연구에서는 클라우드 컴퓨팅을 위협하는 요소와 방지책, 해외 각국의 클라우드 컴퓨팅 보안에 관한 정책을 소개하고 창조경제 시대에 맞는 클라우드 컴퓨팅 보안에 관한 방향성을 제시해 보고자 한다.

*이화여자대학교 경영대학 경영학과 교수 (hdyang@ewha.ac.kr) **이화여자대학교 경영학과 석사과정 (sw4822@hotmail.com)

Ⅰ. 서론

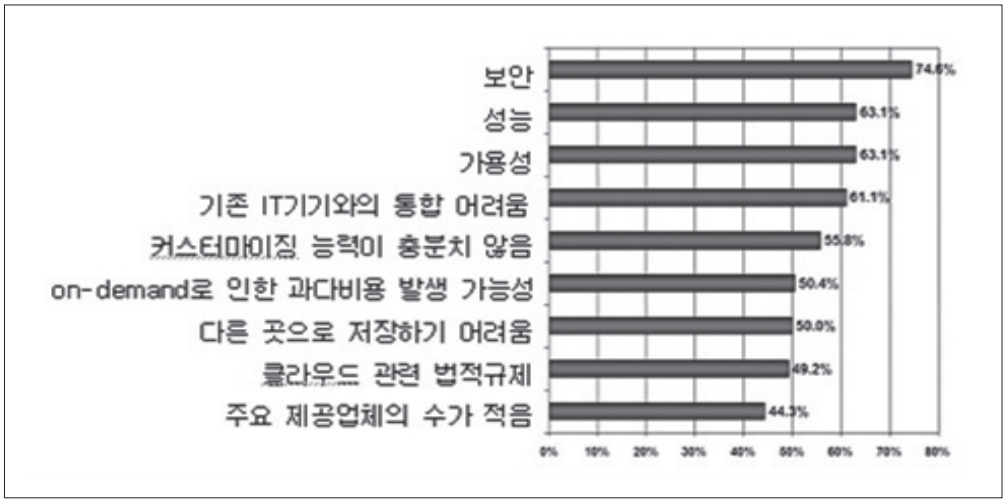
지난 10년을 돌이켜보면 통신수단인 정보통신기술의 급진전이 있었고, 이러한 기술의 발전에는 인터넷이 매우 중요한 역할을 수행해왔다. 지금도 무수히 많은 온라인 서비스가 생성되고 있고, 모바일 기기의 사용량이 증가되어 언제든지 정보를 생성, 가공하거나 저장할 수 있게 되었다. 이에 따라 데이터의 양도 방대해져서 최근에는 이러한'빅 데이터'들을 어떻게 가공하여 필요한 정보만을 추출할 수 있는지에 관한 논의도 활발히 진행 중이다. 이렇게 많은 양의 데이터를 하나의 PC에 저장하기에는 무리가 따르고 다중의 전자 기기를 가지고 있는 사람들은 기기마다 연동된 서비스를 이용하고자 하는 욕구가 있기 때문에 클라우드 컴퓨팅 서비스가 등장하게 되었다.

최근 정부에서 강조하는 미래 경제 성장 동력의 주요 주제 중 하나가 '창조경제'이다. '창조경제'란 국민의 창의성과 상상력을 기술에 접목하여 새로운 경제적 가치를 창출하고자 하는 경제 전략을 의미한다. 정부는 창조경제를 통해 새로운 성장 동력을 창출하고 이를 바탕으로 새로운 시장과 새로운 일자리를 만들어 가는 것에 목적을 가지고 있다. 현재 창조 경제에 부합되고 창조 경제의 실현을 위해 가장 주시해야할 서비스가 클라우드 컴퓨팅 서비스라고 생각한다. 클라우드 컴퓨팅은 IT 업계에서 몇 년간 계속 이슈로 제기되어 왔고, 최근에는 서비스의 활성화도 이루어지고 있다. 앞으로 클라우드 컴퓨팅은 빅 데이터와 결합하여 그 중요성이 더욱더 부각될 것으로 전망되므로 지속적으로 클라우드 컴퓨팅에 관심을 가져야 한다.

Ⅱ. 클라우드 컴퓨팅 보안 사고

클라우드 컴퓨팅은 사용자가 프로그램을 PC에 설치할 필요 없이 인터넷 환경만 구축되어 있다면 언제든 원하는 서비스를 이용할 수 있고, 데이터가 온라인상에 위치해 있기 때문에 여러 기기와 연동이 잘 된다는 장점을 가지고 있다. 또한 소프트웨어를 각 기기마다 설치할 필요가 없기 때문에 IT 비용의 절감에도 많은 도움이 된다. 반면 클라우드 컴퓨팅의 저장 공간이 충분하다고 하더라도 사용자가 모든 애플리케이션을 지원받지는 못하므로 애플리케이션의 설치나 서비스를 지원받을 시에 어려움이 따를 수 있고, 서버가 공격 받으면 개인 정보의 유출이 우려 된다는 단점을 안고 있다. 이러한 정보의 유출과 개인정보와 같은 보안 문제는 클라우드 컴퓨팅 서비스를 위협하는 가장 심각한 문제로 제기되고 있다.

지난 2009년에 구글의 gmail이 두 시간 정도 서비스가 중단된 사건으로부터 시작하여 아마존, 세일즈 포스 닷컴, 애플의 모바일 미, 윈도우 애저 등 클라우드 컴퓨팅을 시작한 많은 기업들이 지난 몇 년간 서비스 장애를 경험하였다. 특히 지난 2009년에는 이베이의 결제 시스템인 페이팔이 2시간동안 정지되면서 수백 만 명의 사람들의 중단되는 사고가 있었고, 2011년 아마존 EC2는 미국 버지니아 북부데이터센터 장애로 11시간 동안 서비스 중단된 사건이 발생한바 있다. 이러한 문제는 클라우드 서비스 기업들에 막대한 피해를 주었을 뿐만 아니라 시간이 지나면서 클라우드 컴퓨팅 사용자가 증가하고 있기 때문에 보안 장애를 겪었을 때의 피해규모도 예전에 비해 훨씬 커지고 있는 추세이다.



출처: IDC, 2008

[그림 1] 클라우드 컴퓨팅 사용으로 발생가능한 문제점

그렇다면 클라우드 서비스에 문제가 발생했을 시 소비자는 얼마만큼의 보상을 받을 수 있을까?

