KICA 한국정보인증

SaaS형 MFA(2차 인증) 서비스

signplus

한국정보인증(주)

Contents

회사 개요

차세대 인증 기술을 선도하는 '한국정보인증'

한국정보인증은 차세대 인증 기술을 선도하는 IT보안 전문 기업입니다.
20여 년간 전자서명 인증서비스 / 보안인증솔루션 운용 능력을 기반으로 자율주행 보안인증 플랫폼 및 생체인증 서비스 등
보다 안전하고 편리한 세상을 만들기 위해 노력하고 있습니다.

- 국가 지정 제 1호 공인인증기관
- 본인확인기관 / 전자서명사업자 허가
- 국정원 보안성 검토필 제품 인증 획득
- 국내 최초 FIDO 인증 상용화 (삼성페이)
- 국내 최초 OTP 개발·공급사

회사명	한국정보인증 주식회사
대표이사	김상준
설립일	1999년 7월 2일
자본금	208억원
임직원수	142명
매출액	878억
사업영역	PKI 기반 인증 서비스 및 기업/금융 인증 보안 솔루션
주소	경기도 성남시 분당구 판교로 242 판교디지털센터 C동 5층
홈페이지	www.kica.co.kr
연락처	전화 1577-8787 팩스 02-323-8513

비즈니스 영역

국내 No.1 인증서비스 & 인증 솔루션

국내 1호 공인인증기관으로 시작으로 정보보안 서비스의 대표 기업 한국정보인증은
공공, 금융, 교육, 기업 등 3,000여 개의 사용처를 대상으로 현재 인증 및 보안 서비스, 솔루션 등을 제공하며
법인인증서 및 국내 OTP 시장, 2차 인증 시장(조달기준)의 국내 점유율 1위를 유지하고 있습니다.

클라우드 인증

통합 인증 보안 서비스
ID/PW에 2차인증
(생체인증,OTP 등)을 적용한
SaaS형 보안 서비스

생체인증 및 페이 서비스
지문, 홍채, 안면 등 생체 기반
비밀번호 대체 서비스 및
국내 최초 생체인증서비스
ex)삼성페이,LG페이

통합인증 보안
전자금융 OTP 인증

통합 인증 보안 솔루션
ID/PW에 2차 인증
(생체인증,OTP, QR 등)을
적용한 보안 플랫폼

전자금융용 OTP
안전한 전자금융거래를 위한
인증보안 서비스

전자서명 인증

공동인증서비스
전자입찰, 전자세금계산서
등에 쓰이는 공동인증서 발급,
솔루션

S-PASS(간편인증)
안전하고 간편한
전자서명인증 서비스

자율주행 보안/
IOT 보안

자율주행차량 관련 R&D
차량 프라이버시 보호형
Vehicular PKI 인프라 기술
개발

IOT 기기인증 서비스
IOT 기기를 대상으로한
인증서 발급 서비스

전자계약

Sign OK
회원가입 필요 없는 편리한
전자 계약 서비스
이메일, SMS, MMS 통한
모바일 계약 기능

SSL
(보안서버인증서)

<SSL/TSL>
웹서버 간 데이터 암호화
프로토콜 서비스

Contents

MFA(2차 인증) 필요성

인증도용으로 시작하는 해킹

2022년 주요 기업 해킹 평균 피해액

43억원

생체인증, OTP 등 추가 인증 절차
통과 시에만 시스템 접속 허용

보안정보 내부자 유출이 70%

연간 주요 기업 정보 유출 피해액

56조원

생체인증, mOTP 기반한 인증 정보로
보안 위반 방지, 로그인 로그 관리

비밀번호 정책의 낮은 실효성

비밀번호 변경 따른 스트레스 체감도

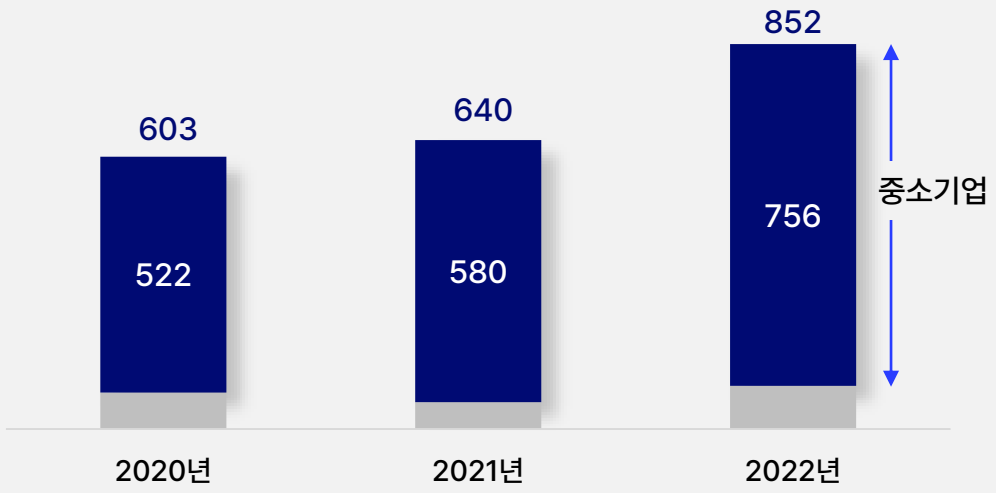
78%

FIDO(생체인증), OTP 등 사용으로
비밀번호 정책 보완 및 편리성 증대

MFA(2차 인증) 필요성

사이버 보안 역량 취약으로 해킹 주요 타겟

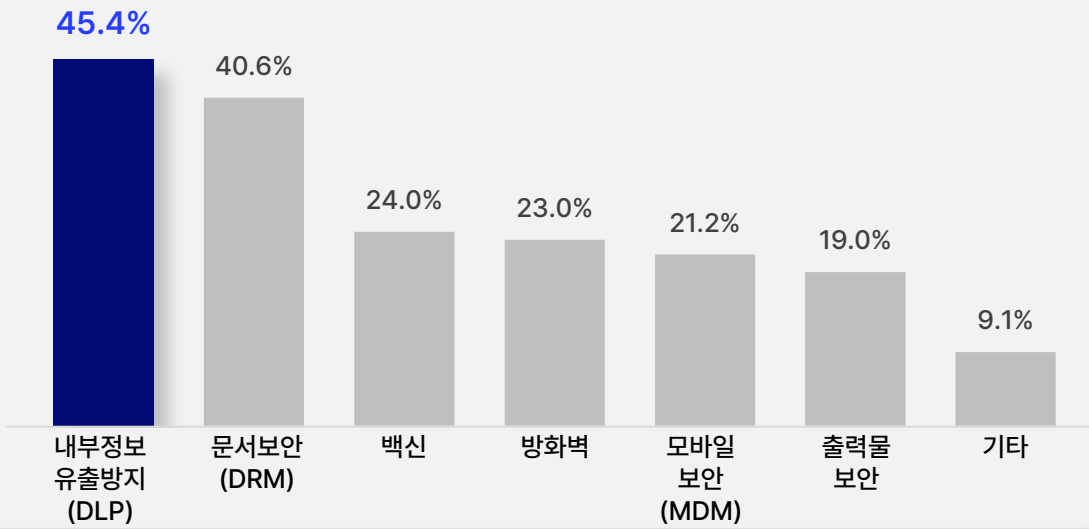
KISA 사이버 보안 침해사고 신고 현황



생체인증(FIDO), OTP 등 2차인증 도입으로
사이버 보안 역량 보완 및 내·외부 리스크 사전 예방

향후 도입을 희망하는 정보보호 솔루션

우선 투자 계획인 IT보안 분야



SaaS형 MFA(2차 인증) 구독 서비스로
중소기업 비용부담 해소, 보안 역량 향상에 기여

MFA(2차 인증) 필요성

ISMS 인증 기준 및 추가인증 도입 관련 법규

개인정보보호법 제29조
(안전조치의무)

개인정보의 기술적·관리적 보호조치 기준 제4조 4항
(접근통제)

개인정보의 안전성 확보 조치 기준 제5조
(접근 권한의 권리)
"...비밀번호를 5회 이상 틀린 경우, **추가인증으로 접근권한자임을 확인**..."

