GNX Co., Ltd.

LOGICNOID AIPhone™

The Blue Book of GNX Logicnoid AIPhone™

설명서·매뉴얼·참고서

운영자/기술담당자/인수인계용 공식 청서

문서 등급	Confidential - Licensing / Verification Draft v1.0
작성 기준일	2026-04-29
작성 근거	제공 소스코드, 특허 출원/명세 자료, 법인 및 통신사업 증빙 문서
용도	라이선스 협상, 기술 검증, 보안 실사, 운영 참조
공백 제외 본문 글자 수	6,847자 이상
비고	운영 비밀값, 개인식별번호, 원문 자격증명은 본 문서에서 재기재하지 않음

커버서

본 문서는 GNX Logicnoid AIPhone™ 및 연계 도메인 logicnoid.com, 안전.한국의 라이선싱 및 기술 검증을 위해 작성된 공식 정리본이다. 제공된 실행 소스와 출원 명세서, 출원 사실 증명, 우선심사 결정, 법인/사업자/통신 관련 증빙을 기준으로 기술적 주장과 현행 구현을 분리하여 정리하였다. 문서의 목적은 투자자, 리더, 보안전문가, 기술실사 담당자가 동일한 기준으로 시스템의 원리, 권리화 근거, 보안 통제, 운영 구조, 보완 조건을 검토할 수 있도록 하는 데 있다. 법률 의견서 또는 외부 보안인증서가 아니며, 정식 계약 전에는 별도 법률 검토, 침투시험, 개인정보 영향평가, 클라우드 구성 검토가 병행되어야 한다.

목차

1. 운영 원리 총론	
1.1	시스템 정체성
1.2	핵심 용어
1.3	역할과 접근권한
2. 아키텍처와 모듈	
2.1	서비스 계층
2.2	저장소와 vault
2.3	외부 연동
3. 주요 플로우 매뉴얼	
3.1	gWN 등록과 로그인
3.2	AIPhone/안전.한국/PrivateCall
3.3	ZET와 소유권 변경
4. API 및 데이터 운용 기준	
4.1	엔드포인트 그룹
4.2	데이터 모델
4.3	로깅과 관측
5. 보안 운영 절차	
5.1	시크릿과 키
5.2	접근통제
5.3	사고 대응
6. 관리자 운용과 배포	
6.1	일일 운영
6.2	백업과 복구
6.3	릴리스 체크리스트
7. 참고서 및 부록	
7.1	용어집
7.2	확장 설계
7.3	운영 인수인계

근거 자료 색인

자료	실사상 의미
AIPhone 출원사실증명원	특허-2026-0014512, 출원일 2026.01.25, 명칭: 전화번호 비노출 기반 텍스트 식별자 통신 아이덴티티 보안 통신 시스템
AIPhone 명세서	실제 전화번호 비노출, 텍스트 식별자, 디스플레이 레디, 상호 의존적 세션, 마켓플레이스 엔진 등 권리 구성
KIPO WNS 명세서	문자열 입력 정규화, 내부 전용 의미 해석 토큰, 상태 결합 판단, 강제 경유 실행 제어 구조
WNS 우선심사결정서	출원번호 10-2026-0010237, 우선심사대상 인정 통지
법인/사업자/통신 증빙	GNX Co., Ltd. 법인성, 사업자등록, 통신판매업 신고, 부가통신사업 신고 확인 자료
theLogoofLogicnoidcom.txt	EC2 배치 메인 로직 엔진으로 제공된 Python 기반 서비스 코드와 프런트엔드/신호 처리 로직

제1장 운영 원리 총론

1.1 시스템 정체성

GNX Logicnoid AIPhone™은 텍스트 식별자를 중심으로 통신, 인증, 표시, 자산 관리, 안전 수신망을 묶는 서비스다. 운영상 AIPhone은 사용자의 실제 전화번호를 직접 드러내지 않고 gWN 또는 텍스트 기반 식별자를 통해 호출 관계를 형성하려는 계층으로 이해한다. logicnoid.com은 gWN 등록, 로그인, 마켓, ZET, 관리자 기능을 제공하는 중심 도메인이고, 안전.한국은 숫자형 전화번호 기반 공개 수신/검증 흐름을 제공하는 보조 도메인으로 정리한다. PrivateCall은 외부 글로벌 노드와 S2S로 신호를 교환하는 고신뢰 또는 VVIP 흐름으로 취급한다.