현재 주요 클라우드 서비스 제공 업체의 SLA는 일반적으로 99.50%~99.95% 수준이다. 즉 월 가동시간을 최대 99.50%에서 99.95%까지 보장해 주는 것인데, 99.50%면 장애 시간이 1년에 약 44시간(2592분), 99.95%의 경우 4.4시간을 넘지 않아야 한다. 업체들은 SLA 보장 수준에 따라 보통 3개월 평균 사용금액의 10%~50%의 요금을 보상하고 있다. 만약 월 사용료가 평균 3만원인데, 1시간의 장애가 났다고 했을 때 99.50%의 SLA를 보장하는 업체의 서비스를 이용할

경우 3000원의 금액을 보상받게 되는 것이다. (백지영, "[기획/클라우드 서비스 비교] 장애발생 시 얼마나 보상받을까", 디지털데일리, 2013.10)

데이터의 중요도에 따라 보상 금액에 대한 인지도도 달라지겠지만 아직까지 클라우드 서비스가 초창기라 SLA나 보상금액에 대한 규정이 확실하게 정해지지 않은 상황이라는 것을 고려한다고 해도 너무 낮은 수치임에는 틀림없다. 이러한 이유로 아직까지 많은 사용자가 클라우드에 데이터를 저장하는 것에 대해 불신을 가지고 있다. 그러므로 클라우드 컴퓨팅의 안정적인 서비스의 확산을 위해서 보안문제는 반드시 선결되어야 할 과제이다.

Ⅲ. 클라우드 컴퓨팅 보안 위협

클라우드 컴퓨팅의 보안은 크게 기술적 보안과 운영적 보안으로 분류할 수 있다. 주로 서비스 제공자와 관련된 기술적인 보안에는 인프라, 데이터, 스토리지, 통신이나 애플리케이션에 관련된 보안으로 구성된다. 반면 운영적 보안은 서비스 제공자와 이용자 모두와 관련된 보안으로 서비스 정책 수립이나 조직의 운영 방안, 자산 통제, 사고 관리, 서비스 연속성과 같은 요소들이 포함되어 있다.

이러한 클라우드 컴퓨팅의 보안과 관련하여 CSA(Cloud Service Alliance)에서는 2010년 3월 클라우드 컴퓨팅의 위협을 정리한 보고서 "Top Threats to Cloud Computing V1.0"을 발표하였다. 이번 절에서는 CSA에서 발표한 '클라우드 컴퓨팅 7대 위협'을 통해 클라우드 컴퓨팅의 보안을 위협하는 요소는 무엇이 있는지와 이러한 위험을 방지하기 위해 어떠한 노력을 기울여야 하는지에 대해 알아보도록 하자.

1. 클라우드 컴퓨팅 서비스의 남용과 불손한 사용

IaaS 제공업자들은 클라우드 컴퓨팅 서비스가 시작되자 고객들에게 무제한의 컴퓨팅 서비스와 네트워크, 그리고 저장 공간에 대한 환상을 주었다. 예를 들면 서비스 초창기에 고객들은 자신의 신용카드를 이용해서 즉각적으로 클라우드 서비스에 접속할 수 있었다. 몇몇 서비스 제공업자들은 심지어 무료로 체험할 수 있는 기간을 제공하기도 하였다. 클라우드 서비스가 인터넷 상에서 진행되므로 익명성이 보장되기 때문에 가능한 일들이었고, 클라우드 컴퓨팅 서비스 내에서 서비스의 등록, 사용모델, 스팸 데이터나 악성코드의 유포와 같은 범죄행위가 자주 일어나게 되었다.

이러한 클라우드 컴퓨팅 서비스의 남용과 불손한 방식의 사용을 막기 위해서는 최초에 등록할 때 사용자들의 신원을 검증할 수 있는 프로세스가 필요하다. 또한 신용카드를 사용할 때 좀 더 강화된 모니터링을 하거나 자체적인 네트워크 블록(network block)을 위한 공공의 블랙리스트를 모니터링을 해야 하는 등의 노력이 필요할 것으로 전망된다.

2. 안전하지 않은 인터페이스와 API

클라우드 컴퓨팅 제공업자들은 고객들이 클라우드 서비스를 관리하거나 서비스와 상호작용할 때 필요한 소프트웨어 인터페이스나 API를 노출시길 수 있다. 클라우드 컴퓨팅의 보안은 인증에서부터 암호에 접근하는 것, 모니터링과 같은 인터페이스들은 법적인 망을 피하기 위해 우연히 익명으로 접근하는 것에 대한 보호 기능을 제공하도록 설계되어야 한다.

불안정한 인터페이스와 API의 해결을 위해서는 첫째, 클라우드 제공업자의 인터페이스 보안 모델을 분석해야 하고 둘째, 암호화의 전송과 인증을 보다 더 엄격하게 해야한다.예를 들면 클라우드 컴퓨팅에 접근할 때, 접근 제어가 잘 이루어지는지를 확인해야 한다. 셋째, API와 관련된 것들 것 연결고리를 파악하는 일도 물론 중요하겠다.

3. 악의적인 내부자들

악의적인 내부자의 위협은 대부분의 조직에 매우 잘 알려져 있다. 제공업자들은 어떻게 직원들이 물리적인 자산에 접근하는지, 어떻게 이러한 직원들을 모니터링 하는지, 어떻게 법적 분쟁을 해결할 수 있는지를 드러내기가 쉽지 않다. 또한 클라우드 컴퓨팅이라는 말이 갑작스럽게 떠오르게 되면서 경험이 적은 직원들을 급하게 채용하여 도덕성이 부족한 직원들을 채용하게될 위험이 높아지게 되었다. 이러한 복잡한 문제들을 해결하기 위한 클라우드 컴퓨팅을 전담하는 직원들을 위한 기준과 관행은 거의 없기 때문에 아마추어 해커, 조직 범죄자들, 산업 스파이 등의 공격자들은 클라우드 컴퓨팅을 매우 매력적인 서비스로 인식할 것이다.

