삼정 KPMG

ISSUE MONITOR

May 2016

삼정KPMG 경제연구원

국내 클라우드 도입 이슈 분석

: 주요국 관련 정책을 중심으로

Contacts

The contacts at KPMG in connection with this report are:

유경진
선임연구원
Tel: +82 2 2112 3018
kyungjinyu@kr.kpmg.com

© 2016 Samjong KPMG ERI Co., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

Contents

	Page
Executive summary	**3**
클라우드 서비스의 부상	**4**
- 클라우드 개념 및 분류	4
- 클라우드 산업의 중요성 증대	5
국내 클라우드 도입 현황 및 이슈	**7**
- 클라우드 관련 정책	7
- 보안에 대한 우려	8
- 공공부문에 민간 클라우드 활성화를 저해하는 기존 정책	9
- 클라우드 활성화와 맞지 않는 산업별 규제	11
해외 클라우드 도입 정책	**13**
해외 클라우드 보안 정책	**16**
해외 클라우드 관련 이용자 보호 제도	**19**
국내 클라우드 도입 활성화를 위한 정책: Speed up 필요	**21**

본 보고서는 삼정KPMG 경제연구원(주)과 KPMG member firm 전문가들이 수집한 자료 및 정보를 바탕으로 일반적인 정보를 제공할 목적으로 작성되었으며, 보고서에 포함된 자료는 해당 분야 정보의 완전성, 정확성 및 신뢰성을 확인하기 위한 절차를 거친 것은 아닙니다. 본 보고서는 특정 기업이나 개인의 개별 사안에 대한 해답을 제공할 목적으로 작성된 것이 아니며, 구체적인 의사결정이 필요한 경우에는 반드시 당 법인의 전문가와 상의하여 주시기 바랍니다. 또한 본 보고서는 삼정KPMG의 사전 동의 없이 무단 배포, 인용, 발간 복제할 수 없습니다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

Executive Summary

2016년 5월 18일 제5차 규제개혁장관회의에서 정부는 클라우드 활성화를 저해하는 일부 규제를 개정하기로 결정했다. 또한 '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률'을 2015년 9월부터 시행하였으며, 'K-ICT 클라우드 컴퓨팅 활성화 계획'을 확정하였다(2015년 11월). 이처럼 정부에서 국내 클라우드 도입을 활성화하기 위해 다각도로 노력하고 있으나, 국내 클라우드 도입은 여전히 미진한 상황이다. 이에 본 보고서에서는 국내 클라우드 도입 활성화를 저해하는 요인을 살펴보고 주요국의 클라우드 도입 사례를 통해 국내 실정에 적합한 클라우드 도입 활성화 방안을 제시한다.

Executive Summary

■ 클라우드는 IT산업의 패러다임을 변화시킴

- 클라우드 컴퓨팅은 IT 자원을 필요한 만큼 대여하여 원하는 시점에 네트워크를 통해 사용하는 컴퓨팅 환경으로, IT 자원을 임대해서 사용하는 개념임
- 사물인터넷, 인공지능, 빅데이터 등 주요 기술발전과 함께 데이터량이 폭증하며, 클라우드가 산업 성장을 뒷받침하고, 기술을 구현하는 기반으로 자리잡음
- 주요국에서는 클라우드 활성화 정책을 통해 클라우드 도입률이 우리나라에 비해 매우 높은 상황으로 정부는 클라우드 도입 활성화 정책을 시행하였으나, 아직 성과가 미진하여 클라우드 도입 관련 주요 이슈를 살펴보고 해외 사례를 통해 국내 실정에 적합한 활성화 방안을 모색하고자 함

■ 국내 클라우드 도입 현황 및 이슈

- 정부는 클라우드 산업 육성을 위한 지원 근거를 마련하고, 서비스 이용 환경을 조성하기 위해 관련 법과 정책을 마련하였으나, 보안에 대한 우려, 공공부문에 클라우드 활성화를 저해하는 기존 정책, 산업별 규제로 인해 정책의 실효성이 떨어지는 상황
- 정보를 외부에 위탁하는 클라우드의 특성으로 인해 보안에 대한 우려가 클라우드 도입에 가장 큰 걸림돌로 작용하며, 망분리 정책, 정부의 기관별 분류에 따른 클라우드 도입 정책, 비용과 시간이 소요되는 인증 등 정책적 요인과 금융, 교육, 의료 등 각 산업별 규제 등이 클라우드 활성화 저해요인으로 작용

■ 해외 클라우드 도입 사례

- 미국, 영국 등 클라우드 선진국은 'Cloud First Policy'를 통해 공공기관을 중심으로 클라우드 컴퓨팅을 선제적으로 도입하여 클라우드 시장을 활성화시켰으며, 특히 영국은 데이터 보안 분류 체계 간소화로 클라우드 도입을 촉진함
- 미국은 'FedRAMP'라는 높은 수준의 보안인증제도를 활용하여 보안문제와 중복인증에 따른 비효율성을 해결하였으며, 일본, 영국, 싱가포르 등도 공공기관에 클라우드 도입을 위한 보안인증제도를 운영하고 있음
- 클라우드 이용자 및 정보보호를 위해 각국에서 다양한 법제도를 운영 중이며, 클라우드 기업이 대부분 미국기업이기 때문에 대부분의 국가에서 해외 정보 유출 예방 및 대응을 위한 제도가 활성화되어 있음

■ 국내 클라우드 활성화 방안

- 주요국에서는 클라우드 활성화를 위해 공공부문에 클라우드를 선제적으로 도입하여 안전성을 검증하고, 검증된 클라우드 서비스를 민간에 확산시키는 정책을 시행하였으며, 이러한 사례를 바탕으로 국내에서도 클라우드 도입 활성화 방안을 모색함
- 정부는 클라우드 도입을 위한 기관별 분류 등 클라우드 활성화 정책과 대치되는 기존 정책들을 개선하고, 관련 절차 간소화, 세제 혜택 및 비용 지원 등 실효성있는 정책을 펼칠 필요가 있음
- 보안 우려를 해소하기 위해 정부는 보안인증제도, 사고예방 및 대응 체계 마련에 힘쓰는 한편, 서비스 제공업체는 스스로 보안수준을 제고하고, 보안인증을 획득하여 서비스 이용자에게 신뢰를 제공할 필요가 있으며, 서비스 이용자는 인식 전환 및 보안 사고 예방을 위해 노력할 필요
- 금융, 의료, 공공부문 등 클라우드 도입으로 산업경쟁력 제고가 예상되는 분야에서는 클라우드 도입의 걸림돌이 되는 규제 개선 필요

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

클라우드 서비스의 부상

> "클라우드 컴퓨팅은 전 세계적으로 IT 환경의 패러다임을 변화시킴"

클라우드의 개념 및 분류

클라우드 컴퓨팅은 IT 자원을 필요한 만큼 대여하여 원하는 시점에 네트워크를 통해 사용하는 컴퓨팅 환경이다. 즉, IT 자원이 필요한 개인 혹은 기관에서 물리적인 IT 자원을 고정적으로 설치하여 사용하지 않고, 필요한 시점에 필요한 만큼의 IT 자원을 임대해서 사용하는 개념이다. 사물인터넷, 인공지능, 빅데이터 등 주요 기술발전과 함께 데이터량이 폭증하며, 클라우드가 산업 성장을 뒷받침하고, 기술을 구현하는 기반으로 자리잡고 있다.

클라우드 컴퓨팅은 클라우드 인프라의 위치와 운영 기준에 따른 분류로 배치 모델(Deployment Model)과 이용자가 클라우드 컴퓨팅 서비스에 접근할 수 있는 형태에 따른 분류로 서비스 모델(Delivery Model)로 구분된다. 배치 모델은 클라우드의 이용 목적 및 시스템의 위치에 따른 분류로서 퍼블릭 클라우드(Public Cloud), 프라이빗 클라우드(Private Cloud), 하이브리드 클라우드(Hybrid Cloud), 커뮤니티 클라우드(Community Cloud)로 분류된다.

클라우드 서비스 유형별 특징

구분		주요 특징
배치 모델	Public Cloud	• 누구든지 이용하도록 구현되는 것으로 일반 이용자 또는 대기업에게 사용량에 따라 과금하는 형태로 제공되는 서비스 • 퍼블릭 클라우드의 인프라는 서비스를 판매한 업체가 소유
	Private Cloud	• 특정 조직 내부에서 클라우드컴퓨팅 사용 환경을 제공하여 폐쇄적으로 구현하는 서비스 • 프라이빗 클라우드 인프라는 해당기관 또는 제3자에 의해 관리될 수 있으며, 영역 내/영역 외에 이용자가 조직에 포함되는 여부에 따라 권한 할당이 가능
	Hybrid Cloud	• 퍼블릭 클라우드와 프라이빗 클라우드의 혼재된 형태로 중요자료는 프라이빗 클라우드에 보관하고, 부분적으로 퍼블릭 클라우드를 활용하는 형태로 운영 • 데이터와 애플리케이션의 이동을 가능하게 하는 표준기술로 하나로 묶거나 2개 이상의 클라우드를 통합함
	Community Cloud	• 비슷한 환경의 기관 및 단체들이 공통으로 사용하기 위한 목적으로 만들어진 서비스 • 분산되어 있는 관계사항(목적, 정책, 보안요구사항, 협약 등)을 공유함
서비스 모델	IaaS	• 서버, 프로세서, 네트워크, 스토리지 등 인프라스트럭쳐를 가상화 환경으로 만들어 필요에 따라 인프라 자원을 사용할 수 있도록 하는 서비스
	PaaS	• 이용자가 애플리케이션을 개발·테스트·구축할 수 있는 통합된 플랫폼을 제공하는 서비스로서, 이용자는 PaaS를 통해 새로운 애플리케이션을 개발하기도 하고, 다른 SaaS 서비스를 제공하기도 함 • 이용자는 클라우드 인프라, 네트워크, 서버, 운영체제, 스토리지에 대한 관리/제어 권한이 없지만 이용자가 구성한 애플리케이션과 호스팅한 애플리케이션 시스템 환경의 구성 및 관리 권한을 가질 수 있음
	SaaS	• 일정관리, 주소록, CRM용 프로그램, 오피스 프로그램 등 다양한 소프트웨어를 웹을 통해 임대해 사용할 수 있도록 제공하는 서비스

Source: 미래창조과학부

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

> 퍼블릭 클라우드는 비용절감 및 신속성,
>
> 프라이빗 클라우드는 보안성에 장점이 있음

퍼블릭 클라우드는 불특정 다수의 이용자를 위해 개방적 형태로 제공되는 클라우드 컴퓨팅 서비스로 하나의 서버에 다수의 정보가 함께 저장되는 형태로 비용절감 및 신속성의 장점이 있다. 그러나 각 클라우드 이용자의 요구에 부합하는 클라우드 컴퓨팅 환경을 구성할 수 있는 유연성 면에서는 한계가 있다. 프라이빗 클라우드는 특정 이용자에게만 폐쇄적으로 제공되는 서비스로 전용 클라우드 인프라를 구축 및 관리함으로써, 데이터의 저장 및 처리도 해당 조직 내에서 처리할 수 있다는 특징이 있다. 주로 보안을 우선시하는 경우에 이용되며, 사용 기관의 목적에 맞춤형 서비스를 제공할 수 있는 유연성은 높지만 초기 도입 비용이 비싸고 구축에도 시간이 걸리는 단점이 있다. 하이브리드 클라우드는 프라이빗 클라우드(보안성)와 퍼블릭 클라우드(비용절감·신속성)의 장점을 결합한 서비스이다.

