

N E W N A L

퍼스널 데이터 노드

기업이 고객 데이터를 직접 수집·보관하지 않고,
고객이 허락한 더 넓은 범위의 개인 데이터로 서비스를 만드는
뉴날의 데이터 관리 구조

퍼스널 데이터 노드의 정의와 구조, 데이터 스피어를 통한 데이터 공유 방식,
기업이 얻는 이점, 공개 원장(InfraBlockchain)의 역할을 설명합니다.

NEWNAL Inc. · 2026

목차

개요	3
기업이 직면한 네 가지 문제	3
뉴날의 해결 방식	3
기업의 이점	3
검증	3
1. 용어 정의	4
2. 퍼스널 데이터 노드	4
2.1 정의	4
2.2 "고객이 소유한다"의 뜻	5
2.3 노드의 구성	5
3. 데이터 스피어와 서비스 에이전트 노드	6
3.1 데이터 스피어	6
3.2 서비스 에이전트 노드	6
3.3 전체 구조와 데이터 흐름	7
3.4 기업 쪽에서 본 변화	7
4. 신원과 키	8
5. 공개 원장 — 무엇을 기록하고, 왜 InfraBlockchain인가	8
5.1 원장에 기록되는 것	8
5.2 왜 공개 원장이고, 왜 InfraBlockchain인가	9
6. 보안	9
7. 파트너 기업의 역할과 도입	10
7.1 도입 경로	10
7.2 기존 회원 기능의 대체	10
8. 기존 인프라와 규제	11
9. 자주 묻는 질문	11

개요

기업이 직면한 네 가지 문제

문제	내용
① 개인화에는 개인 데이터가 필요하다	AI가 고객을 알려면 고객의 데이터가 필요합니다. 데이터가 없는 AI는 모든 고객에게 같은 답을 합니다.
② 모으면 책임이 생긴다	고객 데이터를 자사 서버에 모으는 순간 보관·유출·규제의 책임이 생깁니다. 열람 권한을 가진 내부자와 계정을 탈취한 공격자는 보안 투자로 막기 어렵습니다.
③ 자기 데이터만으로는 부족하다	기업 서버에는 자기 서비스에서 생긴 데이터만 있습니다. 고객의 건강·생활·소비를 함께 아는 서비스는 어느 한 기업도 만들 수 없고, 제휴로 데이터를 받으면 전송과 보관의 책임이 다시 생깁니다.
④ 기업마다 같은 인프라를 구축한다	수집 체계, 저장소, 보안 인력, 동의 관리, 유출 대응을 기업마다 각자 구축합니다. 같은 고객의 데이터를 위해 기업 수만큼 같은 인프라가 반복됩니다.

네 문제의 원인은 하나입니다. 데이터가 **기업 단위**로 모인다는 것입니다. 기업 단위 구조에서는 개인화를 위해 데이터를 더 모을수록 보관 책임도 함께 커집니다.

뉴날의 해결 방식

뉴날은 데이터가 모이는 단위를 기업에서 **개인**으로 바꿨습니다. 고객 한 사람마다 **퍼스널 데이터 노드**라는 개인별 클라우드 서버가 있고, 고객의 데이터는 이 노드에 모입니다. 기업은 고객에게 **데이터 스피어**라는 공유 범위를 제안하고, 고객이 허락한 스피어의 데이터만 기업의 **서비스 에이전트 노드**로 동기화됩니다. 서비스 기능과 AI 에이전트는 서비스 에이전트 노드에서 실행되고, 기업의 기존 시스템과 웹·앱은 그 결과를 API로 받습니다. 두 노드는 모두 기밀 컴퓨팅 환경에서 공개된 소스코드로 실행됩니다. 따라서 클라우드 인프라를 운영하는 주체(뉴날 포함)도 처리 중인 개인 데이터에 접근할 수 없습니다. 어떤 노드가 무엇을 허락했고 누가 언제 접근했는지에 대한 검증 정보는 뉴날 밖의 공개 원장(InfraBlockchain)에 기록됩니다.

기업의 이점

첫째, 자기가 모은 데이터가 아니라 고객이 허락한 데이터 전체로 서비스를 만듭니다. 기존 데이터는 그대로 유지되고, 다른 서비스·기관·디바이스가 노드에 기록한 데이터 가운데 고객이 허락한 부분이 더해집니다. 기업이 직접 수집하는 방식으로서는 확보할 수 없는 범위입니다.

둘째, 개인 데이터 수집·보관 인프라를 기존 시스템에서 떨어냅니다. 개인 데이터의 수집·보관·동의 관리·접근 통제는 퍼스널 데이터 노드와 서비스 에이전트 노드가 담당합니다. 기업의 기존 시스템은 퍼스널 데이터 노드에 직접 연결되지 않고 서비스 에이전트 노드의 API만 호출합니다. 서비스 에이전트 노드는 뉴날이 관리형 서비스(Managed Service)로 구축·운영하거나, 기업이 뉴날의 공개 프레임워크로 직접 구축합니다.

검증

뉴날이 개발·운영한 백신 패스 COOV를 대한민국 4,300만 명이 사용했고, 하루 최대 3,000만 건을 검증했으며, 2억 6천만 개의 DID를 발급했습니다. 원본은 발급 기관의 서버에 남았고 개인의 디바이스에는 검증 가능 자격증명만 저장되었습니다. COOV가 국가 규모로 검증한 것은 DID, 검증 가능 자격증명, 공개 원장입니다. 퍼스널 데이터 노드와 서비스 에이전트 노드는 그 위에 더해진 구성 요소이며 현재 뉴날 aios에서 운영 중입니다. 등록·출원 특허는 90건 이상입니다.