개인정보의 안전성 확보 조치 기준 제6조
(접근통제)
"...외부에서 접속한다면, 안전한 접속수단이나 **추가인증 수단을 적용**..."

개인정보 보호법에서는
추가인증(인증서 OTP 등)
도입과 관련해서
의무화할 것을 명시함

추가 인증 수단

공동/사설인증
(PKI)

일회성 비밀번호
(OTP)

생체인증
(FIDO)

SignPLUS 개요

누구나 손쉽게 사용 가능한 SaaS형 2차인증 서비스

별도 서버 구축이 필요 없는 SaaS형

User 수 기반 라이선스 구매의 구독 서비스(월간/연간)

FIDO(지문, Face ID), OTP 다양한 인증 지원

오류에 대한 상시 패치 및 업그레이드 지원

웹 및 오픈 네트워크 업무시스템 연동 지원

다양한 인증방안

- 고객사에 최적화된 인증 방법
- 생체인증, OTP 등 다양한 방법

클라우드 기반 솔루션

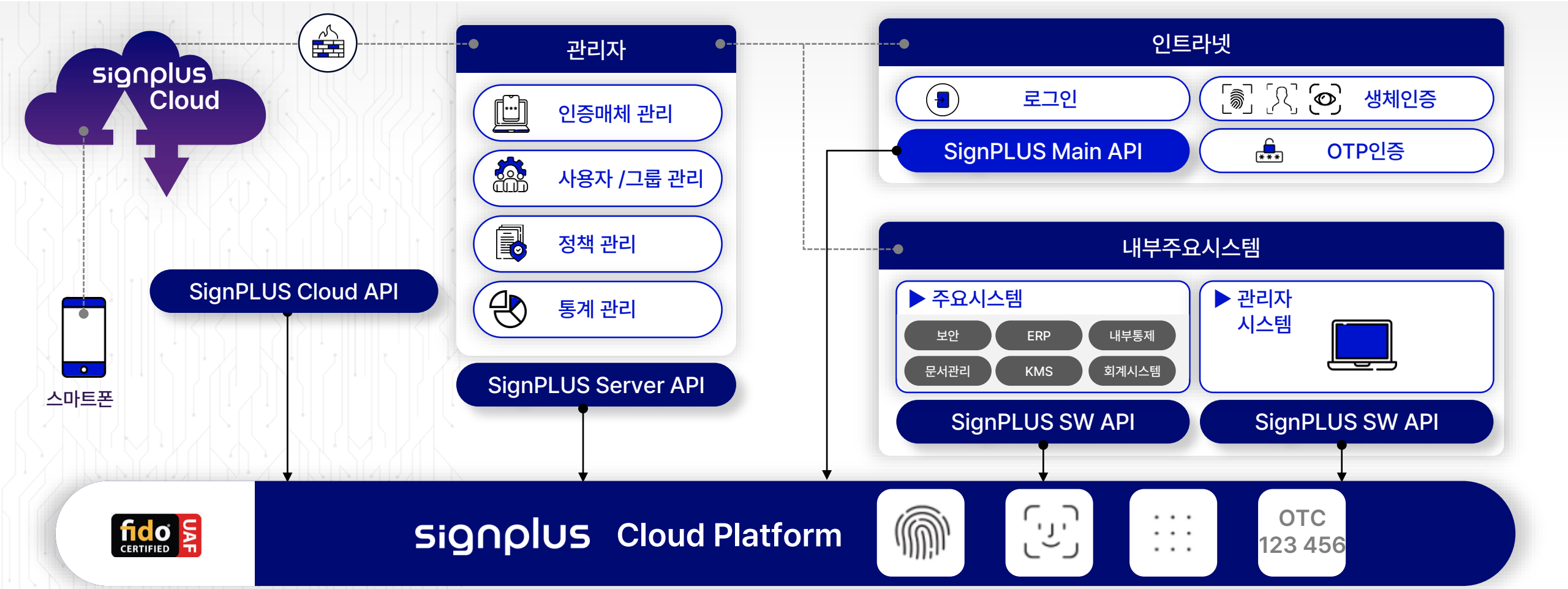
- 클라우드 형태 관리 편의성 극대화
- 손쉬운 업데이트, 시스템 연동

신뢰성 보장 운영 환경

- 안정적인 운영 시스템
- 안전한 키관리 백엔드 시스템

SignPLUS 시스템 구성

회사 내부 인트라넷 & 주요 시스템 접근 관리 기능 및 모듈 제공



SignPLUS 장점

클라우드 전환 시대, 보안을 서비스로 편리하게

기업과 금융, 공공 모든 분야에서 IT인프라가 클라우드 환경으로 전환되고 있습니다.
클라우드 환경의 SaaS, MFA 'SignPLUS'를 통하여 보안에서도 IT인프라 전환의 이점을 누릴 수 있습니다.

도입비용이점

저렴한 라이선스
"1 User 3,000원/월"

필요한 라이선스
수량/기간에 따라 결제

서버 구축 **Zero**,
유지보수 비용 **Zero**

서버 및 솔루션 관리의 편리함

인프라 관리의 피로도는 **LOW**

관리자 대시보드로
유저 관리 편의성 **High**

EOS, 업그레이드 관리
필요 없는 **SaaS**

SignPLUS 차별성

타사 대비 더 편리하고, 더 안전한 서비스

차별성

타사	구분	Sign Plus	비교
구글 인증모듈 설치 + 인증 체계 구성 필요	구축/연동 방법	**API 연동**	API로 쉽게 연동함으로써 별도 실행 파일 다운로드 불필요 및 사용 편의성 증대
미제공	관리자 콘솔	**제공**	관리자 페이지에서 MFA 발급에 대한 자체 관리 및 파악에 용이
별도 로그 관리 없음	로그 관리 항목	**로그 인증 내역 및 통계 제공**	사고 발생 시 데이터 복원, 사고원인 규명 등 가능
모바일 OTP	인증매체 지원	**생체인증(FIDO), 모바일 OTP**	인증수단 선택 통한 빠르고 간편한 본인인증 진행
백업 복구코드 입력(계정연동방식)	재발급 방법	**사용자가 APP에서 재발급**	사용자의 문제 발생에 따른 요청 시 대응 가능
연동시스템 별 재등록 후 사용	재발급 시 로그인 변경	**APP 재등록 후 즉시 사용**	사용자 인증매체 분실에 따른 관리자 공수 최소화

