AGR - IX - 2022 - ② - 335

금융분야 클라우드컴퓨팅서비스 이용 가이드

2022. 11.

금융미래를 열어가는 금융보안파트너
금융보안원
FINANCIAL SECURITY INSTITUTE

CONTENTS

제1장 가이드 개요 ····· 1

1. 목적 ····· 2
2. 가이드의 효력 ····· 2
3. 구성 ····· 3
4. 기본 원칙 ····· 3
5. 적용 범위(예시) ····· 4
6. 용어 ····· 11

제2장 클라우드서비스 이용 절차 ·· 15

1. 클라우드서비스 이용 절차 개요 ····· 17

제3장 업무 선정 및 중요도 평가 ·· 21

1. 이용대상 선정 ····· 22
2. 중요도 평가 기준 및 항목 ····· 23
3. 중요도 평가 절차 ····· 24

제4장 클라우드서비스 제공자 평가 27

1. 클라우드서비스 제공자 안전성 평가 개요 ····· 30
2. 평가 절차 및 방법 ····· 32
3. 평가 항목 및 생략기준 ····· 34

제5장 업무 연속성 계획 및 안전성 확보조치 방안 수립 ····· 43

1. 업무 연속성 계획 수립 ····· 47
2. 안전성 확보조치 방안 수립 ····· 54

제6장 정보보호위원회 심의·의결 77

제7장 계약 체결 ····· 81

1. 기본 포함사항 ····· 84
2. 추가 포함사항 ····· 92

제8장 이용 및 보고 ····· 99

1. 보고 ····· 100
2. 보고 방법 ····· 103
3. 클라우드 이용 관련 리스크 관리 ··· 104

제9장 이용 종료 ····· 107

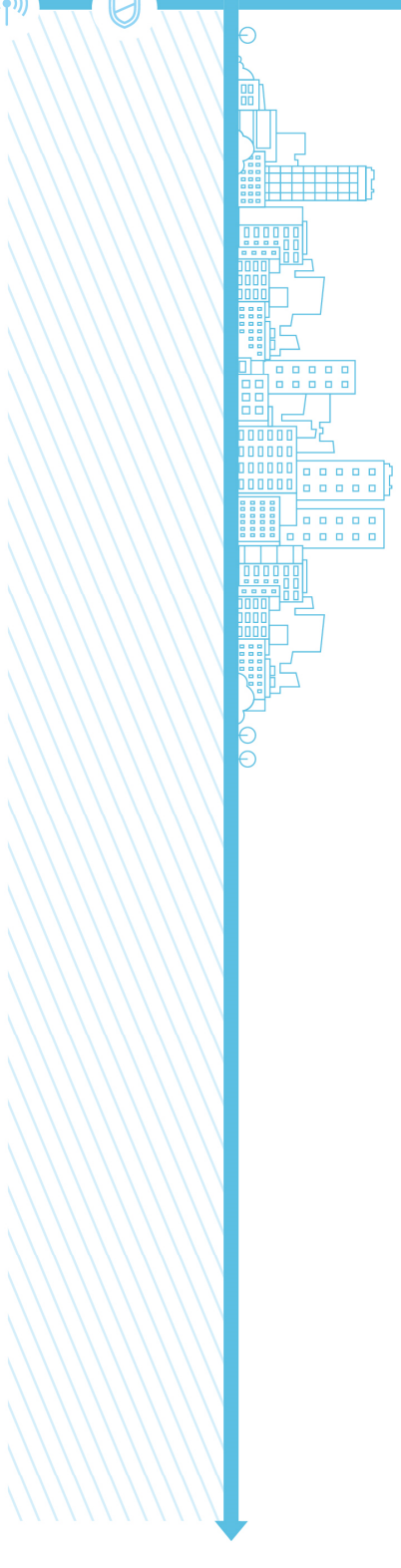
부록 1 업무중요도 평가 방법 및 사례 예시 ····· 111

부록 2 클라우드 서비스 제공자 집중 리스크 관리시 고려사항 119

1. 금융회사의 클라우드서비스 제공자 집중 리스크 관리시 고려사항 ····· 120
2. 국외 클라우드 서비스 제공자(제3자)에 대한 리스크 대응방안 ····· 121

별 첨 금융분야 망분리 및 클라우드 규제 개선 관련 FAQ ····· 125

1. FAQ 답변 활용 시 고려사항 ····· 126
2. SaaS 서비스 이용 시 고려사항 ····· 126
3. 금융분야 망분리 및 클라우드 규제개선 관련 FAQ ····· 127



금융분야 클라우드컴퓨팅서비스 이용 가이드

제 1 장

가이드 개요

1. 목적
2. 가이드의 효력
3. 구성
4. 기본 원칙
5. 적용범위(예시)
6. 용어

제1장 가이드 개요

1 목적

이 가이드는 금융회사 또는 전자금융업자(이하 '금융회사')가 클라우드컴퓨팅 서비스(이하 '클라우드서비스')를 이용하고자 할 경우 요구되는 세부절차와 금융시스템 안전성 및 금융소비자 보호를 위해 필요한 사항을 안내하는 것을 목적으로 함

금융회사는 클라우드서비스를 이용함에 있어 적절한 보안 대책을 수립·운영하기 위해 이 가이드를 활용할 것을 권고함

2 가이드의 효력

금융회사가 클라우드서비스를 이용하고자 할 경우 「전자금융감독규정」(이하 '감독규정'), 「금융회사의 정보처리 업무 위탁에 관한 규정」(이하 '정보처리위탁규정') 등을 반드시 준수하여야 함

이 가이드의 내용과 관련 법규가 서로 일치하지 않는 경우에는 법규에 규정된 내용이 가이드보다 우선함

가이드에 포함되어 있으나 법규에는 규정되지 않는 내용을 금융회사가 준수할 의무는 없음

3 구성

이 가이드는 본문(제2장~제9장)과 부록, 별첨으로 구성

본문에서는 금융회사가 클라우드서비스 이용 시 준수해야 할 절차, 보안대책 등을 설명하고 있으며, 부록에서는 금융회사가 감독규정 제14조의2제1항제1호에 따른 업무중요도 평가방법 및 사례 안내, 제1항제2호에 따른 클라우드서비스 제공자의 안전성을 평가하기 위한 세부기준을 안내하고, 별첨에서는 금융위원회에서 발표한 전자금융감독규정 개정에 따른 FAQ 내용을 포함하고 있음

4 기본 원칙

전자금융업무와 관련한 정보처리시스템을 해당 금융회사를 위하여 운영하는 사업자는 전자금융보조업자에 해당하므로, 전자금융업무 관련 정보처리에 클라우드서비스를 이용하는 경우 클라우드서비스 제공자 또한 전자금융보조업자에 해당함

정보처리의 위탁이라 함은 금융회사가 자신의 정보처리(전산설비를 활용하여 정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 및 기타 유사한 행위를 하는 것) 업무를 제3자로 하여금 계속적으로 처리하도록 하는 행위를 말하므로, 금융회사가 클라우드서비스 제공자와 계약을 체결하고 클라우드서비스를 이용하는 행위는 정보처리위탁규정 제2조제6항에 따라 정보처리의 위탁에 해당함

전자금융거래법 제11조에 따라 전자금융거래와 관련하여 클라우드서비스 제공자의 고의나 과실은 금융회사의 고의나 과실로 봄

전자금융사고 발생 시 클라우드서비스 이용을 이유로 금융회사의 책임이 면제되지 않으며, 금융회사는 클라우드서비스 제공자가 관계 법령을 준수하도록 관리·감독 하여야 함

5 적용 범위(예시)

감독규정 제14조의2는 금융회사가 클라우드컴퓨팅법 제2조제3호*에 따른 클라우드컴퓨팅서비스를 이용하는 경우 관련 절차를 준수하도록 규정

* 클라우드컴퓨팅법 제2조제3호에서 규정하고 있는 것 이외의 클라우드서비스를 이용하는 경우에는 감독규정 제14조의2의 절차를 준수하지 않아도 무방(다만, 같은 조 제8항에 따른 예외 필요 시 제1항의 절차 준수 필요)

▶ 클라우드컴퓨팅 주요법령 해설서('17.11월) 中

(요약 中)
□ 총론
2 클라우드컴퓨팅법 제21조의 적용 대상
클라우드컴퓨팅서비스는 원칙적으로 상용(商用)으로 제공되는 서비스이어야 됩니다. 여기서 상용 이란 무상 유상에 구애받지 않고 상업용으로 제공되는 것을 의미하므로 무상이라 하더라도 상용으로 제공되고 있다면 포함될 수 있습니다. 커뮤니티나 하이브리드 등의 방식으로 구축된 클라우드컴퓨팅시스템이라도 서비스의 전부 또는 일부를 클라우드컴퓨팅서비스 제공자가 상용으로 제공하고 있다면 그 범위 내에서 제21조의 클라우드컴퓨팅서비스로 볼 수 있습니다.

Ⅱ. 법 제21조의 적용 대상
1. 법 제21조의 적용 분야
○ 인·허가 등이 요구되는 업종
- 제21조는 업종이나 업태의 구분 없이 또는 민간이나 공공의 구분 없이 해당 법령에서 인가·허가·등록·지정 등의 요건으로 전산시설등의 구비 의무를 규정하고 있는 경우에는 모두 적용 대상이 됩니다.
- 법령에 의해서 인·허가 등이 요구되고 있는 대표적인 분야로는 금융, 의료, 교육, 정보통신 등이 있지만 이에 한정되지 아니합니다. 특히 최근 다양한 전통산업 분야에서 ICT를 활용한 신산업·신서비스가 등장하고 있어 ICT에 대한 의존도가 확대되고 될 것으로 전망됨에 따라 전산시설등의 요건을 규정하는 법령의 수도 많아질 수 것으로 예상됩니다.

○ 그 밖의 인 허가 등의 대상 분야
- 정부를 대신해서 각종 인가 및 평가 업무, 조사·검사 업무 등을 대행하는 기업이나 기관·단체·개인에 대해서도 평가·인증·검사기관의 지정 등의 요건으로 전산시설등의 구비를 요구하는 경우가 많습니다. 이 경우에도 전산시설등의 구비 요건을 클라우드컴퓨팅서비스로 대체할 수 있습니다.

2. 클라우드컴퓨팅서비스의 범위
○ 클라우드컴퓨팅서비스의 개념
- 법 제21조에서 다른 법령에서 규정하고 있는 전산시설등의 구비요건을 대체할 수 있는 클라우드컴퓨팅서비스는 상용(商用)으로 제공되는 서비스여야 됩니다.

- 법 제2조 제3호가 클라우드컴퓨팅서비스를 '클라우드컴퓨팅을 활용하여 상용으로 타인에게 정보통신자원을 제공하는 서비스'로 정의하고 있기 때문입니다
- 상용으로 타인에게 제공하는 클라우드컴퓨팅서비스여야 하므로 타인이 아닌 자기 스스로 이용을 위하여 구축한 전산시설등은 비록 클라우드컴퓨팅기술을 도입한 것이라도 이 법의 클라우드컴퓨팅서비스에 해당하지 아니합니다.
- 여기서 "상용"이란 무상·유상에 구애받지 않고 상업용으로 제공되는 것을 의미하므로 무상으로 제공되는 클라우드컴퓨팅서비스라도 상용으로 제공되고 있다면 포함될 수 있습니다. 무상으로 클라우드컴퓨팅서비스를 제공하더라도 광고를 통해서 수익을 올리고 있다면 상용에 해당합니다.
- 반면 전산시설등의 사용 수수료를 내더라도 상용(商用)으로 제공되는 클라우드컴퓨팅서비스가 아니라면 이 법에서 말하는 클라우드컴퓨팅서비스에 해당하지 아니합니다. 예컨대 협회, 단체 등이 전용으로 구축한 클라우드컴퓨팅서비스는 포함되지 않습니다.

ㅇ 클라우드컴퓨팅서비스의 유형

- 클라우드컴퓨팅서비스는 서비스의 운영 방식(배치 모델)에 따라 일반적으로 1) 프라이빗 클라우드컴퓨팅서비스, 2) 퍼블릭 클라우드컴퓨팅서비스, 3) 커뮤니티 클라우드컴퓨팅서비스, 4) 하이브리드 클라우드컴퓨팅서비스 등으로 나뉩니다.
- 이 중에서 상용으로 제공되는 클라우드컴퓨팅서비스는 주로 퍼블릭 클라우드컴퓨팅서비스입니다. 직접 개발·구축·운영·관리하는 경우에는 원칙적으로 이 법에서 규정하고 있는 클라우드컴퓨팅서비스에 해당하지 않습니다.
- 커뮤니티 클라우드컴퓨팅서비스나 하이브리드 클라우드컴퓨팅서비스도 서비스의 배치 및 운영 방식만 다를 뿐 상용으로 제공이 가능하므로 상용으로 제공 이용되고 있는 한, 이 법에서 규정하고 있는 클라우드컴퓨팅서비스에 포함될 수 있습니다.
- 커뮤니티, 하이브리드 등의 방식으로 구축된 클라우드시스템이라도 서비스의 전부 또는 일부를 클라우드컴퓨팅서비스 제공자가 유상으로 제공하고 있다면 그 범위 내에서 제21조에서 규정하고 있는 클라우드컴퓨팅서비스로 볼 수 있습니다,

ㅇ 클라우드컴퓨팅서비스의 범위

- 클라우드컴퓨팅 기술로 제공될 수 있는 서비스는 실무적으로 응용소프트웨어 서비스(SaaS), 플랫폼 서비스(PaaS), IT 인프라 서비스(IaaS) 등으로 나뉘고 있으나 기술적으로 클라우드컴퓨팅 기술을 통해서 제공될 수 있는 서비스의 범위에는 제한이 없습니다.
- 법 제21조도 클라우드컴퓨팅서비스로 대체가 가능한 전산시설등의 대상 및 범위에 대해서 특별한 제한을 두고 있지 아니하므로 정보통신기기, 정보통신설비, 소프트웨어 등 모든 정보통신자원을 클라우드컴퓨팅서비스로 대체가 가능합니다

클라우드컴퓨팅법 제2조제3호에 따른 '클라우드컴퓨팅서비스'란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스로서 ①서버, 저장장치, 네트워크 등을 제공하는 서비스, ②응용프로그램 등 소프트웨어를 제공하는 서비스, ③응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스, ④그 밖에 ①~③의 서비스를 둘 이상 복합하는 경우를 의미

본 예시는 **기존 법령해석 및 비조치 의견서를 기반으로 분류한 참고 사례로서,** 각 금융회사 등에서 **정확한 적용 범위를 판단 하고자 할 때, 각 사의 이용 목적 및 이용 환경 등에 맞게 법령 해석 또는 비조치 의견을** 관련 절차에 따라 접수하여 **확인 필요**

가. 적용 대상 클라우드(예시)

- 무상으로 제공하더라도 광고를 통해 수익을 올리는 등 상업용으로 제공 중인 클라우드서비스
- 자체적으로 구축하거나 협회, 단체, 계열사 등이 구축한 클라우드시스템이라도 서비스의 전부 또는 일부를 소속 구성원 이외를 대상으로 상용으로 제공하고 있다면 그 범위 내에서 대상에 포함

나. 미적용 대상 클라우드(예시)

- 해당 금융회사의 자원(시스템·네트워크 등 포함)이 타 사용자와 물리적으로 분리되어 공유되지 않도록 전용으로 구축(아웃소싱 포함)한 클라우드서비스

  ※ 타인이 개발·구축·운영·관리하는 경우에도 해당 전산 시설이 타 사용자와 물리적으로 분리되어 공유되지 않는 경우 포함

- 금융지주, 금융IT 회사, 협회 등이 소속 구성원 전용(구성원 이외 사용자와 물리적으로 분리되어 공유되지 않음)으로 구축한 클라우드서비스(소속 구성원만을 대상으로 서비스 제공하면서 감독규정을 모두 준수하고, 서비스 제공에 따른 최소한의 대가를 받는 경우도 非상용 클라우드로 인정 가능)

  ※ 단, 금융지주, 금융IT 회사 등에서 감독규정 제11조제11호 및 제12호, 제15조제1항 제5호를 준수하면서 非상용 프라이빗 클라우드서비스 등을 구축·운영하여 금융 계열사 내에서 사용하는 경우에만 해당

- 기업홍보 등의 목적으로 유튜브(Youtube) 및 페이스북(Facebook)등과 같은 클라우드 기반의 웹서비스를 단순 이용하는 경우

참고 적용 범위 관련 법령해석 회신문 및 비조치의견서

▶ 법령해석 회신문(190152, `19.7.3.)
: 정보처리업무위탁 및 클라우드컴퓨팅서비스 이용 해당 여부

〈 질의요지 〉
고객이 스마트폰으로 촬영하는 공과금 고지서 이미지에 대해 고객이 선택적으로 제휴사에서 제공하는 OCR 텍스트 변환 기능을 이용하고, 은행 서버와 제휴사 서버 간에는 통신/정보 교환 없이 고객 스마트폰만이 제휴사 서버와 API 통신으로 고지서 이미지의 텍스트 변환이 이루어질 경우, 은행의 정보처리 업무 위탁 및 클라우드 컴퓨팅 서비스 이용 해당여부

〈 회답 〉
□ "정보처리의 위탁"이라 함은 금융회사가 자신의 정보처리 업무를 제3자로 하여금 계속적으로 처리하도록 하는 행위를 의미합니다"(「금융회사의 정보처리 업무 위탁에 관한 규정」 제2조 제6항)
○ 따라서 OCR 서비스가 금융회사 자신의 정보처리 업무가 아니라면 동 규정이 적용되지 않으며, 이 경우 정보처리 업무 위탁의 한 유형인 전자금융감독규정상의 클라우드서비스 이용 관련 규정도 적용된다고 보기 어렵습니다.

〈 이유 〉
□ 질의하신 사항은 금융회사가 고객정보를 위탁·전송하지 않으며(은행 서버와 해당 업체 서버 간 통신/정보 교환도 없음),
○ 고객이 OCR 서비스를 제공하는 업체와 직접 정보 제공 동의, 이용 계약을 체결하는 경우에 정보처리 업무 위탁의 해당 여부 등입니다.

□ "정보처리의 위탁"이라 함은 금융회사가 자신의 정보처리 업무를 제3자로 하여금 계속적으로 처리하도록 하는 행위를 의미합니다.(「금융회사의 정보처리 업무 위탁에 관한 규정」 제2조 제6항)
○ 따라서 금융회사 자신의 정보처리 업무가 아니라면 동 규정이 적용되지 않으며, 이 경우 정보처리 업무 위탁의 한 유형인 전자금융감독규정상의 클라우드 서비스 이용 관련 규정도 적용된다고 보기 어렵습니다.
○ 질의사항은 OCR서비스 제공 업체가 자신의 서비스 업무를 처리할 목적으로 고객정보를 직접 수집·처리하고, 금융회사 - OCR서비스 제공자간 고객정보의 전송행위도 이루어지지 않으므로(이미지의 텍스트 변환 결과는 고객 스마트폰에 저장) 정보처리 업무위탁, 금융회사의 클라우드 서비스 이용 행위(클라우드 서비스는 OCR서비스 제공자가 이용)라고 보기는 어렵습니다.

▶ 법령해석 회신문(190042, `19.3.20.)
: 전자금융업자의 클라우드 서비스 이용 관련 질의

〈 질의요지 〉
1. 전자금융업자가 국내에 전산센터를 둔 해외 클라우드 사업자의 서비스를 이용하는 것이 가능한지?
2. 전자금융업자가 개인신용정보를 처리하는 경우에도 국내에 전산센터를 둔 해외 클라우드 사업자의 서비스를 이용할 수 있는지?
3. 전자금융업자와 클라우드제공자 간에 VPN을 사용하여 접속하는 것이 가능한지 여부
4. 클라우드서비스제공자 선정 시 정보보호위원회에서 심의해야 하는 평가항목은?
5. 전자금융업자의 시스템과 분리된 별도의 망에 구성된 시스템 간에 데이터/보안 암호키를 공유할 수 있는지?
6. 클라우드의 경우 논리적 망분리가 허용되는 것인지?

참고 적용 범위 관련 법령해석 회신문 및 비조치의견서

〈 회답 〉

□ 전자금융업자가 개인신용정보를 클라우드 서비스를 통해 처리하고자 할 경우 국내에 이미 전산센터를 갖춘 해외 클라우드의 사업자의 서비스를 이용하는 것이 가능합니다.

* 다만, 개인신용정보는 국내(전산센터)에서 처리되어야 함

○ 또한, 고유식별정보, 개인신용정보를 제외한 비중요정보를 클라우드를 통해 처리하는 경우에는 해외 소재 클라우드도 이용할 수 있습니다(질의 1, 2에 대한 답변).

□ 전자금융업자가 클라우드 서비스에 연결해야 할 경우 VPN을 이용하는 것이 가능합니다(질의 3에 대한 답변).

□ 전자금융업자는 클라우드서비스를 이용할 경우 중요도 평가 결과, 자체 업무 위수탁 운영기준, 클라우드서비스 제공자 건전성 및 안전성 평가 결과에 대해 정보보호위원회를 개최하여 심의·의결하여야 합니다(질의 4에 대한 답변).

□ 전자금융업자의 시스템과 타 시스템간 정보 공유가 필요할 경우 해당 정보와 관련한 암호키를 공유할 수 있으나, 이 경우에도 해당 암호키는 접근통제 정책을 통해 안전하게 관리할 필요가 있습니다(질의 5에 대한 답변).

□ 전자금융업자가 클라우드컴퓨팅서비스 이용절차에 따라 클라우드서비스를 이용하는 경우에는 물리적 망분리의 예외가 인정됩니다(전자금융감독규정 제14조의2 제8항).

〈 이유 〉

□ 현행 규정은 전자금융업자가 개인신용정보를 클라우드 서비스를 통해 처리하는 경우에는 해당 정보처리시스템을 국내에 설치토록 하고 있음(전자금융감독규정 제14조의2제8항)

○ 동 규정은 개인신용정보 보호, 감독가능성 확보를 위해 정보시스템의 위치를 국내로 제한한 것이므로, 전자금융업자는 국내에 이미 전산센터를 갖춘 해외 클라우드의 사업자의 서비스도 이용할 수 있음

○ 한편, 고유식별정보, 개인신용정보를 포함하지 않은 비중요정보 시스템에 한정된 클라우드 서비스를 이용할 경우에는 해외 소재 클라우드도 이용할 수 있음

□ 전자금융업자의 업무용 단말기, 내부망 정보처리시스템을 클라우드서비스 제공자 구간에 위치한 내부망 정보처리시스템에 연결하거나, 관리용 단말기를 클라우드 서비스에 연결해야 하는 경우 VPN을 이용하는 것이 가능함(전자금융감독규정 제14조의2 제8항)

□ 전자금융업자는 중요도 평가 결과, 자체 업무 위수탁 운영기준, 클라우드서비스 제공자 건전성 및 안전성 평가 결과에 대해 정보보호위원회를 개최하여 심의·의결 하여야 함(전자금융감독규정 제14조의2제2항)

□ 현행 규정은 전자금융업자로 하여금 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리토록 하고 있음(전자금융감독규정 제31조)

○ 암호키에 대해 비인가접근을 방지하기위해 암호키에 대한 접근제어 정책을 수립하여야 함

○ 즉, 암호화 키는 접근이 통제된 보안네트워크에 저장하고, 클라우드서비스 제공자의 직원이나 동일 클라우드서비스를 이용하는 외부 기관이 접근할 수 없도록 조치가 필요

○ 전자금융업자의 시스템과 타 시스템간 정보 공유가 필요할 경우 해당 정보와 관련한 암호키를 공유할 수 있으나, 이 경우에도 해당 암호키는 접근통제 정책을 통해 안전하게 관리할 필요

참고 적용 범위 관련 법령해석 회신문 및 비조치의견서

□ 전자금융업자가 클라우드컴퓨팅서비스 이용절차(전자금융감독규정 제14조의2)에 따라 클라우드서비스를 이용하는 경우에는 물리적 망분리의 예외가 인정됨(전자금융감독규정 제14조의2 제8항)

* 망분리 예외와 관련한 구체적 사항은 전자금융감독규정 시행세칙상 망분리 대체 정보보호통제 수칙(전자금융감독규정 시행세칙 제2조의2), 금융분야 클라우드 이용가이드라인을 참조

▶ 비조치의견서(190057, `20.1.13.): 전자금융업자가 고객정보를 제3자에게 제공시 금감원 보고대상에 해당되는지 여부

※ 비조치의견서는 신청자의 특정 행위에 대한 의견으로서 일반적 효력을 가지지 않음에 유의

〈 요청대상 행위 〉

□ 전자금융업자가 정보 주체의 동의를 받아 개인신용정보 등을 제3자에게 제공*하고, 그 제3자가 제공받은 정보를 클라우드컴퓨팅서비스를 이용하여 처리하는 경우

* 제3자 제공 시 개인정보보호법, 정보통신망법, 신용정보법 등 개인정보 관계 법령을 준수하고 정보주체의 동의를 받는 것을 전제로 함

○ 「전자금융감독규정」 제14조의2에 따른 금융감독원 사전보고 대상에 해당하는지 여부

〈 판단 〉

□ 전자금융업자가 자신의 정보처리 업무를 위탁하는 것이 아닌 고객 정보를 제3자에게 단순 제공하는 것은 「전자금융감독규정」 제14조의2에 따른 사전보고 대상에 해당하지 않습니다.