1. 용어 정의

용어	뜻
퍼스널 데이터 노드 (Personal Data Node)	고객 한 사람마다 하나씩 할당되는 개인별 클라우드 서버입니다. 고객의 데이터를 암호화해 보관하고, 허락한 스피어 범위로만 데이터를 제공하며, 접근 기록을 남깁니다. 본 문서의 '노드'는 퍼스널 데이터 노드를 뜻합니다.
서비스 에이전트 노드 (Service Agent Node)	스피어 접근 권한을 가진 서버입니다. 스피어에 참여한 고객 노드들의 레코드를 동기화해 서비스용 데이터 뷰를 만들고, 서비스 기능과 AI 에이전트를 실행해 API로 제공합니다.
데이터 스피어	스피어 소유자가 정의한 데이터 서식과 용도 단위의 공유 범위입니다. 고객이 참여를 허락하면 노드 안에 그 스피어의 저장소가 생깁니다. 한 기업이 용도별로 여러 스피어를 둘 수 있습니다.
스피어 소유자	스피어를 개설하고 데이터 서식·API 계약·참여 자격을 정하며, 서비스 에이전트 노드에 스피어 접근 자격증명을 발급하는 주체입니다. 기업이 소유자가 될 수 있습니다.
스피어 접근 자격증명 (Sphere Access Credential)	스피어 소유자가 서비스 에이전트 노드에 발급하는 증명입니다. 노드는 이 증명을 검증한 뒤 해당 스피어의 데이터만 제공합니다.
데이터 뷰	서비스 에이전트 노드가 참여 고객들의 스피어 레코드를 모아 서비스 구현에 맞게 구성한 데이터입니다. 기존 방식의 고객 데이터베이스가 있던 자리에 해당합니다.
DID	실명이나 회사 계정 대신 사람·서비스를 가리키는 분산 식별자입니다. DID의 키 목록과 노드의 접근 주소는 공개 원장의 DID Document에 등록됩니다.
검증 가능 자격증명 (Verifiable Credential)	기관·기업이 개인에게 발급하고 누구나 진위를 검증할 수 있는 증명입니다. 원본은 발급 기관에 남고 증명만 노드에 저장됩니다. 서비스 에이전트 노드에 발급되는 스피어 접근 자격증명과는 다른 것입니다.
공개 원장 (InfraBlockchain)	DID Document, 스피어 정의, 정산 토큰과 접근 기록의 검증 정보가 기록되는 퍼블릭 블록체인입니다. 가상화폐 발행 없이 동작하고 데이터 원본은 저장하지 않습니다.
기밀 컴퓨팅 환경	메모리까지 암호화되어 클라우드 관리자도 소프트웨어 접근으로는 내용을 열람할 수 없는 실행 영역입니다. 실행 중인 코드가 공개된 코드와 같은지 외부에서 검증할 수 있습니다(원격 증명).
역로그인 (Reverse Login)	서비스가 고객의 노드에 스피어 참여를 요청하고 고객이 승인하는 방식입니다. 고객이 서비스에 로그인해 데이터를 넘기는 기존 방향과 반대입니다.

2. 퍼스널 데이터 노드

2.1 정의

퍼스널 데이터 노드는 고객 한 사람마다 하나씩 할당되는 **개인별 클라우드 서버**입니다. 노드는 고객의 데이터를 암호화해 보관하고, 고객이 허락한 데이터 스피어의 범위로만 서비스에 데이터를 제공하며, 모든 접근을 기록합니다. 노드는 기밀 컴퓨팅 환경에서 실행되고, 회사 계정이 아니라 고객의 DID로 공개 원장에 등록됩니다. 노드의 통제권은 고객에게 있습니다.

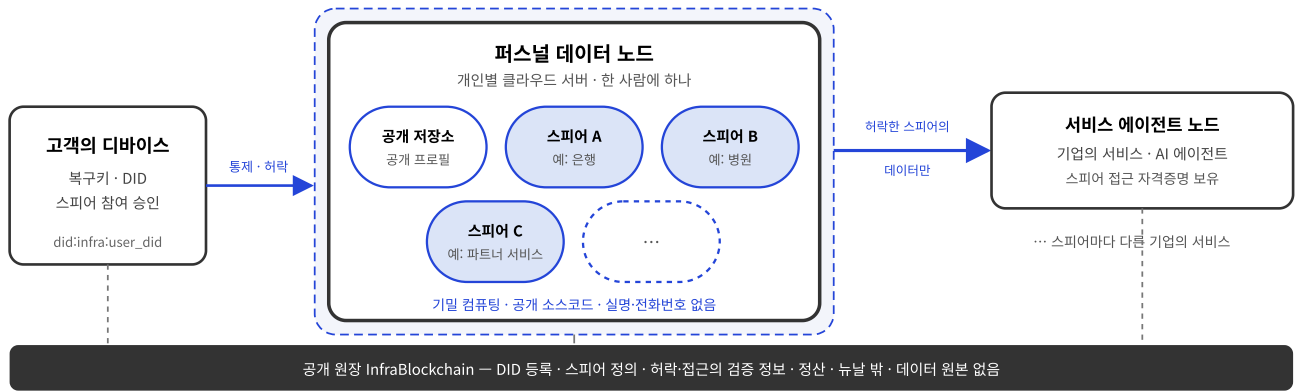


그림 1. 고객의 디바이스가 노드를 통제하고 스피어 참여를 승인하며, 노드는 허락한 스피어의 데이터만 해당 서비스에 제공합니다. 검증 정보는 뉴날 밖의 공개 원장에 남습니다.

