

해와 없는 버전

금융권 클라우드 이용 확대 방안

2018. 7.

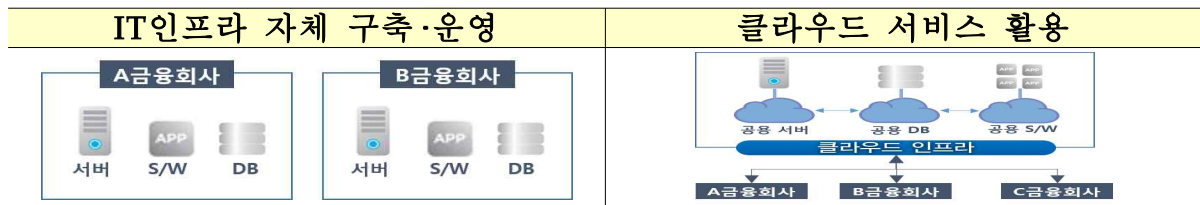
금 융 위 원 회

목 차

I. 추진 배경	1
II. 금융분야 클라우드 현황	3
1. 이용 현황	4
2. 클라우드 이용 규제·감독	6
III. 그간의 클라우드 이용규제 평가 및 개선방향	7
1. 클라우드 이용 측면	7
2. 개인정보보호 측면	8
3. 금융보안 측면	8
4. 관리·감독 측면	9
IV. 클라우드 활성화를 위한 제도개선 방안	10
1. 클라우드 컴퓨팅 허용 이용범위 확대	11
2. 클라우드 서비스 기준 도입	14
3. 클라우드 서비스 이용 감독·검사 강화	17
V. 기대 효과	19
VI. 향후 계획	19

I. 추진 배경

- ICT기술 발전에 따라 금융분야의 디지털화(digitalization)가 폭넓게 확산
 - 디지털 혁명을 대표하는 기술인 A(AI,인공지능) · B(BlockChain) · C(Cloud) · D(BigData) 등이 기술과 금융의 융합을 주도
- 이 가운데 클라우드(Cloud)는 금융회사의 외부주문(아웃소싱)의 하나로 IT자원의 직접 구축없이도 필요한 만큼 빌려쓰는 공유환경을 제공
 - 클라우드 이용자는 다양한 IT서비스를 빌려서 이용하고, 이용량에 따라 비용을 지불하므로 업무생산성 증진과 비용절감이 가능



* 과학에서 구름(Cloud)처럼 먼 거리에서 시각적으로 보이는 물건들의 커다란 집합체를 의미하는 클라우드는 인터넷 상에 자료를 저장해두고 사용자가 필요한 자료, 프로그램을 자신의 컴퓨터에 설치하지 않고도 인터넷 접속으로 언제 어디서나 이용할 수 있는 서비스를 말함

- 그간 정부는 금융권 클라우드 활성화를 위해 전자금융감독규정을 개정하고, 클라우드 서비스 이용 가이드를 마련('16.10월)
 - 보안사고 등 부작용 방지를 위해 고유식별정보, 개인신용정보를 제외한 '비중요정보'에 한해 클라우드(퍼블릭) 이용을 허용

클라우드 유형	프라이빗(Private)	퍼블릭(Public)	하이브리드(Hybrid)
서비스 특징	망분리, 비공개 방식 (한정된 사용자)	인터넷 망, 공용방식 (불특정 다수)	중요업무 → 프라이빗 비중요업무 → 퍼블릭
현재 활용상 제약	특별한 제약 없음	개인신용정보 등 중요정보 처리 불가	'비중요정보' 지정 후 사용

- 다만, 최근 AI · 빅데이터 등 新기술과 금융 접목 확대로 금융권 클라우드 활용과 관련한 추가 규제정비의 필요성이 증가
 - 특히, 은행 · 카드, 핀테크기업 등 각 업권에서 클라우드 규제완화 건의가 지속적으로 제기되어 왔고, 관계기관 · 전문가의 의견을 수렴*
 - * 핀테크 활성화 릴레이 간담회(4.11), 금융분야 클라우드 간담회(4.17), 테크자문단 회의(6.12)

⇒ 보안장치, 감독체계 강화를 전제로 금융회사 · 핀테크기업이 안정적으로 클라우드를 활용할 수 있도록 제도 개선을 검토

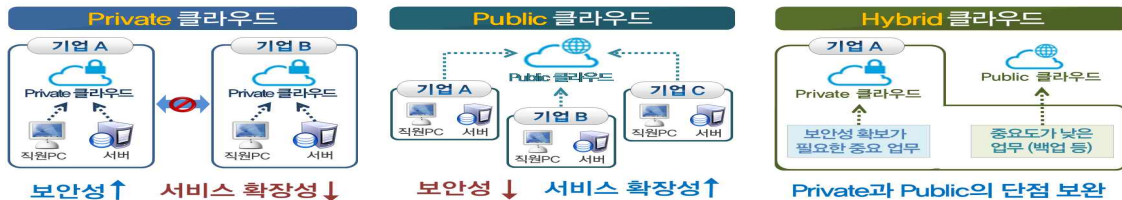
□ **(개념)** 전산설비를 직접 구축하지 않고, 전문업체로부터 인터넷을 통해 필요한 IT자원을 탄력적으로 제공받아 사용하는 컴퓨팅 환경

□ **(분류)** 서비스로 제공받는 IT자원과 공유하는 이용자의 범위를 기준으로 다음과 같이 분류 가능

- **(서비스 대상)** ① 서버·저장장치·네트워크 등의 전산 인프라(IaaS)¹⁾
② 응용프로그램 개발환경(PaaS)²⁾ ③ 응용프로그램(SaaS)³⁾

1) Infrastructure as a Service, 2) Platform as a Service, 3) Software as a Service

- **(공유범위)** 서비스에 대한 공유 범위에 따라 ① Public(불특정 다수),
② Private(특정회사), ③ Hybrid 클라우드로 구분



□ **(주요특징)** 서비스대상과 공유범위에 따라 상이*할 수 있으나 일반적 특징은 다음과 같음

* 프라이빗 클라우드는 ①,②,③이 해당되지 않을 수 있음

- ① **(IT자원공유)** 이용자의 요구에 따라 탄력적으로 이용할 수 있도록 IT자원을 집적하여 다수의 고객과 공유
- ② **(가상화)** 집적된 IT자원을 가상화 기술*(Virtualization)을 이용해 논리적 단위로 분할하여 서비스를 제공

* 한 대의 서버를 여러 대처럼 또는 여러 대를 한 대처럼 사용하는 기술

- ③ **(인터넷 연결)** 원격에 있는 IT자원에 인터넷을 통해 접속

□ **(활용효과)** 금융회사의 경우 급증하는 정보량과 복잡해지는 IT시스템에 대응한 유연한 IT인프라 확보, 비용절감, 신기술 접목 확대 등 가능

