대통령령 제 호

전자금융감독규정 일부개정규정안

전자금융감독규정 일부를 다음과 같이 개정한다.

제6조제1항제1호를 다음과 같이 한다.

1. 「전자서명법」 제2조제2호에 따른 전자서명으로 다음 각 목의 요건이 구비된 전자서명을 한 전자문서

가. 전자서명을 생성하기 위하여 이용하는 전자적 정보(이하 "전자서명생성정보"라 함)가 본인에게 유일하게 속할 것

나. 전자서명 당시 본인이 전자서명생성정보를 지배·관리하고 있을 것

다. 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것

라. 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것

제24조제1항 중 "제23조제9항에"를 "제23조제10항에"로 한다.

제34조를 다음과 같이 한다

제34조(전자금융거래 시 준수사항) 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.

1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다)

2. 전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌 개설, 중요거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우, 동 서비스를 제공할 수 있도록 시스템을 갖출 것

3. 전자금융거래에 사용되는 접근매체를 발급받기 위해서는 반드시 실명확인 후 교부할 것.

4. 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려할 것

5. 금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

제36조제1항 중 "정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행하고자 하는 경우 금융감독원장이 정하는 기준과 절차에 따라 보안성심의를 실시하여야 한다."을 "다음 각 호의 행위를 하고자 하는 경우 금융감독원장이 정하는 기준과 절차에 따라 보안성심의를 실시하여야 한다."로 하고 다음 각 호를 신설한다.

1. 정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행

2. 복수의 금융회사 또는 전자금융업자가 공동으로 전자금융거래 관련 표준을 제정

제36조제2항 본문 중 "신규 전자금융업무가 제공 또는 시행된"을 "제1항 각

호의 행위를 수행한”으로 하고, 단서에서 “다만, 신규 ”를 “다만, 제1항제1호에 따른 보안성심의의 경우 신규”로 하며 동조 제3항에서 “신규 전자금융업무의 보안수준”을 “보안수준”으로 하고, 동조 제4항에서 “기관은 자체 ”를 “ 기관은 제1항제1호에 따른 자체”로 한다.

제37조의2제2항 중 “「정보통신산업 진흥법 시행규칙」 제7조의 지식정보보안 컨설팅전문업체”를 “「정보보호산업의 진흥에 관한 법률 시행규칙」 제8조의 정보보호 전문서비스 기업”으로 한다 .

제37조의3제1항제2호를 다음과 같이 한다.

2.「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호전문서비스 기업

제42조의2를 다음과 같이 신설한다.

제42조의 2(거래금액 기준)

① 법 제30조제3항제1호에서 “금융위원회가 정하는 기준”이라 함은 당해 전자금융업에 대한 분기별 결제대행금액(이용자가 지급한 재화 및 용역의 매출총액), 결제대금예치금액 또는 전자고지결제금액이 30억원 이하에 해당하는 경우를 말한다.

② 법 제30조제4항에서 “금융위원회가 정하는 기한”이라 함은 신고한 때로부터 6월 이내를 말한다.

③ 등록 자본금 초과시 신고와 관련한 절차 및 방법 등 세부사항은 금융감독원장이 정하는 바준에 따른다.

별표 제1호 서식을 삭제한다.

부 칙

이 규정은 2016년 6월 30일부터 시행한다.

신・구조문대비표

현 행	개 정 안
제6조(추심이체 출금 동의의 방법 등) ① 시행령 제10조제1호에서 "금융위원회가 정하여 고시하는 전자문서"라 함은 다음 각 전자문서을 말한다.	제6조(추심이체 출금 동의의 방법 등) ① ----------.
1. 공인전자서명한 전자문서	1. 「전자서명법」 제2조제2호에 따른 전자서명으로 다음 각 목의 요건이 구비된 전자서명을 한 전자문서 가. 전자서명을 생성하기 위하여 이용하는 전자적 정보(이하 "전자서명생성정보"라 함)가 본인에게 유일하게 속할 것 나. 전자서명 당시 본인이 전자서명생성정보를 지배·관리하고 있을 것 다. 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것 라. 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것
2. ~3. 삭제 <2015.3.18.>	2. ~3 (현행과 같음)
③~④ (생략)	③~④ (현행과 같음)