1.2 핵심 용어

WN은 미소유 또는 등록 대기 상태의 문자열 식별자이고, gWN은 이메일과 비밀번호 및 CSS 계열 코드가 결합된 내부자 식별자이다. MCSS는 소유권 또는 마스터 성격의 코드, CSS는 표시/검증 계열 코드, SCSS는 세션 행위를 보호하는 단기 세션 코드로 운영한다. ZET는 서비스 내부 사용량, 충전, 이전에 쓰이는 포인트성 원장 단위이다. 안전.한국 계정은 전화번호와 이메일, 비밀번호 해시를 safe registry에 기록한다. SIGNALING_VAULT는 offer, answer, ICE, hangup 등 통신 이벤트를 임시로 보관하는 신호 저장소이다.

1.3 역할과 접근권한

운영 역할은 일반 사용자, gWN 내부자, 안전.한국 사용자, 관리자, S2S 피어, 결제 웹훅 송신자로 구분한다. 일반 사용자는 WN 조회와 신청을 수행하고, gWN 내부자는 로그인 후 호출, ZET, 소유권 변경, 마켓 기능을 이용한다. 안전.한국 사용자는 공개 수신망에서 숫자형 대상에 대한 수신 확인을 수행한다. 관리자는 WN 생성/삭제, 가격 변경, 오픈 상태 변경, rank 변경, 신청 내역 관리, 로그 조회를 수행한다. S2S 피어는 사전에 합의된 인증 헤더로 PrivateCall 신호와 레지스트리를 교환한다. 운영 문서상 관리자와 S2S 피어는 반드시 별도 비밀값, IP 제한, MFA, 감사 로그를 갖추어야 한다.

> 요약문: 제1장은 AIPhone의 운영 정체성을 텍스트 식별자 기반 통신 플랫폼으로 정의한다. WN/gWN, MCSS/CSS/SCSS, ZET, 안전.한국, SIGNALING_VAULT를 정확히 구분해야 일상 운영과 장애 대응이 가능하다.

제2장 아키텍처와 모듈

2.1 서비스 계층

현행 구현은 Python 표준 http.server 계열을 확장한 NobleHandler와 ThreadingSimpleServer가 모든 라우팅을 처리한다. 프로세스는 127.0.0.1:8000에서 실행되므로 외부 공개는 Nginx, ALB, Cloudflare Tunnel, 리버스 프록시 등 앞단 계층을 통해 이루어지는 것으로 해석한다. GET 라우트는 메인, vault, oneword, zet, change, 안전.한국 HTML을 제공하고, POST 라우트는 등록, 로그인, 신호, 결제, 관리자, S2S, 안전.한국 계정 기능을 JSON으로 처리한다. 프런트엔드 JavaScript는 WebRTC PeerConnection, ICE 후보 큐, 상태 표시, 결제 폴링, 이메일 인증 흐름을 포함한다.

2.2 저장소와 vault

저장소는 gnx_registry.vault, gnx_safe_registry.vault, gnx_bank.vault, gnx_zet_bank.vault, gnx_applied.vault, privatecall_registry.vault로 분리되어 있다. 각 vault는 문자열 직렬화 후 키 기반 변환을 거쳐 파일로 저장된다. 운영 매뉴얼에서는 이 구조를 초기 파일 기반 저장소로 부르고, 상용 운영에서는 PostgreSQL 또는 DynamoDB, Redis, S3/KMS 백업으로 이전하는 절차를 별도로 둔다. 파일 락은 단일 프로세스 내부의 동시성에는 도움이 되지만 다중 프로세스, 컨테이너 스케일아웃, 장애복구 환경에서는 충분하지 않다.

2.3 외부 연동

외부 연동은 세 종류다. 첫째, SMTP는 인증코드, 호출 알림, 소유권 이전, 결제 오류 안내 메일을 발송한다. 둘째, S2S는 globalgnx.com의 /api/s2s/inbound로 PrivateCall 관련 신호를 전송하거나 수신한다. 셋째, 결제 웹훅은 입금자명과 금액을 bank ledger에 기록하고, ZET 충전 화면은 이를 폴링하여 매칭 여부를 확인한다. 운영 환경에서는 SMTP 계정, S2S 비밀값, 웹훅 키, 도메인 인증, SPF/DKIM/DMARC, 요청 서명 검증, 재전송 방지 토큰을 모두 별도 관리해야 한다.

요약문: 제2장은 구현 아키텍처를 단일 Python 서비스, 파일 vault, SMTP, S2S, 결제 웹훅으로 설명한다. 엔터프라이즈 운영에서는 웹서버, 데이터베이스, 캐시, 비밀관리, 관측 시스템을 분리해 확장해야 한다.