서비스 모델은 이용자가 클라우드 컴퓨팅 서비스에 접근할 수 있는 형태에 따른 분류로 IaaS(Infrastructure as a Service), PaaS(Platform as a service), SaaS(Software as a Service)로 분류된다. IaaS는 처리장치, 스토리지, 네트워크 등 기반 컴퓨팅 자원을 클라우드 인프라를 통해 제공하는 것을 의미하며, PaaS는 애플리케이션을 개발하고 테스트할 수 있는 통합된 플랫폼을 클라우드 인프라를 통해 제공하는 것을 의미한다. 마지막으로 SaaS는 클라우드 서비스 제공자의 애플리케이션을 사용할 수 있도록 클라우드 인프라를 통해 제공하는 것을 의미한다.

클라우드 산업의 중요성 증대

세계적으로 ICT활용 패러다임이 정보시스템을 자체 구축하는 방식에서 클라우드 컴퓨팅으로 전환 중에 있다. 클라우드 컴퓨팅은 IT자원의 비용효율 극대화를 추구하며, 인프라 투자에 대한 부담을 감소시켜 환경 변화에 민감하게 대응할 수 있게 한다. 또한 IT자원 운용과 관련된 비핵심 업무를 아웃소싱 함으로써 조직 핵심 역량을 강화할 수 있다는 장점이 있다.

클라우드 컴퓨팅 도입 효과

구분	주요 내용
비용 절감	• ICT자원을 빌려서 사용함으로써 HW·SW 구매 및 유지·관리의 필요성이 없어 비용절감 가능
생산성 향상	• 인터넷만 연결되면 언제, 어디서나, 스마트폰 등 다양한 단말기를 통해 업무 가능
효율성 증가	• 갑작스러운 ICT자원의 수요 변화에 신속하고 탄력적인 대응이 필요한 만큼 ICT 자원의 활용이 가능하여 비즈니스 효율성 증가
창업 활성화	• ICT에 대한 초기 투자비용이 절감되어 적은 투자비용으로도 창업이 가능하여 쉬운 창업(Lean Startup) 가능

Source: 정보통신산업진흥원

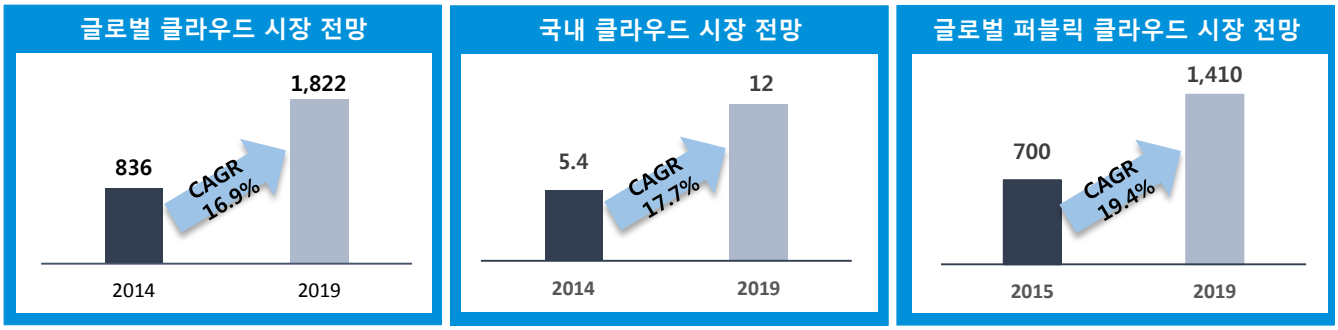
© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

> 클라우드 시장 규모가 2019년까지 연평균 19.4% 성장할 것으로 전망

가트너에 따르면 글로벌 클라우드 시장규모는 2014년 836억 달러에서 2019년 1,882억 달러로 연평균 16.9% 성장할 것으로 예상되며, 국내 클라우드 시장규모는 2014년 5.4억 달러에서 2019년 12억 달러로 연평균 17.7% 급성장할 것으로 예상된다. 또한 IDC에서 2016년 초에 발표한 보고서에 따르면 글로벌 퍼블릭 클라우드 서비스 시장 규모가 연평균 19.4%씩 성장해 2019년에는 1,410억 달러에 달할 것으로 전망했다. 이는 전체 IT 시장 성장률에 6배에 달하는 수치이다.

(단위: 억 달러)



Source: 가트너, IDC, 미래창조과학부, 삼정KPMG 경제연구원 재구성

> 우리나라는 주요국 대비 클라우드 도입 수준이 매우 저조한 상황

주요국에서는 클라우드 도입을 장려하는 정책을 적극적으로 펼쳐 클라우드 도입 수준이 매우 높은 상황이다(도입 기업·기관 수 기준 도입률: 미국·영국 40%, 일본 33% 수준, CDW, 2013년 기준). 그러나 국내 클라우드 도입률은 도입 기관수 기준 4.7%이다(한국정보화진흥원, 2014년 기준). 글로벌 기업에 비해 국내 기업의 기술력, 인력, 인지도 등이 떨어지며, 보안 우려, 도입 기준 부재 등으로 인해 주요국에 비해 클라우드 도입률이 매우 떨어지는 상황이다. 이에 정부는 '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률'(이하, '클라우드 발전법')을 2015년 9월부터 시행하였으며, 'K-ICT 클라우드 컴퓨팅 활성화 계획'을 확정하였다(2015년 11월). 또한 2016년 5월 제5차 규제개혁장관회의에서 클라우드 활성화를 위해 금융, 의료, 공공 분야의 일부 규제를 개정하기로 결정했다. 법이 시행된 지 약 7개월이 경과하였으나 국내 클라우드 도입은 여전히 미진한 상황이다.

김대중 정부 시절 IT 산업 발전의 기본 인프라인 네트워크 구축(광케이블을 이용한 초고속망)으로 국내 IT 산업이 빠르게 성장할 수 있었다. 우리나라는 초고속 인터넷 보급률 1위(2013년) 등 클라우드 확산을 위한 최고의 인프라를 보유하고 있음에도 불구하고 과거와 같은 추진력 부족으로 클라우드 활성화에 난항을 겪고 있다. 이에 본 보고서에서는 국내 클라우드 도입 현황 및 주요 이슈들을 살펴보고, 주요국에서 클라우드를 활성화시키기 위한 도입 및 보안 정책과 이용자 보호 제도 등을 분석하여 국내 클라우드 도입을 활성화하기 위한 정책적 시사점을 제시한다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

국내 클라우드 도입 현황 및 이슈

우리나라는 세계 최고 수준의 IT 인프라를 보유하고 있음에도 불구하고 IT 산업의 판도를 바꾸고 있는 클라우드를 적극적으로 활용하고 있는 글로벌 기업들에 비해 국내 기업들의 활용도는 턱없이 낮은 수준이다. 2015년 시스코와 IDC의 조사에 의하면 국내 기업 10곳 중 4곳은 클라우드 전략 자체가 없으며, 클라우드에 최적화된 비즈니스 전략을 갖고 있는 곳은 전무한 것으로 나타났다. 클라우드에 대한 이해와 운영 현황을 토대로 평가한 클라우드 성숙도 역시 우리나라는 미국(34%), 중남미(29%), 영국(27%) 등 클라우드 선진 국가들뿐만 아니라 세계 평균(25%)보다도 떨어지는 18%에 불과한 것으로 나타났다. 또한 클라우드를 도입한 기업은 구축 앱 1개당 도입 이전 대비 비용이 16억 원 가량 절감한 것으로 나타났다. 특히, 최적화된 클라우드 전략을 갖춘 기업들의 경우 평균적으로 IT 비용 77% 절감, IT 서비스 및 앱 운용 시간 99% 감소 등의 효과를 본 것으로 나타나 클라우드 도입 효용이 무척 높은 것으로 나타났다.

> **"IDC 조사 결과, 기업의 비용 절감 등 클라우드 도입 효용이 매우 높은 것으로 나타남"**

이처럼 클라우드 컴퓨팅은 세계적인 급성장 분야임에도 우리나라는 일부 클라우드 서비스 제공 기업을 제외하고 규모가 영세하고, 도입 수준이 저조하여 새로운 기회를 충분히 활용하지 못하고 있는 상황이다. 이는 클라우드 이용에 대한 보안 우려와 클라우드 환경에 맞지 않는 기존 제도 등에 기인한다.

클라우드 관련 정책

정부는 클라우드 산업 육성을 위한 지원 근거를 마련하고, 클라우드 산업 발전을 저해하는 기존 규제를 개선하며, 안전하게 서비스를 이용할 수 있는 환경을 조성하고자 법률을 제정하였다. '클라우드 발전법'은 국내 클라우드 산업 육성과 이용자 보호를 핵심내용으로 하고 있다. 또한 정부는 공공부문에 클라우드를 선제적으로 도입함으로써 민간부문의 클라우드 이용을 확산하고, 국내 클라우드 생태계 구축을 목표로 2015년 11월 'K-ICT 클라우드 컴퓨팅 활성화 계획'을 확정했다.

