
 금융위원회	보 도 자 료			 금융감독원
	보도	2016.6.30.(목) 조건 이후	배포	
책 임 자	금융위 전자금융과장 김 동 환(02-2100-2970)	담 당 자	김 영 민 사무관 (02-2100-2975)	
	금감원 IT금융정보보호단장 (대행) 김 윤 진(02-3145-7850)		구 원 호 팀장 (02-3145-7415)	

제 목 : “금융권도 클라우드를 활용할 수 있습니다”

-「전자금융감독규정 일부개정규정안」변경예고 (‘16.6.30~16.8.9(40일간))

<p>■ 금융권 클라우드 이용 활성화를 위해 관련 규제가 개선됩니다.</p> <ul style="list-style-type: none"> - 중요정보 처리시스템을 제외한 모든 시스템의 클라우드 이용 허용 - 클라우드 이용 시스템에 대해 물리적 망분리 등 규정 예외 적용 <p>■ 소비자 보호 강화를 위해 카드정보저장 PG업자의 책임보험 가입 금액 기준이 상향(1억 → 10억)됩니다.</p> <ul style="list-style-type: none"> - 반면, 핀테크 활성화를 위해 전자금융업자 건전성 기준은 개선됩니다.

1 개정 배경

- **클라우드(클라우드컴퓨팅 서비스) 등 새로운 IT 기술이 확산**되고, 핀테크 산업이 활성화됨에 따라 변화된 현실에 맞게 **관련규제를 합리적으로 개선**하고,
- **간편결제 활성화에 따른 소비자 보호 강화**, 보안위협 대응을 위한 **금융보안원의 역할 명확화** 등을 위한 제도개선 사항 반영

2 주요 개정 내용

< 클라우드 이용 활성화 >

□ 클라우드 이용 활성화를 위한 관련 규제 개선 (규정 §7의2)

- (현행) 정보보호의 중요성과 상관없이 금융회사의 모든 시스템에 대해 물리적 망분리 등 높은 수준의 보안 규제를 일률적으로 적용함에 따라,
 - 고객정보 보호와 무관한 시스템*도 클라우드 이용이 어려운 과도한 측면이 있었음

* 예) 상품개발, 리스크관리, 경영지원 등 고객정보를 처리하지 않는 시스템

- (개선) 개인신용정보 등 고객정보 처리시스템을 제외한 전산시스템에 대해서는 금융회사가 자율적으로 클라우드를 이용할 수 있도록 개선
 - 클라우드 이용 시스템에 대해서는 클라우드 활용을 어렵게 하는 물리적 망분리 등 일부 규제도 적용을 제외

※ 금융회사의 안전한 클라우드 이용을 지원하기 위해 클라우드 활용 및 관련 보안 대책 적용 예시 등을 담은 금융보안원 가이드라인 등 배포

[기대효과] A증권사는 빅데이터 기반의 통계·분석 시스템 신규 도입 방식으로 클라우드 이용을 검토하였으나 물리적 망분리 등 관련 규제로 인해 도입이 사실상 불가능하였음

→ 금융회사가 지정한 클라우드 활용 시스템의 경우 물리적 망분리 등 규제 적용 대상에서 배제함에 따라 해당 시스템을 클라우드로 도입 가능

⇒ 전산시스템을 직접 구입하는 것 대비 50% 이상의 비용절감 효과 기대

< 전자금융업 관련 제도 개선 >

① 카드정보저장 전자금융업자의 책임보험 금액 기준 상향 (규정 §5)

- (현행) 간편결제 서비스 제공 등을 위해 고객의 신용카드 등의 정보를 저장하는 PG업자에게도 일반 PG업자와 동일한 금액(1억)의 보험 가입 또는 준비금 적립 기준 적용

→ (개선) 카드정보저장 PG업자의 경우 실질적으로 거래 승인 기능을 수행하고 거래에 대한 책임도 부담하는 등 일반 PG업자에 비해 전자 금융사고 발생 시 보상 책임 범위가 크므로,

- 피해자에게 적절한 수준의 보상이 이루어 질 수 있도록 보험 가입 또는 준비금 적립 금액 기준 상향(1억 → 10억)

※ 카드사의 보험 가입 또는 준비금 적립 최소금액(10억)과 동일

② 금융사고 피해보상을 위한 준비금의 지급절차 마련 의무화 (규정 §5)