특장점

보안성

표준 해시알고리즘을 통해
일회용 암호키로 데이터 보호

편리성

한 번만 연동 또는 등록하면
별도 추가 작업이 불필요

관리성

제공된 로그 및 발급 관리로
문제 원인 파악 및 대응 가능

SignPLUS 기술 우수성

FIDO와 OTP를 융합한 안전한 인증 제공

최고의 인증 보안을 위한 기술 적용

- 표준을 준수하여 확장성 보장
- FIDO 국제 인증 획득
- OTP 기술과 융합 편리성 극대화

검증된 기술력

FIDO 서버

FIDO 클라이언트

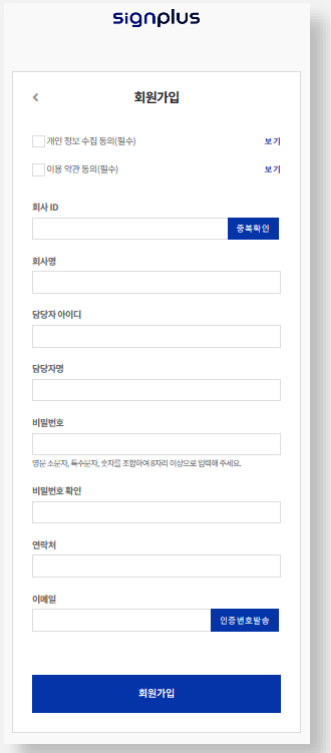
FIDO 보이스 인증장치

Contents

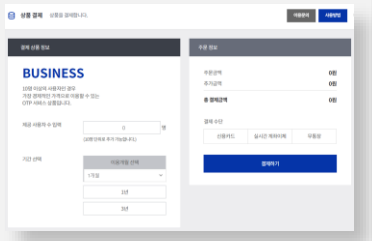
SignPLUS 도입 방법(관리자)

SignPLUS 연동 절차

회원가입

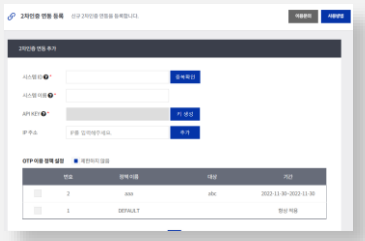


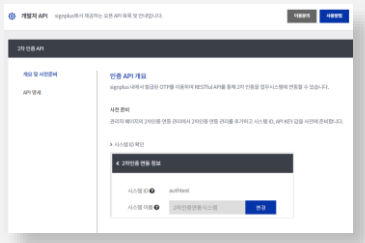
상품결제



관리자 회원가입 후, 상품 결제(카드, 계좌이체) 진행

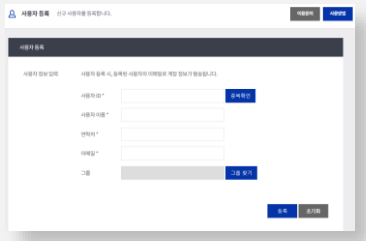
개발자 가이드

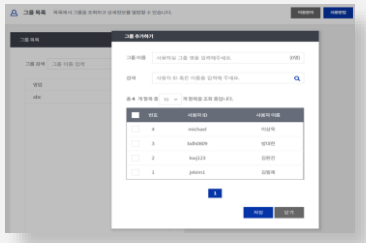




관리자 페이지 내 '개발자 가이드' 따라 연동할 업무시스템 연동 진행

사용자(일반 사용자) 추가

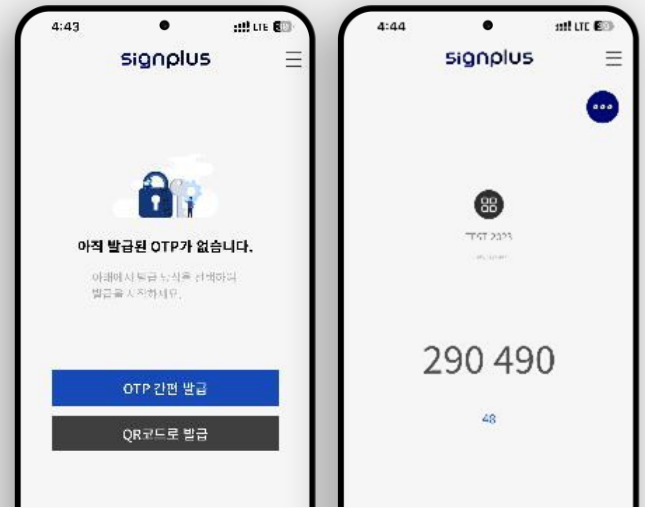




사용자 등록 메뉴 통해 일반 사용자 개별 및 일괄 등록

일반 사용자들 대상 간편발급 안내 진행

간편 발급



앱스토어, 플레이마켓 통해 SignPLUS 다운로드

회사코드 / 개인ID&PW 통한 간편발급 진행

SignPLUS 발급 방법(사용자)

SignPLUS 인증매체 발급 절차

관리자가 사용자 등록

- 관리자 페이지 내 사용자 등록
- 사용 인원의 ID, 이름, 이메일 등 등록

signplus app다운

원터치로 간편발급

- 사용자는 앱 실행 후 간편 발급 진행
- 별도 추가 작업 없이 바로 발급

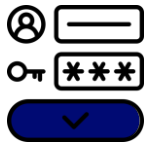
계정정보 입력

SignPLUS로 사용자 인증

- 회사 코드, 사용자 ID, 초기 PW 등 입력
- 개인정보 동의 및 본인확인 후 발급 완료

SignPLUS 인증(로그인) 절차

SignPLUS 인증(로그인) 절차



업무시스템 ID/PW 입력

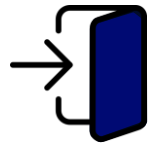
- 업무시스템 로그인창 내 ID/PW 입력
- SignPLUS App 자동 실행 또는 Push 터치