〈 판단이유 〉

□ 「전자금융감독규정」 제14조의2에 따른 클라우드컴퓨팅서비스 이용은 금융회사 및 전자금융업자가 자신의 정보처리 업무를 클라우드서비스제공자로 하여금 계속적으로 처리하게 하는 정보처리 위탁 행위에 해당하는데*,

* '금융분야 클라우드컴퓨팅서비스 이용 가이드'('19.1월), 「금융회사의 정보처리 업무 위탁에 관한 규정」 제2조제6항

○ 마케팅 제휴 등으로 인해 고객 정보를 제3자에게 단순 제공하는 것은 자신의 정보처리 업무를 타인에게 위탁하는 것이 아니므로 동 규정의 적용을 받지 않습니다.

▶ 비조치의견서(190037, `19.11.4.): 전자금융업자의 자사 클라우드 서비스 이용 가능 여부

※ 비조치의견서는 신청자의 특정 행위에 대한 의견으로서 일반적 효력을 가지지 않음에 유의

〈 요청대상 행위 〉

□ 전자금융업자가 「전자금융감독규정」 제14조의2에 따라 본인이 운영하는 상용 클라우드 서비스를 이용하는 것이 가능한지 여부

□ 자사 클라우드 서비스 이용이 가능할 경우 동 규정 제3항에 따른 사전보고 제출 서류는 어떻게 되는지

〈 판단 〉

□ 금융회사 및 전자금융업자가 본인이 운영하는 상용 클라우드 서비스를 이용하는 것은 가능하며, 이 경우에도 「전자금융감독규정」 제14조의2의 절차를 준수해야 합니다.

□ 자사 클라우드 서비스 이용에 따른 사전보고시 위탁계약서 등 위탁관계에 따른 서류를 제출할 필요는 없으나, 상용 클라우드 이용과 관련된 서류로 대체하여 제출해야 합니다.

참고 적용 범위 관련 법령해석 회신문 및 비조치의견서

〈 판단이유 〉

□ 「전자금융감독규정」 제14조의2에서 자사 클라우드 서비스 이용을 제한하고 있지 않으므로 금융회사 및 전자금융업자는 본인이 운영하는 상용 클라우드 서비스를 이용할 수 있습니다.

○ 다만, 이 경우에도 중요도 평가 등 동 규정에서 요구하고 있는 클라우드 이용 절차를 모두 준수해야 합니다.

□ 자사 클라우드 서비스 이용에 따른 사전보고시 위탁계약서 등 위탁관계에 따른 서류 제출할 필요는 없으나, 상용 클라우드 이용과 관련된 서류로 대체*하여 제출해야 합니다.

* 예) 업무위수탁 운영 기준 → 상용 클라우드 이용에 따른 운영 기준

○ 세부적인 제출서류 및 보고절차는 금융감독원 담당자(02-3145-7424)에게 문의하시기 바랍니다.

▶ 비조치의견서(190011, '19.5.27.): 스타트업 개발환경 지원 목적의 클라우드 이용시 「전자금융감독규정」 적용 여부

※ 비조치의견서는 신청자의 특정 행위에 대한 의견으로서 일반적 효력을 가지지 않음에 유의

〈 요청대상 행위 〉

□ 은행이 핀테크 기업을 지원하기 위한 OO개발지원센터를 운영하면서 스타트업이 사용하기 위한 개발용 클라우드 환경을 제공하는 경우, 「전자금융감독규정」 제14조의2에 따른 관련 절차*를 이행해야 하는지 여부

* 정보처리시스템 중요도 평가, 클라우스서비스 제공자(CSP)에 대한 건전성 및 안전성 평가, 자체 업무위·수탁 운영기준 마련·준수 등

〈 판단 〉

□ 금융회사가 자신의 정보처리 업무를 처리하는 것이 아닌 스타트업에 개발 환경을 지원하기 위해 클라우드를 이용하는 경우에는, 「전자금융감독규정」 제14조의2에 따른 절차가 적용되지 않음

〈 판단이유 〉

□ 「전자금융감독규정」 제14조의2에 따른 클라우드 이용은 금융회사의 정보처리 위탁에 해당*하는바,

* 「금융분야 클라우드컴퓨팅서비스 이용 가이드」 p.3

○ '정보처리 위탁'은 금융회사가 자신의 정보처리 업무를 제3자로 하여금 계속적으로 처리하게 하는 것을 의미하므로(「금융회사의 정보처리 업무 위탁에 관한 규정」 제2조제6항)

○ 금융회사가 자신의 정보처리 업무를 처리하는 것이 아닌 스타트업에 개발 환경을 지원하기 위해 클라우드를 이용하는 경우에는 동 규정이 적용되지 않음

6 용어

이 가이드에서 사용되는 용어는 감독규정 제2조 및 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조의 정의를 따름

▶ 감독규정

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "전산실"이라 함은 전산장비, 통신 및 보안장비, 전산자료 보관 및 출력장비가 설치된 장소를 말한다.
2. "전산자료"라 함은 전산장비에 의해 입력·보관·출력되어 있는 자료를 말하며 그 자료가 입력·출력되어 있는 자기테이프, 디스크, 디스켓, 콤팩트디스크(CD) 등 보조기억매체를 포함한다.
3. "정보처리시스템"이라 함은 전자금융업무를 포함하여 정보기술부문에 사용되는 하드웨어(hardware)와 소프트웨어(software)를 말하며 관련 장비를 포함한다.
4. "정보기술부문"이라 함은 컴퓨터 등 정보처리능력을 가진 장치를 이용하여 정보를 수집·가공·저장·검색·송신 또는 수신을 행하는 금융회사 또는 전자금융업자의 업무, 인력, 시설 및 조직을 말한다.
5. "정보보호" 또는 "정보보안"이라 함은 컴퓨터 등 정보처리능력을 가진 장치를 이용하여 수집·가공·저장·검색·송신 또는 수신되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 기술적·물리적·관리적 수단을 강구하는 일체의 행위를 말하며 사이버안전을 포함한다.
6. "정보보호시스템"이라 함은 정보처리시스템 내 정보를 유출·위변조·훼손하거나 정보처리시스템의 정상적인 서비스를 방해하는 행위로부터 정보 등을 보호하기 위한 장비 및 프로그램을 말한다.
7. "해킹"이라 함은 접근을 허가받지 아니하고 전자금융기반시설에 불법적으로 침투하거나 허가받지 아니한 권한을 불법적으로 갖는 행위 또는 전자금융기반시설을 공격하거나 해를 끼치는 행위를 말한다.
8. "컴퓨터악성코드"(이하 "악성코드"라 한다)라 함은 컴퓨터에서 이용자의 허락 없이 스스로를 복사하거나 변형한 뒤 정보유출, 시스템 파괴 등의 작업을 수행하여 이용자에게 피해를 주는 프로그램을 말한다.
9. "공개용 웹서버"라 함은 인터넷 이용자들이 웹페이지를 자유롭게 보고 웹서비스(월드 와이드 웹을 이용한 서비스를 말한다)를 이용할 수 있게 해주는 프로그램이 실행되는 장치를 말한다.
10. "정보통신망"(이하 "통신망"이라 한다)이라 함은 유·무선, 광선 등 정보통신 수단에 의하여 부호·문자·음향·영상 등을 처리·저장 및 송·수신할 수 있는 정보통신 조직형태를 말한다.

▶ 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "클라우드컴퓨팅"(Cloud Computing)이란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원(이하 "정보통신자원"이라 한다)을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계를 말한다.
2. "클라우드컴퓨팅기술"이란 클라우드컴퓨팅의 구축 및 이용에 관한 정보통신기술로서 가상화 기술, 분산처리 기술 등 대통령령으로 정하는 것을 말한다.
3. "클라우드컴퓨팅서비스"란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하는 것을 말한다.

4. “이용자 정보”란 클라우드컴퓨팅서비스 이용자(이하 “이용자”라 한다)가 클라우드컴퓨팅서비스를 이용하여 클라우드컴퓨팅서비스를 제공하는 자(이하 “클라우드컴퓨팅서비스 제공자”라 한다)의 정보통신자원에 저장하는 정보(「지능정보화 기본법」 제2조제1호에 따른 정보를 말한다)로서 이용자가 소유 또는 관리하는 정보를 말한다.

▶ 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령

제2조(클라우드컴퓨팅기술) 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」(이하 “법”이라 한다) 제2조제2호에서 “대통령령으로 정하는 것”이란 다음 각 호의 어느 하나에 해당하는 기술을 말한다.

1. 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원(이하 “정보통신자원”이라 한다)을 가상으로 결합하거나 분할하여 사용하게 하는 기술
2. 대량의 정보를 복수의 정보통신자원으로 분산하여 처리하는 기술
3. 그 밖에 정보통신자원의 배치와 관리 등을 자동화하는 기술 등 클라우드컴퓨팅의 구축 및 이용에 관한 정보통신자원을 활용하는 기술

제3조(클라우드컴퓨팅서비스) 법 제2조제3호에서 “대통령령으로 정하는 것”이란 다음 각 호의 어느 하나에 해당하는 서비스를 말한다.

1. 서버, 저장장치, 네트워크 등을 제공하는 서비스
2. 응용프로그램 등 소프트웨어를 제공하는 서비스
3. 응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스
4. 그 밖에 제1호부터 제3호까지의 서비스를 둘 이상 복합하는 서비스

FSI FINANCIAL SECURITY INSTITUTE
금융미래를 열어가는 금융보안파트너

금융분야 클라우드컴퓨팅서비스 이용 가이드

제 2 장

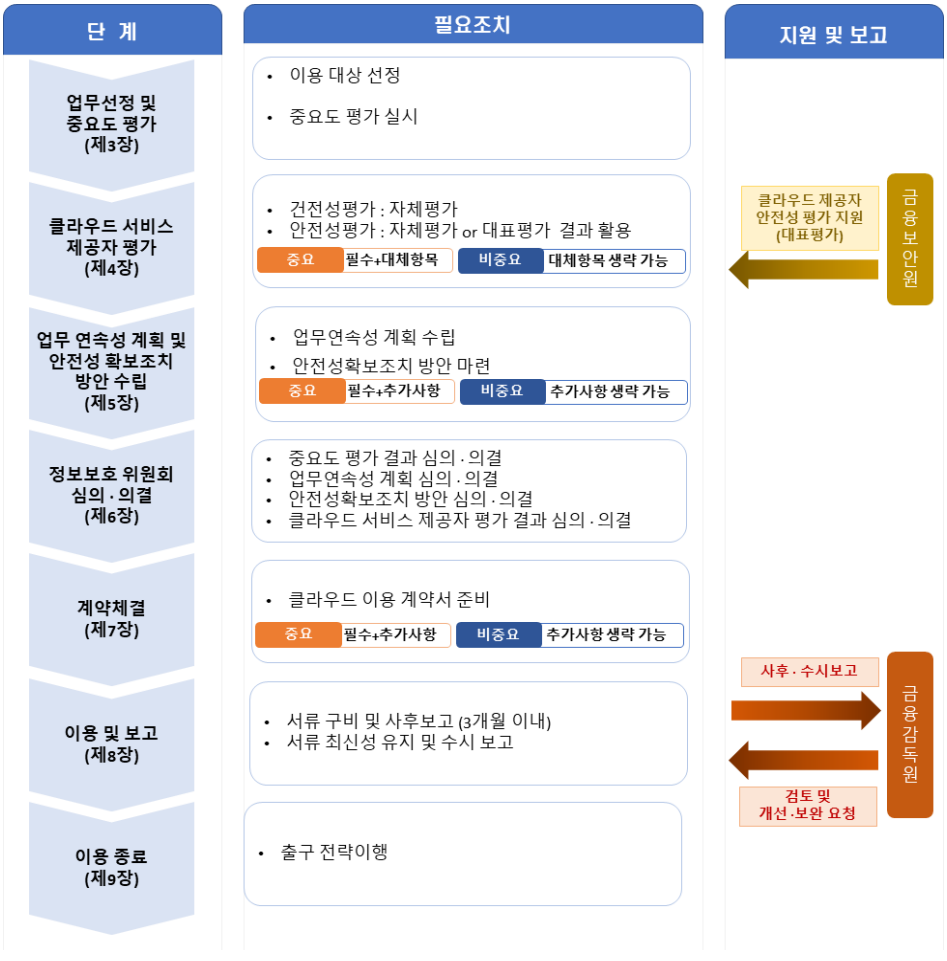
클라우드서비스 이용절차

1. 클라우드서비스 이용절차 개요

제2장 클라우드서비스 이용절차

금융회사는 클라우드서비스 이용 시 다음 절차에 따라 필요한 조치를 수행함으로써 감독규정 제14조의2(클라우드서비스 이용 절차)를 준수하고 적절한 보안수준을 확보하여야 함

〈그림1. 클라우드서비스 이용 절차〉



1 클라우드서비스 이용 절차 개요

가. 업무 선정 및 중요도 평가 (제3장)

- 이용 대상 정보처리 업무 선정
  - 금융회사는 정보처리 업무 중 정보처리의 규모, 클라우드서비스 이용에 따른 비용절감, 업무 효율성 증가 등을 종합적으로 검토하고, 클라우드 서비스 이용 여부를 결정하여야 한다.
- 이용 대상 정보처리 업무 중요도 평가
  - 금융회사는 해당 업무가 취급하는 정보의 중요도*, 클라우드서비스 이용이 전자금융거래의 안전성 및 신뢰성에 미치는 영향 등을 바탕으로 중요도 평가를 수행하여야 한다.

* 이하, 본 가이드에서는 제14조의2제1항제1호 각 목의 기준에 따른 이용업무의 중요도 평가 후 중요도가 '높음'에 해당하는 업무를 중요 업무, 중요도가 '낮음'에 해당하는 업무를 비중요 업무로 칭함([부록1] 참조)

나. 클라우드서비스 제공자 평가 (제4장)

- 이용 목적, 업무 중요도, 현재 위수탁 현황 등을 고려하여 업체를 선정
- 클라우드서비스 제공자 건전성* 및 안전성 평가** 수행

* 건전성 평가의 경우 금융회사 또는 전자금융업자에서 자체적으로 수행

** 침해사고대응기관의 대표평가 결과를 공유받는 경우 활용 가능

※ **(중요 업무)** 이용영역에 대해 필수, 대체 항목을 모두 평가해야 하나, 지정된 클라우드 보안인증을 클라우드서비스 제공자가 보유·유지 하는 경우 대체 항목 생략 가능(필수 항목 생략 불가)

※ **(비중요 업무)** 이용 영역에 대해, 필수 항목 평가필요(대체 항목 생략 가능)

다. 업무 연속성 계획 및 안전성 확보조치 방안 수립 (제5장)

- 업무 연속성 계획(출구전략 포함) 및 안전성 확보조치 방안 수립
  - 금융회사는 클라우드서비스 이용에 따른 업무연속성 계획, 안전성 확보조치 방안 등을 수립하여야 한다.

※ **(중요 업무)** 감독규정 〈별표 2의3〉 클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획, 〈별표 2의4〉 클라우드컴퓨팅서비스 이용과 관련한 안전성 확보조치에서 필수, 추가사항 모두 준수 필요

※ **(비중요 업무)** 업무 연속성 계획, 안전성 확보조치에서 필수 사항 준수 필요(추가 사항 생략 가능)

라. 정보보호위원회 심의·의결 (제6장)

- 정보보호위원회 심의·의결*을 통해 계약 추진 및 클라우드서비스 이용 여부를 최종 결정

  * 중요도 평가 결과, 클라우드서비스 제공자 평가 결과, 업무 연속성 계획 및 안전성 확보조치 방안

마. 계약 체결 (제7장)

- 본 가이드 제7장의 내용을 참고하여 계약 체결

  ※ **(중요 업무)** 감독규정 〈별표 2의5〉 클라우드컴퓨팅서비스 위수탁 계약서 주요 기재사항에서 기본 포함사항, 추가 포함사항 모두 포함 필요

  ※ **(비중요 업무)** 기본 포함사항 기재 필요(추가 포함사항 생략 가능)

바. 이용 및 보고 (제8장)

- 관련 서류 구비, 최신성 유지 및 금융감독원장 요청 시 지체 없이 제공
- 감독규정 제14조2의제4항 각 호의 사유가 발생하는 경우 사유가 발생한 날로부터 3개월 이내에 보고
- '다. 업무 연속성 계획 및 안전성 확보조치 방안 수립' 단계에서 수립된 업무 연속성 계획 및 안전성 확보조치를 준수하여 클라우드 이용 관련 보안 관리 실시

사. 이용 종료 (제9장)

- 클라우드서비스 제공자 파산, 서비스 중단, 서비스 품질 저하, 규제 환경 변화 또는 기타 금융회사의 필요에 따른 클라우드서비스 전환·종료 시 기 수립한 출구 전략에 의거 데이터 이전 및 파기 등 실시

FSI FINANCIAL SECURITY INSTITUTE
금융미래를 열어가는 금융보안파트너

금융분야 클라우드컴퓨팅서비스 이용 가이드

제3장

업무선정 및 중요도 평가

1. 이용대상 선정
2. 중요도 평가 기준 및 항목
3. 중요도 평가 절차

제3장 업무선정 및 중요도 평가

1 이용대상 선정

금융회사는 정보처리업무 중 클라우드서비스 이용에 따른 효율성 등을 감안하여 이용대상을 선정하여야 한다.

- 다음의 예시와 같이 자체 시스템 구축에 비하여 클라우드서비스 이용이 유리하다고 판단되는 경우 클라우드서비스 이용을 적극 고려할 수 있다.

① AI, 빅데이터 등 신기술 활용으로 대량의 컴퓨팅 자원이 단기간에 요구되는 경우
② 신규 또는 파일럿 서비스를 구축하여야 하나, 시스템 사용량 규모에 대한 사전 예측이 어려운 경우
③ 시스템 사용량의 변동이 매우 큰 서비스인 경우
④ 짧은 시간 안에 구축이 필요하거나 기술 변화에 대한 민첩한 대응이 요구되는 경우
⑤ 사전 테스트 등 임시적으로 대용량의 시스템이 필요한 경우
⑥ 클라우드서비스 도입 또는 전환에 필요한 초기 투자비용보다 클라우드서비스 이용에 따른 운영비용 절감이 더 크다고 판단되는 경우
⑦ 자체 시스템을 안전하게 보유·운영할 역량이 부족하나, 내부 운영 인력 등이 클라우드서비스 이용에 필요한 역량을 충분히 갖추고 있는 경우
⑧ 기타 금융회사의 전략 이행을 위해 필요하다고 판단되는 경우

- 그러나, 금융회사의 핵심 업무 수행을 위한 정보처리에 대해서는 효율성 이외에도 업무 중요도, 취급 정보의 민감도, 경영전략 등 다양한 요소를 종합적으로 고려해야 한다.

2 중요도 평가 기준 및 항목

클라우드서비스를 이용하고자 하는 금융회사는 감독규정 제14조의2제1항제1호 기준에 따른 업무 중요도 평가를 위하여 세부 평가항목 수립이 필요

▶ 감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 제1항제1호

1. 다음 각 목의 기준에 따른 이용업무의 중요도 평가
   - 가. 규모, 복잡성 등 클라우드컴퓨팅서비스를 통해 처리되는 업무의 특성
   - 나. 클라우드컴퓨팅서비스 제공자로부터 제공받는 서비스가 중단될 경우 미치는 영향
   - 다. 전자적 침해 행위 발생시 고객에게 미치는 영향
   - 라. 여러 업무를 같은 클라우드컴퓨팅서비스 제공자에게 위탁하는 경우 해당 클라우드컴퓨팅서비스 제공자에 대한 종속 위험
   - 마. 클라우드컴퓨팅서비스 이용에 대한 금융회사 또는 전자금융업자의 내부통제 및 법규 준수 역량
   - 바. 그 밖에 금융감독원장이 정하여 고시하는 사항

참고 중요도 평가 항목 (예시)

[기준 1] 규모, 복잡성 등 클라우드를 통해 처리되는 업무의 특성
해당서비스와 연계된 외부 기관 수
해당서비스와 연결된 내부 시스템 수
업무기능 및 대상
직전 3개월 동안 일평균 서비스 접속자 또는 비율
[기준2] 클라우드컴퓨팅서비스 제공자로부터 제공받는 서비스가 중단될 경우 미치는 영향
업무에 미치는 영향도
중단에 따른 손해금액/사업 전체 매출 금액 비율
비상대응계획 상의 복구 목표 시간(RTO)
[기준 3] 전자적 침해 행위 발생시 고객에게 미치는 영향
고객에게 직·간접적으로 미치는 영향
처리정보 유형에 따른 영향
[기준 4] 여러 업무를 같은 클라우드컴퓨팅 제공자에게 위탁하는 경우 해당 클라우드 컴퓨팅서비스 제공자에 대한 종속 위험
동일 CSP에 대한 업무 의존도
클라우드 환경 구성 방식(멀티클라우드 등)
[기준 5] 클라우드컴퓨팅서비스 이용에 대한 금융회사 및 전자금융업자의 내부통제 및 법규 준수 역량
법적 규제 및 보안요구사항 준수 요구
계약, 보안 등 요구사항 준수여부 관리 감독 수행

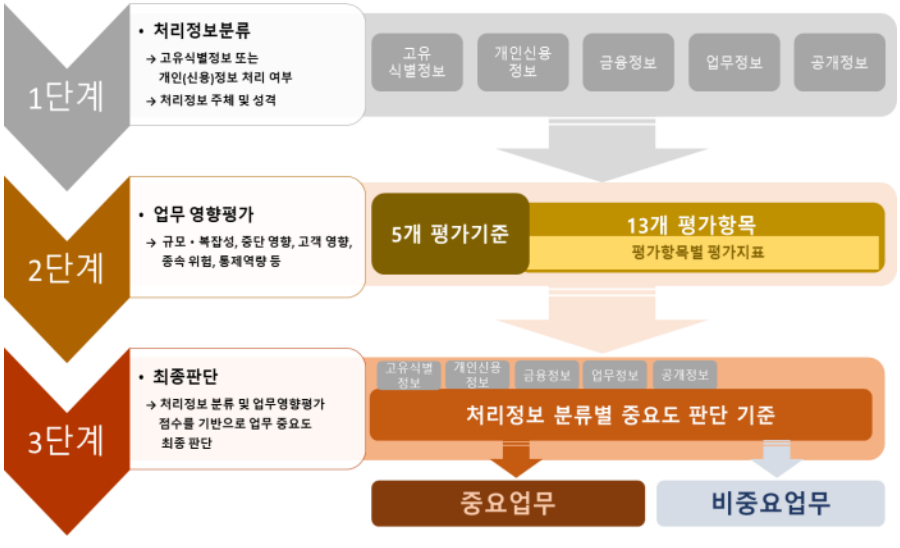
3 중요도 평가 절차

금융회사 자체적으로 수립한 평가절차에 따른 평가방법을 마련하고 중요 업무 여부를 최종 판단하고 그에 따른 이용절차를 준수하여야 함

[중요도 평가 절차 (예시)]

① **(처리정보 분류)** 고유식별정보, 개인신용정보를 처리하고 있는지 여부를 확인하고, 처리정보의 주체(고객, 내부직원 등) 및 성격(대외 공개 등)에 따라 금융정보, 업무정보, 공개정보로 분류
② **(업무 영향 평가)** 평가항목별 평가지표에 따라 평가(상, 중, 하, N/A)하고 항목별 배점에 평가에 따른 점수 가중치를 반영한 점수를 합산하여 점수화
③ **(최종 판단)** 처리정보 유형 별 중요 판단기준에 따라 중요업무 여부를 최종적으로 판단

〈 그림2. 클라우드 이용업무 중요도 평가 절차도〉



※ 중요도 평가 방법 및 평가 사례 예시는 [부록1] 참조

FSI FINANCIAL SECURITY INSTITUTE
금융미래를 열어가는 금융보안파트너

금융분야 클라우드컴퓨팅서비스 이용 가이드

제 4 장

클라우드서비스 제공자 평가

1. 클라우드서비스 제공자 안전성 평가 개요
2. 평가 절차 및 방법
3. 평가 항목 및 생략 기준

제4장 클라우드서비스 제공자 평가

「전자금융감독규정」〈별표 2의2〉에 따라 클라우드서비스 제공자를 평가하고, 그 결과에 따라 계약 추진 및 이용 여부를 최종 결정하여야 한다.

> **▶ 감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**
> ① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.
> 2. 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가(단, 제1호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 〈별표2의2〉의 평가항목 중 필수항목만 평가할 수 있다.

이때, 클라우드컴퓨팅서비스 제공자의 안전성 평가는 「전자금융감독규정」제14조의2제3항에 따라 침해사고대응기관이 수행한 평가 결과를 활용* 할 수 있다.

> **▶ 감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**
> ③ 금융회사 또는 전자금융업자는 제1항제2호의 평가를 직접 수행하거나 제37조의4제1항의 침해사고대응기관이 수행한 평가 결과를 활용할 수 있다.
>
> **▶ 감독규정 제37조의4(침해사고대응기관 지정 및 업무범위 등) 中**
> ③ 침해사고에 대응하기 위한 침해사고대응기관은 다음 각 호의 자로 한다.
> 1. 금융보안원

* 평가 결과 활용에 관한 지원사항은 금융보안원에 별도 문의 필요

또한, 고유식별정보 또는 개인신용정보를 처리하는 업무의 경우, 해당 정보를 처리하는 모든 시스템을 국내에 설치하여야 하고, 해당 전산실 내에 무선통신망이 설치되어있지 않아야 한다는 점을 고려하여 제공자를 선정한다.

▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**

⑧ 제1항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보처리시스템이 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다. 다만, 금융회사 또는 전자금융업자(전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자는 제외한다)가 **고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.**

▶ **정보처리시스템 국내 설치 예외**

- 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 감독규정 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자(국내 설치 요건 및 무선통신망 설치 금지 예외)

그리고, 금융회사는 클라우드서비스 제공자와 협의하여 클라우드서비스 안전성 평가 결과* 중 미흡한 사항을 개선·조치할 수 있도록 방안을 수립하여야 한다.

* 금융보안원 대표평가, 금융회사 자체평가

1 클라우드서비스 제공자 안전성 평가 개요

금융회사는 클라우드서비스를 이용하고자 하는 경우 감독규정 〈별표 2의2〉의 항목을 포함한 클라우드서비스 제공자의 안전성을 평가*해야 함

* 금융회사 필요 시 다양한 평가기법(인터뷰, 실사, 시연, 실증, 테스트 등)을 활용하여 평가 가능

가. 평가 절차 및 방법

- **(중요 업무)** 종합 평가(최초, 3년 주기) + 정기 평가(매년)
  - 종합 평가 : 현장점검
  - 정기 평가 : 매년 서면점검
- **(비중요 업무)** 종합 평가(최초, 3년 주기) + 정기 평가(매년)
  - 종합 평가 : 서면점검 가능
  - 정기 평가 : 매년 서면점검(단, 금융회사 판단하에 생략가능)

나. 평가 항목 및 평가 생략 기준

- **(평가 항목)** 필수 + 대체
- **(평가 생략 기준)** 비중요업무인 경우 '대체 항목' 생략이 가능하며, 중요업무인 경우 국내·외 클라우드 보안인증* 등을 취득·유지하고 있는 클라우드서비스 제공자에 대해 '대체 항목' 생략 가능

  * 본 부록「제2장 평가항목 및 평가 생략 기준」中 국내·외 인증제도 참조

다. 대표평가 활용 및 공유

- 클라우드서비스 제공자 안전성 평가의 주체는 기본적으로 금융회사이며, 감독규정(제14조2의제3항)에 의거 침해사고대응기관이 대표로 평가한 결과를 공유받아 활용 가능 (건전성 평가는 금융회사에서 직접 수행)
  - 침해사고대응기관은 금융회사들을 대표하여 평가를 진행할 수 있으며, 인력 및 예산 상황 등에 따라 지원 여부 및 일정을 조정할 수 있음

다만, 침해사고대응기관의 평가결과는 유효기간 내에서만 활용 가능

- 침해사고 대응기관의 평가결과의 기본 유효기간은 각 클라우드 서비스 제공자 별 평가결과 공유일로부터 다음 해 12월 31일까지 유효. 다만, 유효기간 내 차기 평가가 진행된 경우 기존 평가 결과의 유효기간은 차기 평가 결과 공유일까지 유효

▶ 침해사고 대응기관 평가결과 유효기간 적용 예시

예) 대표평가 결과 '22.9.30일 공유, 차년도 대표평가 결과 '23.9.20일 공유

1) '22년에 대표평가 결과를 활용하고, '23년도에는 자체평가 하는 경우
   : '22년도 평가 결과는 23.12.31일까지 유효, 다만, 금융회사 자체평가를 통해 평가 결과를 '23년 12월 말일까지 최신화 하여야 함
2) '22년에 대표평가 결과를 활용하고, '23년도에도 대표평가 결과를 활용하는 경우
   : '22년도 평가 결과는 '23.9.20일까지 유효하며, '23년도 대표평가 결과는 '24.12.31일 또는 차년도 평가 결과 공유일까지 활용 가능

2 평가 절차 및 방법

가. 종합 평가

(평가 시기) 금융회사가 특정 클라우드서비스를 최초 이용 시 또는 매 3년마다 종합 평가 실시

- 기존 이용 중인 클라우드서비스 제공자라도 아래의 경우 평가 실시
  - ① 이용 영역 변경·확대(예:SaaS→SaaS, IaaS) 시(신규 이용 영역 한정 평가)
  - ② 개정된 감독규정 시행('19.1.1.) 이전에 비중요정보의 처리를 위탁 중인 클라우드서비스 제공자에게 개인신용정보 등의 처리를 추가로 위탁한 경우
  - ③ 업무 중요도 평가 결과 중요도가 '비중요'에서 '중요'로 변경된 경우 등

(평가 절차 및 방법) ①(클라우드서비스 제공자) **자가점검 실시** → ②(금융회사) **결과 검증**(현장 또는 서면) → ③(금융회사) **확인평가**(미흡사항 보완 및 확인)

- (자가점검) 평가항목 별 증적이 포함된 자가점검 결과를 금융회사에 제출, 동일 평가항목에 대해 금융회사가 인정하는 보안인증 결과를 증적으로 활용 가능
- (결과검증) 중요 업무는 현장점검 실시, 그 외 업무는 서면점검 실시 가능
- (확인평가) 점검결과 나타난 미흡사항에 대한 조치여부를 확인(단, 미흡사항이 있는 경우에도 미흡사항에 대한 리스크 분석, 대체 보완 방안 마련 및 정보보호위원회 심의·의결 등이 있는 경우 금융회사의 결정에 따라 클라우드서비스 이용은 가능)

  ※ 결과 검증과 동일하게 평가하되, 단순·경미사항에 한해 서면(증적 확인)평가로도 수행 가능
- 다만, 아래의 경우 정보보호위원회 심의·의결을 거쳐 기존 평가 결과 활용 가능

  ※ 다만, 중요 업무 추가 위탁 시 기존 평가가 해당 수준(현장 평가 등)으로 이루어진 경우에 한함
  - ① 기존에 평가를 완료한 클라우드서비스와 동일한 범위 내에서 추가로 이용하는 경우
  - ② 침해사고대응기관의 대표평가 결과를 공유받은 경우

  ※ 다만, 공유받는 평가결과의 범위가 이용하고자 하는 범위와 일치하는 경우에 한함

나. 정기 평가

- **(평가 시기)** 클라우드서비스 제공자의 보안수준 유지 여부를 지속 검증하기 위해 종합평가 종료 後 매 1년 마다* 정기 평가 실시

  * 종합평가 완료 후 다음 해부터 매년 12월31일까지 수행

  - 클라우드서비스 제공자의 보안성에 중대한 변화* 등이 있는 경우 필요 시 평가 주기와 무관하게 정기 평가 실시 가능

    * 클라우드서비스 제공자의 보안사고 발생, 클라우드 IT인프라 전면 재구축 등

  - 비중요업무인 경우 정기 평가 생략 가능

- **(평가 절차 및 방법*)** ① (클라우드서비스 제공자) **자가점검 실시** → ② (금융회사) **결과 검증**(서면) → ③ (금융회사) **확인평가**(미흡사항 보완 및 확인)

  - 정기 평가는 서면점검이 원칙(단, 금융회사가 필요하다고 판단하는 경우 클라우드서비스 제공자와 협의를 거쳐 현장점검 수행 가능)
  - 침해사고대응기관의 대표평가의 결과로 정기 평가 대체 가능

3 평가 항목 및 생략기준

가. 필수 항목

- 금융회사 및 전자금융업자가 금융분야에서 요구하는 보안수준을 확보하기 위해 필수적으로 요구되는 사항을 평가
  - 국내·외 클라우드 보안인증 등의 취득 여부 및 중요, 비중요업무와 관계없이 반드시 평가 필요

    ※ 금융회사가 인정하는 보안인증 결과 또는 제3자 감사보고서에 동일 항목이 있는 경우 해당 결과를 증적자료로 활용 가능

나. 대체 항목

- 금융회사 및 전자금융업자가 업무수행에 필요한 최소한의 보안수준을 확보하기 위해 요구되는 사항을 평가
  - **(중요 업무)** 국내·외 클라우드 보안인증 등을 취득·유지하고 있는 클라우드 서비스 제공자에 대해서는 '대체 항목' 평가 생략 가능

    ※ 단, 금융회사가 사용하려는 물리적 시설(데이터 센터 등)과 서비스가 취득한 인증의 범위에 반드시 포함될 필요 (인증서 또는 인증기관이 발급한 서류에 관련 사실이 명시될 필요)

구분	인증제도명	선정사유
국내	클라우드 서비스 보안인증제(CSAP)	① 국가기관 또는 공신력 있는 전문 기관에서 주관 ② 다수 국내·외 사업자가 해당 인증 취득 ③ 평가항목이 본 제공기준과 상당수 유사
	ISMS-P (*)	
해외	FedRAMP(High)	
	CSA STAR Certification(Gold)	
	MTCS(Level 3)	
	ISO 27017 인증	
	SOC2 Type II (*)	

* 클라우드 특화 인증이 아닌 2개 인증(ISMS-P, SOC2 Type2)은 「가상화 보안에 관한 사항(감독규정 〈별표2의2〉 8.가상화 및 인프라보안)」 별도 점검 필요

  - **(비중요 업무)** 전자금융감독규정 제14조의2제1항제1호에 따라 비중요업무로 분류된 경우 '대체 항목' 평가 생략 가능

▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**

① 금융회사 또는 전자금융업자는「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.

2. 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가(단, 제1호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 〈별표2의2〉의 평가항목 중 필수항목만 평가할 수 있다.

⑧ 제1항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보처리시스템이 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다. 다만, 금융회사 또는 전자금융업자(전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자는 제외한다)가 **고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.**

▶ 감독규정 〈별표 2의2〉

금융분야 클라우드컴퓨팅서비스 제공기준(제14조의2 관련)

금융회사 또는 전자금융업자는 아래의 항목을 포함하여 클라우드서비스 제공자의 건전성 및 안전성을 평가하되, 제14조의2제1항제1호에 따라 비중요업무로 분류된 경우 또는 클라우드서비스 제공자가 국내·외의 클라우드서비스 관련 보안인증 등을 취득하여 유지 중임을 확인한 경우 대체 항목에 관한 평가는 생략할 수 있다.

구분		평가항목	항목	적용대상
1. 정보보호 정책 및 법규 준수	1.1 정보보호 정책	1.1.1. 조직 전반에 적용하고 있는 정보보호 정책 및 지침 또는 규정을 수립·시행하고 있는가?	대체	IaaS, PaaS, SaaS
		1.1.2. 정기적으로 정보보호정책의 타당성을 검토, 평가하여 수정, 보완하기위한 절차를 마련하고 이행하고 있는가?	대체	IaaS, PaaS, SaaS
	1.2 정보보호 조직	1.2.1 조직의 정보보호를 위한 전담조직을 구성하여 안전성 확보 및 이용자 보호 등 정보보호 활동을 효과적으로 수행하고 있는가?	대체	IaaS, PaaS, SaaS
		1.2.2 정보보안 및 정보자산과 관련된 모든 인력의 역할과 책임을 정의하고, 이용자의 정보보호 역할과 책임을 명확하게 정의하고 있는가?	대체	IaaS, PaaS, SaaS
	1.3 법 및 정책 준수	1.3.1 이용자가 법령 등 의무준수를 위해 필요한 사항을 지원 및 협조하도록 체계가 마련되어있는가?	필수	IaaS, PaaS, SaaS

구분		평가항목	항목	적용대상
	1.4 보안감사	1.4.1 접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되고, 비인가 된 접근 및 변조로부터 보호되고 있는가?	필수	IaaS, PaaS, SaaS
2. 인적보안	2.1 내부인력 보안	2.1.1 클라우드서비스의 시스템 운영, 개발, 보안 등에 관련된 모든 임직원을 주요 직무자로 지정하여 관리하고 있는가?	대체	IaaS, PaaS, SaaS
		2.1.2 권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위협을 줄이기 위하여 직무 분리 기준을 수립·적용하고 있는가?	대체	IaaS, PaaS, SaaS
		2.1.3 조직 내 인력의 인사 변경 발생시 지체없이 해당 사용자의 정보자산 반납, 접근 권한 변경 및 회수가 이루어 지고 있는가?	대체	IaaS, PaaS
	2.2 외부인력 보안	2.2.1 외부인력에 대한 보안요구사항 준수 여부를 주기적으로 점검하고 위반사항이나 침해사고 발생 시 적절한 조치를 수행하고 있는가?	대체	IaaS, PaaS
3. 위험평가 및 관리	3.1 자산 식별 및 분류	3.1.1 클라우드컴퓨팅서비스에 사용된 정보자산 (정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류 기준 수립하고 식별된 자산의 목록을 작성하여 관리하고 있는가?	대체	IaaS, PaaS, SaaS
	3.2 자산 변경관리	3.2.1 시스템 통합, 전환 및 재개발 시 클라우드 컴퓨팅 서비스 운영에 지장을 초래하지 않도록 통제절차를 마련하여 적용하고 있는가?	대체	IaaS, PaaS, SaaS
	3.3 위험관리	3.3.1 클라우드서비스를 제공하기 위한 핵심자산 및 서비스를 대상으로 주기적으로 취약점 점검을 수행하고, 발견된 위험에 대한 보완조치를 수행하고 있는가?	대체	IaaS, PaaS, SaaS
4. 서비스 공급망 관리	4.1 공급망 관리정책	4.1.1 공급망과 관련한 보안 요구사항을 정의하는 관리정책을 수립하고 이행하는가?	대체	IaaS, PaaS, SaaS

구분		평가항목	항목	적용대상
	4.2 공급망 변경관리	4.2.1 공급망 상에서 발생하는 모든 기록 및 보고서에 대해 정기적으로 모니터링 및 검토를 수행하는가?	대체	IaaS, PaaS
5. 업무연속성 계획 및 재해복구	5.1 장애대응	5.1.1 클라우드서비스가 중단되지 않도록 업무 지속성 확보방안을 수립하고 이행하는가?	대체	IaaS, PaaS, SaaS
		5.1.2 클라우드서비스 중단이나 피해가 발생한 경우 장애 보고 절차에 따라 장애상황을 기록하고 이용자에게 현황을 파악할 수 있도록 관련 정보를 제공하는가?	필수	IaaS, PaaS, SaaS
		5.1.3 클라우드서비스 중단이나 피해가 발생하는 경우, 재해복구목표시간 내 서비스의 장애를 처리하고 복구할 수 있는가?	대체	IaaS, PaaS, SaaS
	5.2 서비스 가용성	5.2.1 가상화 서버, 설비 등 정보처리설비의 장애로 인해 서비스가 중단되지 않도록 관련 설비를 이중화하고, 백업 체계를 마련하고 이행하는가?	필수	IaaS, PaaS, SaaS
		5.2.2 주기적으로 서비스 연속성(가용성) 확보를 위한 점검을 수행하고 있는가?	대체	IaaS, PaaS
6. 침해사고 대응 및 관리	6.1 침해사고 대응 절차 및 체계	6.1.1 해킹 등 전자적 침해행위로 인한 피해 발생 시 대응을 위한 침해사고 대응절차를 수립하고 이행하는가?	대체	IaaS, PaaS, SaaS
		6.1.2 침해사고 발생 시 신속한 대응이 가능하도록 주기적으로 침해사고 대응절차에 기반한 훈련을 실시하고 있는가?	대체	IaaS, PaaS, SaaS
		6.1.3 금융권 통합 보안관제수행을 위한 지원 체계가 마련되어 있는가?	필수	IaaS, PaaS
	6.2 침해사고 대응	6.2.1 침해사고 발생 시 침해사고 대응절차에 따라 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알리고 있는가?	필수	IaaS, PaaS, SaaS
7. 사용자 인증 및 접근통제	7.1 접근통제 정책	7.1.1 비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하고 이행하는가?	대체	IaaS, PaaS, SaaS

구분		평가항목	항목	적용대상
	7.2 접근권한 관리	7.2.1 클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 검토하고 있는가?	대체	IaaS, PaaS, SaaS
		7.2.2 이용자의 정보처리시스템과 관련된 단말기 및 전산자료에 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련하고 적용하고 있는가?	필수	IaaS, PaaS, SaaS
	7.3 사용자 식별 및 인증	7.3.1 이용자가 클라우드서비스 이용 시 추가 인증수단을 요청하는 경우 이를 제공하고 있는가?	대체	IaaS, PaaS, SaaS
		7.3.2 이용자의 안전한 클라우드서비스 이용을 위해 계정 및 패스워드 등의 관리절차 마련하고 안내하고 있는가?	대체	IaaS, PaaS, SaaS
8. 가상화 및 인프라 보안	8.1 가상화 보안	8.1.1 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하고 있는가?	대체	IaaS, PaaS, SaaS
		8.1.2 이용자가 클라우드서비스 이용 중 가상자원*을 삭제할 경우 삭제대상과 관련된 모든 자원이 복구되지 않는 방법으로 삭제되는가? * 가상머신(이미지,백업,스냅샷등),가상스토리지,가상소프트웨어,가상환경설정정보등	필수	IaaS, PaaS, SaaS
		8.1.3 가상자원에 대한 무결성을 보장하고 가상자원 손상 시 이용자에게 안내하고 있는가?	필수	IaaS, PaaS, SaaS
		8.1.4 하이퍼바이저 등 물리적/논리적 가상화 서버(기능) 및 인터페이스에 대한 보안관리 및 접근통제를 수행하고 있는가?	대체	IaaS, PaaS
		8.1.5 가상자원 관리 시스템*과 가상 소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 관리적, 물리적, 기술적 보호대책을 수립하고 이행하는가? * 가상자원을 제공하기 위한 웹사이트(클라우드 포탈, 클라우드 콘솔, API등)	필수	IaaS, PaaS, SaaS

구분		평가항목	항목	적용대상
	8.2 가상환경 보호	8.2.1 이용자의 가상환경 보호를 위한 악성코드 방지 대책을 수립하고 이행하는가?	대체	IaaS, PaaS, SaaS
	8.3 인프라 보안	8.3.1 클라우드서비스와 관련된 내외부 네트워크를 보호하기 위한 정보보호시스템을 설치하고 운영하고 있는가?	대체	IaaS, PaaS, SaaS
		8.3.2 업무, 서비스 등을 고려한 영역 간 네트워크를 분리하여 운영하고 있는가?	대체	IaaS, PaaS, SaaS
		8.3.3 이용자의 가상환경 보호 및 네트워크 분리를 위해 필요한 기능을 제공하는가?	필수	IaaS, PaaS
9. 개발 및 운영 보안	9.1 시스템 분석 및 설계	9.1.1 보안감사증적(로그)의 정확성을 보장하기 위해 표준시각으로 동기화하고 있는가?	대체	IaaS, PaaS, SaaS
	9.2 구현 및 시험	9.2.1 테스트 시 이용자 정보 사용을 금지(부하테스트 등의 불가피한 경우 이용자 정보 변환 사용 및 테스트 종료 즉시 삭제)하고 있는가?	대체	IaaS, PaaS, SaaS
10. 암호화 및 데이터 보호	10.1 데이터 보호	10.1.1 데이터 분류기준에 따라 데이터를 분류하고 관리하고 있는가?	대체	IaaS, PaaS, SaaS
		10.1.2 이용자의 데이터 소유권을 명확하게 확립하고 있는가?	대체	IaaS, PaaS, SaaS
		10.1.3 입•출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 보장하고 있는가?	대체	IaaS, PaaS, SaaS
		10.1.4 데이터에 대한 접근제어, 위•변조 방지 등 데이터 처리에 대한 보호기능을 이용자에게 제공하고 있는가?	대체	IaaS, PaaS, SaaS
		10.1.5 이용자의 데이터가 처리되는 위치를 추적하기 위한 방안을 제공하고 있는가?	대체	IaaS, PaaS, SaaS

구분		평가항목	항목	적용대상
		10.1.6 이용자의 클라우드서비스 이용 계약 종료 시 이용자의 모든 가상자원은 복구가 불가능하도록 삭제하고 있는가?	필수	IaaS, PaaS, SaaS
	10.2 암호화	10.2.1 이용자 데이터 처리 시 암호화를 적용하여 보호하고 있는가?	대체	IaaS, PaaS, SaaS
		10.2.2 암호키의 안전한 관리 절차를 수립하고 안전하게 보관하고 있는가?	대체	IaaS, PaaS, SaaS
11. 물리적 보안	11.1 물리적 보호구역	11.1.1 전산실 내 주요시설에 출입통제, 감시제어를 위한 설비가 마련되어 있는가?	필수	IaaS, PaaS
		11.1.2 고유식별정보 또는 개인신용정보 처리 시 전산실 내 무선통신망 사용을 제한(통제) 하고 있는가?	필수	IaaS, PaaS, SaaS
		11.1.3 사무실 및 설비 공간에 대한 물리적인 보호방안을 수립하고 적용하고 있는가?	대체	IaaS, PaaS
	11.2 정보처리 시설 및 장비보호	11.2.1 고유식별정보 또는 개인신용정보를 처리하는 모든 정보처리시스템을 국내에 설치하고 있는가?	필수	IaaS, PaaS, SaaS
		11.2.2 각 보안 구역의 중요도 및 특성에 따라 화재, 누수, 전력 이상 등 자연재해나 인재에 대비하여 화재감지기, 소화 설비, 누수 감지기, 항온 항습기, 무정전 전원장치(UPS), 이중 전원선 등의 설비를 갖추고 있는가?	필수	IaaS, PaaS
		11.2.3 정보처리시설 내 이용자 정보(자료)가 저장된 장비를 폐기하는 경우 복구가 불가능하도록 처리하고 있는가?	대체	IaaS, PaaS

FSI FINANCIAL SECURITY INSTITUTE
금융미래를 열어가는 금융보안파트너

금융분야 클라우드컴퓨팅서비스 이용 가이드

제 5 장

업무 연속성 계획 및 안전성 확보조치 방안 수립

1. 업무 연속성 계획 수립
2. 안전성 확보조치 방안 수립

제5장 업무 연속성 계획 및 안전성 확보조치 방안 수립

금융회사는 클라우드서비스에 대해 예상치 못한 재해 또는 사고 발생 시 업무 연속성에 미칠 수 있는 영향을 파악하고, 데이터 백업, 재해복구 및 침해 사고대응 훈련계획, 출구 전략 등을 포함한 업무 연속성 계획을 수립하고, 보안사고의 예방을 위한 안전성 확보조치 방안을 수립·이행하여야 함

▶ **감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中**

① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.

3. 클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획 및 안전성 확보조치의 수립·시행(단, 제1호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 〈별표 2의2〉 및 〈별표 2의4〉의 필수사항만 수립·시행할수 있다.)

⑤ 제4항에 따라 금융감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.