노드는 고객마다 전용 물리 서버를 두는 것이 아닙니다. 하나의 물리 서버에 논리적으로 분리된 여러 노드가 실행되며, 데이터 저장소·접근 정책·접근 기록·정산이 DID 단위로 분리됩니다. 노드는 데이터가 담기는 공간이 아니라 고객의 DID로 동작하는 서버이고, 데이터베이스와 클라우드는 노드가 사용하는 부품입니다.

2.2 "고객이 소유한다"의 뜻

노드는 클라우드에서 실행되고, 고객의 디바이스에는 복구키와 소량의 비공개 데이터만 있습니다. 본 문서에서 소유는 저장 위치가 아니라 다음 세 조건을 뜻합니다.

조건	내용
등록	노드는 고객의 DID로 공개 원장에 등록됩니다. 어느 회사의 계정 체계에도 속하지 않습니다.
키	노드의 서명키와 데이터 키를 교체·폐기할 수 있는 최상위 복구키는 고객에게 있습니다. 뉴날, 클라우드 운영자, 파트너 기업은 이 권한이 없습니다.
이동	고객은 공개 원장에 등록된 노드의 접근 주소를 바꿔 노드를 다른 클라우드나 운영자로 옮길 수 있습니다. 노드의 소재지를 관할별로 둘 수 있습니다.

2.3 노드의 구성

구성	내용	기술
보관	고객의 데이터를 노드별 데이터 키로 암호화해 보관합니다. 저장소는 공개 저장소와 스피어별 저장소로 나뉩니다. 데이터 키의 보관과 제공 방식은 4장에서 설명합니다.	노드별 데이터 키
실행	공개된 노드 서버 코드가 기밀 컴퓨팅 환경에서 실행됩니다. 클라우드 관리자도 내용을 열람하지 못하고, 실행 중인 코드가 공개 코드와 같은지 외부에서 검증할 수 있습니다.	기밀 컴퓨팅, 원격 증명, 오픈 소스
신원	실명·계정이 아니라 DID로 등록됩니다. 식별·연락·인증을 DID가 담당하므로 노드의 시스템 식별자에 실명·전화번호가 없습니다.	DID, DID Document
키	서명키와 데이터 키는 서버측 HSM에, 두 키를 교체할 수 있는 복구키는 고객의 디바이스에 있습니다. 자세한 내용은 4장에서 설명합니다.	HSM, 디바이스 보안 영역, 다중 키 DID
접근 통제	검증을 통과한 서비스 에이전트 노드에만, 고객이 허락한 스피어 범위의 데이터를 제공합니다. 허락을 철회하면 동기화가 중단됩니다.	스피어 정의(공개 원장), 원격 증명 검증
기록	허락과 접근을 노드에 기록하고 고객에게 통보합니다. 기록의 검증 정보는 공개 원장에 앵커링됩니다.	노드 로그, 공개 원장 앵커링

구성	내용	기술
검증 가능 자격증명 수신	병원·기관·기업이 개인에게 발급한 검증 가능 자격증명이 노드에 전달됩니다. 원본은 기관에 남습니다.	Verifiable Credential (COOV 방식)
통신	노드·디바이스·서비스 에이전트 노드 사이의 연락은 DID로 상호 인증된 종단간 암호화 통신입니다.	DID 기반 종단간 암호화
정산	어떤 스피어가 어떤 데이터를 사용했는지 DID 단위로 집계되어 사용료와 수익이 정산됩니다.	공개 원장 토큰 계약

이 구조는 네 가지가 한 노드에서 함께 성립할 때만 성립합니다. **기밀 실행과 공개 코드**가 없으면 운영자가 내용을 열람할 수 있어 노드는 회사 서버의 다른 이름이 됩니다. **복구키가 고객에게** 없으면 서명키와 데이터 키를 쥔 운영자가 노드의 주인을 대신합니다. **DID 등록**이 없으면 노드는 실명이나 회사 계정에 묶여 한 회사의 자산이 됩니다. **뉴날 밖의 공개 원장**이 없으면 기록이 바뀌지 않았다는 것은 뉴날의 약속으로만 남습니다. 뉴날은 이 네 조건을 한 구조로 묶어 운영합니다.

3. 데이터 스피어와 서비스 에이전트 노드

3.1 데이터 스피어

데이터 스피어는 스피어 소유자가 정의한 공유 범위입니다. 소유자는 스피어의 데이터 서식, API 계약, 참여 자격을 정해 공개 원장에 등록합니다. 고객이 참여를 허락하면 고객의 노드 안에 그 스피어의 저장소가 생기고, 고객의 노드와 서비스가 거기에 레코드를 기록합니다. **기업이 서비스를 개발하기 위해 다수의 데이터 스피어를 생성할 수 있습니다.** 서비스 하나를 만들 때에도 프로필 스피어, 활동 스피어, 결제 스피어처럼 용도별로 스피어를 나눌 수 있고, 고객은 스피어 단위로 허락과 철회를 합니다.