signplus app실행

SignPLUS로 MFA 인증

- **OTP |** SignPLUS에서 OTP 확인 후 입력
- **생체인증 |** SignPLUS에서 생체인증 진행

OTP FIDO 인증진행

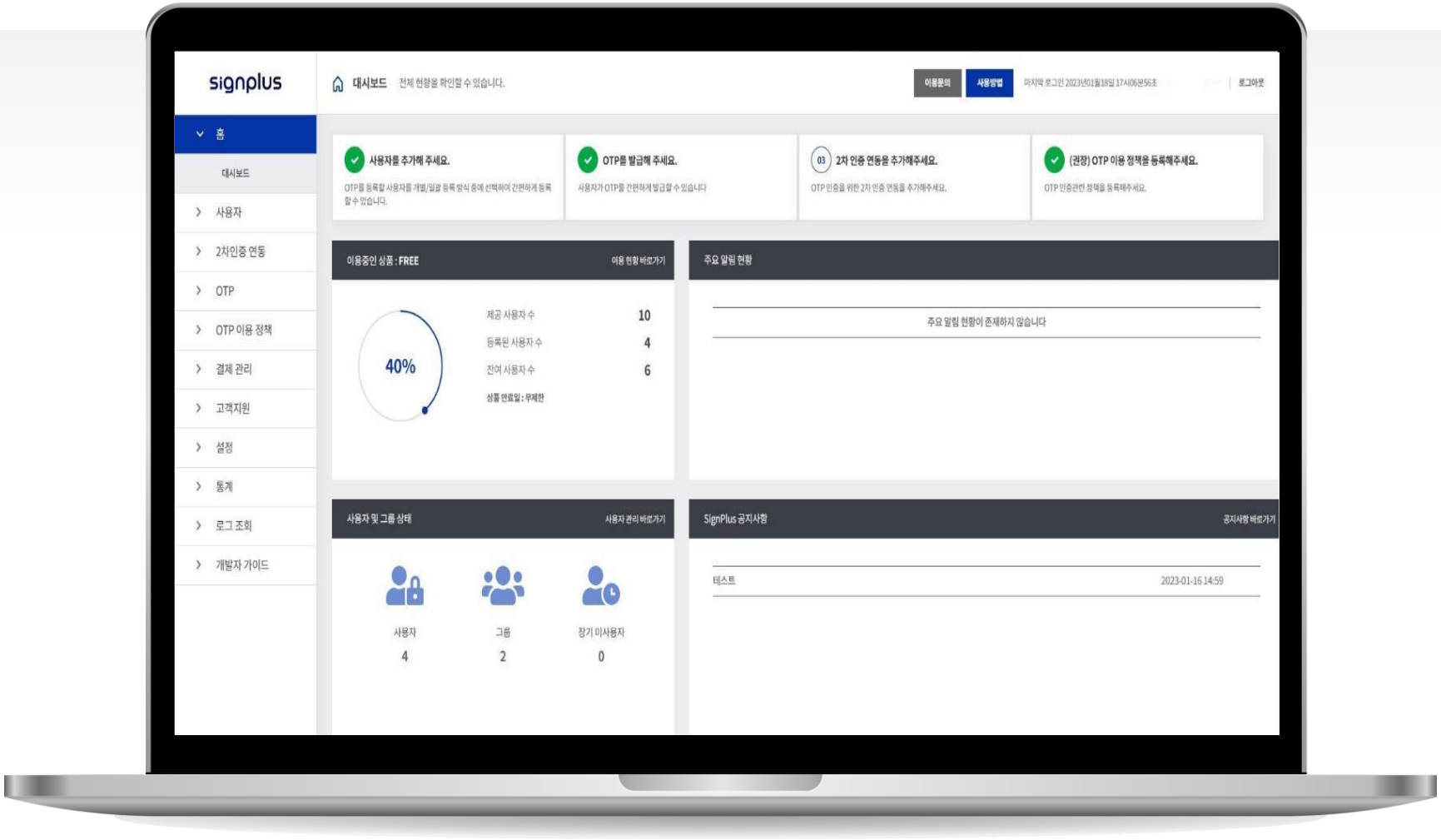


업무시스템 로그인 완료

- **OTP |** 로그인창 내 OTP 입력 후 로그인
- **생체인증 |** 생체인증 완료 후 자동 로그인

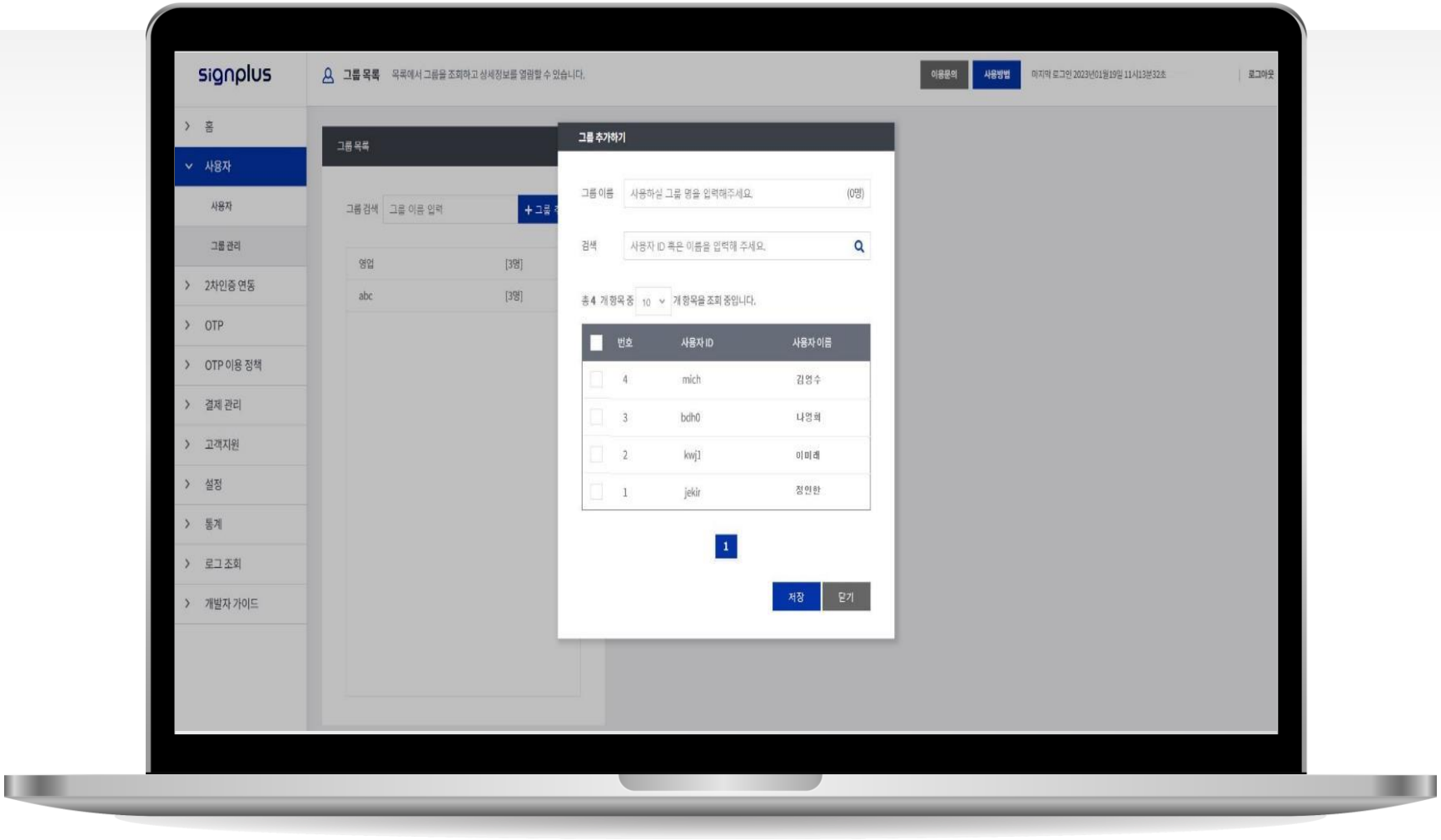
홈(대시보드)

관리자 포털의 홈(대시보드)를 통해 전체적인 서비스 사용 현황을 살펴볼 수 있습니다.