4. 제1항제3호에 따른 **업무 연속성 계획 및 안전성 확보조치에 관한 사항**
6. 〈별표 2의5〉의 계약서 주요 기재사항을 포함한 클라우드 컴퓨팅서비스 이용계약서

금융회사는 클라우드서비스 이용 시에도 전자금융감독규정의 요구사항을 모두 준수*하여야 하며, 업무 연속성 계획 및 안전성 확보조치 방안 마련 시 전자금융감독규정 〈별표 2의3〉, 〈별표 2의4〉, 〈별표2의5〉와 같은 규제 준수가 필요한 사항을 반드시 고려하여야 함

* 감독규정 제14조의2 제8항에 따른 예외 사항 제외

더불어, 클라우드컴퓨팅서비스 이용과 관련한 업무연속성 계획 및 안전성 확보조치의 수립·시행 시 중요업무로 판단된 경우 전자금융감독규정 〈별표 2의3〉, 〈별표 2의4〉, 〈별표 2의5〉에서 명시된 필수사항 및 추가사항을 모두 포함 하여야

하고, 비중요업무로 판단된 경우 필수사항을 포함하고 추가사항은 생략하여 수립·이행할 수 있음

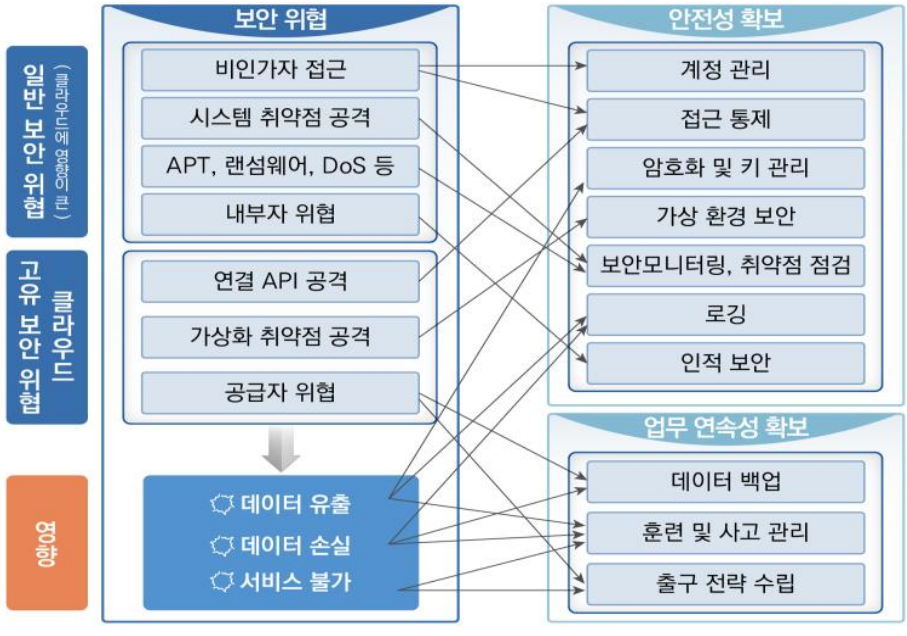
또한, 해당 가이드에서는 일반적인 클라우드서비스 이용 상황을 고려하여 법규상 요구되는 의무사항과 법규상 요구되지 않지만 추가로 고려할 사항을 포함하고 있으며, 이 가이드에 포함되지 않은 사항이라 할지라도 법규에서 요구하는 사항이 존재하는 경우, 클라우드서비스 이용 환경에서도 반드시 준수 하여야 함

※ 클라우드서비스 관련 보안 위협

- 일반적인 보안 위협 中 클라우드서비스 이용 시 영향이 큰 위협
  : 비인가자 접근, 시스템 취약점 공격, APT·랜섬웨어·DoS, 내부자 위협 등
- 클라우드서비스 고유의 보안 위협
  : 연결 API 공격(설정 오류, 접근통제 미비 등), 가상화 취약점 공격, 공급자 위협 등

⇨ 업무 연속성 계획 및 안전성 확보조치 방안 수립 시 적극 고려

〈그림3. 클라우드서비스 관련 보안 위협〉



참고 클라우드 서비스 관련 사고 사례

〈 클라우드 서비스 사고 사례 조사 〉

사고유형	발생연월	사고개요	발생원인	피해내역
데이터 유출	21.12	가상자산 플랫폼 H사 이용자 정보 유출	결제소프트웨어의 Log4Shell 취약점	개인정보, 비밀번호 등 200만명의 이용자 정보 유출
	21.12	네트워크 장비업체 B사의 정보 유출	내부 직원이 해커로 가장하여 정보 유출	내부 데이터 및 서명키 등이 유출
	21.10	C사의 내부 문서 및 데이터가 온라인 상에 노출	비인가자가 클라우드 데이터에 접근 가능하게 설정	클라우드 접속키, B사 소스코드 등이 유출
	21.07	클라우드 사업자에서 제공하는 데이터베이스의 취약점으로 정보 노출	권한상승 취약점을 통해 다른 클라우드 서비스 사용자의 DB접근 가능	이메일 주소 등 2억 5천만개의 데이터 유출
데이터 손실	22.04	D사 클라우드 기반 소프트웨어 제공 서비스 접속 불가	유지보수 작업 중 고객 사이트 삭제	고객 사이트 삭제 및 400여개의 고객 서비스 중지
	21.01	E사 정보유출 및 서비스 삭제	노출된 클라우드 서비스에서 접속정보 탈취	300만명의 개인정보 등을 유출한 후 클라우드 데이터 삭제
서비스 불가	22.03	F국가 지방자치단체 클라우드 시스템 스팸메일 발송	권한 설정 오류로 비인가자의 메일 발송 가능 상태로 운영	스팸메일 91만여건 발송
	21.07	G사 원격 관리 클라우드 서비스에서 랜섬웨어 배포	원격 관리 도구의 취약점으로 해킹	MSP 50여개의 고객 랜섬웨어 감염
	22.02	A사 클라우드 서울 데이터센터 20여분간 장애 발생	가상서버 인터넷 연결 문제	해당 클라우드 서비스 사용자의 접속 마비
	18.11	A사 클라우드 서울 리전(Resion) 접속 장애	엔지니어 내부 DNS 설정 오류	온라인 서비스업, 항공사, 금융사등의 서비스 중단

1 업무 연속성 계획 수립

1) 데이터 백업 등 장애 대비

가. 필수 사항

▶ 전자금융감독규정 요구사항

check

클라우드 환경에서도 모두 준수할 필요

- 비상시에 대비하여 보조기억매체 등 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운용할 것(제13조제1항제6호)
- 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것(제13조제1항제8호)
- 주요 백업 전산자료에 대하여 정기적으로 검증할 것(제13조제1항제9호)
- 정보처리시스템의 장애발생 시 장애일시, 장애내용 및 조치사항 등을 기록한 장애상황기록부를 상세하게 작성·보관할 것(제14조제3호)
- 시스템 통합, 전환 및 재개발 시 장애 등으로 인하여 정보처리시스템의 운영에 지장이 초래되지 않도록 통제 절차를 마련하여 준수할 것(제14조제5호)
- 중요도에 따라 정보처리시스템의 운영체계 및 설정내용 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1년 이상 기록·관리할 것(제14조제8호)
- 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것(제15조제2항제6호)
- 전산장애 발생 시 전산자료 손실에 대비한 백업(backup)장치를 구비할 것(제50조제1항제3호)

▶ 규정 준수 시 고려사항

- 기존과 동일한 백업장치 이용, 클라우드서비스 내 백업 서비스 이용, 타 클라우드서비스를 백업장치로 이용 등 다양한 데이터 백업 방법 활용 가능
- 통제 절차(제14조제5호) 마련을 위해 클라우드 전환, 클라우드서비스 상 재개발 과정에 대한 통제 절차가 포함될 필요

나. 추가 사항

- 클라우드서비스와 관련된 중요 설정파일, 가상 시스템 이미지 등을 데이터 백업에 포함

2) 이중화 또는 예비장치 확보 등

가. 필수 사항

▶ 전자금융감독규정 요구사항

check **클라우드 환경에서도 모두 준수할 필요**

- 금융회사 또는 전자금융업자는 제1항의 규정에 따른 업무지속성 확보대책의 실효성·적정성 등을 매년 1회 이상 점검하여 최신상태로 유지하고 관리하여야 한다.(제23조제3항)
- 금융회사 또는 전자금융업자는 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하여야 한다.(제23조제7항)

▶ 규정 준수 시 고려사항

- 이중화 또는 예비장치 확보는 ❶금융회사 내 주전산센터-클라우드 재해복구센터, ❷클라우드 내 주전산센터-금융회사 내 재해복구센터, ❸A클라우드 내 주전산센터-B클라우드 내 재해복구센터 등 다양한 구성 가능
- 동일 클라우드서비스 제공자 내 이중화 또는 재해복구센터를 구축·운용하고자 할 경우, 동시 장애 발생 가능성, 센터간 거리, 데이터의 국외 이전 가능 여부 등을 반드시 확인

나. 추가 사항

- 클라우드서비스 제공과 관련된 지리적 특성, 동시 장애 발생 가능성 등을 고려하여 중복 설계 및 구성

3) 훈련 및 사고 관리

가. 필수 사항

▶ 전자금융감독규정 요구사항

check

클라우드 환경에서도 모두 준수할 필요

- 금융회사 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 피해 발생 시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 한다.(제15조제4항)
- 악성코드 감염에 대비하여 복구 절차를 마련할 것(제16조제1항제3호)
- 금융회사 또는 전자금융업자는 악성코드 감염이 발견된 경우 악성코드 확산 및 피해를 최소화하기 위하여 필요한 조치를 신속하게 취하여야 한다.(제16조제2항)
- 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보방안을 수립·준수하여야 한다.(제23조제1항)
  1. 상황별 대응절차
  2. 백업 또는 재해복구센터를 활용한 재해복구계획
  3. 비상대응조직의 구성 및 운용
  4. 입력대행, 수작업 등의 조건 및 절차
  5. 모의훈련의 실시
  6. 유관기관 및 관련업체와의 비상연락체계 구축
  7. 보고 및 대외통보의 범위와 절차 등
- 제4항에 따른 행동매뉴얼 또는 제5항에 따른 비상대책에는 제1항의 규정에 따른 업무지속성 확보대책이 반영되어야 한다.(제23조제6항)
- 금융회사 또는 전자금융업자는 제23조제4항에 따른 행동매뉴얼 또는 같은 조 제5항에 따른 비상대책에 따라 연 1회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고하여야 한다. 이때, 제23조제10항에 따른 재해복구전환훈련을 포함하여 실시할 수 있다.(제24조제1항)
- 금융위원회는 금융분야의 비상대응능력을 강화하기 위하여 금융회사 또는 전자금융업자를 선별하여 금융분야 합동비상대응훈련을 실시할 수 있다.(제24조제2항)
- 금융위원회는 제2항의 규정에 따른 합동비상대응훈련을 실시할 때, 다음 각 호의 기관에게 지원을 요청할 수 있다.(제24조제3항)
  1. 「정부조직법」 제15조에 따른 "국가정보원(국가사이버안전센터)"
  2. 「경찰법」 제2조에 따른 "경찰청(사이버테러대응센터)"
  3. 침해사고대응기관
  4. 그밖에 비상대응훈련의 실효성 확보를 위하여 금융위원회가 필요하다고 인정하는 기관
- 금융회사 또는 전자금융업자는 제1항 및 제2항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.(제24조제4항)

▶ 규정 준수 시 고려사항

- 클라우드서비스를 이용하고 있다는 이유로 규정 상의 대책·훈련 등의 범위에서 해당 업무 또는 시스템이 제외되지 않도록 주의
- 훈련 및 사고관리 절차는 긴급한 상황이 클라우드서비스 사업자 영역에 발생하는 경우와 클라우드서비스 내 금융회사 정보처리시스템 영역에 발생하는 경우로 구분하여 마련할 필요

나. 추가 사항

- 훈련 및 사고관리 계획에 클라우드서비스 제공자의 역할, 책임, 비상연락망 등이 포함되도록 고려

다. 권고 사항

- 클라우드서비스 제공자에 협조를 얻어 합동훈련을 진행하고, 클라우드서비스 제공자의 자체 재해복구 훈련 계획 및 주기적인 훈련 실시 여부를 확인
- 중요도가 높은 시스템의 경우 해당 클라우드서비스 제공자와 침해사고대응기관 간 24시간 소통이 가능한 핫라인 구축
- 감독규정 제23조제9항에 따라 선정된 핵심업무 이외에 대해서도 클라우드서비스 제공자와 사전 협의 등을 거쳐 업무별 복구목표시간 및 복구목표시점을 결정

4) 비상대책 수립

가. 필수 사항

▶ 전자금융감독규정 요구사항

check

클라우드 환경에서도 모두 준수할 필요

- 금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립·운영할 것(제23조제5항)

나. 추가 사항

- 계약 변경, 파산 등과 같은 중대한 상황 발생에 대비한 공급 대체 방안, 업무 복구 가능성 식별 등 출구 전략 수립 고려

5) 출구전략 수립(참고)

가. 주요 고려사항

▶ 출구 전략의 구성

- 출구 전략이 필요한 상황을 정의하는 이행 지표와 이행 시 세부 절차를 정의하는 세부 이행 절차로 구성

▶ 출구 전략 이행 지표 수립 및 모니터링

- 출구 전략 이행이 필요한 상황을 사전에 정의하고, 해당 상황임을 판단할 수 있는 지표를 수립하고 모니터링
- 출구 전략이 이행될 경우 성공적인 출구 전략 이행을 평가할 수 있는 기준을 사전에 정의

  ※ (예) 서비스 제공 또는 규제 체제 준수에 부정적 영향을 미치지 않으며 서비스 제공의 연속성과 품질에 지장을 주지 않고 클라우드서비스 위탁 계약을 종료

▶ 출구 전략 이행 절차 정의

- 출구 전략 이행을 위한 관련 조직별 역할 및 책임을 사전에 정의
- 출구 전략에는 다음의 사항을 포함한 개별 정보처리시스템에 대한 세부 이행 절차와 이에 필요한 인적·물적 자원 및 예상 소요 시간을 정의
  - 출구 전략 이행 방법(이전, 대체, 재개발 등)
  - 대체 사업자 또는 솔루션
  - 기존 클라우드서비스 제공자 시스템에서 데이터를 복구할 수 없도록 파기하는 절차 및 방법
  - 업무 연속성을 유지하면서 기존 업무 및 데이터를 대체 시스템에 이전하는 절차 및 방법
  - 이전 시점 및 소요시간, 인력 및 비용

나. 기타 고려사항

- 중요도가 높은 정보처리시스템에 대해서는 세부 이행 절차가 원활하게 진행되지 않는 경우를 위한 대안 마련 등 보다 정밀한 계획을 수립하고, 출구 전략 이행이 용이한 구현 방식을 고려

> **※ (참고) 구현 방식에 따른 출구 전략 이행 용이성**
> - (IaaS) 컨테이너 방식 이용 시 출구 전략 이행이 용이, 클라우드서비스 제공자의 관리 서비스 등에 의존도가 높으면 이행 용이성이 떨어짐
> - (PaaS, SaaS) 클라우드서비스 제공자가 자체 인프라가 아닌 제3의 IaaS 제공자 인프라를 이용하여 서비스를 제공하는 경우 상대적으로 출구 전략 이행 용이

- 출구 전략 관련 훈련 및 이행을 위해 클라우드서비스 제공자의 지원을 충분히 받을 수 있도록 계약서에 관련 내용을 명시

  ※ 출구 전략 이행을 위해 필요한 계약서 명시사항은 「제7장 계약 체결」 참조

- 기업의 출구 전략은 운영 중단 등 관리할 수 없는 스트레스 상황*을 가정하여 문서화 및 테스트 수행

  * 제3자의 장애 또는 파산 등 계획되지 않고 갑작스럽게 발생하는 상황을 의미

  - 출구 전략에는 데이터 또는 서비스의 기업 내 복구나 백업 서비스 공급자에게 이전 등 운영 복원력을 유지하는 방법 포함
  - 기업은 비즈니스 연속성 및 출구 전략에 대해 실행 가능성이 변경될 수 있는 요소* 등을 고려하여 정기적으로 검토 수행

    * (예) 클라우드서비스제공자가 제공하는 가용영역(AZ) 또는 리전(Region)의 증가, 기업의 비즈니스 요구사항 변경, 대체 서비스 제공자의 출현, 데이터 및 애플리케이션 포팅 기술 개발 등

    ※ 영란은행은 운영 중단 사태 등에 대한 금융회사의 운영 복원력을 평가하기 위해 격년별로 시나리오 기반 스트레스(Stress) 테스트를 수행하고 그 결과를 공개

2 안전성 확보조치 방안 수립

1) 계정 관리

가. 필수 사항

▶ 전자금융감독규정 요구사항

check 클라우드 환경에서도 모두 준수할 필요

- 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것(제13조제1항제1호)
- 제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.(제13조제2항)
- 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것(제13조제1항제2호)
- 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것(제13조제1항제14호)
- 정보처리시스템의 운영체제 계정으로 로그인할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것(제14조제9호)
- 정보처리시스템 운영체제 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링체계를 수립하고, 이상 징후 발생 시 필요한 통제 조치를 즉시 시행할 것(제14조제10호)
- 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것(제17조제1항제2호)

▶ 규정 준수 시 고려사항

- 클라우드서비스 내 정보처리시스템에 접근하는 계정뿐만 아니라 클라우드서비스 관리자·이용자 계정(관리 콘솔* 접근 계정)도 계정 관리 대상에 포함

* 금융회사가 클라우드서비스 내의 자원을 관리하기 위해 사용하는 도구 및 사이트 등

- 계정의 등록·변경·폐기 관련 로그 관리 시 클라우드서비스 내 계정 감사, 활동 내역 추적 기능 등 활용 가능
- 클라우드서비스 내에서 운영되는 정보처리시스템 운영체제 계정, 관리 콘솔 접근 주요 계정 및 공개용 웹서버 접근 계정에도 추가 인증수단이 요구되며, 클라우드서비스에서 제공하는 멀티팩터 로그인 방식 등 활용 가능
  - 특별 권한 계정에 대해서는 하드웨어 멀티팩터 인증 기기 등을 사용하여 관리

나. 추가 사항

- 클라우드 관리 콘솔에 접근하는 관리자 계정에 대한 이중인증 등 강화된 보안 조치 적용

다. 권고 사항

- 클라우드서비스 이용에 있어 각 사용자의 기능과 역할에 따라 그룹을 구분하고, 그룹별로 적절한 권한을 할당하여 관리
  - 클라우드서비스 내 계정 관리 설정에 대한 금융회사 내부정책을 수립하고 계정별 권한 관리 매트릭스를 작성하여 시스템에 적용
  - 최고 권한 계정 사용은 최소화할 수 있도록 조치(접근키 삭제 등)
  - 계정에 부여하는 역할과 권한을 업무에 필요한 최소한의 범위로 제한

〈그룹 구분 예시〉

그룹	권한
보안 관리자	보안 그룹 및 규칙 생성/수정/삭제
개발자	개발 인스턴스 시작/중지/종료 권한
운영자	프로덕션 시작/중지/종료 권한
계정 관리자	사용자 추가/삭제

- 클라우드 이용 관련 계정들의 권한 관리, 클라우드 시스템 자원 추가/수정/삭제, 주요 자원/API 접근 등 특별 권한이 있는 계정을 식별하여 집중 관리하고, 비인가된 계정의 생성, 비인가자의 계정 사용 등을 모니터링

  ※ (집중 관리 예시) 사용 이력·접근 기록 로깅 및 주기적 검토, 멀티팩터 인증, 주기적 재인증, 설정 변경 요청·승인 절차 공식화, 특권 계정 관리자와 일반 사용자 계정 관리자 분리 등

- 클라우드서비스 이용 계정별로 필요한 컴퓨팅 파워, 저장 공간, 소프트웨어 라이센스 등을 고려한 비용 계획을 마련

  - 각 계정별로 비용 지출 상한선을 지정하여 이를 초과하는 경우 사용이 제한되거나 별도의 소명을 거쳐 계속 사용될 수 있도록 조치
  - 비인가자의 클라우드서비스 이용 등으로 인해 과다한 비용이 발생하지 않도록 모니터링

    ※ 클라우드서비스 내 비용 관리 기능, 사용량 보고서 등을 활용하여 추적 가능하며, 비용 관련 지표를 설정하여 추적·관리하고, 설정된 예산 금액을 초과할 경우 알림을 받을 수 있도록 설정

2) 접근 통제

가. 필수 사항

▶ 전자금융감독규정 요구사항

check 클라우드 환경에서도 모두 준수할 필요

- 전산자료의 보유 현황을 관리하고 책임자를 지정·운영할 것(제13조제1항제3호)
- 전산자료 및 전산장비의 반출·반입을 통제할 것(제13조제1항제5호)
- 정보처리시스템 접속 시 5회 이내의 범위에서 미리 정한 횟수 이상의 접속 오류가 발생하는 경우 정보처리시스템의 사용을 제한할 것(제13조제1항제12호)
- 금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용하여야 한다. 다만, 정보처리시스템 관리자의 주요 업무 관련 행위는 책임자가 제28조제2항에 따라 이중확인 및 모니터링을 하여야 한다.(제13조제5항)
- 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것(제32조제1호)
- 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 변경할 것(제32조제2호가)
- 시스템마다 관리자 비밀번호를 다르게 부여할 것(제32조제2호다)
- 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것(제32조제3호)

▶ 규정 준수 시 고려사항

- 클라우드서비스 내 정보처리시스템 접근 계정 및 처리되는 전산자료 뿐만 아니라 클라우드 관리 콘솔 접근 계정 및 처리되는 전산자료도 접근 권한을 적절하게 통제
- 클라우드 관리 콘솔 접근 계정 비밀번호에 대해서도 비밀번호 규칙을 준수하고, 관리 콘솔 접속 오류가 다수 발생하는 경우 사용을 제한

나. 추가 사항

- 클라우드시스템 접근 절차를 문서화하고 관리 콘솔 관리자 계정의 경우 별도로 분리된 단말에서만 접근하도록 조치

다. 권고 사항

- 클라우드시스템에 접근하는 모든 절차와 경로가 일관된 방식으로 통제될 수 있도록, 관련 절차를 문서화하여 정기적으로 검토
  - 특별 권한이 있는 계정은 금융회사 내 별도로 분리된 단말기에서만 접근 가능하도록 함
  - 시스템 접근에 접근키가 사용될 경우 접근키에 대한 관리 방안을 수립
  - 클라우드시스템 관리 등을 위해 클라우드서비스 제공자가 금융회사 시스템 또는 소프트웨어에 접근할 가능성이 있는 경우 클라우드서비스 제공자의 해당 접근을 모두 기록하고 이를 주기적으로 검토
- 클라우드시스템을 통해 송수신되는 모든 정보에 대해서는 가능한 범위에서 기존의 금융회사 데이터 관리 및 통제 원칙을 적용
  - 특히, 클라우드 시스템 간의 접속 및 정보 송수신에 대해서도 외부시스템과 동일하게 통제를 적용하는 등 제로트러스트 모델(Zero Trust Model)*을 지향하여 설계

    * 내·외부 자원 모두 잠재적으로 악성 요인이 있음을 간주하고, 각 시스템이 모든 접근을 검증하도록 하는 모델
  - 필요 시, 클라우드 환경에서의 데이터 보안 및 관리 가시성 확보, 위협 탐지 및 접근 통제 등을 보조하는 솔루션 도입 등을 검토
- 클라우드 환경 접근 통제 설정 방법에 대해 클라우드서비스 제공자와 충분히 논의하여 설정 오류*를 통한 정보 유출 등에 유의

  * 클라우드 환경에서 이용 중인 데이터베이스 설정 오류로 인한 정보 유출 사고 다수 발생

  ※ (예시) 각 이용자에 역할에 맞는 세부 접근 정책 부여, 모든 자원에 대한 기본 접근 권한 삭제, 클라우드서비스 제공자 또는 제3자의 설정 오류 탐지 솔루션 및 데이터 손실 방지 솔루션 활용, 특권 계정의 오용을 방지하기 위해 클라우드서비스 제공자가 제공하는 설정 모범 사례 활용

참고 접근통제 및 네트워크 정보보호 요구사항(출처: KISA 클라우드 정보보호 안내서)

접속 관리 및 제한	① 서비스 연결은 승인하기 전에 모든 사용자(또는 단말기)의 접속은 정책에서 규정된 절차에 따라 인증하고, 접속로그를 관리하며 모니터링을 해야 한다. • 인증 시 사용하는 패스워드 조합 규칙 준용 – 세 가지 종류 이상의 문자구성으로 8자리 이상의 길이로 구성된 문자열 – 두 가지 종류 이상의 문자구성으로 10자리 이상의 길이로 구성된 문자열 • 로그인 횟수제한(5회), 잠김해제(120초) 준용 • 하나의 사용자가 동시에 여러 세션을 소유하는 것을 제한 ② 통신 세션의 기밀성을 보장하기 위해 안전한 암호 기술을 적용한다. • 통신세션 기밀성은 SSL/TLS, VPN 등 안전한 보호기술 적용 ③ 내부정책에서 제한하는 모바일 단말기의 통제 대책을 마련한다.
계정 분할 및 권한 최소화	① 서로 다른 이용자 계정의 충돌을 최소화하기 위하여 접근을 허용하는 영역이나 권한 등을 분리한다. ② 사용자에 부여하는 역할·권한을 최소한의 범위로 제한해야 한다. ③ 정책서의 계정관리 주기에 따라 점검 및 이용자 변경 사항은 즉시 정책에 반영한다.
네트워크	① 네트워크 접근통제를 H/W 형태, S/W 형태, API 형태 중 어떤 것을 선택할 것인지 고려해야 한다. ※ 클라우드서비스 업체에서 제공하는 방식에 대해 확인필요 • H/W 형태: 기존 온프레미스 환경과 동일 • S/W 형태: 서버에 접근통제 솔루션을 설치하는 방식으로 여러 대를 설치해야 할 수 있음 • API 형태: 기존의 네트워크 솔루션 기반의 접근통제 방식과는 다른 개념으로 성능 및 네트워크와 무관하게 원하는 방식으로 그룹을 묶어서 접근통제 가능 ② 네트워크 트래픽 도청이나 데이터 유출 방지를 위해 통신 암호화를 적용하여 관리한다. ③ 사용자의 네트워크 접속·인증을 위한 신분확인 메커니즘을 도입한다. ④ 네트워크 가용성이 침해하는 서비스거부공격(DoS)에 대한 대책을 마련한다. ⑤ 이(異)기종 네트워크의 연동에 따른 보안대책을 고려한다. ⑥ 네트워크 장애에 대비하여 네트워크 분할 또는 이중화하여 관리한다. ⑦ 네트워크 장애에 대비하여 보안관제 체계 구축을 고려한다.

