금융보안원 종합감사 결과

2020. 2.

금 융 위 원 회

감사담당관실

목 차

Ⅰ. 감사실시 개요

□ 법적근거

○ **민법 제37조* 및 금융위 소관 비영리법인 설립·감독규칙**(총리령) **제9조**

* 법인의 사무는 주무관청이 감사, 감독한다.

* 금융보안원은 금융결제원 및 코스콤의 정보공유분석센터와 금융보안연구원의 기능을 통합하여 2015.4.10.에 설립

□ 감사기간 : 2019. 8. 28(수) ~ 9.10(화), 10일(근무일 기준)

* 최근 감사는 '16.5월 실시

□ 감사대상 : 고유사업, 예산·회계, 조직·인력, 임직원 복리, 내부통제 등 조직운영 전반

□ 감사요원 : 감사담당관 외 8명(외부전문가 3명 포함)

□ 감사중점

○ 수행사업의 설립목적 부합성

- 금융권 침해예방 및 대응 등 주요업무 처리실태

○ 예산집행·회계처리, 자금관리, 계약사무의 적정성

○ 인력 및 조직관리 실태

○ 임직원 보수·복리후생 지원의 적정성

○ 정관 등 제규정 준수 여부

○ 내부통제 실효성 등

II. 금융보안원 현황

1. 일반현황

□ 연 혁

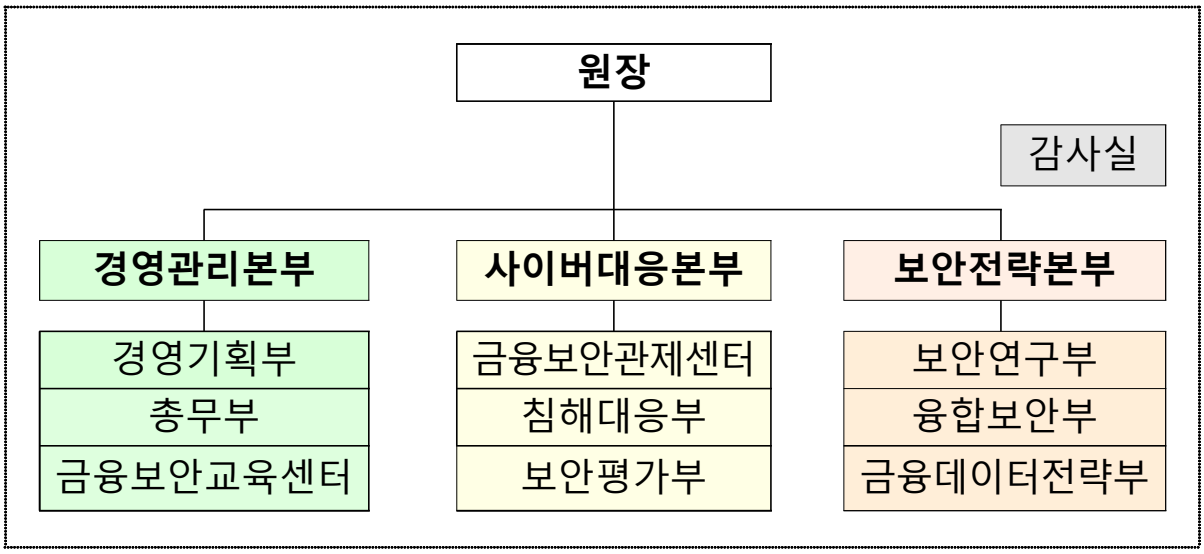
- ○ ’15.3.18. 침해사고대응기관 지정
- ○ ’15.3.31. 금융위원회 비영리사단법인 설립 허가
- ○ ’15.4.3. 금융정보공유·분석센터(금융ISAC) 구축 통지
- ○ ’15.4.10. 사단법인 금융보안원 출범
- ○ ’15.7.10. 정보보호관리체계(ISMS) 인증기관 지정
- ○ ’16.8.31. 금융분야 개인정보 비식별조치 지원 전문기관 지정
- ○ ’19.7.1. 정보보호 및 개인정보보호 관리체계(ISMS-P)통합 인증기관 지정

□ 소재지 : 경기도 용인시 수지구 대지로 132

□ 조직/인원 : 3본부 7부 1실 2센터 29팀, 총 211명(임원 포함)

* **원장**(상 근) : 김영기(63년생) / 성균관대(경영), 금융감독원 부원장보
감사(비상근) : 임석재(63년생) / 방송통신대(경영), 신한카드 상무(CISO), 신한데이터시스템 정보보호본부장(現)

