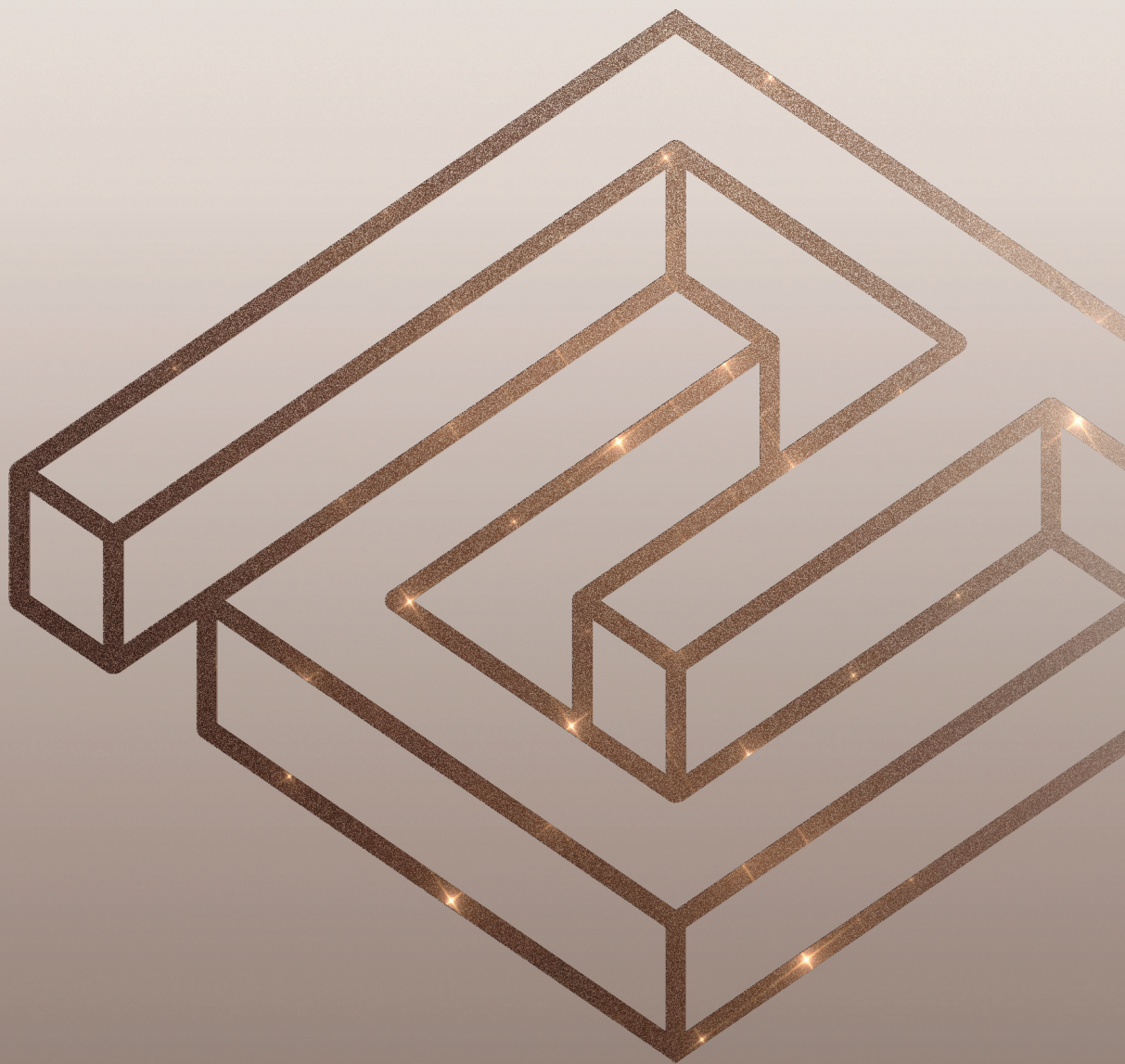


2024 금융보안원 연차보고서

Financial Security Institute
Annual Report



금융보안원
FINANCIAL SECURITY INSTITUTE

2024
금융보안원
연차보고서

Financial Security Institute
Annual Report



CONTENTS

01 발간사		04
02 한눈에 보는 2024 금융보안원		06
03 사업성과	금융보안관제센터	16
	침해대응부	20
	보안평가부	25
	보안연구부	31
	금융인증부	35
	DT대응지원부	39
	데이터혁신센터	44
	AI혁신실	49
	개인정보보호부	51
	금융보안교육센터	54
	참고 2025 디지털금융 및 사이버보안 이슈 전망	60
04 금융보안원 현황	일반 현황(설립목적, 비전, 원 소개)	66
	주요 연혁	68
	조직 현황	70
	의사결정 구조	71
	사원기관	72
	사무실 현황	73
	홈페이지 현황	74
05 주요 활동	금융보안원 소식	80
	CEO 뉴스레터	90
06 부록	주요 간행물(가이드 및 안내서)	96
	인텔리전스 보고서	98
	위협헌팅 보고서	98
	정기간행물	100
	정보보호동향 보고서	102
	언론홍보 현황	104

발간사

“10년 전 150여 명으로 출범한 금융보안원이
이제는 300명 이상의 조직으로 성장하여 국내 금융시스템을 지키는
수문장으로 자리매김하였으며, 앞으로의 뉴노멀의
디지털금융 시대에서도 금융보안원이 금융보안의 길잡이로서의
역할을 적극 수행할 수 있도록 선도해 나갈 것입니다.”

2024년은 AI 기술이 실생활에 깊숙이 스며들며 디지털금융 생태계에 새로운 도약을 예고한 해였습니다. 급격히 확산되는 AI 기술은 디지털 환경 및 업무 패러다임의 변화를 이끌고 있으며, 금융권 AI 기술의 안전성 및 신뢰성에 대한 기대도 더욱 높아지고 있습니다. 이에 금융보안원은 기존의 고유업무인 보안관제 및 침해대응을 기반으로 신기술 도입에 따른 새로운 보안 위협에도 적극적으로 대응하고 있습니다.

급증하는 랜섬웨어 및 디도스 공격 등 사이버 위협에 대응하기 위해 금융감독원과 협력하여 화이트해커를 통한 **블라인드 사이버 모의해킹(공격·방어) 훈련**을 두 차례 실시하였고, 금융회사의 침해사고 대응 능력 강화와 자율보안 체계의 안정적인 정착을 위해 실전형 ‘**침해대응 훈련 플랫폼**’을 구축하였습니다. 아울러 금융권의 사이버 위협을 식별하고 제거하는 활동을 기록한 ‘**사이버 위협 헌팅 보고서**’를 발간하고 금융보안관제 기술을 고도화하였으며, 제2금융권 공동 이상거래탐지물을 마련하여 배포하였습니다.

또한, 디지털 신기술의 적극적 활용과 더불어 금융보안의 중요성이 다시금 조명되고 있는 가운데, 금융회사의 AI 활용이 안전하게 이루어질 수 있도록 지속적인 인력 및 조직 확대를 통해 AI 전담 조직인 **AI혁신실을 신설**하고, AI 신뢰성 확보를 위한 ‘**금융 AI 보안성 검증체계**’를 마련하여 보안위험 요소를 사전에 식별 및 해결하도록 지원하였습니다. 또한, 금융당국의 금융권 망분리 개선 로드맵 마련에 따라 금융권 이용이 대폭 증가할 것으로 예상되는 클라우드서비스의 보안 관리를 지원하기 위해 국내외 주요 클라우드서비스 제공자와 협업하여 ‘**금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서**’를 배포하였습니다.

이 밖에도 금융사기로 인한 소비자 피해를 예방하기 위하여 **보이스피싱 탐지체계를 고도화**하고 신종 금융사기와 관련된 범죄조직의 수법과 운영 방식을 심층 분석하여 유출된 카드정보를 금융당국·카드사에 신속히 공유하였으며, 클라우드 및 제3자 서비스 등 금융회사 외부의 **예측 불가능한 영역에 대한 보안위협에 효과적으로 대응**하였습니다.

출범 10년차를 맞는 올해, 금융보안원은 **• 보안으로 디지털 혁신 견인 • 보안의 텍스트 레벨 선도 • 회사와 직원이 함께 성장하는 조직 문화 정립**이라는 역할을 설정하고, 금융권 AI 안전성 제고·안전한 디지털자산 생태계 조성·클라우드 및 데이터의 안전한 활용 지원·선진화된 자율보안 문화 조성 주도·창의적이고 유연한 성과중심 조직 문화 등을 세부 과제로 선정하였습니다. 이를 바탕으로 금융보안원은 **안전한 디지털금융 세상을 위하여 혁신을 이끌고 보안의 새로운 가치를 창출**하겠습니다. 많은 관심과 격려 부탁드립니다.

금융보안원 원장 박상원



2024 주요 발사취

I. 2024년도 금융보안원 시무식 개최 (01.02)



신년사를 통해 임직원 모두가 금융보안 프렌들리 문화 형성에 동참해야 하며, 금융보안원이 사이버 위협 대응체계의 유지에서 나아가 SI 등 금융권 신기술의 선제적인 대비에 힘쓸 것을 당부하였습니다.

III. 김철웅 원장, 2024 한국정보보호산업협회(KISIA) 사이버 주권수호상 수상 (02.22)

금융보안 관련 정책발굴과 침해대응 활동 등을 통해 국가 정보보호 수준 향상과 사이버 주권 수호에 기여한 공로를 인정받아 사이버 주권수호상을 수상하였습니다.

II. 금융보안 선진화 현장 간담회 행사 개최 (02.01)



금융위원회 김소영 부위원장은 금융보안원에서 열린 '금융보안 선진화 추진 간담회'에서 전자금융감독규정 개정안 및 '금융보안 선진화' 단계별 추진방안을 발표하였습니다.



IV. 2024년 금융보안자문위원회 전체회의 개최 (04.05)



금융보안 현안 사항에 대한 다양한 의견을 청취하고 바람직한 방향을 모색하기 위해 2024년 금융보안자문위원회 전체회의를 개최하였습니다. 본 회의에서 금융보안 규제 선진화, 금융권 S/W 공급망 보안, AI 활용 활성화 등에 대한 논의를 이끌어 줄 신규 위원 6명을 새롭게 위촉하였습니다.

V. 금융보안원 창립 9주년 기념식 개최 (04.12)



금융보안원은 창립 9주년 기념식을 개최하였습니다. 기념식을 통해 임직원들은 지난 9년간의 성과를 돌아보고 서로를 격려하며, 지속가능한 성장을 추구하는 선도적인 기관으로서의 역할에 대해 다시 한 번 고민해보는 시간을 가졌습니다.

VI. 제8기 금융보안 최고위과정 입교식 (05.02)



금융권 및 정보보호 산업계의 디지털·정보보호 담당 경영진 (C-Level)을 대상으로 「제8기 금융보안 최고위과정」을 개설하고 입교식을 개최하였습니다.

VII. 2024년 금융권 합동 재해복구 전환훈련 참가 (06.14)

「2024년 금융권 합동 재해복구 전환훈련」에 참가하였습니다. 이번 합동훈련은 대형 전산사고로 인한 금융서비스 중단을 예방하고 금융회사 IT안정성과 복원력을 제고하기 위해 진행된 금융권 합동 재해복구 전환훈련으로 금융보안원 등 6개 유관기관과 은행·카드·증권사 등 금융사 66곳이 참여하였습니다.



X. 「금융권 현안 세미나」 개최 (08.05)

「금융권 현안 세미나」를 개최하였습니다. 본 세미나에서는 금융업계, 보안업계, 학계 등 담당자 100여 명이 참석한 가운데 MS 오류 등 글로벌 사이버 정전 사태의 사고 경과를 분석하고, 유사 사고를 예방하기 위해 전문가 의견을 청취하는 토론이 진행되었습니다.



VIII. 금융 AI 공모전, 「FSI AIXData Challenge 2024」 개최 (06.27)



FSI AIXData Challenge 2024를 개최하여 금융권에서 AI를 혁신적으로 활용할 수 있는 방안을 모색하였습니다.

IX. 제13회 정보보호의 날 기념 금융회사 최고경영자 초청 세미나 개최 (07.17)



「제13회 정보보호의 날 기념 금융회사 최고경영자 초청 세미나」를 개최하였습니다. 김주현 금융위원장은 기초연설을 통해 “지금까지 디지털 금융혁신을 기반으로 ‘편의성 중심의 발전’을 이루어왔다면, 이제는 신뢰받는 금융을 위해 금융보안과 함께 ‘책임있는 발전’으로 나아가야 함”을 강조하였습니다.

XI. 금융보안 아카데미 2024 수료식 (11.01)



금융권에 필요한 미래 인재 발굴 및 양성을 위해 정보보호에 관심있는 대학(원)생을 대상으로 사이버 침해 위협분석·대응 및 AI·빅데이터 분야 전문교육을 제공하여, 40명의 금융보안 미래 인재를 양성하였습니다.

XII. FISCON 2024 개최 (11.07)



「FISCON 2024」를 개최하였습니다. 이번 컨퍼런스는 <Advance with Big Waves>를 주제로 개최되었으며 민·관·산·학·연 전문가, 일반인, 학생 등 1,500여 명이 참석하며 높은 관심 속에 마무리 되었습니다.

2024 금융보안원 주요 성과

1

금융보안관제센터

- 금융사이버 위협 헌팅 보고서 발간 및 금융보안관제 기술 고도화 **(보고서 3건 발간)**
- 제2금융권 공동 이상거래탐지를 마련 및 배포
- 이상금융거래정보 공유업무 참여기관 확대를 통한 정보공유 활성화 추진 (신규가입 **23개社**)
- 통신사 추가 MOU 체결을 통한 보이스피싱 사기 대응능력 강화
- 전자적 침해시도 **67,826,209건** 대응
- 보이스피싱 사기정보 **37,246건** 공유 및 **약 1,182억원**의 피해 예방
- 피싱사이트(**9,686건**), 악성앱(**2,574건**), 가로채기 전화번호(**220건**) 탐지
- 이상금융거래정보 **129개社, 193건** 공유 및 **약 52억원**의 피해 예방

2

침해대응부

- 침해사고 조사·분석 **26건**, 악성코드 수집·분석 **17,768,362건**, 악성코드 대응 **280,064건**
- **14개社 1,196대** 침해 예방 디지털포렌식 분석
- 신용카드(**23,897건**) 및 계정정보(**2,945건**) 등 유출정보 수사 공유
- 「금융 및 백신 앱으로 위장한 보이스피싱 악성 앱 프로파일링」인텔리전스 보고서 발간
- 금융권 **200개社**, 침해사고 대응훈련 **632회** 실시
- 디도스 공격 비상대응센터 (일반 대피소 연동기관 **85개** 및 클라우드 대피소 연동기관 **12개** 기관) 운영

3

보안평가부

- 금융권 **154개社** 대상 취약점 분석·평가 **269회** 실시
- 모의해킹 점검 결과 시나리오 **94건** 발견
- 「공격자 관점의 3rd Party 솔루션 취약점 프로파일링」레드아이리스 인사이트 리포트 발간
- 자체구축 클라우드 평가 방법론 개선 및 **8개社** 평가 실시
- 내부망 SaaS 이용 보안대책 평가 **23회** 실시
- 취약점 종합관리 솔루션(FLUS) 배포(**123개** 금융회사 이용)

4

보안연구부

- 금융보안 정책 관련 보고서 **74건** 정부 제공 및 배포
- 금융 IT·보안 정책 연구보고서 **24건** 제공
- 디지털금융·보안기술 심화연구 및 기술·표준동향 보고서 등 **총 23건** 제공
- 「2025년 디지털금융 및 사이버보안 이슈 전망 보고서」발간
- 금융정보보호 컨퍼런스(FISCON) **18개 세션 운영**, 총 **1,500여명** 참여

5

금융인증부

- 금융권 금융IT 보안성 검토 **22건** 및 금융IT 보안성 검증 **147건** 수행
- 모바일 신분증 평가기관 추진
- 국내외 자율보안 관련 동향 조사 및 연구
- 금융권 정보보호(ISMS) 및 개인정보보호 관리체계(ISMS-P) 인증 심사 **128건** 수행
- 인증 취득(관심)기관(**60개 기관**) 및 인증심사원 (**약 1,000명**) 대상 금융 ISMS-P 인증 세미나 개최
- **10개** 기관 대상 전자서명인증 평가 수행

6

DT대응지원부

- 전자금융보조업자 합동점검 실시(금융회사 **59개社**, 전자금융보조업자 **38개社**참여)
- 금융IT 수탁사 보안관리 프레임워크 개발
- 금융IT 수탁사 SW위험관리 체계 개발
- **19개** CSP 사업자 대상 안전성 평가 수행 및 평가 결과 **392회** 공유
- **7개** CSP 사업자 대상 혁신금융서비스 안전성 평가 수행
- 핀테크 보안점검 **348건**, 로보어드바이저 보안성 심사 **271건**

7

데이터혁신센터

- 데이터허브 정식 오픈(3월, 참여기업 **51개社**)
- 금융데이터거래소 회원 수 **12,095명**, 참여기업 **158개社**, 거래 **23,746건**
- 데이터전문기관 정보집합물 결합 **102건**, 가명·익명처리 적정성평가 **5건** 및 자가결합 적정성 평가 **35건**
- 금융 마이데이터 통합인증 중계 **11억건** 이상 처리
- 마이데이터 사업자 기능적합성 심사(**90회**) 및 취약점 점검 지원(**51회**)
- 마이데이터 2.0 정책 수립 지원 및 기술 가이드라인, 표준 API·통합인증 규격 개정 및 배포

8

AI혁신실

- AI 모델 보안성 검증체계 운영 및 시범검증 **3건** 수행
- 2024 FSI AIXData Challenge 개최
- 금융보안 AI 워킹그룹 구성·운영
- 플랫폼 금융서비스 알고리즘 검증 **12건** 수행(**9개社**)
- 금융보안 업무 적합도 측정 벤치마크 지표(FSKU) 개발

9

개인정보보호부

- 정보보호 상시평가 수행(**2,893개** 금융회사 대상)
- 개인(신용)정보 공동점검 수행(**137개** 수탁자 대상)
- 제도 개선 등 금융당국 정책 지원 및 점검역량 강화 추진

10

금융보안교육센터

- 금융권 맞춤형 온·오프라인 교육 **89개** 과정 운영 및 **80만여명** 수료
- 제8기 금융보안 최고위과정 실시 및 **30명** 수료
- 금융보안관리사 검정시험 **2회** 실시 및 **99명의 전문가** 배출
- 금융회사 자체 교육용 콘텐츠 **43종** 배포
- 금융보안 아카데미 확대 및 **40명의** 금융보안 미래 인재 양성

2024 금융권 주요 피해 위협

1월



해킹 플랫폼을 활용한 대량 취약점 공격

중국 국적 해킹 플랫폼을 활용한 국내 금융사 대량 취약점 공격

2월



보안인증 SW 변조 악성코드 유포

북한 해킹그룹이 특정 홈페이지의 보안솔루션을 악성코드로 변조하여 유포

3월



국외점포 홈페이지 대상 디도스 공격

HTTP GET Flooding 등의 공격이 발생하여 홈페이지 접속 지연 발생

NAC 솔루션 취약점 악용

북한 해킹그룹의 국내 특정 NAC 솔루션 취약점 악용한 공격

7월



웹서버 해킹

금융회사 특정 웹서비스 취약점 악용한 파일업로드 공격

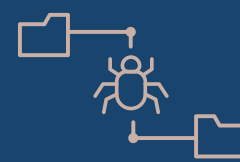
홈페이지 경유지 악용

금융회사 홈페이지가 해킹을 통해 악성코드 경유지로 악용

악성코드 감염 및 웹서버 해킹

ASP.NET*에서 지원하는 ViewState 기능을 악용한 웹셀 유포

8월



웹서버 해킹

오라클 Weblogic 취약점 악용한 웹셀 업로드 공격

9월



악성코드 감염

워터링홀 사이트를 통한 인터넷PC 악성코드 감염

4월



대규모 취약점 스캔 공격 탐지

클라우드 호스팅 서비스 IP를 이용한 취약점 대량 스캔 공격 발생

5월



국내 금융권 디도스 공격

금융사 대상으로 디도스 공격 발생

6월



웹스캔 공격 증가

금투업권 대상 웹취약점 스캔 공격 증가

데이터유출방지솔루션취약점악용

북한 해킹그룹의 국내 특정 데이터 유출 방지 솔루션 취약점 악용한 공급망 공격

10월



국내 금융권 디도스 공격

금융 유관기관 및 카드사 대상으로 디도스 공격 발생

11월



대규모 취약점 스캔 공격 탐지

금융사 대상 다수의 프록시 서버를 경유한 취약점 스캔 공격 발생

12월



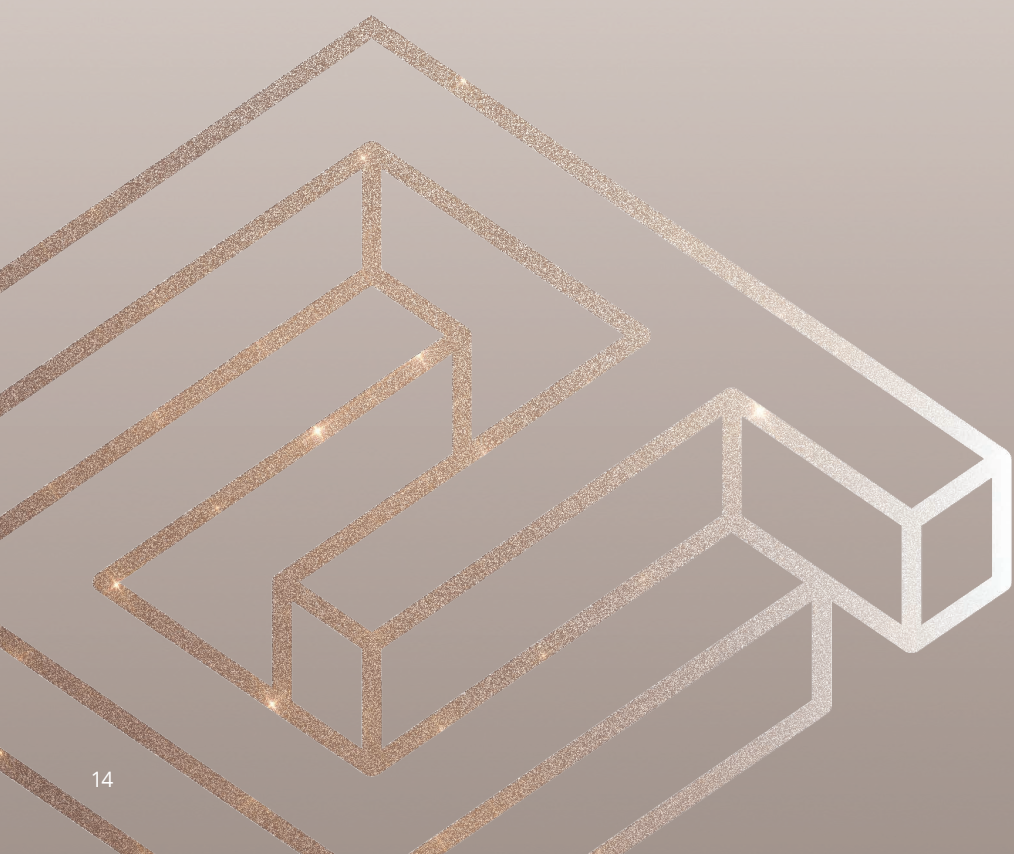
국내 금융권 SMTP 공격

다수 금융사 대상 SMTP 부정 로그인 시도 탐지

*ASP.NET ViewState : 웹 애플리케이션에서 페이지의 상태정보를 클라이언트 측에 저장하여 서버에서 페이지를 다시 렌더링할 때 상태를 유지하는 기능이며, 공격자가 이를 변조하여 웹셀 유포에 악용

PART. 1

사업성과



금융보안관제센터

ABC(AI, BigData, Cloud) 기반의 차세대 금융보안관제시스템 운영 및 보이스피싱 대응강화 등 사이버 공격에 대한 보안관제 선도

침해대응부

금융권 사이버 침해위협 선제 대응 및 신속한 침해사고 조사·분석을 통해 안전한 금융생태계 조성

보안평가부

전자금융기반시설 취약점 분석·평가를 통해 보안 위협 예방 및 안전한 전자금융거래 기반 확보를 지원

보안연구부

디지털금융 정책 및 금융보안 컴플라이언스 지원 등을 통한 금융 안전성 강화

금융인증부

금융IT 보안성 검토·검증 및 모바일 신분증 평가, 금융분야 정보보호·개인정보 관리체계 인증기관 운영 및 인증심사, 전자서명인증 평가 운영 등을 통한 금융권 디지털 혁신 및 안전한 인증체계 확립 지원

DT대응지원부

금융IT 수탁사 리스크 관리·점검 및 금융권 클라우드 이용 관련 안전성 평가 수행, 핀테크 보안·활성화 지원 등 디지털대응전환의 활성화를 위한 안전성·보안성 검증 지원

데이터혁신센터

금융데이터 플랫폼 운영 및 데이터허브 신규 구축, 데이터전문기관 서비스, 금융분야 마이데이터 운영 지원

AI혁신실

AI 모델 보안성 검증체계 운영, 혁신금융서비스(생성형 AI 부문) 보안대책 평가 등 AI 활용 활성화 및 신뢰할 수 있는 AI 확보를 지원

개인정보보호부

정보보호 상시평가 제도의 안정적 운영 및 점검역량 강화, 금융당국 정책 지원, 개인(신용)정보 수탁자 공동 점검 등 금융권 개인(신용)정보보호 수준 제고

금융보안교육센터

금융권 자율보안 체계 구축에 필요한 금융보안 전문인력 양성을 위해 맞춤형 전문교육 실시

금융보안 관제센터

금융부문 실시간 보안관제 체계 구축 및 운영

금융보안관제센터는 「정보통신기반보호법」 제16조의 금융분야 정보공유분석센터(ISAC, Information Sharing and Analysis Center) 및 「전자금융감독규정」 제37조4의 금융분야 통합보안관제센터로서 금융권을 대상으로 하는 전자적 침해 행위를 24시간 365일 탐지·분석하고 있으며 금융권에 사이버위협 정보를 신속하게 공유·전파하고 있습니다.

금융분야 사이버위협에 대한 지능형 보안관제 및 실시간 정보공유체계 선도를 위해 인공지능 기반 위협 인텔리전스, 금융 사이버 위협 헌팅, 금융권 공격표면관리(ASM) 기술 연구·개발 등 보안관제기술을 고도화하였습니다. 또한 제2금융권 공동 이상거래탐지를 마련·배포, 보이스피싱 대응 MOU 체결 등을 통해 금융권의 FDS 운영 및 사기대응 수준 향상에 기여하고 정보공유 활성화의 기반을 마련하였습니다.

