

VERITAS™

금융위원회 전자금융 감독규정 정비 계획

Veritas Korea

국내 시중은행의 Public Cloud 소산관련 법령 해석 사례

금융감독규정에 있는 백업자료 소산방안 클라우드 전환 문의 합니다	
처리구분	완료
공개여부	Y
등록자	관리자
회신일	2023-04-11
첨부파일	<p> 법령해석 회신문(230058)-hwp</p> <p>안녕하세요 백업자료 소산 업무를 클라우드 전환 관련 문의 합니다</p> <p>당행의 백업단계가 아래와 같습니다</p> <p>1차) 운영 주센터 백업(VTL) 수행 2차) DR센터 백업 온라인 소산(VTL) 수행 3차) 운영 주센터 백업(VTL) --> PTL을 통한 --> 테이프 백업 수행 --> 해당 테이프를 내화 금고에 저장 관리 중</p> <p>"전자금융감독규정 제13조 8. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것"</p> <p>위 내용을 충족하기 위해 "DR센터 온라인 소산 + 테이프 미디어 테이프의 내화 금고 저장" 하는 방식으로 소산업무 운영 중인데요</p> <p>해당 백업자료 소산 업무 부분을 클라우드 저장 방식으로 전환 검토 중입니다 (기존 원격지 소산, 테이프 미디어 방식은 마운팅 --> 클라우드로 전환하여 운영 예정)</p> <p>클라우드 자체적으로 여러 데이터 센터에 중복 저장 관리 해주기 때문에 안전한 장소에 저장하는 감독규정을 만족할 수 있을 것으로 자체적으로 해석 하고 있습니다</p> <p>백업자료 소산 처리 부분을 기존의 테이프 미디어 저장 방식이 아닌 클라우드 저장 방식으로 전환 하는게 전자금융 감독규정의 안전한 백업소산 요건을 만족할 수 있는지 문의 드립니다</p> <p>감사합니다!!</p>

회답	<p>□ 귀하가 질의하신 내용만으로는 명확하게 판단하기 어려우나, 클라우드를 통한 전산자료의 소산이 전산자료가 안전지역에 중복 저장되는 방식인 경우 해당 규정을 준수한 것으로 사료됩니다.</p> <p>○ 다만, 이 경우 전자금융감독규정 제14조의2에 따라 클라우드컴퓨팅서비스 이용절차를 준수하여야 합니다.</p>
이유	<p>□ 금융회사 등은 「전자금융감독규정」제13조 제1항 제8호에 의거 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리 하여야 합니다.</p> <p>○ 이 경우 금융회사 등은 해당 소산 방식이 안전한 위치에 중복 저장되는지 여부를 자율적으로 판단하여 전산자료의 원격 안전지역 소산을 위해 클라우드를 활용하는 것이 가능합니다.</p> <p>* 전산자료가 물리적으로 떨어진 위치에 중복 저장되며 안전하게 보관·유지되는지 여부 등</p> <p>○ 다만, 금융회사 등이 전산자료 소산업무에 클라우드컴퓨팅서비스를 이용하는 경우 현행 「전자금융감독규정」제14조의2에 따라 이용절차 등을 준수하여야 하므로 이를 참고해주시기 바랍니다.</p> <p>□ 「전자금융거래법」제21조 제3항의 내용과 현행 규정에서 전산자료 소산에 대한 세부적인 내용을 정하고 있지 않는 바, 금융회사 등은 관련 규정을 준수하기 위한 보안기술 및 서비스 등을 자율적으로 선택하여 활용할 수 있습니다.</p>

[Source]

https://better.fsc.go.kr/fsc_new/replyCase/LawreqDetail.do?stNo=11&muNo=117&muGpNo=75&lawreqIdx=4200



법령해석문

[금융감독 법령 해석]

- 주센터와 DR센터간 VTL을 이용한 환경에서 원격복제를 수행중인 고객사
- 기존 원격지 DR 및 테이프 소산을 Public Cloud로 전환 하여도 금융 감독 규정을 만족할 수 있는지 문의
- 법령의 해석 및 답변은 “클라우드를 통한 전산자료의 소산이 전산자료가 안전지역에 중복 저장되는 방식인 경우 해당 규정을 준수하는 것으로 사료”
- Public Cloud 소산을 진행 해도 금융감독규정을 충족함

3 주요 강화 규정

(1) 재해복구센터 설치의무 확대(§23)