- 핀테크기업은 클라우드 활용시 손쉬운 개발환경 구축, 보안성 제고, 리스크 대비 비용절감*, 고객정보를 이용한 다양한 서비스 개발이 가능

* (사례) 클라우드형 웹서버 시스템을 도입한 A사의 경우 국내외 데이터 센터를 클라우드로 일원화 하면서 연간 관리 비용을 30~50% 절감

II. 금융분야 클라우드 현황

1. 이용 현황

□ (국내) 총 38개 금융회사(73건)에서 업무처리, 부가서비스 제공 등 목적으로 클라우드 시스템을 이용('18.3월)

○ 주로 개인정보와 관련이 없는 내부업무처리(43.8%), 고객서비스(27.4%), 회사·상품 소개(15.1%) 등에 활용중

※ (국내) : KT·네이버·코스콤 등, (국외) : MS, IBM, 구글, 아마존(AWS) 등

<업무용도별 클라우드 시스템 활용현황>

용도	건수	비중(%)	구체적 업무 용도
내부업무처리	32	43.8	인사관리(HR), 이메일·메신저, 직원교육, 차량관리 등
고객 서비스	20	27.4	고객상담, 투자정보 제공, 이미지 저장, 설문조사 등
회사·상품 소개	11	15.1	회사 소개, 서적·음반·전시 소개, 투자상품 소개
정보분석	8	11.0	장외 파생상품 평가, 영업활동·수익분석, 정보분석 등
보험계리	2	2.7	보험계리분석
합계	73	100.0	

□ (해외) 용도가 제한되어 있는 국내에 비해 해외는 금융회사별 수요에 따라 다양한 방식으로 클라우드 서비스를 이용중

○ 일부 금융회사는 내부 지원업무 뿐만 아니라 बैं킹 서비스와 같은 핵심시스템도 클라우드 서비스로 이전

< 해외 금융회사별 클라우드 이용사례 >

이용대상 구분	클라우드 이용사례
전체(핵심) 시스템	(영국, Oaknorth은행) 전체 시스템을 아마존 클라우드로 이전 (호주, Westpac은행) 전체 시스템의 70%를 클라우드로 이전(3년내) (일본, MUFG) 계정계 시스템을 클라우드로 이전(장기계획)
금융서비스 등 일부 시스템	(홍콩, HSBC) 빅데이터 관련 파일럿 프로젝트를 클라우드로 수행 (영국, AXA) 구글 클라우드의 인공지능(AI) 엔진을 이용하여 고객별 위험 예측 및 보험금 산정 등에 활용
내부 업무용 시스템	(미국, BoA) 고객관리 시스템을 클라우드로 구축 (영국 AXA 등) 클라우드 기반 오피스 환경(MS Office 365 등) 구축

⇒ 해외는 클라우드를 통해 금융회사 고유 서비스 제공 뿐만 아니라 AI·빅데이터 등 신기술 활용을 적극 추진중이나, 국내는 내부 업무처리나 부가서비스 등 활용 분야가 제한적

2. 클라우드 이용 규제·감독

<국내 제도 현황>

< 그간의 추진 경과 >

- 과기부는 클라우드 발전법을 제정('15년)하고, 클라우드 선도국가로의 도약을 위해 제1차 기본계획('16~'18)을 수립

※ 금융·의료·교육 분야에서 클라우드 이용을 저해하는 규제 발굴 및 개선 (규제개혁장관회의, '16.5월, 과기정통부, 교육부, 복지부, 금융위)

- 현재 2차 기본계획('19-'21) 수립을 준비중으로, 민관합동 "SW, 구름타고 세계로 TF"를 통해 애로사항을 점검하고 개선방안을 도출

- 금융위도 금융분야 클라우드 서비스 활용 확산을 위해 클라우드 TF 구성*('16.3월) 및 제도개선 방안을 마련·추진('16.5월~)

* 금융위, 금감원, 금융보안원, 금융회사, 클라우드 사업자, 법률전문가 등으로 구성

□ 금융회사·전자금융업자는 클라우드 컴퓨팅 이용을 위해 전자금융거래에 미치는 영향이 낮은 시스템을 **비중요정보 처리시스템**으로 지정 가능 (전자금융감독규정 제14조의2 신설, '16.10.5)

○ 금융회사 등은 정보자산의 중요도에 따라 '비중요정보 처리시스템' 지정이 가능하며, 해당 시스템에 대해서는 물리적 망분리 등 클라우드 이용이 제한되는 규정이 적용되지 않음

○ 다만, 개인신용정보와 고유식별정보를 처리하는 정보처리시스템은 **비중요 시스템**으로 지정이 불가

* 전자금융감독규정 제14조의2 : 정보자산의 중요도에 따라 비중요 시스템 지정 후 망분리 등의 예외를 적용(다만, 개인신용정보와 고유식별정보는 지정 불가)

○ 클라우드 이용 대상 시스템, 비중요정보 처리시스템 지정 기준, 시스템 보호대책 등에 관한 '금융권 클라우드 서비스 이용 가이드' 배포('16.10.14)

※ 반면, 非금융분야는 클라우드 이용제한이 없으며, 개인정보보호법 등에 따른 정보보호·제공에 관한 규제를 적용

□ 클라우드 아웃소싱의 하나로 「정보처리 업무위탁」에 해당하며, 제공자는 「전자금융보조업자」로서 제한적으로 감독을 받음

- 금융회사·전자금융업자는 관련 시스템을 ① '비중요정보 처리 시스템'으로 지정하고, ② 정보처리업무 위탁보고* 후 '금융권 클라우드 서비스 이용 가이드라인'을 준수하면서 서비스 이용 가능

* 금융회사의 정보처리 업무위탁에 관한 규정 제7조

- **(보조업자의 책임)** 클라우드 서비스 제공자의 고의·과실은 금융회사의 고의·과실로 간주되고, 이용자 손해를 금융회사와 연대하여 배상

* 전자금융거래법 제11조

- **(금융회사 준수사항)** 클라우드 서비스 이용시 아웃소싱에 대한 보안·비상·백업대책 등을 수립·운영하고 보안점검을 실시해야 함

구분	내용	관련 조항
금융회사	<ul style="list-style-type: none"> ▪ 해킹·개인정보유출 등에 대비한 보안대책 수립 ▪ 시스템 장애 등 서비스 중단 비상대책 수립 ▪ 업무지속성을 위한 중요 전산자료 백업대책 수립 ▪ 정보관리 보안유지를 위한 내부통제방안 수립·운영 ▪ 전자금융보조업자의 재무건전성 및 서비스 품질수준을 연 1회 이상 평가하고 결과를 감독당국(금감원)에 보고 	감독규정 제60조 제1항, 제2항
감독당국	<ul style="list-style-type: none"> ▪ 금융회사 정보기술부문 실태평가에 전자금융보조업자의 재무건전성 및 서비스 품질수준 평가여부 반영 	감독규정 제60조 제3항

