FINE 파인 금융소비자 정보포털

전자금융 감독규정 해설

2017. 5

FSS www.fss.or.kr
FINANCIAL SUPERVISORY SERVICE

금융감독원

※ 동 해설서는 전자금융감독규정 및 동규정 시행세칙의 내용을 관련 업무 종사자가 이해하기 쉽게 만든 내용으로, 개별 사안에 따라 행정관청의 유권해석은 본 해설서 내용과 상이할 수 있음을 알려드립니다.

머 리 말

2000.12월 각 금융업법에서 정하는 IT 및 전자금융거래에 대한 감독·검사를 위해 제정하여 운영해온 금융기관 전자금융업무 감독규정 및 시행세칙이 2007.1월 전자금융거래법의 제정·시행으로 법과 시행령에 위임한 사항을 반영하여 전면 개정됨으로써 비로소 일관된 전자금융거래 규제 체계가 마련되었고, 이용자 보호 및 전자금융서비스의 개선에도 많은 발전이 있었습니다.

그렇지만 그 이후 정보기술부문의 급속한 발전과 핀테크 등에 의한 새로운 전자금융서비스의 출현으로 IT 보안의 중요성이 더욱 부각되는 한편, 금융회사의 기술과 창의에 의한 혁신을 저해하지 않도록 규제체계를 개선할 필요성이 지속적으로 제기되어 왔습니다.

이에 금융위원회와 금융감독원은 전자금융거래법 시행 이후 지난 9년간 수차례에 걸쳐 전자금융거래 감독규정 및 시행세칙을 개정해 왔습니다. 예컨대, 2013년에는 IT부문의 보안을 근본적으로 향상시키기 위하여 망분리 요건을 의무화한 바 있으며, 2015년에는 자율보안체제 정착을 지원하고 혁신을 도모하고자 금융감독원에 의한 사전 보안성심의 제도와 공인인증서 의무사용 규제 등을 전면 폐지한 바 있습니다.

이러한 점을 감안하여 2007년 및 2009년에 발간하였던 전자금융감독규정 해설서를 그간 개정된 규정 내용 및 개정취지 등을 반영하고 전면 보강하여 다시 발간하고자 합니다. 아무쪼록 금융회사, 전자금융업자 및 이용자 여러분들의 이해에 도움이 되기를 바랍니다.

아울러 바쁜 업무 중에도 이 책을 집필한 구원호 팀장 이하 김동일·천윤정·노경록·최진영 선임조사역 그리고 내용 전반에 대해 의견을 주신 금융위원회 전자금융과 여러분들에게 진심으로 감사드립니다.

2017년 5월

금융감독원 IT·금융정보보호단 선임국장 최 성 일

목 차

FSS Financial Supervisory Service

5장 전자금융업의 허가와 등록 및 업무

6장 전자금융업무의 감독

7장 보 칙

전자금융감독규정 해설

1장 주요내용

제1장 주요내용

1. 연혁

2000.12. 금융기관 전자금융업무감독규정(금융감독위원회공고 제2000-117호) 제정
2001. 4. 금융기관 전자금융업무 감독규정 및 동 시행세칙 시행
2006.12. 전자금융감독규정(금융감독위원회공고 제2006-88호) 전부개정
2007. 1. 전자금융거래법(법률 제7929호, 2006.4.28. 제정) 시행
2007. 6. 전자금융감독규정(금융감독위원회공고 제2007-42호) 일부개정
2007. 9. 전자금융감독규정(금융감독위원회공고 제2007-120호) 일부개정
2008. 1. 전자금융감독규정(금융감독위원회공고 제2008-4호) 일부개정
2008. 4. 전자금융감독규정(금융위원회고시 제2008-8호) 일부개정
2008. 7. 전자금융감독규정(금융위원회고시 제2008-21호) 일부개정
2009. 8. 전자금융감독규정(금융위원회고시 제2009-50호) 타법개정
2010. 6. 전자금융감독규정(금융위원회고시 제2010-18호) 일부개정
2011.10. 전자금융감독규정(금융위원회고시 제2011-18호) 전부개정
2012.10. 전자금융감독규정(금융위원회고시 제2012-26호) 일부개정
2013. 6. 전자금융감독규정(금융위원회고시 제2013-20호) 일부개정
2013.12. 전자금융감독규정(금융위원회고시 제2013-39호) 일부개정
2013.12. 전자금융감독규정(금융위원회고시 제2013-44호) 일부개정
2015. 2. 전자금융감독규정(금융위원회고시 제2015-3호) 일부개정
2015. 3. 전자금융감독규정(금융위원회고시 제2015-7호) 일부개정
2015. 6. 전자금융감독규정(금융위원회고시 제2015-18호) 일부개정
2016. 6. 전자금융감독규정(금융위원회고시 제2016-24호) 일부개정
2016.10. 전자금융감독규정(금융위원회고시 제2016-37호) 일부개정

2. 기본개념

가. 전자금융거래의 정의

▣ 전자금융거래법은 전자금융거래를 '이용자가 전자금융업무(금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하는 것)를 비대면의 자동화된 방식으로 이용하는 거래'로 정의(제2조제1호)

※ 관계 법령

〈 법 〉

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. "전자금융거래"라 함은 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공(이하 "전자금융업무"라 한다.)하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.

나. 전자금융거래의 개념 요소

▣ 전자금융거래가 성립하기 위해서는 ㈀금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공("전자금융업무")하고 ㈁이용자가 비대면의 자동화된 방식으로 이를 이용하여야 함

- '전자금융업자'란 전자화폐의 발행 및 관리, 전자자금이체, 직불전자지급수단의 발행 및 관리, 선불전자지급수단의 발행 및 관리, 전자지급결제대행, 결제대금예치, 전자고지결제 등의 업무를 행하고자 금융위원회의 허가를 받거나 금융위원회에 등록을 한 사업자(금융회사 제외)를 말함

▣ 전자금융업무의 형태 : 금융상품 및 금융서비스를 '전자적 장치'를 통하여 제공

- 전자적 장치를 '통하여 제공'한다는 의미
  - 금융상품 및 서비스를 전자적 장치를 통하여 제공한다는 것은 이용자가 비대면으로 전자적 장치를 통하여 금융상품 및 서비스에 직접 접근할 수 있게 하는 정도에 이르러야 함을 의미
  - 단순히 전자적 장치를 금융회사 또는 전자금융업자의 업무에 활용하는 것만으로는 전자적 장치를 통한 제공에 해당되지 않음

– 예컨대 이용자가 금융회사 종사자와 대면하여 자금이체 지시를 한 경우에 금융회사 종사자가 거래지시 이행을 위하여 전자적 장치를 활용하는 경우, 이를 전자적 장치를 통한 제공이라 할 수 없음

※ 관계 법령

〈 법 〉

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

8. "전자적 장치"라 함은 전자금융거래정보를 전자적 방법으로 전송하거나 처리하는데 이용되는 장치로서 현금자동지급기, 자동입출금기, 지급용단말기, 컴퓨터, 전화기 그 밖에 전자적 방법으로 정보를 전송하거나 처리하는 장치를 말한다.

▣ 전자금융업무의 객체 : 금융상품 및 서비스

- 전자금융거래법은 '금융기관' 및 '전자금융업자'만을 정의하고 '금융상품 및 서비스' 개념에 대해 별도로 정하고 있지 않음
- '금융상품 및 서비스'에 대하여 다음과 같은 견해가 있을 수 있음
  - '금융'의 개념을 중시하여 금융기관 또는 전자금융업자가 자금의 융통과 관계된 상품 또는 서비스를 제공하는 경우에 국한하는 견해(협의의 개념)
  - 금융상품 및 서비스에 대한 정의를 별도로 하지 않은 점을 감안, '금융상품 및 서비스'란 금융기관 또는 전자금융업자가 제공하는 금융 관련 상품 및 서비스 일반을 의미한다고 해석하는 견해(광의의 개념)
- 전자금융업무의 범위는 전자금융거래의 대중화, 다양화 및 이용자 보호 등을 고려할 때 광의의 개념으로 보는 것이 타당함
  - 따라서 인터넷을 통한 신용정보, 자산보유 또는 거래내역 조회 서비스 제공도 전자금융업무에 해당함

▣ 접근매체

- 접근매체는 자동화기기, 전화기 및 컴퓨터 등의 전자적 장치를 이용하기 위한 수단이며, 전자적 장치를 통하여 전자금융거래에 이용되는 경우 접근매체의 효력이 발생됨
  - 예컨대 이용자가 예금통장(뒷면의 Magnetic Stripe)을 이용하여 자동화 기기에서 출금을 한 경우 예금통장은 접근매체로 간주됨

– 하지만 이용자와 금융회사(또는 전자금융업자) 간 전자금융거래계약이 체결되지 않아 전자적 장치를 통해 거래를 할 수 없는 예금통장의 경우 접근매체에 해당하지 않음(대법원 2010. 5. 27. 선고 2010도2940 판결 참조)

※ 관계 법령

〈 법 〉

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

10. "접근매체"라 함은 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다.
    가. 전자식 카드 및 이에 준하는 전자적 정보
    나. 「전자서명법」 제2조제4호의 전자서명생성정보 및 같은 조 제7호의 인증서
    다. 금융회사 또는 전자금융업자에 등록된 이용자번호
    라. 이용자의 생체정보
    마. 가목 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호

▣ 비대면성

● 금융기관 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하는 것

– 이러한 비대면성은 전자금융거래의 준비단계에서는 요구되지 않지만, 거래단계에서는 거래지시단계 및 거래처리 단계에서 모두 필요함

– 따라서 비대면성의 판단은 거래지시의 시점을 기준으로 하여야 하며, 준비단계에서 금융기관 또는 전자금융업자의 종사자와 대면했다는 사실은 전자금융거래의 비대면성 판단에 영향을 미치지 않음

▣ 자동화된 방식

● 전자금융거래는 이용자가 전자금융업무를 자동화된 방식으로 이용하는 거래임

– 전자적 장치를 통하여 제공되는 전자금융업무를 금융기관 또는 전자금융업자의 종사자와 대면하거나 의사소통을 하지 아니하고 이용하는 경우, 대체로 자동화된 방식의 이용이 될 것임

– 이러한 '자동성'의 요건도 비대면성 요건과 마찬가지로 전자금융거래의 준비단계에서는 요구되지 아니하며, 거래단계에서는 거래지시단계와 거래처리단계 전반에 걸쳐 요구된다고 할 것임

– 따라서 단일한 거래의 거래지시는 접근매체를 통하여 자동적으로 이루어지나, 거래의 완결과정에서 인위적인 판단이 개입하는 경우에는 전자금융거래라 할 수 없음[1)]

다. 적용 대상

※ 관계 법령

〈 법 〉

제2조(정의) 3. "금융회사"란 다음 각 목의 어느 하나에 해당하는 기관이나 단체 또는 사업자를 말한다.

가. 「금융위원회의 설치 등에 관한 법률」 제38조제1호부터 제5호까지, 제7호 및 제8호에 해당하는 기관
나. 「여신전문금융업법」에 따른 여신전문금융회사
다. 「우체국예금·보험에 관한 법률」에 따른 체신관서
라. 「새마을금고법」에 따른 새마을금고 및 새마을금고중앙회
마. 그 밖에 법률의 규정에 따라 금융업 및 금융 관련 업무를 행하는 기관이나 단체 또는 사업자로서 대통령령이 정하는 자

〈 시행령 〉

제2조(금융회사의 범위) 「전자금융거래법」(이하 "법"이라 한다) 제2조제3호마목에서 "대통령령이 정하는 자"라 함은 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 「한국산업은행법」에 따른 한국산업은행
2. 「중소기업은행법」에 따른 중소기업은행
3. 「한국수출입은행법」에 따른 한국수출입은행
4. 「산림조합법」에 따른 조합과 그 중앙회의 신용사업부문
5. 「농업협동조합법」에 따른 조합
6. 「수산업협동조합법」에 따른 조합
7. 「자본시장과 금융투자업에 관한 법률」에 따른 거래소
8. 「자본시장과 금융투자업에 관한 법률」에 따른 한국예탁결제원
9. 「금융지주회사법」에 따른 금융지주회사와 「금융지주회사법 시행령」 제2조제2항제1호에 해당하는 회사
10. 「보험업법」에 따른 보험협회와 보험요율산출기관
11. 「화재로 인한 재해보상과 보험가입에 관한 법률」에 따른 한국화재보험협회
12. 「자본시장과 금융투자업에 관한 법률」에 따른 한국금융투자협회
14. 「신용정보의 이용 및 보호에 관한 법률」에 따른 신용정보회사와 종합신용정보집중기관
15. 「금융회사부실자산 등의 효율적 처리 및 한국자산관리공사의 설립에 관한 법률」에 따른 한국자산관리공사
16. 「한국주택금융공사법」에 따른 한국주택금융공사
17. 「신용보증기금법」에 따른 신용보증기금
18. 「기술신용보증기금법」에 따른 기술신용보증기금
19. 「기술보증기금법」에 따른 기술보증기금

1) 예컨대 인터넷을 통한 대출 신청의 경우, 전자적 장치를 통하여 약관 등으로 정한 요건 심사가 자동적으로 이루어져 대출이 실행된다면, '대출'이라는 독립된 거래로서 전자금융거래에 해당하나, 단순히 신청만을 인터넷으로 접수하고 이에 대한 심사가 별도로 이루어진 후에 자금이체의 방법으로 대출이 실행된다고 하여도 이를 전자금융거래라 할 수 없음

전자금융감독규정 해설

2장 총 칙

FSS www.fss.or.kr
FINANCIAL SUPERVISORY SERVICE

제2장 총 칙

1. 규정 목적

〈 감독규정 〉
제1조(목적) 이 규정은 「전자금융거래법」(이하 "법"이라 한다) 및 동법 시행령(이하 "시행령"이라 한다)에서 금융위원회에 위임한 사항과 그 시행에 필요한 사항 및 다른 법령에 따라 금융감독원의 검사를 받는 기관의 정보기술부문 안전성 확보 등을 위하여 필요한 사항을 규정함을 목적으로 한다.

〈 시행세칙 〉
제1조(목적) 이 세칙은 「전자금융거래법」(이하 "법"이라 한다) 및 동법 시행령(이하 "시행령"이라 한다)과 「전자금융감독규정」(이하 "규정"이라 한다)에서 금융감독원장(이하 "감독원장"이라 한다)에게 위임한 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

▣ 전자금융거래법(이하 '법') 및 동법 시행령(이하 '시행령') 제정에 따라 동 법령에서 위임되거나 시행에 필요한 사항 등을 감독규정 및 시행세칙 등으로 정함

- 전자금융업자의 전자금융업 진입 요건 및 안전한 전자금융거래를 위해 필요한 정보기술부문의 안전성 기준 등을 중심으로 규정

▣ 전자금융감독규정은 전자금융거래법 및 동법 시행령에 근거하였고,

- 금융위 규정사항 중 중요한 의사결정이 요하지 않는 사항에 대하여 범위를 설정하여 감독원장에게 위탁하였으며(시행령 제30조), 동 사항에 대해 전자금융감독규정시행세칙으로 규정

※ 관계 법령

〈 시행령 〉

제30조(권한의 위탁) ① 금융위원회는 법 제48조에 따라 다음 각 호의 업무를 금융감독원장에게 위탁한다.

1. 법 제21조제2항에 따른 인증방법에 관한 기준의 설정

1의2. 법 제21조제4항에 따른 정보기술부문에 대한 계획의 접수

1의3. 법 제21조의3제1항에 따른 취약점 분석·평가 결과의 접수

1의4. 법 제25조에 따른 약관의 제정 및 변경 보고의 접수, 약관 변경의 권고

(이하 생략)

2. 용어의 정의

〈 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 정보처리시스템내 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.

〈 시행세칙 〉

제2조(정의) 이 세칙에서 별도로 정하지 아니한 용어는 법·시행령·규정에서 정하는 바에 따른다.

▣ 전자금융거래법 및 시행령에서 별도로 정의하지 않은 용어에 대해 정의를 규정

▣ 용어별 해설

- 정보보호시스템 : 정보처리시스템내 정보를 유출·위변조·훼손하거나 정보처리시스템의 정상적인 서비스를 방해하는 행위로부터 정보 등을 보호하기 위한 장비 및 프로그램으로 침입차단시스템(Firewall), 가상사설망(VPN:Virtual Private Network), 침입탐지시스템(IDS: Intrusion Detection System), 침입방지시스템(IPS: Intrusion Prevention System) 등이 있음

- 컴퓨터악성코드 : 컴퓨터에서 이용자의 허락 없이 스스로를 복사하거나 변형한 뒤 정보유출, 시스템 파괴 등의 작업을 수행하여 이용자에게 피해를 주는 프로그램

- 공개용 웹서버 : 인터넷 이용자들이 웹페이지를 자유롭게 보고 웹서비스(월드 와이드 웹을 이용한 서비스를 말한다)를 이용할 수 있게 해주는 프로그램이 실행되는 장치

※ 관계 법령

〈 시행령 〉

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. "전자금융거래"라 함은 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공(이하 "전자금융업무"라 한다)하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.
2. "전자지급거래"라 함은 자금을 주는 자(이하 "지급인"이라 한다)가 금융회사 또는 전자금융업자로 하여금 전자지급수단을 이용하여 자금을 받는 자(이하 "수취인"이라 한다)에게 자금을 이동하게 하는 전자금융거래를 말한다.
3. "금융회사"란 다음 각 목의 어느 하나에 해당하는 기관이나 단체 또는 사업자를 말한다.
   가. 「금융위원회의 설치 등에 관한 법률」 제38조제1호부터 제5호까지, 제7호 및 제8호에 해당하는 기관
   나. 「여신전문금융업법」에 따른 여신전문금융회사
   다. 「우체국예금·보험에 관한 법률」에 따른 체신관서
   라. 「새마을금고법」에 따른 새마을금고 및 새마을금고중앙회
   마. 그 밖에 법률의 규정에 따라 금융업 및 금융 관련 업무를 행하는 기관이나 단체 또는 사업자로서 대통령령이 정하는 자
4. "전자금융업자"라 함은 제28조의 규정에 따라 허가를 받거나 등록을 한 자(금융회사는 제외한다)를 말한다.
5. "전자금융보조업자"라 함은 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자 또는 결제중계시스템의 운영자로서 「금융위원회의 설치 등에 관한 법률」 제3조에 따른 금융위원회(이하 "금융위원회"라 한다)가 정하는 자를 말한다.
6. "결제중계시스템"이라 함은 금융회사와 전자금융업자 사이에 전자금융거래정보를 전달하여 자금정산 및 결제에 관한 업무를 수행하는 금융정보처리운영체계를 말한다.

7. “이용자”라 함은 전자금융거래를 위하여 금융회사 또는 전자금융업자와 체결한 계약(이하 “전자금융거래계약”이라 한다)에 따라 전자금융거래를 이용하는 자를 말한다.
8. “전자적 장치”라 함은 전자금융거래정보를 전자적 방법으로 전송하거나 처리하는데 이용되는 장치로서 현금자동지급기, 자동입출금기, 지급용단말기, 컴퓨터, 전화기 그 밖에 전자적 방법으로 정보를 전송하거나 처리하는 장치를 말한다.
9. “전자문서”라 함은 「전자문서 및 전자거래 기본법」 제2조제1호에 따른 작성, 송신·수신 또는 저장된 정보를 말한다.
10. “접근매체”라 함은 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다.
    가. 전자식 카드 및 이에 준하는 전자적 정보
    나. 「전자서명법」 제2조제4호의 전자서명생성정보 및 같은 조제7호의 인증서
    다. 금융회사 또는 전자금융업자에 등록된 이용자번호
    라. 이용자의 생체정보
    마. 가목 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호
11. “전자지급수단”이라 함은 전자자금이체, 직불전자지급수단, 선불전자지급수단, 전자화폐, 신용카드, 전자채권 그 밖에 전자적 방법에 따른 지급수단을 말한다.
12. “전자자금이체”라 함은 지급인과 수취인 사이에 자금을 지급할 목적으로 금융회사 또는 전자금융업자에 개설된 계좌(금융회사에 연결된 계좌에 한한다. 이하 같다)에서 다른 계좌로 전자적 장치에 의하여 다음 각 목의 어느 하나에 해당하는 방법으로 자금을 이체하는 것을 말한다.
    가. 금융회사 또는 전자금융업자에 대한 지급인의 지급지시
    나. 금융회사 또는 전자금융업자에 대한 수취인의 추심지시(이하 “추심이체”라 한다)
13. “직불전자지급수단”이라 함은 이용자와 가맹점간에 전자적 방법에 따라 금융회사의 계좌에서 자금을 이체하는 등의 방법으로 재화 또는 용역의 제공과 그 대가의 지급을 동시에 이행할 수 있도록 금융회사 또는 전자금융업자가 발행한 증표(자금을 융통받을 수 있는 증표를 제외한다) 또는 그 증표에 관한 정보를 말한다.
14. “선불전자지급수단”이라 함은 이전 가능한 금전적 가치가 전자적 방법으로 저장되어 발행된 증표 또는 그 증표에 관한 정보로서 다음 각 목의 요건을 모두 갖춘 것을 말한다. 다만, 전자화폐를 제외한다.
15. “전자화폐”라 함은 이전 가능한 금전적 가치가 전자적 방법으로 저장되어 발행된 증표 또는 그 증표에 관한 정보로서 다음 각 목의 요건을 모두 갖춘 것을 말한다.
    가. 대통령령이 정하는 기준 이상의 지역 및 가맹점에서 이용될 것
    나. 제14호 가목의 요건을 충족할 것
    다. 구입할 수 있는 재화 또는 용역의 범위가 5개 이상으로서 대통령령이 정하는 업종 수 이상일 것
    라. 현금 또는 예금과 동일한 가치로 교환되어 발행될 것
    마. 발행자에 의하여 현금 또는 예금으로 교환이 보장될 것
16. “전자채권”이라 함은 다음 각 목의 요건을 갖춘 전자문서에 기재된 채권자의 금전채권을 말한다.
    가. 채무자가 채권자를 지정할 것
    나. 전자채권에 채무의 내용이 기재되어 있을 것
    다. 「전자서명법」 제2조제3호의 공인전자서명이 있을 것
    라. 금융회사를 거쳐 제29조제1항의 규정에 따른 전자채권관리기관(이하 “전자채권관리기관”이라 한다)에 등록될 것

마. 채무자가 채권자에게 가목 내지 다목의 요건을 모두 갖춘 전자문서를「전자문서 및 전자거래 기본법」제6조제1항에 따라 송신하고 채권자가 이를 같은 법 제6조제2항의 규정에 따라 수신할 것

17. "거래지시"라 함은 이용자가 전자금융거래계약에 따라 금융회사 또는 전자금융업자에게 전자금융거래의 처리를 지시하는 것을 말한다.
18. "오류"라 함은 이용자의 고의 또는 과실 없이 전자금융거래가 전자금융거래계약 또는 이용자의 거래지시에 따라 이행되지 아니한 경우를 말한다.
19. "전자지급결제대행"이라 함은 전자적 방법으로 재화의 구입 또는 용역의 이용에 있어서 지급결제정보를 송신하거나 수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 것을 말한다.
20. "가맹점"이라 함은 금융회사 또는 전자금융업자와의 계약에 따라 직불전자지급수단이나 선불전자지급수단 또는 전자화폐에 의한 거래에 있어서 이용자에게 재화 또는 용역을 제공하는 자로서 금융회사 또는 전자금융업자가 아닌 자를 말한다.
21. "전자금융기반시설" 이란 전자금융거래에 이용되는 정보처리시스템 및「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조제1항제1호에 따른 정보통신망을 말한다.
22. "전자적 침해행위" 란 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 전자금융기반시설을 공격하는 행위를 말한다.

3. 전자금융보조업자

〈 감독규정 〉

제3조(전자금융보조업자의 범위) 법 제2조제5호에서 "금융위원회가 정하는 자" 라 함은 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 정보처리시스템을 통하여「여신전문금융업법」상 신용카드업자의 신용카드 승인 및 결제 그 밖의 자금정산에 관한 업무를 지원하는 사업자
2. 정보처리시스템을 통하여 은행업을 영위하는 자의 자금인출업무, 환업무 및 그 밖의 업무를 지원하는 사업자
3. 전자금융업무와 관련된 정보처리시스템을 해당 금융회사 또는 전자금융업자를 위하여 운영하는 사업자
4. 제1호 부터 제3호의 사업자와 제휴, 위탁 또는 외부주문(이하 "외부주문등" 이라 한다)에 관한 계약을 체결하고 정보처리시스템을 운영하는 사업자

▣ 금융회사 및 전자금융업자와 직접 계약을 체결하고 관련된 업무를 수행하는 사업자는 전자금융보조업자로 분류하여야 하나

- 이들 사업자와 재위탁 계약을 체결한 사업자들 중 전자금융거래와 직접적인 관련이 없는 단순 콜센터, DM 발송 업체 등은 제외
- 내부에 상주하지 않는 콜센터, 쇼핑몰, 외부통신회선 관리, IDC 등도 전자금융보조업자의 범위에 포함되지 않음

※ 전자금융보조업자 예시

서비스 형태	주요업체
VAN사업자	KICC, KSNet, KMPS 등
ATM관리 아웃소싱업체	NICE, 한네트, 웹캐시, 노틸러스효성 등
자금이체대행 PG	금융결제원 등
전자고지납부업체	한국인터넷빌링, 금융결제원 등
결제중계시스템 운영자	금융결제원, 한국예탁결제원 등
공동수탁기관	KOSCOM, 저축은행중앙회 등

▣ 전자금융거래와 관련하여 전자금융보조업자의 고의나 과실로 인한 손해에 대해서는 금융회사 또는 전자금융업자가 배상책임을 가짐(금융회사 등은 전자금융보조업자에 대해 구상 가능)

※ 관계 법령

〈 법 〉

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

5. "전자금융보조업자"라 함은 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자 또는 결제중계시스템의 운영자로서 「금융위원회의 설치 등에 관한 법률」 제3조에 따른 금융위원회(이하 "금융위원회"라 한다)가 정하는 자를 말한다.

〈 법 〉

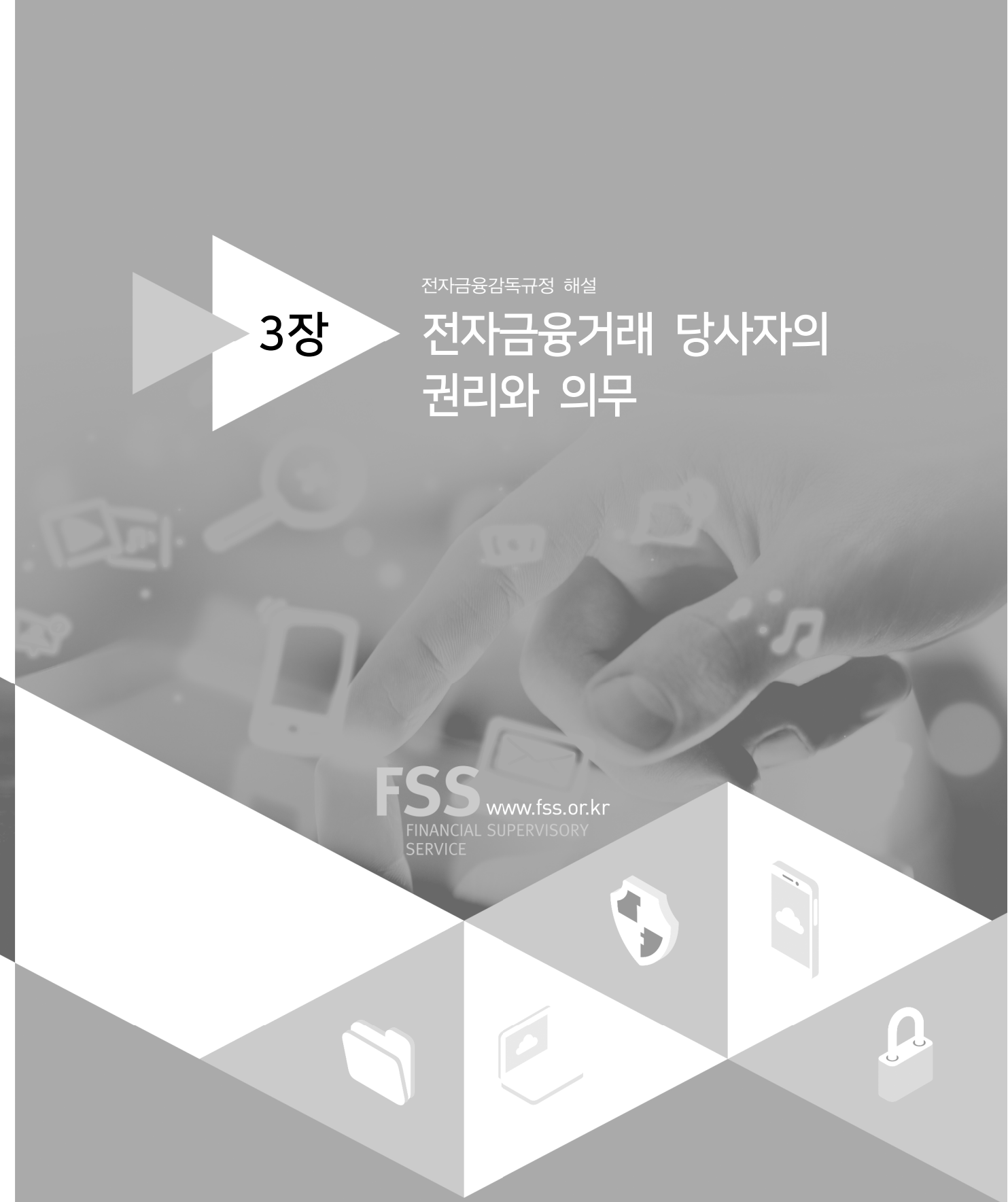
제11조(전자금융보조업자의 지위) ① 전자금융거래와 관련하여 전자금융보조업자(전자채권관리기관을 포함한다. 이하 이 장에서 같다)의 고의나 과실은 금융회사 또는 전자금융업자의 고의나 과실로 본다.

② 금융회사 또는 전자금융업자는 전자금융보조업자의 고의나 과실로 인하여 발생한 손해에 대하여 이용자에게 그 손해를 배상한 경우에는 그 전자금융보조업자에게 구상할 수 있다.

③이용자는 금융회사 또는 전자금융업자와의 약정에 따라 금융회사 또는 전자금융업자에게 행하는 각종 통지를 전자금융보조업자에게 할 수 있다. 이 경우 전자금융보조업자에게 한 통지는 금융회사 또는 전자금융업자에게 한 것으로 본다.

전자금융감독규정 해설

3장 전자금융거래 당사자의 권리와 의무



FSS www.fss.or.kr
FINANCIAL SUPERVISORY SERVICE

제3장 전자금융거래 당사자의 권리와 의무

1. 확인에 필요한 구체적인 거래 내용

〈 감독규정 〉
제4조(확인에 필요한 구체적인 거래내용) 시행령 제7조제4항제6호에서 "금융위원회가 정하여 고시하는 사항"이란 다음 각 호를 말한다.
1. 법 제8조에 따른 오류정정 요구사실 및 처리결과에 관한 사항
2. 전자금융거래 신청, 조건변경에 관한 내용

▣ 금융회사 또는 전자금융업자는 이용자가 자신의 전자금융거래 서비스에 대한 거래내용을 전자적 장치 등을 통해서 확인할 수 있도록 하여야 함

- 전자금융 거래내용에 대한 범위
  - 전자금융거래의 종류, 금액 및 전자금융거래의 상대방에 관한 정보
  - 전자금융거래의 거래일시, 전자적 장치의 종류 및 전자적 장치를 식별할 수 있는 정보 등
  - 이용자의 오류정정 요구사실 및 처리결과와 전자금융거래신청 및 조건변경에 관한 내용도 기록·보관하여야 함

▣ 해설

- 전자금융 거래확인에 필요한 시스템은 법에서 정해진 요건대로 반드시 갖추어야 함
- 많은 경우 장애나 오류가 발생하였음에도 이를 고객들에게 알리지 않거나, 법에서 정해진 내용이 제공되지 않을 경우 법적 책임을 지게 되는 경우가 있으므로 주의가 요구됨

2. 전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준

〈 감독규정 〉

제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준) ① 금융회사 또는 전자금융업자가 법 제9조 제4항에 따라 전자금융사고 책임이행을 위한 보험 또는 공제에 가입하는 경우 보상한도는 다음 각 호에서 정하는 금액 이상이어야 한다.

1. 「금융위원회의 설치 등에 관한 법률」 제38조제1호(다만, 「은행법」에 의한 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다) 및 제7호의 회사, 「전자금융거래법 시행령」 제2조제2호의 회사 : 20억원
2. 「금융위원회의 설치 등에 관한 법률」 제38조제8호의 회사, 「전자금융거래법」 제2조제3호나목(신용카드업자에 한한다) 및 다목의 회사, 「전자금융거래법 시행령」 제2조제1호의 회사, 「은행법」에 따른 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점 : 10억원
3. 「금융위원회의 설치 등에 관한 법률」 제38조제2호(다만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 : 5억원
4. 제1호 부터 제3호 이외의 금융회사 : 1억원. 다만, 제1호 부터 제3호 이외의 금융회사들이 관련 법령에 의해 당해 금융회사를 구성원으로 하는 금융회사를 통해 전자금융거래 관련 정보기술부문의 주요부분을 공동으로 이용하는 경우, 정보기술부문의 주요부문을 제공하는 금융회사가 공동 이용 금융회사 전체의 사고를 보장하는 내용으로 제2호의 금액(시행령 제2조제5호의 금융회사는 제1호의 금액) 이상의 보험 또는 공제에 가입하면 공동 이용 금융회사는 본호의 보험 또는 공제에 가입한 것으로 본다.
5. 법 제28조제2항제1호 및 제2호의 전자금융업자 : 2억원
6. 법 제28조제2항제4호의 전자금융업자 중 제1호 또는 제2호에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자 : 10억원
7. 제5호, 제6호 이외의 전자금융업자 : 1억원

② 금융회사 또는 전자금융업자가 전자금융사고 책임이행을 위한 준비금을 적립하는 경우에는 제1항 각 호에서 정한 금액 이상의 금액을 보유하고 책임이행이 신속히 이루어 질 수 있도록 준비금 관리 및 지급에 관한 내부 절차를 수립하여 운영하여야 한다.

③ 금융회사 또는 전자금융업자가 보험 또는 공제 가입과 준비금 적립을 병행하는 경우 보험 또는 공제의 보상한도는 제1항에서 정한 금액에서 준비금 적립액을 차감한 금액 이상으로 한다.

④ 제1항 부터 제3항의 규정은 전자금융업무를 취급하지 않는 금융회사에 대하여는 적용하지 아니한다.

▣ 전자금융거래 서비스를 제공하는 금융회사 및 전자금융업자는 보험(공제) 또는 준비금을 적립해야 함

- 금융회사 및 전자금융업자에 대한 보험금액은 전자금융거래액 및 과거 전자금융사고 등을 참고하여 권역별로 결정함

▣ 해설

- 전자금융업무를 취급하지 않는 금융회사는 보험 등에 가입할 의무 없음

- 복수 업종의 전자금융업무를 하는 경우 각 해당 보험금액을 합산하여 준비금 적립 또는 보험가입
- 금융회사가 보험 대신 준비금을 적립할 경우 동사가 적립해야 할 적립금액은 보험금액과 일치함
- 보험(공제)과 준비금을 병행하는 경우에는 각각의 합이 기준금액을 충족하면 가능
- 단위조합 등이 전자금융거래 관련 정보기술부문의 주요 부분을 공동으로 이용하여, 현행 보험제도 하에서 공동 이용 금융회사 전체의 사고를 보장하는 내용으로 책임보험에 가입하는 것은 가능토록 함
- 신용카드, 직불카드 등 거래지시에 사용되는 접근매체 정보를 저장하여 전자지급결제 대행업무를 수행하는 경우 10억원(제1항제6호)

3. 추심이체 출금동의의 방법

〈 감독규정 〉

제6조(추심이체 출금 동의의 방법 등) ① 시행령 제10조제1호에서 "금융위원회가 정하여 고시하는 전자문서"라 함은 다음 각 전자문서을 말한다.

1. 「전자서명법」 제2조제2호에 따른 전자서명으로 다음 각 목의 요건을 구비된 전자서명을 한 전자문서
   가. 전자서명을 생성하기 위하여 이용하는 전자적 정보(이하 "전자서명생성정보"라함)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. 「전자서명법」 제2조제2호에 따른 전자서명으로 다음 각 목의 요건을 구비된 전자서명을 한 전자문서
   가. 서명 전 실명증표를 통해 본인확인
   나. 전자문서가 생성된 이후 서명자가 지급인 본인임을 확인 가능
   다. 전자서명 및 전자문서에 대한 위변조 여부 확인이 가능
   라. 전자문서를 고객에게 전송한 이후 고객이 취소할 수 있는 충분한 기간 부여
3. 삭제

② 시행령 제10조제1호 및 제2호에서 "금융위원회가 정하는 방법"이라 함은 다음 각 호의 방법을 말한다.

1. 전화 녹취
2. 음성응답 시스템(Audio Response System : ARS)

③ 지급인(출금계좌의 실지명의인을 포함한다)이 출금의 동의를 해지하는 경우에도 제1항 및 제2항의 규정을 준용한다.

④ 금융회사·전자금융업자 또는 수취인은 제1항 각 호의 출금 동의의 방법을 운용함에 있어 다음 각 호의 어느 하나에 해당하는 사실을 확인하여야 한다.

1. 지급인과 추심이체 출금계좌 실지명의인이 동일인인 사실
2. 지급인과 추심이체 출금계좌 실지명의인이 동일인이 아닐 경우에는 지급인이 당해 계좌에서 출금할 수 있는 권한을 보유하고 있는 사실

▣ 규정 개정('16.6.30.)으로 금융회사 또는 전자금융업자는 기존 공인인증서 외 해당 기관에서 발급하는 사설인증서도 일정 요건을 갖춘 경우 추심이체 출금동의의 방법으로 인정

▣ 음성응답시스템(ARS)로 추심이체 출금동의를 받는 경우 녹취하여 관련 자료를 금융회사 등에게 전달하여야 하는 것이 기존 해석이었으나, 지급인의 육성이 포함되지 않은 경우 본인확인이 가능한 ARS 로그기록 등을 통해 대체 가능

※ 법령해석('15.11.6.)

〈 질의 〉

▣ 「국세징수법」 등에 따른 과세관청의 강제징수 절차 진행과 관련하여 금융회사가 「전자금융거래법」 제15조상 추심이체에 대한 지급인의 동의 획득 의무를 지는지 여부

〈 회신 〉

▣ 「국세징수법」 등에 따른 과세관청의 강제징수 절차 진행에 따라 금융회사가 채무자의 압류자산을 추심하는 경우 금융회사는 「전자금융거래법」 제15조상 추심이체에 대한 지급인의 동의를 획득하지 않아도 됩니다.

〈 이유 〉

▣ 과세관청의 강제징수는 「국세징수법」 등에 따른 권한 및 절차에 따른 것으로 「전자금융거래법」 제3조상 다른 법률에 특별한 규정이 있는 경우에 해당하여 추심이체에 대한 지급인의 동의 없이 과세관청의 강제징수 절차 진행이 가능합니다.

※ 법령해석('16.1.19.)

〈 질의 〉

▣ 납입기일이 속한 해당 월에 잔고가 부족한 경우 납입기일이 속한 해당 월의 불특정일자에 해당 이체계좌(지급인이 기동의한 계좌)에서 출금을 하도록 지급인으로부터 서면으로 동의를 받는 경우에 이체일 이후에 지속적으로 인출하는 방식이 가능한지 여부

〈 회신 〉

▣ 약관, 청약서 등을 통해 지급인으로부터 보험료 납입기일 이후 매영업일 또는 보험사가 특정하는 출금일에 미납된 금액을 인출할 수 있다는 내용의 사전 동의를 받은 경우에는 최초 납입기일 이후 출금이 가능합니다.

〈 이유 〉

▣ 「전자금융거래법」 제15조에서는 지정된 방법에 따라 지급인의 동의를 받는 경우 추심이체를 허용하고 있으며, 잔고 부족등의 이유로 추심이체가 안된 경우의 재시도 방법 등에 대해서는 정의하고 있지 않습니다.

따라서 약관 또는 청약서 등에 관련 내용을 기재하여 지급인의 동의를 받은 경우에는 납입기일 이후에 출금이 가능할 것입니다. 또한, 신용카드사의 경우에도 지급인의 동의를 받아 이용대금결제일 이후에 미결제된 금액을 인출하고 있는바, 보험사와 카드사를 달리 규정할 특별한 이유가 없습니다.

※ 비조치의견서('15.11.24.)

〈 요청대상 행위 〉

▣ 대출고객이 홈페이지나 앱을 통해 원리금을 선결제하는 서비스*를 운영할 경우, 서비스 신청 단계에서 고객 대면확인이 필요한지 여부

* 대출고객이 웰컴저축은행 홈페이지 또는 앱에 접속하여(로그인 필요) 대출 원리금 선결제 신청서(추심이체에 대한 동의 내용 포함) 작성 및 공인인증서 인증을 완료하면 고객계좌에서 신청금액만큼 추심 이체됨

〈 판단 〉

▣ 선결제 서비스 신청서에 추심이체 동의 내용이 포함되어 있고, 신청서 제출시 공인인증서를 통한 인증(전자서명)을 하였다면 별도의 대면확인 절차는 필요하지 않습니다.

〈 판단이유 〉

▣ 전자금융 관련 법규에서는 추심이체 동의 방법으로 공인전자서명*한 전자문서, 녹취, ARS와 같은 비대면 방법을 인정하고 있는바(전자금융거래법 시행령 제10조 및 감독규정 제6조)

* 공인인증서에 기초한 전자서명(전자서명법 제2조제2호)

○ 홈페이지 또는 앱을 통한 선결제 서비스 신청 시에 공인인증서 인증절차를 통해 추심이체 출금 동의를 받은 경우 별도의 대면확인 절차는 필요하지 않습니다.

○ IT검사매뉴얼 중 '전자금융 신청단계의 적정성' 점검항목은 동 규정의 내용과 상충하지 않도록 개정('15.11.9.)되었으니 이 점 참고하시기 바랍니다.

4. 정보보호최고책임자(CISO)의 지정대상

〈 감독규정 〉

제6조의2(정보보호최고책임자의 지정대상) ① 시행령 제11조의3제1항 후단에서 "금융위원회가 정하여 고시하는 상시 종업원 수의 산정방식"이란 「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 말한다.

② 시행령 〈별표 1〉의 제3호나목 단서에서 "금융위원회가 정하여 고시하는 산정방식"이란 「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 말한다.

▣ 금융회사 또는 전자금융업자는 전자금융업무 및 그 기반이 되는 정보기술부문 보안을 총괄하여 책임질 정보보호최고책임자(CISO)를 지정하여야 함(법 제21조의2)

- 전자금융업무를 하지 않는 은행, 증권사, 보험회사, 신용카드사, 신용정보회사 등은 예외(법 제3조, 시행령 제5조)

※ 관계 법령

〈 법 〉

제21조의2(정보보호최고책임자 지정) ① 금융회사 또는 전자금융업자는 전자금융업무 및 그 기반이 되는 정보기술부문 보안을 총괄하여 책임질 정보보호최고책임자를 지정하여야 한다.

② 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자는 정보보호최고책임자를 임원(「상법」 제401조의2제1항제3호에 따른 자를 포함한다)으로 지정하여야 한다.

③ 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자의 정보보호최고책임자는 제4항의 업무 외의 다른 정보기술부문 업무를 겸직할 수 없다.

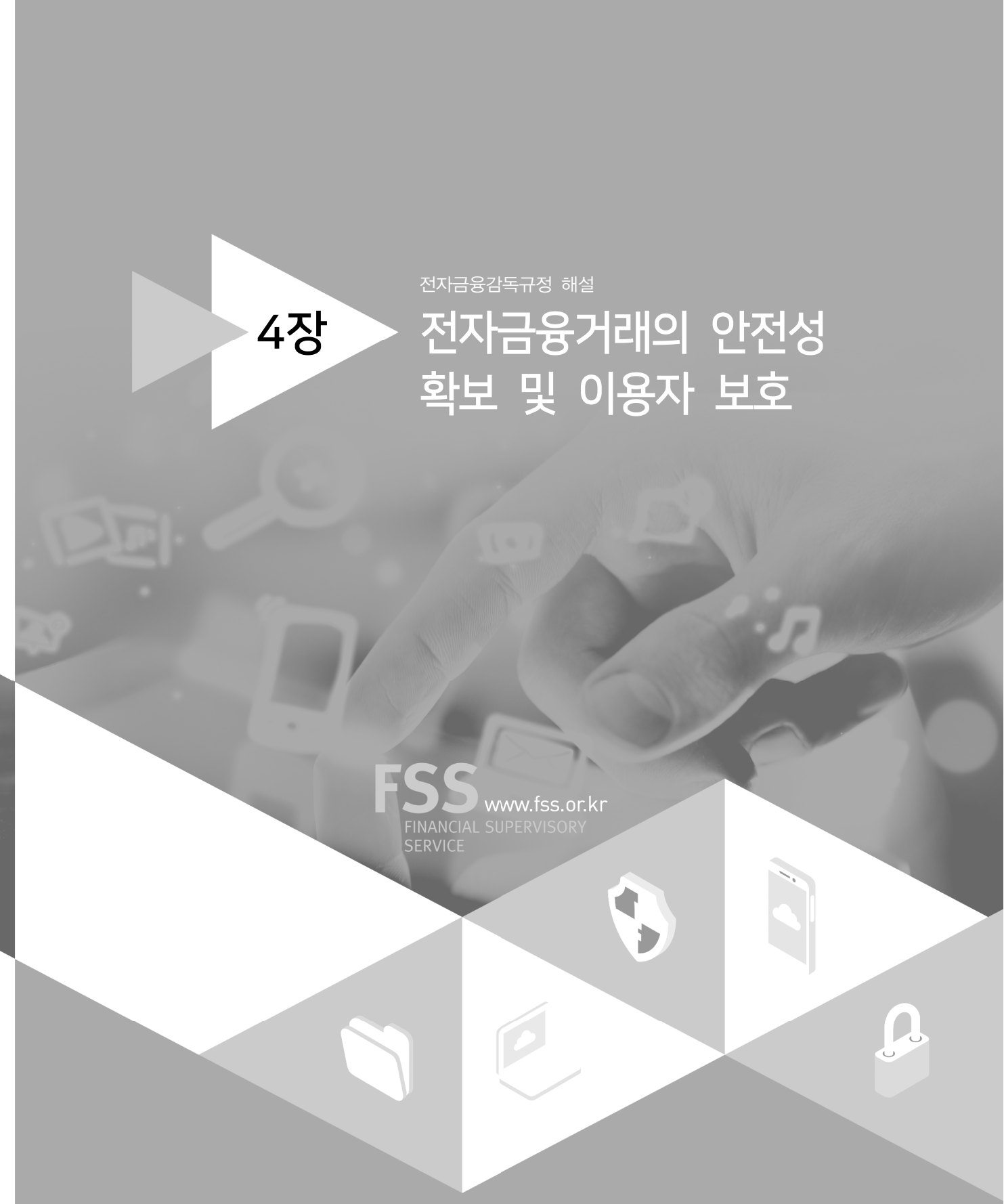
④ 제1항에 따른 정보보호최고책임자는 다음 각 호의 업무를 수행한다.

1. 제21조제2항에 따른 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립
2. 정보기술부문의 보호
3. 정보기술부문의 보안에 필요한 인력관리 및 예산편성
4. 전자금융거래의 사고 예방 및 조치
5. 그 밖에 전자금융거래의 안정성 확보를 위하여 대통령령으로 정하는 사항

⑤ 정보보호최고책임자의 자격요건 등에 필요한 사항은 대통령령으로 정한다.