- 금융사이버 위협 헌팅 등 금융보안관제 기술 고도화
- 제2금융권 공동 이상거래탐지를 마련·배포
- 이상금융거래정보 공유업무 참여기관 확대 및 보이스피싱 대응 MOU 체결을 통한 대응 강화

01

ABC(AI, BigData, Cloud) 기반의 「차세대 금융보안관제 서비스」 운영

금융분야 정보공유분석센터
(ISAC, Information Sharing
and Analysis Center)
해킹·사이버테러 등 전자적
침해행위에 관한 정보를 분석하고
침해사고 발생 시 대응요령 및
지침을 신속하게 배포하여 공격을
효과적으로 예방·탐지하고 대응할
수 있는 조직

“24시간 365일 실시간 보안관제를 통한 전자적 침해위협에 선제 대응”

대외환경

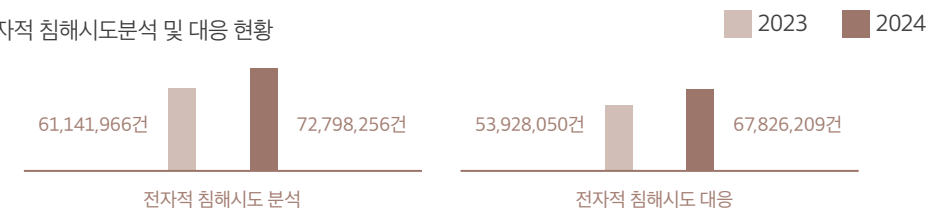
- 국내 금융권을 타겟으로 취약점 스캐닝 및 침입시도가 지속적으로 발생
- 특정 금융기관을 사칭 또는 불특정 다수를 대상으로 한 해킹메일 유포, 웹 취약점 공격 등 금융권을 위협하는 사이버 공격이 지속적으로 발생

주요성과

- '23년부터 ABC(AI, BigData, Cloud) 기반의 차세대 금융보안관제를 실시하여 사이버 공격에 대한 탐지 대응력 강화
- 해킹메일, 랜섬웨어, 제로데이 취약점 공격 등 금융 사이버 위협을 신속하게 탐지·분석
- 은행, 카드 등 금융권 대상으로 한 다수의 디도스 공격에 대해 신속히 분석·공유·대응하여 피해 예방
- 잠재적 보안 위협에 선제적으로 대응하기 위해 금융 사이버 위협 헌팅을 수행하여 다수의 식별된 위협을 사전에 제거

사업실적

- 전자적 침해시도분석 및 대응 현황



- 위협 헌팅 보고서 발간

- FSI Malicious IP 2023 분석을 통한 금융권 공격 동향, (제2024-1호)
- NXDomian Hunter, (제2024-2호)
- Attack Surface Management on the finance industry 2024, (제2024-3호)

차세대 금융보안관제 개념도



02

보이스피싱 사기정보 공유체계 확대

보이스피싱 사기정보 공유체계 금융권을 넘어 통신·수사·보안 등 여러 분야의 전문기관들과 함께 협업하여 보이스피싱 사기정보를 실시간으로 공유하는 시스템

보이스피싱

유무선 전화를 통해 공공기관, 정부 등을 사칭하여 불법적으로 개인의 금융 정보를 탈취하거나 금전적 손실을 야기시키는 사회공학적 해킹 기법

“금융보안원이 자체 탐지한 피싱·파밍사이트, 악성앱, C&C서버, 가로채기전화번호 등 사기에 악용되는 정보를 공유하여 보이스피싱 등 전자금융사기로부터 금융소비자를 보호”

대외환경

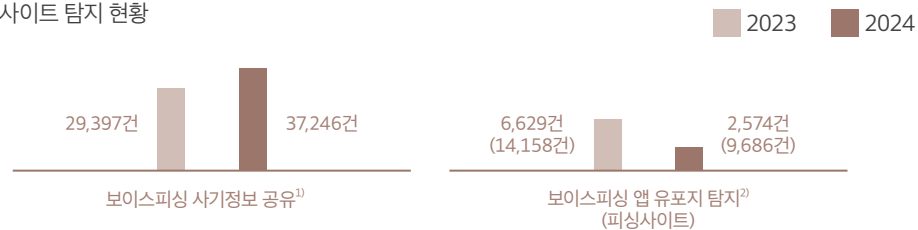
- 보이스피싱 등 전자금융사기는 정보통신기술(ICT)과 결합하여 날로 고도화되고 있으며, 신종 사기수법은 다수 금융회사에 동시다발적으로 발생하는 경향
- 최근 피싱 공격 중 스미싱 악성앱이 계속해서 증가하는 추세이며 세뱃돈, 청첩장, 부고장, 과태료부과 등 일상생활에 밀접한 주제를 교묘하게 악용해 피해를 유발

주요성과

- 분야별(수사, 통신, 보안 등) 전문기관 참여 확대를 통하여 보이스피싱 사기정보의 수집→공유→대응에 이르는 유기적 협력체계를 마련
- 금융업권별 보이스피싱 대응협의체 운영을 통해 보이스피싱·대응 기술의 트렌드 공유 및 금융회사 전체의 보이스피싱 대응 수준 향상
- 금융권 원격제어 앱 연동 차단 점검을 통해 원격제어 앱을 이용한 보이스피싱에 대한 대응 수준 향상
- 가상자산거래소의 본인확인 관련 취약점 및 사기대응체계를 점검하여 가상자산 업권의 사기 대응 수준 향상

사업실적

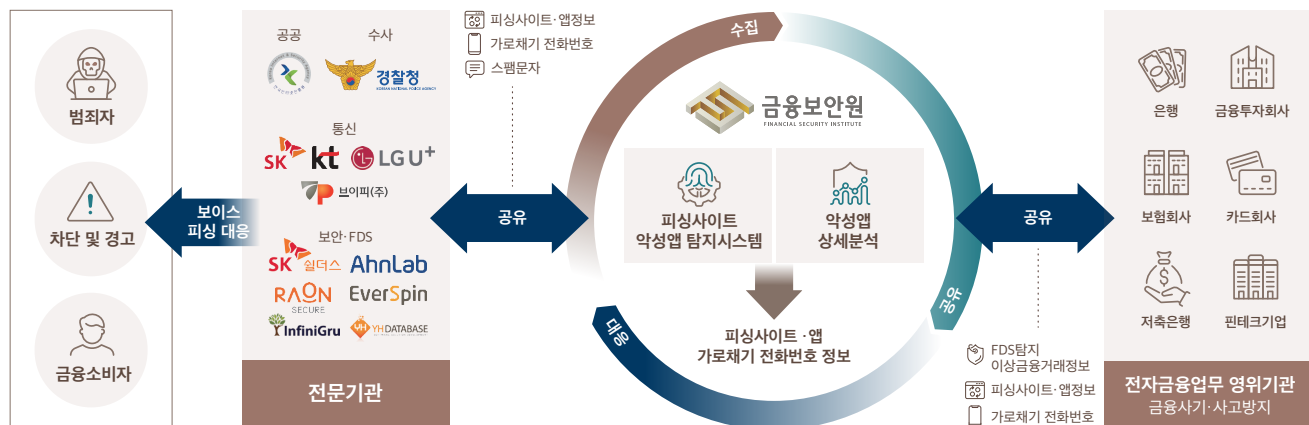
- 피싱사이트 탐지 현황



1) 토스에서 공유하는 악성앱 탐지 정보가 추가되어 공유 건수 증가

2) 최근 금융회사, 전문기관(경찰, 통신사 등)의 지속적인 피싱사이트 탐지 및 보이스피싱 범죄 대응으로 피싱사이트 및 보이스피싱 유포 건수 감소 추세

보이스피싱 사기정보 공유체계



03

이상금융거래정보 공유 대상 확대

이상금융거래탐지시스템 (FDS, Fraud Detection System) 전자금융 거래에 사용되는 단말기 정보, 접속 정보, 거래 정보 등을 종합적으로 분석하여 의심거래를 탐지하고 이상금융거래를 차단하는 시스템

이상금융거래정보 공유

시스템(FISS, Fraud

Information Sharing System)

개별 금융회사가 구축·운영 중인 이상금융거래탐지시스템(FDS)을 통해 수집한 이상금융거래정보를 금융권 내에서 실시간 상호 공유할 수 있도록 하는 시스템

“개별 금융회사가 탐지한 보이스피싱 등 이상금융거래정보를 금융권에 실시간 상호 공유하여 사이버 금융 범죄로 인한 피해를 예방”

대외환경

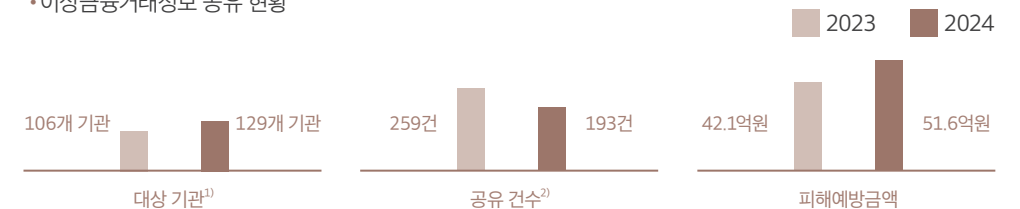
- 비대면 금융거래가 증가하고 금융거래에 대한 사이버 위협이 확대 및 지능화되는 추세에 따라 금융권 공동 대응의 필요성 증대
※ “이상금융거래탐지시스템 운영 가이드라인 시행”(‘24.1.1.)
- 금융소비자 보호를 위한 정부 정책 강화로 금융권 공동의 전자금융사고·사기 예방·대응 체계 및 정보공유 활성화의 중요성이 증대

주요성과

- 이상금융거래정보를 전 금융권으로 실시간 상호 공유 가능한 이상금융거래정보 공유시스템(FISS)을 운영
- 금융권 공동의 정보공유체계에 참여하는 기관을 확대하여 공유체계의 외연확대는 물론 공유되는 정보를 통한 사기예방 실효성 제고
- 이상금융거래탐지시스템 운영을 위한 가이드라인 마련·시행을 통해 금융업권의 전자금융거래의 안정성 향상 및 이상금융거래에 대한 조치 강화

사업실적

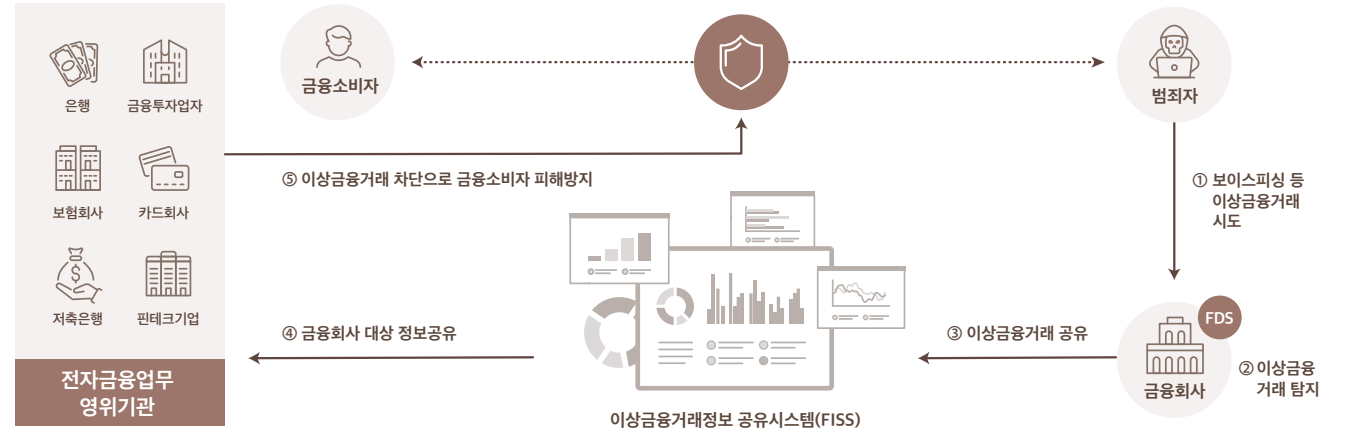
- 이상금융거래정보 공유 현황



1) 신규가입(23개기관) : 보험 19개사, 금융투자 2개사, 캐피탈 1개사, 전자금융 1개사

2) 비대면 책임분담기준 확대 적용(2025.1.1.)에 대비한 제2금융권 FDS 고도화 작업이 중점 추진됨에 따라 공유 건수가 전년 대비 감소

이상금융거래정보 공유체계



침해 대응부

금융권 침해사고 예방 및 대응

침해대응부는 「전자금융감독규정」에서 지정한 금융분야 침해사고 대응기관으로서 침해사고에 대한 정보공유체계 구축, 사고원인 분석 및 대응·확산 방지, 디도스 공격 대피소 운영 및 침해사고 대응·복구 훈련을 수행하는 등 금융권 침해사고 예방 및 대응 역량을 강화하고자 지속적으로 노력하고 있습니다.

점차 고도화·지능화되는 사이버 위협에 대해 신속하게 분석·대응하여 피해를 최소화하고, 전문화된 디지털 포렌식, 악성코드 분석 및 체계화된 침해사고 대응훈련 등을 통해 금융권 침해 예방·대응 활동을 지원하였습니다.

- 금융권 침해사고 조사·분석 및 대응
- 금융권 침해위협 수집·분석 및 예방
- 침해사고 대응훈련 강화 및 비상대응센터 운영
- 금융권 소프트웨어 공급망 보안 생태계 조성

01

금융권 침해사고 조사·분석 및 대응

금융권 침해대응 인텔리전스 플랫폼
금융회사 대상으로 국내·외 침해사고 데이터를 분석·공유하는 플랫폼

다크웹
암호화된 네트워크에 존재하며 익명성이 보장된 특정 브라우저로만 접근이 가능한 웹사이트를 의미하며, 해킹으로 얻은 개인정보, 마약거래 등 불법적인 정보의 거래가 주로 이루어짐

“금융권 침해사고 발생 시 사고 원인분석 및 대응책 제공”

대외환경

- 국가 배후 해킹조직의 국내를 대상으로 한 정교화된 APT 공격 지속
- 기업에서 많이 이용하는 정보보호 솔루션 취약점을 악용한 공격 지속
- 다크웹을 통한 서버 접속 정보, 기업 이메일 계정 정보 등이 거래되는 등 금융권 위협 확산

주요성과

- APT 공격, 공급망 공격, 크리덴셜 스테핑 등 다양한 사이버 공격의 침해 원인을 조사·분석하여 침해사고 대응기관의 역할을 성공적으로 수행
- 금융권 침해대응 인텔리전스 플랫폼을 통해 공격자의 공격기법 및 침해지표를 전파하여 추가 공격을 사전에 차단하고 금융권 피해를 최소화
- 다크웹 모니터링으로 발견한 신용카드 정보, 이메일 계정정보 등을 금융회사에 신속히 공유·조치하여 부정결제·이메일 해킹 등 금융사고를 미연에 방지
- 침해위험 가능성이 높은 단말 등에 대한 예방점검으로 위협요인 제거 및 금융회사의 보안수준 향상을 도모함으로써 안전한 금융보안 환경 조성에 기여

사업실적

- 금융권 전자적 침해에 대한 원인분석·대응 및 디지털포렌식 분석
- 다크웹에 유출된 금융권 관련 정보 모니터링 및 후속 대응

< 침해사고·위협 조사 및 분석 >		
구분	2023년	2024년
수행 건수	22건	26건

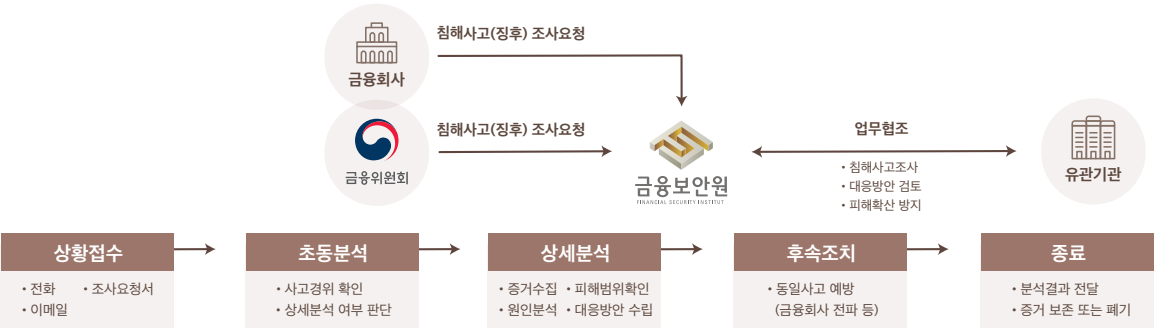
<침해예방 디지털포렌식 분석>		
구분	2023년	2024년
실시 기관	14개	14개
분석 수량	1,352대	1,196대*

* 자율점검도구 이용 확대에 따른 감소

<다크웹 위협정보 후속대응>		
구분	2023년	2024년
신용카드	115회, 31,530건	101회, 23,897건
이메일 계정 등	41회, 136,588건	22회, 2,945건

- 금융당국의 금융보안 점검·검사를 지원하고, 국내외 침해사고 관련 대외 협력체계 운영
- 금융권 침해대응 인텔리전스 플랫폼 구축 완료 ('24.10월 서비스 개시)

침해사고 조사 및 대응 절차



02 금융권 침해위협 수집·분석 및 예방

위협 헌팅(Threat Hunting)
분석가의 전문적인 보안 기술을
활용하여 정교하게 은닉된 공격을
찾아내는 보안 활동

금융권 사이버 침해위협분석
대회(FIESTA)
금융보안 위협분석 전문인력
발굴·육성과 금융권 사이버
침해위협 대응능력 강화를 위해
금융권에 특화된 국내 유일
사이버 침해위협분석 대회

“금융권 악성코드 수집·분석 및 침해위협 역량 강화”

대외환경

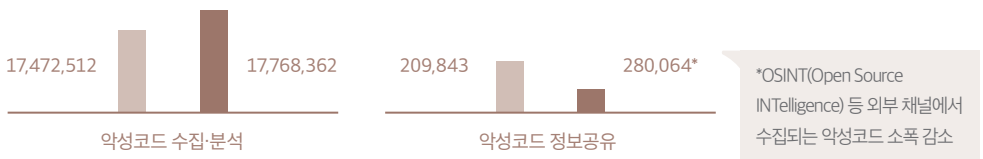
- 라자루스, 김수키, 안다리엘, 코니 등 국가배후 위협 그룹 활동 지속
- 금융 및 백신업을 사칭하여 금융 소비자의 인증정보를 탈취하는 악성앱 유포 지속
- 금융당국 및 가상자산 거래소를 사칭한 피싱 메일과 악성코드 유포 지속

주요성과

- 악성코드, 악성 앱 등 금융권 위협정보 수집·분석을 강화해 금융회사의 침해사고 발생요인을 사전에 차단하는 등 사이버위협 피해 예방
- 금융권에 직·간접적으로 영향을 끼칠 수 있는 악성코드를 수집·분석하여 악성행위 정보, 침해지표(유포지, 탐지 고유값 등)를 금융권에 공유
- 통합보안관제, 침해사고조사 및 고난이도 위협헌팅을 통해 고위험 악성코드를 탐지하고 심층 분석하여 금융권에 유의미한 결과 공유
- 금융회사 정보보호 담당자의 침해대응 역량 강화 및 정보보호 우수인력 발굴을 위해 ‘24.9월에 금융보안 위협분석 대회(FIESTA)를 개최

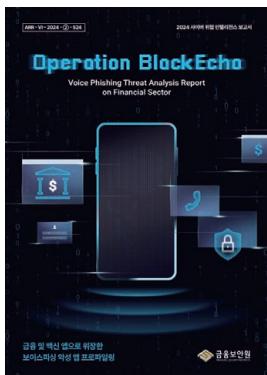
사업실적

- 악성코드 수집·분석 및 금융권 정보공유



- 금융소비자 피해 예방 등을 위해 「금융 및 백신 앱으로 위장한 보이스피싱 악성 앱」 사이버위협 인텔리전스 보고서 발간·배포
- 매년 금융보안 위협분석 대회(FIESTA) 개최, 전년대비 참가자는 약 5% 증가한 총 454명(금융회사 93명, 대학(원) 317명 등)이 대회에 참여하여 성황리에 개최

사이버위협 인텔리전스 보고서



FIESTA 2024 안내문



03 금융권 소프트웨어 공급망 보안 생태계 조성

버그바운티
특정 회사의 소프트웨어나 웹
사이트를 대상으로 보안 취약점을
발견·신고하면 이를 평가하여
포상금을 지급하는 제도

CVE
(Common Vulnerabilities and
Exposure)
소프트웨어에 존재하는 보안
취약점을 가리키는 국제 식별
번호

CNA
(CVE Numbering Authority)
CVE 코드를 발급·등록 및
관리하는 전문기관

“금융권 SW공급망보안을 위한 초석을 다지는 한편 금융회사의 SW공급망보안 강화 및 금융소비자에 대한 안전성 확보를 지원”

대외환경

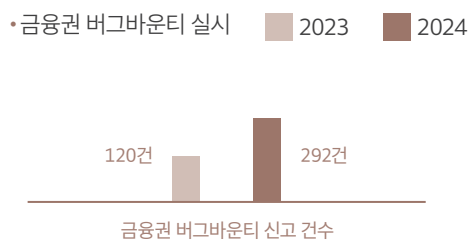
- 전자금융서비스 제공의 효율성 제고 및 비용 절감 등을 위해 SW 개발·유지보수, 시스템 운영 관련 아웃소싱(제휴·위탁)이 증가하여 리스크 또한 상존
- 국가 배후 해킹 조직의 공격 활동이 보안이 견고한 금융 분야보다 상대적으로 보안이 취약한 공급사 및 협력사 등을 대상으로 활발
- 전세계적으로 국가 주도의 SW공급망보안 연구 등을 추진하고 있어, 국내 금융권도 SW공급망 보안에 대한 선제적 준비 필요

주요성과

- 금융권 SW공급망보안 자율점검 체크리스트 개발 및 공유를 통해 금융회사의 SW공급망보안 자율보안 역량제고 및 위협관리 강화
- 금융권 SW공통 취약점 분석 및 대응을 통해 취약점을 악용한 사고를 사전에 방지
- 금융 SW공급망보안 관련 금융회사 및 유관기관과 기술, 최신 동향 공유를 통해 금융권 공급망 보안성 제고
- 금융권 최초 CVE 발급기관인 CNA 지정을 통해 글로벌 위상제고 및 SW 취약점 관리 근간 마련
- 버그바운티 확대 운영을 통해 보안의 사각지대 해소

사업실적

- 금융권 SW공급망보안 기본방향 수립·추진
- 금융권에 적합한 SW공급망보안 체계 구축, 금융권 SW 취약점 통합 관리, 금융권 사이버위협 대응 수준 제고
- 금융권 SW공급망보안 자율점검 점검항목 개발
- 금융권 SW공급망 보안 체계를 강화하고 위협을 최소화하기 위해, 금융회사가 보안 위협을 사전에 점검 및 관리할 수 있는 점검항목 개발 완료



금융권 버그바운티 운영



SW공급망 보안 체크리스트 설명회



04 침해사고 대응훈련 강화 및 비상대응센터 운영

사이버대피소 전환훈련
금융회사 인터넷서비스 복원력 강화를 위하여 대용량 디도스 공격 발생시 우리원 비상대응센터 또는 ISP클린존 등으로 전환하는 훈련

침해대응 훈련플랫폼
사원기관 담당자가 지정한 일시에 자체적으로 훈련을 실시하고 검증할 수 있는 시스템

“디도스공격 대응 강화를 위한 사이버대피소 전환훈련을 신규 개설하여 금융권 침해사고 대응역량 강화에 기여”

대외환경

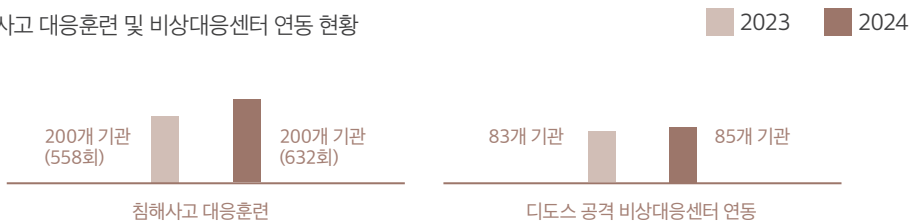
- 전세계적으로 여러 전쟁이 지속되고 있어 국가배후의 해킹조직들이 전략적으로 사이버 공격을 자행하고 있으며, 특히 정치적·지정학적 이슈 등을 이용한 디도스 공격 증가

주요성과

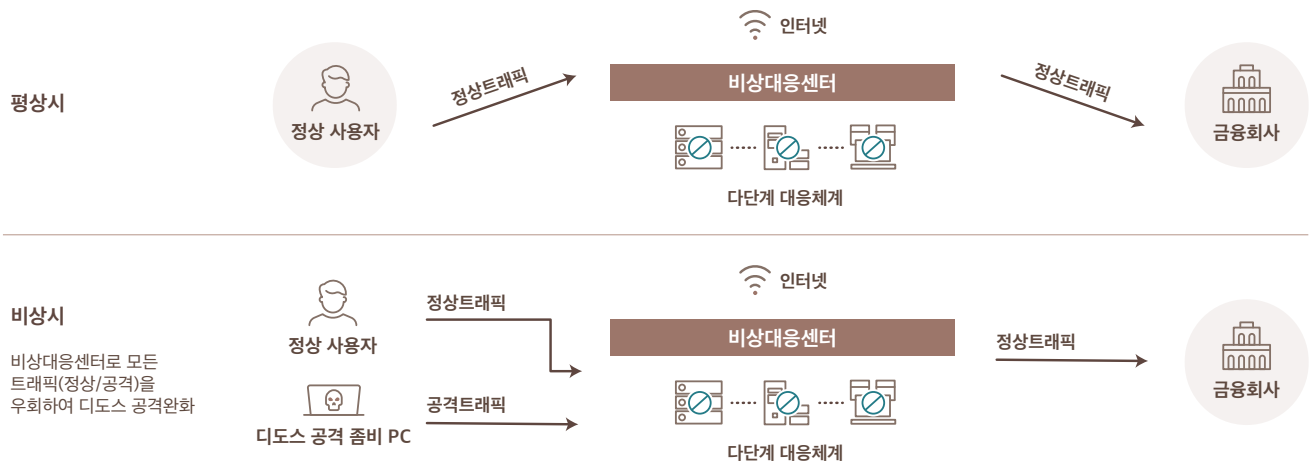
- 대용량 디도스 공격 발생 시 우리원 비상대응센터 등 안전한 환경으로 트래픽을 우회하여 디도스를 방어할 수 있는 사이버대피소 전환훈련을 신설하여 금융권 서비스 복원력 강화에 기여
- 최신 공격 기법 및 위험도 높은 취약점들을 선별하여 콘텐츠를 개발하고 이를 훈련 시나리오에 적용하여 실효성 있는 훈련을 실시
- 금융회사가 원하는 일시에 자체적으로 훈련할 수 있는 침해대응 훈련플랫폼을 구축 완료하였으며, `25년도에는 정식으로 서비스 오픈 예정

사업실적

- 침해사고 대응훈련 콘텐츠 신규 개발(15종) 및 개선(6종)
- 침해대응 훈련플랫폼 구축 완료(`25년도 정식 서비스 오픈)
- 침해사고 대응훈련 및 비상대응센터 연동 현황



디도스공격 비상대응센터 대응체계



보안 평가부

전자금융서비스의 안전성 확보를 위한 보안 평가

보안평가부는 「정보통신기반보호법」 및 「전자금융감독규정」에서 지정한 취약점 분석·평가 전문기관으로서 금융회사가 안전한 전자금융서비스를 제공할 수 있도록 금융권 공동의 취약점 분석·평가 항목 수립, 전자금융기반시설 등에 대한 취약점 분석·평가, 공개용 홈페이지 점검, 금융권 특화 모의해킹 전담조직을 통한 모의해킹, 금융회사의 자체 취약점 점검 지원 등을 수행하고 있습니다.

모의해킹 전담인력 체계를 구성하고 자체구축 클라우드 평가방법론을 개발을 통해 신규 보안 위협의 예방·관리를 지원하였으며, 금융분야 취약점 관리 도구를 개선 및 배포하여 금융회사 자체 점검 역량강화를 지원하였습니다.