> **"정부는 국내 클라우드 도입 활성화를 위해 관련 법 제정 및 정책 수립"**

'클라우드 발전법'은 공공기관의 클라우드 사업에 민간 기업의 서비스를 도입할 수 있는 법적 근거를 마련하여 주요 클라우드 선진국들과 같이 공공기관에 클라우드를 선제적으로 적용하여 민간에 확산시키려는 정부 정책의 기반이 된다고 볼 수 있다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

그러나 정부의 클라우드 활성화를 위한 적극적인 정책과 클라우드 컴퓨팅의 비용 효율적인 이점에도 불구하고 기업과 공기관에서 클라우드의 구축 및 도입은 상대적으로 미진한 상황이다. 클라우드 컴퓨팅 도입이 늦어지는 이유는 (1) 자사 정보에 대한 보안문제와 (2) 공공부문에 민간 클라우드 활성화를 저해하는 기존 제도 운영의 문제, (3) 클라우드 활성화를 저해하는 산업별 규제를 들 수 있다.

보안에 대한 우려

> "보안에 대한 우려가 클라우드 도입에 가장 큰 걸림돌로 작용"

조직에서 클라우드의 구축 및 도입을 추진할 때 가장 큰 걸림돌은 보안 문제이다. 정보를 외부에 위탁하는 클라우드의 특성으로 보안에 대한 우려의 시각이 있기 때문이다. 정보통신산업진흥원에 따르면 민간기업의 30.6%, 공공기관의 33.3%가 클라우드 서비스 도입 시 데이터 보호를 가장 중요하게 생각하는 것으로 나타났다. 실제로 클라우드 서비스 관련 보안 사고들이 발생하였으며, 이러한 사고는 클라우드 서비스 기업과 이용자들에게 막대한 피해를 주었다.

클라우드 서비스 보안사고 사례

서비스 제공자	보안사고 사례
구글	• 태국의 ISP를 이용한 세션 하이재킹 공격 발생
	• 2011년 2월, 50만명의 이용자가 메시지 및 주소록이 사라지는 사고 발생(원인규명 안됨)
MS	• 2010년 12월, 서비스 환경설정 오류로 인해 클라우드 상의 기업정보가 타인에게 열람됨
아마존	• 2011년, 아마존의 가상서버 임대서비스(EC2)에 가명으로 가입 후 가상서버를 대여해 소니 플레이스테이션 네트워크 해킹
애플	• 2014년, 유명 여배우들의 계정 탈취를 통한 누드사진 유출
	• 2012년, iCloud, Gmail, Twitter 계정분석을 통한 맷호난 기자의 계정 탈취 및 모든 개인자료 삭제
VMWare	• 2012년, Vmware Image에 CRISIS 악성코드 삽입
Dropbox	• 2012년, 이용자 이메일 명단 유출 및 스팸전송
에버노트	• 2013년 2월, 백도어 활동, C&C 서버의 수집정보 은닉 장소로 에버노트 이용
Vaserv.com	• 2009년 6월, 가상화 플랫폼(Hyper-VM)에 대한 제로데이 공격으로 10만 고객사 웹사이트 삭제
ZenDesk	• 2013년 2월, ZenDesk 시스템 해킹을 통한 개인정보 유출
Dream Host	• 2012년 1월, DreamHost DB 해킹으로 인한 개인정보 유출
KT	• 유클라우드(uCloud) 서버 스위치와 스토리지 오작동으로 인한 서비스 장애 발생
어도비	• 290만명 개인정보 유출
야후	• 45만명의 이용자 정보 유출
코드스페이스	• 디도스 공격으로 모든 자원 삭제

Source: 언론 보도자료 기반 삼정KPMG 경제연구원 재구성

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

이와 같은 보안사고는 잠재적 클라우드 이용자에게 보안에 대한 우려를 더욱 심화시켰다. 현재 클라우드 시장이 급성장하는 추세로 클라우드 컴퓨팅 이용자 또한 증가하고 있어 향후 보안사고 발생할 경우 그 피해규모는 과거보다 더욱 커질 것으로 예상된다.

따라서 클라우드 이용을 활성화하고, 관련 산업을 육성하기 위해서는 이용자들에게 클라우드를 안전하게 이용할 수 있다는 신뢰감을 줄 필요가 있다. 그러나 국내에서 클라우드가 이제 막 시작하는 단계이다 보니, 클라우드 보안은 물론이고 클라우드를 어떻게 활용해야 하는지에 대한 인식도 부족한 상황이다. 또한 국내 시장은 퍼블릭 클라우드를 이용하기보다 데이터센터 내 물리서버를 두고 이용하는 것을 더 선호하는 경향이 있다.

'클라우드 발전법'을 비롯하여 '정보통신기반보호법', '정보통신망이용촉진 및 정보보호 등에 관한 법률', '개인정보보호법', '통신비밀보호법', '신용정보이용 및 보호 등에 관한 법률' 등을 통해 클라우드 서비스 이용자 및 정보를 보호하기 위한 다양한 법률이 시행되고 있다. 그러나 현재 정책상으로는 클라우드 서비스 사업자의 정보보호 수준을 객관적으로 확인할 수 없어 이용자의 신뢰성이 부족하고, 정보유출, 해킹 등의 클라우드 사고 발생 시 대응하고 복구하는 체계가 명확히 정립되어 있지 않은 상황이다. 또한 가입·이용·사고발생·이용종료 등 클라우드 서비스 이용과정에서 발생할 수 있는 이용자 보호제도가 정착되어 있지 않으며, 클라우드 서비스의 보안 수준을 검증할 수 있는 국가 차원의 보안인증체계도 활성화되어 있지 않은 상황이다.

"우리나라는 보안에 대한 우려를 불식시킬 수 있는 제도적 뒷받침이 부족한 상태"

공공부문에 민간 클라우드 활성화를 저해하는 기존 정책

망분리란 기업 또는 공공기관 내부의 네트워크와 외부 네트워크를 완전히 분리시키는 것을 의미한다. 정부는 외부의 사이버테러로 인한 대형 보안사고를 막는다는 취지로 정보통신법을 개정(2012년)하여, 공공기관과 일정 규모의 기업을 대상으로 망분리를 의무화 시켰다. 이러한 망분리는 '물리적 망분리'와 '논리적 망분리'로 나누어지는데 '물리적 망분리'는 내부에서 업무용 PC와 개인용 PC의 구분을 확실하게 하는 것이고, '논리적 망분리'는 PC 한대에 데스크톱 가상화 기술을 이용해 내·외부 네트워크를 분리시키는 것이다.

"보안을 위한 망분리 정책이 공공부문에 퍼블릭 클라우드 도입을 제한"

망분리 정책은 클라우드 이용의 전제 조건인 인터넷 이용이 가능한 인터넷 PC의 기능을 크게 제한하기 때문에 퍼블릭 클라우드의 활용이 불가능하다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

이로 인해 'K-ICT 클라우드 활성화 계획'의 일환으로 조성되는 울산과 안산의 산업 클라우드 단지, 정부통합전산센터의 G-클라우드, 상암 클라우드 데이터센터 등이 모두 프라이빗 클라우드 형태로 구축되고 있다.

"클라우드 도입을 위한 기관별 분류 기준 등이 공공부문의 클라우드 도입 저해요인으로 작용"

현재 정부는 민간 클라우드 도입을 위해 정부 기관별 분류와 정보자원의 중요도에 따른 분류를 통해 중요도가 낮은 공공 데이터부터 우선적으로 민간 클라우드를 도입하겠다는 계획을 취하고 있다. 그러나 'K-ICT 클라우드 활성화 계획'에 따르면 중앙행정기관은 민간 클라우드 도입이 불가능하다. 중앙행정기관은 현재 행정자치부 정부통합전산센터가 마련한 정부 전용 클라우드인 'G-클라우드'만 이용할 수 있도록 했으며, 지자체나 공공기관은 자체 클라우드 구축(프라이빗 클라우드)을 권고하고 있다. 민간 클라우드를 우선 검토하도록 한 대상은 공공기관 가운데서도 정보자원 중요도가 '하'에 속하는 부분뿐이다. 정부의 이러한 접근 전략으로 인해 공공부문에서 민간 클라우드 활용은 매우 제한적일 수 밖에 없다. 또한 정보자원의 중요도에 따라 '상, 중, 하' 등급을 부여하는 '정보자원 등급제'도 현재 초안만 마련된 상태이다.

정보자원 중요도에 따른 클라우드 우선 적용 원칙

대상기관	정보자원중요도		
	상	중	하
중앙 행정기관	• G-클라우드	• G-클라우드	• G-클라우드 우선
지자체	• 자체 클라우드	• 자체 클라우드 • 민간 클라우드 검토	• 자체 클라우드 • 민간 클라우드 검토
공공기관	• G-클라우드 • 자체 클라우드	• 민간 클라우드 검토	• 민간 클라우드 우선

Source: 미래창조과학부

"비용이 크고, 준비기간이 오래 걸리는 CC인증에 대한 개선 필요"

또한 공공기관에 클라우드를 도입하기 위해서는 클라우드에 사용하는 하드웨어 장비나 소프트웨어 솔루션 등에 대해 각각 기존의 CC(Common Criteria, 공통평가기준)인증과 클라우드 환경을 위한 정보보호인증을 받아야 한다. 국가정보원에서 인증해주는 CC인증은 1억 원 이상의 비용과 1년 이상의 기간이 소요된다. 업계에서 대체 방안을 강구할 것을 요청하여, 정부는 인증제도의 비용을 줄이고 기간을 단축하겠다고 발표했으나, 구체적인 계획은 미정이다. 현재 국내 공공기관의 민간 클라우드 이용률은 0%다. 미래창조과학부 등 관계부처는 올해 최대 3% 수준까지 공공기관의 민간 클라우드 이용률을 높이겠다는 목표를 갖고 있지만, 관련 정책의 개선이 없다면 달성이 어려울 것으로 예상된다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