전자금융감독규정 해설

4장 전자금융거래의 안전성 확보 및 이용자 보호



FSS www.fss.or.kr
FINANCIAL SUPERVISORY SERVICE

제4장 전자금융거래의 안전성 확보 및 이용자 보호

제1절 통칙

1. 전자금융거래 종류별 안전성 기준

〈 감독규정 〉
제7조(전자금융거래 종류별 안전성 기준) 법 제21조제2항의 "금융위원회가 정하는 기준"이라 함은 다음 각 호의 내용에 관하여 제8조부터 제37조에서 정하는 기준을 말한다.
1. 인력, 조직 및 예산 부문
2. 건물, 설비, 전산실 등 시설 부문
3. 단말기, 전산자료, 정보처리시스템 및 정보통신망 등 정보기술부문
4. 그 밖에 전자금융업무의 안전성 확보를 위하여 필요한 사항

▣ 전자금융거래법 제21조제2항에서 규정한 "금융위원회가 정하는 기준"에 전자금융감독규정 제8조~제37조가 해당

※ 관계 법령

〈 법 〉
제21조(안전성의 확보의무) ① 금융회사·전자금융업자 및 전자금융보조업자(이하 "금융회사등"이라 한다)는 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다.
② 금융회사등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문, 전자금융업무 및 「전자서명법」에 의한 인증서의 사용 등 인증방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다.
③ 금융위원회는 제2항의 기준을 정할 때 특정 기술 또는 서비스의 사용을 강제하여서는 아니 되며, 보안기술과 인증기술의 공정한 경쟁이 촉진되도록 노력하여야 한다.

④ 대통령령으로 정하는 금융회사 및 전자금융업자는 안전한 전자금융거래를 위하여 대통령령으로 정하는 바에 따라 정보기술부문에 대한 계획을 매년 수립하여 대표자의 확인·서명을 받아 금융위원회에 제출하여야 한다.

제2절 인력, 조직 및 예산 부문

1. 인력, 조직 및 예산

〈 감독규정 〉

제8조(인력, 조직 및 예산) ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다.

1. 정보처리시스템 및 전자금융업무 관련 전담 조직을 확보할 것
2. 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것
3. 전산인력의 자질향상 및 예비요원 양성을 위한 교육 및 연수프로그램을 운영할 것
4. 정보보호최고책임자는 임직원이 정보보안 관련법규가 준수되고 있는지 정기적으로 점검하고 그 점검결과를 최고경영자에게 보고할 것
5. 최고경영자는 임직원이 정보보안 관련법규를 위반할 경우 그 제재에 관한 세부기준 및 절차를 마련하여 운영할 것

② 금융회사 또는 전자금융업자는 인력 및 예산에 관하여 다음 각 호의 사항을 준수하도록 노력하여야 한다.

1. 정보기술부문 인력은 총 임직원수의 100분의 5 이상, 정보보호인력은 정보기술부문 인력의 100분의 5 이상이 되도록 할 것
2. 정보보호예산을 정보기술부문 예산의 100분의 7 이상이 되도록 할 것

③ 제2항 각 호의 사항을 이행하지 못하는 금융회사 또는 전자금융업자는 그 사유 및 이용자 보호에 미치는 영향 등을 설명한 자료를 해당 금융회사 또는 전자금융업자가 운영하는 홈페이지 등을 통해 매 사업연도 종료 후 1개월 이내에 공시하여야 한다. 다만, 허가, 등록 또는 인가를 마친 후 1년이 지나지 않은 금융회사 또는 전자금융업자는 공시하지 아니할 수 있다.

④ 제2항제1호의 인력에 관한 기준은 〈별표 1〉과 같으며, 제2항제2호의 예산에 관한 기준은 〈별표 2〉와 같다.

▣ 정보처리시스템 및 전자금융업무 개발과 운영업무를 담당하는 인력, 조직 및 예산을 통제하고 금융사고 없이(기밀성, 무결성, 가용성 보장 등) 전산시스템을 운용하는데 필요한 인력, 조직 및 예산 관리 체계를 마련

▣ 해설

- 정보처리시스템 및 전자금융업무의 안정적 운영에 필요한 적정인력으로 구성된 전담조직을 확보(제1항제1호)

- 외부주문등에 관한 계약을 체결하는 금융회사 또는 전자금융업자는 계약내용의 적정성을 검토할 수 있고 외부주문 업체에 대한 통제력을 상실하지 않고 직접 외부주문을 통제할 수 있도록 필요조직 및 인력을 갖추고 내부통제용 시스템을 별도 구축(제1항제2호)

- 전산인력(외부 용역직원 포함)에 대한 개인 경력개발 계획 및 연간 교육계획에 의하여 필요한 교육 및 연수프로그램을 마련하고 내부 승인절차를 거쳐 직무 교육 및 연수가 실시되어야 하며 교육연수의 목적 및 수준은 전산인력의 업무 특성이 적절하게 반영(제1항제3호)

  - 고객 데이터에 직접 접근할 수 있는 권한이 있는 직원(내부 및 외부주문업체 직원 포함)에 대하여는 정보보호 교육 및 윤리교육

  - 제19조의2에서 정한 정보보호 교육 시간은 최소한의 기준

- 정보보호최고책임자는 임직원의 보안법규 인식 저하에 의한 사고를 예방할 수 있도록 정기적으로 임직원의 IT보안법규 준수여부를 점검(제1항제4호)

- 최고경영자는 자체 보안점검에 따른 위규사항 발견시 관련법규를 위반한 임직원에 대해 제재할 수 있는 처벌 기준을 금융회사 내규에 마련하여 시행(제1항제5호)

- 정보기술부문 인력 5%, 정보보호 인력 5%, 정보보호 예산 7%의 기준은 최소한의 기준이므로 조직의 현황과 특성에 맞도록 인력과 예산을 확보하는 것이 필요(제75조 제2항 참조)

- 정보보호 예산에 포함되는 예산은 별표 2에 규정한 바를 준용하되 건물 경비, 전화/FAX 등 전자금융거래와 관련되지 아니한 장비의 구입, 운영 등에 소요되는 비용은 포함되지 않음

- 인력 및 예산이 권고기준에 미충족하는 금융회사등은 그 사유 및 이용자 보호에 미치는 영향 등을 공시(제3항), 등록·허가·인가로부터 1년이 지나지 않은 신규 금융회사 및 전자금융업자는 공시하지 않을 수 있음

※ 인력 및 예산 권고기준 미충족 사유 등 공시 대상(예시) – 제3항

▣ '16.1.1일자 신규 등록한 전자금융업자의 경우 '17.12.31.까지 최대 2년간* 공시의무가 없으며, '18.1.1.을 기준으로 인력·조직·예산기준을 미충족할 경우 '18.1.1.~1.31. 기간 중 공시하여야 함

* '16.1.1.~12.31. : 등록·허가·인가로부터 1년이 지나지 않음
'17.1.1.~12.31. : 사업연도가 종료되지 않음

※ 인력비율 산정방법(예시) – 전자금융감독규정 별표1 참조

(1) 총임직원수 : 10,000명

(2) 정보기술부문 인력 비율 : 5% [(500명/10,000명)×100]

금융회사 내부인력		전산자회사등의 인력			금융회사 외주 인력(6)③	내부정보 기술부문 인력 (7=1+2)	전산 자회사 인력 (8=3+4)①	인정 외주인력 (9)②	정보기술 부문인력 (7+8+9)
정규직 (1)	계약직 (2)	정규직 (3)	계약직 (4)	재하청 인력(5)					
150명	50명	70명*	30명*	100명	600명	200명	100명	200명	500명

* 전산자회사 등의 인력 중 70명과 30명 부분은 운영비용분담비율을 반영한 인력규모임

① 전산자회사등*의 인력(200명) 중 전산자회사의 재하청인력(100명)을 제외하고 운영비용분담률에 해당하는 정보기술부문 인력 인정

* 1) 금융지주회사의 IT자회사
2) 금융회사 또는 금융회사의 동일 기업집단이 지분을 50%를 초과하여 소유하는 IT(손)자회사
3) 회원사의 전자금융시스템 운영을 공동수탁하는 기관(코스콤, 저축은행중앙회, 신협중앙회 등)

② 외주인력(600명)중 내부IT인력(200명)을 초과하는 인력(400명)은 제외하고 내부IT인력(200명)범위 내에서 외주인력(200명)을 정보기술부문 인력으로 인정

③ 재하청 인력은 외주인력 인정 범위내에서 인정하며 위탁금융회사의 하청인력을 초과할 수 없음

(3) 정보보호 인력 비율 : 5% [(25명/500명)×100]

금융회사 내부인력		전산자회사등의 인력			금융회사 외주 인력(6)③	내부정보 보호인력 (7=1+2)	전산 자회사 인력 (8=3+4)①	인정 외주인력 (9)②	정보보호 인력 (7+8+9)
정규직 (1)	계약직 (2)	정규직 (3)	계약직 (4)	재하청 인력(5)					
7명	3명	3명	2명	10명	30명	10명	5명	10명	25명

* 전산자회사등의 인력 중 3명과 2명 부분은 운영비용분담비율을 반영한 인력규모임

① 전산자회사등*의 인력(15명) 중 전산자회사의 재하청인력(10명)을 제외하고 운영비용분담률에 해당하는 정보보호 인력 인정

* 1) 금융지주회사의 IT자회사
2) 금융회사 또는 금융회사의 동일 기업집단이 지분을 50%를 초과하여 소유하는 IT(손)자회사

3) 회원사의 전자금융시스템 운영을 공동수탁하는 기관(코스콤, 저축은행중앙회, 신협중앙회 등)

② 외주인력(30명)중 내부정보보호인력(10명)을 초과하는 인력(20명)은 제외하고 내부정보보호인력(10명) 범위내에서 외주인력(10명)을 정보보호 인력으로 인정

③ 재하청 인력은 외주인력 인정 범위내에서 인정하며 위탁금융회사의 하청인력을 초과할 수 없음

2. 정보보호위원회의 운영

〈 감독규정 〉

제8조의2(정보보호위원회 운영) ① 금융회사 또는 전자금융업자는 중요 정보보호에 관한 사항을 심의·의결하는 정보보호위원회를 설치 운영하여야 한다.

② 정보보호위원회의 장은 정보보호최고책임자로 하며, 위원은 정보보호업무 관련 부서장, 전산운영 및 개발 관련 부서장, 준법업무 관련 부서의 장 등으로 구성한다.

③ 정보보호위원회는 다음 각 호의 사항을 심의·의결한다.

1. 법 제21조제4항에 따른 정보기술부문 계획서에 관한 사항
2. 법 제21조의2제4항제1호에 관한 사항
3. 법 제21조의3에서 정한 취약점 분석·평가 결과 및 보완조치의 이행계획에 관한 사항
4. 전산보안사고 및 전산보안관련 규정 위반자의 처리에 관한 사항
5. 기타 정보보호위원회의 장이 정보보안업무 수행에 필요하다고 정한 사항

④ 정보보호최고책임자는 정보보호위원회 심의·의결사항을 최고경영자에게 보고하여야 한다.

⑤ 최고경영자는 특별한 사정이 없는 한 정보보호위원회의 심의·의결사항을 준수하여야 한다.

▣ 정보보호위원회는 정보보호와 관련된 정책, 사업, 징계 등 정보보호와 관련된 중요한 결정을 수행하는 조직임. 동 위원회의 결과에 대하여 최고경영자는 준수하여야 함으로 의사 결정에 신중함이 요구됨

▣ 해설

- 정보보호위원회는 IT업무 추진위원회와 구분되어야 하며 구성원도 정보보호업무 수행 부서와 업무의 개발 운영부서, 검사부(준법감시조직) 등 관련 부서의 장이 참여하는 것이 필요
- 또한 IT부문 전반에 관한 계획서도 심의·의결(제3항제1호)

제3절 시설 부문

1. 건물에 관한 사항

〈 감독규정 〉

제9조(건물에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다.

1. 건물 출입구는 경비원에 의하여 통제하고 출입통제 보안대책을 수립·운용할 것
2. 비상시 대피를 위한 비상계단 및 정전대비 유도등을 설치할 것
3. 번개, 과전류 등 고전압으로 인한 전산장비 및 통신장비 등의 피해 예방을 위하여 피뢰설비를 갖출 것
4. 서버, 스토리지(Storage) 등 전산장비 및 통신장비 등의 중량을 감안한 적재하중 안전대책을 수립·운용할 것
5. 화재발생 시 조기진압을 위한 소화기 및 자동소화설비 등을 갖추고, 화재전파방지를 위한 배연설비설치 등 화재예방 안전대책을 수립·운용할 것
6. 화재발생 위험이 높은 지역, 상습 침수지역 및 진동피해 발생지역 등 외부환경에 의하여 전산장비 등이 영향을 받을 수 있는 지역은 제외할 것

▣ 자연재해, 인적재해 등의 내·외부 충격으로 부터 전산실을 보호하기 위한 대책 마련

▣ 해설

- 출입을 신청한 내·외부 직원이 전산센터 내의 데이터 및 시설에 업무상 접근이 필요한 직원인지 확인, 이들 직원이 출입허가를 받고 출입할 수 있는 절차를 마련 및 외부 직원이 출입할 경우에는 내부 직원이 동반(제1호)
  - 출입 허가자 명단을 관리하고 내·외부직원의 출입기록은 철저히 관리되어야 하며 보안관리자가 정기적으로 점검. 특히 자동판매기 관리, 청소 용역원 등에 대한 직접 또는 간접 인력 관리
  - 외부인이 쉽게 접근할 수 있는 경로가 있는지, 물리적 차폐시설이나 불법접근을 확인할 수 있는 공간이 있는지 점검
- 비상사태 발생시 전산실 상주 직원들이 안전하게 대피할 수 있도록 전산센터의 각 통로에는 비상구 표시가 있어야 하며 비상계단 및 정전대비 유도등을 설치(제2호)

- 번개, 과전류 등으로 부터 전산장비, 통신장비, 통신회선 등의 피해를 예방하기 위하여 “건축법 및 건축물의 설비기준 등에 관한 규칙” 제20조(피뢰설비)를 준용하여 피뢰설비를 설치(제3호)

- 전산센터의 적재하중에 대한 안전대책을 수립할 경우에는 “건축물의 구조기준 등에 관한 규칙(국토교통부령 제260호)” 또는 “집적정보통신시설보호지침(미래창조과학부 고시 제2014-109호)”을 참조하며, 적재하중이 큰 UPS 등은 지하층에 분산 배치하여 적재물의 하중 과다로 인하여 전산센터에 피해가 발생하지 않도록 조치(제4호)

- 전산실 구축 시에는 건물 설계서, 소방안전진단서 검토 및 면담을 통해 내화자재를 사용하였는지, 소화설비를 갖추고 있는 건물인지, 건물 하중에 적절한 구조로 이루어졌는지, 노후화 또는 구조 변경으로 인한 이상이 없는지 확인하고 있다면 적절하게 대처(제5호)

  - 화재시 확산방지 및 대피를 위해 인접건물과 충분한 간격을 확보하거나 화재 방화벽을 설치하여 화재 발생 시에도 피해가 최소화 되도록 전산실을 관리

  - 건물의 규모 및 소방대상물의 규모·용도 및 수용인원 등을 고려하여 소화기 및 자동소화설비, 배연설비 등의 소방시설을 설치 및 유지하여야 하며, 이를 위해 “화재예방, 소방시설 설치·유지 및 안전관리에 관한 법률” 등 소방 관련법을 준수

- 화재, 진동, 먼지, 유독가스, 염분, 홍수, 누수, 침수 등의 위험이 높은 곳은 재해로 인하여 전산센터 가동에 영향을 미칠 수 있으므로 상기위험이 있는 장소에는 전산센터 구축 금지(제6호)

2. 전원, 공조 등 설비에 관한 사항

〈 감독규정 〉

제10조(전원, 공조 등 설비에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다.

1. 전원실, 공조실 등 주요 설비시설에 자물쇠 등 출입통제장치를 설치할 것
2. 전원, 공조, 방재 및 방범 설비에 대한 적절한 감시제어시스템을 갖출 것
3. 전산실의 전력공급 중단에 대비하여 자가발전설비를 갖출 것
4. 전력공급 장애 시 전력선 대체가 가능하도록 복수회선을 설치하고 전력공급의 연속성 유지를 위한 무정전전원장치(Uninterruptible Power Supply : UPS)를 갖출 것
5. 과전류, 누전에 의한 장애 방지를 위하여 과전류차단기, 누전경보기 등을 설치하고 일정한 전압 및 주파수 유지를 위한 정전압정주파수장치(Constant Voltage Constant Frequency : CVCF)를 갖출 것

6. 전산실에 공급되는 전원 및 공조 설비는 부하가 큰 설비부분과 분리하여 설치하고 공조 설비 상태 점검을 위한 압력계, 온도계 등을 갖출 것
7. 전산실에 24시간 동안 적정한 온도 및 습도를 유지하기 위해서 자동제어 항온·항습기를 갖출 것

▣ 주요 정보가 저장되어 있는 전산실에 대한 출입 통제 및 정보처리시스템의 운영 연속성을 보장하기 위하여 부대설비를 운영하여 자연 재해, 기술적 재해 등 비상사태 발생에 대비한 예방책 마련

▣ 해설

- 전원실, 공조실, 통신실 등은 외부인 또는 비 인가자의 출입을 통제할 수 있도록 통제구역으로 설정하여 '출입통제지역'임을 표시하고, 자물쇠, 출입카드, 지문인식기 등의 출입통제장비 구비(제1호)
- 전원, 공조, 방재 및 방범 등의 설비에 대한 상시감시를 위하여 기기별 작동상황 및 사고발생 여부를 실시간으로 파악할 수 있는 중앙감시시설 및 CCTV, 실시간 경보장치 등을 구축·운영(제2호)
- 외부 전력공급 장애에 대비하여 충분한 용량의 전원공급이 가능하고 추가적인 연료 보충 없이도 전력을 공급할 수 있는(예시 : 2시간 이상) 자가발전설비 구비(전산실이 자체 건물이 아닌 경우에는 입주사 제공 가능)(제3호)
- 전산실의 외부 전력공급 중단, 순간 정전에 대비하여 전력선을 이중화하고 무정전전원장치(UPS)를 갖추어야 함. (예시 : UPS는 정보시스템의 3개월간의 평균 순간 사용전력의 130%에 해당하는 전력을 최소 20분 이상 공급할 수 있는 용량을 확보하고, UPS 상호 백업이 가능하도록 동일한 용량을 사용 – 집적정보통신시설보호지침)(제4호)
- 안정적인 전원공급을 위하여 과전압, 누전, 전압변동, 주파수 변동 등으로 인한 전원 이상을 방지하는 과전류차단기, 누전경보기, 정전압안정주파수(CVCF:Constant Voltage Constant Frequency) 등의 장비 구비(제5호)
- 전산실에 안정적인 전원공급을 위하여 전원설비는 전산장비의 부하가 큰 설비부분과 분리하여 운영하고, 공조 설비에 대한 정기적인 상태 점검을 위하여 각종 계측장치를 설치하여 점검 실시(제6호)

● 전산기기는 온도와 습도에 매우 예민하게 반응하므로 항상 최적의 운영환경을 유지할 수 있도록 전산기기가 설치된 장소는 24시간 동안 적정한 온도와 습도를 유지하기 위해서 자동제어 항온항습기 운영(제7호)

※ 법령해석('15.7.3.)

〈 질의 〉

▣ 전력선 복수회선 구간 범위에 대해서 아래와 같이 질의하셨습니다.

○ 일반 건물 내 층간 복수 전력선 운영은 전문 데이터센터 건물이 아니면 분전반, 관련 장비 설치 공간 등 구조적인 이유로 층간 전력선 이중화 구축에 어려움이 있는바, 건물유입 전력선, 건물 내 층간 전력선, 전산실 내 전력선 구간 전체에 대하여 복수회선을 설치해야 하는지 여부

※ (관련 규정)「전자금융감독규정」제10조제4호 : 전력공급 장애 시 전력선 대체가 가능하도록 복수회선을 설치하고 전력공급의 연속성 유지를 위한 무정전 전원장치(Uninterruptible Power Supply: UPS)를 갖출 것

〈 회신 〉

▣ 「전자금융감독규정」 제10조제4호는 전산실이 위치한 건물의 전원에 관한 준수사항으로서, 동 전산실에 전력공급상 장애가 발생할 시에도 금융거래의 연속성을 보장하고자 하는 것입니다.

▣ 따라서 전산실이 위치한 건물의 인입 전력선이 이중화되어야 전력공급 장애로 인한 서비스 중단을 방지할 수 있으며, 이에 따라 건물은 물론 전산실까지 복수의 전력선을 갖추어야 합니다.

〈 이유 〉

▣ 갑작스런 전력공급 장애에 대비하고 전산실 내에 위치한 정보처리시스템의 안정적인 운용을 위해서는 전산실 내의 전력공급 이중화가 필요하며, 이를 위해서는 건물 외부에서 인입되는 단계부터 복수의 전력회선을 갖추어야 합니다.

3. 전산실 등에 관한 사항

〈 감독규정 〉

제11조(전산실 등에 관한 사항) 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다.

1. 화재·수해 등의 재해 및 외부 위해(危害) 방지대책을 수립·운용할 것
2. 상시 출입문은 한 곳으로 정하며 상시 출입은 업무와 직접 관련이 있는 사전 등록자에 한하여 허용하고, 그 밖의 출입자에 대하여는 책임자의 승인을 받아 출입하도록 하며 출입자 관리기록부를 기록·보관할 것
3. 상시 출입이 허용된 자 이외의 출입자의 출입사항에 대하여는 전산실의 규모 및 설치장소 등을 감안하여 무인감시카메라 또는 출입자동기록시스템 설치 등 적절한 조치를 취하여 사후 확인이 가능하도록 할 것
4. 출입문은 이중 안전장치로 보호하며 외벽이 유리인 경우 유리창문을 통하여 접근할 수 없도록 조치할 것
5. 천정·바닥·벽의 침수로 인한 정보처리시스템의 장애가 발생하지 않도록 외벽과 전산장비와의 거리를 충분히 유지하고 이중바닥설치 등 방안을 강구할 것

6. 적정수준의 온도·습도를 유지하기 위하여 온도·습도 자료 자동기록장치 및 경보장치 설치 등 적절한 조치를 취할 것
7. 케이블이 안전하게 유지되도록 전용 통로관 설치 등 적절한 보호조치를 강구할 것
8. 정전에 대비하여 조명설비 및 휴대용손전등을 비치할 것
9. 집적정보통신시설(Internet Data Center : IDC) 등과 같이 다수의 기관이 공동으로 이용하는 장소에 정보처리시스템을 설치하는 경우에는 미승인자가 접근하지 못하도록 적절한 접근통제 대책을 마련할 것
10. 다음 각 목의 중요 시설 및 지역을 보호구역으로 설정 관리할 것
    가. 전산센터 및 재해복구센터
    나. 전산자료 보관실
    다. 정보보호시스템 설치장소
    라. 그 밖에 보안관리가 필요하다고 인정되는 정보처리시스템 설치장소
11. 국내에 본점을 둔 금융회사의 전산실 및 재해복구센터는 국내에 설치할 것
12. 무선통신망을 설치하지 아니할 것

▣ 정보처리시스템에 대한 물리적 보호를 위하여 화재, 수해 등의 재해 발생 시 업무의 연속성을 확보하기 위한 재해복구 시설 구축과 비인가자에 의한 정보처리시스템의 접근을 방지하기 위한 전산실 보호 대책 마련

▣ 해설

● 위해방지 대책은 화재, 수해, 지진 등의 자연재해, H/W·S/W의 장애, 운용요원의 고의 또는 실수, 사이버테러 또는 해킹 등으로 인하여 전산실의 기능이 마비되는 것을 방지하기 위한 대책으로 다음의 사항을 포함하여 실현 가능한 대책 수립(제1호)

- 화재 등의 재해방지를 위한 설비 구축 및 점검 절차

【예시1】 화재진압시설의 경우 컴퓨터실 내부와 외부에서 작동이 가능토록 하여 비상시 대응이 용이하도록 함

【예시2】 수해 방지를 위하여 전산실의 지하층 설치 금지, 전산실 천장 수도관 설치 금지 등

【예시3】 화재 진압용 시설은 인원 사상이 되지 않는 재료를 사용하여야 하며 정기적으로 점검을 실시하여 유사시 미 작동으로 인한 피해를 방지 등

- 비상시 연락체계 구축(내부, 외부)

- 화재 등의 비상사태 발생시 대응 절차 수립

【예시】 반출자료, 반출 우선 순위, 반출자, 화재진압 등에 대하여 사전 정의

- 훈련 계획 및 훈련실시(대상, 주기 등)

【사례】 A금융회사 옥상에 위치한 냉각탑이 동파되어 유출된 물이 건물 외벽을 타고 전산실로 유입되어 전산실 바닥이 침수로 인하여 전산시스템의 작동이 중단됨

【사례】 B금융회사에서 전산실 천정을 통과하는 수도관의 수압 테스트를 실시하던 중 상수관이 파괴되어 서버가 침수되어 마비되는 사고 발생

● 전산실의 출입통제를 위하여 다음 사항을 포함한 대책 수립(제2호 내지 제4호)

- 상시출입이 필요한 직원은 최소화하고 불필요한 직원이 상시출입 인가를 받지 않도록 주의

【예시】 부서장, 시스템프로그래머 등 IT·보안담당자의 대부분이 등록된 사례가 많으므로 등록을 제한하도록 주의가 필요

- 전산실 상시 출입문은 여러 곳이 아닌 한 곳으로 정하여 비인가자에 대한 철저한 전산실 출입통제. 전산실 출입문은 2중 안전장치를 설치하여 외력으로 침입할 수 없도록 통제(제4호)

【예시】 전산부서를 통해 전산실에 출입하는 경우 전산부서 출입문, 전산실 출입문을 이중으로 통과

- 소방법 등에 따라 출입문 이외에 비상구를 설치할 경우 출입구는 2개로 설치하되 상시 출입을 하나로 하는 것이 필요

- 또한 서버룸은 OP룸, 통신룸, 유지보수 직원 룸 등과 완전 분리하도록 조치. Access Floor 밑을 통한 서버 룸 접근을 차단

- 출입자 관리기록부 기록 및 기록내용 확인 철저. 특히, 유지보수 업체 직원에 대한 출입기록 철저

- 출입자동기록시스템 설치

※ (예시) 물리적 보안대책이 필요한 전산실

- 주전산기, 서버, 광단국 장비가 위치한 장소
- 시스템 및 네트워크를 모니터링 또는 통제할 수 있는 장소
- 데이터저장 매체 보관장소
- 통신회선 분배장치(MDF/IDF)가 위치한 장소 등

- 전산실의 천정, 바닥, 벽 등을 통하여 침수가 발생하는 경우 정보처리시스템의 장애 또는 고장의 원인이 되므로 전산장비는 외벽과 일정한 거리를 두고 설치하고, 바닥을 이중으로 구성하는 등 누수 시에도 전산시스템, 통신 및 전원케이블에 영향을 최소화 하도록 조치(제5호)

- 정보처리시스템은 온도와 습도에 매우 예민하게 반응하므로 항상 최적의 운영환경을 유지할 수 있도록 온·습도 자동기록 장치 및 고온, 고습, 저온 및 저습 시 자동으로 알려주는 경보시스템을 구축하여 최적의 운영 환경 유지(제6호)

- 작업자의 실수 등에 의하여 전원케이블, 통신케이블의 손상을 방지하고 전산실 바닥 침수 시에도 피해를 최소화시키기 위하여 전용 통로관(바닥에서 일정한 높이에 설치)을 설치하는 등 보호조치 마련(제7호)

- 전산실의 정전 시에도 업무수행이나 대피가 용이하도록 자동조명설비 또는 휴대용 손전등 비치(제8호)

- 집적정보통신시설, 계열사 공동 전산센터 등과 같이 다수의 기관이 공동으로 이용하는 장소에 정보처리시스템을 설치하는 경우 각 정보처리시스템에 대하여 물리적·논리적 접근통제가 모두 가능하며 추가적으로 미승인자가 접근하지 못하도록 철저한 관리가 필요

  ※ (예시) 정보처리시스템 구성상 불가피하게 공동으로 이용하는 농협 단위조합, 상호저축은행중앙회, 코스콤과 같이 보안성심의를 완료한 경우에는 공동이용 허용

- 국내에 본점을 둔 금융회사의 전산실 및 재해복구센터는 국내에 설치해야 하며, 전산실 및 정보처리시스템에 대한 물리적·논리적 통제체계를 구축하고 비상사태 발생에 대비한 복구훈련 실시 등 국내 법규 및 규정 준수(제11호)

- 전산실 내 무선통신망의 설치 금지(제12호)

제4절 정보기술부문

1. 단말기 보호대책

〈 감독규정 〉
제12조(단말기 보호대책) 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다.
1. 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치할 것
2. 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지할 것
3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것
4. 정보유출, 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 및 휴대용 전산장비에 접근하는 것을 통제할 것
5. 삭제

▣ 정보처리시스템에 접근할 수 있는 단말기(이하 개인용 컴퓨터 포함)를 제한함으로써 비인가자에 의한 정보 유출 및 악성코드 감염, 프로그램 변경, 불법 거래 등 방지를 목적으로 하는 단말기 보호 대책을 마련·운영

▣ 해설

- 업무담당자 이외의 자가 내부 정보통신망과 연결된 단말기를 무단으로 조작하여 전산자료를 수정, 삭제, 조회하지 못하도록 단말기에 대한 보호대책 마련(제1호)
  - 로그인 비밀번호, 일정시간 단말기 사용중지 시 화면보호기능 설정 및 비밀번호 재입력, 취급자 지정 등 단말기 접근통제
- 정보처리시스템에 접속하는 단말기에 대해 사용자인가 정보를 기록·유지함으로써 필요시 정보처리시스템 사용자의 정당성 확인을 위해 사용자인가 정보에 대한 조회가 가능하도록 조치(제2호)
- 중요단말기가 외부에 반출되거나 인터넷 및 그룹웨어에 접속되는 경우 해커가 침입하거나 해킹프로그램 또는 악성코드에 감염되어 내부 정보유출 및 자료파괴 등 피해가 발생할 수 있으므로 이를 방지하기 위하여 중요단말기는 외부 반출, 인터넷 접속, 그룹웨어 접속 금지 등 강화된 보호대책을 적용(제3호)

● (예) CD/ATM은 인터넷 접속을 차단하고 인터넷망과 분리된 폐쇄망을 이용하며, CD/ATM관리 서버에 연결되는 관리자 단말기를 중요단말기로 지정하고 이외의 단말기에서는 CD/ATM 및 관리서버 접속 차단

〈 중요 단말기 유형 〉

정보처리시스템 또는 DB에 직접 접근이 가능한 권한이 부여되는 단말기

● 보조기억매체나 휴대용전산장비 등이 내부통신망에 연결된 단말기에 접속되는 경우 동 매체나 장비를 이용한 정보유출 및 악성코드 감염이 발생할 수 있으므로 사고 방지를 위하여 내부통신망에 접속하는 단말기는 보조기억매체 및 휴대용 전산장비 등 접근을 통제(제4호)

- 외주개발을 위해 투입된 외주직원이 사용하는 단말기에도 동일 수준의 접속통제를 적용
- 용도에 따라 USB 쓰기/읽기 기능 차단, USB 사용시 책임자의 사전 승인, 보안 정책에 따른 USB 관리 기록

※ 비조치의견서('15.6.8.)

〈 요청대상 행위 〉

▣ 단말기별 취급자를 지정하고, 단말기를 켤 때 및 운영체제(O/S)에 접속할 때 각각 비밀번호를 설정·입력하며, 화면보호기능을 설정한 것이

○ 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치*한 것인지 여부

* 전자금융감독규정 제12조제1호

〈 판단 〉

▣ 요청대상 행위는 적절한 조치에 해당하는 것으로 판단되는바, 특별한 사정이 없는 한 제재대상에 해당하지 않습니다.

〈 판단이유 〉

▣ 전자금융감독규정 제12조(단말기 보호대책) 제1호에 의해 금융회사 또는 전자금융업자는 '업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치'하여야 하는데, 구체적인 조치 방법은 금융회사 등이 자율적으로 결정하여 운영할 수 있는바,

○ 단말기별로 취급자를 지정하며 비밀번호를 2중으로 설정하게 하고 화면보호기 등을 설정할 경우 단말기가 무단으로 부팅·사용되거나 작업 중 권한 없는 자가 임의로 사용하는 것을 예방할 수 있다고 판단됩니다.*

* 구 전자금융감독규정 제12조제1호(2015.2.3. 개정 전)는 '업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 단말기별 취급자 및 비밀번호를 지정하고 화면보호기능을 부여'하도록 명시하고 있었음

▣ 다만, 비밀번호 설정·입력과 관련하여 전자금융감독규정 제32조(내부사용자 비밀번호 관리)를 준수해야 합니다.

2. 전산자료 보호대책

〈 감독규정 〉

제13조(전산자료 보호대책) ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.

1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것
2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것
3. 전산자료의 보유현황을 관리하고 책임자를 지정·운영할 것
4. 전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것
5. 전산자료 및 전산장비의 반출·반입을 통제할 것
6. 비상시에 대비하여 보조기억매체 등 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운용할 것
7. 정기적으로 보조기억매체의 보유 현황 및 관리실태를 점검하고 책임자의 확인을 받을 것
8. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것
9. 주요 백업 전산자료에 대하여 정기적으로 검증할 것
10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 법인인 이용자 정보는 금융감독원장이 정하는 바에 따라 이용자의 동의를 얻은 경우 테스트 시 사용 가능하며, 그 외 부하 테스트 등 이용자 정보의 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)
11. 정보처리시스템의 가동기록은 1년 이상 보존할 것
12. 정보처리시스템 접속 시 5회 이내의 범위에서 미리 정한 횟수 이상의 접속 오류가 발생하는 경우 정보처리시스템의 사용을 제한할 것
13. 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)
14. 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것

② 제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.

③ 금융회사 또는 전자금융업자는 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경·조회내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 한다.

④ 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록·유지되어야 한다.

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

⑤ 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.

〈 시행세칙 〉

제2조의4(법인 이용자 정보의 사용에 대한 동의) 규정 제13조제1항제10호에 따라 동의를 얻는 경우 다음 각 호의 사항을 정보주체에게 사전에 알려야 한다.

1. 테스트의 목적 및 기간
2. 사용되는 이용자 정보의 항목
3. 테스트 기간 중 정보유출 방지를 위한 통제 계획
4. 테스트 종료 후 테스트에 사용된 이용자 정보의 파기 계획

▣ 금융회사 또는 전자금융업자가 보유하고 있는 고객정보 등 중요정보의 외부유출 및 불법 사용을 방지하고, 정보 파괴시 신속한 복구가 가능하도록 대책을 수립하며, 사고발생시 추적이 용이하도록 정보처리시스템 접속 및 이용자정보 조회 로그 등 정보처리시스템 가동기록 유지

▣ 해설

- 사용자 계정과 비밀번호는 개인별 부여를 원칙으로 하며, 사용자 계정에 관한 등록·변경·폐기 등 절차를 마련하여 체계적으로 관리함. 다만, 시스템의 특성상 공동 사용이 불가피한 사용자 계정(예: UNIX의 "root" 등)은 사용자 개인별 사용 내역이 파악될 수 있도록 사용자 IP, 접근시간 등 개인별 세부 사용내역을 기록·유지함으로써 추후에 추적 및 확인이 가능하도록 관리(제1항제1호, 제2항)

- 내부직원 퇴직이나 외주직원 계약 종료 및 해지 등 사유발생시 해당 사용자계정을 삭제하여 기존 계정을 이용한 시스템 접근이 차단되도록 조치. 다만, 사용자 계정의 삭제가 불가능한 경우에는 반드시 비밀번호를 변경하고 실사용자 이름을 바꾸어 사용함(제1항제1호)

- 모든 사용자 계정은 현재 사용하고 있는 실제 직원이 확인될 수 있도록 등록·관리하여야 하며, 변경내용 등에 대한 세부내역을 기록·관리(제1항제1호)

- 외부사용자에게 사용자계정을 부여할 경우 업무수행에 필요한 최소 권한만을 부여하여 불필요한 업무수행 및 자료접근을 차단하고, 계약기간의 적절한 관리를 통해 계약 종료 또는 해지시 해당시스템 접속이 차단되도록 통제장치를 마련함으로써 외주직원에 의한 정보유출 등 침해사고 방지(제1항제2호)

- 전산자료의 적절한 관리와 통제를 위하여 전산자료 보유현황을 관리하고 책임자를 지정하여 운영하며, 사용자별 접근권한(읽기, 쓰기, 변경, 삭제 등)을 구분하여 권한에 따라서 접근할 수 있는 자료를 한정하며, 중요자료에 대한 변경 및 삭제 권한은 최소한의 사용자에게 부여(제1항제3호, 제4호)

- 고객정보 및 금융거래 정보에 대한 조회는 업무상 관련성이 없는 경우에는 엄격히 제한(제1항제4호)

- 전산자료 및 장비를 반출하거나 반입할 경우에는 반·출입 사항을 기록 관리하여야 하며, 반출된 전산자료는 목적 외 사용이 되지 않도록 하여야 하고, 사용 용도가 완료된 후에는 즉시 회수 또는 파기토록 조치(제1항제5호)

- 노트북 또는 PC를 반출시에는 중요자료가 수록되어 있는가를 확인을 하여야 하며, 외부에서 반입된 PC 또는 디스크 등 보조 기억장치 내에 악성코드, 해킹프로그램이 수록되지 않았는가를 확인(제1항제5호)

- 보조기억매체는 보유현황, 사용자, 사용용도 등이 파악될 수 있도록 관리대장을 통해 관리되어야 하며, 비상시 대비 보조기억매체 등 전산자료에 대한 안전지출 및 긴급 파기를 위한 계획을 수립하여 운용하고, 보조기억매체 파기는 매체에 수록된 정보의 복구가 불가능하도록 완전 파기 조치함(제1항제6호, 제7호)

- 전산자료의 백업 대상 및 주기는 전산센터 시스템에 저장된 데이터 및 프로그램 등이 완전히 파괴된 경우에도 시스템의 정상적인 복구가 가능한 수준으로 백업 및 관리되어야 하며, 백업자료(보조기억매체)는 추후 사용편의를 위해 식별이 용이하도록 보유현황을 관리(제1항제8호)

- 백업자료의 소산은 전산센터의 화재, 수해 등 재해로 인하여 데이터 및 프로그램의 사용이 불가능할 경우에도 복구가 가능하도록 전산센터로부터 원격지에 위치한 적절한 장소에 보관하여야 하며, 관련법에서 정한 보존기간 및 업무중요도를 고려하여 소산대상 및 보존기간을 정함. 특히, 프로그램 및 시스템 프로그램이 누락되지 않도록 하고, 매뉴얼, 시스템 설계서 등의 관련문서[2]를 포함(제1항제8호)

- 소산장소는 백업자료가 손상되지 않도록 환경을 유지하여야 하며, 정기적으로 자료를 점검하여 항시 사용이 가능토록 유지하여야 하고 소산장소의 접근통제 필요(제1항제8호)

- 주요 백업 전산자료는 비상사태 발생시 복구를 위해 사용될 수 있도록 전산자료의 무결성 등을 정기적으로 점검(제1항제9호)

2) 관련문서(Documentation) : 단위업무별로 구성된 전산시스템의 업무개요, 흐름도(flow-chart), 관련 파일들의 양식(file lay-out), 프로그램 설명서 등을 집합하여 단위업무의 전산시스템의 수정, 보완, 유지, 관리의 효율화를 위하여 구성한 지침서

- 전산업무 개발 또는 프로그램을 변경하는 경우 테스트 목적으로 실이용자 정보의 사용을 금지, 필요시 이용자 식별이 불가능하도록하여 사용하고, 테스트 종료 즉시 테스트 데이터 삭제 조치(제1항제10호)

  - 다만, 법인인 이용자 정보는 테스트의 목적 및 기간, 사용되는 이용자 정보의 항목 등을 사전에 고지한 후 동의를 얻어 사용 가능

- 고객 인적사항, 금융거래 정보 등 이용자 정보가 포함된 조회나 출력시 이용자가 노출되지 않도록 이용자 식별정보를 통제(마스킹 등)하며,

- 계정계, 정보계, 업무서버, 네트워크 장비 등 정보처리시스템의 가동기록[3]은 전산기기의 가동, 업무처리와 관련하여 주전산기 또는 서버에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근 기록과 전산자료를 사용한 일시, 사용자 및 자료의 내용 등을 확인할 수 있는 접근 기록 등이 자동기록 되도록 하고 1년 이상 보존(제1항제11호, 제4항)

  - (예) 시스템 로그, 콘솔로그 등

- 정보처리시스템 접속에 실패한 접근 시도에 대해서도 기록·유지하고, 접근시도 실패가 일정횟수(5회 이내의 범위)이상 반복적으로 발생하는 경우 시스템 사용을 제한하고 중점 점검(제1항제12호)

- 단말기에는 이용자 정보(계좌번호, 개인인적사항 등)등 주요정보를 보관하지 아니하고 단말기를 공유하지 않도록 조치하며, 불가피하게 단말기에 보관할 필요가 있는 경우에는 보관사유·보관기간 및 관리 비밀번호 등을 정하여 책임자 승인을 받을 것(제1항제13호)

  - 단말기에 이용자 정보를 저장하지 않았더라도 이용자 정보보다 넓은 개념인 전산자료의 보호를 위해 단말기 공유 금지

- 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용중지, 공동 사용 계정변경 등 조치하고 접근권한을 회수하여 이전 계정 및 권한으로 정보처리시스템에 접속할 수 없도록 통제(제1항제14호)

3) 시스템 가동기록은 시스템이 최초 가동된 시각, 시스템 자원(CPU, 메모리, 디스크 등) 상태기록, 시스템 장애상태 등을 확인할 수 있는 기록을 의미하고, 접근기록은 정보시스템에 사용자가 접근한 기록으로 접근시간, 접근ID, 접근IP, 작업내용, 처리결과 등을 의미

- 단말기를 통해 이용자 정보를 조회하는 경우 사용자, 사용일시, 조회 또는 변경내용, 접속방법 등이 시스템에 자동기록 되도록하여 추후 추적 및 확인이 가능하도록 조치하며, 조회기록은 1년 이상 보존함(제3항)

- 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 의한 사고예방을 위해 관리자의 업무행위에 대해 적절한 통제장치를 마련하여 운영하고, 또한 관리자가 전산원장, 이용자 정보 등 주요정보가 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중 확인하고 작업수행 내역에 대해 정기적으로 모니터링 실시(제5항, 제28조제2항)

※ 법령해석('15.10.12.)

〈 질의 〉

▣ 「전자금융감독규정」 제13조제1항제13호에서 "단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)"이라고 정하고 있는바, 단말기에 이용자 정보 등 주요 정보를 보관하고 있지 않은 경우 단말기 공유가 가능한지 여부

〈 회신 〉

▣ 「전자금융감독규정」 제13조제1항제13호에 따라 금융회사 및 전자금융업자는 단말기에 이용자 정보 등 주요 정보를 보관하고 있지 않더라도 단말기를 공유하는 것이 금지됩니다.

〈 이유 〉

▣ '전산자료'는 전산장비에 의해 입력·보관·출력되어 있는 자료를 말하며 그 자료가 입력·출력되어 있는 보조기억매체를 포함합니다(「전자금융감독규정」 제2조제2호).

○ 「전자금융감독규정」 제13조제1항은 이 같은 '전산자료'의 유출·파괴 등을 방지하기 위해 보유현황의 관리, 책임자 지정·운영, 업무별 접근권한 통제, 비상시 안전지출 및 긴급파기, 정기적 백업, 정보처리시스템의 접근 통제 등을 요구하고 있습니다.

○ 동항 제13호 또한 이용자 정보보다 넓은 개념인 '전산자료'의 유출·파괴 등을 방지하기 위한 취지로, 결과적으로 이용자 정보가 포함되어 있지 않더라도 단말기의 공유를 금지하는 것으로 해석해야 할 것입니다.

※ 비조치의견서('16.9.8.)

〈 질의 〉

▣ OO은행은 사업구조개편에 따라 은행과 상호금융 계정계 시스템을 분리·구축하는 사업을 추진 중(예정일: '17.1.31)

○ 전환시스템 운영 전 이용자 정보를 사용하여 전 영업점을 대상으로 사전 정합성 검증*을 실시하는 것이 전자금융감독규정 제13조제1항제10호 위반에 따른 조치대상에 해당하는지 여부

* 특정 거래일에 발생한 금융거래를 구축 중인 전환시스템을 이용하여 재수행하고 그 결과를 상호 비교

〈 회신 〉

▣ 이용자 정보를 테스트 용도로만 제한하여 사용한 후 즉시 삭제하는 한편, 정보 유출을 방지하기 위한 내부통제기준을 마련하는 등 안전성을 확보하여 정합성 검증을 실시하는 경우 감독규정 제13조제1항제10호 위반으로 조치하지 않을 예정입니다.

〈 이유 〉

▣ 동 규정의 취지가 전산자료 유출 방지 및 전자금융거래의 안전성 확보라는 점을 고려하여

○ 시스템의 안전성 확보를 위해 부득이하게* 이용자 정보를 테스트 용도로만 제한하여 사용한 후 즉시 삭제하는 한편,

○ 외부주문에 대한 보안관리방안** 및 실제 운영시스템과 동일한 수준의 보안 대책***을 적용하는 등 검증 작업시 정보 유출을 방지하기 위한 내부통제기준을 마련한 경우에 한하여 이용자 정보를 사용한 정합성 검증을 허용

* 정합성 검증은 실제 발생한 거래지시를 전환시스템으로 재처리하고 그 결과를 실거래 데이터와 비교하는 절차로 이용자 정보·실거래 데이터 없이 효율적인 검증 곤란

** 전자금융감독규정 제60조①항7호 및 동 시행세칙 제9조의2①항

*** 비인가 전산장비·무선통신 접속 통제, 해킹 방지대책, 악성코드 감염 방지 대책, 사용자 권한 및 비밀번호 설정·운영, 이용자 비밀번호 암호화 등

3. 정보처리시스템 보호대책

〈 감독규정 〉

제14조(정보처리시스템 보호대책) 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다.

