都市をAI化するアーキテクチャ

SOMS — Symbiotic Office Management System

各建物にローカルLLM+GPUを配置し、都市を自律的に思考する空間に変える。
Core Hub アーキテクチャの Phase 0 実証。

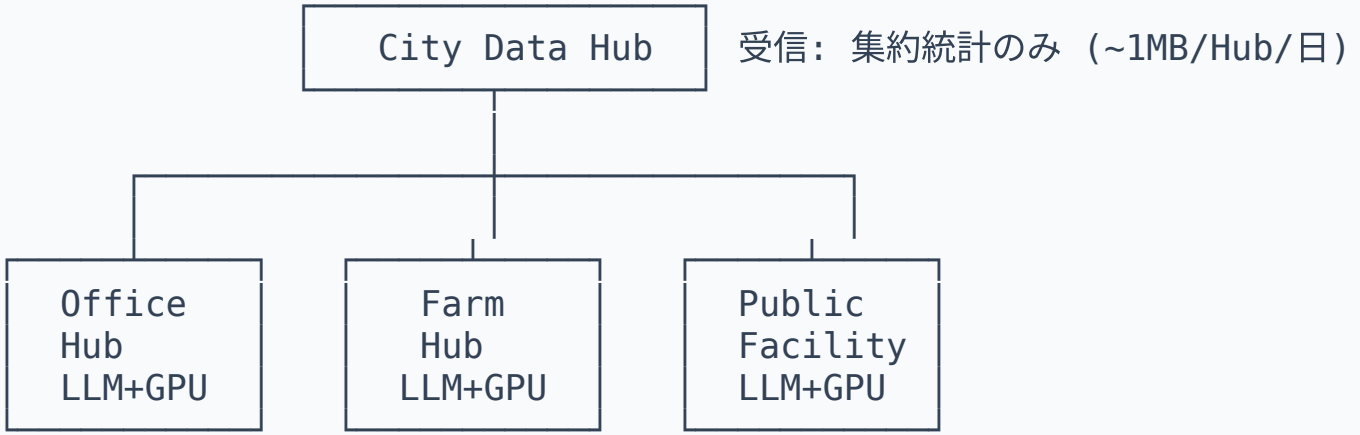
スマートシティの構造的課題

現在の「スマートシティ」には、繰り返し指摘される共通の問題がある。

標榜	実態
データ駆動の都市経営	センサーデータはクラウドに集約。自治体はAPI経由で自身のデータを購入する
AIによるリアルタイム最適化	推論はクラウド上。ネットワーク障害で全機能が停止する
市民のための技術	カメラ映像の保管・アクセス権限が外部企業に帰属する
リアルタイム分析	クラウド往復で数百ms〜秒の遅延。エッジ処理との差は桁違い

データが生まれる場所（建物）と処理される場所（クラウド）が物理的に分離している。ローカルGPUによるLLM推論が実用水準に達した現在、この構造を見直す余地がある。

Core Hub: 建物単位の自律AI拠点



各建物にGPU1台のサーバーを配置し、センサーとカメラの全データをローカルで処理する。Hub間で生データの交換は行わない。システムプロンプト（行動原則）とセンサー構成を差し替えるだけで、オフィス・農場・店舗・公共施設に展開可能。ネットワーク切断時も自律動作を継続する。

三層データ処理: 50,000:1 の圧縮

層	データ量 (1拠点/日)	処理内容
Layer 0: 物理信号	~50 GB	カメラ映像 + 全センサー生値。RAM上で処理、ディスク保存なし
Layer 1: Core Hub	~500 MB	ローカルLLM + YOLOで構造化JSON生成。元データの99%を破棄
Layer 2: City Data Hub	~1 MB	1時間集約の統計値のみ。気温平均、CO2ピーク、在室率

映像はYOLO推論完了と同時に破棄される。Hub本体を物理的に撤去すれば全生データが消失する。GDPRコンプライアンスの最も確実な実現方法: データを送信しないこと。

SOMS: Phase 0 — 1つのオフィスで全機能を実証

SOMS は Core Hub アーキテクチャの最初の実装。オフィス1部屋を対象に、GPU1台 + Docker 11サービスで全フローを動作検証する。クラウド月額費用 $0。

