공 개

의안번호	제 376 호
의 결 연 월 일	2026. 8. 4. (제 1 차 서면)

의결사항

금융보안원에 대한 전기통신금융사기 정보공유분석기관 지정안

금융위원회회의 안건

제 출 자	위원장 이 억 원
제출 연월일	2026. 8. 4.

1. 의결주문

금융보안원에 대한 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」(법률 제21320호, 2026.2.3. 공포, 2026.8.4. 시행. 이하 같다) 제13조의4에 따른 전기통신금융사기 정보공유분석기관 지정안을 별지와 같이 의결한다.

2. 제안이유

금융보안원이 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」제13조의4에 따른 전기통신금융사기 정보공유분석기관 지정을 신청해옴에 따라 이를 검토하여 지정하고자 하는 것임

3. 주요내용

금융보안원의 전기통신금융사기 정보공유분석기관 지정 요건 충족여부를 검토한 결과 요건을 모두 충족하고 있으므로, 동사를 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」제13조의4에 따른 전기통신금융사기 정보공유분석기관으로 지정하고자 함

4. 참고사항

가. 관련 법령 : 【붙임】 참조

5. 안건 공개여부 : 공개

(별지)

금융보안원의 전기통신금융사기 정보공유분석기관 지정

금융보안원의 전기통신금융사기 정보공유분석기관 지정 신청에 대하여 다음과 같이 지정한다.

- 다 음 -

1. 상 호 : 금융보안원

2. 지정 내용 : 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」제13조의4에 따른 전기통신금융사기 정보공유분석기관

3. 지정일 : 2026. 8. 4.

【붙임】

관련 법령

<전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 시행령>

제10조의5(정보공유분석기관의 지정 등) ① 법 제13조의4제1항에 따라 정보공유분석기관(같은 항 각 호 외의 부분에 따른 정보공유분석기관을 말한다. 이하 같다)으로 지정받으려는 자는 다음 각 호의 요건을 모두 갖추어야 한다.

1. 「민법」 제32조에 따라 설립된 비영리법인일 것
2. 전기통신금융사기에 관한 정보의 분석 및 제공 업무를 수행하기에 충분한 전산설비 및 인력을 갖출 것
3. 전기통신금융사기에 관한 정보의 분석 및 제공 업무를 수행하기 위한 운영기준을 마련할 것
4. 전기통신금융사기에 관한 정보의 유출 및 전기통신금융사기에 관한 정보를 처리하는 기반시설에 대한 침해사고 등을 방지하기 위한 위험관리체계와 내부통제장치가 마련되어 있을 것
5. 건전한 재무상태 및 사회적 신용을 갖추고 있을 것

② 제1항에 따른 지정 요건에 관한 세부 사항은 금융위원회가 정하여 고시한다.

<전기통신금융사기 피해방지에 관한 규정>

제6조(정보공유분석기관 지정 등에 관한 세부사항) ① 영 제10조의5제2항에 따른 정보공유분석기관 지정 요건에 관한 세부사항은 별표 1과 같다.

② 영 제10조의5제3항 각 호 외의 부분에서 “금융위원회가 정하여 고시하는 지정신청서”란 별지 제1호서식을 말한다.

③ 금융위원회는 금융감독원장으로 하여금 제2항에 따른 신청내용이 영 제10조의5제1항 및 제2항에 따른 지정 요건을 충족하는지 심사하게 할 수 있다.

④ 영 제10조의5제4항에서 “금융위원회가 정하여 고시하는 지정서”란 별지 제2호서식을 말한다.

제9조(기술적·물리적·관리적 보안대책) 영 제10조의6제8항 각 호외의 부분 후단에 따라 정보공유분석기관이 수립·시행하여야 할 기술적·물리적·관리적 대책의 구체적인 기준은 별표 2와 같다.