1. 주요 정보처리시스템에 대한 구동, 조작방법, 명령어 사용법, 운용순서, 장애조치 및 연락처 등 시스템 운영매뉴얼을 작성할 것
2. 데이터베이스관리시스템(Database Management System : DBMS)·운영체제·웹프로그램 등 주요 프로그램에 대하여 정기적으로 유지보수를 실시하고, 작업일, 작업내용, 작업결과 등을 기록한 유지보수관리대장을 작성·보관할 것
3. 정보처리시스템의 장애발생 시 장애일시, 장애내용 및 조치사항 등을 기록한 장애상황기록부를 상세하게 작성·보관할 것
4. 정보처리시스템의 정상작동여부 확인을 위하여 시스템 자원 상태의 감시, 경고 및 제어가 가능한 모니터링시스템을 갖출 것

5. 시스템 통합, 전환 및 재개발 시 장애 등으로 인하여 정보처리시스템의 운영에 지장이 초래되지 않도록 통제 절차를 마련하여 준수할 것
6. 정보처리시스템의 책임자를 지정·운영할 것
7. 정보처리시스템의 운영체계, 시스템 유틸리티 등의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정 작업을 할 것
8. 중요도에 따라 정보처리시스템의 운영체제 및 설정내용 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1년 이상 기록·관리할 것
9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것
10. 정보처리시스템 운영체제(Operating System) 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링체계를 수립하고, 이상 징후 발생 시 필요한 통제 조치를 즉시 시행할 것

▣ 정보처리시스템이 정상적으로 안전하게 운영되고 장애 발생시 신속하게 복구 및 정상 가동되는데 필요한 대책 수립

▣ 해설

- 비상시 정보처리시스템의 신속한 구동 및 조작, 업무 담당자 유고시 대체인력에 의한 원활한 시스템 운영을 위하여 정보처리시스템 및 주요 프로그램에 대한 운영매뉴얼을 작성하여 지정된 장소(전산실 및 재해복구센터)에 보관 및 관리(제1호)
  - 운영매뉴얼은 정보처리시스템 및 프로그램 등 주요프로그램의 변경사항이 발생하는 경우 현재 상태를 반영하여 최신상태 유지

- 정보처리시스템 및 주요 프로그램(DBMS, 운영체제, Web 및 WAS 서버 등)은 장애 예방을 위해 정기적으로 유지보수 되어야 하며, 외부업체로부터 유지보수를 받는 경우 고객정보 등의 중요정보가 유출되지 않도록 주의하고 유지보수 내용을 기록한 유지보수관리대장을 작성·보관(제2호)

- 정보처리시스템의 장애예방을 위해 시스템의 모든 장애 발생은 장애상황기록부에 기록하여 관리하며, 시스템의 정상작동여부 확인이 가능하도록 시스템의 자원 상태를 감시하고, 장애 등 이상 징후 발생시 경고 및 제어가 가능한 모니터링 시스템을 구축(제3호, 제4호)

- 정보처리시스템의 통합, 전환 및 재개발 시 기 운영시스템 및 신규 도입 시스템의 장애, 업무 지연 등의 사고 발생으로 정보처리시스템 운영에 지장을 초래하지 않도록 사전에 철저한 검증을 실시하는 등 통제절차를 마련하여 운영(제5호)

- 정보처리시스템의 관리책임자를 지정·운영하고, 관리책임자는 해당 정보처리시스템에 문제가 발생하지 않도록 운영, 유지보수, 보안관리 등의 시스템 관리업무 총괄(제6호)

- 정보처리시스템 관리책임자는 정보처리시스템의 안전한 운영을 위하여 시스템 운영체제 및 유틸리티 등 주요 소프트웨어에 대해 주기적으로 보정(patch)사항이 발표되는지 확인하고 필수적인 보정사항이 발표되는 경우에는 테스트 시스템에 우선 적용하여 테스트를 실시하고 시스템 운영에 지장을 초래하지 않을 경우 즉시 실 운영시스템에 적용(제7호)

- 정보처리시스템의 운영체제 삭제 등 비상상황 발생시 신속하게 정상복구가 가능하도록 정보처리시스템의 운영체제 및 설정내용 등을 정기적으로 백업하여 원격 안전지역에 소산하고, 백업자료는 정기적 검증을 실시하며 1년 이상 보관(제8호)

- 정보처리시스템의 운영체제 계정에 대한 보안강화를 위하여 로그인시 계정 및 비밀번호 이외의 별도의 안전한 추가인증 절차를 반드시 시행하고, 운영체제 계정의 작업수행에 대한 이상 징후 발생 시 필요한 통제 조치가 즉시 시행될 수 있도록 모니터링 체계수립(제9호, 제10호)

4. 비중요 정보처리시스템의 지정

〈 감독규정 〉

제14조의2(비중요 정보처리시스템 지정) ① 금융회사 또는 전자금융업자는 자체적으로 수립한 정보자산 중요도 평가기준에 따라 전자금융거래의 안전성 및 신뢰성에 미치는 영향이 현저히 낮은 정보처리시스템을 비중요 정보처리시스템으로 지정할 수 있다. 다만, 개인의 고유식별정보 또는 「신용정보의 이용 및 보호에 관한 법률」에 따른 개인신용정보를 처리하는 정보처리시스템은 비중요 정보처리시스템으로 지정할 수 없다.

② 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템 지정시 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

③ 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템을 지정한 날로부터 7일 이내에 금융감독원장이 정하는 양식에 따라 정보자산 중요도 평가기준, 지정 결과, 관리 방안 등을 포함한 보고서를 금융감독원에 제출하여야 한다.

④ 금융감독원장은 제3항에 따라 제출한 보고서를 검토한 결과, 평가 기준, 지정 결과, 관리 방안 등이 적합하지 않다고 판단되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

⑤ 제1항의 비중요 정보처리시스템만 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항 제5호를 적용하지 아니한다.

〈 시행세칙 〉
제2조의3(비중요 정보처리시스템의 보고) 규정 제14조의2제3항에 따라 감독원장이 정하는 양식은 별지 제6호 서식에 따른다.

▣ 금융회사 및 전자금융업자는 클라우드컴퓨팅 등을 이용하기 위하여 고유식별정보 및 「신용정보의 이용 및 보호에 관한 법률」에 따른 개인신용정보를 제외한 정보를 처리하는 시스템을 비중요 정보처리시스템으로 지정할 수 있음

▣ 해설

- 전산실 및 재해복구센터의 국내 설치(제11조제11호), 무선통신망의 설치 금지(제11조제12호) 및 전산센터 물리적망분리(제15조제1항제5호) 규정의 적용을 받지 않을 수 있음

- 클라우드컴퓨팅 서비스 이용을 위해 반드시 비중요정보처리시스템의 지정이 필요한 것은 아니며, 비중요정보처리시스템 지정시 적용되지 않는 규정(제11조제11호 및 제12호, 제15조제1항제5호) 및 전자금융감독규정시행세칙 제2조의2(망분리 예외 적용시) 등을 모두 준수할 경우 비중요정보처리시스템의 지정 없이 클라우드컴퓨팅 서비스 이용이 가능

  – 또한 개인의 고유식별정보와 신용정보법에 의한 개인신용정보를 법규상 절차에 따라 비식별화 조치를 한 경우에도 비중요정보처리시스템으로 지정 가능

5. 해킹 등 방지대책

〈 감독규정 〉
제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.
1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영
2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시
3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)
4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것
5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기

어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)

② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 삭제
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. 정보보호시스템의 원격관리를 금지하고 주기적으로 작동 상태를 점검할 것
5. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것

③ 제1항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 운영결과는 1년 이상 보존하여야 한다.

④ 금융회사 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 한다.

⑤ 삭제

⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다.

1. 무선통신망 이용 업무는 최소한으로 국한하고 법 제21조의2에 따른 정보보호최고책임자의 승인을 받아 사전에 지정할 것
2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안대책을 수립할 것
3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링체계를 운영할 것
4. 비인가 무선접속장비(Access Point : AP) 설치·접속여부, 중요 정보 노출여부를 주기적으로 점검할 것

〈 시행세칙 〉

제2조의2(망분리 적용 예외) ① 규정 제15조제1항제3호에서 금융감독원장의 확인을 받은 경우란 내부 업무용 시스템을(규정 제12조의 중요단말기는 제외한다) 업무상 필수적으로 특정 외부기관과 연결해야 하는 경우를 말한다(다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다).

② 규정 제15조제1항제5호에서 금융감독원장이 인정하는 경우란 다음 각 호와 같다.

1. 「금융회사의 정보처리 업무 위탁에 관한 규정」에 따라 정보처리 업무를 국외 소재 전산센터에 위탁하여 처리하는 경우(다만, 해당 국외 소재 전산센터에 대해서는 물리적 방식 외의 방법으로 망을 분리하여야 하며, 이 경우에도 국내 소재 전산센터 및 정보처리시스템 등은 물리적으로 망을 분리하여야 한다)
2. 업무상 외부통신망과 연결이 불가피한 다음의 정보처리시스템(다만, 필요한 서비스번호(port)에 한하여 연결할 수 있다)
   가. 전자금융업무의 처리를 위하여 특정 외부기관과 데이터를 송수신하는 정보처리시스템
   나. DMZ구간 내 정보처리시스템과 실시간으로 데이터를 송수신하는 내부통신망의 정보처리시스템
   다. 다른 계열사(「금융회사의 정보처리 업무 위탁에 관한 규정」 제2조 제3항의 "계열사"를 말한다)와 공동으로 사용하는 정보처리시스템
3. 규정 제23조의 비상대책에 따라 원격 접속이 필요한 경우
4. 전산실 내에 위치한 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기와 외부통신망과의 연결 구간, 규정 제15조제1항제3호의 내부 업무용 시스템과의 연결 구간을 각각 차단한 경우

③ 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 〈별표 7〉에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.

▣ 인터넷 등 공개된 외부 통신망과 접속되는 내부 정보통신망 및 정보처리시스템을 해킹 등 전자적 침해 행위로부터 보호하기 위하여 침입차단시스템 등 정보보호시스템을 설치하고, 침해행위 발생 즉시 침해사실을 탐지하여 대응할 수 있도록 대응 체계 구축

▣ 해설

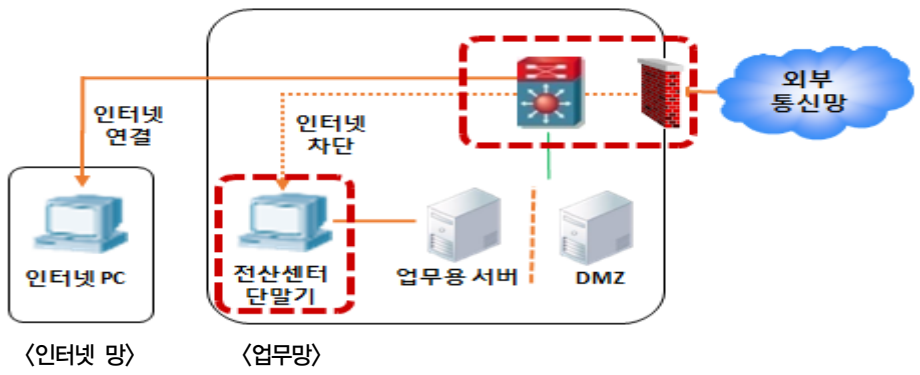
- 내부 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해 행위로부터 보호하기 위하여 침입차단 및 침입탐지시스템, 암호화프로그램, 등 정보보호시스템을 설치 및 운영(제1항제1호)
  - 대내외에서 정보처리시스템에 접속하는 경우 정보보호시스템을 우회하여 접속하지 못하도록 보안정책을 적절히 적용
- 운영체제 등 시스템프로그램 취약점을 이용한 침해에 대비하여 시스템프로그램의 보안 취약점 개선 등 긴급하고 중요한 사항은 즉시 보정작업 실시(제1항2호)

※ 금융회사등의 망분리(제1항제3호 및 제5호)

(1) 전산센터 망분리

- 전산센터 내에 위치한 정보시스템의 운영, 개발, 보안 목적으로 정보처리시스템(서버)에 직접 접속하는 단말기(전산센터 단말기)는 인터넷 등 외부통신망과 물리적으로 분리해야함(제1항제5호)
- 물리적 망분리란 통신회선을 업무용과 인터넷용으로 물리적으로 분리하고 별도 단말기를 사용하여야 하는 것으로 방화벽 정책 설정만으로 분리하는 방식은 물리적 망분리라고 할 수 없음
  - 또한, 단일 단말기에서 가상화 솔루션을 이용하여 망을 분리한 경우에도 물리적 망분리라고 할 수 없음(그림 1)

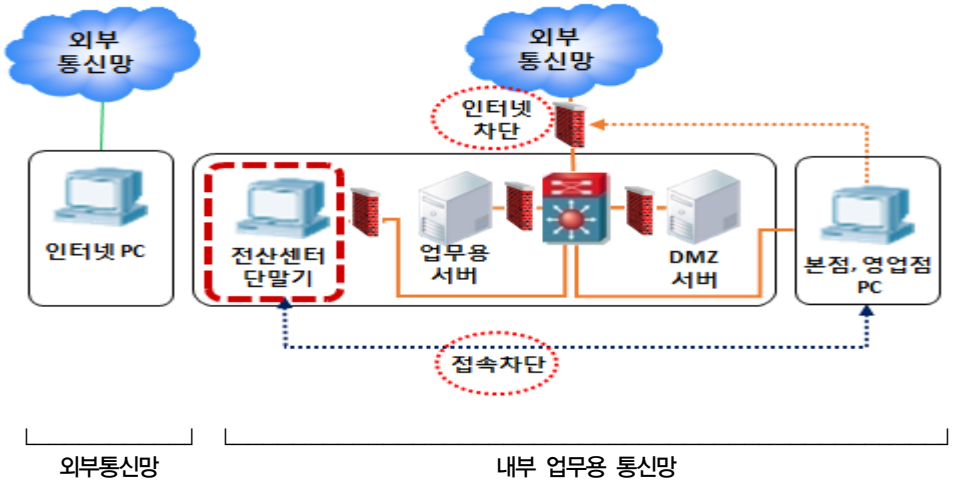
(그림1) 방화벽 정책만을 이용한 전산센터 단말기의 망분리



● 망분리를 완료한 시스템과 망분리를 적용하지 않은 시스템이 같은 내부망에 있는 경우, 망분리가 되지 않은 단말기를 통해 내부망에 악성코드 유입 등이 발생할 수 있으므로,

– 망분리 미적용 단말기를 통해 망분리를 적용한 시스템과 망분리를 적용하지 않은 시스템 사이는 방화벽 등의 네트워크 장비로 차단필요(그림2)

(그림2) 전산센터 단말기의 물리적 망분리 구성 예시



● 전산실 내에 위치한 정보처리시스템(서버)은 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(제1항제5호)

〈 전산센터 망분리 예외 〉

- 정보처리 업무를 국외 소재 전산센터에 위탁하여 처리하는 경우, 국외소재 전산센터는 논리적 망분리 가능(세칙 제2조의2제2항제1호)
- 업무상 불가피한 경우 내부망의 서버에서 특정 외부기관(참고1)과 연결가능 (세칙 제2조의2제2항제2호가목)
- DMZ 내 인터넷 뱅킹 등 공개서버(Web 서버)와 내부서버(WAS) 연결 가능 (세칙 제2조의2제2항제2호나목)
- 다른 계열사와 공동으로 사용하는 인트라넷, 이메일 시스템, 회계시스템과 내부 서버는 연결 가능(세칙 제2조의2제2항제2호다목)
- 비상시 제한적으로 외부망에서 내부망으로 원격 접속 가능(세칙 제2조의2제2항제3호)

(2) 본점·영업점 망분리

- 내부통신망과 연결된 본점 영업점 PC 및 프린터 등 주변 기기는 물리적 또는 논리적 방식으로 망분리(제1항3호)

〈 본점·영업점 망분리 예외(시행세칙 제2조의2제1항) 〉

– 업무상 불가피한 경우 내부망의 서버에서 특정 외부기관(참고1)과의 연결가능 (세칙 제2조의2제1항)

〈참고〉 특정 외부기관의 범위

– 행정자치부, 금융협회, 금융결제원, 예탁결제원, 코스콤, 금융보안원, 공인인증기관 등의 정부 또는 금융 유관기관

– 그 외 업무상 연결이 필요한 전자금융보조업자

※ 시행세칙 제2조의2의 취지는 망분리로 인한 업무의 비효율을 완화하고자 일부 필수적인 외부기관과의 연결을 허용하는 것으로, 불특정 다수가 접속하는 인터넷 포탈 등은 제한

(3) 망분리 예외 적용 절차

- 세칙 제2조의2제1항 또는 제2항에 의하여 전산센터 및 본점 영업점 망분리 예외를 적용하는 경우 ①자체위험성 평가를 실시하고 ②세칙 〈별표7〉에서 정한 망분리 대체 정보보호 통제를 적용하고 ③정보보호위원회 승인 후 적용(세칙 제2조의2제3항)

● 외부기관과 내부통신망 연결시 유의사항(제3호, 제5호)

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

〈 망분리 대체 정보보호통제 〉

대책	세부사항
내부망 보안 강화	– 업무망에 반입되는 전산자료 대상으로 악성코드 감염여부 진단·치료 대책 수립
외부망 보안 강화	– 지능형 해킹(APT)차단 대책 수립 – 외부망을 통해 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링 대책 수립
메일 시스템 보안 강화	– 본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립 – 메일을 통한 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링 대책 수립
단말기 보안 강화	– PC 사용자의 관리자 권한 제거 – 승인된 프로그램만 설치·실행토록 대책 수립 – 단말기 전산 자료 암호화 저장
원격 접속 통제 수립	– 원격접속 기준 및 절차가 포함된 보안정책 수립 – 불법 원격접속을 방지하기 위한 사용자인증, 암호화 등의 보안대책을 수립 – 원격접속은 책임자의 승인을 받은 사전 등록자에 한하여 허용하며 원격접속 관리 기록부를 기록·보관 – 원격에서 접속하는 외부 단말기와 내부 업무용 시스템 구간의 암호화 통신 – 원격접속 사용자는 아이디·비밀번호 이외에 추가 인증수단을 적용 – 원격에서 접속하는 외부 단말기의 악성코드 감염 예방 대책 수립·적용 – 원격접속 가능한 내부 업무용시스템의 접근 통제 수립·적용 – 원격으로 접속하여 수행한 모든 작업 내역 기록하고 매일 이상여부 점검 실시 및 책임자가 확인

● 침입차단시스템(Firewall) 등 정보보호시스템 설치장소는 비인가자 출입통제 등 보안관리를 철저히 하고 다음 사항 준수 및 점검(제2항)

- 업무목적상 필요한 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거
- 보안정책의 임의변경 금지(변경 통제절차 준용)

- 정보보호시스템의 원격관리를 금지하고 주기적으로 작동상태 점검
- 일반사용자계정 또는 제조사 설정 비밀번호 존재 여부
- 환경설정에 관련된 파일의 접근허용모드 정당 설정 여부
- 관리자 권한을 도용할 수 있는 프로그램 변경 및 은닉 여부
- 비인가자의 침입여부를 확인하기 위한 시스템 접근기록 등

● 규정 제23조의 비상대책 등 수립 시 해킹 및 사이버테러 발생에 즉시 대처 가능한 대응체계 및 비상연락망 등을 포함해야 하며, 정보처리시스템의 해킹 및 취약점에 대한 정기 진단 및 분석을 실시하고 분석결과 문제점에 대한 보완대책을 수립·시행하여 해킹 및 취약점에 의한 피해가 발생하지 않도록 조치(제4항)

● 무선통신망 설치 및 운용시 준수사항(제6항)

- 업무는 AP의 기능 단위가 아닌 분장 단위를 의미(청약업무, 민원처리 업무, 상담 업무 등)
- 비인가자에 의한 무선AP 접근을 방지하기 위하여 무선AP의 SSID 브로드캐스팅을 금지하고 숨김 기능을 적용하여 비인가자에게 무선AP가 노출되지 않도록 하며, 사용자 인증 강화를 위하여 사용자 ID/패스워드 이외에 단말기 MAC주소 인증 등을 추가한 인증방식을 적용
- 내부의 비인가 무선AP 설치 및 접속여부를 주기적으로 점검하고 통제하여 악의적인 의도로 설치된 비인가AP에 의한 중요정보 유출 방지
- 무선통신은 특성상 데이터가 실린 전파신호의 도청이 가능하여 무선통신망에서 데이터 암호화가 매우 중요하므로 보안이 취약한 WEP(Wired Equivalency Protocol) 방식보다는 WPA(Wi-Fi Protected Access)/WPA2방식 적용을 권장

※ 법령해석('15.12.7.)

〈 **질의요지** 〉

▣ 외부통신망에 위치한 보험설계사 및 GA대리점 사용 단말기의 경우에도 「전자금융감독규정」 제15조제1항 제3호에 따라 인터넷 등 외부통신망과 분리·차단 및 접속금지 하여야 하는 대상에 해당되는지 여부

▣ 이 경우, 보험설계사 및 GA대리점 단말기에 대해 VPN을 통해 인증된 사용자에 한하여 접속하도록 하고 일부 사이트(타 보험사 홈페이지 및 일부 포털 등)에 한하여 제한적으로 외부망 접근을 허용한 경우 망분리를 준수하고 있다고 판단할 수 있는지 여부

〈 회답 〉

▣ 외부통신망에 위치한 보험설계사 및 GA대리점 사용 단말기가 업무 처리 등을 위해 보험회사의 내부통신망에 연결되어 있는 경우 「전자금융감독규정」 제15조제1항제3호의 망분리 적용대상에 해당합니다.

○ 다만, 보험설계사나 외주직원의 단말기가 내부망과 분리된 망(DMZ 등)에 위치한 시스템에만 접속하는 경우에는 망분리 적용대상에 포함되지 않습니다.

▣ 제한적이라 할지라도 보험회사의 내부망에 연결되어 있는 단말기에 외부망 접근을 허용하는 것은 망분리 원칙을 위배하고 있는 것으로 보이며, 해당 단말기는 보험회사의 본점·영업점 단말기 수준의 망분리 기준에 적합하도록 운영되어야 할 것입니다.

〈 이유 〉

▣ 보험설계사 및 GA대리점은 「보험업법」에 따라 보험계약의 체결을 대리하는 등의 업무를 수행하고 있으며 이에 따라 보험회사의 영업점과 같이 내부 업무용시스템에 접속하여 업무를 처리할 필요가 있을 것으로 판단되는바,

○ 이러한 범위 내에서 해당 단말기는 「전자금융감독규정」 제15조제1항제3호의 '내부통신망과 연결된 내부업무용 시스템'에 해당되어 망분리 적용대상입니다.

▣ 보험설계사 및 GA대리점 사용단말기가 내부통신망에 연결되어 있는 경우 사실상 보험회사의 본점·영업점 단말기 역할을 수행하는 것으로 판단되므로 그와 동일한 수준의 보안통제가 필요할 것입니다.

○ 특히, 해당 단말기에서 보험회사 내부 전산망 이외에 외부 인터넷망을 동시에 사용하는 경우 악성코드 전파 등 비인가 접속 가능성이 있으므로 보험회사의 망분리 정책을 따르는 것이 적정합니다.

※ 법령해석('15.12.22.)

〈 질의요지 〉

▣ 논리적 및 물리적 망분리를 함에 있어 클라우드컴퓨팅서비스를 이용한 인터넷망 구성이 「전자금융감독규정」상 망분리 규정을 충족하는지 여부

〈 회답 〉

▣ 「전자금융감독규정」 제15조제1항에서는 전자금융거래의 안전성 확보를 위해 정보처리시스템 및 정보통신망의 해킹 방지를 위해 내부 업무용시스템은 인터넷 등 외부통신망과 분리·차단하도록 하고 있고, 전산실 내에 위치한 정보처리시스템과 이에 접속하는 단말기는 외부통신망과 물리적으로 분리를 하도록 하고 있으나, 망분리 방식을 특정하고 있지는 않습니다. 따라서 클라우드컴퓨팅서비스 이용 여부와 상관없이 망구성만으로 망분리 규정 만족 여부를 판단하시면 됩니다.

○ 다만, 망분리를 위한 시스템 설치 및 운영을 외부업체에 위탁할 경우, 「전자금융거래법」 제40조제6항의 정보보호 관련 업무 재위탁 금지, 「전자금융감독규정」 제15조제2항의 정보보호시스템의 설치 및 운영기준, 같은 규정 제60조의 외부주문등에 대한 기준 및 「금융회사의 정보처리 업무 위탁에 관한 규정」 등 관련 규정을 준수하여야 할 것입니다.

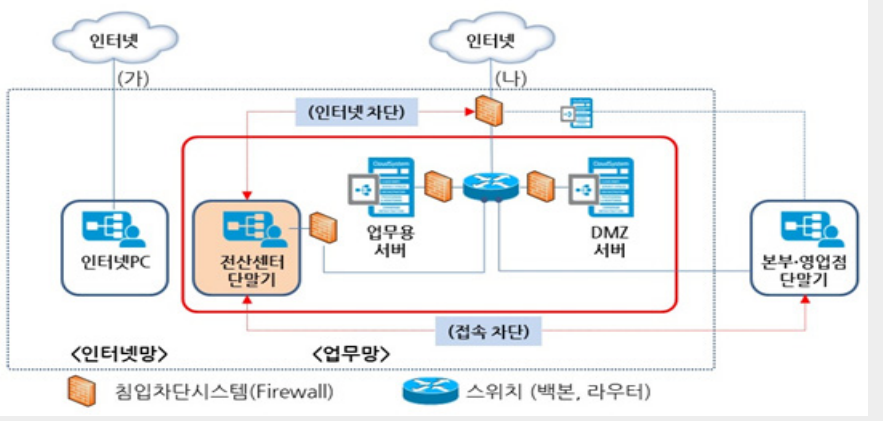
〈 이유 〉

▣ 「전자금융감독규정」상 망분리 방식은 특정하고 있지 않으며, 금융회사가 적절한 방식을 선택할 수 있습니다.

※ 비조치의견서('16.1.27.)

〈 요청대상 행위 〉

▣ 당 금융회사의 전산센터 단말기 물리적 망분리 방식이 전자금융감독규정 제15조제1항제5호에 위반되는지 여부



〈 판단 〉

▣ 전산센터 단말기를 인터넷과 물리적으로 분리하고, 시행세칙 제2조의2에 따라 망분리 예외가 적용된 정보처리시스템·내부 업무용 단말기와 연결을 방화벽 및 네트워크장비로 차단·통제하는 경우 전자금융감독규정 제15조제3호 및 제5호에 위배되지 않습니다.

〈 판단이유 〉

▣ 전자금융감독규정 제15조제1항제5호는 전자금융거래의 안전성 확보 및 정보처리시스템 및 정보통신망의 해킹 방지를 위해 전산실 내에 위치한 정보처리시스템과 이에 접속하는 외부통신망과 물리적으로 분리하도록 규정하였습니다.

- ○ 물리적 망분리란 통신망을 물리적으로 업무용과 인터넷용으로 분리하고 별도 단말기를 사용하여야 하는 것으로 방화벽 정책 설정으로만 분리하는 방식은 물리적 망분리라고 할 수 없습니다.
- ○ 다만, 전산실 내 정보처리시스템의 운영 등의 목적으로 직접 접속하는 단말기의 경우 금융회사는 시행세칙 제2조의2에 따라 외부통신망과 연결되는 내부 업무용시스템·정보처리시스템을 통해 간접적으로 외부통신망과 연결될 수 있으므로
- ○ 해당 연결지점을 통해 악성코드 유입 및 정보유출이 발생하지 않도록 방화벽 등의 네트워크 장비로 차단·통제하여야 합니다.

※ 비조치의견서('16.2.29.)

〈 요청대상 행위 〉

▣ 아래와 같은 통제를 전제로 당사 인터넷망을 무선통신망으로 사용하는 것이 전자금융감독규정 제15조 제6항을 준수하는지 여부

1. 인터넷망에 대한 무선통신망 이용에 대하여 CISO 사전 승인 처리하여 사용 예정

2. 무선통신망 불법 접속을 막기 위해 승인된 무선AP/사용자/단말기만 접속할 수 있도록 통제 적용할 것이며, 암호화 적용 예정
3. 현재 내부망에 연결된 단말기들은 무선통신망에 접속을 차단하는 솔루션을 적용하고 있으며, 비인가 무선AP들의 내부망 접속도 자동 차단되며, 실시간 모니터링 체계를 운영하고 있으며, 인터넷망도 동일한 통제체계를 운영할 예정
4. NAC(Network Access Control) 솔루션으로 비인가 무선AP의 설치·접속여부는 실시간으로 확인되며, 자동으로 당사 인터넷망 접속이 차단되도록 정책이 적용될 것이며, 주기적으로 무선AP에 대한 보안점검을 할 예정

〈 판단 〉

▣ 물리적 망분리가 이루어진 상태에서 무선통신망을 외부 인터넷망의 접속 용도로 사용을 제한하고, 질의사항에서 정한 통제 조치가 적절히 적용될 경우 전자금융감독규정 제15조제6항에 위배되지 않음

〈 판단이유 〉

▣ 전자금융감독규정 제15조의 취지는 금융회사 및 전자금융업자로 하여금 해킹과 같은 전자적 침해행위로부터 내부 업무망 및 이와 연계된 정보처리시스템을 보호하기 위한 것으로

○ 무선통신망을 인터넷망 접속 용도로 한정하여 이를 통한 내부망 접속이 차단될 경우, 귀사에서 제시한 통제장치가 적절히 적용됨을 전제로 전자금융감독규정 제15조제6항에 위배되지 않습니다.

▣ 다만, 비인가 무선AP가 내부망에 접속할 경우 즉시 차단하는 조치, 내부망에 연결된 정보처리시스템의 무선AP 접속 차단 조치가 적절히 시행될 필요가 있습니다.

※ 비조치의견서('16.4.14.)

〈 요청대상 행위 〉

▣ 지점 사용자 망분리 수행 시 지점과 전산센터간 통신회선을 1회선으로 구성하고 회선 양끝 연결을 VPN(내부망, 외부망)으로 구분하여 망분리 구성이 가능한지 여부

1. 통신 회선 : 1회선
2. VPN : 2대(내부망 1대, 외부망 1대)
3. 통신 방법
   - 내부망 : 업무PC → 내부망 VPN(지점) → 통신회선(공용) → 내부망 VPN(전산센터) → 내부시스템
   - 외부망 : 인터넷PC → 외부망 VPN(지점) → 통신회선(공용) → 외부망 VPN(전산 센터) → 인터넷

〈 판단 〉

▣ 전자금융감독규정 제15조제1항제3호에 따라 내부통신망과 연결된 업무용시스템의 망분리가 이루어진 상태에서, VPN(가상사설망) 장비를 이용하여 하나의 통신 회선에서 내부망과 외부망을 분리하여 사용하는 경우 전자금융감독규정 제15조제1항제3호에 의한 망분리 의무 규정에 위배되지 않습니다.

〈 판단이유 〉

▣ 지점 단말기는 전자금융감독규정 제15조제1항제3호에 따라 내부통신망과 연결된 내부 업무용시스템을 외부통신망과 분리·차단하거나 접속을 금지하여야 하며,

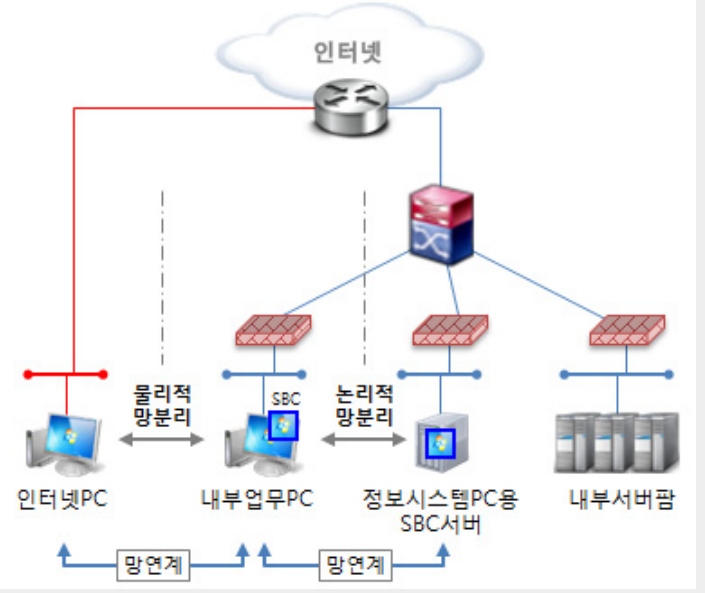
○ 이와 같은 망분리는 외부통신망과의 분리·차단 등을 의미하는 것으로 통신회선에서의 물리적인 분리에 대한 의무사항을 내포하지는 않습니다.

▣ 다만, 하나의 통신 회신에서 VPN 장비로 내·외부망을 분리할 경우 내부 업무용시스템을 외부통신망으로부터 분리하기 위한 VPN 정책설정에 유의하시기 바랍니다.

※ 비조치의견서('16.6.9)

〈 요청대상 행위 〉

▣ 정보처리시스템 운영·개발·보안 목적의 단말기를 별도의 업무用 SBC(Server Based Computing)방식으로 구성하는 것이 가능한지 여부



〈 판단 〉

▣ 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기(이하 '전산센터 단말기')를 SBC로 구성하는 것은 전산센터 단말기가 외부통신망으로부터 물리적으로 분리된 것으로 볼 수 없어 관련 규정에 위배됩니다.

〈 판단이유 〉

▣ 금융회사는 전자금융거래의 안전성 확보 및 정보처리시스템 등의 해킹 방지를 위해 전산실 내에 위치한 정보처리시스템을 외부통신망으로부터 물리적으로 분리하여야 합니다.(전자금융감독규정 제15조제1항제5호)

▣ 금융회사 등은 전자금융감독규정시행세칙 § 2의2②iv에 따라 전산센터 단말기와 외부통신망과 연결구간, 업무용 시스템과의 연결 구간을 각각 차단한 경우는 물리적 망분리를 적용하지 않을 수 있으나,

○ 문의하신 구성은 전산센터 단말기가 업무용 단말기에 설치된 SBC Client를 통해 접속하는 방식으로, 두 단말기의 연결구간이 차단되었다고 볼 수 없어 물리적 망분리 예외규정에 해당하지 않습니다.

※ 비조치의견서('16.6.9.)

〈 요청대상 행위 〉

▣ 망분리 관련 보안솔루션 적용시 보안망, 인터넷망, 업무망으로 분리하고 방화벽을 통해 각각의 보안솔루션을 포트만 오픈하며, 업무망 및 인터넷망을 관리하는 것이 가능한지 여부

〈 판단 〉

▣ 요청하신 방식의 경우 「전자금융감독규정」제15조제1항제3호에 위배되는 것으로 판단됩니다.

〈 판단이유 〉

▣ 금융회사는 전자금융거래의 안전성 확보 및 정보처리시스템 등의 해킹 방지를 위해 「전자금융감독규정」 제15조제1항제3호에 따라 내부통신망과 연결된 내부 업무용시스템을 인터넷 등 외부통신망과 분리·차단하거나 접속을 금지시켜야 합니다.

▣ 방화벽과 같은 보안장비를 이용하여 통제하더라도 외부망에서 업무망으로 접속할 수 있는 방법이 열려 있을 경우 외부망과 내부망을 분리·차단한 것에 해당하지 않으므로,

○ 하나의 보안솔루션을 인터넷망과 업무망 모두에서 사용하기 위해 네트워크 간 접속이 가능한 경우 위 규정에 위배된다고 할 수 있습니다.

▣ 아울러 금융전산 망분리 가이드라인('13.9월)은 존속기간이 경과하여 효력이 소멸하였음을 알려드립니다.

※ 비조치의견서('16.6.16.)

〈 요청대상 행위 〉

▣ 물리적 망분리를 한 상태에서 보안USB 서버, 내부정보유출방지(DLP) 서버, 네트워크접근제어(NAC) 서버, 패치관리시스템(PMS)을 인터넷망에 구축해야 하는지 여부

〈 판단 〉

▣ 물리적 망분리와 관계없이 단말기 보호 및 정보처리시스템의 안전한 운영 등을 위해 관련 규정을 준수하여야 합니다.

〈 판단이유 〉

▣ 금융회사는 정보유출 등의 방지를 위하여 보조기억매체 및 휴대용 전산장비에의 접근을 통제하는 등 단말기 보호를 위해 필요한 사항을 준수하여야 하며(전자금융감독규정 제12조),

○ 긴급하고 중요한 보정사항에 대해서는 즉시 보정 작업을 하는 등 정보처리시스템의 안전한 운영을 위하여 필요한 보호대책을 수립·운용하여야 합니다(전자금융감독규정 제14조).

▣ 이는 금융회사의 단말기 및 정보처리시스템을 보호하기 위한 것으로 망분리와 관계없이 정보 유출 또는 정보 처리시스템의 불안전한 운영과 관련한 위험이 있다면 해당 규정을 준수하여야 할 것입니다.

※ 비조치의견서('16.6.16.)

〈 요청대상 행위 〉

▣ 정보처리시스템에 직접 접근할 수 있는 권한이 없고, 개인정보를 취급하지 않는 임직원이 어플리케이션을 통해 제한된 업무만을 취급하기 위해 업무망에 원격 접속을 할 경우 망분리관련 규정을 위반하는지 여부

〈 판단 〉

▣ 전자금융감독규정시행세칙 제2조의2에서 정한 예외 사항에 해당하지 않을 경우 망 분리 의무를 규정한 전자금융감독규정 제15조제1항제3호를 위반하는 것으로 판단됩니다.

〈 판단이유 〉

▣ 금융회사는 전자금융감독규정 제15조제1항제3호에 따라 내부망과 연결된 내부 업무용시스템을 외부통신망으로부터 분리·차단 등의 조치를 취하여야 합니다.

○ 재택근무 및 출장 등을 위한 원격 접속의 경우 외부 인터넷망과의 연결로 인하여 악성코드의 업무망으로의 유입 등의 위험을 배제할 수 없어 망분리 예외로 인정하기 어려울 것으로 판단됩니다.

※ 비조치의견서('16.8.4.)

〈 요청대상 행위 〉

▣ 전산센터 내에 정보처리시스템을 운영, 개발 및 보안 등을 위해 직접 접속하는 전산센터 (중요)단말기를 가상PC(VDI)로 구성하여 운영할 경우 물리적 망분리 요건을 충족하는지 여부

〈 판단 〉

▣ 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기(이하 '전산센터 단말기')를 가상PC(VDI)로 구성하는 것은 전산센터 단말기를 외부통신망으부터 물리적으로 분리한 것으로 볼 수 없어 관련 규정을 준수하지 못한 것으로 보입니다.

〈 판단이유 〉

▣ 금융회사는 정보처리시스템 등의 해킹 방지를 위해 전산실 내에 위치한 정보처리시스템 및 전산센터 단말기를 외부통신망으로부터 물리적으로 분리하여야 하나(전자금융감독규정 제15조제1항제5호),

○ 전산센터 단말기와 외부통신망 및 내부 업무용시스템과의 연결구간을 각각 차단한 경우 등 예외 사유에 해당할 경우 관련 규정에 따라 물리적으로 분리하지 않을 수 있습니다(동 규정 시행세칙 제2조의2제2항제4호).

▣ 전산센터 단말기를 내부 업무용시스템에 연결하여 가상PC(VDI)를 구성하면 동일한 단말기에서 전산실 내 정보처리시스템과 내부 업무처리시스템에 대한 접근이 가능해집니다.

○ 물리적 망분리는 별도의 회선과 단말기를 사용하는 것이므로 가상PC(VDI)를 구성하여 하나의 단말기로 내부 업무용시스템과 전산실 내 정보처리시스템에 접근 가능할 경우 동 단말기는 물리적으로 분리된 것으로 보기 어려우며,

○ 전산센터 단말기를 가상PC(VDI)로 구성하는 것은 내부 업무용시스템과의 연결 구간을 방화벽으로 차단한 것과 같은 것으로 보기에는 아직까지 충분히 실증되었다고 보기 어려우므로 물리적 망분리 예외에 해당하지는 않는 것으로 해석됩니다.

※ 비조치의견서('16.8.4.)

〈 요청대상 행위 〉

▣ 직원의 출장 또는 자택 근무 등으로 인하여 외부 인터넷망에서 회사 내부망 접속이 필요한 경우, 내부 승인절차를 거친 후 방화벽으로 분리·독립된 내부망의 VDI(Virtual Desktop Infrastructure : 데스크탑 가상화)를 통하여 업무처리가 가능한지 여부

〈 판단 〉

▣ 원격접속을 위해 기존 내부 업무용망과 분리·독립된 망을 별도로 구성하여 차단·통제 조치를 할 경우 전자금융감독규정 제15조제1항제3호에서 정한 망분리 규정을 준수한 것으로 볼 수 있습니다.

〈 판단이유 〉

▣ 금융회사는 내부 업무용시스템이 악성코드에 감염되어 정보유출·자료파괴 등 해킹 공격에 노출되는 것을 방지하기 위하여 내부통신망과 연결된 내부 업무용 시스템을 외부통신망과 분리·차단 및 접속금지 조치를 하여야 합니다(전자금융감독규정 제15조제1항제3호).

▣ 외근직원의 원격 근무를 위해 방화벽으로 분리·독립된 VDI를 별도로 구성한 경우 내부 업무용시스템은 외부통신망으로부터 차단된 것으로 볼 수 있어 관련 규정에서 정한 망분리 의무를 준수한 것으로 보여집니다.

○ 다만 비인가자의 내부망 접속 방지, 통신구간에 대한 암호화 등 정보유출 및 악성코드 감염 등의 사고를 방지하기 위한 보안대책의 수립·운영에 주의를 기울여 주시기 바랍니다.

※ 비조치의견서('16.11.24.)

〈 요청대상 행위 〉

▣ 전산실 내 정보처리시스템의 운영·개발·보안 목적으로 직접 접속하는 단말기(이하 '전산센터 단말기')를 내부 업무용시스템과의 연결 구간을 차단하고, 내·외부망과 방화벽으로 각각 차단된 가상PC(VDI)를 통해 전산실 내 정보처리시스템에 접속하는 것이 가능한지 여부

〈 판단 〉

▣ 귀사가 구성하고자 하는 가상PC가 '전산실 내에 위치한 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기'에 해당할 경우 외부통신망 과의 연결 구간 및 내부 업무용 시스템과의 연결 구간을 각각 차단한다면 시행 세칙 제2조의2제2항제4호에서 정한 예외규정을 준수한 것으로 보입니다.

〈 판단이유 〉

▣ 금융회사는 정보처리시스템 등의 해킹 방지를 위해 전산실 내에 위치한 정보처리시스템 및 전산센터 단말기를 외부통신망으로부터 물리적으로 분리하여야 하나(전자금융감독규정 제15조제1항제5호),

○ 전산센터 단말기와 외부통신망 및 내부 업무용시스템과의 연결 구간을 각각 차단한 경우 등 예외사유에 해당할 경우 관련 규정에 따라 물리적으로 분리하지 않을 수 있습니다(동 규정 시행세칙 제2조의2제2항제4호).

▣ 전산센터 단말기를 내·외부망과의 연결구간이 각각 차단된 VDI로 구성한다면 망분리 예외를 규정한 전자금융감독규정 시행세칙 제2조의2 제2항제4호를 준수하는 것으로 볼 수 있으며, 내부망과 차단된

단말기로 위 VDI에 접속하더라도 내·외부망과는 여전히 차단되어 망분리 예외규정에 해당하는 것으로 보입니다.

○ 다만 비인가자의 내부망 접속 방지, 통신구간에 대한 암호화 등 정보유출 및 악성코드 감염 등의 사고를 방지하기 위한 보안대책의 수립·운영에 주의를 기울여 주시기 바랍니다.

※ 비조치의견서('16.12.19.)

〈 요청대상 행위 〉

▣ 지도서비스 제공 업체를 망분리 예외 규정에 의한 '특정 외부기관'으로 지정 하여 전자금융감독규정시행세칙 제2조의2제1항에 따라 내부통신망과 연결된 내부업무용 시스템에서 접속 가능한지 여부

〈 판단 〉

▣ 불특정 다수가 이용하는 지도서비스 제공 업체는 전자금융감독규정시행 세칙 제2조의2제1항에 의한 '특정 외부기관'에 포함되지 않아 망분리 예외 대상으로 보기 어렵습니다.

〈 판단이유 〉

▣ 금융회사는 정보처리시스템 등의 해킹 방지를 위해 내부통신망과 연결된 내부 업무용시스템에 대해 인터넷 등 외부통신망과 분리·차단 및 접속 금지 등의 조치를 하여야 하며(전자금융감독규정 제15조제1항제3호),

○ 내부 업무용시스템을 업무상 필수적으로 특정 외부기관과 연결해야 하는 경우, 예외적으로 망분리 대체 정보보호통제 적용, 정보보호위원회 승인 등의 절차를 거쳐 분리·차단 등의 조치를 하지 않을 수 있습니다(전자금융감독규정시행세칙 제2조의2제1항, 제4항).

▣ 시행세칙 제2조의2제1항에서 업무상 필수적으로 연결이 필요한 '특정 외부 기관'에는 정부, 금융유관기관 및 전자금융보조업자 등과 같이 전자금융업 무의 수행을 위해 반드시 필요한 기관이 포함되나

○ 금융회사와 별도의 계약 등에 따라 보안이 관리되지 않고 불특정 다수가 접속하는 서비스 운영 업체의 경우에는 특정 외부기관으로 보기 어렵습니다.

6. 악성코드 감염 방지대책

〈 감독규정 〉

제16조(악성코드 감염 방지대책) ① 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다.

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

② 금융회사 또는 전자금융업자는 악성코드 감염이 발견된 경우 악성코드 확산 및 피해를 최소화하기 위하여 필요한 조치를 신속하게 취하여야 한다.

▣ 악성코드(Malicious Code)는 컴퓨터에서 사용자의 허락 없이 스스로를 복사하거나 변형한 뒤 정보유출, 시스템 파괴 등의 작업을 수행하여 사용자에게 피해를 주는 프로그램으로 웜, 바이러스, 트로이목마, 스파이웨어, 애드웨어, 루트킷 등으로 분류

- 악성코드 감염경로는 스팸메일, 이동식저장매체, 악성코드가 포함된 웹페이지 접속, 메신저, P2P프로그램 등이 주요 경로
- 또한, 악성코드에 감염된 경우에는 전파 속도가 빠르고 치료 및 데이터 복원을 위해 금전적·시간적·심리적인 손해뿐만 아니라 해당 금융회사의 신뢰도에 치명적인 영향을 줄 수 있으므로 실효성 있는 대책 마련 필요

▣ 해설

- 악성코드 감염을 방지하기 위하여 다음 사항에 유의하여 정보처리시스템을 관리(제1항)
  - 출처, 유통경로 및 제작자가 명확하지 아니한 응용프로그램은 악성코드 검색프로그램으로 진단 후 사용
  - 전산시스템의 규모, 메일서버의 중요성 등을 고려하여 필요한 경우 악성코드 검색서버를 설치하여 외부에서 들어오는 메일 등에 대하여 사전 검색할 수 있는 체계 구축
  - 개인용 단말기 및 서버군의 악성코드 감염여부에 대하여 정기적으로 점검 실시 및 기록 보관
  - 정기적으로 악성코드 검색프로그램의 엔진 업데이트를 수행하도록 엔진 업데이트의 예약을 설정한 후 사용
  - 악성코드 검색 및 치료 프로그램의 실시간 감시 기능을 이용하여 정보처리시스템 보호
- 악성코드 감염이 발견된 경우 업무 담당자는 악성코드 확산 및 피해를 최소화하기 위하여 다음과 같이 적절한 조치 실행(제2항)
  - 악성코드 감염사실을 신속히 신고할 수 있도록 연락체계 구축
  - 악성코드에 감염된 시스템의 사용중지 또는 내부망에서 분리
  - 악성코드 검색 및 치료 프로그램을 이용하여 악성코드 치료
  - 감염확산 방지를 위하여 사용자에게 관련 사실 및 보안조치사항을 즉시 전달
  - 감염의 재발을 방지하기 위하여 원인분석 및 예방조치 수행

7. 홈페이지 등 공개용 웹서버 관리대책

〈 감독규정 〉

제17조(홈페이지 등 공개용 웹서버 관리대책) ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.

1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간"이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것
2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것
3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것
4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)

② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.

1. 게시자료에 대한 사전 내부통제 실시
2. 무기명 또는 가명에 의한 게시 금지
3. 홈페이지에 자료를 게시하는 담당자의 지정·운용
4. 개인정보의 유출 및 위·변조를 방지하기 위한 보안조치

③ 삭제

④ 금융회사 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 한다.

⑤ 금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.