클라우드 활성화와 맞지 않는 산업별 규제

> "공공, 금융, 의료 등 주요 산업분야에서 클라우드 활성화 정책과 충돌하는 규제 존재"

국내 클라우드 활성화를 저해하는 주요 이슈 중 하나로 각 산업별 규제를 들 수 있다. 클라우드가 가장 활발히 활용될 것으로 예상되는 공공, 금융, 의료, 교육 등 주요 산업분야의 법 규제나 기존 관행이 클라우드 활성화에 장애물이 되고 있다. 이에 클라우드 활성화를 저해하는 불필요한 규제 개선을 위해 2015년 '클라우드 활성화 민간 규제개선 추진단'이 출범하였다. 또한 한국클라우드산업협회는 클라우드 사업자의 각종 규제 관련 애로사항을 해소하기 위한 'Cloud Help Center'를 운영하고 있다. 금융 분야 정보처리 위탁 규정('금융회사의 정보처리 및 전산설비 위탁에 관한 규정')은 정보처리의 제3자 위탁을 제한하고 있었으나 2015년 7월 개정됐고, 교육 분야의 도로교통법은 학원 내 서버 컴퓨터 등을 갖추도록 하고 있었으나 중앙집중식 서버 이용이 가능하도록 개선된 상태다. 또한 금융 분야의 망분리 규제, 교육 분야의 전산설비 규제, 의료 분야의 전자의무기록 관리보관을 위한 장비시설에 관한 규제 등이 2016년 내에 개선될 예정이다. 그러나 클라우드 활성화 정책과 맞지 않아 개정되어야 할 규제들이 훨씬 더 많이 남아있어, 규제 발굴 및 개선이 시급한 실정이다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

클라우드 컴퓨팅 규제개선 추진 현황

분야	규제명	법령	규제내용	비교
금융 (금융위)	전자금융업 감독 일반	정보처리위탁규정	• '금융회사의 정보처리 및 전산설비 위탁에 관한 규정'은 정보처리의 제3자 위탁을 제한하고 있었으나, 가능하도록 개선됨(2015.7월)	완료
교육 (경찰청)	운전학원 등 등록	도로교통법(제101조, 제104호) 및 시행령 (별표 5)	• '운전학원 학사관리 전산시스템 표준규격 고시'는 학원 내에 서버 컴퓨터 등을 갖추도록 하고 있었으나 중앙집중식 서버 이용이 가능하도록 개선(2015.5월)	완료
의료 (보건복지부)	전자의무 기록	의료법(제23조) 및 시행규칙(제16조)	• '전자의무기록 관리보존을 위한 장비시설'을 병원에 갖추도록 하고 있어(유권해석), 대안(시행규칙 개정)을 마련하여 제도 개선 중	시행규칙 입법 예고
교육 (교육부)	사이버대학 설립인가 기준 및 절차	평생교육법, 사이버 대학 설립·운영 규정 (원격교육 설비 기준 고시)	• '원격교육 설비 기준 고시'는 서버 설비 기준 등에서 '물리적으로 별도의 서버를 구성'하여야 한다고 규정하고 있음	개정 예정 (2016.6월)
금융 (금융위)	전자금융업 감독 일반	전자금융감독규정 (제15조) 및 시행세칙(제2조의2)	• 시행세칙 신설에도 불구하고 국내 소재 전산센터 및 정보처리시스템은 물리적 망분리를 요구(시행세칙제2조의2제2항)하여 규제 잔존	개정 예정 (2016.9월)
보건·의료 (보건복지부)	기탁등록 보존기관 지정	생명연구자원의 확보·관리 및 활용에 관한 법률(제8조) 및 시행령(제3조)	• 기탁등록보전기관 지정 요건: 생명연구자원 정보시스템 운영을 위한 전산장비, 백업시설 및 보안시설을 보유하고 이를 관리할 수 있는 전산담당자를 1명 이상 확보할 것	검토 중
ICT일반 (미래부)	공인전자 문서센터의 지정	전자문서 및 전자 거래기본법(제31조의2) 및 시행령 (제15조의 4) (공인전자문서센터 시설 및 장비 등에 관한 규정)	• 네트워크 보안기능을 구현하기 위하여 물리적으로 분리된 둘 이상의 네트워크 회선을 갖추어야 함 • 시스템을 안전하게 운영하기 위하여 시스템 운영실을 별도의 통제구역으로 구획하여야 함	검토 중
	공인전자 문서 중계자의 지정	전자문서 및 전자 거래기본법(제31조의2) 및 시행령 (제15조의14) (공인전자문서중계자 인력·기술 능력, 시설·장비 규정)	• 시설·장비 및 정보를 안전하게 운용하기 위한 보호설비로서 물리적으로 분리된 둘 이상의 망 회선 요구 • 중계자의 시설 및 장비를 위한 공간은 물리적으로 출입통제가 가능한 별도의 통제구역으로 구획	검토 중
주택 (국토부/ 미래부)	초고속 정보통신 건물 인증	지능형 홈네트워크 설치 및 기술기준(제13조)	• 아파트 단지가 '초고속정보통신건물'로 인증받기 위해서는 관련 규정에 따라, 반드시 단지 내에 서버를 설치·관리 해야함	검토 중

Source: 정보통신산업진흥원, 언론 보도자료 기반 삼정KPMG 경제연구원 재구성

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

해외 클라우드 도입 정책

국내 클라우드를 도입을 저해하는 요소로 보안에 대한 우려, 정책과 규제 개선 등을 해소하기 위해서는 정책적 지원이 필수적이다. 클라우드가 이미 활성화된 주요국에서 이러한 저해 요인을 극복하기 위해 클라우드 도입 정책과 보안정책, 이용자·정보 보호제도 등을 시행하였다. 국내에서 시행중인 클라우드 활성화 정책의 문제점을 해소하기 위해 주요국에서 과거 유사한 상황에서 취한 정책적 대응방안을 살펴본다.

미국: 'Cloud First Policy' 정책으로 공공부문에 우선 도입 추진

> "국가 정보화 예산의 25%를 클라우드 도입에 활용 권고"

2010년 미국 연방정부는 공공기관을 중심으로 한 클라우드 우선정책인 'Cloud First Policy'를 발표하고, 연평균 800억 달러 규모의 국가 정보화 예산의 25%를 클라우드 컴퓨팅 도입에 활용하도록 권고하며, 다양한 부처 및 공공기관에 글로벌 사업자의 서비스를 도입하였다. 또한 연방 정부의 정보자산 등급을 상, 중, 하로 구분하고, 중, 하 등급의 정보자산에 민간 클라우드 적용을 허용하였다. 공공기관을 중심으로 클라우드를 선제적으로 도입하여 클라우드 시장을 활성화하는 것을 목표로 하였으며, 미 재무부가 중앙 부처 중 최초로 주요 웹사이트를 아마존의 클라우드 서비스로 이관하였고, 2013년 미국 중앙정보국(CIA)은 아마존웹서비스(AWS)와 10년간 6억 달러 규모의 클라우드 구축 계약을 체결했다. 2014년에는 IBM이 미국 캘리포니아주와의 계약을 통해 '캘클라우드(Calcloud)'를 통한 IaaS 구축으로 컴퓨팅, 스토리지, 네트워크, 재해복구(DR)의 프라이빗 클라우드 구축을 시작했으며, LA, 뉴욕, 마이애미 등은 각각 구글, IBM, MS와 계약하여 현재는 다양한 공공기관에서 민간 클라우드를 이용하고 있다.

미국 캘리포니아에서 도입한 'CalCloud'는 캘리포니아주 167개 모든 공공기관이 함께 사용하는 클라우드 시스템으로 클라우드 도입 이전에는 공공기관이 개별적으로 약 600여개의 데이터 센터를 운영하고 있었다. 2014년 3월 민간기업인 IBM이 AT&T와의 계약을 통해 향후 5~7년 내 'CalCloud'를 구축 및 위탁 운영하기로 했다. 캘리포니아 주정부는 'Cloud First' 정책을 공표하고 이를 바탕으로 모든 주정부 기관 및 산학단체의 기존 또는 신규 시스템 업데이트와 구매는 'CalCloud'의 IaaS를 사용하도록 지시하였다.

> "클라우드 업체들 간 경쟁을 통해 보안수준을 제고하고, 글로벌 경쟁력 확보"

NIST(미국국립표준기술연구소, National Institute of Standards and Technology)는 미국 정부기관 내 안전하고 효과적인 클라우드 컴퓨팅 도입을 촉진하기 위하여 '클라우드컴퓨팅 기술 로드맵'(2014.10월)을 수립하였다. 이는 호환성(Interoperability), 이동성(Portability), 보안 표준(Security Standards), 가이드라인(Guidelines), 기술성(Technology) 등 최우선 요구사항과 이를 실현하기 위한 액션플랜 도출에서 보안 관련 사항을 중요시 하였다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

이처럼 공공부문에 선제적으로 클라우드를 도입하는 'Cloud First Policy'의 효과로 미국 공공분야는 각종 전산자원을 효율적으로 운영하면서 유지·보수비용을 절감하였다. 또한 미국 클라우드 업체들은 치열한 입찰경쟁 속에 보안 등 자체 서비스를 강화하여 글로벌 클라우드 강자로 부상하였다.