機能	技術	状態
自律判断 (脳)	Qwen2.5 14B, ReActループ (5ツール, 最大5反復, 3層安全機構)	稼働
メッセージバス (神経系)	MQTT + MCP (JSON-RPC 2.0 over MQTT)	稼働
画像認識 (視覚)	YOLOv11 物体検出 + 姿勢推定, 4層活動分析	稼働
環境センサー (触覚)	SensorSwarm Hub+Leaf (4種トランスポート), 6種ドライバ	稼働
音声合成 (声)	VOICEVOX, 拒否ストック100件事前生成, 4トーン	稼働
タスク報酬 (経済)	複式簿記, デマレッジ2%/日, 5%焼却, PWAウォレット	稼働

設計方針: Node-RED・LangChain・Kubernetesを使わない。Python + MQTTによる純粋なイベント駆動。LLM自身がシステム構造を理解できる透明性を優先した。

アーキテクチャ概要

全層がMQTT (Mosquitto) で疎結合に接続。MCP (Model Context Protocol) を MQTT上に実装し、ESP32のような省電力マイコンでもLLMのツール呼び出しに直接応答できる。

動作デモ: CO2検知から解決まで

```
[T+0s]   ESP32センサー: CO2 = 1050ppm (閾値超過)
         → MQTT: office/kitchen/sensor/co2_01/co2 → {"value": 1050}

[T+3s]   ReActサイクル開始 (イベントバッチ遅延完了)
         → LLM: "CO2が高い。3人在室、換気が必要"

[T+4s]   LLM → get_active_tasks() → 既存の換気タスクなし
         → create_task(title="キッチンの換気", bounty=1500, urgency=3)

[T+5s]   Sanitizer検証通過 → タスク作成 + VOICEVOX音声合成

[T+10s]  ダッシュボードにカード表示 + 音声自動再生

[T+??s]  人間が受諾 → 窓を開ける → 完了報告 → Wallet: 1500ポイント振替
```

APIで操作できない物理タスクを、経済的インセンティブで解決する。
全自動ではなく、人間の自由意志を尊重した共生モデル。

SensorSwarm: 建物全体の高密度カバレッジ

WiFi接続のセンサーだけではAP帯域とチャネル干渉がボトルネックになる。SensorSwarmは Hub+Leaf の2層構造でこの制約を回避する。

```
[Brain] ←MQTT→ [SwarmHub (ESP32, WiFi+MQTT)]
                    ├── ESP-NOW → [Leaf: 温湿度] 無線200m, バッテリー駆動
                    ├── UART    → [Leaf: PIR+照度] 有線, Pi Pico
                    ├── I2C     → [Leaf: ドアセンサー] 有線, ATtiny
                    └── BLE     → [Leaf: 計画中] nRF54ターゲット
```

	Hub	Leaf
WiFi	あり (MQTT接続)	不要 (Hub経由)
プロトコル	MCP (JSON-RPC 2.0)	バイナリ (5-245B, XOR checksum)
デバイスID	`swarm_hub_01`	`swarm_hub_01.leaf_env_01`

LeafはWiFiスタック不要で消費電力が低い。バッテリー駆動が実用的になる。Hubが集約してMQTTに発行するため、Brain側からは各Leafが独立したセンサーとして見える。

物理タスク経済: AIと人間の共生

AIが自律判断できても、物理世界への介入手段は限られる。窓を閉める、コーヒーを淹れる、ホワイトボードを拭く——こうした作業はAPIで操作できない。

SOMSの設計: LLMが状況を判断し、タスクを生成し、報酬を提示する。人間が自由意志で受諾し、遂行する。

要素	内容
タスク報酬	500〜5000ポイント (難易度・緊急度に比例)
台帳	複式簿記 (1取引 = DEBIT + CREDIT の2行)
デフレ機構	送金手数料5%焼却 + デマレッジ2%/日
XP乗数	デバイス運用貢献に応じて報酬1.0x〜3.0x
ダッシュボード	アカウント不要のキオスク (タスク表示 + 報酬バッジ + 音声通知)
ウォレットPWA	スマートフォンで残高管理・QRスキャン受取・P2P送金

農場Hubなら「収穫タスク」、店舗Hubなら「品出しタスク」——同じ経済フレームワークが領域を問わず機能する。

データ主権: 物理的な保証

データ分類	処理場所	保存	外部送信
カメラ映像	Core Hub RAM	なし (推論後即破棄)	不可
音声波形	Core Hub RAM	なし	不可
生テレメトリ	Core Hub	Event Store (90日)	不可
LLM判断ログ	Core Hub	Event Store (90日)	不可
集約統計	Core Hub	Data Mart	City Hub送信

暗号化: WPA3 + MQTT over TLS (Sensor→Hub) / TLS 1.3 + mTLS (Hub→City Hub)