3) 네트워크 보안

가. 필수 사항

▶ 전자금융감독규정 요구사항

check

클라우드 환경에서도 모두 준수할 필요

- 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지할 것. 다만, 다음 각목의 경우에는 그러하지 아니하다. (제15조제1항제3호)
  - 가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우 (단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용한 경우에 한한다
  - 나. 업무 특성상 분리하기 어려운 경우로서 금융감독원장이 인정하는 경우
- 규정 제15조제1항제3호에서 금융감독원장의 확인을 받은 경우란 다음 각호와 같다. (시행세칙 2조의2제1항)
  1. 내부통신망에 연결된 단말기가 업무상 필수적으로 외부기관과 연결해야 하는 경우 (다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다.)
  2. 규정 제12조의 보안대책을 적용한 단말기에서 전용회선과 동등한 보안수준을 갖춘 통신망을 이용하여 외부망으로부터 내부 업무용시스템으로 원격접속 하는 경우
- 무선통신망 이용 업무는 최소한으로 국한하고 정보보호최고책임자의 승인을 받아 사전에 지정할 것(제15조제6항제1호)
- 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(DMZ구간)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것(제17조제1항제1호)
- 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다.(제18조)
  1. 내부통신망에서 사용하는 IP주소의 경우 사설 IP주소 사용 등으로 보안을 강화하며 내부 IP주소체계의 외부유출을 금지할 것
  2. 개인별로 내부 IP주소를 부여하여 유지·관리할 것
  3. 내부 IP주소 및 외부 IP주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관할 것
  4. 정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP주소를 사용할 것. 다만, 외부직원 등과의 공동작업 수행 등 네트워크의 분리가 어렵다고 금융감독원장이 정하는 경우에는 업무특성별로 접근권한을 분리하여 IP주소를 사용할 수 있다.
  5. 내부통신망은 다른 기관 내부통신망과 분리하여 사용할 것

▶ 규정 준수 시 고려사항

- 클라우드서비스 내 네트워크 분리 기능(Virtual Private Cloud, Virtual Network 등) 등을 활용하여 사설 IP 주소를 부여하고, 외부통신망과 분리 차단하여 논리적 망분리를 구현
- 공개용 웹서버는 내부 업무용시스템을 위해 구축한 클라우드 네트워크 영역과 별도로 독립된 클라우드 네트워크 영역을 이용하여 구축(이 때, 동일 가상 사설 클라우드 내에 별도 컨테이너로만 구분된 경우 논리적으로 분리되었다고 판단될 수 없음)
- 서버·DB 등에 대해 Public 권한 사용 금지를 기본 원칙으로 하고, 필요 시 관리자 승인 등의 절차를 갖추도록 하여 과실로 인한 정보 유출 방지
- 무선통신망에 대한 사용자 인증, 암호화, 차단시스템 구축(제15조제6항제2~4호) 등은 클라우드서비스 제공자 평가 결과*로 판단 가능

  * 클라우드서비스 제공자 안전성 평가 결과 해당 제공자가 데이터센터 내에 무선통신망을 이용 중인 경우 고유식별정보 또는 개인신용정보 처리 불가(제14조의2제8항)

나. 추가 사항

- 시스템간 연계 및 클라우드 서비스 내 주요 통신 채널에 대한 암호화 적용

다. 권고 사항

- 모든 가상 프라이빗 클라우드가 기본적으로 모든 트래픽을 차단하도록 기본 보안 그룹을 설정하고, 최소 접근 권한 원칙을 사용
- 원격 서버 관리 포트, SSH 접근 포트에 대한 수신을 기본적으로 차단하고 업무에 필요한 IP만 제한적으로 허용

4) 금융회사 내부시스템과 클라우드 시스템 연계

가. 필수 사항

▶ 전자금융감독규정 요구사항

check 클라우드 환경에서도 모두 준수할 필요

- 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치할 것(제12조제1호)
- 정보유출, 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 및 휴대용 전산장비에 접근하는 것을 통제할 것(제12조제4호)
- 전산실 내에 위치한 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것. 다만, 다음 각목의 경우에는 그러하지 아니하다.(제15조제1항제5호)
  - 가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용한 경우에 한한다)
  - 나. 업무 특성상 분리하기 어려운 경우로서 금융감독원장이 인정하는 경우
- 전화 등 거래수단 성격 상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 사용할 것(다만, 전용선을 사용하는 경우로서 자체 보안성심의를 실시한 경우는 제외)(제34조제1호)
- 금융회사와 전자금융보조업자 간의 접속은 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다)을 사용할 것(제60조제1항제5호)
- 전자금융업무의 처리를 위하여 클라우드 내 정보처리시스템과 데이터 송수신이 불가피한 정보처리시스템의 경우, 필요한 서비스번호(port)에 한하여 연결 가능 (시행세칙 제2조의2제2항제2호)
- 자체 위험성 평가를 실시하고, 감독규정 시행세칙 〈별표7〉에서 정한 망분리 대체 정보보호 통제를 적용하고 정보보호위원회 승인 후 이용할 것(시행세칙 제2조의2제3항)

▶ 규정 준수 시 고려사항

- 클라우드서비스 내 정보처리시스템에 접근하거나 클라우드 관리 콘솔에 접근하는 금융회사 단말기에 대해서도 단말기 보호대책(제12조)을 준수

- 금융회사와 클라우드 시스템 간 연결 구간에 침입차단시스템 등 정보보호시스템 통제를 적용하여 필요한 서비스포트의 접근만 허용하고 그 외의 서비스는 차단
- 접속 로그를 주기적으로 분석, 수시로 보안도구를 이용한 정보통신망 취약성 점검

〈 감독규정 해설서 p.57 中 〉

▶ **외부기관과 내부통신망 연결시 유의사항(제3호, 제5호)**

- 업무 특성상 내부통신망과 외부통신망의 연결이 불가피한 경우 침입차단시스템 등 정보보호 시스템의 통제에 의해 필요한 서비스포트의 접근만 허용하고 그 외의 서비스는 차단하여 외부 통신망에서 내부통신망으로 인가되지 않은 접근을 통제
- 외부통신망 연결에 따른 보안취약성 해소를 위하여 접속 로그를 주기적으로 분석하고 수시로 보안 도구를 이용한 정보통신망의 취약성을 점검

※ 관련 상세내용은 감독규정 시행세칙 [별표 7] 망분리 대체 정보보호통제 내용 참고

나. 추가 사항

- 내부시스템과 클라우드 시스템 간 연계되는 데이터의 식별 및 관리 필요

다. 권고 사항

- 클라우드 관리 콘솔 접근 가능 IP, 단말기 및 업무 담당자를 지정하여 관리
- 해당 단말에서 다른 사이트 접근을 차단하고 다른 목적으로의 사용을 금지
- 해당 단말에서 클라우드 관리 콘솔 로그인 시 지정된 계정 이외의 계정(개인 계정 등)으로 로그인할 수 없도록 관리
- 규정에서 요구하는 영역 이외에도 모든 통신 채널 암호화를 적용하고, 지정된 중요단말기 로그인 시 멀티팩터 인증을 실시
- 외부망 접근을 통한 중요 업무 수행 시 사전 승인 및 통제 절차 실시

참고 비조치의견서

: 재택근무시 퍼블릭클라우드 VDI 활용에 관한 비조치의견서 요청서 (210052, `21.10.20.)

※ 비조치의견서는 신청자의 특정 행위에 대한 의견으로서 일반적 효력을 가지지 않음에 유의

〈 요청 대상 행위 〉

□ 재택근무용으로 퍼블릭 클라우드에 VDI를 구축할 경우, 퍼블릭 클라우드 內 원격접속 전용 VDI(ex: MS Azure VDI 등)를 사내공개망의 VDI와 동일하게 사내망에 속하는 업무용 단말기(규정 제15조제1항제3호 적용 대상)로 볼 수 있는지 여부

〈 판단 〉

□ 퍼블릭 클라우드 內 원격접속 전용 VDI는 업무용 단말기로 볼 수 있습니다.

〈 판단이유 〉

□ '21.1.1. 「전자금융감독규정시행세칙」이 개정·시행되어, 금융회사 임직원의 업무용 단말기에서 전용회선과 동등한 보안수준을 갖춘 통신망을 이용하여 내부 업무용시스템으로 원격접속이 가능해졌습니다.

◦ 내부망에 접근하는 방식은 회사가 자유롭게 선택할 수 있으며, VDI(Virtual Desktop Infrastructure)를 통한 간접접속 방식으로 인터넷 클라우드 기반의 VDI서비스 활용도 가능합니다.(재택근무안내서 2p)

□ 인터넷 클라우드 기반의 VDI서비스를 이용할 경우,

◦ 금융회사 임직원은 동 VDI의 가상 업무용 단말기를 경유하여 내부 업무용시스템에 접속하기 때문에, 동 VDI의 가상 업무용 단말기는 「전자금융감독규정」 제15조제1항제3호 적용 대상이라고 판단됩니다.

: 프라이빗 클라우드 서버 환경으로 구축시 운영계와 개발계(검증 포함)를 물리적으로 분리해야 하는지 (200036, `20.5.14.)

※ 비조치의견서는 신청자의 특정 행위에 대한 의견으로서 일반적 효력을 가지지 않음에 유의

〈 요청 대상 행위 〉

□ 서버 가상화를 이용하여 운영용 서버와 개발·검증용 서버를 분리구성하고, 네트워크 가상화를 이용하여 운영망과 개발·검증망을 분리하여 사용하는 것이 전자금융감독규정 제15조제1항제5호 및 제18조제4호를 위배하는지 여부

〈 판단 〉

□ 요청 행위는 전자금융감독규정 제15조제1항제5호 및 제18조제4호를 위배하지 않는 것으로 판단됩니다.

〈 판단이유 〉

□ 금융회사는 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 하며(전자금융감독규정 제15조 제1항 제5호)

◦ 정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP 주소를 사용하여야 합니다. (전자금융감독규정 제18조제4호)

□ 동 조항에서는 정보처리시스템을 인터넷 등 외부통신망으로 물리적으로 분리하도록 하고 전산센터 직원 및 외부직원간의 네트워크를 분리하도록 정하고 있으나 전산실 내 정보처리시스템간 연결에 대해서는 별도로 정하고 있지 않은 바,

◦ 귀사에서 문의하신 서버 가상화를 이용하여 운영용 서버와 개발·검증용 서버를 분리구성하고, 네트워크 가상화 기술을 이용하여 운영망과 개발·검증망을 분리하여 사용하는 것은 전자금융감독규정 제15조제1항 제5호 및 제18조제4호를 위배하지 않는 것으로 판단됩니다.

5) 암호화 및 키 관리

가. 필수 사항

▶ 전자금융감독규정 요구사항

check

클라우드 환경에서도 모두 준수할 필요

- 금융회사 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하여야 한다.(제31조제1항)
- 금융회사 또는 전자금융업자는 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.(제31조제2항)
- 비밀번호는 다음 각 목의 사항을 준수할 것(제32조제2호)
  - 가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 변경
  - 나. 비밀번호 보관 시 암호화
  - 다. 시스템마다 관리자 비밀번호를 다르게 부여
- 금융회사 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록 하여야 한다. 다만 비밀번호의 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리 하여야 한다.(제33조제1항)
- 개인정보보호법·신용정보보호법·정보통신망법 등에 따른 중요정보의 저장 및 송수신 시 암호화 조치

▶ 규정 준수 시 고려사항

- 암호 및 인증시스템에 적용되는 키는 금융회사 내부 시스템, 클라우드서비스 제공자의 보안네트워크 서비스 등 접근이 통제된 보안네트워크에 저장
  - 클라우드서비스 제공자의 직원이나 동일 클라우드서비스를 이용하는 외부 기관이 접근할 수 없도록 안전하게 관리되어야 함

나. 추가 사항

- 클라우드서비스 제공자 등 외부자의 키 접근 가능성을 고려하여 키의 수명 주기별 보안관리 방안 수립

다. 권고 사항

- 암호화 키의 안전한 생성 및 관리를 위해 HSM(Hardware Security Modules) 이용을 권장
- 중요한 가상머신에 대해서는 고객 관리 키로 암호화

〈암호화 관련 참고 규정〉

▶ 고유식별정보 암호화(개인정보보호법)

제24조(고유식별정보의 처리 제한) ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

제24조의2(주민등록번호 처리의 제한) ② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

▶ 개인신용정보 암호화(신용정보의 이용 및 보호에 관한 법률)

제17조(처리의 위탁) ④ 신용정보회사등은 제2항에 따라 신용정보의 처리를 위탁하기 위하여 수탁자에게 개인신용정보를 제공하는 경우 특정 신용정보주체를 식별할 수 있는 정보는 대통령령으로 정하는 바에 따라 암호화 등의 보호 조치를 하여야 한다.

▶ 개인정보의 기술적·관리적 보호조치 기준

제1조(목적) ① 이 기준은 「개인정보 보호법」(이하 "법"이라 한다)제29조 및 같은 법 시행령 제48조의2제3항에 따라 정보통신서비스제공자등(법 제39조의14에 따라 준용되는 자를 포함한다. 이하 같다)이 이용자의 개인정보를 처리함에 있어서 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성 확보를 위하여 필요한 기술적·관리적 보호조치의 최소한의 기준을 정하는 것을 목적으로 한다.

제6조(개인정보의 암호화) ① 정보통신서비스 제공자 등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

② 정보통신서비스 제공자등은 다음 각호의 정보에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.

1. 주민등록번호 2. 여권번호 3. 운전면허번호 4. 외국인등록번호 5. 신용카드번호 6. 계좌번호 7. 바이오정보

③ 정보통신서비스 제공자등은 정보통신망을 통해이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer)인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

④ 정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.

6) 로깅

가. 필수 사항

▶ 전자금융감독규정 요구사항

check **클라우드 환경에서도 모두 준수할 필요**

- 정보처리시스템의 가동기록은 1년 이상 보존할 것(제13조제1항제11호)
- 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공 여부와 상관없이 자동으로 기록·유지되어야 한다.(제13조제4항)
  1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
  2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록
  3. 정보처리시스템내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록
- 내부 IP주소 및 외부 IP주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관할 것(제18조제3호)
- 금융회사 또는 전자금융업자는 정보처리시스템의 장애예방 및 성능 최적화를 위해 정보처리시스템의 사용 현황 및 추이 분석 등을 정기적으로 실시하여야 한다.(제25조)

▶ 규정 준수 시 고려사항

클라우드서비스 내 정보처리시스템, 관련 설정 내용 및 처리되는 전산자료에 대해 로그* 관리를 실시할 필요

* 클라우드서비스 내 정보처리시스템 및 전산자료 뿐만 아니라 클라우드 관리 콘솔 및 각 인스턴스도 정보처리시스템 및 전산자료에 포함될 수 있으므로 이와 관련하여 규정에서 요구되는 접근기록 등을 관리할 필요

금융회사가 기존에 이용 중인 로깅 방식과 클라우드서비스에서 제공하는 로깅 기능을 모두 활용 가능하며, 규정 준수가 가능한 범위에서 유리한 방식 활용

- 클라우드서비스에서 제공하는 로깅 기능 활용 시 모든 이용중인 서비스 및 이용자에 대한 로깅 기능을 활성화하고, 로그 보존 기간을 1년 이상으로 설정

- 로그 데이터에 대해서도 관련 법령 및 내부 보안정책 등에 따라 암호화, 접근통제 등의 적절한 보호조치 적용 필요
  - 특히, 로그를 클라우드서비스 내에 저장할 경우 로그가 저장된 영역에 외부에서 접근할 수 없도록 접근통제 및 암호화 설정

나. 추가 사항

- 클라우드 관리 콘솔 관리자 등 주요 계정에 대한 활동 내역 로깅 및 주기적 검토

다. 권고 사항

- 로그 기록은 추후 사고 발생 시 조사(포렌식 조사 포함) 및 대응이 가능하도록 시간, 이용자, 주요 행위 등을 필수적으로 포함하여 구체적으로 기록
  - 아울러, 로그에 빠른 접근 및 검색이 가능하도록 하고, 로그 접근 내역을 추적하고 보존 기간을 철저히 준수하도록 관리
  - 특히 클라우드서비스 관련 설정내용 및 클라우드서비스 제공자 측 기록에 대해 추후 사고 발생 시 수집·조사방법 등을 사전에 확인
- 클라우드서비스 내 모든 이용 중인 서비스 및 이용자에 대한 로깅 기능을 활성화하여, 이용 일시, 이용자 ID 및 접속 IP, 이용 내용 등을 기록
- 클라우드서비스의 특성상 쉽게 발생할 수 있는 시스템 및 네트워크 구성의 변경, 시스템 자원의 변경 등*을 확인할 수 있는 로그를 함께 기록·유지할 필요

  * (예) 계정·권한·보안그룹 관리(생성/변경/삭제), 가상 프라이빗 클라우드 네트워크 정책 관리, 저장소 관리, 저장소 접근 및 데이터 읽기/쓰기 등
- 보안 로그, 중요 시스템 및 관리자 이용 로그 등 중요 로그는 독립적인 시스템에 보관하거나 클라우드서비스 내 로그 파일 유효성 검사 기능을 활용하는 등 무결성이 보장될 수 있도록 관리하고, 자동화 도구 등을 활용하여 주기적으로 검토

7) 가상 환경 보안

가. 추가 사항

- 가상 이미지 템플릿을 최신 상태로 유지하고, 이미지 무결성 등 보안사항을 주기적으로 점검

나. 권고 사항

- 클라우드서비스 하드웨어, 가상 이미지, 가상화 관리 소프트웨어(하이퍼바이저 등)에 대한 위협요인을 고려한 보안관리 활동을 수행 및 가상 네트워크, 컨테이너 등 활용 시 표준 이미지, 표준 보안 설정, 생성/변경/회수 등에 대한 관리 방안을 수립하여 준수

참고 **서버 및 가상화 보안 정보보호 요구사항(출처: KISA 클라우드 정보보호 안내서)**

공통	① 바이러스, 웜, 트로이목마 등의 악성코드 예방을 위해 서버 및 가상환경을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 적용한다. 특히, 가상환경의 경우 이상 징후 발견 시 사용 중지 및 격리 조치를 수행할 수 있는 체계를 갖추고 운영한다.
가상화 보안	① 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립한다. ② 가상자원에 대한 무결성 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 한다. ③ 호스트 OS 및 하이퍼바이저를 모니터링 하고 악성코드 감염예방을 위해 주기적인 보안 패치를 시행한다. ④ 가상화 실행 이력은 스냅샷 등 이미지 형태로 저장·관리하는 방안 등 안전한 저장 방법으로 관리한다. ⑤ 가상화 OS의 내·외부 데이터 이용에 대한 로그 정보를 관리한다. ⑥ 가상머신별 자원 사용량 제한하여 특정 가상머신의 자원이 남용되지 않도록 한다. ⑦ 호스트와 가상영역 간의 경계를 명확히 구분하고 운영한다.
서버 보안	① 클라우드서비스 운영 시 시스템에 대해 기술적 보호대책을 수립하고 적용한다. • 웹서버, DB서버, 클라우드 인프라 관리서버 등 운영 시 다음의 보호대책 적용 – 송·수신 시 SSL/TLS 통신 적용, 불필요한 서비스 및 포트 차단 – 접근권한 설정, 백신설치 및 OS 최신 패치 – 불필요한 소프트웨어, 스크립트, 실행파일 등 설치 금지 – 불필요한 페이지(테스트페이지) 및 에러처리 미흡에 따른 시스템 정보 노출 방지 – 주기적인 보안패치 및 취약점 점검 실시 등 ② 공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호한다. ※ 보안솔루션 구축 시 고려사항 기존 IT환경에서는 일반적으로 H/W 형태 보안솔루션(Firewall, IPS, IDS, Web Application firewall 등)을 구축하지만, 가상환경에서는 유연한 확장성을 고려하여 S/W 방식으로 구축하는 것이 일반적이다. 따라서 확장성이 반드시 보장되어야 한다면 호스트 기반의 보안솔루션을 설치하는 것이 적합한 방법이다.

8) 보안 모니터링 및 취약점 분석·평가

가. 필수 사항

▶ 전자금융감독규정 요구사항

check

클라우드 환경에서도 모두 준수할 필요

- 주요 정보처리시스템에 대한 구동, 조작방법, 명령어 사용법, 운용순서, 장애조치 및 연락처 등 시스템 운영매뉴얼을 작성할 것(제14조제1호)
- 데이터베이스관리시스템(Database Management System : DBMS)·운영체제·웹 프로그램 등 주요 프로그램에 대하여 정기적으로 유지보수를 실시하고, 작업일, 작업내용, 작업결과 등을 기록한 유지보수관리대장을 작성·보관할 것(제14조제2호)
- 정보처리시스템 책임자를 지정·운영할 것(제14조제6호)
- 정보처리시스템의 운영체계, 시스템 유틸리티 등의 긴급하고 중요한 보정(patch) 사항에 대하여는 즉시 보정 작업을 할 것(제14조제7호)
- 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템을 설치 및 운영(제15조제1항제1호)
- 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시(제15조제1항제2호)
- 제1항1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다.(제15조제2항)

  2. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것
  3. 보안정책의 승인·적용 및 보안정책의 등록, 변경 및 삭제에 대한 이력을 기록·보관할 것
  4. 정보보호시스템 원격관리를 금지할 것. 다만, 원격관리가 불가피한 경우 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다) 사용, 접근통제 등을 포함한 원격 접속 보안 대책을 수립·운영할 것
  5. 정보보호시스템의 작동 상태를 주기적으로 점검할 것
  6. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것
- 제1항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 정보보호시스템의 운영결과는 1년 이상 보존하여야 한다.(제15조제3항)
- 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다.(제16조제1항)

  1. 응용프로그램을 사용할 때에는 악성코드 검색프로그램 등으로 진단 및 치료 후 사용할 것

2. 악성코드 검색 및 치료프로그램은 최신상태로 유지할 것
3. 악성코드 감염에 대비하여 복구 절차를 마련할 것
4. 제12조제3호에 따른 중요 단말기는 악성코드 감염여부를 매일 점검할 것

- 클라우드서비스 내 구성한 전자금융기반시설에 대해 취약점 분석·평가를 실시하여 (연 1회 이상, 홈페이지는 6개월에 1회 이상 필수) 그 결과를 금융위원장에게 제출하는 결과보고서에 포함할 것(제37조의2)

※ 의무 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있음(제37조의2제6항)

※ 이외 필수사항의 경우 제37조의2 전문을 확인할 것

▶ 규정 준수 시 고려사항

- 정보처리시스템 보정(patch) 작업 등을 위해 클라우드서비스 내 패치 관리 기능 등 활용 가능
- 침입 탐지/방지 시스템, 웹 방화벽, DDoS 대응 장비, 악성코드 검색 및 치료 프로그램 등에 대해 해당 클라우드서비스 상의 부가 기능 이용, 자체 시스템 활용 등 다양한 방법으로 운영 가능하며, 사고 방지를 위해 필요한 부분을 충분히 포함하고 있는지 확인하고 미흡한 부분에 대한 별도 보완조치 필요
- 클라우드서비스 제공자가 제공 중인 정보보호시스템 기능을 이용 중인 경우에도 규정에서 요구하는 보안정책 관리, 보안 대책 수립, 주기적 점검* 등은 필수적

  * 작동 상태는 클라우드서비스 제공자가 제공하는 주기적인 레포트 등을 통해 확인 가능

- 취약점 분석·평가 수행 시 침해사고대응기관에서 마련한 취약점 분석·평가 항목 중 클라우드 관련 내용 등을 고려하며, 필요 시 클라우드서비스 제공자에게 협조를 요청할 수 있도록 계약서에 관련 내용을 명시
- 주요 정보처리시스템을 클라우드서비스 내에 구성할 경우 시스템 운영매뉴얼 개정이 필요하며, 해당 정보처리시스템 뿐만아니라 해당 시스템과 직접적으로 연관된 클라우드서비스 운영 방법도 운영매뉴얼에 포함할 필요

나. 추가 사항

- 클라우드서비스 내 주요 변경 사항에 대한 실시간 경보 설정 및 모니터링 실시
- 주요 정보처리시스템의 경우 침해사고 대응기관의 통합보안관제 적용

다. 권고 사항

- 보안 로그, 중요 시스템 및 관리자 이용 로그 등* 중요 로그를 실시간으로 모니터링하고 주기적으로 분석

  * (예) 멀티팩터 인증없는 관리 콘솔 로그인, 무단 API 호출, 관리자 계정 로그인 등

  - 특히, 「6) 로깅」에 따라 기록·유지 설정한 클라우드서비스 주요 변경 사항*에 대해 실시간 경보를 설정하여 모니터링 실시

    * (예) 계정·권한·보안그룹 관리(생성/변경/삭제), 가상 프라이빗 클라우드 네트워크 정책 관리, 저장소 관리, 저장소 접근 및 데이터 읽기/쓰기 등

9) 인적 보안

가. 필수 사항

▶ 전자금융감독규정 요구사항

check **클라우드 환경에서도 모두 준수할 필요**

- 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것(제8조제1항제2호)
- 전산인력의 자질향상 및 예비요원 양성을 위한 교육 및 연수프로그램을 운영할 것(제8조제1항제3호)

▶ 규정 준수 시 고려사항

- 클라우드서비스 관련 계약 체결 시 법무·준법 부서 등 외부주문등의 계약 체결 통제 조직·인력을 통해 계약내용의 적정성 검토 및 통제 실시
- 전산인력 자질향상 등을 위한 교육 및 연수프로그램 운영 시 클라우드서비스 이용 관련 교육 및 연수프로그램 추가를 반드시 고려

나. 추가 사항

- 클라우드서비스 제공자 및 클라우드 서비스 운영을 위탁받은 관리형 서비스 제공자 등의 권한과 책임을 식별하고 관리

다. 권고 사항

- 클라우드서비스 관련 보안 사고 중 이용자 및 관리자의 고의 또는 과실로 인한 사고 비율이 높다는 점을 반드시 인지
- 금융회사 내 클라우드서비스 이용자 및 관리자를 대상으로 서비스 이용 및 관리 절차, 보안리스크 및 대응 방안, 법적 요구사항 등에 대해 주기적인 교육 실시

- **클라우드서비스 제공자의 업무수행인력 관리 방안과 직원 보안 교육 계획 및 결과(대상 직원 수, 이수 시간 등) 등을 공유받아 검토하고 필요 시 시정 요구**
  - 특히, 클라우드서비스 운영을 외부에 위탁할 경우 해당 업무수행인력 관리 방안과 보안 교육 계획 및 결과 등을 검토 대상에 반드시 포함

FSI FINANCIAL SECURITY INSTITUTE
금융미래를 열어가는 금융보안파트너

금융분야 클라우드컴퓨팅서비스 이용 가이드

제 6 장

정보보호위원회 심의·의결

제6장 심의·의결

금융회사는 중요도 평가 결과, 클라우드서비스 제공자 평가 결과, 업무 연속성 계획 및 안전성 확보조치 방안에 대해 정보보호위원회를 개최하여 심의·의결하여야 한다.