미국 공공기관 클라우드 서비스 도입 현황

분야	주요 내용
정부 조달	• Verizon, 정부 공동 구매 조달 기관과 클라우드 서비스 제공 협약 체결(2014.4월)
민원처리	• 산림청, 클라우드 기반 지식관리 시스템 구축 • 사회보장국, 클라우드 기반 FAQ 시스템 구축
정보관리 및 제공	• 국방정부시스템국, 클라우드 기반 콘텐츠 전송시스템 제공 • 국립항공우주국, 클라우드 기반 이미지 제공
행정 및 협업	• 국립해양대기청, 클라우드 기반 통합메시징 서비스 • 농무부, 21개 이메일 시스템 통합
의료	• 보건국, 전자건강기록 시스템에 클라우드 도입

Source: KT경제경영연구소

영국: 데이터 보안 분류 체계 간소화를 통해 공공부문에 클라우드 적극 도입

2009년 영국 정부는 IT 인프라 비용 효율화를 위해 공공기관을 대상으로 한 클라우드 서비스 도입 필요성을 제기했으며, 이에 클라우드 이용 활성화를 위해 2011년부터 공공 클라우드 전략인 'G-클라우드'를 도입했다. 2012년 2월, 'G-클라우드'의 일환으로 공공기관들이 민간 기업의 클라우드 서비스를 거래할 수 있도록 클라우드 서비스 쇼핑 포털 'Cloud Store'를 개설하였다. 또한 클라우드 컴퓨팅 비용절감 효과를 영국 정부의 전 공공기관으로 확대하기 위해 'Cloud First Policy'(2013년 5월)를 발표하고, 공공기관의 IT 인프라 구축 시 클라우드 서비스 도입을 고려하는 것을 의무화하였다. 약 2,000개 기업(이중 80% 중소기업)의 1만 9,553개 서비스가 클라우드 스토어에 등록되었으며, 부처별 전산실을 클라우드로 개선하는 것이 아니라 부처별 맞춤형 시스템을 도입하도록 하였다. 이에 2011년 클라우드 전략 수립 이후 현재까지 절감액이 약 2,000억 원에 달하는 것으로 예상되며, 4~5년 만에 클라우드 도입 기관 수 기준으로 클라우드 이용률이 40% 수준에 도달하였다.

> "공공기관들이 민간 기업의 클라우드 서비스를 거래할 수 있는 'Cloud Store' 개설"

영국 내각사무처는 공공기관의 클라우드 도입을 지원하기 위해 기존에 6단계로 분류되어 있던 데이터 보안 분류 체계를 3단계로 간소화하였다(2014년 4월).

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

영국 정부의 데이터 보안 분류 체계	
변경 전	변경 후
일급 기밀 정보(Top Secret)	일급 기밀 정보(Top Secret)
중요 기밀 정보(secret)	중요 기밀 정보(secret)
기밀 정보(Confidential)	공공 데이터(Official)
접근 제한 정보(Restricted)	
보호 정보(Protect)	
비 기밀 정보(unclassified)	

Source: 언론보도자료 기반 삼정KPMG 경제연구원 재구성

영국은 데이터 보안 분류 체계를 정비하면서 분류 대상 데이터의 90% 이상이 'Official'로 분류될 수 있도록 고려하여 기준을 수립했으며, 실제로 공공 데이터 대부분은(93%) 가장 낮은 수준인 'Official' 등급으로 분류되었다. 이러한 공공 데이터 보안 수준 완화로 민간 클라우드 사업자의 공공 클라우드 시장 진출이 활성화되었으며, 공공기관 역시 효과적인 클라우드 서비스 구축이 가능해졌다. 그 외 유럽과 중국은 시범사업을 통해, 호주와 일본은 공공부문 선제 도입을 통해 클라우드 도입을 활성화 하였다.

주요국 클라우드 도입 정책	
분야	주요 내용
미국	• 'Cloud First Policy'를 통해 공공부문에 선제적으로 클라우드를 도입하여 민간으로 확산 • 국가 정보화 예산의 25%를 클라우드 컴퓨팅 도입에 활용하도록 권고
영국	• 'Cloud First Policy'를 통해 공공부문에 선제적으로 클라우드를 도입하여 민간으로 확산 • 공공부문에 도입 활성화를 위해 데이터보안 분류 체계를 6단계→3단계로 간소화하고, 공공데이터를 가장 낮은 수준의 보안 등급을 받도록 설계
유럽	• '유로 클라우드 프로젝트'는 유럽 연합 차원의 체계적인 클라우드 확산을 위해 영국, 프랑스 등 일부 국가에 시범 적용 후, 적용 결과를 바탕으로 전역으로 확산시킬 계획 • 클라우드 컴퓨팅 표준화와 인증, 안전 및 공정 계약, 파트너십 제휴 등에 주력
호주	• 'Cloud First Policy'를 통해 공공부문에 클라우드 활성화를 통해 민간 확산 유도 • 이를 위해 클라우드 도입에 필요한 의사결정 및 행정절차를 간소화함
일본	• 공공부문에 클라우드를 선제적으로 도입하는 '가스미가세키 프로젝트'를 추진하였으며, 지자체를 대상으로 클라우드 시스템을 대대적으로 도입 • 2021년까지 모든 정부 정보 시스템의 클라우드화를 통해 운영비용 30% 절감, 지자체 정보 시스템 클라우드화 촉진 목표 발표
중국	• 베이징, 상하이, 선전, 항저우, 무시 등 5개 도시에서 클라우드 컴퓨팅 시범사업 추진 • 공공 클라우드 컴퓨팅 서비스 플랫폼 건설과 빅데이터 서비스, 솔루션 계획 및 보급을 중점 지원하기 위해 '클라우드 컴퓨팅 제13차 5개년 계획' 발표(2014.8월)
싱가포르	• '아시아 태평양 클라우드 컴퓨팅 허브' 구축을 위한 각종 육성 정책을 시행 중이며, 세계 최초로 데이터센터 파크(DCP, Data Center Park) 구축 • 'Productivity and Innovation Credit'을 통해 클라우드 컴퓨팅 관련 기업 활동에 세제 혜택 부여

Source: 삼정KPMG 경제연구원

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

해외 클라우드 보안 정책

"보안 인증 프로그램인 'FedRAMP' 운영으로 보안에 대한 신뢰성 제고"

미국: 까다로운 보안인증제도 운영으로 취득 기업의 경쟁력 제고

2012년 6월, 미연방 조달청(General Service Administration: GSA)은 안전한 클라우드 환경을 담보하기 위해 공공분야 클라우드 보안 인증 프로그램인 'FedRAMP(Federal Risk and Authorization Management Program)'를 발표했다. FedRAMP는 기존 IT 환경 하에서 발생하는 예산 활용의 비효율성과 자원관리 시스템 취약성, 조달 프로세스의 복잡성 등을 개선하려는 목적에서 제정되었다. 2012년 6월 GSA가 FedRAMP의 공식 실행을 발표하면서 인증 작업을 개시하였으며, 17개 분야, 325개 통제기준으로 구성되어 있다. 각 항목마다 중요도와 민감도에 따라 가중치를 부여해 보안등급이 'Low-level', 'Moderate-level'로 나누어 엄격하게 구성되어 있으며, 'NIST SP 800-53 지침(미 연방정부의 정보시스템 및 개인정보 보안지침)'을 기반으로 인증체계가 설계되었다. FedRAMP는 인증 후 지속적인 모니터링을 수행하는데, 연방 정부가 조달한 클라우드 서비스 항목에 대해 정기적으로 보고서를 작성하도록 요구한다. 기간 내 해당 보고서를 제출하지 않을 경우 인증효력을 상실할 수 있으며, 이러한 사후관리를 통해 클라우드 서비스의 보안 수준을 일정하게 유지하도록 하고 있다.

FedRAMP 인증 유지를 위한 제출 보고서

제출 보고서	주기
사고보고	연속 및 지속
사고대응계획 및 테스트 보고서	분기별
POA&M 업데이트	매년
취약점 스캔 보고서	매년
시스템 보안 계획 업데이트	매년
IT 비상 계획 업데이트 & 테스트 보고서	매년
IT 보안 인식 훈련 기록	매년
구성 관리 계획 업데이트	매년
물리 접근 검토	매년
보안 평가	매년
IT 보안 정책	매년

Source: 한국인터넷진흥원

미국은 FedRAMP 도입으로 연방정부 클라우드 이용에 가장 큰 장애요인인 보안문제는 물론, 중복인증에 따른 비효율성을 해결하여(IT 예산의 10~20% 절감) 국무부, 재무부 등 7개 부처가 101개의 클라우드(48개는 민간 클라우드)를 이용하고 있다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

다만 높은 보안수준을 요구하는 'NIST SP 800-53'을 기반으로 함에 따라 통제항목 수가 많고 인증절차가 복잡하나, 인증 취득 시 보안수준을 인정받아 글로벌 경쟁력을 확보할 수 있다는 장점이 있다.

일본: 정보보호 표준에 클라우드 특성을 반영한 인증제도 운영

일본은 정부에서 클라우드 정보보안 관리지침을 수립·발표하고, 민간단체인 '일본정보감사협회(JASA)'는 퍼블릭 클라우드 서비스를 대상으로 외부 전문가 등을 활용하여 정보보안 감사를 실시한다. '정보보안 관리지침'은 일본 정보보호 표준(JISQ 27001) 및 국제표준(ISO 27001:2013)을 기반으로 클라우드 특성을 반영해 총 12개 분야 135개 통제항목으로 구성되어 있다.

재단법인 멀티미디어 진흥센터(Foundation for Multimedia Communications, FMCC)는 2008년 'ASP-SaaS 서비스 정보 공개 인증', 2012년 'IaaS-PaaS 서비스 공개 인증', 2012년 '데이터 센터 서비스 정보 공개 인증'을 시행 중인데, 이러한 3가지 서비스 영역 인증 제도를 '클라우드 서비스 안전·신뢰성에 관한 정보 공개 인증제도'라고 총칭하여 운영하고 있다. 인증 유효기간은 2년이다.

영국: 3BIL 수준으로 구분하여 보안인증 실시

영국은 정부기관에서 이용하는 클라우드 서비스인 'G-클라우드'에 대한 안전성 확보를 위해 '클라우드 서비스 보안원칙' 준수 여부를 인증하는 제도를 운영한다. 이는 국제표준화기구에서 제정한 정보보호 관리체계에 대한 국제표준 ISO 27001을 기반으로 클라우드 특성을 고려하여 개발되었으며, CESG(국가정보보증기술국)에서 인증을 실시한다. G-클라우드의 인가는 BIL(Business Impact Level) 수준으로 구분된다.