- **(감독·검사)** 금융회사의 정보처리업무 위탁계약 시정·보완 요구권, 보조업자에 대한 수탁계약서·부속자료 등의 제출요구권 보유

구분	내용	관련 조항
금융위	<ul style="list-style-type: none"> ▪ 정보처리업무 위탁계약에 대한 시정·보완 지시 	법40조 2항
금감원	<ul style="list-style-type: none"> ▪ 수탁계약서·부속자료 등의 직접 제출요구 - 자료제출 거부 및 부실자료 제출시 조사 실시 가능 (진술서 및 관련장부·서류·물건 제출, 관계인 출석 등) 	법40조 3항, 4항, 5항

⇒ 클라우드 서비스 제공자와 계약관계에 있는 금융회사가 점검하며, 금융당국의 제공자에 대한 직접 감독권은 없음

〈해외 제도 현황〉

- 주요 선진국은 클라우드 이용을 직접 규제하지 않고, 가이드라인을 통해 자율준수토록 하고있으며, 감독 방식은 국별로 차이가 있음
 - EU·영국·싱가포르는 금융당국의 권고 또는 지침으로 운영하고, 미국은 금융당국 차원의 특별한 규정은 없음^{*}
 - * 자문기구인 연방검사위원회(FFIEC, Federal Financial Institutions Examination Council), 「아웃소싱 클라우드 컴퓨팅」('12.7)에서 금융회사 클라우드 이용시 유의사항을 명시
 - 주요국들은 권고 또는 지침 등을 통해 클라우드 제공업체, 보안 및 감독 관련 내용을 계약서에 명시적으로 포함하도록 요구
 - 다만, 클라우드 제공업체에 대해 EU·영국은 직접 감독하는 반면, 싱가포르·미국은 금융회사를 통해 간접적으로 감독(전자금융거래법상 전자금융보조업자를 감독하는 방식과 동일)

국가명	지침명 및 내용	제정기관	제정(발효)시기
EU	클라우드 제공자 업무위탁에 관한 권고 - 중요업무 위탁시 클라우드 제공자, 서비스 국가, 저장위치 등을 관할 당국에 통보 - 금융회사, 위임된 제3자에게 위탁업무와 관련 접근권 및 현장감사권 부여 등 계약 명시	은행청 (EBA)	'18.7월 발효
영국	클라우드 및 제3자 IT아웃소싱 관련 지침 - 중요업무 위탁시 문서화된 근거 필요 - 클라우드 제공자 사업장 관할지에 따라 영국 법률 규율여부 확인(감사 및 규제 권한 보장)	금융감독청 (FCA)	'16.7월 제정
미국	아웃소싱 클라우드 컴퓨팅 - 소비자 데이터가 국외에서 저장 또는 처리될 경우 해당 국가 관련 규정 확인 - 프라이버시 법규 관련 책임, 보안사고에 대한 보고의무 등 법적의무 계약 명시	검사협의회 (FFIEC)	'12.7월 제정
싱가포르	아웃소싱 가이드라인 - 클라우드 제공자 실사 및 위험관리 수행 - 금융회사의 클라우드 제공자 관리·감독 책임	통화국 (MAS)	'16.7월 제정

⇒ 일반적으로 금융회사가 접근권·현장감사권 등 관리·감독 책임을 가지며, EU의 경우 감독당국의 감독권 확보(자료제공요구)도 권고

Ⅲ. 그간의 클라우드 이용규제 평가 및 개선방향

1. 클라우드 이용 측면

- '16.10월, 금융권 클라우드 도입시 개인신용정보의 민감성 등을 고려해 중요도에 따라 정보를 구분하고, '비중요정보'에 한해 클라우드 이용을 허용하면서 안전성을 지속 테스트(클라우드 활성화 前단계 조치)
 - 지난 2년간 금융회사는 내부 업무처리 등에 어느정도 비용절감 효과를 거둔 반면, 직접적인 사업모델 개발에는 제한
 - 외부 저장장치로써의 효과 외에 서비스 적용·개발을 위한 인프라로는 적극 활용하지 못함
 - 핀테크기업은 IT설비 구축과 같은 초기 시장진입 비용 부담으로 새로운 아이디어를 활용한 창업 및 서비스 개발에 제약
 - 반면, 해외에서는 이용상 제한이 없어 클라우드로 新서비스 출시기간을 단축하는 등 경쟁력을 강화하는 추세
- ⇒ 금융회사·핀테크기업이 비용절감, 생산성 제고와 동시에 새로운 서비스를 개발할 수 있도록 클라우드 이용범위를 확대할 필요

1. 금융업권·핀테크업계 건의사항 : 지속

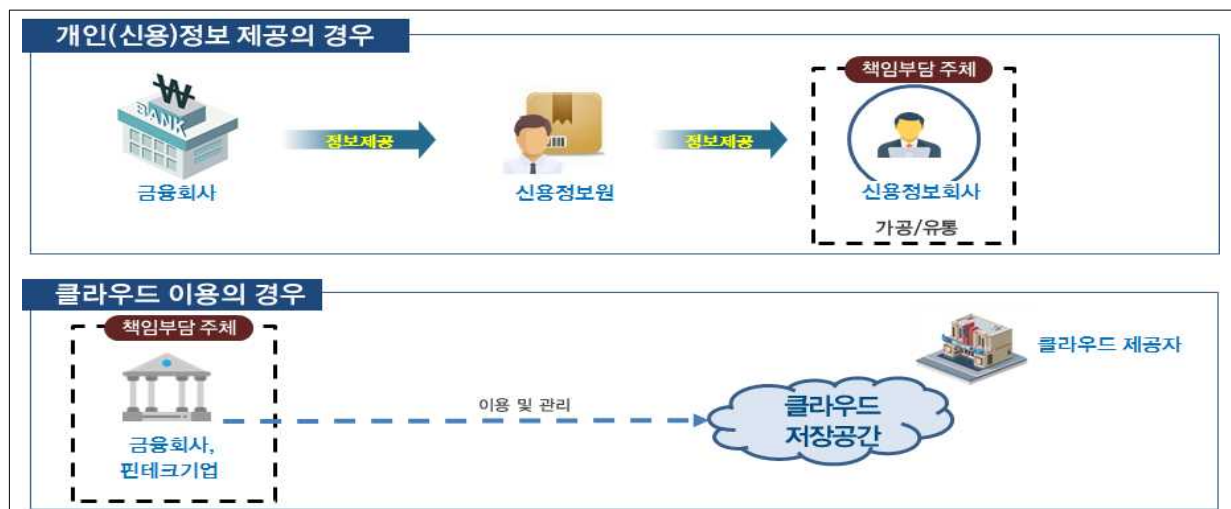
- 개인신용정보를 처리하는 시스템의 클라우드 이용을 제한하는 전자금융감독규정 개정을 요구(은행·금융투자 등 금융업권, 핀테크)