제3장 주요 플로우 매뉴얼

3.1 gWN 등록과 로그인

등록 흐름은 사용자가 WN을 선택하고 이메일 인증코드를 받은 뒤 비밀번호와 코드로 register를 호출하는 방식이다. WNSLogic.register는 문자열을 소문자와 공백 제거 기준으로 정규화하고, 비밀번호는 해시 토큰으로 저장하며, MCSS와 CSS를 생성한다. OneWord 또는 TwoWord 카테고리에 따라 value와 ZET 리워드가 산출될 수 있다. 로그인 흐름은 ignite가 WN과 비밀번호를 확인하고, 상태가 gWN이면 새 CSS와 SCSS를 생성하여 INSIDE 응답을 반환한다. gnxceo 최고권한 경로는 운영상 비상 계정으로만 취급하고, 정식 운영에서는 폐쇄하거나 break-glass 절차로 격리해야 한다.

3.2 AIPhone/안전.한국/PrivateCall

AIPhone 호출은 /api/signal/send로 offer를 저장하고, 수신자가 /api/signal/receive로 신호를 가져가며, 연결 과정에서 answer, ICE, hangup, reject, cancel이 처리된다. offer가 일정 시간 대기하면 monitor_and_alert가 이메일 알림을 발송한다. 안전.한국은 전화번호와 이메일 인증으로 safe registry를 만들고, 공개 호출 또는 수신 확인 흐름에서 숫자형 대상과 연결된다. PrivateCall은 call_type이 private일 때 S2S 송신과 dormant_private_alert를 통해 외부 레지스트리 이메일 알림을 병행한다. 운영자는 이 세 흐름의 목적과 데이터 범위가 다르다는 점을 사용자 약관과 로그 정책에 반영해야 한다.

3.3 ZET와 소유권 변경

ZET는 사용량 과금, 충전, 이전에 활용된다. apply_usage_fee는 gnxceo를 제외한 사용자에 대해 호출 횟수를 누적하고 5회마다 1 ZET를 차감하는 구조다. ZET 충전은 금액과 입금자 매칭 후 이메일 코드 확인으로 잔액을 증가시킨다. /api/zet/transfer는 문장형 payload에서 @대상 식별자와 금액을 추출하여 내부 잔액을 이전한다. 소유권 변경은 change/auth와 change/confirm 흐름으로 인증 후 owner, pwd, master_css, css, birth_date를 갱신하고 이전 안내 메일을 발송한다. 상용 운영에서는 ZET를 법정 전자금융/포인트 규제 관점에서 검토하고 환불, 유효기간, 회계처리를 문서화해야 한다.

요약문: 제3장은 사용자 흐름을 등록/로그인, 통신 호출, 공개 안전망, PrivateCall, ZET, 소유권 변경으로 나누어 설명한다. 운영자는 각 흐름의 인증 조건, 데이터 저장 위치, 알림 방식, 법적 표시 의무를 분리해 관리해야 한다.

제4장 API 및 데이터 운용 기준

4.1 엔드포인트 그룹

공개/사용자 그룹에는 /check_wn, /send_code, /register, /ignite, /api/market, /api/apply_wn이 있다. 통신 그룹에는 /api/signal/send, /api/signal/receive, /api/public_call, /api/check_resonance가 있다. ZET/결제 그룹에는 /api/zet/req_code, /api/zet/charge, /api/zet/deduct, /api/zet/transfer, /api/verify_transfer, /api/bank_webhook이 있다. 안전.한국 그룹에는 /safe/send_code, /safe/register, /safe/login, /api/safe_tower/list, /api/safe_tower/delete가 있다. 관리자 그룹에는 /admin/users, /admin/create, /admin/delete, /admin/update_val, /admin/toggle_open, /admin/toggle_rank, /admin/logs 등이 있다. S2S 그룹에는 /api/s2s/sync_registry, /api/s2s/inbound가 있다.

4.2 데이터 모델

registry의 사용자 레코드는 type, color, value, owner, real_name, status, condition, category, pwd, market_open, master_css, css, rank, birth_date를 포함한다. safe registry는 전화번호를 키로 이메일과 비밀번호 토큰을 저장한다. ZET bank는 gWN별 잔액 맵이며, bank ledger는 입금자, 금액, timestamp를 담은 배열이다. applied registry는 WN 신청자 이메일, 가격, timestamp, market_open 상태를 기록한다. private registry는 전화번호, fingerprint, email, timestamp를 저장한다. 민감 필드는 최소화하고, 운영 전 데이터 사전과 보존기간, 삭제 기준을 별도로 작성해야 한다.