문제의 해결을 위해서는 첫째, 직원들과 계약을 체결할 시에 인사 관리 요건을 명확하게 규정하고, 둘째, 전반적인 정보 보안에 관한 문제와 관리 운영 방식에 대한 투명성 및 규정의 준수를 직원들에게 요구해야 한다. 셋째, 보안을 위반 했을 때 그것을 어떻게 알릴지에 관한 프로세스를 규정하는 일도 중요하다.

4. 기술 문제의 공유

IaaS 회사들은 인프라의 공유를 통하여 안정적인 서비스를 제공하고 있다. 특히 클라우드 컴퓨팅이 공유하는 인프라 중에서 가장 중요한 것이 가상화 서비스이다. 가상화 서비스는 인터넷과 최근의 스마트 기기의 발달로 인하여 주목 받게 된 기술이다. 오늘날의 가상화와 비슷하게 사용되는 1960대의 중요 기술이 메인 프레임은 그 당시에 활용률이 낮다는 문제점을 가지고 있었다. 이에 IBM은 비용에 비해 효율성이 떨어지는 메인 프레임을 몇 개의 가상 시스템으로 분할하는데 성공하였고 이것은 곧 가상화의 기원이 되었다. 가상화 시스템으로 인하여 여러 프로세스를 동시에 실현하는 일이 가능해졌으며 비용 또한 매우 절감할 수 있게 되었으므로 매우 혁신적인 프로그램이며 동시에 친환경적인 그린 IT를 실현하는 데에도 많은 도움이 되었다.

[가상화의 종류]

1) 하드웨어 가상화

하드웨어 가상화는 물리적인 서버의 효율적 사용을 위해서 하나의 서버를 논리적으로 분할하여 여러 개의 서버처럼 만드는 기술을 말한다. 이 기술의 목적은 관리의 유용성과 비용 절감에 있으며 분할된 서버는 자체적으로 운영 체제나 애플리케이션을 실행할 수 있으므로 물리적인 컴퓨터와 동일 기능을 수행한다고 볼 수 있다. 그러나 가상 머신은 소프트웨어로만 구성되므 있으므로 하드웨어 리소스와 분리되어 사용하지는 못한다.

2) 스토리지 가상화

스토리지 가상화는 물리적인 저장 공간이나 논리적 저장공간 안에 존재하면서 간소화된 논리적 스토리지 리소스 보기를 제공하는 추상계층이라 볼 수 있다. 정확한 의사 결정을 내리기 위해서 기업과 조직, 조직내 사용자들은 엄청난 데이터를 사용하고 있고, 최근에는 클라우드 빅 데이터와 같은 이슈들도 주목받고 있기 때문에 데이터를 저장, 관리할 수 있는 스토리지의 운영이 무엇보다도 중요해지고 있다. 스토리지 가상화는 애플리케이션에 영향을 미치지 않으면서 자원의 효율성을 증대시키기 때문에 많은 조직에서 여기에 주목하고 있다.

3) 네트워크 가상화

네트워크 가상화는 물리적인 통신 자원들을 분할하여 여러 사용자에게 독립적으로 자원을 분배하는 기술을 의미한다. 인터넷 환경에서 애플리케이션 수요에 능동적으로 대응하기 위해서는 네트워크에 대해서도 서버와 스토리지 수준의 가상화가 요구된다. 많은 기업들이 현재 이 기술의 개발에 집중하고 있다.

그러나 클라우드 컴퓨팅의 핵심기술이 이 가상화 기술은 데이터를 도덕적이지 못한

사람들에게 넘겨주는 수단으로 악용될 수도 있다.

이를 방지하기 위해서는 설치나 구성에 대해 모범적일 수 있는 보안 정책의 구현, 무단 변경이나 활동에 대한 환경을 모니터링, 강력한 인증 및 액세스 제어를 장려하거나 패치 적용 및 취약성 개선을 위한 서비스 수준 계약(SLA)를 시행, 취약성 검사 및 구성 감사를 시행하는 등의 노력이 필요하다.

5. 데이터 손실

데이터를 손상시키는 방법에는 여러 가지 종류가 있다. 백업 없이 데이터를 삭제하거나 변경하는 것은 좋은 예가 될 수 있다. 데이터를 클라우드로 옮기게 되면 데이터가 백업되는지 확인하는 일은 더더욱 어려워질 수 밖에 없다. 이 과정에서 데이터가 중간에서 해커들에 의해 유출될 수 있는 가능성이 커지게 된다. 이 경우에 데이터를 보호하기 위한 기존의 데어는 무용지물이 될 수 있으며 이러한 일들을 감시하기는 매우 어려워 질 수 있다. 데이터 손실이나 유출의 위험을 줄이기 위해서는 다음과 같은 조치를 취해야만 한다.

-강력한 API 액세스 제어 정책의 시행
-전송 데이터를 암호화 하고 무결성을 보장
-설계 및 런타임 시에 데이터 보호를 분석
-강력한 키의 생성, 저장 및 관리, 폐기 정책의 시행
-영구적인 미디어를 개방하기 전에 소거하도록 제공자들과 계약 유지
-제공업자와의 계약 체결 시 백업 및 보존전략을 시행하도록 요구

6. 계정이나 서비스의 트래픽 하이재킹(hijacking)

'피싱'으로 알려진 이 수업은 어떤 사람이 클라우드 제공업자에게 고객의 계정을 사칭하여 정보를 빼내고 악의적인 의도를 가지는 제 3자와 데이터를 공유하는 것을 의미한다. 클라우드 컴퓨팅은 각종 악성 사이트로 유도되는 하이재킹 서비스에 유독 취약하다. 이러한 리스크를 줄이기 위해서는 첫째, 사용자와 서비스 간의 계정의 공유를 금지해야 한다. 둘째, 강력한 이중 인증 기술을 사용해야 한다. 셋째, 무단 접근을 탐지하기 위해서 사전에 예방적 모니터링을 해야한다. 마지막으로, 클라우드 제공자의 보안 정책과 SLA를 잘 숙지하고 이해하는 노력이 있어야 한다.

7. 공개되지 않은 위협

CSA에서 7번째로 제시한 클라우드 보안 위협은 이른바 '광대한 위협'으로 불린다. 클라우드 컴퓨팅이 제대로 자리잡기 전까지는 분명하게 드러나지 않을지도 모른다. 일부 기업들은 여전히 클라우드 컴퓨팅의 보안 위협을 제대로 인식하지 못한 채 클라우드 컴퓨팅이 주는 장점들에만 주목하고 있다. 서비스 제공업자들의 투명성은 떨어지게 되고 고객들은 시스템의 구성이나 소프트웨어 실행에 많은 어려움을 겪게 된다. CSA는 다음과 같은 조치들을 통하여 이러한 알 수 없는 위험들을 줄이라고 말하고 있다.