2. 클라우드간담회('18.4.17), 테크자문단회의('18.6.11)

- 핀테크기업의 경우 초기 IT인프라를 갖추는 기술진입과 사용량 증가 등 확장 용이성이 좋은 클라우드를 선호(A핀테크기업)
 - * 해외 클라우드 서비스를 많이 사용하는 크라우드펀딩 회사의 경우 중요 금융거래 정보가 클라우드 서비스에 사용되는 상황
- 신용정보 관리, AI기술 활용을 위해 빅데이터 분석에 클라우드 서비스 이용 및 관련회사 추가 데이터 확보 필요(B카드사)
- 리스크 업무와 파생업무에 고성능 서버가 필요, 시장변동성이 심한 HTS, MTS와 같은 채널에 클라우드 적용이 더욱 필요한 실정(C금융투자회사)

2. 개인정보보호 측면

- 클라우드를 금융회사가 IT자원을 빌려서 사용하는 것으로서 개인정보의 제공·유통과는 관련이 없음
 - 금융회사는 개인정보를 클라우드 내에서만 저장·활용할 뿐, 제공·유통하지 않아 개인정보 남용·침해 문제는 발생하지 않음
 - * 개인(신용)정보 제공의 경우 개인(신용)정보를 제공받는 자가 관리·감독책임이 있는 반면, 클라우드는 금융회사가 자기통제하에 관리·감독
 - 현재 개인정보보호 법령상 클라우드 활용을 금지하는 규정은 없으며, 금융권 아닌 다른 분야에서는 클라우드를 제한없이 활용중
 - * 신용정보의 경우 신용정보법에 따라 기술적·관리적 보호조치 준수시 위탁처리가 가능, 고유식별정보도 개인정보보호법상 위탁처리를 제한하는 규정은 없음
- ⇒ 개인정보보호법·신용정보법을 기준으로 보호조치를 강화하되 전자금융감독규정에만 존재하는 클라우드 제한 규정 정비 필요



3. 금융보안 측면

- 금융보안의 중요성, 지정학적 특수성을 고려한 사이버 리스크에 대비한 보안강화 노력도 필요
- 경제적 이익을 목표로 한 사이버침해 공격이 빈발하고 있어 방대한 정보를 보유하고 있는 금융분야의 경우 유출시 피해규모 등 파급효과가 큰 점을 고려해야 함
 - * '11년 3.4 디도스 공격, '13년 3.20 사이버테러, '17년 ATM 이용자 정보 유출 등

- 현재 금융회사가 클라우드 이용시 보호장치*가 작동하고 있으나, 향후 중요정보로 확대시 보다 엄격한 보안체계를 구비할 필요

* 클라우드를 이용하는 경우에도 금융회사 전산실 물리적 망분리와 내부 업무용 시스템의 망분리 체계는 현행과 동일하게 유지되며, 클라우드 시스템과 전용회선(가상사설망 포함)으로 연결하도록 규정해 안전성을 유지(전자금융감독규정)

- 특히, 자본·설비가 영세한 핀테크기업은 보안성을 높일 수 있는 클라우드를 활용하지 못해 보안수준이 낮아 경쟁력이 취약

⇒ 클라우드 이용범위를 확대하되, '중요정보'에 대한 보호장치를 강화하고 금융권 자율 보안수준을 향상시킬 필요

4. 관리·감독 측면

- 클라우드 서비스 제공자는 전자금융보조업자로서 감독을 받으나 금융당국의 직접 감독대상은 아님

- 현행 전자금융감독체계는 클라우드 서비스 제공자를 포함한 전자금융보조업자에 대한 직접 감독권이 미비
(금융회사가 전자금융보조업자에 대해 정기점검 등을 통해 관리·감독)

⇒ 클라우드 이용확대 조치와 함께 클라우드 서비스 제공자에 대한 금융당국의 감독방안을 보강할 필요

- ◇ 지난 2년간 금융권의 클라우드 활용 경험, 클라우드를 활용한 기술·금융융합 추세 가속화 등을 종합적으로 감안하여 클라우드 이용 확대 방안을 마련(관련 규정 정비 후 '19.1월 시행 목표)
- ◇ 클라우드 이용 확대와 병행하여 ①금융권의 보안수준 및 관리체계를 강화해 보안문제 우려를 해소하고, ②해외사례와 같이 관리·감독체계를 보다 효과적으로 구축

Ⅳ. 클라우드 활성화를 위한 제도개선 방안

〈 기본 방향 〉

1. 클라우드 서비스 이용범위 확대

- 금융회사, 핀테크기업이 클라우드를 활용하여 혁신적 상품과 서비스 개발이 가능하도록 이용범위를 확대
 - 개인신용정보·고유식별정보도 국내소재 클라우드를 이용할 수 있도록 개선
- ※ 국외소재 클라우드 허용은 국내소재 클라우드 운영 이후 문제점 등을 고려하여 중·장기적으로 검토

2. 클라우드 서비스 이용·제공 기준 마련

- 중요정보 처리시스템의 안전성을 확보하기 위해 클라우드 이용(금융회사), 제공(제공자)시 기준을 도입하고 운영방안을 수립
 - (금융회사) 중요정보 클라우드 이용시 안전성 관리를 강화
 - (제공자) 금융의 특수성을 반영해 클라우드 서비스 제공자가 기본적으로 준수해야 할 기준을 마련
- * ‘중요정보’의 경우 기존 금융권 전산시스템에 준하는 보안수준을 충족하도록 함

3. 클라우드 서비스 감독·검사 강화

- 클라우드 활용 확대를 고려하여 금융권 클라우드 이용현황에 대한 모니터링을 강화하고, 적절한 감독·검사 체계 마련
 - 클라우드 서비스 이용 관련 금융회사의 보고의무 강화
 - 전자금융보조업자(클라우드 서비스 제공자)에 대한 감독당국의 직접 감독·조사권을 확보하는 방안을 검토(법개정 사항)

1. 클라우드 컴퓨팅 이용범위 확대

◆ 금융회사와 핀테크기업이 클라우드를 통해 활용할 수 있는 정보의 범위를 확대(비중요정보限 → 개인신용정보·고유식별정보)

□ (현행) 개인신용정보·고유식별정보*를 제외한 비중요정보 처리 시스템에 한하여 클라우드 서비스를 활용 가능

* 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호

○ 단 한건의 개인신용정보·고유식별정보만 있어도 클라우드의 이용이 제한되어 핀테크기업에게 진입장벽*으로 작용

* 핀테크기업이 新서비스를 출시하려고 해도 간편 결제·송금 등의 초기 시스템 구축 비용 문제로 원활한 서비스 개발이 어려움

- 또한, 클라우드를 이용하는 핀테크기업은 금융회사 업무를 위탁받아 新서비스를 테스트하는 규제 샌드박스 활용도 어려움

* 금융회사 업무를 위탁받아 혁신 금융서비스 테스트 → 금융거래·소비패턴을 클라우드에서 분석하려고 할 경우 개인신용정보가 있으면 사실상 분석이 곤란

