참고자료

금융권 클라우드 이용 확대 관련 Q&A

2018. 12.

금 융 위 원 회

목 차

1. 중요정보의 클라우드 허용에 따른 보안성 저하 우려에 대한 대책은?

□ 개인신용정보와 같은 중요정보도 클라우드로 이용하는 만큼, 금융회사 스스로 **엄격한 내부통제·보안 방안을 갖출 필요**

○ 금융회사는 **자체 정보보호위원회***에서 **클라우드 제공자의 건전성·안전성을 평가**하여 이용

* 금융회사의 정보보호최고책임자를 위원장으로 하며, 위원은 정보보호업무 관련 부서장, 전산운영 및 개발 관련 부서장, 준법업무 관련 부서의 장 등으로 구성

□ 아울러, 클라우드 제공자는 **전자금융거래법·신용정보법** 등에 따른 **암호화, 데이터 위·변조 방지 등** 보호조치를 준수해야 함

2. 해외 소재 클라우드의 허용 계획은?

□ 클라우드 이용 확대를 추진하면서, **금융보안의 중대성,** 사고 발생시 **소비자 보호·감독 관할 등은** 충분히 고려되어야 함

○ 이에 해외 소재 클라우드 허용은 **국내 소재 클라우드 운영** 이후 성과, 문제점 등을 고려하여 **점진적으로 검토**할 예정

○ 다만, 금융회사는 **국내 클라우드 사업자** 뿐만 아니라, **이미 국내에 전산센터***를 둔 **해외 클라우드 사업자의 서비스도 이용 가능**

* 국내센터 마련: 아마존(AWS), MS, IBM 등 / 구축 검토 : 구글, 오라클 등

□ 개인신용정보를 포함하지 않은 **비중요정보, 비식별 조치된 데이터**는 종전대로 **해외 소재 클라우드도 이용 가능**

3. 클라우드 이용시 클라우드서비스 제공자의 개인정보 열람 등 정보 유출의 위험이 있는 것은 아닌지?

□ 클라우드를 이용하는 경우에도 고객의 **개인정보**는 개인정보보호법·신용정보법에 따라 **암호화**하여 **전송***되며,

○ **클라우드서비스 제공자** 등 접근권한이 없는 자는 **열람이 불가**

* 개인정보보호법, 신용정보법에 따라 **고유식별정보, 개인신용정보**는 정보처리 위탁시 (클라우드 이용) 정보보호를 위한 **암호화 조치**를 하여야 함

※ **데이터의 '암호화 조치'란?**

- **원본 데이터(평문)**를 권한없는 제3자가 알아볼 수 없는 **형태로 치환(암호문)**하여 **전송·저장하는 조치로** 정보 유출시에도 **데이터 보호가 가능**

* 권한있는 이용자는 **원래의 정보를** 복호화 처리(자신이 소유한 키값을 이용해 암호화된 데이터를 원문 상태로 복원)하면 **이용 가능**하다는 점에서 **원래의 데이터가 재식별되지 않는 개인정보의 비식별 조치**와는 구분됨

4. 최근 클라우드 장애 사고 처럼 주요 클라우드 사업자의 서비스 장애 발생할 경우 금융권 주요 서비스가 마비될 가능성이 있지 않은지? 이에 대한 대책은?

□ 사고 발생시 신속한 대응을 위해 국내 전산센터內 **필수 운영 인력**이 **상주***하고, **장애 발생 사실을 지체없이 통지·대응****

○ **관리시스템을 포함**하여 개인신용정보를 처리하는 모든 시스템을 **국내에 설치**토록 하여 **신속한 장애 대응·복구**가 가능토록 함

* 전자금융감독규정 제23조 제2항 제2호 : 비상사태 발생 시 신속한 원상복구를 위한 비상지원인력 확보 등을 명시

** 장애 발생시 이를 지체없이 통보하고, 진행상황 파악 등을 위한 컨택 포인트를 지정한 후 장애원인 분석 및 재발방지 대책을 금융회사에 제공

※ 클라우드 관련 장애·재해가 발생해도 금융서비스가 중단되지 않도록 **중요 전산장비를 이중화하고 백업체계를 구축토록 함**

< 금융 클라우드 안전성 기준 >

데이터 보호	금융권 통합보안관제 지원, **전산자료 접근통제 및 정보시스템 가동 기록 보존**, 중요정보 **암호화 등 데이터 보호**, 개인(신용)정보법 등 금융관련 법령 준수
서비스장애 예방/대응	클라우드 이용시에도 주요 전산장비 **이중화 및 백업체계를 구축**, 서비스 **연속성 보장, 장애 발생시 비상 대응조치·통지 의무**

5. 클라우드 이용과 관련한 사고 발생시 금융회사와 클라우드 서비스 제공자간 법적 책임의 범위는?