-해당 로그와 데이터의 공개

-인프라 세부 정보의 공개(패치 수준이나 방화벽)

-모니터링 및 경고의 보강

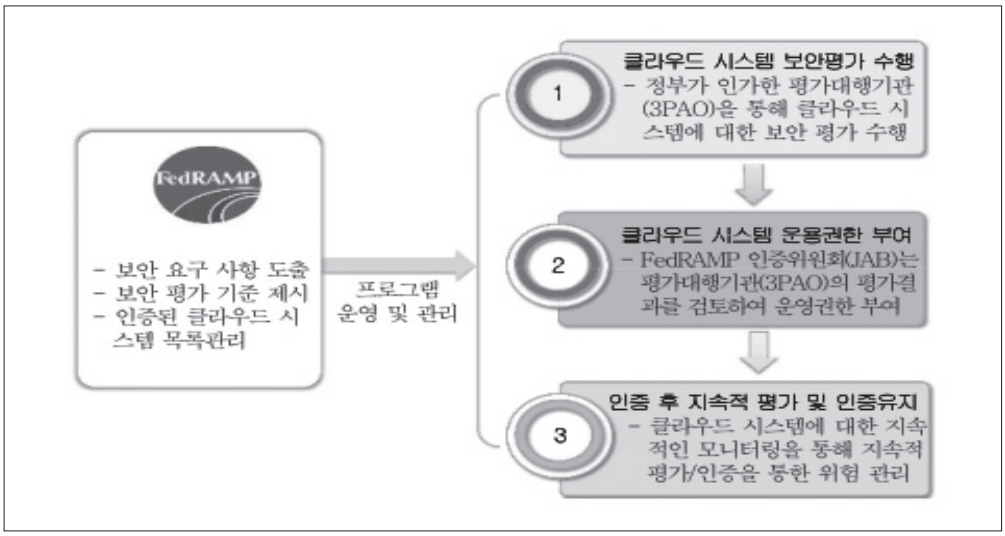
한편 CSA에서는 2012년 아래의 클라우드 컴퓨팅 보안을 위협하는 요소로 아래의 '분산서비스 거부 공격'을 추가로 제시하였는데 '분산서비스 거부 공격'이란 여러 대의 공격자들을 분산적으로 배치하여 동시다발적으로 공격하게 함으로써 특정 사이트를 공격하는 방식이 증대되고 는 것을 의미한다.

Ⅳ. 국내외 정책 동향

1. 미국

미국에서는 클라우드 컴퓨팅 서비스의 보안이 문제로 떠오르자 FedRAMP라는 기관을 창설하였다. 이 기관은 미국 연방정부의 클라우드 제품 및 서비스에 대한 보안 평가와 허가, 그리고 클라우드 관련 서비스의 모니터링을 위해 도입한 프로그램이라 할 수 있다. 모든 보안에 관한 사항을 정리, 분류하여 미 연방정부에 안전하고 정확한 클라우드 서비스를 제공하기 위해 노력하고 있다.

FedRAMP의 보안 인증 절차는 보안 평가수행, ② 운용 권한 부여, ③ 인증 후 지속적 평가 및 인증 유지 등 총 3단계로 구성 된다.



[그림 2] FedRAMP 기반의 인증 프로세스 진행 절차

출처: 장승재, 손경호, 신화수,"美 연방정부 클라우드 서비스 보안인증제도(FedRAMP) 분석 ", 정보통신산업진흥원, 2013.5

2. 일본

일본은 지난 2008년 'ASP, SaaS의 정보보안 대책 가이드라인'을 발표하였다. 이 가이드라인의 항목은 조직/운용적 측면과 물리/기술적 측면으로 나뉜다.

조직이나 운용에 있어서 보안을 위한 지침으로는 기본방침 정의, 정보보안의 조직, 사업자와 정보 자산의 관리, 전반적으로 고용과 관련된 직원에 대한 정보보안, 정보보안 사고관리, 법령과 규칙의 준수, 이용자 책임과 같은 사항들이 있다.

한편 물리/기술적인 사항으로는 공통 정보센터의 시스템 보안에 관한 대책, 소프트웨어, 플랫폼, 하드웨어 관리, 데이터 보호 등에 관한 보안 대책, 네트워크나 건물에 관련된 보안, 기밀성이나 무결성 유지에 관한 보안 등으로 구성되어 있다.

또한 일본은 2011년, ;클라우드 시큐리티 가이드'라는 보안 감사에 관한 가이드라인을 제시하고 2012년 클라우드 보안 감사 제도를 만들었다. 일본은 자국이 미국에 비해 클라우드 서비스 사용자가 상대적으로 낮은 수준(미국의 절반 수준)을 유지할 수밖에 없는 이유를 클라우드 보안에 놓고 이러한 감사 제도를 마련하였다. 클라우드 보안 감사 제도를 통해 서비스 제공자가 보안기준을 명확하게 지키고 있는지를 확인 할 수 있게 되었으며, 사용자들은 좀 더 안심하고 서비스를 이용할 수 있게 되었다.

3. 유럽

유럽의 ENISA(European Network and Information Security Agency)에서는 클라우드 컴퓨팅의 위협요소와 관련하여 정책/조직 위험, 기술적 위험, 법적위험, 클라우드에 특화되지 않은 위험, 이렇게 4가지 영역으로 분류하고 세부적으로는 관리부재, 규제 준수, 서비스 제공자에 의존하는 현상, 관리 인터페이스의 보완, 데이터 보호, 악의적 내부자 등의 35개 항목으로 구분하여 사례 분석 및 위험을 평가하는 절차를 만들었다. 또한 클라우드에 특화된 취약점과 자산을 분류하고 12개의 정보보증 요구사항을 제시하였다.

4. 국내 정책 및 방향성

한국클라우드서비스협회(KCSA)에서는 지난 2012년, '클라우드 서비스 인증제'를 시행하였다. '클라우드 서비스 인증제'란 클라우드 서비스 제공업자를 평가하여 인증을 부여하는 제도를 의미한다. 이 제도의 목적은 클라우드 컴퓨팅의 확산과 경쟁력 강화에 있다.

