특집 02

디지털 금융의 클라우드 보안 강화를 위한 공동 책임 모델 설계

민경조 (테크타카)

목 차

1. 서 론

IT 산업은 짧은 시간에 혁신적으로 발전했다. 기술은 빠르게 발전했지만 법령과 규제는 기술의 발전 속도에 미치지 못하여 여러 부작용이 나타났다. 퍼블릭 클라우드 서비스가 활성화됨에 따라 많은 기업과 기관들이 비즈니스를 위하여 IT 환경을 기존 온-프레미스(On-Premise) 방식에서 퍼블릭 클라우드 기반으로 전환하고 있다. 이러한 추세에 맞춰 국내·외에서 법률 등의 장치가 마련되고 있다. 영국에서는 2011년 '정부 클라우드 전략'을 수립하여 발표하였고, 미국 연방 정부도 2019년 '연방 클라우드 컴퓨팅 전략'을 발표하였다. 국내에서도 2015년 3월 '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률'을 제정하고 9월부터 시행하였다.

하지만 금융권에서는 까다로운 규제를 비롯한 다양한 이유로 클라우드의 도입 속도가 더딘 것이 사실이다. 2022년 4월 금융위원회는 금융분야에서도 클라우드 이용할 수 있도록 '금융분야 클라우드 및 망분리 규제 개선방안'을 발표하였다. 그동안 금융회사 또는 전자금융업자의 클라우드 활용에 어려움으로 작용했던 클라우드 컴퓨팅 서비스에 대한 규제가 일부 완화되었다.

클라우드 서비스 제공자는 여러 이용자에게 서비스를 제공하기 위하여 서비스 구조를 설계하고, 자원 공유 등의 방식을 이용하여 이용자에게 서비스를 제공한다. 공유되는 자원을 사용함으로 인하여 자원을 공유하지 않는 온-프레미스와는 다른 보안에 대한 근본적인 위험이 발생한다. 이러한 차이 때문에 발생하는 위협의 종류와 위협에 대처하는 방식도 달라져야 한다. 하지만 클라우드를 사용하는 많은 기관과 기업은 기존의 온-프레미스에서 사용하는 보안 방식을 사용하고 있으며 이로 인하여 보안의 수준이 낮아지고, 사고가 발생하고 있다. 대부분의 클라우드 보안 사고는 이용자의 잘못으로 인하여 발생하지만, 2018년 11월 AWS 서울 리전 DNS 서버 설정 오류와 같은 클라우드 서비스 제공자의 잘못으로 인한 보안 사고도 발생한다.

이러한 사고가 발생할 경우 책임 소재를 가려주는 기준이 공동 책임 모델이다. 퍼블릭 클라우드

서비스 제공자 대부분 공동 책임 모델, 혹은 비슷한 개념을 정의하고 있다. 공동 책임 모델의 취지는 클라우드 서비스 제공자와 이용자가 협력하여 각자가 통제하는 요소를 보호하고 궁극적으로 클라우드 전체의 보안 수준을 높이는 것이다. 퍼블릭 클라우드 도입 시 서비스 수준 협약(Service Level Agreement, SLA)에 공동 책임 모델을 반드시 포함해야 하는 이유이기도 하다.

2. 클라우드의 보안 위협과 대응

클라우드 컴퓨팅 환경에 구축된 서비스가 늘어나고, 저장되어 처리되는 데이터 양이 늘어남에 따라 클라우드에서의 보안 위협 또한 늘어나고 있다. 가상화, 원격지에 정보 위탁, 특정 사업자에 종속, 모바일 기기로부터 접속함으로 인하여 발생하는 복합적인 보안 위협이 증가하고 있다. 또한 주요 데이터, 인프라 등이 클라우드로 전환되며 멀티·하이브리드 클라우드 환경이 보편화되며 기업 및 기관의 보안관리 영역이 늘어나는 만큼 보안 설정과 공백을 노리는 위협이 증가하고 있다.

2.1 디지털 금융 클라우드의 보안 위협

2019년 미국의 금융지주사인 캐피탈원에서는 1억 600만명, 미국 성인 전체에 달하는 규모의 개인정보 유출 사건이 발생했다. 2005년부터 2019년까지 신용카드를 발급받은 고객들의 이름과 주소, 생년월일을 비롯한 신용점수와 예금잔액 등 세부 금융정보들까지 모두 유출되었다. 캐피탈원은 이와 같은 정보를 AWS(아마존웹서비스)의 인프라에 저장을 하였지만, 방화벽 설정이 미흡하여 정보가 유출됐다.