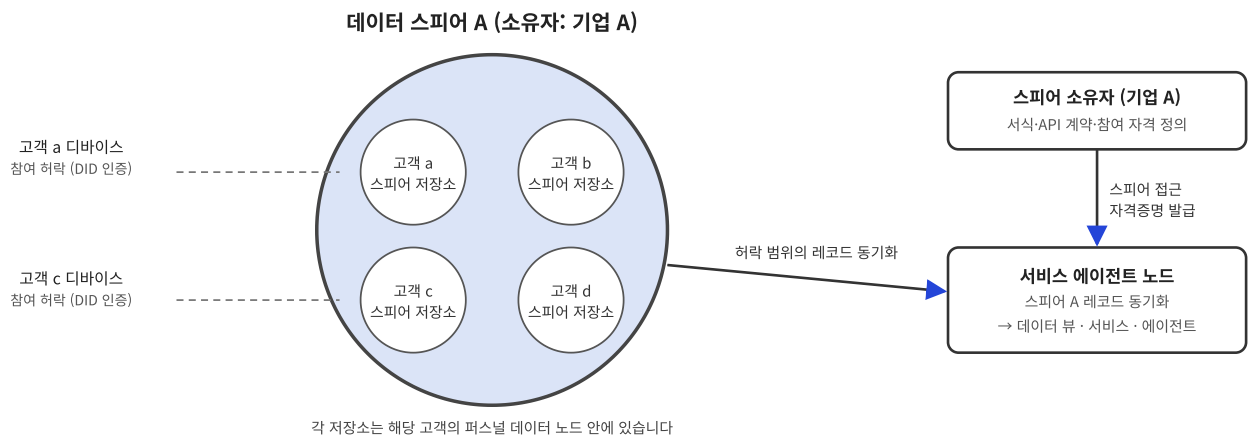


그림 2. 데이터 스피어는 여러 고객의 노드에 걸친 공유 범위입니다. 스피어 소유자가 발급한 접근 자격증명을 가진 서비스 에이전트 노드만 그 범위의 레코드를 동기화합니다.

3.2 서비스 에이전트 노드

서비스 에이전트 노드는 스피어 소유자로부터 접근 권한을 얻어, 스피어에 참여한 퍼스널 데이터 노드들의 레코드를 **동기화**하고, 서비스 구현에 필요한 **데이터 뷰**를 만들며, 실제 서비스 기능과 AI 에이전트가 **실행**되는 서버입니다. 서비스 기능은 API 형태로 기업의 내부 시스템과 웹·앱 클라이언트에 제공됩니다.

서비스와 에이전트는 퍼스널 데이터 노드 안에서 실행되지 않습니다. 고객이 허락한 스피어의 데이터는 퍼스널 데이터 노드에서 서비스 에이전트 노드로 공유되고, 그곳에서 처리됩니다. 따라서 서비스 에이전트 노드는 퍼스널 데이터 노드와 같은 수준으로 보호됩니다.

퍼스널 데이터 노드는 레코드를 보내기 전에 두 가지를 확인합니다. ① 스피어 소유자가 발급한 스피어 접근 자격증명. ② 그 서비스 에이전트 노드가 공개된 코드를 기밀 컴퓨팅 환경에서 실행하고 있다는 원격 증명. 둘 중 하나라도 확인되지 않으면 노드는

데이터를 보내지 않습니다. 이 검증은 뉴날이 운영하는 서비스 에이전트 노드와 기업이 자체 구축한 서비스 에이전트 노드에 똑같이 적용됩니다. 고객이 허락을 철회하면 동기화가 중단되고 데이터 뷰에서 해당 고객의 레코드가 제거됩니다.

서비스 에이전트 노드는 두 방식으로 마련됩니다. **뉴날 관리형 서비스**: 뉴날이 기밀 컴퓨팅 환경에 서비스 에이전트 노드를 구축·운영하고, 기업은 데이터 뷰와 서비스 로직만 정의합니다. **기업 자체 구축**: 기업이 뉴날의 공개 프레임워크로 자사 클라우드에 구축합니다. 이 경우 기업이 담당하는 것은 그 환경의 운영이지 데이터에 대한 접근 권한이 아닙니다. 어느 쪽이든 기업의 기존 시스템은 퍼스널 데이터 노드에 직접 연결되지 않고 서비스 에이전트 노드의 API만 호출하므로, 기존 시스템에 개인 데이터 수집·관리 체계를 두지 않아도 됩니다.