〈표 2〉 클라우드 서비스 인증 측정항목

측정목적	측정내용	측정수	점검수
가용성	신청기관은 클라우드 서비스를 약정된 내용에 따라 상시적으로 제공하기 위해 제반 조치를 하여야 한다.	5	14
확장성	클라우드 서비스 제공자는 클라우드 서비스 수요에 유연하게 자원을 확장하여 제공할 수 있도록 필요한 정책, 인적 물적 자원을 갖추어야 한다.	5	12
성능	클라우드 서비스 제공자는 서비스의 품질(속도)을 보장하기 위해 적절한 성능을 유지하여야 한다. 이를 위해 필요한 정책, 인적 물적 자원 등을 갖추어야 한다.	6	13
데이터 관리	클라우드 서비스 제공자는 클라우드 서비스 이용자의 데이터를 안전하게 보호/관리하기위해 필요한 정책 및 인적, 물적 자원 들을 갖추어야 한다.	5	15
보안	조직의 보안을 효과적으로 구현하기 위해 관리체계를 수립하여야 한다. 또한 조직의 물리적 시설 및 설비를 보호하기 위해 물리적 보호 방안이 마련되어야 한다. 또한 다양한 취약성을 분석하고 그에 대한 적절한 대책을 마련하고 적용하여야 한다.	10	22
서비스 지속성	이용자가 믿고 클라우드 서비스를 이용할 수 있도록 사업자는 인적, 물적 기반을 확보하고 이를 관리하여야 한다.	4	13
서비스 지원	클라우드 서비스 제공자는 이용자의 서비스 만족도를 제고하기 위해 각종 기술지원, 제공방식의 다양성, 수준의 보장 등 지원 체계를 갖추어야 한다.	5	15
계		40	105

출처: 김기철, 허 옥, 김승주, "한국형 클라우드를 위한 정보보호 관리체계 평가 기준", 2013

한편, 한국인터넷진흥원(KISA)와 방통위에서는 '클라우드 서비스 정보보호 안내서'를 제안하였다. 이 안내서는 클라우드 서비스 모델과 주요 기능과 예상되는 보안 위협과 취약점을 소개하고 있다.

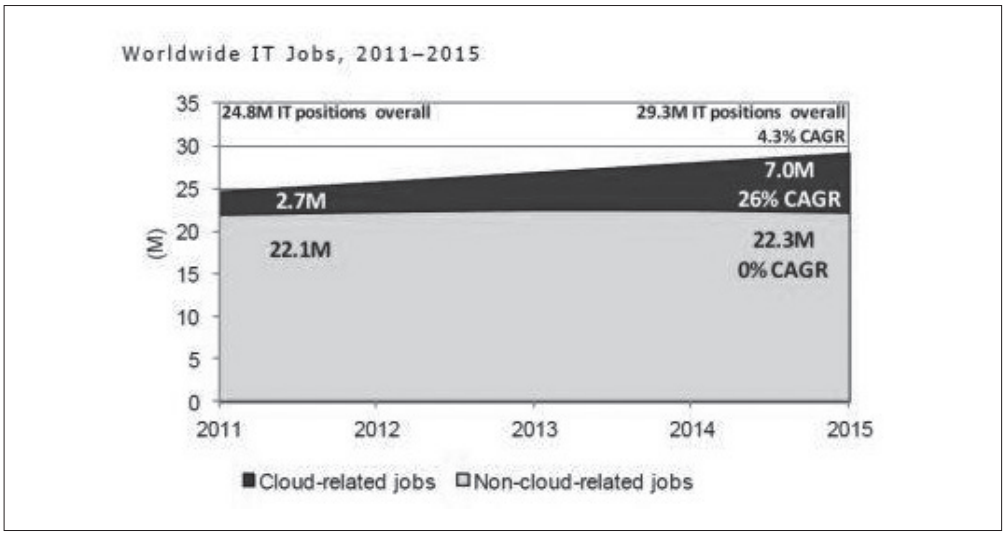
미국, 일본이나 유럽에 비해서 국내의 클라우드 컴퓨팅이 아직 비활성화 되고 있는 이유는 바로 보안에 관한 신뢰성이 부족하기 때문이다. 클라우드 서비스를 받기 위해 인터넷망의 이용은 필수적인 조건인데 보안취약점과 지능화된 해커들의 공격으로부터 자유로울 수 없다면 클라우드 컴퓨팅의 확산에 큰 걸림돌이 될 것이다.

클라우드 컴퓨팅의 활성화를 위해서는 해외의 보안 관리 가이드라인을 따라가기 보다는 해외에서 이미 정립한 가이드라인을 바탕으로 표준에 위배되지 않는 범위에서 국내 실정에 맞는 독자적인 가이드라인을 수립해야 한다. 또한 정립된 보안관리 가이드에 따라 보안의 취약점을 미리 제거해 개인, 조직, 국가의 업무 능력을 향상시켜 창조경제 시대의 IT 서비스 안정성과 신뢰성을 확보하는데 앞장서야 한다.

Ⅴ. 창조경제 실현을 위해 클라우드 컴퓨팅 보안이 나아가야할 길

1. 클라우드 컴퓨팅 관련 인력 양성

2012년도의 IDC에서 제공한 자료를 보면 2011년부터 2015년까지 기간 내의 클라우드 컴퓨팅 전문 인력 수요는 연평균 26% 증가할 것으로 전망하고 있다. 클라우드 컴퓨팅을 제외한 나머지 IT 분야를 통틀어 연평균 증가율이 제로에 가까운 것에 비하면 놀라운 수치이다.



[그림 3] 클라우드 컴퓨팅 전문인력 수요

출처: Cloud environment model, IDC, 2012

클라우드 컴퓨팅에 관련된 인력 수요가 증가하는데 비해 국내 클라우드 컴퓨팅 인력시장은 아직 너무 협소하다. 우리나라는 2000년 이후 경기의 침체 현상 때문에 IT 전문 인력이 해외로 유출되는 경향이 심화되었고 그 결과 IT 분야와 소프트웨어 관련 인력이 매우 부족한 상황에 처해 있다. 현재 많은 조사기관에서는 국내의 주요 이동통신사나 포털사이트에서 사람을 구하기가 매우 어렵다는 조사결과를 내보이고 있다. 인력풀이 좁은 가운데 개발자나 관리자의 몸값이 너무 높아 자금난을 겪는 중소기업에서는 더욱 심각한 구인난을 겪고 있다.