<금융보안원 조직도>



2. 주요업무 추진실적

구분	2016년도	2017년도	2018년도
금융권 침해위협 분석 및 대응 강화			
전자적 침해시도 분석	196만여 건	1,046만여 건	773만여 건
전자적 침해시도 대응	37만여 건	66만여 건	176만여 건
피싱사이트 탐지	5,101건	5,372건	18,422건
통합보안관제 실시기관	186개 기관	190개 기관	190개 기관
악성코드 분석	1,418만여 건	3,519만여 건	4,627만여 건
악성코드 대응	24,496건	28,843건	30,994건
침해사고 조사·분석	22개 기관	32개 기관	32개 기관
침해사고 비상대응훈련	467회	509회	501회
침해사고 대응·복구 훈련 결과 점검	268개 기관	259개 기관	287개 기관
디도스비상대응센터 연동기관	36개 기관	61개 기관	66개 기관
금융권 사이버 위협 인텔리전스보고서 발간	-	2건	2건
금융권 보안사고 예방활동			
이상금융거래정보 공유	897건	956건	138건
취약점 분석·평가	233회	234회	238회
정보보호관리체계 인증 심사	37건	64건	74건
침해 예방 포렌식	-	8개 기관	22개 기관

구분	2016년도	2017년도	2018년도
핀테크 보안·빅데이터 활용 및 보호 지원			
보안성 검토	49건	41건	38건
핀테크 보안상담·컨설팅·수준진단	104건	43건	14건
비대면 실명확인 보안성 테스트	58건	14건	8건
신분증 진위확인 규격적합성 검증	7건	65건	13건
로보어드바이저 보안성 심사	-	28건	9건
오픈플랫폼 취약점 점검	-	39건	78건
개인신용정보 수탁자 점검	-	135건	177건
개인정보 비식별 조치 지원	-	56회	10회
금융보안 정책 지원 및 신기술 연구 강화			
금융보안 정책 검토 및 수립 지원	35건	37건	35건
전자금융 및 금융보안 기술 연구	61건	64건	65건
금융당국 등 점검·검사 지원	87개 기관	15개 기관	15개 기관
표준 개발	-	-	10건
금융보안 교육 강화			
사이버 교육 수료	143만여 명	139만여 명	161만여 명
집합 교육 수료	1,813명	2,215명	2,241명

3. 수입·지출예산 및 결산

① 2016~2019년도 수입·지출 예산

□ 수입예산

(단위 : 백만원)

연도	2016	2017	2018	2019
사원회비	40,985	45,422	49,660	54,836

□ 지출예산

(단위 : 백만원)

연도	2016	2017	2018	2019
합계	**40,985**	**45,422**	**49,660**	**54,836**
인건비	18,445	20,273	22,690	24,064
소유물비	150	814	1,695	1,816
경비	11,451	15,591	17,986	21,726
전산업무비	10,585	8,384	6,989	6,930
예비비	354	360	300	300

② 2016~2018년도 결산

□ 재무상태(B/S)

(단위 : 억원)

과 목			2016	2017	2018[2]
자산	유동자산(예금 등)		133	166	187
	금융리스자산[1]		0	125	154
	유형자산(집기 등)		320	306	292
	무형자산(소프트웨어 등)		9	13	19
	기타자산(보증금 등)		23	24	25
	계		**485**	**634**	**677**
부채 및 순자산	부채	장기차입금(사옥매입)	189	185	179
		금융리스부채[1]	0	123	150
		예수금・미지급비용 등	50	50	21
		소계(A)	239	358	350
	순자산	기본순자산(기본재산)	237	250	251
		미처분 잉여금[3]	7	24	73
		처분 잉여금[4]	2	2	3
		소계(B)	246	276	327
	계(A+B)		**485**	**634**	**677**

주1) 2016년 금융위 정기감사 결과에 따라 2017회계연도부터 반영
2) 2018회계연도부터「공익법인회계기준」적용에 따라 양식 등 변경
3) 유형자산 미상각 잔액 및 선급비용 등 회계상 잉여금 포함
4) 고유목적사업준비금 및 ISMS피해보상준비금 적립

III. 감사실시 결과

1 분야별 감사결과

가 인사·보수 제도 및 운영 관련

① 2015・2016년도 신입직원 공개모집 채용관련

□ 금융보안원의 **2015년도 신입사원 채용** 시 서류전형 평가과정에서 “일반기획” 분야와 “정보보호/전산” 분야 지원자의 출신학교를 국내대학은 가·나·다 3개 등급으로, 외국대학은 가·다 2개 등급으로 구분하여 **출신학교를 차별하여 차등 배점**하였으며,

○ 서류전형 시 **자기소개서 부적격 판단 기준에 해당하는 26명의 지원자를 탈락처리 하여야 하였으나, 26명 전원을 서류전형에 합격처리**하였으며, 그 중 1명은 1차 면접까지 합격 처리하는 등 평가기준에 맞지 않게 전형을 실시

□ **2016년도 금융보안원의 신입직원 채용**과 관련하여 각 전형단계별로 **보훈대상자에게 만점이 아닌 명목상의 10점 또는 5점을 가산점으로 부여**하여 평가