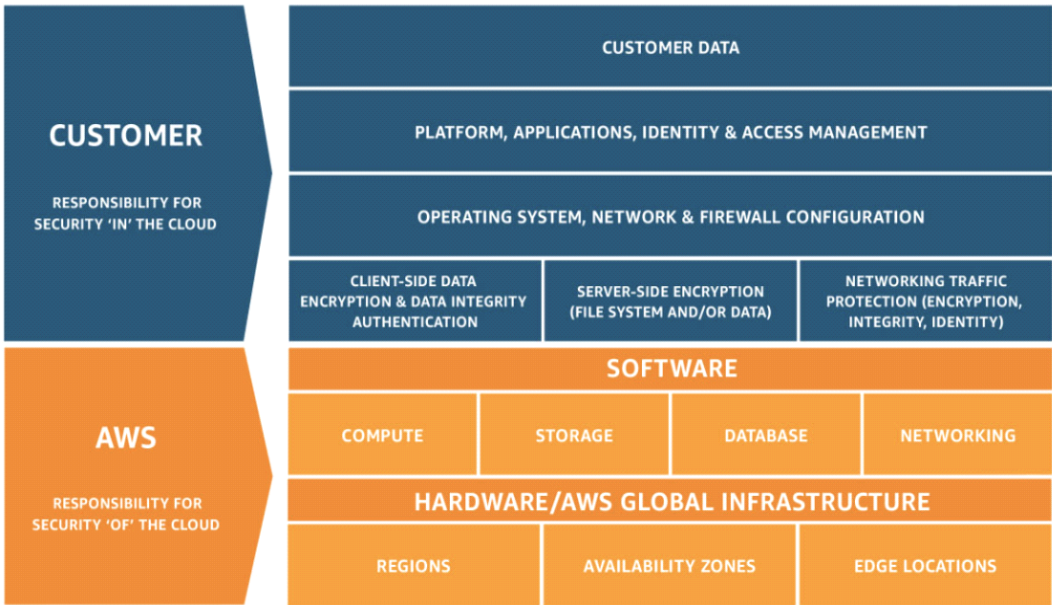
이와 같이 클라우드는 다양한 리스크를 내재하고 있다. 내부적인 요인으로는 클라우드 환경에 대한 전문성 부족, 권한관리 미흡 등으로 인한 시스템 장애 및 사고 발생 위험이 있다. 또한 외부적인 요인으로는 관리감독에 클라우드 서비스 제공자의 협조가 필수라는 점, 주요 클라우드 서비스 제공자의 본사가 외국에 있기 때문에 관리 감독이 어려울 수 있다는 점, 다수의 금융회사가 특정 클라우드 서비스 제공자에 의존할 수 있다는 점 등이 있다.

2.2 디지털 금융 클라우드의 보안 관리

2023년 2월 금융보안원에서 배포한 '금융분야 클라우드 컴퓨팅서비스 이용가이드' 는 금융회사 또는 전자금융업자(이하 '금융회사')가 클라우드 컴퓨팅 서비스(이하 '클라우드 서비스')를 이용하고자 할 경우 요구되는 세부절차와 금융 시스템 안전성 및 금융소비자 보호를 위해 필요한 사항을 안내하는 것을 목적으로 개정되었다. 이 가이드는 금융회사가 클라우드 서비스 이용시 준수해야 할 절차, 보안대책 등을 설명하고 있으며, 금융회사가 클라우드 서비스 제공자의 안전성을 평가하기 위한 세무기준을 안내하고 있다. 특히, 전자금융거래법 제11조에 따라 전자금융거래와 관련하여 클라우드 서비스 제공자의 고의나 과실은 금융회사의 고의나 과실로 판단하며, 전자금융사고 발생 시 클라우드 서비스 이용을 이유로 금융회사의 책임이 면제되지 않으며, 금융회사는 클라우드 서비스 제공자가 관계 법령을 준수하도록 관리·감독할 의무가 있다고 규정하였다. 특히, 7장 '계약 체결'에서 클라우드 서비스 제공자와 금융회사는 각자의 정보보호 역할과 책임의 범위를 명확하게 정의해야 한다고 하였다.

3. 클라우드 서비스 제공자별 공동 책임 모델

공동 책임 모델은 클라우드 서비스를 사용함에 있어 보안과 규정 준수를 클라우드 서비스 제공자



* 출처 : AWS(https://aws.amazon.com/ko/compliance/shared-responsibility-model/)

(그림 1) AWS 의 공동 책임 모델

와 사용자가 책임을 공유한다는 모델이다. 사용자는 게스트 운영 체제 및 다른 관련 어플리케이션 소프트웨어 관리와 보안 그룹(방화벽) 등을 관리할 책임이 있으며, 물리적 및 환경 제어 항목은 전적으로 클라우드 서비스 제공자가 책임을 진다. 또한 패치 관리와 구성 관리, 인지 및 교육 등에 대해서는 책임을 공유한다.