이렇게 클라우드 컴퓨팅 인력이 부족한 이유는 여전히 우리 사회에 이공계 기피현상이 심각하기 때문이다. 고등학교 때 문이과를 선택해야 하는 현재의 양분화된 교육체계 속에서 단순히 수학이나 과학에 흥미를 잃은 많은 학생들이 문과로 진학하게 되면서 이과계열 지망학생이 현저히 감소하게 되었고 이러한 현상은 대학 진학에 영향을 미치게 되면서 이공계열로 진학하는 학생이 급격히 줄어들게 되었다. 또한 우수 학생들 역시 이공계열 보다는 보다 안정적인 의학계열로 진학하고 있다. 또한 타 전공에 비해 과학기술 분야의 변화가 빨라 장래의 직업비전이 약하다는 인식이 있는데 이러한 문제들 역시 과학기술 분야의 인력 자원 감소의 원인이 되고 있다.

그렇다면 클라우드 컴퓨팅의 인력부족 현상을 막기 위해서는 어떤 노력을 기울어야 하는가? 우선, 과학 분야 인력에 대한 경제적 보상이 확실하게 이루어질 수 있도록 정부 차원에서 많은 개선 방안을 내놓아야 할 것이다. 이공계 육성과 우수 인력의 유치를 위해서는 좋은 연구 환경을 조성해 주고 아낌없는 투자가 뒷받침 되어야 할 것이다.

또한 창의력을 증진시키기 위해 그동안 정부가 축적 해놓은 논문이나 보고서 등 국가 지식 자산을 모아 시스템에 통합시키고 이 자산을 국가 경제를 위한 창조적인 아이디어의 원천으로 삼으며 창조적 아이디어를 즉각적으로 기업에 연계시켜 상용화 하는 방안을 마련해야 한다.

마지막으로 클라우드 컴퓨팅 보안에 맞는 교육 프로그램을 만들어 전문 인력을 양성해야 한다. 클라우드 컴퓨팅 보안에 특화된 교육과정을 위해서 정부차원에서의 지원이 이루어져야 하며 R&D 프로젝트를 통해 기업과의 연계에 앞장서야 한다. 대학 및 인력 양성소에 대한 장려 정책도 반드시 필요할 것이다.

2. 정부 차원에서의 창업 지원 노력

일자리 창출과 창조 경제의 성장을 위해 클라우드 컴퓨팅 보안 관련 창업 지원의 활성화가 이루어져야 한다. 우수 아이디어나 기술이 창업으로 이어질 수 있도록 경제적 지원을 하고 멘토링이나 사업 타당성 검증, 투자 유치 지원 등의 정책지원을 강화하는 노력이 필요하다. 젊은

아이디어와 클라우드 컴퓨팅의 융합을 통하여 벤처 창업을 촉진시킬 수 있으므로 많은 프로그램과 시스템을 지원해야 한다. 실제로 최근에는 게임 어플을 통해 아기 나무를 키우면 실제로 나무가 심어지는 'Tree Planet'이나 시간이나 거리, 칼로리를 측정하여 걸은 만큼 기부되며 건강관리도 할 수 있는 애플리케이션인 'BigWalk'와 같이 IT를 통해 사회 문제를 해결하고자 하는 노력들이 보이고 있다. 정부는 이러한 예와 비슷한 형태의 소셜 벤처의 창업을 적극적으로 지원하여 창의적 아이디어를 현실화 시켜 창조경제를 이끌어 나갈 수 있는 원동력으로 삼아야 한다.

미국의 오바마 정부는 창의적인 제품의 시장 진출을 지연시키고 고임금의 일자리 창출을 막는 특허 기술 처리기간을 기존의 35개월에서 20개월로 단축시켜 우수한 특허 기술이 일 년 안에 시장에 출시될 수 있는 three-trck 모델을 제시하였다. 또한 창조 경제의 추진과제로 세계 최고의 인력을 양성, 기초 연구 분야의 미국 주도권 강화, IT 에코시스템 구축, 시장기반 혁신 촉진을 위한 R&E(Research & Experiment) 세액공제, 효율적 지식 재산 정책을 통한 재능과 독창성 촉진 등을 제시하였다. (차두원, 유지연 "창조경제 개념과 주요국 정책 분석", 한국과학기술기획평가원, 2013)우리도 미국 정부와 같이 우수한 아이디어를 가진 벤처 기업들의 창업을 위한 정책적 기반을 마련해야 한다.

물론 클라우드 컴퓨팅에 대한 인식과 환경이 아직까지는 대중화되지 않은 시점에서 클라우드 컴퓨팅, 그것도 클라우드 컴퓨팅 보안에 관한 사업 아이템이 많지는 않을 것이다. 하지만 벤처 기업의 몰락이나 경기침체의 상황 속에서 정부가 좀 더 나서서 IT 업계의 창업과 관련 인력의 양성을 지원해 준다면 중소기업이나 중견기업을 상위 규모의 기업으로 끌어 올릴 수 있는 원동력으로 작용할 것이며, 클라우드 관련 신생회사도 증가하게 될 것이다. 창조 경제의 실현을 위해 클라우드 컴퓨팅 보안 관련 창업은 중소기업에게 글로벌 경쟁력을 심어 줄 수 있을 뿐 아니라 관련 일자리의 창출로 인해 청년 실업 문제의 해소에도 많은 도움을 줄 수 있을 것으로 전망된다.

3. 표준화 전략

창조 경제의 실현을 위해 글로벌화는 필수적인 조건인데 이에 발맞춰 클라우드 컴퓨팅 보안 분야도 세계 클라우드 컴퓨팅 시장에 진출하기 위해서는 반드시 표준에 관한 규정이 필요하다. 해외 여러 기구에서 진행 중인 클라우드 컴퓨팅 표준화 동향은 다음과 같다.