○ 자기소개서 심사시에는 **개별 평가항목 중 한 가지 항목만 ‘하’를 받더라도 종합등급을 ‘하’로 평가하는 등 종합등급 평가가 매우 부적정하게 이루어져 지원자 18명이 탈락**하였음

○ 2016년 서류전형 평가시 **‘빅데이터 분석 및 평가’ 분야에서 8명, ‘빅데이터 시스템 운영’ 분야에서 16명이 각각 종합점수에서 고득점을 받았음에도 탈락**하였음

○ 또한, 2차 면접과정에서 채용계획과 상이하게 '빅데이터 분석 및 평가' 분야에서 **당초 채용예정 인원(2명)보다 1명 적게, '정보보호/전산'분야에서 채용 예정 인원(8명)보다 1명을 추가 합격**시키는 등 합리적인 이유나 근거 없이 **채용인원을 임의로 변경**하였음

⇒ **① 향후 채용과정의 공정성 제고를 위해 인사관리규정 등에 따라 채용업무관리를 철저히 할 필요(기관주의)**
② 2015년 신규채용과정에서 학교별 차등 등 채용관리업무 부적정으로 담당부장 ○○○(주의촉구)
③ 2015년 신규채용과정에서 학교별 차등 등 채용관리업무 부적정 및 2016년 신규채용과정에서 채용계획과 달리 임의적인 미경력 지원자 탈락 조치 및 합격인원 변경 등은 업무처리상 중대한 과실에 해당하므로 담당팀장 ○○○(문책요구)
④ 2016년 신규채용과정에서 채용계획과 달리 임의적인 미경력 지원자 탈락 조치 및 합격인원 변경 등은 업무처리상 중대한 과실에 해당하므로 담당부장 ○○○은 인사자료로 활용(인사자료 통보)

② 직급별 정원책정 결정방식 개선 필요

□ 금융보안원 직원 승진임용은 매년초 정기인사를 실시하기 이전에 연도별 총정원 및 인건비 예산범위 내에서 **원장 전결로 직급별 정원 책정을 결정***한 후, 직급별 현원과의 차이(결원)에 따라 **승진 인원 규모**를 산정하고 있으나

○ **직급별 정원 책정**은 상위 직급 증가시 승진 규모 증가로 연결되어 인건비 상승을 초래하는 등으로 이사회 등 상위 회의체에서 **주요한 예산 심의 사항**으로 다루어져야 할 사안임

⇒ **직급별 정원책정은 매년 익년도 예산에 반영하여 이사회 등 상위 회의체의 승인을 받도록 하고, 인사운영의 투명성을 제고하기 위하여 '정·현원 규정'을 마련할 필요 (개선요구)**

③ 승진 인사 인원 배수 운영 일관성 미흡

□ 금융보안원 2017년 제1차 인사위원회('17.2.6)에서 심의한 3급 및 4급 승진인사에서는 현행 규정상 승진후보자 배수를 현실에 맞게 조정이 필요하다는 이유로 **모두 2배수로 배수범위를 조정*** 하여 심의를 하였음

* 현행 규정상 필요한 경우 원장의 승인을 받아 인원 배수 범위 조정이 가능(인사관리규정 제105조⑤단서)

□ 한편, 금융보안원 2019년 제1차 인사위원회('19.1.2)에서 1급 승진 3명 및 2급 승진 2명을 실시하면서, 1급 승진후보자 명부에 부서장과 팀장이, 2급 승진후보자 명부에 팀장과 차장이 상존함에 따라 **일부 특정직책자들이 저평가**된다는 이유로 **승진인원 배수를 조정 (현행 4배수→ 1급 6배수, 2급은 7배수)**하는 등 인사의 **일관성이 미흡**

⇒ **승진인사시 수시로 배수조정이 가능토록 규정되어 인사운영 투명성을 훼손할 소지가 있는 단서조항을 삭제하고, 장기적으로 특정 직책자 저평가 발생 문제 개선방안을 강구할 것(개선요구)**

④ 저성과자 제도 및 임금피크제 운영 부적정

□ 금융보안원은 「중장기 조직활성화를 위한 인사관리방향」('16.12.29, 원장) 등에 의거, **부서장급 2명*에 대한 직책해지를 결정**('17.2.6)하면서, 직원 개개인에게 **사전에 세부절차나 결정기준*을 충분히 고지하는 것이 타당**함에도

* 최근 2개년 내의 1개년 근무성적평정 점수가 하위 20% 이내인 자 중에서 최근 2개년 평균 근무성적평정 또는 관리능력평정 점수가 하위 20%이내인 자 등(부서장급인 경우)

- **사전에 공문이나 공지사항 등을 통한 충분히 공지가 없이** 저성과자 결정기준도 알 수 없는 상황에서 규정 신설 후 다음 연도 초에 **그간의 근무성적(2년내지 1년)만으로 결정하는 것은 합리적인 업무처리라고 보기 어려움**