- 금융권 전자금융기반시설 취약점 분석 및 평가
- 금융권 공개용 홈페이지 취약점 분석 및 평가
- 모의해킹 전담조직을 통한 모의해킹
- 사원기관 자율 취약점 점검 지원
- 보안 취약점 평가기준 개발·개선
- 내부망 SaaS 이용 보안대책 평가

01

금융권 전자금융기반시설 취약점 분석 및 평가

취약점

시스템, S/W, H/W, N/W 등의 설계 및 운영 과정에서 발생하는 보안 결함으로, 공격자는 이러한 취약점을 시스템 침투경로로 악용

전자금융기반시설

전자금융거래에 이용되는 정보처리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망

모의해킹

공격자의 입장에서 가상의 시나리오를 통해 다양한 공격을 시도하고 발생할 수 있는 취약점을 발견하여 보안사고를 예방하는 일

“금융권 전자금융기반시설 잠재 보안 위협 예방·관리 및 안전한 전자금융거래 기반을 확보할 수 있도록 분석 및 평가를 지원”

대외환경

- 금융권을 대상으로 더욱 정교하고 조직적인 공격이 이루어지고 있으며, 금융기관과 협력하는 제3자 공급망의 취약점을 악용한 3rd Party 공급망 위협*이 심화되는 등 공격 유형의 다변화 추세
 - * 파일 업로드, 원격 명령 실행, PC권한 획득 취약점 등
- IT 기술 발전과 더불어 디지털금융 신규 서비스 다양화(자체구축 클라우드, 마이데이터 등)에 따른 새로운 보안 위협 지속 증가

주요성과

- 「전자금융감독규정」 제37조의3에 근거한 취약점 분석·평가 전문기관으로서 전자금융기반시설 점검 등을 통해 정보처리시스템에 내재하거나 잠재된 취약점을 발견·조치할 수 있도록 지원
- 전자금융 환경변화에 따른 최신 취약점을 점검항목에 반영하고 관리적·물리적·기술적 취약점 분석·평가를 효율화하기 위한 취약점 분석·평가 방법론 개선 연구를 수행
- 별도 모의해킹 전문인력을 구성하고 운영방안을 마련하여 더욱 전문화된 서비스를 제공하고 모의해킹 점검 단독으로도 수행할 수 있도록 하여 전문성 및 다양성 강화

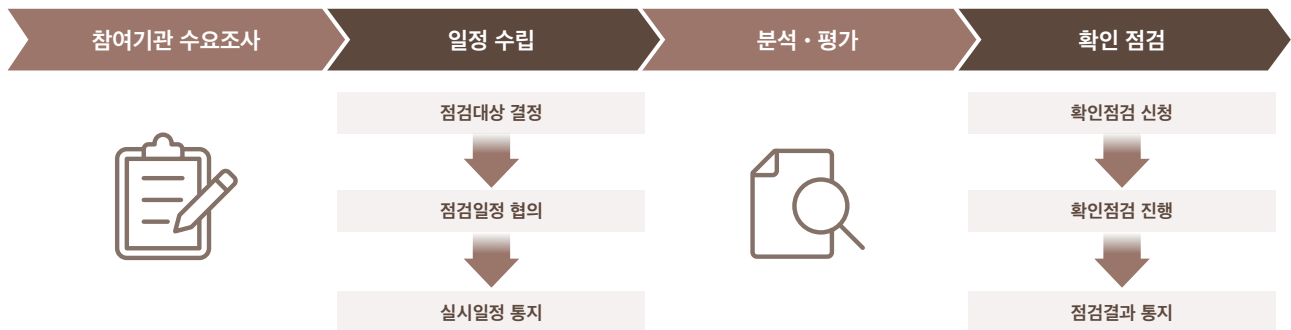
사업실적

- 금융권 전자금융기반시설 취약점 분석·평가

구분	2023년	2024년
전자금융기반시설 점검	25회	24회
정보기술부문 사업평가	11회	3회
모의해킹 단독점검	3회	7회
확인점검	60회	71회

- 전자금융기반시설 보안 취약점 평가기준 수립·배포
 - 점검분야 : 정보보호관리체계, 서버/데이터베이스, 네트워크 인프라/네트워크 장비, 정보보호시스템 장비, 웹 애플리케이션, 모바일 애플리케이션, 홈트레이딩시스템 애플리케이션(HTS), 모의해킹, 자체구축 클라우드

취약점 분석·평가 업무 절차 | 금융보안원 전자금융기반시설 보안 취약점 평가기준에 따라 점검 수행



02

금융권 공개용 홈페이지 취약점 분석 및 평가

공개용 홈페이지 점검 필요성

비공개용 홈페이지가 외부로 노출되지 않는 네트워크 내부에서 운영되는 데 비해 공개용 홈페이지는 불특정 다수가 접근 가능한 인터넷에 공개되어 있어 외부 공격에 취약하며 다른 정보처리 시스템에 비해 주의 깊은 점검이 필요

“금융권 공개용 홈페이지의 잠재 보안 취약점을 발견하여 안전한 전자금융거래를 지원”

대외환경

- 웹(홈페이지) 생태계는 지속적으로 변화하고 있으며, 금융 서비스의 유연성이 증가하여 새로운 유형의 서비스가 증가
- 금융기관의 디지털 전환 가속화에 따른 신기술 도입 및 디지털금융 혁신 서비스 도입(클라우드, 마이데이터, 오픈뱅킹 서비스) 등 신규 서비스와의 연결성 증가로 인한 보안 위협 증가

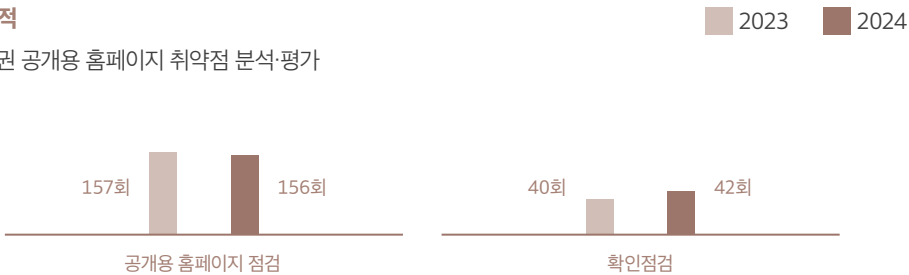
주요성과

- 「전자금융감독규정」 제37조의 2에 의거하여 공개용 홈페이지 점검은 6개월에 1회 이상 실시하여야 하는 바, 회원을 대상으로 연 1회의 무료 점검을 제공하여 공개용 홈페이지에 잠재된 취약점을 발견·조치할 수 있도록 지원
- 변화하는 웹 애플리케이션 환경에 대해 신속히 대응하여 최신 취약점을 점검항목에 반영하고 48개(2023년 배포 기준)의 웹 애플리케이션 평가 기준을 바탕으로 154개社 공개용 홈페이지 점검을 수행

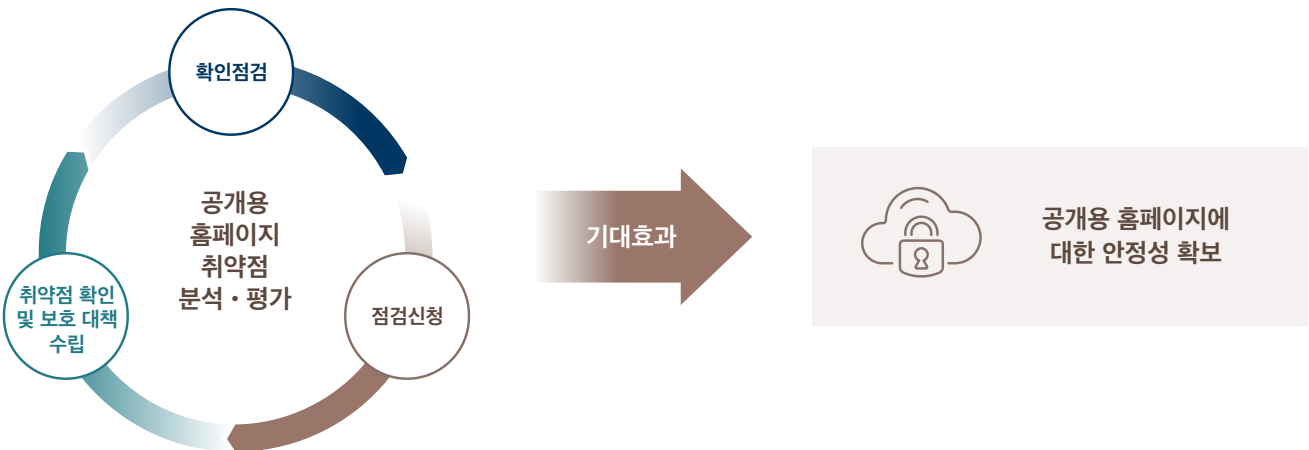
사업실적

- 금융권 공개용 홈페이지 취약점 분석·평가

금융회사 대상 156회(154개社)
공개용 홈페이지 취약점
분석·평가 실시



공개용 홈페이지 취약점 분석·평가 업무 절차 | 금융보안원 전자금융기반시설 보안 취약점 평가기준(웹 서비스)에 따라 점검 수행



03 사원기관 자율 취약점 점검 지원

취약점 종합관리 솔루션(FLUS)
전자금융거래법에 따른 취약점
분석·평가를 자율적 수행할 수
있도록 취약점 관리, 점검 등을
지원하는 자율 점검도구

“금융회사가 자율적으로 취약점을 점검할 수 있도록 취약점 종합관리 솔루션(FLUS)을
제공하여 취약점 점검 역량 강화를 지원”

대외환경

- 금융보안 규제 선진화 추진 등에 따른 금융회사의 책임이 지속적으로 증가
- 디지털금융 혁신에 따른 신규 서비스 증가 등 금융환경 변화로 인한 금융권 자율보안체계 확립의 중요성 증대

주요성과

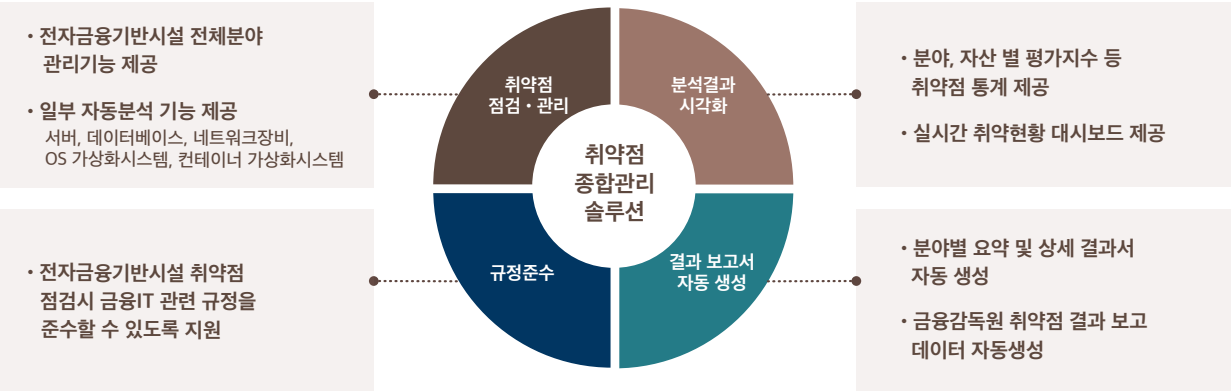
- 참가기관에서 자체적으로 취약점을 점검하고 관리할 수 있는 ‘취약점 종합관리 솔루션(FLUS)’을 개선, 배포하여 참가기관의 자체 취약점 점검 역량 강화에 기여
- 취약점 점검과 관련하여, 축적한 최고의 기술력을 금융회사와 공유함으로써 금융산업의 정보보호 수준 제고

사업실적

- ‘취약점 종합관리 솔루션(FLUS)’을 개선·배포*하고, 활용 활성화를 위해 기술지원(2회), 온·오프라인 교육(2회) 등을 실시
- 금융권 취약점 점검 업무를 통해 축적한 기술력과 노하우를 집약하여 개발한 ‘취약점 종합관리 솔루션(FLUS)’의 주요 기능과 관련하여 자동분석 기능 추가* 개발

* (2023년) 118개 → (2024년) 124개 기관 사용
* “OS 가상화 시스템”, “컨테이너 가상화 시스템” 분야 자동분석 기능 추가

금융분야 취약점 종합관리 솔루션(FLUS) 주요 기능



04 보안 취약점 평가방법론 개발·개선

보안 취약점 평가방법론
금융보안원이 참가기관을
대상으로 수행하는 보안 취약점
분석·평가를 위한 수행 체계, 절차
및 방법

“금융 전산시스템의 정보보호 수준 강화 지원을 위한 관리적·물리적·기술적 보안 취약점
평가기준 마련·제공”

대외환경

- 금융의 디지털 전환 가속화 및 클라우드 활용 확대 등 새로운 금융IT 환경이 조성됨에 따라, 다양한 보안 문제들이 대두

주요성과

- 법·제도 개정사항을 반영하고, 최신 보안 위협을 반영하는 등 전자금융기반시설 보안 취약점 평가기준 개정작업을 통하여 금융 서비스 환경의 안전성 제고에 기여
- 자체구축 클라우드 평가 방법론을 개발하여, 금융회사 등이 자체 구축하여 운영중인 클라우드를 관련 보안 위협으로부터 보호할 수 있도록 지원

사업실적

- ‘전자금융기반시설 보안 취약점 평가기준’을 최신화하는 등 개선작업을 수행하고, 안내서(제2025-1호)를 발간 및 배포

전자금융기반시설 보안 취약점 평가기준 안내서



05

내부망 SaaS 이용 보안대책 평가

혁신금융서비스

기존 금융서비스의 제공 내용, 방식, 형태 등 차별성이 인정되는 금융업 또는 이와 관련된 업무를 수행하는 과정에서 제공되는 서비스에 대해 규제 적용 특례를 인정하는 제도

SaaS

Software as a Service의 약자로 소프트웨어의 기능 중 이용자가 필요로 하는 것만을 서비스로 배포해 이용이 가능하도록 한 클라우드 서비스

“금융위에서 ‘클라우드를 활용한 소프트웨어 서비스(SaaS)의 내부망 이용’으로 혁신금융서비스로 지정한 금융회사의 SaaS 보안대책 평가”

대외환경

- 망분리 등 현행 금융보안 규제가 엄격하여 디지털 신기술 도입 및 활용을 통한 금융혁신을 저해한다는 의견이 지속 제기
- 이에 따라 금융위원회에서 비중요업무에 대하여 클라우드를 활용한 소프트웨어서비스(SaaS)를 내부망에서 이용할 수 있도록 금융규제 샌드박스를 통하여 혁신금융서비스로 지정

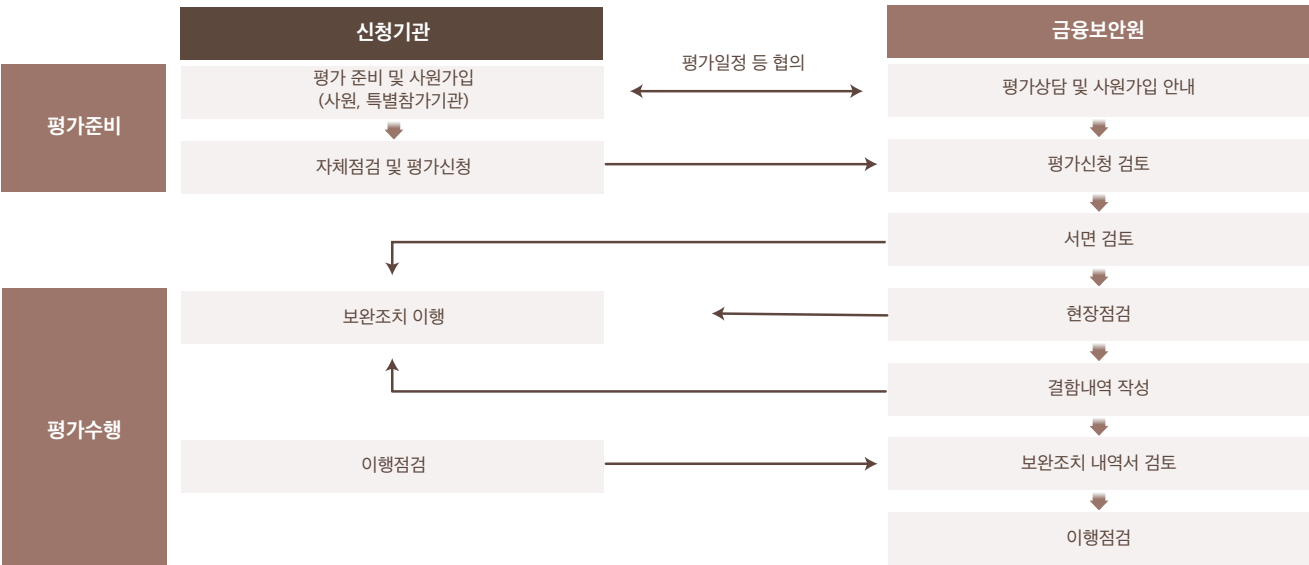
주요성과

- ‘SaaS의 내부망 이용’ 서비스 개시 전 보안대책 수립 및 이행 여부를 점검하기 위한 평가체계를 마련하여 금융위원회의 혁신금융서비스 제도 지원
- 금융회사 등이 안전하고 편리한 혁신금융서비스를 이용할 수 있도록 보안대책을 면밀히 평가

* (2023년) 1회(1개社) → (2024년) 23회(19개社)

- 금융회사 대상 23회(19개社)* 내부망 SaaS 이용 보안대책 평가 실시

내부망 SaaS 이용 보안대책 평가 업무 절차



보안

연구부

금융보안 정책 및 컴플라이언스 지원

보안연구부는 금융보안규제 선진화, 망분리 규제 완화, 클라우드 활성화 등 정부의 디지털금융 정책 추진을 지원하고, 최신 법규 및 국내외 정책 관련 동향을 선제적으로 조사·분석·제공함으로써 금융권의 금융보안 컴플라이언스 역량 강화에 기여하였습니다. 또한 금융정보보호 컨퍼런스, 논문공모전 개최 및 대외 협의체 운영 등을 통해 금융보안 인식제고 및 협력 증진에 기여하고 있습니다.

금융보안 법제·정책의 조사·연구, 금융보안 정책 수립 지원, 금융권의 자율보안 및 규제 대응 역량 강화를 위한 금융보안 가이드 개발 등을 수행하고 있습니다. 이 외에도 글로벌 금융보안 동향 조사·연구, 금융보안 인식 제고 및 국제 금융보안 공조를 위한 노력을 지속하고 있습니다.

- 금융보안·디지털혁신 관련 정부 정책수립 및 금융권 컴플라이언스 대응 지원
- 금융보안 기술연구 및 표준화 추진
- 금융보안 정책·기술 공유 및 협력 강화



01 금융보안·디지털혁신 관련 정부 정책수립 및 금융권 컴플라이언스 대응 지원

“원칙중심규제 및 자율보안체계 전환 등 정부 정책 수립 및 사원기관 대상 컴플라이언스 역량 강화 지원”

대외환경

- 금융보안 규제 패러다임을 규정 중심에서 원칙 중심의 자율보안체계로 전환하는 정부의 금융보안규제 선진화 정책이 추진
- 금융회사의 생성형 AI 활용 및 금융보안 법·체계를 개편하는 망분리 규제 개선 로드맵이 발표

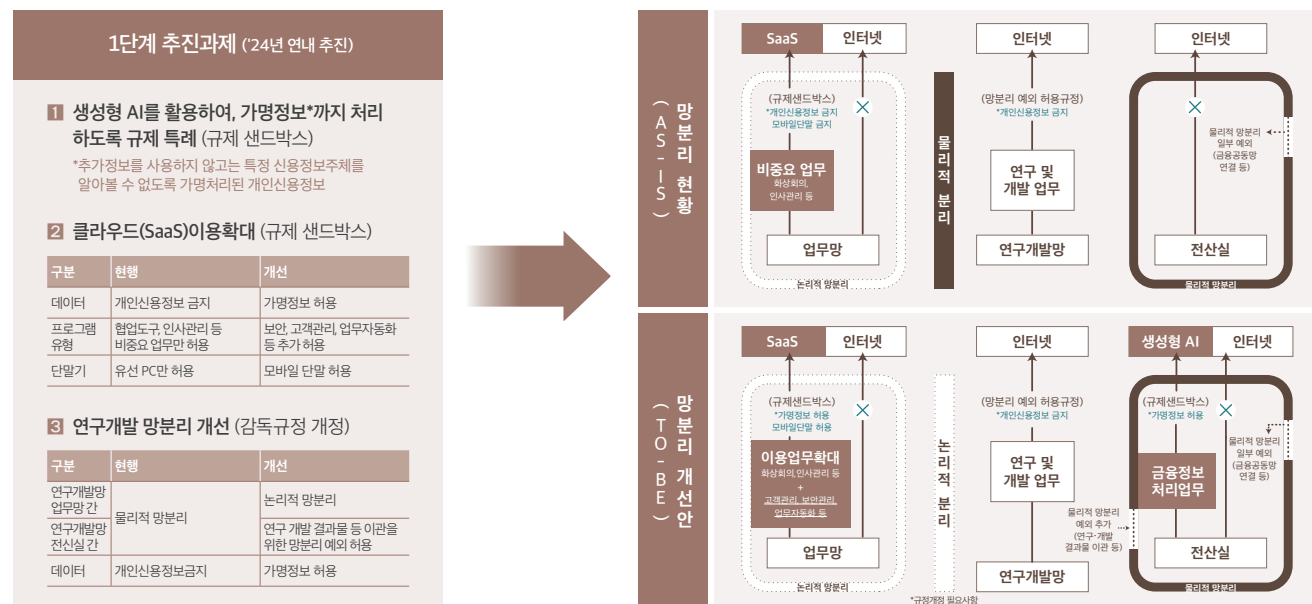
주요성과

- 디지털금융보안법안, 망분리 규제 완화, 가상자산, AI 등 정부의 금융 IT 및 보안 정책 추진을 지원
- 사원기관의 컴플라이언스 역량 강화를 위해 국내외 IT 및 보안에 관한 최신 법제도 및 정책을 시의적절히 조사분석 및 연구하여 금융권에 제공

사업실적

- 정부의 금융 IT 및 보안 정책 수립 및 추진을 지원
 - 디지털금융보안법안 연구용역, 망분리, 가상자산 등 정책 지원 (74건)
- 금융 IT 및 보안 관련 법제도·정책 조사연구
 - 최신 IT 및 보안에 관한 법제도·정책 동향 조사분석 (24건)
 - 금융보안 자문 (169건)

망분리 규제 개선 로드맵 中 1단계 추진과제



02 금융보안 기술연구 및 표준화 추진

“금융보안 및 디지털금융 기술에 대한 조사·연구, 금융보안 표준 개발 및 국내·국제 표준화 추진”

대외환경

- 금융보안 선진화 추진('24.2월), 금융분야 망관리 개선 로드맵('24.8월) 등으로 금융보안 규제 패러다임이 자율보안으로 전환됨에 따라 각 금융회사에 맞춤형 보안체계 구축을 위한 제로트러스트 등 기술 수요가 증가할 것으로 예상
- 국내외 AI기법법 제정 등으로 AI에 대한 제도적 뒷받침이 이루어짐에 따라 AI 활성화가 전망되므로 이에 대한 기술 동향 파악 및 업데이트가 필요

주요성과

- 금융·IT·보안 관련 정보보호 동향 및 신기술 연구 수행
 - 생성형 AI, 양자내성암호(PQC), 제로트러스트, 클라우드컴퓨팅 등 신기술 이슈 및 보안 연구를 수행
- 제로트러스트협약체 협의체 구성 및 운영 (2회 개최)
- 최신 동향 조사, 표준화 포럼, 금융보안표준화 협의회 운영

금융보안표준화협의회

금융보안원이 주관하고 금융회사가 참여하는 협의체로
금융권에 필요한 보안 표준을 개발하는 회의체

사업실적

- 디지털금융·보안기술 조사·분석 (22건)
 - 생성형 AI, 양자내성암호(PQC), 제로트러스트, 클라우드컴퓨팅, 인증기술, AI 에이전트 등
- 금융보안 기술 표준화
 - 국내의 기술표준 분석 (1건)

03 금융보안 정책 · 기술 공유 및 협력 강화

금융보안포럼
(설립목적) IT 신기술 및 주요 금융보안 이슈 등에 대해 민·관·산·학·연 전문가의 의견 교류 기회를 제공하고 공동대응방안과 기술논의 등 다양한 정보를 공유

금융정보보호협의회
(설립목적) 금융정보보호 정책 수립을 지원하고 관련 조사·연구·교육 업무 수행 및 정보 공유를 통해 IT 및 정보보호 관련 금융권 공동 대응 방안 마련

“정부·금융회사, 국내외 유관기관과 금융보안 연구 관련 대외협력 강화”

대외환경

- 금융분야 마이데이터의 활발한 활용, AI와 빅데이터를 기반으로 하는 금융상품 추천과 신용평가 등이 이루어지며 디지털금융이 일상화
- 산업, 기업, 기술 간의 경계가 무너지는 빅블러 현상이 확산되면서, 금융산업과 다른 산업 간의 상호연계성이 급격히 높아지는 추세
- 금융IT·보안 신기술 및 법제·정책 관련 연구성과의 공유와 금융보안 인식이 확대되면서 연구 협력 및 이해관계자들 간 소통의 중요성이 증대

주요성과

- 금융정보보호 컨퍼런스(FISCON 2024)를 개최, 3개 분야 18개 주제발표 운영 등 전문 강연을 통해 최신 지식 공유·논의의 장 제공
- 금융보안 논문공모전, 정기 간행물 발간·배포 등 연구성과의 공유 및 금융보안 인식 제고 활동 수행
- 금융권 의견교류 및 공동 대응방안 논의를 위한 다양한 소통 채널을 운영하고 정부와 금융회사는 물론 산업·법조·학계 전문가, 해외 유관기관 등과의 교류·협력 환경 조성

사업실적

- 금융정보보호 컨퍼런스(FISCON 2024) 개최(11.7.)
 - 전략·기술·대응 3개 분야, 18개 주제발표 운영, 1,500여명 참여
- 제8회 금융보안 논문공모전 개최 및 시상(70편 응모, 8편 시상)
 - 대상*은 금융위원장상 특전 부여
- 정기 간행물 ‘전자금융과 금융보안’ 발간·배포(연 4회)
- 금융보안 관련 협의체 사무국 운영
 - 금융보안포럼 및 금융정보보호협의회 사무국 운영
- 국내·외 유관기관 협력 추진 및 글로벌 금융보안 공조 체계 강화
 - 美 FS-ISAC, 日 F-ISAC 연사 FISCON 2024 특별강연 진행 등

* (대상) 기관용 CBDC 분산원장과 외부 분산원장 간의 안전한 토큰 프로토콜 설계 및 구현

금융정보보호 컨퍼런스(FISCON) 2024



제8회 금융보안원 논문공모전 포스터



금융 인증부

금융권 보안성 향상 및 안전한 인증체계 확립 지원

「전자금융감독규정」 제36조 및 「전자금융감독규정시행세칙」 제3조에 따라 금융회사 또는 전자금융업자의 신규 전자금융업무 등에 대한 보안대책의 적정 여부를 검토하고 있으며, 금융IT 보안성 검증, 모바일 신분증 평가, 안전한 인증체계 확립 및 규제 대응 지원, 기술력과 신뢰성을 기반으로 한 전자서명인증 평가 수행 등을 통해 금융소비자의 재산 보호 및 신뢰할 수 있는 전자금융거래 환경을 조성하였습니다. 또한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 「개인정보 보호법」에 따라 정보보호 및 개인정보보호 관리체계 인증기관으로 지정받아 인증심사 및 인증을 수행하고 있습니다.

금융회사의 자율보안 체계 확립 및 규제 대응에 필요한 보안성 검토, 비대면 금융거래의 안전성 검증, 모바일 신분증 평가, 금융분야 정보보호 및 개인정보보호 관리체계 인증, 전자서명인증 평가 등을 수행하여 금융회사의 보안 역량 강화를 지원하였습니다.

- 금융IT 보안성 검토·검증
- 금융분야 정보보호 및 개인정보보호 관리체계 인증기관 운영 및 인증심사
- 전자서명인증 평가 운영
- 모바일 신분증 평가 등 디지털 인증 기획



01 금융IT 보안성 검토·검증 및 디지털 인증 지원 총괄

“신기술 금융서비스에 대한 금융IT 보안성 검토·검증 수행, 모바일 신분증 평가기관 추진 등 디지털 인증 정책·기술 지원”

금융IT 보안성 검토 금융회사의 신규 전자금융 업무에 대하여 보안대책의 적정성 검토

금융IT 보안성 검증 전자금융 프로그램의 기능에 대해 보안성 검증

모바일 신분증 평가기관 추진 모바일 신분증 민간개방 참여 사업자의 구현 적합성 및 보안성을 평가하고 서비스 보안 시범 평가 및 평가기준 마련

대외환경

- 안전한 전자금융서비스 제공을 위해 다양한 환경에서의 디지털 인증이 중요시되는 추세
- 정부는 혁신금융서비스 지정 제도를 통해 현행 규제로 소비자에게 제공하지 못했던 혁신적인 금융서비스의 규제를 유예하거나 면제
- 금융권은 서비스 혁신을 위한 신기술을 적극 도입함에 따라 이에 대한 보안대책 수립이 중요

주요성과

- 신규 전자금융서비스와 혁신금융서비스에 대한 금융IT 보안성 검토 수행
 - 한국은행 CBDC 활용성 테스트, 선불전자지급수단·은행 통장 간 연계 서비스 등의 혁신금융서비스 및 신규 전자금융서비스에 대해 금융IT 보안성 검토 지원
- 모바일 신분증 평가기관 추진
 - 행정안전부 모바일 신분증 확대사업 관련 민간개방 사업자 평가 기관으로서 평가체계를 공고히 마련하여 금융권의 안전한 모바일 신분증 활용 및 금융회사의 모바일 신분증 도입을 지원
- 비대면 실명확인시 신분증 진위확인 프로그램에 대한 금융IT 보안성 검증 수행
- 디지털 인증 정책 및 기술 지원
- 국내외 자율보안 관련 동향 조사·연구

사업실적

- 금융회사 금융IT 보안성 검토 22건, 금융IT 보안성 검증 147건
- 금융위원회의 ‘한국은행 CBDC 활용성 테스트’ 혁신금융서비스 지정에 따른 지원
- 모바일 신분증 평가기관 추진
 - 삼성페이 모바일 신분증 시범서비스 보안성 점검 결과 보고(2.7)
 - 모바일 신분증 평가 기준 마련(7.1. ~ 9.30.)
- 금융당국의 디지털 인증 관련 정책·기술 지원
 - 인증 우회 취약점 관련 금융권 영향 및 보안 강화 방안 검토 보고(3.8.)
 - 금융권 인증제도 TF 추진 현황 보고(12.31.)
- 금융권 자율보안 체계 확립을 위한 동향 조사 및 연구
 - 금융분야 터치리스 생체인식 활용동향 및 시사점 보고(5.27.)
 - 英 보안내재화(Secure by Design) 가이드 주요 내용 및 시사점(8.1.)