□ 클라우드 이용 관련 소비자 피해 발생시 **금융회사, 클라우드 제공자**가 고객에게 **연대배상 책임**을 부담함으로써 **두텁게 보호**

* 클라우드 이용시 위탁자인 금융회사는 수탁자인 클라우드 제공자와 연대하여 손해배상책임을 부담(업무위탁 규정 제3조 제5항, 전금법 제11조 제1항 등)

○ 또한, **손해배상·계약해지, 재판관할 사항** 등을 명시토록해 금융회사·클라우드 제공자간 **법적 책임관계를 명확화**

구분	고객 손해발생시 책임 (이용자→금융회사·클라우드제공자)	클라우드제공자 책임범위 명시 (금융회사·클라우드제공자)
책임 관계	사고발생시 **금융회사**가 **1차적 손해배상 책임**의 **주체**이며, **클라우드 제공자**는 수탁자로서 **연대배상책임을 부담**	고의과실로 **서비스 품질 저하, ·장애 등** 발생시 **클라우드제공자의 책임범위, 재판관할 등을 사전에 명시해** 분쟁을 예방

6. 美정부가 CLOUD법에 따라 미국 클라우드 서비스업체에 저장되는 우리 국민의 정보에 접근할 수 있다는데?

□ **국내 클라우드** 시스템은 미국 해외 정보 이용법(CLOUD법)*에 따른 美**정부의 데이터 제공 요청에 반드시 따라야 하는 것은 아님**

* Clarifying Lawful Overseas Use of Data Act

○ 동 법은 **범죄조사**에 필요한 해외 소재 데이터 확보·안보 유지를 위해 제정한 것으로, **외국 정부 법령을 고려하여 데이터를 요청**할 수 있도록 함

* ① 고객 또는 가입자가 미국인이 아니며 미국에 거주하지 않고, ② 요구된 데이터 공개로 인해 사업자가 자격 있는 외국 정부의 법을 위반할 중대한 위험이 있는 경우, 사업자는 미국 정부의 데이터 요구에 대한 각하 또는 변경을 법원에 청구할 수 있음 (Clarifying Lawful Overseas Use of Data Act §2703)

※ 범죄 수사를 위한 외국 정부의 정보제공 요청시 **국내법 위반 소지가 있을 경우 거부가 가능**

- 클라우드 제공자는 해당국의 **관계 법령을 사전 보고**하고, 정보제공 요청이 있을 경우 **금융당국·금융회사에 사전 통지하여 동의 받도**록 함

* 미국 CLOUD법은 미국정부의 범죄 조사를 위한 것으로, 정보 접근에 있어 외국인에 대해서는 예외가 인정되고 있음

7. 외국계 클라우드 사업자는 국내 개인정보보호 관련 법규를 따르지 않아 개인정보 보호에 취약한 것 아닌지?

□ 외국계 클라우드 사업자도 **국내 개인정보보호 법령을 준수**해야 함

○ 따라서, **중요정보 암호화, 접속기록 위·변조 방지, 시스템 접근 통제** 등 개인정보 보호 관련 제반 보호조치 사항을 준수해야 함

<참고 : 개인정보보호법·신용정보법상 안전성 확보 장치>

(**신용정보법 제17조 등**) 신용정보 위탁 제공시 암호화 등 보호조치 준수, 위탁 업무범위를 초과한 이용금지, 수탁자 교육, 재위탁 금지 등
(**개인정보보호법 제26조**) 제3자 업무 위탁시 목적외 개인정보처리 금지, 기술적·관리적 보호조치 준수, 수탁자 관리·감독 의무 등
(**개인정보보호법 제24조 및 제24조의2**) 암호화 등 안전성 확보조치 준수

8. 개정안은 클라우드서비스 제공자의 관리시스템을 국내에 설치하여야 하는지 여부가 불명확한데?