□ 한편, 금융보안원은 **『임금피크제 운영규정』** 제3조(임금피크제 적용 기준일)에도 근거하지 않는 **'임금피크제 예정 직원*'**이라는 것을 두어 임금피크제 적용일이 도래하지 않은 상황에서도 **사실상 사전에 소급 적용이 가능하도록 운영****

* 연초 정기인사시 당해 연도 및 **익년도 1월에 임금피크제 적용을 받은 직원**을 조사역으로 발령(임금피크제 세부 운영방안 수립, '17.12.26)

** 임금피크제 예정직원의 경우 보수 등 처우면에서 사실상 **직위해지된 저성과자와 유사**함

⇒ 개인신상에 관한 제도 도입시에는 사전에 충분히 공지하고, 현재 시행근거가 미흡하고 고용불안정을 야기할 소지가 있는 "임금피크제 예정직원" 제도는 개선할 필요 (통보)

⑤ 임직원 성과급 지급제도 개선 필요

□ 최근 4년간 금융보안원 임원의 성과연봉 지급을 위한 **성과연봉 지급율*** 현황을 살펴보면 상무 3명의 경우 '18년도 및 '19년도에는 **개인별 격차가 없이 동일하게 성과연봉을 지급**하고 있는 실정

* 성과연봉(성과급) = 기본연봉 × 성과연봉 지급율

□ 한편, 직원 성과급률의 경우 최고등급(370%)과 최저등급(290%)간의 격차가 80%p이지만, 10명수준인 부서장급 정원을 감안할 경우 인원비율상 S등급에 해당되는 인원이 없게 되므로, **사실상 최고등급인 A등급(340%)과 최저등급 격차는 50%p수준에 불과**하고,

○ 인원비율의 경우는 C등급(40%)과 D등급(30%)에 전체인원의 70%가 배정됨에 따라 **실제로는 대대수 직원이 300%수준의 성과상여금이 지급**되므로 공정한 성과보상을 통한 동기유발 및 이를 통한 조직발전이라는 성과상여금 본래의 취지를 구현하기에는 한계가 있음

<성과급률표>

구 분	S등급	A등급	B등급	C등급	D등급
성과급률	370%	340%	310%	**300%**	**290%**
인원비율	5%	10%	15%	**40%**	**30%**

※ A기관(예시) : 개인별 최고등급과 최저등급 차등폭(250%p),
인원배율(S등급 5%, A등급 25%, B등급 40%, C등급 25%, D등급 5%)

⇒ 조직내 성과주의 문화가 확산될 수 있도록 개인별 지급률 차등 확대, 인원비율 조정 등 성과급 제도 개선 필요 (통보)

⑥ 퇴직자 보수 일할계산 적용 필요

□ 금융보안원 임직원이 퇴직하는 경우『보수규정』제16조 및 「임원 보수 및 퇴직금 지급기준」에 따라 해당 퇴직월의 보수 전액을 지급하도록 규정

○ 이에 따라 '16년이후 퇴직자의 퇴직월 보수 지급실태를 살펴보면, 총 4명의 퇴직자의 경우 **해당 근무일수에 따른 일할계산하지 않고 보수 전액을 지급**

⇒ 퇴직자 보수 과다지급 논란이 제기되지 않도록 현행 퇴직자 보수지급제도를 개선할 필요 (개선요구)

나 예산 집행/회계처리

① 금융보안원 회비 납부 지연 개선 필요

□ 최근 3년간 회원사의 금융보안원 회비 지연 납부 내역을 보면 **납부기일을 도과한 사원 비율이 전체의 22.6%~51.9%**에 달하고, **2개월의 유예기간을 도과한 사원 비율도 1.0%~3.3%**가 존재

○ 금융보안원은 회비 납부 지연 사원과 관련하여 이사회의 의결을 거쳐 **미납 회비에 가산금을 부과하거나 사원의 권리에 해당하는 서비스 이용을 제한한 사실이 없음**

□ 한편, 2019년 상반기 회비 납부기일을(2019.1.31.) 3개월여 도과하여 회비를 납부한(2019.5.7.) A은행의 경우 **회비 미납 기간 동안 정관 제8조제5항에 따라 대의원의 권리를 행사할 수 없는 상황**이었는데

○ 금융보안원은 이를 간과하여 2019.4.3. 개최된 **금융보안원 대의원회에서 A은행장의 서면의결**을 받은 사실이 있음

⇒ 사원 회비미납시 의결권 행사 불가능 고지 등을 포함한 회부납부 지연 방지 대책을 마련·시행할 필요 (통보)

② 예산 불용률을 감안한 적정 예산편성 필요

□ 2016년~2019년 금융보안원의 **예산액 증가율은 연평균 9.3%**로 **매년 크게 증가**하고 있는데,

○ 주요 증가요인은 인건비 증가, 보안시설 설치·연구용역 확대 등 경비 증가, 노후PC 교체·디도스비상대응센터 시스템 교체 등 유·무형자산 증가 등에 따른 것임