AWS, Microsoft Azure 와 같은 글로벌 클라우드 서비스 제공자 및 Naver NCP 와 같은 국내 클라우드 서비스 제공자를 비롯하여 정보기술 자문 회사인 Gartner 또한 공동 책임 모델을 제시하고 있다. 일반적으로 다만, 각 회사별로 책임 영역의 구분과 책임의 소유자에 대해서는 각 제공자별로 차이가 있다.

Gartner는 책임 영역을 6개로 구분하여 가장 포괄적이니 공동 책임 모델을 제시하고 있으며, AWS는 8개, Azure는 10개로 구분하고 있고, NCP 는 11개로 구분하여 가장 세분화된 공동 책

〈표 1〉 클라우드 서비스 제공자별 공동 책임 모델에 대한 항목 수

구분	항목 수			
	AWS	Azure	NCP	Gartner
Data	2	1	1	1
Device	-	1	-	-
Virtual Infrastrcture	3	2	2	2
IAM	1	2	-	-
Platform		-	-	1
Application		1	3	1
Physical Layer	2	2	5	1

임 모델을 제시하고 있다.

4. 디지털 금융을 위한 클라우드 컴퓨팅 공동 책임 모델

클라우드 컴퓨팅을 사용함에 있어 공동 책임 모델은 사용자의 운영 부담을 경감할 수 있지만, 제공자와 사용자 사이의 책임이 명확하지 않아 서로 책임을 회피하는 수단이 될 수 있다. 그렇기 때문에 책임을 명확히 구분할 수 있는 공동 책임 모델이 필요하다. 특히, '금융분야 클라우드 컴퓨팅 서비스 이용가이드'에서는 금융회사와 클라우드 서비스 제공자의 책임 관계를 명확히 구분하여야 한다고 하였다.

〈표 2〉 디지털 금융의 클라우드 보안 강화를 위한 공동 책임 모델

구분	통제 영역	통제 요소	Responsibilities		
			IaaS	PaaS	SaaS
Data	Customer Content	데이터 분류 및 관리 (보호 등급, 권한 관리, 백업/복구)	F	F	F
	Client Data Encryption	데이터 암호화	F	F	F
Device	Device(Mobile and PCs)	단말 보안	F	F	F
Application	Interfaces	API 무결성 보장	F	F	P
	Applications	성능 및 확장성 관리	F	F	P
		백업/복구 관리	F	F	P
		변경 관리	F	F	P
		모니터링	F	F	P
	Solution Stack (Programming Languages)	Secure Coding	F	F	P
IAM	Accounts and Identities	계정 관리	F	F	F
		자원 격리	F	F	F
	Identity and Directory Infrastructure	사용자 분류	F	F	F
		권한 통제	F	F	F
Virtual Infrastructure	Operating Systems(OS)	가상 서버 보안	F	P	P
	Network Controls(Protection)	가상 네트워크 보안	F	P	P
	Virtual Machines	가상화 보안	F	P	P
		성능 및 확장성 기술	F	P	P
		서버 측면의 암호화	F	P	P
Physical Layer	Hypervisors	분산 시스템 구조	P	P	P
		가상화 시스템 구조	P	P	P
		성능 및 확장성 기술	P	P	P
	Data Storage(Hard Drives, Removable Disks, Backups, etc)	스토리지 보안	P	P	P
	Network(Interfaces and Devices, Communication Infrastructure)	네트워크 보안	P	P	P
	Physical Facilities/Data Centers	물리 시설에 대한 관리/보안	P	P	P
		데이터센터의 위치(지역, 가용영역 등)	P	P	P

* Responsibilities : F(금융회사), P(클라우드 서비스 제공자)

클라우드 서비스 제공자와 사용자 사이의 책임을 명확하기 위하여 (표 2)와 같은 디지털 금융 클라우드를 위한 공동 책임 모델을 설계하였다. '전자금융감독규정'을 비롯한 금융권의 별도의 강화된 보안 규제 및 규정을 준수하기 위하여 금융회사의 책임을 강조하였다. 전자금융거래법 제11조에 따라 전자금융거래와 관련하여 클라우드 서비스 제공자의 고의나 과실은 금융회사의 고의나 과실로 판단한다. 이러한 이유로 제안한 모델에서 금융회사는 책임의 소재가 클라우드 서비스 제공자에게 있다고 하여도 금융 회사의 책임이 면책되지 않는다는 사실을 인지하고, 클라우드 서비스 제공자를 관리·감독할 의무가 있다.