○ (현행) 전자금융사고 발생 시 피해보상을 위해 금융회사 등의 보험 가입 또는 준비금 적립을 의무화하고 있으나,

- 외부보험사가 지급하는 보험과는 달리 준비금의 경우 자체적으로 관리·지급함에 따라 신속한 보상이 이루어지지 못할 우려

→ (개선) 피해보상이 신속하게 이루어 질 수 있도록, 준비금을 적립하는 금융회사의 준비금 관리·지급 관련 절차 마련 의무화

③ 전자금융업자 안전자산 유지의무 기준 개선 (규정 §63)

○ (현행) PG업자 등에 대해 총자산 대비 안전자산*을 10% 이상 보유 하도록 규정하여, 통신사 등 전체 사업규모 대비 전자금융업 영업 비중이 낮은 경영 PG업자에게 과도한 규제로 작용

* 현금, A등급이상 회사채, 국채, 은행채 등 투자위험성이 낮은 자산

→ (개선) 동 규정의 규율 취지가 가맹점에 대한 미정산 잔액의 안정적 지급임을 고려, 안전자산 유지 기준을 “총자산대비 10%의 안전자산 보유” 또는 “미정산 잔액 대비 100%의 안전자산 보유”로 개선

[사례예시] 주력 사업분야 외 PG업을 겸업하는 B 전자금융업자의 경우, 주력 사업분야와 관련된 대규모 고정자산을 유지하고 있어 현행 총자산 대비 안전자산 기준 유지가 사실상 불가능

→ “총자산대비 10%의 안전자산 보유” 또는 “미정산 잔액 대비 100%의 안전자산 보유” 중 한 기준만 충족하면 되므로, 미정산 잔액 만큼의 안전자산 보유로 규정 준수 가능

< 침해사고 대응기관(금융보안원) 역할 명확화 >

① 금융권 통합보안관제 센터 운영 근거 명확화 (규정 §37의4)

- (현행) 침해사고 대응기관(금보원)에서 금융권 보안성 확보를 위해 금융권 통합보안관제*업무를 수행중이나,

- * 사이버 공격 시도를 실시간으로 탐지.분석하고 이를 전체 금융회사에 공유하여 사이버 공격을 사전 차단하는 체계

- 현행 규정 상 침해사고대응기관의 업무에는 포함되지 않아 관제업무의 안정적 수행을 위한 법령상 근거 미흡

→ (개선) 침해사고대응기관의 업무에 금융권 통합보안관제 센터 운영을 추가하여 안정적 관제업무 수행 근거 마련

② 금융회사 사용 소프트웨어 취약점 조사.분석 근거 마련 (규정 §37의4)

- (현행) 최근 보안 소프트웨어 취약점을 이용한 보안업체 대상 해킹 사고* 및 이를 이용한 금융권 침해시도 등 발생

- * I사 코드서명 인증서 유출 사고, N사 솔루션 취약점 이용 해킹 사고 등

- 금융보안원이 이러한 침해시도를 사전에 탐지.차단할 수 있도록 금융회사 보안 소프트웨어 취약점 조사.분석 등의 수행을 위한 근거 마련 필요

- ※ 금융보안원은 I사 사고 사실을 최초 발견하고 해당 회사 통보 등 초동조치를 수행 하였으나, 소프트웨어에 대한 조사.분석을 위한 근거 규정이 없어 소프트웨어 취약점을 이용한 침해시도의 선제적 대응에 애로

→ (개선) 침해사고대응기관(금보원)이 금융회사가 사용중인 소프트웨어를 조사.분석할 수 있는 근거 마련

[사례예시] 금융보안원은 악성코드 발견을 통해 보안업체인 I사 사고 사실을 최초 발견하고 해당 회사 통보 등 초동조치를 수행

→ 금융권에서 사용중인 소프트웨어를 조사.분석하여 사고로 이어질 수 있는 취약점을 사전에 발견.대응하는 등 소프트웨어 취약점을 사용한 침해시도의 선제적 대응 가능

3 향후 추진계획

- 규정변경예고 : '16.6.30 ~ '16.8.9 (40일간)
- 규정변경예고, 규제심사를 거쳐 '16.9월 금융위에서 의결

※ 개정안의 세부내용은 다음에서 확인할 수 있습니다.

금융위원회(www.fsc.go.kr) → 지식마당 → 법령정보 → 입법예고/규정변경예고

 공공누리 공공저작물 자유이용허락	 출처표시	본 자료를 인용 보도할 경우 출처를 표기해 주십시오. http://www.fsc.go.kr	금융위원회 대 변 인 prfsc@korea.kr	 넓게 듣겠습니다 바르게 알려겠습니다
--	---	---	-------------------------------	--