○ 금융회사 등이 AI·빅데이터 등 新기술을 이용해 새로운 상품·서비스를 개발*하는데 개인신용정보를 활용할 수 없어 제약

* AI·빅데이터는 고도의 전문성과 더불어 대용량·고성능의 IT인프라가 필요하여 클라우드 이용이 보다 적합

- 클라우드 기반의 AI알고리즘을 이용해 고객 질의에 응대할 경우, 맞춤형 서비스를 제공하지 못하고 단순 상담(챗봇)에 국한

- 클라우드를 통해 신용평가·심사, 리스크 분석, 금융사기 등 이상 징후 분석시 빅데이터를 활용할 수 없어 단순 트렌드 분석만 가능



□ (개선) 개인신용정보, 고유식별정보를 처리하는 중요정보 처리 시스템도 클라우드를 활용할 수 있도록 규제를 개선

① 현재 전자금융감독규정에만 존재하는 클라우드 제한 규정을 정비해 이용범위를 확대(비중요정보限 → 개인신용정보·고유식별정보)

* 전자금융감독규정 제14조의2 : 금융회사는 개인신용정보, 고유식별정보를 제외한 비중요정보 처리시스템에 한해 퍼블릭 클라우드 활용이 가능

- 개인신용정보도 클라우드를 적극 활용할 수 있도록 함으로써 금융회사·핀테크기업의 혁신 상품, 맞춤형 서비스 개발을 활성화

* 미국, 중국 등의 新기술 기반회사는 클라우드를 이용해 대량의 데이터를 유연하게 처리하고, 고객정보를 바탕으로 맞춤형 서비스를 개발·제공중

- 나아가 고유식별정보 활용시 일시적 거래량 집중에 장애 없이 금융서비스를 제공할 수 있고 AI기반 대화형 뱅킹서비스도 가능

* 개인신용정보에 한해 클라우드 이용을 허용할 경우 대고객 서비스를 제공하는 시스템은 클라우드 이용이 사실상 제한되어 규제개선 실익이 낮음

② 사고 발생시 법적분쟁, 소비자 보호·감독 관할, 개인정보보호 등의 문제로 국내 소재 클라우드에 한해 우선 허용(국외는 중장기 검토)

* 금융회사가 사용하는 클라우드 기반 시스템이 해외에 위치할 경우 사고발생시 사고조사 및 대응이 어려우며 감독·검사 또한 제대로 이루어지지 못할 우려

③ 다만, 개인신용정보·고유식별정보는 클라우드 활용 여부와 상관없이 개인정보보호법·신용정보법 등 개인정보보호 법령에 따라 보호·관리

< 개인정보보호법, 신용정보법상 보호조치 >

(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

〈예시〉 클라우드 이용범위에 따른 금융권 적용사례

클라우드 이용	확대 前	확대 後	
	비중요정보만 가능(현행)	개인신용정보	개인신용정보+ 고유식별정보
AI활용 대고객 서비스(챗봇 등)	△ * 단순상담만 가능	○ 고객 편의성 ↑ * 개인 맞춤형 금융상담	◎ 고객 편의성 ↑ * 계좌개설 등 모든 전자 금융 서비스 제공 가능
빅데이터 분석	△ * 비식별 조치후 제한적 분석	○ 분석 실효성 ↑ * 개인 맞춤형 결과 도출 * 비식별 조치없이(통상 2~3개월 소요) 실시간 분석	◎ 분석 실효성 ↑ * 고유식별정보를 기준 업권간 연계 분석
인터넷뱅킹 · HTS 등	× 이용불가	△ 사실상 제약 * 고유식별정보 처리 기능 분리가 필요해 이용실익 낮음	○ 관리 효율성 ↑ * 시간대별 효율적 운영, 월말 · 명절 등 일시 접속량 폭주에 대응
재해복구센터 구축	× 이용불가	× 이용불가	○ 비용절감 효과 ↑ * 상황발생시 즉시 대응 용량 확대
고성능 컴퓨팅 (파생상품 개발, 보험 손해액 산정 등 활용)	× 이용불가	○ 비용절감 효과 ↑ * 사용량에 따라 비용 지급	
대고객 신규 서비스 구축 (신규 모바일 앱 및 뱅킹 서비스, 홈페이지 등)	△ * 홈페이지, 설문조사 등 단순 서비스만 가능	△ 사실상 제약 * 고유식별정보 처리 기능 분리가 필요해 이용실익 낮음	○ 서비스 출시기간 ↓ * 필요시 신속한 인프라 구성
콜센터, CRM(고객관리) 등	× 이용불가	○ 최신 서비스 활용 ↑ * 시스템 구축없이 SaaS 이용	
오픈 API 제공	× 이용불가	○ 서비스 확장성 ↑ * 이용량 증가에 따른 추가자원 확보 용이	
혁신 서비스 테스트	× 이용불가	○ 비용절감 효과 ↑ * 신속한 인프라 구성 및 실험후 자원 반납	

2. 클라우드 서비스 기준 도입

◆ 클라우드 서비스 이용을 확대하되, 금융보안의 중대성을 고려해 금융권 클라우드 서비스 이용·제공 기준을 수립·운영

* '비중요정보'에 대해서 기존 안전성 확보 조치를 유지하되, '중요정보'는 보다 강화된 보호조치 기준을 수립·시행

□ (현행) 비중요정보 처리시스템에 한하여 클라우드의 이용이 가능하도록 물리적 망분리*의 예외를 인정

* (전자금융감독규정 제15조 : 해킹방지대책) 내부 정보처리시스템과 해당 시스템의 운영·개발 등 목적으로 직접 접속하는 단말기를 인터넷 등 외부통신망으로부터 물리적으로 분리

○ '비중요정보'는 '금융권 클라우드 이용 가이드'상 보호조치를 준수하도록 하고, 개인신용정보 등 '중요정보'의 경우 이용을 제한

□ (개선) 중요정보 처리시스템의 안전성을 확보하기 위해 클라우드 이용(금융회사), 제공(제공자)시 기준을 도입하고 운영방안을 수립

① 클라우드 서비스 이용·제공 기준 마련(금융권 클라우드 서비스 가이드라인)