□ 한편, 2016년~2018년 금융보안원 **예산 불용률도 연평균 6.2%**로 **매년 30억원 정도의 불용액이 발생**하고 있고, 특히 소유물비(유·무형자산)의 경우 연평균 불용률이 9.6%, 경비의 경우 연평균 불용률이 7.5%에 달하여 **과도한 예산 편성**이라고 할 수 있음

⇒ 향후 예산 불용율을 감안하여 적정 예산이 편성될 수 있도록 예산편성 개선방안을 마련·시행할 필요 (개선요구)

③ 국외여비 지급제도 개선 필요

㉮ 일당체재비에서 숙박비를 분리하고 실비로 지급할 필요

□ 금융보안원은 국외여비의 일당체재비를 여행일수에 따라 지급한다고 규정하고(여비규정 제3조제3항), **직원의 숙박비를 실비가 아닌 정액제로 운영**(여비규정 별표 제3호)

○ 여행일수에 따라 지급한다는 여비규정으로 인하여 실제 2016년 국외출장시 **숙박비를 약 150만원 초과 지급**

㉯ 부대비용 정액지급 제도 개선 필요

□ 금융보안원은 여권·비자 발급 수수료, 국외여행보험료, 입국·출국세, 예방접종비, 통신비, 자료수집비 등에 활용하기 위하여 국외출장자에게 '부대비용'을 정액으로 지급(여비규정 제22조, 별표 제3호)

○ 그러나 국외출장자에게 **실제 소요되지 않은 '부대비용'을 정액으로 일괄 지급하는 것은 불합리**

㉰ 임직원 위탁교육과정 국외연수시 국외여비 지급 폐지 필요

□ 금융보안원의 대부분 위탁교육과정에는 국외연수가 포함되어 있고, 이 경우 금융보안원에서 **국외연수비를 지원함에도 불구하고, 여비규정 제21조제3항*을 근거로 위탁교육과정 국외연수시 2016년이후 총 19명(총 10,760,109원)에 대해 일비 및 부대비용을 지급**

* 연수 국외여행자에게는 업무출장 국외여행자 일당체재비의 75%를 지급하되, 여행기간이 30일을 초과하면 그 초과일수의 일당체재비는 30% 감액 지급하고 여행기간이 60일을 초과하면 그 초과일수는 월당체재비로 지급한다.

○ 그러나, 여비규정 제21조제3항은 국외연수비를 별도로 지원하지 않는 경우 국외여비에서 지원할 수 있는 것으로 보아야 하고, **국외연수비를 모두 지원하고 있는 교육생에게 국외여비를 추가로 지원하는 것은 중복 지급**에 해당

⇒ **① 국외출장시 숙박비를 실제 숙박일수에 따른 지급 및 상한액 범위내에서 실비로 지급하고(개선요구) ② 부대비용은 실제 소요된 금액만큼 지원하며(개선요구) ③ 임직원 위탁교육과정 국외연수시 국외여비 추가 지급분은 환수조치 (시정요구)**

④ 재무제표 계정과목 회계처리 오류

□ **(당기법인세자산·부채 표시)** 일반기업회계기준 제22장 **'법인세회계'***에 따라 당기법인세자산과 당기법인세부채를 각각 상계하여 표시해야 함에도, 금융보안원은 선급법인세를 당기법인세자산으로 표시하고, 법인세 부담액은 당기법인세부채로 표시

* 당기법인세부채와 당기법인세자산이 **동일한 과세당국과 관련된 경우**에는 **각각 상계하여 표시**

○ 그 결과, 현행 재무제표에는 **당기법인세 자산과 부채가 '16년 약 4.6백만원, '17년 약 2.7백만원, '18년 약 13백만원이 각각 과대계상**

□ **(고유목적사업준비금 환입)** 금융보안원은 **준비금 환입액을 운영성과표 본문에 표시**하였으나, 공익법인회계기준 제24조에 따르면 **준비금을 부채로 인식한 경우에 한하여 환입액을 운영성과표 본문에 표시**해야 하므로, 준비금 환입액에 대하여 **자본항목 간의 계정 대체로 주석에 기재해야 함**

○ 또한, 고유목적사업준비금(자본)의 환입액은 수익의 정의를 충족하지 않으므로, 금융보안원이 재무제표에 인식한 고유목적사업준비금 환입액에 대하여 **수익이 아닌 자본 항목 간의 계정 대체로 주석에 기재**해야 함

⇒ **공익법인회계기준 등에 부합하도록 당기법인세 자산·부채 표시 및 고유목적사업준비금 환입 회계처리를 개선할 필요(시정요구)**

⑤ 시설대여(리스)계약 감가상각 회계처리 관련

□ 시설대여(리스)계약은 일반기업회계기준 제11장 '무형자산'의 문단 11.3에 따라 **유형자산과 무형자산의 요소를 동시에 갖춘 자산**의 경우 **더 중요한 요소에 따라 자산을 분류**하여야 함에도 금융보안원은 **금융리스자산에 대하여 리스기간**(5년)**에 걸쳐 감가상각***하고 있음