ネットワーク障害時はローカルキューに蓄積し、復旧後に一括送信。自律動作は通信状態に依存しない。Hub撤去 = 全生データ消失。これが物理的なデータ主権の保証となる。

都市の呼吸パターン: 分散観測から都市知能へ

複数のCore Hubが稼働するPhase 2以降、単一拠点では見えなかったパターンが浮かび上がる。

```
Hub-A (オフィス街):  CO2ピーク 9:00, 13:00
Hub-B (商業施設):    CO2ピーク 11:00, 15:00, 19:00
Hub-C (住宅街):      CO2ピーク 7:00, 20:00
```

City Data Hubの時空間分析で人流が可視化される:
住宅街 (朝7時) → オフィス街 (9時) → 商業施設 (昼・夕方) → 住宅街 (夜20時)

この洞察を得るために送信したデータ: 各Hubの1時間平均CO2値のみ（数バイト/Hub/時間）。都市計画（換気設備配置、緑地計画）への入力データとなる。

領域特化: 同一アーキテクチャの多領域展開

Hub種別	センサー構成	LLMの行動原則	タスク例
オフィス (SOMS)	温湿度, CO2, カメラ	快適性・健康・生産性	換気, 清掃, 備品補充
農業	pH, EC, 水温, 照度	水耕栽培の生育環境	養液調整, 収穫判断
水槽	水温, pH, TDS	水生生物の環境管理	給餌, 水換え
店舗	人流カメラ, 温湿度	顧客体験と在庫	品出し, 陳列変更
公共施設	騒音, 振動, 気象	安全管理と設備保全	点検, 修繕

全Hubが共通のMCP over MQTTプロトコルとData Martスキーマを使用。City Data Hubは異種Hubのデータを統一的に集約・分析できる。

競合優位性

1. 自律的ローカルAI

各建物がGPU1台で自律的に判断する。クラウド月額費用 $0。ネットワーク切断時も動作を継続。

2. 50,000:1 データ主権

50GBの生データから1MBの構造化統計のみ送信。映像はRAM処理・即時破棄。物理的なプライバシー保証。

3. スケーラブルなエッジ

SensorSwarm Hub+Leafで建物全体を高密度にカバー。WiFi不要のLeafノードはバッテリー駆動が可能。

4. 物理タスク経済

APIで操作できない物理タスクを、人間との経済的な協働で解決する。複式簿記 + デマレッジで経済圏を持続可能に運用。

ロードマップ: 1オフィスから都市へ

Phase	内容	規模	完了条件
0 (現在)	単一オフィスでE2E実証	1 Hub	24h連続稼働, E2E <10秒, 適切判断 >80%
1	多ゾーン + Data Lake	1 Hub, 10+ノード	10+同時接続, 30日蓄積, 月5件の洞察
2	複数Core Hub + City Data Hub	2-3 Hub	Hub間通信99.9%, 孤立72h, クロスHub分析3件+
3	都市展開 + ゼロタッチ配備	10+ Hub	外部送信0B, 都市計画入力1件+

Phase 0で検証した設計要素 — MCP over MQTT, ReActループ, WorldModel, 憲法的AI, per-channelテレメトリ, タスク経済 — はPhase 3の都市展開まで変更不要。

Phase 0 の達成状況と実測パフォーマンス

コンポーネント	状態
ReAct認知ループ (5ツール, 3層安全機構)	稼働
WorldModel (指数減衰加重平均, 4種イベント検知)	稼働
MCP over MQTT (JSON-RPC 2.0, ESP32実機通信済み)	稼働
Perception (YOLOv11 検出+姿勢, 4層活動分析, カメラ自動検出)	稼働
SensorSwarm (Hub+Leaf, ESP-NOW/UART/I2C, バイナリプロトコル)	稼働
Dashboard + Voice + Wallet + PWA	稼働
仮想テスト環境 + E2E統合テスト (7シナリオ)	稼働

AMD RX 9700 (RDNA4) + Qwen2.5 14B (Q4_K_M): LLM推論 ~51 tok/s, 正常時応答 3.3秒, ツール呼び出し 6.6秒

都市をAI化するアーキテクチャ

> データの処理を建物内で完結させ、最小限の構造化情報だけを共有する。
> 単一拠点では見えなかった都市規模のパターンが、そこから浮かび上がる。

GPU1台。Docker 11サービス。クラウド月額 $0。50,000:1 のデータ圧縮。

1つのオフィスから始まる、都市のAI化。

GitHub: `Office_as_AI_ToyBox`