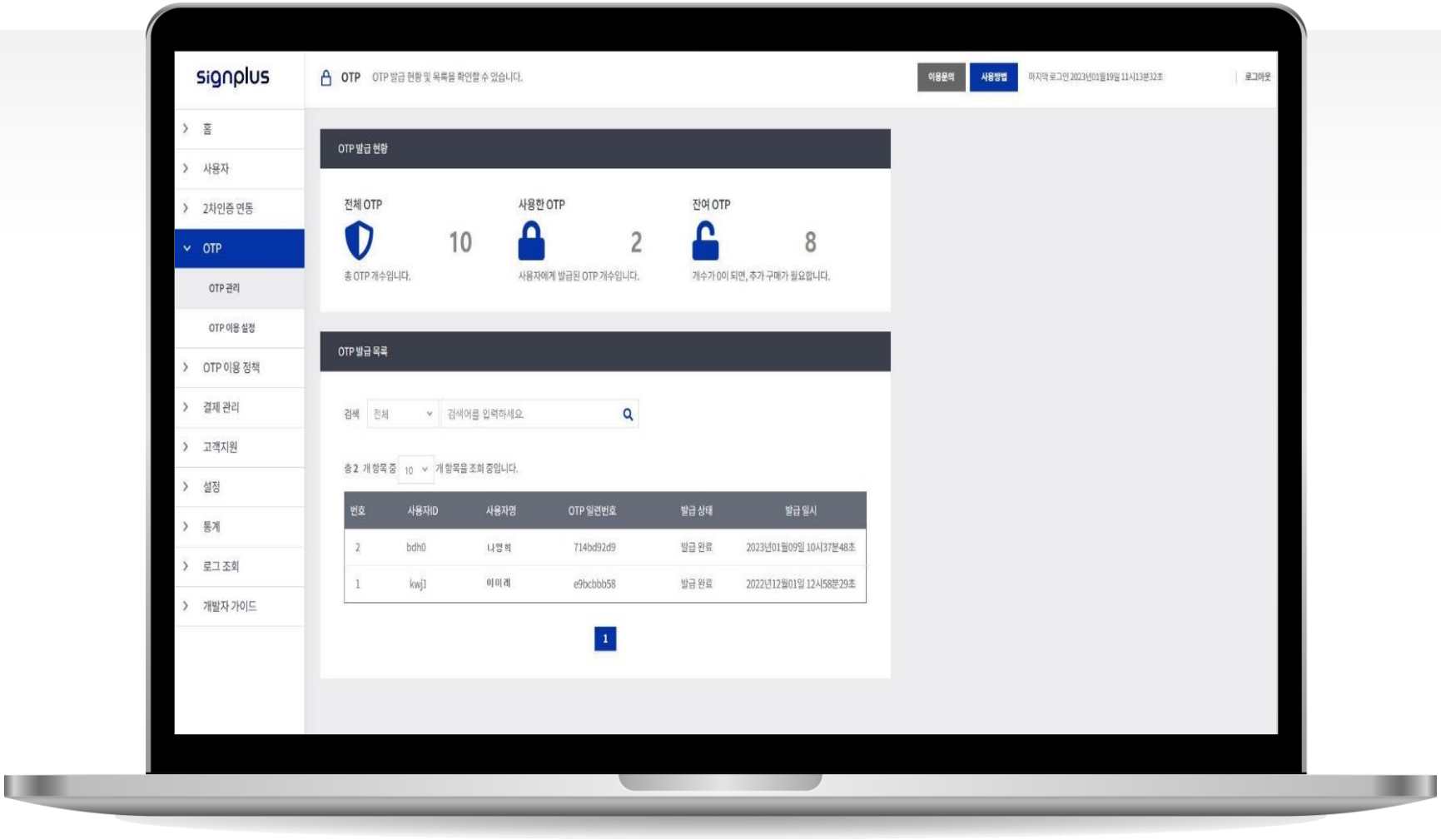
사용자/그룹 관리

관리자 포털의 사용자/그룹 관리를 통해 사용자를 등록하고 그룹별 구분 및 정책 설정할 수 있습니다.



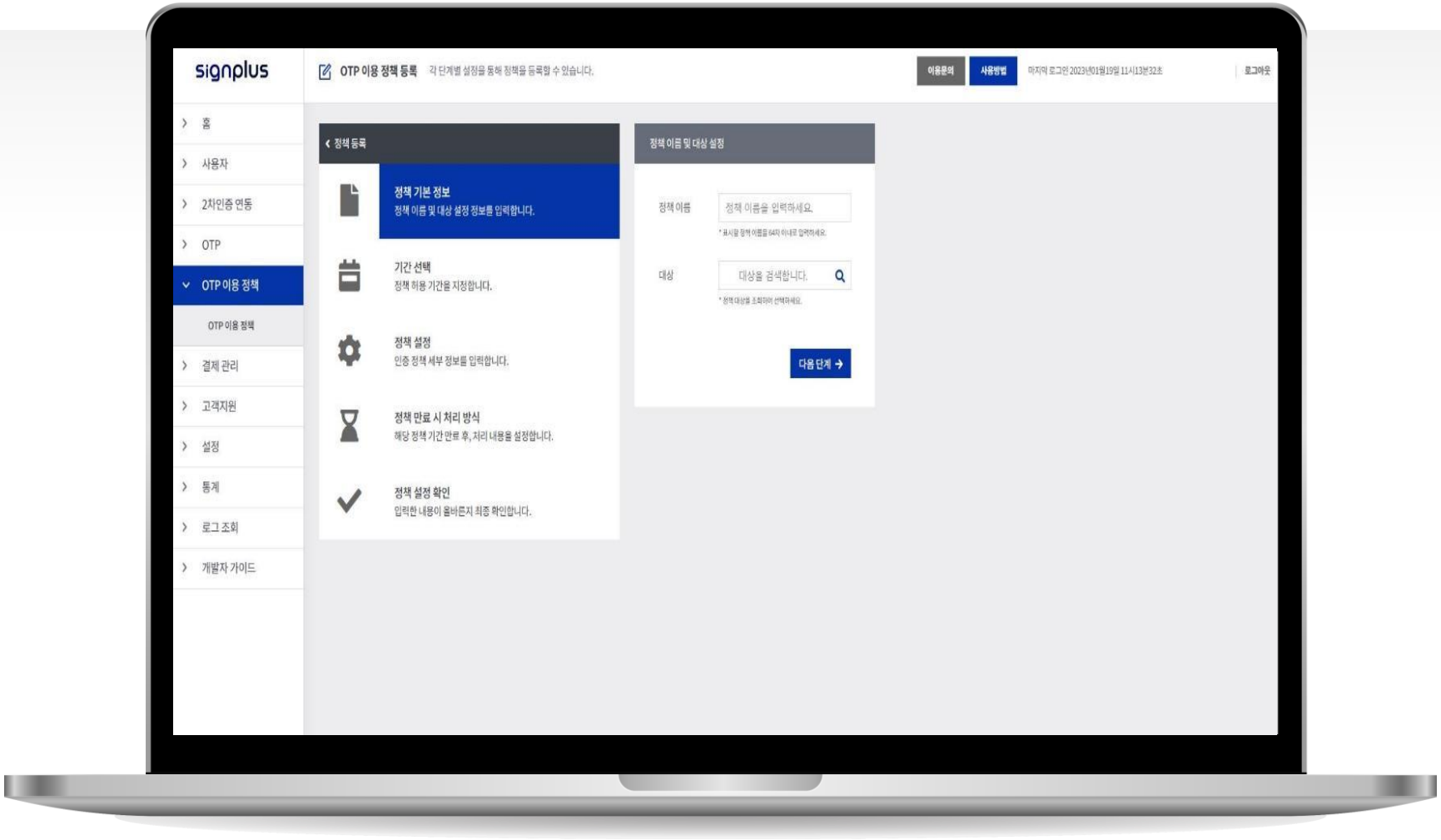
OTP 관리/이용 설정

관리자 포털의 OTP 관리 설정을 통해 간편하게 OTP를 발급 및 폐기할 수 있습니다.