〈표 3〉 해외 클라우드 컴퓨팅 표준화 동향

분류	목표
OCC	● 클라우드간 상호호환성을 위한 표준과 프레임워크를 개발 ● 클라우드 컴퓨팅을 위한 참조 구현 ● 클라우드 컴퓨팅 테스트베드 관리
CCIF	단일화된 방법으로 정보를 교환하는 하나 이상의 클라우드 플랫폼을 위한 프레임워크와 온톨로지를 개발
OGF	표준의 WBEM 등을 개발하였고 시스템 자원 관리를 위한 영역별 관리 항목을 정의하는 프로파일(management profile) 표준을 개발
DMTF	기업 및 네트어크 환경을 대상으로 표준 및 통합 기술을 개발하여 상호호환성을 보장하기 위한 표준을 개발중
ISO/IEC JTC1 CS38 SGCC	● 클라우드컴퓨팅의 개념/용어 정리 ● 클라우드 컴퓨팅 표준 관련 기구와의 협력
CSA	● 클라우드 컴퓨팅 보안 보장을 위하여 모범 사례 및 보안 가이드라인을 개발 ● 다양한 형태로 클라우드 컴퓨팅에 보안 및 교육을 제공

OCC : Open Cloud Consortium
CCIF : Cloud Computing Interoperability Forum
DMTF : Distributed Management Task Force
OGF : Open Grid Forum
SGCC : Study Group Cloud Computing
CSA : Cloud Security Alliance
출처: 이경호, "Security Management for Constructing Secure Smart Office", 시큐베이스, 2011.6

클라우드 컴퓨팅은 전통적으로 소프트웨어 플랫폼 기술을 포함하여 가상화 및 운영체제 기술에 강점을 지닌 기업들이 주도하고 있어 상대적으로 이 분야에 기술격차가 있는 우리나라는 제품간의 보안이나 이식성, 상호호환성에 상당한 문제가 발생할 것으로 보인다. 따라서 이러한 문제를 사전에 대비하여 다양한 표준화 전략을 수립해 나가야 한다.

단기적으로는 국제 표준화 추세에 따라 부분적으로 수용한다는 입장에서 국내표준과 병행하는 노력이 필요하며, 장기적으로는 우리나라가 강점을 지닌 우수한 IT 인프라 및 단말 제조 역량을 기반으로 차별화된 국제표준화 추진이 요구된다. 즉, 클라우드 컴퓨팅은 해외 각국의 치열한 시장 선점의 노력이 우려되긴 하지만 국내 클라우드 컴퓨팅 시장은 초기 확산단계에 있기 때문에 원천 기술의 확보에 주안점을 두고 표준화 전략을 추진해 나가야 한다.

또한 해외에서 추진 중인 가이드라인을 바탕으로 국내 실정에 맞는 보안관리 표준화 체계를 만들어 나가야 할 것이다.

국내 클라우드 컴퓨팅 표준화는 다음 표와 같이 진행 중이다. 최근에는 국내에서도 클라우드 컴퓨팅 관련 기구들이 많이 창설되어 표준화에 대해 활발히 연구 중이다.

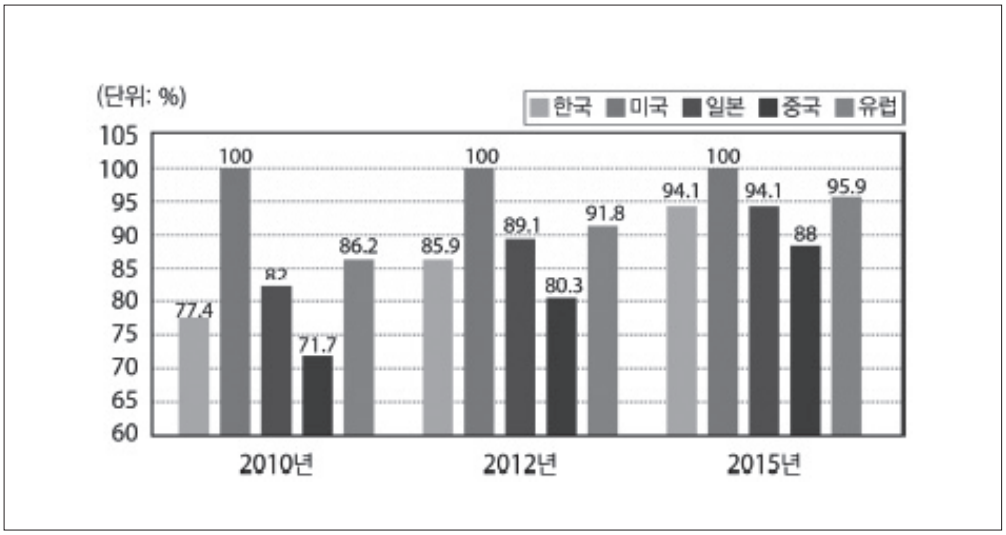
〈표 4〉 해국내 클라우드 컴퓨팅 표준화 동향

분류	목표
한국 클라우드 서비스 협의회	● 인터넷 기반 클라우드 제품 및 서비스 시험/ 인증 테스트 베드 제송 ● 클라우드 서비스 표준화
클라우드 컴퓨팅 산업 포럼	한국형 클라우드 컴퓨팅 모델 개발 국내외 클라우드 컴퓨팅 표준 개발
공공부분 클라우드 컴퓨팅 협의회	IT 자원 및 관리 효율화
클라우드 컴퓨팅 포럼	민간 중심의 클라우드 컴퓨팅 국내 표준개발 및 관련 산업 활성화

출처 : ETRI , "클라우드 컴퓨팅 표준화 동향 및 전략"

4. 기술력 강화

국내 클라우드 컴퓨팅 보안 해결을 위해 기술력 강화는 필수적 조건이다. 현재 클라우드 컴퓨팅 관련 기술의 우위를 차지하고 있는 국가는 단연 미국이다. 현재로서는 미국의 클라우드 컴퓨팅 기술수준이 압도적으로 높다고 볼 수 있다. 2010년 미국과 국내 기술의 기술 격차는 77%로 조사 되었다.



[그림 4] 국내외 클라우드 컴퓨팅 기술 수준 및 향후 전망

출처: KEIT, 2010년 IT 기술수준조사 분석 보고서, 2010

해외의 경우에 초기 클라우드 컴퓨팅 주도권 확보를 위해서 인프라의 구축에 상당한 집중력을 나타내었고 클라우드 컴퓨팅의 시장 확대를 위해 기술 개발에 많은 투자를 하고 있다.