G-클라우드 BIL 평가

분야	주요 내용
BIL/BIL1	• ISO/IEC 27001 인증 기반으로 이루어지며, 인증 범위는 서비스 제공자와 범정부인가처(PGA) 협의로 결정됨
BIL2	• 서비스 제공자는 ISO 27001 인증서와 함께 RMADS(위험관리 인가문서)와 잔여 위험 및 미해결 이슈 등의 정보를 증적으로 제출
BIL3	• 영국 정부의 정보보증(IA) 표준 및 지침에 따르는지 점검하기 위하여 PGA가 직접 현장 실사를 수행(국외도 해당)
BIL4	• BIL4이상의 기밀은 사설 클라우드 서비스로 구현되어야 함

Source: 한국클라우드보안협회

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

싱가포르: 보안 인증 취득비용의 70% 정부에서 지원

민간 클라우드 서비스 제공자에 대한 안전성 확보를 위해 MTCS(Multi-tier Cloud Security) 인증을 도입하여 운영 중이다. MTCS는 자율 인증이지만 공공 클라우드 입찰 시 필수 요건이며, 유효기간은 인증 취득 후 3년으로 제한된다. 클라우드 사업자의 MTCS 총 취득비용의 70%를 정부에서 지원하고 있다. MTCS는 국제표준(ISO 27001:27005)을 바탕으로 총 19개 분야 117개 통제항목을 제시하고 있으며, 항목별 보안등급을 보안 수준이 낮은 일반적인 서비스, 일반적으로 기업에서 요구하는 서비스, 특정 기업에서 요구하는 서비스의 3단계로 구분하고 있다.

MTCS 항목별 보안등급 기준 예시 평가

구분	설명	예시
1단계	• 보안수준이 낮은 일반적인 서비스	• 시험 및 개발, 공공 정보 웹사이트 등
2단계	• 일반적으로 기업에서 요구하는 서비스	• 이메일, CRM, 개인식별정보 등
3단계	• 특정 기업에서 요구하는 서비스	• 금융, 민감한 정보를 요구하는 헬스케어 시스템 등

Source: 한국인터넷진흥원

해외 클라우드 보안인증 운영현황

국가	인증명	인증기준	인증기관	평가기관	비고
미국	FedRAMP	NIST SP 800-53	FedRAMP PMO (운영사무국)	공인기관 (총 38개 기관)	• 연방정부에 도입되는 민간 클라우드 서비스 대상 • 국가 인정 공인기관에서 평가
영국	UK G-클라우드	ISO-IEC 27001 +자체규정	CESG (국가정보 보증기술국)	-	• 국가 인정 공인기관에서 평가
일본	JCISPA	클라우드 정보보안 기준	JASA (일본 정보 보안감사협회)	JASA(인증 심사위원회)	• 퍼블릭 클라우드 서비스 대상 • 민간 협회에서 운영
	ASP·SaaS 인증 IaaS·PaaS인증 데이터센터 인증	클라우드서비스 관한 정보공개 지침	ASPIC(일본 ASP 산업협회)	ASPIC(인증 심사위원회)	• 국가에서 인정한 협회에서 수행
싱가포르	MTCS-SS	ISO-IEC 27001 +자체규정	ITSC (정보기술 표준위원회)	공인기관 (총 7개 기관)	• 국가 인정 공인기관에서 평가
호주	ASD CCSL	ISO-IEC 27001 +자체규정	ASD (호주 신호국)	IRAP(인증 심사위원회)	• 독립적 보안 등록 평가자가 수행한 종합적인 평가를 승인

Source: 한국인터넷진흥원

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

해외 클라우드 이용자보호 제도

"미국: 자국 내 정보에 대한 정부의 감시와 조사권을 폭넓게 인정"

미국: 정보유출 방지를 위해 정부의 감시와 조사권 강화

미국은 클라우드 활용 중 정보보호에 관한 문제가 발생하는 경우 각 영역의 개별법을 통해 규제한다. '미국 보호법(Protect Americana Act)'에서는 미국 영토 내의 사람이나 단체에 대한 통신제한 조치는 법원의 명령이나 관리 하에 이루어지도록 하고 있다. '데이터 침해 통지법(Data Breach Notification Act)'에서는 정부기관과 기업이 개인정보가 이미 공개됐거나 공개되었을 것으로 추정될 때 당사자에게 그 사실을 고지해야 하며 대규모 데이터 침해가 벌어졌을 경우, 정부기관과 기업은 미국첩보부에 보고하도록 하고 있다. '개인정보보호와 보안법(Personal Data Privacy and Security Act)'에서는 민감한 정보에 대한 침해 위험 평가와 취약성 테스트, 통제 등에 관한 가이드라인을 제시하고 있다. 개인정보를 보관하고 있는 기관이 침해사고가 발생했을 때 잠재적 피해자와 사법 기관에 그 사실을 통보하도록 하고 있다.

'전기통신비밀보호법(ECPA: Electronic communications Privacy Act)'은 전자통신기록에 불법적으로 접근하거나 보유 정보를 허가없이 공개하는 것을 예방하고자 제정된 것으로 클라우드 서비스 이용자의 개인 프라이버시를 보장받을 수 있도록 하고 있다. 'GLB Act(Gramm-Leach Bliley Act)'는 기업들이 고객정보 보호방법에 대해 설명한 보안계획서를 직접 작성하도록 하여 클라우드 이용자에게 개인정보를 안전하게 보호한다는 것에 대한 신뢰를 제고할 수 있도록 하고 있다. '애국법(USA PATRIOT Act)'은 컴퓨터를 통한 외부자의 공격에 대한 법집행 절차로 정부의 감시와 조사권을 폭넓게 인정하여 클라우드 컴퓨팅 서비스를 통한 국가 정보의 유출 등을 방지하기 위한 법으로서의 역할을 하고 있다.

"유럽: 미국 기업으로의 정보유출을 막기 위해 해외 클라우드 서비스 기업에 대한 규제에 집중"

유럽: 해외 기업으로 정보유출 방어에 집중

EU의 초기 클라우드 컴퓨팅 관련 법제도는 활성화에 중점을 두었으나, 최근에는 클라우드 컴퓨팅 서비스 기업이 대부분 미국 기업이라는 것에 중점을 두고 서비스 이용자들의 개인정보가 해외로 유출되는 것을 막기 위한 해외 클라우드 컴퓨팅 서비스 기업들에 대한 규제에 집중하고 있다. '데이터보호법'은 유럽연합의 데이터보호 지침에 관한 요구에 따라 발표되었으며, 정부기관이나 개인 기업들이 보유하는 기록들에 대한 내용들을 규제하고 개인정보의 사용에 대한 제한, 기록의 정정과 접근, 정보를 보유하는 기관이 정보위원장에 해당 기록을 등록하도록 의무화하고 있다. '프라이버시 및 전자통신규칙(Privacy and Electronic Communications Regulations)'은 통신서비스의 보안문제, 통신의 비밀보장과 관련한 프라이버시 보호 문제 등을 규정하고 있다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

일본: 개인정보 유출사고를 기점으로 관련 법률 제정

2011년 클라우드 서비스 업체 'First Server'의 초대형 전산장애로 대규모 개인정보가 유출되면서 클라우드 환경에서의 정보보호의 중요성이 더욱 부각되었다. 이후 총무성을 중심으로 클라우드 서비스에 있어서 정보 보유 및 관리에 대한 가이드라인을 만들어 배포하고 있으며, 개별법적으로 클라우드 컴퓨팅 환경에서 정보 보호에 대한 내용을 포함하는 법률들을 각 분야별 정부 기관에서 시행하고 있다.

'고도정보통신 네트워크 사회형성 기본법'은 대표적인 IT법률로 고도 정보통신 네트워크 사회의 형성에 관한 시책을 신속하고 중점적으로 추진하는 것을 목표로 하고 있으며 네트워크의 안전성 및 신뢰성, 개인정보보호의 확보를 기본방침 중 하나로 정하고 있다. '특정 전기통신서비스제공자의 손해배상 책임 제한 및 발신자 정보의 개시에 관한 법률'은 인터넷 이용자의 권리침해로부터 일정 부분 온라인서비스제공자를 보호하고 정보의 유통을 촉진시키기 위해 제정되었다. 인터넷에서 송수신되는 정보에 의해서 피해를 받은 경우 전기통신서비스제공자 등은 일정한 기준에 따라 배상 책임을 지게 되며, 동시에 정보의 발신자를 공시하는 권리를 인정한다.

해외 클라우드 이용자보호 법제도 현황

	미국	EU	일본
클라우드 관련법 동향	• 개별법들의 개정을 통해 클라우드 환경에서 발생할 수 있는 보안 사고로부터 정보보호 • 민간 자율규제 원칙 • 클라우드 컴퓨팅법 제안	• 1998년 10월, EU 개인정보지침 발표 및 가맹국의 국내법과 조화 • ENISA(유럽정보보안기구) 주도 클라우드 환경의 활성화와 개인정보보호를 포함한 보안에 대한 범유럽적 지침과 규칙 발표	• 총무성 가스미가세키 프로젝트를 통해 클라우드 컴퓨팅 활성화와 법제도 마련 • 경제산업성 'SaaS용 SLA' 가이드라인 발표(개인정보 관리 및 취급과 보안 방법을 세분화)
법제도 정비	• 미국보호법 • 데이터침해통지법 • 개인정보보호와 보안법 • 전기통신비밀보호법 • GLB 법 • 공적신용정보법 • 프라이버시법 • 금융프라이버시법 • 전자통신프라이버시법 • 컴퓨터보안법 • 의료프라이버시법	• EU 데이터 보호 지침 • EU 데이터 온라인 보호 지침 • 전자통신영역에서 개인정보처리 및 프라이버시 보호에 관한 지침	• 고도 정보통신 네트워크 사회 형성 기본법 • 개인정보보호법 • 특정 전기통신 서비스 제공자의 손해배상 책임 제한 및 발신자 정보의 개시에 관한 법률 • JIS Q 15001(PIM S)

Source: 한국인터넷진흥원, 삼정KPMG 경제연구원 재구성

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

국내 클라우드 도입 활성화를 위한 정책: Speed up 필요

사물인터넷, 인공지능, 빅데이터 등 기술 발전과 함께 클라우드가 세계 IT 시장에서 새로운 패러다임으로 자리잡고 있으며, 향후 클라우드 시장규모가 급격히 성장할 것으로 예상되어, 주요국에서는 이미 클라우드 도입이 활발히 이루어지고 있다. 국내에서도 클라우드 도입 활성화를 위해 2015년 9월 '클라우드 발전법'을 시행하고, 같은 해 11월 'K-ICT 클라우드 컴퓨팅 활성화 계획'을 확정했다.