5. 결 론

IT 산업은 짧은 시간에 혁신적으로 발전했다. 기술은 빠르게 발전했지만 법령과 규제는 기술의 발전 속도에 미치지 못하여 여러 부작용이 나타났다. 특히나 민감한 개인정보를 처리해야 하는 금융권에서는 이러한 규제로 클라우드의 도입 속도가 더딘 것이 사실이다.

클라우드 컴퓨팅은 빠르게 발전하고 있는 IT 산업에서 핵심 분야이며, 가장 빠르게 성장하고 있는 산업이기도 하다. AI, Big Data, Block Chain 등 최근 각광받는 모든 기술이 클라우드 컴퓨팅을 활용하여 발전하고 있다. 클라우드 컴퓨팅을 사용하게 되면 유연성, 확장성, 편의성 등의 장점을 활용하여 기업에 맞는 IT 환경을 구축할 수 있다. 하지만 디지털 금융의 경우 클라우드 서비스를 이용하기 위하여 업무선정 및 중요도 평가, 클라우드 서비스 제공자 평가, 업무 연속성 계획 및 안전성 확보조치 방안 수립, 정보보호위원회 심의·의결, 계약 체결, 이용 및 보고와 같은 절차를 준수해야 하고 그에 맞는 까다로운 규제를 준수해야 하기 때문에 도입이 지연되거나 검토 단계에서 취소되는 일이 발생한다.

전자금융거래와 관련하여 클라우드 서비스 제공자의 고의나 과실은 금융회사의 고의나 과실로 본다는 기본 원칙이 있지만, 클라우드 서비스 제공자의 책임을 면제해 주지는 않는다. 1차적인 책임은 금융회사에게 있더라도 명백히 클라우드 서비스 제공자의 고의나 과실이 있다면 그 책임은 클라우드 서비스 제공자에게 있다.

클라우드 서비스는 기본적으로 공동 책임 모델을 기반으로 서비스 수준 협약(SLA)가 구성되어 있다. 클라우드 서비스 제공자는 서비스를 제공함에 있어 이용자의 보안에 대하여 완전하게 책임지지 않는다는 것이다. 이용자에게 책임을 전가하는 것이 아니라 클라우드 서비스 제공자가 책임질 수 있는 범위와 책임질 수 없는 범위를 구분하는 것이다. 하지만 공동 책임 모델은 각 클라우드 서비스 제공자마다 별도의 모델을 공개하고 있어 표준화되지 않고, 제도적으로도 법규가 정비되지 않아 사고 발생시 클라우드 서비스 제공자와 금융회사 사이의 책임소재 분쟁이 발생할 수 있고, 지속적인 책임소재 분쟁은 다수의 개인고객이 피해를 보는 상황이 야기될 수 있다.

금융회사에서 클라우드 컴퓨팅을 사용하기 위하여 준수해야 하는 법규는 '클라우드컴퓨팅법, 전자금융감독규정, 개인정보보호법, 정보통신망법, 신용정보법' 등이 있다. 해당 법규에 공동 책임 모델을 기반으로 한 클라우드에서의 각 분야에 대한 책임 범위를 포함하여야 할 것이다.

참 고 문 헌

[1] 김민석, 금융 클라우드 보안을 위한 제도적 · 기술적 보안 방안, 2020년 8월
[2] 한국인터넷진흥원(2017). 클라우드 정보보

호 안내서. KISA-2017-003
[3] 금융보안원(2023), 금융분야 클라우드컴퓨팅 서비스 이용 가이드, AGR-X-20230-2-231.
[4] 서광규(2018), 클라우드서비스 활성화를 위한 서비스수준협약(SLA) 프레임워크, 융합정보논문지,8:6, 173-186
[5] CIS (2020), Cloud Security and the Shared Responsibility Model with CIS. Center for Internet Security 2020.
[6] Michael Lane, Anup Shrestha and OmarAli (2017), Managing the Risks of Data Security and Privacy in the Cloud: A Shared Responsibility between the Cloud Service Providerand the Client Organisation. The Bright Internet Global Summit 2017, Seoul, Korea
[7] CSA (2020), Top Threats to Cloud Computing. Cloud Security Aliance, 2020

저 자 약 력

민 경 조

이메일 : kyungjo85@gmail.com

- 2011년 인하대학교 정보통신공학과 (학사)
- 2022년 중앙대학교 산업융합보안학과 (석사)
- 2011년~2016년 (주)SK / 대리
- 2016년~2019년 (주)쿠팡 / Sr.Security Engineer
- 2019년~2020년 (주)메쉬코리아 / 팀장
- 2021년~현재 (주)테크타카 / 팀장
- 관심분야 : 클라우드 보안, 금융 보안, 보안 자동화, 개인정보보호