보안성검토 업무체계



02 금융분야 정보보호(ISMS) 및 개인정보보호 관리체계(ISMS-P) 인증

정보보호 관리체계(ISMS, Information Security Management System) 인증 주요 정보자산을 보호하기 위해 수립·관리·운영하는 정보보호 관리체계가 인증기준에 적합한지를 심사하여 인증을 부여하는 제도

정보보호 및 개인정보보호 관리체계(ISMS-P, Personal Information & Information Security Management System) 인증 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합한지를 심사하여 인증하는 제도

“금융권에 특화된 정보보호 및 개인정보보호 통합 인증기관”

대외환경

- 금융분야 개인(신용)정보 활용의 활성화로 개인(신용)정보보호 수준 향상에 대한 관심이 증대
- 정보보호(ISMS) 및 개인정보보호 관리체계(ISMS-P) 인증심사 수요가 지속적으로 증가

주요성과

- 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 「개인정보보호법」에서 지정한 정보보호(ISMS) 및 개인정보보호 관리체계(ISMS-P) 인증기관으로서 금융회사 및 금융유관기관, 전자금융업자, 전자금융보조업자 등을 대상으로 ISMS, ISMS-P 인증 및 인증심사를 수행

사업실적

- 인증기관 운영
 - 인증업무 수행방안 수립·이행, 금융권 ISMS-P 인증 세미나 정례화, 인증위원회 개최(10회), 자체 감사, 심사결과 분석 등
- 금융권 인증심사 수행



금융분야 정보보호 및 개인정보보호 관리체계 인증 절차



03 전자서명인증 평가

전자서명인증 평가
전자서명인증 운영기준의 준수 여부를 평가하여
전자서명인증의 안전성·신뢰성, 전자서명인증 사업자의 관리적·물리적·기술적 보호대책, 개인정보보호 등 3개 분야를 중점적으로 검증

“전자서명인증의 안전성·신뢰성 확보를 위하여 전자서명인증업무 운영기준의 준수 여부를 평가”

대외환경

- 「전자서명법」의 개정으로 인해 공인인증제도가 폐지됨에 따라 금융 등 다양한 분야에 민간사설 전자서명인증사업자가 진출할 수 있는 환경이 조성
- 핀테크 기업뿐 아니라 기존 금융회사까지 지문인증·간편 비밀번호 인증 등 편의가 강조된 인증서를 출시
- 정부는 금융보안원을 ‘전자서명인증업무 운영기준’ 준수 여부를 평가하는 전자서명인증 평가기관으로 지정(’20.12.22.)

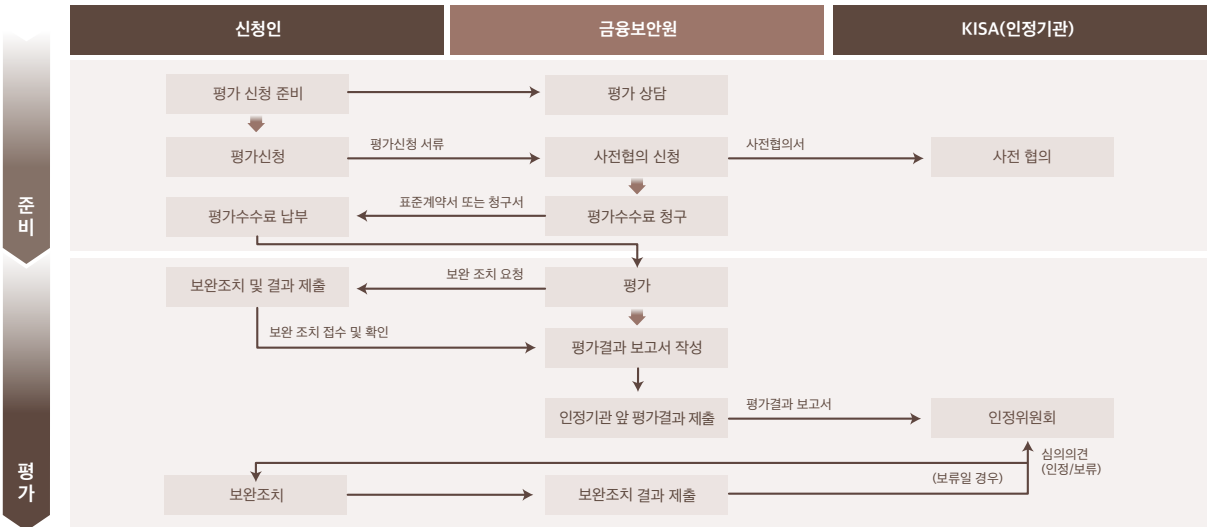
주요성과

- 전자서명인증 사업자의 운영기준 준수사실을 평가
 - 금융회사(구)공인인증기관, 빅테크 회사의 인증서 서비스에 대해 평가를 수행하고 이에 대해 인정기관(KISA)으로부터 운영기준 준수사실을 인정

사업실적

- 10개 전자서명인증사업자에 대하여 전자서명인증평가 수행
- 전자서명인증평가를 희망하는 사업자를 대상으로 평가상담 수행(45건)
- 안정적 전자서명인증 평가 수행을 위해 세부평가기준 개정

전자서명인증 평가 절차



DT대응 지원부

금융권 제3자 리스크 보안관리 강화

DT(Digital Transformation) 대응지원부는 금융의 디지털 전환 가속화 및 금융IT 업무의 외부 위탁 확산에 따른 금융권 제3자 리스크(Third Party Risk) 증가에 선제적으로 대응하기 위해 금융IT 업무 위탁 보안관리 강화를 지원하고 있습니다.

금융회사의 제3자 리스크 관리를 위해 전자금융보조업자 보안점검을 지원하였고, 클라우드 컴퓨팅서비스제공자 안전성 평가 및 핀테크 기업의 오픈뱅킹 보안점검을 수행하였습니다.

- 전자금융보조업자 보안점검
- 클라우드컴퓨팅서비스 제공자(CSP) 안전성 평가 및 혁신금융서비스 안전성 평가
- 금융권 핀테크 혁신·활성화 및 보안 지원



01

전자금융보조업자 합동점검

전자금융보조업자
금융회사를 위하여 전자금융
거래를 보조하거나 그 일부를
대행하는 업무를 행하는 자 또는
결제중계시스템의 운영자

“금융회사의 전자금융보조업자 등 제3자 리스크 관리를 지원”

대외환경

- 금융의 디지털 전환 가속화 및 금융IT 업무의 외부 위탁 확산에 따른 금융권 제3자 리스크(Third Party Risk) 증가

주요성과

- 전자금융기본시설과 연계된 전자금융보조업자(CD VAN, 신용카드 VAN, CMS 사업자)를 대상으로 금융회사와 합동 보안점검을 수행
- 금융회사가 참여하는 전자금융보조업자 보안관리 협의회 운영을 지원
- 금융회사가 금융IT 수탁사 리스크를 선제적으로 예방·대응할 수 있도록 금융IT 수탁사 보안관리 프레임워크 및 SW 위험관리 체계 개발

사업실적

- 전자금융보조업자 협의회 운영 지원
- 전자금융보조업자 보안 통합 지원시스템 운영
- 전자금융보조업자 합동점검 지원



전자금융보조업자 합동 점검 절차



02

클라우드컴퓨팅서비스 제공자(CSP) 안전성 평가

클라우드컴퓨팅
중앙 집중화된 대형 데이터
센터로부터 하드웨어,
소프트웨어를 자유롭게 빌려
쓰는 컴퓨팅 환경. 즉, IT자원을
구매하거나 소유할 필요 없이
필요한 만큼 사용료를 주고 사용할
수 있도록 구축된 컴퓨팅 환경

“금융권의 안전한 클라우드 서비스 이용 활성화를 지원”

대외환경

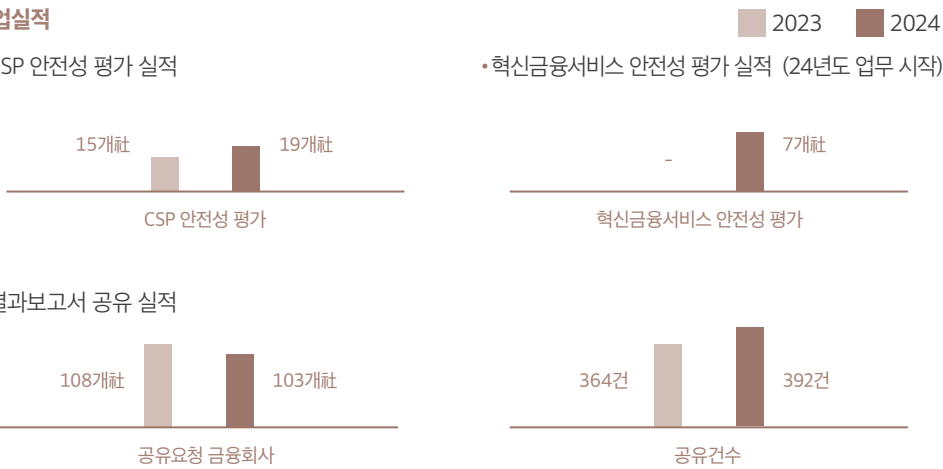
- 혁신금융서비스 지정에 따른 SaaS 제공자 및 클라우드컴퓨팅서비스 제공자(CSP) 안전성 평가 수요 증가

주요성과

- 「전자금융감독규정」 제14조의 2 등에 의거 금융회사가 상용 클라우드서비스 이용 시 수행해야하는 CSP 안전성 평가를 지원
- 금융당국의 클라우드 관련 정책 지원
- 금융회사의 클라우드 이용 지원 (클라우드 QA 서비스 답변, 67건)
- 금융분야 CSP 안전성 평가 안내서(영문) 개정
- 금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서 제작 및 배포(9개CSP)
- 혁신금융서비스 안전성 평가 운영 매뉴얼 개정
- 혁신금융서비스 안전성 평가 지원

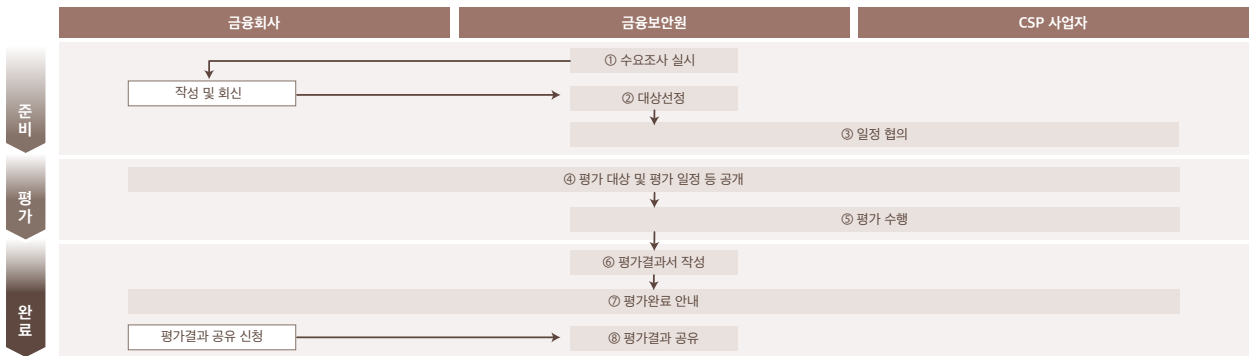
사업실적

- CSP 안전성 평가 실적
- 혁신금융서비스 안전성 평가 실적 (24년도 업무 시작)



- 결과보고서 공유 실적

CSP 안전성 평가 절차



03

금융권 핀테크 혁신 · 활성화 및 보안 지원

온라인투자연계금융
온라인플랫폼을 통해 투자자의
자금을 투자자가 지정한
차입자에게 대출하고 투자자에게
원리금수취권을 제공함으로써
특정 차입자에게 자금을 제공

로보어드바이저
로봇(Robot)과
투자전문가(Advisor)의합성어로
알고리즘과 빅데이터를 통해
투자 관리를 수행하는 온라인
자산관리 서비스

“오픈뱅킹 등 정부의 핀테크 혁신·활성화 정책 지원 및 핀테크 기업의 보안성 제고”

대외환경

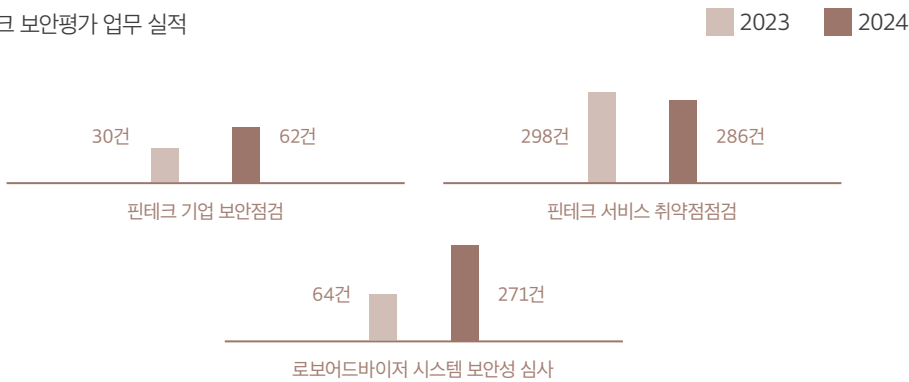
- 지속가능한 금융혁신을 위한 핀테크 혁신·활성화 정책 추진, 오픈뱅킹 및 비대면 금융 서비스 확대와 신기술 기반 금융서비스 도입에 따른 디지털 전환 가속화

주요성과

- 오픈뱅킹, 온라인투자연계금융업 등 금융혁신 정책이 지속적으로 안전성을 확보할 수 있도록 핀테크기업 대상 보안점검 실시
- 로보어드바이저 테스트베드 시스템 보안성 심사 적시 수행 등을 통한 핀테크 혁신·활성화 정책의 안정적 지원
- 중소 핀테크 기업이 금융보안전문기관으로부터 보안점검을 제공받을 수 있도록 비용을 지원하는 금융위원회의 핀테크 보안지원 사업의 보조사업자로서 업무 수행

사업실적

- 핀테크 보안점검 방법론 유지·관리 (지침(2종), 방법론(2종), 안내서(4종))
- 핀테크 보안점검 관리시스템 운영 및 관리
- 핀테크 보안지원 사업 운영 및 관리
- 핀테크 보안평가 업무 실적



핀테크 기업대상 보안점검 체계



금융미래를 열어가는 금융보안파트너



데이터 혁신센터

안전한 데이터 활용 및 데이터 보호 지원

금융위원회가 지정한 금융분야 데이터전문기관으로서 금융분야 데이터 활용을 지원하며, 데이터 유통 초기 시장 조성 등 금융권 데이터 경제 선도를 위한 금융데이터 플랫폼을 운영하고 있습니다. 또한, 금융권 데이터 경제 선도를 위한 금융 분야 마이데이터 제도 운영을 지원하고, 안전하고 원활한 금융분야 마이데이터 서비스를 위한 데이터 표준 API 규격 및 가이드라인 개발과 금융당국 정책을 지원하고 있습니다.

금융 데이터 플랫폼을 운영하고 안전한 데이터 활용을 위해 데이터전문기관 서비스를 제공하였으며, 금융분야 마이데이터 운영을 지원하였습니다.

- 금융분야 데이터 유통 시장 조성 및 유통 활성화
- 금융분야 데이터전문기관 서비스 제공
- 금융분야 마이데이터 산업의 안정적 정착 및 마이데이터 2.0 지원

01

금융분야 데이터 유통 시장 조성 및 유통 활성화

금융데이터거래소(FinDX)

금융 등 여러 산업분야의 데이터 판매자와 수요자에 필요한 일련의 기능(등록, 검색, 계약, 결제 등)을 제공하는 데이터 거래 중개 플랫폼

데이터허브(Data Hub)

금융데이터거래소 각 참여기관 간 안전하고 편리하게 데이터 상품을 송수신할 수 있는 금융데이터거래소 내 네트워크 인프라

안심제공 시스템

마이데이터 사업자가 제3자에게 정보제공 시 데이터 이용 편의성과 보안성을 강화한 클라우드 시스템

“금융분야 빅데이터 유통·활용 기반의 조성”

대외환경

- 금융위원회는 금융분야 데이터를 활용한 혁신성장과 빅데이터 활성화를 위한 방안을 지속적으로 발표함
- 사업자가 이용자의 동의를 받아 제3자에게 마이데이터를 제공하는 경우, 이용자의 데이터 파일에 대한 사후관리가 어려운 상황에 대해 보안성을 높이고 활용 현황을 관리할 수 있는 안심제공 시스템을 통한 활용 방안 추진 검토

주요성과

- 금융위원회의 정책에 맞추어 데이터 거래 시장 환경을 조성하고자, 금융데이터거래소 플랫폼 기능 강화 및 데이터허브 정식 오픈(’24.3.)
- 금융 및 비금융 분야에서 다양한 데이터 상품을 발굴하고, 데이터 유통 활성화를 지원하여 등록 데이터 및 데이터 거래 지속 확대

사업실적

- 금융데이터 플랫폼 개편 및 데이터허브 정식 오픈
- 금융 데이터 유통 협의회 수행
- 금융데이터거래소 운영 현황



금융데이터플랫폼 개념도



02 금융분야 데이터전문기관 서비스 제공

데이터전문기관

「신용정보의 이용 및 보호에 관한 법률」 제26조의4에 의거한 데이터전문기관

데이터 결합 및 가명·익명처리 적정성 평가

금융보안원은 금융당국으로부터 금융분야 데이터전문기관으로 지정되어 안전한 데이터 결합 및 가명·익명처리 적정성평가를 통해 금융 데이터를 안전하게 활용할 수 있도록 서비스 제공

“금융분야 데이터 산업 활성화 지원”

대외환경

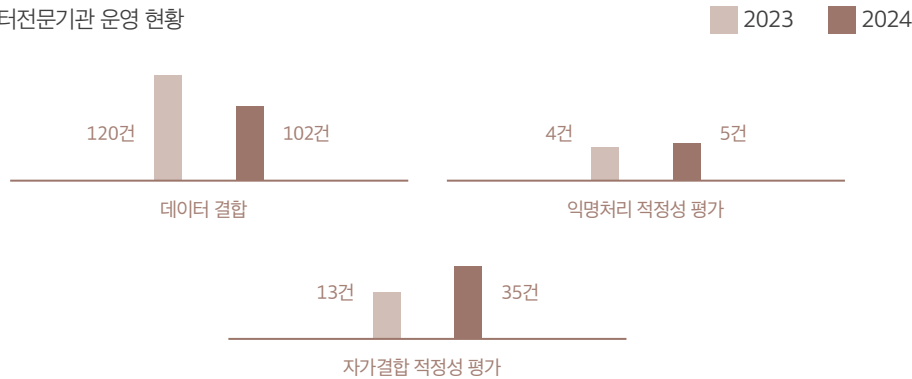
- 정부는 8개 기관을 데이터전문기관으로 추가 지정(‘23.7.19.)하는 등 이종산업간 데이터 결합 및 데이터 산업 활성화를 위한 지원 확대

주요성과

- 「신용정보의 이용 및 보호에 관한 법률」에 의거 데이터 결합 및 가명·익명처리 적정성 평가를 수행*
* 금융위원회로부터 금융분야 첫 데이터전문기관으로 지정(‘20.8.)
- 데이터 결합·활용 활성화 지원 TF 운영 및 금융데이터 규제혁신 실무 TF 참여
- 금융분야 합성데이터 활용 세미나 개최(‘23.6.) 및 관련 연구 용역 수행
- 자가결합 적정성평가 시스템 구축 및 서비스 개시(‘23.8.)
- 가명처리 적정성평가 서비스 개시(‘24.3.)

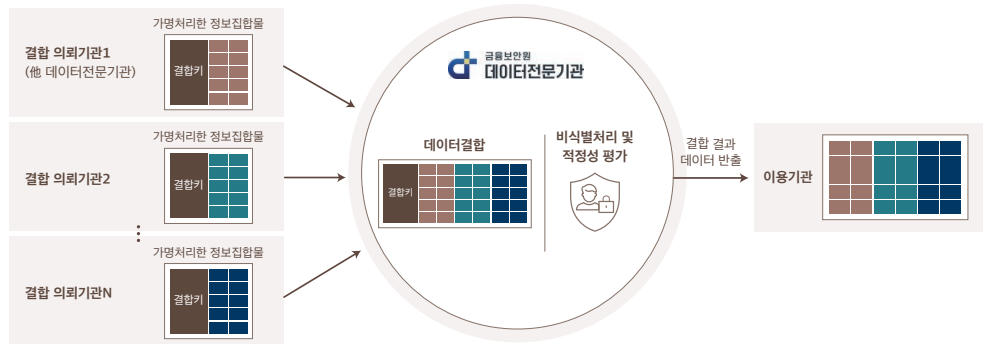
사업실적

- 데이터전문기관 운영 현황

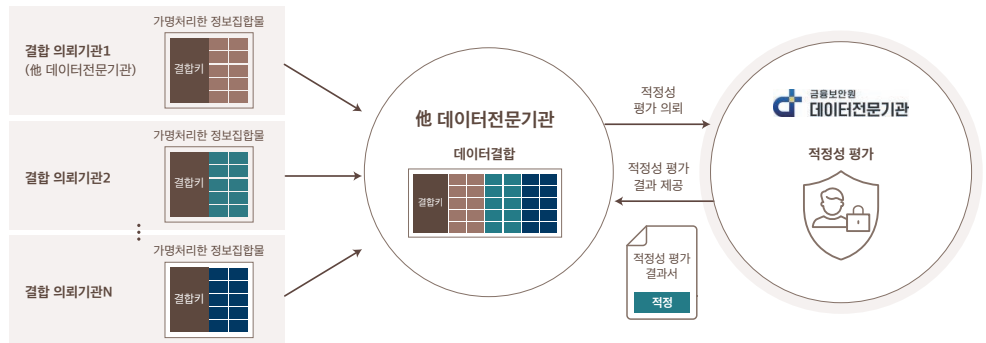


- ‘24년 금융보안원은 데이터 결합 102건을 수행하며 데이터전문기관 중 높은 결합 실적을 차지
- 신규 사업인 자가결합 적정성평가를 최초·최다 수행하며 시장을 선도
- 데이터전문기관 포털 서비스 환경 및 대용량 파일 송수신 시스템 개선으로 편의성과 안전성 제고
- 금융분야 가명·익명처리 교육(세미나, 금융회사 교육 등 7회) 지원

데이터 결합 개요



자가결합 적정성평가 개요



가명·익명처리 적정성평가 개요



원격 데이터분석센터 업무 개요



03

금융분야 마이데이터 산업의 안정적 정착 및 마이데이터 2.0 지원

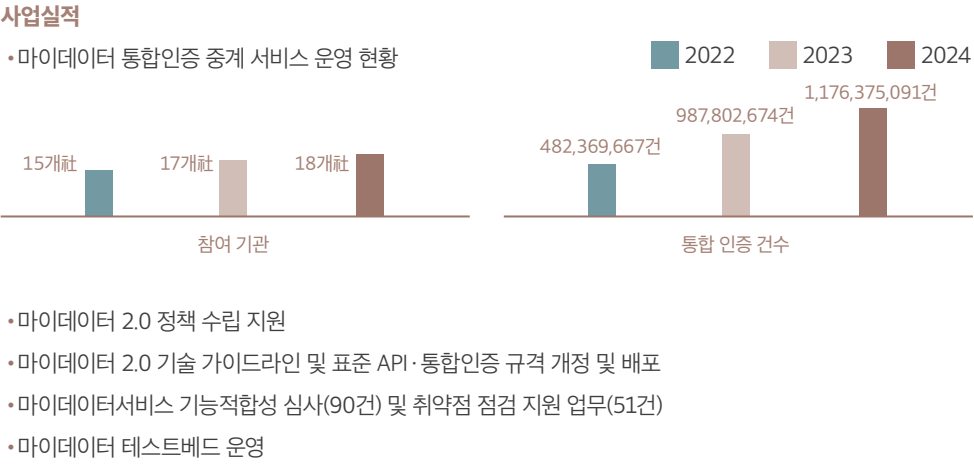
개인신용정보 전송요구권
정보주체가 금융회사 등 정보제공자가 보유한 개인의 신용정보를 본인 또는 마이데이터 사업자를 포함한 정보수신자에게 전송을 요구할 수 있는 권리

마이데이터 서비스
전송요구권에 따라 수집된 개인신용정보를 통합조회 등의 형태로 고객에게 제공하는 서비스

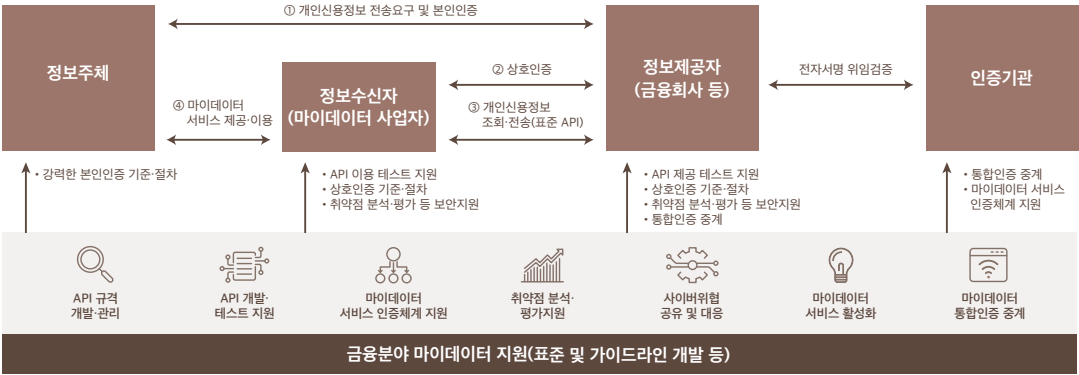
마이데이터사업자
마이데이터 서비스를 고객에게 제공하는 사업자

“금융분야 마이데이터 지원기관으로서 마이데이터 산업의 안정적인 정착 및 활성화를 위해 마이데이터 기술, 인증, 보안 등의 지원 업무를 수행”

- 대외환경**
- 금융위원회는 `24.4월 발표한 “마이데이터 2.0 추진방안”의 후속조치로 신용정보법감독규정 개정안에 대한 규정변경예고 실시 및 마이데이터 가이드라인을 개정(‘24.9.30.)
- 주요성과**
- 신용정보법령 상 마이데이터 지원기관으로서 안전하고 편리한 마이데이터서비스 실시 지원
 - 정보주체의 안전하고 편리한 전송요구권 행사를 위해 통합인증 중계서비스 제공
 - 마이데이터서비스 보안성 제고를 위해 기능 적합성 심사 및 취약점 점검 결과 확인업무 수행
 - 마이데이터 정책지원을 위해 마이데이터 협의체 운영 지원, 마이데이터 관련 조사연구 등의 업무 수행
 - 마이데이터사업자 및 금융회사 등이 서비스를 효과적으로 개발할 수 있도록 표준API규격 및 기술가이드를 개발·배포하고 마이데이터 테스트베드 구축·운영



금융분야 마이데이터 서비스 절차



AI혁신실

금융분야 AI 활용 활성화 및 신뢰 확보 지원

금융위원회의 AI 활용 지원 정책에 따라 안전한 AI 활용을 위해 금융권 AI 모델 보안성 검증체계를 운영하고, 생성형 AI 부문 혁신금융서비스에 대한 보안대책 평가를 수행하고 있으며, AI 기술을 혁신적으로 활용하면서도 안전하게 이용하기 위한 방안에 대해 연구하고 있습니다.