- (필요성) 카카오 데이터센터 화재 이후 재해발생시 재해복구센터를 이용한 신속한 업무연속성 회복 필요성이 확대
 - 현재, 재해복구센터 구축 의무가 없는 중소 금융회사, 전자금융업자*의 경우 화재 등 재해발생에 취약한 측면
 - * 현재, 중소기업회사 중 카드사, 중앙회 전산을 이용하는 일부 저축은행만이 DR센터 의무구축(그외 여전사·저축은행 및 전금업자는 의무 X)
 - (주요내용) 일정 기준*을 충족하는 ① 전금업자, ② 여전사(리소·합부금융·신기술) ③ 저축은행에 대해 DR센터 구축 의무화
 - * (기준안) ①총거래액 2조원 이상(36개사, (28개사 기구축)) ②총자산 2조원 이상(10개사, (6개사 기구축)) ③자체전산 저축은행(12개사, (12개사 기구축))
- ※ (참고) 기준안을 따를시, 58개사가 의무대상에 편입되나 이 중 47개사가 DR센터를 이미 구축하여 규제부담이 크지 않음

(3) 클라우드 아웃소싱 등 제3자 리스크

- “클라우드 이용절차(§14의2)”는 제3자 리스크 관리 관련 중요 규정으로 최근에 개정(22.12월)되었음을 감안하여 현행 유지
 - ※ 단, 보고의무 범위를 명확화(기존 클라우드 계약을 통해 신규업무를 처리하는 경우 등)하고, 양식·서류 등 세부 내용은 삭제 후 세칙에 위임
 - “외부주문(outsourcing) 기준(§60)”은 외부 주문·계약·위탁 등과 관련한 타 규정과 일부 내용이 중복되는 측면이 있으나,
 - 제3자 리스크 관리 측면에서 규정내용을 유지하되, 향후 클라우드·망분리 등과 함께 규제개선 방안 종합검토
- ☞ (참고) 클라우드 이용절차, 외부주문 기준 등의 경우, 향후 망분리 규제검토와 더불어 규율체계 합리화·효율화 검토

(2) 사이버 복원력(Cyber Resilience) 관련 조항

- “전산자료 보호대책(§13), 정보시스템 보호대책(§14)”은 카카오 화재로 촉발된 자료보호, 백업 등 중요성을 고려하여 유지
 - ※ 단, 전산자료 보호대책 분산된 규정은 통합(§13① i, ii, iv → §13① i 로 원칙화)하고, 중복된 기록 보존의무는 §14(정보처리시스템 보호대책)로 일원화
- “비상대책 수립·운용(§23), 비상훈련(§24)”은 장애·재해시 신속한 복구시간설정* 등 운영복원력 관련 핵심조항으로 현행 유지
 - ※ 단, 지나치게 세부적인 사항(§23.② i~iv, 비상지원인력 확보·운영 관련 세부사항 등)은 각 호를 삭제하고 해설서로 전환
- “해킹 방지(§15)” 조항에 사이버 복원력 개념 명시
 - * (현행) 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련 → (개선) 피해 최소화 및 신속한 복구를 위한 대책을 수립·운용

5 주요 조정 규정

(1) 사고보고 위반시 과태료 부과(§73) (※ §37의5로 이동)

- (필요성) 보안사고 등에 조기 대응을 위해서는 금융당국에 대한 신속한 사고보고 체계의 정립이 필요하나,
 - 침해사고 등에 대한 구체적인 통지 방법이 없고, 기타 사고 보고 미이행시 과태료 부과 근거가 없어 규범력 확보에 애로
- (주요내용) 침해사고 등에 관한 구체적 통지 절차를 마련(§37의4)하고, 보고의무 위반시 과태료 부과가 되도록 조문 이동(§37의5)*
 - * 6장 보칙(§73)에 규정된 사고보고 규정을 3장 안전성 확보(§37의5)로 이동할 경우 사고보고 위반시 법률 §21.② 위반에 해당되므로 과태료 부과 가능

[전자금융 감독규정]

- DR센터의 설치 의무가 확대 되어, 총거래액 2조원 이상 전금업자, 여전사, 저축은행도 대상으로 삼음
- 사이버 복원력 관련 조항의 경우 운영복원력 관련 핵심 조항이 있어, 피해 최소화, 신속한 복구 대책 수립 및 운용 할 것을 명시
- 클라우드 아웃소싱의 제3자 리스크 관련 규율체계 합리화 및 효율화를 검토
- 보안사고등의 사고 보고 위반시 과태료 부과 가능하다는 항목 존재

VERITAS™

Thank You