제24조(비상대응훈련 실시) ① 금융회사 또는 전자금융업자는 제23조제4항에 따른 행동매뉴얼 또는 같은 조 제5항에 따른 비상대책에 따라 연 1회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고하여야 한다. 이때, 제23조제9항에 따른 재해복구전환훈련을 포함하여 실시할 수 있다. ②~③ 생략	제24조(비상대응훈련 실시) ① ---------- 제23조제10항에 ---------- ②~③ 생략
제34조(전자금융거래 시 준수사항) ① 금융회사 또는 전자금융업자는 다음의 경우를 제외하고는 전자자금이체 시 보안카드를 포함한 일회용 비밀번호를 적용하여야 한다. 1. 자동화기기(CD/ATM)를 이용한 자금이체의 경우 2. 제휴 금융회사에서 실명 확인 후 개설된 증권계좌와 연계된 본인명의의 실명확인 계좌로 이체하는 경우 3. 「자본시장과 금융투자업에 관한 법률」에 의한 투자매매업자・투자중개업자를 방문하여 등록한 실명 확인된 본인명의 계좌로 이체하는 경우 4. 신용카드 대출서비스를 실명확인된 본인명의 계좌로 이체	제34조(전자금융거래 시 준수사항) 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다. 1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다) 2. 전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌 개설, 중요거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우,

하는 경우

5. 보험회사의 보험금, 대출금 등을 실명 확인된 본인명의의 보험료납입 계좌로 이체하는 경우

6. 법인이 금융회사와 연결된 전용회선을 이용하여 전자자금이체를 하는 경우

7. 등록금, 원서접수비 등 본인확인이 가능하고 입금계좌가 지정되어 있는 경우

8. 그 밖에 금융감독원장이 필요하다고 인정하는 경우

② 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.

1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다)

2. 전자금융사고를 예방하기 위동 서비스를 제공할 수 있도록 시스템을 갖출 것

3. 전자금융거래에 사용되는 접근매체를 발급받기 위해서는 반드시 실명확인 후 교부할 것.

4. 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려할 것

5. 금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

② 삭 제

하여 비대면 전자금융거래를 허용하지 않는 계좌 개설, 중요거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우, 동 서비스를 제공할 수 있도록 시스템을 갖출 것

3. 전자금융거래에 사용되는 일회용 비밀번호(OTP를 포함한다. 이하 이 조에서 같다) 등의 접근매체를 발급받기 위해서는 반드시 본인 실명증표를 확인한 후 교부할 것. 단, 이용한도가 <별표 3>에서 정하는 금액 미만으로 제한된 직불전자지급수단의 경우 「전자서명법」에 의한 공인인증서와 일회용 비밀번호 등 복수의 본인확인 수단을 통해 본인확인 후 교부할 수 있다.

4. 일회용 비밀번호 등 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려할 것

5. 금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램

(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것	
제36조(자체 보안성심의) ① 금융회사 또는 전자금융업자는 정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행하고자 하는 경우 금융감독원장이 정하는 기준과 절차에 따라 보안성심의를 실시하여야 한다.	제36조(자체 보안성심의) ① 금융회사 또는 전자금융업자는 다음 각 호의 행위를 하고자 하는 경우 금융감독원장이 정하는 기준과 절차에 따라 보안성심의를 실시하여야 한다. 1. 정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행 2. 복수의 금융회사 또는 전자금융업자가 공동으로 전자금융거래 관련 표준을 제정
② 금융회사 또는 전자금융업자는 제1항에 따른 심의(이하 "자체보안성심의"라 한다)를 마친 후 신규 전자금융업무가 제공 또는 시행된 날로부터 7일 이내에 금융감독원장이 정하는 자체 보안성심의 결과보고서를 금융감독원에 제출하여야 한다. 다만, 신규 전자금융업무가 제공 또는 시행된 날을 기준으로 과거 1년 이내에 전자금융사고가 발생하지 않은 기관으로서 금융감독원장이	② 금융회사 또는 전자금융업자는 제1항에 따른 심의(이하 "자체보안성심의"라 한다)를 마친 후 제1항 각 호의 행위를 수행한 날로부터 7일 이내에 금융감독원장이 정하는 자체 보안성심의 결과보고서를 금융감독원에 제출하여야 한다. 다만, 제1항제1호에 따른 보안성심의의 경우 신규 전자금융업무가 제공 또는 시행된 날을 기준으로 과거 1년 이내에 전자금융사고가 발생하지 않은 기