3.3 전체 구조와 데이터 흐름

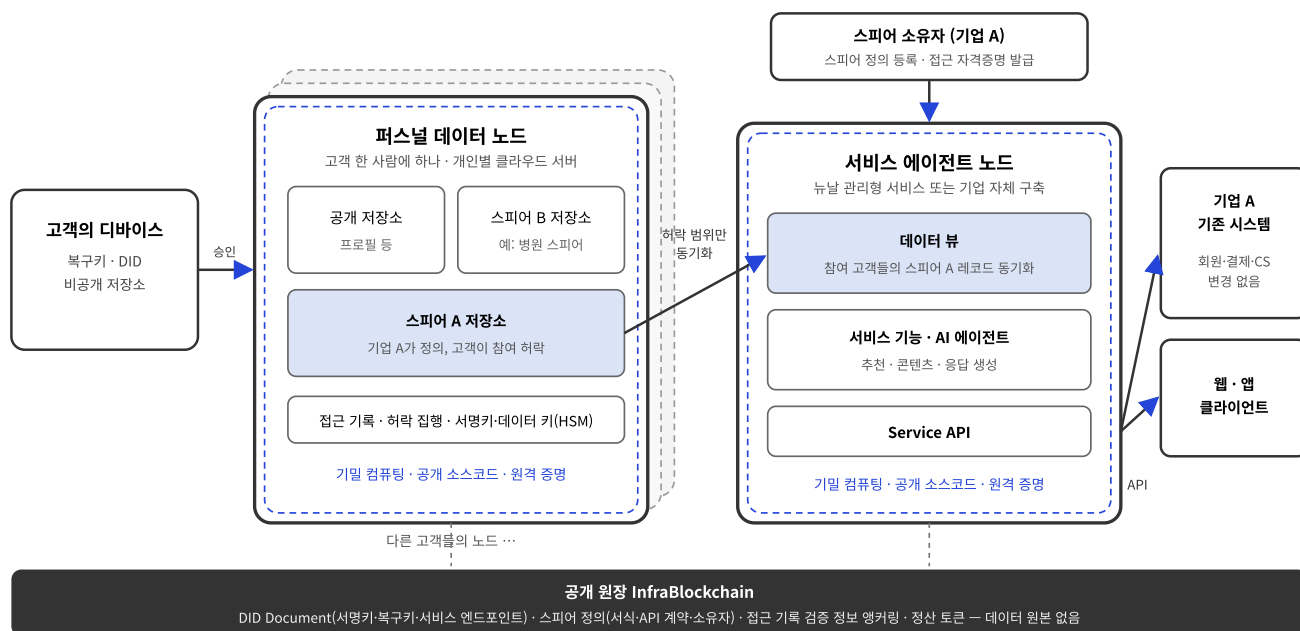
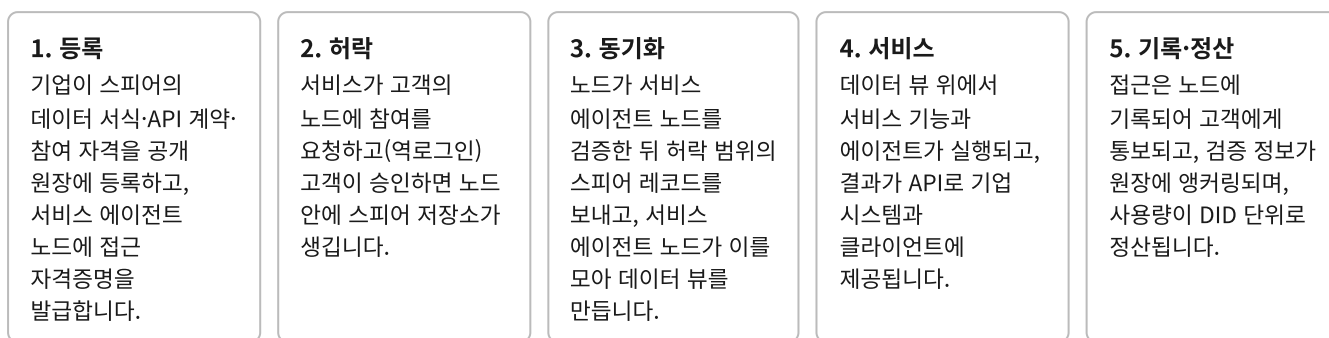


그림 3. 고객은 디바이스에서 스피어 참여를 승인하고, 서비스 에이전트 노드는 허락된 스피어의 레코드만 동기화해 서비스를 실행하며, 기업의 기존 시스템과 클라이언트는 API로 결과를 받습니다. 검증 정보는 뉴날 밖의 공개 원장에 남습니다.



3.4 기업 쪽에서 본 변화

기존 방식에서 고객 데이터베이스가 있던 자리에 서비스 에이전트 노드의 데이터 뷰가 있습니다. 데이터 뷰는 기업이 정의한 스피어에 참여한 고객들의 데이터로 구성됩니다. 여기에는 두 종류가 들어갑니다. 하나는 기업이 현재 보유한 데이터 가운데 고객의 노드 안 스피어 저장소에 기록한 부분입니다. 다른 하나는 다른 서비스·기관·디바이스가 노드에 기록한 데이터 가운데 고객이 이 스피어에 추가로 허락한 부분입니다. 기존 데이터베이스의 데이터는 스피어 저장소에 기록하기 전까지는 데이터 뷰에 포함되지 않으며, 기업은 서비스 단위로 필요한 만큼만 옮깁니다. 개인 데이터는 기업의 기존 시스템이 아닌 서비스 에이전트 노드에 있으므로, 기존 시스템은 개인 데이터를 수집·보관하지 않고 API 결과만 다룹니다. 기업의 고객 데이터베이스는 사라지는 것이 아니라 보호된 데이터 뷰로 바뀌고, 데이터의 범위는 확장됩니다.

4. 신원과 키

결론부터 말하면, 뉴날도 클라우드 운영자도 노드의 데이터를 열 수 없고, 노드의 주인을 바꿀 수 있는 권한은 고객에게만 있습니다. 이것을 가능하게 하는 것이 키의 배치입니다. 하나의 DID에는 권한이 다른 여러 키가 등록되고, 키 목록과 노드의 접근 주소는 공개 원장의 DID Document에 기록됩니다. 서명키와 데이터 키는 노드가 동작하는 서버 쪽 HSM(Hardware Security Module)에, 그 두 키를 교체할 수 있는 복구키는 고객 쪽에 있습니다.

키	위치와 역할	보장하는 것
서명키	노드가 클라우드에서 고객 대신 서명하는 데 쓰는 키입니다. 서버측 HSM에 보관되어 반출되지 않고, 서명에만 사용됩니다.	노드가 디바이스 없이도 동작합니다. 키 원문이 서버 메모리나 디스크에 노출되지 않습니다.
데이터 키	노드의 저장 데이터를 암호화하는 노드별 키입니다. 서명키와 같이 서버측 HSM이 보관하며, 레코드의 실제 암호화와 복호화는 노드 실행 환경 안에서 이 키로 처리됩니다. HSM은 원격 증명을 통과한 노드 실행 환경에만 키를 제공하고, 관리자 권한으로는 키를 꺼낼 수 없습니다. 고객은 복구키로 데이터 키를 교체할 수 있습니다.	저장 데이터는 증명된 노드 실행 환경 안에서만 복호화됩니다. 디스크 사본을 확보해도 내용을 읽을 수 없고, 키가 의심되면 고객이 교체합니다.
복구키	노드가 사용 중인 서명키와 데이터 키를 교체·폐기할 수 있는 최상위 권한의 키입니다. 고객의 디바이스 보안 영역에 저장되고, 고객이 백업할 수 있습니다. 여러 개를 만들어 일부는 신뢰할 수 있는 복구키 보관 서비스에 맡길 수 있습니다.	노드의 주인을 바꿀 수 있는 권한은 고객에게만 있습니다. 운영자 교체와 노드 이동이 가능합니다.
복구키 보관 서비스	고객이 맡긴 복구키를 고객 단위로 분리해 보관하고, 등록 시 설정한 본인 확인을 통과한 고객에게만 복구 절차를 제공합니다. 관리자 권한으로는 키를 조회할 수 없습니다.	디바이스와 백업을 모두 잃어도 DID를 복구할 수 있습니다. 한 번의 침입으로 여러 고객의 키를 얻는 방법이 없습니다.