- (금융회사) 중요정보 클라우드 이용시 정보보호 의무 준수, 서비스 제공자 관리·감독, 중요장비 이중화 등 안전성 관리를 강화

→ 금융회사의 서비스 도입검토, 이용계약, 운영관리, 사후처리 등 모든과정에서 필요한 클라우드 관리 및 보안요구사항을 포함

* 서비스 연속성 보장, 정보보호 의무, 감독·검사권 수용 등을 서비스 이용 계약에 포함하여 클라우드 서비스 제공자에 대한 관리·감독 수행, 중요장비의 이중화, 클라우드 시스템 및 데이터의 물리적 위치 제한(국내로 한정) 등

- (제공자) 금융 특수성을 반영해 금융회사 수준의 시스템 구축·운영, 암호화 적용 등 클라우드 서비스 제공자가 준수해야 할 기준을 마련

→ '중요정보'의 경우 기존 금융권 전산시스템과 유사한 수준의 보안 요구사항을 제공기준에 반영하여 사고발생을 미연에 방지

* 클라우드 정보보호 기준 고시의 통제항목에 더하여 금융 고유 특수성을 반영 (건물, 전원·공조, 전산실 등에 대하여 금융회사 수준의 구축 및 운영, 검증필 암호화 기술 적용, 통합보안관제 제반환경 지원 등)

- (책임 명확화) 금융회사와 제공자간 클라우드 이용 계약 체결시 개인정보유출, 전자적 침해사고 등에 대한 책임 소재를 명확히 규정

< 클라우드 제공 관련 규정 >

☐ 「클라우드컴퓨팅서비스 정보보호에 관한 기준 고시」(과기정통부) 주요 통제항목

구분	주요 통제항목	내용
관리적 보호조치	정보보호정책, 인적보안, 자산관리, 공급망 관리, 침해사고 관리 등	정보보호 정책 타당성 및 효과 검증, 직무분리, 자산식별 및 위험관리, 침해사고 대응절차 수립 등
물리적 보호조치	보안구역 지정, 물리적 접근제어, 시설보호, 장비 반출입 등	물리적 보호구역 지정, 출입통제, 보호설비 구비, 시설 및 장비 유지보수, 장비 반출입 통제 등
기술적 보호조치	가상화 보안, 접근통제, 네트워크 보안, 데이터보안, 암호화 등	가상자원 모니터링, 악성코드 통제, 접근권한 관리, 네트워크 분리, 데이터 보호·무결성 확인, 암호정책 수립 등

☐ 공공기관용 클라우드 컴퓨팅서비스 추가 보호조치(과기정통부)

구 분			세 부 조 치 사 항
공 공 기 관	관 리 적 보 호 조 치	보안서비스 수준 협약	○ 공공기관의 보안 요구사항이 반영된 보안서비스 수준 협약 ○ 클라우드서비스 관련 정보보호 정보를 공공기관에 제공
		도입 전산장비 안전성	○ 서버·PC 가상화 솔루션 및 정보보호 제품 중에 CC인증이 필수적인 제품군은 국내·외 CC인증을 받은 제품을 사용
		보안관리 수준	○ 클라우드 운영 장소 및 망은 공공기관 내부 정보 시스템 운영 보안 수준에 준하여 보안 관리
		사고 및 장애 대응	○ 사고 또는 장애 발생 시 공공기관 사고·장애 대응 절차에 따라 대응하고, 공공기관의 사고·장애 대응에 적극 협조
	물 리 적 보 호 조 치	물리적 위치 및 분리	○ 클라우드 시스템 및 데이터의 물리적 위치는 국내로 한정 ○ 공공기관용 클라우드의 서버, 네트워크, 보안장비, 출입통제, 운영인력 등은 일반 클라우드서비스 영역과 분리하여 운영
		중요장비 이중화 등	○ 네트워크 스위치, 스토리지 등 중요장비를 이중화 ○ 서비스의 가용성을 보장하기 위해 백업체계를 구축
	기 술 적 보 호 조 치	검증필 암호화 기술	○ 중요자료를 암호화하는 수단을 제공하는 경우에는 검증필 국가표준암호화 기술을 제공
		보안관제 제반환경 지원	○ 공공기관에 클라우드 서비스 보안관제 수행에 필요한 제반 환경을 지원하여야 함

☐ 금융권 특화 보안기준(예시)

- ① 클라우드 시스템 및 데이터의 물리적 위치를 국내로 한정
- ② 금융회사 및 위임된 제3자에게 관련 접근권 및 현장감사권 부여
- ③ 클라우드 서비스 중단 및 데이터 소실에 대비한 금융권 백업체계 마련
- ④ 취약점 분석·평가, 비상대응훈련, 통합보안관제에 필요한 제반환경 지원
- ⑤ 침해사고 및 장애 발생에 따른 보고절차 준수 및 조사·대응
- ⑥ 건물, 전원·공조, 전산실 등에 대하여 금융회사 수준의 구축 및 운영

② 금융분야 클라우드 서비스 기준 운영방안

- (자율통제 또는 인증제) 클라우드 서비스 이용·제공 기준을 토대로
^①금융회사 자율적으로 클라우드 이용을 결정하는 방식(EU 등 해외방식)
 또는 ^②금융 클라우드 인증제 도입 방식(국내 공공클라우드 방식)을 검토

⇒ 동 방식은 금융권 클라우드 서비스 이용 활성화를 위한 제도 개선 TF*('18.7월중 출범)를 통해 검토 추진

* 금융위, 금감원, 금보원, 금융회사, 전문가 등

< 금융분야 클라우드 서비스 이용·제공 방안 >

(1안) 금융분야 클라우드 서비스 기준을 통한 자율 통제방식

- 금융권 클라우드 서비스 제공시 관련기준 등을 가이드로 마련하고 해당 가이드에 대해 금융회사 등이 자율적으로 준수토록 통제

- 클라우드 사고발생시 보상, 사고대응체계 구축 등 금융권 클라우드 사용에 특화된 내용을 금융회사가 내부통제 절차에 따라 관리·감독

* 금융회사가 관련 기준을 토대로 클라우드 이용(이용범위 결정 등)부터 점검, 사후관리 단계까지 자율적으로 통제하고 클라우드 서비스 제공자를 관리·감독

(2안) 금융분야 특화 클라우드 서비스 인증 평가 방식

- 금융분야 클라우드 보안 서비스 인증제를 도입하고, 보안성 평가를 통과한 클라우드컴퓨팅 사업자를 통해 서비스 제공

- 과기정통부의 경우 클라우드 보안 서비스 인증제*를 통해 공공기관의 민간 클라우드 서비스 이용을 허용

* 한국인터넷진흥원(KISA)이 관리적/물리적/기술적 보호조치 및 공공기관용 추가 보호조치 등 총 14개 부문 117개를 통제항목으로 평가하여 인증 (KT, NBP, 가비아, LG CNS, NHN엔터테인먼트가 인증을 취득 ('18.4))