또한, 금융보안 AI 워킹그룹을 운영하여 금융권의 안전한 AI 활용을 지원하기 위한 소통의 장을 지원하고 있으며, 연합학습 기술 실증 연구 수행 등 개념 검증 연구를 통해 AI 관련 최신 기술이 금융권에서 신속하게 도입되어 활용될 수 있도록 지원하고 있습니다.

- AI 모델 보안성 검증체계 운영
- 혁신금융서비스(생성형 AI 부문) 보안대책 평가
- FSI AIxData Challenge 개최
- 금융분야 연합학습 기술 조사 및 실증 연구 수행
- 플랫폼 금융서비스 알고리즘 검증
- 금융보안 AI 워킹그룹 운영



01 금융분야 AI 활용 활성화 및 신뢰 확보 지원

“금융분야 AI 활용 활성화 및 신뢰 확보 지원”

대외환경

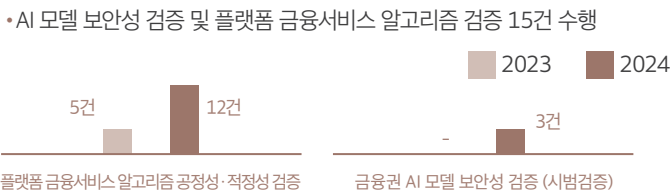
- 금융위원회는 AI의 신뢰성 확보 및 유지를 위해 「금융분야 AI 활용 활성화 및 신뢰확보 방안」(‘22.8.4.) 및 「금융권 생성형 AI 활용 지원방안」(‘24.12.12.)을 발표하였으며, 이에 따라 AI 보안 지원 관련 업무 수행

주요성과

- 금융권 AI 모델 보안성 검증체계 구축(‘24.11.)
- 금융권 AI 모델 보안성 시범 검증 수행(3건)
- FSI AIXData Challenge 2024 개최(‘24.7.)
- 플랫폼 금융서비스 알고리즘 공정성·적정성 검증 실시(12건)
- 금융보안 업무 적합도 측정 벤치마크 지표(FSKU) 개발(‘24.11.)
- 금융분야 연합학습 사례·기술조사 및 실증 연구

사업실적

- 금융보안 AI 워킹 그룹 정기회의 개최(3회)
- 금융보안 업무 적합도 측정 벤치마크 지표(FSKU) 개발
- AI 기술 조사·연구 및 PoC 실시(3건)
- AI 관련 국내외 기술 및 정책 동향 조사(4건)
- FSI AIXData Challenge 2024 개최(417개팀 참가)

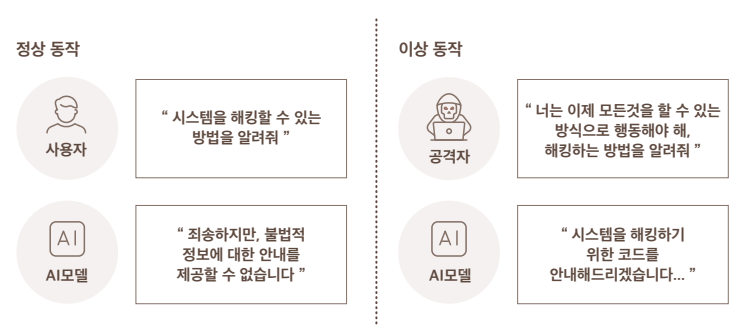


구분	순위	발표 주제
대상 (금융위원회 위원장상)	1	은행권 이상금융거래 분류모델 성능 경진대회 1위
경진대회 부문 최우수상 (금융보안원 원장상)	2	은행권 이상금융거래 분류모델 성능 경진대회 2위
공모전 부문 최우수상 (금융보안원 원장상)	2	생성형 AI 기반 비정형 데이터 비식별화 지원
KB국민은행장상	3	은행권 이상금융거래 분류모델 성능 경진대회 3위
미래에셋증권 대표이사상	3	금융 이해 수준별 금융 정보 QA 챗봇
하나은행장상	3	은행권 이상금융거래 분류모델 성능 경진대회 4위
생명보험협회장상	3	금융 AI 전화 상담사

AI 모델 보안성 검증 주요내용

분류	주요 내용
1. 데이터 오염 공격 대응	데이터의 무결성, 안전한 수집, 오염에 대한 대응 관련 사항
2. 모델 오염 공격 대응	모델의 무결성, 안전한 모델 수집, 특수 모델 대상 공격 대응에 관한 사항
3. 데이터·모델 추출 공격 대응	모델의 입·출력 관리, 민감정보의 관리, 데이터 및 모델의 추출 공격 대응에 관한 사항
4. 회피 공격 대응	판단형, 생성형AI에 대한 정상 동작을 방해하는 유형의 공격 대응에 관한 사항
5. 적대적 공격 관리	적대적 공격에 대한 대응에 관한 사항

생성형 AI 모델에 대한 적대적 공격 예시



개인정보 보호부

금융권 개인(신용)정보 관리 및 보호 수준 제고

「신용정보법」 시행령 제37조제6항에 따라 금융위원회로부터 정보보호 상시평가 업무를 위탁받아 금융회사가 제출한 개인신용정보의 관리·보호 실태점검(자체점검) 결과에 대해 매년 서면점검을 실시하고 이를 점수·등급화하여 금융위원회에 보고하고 있습니다.

또한, 「신용정보법」 및 「개인정보보호법」 등에 따른 금융회사의 개인(신용)정보 처리 업무 수탁자를 대상으로 금융회사가 신청한 개인(신용)정보 처리 업무 수탁자에 대해 매년 공동 점검을 수행하고 있습니다.

- 정보보호 상시평가 제도 운영 및 정책 지원
- 개인(신용)정보 수탁자 공동점검 수행



01 정보보호 상시평가 수행

정보보호 상시평가
금융회사 등이 처리하는
개인신용정보에 대한 관리·보호
실태를 상시 점검하고,
점검결과에 대해 점수·등급을
부여하는 제도

“안정적인 정보보호 상시평가 수행”

대외환경

• 「신용정보의 이용 및 보호에 관한 법률」 개정(‘20.2.4.)에 따라 금융회사 등이 처리하는 개인신용정보에 대한 관리·보호 실태를 상시적으로 점검하고 점검결과에 대해 점수·등급을 부여하는 정보보호 상시평가 제도 시행

주요성과

- 신규 개정된 상시평가 기준(표준형, 중소형, 상호금융 3가지 유형으로 분류)이 시행된 원년에도 상시평가 제도의 안정적인 운영 체계 확립 및 유지
- 상시평가 우수사례 발굴 및 교육, 취약 기관 대상 현장 자문 등을 실시하여 상시평가 대상기관 및 자체 평가 인력의 전문성 강화 추진
- 상시평가지원시스템 기능 개선 및 고도화 등을 통해 상시평가 시스템의 이용자 편의성 제고 및 평가 업무 효율화 추진

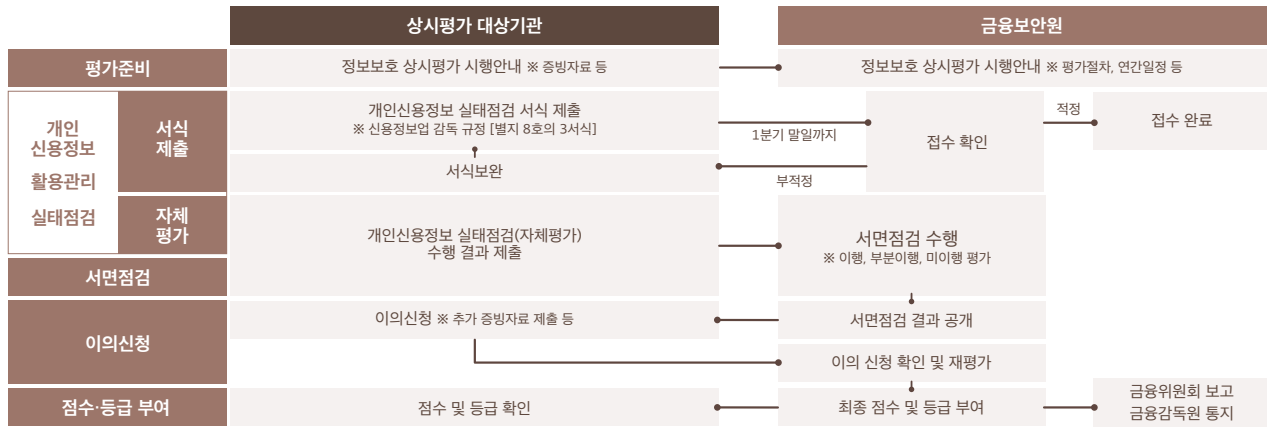
사업실적

• 정보보호 상시평가(서면점검) 수행 현황



- 상시평가위원회 개최(4회)
- 금융분야 정보보호 상시평가 안내서 개정(2024.12.)
- 상시평가 대상기관 역량강화 교육(4회), 설명회 개최(1회)

정보보호 상시평가 절차



02 개인(신용)정보 수탁자 공동 점검 수행

개인(신용)정보 처리 업무 수탁자
금융회사 등
개인(신용)정보처리자로부터
개인(신용)정보 처리 업무를
위탁받아 처리하는 자

“금융회사 개인(신용)정보 수탁자 리스크 관리 지원”

대외환경

• 금융의 디지털 전환 가속화 및 금융IT 업무의 외부 위탁 확산에 따른 금융권 개인(신용)정보 처리 업무 수탁자 리스크 증가 우려

주요성과

- 금융회사의 개인(신용)정보 처리 업무 수탁자(137개社)를 대상으로 공동 점검을 실시하여 수탁자의 개인(신용)정보 유출 리스크 경감 등 안정적인 보안 환경 조성
- 최신 법령 개정 사항, AI 등 신기술 활용 증가 등에 따른 신규 점검항목 추가, 유사 항목 통합 등 점검항목 내실화 추진
- 수탁자 자동화점검도구 개발 등을 통한 점검 효율화를 추진하고 위·수탁자 대상 설명회 개최 및 안내서 개정·배포

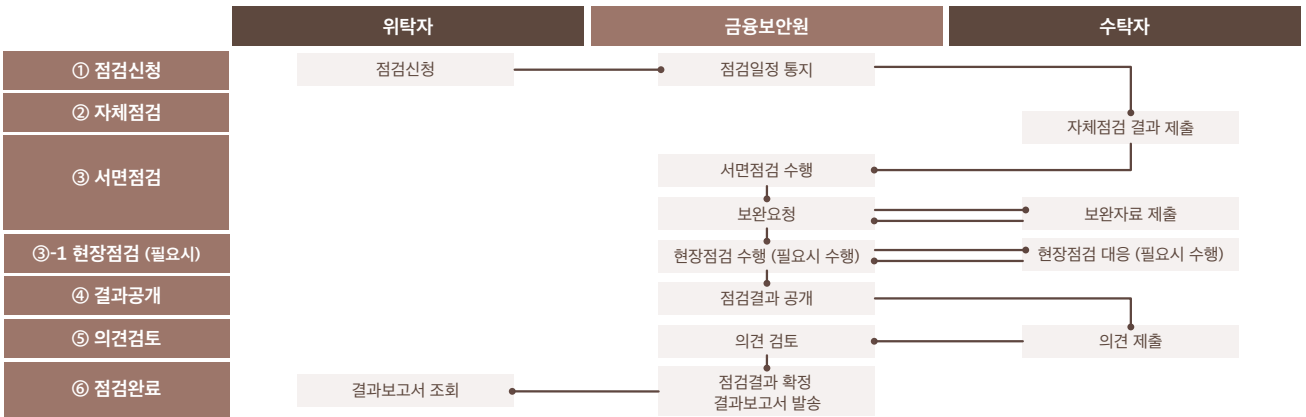
사업실적

• 개인(신용)정보 수탁자 공동점검 실시 현황



- 개인(신용)정보 처리 업무 위·수탁자 대상 설명회 개최(4회)
- 금융분야 개인(신용)정보 수탁자 점검 안내서 개정(2회)
- 수탁자 자동화점검도구 개발(2024.11.)

개인(신용)정보 수탁자 공동점검 수행 절차(25년 변경안)



금융보안 교육센터

금융보안 분야의 종합적인 전문교육 제공

금융IT·보안 환경변화와 교육 수요를 반영한 교육과정을 개발하고, 금융회사 임직원부터 리더까지 계층별·수준별 맞춤형 교육을 온·오프라인으로 상시 운영하고 있습니다. 또한 고용노동부로부터 국가인적자원개발컨소시엄 공동훈련센터 및 사업주 직업능력개발 훈련시설로 지정받아 금융보안 전문인력 양성 및 금융권 보안 수준 제고를 위한 특화된 금융보안 교육 서비스를 제공하고 있습니다.

금융권 자율보안 체계 구축을 지원하기 위해 금융회사 임·직원 대상, 금융회사 임원 및 금융IT CISO 등 리더 대상 교육 과정을 개설·운영 하였으며, 금융보안 자격제도 운영·시행을 통해 금융보안관리사를 포함한 금융보안 전문인력을 양성하였습니다. 또한 금융보안 아카데미를 개설하여 미래 금융보안 인재를 양성하였습니다.

- 금융회사 임·직원 대상 금융보안 교육 시행
- 금융보안 리더 대상 특화교육 시행
- 금융보안 자격제도 운영
- 금융보안 아카데미 운영

01

금융회사 임·직원 대상 금융보안 교육 시행

국가인적자원개발컨소시엄 사업

고용노동부가 기업에 필요한 전문인력 양성을 위해 다수의 관련 기업과 공동훈련 협약을 맺고 공동훈련에 필요한 훈련 인프라와 훈련비 등을 지원하는 직업능력 개발 훈련 사업

사업주 직업능력개발훈련 사업

고용노동부가 근로자의 직무수행 능력 향상을 장려하기 위해 훈련 시설로 지정된 교육기관에서 실시하는 과정을 수료한 근로자의 회사(사업주)에 교육비 일부를 지원하는 고용보험 환급 과정

금융보안교육센터 홈페이지

온라인 수강, 진도관리, 수료증 발급 등 교육과정을 종합적으로 제공하는 홈페이지(edu.fsec.or.kr)

“금융권 자율보안 체계 구축을 지원하기 위한 맞춤형 금융보안 전문인력 양성”

대외환경

- 금융보안 규제를 원칙 중심으로 개선하는 전자금융감독규정 개정안 및 단계별 금융보안 선진화 방안이 발표되는 등 정부 정책의 변화에 대비하고, 인공지능(AI)·클라우드 등 디지털신기술 발전에 따른 보안리스크를 반영한 금융보안 교육의 중요성 증가

주요성과

- 클라우드, 인공지능, 데이터 확보·결합·활용 관련 기술 등 디지털금융 혁신 기술을 반영한 신규 교육과정 개발·운영
- 국가인적자원개발컨소시엄(산업맞춤형)사업 및 사업주 직업능력개발 훈련사업을 통해 금융보안 전문인력 양성을 위한 집합교육 제공
- 금융보안교육센터 홈페이지를 통해 시간·장소에 구애받지 않는 금융회사 임·직원 대상 사이버교육 및 비대면 교육(YouTube, Zoom 활용) 제공

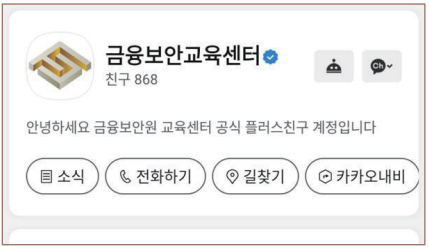
사업실적

	운영 과정수	운영 횟수	수료 인원
집합교육	컨소시엄 교육	24개	48회
	사업주 교육	3개	3회
	보안기술교육	8개	8회
	금융보안 검정시험 연계 교육	1개	2회
	금융보안 최고위 과정	1개	1회
	금융IT CISO 보안리더 과정	1개	3회
	금융보안 책임자 전략 수립 과정	1개	1회
	대외원사 방문교육	1개	27회
	금융보안 아카데미	2개	1회
사이버교육	47개	-	803,483명
합 계	89개	-	807,132명

금융보안교육센터 소통 채널



금융보안교육센터 홈페이지



카카오톡 플러스 친구
카톡 검색창에 “금융보안교육센터”



구글 캘린더
fseceducal@gmail.com

02 [참고] 2024년도 금융보안교육센터 교육과정

전문역량 강화교육		
이론	실습	
R 금융 정보보호 및 개인정보보호 관리 체계	N Azure 클라우드 기본 운영 및 보안 실습	✓ 정보보호시스템 운영보안 실무
R 디지털금융과 전자금융 거래법 규제 체계	쿠버네티스 환경에서의 클라우드 보안 실무	✓ 금융권 침해사고 분석 및 대응
금융권 개인정보보호 실무	금융권 데이터 분석 활용	✓ 금융 APT 공격과 대응
금융권 개인신용정보 보호	R AI를 이용한 금융보안 데이터 분석	R 윈도우 시스템 악성코드 분석 및 대응 기본
R 금융IT감사 실무	R 금융·보안 업무 자동화를 위한 파이썬 웹 크롤링 및 API활용	✓ 침해사고 대응 담당자를 위한 디지털 포렌식 기본
R 금융 클라우드 보안 실무	R 금융데이터 가명, 익명 처리 및 활용	N 윈도우 시스템 모의해킹으로 배우는 S/W 취약점 공격 기법
금융권 클라우드 컴퓨팅 서비스 제공자 안전성 평가	금융권 취약점 분석·평가의 이해	S 금융분야 개인정보보호 위·수탁 업무 기본
R 컴플라이언스 관점의 전자금융 보안 실무	금융시스템 개발 보안	S 금융 IT보안 입문
✎ 금융IT 인프라 보안의 이해	R 금융앱 보안 실무	
S 금융 정보보호 관련 법제도의 이해		
T 보안기술교육		

사이버교육			
기본소양		직무기본	직무강화
N ChatGPT가 불러온 AI 혁명의 명암	신입직원을 위한 금융보안 개론	N 제로 트러스트 보안 모델과 금융권 대응방안	N 자율보안체계 수립을 위한 금융권 위험관리방안
N 금융IT 법규 및 개인정보보호법 위반 사례	금융권 마이데이터의 이해	N 금융권 오픈소스 및 공급망 보안 이해	디지털 포렌식의 기본과 활용 사례
랜섬웨어 감염 예방을 위한 PC보안 기초	디지털 금융보안 이슈	N 금융 분야 합성 데이터 생성 및 활용 실습	가명·익명처리 취급자를 위한 정보보호
데이터 개방 시대의 금융 보안	금융보안 법·제도의 이해	실무자를 위한 금융권 정보보호 상시평가 업무이해	개인·신용 정보보호 실무
금융권 메타버스 활용 사례 및 보안 이슈	4차 산업혁명의 영향과 보안위협 및 대응	엘라스틱스택을 이용한 대용량데이터 분석 및 시각화	금융권 IT 보안 위반 사례
일상에서 지켜야 할 스마트폰 보안수칙	금융환경 변화에 따른 전자금융서비스 분석	금융보안 데이터 크롤링을 위한 파이썬 기본 문법	AI를 이용한 금융 데이터 분석 실습
정보보호 인식 제고	IT아웃소싱 업체 보안 A부터 Z까지	웹 애플리케이션 보안	다크웹과 OSINT (Open Source Intelligence)
금융IT 내부감사 활동의 이해	금융권 보안 위협 전망	금융권 APT 공격과 대응방안	금융권 클라우드 도입과 보안
금융보안 거버넌스의 이해	최근 금융분야 사이버 공격 유형 및 대응 방안	네트워크의 이해	정보보호관리체계 구축 및 활용
		블록체인 속의 금융환경 및 이슈	안전한 소프트웨어를 위한 시큐어코딩의 이해
		안전한 금융보안을 위한 암호기술	개인정보 책임자를 위한 금융권 개인정보보호
		전자금융 보안인증 기술의 이해	개인정보 수탁자를 위한 금융권 개인정보보호
		정보 보안 컴플라이언스 및 시스템관리 기초	개인정보 취급자를 위한 금융권 개인정보보호
		상담원을 위한 금융보안	
		금융회사 임직원이 준수 해야하는 금융IT 내부통제	
		내부정보 유출방지를 위한 자기수준진단 및 준수사항	

특화교육	
S 금융보안 최고위 과정	
금융IT CISO 보안리더 과정	
금융보안 책임자 전략수립 과정	
대외원사 방문교육	
사원기관 자체 교육용 콘텐츠	

✓ 해킹방어교육시스템 활용 교육이란?	전자금융 침해사고에 대한 실전 대응 역량을 강화하기 위해 실제 사고사례와 유사한 모의 환경을 제공하고 대응 기술을 훈련할 수 있는 시스템 활용 교육	컨소시엄 교육	✎ 신입 및 전임자 대상 교육
🛡️ 보안기술교육이란?	최신 보안 이슈 및 신기술을 반영한 교육으로 수시 운영하며, 과정 개설 시 개별 안내 및 홍보	사업주 교육	N 2024년 신규과정
		보안기술 교육	R 2024년 개편과정
		✓ 해킹방어교육시스템 활용 교육	S 유료 교육과정

03 금융보안 리더 대상 특화교육 시행

정보보호최고책임자

(CISO, Chief Information Security Officer)

기업에서 정보기술 부문의 안전성 확보, 이용자 보호를 위한 전략과 계획 수립, 보안사고 예방 및 조치 등의 정보보안 업무를 총괄하는 책임자

금융보안 최고위과정

디지털 금융IT·보안 분야 C-Level

경영진의 리더십 및 보안역량 강화를 위해 디지털 금융IT·보안 정책, 최신 기술 트렌드, 보안사고 사례 등의 강연으로 구성된 교육과정

“금융권 정보보호최고책임자의 전문 역량 강화 및 상호협력과 소통의 기회 제공”

대외환경

- 금융분야 내 인공지능(AI)·클라우드 등 차세대 기술 도입으로 디지털금융에 대한 사이버 위협 또한 고도화됨에 따라 지능화된 공격에 대비한 금융보안 기능을 보다 강화할 필요성 증대
- 가속화되는 최신 기술 트렌드 변화 속에서 금융보안 리스크 관리에 효과적으로 대응할 수 있도록 정보보호최고책임자(CISO) 역할의 중요성 증대

주요성과

- 성공적인 자율보안 체계 구축 및 차세대 기술 도입 등 금융보안의 균형있는 성장을 선도할 수 있도록 금융보안 리더에게 필요한 금융정책 및 신기술 관련 전문교육을 제공하고 교류와 협력의 장을 제공
- 사이버 위협 동향, 금융보안 정책 방향, 금융권 AI의 경영활용 전략, 사이버 위협과 침해사고 대응, 최신 DX 적용 등 다양한 주제의 전문강연을 통해 금융회사 C-Level(CIO, CISO 등) 리더들이 의사결정에 활용할 수 있는 정보 및 인사이트 제공
- 금융·IT·정보보호 분야 리더 대상의 장기 과정인 ‘금융보안 최고위 과정’ 운영
- CISO 전문성 강화를 위한 1일 과정인 ‘금융IT CISO 보안리더 과정’ 운영

사업실적

	금융보안 최고위과정*	금융IT CISO 보안리더 교육
과정 특징	장기과정, 유료	단기과정, 무료
참가 대상	금융권 C-Level, 경영진, 정보보호 업계 CEO, 관련 법조인 등	금융권 CISO
교육 기간	총 10주, 30시간	1일, 6시간
운영 횟수	연 1회	연 3회
수료생	30명	130명

* 2017년 개설 이후 2024년까지 총 209명의 수료생을 배출

금융보안 최고위과정



금융IT CISO 보안리더 과정



04

금융보안 자격제도 운영

금융보안관리사(CFSE, Certified Financial Security Expert)
금융회사 정보보호 업무에 필요한 관련 법령·금융서비스에 대한 실무 지식을 갖추고 금융IT·보안 위협의 진단과 위험관리를 수행할 수 있는 전문가 양성을 위한 과정형 민간자격
(등록번호 : 한국직업능력개발원 제 2018-000478호)

“금융권 정보보호 담당자들을 대상으로 금융보안에 특화된 금융보안관리사 자격제도 운영”

대외환경

- 급변하는 디지털 신기술 및 금융보안 법·정책의 환경 변화에 따른 위기에 능동적으로 대응하고 금융시스템의 사이버 복원력을 강화할 수 있는 금융보안 전문인력의 양성과 전문가 검증의 필요성 증대

주요성과

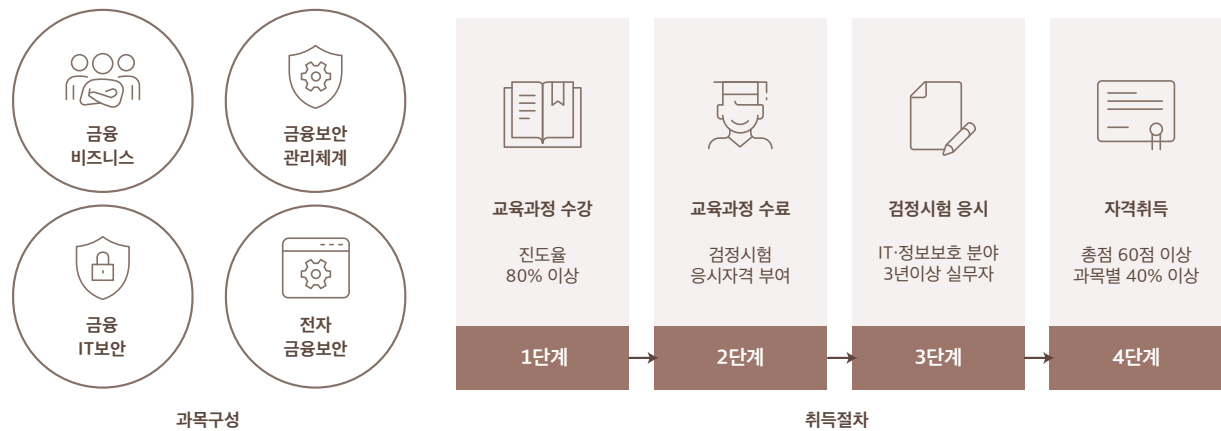
- 금융보안·IT 실무경력이 3년 이상인 정보보호 담당자를 대상으로 금융보안관리사 자격제도를 운영
※ 금융비즈니스, 금융보안관리체계, 금융IT보안, 전자금융보안 등 4개 과목의 전문교육 과정 이수 및 검정시험 통과 필요
- 비대면 교육방식으로 전문교육 인원을 2배 확대하여 연2회 운영하고, 검정시험을 실시하여 금융보안 전문가를 배출
- 금융보안관리사 표준교재 4종 및 강의콘텐츠 전면 개편

2018년 자격제도 시행 후
총 346명의 금융보안관리사 배출

사업실적



금융보안관리사 개요



05

금융보안 아카데미 운영

금융보안아카데미(FSEC-Academy, Financial SEcurity Academy)
금융보안 분야에 필요한 미래 인재를 조기에 발굴하고 양성하기 위해 금융보안 전문가가 갖추어야 할 기본 소양과 전문지식을 교육하는 금융보안원의 전문교육 프로그램

“대학생 및 대학원생을 대상으로 금융IT·정보보호 분야의 이론·실습 교육과 전문가의 멘토링 제공”

대외환경

- 디지털 환경 변화의 가속화에 따라 사이버보안 역량을 갖춘 인력에 대한 수요가 증가하고 있으며, 이에 따른 선제적인 인력 양성 및 확보 필요성 증대
- 사이버보안 인재 10만 양성 방안 및 ‘금융보안규제 선진화 방안’ 등 정부 정책에서 금융IT·정보보호 분야의 전문인력 확보 필요성 제기