▶ 감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 中

② 금융회사 또는 전자금융업자는 제1항 각 호에 따른 평가결과, 업무연속성 계획 및 안전성 확보조치에 대하여 제8조의2에 따른 정보보호 위원회 심의·의결을 거쳐야 한다.

참고 비조치의견서(190003, `19.2.25.)

: 클라우드 서비스 도입시 정보보호위원회 심의·의결이 필수적인지 여부 등

※ 비조치의견서는 신청자의 특정 행위에 대한 의견으로서 일반적 효력을 가지지 않음에 유의

〈 요청대상 행위 〉

□ OO회사의 자체메일이 아닌 상용메일을 수신하기 위해 동 메일 수신 전 클라우드 서비스를 이용하여 악성코드 유무를 탐지 후 클린 메일만 OO회사로 수신하는 서비스의 경우

○ 금융회사 자체 정보보호위원회 심의·의결을 거치지 않고 도입할 수 있는지 여부 및 위의 클라우드 서비스에서 해당 사업자의 서버가 국내 및 해외에 위치하여 동작할 때 「전자금융감독규정」을 위반할 소지가 있는지 여부

〈 판단 〉

□ 금융회사는 클라우드 서비스 이용대상 업무에 대해 중요도 평가를 실시하여야 하며, 자체 업무 위·수탁 운영기준 및 클라우드 서비스 제공자 평가결과에 대해 정보보호위원회를 개최하여 심의·의결하여야 하고,(「전자금융감독규정」 제14조의2제2항)

○ 금융회사가 클라우드 서비스 이용대상 업무에 대해 중요도를 평가한 결과 「전자금융감독규정」상 중요업무*로 판단될 경우, 해당 클라우드서비스 제공자의 정보처리시스템은 반드시 국내에 위치하여야 함(동조 제8항)

* 「전자금융감독규정」 제14조의2 제3항 제1호, 제2호

참고 비조치의견서(190003, `19.2.25.)

〈 판단 이유 〉

□ 금융회사 등이 본연의 업무인지 여부와 무관하게 클라우드 서비스를 이용하여 관련 업무를 처리하고자 하는 경우에는 업무 중요도 평가, 자체 업무 위·수탁 운영기준 마련, 클라우드 서비스 제공자 평가 등의 절차를 거치고 관련사항에 대해 정보보호위원회의 심의·의결을 거쳐야 함

□ 특히, 고유식별정보 또는 개인신용정보가 클라우드를 통해 처리되거나 클라우드를 통해 처리되는 업무가 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미친다고 판단될 경우에는,

○ 해당 클라우드 서비스 제공자의 정보처리시스템이 국내에 위치하여야 할 것으로 판단됨

금융분야 클라우드컴퓨팅서비스 이용 가이드

제 7 장

계약 체결

1. 기본 포함사항
2. 추가 포함사항

제7장 계약 체결

클라우드서비스 이용은 정보처리 위탁에 해당하므로, 정보처리위탁규정 제4조 제3항에 따른 계약서 포함사항 및 전자금융감독규정 [별표 2의5]의 위수탁 계약서 주요 기재사항도 반드시 명시하여야 하며, 비중요업무로 분류된 경우 기본 사항만을 포함하고, 중요 업무로 분류된 경우 기본 사항과 추가 사항을 모두 포함하여야 한다.

또한, 금융회사 등의 정보처리 업무를 클라우드서비스 제공자와의 직접계약이 아닌 간접계약(재위탁, MSP* 등)의 형태**로 수탁사(제3자)를 통해 처리하려는 경우에도 금융회사 등은 『전자금융감독규정』 제14조의 2에 따른 이용절차를 준수하여야 하며, 그에 따른 전자금융감독규정 [별표 2의5]의 위수탁 계약서 주요 기재사항에 대해서는 금융회사가 클라우드서비스제공자(CSP)와 직접 계약을 체결할 때와 동등한 효력을 가지도록 관련 계약에 반영하여야 한다.

* MSP(Managed Service Provider, 관리형서비스 사업자)

** 금융회사 등의 정보처리 업무를 수탁받은 업체가 수탁받은 정보처리 업무를 클라우드를 이용하여 지속적으로 처리하는 경우 등(예외의 경우는 '별첨. 금융분야 망분리 및 클라우드 규제 개선관련 FAQ 답변 내 4번항목 참고)

※ 규정에 명시된 것 이외의 사항은 금융회사가 자체적으로 판단하여 계약서에 기재하는 권고 사항임

▶ 정보처리위탁규정 제4조(정보처리의 위탁) 中

③ 금융회사는 제1항에 따른 정보처리 위탁계약을 체결할 경우 데이터에 대한 접근통제, 전산사고 등에 따른 이용자 피해에 대한 위·수탁회사간의 책임관계, 수탁회사에 대한 감독당국의 감독·검사 수용의무, 수탁회사의 분쟁해결 과정에서의 재판관할 등을 계약 내용에 반드시 포함하여 위탁에 따라 발생할 수 있는 책임관계를 명확히 하여야 한다.

▶ 감독규정 [별표 2의5] 클라우드컴퓨팅서비스 위수탁 계약서 주요 기재사항 中

가. 기본 포함사항

- 클라우드서비스 이용 대상 업무 및 시스템 개요
- 위탁하는 업무 데이터에 관한 사항
- 위수탁 계약 및 재위탁 관련 중요 변경사항이 있는 경우 통보필요 사항
- 감독당국 또는 내외부 감사인의 조사·접근 수용 의무
- 비상대응훈련, 취약점 분석·평가, 침해사고 대응훈련 등 협조 사항
- 클라우드서비스 제공자의 보안관리 수준 등에 관한 사항
- 정보보호 의무 및 서비스 연속성 보장 등 보안 요구사항
- 서비스에 악영향을 미칠 수 있는 경우 계약 해지 권한 보유
- 서비스 제공 수준(SLA) 모니터링 및 시정조치 권리
- 고객정보보호 및 비밀유지
- 위탁 계약 종료 시 데이터 파기
- 관련 법률 준수 및 보고 관련 의무

나. 추가 포함사항

- 금융회사 등이 위탁한 정보처리가 실제 수행되는 위치
- 서비스 제공 중단 시 데이터 접근권한 등 비상대책에 관한 사항
- 위탁업무를 다른 수탁자나 금융회사로 이전할 경우 지원의무 및 전환계획
- 합병·분할, 계약상 지위의 양도, 재위탁 등 중요 상황 발생시 대책
- 재위탁 또는 재위탁의 변경 등 금융회사의 동의가 필요한 사항
- 재위탁 관련 클라우드서비스 제공자의 관리·감독 의무

1 기본 포함사항

가. 클라우드서비스 이용 대상 업무 및 시스템 개요

▶ 규정 준수 시 고려사항

- 금융회사는 클라우드서비스를 이용함에 있어, 이용하고자 하는 업무와 시스템에 대한 개요를 계약서 내에 명시하여야 함
- 클라우드서비스 제공자는 클라우드서비스 이용 관련 모든 정보(서비스 위탁 규모 등 포함)를 금융회사가 위탁한 업무 범위 내에서만 처리하여야 함
- 클라우드서비스 제공자는 금융소비자의 고유식별정보 또는 개인신용정보가 처리되는 모든 시스템(일시적으로 처리되는 시스템 포함)이 국내에 설치되어 있고, 해당 전산실 내에 무선통신망이 설치되어있지 않도록 보장

나. 위탁하는 업무 데이터에 관한 사항

▶ 규정 준수 시 고려사항

- 금융회사가 클라우드서비스를 이용하여 처리하는 모든 정보는 금융회사의 소유로서 금융회사는 이 정보에 대해 언제든지 조회, 수정, 삭제할 수 있는 권리를 가지며, 클라우드서비스 제공자는 이를 제한하거나 정보에 대한 어떠한 권리도 주장할 수 없음
- 클라우드서비스 제공자는 금융회사가 처리를 위탁한 정보를 제3자(국외정부, 수사기관 등 포함)에게 제공하도록 규정하는 관련 법령*에 대해 사전에 파악하여 금융회사에 알려야 함(추가, 변경사항 포함)

* 정보 제공 사실을 알리는 것을 금지하는 조항이 있는 경우 해당 조항도 포함하여 금융회사에 알려야 하며, 실제 정보제공이 요구되었으나 해당 조항에 따라 금융회사에 알리는 것이 불가한 경우에는 금융위, 금감원에 별도 통지할 것

- 해당 법령에 따라 정보제공이 요구되는 경우 정보를 제공하기 전에 금융위, 금감원 및 금융회사에 통지하고, 관계국의 법령, 국가간 상호협정 등에서 정한 적법한 절차에 따라 처리하여야 함
  - 단, 원칙적으로 정보주체의 동의를 받도록 하는 「개인정보보호법」, 「신용정보의 이용 및 보호에 관한 법률」 등을 준수하여야 함

금융회사의 데이터가 국외에서 처리되는 경우(고유식별정보·개인신용정보 이외) **클라우드서비스 제공자는 정보처리, 보안 관리 등에 대한 해당 국가의 법적 의무사항에 대해 사전에 파악하여 금융회사에 통지하고,**

- 관련 법적 의무사항이 신규로 제정 또는 변경되는 경우 이를 파악하여 금융회사에 통지

> **▶ 정보처리시스템 국내 설치 예외**
> - 개정된 감독규정 시행('19.1.1.) 이전에 정보처리위탁규정에 따라 정보처리 업무를 국외 소재 전산센터에 위탁하여 클라우드서비스를 이용하고 있는 경우 예외(감독규정 부칙 제2조)
> - 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 감독규정 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자(국내 설치 요건 및 무선통신망 설치 금지 예외)

다. 위수탁 계약 및 재위탁 관련 중요변경사항이 있는 경우 통보필요 사항

▶ 규정 준수 시 고려사항

클라우드서비스 제공자가 일부 업무를 재위탁할 경우 재위탁 업무의 범위 및 재수탁자 정보 등을 금융회사에 명확하게 제공하여야 함

- 클라우드서비스 제공자는 업무 재위탁 시 재수탁자가 원계약을 준수하도록 하고, 재위탁 계약서에 본 가이드의 계약서 명시사항 중 관련 부분을 포함하여야 함

클라우드서비스 제공자는 서비스 제공과 관련된 중요 업무의 신규 재위탁 또는 기존 재위탁의 중요 사항 변경 시 금융회사에 사전 통지하여야 하며,

- 금융회사는 이에 따른 보안리스크 증가 등 서비스 영향이 크다고 판단되는 경우 계약을 해지할 수 있음

라. 감독당국 또는 내외부 감사인의 조사·접근 수용 의무

▶ 규정 준수 시 고려사항

- 금융위, 금감원, 침해사고대응기관, 금융회사 사내·사외 감사(정보보호담당자 포함) 및 금융회사가 임명한 제3자(이하 '금융위, 금감원 및 내외부 감사인')는 조사·접근을 수행*할 수 있으며,

  * 금융회사가 지정한 제3자의 감사보고서 검토로 내외부 감사인의 조사·접근을 일부 대체할 수 있음(단, 금융위, 금감원, 침해사고대응기관의 조사·접근은 대체할 수 없음)

  - 클라우드서비스 제공자는 이를 위해 현장 방문, 관련 자료 제출 요구 및 검사에 적극 협조

- 금융위, 금감원 및 내외부 감사인은 클라우드서비스에 이용되는 모든 범위의 장치, 시스템, 네트워크 및 데이터에 접근할 수 있음

- 금융위, 금감원은 클라우드서비스 제공자를 대상으로 감독·검사를 수행할 수 있고,

  - 내외부 감사인은 클라우드서비스 제공자를 대상으로 감사를 수행할 수 있으며, 필요 시 다수 금융회사가 공동으로 또는 위탁받은 제3자를 통해 감사를 수행할 수 있음

- 금융위, 금감원 및 내외부 감사인은 클라우드서비스 제공자에게 제3자 인증 또는 내부 감사 보고서의 제출을 요구할 수 있고,

  - 금융회사 업무와 관련된 대상에 대해 내부 감사 보고서의 보완을 요구할 수 있음

- 금융위, 금감원 및 내외부 감사인은 감독·검사 및 감사 수행 또는 인증·감사 보고서 검토 결과 지적된 사항에 대해 지체 없이 조치할 것을 요구할 수 있음

  - 관련 법적 의무사항이 신규로 제정 또는 변경되는 경우 이를 파악하여 금융회사에 통지

마. 비상대응훈련, 취약점 분석·평가, 침해사고 대응훈련 등 협조 사항

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자는 재해 또는 사고 발생 시 신고 절차, 복구 및 대응 절차 등을 마련하고 주기적으로 훈련을 실시하여야 함
  - 관련 직원을 모두 포함한 비상 연락 체계를 마련하고, 복구목표시간 및 복구목표시점 요건을 금융회사와 사전에 합의하여야 하며, 필요 시 공동 훈련을 실시하여야 함
- 클라우드서비스 제공자는 금융회사 및 침해사고대응기관이 감독규정 제24조, 제37조의3 및 제37조의4에 따라 수행하는 비상대응훈련, 재해복구전환훈련, 통합보안관제, 침해사고대응훈련, 취약점 분석·평가 등을 수행할 수 있도록 지원하여야 함
- 클라우드서비스 제공자는 제공자가 관리하는 영역(인프라 등)에 대해 주기적으로* 제3자 또는 자체전담반**에서 취약점 분석·평가를 수행하고 조치하였음을 금융회사에 통지(금융위 또는 금감원 요청 시 세부 수행 결과를 제출)하여야 함

  * 이용 대상의 중요도에 따라 매년, 중대 변경 시 등 금융회사에서 적정한 주기를 판단하여 구체적으로 명시

  ** 전자금융감독규정 제37조의2 제2항의 요건을 만족하는 자체전담반

  - 또한, 금융회사는 관련 보안사고 발생 등 필요 시 클라우드서비스 제공자에 추가적인 점검 수행을 요구할 수 있음

바. 클라우드서비스 제공자의 보안관리 수준 등에 관한 사항

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자는 「제4장] 금융분야 클라우드서비스 제공자 안전성 평가 기준」 내 서비스 제공기준을 금융회사가 요구하는 수준으로 상시 만족하여야 함

사. 정보보호 의무 및 서비스 연속성 보장 등 보안 요구사항

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자와 금융회사는 각자의 정보보호 역할과 책임의 범위, 사고발생에 따른 손해배상 및 계약해지 관련 사항을 명확하게 정의하여야 함
  - 특히, 클라우드서비스 제공자는 장애 예방 등 적절한 수준의 서비스 품질을 보장하고 정보보호 역할과 책임을 다하기 위해 노력하여야 함
- 금융회사는 클라우드서비스 제공자의 업무수행인력에 대하여 사전 신원조회 실시(신원보증보험증권 징구로 갈음할 수 있음) 또는 대표자의 신원보증서를 징구할 수 있고,
  - 클라우드서비스 제공자는 업무수행인력 내역 및 인력변경 시 인수인계에 관한 사항 등을 포함한 업무수행인력 관리방안을 제출하여야 함(감독규정 제60조 제1항제13호)
- 클라우드서비스 제공자는 위탁 업무 관련 법규 및 자율규제를 준수하고, 금융회사의 위탁 업무 모니터링을 지원하여야 함
- 클라우드서비스 제공자는 금융회사에서 수립한 업무 연속성 계획 및 안전성 확보조치 방안이 적절하게 이행될 수 있도록 협조 및 지원하여야 함

아. 서비스에 약영향을 미칠 수 있는 경우 계약 해지 권한 보유

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자의 관련 법령, 계약상 의무 위반 등으로 인해 금융소비자에게 손해가 발생하는 경우에는 클라우드서비스 제공자는 금융회사와 연대하여 배상책임을 부담
  - 클라우드서비스 제공자의 귀책사유로 금융소비자에게 발생한 손해를 금융회사가 우선 배상한 경우 금융회사는 클라우드서비스 제공자에게 구상권을 행사할 수 있음

- 클라우드서비스 제공자가 전자금융거래법, 신용정보법, 개인정보보호법 등 관련 법령* 또는 계약상 의무 위반이 원인**이 되어
  - 금융회사 또는 금융소비자에게 손해를 끼친 경우, 금융회사는 별도의 불이익 없이 서비스 이용계약을 해지할 수 있으며, 클라우드서비스 제공자에게 손해배상을 청구할 수 있음

* 「전자금융거래법」, 「신용정보의 이용 및 보호에 관한 법률」, 「금융기관의 업무위탁 등에 관한 규정」, 「금융회사의 정보처리 업무 위탁에 관한 규정」 등 금융 관련 법령, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」, 「개인정보보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등

** 클라우드서비스 제공자가 전자금융거래 법령을 포함한 관계 법령 또는 이용 계약상의 의무를 미이행·위반한 경우에는 클라우드서비스 제공자의 고의 또는 과실이 있는 것으로 볼 수 있음

- 금융회사가 클라우드서비스 제공자에게 청구할 수 있는 손해배상의 범위는 서비스 중단 또는 자료 유출 등으로 인한 직접적인 피해뿐만 아니라, 금융회사의 대외 신뢰도 저하 등 간접적인 피해도 포함됨

- 클라우드서비스 제공자에 의해 관련 법령 위반, 반복적인 계약상 의무 불이행, 중요 계약사항의 위반(금융위·금감원의 조사·접근권 관련 의무 미이행 등) 등이 발생할 경우 금융회사는 위약금 등 불이익 없이도 계약해지가 가능하여야 함

자. 서비스 제공 수준(SLA) 모니터링 및 시정조치 권리

▶ 규정 준수 시 고려사항

- 금융회사와 클라우드서비스 제공자 간 사전 협의를 거쳐 서비스 수준 협약(SLA)*, 구체적 손해배상 규정** 등을 정하고,
  - 불가항력으로 인한 사고 등 클라우드서비스 제공자의 책임이 면제되는 사유 및 범위를 구체적으로 명시

* SLA(Service Level Agreement): 클라우드서비스 제공자가 금융회사 등 이용자에게 제공하는 서비스의 수준을 정량 기준 등을 통해 명확히 제시하고, 이에 미달하는 경우 손해를 배상토록 하여 서비스의 품질을 보장하기 위한 약정

** 클라우드서비스 제공자는 금융회사와 사전에 협의하여 정한 손해배상 규정에 따라 구체적인 손해를 산출하고, 금융회사에게 해당 손해액을 지급토록 함

- 또한, 서비스 수준 협약(SLA)에 따라 클라우드서비스 제공자가 서비스를 제공하고 있는지 지속적으로 모니터링 하여야 함

사전 협의된 서비스 수준을 클라우드서비스 제공자의 귀책 사유로 인해 유지하지 못할 경우 클라우드서비스 제공자는 이로 인해 금융회사에 발생하는 손해를 배상하여야 함

- 또한, 이후 같은 상황이 재발되지 않도록 금융회사는 시정조치를 요구할 수 있어야 함

차. 고객정보보호 및 비밀유지

▶ 규정 준수 시 고려사항

금융회사가 클라우드서비스를 이용하여 처리하는 모든 정보는 금융회사의 소유로서 금융회사는 이 정보에 대해 언제든지 조회, 수정, 삭제할 수 있는 권리를 가지며, 클라우드서비스 제공자는 이를 제한하거나 정보에 대한 어떠한 권리도 주장할 수 없음

클라우드서비스 제공자는 모든 정보 전송 시 암호화 기술을 적용하여야 하며, 정보의 비인가 접근 및 유출 등을 방지하기 위해 충분한 보호수단을 적용하여야 함

클라우드서비스 제공자는 클라우드 서비스를 제공함에 있어, 취득한 금융회사 데이터에 대한 비밀유지 서약을 준수하여야 함

클라우드서비스 제공자는 금융회사가 클라우드서비스 제공자와 네트워크 연결이 필요할 경우 전용회선 또는 전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 이용할 수 있도록 지원하여야 함

클라우드서비스 제공자는 직원 보안 교육을 주기적으로 실시하고, 금융회사가 요청할 경우 교육 계획 및 수행 결과를 제출하여야 함

- 특히, 금융회사 관련 업무 수행에 따른 비밀유지 의무 준수 및 위반 시 처벌내용 등에 대한 내용을 보안 교육에 포함하여야 함(감독규정 시행세칙 [별표 5의2])

※ 다만, 금융회사 관련 업무수행인력을 특정할 수 없을 경우, 해당 데이터센터 근무 인력 등 금융회사 서비스 제공과 직접적으로 연관되어 있는 인력으로 한정하여 실시 가능

카. 위탁 계약 종료 시 데이터 파기

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자는 금융회사가 자신의 정보를 파기할 수 있는 신뢰성 있는 수단을 제공하여야 하며, 금융회사가 제공되는 수단을 적절하게 이용할 경우 파기된 정보는 복구 불가능함을 보장*하여야 함

  * 예) 복구 불가능한 방법을 통해 파기 되었음을 파기 확인서 등을 통해 확인

  - 특히, 금융회사가 이용하는 시스템의 물리적 영역이 변경되거나, 이용을 종료하여 접근할 수 없는 경우에도 금융회사가 기 이용한 물리적 영역에 저장된 정보는 복구 불가능한 수준으로 파기되어야 함
  - 아울러, 전자금융거래기록의 경우 「전자금융거래법」 제22조 및 동법 시행령 제12조를, 개인신용정보의 경우 「신용정보법」 제20조의2 및 「개인정보보호법」 제21조 등 관계 법령을 준수하여 파기할 수 있도록 지원
  - 이때, 재위탁된 정보, 관리 서비스 및 주변 솔루션 내 정보 등도 동일하게 처리

타. 관련 법률 준수 및 보고 관련 의무

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자는 위탁 업무 관련 법규 및 자율규제를 준수하고, 금융회사의 위탁 업무 모니터링을 지원하여야 함

- 클라우드서비스 제공자와 금융회사 간의 분쟁으로 소송이 제기되는 경우 민사소송법이 정한 법원을 관할 법원으로 하고, 당사자 일방이 외국사업자인 경우에는 대한민국 법원이 국제 재판관할권을 가짐

  - 기타 계약의 성립, 효력, 해석 및 이행과 관련하여서는 대한민국의 법을 적용

2 추가 포함사항

가. 금융회사 등이 위탁한 정보처리가 실제 수행되는 위치

▶ 규정 준수 시 고려사항

- 클라우드서비스를 이용하는 업무, 처리되는 데이터, 데이터가 처리되는 물리적 위치(시·군 단위까지)에 대해, 금융위원회(이하 '금융위') 또는 금융감독원(이하 '금감원')의 요청이 있는 경우 클라우드서비스 제공자는 데이터 처리가 실제 수행되는 위치를 고지

나. 서비스 제공 중단 시 데이터 접근권한 등 비상대책에 관한 사항

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자는 서비스 지연 또는 중단이 발생할 경우에 대비 신속하게 대응 및 복구할 수 있는 절차와 체계를 마련하여 사전에 금융회사에 알려야 함
  - 특히, 중요정보를 클라우드서비스를 통하여 처리하는 경우, 클라우드서비스 제공자는 장애, 보안사고 등 유사 시 신속한 대응을 위해 필요한 시스템 운영 관련 상주 인력을 국내에 확보하고, 원활한 사고 대응을 위해 해당 인력의 관리시스템 접근 권한 등을 확보하여야 함
    - 또한, 금융회사 담당자의 경우 자사(금융회사)의 데이터에 대한 접근권한 등을 확보하여야 함
- 사고 발생 시, 클라우드서비스 제공자는 이를 인지한 즉시 금융회사에 통지(침해사고의 경우 침해사고대응기관에도 통지)하고, 사고 조사 및 피해 복구에 적극 협조*하여야 함

* 사고 원인분석을 위한 자료 보전 및 제출, 현장 조사, 인력 지원, 피해 확산·재발 방지 및 복구를 위해 필요한 조치 등

- 아울러, 클라우드서비스 제공자는 사고 조사를 위해 필요한 주요데이터(로그, 가상화 이미지 등)를 금융회사에 제공할 수 있도록 기술적 방안을 마련해야 함

※ 금융회사는 정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무 중단 또는 지연, 전산자료 또는 프로그램의 조작과 관련된 금융사고, 전자적 침해사고 등 관련 규정에서 정한 사고 발생 시 지체 없이 금융감독원에 보고하여야 하고(감독규정 제73조), 클라우드서비스 제공자는 침해사고 발생·이용자 정보 유출 시 지체 없이 그 사실을 해당 이용자에게 알려야 하며, 특히 이용자 정보 유출 시 과학기술정보통신부장관에게 보고하여야 함(클라우드컴퓨팅법 제25조)

다. 위탁업무를 다른 수탁자나 금융회사로 이전할 경우 지원의무 및 전환계획

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자는 금융회사의 클라우드서비스 전환 및 종료 관련 절차에 적극적으로 협조하여야 함
- 클라우드서비스 제공자는 금융회사의 클라우드서비스 이용이 종료되는 경우 업무 중단 없이 금융회사가 정보를 이전할 수 있도록 지원하여야 하며,
  - 클라우드서비스 제공자는 금융회사에게 정보 이전을 위한 충분한 시간을 제공하고, 정보를 최종 삭제하기 전에 금융회사의 확인을 받아야 함
- 클라우드서비스 제공자의 사정에 의해 서비스를 종료할 경우, 클라우드서비스 제공자는 다른 클라우드서비스 제공자로의 이전 등 대안을 제시하여야 함
- 금융회사는 클라우드서비스의 전환 및 종료 절차에 대한 모의훈련을 주기적으로 실시할 것을 요구할 수 있음

라. 합병·분할, 계약상 지위의 양도, 재위탁 등 중요 상황 발생시 대책

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자는 클라우드서비스 제공과 관련된 업무를 다른 사업자에게 위탁할 경우 해당 수탁자가 금융회사와의 계약 내용을 준수하도록 관리·감독하여야 함

- 재위탁 관계에서 금융회사에 발생한 손해에 대하여는 원위탁자(클라우드서비스 제공자)가 우선 배상하여야 함(재위탁 받은 업체의 고의·과실은 클라우드서비스 제공자의 고의·과실로 간주)

원칙적으로 정보기술부문의 정보보호와 관련된 업무를 위탁받은 전자금융보조업자는 해당업무를 제3자에게 재위탁할 수 없음(전자금융거래법 제40조제6항)

- 다만, 전자금융거래정보의 보호와 관련된 전산장비·소프트웨어에 대한 개발·운영 및 유지관리 업무를 재위탁하는 경우로 다음 사항을 준수하는 경우 가능(감독규정 제60조제4항)
  - 재수탁업자가 재위탁된 업무를 처리함에 있어 금융거래 정보의 변경이 필요한 경우에는 위탁회사 또는 원수탁업자의 개별적 지시에 따라야 하며, 위탁회사 또는 원수탁업자는 변경된 정보가 지시 내용에 부합하는지 여부를 확인하여야 함
  - 위탁업무와 관련된 이용자의 금융거래정보는 위탁회사의 전산실 내에 두어야 함. 다만, 재수탁업자가 이용자의 정보를 어떠한 경우에도 알지 못하도록 위탁회사 또는 원수탁업자가 금융거래정보를 처리하여 제공한 경우에는 위탁회사의 관리·통제하에 재수탁회사 등 제3의 장소로 이전 가능함

참고 법령해석 회신문(200036, '20.5.4.)