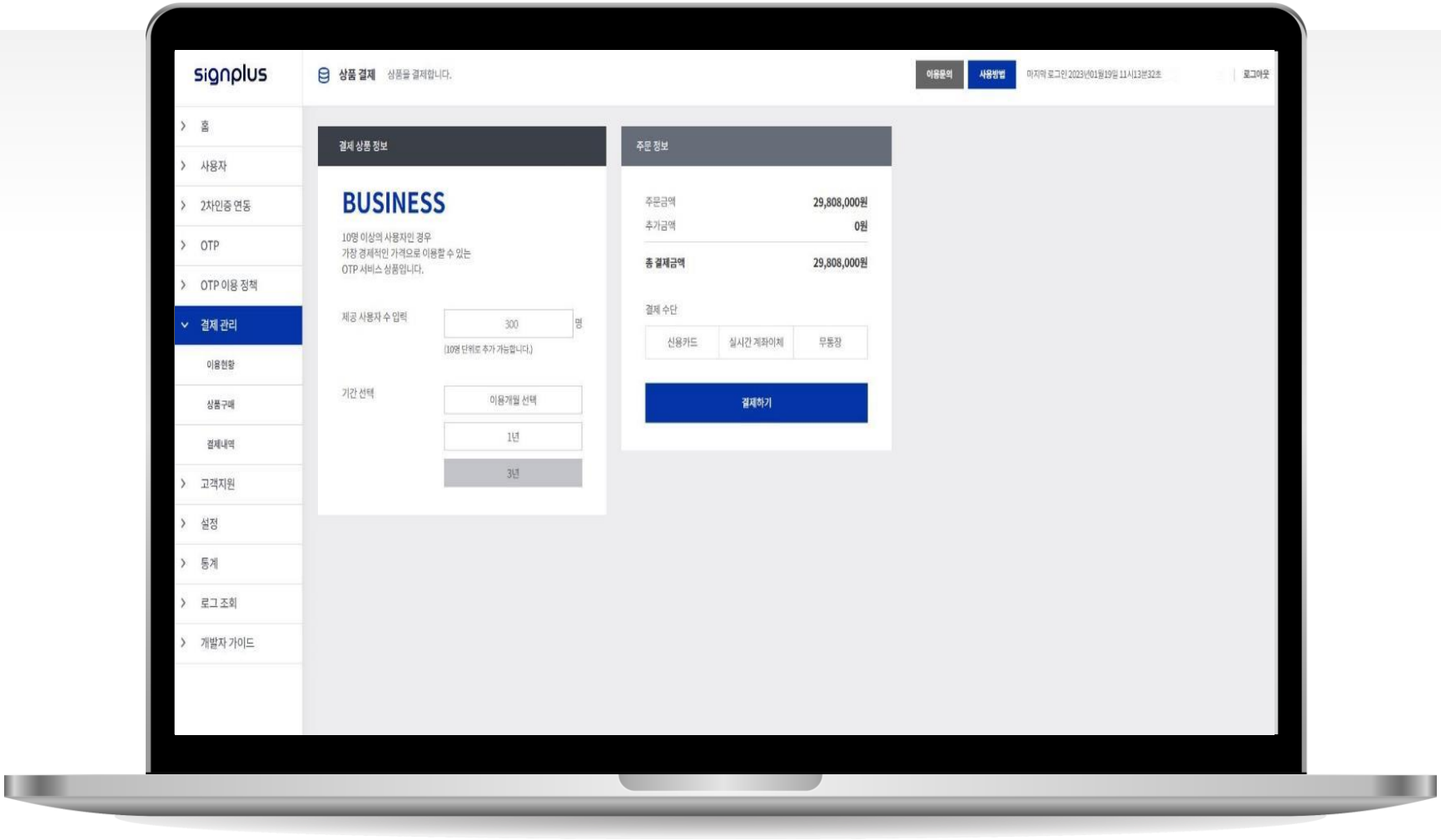
정책 설정

관리자 포털의 OTP 이용 설정을 통해 유효 정책을 설정할 수 있습니다.



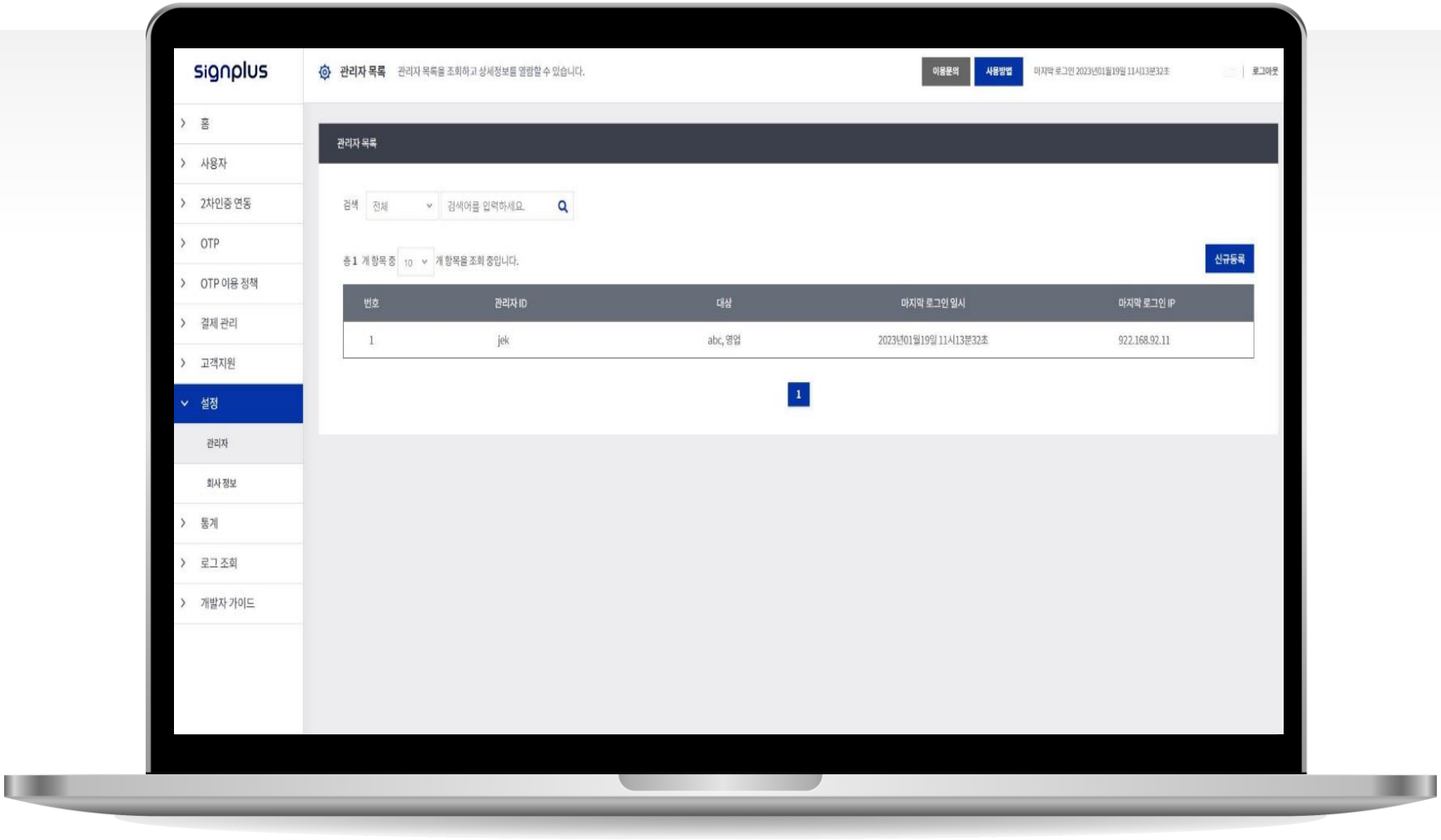
결제 관리

관리자 포털의 결제 관리를 통해 사용 중인 상품을 확인하고 유저 라이선스를 추가 구매할 수 있습니다.