정하는 기준에 해당하는 금융회사 또는 전자금융업자는 그러하지 아니하다.	관으로서 금융감독원장이 정하는 기준에 해당하는 금융회사 또는 전자금융업자는 그러하지 아니하다.
③ 금융감독원장은 제2항에 따라 제출받은 자체 보안성심의 결과보고서를 검토한 결과, 신규 전자금융업무의 보안수준이 충분하지 않다고 인정되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다	③ 금융감독원장은 제2항에 따라 제출받은 자체 보안성심의 결과보고서를 검토한 결과, 보안수준이 충분하지 않다고 인정되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다
④ 제2항 및 제3항에도 불구하고 다음 각 호의 기관은 자체 보안성심의 결과보고서의 제출을 하지 아니할 수 있다. 1. 「우체국예금·보험에 관한 법률」에 의한 체신관서 2. 「새마을금고법」에 의한 새마을금고 및 새마을금고중앙회 3. 「한국수출입은행법」에 따른 한국수출입은행 4. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관	④ 제2항 및 제3항에도 불구하고 다음 각 호의 기관은 제1항제1호에 따른 자체 보안성심의 결과보고서의 제출을 하지 아니할 수 있다. 1. 「우체국예금·보험에 관한 법률」에 의한 체신관서 2. 「새마을금고법」에 의한 새마을금고 및 새마을금고중앙회 3. 「한국수출입은행법」에 따른 한국수출입은행 4. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등) ① (생략) ② 금융회사 및 전자금융업자는 취약점 분석·평가를 위하여 정보	제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등) ① (생략) ② 금융회사 및 전자금융업자는 취약점 분석·평가를 위하여 정보

보호최고책임자(정보보호최고책임자가 없는 경우 최고경영자가 지정한다)를 포함하여 5인 이상으로 자체전담반을 구성하여야 하며, 구성원 중 100분의 30 이상은 「정보통신산업 진흥법 시행규칙」 제7조의 지식정보보안 컨설팅전문업체 지정기준에서 정한 고급 기술인력 이상의 자격을 갖춘 자이어야 한다. 다만, 제37조의3제1항에 따른 평가전문기관에 위탁하는 경우에는 자체전담반을 구성하지 아니할 수 있다. ③~⑤ (생략)	보호최고책임자(정보보호최고책임자가 없는 경우 최고경영자가 지정한다)를 포함하여 5인 이상으로 자체전담반을 구성하여야 하며, 구성원 중 100분의 30 이상은 「정보보호산업의 진흥에 관한 법률 시행규칙」 제8조의 정보보호 전문서비스 기업 지정기준에서 정한 고급 기술인력 이상의 자격을 갖춘 자이어야 한다. 다만, 제37조의3제1항에 따른 평가전문기관에 위탁하는 경우에는 자체전담반을 구성하지 아니할 수 있다. ③~⑤ (생략)
제37조의3(전자금융기반시설의 취약점 분석·평가 전문기관의 지정 등) ① 전자금융기반시설의 취약점 분석·평가를 위한 평가전문기관은 다음 각 호의 자로 한다. 1. 「정보통신기반 보호법」 제16조에 따라 금융분야 정보공유·분석센터로 지정된 자 2. 「정보통신산업 진흥법」 제33조에 따라 지정된 지식정보보안 컨설팅전문업체 3. 침해사고대응기관 4. 금융위원장이 지정하는 자	제37조의3(전자금융기반시설의 취약점 분석·평가 전문기관의 지정 등) ① 전자금융기반시설의 취약점 분석·평가를 위한 평가전문기관은 다음 각 호의 자로 한다. 1. 「정보통신기반 보호법」 제16조에 따라 금융분야 정보공유·분석센터로 지정된 자 2. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호전문서비스 기업 3. 침해사고대응기관 4. 금융위원장이 지정하는 자