* 감가상각 : 자산의 **감가상각대상금액을** 그 **자산의 내용연수에 걸쳐 체계적으로 각 회계기간에 배분**하는 것

○ 그 결과, 현행 재무제표에는 **감가상각비가 '17년 약 512백만원, '18년 약 724백만원이 과소계상**되어 있으며, **금융리스자산 장부금액이 '17년 약 512백만원, '18년 약 1,236백만원이 과대계상**

⇒ **공익법인회계기준 등에 부합하도록 금융리스자산 감가상각 회계처리방식을 개선할 필요(시정요구)**

다 복리/후생관련

① 연차휴가 활성화 필요

□ 금융보안원은 직원에게 연간 최대 25일의 연차휴가를 부여

○ 그런데, 2016년~2018년 **3년간 직원 평균 연차휴가 소진일은 1.3일에 불과**하고, 미소진 연차휴가일수 모두 연차휴가보상금을 지급

□ 반면, "직원의 후생복지와 신체단련을 위해 필요한 경우"등에 사용할 수 있는 **특별휴가는 연간 총 5일을 부여**하고 있으며,

○ 2016년~2018년 3년간 특별휴가 5일은 모두 소진

⇒ 연차휴가의 의무적 사용일 설정 등 연차휴가 활성화 방안을 마련하여 시행할 필요(통보)

② 업무용 차량 관리 부적정

□ 금융보안원은 업무용 차량 운영방안(2015.5.4. 원장 결재)에 따라 공용 차량 3대의 경우 배차 신청서, 공용차량 교부대장(운행일지)를 작성하고 있으나,

○ 임원 전용차량 4대는 **차량 운행일지 자체를 작성하고 있지 않음.**

□ 또한, 임원 전용차량에 대하여 예산 범위 내에서 다음과 같이 **유류비를 지급하고 있으나 지급기준도 미비**

⇒ 임원 전용차량의 체계적인 관리와 투명한 예산 집행을 위하여 차량운행일지 기록 철저 및 유류비 지급 기준 마련 등 업무용 차량관리를 개선할 필요(개선요구)

라 고유업무

① 금융보안 정보공유 대상 확대 필요

□ 금융보안원은 침해사고대응기관으로 금융회사 등에 대한 정보공유체계로 '금융보안 정보공유 포털'을 구축(2003년)하여, 금융회사 보안관제정보(보안관제 및 침입탐지 정보 등 14개 항목)와 일반정보(보안권고문, 주요 위협정보 등 9개 항목)로 구분하여 제공

○ 아울러, '금융보안 정보공유 포털'은 「정관」에 따라 총회에서 정하는 기준에 따라 가입금을 납부하는 **190개 사원사를 대상으로만 사용권한을 제한하는 문제점**을 해소하고자 전체 금융회사 등을 대상으로 침해사고 위기경보 등을 제공하기 위하여 '전 금융회사 위기경보 전파 체계 수립계획(안), ('19.6., 금융보안관제센터)'에 따라 **'금융보안레그테크 시스템' 개선** 구축을 추진

○ 다만, '전 금융회사 위기경보 전파 체계 수립계획(안)'에 따르면 개선 구축된 '금융보안레그테크 시스템'을 통해서도 **사원기관 외 금융회사에 대해서는 위기경보 및 금융위원회 전파사항에 관한 정보만을 제공**하도록 제한하고 있으나, **금융보안사고 특성상 금융업권 전반에 미치는 부작용**을 감안할 필요

⇒ **금융업권 전반에 대한 사이버위협 및 침해사고 등의 예방을 위하여 보안권고문, 위협정보 및 취약점 정보 등 주요 금융보안 정보를 사원기관 이외 전체 금융회사를 대상으로 제공할 수 있도록 정보제공 대상 범위 조정 등 관련 시스템 및 절차를 개선할 필요(통보)**

② 금융회사 등에 대한 보안성심의 결과 활용 강화

□ **금융보안원**은 금융회사 등에서 수립한 시스템 보호 대책 등에 대해 관리적·물리적·기술적 관점에서 보안대책의 적정성에 대한 **보안성 검토를 수검대상 기간(2016.5.14. ~ 2019.7.31.) 중 총 118건 수행**

○ 다만, 금융보안원의 보안성검토 결과가 금융회사 등의 자체 보안성 심의에 참고자료로 전달·활용되고 있어, **보안성 검토 결과 발견된 중요 취약점 등에 대한 금융회사 등의 개선계획의 적정성 여부, 조치 이행완료 여부 등의 확인이 곤란**한 실정