디바이스를 잃어도 노드는 클라우드에서 계속 동작합니다. 고객은 백업한 복구키나 복구키 보관 서비스로 새 디바이스에 복구키를 등록하고, 필요하면 서명키와 데이터 키를 교체합니다. 미성년 고객의 복구에는 보호자가 참여합니다.

5. 공개 원장 — 무엇을 기록하고, 왜 InfraBlockchain인가

5.1 원장에 기록되는 것

기록	원장에 직접 기록	노드에 보관, 검증 정보만 앵커링
등록 (누구의 노드인가)	DID Document: 서명키, 복구키, 서비스 엔드포인트	—
스피어 정의	소유자 DID, 데이터 서식, API 계약, 참여 자격	—
허락과 접근	—	어떤 스피어에 참여했고 누가 언제 무엇을 동기화했는지는 노드에 기록되고, 그 기록의 해시가 주기적으로 원장에 앵커링됩니다.
정산	토큰 계약: 사용료·수익의 이전	스피어별 사용량 집계는 노드에서 산출됩니다.

접근 기록의 원문을 원장에 올리지 않는 이유는 두 가지입니다. 어느 DID가 어떤 서비스와 연결되었는지 자체가 민감한 정보이고, 수천만 명의 접근 기록을 매건 기록하는 것은 어떤 원장도 감당하기 어렵기 때문입니다. 앵커링된 검증 정보만으로도 기록이 사후에 바뀌지 않았음을 뉴날을 거치지 않고 확인할 수 있습니다.

5.2 왜 공개 원장이고, 왜 InfraBlockchain인가

등록·스피어 정의·검증 정보는 세 조건을 만족해야 합니다. 뉴날 단독으로 바꿀 수 없어야 하고, 고객·기업·감사인이 뉴날을 거치지 않고 검증할 수 있어야 하며, 서로 믿지 않는 여러 기업이 같은 기록을 공유해야 합니다. 뉴날이 소유한 데이터베이스는 첫째와 둘째를, 어느 한 기업의 장부는 셋째를 만족하지 못합니다.

InfraBlockchain의 특성	내용	결과
가상화폐를 발행하지 않는다	네트워크 운영에 자체 가상화폐가 없습니다. 수수료는 법정화폐에 연동된 토큰으로 지불됩니다.	수수료가 안정적이고 정부·금융 기관이 사용할 수 있습니다. 대한민국 정부가 COOV를 채택할 수 있었던 조건입니다.
퍼블릭이다	누구나 기록을 조회하고 검증할 수 있습니다.	고객, 기업, 감사인, 규제 기관이 뉴날을 거치지 않고 확인합니다.
Proof-of-Transaction	채굴이나 보유량이 아니라 실제 서비스 트랜잭션 처리 실적으로 블록 생성자를 정합니다. 블록 생성자는 신원이 확인된 복수의 서비스 제공자입니다.	책임 주체가 분명하고, 채굴에 따른 전력 소모가 없으며, 뉴날 단독으로 기록을 바꿀 수 없습니다.
데이터 원본을 기록하지 않는다	원장에는 등록·정의·검증 정보·정산만 있습니다.	삭제권과 충돌하지 않고, 원장이 유출되어도 데이터가 없습니다.
국가 규모에서 운영되었다	COOV의 원장으로 국가 규모 서비스를 운영했습니다 (개요의 검증 참조).	성과와 안정성이 운영 기록으로 증명됩니다.

6. 보안

공격 경로	회사 서버 방식	퍼스널 데이터 노드 + 서비스 에이전트 노드
내부 직원이 권한으로 유출	정당한 권한으로 전체 고객 데이터를 조회하므로 보안 시스템이 막지 못합니다.	고객 데이터를 열람할 수 있는 운영자 권한이 없습니다. 뉴날의 관리자 권한은 노드를 운영하는 권한이지 내용을 열람하는 권한이 아닙니다.
외부 공격자가 직원 계정 탈취	탈취한 권한으로 데이터베이스에 접근합니다.	탈취할 계정에 열람 권한이 없습니다. 파트너 기업 직원도 스피어 범위 밖의 데이터는 서비스 에이전트 노드에 존재하지 않아 접근할 수 없습니다.
외부 공격자가 서버 침입	수백만 명의 데이터가 실명·연락처와 함께 한 번에 복사됩니다.	데이터는 노드별로 암호화되어 있고 복호화 키는 서버 밖으로 나오지 않습니다. 시스템 식별자는 DID이고, 서비스 에이전트 노드에는 해당 스피어 범위의 데이터만 있습니다.
클라우드 관리자가 서버 내부 열람	최고 권한 관리자가 메모리와 디스크를 열람합니다.	소프트웨어 접근으로는 열람하지 못하고, 디스크 사본으로는 내용을 읽을 수 없습니다(4장). 실행 중인 메모리에 대한 물리적 공격은 남으며, 뉴날은 하드웨어 제조사의 보안 업데이트를 적용하고 한 실행 환경이 다루는 범위를 제한해 영향을 줄입니다.
운영자가 공개하지 않고 코드를 변경	외부에서 알 수 없습니다.	노드 서버 코드가 공개되어 있고, 실행 중인 코드가 공개 코드와 같다는 증거(원격 증명)를 하드웨어 제조사의 증명 체계로 제3자가 검증합니다.
파트너 서비스가 범위 밖 접근	허락 범위는 약속으로만 지켜집니다.	스피어 정의가 공개 원장에 있고, 노드는 접근 자격증명이 가리키는 스피어 밖의 데이터를 전달하지 않습니다. 범위 안 접근도 기록되어 통보됩니다.