[별표 1]

정보공유분석기관 지정의 세부요건 (제6조제1항 관련)

Ⅰ. 인력 및 조직

가. 정보공유분석기관의 역할을 적절히 수행하기 위한 전문성을 갖춘 다음의 어느 하나에 해당하는 인력을 8명 이상 상시 고용하고, 데이터 및 보안 전문인력, 법률 전문인력을 각각 최소 2명 이상 포함할 것

(1) 데이터 및 보안 전문인력

①. 「국가기술자격법」에 따른 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사 자격을 취득한 자로서 2년 이상 관련 업무(개인정보 보호, 데이터 공유·분석·활용 등 업무. 이하 (1)에서 같다)를 수행한 경력이 있는 자

②. 관련 분야(컴퓨터공학, 정보보호학, 데이터베이스공학, 통계학, 수학 등 이하 (1)에서 같다)에서 박사 학위를 취득한 자로서 2년 이상 관련 업무를 수행한 경력이 있는 자

③. 관련 분야에서 석사 학위를 취득한 자로서, 4년 이상 관련 업무를 수행한 경력이 있는 자

④. 관련 분야에서 학사 학위를 취득한 자로서 6년 이상 관련 업무를 수행한 경력이 있는 자

⑤. 관련 분야에서 8년 이상 관련 업무를 수행한 경력이 있는 자

(2) 법률 전문인력

①. 변호사의 자격을 소지한 자로서 1년 이상 관련 법률 업무(개인정보 보호, 데이터 공유·분석·활용 등 관련 법률 자문 또는 지원 업무. 이하 (2)에서 같다)를 수행한 경력이 있는 자

②. 법학박사 학위를 취득한 자로서 2년 이상 관련 법률 업무를 수행한 경력이 있는 자

③. 법학석사 학위를 취득한 자로서 4년 이상 관련 법률 업무를 수행한 경력이 있는 자

④. 법학학사 학위를 취득한 자로서 6년 이상 관련 법률 업무를 수행한 경력이 있는 자

⑤. 8년 이상 관련 법률 업무를 수행한 경력이 있는 자

나. 정보공유분석기관의 임원이 다음을 충족할 것.

①. 최근 5년간 「신용정보의 이용 및 보호에 관한 법률」 제25조제2항제1호에 따른 종합신용정보집중기관에 같은 법 제2조제1호의4나목에 해당하는 정보가 등록된 사실이 없을 것

②. 「금융회사의 지배구조에 관한 법률」 제5조제1항 각 호의 어느 하나에 해당하지 아니할 것. 이 경우 "금융관계법령"은 금융관계법령 및 「개인정보보호법」으로 본다.

Ⅱ. 시설 및 설비

가. 전산설비

구성	세부 요건
시스템 구성	1. 시스템 구성에 다음 항목을 포함할 것 가. D/B서버 나. WEB서버 다. 통신서버 라. 보안서버 및 통신구간 암호화 시스템 마. 그 밖의 주변장치 2. 백업 및 복구시스템 3. 시스템 보안 및 시설 보안을 포함한 보안관리 체계
시스템 성능	1. 사기정보제공기관으로부터의 통신사기정보 수집 및 사기정보이용기관에의 제공을 적절하게 처리할 수 있는 성능을 갖출 것 2. 보유한 통신사기정보를 적절하게 분석·활용할 수 있는 성능을 갖출 것 3. 백업 및 복구작업이 최소한의 시간내에 가능할 것
보안체계	1. 방화벽(Fire-Wall)을 갖출 것 2. 침입을 탐지·경고·차단할 수 있는 보안시스템을 갖출 것 3. 인터넷 및 내부 업무용 네트워크와 통신사기정보의 공유·분석을 위한 네트워크를 분리하여 운용할 것 4. 정보이용자 확인 체계(사용자 인증)를 갖출 것 5. 데이터 암호화처리 체계를 갖출 것 6. 외부침입 방지, 출입자관리 통제 및 데이터 반출·반입 통제에 대한 대책을 강구할 것 7. 백업 및 소산관리 대책을 강구할 것