⇒ **금융보안원의 보안성심의 결과 발견된 금융회사의 중요 취약점 등에 대한 금융회사의 개선계획 및 조치 이행완료 여부 등을 확인할 수 있도록 관련 절차를 개선할 필요(개선요구)**

③ 침해사고 조사관련 산출물 등에 대한 관리절차 개선 필요

□ 금융보안원은 수검대상 기간(2016.5.14. ~ 2019.7.31.) 중 금융회사 등에서 발생한 홈페이지 고객정보유출, ATM악성코드 감염사고 등 조사 완료된 **총 6건의 침해사고에 대해 사고원인 등을 분석하고 침해사고 분석보고서를 작성*하였으나**

* 감사착수일 현재, 총 6건의 침해사고 분석대상 중 증거가 수집된 4건의 침해사고에 대해서는 분석에 활용되었던 이미징 파일을 독립된 폐쇄망 내에 증거자료로 별도 보관하고 있음

○ 디지털 포렌식 수행을 위한 **이미징 파일 등에는 개인정보, 금융거래 내역 등 민감자료가 다수 포함될 우려가 있는 중요 전산자료임에도 동 자료에 대한 보관사유 등 세부적인 관리절차가 미흡**한 실정

⇒ **디지털포렌식 수행을 위한 이미징 파일에는 개인정보, 금융거래내역 등 민감자료가 다수 포함될 우려가 있으므로, 동 자료의 보관, 보호대책 등 관리절차를 개선할 필요(개선요구)**

④ 침해사고 대응·복구 훈련결과 점검절차 개선 필요

□ 금융보안원 '**2018년 침해사고 대응 및 복구훈련 점검 결과(2019.2.)**'에 따르면 금융보안원은 훈련유형을 악성코드 대응, 서버해킹, 디도스 대응으로 구분하고 있으며, 훈련결과 점검기준은 '적합*' 및 '부적합'으로 평가하고 있음

* 적합 : 침해사고 대응 및 복구훈련시 금융회사 등의 대응상황에 따라 '정상대응' 및 '부분대응'으로 훈련결과가 확인될 경우 '적합'으로 처리함

○ 동 보고서에는 침해훈련 공격에 대한 탐지·대응이 일부 미흡하거나, 훈련으로 인해 서비스 지연·단절이 발생하는 경우 '부분대응'으로 별도 분류된 금융회사 등이 총 48개사로 기재되어 있으나,

○ **해당 금융회사들의 명세 및 미흡사항 등 세부내역이 누락**되어 있어, **훈련결과에 따른 개선·보완 필요여부를 판단하기에는 다소 미흡**한 실정

⇒ **침해사고 대응·복구 훈련결과에 대한 점검·평가시 훈련점검 결과가 미흡한 금융회사 및 세부내용 등이 점검결과보고서에 충분히 기재될 수 있도록 개선할 필요(개선요구)**

⑤ 개인정보처리시스템 접속기록 보관 및 점검강화 필요

□ 금융보안원은 현재 개인정보처리자로서 **학습관리시스템 등 다수의 개인정보처리시스템을 보유**하고 있으며,「정보보호시행세칙」에 따라 수집, 저장, 보관 등의 운영을 하고 있음

○ 이에 따라 '개인정보 안전성 확보조치 실태점검'을 실시(교육센터 개인정보처리 실태점검 결과보고, 2018.10.17.)하고 있으나 **접속기록의 보관 및 점검 방법에 있어 개선이 필요***

* 현재 **접속기록을 6개월만 보관하고 반기 1회만 점검을 실시**하고 있으며 **행위(조회건수, 다운로드 건수)에 대한 점검 절차가 마련되어 있지 않음**

⇒ **개인정보 안정성 확보를 강화하기 위하여 접속기록의 보관기간 확대, 점검주기 단축, 점검절차 내규 반영 및 개인정보처리취급자 지정 등 관련 절차를 개선할 필요(개선요구)**

⑥ 정보보호시스템 운영관련 승인절차 개선

□ 금융보안원 정보보호시스템 중 유해사이트차단, DLP(데이터 유출방지) 등 정보보호시스템의 정책 예외 처리, 관제망 VDI 계정에 대한 승인 및 단말기 보안관리 등을 모두 팀장 승인으로 처리하고 있으나

○ 정보보호규정 시행세칙 제6조, 제18조, 19조 및 직제규정 시행세칙 [별표 제2호] 직무전결기준표 등에 따르면 위 사항들은 모두 부서장의 승인으로 처리되어야 함

⇒ **정보보호시스템 운영 및 관리 등에 대한 승인절차를 관련 내규에 맞도록 개선할 필요 (통보)**

마 계약업무

① 과도한 수의계약 비중 개선 필요

□ 국가를 당사자로 하는 계약에 관한 법률 시행령은 2016.1.1.부터 수의계약에 의할 수 있는 사유로 **"추정가격이 2천만원 이하인 물품의 제조·구매계약 또는 용역계약"으로 수의계약 사유를 엄격**히 하고 있음에도(제26조제1항5호),

○ 금융보안원 계약 및 자산관리규정 시행세칙 제63조(수의계약 집행기준) 제1항 제4호는 물품의 제조·구매·용역·그 밖의 계약 시 **예정금액이 5천만원 이하인 경우 수의계약**을 할 수 있도록 하고 있음

○ 그 결과, 2016.4월~2019.8월 중 금융보안원이 체결한 2천만원 이상 계약 195건 중 **119건(61.0%)이 수의계약**이고, 그 중 69건(전체 195건 대비 35.4%)의 사유가 "5천만원 이하"였음.