▣ 공개용 웹서버는 외부 이용자에게 홈페이지 및 업무서비스를 제공하기 위해 운영되므로 내부서버와 달리 외부로부터 접근이 허용되므로 보안상 취약점을 이용한 해커의 공격에 취약하여 이에 대한 보안 조치가 필요

▣ 해설

- 웹서버, 메일서버 등 공개용 웹서버를 외부 해킹 등 악의적인 접근으로부터 보호하기 위해 1차 침입차단시스템과 2차 침입차단시스템 사이(DMZ구간)에 설치하고 네트워크 및 웹 접근제어 수단 등으로 보호(제1항제1호)
  - 공개용 웹서버가 침해당하더라도 외부 유해 트래픽이 웹서버를 경유해서 내부 네트워크로 침입이 불가능하도록 침입차단시스템 구성
- 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자로 제한하고 보안강화를 위하여 사용자ID/패스워드 인증이외에 추가적인 인증수단을 적용(제1항제2호)

- 공개용 웹서버 운영에 필요한 최소한의 서비스만을 제공하고 불필요한 서비스는 반드시 제거(제1항제3호)
  - 공개용 웹서버에서는 개발 및 테스트 도구 등의 사용을 금지하며, 공개용 웹서버에 반영하기 위한 프로그램의 변경, 수정 및 테스트는 반드시 별도의 개발 및 테스트 서버에서 실시

- 공개용 웹서버 해킹에 의한 이용자 정보 등 주요정보 유출방지를 위하여 DMZ구간 내에는 이용자 정보 등 주요 정보의 저장 및 관리를 금지함 다만, 거래로그 관리를 위해 이용자 정보 등의 저장이 필요한 경우에는 반드시 암호화하여 저장·관리(제1항제4호)

- 공개 게시자료에 대한 사전 내부통제는 업무종류, 내용 등에 대하여 포괄적으로 적용하며 게시자료의 개인정보 포함여부 등에 대한 내부통제 절차를 마련·실시하고, 자료게시 담당자를 지정하고 자료게시는 지정된 담당자로 제한(제2항제1호, 제3호)

- 자료게시는 무기명 또는 가명 게시를 금지하여 게시자료에 대한 신뢰도 확보와 문제발생시 책임관계 명확화(제2항제2호)

- 홈페이지 서버 등에 게재되는 내용에는 개인정보 등 중요정보가 유출되거나 위·변조되지 않도록 게시기간이 만료된 정보의 삭제, 개인을 식별할 수 있는 정보는 마스킹하여 게재, 화면 위·변조 방지 등의 조치(제2항제4호)

- 공개용 웹서버의 취약점이 노출되어 해커의 공격을 받지 않도록 주기적으로 점검을 실시하고 적절한 대응조치를 마련하여 비인가자의 접근을 허용하거나 서버에 저장된 고객정보 유출 및 웹서버의 비정상적인 동작을 야기하는 일련의 공격에 대응(제4항)

- 직원들이 단말기를 이용하여 음란, 도박 등 업무와 관련이 없는 인터넷 사이트에 접근할 경우 동 사이트를 통하여 스파이웨어, 바이러스 등 악성코드에 감염되고 내부통신망을 통해 조직 내에 전파될 우려가 있으므로 불필요한 사이트의 접근 통제대책을 강구(제5항)

8. IP주소 관리대책

〈 감독규정 〉

제18조(IP주소 관리대책) 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다.

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

▣ IP는 외부에서 해킹 시 가장 먼저 필요한 정보이므로 내부 IP는 외부에 노출되지 않도록 하여야 함. 즉, 외부 접속용 IP는 공인 IP체계, 내부IP는 사설 IP체계를 사용하고 NAT[4] (Network Address Translation)기능을 이용하여 IP를 관리

▣ 해설

- 내부망에서 사용하는 IP주소는 사설주소체계를 사용하고, 공인IP를 제외하여 구성. 외부로 접속시 NAT기능을 이용하여 사설주소체계를 공인주소로 변환(제1호)
- 내부직원의 개인별 IP 사용은 보안사고의 예방 및 사고 발생 시 원인 추적을 위한 것으로 반드시 개인별로 부여하고 가능한 고정IP를 부여. 다만, 업무담당자(네트워크 관리자 등)가 개인별로 IP를 부여하고 개인별 IP 부여 및 변경현황을 기록·관리할 경우 DHCP(Dynamic Host Configuration Protocol)방식도 사용 가능(제2호)
- 내부직원이 인터넷접속 시 접속일시, 출발지 및 목적지 IP, 접속포트(Port), 사설IP주소 등을 포함하여 1년 이상 기록·보관(제3호)
- 정보처리시스템의 개발담당, 운영담당, 외주직원 등에 대해 업무특성별로 네트워크를 분리하여 IP를 부여함으로써 각 네트워크별 업무특성에 따른 적절한 접근권한 통제 등 보안정책을 적용하여 보안 강화(제4호)

4) 공개된 인터넷과 사설망 사이에 방화벽(Firewall)을 설치하여 외부 공격으로부터 사용자의 통신망을 보호하는 기본적인 수단으로 활용할 수 있음. 이때 외부 통신망 즉 인터넷망과 연결하는 장비인 라우터에 NAT를 설정할 경우 라우터는 자신에게 할당된 공인 IP주소만 외부로 알려지게 하고, 내부에서는 사설 IP주소만 사용하도록 하여 필요시에 이를 서로 변환시켜 줌. 따라서 외부 침입자가 공격하기 위해서는 사설망의 내부 사설 IP주소를 알아야 하기 때문에 공격이 불가능해지므로 내부 네트워크를 보호할 수 있음

● 한 건물에 여러 기관이 상주하는 경우 금융회사 및 전자금융업자는 같은 건물에 상주하는 다른기관과 네트워크를 적절히 분리하여 내부망을 구성하고 타 기관에서 금융회사 및 전자금융업자의 침입차단시스템을 우회한 내부망 접속 금지(제5호)

※ 비조치의견서('15.7.30.)

〈 요청대상 행위 〉

▣ 외주직원이 운영시스템과 같은 내부망에 업무상 반드시 접속이 필요한 경우 내부 IP를 발급하는 행위가 전자금융감독규정 제18조에 위반되는지 여부

〈 판단 〉

▣ 요청대상 행위는 전자금융감독규정 제18조에 위반되지 않는 것으로 판단됩니다.

〈 판단이유 〉

▣ 전자금융감독규정 제18조제4호에 따르면, "정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP를 사용" 해야 하는데,

○ 이는 업무의 종류에 따라 IP그룹을 별도로 지정하여 해당 업무와 무관한 자의 접근을 제한하라는 의미로, 외주직원은 반드시 외부IP를 사용해야 한다고 볼 수는 없는 것으로 사료됩니다.

▣ 따라서 정보처리시스템 접근권한이 분리되어 있고 업무상 필요한 경우 외주직원에 대한 내부IP부여도 가능한 것으로 판단됩니다.

※ 비조치의견서('15.9.30.)

〈 질의 〉

▣ IP주소 부여와 관련하여 다음의 각 관리방안이 전자금융감독규정(이하 '감독규정') 제18조를 준수한 것인지 여부

○ (1안)PC별로 고정IP를 부여하되 PC당 2인의 사용자를 등록하고 사용자 인증을 거쳐 사용하는 방법

○ (2안)개인별로 IP를 부여하되 고정IP가 아닌 DHCP방식*으로 부여하고 변경현황을 관리하는 방법

* DHCP(Dynamic Host Configuration Protocol)서버로부터 임의의 유동IP를 할당받아서 쓰는 방식

〈 회신 〉

▣ 1안은 감독규정 제18조에 위반되나, 2안의 경우 동 규정을 준수한 것으로 판단됩니다.

〈 이유 〉

▣ 전자금융감독규정 제18조제4호에 따르면, "정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP를 사용"해야 하는데,

○ 이는 업무의 종류에 따라 IP그룹을 별도로 지정하여 해당 업무와 무관한 자의 접근을 제한하라는 의미로, 외주직원은 반드시 외부IP를 사용해야 한다고 볼 수는 없는 것으로 사료됩니다.

▣ 따라서 정보처리시스템 접근권한이 분리되어 있고 업무상 필요한 경우 외주직원에 대한 내부IP부여도 가능한 것으로 판단됩니다.

※ 비조치의견서('15.11.6.)

〈 질의 〉

▣ 외주직원이 운영시스템과 같은 내부망에 업무상 반드시 접속이 필요한 경우 내부 IP를 발급하는 행위가 전자금융감독규정 제18조에 위반되는지 여부

〈 회신 〉

▣ 요청대상 행위는 전자금융감독규정 제18조에 위반되지 않는 것으로 판단됩니다.

〈 이유 〉

▣ 전자금융감독규정 제18조제4호에 따르면, "정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP를 사용"해야 하는데,

○ 이는 업무의 종류에 따라 IP그룹을 별도로 지정하여 해당 업무와 무관한 자의 접근을 제한하라는 의미로, 외주직원은 반드시 외부IP를 사용해야 한다고 볼 수는 없는 것으로 사료됩니다.

▣ 따라서 정보처리시스템 접근권한이 분리되어 있고 업무상 필요한 경우 외주직원에 대한 내부IP부여도 가능한 것으로 판단됩니다.

제5절 정보기술부문 내부통제

1. 정보기술부문 계획서

〈 감독규정 〉

제19조(정보기술부문 계획서 제출 절차 등) ① 시행령 제11조의2에 따라 금융위원회에 정보기술부문 계획서를 제출해야 하는 금융회사 또는 전자금융업자는 현실적이고 실현 가능한 장·단기 정보기술부문 계획을 매년 수립·운용하여야 한다.

② 금융위원장은 금융감독원장으로 하여금 정보기술부문 계획서의 적정성 등을 평가한 후 관련보고서를 제출하게 할 수 있다.

▣ 정보화는 많은 투자비용이 소요되고, 전산화 방향이 금융회사 및 전자금융업자의 경영전략에 부합되지 않을 경우에는 대외 경쟁력을 상실하게 될 뿐만 아니라 기 투자된 비용을 회수하기가 곤란하여 예산낭비를 초래하므로 이를 방지하기 위해 적절하고 타당한 장·단기 계획을 수립하여 정보화 추진

▣ 해설

- 정보화계획은 전략기획(장기계획)과 운용계획(단기계획)으로 구분하여 실현가능한 장·단기 정보기술부문 계획을 매년 수립(제1항)하여 대표자의 확인·서명을 받아 금융감독원에 제출

※ 관계 법령

〈 법 〉

제21조(안전성의 확보의무) ④ 대통령령으로 정하는 금융회사 및 전자금융업자는 안전한 전자금융거래를 위하여 대통령령으로 정하는 바에 따라 정보기술부문에 대한 계획을 매년 수립하여 대표자의 확인·서명을 받아 금융위원회에 제출하여야 한다.

〈 시행령 〉

제11조의2(정보기술부문 계획수립의 대상 금융회사 등) ② 법 제21조제4항에 따른 정보기술부문에 대한 계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 정보기술부문의 추진목표 및 추진전략
2. 정보기술부문의 직전 사업연도 추진실적 및 해당 사업연도 추진계획
3. 정보기술부문의 조직 등 운영 현황
4. 정보기술부문의 직전 사업연도 및 해당 사업연도 예산

5. 그 밖에 안전한 전자금융거래를 위하여 정보기술부문에 필요한 사항으로서 금융위원회가 정하여 고시하는 사항

③ 법 제21조제4항에 따른 정보기술부문에 대한 계획은 매 사업연도 초일(初日)부터 3개월 이내에 금융위원회에 제출하여야 한다.

④ 제2항에 따라 정보기술부문에 대한 계획에 포함되어야 하는 사항의 세부내용이나 제출방법 등에 관하여 필요한 사항은 금융위원회가 정하여 고시한다.

제30조(권한의 위탁) ①금융위원회는 법 제48조에 따라 다음 각 호의 업무를 금융감독원장에게 위탁한다.

1의2. 법 제21조제4항에 따른 정보기술부문에 대한 계획의 접수

▣ 시행령 개정에 의거, 정보기술부문 계획서 제출처가 금융위에서 금감원으로 변경됨에 따라 업무보고서 내 접수 시스템 마련

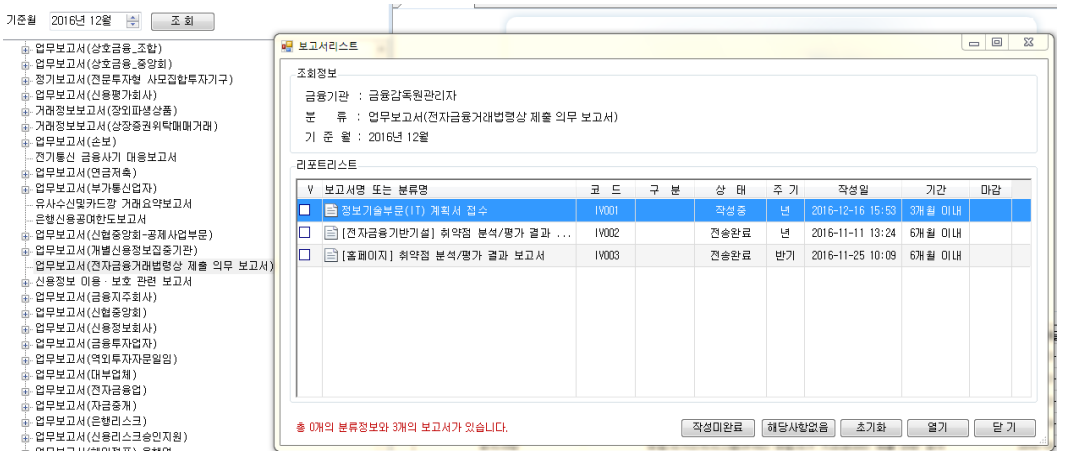
- '17년 1월부터 제출하는 정보기술부문 계획서는 금융정보교환망*의 「금융감독원 보고서 작성기」를 이용하여 제출

  * 금융정보교환망 : fines.fss.or.kr, 헬프데스크 : 02)3145-5401/5413

▣ 기준월을 회계연도 마감월로 선택하여 조회를 누르면, 업무보고서(전자금융거래법령상 제출의무 보고서)가 선택되며,

- 이 중 '정보기술부문(IT) 계획서 접수'를 선택하여 보고서 제출 전 자체 체크리스트 점검 후 보고서를 제출

※ 보고서 제출은 회계연도 마감 이후 3개월 이내에 회계연도 마감월의 보고서 항목을 조회하여 제출(마감 이후 제출 불가)



(참고) 정보기술부문 계획서 제출 유의사항

▣ 정보기술부문 계획서 양식*을 준수하고, 제출 전 체크리스트를 통해 스스로 필수 제출 항목의 이행 여부의 확인

* (첨부1) 정보기술부문 연간 계획서 양식 참고

- 또한, 작성한 정보기술부문 계획서 내용의 전자금융거래법령 및 규정 준수 여부에 대해 스스로 점검 후 제출

〈 정보기술부문 계획서 점검 자체 체크리스트 〉

평가 항목	평가 근거	정보기술부문 계획서 자체 점검	
		제출 포함 여부	법규 준수여부
①제출 기한 준수 (3개월 이내 제출)	令 § 11의2 ③	YES/NO/대상외	–
②대표이사의 확인 후 제출	法 § 21 ④	YES/NO/대상외	–
③정보보호위원회의 심의·의결	規 § 8의2 ③	YES/NO/대상외	–
④(내용) 추진 목표 및 전략	令 § 11의2 ②	YES/NO/대상외	적정/부적정
⑤(내용) 직전 연도 추진 실적	令 § 11의2 ②	YES/NO/대상외	적정/부적정
⑥(내용) 당해 연도 추진 계획	令 § 11의2 ②	YES/NO/대상외	적정/부적정
⑦(내용) 조직 등 인력 운영 현황	令 § 11의2 ②	YES/NO/대상외	적정/부적정
⑧(내용) 전년 및 금년 예산	令 § 11의2 ②	YES/NO/대상외	적정/부적정

2. 정보보호교육

〈 감독규정 〉

제19조의2(정보보호 교육계획의 수립 시행) ① 정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 필요한 교육프로그램을 개발하고, 다음 각 호의 기준에 따라 매년 교육계획을 수립·시행하여야 한다.

1. 임원 : 3시간 이상(단, 정보보호최고책임자는 6시간 이상)
2. 일반직원 : 6시간 이상
3. 정보기술부문업무 담당 직원 : 9시간 이상
4. 정보보호업무 담당 직원 : 12시간 이상

② 최고경영자는 정보보호교육을 실시한 이후 대상 임직원에 대해 평가를 실시하여야 한다.

③ 제1항의 교육프로그램 개발과 정보보호교육은 정보보호 전문 교육기관에 위탁할 수 있다.

▣ 정보보호를 위해 가장 중요한 것은 임직원의 보안인식이므로 보안인식 강화를 위해 매년 임직원에 대한 정보보호 교육계획을 수립하여 시행

▣ 해설

- 정보보호최고책임자는 임·직원의 정보보호 인식제고 및 업무수행역량강화를 위하여 일반임원, CISO, 일반직원, IT담당직원, 정보보호업무 담당직원 등 임직원의 역할 및 직무에 따라 최소 이수교육시간 이상이 이행될 수 있도록 연간 정보보호교육계획을 수립·운영하며, 교육효과 제고를 위하여 교육 후 평가 실시(제1항, 제2항)
  - 금융회사 자체적 기준에 의하여 평가 가능하며 위탁기관 평가 기준을 활용할 수 있으나, 평가 없이 특정 교육 과정의 이수만으로 대체 불가
- 임직원 역할 및 직무별 최소이수교육시간
  - 임원 : 3시간 이상(단, 정보보호최고책임자는 6시간 이상)
  - 일반직원 : 6시간 이상
  - 정보기술부문업무 담당 직원 : 9시간 이상
  - 정보보호업무 담당 직원 : 12시간 이상
- 집합교육이 아닌 온라인교육으로도 수행 가능

※ 법령해석('15.10.28.)

〈 질의 〉

▣ 「전자금융감독규정」 제19조의2에 따라 정보보호 교육계획을 수립·운영하는 경우에, 그룹 계열사 등에 파견 중인 임직원에 대해서는 서면 자료 배포를 통해 정보보호교육을 시행할 수 있는지 여부

〈 회신 〉

▣ 그룹 계열사 등에 파견 중인 임직원에 대해 서면 자료 배포 등을 통해 정보보호교육을 시행할 수 있습니다.

〈 이유 〉

▣ 「전자금융감독규정」은 동 규정 제19조의2에 따른 정보보호 교육계획의 수립 및 운영과 관련하여 정보보호 교육의 형태 및 내용을 특정하여 제한하고 있지 않으며, 해당 금융회사 등의 정보보호최고책임자의 판단에 따라 임직원의 정보보호역량 강화를 위하여 필요한 수준의 정보보호 교육을 적절한 방식을 통해 시행하면 됩니다.

▣ 따라서 대면을 통한 정보보호 교육이 어렵고, 정보보호 교육 수료의 필요성이 비교적 낮은 금융회사 외 그룹 계열사 파견 임직원에 대해서는 서면 자료 배포를 통한 정보보호 교육도 무방할 것입니다.

3. 정보처리시스템 구축 및 전자금융거래 관련 사업 추진

〈 감독규정 〉

제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진) 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업을 추진하는 경우에 다음 각 호의 사항을 준수하여야 한다.

1. 조직에 미치는 영향이 크거나 내부직무전결기준에 따라 부서장 전결 금액 이상의 사업 추진 시에는 사전에 충분한 타당성 검토를 실시할 것
2. 정보처리시스템의 신규 사업 및 통합·전환·재개발 등과 같은 주요 추진사업에 대하여 비용 대비 효과 분석을 실시할 것
3. 타당성 검토와 비용 대비 효과분석 결과는 전산운영위원회 등 독립적인 조직의 승인을 받을 것
4. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 분석·설계 단계부터 보안대책을 강구할 것

▣ 대규모 IT사업 추진 시 불필요한 투자결정 및 과잉 중복투자 방지를 위하여 금융회사 또는 전자금융업자의 장기 발전방향, 금융환경의 변화 등을 반영하여 타당성 검토 및 효과분석을 실시하고 그 결과를 전산운영위원회의 승인을 받아 IT사업 추진의 효율성 확보 및 투명성 제고

▣ 해설

- 시스템 통합 및 재개발, 경영전략상 중요하다고 인정되는 사업 등 조직에 미치는 영향이 크다고 판단되는 사업, 부서장 전결 금액 이상의 IT사업 추진 시 사전에 충분한 타당성 검토를 실시(제1호)
  - 사전검토 실시와 관련된 제반사항(사전검토 대상 및 범위, 담당부서 또는 담당자, 검토시기 및 세부적인 검토방법 등)에 대해 자체적인 기준을 설정·운영
  - IT사업추진을 위한 타당성 검토 시 IT부서 실무책임자가 참여하여 IT사업 추진방향(자체개발, 용역 등), 선정된 Solution, 업체선정 등에 대하여 IT부서 실무책임자의 의견을 반영할 수 있는 장치(내부규정 또는 업무처리절차에 반영 등)를 마련하고, 사전검토 결과에 대해 IT업무 협의회 등과 같은 내부 기구에 승인 또는 심의 절차 준수
- 일정금액 이상의 정보처리시스템 신규 사업, 통합, 전환, 재개발 등 주요 추진사업에 대한 정당성 및 효과성 확보를 위하여 비용 대비 효과분석을 실시(제2호)
  - 비용 대비 효과분석 시 IT부서는 물론 업무부서 등 타부서를 참여 시켜 IT 부서에서 독단적으로 결과를 산출하지 못하도록 투명성을 확보하고, IT사업에 따른 경제적 효과와 고객편의 증진 등 부수효과에 대하여 제3자의 입장에서 충분한

객관성이 확보될 수 있도록 구체적이며 객관적으로 분석 실시

- IT업무에 대한 타당성 검토와 비용 대비 효과분석 결과는 전산운영위원회의(IT운영위원회 등)와 같은 독립적인 조직의 승인을 받아 시행될 수 있도록 체계화 하여 투명성과 공정성을 제고(제3호)

- 정보처리시스템이 취약점을 내포하는 경우 해커의 침입경로로 이용될 수 있으므로 취약점이 노출하지 않도록 정보시스템 개발 초기단계(개발 및 분석)부터 적극적으로 보안성을 검토하여 보안대책 강구(제4호)

  – 개발 초기단계부터 보안이 고려되지 않고 개발된 시스템을 서비스 개시이후 보안성 강화를 위하여 변경시 개발 초기단계보다 훨씬 더 많은 시간 및 비용이 소요되는 등 어려움 발생하므로 개발 초기단계부터 적극적으로 보안성 검토 실시 필요

4. 정보처리시스템 구축 및 전자금융거래 관련 계약

〈 감독규정 〉

제21조(정보처리시스템 구축 및 전자금융거래 관련 계약) 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다.

1. 적합한 업체를 공정하게 선정하기 위하여 객관적인 업체 선정 기준 및 절차를 마련·운용할 것
2. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 제1호에 따른 기준 및 절차의 내용에는 정보보안 관련 사항을 포함할 것
3. 공정하고 합리적인 예정가격 산출 기준을 수립·적용할 것
4. 계약금액, 구축완료일자, 납품방법 및 대금지급방법 등 계약이행에 필요한 내용을 포함한 계약서 작성 기준을 수립·운용할 것
5. 구매 또는 개발한 제품의 소유권, 저작권 및 지적재산권 등의 귀속관계를 명확히 하여 사후 분쟁이 발생하지 않도록 할 것
6. 납품 또는 개발이 완료된 소프트웨어 등에 대하여 공급업체 파산 등 비상사태에 대비한 대책을 마련·운용할 것
7. 검수는 개발자, 계약자 등 이해당사자를 배제하여 공정하게 실시할 것
8. 계약조항을 이행하지 못하는 사유가 발생하였거나 계약조항을 변경할 경우에는 검사부서의 승인을 받을 것
9. 내부감사규정에 따라 감사가 정한 금액 이상의 계약에 대하여는 자체 감사를 실시하거나 검사부서의 승인을 받을 것

▣ 정보처리시스템 도입, 구축, 운영 및 전자금융거래 관련 계약 시 명확한 기준 없이 당사자 간에 계약이 체결되는 경우, 불필요한 비용 지출 또는 비용의 과잉지출 등으로 손실이 발생할 수 있으므로 업체선정을 위한 객관적이고 합리적인 기준을 마련하여 계약의 투명성 및 공정성 확보

▣ 해설

- 정보처리시스템 구축 및 전자금융거래 관련 계약시 공개경쟁입찰, 제한경쟁입찰, 수의계약 등 계약업체 선정을 위한 제반 절차 및 기준을 마련하고 합리적인 예정가격을 산출하기 위한 기준을 마련하여 업체선정 및 계약금액의 적정성과 공정성을 확보(제1호, 제3호)

- IT사업 관련 계약서상에 계약이행에 필요한 주요 사항이 누락되지 않도록 계약서 작성 기준을 마련하여 계약내용을 적정하게 작성하며, 구매 또는 개발한 제품(소프트웨어, 하드웨어 등)의 소유권, 저작권 및 지적재산권 등의 귀속관계를 명확히 하여 사후 분쟁이 발생하지 않도록 조치(제4호, 제5호)

- 납품 또는 개발이 완료된 소프트웨어 등에 대하여 공급업체 파산 등 비상사태에 대비하여 문서화 및 인수/인계를 철저히 하고, 대체 서버 확보 방안 강구 등 대책을 수립하고 프로그램에 대한 사용권한만 확보한 경우에는 프로그램 소스를 제3자에게 보관하는 등의 대책 강구(제6호)

- 정보처리시스템 도입 및 구축 후 검수는 이해당사자를 배제한 제3자에 의해 객관적이고 공정하게 실시 될 수 있도록 조치(제7호)

〈참고〉 이해당사자의 범위
– 계약자, 개발자 및 해당 부서를 포함하며, 검수조서 작성시에는 이해당사자를 완전히 배제

- 공급자 또는 외부주문업체가 계약조항을 이행하지 못하는 사유가 발생하였거나 계약조항을 변경할 경우에는 과실 유·무에 따른 책임소재에 관한 내용을 계약서에 반영하고 검사부서의 승인을 받도록 하여 업무를 공정하게 처리하고, 내부 감사규정에서 정한 일정 금액 이상의 계약 건은 계약의 적정성 및 공정성이 확보될 수 있도록 자체 감사 실시 및 검사부서 승인(제8호, 제9호)

5. 정보처리시스템 감리

〈 감독규정 〉
제22조(정보처리시스템 감리) 금융회사 또는 전자금융업자는 정보처리시스템의 안전성 및 효율성 확보를 위하여 다음 각 호의 사항을 포함한 정보처리시스템 감리 지침을 작성·운용하여야 한다.
1. 목적 및 대상, 시스템 감리인, 감리시기 및 계획 등 일반기준
2. 기획, 개발 및 운용의 감리 실시 기준
3. 지적사항 및 개선사항 등 감리 후 보고 기준
4. 전자금융업무와 관련된 외부주문등에 대한 감리 기준

▣ 정보처리시스템 구축 및 관련 프로젝트 수행에 있어 안전성 및 효율성 향상을 위하여 전산감리 대상, 감리인 자격, 감리절차 등에 대한 실현가능한 합리적인 자체 기준을 수립하여 이행

▣ 해설

● 일반적으로 감사는 위법, 부당, 부정에 대한 적발 및 지적과 시정에 목적을 두는 반면 전산감리는 성과의 극대화를 위하여 기술적인 측면에서 기획, 개발, 운영단계에 이르기까지 단계별 또는 종합적으로 합리성, 타당성, 신뢰성, 안전성 및 효율성 등을 조사하고 감독하는 평가행위로 감사부서의 전산감사 업무와 구분

감사와 감리 비교표

구 분	감 사	감 리
수 행 업 무	– 회계적 측면의 예산에 대한 바른 집행과 집행결과에 대한 합법성, 정당성, 적정성을 조사하고 검증	– 기술적 측면에서 프로젝트가 기본계획과 설계대로 되었으며 효율성, 신뢰성, 품질보증 등 기술적 요건이 보장되고 있는가를 감독, 지도하고 평가
	– 완료된 행위를 대상으로 잘못의 지적과 시정에 역점을 두며, 사후적인 성격이 강함	– 성과의 극대화를 위한 관리적 성격이 강함

● 전산감리[5]에 대한 세부기준은 금융회사 또는 전자금융업자가 자율적으로 수립하고 감리수행은 외부감리인 또는 내부인력도 가능하나, 전산감리인은 해당 사업에 대하여 독립성 및 기술적 적격성 확보

● 전산감리 지침에 포함되어야 할 내용(예시)

- 목적 및 대상 기준
- 감리시기 및 절차(사전/사후/단계별, 준비/계획/조사/감리/보고 등)
- 감리인 자격요건 및 역할(독립성 및 전문성, 책임 및 권한 등)
- 기획, 분석/설계, 개발 및 구현, 도입, 운용 등의 감리 실시
- 지적사항, 개선사항 등 감리 후 보고 및 시정조치 등
- 특히, 외부주문에 의해 공급되는 전자금융업무 관련 정보처리시스템은 전자금융업무의 안전성 및 효율성 확보를 위해 적극적인 감리실시 필요

6. 비상대책

〈 감독규정 〉

제23조(비상대책 등의 수립·운용) ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보방안을 수립하여야 한다.

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 비상연락체제 구축
7. 보고 및 대외통보의 범위와 절차 등

② 제1항에 따른 업무지속성 확보대책에는 비상사태에 대비한 다음 각 호의 안전대책이 반영되어야 한다.

1. 파업 시 핵심전산업무 종사자의 근무지 이탈에 따른 정보처리시스템의 마비를 방지하기 위하여 비상지원인력을 확보·운영할 것
2. 비상사태 발생 시에도 정보처리시스템의 마비를 방지하고 신속히 원상복구가 될 수 있도록 정보처리시스템 운영에 대한 비상지원인력 또는 외부 전문업체를 활용하는 방안을 수립·운영할 것
3. 비상지원인력이 사용법을 충분히 이해하고 업무운용이 가능한 수준으로 전산시스템 운영지침서, 사용자 매뉴얼 등을 쉽고 자세하게 작성하고 최신상태로 유지할 것

5) 감리대상으로부터 독립성을 확보한 제3자가 안전성, 신뢰성, 보안성, 효율성, 경제성, 준거성 등의 다양한 관점에서 정보처리시스템 구축에 대한 종합적인 분석 및 평가를 통하여 문제점을 발견하고 개선하도록 하는 것을 의미

4. 핵심전산업무 담당자 부재 시에도 비상지원 인력이 업무를 수행할 수 있도록 비상지원인력에 대한 연수를 실시할 것

③ 금융회사 또는 전자금융업자는 제1항의 규정에 따른 업무지속성 확보대책의 실효성·적정성 등을 매년 1회 이상 점검하여 최신상태로 유지하고 관리하여야 한다.

④「국가위기관리기본지침」에 따라 금융위원회가 지정한 금융회사는 금융위원회의 「금융전산분야위기대응실무매뉴얼」에 따라 위기대응행동매뉴얼(이하 "행동매뉴얼"이라 한다)을 수립하고 이를 금융위원회에 알려야 한다.

⑤ 금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립하여야 한다.

⑥ 제4항에 따른 행동매뉴얼 또는 제5항에 따른 비상대책에는 제1항의 규정에 따른 업무지속성 확보대책이 반영되어야 한다.

⑦ 금융회사 또는 전자금융업자는 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하여야 한다.

⑧ 다음 각 호의 금융회사는 시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모·인력을 구비한 재해복구센터를 주전산센터와 일정거리 이상 떨어진 안전한 장소에 구축·운용하여야 한다.

1. 「은행법」에 의해 인가를 받아 설립된 은행(다만, 「은행법」제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다)
2. 「한국산업은행법」에 의한 한국산업은행, 「중소기업은행법」에 의한 중소기업은행, 「농업협동조합법」에 의한 농협은행, 「수산업협동조합법」에 의한 수산업협동조합중앙회의 신용사업부문
3. 「자본시장과 금융투자업에 관한 법률」에 의한 투자매매업자·투자중개업자(다만, 「자본시장과 금융투자업에 관한 법률」 제12조에 의해 인가를 받은 외국 투자매매업자·투자중개업자의 지점 등은 제외한다)
4. 「자본시장과 금융투자업에 관한 법률」에 의한 증권금융회사 및 한국예탁결제원
5. 「자본시장과 금융투자업에 관한 법률」에 의한 거래소
6. 「여신전문금융업법」에 의한 신용카드업자(다만, 법인신용카드 회원에 한하여 신용카드업을 영위하는 자는 제외한다)
7. 「보험업법」에 의한 보험요율산출기관
8. 「상호저축은행법」에 의한 상호저축은행중앙회
9. 「신용협동조합법」에 의한 신용협동조합중앙회
10. 「보험업법」에 의한 보험회사

⑨ 제8항 각 호의 금융회사는 업무별로 업무지속성 확보의 중요도를 분석하여 핵심업무를 선정하여야 하며, 업무별 복구목표시간을 정하여야 한다. 이 경우 핵심업무의 복구목표시간은 3시간 이내로 하되, 「보험업법」에 의한 보험회사의 핵심업무의 경우에는 24시간 이내로 한다.

⑩ 제8항의 규정에 따른 재해복구센터를 운영하는 금융회사는 매년 1회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련을 실시하여야 한다.

▣ 정보처리시스템의 장애, 사고, 재해, 파업 등으로 인한 중단 사태에 대비하여 업무지속성 확보방안이 마련될 수 있도록 비상대책을 수립하고 이에 대한 정기적인 훈련을 실시

▣ 해설

● 장애, 재해, 파업, 전자적 침해 등 발생 가능한 모든 위험으로 부터 업무가 중단되지 않도록 다음의 사항을 포함한 업무지속성 확보방안을 수립(제1항)

- 장애, 재해, 파업, 전자적 침해 등 각 비상 상황별 적절한 대응절차
- 백업 또는 재해복구센터를 활용한 재해복구 계획
- 사고 발생시 신속하게 대응할 수 있도록 비상대응조직 구성 및 운용
- 비상상황 발생에도 지속적으로 업무처리가 가능하도록 입력대행, 수작업 등의 조건 및 절차 마련
- 업무지속성 확보방안의 실효성이 제고될 수 있도록 정기적으로 상황별 모의훈련 실시
- 발생 상황의 금융업계 파급 차단 및 신속한 해결을 위한 유관기관 및 관련업체와의 비상체계 구축
- 상황발생에 대한 보고 및 대외통보의 범위와 절차 등

● 비상사태가 발생할 경우에도 정보처리시스템의 정상적인 운영이 가능하도록 업무지속성 확보대책에는 비상지원인력 확보 등 다음의 안전대책을 포함(제2항)

- 파업으로 핵심업무 종사자가 근무지를 이탈하는 경우에도 정상적인 정보처리시스템 운영이 가능하도록 비상지원인력 확보
- 비상사태가 발생하는 경우 정보처리시스템의 마비방지 및 신속한 원상복구를 위하여 정보처리시스템 운영에 대한 비상지원인력 또는 외부 전문업체 활용방안 수립·운영
- 전산시스템 운영에 필요한 운영지침서, 사용자매뉴얼 등을 최신상태로 유지하고, 비상지원인력에 대해 담당업무 연수를 정기적으로 실시하여 비상사태 발생시 업무수행이 원활하게 이루어지도록 조치

● 업무지속성 확보대책의 실효성 및 적정성 등을 매년 1회 이상 점검하고 최신상태를 유지하여 실제 비상사태 발생시 전자금융업무가 중단없이 서비스되도록 조치(제3항)

● 비상대책(위기대응매뉴얼 포함)의 내용은 장애 및 재해 유형에 따라 복구절차, 복구 예상시간, 복구 우선순위, 담당자, 연락체계 등을 구분하여 수립(제4항, 제5항)

〈예시〉 전산센터 마비에 대비한 비상대책 포함 요소
- 재해 선포 절차(예: 결정자, 선포자 등)
- 대체시스템 가동에 필요한 데이터 및 프로그램의 준비(예: 데이터 백업, 당일거래기록 백업, 관련 프로그램 백업 등)
- 대체시스템 가동 절차(예: 업무별 담당자, 담당자별 처리절차, 시스템 및 통신망 가동절차, 대체시스템 확인 절차, 영업점 처리절차 등)
- 훈련 및 테스트 계획(예: 훈련 대상, 주기 등)
- 정상 시스템 전환 절차(예: 데이터 확인, 정상화 선언)

● 비상대책(위기대응매뉴얼 포함)은 모든 서비스를 동시에 대체할 수 있도록 계획할 수 있으나, 비용, 기기 용량, 신속성 등을 고려하여 긴급한 업무 중심으로 대상을 선정할 것인지 모든 서비스를 대상으로 선정 할 것인지에 대하여 자율적으로 결정하며, 위기대응매뉴얼을 수립한 금융회사는 금융위원회에 알림(제4항)

● 비상대책(위기대응매뉴얼 포함)은 수립 및 문서화하는 것으로 완료 된 것이 아니고 이에 대한 정기적인 훈련이 더욱 중요하며, 시스템 환경이 변화된 경우 이를 즉시 비상대책에 반영하여야 함(제3항, 제5항)

● 위기대응행동매뉴얼 또는 비상대책에는 업무지속성 확보대책을 반영(제6항)

● 서버, 데이터 저장장치, 통신 중계 장치 등의 주요 전산장비 및 통신회선에 대하여는 장애발생에 대비하여 이중화 또는 예비 장비를 확보하여야 하며, 예비 장비를 보유하고 있지 않을 경우에는 납품업체 또는 제조업체와 계약을 통하여 예비 장비를 우선 수급받을 수 있도록 조치(제7항)

● 주 전산센터 가동중단에 대비하여 구축한 재해복구센터는 재해발생시 주 전산센터와 동일한 재해에 영향을 받지 않도록 주 전산센터로부터 일정거리 이상 떨어진 안전한 장소에 구축·운영(제8항)

● 제8항의 규정에 따른 금융회사 등은 자체적으로 업무의 중요도를 분석하여 핵심업무를 선정하고, 핵심업무가 주센터를 통한 서비스가 곤란한 경우에도 재해복구센터를 이용하여 복구목표시간내에 서비스가 가능하도록 업무지속성이 확보되어야함. 이 경우 복구목표시간은 3시간 이내이며, 보험회사는 24시간 이내임(제9항)

〈예시〉 핵심업무('17.4월 금융회사 재해복구센터 구축·운영 가이드-금융보안원 참고)

(은행) 개인. 여신·수신, 기업 여신·수신, 어음 / 수표, 연금, 방카슈랑스, 환전, 외화예금, 수출입, FX / 파생상품, 송금, SWIFT, 모바일·인터넷 뱅킹, CD / ATM, 텔레뱅킹, 금융결제원 공동망(CD, 전자금융, 타행환, ARS) 등

(증권) 주식, 채권, 선물 / 옵션, 기타파생상품, 펀드, 입출금관리, 입출고관리, 소액지급, 모바일·인터넷뱅킹, 모바일·인터넷 트레이딩. CD / ATM, 텔레뱅킹 / ARS, 계좌개설, 계좌원장, 잔고관리 등

(보험) 사고접수, 사고조사, 보험금지급, 대출신청, 대출심사, 대출금지급, 신규계약, 계약심사, 계약변경 등

(카드) 국내·외 온라인 승인, 국내·외 오프라인 승인, 회원한도 관리, 회원정보 관리, 신용정보 관리, 카드정산·청구, 실시간 입금·자동이체, 가맹점 대금지급·정보관리, 매입 심사·연계, 현금서비스(이체 / 지급), 신용판매(일시불 / 할부), 온라인결제[승인], ISP인증, 모바일카드, 카드 발급·조회 등

- 제8항의 규정에 의거 재해복구센터를 운영하는 금융회사는 매년 1회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련을 실시(제10항)

7. 비상대응훈련

〈 감독규정 〉

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, 제23조제10항에 따른 재해복구전환훈련을 포함하여 실시할 수 있다.

② 금융위원회는 금융분야의 비상대응능력을 강화하기 위하여 금융회사 또는 전자금융업자를 선별하여 금융분야 합동비상대응훈련을 실시할 수 있다.

③ 금융위원회는 제2항의 규정에 따른 합동비상대응훈련을 실시할 때, 다음 각 호의 기관에게 지원을 요청할 수 있다.

1. 「정부조직법」 제15조에 따른 "국가정보원(국가사이버안전센터)"
2. 「경찰법」 제2조에 따른 "경찰청(사이버테러대응센터)"
3. 침해사고대응기관
4. 그밖에 비상대응훈련의 실효성 확보를 위하여 금융위원회가 필요하다고 인정하는 기관

▣ 위기대응행동매뉴얼 및 비상대책을 수립한 금융회사 또는 전자금융업자는 위기대응행동매뉴얼 또는 비상대책에 따라 비상대응훈련을 연 1회 실시하여 재해, 장애 등 비상사태 발생시에도 업무지속성 확보

▣ 해설

● 금융회사 또는 전자금융업자는 장애, 재해, 파업, 전자적 침해 등 발생 가능한 모든 위험으로 부터 업무 중단방지 및 신속한 복구를 위하여 위기대응행동매뉴얼 및 비상대책에 따라 연 1회 비상대응훈련을 실시하여야 하며, 이때 재해복구훈련을 포함하여 실시할 수 있으며, 훈련실시 결과를 금융위원회에 보고(제1항)

8. 정보처리시스템의 성능관리

〈 감독규정 〉
제25조(정보처리시스템의 성능관리) 금융회사 또는 전자금융업자는 정보처리시스템의 장애예방 및 성능의 최적화를 위하여 정보처리시스템의 사용 현황 및 추이 분석 등을 정기적으로 실시하여야 한다.

▣ 최적의 정보처리시스템 용량 확보를 통한 장애예방 및 성능 최적화를 실현함으로써 시스템의 가용성 확보 및 대고객 서비스를 제고하고, 효과적인 자원 활용을 통한 비용 절감 등을 동시에 추구하기 위하여 정기적으로 정보처리시스템 자원의 사용현황 및 추이 분석 실시

▣ 해설

● 정보처리시스템의 용량 부족으로 인한 서비스 지연, 장애 등을 방지하기 위하여 다음과 같은 조치를 시행하고 결과를 기록·보관

- 전산기기에 대한 용량분석(Capacity Planning)
- 피크타임(peak time) 기준의 시스템 상태, 이용도 모니터링 및 응답 시간 지연 등의 이상 징후 발생시 원인 분석
- 시스템 용량 확장 시점 예측을 위한 이용도 분석(CPU, Storage Memory, I/O Channel 등)
- 신규업무 개발시 전산시스템의 수용능력을 평가하여 기 운영 업무에 영향을 주지 않도록 조치
- 미사용 시스템의 자원분석을 통하여 적정배분 사용 등

9. 직무분리

〈 감독규정 〉

제26조(직무의 분리) 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다.

1. 프로그래머와 오퍼레이터
2. 응용프로그래머와 시스템프로그래머
3. 시스템보안관리자와 시스템프로그래머
4. 전산자료관리자(librarian)와 그 밖의 업무 담당자
5. 업무운영자와 내부감사자
6. 내부인력과 전자금융보조업자 및 유지보수업자 등을 포함한 외부인력
7. 정보기술부문인력과 정보보호인력
8. 그 밖에 내부통제와 관련하여 직무의 분리가 요구되는 경우

▣ 직무분리는 동일인이 여러 업무를 수행함으로 인하여 발생할 수 있는 시스템 조작, 원장 변경 등의 사고를 방지하기 위한 것으로, 직무분리는 담당업무별로 업무를 분리하는 것이 바람직하며 최대한 상호견제가 이루어질 수 있도록 통제체계 마련·운영

▣ 해설

- 직무분리의 일반적인 방법
  - 입력·승인·확인 등 모든 거래과정이 동일 직원에 의해 처리되지 않도록 분리
  - 프로그램 개발자와 시스템 운영자 분리
  - 데이터베이스 관리자와 시스템 및 응용 프로그래머 분리
  - 시스템 프로그래머의 작업에 대한 자체 감사자의 통제
  - 전산기기 운영자(Operator)에 대한 자체 감사자 또는 시스템 프로그래머의 통제
  - Batch 프로그램에 의한 온라인 데이터베이스 접근 통제
  - 업무개발자와 관리자의 분리
  - 내부감사자 및 보안 관리자의 타 업무 겸임 금지

※ (참고)직무별 설명

직 무	설 명
프로그래머	컴퓨터 프로그래밍을 하고 소프트웨어를 개발하는 자 프로그램의 운영 또는 개발을 담당하지 않는 프로그래머는 제한된 프로그램에 대해서만 접근을 허용
오퍼레이터	정보처리시스템을 조작하여 운용하는 자 프로그램 소스를 직접 확인하거나 수정하여서는 안됨 실행용(Production) 전산원장을 이용하는 배치작업을 담당자의 의뢰 없이는 오퍼레이터의 임의 수행 금지 및 프로그램개발자의 직접 실행 금지
응용프로그래머	(시스템 유지보수 기능을 하는 프로그램을 제외) 사용자를 위한 프로그램을 개발하는 자 응용프로그래머가 운영체제 실행 명령어를 사용하는 것을 금지하여야 하며, 특히 어셈블러와 같은 기계어에 가까운 저급언어를 사용할 경우에는 더욱 통제를 철저히 실시
시스템프로그래머	운영체제, 데이터베이스시스템 및 어플리케이션 개발을 지원하는 기술적 지원그룹으로 소프트웨어 공급 업자, 응용프로그래머, 컴퓨터 운영요원 사이의 매개 역할을 담당
시스템보안관리자	비인가된 접근으로부터 통신 네트워크 및 시스템, 응용서비스 등을 보호하는 역할을 담당
전산자료관리자 (Librarian)	전산자료 및 관련 매체를 관리하는 자

10. 전산원장 통제

〈 감독규정 〉

제27조(전산원장 통제) ① 금융기관 또는 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립·운용하여야 한다.

② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.

③ 금융회사 또는 전자금융업자는 대차대조표 등 중요 자료의 계상액과 각종 보조부·거래기록·전산원장 파일의 계상액에 대한 상호일치 여부를 전산시스템을 통하여 주기적으로 확인하여야 한다.

④ 금융회사 또는 전자금융업자는 제3항에 따른 확인 결과 불일치가 발견된 때에는 그 원인 및 조치 내용을 전산자료의 형태로 5년간 보존하여야 한다.

⑤ 금융회사 또는 전자금융업자는 이용자 중요원장에 직접 접근하여 중요원장을 조회·수정·삭제·삽입하는 경우에는 작업자 및 작업내용 등을 기록하여 5년간 보존하여야 한다.

▣ 전산원장은 금융회사의 가장 중요한 정보로 고객 본인의 정상적인 거래 시에만 변경되어야 하나 프로그램 오류, 거래오류, 시스템 장애 등으로 인하여 변경이 불가피한 경우에는 엄격한 통제절차에 의하여 변경이 이루어지도록 하고 사후 철저한 검증 실시

▣ 해설

● 전산시스템 장애 또는 프로그램 오류 등에 의한 전산원장 변경절차 수립 시 다음 사항을 고려

- 변경대상 및 방법 명시 : 사전에 변경대상을 지정하여 변경 대상정보에 대하여만 변경토록 하고, 만약 절차에 지정된 변경 대상 이외의 정보에 대하여 변경이 필요한 경우에는 변경절차에 변경 대상 및 방법을 추가(제1항)
- 변경전후 내용의 자동기록 및 보존 : 온라인 이외의 방법으로 변경이 일어날 경우 거래 Log에 기록이 되지 않기 때문에 별도의 프로그램이 작성되어 있지 않을 경우 변경 내용에 대한 확인이 불가능하므로 반드시 변경 전·후 내용이 기록되도록 프로그램이 준비되어 있어야 하고, 동 기록은 5년간 보관·관리(제5항)

● 원장수정은 불법수정과 고객정보 유출 등의 사고예방을 위하여 전담자를 지정하고 전용단말기를 통해 수정할 수 있도록 하며 자체 감사부서의 상시감시대상에 포함하여 모니터링 실시(제2항)

● 전산원장 수정의 경우에는 제3자가 수정의 정당성을 사전 승인토록 하고, 원장 수정 전후내역을 전산기록(logging)하고 5년간 보존(제2항, 제5항)

- 전산원장 변경시 제3자의 범위는 객관적으로 확인이 가능한자로 감사부서, IT자체 감사 부서, 준법감시팀 등이 해당됨
- 정기적으로 실행되는 일괄작업(BATCH)의 경우 최초 1회시에만 적용하여도 가능

● 주요 자료의 계상액과 각종 보조부, 거래기록, 전산원장 파일의 계상액이 상호불일치할 경우 불일치 내용, 원인, 조치 사항을 전산시스템으로 5년간 보관하여 추후 사고 발생시 근거자료로 활용(제4항)

● 사고발생시 사고원인 추적 및 근거자료로 활용이 가능하도록 중요전산원장 접근(조회, 수정, 삭제, 삽입 등) 로그를 작업자, 작업일시, 작업내용 등의 전산자료 형태로 5년간 기록·보관(제5항)

11. 거래통제

〈 감독규정 〉
제28조(거래통제 등) ① 금융회사 또는 전자금융업자는 사고위험도가 높은 거래에 대하여는 책임자 승인거래로 처리토록 하는 등 전산시스템에 의한 이중확인이 가능하도록 하여야 한다.
② 금융회사 또는 전자금융업자는 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 해야 한다.