: 클라우드와 관련하여 전자금융감독규정 제60조 제4항의 적용여부 및 해석 요청

〈 질의 요지 〉

- 「전자금융거래법」 상 금융회사 또는 전자금융업자가 클라우드컴퓨팅서비스 제공자와 계약을 맺고 클라우드컴퓨팅서비스를 이용하면서 정보보호와 관련된 업무 역시 위탁한 때, 전자금융감독규정 제60조 제4항의 요건을 갖춘 경우 금융회사의 정보보호와 관련된 업무를 재위탁하는 것이 가능한지 여부(특히, 금융회사 등이 클라우드컴퓨팅을 이용할 때,위 감독규정 제60조 제4항 제2호의 요건 중 위탁회사의 전산실의 범위에 클라우드 전산센터가 포함되는지 여부)

〈 회답 〉

□ 「전자금융거래법」 제40조 제6항 단서에 따라 금융회사 등이「전자금융감독규정」 제60조 제4항 제1호 및 제2호의 기준을 준수하는 경우에는 정보보호와 관련된 업무의 재위탁이 가능합니다.

○ 한편, 금융회사 등이 제3자가 제공하는 클라우드컴퓨팅서비스를 이용하는 경우에도 「전자금융거래법」 제28조, 「전자금융감독규정」제14조의2, 제50조 제1항 제2호 및 제4호에 따라 허가·등록의 요건으로서 전산설비·기기 등을 갖추었다고 볼 수 있으므로,

- 「전자금융감독규정」 제60조 제4항 제2호의 요건과 관련한 위탁회사인 금융회사 등의 전산실의 범위에는 제3자인 클라우드컴퓨팅서비스 제공자의 전산센터도 포함된다고 판단됩니다.

참고 법령해석 회신문(200036, `20.5.4.)

〈 이유 〉

□ 「전자금융거래법」 제40조 제6항의 정보보호 관련 업무의 재위탁 제한규정은 전자금융거래정보의 보호 및 안전한 처리를 목적으로 도입되었습니다.

○ 「전자금융거래법」에서의 정보보호 관련 업무는 전자금융거래의 안정성 확보 및 이용자 보호를 위한 업무로서(「전자금융거래법」§21의2④ 등), 방화벽 운용, 시스템 모니터링 등 보안 인프라 운영과 취약점 분석평가, IT내부통제 관리 등의 업무를 포괄하며,

- 정보의 외부유출 방지 등을 위해 금융회사 등의 정보보호최고책임자(CISO)가 통솔해야 하는 업무이므로 원칙적으로 재위탁을 제한하되, 단서규정을 두어 일정한 조건을 준수하는 경우에 한하여 제한적으로 재위탁을 허용하였습니다.

□ 아울러,「전자금융감독규정」 제60조 제4항 각 호에서는 전자금융거래정보의 보호 목적 달성을 위해 다음과 같이 재위탁의 기준을 구체화하고 있으므로, 해당 기준을 준수하는 경우에는 재위탁이 가능합니다(「전자금융감독규정」§60④ Ⅰ, Ⅱ).

i) 재수탁업자가 재위탁된 업무를 처리함에 있어 금융거래 정보의 변경이 필요한 경우에는 위탁회사 또는 원수탁업자의 개별적 지시에 따라야 하고, 위탁회사 또는 원수탁업자는 변경된 정보가 지시 내용에 부합하는지 여부를 확인할 것

ii) 위탁업무와 관련된 이용자의 금융거래정보는 “위탁회사의 전산실” 내에 둘 것(다만, 재수탁업자가 이용자의 이용자 정보를 어떠한 경우에도 알지 못하도록 위탁회사 또는 원수탁업자가 금융거래정보를 처리하여 제공한 경우에는 위탁회사의 관리·통제 하에 재수탁회사 등 제3의 장소로 이전 가능)

□ 이 경우 「전자금융감독규정」 제60조 제4항 제2호의 위탁회사의 "전산실"이라 함은 전산장비, 통신 및 보안장비, 전산자료 보관 및 출력장비가 설치된 장소를 의미하고(「전자금융감독규정」§2 Ⅰ),

○ 금융회사 등이 제3자가 제공하는 클라우드컴퓨팅서비스를 이용하는 경우에도 「전자금융거래법」제28조, 「전자금융감독규정」제14조의2, 제50조 제1항 제2호 및 제4호에 따라 허가·등록의 요건으로서 전산설비·기기 등을 갖추었다고 볼 수 있으므로

- 위탁회사인 금융회사 등의 전산실의 범위에는 제3자인 클라우드 컴퓨팅서비스 제공자의 전산센터도 포함된다고 판단됩니다.

□ 다만, 클라우드 서비스 제공자가 위탁받은 업무를 재위탁하는 경우에는 금융회사 등과 체결된 클라우드컴퓨팅 서비스 이용계약(위·수탁 계약) 및 「전자금융감독규정」 제14조의2 제1항 제3호에 따라 마련된 금융회사 등의 자체 업무 위·수탁 운영기준을 준수하여야 합니다(금융보안원, 금융분야 클라우드컴퓨팅서비스 이용가이드 64면 등 참조).

○ 또한, 재위탁에 따른 재수탁자도 전자금융거래법 제2조 제5호에 따른 전자금융보조업자의 범위에 포함되므로 법 제40조 및 감독규정 제60조에 따른 의무사항을 준수하여야 합니다.

마. 재위탁 또는 재위탁의 변경 등 금융회사의 동의가 필요한 사항

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자는 서비스 제공과 관련된 중요 업무의 신규 재위탁 또는 기존 재위탁의 중요 사항 변경 시 금융회사에 사전 통지하여야 하며,
  - 금융회사는 이에 따른 보안리스크 증가 등 서비스 영향이 크다고 판단되는 경우 계약을 해지할 수 있음

바. 재위탁 관련 클라우드서비스 제공자의 관리·감독 의무

▶ 규정 준수 시 고려사항

- 클라우드서비스 제공자는 클라우드서비스 제공과 관련된 업무를 다른 사업자에게 위탁할 경우 해당 수탁자가 금융회사와의 계약 내용을 준수하도록 관리·감독하여야 함
  - 재위탁 관계에서 금융회사에 발생한 손해에 대하여는 원위탁자(클라우드서비스 제공자)가 우선 배상하여야 함(재위탁 받은 업체의 고의·과실은 클라우드서비스 제공자의 고의·과실로 간주)

FSI FINANCIAL SECURITY INSTITUTE
금융미래를 열어가는 금융보안파트너

금융분야 클라우드컴퓨팅서비스 이용 가이드

제 8 장

이용 및 보고

1. 보고
2. 보고 방법
3. 클라우드 이용 관련 리스크 관리

제8장 이용 및 보고

1 보고

가. 서류 구비

▶ 감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 제5항

⑤ 제4항에 따라 금융감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.
1. 「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조제1항 각 호에 관한 서류
2. 제1항제1호에 따른 업무의 중요도 평가 기준 및 결과
3. 제1항제2호에 따른 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가 결과
4. 제1항제3호에 따른 업무 연속성 계획 및 안전성 확보조치에 관한 사항
5. 제2항에 따른 정보보호위원회 심의·의결 결과
6. 〈별표 2의5〉의 계약서 주요 기재사항을 포함한 클라우드컴퓨팅서비스 이용계약서

⑥ 클라우드컴퓨팅서비스를 이용하는 금융회사 또는 전자금융업자는 제4항에 따른 보고의무와 관계없이 제5항 각호에 따른 서류를 최신상태로 유지하여야 하며, 금융감독원장의 요청이 있을 경우 이를 지체 없이 제공하여야 한다.

※ 중요도 평가 결과와 무관하게 전자금융감독규정 제14조의2제4항에 따른 보고의 의무와 관계없이 다음 각 서류를 구비, 최신 상태로 유지하고, 금융감독원장 요청 시 이를 지체 없이 제공하여야 함

정보처리위탁규정 제7조제1항 각 호에 관한 서류

※ 위탁계약서(안) 사본 이외에는 계약서 조항이 아닌 이를 확인할 수 있는 서류 제출

- 위탁계약서(안) 사본
- 「금융기관의 업무위탁 등에 관한 규정」 제3조의2에 따라 금융기관이 마련하고 준수하여야 할 '업무위수탁 운영기준'
- 업무위탁 계약이 이 규정 등 관련법령에 위배되지 아니한다는 준법감시인(준법감시인이 없는 경우, 감사 등 이에 준하는 자)의 검토의견 및 관련자료 사본

- 위탁의 필요성 및 기대효과
- 위탁에 따른 업무처리절차의 주요 변경내용
- 정보처리업무 운영에 대한 감독기관의 실질적 감독가능성을 확인할 수 있는 서류
- 위탁계약 상대방(재위탁 예정시 재위탁계약 상대방 포함)에 관한 사항(상호, 자본금 규모, 소재지, 주된 업종, 개인의 경우 대표자 인적사항 등)
- 전산사고 및 정보유출 등 발생시 피해자 구제절차

이용업무의 중요도 평가 기준 및 결과(제3장 참조)

- 중요도 평가 기준
- 중요도 평가 결과

클라우드서비스컴퓨팅 제공자의 건전성·안전성 등에 대한 평가 결과([제4장] 참조)

- 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 평가 결과(감독규정 〈별표 2의2〉 참조)

※ 비중요업무로 분류된 경우 또는 클라우드서비스 제공자가 국내·외의 클라우드 서비스 관련 보안인증 등을 취득하여 유지하고 있는 경우 대체 항목 생략 가능

관련 업무 연속성 계획 및 안전성 확보조치에 관한 사항(제5장 참조)

- 업무 연속성 계획(감독규정 〈별표 2의3〉 참조)
- 안전성 확보조치에 관한 사항(입증자료 포함, 감독규정 〈별표 2의4〉 참조)

※ 비중요업무로 분류된 경우 필수 사항 준수 필요(추가 사항 생략 가능)

이용업무 중요도와 클라우드서비스 제공자의 건전성·안전성 등 평가결과 및 업무 연속성 계획, 안전성 확보조치에 대한 정보보호위원회 심의·의결 결과(회의록 포함)

- 정보보보위원회 심의·의결 결과
- 정보보호위원회 안건 자료
- 정보보호위원회 회의록 및 의사록

클라우드컴퓨팅서비스 이용 계약서

- 클라우드컴퓨팅서비스 이용 계약서(감독규정 〈별표 2의5〉 참조)

※ 비중요업무로 분류된 경우 계약서 내 기본사항만 포함 가능

나. 사후 및 수시 보고

금융회사 또는 전자금융업자는 다음 중 어느 하나에 해당하는 사유가 발생한 경우 발생한 날로부터 3개월 이내*에 발생 사유, 관련 자료 및 대응 계획을 첨부하여 금융감독원장에게 보고하여야 함

* 클라우드를 이용한 개발·테스트 등으로 이용 계약 체결 후 실제 업무수행까지 3개월 이상 소요될 경우 클라우드서비스와 금융회사 내부망(연구·개발망 제외)간 연계 후 3개월 이내

※ 신규 금융회사 및 전자금융업자의 경우 허가 및 등록이 완료된 이후 사후보고 필요

▶ 감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등) 제4항

④ 금융회사 또는 전자금융업자는 다음 각 호의 어느하나에 해당하는 사유가 발생한 날로부터 3개월 이내에 발생 사유, 관련 자료 및 대응계획을 첨부하여 금융감독원장에게 보고하여야 한다.

1. 클라우드컴퓨팅서비스 이용 계약을 신규로 체결하는 경우
2. 클라우드컴퓨팅서비스 제공자의 합병, 분할, 계약상 지위의 양도, 재위탁 등 중대한 변경사항이 발생한 경우
3. 클라우드컴퓨팅서비스 제공자가 서비스품질의 유지, 안전성 확보 등과 관련한 중요계약사항을 이행하지 아니한 경우
4. 제1항제2호 또는 제3호에 관한 중대한 변경사항이 발생한 경우

※ 「감독규정개정안」제14조의2제4항에 따른 사후보고를 한 경우 「정보처리위탁규정」 제7조 제1항 내지 제3항 및 제4항제2호 본문에 따라 보고한 것으로 간주

참고 비조치의견서(220036, `22.7.21.)

: 클라우드컴퓨팅 서비스이용에 따른 금감원 신고 대상 여부

※ 비조치의견서는 신청자의 특정 행위에 대한 의견으로서 일반적 효력을 가지지 않음에 유의

〈 요청 대상 행위 〉

□ 금융회사가 계열사의 클라우드서비스를 이용할 경우, 「전자금융감독규정」 제14조의2(클라우드컴퓨팅서비스 이용절차 등)에 따른 절차를 이행해야 하는지 여부

〈 판단 〉

□ 아래 내용을 참고하시기 바랍니다.

〈 판단이유 〉

□ 「전자금융감독규정」 제14조의2는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」(이하 '클라우드법') 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우에 적용되는 조항으로

◦「클라우드법」 제2조제3호에 정의하는 클라우드컴퓨팅서비스란 클라우드컴퓨팅을 활용하여 상용*으로 타인에게 정보통신자원을 제공하는 서비스를 의미합니다.

참고 비조치의견서(220036, `22.7.21.)

* 클라우드컴퓨팅 주요법령 해설서(2017.11, 과학기술정보통신부)

"상용"이란 무상·유상에 구애받지 않고 상업용으로 제공되는 것을 의미하므로 무상으로 제공되는 클라우드컴퓨팅서비스라도 상용으로 제공되고 있다면 포함될 수 있고, 무상으로 클라우드컴퓨팅서비스를 제공하더라도 광고를 통해서 수익을 올리고 있다면 상용에 해당합니다.

반면 전산시설 등의 사용 수수료를 내더라도 상용(商用)으로 제공되는 클라우드컴퓨팅서비스가 아니라면 이 법에서 말하는 클라우드컴퓨팅서비스에 해당하지 아니합니다. 예컨대 협회, 단체 등이 전용으로 구축한 클라우드컴퓨팅서비스는 포함되지 않습니다.

□ 귀사의 계열사가 제공하는 클라우드컴퓨팅서비스가 '非상용' 서비스에 해당하는 한 「클라우드법」에서 말하는 클라우드컴퓨팅서비스에 해당되지 아니하므로,

◦「전자금융감독규정」 제14조의2에서 규율하는 클라우드컴퓨팅서비스에도 해당되지 않는 것으로 판단됩니다.

◦다만, 망분리 관련 규정인 「전자금융감독규정」 제15조 등 관련 법규를 철저히 준수하시기 바랍니다.

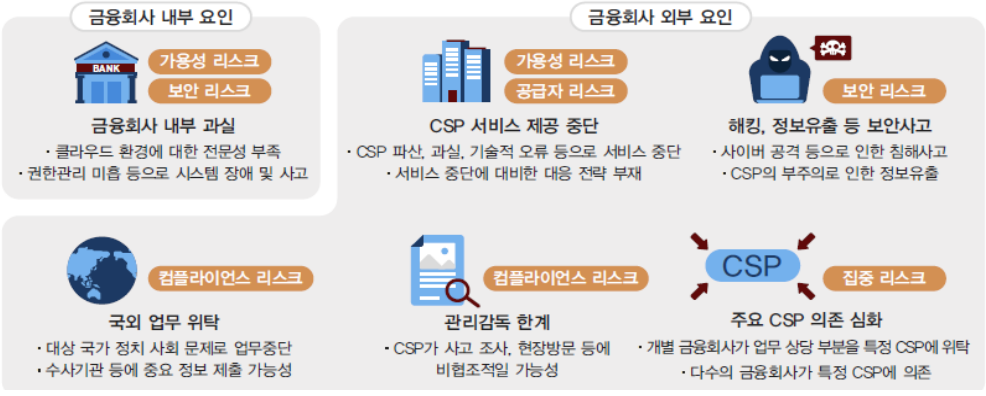
2 보고 방법

금융회사는 감독규정 시행세칙 '별지 제6호 이용대상 정보처리시스템 지정보고' 서식에 따라 구비된 서류를 첨부하여 전자문서교환시스템을 통해 전자공문으로 제출

※ 보고 서류가 누락되거나 안전성 확보조치 등이 충분하지 않다고 판단하는 경우 개선·보완을 요구할 수 있으므로, 공문 제출 전에 금융감독원 담당자와 사전 협의를 권고(의무사항은 아님)

3 클라우드 이용 관련 리스크 관리

〈그림4. 클라우드 이용 관련 리스크〉



- 클라우드서비스를 이용함에 있어 기 수립된 업무 연속성 계획 및 안전성 확보 조치 방안을 바탕으로 관련 리스크를 지속적으로 관리하여야 함
- 필요한 경우 관련 규제의 준수 또는 업무 연속성 계획 및 안전성 확보조치 방안의 이행을 위해 클라우드서비스 제공자에게 협조를 요구할 수 있음
  - 금융위·금감원의 조사·접근(현장방문 포함), 통합보안관제·취약점 분석평가·비상대응훈련 등이 원활하게 수행될 수 있도록 클라우드서비스 제공자에게 적극적인 협조를 요청하여야 함
  - 다만, 금융위·금감원의 요구, 사고발생, 법적 요구사항(클라우드서비스 제공자 안전성 평가 등) 등 반드시 필요한 경우에만 현장 방문 등을 요구하여야 함
- 수시보고 대상이 되는 클라우드서비스 제공자의 재위탁 등 변동사항이 있는 경우 관련 보안리스크를 평가하고 필요 시 보완조치 수행
- 특정 클라우드서비스 제공자에 서비스가 집중되지 않도록 유의하고, 특히 중요도가 높은 정보처리시스템에 대해서는 클라우드서비스 제공자에 대한 의존도가 과다하지 않도록 관리하여야 함

  ※ 집중리스크 관련 상세내용은 ([부록2] 참조)

FSI FINANCIAL SECURITY INSTITUTE
금융미래를 열어가는 금융보안파트너

금융분야 클라우드컴퓨팅서비스 이용 가이드

제 9 장

이용 종료

제9장 이용 종료

금융회사는 클라우드서비스 제공자의 **파산, 서비스 중단, 서비스 품질 저하, 규제 환경의 변화 또는 기타 금융회사의 필요에 따라** 클라우드서비스를 전환 또는 종료할 경우 「제5장 업무 연속성 계획 및 안전성 확보조치 방안 수립」에서 수립한 출구 전략에 의거하여 데이터 이전 및 파기 등을 실시하여야 한다.

또한, 금융회사는 기존에 이용중인 클라우드서비스 제공자를 변경(전환)하는 경우 「제8장 이용 및 보고」을 참고하여 금융감독원에게 보고하여야 한다.

FSI FINANCIAL SECURITY INSTITUTE
금융미래를 열어가는 금융보안파트너

금융분야 클라우드컴퓨팅서비스 이용 가이드

부록 1

업무중요도 평가 방법 및 사례 예시

금융회사는 클라우드서비스를 이용하고자 하는 경우 감독규정 14조의2 제1항 중요도 평가 기준에 따라 클라우드 이용업무 중요도 평가를 진행해야 하며, 본 부록은 금융회사의 이해를 돕기 위한 예시로서 **의무 준수 대상이 아니며, 관련 중요도 평가 기준, 평가방법 및 배점 등은 세부 내용은 각 금융회사가 내부 업무 사정에 따라 수립**하여 적용하여야 함

참고 중요도 평가 방법 (예시)

(1단계 : 처리정보 분류) 처리정보를 고유식별정보, 개인신용정보, 금융정보, 업무정보, 공개정보로 분류

처리정보	유 형
고유식별 정보	법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 면허번호, 외국인등록번호 중 어느 하나에 해당하는 정보
개인신용 정보	기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보로서 해당 정보의 성명, 주민등록번호 및 영상 등을 통하여 특정 개인을 알아볼 수 있는 정보 또는 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보
금융정보	고객의 금융거래 관련 정보, 금융회사의 업무 기밀 정보, 전자금융거래 관련 고객 인증 정보 등 처리
업무정보	전자금융업무와 직접 관련은 없으나 금융회사의 통상적 업무 처리에 활용되는 내부 정보, 전자금융거래와 무관한 대고객 업무 관련 정보 예) 직원 정보, 일반 기획문서, 금융회사 홈페이지 정보, 쇼핑몰 정보 등
공개정보	대외 노출되어도 무방한 정보 예) 인터넷에서 수집한 데이터, 홍보자료 등

(2단계 : 업무 영향 평가) 평가항목별 평가 결과에 따른 점수 가중치*를 반영한 점수를 합산

* 평가항목 별 결과에 따른 점수 가중치

상	중	하	해당없음
배점 × 100%	배점 × 50%	배점 × 20%	배점 × 0%

□ **(평가기준)** 규모, 복잡성 등 클라우드를 통해 처리되는 업무의 특성 (배점 : 20점)

- 해당서비스와 연계된 외부 기관 수 (배점 : 5점)

상	중	하	해당없음
50개 이상 또는 10% 이상	20~49개 또는 5~9%	1~19개 또는 1~5%	0개 또는 1% 미만

참고 중요도 평가 방법 (예시)

- 해당서비스와 연결된 내부 시스템 수 (배점 : 5점)

상	중	하	해당없음
30개 이상 또는 10% 이상	10~29개 또는 5~9%	1~9개 또는 1~4%	0개 또는 1% 미만

- 업무기능 및 대상 (배점 : 5점)

상	중	하	해당없음
대고객 서비스 제공 업무 (직접이용)	금융상품 및 대외계 등 연계 업무 (간접이용)	서비스 지원 업무	사내 후선 업무

- 직전 3개월 동안 일평균 서비스 접속자 또는 비율* (배점 :5점)
  * 3개월 일평균 서비스 접속자 수/전체 고객 수 또는 전체 임직원수
  * 신규서비스의 경우 해당없음

상	중	하	해당없음
30% 이상 또는 100만명	10~29% 또는 10만명	1~9% 또는 1만명	1% 미만 또는 1만명 미만

□ **(평가기준)** 클라우드컴퓨팅서비스 제공자로부터 제공받는 서비스가 중단될 경우 미치는 영향 (배점 : 30점)
- 업무에 미치는 영향도* (배점 : 10점)

  * 성능 결함 또는 장애 시 업무에 미치는 영향도

상	중	하	해당없음
업무 중단 등 심각한 영향	업무 지연 등 중대한 영향	이용 불편 등 경미한 영향	영향없음

- 중단에 따른 손해금액/사업 전체 매출 금액 비율* (배점 : 10점)
  * 성능 결함 또는 장애 시 발생되는 손해

상	중	하	해당없음
10% 이상 또는 5억원 이상	5~9% 또는 1~3억원	1~4% 또는 5천만원 ~1억원	1%미만 또는 5천만원 미만

- 비상대응계획 상의 복구 목표 시간(RTO) (배점 : 10점)