나. 업무공간과 사무장비

(1) 통신사기정보를 안전하게 공유·분석하기 위한 전용 시스템 및 분리된 사무공간을 갖출 것

(2) 정보공유분석기관 업무 수행 인원 대비 충분한 업무공간 및 사무장비를 갖출 것

(3) 내부기관 및 감독기관 등이 감독·검사업무를 수행함에 있어 법적 장애가 없을 것

다. 업무의 연속성을 유지할 수 있는 보완설비

(1) 파업 등 불시사태 또는 비상사태에 대비한 비상계획(Contingency Plan)이 마련되어 있을 것

Ⅲ. 재정능력 및 관리체계

가. 신청인의 기본재산이 80억원 이상일 것

나. 신청인의 설립 취지와 현재 영위하고 있는 사업영역이 정보공유분석기관의 업무 수행에 적합할 것

다. 통신사기정보를 안전한 수집·제공·관리·분석 및 파기하기 위한 위험관리체계 및 내부통제장지를 마련할 것

[별표 2]

기술적·물리적·관리적 보안대책 마련 기준 (제9조 관련)

Ⅰ. 목 적

이 기준은 제9조에서 정하는 통신사기정보 처리의 안전성 확보를 위한 기술적·물리적·관리적 대책의 구체적인 기준을 정함을 목적으로 한다.

Ⅱ. 기술적·물리적·관리적 보안대책

1. 접근통제

① 정보공유분석기관은 통신사기정보를 처리하는 전산시스템(이하 "통신사기정보처리시스템"이라 한다)에 대한 접근권한을 전기통신금융사기 정보의 분석 및 제공 업무에 필요한 최소한의 인원에게만 부여한다.

② 정보공유분석기관은 전보 또는 퇴직 등 인사이동이 발생하여 통신사기정보를 처리하는 업무를 담당하는 자(이하 "통신사기정보취급자"라 한다)가 변경되었을 경우 지체 없이 통신사기정보처리시스템의 접근권한을 변경 또는 말소한다.

③ 정보공유분석기관은 제1항 및 제2항에 따른 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.

④ 정보공유분석기관은 통신사기정보처리시스템에 침입차단시스템과 침입탐지시스템을 설치하여 보호한다.

⑤ 정보공유분석기관은 통신사기정보취급자가 추측하기 쉬운 단어나 숫자를 비밀번호로 이용하지 않도록 비밀번호 작성규칙을 수립하고 이행한다.

⑥ 정보공유분석기관은 취급 중인 통신사기정보가 권한이 없는 제3자가 접근할 수 없도록 통신사기정보처리시스템 및 통신사기정보취급자의 정보처리기기를 설정한다.

⑦ 정보공유분석기관은 통신사기정보처리시스템 관련 개발업무에 사용되는 업무장소 및 전산설비는 운영업무용과 분리하여 설치·운영한다.

⑧ 정보공유분석기관은 업무목적을 위하여 불가피한 경우에만 외부사용자에게 통신사기정보처리시스템에 대한 최소한의 접근권한을 부여하고, 권한 부여에 관한 기록을 3년 이상 보관하는 등 적절한 통제시스템을 갖추어야 한다.

2. 접속기록의 위·변조방지

① 정보공유분석기관은 통신사기정보취급자가 통신사기정보처리시스템에 접속하여 통신사기정보를 처리한 경우에는 처리일시, 처리내역 등 접속기록을 저장하고 이를

월 1회 이상 정기적으로 확인·감독한다.

② 정보공유분석기관은 통신사기정보처리시스템의 접속기록을 1년 이상 저장하고, 위·변조되지 않도록 별도 저장장치에 백업 보관한다.

3. 통신사기정보의 암호화 처리 및 외부망 분리

① 정보공유분석기관은 사기정보제공기관 및 사기정보이용기관과 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다)으로 통신사기정보를 송·수신하여야 하며, 보안서버 구축 등의 조치를 통해 통신사기정보를 암호화하여야 한다. 보안서버는 다음 각 호의 어느 하나의 기능을 갖추어야 한다.