▣ 일정금액 이상의 고액인출, 각종 사고신고, 계좌일괄조회, 정정거래 등 사고위험도가 높거나 이상거래의 개연성이 있는 업무에 대해서는 업무 담당자가 단독으로 처리할 경우 사고위험이 높으므로 책임자가 정보처리시스템에 의하여 실무자가 확인된 결과를 재확인

▣ 해설

- 책임자 승인거래 업무 범위에 대하여 사전에 지정하고, 신규업무 개발 시에는 책임자 승인거래 대상 여부를 확인하여 해당되는 업무는 반드시 추가하고 현재 운영되고 있는 책임자 승인거래 대상 및 범위에 대하여 확인(제1항)

- 책임자승인 방식은 책임자의 개입 없이 담당자가 단독으로 업무를 처리 할 수 없도록 비밀번호 방식 보다는 물리적 수단(카드키, 지문, OTP 등)에 의한 인증 방식의 적용을 권고하고 책임자 부재 등 부득이한 경우에는 책임자가 사전에 지정한 업무대행자가 확인하도록 전산시스템을 개발

- 전산원장, 이용자정보, 전자금융거래 정보 등이 저장되어 있는 정보처리시스템에 대한 중요작업 수행시 정보유출 등의 사고 예방을 위하여 책임자가 작업내용 이중 확인(제2항)

12. 프로그램 통제

〈 감독규정 〉
제29조(프로그램 통제) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다.
1. 적용대상 프로그램 종류 및 등록·변경·폐기 방법을 마련할 것
2. 프로그램 변경 전후 내용을 기록·관리할 것
3. 프로그램 등록·변경·폐기내용의 정당성에 대해 제3자의 검증을 받을 것
4. 변경 필요시 해당 프로그램을 개발 또는 테스트 시스템으로 복사 후 수정할 것

5. 프로그램에 대한 접근은 업무담당자에 한정할 것
6. 운영시스템 적용은 처리하는 정보의 기밀성·무결성·가용성을 고려하여 충분한 테스트 및 관련 책임자 승인 후 실시할 것
7. 프로그램 반출, 실행프로그램의 생성 및 운영시스템 등록은 전산자료 관리자 등 해당프로그램 담당자 이외의 자가 수행할 것
8. 운영체제, 데이터베이스관리프로그램 등의 시스템 프로그램도 응용프로그램과 동일한 수준으로 관리할 것
9. 프로그램 설명서, 입·출력 레코드 설명서, 프로그램 목록 및 사용자·운영자지침서 등 프로그램 유지보수에 필요한 문서를 작성·관리할 것
10. 전자금융거래에 사용되는 전산프로그램은 실제 업무를 처리하는 정보처리시스템에 설치하기 전에 자체 보안성 검증을 실시할 것

▣ 프로그램은 전산업무처리의 근본으로 이에 대한 관리 및 변경은 신중하게 통제되어야 하며 특히, 보유 프로그램 목록 관리, 프로그램 변경 및 접근 통제 실시

▣ 해설

- 정보처리시스템에서 사용되고 있는 모든 프로그램에 대하여 목록을 작성(전자파일 포함)하여 관리하고 (제1호)
- 프로그램 변경시 프로그램 소스 관리를 위하여 현재 사용 중인 최신버전의 프로그램(소스)를 변경하여야 하며, 구버전의 프로그램을 변경하지 않도록 프로그램 변경관리 절차를 수립하여 운영하여야 하고 가급적 자동화된 프로그램 소스 관리툴(형상관리 도구)을 활용(제2호)
- 프로그램의 변경은 변경사유가 명확하여야 하고, 변경내용에 대한 확인 및 실시스템(Production System) 적용은 해당 프로그램 개발자가 아닌 제3자에 의하여 정확히 이루어 질 수 있도록 절차를 마련(제3호)
- 보관중인 프로그램 소스에 대한 접근은 업무담당자로 한정하며, 프로그램 소스 접근 통제 및 관리 절차를 수립·운영(제5호)
- 사용 중인 프로그램 변경을 위한 반출, 실행프로그램 생성 및 운영시스템 등록 업무를 개발담당자가 직접 수행하는 것을 금지(제7호)
- 중요도가 높은 시스템 운영체제, 데이터베이스관리프로그램 등의 시스템 프로그램의 변경 또는 패치프로그램 적용 시 충분한 테스트를 실시하고 관리 권한을 최소한으로 한정하는 등 관리통제를 강화하여 업무서비스 장애 발생 가능성 최소화(제8호)

- 프로그램 담당자의 사직, 유고, 업무이동 등으로 담당자가 변경되는 경우 프로그램 관리가 원활하게 이루어 질 수 있도록 관련 문서를 상세히 작성하고 최신 상태 유지(제9호)

- 전자금융거래용 전산프로그램은 보안 취약성을 내포하는 경우 해커에 의한 침입경로 및 악성코드 유포 수단으로 사용될 수 있으므로 실 운영시스템에 반영하기 전에 취약점 점검 등 프로그램에 대한 자체 보안성 검증 실시(제10호)

13. 일괄작업에 대한 통제

〈 감독규정 〉

제30조(일괄작업에 대한 통제) 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위하여 다음 각 호의 사항을 준수하여야 한다.

1. 일괄작업은 작업요청서에 의한 책임자의 승인을 받은 후 수행할 것
2. 일괄작업은 최대한 자동화하여 오류를 최소화할 것
3. 일괄작업 수행 과정에서 오류가 발생하였을 경우 반드시 책임자의 확인을 받을 것
4. 모든 일괄작업의 작업내용을 기록·관리할 것
5. 책임자는 일괄작업 수행자의 주요업무 관련 행위를 모니터링할 것

▣ 일괄작업의 경우 하나의 프로그램에 의하여 대량 자료가 변경되기 때문에 데이터의 무결성·신뢰성·정확성을 유지하기 위하여 작업처리에 대한 철저한 통제 실시(일괄작업으로 전산원장을 변경하는 경우에도 규정 제27조 준수 필요)

▣ 해설

- 일괄작업은 표준화된 작업의뢰서를 작성하고 업무담당 책임자의 승인 하에 운영요원에게 제출되어야 하며, 운영요원에 의해 일괄작업 내용이 변경되거나 부당작업이 수행되지 아니하도록 작업통제 절차를 수립(제1호)

- 일괄작업에 대한 책임자의 승인은 정형화된 경우에는 일괄하여 승인할 수 있으나, 비정형화된 경우에는 건별로 승인(제1호)

- 일괄작업의 수작업 처리 오류로 인해 발생하는 시스템 지연가동 또는 장애 최소화를 위하여 일괄작업을 최대한 자동화(제2호)

● 일괄작업 수행과정에서 오류가 발생하는 경우 작업을 중단하고 해당업무 책임자의 확인을 받도록 하고 오류일시, 오류내용, 확인자 등을 기록·관리(제3호, 제4호)

● 일괄작업은 시스템 운영에 중대한 영향을 미칠 수 있으므로 사고예방을 위하여 책임자는 일괄작업 수행자의 비정형 일괄작업, 오류처리, 비정상 작업종료 등 주요업무 관련 행위를 모니터링(제5호)

14. 암호프로그램 및 키 관리 통제

〈 감독규정 〉

제31조(암호프로그램 및 키 관리 통제) ① 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.

② 금융회사 또는 전자금융업자는 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.

▣ 암호프로그램과 암호키가 유출될 경우 금융거래에서 가장 중요한 고객정보인 주민번호, 계좌 비밀번호, 일회용비밀번호 등의 유출사고로 이어질 수 있으므로 일반프로그램보다 더욱 철저히 관리

▣ 해설

● 암호프로그램 및 암호키는 전담 담당자를 지정하여 관리토록 하고, 전산부서 직원인 경우에도 담당자 이외에는 접근통제 철저(제1항)

– 특히, 프로그램 내에 하드코딩된 키로 암호화하지 않도록 주의

● 암호프로그램의 소스는 M/T, IC카드 등의 보조저장매체를 이용하여 별도로 보관하여야 하며 서버, 개발자 PC 등에 소스 저장 금지, 또한 암호화프로그램이 복사된 보조저장매체는 비밀문서에 준하여 안전한 장소에 보관(제1항)

● 암호프로그램 관련 설계서도 암호프로그램과 동일하게 비밀문서에 준하여 관리(제1항)

● 암호프로그램을 외부주문에 의하여 개발한 경우 사용되는 키는 외부주문업체로부터 인수 즉시 변경하여야 하며 암호키의 생성, 운용, 주입 및 폐기는 해당 금융회사 또는 전자금융업자의 지정된 담당자가 직접 수행(제2항)

- 실 시스템의 암호 및 인증시스템에서 이용하고 있는 키와 테스트 시스템에서 테스트용으로 사용되고 있는 키는 동일한 키의 사용 금지(제2항)

15. 내부사용자 비밀번호 관리

〈 감독규정 〉

제32조(내부사용자 비밀번호 관리) 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것
2. 비밀번호는 다음 각 목의 사항을 준수할 것
   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
3. 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

▣ 내부사용자의 비밀번호는 정보처리시스템에 직접 접근하여 고객 정보, 금융거래 정보 등에 접근할 수 있는 권한을 부여하는 핵심 정보이므로 비밀번호 유출방지 대책 마련

▣ 해설

- 금융회사 내부사용자가 본인의 담당업무에 대해서만 정보시스템에 저장되어 있는 정보를 열람, 출력할 수 있도록 금융회사 내부사용자에 대하여 담당업무별로 비밀번호 설정·운영(제1호)

- 비밀번호 설정 시 아래와 같은 경우에는 비밀번호로 등록이 되지 않도록 관련 프로그램에 반영(제2호)

  – 비밀번호의 자릿수가 8자리 미만인 경우

  – 비밀번호가 사용자계정(ID)을 포함하는 경우

  – 영문자, 숫자, 특수 문자를 혼합하지 않은 경우

- 주민등록번호, 전화번호 등 쉽게 유추 가능한 개인 신상정보, 연속 숫자 및 동일 숫자나 문자를 연속해서 사용하지 않도록 조치 필요(제2호)

- 시스템 관리자 비밀번호는 해킹 등에 의한 비밀번호 유출에 대비하여 비밀번호를 시스템마다 다르게 부여하여 보안 강화(제2호)
- 비밀번호는 암호화하되 업무포털 등의 사용자 계정 비밀번호뿐만 아니라 그 외 서버나 DB의 접속을 위한 사용자 계정 비밀번호도 암호화 필요(제2호)
- 내부사용자의 비밀번호 오류 허용 횟수는 5회 이내의 범위에서 금융회사에서 자율적으로 정하여 운영하고, 오류 횟수는 일 단위가 아니고 누적횟수를 적용(제3호)
- 비밀번호 입력 오류횟수를 초과하지 않은 상태에서 정상적인 비밀번호를 입력하는 경우에는 누적 오류발생 횟수를 '0'으로 변경 가능(제3호)

16. 이용자 비밀번호 관리

〈 감독규정 〉

제33조(이용자 비밀번호 관리) ① 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·관리하여야 한다.

② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. 주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가
2. 통신용 비밀번호와 계좌원장 비밀번호를 구분해서 사용
3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시 해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)
4. 금융회사가 이용자로부터 받은 비밀번호는 거래전표, 계좌개설신청서 등에 기재하지 말고 핀패드(PIN pad) 등 보안장치를 이용하여 입력 받을 것
5. 신규 거래, 비밀번호 변경, 이체 신청과 같이 비밀번호를 등록·사용하는 경우 사전에 신청서 등에 기입하지 않고, 핀패드 등 보안장치를 이용하거나 이용자가 사후에 전자적 장치를 이용하여 직접 입력하는 방식으로 운영할 것

▣ 이용자의 비밀번호는 예금거래, 주식거래, 보험청약 등에서 핵심이 되는 정보로서 금융회사 직원이라 하여도 임의로 조회 금지

● 이용자는 여러 종류의 비밀번호를 암기하기가 어려워 본인의 신상과 관련이 있는 숫자를 사용하는 것이 일반적이므로 전산 시스템에서 유추 가능한 비밀번호의 등록을 제한하고, 일정횟수 이상의 입력 오류 발생 시에는 사용을 정지시킴으로써 전자금융사고 예방

▣ 해설

● 접속용 비밀번호, 원장비밀번호, 현금카드 비밀번호 등과 같은 이용자 비밀번호는 암호화 하도록 하고, 정보처리시스템에 저장하여 금융회사 업무담당자도 조회가 불가능하도록 운영(제1항)

– 비밀번호 조회가 불가피할 경우 조회 사유·내용 등을 기록·관리

● 비밀번호 설정 시 아래와 같은 경우에는 비밀번호 등록이 불가하도록 시스템 구현(제2항)

– 이용자의 주민등록번호, 전화번호 등과 같이 쉽게 유출가능한 개인 신상정보를 이용한 비밀번호

– 연속숫자, 연속문자, 동일숫자, 이름 등과 같이 제3자가 비밀번호를 쉽게 유추할 수 있는 경우

– 이용자가 전자금융거래 이용을 위하여 금융회사 또는 전자금융업자의 정보처리시스템에 접속시 사용하는 로그인 비밀번호, ARS 비밀번호 등을 계좌원장 비밀번호와 동일하게 설정하는 경우

– 전자금융거래를 이용하기 위하여 채널 접속에 사용하는 비밀번호는 영·숫자·특수문자를 혼합하여 보안성을 강화, 다만 유선 전화와 같이 영문 입력이 곤란한 경우에는 숫자로만 설정 가능

● 이용자가 전자금융수단을 이용하여 비밀번호를 입력시 금융회사가 사전에 정한 일정 횟수(예, 3회 등)를 초과 입력한 비밀번호에 대하여 입력 오류가 발생한 경우 즉시 해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여(제2항제3호)

● 계좌원장 비밀번호, 이체 비밀번호 등 비밀번호가 인터넷뱅킹, 자동화기기(CD/ATM), 텔레뱅킹 등과 같이 다양한 형태의 전자금융거래에서 공통으로 이용되는 경우 입력오류 횟수를 모든 전자금융거래에 대하여 통산하여 적용(제2항제3호)

※ (참고)비밀번호 오류시 거래 제한

유형	설명
계좌원장 비밀번호 오류	이체, 출금, 조회(계좌원장 비밀번호를 입력하는 경우에 한정) 등 계좌원장 비밀번호를 이용하는 전자금융거래 제한
일회용비밀번호 오류	인터넷뱅킹, 텔레뱅킹 등에서 일회용비밀번호를 사용하는 전자금융거래 제한
특정 전자금융거래에서만 사용하는 비밀번호 오류	해당 전자금융거래만 제한 예) ARS 전용 이체비밀번호 오류횟수 초과시 ARS 이체만 불가, 조회 가능

※ 법령해석('15.3.11.)

〈 질의 〉

▣ ACS(Auto Call System)를 통한 비밀번호 입력방식이 전자금융감독규정 제33조(이용자 비밀번호 관리) 제2항 제4호 내지 5호에서 규정하고 있는 '핀패드 등 보안장치 또는 전자적 장치'에 해당하는지 여부

〈 회신 〉

▣ 귀 사의 ACS는 전자금융감독규정 제33조제2항제4호 또는 제5호에서 규정하고 있는 핀패드(Pin-Pad)와 동등 또는 유사한 방식으로 판단됩니다.

〈 이유 〉

▣ 핀패드는 통상 고객의 통장개설 신청서, 전표 등에 기재된 비밀번호가 금융회사 직원의 업무처리 또는 전표 폐기과정에서 유출되는 것을 방지하기 위하여,

○ 고객이 거래용지 등에 비밀번호를 쓰는 대신 손으로 직접 입력할 수 있게 하는 장치(금융용어사전, 금융감독원)를 의미합니다.

▣ 귀 사의 ACS는 고객이 비밀번호를 신청서, 전표 등에 기재하지 않고 고객의 단말기를 이용하여 직접 입력한다는 점에서 본질적으로 핀패드와 동등 또는 유사한 방식으로 판단됩니다.

○ 다만, 귀 사의 ACS는 통상 금융회사의 비밀번호 입력기를 사용하는 통상적 핀패드와 달리 고객의 단말기를 사용한다는 점에서 더욱 엄격한 관리가 필요할 것으로 판단됩니다.

※ 법령해석('15.10.23.)

〈 질의 〉

▣ 이용자의 계좌원장 비밀번호 입력 오류로 인해 「전자금융감독규정」 제33조제2항제3호에 따른 본인확인절차가 필요한 경우, 동 조항상 본인확인 절차가 '지점 방문을 통한 대면 확인'만을 의미하는 것인지 여부

〈 회신 〉

▣ 「전자금융감독규정」 제33조제2항제3호에 따른 본인확인절차는 원칙적으로 지점 방문을 통한 대면 확인만을 의미하는 것은 아니며, 비대면 인증기술을 통한 비대면 본인확인도 가능합니다.

〈 이유 〉

▣ 「전자금융감독규정」 제33조제2항제3호는 본인확인절차를 대면 또는 '실명증표의 확인' 등으로 특정 방식으로 한정하고 있지 않은바, 금융회사의 판단에 따라 적절한 본인확인 절차를 적용토록 함이 바람직합니다.

제6절 전자금융업무

1. 전자금융거래 시 준수사항

〈 감독규정 〉
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
② 삭제

▣ 전자금융거래는 인터넷 등 공개된 통신망을 이용한 비대면 거래로 데이터 전송 중 고객정보 유출, 타인으로 위장한 거래, 거래정보의 송·수신 과정에서 위·변조 등의 위험이 상존하기 때문에 안전한 전자금융거래 보호대책 마련 필요

▣ 해설

- 전자금융거래에 사용되는 전자적 장치 중 유선전화기와 같이 암호화를 적용 시킬 수 없는 경우를 제외한 모든 전자금융거래는 송·수신 정보를 암호화 하여 통신회선에서의 불법적인 정보유출 방지 및 유출 시에도 알 수 없도록 조치(제1호)

  다만, 금융회사 또는 전자금융업자와 이용자 간(법인 포함) 전용회선을 설치하여 정보를 송·수신하는 경우로써 자체 보안성 심의를 받은 경우에는 암호화 예외 가능

- 전자금융거래 이용을 원하지 않는 이용자의 예금과 금융거래 정보를 보호하기 위하여 금융회사는 모든 예금계좌(요구불, 저축성, 신탁 등)를 보안계좌[6]로 설정 또는 개설이 가능하도록 시스템 구축(제2호)

6) 온라인거래 수단인 "인터넷뱅킹, 텔레뱅킹, 모바일뱅킹, 온라인 계좌이체(전자상거래), 콜센터 또는 전화를 통한 거래"로 이체·조회 등 모든 거래가 불가능한 계좌를 말하며 상기 업무를 제외한 나머지 업무는 일반계좌와 동일(영업점에서 직접 대면을 통한 거래(조회, 이체, 입금 등) 및 CD/ATM거래, 입금거래 등은 제한이 없음) 특히, 고객이 영업점에 전화를 걸어 계좌의 조회를 요청하는 경우에도 보안계좌인 경우에는 거래내역을 유선상으로 알려줄 수 없음

- 전자금융거래 이용자가 주요 금융거래 내역 및 제3자의 부정사용 여부에 대한 모니터링을 할 수 있도록 거래내역을 실시간으로 확인할 수 있는 문자메세지(SMS 서비스) 및 이메일(e-Mail) 알림 서비스를 요구하는 경우 서비스 제공이 가능하도록 시스템 구축(제2호)

- 전자자금이체 거래 시 접근매체(전자식 카드 및 전자적 정보, 전자서명법 제2조 제4호의 전자서명생성정보 및 같은 조 제7호의 인증서, 이용자의 생체정보 등)를 발급하는 경우 금융회사 또는 전자금융업자는 전자금융거래 이용자 본인의 실명을 확인한 후 교부(제3호)

- 금융회사 또는 전자금융업자가 보안카드 및 일회용비밀번호 등 거래인증수단을 채택시 인증수단의 안전성, 보안성, 이용편의성 등을 충분히 고려하여 결정(제4호)

- 전자금융거래를 위해 이용자에게 제공하거나 거래처리에 이용되는 전자금융거래 프로그램(거래전문포함)을 해킹이나 악성코드 감염 등에 의한 위·변조 사고를 예방하기 위하여 전자금융거래프로그램에 대한 무결성 검증 방법 제공(제5호)

2. 이용자유의사항 공지

〈 감독규정 〉

제35조(이용자 유의사항 공지) 금융회사 또는 전자금융업자는 전자금융거래의 안전한 수행을 위하여 이용자에게 다음 각 호의 사항을 준수하도록 공지하여야 한다.

1. 비밀번호 유출위험 및 관리에 관한 사항
2. 금융기관 또는 전자금융업자가 제공하고 있는 이용자 보호제도에 관한 사항
3. 해킹·피싱 등 전자적 침해 방지에 관한 사항
4. 본인확인 절차를 거쳐 비밀번호 변경이 가능하도록 정보처리시스템을 구축하고 비밀번호 변경 시 같은 번호를 재사용하지 않도록 할 것

▣ 전자금융거래이용자가 안전한 전자금융거래를 수행할 수 있도록 개인정보유출방지, 금융이용자 보호제도 및 비밀번호 관리에 관한 사항 공지

▣ 해설

- 금융회사 또는 전자금융업자는 전자금융거래 이용자 유의사항을 홈페이지 게시 등 전자적인 방법 또는 우편물 등을 통하여 이용자에게 공지

3. 자체 보안성심의

〈 감독규정 〉

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 "자체 보안성심의"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 기관으로서 금융감독원장이 정하는 기준에 해당하는 금융회사 또는 전자금융업자는 그러하지 아니하다.

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 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

〈 시행세칙 〉

제3조(자체 보안성심의 기준 등) ① 규정 제36조제1항에 따른 금융감독원장이 정하는 기준과 절차란 다음 각 호를 말한다.

1. 정보통신망을 이용하여 신규전자금융업무를 수행하는 경우 〈별표 1〉의 기준에 따라 보안성심의를 실시한 후 정보보호최고책임자의 승인을 받을 것
2. 공동으로 전자금융거래 관련 표준을 제정하는 경우 〈별표 1의2〉의 기준에 따라 보안성심의를 실시할 것 (다만, 이 경우 특정 금융회사 또는 전자금융업자가 다른 금융회사등을 대표하여 규정 제36조제2항에 따른 자체 보안성심의 결과보고서를 제출할 수 있음).

② 금융회사 또는 전자금융업자가 규정 제36조제2항에 따라 제출하는 자체 보안성심의 결과보고서의 양식은 제1항제1호의 경우 별지 제3호 서식에, 제1항제2호의 경우 별지 제4호 서식에 각각 따른다.

③ 금융회사 또는 전자금융업자는 제1항에 따른 자체 보안성심의를 수행함에 있어 필요한 경우 규정 제37조의4제1항의 침해사고대응기관, 「정보통신기반보호법」 제16조제1항의 정보공유·분석센터 등 외부기관에 보안대책의 적정성 여부 등에 대한 검토를 의뢰할 수 있다.

④ 규정 제36조제2항 단서에서 "금융감독원장이 인정하는 기준"이란 다음 각 호에서 정하는 요건을 충족하는 것을 말한다.

1. 전자금융업자 : 법 제28조에 따라 금융위원회로부터 허가를 받았거나 금융위원회에 등록한 날 및 전자금융업무를 신규로 수행한 날로부터 1년이 경과하였을 것.
2. 금융회사 : 전자금융업무를 신규로 수행한 날로부터 1년이 경과하였을 것

▣ 금융회사 또는 전자금융업자의 정보통신망을 이용하여 이용자를 대상으로 신규로 전자금융업무를 수행하는 경우 전자금융업무의 안전성이 확보될 수 있도록 금융감독원장이 정한 거래당사자 인증, 거래정보의 기밀성 및 무결성, 정보유출 방지대책 등 기준과 절차에 따라 자체 보안성심의를 실시하여 전자금융업무의 보안 문제점을 제거

▣ 해설

● 금융회사 또는 전자금융업자는 전자금융업무를 신규로 추진하고자 하는 경우 금융감독원장이 정한 자체 보안성심의 기준에 따라 보안성 심의를 실시하고 정보보호최고책임자의 승인을 받은 후 전자금융업무가 제공 또는 시행된 날로부터 7일 이내에 보안성심의 결과 보고서를 금융감독원에 제출

신규 전자금융업무의 제공 또는 시행일 기준으로 과거 1년 이내에 전자금융사고가 발생하지 않은 금융회사 등은 자체 보안성 심의 결과를 금융감독원 제출 면제(제1항제1호)

- 다만, 신규등록한 전자금융업자 또는 전자금융서비스를 최초 제공한지 1년이 지나지 않은 금융회사는 '1년 이내 전자금융사고가 발생하지 않은 기관'에 포함되지 않음(시행세칙 제3조제4항)
- 즉, 자체 보안성심의가 면제되는 대상은 해당 전자금융업무를 신규로 수행한지 1년이 넘은 금융회사나 전자금융업자 중 최근 1년 동안 전자금융사고가 발생하지 않은 회사
- 여기서의 '전자금융업무'란 PG업, 에스크로업과 같이 전자금융업 등록 단위가 아닌 계좌이체, 멤버십 기능 추가, 본인인증 방식 추가 등 세부적 단위의 업무를 의미

● 금융회사 또는 전자금융업자 공동으로 표준 제정시 보안성심의 실시 및 사후 보고 필요(제1항제2호)

- 공동 표준안 제정시 보안성심의에 관한 자료는 표준 제정에 참여한 금융회사 중 대표 금융회사가 제출 가능

● 전자금융업무에 대한 자체 보안성심의 기준 및 절차는 금융감독원장이 정한 심의 기준〈시행세칙 별표1〉에 따라 보안성심의를 실시하고 정보보호최고책임자의 승인을 받는 것을 의미(세칙 제3조제1항제1호)

- 공동 표준 제정에 대한 자체 보안성심의는 〈시행세칙 별표1의2〉에 따라 실시 (세칙 제3조제1항제2호)

● 금융회사 등이 자체 보안성 심의를 실시할 때 필요한 경우 침해사고대응기관, 정보공유·분석센터(금융보안원) 등 외부 전문기관에 의뢰하여 심의대상 전자금융업무에 대한 보안대책의 적정성 여부 검토 가능

※ 법령해석('16.1.12.)

〈 질의 〉

▣ 「전자금융감독규정」상 자체 보안성 심의 대상인 "신규 전자금융업무"의 구체적 의미

〈 회신 〉

▣ 금융당국에서는 금융회사 및 전자금융업자의 부담을 완화하고 자율적인 보안수준 확보 노력을 유도하고자 과거 금융감독원에서 수행하는 보안성심의 제도를 폐지하고 자체 보안성심의를 수행 보고토록 하고 있으며, 자체 보안성 심의 대상은 「전자금융감독규정」 제36조에서 "신규 전자금융업무"로 규정하고 있습니다.

▣ 이때 '전자금융업무'란 PG업, 에스크로업과 같이 전자금융업 등록 단위가 아닌 계좌이체, 멤버십 기능 추가, 본인인증 방식 추가 등 세부적 단위의 업무를 뜻합니다.

따라서 예시하신 (i)신규로 전자금융업 중 하나를 등록하면서 약관도 제정하여 신고하는 경우, (ii)기존에 전자금융업으로 등록하고 약관 신고도 마친 전자금융서비스를 영위 중 기존 전자금융업 서비스 중 일부 서비스에 새로운 유형의 전자금융서비스를 추가하여 출시하는 경우, (iii)기존 전자금융업 등록한 서비스와 동일 유형의 전자금융서비스를 추가로 출시하는 경우와 더불어 (iv)기존 전자금융업으로 등록한 서비스의 전자금융업무 유형을 유지하면서 관련한 서비스를 추가로 출시하는 경우, (v)기존 전자금융업으로 등록된 서비스의 일부 변경, 개편, 기능추가 등의 경우에도 새로운 서비스가 추가된다면 신규에 해당하는 것으로 볼 수 있습니다.

다만, (iv), (v)의 경우 단순 메뉴 추가, 디자인 변경 등 신규성이 있다고 보기 어려운 경우도 많습니다. 이런 경우 보안성심의의 목적에 맞게 보안리스크가 상당히 증가하는 경우에만 신규성이 있다고 판단하고 있습니다.

▣ 또한, 금융당국은 자율 보안수준 확보라는 목적에 맞춰 금융회사 및 전자금융업자가 자체 보안리스크 평가 기준을 내규화하여 평가결과에 따라 신규성을 판단하도록 유도하고 있습니다.

▣ 따라서 명백히 신규성이 있다고 판단되는 (i), (ii), (iii)의 경우 및 (iv), (v)의 경우 중 자체 내규에 따라 신규성이 있다고 판단되는 경우 자체보안성심의를 실시하시면 됨을 알려드립니다.

〈 이유 〉

▣ 「전자금융감독규정」 제36조의 자체 보안성심의는 보안성 수준에 대한 심의를 하는 것으로 신규성의 기준은 보안관점에서 볼 때 신규성입니다.

* (예시) 당초 조회기능만 제공하던 모바일금융서비스 앱에서 신규로 이체 등 거래를 추가할 경우 보안리스크가 증가하고 증가한 수준이 보안에 미치는 영향이 상당하다고 판단될 때 이를 신규로 판단하여 자체 보안성심의 실시 및 금융감독원 제출 필요

※ 법령해석('16.5.2.)

〈 질의요지 〉

▣ 은행의 「핀테크 오픈플랫폼」에서 제공하는 API를 활용하여 핀테크 기업이 제작한 핀테크 서비스가 신규 전자금융업무에 해당할 경우,

○ 동 핀테크서비스에 대해 은행이 보안성심의 실시 및 결과보고를 해야 하는지 여부

〈 회신 〉

▣ 신규 전자금융업무를 수행하는 핀테크 기업이 전자금융업자에 해당하는 경우 「전자금융감독규정」 제36조의 자체 보안성 심의를 실시하여야 합니다.

▣ 은행이 핀테크 기업에 API를 제공하는 데에 그치고 직접 전자금융업무를 수행하지 않는 경우에는 해당 조항에 따른 보안성 심의 실시 및 결과보고 의무의 적용을 받지 않습니다.

〈 이유 〉

▣ 「전자금융감독규정」 제36조(자체 보안성심의)는 금융회사 또는 전자금융업자가 신규 전자금융업무를 수행하는 경우 자체적으로 보안성심의를 실시하도록 규정하고 있습니다. 따라서 '금융회사 또는 전자금융업자'가 아닌 경우 또는 직접 '전자금융업무를 수행'하지 않는 경우에는 해당 조항의 적용을 받지 않는 것으로 판단됩니다.

▣ 다만, 보안성심의 실시 주체와 별개로 핀테크 기업과 협약을 맺어 API를 제공하는 은행의 신뢰 유지 및 금융소비자 보호 등의 측면을 고려하여 금융보안원을 통한 보안 컨설팅 등 해당 서비스의 안정성 확보에 충분한 노력을 기울여야 할 것입니다.

금융감독원장이 정한 자체 보안성심의 기준(신규 전자금융업무)

	심의기준
1	거래 당사자 인증
2	거래정보의 기밀성 및 무결성
3	정보처리시스템 보호대책
4	고객 단말기 보호대책
5	정보유출 방지대책
6	이상금융거래 방지대책
7	시스템 가용성 확보 및 비상대책
8	시스템 설치장소에 대한 물리적 접근통제

※ 전자금융업무 유형에 따라 자체적으로 심의기준 추가수정 가능

금융감독원장이 정한 자체 보안성심의 기준(공동 표준안)

	심의기준
1	컴플라이언스 준수
2	사용자 접근성
3	호환성 지원
4	서비스 품질 보장(안정성)
5	불필요한 기능 제거(간결성)
6	표준화 그룹 체계 관리

※ 공동표준안의 유형에 따라 자체적으로 심의기준 추가수정 가능

4. 인증방법 사용기준

〈 감독규정 〉

제37조(인증방법 사용기준) 금융회사 또는 전자금융업자는 전자금융거래의 종류·성격·위험수준 등을 고려하여 안전한 인증방법을 사용하여야 한다.

▣ 금융회사 또는 전자금융업자가 전자금융거래 이용자 신원확인, 거래내용의 위·변조, 거래사실의 부인방지 등을 위해 전자금융거래 시 적용하였던 공인인증서의 사용의무가 폐지되고, 금융회사 등이 전자금융거래의 종류·성격·위험수준 등을 고려하여 전자금융거래의 안전성 및 정당성 확보에 가장 적합하다고 판단되는 인증방법 사용

※ 법령해석('16.5.2.)

〈 질의 〉

▣ 공인인증서 대신 가상번호(VASCO 토큰) 인증을 인터넷뱅킹의 인증방법으로 사용하는 것이 가능한지 여부

〈 회신 〉

▣ 전자금융거래에 있어서 공인인증서 대신 「전자금융감독규정」 제37조(인증방법 사용기준)에 따라 안전하다고 판단되는 인증방법을 사용하는 것이 가능합니다.

〈 이유 〉

▣ 「전자금융거래법」 제21조(안전성의 확보의무)는 전자금융거래의 안전성 및 신뢰성을 확보하는 것을 전제로 특정 기술 또는 서비스의 사용을 강제하지 않는 '기술중립성 원칙'을 명확히 하고 있으며, 「전자금융감독규정」 제37조도 전자금융거래에 있어 특정한 인증방법(예 : 공인인증서)을 한정하고 있지 않으므로 금융회사 또는 전자금융업자의 판단과 책임 하에 안전한 인증방법을 적절히 선택하여 사용할 수 있다고 봄이 타당합니다.

※ 비조치의견서('16.5.27.)

〈 질의요지 〉

▣ 인터넷/스마트뱅킹을 통한 전자자금이체 거래시 ○○안심보안카드*를 인증방법으로 사용할 경우,

* ○○안심보안카드를 스마트폰에 접촉하여 본인임을 인증하고, 이체 거래시 보안카드번호를 입력하는 2단계 인증절차를 수행

○ 동 인증방법이 전자금융감독규정 제37조에서 정한 안전한 인증방법에 해당하는지 여부

〈 회답 〉

▣ 금융회사는 전자금융거래에 사용되는 인증방법을 자율적으로 선택하여 사용할 수 있습니다.

○ 다만, 개정 법규의 취지에 따라 금융회사 자체적으로 보안 및 인증방법에 대한 안전성을 확보해야 하오니 이 점 유념하시기 바랍니다.

〈 판단이유 〉

▣ 전자금융거래법 제21조제3항 및 전자금융감독규정 제37조의 내용을 고려*할 때 금융회사는 전자금융거래에 사용되는 인증방법을 자율적으로 선택할 수 있습니다.

* 특정 기술 또는 서비스의 사용을 강제하지 않는 '기술 중립성 원칙'이 도입됨에 따라 경쟁촉진적인 인증기술 사용을 위해 전자금융거래시 공인인증서 등을 사용하도록 한 의무를 폐지(금융위원회 고시 제2015-7호)

5. 전자금융기반시설의 취약점 분석·평가주기, 내용 등

※ 관계 법령

〈 법 〉

제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등) ① 전자금융기반시설의 취약점 분석·평가는 총자산이 2조원 이상이고, 상시 종업원 수(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다) 300명 이상인 금융회사 또는 전자금융업자이거나 「수산업협동조합법」, 「산림조합법」, 「신용협동조합법」, 「상호저축은행법」 및 「새마을금고법」에 따른 중앙회의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하여야 한다.

② 금융회사 및 전자금융업자는 취약점 분석·평가를 위하여 정보보호최고책임자(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 제1항에 따른 금융회사 및 전자금융업자 이외의 자의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하되 자체전담반을 구성하지 아니할 수 있다. 이 경우 취약점 분석·평가의 내용은 금융감독원장이 정한다.

④ 금융회사 및 전자금융업자는 해당 주기 내에 평가 대상 시설과 평가기간을 나누어 평가할 수 있다.

⑤ 금융회사 또는 전자금융업자는 취약점 분석·평가에 따라 이행계획을 수립·시행하여야 하며 다음 각 호의 사항을 준수하여야 한다.

1. 취약점 분석·평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치의 시행
2. 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우에는 최고경영자 승인을 득할 것

3. 이행계획의 시행 결과는 최고경영자에게 보고할 것

〈 시행세칙 〉

제7조의2(전자금융기반시설의 취약점 분석·평가의 내용) 규정 제37조의2제3항에 따라 감독원장이 정하는 취약점 분석·평가의 내용는 별표 3과 같다

▣ 금융회사 또는 전자금융업자는 전자금융기반시설에 대하여 관리적, 물리적, 기술적 취약점을 연 1회 이상(홈페이지는 6개월에 1회 이상)점검하여 식별된 보안 취약점을 제거 또는 보완함으로써 전자금융기반시설의 기밀성, 가용성, 무결성 확보를 통해 대내외 위협으로부터 조직의 정보자산을 안전하게 보호하고 이용자에게 안전한 전자금융거래 서비스를 제공

▣ 해설

- 총자산이 2조원 이상이고 상시종업원이 300명 이상인 금융회사 또는 전자금융업자와 수산업협동조합, 산림조합, 신용협동조합, 상호저축은행법 및 새마을금고법에 따른 중앙회는 정보보호최고책임자를 포함한 5인 이상(30%이상은 고급기술인력 이상의 자격을 갖출 것)으로 자체 전담반을 구성하거나, 규정 제37조의3제1항에 따른 외부평가전문기관에 위탁하여 전자금융기반시설에 대한 취약점 분석·평가를 연 1회 이상(홈페이지는 6개월에 1회 이상)실시(제1항, 제2항)

- 제37조의2제1항에 해당하지 않는 금융회사 또는 전자금융업자는 연 1회 이상(홈페이지는 6개월에 1회 이상)실시하되 자체 전담반을 구성하지 않고 취약점 분석·평가 실시 가능, 이 경우 금융감독원장이 정한 취약점 분석·평가 내용에 따라 실시(제3항)

전자금융기반시설 취약점 분석·평가 내용〈시행세칙 별표3〉

평가 부문	평가 항목
관리적 보안	– 정보보호 정책 – 정보보호 조직 및 인력 – 내부통제 – 정보보호 교육 및 훈련 – 자산관리 – 업무연속성 관리 – 사고관리 – 정보시스템 도입·개발·유지보수
물리적 보안	– 전산설비 보안 – 전산센터 보안
기술적 보안	– 인터넷 전자금융 보안 – 모바일 전자금융 보안 – 접근통제 – 전산자료 보안 – 서버 보안 – 데이터베이스 보안 – 웹 서비스 보안 – 단말기 보안 – 네트워크 보안 – 정보보호시스템 보안

- 금융회사 또는 전자금융업자는 해당 주기 내에 평가대상 시설과 평가기간을 나누어 시행 가능하며, 취약점 분석·평가에 따라 이행계획을 수립·시행하며 다음 사항을 준수(제4항, 제5항)
  - 취약점 분석·평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치 시행
  - 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우는 최고경영자 승인
  - 이행계획의 시행 결과는 최고경영자에게 보고

▣ 취약점·분석 평가 결과 보고서 제출처가 금융위에서 금감원으로 변경됨에 따라 업무보고서 내 접수 시스템 마련

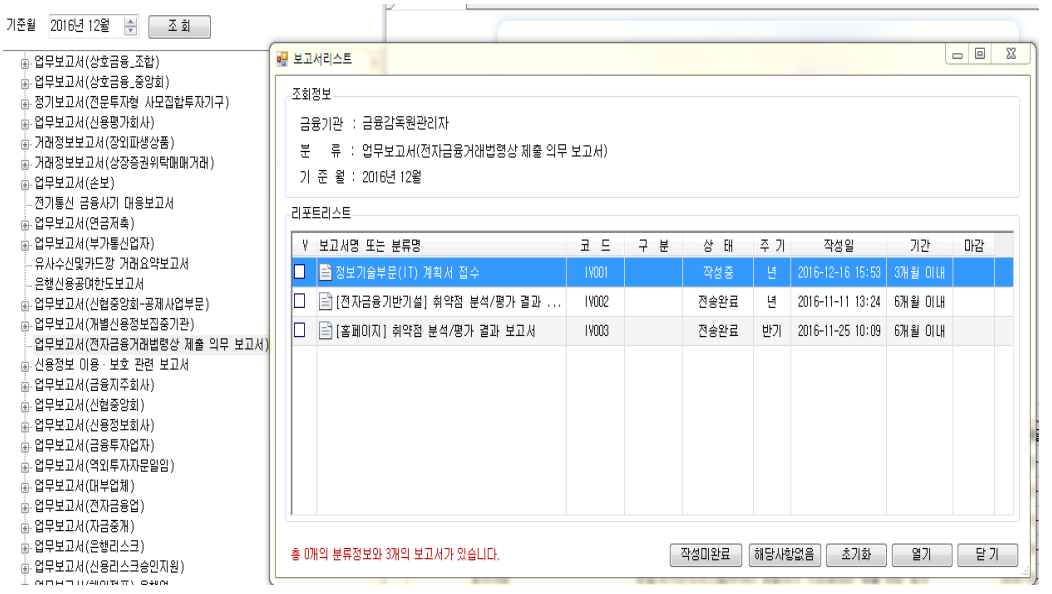
- '17년부터 제출하는 취약점·분석 평가 결과 보고서는 금융정보교환망*의 「금융감독원 보고서 작성기」를 이용하여 제출

  * 금융정보교환망 : fines.fss.or.kr, 헬프데스크 : 02)3145-5401/5413

● 기준월을 회계연도 마감월로 선택하여 조회를 누르면, 업무보고서(전자금융거래법령상 제출 의무 보고서)이 선택되며, 이 중 '취약점 분석·평가 결과 보고서'를 선택하여 보고서 제출 전 자체 체크리스트 점검 후 보고서를 제출

※ 홈페이지 취약점 평가 보고서의 경우 "회계연도 마감월", "회계연도 마감월+6개월"으로 1년에 2번 보고서 제출이 필요함

예) 12월이 회계마감월인 경우, 매년 12월, 6월 기준월 업무보고서를 검색하여 제출



※ 법령해석('15.10.15.)

〈 질의 〉

▣ 금융거래정보 미포함 홈페이지의 경우 전자금융기반시설의 취약점 분석·평가 대상에서 제외되는지 여부

* (사실관계) ○○자산운용의 경우 전자금융거래가 발생하는 펀드거래시스템 일체(거래 전용 홈페이지 포함)를 코스콤에 외주를 주고 있으며, 해당 시스템에 대해서는 매년 취약점을 분석하여 보고하고 있음
그러나 ○○자산운용의 홈페이지는 금융거래와 관련한 정보는 일체 보유하고 있지 않으며 코스콤에서 위탁운용하고 있는 펀드거래시스템에 단순 링크만 해놓고 있음

〈 회신 〉

▣ 「전자금융거래법」 제21조의3제1항에 따르면 금융회사 및 전자금융업자는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 '전자금융기반시설'에 대하여 취약점 분석·평가를 실시하고 그 결과를 금융위원회에 보고하여야 하나,

▣ 금융회사 및 전자금융업자가 운영하는 홈페이지가 「전자금융거래법」 제2조제21호의 '전자금융기반시설'에 해당되지 않을 경우, 즉 전자금융거래에 이용되지 않거나 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계가 없는 경우에는 같은 법 제21조의3제1항에 따른 취약점 분석·평가 대상이 아닙니다.

〈 이유 〉

▣ 「전자금융거래법」 제21조의3제1항은 금융회사 및 전자금융업자에 대해 전자금융거래의 안전성과 신뢰성을 확보하기 위해 전자금융기반시설에 대하여 취약점 분석·평가를 실시하도록 하고 있습니다.

▣ 한편, 같은 법 제2조제21호에서는 '전자금융기반시설'에 대하여 '전자금융거래에 이용되는 정보시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망'으로 정의하고 있고, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에서는 '정보통신망'에 대하여 '전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제'로 정의하고 있습니다.

▣ 이상 각 법률의 정의에 따라 금융회사 및 전자금융업자가 운영하는 홈페이지가 전자금융거래에 이용되지 않거나 정보의 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 사용하지 않는 경우 「전자금융거래법」 제21조의3제1항에 따른 취약점 분석·평가 의무가 없습니다.

6. 전자금융기반시설의 취약점 분석·평가 전문기관의 지정 등

〈 감독규정 〉

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 금융회사 및 전자금융업자는 시행령 제11조의5제3항에 따른 전자금융기반시설의 취약점 분석·평가 결과 보고서를 금융위원장에게 제출하여야 하며, 금융감독원장은 결과보고서를 분석하여 매분기 1개월 이내에 금융위원장에게 보고하여야 한다.

③ 금융위원장은 취약점 분석·평가 결과보고서에 근거하여 필요시 금융회사 및 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

▣ 금융회사 또는 전자금융업자가 취약점 분석·평가 실시를 위탁 가능한 외부평가전문 기관을 지정하고, 그 실시 결과를 금융위원회에 보고하도록 하여 전자금융기반시설에 대한 취약점 분석·평가의 실효성 제고

▣ 해설

● 전자금융기반시설에 대한 취약점 분석·평가를 자체 실시하거나 외부평가전문 기관에 위탁하여 실시한 후 그 결과보고서를 금융감독원에 제출

※ 관계 법령

〈 시행령 〉

제11조의5(전자금융기반시설 취약점 분석·평가의 절차 및 방법 등)

③ 금융회사 및 전자금융업자는 법 제21조의3제1항에 따라 전자금융기반시설의 취약점 분석·평가를 하였을 때에는 다음 각 호의 사항이 포함된 결과보고 및 보완조치 이행계획서를 그 취약점 분석·평가 종료 후 30일 이내에 금융위원회에 제출하여야 한다.

1. 취약점 분석·평가의 사유, 대상, 기간 등 실시개요
2. 취약점 분석·평가의 세부 수행방법
3. 취약점 분석·평가 결과
4. 취약점 분석·평가 결과에 따른 필요한 보완조치의 이행계획
5. 그 밖에 취약점 분석·평가의 적정성을 확보하기 위하여 필요한 사항으로서 금융위원회가 정하여 고시하는 사항

7. 침해사고대응기관

〈 감독규정 〉

제37조의4(침해사고대응기관 지정 및 업무범위 등) ① 침해사고에 대응하기 위한 침해사고대응기관은 다음 각 호의 자로 한다.

1. 금융보안원
2. 삭제
3. 금융위원장이 지정한 자

② 침해사고대응기관은 다음 각 호의 업무를 수행한다.

1. 침해사고에 관한 정보의 수집·전파를 위한 정보공유체계의 구축
2. 침해사고의 예보·경보 발령내용의 전파
3. 침해사고의 원인분석과 신속한 대응 및 피해 확산방지를 위해 필요한 조치
4. 금융회사 및 전자금융업자와 관련된 해킹 등 전자적 침해행위 정보를 탐지·분석하여 즉시 대응 조치를 하기 위한 기구(이하 "금융권 통합 보안관제센터"라 한다)의 운영

③ 금융위원장은 침해사고대응기관을 포함하여 침해사고조사단을 구성할 수 있다.

④ 금융위원장은 제2항에 따른 침해사고 긴급대응을 위한 침해사고대응기관의 업무 수행 또는 제3항에 따른 침해사고 원인분석 및 긴급조치를 위하여 금융회사 및 전자금융업자, 전자금융보조업자에 협조를 요청할 수 있다.