BSA(Business Software Alliance)가 글로벌 IT시장의 80%를 차지하는 총 24개 IT 강국의 클라우드 컴퓨팅 관련 정책에 대해 평가한 결과, 일본이 1위를 차지하고, 그 뒤로 미국, 독일, 캐나다, 프랑스가 상위권에 위치한 것으로 나타났다. 한국은 2013년 8위에서 2016년 12위로 4단계 하락한 것으로 나타났다. 이는 국내 클라우드 컴퓨팅 관련 법규 및 제도적 기반이 클라우드 활성화에 긍정적인 영향을 미치지 못하고 있음을 의미하며, 실제로 법이 시행된 지 7개월이 경과한 현재 국내 클라우드 도입은 미진한 상황이다. 정부는 클라우드 활성화 정책의 일환으로 제5차 규제개혁장관회의(2016년 5월)에서 클라우드 확산을 막는 일부 규제를 개선하기로 결정했다. 이처럼 정부에서 클라우드 활성화를 위해 적극적으로 정책적 지원을 하고 있으나, 클라우드 선진국을 따라잡기 위해서는 좀 더 속도를 낼 필요가 있다.

> "클라우드 컴퓨팅 관련 정책 수준이 주요국 대비 미흡한 것으로 조사"

특히, 공공부문에 선제적 도입을 위한 실효성 있는 정책을 수립할 필요가 있으며, 클라우드 도입에 가장 큰 애로사항인 보안 이슈를 해소할 수 있는 방안 마련이 필요하다. 또한 산업별 관련 규제 완화를 통해 클라우드 도입을 활성화 해야한다.

국내 클라우드 활성화 방안

- 공공부문에 선제적 도입을 위한 실효성 있는 정책 수립
- 클라우드 활용에 대한 보안 이슈 해소
  - ① 정부의 보안인증 및 이용자 보호 제도 도입
  - ② 클라우드 업체의 보안 수준 제고
  - ③ 이용자의 인식 전환 및 정보보호 노력
- 산업별 규제 완화를 통해 클라우드 도입 활성화

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

공공부문에 선제적 도입을 위한 실효성있는 정책 수립

> 공공부문 클라우드 도입을 위해 기관별 분류보다 중요도에 따른 분류를 우선시 할 필요

주요국에서는 클라우드를 활성화 시키기 위해 공공부문에 클라우드를 선제적으로 도입하여 안전성을 검증하고, 검증된 클라우드 서비스를 민간에 확산시키는 정책을 시행했다.

현재 정부에서도 공공부문에 클라우드 선제 도입을 통해 민간으로 확대시키는 전략을 취하고 있으나, 공공부문 클라우드 도입에 있어 데이터의 중요도보다 기관별 분류를 우선하고 있어 공공부문에 민간 클라우드가 확산되기는 어려운 상황이다. 중앙행정기관의 데이터는 중요도와 관계없이 무조건 'G-클라우드'를 활용하도록 되어 있으며, 공공기관의 정보자원 중 중요도가 낮은 데이터만 민간 클라우드 활용을 권고하고 있다. 국내 클라우드 확산을 위해서는 기관별 분류보다 중요도에 따른 분류를 우선할 필요가 있다. 또한 데이터의 중요도에 관해서도 영국의 사례와 같이 중요하지 않은 공공데이터는 낮은 중요도 등급을 부여받아 클라우드를 적극 활용할 수 있도록 '정보자원 등급제'를 설계할 필요가 있다. 영국은 클라우드 활성화를 위해 데이터 분류체계를 6단계→3단계로 간소화하였으며, 공공 데이터의 대부분을 가장 낮은 보안 수준인 'Official' 등급으로 포함하였다.

또한 공공부문에 클라우드 도입을 위해 수반되는 다양한 절차와 의사결정 과정을 간소화하고(호주), 클라우드 인증에 소요되는 비용 지원 또는 클라우드 기업에 세제 혜택(싱가포르) 등을 통해 공공부문에 클라우드 도입을 활성화하고 클라우드 시장에서 국내 기업들이 더욱 활발히 활동할 수 있도록 정부는 실효성 있는 정책을 통해 적극적으로 지원할 필요가 있다.

클라우드 활용에 대한 보안 이슈 해소

> 보안 우려 해소를 위해서는 정부의 인증제도, 서비스 제공자의 보안수준 제고, 고객의 인식전환 등이 필요

클라우드 활성화의 보안 이슈를 해소하기 위해서는 정부의 보안인증 및 이용자 보호제도, 서비스 업체의 보안력, 서비스 이용자의 인식전환과 정보보호 노력 등이 모두 필요하다. 정부는 보안인증제도를 운영하여 클라우드 서비스의 보안수준을 보장해주고, 보안 사고발생 시 대응체계를 수립하는 등 이용자를 보호하기 위한 제도를 구축할 필요가 있다. 서비스 업체는 보안 수준을 제고하고 공신력있는 인증을 획득함으로써 고객에게 신뢰를 제공해야 한다. 이를 통해 서비스 이용자는 막연한 보안 우려를 해소하는 한편, 클라우드를 활용하면서 스스로 정보를 보호하기 위한 보안 노력을 기울일 필요가 있다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

① 정부의 보안인증 및 이용자 보호 제도 도입

클라우드와 관련된 정보보안 정책은 다른 IT 환경과는 다르게 정보보호가 강제 또는 규제의 성격을 갖는다기보다 클라우드 이용에 가장 큰 장애요인인 정보보호 우려를 불식시킴으로써 서비스 이용 활성화를 위한 발판을 마련해주는 역할을 한다고 볼 수 있다.

클라우드 선진국인 미국은 외부 자료 유출에 대한 경계가 매우 강할 것으로 예상되는 미 중앙정보국(CIA)이 아마존웹서비스(AWS)를 이용해 클라우드를 구축했다. CIA는 AWS가 제공하는 퍼블릭 클라우드의 기능을 그대로 옮겨가 프라이빗 클라우드를 구축했으며, 최근에는 미 연방항공국(FAA)도 AWS 클라우드 도입을 결정했다. 이는 미국이 클라우드를 안심하고 이용할 수 있도록 보안 인증제도를 철저히 운영하여 퍼블릭 클라우드의 보안 수준을 제고하고 이에 대한 인식을 변화시킨 것에 기인한다. 미국뿐만 아니라 영국, 일본 등 클라우드 선진국에서는 클라우드 활용에 대한 보안 수준을 보장해 주기 위해 신뢰성있는 보안인증제도를 운영하고 있다. 우리나라도 이용자 신뢰도 향상 및 서비스 제공자의 보안수준을 제고하고자 '정보보호에 관한 기준 고시(안)'을 제정했다. 개인정보나 기밀 사항 등 민감한 정보를 다루는 공공부문은 보다 높은 수준의 보안성 및 심도있는 검증이 요구되기 때문에 공공기관이 안전하게 민간 클라우드를 이용할 수 있도록 보장해주는 제도적 장치를 마련한 것이다.

정보보호 고시(안)의 주요 내용을 살펴보면 정보의 공유·위탁 특성을 감안해 데이터 보호 및 암호화가 강화됐으며, 클라우드 핵심기능인 가상화의 중요성을 고려해 가상화 보안 부문을 가상화 인프라와 가상화 운영환경으로 세분화했다. 또한 이용자 보호를 위해 '클라우드 발전법'에서 규정한 침해사고 및 장애발생 보고, 정보 공개 등을 반영했으며, 전산장비 안전성, 물리적 분리, 이중화 및 백업체계 구축 등 공공기관에서 이용할 경우 필요한 사항들이 추가됐다.

클라우드 정보보호 기준(안)

구분	주요 내용
관리적 조치	• 정보보호 정책 및 조직, 인적보안, 자산관리, 서비스 공급망관리, 침해사고 관리, 서비스 연속성 관리, 준거성
물리적 조치	• 물리적 보호구역 지정 및 보호, 정보처리 시설 및 장비보호
기술적 조치	• 가상화 보안, 접근통제, 네트워크 보안, 데이터 보호·암호화, 시스템 개발 및 도입 보안
공공기관추가 조치사항	• 보안서비스 수준 협약, 도입전산장비 안전성, 물리적 분리, 이중화 및 백업체계 구축, 암호화 기술 제공, 보안관제 제반환경 지원

Source: 미래창조과학부

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

아울러 클라우드 서비스 제공자가 정보보호 기준 준수 여부를 미래부에 확인 요청하는 경우 전문기관(한국인터넷진흥원)을 통해 시험·평가를 실시할 수 있도록 했다. 정보보호 고시(안)은 미국, 유럽 등 주요국의 보안인증제도, 국제표준(ISO 27001)과 '클라우드 발전법'에서 규정한 정보보호 조치사항 등을 핵심요소로 삼아 관리적·물리적·기술적 보호조치 및 공공기관용 추가 보호조치 등 총 14개 부문의 118개 통제항목으로 마련됐다. 해당 고시(안)에 따른 클라우드 서비스 보안인증은 2016년 5월부터 클라우드 서비스 업체의 신청을 받을 예정이며, 소요되는 기간은 최소 3개월로 예상된다.

정보보호 고시(안)이 마련되면서 클라우드 서비스 제공자의 정보보호 수준 및 이용자 신뢰도가 향상될 수 있을 것으로 예상되나, 현재 발표된 고시(안)은 IaaS 중심으로 구성되어 있으며, PaaS, SaaS에 대한 보호조치는 일부만 포함되어 있어 추가적인 보완이 필요하다. 미국의 'FedRAMP'는 공공부문에 클라우드를 도입하기 위해 취득해야 하는 보안인증제도로 절차가 까다롭다는 단점이 있지만 엄격한 평가 기준으로 인해 해당 인증을 취득한 클라우드 업체들은 글로벌 시장에서 보안 수준을 인정받아 경쟁력을 확보할 수 있었다. 우리나라도 보안인증제도를 취득한 기업의 신뢰성을 보장할 수 있도록 새롭게 지정한 보안인증제도를 보다 정교하게 설계하고 활성화시킬 필요가 있다.