뉴날이 유출 사고를 막는 방법은 침입을 완전히 차단하는 것이 아닙니다. 침입해도 대규모로 얻기 어렵고, 얻은 데이터가 시스템 식별자인 DID 외에는 사람과 연결되지 않게 만드는 것입니다. 스피어 안에 기업이 이름이나 연락처를 넣었다면 그 데이터는 스피어 범위 안에서 보호될 뿐 식별 불가능해지는 것은 아닙니다. 그래서 뉴날은 민감도가 높은 데이터는 가능한 한 데이터 스피어에 저장하지 않도록 권장합니다.

남는 위험은 세 가지입니다. 특정 고객의 디바이스를 표적으로 공격하면 그 고객의 복구기가 노출될 수 있습니다. 기업이 자체 구축한 서비스 에이전트 노드의 가용성과 운영은 기업의 책임입니다(데이터 접근 통제는 3.2의 검증으로 동일하게 적용됩니다). 결제 대행사와 판매 채널에 남는 결제 정보는 노드 구조 밖입니다.

7. 파트너 기업의 역할과 도입

파트너 기업의 역할	파트너 기업이 담당하지 않는 업무	파트너 기업의 이점
서비스 기획과 운영, 브랜드·판매·가격·상품 구성	개인 데이터 수집·보관 인프라 구축	고객이 허락한 데이터 전체로 만드는 개인화 서비스
스피어 설계와 등록 (뉴날이 함께 합니다)	로그인·본인 확인·알림 인프라 구축	기존 시스템에 개인 데이터가 쌓이지 않음
데이터 뷰와 서비스 로직, 콘텐츠·추천·AI 응답의 설계	유출 대응 체계와 보안 인력 (관리형 서비스 사용 시)	서비스 시작 전에 데이터를 확보할 필요 없음
고객에게 허락을 요청하는 화면과 문구	동의 관리·접근 기록 체계 구축	DID 단위의 자동 정산, 판매·구독 수익
결제 (현재 사용하는 채널 그대로)	—	다른 기업이 이미 연결한 고객의 노드에 스피어 등록만으로 시작

7.1 도입 경로

1. 스피어 설계 새 서비스에 필요한 데이터를 용도별 스피어로 나누어 서식과 API 계약을 정의하고 공개 원장에 등록합니다. 뉴날이 설계를 함께 합니다.	2. 서비스 에이전트 노드 준비 뉴날 관리형 서비스를 신청하거나, 공개 프레임워크로 자체 구축합니다. 데이터 뷰와 서비스 로직을 구현하고 API를 정의합니다.	3. 기존 시스템 연결 기존 회원에게 "우리 회원이다"라는 검증 가능 자격증명을 발급해 고객의 노드와 연결하고, 새 서비스에 필요한 기존 데이터가 있으면 해당 고객의 스피어 저장소에 기록합니다. 기존 시스템은 서비스 에이전트 노드의 API를 호출합니다. 회원 체계·결제·CS는 그대로입니다.
---	--	--

세 단계만으로 새 서비스를 시작할 수 있습니다. 기존 데이터베이스의 개인 데이터를 스피어 저장소로 옮기는 범위와 시점, 그리고 옮긴 뒤 서버의 사본을 삭제할지는 기업이 서비스 단위로, 기업의 일정에 맞춰 선택합니다. 옮기지 않은 데이터는 데이터 뷰에 포함되지 않고, 옮긴 만큼 기존 시스템의 보관 책임과 인프라 비용이 줄어듭니다.

7.2 기존 회원 기능의 대체

기능	기존 방법	노드 구조의 방법
로그인·본인 확인	아이디, 비밀번호, 전화번호 인증	DID와 디바이스가 증명합니다. 기존 회원은 검증 가능 자격증명으로 연결됩니다.
연락·알림	전화번호, 이메일, 앱 푸시	DID로 상호 인증된 암호화 통신입니다. 고객이 허락한 상대만 연결됩니다.
구독·자격 확인	계정에 결제 이력을 연결	"해당 DID의 구독은 유효하다"는 검증 가능 자격증명만 검증합니다.

기능	기존 방법	노드 구조의 방법
개인화 · 추천	서버의 이용자 프로필과 결합	서비스 에이전트 노드의 데이터 뷰에서 허락 범위의 데이터로 결합합니다.
결제 · 환불 · CS	계정 조회	현재 사용하는 판매 채널과 결제 대행사가 계속 담당합니다.
본실 · 복구	주민번호, 전화번호로 본인 확인	고객이 주도하는 복구키 절차입니다. 미성년 고객은 보호자가 참여합니다.

8. 기존 인프라와 규제

노드는 클라우드, AI 모델, 운영체제를 대체하지 않습니다. 클라우드는 노드를 실행하고, AI 모델은 서비스 에이전트 노드 안에서 허락 범위의 맥락으로 동작하며, 뉴날 aios는 전용 디바이스에는 운영체제로, 기존 디바이스에는 계층으로, 디바이스가 없는 서비스에는 노드 실행 계층으로 탑재됩니다. 노드 기반 서비스와 AI 에이전트의 이용이 늘수록 클라우드와 AI 모델의 사용량도 함께 늘어납니다. 뉴날은 기존 인프라 회사의 경쟁자가 아니라 사용자입니다.