□ 현재 전자금융감독규정은 국내에 본점을 둔 금융회사의 **전산실 및 재해복구센터**를 **국내에 설치**토록 하고있음(제11조 제11호)

○ 전산실은 전산장비, 통신·보안장비, 전산자료가 보관된 장소를 의미하므로 **정보처리시스템을 포함**하고 있음(제2조 제1호)

□ 또한, **개인신용정보**를 처리하는 업무의 **정보처리시스템을 국내에 설치하도록 명시**(개정안 제14조의2 제8항)

○ 관련 법령 정의상 **클라우드 관리시스템**도 **'정보처리시스템'***에 해당하므로 개인신용정보를 처리하는 경우 이를 **국내에 두어야 함**

* 전자금융감독규정 제2조제3호 : "정보처리시스템"이라 함은 **전자금융업무를 포함하여 정보기술부문에 사용되는 하드웨어와 소프트웨어**를 말하며 **관련 장비를 포함한다**

9. 외국계 클라우드 서비스 업체에 대하여 감독·조사권이 실질적으로 확보될 수 있는 것인지?

□ 금융회사·클라우드 제공자간 계약 체결시 현장방문을 포함한 **클라우드 제공자의 감독·검사 의무**를 **계약서에 명시**토록 함

○ 감독당국은 사고 발생, 예방·점검 등 필요시 **자료제출 요구, 현장점검**을 통해 **관리·감독**할 수 있으며,

* EU, 영국 등 해외 사례와 같이 클라우드 이용 계약서에 금융회사와 감독당국의 조사·접근권을 명시토록 함

○ 관리시스템을 포함한 **개인신용정보를 처리하는 모든 시스템을 국내에 두도록 해** 감독당국의 **신속한 현장 감독·조사**가 가능

□ 국내외 클라우드 운영 상황, 해외 사례 분석 등을 토대로 클라우드 제공자(전자금융보조업자)에 대한 감독당국의 **감독·조사권을 보다 강화**(법개정 사항)하는 방안을 추진

10. 클라우드 보안 수준과 관련해 국내외 클라우드 업체간 규제 형평성의 차이는 발생하지 않는지?

□ 금융 클라우드 서비스 제공 관련 보호조치 기준에서 제시하는 안전성 확보조치 사항은 **국내외 클라우드 사업자 모두에게 동일**

○ 클라우드 안전성 확보조치 평가·검증과 관련하여 국내의 경우 **클라우드 서비스 보안인증(CSAP)**이 있으며

○ 해외의 경우 **FedRAMP(미국), CSA STAR(글로벌 협회), MTCS(싱가포르)** 등 국내 기준에 부합하는 일정한 인증을 받은 경우 이에 상응하는 보호조치를 갖춘 것으로 간주

* 관련 인증은 기본 보호조치에 관한 사항을 포함하고 있으며, **금융부문 추가 보호조치 사항은 평가를 생략할 수 없음**

○ 다만, 이경우에도 운영과정에서 미비점이 발견될 경우 금융회사·감독당국의 관리·감독을 통해 **보완 등 조치가 가능함**

- **FedRAMP** : 미국 정부 주관의 클라우드 보안인증 기준으로, 미국 정부에서 클라우드 이용 시 필수로 요구됨
- **CSA STAR** : 클라우드 보안협회 주도의 ISO 표준 기반의 인증 제도로, 민간 클라우드 인증 중 국제적으로 가장 인정받고 있음
- **MTCS** : 싱가포르 공공기관에서 운영 중인 인증 제도로, 싱가포르 공공기관 뿐만아니라 금융기관에서 클라우드 이용 시 필수로 요구됨

11. 해외 클라우드 사업자가 국내외 클라우드 보안인증을 취득하기만 하면 운영관리나 물리적 보호조치에 대한 관리·감독을 건너뛸 수 있게 되는 것 아닌지?

□ **국내·외 유효한 클라우드 관련 보안인증***을 취득·유지하고 있는 클라우드 서비스에 대해서는

* 금융 클라우드 이용 가이드에서 **적합한 인증범위 · 등급을 명시**할 계획

○ **인증기준이** 현행법상 클라우드가 갖추어야 할 **기술적·관리적·물리적 보호조치 기준을 이미 포함**하고 있어 이를 평가한 것으로 봄

* 관련 인증은 기본 보호조치에 관한 사항을 포함하고 있으며, **금융부문 추가 보호조치 사항은 평가를 생략할 수 없음**

○ 클라우드 **보안인증 외에도** 금융회사가 수행하는 클라우드서비스 제공자에 대한 **안전성 평가를 금융보안원이 지원**하여 안전성이 확보된 클라우드만을 이용할 수 있도록 내부 통제를 강화

○ 한편, 실제 운영과정에서 미비점이 발견될 경우 금융회사 또는 감독당국의 관리·감독을 통해 **보완 등 조치가 가능함**