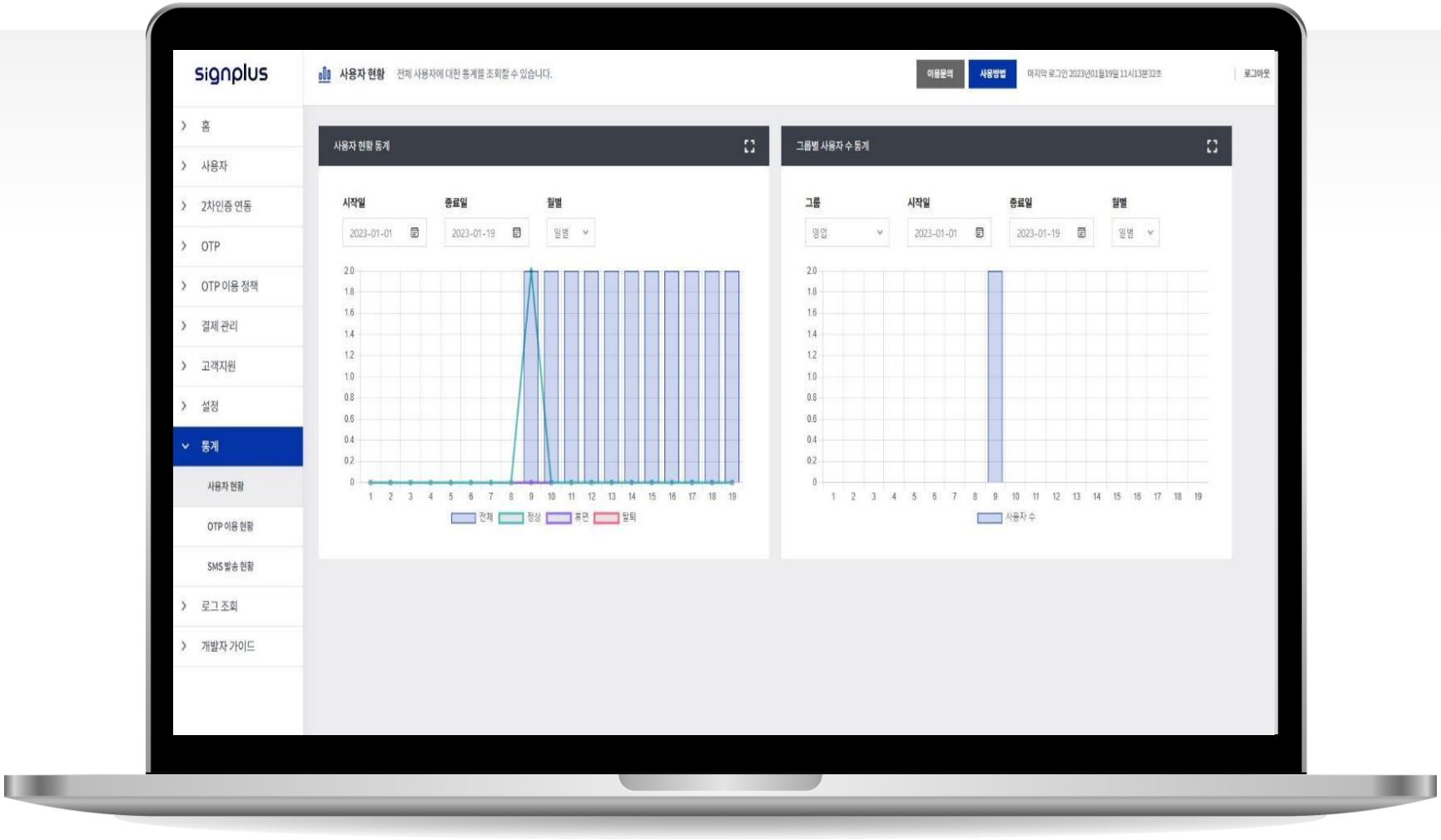
설정/관리자

관리자 포털의 설정/관리자를 통해 MFA 마스터 권한을 가진 관리자를 추가, 제거할 수 있습니다.



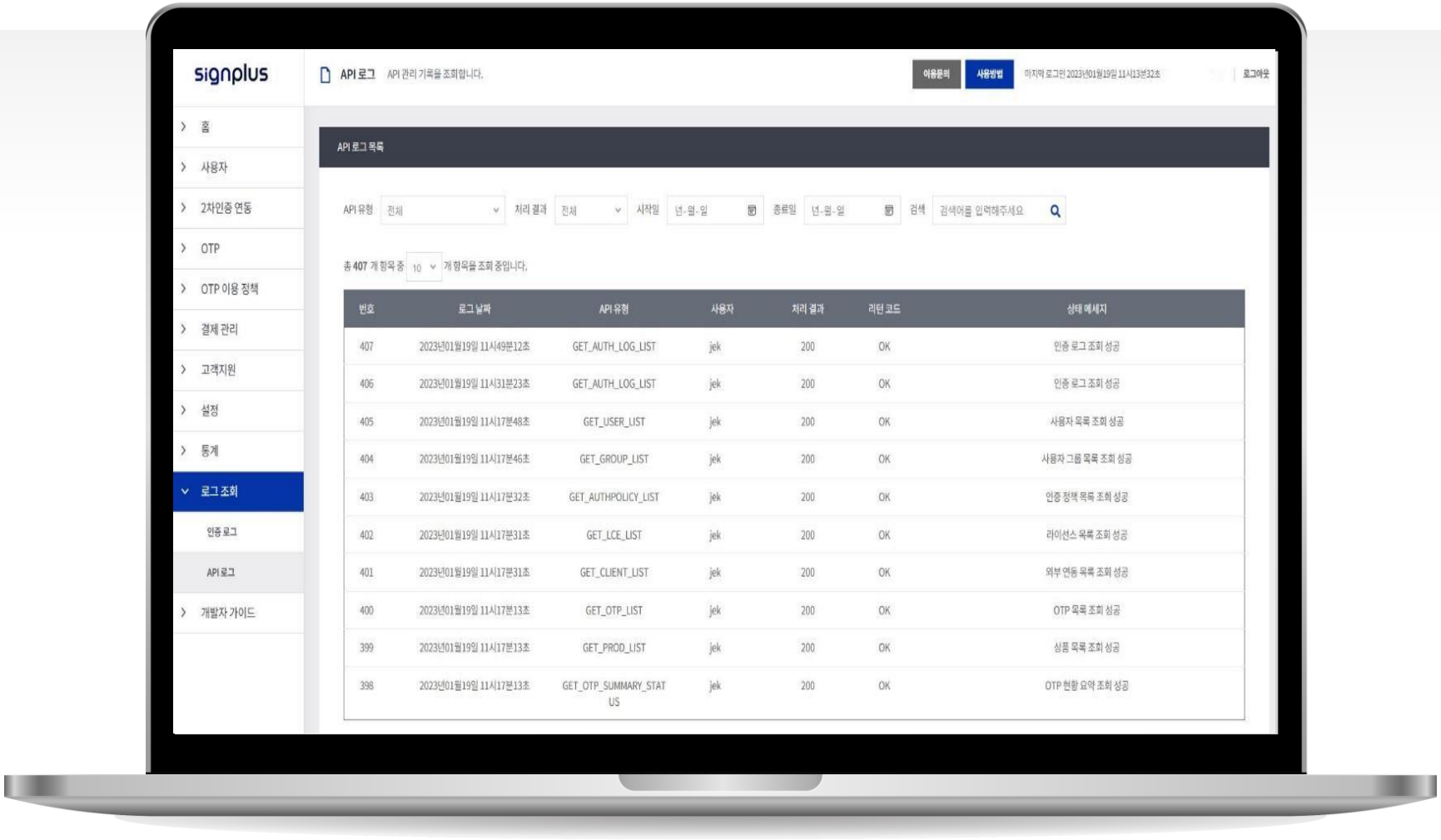
통계

관리자 포털의 통계를 통해 사용자 및 인증매체 발급현황, 매체별 인증 현황 등을 살펴볼 수 있습니다.