⑤ 금융회사 및 전자금융업자는 침해사고에 대한 대응능력 확보를 위하여 연 1회 이상 침해사고 대응 및 복구훈련 계획을 수립·시행하여야 하며 그 계획 및 결과를 침해사고대응기관의 장에게 제출하여야 한다.

다만 다음 각 호의 어느 하나에 해당하는 금융회사는 그러하지 아니한다.
1. 법 제2조제3호가목의 금융회사 중 신용협동조합
2. 법 제2조제3호다목·라목의 금융회사
3. 시행령 제2조제4호부터 제6호까지의 조합
4. 시행령 제5조제2항의 요건을 충족한 금융회사
⑥ 금융위원장은 침해사고대응기관의 장으로 하여금 침해사고 대응·복구 및 훈련결과를 점검하고 보완이 필요하다고 판단되는 경우 개선·보완을 요구할 수 있다.
⑦ 금융위원장은 침해사고대응기관의 장으로 하여금 시행령 제11조의6제1항제4호에 따른 보안취약점 통보를 위하여 금융회사 및 전자금융업자가 사용하고 있는 소프트웨어에 대한 조사·분석을 실시하게 할 수 있다.

▣ 금융위원회는 침해대응기관을 지정하여 금융회사 또는 전자금융업자의 침해사고에 대한 정보공유체제 구축, 예보 및 경보 발령내용 전파, 원인분석과 신속한 대응을 통한 피해 확산 방지, 금융회사 또는 전자금융업자의 침해사고 대응능력 확보를 위해 침해사고 대응 및 복구 훈련 계획을 수립·시행

▣ 해설

● 금융회사 또는 전자금융업자는 해킹, 악성코드, 서비스 거부(DDoS) 공격 등 전자적 침해에 대한 대응능력 확보를 위해 연 1회 이상 침해사고 대응 및 복구 훈련 계획을 수립하여 시행하고 그 결과를 침해사고대응기관(금융보안원)의 장에게 제출(제5항)

〈 전자적 침해행위(예시) 〉

위기유형	상세설명
해킹	접근권한이 없거나 접근권한을 초과하여 전산시스템 및 전산망에 접근하여 데이터를 조작·파괴·은닉 또는 유출
악성코드	컴퓨터바이러스·논리폭탄 등 악성 프로그램을 투입하여 전산시스템 및 전산망의 운영 방해 또는 데이터 파괴
서비스 거부	일시에 대량의 선호를 보내거나 부정한 명령의 처리 등을 통해 전산시스템 및 전산망 운영 방해 또는 정보처리 오류 발생

〈 침해사고 대응 및 복구훈련 계획 항목 〉

유 형	세부항목(예시)
훈련계획	훈련목적, 훈련참여자, 훈련기간, 훈련대상 - 훈련조직 구성(담당자 임무부여 포함) - 유관기관 및 관련업체와의 비상연락체제 구축
	훈련 시나리오, 훈련 절차 및 방법 등 - 상황별 대응절차·방안(수립된 비상대책 준용)
훈련결과	수립한 훈련계획에 대한 이행여부
	내부평가 및 개선사항 도출 등
	개선이행 계획 수립 등

- 침해사고대응기관(금융보안원)은 침해사고 대응 및 복구 훈련 계획 및 결과를 점검하고 점검결과와 필요한 경우 개선·보완 사항을 포함하여 제출기관에게 전달
- 금융회사 또는 전자금융업자는 훈련 실효성 확보를 위하여 통지 받은 개선·보완 사항을 차기년도 훈련 계획에 반영·실행
- 전자적 침해에 대한 대응능력 확보를 목적으로 하는 침해사고 대응 및 복구훈련은 위기대응행동매뉴얼 또는 비상대책을 통한 업무 중단방지와 신속한 복구를 목적으로 하는 비상대응훈련(규정 제24조)과 훈련목적 등 제반 사항이 상이함

〈 훈련 간 비교 〉

훈련 구분	침해사고 대응·복구훈련	비상대응훈련
관련규정	규정 제37조의4	규정 제24조
훈련목적	침해사고에 대한 대응능력 확보	장애, 재해, 파업, 전자적 침해 등 발생가능한 모든 위험으로 인한 업무 중단 방지와 신속한 복구
훈련범위	전자적 침해	자연 재해, 인적 재해, 기술적 재해, 전자적 침해
훈련주기	연 1회 이상	연 1회 (재해복구전환훈련은 연1회 이상)
훈련실시	금융회사등의 침해사고대응·복구훈련 계획에 따라 실시	금융회사등의 위기대응행동매뉴얼 또는 비상대책에 따라 실시 (재해복구훈련 포함 가능)
훈련결과	침해사고대응기관의 장에게 제출	금융위원회에 보고

- 전자적 침해에 대한 비상대응훈련을 수행한 경우 이를 침해사고대응·복구훈련으로 갈음할 수 있으며, 침해사고 대응 및 복구훈련 결과로 별도 제출하여야 함

〈참고〉 침해사고 대응 및 복구 훈련 결과 제출 관련 Q&A

Q1 모든 금융회사가 침해사고 대응 및 복구 훈련 결과(계획)를 제출하여야 하나요?

A1 감독규정 제37조의4제5항제1호부터 제4호까지에 해당하는 금융회사의 경우 훈련 결과를 제출하지 않습니다.

※ 금융회사는 예외조항(전자금융업무 수행여부 등)을 확인하여 예외조항에 해당되지 않는 경우에는 반드시 훈련결과를 제출할 수 있도록 하여야 합니다.

Q2 침해사고 대응 및 복구 훈련 결과(계획 포함)는 어떤 방법으로 제출하는 건가요? 제출 시기도 궁금합니다.

A2 금융회사 또는 전자금융업자는 훈련 실시 및 내부 책임자에게 보고 후 침해사고대응기관(금융보안원)이 제공하는 방법(금융보안원 정보공유체계, 이메일 등)으로 침해사고 대응 및 복구 훈련 결과(계획 포함)를 제출하시면 됩니다.

※ 제출 시기는 훈련결과에 대한 내부보고 후 1 개월 이내 권고

Q3 금융회사 또는 전자금융업자가 침해사고대응·복구훈련결과보고서를 침해사고대응기관에 제출함으로써 금융위원회 앞 전자적 침해에 대한 비상대응훈련결과보고서 보고 의무를 이행한 것으로 볼 수 있는지 궁금합니다.

A3 불가능합니다. 비상대응훈련 결과는 금융위원회에 보고하고, 침해사고 대응 및 복구훈련 결과는 침해사고대응기관(금융보안원)으로 제출하여야 합니다.

Q4 전자금융거래 시스템을 위탁하여 임대 운영하거나 해외에 있는 시스템을 사용하여 전자금융거래 시스템을 직접 보유하지 않은 경우에도 전자금융업무가 있다면 침해사고대응 및 복구 훈련 계획을 수립 시행하고 결과를 제출하여야 하나요?

A4 어떤 경우에도 전자금융업무를 취급하는 금융회사 또는 전자금융업자는 침해사고대응 및 복구 훈련 계획을 수립 시행하고 결과를 제출하여야 합니다.

Q5 침해사고대응기관(금융보안원)이 금융회사 또는 전자금융업자가 제출한 침해사고대응·복구훈련 결과보고서를 취합하여 전자적 침해에 대한 비상대응훈련 결과로 금융위원회에 보고할 수는 없나요?

A5 침해사고대응기관(금융보안원)이 금융회사 또는 전자금융업자가 제출한 침해사고 대응 및 복구 훈련 결과를 취합하여 전자적 침해에 대한 비상대응훈련 결과로 금융위원회에 보고하는 것은 불가합니다. 또한, 금융회사 또는 전자금융업자가 외부기관을 통해 합동훈련 등을 수행한 경우에도 금융회사 또는 전자금융업자가 직접 제출하여야 합니다.

Q6 침해사고대응기관(금융보안원)으로부터 침해사고대응훈련 실시와 관련하여 지원을 받고자 하는 경우, 어떻게 하여야 하나요?

A6 훈련 실시 직전연도 말까지 침해사고대응기관(금융보안원)으로 훈련 참여 신청을 하시면 됩니다. 금융보안원 사원이 아닌 경우에는 사전에 금융보안원 사원 자격 취득이 필요합니다.

8. 정보보호최고책임자(CISO)의 업무

〈 감독규정 〉

제37조의5(정보보호최고책임자의 업무) 정보보호최고책임자는 정보보안점검의 날을 지정하고, 임직원이 금융감독원장이 정하는 정보보안 점검항목을 준수했는지 여부를 매월 점검하고, 그 점검 결과 및 보완 계획을 최고경영자에게 보고하여야 한다.

〈 시행세칙 〉

제7조의3(정보보호최고책임자의 업무) 규정 제37조의5에 따라 감독원장이 정하는 정보보안 점검항목은 별표 3-2와 같다.

▣ 정보보호최고책임자는 임직원 정보보안 인식 강화 및 보안사고 예방을 위하여 금융감독원장이 정한 정보보안 점검항목에 따라 매월 전사적 정보보안 점검의 날을 지정하여 점검을 실시

▣ 해설

- 정보보호최고책임자는 정보보안 인식강화 및 사고예방을 위하여 매월 보안점검의 날을 지정하고, 금융감독원장이 정한 보안점검 항목에 대한 임직원의 준수 여부를 점검하고, 그 점검 결과 및 보완계획을 최고경영자에게 보고하여 조직의 정보보안 수준 강화
  - 최고경영자에게 매월 보고가 필요하나 반드시 결재를 요하지는 않으며, 규정 제8조 제1항제4호의 점검결과(임직원의 정보보안 법규 준수 여부 점검결과)와 함께 보고하여도 무방함

금융감독원장이 정한 정보보안 점검항목 〈시행세칙 별표 3-2〉

	점검항목
전산실	상시출입자외 출입자에 대한 책임자 승인 및 출입자관리기록부 기록·보관 여부
	무인감시카메라 또는 출입자동기록시스템 등의 정상 작동 여부
단말기	업무담당자 이외의 단말기 무단조작 금지 조치 여부
	정보처리시스템 접속 단말기의 정당한 사용자인가를 확인할 수 있는 기록 유지 여부
	중요 단말기의 외부 반출 금지 여부
	중요 단말기의 인터넷 접속 금지 여부
	중요 단말기의 그룹웨어 접속 금지 여부
	단말기에서 보조기억매체 및 휴대용 전산장비 접근 통제 여부
전산자료	개인별 사용자계정과 비밀번호 부여 여부
	사용자계정과 비밀번호 등록·변경·폐기의 체계적 관리 여부
	이용자 정보 조회·출력 통제 여부
	테스트시 이용자 정보 사용 금지 및 불가피한 경우 이용자정보를 변환하여 사용하고 테스트 종료 즉시 삭제 여부
	단말기에 이용자 정보 등 주요정보 보관을 금지하고 불가피한 경우 책임자의 승인을 받고 있는지 여부
	단말기 공유 금지 여부
	전산자료 및 전산장비의 반출·반입 통제 여부
	사용자 인사 조치시 지체 없이 해당 사용자계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템 접근을 통제하고 있는지 여부
정보처리시스템	내부통신망의 비인가 전산장비·무선통신 접속 통제 여부
해킹 등 방지대책	해킹 등을 방지하기 위한 정보보호시스템의 정상 작동 여부
	정보보호시스템에 최소한의 서비스번호와 기능만을 적용하고 있는지 여부
	정보보호시스템에 업무목적이외 기능 및 프로그램 제거 여부
	정보보호시스템의 원격관리 금지 여부
	시스템프로그램 등 긴급하고 중요한 보정사항에 대한 즉시 보정작업 실시 여부
	무선통신망 이용 업무에 대한 승인 및 사전 지정 여부
악성코드	악성코드 검색 및 치료프로그램의 최신상태 유지 여부
	중요 단말기의 악성코드 감염여부를 매일 점검하고 있는지 여부
공개용 웹서버	사용자계정에 아이디·비밀번호 이외 추가 인증수단 적용 여부
	DMZ구간 내 이용자 정보 등 주요정보를 저장, 관리하지 않는지 여부
내부사용자 비밀번호	접근자 비밀번호 설정·운영 여부
	비밀번호 보관시 암호화 여부
이용자 비밀번호 관리	정보처리시스템 및 전산자료에 보관하고 있는 이용자 비밀번호 암호화 보관 여부
이용자 유의사항	비밀번호 유출위험 및 관리에 관한 사항의 공지 여부
	제공하고 있는 이용자보호 제도에 관한 사항의 공지 여부
	해킹·피싱 등 전자적 침해방지에 관한 사항의 공지 여부
전자금융 사고보고	전자적 침해행위에 대한 보고 및 조치 여부

※ 월보안 점검 방법(예시)

〈 전산실 〉

▣ 상시출입자 이외의 경우 전산실 출입에 따른 출입자관리기록부 기록 및 책임자 승인여부 확인(출입자에 대한 출입일시, 출입사유, 출입자 소속 등이 기록 여부 확인)

▣ 출입자의 출입내역 사후 확인이 가능하도록 내부 규정에 따라 녹화상태, 이전 기록 확인 등이 가능하도록 기록되고 있는지 확인

〈 단말기 〉

▣ 업무담당자의 단말기에 대한 제3자의 접근 가능 여부 확인(화면보호기 등)

▣ 정보처리시스템 접속 단말기는 내부기준에 따라 배정되고 있는지 확인

▣ 중요 단말기의 반출 여부 확인 (하드웨어 탈부착여부 확인 포함)

▣ 중요 단말기에서 인터넷 접속 여부 및 정책 확인

▣ 중요 단말기의 그룹웨어 접속 여부 및 정책 확인

▣ 인가되지 않은 보조기업매체, 휴대용 전산장비의 연결 및 사용가능 여부 실사, 관련 보안프로그램 정책 확인

〈 전산자료 〉

▣ 시스템별 계정 및 비밀번호가 내부기준에 맞게 관리되고 있는지 확인

▣ 입사, 전보, 퇴사 등 인사변동 발생 시 내부기준에 따라 관리되고 있는지 확인

▣ 내부기준에 따라 이용자 정보의 조회 및 출력이 통제되는지 확인

▣ 전산업무개발 또는 프로그램 변경 시 사용하는 데이터의 작성 또는 변환 절차 등에 대한 내부기준 마련 여부 확인

▣ 이용자정보를 변환하거나 임의의 데이터를 생성하여 사용하고 있는지 확인

▣ 단말기에 이용자정보 등 주요정보가 보관되고 있는지 확인(책임자승인 여부 포함)

▣ 단말기별 사용자 지정 여부 확인(공유금지 확인)

▣ 전산자료 및 전산장비의 반출·반입시 통제 및 승인절차 수행 여부 확인

▣ 반출입관리대장(또는 시스템)을 통해 전산자료 및 전산장비의 반출·반입 일시, 담당자, 목적, 관리자 확인 등의 내용이 적정한지 여부 확인

▣ 입사, 전보, 퇴사 등 사용자관리가 필요한 인사변동에 대하여 사용자계정과 비밀번호의 등록· 변경·폐기가 즉시 반영되는지 여부 확인

〈 정보처리시스템 〉

▣ 실제 내부통신망에 비인가 전산장비·무선통신 접속 시도 및 관련 보안프로그램의 정책 확인

〈 해킹 등 방지대책 〉

▣ 정보보호시스템 리스트 및 정상 동작 유지보수 관리 기록 및 실제 확인

▣ 방화벽 정책 확인 등을 통한 정보보호시스템에 최소한의 서비스번호와 기능만을 적용하고 있는지 여부 확인

▣ 정보보호시스템(S/W방화벽 등)에 업무목적이외 기능 및 프로그램 제거 여부

▣ 방화벽 정책 확인 등을 통한 정보보호시스템의 원격관리 금지 여부 확인

▣ 긴급하고 중요한 보정사항에 대한 리스트 확인 및 적용 여부 확인(OS 업데이트 등)

▣ 무선통신망 사용현황 파악 및 설치·운영 중인 모든 무선통신망에 대한 정보보호최고책임자 승인 여부 확인

〈 악성코드 〉

▣ 악성코드 검색 및 치료프로그램의 최신상태를 관리자화면 또는 이용자 단말기에서 확인

▣ 중요 단말기의 악성코드 감염여부 점검여부를 관리자화면 또는 이용자 단말기에서 확인

〈 공개용웹서버 〉

▣ 공개용 웹서버에 사용자가 접근할 경우 아이디·비밀번호 외 OTP, 공인인증서 등 추가 인증 수단 적용 여부 확인

▣ DMZ구간 내 이용자 정보 등 주요정보를 저장 여부 확인
(단, 거래로그 관리의 경우 암호화 저장, 관리 확인 및 적기 폐기 여부 확인)

〈 내부사용자 비밀번호 〉

▣ 접근자 비밀번호에 대한 설정 여부 확인 및 내부 패스워드 관련 규칙을 적용했는지 확인

▣ 내부사용자 비밀번호는 안전한 암호화 알고리즘(예 : 128비트 이상)을 통해 일방향 암호화 적용여부 확인

〈 이용자 비밀번호 관리 〉

▣ 정보처리시스템 및 전산자료에 보관하고 있는 이용자 비밀번호는 안전한 암호화 알고리즘(예 : 128비트 이상)을 통해 일방향 암호화 적용여부 확인

〈 이용자 유의사항 〉

▣ 비밀번호 유출위험 및 관리에 관한 사항을 홈페이지 게시 또는 이메일 발송 등 확인

▣ 제공하고 있는 이용자보호 제도에 관한 사항을 홈페이지 게시 또는 이메일 발송 등 확인

▣ 해킹·피싱 등 전자적 침해방지에 관한 사항을 홈페이지 게시 또는 이메일 발송 등 확인

〈 전자금융사고보고 〉

▣ 침해사고 발생 시 법률이나 내부규정 등에 따라 관계기관(금융감독원 등)에 신고가 필요한 경우신속하게 보고했는지 여부 확인

▣ 보고서 작성 시 처리 일시, 처리 방법 등 주요 진행경과를 보고했는지 확인

9. 금융위가 정하는 보관자료 및 거래기록 등

〈 감독규정 〉
제38조(금융위원회가 정하는 보관자료 및 거래기록 등) 시행령 제12조제1항제2호다목에서 "금융위원회가 정하여 고시하는 거래기록"이라 함은 제4조제1호의 기록을 말한다.

▣ 이용자가 전자금융거래에 오류가 있음을 인지하여 금융회사 또는 전자금융업자에게 정정을 요구하거나 금융회사 또는 전자금융업자 스스로가 오류를 인지하여 조치하는 오류정정 요구사실 및 처리결과에 관한사항의 기록 및 보존

▣ 해설

- 금융위원회가 정하여 고시하는 거래기록은 법 제8조에 따른 오류정정 요구사실 및 처리결과에 관한 사항으로서 이용자가 전자금융거래에 오류가 있음을 인지하여 금융회사 또는 전자금융업자에게 정정을 요구하거나 금융회사 또는 전자금융업자 스스로가 오류를 인지하여 조치하는 오류정정 요구사실 및 처리결과에 관한 사항을 1년간 보존

※ 관계 법령

〈 시행령 〉
제12조(전자금융거래기록의 보존기간·보존방법 및 파기 절차·방법 등) ① 법 제22조제1항 및 제3항에 따른 전자금융거래기록의 종류별 보존기간은 다음 각 호와 같다.
1. (생 략)
2. 다음 각 목의 전자금융거래기록은 1년간 보존하여야 한다.
   가. 건당 거래금액이 1만원 이하인 전자금융거래에 관한 기록
   나. 전자지급수단의 이용과 관련된 거래승인에 관한 기록
   다. 그 밖에 금융위원회가 정하여 고시하는 전자금융거래기록

※ 관계 규정

〈 감독규정 〉
제4조(확인에 필요한 구체적인 거래내용) 시행령 제7조제4항제6호에서 "금융위원회가 정하여 고시하는 사항"이란 다음 각 호를 말한다.
1. 법 제8조에 따른 오류정정 요구사실 및 처리결과에 관한 사항
2. 전자금융거래 신청, 조건변경에 관한 내용

10. 전자지급수단의 이용한도

〈 감독규정 〉
제39조(전자지급수단의 이용한도) 시행령 제13조제2항부터 제4항에 따라 금융위원회가 정하는 전자지급수단의 구체적인 이용한도는 〈별표3〉과 같다.

전자지급수단의 세부적 이용한도〈감독규정 별표3〉

가. 전자화폐 및 선불전자지급수단 발행권면 최고한도

(단위 : 만원)

구 분	발행권면 한도	
	무기명식[1]	기명식[2]
전자화폐	5	200
선불전자지급수단	50	200

1) 실지명의 확인이 없거나 예금계좌와 연결되지 않고 발행된 전자화폐 내지 선불전자지급수단
2) 실지명의가 확인되거나 예금계좌와 연결되어 발행된 전자화폐 내지 선불전자지급수단

나. 전자자금이체한도(지급이체의 경우)

(단위 : 억원)

구 분		1회 이체한도	1일 이체한도
현금카드[1]	인출한도	0.01	0.06
	이체한도	0.06	0.3
텔레뱅킹[2]	개인	0.5	2.5
	법인	1	5
인터넷뱅킹[3]	개인	1	5
	법인	10	50
모바일뱅킹[4]		1	5
메일뱅킹[5]		0.1	0.5

1) 금융회사의 자동화기기(CD/ATM)에서 현금을 인출하기 위해 사용하는 접근매체
2) 유선전화를 통하여 예금조회, 자금이체 등의 업무를 수행하는 전자금융방식
3) 유무선 인터넷을 통해 예금조회, 자금이체 등의 업무를 수행하는 전자금융방식
4) 이동통신용 기기에 IC칩을 넣거나 뱅킹용 프로그램을 다운로드하여 예금조회, 자금이체 등의 업무를 수행하는 전자금융방식
5) 예금계좌와 연결된 전자우편 주소(기타 전화번호)를 통해 자금이체 등의 업무를 수행하는 전자금융방식

* 전자자금이체시 제34조 및 제37조의 규정에서 정한 사항을 준수하여야 한다.

다. 직불전자지급수단 이용한도

(단위 : 만원)

구 분	1회 이용한도	1일 이용한도
직불전자지급수단	10000	10000
실명증표확인 외의 본인확인수단을 이용하여 발급된 직불전자지급수단	200	200

11. 약관교부 방법 및 관련 보고

〈 감독규정 〉

제40조(약관교부 방법 등) ① 전자금융업무를 수행하는 금융회사 및 전자금융업자는 전자금융거래와 관련한 약관(이하 "약관"이라 한다)을 별도로 마련하여야 한다.

② 금융회사 또는 전자금융업자는 이용자와 전자금융거래의 계약을 체결함에 있어 이용자의 요청이 있는 경우 전자문서의 전송(전자우편을 이용한 전송을 포함한다), 모사전송, 우편 또는 직접 교부의 방식으로 전자금융거래 약관의 사본을 이용자에게 교부하여야 한다.

③ 금융회사 또는 전자금융업자는 이용자와 전자금융거래의 계약을 체결함에 있어 이용자가 약관의 내용에 대한 설명을 요청하는 경우 다음 각 호의 어느 하나의 방법으로 이용자에게 약관의 중요내용을 설명하여야 한다.

1. 약관의 중요내용을 이용자에게 직접 설명
2. 약관의 중요내용에 대한 설명을 전자적 장치를 통하여 이용자가 알기 쉽게 표시하고 이용자로부터 해당 내용을 충분히 인지하였다는 의사표시를 전자적 장치를 통하여 수령

④ 금융회사 또는 전자금융업자는 약관을 변경하는 때에는 그 시행일 1월 전에 변경되는 약관을 해당 전자금융거래를 수행하는 전자적 장치(해당 전자적 장치에 게시하기 어려울 경우에는 이용자가 접근하기 용이한 전자적 장치로서 당해 금융회사등이 지정하는 대체장치를 포함한다. 이하 이 조에서 같다)에 게시하고 이용자에게 통지하여야 한다. 다만, 이용자가 이의를 제기할 경우 금융회사 또는 전자금융업자는 이용자에게 적절한 방법으로 약관 변경내용을 통지하였음을 확인해 주어야 한다.

⑤ 금융회사 또는 전자금융업자가 법령의 개정으로 인하여 긴급하게 약관을 변경한 때에는 변경된 약관을 전자적 장치에 최소 1월 이상 게시하고 이용자에게 통지하여야 한다.

제41조(약관 제정 또는 변경에 따른 보고 등) ① 법 제25조제1항 단서에서 "금융위원회가 정하는 경우"란 다음 각 호와 같다.

1. 이용자의 권익을 확대하거나 의무를 축소하기 위한 약관의 변경
2. 금융감독원장에게 보고된 약관의 내용과 동일하거나 유사한 약관의 제정 또는 변경
3. 그 밖에 이용자의 권익이나 의무에 불리한 영향이 없는 경우로서 금융감독원장이 정하는 약관의 제정 또는 변경

② 금융회사 또는 전자금융업자가 전자금융거래 약관을 제정 또는 변경하고자 하는 경우에는 해당 약관 및 약관내용을 이해하는데 필요한 관련서류를 시행예정일 45일 전까지 금융감독원장에게 제출하여야 한다. 이 경우 약관 및 관련서류는 전자문서로 제출할 수 있다.

③ 금융감독원장은 제2항의 규정에 따라 제출받은 약관을 심사하고 건전한 금융거래질서의 유지를 위하여 약관내용의 변경이 필요하다고 인정하는 경우 해당 금융회사 또는 전자금융업자에 대하여 약관의 변경을 권고할 수 있다.
④ 제3항의 규정에 따라 변경권고를 받은 금융회사 또는 전자금융업자는 권고의 수락여부를 금융감독원장에게 보고하여야 한다.

▣ 전자금융거래와 관련한 약관 교부방법 및 약관제정 또는 변경에 따른 보고 사항들을 상세히 규정하여 이용자를 보호함

▣ 해설

- 전자금융업무를 수행하는 금융회사 또는 전자금융업자는 전자금융거래와 관련한 별도의 약관을 마련하여 이용자의 요청이 있을 경우 전자문서의 전송, 모사전송(FAX), 우편 또는 직접교부 방식으로 전자금융거래 약관의 사본을 이용자에게 교부하여야 함

- 이용자가 약관의 내용에 대한 설명을 요청할 경우 중요 내용을 직접 설명하거나 또는 전자적 장치를 통하여 이용자가 알기 쉽게 표시하고 이용자로부터 해당 내용을 충분히 인지하였다는 의사표시를 전자적 장치를 통하여 수령*하여야 함

  * 금융회사 및 전자금융업자는 이용자에게 pop-up창을 띄우거나 이메일 통지를 통한 전자서명 동의방식, 기타 인터넷창에서 동의 의사표시를 직접 받을 수 있음

- 금융회사와 전자금융업자는 약관 변경시 그 시행일 1월전에 금융위가 정한 방법에 따라 게시하고 이용자에게 통보를 의무화

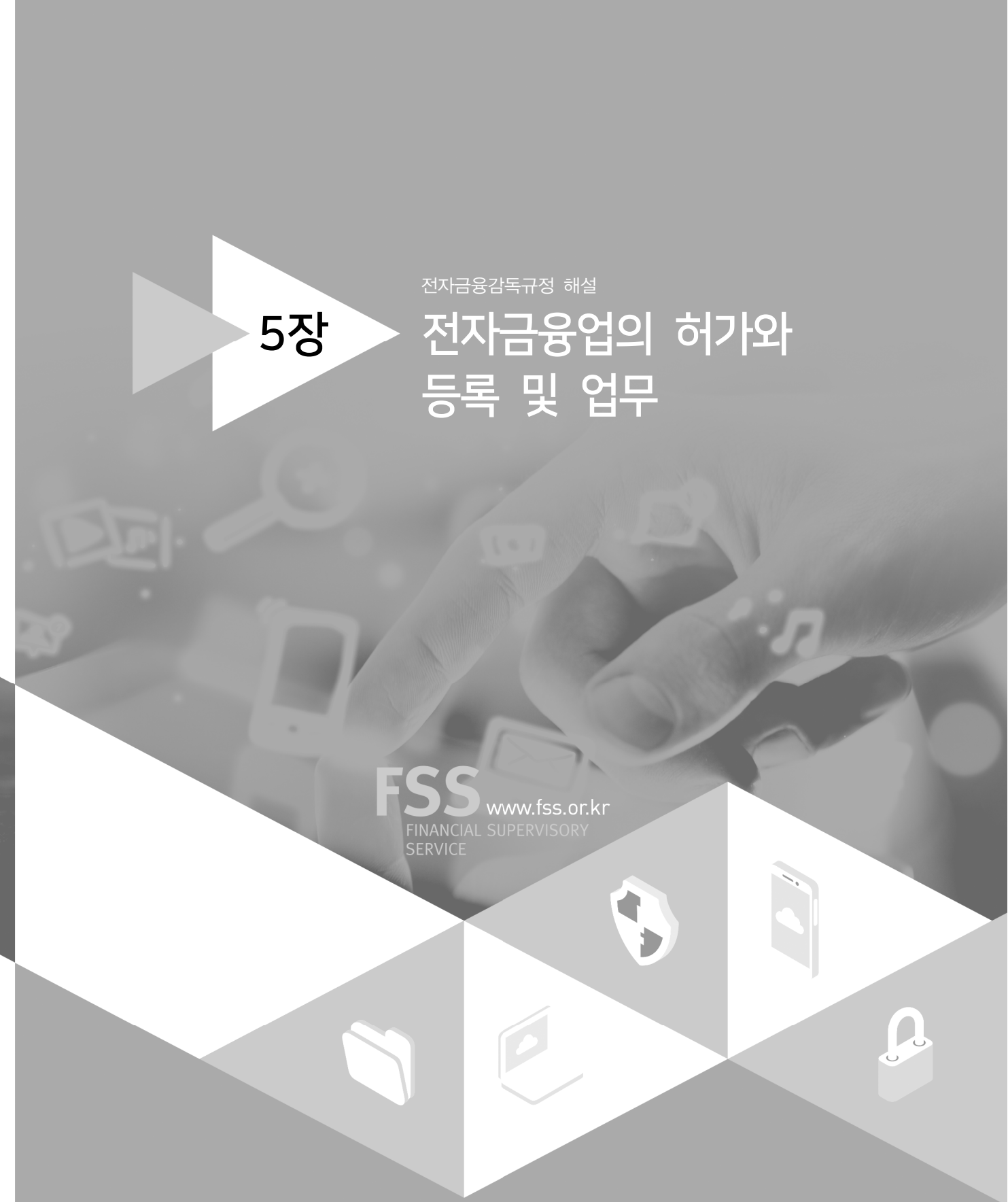
  – 다만, 변경내용의 게시나 통지사실에 관해 이용자가 이의를 제기할 경우 금융회사 또는 전자금융업자는 변경내용 게시·통지사실에 관해 입증하여야 함(※ 입증하지 못할 경우 약관 변경효력이 없음)

- 금융회사와 전자금융업자는 약관 제정·변경시 약관 시행예정일 45일 전까지 관련 서류를 감독원장에게 제출하여야 함

  – 감독원장은 제출받은 약관을 심사하고 약관변경이 필요하다고 판단한 경우 해당 금융회사 또는 전자금융업자에 약관변경을 권고할 수 있으며, 해당 기관은 변경권고 수락여부를 보고해야 함

전자금융감독규정 해설

5장 전자금융업의 허가와 등록 및 업무



FSS www.fss.or.kr
FINANCIAL SUPERVISORY SERVICE

제5장 전자금융업의 허가와 등록 및 업무

1. 개요

▣ 이용자 보호 및 전자금융거래의 안정성 확보를 위해 전자금융업 영위시 허가와 등록을 의무화하고 있으며, 영위할 업종에 따라 허가와 등록 대상을 구별하고 있음

- 전자금융업 영위기관이 금융회사인 경우 전자금융업종에 따라 일부 허가 또는 등록을 면제받을 수 있으며, 선불전자지급수단의 발행 및 관리업의 경우 미상환잔액의 규모 및 사용되는 범위 등이 일정규모 이하일 경우 등록을 면제하고 있음

▣ 미허가 및 미등록 영업시 벌금 등의 처벌을 통해 허가 및 등록을 강제

※ 미허가 또는 미등록 영업시 3년 이하의 징역 또는 2천만원 이하의 벌금에 처할 수 있음(법 제49조제4항제5호)

2. 허가 대상 업무 및 면제요건

가. 법령상 근거

▣ 전자화폐의 발행 및 관리업무를 행하고자 하는 자는 금융위원회의 허가를 받아야 함 (법 제28조)

나. 법 및 시행령 해설내용

▣ 법에서는 전자화폐의 발행 및 관리 업무를 수행하고자 하는 경우 금융위원회의 허가를 받도록 하는 한편,

- 은행법상 금융회사 등 특정 금융회사에 대해 허가를 면제하고 있음

▣ 전자화폐 발행 및 관리업 허가면제 금융회사

- 은행법에 따른 금융회사(은행)
- 우체국예금·보험에 관한 법률에 따른 체신관서
- 새마을금고법에 따른 새마을금고 및 새마을금고연합회
- 상호저축은행 및 중앙회, 신용협동조합 및 중앙회, 농업협동조합중앙회의 신용사업부문, 수산업협동조합중앙회의 신용사업부문
- 여신전문금융업법에 따른 여신전문금융회사 중 신용카드사업자
- 한국산업은행, 한국정책금융공사, 중소기업은행, 한국수출입은행, 산림조합 및 중앙회의 신용사업부문, 농업협동조합, 수산업협동조합

제1절 허가 및 등록의 대상과 절차

1. 총발행잔액의 산정방법 등

〈 감독규정 〉

제42조(총발행잔액의 산정방법 등) ① 시행령 제15조제5항에 따른 선불전자지급수단 발행 시 총발행잔액은 등록신청일이 속하는 사업연도의 직전 사업연도 1분기(직전 사업연도 1분기말 이후에 사업을 개시한 경우에는 사업개시한 날이 속하는 분기를 말한다)부터 등록신청일 직전 분기까지 각 분기말 미상환 발행잔액의 단순평균으로 한다. 다만, 사업기간이 3월 미만인 경우에는 등록신청일 직전 월말 미상환 발행잔액으로 한다.

② 법 제28조제3항제1호다목에 따라 금융위원회에 등록하지 아니하고 선불전자지급수단을 발행하는 자는 매분기말 기준으로 선불전자지급수단의 미상환잔액을 평가하여 이를 시행령 제15조제6항에 따른 지급보증, 상환보증보험 또는 공제에 반영하여야 한다.

제42조의2(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.

〈 시행세칙 〉

제8조의3(거래금액 기준 초과시 신고 등) ① 법 제30조제3항제1호에 해당하는 전자금융업자는 분기별 거래총액(결제대행금액, 결제대금예치금액 또는 전자고지결제금액)이 규정 제42조의2제1항에 따른 거래금액 기준을 초과한 경우 해당 분기 종료 후 45일 이내에 별지 제5호 서식에 따라 감독원장에게 초과 내역 및 자본금 증액 계획을 신고하여야 한다.

② 제1항에 따른 신고를 마친 자는 법 제30조제4항에 따른 자본금 요건을 갖춘 후, 신고한 때부터 6개월 이내에 자본금 납입 증명서류 등 관련 서류를 감독원장에게 제출하여야 한다.

※ 관계 법령

〈 법 〉

제30조(자본금) ①~② (생략)

③제28조제2항제4호·제5호 및 제29조의 규정에 따라 등록할 수 있는 자는 「상법」제170조에서 정한 회사 또는 「민법」제32조에서 정한 법인으로서 업무의 종류별로 자본금·출자총액 또는 기본재산이 다음 각 호의 구분에 따른 금액 이상이어야 한다.

1. 분기별 전자금융거래 총액이 30억원 이하의 범위에서 금융위원회가 정하는 기준 이하로 운영하고자 하는 자(제29조에 따라 등록을 하고자 하는 자는 제외한다): 3억원 이상으로 대통령령으로 정하는 금액
2. 제1호 외의 자: 5억원 이상으로 대통령령으로 정하는 금액

④ 제3항제1호에 해당하는 자가 제28조에 따라 등록을 한 후 2분기 이상 계속하여 제3항제1호의 금융위원회가 정하는 기준을 초과하는 경우에는 그 내용을 금융위원회에 신고하고 금융위원회가 정하는 기한 내에 제3항제2호에서 정하는 자본금요건을 갖추어야 한다.

▣ 개정된 전자금융거래법은 핀테크 활성화를 위해 소규모 전자금융업자에 대해서는 등록 자본금을 완화

▣ 해설

- 소규모 전자금융업자로 등록한 후 2분기 이상 연속하여 기준 초과시에는 6개월 내에 자본금을 증액하여야 함('16.3.29. 법개정)

2. 허가등 절차의 구분

〈 감독규정 〉

제43조(허가등 절차의 구분) 다음 각 호의 허가 또는 인가(이하 "허가등"이라 한다)의 절차는 허가등 사항에 대한 사전심사 및 확실한 실행을 위하여 허가등의 이전에 예비적으로 행하는 의사표시(이하 "예비허가등"이라 한다)와 허가등으로 구분한다.

1. 법 제28조제1항의 규정에 의한 전자화폐의 발행 및 관리 업무의 허가
2. 법 제45조에 의한 합병 등의 인가

3. 예비허가 등

〈 감독규정 〉

제44조(예비허가등) ① 예비허가등을 신청하고자 하는 자는 금융감독원장이 정하는 바에 따라 〈별지 제3호 서식〉에 따른 관련 신청서 및 첨부서류를 금융위원회에 제출하여야 한다.

② 금융위원회는 예비허가등의 심사를 위하여 필요하다고 인정하는 때에는 예비허가등의 신청에 대하여 이해관계인의 의견을 요청할 수 있고, 금융시장에 중대한 영향을 미칠 우려가 있다고 판단되는 경우 공청회를 개최할 수 있다.

③ 금융위원회는 제2항의 규정에 의하여 접수된 의견 중 신청인에게 불리한 의견에 대하여는 신청인에게 소명하도록 기한을 정하여 통보할 수 있다.

④ 금융감독원장은 예비허가등의 신청내용에 대한 진위여부를 확인하고 이해관계인, 일반인 및 관계기관 등으로부터 제시된 의견을 감안하여 신청내용이 관련 법령과 이 장 제2절에서 규정하는 허가등 세부기준에 부합되는지 여부를 심사하여야 한다.

⑤ 금융감독원장은 사업계획의 타당성을 평가하기 위하여 평가위원회를 구성·운영할 수 있으며 신청내용의 확인, 발기인 및 경영진과의 면담 등을 위하여 실지조사를 실시할 수 있다.

⑥ 금융위원회는 예비허가등의 신청에 대하여 관련 법령과 이 장 제2절에서 규정하는 허가의 세부기준을 감안하여 예비허가등의 여부를 결정한다.

⑦ 금융위원회는 예비허가등 시에 조건을 붙일 수 있으며 예비허가등을 거부하는 경우 이를 서면으로 신청인에게 통보하여야 한다.

⑧ 금융위원회는 합병, 영업양도 등 구조조정 및 이용자보호 등을 위하여 신속한 처리가 필요하거나 예비허가등의 신청 시 허가등의 요건을 갖추었다고 판단되는 때에는 예비허가등의 절차를 생략할 수 있다.

4. 허가 등

〈 감독규정 〉

제45조(허가등) ① 신청인은 예비허가등의 내용 및 조건을 이행한 후 금융감독원장이 정하는 바에 따라 〈별지 제4호 서식〉에 따른 관련 신청서 및 첨부서류를 금융위원회에 제출하여야 한다.

② 금융위원회는 허가등의 신청에 대하여 관련 법령과 이 장 제2절에서 규정하는 허가의 세부기준에 따라 심사하여 허가여부를 결정한다.

③ 허가등에는 조건을 붙일 수 있으며 허가를 거부하는 경우에는 이를 서면으로 신청인에게 통보하여야 한다.

④ 금융위원회는 예비허가등의 내용 및 조건의 이행여부를 확인하기 위하여 실지조사를 실시할 수 있으며, 신청인은 이에 적극 협조하여야 한다.

⑤ 신청인은 예비허가등 또는 허가등 시에 부과된 조건이 있는 경우 그 이행상황을 이행기일 경과 후 지체 없이 금융위원회에 보고하여야 한다.

제46조(보완서류 등의 제출) 금융위원회는 예비허가등 또는 허가등의 심사 시 보완서류 등의 추가자료가 필요한 경우 신청인에게 기한을 정하여 그 자료의 제출을 요구할 수 있다.

제47조(허가등 사실의 공고) 금융위원회는 허가등의 신청을 승인한 경우에는 지체 없이 그 내용을 관보에 공고하고 인터넷 등을 이용하여 일반인들에게 알려야 한다.

▣ 허가 또는 인가(이하 “허가등” 이라함)의 절차는 허가등 사항에 대한 사전심사 및 확실한 실행을 위하여 허가 등의 이전에 예비적으로 행하는 의사표시(이하 “예비허가등” 이라함)와 허가등으로 절차를 구분하고 있음

- 신청인은 예비허가 등의 내용 및 조건을 이행한 후 허가 등 신청서 및 첨부서류를 금융위에 제출하여 심사를 받음

▣ 해설

- 예비허가 및 예비인가제도
  - 허가 및 인가에 있어 신청인의 예측가능성을 제고하고 행정의 효율성을 확보하기 위해 사전 인·허가 제도를 도입하여 신청인의 편익을 도모하고자 함
- 예비허가 및 예비인가 대상(전자화폐발행 및 관리업에 한함)
  - 전자화폐발행 및 관리업무의 허가
  - 전자화폐발행 및 관리업자의 다른 금융회사 또는 및 전자금융업자와의 합병 인가
  - 전자화폐발행 및 관리업의 해산 또는 전자금융업무의 폐지인가

- 전자화폐발행 및 관리업 전부 또는 일부의 양도와 양수 인가

● 금융위는 허가의 세부기준에 따라 심사하여 허가여부를 결정

- 허가 등에는 조건을 붙일 수 있으며, 허가를 거부할 경우에는 반드시 서면으로 신청인에게 통보하여야 함
- 금융위는 예비허가 등의 내용 및 조건의 이행여부를 확인하기 위해 실지조사를 실시할 수 있음

● 금융위는 예비허가 등 또는 허가 등의 심사시 보완서류 등의 추가자료가 필요한 경우 신청인에게 기한을 정하여 그 자료의 제출을 요구할 수 있고,

- 허가 등의 신청을 승인할 경우에는 지체없이 그 내용을 관보에 공고하여 일반인에게 알려야 함

5. 등록

〈 감독규정 〉

제48조(등록) ① 법 제28조 및 제29조에 따라 등록을 신청하고자 하는 자는 금융감독원장이 정하는 바에 따라 〈별지 제5호 서식〉에 따른 등록신청서를 금융감독원에 제출하여야 하며 금융감독원장은 등록신청일로부터 20일 이내에 서면으로 등록여부를 통지한다. 다만, 제3항의 실지조사에 걸린 기간은 통지기간에 산입하지 아니한다.

② 금융감독원장은 신청인의 등록 신청에 대하여 이 장 제2절의 심사기준에 따라 등록 여부를 결정한다.

③ 금융감독원장은 등록의 내용 및 조건의 이행여부를 확인하기 위한 실지조사를 실시할 수 있다.

④ 금융감독원장은 등록 신청을 수리한 경우에는 지체 없이 그 내용을 관보에 공고하고 인터넷 등을 이용하여 일반인들에게 알려야 한다.

▣ 등록 신청인은 등록신청서를 금융감독원에 제출하여야 하며 감독원장은 등록신청일로부터 20일 이내에 서면으로 등록여부를 통지함

▣ 해설

● 감독원장은 신청인의 등록 신청에 대하여 자본금, 재무건전성 및 인적·물적 요건 등의 심사기준에 따라 등록 여부를 결정

● 감독원장은 등록의 내용 및 조건의 이행여부를 확인하기 위한 실지조사를 실시할 수 있고, 등록을 완료한 경우에는 지체 없이 그 내용을 관보에 공고 및 인터넷 등을 이용하여 일반인들에게 알려야 함

6. 기재가 생략되는 출자자의 범위

〈 감독규정 〉

제49조(기재가 생략되는 출자자의 범위) 시행령 제20조제1항제3호에서 "금융위원회가 정하여 고시하는 소액출자자"라 함은 허가 또는 등록대상 전자금융업자가 되고자 하는 법인의 의결권 있는 발행주식총수의 100분의 1 이하의 주식을 소유하는 자를 말한다.

〈참고〉 **전자금융업 등록 관련 절차**

1. **등록 협의** : 방문 또는 유선으로 등록업무 상담

2. **등록 신청** : 금융감독원에 신청서 제출

3. **등록 심사** : 등록신청(접수)일 기준 20일 이내 여부통보
   - 서류 심사 : 제출서류 심사
   - 실지 조사 : 등록신청업체 현지 조사
   - 신원 조회 : 신청인 및 대주주 등에 대한 결격사유 조회
   - 보완 요청 : 등록신청일 기준 10일 이내 등록관련 서류 보완요청

4. **등록 완료**
   - 등록완료통보 : 등록신청 업체 공문발송(우편)
   - 관보공고요청 : 행자부에 관보공고 요청
   - 홈페이지공고 : 홈페이지에 등록사실 공고

제2절 허가 및 등록의 세부요건

1. 인력 및 물적 시설 세부요건

〈 감독규정 〉

제50조(인력 및 물적 시설 세부요건) ① 법 제28조 및 제29조에 따라 허가를 받거나 등록을 하고자 하는 자는 인력과 물적 시설에 대한 다음 각 호의 요건을 모두 갖추어야 한다.

1. 신청 당시 전산업무 종사 경력이 2년 이상인 임직원을 5명 이상 확보하고 있거나 허가·등록 시점에 확보 가능할 것
2. 전자금융업을 원활히 영위하는데 필요한 전산기기를 보유할 것
3. 전산장애 발생 시 전산자료 손실에 대비한 백업(backup)장치를 구비할 것
4. 전자금융업의 원활한 영위를 위한 각종 프로그램을 보유할 것
5. 전산자료 보호 등을 위한 적절한 정보처리시스템 관리방안을 확보하고 정보보호시스템 등 감시운영체제를 구축할 것
6. 전산실 등의 구조 및 내장, 설비 등의 안전성을 확보하고 적절한 보안대책을 수립할 것

② 국외에서 주로 영업하는 국외 사이버몰(" 국외 사이버몰" 이란 컴퓨터 등과 정보통신설비를 이용하여 재화 등을 거래할 수 있도록 설정된 가상의 영업장으로서 운용자의 사무소가 국외에 있는 경우를 말한다. 이하 같다)에서의 상거래에 수반한 전자지급결제대행업을 영위할 목적으로 전자금융업을 등록하고자 하는 자는 제50조제1항의 규정에도 불구하고 다음 각 호의 요건을 모두 충족한 경우 등록할 수 있다.

1. 국외에 소재한 계열사(「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」 제2조제3항의 "계열사"를 말한다. 이하 같다)와 이용계약을 체결하였고, 계열사의 인력 및 물적 시설이 제50조제1항 각 호의 세부요건을 충족할 것
2. 제1호의 규정에도 불구하고 전자금융업을 등록하고자 하는 자는 신청 당시 법령 준수업무와 이용자 민원처리업무를 담당할 3명 이상의 임직원(전산업무 종사 경력이 2년 이상인 임직원 1명을 포함하여야 한다)은 직접 확보하고 있거나 등록시점에 확보 가능할 것
3. 신청 당시 계열사의 인력 또는 물적시설을 통해 5개국 이상의 국가에서 전자지급결제대행업무가 수행되고 있을 것

③ 제2항에 따라 등록을 하려는 자가 계열사의 인력 또는 물적시설의 이용계약을 체결하는 경우에는 「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」을 적용한다. 다만, 동 규정의 제7조는 적용하지 아니한다.