상	중	하	해당없음
3시간 이하	24시간 이하	48시간 이하	48시간 초과

참고 중요도 평가 방법 (예시)

□ **(평가기준)** 보안 침해 발생시 고객에게 미치는 영향 (배점 : 30점)
- 고객에게 직·간접적으로 미치는 영향 (배점 : 10점)

상	중	하	해당없음
자산손실, 개인신용정보 노출 등 심각한 영향 발생	신뢰도, 사회적 이미지 손상 등 중대한 영향 발생	업무 지연, 서비스 이용 불편 등 경미한 영향 발생	영향 없음

- 처리정보 유형에 따른 영향 (배점 : 20점)

상	중	하	해당없음
고유식별정보, 개인신용정보	금융정보	업무정보	공개정보

□ **(평가기준)** 여러 업무를 같은 클라우드컴퓨팅 제공자에게 위탁하는 경우 해당 클라우드 컴퓨팅서비스 제공자에 대한 종속 위험 (배점 : 10점)

- 동일 CSP에 대한 업무 의존도 (배점 : 5점)

상	중	하	해당없음
10개 이상	5~9개	1~4개	0개

- 클라우드 환경 구성 방식(멀티클라우드 등) (배점 : 5점)

상	중	하	해당없음
다수 사업자 기반 (실시간 동기화)	다수 사업자 기반 (백업환경)	단일 사업자 기반 (별도백업)	단일 사업자

□ **(평가기준)** 클라우드컴퓨팅서비스 이용에 대한 금융회사 및 전자금융업자의 내부통제 및 법규 준수 역량 (배점 : 10점)

- 법적 규제 및 보안요구사항 준수 요구 (배점 : 5점)

상	중	하	해당없음
법규 및 내부규정 준수 요구	법규 또는 내부규정 준수 요구	사업자가 수립한 정책 준수 요구	별도 준수 요구 없음

- 계약, 보안 등 요구사항 준수여부 관리 감독 수행 (배점 : 5점)

상	중	하	해당없음
연 2회 이상 수행	연 1회 수행	필요 시 수행	수행하지 않음

참고 중요도 평가 방법 (예시)

(3단계 : 최종 판단) 처리정보 유형에 따른 판단기준에 따라 중요업무 여부를 최종 판단

처리 정보 유형	업무 영향평가	최종 평가
고유식별정보 또는 개인신용정보	20점 이상	중요
	20점 미만	비중요
금융정보	40점 이상	중요
	40점 미만	비중요
업무정보	60점 이상	중요
	60점 미만	비중요
공개정보	80점 이상	중요
	80점 미만	비중요

참고 중요도 평가 사례

□ (1단계) 처리정보 분류

구분	분류결과		
	A서비스	B서비스	C서비스
처리정보	금융정보	개인신용정보	업무정보

□ (2단계) 업무 영향평가

평가기준	평가항목	평가결과		
		A서비스	B서비스	C서비스
규모, 복잡성 등 클라우드를 통해 처리되는 업무의 특성	해당서비스와 연계된 외부 기관 수	1	0	0
	해당서비스와 연결된 내부 시스템 수	1	1	1
	업무기능 및 대상	5	0	5
	직전 3개월 동안 일평균 서비스 접속자 비율	2.5	0	5
클라우드컴퓨팅서비스 제공자로부터 제공받는 서비스가 중단될 경우 미치는 영향	업무에 미치는 영향도	2	2	2
	중단에 따른 손해금액/사업 전체 매출 금액 비율	0	0	0
	비상대응계획 상의 복구 목표 시간(RTO)	10	0	0
보안 침해 발생시 고객에게 미치는 영향	고객에게 직·간접적으로 미치는 영향	10	0	2
	처리정보 유형에 따른 영향	10	4	4
여러 업무를 같은 클라우드 컴퓨팅 제공자에게 위탁하는 경우 해당 클라우드 컴퓨팅 서비스 제공자에 대한 종속 위험	동일 CSP에 대한 업무 의존도	5	20	2
	클라우드 환경 구성 방식 (멀티클라우드 등)	2	2.5	2
클라우드컴퓨팅서비스 이용에 대한 금융회사 및 전자금융업자의 내부통제 및 법규 준수 역량	법적 규제 및 보안요구사항 준수 요구	5	2.5	5
	계약, 보안 등 요구사항 준수여부 관리 감독 수행	5	2.5	2.5
합계		58.5	34.5	30.5

□ (3단계) 최종판단

○ 중요도 판단 결과

구 분	최종판단		
	A서비스	B서비스	C서비스
(1단계) 처리정보	금융정보	개인신용정보	업무정보
(2단계) 업무영향평가	58.5	34.5	30.5
(3단계) 최종 판단	**중요(58.5≧40점)**	**중요(34.5≧20점)**	비중요(30.5<60점)

※ 본 사례는 중요도 평가 방법 예시에 따라 가상의 서비스를 대상으로 모의 평가한 결과임

FSI FINANCIAL SECURITY INSTITUTE
금융미래를 열어가는 금융보안파트너

금융분야 클라우드컴퓨팅서비스 이용 가이드

부록 2

금융회사의 클라우드서비스 제공자 집중리스크 관리시 고려사항

1. 금융회사의 클라우드서비스 제공자 집중 리스크 관리시 고려사항
2. 국외 클라우드 서비스 제공자(제3자)에 대한 리스크 대응방안

1 금융회사의 클라우드서비스 제공자 집중 리스크 관리시 고려사항

금융분야에서는 전자금융감독규정 개정에 따른 클라우드 규제개선에 따라 **디지털 신기술**의 **도입·활용**이 **확산**될 것으로 **예상**됨

다만, **클라우드서비스**를 이용하는 금융회사에서는 **재해 및 재난, 장애(이하 '전산사고') 발생 등을 대비**하고, **안정적인 시스템 운영**을 위해 특정 클라우드서비스 제공자(제3자)에 대한 **집중 리스크**를 **고려**할 필요가 있음

특히, 금융회사가 **다수의 업무**를 **특정 클라우드서비스 제공자**를 통해서 **처리**할 경우, 전산사고 등으로부터 핵심업무가 중단되지 않도록 **아래의 사항**을 **고려할 것을 권고함**

- **클라우드 환경**의 특수성을 **고려**한 **업무지속성 확보방안** 및 **재해복구계획**을 **수립**하고 해당 계획의 **실효성 제고**를 위한 **다양한 모의훈련 실시**
- 클라우드를 통해 처리되는 **정보 및 업무**의 **중요성** 등을 **감안**하여 클라우드 이용부서 및 내부통제부서 등의 **주기적인 위험평가 실시**
- **클라우드서비스 제공자**에 대한 **업무**(시스템) **집중 리스크**를 정기적으로 **분석**하고 **다중 공급업체 전략 적용**(멀티 클라우드 등) **필요성 등**을 **검토**
- **전산사고 등**으로부터 **데이터**를 안전하게 **보존**하고, 업무지속성 확보를 위해 주 전산센터 및 재해복구센터 역할을 하는 **클라우드 전산센터**를 **일정거리 이상 원격지**에 **분산 구축**
- 클라우드서비스 제공자와의 **이용계약 체결시** 클라우드 전산센터의 전산사고 발생에 따른 **피해보상대책**(소비자피해보상 포함)의 **적정성**을 **검토**

2 국외 클라우드 서비스 제공자(제3자)에 대한 리스크 대응방안

가. 제3자 관리시 집중 리스크에 대한 평가 (영국)

- 국외에서는 모든 제3자 계약의 중요성을 평가하여 중요 아웃소싱을 식별하고 의존 위험과 집중 위험 등을 주기적으로 평가하도록 함
  - 아울러, 클라우드사업자 등 시스테믹 리스크를 가진 제3자는 중요 IT 서비스 제공자로 지정하여 감독당국이 직접 규제 수행을 검토

    ※ 영국 금융당국은 클라우드 제공자(CSP)와 같은 제3자의 시스테믹 리스크를 고려하여 일부 제3자를 지정하고 규제하는 방안을 검토중이라고 밝힘(로이터, '21.10월)

나. 아웃소싱 원칙 내 집중위험 (아웃소싱 원칙 개정, IOSCO)

- 복수의 금융회사가 의존하는 제품이나 서비스 설계의 잠재적 결함이 모든 사용자에게 영향을 미칠 가능성 존재
  - 복수의 회사가 사용하는 소프트웨어의 취약점으로 인해 모든 금융회사의 시스템이 영향을 받을 수 있으며,
  - 동일한 재해 복구 사이트 등에 의존하는 경우 비즈니스 연속성 유지를 위해 준비된 자원이 감소되거나 손상받을 수 있음

다. 클라우드 서비스의 제3자 의존위험 (클라우드 서비스의 제3자 의존성, FSB)

- 클라우드 활용이 특정업체에 집중됨으로 인해 효과적인 경쟁이 줄어듦에 따라 금융회사가 CSP를 쉽게 변경할 수 없게 되는 등 의존성이 과도해질 우려
  - 의존 위험은 금융안정성도 저해할 수 있음에 따라 금융회사는 혁신과 복원력 사이의 균형(Trade-off)을 따져 다중 공급업체(multi-vendor) 전략을 적용하는 등 조치*를 검토

    * 컨테이너화, 멀티 클라우드, 백업 및 다중화 등은 단일 장애 지점(single point of failure) 관련 위험을 관리하고 복원력을 증진시킬 수 있는 전략

라. 운영위험 관리 및 제3자 위험방지 요건 (클라우드 아웃소싱 가이드라인, ESMA)

금융회사가 클라우드 서비스를 이용할 경우 운영위험 관리 및 제3자 위험 방지를 위해 준수해야 하는 요건을 명시

- 비례성 원칙에 따라 중요 아웃소싱인 경우 보안조치 등을 강화하고 규모 및 복잡성이 적은 기업은 완화된 조치를 적용 가능

※ 집중위험이 확인될 경우 관할당국은 해당 위험을 모니터링하고 잠재적 영향을 평가

▶ 중요 클라우드 아웃소싱에 대한 요구사항

- 계약 관련 세부 정보 포함하여 아웃소싱 레지스터 등록
- 클라우드 아웃소싱 계약의 결과로 발생할 수 있는 위험 평가
- 동일한 CSP 사용으로 인한 집중 위험 발생 가능성 고려
- CSP에 대한 평판 분석 등 적합성 평가 실시
- 데이터 처리 및 저장 위치 등을 포함한 서면 계약 요건
- API 보안, 비즈니스 연속성 관리, 규정 준수 모니터링 수행
- 클라우드 아웃소싱 계약의 종료 가능 여부 평가
- 서브 아웃소싱 허용 여부를 고려한 아웃소싱 계약 체결
- 관할 당국에 클라우드 아웃소싱 계획 보고

참고 공급업체 의존 위험 최소화 사례 (자료제공: 가트너)

1. 개요

□ 미국의 금융회사인 AgCredit*은 SaaS 서비스 공급업체에 의존될 수 있는 위험을 사전에 해소하여 클라우드 투자 속도와 혁신의 이점을 동시에 가져감에 따라 해당 사례를 조사·분석

* 연간 수익 4억 달러(한화 약 5,000억원), 직원 수 약 500명 규모의 중견 금융회사

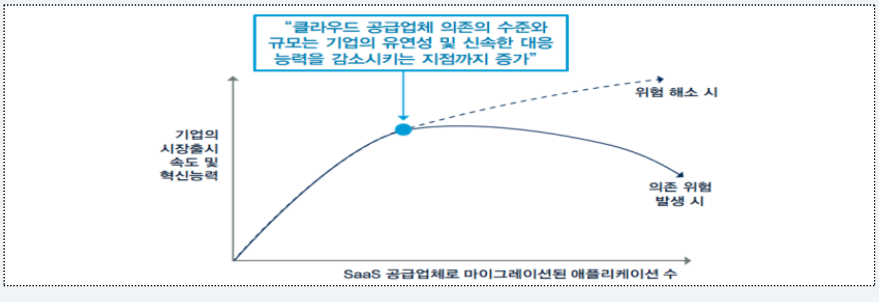
2. AgCredit의 사례 연구

(가) 공급업체 의존 원인 분석

□ AgCredit은 SaaS 공급업체와의 계약을 해지하는 것이 계약을 체결하는 것보다 복잡하고 어려우며 비용이 증가함을 인지

○ SaaS 공급업체에 의존되는 주요원인이 기업 데이터에 대한 공급업체의 과도한 통제 등이 원인이라는 사실을 파악

[SaaS 공급업체 의존이 속도에 미치는 영향(출처: AgCredit)]



참고 공급업체 의존 위험 최소화 사례 (자료제공: 가트너)

○ 데이터는 SaaS 공급업체의 형식에 맞게끔 변환됨에 따라 데이터 통제를 하기 위해 공급업체에 의존하게 되는 구조

[기업이 클라우드 공급업체에 의존되는 상황]

① 클라우드 공급업체는 기업의 데이터를 저장하고 불균형적으로 통제
② 클라우드 공급업체는 데이터 흐름을 관리할 수 있는 전문지식과 기능 소유
③ 클라우드 공급업체는 예외의 여지가 제한된 표준화된 계약서를 활용

□ 과거와는 달리 새로운 기능을 활용하지 못하는 등의 기회 비용이 발생할 경우 혁신이 지연되고 유연한 대처가 어려움에 따라 기업은 클라우드 이용을 지속적으로 확대하는 상황

○ 그러나 클라우드를 활용하면 온프레미스 환경 대비 혁신의 기회 비용에 이점이 있는 반면, 공급업체를 변경 또는 대체하는 경우 온프레미스 환경 보다 오히려 비용이 크게 증가

○ 이러한 이유로 기업은 클라우드 업체 변경이나 온프레미스 환경으로의 복원을 꺼리며 공급업체에 의존되는 결과 초래

(나) 공급업체 의존 해결책

□ AgCredit은 의존 위험에 따른 데이터 유출 등 사고 발생 시 평판 위험을 우려하여 다음과 같은 위험 해소방안을 추진

① 클라우드 공급업체와 계약하기 전 데이터 백업 전략 설계
- 공급업체에서 제공하는 API의 호환성을 검증하고 데이터 접근권을 확보

② 클라우드 공급업체와의 단일 연결지점 설계 및 내부관리
- 연결구간을 단일화(최소화)하고 데이터 교환 표준을 통합하여 복잡성 해소

③ 협력적인 분리를 보장하기 위해 사전에 출구조항을 협상
- 위약금이나 수수료 등 없이 관계를 종료할 수 있도록 강력한 계약 체결

□ AgCredit은 의존 위험 해소방안을 체계화하여 기업실사 시 사내 복원 가능성, 대체 가능성 등을 파악하는 노력을 감소시킴

금융분야 클라우드컴퓨팅서비스 이용 가이드

별첨

금융분야 망분리 및 클라우드 규제개선 관련 FAQ

1. FAQ 답변 활용 시 고려사항
2. SaaS 서비스 이용 시 고려사항
3. 금융분야 망분리 및 클라우드 규제개선 관련 FAQ

1 FAQ 답변 활용 시 고려사항

이 가이드 [별첨]은 금융위원회 「금융분야 망분리 및 클라우드 규제개선 관련 FAQ」 및 유권해석을 정리한 내용으로서,

금융회사 등에서 클라우드서비스를 이용함에 있어 적절한 보안 대책을 수립·운영하기 위해 이 [별첨]을 활용할 것을 권고함

2 SaaS 서비스 이용 시 고려사항

금융회사 등에서 SaaS 서비스 이용 시 아래 같은 사항에 대해 검토하는 것을 권고함

구분	판단 기준 예시(아래 요건을 모두 만족할 경우 감독규정 제14조의2 적용)
금융회사의 정보처리위탁	금융회사가 자신의 정보처리 업무를 제3자로 하여금 계속적으로 처리하는지 여부(정보처리위탁규정 제2조제6항) - 금융회사의 업무 관련 정보가 처리되지 않는 것이 분명한 경우는 제외 가능 - 금융회사에서 수행하는 정보처리 업무에 해당되지 않는 경우는 제외 가능 (금융회사의 업무 목적이 아닌 사적 목적의 단순 웹사이트 방문, 검색 등) - 제3자를 통한 계속적 정보처리가 아닌 경우는 제외 가능(일회성 처리 등)
클라우드 서비스	이용자 요구 등에 따라 IT자원을 신축적으로 이용(클라우드컴퓨팅법 §2·1)
	가상화 기술, 분산처리 기술 등의 적용(클라우드컴퓨팅법 §2·2) - 클라우드컴퓨팅기술(멀티테넌시 등)이 적용되지 않는 경우는 미해당
	소프트웨어 개발·배포·운영·관리 등을 위한 환경을 상용으로 제공하는 서비스 (클라우드컴퓨팅법 §2·3) - 불특정 다수가 웹을 통해 무료로 활용 가능하며, 소프트웨어 기반의 서비스가 아닌 일반적인 웹 기능만을 제공하는 웹사이트 등은 예외

3 금융분야 망분리 및 클라우드 규제개선 관련 FAQ

(FAQ) 1.「전자금융감독규정」 개정안에서 제시한 업무중요도 평가의 기준별 세부항목 예시

□ 개정안에 따르면 금융회사 등은 클라우드를 이용하려는 업무의 중요도를 제14조의2제1항제1호 기준에 따라 평가하여야 하며,

- ㅇ 세부 평가항목이나, 특정한 업무가 중요업무에 해당하는지 여부는 개별 금융회사 등이 자율적으로 결정할 사항입니다.
- ㅇ 다만, 규제 준수의 이해를 돕기 위해 중요도 평가 기준별 세부 평가항목을 다음과 같이 예시하므로 참고하시기 바랍니다.

〈 중요도 평가 기준별 세부 평가항목 예시 〉

중요도 평가 기준 (안 제14조의2제1항제1호)	세부 평가항목
규모, 복잡성 등 클라우드를 통해 처리되는 업무의 특성	해당 서비스와 연계된 외부 기관의 수
	해당 서비스와 연결된 내부 시스템의 수
	업무기능 및 대상(대고객 서비스, 금융상품 및 대외 연계, 서비스 지원업무, 후선업무 등)
	직전 3개월 동안 일평균 서비스 접속자 수
	자산 중요도 평가
클라우드컴퓨팅서비스 제공자로부터 제공받는 서비스가 중단될 경우 미치는 영향	업무에 미치는 영향도(성능 결함 또는 장애 시)
	중단에 따른 손해금액/사업전체 매출 금액 비율
	비상대응계획상의 복구목표 시간(RTO)
전자적 침해 행위 발생시 고객에게 미치는 영향	고객에게 직·간접적으로 미치는 영향
	개인신용정보 및 고유식별정보 처리 여부
여러 업무를 같은 CSP에게 위탁하는 경우 해당 CSP에 대한 종속 위험	동일 CSP에 대한 업무 의존도
	클라우드 환경 구성 방식(멀티클라우드 등)
클라우드컴퓨팅서비스 이용에 대한 금융회사 또는 전자금융업자의 내부통제 및 법규 준수 역량	법적 규제 및 보안 요구사항 준수 요구
	계약, 보안 등 요구사항 준수 여부 관리 감독 수행

(FAQ) 2. 클라우드 기반 소프트웨어(예 : 구독방식의 소프트웨어)에 대한 CSP 평가의 적용 여부

□ 금융회사 등이 SaaS 서비스를 업무에 활용하기 위해서는 감독규정 제14조2의 이용 절차를 모두 준수하여야 합니다.

- ㅇ 다만, 금융회사 등의 편의성을 제고하기 위해 업계 수요가 큰 SaaS 서비스에 대해 금융보안원이 CSP 대표평가를 수행하고 금융회사가 그 결과를 활용할 수 있도록 하겠습니다.

□ 한편, 금융회사 등이 클라우드 기반의 웹서비스를 단순 이용하는 경우*에는 감독규정 14조의2가 적용되지 않습니다.

* (예시) 기업 홍보를 목적으로 유튜브(Youtube) 및 페이스북(Facebook)에 자료를 게시하는 경우

※ '23년부터 SaaS 서비스에 대한 대표평가(금융보안원) 실시 예정

(FAQ) 3. 비중요업무에 대해 SaaS 형태의 소프트웨어를 사용하는 경우 망분리 예외 가능성

□ 금융위·금감원은 그간 금융권에 획일적으로 적용되어온 망분리 규제를 단계적으로 완화해나갈 계획*입니다.
* '클라우드 및 망분리 규제개선방안'('22.4.15일)

□ 구체적으로, 보안사고 최소화, 금융권의 보안역량 강화 필요성 등을 감안하여 다음과 같은 단계로 추진할 예정입니다.

❶ 금융규제 샌드박스 등을 통해 망분리 예외조치를 허용했던 "고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적"의 경우에 망분리 예외를 우선 허용*하겠습니다.
* 「전자금융감독규정」 개정안에 旣 반영

❷ 금융거래와 무관하고 고객거래정보를 다루지 않는 경우 샌드박스 제도를 통해 SaaS 형태의 소프트웨어 사용에 대한망분리 예외조치를 허용*하겠습니다.
* 단, 부가 조건을 통해 정보보호를 위한 보완 장치 마련 필요

❸ 비중요업무 등에 대한 망분리 예외조치의 성과, 금융회사 등의 책임성 확보 등을 감안하여,
- ①망분리 대상업무 축소, ②망분리 방식에 대한 선택권 부여 등을 검토할 계획입니다.

□ 특히, ❷와 관련해 내년 초에 금융협회를 통해 수요를 취합*한 후 규제 샌드박스를 통해 일괄적으로 처리할 예정입니다.
* 예시 : SaaS 형태의 소프트웨어, 인사 등 경영지원업무에 대한 망분리 예외

(FAQ) 4. 클라우드 간접이용(재위탁 등)의 경우에 「전자금융감독규정」상 클라우드 이용규제 적용여부

□ 금융회사 등의 정보처리업무를 수탁받은 업체가 수탁받은 정보 처리 업무를 클라우드를 이용하여 처리하려는 경우에도,
○ 금융회사 등은 「전자금융감독규정」의 클라우드 이용절차를 준수하여야 합니다.

□ 다만, 수탁업체의 클라우드 이용이 금융회사의 정보처리 위탁에 해당하지 않는 것으로 판단될 경우*에는 감독규정 제14조의2가 적용되지 않습니다.
* (예시) 수탁업체의 클라우드 이용이 금융회사의 정보처리와 관계없이 수탁업체 자신의 업무수행을 위한 것임이 분명한 경우

(FAQ) 5. 「전자금융감독규정」 개정에 따른 클라우드서비스 이용시 보고 절차의 변화

□ 감독규정 개정에 따른 금융회사 등의 클라우드 이용 보고절차는 다음과 같이 개선됩니다.

[기존 전자금융감독규정]

중요 업무	신규 이용 (감독규정 §14·2③)	7영업일 이전 사전보고
	중대한 변경 등 (감독규정 §14·2⑥)	7영업일 이내 사후보고
	일부/경미한 변경 등 (정보처리위탁규정 §7④1)	반기현황 사후보고
비중요 업무	신규 이용 (정보처리위탁규정 §7④2)	반기현황 사후보고
	중대한 변경 등 (감독규정 §14·2⑥)	7영업일 이내 사후보고
	일부/경미한 변경 등 (정보처리위탁규정 §7④1)	반기현황 사후보고

[전자금융감독규정 개정안]

중요 및 비중요 업무	신규 이용 및 중대한 변경 등 (감독규정 개정안 §14·2④)	3개월 이내 사후보고
	일부/경미한 변경 등 (정보처리위탁규정 §7④1)	반기현황 사후보고

※ 「감독규정개정안」제14조의2제4항에 따른 사후보고를 한 경우 「정보처리위탁규정」제7조제1항 내지 제3항 및 제4항제2호 본문에 따라 보고한 것으로 봅니다.

□ 또한, 旣이용 중인 클라우드 서비스를 통해 새로운 업무를 추가 처리하려고 할 때에도 제14조2 제4항 각 호에 해당하는 경우 보고가 필요합니다.

(FAQ) 6. 전자금융업자가 금융거래정보 이외의 정보처리업무를 위탁하는 경우에도 사후보고를 해야 하는지?

□ 전자금융업자는 現「전자금융감독규정」및 「정보처리업무위탁규정*」에 따라, 비중요업무에 대해 금융거래정보 이외의 정보를 클라우드로 처리하는 경우에는 별도 보고의무가 없습니다.

* 정보처리업무위탁규정 제7조제4항제2호 단서

○ 「전자금융감독규정」개정 이후에도 현행과 같이 비중요업무에 대해 금융거래정보 이외의 정보를 클라우드로 처리하는 경우 클라우드 이용보고의 대상이 아님을 알려드립니다.

※ (예시) 전자금융업자가 전자상거래 쇼핑몰 관련 비금융업무 등을 클라우드 시스템을 통해 처리하고자 하는 경우 등

금융분야 클라우드컴퓨팅서비스 이용 가이드

발행일 : 2022.11월

발행인 : 김 철 웅

발행처 : 금융보안원

주 소 : 경기도 용인시 수지구 대지로 132

FINANCIAL SECURITY INSTITUTE

FSI FINANCIAL SECURITY INSTITUTE

금융미래를 열어가는 금융보안파트너

안전하고 편리한 금융미래,
금융보안원이 열어가겠습니다.