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

② 정보공유분석기관은 통신사기정보를 PC에 저장할 때에는 이를 암호화해야 한다.

③ 정보공유분석기관은 다음 각 호의 기준에 따라 개인식별정보의 암호화 등의 조치를 취하여야 한다.

1. 정보통신망을 통하여 송수신하거나 보조저장매체를 통하여 전달하는 경우에는 암호화하여야 한다.
2. 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone) 에 저장할 때에는 암호화하여야 한다.
3. 정보공유분석기관이 내부망에 개인식별정보를 저장하는 경우에는 암호화하여야 한다.
4. 업무용 컴퓨터에 저장하여 관리하는 경우에는 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화하여야 한다.

4. 컴퓨터바이러스 방지

① 정보공유분석기관은 통신사기정보처리시스템 및 통신사기정보취급자의 정보처리기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 한다.

② 제1항에 따른 백신 소프트웨어는 월 1회 이상 주기적으로 갱신·점검하고, 바이러스 경보가 발령된 경우 및 백신 소프트웨어 제작 업체에서 업데이트 공지를 한 경우에는 즉시 최신 소프트웨어로 갱신·점검하여야 한다.

5. 출력·복사시 보호조치

① 정보공유분석기관은 통신사기정보처리시스템에서 통신사기정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화한다.

② 정보공유분석기관은 통신사기정보를 조회하는 경우 조회자의 신원, 조회일시, 대상정보, 목적, 용도 등의 기록을 관리하여야 하며, 영 제10조의4제14항에 따른 운영기준에 따라 사기정보이용기관에 통신사기정보를 제공하는 경우 이외의 경우로서 통신사기정보취급자가 통신사기정보를 보조저장매체에 저장하거나 이메일 등의 방법으로 외부에 전송하는 경우에는 관리책임자의 사전 승인을 받아야 한다.

③ 통신사기정보취급자는 제1항 및 제2항의 준수에 필요한 내부시스템을 구축하여야 하며 사전 승인시 승인신청자에게 관련 법령을 준수하여야 한다는 사실을 주지시켜야 한다.

6. 통신사기정보보호최고책임자 지정

① 정보공유분석기관은 다음 각 호의 업무를 담당하는 통신사기정보보호책임자를 지정하여야 한다. 이 경우 통신사기정보보호최고책임자는 임원인 자로 지정하여야 하며, 「개인정보 보호법」 또는 「전자금융거래법」에 따른 정보보호최고책임자, 「신용정보의 이용 및 보호에 관한 법률」에 따른 신용정보관리·보호인을 겸임할 수 있다.

1. 통신사기정보의 관리 및 보호 계획의 수립 및 시행
2. 통신사기정보의 관리 및 보호 실태, 관련 법령 및 규정 준수 여부에 대한 점검 및 개선
3. 통신사기정보 유출 등을 방지하기 위한 내부통제시스템의 구축 및 운영
4. 통신사기정보취급자에 대한 관리·감독 및 교육
5. 통신사기정보 처리업무를 위탁하는 경우 수탁자의 관리 및 감독
6. 통신사기정보 열람 및 정정청구 등 정보주체의 권리행사 및 피해구제
7. 통신사기정보 유출시 대응 계획의 수립 및 시행

② 통신사기정보보호책임자는 제1항의 업무처리에 따른 기록을 3년간 보존하며, 점검결과를 최고경영자에 보고하고 업무처리절차에 적절히 반영하여야 한다.

7. 제재기준 마련

정보공유분석기관은 통신사기정보의 유출 및 오·남용에 대한 자체 제재기준을 마련하여야 한다.

< 의안 소관 부서명 >

	금융위원회	금융감독원
소관부서	금융안전과	금융사기대응단
연 락 처	02-2100-2975	02-3145-8150