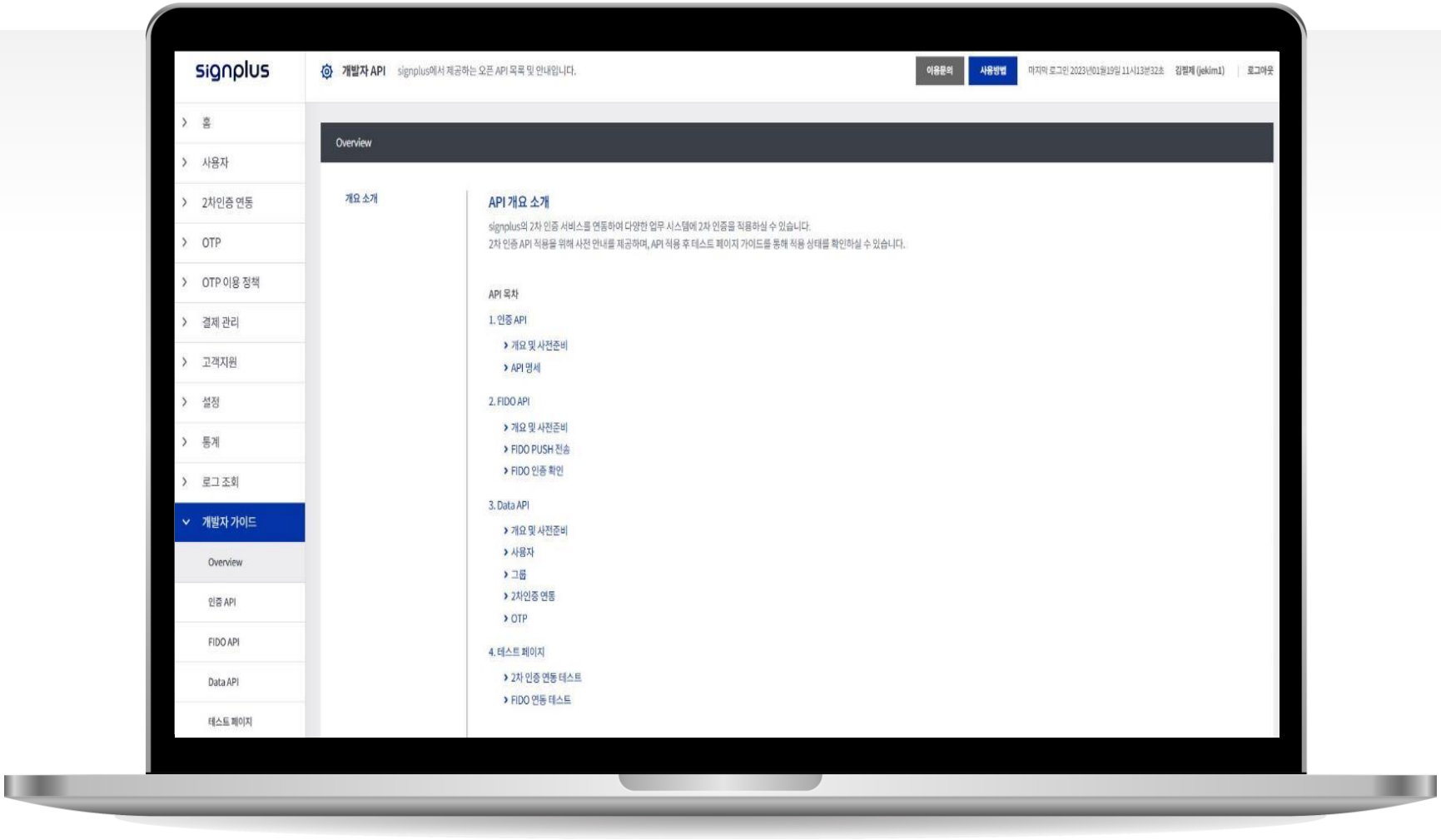
로그 조회

관리자 포털의 로그 조회를 통해 인증 로그 및 API 로그를 검색하고 살펴볼 수 있습니다.



개발자 가이드

관리자 포털의 개발자 가이드를 통해 서비스 이용 방법에 대한 도움을 얻을 수 있습니다.



MFA(2차 인증)도입 관련 법령

추가인증 도입 관련 법령

▶ 개인정보 보호법 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 **안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치**를 하여야 한다.

▶ 개인정보의 안전성 확보 조치 기준 제5조(접근 권한의 관리)_(6항)

개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

▶ 개인정보의 안전성 확보 조치 기준 제6조(접근통제)

개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 **안전한 인증수단**을 적용하여야 한다.

▶ 개인정보의 기술적•관리적 보호조치 기준 제4조 4항(접근통제)

정보통신서비스 제공자 등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 **안전한 인증 수단**을 적용하여야 한다

주요 공공기관 추가인증 도입 배경

▶ 국정원 정보보안 관리 실태 평가

(평가항목(5.2.1) 아이디, 패스워드 OTP 추가 인증 도입)

▶ 중요 정보시스템 접근 시 추가 인증을 통한 보안성 강화

▶ 외부 유지보수 및 용역업체, 프로젝트 인력 등에 의한 보안사고 및 업무과실 발생 시 책임소재 파악과 원인규명에 필요한 내부통제 및 감사체계 마련 필요

▶ 정보보호 컴플라이언스 준수 요구 강화

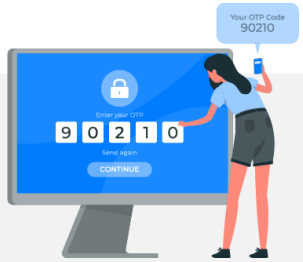
▶ 개인정보보호실태 점검 기준 준수 또는 보완 조치

▶ 외부메일 보안을 위한 2차 인증 도입

MFA(2차 인증)도입 관련 법령

개인정보의 안전성 확보 조치 기준 제5조(접근 권한의 관리)_(6항)

개인정보처리자는 개인정보처리시스템에 권한 없는 자의 비정상적인 접근을 방지하기 위하여 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우에는 개인정보처리시스템에 접근을 제한하는 등 기술적 조치를 하여야 한다.



해설

계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자 계정 잠금 등의 조치를 취하거나 계정정보.비밀번호 입력과 동시에 추가적인 인증 수단(**인증서,OTP 등**)을 적용하여 정당한 접근 권한 자임을 확인하는 등의 조치를 취하는 것을 말한다

출처. 개인정보의 안전성 확보조치 기준 해설서 / 행정안전부 / 2019

개인정보의 안전성 확보 조치 기준 제6조(접근통제)

개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

해설

- 접속수단의 예시 : 가상사설망(VPN), 전용선 등
- 인증수단의 예시 : 인증서(PKI), 보안토큰, 일회용 비밀번호(OTP) 등

인증수단만을 적용하는 경우, 통신 보안을 위한 암호화 기술의 추가 적용이 필요할 수 있으므로 보안성 강화를 위해 안전한 접속수단을 권고한다.

출처. 개인정보의 안전성 확보조치 기준 해설서 / 행정안전부 / 2019

KICA MFA Reference

기업

KICA MFA Reference

공사 / 공공기관

KICA MFA Reference

전자금융거래용

NH Bank, NH투자증권, KB국민은행, KB증권, KB손해보험, MG새마을금고, 신협, 저축은행중앙회, 산림조합중앙회, 우정사업본부, 우리은행, 우리종합금융, 우리에프아이에스, kakaobank, IBK기업은행, 한국은행, 삼성증권, 대신증권, KYOBO 교보증권, 키움증권, 신한은행, 제주은행, 신한생명, 신한카드, 신한금융투자, Heungkuk Finance Group, 신영증권, K bank, 한화투자증권, 한국증권금융, 하나은행, standard chartered SC제일은행, citi, KDB산업은행, DGB대구은행, eBEST, 하이투자증권, LEADING, 유진투자증권, meritz 메리츠증권, Sh 수협은행, 광주은행, 전북은행, BNK 경남은행, BNK 투자증권, 생명보험협회, 은행연합회, 한국신용정보원, koscom FUND SERVICES

해외

미국, 일본, 영국, 인도, 인도네시아, 베트남, 카자흐스탄, 우즈베키스탄, 싱가포르, 터키, 독일, 홍콩, 호주, 멕시코, 미얀마, 필리핀

경기도 성남시 분당구 판교로 242, C동 5층
signplus@signgate.com
02-360-3147

KICA 한국정보인증