<금융회사 클라우드 이용방안별 분석>

구분	클라우드 서비스 자율 통제방식	금융분야 인증 클라우드
장점	<ul style="list-style-type: none"> · 신속·저렴한 서비스 · 다양한 사업자 이용 	<ul style="list-style-type: none"> · 신뢰성 보장 · 금융회사 서비스 이용 용이 · 사업자 관리·감독 문제 해소
단점	<ul style="list-style-type: none"> · 보안사고 우려 상존 · 보안관련 금융회사 투자 필요 · 사업자 관리·감독 어려움 	<ul style="list-style-type: none"> · 별도 인증체계 확보 필요 · 제도 준비기간 소요(1~2년 소요 예상)

3. 클라우드 서비스 이용 감독·검사 강화

◆ 금융회사 클라우드 서비스 이용 관련 보고의무를 강화하고, 클라우드 서비스 제공자에 대한 감독·조사업무 근거를 마련

□ (현행) 금융회사가 전자금융보조업자(클라우드)와 계약시 전자금융 거래의 안전성·신뢰성 확보를 위해 일정 기준을 준수토록 요구

○ 클라우드 제공업체에 대한 감독당국의 직접 감독권한은 없으며, 금융회사가 클라우드 이용시 보안대책을 수립하고 정기점검 실시

□ (개선) 금융회사를 통한 간접 감독을 강화하는 한편, 법령개정을 통해 전자금융보조업자에 대한 감독·조사 근거를 마련

* 영국, EU 등은 금융권 클라우드 이용을 확대하면서 이에 상응하는 감독을 강화중 → 금융당국의 클라우드 서비스 제공자에 대한 감독권 확보를 권고

① (보고 의무화) 금융회사 클라우드 이용시 주요내용 보고를 의무화

- 신용정보의 클라우드 이용시 위탁 주요사항 등에 대한 금융회사의 보고의무를 부여하여 감독당국 상시 모니터링을 강화
- 금융회사 규모(자산규모, 고객수), 위탁정보 종류(중요정보 여부) 및 처리량 등에 따라 보고의무를 차등화하는 방안을 검토

<금융회사의 클라우드 이용 보고(예시)>

가. '중요정보' 클라우드 이용 보고

- 클라우드 서비스 제공자, 데이터 저장위치, 정보처리 현황(정보 유형·정보량) 등 주요사항을 감독당국에 보고

나. '비중요정보'라도 감독당국 요청시 보고

- 클라우드 유형 등 위탁 계약 관련 최신 정보를 유지하고 감독당국 요청시 제공

* 클라우드 서비스 제공자의 재무건전성, 계약의 변경사항, 비상계획 및 테스트결과 등에 대한 보고내용을 포함

② (직접 감독·조사) 전자금융보조업자에 대한 감독당국의 직접 감독·조사 근거를 마련하는 방안을 검토

- 침해사고·장애 발생시 정확한 원인분석을 위해 자료수집 및 현장검사 등 직접 감독·조사업무 근거를 마련
- 현행 규정상 클라우드 서비스 제공자(보조업자)에 대한 '조사권'에 현장출입권 등을 부여(법 제40조제5항, 감독규정 제61조 개정)

< 「금융권 클라우드 이용확대」 단계별 추진계획 >



V. 기대 효과

① 핀테크기업들이 특별한 제약없이 클라우드를 활용해서 적은 비용으로 쉽게 혁신 서비스를 개발할 수 있는 여건을 마련

○ 보안성을 확보한 클라우드를 통해 핀테크기업은 초기 시스템 구축·관리 비용 부담을 덜고, 핀테크 서비스 안전성은 향상

* 클라우드 활용시 신규 시스템 구축 비용을 약 30% 절감 가능

② 금융권은 클라우드 플랫폼을 이용해서 빅데이터 및 인공지능 기술을 보다 자유롭게 테스트하고 혁신적인 서비스를 출시

○ 복잡해지는 국내외 금융규제 환경변화에도 빠르고 유연하게 대응

(사례) IFRS17 플랫폼 구축시 클라우드를 통해 비용부담을 줄이고, 보험계리분석·회계관리·투자분석 프로그램 등을 쉽게 이용

* 2021년부터 보험회사에 새로운 보험계약 회계기준인 IFRS17 적용 예정, IFRS17 시스템 신규 구축 시 고성능 연산 능력이 필요해 보험회사에 부담

③ 금융회사·핀테크기업이 클라우드를 활용해 협력을 강화하고, 각자의 강점을 발휘함으로써 국내 금융산업 경쟁력도 향상

* 예) 금융회사는 API 등 핀테크 서비스 개발을 위한 클라우드 인프라 제공 → 핀테크 기업은 클라우드 내에서 안전하고 쉽게 핀테크 서비스를 개발

VI. 향후 계획

□ 금융권 클라우드 제도개선 TF* 구성 : 7월

* 금융감독원, 금융보안원, 금융회사, 클라우드 서비스 업체, 전문가 등

○ 감독규정 개정안 마련 → 업계, 전문가 의견 수렴(간담회 등, 8월~9월)

* 업계 수렴 의견, 제도개선 효과 등을 종합 검토하여 제도개선(안)을 확정하고, 「전자금융감독규정」 개정을 추진

□ 「금융권 클라우드 서비스 가이드라인」 개정 : 8~12월

□ 전자금융감독규정 개정안 시행 : '19.1월(예정)

① [EU] EBA(유럽은행청)은 클라우드 이용자 유의사항 등을 명시한 「클라우드 제공자 업무 위탁에 대한 권고」를 발표('18.7월 발효)

- 금융회사는 위탁 대상 업무에 대한 중요도 평가를 통해 중요 업무 선별, 중요 업무를 클라우드 제공자에 위탁 시
 - 클라우드 제공자의 법인명, 클라우드 서비스 수행 국가 및 데이터 저장 위치 등을 관할 당국에 통보
 - 중요 업무 여부와 관계없이 클라우드 유형 등 위탁 계약 관련 최신 정보를 유지하고 관할 당국에서 요청 시 제공해야함
- 금융회사 및 위임된 제3자에게 위탁 업무 관련 접근권 및 현장감사권을 부여하도록 클라우드 제공자와 서면으로 계약 체결할 것
- 정보 전송 시 정보보호 의무 및 서비스 연속성 보장 등의 보안 요구사항을 위탁계약에 명시적으로 포함, 위탁 결정 전 보안 관련 사항을 확인하고, 위탁 후 보안 조치 이행 모니터링 등 관련 위험 관리 실시
- 클라우드 제공자가 위치하는 국가에서 요구하는 컴플라이언스 및 법적 위험성에 대한 평가를 통해 위탁하는 데이터 처리 위치 고려

② [영국] FCA(금융감독청)에서 금융회사의 클라우드 이용(퍼블릭 클라우드 포함) 명시적 허용 및 컴플라이언스 의무 등을 명시한 「클라우드 및 제3자 IT 아웃소싱 관련 지침」을 발표('16.7월)