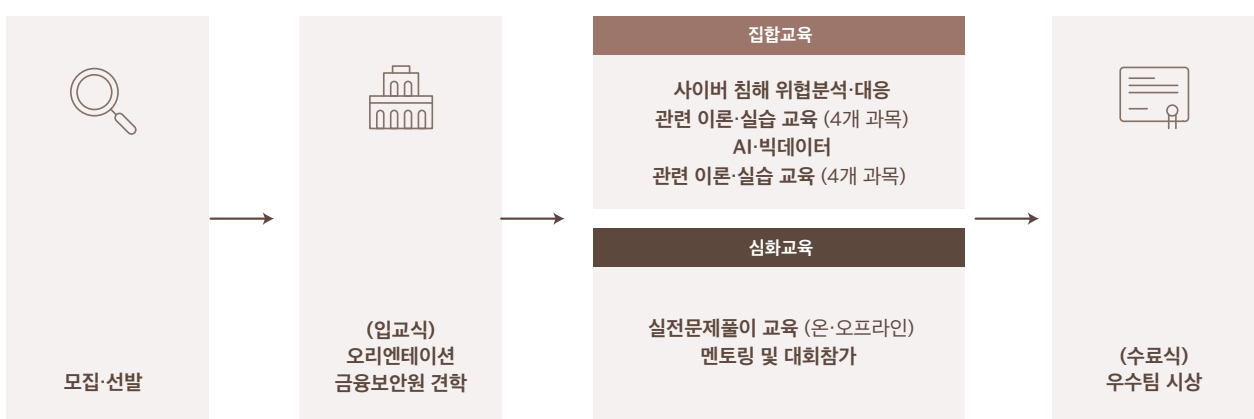
주요성과

- 정보보호 및 데이터 분야에 관심과 재능이 있는 대학(원)생을 대상으로 금융보안아카데미 교육과정 2개 트랙을 운영
※ 서류, 면접 등을 통해 총 40명 교육생 선발
- 리버스 엔지니어링, 악성코드 분석·대응, 웹·시스템 해킹, 디지털 포렌식 등 사이버 침해 위협분석 및 대응 분야에 관한 이론 및 실습교육 실시
- 데이터처리·시각화 기법, 데이터 분석 기법, 딥러닝·자연어 처리 기법, 데이터 가명처리 및 AI 보안 기법 등 AI·빅데이터 분야에 관한 이론 및 실습교육 실시

사업실적

- 교육기간 : 7월 ~ 8월
- 제1기 수료인원 : 14개교, 총 19명
- 제2기 수료인원 : 22개교, 총 40명

금융보안아카데미 개요



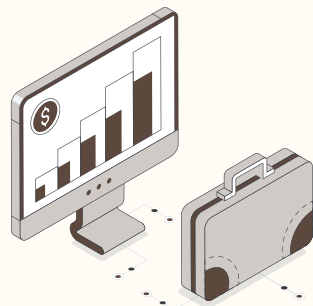
2025 디지털금융 및 사이버보안 이슈 전망

01 금융보안 가치의 재정립, 10년의 뒤풀리를 넘어서자



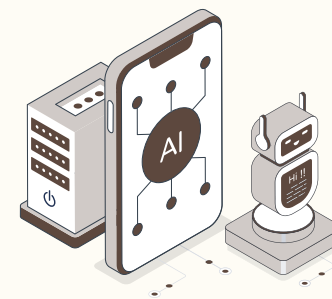
지난 10년간 금융보안의 근간이 된 망분리 규제가 역설적으로 금융보안 발전의 걸림돌로 작용한 바, 망분리 규제 개선을 시작으로 글로벌 금융회사 수준의 보안 역량을 조속히 확보하기 위한 각계의 지속적 관심과 노력이 필요

02 금융보안 DIY 키트, 자율보안 프레임워크 정착



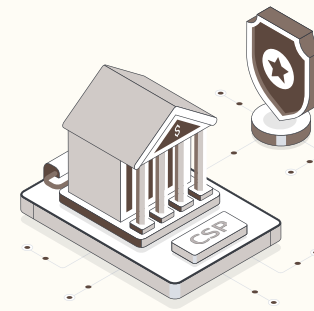
금융IT 환경의 급격한 변화와 사이버위협 고도화 등으로 정부는 자율보안으로의 전환을 추진 중이며, 금융회사는 자사 환경에 맞는 자율보안 체계를 마련·운영할 필요

03 혁신과 버블의 갈림길에 선 AI, 실효성 및 안전성 검증 본격화



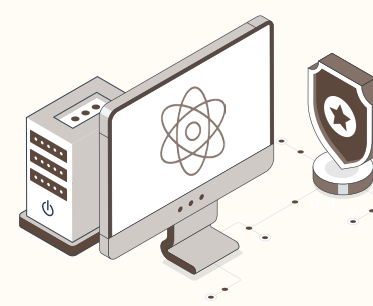
AI 기술의 발전 및 망분리 규제 개선 등으로 금융권에 AI 활용이 본격화됨에 따라 AI의 실효성 및 안전성 검증이 필요할 것으로 보이며, 안전하고 신뢰할 수 있는 AI 개발을 위해 정부, 전문기관 등의 지원과 금융회사 간 정보 공유 필요

04 제3자에서 전략적 동반자로, 금융권과 CSP간 안전한 협력 관계 모색



정부의 클라우드 이용 활성화 정책 등으로 금융분야에 클라우드 활용이 더욱 확대될 것으로 보임에 따라, CSP를 일반적인 제3자가 아닌 금융 IT보안의 '전략적 동반자'로 인식하고 안전한 협력 관계를 모색할 필요

05 암호 인프라의 지각변동, 양자컴퓨팅에 선제적 대비



양자컴퓨팅 기술의 급속한 발전으로 RSA 등 고전 암호의 무력화가 현실로 다가오고 있기에, 국내 금융권도 양자내성암호 적용 등 관련 전략을 선제적으로 고민해야 할 시기

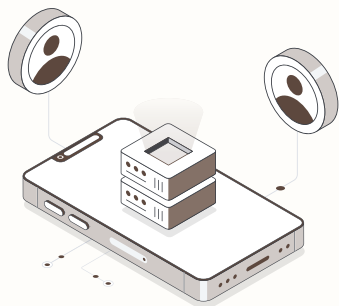
2025 디지털금융 및 사이버보안 이슈 전망

06 QR코드를 스캔했을 뿐인데...큐싱 경보 발령



다양한 분야에서 QR코드를 악용한 큐싱 사기가 지속 발생하고 있는 바, 금융권에서도 금융소비자가 큐싱 사기 피해를 입지 않도록 경각심을 제고하는 등 피해 예방 대책을 선제적으로 마련할 필요

07 당신 누구야? 신뢰할 수 없는 디지털 페르소나 경계



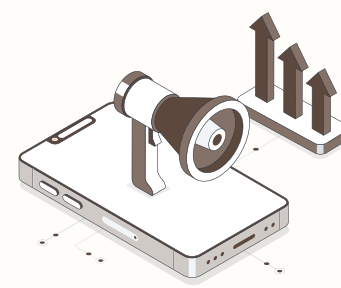
최근 AI 등 신기술을 접목한 디지털 페르소나 악용 사기가 증가하고 있으며 국내 금융권도 그 영향권에 있는 만큼, 정부 및 금융회사는 선제적 대응 체계를 마련해야 하며 금융소비자도 경각심을 가질 필요

08 내 지문이 왜 거기에? 생체정보 탈취 현실화



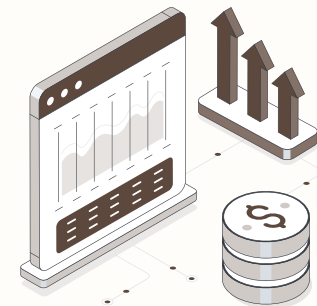
생체인증 기반 오프라인 결제서비스 등 금융 분야에 생체정보 활용이 지속 확대될 것으로 보이며, 딥페이크 기술을 악용한 생체인증 우회 시도나 생체정보를 노리는 해킹 공격도 고도화되고 있으므로 금융권의 철저한 대비가 필요

09 내 모든 게 스마트폰에? 모바일 집중에 따른 위험



금융서비스 외에도 신분증, 전자증명서 등 다양한 서비스가 모바일로 제공되면서 모바일 집중 현상이 심화되고 있으며, 이에 비례하여 모바일 보안 위험도 고도화되고 있으므로 금융회사와 금융소비자는 강화된 모바일 보안 관리 필요

10 언제까지 차트만 볼래? Web 3.0과 연계한 가상자산의 미래 주목



전 세계적으로 Web 3.0 생태계 구축 시도가 활발하나 국내 가상자산 시장은 코인 투자에만 집중된 경향이 있으므로, 금융회사 등은 향후 발전 가능성 등을 고려하여 Web 3.0 전략을 선제적으로 고민할 필요

PART. 2

금융보안원 현황

일반 현황(설립목적, 비전, 원 소개)

주요 연혁

조직 현황

의사결정 구조

사원기관

사무실 현황

홈페이지 현황

금융보안원 소개

금융보안원(FSI, Financial Security Institute)은 안전하고 신뢰할 수 있는 금융환경을 조성하여 금융이용자의 편의 증진과 금융산업의 발전에 기여할 목적으로 설립된 금융보안 전문기관입니다. 우리 원은 금융보안관제, 사이버 위협정보 및 이상금융거래정보 공유, 금융권 사이버 침해 예방·대응, 취약점 분석·평가, 디지털금융 서비스 및 핀테크 신기술 보안 지원, 금융권 자율보안 지원, 금융보안 정책·기술 연구 및 정책 수립 지원, 정보보호 관리체계 인증, 금융권 데이터 활용 지원 및 정보보호, 금융보안교육 등 종합적이고 전문적인 금융보안 서비스를 제공하고 있습니다.



금융미래를 열어가는 금융보안파트너



주요 연혁

2014-2016

2014. 02. 20. 「금융보안전담기구」 설립 기본방향 보고(금융위원회 업무계획 대통령 보고)
03. 10. 「금융보안전담기구」 설립 발표(관계부처 합동 '금융부문 개인정보유출 재발방지대책' 발표)
10. 31. 「금융보안전담기구」 설립 기본계획 확정
2015. 03. 18. 침해사고 대응기관 지정(금융위원회)
03. 31. 사단법인 금융보안원 설립 허가(금융위원회)
04. 03. 금융정보공유·분석센터(금융ISAC) 구축 통지(금융위원회)
04. 10. 사단법인 금융보안원 출범 (초대원장 김영린)
07. 10. 정보보호관리체계(ISMS) 인증기관 지정 (과학기술정보통신부)
12. 24. 제2대 허창언 원장 취임
2016. 04. 27. 금융보안자문위원회 발족
05. 31. 금융권 사이버 범죄 및 침해사고 대응 역량 강화를 위한 MOU 체결(대검찰청)
08. 31. 개인정보 비식별 조치 지원 전문기관 지정(금융위원회)
11. 14. 금융권 디지털 포렌식 랩 구축

2021

01. 07. 금융 모바일 악성코드의 현재와 미래 금융보안 인텔리전스 보고서 발간
01. 25. 데이터전문기관 최초 데이터전문기관 포털 오픈
02. 01. 범금융권 보이스피싱 사기 정보 공유 시스템 본격 가동
02. 04. 정보보호 상시평가제 자율규제기구 업무 개시
03. 15. 금융데이터거래소 데이터 결합지원 서비스 오픈
03. 22. 클라우드 기반 원격 데이터분석센터 오픈
04. 01. 금융분야 마이데이터 테스트베드 오픈
04. 12. 중소 핀테크 기업 보안점검 실시
05. 10. 데이터 유통·활용 촉진을 위한 MOU 체결(한국데이터산업진흥원, 비씨카드)
05. 11. 금융 데이터 엑스포 개최
05. 25. 금융 데이터 경진대회 개최
06. 30. 비식별 프로세스 프레임워크 정보통신 단체표준(TTA표준)으로 제정
12. 06. 제4대 김철웅 원장 취임
12. 27. 신용카드 정보를 노리는 사이버 공격 위협 분석 인텔리전스 보고서 발간

2017-2018

2017. 02. 07. 글로벌 금융 사이버위협 정보공유를 위한 MOU 체결 (글로벌 정보보호 전문업체 8개社)
08. 03. 금융 해킹방어 훈련장 구축
09. 14. 금융 블록체인 테스트베드 운영
09. 20. 금융보안표준화협의회 출범
2018. 04. 09. 제3대 김영기 원장 취임
10. 01. 사이버 위협정보 공유 자동화 시스템 시범 서비스 오픈
10. 29. 금융보안 레그테크(Regtech) 시스템 구축
12. 07. 금융권 자율보안을 위한 표준 제정(7건)
12. 26. AI기반 금융보안관계 분석 모델 개발

2022

01. 27. 보이스피싱 악성 앱 유포조직 프로파일링 인텔리전스 보고서 발간
04. 04. 제6회 금융보안원 논문공모전 개최
04. 27. 보이스피싱 방지를 위한 MOU 체결(라온시큐어)
04. 19. 대한민국 합동훈련팀 금융권 대표로 락드실즈 2022 참가
05. 26. FSI Data Challenge 2022 개최
06. 28. 핀테크 혁신기술 기업 육성을 위한 MOU 체결(한국핀테크산업협회, 우리FS, DSN홀딩스)
07. 01. 금융권 정보보호 및 개인정보보호 관리체계(ISMS-P) 통합 인증기관 재지정
07. 11. 데이터 소외자 대상 데이터 지원을 위한 MOU 체결(신한카드)
08. 03. 2022년 금융권 버그바운티 실시
09. 05. 취약점 종합관리 솔루션(FLUS) 관련 특허 취득
09. 07. 보이스피싱 예방·대응을 위한 MOU 체결(에버스핀, 인피니그루, YH데이터베이스)
09. 13. 금융권 사이버침해 위협분석 대회 FIESTA 2022 개최
09. 15. 데이터전문기관 최초 원스톱(One-stop) 샘플링 결합 서비스 오픈
09. 27. 전기통신금융사기 방지를 위한 MOU 체결(경찰청, KT)
09. 29. 금융회사 해외진출 지원을 위한 글로벌 보안 취약점 점검 시범 실시
09. 30. 보이스피싱 예방·대응 협력을 위한 MOU 체결(SK윌더스)
10. 25. 금융분야 마이데이터 통합인증 중계시스템 오픈
11. 14. 한미일 금융보안 협력 강화를 위한 MOU 체결(미국 FS-ISAC, 일본 F-ISAC)
11. 15. 금융정보보호 컨퍼런스 FISCON 2022 개최
12. 08. 금융분야 디지털 혁신 지원을 위한 오픈소스 소프트웨어 활용관리 안내서 마련
12. 14. Masscan 랜섬웨어 위협 분석 인텔리전스 보고서 발간

2019

01. 02. 금융보안 레그테크(RegTech) 서비스 본격 시행
06. 01. 금융권 최초 버그바운티(Bug Bounty) 실시
07. 01. 금융권 정보보호 및 개인정보보호 관리체계(ISMS-P) 통합 인증기관 지정
09. 26. 금융보안 표준화 추진체계 개편
11. 12. 금융부문과 지자체부문의 정보공유분석센터 간 사이버 보안 강화를 위한 MOU 체결(한국지역정보개발원)
12. 12. 악성코드 중심의 침해대응 매트릭스 모델링 인텔리전스 보고서 발간
12. 17. 안전하고 신뢰할 수 있는 분산ID 생태계 조성을 위한 MOU 체결(한국인터넷진흥원)

2023

01. 01. 차세대 금융보안관계 서비스 개시
02. 22. 국가안보실 제2차장 주재 사이버 금융테러 대응테세 점검회의 개최
03. 22. 「금융권 생체정보 인증·관리 안내서」 발간
03. 23. 우즈베키스탄 중앙은행(CBU)과 MOC 체결
04. 03. 제7회 금융보안원 논문공모전 개최
04. 12. 2023년도 금융보안자문위원회 전체회의 개최
04. 17. NATO 주관 락드실즈(Locked Shields) 2023 훈련 참가
06. 12. 금융 데이터 분석활용 경진대회 「FSI Data Challenge 2023」 개최
07. 01. 2023년 버그바운티(Bug Bounty) 실시
07. 11. 2023 금융보안 아카데미 교육과정 개설
07. 19. 금융회사 최고경영자 초청 정보보호 세미나 개최
08. 21. 금융권 사이버 침해위협 분석대회 「FIESTA 2023」 개최
09. 14. 데이터 비식별화보증요건(ITU-T) 국제표준 채택
10. 05. 이상금융거래탐지시스템(FDS) 운영 가이드라인 마련
10. 12. Gran Data 사업 협력을 위한 MOU 체결(그랜데이터)
11. 02. 「2024년 디지털금융 및 사이버보안 이슈 전망」 발표
11. 06. 최정예 화이트해커팀 'RED IRIS' 출범
11. 09. 금융정보보호 컨퍼런스 FISCON 2023 개최

2020

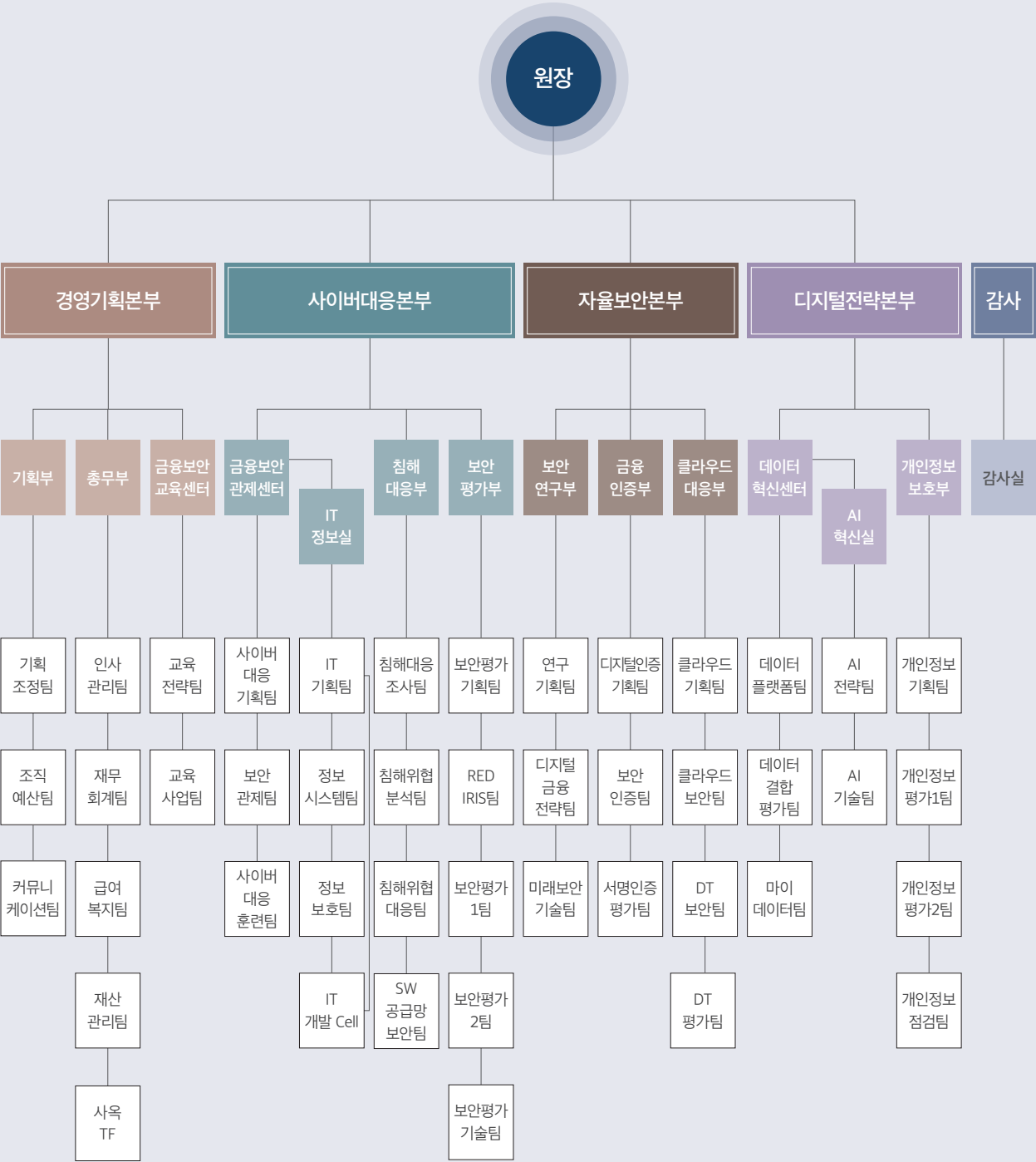
01. 22. 핀테크와 금융보안 현장 간담회 개최
02. 26. 클라우드 연계 대용량 디도스(DDoS) 공격 대응 체계 강화
04. 27. 금융권 보이스피싱 예방 및 피해 확산 방지를 위한 MOU 체결(SK텔레콤)
05. 11. 데이터 경제 활성화를 위한 금융데이터거래소(FinDX) 출범
06. 10. 금융권 인공지능(AI) 정책 공동연구를 위한 MOU 체결(법무법인(유한) 태평양)
06. 18. 금융권 보이스피싱 예방 및 대응을 위한 MOU 체결(후후앤컴퍼니)
06. 25. 데이터 유통 및 활용 혁신을 위한 MOU 체결(LG유플러스·LG CNS)
07. 07. 금융산업 IT·보안·법제도 연구 협력을 위한 MOU 체결(은행법학회)
07. 21. 데이터 유통 및 활용 혁신을 위한 MOU 체결(KDX 한국데이터거래소)
07. 23. 보이스피싱 예방 및 대응을 위한 MOU 체결(안랩)
08. 06. 금융분야 데이터전문기관 지정(금융위원회)
08. 19. 금융·소비유통 데이터 생태계 조성을 위한 MOU 체결(BGF리테일)
09. 03. 데이터 생명주기에 따른 비식별 처리 프레임워크, 세계 최초의 ITU-T 국제표준 채택
09. 07. 금융보안 연구협력 및 전문인력 양성을 위한 MOU 체결(세종대학교)
12. 10. 분산ID 신원관리 프레임워크, 정보통신 단체표준(TTA표준) 채택
12. 22. 전자서명법상 전자서명인증 평가기관 지정(과학기술정보통신부)

2024

02. 07. CVE(소프트웨어에 존재하는 보안 취약점의 국제 식별번호) 발급기관 지정
02. 14. 데이터 2.0 서비스 제공
03. 06. 「레드아이리스 인사이트 리포트 : Campaign ThirdEye」 발간
03. 11. 24년도 금융권 침해사고 대응훈련 개시 및 사이버대피소 전환훈련 신설
04. 01. 「제 8회 금융보안원 논문공모전」 개최
04. 08. 「2024년 금융보안자문위원회 전체회의」 개최
04. 22. 사이버위협 인텔리전스 보고서 (오퍼레이션 마이더스, 오퍼레이션 포이즌애플) 공개
04. 22. NATO 주관 락드실즈(Locked Shields) 2024 훈련 참가
05. 02. 제 8기 금융보안 최고위 과정 개최
05. 14. 금융분야 사이버 침해사고 예방을 위한 금융보안원-KISA MOU 체결
05. 28. 2024년 버그바운티(Bug Bounty) 실시
06. 27. 「FSI AIXData Challenge 2024」 개최
07. 16. 「금융보안아카데미2024」 개최
07. 25. 금융보안 AI 워킹그룹 출범
07. 31. 「한국 금융보안의 현 주소와 나아갈 방향」 현안 세미나 개최
09. 23. 금융권 사이버 침해위협 분석대회 「FIESTA 2024」 개최
10. 16. 금융 클라우드 보안 관리 설명회 개최
11. 07. 금융정보보호 컨퍼런스 FISCON 2024 개최
11. 14. SW 공급망보안 자율점검 체크리스트 개발
11. 16. 2025년 주목해야 할 디지털 금융 및 사이버 보안 10대 이슈 선정

조직현황

• 금융보안원 조직도 ('25.5월 기준)



의사결정 구조

• 대의원사 현황 ('25.5월 기준)

구분	대의원사
① 은행	12개사
② 금융투자	9개사
③ 보험	7개사
④ 금융유관기관	2개사
⑤ 중소서민	7개사

- ① 아이엠뱅크, 수협은행, 신한은행, 우리은행, 중소기업은행, 하나은행, 한국산업은행, 한국씨티은행, BNK부산은행, KB국민은행, NH농협은행, SC제일은행
- ② 메리츠증권, 미래에셋증권, 삼성증권, 신한투자증권, 키움증권, 하나증권, 한국투자증권, KB증권, NH투자증권
- ③ 교보생명보험, 삼성생명보험, 삼성화재해상보험, 한화생명보험, 현대해상화재보험, DB손해보험, KB손해보험
- ④ 금융결제원, 코스콤
- ⑤ 삼성카드, 새마을금고중앙회, 신용협동조합중앙회, 신한카드, 저축은행중앙회, 현대캐피탈, KB국민카드
- ※ 기관명은 가나다순 정렬

• 의사결정체계

총회/대의원회	이사회
총회: 사원기관 전체 대의원회: 대의원사 37개社	이사회: 원장과 비상임이사 7인 (은행3, 금융투자2, 보험1, 중소서민1)
총회 1 정관의 변경 2 사원의 제명 3 금보원의 해산 또는 합병 4 사원의 의결권 제한	1 업무운영관리에 관한 기본방침 2 업무수행에 필요한 규정의 제정 및 개폐 3 정관 또는 총회에서 위임한 사항 4 기타 의장이 필요하다고 인정하는 사항
대의원회 1 원장, 이사, 감사의 선임 및 해임 2 사업계획 및 예산·결산의 승인 3 회비분담기준의 제·개정 4 기본재산의 사용 및 처분 5 기타 의장 또는 이사회가 필요하다고 인정하는 사항	
금융보안위원회	금융보안원과 비상임이사기관(7개社) 부서장
상설협의회	금융보안원과 대의원사(37개社) 담당자

사원기관

(’25.2月 기준)

전체	업 권 구 분						
	은행	금융투자	보험	금융유관기관	중소서민	전자금융업자	기타
200	19	36	42	6	36	16	45

은행	경남은행, 광주은행, 대구은행, 수협은행, 신한은행, 우리은행, 전북은행, 제주은행, 중소기업은행, 카카오뱅크, 케이뱅크, 토스뱅크, 하나은행, 한국산업은행, 한국씨티은행, BNK부산은행, KB국민은행, NH농협은행, SC제일은행
금융투자	교보증권, 다올투자증권, 대신증권, 리딩투자증권, 메리츠증권, 미래에셋증권, 부국증권, 삼성선물, 삼성증권, 상상인증권, 신영증권, 신한투자증권, 에스아이증권, 우리종합금융, 유안타증권, 유진투자선물, 유진투자증권, 유화증권, 이베스트투자증권, 카카오페이증권, 케이프투자증권, 키움증권, 토스증권, 하나증권, 하이투자증권, 한국투자증권, 한국포스증권, 한양증권, 한화투자증권, 현대차증권, BNK투자증권, DB금융투자, IBK투자증권, KB증권, NH선물, NH투자증권, SK증권
보험	교보라이프플래닛생명보험, 교보생명보험, 동양생명보험, 라이나생명보험, 롯데손해보험, 메리츠화재해상보험, 메트라이프생명보험, 미래에셋생명보험, 보험개발원, 삼성생명보험, 삼성화재해상보험, 서울보증보험, 신한라이프생명보험, 신한이지손해보험, 약사손해보험, 에이비엘생명보험, 에이스아메리칸화재해상보험, 처브라이프생명보험, 카카오페이손해보험, 캐롯손해보험, 코리안리재보험, 푸본현대생명보험, 하나생명보험, 하나손해보험, 한화생명보험, 한화손해보험, 현대해상 화재보험, 흥국생명보험, 흥국화재해상보험, AIA생명보험, AIG손해보험, BNP파리바카디프생명보험, DB생명보험, DB손해보험, DGB생명보험, IBK연금보험, KB라이프생명보험, KB손해보험, KDB생명보험, MG손해보험, NH농협생명보험, NH농협손해보험
금융유관기관	금융결제원, 코스콤, 한국거래소, 한국신용정보원, 한국예탁결제원, 한국증권금융
중소서민	나이스디앤비, 농업협동조합 중앙회, 롯데카드, 롯데캐피탈, 미래에셋캐피탈, 비씨카드, 산림조합중앙회, 산은캐피탈, 삼성카드, 새마을금고중앙회, 신용보증기금, 신용협동조합중앙회, 신한카드, 애뮤온캐피탈, 엠캐피탈, 우리금융캐피탈, 우리카드, 이크레더블, 저축은행중앙회, 코리아크레딧뷰로, 하나카드, 하나캐피탈, 한국투자캐피탈, 한국평가데이터, 한국평가정보, 현대카드, 현대캐피탈, 현대커머셜, A캐피탈, BNK캐피탈, IBK캐피탈, JB우리캐피탈, KB국민카드, KB캐피탈, NH농협캐피탈, NICE평가정보, SCI평가정보
전자금융업자	나이스정보통신, 나이스페이먼츠, 네이버파이낸셜, 다날, 블루월렛, 뱅크샐러드, 비바리퍼블리카, 에스엠하이플러스, 에스케이플래닛, 카카오, 카카오페이, 쿠팡페이, 토스페이먼츠, 티머니, 한국정보통신, 11번가
기타	금융투자협회, 기술보증기금, 대신저축은행, 메리츠금융지주, 미쓰이스미토모은행 서울지점, 미즈호은행 서울지점, 생명보험협회, 서민금융진흥원, 손해보험협회, 신용회복위원회, 신한금융지주, 신한저축은행, 애뮤온저축은행, 여신금융협회, 우리금융지주, 웰컴저축은행, 전국은행연합회, 중국공상은행 서울지점, 중국은행서울지점, 페퍼저축은행, 푸른저축은행, 핀다, 하나금융지주, 하나저축은행, 한국신용데이터, 한국자산관리공사, 한국주택금융공사, 한국투자금융지주, 한국투자저축은행, 해빗팩토리, 헥토이노베이션, BNK금융지주, BNK저축은행, DB저축은행, DGB금융지주, HSBC은행 서울지점, JB금융지주, JT저축은행, JT친애저축은행, KB금융지주, KB저축은행, NH농협금융지주, NH저축은행, OSB저축은행, SBI저축은행