▣ 전자금융업의 원활한 수행을 위해 필요한 최소한의 인적/물적 시설요건을 규정함

전자금융업 물적 설비 현황 점검리스트(참고)

항 목	제출서류
1. 전자금융업을 원활히 영위하는데 필요한 전산기기 보유	
① 전자금융업을 원활히 영위하는데 필요한 주전산기기, 어플리케이션 서버, DB서버, 웹서버, 저장장치 및 출력장치 등 보유	전산기기 목록
② 대외 금융회사, 가맹점 또는 지점 등과 자료의 송·수신 등을 위한 통신제어장치, 통신서버, 통신회선 등 전자금융업무를 지원하기 위한 내·외부 통신망 구축	통신기기 목록
2. 전산장애 발생시 전산자료 손실에 대비한 백업장치 구비	
① 백업장치를 구비하고 중요도에 따라 프로그램, 데이터, 로그 등 전산자료를 정기백업 및 안전지역에 소산	백업계획서
② 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템 마비 방지, 자료 손실 방지 및 신속한 복구를 위한 비상대책 수립	비상계획서
③ 중앙 처리장치, 데이터저장장치 등 주요 전산장비 및 통신망에 대하여 이중화 또는 예비 장치를 확보	주요 전산장비·통신회선 등의 이중화 구성도
3. 전자금융업의 원활한 영위를 위한 각종 프로그램 보유	
① 주요 업무별·기능별 각종 프로그램을 보유	프로그램 보유 현황
② 프로그램 등록·변경·폐기 시 통제방안 마련	프로그램 등록·변경·폐기 절차
4. 전산자료 보호 등을 위한 정보처리시스템 관리방안 확보	
① 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기 등에 관하여 체계적으로 관리(외부사용자에게 사용자계정을 부여하는 경우 적절한 통제장치 마련)	계정·비밀번호 부여 절차 및 관리현황
② 담당업무에 따른 전산자료의 입력·출력·열람 등 접근권한 통제	전산자료 접근 권한 부여절차 및 관리현황
③ 전산자료 및 전산장비의 반출·입 통제	전산자료 반출·입 관리 대장
④ 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용을 금지(불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제)	전산개발 규정
⑤ 단말기를 통한 이용자정보 조회시 사용자, 사용일시, 변경 또는 조회내용, 접속방법 등이 정보처리시스템에 자동 기록되도록 하고, 그 기록을 1년 이상 보존	자동 기록된 내용의 샘플자료
⑥ 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망 사이의 독립된 통신망(DMZ)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호	DMZ을 포함한 네트워크 구성도
⑦ 공개용 서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가인증 수단을 적용	웹서버 계정부여 현황, 추가인증 수단 현황

항 목	제출서류
⑧ 개인정보의 유출, 위·변조 방지를 위한 보안조치	개인정보 보유현황, 정보유출 방지 대책
⑨ 공개용 웹서버가 해킹공격에 노출되지 않도록 취약점에 대하여 적절한 대응조치 강구	취약점에 대한 점검 및 대응현황
5. 정보보호시스템 등 감시운영체제 구축	
① 전산자료 보호 등을 위한 적절한 정보처리시스템 관리방안을 확보하고 정보보호시스템 등 감시운영체제를 구축	정보보호시스템 (침입차단시스템, 침입탐지시스템, VPN 등)구축 현황
② 내부통신망과 연결된 내부 업무용시스템 및 정보처리시스템은 인터넷 등 외부통신망과 분리·차단 및 접속금지	망분리 현황
③ 악성코드 감염 방지대책 마련	악성코드 감염 방지 프로그램 현황 및 복구 절차서
6. 전산실 안전성 확보 및 적절한 보안대책 수립	
① UPS, 항온항습기, 자가발전설비, 자동소화설비, 접지 시설 등 안정적인 전산실 운영에 필요한 기본 설비 확보	전산실 설비 목록
② 화재·수해 등의 재해 및 외부로부터의 위해 방지대책 수립·운용	비상대책
③ 전산실, 전산자료보관실, 정보보호시스템 설치장소 등 보안관리가 필요한 정보처리시스템 설치장소를 보호구역 설정	보호구역 지정 현황
④ 전산실 출입문은 한 곳으로 정하며 상시출입은 업무와 직접 관련이 있는 자에 한하여 허용하고, 그 밖의 출입자에 대하여는 관리책임자의 승인을 받아 출입하도록 하며 출입자 관리기록부 기록·보관	전산실 출입자 관리기록부
⑤ 전산실의 규모, 설치장소 등을 감안하여 무인감시카메라 또는 출입자동기록시스템을 설치하여 사후확인이 가능하도록 조치	출입자 감시장치 운영현황
⑥ 전산실 출입문은 2중 안전장치로 보호하며 외벽이 유리인 경우 유리창문을 통하여 접근할 수 없도록 조치	전산실 배치도

2. 국외 사이버몰을 위한 전자지급결제대행업

〈 감독규정 〉

제50조의2(국외 사이버몰을 위한 전자지급결제대행업) ① 제50조제2항에 따라 등록하고자 하는 경우 시행령 제20조제2항제8호에 따라 다음 각 호의 서류를 제출하여야 한다.

1. 「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」 제7조제1항 각 호의 서류
2. 등록신청자 및 계열사의 수탁업무 수행 과정에서의 법·시행령 및 이 규정 등 준수에 대한 확약서
3. 신청 시점에 전자지급결제대행업무를 수행하고자 하는 국외 사이버몰에 대한 다음 각 목의 사항(해당 국가의 법령 등에서 이와 유사한 것으로 인정되는 사항을 포함한다)을 기재한 서류
   가. 「전자상거래 등에서의 소비자보호에 관한 법률」 제10조제1항 각 호의 서류
   나. 신청일 직전연도에 사이버몰에서 체결된 전자상거래 중 국내에 소재한 소비자와 사업자 간 거래의 비중

② 제50조제2항에 따라 등록을 한 자는 국외에서 주로 영업하는 국외 사이버몰을 통한 상거래에 대해서만 전자지급결제대행업을 영위하여야 한다.

③ 금융감독원장은 국외에서 주로 영업하는 국외 사이버몰의 판단기준 등 필요한 사항을 정할 수 있다.

〈 시행세칙 〉

제8조의2(국외에서 주로 영업하는 국외 사이버몰의 판단기준) 규정 제50조의2제3항에 따라 감독원장은 국외에서 주로 영업하는 국외 사이버몰을 판단하는데 있어 다음 각 호의 사항 등을 고려한다.

1. 사이버몰 운용자의 사무소, 인적·물적 시설의 소재지
2. 사이버몰에서 이루어지는 상거래 대상 국가의 수
3. 사이버몰에 대한 국외 감독당국, 규제기관의 감독·규제여부
4. 사이버몰에서 체결된 전자상거래 중 국내에 소재한 소비자와 사업자간 거래의 비중
5. 규정 제50조의2제2항에 따른 제한을 회피하기 위한 사이버몰 여부

3. 재무건전성 세부기준 및 계산방법

〈 감독규정 〉

제51조(재무건전성 세부기준 및 계산방법 등) ① 시행령 제18조제1항 및 제2항에 따라 금융위원회가 정하는 재무건전성 기준은 다음 각 호와 같다.

1. 시행령 제18조제1항의 규정에 따른 기관 중 「금융산업의 구조개선에 관한 법률」 제2조제1호의 금융회사에 해당하는 기관은 그 기관의 설립·운영 등에 관한 법령상 경영개선권고, 경영개선요구 또는 경영개선명령 등의 요건이 되는 재무기준에 해당하지 아니할 것
2. 제1호 이외의 경우에는 다음 각 목의 요건을 충족할 것
   가. 시행령 제18조제1항의 규정에 따른 금융회사 중 「금융산업의 구조개선에 관한 법률」 제2조제1호의 금융회사에 해당하지 않는 기관은 자기자본 대비 부채총액의 비율이 100분의 200 이내일 것. 다만, 금융회사 업무의 성격 및 재무 구조 등을 감안할 때 부채비율 기준을 적용하지 아니하고, 「금융산업의 구조 개선에 관한 법률」 제2조제1호 각 목 중 어느 하나의 금융회사(이하 "기준 금융회사"라 한다)의 재무건전성 기준을 적용하는 것이 적절하다고 금융위원회가 승인하는 경우에는, 기준 금융회사의

설립, 운영 등에 관한 법령에 따라 산출한 재무 비율이 같은 법령상의 경영개선권고, 경영개선요구 또는 경영개선명령 등의 요건이 되는 기준에 해당하지 아니할 것

나. 법 제28조제1항에 따른 허가대상 전자금융업일 경우에는 자기자본 대비 부채총액의 비율이 100분의 180 이내일 것

다. 법 제28조제2항 및 제29조에 따른 등록대상 전자금융업일 경우에는 자기자본·출자총액 또는 기본재산 대비 부채총액의 비율이 100분의 200 이내일 것

② 제1항제2호의 부채비율은 신청일이 속하는 사업연도의 직전 사업연도말 대차대조표(최근 대차대조표를 사용하고자 하는 경우에는 신청일 최근 분기말 대차대조표 또는 회계법인의 확인을 받은 신청일 최근 대차대조표) 상의 자기자본 및 부채총액을 이용하여 산출한다. 이 경우 전자화폐·선불전자지급수단의 미상환잔액 및 전자자금이체·전자지급결제대행·결제대금예치·전자고지결제·「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스 등의 업무를 영위하는 자가 이용자와의 거래 관계에서 일시 보관하는 금액(이하 "미정산 잔액"이라 한다)은 부채총액에서 차감한다.

③ 제1항에도 불구하고 다음 각 호의 요건을 갖춘 신청인의 재무건전성 기준은 자기자본 대비 부채총액의 비율이 100분의 1500 이내일 것으로 한다.

1. 정부등이 자본금·출자총액 또는 기본재산의 100분의 10 이상을 소유하고 있거나 출자하고 있을 것
2. 신청인의 사업 수행이 곤란하게 되는 경우 정부등이 해당 사업을 인수할 것을 확약하는 등 그 사업의 연속성에 대하여 정부등이 보장하고 있을 것
3. 사업 개시 후 5년 이내 제1항의 재무건전성 기준을 충족하는 것을 내용으로 하는 실현가능한 재무구조 개선계획을 수립하여 관련서류와 함께 제출할 것

▣ 감독규정은 법 및 시행령의 위임을 받아 재무건전성 기준을 구체적으로 정하고 있음

▣ 해설

가) 재무건전성 요건

● 금융감독원의 검사 대상기관

– 「금융산업의 구조개선에 관한 법률」 제2조제1호의 금융회사*에 해당하는 기관(적기시정조치 적용 대상 금융회사)은 그 기관의 설립·운영 등에 관한 법령상 경영개선권고, 경영개선요구 또는 경영개선명령 등의 요건이 되는 재무기준에 해당하지 아니하여야 하며,

* 은행, 중소기업은행, 투자매매업자·투자중개업자, 집합투자업자, 투자자문업자·투자일임업자, 보험회사, 상호저축은행, 신탁업자, 종금사, 금융지주회사, 여신전문금융회사, 주택저당채권유동화회사

– 「금융산업의 구조개선에 관한 법률」 제2조제1호의 금융회사에 해당하지 않는 기관(적기시정조치 미적용 대상 금융회사)은 자기자본 대비 부채총액의 비율이 200% 이내이어야 함

다만, 적기시정조치 대상이 아닌 금융회사에 대해, 금융위가 승인하는 경우 동 부채비율(200% 이내)을 적용하지 않고 해당 금융회사의 설립, 운영 등에 관한 법률에 따라 산출한 재무비율이 동법상의 적기시정조치 기준에 해당하지 않으면 재무건전성 요건은 충족한 것으로 간주

- 검사 대상기관이 아닌 경우
  - 허가대상 전자금융업(전자화폐의 발행 및 관리업)의 경우 부채비율이 180%이내이어야 하고, 그 외 등록대상 전자금융업의 경우 부채비율이 200%이내이어야 함

나) 부채비율에 관한 특례

- 정부 관련 사업에 있어 이용자 보호 및 거래안전 확보를 위한 다음 요건을 모두 갖춘 경우 부채비율이 1,500%이하이면 등록을 허용
  - 정부 등(지자체 포함)이 자본금·출자총액 또는 기본재산의 100분의 10 이상을 소유하고 있거나 출자하고 있을 것
  - 신청인의 사업 수행이 곤란하게 되는 경우 정부 등이 해당 사업을 인수할 것을 확약하는 등 그 사업의 연속성에 대하여 정부 등이 보장하고 있을 것
  - 사업 개시 후 5년 이내 해당 전자금융업이 요구하고 있는 재무건전성 기준을 충족하는 것을 내용으로 하는 실현가능한 재무구조개선계획을 수립하여 관련서류와 함께 제출할 것

다) 부채비율의 산정방식 및 산정시점

- 산정방식
  - 부채비율은 자기자본(기본재산 또는 출자총액) 대비 부채총액으로서, 전자화폐·선불전자지급수단의 미상환잔액 및 전자자금이체·전자지불결제대행·결제대금예치·전자고지결제 등의 업무를 영위하는 자가 이용자와의 거래 관계에서 일시 보관하는 금액은 부채총액에서 차감하여 산정
- 산정시점
  - 원칙적으로 신청일이 속하는 사업연도의 직전 사업연도말 대차대조표를 기준으로 하되, 신청일 최근 분기말 대차대조표(또는 재무상태표, 이하 동일)도 사용할 수 있으며, 회계법인의 확인을 받은 경우 신청일 최근 월말 대차대조표를 기준으로 할 수 있음

4. 사업계획에 관한 요건

〈 감독규정 〉

제52조(사업계획에 관한 요건) 법 제28조에 따라 허가를 받고자 하는 자의 사업계획은 다음 각 호의 요건을 모두 갖추어야 한다.

1. 영업개시 후 3년간 추정재무제표 및 수익전망이 전자화폐 내지 선불전자지급수단 발행업계의 과거 수익상황 등에 비추어 타당성이 있고 그 내용이 해당 신청회사의 영업계획에 부합할 것
2. 전자화폐 발행업을 원활히 영위하는데 필요한 이용자 확보계획이 구체적이고 타당하며 실현가능성이 있을 것
3. 영위하고자 하는 영업의 내용이 법령에 위반되지 아니하고 투자자보호나 건전한 금융질서를 저해할 우려가 없을 것

▣ 허가대상 업무인 전자화폐의 발행 및 관리업의 경우 이용자 보호 필요성에 따라 업무의 연속성, 안정성을 확보할 수 있는 보장 장치가 필요한 바,

허가시 사업계획에 관해 신청인의 수익전망, 이용자 확보 계획 및 투자자 보호 가능성에 대한 심사를 의무화

▣ 해설

● 사업계획에 관한 요건

- 영업개시 후 3년간 추정재무제표 및 수익전망이 전자화폐 내지 선불전자지급수단 발행업계의 과거 수익상황 등에 비추어 타당성이 있고 그 내용이 해당 신청회사의 영업계획에 부합할 것
- 전자화폐 발행업을 원활히 영위하는데 필요한 이용자 확보계획이 구체적이고 타당하며 실현가능성이 있을 것
- 영위하고자 하는 영업의 내용이 법령에 위반되지 아니하고 투자자보호나 건전한 금융질서를 저해할 우려가 없을 것

5. 주요출자자에 관한 요건

〈 감독규정 〉

제53조(주요출자자에 관한 요건) 주요출자자(시행령 제18조제3항에 따른 주요출자자를 말한다)는 〈별표 4〉에서 정한 요건을 충족하여야 한다.

6. 허가 및 등록신청 결격자

〈 감독규정 〉
제54조(허가 및 등록신청 결격자) 법 제32조제4호의 규정에서 "금융위원회가 정하는 자"라 함은「신용정보의 이용 및 보호에 관한 법률」제25조 제2항 제1호의 종합신용정보집중기관에 다음 각호 중 어느하나의 신용정보가 등록된 자를 말한다.
1. 어음·수표 거래정지처분 또는 부도거래정보
2. 대출금 등의 용도 외 유용 사실
3. 부정한 방법으로 대출을 받는 등 금융거래질서를 문란하게 한 사실

▣ 전자금융업 허가·등록을 신청하려는 자가 신용정보법상 연체정보·금융질서문란정보 등이 기록되어 있는 경우 허가·등록신청 결격사유로 처리하고자 함

▣ 해설

● '약정한 기일 내에 채무를 변제하지 아니한 자'라 함은 종합신용정보집중기관에 "신용판단정보"* 등이 기록된 자를 말함

* 1) 대출금 등의 연체 내용 2) 대위변제·대지급 발생 사실, 3) 어음 또는 수표의 거래정지처분을 받은 사실, 4) 대출금 등을 용도 외로 유용한 사실 및 부정한 방법으로 대출을 받는 등 신용질서를 문란하게 한 사실 등을 의미함

※ 신용정보의 이용 및 보호에 관한 법률 시행령 (별표 2) 참조

종합신용정보집중기관을 통하여 집중관리·활용되는 신용정보의 범위 〈별표2〉
(신용정보의 이용 및 보호에 관한 법률 시행령 제21조제3항 관련)

1. 개인

구 분	집중관리·활용 대상 정보
가. 식별정보	성명 및 개인식별번호
나. 신용거래정보	1) 대출·당좌거래 등에 관한 거래정보로서 다음 가)부터 다)까지의 정보 가) 대출 현황 나) 당좌예금·가계당좌예금의 개설 및 해지 사실 다) 담보 및 채무보증 현황 2) 신용카드에 관한 거래정보로서 다음 가)부터 다)까지의 정보 가) 신용카드의 발급·해지 사실 및 결제·미결제 금액(결제금액은 해당 신용정보를 보유한 신용카드업자가 동의하는 경우만 해당한다) 나) 2개 이상의 신용카드를 소지한 신용정보주체의 신용카드 이용금액, 이용한도, 신용카드에 의한 현금융통한도 다) 신용카드의 분실·도난 등 사고 발생, 그 발생한 사고 종결에 따른 보상, 그 밖의 사고 종결의 처리 사실 3) 보험상품에 관한 거래정보로서 다음 가) 및 나)의 구분에 따른 정보. 이 경우 보험계약자가 기업, 법인 및 단체인 경우에도 피보험자 또는 보험금청구권자(보험수익자, 피보험자 또는 손해보험계약의 제3자 등으로서 보험금을 청구할 권리가 있는 자를 말한다. 이하 같다)가 개인인 경우에는 그 보험상품을 포함한다. 가) 보험계약의 체결에 관한 정보: 보험계약 현황, 보험계약의 피보험자 또는 보험금청구권자에 관한 정보(성명, 개인식별번호, 직업 및 보험계약자와의 관계에 관한 정보를 말한다) 및 해당 보험계약을 모집한 모집업무수탁자에 관한 정보 나) 보험금의 청구 및 지급에 관한 정보: 보험금의 청구·지급 현황, 보험금의 지급 사유(질병에 관한 정보, 손해보험계약에 따른 보험목적에 생긴 손해 사실, 그 밖의 보험사고에 관한 정보를 포함한다), 보험금청구권자(책임보험계약에 따라 손해를 보상받는 피해자를 포함한다)에 관한 정보(성명, 개인식별번호, 피보험자와의 관계에 관한 정보를 말한다)
다. 신용도판단정보 등	1) 대출금, 신용카드 대금, 시설대여 이용료 등의 연체 사실 2) 대위변제·대지급 발생 사실 3) 어음·수표의 거래정지처분을 받은 사실 및 그 부도 사실 4) 증권의 투자매매업·투자중개업에 관한 정보로서 다음 가) 및 나)의 정보 가) 증권시장에 상장된 증권의 매매와 관련하여 투자중개업자에게 매수대금 또는 매도증권을 결제일까지 납입하지 아니한 사실 나) 증권시장에 상장된 증권의 매매를 위하여 투자자에게 제공하는 매수대금의 융자 또는 매도증권의 대여 거래에 관한 정보로서 상환 또는 납입기일까지 그 거래에 따른 채무를 이행하지 아니한 사실

	5) 금융질서 문란 정보로서 다음 가)부터 라)까지의 정보 가) 대출금 등을 용도 외로 유용한 사실 및 부정한 방법으로 대출을 받는 등 신용질서를 문란하게 한 사실 나) 거짓이나 그 밖의 부정한 방법으로 신용카드를 발급받거나 사용한 사실 다) 보험사기 사실 라) 그 밖에 가)부터 다)까지의 사실과 비슷한 것으로서 금융질서를 문란하게 한 사실 6) 공공기관이 만들어 낸 정보로서 다음 가)부터 마)까지의 정보 가) 법원의 회생·간이회생·개인회생과 관련된 결정, 파산선고·면책·복권과 관련된 결정, 채무불이행자명부의 등재·말소 결정 사실 나) 국세·지방세·관세 또는 국가채권과 벌금·과태료·과징금·추징금 등의 체납 관련 정보 다) 사회보험료·공공요금 또는 수수료 등 관련 정보 라) 주민등록 관련 정보로서 출생·사망·이민·부재에 관한 정보, 주민등록번호·성명의 변경 등에 관한 정보 마) 다른 법령에 따라 국가, 지방자치단체 또는 공공기관으로부터 받은 행정처분에 관한 정보 중에서 금융거래 등 상거래와 관련된 정보

2. 기업 및 법인

구 분	집중관리·활용 대상 정보
가. 식별정보	기업 및 법인의 상호 및 명칭, 사업자등록번호, 법인등록번호 및 고유번호, 본점·영업소 및 기관의 소재지, 종목, 대표자의 성명·개인식별번호
나. 신용거래정보	1) 대출·당좌거래 등에 관한 거래정보로서 다음 가)부터 사)까지의 정보 가) 대출·지급보증 등 신용공여 현황 나) 시설대여 현황 다) 신용보증 현황 라) 보증보험 현황 마) 담보 및 채무보증 현황 바) 당좌예금·가계당좌예금의 개설 및 해지 사실 사) 가)부터 바)까지의 정보로서 해당 기업 및 법인의 기술과 관련된 기술성·시장성·사업성 등을 종합적으로 평가함으로써 만들어진 정보 2) 신용카드에 관한 거래정보로서 다음 가) 및 나)의 정보 가) 신용카드의 발급·해지 사실 및 결제·미결제 금액(결제금액은 해당 신용정보를 보유한 신용카드업자가 동의하는 경우만 해당한다) 나) 신용카드의 분실·도난 등 사고 발생, 그 발생한 사고 종결에 따른 보상, 그 밖의 사고 종결의 처리 사실
다. 신용도판단정보(제2조제1항제3호 각 목의 어느 하나에 해당하는 자의 정보도	1) 기업 및 법인의 신용도 판단 정보로서 다음 가)부터 바)까지의 정보 가) 대출금, 신용카드 자금, 시설대여 이용료 등의 연체 사실 나) 대위변제·대지급 발생 사실 다) 신용보증기금이 대위변제한 사실 라) 어음·수표의 거래정지처분을 받은 사실 및 그 부도 사실

포함한다)	마) 무보증사채의 상환불이행 사실 바) 가)부터 마)까지의 정보로서 해당 기업 및 법인의 기술과 관련된 기술성·시장성·사업성 등을 종합적으로 평가함으로써 이루어진 대출, 신용보증 등에 대하여 연체, 대위변제 등이 발생한 사실 2) 증권의 투자매매업·투자중개업에 관한 정보로서 다음 가) 및 나)의 정보 가) 증권시장에 상장된 증권의 매매와 관련하여 투자중개업자에게 매수대금 또는 매도증권을 결제일까지 납입하지 아니한 사실 나) 증권시장에 상장된 증권의 매매를 위하여 투자자에게 제공하는 매수대금의 융자 또는 매도증권의 대여 거래에 관한 정보로서 상환 또는 납입기일까지 그 거래에 따른 채무를 이행하지 아니한 사실 3) 금융질서 문란 정보로서 다음 가)부터 라)까지의 정보 가) 대출금 등을 용도 외로 유용한 사실 및 부정한 방법으로 대출을 받는 등 신용질서를 문란하게 한 사실 나) 거짓이나 그 밖의 부정한 방법으로 신용카드를 발급받거나 사용한 사실 다) 보험사기 사실 라) 그 밖에 가)부터 다)까지의 사실과 비슷한 것으로서 금융질서를 문란하게 한 사실 4) 공공기관이 만들어 낸 정보로서 다음 가)부터 마)까지의 정보 가) 법원의 회생·간이회생·개인회생과 관련된 결정, 파산선고·면책·복권과 관련된 결정, 채무불이행자명부의 등재·말소 결정 사실 나) 국세·지방세·관세 또는 국가채권과 벌금·과태료·과징금·추징금 등의 체납 관련 정보 다) 사회보험료·공공요금 또는 수수료 등 관련 정보 라) 주민등록 관련 정보로서 출생·사망·이민·부재에 관한 정보, 주민등록번호·성명의 변경 등에 관한 정보 마) 다른 법령에 따라 국가, 지방자치단체 또는 공공기관으로부터 받은 행정처분에 관한 정보 중에서 금융거래 등 상거래와 관련된 정보
라. 신용거래능력 판단정보 등	1) 계열기업체 현황 등 회사의 개황 2) 사업의 내용 3) 재무제표 등 재무에 관한 사항 4) 자본금 증자 및 사채 발행 현황 5) 기업의 영업에 관한 정보로서 다음 가) 및 나)의 정보 가) 정부조달 실적 또는 수출·수입액 등의 관련 정보 나) 기술신용정보 및 이와 관련된 신용정보 6) 기업등록 관련 정보로서 설립, 휴업·폐업, 양도·양수, 분할·합병, 주식 또는 지분 변동 등에 관한 정보

7. 신청에 따른 등록말소 및 이용자보호조치

〈 감독규정 〉

제55조(신청에 따른 등록말소 및 이용자 보호조치) ① 법 제34조에 따라 등록의 말소를 신청하고자 하는 전자금융업자는 〈별지 제6호 서식〉에 따른 등록말소신청서를 금융위원회에 제출하여야 한다.

② 법 제34조에 따라 등록의 말소를 신청하고자 하는 전자금융업자는 신청 이전에 이용자 보호조치 계획을 금융위원회에 제출하여야 한다.

③ 금융위원회는 제1항의 전자금융업자가 제출한 계획이 이용자 보호에 충분하지 않은 경우에 그 보완을 요구할 수 있다.

▣ 전자금융업자의 등록 말소로 인한 이용자의 피해를 방지하기 위해 전자금융업자는 등록말소 신청 이전에 이용자 보호조치 계획을 금융위에 제출하여야 함

▣ 해설

- 금융위에 제출된 이용자 보호조치 계획이 이용자 보호에 충분하지 않을 경우 금융위는 보완을 요구할 수 있으며,
- 동 요구사항이 충분히 이행되지 않을 경우 전자금융업자에 대한 등록말소는 완료될 수 없음

※ 업자가 자기의사에 따라 전자금융업을 폐지하려는 등록말소와 달리 등록취소는 일정한 요건*에 해당될 경우 업자의 의사와 상관없이 감독당국이 취하는 행정행위를 말함

* 법 제43조제1항제1호 ~ 제5호에 해당하는 경우

제3절 전자금융업의 업무

1. 전자화폐 발행업자의 겸업가능 업무

〈 감독규정 〉
제56조(전자화폐 발행업자의 겸업가능 업무) 시행령 제22조제1항제3호에서 "금융위원회가 정하여 고시하는 업무"란 다음 각 호의 어느 하나에 해당하는 업무를 말한다.
1. 전자화폐 발행 및 관리를 위한 가맹점의 모집
2. 전자화폐 발행 및 관리를 위한 인터넷 홈페이지의 운영 및 이를 통한 통신판매 중개

▣ 개요

- 감독규정에서 전자화폐발행업자가 겸업가능한 업무의 범위를 정함

▣ 해설

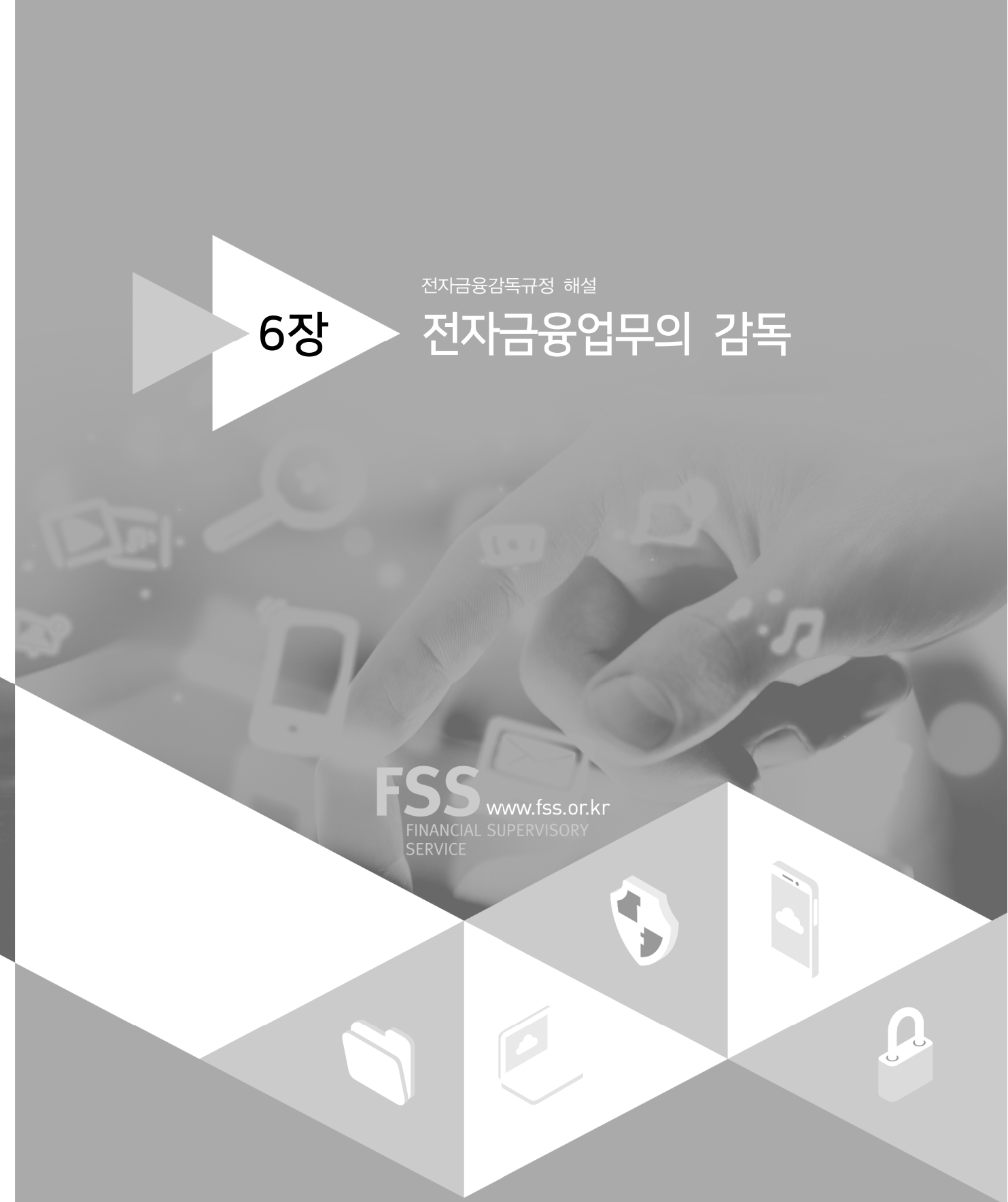
- 전자화폐발행업자는 원칙적으로 겸업이 금지됨
- 겸업이 허용되는 업무
  - 등록 대상 전자금융업무(등록을 전제)
  - 전자금융업과 관련된 정보처리시스템 및 소프트웨어의 개발·판매·대여
  - 금융회사 및 전자금융업자를 위한 전자금융업무의 일부 대행
  - 전자화폐 발행 및 관리를 위한 가맹점의 모집
  - 전자화폐 발행 및 관리를 위한 인터넷 홈페이지의 운영 및 이를 통한 통신판매 중개

2. 수수료 및 준수사항 등의 고지방법

〈 감독규정 〉
제57조(수수료 및 준수사항 등의 고지방법) 법 제38조제3항 각 호의 사항은 다음 각 호의 방법 중 제1호의 방법을 포함한 둘 이상의 방법으로 가맹점에게 알려야 한다.
1. 가맹점에의 개별 통보
2. 전국적으로 보급되는 일간신문에의 공고
3. 해당 금융회사 또는 전자금융업자 영업장 및 인터넷 홈페이지에의 게시

전자금융감독규정 해설

6장 전자금융업무의 감독



제6장 전자금융업무의 감독

1. 정보기술부문 실태평가

〈 감독규정 〉

제58조(금융회사의 정보기술부문 실태평가 등) ① 금융감독원장은 금융회사의 정보기술부문의 건전성 여부를 감독하여야 한다.

② 금융감독원장은 업무의 성격 및 규모, 정보기술부문에 대한 의존도 등을 감안하여 〈별표 5〉에 규정된 금융회사(이하 이 조에서 '은행등'이라 한다)에 대하여 검사를 통해 정보기술부문 운영 실태를 평가하고 그 결과를 경영실태평가 등 감독 및 검사업무에 반영하여야 한다.

③ 제2항에 의한 실태평가는 1등급(우수), 2등급(양호), 3등급(보통), 4등급(취약), 5등급(위험)의 5단계 등급으로 구분한다.

④ 금융감독원장은 제2항에 따른 정보기술부문 실태평가 결과 종합등급이 4등급인 경우에는 해당 은행등에게 이의 개선을 위한 확약서 제출을 요구할 수 있으며, 종합등급이 5등급이거나 직전 정보기술부문 실태평가 결과에 비해 평가등급이 2등급 이상 하향된 경우에는 취약점 개선대책의 수립·이행을 내용으로 하는 양해각서를 체결할 수 있다.

⑤ 제4항의 확약서는 대표자의 승인을 받아 제출하고, 양해각서는 해당 은행등의 이사회 재적이사 전원의 서명을 받아 체결한다.

⑥ 금융감독원장은 확약서 또는 양해각서의 이행상황을 점검하여 그 이행이 미흡하다고 판단되는 경우에는 확약서를 다시 제출받거나 양해각서를 다시 체결할 수 있다.

⑦ 확약서 또는 양해각서의 효력발생일자, 이행시한 및 이행상황 점검주기는 각 확약서 또는 양해각서에서 정한다. 다만, 이행상황 점검주기를 따로 정하지 않은 경우 은행등은 매분기 익월말까지 분기별 이행상황을 금융감독원장에게 보고하여야 한다.

⑧ 제2항에 따른 정보기술부문 실태평가 결과는 경영실태평가 세부 평가항목 중 경영관리 또는 위험관리 항목의 평가비중에서 최소 100분의 20 이상 반영되어야 하며, 금융감독원장은 정보기술부문 실태평가 결과가 4등급 이하인 은행등에 대해 경영실태평가 2등급 이상으로 평가할 수 없다.

⑨ 제2항에 의한 정보기술부문의 실태평가를 위한 세부 사항은 금융감독원장이 정한다.

〈 시행세칙 〉

제9조(정보기술부문 실태평가 방법 등) ① 규정 제58조에 따른 정보기술부문 실태평가는 검사기준일 현재 평가대상기관의 정보기술부문 실태를 IT감사, IT경영, 시스템 개발·도입·유지 보수, IT서비스 제공 및 지원, IT보안 및 정보보호의 부문별로 구분 평가하고 부문별 평가결과를 감안하여 종합평가한다.

② 제1항의 규정에 따른 부문별 세부 평가 항목은 별표 4와 같다.

③ 규정 제58조제3항의 평가등급별 정의는 별표 5와 같다.

▣ 개요

● 금융회사 IT부문 실태평가는 IT분야를 종합적이고 통일적인 방식에 의해 일정한 등급으로 평가함으로써, 일반부문 경영실태평가(CAMELS)를 보완하고 나아가 IT부문의 안전성 및 건전성을 확보토록 하는데 의의가 있음

* 전자금융업자의 경우 IT경영실태평가 대신 IT부문의 안전성을 점검함(※ 전자금융업자에 대해서는 IT경영실태평가를 실시하지 않음)

▣ 해설

● 기본운용 방향

– IT부문 실태평가는 일반 업무검사와 분리하여 IT부문을 별도로 평가하는 독립 평가체제임

– IT부문 실태평가는 「부문검사」로 운영하며, IT분야의 전문성 및 특수성에 상응하는 평가기준('IT부문 실태평가용 체크리스트')에 의해 IT부문 실태평가등급을 일반부문 종합검사결과와는 별개로 독립적으로 부여하고, 필요시에는 영업점의 전산운영실태를 파악하기 위한 연결검사를 실시함

● 평가대상 금융회사

– IT부문 실태평가는 일반업무의 성격 및 규모, IT부문에 대한 의존도 등에 비추어 IT부문 리스크가 높은 금융회사와 네트워크가 집중된 금융 유관기관을 대상으로 실시

– IT부문 리스크가 높은 중추 금융회사

○ 은 행 : 국내 시중은행, 지방은행, 특수은행

○ 증 권 : 국내 증권회사

○ 보 험 : 국내 생명보험사, 국내 손해보험사

○ 비은행 : 신용카드사, 상호저축은행, 종금사, PG(고객정보 보유)

– 네트워크가 집중되어 있는 금융 유관기관

○ 증 권 : 한국거래소, 한국예탁결제원, 증권금융회사

○ 보 험 : 보험개발원

○ 비은행 : 상호저축은행연합회, 신협중앙회

※ 금융감독원의 검사대상 금융회사 및 전자금융업자 중 IT부문 경영실태평가 대상에서 제외된 중소형 금융회사 및 전자금융업자의 경우에는 별도의 검사방법에 의거하여 IT부문 검사를 실시함

● 평가부문 및 평가 항목

– IT부문을 전산감사(Audit), 전산경영(Management), 시스템 개발·도입·유지보수, IT서비스 제공·지원, IT 보안 및 정보보호의 5개 부문으로 분류하여 평가한 후, 이를 토대로 종합평가를 실시

– 위의 5개 부문에 대하여 총 25개의 평가항목을 설정하되 전산업무의 특성상 모두 비계량 지표를 기준으로 평가

〈 정보기술부문 평가항목 〉

평가 부문	평가 항목수(대분류)
IT감사	3
IT경영	6
시스템 개발·도입·유지보수	4
IT서비스 제공 및 지원	7
IT 보안 및 정보보호	5
계	25

● 평가 등급

– 개별 금융회사의 IT부문 실태평가는 절대평가방식으로 이루어지며, 세부항목평가, 부문별 평가, 종합등급평가 등 각 단계마다 1등급(우수), 2등급(양호), 3등급(보통), 4등급(취약), 5등급(위험)의 5단계로 구분하여 평가등급을 부여

● 가중치

– 각 부문별 평가항목 및 세부평가항목에 가중치는 부여하지 않으나, 검사반장이 각 부분별 등급평가 및 종합등급 평가시에 해당 금융회사의 업무형태, IT리스크 등을 반영하여 등급평가를 할 수 있도록 함으로써 해당 금융회사의 특수성을 평가에 반영할 수 있도록 함

● 평가 시기

- 금융회사에 대한 IT부문 경영실태평가는 IT검사부서의 독자적인 검사계획에 따라 실시하되, 원칙적으로 금융회사 관련 소관 서비스국의 본점 종합검사 시기에 맞추어 실시하여 IT부문 경영실태평가 결과를 적기에 일반부문 경영실태평가에 반영할 수 있도록 함
- 다만, 다음과 같은 경우에는 IT검사를 일반분야 종합검사실시 시기보다 앞당기거나 늦추어 실시하는 등 탄력적으로 운영함
  - ○ 일반분야 종합검사가 특정 시기에 집중되어 IT검사인력 사정으로 동시에 검사 실시가 곤란한 경우
  - ○ 일반분야 종합검사와 IT검사를 동시에 실시하는 경우 피검사기관의 제한된 IT 인력으로는 일반분야 검사요구자료 및 IT검사 수검자료 작성 등이 중복되어 수검 부담이 과중하다고 판단되는 경우 등

● 평가결과의 활용

- 종합평가가 1등급인 금융회사에 대해서는 향후 IT부문 경영실태 평가를 위한 검사를 생략하거나, 검사를 실시하는 경우에도 검사기간을 단축하고, 검사범위를 축소하는 등 우대 조치함
- 종합평가가 2등급인 금융회사에 대해서는 향후 IT부문 경영실태평가시 검사기간을 단축하고 취약부문 위주의 부문검사를 실시함
- 종합평가가 3등급인 금융회사에 대해서는 전산부문 취약부문에 대해 자체적으로 개선계획을 수립·추진토록 하며, 이행 사항에 대하여 다음 검사시 중점 점검함
- 종합평가가 4등급인 금융회사에 대해서는 일반부문 경영실태평가 등급 산정시 IT 취약분야를 적극 반영토록 하고, 향후 IT부문 실태평가시 검사기간을 확대하며, 필요시에는 약정서를 요구하거나 양해각서를 체결할 수 있음
- 종합평가가 5등급인 금융회사에 대해서는 해당 취약부문 또는 전체 전산업무에 대하여 즉각 개선토록 조치하고, 일반부문 경영실태 평가등급의 하향조정 등을 해당 검사국에 요청
  - ○ IT부문의 경영실태평가 및 취약분야에 대한 검사를 타 금융회사에 최우선하여 실시하고, 필요시에는 약정서를 요구하거나 양해각서를 체결할 수 있음

〈 정보기술부문 실태평가 부문별 평가항목(시행세칙 별표4) 〉

평가 부문	평가 항목
1. IT 감사	– IT감사조직 및 요원 – IT감사 실시 내용 – IT감사 사후관리 및 기타
2. IT 경영	– IT부서 조직 및 요원 – IT관련 내규(규정, 지침, 절차, 편람 등) – IT계획 및 방향제시 – 비상계획 – 경영정보시스템(MIS) – IT 인력 및 예산의 적정성
3. 시스템 개발, 도입 및 유지보수	– 시스템 개발, 도입 및 유지보수 관련 조직 및 요원 – 시스템 개발, 도입 및 유지보수 관련 내규(규정, 지침, 절차 등) – 시스템 개발, 도입, 유지보수 현황 – 내부통제용 시스템, 시스템통합 등
4. IT서비스 제공 및 지원	– IT서비스 제공/지원 관련 조직 및 요원 – IT서비스 제공/지원 관련 내규(규정, 지침, 절차 등) – 시설 및 장비 – 운영통제 – 통신망 – 최종사용자컴퓨팅 – 전자금융거래 등
5. IT 보안 및 정보보호	– IT 보안 절차 – IT 보안 리스크 평가 – IT 보안 및 정보보호전략 – IT 보안 통제 구현 – IT 보안 모니터링

2. 외부주문등에 대한 기준

〈 **감독규정** 〉

제60조(외부주문등에 대한 기준) ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 외부주문등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영
2. 금융회사와 이용자 간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지
3. 계좌번호, 비밀번호 등 이용자 금융정보 무단보관 및 유출 금지
4. 접근매체 위·변조, 해킹, 개인정보유출 등에 대비한 보안대책 수립
5. 금융회사와 전자금융보조업자 간의 접속은 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다)을 사용
6. 정보처리시스템 장애 등 서비스 중단에 대비한 비상대책 수립
7. 외부주문등의 입찰·계약·수행·완료 등 각 단계별로 금융감독원장이 정하는 보안관리방안을 따를 것
8. 업무지속성을 위한 중요 전산자료의 백업(backup)자료 보존 및 백업설비 확보 등 백업대책 수립
9. 정보관리의 취약점을 최소화하고 보안유지를 위한 내부통제방안을 수립·운용하고, 통제는 제8조제1항제2호의 조직에서 수행
10. 전자금융보조업자에 대한 재무건전성을 연1회 이상 평가하여 재무상태 악화에 따른 도산에 대비하고 전자금융보조업자의 주요 경영활동에 대해 상시 모니터링을 실시
11. 전자금융보조업자가 제공하는 서비스의 품질수준을 연1회 이상 평가할 것
12. 전자금융보조업자가 사전 동의 없이 다시 외부주문등 계약을 체결하거나 계약업체를 변경하지 못하도록 하고, 사전 동의시 해당 계약서에 제7호의 사항을 기재하도록 통제
13. 업무수행인력에 대하여 사전 신원조회 실시 또는 대표자의 신원보증서 징구, 인력변경시 인수인계에 관한 사항 등을 포함한 업무수행인력 관리방안 수립
14. 외부주문등은 자체 보안성검토 및 정기(금융감독원장이 정하는 중요 점검사항에 대해서는 매일) 보안점검 실시

② 금융회사 또는 전자금융업자는 제1항제10호 및 제11호의 평가결과를 금융감독원장에게 보고하여야 한다.

③ 금융감독원장은 제2항의 규정에 따른 평가결과 보고를 접수하고, 그 평가실시 여부를 제58조제2항의 규정에 따른 정보기술부문 실태평가에 반영할 수 있다.

④ 법 제40조제6항 단서에서 "금융위원회가 인정하는 경우"란 전자금융거래정보의 보호와 관련된 전산장비·소프트웨어에 대한 개발·운영 및 유지관리 업무를 재위탁하는 경우로서 다음 각 호의 사항을 준수하는 경우를 말한다.

1. 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
2. 위탁업무와 관련된 이용자의 금융거래정보는 위탁회사의 전산실 내에 두어야 함. 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 가능함

〈 시행세칙 〉
제9조의2(외부주문등에 대한 기준) ① 규정 제60조제1항제7호에 따라 감독원장이 정하는 보안관리방안은 별표 5-2와 같다.
② 규정 제60조제1항제14호에 따라 감독원장이 정하는 중요 점검사항은 별표 5-3과 같다.