4.3 로깅과 관측

현재 로깅은 server.log와 MEMORY_LOGS에 주요 이벤트를 남긴다. 예를 들어 Identity Alchemy, Supreme Login, Signal Delivery, S2S Inbound/Outbound, Bank Webhook, Payment Matched, Safe Tower Delete 등이 기록된다. 운영 매뉴얼은 로그 레벨, 개인정보 마스킹, 보존기간, 접근권한, 장애 알림 조건을 정의해야 한다. 권장 관측 지표는 로그인 성공/실패율, offer 대기 수, signal delivery 지연, 이메일 발송 실패율, ZET 잔액 변경 건수, 결제 매칭 실패율, S2S 실패율, 관리자 변경 이벤트, vault 저장 실패, CPU/메모리/디스크 사용량이다.

> 요약문: 제4장은 API를 사용자, 통신, ZET, 안전.한국, 관리자, S2S로 그룹화한다. 데이터 모델과 로그는 기능 운영의 핵심이지만 개인정보와 보안 이벤트를 포함하므로 마스킹과 무결성 보존이 필수다.

제5장 보안 운영 절차

5.1 시크릿과 키

운영 전 가장 먼저 할 일은 모든 비밀값을 소스에서 제거하는 것이다. SYSTEM_SALT, ROOT_KEY, SMTP 비밀번호, S2S 비밀, 은행 웹훅 키, 도메인 인증 토큰은 AWS Secrets Manager 또는 Parameter Store SecureString에 저장하고, 배포 시 IAM Role로 주입한다. 비밀값은 서비스 계정별로 분리하고, 최소 90일마다 회전하며, 사고 의심 시 즉시 폐기한다. 문서와 로그에는 실제 값을 절대 쓰지 않는다. 암호화 키는 데이터 암호화 키와 토큰 서명 키를 분리하고, 키 버전과 키 폐기 절차를 둔다.

5.2 접근통제

관리자 API는 외부 인터넷에 직접 노출하지 않는다. VPN, Zero Trust Access, mTLS, 관리자 MFA, IP allowlist, RBAC를 적용한다. /admin/users와 /admin/logs는 개인정보와 내부 잔액, 신청 내역이 노출될 수 있으므로 read 권한과 write 권한을 분리한다. /api/bank_webhook과 /api/s2s/inbound는 공유 키 비교만으로는 부족하므로 HMAC 서명, 타임스탬프, nonce, 재전송 방지 저장소를 적용한다. /api/signal/send는 SCSS 검증 예외를 최소화하고, sender 유형별 정책을 명시한다.

5.3 사고 대응

사고 유형은 비밀값 노출, 관리자 오남용, ZET 잔액 변조, 수신망 오작동, S2S 위조 요청, 이메일 발송 실패, vault 손상, 개인정보 유출 의심으로 나눈다. 공통 절차는 탐지, 격리, 비밀값 회전, 로그 보존, 영향 범위 산정, 사용자 통지 여부 검토, 복구, 사후 개선이다. 즉시 조치로는 관리자 라우트 차단, S2S 키 폐기, SMTP 계정 잠금, bank webhook 비활성화, registry 백업에서 복원, ZET ledger 동결을 둔다. 사고 이후에는 원인 분석 보고서와 재발 방지 항목을 릴리스 체크리스트에 반영한다.

> 요약문: 제5장은 보안 운영의 우선순위를 시크릿 관리, 접근통제, 사고 대응으로 둔다. 현행 기능을 안전하게 유지하려면 관리자와 S2S, 결제, vault, 로그를 별도 통제영역으로 격리해야 한다.

제6장 관리자 운용과 배포

6.1 일일 운영

일일 점검은 프로세스 상태, 디스크 여유 공간, SSL 인증서 만료, 최근 오류 로그, 이메일 발송 실패, S2S 오류, 결제 매칭 실패, 관리자 변경 이력, vault 파일 수정시간, 백업 완료 여부를 확인하는 방식으로 수행한다. 운영자는 임의로 vault 파일을 직접 편집하지 않고 관리자 도구 또는 승인된 마이그레이션 스크립트를 사용한다. 사용자 요청 처리 시에는 본인확인, 요청 사유, 처리자, 처리시각, 변경 전후 값을 남긴다. 가격 변경, rank 변경, 계정 삭제, 안전.한국 삭제는 이중 승인 대상으로 둔다.

6.2 백업과 복구

파일 vault 운영 단계에서는 매시간 증분 백업과 매일 전체 백업을 수행하고, 백업은 KMS 암호화된 S3 버킷에 보관한다. 복구 시험은 주 1회 샌드박스에서 수행하며, registry, safe registry, zet bank, applied registry, private registry 간 참조 무결성을 점검한다. bank ledger와 ZET bank는 회계적 의미가 있으므로 변경 로그와 백업을 동시 보존해야 한다. 데이터베이스 이전 후에는 point-in-time recovery와 스냅샷 복구 절차를 적용한다.