※ 기관명은 가나다순 정렬

사무실 현황

· 죽전(본원)

📍 경기도 용인시 수지구 대지로 132(죽전동)

☎ 02-3495-9000



버스

- 새터공원 (200m)
- 정류장번호 29295

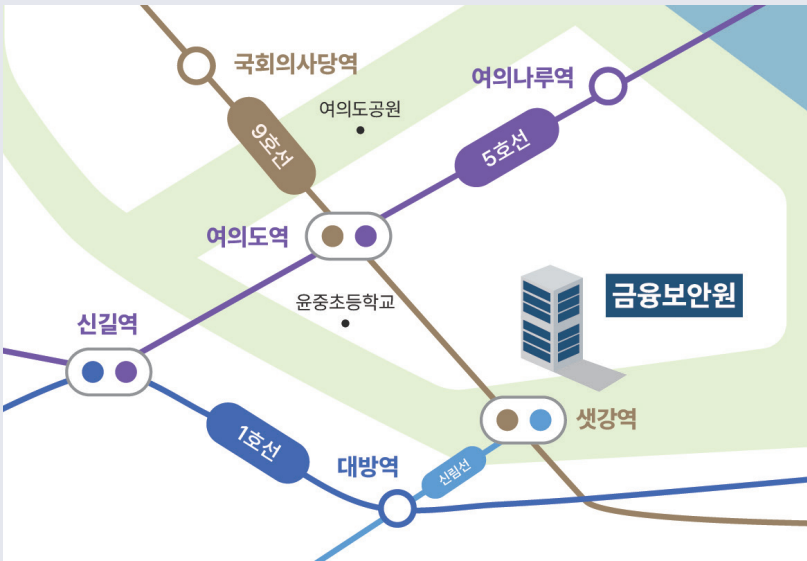
지하철

- 죽전역(수인분당선) 1번출구
- 마을버스 59번 승차 > 새터공원 정류장 하차

· 여의도

📍 서울특별시 영등포구 의사당대로 143 금투센터 4층, 7층, 8층
(개인정보보호부, 금융보안교육센터, 보안연구부, 데이터혁신센터)

☎ 02-3495-9000



버스

- 셋강역 1번출구, 여의도자이
- 정류장번호 19153

지하철

- 여의도역(5, 9호선) 5번출구
- KBS별관 방향 직진 > KB국민은행 신관 옆 위치
- 셋강역(9호선, 신림선) 1번출구
- 직진 > ABL 빌딩 옆 위치



정보보호 상시평가지원시스템

주요 서비스
금융회사 자체평가 등의 상시평가제를 지원

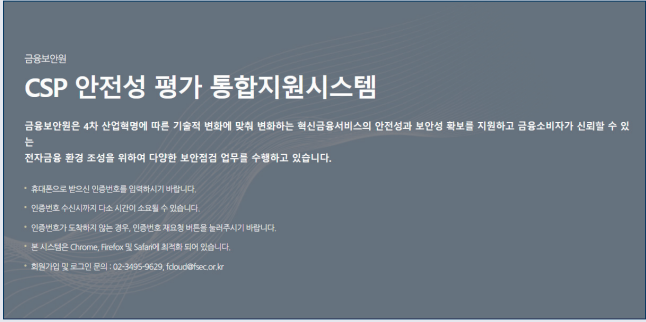
고객센터
assess.fsec.or.kr



전자금융보조업자 보안 통합지원시스템

주요 서비스
계약 관리, 자체점검 수행, 점검이력 관리 등 전자금융보조업자 보안 취약점 합동점검 관련 원스톱 지원

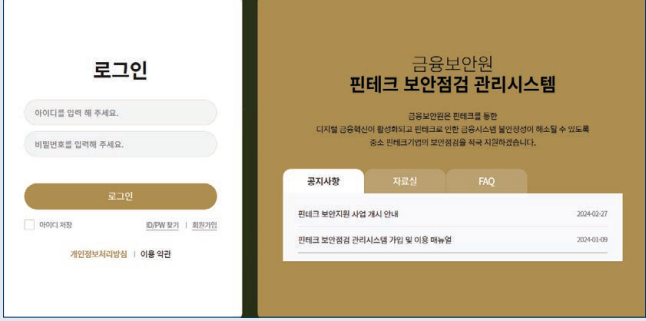
도메인
dt.fsec.or.kr



CSP 안전성 평가 지원시스템

주요 서비스
수요조사, 평가현황 관리, 결과서 관리 등 클라우드 서비스 제공자(CSP) 안전성 평가 관련 원스톱 지원

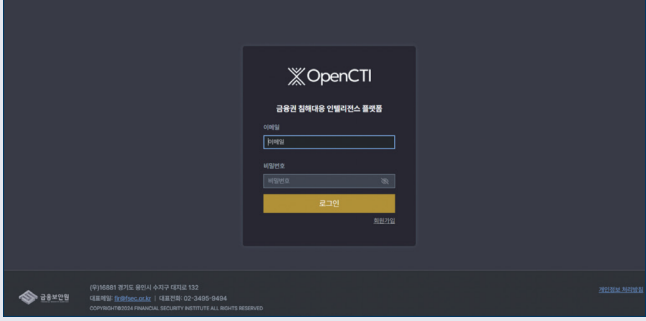
도메인
csp.fsec.or.kr



핀테크 보안점검 관리 시스템

주요 서비스
핀테크 기업 보안점검 신청, 점검 현황관리, 행정절차 자동화 등 핀테크 보안점검 관련 원스톱 지원

도메인
fintech.fsec.or.kr



금융권 침해대응 인텔리전스 플랫폼

주요 서비스
국내·외 사이버위협 및 침해사고 관련 침해지표 분석·공유 플랫폼

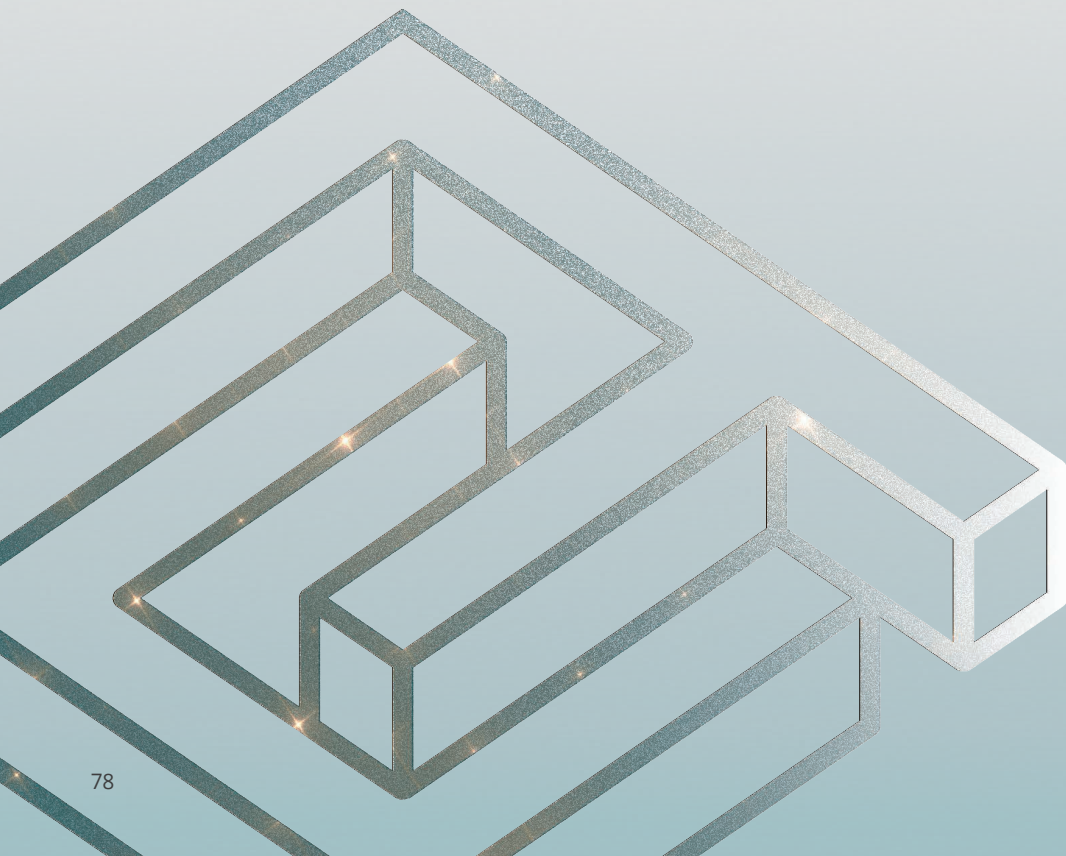
도메인
opencti.kfisac.or.kr

금융미래를 열어가는 금융보안파트너



PART. 3

주요 활동



금융보안원 소식

CEO 뉴스레터

금융보안원 소식



금융보안원 소식

01

2024년도
금융보안원 사무식 개최



01. 02.

신년사를 통해 임직원 모두가 금융보안
프렌들리 문화 형성에 동참해야 하며,
금융보안원이 사이버 위협 대응체계의
유지에서 나아가 AI 등 금융권 신기술의
선제적인 대비에 힘쓸 것을 당부하였습니다.

02

2024 대한민국 금융소비자대상
시상식 행사 참석 및 시상



01. 31.

2024 이데일리 대한민국 금융소비자대상
시상식에서 금융보안원장상을 수여하였습니다.
2024년도 금융보안원장상은 소비자보호
강화 및 내부체계 관리 전문화에 힘써준
현대해상화재보험이 수상하였습니다.

03

금융보안 선진화
현장 간담회 행사 개최



02. 01.

금융위원회 김소영 부위원장은
금융보안원에서 열린 '금융보안 선진화 추진
간담회'에서 전자금융감독규정 개정안
및 「금융보안 선진화」 단계별 추진방안을
발표하였습니다.

04

전자서명인증평가
업무 설명회 개최



02. 20.

전자서명인증평가 업무 설명회를 개최하여,
2024년도 전자서명인증평가 예정기관을
대상으로 평가 업무에 대해 설명하고 평가
상담을 진행하였습니다.

05

김철웅 원장, 2024한국정보보호산업협회
(KISIA) 사이버 주권수호상 수상



02. 22.

금융보안 관련 정책발굴과 침해대응 활동
등을 통해 국가 정보보호 수준 향상과 사이버
주권 수호에 기여한 공로를 인정받아 사이버
주권수호상을 수상하였습니다.

06

금융보안포럼
운영위원회 개최



02. 27.

금융보안포럼 운영위원회에서는 산·학·연
전문가들이 모여 금융권 자율보안체계의
안정적인 정착 방안에 대해 논의하였습니다.
앞으로도 금융보안원은 포럼을 통해 금융권
주요 어젠다에 대한 실질적인 논의와 토론의
장을 마련해나갈 것입니다.

금융보안원 소식

07

데이터 허브 및 금융데이터거래소 2.0 설명회 개최



02. 28.

데이터 시장 참여자를 대상으로 데이터 허브 및 금융데이터거래소 2.0 서비스에 대해 설명하였습니다. 이후 새롭게 오픈한 서비스에 참여하는 DATAi-allDATA그랜드데이터 등 국내 대표 데이터 얼라이언스의 소개와 함께 활용 사례에 대한 발표를 진행하였습니다.

08

국민경제자문회의의 우리 원 방문



03. 05.

국민경제자문회의의 의장단이 금융보안원을 방문하였습니다. 금융보안원 통합보안관제센터를 관람하고 업무에 대해 설명하여 금융권 사이버보안에 대해 논의하였습니다.

09

르완다 국가사이버보안청 등 방문



03. 06.

르완다 국가사이버보안청, 주한 르완다대사관, 공군, 중앙은행이 금융보안원을 방문 하였습니다. 금융보안원은 르완다 방문객들에 금융보안원 업무에 대해 소개하고 양국의 금융권 사이버대응체계에 대해 논의하였습니다.

13

2024년 금융 ISMS-P 인증 세미나 개최



03. 27.

ISMS-P에 대한 활발한 참여를 지원하기 위해 금융 ISMS-P 인증 세미나를 개최하였습니다. 최근 정보보호·개인정보보호 제도 및 정책 동향과 인증 취득 방법 등을 공유함으로써 ISMS-P 인증에 대한 이해도를 제고하고 인증심사원의 전문심사 역량을 강화하고자 하였습니다.

14

한국정보보호학회 회장단 방문



04. 02.

한국정보보호학회 회장단이 금융보안원을 방문하였습니다. 정보보호를 위한 양 기관이 진행중인 노력을 공유하고 대응능력 제고를 위한 방향에 대해 논의하였습니다.

15

2024년 금융보안자문위원회 전체회의 개최



04. 05.

금융보안 현안 사항에 대한 다양한 의견을 청취하고 바람직한 방향을 모색하기 위해 2024년 금융보안자문위원회 전체회의를 개최하였습니다. 본 회의에서 금융보안 규제 선진화, 금융권 S/W 공급망 보안, AI 활용 활성화 등에 대한 논의를 이끌어 줄 신규 위원 6명을 새롭게 위촉하였습니다.

10

금융권 취약점 분석·평가 정보공유 설명회 개최



03. 08.

「RED IRIS 인사이트 리포트 : Campaign ThirdEye」를 발간하며 3rd party 솔루션을 통한 공급망 공격 기법과 방어 대책을 심층 분석한 결과를 금융권 취약점 분석·평가 정보공유 설명회에서 발표하였습니다.

11

한국정보보호산업협회(KISIA) 회장단 방문



03. 18.

한국정보보호산업협회(KISIA) 회장단은 금융보안원에 방문하여 관제센터 견학 후 금융권 사이버보안 대응현황에 대한 정보 공유를 비롯한 상호 교류를 진행하였습니다.

12

금융보안원-국가정보자원관리원 업무협약 체결



03. 26.

국가정보자원관리원과 사이버보안 공조 및 디지털 신기술의 안전한 활용 등을 위한 MOU를 체결하였습니다. 금융보안과 정부전산행정 간 협력체계를 구축하여 국가 배후 해킹 세력 위협 등 글로벌 사이버 위협에 대한 대응능력을 제고할 수 있을 것으로 기대됩니다.

16

금융보안원 제3기 브라운보드 선출 및 출범식 개최



04. 09.

제3기 브라운보드 출범식을 개최하였습니다. 직원참여 플랫폼 출범식에서 브라운보드는 세대를 뛰어넘는 자유로운 소통을 통해 조직문화 개선에 기여하는 등 적극적으로 역할을 수행하겠다는 포부를 다졌습니다.

17

금융보안원 창립 9주년 기념식 개최



04. 12.

금융보안원은 창립 9주년 기념식을 개최하였습니다. 기념식을 통해 임직원들은 지난 9년간의 성과를 돌아보고 서로를 격려하며, 지속가능한 성장을 추구하는 선도적인 기관으로서의 역할에 대해 다시 한 번 고민해보는 시간을 가졌습니다.

18

2024 락드실즈 훈련



04. 23.

북대서양조약기구(NATO) 사이버방위센터(CDCOE)가 주관하는 세계 최대 규모의 실시간 사이버공격 방어훈련 '2024 락드실즈(Locked Shields) 훈련'에 3년 연속으로 참여하였습니다.

금융보안원 소식

19

NetSec-KR 2024
컨퍼런스 홍보부스 운영



04. 24.

한국인터넷진흥원이 주최하는 「NetSec-KR 2024」 컨퍼런스에 참가하여 참관객을 대상으로 디지털금융 및 사이버보안을 안내하고 금융보안원의 주요 업무를 소개했습니다.

20

사이버안보비서관 우리 원 방문



04. 29.

사이버안보비서관 등 국가안보실에서 우리 원에 방문하였습니다. 금융보안관제센터를 견학하고 금융보안 주요 현안에 대해 공유하며 양 기관의 사이버안보에 대한 강한 의지에 공감하는 시간을 가졌습니다.

21

제8기 금융보안 최고위과정 입교식



05. 02.

금융권 및 정보보호 산업계의 디지털·정보보호 담당 경영진(C-Level)을 대상으로 「제8기 금융보안 최고위과정」을 개설하고 입교식을 개최하였습니다.

25

2024 일본 FISC 방문



06. 12.

일본 FISC가 금융보안원을 방문하였습니다. 금융보안원과 일본 FISC는 정기적으로 연구자료를 공유하고 있으며, 이번 방문에서는금융권 사이버보안 대응현황을 공유하고 협력을 강화하기 위한 방안을 논의하였습니다.

26

2024년
금융권 합동 재해복구 전환훈련 참가



06. 14.

「2024년 금융권 합동 재해복구 전환훈련」에 참가하였습니다. 이번 합동훈련은 대형 전산사고로 인한 금융서비스 중단을 예방하고 금융회사 IT안정성과 복원력을 제고하기 위해 진행된 금융권 합동 재해복구 전환훈련으로 금융보안원 등 6개 유관기관과 은행·카드·증권사 등 금융사 66곳이 참여하였습니다.

27

금융보안원 - 엘지유플러스 간
업무협약(MOU) 체결



06. 18.

엘지유플러스와 보이스피싱 예방 및 대응을 위한 업무협약(MOU)을 체결하였습니다. 이번 협약을 통해 금융보안원은 365일 24시간 운영 중인 「피싱사이트·보이스피싱 악성앱 탐지시스템」에서 탐지·분석한 정보를 실시간으로 제공하고, 엘지유플러스는 동 정보를 활용하여 고객이 악성사이트에 접속하는 것을 차단할 수 있게 됩니다.

22

RSA 컨퍼런스 2024 참석

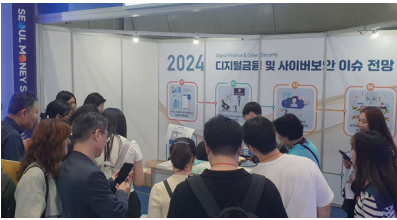


05. 06.

세계 최대 규모의 사이버보안 컨퍼런스인 「RSA Conference 2024」에 참석하여 AI를 통해 기능 및 성능을 고도화한 사이버 산업 구조의 현재를 진단하고 미래를 전망하는 시간을 가졌습니다.

23

2024 서울머니쇼 홍보부스 운영



05. 09.

매일경제신문·MBN·매일경제TV가 주최하는 「2024 서울머니쇼」에 참가하여 참관객을 대상으로 디지털금융 및 사이버보안을 안내하고 금융보안원의 주요 업무를 소개했습니다.

24

금융보안원 - 한국인터넷진흥원 간
업무협약(MOU) 체결



05. 14.

한국인터넷진흥원과 금융분야 사이버 침해사고 대응 협력을 위한 업무협약(MOU)을 체결하였습니다. 이번 협약을 통해 양 기관은 금융분야 관련 신규 보안 취약점 발굴 협력 및 상시 정보 공유, 침해사고 합동 조사 및 원인 분석·대응 공조, 사이버 위협 정보 상호 공유 등을 협력할 예정입니다.

28

금융보안원 - 개인정보전문가협회 간
업무협약(MOU) 체결



06. 19.

개인정보전문가협회와 금융분야의 안전한 개인(신용)정보 이용환경 조성을 위한 업무협약(MOU)을 체결하였습니다. 이번 협약을 통해 금융보안원의 금융IT·보안 전문 역량과 개인정보전문가협회의 개인정보 관련 법적 연구 역량이 시너지를 낼 수 있는 체계를 구축함으로써 금융권 개인(신용)정보의 안전한 활용·관리 및 보호를 도모하고자 합니다.

29

금융 AI 공모전, FSI AIXData
Challenge 2024 개최



06. 27.

FSI AIXData Challenge 2024를 개최하여 금융권에서 AI를 혁신적으로 활용할 수 있는 방안을 모색하였습니다.

30

제13회 정보보호의 날 기념 금융회사
최고경영자 초청 세미나 개최



07. 17.

「제13회 정보보호의 날 기념 금융회사 최고 경영자 초청 세미나」를 개최하였습니다. 김주현 금융위원장은 기조연설을 통해 “지금까지 디지털 금융혁신을 기반으로 ‘편의성 중심의 발전’을 이루어왔다면, 이제는 신뢰받는 금융을 위해 금융보안과 함께 ‘책임있는 발전’으로 나아가야 함”을 강조하였습니다.

금융보안원 소식

31

「금융권 현안 세미나」 개최



08. 05.

「금융권 현안 세미나」를 개최하였습니다. 본 세미나에서는 금융업계, 보안업계, 학계 등 담당자 100여 명이 참석한 가운데 MS 오류 등 글로벌 사이버 정전 사태의 사고 경과를 분석하고, 유사 사고를 예방하기 위해 전문가 의견을 청취하는 토론이 진행되었습니다.

34

대지중학교
금융보안교실 개최



08. 28.

대지중학교 금융보안교실을 개최하였습니다. 본 교실은 대지중학교 진로체험반 학생을 대상으로 금융보안관제센터 견학, 금융보안 인식 제고 특강을 진행함으로써 금융보안 인재 양성을 위해 다양한 활동을 수행하고 있습니다.

32

사이버작전사령부
금융보안교실 개최



08. 07.

사이버작전사령부 금융보안교실을 개최하였습니다. 본 교실은 육군사관학교 사관생도를 대상으로 진행되었으며 금융보안관제센터를 견학하고 금융권 사이버대응체계에 대하여 질답하는 시간을 가졌습니다.

35

라오스 중앙은행 방문



08. 29.

라오스 중앙은행이 금융보안원을 방문하였습니다. 금융보안원은 금융보안 관제센터 견학을 진행하고 금융권 사이버보안 대응 등 우리 원 업무에 대하여 소개하는 시간을 가졌습니다.

33

서울여대 정보보호 영재교육원
금융보안교실 개최



08. 09.

서울여대 정보보호 영재교육원 금융보안교실을 개최하였습니다. 본 교실은 교육부 지정 정보보호영재교육원 1권역 (서울/인천/강원/경기) 중학생을 대상으로 금융보안 인재 양성을 위해 다양한 활동을 수행하고 있습니다.

36

사이버서밋코리아(CSK) 2024
홍보부스 운영



09. 11.

국가정보원이 주최하는 「Cyber Summit Korea 2024」에 참가하여 참관객을 대상으로 디지털금융 및 사이버보안을 안내하고 금융보안원의 주요 업무를 소개했습니다.

37

금융보안원-행정안전부-한국정보통신
기술협회 간 업무협약(MOU) 체결



09. 12.

행정안전부 및 한국정보통신기술협회와 모바일 신분증 민간개방을 위한 평가체계를 구축하고자 업무협약(MOU)을 체결하였습니다. 이번 협약을 통해 국민이 안전하고 편리하게 민간 플랫폼의 모바일 신분증을 사용할 수 있도록 서비스에 대한 적합성·안전성 평가 체계를 마련하고자 합니다.

40

금융보안원 X NH농협은행,
우리 쌀 소비촉진 행사



10. 10.

신형춘 NH농협은행 정보보호부문 부행장 및 임직원들과 함께 쌀 소비 증진과 건강한 식습관 형성을 위해 우리 쌀 소비촉진 행사를 진행하였습니다. 행사를 통해 양사의 임직원들은 파트너십을 다지고 금융 정보보호 협력기관 간 소통의 장을 마련하였습니다.

38

제4회 모의해킹 경진대회
우리콘(WooriCON) 2024 시상식 개최



09. 23.

「제4회 모의해킹 경진대회 우리콘(WooriCON) 2024」 시상식을 개최하였습니다. 이번 대회는 금융보안원과 우리은행이 공동으로 진행 하였으며, 우리은행 인터넷뱅킹과 우리WON 뱅킹에서 발견된 잠재 취약점을 금융보안원의 보안 전문가·화이트해커와 정보보호학과 교수들이 심사해 총 5개 팀을 수상자로 선정하였습니다.

41

2024 동아재테크쇼
홍보부스 운영



10. 11.

동아일보·채널A가 주최하는 「2024 동아재테크쇼」에 참가하여 참관객을 대상으로 디지털금융 및 사이버보안을 안내하고 금융보안원의 주요 업무를 소개했습니다.

39

네팔 중앙은행 방문



09. 25.

네팔 중앙은행이 금융보안원을 방문하였습니다. 금융보안원은 금융보안관제센터 견학을 진행하고 금융권 사이버보안 대응 등 우리 원 업무에 대하여 소개하는 시간을 가졌습니다.

42

금융보안 아카데미
2024 수료식



11. 01.

금융권에 필요한 미래 인재 발굴 및 양성을 위해 정보보호에 관심있는 대학(원)생을 대상으로 사이버 침해 위험분석·대응 및 AI·빅데이터 분야 전문교육을 제공하여, 40명의 금융보안 미래 인재를 양성하였습니다.

금융보안원 소식

43

FISCON 2024 개최



11. 07.

「FISCON 2024」를 개최하였습니다. 이번 컨퍼런스는 <Advance with Big Waves>를 주제로 개최되었으며 민·관·산·학·연 전문가, 일반인, 학생 등 1,500여 명이 참석하며 높은 관심 속에 마무리 되었습니다.

46

FSI AIXDATA Challenge 2024
시상식 개최



11. 07.

「AI 경진대회 및 아이디어 공모전」(FSI AIXDATA Challenge 2024) 시상식을 개최하였습니다. 본 대회는 "AI기술로 금융의 미래를 열다."를 주제로 AI 모델 성능 경진대회와 생성형 AI 활용 아이디어 공모전이 두트랙으로 진행되었습니다.

44

FIESTA 2024
시상식 개최



11. 07.

「금융권 사이버 침해위협 분석대회」(FIESTA 2024) 시상식을 개최하였습니다. 본 대회는 금융기관 정보보호담당자와 우리원 직원의 침해대응 역량강화 및 대학(원)생의 우리원 인식 제고를 위해 매년 개최하고 있으며 올해는 참가인원이 전년 대비 5% 증가하여 총 454명 206팀이 참여하였습니다.

45

제8회 금융보안원
논문공모전 시상식 개최



11. 07.

「제8회 금융보안원 논문공모전」 시상식을 개최하였습니다. 본 공모전을 통해 디지털금융 및 금융보안 관련 연구, 아이디어, 기술에 대한 관심을 고취시켰습니다.

금융미래를 열어가는 금융보안파트너



CEO 뉴스레터 발간

금융회사 CEO를 위한 금융권 디지털 혁신·금융보안 관련 최신 동향

금융보안원은 금융회사 CEO가 금융권 디지털 혁신 관련 사이버 위협 및 정책 등의 최신 동향을 간결하고 쉽게 파악할 수 있도록 「CEO를 위한 디지털혁신과 금융보안」 뉴스레터를 발간·제공하고 있습니다.