▣ 금융회사 및 전자금융업자는 전자금융거래와 관련 전자금융보조업자와 제휴 또는 외부주문에 관한 계약을 체결하거나 변경하는 때 전자금융거래의 안전성 및 신뢰성과 금융회사 및 전자금융업자의 건전성을 확보할 수 있도록 금융위가 정하는 기준 준수(법 제40조)

▣ 금융회사 또는 전자금융업자가 IT업무의 전부 또는 일부를 전자금융보조업자와 제휴 또는 외부주문하는 경우, 동 제휴 등으로 인한 고객정보 유출 및 정보처리시스템 장애를 방지하기 위한 관련기준을 정함

▣ 해설

- 금융회사의 핵심업무가 외부업체에 종속되지 않도록 필요최소조건을 마련하여 관련 리스크를 최소화할 필요
  - 금융회사 및 전자금융업자가 아웃소싱 도입 초기단계부터 보다 엄격한 규정을 적용함으로써 관련리스크 제거를 위한 모범규준(best practice)을 사전에 고려하여 반영하도록 유도
- 정보처리시스템의 설치 장소에 대한 통제와 관련해서는 규정 제9조 내지 제11조를 준수하도록 함
- 외부주문업체에 의한 컴퓨터 기록 또는 통신상 자료의 유출방지와 유출되더라도 그 내용을 확인할 수 없도록 중요 자료를 암호화하여 보관하여야 함(제3호, 제4호)
- 외부주문업체는 계약서상 사용하도록 인정된 사항 이외의 금융회사 또는 전자금융업자의 정보를 임의로 사용하거나 공개하지 못함(규정제60조)
- 불가피하게 이용자 정보 등이 필요한 경우 규정 제13조(전산자료 보호대책) 준수 (예시1 : 테스트 시 이용자 정보를 변환하여 사용하고 테스트 종료시 즉시 삭제, 예시2 : 이용자정보 조회시 사용자, 사용일시, 변경·조회 내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고 그 기록을 1년 이상 보존)

- 외부주문업체가 자료의 생성, 전송, 처리, 유지 및 저장되는 동안에 물리적 또는 논리적 통제절차를 통해 비인자의 접근, 수정, 파괴 정보의 공개 등을 방지하도록 물리적·논리적 보안 대책을 수립(제4호)

- 금융회사는 제휴 또는 외부주문업체와의 접속은 전용회선(물리적 전용회선에 준하는 VPN방식 포함)을 이용(제5호)

- 외부주문업무의 화재, 홍수, 해킹 등 재난으로 인한 서비스 중단과 외부주문 업체의 도산으로 인한 서비스 중단으로 구분하여 형태별 비상대책을 수립하여야 함(제6호)

- 금융회사 또는 전자금융업자가 외부주문을 하는 경우 계약 단계별로 금감원장이 정하는 보안관리방안을 준수해야 함(제7호, 시행세칙 제9의2)

- 금융회사 또는 전자금융업자는 업무연속성 확보를 위하여 고객 정보 및 금융거래 정보를 포함한 주요 전산자료의 백업자료 보존 및 백업설비 확보 등 백업대책을 수립(제8호)

- 정보유출 방지를 위해 외부주문업체의 시스템개발 및 유지보수 정책이 내부 가이드라인 및 제약조건 등에 부합하는지 점검 필요(제9호)

- 전자금융보조업자에 대한 재무건전성 및 서비스품질수준을 연 1회 이상평가(제10호, 제11호)

- 외부주문업체와의 계약을 통하여 외부주문업체가 위탁자의 사전 동의 없이 제3자에게 외부주문 대상 업무를 재위탁하거나 재위탁업체를 변경하는 행위 금지(제12호)

- 금융회사 또는 전자금융업자가 외부주문업체의 재위탁을 허용할 경우 재수탁자의 적격성 기준을 자체적으로 수립하여 운용(제12호)

- 외부주문업체는 프로그램 등록·변경·폐기 방법, 변경 전·후 내용의 기록 및 관리·등록·변경·폐기 내용의 정당성에 대한 제3자 검증, 변경 필요시 복사 후 수정, 접근 담당자 한정 등에 대한 절차 수립·운영하여야 함(제13호)

- 외부주문 등은 자체보안성 검토 및 보안점검 실시하며, 금감원장이 정하는 중요 점검사항은 매일 점검(제14호)

〈별표 5-2〉보안관리방안

단계	세부사항
입찰	○ 입찰 공고 이전에 투입이 예상되는 자료·장비 가운데 보안관리가 필요한 사항에 대하여 금융회사 또는 전자금융업자의 내부관리기준과 관련 법규를 검토하고 필요한 보안요구 사항을 마련 ○ 입찰 공고시에 금융회사 또는 전자금융업자가 자체 작성한 중요정보, 부정당업자 제재조치, 기밀유지 의무 및 위반시 불이익 등을 정확히 공지 ○ 제안서 평가요소에 자료·장비·네트워크 보안대책 및 중요정보 관리 방안 등 보안관리 계획의 평가항목 및 배점기준 마련 ○ 업체가 입찰제안서에 제시한 용역사업 전반에 대한 보안관리 계획이 타당한지를 검토하여 사업자 선정시에 이를 반영
계약	○ 계약서 작성 초기 단계부터 정보보안사항 포함여부에 대한 검토 실시 ○ 용역사업에 투입되는 자료·장비 등에 대해 대외보안이 필요한 경우 보안의 범위·책임을 명확히 하기 위해 사업수행 계약서와 별도로 비밀유지계약서 작성 ○ 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반시 손해배상 책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시 ○ 용역사업 참여인원은 금융회사 또는 전자금융업자의 사전 동의 없이 용역업체가 임의로 교체할 수 없도록 명시 ○ 금융회사 또는 전자금융업자의 요구사항을 사업자에게 명확히 전달키 위하여 작성하는 과업지시서·계약서(입찰 공고 포함)에 인원·장비·자료 등에 대한 보안조치 사항과 정보유출 및 부정당업자에 대한 손해배상 내용 등을 정확히 기술 ○ 용역업체가 사업에 대한 하도급 계약을 체결할 경우 원래 사업계약 수준의 비밀 유지 조항을 포함토록 조치 ○ 규정 제7조 각호에 규정한 사항의 준수를 위하여 외부주문업체 등의 협조가 요구되는 사항
수행	[인력] ○ 용역사업 참여인원에 대해서는 '정보 유출' 방지 조항 및 개인의 자필 서명이 들어간 보안서약서 징구 ○ 용역사업 수행前 참여인원에 대해 법적 또는 금융회사 또는 전자금융업자의 규정에 따른 비밀유지 의무 준수 및 위반시 처벌내용 등에 대한 보안교육 실시 * 유출 금지 대상정보 및 정보 유출시 부정당업자 제재조치 등에 대한 교육 병행 ○ 금융회사 또는 전자금융업자는 사업 수행 중 업체 인력에 대한 보안점검 실시, '유출금지 대상정보' 외부 유출여부 확인 [자료] ○ 계약서 등에 명시한 중요정보를 업체에 제공할 경우 자료관리 대장을 작성, 인계자·인수자가 직접 서명한 후 제공하고 사업완료시 관련자료 회수 ○ 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 금융회사 또는 전자금융업자의 파일서버에 저장하거나 금융회사 또는 전자금융업자가 지정한 PC에 저장·관리 ○ 용역사업 관련 자료는 인터넷 웹하드·P2P 등 인터넷 자료공유사이트 및 개인메일함에 저장을 금지하고 금융회사 또는 전자금융업자와 용역업체간 전자우편을 이용해 전송이 필요한 경우에는 자체 전자우편을 이용하고, 첨부자료 중 중요정보 포함자료는 암호화 후 수발신

	○ 금융회사 또는 전자금융업자가 제공한 사무실에서 업체가 용역사업을 수행할 경우, 유출금지 대상 정보가 포함된 자료는 매일 퇴근시 시건장치가 된 보관함에 보관 ○ 용역사업 수행으로 생산되는 산출물 및 기록은 금융회사 또는 전자금융업자가 인가하지 않은 비인가자에게 제공·대여·열람을 금지 **[사무실·장비]** ○ 용역사업 수행장소는 금융회사 또는 전자금융업자 전산실 등 중요시설과 분리하고 CCTV·시건장치 등 비인가자의 출입통제 대책을 마련 ○ 용역업무를 수행하는 공간에 대한 보안점검을 정기적으로 실시 ○ 용역직원이 노트북 등 관련 장비를 외부에서 반입하여 내부망에 접속시 악성코드 감염여부 및 반출시마다 자료 무단반출 여부 확인 ○ 인가받지 않은 USB메모리 등의 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 금융회사 또는 전자금융업자의 승인하에 사용 **[내·외부망 접근시]** ○ 금융회사 또는 전자금융업자는 개발시스템과 운영시스템을 분리하고, 용역업체는 업무상 필요한 서버에만 제한적 접근 허용 ○ 용역사업 수행시 금융회사 또는 전자금융업자 전산망 이용이 필요한 경우 - 사업 참여인원에 대한 사용자계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 차등 부여하되 허용되지 않은 금융회사 또는 전자금융업자의 내부문서 접근 금지 - 계정별로 부여된 접속권한은 불필요시 즉시 해지하거나 계정을 폐기 - 참여인원에게 부여한 계정은 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인 - 금융회사 또는 전자금융업자는 내부서버 및 네트워크 장비에 대한 접근기록 이상 여부를 정기 점검 ○ 용역업체에서 사용하는 PC는 인터넷 연결을 금지하되, 사업수행상 연결이 필요한 경우에는 금융회사 또는 전자금융업자의 보안통제하에 제한적 허용 ○ 용역업체 사용 전산망에서 P2P, 웹하드 등 인터넷 자료공유사이트로의 접속을 원천 차단
완료	○ 사업 완료 후 생산되는 최종 산출물 등 대외보안이 요구되는 자료는 대외비 이상으로 작성·관리하고 불필요한 자료는 삭제 및 폐기 ○ 용역업체에 제공한 자료, 장비와 중간·최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도 보관 금지 ○ 용역사업 완료 후 업체 소유 PC·서버의 하드디스크·휴대용 저장매체 등 전자기록 저장매체는 복원이 불가능한 방법으로 완전 삭제 후 반출 ○ 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업관련 자료를 보유하고 있지 않다는 대표자 명의의 확약서 징구

〈별표 5-3〉 중요 점검사항

	점검 항목
1	이용자 정보의 조회·출력에 대한 통제 및 이용자 정보 조회시 사용자, 사용일시, 변경·조회내역, 접속방법 기록·관리
2	테스트시 이용자 정보 사용금지(부하 테스트 등 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제)
3	운영시스템 접속·사용 통제
4	내부통신망의 비인가 전산장비·무선통신 접속 통제(정보처리시스템을 이용한 통제 장치 마련시 통제장치에 대한 일일점검으로 대체 가능)
5	전산자료 및 전산장비 반출·반입 통제
6	전산실 등 출입자 관리기록부 기록·보관
7	인터넷(무선통신망 포함) 사용 통제(정보처리시스템을 이용한 통제 장치 마련시 통제장치에 대한 일일점검으로 대체 가능)
8	운영체제 및 악성코드 치료프로그램을 최신으로 유지
9	USB 등 보조기억매체 사용 통제
10	단말기에 이용자 정보 등 중요정보 보관 금지

※ 법령해석('15.3.12.)

〈 질의 〉

(1) 외부주문등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소와 내부업무장소를 분리하는 경우, 그 분리의 정도 ① 부서를 구분하여 표시하거나 파티션으로 구획하는 등 외부에서 인지가능한 정도로만 분리 ② 칸막이 등을 이용하여 공간을 바닥부터 천장까지 분리 ③ 별도의 공간으로 분리(다른 층 또는 다른 출입문 이용)

〈 회신 〉

(1) 외부주문시 정보시스템 개발업무에 필요한 인적·물적 시설은 칸막이, 별도 공간 등 외부에서 인지 가능한 수준으로 분리하여 운영하여야 합니다. (2) 개발에 사용되는 정보시스템과 통신망은 운영시스템과 물리적으로 분리하여 운영시스템에 대한 비인가자의 접근을 원천적으로 차단하여야 합니다. (3) 또한, 물리적 분리 이외에 관리통제가 엄격하게 이루어 지도록 정보시스템 접근 통제, 인적통제 등 내부통제장치가 마련되어야 합니다.

〈 이유 〉

(1) 외부주문에 의한 정보시스템 개발업무에 사용되는 공간은 내부업무장소와 칸막이, 별도공간으로 분리하여 운영하도록 함으로써 중요정보 유출, 부주의, 관리소홀로 인한 사고 등을 방지하고 이에 따른 책임을 명확히 하기 위함입니다.

(2) 외부 주문에 의한 정보시스템 개발시 개발업무에 사용되는 정보시스템 및 통신망은 운영시스템과 물리적으로 분리하여 운영되어야 하며, 이는 보안 취약요인을 사전에 차단하고 보안이 취약한 개발시스템으로

부터 운영시스템으로의 악성코드 전이, 접근통로 이용 등을 원천적으로 차단하여 운영시스템을 안전하게 보호하기 위함입니다.

(3) 또한, 업무장소와 전산설비를 내부 업무용과 분리하여 설치·운영함에 있어서 물리적 분리의 실효성을 확보하기 위하여 접근통제, 인적통제, 출입통제 등 관리통제가 엄격하게 이루어지도록 내부통제 장치를 마련하여 운영하여야 합니다.

※ 관련규정 : 제60조(외부주문등에 대한 기준) ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문 등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 1. 외부주문등에 의한 정보처리시스템의 개발 업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영

※ 법령해석('15.4.28.)

〈 질의 〉

▣ 정보기술부문의 정보보호와 관련 업무를 위탁 받은 전자금융보조업자가 해당 업무를 제3자에게 재위탁할 수 있는 범위

* (사실관계) 금융회사가 보안업무의 일부를 전산업체에게 위탁하였고, 해당 전산업체는 수탁 보안업무의 일부를 재위탁하여 운영 하고 있음. 재수탁업자의 수행업무는 보안토큰 및 방화벽 운영, 네트워크 트래픽 분석 등 보안 인프라를 운영하는 업무일 뿐이어서 금융거래정보 및 이용자 정보를 취급하는 업무와는 관련이 없음

〈 회신 〉

▣ 전자금융거래법에서의 정보보호 관련 업무는 정보보호최고책임자(CISO)가 통솔하는 업무로서 정보기술부문의 보호를 위한 방화벽 운용·시스템모니터링 등 보안인프라 운영과 취약점 분석·평가, IT내부통제 관리 등의 업무를 말하며, 법 제40조제6항에서는 정보기술부문의 정보보호와 관련된 업무에 대한 재위탁을 원칙적으로 금지하고 있습니다. 다만 전자금융감독규정 제60조제4항 각 호의 요건을 충족한다면 재위탁이 허용될 수 있습니다.

〈 이유 〉

▣ 전자금융거래법 제40조제6항의 재위탁 금지규정은 전자금융거래정보의 보호 및 안전한 처리를 목적으로 설치된 조항이며, 후단의 단서 규정은 이러한 목적을 달성하기 위한 조건을 준수할 경우 제한적으로 재위탁을 허용하는 것입니다. 전자금융감독규정 제60조제4항 각 호의 내용은 전자금융거래정보의 보호 목적 달성을 위해 보다 철저한 내부통제를 실시하고, 외부반출이 필요한 경우에는 관련정보를 이용하거나 다른 정보와 결합하여 금융거래정보를 식별할 수 없도록 조치를 하여야 함을 규정한 것입니다. 따라서 그러한 조건이 충족된다면 재위탁을 허용할 수 있을 것입니다.

한편, 재위탁에 따른 재수탁자도 전자금융거래법 제2조제5호에 따른 전자금융보조업자의 범위에 포함되므로 법 제40조 및 감독규정 제60조에 따른 의무사항을 준수하여야 합니다.

※ 법령해석('15.4.28.)

〈 질의 〉

▣ 전자금융거래법 제40조제6항의 전자금융보조업자의 정보보호업무 재위탁 금지 예외 인정 관련 문의

1. 당사는 사업을 진행하며, 고객사에 금융서비스를 제공함에 (1)보안인프라를 운영하는 업무 또는 (2)부수적

으로 정보보호업무를 수행하는바, (1)단순 보안인프라를 운영 업무와 (2)부수적으로 이루어지는 정보보호업무의 경우에도, 전자금융거래법 제40조제6항 본문에 해당되어, 정보기술부문의 정보보호와 관련된 업무를 위탁 받은 전자금융보조업자로서 제3자에게 해당업무를 재위탁해서는 안되는지 여부

2. 재위탁 금지사유에 해당되는 경우에, 전자금융거래법 제40조제6항 단서 및 전자금융감독규정 제60조제4항의 "금융위원회가 인정하는 경우"로 인정되어 위탁가능하기 위한 요건은 "전자금융감독규정 제60조제4항"의 "요건"만을 충족하면 가능한지 여부

〈 회신 〉

▣ 보안토큰 및 방화벽 운영, 네트워크 트래픽 분석 등 보안인프라 운영 업무의 경우 전자금융거래정보를 주업무로 취급하지 않더라도 정보기술부문의 정보보호와 관련된 업무로서 원칙적으로 재위탁 금지대상에 포함됩니다. 다만, 전자금융거래법 제40조제6항의 단서 규정에 따라 전자금융감독규정 제60조제4항 각 호에 대하여 준수할 경우 재위탁이 예외적으로 허용된다고 하겠습니다.

〈 이유 〉

▣ 전자금융거래법 제40조제6항의 재위탁 금지조항은 전자금융거래정보의 보호 및 안전한 처리를 목적으로 설치된 조항이며, 후단의 단서 규정은 이러한 목적을 달성하기 위한 조건을 준수할 경우 제한적으로 재위탁을 허용하는 것입니다. 전자금융감독규정 제60조제4항 각 호는 전자금융거래정보의 보호 목적 달성을 위해 보다 철저한 내부통제를 실시하고, 외부반출이 필요한 경우에는 관련정보를 이용하거나 다른 정보와 결합하여 금융거래정보를 식별할 수 없도록 조치를 하여야 함을 규정한 것입니다.

방화벽, 네트워크 트래픽 분석 설비 등 정보보안 설비는 금융거래정보를 주업무로 취급하지 않지만, 네트워크 및 서버에 금융거래 정보가 유통될 가능성이 있으므로 보안 인프라 운영에 대한 재위탁은 전자금융감독규정 제60조제4항 각 호의 요건을 충족하는 경우에만 허용됩니다.

※ 비조치의견서('15.6.8.)

〈 요청대상 행위 〉

▣ 특정기간(예 : 3개월) 동안 근무하는 외주직원에 대해서는 중요 점검사항*을 매일 점검하지 않고 인력변동 등 특별한 사유 발생시 또는 매월 정기적으로 점검하는 것이 가능한지 여부

* 전자금융감독규정 제60조①제14호 및 전자금융감독규정시행세칙 별표5-3

〈 판단 〉

▣ 요청대상 행위는 전자금융감독규정 제60조①제14호에 위반되는 것으로 제재대상에 해당됩니다.

〈 판단이유 〉

▣ 전자금융감독규정 제60조①제14호는 외주용역 과정의 정보유출을 차단하기 위한 것으로 중요 점검사항에 대해서는 매일 점검하도록 규정하고 있으며, 이에 대한 예외를 인정하고 있지 않습니다.

※ 법령해석('15.7.1.)

〈 질의 〉

▣ 당행의 외주개발직원은 △△은행 건물에 상주하며 당행에서 제공하는 △△은행 전용 PC를 사용하여 개발을 지원하고 있고, 망분리 규정에 따라 모든 외주직원 포함 전산직원의 인터넷 접속이 차단되었으며 현장관리인 및 담당관리자의 점검을 통해 보안이 통제되고 있음

▣ 또한 당행은 시스템 환경을 가) 실환경, 나) 사용자테스트용 환경, 다) 개발환경으로 나누어 외주 포함 모든 개발직원이 다) 개발환경 이외의 다른 환경에는 접속하지 못하도록 개발자의 실환경 접근관리 규정에 따라 엄격히 통제되고 있음

그리고 위의 가), 나), 다) 환경은 모두 물리적으로 분리되어 있어 개발자가 가) 실환경 및 나) 사용자테스트용 환경에 접근할 수 있는 방법은 없음

(1) 당행의 위와 같은 통제 방법이 「전자금융감독규정」 제60조제1항제1호(외부주문 등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치, 운영)를 준수한다고 볼 수 있는지

(2) '개발업무에 사용되는 전산설비를 내부업무용과 분리'하라는 의미가 외주 개발 직원이 당행 네트워크에 직접 접속하지 못하도록 망을 분리하고 별도의 개발환경을 마련해야 한다는 것인지

(3) 위의 '외부 주문 등에 의한 정보처리시스템 개발'이 유지보수를 위해 상주하는 경우를 제외하고 프로젝트만을 의미하는 것인지

〈 회신 〉

▣ (1) 주어진 조건에서 개발업무에 필요한 인적·물적 시설이 칸막이, 별도 공간 등 외부에서 인지 가능한 수준으로 내부업무용과 분리되어 있고, 현장관리인 및 담당관리자의 점검을 통해 접근통제, 인적통제 등의 내부통제가 이루어진다면 「전자금융감독규정」 제60조제1항제1호를 준수하는 것으로 볼 수 있습니다.

(2) 외주 개발 직원이 내부 업무용시스템에 접속하지 못하도록 망을 분리하고, 별도의 개발환경을 마련하여 내부 업무용시스템에 대한 비인가자의 접근을 원천적으로 차단하는 경우 '개발업무에 사용되는 전산설비를 내부업무용과 분리'한 것으로 볼 수 있습니다.

(3) 「전자금융감독규정」 제60조제1항제1호의 '외부주문 등에 의한 정보처리시스템 개발'의 경우 정보처리시스템에 대한 유지보수를 위해 상주하는 것은 제외됩니다.

〈 이유 〉

▣ (1) 「전자금융감독규정」 제60조제1항제1호는 외부주문에 의한 정보시스템 개발업무에 사용되는 공간을 내부 업무장소와 분리하여 운영하도록 하고, 개발업무에 사용되는 전산설비는 내부 업무용 시스템과 분리하도록 함으로써 중요정보 유출, 부주의, 관리소홀로 인한 사고 등을 방지하고 이에 따른 책임을 명확히 하기 위함입니다.

(2) 개발업무에 사용되는 전산설비를 내부업무용과 분리하라는 의미는 외주 개발 직원이 내부 업무용 시스템에 직접 접속하지 못하도록 함으로써 비인가자의 접근을 원천적으로 차단하려는 것입니다. 이는 보안취약요인을 사전에 차단하고 보안이 취약한 개발시스템으로부터 내부 업무망으로의 악성코드 전이, 접근통로 이용 등을 차단하기 위함입니다.

(3) 「전자금융감독규정」 제60조제1항제1호는 정보처리시스템 개발업무와 관련하여 준수하여야 사항이며, 유지보수를 위한 업무에까지 적용되는 규정은 아닙니다.

한편, 재위탁에 따른 재수탁자도 전자금융거래법 제2조제5호에 따른 전자금융보조업자의 범위에 포함되므로 법 제40조 및 감독규정 제60조에 따른 의무사항을 준수하여야 합니다.

※ 법령해석('15.10.28.)

〈 질의 〉

▣ 당사의 계열사로 하여금 시스템 개발 업무를 서로 분리된 장소 및 설비 하에 수행 중인데, 기존 시스템 운영 직원이 차세대 시스템 점검 및 일부 개발 목적으로 운영 장소에서 운영시스템에 접속하는 PC를 이용하여 개발용 정보처리시스템에 접속하도록 허용해도 되는지 여부

* (사실관계) A사는 당사의 차세대 시스템 개발을 위하여 별도의 개발실에서 외주인력과 함께 개발을 수행 중(개발장소 및 시스템 물리적 분리). 이와 별도로 당사는 개발 시스템의 철저한 점검, 시스템 오픈 후의 운영 안정성을 확보하기 위하여 시스템 운영 인력에게 운영 업무와 병행하여 동일 장소에서 신규로 개발되고 있는 차세대 시스템에 개발환경으로 접근, 테스트·점검 및 개발업무를 수행하도록 하고자 함

〈 회신 〉

▣ 「전자금융감독규정」제60조제1항제1호에서 외부주문등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소 및 전산설비를 내부 업무용과 분리하여 설치·운영하도록 하는 것은 운영시스템에 대한 비인가 접근 및 변경 위험 방지, 중요자료 접근통제, 해킹 등 침해사고 예방, 정보유출 방지 등 외주업체에 의한 보안사고 예방을 위한 기본적인 물리적 보안조치입니다.

○ 운영시스템에 접속하는 PC와 시스템 개발 수행사의 네트워크를 연결하게 되면 불법적인 외부접근 통로로 사용될 가능성이 있고 중대한 보안위협이 되는 바, 국제표준(ISO27001) 및 정보보호관리체계(「정보통신망법 이용촉진 및 정보보호 등에 관한 법률」) 인증의 통제항목에서도 개발, 테스트, 운영 설비를 분리하도록 하고 있습니다.

▣ 질의하신 내용과 관련하여 이상과 같은 사유로 개발업무 점검 등의 편의성을 위해 '운영시스템에 접속하는 PC를 이용하여 개발용 정보처리시스템에 접속하도록 허용'하는 것은 불가함을 알려드립니다.

○ 만약, 시스템 운영 인력을 활용하여 시스템 운영 장소에서 개발시스템 점검 및 일부 개발업무를 수행하고자 할 경우, 금융회사 정보보호최고책임자의 승인을 받아 별도의 공간에 업무망과 분리된 전용단말기를 설치하고 해당 단말기는 본체·USB포트·통신포트 봉인, 무선통신·인터넷 차단, CD·외장메모리 등 저장매체 사용장치 탈거, DRM 적용, 문서편집기 삭제, 업무담당외 사용금지, 접속기록 유지, 단말기 반출시 저장장치 파쇄 등 철저한 단말기 보안관리를 실시하여야 할 것입니다.

〈 이유 〉

▣ 「전자금융감독규정」 제60조제1항제1호에서 '외부주문등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영' 하도록 하는 것은 운영시스템에 대한 비인가 접근 및 변경 위험 방지 등 외주업체에 의한 보안사고 예방을 위한 기초적인 물리적 보안조치입니다.

▣ 시스템 개발사가 금융회사의 계열사라 하더라도 엄밀하게는 외주용역업체이고, 시스템 개발 단계에서는 다양한 개발환경으로 인해 각종 보안취약점들이 존재할 수 있습니다. 이에 따라 금융회사의 핵심 전산시설

운영과 전산개발은 분리하여 처리되어야 하며 핵심시설에 직접 접속하는 시스템 운영업무와 개발업무를 동일한 단말기에서 수행할 수는 없습니다.

※ 비조치의견서('16.2.18.)

〈 질의 〉

▣ 인력 및 하드웨어/소프트웨어 유지보수 업체와의 계약기간이 완료하여 재계약을 체결하는 경우,

○ 외주업체로부터 용역사업 관련 자료를 보유하고 있지 않다는 대표자 명의의 확약서*(이하 '확약서')를 징구해야 하는지 여부

* 전자금융감독규정 제60조①항7호 및 시행세칙 제9조의①항〈별표 5-2〉 보안관리방안

〈 판단 〉

▣ 용역의 내용이 동일하고 단지 계약기간을 연장하기 위해 재계약을 체결하는 경우 확약서를 징구할 필요가 없습니다.

○ 다만, 계약내용이 일부 변경되어 자료 폐기가 필요하거나 계약기간 종료 이후에 재계약이 이루어지는 경우 확약서를 징구해야 합니다.

〈 판단이유 〉

▣ 관련 법규에서 용역업무의 수행·완료 단계를 구별하고 있고 완료 단계에서 사업종결 후 관련 자료의 폐기 및 산출물의 관리 방법에 대해 정하고 있다는 점을 고려할 때,

○ 동 규정상의 '완료'는 외주주문에 의한 용역사업이 완전히 종결되는 것으로 해석하는 것이 타당합니다.

▣ 계약기간을 연장하기 위해 재계약을 체결하는 경우에는 확약서를 징구할 필요가 없으나,

○ 계약 내용이 일부 변경되어 자료 폐기가 필요*하거나 계약기간 종료 이후에 재계약이 이루어지는 경우 외부주문 보안관리방안에 따라 확약서를 징구해야 합니다.

* (예) 유지보수 대상 하드웨어/소프트웨어가 변경될 경우 변경 전 하드웨어 등에 대한 자료를 폐기

3. 전자금융보조업자의 자료제출

〈 감독규정 〉

제61조(전자금융보조업자 자료제출 기준) ① 금융감독원장은 전자금융보조업자에 대해 외부주문등과 관련한 계약서, 계약서 부속자료 및 그 밖의 전자금융업무와 관련한 자료 등을 직접 요구할 수 있다.

② 제1항에 따른 자료제출 요구시 전자금융보조업자는 특별한 이유가 없는 한 자료제출에 응하여야 한다.

▣ 금융감독원장은 금융회사 또는 전자금융업자에 대한 검사업무 수행시 제휴 또는 외부주문과 관련하여 전자금융보조업자에게 자료제출을 직접요구할 수 있음

▣ 해설

- 전자금융보조업자에 대한 자료제출 요구시 금융회사 및 전자금융업자의 검사업무수행에 필요한 최소한의 범위내에서 자료를 요구하며, 요구자료는 제휴나 외부주문관련 계약서 및 계약서 부속자료 등으로 한정
- 자료제출 요구시 전자금융보조업자는 특별한 이유가 없는 한 자료제출에 응하여야 함

4. 업무보고서

〈 감독규정 〉

제62조(업무보고서의 제출) ① 법 제42조에 따라 금융회사 및 전자금융업자는 금융감독원장이 정하는 바에 따라 업무보고서를 금융감독원장에게 제출하여야 한다. 다만, 법 제2조제1호에 따른 전자금융업무를 하지 아니하는 금융회사는 그러하지 아니하다.

② 제1항에 따른 업무보고서 제출은 정보통신망(「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」 제2조의 규정에 의한 정보통신망을 말한다)을 이용한 전자문서의 방법에 의할 수 있다.

③ 제1항의 업무보고서 제출에 관한 세부적인 절차, 양식 등에 관해서는 금융감독원장이 별도로 정한다.

〈 시행세칙 〉

제10조(업무보고서의 제출) ① 금융회사 또는 전자금융업자는 규정 제62조에 따른 업무보고서를 분기말 현재로 작성하여 매분기 종료 후 45일 이내에 감독원장에게 제출하여야 한다.

② 업무보고서 양식 및 기재사항은 별지 제1호서식에 따른다.

※ 관계 법령

〈 법 〉

제39조(감독 및 검사) ①금융감독원(「금융위원회의 설치 등에 관한 법률」 제24조제1항의 규정에 따른 "금융감독원"을 말한다. 이하 같다)은 금융위원회의 지시를 받아 금융회사 및 전자금융업자에 대하여 이 법 또는 이 법에 의한 명령의 준수여부를 감독한다.

②금융감독원장은 제1항의 규정에 따른 감독을 위하여 필요한 때에는 금융회사 또는 전자금융업자로 하여금 그 업무 및 재무상태에 관한 보고를 하게 할 수 있다.

▣ 금융회사 및 전자금융업자의 전자화폐 발행, 선불전자지급수단발행 및 전자지급결제대행 등의 이용현황과 전자금융업자의 재무현황 등의 상시 감시를 위하여 주기적으로 업무보고서를 받음

▣ 해설

● 총 19개의 업무보고서가 있으며, 보고서의 성격에 따라 연간, 반기, 분기로 보고주기가 결정됨

〈 업무보고서 목록 〉

번호	보고서명	작성 주기
1	회사 일반현황	년간
2	인원 및 지점현황	년간
3	대차대조표(총괄)	반기
4	손익계산서	반기
5	전자금융업 영업실적 보고서	반기
6	투자위험성이 낮은 자산현황	반기
7	전자금융사고 책임이행보험 가입(준비금적립) 현황	반기
8	정보기술 및 정보보호부문 인력현황	반기
9	정보기술 및 정보보호부문 예산현황	반기
10	CISO(정보보호최고책임자) 지정현황	반기
11	전자금융거래를 위한 외부주문 현황	반기
12	전자화폐 발행 및 이용현황	분기
13	선불전자지급수단 발행 및 이용현황	분기
14	직불전자지급수단 발행 및 이용현황	분기
15	전자지급결제대행 이용현황	분기
16	결제대금예치 이용현황	분기
17	전자고지결제 이용현황	분기
18	전자채권 등록 현황	분기
19	경영지도기준 보고서	반기

* (1~6) : 전자금융업자만 작성(금융회사 작성제외)
* (7~19) : 해당업 영위를 위해 허가·등록(면제포함)업자 작성(금융회사, 전자금융업자)

● 업무보고서의 제출기한은 매분기 종료 후 45일 이내임

– 보고서 제출방식은 금융감독원의 '금융정보교환망(FINES; Financial Information Exchange System)'에 접속하여 항목별로 직접 보고자료를 입력하는 것을 원칙으로 하되, 불가피한 경우 서면보고도 가능

● 금융감독원장은 정기적인 업무보고서외에 감독상 필요한 사항에 대해 자료제출을 요구할 수 있으며, 금융회사 및 전자금융업자는 자료제출 요구에 응하여야 함

※ 금융회사의 경우 기존 개별 금융업법(은행법, 자본시장법, 보험업법, 여신전문금융업법, 상호저축은행법 등)에 따라 금감원 감독 각국으로 보고하던 전자금융보고서 이외 전자금융거래법에 따른 전자금융업무 보고서도 작성(관련 전자금융업무를 하는 경우에 한함)하여 보고하여야 함

5. 경영지도기준

〈 감독규정 〉

제63조(전자금융업자 경영지도기준) ① 법 제42조제2항에 따른 구체적인 경영지도기준은 다음과 같다.

1. 법 제30조 및 시행령 제17조에 따른 허가나 등록요건 상 최소자본금·출자총액 또는 기본재산 기준을 항상 충족할 것
2. 총자산에서 총부채를 감한 자기자본이 항상 0을 초과할 것
3. 미상환잔액 대비 자기자본 비율은 100분의 20 이상일 것(전자화폐 및 선불전자지급수단 발행자에 한한다)
4. 총자산 대비 투자위험성이 낮은 자산의 비율은 100분의 10 이상으로 유지하거나 미정산 잔액 대비 투자위험성이 낮은 자산의 비율을 100분의 100 이상으로 유지할 것. 단, 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자 및 법 제28조제2항제3호의 규정에 따라 등록을 한 전자금융업자는 제외한다. 이 때 투자위험성이 낮은 자산은 〈별표 6〉와 같다.
5. 유동성 비율은 다음 각 목과 같이 유지할 것
   가. 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자 : 100분의 60 이상
   나. 법 제28조제2항제3호의 규정에 따라 등록을 한 전자금융업자 : 100분의 50 이상
   다. 그 밖의 등록대상 전자금융업자 : 100분의 40 이상

② 제1항에서 정하는 비율의 구체적 산정기준은 금융감독원장이 정한다.

③ 금융감독원장은 제1항의 경영지도비율이 악화될 우려가 있거나 경영상 취약부문이 있다고 판단되는 전자금융업자에 대하여 이의 개선을 위한 계획 또는 약정서를 제출토록 하거나 해당 전자금융업자와 경영개선협약을 체결할 수 있다. 다만, 제64조 부터 제66조까지의 규정에 의한 경영개선권고, 경영개선요구 또는 경영개선명령을 받고 있는 전자금융업자의 경우에는 그러하지 아니하다.

〈 시행세칙 〉

제11조(경영지도비율 산정기준) 규정 제63조제2항에 따른 경영지도비율의 구체적 산정기준은 별표 6과 같다.

▣ 경영지도기준은 금융감독당국이 사전적으로 금융회사 및 전자금융업자에 기본이 되는 경영지표를 제시하여, 건전경영을 유지하고 사후적으로 감독상의 보상과 제재를 통해 책임경영을 도모하려는 취지로 도입

※ 관계 법령

〈 법 〉

제42조(회계처리 구분 및 건전경영지도) ①금융회사 및 전자금융업자는 자금운용과 전자금융거래와 관련한 업무의 성과를 분석할 수 있도록 제28조제1항 및 제2항에 규정된 업무별로 다른 업무와 구분하여 회계처리하고, 금융위원회가 정하는 바에 따라 전자금융거래와 관련한 업무 및 경영실적에 관한 보고서를 작성하여 금융위원회에 제출하여야 한다.

②금융위원회는 전자금융거래와 관련한 업무를 수행하는 금융회사 또는 전자금융업자의 건전경영을 지도하고 전자금융사고를 예방하기 위하여 대통령령이 정하는 바에 따라 다음 각 호의 사항에 관한 경영지도기준을 정할 수 있다.

1. 자본의 적정성에 관한 사항
2. 자산의 건전성에 관한 사항
3. 유동성에 관한 사항
4. 그 밖에 경영의 건전성 확보를 위하여 필요한 사항

③금융위원회는 제28조제1항의 규정에 따라 허가를 받은 금융회사 또는 전자금융업자가 제2항의 경영지도기준을 충족하지 못하는 등 경영의 건전성을 크게 해할 우려가 있다고 인정하는 때에는 자본금의 증액, 이익배당의 제한 등 경영개선을 위하여 필요한 조치를 요구할 수 있다.

④제28조제1항의 규정에 따라 허가를 받은 금융회사 또는 전자금융업자의 재무상태가 제2항의 경영지도기준에 미달하거나 거액의 금융사고 또는 부실채권의 발생으로 인하여 제2항의 경영지도기준에 미달하게 될 것이 명백하다고 판단되는 때에 필요한 조치 등에 관하여는 「금융산업의 구조개선에 관한 법률」제10조, 제11조제1항·제4항·제5항, 제13조의2, 제14조, 제14조의2부터 제14조의4까지, 제14조의7, 제15조부터 제19조까지, 제27조 및 제28조를 준용한다.

〈 시행령 〉

제24조(경영지도의 기준) 법 제42조제2항에 따른 경영지도의 기준에는 다음 각 호의 사항이 포함되어야 한다. 〈개정 2012.5.7.〉

1. 법 제28조 또는 법 제29조에 따른 허가 또는 등록의 요건인 자본금의 유지에 관한 사항
2. 자기자본의 보유기준에 관한 사항
3. 유동성부채에 대한 유동성자산의 보유기준에 관한 사항
4. 총자산 대비 투자위험성이 낮은 자산의 비율에 관한 사항(선불전자지급수단의 발행인 및 전자화폐발행자의 경우는 제외한다)
5. 미상환잔액 대비 자기자본의 비율에 관한 사항(선불전자지급수단의 발행인 및 전자화폐발행자에 한한다)

▣ 해설

- 전자금융업자는 금융위가 정하는 자본적정성, 자산건전성 등을 준수하여야 하며, 금융감독원장은 경영지도비율이 악화될 우려가 있거나 경영상 취약부문이 있다고 판단되는 전자금융업자에 대하여 경영개선계획이나 약정서를 제출토록 할 수 있음

〈 경영지도기준 요약표 〉

구 분	내 용	기 준
자본적정성	최소자본금 유지	허가·등록시 자본금요건 항시충족
	자기자본 유지	총자산이 총부채보다 항상 클 것
	미상환잔액 대비 자기자본비율*	20% 이상 (전자화폐, 선불전자지급수단발행업에만 적용)
자산건전성	총자산 대비 투자위험도가 낮은 자산비율	20% 이상 (전자화폐, 선불전자지급수단발행업에만 적용)
		10% 이상(이외 전자금융업)
유동성	유동부채 대비 유동자산비율	60% 이상 (전자화폐발행업에만 적용)
		50% 이상 (선불전자지급수단발행업에만 적용)
		40% 이상 (이외 전자금융업)

* 미상환잔액 대비 자기자본비율 = $\frac{\text{자기자본}}{\text{미상환잔액}} \times 100$

** 금융회사는 경영지도기준의 적용을 받지 않음

6. 적기시정조치

〈 감독규정 〉

제64조(경영개선권고) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당되는 경우에는 해당 전자금융업자에 대하여 필요한 조치를 이행하도록 권고하여야 한다.

1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 20 미만인 경우
2. 거액의 금융사고 또는 부실채권의 발생으로 제1호의 기준에 해당될 것이 명백하다고 판단되는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다.

1. 인력 및 조직운영의 개선
2. 경비절감
3. 고정자산투자, 신규업무영역에의 진출 및 신규출자의 제한
4. 부실자산의 처분
5. 자본금의 증액 또는 감액
6. 이익배당의 제한
7. 특별대손충당금의 설정

③ 금융위원회는 제1항에 의한 권고를 하는 경우 해당 전자금융업자 및 관련 임원에 대하여 주의 또는 경고 조치를 취할 수 있다.

제65조(경영개선요구) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당되는 경우에는 해당 전자금융업자에 대하여 필요한 조치를 이행하도록 요구하여야 한다.

1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 10 미만인 경우

2. 거액의 금융사고 또는 부실채권의 발생으로 제1호의 기준에 해당될 것이 명백하다고 판단되는 경우
3. 제64조제1항의 규정에 의해 경영개선권고를 받은 전자금융업자가 경영개선계획의 주요사항을 이행하지 않아 제69조제8항의 규정에 의해 이행촉구를 받았음에도 이를 이행하지 아니하는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다.

1. 조직의 축소
2. 위험자산의 보유제한 및 처분
3. 자회사의 정리
4. 임원진 교체 요구
5. 영업의 일부정지
6. 합병, 제3자 인수, 영업의 전부 또는 일부 양도계획의 수립
7. 제64조제2항에서 정하는 사항

제66조(경영개선명령) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당하는 경우에는 해당 전자금융업자에 대해 필요한 조치를 이행하도록 명령하여야 한다.

1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 5 미만인 경우
2. 제65조제1항의 규정에 의해 경영개선요구를 받은 전자금융업자가 경영개선계획의 주요사항을 이행하지 않아 제69조제8항의 규정에 의해 이행촉구를 받았음에도 이를 이행하지 아니하거나 이행이 곤란하여 정상적인 경영이 어려울 것으로 인정되는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다. 다만, 영업의 전부정지, 영업의 전부양도, 계약의 전부이전 또는 주식의 전부소각의 조치는 제1항제1호의 기준에 미달하고 건전한 전자금융거래질서나 이용자의 권익을 해할 우려가 현저하다고 인정되는 경우에 한한다.

1. 주식의 전부 또는 일부 소각
2. 임원의 직무집행 정지 및 관리인의 선임
3. 6월 이내의 영업의 정지
4. 계약의 전부 또는 일부의 이전
5. 제65조제2항에서 정하는 사항

▣ 허가를 받은 금융회사 및 전자금융업자가 경영지도기준을 충족하지 못할 경우 금융위는 경영개선을 위해 필요한 조치를 요구할 수 있음(법 제42조)

▣ 적기시정조치란 금융회사(전자금융업자)의 건전성을 자본충실도, 경영실태평가 결과 등 경영상태를 기준으로 몇 단계의 등급으로 나누어, 경영상태가 악화된 금융회사에 대해 금융감독당국이 단계적으로 시정조치를 부과해 나가는 제도를 의미함

- 적시시정조치는 부실화 징후가 있는 금융회사에 대하여 적기에 경영개선을 유도 강제함으로써 부실화를 예방하고 경영취약부문의 정상화를 도모하는 건전성감독 수단으로서의 성격을 지님

▣ 금융위는 허가를 받은 전자화폐업자가 경영지도기준을 충족하지 못하는 등 경영 건전성이 크게 훼손될 우려가 있다고 인정하는 경우 인력 및 조직운영의 개선, 조직의 축소, 주식의 전부 및 일부 소각 등 단계적으로 필요한 조치를 취할 수 있음

▣ 해설

● 경영개선권고는 가장 낮은 단계의 적기시정조치로서 금융위가 권고의 주체가 됨

– 금융위는 경영개선권고 대상인 금융회사 및 전자금융업자에 대하여 조직, 인력 운용의 개선, 자본금의 증액 또는 감액 및 신규업무 제한 등을 권고할 수 있음

● 경영개선요구는 경영개선권고보다 한 단계 높은 강도의 적기시정조치로서 금융위가 조치권자가 됨

– 금융위는 경영개선요구 대상인 금융회사 및 전자금융업자에 대하여 조직의 축소, 점포폐쇄 및 신설제한, 임원진 교체 요구, 영업의 일부 정지 등의 조치를 취할 수 있음

● 경영개선명령은 부실정도가 심한 경우에 내릴 수 있는 가장 강력한 적기시정조치로서 적기시정조치가 퇴출수단으로 활용될 수 있는 단계이며, 경영개선요구와 마찬가지로 금융위가 조치권자가 됨

– 금융위는 경영개선명령 대상인 전자화폐업자에 대하여 주식 소각, 영업의 정지 및 양도, 외부 관리인 선임 및 합병 등의 조치를 취할 수 있음

– 경영개선요구가 부과된 전자화폐업자가 경영개선의 주요사항을 이행하지 않아 이행 촉구를 받았음에도 이를 이행하지 아니하거나 이행이 곤란하여 정상적인 영업이 어려울 것으로 인정되는 경우 발동

전자금융감독규정 해설

7장 보 칙

제7장 보 칙

1. 정보기술부문 및 전자금융사고 보고

〈 감독규정 〉

제73조(정보기술부문 및 전자금융 사고보고) ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다.

1. 정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무가 중단 또는 지연된 경우
2. 전산자료 또는 프로그램의 조작과 관련된 금융사고가 발생한 경우
3. 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로인해 이용자가 금전적 피해를 입었다고 금융회사 또는 전자금융업자에게 통지한 경우
4. 법 제9조제1항의 규정에서 정하는 사고

② 금융회사 및 전자금융업자는 제1항에 따른 사고보고를 고의로 지연하거나 숨긴 자에 대하여 소정절차에 따라 징계 등 필요한 조치를 취하여야 한다.

③ 금융감독원장은 제1항에 따라 보고 받은 내용을 지체 없이 금융위원장에게 보고하여야 하며, 제1항 제3호에 따른 사고 발생시에는 제37조의4제1항 각 호에 따른 침해사고대응기관에도 알려야 한다.

④ 제1항의 사고보고와 관련하여 사고보고 절차 및 방법 등 세부사항은 금융감독원장이 정하는 바에 따른다.

〈 시행세칙 〉

제12조(정보기술부문 사고보고) ① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융 사고가 발생한 경우 별지 제2호서식에 따라 즉시 보고하여야 한다.

② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다.

1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다.
2. 중간보고 : 제1호의 즉시보고 후 제3호의 조치완료 시까지 2월 이상 소요될 경우에는 인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다.
3. 종결보고 : 피해금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다.

③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다.

④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.

▣ 전자금융감독규정 제73조에서 명시한 『중대한 사고』의 기준(추후 변동 가능)

① 10분 이상 전산업무 지연 및 중단

- 대상 : 대고객 업무
- 영향도 : 영업점 2개 점포 이상 동시 영향 시

보고대상	예시
O	A통신사 회선 장애로 대고객 ARS 인증 서비스 10분간 불능
O	ELW LP시스템 장애로 호가제출이 10분간 정지
O	인터넷 뱅킹 서비스 중 적금계좌 조회가 10분간 불능
O	자행 공인인증서 로그인은 가능 하지만, 타행 인증서 로그인이 10분간 불가
X	B 영업점 ATM기 2대 장애로 30분간 사용 불능
X	건물 일시 정전으로 인해 C 영업점 10분간 업무 정지
X	직원 E-Mail서버가 다운되어 30분간 관련 업무 불가 (고객 서비스에는 아무런 영향이 없음)
X	주말·야간 시스템 점검 등 고객에게 사전 공지한 업무중단의 경우
X	D 위수탁사의 시스템 장애의 여파로 E, F 카드사의 카드 결제 업무 불가(D 위수탁사가 금융회사, 또는 전자금융업자로 시스템 장애에 대한 사항 및 E, F 카드사의 결제업무 불가 사항을 포함하여 EFARS에 기 보고 완료한 경우 E, F 카드사는 사고 보고를 할 필요가 없음)
O	G 위수탁사의 시스템 장애의 여파로 H, I 은행 모바일 뱅킹 10분간 정지 (G 위수탁사가 금융회사, 또는 전자금융업자가 아니어서 사고 보고 대상이 아닌 경우, H, I 은행 모두 사고 보고 필요)

② 전산자료 및 프로그램 조작과 관련된 금융사고 발생시

- 범위 : 조작의 고의성과 상관없이 보고

※ 단 업무 처리과정에서 일상적·반복적으로 발생하는 사고로서 고객의 인지 및 피해가 발생하지 않는 경우는 제외

보고대상	예시
O	프로그램 오류로 인해 보통예금 계좌의 이자 100원이 누락된 경우
O	개발자의 실수로 인해 DB 정보가 잘못 업데이트 되어 서비스에 영향
X	새벽1시 이자지급을 위한 배치작업 수행 후 결과를 확인하는 과정에서 오류가 발견되어 배치작업 재수행

③ 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로 인해 이용자가 금전적 피해를 입었다고 금융기관에 통지한 경우

- 대상 : DDoS 피해, 해킹으로 인한 사고(정보유출, 시스템 장애, 시스템 변조, 금융사고 등)

보고대상	예시
O	해킹으로 인해 금융회사 홈페이지가 변조
O	해킹으로 인해 금융회사 고객정보가 유출 또는 원장정보의 일부 삭제
X	고객정보가 담긴 출력물, USB를 외주직원이 유출 * 전자금융사고 보고 대상은 아니나, 소관 검사국에는 보고

④ 법 제9조제1항의 규정에서 정하는 사고

- 대상 : 카드위변조, 보이스 피싱, 파밍, 악성코드 등으로 획득한 접근매체(공인인증서, 복제카드 등)를 이용하여 전자금융거래(계좌이체, 온라인 결제 등)가 발생한 경우
- 범위 : 금액에 상관없이 신고한 경우 보고

보고대상	예시
O	보이스피싱으로 획득한 정보를 이용하여 제3자가 게임사이트에서 계좌이체를 이용한 결제가 발생한 경우
O	공인인증서 부정재발급으로 이용자에게 손해가 발생한 경우
X	보이스피싱으로 피해자가 직접 계좌이체를 수행한 경우