②~③ (생략)	②~③ (좌동)
< 신 설>	제42조의 2(거래금액 기준) ① 법 제30조제3항제1호에서 “금융위원회가 정하는 기준”이라 함은 당해 전자금융업에 대한 분기별 결제대행금액(이용자가 지급한 재화 및 용역의 매출총액), 결제대금예치금액 또는 전자고지결제금액이 30억원 이하에 해당하는 경우를 말한다. ② 법 제30조제4항에서 “금융위원회가 정하는 기한”이라 함은 신고한 때로부터 6월 이내를 말한다. ③ 등록 자본금 초과시 신고와 관련한 절차 및 방법 등 세부사항은 금융감독원장이 정하는 바에 따른다.
<별지 제1호 서식> 작 성 자 : (직 위) 전화번호 : **보안성심의 신청서** 문서번호 20 . . . 수 신 참 조 제 목 보안성심의 요청	< 삭 제>

전자금융감독규정 제36조에 따라 붙임과 같이 보안성심의를 요청합니다.

붙 임 보안성심의 요청내용 1부. 끝.

○ ○ ○ ○ 기관 대표이사 (인)

(붙임)

보안성심의 요청내용

1. 업무명 :

2. 적용예정일 :

3. 업무개요(적용업무) :

4. 업무처리 절차 :

5. 시스템 및 네트워크 구성도 :

6. 관리체계 :
   □ 기기별 담당자
   □ 관련 규정 또는 지침

7. 전문처리(암호화) 절차 :

8. 보호대책(예)

구 분	보안 취약점	대 책	세부 내용	비 고
사용자 단말기	- 비밀번호 노출 - 비인가자 사용	- 비밀번호 출력방지 - OTP 사용	- 비밀번호 '*'표시 - 인증서버 및 인증프로그램 사용	-OTP 및 인증기능 별첨자료 참조
네트워크 구간				
DMZ구간				
금융기관 내부				

※ 기밀성, 무결성, 인증에 대한 방안 명시(사용알고리즘, 키관리 등)

9. 사용 시스템 현황

시스템명 (용도)	모델명 (제조사)	OS	시스템 제원				처리용량	신규 도입 여부
			CPU	메모리	DISK	캐쉬		

10. 통신 회선, 접속속도, 통신방식 및 적용 보안 솔루션

11. 금융기관 자체 보안성심의 결과

□ 20 년 월 일 완료 : 붙임 자체보안성심의 결과 참조

12. 담당자

소 속	직 위	이 름	담당업무	연락처	e-mail

※ 상기 항목중 보안성심의 요청 업무상 해당사항이 없는 항목은 제출 자료에 제외 가능

(별 첨)

○ 사업목적 및 추진계획
○ 사업계획서(신규사업에만 적용)
○ 기술제안요구서
○ 정보통신망 구성도
○ 자체보안대책 강구사항
- 보안관리수행체계(조직, 인원)
- 자체보안심의결과
- 정보통신시스템 설치장소의 보안통제현황(시스템 설치의 경우)
- 보안시스템, 단말기, 통신망, 고객정보 등의 보안요소별 보안대책
- 백업, 소산, 비상대책 등에 대한 대응방안
- 전산센터(백업센터)에 대한 가용성, 방호성 및 방재성 확보 현황 등

○ 기타(해당사항 있는 경우)
- 주센터 및 재해복구센터 위치
- 재해복구 목표시간 및 재해복구 대상 업무
- 재해복구 시스템 백업 및 복구 절차
- 주 센터 대비 전산시스템 용량(주요 전산시스템)

시스템명 *	주센터장비 제원 (CPU, 메모리, DISK 등)	재해센터장비 제원 (CPU, 메모리, DISK 등)	주센터대비 처리용량(%)	비 고

* 메인프레임, DB서버, 인터넷뱅킹서버, 주 Storage 등 주요 전산시스템

- 업무처리 절차 세부 내용
- 암호 및 인증 프로그램 세부 내용
- 암호장비 세부 제원
- 계약서 등