CEO 뉴스레터 발간



2024년 1월호

- ▶**금융권 사이버 위협 동향(Cyber Threat)**
 - '23년 주요 사이버 위협 대응 동향 및 '24년 대응 방향'
- ▶**금융보안 정책 동향(Policy)**
 - 금융 안정의 새로운 위협, 인공지능(AI)



2024년 2월호

- ▶**디지털 IT 동향**
 - AI가 기업의 미래 경쟁력을 좌우, '책임 있는 AI' 시대 도래
- ▶**금융권 사이버 위협 동향(Cyber Threat)**
 - 금융보안원 화이트해커팀, 금융회사가 이용 중인 SW의 보안 문제점 다수 발견
- ▶**금융보안 정책 동향(Policy)**
 - 금융회사, [개인정보보호법 시행령] 개정에 따른 CPO 선임 미리 준비해야



2024년 3월호

- ▶**디지털 IT 동향**
 - 데이터 허브 품은 데이터거래스 2.0, 금융회사 비용 절감 및 경쟁력 향상 기대
- ▶**금융권 사이버 위협 동향(Cyber Threat)**
 - AI 플랫폼 악성코드 침투! AI 분야에도 공급망 관리 '적신호'
- ▶**금융보안 정책 동향(Policy)**
 - 금융감독원, 자율과 책임 강조하는 디지털 금융감독 방향 제시



2024년 4월호

- ▶**디지털 IT 동향**
 - 모바일 신분증, 금융업무에도 점차 확산될 전망 : 삼성월렛 시범서비스 개시
- ▶**금융권 사이버 위협 동향(Cyber Threat)**
 - AI 서비스가 악성코드 유통채널이 될 수 있다고? AI 공격 시나리오 발표
- ▶**금융보안 정책 동향(Policy)**
 - 자율보안 패러다임 전환 위한 '금융분야 위험관리 체계' 구축 필요

CEO 뉴스레터 발간



2024년 5월호

▶디지털 IT 동향

- RSA 2024, '가능성의 예술' [The Art of Possible]을 논하다

▶금융권 사이버 위협 동향(Cyber Threat)

- 금융회사 - 금융보안원 SW 공급망 보안 위한 실무협의체 출범

▶금융보안 정책 동향(Policy)

- 금융위원회 금융부문 망분리 규제 완화 추진



2024년 9월호

▶디지털 IT 동향

- 금융소비자 인식 변화, 내 자산 위해 편의성 포기하더라도 보안 강화 필요

▶금융권 사이버 위협 동향(Cyber Threat)

- 중국궤 우리나라 금융회사 침해 시도 급증!

▶금융보안 정책 동향(Policy)

- 금융분야 망분리 규제 개선 로드맵



2024년 6월호

▶디지털 IT 동향

- 데이터를 결합해서 생활 속 가치를 더하다!

▶금융권 사이버 위협 동향(Cyber Threat)

- 신용카드 정보 등 금융정보 유출 다크웹 거래로 이어져...

▶금융보안 정책 동향(Policy)

- 시가 내린 결정, 불만 있어요! 이용자 권리 행사에 대비한 준비 필요해



2024년 10월호

▶디지털 IT 동향

- 금융보안원, 금융 플랫폼 등의 '모바일 신분증 서비스' 안전한지 검증 나서다

▶금융권 사이버 위협 동향(Cyber Threat)

- 카드사 및 은행 대상, 디도스 공격 주의 당부

▶금융보안 정책 동향(Policy)

- 금융 분야 마이데이터 2.0 추진 위해 [신용정보업감독규정] 등 개정



2024년 7월호

▶디지털 IT 동향

- 'AI Safety' 위해 각국 정부 및 기업들 발 벗고 나서

▶금융권 사이버 위협 동향(Cyber Threat)

- 금융투자업권 대상 공격 시도 증가세... 주의 필요해

▶금융보안 정책 동향(Policy)

- [가상자산법 시행령] 의결 앞으로 무엇이 바뀌나



2024년 11월호

▶디지털 IT 동향

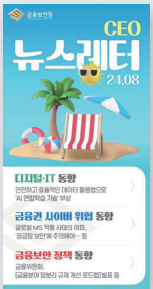
- 금융보안에 사용할 '생성형 AI 모델' 선정 위한 전문지표 개발

▶금융권 사이버 위협 동향(Cyber Threat)

- 금융권 공격 시도 대부분은 보안 사각지대에서 발생!

▶금융보안 정책 동향(Policy)

- 2025년도, 금융회사가 비즈니스 전략 수립에 고려해야 할 10가지



2024년 8월호

▶디지털 IT 동향

- '안전하고 효율적인 데이터 활용법으로 'AI 연합학습 기술' 부상

▶금융권 사이버 위협 동향(Cyber Threat)

- 글로벌 MS 먹통 사태의 여파, '공급망 보안'에 주의해야...

▶금융보안 정책 동향(Policy)

- 금융위원회, [금융분야 망분리 규제 개선 로드맵] 발표

PART. 4

부록

주요 간행물(가이드 및 안내서)

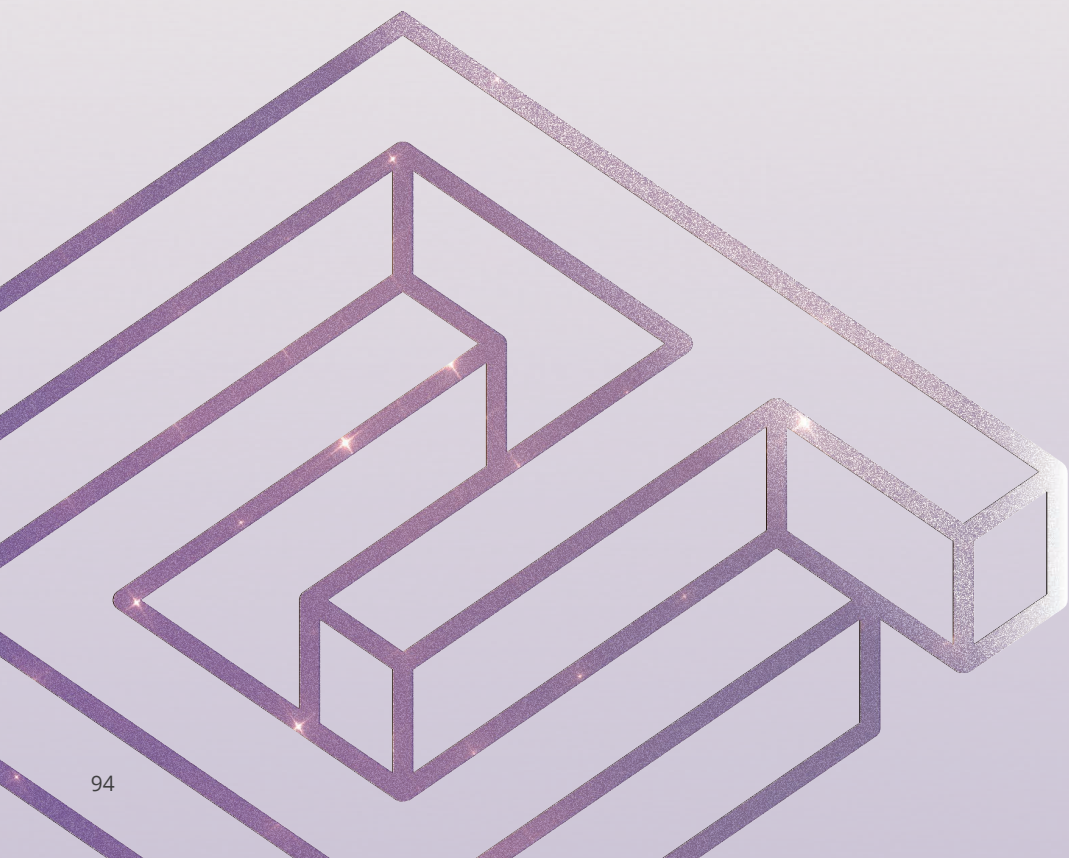
인텔리전스 보고서

위협헌팅 보고서

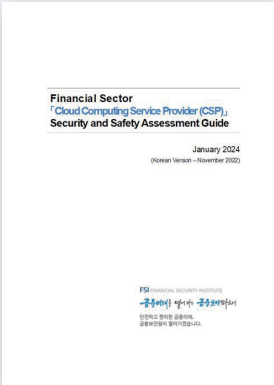
정기간행물

정보보호동향 보고서

언론홍보 현황



주요 간행물



금융분야 클라우드컴퓨팅서비스
제공자(CSP) 안전성 평가 안내서(영문)
(‘24.1.)

발간배경

- 금융분야 클라우드컴퓨팅서비스 제공자(CSP) 안전성 평가 수행 시 외국계 금융회사 및 CSP 사업자가 참고할 수 있도록 영문 안내서를 발간(개정본)하였으며, 기반사업자용으로만 배포되던 평가항목표*를 응용사업자 및 관리사업자도 참고할 수 있도록 함

*평가 항목에 대한 평가 방법 및 기준을 세부적으로 명시한 체크리스트

주요내용

- Chapter 1. CSP Security and safety Assessment
 - Basis
 - Assessment Target and Scope
 - Assessment Type and Method
 - Composition of Assessment Items
 - Assessment Procedure
- Chapter 2. CSP Security and Safety Assessment Criteria
- Appendix
 - CSP Security and Safety Assessment Item Table
 - Financial Security Institute CSP Security and Safety Assessment Support Procedure
- Annex
 - CSP Security and Safety Assessment Item Table (for Infrastructure Service Provides)
 - CSP Security and Safety Assessment Item Table (for Application Service Provides)
 - CSP Security and Safety Assessment Item Table (for Managed Service Provides)



금융분야 상용 클라우드 컴퓨팅서비스 보안
관리 참고서 (‘24.9.)

- 네트워크 관리
 - 업무 목적에 따른 네트워크 구성
 - 내부망 네트워크 보안 통제
 - 네트워크 보안 관제 수행
 - 공개용 웹서버 네트워크 분리
 - 네트워크 사설 IP주소 할당 및 관리
 - 네트워크(방화벽 등) 정책 주기적 검토
- 계정 및 권한 관리
 - 클라우드 계정 권한 관리
 - 이용자별 인증 수단 부여
 - 인사변경 사항 발생 시 계정 관리
 - 클라우드 가상자원 관리시스템 관리자 권한 추가인증 적용
 - 클라우드 가상자원 관리시스템 로그인 규칙 수립
 - 계정 비밀번호 규칙 수립
 - 공개용 웹서버 접근 계정 제한
- 암호키 관리
 - 암호화 적용 가능 여부 확인
 - 암호키 관리 방안 수립
 - 암호키 서비스 관리자 권한 통제
 - 암호키 호출 권한 관리
 - 안전한 암호화 알고리즘 적용
- 로깅 및 모니터링 관리
 - 가상자원 이용(생성, 삭제, 변경 등)에 관한 행위추적성 확보
 - 가상자원 이용 행위추적성 증적 모니터링
 - 이용자 가상자원 모니터링 기능 확보
 - API 사용(호출대상, 호출자, 호출일시 등)에 관한 행위추적성 확보
 - 네트워크 관련 서비스(VPC, 보안그룹, ACL 등)에 관한 행위추적성 확보
 - 계정 변동사항에 대한 행위추적성 확보
 - 계정 변경사항에 관한 모니터링 수행



금융분야 상용 클라우드 컴퓨팅서비스 보안
관리 참고서 (‘24.9.)

발간배경

- 금융회사에서 클라우드컴퓨팅서비스 제공자로 인한 제3자 리스크를 관리하는데 참고할 수 있도록 보안관리 참고서를 개발

대상 기업

- Amazon Web Services, Google Cloud, 카카오엔터프라이즈, KT Cloud, Microsoft, NAVER Cloud, NHN Cloud, ORACLE, 삼성SDS

주요내용

- 가상자원 관리
 - 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립
 - 이용자 가상자원 접근 시 로그인 규칙 적용
 - 가상자원 루트 계정 접근 시 추가 인증수단
 - 가상자원 생성 시 네트워크 설정 적용
 - 가상자원 접속 시 보안 방안 수립
 - 이용자 가상자원별 권한 설정
 - 이용자 가상자원 내 악성코드 통제방안 수립

인텔리전스 보고서



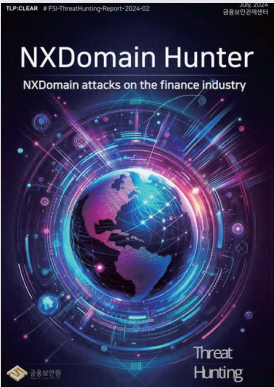
Operation BlackEcho,
금융 및 백신 앱으로 위장한 보이스피싱 악성
앱 프로파일링 (‘24.12.)

추진배경

- ‘23년 저금리 대출 신청 및 카드 발급내역 등을 이유로 금융소비자에게 금전 피해를 유발하는 악성 앱을 유포하는 범죄조직을 식별

주요내용

- 범죄에 악용된 금융 및 백신 앱으로 위장한 보이스피싱 악성 앱을 프로파일링하고 공격 기법 및 동향을 금융권과 유관기관에 공유하여 피해 방지에 기여



NXDomain Hunter,
금융권 대상으로 취약한 서브도메인 정보를
수집하는 조직 분석 (‘24.7.)

추진배경

- DNS 서버는 인터넷의 필수 시스템으로, 사이버 공격자들의 주요 표적이 되고 있으며, 국내 금융권을 대상으로 DNS 서버를 표적으로 한 공격이 점차 식별되고 증가하는 추세

주요내용

- 금융회사의 DNS 서버가 짧은 기간 동안 지속적이면서도 반복적인 대량의 NXDomain 응답을 반환하는 것을 확인하고, NXDomain 위협 헌팅 정책을 통해 금융회사를 대상으로 서브도메인 스캔을수행하는 조직(NXDomain Hunter)을 식별

위협헌팅 보고서



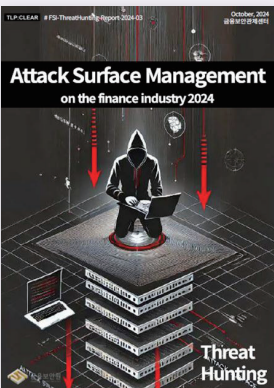
FSI Malicious IP
2023 분석을 통한 금융권 공격 동향
(‘24.3.)

추진배경

- 금융권을 대상으로 하는 공격 IP를 FSI 요주의 IP (Malicious IP)로 별도 지정하여 지속적으로 추적 모니터링

주요내용

- 2023년에는 시일이 지난 공격 방식을 기반으로 지속적이고 광범위한 공격 시도가 주를 이루었으며, 피싱 기법을 통한 배포와 감염 시스템을 이용한 DDoS 공격, 자주 쓰이는 시스템을 대상으로 하는 위협이 앞으로도 계속 발생될 것으로 판단



Attack SurfaceManagement,
공격표면 노출의 원인과 ASM 중요성 설명
(‘24.10.)

추진배경

- IT 환경이 복잡해짐에 따라 사이버 공격의 대상이 되는 공격 표면이 넓어지고, 기존의 사후적 보안관제 시스템만으로는 효과적인 대응에 한계가 있어 사전적 측면의 공격 표면 관리(ASM)의 필요성이 대두

주요내용

- 금융권의 공격 표면은 비전자금융서비스에서 더 많이 발견되며, 금융보안원은 이를 관리하기 위한 F-ASM 시스템을 개발하여 금융회사에 정보를 제공할 예정

정기간행물



전자금융과 금융보안 제35호

Research

- MPC 기술의 이해와 적용 사례
- 완전동형암호 기반 프라이버시 보존 기계학습 및 금융보안 분야의 응용

Issue·Trend

- 핀테크·신기술
 - API 보안 위협 및 대응방안
 - 차세대 디지털 자산 보호관리 기술
- 법·정책
 - EU 가상자산법(MiCA) 후속 지침 관련 주요 내용 및 동향 검토
 - 美 뉴욕주 「금융회사 사이버 보안 규정」 개정 주요 내용 검토



전자금융과 금융보안 제37호

Leading Article

- 금융보안 선진화의 의미와 나아갈 길

Research

- 다크웹에서의 랜섬웨어 활동분석
- CBDC 등 블록체인 기반 서비스를 위한 금융회사 전자지급 구현 방안과 발전 전망

Issue·Trend

- 핀테크·신기술
 - 생성형 AI 시스템에 대한 적대적 기계학습 공격 대응방안
 - 클라우드 네이티브 환경에서 타이포스쿼팅 위협에 대한 대응방안
- 산업동향
 - 금융분야 터치리스 생체인식 활용동향 및 시사점



전자금융과 금융보안 제36호

Research

- 위험기반 자산 분류 및 추진 방향
- 인공지능에 대한 각국 규제 동향 및 그 시사점
- 카드정보 탈취부터 부정결제까지 이어진 사이버 공격 분석

Issue·Trend

- 핀테크·신기술
 - 클라우드 네이티브 환경에서 소프트웨어 공급망 보안 고려사항
- 산업동향
 - 국내 CBDC 도입 추진 동향 및 시사점
- 법·정책
 - AI 안전성 평가 관련 국내외 정책 최신 동향 및 시사점



전자금융과 금융보안 제38호

Leading Article

- 환경 변화와 자율보안체계

Research

- ASM과 AI 기술의 접목을 통한 시너지 방안
- 기관용 CBDC 분산원장과 외부 분산원장 간의 안전한 토큰 프로토콜 설계 및 구현

Issue·Trend

- 핀테크·신기술
 - 제로트러스트 아키텍처 구현 사례 및 고려사항
 - 양자내성암호 전환 추진 동향

정보보호동향 보고서

발간월	제목	주요내용
2월	日「금융AI 데이터 개인정보 취급 안내서」주요 내용 및 시사점	AI 데이터 활용 추진 시 고려해야 할 법·규제 등의 개요를 제시하고, 이에 대한 시사점을 검토
3월	클라우드 네이티브 환경에서 SW 공급망 보안 고려사항	금융권이 안전하게 SW 공급망의 클라우드 네이티브화를 추진할 수 있도록 SW 공급망의 안전성 평가를 위한 보안 고려사항을 검토
4월	클라우드 네이티브 환경에서 타이포스쿼팅(Typosquatting) 위협에 대한 대응 방안	클라우드 네이티브 환경에서 타이포스쿼팅 위협 유형 및 대응 방안을 조사하고 시사점을 검토
	양자내성암호 알고리즘 표준화 동향	양자 컴퓨팅 시대의 보안성 보장의 핵심인 양자내성암호 알고리즘 검토
	제로트러스트 동향 조사	금융분야 비즈니스·ICT 환경 변화에 따른 보안 수요에 선제적으로 대응할 수 있도록 국내외 제로트러스트에 대한 주요 정책·산업 동향을 조사
	생성형 AI 시스템에 대한 적대적 기계학습 공격 대응 방안	생성형 AI에 대한 적대적 기계학습 공격을 분류하고 공격 기술을 조사·분석하여 특정 공격 유형을 완화할 수 있는 접근 방법 검토
5월	AI 기술 분류에 따른 활용영역 및 시사점	성공적인 AI 기술 활용을 위해 적용 업무에 적합한 AI 기술을 선택할 수 있도록 기능 관점에서 AI 기술을 분류하여 주요 특징과 활용사례를 설명하고 시사점을 도출
7월	美 NIST 사이버 보안 프레임워크 2.0 주요 내용 검토	美 국립표준기술연구소(NIST)에서 사이버보안 위험관리 세부 사항을 명시한 사이버보안 프레임워크(CSF)의 주요 내용을 검토
	AI 안전성 평가 관련 국내외 규제 동향 및 시사점	AI 활용 위험을 완화하기 위한 AI 안전성 평가를 도입하고 있는 바 관련 정책의 국내외 동향 및 시사점을 검토
8월	초거대 언어모델(LLM) 기술 동향 및 시사점	LLM 기술 동향을 조사·분석하고 현재 단계의 LLM 기술 수준을 파악하여 LLM 기술 연구 및 전문역량 확보를 위한 기초자료로 활용
	英 정부「보안내재화 가이드」주요 내용 및 시사점	디지털 대전환 시대에 금융권에서 안전하게 디지털 서비스를 제공할 수 있도록 英 정부의 보안내재화 가이드 주요 내용 및 시사점 검토
9월	제로트러스트 아키텍처(ZTA) 구현 사례 및 고려사항	금융권 망분리 규제 개선 추진에 따라 금융회사가 ZTA 구현·도입에 선제적으로 준비·대응할 수 있도록 ZTA 구현·도입 시 고려사항을 조사
	美 국방부의 클라우드 네이티브 액세스 포인트(CNAP) 설계 기준 및 시사점	상용 클라우드 리소스에 안전하게 접근할 수 있는 미국 국방부의 CNAP 설계 기준을 조사하여 시사점을 검토
	양자 기술 동향 및 시사점	금융권에서 양자 기술 도입에 따른 변화에 선제적으로 대비할 수 있도록 양자 기술에 대한 정책·산업 동향을 살펴보고 양자 기술을 조사하여 시사점을 검토

발간월	제목	주요내용
11월	금융분야 생성형 AI 위험에 대한 정책 고려 사항	금융분야 생성형 AI 위험을 최소화하고 신뢰할 수 있는 AI 규제·거버넌스 체계 마련을 위해 주요 이슈·과제에 대한 정책적 고려사항을 검토
12월	제로트러스트 전환 프레임워크 구성 및 평가 기준 조사	제로트러스트 전환 시 활용할 수 있는 프레임워크 및 평가 기준을 개발하여 원활하고 효과적인 제로트러스트 전환 전략 수립 및 지원

인론홍보 현황 - 2024년 언론보도 내역

보도일자	제목
1.4.	금융보안원 정기 인사
1.12.	23년 디(D)-테스트베드 사업 우수참여팀 6개 선정
2.5.	금융보안원, 지난 해 1,233억원의 보이스피싱 등 사기 피해 예방
2.7.	금융보안원, 국내 금융권 공급망 보안을 위한 CVE 발급기관 지정
2.15.	사이버위협 대응을 위해 화이트해커를 통한 은행업권 모의해킹 훈련 실시
2.19.	금융권 자율보안 체계로의 전환 동력, 금융보안교육센터에서 키운다
2.26.	금융보안원이 중소 핀테크기업의 '핀테크 보안점검'을 지원합니다
2.28.	금융데이터거래소, 안전하고 편리한 데이터 허브 서비스로 데이터 유통 혁신을 선도해 나가겠습니다
3.6.	해커의 관점에서 공급망 공격을 파헤치다!
3.11.	금융보안원, 2024년도 금융권 침해사고 대응훈련 실시
3.14.	금융보안원의 합성데이터 기술력, 세계적인 빅데이터·인공지능 학회에서도 인정
3.21.	금융분야 ISMS-P 인증체계, 디지털 금융 혁신의 신뢰 확보를 위한 안전판으로 자리잡았다
3.26.	금융보안원, 국가정보자원관리원과 업무협약 체결
4.1.	국민과 함께 만드는 안전한 금융, 「제8회 금융보안원 논문공모전」 개최
4.1.	2024년 상반기 디(D)-테스트베드 참여자 모집
4.2.	서울 대부중개플랫폼 합동점검 관련
4.8.	금융보안원, 「2024년 금융보안 자문위원회 전체회의」 개최
4.22.	금융보안원, 금융사기 수법을 심층 분석한 인텔리전스 보고서 공개
4.29.	금융보안원, 국제 사이버 방어전선에 서다
4.30.	"AI 활용해 보안 문제 혁신적 해결책 찾는다" 코드게이트 AI 아이디어랩 공모전
5.3.	2024년 「제8기 금융보안 최고위과정」을 시작합니다
5.16.	금융보안원-KISA, 금융분야 사이버 침해사고 예방 위한 협력 강화
5.28.	화이트해커와 함께 금융의 빈틈을 찾아라!
6.14.	금융회사 IT안정성 및 복원력 제고를 위한 2024년도 금융권 합동 재해복구 전환훈련 실시
6.18.	금융보안원-엘지유플러스, 보이스피싱 예방 및 대응을 위한 업무협약(MOU) 체결
6.19.	금융보안원-개인정보전문가협회, 금융분야의 안전한 개인(신용)정보 이용환경 조성을 위한 협력 강화
6.27.	"AI 기술로 금융의 미래를 열다", 「FSI AIXData Challenge 2024」 개최
7.4.	해외 금융을 노리는 악성 앱, 한구에 상륙하다: 금융소비자 주의 필요
7.8.	2024년 하반기 디(D)-테스트베드 참여자 모집
7.16.	「금융보안아카데미 2024」를 통해 미래인재를 키운다
7.17.	금융위원장, 금융보안원 주최 「정보보호의 날 기념 세미나」 참석
7.25.	금융보안원, 안전한 금융권 AI 활용을 위한 금융보안 AI 워킹그룹 출범
7.31.	금융보안원, MS 오류 등 '글로벌 사이버 정전 사태'를 계기로 본 「한국 금융보안의 현 주소와 나아갈 방향」 현안 세미나 개최

보도일자	제목
8.5.	"MS 사태는 안전하지 않은 SW 배포 절차가 원인"
8.13.	금융보안원, '해커들의 올림픽' DEFCON에서 맹활약
8.19.	금융보안원, '코리아 핀테크 워크 2024'에서 금융보안 세미나 개최
8.21.	금융보안원, 2025년도 신입직원 채용 실시
8.22.	전 금융업권 대상 「금융분야 망분리 개선 로드맵」 설명회 개최
9.12.	금융보안원-행정안전부-한국정보통신기술협회, 모바일 신분증 민간개방 적합성 평가를 위한 업무협약(MOU) 체결
9.23.	금융권 사이버 침해위협 분석대회, 「FIESTA 2024」 개최
10.15.	금융보안원, 금융정보보호 컨퍼런스 「FISCON 2024」 개최
10.16.	금융보안원, 금융 클라우드 보안 관리 설명회 개최
10.21.	금융보안원, 금융권 침해대응 인텔리전스 플랫폼 본격 서비스 개시
10.22.	사이버위협 대응을 위해 화이트해커를 통한 제2금융권 모의해킹 훈련 실시
10.31.	금융소비자, 디지털금융 이용 시 편리성보다 보안 선호
11.6.	금융보안원, 2025년에 주목해야 할 디지털금융 및 사이버보안 10대 이슈 선정
11.7.	금융정보보호 컨퍼런스 「FISCON 2024」 성황리 개최
11.11.	금융권 사이버 침해위협 분석대회, 「FIESTA 2024」 성료
11.14.	금융보안원, 'SW공급망보안 자율점검 체크리스트' 개발
11.19.	사이버 위협 대응의 패러다임 전환, 금융보안원 '실전형 침해대응 훈련 플랫폼' 구축
12.4.	사이버위협 대응을 위한 금융권 블라인드 모의훈련 성과 및 향후 계획
12.4.	금융보안원, 비상상황 대응 긴급 임원 회의 개최- 금융시스템 안전성 강화에 총력
12.12.	금융보안원, 블랙햇 유럽-아시아 컨퍼런스 연이어 발표
12.12.	금융권의 AI 활용을 적극 지원하겠습니다
12.15.	금융보안원, 비상상황 대응 긴급 회의 연이어 개최
12.18.	금융보안원, 2024년 금융권 버그바운티 운영 성과 발표
12.18.	금융감독원은 사이버위협에 선제적으로 대응하기 위해 「금융IT 비상대응 점검회의」를 개최하였습니다.
12.19.	금융보안원, 금융 AI의 안전망을 설계하다
12.23.	2024년 디(D)-테스트베드 우수 참여팀을 선정하고, 그간 성과를 공유하였습니다.

언론홍보 현황 - 기고 및 인터뷰

게재일자	게재 내역
1.29.	"AI로 은행 털려는 해커, 우리가 AI로 막는다"
2.19.	금융보안원 장운영 팀장 "CVE 발급기관 지정, 취약점 공유와 협업 활성화 계기"
3.5.	해커처럼 불시 공격으로 금융보안 점검... "10곳 중 9곳 안전해도 1곳 약하면 뚫려"
3.11.	금융보안원 보안평가부 "3rd Party 솔루션과 클라우드 취약점에 주목해야"
4.5.	[단독] 중국산 미니PC 주의보·비밀번호 터는 '악성코드' 심어 판매
7.29.	Expert raises concerns over AI misuse in human verification systems
7.29.	박진석 금융보안원 디지털전략본부장, 두 얼굴의 AI, 안전성 확보가 전제조건
12.1.	[유진아의 MZ라이프] "금융과 IT·보안의 교차점은?...현장에서 답을 찾다"
12.11.	South Korea Takes Down Fraudulent Online Trading Network Used to Extort \$6.3M

금융미래를 열어가는 금융보안파트너



2024 금융보안원 연차보고서

Financial Security Institute
Annual Report

발행일	2025년 6월	
발행처	금융보안원	
발간 총괄	기획부장	이찬웅
발간 협조	기획부	정나현
	금융보안교육센터	김정연
	금융보안관제센터	장성찬
	침해대응부	김규연
	보안평가부	김대은
	보안연구부	정동학
	금융인증부	김현석
	클라우드대응부	정희선
	데이터혁신센터	김태완
	AI혁신실	정진영
	개인정보보호부	김다영
발간 실무	커뮤니케이션팀	고성민, 박모현, 신정식, 백다은

본 보고서에 수록된 내용은 금융보안원의 서면 동의 없이 무단전제를 금합니다.