국내 클라우드 컴퓨팅의 보안 기술이 경쟁우위의 확보를 위해서는, 기술력 강화를 위해서 기술의 중요도와 시장에서의 잠재력을 고려하여 개발 시장을 세분화 하는 전략을 펼쳐야 한다.

예를 들면, 중요도가 큰 기술은 정부차원에서, 중요도가 낮은 기술은 민간 차원에서 개발하게 되면 동시다발적으로 개발하는 것에 비해 훨씬 빠르고 효율적으로 기술을 개발할 수 있다.

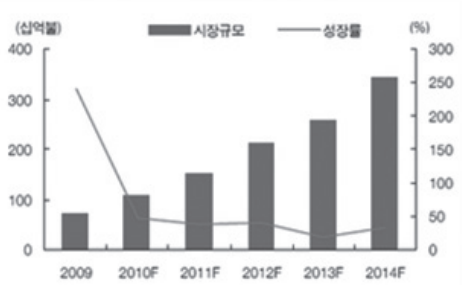
또한 국내외 기술 격차가 지나치게 커서 단기적 극복이 어려운 분야의 경우에는 전략적 제휴를 통해 기술격차를 서서히 극복하는 것도 하나의 방법이라 할 수 있다. 중장기적으로는 국내의 우수한 단말기 제조 기술과 컨버전스 기술, 혹은 유비쿼터스 기술을 모바일 클라우드와 접목시켜 독자적인 기술 선점 전략을 취해 나가야 한다.

Ⅳ. 결론

정부가 창조경제를 주요 정책으로 내놓은 것의 목적은 변화를 통하여 경기의 침체에서 벗어나고자 함에 있다. 스마트폰 등의 단말기 사업을 통해 세계 시장 속에 우뚝 선 우리나라는 지난 10년 동안 IT 산업에서의 놀라운 능력과 잠재력을 발견 하였다. 물론 세계 경제의 빠른 변화에 민첩하게 대응하고 있다고 생각되지만 장기적인 관점에서는 일을 진행함에 다소 무리가 있어 보인다.

창의적 인재의 양성이나 창조적 아이디어를 가진 벤처의 창업, 다양한 분야의 융합을 통한 신시장 창출과 같은 과제들은 단기간 내에 이루어지는 것이 아니며 많은 시간과 시행착오를 거쳐야 현실화 되어 부가가치를 창출해 낼 수 있는 과제들이다. 따라서 앞으로는 성급한 판단보다는 시간을 두고 새로운 관점으로 IT 관련 정책에 접근해야할 필요가 있다.

클라우드 컴퓨팅은 초기 시장에 비해 성장률은 다소 낮아지겠지만 앞으로도 계속해서 발전해 나갈 주요 IT 분야이며 시장 규모도 더욱 커질 전망이다. 특히, 클라우드 보안 분야의 경우 가트너는 2015년까지 전체 IT 보안 제품 중의 10% 정도를 클라우드 기반의 서비스로 제공하게 되며, 그 때까지 클라우드 보안 시장 규모는 약 42억 달러 정도가 될 것이라고 내다보았다.



[전 세계 시장 규모 전망]

(단위: M$)

구분	2010	2011	2012	2013	2014
SaaS	58	83	120	164	216
PaaS	12	21	34	56	83
IaaS	27	45	72	108	161
총계	97	149	226	328	460

[전 세계 시장 규모 전망]

[그림 5] 국내외 클라우드 컴퓨팅 시장 전망

출처: IDC, HMC 투자증권

혁신적인 아이디를 통해 신 시장을 창출하도록 정책적 기반을 마련하고 이러한 제반환경이 조성되었을 때 창조경제가 발전할 수 있다. 앞으로, 투자 가치가 높은 클라우드 컴퓨팅과 보안에 관하여 높은 관심을 가지고 장기적으로 해당 산업분야의 전문성과 아이디어의 구현을 중심으로, 정책 구도를 재구성 한다면 국내 실정에 맞는 클라우드 보안 정책이 수립될 것이며 이는 창조경제를 이끄는 힘이 될 것으로 기대된다.

참고문헌

강원영, “최근 클라우드 컴퓨팅 동향”, 한국인터넷진흥원

금융보안연구원, “금융부문 클라우드 컴퓨팅 보안 가이드” 2010.12

김승주, “우리 보안 분야는 창조 경제 시대를 맞을 준비가 되었는가?”, 인터넷정보보호, 정책 연구, 2013

김병일, 신헌문, “클라우드 컴퓨팅 생태계 및 정책 방향”, ETRI, 2012

방송통신위원회,“민간 부문의 클라우드 도입 실무 가이드라인”, 2012..12

백지영, “[기획/클라우드 서비스 비교] 장애 발생시 얼마나 보상받을까”, 디지털데일리, 2013.10

이경호, “Security Management for Constructing Secure Smart Office”, 시큐베이스, 2011.6

이승윤, “국내외 클라우드 컴퓨팅 표준화 동향”, TTA 저널 vol.139, 2012..1

이유지, “[기획/2011 클라우드⑨] 반드시 넘어야할 산, ‘클라우드 보안’… 어디까지?”, 디지털데일리, 2011.1

이중현, “창조경제와 클라우드”, ETNews [ET 단상], 2013.5.27.

정성재,배유미, “클라우드 보안 위협요소와 기술 동향 분석”, 보안공학연구논문지 제 10권 제 2호, 2013. 4

장승재, 손경호, 신화수,“美 연방정부 클라우드 서비스 보안인증제도(FedRAMP) 분석”, 정보통신산업진흥원, 2013.5

차두언, 유지연,“ 창조경제 개념과 주요국 정책 분석”, 한국과학기술기획평가원, 2013.1 CSA, "Top Threats to Cloud Computing V1.0", 2010

ETRI , “클라우드 컴퓨팅 표준화 동향 및 전략”

IT WORLD, “2015년까지 IT 보안 제품 중 10%가 클라우드로 제공” : 가트너, 2013.4

KISA, "클라우드 서비스 보안관리 가이드라인", 2010.10

HP, "클라우드 컴퓨팅을 위협하는 7가지 보안 문제", 2010

http://blog.naver.com/janlssary?Redirect=Log&logNo=10169683434