> "공신력 있는 보안인증제도를 통해 국내 기업의 신뢰성 및 경쟁력 제고에 기여"

클라우드 서비스 이용자 및 정보 보호를 위한 관련 제도들은 주요국에서도 각국의 상황에 따라 상이한 것으로 나타났다. 클라우드 컴퓨팅 서비스를 제공하는 기업들이 대부분 미국 기업이기 때문에 대부분의 국가들의 관련 제도는 정보의 해외 유출 등을 어떻게 예방하고 방어할 것인지에 치중된 것으로 나타났다. 반면 미국은 정보보호를 위해 필요한 경우에 각 개별법의 적용을 받는 한편, 각 분야 개별법을 통해 개인정보 유출을 방지하고, 애국법 등으로 자국 내 정보에 대한 정부의 접근 권한을 강화하는 것으로 나타났다.

우리나라는 클라우드 서비스 이용자 및 정보를 보호하기 위해 다양한 법제도들이 산재하고 있다. 클라우드 이용자 보호에 특화된 제도적 장치 마련을 위해 '클라우드 발전법'을 시행하고, 이에 따라 보안사고 예방, 대응체계와 이용자 정보 보호제도 등을 정보보호 고시(안)을 통해 마련하였다. 사고 발생 시 즉각적으로 서비스 이용자에게 사고내용을 보고하도록 하였으며, 이용자가 사업자와 대등한 입장에서 이용계약을 체결하여 피해가 발생하지 않도록 이용자 정보의 보호 및 관리, 사고·장애 시 고지, 계약의 해지, 손해배상 등을 규정하고 있는 표준계약서를 제정·권고하였다. 또한 서비스 중단 시 이용자 정보 손실 방지를 위해 제3의 기관에 데이터를 보관하는 임치제도를 도입하고, 사고 발생시 피해 보상을 위한 보증보험 가입을 확대하였다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

> 클라우드 선진국을 빠르게 추격하기 위해서는 클라우드 활성화를 위한 정책적 뒷받침이 그 첫걸음

주요국에 비해 클라우드 시장 진입이 늦은 우리나라가 클라우드 시장에서 우위를 선점하기 위해서는 우선 선도자들을 빠르게 추격할 필요가 있다. 이러한 추격의 가장 큰 장애요인이 보안에 대한 우려이며, 이를 해결하기 위한 정부의 제도적 지원이 빠른 추격의 첫 걸음이라 할 수 있다. 주요국의 관련 정책 및 제도들을 벤치마킹하여 설계된 정부의 보안인증제도와 이용자 보호제도 등이 멀지 않은 미래에 활성화될 것으로 예상되며, 이러한 정책들이 시행착오를 최소화하고, 효과적으로 추진되기 위해서는 제도 제정 및 시행 초기부터 다양한 이해관계와 환경적 요인을 고려하여 국내 실정을 반영할 필요가 있다.

② 클라우드 업체의 보안 수준 제고

클라우드 컴퓨팅이 활성화되기 위해서 클라우드 서비스를 제공하는 사업자들은 제공하는 IT 인프라가 신뢰할 수 있으며, 그 속에 저장되는 고객들의 정보가 안전하게 보호되고 있다는 것을 고객들에게 인식시킬 필요가 있다. 클라우드 서비스 제공자는 클라우드 컴퓨팅을 위한 안전한 보안 플랫폼을 구축해 외부 침입자로부터의 공격을 방어해야 하며, 클라우드 내부 악의적인 이용자로부터의 공격을 모니터링하고 차단하는 기술을 갖추어야 한다.

클라우드 컴퓨팅 같은 거대 IT 인프라를 보호하기 위해서는 수준높은 보안 인력 및 기술을 활용해 보안장벽을 구축해야 한다. 이용자들에게 투명한 보안 서비스를 구축해 이용자 편의성을 증진해야 하며, 보안시스템 구축으로 인한 시스템 성능 훼손을 최소화해야 한다. 또한 자연재해나 사고로 인한 IT 자원의 손실을 방지하기 위해 재난복구 및 데이터백업 시스템을 구축해야 한다.

> 클라우드 서비스 제공자는 보안사고 예방 및 대응을 위한 기술 개발 필요

더불어 스스로의 보안수준을 공신력있는 기관에서 인증받아 신뢰성을 제고할 필요가 있다. 한국인터넷진흥원에서 국내 실정에 적합한 보안인증제도를 수립하여 2016년 5월 시행할 계획에 있으나, 현재는 IaaS 서비스만을 대상으로 한 보안인증제도만 준비된 상황이다.

클라우드 서비스 업체들은 ISO 27001과 같은 정보보호 관리체계에 대한 국제표준인증, 정보보호관리체계인증(ISMS) 또는 서비스 제공과 운영절차들의 관리 수준 및 신뢰성을 검증해 발급하는 SOC(Service Organization Control) 인증 등을 취득하여 스스로 보안수준을 증명하기 위해 노력할 필요가 있다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

> 서비스 이용자에게 신뢰를 줄 수 있도록 보안인증 취득 노력 필요
>
> 또한 보안인증 취득 후에도 꾸준히 보안수준 제고 노력 필요

그러나 보안인증을 취득한 것이 보안문제가 전혀 없다는 것을 의미하지는 않으며, 서비스 제공을 위한 최소한의 기준을 충족했다는 의미로 볼 수 있다. 서비스 업체는 보안인증 취득 후에도 꾸준히 보안수준을 제고하기 위한 노력을 기울일 필요가 있다.

③ 이용자 인식 전환 및 정보보호 노력

정부의 보안인증제도와 서비스 제공자의 보안 수준 제고 노력을 통해 보안 이슈가 해소되었더라도 클라우드 보안사고가 발생할 경우, 클라우드 보안에 대한 우려는 재현될 가능성이 높다.

> 서비스 이용자로 인한 보안사고 발생 가능성을 고려하여 이용자 수준에서 정보보호 노력

CSA(Cloud Security Alliance, 클라우드 보안 동맹)에서 IT 전문가들을 대상으로 실시한 설문에 의하면 응답자의 64.9%가 클라우드가 기업 내 네트워크보다 더 안전하다고 답했다. 또한 가트너는 '2016년 발생하는 보안사고의 95%는 클라우드 기업이 아니라 이용자 때문일 것'이라고 예측했다. 클라우드 서비스를 도입한 경우, 이용자 역시 보안에 대한 인식을 전환하고, 사고를 방지하기 위해 투자를 강화할 필요가 있다. 클라우드 업체들이 이용자의 보안 우려를 해소하기 위해 경쟁적으로 보안 수준을 제고하는 현 상황에서는 서비스 제공자보다 이용자로 인해 보안사고가 발생할 가능성이 더 높다고 판단된다.

클라우드를 사용하면서 보안 사고가 일어날 경우, 서비스 이용자만 피해를 보는 것이 아니라 클라우드를 도입하려 했던 잠재적 이용자들도 클라우드에 대해 부정적으로 생각할 수 있다. 또한 클라우드 서비스 제공자도 해당 기업으로 인해 비즈니스에 영향을 받을 수 있기 때문에 이용자도 정보보호를 위해 노력을 기울일 필요가 있다.

산업별 규제 완화를 통해 클라우드 도입 활성화

산업 규제로 인해 클라우드를 도입하지 못한 사례로 최근 인터넷전문은행 사례를 들 수 있다. 카카오는 카카오뱅크를 구축할 때 퍼블릭 클라우드 형태의 인프라를 생각했지만 금융감독원에서 이를 거절하여 큰 비용을 들여 전통적인 전산실 형태의 프라이빗 인프라를 구축하기로 했다.

KT 컨소시엄 주도의 인터넷전문은행 케이뱅크의 경우 KT가 구축해 놓은 '유클라우드' 인프라를 활용하고자 했으나, 기존 금융규제에 인터넷전문은행과 같은 신산업에서 금융감독원의 전자금융 감독규정 등에 따라 클라우드 컴퓨팅을 활용할 수 없는 상황이다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

국내 클라우드 도입 이슈 분석: 주요국 관련 정책을 중심으로

전자금융감독규정(제15조 해킹 방지 대책 등)에 따르면 전자상거래, 금융결제 등을 위한 클라우드 시스템의 업무망은 인터넷 등 외부통신망으로부터 물리적으로 분리할 것을 명시하고 있으며, 방화벽이나 IPS, 웹 방화벽 등 보안제품에 대한 원격 접근도 금지하고 있다. 그러나 특성상 클라우드 시스템의 경우 원격 관제가 불가피하기 때문에 이를 허용하지 않고 있는 기존 금융감독 규정과 클라우드 활성화 정책은 정면으로 충돌된다.

"클라우드 도입으로 경쟁력 제고가 예상되는 산업에 대해서 규제 개선 필요"

제5차 규제개혁장관회의에서 정부는 클라우드 이용 관련 규제를 개선할 목적으로 우선 파급효과가 클 것으로 기대되는 금융, 의료, 교육 분야의 서버·망분리 지침을 개선하겠다고 발표했다. 그러나 민감한 정보를 제외한 업무에 대해서만 물리적 망분리의 예외를 허용한다는 방침으로 정보의 민감성에 대한 기준부터 명확하게 설정해야 해당 규제 개선이 효과적으로 작용할 것으로 판단된다. 또한 이 외에도 클라우드를 예상하지 못한 상태에서 도입된 숨은 규제들이 많이 존재하고 있으며, 이러한 규제들로 인해 기업에서 클라우드의 활용이 제한되는 경우가 있다. 클라우드의 도입이 모든 산업에서 필수는 아니며, 모든 산업에서 도움이 될 것이라는 보장은 없다. 그러나 각 산업의 발전을 저해하지 않는 선에서 클라우드 도입을 통해 다양한 이점을 얻을 수 있는 경우에는 각 산업의 규제를 적절한 선에서 개선하여 산업의 경쟁력을 제고할 필요가 있다.

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

삼정KPMG 경제연구원

김범석
원장
T: 02-2112-0770
E: edwardkim@kr.kpmg.com

이광열
상무이사
T: 02-2112-0062
E: kwangryeolyi@kr.kpmg.com

유경진
선임연구원
T: 02-2112-3018
E: kyungjinyu@kr.kpmg.com

김주형
연구원
T: 02-2112-7769
E: jkim81@kr.kpmg.com

kpmg.com/kr

© 2016 Samjong KPMG ERI Inc., the Korean member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Korea.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.