⇒ 과도한 수의계약 비중 개선 등 계약의 투명성을 강화하기 위하여 계약관련 내규를 관련 법령에 부합하도록 개정할 필요 (개선요구)

바 모범사례

① 안전한 금융보안 환경 조성

□ **(신종 보이스피싱 대응 강화)** 피싱사이트 탐지·차단을 통해 **'19년에만 약 1,922억 원의 피싱 피해를 예방**

* 피싱사이트 1개당 피해 예방금액은 약 515만원('17년 경찰청 통계연보 기준)

○ **전기통신금융사기 피해가 지속**됨에 따라 보이스피싱 **유포사이트 탐지 프로그램 추가 개발 등 자체시스템을 더욱 고도화**('19.1월)

* 전기통신금융사기(보이스피싱) 방지 종합대책('18.12.18)의 추진과제

- 시스템 고도화 이후 **피싱사이트 탐지 건수 대폭 증가***

* ('17년) 5,372건 ('18년) 18,422건 ('19.8월) 37,329건

□ **(침해사고 예방을 위한 디지털포렌식 수행)** 침해위협이 높은 금융회사의 PC 등에 대한 점검을 통해 외부침해 가능성 및 자료유출 위협 여부를 확인·조치할 수 있도록 지원함으로써 **침해사고 사전예방 및 직원들의 보안의식 제고에 기여**

○ 금융회사의 주요 침해사고 발생 위협이 높은 업무개발 및 외주용역PC 등을 대상으로 **침해예방 디지털 포렌식 분석 사업을 상시적으로 수행**

○ 기존 윈도우 OS PC 에서 윈도우 OS 서버, Mac OS PC 등 다양한 운영체제로 분석 대상을 확대하는 등 적극적인 점검을 수행('19.3월~)

* 2019년 금융회사의 점검 수요는 2017년 대비 175% 증가(8개→22개), 점검대상 PC 대수는 185% 증가(471대→1,340대)

⇒ **모범사례를 널리 알리고 소관 부서에 대하여는 표창 등을 하여 사기를 높여 줄 필요 (통보)**

2 분야별 지적내역 및 조치계획

□ 분야별 지적내역

지적분야	지적내용	처분내용
인사/보수제도 및 운용 관련 (6)	■ 2015·2016년도 신입직원 공개모집 채용관련	기관주의 문책요구 (前팀장 ○○○) 개인주의 (前부장 ○○○) 통보(인사자료) (前부장 ○○○)
	■ 직급별 정원책정 결정방식 개선 필요	개선요구
	■ 승진인사 인원 배수 운영 일관성 미흡	개선요구
	■ 저성과자 제도 및 임금피크제 운영 부적정	통보
	■ 임직원 성과급 지급제도 개선 필요	통보
	■ 퇴직자 보수 일할계산 적용 필요	개선요구
예산 집행/회계처리 관련 (5)	■ 금융보안원 회비 납부 지연 개선 필요	통보
	■ 예산불용률을 감안한 적정 예산 편성 필요	개선요구
	■ 국외여비 지급제도 개선 필요	시정요구(개선요구포함)
	■·재무제표 계정과목 회계처리 오류	시정요구
	■ 시설대여(리스)계약 감가상각 회계처리관련	시정요구
복리·후생 관련(2)	■ 연차휴가 활성화 필요	통보
	■ 업무용 차량관리 부적정	개선요구
고유업무 관련 (6)	■ 금융보안 정보공유 대상 확대 필요	통보
	■ 금융회사 등에 대한 보안성심의 결과 활용 강화	개선요구
	■ 침해사고 조사관련 산출물 등에 대한 관리절차 개선	개선요구
	■ 침해사고 대응·복구 훈련결과 점검절차 개선 필요	개선요구
	■ 개인정보처리시스템 접속기록 보관 및 점검 강화	개선요구
	■ 정보보호시스템 운영관련 승인절차 개선	통보
계약관련 (1)	■ 과도한 수의계약 비중 개선 필요	개선요구
모범사례 (1)	■ 안전한 금융보안 환경 조성	통보(모범사례)

□ 조치계획

○ 「금융위원회 감사규정」 제14조에 따라 금융보안원에 통보하여 2개월 이내에 적의 조치토록 요구