6.3 릴리스 체크리스트

릴리스 전에는 소스 해시, 의존성 목록, 비밀값 제거, 정적 분석, 단위 테스트, API 권한 테스트, 수동 시나리오 테스트, 마이그레이션 리허설, 백업 확인, 롤백 계획, 약관/개인정보 문구 변경 여부를 확인한다. 배포 후에는 30분, 2시간, 24시간 기준으로 로그와 지표를 관찰한다. 장애 시에는 즉시 이전 버전으로 롤백하고, registry와 ZET 상태 변경이 발생한 경우 데이터 복구 절차를 병행한다. 릴리스 노트에는 기능 변경, 보안 변경, 데이터 변경, 운영자 행동 필요사항을 분리해 적는다.

> 요약문: 제6장은 일일 운영, 백업/복구, 릴리스 절차를 공식화한다. 운영 안정성은 기능 수가 아니라 변경 통제, 백업 검증, 롤백 가능성, 이중 승인, 감사 로그에 의해 결정된다.

제7장 참고서 및 부록

7.1 용어집

AIPhone은 전화번호 비노출형 통신 아이덴티티 시스템을 뜻한다. Logicnoid는 문자열 식별자와 실행 제어를 결합한 GNX 서비스 체계의 명칭으로 사용한다. WN은 등록 가능한 문자열 식별자, gWN은 소유자와 인증정보가 연결된 내부자 식별자, ZET는 내부 포인트성 사용 단위, MCSS는 마스터 코드, CSS는 회전 표시 코드, SCSS는 세션 검증 코드, Safe Korea는 안전.한국 공개 수신망, PrivateCall은 비공개 고신뢰 호출 흐름, S2S는 서버 간 신호 교환을 의미한다.

7.2 확장 설계

확장판은 서비스 코어, 아이덴티티 서비스, 시그널링 서비스, 결제/포인트 서비스, 관리자 서비스, 알림 서비스, 감사 서비스로 분리한다. API Gateway는 인증과 rate limit을 수행하고, Redis는 신호 큐와 nonce 저장소로 사용하며, PostgreSQL은 registry와 ZET 원장을 저장한다. KMS는 암호화 키를 관리하고, CloudWatch 또는 OpenTelemetry는 로그와 지표를 수집한다. 프런트엔드는 도메인별 앱으로 분리하되 공통 인증과 식별자 정책은 중앙 서비스에서 제공한다.

7.3 운영 인수인계

인수인계 패키지는 소스 저장소, 배포 스크립트, 환경변수 목록, 비밀값 주입 방식, 도메인/DNS 자료, TLS 인증서 갱신 방법, 데이터 사전, API 명세, 관리자 매뉴얼, 장애 대응 문서, 백업/복구 절차, 테스트 계정, 연락망, 법무 증빙, 변경 이력으로 구성한다. 인수인계 회의에서는 등록, 로그인, AIPhone 호출, 안전.한국 호출, ZET 충전, ZET 이전, 소유권 변경, 관리자 가격 변경, 장애 복구를 실제로 시연해야 한다. 라이선스 수령자는 이 절차를 통과해야 운영권을 안정적으로 행사할 수 있다.

> 요약문: 제7장은 용어, 확장 설계, 인수인계를 정리한다. 청서는 시스템을 설명하는 문서인 동시에 운영자가 같은 방식으로 배포, 점검, 복구, 이전을 수행하게 만드는 기준서다.

부속 표준표

운영 체크리스트

주기	운영 항목
일일	프로세스, 디스크, 로그, 이메일, S2S, 결제 매칭, 백업 완료 여부 점검
주간	복구 리허설, 사용자/관리자 권한 점검, 로그 보존 상태 확인
월간	비밀값 회전 계획 확인, 취약점 패치, 의존성 목록 갱신
릴리스 전	테스트, 비밀값 제거, 롤백 계획, 데이터 마이그레이션 리허설
사고 시	격리, 키 회전, 로그 보존, 영향 범위 산정, 복구, 보고

요약문: 운영 체크리스트는 실제 서버 운용자가 동일한 절차로 점검하고 기록하게 만드는 최소 표준이다.

최종 고지

본 문서는 제공 자료를 기준으로 작성된 공식급 정리본이며, 외부 법률 의견서, 특허 등록 확정서, 보안 인증서, 개인정보 영향평가 결과서를 대체하지 않는다. 외부 제공 시에는 NDA, 원본 증빙 대조, 비밀값 제거 확인, 개인정보 마스킹을 선행해야 한다.