규제가 요구하는 것	노드 구조의 대응
최소 수집 (GDPR 제5조)	시스템 식별자로 실명·연락처를 수집하지 않고, 스피어 단위로 필요한 데이터만 공유합니다.
동의만큼 쉬운 철회 (제7조)	스피어 단위로 철회하면 동기화가 중단되고 데이터 뷰에서 제거됩니다.
설계 단계의 프라이버시 (제25조)	접근 통제가 구조에 내장되어 있습니다.
삭제권 (제17조) · 이동권 (제20조)	원본은 고객의 노드에 있고, 고객은 노드 전체를 다른 클라우드로 옮길 수 있습니다.
열람권 (제15조)	모든 접근이 기록되고 본인에게 통보됩니다.
국외 이전 제한 (제5장)	노드와 서비스 에이전트 노드의 소재지를 관할별로 둘 수 있습니다.
아동 보호 (제8조 · COPPA)	아동의 식별자와 연락처를 수집하지 않으며, 결제와 동의의 주체는 보호자입니다.

위 표는 법적 판단을 대신하지 않습니다. 파트너 기업의 처리자·수탁자 지위를 포함한 관할별 세부 적용은 파트너 기업의 법무 검토와 함께 확정하며, 뉴날은 필요한 기술 자료를 제공합니다.

9. 자주 묻는 질문

Q1. 노드는 데이터베이스와 무엇이 다른가? 데이터베이스는 소유 회사의 계정을 기준으로 접근을 통제합니다. 노드는 고객의 DID와 스피어 허락을 기준으로 통제하고, 허락 범위 밖의 데이터는 전달하지 않습니다. 데이터베이스와 클라우드는 노드 안에서 사용되는 부품입니다.

Q2. 회원 DB가 없으면 고객 수와 활성 고객을 어떻게 아는가? 기업의 스피어에 참여한 고객 전원이 기업의 고객입니다. 고객 수·활성 여부·구독 상태는 서비스 에이전트 노드에서 DID 단위로 집계됩니다. 집계의 기준은 DID이므로, 기업이 스피어에 실명이나 연락처를 포함하지 않는 한 고객을 식별하는 명단은 생기지 않습니다.

Q3. 고객 수백만 명이면 노드도 수백만 개인데 비용은? 노드는 고객마다 전용 서버가 아니라 기밀 VM 안에서 논리적으로 분리된 클라우드 서버입니다. 비용은 활성 고객 수에 비례하며, 기업이 기존 시스템의 보관·보안·유출 대응에 지출하던 비용이 줄어듭니다.

Q4. 서비스 에이전트 노드에 데이터가 모이면 결국 기업 서버와 같지 않은가? 세 가지가 다릅니다. 고객이 스피어 단위로 허락한 데이터만 있습니다. 운영자도 열람할 수 없습니다. 철회하면 제거됩니다. 기업의 기존 시스템에는 개인 데이터가 쌓이지 않습니다.

Q5. 스피어 소유자인 기업은 참여 고객의 데이터를 모두 열람할 수 있는가? 스피어 소유자의 권한은 스피어를 정의하고 참여 자격과 접근 자격증명을 관리하는 것입니다. 고객 데이터는 고객이 허락한 범위에서 서비스 에이전트 노드로만 동기화되며, 그 밖의 경로로 열람하는 권한은 없습니다.

Q6. 고객이 디바이스를 분실하면? 노드는 클라우드에서 계속 동작합니다. 고객은 백업한 복구키나 복구키 보관 서비스로 DID를 복구하고 새 디바이스를 등록합니다. 미성년 고객은 보호자가 참여합니다.

Q7. 사고가 발생하면 누가 책임지는가? 퍼스널 데이터 노드와 공개 원장, 그리고 관리형 서비스로 제공하는 서비스 에이전트 노드의 운영은 뉴날의 책임이며, 뉴날은 이행을 외부 감사로 증명합니다. 기업이 자체 구축한 서비스 에이전트 노드의 운영은 기업의 책임입니다.

Q8. 수사기관이 데이터를 요구하면? 뉴날이 제출할 수 있는 것은 암호화된 저장소와 접근 기록입니다. 뉴날의 관리자 권한으로는 데이터 키를 꺼낼 수 없으므로(4장), 저장소의 내용을 열람해 제출할 수 없습니다. 데이터의 내용을 제공할지는 노드의 주인인 고객이 결정합니다.

Q9. 블록체인이면 느리고 비싸지 않은가? 원장에는 등록·정의·검증 정보·정산만 기록되고 접근 기록 원문과 데이터는 노드에 있습니다. InfraBlockchain은 가상화폐 없이 동작해 수수료가 안정적이며, COOV에서 국가 규모로 운영되었습니다.

Q10. 고객이 사연이나 후기에 자기 이름을 기재하면? 시스템이 막을 수 없습니다. 뉴날의 주장은 "식별이 불가능하다"가 아니라 "기록을 실제 인물과 연결하는 실명·연락처·계정이 시스템 식별자에 없다"입니다.

문의 파트너십 문의 partner@newnal.com

고객 데이터는 고객의 퍼스널 데이터 노드에 있습니다. 파트너 기업은 고객이 허락한 데이터 스피어로 서비스를 만들고, 기존 시스템에 개인 데이터를 두지 않습니다. 노드와 공개 원장은 뉴날이 운영하고 책임집니다.