- (법적 요구사항) 중요 업무 아웃소싱 시 해당 결정의 근거가 되는 문서화된 명확한 비즈니스 사례 또는 이유를 보유
 - 아웃소싱이 기업의 운영리스크를 악화시키지 않도록 하고, 정확한 계약 기록을 유지
 - 제공자 사업장 관할지를 파악, 영국 법률에 의한 규율 여부 확인(그렇지 않은 경우 해당 사업장 감사 및 규제 권한 등 보장)
 - 데이터보호법(DPA, '98년) 준수, 이를 통해 발생할 수 있는 법적 또는 규제 의무 및 요구사항 고려, SYSC 8(FCA 핸드북-아웃소싱 관련) 등 준수
- (리스크 관리) 리스크 평가 실시 및 기록, 전반적인 법적·운영리스크 파악, 제공자 파산 시, 데이터 유출 시 조치방법 등 고려
- (보안) 실사·감사 등 진행 시 ISO 등 국제 표준 준수, 제공자 자산 등에 대한 보안 리스크 평가* 진행
 - * 데이터 거주 정책 확인, 데이터 유출 시 보고 절차 준수, 데이터 분리 저장 현황 확인, 데이터 민감도를 고려한 전송 및 저장 시 암호화 등
- (기타) 효과적인 데이터 접근, 제공자의 사업 관할지* 접근 등
 - * 사업관할지가 사무실, 운영센터 등이 될 수 있으나, 데이터 센터를 반드시 포함하지는 않음(일부 사업자는 보안상 데이터 센터 접근 제한 가능)

③ [미국] FFIEC(검사협의회)에서 금융권 클라우드 이용시 주의사항을 명시한 「아웃소싱 클라우드 컴퓨팅」을 발표('12.7월)

- 다른 클라우드 이용자와 데이터 저장소가 공유되는 경우, 금융기관의 데이터에 대한 무결성과 기밀성 보호를 위한 서비스 제공자의 통제 사항 확인, 재해복구(DR) 및 업무연속성계획(BCP)의 적절성 확인
- 소비자 데이터가 국외에서 저장 또는 처리될 경우, 해당 국가의 관련 규정 확인
- 클라우드 컴퓨팅 서비스 제공자와 계약 시 금융기관의 프라이버시 법규 관련 책임, 보안사고 시 보고 의무, 정보 유출 시 소비자 및 당국에 보고해야 하는 법적 의무 등 명시

④ [일본] 금융당국의 지침 등은 없으나 자율규제기구인 FISC의 시스템 안전대책 기준·해설서 內 클라우드 통제항목 명시

- 클라우드 서비스를 이용시 아래의 안전대책을 강구
 - 클라우드 제공자 거점이 금융회사가 통제가능한 지역에 소재할 것
 - 클라우드 이용 계약시 금융회사의 감사권한 등 권리를 명기할 것
 - 클라우드 제공자에 대한 정기적 감사를 실시할 것
 - 금융회사의 클라우드 제공가산 책임범위를 명확히 설정할 것 등

⑤ [싱가포르] MAS(통화국)는 클라우드 서비스도 아웃소싱의 하나로 명시하고 「아웃소싱 가이드라인」('16.7월) 준수토록 규정

- 클라우드 이용시 금융회사는 클라우드 제공자에 대한 실사를 실시하고, 가이드에 명시된 아웃소싱 위험관리를 수행
- 데이터가 혼재되어 있는 클라우드의 특성을 인식하여 아래의 보안조치 이행
 - 데이터 접근, 기밀성, 무결성 보장 등을 위한 금융회사의 적극적 조치
 - 클라우드 제공자가 적정한 통제를 통해 고객데이터를 명확히 분리하는지 확인 등
- 금융회사는 클라우드 제공자를 관리·감독하고 도입에 따른 궁극적 책임을 부담 등

⑥ [호주] APRA(금융감독청)은 아웃소싱 규정(CPS 231) 및 「공유 컴퓨팅 서비스(클라우드 포함) 관련 아웃소싱에 대한 정보 사항」('15.7월)을 통해 금융회사의 클라우드 이용시 통지의무 등을 명시

- 중요 아웃소싱 경우에 한해 국내는 APRA에 통지하고, 국외 또는 내재된 위험이 높을 경우* APRA와 사전 협의할 것을 권고

* 퍼블릭 클라우드 사용시 등

참고3

국내외 금융권 클라우드 서비스 이용 현황 및 계획

금융회사	현황 및 계획
Societe Generale	- 전체 서버의 40%를 클라우드로 운영 中 (하이브리드 방식) - '20년까지 80%로 확대할 계획
ABN AMRO	- '15년 중반부터 클라우드 이전 작업 시작 - '19년말까지 860개 어플리케이션 이전 예정
Deutsche Bank	- IT인프라의 36%를 클라우드로 운영 中 (프라이빗 방식) - 3년 內 80%까지 확대 목표
Credit Suisse	- IT인프라의 약 17%를 클라우드로 이전 - '20년까지 60%로 확대 목표
Mediobanca	- IBM과 클라우드 서비스(SaaS 및 PaaS) 이용 계약(10년) 체결
Danske Bank	- IBM과 클라우드 서비스 이용계약(10년) 체결(인공지능 플랫폼 왓슨 사용 포함)
Lloyds	- IBM과 클라우드 서비스 이용계약 체결 (이전에 약 3년 소요 예상)
Barclays Bank	- 클라우드 서비스 이용증가로 은행 데이터 센터 축소 계획 (30개 → '19년 4개)
HSBC	- 빅데이터 시스템의 클라우드 운영을 위해 구글과 협의 진행
Standard Chartered	- '17년부터 클라우드 인프라 도입 추진
SMFG	- 퍼블릭 클라우드를 이용한 차세대 작업 환경 구축 추진
J.P. Morgan	- '16년에 프라이빗 클라우드 Gaia 도입 - 향후 2년간 매년 2배씩 클라우드 이용비중 증가 계획
Bank of America	- 클라우드 서비스 이용증가로 '17년에 3개 데이터 센터 폐쇄 - 보안 민감성이 낮은 업무를 중심으로 퍼블릭 클라우드 이용 검토
Citigroup	- 클라우드로의 이전을 통해 12,000개 서버를 제거 - '20년까지 PC 8만대를 제거하고 모바일 환경으로 이전계획
KB 금융그룹	- 클라우드 기반 HR 시스템 도입 - 아마존 클라우드 기반 메시지 뱅킹 서비스 플랫폼 사용
신한 금융그룹	- 미국 및 일본 지점에서 클라우드 서비스 도입 추진 - 미국지점 인터넷뱅킹 플랫폼을 아마존 클라우드에 구축
우리은행	- 은행 고유의 메시징 시스템을 클라우드 환경에서 운영

※ 출처 : Digitalization in Banking : on the cusp of operational revolution? (모건스탠리)